第3部 情報の取扱い

3.1 情報の取扱い

3.1.1 情報の取扱い

目的・趣旨

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下本款において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての職員等が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、職員等は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

なお、国の行政機関における秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本統一基準の規定に基づき、適切に情報が取り扱われるよう留意すること。また、独立行政法人及び指定法人における機密性３情報の管理に関しては、本統一基準の規定に基づき対策を講ずること。

遵守事項

(1) 情報の取扱いに係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。

（ア） 情報の**格付及び取扱制限についての定義**

（イ） 情報の**格付及び取扱制限の明示等**についての手続

（ウ） 情報の格付及び取扱制限の継承、見直しに関する手続

【 基本対策事項 】

＜3.1.1(1)(a)関連＞

3.1.1(1)-1 統括情報セキュリティ責任者は、情報の取扱いに関する運用規程として、以下を全て含む**手順を整備**すること。

a) 情報のライフサイクル全般にわたり必要な手順（業務の遂行以外の目的での情報の利用等の禁止等）

b) 情報の入手・作成時の手順

c) 情報の利用・保存時の手順

d) 情報の提供・公表時の手順

e) 情報の運搬・送信時の手順

f) 情報の消去時の手順
g) 情報のバックアップ時の手順

＜3.1.1(1)(a)(イ)関連＞

3.1.1(1)-2 統括情報セキュリティ責任者は、情報の格付及び取扱制限の**明示の方法**について、以下を例とする内容を、情報の取扱いに関する運用規程に含めて整備すること。

a) 電磁的記録として取り扱われる情報に明示する場合
- 電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
- 電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
- フォルダ単位等で取り扱う情報は、フォルダ名に記載
- 電子メールで取り扱う情報は、電子メール本文又は電子メール件名に記載
- チャットツールで取り扱う情報は、**チャットルーム名等に記載**

b) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合
- 保存する電磁的ファイル又は文書等の単位ごとに記載
- 外部電磁的記録媒体本体に記載

c) 書面に印刷されることが想定される場合
- 書面のヘッダ部分等に記載
- 冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載

d) 既に書面として存在している情報に対して格付や取扱制限を明示する場合
- 手書きによる記入
- スタンプ等による押印

3.1.1(1)-3 統括情報セキュリティ責任者は、情報の格付及び取扱制限の**明示を省略**する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、情報の取扱いに関する運用規程に含めて整備すること。

＜3.1.1(1)(a)(ウ)関連＞

3.1.1(1)-4 統括情報セキュリティ責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例とする内容を、情報の取扱いに関する運用規程に含めて整備すること。

a) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承すること。

b) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直すこと。

c) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直すこと。

d) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

e) 完全性及び可用性については、作成時又は**複製時に適切な格付を決定**すること。

f) 他者が決定した情報の格付及び取扱制限を**見直す必要がある場合**には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本款において「決定者等」という。）に確認を求めること。

（解説）

- **遵守事項 3.1.1(1)(a)(ア)「格付及び取扱制限についての定義」について**

「統一基準 1.2 (1) 情報の格付の区分」及び「統一基準 1.2 (2) 情報の取扱制限」にて規定している情報の格付及び取扱制限の定義に基づき、機密性、完全性、可用性に係る情報の格付と取扱制限について、機関等の基準を整備する必要がある。取扱制限については、1.2(2)【参考４】取扱制限の例も参照のこと。

なお、文書管理ガイドラインにおいて、「文書の作成者は、当該文書が極秘文書又は秘文書に該当すると考えられる場合には、それぞれに準じた管理を開始する」とされており、指定前の秘密文書も、機密性３情報として管理することが求められる。また、独立行政法人及び指定法人における機密性３情報についても同様の管理が求められるが、法人において機密性３情報を取り扱わない場合は、統一基準群における機密性３情報に係る規定について、対策基準の策定においてその必要性も含め検討し、法人の実情に合わせて規定するとよい。

- **遵守事項 3.1.1(1)(a)(イ)「格付及び取扱制限の明示等」について**

秘密文書においては、文書管理ガイドラインにおける「秘密文書表示」を行った場合には、別途「機密性３情報」に係る明示等を行う必要はない。

- **基本対策事項 3.1.1(1)-1「手順を整備」について**

a)～g)は、遵守事項 3.1.1(2)～(8)における職員等を名宛人とした対策事項とそれぞれ対応している。本事項では、これらの内容を包含する形で手順を定めることを求めている。

- **基本対策事項 3.1.1(1)-2「明示の方法」について**

当該情報を参照する者が、情報の格付及び取扱制限を確実に視認することができるよう、当該情報に記載することによる明示を原則とする。また、情報の格付及び取扱制限の明示については、以下の事項についても留意が必要である。

  - 本文において格付を明示することに加え、ファイル名の先頭に格付を付す。(例：「【機２】○○整備計画」)
  - 格付及び取扱制限の明示と併せて、情報の作成者又は入手者の氏名、所属、連絡先等も記載する。
  - 文書の一部の情報に取扱制限を追加するときは、追加する取扱制限を当該情報に近接した場所に明記する。
  - 電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記する。
  - 文書の作成者名、組織名その他の記録に使用できる「プロパティ」に格付の区分を記載することは明示に当たらない。

- **基本対策事項 3.1.1(1)-2 a)「電子メール本文又は電子メール件名に記載」について**

電子メールを引用する場合は、引用する電子メールで取り扱っている情報の機密性に係る格付及び取扱制限を継承した上で、作成する電子メールが上位の格付及び取扱

制限の情報を取り扱う場合は、その反映に留意が必要である。

- **基本対策事項 3.1.1(1)-2 a)「チャットルーム名等に記載」について**

チャットツールで情報を取り扱う場合は、チャットツールで投稿するメッセージごとに格付及び取扱制限を記載することは運用上困難であることが想定されることから、チャットルームのルーム名等、チャットルームの参加者全てが確実に視認できる箇所に情報の格付及び取扱制限を記載することが考えられる。

また、チャットツールの利用者が職員等に限定されており、かつ、チャットツールで取り扱うことのできる情報の格付及び取扱制限をチャットツールの利用手順書等に明記した上で利用者である職員等に周知されている場合等、チャットツールの利用者全てがチャットツールで取り扱う情報の格付及び取扱制限について共通の認識となる場合においては、基本対策事項 3.1.1(1)-3 を参考に明示を省略することも考えられる。

- **基本対策事項 3.1.1(1)-3「明示を省略」について**

情報の格付及び取扱制限を確実に視認することができるよう、当該情報に明示しておくことが原則ではあるが、必要な場合には、以下を例に明示が省略可能な条件について定めておくとよい。

- 情報システムに記録される情報の格付及び取扱制限を当該情報システムの手順書等により明記し、当該情報システムの利用者にあらかじめ周知している場合
- 情報の格付及び取扱制限の省略時における当該情報の格付及び取扱制限の取扱について、取扱手順に規定し、職員等にあらかじめ周知している場合

ただし、格付及び取扱制限の明示を省略した場合には、以下の事項に注意が必要である。

- 格付及び取扱制限の省略を認識できない者への情報の提供

  格付の区分及び取扱制限が明示されていない要保護情報を、格付及び取扱制限の決定内容を認識できない職員等に提供する必要が生じた場合（例えば、他機関等に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限を明示した上で提供するなどしなければならない。
- 取扱制限の明示を省略した場合における取扱制限の追加・変更

  例えば、ある文書の取扱制限の明示を省略している場合であって、当該文書の一部に取扱制限を追加するときは、追加する取扱制限を明示すること。

- **基本対策事項 3.1.1(1)-4 e)「複製時に適切な格付を決定」について**

複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、完全性及び可用性については、適宜、複製の目的に応じて格付を決定する必要がある。

- **基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について**

利用する元の情報への修正、追加又は削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は当該決定

者の上司に相談し、その是非を検討することになる。決定者等による見直しが無い限り、当該情報の利用者がこれらの者に無断で、格付又は取扱制限を変更することは許されない。

なお、見直しを行わなければならない場合については、以下を参考に規定すること。

- 作成時には要機密情報だった情報の機密性が失われた場合（時間の経過により変化した場合）
- 機密性３情報として格付されている資料等から機密性３情報に係る部分を全て削除した場合
- 取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
- 取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合
- 格付及び取扱制限を決定した際の判断が不適切であったと考えられる場合
- 行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等における情報の取扱いに変更がある場合

遵守事項

(2) 情報の目的外での利用等の禁止

(a) 職員等は、自らが担当している業務の遂行のために必要な範囲に限って、**情報を利用等**すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(2)(a)「情報を利用等」について**

情報は、業務の目的を達成するために利用等するのであって、業務の遂行以外の目的で情報を利用等すべきではない。国家公務員法 第100条 第1項においても、「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。」と定められている。

情報の目的外利用に当たる場合としては、例えば、業務上知り得た情報をソーシャルメディアの個人アカウントの掲示板等に掲示する、私的にウェブ上の各種サービス（SNS 等）を利用する際に、業務に使用しているメールアドレスと主体認証情報を利用するなどの行為が考えられる。その他にも、情報の利用形態は様々であり、注意が必要である。

なお、本条で対象としている情報は、職員等が従事する業務において利用する機関等の情報システムから入手可能な業務に係る情報（業務上知り得る情報）や、情報システムにおいて利用される主体認証情報（パスワード等）であり、情報システムの仕様やデータ設定等に係る情報（メールアドレス等）も含んでいる。一方、業務時間外に自宅等の私物端末から機関等のウェブサイトにアクセスして、公表されている情報を入手するなどの行為については、本条の対象とはしていない。

遵守事項

(3) 情報の格付及び取扱制限の決定・明示等

(a) 職員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき**格付及び取扱制限を決定**し、明示等すること。

(b) 職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を**継承**すること。

(c) 職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「**決定者等**」という。）**に確認し、その結果に基づき見直す**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(3)(a)「格付及び取扱制限を決定」について**

格付及び取扱制限が不十分な場合、情報漏えい等のリスクが高まるが、一方で、情報の利用を円滑に行うためには、格付及び取扱制限を必要以上に高くしないようにする必要がある。そのため、格付及び取扱制限を決定する際には、機関等の基準に照らして、要件に過不足が生じないようにすること。例えば、機密性１情報に相当する公開しても差し支えない情報をむやみに要機密情報に決定すると、過度な保護対策を求めることになり、業務の効率的な運営に支障をきたすおそれがある。

また、他機関等との情報の受け渡しを行う際には、統一基準との格付定義の差分に関する情報を当該機関等から得るなどして、自機関等の基準との差分について考慮の上、格付及び取扱制限を決定する必要がある。

- **遵守事項 3.1.1(3)(b)「継承」について**

業務資料等を参考に新たに別の資料を作成する場合等において、元となった資料等に記載されていた情報の機密性に関する格付及び取扱制限について、新たに作成した資料等に適切に引き継ぐことを求めている。例えば機密性３情報を他の資料等に転用する場合においては、当該資料に記載されている転用部分については機密性３情報として取り扱われるべきである。また、要保全情報又は要安定情報を複製する場合については、複製された情報に対して過度な保護対策を求めないように、完全性１情報又は可用性１情報として格付を見直し再決定することが望ましい。ただし、バックアップを原本として情報を保管する目的で複写する場合は、要保全情報とすべきであるなど、状況に応じた適切な判断が求められる。

- **遵守事項 3.1.1(3)(c)「決定者等に確認し、その結果に基づき見直す」について**

  「（解説）基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照のこと。

遵守事項

(4) 情報の利用・保存

(a) 職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ること。

(c) 職員等は、要保護情報について**要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること**。

(d) 職員等は、**保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること**。なお、**独立行政法人及び指定法人における職員等**は、機密性３情報を機器等に保存する際、以下の措置を講ずること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

(ア) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。

(イ) 当該情報に対し、暗号化による保護を行うこと。

(ウ) 当該情報を保存した機器等について、**盗難及び不正な持ち出し等の物理的な脅威から保護するための対策**を講ずること。

(e) 職員等は、USB メモリ等の**外部電磁的記録媒体**を用いて情報を取り扱う際、**定められた利用手順**に従うこと。

【 基本対策事項 】

＜3.1.1(4)(a)(d)関連＞

3.1.1(4)-1 職員等は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講ずること。

a) 要保護情報を**放置しない**こと。

b) 要機密情報を**必要以上に複製しない**こと。

c) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずること。

d) 電磁的記録媒体に要保全情報を保存する場合には、**電子署名の付与を行うなど**、改ざん防止のための措置を講ずること。

e) 情報の**保存方法を変更**する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずること。

3.1.1(4)-2 職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

（解説）

- **遵守事項 3.1.1(4)(c)「要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること」について**

機関等外で開催される会議への出席等の際に、要機密情報を用いて情報処理を行う場合は、のぞき見の防止や不要となった情報の削除等の措置を講ずるなど、情報の格付や取扱制限に応じて適切な安全管理措置を講ずる必要がある。この際、技術的な対策については、遵守事項 6.1.2(1)(b)及び遵守事項 6.1.3(2)(c)に基づき定められた安全管理措置を参考にするとよい。

- **遵守事項 3.1.1(4)(d)「保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること」について**

情報システムに、ファイルに対する書込権限者の制限や、ファイルのセキュリティ設定でパスワード設定等のアクセス制御機能が装備されている場合、当該情報の格付及び取扱制限に従って、必要なアクセス制御の設定を行うことが求められる。例えば、取扱制限として閲覧範囲の制限が指定されている場合は、第三者等から参照されないよう、読取制限の属性を付与することや、要保全情報であれば、第三者等から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

アクセス制御は、サーバ装置、端末、OS、アプリケーション、ファイル等を単位に行うことができるため、これらを選択し組み合わせて、適切なアクセス制御を実現するとよい。

なお、文書管理ガイドラインの秘密文書の管理に関するモデル要領において、「秘密文書については、インターネットに接続していない電子計算機又は媒体等に保存し、暗号化等による保護を行うとともに、当該秘密文書を記録する電子計算機、媒体等について、保存を金庫等で行うなどにより物理的な盗難防止措置を施すこと。秘文書については、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機でも保存することができる。」とされている。

- **遵守事項 3.1.1(4)(d)「独立行政法人及び指定法人における職員等」について**

本項(ア)から(ウ)の各号は、独立行政法人及び指定法人の職員等が機密性３情報を取り扱う場合において、文書管理ガイドラインの求める秘密文書の管理と同等の対策となるよう規定している。文書管理ガイドラインでは秘密文書を極秘文書と秘文書に区分しているが、独立行政法人及び指定法人は当該ガイドラインの対象外であることから、当該ガイドラインが求める秘密文書の管理がなされているとは限らないため、本項各号は秘密文書の中でもより高い水準のセキュリティ対策が求められる極秘文書相当の対策となっている。

ただし、国の行政機関と同様に文書管理ガイドラインの秘密文書の管理に基づき機密性３情報を極秘文書と秘文書に区分し、国の行政機関と同等の管理を行っている独立行政法人及び指定法人においては、秘文書に相当する情報については秘文書相当の対策を講ずることをもって代えることも可能である。（文書管理ガイドラインの秘密文書の管理に関するモデル要領については、「（解説）遵守事項 3.1.1(4)(d)「保存する情報

にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること」について」を参照のこと。）

- **遵守事項 3.1.1(4)(d)(ウ)「盗難及び不正な持ち出し等の物理的な脅威から保護するための対策」について**

  端末についての対策例は基本対策事項 6.1.1(1)-2、サーバ装置についての対策例は基本対策事項 6.2.1(1)-2 を参照のこと。

- **遵守事項 3.1.1(4)(e)「外部電磁的記録媒体」について**

  外部電磁的記録媒体には、USB メモリ等の、繰返し情報を書き換えできる媒体と、CD-R 等の書き換えできない媒体が存在する。特に前者の媒体を利用する場合は、不正プログラムに感染するおそれが大きいため、その取扱いには細心の注意が必要である。（具体的な対策等については、【参考 8.1.1-1】を参照のこと。）

- **遵守事項 3.1.1(4)(e)「定められた利用手順」について**

  遵守事項 8.1.1(1)(b)において定められた実施手順を指す。

- **基本対策事項 3.1.1(4)-1 a)「放置しない」について**

  悪意ある第三者等による不正な操作や盗み見等を防止することを求める事項である。例えば、離席する際には、ロック付きスクリーンセーバを起動する又はログアウトして画面に情報を表示しない、机の上に書類を放置して長時間離席しない、印刷した書面を速やかに回収し出力トレイに放置しないこと等を徹底する必要がある。

- **基本対策事項 3.1.1(4)-1 b)「必要以上に複製しない」について**

  電磁的記録は比較的容易に複製することができるという特性があり、可用性の観点から複製された情報が多数の端末に散在する傾向になることが想定されるため、機密性３情報に該当しない情報であっても、複製は必要最小限にとどめるよう留意が必要である。

  なお、秘密文書に関しては、文書管理ガイドラインにおいて、「秘密文書の複製等は必要最小限にとどめること。」と定められていることに留意が必要である。

- **基本対策事項 3.1.1(4)-1 d)「電子署名の付与を行うなど」について**

  改ざん防止のための措置としては、電子署名を付与することや、情報を更新する必要がある主体に対してのみ更新権限を付与すること等が考えられる。保護を行う情報の格付、取扱制限等に応じて適切な措置を講ずるとよい。

  電子署名を付与した場合、電子署名を付与した者が真正であること、電子署名が付与された情報が改ざんされていないことを検証することができる。しかし、電子署名を付与するだけでは、電子署名が付与された情報がどの時点において存在していたかを検証することができない。

  この検証を可能とするためにはタイムスタンプを付与する必要がある。タイムスタンプを付与することによって、タイムスタンプを付与した時点において情報が存在していたこと、また、タイムスタンプを付与した後に情報が改ざんされていないことを検証することができる。

検証できることが電子署名とタイムスタンプによって異なることを踏まえ、情報の格付及び取扱制限に応じて適切な方法を用いるとよい。

なお、電子署名やタイムスタンプにはどちらも有効期限が存在する。電子署名やタイムスタンプの有効期限が切れた後においても電磁的記録媒体に保存する要保全情報に対して改ざん防止のための措置を講ずる必要がある場合は、さらに新たなタイムスタンプを付与することによって、電子署名やタイムスタンプの有効期限後であっても検証が可能となる、長期署名の仕組みを利用するとよい。

当該仕組みを利用できない場合は、原則として「電子政府推奨暗号リスト」に記載された暗号化方式を用いた電子署名を当該情報に再度付与する方法も考えられる。しかし、この方法を用いる場合はタイムスタンプを付与しないため、電子署名が再度付与された情報がどの時点において存在していたかを検証することができないことに留意が必要である。

- **基本対策事項 3.1.1(4)-1 e)「保存方法を変更」について**

  当該情報が記載されている文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか、利用の制限についての意見を付すなどして移管する必要がある。その際、パスワードを設定していた場合は解除するなどして、移管先がその内容を参照できるように配慮が必要である。

遵守事項

(5) 情報の提供・公表

(a) 職員等は、情報を公表する場合には、当該情報が**機密性１情報に格付されるもの**であることを確認すること。

(b) 職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の**決定者等に相談**し、その決定に従うこと。また、**提供先において**、当該情報に付された格付及び取扱制限に応じて**適切に取り扱われるよう**、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

(c) 独立行政法人及び指定法人における職員等は、機密性３情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。

(d) 職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの**不用意な情報漏えい**を防止するための措置を講ずること。

【 基本対策事項 】

＜3.1.1(5)(d)関連＞

3.1.1(5)-1 職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

（解説）

- **遵守事項 3.1.1(5)(a)「機密性１情報に格付されるもの」について**

保有する情報をウェブサイト等により広く国民に提供する場合、公表しようとする情報の格付の適正さを再度検討し、格付及び取扱制限の明示を削除するなどを考慮する必要がある。

なお、情報の公表ではないものの、電子調達システム等において調達情報を委託先候補事業者に閲覧を許可する場合が考えられる。情報システムの構成図等サイバー攻撃を企図する者が有利になるような情報については、開示対象者と機密保持契約を締結するなどして厳重な管理のもと閲覧を許可するなど、細心の注意が必要である。

- **遵守事項 3.1.1(5)(b)「決定者等に相談」について**

「(解説) 基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照のこと。

- **遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について**

要保護情報を機関等外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の取扱い上の留意事項を提供先へ確実に伝達する必要がある。

伝達方法としては、他機関等や委託先等の情報の提供先に、対策基準や情報の取扱いに関する手順書、統一基準との格付定義の差分に関する説明等を提示し、格付や取扱制限に応じた取扱方法を示す方法が考えられる。この場合、格付の区分だけを示しても、提供先においては当該格付区分がどのように取り扱われるべきものであるか認識でき

ない可能性があるため、当該格付の区分の定義について提供先に事前に周知する必要がある。また、提供する情報を適切に管理するために必要な措置が具体的に分かるようにする（例えば、「委員以外への再配布を禁止する」と明示する。）など、格付以外の方法で取扱方法を示すことも考慮する必要がある。

- **遵守事項 3.1.1(5)(d)「不用意な情報漏えい」について**

  情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。

  また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

遵守事項

(6) 情報の運搬・送信

(a) 職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

(b) 職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

【 基本対策事項 】

＜3.1.1(6)(a)関連＞

3.1.1(6)-1 職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、**セキュアな運送サービス**を提供する運送事業者により運搬すること。

3.1.1(6)-2 職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬する場合には、以下を例とする情報漏えいを防止するための対策を講ずること。

a) **運搬する情報を暗号化する**こと。

b) 分割後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を**複数の情報に分割し**、それぞれ異なる経路及び手段を用いて運搬すること。

c) 主体認証機能や暗号化機能等を備える**セキュアな外部電磁的記録媒体**を利用すること。

＜3.1.1(6)(b)関連＞

3.1.1(6)-3 職員等は、要機密情報である電磁的記録を機関等外通信回線を使用して送信する場合には、以下を例とする情報漏えいを防止するための対策を講ずること。

a) **送信する情報を暗号化する**こと。

b) **通信経路全般が暗号化**されている通信経路を用いて送信すること。

c) 分割後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を**複数の情報に分割し**、それぞれ異なる経路及び手段を用いて送信すること。

3.1.1(6)-4 職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

a) 機関等管理の通信回線を用いて送信すること。

b) 信頼できる通信回線を使用して送信すること。

c) VPN を用いて送信すること。

d) S/MIME 等の暗号化された電子メールを使用して送信すること。

e) 機関等独自で運用している又は機関等が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用すること。

（解説）

- **基本対策事項 3.1.1(6)-1「セキュアな運送サービス」について**

運搬する情報の内容により、受取の際に本人確認を行うサービス（例えば、本人限定受取郵便）や、専用車両による配達サービス、配達状況の追跡が可能なサービス等から、必要なサービスを選定することが求められる。

- **基本対策事項 3.1.1(6)-2 a)「運搬する情報を暗号化する」について**

暗号化する際に設定するパスワードやパスフレーズ（以下本解説において「鍵」という。）は、十分な長さと複雑さを有することが求められる。また、鍵を暗号化された情報と同じ経路で送信等したり、第三者が容易に知り得る方法で送信等したりしてしまうと、第三者によって情報が復号されるおそれが高くなると考えられることから、例えば、事前の面会時に共有しておいたり、事前に共有できない場合は暗号化された情報とは別の経路で送信するなどして秘匿性を確保することが必要である。

十分な長さと複雑さを有する鍵としては、例えば、パスワードエントロピーとして 128 ビットを要する（パスワードの解析に 2 の 128 乗回の試行を要する）とした場合、英大文字・英小文字・数字（62 種の文字）を用いたランダム生成では、22 文字程度が必要であると言える。利用者が記憶しやすいランダム生成の鍵として、ランダムに複数の単語を選んでつなげる場合には、例えば、11 万語の辞書からであれば 8 語、2 万語の辞書からであれば 9 語程度を用いる必要があると言える。

十分な長さと複雑さの鍵の使用を利用者に守らせるためには、鍵のランダム生成を支援する機能を提供することが考えられる。

なお、暗号化する際に用いる暗号アルゴリズムや鍵長などの暗号化方式は、遵守事項 8.1.1(7)(a)の規定に従い、定められた暗号化方式を用いる必要がある。

- **基本対策事項 3.1.1(6)-2 b)・基本対策事項 3.1.1(6)-3 c)「複数の情報に分割し」について**

暗号技術の一種である秘密分散技術を用いて、秘匿すべき情報を複数のデータに分割することで、そのうちの一つを窃取しても元の情報を一切復元できないようにすることができる。この分割されたデータのそれぞれを異なる経路で運搬・送信する（例えば、片方を電子メールで送信し、もう片方を DVD や USB メモリ等の外部電磁的記録

媒体で郵送するなど）ことにより、情報漏えいを防止することができる。なお、秘密分散技術自体が暗号技術の一種であるので、これにより分割されたデータをさらに暗号化する必要はなく、暗号鍵も必要ない。

- **基本対策事項 3.1.1(6)-2 c)「セキュアな外部電磁的記録媒体」について**

セキュアな外部電磁的記録媒体が備える機能としては、主体認証機能、暗号化機能の他、不正プログラムの検閲・駆除機能、遠隔データ消去機能、接続管理機能等がある。USB メモリ等の外部電磁的記録媒体の運搬に当たっては、必要最小限の情報のみを保存するよう留意するとともに、盗難・紛失等による情報漏えいに備え、当該機能を適切に利用する必要がある。

- **基本対策事項 3.1.1(6)-3 a)「送信する情報を暗号化する」について**

暗号化する際に設定するパスワードやパスフレーズ（以下本解説において「鍵」という。）の長さや複雑さ等については、「（解説）基本対策事項 3.1.1(6)-2 a)「運搬する情報を暗号化する」について」を参照のこと。

本基本対策事項は、送信する情報自体を暗号化することを求めている。送信する情報自体を暗号化することによって、暗号化通信がなされていない通信経路において盗聴が行われた場合でも、暗号化された情報の漏えいを防止することができる。

一方、鍵を送信先に伝える際には、暗号化された情報と同じ経路で鍵を送信する方法（いわゆる PPAP）等を用いることにより、第三者によって情報が復号されるおそれが高くなるため、留意すべき点が存在する。当該留意点は「（解説）基本対策事項 3.1.1(6)-2 a)「運搬する情報を暗号化する」について」を参照のこと。また、電子メールに本基本対策事項を実施した場合の例として、要機密情報が含まれているファイルを暗号化して添付し、送信することが挙げられるが、受信側の電子メールサーバ等において、電子メールに添付された暗号化ファイルを破棄する対策が行われている場合、添付された暗号化ファイルが受信者に届かないことにも留意が必要である。

- **基本対策事項 3.1.1(6)-3 b)「通信経路全般が暗号化」について**

通信経路における盗聴による情報漏えいを防止するために、通信経路全般における暗号化通信を求めている。

例えば、オンラインストレージ等のファイル共有サービスを利用する場合、機関等外通信回線に接続された機器とファイル共有サービスの間の通信において TLS 通信等の暗号化通信が確実に実施されている場合は、通信経路全般が暗号化されていると考えられる。なお、通信経路上の機器において監視を目的とした復号が行われている場合がある。この場合は、復号を行う目的が情報窃取等の不正な目的ではないことが確認できた場合等、通信経路の途中で復号されたとしても情報漏えいの可能性がないと判断できる場合は、通信経路全般が暗号化されていると考えられる。

また、情報を送受信する機器同士においてエンドツーエンド（E2E）の暗号化を行っている場合も、通信経路全般が暗号化されていると考えられる。

なお、機関等外の者に電子メールを送信する場合、基本対策事項 6.2.2(1)-6 a)で規定する SMTP による電子メールサーバ間通信を TLS による保護を行う対策では、最終的

な受信先の電子メールサーバまでの通信及び電子メールサーバと電子メールクライアント間の通信が全て保護されることは保証されていないため、必ずしも通信経路全般が暗号化されていると考えることができないことに留意が必要である。

- **基本対策事項 3.1.1(6)-4 b)「信頼できる通信回線」について**

  例えば、空港や商業施設等が提供する無線 LAN 等の通信回線は、秘匿性や安全性、管理状況が不明であり、通信内容の盗聴やなりすましによる情報の窃取等のおそれがあるため、要保護情報を送信する場合にこれを用いるべきではない。ただし、「(解説)基本対策事項 3.1.1(6)-4 c)「VPN」について」に記載のとおり、端末等と情報システムとの間で VPN 接続等による通信の暗号化を実施する場合は、この限りでない。

- **基本対策事項 3.1.1(6)-4 c)「VPN」について**

  例えば、モバイル通信網を経由して端末等をインターネットに接続させる装置（以下本解説において「モバイル通信網接続装置」という。無線 LAN 接続型や USB 接続型などがある。）を利用して、外部から機関等の情報システムにアクセスする場合、仮にモバイル通信網接続装置が利用者の意図しない不正な動作をしていたとしても、VPN 接続等による通信の暗号化を実施することで、機密性の格付によらず当該機器による情報漏えいを防止することができる。ただし、この場合は、モバイル通信網接続装置の VPN 機能を利用するのではなく、端末等と当該情報システムとの間で VPN 接続を確立する必要がある。これは、端末等と当該情報システムとの間で VPN 接続が確立されていれば、モバイル通信網接続装置上を流れる通信は暗号化されているため、モバイル通信網接続装置上における盗聴による情報漏えい等を防止することが可能となるためである。なお、USB 接続型のモバイル通信網接続装置の利用に際しては、上記に加え、一般の USB メモリと同様に USB 接続についての安全性にも配慮する必要がある。

- **基本対策事項 3.1.1(6)-4 e)「機関等独自で運用している又は機関等が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境」について**

  情報の漏えい、改ざん、利用不可能となる脅威への対策、情報セキュリティインシデント発生時の対処等が適切に実施されている等の、セキュリティが十分に確保されたウェブメールサービス又はオンラインストレージ環境を利用する必要がある。

  機関等独自で運用している場合は、統一基準群に従った運用がなされているため、セキュリティが十分に確保されていると考えられる。また、クラウドサービスを利用する場合は、セキュリティが十分確保されていることを機関等が確認した上で利用の承認しているクラウドサービスを利用する必要がある。クラウドサービスを利用して要機密情報を取り扱う場合は、4.2.1「クラウドサービスの選定（要機密情報を取り扱う場合）」及び 4.2.2「クラウドサービスの利用（要機密情報を取り扱う場合）」、クラウドサービスを利用して要機密情報を取り扱わない場合は、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」を参照のこと。

遵守事項

(7) 情報の消去

(a) 職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

(b) 職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

(c) 職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

【 基本対策事項 】

＜3.1.1(7)(b)関連＞

3.1.1(7)-1 職員等は、端末やサーバ装置等をリース契約で調達する場合は、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、以下を例とする対策を行うこと。

a) リース契約の調達仕様書に記載し、契約内容にも含めること。

b) リース契約終了に伴う情報の抹消について、役務提供契約を別途締結すること。

（解説）

- **遵守事項 3.1.1(7)(a)「速やかに情報を消去」について**

情報セキュリティの観点からは、不正プログラム感染による情報窃取や操作ミスによる情報漏えい等を防ぐ観点から、職務上不要となった情報を速やかに消去する必要があるが、その際には、公文書管理法等で保存が求められる情報を誤って消去しないよう、注意が必要である。

- **遵守事項 3.1.1(7)(b)「抹消する」について**

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法を、「表 3.1.1-1　情報の抹消方法の例」に例示する。

表 3.1.1-1　情報の抹消方法の例

種類	情報の抹消方法	電磁的記録媒体（例）	情報の機密性	
			低い	高い
消去	データ抹消ソフトウェア （もとのデータに異なるランダムなデータを複数回上書きすることで抹消する）	ﾊｰﾄﾞﾃﾞｨｽｸ SSD USB ﾒﾓﾘ	○	－
	ATA コマンド「SECURITY ERASE UNIT」	SSD	○	－
除去	暗号化消去 （情報を電磁的記録媒体に暗号化して記録しておき、情報の復号に用いる鍵を抹消することで情報の復号を不可能にする）	ﾊｰﾄﾞﾃﾞｨｽｸ SSD	○	○
	ATA コマンド「Enhanced SECURITY ERASE UNIT」	ﾊｰﾄﾞﾃﾞｨｽｸ	○	○
	SCSI コマンド「SCSI SANITIZE」や「SCSI Format」	ﾊｰﾄﾞﾃﾞｨｽｸ SSD	○	○
	ATA コマンド「BLOCK ERASE」	SSD	○	○
	消磁 （磁気記録方式に対応した消磁装置に入れて媒体内の全てのデータを抹消する）	ﾊｰﾄﾞﾃﾞｨｽｸ	○	○
破壊	物理的破壊 （媒体種類に応じた専用の破壊装置等で媒体を溶融・粉砕・焼却・細断するなどしてデータ復旧が不可能となるまで破壊する）	ﾊｰﾄﾞﾃﾞｨｽｸ SSD USB ﾒﾓﾘ 光学媒体	○	○

○：適用可

－：適用不可

暗号化消去は、情報の抹消が高速に行えることや部分的な抹消が行えること等のメリットがあるため、機密性の高さによらず、抹消するための方法として優先的に検討するとよい。

また、クラウドサービスの利用を終了する際のクラウドサービスで取り扱った要機密情報を廃棄する方法については、遵守事項 4.2.2(5)「クラウドサービスを利用した情報システムの更改・廃棄時の対策」を参照のこと。

なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施し実施結果の記録を残すことや情報の抹消を外部の民間事業者等へ業務委託することも考えられ

るが、業務委託を実施する場合は、情報が適正に抹消されたことの証拠となる記録及び証明書の提出を求める、職員等による立ち合いを行う等、委託先での履行状況を確認することが重要である。

- **遵守事項 3.1.1(7)(c)「復元が困難な状態にする」について**

  電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却、溶解等により、復元が困難な状態にする必要がある。

  なお、廃棄すべき書類が大量にあるなどの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。また、無人の執務室に設置されている又は設置場所及び利用場所が確定していないなどの環境で利用される情報システム、外部電磁的記録媒体等については、不要な情報を可能な限り事前に抹消することが望ましい。

- **基本対策事項 3.1.1(7)-1「返却時の情報の抹消方法」について**

  リース契約で調達した機器を返却する時の情報の抹消方法として暗号化消去を採用する場合、CRYPTREC「電子政府推奨暗号リスト」に記載の安全性及び実装性能が確認された暗号アルゴリズムを使用し、OS やハードウェアの機能により、電磁的記録媒体へ書き込まれる情報が自動的に暗号化されるように設定された端末やサーバ装置等を導入し、運用の全期間を通じて暗号化することが前提となる。

  また、暗号化された情報の復号に用いる鍵については、基本対策事項 7.1.5(1)-3 b)で策定を求めている管理手順に従って適切に管理するとともに、暗号化消去を行う際にはバックアップも含め鍵を確実に消去することが重要である。

  さらに、暗号化消去による情報の抹消処理の信頼性を担保するため、暗号化消去の実施記録を残しておくことが望ましい。

遵守事項

(8) 情報のバックアップ

(a) 職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

(b) 職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。

(c) 職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

【 基本対策事項 】

＜3.1.1(8)(a)関連＞

3.1.1(8)-1 職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。

＜3.1.1(8)(b)関連＞

3.1.1(8)-2 職員等は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。要保全情報又は要安定情報である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、以下を例とする情報システムや情報とバックアップが同時に破壊されない保管場所を選定すること。

a) バックアップ取得元の情報システムが接続するネットワークから物理的に隔離された保管場所

b) バックアップ取得元の情報システムが接続するネットワークから論理的に隔離された保管場所

（解説）

- **遵守事項 3.1.1(8)(a)「適切な方法で情報のバックアップを実施する」について**

災害や情報セキュリティインシデント等の危機的事象が発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。以下の例を参考に、情報のバックアップ方法について考慮するとよい。

- 想定する危機的事象（地震、津波、火災、高出力電磁波、感染症、情報セキュリティインシデント等）
- バックアップの対象（対象とするシステム、データ、ソフトウェアその他）
- バックアップの範囲（フルバックアップ、差分バックアップ等）
- バックアップを保存する電磁的記録媒体等の種類
- バックアップの周期、頻度、世代管理の方法
- 使用するバックアップツール

- バックアップデータの秘匿性確保、改ざん防止の方法

バックアップの周期を短くすることで、危機的事象発生時点に近い状態に復旧できる可能性が高くなるため、バックアップの周期は可能な限り短くすることが望ましい。

しかし、サイバー攻撃を検知するまでに長期間を要する不正プログラムの存在が確認されており、バックアップの周期が短く、かつ、保存しているバックアップの世代が少ない場合は、バックアップしている全ての世代に不正プログラムが混入してしまう可能性がある。そのため、過去の事例等から不正プログラムの潜伏期間を想定し、情報の格付、取扱制限等を踏まえた上で、バックアップの周期や世代管理の方法等を定めるとよい。

また、復旧に用いるべきバックアップデータを事前に特定することが重要である。そのため、バックアップデータに対して最新の定義ファイルが適用された状態の不正プログラム対策ソフトウェア等による検査を行うとよい。

さらに、継続的に運用管理していく中においてバックアップ用の媒体が適切に挿入されていない等の運用ミスが発生するケースや、年数が経過することでデータ量が増大し想定時間内にバックアップが取得できないケース等が考えられるため、バックアップが適切に実施されていることを適宜確認するとよい。

- **遵守事項 3.1.1(8)(b)「格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め」について**

バックアップデータに要機密情報が含まれる場合は、バックアップデータの盗難・紛失による情報漏えい等を回避するために、バックアップデータを要管理対策区域に保管することが望ましい。また、バックアップデータを保存する媒体の耐久性にも留意し、定期的に媒体を新しいものに入れ替えるなども考慮するとよい。

バックアップデータの保存場所及び保存方法等の一例としては、バックアップデータのコピーを複数取得したうえで、取得したバックアップデータを異なる複数の種類の電磁的記録媒体に保存し、電磁的記録媒体の内の少なくとも１つはバックアップ取得元の情報システムとは異なる場所に保管する方法が挙げられる。当該方法により、全てのバックアップデータを同時に喪失するリスクを低減することが可能となる。一方で、バックアップに係るコストの増加に繋がる可能性があるため、情報の格付、取扱制限等に応じて、当該方法を検討するとよい。

- **基本対策事項 3.1.1(8)-2「重要な設計書」について**

情報システムの委託先から書面のみで提示された設計書類等、情報システムに記録されていない書面のみの情報であって、紛失、改ざん等により情報システムの運用に支障を及ぼす可能性のあるものを指している。バックアップが外部に流出することにより、攻撃者に有利になるものについては、保管の際に機密性を確保することにも留意が必要である。

- **基本対策事項 3.1.1(8)-2「適切な保管場所を選定する」について**

危機的事象を想定してバックアップを取得する場合は、完全性等の要求に応じ、想定する危機的事象に耐性のある保管庫や施設、同時被災しない遠隔地に保管すること等

が考えられる。また、遠隔地に保管するに当たっては、実際にバックアップを用いた復旧に要する時間が、情報システム運用継続計画における復旧目標時間内に納まるよう、緊急時のバックアップデータの配送手段、配送時間等を考慮し、保管場所を決定する必要がある。

- **基本対策事項 3.1.1(8)-2「情報システムや情報が破壊される情報セキュリティインシデント」について**

  端末及びサーバ装置並びにそれらとネットワーク接続された共有フォルダ等の情報を破壊するランサムウェア等によって生ずる情報セキュリティインシデントを想定している。

- **基本対策事項 3.1.1(8)-2「必要に応じて」について**

  情報システムや情報とバックアップが同時に破壊されることによる業務上の支障や、可能性等を考慮し、本基本対策事項を講ずるバックアップの対象を選定するとよい。

  例えば、バックアップ取得元の情報システムと同じネットワーク内にバックアップを保管している場合は、情報システムや情報とバックアップが同時に破壊される可能性が高いことが考えられるため、基本対策事項を講ずるバックアップの対象とすべきである。

  また、追記不能設定がなされた媒体にバックアップを保存する等、本基本対策事項に示すバックアップの保管場所以外による対策によって、バックアップが破壊される可能性が低いと考えられる場合は、当該バックアップを本基本対策事項の対象外としてもよい。

- **基本対策事項 3.1.1(8)-2「情報システムや情報とバックアップが同時に破壊されない保管場所を選定する」について**

  攻撃を受けた情報システムや情報が格納されている場所からバックアップ保管場所にアクセスができる場合、情報システムや情報と同時にバックアップも破壊されてしまう可能性があるため、情報システムや情報が格納されている場所から物理的又は論理的に隔離された場所にバックアップを保管することが重要である。

  バックアップの保管場所によって、情報システムや情報とバックアップが同時に破壊されない可能性や、バックアップから復旧する際に要する時間等の違いが生じる。それらの違い等を踏まえた上で、バックアップの保管場所を選定するとよい。

  なお、バックアップを取得する際はバックアップ取得元の情報システムとバックアップ保管媒体をネットワークで繋ぐ必要があるため、バックアップ取得中に情報セキュリティインシデントが発生した場合、情報システムや情報とバックアップが同時に破壊される可能性がある。そのため、バックアップ取得中はバックアップ取得元の情報システムの動作を停止又は制限する等により情報セキュリティインシデントが発生する可能性を下げるとよい。また、バックアップを取得する際に使用するバックアップ保管媒体は、過去に取得したバックアップが保管されていない媒体や、破壊が許容されるバックアップのみが保管された媒体を使用すること等によって、情報セキュリティインシデントが発生した場合の被害を低減させるとよい。

- **基本対策事項 3.1.1(8)-2 a)「物理的に隔離された保管場所」について**

物理的な隔離とは、情報システムや情報が格納されている場所とバックアップ保管場所のネットワークが物理的に繋がっていないことを想定している。

例えば、バックアップ保管媒体をネットワークから完全に切り離して保管する場合は、物理的な隔離が行われていると考えられる。

バックアップ保管媒体をネットワークから完全に切り離して保管する場合、情報システムや情報とバックアップが同時に破壊される可能性は著しく低いことが考えられる。しかし、ネットワークから切り離す際は一般的に人手を介する必要がある。そのため、自然災害や感染症等の危機的事象発生時に、必要な人手が不足する可能性があることを踏まえた上で、本基本対策事項を検討するとよい。

- **基本対策事項 3.1.1(8)-2 b)「論理的に隔離された保管場所」について**

論理的な隔離とは、情報システムや情報が格納されている場所とバックアップ保管場所の間の通信経路が論理的に分離されていることを想定している。

例えば、情報システムや情報が格納されている場所とバックアップ保管場所の間の通信経路が、アクセス制御による通信経路の分離を行っている場合は、論理的な隔離が行われていると考えられる。アクセス制御による通信経路の分離については、「（解説）基本対策事項 6.4.1(1)-1 b)「セグメント間の通信を必要最小限とするアクセス制御を行う」について」を参照のこと。

なお、「（解説）基本対策事項 3.1.1(8)-2 a)「物理的に隔離された保管場所」について」に記載のとおり、物理的に隔離された保管場所の場合、情報システムや情報とバックアップが同時に破壊される可能性は著しく低いことが考えられる。一方、論理的に隔離された保管場所を検討する際は、バックアップ保管場所で情報セキュリティインシデントが発生する可能性を考慮することが重要である。当該インシデントが発生するケースを以下に例示する。

- アクセス制御等による通信経路の論理的な分離が適切に行われていない
- 通信経路の分離を行っていた通信回線装置等に不正侵入され設定を変更される
- バックアップ保管場所が、情報システムや情報が格納されている場所とバックアップ保管場所の間の通信経路とは別の通信経路（例えば、保守作業に用いる通信経路）に接続されている

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

遵守事項

(1) 要管理対策区域における対策の基準の決定

(a) 統括情報セキュリティ責任者は、**要管理対策区域の範囲を定める**こと。

(b) 統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を全て含む対策の基準を運用規程として定めること。

(ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための**入退管理対策**。

【 基本対策事項 】

＜3.2.1(1)(b)(ア)(イ)関連＞

3.2.1(1)-1 統括情報セキュリティ責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を運用規程として定めること。

a) 下表のとおり、３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

3.2.1(1)-2 統括情報セキュリティ責任者は、クラス１の区域について、以下を全て含む施設

の整備、設備の設置等の物理的な対策及び入退管理対策の基準を運用規程として定めること。

a) 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

b) 不特定の者が容易に立ち入らないように、**立ち入る者の身元、訪問目的等の確認を行うための措置**を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

c) 要管理対策区域に不正に立ち入った者を容易に判別することができるように、以下を全て含む措置を講ずること。

- 職員等は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とすること。
- 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収すること。

3.2.1(1)-3 統括情報セキュリティ責任者は、クラス２の区域について、以下を全て含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を運用規程として定めること。

a) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は職員等が窓口を常に目視できるような措置を講ずること。

b) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

c) **クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

3.2.1(1)-4 統括情報セキュリティ責任者は、クラス３の区域について、以下を全て含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を運用規程として定めること。

a) クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

b) **クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

c) クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。

3.2.1(1)-5 統括情報セキュリティ責任者は、以下を例とする、区域への<u>クラスの割当ての基準</u>を運用規程として定めること。

a) クラスの割当ての基準を以下のように定める。

- サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。
- 一般的な執務室や執務室内の会議室には、職員等以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

（解説）

- **遵守事項 3.2.1(1)(a)「要管理対策区域の範囲を定める」について**

執務室やサーバ室のほか、複数の機関等で共用する会議室や職員等が書面やモバイル端末等を運搬するときの安全性を高めるために、執務室間や会議室に接続されている廊下等も要管理対策区域に含めることを考慮してもよい。

なお、要管理対策区域外で業務を行う必要がある場合には、施設及び環境に係る対策が講じられないことから情報の漏えい等の可能性が高くなる。情報の漏えい等の可能性を低減するためには、要管理対策区域外でのモバイル端末の利用に関する遵守事項（遵守事項 6.1.2(1)及び(2)、遵守事項 6.1.3(1)～(4)等）を参照し、適切な対策を行う必要がある。

- **遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について**

基本対策事項 3.2.1(1)-2～4 に示した対策の基準のほか、以下の対策を基準に含めてもよい。

- 共連れ（立入りを許可された者が立ち入る際に、立入りを許可されていない者を同時に立ち入らせるような行為）を防止する措置

  具体的な対策として、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。
- 立入りを許可されていない者の侵入等、区域の安全性が侵害された場合に追跡することができるように、立入り及び当該区域からの退出を記録及び監視する措置

  「記録及び監視する」具体的な対策として、警備員、監視カメラ等による記録及び監視のほか、要管理対策区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。継続的に立入りが許可されている者以外の者の立入りがあった場合には、立入りの記録として立ち入った者の氏名及び

所属、訪問目的、訪問相手の氏名及び所属、訪問日、立入り及び退出の時刻を記録することが挙げられる。

- 受渡業者と物品の受渡しを行う場所の制限

  なお、「受渡業者」とは、職員等との物品の受渡しを行う者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

- **基本対策事項 3.2.1(1)-2 b)「立ち入る者の身元、訪問目的等の確認を行うための措置」について**

クラス１の区域に「立ち入る者」について、継続的に立入りを許可された者のほか、一時的に立ち入る者（訪問者）がある。継続的に立入りを許可された者として、職員等や一定期間立入りを認められ、認められたことを示す許可証（入館カード等）が貸与されている業者等を想定している。また、一時的に立ち入る者として、不定期に訪れる来客や受渡業者等を想定している。

「身元、訪問目的等の確認を行うための措置」の具体的な対策として、以下が挙げられる。

- セキュリティゲートの設置、警備員や受付係等の配置をして立ち入る者に身分証明書等の提示を求める。
- 一時的に立ち入る者の氏名及び所属、訪問目的等を記録する。

- **基本対策事項 3.2.1(1)-3 c)「クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。

  なお、IC カード等による主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずることが望ましい。
- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
- 立入りを監視する警備員、受付係等を配置している場合は、許可する者が警備員等にあらかじめ一時的に立ち入る者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日時等を伝えておき、一時的に立ち入る者が来訪した際に警備員、受付係等が照合する。

クラス２の区域への立入り時の「許可された者であることの確認」について、クラス１の区域への立入り時に「身元、訪問目的等の確認」ではなく「許可された者であることの確認」を行っている場合においては、それをもって代替してもよい。

- **基本対策事項 3.2.1(1)-4 b)「クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主

体認証を行う。

- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
- 継続的に立入りが許可されている者のみに、常時施錠される扉の鍵を貸与したり、解錠するための暗証番号を通知したりしておき、鍵の所持や入力した暗証番号の一致により、確認する。

- **基本対策事項 3.2.1(1)-5「クラスの割当ての基準」について**

各区域へのクラスの割当ての基準の策定に当たっては【参考 3.2.1-1】を参考にするとよい。本基本対策事項においては、例としてサーバ室や日常的に機密性が高い情報を取り扱う執務室にはクラス３、一般の執務室や執務室内の会議室にはクラス２を割り当てるという基準を示している。

統括情報セキュリティ責任者は、区域情報セキュリティ責任者に、管理する区域で取り扱う情報、設置される情報システムの特性から、外部からの侵入があった場合の被害の大きさを考慮してクラスを決定させる必要があることを踏まえ、本基本対策事項で示す基準を参考とし、クラスの割当ての基準を定める必要がある。

また、業務の単位でクラスの割当ての基準（例：○○、××に関係する業務を行う執務室はクラス３、これら以外の業務を行う執務室はクラス２）を定めておくことも考えられる。

【参考 3.2.1-1】 要管理対策区域へのクラスの割当ての例

要管理対策区域へのクラスの割当ての例を図 3.2.1-1～3 に示す。

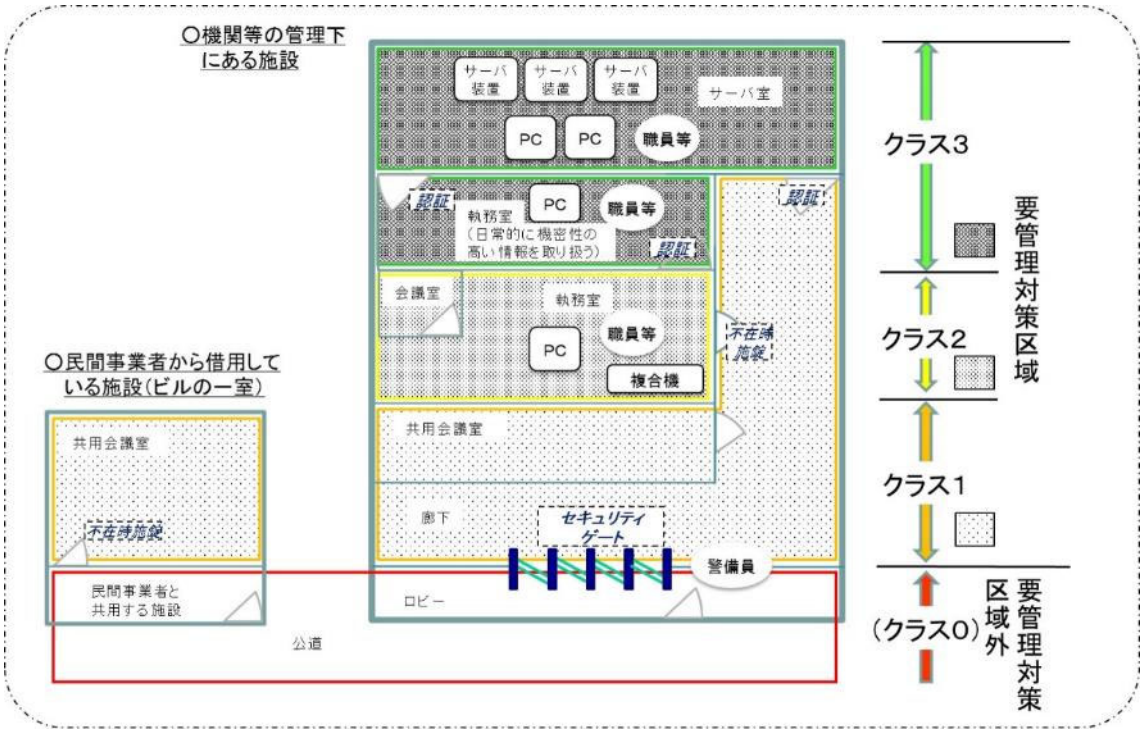


図 3.2.1-1 要管理対策区域へのクラスの割当ての例１（庁舎又は民間事業者から借用する施設）

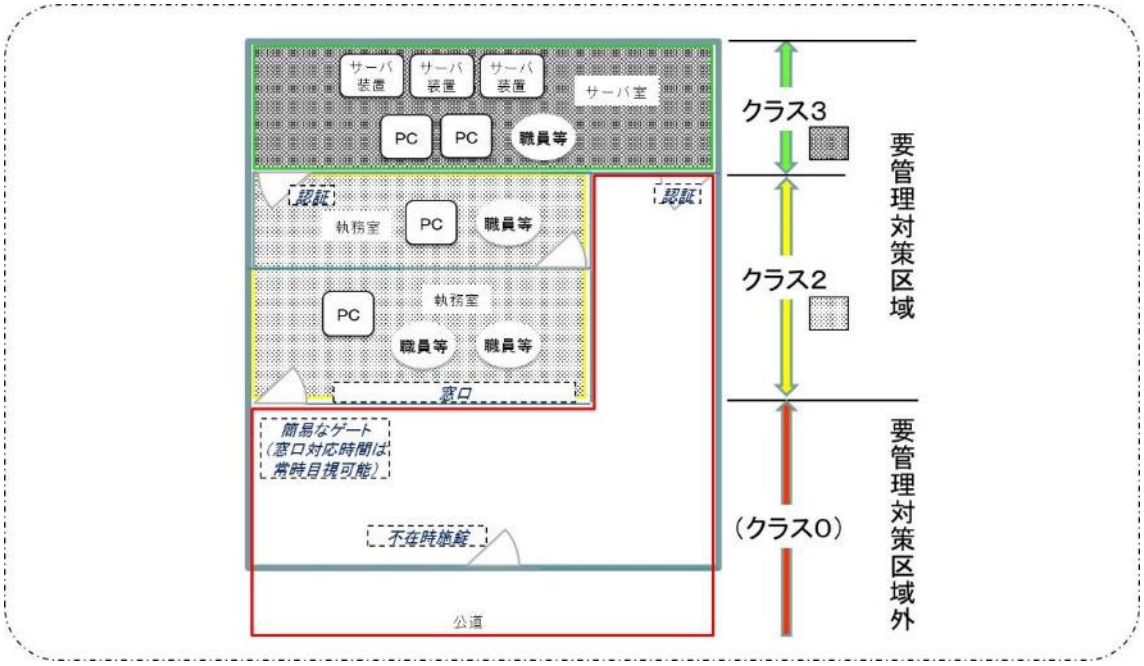


図 3.2.1-2 要管理対策区域へのクラスの割当ての例２（窓口のある執務室）

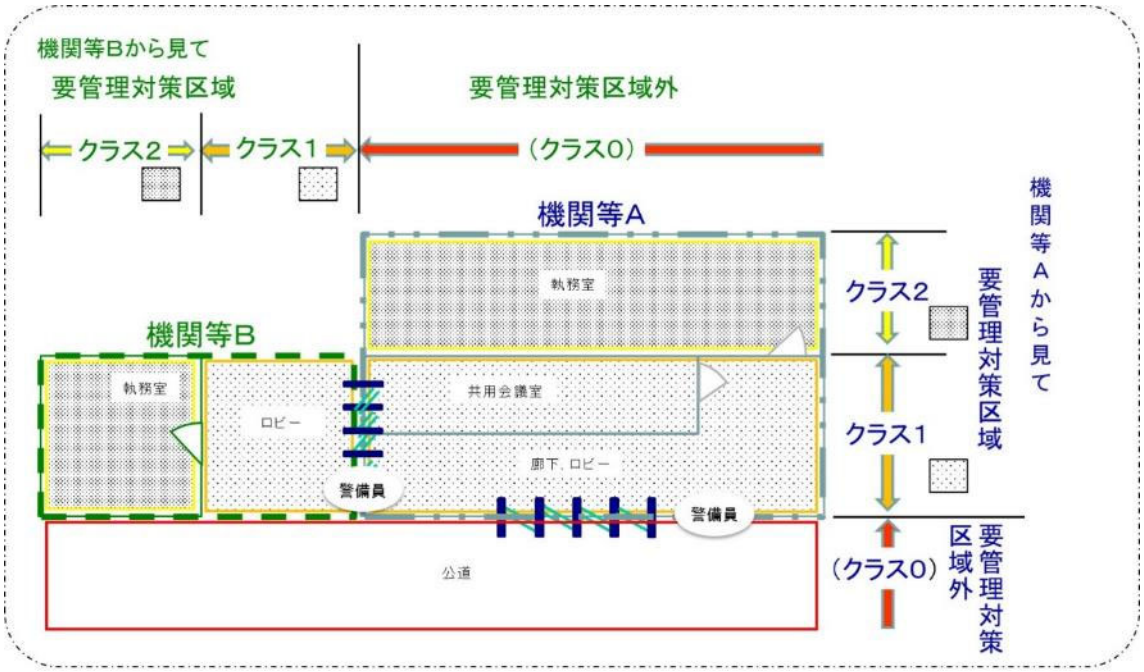


図 3.2.1-3 要管理対策区域へのクラスの割当ての例３
（複数の機関等で共用する施設）

遵守事項

(2) 区域ごとの対策の決定

(a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。

(a) 区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

【 基本対策事項 】

＜3.2.1(2)(b)関連＞

3.2.1(2)-1 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。

（解説）

- **遵守事項 3.2.1(2)(a)「施設及び執務環境に係る対策を行う単位ごとの区域を定める」について**

  複数の部局で共用する廊下等については、施設管理の観点での各部門の管理範囲を確認した上で「施設及び執務環境に係る対策を行う単位ごとの区域」を定めるとよい。共用する施設の区域情報セキュリティ責任者の定め方については、「(解説) 遵守事項 2.1.1(4)(b)「区域情報セキュリティ責任者」について」を参照のこと。

- **基本対策事項 3.2.1(2)-1「割り当てるクラスを決定する」について**

  クラス３、クラス２以外の要管理対策区域はクラス１となることにも留意して決定する必要がある。クラス１の区域は、不特定の者が容易に立ち入れない程度の安全性が確保された区域である。したがって、原則として、盗難や盗み見等への対策が講じられていない端末や書面が置かれる区域にクラス１を割り当ててはならない。やむをえずクラス１の区域に端末を置く必要がある場合（例：来訪者受付に職員等や来訪者の名簿を閲覧するための端末を置く場合）には、セキュリティワイヤ等で固定することや、常時目視により監視するなどの措置を講ずる必要がある。

- **基本対策事項 3.2.1(2)-1「当該区域において実施する対策を決定する」について**

  周辺の区域のクラスや管理状況も確認して具体的な対策を決定するとよい。例えば、クラス３の区域がクラス０の区域と接続している場合は、クラス３の区域の扉の施錠管理をより厳重にすることが考えられる。また、民間事業者が管理するビルの部屋を借りて業務を行っているような場合は、当該ビルの共用部分等では十分な対策が講じら

れないことが想定される。そのような場合には、借用している部屋の入退管理の強化や共用施設での業務の禁止を徹底すること等により、安全性を高めることが重要である。

なお、必要な対策が施設管理等の別の仕組みにより実施されている場合については、その対策をもって代替しても構わない。

- **基本対策事項 3.2.1(2)-1「個別の対策」について**

個別の対策については、「(解説) 遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について」に示した例（対策の基準となっていない場合）のほか、以下に示す例を参考に決定するとよい。

- 機関等の施設内の案内板等において、サーバ室等の所在の表示を禁止する。
- 外部から室内が見えるような場所にある会議室において、要機密情報の取扱い時はブラインドを閉じる。
- 外部の者が周辺の会議室等へ出入りする時間帯には、執務室の扉を施錠する又は開放しない。
- 低階層の窓際等における無線 LAN の傍受対策を行う。
- ワイヤレスマイクの電波が室外にも到達するような会議室において、要機密情報の取扱い時はワイヤレスマイクの使用を禁止する。
- ディスプレイケーブル等から生ずる電磁波から情報が漏えいするおそれがある場合には電磁波軽減フィルタを取り付けるなどの対策(テンペスト対策)を行う。
- 飲食物をこぼした際に情報システムの運用上の障害が発生するような場所での飲食を禁止する。
- 情報システムに関係する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行う。
- クラス３の区域の中でもより厳重な管理が必要な区域において、機器の持込み、利用、持ち出しについて制限を設ける。
- 会議室において、重要な情報を取り扱う会議が開催される時間帯には機器の持込み、利用について制限を設ける。

機器の持込み、利用、持ち出しの制限について詳細を以下に示す。

- 「機器の持込み」とは、職員等が、執務室に業務に関係しない機器を持ち込むことや情報システムが設置される区域に当該情報システムに関係しない機器を持ち込むことを指す。「機器」には、モバイル端末、デジタルカメラ等の撮影機器、IC レコーダー等の録音機器、USB メモリ等の外部電磁的記録媒体等が含まれる。また、私物のスマートフォン等の機関等支給以外の機器も含まれる。以下に示すように、利用のみを禁止する対策もあるが、例えば、持ち込まれたスマートフォンが不正プログラムに感染していて、持ち込んだ者の意図に反して撮影や録音をされるという脅威も存在するため、持ち込ませないという対策も考えられる。
- 「機器の利用」とは、職員等が、持ち込んだ機器を利用することを指す。「利用」には、モバイル端末の起動や、デジタルカメラ等による撮影、IC レコーダー等による録音等が含まれる。管理する区域で取り扱う情報の機密性の高さに応じ

て、利用の制限を設けるか決めるとよい。スマートフォン等の通常電源をオンにしている機器であれば、立ち入る際に電源をオフにさせるという対策も有効である。

- 「機器の持ち出し」とは、情報システムが設置される区域から当該情報システムに関係する者が、当該情報システムに関係するサーバ装置、端末、外部電磁的記録媒体等を持ち出すことを指す。情報セキュリティインシデント発生時に追跡等できるように、機器の持ち出し時には、持ち出しの記録を取ることが考えられる。記録の内容としては、持ち出しを行う者の氏名及び所属、日時、機器名、事由等が挙げられる。

遵守事項

(3) 要管理対策区域における対策の実施

(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。職員等が実施すべき対策については、**職員等が認識できる措置を講ずる**こと。

(b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために**物理的な対策**を講ずること。

(c) 職員等は、**利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する**こと。また、職員等が機関等外の者を立ち入らせる際には、当該機関等外の者にも当該区域で定められた対策に従って利用させること。

【 基本対策事項 】

＜3.2.1(3)(a)関連＞

3.2.1(3)-1 区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する職員等に周知すること。

a) 扉の施錠及び開閉に関する利用手順

b) 一時的に立ち入る者が許可された者であることを確認するための手順

c) 一時的に立ち入る者を監視するための手順

（解説）

- **遵守事項 3.2.1(3)(a)「職員等が認識できる措置を講ずる」について**

当該区域のクラスや当該クラスにおいて職員等が実施すべき対策を周知することが考えられる。扉の施錠や一時的に立ち入る者が許可された者であることの確認等の職員等に実施させる事項については、利用手順を定めて周知するとよい。

なお、関係者限りで利用する区域については、関係者のみに周知することでも構わない。

- **遵守事項 3.2.1(3)(b)「物理的な対策」について**

地震、火災、停電等の災害から情報システムを保護するための対策を指す。

具体的な対策として、例えば、サーバラックの利用のほか、以下の設置が挙げられる。

- ハロゲン化物消火設備
- 無停電電源装置
- 自家発電装置
- 空調設備
- 耐震又は免震設備

これらの対策については、必ずしも区域情報セキュリティ責任者単独で実施できるものではないが、例えば、情報システムに関係する対策であれば情報システムセキュリティ責任者、施設管理に関係する対策であれば施設管理を行う部門の関係者と調整することが求められる。

また、情報システムへの対策として、作業する者が災害によりサーバ装置等に近づく

ことができない場合に、作業する者の安全性を確保した上で遠隔地からサーバ装置等の電源を遮断できるようにする機能を設けておくことも考えられる。

- **遵守事項 3.2.1(3)(c)「利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する」について**

  職員等は、自身が所属する機関等が管理する区域を利用する場合は、自機関等が定めた対策に従って利用することが求められる。一方、他の機関等が管理する区域を利用する場合には、他の機関等が定めた対策に従って利用する必要がある。

第4部 外部委託

4.1 業務委託

4.1.1 業務委託

目的・趣旨

機関等外の者に、調査・研究等の業務を委託、あるいは情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先に提供する要保護情報等を適切に保護するための情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

業務委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても、前述のように委託先に提供した情報が適切に保護されるための情報セキュリティ対策が確実に実施される必要のある業務委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、委託業務でクラウドサービスを利用する場合は、委託先においてもクラウドサービス特有のリスクがあることから、4.2「クラウドサービス」で規定する内容についても取り扱う情報の格付、委託する業務や利用するクラウドサービスの特性等に応じて委託先への要求事項に含める必要がある。また、情報システムに関する業務を委託する際は、情報システムに関する別のリスクがあることから、4.1.2「情報システムに関する業務委託」に規定する内容についても実施する必要がある。さらに、機器等を調達する場合には、調達する機器等におけるサプライチェーン上のリスクがあることから、4.3「機器等の調達」で規定する内容についても実施する必要がある。

＜業務委託の例＞

- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
- プロジェクト管理支援業務の委託
- 調査・研究業務（調査、研究、検査等）の委託
- ウェブサイトの運用業務の委託

遵守事項

(1) 業務委託に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備すること。

(ア) 委託先への提供を認める情報及び委託する業務の範囲を判断する基準（以下

本款において「委託判断基準」という。）

（イ） 委託先の選定基準

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(1)(a)(ア)「委託判断基準」について**

委託先に許可されていない情報の提供が行われないように、委託先に提供する情報に関する機関等の基準を規定することを求めている。規定すべき内容としては、以下の例が考えられる。

- 業務委託を許可（又は禁止）する業務の範囲（委託先に開示できない情報を取り扱う業務は業務委託不可等）
- 業務委託への提供を許可（又は禁止）する情報の範囲（委託業務に関係しない情報は提供不可等）
- 格付及び取扱制限その他提供する情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（機密性３情報は要管理対策区域外での取扱いを禁止するなど）

特に、委託業務で取り扱われる情報に対して国外の法令等が適用される場合があり、国内であれば不適切と判断されるアクセス等が行われる可能性があることに注意が必要である。

- **遵守事項 4.1.1(1)(a)(イ)「委託先の選定基準」について**

統括情報セキュリティ責任者は、委託先の選定基準の整備に当たって、当該委託先が、事業の継続性を有し存続する可能性が高く、機関等の対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。

選定基準としては、委託先が対策基準を遵守し得る者であること、対策基準と同等の情報セキュリティ管理体制を整備していること、対策基準と同等の情報セキュリティ対策の教育を委託先の事業従事者に対して実施していること、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずること等が挙げられる。

参考：内閣官房国家サイバー統括室「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ）
（https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf）

また、機関等の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を機関等内で統一的に整備することが重要である。

委託先の選定基準策定に当たって、委託先の情報セキュリティ水準の評価方法を整備する際、例えば、ISO/IEC 27001 等の国際規格とそれに基づく認証制度の活用、情

報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用も考えられる。また、サプライチェーン強化に向けたセキュリティ対策評価制度(注)が運用開始された際は、これを活用することも考えられる。

なお、委託先の選定基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、業務委託の実施時に反映する必要がある。

（注）サプライチェーン全体でのサイバーセキュリティ対策強化の観点から、国家サイバー統括室と経済産業省で構築中のサプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）。2026 年 3 月に制度構築方針が公表されている。

遵守事項

(2) 業務委託実施前の対策

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施すること。

(ア) 委託する業務内容の特定

(イ) 委託先の選定条件を含む仕様の策定

(ウ) 仕様に基づく委託先の選定

(エ) 契約の締結

(オ) 委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求めること。

(ア) 仕様に準拠した提案

(イ) 契約の締結

(ウ) 委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

【 基本対策事項 】

＜4.1.1(2)(a)(イ)関連＞

4.1.1(2)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、以下の内容を全て含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様にも含めること。また、委託業務において、クラウドサービスを用いて委託業務に係る情報を取り扱うことが考えられる場合は、取り扱う情報の格付、委託する業務や利用するクラウドサービスの特性等に応じて、4.2「クラウドサービス」で規定する内容についても仕様に含めること。

a) 委託先に提供する情報の委託先における目的外利用の禁止

b) 委託先における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制

c) 情報セキュリティインシデントへの対処方法

d) 情報セキュリティ対策その他の契約の履行状況の確認方法

e) 情報セキュリティ対策の履行が不十分な場合の対処方法

4.1.1(2)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、以下の内容の全てを必要に応じて仕様に含めること。

a) 監査の受入れ

b) サービス品質の保証

＜4.1.1(2)(a)(イ)(エ)関連＞

4.1.1(2)-3 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うこと。

＜4.1.1(2)(a)(ウ)関連＞

4.1.1(2)-4 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、基本対策事項 4.1.1(2)-1 及び 2 の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、仕様に含めること。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。

＜4.1.1(2)(b)(ア)関連＞

4.1.1(2)-5 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、以下の内容を全て含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。

a) 当該委託業務に携わる者の特定
b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

（解説）

- **遵守事項 4.1.1(2)(a)(ア)「委託する業務内容の特定」について**

遵守事項 4.1.1(1)において、各機関等で定めた委託判断基準及び委託先の選定基準に基づいて、案件における業務委託の可否及び業務委託範囲や作業の定義、委託先の能力条件等、仕様の前提となる事項を明確にする必要がある。

- **遵守事項 4.1.1(2)(a)(オ)「秘密保持契約（NDA）の締結」について**

秘密保持契約（NDA）の締結に当たっては、必要な事項を契約書に記載することにより、業務委託の契約に含めてもよい。また、業務委託実施前において、見積書等を取得するために見積依頼先に要機密情報を閲覧させる場合にも、これに準じた対応を行うことが望ましい。

契約書等に記載する事項としては、以下の例が考えられる。

- 秘密情報の定義
- 秘密保持義務
- 目的外利用の禁止
- 秘密情報の保持・管理
- 秘密情報の返還・破棄
- 有効期間・存続条項

- **基本対策事項 4.1.1(2)-1「委託先の選定条件とし、仕様にも含める」について**

一般競争入札の中でも総合評価落札方式で行う場合は、本基本対策事項各号について、評価の際に入札者に対し提出を求めるなど、選定条件を満たしているかの確認をする必要がある。また、事前に評価を行えない最低価格落札方式等で行う場合であっても、仕様書に対する履行能力証明書等を提出させるなどにより、本基本対策事項各号につ

いて契約時までに提出することを確約させる必要がある。

なお、委託事業の内容によっては、一部の条件が設定不可能な場合や意味をなさない場合も考えられるため、そのような場合には、除外することもやむを得ない。

- **基本対策事項 4.1.1(2)-1 a)「委託先に提供する情報の委託先における目的外利用の禁止」について**

目的外利用に当たる場合としては、例えば、委託先が当該委託業務で提供を受けた機関等が利用するソフトウェアの情報を保有し、今後の営業活動で利用するなどが考えられる。

- **基本対策事項 4.1.1(2)-1 b)「情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制」について**

情報セキュリティ対策の具体的な実施内容については基本対策事項 4.1.1(3)-1 に示す情報セキュリティ対策を参照して、委託内容に応じて仕様書にも記載する必要がある。また、情報セキュリティに関する認証等として、例えば情報セキュリティ管理全般についての ISO/IEC 27001 等の取得を委託先に要求することも考えられる。

- **基本対策事項 4.1.1(2)-1 c)「情報セキュリティインシデントへの対処方法」について**

委託先において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、委託先の選定条件として仕様に含めておき、委託先と事前に合意する必要がある。対処方法について合意していないと、インシデントが発生しているにもかかわらず委託先と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、事前に合意することが重要である。

対処方法には、例えば、復旧を優先する場合は委託業務を一時的に停止するための手順を規定し、業務継続を優先する場合は、委託事業を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る委託先と機関等間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

- **基本対策事項 4.1.1(2)-1 d)「情報セキュリティ対策その他の契約の履行状況の確認方法」について**

情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや監査を実施してその結果を確認すること等が考えられる。監査の内容には、請け負わせる業務のうち監査の対象とする範囲、実施者（機関等が指定する第三者、委託先が選定する第三者、機関等又は委託先において当該業務を行う部門とは独立した部門）、実施方法（監査基準の概要、実施場所等）等、当該監査を受け入れる場合の委託先の負担及び委託先の情報セキュリティポリシーとの整合性等を委託先が判断するために必要と考えられる事項を含める。

監査により履行状況を確認する場合は、基本対策事項 4.1.1(2)-2 a)に示す監査の受入れを調達仕様書に明記することが望ましい。

なお、契約内容の中で委託先における情報セキュリティ対策以外の内容についても、機関等の情報セキュリティに影響を及ぼす内容であると考えられる場合は、その履行状況についても確認することが求められる。情報セキュリティ対策以外の内容としては、例えば、委託先の資本関係、国籍に関する情報等についての契約後の変化などが考えられる。

- **基本対策事項 4.1.1(2)-1 e)「情報セキュリティ対策の履行が不十分な場合の対処方法」について**

情報セキュリティ対策の履行が不十分である場合の対処方法としては、例えば、委託先と改善について協議を行い、合意した改善策を実施させること等が考えられる。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、遵守事項 4.1.1(2)に係る取決めについて、契約する者に対して依頼する必要がある。

- **基本対策事項 4.1.1(2)-2「取り扱う情報の格付等を勘案し、以下の内容の全てを必要に応じて仕様に含める」について**

要保護情報を委託先にて取り扱う場合には、必要時に情報セキュリティ対策の履行状況の報告を求めるものである。また、委託先への立入検査又は情報セキュリティに関する監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む委託先と合意した事項について、契約に含めるなどにより明確にすることが必要である。

また、要安定情報を取り扱う場合には、サービス品質の保証について委託先と契約を取り交わすことを検討する必要がある。サービス品質に関しては、セキュリティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、委託先に保証させることが重要である。

- **基本対策事項 4.1.1(2)-3「情報の取扱手順」について**

格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、委託先においても機関等の対策基準に定める内容と同等の取扱いが行われるよう、委託先と事前に合意することが重要である。また、委託先に提供する情報は必要最小限にとどめる必要があるが、委託先のシステムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、委託先における情報の取扱状況を適宜把握することも重要である。

- **基本対策事項 4.1.1(2)-4「再委託先」について**

「再委託先」には、再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む。

遵守事項

(3) 業務委託実施期間中の対策

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施すること。

(ア) 委託判断基準に従った要保護情報の提供

(イ) 契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認

(ウ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求めること。

(ア) 情報の適正な取扱いのための情報セキュリティ対策

(イ) 契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告

(ウ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

【 基本対策事項 】

＜4.1.1(3)(b)(ア)関連＞

4.1.1(3)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託業務における情報の適正な取扱いを委託先に担保させるため、以下の内容を全て含む情報セキュリティ対策について、あらかじめ委託先との契約に含めた上で、委託期間を通じて、情報の格付等に応じた実施を求めること。

a) 情報セキュリティインシデント等への対処能力の確立・維持

b) 情報へアクセスする主体の識別とアクセスの制御

c) ログの取得・監視

d) 情報を取り扱う機器等の物理的保護

e) 情報を取り扱う要員への周知と統制

f) セキュリティ脅威に対処するための資産管理・リスク評価

g) 委託先が取り扱う情報及び当該情報を取り扱うシステムの完全性の保護

h) セキュリティ対策の検証・評価・見直し

（解説）

- **遵守事項 4.1.1(3)(a)(ア)「委託判断基準に従った要保護情報の提供」について**

情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基

準又はそれを反映した仕様に従って業務委託を実施することが重要である。委託判断基準には、提供する要保護情報の適切な取扱いを担保する観点から、業務委託を許可（又は禁止）する業務や提供する情報の範囲、情報を取り扱う場所等が定められているため、業務委託実施期間中の委託先への要保護情報の提供は、これらの基準に従って行われる必要がある。

業務委託契約開始から終了に至るまでに行う委託先への要保護情報の提供に伴う情報の漏えい・滅失・改ざん等を防止するためには、委託業務に携わる職員等それぞれが委託先との情報の授受時に情報セキュリティを確保することが重要である。職員等は、委託先に要保護情報を提供する場合は、提供情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供することが求められる。

委託先への情報の提供に関する解説については、「（解説）遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について」を参照のこと。

- **遵守事項 4.1.1(3)(a)(イ)「契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認」について**

情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報セキュリティ対策の履行状況の確認に当たっては、当該対策の適切な履行が業務委託の実施期間又は契約期間の全般にわたって担保されていることを確認する必要がある。こうした趣旨から、履行状況の確認は、契約締結時に一度だけ行うのではなく、契約期間や確認内容に応じて適切な頻度を設定した上で、継続的に行うことが求められる。

委託先における情報セキュリティ対策の履行状況の確認に際し、委託先から報告を受ける等の方法に加えて監査を実施することとした場合には、あらかじめ契約に定めた監査の範囲及び実施方法に従い機関等自らが監査を行う以外に、第三者監査を行わせることも考えられる。

- **遵守事項 4.1.1(3)(a)(ウ)「対処の要求」について**

職員等は、業務委託において、情報セキュリティインシデントや情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告することが求められる。

- **遵守事項 4.1.1(3)(b)(ア)「情報の適正な取扱いのための情報セキュリティ対策」・基本対策事項 4.1.1(3)-1「委託業務における情報の適正な取扱いを委託先に担保させる」について**

遵守事項 4.1.1(3)(b)(ア)における「情報の適正な取扱いのための情報セキュリティ対策」とは、業務委託に伴い提供される機関等の要保護情報等を漏えい・滅失・改ざん等のリスクから保護する目的で、機関等が委託先に求めるものであり、その内容は基本対策事項 4.1.1(2)-1 b)が要求するセキュリティ対策の「実施内容」と同一である。すなわち、基本対策事項 4.1.1(3)-1 a)から h）においては、機関等が委託先に求めるべきセキュリティ対策の全体像を示すことを意図している。

統一基準群は機関等に対して求められる規範・基準であることから、多くの場合民間企業である業務委託先に対してその遵守を要求することは、実効性等の観点から必ず

しも適切でない場合も生じうると考えられる。機関等が委託先に求めるべきセキュリティ対策について委託先と合意形成を目指す際には、国際的な基準・標準等も参照した上で、より汎用性の高い基準・標準等を活用することも有用である。

非政府機関における要保護情報等の取扱いに係る情報セキュリティ対策の基準としては、National Institute of Standards and Technology（NIST、米国国立標準技術研究所）が、Special Publication（SP）800-171 として、”Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”（連邦政府外のシステムと組織における管理された非格付情報の保護）という文書（以下「NIST SP800-171」という。）を公表している。機密扱いではないものの保護が要求される連邦政府の情報を連邦政府外で取り扱わせる際の情報セキュリティ要求事項について、米連邦政府機関が参照している基準群との整合を取りつつまとめた要件集として、同文書は参考になりうる。

基本対策事項 4.1.1(3)-1 の a)から h）は、NIST SP800-171 の内容を参考に機関等が委託先に求めるべきセキュリティ対策を分類して、全体として機関等が業務委託時においても統一基準群の要求事項を満たせるように対策項目を提示している。

表 4.1.1-1　基本対策事項 4.1.1(3)-1 と NIST SP800-171 の参考となる管理策群

基本対策事項	NIST SP800-171 の管理策群
a) 情報セキュリティインシデント等への対処能力の確立・維持	3.6 Incident Response
b) 情報へアクセスする主体の識別とアクセスの制御	3.1 Access Control 3.5 Identification and Authentication
c) ログの取得・監視	3.3 Audit and Accountability
d) 情報を取り扱う機器等の物理的保護	3.8 Media Protection 3.10 Physical Protection
e) 情報を取り扱う要員への周知と統制	3.2 Awareness and Training 3.9 Personnel Security 3.15 Planning
f) セキュリティ脅威に対処するための資産管理・リスク評価	3.4 Configuration Management 3.7 Maintenance 3.11 Risk Assessment 3.17 Supply Chain Risk Management
g) 委託先が取り扱う情報及び当該情報を取り扱うシステムの完全性の保護	3.13 System and Communications Protection 3.14 System and Information Integrity 3.16 System and Services Acquisition
h) セキュリティ対策の検証・評価・見直し	3.12 Security Assessment and Monitoring

- **基本対策事項 4.1.1(3)-1 a)「情報セキュリティインシデント等への対処能力の確立・維持」について**

要保護情報等の提供を伴う業務委託において当該情報が適切に保護されるための対

策としては、情報セキュリティインシデント等が万一発生した場合にも、被害を防止又は最小化する必要がある。

そのため、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合に、委託先が機関等に的確な報告を行いつつ、それらの事態に迅速かつ適正に対処できるよう、報告手順及び対処手順を確立し、維持することを明示的に求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

- 識別・防御・検知・対応・復旧を例とした、準備から事後処理に至る全般的な情報セキュリティインシデント対処プロセスを確立する。
- 当事者及び関係者の役割を含む体制をあらかじめ定める。
- 情報セキュリティインシデント対処体制、責任者、委託業務担当者から当該体制への報告フロー等の概要について、対処能力の証明として契約締結までに説明ができるようにする。
- 情報セキュリティインシデント対応トレーニングを計画し、実施する。
- 委託期間中に情報セキュリティインシデント等の検出有無等について定期的な報告を行う。
- 情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、委託先が受託事業を一時中断するなどの必要な措置を講じた上で、報告手順に従い遅滞なく機関等に報告を行うとともに対処を行う。

- **基本対策事項 4.1.1(3)-1 b)「情報へアクセスする主体の識別とアクセスの制御」について**

委託業務に関して機関等が提供する要保護情報等及びそれを取り扱う情報システムにアクセスする主体を特定し、それが正当な主体であることを検証するための主体の識別及び主体認証を行うことを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

- 主体認証やその属性ごとにアクセス制御を行い、管理者権限を持つ場合には必要最低限の権限と利用に制限した上で、ログを取得する。
- システム利用者及び使用機器を一意に特定する。
- 特権アカウントへのアクセスに多要素主体認証を採用する。
- 可能な限り、非特権アカウントへのアクセスに多要素主体認証を採用する。
- リモートアクセスを実施する際は、通信経路の暗号化やその通信の監視等の対策を行う。
- 無線 LAN を利用する際は、通信路の暗号化や無線 LAN へのアクセス主体の認証等の対策を行う。
- 強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用する、初期パスワードの変更など主体認証情報に関する対策を行う。

- **基本対策事項 4.1.1(3)-1 c)「ログの取得・監視」について**

委託業務に関して機関等が提供する要保護情報等を取り扱う情報システムへの不正アクセスを検知・抑止するためのログを取得・監視すること及び要保護情報等にアクセスする全てのシステム利用者についてシステム操作履歴を取得することを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

  - ログの取得対象は継続的に見直しを実施する。
  - ログの取得プロセスの障害監視を行う。
  - 取得したログ情報やその分析内容に応じて、不正アクセスや異常操作への対応が取れるようプロセス設計を行う。
  - ログの分析機能やレポート作成機能を提供する。
  - 取得したログ情報及びログ取得機能について改変・削除から保護し、ログ取得機能の管理者権限付与を最低限の対象に限定する。

- **基本対策事項 4.1.1(3)-1 d)「情報を取り扱う機器等の物理的保護」について**

委託業務に関して機関等が提供する要保護情報等を格納する装置、機器、記録媒体、及び紙媒体の使用や保管に係る対策を実施することを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

  - 情報又は機器等へのアクセスを許可されている要員だけに認める。
  - 機器等の廃棄時又は再利用時にデータを抹消又は破壊する。
  - 外部電磁的記録媒体を使用する場合、運送時におけるセキュアな外部電磁的記録媒体の使用や、使用を想定しない USB ポートの無効化、委託事業以外での使用制限等の対策を行う。
  - 委託事業の実施場所について、鍵等の管理や入退室記録等、入退管理対策を行う。
  - 委託先がテレワークを実施する場合、情報セキュリティ対策を行う。

- **基本対策事項 4.1.1(3)-1 e)「情報を取り扱う要員への周知と統制」について**

委託業務に従事する委託先の従業員等及び機関等が提供する要保護情報等を取り扱う情報システムにアクセスを許可する委託先の従業員等に情報セキュリティポリシー、行動指針等を示し、情報セキュリティ意識を向上させること、また、業務上遵守すべき情報セキュリティ対策に関する事項を確実に認識させることを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

  - 情報セキュリティに係る業務及び責務の遂行に必要な訓練等を確実に受講させる。
  - 委託業務に伴う情報を取り扱う従業員等の資格条件を明確にする。
  - これら従業員等の異動・退職等の際に情報を保護すること等を求める。

- **基本対策事項 4.1.1(3)-1 f)「セキュリティ脅威に対処するための資産管理・リスク評価」**

について

委託業務に関して機関等が提供する要保護情報等を取り扱う情報システムに用いる機器等について、ソフトウェアバージョンや設定情報の文書化や変更による悪影響の防止等の適切な構成管理を実施すること、要保護情報等を取り扱う情報システムの運用管理で用いるツール・技法・仕組み・要員を組織的に管理すること、要保護情報等を取り扱う情報システムの運用や情報の処理・保管・送信に伴うリスクについてサプライチェーンも含め継続的に評価することを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

- 情報システムの変更に係る検知機能やログ解析機能を実装する。
- 外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時に多要素主体認証を要求する。
- 定期的及び重大な脆弱性の公表時に脆弱性検査を実施し、適時な脆弱性対策を行う。

- **基本対策事項 4.1.1(3)-1 g)「委託先が取り扱う情報及び当該情報を取り扱うシステムの完全性の保護」について**

委託業務に関して機関等が提供する要保護情報等を取り扱う情報システムが接続するネットワークの外部境界及び主要な内部境界において、通信又は送受信データを監視し、制御し、保護するとともに、セキュリティバイデザインの考え方等の情報セキュリティを確保するために有効なシステム開発方法論を採用することを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

- 定期的な検索等によりシステムの欠陥を適時に検出し是正する。
- 悪意あるコードに対する保護措置を講ずる。
- 脆弱性に係る注意喚起の監視と対処を行う。
- 安全性の高いアルゴリズム及び鍵長による暗号化及び電子署名機能を実装し、暗号鍵を適切に管理する。
- 業務に必要な通信だけを許可し、許可していない不正な通信の発生を防止する。
- 不正利用防止のための職務分掌の徹底及び事後追跡のためのログの取得・管理・分析体制を整備する。

- **基本対策事項 4.1.1(3)-1 h)「セキュリティ対策の検証・評価・見直し」について**

委託業務に関して機関等が提供する要保護情報等を取り扱う委託先組織に対して、自らのセキュリティ対策を評価して、必要な是正を行うことを求める。

取り扱う情報の格付等を勘案し、以下の対策の実施を委託先に求めることが考えられる。

- システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施する。
- システムの欠陥の是正及び脆弱性対策等のセキュリティ対策が有効に機能していることの継続的な監視と確認を行う。
- システム境界・運用環境・セキュリティ要求事項の実装方法及び関連システムに

関する考慮事項等の文書化と定期的な見直しを行う。

遵守事項

(4) 業務委託終了時の対策

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施すること。

(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(イ) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求めること。

(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(4)(a)(ア)「業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収」について**

  業務委託終了時の検収に当たっては、納入品の検査・検証だけでなく、委託先に求めるセキュリティ対策が、委託開始時から終了時に渡って適切に実施されたことを併せて確認する必要がある。確認に当たっては、遵守事項 4.1.1(3)(b)で委託先へ求める対策を対象に、委託先とあらかじめ具体的な確認手段について合意した上で実施することが望ましい。

- **遵守事項 4.1.1(4)(a)(イ)「情報が確実に返却、廃棄又は抹消されたことの確認」について**

  当該遵守事項を職員等に求めるに当たり、委託先とも具体的な確認手段を定め、事前に合意することが望ましい。情報が完全に廃棄又は抹消されたことを確認することが困難な場合は、確認書を委託先に提出させるなどの方法も考慮する必要がある。

  情報の抹消については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」を参照し、確認手段を定めるとよい。

  なお、情報システムの廃棄を業務委託する場合は、「（解説）遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について」を参照のこと。

4.1.2 情報システムに関する業務委託

目的・趣旨

機関等外の者に、情報システムやアプリケーションプログラムの開発・運用・保守等の情報システムに関する業務を委託する際は、4.1.1「業務委託」で規定する内容に加え、委託先によって情報システムに機関等の意図せざる変更が加えられないための対策や、情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策等の情報システムに関する業務委託に特有の対策を講ずる必要があるこれらについても、委託先への要求事項として調達仕様書等に定め、委託の際の契約条件とする必要がある。

＜情報システムに関する業務委託の例＞

- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- 機関等内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務の委託（ホスティング型プライベートクラウド）

遵守事項

(1) 情報システムに関する業務委託における共通的対策

(a) 情報システムセキュリティ責任者は、<u>情報システムに関する業務委託</u>の実施までに、委託先の選定条件に情報システムに機関等の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。

【 基本対策事項 】

＜4.1.2(1)(a)関連＞

4.1.2(1)-1 情報システムセキュリティ責任者は、以下の内容を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託の委託先の選定条件に加え、仕様にも含めること。

a) 委託先企業若しくはその従業員、再委託先又はその他の者によって、<u>情報システムに機関等の意図せざる変更が加えられないための管理体制</u>

b) <u>委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報提供</u>

（解説）

- **遵守事項 4.1.2(1)(a)「情報システムに関する業務委託」について**

情報システムに関する業務委託については、情報システムやアプリケーションプログラムの開発・運用・保守等のように、機関等の情報システムに直接的に影響を及ぼす

ことが可能な業務委託を想定している。

【参考 4.1.2-1】 「業務委託」、「情報システムに関する業務委託」、「機関等向けに情報システムの一部の機能を提供するサービス」、「クラウドサービス」、「機器等の調達」の関係のイメージ例

「業務委託」、「情報システムに関する業務委託」、「機関等向けに情報システムの一部の機能を提供するサービス」、「クラウドサービス」、「機器等の調達」の関係のイメージを図 4.1.2-1 に示す。

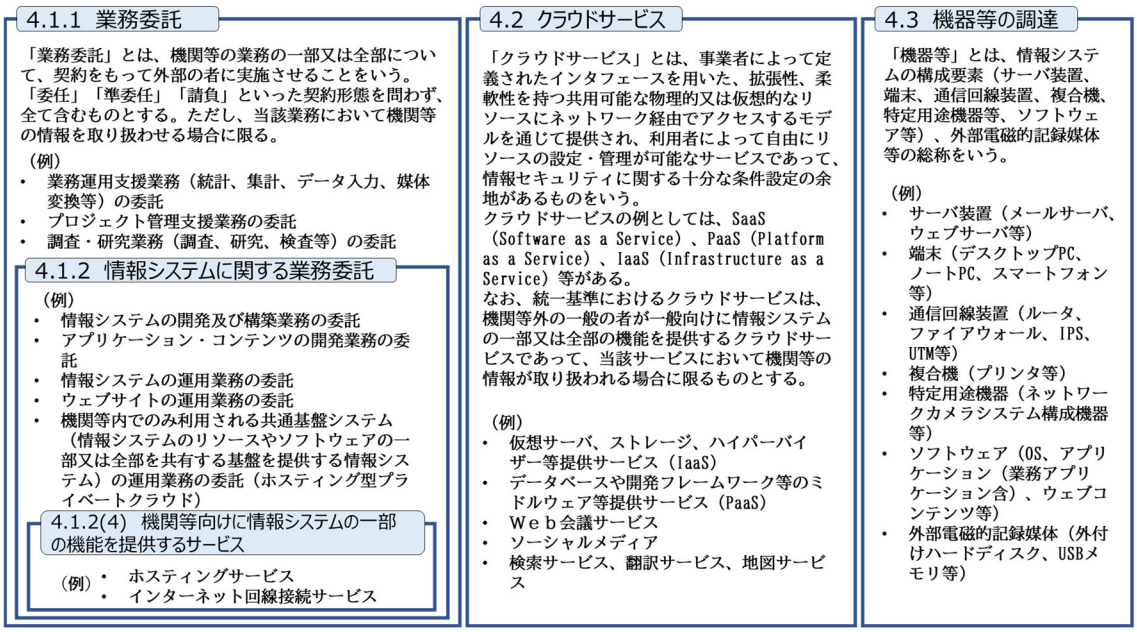


図 4.1.2-1 「業務委託」、「情報システムに関する業務委託」、「機関等向けに情報システムの一部の機能を提供するサービス」、「クラウドサービス」、「機器等の調達」の関係のイメージ

- **基本対策事項 4.1.2(1)-1 a)「情報システムに機関等の意図せざる変更が加えられないための管理体制」について**

  具体的に調達仕様書等に記載する事項としては、以下の例が考えられる。

  - 情報システムの開発工程において、機関等の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。
  - 情報システムに機関等の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、機関等と委託先が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

- **基本対策事項 4.1.2(1)-1 b)「委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報提供」について**

  基本対策事項 4.1.2(1)-1 a)における管理体制等を確認する際の参照情報として用い

るため、提供を求める規定である。

- **基本対策事項 4.1.2(1)-1 b)「委託事業の実施場所」について**

  要安定情報を取り扱う情報システムに関する業務委託において、自然災害その他による影響を考慮し、実施場所の立地条件を事前に考慮する必要がある。

遵守事項

(2) 情報システムの構築を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求めること。

(ア) 情報システムのセキュリティ要件の適切な実装

(イ) 情報セキュリティの観点に基づく試験の実施

(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策

【 基本対策事項 】

＜4.1.2(2)(a)(イ)関連＞

4.1.2(2)-1 情報システムセキュリティ責任者は、情報セキュリティの観点に基づく試験の実施について、調達仕様書に記載するなどして、以下を全て含む事項の実施を委託先に求めること。

a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。

b) 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

c) 情報セキュリティの観点から実施した試験の実施記録を保存すること。

＜4.1.2(2)(a)(ウ)関連＞

4.1.2(2)-2 情報システムセキュリティ責任者は、開発工程における情報セキュリティ対策として、調達仕様書に記載するなどして、以下を全て含む事項の実施を委託先に求めること。

a) ソースコードが不正に変更・消去されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

- ソースコードの変更管理
- ソースコードの閲覧制限のためのアクセス制御
- ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

（解説）

- **遵守事項 4.1.2(2)(a)（ア）「情報システムのセキュリティ要件」について**

  情報システムのセキュリティ要件については、遵守事項 5.2.1(3)を参照のこと。

- **基本対策事項 4.1.2(2)-1 a)「運用中の情報システムに悪影響」について**

  運用中の情報システムを利用してソフトウェアの作成及び試験を行う場合は、運用中の情報システムに悪影響が及ぶことを回避することが大前提となる。

  また、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにする必要がある。

- **基本対策事項 4.1.2(2)-1 b)「情報セキュリティの観点から必要な試験」について**

  攻撃が行われた際に情報システムがどのような動作をするかを試験する項目として想定しており、具体的には、想定の範囲外のデータの入力を拒否できるか、サービス不能攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、レースコンディションが発生しないか（「(解説) 基本対策事項 6.6.1(3)-1 l)「レースコンディション脆弱性」について」を参照のこと。）といった項目が挙げられる。

  なお、セキュリティ機能の試験だけにとどまらず、情報システムの脆弱性の有無、必要なチェック機能の欠如等について、必要な試験が網羅されるよう留意する必要がある。

- **基本対策事項 4.1.2(2)-1 c)「実施記録」について**

  「実施記録」とは、試験の項目、実施結果、実施時に判明した不具合及び当該不具合の修正の記録等を指し、これらを保存することにより、脆弱性を発見した場合の対処に利用できるようにすることが求められる。

- **基本対策事項 4.1.2(2)-2「開発工程における情報セキュリティ対策」について**

  情報システム開発に係る情報資産についてセキュリティを維持するための手順及び環境を定めることを求めている。

  具体的な手順としては、例えば、調達仕様書、ソースコード等の成果物に対して情報システムのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツール等が考えられる。

  開発環境については、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用するサーバ装置及び端末の設置場所及びアクセス制御の方法等がある。

  なお、情報システム開発を業務委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を事前に整備する必要がある。

- **基本対策事項 4.1.2(2)-2 c)「設計レビュー」について**

  情報システムの設計について、脆弱性の原因となる設計の不具合をなくすために、設計レビューの実施が求められる。

  一般に設計レビューには、①レビュー対象内にあるエラーの発見を第一目的とし、開発責任者等が実施する確認手法、②開発担当者自身が開発関係者を集め、レビュー対象プログラムを実行の流れに従って追跡し確認する手法等があり、これらを、いつ、誰が、何に対して実施するのか、といったことを定める必要がある。

- **基本対策事項 4.1.2(2)-2 c)「ソースコードレビュー」について**

  ソースコードに脆弱性が混入しないように、ソースコードレビューの範囲及び方法について、あらかじめ定めておくことが求められる。例えば、脆弱性の原因となるソースコードについては、開発言語ごとに典型的なパターンが知られていることから、ソースコードレビューによる検証が有効な場合がある。なお、ソースコードレビューについては、開発する情報システムだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。

遵守事項

(3) 情報システムの運用・保守を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求めること。

(b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、**当該対策による情報システムの変更内容**について、契約に基づき、委託先に速やかな報告を求めること。

【 基本対策事項 】

＜4.1.2(3)(a)関連＞

4.1.2(3)-1 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を全て含む要件を調達仕様書に記載するなどして、契約に基づき、委託先に実施を求めること。

a) 情報システムの**運用環境に課せられるべき条件**の整備

b) 情報システムのセキュリティ監視を行う場合の**監視手順**や連絡方法

c) 情報システムの**保守における情報セキュリティ対策**

d) 運用中の情報システムに**脆弱性が存在することが判明**した場合の情報セキュリティ対策

（解説）

- **遵守事項 4.1.2(3)(b)「当該対策による情報システムの変更内容」について**

情報セキュリティ対策を実施することにより、ソフトウェアのバージョン等、遵守事項 5.2.2(1)(d)で整備することとされている情報システム関連文書の内容に変更が生じる可能性がある。情報セキュリティ対策を実施するためには情報システムの状態を正確に把握する必要があることから、情報セキュリティ関連文書の内容を最新に保つために、当該文書で管理している項目について報告を求めることが重要である。

- **基本対策事項 4.1.2(3)-1 a)「運用環境に課せられるべき条件」について**

情報システムの運用環境に課せられるべき条件としては、物理的、接続的（ネットワーク環境）及び人的側面が考えられる。どのような条件を設定するかによって想定される脅威が異なってくるため、脅威を想定する上で必要となる条件は全て調達仕様書、契約書等に記載する必要がある。

物理的側面とは、サーバ装置を設置する場所の特定、耐震･防火に関する基準、電源供給に関する基準等に関する条件を示すものである。

接続的（ネットワーク環境）側面とは、情報システムが接続される通信回線の種類やクラウドサービスをネットワーク経由で利用する場合の条件等を示すものである。

人的側面とは、対象とするシステムの管理者や業務担当職員等の信頼性に関する条件、当該システムに関わる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものである。

- **基本対策事項 4.1.2(3)-1 b)「監視手順」について**

情報システムのセキュリティ監視を業務委託する場合の監視手順等については、「(解説) 基本対策事項 7.1.6(1)-3「監視手順」について」及び「(解説) 基本対策事項 7.1.6(1)-4「セキュリティ監視を専門の外部事業者に業務委託」について」を参照のこと。

- **基本対策事項 4.1.2(3)-1 c)「保守における情報セキュリティ対策」について**

情報システムの保守においては、保守担当者が作業中に権限外の情報にアクセスできないよう、アクセス制御や権限管理を考慮する必要がある。また、保守担当者へのなりすましが脅威として想定される場合には、保守担当者に対する主体認証が実装された情報システムのセキュリティ要件を考慮する必要がある。さらに、インターネット等の外部ネットワークである機関等外通信回線から機関等内通信回線に接続された機器等に対して行うリモート運用やリモート保守を業務委託する場合は、遵守事項 6.4.1(2)(c)を遵守する必要がある。

- **基本対策事項 4.1.2(3)-1 d)「脆弱性が存在することが判明」について**

ソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性は日々新たなものが報告されており、調達時に策定した脆弱性についての対策要件だけでは十分に対処できない可能性もあり得る。

また、運用・保守を行う委託先が、情報システムの構築を行った委託先と異なる場合、情報システム運用開始後に発見された脆弱性に対して、情報システムの構築を行った委託先のみでは対処することが困難な場合もあり得る。そのため、運用・保守を行う委託先に対して、運用開始後に発見された脆弱性への対処を求めることも、契約又は調達仕様書において考慮する必要がある。

遵守事項

(4) 機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、**機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス**（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加えること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定すること。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

(d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行うこと。

(e) 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該**利用申請を審査**し、利用の可否を決定すること。

(f) 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、**承認済み業務委託サービスとして記録**し、**業務委託サービス管理者を指名**すること。

【 基本対策事項 】

＜4.1.2(4)(a)関連＞

4.1.2(4)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託サービスの中断や終了時に円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを委託先の選定条件に加え、仕様にも含めること。

a) 取り扱う情報の可用性区分の格付に応じた、業務委託サービス中断時の復旧要件

b) 取り扱う情報の可用性区分の格付に応じた、業務委託サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

4.1.2(4)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託サービスの利用を通じて機関等が取り扱う情報に対して**国内法以外の法令及び規制が適用されるリスク**を評価して委託先を選定し、必要に応じて**機関等の情報が取り扱われる場所**及び契約に定める準拠法・裁判管轄を委託先の選定条件に加え、仕様にも含めること。

＜4.1.2(4)(b)関連＞

4.1.2(4)-3 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、業務委託サービスを選定すること。また、業務委託サービスのセキュリティ要件として**セキュリティに係る国際規格等**と同等以上の水準を求めること。

＜4.1.2(4)(c)関連＞

4.1.2(4)-4 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、監査による報告書の内容、各種の認定・認証制度の適用状況等から、業務委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

（解説）

- **遵守事項 4.1.2(4)(a)「機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス」について**

  機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービスには、ホスティングサービス、インターネット回線接続サービスなどが考えられる。なお、業務委託サービスは、契約をもって外部の者に実施させる「業務委託」により提供を受けるサービスであることから、遵守事項 4.1.2(4)(b)で定めるセキュリティ要件を調達仕様書に個別に記載するなどにより情報セキュリティを確保する必要がある。また、定型約款や規約等への同意のみで利用可能となるサービスは、機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱うために必要なセキュリティ要件を満たすことが一般的に困難であることから、業務委託サービスには含まれない。

- **遵守事項 4.1.2(4)(e)「利用申請を審査」について**

  業務委託サービスの利用申請の審査においては、利用申請されたサービスが、委託先の選定基準と当該サービスのセキュリティ要件の両者を満たす場合に承認される必要がある。また、利用申請の審査をする時期については、当該業務委託の契約前までに行うことが望ましい。

- **遵守事項 4.1.2(4)(f)「承認済み業務委託サービスとして記録」について**

  承認済みの業務委託サービスについては、同一の業務委託サービスの利用申請があった場合における審査の参考となるが、利用申請ごとに条件の異なることが想定されるため、審査の経緯や条件についても併せて記録することが望ましい。

- **遵守事項 4.1.2(4)(f)「業務委託サービス管理者を指名」について**

  業務委託サービスの利用は利用申請ごとに条件の異なることが想定されるため、仮に同一部局内で既に同一のサービスの承認があっても、業務内容や情報の格付、利用者の所属する組織の違いに応じて「業務委託サービス管理者」をそれぞれ立てた方が管理が容易になる場合が考えられる。「業務委託サービス管理者」を指名する際には、当該業務委託サービスが情報システムの調達を伴うものの場合は「情報システムセキュリティ責任者」、職員等の利用登録のみで利用可能なものは「課室情報セキュリティ責任者」のように申請内容を加味した上で決定することが望ましい。

- **基本対策事項 4.1.2(4)-2「国内法以外の法令及び規制が適用されるリスク」について**

  国内法以外の法令及び規制が適用されるリスクとして、適正なかつ透明性のある手続（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形でデータセ

ンター内のデータが外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には留意する必要がある。なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、機関等の管理する暗号鍵で情報を暗号化するなどの措置を検討する必要がある。

- **基本対策事項 4.1.2(4)-2「機関等の情報が取り扱われる場所」について**

  バックアップデータ、サーバ装置内のデータ等、機関等の情報が存在し得る場所全てを機関等の情報が取り扱われる場所として考慮する必要がある。

- **基本対策事項 4.1.2(4)-3「セキュリティに係る国際規格等」について**

  セキュリティに係る国際規格としてはISO/IEC 27000 ファミリーによるISMS 認証の国際規格を参考にするとよい。

- **基本対策事項 4.1.2(4)-4「監査による報告書の内容、各種の認定・認証制度の適用状況等から、業務委託先の信頼性が十分であることを総合的・客観的に評価し判断すること」について**

  業務委託先の信頼性が十分であることを総合的に判断するためには、業務委託サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、業務委託先のセキュリティ対策を含めた経営が安定していること、業務委託サービスに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

  このような評価に当たって、業務委託先が業務委託サービス利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。その場合、監査や認証等によって保証される対象範囲が業務委託先の全部又は一部の場合があるので、機関等が利用する業務委託サービスが当該対象範囲に含まれていることを確認する必要がある。また、監査の場合には、監査項目の網羅性に留意して、重要な監査項目が除かれていないか、監査意見に除外事項（内部統制の不備）が含まれていないかなどを確認する必要がある。さらに、その監査や認証等によっては、業務委託先の経営の安定性やサプライチェーン・リスク等は上記の評価に含まれていないことが考えられるため、これらのリスクについては機関等において評価する必要がある。

  なお、参考となる認証には、業務委託先等のセキュリティに係る内部統制の保証報告書であるSOC 報告書（System and Organization Controls Report）を活用することも考えられる。特に、SOC2（SOC for Service Organizations: Trust Services Criteria）・SOC3（SOC for Service Organizations: Trust Service Criteria for General Use Report）は、米国公認会計士協会が開発した「セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する Trust サービス基準」で定義された５つの Trust サービスのカテゴリーのうち、「セキュリティ」に係る規準を含む１つ以上のカテゴリーに関する規準を適用したものであるため、業務委託サービス提供者及びサービスに対する評価の際の参考となり得る。

  参考：米国公認会計士協会「System and Organization Controls: SOC Suite of

Services」
（https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services）

4.2　クラウドサービス

4.2.1　クラウドサービスの選定（要機密情報を取り扱う場合）

目的・趣旨

機関等が委託先に取扱いを委ねる情報は、当該委託先によって適正に取り扱われなければならないが、クラウドサービスにおけるセキュリティ対策の詳細を直接確認することは一般に容易ではない。このため機関等がクラウドサービスを利用して要機密情報を取り扱う場合は、クラウドサービスの特性を理解し、機関等によるクラウドサービス提供者へのガバナンスの有効性や、利用の際のセキュリティ確保のために必要な事項を十分に考慮し、機関等とクラウドサービス提供者の役割や責任分担を明確にした上で、クラウドサービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

＜クラウドサービスの例＞

- 仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
- データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
- Ｗｅｂ会議サービス
- ソーシャルメディア
- 検索サービス、翻訳サービス、地図サービス

なお、民間事業者等が不特定多数の利用者に対して提供する、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできないため、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の規定を遵守する必要がある。

遵守事項

(1) クラウドサービスの選定に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程を整備すること。

(ア) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 4.2 節において「**クラウドサービス利用判断基準**」という。）

(イ) クラウドサービスの選定基準

(ウ) クラウドサービスの**利用申請の許可権限者**と利用手続

(エ) **クラウドサービス管理者**の指名とクラウドサービスの利用状況の管理

【 基本対策事項 】

＜4.2.1(1)(a)(ア)関連＞

4.2.1(1)-1 統括情報セキュリティ責任者は、遵守事項 4.1.1(1)(a)(ア)で整備を求めている「委託判断基準」と同等の基準とするとともに、クラウドサービス特有の脅威やクラウド

サービスで利用する業務等を踏まえた上でクラウドサービス利用判断基準を策定すること。

＜4.2.1(1)(a)(イ)関連＞

4.2.1(1)-2 統括情報セキュリティ責任者は、クラウドサービスの選定基準について、遵守事項 4.1.1(1)(a)(イ)で整備を求めている「委託先の選定基準」と同等の基準とするとともに、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP 等クラウドサービスリスト」という。）から選定することを策定すること。

＜4.2.1(1)(a)(ウ)関連＞

4.2.1(1)-3 統括情報セキュリティ責任者は、機関等において要機密情報を取り扱う場合のクラウドサービスの利用手続を、以下を全て含める内容を定めること。

a) 利用申請の許可権限者

b) 申請内容

- ISMAP 等クラウドサービスリストの登録番号
- クラウドサービスの名称（必要に応じて機能名までを含む。）
- クラウドサービスリストの種類（ISMAP か ISMAP-LIU か。）
- クラウドサービス提供者の名称
- 利用目的（業務内容）
- 取り扱う情報の格付
- 利用期間
- 利用申請者（所属・氏名）
- 利用者の範囲（機関等内に限る、部局内に限る など）
- 選定時の確認結果

＜4.2.1(1)(a)(エ)関連＞

4.2.1(1)-4 統括情報セキュリティ責任者は、機関等におけるクラウドサービスの利用状況の管理について、以下を例に運用規程を整備すること。

a) 利用申請の許可権限者は、申請ごとにクラウドサービス管理者を指名すること。

b) 利用承認したクラウドサービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新のクラウドサービスの利用状況を把握できるようにする。また、記録する際は、以下を例とする項目を記録し機関等内で共有すること。

- ISMAP 等クラウドサービスリストの登録番号
- クラウドサービスの名称（必要に応じて機能名までを含む。）
- クラウドサービスリストの種類（ISMAP か ISMAP-LIU か。）
- クラウドサービス提供者の名称
- 利用目的（業務内容）
- 取り扱う情報の格付
- 利用期間
- 利用申請者（所属・氏名）
- 利用者の範囲（機関等内に限る、部局内に限る など）
- クラウドサービス管理者（所属・氏名）

（解説）

- **遵守事項 4.2.1(1)(a)(ア)「クラウドサービス利用判断基準」について**

クラウドサービスの利用においても、遵守事項 4.1.1(1)(a)(ア)で整備を求めている「委託判断基準」と同等の基準として含める必要がある。また、「クラウドサービス利用判断基準」に含める内容としては、以下の事項を検討するとよい。

- クラウドサービス利用者がクラウドサービスを利用する際の接続方法(テレワーク等により、機関等外通信回線から直接クラウドサービスにアクセスすることの可否等)
- クラウドサービス特有の脅威を踏まえて、クラウドサービスを利用して行うことが可能な業務や利用不可とする業務
- クラウドサービスで取扱う情報の格付、取扱制限等に応じた、情報の保存を許可（又は禁止）する国・地域
- クラウドサービス特有の脅威やクラウドサービスを利用して行う業務の特性等を踏まえて、ISMAP（Information system Security Management and Assessment Program）のみを許容することや ISMAP-LIU（ISMAP for Low-Impact Use）も含めて許容すること等

クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切なクラウドサービス提供者を選定することにより以下のようなリスクを低減することが考えられる。

- クラウドサービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、クラウドサービス提供者の運用詳細は公開されないためにクラウドサービス利用者にブラックボックスとなっている部分があり、クラウドサービス利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。
- オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス提供者との間の責任分界点やサービスレベルの合意が容易ではない。
- クラウドサービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つのクラウドサービス基盤で共用することとなるため、他の利用者の設定不備がクラウドサービス基盤全体のパフォーマンスへ影響を与えることや、クラウドサービス基盤のアクセス制御不備等により、他の利用者へ情報が漏えいするリスクが存在する。
- クラウドサービスに保存する情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることに伴うリスクが存在する。
- サーバ装置等機器の整備環境がクラウドサービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

なお、情報セキュリティ確保のためにクラウドサービス利用者自らが行うべきこと

と、クラウドサービス提供者に対して求めるべきこと等をまとめたガイドラインについては、以下の取組を参考にするとよい。

参考：デジタル庁「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」
（https://www.digital.go.jp/resources/standard_guidelines/）

参考：総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」
（https://www.soumu.go.jp/main_content/000771515.pdf）

参考：経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（2013 年度版）
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）

参考：経済産業省「クラウドセキュリティガイドライン活用ガイドブック」（2013 年度版）
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf）

参考：公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」
（https://www.fisc.or.jp/document/fintech/file/190_0.pdf）

- **遵守事項 4.2.1(1)(a)(ウ)「利用申請の許可権限者」について**

  クラウドサービスの利用申請の許可権限者は、原則として統括情報セキュリティ責任者が行うことを想定しているが、組織の規模や特性に応じて柔軟に定めてよい。ただし、利用を承認したクラウドサービスの記録は機関等内で共有できるようにすることが求められる。

- **遵守事項 4.2.1(1)(a)(エ)「クラウドサービス管理者」について**

  クラウドサービスの利用申請の許可権限者は、承認する際に当該申請に対する「クラウドサービス管理者」を指名することが求められるが、具体的には、情報システム（の構成要素）として調達・導入されるクラウドサービスについては情報システムセキュリティ責任者、その他の利用者自身の登録のみで利用可能なサービスについては課室情報セキュリティ責任者又は利用申請者自身を指名することを想定している。

- **基本対策事項 4.2.1(1)-2「ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP 等クラウドサービスリスト」という。）から選定する」について**

  クラウドサービスの選定においては、ISMAP の原則利用の考え方に基づき ISMAP において登録されたクラウドサービスから選定する必要がある。そのため、クラウドサービスの選定基準においては、ISMAP 等クラウドサービスリストから選定すること

を定める必要がある。やむを得ず ISMAP 等クラウドサービスリスト以外のクラウドサービスを選定する場合は、ISMAP の原則利用の考え方に基づき、最高情報セキュリティ責任者の責任において、ISMAP 制度で求めている要求事項や管理基準を満たしていることを確認することをクラウドサービス選定基準に含める必要がある。

なお、ISMAP においては、統一的なセキュリティ要求基準に基づき安全性評価がなされたクラウドサービスを、ISMAP 等クラウドサービスリストに登録している。登録がなされたクラウドサービスの詳細情報には、ISMAP に言明された内容として、詳細なサービス機能やリージョンの情報、ISMAP の基本言明要件のうち実施している統制目標の管理策、準拠法/裁判管轄等の情報等が公開されている。機関等においては、これらの情報も踏まえた上でクラウドサービスを選定することも選定基準に含めるとよい。

ISMAP 原則利用の考え方については、「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」及び ISMAP に関連する制度規程等を参照すること。

参考：サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」
（https://www.cyber.go.jp/policy/group/general/ismap.html）

参考：政府情報システムのためのセキュリティ評価制度（ISMAP）
（https://www.cyber.go.jp/policy/group/general/ismap.html）
（https://www.ismap.go.jp）

- **基本対策事項 4.2.1(1)-3 b)「クラウドサービスの名称」について**

  クラウドサービスの中には複数のサービス（機能）を含んだものが存在する。含まれる個々のサービス（機能）において情報セキュリティの対策が異なる場合は、個々のサービスに分割して申請する必要がある。

- **基本対策事項 4.2.1(1)-3 b)「クラウドサービスリストの種類」について**

  ISMAP と ISMAP-LIU では枠組みが異なるため、申請時においてどちらの申請か明らかにする必要がある。

- **基本対策事項 4.2.1(1)-3 b)「選定時の確認結果」について**

  クラウドサービスの利用申請時には、申請前に実施した選定におけるセキュリティ要件の確認結果の提出が求められる。確認結果には、ISMAP 等クラウドサービスリストの詳細情報において対象外としている管理策があった場合の確認結果や機関等の情報が取り扱われる国や地域についての検討結果等を含める必要がある。

- **基本対策事項 4.2.1(1)-4「クラウドサービスの利用状況」について**

  クラウドサービスの中には職員等が直接登録し利用可能なものがあり、その利用状況を機関として一元的に把握するのが困難であることが多い。シャドーIT は監視が不

十分になりやすく、セキュリティリスクが高まる等の問題がある。そのため、シャドーIT の対策としては、職員等がクラウドサービスを利用する場合に必ず申請を行い機関等が承認を行う運用が考えられる。また、CASB（Cloud Access Security Broker）と呼ばれる“クラウドサービスの利用度の可視化”や“アクセス制御”などの機能を持つサービス等を利用することで、実際の利用状況を調査・監視することも可能になるので、導入を検討することも考えられる。

遵守事項

(2) クラウドサービスの選定

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討すること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めること。

(ア) クラウドサービスに求める情報セキュリティ対策

(イ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(ウ) クラウドサービスに求めるサービスレベル

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則としてISMAP 等クラウドサービスリストからクラウドサービスを選定すること。

【 基本対策事項 】

＜4.2.1(2)(b)(ア)関連＞

4.2.1(2)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスに求めるセキュリティ要件策定に当たっては、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準を求めること。

＜4.2.1(2)(b)(ア)(イ)(ウ)関連＞

4.2.1(2)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務に特有のリスクを踏まえ、クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法、クラウドサービスに求める情報セキュリティ対策やサービスレベル等をクラウドサービスに求めるセキュリティ要件に含めること。

＜4.2.1(2)(c)関連＞

4.2.1(2)-3 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを選定するに当たっては、ISMAP 等クラウドサービスリストの詳細情報等を用いて、(2)(b)で定めたセキュリティ要件を満たしていることを確認すること。

（解説）

- **遵守事項 4.2.1(2)(b)(イ)「情報が保存される国・地域」について**

クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって情報が保存される国や地域を指定することができるものもある。また、定型約款等において情報の保存される国や地域が指定されているサービスも存在する。そのため、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要がある。適切なかつ透明性のある手続き（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形でクラウドサービス内の情報が外国の法執行機関の命令に

より強制的に開示されるといったリスクがあると判断される場合には留意する必要がある。なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、機関等の管理する暗号鍵で情報を暗号化するなどの措置を検討するとよい。ただし、この場合において、暗号鍵管理にクラウドサービス等を利用する場合には暗号鍵に係る情報が保存される国や地域にも注意が必要である。

- **遵守事項 4.2.1(2)(b)(イ)「廃棄の方法」について**

クラウドサービスの利用を終了する際、クラウドサービスに保存した情報を確実に抹消する必要がある。そのため、クラウドサービスを選定する際に、情報を確実に抹消する方法を定めておく必要がある。例えば、暗号化消去を用いる場合は、機関等で用意した暗号化に用いる鍵を当該クラウドサービスで利用することができることを条件にすることや、やむを得ずクラウドサービス提供者が暗号鍵を管理する場合、情報を保存する前に機関等が管理する別の暗号鍵を用いて暗号化するなどの要件を定めることが考えられる。

- **遵守事項 4.2.1(2)(b)(ウ)「サービスレベル」について**

クラウドサービスにおいては、利用するサービスごとにサービス品質保証が定められている。情報システムの一部にクラウドサービスを利用する場合は、クラウドサービスが停止した際の影響度によっては、情報システム全体のサービスレベルを低下させる可能性があるため、利用するクラウドサービスのサービス品質について許容できる範囲を事前に定めておく必要がある。また、クラウドサービスで情報セキュリティに関する問題が発生した際や一般的な問い合わせに関するサポートの対応時間等についても許容できる範囲を定め、クラウドサービスを選定する必要がある。

- **遵守事項 4.2.1(2)(c)「原則として ISMAP 等クラウドサービスリストからクラウドサービスを選定する」について**

クラウドサービスの選定においては、原則として ISMAP 等クラウドサービスリストから選定する必要がある。やむを得ず ISMAP 等クラウドサービスリスト以外のクラウドサービスを選定する場合は、ISMAP の原則利用の考え方に基づき、最高情報セキュリティ責任者の責任において、ISMAP 制度で求めている要求事項や管理基準を満たしていることを確認する必要がある。

ISMAP 原則利用の考え方については、「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」を参照すること。

また、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずる必要がある。

参考：サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」

（https://www.cyber.go.jp/policy/group/general/ismap.html）

参考：ISMAP クラウドサービスリスト
（https://www.ismap.go.jp/csm?id=cloud_service_list）

参考：内閣官房国家サイバー統括室「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ）
（https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf）

- **基本対策事項 4.2.1(2)-1「ISMAP 管理基準の管理策基準が求める対策と同等以上」について**

クラウドサービスのセキュリティ要件策定に当たっては、ISMAP 管理基準の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）を原則として全て満たす対策を含める必要があることに注意し、また、各機関等において定められた対策基準から求められる内容も全て反映されるようにする必要がある。

なお、機密性 3 情報をクラウドサービスで取り扱う場合には、ISMAP 管理基準が想定する情報の格付を踏まえ、ISMAP 管理基準の管理策基準の末尾に B が付された詳細管理策に加え、B が付されていない詳細管理策を複数要求するなど、追加で必要となる対策をセキュリティ要件に含める必要がある。

参考：政府情報システムのためのセキュリティ評価制度（ISMAP）、政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準
（https://www.cyber.go.jp/policy/group/general/ismap.html）
（https://www.ismap.go.jp）

- **基本対策事項 4.2.1(2)-3「ISMAP 等クラウドサービスリストの詳細情報等」について**

ISMAP 等クラウドサービスリストの詳細情報には、対象外としている管理策が含まれている可能性があるため、当該項目が対象外であっても機関等が求めているセキュリティ要件を満たすことができるかを確認する必要がある。

遵守事項

(3) クラウドサービスの利用に係る調達

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得ること。また、調達仕様の内容は、契約に含めること。

【 基本対策事項 】

＜4.2.1(3)(b)関連＞

4.2.1(3)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、調達仕様の内容を契約に含める際、クラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

（解説）

- **遵守事項 4.2.1(3)(a)「クラウドサービスを調達する場合」・遵守事項 4.2.1(3)(b)「クラウドサービスを調達する場合」について**

本項は、クラウドサービスを調達する場合に限り遵守することが求められる。

なお、調達を伴わない場合は本項の対象外であるが、遵守事項 4.2.1(2)「クラウドサービスの選定」に基づき、クラウドサービスを選定する必要がある。

- **基本対策事項 4.2.1(3)-1「役割及び責任の範囲が明確になっていることを確認」について**

クラウドサービスの提供形態及び提供機能は多様であることから、その情報セキュリティ対策の実施においても、クラウドサービス提供者が行う場合、クラウドサービス利用者がクラウドサービスの機能を用いて行う場合、クラウドサービス利用者が自ら行う場合等が考えられる。情報セキュリティ対策の詳細や実施主体が明確でない状況で情報セキュリティインシデントが発生した場合、その対応（ログの確認等）において問題が生じることが想定されることから、情報セキュリティ確保のためにクラウドサービス利用者が自ら行うべきことと、クラウドサービス提供者が行うべきことを明確にした上で、調達及び契約を進める必要がある。

遵守事項

(4) クラウドサービスの利用承認

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行うこと。

(b) 利用申請の許可権限者は、前項におけるクラウドサービスの**利用申請を審査**し、利用の可否を決定すること。

(c) 利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、**クラウドサービス管理者を指名**すること。

【 基本対策事項 】

＜4.2.1(4)(b)関連＞

4.2.1(4)-1 利用申請の許可権限者は、クラウドサービスの利用申請の審査においては、以下を全て含む内容を審査し、利用の可否を決定すること。

a) クラウドサービス提供者が、業務に特有のリスクを踏まえたクラウドサービス提供者の選定条件を満たしていること。

b) 利用するクラウドサービスのセキュリティ要件が、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準であること。

c) クラウドサービスで取り扱う情報が保存される国・地域及び情報の廃棄方法が、機関等が求めるセキュリティ要件を満たしていること。

d) クラウドサービスに求めるサービスレベルが、機関等が求めるセキュリティ要件を満たしていること。

（解説）

- **遵守事項 4.2.1(4)(b)「利用申請を審査」について**

利用申請の審査においては、利用申請されたクラウドサービスが、クラウドサービス提供者の選定基準とクラウドサービスのセキュリティ要件の両者を満たす場合に承認される必要がある。また、利用申請の審査をする時期については、クラウドサービスの契約前までに行うことが望ましい。

利用申請されたクラウドサービスの確認においては、単に ISMAP 等クラウドサービスリストに掲載されていることにとどまらず、当該リストの内容についても確認することが重要である。具体的には ISMAP 等クラウドサービスリストに掲載されているクラウドサービスの中には、ISMAP 管理基準で求めている項目において、一部の要件について合理的な適用が不適当と判断して対象外としているものが存在するが、対象外とした項目が機関等の求めている基準を満たしているか、取り扱う情報が保存される国・地域及び情報の廃棄方法が要件を満たしているか、求めるサービスレベルを満たしているか等を確認する必要がある。

- **遵守事項 4.2.1(4)(c)「クラウドサービス管理者を指名」について**

  クラウドサービスの利用は利用申請ごとに条件の異なることが想定されるため、仮に同一部局内で既に同一のクラウドサービスの承認があっても、業務内容や情報の格付、利用者の所属する組織の違いに応じて「クラウドサービス管理者」をそれぞれ立てることで管理が容易になる場合が考えられる。「クラウドサービス管理者」を指名する際には、当該クラウドサービスが情報システムの調達を伴うものの場合は「情報システムセキュリティ責任者」、職員等の利用登録のみで利用可能なものは「課室情報セキュリティ責任者」のように申請内容を加味した上で決定することが望ましい。

4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）

目的・趣旨

クラウドサービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後のクラウドサービスを利用した情報システムの導入・構築、運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。

クラウドサービスのサービス内容は非常に早いサイクルで変化しており、新たに追加される機能を活用することで業務の効率化や情報セキュリティの向上を図ることができる。一方で、構築時には想定していなかった脅威や脆弱性が発生する可能性もある。したがって、クラウドサービスの利用においては、情報セキュリティ対策の定期的な確認による見直しをすることで、セキュリティ要件の追加及び修正を漏れなく実施することが求められる。さらに、クラウドサービスへのアクセス権限については、機関等の業務やクラウドサービスの利用環境等の変化に応じて、定期的な確認による見直しをすることが重要である。

なお、本款ではクラウドサービスを利用する場合のライフサイクルの各段階において、特に必要となる情報セキュリティ対策を示しており、情報システム全体のライフサイクルの各段階で必要な情報セキュリティ対策については、5.2「情報システムのライフサイクルの各段階における対策」で定める遵守事項についても併せて遵守する必要がある。

遵守事項

(1) クラウドサービスの利用に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備すること。

(b) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備すること。

(c) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備すること。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) クラウドサービスの利用のために作成したアカウントの廃棄

【 基本対策事項 】

＜4.2.2(1)(a)関連＞

4.2.2(1)-1 統括情報セキュリティ責任者は、不正なアクセスを防止するため、以下を全て含む構築時におけるアクセス制御に係る基本方針を運用規程に含めること。

a) クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

b) クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御
c) クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者に対する強固な認証技術の利用
d) クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認及び要求事項を満たすための措置の実施
e) クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることの確認及び適切なアクセス制御の実施
f) クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制
g) クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施
h) インターネット等の機関等外通信回線から機関等内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施
i) クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うための必要なログの管理

4.2.2(1)-2 統括情報セキュリティ責任者は、取り扱う情報の機密性保護のため、以下を全て含む構築時における暗号化に係る基本方針を運用規程に含めること。
a) クラウドサービス内及び通信経路全般における暗号化の確認及び適切な実施
b) 情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認

4.2.2(1)-3 統括情報セキュリティ責任者は、以下を全て含む構築時における開発時のセキュリティ対策に係る基本方針を運用規程に含めること。
a) クラウドサービスを利用する場合のクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用
b) クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアのクラウドサービス上におけるライセンス規定

4.2.2(1)-4 統括情報セキュリティ責任者は、以下を全て含む構築時における設計・設定時の誤り防止に係る基本方針を運用規程に含めること。
a) クラウドサービスを利用する際のクラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用
b) クラウドサービスを利用する際の設定の誤りを見いだすための対策
c) クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視・制御
d) 利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測
e) 利用するクラウドサービス上で要安定情報を取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で構築する場合の可用性を考慮した設計
f) クラウドサービス内における時刻同期の方法の確認

＜4.2.2(1)(b)関連＞

4.2.2(1)-5 統括情報セキュリティ責任者は、以下を全て含む運用・保守時における利用方針に係る基本方針を運用規程に含めること。

a) 責任分界点を意識したクラウドサービスの利用

b) 利用承認を受けていないクラウドサービスの利用禁止

c) クラウドサービス提供者に対する定期的なサービスの提供状態の確認

d) 利用するクラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

4.2.2(1)-6 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス利用に必要な運用・保守時における教育に係る基本方針を運用規程に含めること。

a) クラウドサービス利用のための規定及び手順について

b) クラウドサービス利用に係る情報セキュリティリスクとリスク対応について

c) クラウドサービス利用に関する適用法令や関連する規制等について

4.2.2(1)-7 統括情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービスで取り扱う資産の管理に係る基本方針を運用規程に含めること。

a) クラウドサービス上で利用する IT 資産の適切な管理

b) クラウドサービス上に保存する情報に対する適切な格付・取扱制限の明示

c) クラウドサービスの機能に対する脆弱性対策について、クラウドサービス利用者の責任範囲の明確化と対策の実施

4.2.2(1)-8 統括情報セキュリティ責任者は、不正アクセスを防止するため、以下を全て含む運用・保守時におけるアクセス制御に係る基本方針を運用規程に含めること。

a) 管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

b) クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

c) クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

d) 利用するクラウドサービスの不正利用の監視

4.2.2(1)-9 統括情報セキュリティ責任者は、クラウドサービスで取り扱う情報の機密性保護のため、以下を全て含む運用・保守時における暗号化に係る基本方針を運用規程に含めること。

a) 暗号化に用いる鍵の管理者と鍵の保管場所等の鍵管理機能

b) 鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

c) 鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

4.2.2(1)-10 統括情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービス内の通信の制御に係る基本方針を運用規程に含めること。

a) 利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認

4.2.2(1)-11　統括情報セキュリティ責任者は、以下を全て含む運用・保守時における設計・設定時の誤りの防止に係る基本方針を運用規程に含めること。

a) クラウドサービスの設定を変更する場合の**設定の誤りを防止するための対策**

b) クラウドサービス利用者が行う可能性のある**重要操作の手順書の作成と監督者の指導の下での実施**

4.2.2(1)-12　統括情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービスを利用した情報システムの事業継続に係る基本方針を運用規程に含めること。

a) 不測の事態に対してサービスの復旧を行うために必要な**バックアップの確実な実施**。又は、クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認

b) 要安定情報をクラウドサービスで取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で構築する場合の**十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施**

c) クラウドサービス提供者からの**仕様内容の変更通知に関する内容確認と復旧手順の確認**

d) クラウドサービスで利用している**データ容量、性能等の監視**

＜4.2.2(1)(c)(ア)関連＞

4.2.2(1)-13　統括情報セキュリティ責任者は、以下を全て含む更改・廃棄時における利用終了手順に係る基本方針を運用規程に含めること。

a) クラウドサービスの利用を終了する場合の**移行計画書又は終了計画書の作成**

b) 移行計画書又は終了計画書の**クラウドサービス利用者への事前通知**

＜4.2.2(1)(c)(イ)関連＞

4.2.2(1)-14　統括情報セキュリティ責任者は、以下を全て含む更改・廃棄時における情報の廃棄に係る基本方針を運用規程に含めること。

a) **情報の廃棄方法**

b) 暗号化消去が実施できない場合の**基盤となる物理機器の廃棄方法**

＜4.2.2(1)(c)(ウ)関連＞

4.2.2(1)-15　統括情報セキュリティ責任者は、以下を全て含む更改・廃棄時におけるアカウントの廃棄に係る基本方針を運用規程に含めること。

a) 作成された**クラウドサービス利用者アカウントの削除**

b) 利用した**クラウドサービスにおける管理者アカウントの削除又は返却と再利用の確認**

c) クラウドサービス利用者アカウント以外の**特殊なアカウントの削除と関連情報の廃棄**

（解説）

- **基本対策事項 4.2.2(1)-1 a)「ライフサイクルにおける管理」について**

クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサー

ビス利用者が登録する識別コードに対して、その作成から廃棄に至るまでのライフサイクルにおけるクラウドサービス管理者による管理について以下の項目を定めることを基本方針として運用規程に含めることが求められる。

- オンプレミスの統合 ID 管理基盤との連携や、ID 管理機能提供サービス（IDaaS）との連携方式
- より強力な認証方式の採用（多要素主体認証方式等）
- 管理者権限をもつ識別コードの取扱い

- **基本対策事項 4.2.2(1)-1 b)「ネットワークに対するサービスごとのアクセス制御」について**

同一のクラウドサービス提供者が提供するクラウドサービスであっても、そのサービス内容によってはアクセス方法を限定する必要があるため、サービスごとのアクセス制御を実施することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-1 c)「強固な認証技術の利用」について**

クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者の主体認証情報が漏えいした場合、インターネットから直接管理権限を要する操作が可能となるため、十分に強固な認証技術（例えば、多要素主体認証方式）を利用することを基本方針として運用規程に含めることが求められる。

多要素主体認証方式については、「（解説）基本対策事項 7.1.1(1)-2「多要素主体認証方式」について」を参照のこと。

- **基本対策事項 4.2.2(1)-1 d)「主体認証情報の管理機能が要求事項を満たすことの確認及び要求事項を満たすための措置の実施」について**

機関等が要求する主体認証情報に係る規定、例えば、パスワード等の主体認証情報に係る規定（パスワード長など）に対し、クラウドサービス提供者が提供する機能等が十分かどうか確認を行い、機関等の要求事項を満たすための措置を実施させることを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-1 e)「クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることの確認及び適切なアクセス制御の実施」について**

クラウドサービスを利用するに当たり、クラウドサービスの利用者がクラウドサービスで取り扱う情報やクラウドサービスの機能へアクセスする制御ができることを確認した上でその制御に係る基本方針を運用規程に含めることが求められる。制御に係る基本方針については、以下を例とする機能が利用可能である場合は、利用させるなどを検討するとよい。

- クラウドサービスへ影響を与える重要な操作に対するアクセス制限
- 一定回数続けてログインに失敗した場合のアクセス制限
- 特定の IP アドレス等以外からのアクセス制限
- 機関等支給以外の端末からのアクセス制限
- 利用時間帯や利用する場所によるアクセス制限

- **基本対策事項 4.2.2(1)-1 f)「クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制」について**

  クラウドサービスに影響を与える操作をクラウドサービス利用者が行うことができる場合には、制限を設ける必要があるか検討をするとよい。また、クラウドサービスの構成等の変更は、クラウドサービス提供者が用意した機能の他にユーティリティプログラムが存在する可能性があるため、その利用についても検討するとよい。

- **基本対策事項 4.2.2(1)-1 g)「クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施」について**

  クラウドサービス上に構成される仮想マシンは、展開直後はセキュリティ設定が何もされていない場合があり、外部のネットワークへ接続が可能となっていることがあるため、事前に外部へのネットワークと通信できないようにすることや、やむを得ない場合は速やかに必要なセキュリティ対策を実施させることなどを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-1 h)「適切なセキュリティ対策の実施」について**

  クラウドサービスは、機関等内のネットワークの外にあるため、アクセス管理を厳密に行う必要がある。このアクセス管理は責任分界点としてはクラウドサービス利用者側の責任であるため、クラウドサービス提供者の実施するセキュリティ対策では対応ができない。したがって、クラウドサービスを利用する端末からのアクセスを適切にコントロールする必要がある。インターネット等から直接クラウドサービスへアクセスを許可する場合は、以下を例とする対策を検討し基本方針として運用規程に含めるとよい。

  - 多要素主体認証方式による主体認証
  - アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御を用いたセキュリティ設計
  - CASB の導入
  - デバイス認証による端末アクセス制御

- **基本対策事項 4.2.2(1)-1 i)「必要なログの管理」について**

  クラウドサービスにおけるログの取得は、オンプレミス環境と同様に悪意ある第三者等による外部からの不正侵入や不正操作等の情報セキュリティインシデントの予兆、検知や、情報セキュリティインシデントが発生した際の原因究明等に利用するため特に重要である。よって、クラウドサービスにおけるログの取得についてもオンプレミス環境と同様に適切に取得できるよう設定するとともに、改ざんや消失等が起こらないよう、適切に保全するよう基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-2「暗号化」について**

  クラウドサービス内で取り扱う情報の機密性を保護するため、情報の流通経路全般に渡る暗号化の検討、暗号化方式の選択、暗号鍵の管理などについて基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-2 a)「クラウドサービス内及び通信経路全般における暗号化」について**

  クラウドサービス内及び通信経路全般における暗号化を確認する際は、以下を例とする項目について確認することを基本方針として運用規程に含めることが求められる。特に、クラウドサービスにおいて利用可能な暗号機能にはサーバサイド暗号化とクライアントサイド暗号化があり、両者には鍵管理を含めた暗号機能の実装と運用に関わる責任分界に大きな相違があるため注意が必要である。

  - クラウドサービス上で取り扱われる情報に要機密情報が含まれるか確認し、含まれる場合は通信経路全般において暗号化されていることを確認する。
  - 利用される暗号化方式は、「電子政府推奨暗号リスト」に記載された暗号化方式であること。「電子政府推奨暗号リスト」に記載されていない暗号化方式を採用する場合、「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、リスクを低減するために十分な強度をもち、実際にデータを送受信し復号できることを確認する等により他の情報システムとの連携に問題がないことをクラウドサービス提供者とともに確認する。
  - クラウドサービス提供者が暗号機能を提供する場合は、提供される暗号機能がクラウドサービス利用者の要求事項を満たすことを確認する。
  - クラウドサービス提供者が暗号機能を提供する場合は、提供される暗号機能がクラウドサービス利用者の利用する他の暗号による保護と整合性があることを確認する。
  - クラウドサービス提供者が暗号機能を提供する場合は、暗号機能が提供される範囲を確認する。

- **基本対策事項 4.2.2(1)-2 b)「情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認」について**

  適用する暗号による一連の管理策が、関連する協定、法令及び規制を順守していることを確認することを基本方針として運用規程に含めることが求められる。(「電子政府推奨暗号リスト」に記載されていない暗号化方式を利用する場合、特に輸出規制等に注意が必要である。)

- **基本対策事項 4.2.2(1)-3「開発」について**

  利用するクラウドサービスの開発手順がセキュリティ要件を満たしているかまた、自らのセキュリティ要件との違いがあるかを確認するよう基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-3 a)「クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用」について**

  情報システムの構築を業務委託する際などは、遵守事項 4.1.2(2)(a)(ウ)の内容を調達仕様書に記載することが求められるが、更にクラウドサービスを利用する場合、クラウドサービス特有の手法等が存在するため、その情報をクラウドサービス提供者に要求し利用することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-3 b)「クラウドサービス上におけるライセンス規定」について**

  クラウドサービスにおいて、その仮想基盤は容易にスケールアウト、スケールインが可能であり、CPU 数によるライセンス価格が決定するソフトウェアなどの場合、オンプレミスで利用していた場合よりもはるかに高いライセンス費用が必要になる場合がある。特にクラウドサービスでは、基盤として複数の筐体を利用し仮想基盤を構築しているため、筐体に対するライセンスを使用するとライセンス違反となる場合があるため注意が必要である。やむを得ず筐体に対するライセンスを使用する場合は、クラウドサービスの機能として専用の物理的なサーバ装置を提供するサービスを利用するなど検討するとよい。

  なお、利用するソフトウェアによっては、クラウドサービス用のライセンスや、ソフトウェアを使用した分だけ利用料がかかるサービスなどが存在するので、事前に確認するとよい。

  よって、利用するソフトウェアをクラウドサービスにインストールすることを許可する前に、クラウド固有の使用許諾に関する要求事項を特定しなければならないことを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-4「設計・設定」について**

  クラウドサービスの設定の誤りを防止するために、クラウドサービス提供者からの推奨される設定情報の入手や、設定の誤りを検知する機能や性能を監視する機能の追加などを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-4 a)「クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用」について**

  クラウドサービスにおける情報システムの設計・構築はオンプレミスと同じ手法で十分とは限らない。また、クラウドサービスは提供者によって同様なシステムであってもその設計手法、対策が異なる。よって、クラウドサービスを利用して情報システムを構築する場合、その情報システムのセキュリティの最適化に資する設計、構築に係る情報をクラウドサービス提供者に要求し、不足している知見を補う必要があることを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-4 b)「設定の誤りを見いだすための対策」について**

  クラウドサービスにおいて、クラウドサービスの構成要素（リソース）の設定変更はオンプレミスにおける物理機器に対する変更と比べはるかに容易である。また、設定する内容はオンプレミスと似たものが多いが、クラウドサービス特有の対応（ネットワーク全般における設定等）が必要な場合もある。よって、誤った設定や設定漏れに起因する情報セキュリティインシデントを減らすために以下を例とする対策を検討することを基本方針として運用規程に含めることが求められる。

  - 設定内容のレビュー
  - クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用
  - 設定権限を与えるクラウドサービス利用者の限定
  - 責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化

- 開発プロセスへのセキュリティ対策の組み込み

- **基本対策事項 4.2.2(1)-4 d)「利用するデータ容量や稼働性能についての監視と将来の予測」について**

  クラウドサービスはオンプレミス環境と異なり、要求するデータ容量や性能等のリソースに増減が発生した場合、スケールアウト、スケールイン等によりリソースを柔軟に増減させることが可能なだけでなく、利用実績に応じて自動的にリソースを増減させるサービスも存在するため、リソース不足によるサービス停止とならないよう適切に監視を行う必要がある。また、監視の他にリソースの現在の利用状況や将来の利用予測を行い設計当初の要求と比較することも重要である。よって、クラウドサービスで利用するデータ容量等について監視させるとともに将来の予測を行った上での対策の見直し等を行うことを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-4 f)「時刻同期の方法の確認」について**

  クラウドサービス内において時刻が同期していないと記録されたログ等の時刻の信頼性が下がり、情報セキュリティインシデント発生時の原因解析等に影響を及ぼすため、構築時に当該クラウドサービスにおける時刻同期の方法を確認し、確実に時刻が同期するように設計する必要があることを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-5 a)「責任分界点を意識したクラウドサービスの利用」について**

  クラウドサービスを利用する場合、クラウドサービス提供者との間で協力して情報システム全体の責任を担うことを認識する必要がある。また、その分界点は契約するサービスによって変わるため、契約時に交わされた合意内容を把握する必要がある。これら責任分界点を踏まえた上で運用時における規定や手順等を作成することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-5 b)「利用承認を受けていないクラウドサービスの利用禁止」について**

  本規定はシャドーIT の抑止を目的としたものである。

- **基本対策事項 4.2.2(1)-5 c)「定期的なサービスの提供状態の確認」について**

  クラウドサービスは、クラウドサービス提供者の都合によりそのサービス内容は容易に変更されてしまう場合があるため、クラウドサービス利用の当初に想定したセキュリティ対策が利用期間中に正しく機能しなくなることが想定される。よって、責任共有モデルで、クラウドサービス提供者側の責任として含まれる以下を例とする項目や契約時に同意した項目について、定期的にクラウドサービス提供者に確認することを基本方針として運用規程に含めることが求められる。

  - 情報の保存方法、保存場所、伝送経路
  - 情報の廃棄
  - ログ情報の収集と保存状況
  - 時刻同期の状況

- バックアップの実施
- 不正アクセスの監視

- **基本対策事項 4.2.2(1)-5 d)「情報セキュリティインシデント発生時の連絡体制」について**

利用するクラウドサービスにおいて情報セキュリティインシデントの発生を検知した場合に備えて、連絡する体制を事前に定める必要がある。情報セキュリティインシデントの発生の検知については、クラウドサービス提供者から通知される可能性を考慮し、当該通知を複数の職員等が受け取れるようにすることも重要である。また、連絡先にはクラウドサービス提供者や当該クラウドサービスの設計や構築、運用・保守などを業務委託する場合は、委託先の連絡先も含むように基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-6「運用・保守時における教育に係る基本方針」について**

クラウドサービスの利用はオンプレミスの情報システムと異なり、クラウドサービスごとに知識が必要となる。多くのクラウドサービス利用者は初めて当該サービスを利用することが多く、そのクラウドサービス特有の知識や経験を習得するのに時間を要する。また、クラウドサービスの多くがオンプレミスの情報システムと比較して開発頻度が高く、同一のサービスでも数か月でその仕様が変わるものも少なくない。このような状況に対応するには機関等内での教育だけでは不足することが予想されるため、積極的にクラウドサービス提供者が提供するトレーニングへの参加等を支援し、クラウドサービス利用者の当該クラウドサービスに対する理解を深める必要もある。

- **基本対策事項 4.2.2(1)-7 a)「IT 資産の適切な管理」について**

クラウドサービス利用において、そのサービス内容の設定等を容易に変更できるため、適切な管理と把握が必要となる。また、クラウドサービスによっては利用状況により提供する CPU やバックアップストレージ等のリソースを自動的に拡張するなどの機能を有しているため、オンプレミスで利用していたソフトウェアを導入する際にはライセンス等の管理も必要となる。よって IT 資産の適切な管理の実施を基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-7 c)「責任範囲の明確化と対策の実施」について**

例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドサービスに対するリスクであり、対策を講ずる必要がある。7.2.1「ソフトウェアに関する脆弱性対策」の内容を踏まえた対策の実施や責任分界点がクラウドサービス提供者側の実施する範囲にある場合はクラウドサービス提供者に対策の実施を求め、結果の報告を要求する必要がある。よって、これらの対応について基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-8 a)「アクセス管理と操作の確実な記録」について**

クラウドサービスにはインターネット等から操作するための管理コンソールが用意

されている場合が多いが、この管理コンソールに全体の管理者権限を有する利用者の識別コードでログインすると利用中の情報システムを全て削除できるなど重大な影響を及ぼすため、当該識別コードのアクセス管理は非常に重要である。よって、クラウドサービスの特性を踏まえて識別コードのアクセス管理を確実に実施させることを基本方針として運用規程に含めることが求められる。また、そのような識別コードは悪用された場合、重大な影響を及ぼす可能性があることから、管理できる範囲を限定し、分割することや多要素主体認証の機能を有している場合は適用することが考えられる。多要素主体認証が使用できない場合は、公開鍵認証をするなどが考えられる。公開鍵認証も使用できない場合は、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を有する主体認証情報を用いるのみならず当該識別コードのアクセスログを監視し、不正な利用がないか等の確認を徹底するなどを運用規程に含めるとよい。

強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等については、「(解説) 基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照のこと。

- **基本対策事項 4.2.2(1)-8 b)「割り当てたアクセス権限に対する定期的な確認による見直し」について**

  クラウドサービスは、利用者アカウントへの権限だけではなくサービスごとにアクセス権限を割り当てられる特殊なアカウントが存在する。それらのアカウントへ割り当てた権限も含めて、必要性、妥当性、利用期間、権限の範囲などを定期的に確認し、必要に応じて見直すよう基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-8 c)「ユーティリティプログラムを使用する場合の機能の確認と利用者の制限」について**

  利用するクラウドサービスにおいては、クラウドサービスのリソース(ネットワーク、仮想マシン等) の設定を変更するユーティリティプログラムが存在する場合がある。そのためその機能の利用に関する制限等を基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-8 d)「不正利用の監視」について**

  例えば、機関等外の者と情報を共有することを目的としてクラウドサービスを利用する場合は、利用者に対して注意を促すだけでは情報漏えい等のリスクを防ぐことは困難である。したがって、職員等が利用する情報に対する操作等を監視するための機能として DLP (Data Loss Prevention) などの仕組みを導入することが考えられる。そのため、監視のための機能を、必要に応じてクラウドサービス提供者に要求し、確実な監視が行えるよう基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-9「暗号化に係る基本方針」について**

  クラウドサービスにおいて要機密情報を扱うには情報の流通経路全般において暗号化の対策が必要となるが、クラウドサービスの個々の構成要素において対策を採るこ

とは容易ではないため、クラウドサービス提供者が提供する暗号化機能を利用して対応することが推奨される。暗号化の対策は 7.1.5「暗号・電子署名」のオンプレミスの対応と基本的には同じであるが、鍵の管理をクラウドサービス提供者が行う場合は注意が必要である。基本的に鍵の管理はクラウドサービス利用者側で行う必要があるが、鍵の管理をクラウドサービス提供者が提供するサービスを利用せざるを得ない場合は、詳細な情報をクラウドサービス提供者に要求し、リスク評価を行った上でクラウドサービスに情報を保存する前に機関等が用意した別暗号鍵を用いて保存するなどのリスクを低減するための措置を検討するよう基本方針として運用規程に含めることが求められる。

なお、鍵管理の具体的な手法として、主に以下の手法がある。採用する手法を検討する際は、手法ごとのセキュリティの安全性、導入コスト、運用負荷等を踏まえる必要がある。

- Cloud Native Encryption Service：利用者は鍵管理に関与せず、クラウドサービス提供者が鍵のライフサイクル（作成・保存・削除等）全体に渡って鍵管理を行う手法
- BYOK（Bring Your Own Key）：利用者が作成した鍵をクラウドサービス上の鍵管理システム（Key Management System、以下「KMS」という。）にアップロードし、KMS の機能を用いて管理を行う手法
- HYOK（Hold Your Own Key）：利用者が作成した鍵を KMS へアップロードするが、鍵の漏えいリスク低減のため、鍵の使用後は都度 KMS から鍵を削除する手法
- BYOE（Bring Your Own Encryption）：利用者自らがクラウド上に鍵管理システムを構築し、そのシステム上で鍵管理を行う手法
- MCKMS（Multi Cloud Key Management System）：利用者自らが複数のクラウドサービスを横断するように鍵管理システムを構築する手法

- **基本対策事項 4.2.2(1)-10 a)「他のネットワークと分離されていること」について**

クラウドサービスを利用する場合、クラウドサービス基盤内における自身の利用するネットワークが他のテナント及びクラウドサービス提供者が利用するネットワークと分離され、論理的に独立していることを確認することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-11 a)「設定の誤りを防止するための対策」について**

クラウドサービスの設定を変更する場合の設定誤りはサービス自体の停止などの広範囲な障害につながる可能性があり、それを避けるための対策は重要である。よって、以下を例とする設定の誤りを防止するための対策を行うことについて基本方針として運用規程に含めることが求められる。

- 定期的な設定の確認
- クラウドサービス提供者等が提供するセキュリティ設定・監視ツールの利用
- 設定権限を与えるクラウドサービス利用者の限定
- 責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化

- 開発プロセスへのセキュリティ対策の組み込み
- クラウドサービスの機能追加に係る設定の確認による見直し

なお、クラウドサービスにおける設定の誤りを防止するためのツールとして、CSPM（Cloud Security Posture Management）と呼ばれる製品が存在する。CSPM は、利用するクラウドサービス全体のセキュリティに関する設定不備や構成ミス等を可視化する機能等を有している。そのため、CSPM のような製品を用いて設定の誤りを防止することを基本方針として運用規程に含めることも考えられる。

- **基本対策事項 4.2.2(1)-11 b)「重要操作の手順書の作成と監督者の指導の下での実施」について**

クラウドサービス利用者の操作により利用中のクラウドサービスに重大な障害をもたらすことが予想される操作については、クラウドサービス管理者が指名した監督者の監視の下、実施することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-12 a)「バックアップの確実な実施」について**

クラウドサービスの利用においては、不測の事態に備えて確実なバックアップを取得する必要があるが、その機能をクラウドサービス提供者が提供する機能に委ねている場合もある。よって、クラウドサービス利用に係るバックアップについて確実な実施がなされるよう基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-12 b)「十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施」について**

復旧に係る手順の策定については、複数のリージョンに跨がる障害等のクラウドサービスの大規模障害時も想定して、代替措置も含めた業務への影響を最小限とすることを観点として盛り込むことが考えられる。

- **基本対策事項 4.2.2(1)-12 c)「仕様内容の変更通知に関する内容確認と復旧手順の確認」について**

クラウドサービス提供者によるサービス内容の変更が行われる際の事前通知を受けた場合、その影響範囲・影響度を確認し、必要に応じて対処するとともに、サービス停止等が発生した場合の復旧手順を確認することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-12 d)「データ容量、性能等の監視」について**

クラウドサービスを利用する場合は、利用するクラウドサービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用可能であることを確認する必要がある。また、想定を超える利用が予想される場合は、対策を検討する必要があるため、これらを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-13 a)「移行計画書又は終了計画書の作成」について**

クラウドサービスの利用終了において、クラウドサービス利用者への影響を考慮して移行計画書又は終了計画書を作成する必要があるため、基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-13 b)「クラウドサービス利用者への事前通知」について**

  移行計画書又は終了計画書については、当該サービスを利用する利用者に対して十分な余裕をもって通知することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-14 a)「情報の廃棄方法」について**

  クラウドサービスの利用終了時に、取り扱った全ての情報が、クラウドサービス基盤上から確実に抹消されていることを確認する必要があるため、基本方針として運用規程に含めることが求められる。確実に抹消されていることの確認方法としては、暗号化消去を目的とした情報の暗号化に用いた鍵については、バックアップを含めて抹消することやクラウドサービス提供者に、契約時に同意した情報の廃棄手順の実施報告書を要求し確認することなどが考えられる。

- **基本対策事項 4.2.2(1)-14 b)「基盤となる物理機器の廃棄方法」について**

  暗号化消去が行えないクラウドサービスを利用した場合、クラウドサービス提供者が、クラウドサービスの基盤となる装置等のセキュリティを保った処分又は再利用のための方針及び手順の確実な実施を確認する必要があるため、基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-15 a)「クラウドサービス利用者アカウントの削除」について**

  クラウドサービスを利用終了する際は、終了時に作成したクラウドサービスの利用者アカウントを全て削除することを基本方針として運用規程に含めることが求められる。

- **基本対策事項 4.2.2(1)-15 b)「クラウドサービスにおける管理者アカウントの削除又は返却と再利用の確認」について**

  クラウドサービスの利用を終了する際は、作成したクラウドサービス利用者アカウントが全て削除されていることを確認した上でクラウドサービスにおける管理者アカウントを削除し、又はクラウドサービス提供者に返却すること、及びクラウドサービスにおける管理者アカウントについては再利用されないことをクラウドサービス提供者に確認することを基本方針として運用規程に含めることが求められる。なお、確認する方法としては、クラウドサービス提供者へ直接問い合わせるほか、クラウドサービス提供者が提供するウェブサイトやドキュメントを確認するなどが考えられる。

- **基本対策事項 4.2.2(1)-15 c)「特殊なアカウントの削除と関連情報の廃棄」について**

  クラウドサービスの利用者アカウント以外の特殊なアカウント（ストレージアカウント等）を作成した場合は、サービス利用終了時に確実に削除すること、及び当該アカウントを利用して作成された情報についても廃棄されていることを確認することを基本方針として運用規程に含めることが求められる。

遵守事項

(2) クラウドサービスの利用に係るセキュリティ要件の策定

(a) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、クラウドサービスの**利用に係る内容を確認すること**。

(b) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、**クラウドサービスの利用に係るセキュリティ要件**を策定すること。

【 基本対策事項 】

＜4.2.2(2)(a)関連＞

4.2.2(2)-1 クラウドサービス管理者は、以下を全て含むクラウドサービスの利用に係る内容を確認すること。

a) クラウドサービス提供者が提供する**主体認証情報の管理機能が機関等の要求事項を満たすこと**。

b) **クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること**。

c) クラウドサービス利用者による**クラウドサービスに多大な影響を与える操作の特定**

d) **クラウドサービス内及び通信経路全般における暗号化**

e) クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの**クラウドサービス上におけるライセンス規定**

f) クラウドサービスのリソース設定を変更する**ユーティリティプログラムを使用する場合**の機能

g) **鍵管理機能をクラウドサービス提供者が提供する場合**の鍵管理手順と鍵の種類の情報の要求とリスク評価

h) **鍵管理機能をクラウドサービス提供者が提供する場合**の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

i) 利用するクラウドサービスのネットワーク基盤が**他のネットワークと分離されていること**。

j) **クラウドサービス提供者が提供するバックアップ機能を利用する場合**、求める要求事項が満たされること。

＜4.2.2(2)(b)関連＞

4.2.2(2)-2 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用するアカウント管理に関するセキュリティ機能要件を策定すること。

a) クラウドサービス提供者が付与又はクラウドサービス利用者が登録する**識別コードの作成から廃棄に至るまでのライフサイクルにおける管理**

b) クラウドサービスを利用する管理者権限を保有するクラウドサービス利用者に対する**強固な認証技術**

c) クラウドサービス提供者が提供する**主体認証情報の管理機能が要求事項を満たすための措置**

4.2.2(2)-3 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用するアクセス制御に関するセキュリティ機能要件を策定すること。

a) クラウドサービス上に保存する情報やクラウドサービスの機能に対して**適切なアクセス制御**

b) インターネット等の機関等外通信回線から機関等内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合の**適切なセキュリティ対策**

4.2.2(2)-4 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用する権限管理に関するセキュリティ機能要件を策定すること。

a) クラウドサービス利用者による**クラウドサービスに多大な影響を与える誤操作の抑制**

b) クラウドサービスのリソース設定を変更する**ユーティリティプログラムを使用する場合の利用者の制限**

4.2.2(2)-5 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用するログ管理に関するセキュリティ機能要件を策定すること。

a) クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために**必要なログの管理**

4.2.2(2)-6 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用する暗号化に関するセキュリティ機能要件を策定すること。

a) **クラウドサービス内及び通信経路全般における暗号化**の適切な実施

b) **情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認**

c) **暗号化に用いる鍵の保管場所等の管理**に関する要件

d) クラウドサービスで利用する**暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理**

4.2.2(2)-7 クラウドサービス管理者は、以下を全て含むクラウドサービスを利用する際の設計・設定時の誤り防止に関するセキュリティ要件を策定すること。

a) **クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策**

b) **クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用**

c) **クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用**

d) クラウドサービスの**設定の誤りを見いだすための対策**

4.2.2(2)-8 クラウドサービス管理者は、以下を全て含むクラウドサービス運用時の監視等の運用管理機能要件を策定すること。

a) クラウドサービス上に構成された情報システムのネットワーク設計における**セキュリティ要件の異なるネットワーク間の通信の監視**

b) 利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

c) クラウドサービス内における時刻同期の方法

d) 利用するクラウドサービスの不正利用の監視

4.2.2(2)-9 クラウドサービス管理者は、以下を全て含むクラウドサービスの可用性に関するセキュリティ要件を策定すること。

a) 利用するクラウドサービス上で要安定情報を取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で構築する場合の可用性を考慮した設計

4.2.2(2)-10 クラウドサービス管理者は、以下を全て含む利用するクラウドサービスにおいて情報セキュリティインシデントが発生した際の復旧に関する対策要件を策定すること。

a) 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施

（解説）

- **遵守事項 4.2.2(2)(a)「利用に係る内容を確認すること」について**

運用規程で整備した基本方針において、クラウドサービス管理者はクラウドサービスを利用開始するに当たって事前にクラウドサービスの特性や機能を確認する必要がある。なお、利用するクラウドサービスの形態や特性によっては、確認や適用できないものが存在する可能性がある。よって、クラウドサービス管理者は、利用するクラウドサービスごとに各規定の実施について記録し、対象外（適用不可）と判断した項目については対象外とした際のリスクを低減するための措置を検討した上で、対象外とした理由と検討結果を付記することが求められる。

- **遵守事項 4.2.2(2)(b)「クラウドサービスの利用に係るセキュリティ要件」について**

クラウドサービスの利用に係るセキュリティ要件については､利用するクラウドサービスの形態や仕様によって利用者側の責任において定めるセキュリティ要件の範囲が異なる場合がある。よって、クラウドサービス管理者は、利用するクラウドサービスごとに必要なセキュリティ要件をクラウドサービス提供者が提示している推奨設定や、業界標準、ベストプラクティス等を参照し、策定する必要がある。また、セキュリティ要件を策定するに当たっては、利用するクラウドサービスの機能や構成要素ごとに検討するとともにクラウドサービスの運用や利用終了時のセキュリティ要件についても併せて検討する必要がある。

- **基本対策事項 4.2.2(2)-1 a)「主体認証情報の管理機能が機関等の要求事項を満たすこと」について**

基本対策事項 4.2.2(1)-1 d)において定めている運用規程に基づき、機関等が要求する主体認証情報に係る規定、例えば、パスワード等の主体認証情報に係る規定（パスワード長等）に対し、クラウドサービス提供者が提供する機能等が十分かどうかの確認を実

施する必要がある。

- **基本対策事項 4.2.2(2)-1 b)「クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること」について**

  基本対策事項 4.2.2(1)-1 e)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者がクラウドサービスに保存した情報やクラウドサービスの機能へのアクセスをアクセス制御方針に従って制限できること及びそのような制限を実現することを確実にする仕組みを整備できることを確認する必要がある。

- **基本対策事項 4.2.2(2)-1 c)「クラウドサービスに多大な影響を与える操作の特定」について**

  基本対策事項 4.2.2(1)-1 f)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者に対してクラウドサービスに対するユーティリティプログラムの利用を許可する場合は、そのプログラムの機能を特定し、クラウドサービスの管理策を妨げないようにすることが重要である。

- **基本対策事項 4.2.2(2)-1 d)「クラウドサービス内及び通信経路全般における暗号化」について**

  基本対策事項 4.2.2(1)-2 a)において定めている運用規程に基づき、クラウドサービス内及び通信経路全般における暗号化を確認する際は、以下を例とする項目について確認することが求められる。特に、クラウドサービスにおいて利用可能な暗号機能にはサーバサイド暗号化とクライアントサイド暗号化があり、両者には鍵管理を含めた暗号機能の実装と運用に関わる責任分界に大きな相違があるため注意が必要である。

  - クラウドサービス上で取り扱われる情報に要機密情報が含まれるか確認し、含まれる場合は通信経路全般において暗号化されていることを確認すること。
  - 利用される暗号化方式は、「電子政府推奨暗号リスト」に記載された暗号化方式であること。「電子政府推奨暗号リスト」に記載されていない暗号化方式を採用する場合、「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、リスクを低減するために十分な強度をもち、実際にデータを送受信し復号できることを確認する等により他の情報システムとの連携に問題がないことをクラウドサービス提供者とともに確認すること。
  - クラウドサービス提供者が暗号機能を提供する場合は、提供される暗号機能がクラウドサービス利用者の要求事項を満たすことを確認すること。
  - クラウドサービス提供者が暗号機能を提供する場合は、提供される暗号機能がクラウドサービス利用者の利用する他の暗号による保護と整合性があることを確認すること。
  - クラウドサービス提供者が暗号機能を提供する場合は、暗号機能が提供される範囲を確認すること。

- **基本対策事項 4.2.2(2)-1 e)「クラウドサービス上におけるライセンス規定」について**

  基本対策事項 4.2.2(1)-3 b)において定めている運用規程に基づき、クラウドサービス管理者は、利用するソフトウェアをクラウドサービスにインストールすることを許可

する前に、クラウド固有の使用許諾に関する要求事項を特定しライセンス規定に違反しないか等を確認する必要がある。

なお、クラウドサービスで利用するソフトウェアのライセンスに関する注意点については「(解説) 基本対策事項 4.2.2(1)-3 b)「クラウドサービス上におけるライセンス規定」について」を参照のこと。

- **基本対策事項 4.2.2⑵-1 f)「ユーティリティプログラムを使用する場合」について**

  基本対策事項 4.2.2(1)-8 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスのリソース（ネットワーク、仮想マシン等）の設定を変更するユーティリティプログラムを使用する場合は、その機能を確認する必要がある。

- **基本対策事項 4.2.2⑵-1 g)「鍵管理機能をクラウドサービス提供者が提供する場合」・基本対策事項 4.2.2⑵-1 h)「鍵管理機能をクラウドサービス提供者が提供する場合」**

  基本対策事項 4.2.2(1)-9 b)及び c)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の管理に関する事項において以下を確認した上でリスク評価を実施しリスクを低減するための措置を検討する必要がある。

  - クラウドサービス提供者における鍵管理手順と鍵の種類の情報
  - クラウドサービス提供者における鍵の生成から廃棄に至るまでのライフサイクルにおける情報

- **基本対策事項 4.2.2⑵-1 i)「他のネットワークと分離されていること」について**

  基本対策事項 4.2.2(1)-10 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス基盤内における自身の利用するネットワークが他のテナント及びクラウドサービス提供者が利用するネットワークと分離され、論理的に独立していることを確認することが求められる。

  なお、論理的に独立していることの確認については、例えば利用するクラウドサービスのテナントに対して他のテナントからアクセスが制限されていることなどが考えられる。

- **基本対策事項 4.2.2⑵-1 j)「クラウドサービス提供者が提供するバックアップ機能を利用する場合」について**

  基本対策事項 4.2.2(1)-12 a)において定めている運用規程に基づき、クラウドサービス提供者が提供するバックアップ機能を利用する場合、クラウドサービス管理者は、クラウドサービス提供者にその仕様を要求し要求事項を満たすことを確認する必要がある。また、取得したバックアップが有効であることを定期的に確認する手段についても確認する必要がある。

- **基本対策事項 4.2.2⑵-2 a)「識別コードの作成から廃棄に至るまでのライフサイクルにおける管理」について**

  基本対策事項 4.2.2(1)-1 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードに対して、その作成から廃棄に至るまでの

ライフサイクルにおけるクラウドサービス管理者による管理について以下の項目に留意して策定することが求められる。

- シングルサインオンを行う場合の連携方式
- より強力な認証方式の採用（多要素主体認証方式等）
- 管理者権限をもつ識別コードの取扱い
- 構築時に利用した識別コードの主体認証情報の変更や識別コードの廃棄について

- **基本対策事項 4.2.2(2)-2 b)「強固な認証技術」について**

基本対策事項 4.2.2(1)-1 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者の主体認証情報が漏えいした場合、インターネットから直接管理権限を要する操作が可能となる可能性があるため、十分に強固な認証技術（例えば、多要素主体認証方式）を利用することが求められる。管理用のインタフェースがインターネットに公開されることを避けることと不正アクセスの検知・防御の観点から踏み台サーバを用意し、操作は踏み台サーバからのアクセスのみに限定するなどの対策も考えられる。なお、踏み台サーバへのアクセスにはSSHと公開鍵認証によるアクセスのみを許可するとよい。

- **基本対策事項 4.2.2(2)-2 c)「主体認証情報の管理機能が要求事項を満たすための措置」について**

基本対策事項 4.2.2(1)-1 d)において定めている運用規程に基づき、クラウドサービス管理者は、機関等が要求する主体認証情報に係る規定方針をクラウドサービス利用者が遵守できるための要件を策定することが求められる。例えば、利用者の主体認証情報を設定する際にパスワード長などを設ける機能がある場合は、その機能を用いることを求めるようにするなどが考えられる。

- **基本対策事項 4.2.2(2)-3 a)「適切なアクセス制御」について**

基本対策事項 4.2.2(1)-1 e)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスの利用者がクラウドサービスで取り扱う情報やクラウドサービスの機能へアクセスする制御を定めること。アクセス制御については、例えば、以下の機能が利用可能である場合は、セキュリティ要件として策定すべきか検討するとよい。

- クラウドサービスへ影響を与える重要な操作に対するアクセス制限
- 一定回数続けてログインに失敗した場合のアクセス制限
- 特定のIPアドレス等以外からのアクセス制限
- 機関等支給以外の端末からのアクセス制限
- 利用時間帯や利用する場所によるアクセス制限

- **基本対策事項 4.2.2(2)-3 b)「適切なセキュリティ対策」について**

基本対策事項 4.2.2(1)-1 h)において定めている運用規程に基づき、インターネット等の機関等外通信回線から機関等内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合、接続するデバイスからのアクセス

を適切にコントロールする必要がある。インターネット等から直接クラウドサービスへアクセスする場合は、以下を例とする対策を検討しセキュリティ要件を定めるとよい。

- 多要素主体認証方式による主体認証
- アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御を用いたセキュリティ設計
- CASB の導入
- デバイス認証による端末アクセス制御

- **基本対策事項 4.2.2(2)-4 a)「クラウドサービスに多大な影響を与える誤操作の抑制」について**

基本対策事項 4.2.2(1)-1 f)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスに影響を与える操作等をクラウドサービス利用者が行う場合には、制限を設ける等の検討を行いクラウドサービスの管理策を妨げないようにするセキュリティ要件を定める必要がある。また、クラウドサービスの構成等の変更は、クラウドサービス提供者が用意した機能の他にユーティリティプログラムが存在する可能性があるため、その利用についても制限を設ける等の検討をするとよい。

- **基本対策事項 4.2.2(2)-4 b)「ユーティリティプログラムを使用する場合の機能の確認と利用者の制限」について**

基本対策事項 4.2.2(1)-8 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスのリソース（ネットワーク、仮想マシン等）の設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者を制限するためのセキュリティ要件を定める必要がある。

- **基本対策事項 4.2.2(2)-5 a)「必要なログの管理」について**

基本対策事項 4.2.2(1)-1 i)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスにおけるログの取得についての要件を定める必要がある。利用するクラウドサービスによって取得できるログの種類や取得方法等が異なるため、クラウドサービスごとにセキュリティ要件を定める必要がある。取得すべきログの種類や取得方法等については、クラウドサービス提供者が提示している推奨方法や、業界標準、ベストプラクティス等を参照し、策定する必要がある。なお、クラウドサービスにおいては、複数のサービスのログを一元的に管理するための機能を提供しているものが存在する。そのような機能が提供されている場合は、ログ管理の観点から利用することが望ましい。

- **基本対策事項 4.2.2(2)-6 a)「クラウドサービス内及び通信経路全般における暗号化」について**

基本対策事項 4.2.2(1)-2 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス上で取り扱われる情報に要機密情報が含まれる場合は通信経路全般において暗号化するようにセキュリティ要件を定めること。また、機関等において暗号化を実施する場合は、利用する暗号化方式について、原則として「電子政府

推奨暗号リスト」に記載された暗号化方式を用いること。なお、クラウドサービス提供者が情報の暗号化に用いる鍵を用意する場合は、クラウドサービス提供者において情報の復号が可能な場合があるなどのリスクを評価し、クラウドサービスに情報を保存する前に機関等が用意した別暗号鍵を用いて保存するなどのリスクを低減するための措置を検討した上でセキュリティ要件を定めること。

- **基本対策事項 4.2.2(2)-6 b)「情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認」について**

  基本対策事項 4.2.2(1)-2 b)において定めている運用規程に基づき、セキュリティ要件として定めるクラウドサービスの利用において適用する暗号による一連の要件が、関連する協定、法令及び規制を順守していることを確認することが重要である。(「電子政府推奨暗号リスト」に記載されていない暗号化方式を利用する場合、特に輸出規制等に注意が必要である。)

- **基本対策事項 4.2.2(2)-6 c)「暗号化に用いる鍵の保管場所等の管理」について**

  基本対策事項 4.2.2(1)-9 a)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の保管場所に関するセキュリティ要件を定める必要がある。例えば、暗号鍵の保管場所については、暗号化した情報とは別の場所で管理することや、適正なかつ透明性のある手続き（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で暗号鍵が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場所には保管しないなどが考えられる。暗号鍵の管理については、基本対策事項 7.1.5(1)-3 b)「管理手順を定めること」を参照するとよい。

- **基本対策事項 4.2.2(2)-6 d)「暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理」について**

  基本対策事項 4.2.2(1)-9 c)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の生成から廃棄に至るまでのライフサイクルにおける管理に関するセキュリティ要件を定める必要がある。暗号鍵の管理は重要であり、暗号鍵の複製の可否や暗号鍵の利用者を特定するための要件なども含めると良い。暗号鍵の管理については、基本対策事項 7.1.5(1)-3 b)「管理手順を定めること」についてを参照するとよい。

- **基本対策事項 4.2.2(2)-7 a)「クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施」について**

  基本対策事項 4.2.2(1)-1 g)において定めている運用規程に基づき、クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策に関するセキュリティ要件を定めること。例えば、クラウドサービス上に構成される仮想マシンは、展開直後はセキュリティ設定が何もされていない場合があり、外部のネットワークへ接続が可能となっていることがあるため、事前に外部へのネットワークと通信できないようにすることを要件とすることや十分なセキュリティ対策がなされる要件を事前に定めておく必要がある。なお、具体的な対策としては、仮想マシンの OS に対して最新のセキュ

リティパッチを適用することや不正プログラム対策ソフトウェアを導入することなどが考えられる。

- **基本対策事項 4.2.2(2)-7 b)「クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用」について**

  基本対策事項 4.2.2(1)-3 a)において定めている運用規程に基づき、クラウドサービス管理者は、情報システムの構築を業務委託する際などは、遵守事項 5.2.1(3)(a)(ウ)の内容を調達仕様書に記載することが求められるが、更にクラウドサービスを利用する場合、クラウドサービス特有の手法等が存在するため、その情報をクラウドサービス提供者に要求しクラウドサービスのセキュリティを保つための開発手順等の必要なセキュリティ要件を定めること。

- **基本対策事項 4.2.2(2)-7 c)「クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用」について**

  基本対策事項 4.2.2(1)-4 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用して情報システムを構築する場合、その情報システムのセキュリティの最適化に資する設計、構築に係る情報をクラウドサービス提供者に要求し、不足している知見を補ったうえでセキュリティ要件を定める必要がある。

- **基本対策事項 4.2.2(2)-7 d)「設定の誤りを見いだすための対策」について**

  基本対策事項 4.2.2(1)-4 b)で定めている運用規程に基づき、クラウドサービス管理者は、誤った設定や設定漏れに起因する情報セキュリティインシデントを減らすための以下の対策を検討しセキュリティ要件として定める必要がある。

  - 設定内容のレビュー
  - クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用
  - 設定権限を与えるクラウドサービス利用者の限定
  - 責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化
  - 開発プロセスへのセキュリティ対策の組み込み

- **基本対策事項 4.2.2(2)-8 a)「セキュリティ要件の異なるネットワーク間の通信の監視」について**

  基本対策事項 4.2.2(1)-4 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス上のセキュリティ要件が異なるネットワーク同士の接続間の通信（トラフィック）を監視・制御するためのセキュリティ要件を定める必要がある。通常はこの位置にファイアウォールを構成し、トラフィックの制御を実施する。クラウドサービスによっては、ファイアウォールを細かく設置できるものもあるため、セキュリティ要件を策定する際にその設置箇所等を十分に検討する必要がある。また、これらの間の通信を監視して異常の検知を行うとともに、設定は定期的な確認による見直しを行うことが推奨される。

- **基本対策事項 4.2.2(2)-8 b)「利用するデータ容量や稼働性能についての監視と将来の予**

測」について

基本対策事項 4.2.2(1)-4 d)において定めている運用規程に基づき、クラウドサービス管理者は、リソースを柔軟に増減させることができる機能を有するクラウドサービスを利用する場合、当該クラウドサービスで利用する機能のリソース不足によるサービス停止とならないよう適切に監視を行うことができるようにセキュリティ要件を定めること。また、監視の他にリソースの現在の利用状況や将来の利用予測を行い設計当初の要求と比較できるようにすることも重要である。よって、クラウドサービスで利用するデータ容量等について監視させるとともに将来の予測を行った上での対策の確認による見直し等を行えるようにセキュリティ要件を定めておくことが重要である。なお、クラウドサービス提供者側で監視のためのサービスが用意されていない場合は、手動で定期的に確認する等の対策が求められる。

- **基本対策事項 4.2.2(2)-8 c)「時刻同期の方法」について**

基本対策事項 4.2.2(1)-4 f)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスにおける時刻同期の方法を確認し、確実に時刻が同期するようにセキュリティ要件を定める必要がある。クラウドサービス内において時刻が同期していないと記録されたログ等の時刻の信頼性が下がり、情報セキュリティインシデント発生時の原因解析等に影響を及ぼすおそれがあるため重要である。

- **基本対策事項 4.2.2(2)-8 d)「不正利用の監視」について**

基本対策事項 4.2.2(1)-8 d)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスへの不正利用を検知することが可能な監視機能をクラウドサービス提供者に要求し、監視を行うことをセキュリティ要件として定める必要がある。クラウドサービスの利用者の識別コードを含むクラウドサービス内に保持されるクラウドサービス利用者の情報に対して、クラウドサービス提供者がアクセスするものについてはあらかじめ両者で確認し、サービス利用開始後に当該情報へのアクセス履歴をクラウドサービス利用者が常に監視・確認できることが求められる。

なお、機関等外の者と情報を共有することを目的としてクラウドサービスを利用する場合は、職員等が利用する情報に対する操作等を監視するための機能として DLP などの仕組みを導入することが考えられる。

- **基本対策事項 4.2.2(2)-9 a)「可用性を考慮した設計」について**

基本対策事項 4.2.2(1)-4 e)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用して要安定情報を取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で構築する場合は、構築時に可用性を考慮して設計を行う必要があるためセキュリティ要件を定める必要がある。可用性の設計には、システムの地理的・電源的な独立性を踏まえた冗長化などのオンプレミスで行う対策と同じものも含まれるが、クラウドサービス特有の機能もあるためクラウドサービス提供者に当該サービスの可用性に係る機能等の詳細な情報を要求し、セキュリティ要件に反映させることが求められる。利用するクラウドサービス全体の利用停止に至る障害に対してやむを得ず措置を検討する場合は、マルチクラウドやオンプレ

ミスを含む代替サービスによる冗長化も考えられるが、運用の複雑さや管理の難しさなどを考慮した上で検討する必要がある。

- **基本対策事項 4.2.2(2)-10 a)「バックアップの確実な実施」について**

  基本対策事項 4.2.2(1)-12 a)において定めている運用規程に基づき、クラウドサービス管理者は、不測の事態に対して復旧が行えるように、クラウドサービスの設定内容や保存した情報などのバックアップに係るセキュリティ要件を定める必要がある。なお、クラウドサービスによっては、事前に構成のテンプレートを用意しておき不測の事態に対してそれを適用させ復旧させるものなどが存在するので、クラウドサービス提供者に対して推奨される要件を確認することが望ましい。また、取得したバックアップが有効であることを定期的に確認できるようにセキュリティ要件を定めることも重要である。

遵守事項

(3) クラウドサービスを利用した情報システムの導入・構築時の対策

(a) クラウドサービス管理者は、(1)(a)で定めた運用規程を踏まえて、(2)(b)において定めるセキュリティ要件に従い**クラウドサービス利用における必要な措置を講ずる**こと。また、導入・構築時に**実施状況を確認・記録する**こと。

(b) クラウドサービス管理者は、**情報システムにおいてクラウドサービスを利用する際**には、情報システム台帳及び関連文書に記録又は記載すること。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告すること。

(c) クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備すること。

(ア) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(イ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(ウ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

【 基本対策事項 】

＜4.2.2(3)(c)(ア)関連＞

4.2.2(3)-1 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順を実施手順として整備すること。

a) クラウドサービス利用のための**責任分界点を意識したクラウドサービス利用手順**

b) クラウドサービス利用者が行う可能性のある**重要操作の手順**

＜4.2.2(3)(c)(イ)関連＞

4.2.2(3)-2 クラウドサービス管理者は、以下を全て含む情報システムの運用・監視中に発生したクラウドサービスの利用に係る情報セキュリティインシデントを認知した際の対処手順を実施手順として整備すること。

a) クラウドサービス提供者との**責任分界点を意識した責任範囲の整理**

b) 利用するクラウドサービスのサービスごとの**情報セキュリティインシデント対処に関する事項**

c) 利用するクラウドサービスに係る**情報セキュリティインシデント発生時の連絡体制**

＜4.2.2(3)(c)(ウ)関連＞

4.2.2(3)-3 クラウドサービス管理者は、以下を全て含む利用するクラウドサービスが停止又は利用できなくなった際の復旧手順を実施手順として整備すること。

a) 要安定情報をクラウドサービスで取り扱う場合の**十分な可用性を担保した復旧に係る手順**

（解説）

- **遵守事項 4.2.2(3)(a)「クラウドサービス利用における必要な措置を講ずる」について**

  遵守事項 4.2.2(2)(b)で定めたセキュリティ要件に従ってクラウドサービスを利用し情報システムを構築又はクラウドサービスの設定等を実施するに当たっては、クラウドサービス提供者が提示している推奨設定や、業界標準、ベストプラクティス等を参照し必要な措置を講ずる必要がある。

  ベストプラクティスを参照するに当たっては、クラウドサービス提供者が提供している推奨設定等が存在するが、内閣官房国家サイバー統括室の「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊.クラウド設計・開発編」や総務省が公表している「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」等を参照することも考えられる。

  参考：内閣官房国家サイバー統括室「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊.クラウド設計・開発編」
  （https://www.cyber.go.jp/policy/group/general/sbd_sakutei.html）

  参考：総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」
  （https://www.soumu.go.jp/main_content/000771515.pdf）

- **遵守事項 4.2.2(3)(a)「実施状況を確認・記録する」について**

  遵守事項 4.2.2(1)(a)において定めている運用規程の各項目については、利用するクラウドサービスの形態（IaaS、PaaS、SaaS 等）及び仕様によっては適用できないものも存在する可能性もある。よって、クラウドサービス管理者は、利用するクラウドサービスごとに各規定の実施について記録し、対象外（適用不可）と判断した項目についてはその理由を付記することが求められる。

- **遵守事項 4.2.2(3)(b)「情報システムにおいてクラウドサービスを利用する際」について**

  情報システム台帳の整備内容の網羅性維持のため、クラウドサービス管理者は、クラウドサービスを利用し新規に情報システムを構築した際には、速やかに情報システム台帳に記載の事項を報告する必要がある。

  なお、クラウドサービス管理者は、必要に応じてクラウドサービスの利用に係る関連文書としてクラウドサービスの情報セキュリティ対策を維持するための情報を整備することが望ましい。その際、遵守事項 4.2.2(1)(a)において定めている運用規程の各項目について、対象外（適用不可）と判断した項目については対象外とした際のリスクを低減するための措置の検討結果と対象外とした理由を付記することが求められる。

- **基本対策事項 4.2.2(3)-1 a)「責任分界点を意識したクラウドサービスの利用手順」について**

  基本対策事項 4.2.2(1)-5 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス提供者との責任分界点を踏まえた運用時における規定や

手順等を作成することが求められる。利用するクラウドサービスによって、クラウドサービスの利用者側とクラウドサービスの提供者側の責任範囲が異なる。よって、クラウドサービスを契約する時に交わされた合意内容を把握し、責任分界点を踏まえたクラウドサービスの利用手順を用意する必要がある。

また、利用手順には、基本対策事項 4.2.2(1)-6 において定めた運用規程に基づき、運用・保守時における教育に係る基本方針を含める必要がある。更に、基本対策事項 4.2.2(1)-7 b)において定めている運用規程に基づき、クラウドサービスの利用者に対してクラウドサービス上に保存する情報に対する適切な格付・取扱制限の明示をすることを含める必要がある。利用するクラウドサービスにおいて、情報に対する適切な格付・取扱制限の明示をする機能を有している場合、その機能の使い方等を示すことも考えられる。

- **基本対策事項 4.2.2(3)-1 b)「重要操作の手順」について**

基本対策事項 4.2.2(1)-11 b)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者の操作により利用中のクラウドサービスに重大な障害をもたらすことが予想される操作については、その操作手順を文書化する必要がある。

- **基本対策事項 4.2.2(3)-2 a)「責任分界点を意識した責任範囲の整理」について**

クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって責任範囲が異なってくるが、クラウドサービスで取り扱う情報そのものや、クラウドサービスへアクセスするデバイスに関するセキュリティ対策等は、クラウドサービス利用者の責任範囲であると考えられる。そのような責任分界点を意識し、情報セキュリティインシデントが発生した際にどこまでが利用者の責任範囲、どこからがクラウドサービス提供者の責任範囲であるかを事前に整理する必要がある。

- **基本対策事項 4.2.2(3)-2 b)「情報セキュリティインシデント対処に関する事項」について**

情報セキュリティインシデント対処に関する事項に関しては、クラウドサービスの個別の事情に合わせて検討する必要がある。クラウドサービス管理者は、情報セキュリティインシデントを認知した際、機関等で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処する必要がある。情報セキュリティインシデントの対処方法については、利用するクラウドサービスの形態や仕様によって、契約に基づきクラウドサービス提供者に対処を講じさせる必要もある。利用するクラウドサービスの責任分界点を意識した責任範囲については、基本対策事項 4.2.2(3)-2 a)で整理しており、その責任範囲を踏まえて、クラウドサービス利用者とクラウドサービス提供者が行う対処を整理し、検討するとよい。そのような事情を踏まえて利用するクラウドサービスのサービスごとに情報セキュリティインシデント対処に関する事項を情報セキュリティインシデントに係る対処手順に含めておく必要がある。

なお、統括情報セキュリティ責任者が整備する対処手順(「(解説)遵守事項 2.2.4(1)(b)「対処手順」について」を参照のこと。)が、クラウドサービスの事情に応じた内容で

整備されているならば、クラウドサービス別に整備しなくても構わない。

- **基本対策事項 4.2.2(3)-2 c)「情報セキュリティインシデント発生時の連絡体制」について**

  基本対策事項 4.2.2(1)-5 d)において定めている運用規程に基づき、クラウドサービス管理者は、利用するクラウドサービスにおいて情報セキュリティインシデントの発生を検知した場合に、連絡する体制を事前に確認する必要がある。また、連絡先にはクラウドサービス提供者や当該クラウドサービスの構築や運用を業務委託している場合の委託先の連絡先も含めること。

- **基本対策事項 4.2.2(3)-3 a)「十分な可用性を担保した復旧に係る手順」について**

  基本対策事項 4.2.2(1)-12 b)において定めている運用規程に基づき、クラウドサービス管理者は、要安定情報を取り扱うクラウドサービス及び非常時優先業務等を支えるクラウドサービスにおける十分な可用性を担保した復旧に係る手順を事前に整備する必要がある。

  また、遠隔地クラスタなどの冗長構成を採用した場合もフェールオーバー及びフェールバック等の実施手順を用意するとよい。

遵守事項

(4) クラウドサービスを利用した情報システムの運用・保守時の対策

(a) クラウドサービス管理者は、(1)(b)で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に**実施状況を定期的に確認・記録すること**。

(b) クラウドサービス管理者は、クラウドサービスの運用・保守時に**情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合**、情報システム台帳及び関連文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告すること。

(c) クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により**見直し**を適時検討し、必要な措置を講ずること。

【 基本対策事項 】

＜4.2.2(4)(a)関連＞

4.2.2(4)-1 クラウドサービス管理者は、以下を全て含むクラウドサービスの利用に関する情報セキュリティ対策を実施すること。

a) クラウドサービス提供者に対する**定期的なサービスの提供状態の確認**

b) クラウドサービス上で利用する **IT 資産の適切な管理**

4.2.2(4)-2 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用するアカウント管理、アクセス制御、管理権限に関する情報セキュリティ対策を実施すること。

a) 管理者権限をクラウドサービス利用者へ割り当てる場合の**アクセス管理と操作の確実な記録**

b) クラウドサービス利用者に**割り当てたアクセス権限に対する定期的な確認による見直し**

4.2.2(4)-3 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用する機能に対する脆弱性対策を実施すること。

a) **クラウドサービスの機能に対する脆弱性対策の実施**

4.2.2(4)-4 クラウドサービス管理者は、以下を全て含むクラウドサービスを運用する際の設定変更に関する情報セキュリティ対策を実施すること。

a) クラウドサービスのリソース設定を変更する**ユーティリティプログラムを使用する場合**の利用者の制限

b) クラウドサービスの設定を変更する場合の**設定の誤りを防止するための対策**

c) クラウドサービス利用者が行う可能性のある**重要操作に対する監督者の指導の下での実施**

4.2.2(4)-5 クラウドサービス管理者は、以下を全て含むクラウドサービスを運用する際の監視に関する対策を実施すること。

a) 利用するクラウドサービスの**不正利用の監視**

b) クラウドサービスで利用している**データ容量、性能等の監視**

4.2.2(4)-6 クラウドサービス管理者は、以下を全て含むクラウドサービスを運用する際の可用性に関する情報セキュリティ対策を実施すること。

a) 不測の事態に対してサービスの復旧を行うために必要な**バックアップの確実な実施**

b) 要安定情報をクラウドサービスで取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で運用する場合の**十分な可用性の担保、復旧に係る定期的な訓練の実施**

c) クラウドサービス提供者からの**仕様内容の変更通知に関する内容確認と復旧手順の確認**

4.2.2(4)-7 クラウドサービス管理者は、以下を全て含むクラウドサービスで利用する暗号鍵に関する情報セキュリティ対策を実施すること。

a) クラウドサービスで利用する**暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理**の実施

（解説）

- **遵守事項 4.2.2(4)(a)「実施状況を定期的に確認・記録すること」について**

遵守事項 4.2.2(1)(b)において定めている運用規程の各項目については、利用するクラウドサービスの形態（IaaS、PaaS、SaaS 等）によっては適用できないものも存在する可能性もある。よって、クラウドサービス管理者は、利用するクラウドサービスごとに各規定の実施について記録し、対象外（適用不可）と判断した項目についてはその理由と対策を付記することが求められる。また、クラウドサービスは様々な要因で提供サービスの状況が変わることが想定されるため、本確認・記録作業は定期的に繰り返し行うことが求められる。

- **遵守事項 4.2.2(4)(b)「情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合」について**

情報システム台帳の整備内容の網羅性維持のため、クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等への修正又は変更が発生した場合、速やかに情報システム台帳更新又は修正し、統括情報セキュリティ責任者に報告する必要があるが、その報告の方法や時期については、機関等ごとに定めることが望ましい。

なお、クラウドサービス管理者は、必要に応じてクラウドサービスの利用に係る関連文書として整備したクラウドサービスの情報セキュリティ対策を維持するための情報も併せて更新又は修正することが求められる。

- **遵守事項 4.2.2(4)(c)「見直し」について**

クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について、新たな情報セキュリティ上の脅威、情報セキュリティインシデント発生事案例及び情報セキュリティインシデント発生時の影響等を検討した上で、クラウドサービスの情報セキュリティ対策について定期的な確認による見直しを行い、セキュリティ要件の追

加、修正等の必要な措置を講ずることが求められる。

なお、クラウドサービスに変更があった場合やクラウドサービスの外部環境に変化が生じた場合等の際には、定期的な情報セキュリティ対策の確認による見直しに加えて、適時見直すことも重要である。

- **基本対策事項 4.2.2(4)-1 a)「定期的なサービスの提供状態の確認」について**

  基本対策事項 4.2.2(1)-5 c)において定めている運用規程に基づき、責任共有モデルで、クラウドサービス提供者側の責任として含まれる以下を例とする項目や契約時に同意した項目について、定期的にクラウドサービス提供者に確認することが求められる。

  - 情報の保存方法、保存場所、伝送経路
  - 情報の廃棄
  - ログ情報の収集と保存状況
  - 時刻同期の状況
  - バックアップの実施
  - 不正アクセスの監視

- **基本対策事項 4.2.2(4)-1 b)「IT 資産の適切な管理」について**

  基本対策事項 4.2.2(1)-7 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用におけるサービス内容の設定等の変更を、適切に管理し把握する必要がある。また、クラウドサービスによっては利用状況により提供する CPU やバックアップストレージ等のリソースを自動的に拡張するなどの機能を有しているため、オンプレミスで利用していたソフトウェアを導入する際にはライセンス等の管理も必要となる。一方で、クラウドサービスにおける膨大な IT 資産の適切な管理については、手動で管理することは困難である。よって、IT 資産管理ソフトウェアの利用が推奨されるが、クラウドサービスの形態によっては、クラウドサービスの利用料を従量課金としており、その対象となるリソースの管理ツールが用意されていることがあるため、その管理ツールを利用し適切に管理することが求められる。

- **基本対策事項 4.2.2(4)-2 a)「アクセス管理と操作の確実な記録」について**

  基本対策事項 4.2.2(1)-8 a)において定めた運用規程に基づき、クラウドサービス管理者は、クラウドサービスに対する管理者権限を持つ者の操作等について、全て記録され保存されることを確認することが求められる。また、人事異動等により管理者権限を必要とする者が交代する場合などは権限設定の変更が遅れることのないように注意が必要である。

- **基本対策事項 4.2.2(4)-2 b)「割り当てたアクセス権限に対する定期的な確認による見直し」について**

  基本対策事項 4.2.2(1)-8 b)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者に割り当てたクラウドサービスへのアクセス権限について、定期的に確認し、必要に応じて見直す必要がある。見直す対象としては、クラウドサービス利用の目的及び必要性、対象者の妥当性、利用期間、権限の範囲等が挙げられる。また、利用するクラウドサービスによっては、利用者アカウントへの権限だ

けではなくサービスごとにアクセス権限を割り当てられる特殊なアカウントが存在するため、そのような特殊なアカウントについてもアクセス権限を定期的に確認し、必要に応じて見直す必要がある。

- **基本対策事項 4.2.2(4)-3 a)「クラウドサービスの機能に対する脆弱性対策の実施」について**

  基本対策事項 4.2.2(1)-7 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスの機能に対する脆弱性対策を実施する必要がある。例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドサービスに対するリスクであり、対策を講ずる必要がある。7.2.1「ソフトウェアに関する脆弱性対策」の内容を踏まえた対策の実施や責任分界点がクラウドサービス提供者側の実施する範囲にある場合はクラウドサービス提供者に対策の実施を求め、結果の報告を要求する必要がある。

- **基本対策事項 4.2.2(4)-4 a)「ユーティリティプログラムを使用する場合」について**

  基本対策事項 4.2.2(1)-8 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスのリソース（ネットワーク、仮想マシン等）の設定を変更するユーティリティプログラムを使用する場合は、その機能の利用者を制限し、ユーティリティプログラムの使用に関する注意事項を共有することが求められる。

- **基本対策事項 4.2.2(4)-4 b)「設定の誤りを防止するための対策」について**

  基本対策事項 4.2.2(1)-11 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスの設定を変更する場合の設定誤りはサービス自体の停止などの広範囲な障害につながる可能性があり、それを避けるため、以下を例とする設定の誤りを防止するための対策を行うことが求められる。

  - 定期的な設定の確認
  - クラウドサービス提供者等が提供するセキュリティ設定・監視ツールの利用
  - 設定権限を与えるクラウドサービス利用者の限定
  - 責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化
  - 開発プロセスへのセキュリティ対策の組み込み
  - クラウドサービスの機能追加に係る設定の確認による見直し

  なお、クラウドサービスにおける設定の誤りを防止するためのツールとして、CSPM と呼ばれる製品が存在する。CSPM については「（解説）基本対策事項 4.2.2(1)-11 a)「設定の誤りを防止するための対策」について」を参照のこと。

- **基本対策事項 4.2.2(4)-4 c)「重要操作に対する監督者の指導の下での実施」について**

  基本対策事項 4.2.2(1)-11 b)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者の操作により利用中のクラウドサービスに重大な障害をもたらすことが予想される操作については、クラウドサービス管理者が指名した監督者の監視の下、実施させることが求められる。

- **基本対策事項 4.2.2(4)-5 a)「不正利用の監視」について**

  基本対策事項 4.2.2(1)-8 d)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスへの不正利用を検知することが可能な監視機能をクラウドサービス提供者に要求し、監視を行うことが求められる。クラウドサービスの利用者の識別コードを含むクラウドサービス内に保持されるクラウドサービス利用者の情報に対して、クラウドサービス提供者がアクセスするものについてはあらかじめ両者で確認し、サービス利用開始後に当該情報へのアクセス履歴をクラウドサービス利用者が常に監視・確認できることが求められる。

- **基本対策事項 4.2.2(4)-5 b)「データ容量、性能等の監視」について**

  基本対策事項 4.2.2(1)-12 d)において定めている運用規程に基づき、クラウドサービス管理者は、利用するクラウドサービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用可能であることを確認する必要がある。また、想定を超える利用が予想される場合は、対策を検討することが求められる。

- **基本対策事項 4.2.2(4)-6 a)「バックアップの確実な実施」について**

  基本対策事項 4.2.2(1)-12 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス提供者が提供するバックアップ機能を利用する場合、クラウドサービス提供者にその仕様を要求し要求事項を満たすことを確認する必要がある。また、取得したバックアップが有効であることを定期的に確認することも求められる。

- **基本対策事項 4.2.2(4)-6 b)「十分な可用性の担保、復旧に係る定期的な訓練の実施」について**

  基本対策事項 4.2.2(1)-12 b)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用して要安定情報を取り扱う場合及び非常時優先業務等を支える情報システムをクラウドサービス上で運用する場合、十分な可用性を担保するために当該情報システムに係る情報のバックアップからの復旧手順に対して、定期的に訓練を実施することが求められる。また、遠隔地クラスタなどの冗長構成を採用した場合もフェールオーバー及びフェールバックの検証を定期的に行う必要がある。

- **基本対策事項 4.2.2(4)-6 c)「仕様内容の変更通知に関する内容確認と復旧手順の確認」について**

  基本対策事項 4.2.2(1)-12 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス提供者によるサービス内容の変更が行われる際の事前通知を受けた場合、その影響範囲・影響度を確認し、必要に応じて対処するとともに、サービス停止等が発生した場合の復旧手順を確認することが求められる。

- **基本対策事項 4.2.2(4)-7 a)「暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理」について**

  基本対策事項 4.2.2(1)-9 c)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の生成から廃棄に至るまでのライフサイクルにお

ける適切な管理を実施する必要がある。特に情報の抹消において暗号化消去を用いる場合、情報の暗号化に用いる鍵の管理は重要であり、暗号鍵の複製や暗号鍵の利用等に関して適切に管理することが求められる。暗号鍵の管理については、基本対策事項7.1.5(1)-3 b)「管理手順を定めること」を参照するとよい。

遵守事項

(5) クラウドサービスを利用した情報システムの更改・廃棄時の対策

(a) クラウドサービス管理者は、(1)(c)で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずること。また、クラウドサービスの利用終了時に実施状況を確認・記録すること。

【 基本対策事項 】

＜4.2.2(5)(a)関連＞

4.2.2(5)-1 クラウドサービス管理者は、以下を全て含むクラウドサービスの利用終了に関する情報セキュリティ対策を実施すること。

a) クラウドサービスで取り扱った情報の廃棄

b) 暗号化消去が行えない場合の基盤となる物理機器の廃棄

c) 作成されたクラウドサービス利用者アカウントの削除

d) 利用したクラウドサービスにおける管理者アカウントの削除又は返却

e) クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

（解説）

- **遵守事項 4.2.2(5)(a)「実施状況を確認・記録する」について**

遵守事項 4.2.2(1)(c)において定めている運用規程の各項目については、利用するクラウドサービスの形態（IaaS、PaaS、SaaS 等）及び仕様によっては適用できないものも存在する可能性もある。よって、クラウドサービス管理者は、利用するクラウドサービスごとに各規定の実施について記録し、対象外（適用不可）と判断した項目についてはその理由を付記することが求められる。

- **基本対策事項 4.2.2(5)-1 a)「情報の廃棄」について**

基本対策事項 4.2.2(1)-14 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスの利用終了時に、取り扱った全ての情報が、クラウドサービス基盤上から確実に抹消されていることを確認する必要がある。その抹消されていることの確認方法としては、暗号化消去を目的とした情報の暗号化に用いた鍵については、バックアップを含めて抹消することやクラウドサービス提供者に、契約時に同意した情報の廃棄手順の実施報告書を要求し確認することなどが考えられる。また、対象はバックアップ等により複製された物にも及ぶ点に注意が必要である。クラウドサービス管理者は、資産管理ツール等に記録された情報等を使用し、サービス終了時から時期を逸せずに廃棄を漏れなく完了しなければならない。暗号化された情報の廃棄は、復号に用いる鍵に対してそのバックアップを含め確実な廃棄が求められる。以下はクラウドサービス利用終了時に廃棄すべき情報の例である。

  - 仮想リソース（仮想マシン、仮想ストレージ、仮想ネットワーク機器等）
  - ファイル（ストレージサービスに格納したファイル、各サービスのログ、開発関

連ファイル、設定ファイルなど）
- 暗号化された情報の復号に用いる鍵
- ドメイン情報

- **基本対策事項 4.2.2(5)-1 b)「基盤となる物理機器の廃棄」について**

基本対策事項 4.2.2(1)-14 b)において定めている運用規程に基づき、クラウドサービス管理者は、暗号化消去が行えないクラウドサービスを利用した場合、クラウドサービス提供者が、クラウドサービスの基盤となる装置等のセキュリティを保った処分又は再利用のための方針及び手順の確実な実施を確認する必要がある。

- **基本対策事項 4.2.2(5)-1 c)「クラウドサービス利用者アカウントの削除」について**

基本対策事項 4.2.2(1)-15 a)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用終了する際は、利用時に作成されたクラウドサービス利用者アカウントを全て削除する必要がある。

- **基本対策事項 4.2.2(5)-1 d)「クラウドサービスにおける管理者アカウントの削除又は返却」について**

基本対策事項 4.2.2(1)-15 b)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービスを利用終了する際は、作成したクラウドサービス利用者アカウントが全て削除されていることを確認した上でクラウドサービスにおける管理者アカウントを削除し、又はクラウドサービス提供者に返却する必要がある。また、クラウドサービスにおける管理者アカウントについては再利用されないことをクラウドサービス提供者に確認することが重要である。

- **基本対策事項 4.2.2(5)-1 e)「特殊なアカウントの削除と関連情報の廃棄」について**

基本対策事項 4.2.2(1)-15 c)において定めている運用規程に基づき、クラウドサービス管理者は、クラウドサービス利用者のアカウント以外の特殊なアカウント（ストレージアカウント等）を作成した場合は、サービス利用終了時に確実に削除する必要がある。また、当該アカウントを利用して作成された情報についても廃棄されていることを確認する必要がある。

4.2.3 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

目的・趣旨

要機密情報を取り扱わない場合であって、クラウドサービス提供者における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を機関等から送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、要機密情報を取り扱う場合と同等のセキュリティ対策を求めることはクラウドサービスの利用推進を妨げるものであるため、要機密情報を取り扱わない前提でクラウドサービスを利用する場合は、本款で定めた遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) 要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱わない場合）の利用に関する運用規程を整備すること。

(ア) クラウドサービスを利用可能な業務の範囲

(イ) クラウドサービスの利用申請の許可権限者と利用手続

(ウ) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(エ) クラウドサービスの利用の運用規程

【 基本対策事項 】

＜4.2.3(1)(a)(イ)関連＞

4.2.3(1)-1 統括情報セキュリティ責任者は、機関等において要機密情報を取り扱わない前提でクラウドサービスを業務に利用する場合は、以下を例に利用手続を定めること。

a) 利用申請の許可権限者

b) 利用申請時の申請内容

- クラウドサービスの名称（必要に応じて機能名までを含む。）
- クラウドサービス提供者の名称
- 利用目的（業務内容）
- 取り扱う情報の格付
- 利用期間
- 利用申請者（所属・氏名）
- 利用者の範囲（機関等内に限る、部局内に限る など）
- 利用に当たってのリスクが許容できることの確認結果

＜4.2.3(1)(a)(ウ)関連＞

4.2.3(1)-2 利用申請の許可権限者は、機関等における要機密情報を取り扱わない場合のクラウドサービスの利用状況について、以下を例に管理すること。

a) 利用申請の許可権限者は、申請ごとにクラウドサービス管理者を指名すること。

b) 利用承認したクラウドサービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新のクラウドサービスの利用状況を把握できるようにするこ

と。また、記録する際は、以下を例とする項目を記録し機関等内で共有すること。

- クラウドサービスの名称（必要に応じて機能名までを含む。）
- クラウドサービス提供者の名称
- 利用目的（業務内容）
- 取り扱う情報の格付
- 利用期間
- 利用申請者（所属・氏名）
- 利用者の範囲（機関等内に限る、部局内に限る など）
- クラウドサービス管理者（所属・氏名）

＜4.2.3(1)(a)(エ)関連＞

4.2.3(1)-3 統括情報セキュリティ責任者は、機関等において要機密情報を取り扱わない前提でクラウドサービスを業務に利用する場合は、以下を全て含む運用規程を整備すること。

a) サービス利用中の安全管理に係る運用規程

- 適切な主体認証、アクセス制御の管理の実施
- サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
- 情報の滅失、破壊等に備えたバックアップの取得
- 要機密情報の取扱禁止の徹底（利用者への定期的な注意喚起を含む。）

b) 情報セキュリティインシデント発生時の連絡体制

（解説）

- **遵守事項 4.2.3(1)(a)(ア)「利用可能な業務の範囲」について**

情報セキュリティの確保の観点から、要機密情報を取り扱わない場合においてクラウドサービスを利用可能な業務の範囲を定めることを求めている。

クラウドサービスの利用において、要機密情報を取り扱わない場合であっても考慮すべきリスクの例には、以下のようなものがある。統括情報セキュリティ責任者は、以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

- クラウドサービス提供者は、保存された情報を自由に利用することが可能である。また、定型約款、利用規約等でその旨を条件として明示していない場合がある。加えて、クラウドサービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
- 政府が利用等することで結果的に国民一般に、安全・安心なサービスであるとして推奨していると受け取られることがある。
- クラウドサービス提供者が国外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。
- 情報が改ざんされた場合でも、利用形態によってはクラウドサービス提供者が

一切の責任を負わない場合がある。

- 突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。定型約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。
- 保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
- 情報セキュリティインシデントが発生した際に、機関等に対し必要十分な報告がなされないことがある。
- 定型約款及び利用規約の内容が、クラウドサービス提供者側の都合で利用開始後においても定型約款の変更をすることにより、変更後の定型約款の条項について合意があったものとみなし、個別に相手方と合意をすることなく契約の内容を変更することができる場合がある。
- 情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
- 利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

- **遵守事項 4.2.3(1)(a)(イ)「利用申請の許可権限者」について**

クラウドサービスの利用申請の許可権限者は、原則として統括情報セキュリティ責任者が行うことを想定しているが、組織の規模や特性に応じて柔軟に定めてよい。ただし、利用を承認したクラウドサービスの記録は機関等内で共有できるようにすることが求められる。

- **遵守事項 4.2.3(1)(a)(イ)「利用手続」について**

クラウドサービスの利用には利用申請を行う必要があるが、要機密情報を取り扱わないクラウドサービスの利用においても全て利用申請を行うことは、業務に支障を来す可能性がある。よって、職員等が業務に頻繁に利用することが想定されるクラウドサービスに対しては、統括情報セキュリティ責任者が要機密情報を取り扱わないことを前提に以下を例とする当該クラウドサービスの内容を確認し、機関内に承認済みであることを事前に通知する運用も可能である。なお、承認済みとする運用においても、当該クラウドサービスにおけるクラウドサービス管理者を指名する必要がある。

- サービスの定型約款や利用規約の内容
- クラウドサービス提供者の情報セキュリティポリシー及びプライバシーポリシー
- 提供サービスにおけるセキュリティ設定及びプライバシー設定の方法（初期設定を含む。）
- 情報セキュリティインシデント発生時における個別対応の可否（運用実績等を勘案するとよい。）

- **遵守事項 4.2.3(1)(a)(ウ)「クラウドサービス管理者」について**

  利用申請の許可権限者は、承認する際に当該申請に対する「クラウドサービス管理者」を指名することが求められるが、要機密情報を取り扱わない場合のクラウドサービスの利用においては課室情報セキュリティ責任者又は利用申請者自身を想定している。なお、承認済みとして事前に機関内に通知するクラウドサービスにおいては、組織横断的な管理が必要とされる可能性があることから情報システムセキュリティ責任者を想定している。

遵守事項

(2) 要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施

(a) 職員等は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で利用申請の許可権限者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請すること。

(b) 利用申請の許可権限者は、職員等による利用するクラウドサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることの確認結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定すること。

(c) 利用申請の許可権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録すること。

(d) クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずること。

【 基本対策事項 】

＜4.2.3(2)(d)関連＞

4.2.3(2)-1 クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスの利用において以下を全て含む、適切な措置を講ずること。

a) 要機密情報を取り扱わないクラウドサービスの利用に係る安全管理

b) 要機密情報を取り扱わないクラウドサービスで情報セキュリティインシデントが発生した際の連絡体制の整備

（解説）

- **遵守事項 4.2.3(2)(a)「利用に当たってのリスク」について**

個々の業務の遂行において、要機密情報を取り扱わない前提でクラウドサービスの利用を検討する際は、当該サービスの定型約款、利用規約、その他の利用条件を確認し、リスクや課題への対策を明確にした上で、適切に利用の必要性を判断する必要がある。

なお、考慮すべきリスクの例については、「（解説）遵守事項 4.2.3(1)(a)(ア)「利用可能な業務の範囲」について」を参照のこと。

さらに、要機密情報を取り扱わない場合においてクラウドサービスを利用等する際には、次の対応が求められる。

- 調達行為を伴わない場合には、「調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）に基づき、必要な場合において、内閣官房国家サイバー統括室に対し、講ずべき必要な措置について、助言を求める。
- 調達行為を伴う場合には、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）

に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずる。

参考：内閣官房国家サイバー統括室「調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ」（関係省庁申合せ）
（https://www.cyber.go.jp/pdf/policy/kihon-2/ES_moushiawase.pdf）

参考：内閣官房国家サイバー統括室「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ）
（https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf）

- **遵守事項 4.2.3(2)(c)「クラウドサービス管理者を指名」について**

  要機密情報を取り扱わないクラウドサービスの利用は利用申請ごとに条件の異なることが想定されるため、業務内容や利用者の所属する組織の違いに応じて「クラウドサービス管理者」をそれぞれ立てることで管理が容易になる場合が考えられる。

- **遵守事項 4.2.3(2)(c)「クラウドサービスを記録」について**

  利用申請の許可権限者は、承認したクラウドサービスを把握するため記録する必要がある。なお、利用申請の結果を踏まえて、機関内で事前に承認済とするかを判断し、承認済みクラウドサービスとする場合、承認済みとした上でクラウドサービスを記録すること。

- **基本対策事項 4.2.3(2)-1 a)「利用に係る安全管理」について**

  基本対策事項 4.2.3(1)-3 a)において定めている運用規程に基づき、要機密情報を取り扱わない場合のクラウドサービスであっても、適切な安全管理を実施する必要がある。

  例えば、利用するクラウドサービスを管理する機能に対して適切に主体認証、アクセス制御の管理を行う必要がある。クラウドサービス利用者が当該クラウドサービスに保存した情報の公開設定をすることができる機能を有するクラウドサービスであった場合は、公開設定が正しく運用できているかの定期的な確認を実施することやバックアップの機能を有するクラウドサービスであるなら適切なバックアップの取得をするなどを実施する必要がある。また、当該クラウドサービスの利用者に対して定期的な注意喚起を実施することも考えられる。

- **基本対策事項 4.2.3(2)-1 b)「情報セキュリティインシデントが発生した際の連絡体制の整備」について**

  基本対策事項 4.2.3(1)-3 b)において定めている情報セキュリティインシデントが発生した際の連絡体制の他に、利用するクラウドサービスにおけるクラウドサービス提供者や当該クラウドサービスの運用を業務委託している場合等の委託先の連絡先等を含める必要がある。

  なお、統括情報セキュリティ責任者が整備する運用規程が、クラウドサービスの事情に応じた内容で整備されているならば、クラウドサービス別に整備しなくても構わない。

4.3　機器等の調達

4.3.1　機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を運用規程として整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更が加えられない**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

4.3.1(1)-1 統括情報セキュリティ責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を全て含めること。

a) 調達した機器等に不正な変更が見付かったときに、必要に応じて追跡調査や立入検査等、機関等と調達先が連携して**原因を調査・排除できる体制**を整備していること。

b) 「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」(関係省庁申合せ　内閣官房国家サイバー統括室) に基づき、**サプライチェーン・リスクに対応する必要があると判断されるもの**については、必要な措置を講ずること。

4.3.1(1)-2 統括情報セキュリティ責任者は、機器等の選定基準に、機器等に**必要なセキュリティ機能が適切に実装されていること**を含めること。また、IoT 機器等については、対象機器の「**セキュリティ要件適合評価及びラベリング制度（JC-STAR)**」の登録状況と以下の観点を踏まえて、当該制度を選定基準に含めること。

a) 「重要度：低」に分類された情報システムの IoT 機器等については、★１（レベル１）ラベルを取得した製品群からの選定等、**当該制度の★１ラベル取得に求められるセキュリティ適合基準**の機能が実装された機器等とすること。

b) 「重要度：中～高」に分類された情報システムの IoT 機器等については、★１ラベル以上を取得した製品群から選定するなどして、**当該制度の★１ラベル取得に求められるセキュリティ適合基準**に加えて、情報システムの重要度に即したより高度なセキュリティ機能が実装された機器等とすること。

4.3.1(1)-3 統括情報セキュリティ責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、**ISO/IEC 15408 に基づく認証**を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。

4.3.1(1)-4 統括情報セキュリティ責任者は、**ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認**を必要とする場合には、**SBOM（Software Bill of Materials：ソフトウェア部品表）**の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めること。

＜4.3.1(1)(b)関連＞

4.3.1(1)-5 統括情報セキュリティ責任者は、機器等の納入時の確認・検査手続には**以下を全て含む事項を確認できる手続**を定めること。

a) 調達時に指定したセキュリティ要件の実装状況

b) 機器等に不正プログラムが混入していないこと。

（解説）

- **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映する必要がある。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 4.3.1(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、当該事項の適用要否を判断した上で整備することを求めている。

- **遵守事項 4.3.1(1)(a)「不正な変更」について**

ここでいう「不正な変更」とは、機器等の製造工程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことを意味している。

不正な変更が行われない管理がなされていることとは、例えば、機器等の製造工程に

おける不正行為の有無について、定期的な監査を行っていること、機器等の製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われていること等が考えられる。その他、特に高い信頼性が求められる製品を調達する場合は、各製造工程の履歴が記録されているなどの厳格な管理されていることが考えられる。

- **遵守事項 4.3.1(1)(a)「不正な変更が加えられない」について**

機関等は、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクの懸念が払拭できない機器等を調達しないようにする必要があり、機器等の調達において、考慮すべきリスクとして以下のようなものがある。統括情報セキュリティ責任者は、以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、調達の可否を決定する必要がある。

- 機器等を開発・供給する事業者やそのサプライヤー・委託先事業者（再委託先事業者等を含む。）、及び当該機器等の設置や保守等の役務を提供する事業者やその委託先事業者（再委託先事業者等を含む。）について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む。）の立地する場所の法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスク

このサプライチェーン・リスクに対応する方法として、機関等が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。

このような対応をする手段の一つとして、政府調達において、相対の交渉が可能な契約であれば、調達に係る契約の相手方に対して、サプライチェーン・リスクに係る十分な知見をもとに、機器等に関し必要な要件を備えるべく、交渉を通じて個別に求めることが考えられる。

なお、上記の場合においても、関係する国内法令（会計法、予算決算及び会計令、国の物品等又は特定役務の調達手続の特例を定める政令・省令等）及び関係する国際協定（政府調達に関する協定を改正する議定書等）を遵守する必要がある。

こうした考え方を踏まえ、機関等においては、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）に基づき、必要な措置を講ずることが求められる。

- **基本対策事項 4.3.1(1)-1 a)「原因を調査・排除できる体制」について**

OEM（Original Equipment Manufacturer）によって提供される機器等についても、OEM 製品の製造者においても不正な変更が加えられないよう、OEM 製品の販売者が機器等のサプライチェーン全体について適切に管理していることも含めて、要件を定めることが考えられる。また、SBOM を参考とすることも考えられる。

- **基本対策事項 4.3.1(1)-1 b)「サプライチェーン・リスクに対応する必要があると判断されるもの」について**

機器等の調達においては、上述の遵守事項 4.3.1(1)(a)「不正な変更が加えられない」についての解説に記載のサプライチェーン・リスクを十分に考慮した上で、リスクへの対応について適切に検討・判断し、必要な措置を講ずる必要がある。なお、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ内閣官房国家サイバー統括室）の別紙２において「ソフトウェア」が例示されているところであるが、情報システムの基盤を管理又は制御するソフトウェアにおいても、不正な変更が加えられる等の脅威を低減させるために同様の措置を講ずる必要がある。情報システムの基盤を管理又は制御するソフトウェアについては、以下の例が考えられる。

- 端末やサーバ装置、通信回線装置等を制御するソフトウェア
- 統合的な主体認証を管理するソフトウェア
- ネットワークを制御・管理するソフトウェア
- 資産を管理するソフトウェア
- 監視に関連するソフトウェア
- 情報システムのセキュリティ機能として使用するソフトウェア

参考：内閣官房国家サイバー統括室「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ）
（https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf）

- **基本対策事項 4.3.1(1)-2「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について**

本制度は、2024 年８月に経済産業省が公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」に基づき構築されたものであり、インターネットとの通信が行える幅広い IoT 製品を対象として、製品に具備されているセキュリティ機能を共通的な物差しで評価・可視化することを目的としている。

本制度の適合基準ラベル（★１～★４）を確認することで、製品のセキュリティ水準を容易に把握できるとともに、各機関等における個々のセキュリティ対策の実装確認を簡略化できることから、本制度の積極的な利用が推奨される。

2025 年３月から、機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言した適合基準レベル★１ラベル（レベル１）の運用が開始されている。情報システムの重要度（「表 5.1.1-1：情報システムの分類基準（例）」に示した分類基準）の「重要度：低」にあたる情報システムにおいては、調達対象の機器等が★１ラベル取得製品群に存在する場合は、当該製品群から選定することが望ましい。今後、製品種別ごとにより高度なセキュリティ適合基準に対する評価を行う★２ラベル（自己適合宣言）、★３ラベル（第三者認証）以上が順次運用されることとなっている。★３ラベルについては、2026 年２月に通信機器及びネットワークカメラを対象としたセキュリティ要件が公開され、運用開始に向けて準備中で

ある。運用が開始された際には、製品の登録状況等を確認の上、「重要度：中～高」は少なくとも★３以上を IoT 機器等の選定基準とすることを検討している。従って、★１ラベル取得製品の全てが「重要度：中～高」の情報システムが求める情報セキュリティ水準を充足しているわけではないことに留意が必要である。

なお、各種ラベル取得製品が十分に普及した時期を目処に、セキュリティ水準に応じたラベル取得製品の調達を必須化する方針である。

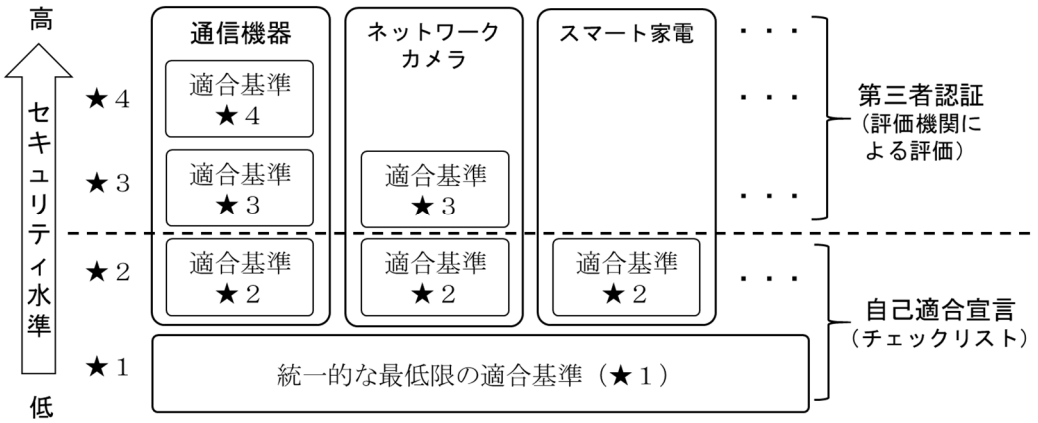


図 4.3.1-1　製品カテゴリーごとの適合基準（イメージ）

参考：情報処理推進機構（IPA）「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」
（https://www.ipa.go.jp/security/jc-star/index.html）

- **基本対策事項 4.3.1(1)-2 a)及び b)「当該制度の★１ラベル取得に求められるセキュリティ適合基準」について**

★１ラベル取得に求められるセキュリティ適合基準とは、最低限 JC-STAR の★１（レベル１）適合基準を原則、全て満たすことを意味している。

従って、対象製品カテゴリーにおける機器の登録状況から、★１以上ラベル取得製品以外の機器等を選定する場合には、★１（レベル１）適合基準を参照し、機器等に実装された機能について、基準への適合状況を確認すること等が求められる。

参考：情報処理推進機構（IPA）「JC-STAR ★１（レベル１）適合基準・評価手順（評価手法・評価ガイド）」
（https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html）

- **基本対策事項 4.3.1(1)-3「ISO/IEC 15408 に基づく認証」について**

機器等の調達においては、ISO/IEC 15408 に基づく認証を取得している製品の優遇を選定基準の一つとすることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。

ISO/IEC 15408 に基づく認証では、第三者によって、対抗する脅威に必要な機能が設計書に反映されていること、その機能が設計どおり実装されていること、開発現場や

製造過程においてセキュリティが侵害される可能性が無いこと、利用マニュアル・ガイダンス等にセキュリティを保つための必要事項が明確に示されていること等が客観的に評価され、評価結果及び既知の情報から懸念される脆弱性についての評定及びテストが実施される。ただし、第三者によって評価・保証される範囲は、適合する Protection Profile（国際標準に基づくセキュリティ要件）や、評価保証レベル（EAL : Evaluation Assurance Level）によって異なるため、どの程度の保証を得ている認証製品であるかを、調達時に確認することが必要となる。

参考：情報処理推進機構（IPA）「IT セキュリティ評価及び認証制度（JISEC）」
（https://www.ipa.go.jp/security/jisec/index.html）

- **基本対策事項 4.3.1(1)-4「ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認」について**

ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認については、当該ソフトウェア及び機器等に関する SBOM の作成、提供等を調達先に求めることや、調達先が安全なソフトウェア開発の慣行に基づく開発を実施していることを確認することが挙げられる。対象となるソフトウェアについては、「（解説）基本対策事項 4.3.1(1)-1 b)「サプライチェーン・リスクに対応する必要があると判断されるもの」について」で例示したソフトウェアが考えられる。

なお、安全なソフトウェア開発の慣行に基づく開発については、NIST が公表している以下のフレームワークを参考にするとよい。

参考：NIST「SP800-218: Secure Software Development Framework （SSDF） Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」
（https://csrc.nist.gov/pubs/sp/800/218/final）

- **基本対策事項 4.3.1(1)-4「SBOM（Software Bill of Materials：ソフトウェア部品表）」について**

ソフトウェアに関する選定基準の一つとして、SBOM の情報を機関等が確認できることに関する基準を加えることで、ソフトウェアの透明性の確認を行うことができる。さらに、脆弱性の特定や修正など対策の効率化の観点から SBOM を活用することも考えられる。

一方で、SBOM の項目は多様であり、SBOM の対応範囲に応じてコストと効果が大きく異なるため、分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。従って、選定基準においては、SBOM の提供有無の二者択一ではなく、SBOM の対象とするソフトウェアの範囲や脆弱性管理の範囲等について、対象ソフトウェアのリスクを踏まえ、調達先への過度な要求とならない範囲で明示するとよい。例えば、利用時のリスクが低いソフトウェアについては、最小限の SBOM 対応範囲に留めることなどにより、コストを抑えることも考えられる。

SBOM や SBOM 対応範囲の考え方については、経済産業省が公表している以下の手引を参考にするとよい。

参考：経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」
（https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf）

- **基本対策事項 4.3.1(1)-5「以下を全て含む事項を確認できる手続」について**

  機器等の納入時の確認・検査手続の具体例として、以下の内容が考えられる。

  - 調達時に指定したセキュリティ要件（機器等に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェア等が最新の脆弱性に対応しているか否か等にも留意）に関する試験実施手順及び試験結果を納品時に報告させて確認
  - セキュリティ要件として調達時に指定した機能が正しく動作することを受入れテストにより確認
  - 内部監査等により不正な変更が加えられていないことを確認した結果を納品時に報告させて確認

第5部 情報システムのライフサイクル

5.1 情報システムの分類

5.1.1 情報システムの分類基準等の整備

目的・趣旨

機関等が所管する情報システムが多様化するなか、自組織で所管する情報システムの情報セキュリティインシデントの発生リスクを低減させるためには、多様な情報セキュリティ対策からその情報システムに求められる対策を過不足無く適切に選択する必要がある。

そのためには、情報セキュリティを取り巻く様々な脅威動向や情報システムにインシデントが発生した際の業務影響度、社会的影響、取り扱う情報、機関等の組織特性等を踏まえて、高度な情報セキュリティ対策が求められる情報システムを判別するための分類基準を定め、分類基準に応じた情報セキュリティ対策を規定することで、自組織が所管する情報システムの分類に応じた適切な対策が講じられるようにすることが重要である。

遵守事項

(1) 情報システムにおける分類のための運用規程の整備

(a) 統括情報セキュリティ責任者は、情報システムの情報セキュリティインシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である**情報システムの分類基準を運用規程として整備する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.1.1(1)(a)「情報システムの分類基準を運用規程として整備する」について**

機関等が所管する情報システムは、取り扱う情報や情報システムを利用して行う業務の内容等により、情報システムを構成する要素や利用方法等が異なる。そのため、個別の情報システムの特性に基づく脅威を踏まえた上で、適切な情報セキュリティの要件を定め対策を講ずることが望ましい。一方で情報システムの規模の大きさ等にかかわらず全ての情報システムに対して、個々の事情に合わせた考え得る全ての脅威に対してリスク評価を行った上で、過不足無く情報セキュリティ対策を講ずることは困難である。そこで、簡易的な判断基準として、情報セキュリティインシデント等が発生した際に業務遂行に影響を及ぼすなど、社会的・経済的な混乱を招くおそれがある高度な情報セキュリティ対策が要求される情報システムを判別するための基準を設けることとする。当該基準は、情報システムにおける情報セキュリティインシデント発生時の業

務影響度、社会的影響、取り扱う情報、自組織の組織特性等を踏まえ分類するための基準であり、分類した基準を用いて高度な情報セキュリティ対策が要求される情報システムに対して、通常のセキュリティ対策だけではなく、追加で高度なセキュリティ対策を講ずることができるようにするためのものである。

具体的に情報システムの分類基準として整備する内容は、表 5.1.1-1 に例示したような情報システムを分類するためのラベルとなる項目と、その項目を判断するための基準となる考え方を示したものが必要となる。また、情報システムセキュリティ責任者が情報システムの分類をする際に判断しやすいよう、ラベルとなる項目ごとに該当すると想定される情報システムを記載することが望ましい。

この分類基準を用いて情報システムセキュリティ責任者が分類を行い（遵守事項 5.2.1(2)(a)）、統括情報セキュリティ責任者がその結果を確認し必要に応じて修正等の指示を行う（遵守事項 5.1.1(3)(a)）ことで、機関等が保有する情報システムを横断的に把握・分類し、個々の情報システムの特性に応じた必要な対策が過不足なく講じられることや、機関等においてより高度な情報セキュリティ対策が必要な情報システムを特定することが重要である。

なお、情報システムの分類基準について参考となる例を表 5.1.1-1 のとおり示す。機関等においては、自組織の役割や組織の特性等を踏まえ本ガイドラインと異なる考え方の情報システムの分類基準を定めることも可能である。機関等における情報システムの分類基準を規定する際は、本ガイドラインに加え、以下を参考にするとよい。

ただし、本ガイドラインと異なる分類基準を採用する場合、本ガイドラインが想定する高度なセキュリティ対策を必要とする情報システムと考え方が異なる可能性があるため、本ガイドライン第 6 部及び第 7 部における基本対策事項を、自組織で定めた情報システムの分類基準に即した、基本セキュリティ対策と追加セキュリティ対策を規定する必要があることに留意する。

参考：デジタル庁「政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～」
（https://www.digital.go.jp/resources/standard_guidelines/）

参考：「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」、「ISMAP-LIU 業務・情報の影響度評価ガイダンス」等
（https://www.ismap.go.jp）

参考：情報処理推進機構（IPA）「非機能要求グレード」
（https://www.ipa.go.jp/archive/digital/iot-en-ci/jyouryuu/hikinou/ent03-b.html）

参考：NIST「SP800-53 rev.5：組織と情報システムのためのセキュリティおよびプライバシー管理策」
（https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000bbdx.pdf）

参考：NIST「SP800-53B：組織と情報システムのための管理策ベースライン」

（https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000bbez.pdf）

表 5.1.1-1　情報システムの分類基準（例）

情報システムの重要度	判断基準	（参考）想定する情報システム
高	・国家安全保障及び治安関係の業務を行う場合 ・機密性の高い情報を取り扱う場合並びに情報の漏えい及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱う場合 ・番号制度関係の業務を行う場合等、個人情報を極めて大量に取り扱う業務を行う場合 ・機能停止等の場合、機関等の業務遂行に著しい影響を及ぼす場合 ・運営経費が極めて大きい場合 ・情報セキュリティインシデント発生時に「情報システムの重要度：高」に分類される他の情報システムに影響を与える場合	・防災、経済、重要インフラに関係する情報システム ・基幹業務システム、LAN や職員が日常的に利用する PC やメール機能を管理する情報システム等の組織の業務の根幹を支える情報システム ・情報システムの基盤として利用する機関等が所管する情報システム（クラウドサービスを利用した共通基盤を含む。） ・対国民向けの情報システムで社会的影響が大きい情報システム ・機密性 3 情報や特定個人情報を取り扱う情報システム ・極めて大量の要保護情報を取り扱う情報システム
中	・「情報システムの重要度：高」を除く要保護情報を取り扱う場合 ・情報セキュリティインシデント発生時に「情報システムの重要度：中」に分類される他の情報システムに影響を与える場合	・要保護情報を取り扱う情報システム（情報セキュリティインシデント発生時に他の情報システムへ影響を与える情報システムを含み、「情報システムの重要度：高」に想定される情報システムを除く。）
低	・「情報システムの重要度：高、中」を除く全て	・要保護情報の取扱いがない情報システム

例示のうち「情報システムの重要度：高」の判断基準については、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」の別紙３「重要性の観点」を基に作成。

遵守事項

(2) 情報システムの分類基準に基づいた情報セキュリティ対策に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、情報システムに求める**分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項**を運用規程として整備すること。

【 基本対策事項 】

＜5.1.1(2)(a)関連＞

5.1.1(2)-1 統括情報セキュリティ責任者は、自組織の特性や国内外の情報セキュリティに関連する動向等を踏まえ、セキュリティベースラインとして全ての情報システムに対し対策を求める「**基本セキュリティ対策**」と、それに加え高度な情報セキュリティ対策を要求する情報システムに対し追加で対策を求める「**追加セキュリティ対策**」を定めること。

（解説）

- **遵守事項 5.1.1(2)(a)「分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項」について**

統括情報セキュリティ責任者は、情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を、情報システムに求める分類基準に応じて「基本セキュリティ対策」と「追加セキュリティ対策」として整備する必要がある。「基本セキュリティ対策」は、情報システムの重要度に関わらず、全ての情報システムにおいて必須の対策を求める具体的な対策事項のことであり、「追加セキュリティ対策」とは、高度な情報セキュリティ対策を要求する情報システムに対して「基本セキュリティ対策」に加えて追加で対策を求める具体的な対策事項のことである。この「基本セキュリティ対策」と「追加セキュリティ対策」については、情報システムの分類基準で整備した分類に応じて、実施するための判断基準を定めておく必要がある。なお、本ガイドラインの表 5.1.1-1 を分類基準として採用する場合の判断基準を「表 5.1.1-2：具体的な対策事項を実施させるための判断基準（例）」に示す。

さらに「基本セキュリティ対策」と「追加セキュリティ対策」で求めている具体的な対策事項については、本ガイドラインの第 6 部及び第 7 部が情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策を定めているので、それらの基本対策事項を参考に定め、運用規程として整備する必要がある。

ただし、本ガイドラインと異なる情報システムの分類基準を採用した場合、自組織で定めた分類基準と本ガイドラインで高度なセキュリティ対策が必要となる情報システムの分類結果が異なることが考えられる。その場合、本ガイドライン第 6 部及び第 7 部における基本対策事項を自組織で定めた分類基準に対応した具体的な対策事項になるように、適切に定めること。

なお、本ガイドラインにおける「基本セキュリティ対策」と「追加セキュリティ対策」の考え方では、全ての情報システムが必須で実施すべき情報セキュリティ対策事項を「基本セキュリティ対策」とし、「表 5.1.1-1：情報システムの分類基準（例）」に示した分類基準において「情報システムの重要度：高」に該当する情報システムが基本セキュリティ対策に加えて、追加で実施すべき情報セキュリティ対策を「追加セキュリティ対策」としている。

さらに、「基本セキュリティ対策」と「追加セキュリティ対策」で求めている具体的な対策事項については、本ガイドラインの第 6 部及び第 7 部における基本対策事項において基本セキュリティ対策（【基本セキュリティ対策】）と追加セキュリティ対策（【追加セキュリティ対策】）に分けて記載をしている。特に記載のないものについては、基本セキュリティ対策として記載している。

表 5.1.1-2　具体的な対策事項を実施させるための判断基準（例）

情報システムの重要度	基本セキュリティ対策	追加セキュリティ対策
高	必須	必須
中	必須	必要に応じて実施
低	必須	必要に応じて実施

- **基本対策事項 5.1.1⑵-1「基本セキュリティ対策」について**

  基本セキュリティ対策とは、情報システムの分類基準に関わらず全ての情報システムにおいて対策を求める具体的な対策事項のこと（セキュリティベースライン）。

- **基本対策事項 5.1.1⑵-1「追加セキュリティ対策」について**

  情報システムの分類基準において、高度な情報セキュリティ対策を要求する情報システムに対し、「基本セキュリティ対策」に加え追加で対策を求める具体的な対策事項のこと。

遵守事項

(3) 情報システムの分類基準に基づいた分類の実施

(a) 統括情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ、実施した結果を報告させること。情報システムセキュリティ責任者から報告を受けた情報システムの分類結果については、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行うこと。

【 基本対策事項 】

＜5.1.1(3)(a)関連＞

5.1.1(3)-1 統括情報セキュリティ責任者は、以下の全ての場合、情報システムセキュリティ責任者に対して分類基準に基づいた情報システムの分類を行わせること。

a) 情報システムの構築又は更改が発生した場合

b) 情報システムで取り扱う情報の格付等に変更が発生した場合

c) 分類の再実施を指示する場合

5.1.1(3)-2 統括情報セキュリティ責任者は、自組織で所管する情報システムの分類結果を確認し、以下の例に該当する場合、報告を受けた情報システムの分類結果の上位への修正指示の要否を検討すること。

a) 業務特性やシステム特性、取り扱う情報等を踏まえると上位の情報システムの分類の適用が望ましいと判断される場合

b) 類似する自組織の情報システムで上位の情報システムの分類が適用されていた場合

（解説）

- **遵守事項 5.1.1(3)(a)「情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ」について**

遵守事項 5.1.1(1)(a)で定めた情報システムの分類基準に基づき、機関等で保有する情報システムを分類するものである。

- **遵守事項 5.1.1(3)(a)「上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行う」について**

情報システムセキュリティ責任者において評価した情報システムの分類結果について、機関等で保有する情報システムの評価状況を踏まえ、分類結果を補正することが望ましい場合がある。そのため、統括情報セキュリティ責任者において、適切な分類結果になるよう、必要に応じて補正を行うこと。

遵守事項

(4) 情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用規程の見直し

(a) 統括情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた情報セキュリティ対策の具体的な対策事項の**運用規程について定期的な確認による見直しをする**こと。

(b) 統括情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認すること。

【 基本対策事項 】

＜5.1.1(4)(b)関連＞

5.1.1(4)-1 統括情報セキュリティ責任者は、以下の全ての場合に分類基準に基づいた情報システムの分類が行われていることを確認すること。

a) 情報システムの構築又は更改を把握した場合

b) 対策推進計画の各種施策や情報セキュリティ監査、本部監査、自己点検等の結果を踏まえ、定期評価や評価の再実施が必要と判断した場合

（解説）

- **遵守事項 5.1.1(4)(a)「運用規程について定期的な確認による見直しをする」について**

法改正や制度改正の発生時や機関等における情報セキュリティインシデント、サイバーセキュリティ分野の脅威動向を踏まえ自組織の情報セキュリティリスクが高まった際に、情報システムの分類基準と分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項の運用規程の見直しを行うこと。

5.2 情報システムのライフサイクルの各段階における対策

5.2.1 情報システムの企画・要件定義

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を業務委託する場合については 4.1「業務委託」、クラウドサービスを利用して情報システムを構築する場合は 4.2「クラウドサービス」、情報システムで利用する機器等を調達する場合は 4.3「機器等の調達」、政府共通利用型システムを利用して情報システムを構築する場合は 5.4「政府共通利用型システム」を参照すること。

遵守事項

(1) 実施体制の確保

(a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、**最高情報セキュリティ責任者に求める**こと。

(b) 最高情報セキュリティ責任者は、前項で求められる体制の確保に際し、情報システムを統括する責任者（デジタル統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.1(1)(a)「最高情報セキュリティ責任者に求める」について**

  最高情報セキュリティ責任者に、セキュリティの維持が実施可能な体制（人員、機器、予算等）の確保を求める事項である。

政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程等に応じた体制を確保する必要がある。したがって、政府共通利用型システムを利用して情報システムを構築する場合は、5.4「政府共通利用型システム」についてを参照のこと。

遵守事項

(2) 情報システムの分類基準に基づいた分類の実施

(a) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、**情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.1(2)(a)「情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告する」について**

  遵守事項 5.1.1(1)(a)で統括情報セキュリティ責任者が定めた情報システムの分類基準に基づき、高度な情報セキュリティ対策が要求される情報システムを判別するため、情報システムの分類をすることを求めている。情報システムの分類をした結果については、統括情報セキュリティ責任者へ報告し、必要に応じて分類結果の修正を行う必要がある。

遵守事項

(3) 情報システムのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等を勘案し情報システムの分類に基づき、**情報システムに求める分類基準に応じた具体的な対策事項**を踏まえて、以下の全ての事項を含む**情報システムのセキュリティ要件**を策定すること。

(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等の**セキュリティ機能要件**

(イ) 情報システム運用時の監視等の運用管理機能要件（**監視するデータが暗号化されている場合は、必要に応じて復号**すること）

(ウ) 情報システムに関連する脆弱性及び不正プログラムについての対策要件

(エ) 情報システムの可用性に関する対策要件

(オ) 情報システムのネットワーク構成に関する要件

(b) 情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、**接続するインターネット回線を定めた上で**、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

(c) 情報システムセキュリティ責任者は、機器等を調達する場合には、「**IT 製品の調達におけるセキュリティ要件リスト**」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

(d) 情報システムセキュリティ責任者は、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ**高度な情報セキュリティ対策を要求する情報システム**については、情報システムの分類に応じて策定したセキュリティ要件について、**最高情報セキュリティアドバイザー等へ助言を求め**、業務の特性や情報システムの特性を踏まえて、**上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いか**を確認すること。

【 基本対策事項 】

＜5.2.1(3)(a)関連＞

5.2.1(3)-1 情報システムセキュリティ責任者は、「**情報システムに係る政府調達におけるセキュリティ要件策定マニュアル**」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。

5.2.1(3)-2 情報システムセキュリティ責任者は、**開発する情報システムが運用される際に想定される脅威**の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、調達仕様書等に明記すること。

＜5.2.1(3)(a)(ア)関連＞

5.2.1(3)-3 情報システムセキュリティ責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、**ST 確認**を受けること。

＜5.2.1(3)(a)(イ)関連＞

5.2.1(3)-4 情報システムセキュリティ責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確にし、情報システム運用時に情報セキュリティ確保のために必要となる**管理機能**や**監視のために必要な機能**を調達仕様書に明記すること。

＜5.2.1(3)(a)(ウ)関連＞

5.2.1(3)-5 情報システムセキュリティ責任者は、開発する情報システムに関連する**脆弱性への対策**が実施されるよう、以下を全て含む対策を調達仕様書等に明記すること。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

b) 開発時に情報システムに**脆弱性が混入されることを防ぐためのセキュリティ実装方針**

c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する機関等への情報提供

5.2.1(3)-6 情報システムセキュリティ責任者は、開発する情報システムに機関等の意図せざる不正なプログラム等が組み込まれないよう、以下を全て含む対策を実施すること。

a) 情報システムで利用する**機器等を調達する場合**は、機関等の意図せざる不正なプログラム等が組み込まれていないことを確認すること。

b) アプリケーション・コンテンツの開発時に**機関等の意図せざる不正なプログラム等が混入されることを防ぐための対策**を講ずること。

c) 情報システムの構築を委託する場合は、委託先において**機関等の意図せざる変更が加えられないための管理体制**を求めること。

＜5.2.1(3)(a)(エ)関連＞

5.2.1(3)-7 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システム**を構築する場合は、RTO（目標復旧時間）、RLO（目標復旧レベル）に応じた以下を全て含むセキュリティ要件について、情報システムを構成する要素ごとに策定し調達仕様書等に明記すること。

a) 端末、サーバ装置及び通信回線装置等の**冗長化に関する要件**

b) 端末、サーバ装置及び通信回線装置並びに取り扱われる情報に関する**バックアップの要件**

c) 情報システムを中断することのできる時間を含めた**復旧に関する要件**

＜5.2.1(3)(a)(オ)関連＞

5.2.1(3)-8 情報システムセキュリティ責任者は、開発する情報システムのネットワーク構成に関する要件について、以下を全て含む要件を調達仕様書等に明記すること。

a) **インターネットやインターネットに接点を有する情報システム（クラウドサー**

ビスを含む。）から分離する</u>ことの要否の判断とインターネットから分離するとした場合の要件

b) 端末、サーバ装置及び通信回線装置上で<u>利用するソフトウェアを実行するために必要な通信要件</u>

c) インターネット上のクラウドサービス等のサービスを利用する場合の<u>通信経路全般のネットワーク構成</u>

d) 機関等外通信回線を経由して機器等に対して<u>リモートメンテナンスすることの要否</u>の判断とリモートメンテナンスすることとした場合の要件

＜5.2.1(3)(c)関連＞

5.2.1(3)-9 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち、製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を全て含む事項を実施すること。

a) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する<u>機器等の利用環境において対抗すべき脅威</u>を分析し、必要なセキュリティ要件を策定すること。

（解説）

- **遵守事項 5.2.1(3)(a)「情報システムに求める分類基準に応じた具体的な対策事項」について**

情報システムに求める分類基準に応じた具体的な対策事項については、遵守事項 5.1.1(2)(a)を参照のこと。

- **遵守事項 5.2.1(3)(a)「情報システムのセキュリティ要件」について**

構築する情報システムにおいて、機器等を調達する場合や業務委託、クラウドサービス、政府共通利用型システムなどを利用する場合には、機関等における役割と責任範囲を踏まえ、構築する情報システムとの関係性を整理した上でセキュリティ要件を策定する必要がある。

業務委託の実施については 4.1「業務委託」、クラウドサービスを利用する場合は 4.2「クラウドサービス」、機器等を調達する場合は 4.3「機器等の調達」、政府共通利用型システムを利用する場合は 5.4「政府共通利用型システム」を参照し適切なセキュリティ要件を策定すること。

また、安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得

る情報を取り扱う情報システムのセキュリティ要件については、「安全保障等の機微な情報等に係る政府情報システムの取扱い」を参照し、策定する必要がある。

参考：デジタル庁「安全保障等の機微な情報等に係る政府情報システムの取扱い」（デジタル社会推進会議幹事会決定）
（https://www.digital.go.jp/resources/standard_guidelines）

- **遵守事項 5.2.1(3)(a)(ア)「セキュリティ機能要件」について**

  情報システムに必要となるセキュリティ機能要件の策定に当たっては、第 7 部「情報システムのセキュリティ機能」を参照し策定すること。その際、情報システムの分類に従って要件を定めるが、取り扱う情報や当該情報システムを利用して行う業務等を踏まえて、追加セキュリティ対策をセキュリティ要件として定める必要がないかを検討することが望ましい。

- **遵守事項 5.2.1(3)(a)(イ)「監視するデータが暗号化されている場合は、必要に応じて復号」について**

  ウェブの常時暗号化（TLS 化）や電子メールサーバ間通信の暗号化（TLS 化）等といった通信の暗号化が社会的に進められ、その利用割合が上昇する中で、不正なプログラム等の脅威が暗号化された通信の中に含まれていると、当該通信の監視による脅威の検知が困難になる。また、機関等自身においても上記の暗号化を進めていけば、その傾向は更に大きくなる。このため、監視に際しては、監視対象のデータが暗号されているかどうかを把握し、対象とする脅威の監視可否に与える影響を考慮した上で復号の要否を判断し、必要と判断した場合にはその対策を講じなければならない。

- **遵守事項 5.2.1(3)(b)「接続するインターネット回線を定めた上で」について**

  構築する情報システムごとに、個々にインターネット回線を構築すると、当該インターネット回線の監視等に係る体制や運用コストが分散し、効率的かつ集中的なセキュリティ監視が行われず、セキュリティ水準が低下するおそれがある。このような観点から、機関等として（又は国の行政機関にあってはこれら機関全体で）インターネット接続口を統合・集約し、集中的なセキュリティ監視を行うなどの取組を行っている場合は、当該取組の範疇とするか否か検討した上で、構築する情報システムに接続するインターネット回線を調達仕様書等において明確にすることを求めている。

  なお、既設のインターネット回線を利用せずに、独立したインターネット回線を調達してセキュリティ監視等の運用を個別に行う場合も想定される。情報システムが取り扱う情報の格付や取扱制限等の特性に従って、既設のインターネット回線の利用可否を判断することが望ましい。

- **遵守事項 5.2.1(3)(c)「IT 製品の調達におけるセキュリティ要件リスト」について**

  「IT 製品の調達におけるセキュリティ要件リスト」には、デジタル複合機、OS、ファイアウォール等の製品分野ごとに一般的に想定されるセキュリティ上の脅威が記載されており、それらが自身の運用環境において該当する場合には、当該脅威に対抗する必要がある。

対抗手段の一つとして、「IT 製品の調達におけるセキュリティ要件リスト」には、IT セキュリティに関わる「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、製品の利用環境や製品に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

参考：経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
（https://www.meti.go.jp/policy/netsecurity/youken.list.ver.2.1_20260121.pdf）

- **遵守事項 5.2.1(3)(d)「高度な情報セキュリティ対策を要求する情報システム」について**

  情報システムセキュリティ責任者は、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえて情報セキュリティに関するリスクを判断するとよい。例えば、本ガイドラインにおける情報システムの重要度：「高」又は「中」に該当する情報システムについては、情報セキュリティに関するリスクが高いと判断することも考えられる。

- **遵守事項 5.2.1(3)(d)「最高情報セキュリティアドバイザー等へ助言を求め」について**

  情報システムセキュリティ責任者は、構築する情報システムのリスクが高いと判断した場合、情報システムの分類に応じて策定したセキュリティ要件については、情報システムの所管部門のみでセキュリティ要件の判断をせずに、最高情報セキュリティアドバイザー等のセキュリティの専門家に評価してもらう必要がある。セキュリティの専門家については、例えば、最高情報セキュリティアドバイザーの他、情報セキュリティ推進部門やデジタル統括アドバイザー、情報セキュリティに関する資格（情報処理安全確保支援士等）保有者、業務委託による第三者機関等の利用も考えられる。

- **遵守事項 5.2.1(3)(d)「上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いか」について**

  セキュリティ要件を定める際には、5.1.1(2)(a)で定める情報システムの分類基準に応じた情報セキュリティ対策のみでだけでなく、情報システムの特性やサイバーセキュリティ分野の脅威動向を踏まえ、追加セキュリティ対策として定義されているセキュリティ対策をセキュリティ要件として盛り込む必要が無いかを検討することが考えられる。

- **基本対策事項 5.2.1(3)-1「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」について**

  「情報システムのセキュリティ要件」には、ハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システム

の運用のセキュリティ要件がある。

なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。

セキュリティ要件の策定には、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用するか又はそれと同等以上のセキュリティ水準となるよう検討を行い、その結果をシステム要件定義書や調達仕様書等の形式で明確にした上で、実装していくことが望ましい。

情報システムのセキュリティ要件を検討する際には、仮想化技術の活用の有無を確認し、物理的に分割されたシステムに限らず、論理的に分割されたシステムであるかを考慮したセキュリティ要件を検討することも重要である。「論理的に分割されたシステム」とは、一つの情報システムの筐体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。

また、外部の情報システムを利用する場合は、第 4 部「外部委託」も参照の上、委託先との管理責任範囲の分担を明確にし、セキュリティ対策の実施に漏れが生じないようにすることも重要である。

このように、情報システムの構築形態及び調達形態に応じてセキュリティ要件を定めることが求められる。

なお、情報システムのセキュリティ要件を定める考え方として、デジタル庁が公表している「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」を参考にするとよい。

参考：内閣官房国家サイバー統括室「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
（https://www.cyber.go.jp/policy/group/general/sbd_sakutei.html）

参考：デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」
（https://www.digital.go.jp/resources/standard_guidelines/）

- **基本対策事項 5.2.1(3)-2「開発する情報システムが運用される際に想定される脅威」について**

汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、全てを独自開発する場合であっても、外部から脆弱性をつかれる可能性があるため、開発する情報システムの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。

また、情報システムを構成する端末、サーバ装置、それらに搭載されているソフトウェア等に関して想定される脅威に対しては、第 6 部で規定された対策が適切に実施されるようにセキュリティ要件を策定することが必要となる。策定に当たっては、運用開始後に適切に対策が講じられるようにシステムの企画段階から留意が必要である。例えば、サーバ装置の運用時に必要になる不正アクセス等の監視機能を実装すること、端末やサーバ装置等に利用を認めるソフトウェア以外のソフトウェアが意図せず混入

されないこと等について留意が必要である。

- **基本対策事項 5.2.1(3)-3「ST 確認」について**

セキュリティ要件の策定に当たっては、脅威に対抗するために妥当なセキュリティ要件となっていることの確認を求める事項である。

セキュリティ要件の妥当性確認には、機関等内でのレビューの実施等の他に、対象とする情報システムが扱う業務及び情報の重要度によっては、セキュリティ要件の策定に関っていない客観的な立場の者による検証を実施することが望ましい。

「ST 確認」とは、情報システムが対抗すべき脅威について適切なセキュリティ要件が策定されていることを確認するために、セキュリティ設計仕様書（ST:Security Target）を IT セキュリティ評価基準（ISO/IEC 15408）に基づき、第三者である評価機関が評価し、その評価結果が妥当であることを認証機関（情報処理推進機構（IPA））が検証し、確認することをいう。

- **基本対策事項 5.2.1(3)-4「管理機能」について**

「管理機能」とは、真正確認、権限管理等のセキュリティ機能を管理するための機能のほか、情報セキュリティインシデントの発生時に行う対処及び復旧に係る機能、証跡保全の機能等を指し、これらの必要性を情報システムの設計時から検討することにより、必要がある場合には情報システムに組み込む必要がある。

- **基本対策事項 5.2.1(3)-4「監視のために必要な機能」について**

情報システム及び取り扱う情報の格付や取扱制限等を考慮して、情報システムの各所において様々なイベントを監視する必要性を見極める必要がある。監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。

監視に係る運用管理機能要件の策定については、遵守事項 7.1.6(1)(a)を参照のこと。

- **基本対策事項 5.2.1(3)-5「脆弱性への対策」について**

脆弱性対策を怠った場合には、セキュリティ侵害の機会を増大することにつながるため、情報システムの企画段階から対策を講じておく必要がある。

脆弱性が存在することが公表されているソフトウェア等については対策が施されているバージョンのものを利用することや、使用するソフトウェアのベンダが脆弱性の発見や脆弱性発見時の対応体制を有していることを確認すること等、開発後の情報システムに脆弱性が存在することが発覚した場合に備えて、調達時の調達仕様書に対策のための要件を記載することが重要である。

- **基本対策事項 5.2.1(3)-5 b)「脆弱性が混入されることを防ぐためのセキュリティ実装方針」について**

「脆弱性が混入されることを防ぐためのセキュリティ実装方針」とは、情報システム開発者が情報システムに脆弱性を混入することを防ぐために、開発時における脆弱性への具体的な対策方法を定めたものである。脆弱性は種類ごとに対策が異なり、懸念さ

れる脆弱性の種類ごとに方針を定める必要がある。具体的に定めるものとして、以下の例が考えられる。

- バッファオーバーフローによる不正なプログラムの挿入及び実行を防ぐために、データを転記する場面においてメモリ領域長とデータ長を検査する処理を付加する。
- SQL インジェクションによるデータベース内の情報の漏えい・改ざんを防ぐために、プレースホルダにより SQL 文を組み立てる。
- OS コマンドインジェクションによる不正なシステム操作を防ぐために、シェルを起動できる言語機能を利用しない。

7.2.1「ソフトウェアに関する脆弱性対策」及び 6.2.3「ウェブ」、6.6.1「アプリケーション・コンテンツの作成・運用時の対策」の規定内容も参考にして、懸念される全ての脆弱性の種類に対して、実装方針を定め、調達仕様書に明記する必要がある。

- **基本対策事項 5.2.1(3)-6 a)「機器等を調達する場合」について**

情報システムで利用する機器等を調達する場合は、当該機器等の製造工程で不正なプログラム等が加えられていないことを確認することが重要である。そのため、情報システムのセキュリティ要件を定める際に調達する機器等に関する要件を企画段階にて定める必要がある。具体的には、4.3「機器等の調達」を参照のこと。

- **基本対策事項 5.2.1(3)-6 b)「機関等の意図せざる不正なプログラム等が混入されることを防ぐための対策」について**

情報システムで提供するアプリケーション・コンテンツの開発においては、自らが開発するソフトウェアのみならず、機関等外のものが提供するソフトウェアを利用することも考えられる。そのため、提供するアプリケーション・コンテンツが不正プログラムを含まないようにする必要がある。具体的には、6.6.1「アプリケーション・コンテンツの作成・運用時の対策」を参照のこと。

- **基本対策事項 5.2.1(3)-6 c)「機関等の意図せざる変更が加えられないための管理体制」について**

情報システムの構築における業務委託において、機関等の意図せざる変更が加えられないための管理体制を求めるため、情報システムの開発工程において、一貫した品質保証体制の下でなされていることを確認できる必要がある。具体的には、4.1「業務委託」を参照すること。

- **基本対策事項 5.2.1(3)-7「要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システム」について**

要安定情報を取り扱う情報システムは、当該情報システムの停止が国民の安全や利益に重大な影響をもたらす可能性があるものや他の情報システムへ重大な影響を及ぼすものなどが存在する。そのような情報を取り扱う情報システムにおいては、情報セキュリティインシデントが発生した際や危機的事象が発生した際にも運用を継続させるための要件を策定することが重要である。

また、各機関の業務継続計画において、非常時優先業務等を支える情報システムとさ

れている情報システムは、危機的事象発生時においても運用を継続させる必要があり、そのためには、情報システム運用継続計画を踏まえて要件を策定する必要がある。また、危機的事象発生時における情報セキュリティに係る対策事項を定めている場合は、その内容も踏まえて検討する必要がある。

情報システムの運用継続計画については、5.3「情報システムの運用継続計画」を参照のこと。

- **基本対策事項 5.2.1(3)-7 a)「冗長化に関する要件」について**

機器等の冗長化に関しては、ハードウェア自体の冗長化やソフトウェアを用いた冗長化のみならず、電源装置の冗長化、設置場所を考慮した冗長化等の物理的な対策も考えられる。また、機関等外のものが提供するサービスや通信回線等を利用する場合は、当該サービスにおけるサービスレベル等を考慮した上で情報システムの冗長化に関する要件を策定する必要がある。

- **基本対策事項 5.2.1(3)-7 b)「バックアップの要件」について**

情報システムや情報を破壊することを目的とした不正プログラムによって、情報セキュリティインシデントが発生した際、情報システムを復旧させるための方法としてバックアップから復旧する方法がある。一方で、適切なバックアップの取得方法や復旧方法に関する要件を定めていない場合、復旧が困難になる可能性がある。よって、情報システムの特性を踏まえて、必要に応じてバックアップに関する要件を定める必要がある。

また、構築する情報システムにおいて、暗号化消去を目的とした情報の暗号化を実施する場合は、暗号化に用いた鍵の管理が重要である。例えば、暗号鍵が何らかの理由により使えなくなった場合は、情報の復元が困難となる。よって、暗号鍵のバックアップに関する要件を定めておく必要がある。なお、暗号鍵の管理については、「(解説) 基本対策事項 7.1.5(1)-3 b)「管理手順を定めること」について」を参照のこと。

- **基本対策事項 5.2.1(3)-7 c)「復旧に関する要件」について**

要安定情報を取り扱う情報システムや非常時優先業務等を支える情報システムなど、業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務等にて利用する情報システムにおいては、危機的事象発生時においても情報システムの運用を継続させる必要がある。そのため、RTO（目標復旧時間）、RLO（目標復旧レベル）を踏まえた情報システムの復旧に関する要件を定めておく必要がある。

- **基本対策事項 5.2.1(3)-8 a)「インターネットやインターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する」について**

標的型攻撃による不正プログラム感染の脅威は避けられないものになっており、外部のネットワークと接続する情報システムは、不正プログラムの感染を前提とした対策を講ずることが重要である。

外部ネットワークとの接続形態を含む情報システムの全体構成は、情報システムにおいて取り扱われる情報の格付や取扱制限、情報システムを利用する業務の形態等によって決定する必要があるが、特に重要な情報を取り扱う情報システムについては、イ

ンターネットからの組織内部への侵入を企図したサイバー攻撃への対策(入口対策)や、組織内部へ侵入した攻撃によるインターネットへの不正通信又は情報流出への対策(出口対策)として、インターネット回線や、インターネットに接点を有する情報システム(クラウドサービスを利用して構築した情報システムを含む。)との間に適切なセキュリティ対策を講じ、通信経路を論理的に分離すること等が求められる。なお、情報システムのネットワーク構成の要件を策定する際は、基本対策事項 6.4.1(1)-1、基本対策事項 7.1.2(1)-1 d)についても併せて検討し、情報システムのネットワーク構成の要件を決定するとよい。また、分離した情報システムの USB ポート等の外部ネットワーク・システムとの接点についても適切に運用することが望ましい。

- **基本対策事項 5.2.1(3)-8 b)「利用するソフトウェアを実行するために必要な通信要件」について**

  機器等において利用するソフトウェアを実行するために必要なポートを開放する場合がある。不必要なポートを開放したままにしていると、それを悪用される可能性があることを踏まえて、ポートを開放する必要性を検討する必要がある。また、悪意ある不正プログラム等により、悪意ある攻撃に使用するためのポートを開放されてしまう可能性もあるため、外部ネットワークへ不正な通信をさせないような対策も重要である。よって、情報システムを構築する場合は、必要となるポート、プロトコル及びサービスを検討した上で有効とするとともに、外部ネットワークとの通信を制限する等の要件を定める必要がある。なお、ポートについては例えば、管理等でよく利用される 20 番、21 番、22 番、23 番、ファイル共有サービス等によく利用される 137 番、138 番、139 番、445 番、リモートデスクトップ等で利用される 3389 番などは、悪用される可能性が高いため開放することの要否を検討し特に注意が必要である。なお、使用しないポートについては原則として閉じる必要がある。

- **基本対策事項 5.2.1(3)-8 c)「通信経路全般のネットワーク構成」について**

  インターネット等の外部ネットワーク上のサービスを利用する情報システムについては、当該サービスとの間に適切なセキュリティ対策を講ずる必要がある。例えば、機関等外通信回線を使用してクラウドサービスにアクセスする場合は、CASB と呼ばれる“クラウドサービスの利用度の可視化”や“アクセス制御”などの機能を持つサービス等を利用し、不正なアクセスを管理するなどの要件を定めることも考えられる。よって、構築する情報システムにおいてインターネット上のサービス等を利用する場合などは、通信経路全般のネットワーク構成を定める必要がある。

- **基本対策事項 5.2.1(3)-8 d)「リモートメンテナンスすることの要否」について**

  構築する情報システムに対して機関等外通信回線を経由してリモートメンテナンスを許可する必要がある機器については、アクセスすることのリスクを検討した上で要否を判断する必要がある。リモートメンテナンスを許可する場合は、不正アクセス等のリスクを低減させるネットワーク構成等の要件を検討する必要がある。なお、リモートからのアクセスが可能な機器等の中には、管理画面等の機能を有しているものや初期の設定からリモートからのアクセスを可能にしているものなどが存在するので、リモー

トからのアクセスを許可しない機器等に関しては、アクセスできないようにすることを求めることなどが考えられる。

リモートメンテナンスについては、遵守事項 6.4.1(2)(c)を参照のこと。

- **基本対策事項 5.2.1(3)-9 b)「機器等の利用環境において対抗すべき脅威」について**

機器等に対するセキュリティ上の脅威は利用環境によって変わるため、調達時にどのような環境で運用するのかを把握し、その環境において存在する脅威及びその脅威に対する脆弱性を分析した上で、必要となるセキュリティ要件を策定する必要がある。

例えば、ネットワークに接続し、通信データとして要機密情報を送受信する場合に盗聴による情報漏えいが想定される場合には、通信データの保護に係るセキュリティ要件が必要となるが、スタンドアロンで利用する場合で、盗聴による情報漏えいが想定されない場合には、通信データの保護に係るセキュリティ要件は不必要なセキュリティ要件となる可能性がある。

また、特定の人物しか物理的にアクセスできないように隔離された場所へ機器等を設置すること等で、誰もが物理的にアクセスできる環境で想定される脅威を軽減することも考えられる。

調達する機器ごとの利用環境において想定される脅威を漏れなく分析した上で、脅威に対抗するために必要十分なセキュリティ要件を策定することが重要である。

5.2.2 情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

なお、情報システムの構築を委託する場合は 4.1「業務委託」、クラウドサービスを利用して構築する場合は 4.2「クラウドサービス」、情報システムで使用する機器等を調達する場合は 4.3「機器等の調達」を参照し遵守する必要がある。

遵守事項

(1) 情報システムの構築時の対策

(a) 情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

(b) 情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

(c) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告すること。

(d) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備すること。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

(イ) 情報システムを構成する通信回線及び通信回線装置関連情報

(e) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備すること。

(ア) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(イ) 情報セキュリティインシデントを認知した際の対処手順

(ウ) 情報システムが停止した際の復旧手順

【 基本対策事項 】

＜5.2.2(1)(a)関連＞

5.2.2(1)-1 情報システムセキュリティ責任者は、情報システムの構築において以下を全て含む情報セキュリティ対策を行うこと。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。
c) 情報システムで使用する機器やソフトウェア等においては、設定の誤りを防止するため、当該提供者が提示している**推奨設定や業界標準、ベストプラクティス等**を参照し、情報システムの各種設定を行うこと。
d) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。
e) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。
f) **脆弱性検査を含む情報セキュリティの観点での試験を実施する**こと。

＜5.2.2(1)(b)関連＞

5.2.2(1)-2 情報システムセキュリティ責任者は、情報システムの運用保守段階へ移行するに当たり、以下を全て含む情報セキュリティ対策を行うこと。
a) 情報セキュリティに関わる運用保守体制の整備
b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
c) 情報セキュリティインシデントを認知した際の対処方法の確立

＜5.2.2(1)(d)(ア)関連＞

5.2.2(1)-3 情報システムセキュリティ責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を全て含む文書を整備すること。
a) サーバ装置及び端末を**管理する職員等**及び利用者を特定する情報
b) サーバ装置及び端末の**機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等**
c) サーバ装置及び端末で利用する**ソフトウェアを動作させるために用いられる他のソフトウェア**であって、以下を全て含むものの種類、名称及びバージョン、入手先、サポート体制等
- 動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの
- フレームワーク等、ソフトウェアを実行するための実行環境となるもの
- プラグイン等、ソフトウェアの機能を拡張するもの
- 静的リンクライブラリ等､機関等がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの
- インストーラー作成ソフトウェア等、機関等がソフトウェアを開発する際に開発を支援するために使用するもの

d) サーバ装置及び端末の**調達仕様書又は設計書**

5.2.2(1)-4 情報システムセキュリティ責任者は、前項 b)及び c)の情報を収集するため、**自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェア**を導入するなどにより、これら情報を効率的に収集する手法を決定すること。

＜5.2.2(1)(d)(イ)関連＞

5.2.2(1)-5 情報システムセキュリティ責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を全て含む文書を整備すること。
a) 通信回線及び通信回線装置を**管理する職員等**を特定する情報

b) 通信回線装置の**機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等**

c) 通信回線及び通信回線装置の**調達仕様書又は設計書**

d) **通信回線の構成**

e) 通信回線装置におけるアクセス制御の設定

f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

g) 通信回線の利用部門

＜5.2.2(1)(e)(ア)関連＞

5.2.2(1)-6 情報システムセキュリティ責任者は、所管する情報システムについて、情報システム構成要素ごとの**セキュリティ維持に関する以下を全て含む運用手順**を実施手順として整備すること。

a) サーバ装置及び端末のセキュリティの維持に関する手順

b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順

c) **インターネット等の外部ネットワーク経由で利用するサービス**のセキュリティの維持に関する手順

d) 通信回線及び通信回線装置のセキュリティの維持に関する手順

e) 端末、サーバ装置、通信回線装置等において利用する**ソフトウェアのセキュリティの維持**に関する手順

（解説）

- **遵守事項 5.2.2(1)(b)「移行手順及び移行環境」について**

情報システムの開発環境、テスト環境から本番運用の環境への移行時において、情報システムに保存されている情報の取扱手順の整備、人為的な操作ミスを防止するための手順・環境の整備、移行の際に関連システム停止が伴う場合には可用性確保のための環境整備等が必要となる。

- **遵守事項 5.2.2(1)(c)「情報システムを新規に構築し、又は更改する際には」について**

情報システム台帳の整備内容の網羅性維持のため、情報システムセキュリティ責任者は、情報システムを新規に構築した際又は更改した際には、速やかに情報システム台帳に記載の事項を報告する必要がある。

なお、情報システム台帳を最新に保つため、情報システム台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、情報システム台帳を更新する必要があるが、その報告の方法や時期については、機関等ごとに定めることが望ましい。

- **遵守事項 5.2.2(1)(c)「情報システム台帳のセキュリティ要件」について**

情報システム台帳に記載する内容については、2.1.2「資産管理」を参照のこと。

- **遵守事項 5.2.2(1)(d)「情報システム関連文書を整備する」について**

当該事項については、各情報システムの運用管理に際して整備した文書に記載する

事項のうち、機関等としての情報セキュリティ対策を行うために一元的に把握する必要があると判断するものを含める必要がある。

文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は電磁的記録として整備してもよい。

また、所管する情報システムに変更があった場合、また、想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になるため、文書の見直しを定期的に行うことをあらかじめ定めておくとよい。

なお、クラウドサービスを利用する際に、事業者から提供される情報が十分でない場合は、利用するクラウドサービスに応じた内容の情報システム関連文書を整備することも考えられる。

- **遵守事項 5.2.2(1)(e)(イ)「情報セキュリティインシデントを認知した際の対処手順」について**

情報セキュリティインシデントを認知した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。

- 業務継続計画で定める当該情報システムを利用する業務の重要性
- 情報システムの運用等の業務委託の内容

また、手順に記載される内容として、以下の例が想定される。

- 情報セキュリティインシデントの内容・影響度の大きさに応じた情報システムに関連する部署等や利用するクラウドサービス、政府共通利用型システム、業務委託先等の連絡先のリスト
- 情報システムを障害等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準、決定権者
- 情報セキュリティインシデントに対する情報システムの構成要素ごとの対処に関する事項
- 不正プログラム対策ソフトウェアでは検知されない新種の不正プログラムに感染した場合やインシデントレスポンスのうち、デジタルフォレンジック等の支援を受けるための外部の専門家の連絡先

なお、統括情報セキュリティ責任者が整備する対処手順（「(解説)遵守事項 2.2.4(1)(b)「対処手順」について」を参照のこと。）が、情報システムの事情に応じた内容で整備されているならば、情報システム別に整備しなくても構わない。

- **遵守事項 5.2.2(1)(e)(ウ)「情報システムが停止した際の復旧手順」について**

当該情報システムが停止した際の影響や停止が許容される時間を考慮し、情報システムの運用を開始するまでに情報システムが停止した際の復旧手順を整備する必要がある。復旧のための手順には、復旧させる機器等の優先度を含めることやバックアップを取得している場合のリストア手順、代替サイトや交換用の機器を準備している場合の切替え手順、復旧時の役割と責任等を記載するとよい。

- **基本対策事項 5.2.2(1)-1「情報セキュリティ対策」について**

  情報システムの構築を業務委託する場合には、遵守事項 4.1.2(2)の内容を委託先に適切に実施させることが求められる。また、情報システムの構築を業務委託せず、機関等自らが構築する場合であっても、同項の内容を参照し、必要な対策を実施することが求められる。

- **基本対策事項 5.2.2(1)-1 c)「推奨設定や業界標準、ベストプラクティス等」について**

  機器等の設定を行う際は、設定の誤りや設定不備を防止するために利用する機器等に関する推奨設定や業界標準、ベストプラクティス等を参照する必要がある。その際、機器等の提供者が提供している推奨設定等を確認することも考えられるが、情報処理推進機構（IPA）の「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」や内閣官房国家サイバー統括室の「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊.クラウド設計・開発編」等も参照することも考えられる。また、具体的な設定値の参考となるよう、米国の政府機関・企業等が協力して設立された非営利団体 CIS（Center for Internet Security）が発行するセキュリティ対策のベストプラクティスである、CIS Benchmarks 等も参考にするとよい。

  参考：情報処理推進機構（IPA）「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」
  （https://www.ipa.go.jp/digital/model/model20201222.html）

  参考：内閣官房国家サイバー統括室「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊.クラウド設計・開発編」
  （https://www.cyber.go.jp/policy/group/general/sbd_sakutei.html）

  参考：CIS Benchmarks
  （https://www.cisecurity.org/cis-benchmarks/）

- **基本対策事項 5.2.2(1)-1 f)「脆弱性検査を含む情報セキュリティの観点での試験を実施する」について**

  脆弱性を検査するためには、専用ツールを用いて脆弱性診断を行うことや、事業者が提供するサービス等を利用して脆弱性診断を行うことが挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、構築する情報システムの構成等によって利用する脆弱性診断を使い分ける必要がある。例えば、ソースコード診断においては、試験を実施する規模により初期の開発段階から試験を組み込むことなども考えられる。また、プラットフォーム診断やウェブアプリケーション診断については、運用開始前に本番環境を前提に実施することが望ましいが、やむを得ず検証環境で実施する場合は、本番環境と同等の構成等において実施することが有効である。脆弱性診断を実施する際は、デジタル庁が公表している以下のガイドラインを参考にするとよい。

  参考：デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」

（https://www.digital.go.jp/resources/standard_guidelines/）

なお、脆弱性診断については、「（解説）基本対策事項 7.2.1(1)-1「脆弱性診断を実施」について」を参照のこと。

- **基本対策事項 5.2.2(1)-3 a)・基本対策事項 5.2.2(1)-5 a)「管理する職員等」について**

  サーバ装置及び端末の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システムの構成要素の管理状況を確実に把握できるようにするとともに、障害等を防止する責任の所在を明確にするために必要な事項である。

- **基本対策事項 5.2.2(1)-3 b)・基本対策事項 5.2.2(1)-5 b)「機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等」について**

  サーバ装置及び端末、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアに脆弱性が存在することにより使用上のリスクが高まった場合に、速やかに脆弱性対策を行うなど、適切に対処するために必要な事項である。また、サポート体制については、サポートが終了した製品を使用することは脆弱性への対応がなされずセキュリティ上のリスクとなるため、情報システムを更改するまでサポートが可能であるかを事前に把握する必要がある。

- **基本対策事項 5.2.2(1)-3 c)「ソフトウェアを動作させるために用いられる他のソフトウェア」について**

  一般に外部から入手するソフトウェアは、ソフトウェア開発元が脆弱性情報を提供する。一方、機関等が開発するソフトウェアについては、機関等自身が開発元として当該ソフトウェアの脆弱性情報を提供する立場となる。機関等は、当該ソフトウェアを国民等に提供する場合のみでなく、機関等自身が利用する場合においても情報セキュリティ対策を実施する必要があることから、いずれの場合においても当該ソフトウェアに組み込まれて使用されるライブラリ等のソフトウェアについても脆弱性情報を把握することが求められる。そのため、組み込まれているライブラリ等についても種類及びバージョンを機関等自身が把握する必要がある。なお、機関等がソフトウェアの開発を委託する場合においては、委託事業者から当該情報を漏れなく入手する必要がある。

  また、システムで使用するソフトウェアには、プラグイン等の機能拡張用のソフトウェアにより機能を追加できるものがある。ただし、機能拡張用のソフトウェアは、元となるソフトウェアと開発元が異なる場合があり、機能拡張用のソフトウェアの脆弱性情報が、元となるソフトウェアの開発元から提供されない可能性がある。そのため、機能拡張用のソフトウェアについても個別に種類及びバージョンを事前に把握する必要がある。

  さらに、情報システムにおいてオープンソースソフトウェアを利用する場合は、脆弱性への対応のために利用状況を把握する必要があるとともに、著作権及び許諾条件を侵害することの無いよう、適切にオープンソースソフトウェアを用いているかを事前に把握する必要がある。なお、オープンソースソフトウェアは、商用ソフトウェアと比べソフトウェアとしてのライフサイクル（サポート期間等）が短く、またサポートが十

分ではない場合があることに注意が必要である。オープンソースソフトウェアについては、以下を参考にするとよい。

参考：経済産業省「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」

- **基本対策事項 5.2.2(1)-3 d)・基本対策事項 5.2.2(1)-5 c)「調達仕様書又は設計書」について**

  情報システムに係る調達仕様書又は設計書は、情報セキュリティ対策の実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。

- **基本対策事項 5.2.2(1)-4「自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェア」について**

  情報システムで使用しているソフトウェア等の IT 資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有する IT 資産管理ソフトウェアを導入することが有用である。

  なお、当該ソフトウェアにはサーバ装置及び端末における USB メモリ等の外部電磁的記録媒体の利用やネットワーク接続を制御する等の機能を持つものもあることから、情報セキュリティ対策の観点も含め検討するとよい。

- **基本対策事項 5.2.2(1)-5 d)「通信回線の構成」について**

  当該事項における通信回線の構成は、情報システムを構成する要素の接続関係を明記した図を想定している。なお、情報システムにおいて利用するクラウドサービスの提供形態や仕様においては、クラウドサービス内の接続関係を示すことが困難な場合があるため、その場合はクラウドサービスまでの接続関係を明記するとよい。また、当該事項には、通信回線の構成図にデータの流れも記載することが望ましい。情報システムを構成する要素ごとに取り扱うデータの種類を把握することで、経路上の脅威を洗い出し、データの流れ上で脅威が発生した時に影響を及ぼす範囲を把握するために必要となる。

- **基本対策事項 5.2.2(1)-6「セキュリティ維持に関する以下を全て含む運用手順」について**

  情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理、ログ管理及び暗号化機能等の設定・変更等の手順が挙げられる。

- **基本対策事項 5.2.2(1)-6 c)「インターネット等の外部ネットワーク経由で利用するサー**

ビス」について

機関等においてインターネット等の外部ネットワーク経由で利用するクラウドサービスや政府共通利用型システムなどのセキュリティを維持するために管理者が実施すべき手順も定めておく必要がある。

- **基本対策事項 5.2.2(1)-6 e)「ソフトウェアのセキュリティ維持」について**

  情報システムの構成要素ごとに利用するソフトウェアのセキュリティ維持に関する手順を定める必要がある。例えば、端末やサーバ装置、通信回線装置の OS に係る脆弱性対策に関する手順だけでなく、機器等のファームウェアに関する脆弱性対策や機関等において作成したアプリケーションに含まれるライブラリやプラグイン等の拡張機能、オープンソースソフトウェアに関する脆弱性対策の手順などを定めておく必要がある。具体的には、公開された脆弱性についての情報を入手する方法や情報を受け取る人又は組織等を決めておくこと、公開された脆弱性の緊急度を判断するための手順、緊急度に応じたセキュリティパッチの適用方針などを手順にするとよい。

遵守事項

(2) 納品検査時の対策

(a) 情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、**情報セキュリティ対策に係る要件が満たされていることを確認する**こと。

(b) 情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、**情報セキュリティ対策に必要な内容が含まれている**ことを確認すること。

【 基本対策事項 】

＜5.2.2(2)(a)関連＞

5.2.2(2)-1 情報システムセキュリティ責任者は、情報システムの受入れ時の確認・検査を行う場合は、以下を全て含む内容を確認すること。

a) 情報システムの構築時に使用し、運用時に**不要となる識別コード**が削除されていること。

b) 機器等において推測可能な**初期値として設定されている主体認証情報等**が変更されていること。

c) 機器等において**公開された脆弱性について対策を実施していること**。

d) 機器等において不要なポートが開放されていない、不要なサービスが起動していない、利用を認めていないソフトウェアが動作していないこと。

（解説）

- **遵守事項 5.2.2(2)(a)「情報セキュリティ対策に係る要件が満たされていることを確認する」について**

情報セキュリティ対策の視点を加味して整備された納入時の確認・検査手続に従い、納入された情報システム及び機器等が要求仕様どおりに正しく動作することの検査を行うことが求められる。

機関等における受入れテストの実施、納入元が実施したテストに関する資料の提出要求及びその検査内容の確認、第三者への受入れテストの委託、ISO/IEC 15408 に基づく第三者認証取得の確認等、検査対象の情報システム及び機器等の特性に応じて適切な検査を実施する必要がある。

- **遵守事項 5.2.2(2)(b)「情報セキュリティ対策に必要な内容が含まれている」について**

情報セキュリティ対策に必要な内容とは、遵守事項 5.2.2(1)(d)(ア)、(イ)及び遵守事項 5.2.2(1)(e)(ア)に記載の情報を意味する。

なお、情報システムの運用保守事業者が交代する場合には、現在の事業者から次期事業者への引継事項の確認も同様に行う必要がある。

- **基本対策事項 5.2.2(2)-1 a)「不要となる識別コード」について**

  情報システムを開発する際に使用したテスト用の識別コードなど、運用時には不要となる識別コードが残っていないことを確認する必要がある。そのような不要な識別コードを把握していない場合、当該識別コードを悪用される可能性があるため、確実な確認をする必要がある。

- **基本対策事項 5.2.2(2)-1 b)「初期値として設定されている主体認証情報等」について**

  情報システムで利用する機器等によっては、初期値として管理者権限を有する識別コードが存在する。そのような識別コードには、初期値として主体認証情報が設定されている可能性があり、当該主体認証情報は、マニュアル等にて公開されている場合がある。よって、機器等において推測可能な初期値として管理者権限を有する識別コードが存在する場合は、当該識別コードを無効にすることや初期値として設定されている主体認証情報を変更するなどの対応がなされていることを確認することが求められる。なお、そのような識別コードが存在する機器等は、端末や通信回線装置のみならず、無停電電源装置や NAS（Network Attached Storage）、ソフトウェアなどの情報システムの構成要素も含まれていることに注意が必要である。

  また、SNMP（Simple Network Management Protocol）と呼ばれる機器等の状態を監視するためのプロトコルで使用するコミュニティ名についても、誰でも知り得る設定値を使用している場合、なりすまし等によって監視対象の機器等の情報を窃取し、踏み台にして悪用されるなどの可能がある。したがって、SNMP で使用するコミュニティ名についても推測可能な初期値として設定されているものは、そのまま使用せずに変更するなどの対応がなされていることを確認することが求められる。

- **基本対策事項 5.2.2(2)-1 c)「公開された脆弱性について対策を実施していること」について**

  情報システムを運用開始する前に当該情報システムで利用する構成要素ごとに公開されている脆弱性について対策を実施していることを確認する必要がある。公開された脆弱性に関する情報については、製品ベンダや脆弱性情報提供サイト等にて確認するとともに、内閣官房国家サイバー統括室や JPCERT/CC、情報処理推進機構（IPA）等からの注意喚起も参照するとよい。

  ソフトウェアの脆弱性対策については、7.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

5.2.3 情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、対策基準に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。なお、情報システムの運用・保守を業務委託する場合は、4.1「業務委託」を参照のこと。

さらに、クラウドサービスを利用して構築された情報システムの運用・保守をする場合は、4.2「クラウドサービス」、政府共通利用型システムを利用して構築された情報システムを運用・保守する場合は、5.4「政府共通利用型システム」を参照すること。

遵守事項

(1) 情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装された**監視を含むセキュリティ機能**を適切に運用すること。

(b) 情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって**機器の構成や設定情報等に変更があった場合**は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

(c) 情報システムセキュリティ責任者は、情報システムの運用・保守において、**情報システム台帳及び関連文書の内容に変更が生じた場合**、情報システム台帳及び関連文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告すること。

(d) 情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により**見直し**を適時検討し、必要な措置を講ずること。

(e) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**について、危機的事象発生時に適切な対処が行えるよう運用をすること。

【 基本対策事項 】

＜5.2.3(1)(a)関連＞

5.2.3(1)-1 情報システムセキュリティ責任者は、情報システムのセキュリティ監視について、以下の内容を全て含む監視手順を定め、**適切に監視運用する**こと。

a) 監視するイベントの種類や重要度
b) 監視体制
c) 監視状況の報告手順や重要度に応じた報告手段
d) 情報セキュリティインシデントの可能性を認知した場合の報告手順
e) 監視運用における情報の取扱い（機密性の確保）

5.2.3(1)-2 情報システムセキュリティ責任者は、情報システムに実装された**セキュリティ機能が適切に運用されていること**を確認すること。

5.2.3(1)-3 情報システムセキュリティ責任者は、情報システムにおいて取り扱う情報について、**当該情報の格付及び取扱制限が適切に守られていること**を確認すること。

5.2.3(1)-4 情報システムセキュリティ責任者は、情報システムで**不要となった識別コードや過剰なアクセス権限等の付与がないか適時見直す**こと。

5.2.3(1)-5 情報システムセキュリティ責任者は、運用中の情報システムにおいて**定期的に脆弱性対策の状況を確認する**こと。

5.2.3(1)-6 情報システムセキュリティ責任者は、運用中の情報システムの**脆弱性の存在が明らかになった場合**には、情報セキュリティを確保するための措置を講ずること。

＜5.2.3(1)(e)関連＞

5.2.3(1)-7 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システムについて、以下を全て含む運用をすること。

a) 情報システムの各構成要素及び取り扱われる情報に関する**適切なバックアップの取得及びバックアップ要件の確認による見直し**
b) 情報システムの構成や設定の変更等が行われた際及び定期的に、**情報システムが停止した際の復旧手順の確認による見直し**

（解説）

- **遵守事項 5.2.3(1)(a)「監視を含むセキュリティ機能」について**

情報システムにおいて実装した監視機能を含む情報システムのセキュリティ機能については、適切に運用する必要がある。なお、情報システムのセキュリティ機能を適切に運用するためには、以下の各款における規定内容に示される対策を行うことが求められる。

- 7.1.1「主体認証機能」
- 7.1.2「アクセス制御機能」
- 7.1.3「権限の管理」
- 7.1.4「ログの取得・管理」
- 7.1.5「暗号・電子署名」
- 7.1.6「監視機能」

- **遵守事項 5.2.3(1)(b)「機器の構成や設定情報等に変更があった場合」について**

情報システムの運用や保守における作業において、情報システムを構成する要素である機器等に変更があった場合や機器等の設定情報に変更が生じた場合は、当初に想

定していた情報セキュリティ対策が有効に機能しているか等の確認をし、不適切な状態にあった場合は、是正する措置等を講ずるなどの対策が求められる。

- **遵守事項 5.2.3(1)(c)「情報システム台帳及び関連文書の内容に変更が生じた場合」について**

  情報システム台帳の整備内容の網羅性維持のため、情報システムセキュリティ責任者は、情報システムの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等への修正又は変更が発生した場合、速やかに情報システム台帳を更新又は修正し、統括情報セキュリティ責任者に報告する必要があるが、その報告の方法や時期については、機関等ごとに定めることが望ましい。

  なお、情報システムセキュリティ責任者は、必要に応じて情報システムに係る関連文書として整備した情報システムの情報セキュリティ対策を維持するための情報も併せて更新又は修正することが求められる。

- **遵守事項 5.2.3(1) (d)「見直し」について**

  情報システムの情報セキュリティ対策について、新たな情報セキュリティ上の脅威、情報セキュリティインシデント発生事案例及び情報セキュリティインシデント発生時の影響等を検討した上で、情報システムの情報セキュリティ対策について定期的に確認し、必要に応じて見直しを行い、セキュリティ要件の追加、修正等の必要な措置を求める事項である。

  所管する情報システムに変更があった場合、情報システムの外部環境に変化が生じた場合等の際には、定期的な情報セキュリティ対策の確認による見直しに加えて、適時見直すことも必要となる。

  また、情報システムにおいて取り扱う情報の格付や取扱制限が変更になった場合は、情報システムの分類が適切であるかを確認し、必要に応じて情報システムの分類を見直す必要がある。なお、情報システムの分類を見直した場合、情報システムの分類基準に基づく具体的な対策事項が変更になるため、情報システムのセキュリティ要件の見直しが必要になることに注意が必要である。

- **遵守事項 5.2.3(1)(e)「要安定情報を取り扱う情報システム」について**

  要安定情報を取り扱う情報システムについては、「(解説) 基本対策事項 5.2.1(3)-7「要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システム」について」を参照のこと。

- **基本対策事項 5.2.3(1)-1「適切に監視運用する」について**

  監視機能については、7.1.6「監視機能」を参照のこと。

- **基本対策事項 5.2.3(1)-2「セキュリティ機能が適切に運用されていること」について**

  運用する情報システムについて、平常時の定期的な確認に加え、外部環境が大きく変化した場合等には、セキュリティ機能が適切に運用されるために、機器等のパラメータ設定、物理的な設置環境、ネットワーク環境、人的な運用体制等について問題が無いことを適宜確認する必要がある。

- **基本対策事項 5.2.3(1)-3「当該情報の格付及び取扱制限が適切に守られていること」について**

  情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更されていることを確認する必要がある。

- **基本対策事項 5.2.3(1)-4「不要となった識別コードや過剰なアクセス権限等の付与がないか適時見直す」について**

  情報システムにアクセスする必要がなくなった識別コードの見直しについては、遵守事項 7.1.1(2)(b)を参照のこと。アクセス権限等の付与に関する見直しについては、遵守事項 7.1.2(1)(b)及び遵守事項 7.1.3(1)(c)を参照のこと。

- **基本対策事項 5.2.3(1)-5「定期的に脆弱性対策の状況を確認する」について**

  脆弱性対策の状況を確認することについては、遵守事項 7.2.1(1)(c)を参照のこと。

- **基本対策事項 5.2.3(1)-6「脆弱性の存在が明らかになった場合」について**

  機関等が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。そのためには、公開された脆弱性についての影響度と緊急度を判断する必要がある。緊急度を判断するためには、公開された脆弱性の深刻度を示す CVSS（Common Vulnerability Scoring System）の値や当該脆弱性を悪用した攻撃の段階（例えば、脆弱性を用いた攻撃手法が出回っている、既に脆弱性を用いた攻撃が確認されているなど）などを考慮して検討するとよい。なお、脆弱性への対処に関する判断については、SSVC（Stakeholder-Specific Vulnerability Categorization）と呼ばれる脆弱性の管理手法を用いて検討することも考えられる。SSVC については、米国の CISA が公表したガイドラインを用いることで、脆弱性対策への優先順位の参考にすることができる。当該ガイドラインでは、「脆弱性の悪用状況」、「脆弱性を悪用した場合の技術的な影響」、「攻撃の自動化の可否」、「業務における必須機能への影響」、「公共福祉への影響」の観点から SSVC 決定木を用いて、脆弱性対応への優先度付けを行うことができる。

  これらを踏まえて、脆弱性を悪用されないための措置を講ずることや、セキュリティパッチを適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。また、情報セキュリティ対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずる必要もある。

  脆弱性に関する情報については、製品ベンダや脆弱性情報提供サイト等から通知を受け取るようにするとともに、内閣官房国家サイバー統括室や JPCERT/CC、情報処理推進機構（IPA）等からの注意喚起も参照するとよい。

  なお、CVSS や SSVC については、以下を参考にするとよい。

  参考：情報処理推進機構（IPA）「共通脆弱性評価システム CVSS v3 概説」

（https://www.ipa.go.jp/security/vuln/scap/cvssv3.html）

参考：Cybersecurity and Infrastructure Security Agency（CISA）「Stakeholder-Specific Vulnerability Categorization」
（https://www.cisa.gov/ssvc）

- **基本対策事項 5.2.3(1)-7 a)「適切なバックアップの取得及びバックアップ要件の確認による見直し」について**

情報システムを構成する各構成要素は、RTO（目標復旧時間）、RLO（目標復旧レベル）を踏まえて必要に応じてバックアップを取得する必要がある。そのバックアップの方法については、OS やアプリケーションなどを含むサーバ装置等全体をバックアップする方法やサーバ装置等の複製を用意する方法などが存在する。また、クラウドサービスの仮想 OS やネットワーク機器に関しては、構成情報をバックアップしておき、危機的事象発生時はバックアップした構成情報を利用し切替えるなどの方法も存在する。よって、バックアップを取得する対象やその方法については、RTO（目標復旧時間）、RLO（目標復旧レベル）を踏まえて決定するとよい。

また、不正アクセス等によって情報システムを破壊する標的型攻撃により取得したバックアップが暗号化されてしまうケースが存在するため、バックアップの世代管理、保存場所や媒体についても考慮する必要がある。例えば、標的型攻撃によりマルウェアが潜伏している状態でバックアップを取得していた場合、復元した際にマルウェアも復元してしまう可能性がある。そのため適切な世代管理を実施することも考えられる。バックアップの保存場所に関しては、バックアップを取得したサーバ装置と同じネットワークにバックアップを保存していた場合、サーバ装置が暗号化された際に、同じネットワーク上に保存したバックアップも同時に暗号化されてしまう可能性がある。そのため、バックアップの保存場所に関しては論理的に切り離されたネットワークに保存することや、バックアップを取得する媒体を物理的な媒体に保存するなど検討するとよい。

さらに、情報システムを運用していく中で構成が変更になることや、当該情報システムを利用して行う業務が変化するなどの可能性もあるため、運用時に定めているバックアップの要件は必要に応じて適時見直しを行う必要がある。

- **基本対策事項 5.2.3(1)-7 b)「情報システムが停止した際の復旧手順の確認による見直し」について**

情報システムが停止した際の復旧手順を作成してから時間が経つと情報システムの構成を変更することや、当該情報システムを利用して行う業務が変化するなどし、有効でなくなる可能性がある。そのため、情報システムの構成や設定の変更等が行われた際及び定期的に、復旧手順の確認をする必要がある。さらに、復旧手順の確認によって不具合が発見された場合は、復旧手順の見直しを行う必要もある。なお、情報システムの運用継続計画において危機的事象発生時の訓練において、復旧手順の不具合等が発見された場合も同様に見直しを行う必要がある。

復旧手順の確認の仕方については、机上における確認の他、実機を用いた確認などの

方法があり、どのような手段を用いて確認するかは、当該情報システムにおける RTO（目標復旧時間）、RLO（目標復旧レベル）や復旧手順を整備してからの経過時間、復旧に係る訓練の度合い等を踏まえて決めるとよい。

5.2.4 情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

(1) 情報システムの更改・廃棄時の対策

(a) 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下を全て含む措置を適切に講ずること。

(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策

(イ) 情報システム廃棄時の不要な情報の抹消

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.4(1)(a)(ア)「情報の移行」について**

情報システムを更改する際は、更改元の情報システムから更改先の情報システムに情報（本番データ）を移行する作業が発生する場合が多いが、移行作業の過程で情報が外部に漏えいすることのないよう、移行用の本番データを適切に管理する必要がある。移行用の本番データの管理手順や外部電磁的記録媒体を使用する場合の安全管理措置等をあらかじめ定めておくとよい。移行作業を業務委託する場合においては、委託先と事前に手順について合意し、調達仕様書に明記する必要がある。

- **遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について**

情報システムの廃棄を行う場合には、情報システムを構成する機器等並びに内部に保存されている情報の格付及び取扱制限を考慮して、適切に抹消する必要がある。要機密情報を保存している情報システムにおいては、情報の抹消が求められる。廃棄の際に本条を考慮すべき機器等としては、サーバ装置や端末以外にも、複合機等の内蔵電磁的記録媒体を備えた機器については同様に考慮する必要がある。第 6 部において機器ごとの廃棄時の対応を規定しているので、併せて考慮されたい。

なお、情報システムの廃棄を業務委託する際は、委託先において情報の抹消が適切に実施されるよう、遵守事項 3.1.1(7)の規定も参考に、抹消方法等について調達仕様書等に明記し事前に合意する必要がある。委託先の抹消作業に関する作業完了届（廃棄したことが証明されるもの）等を書面で受け取るなどして、確実に抹消作業が行われたこと

を確認する必要がある。例えば、抹消作業前には、抹消する個々の記録媒体のユニークな番号（シリアル番号等）を記録し、いつ、誰によって、先の記録媒体の抹消作業が行われたのか等の作業履歴を作業完了届等で把握することが考えられる。

5.2.5 情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策の定期的な確認による見直しや、外部環境の急激な変化等が発生した場合の適時確認を行うことによる見直しが必要となる。また、運用時における定期的な情報セキュリティ対策の確認による見直しの他、対策推進計画に基づく情報セキュリティ対策の見直しや自己点検・監査、本部監査等の結果等を踏まえた機関等内で横断的に改善が必要となる情報セキュリティ対策についての見直しも併せて実施する必要がある。

遵守事項

(1) 情報システムについての対策の見直し

(a) 情報システムセキュリティ責任者は、対策推進計画に基づき情報システムの情報セキュリティ対策を適切に見直すこと。

(b) 情報システムセキュリティ責任者は、機関等内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直すこと。また、措置の結果については、統括情報セキュリティ責任者へ報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.5(1)(a)「対策推進計画に基づき情報システムのセキュリティ対策を適切に見直す」について**

  基本対策事項 2.1.3(4)-1 d)において定めた対策推進計画の情報システムに関する技術的な対策を推進するための取組に基づき、情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を見直す必要がある。当該取組については、組織全体として取り組む対策、脆弱性検査や注意喚起等において明らかとなった課題への対応、セキュリティ強化が必要と判断する情報システムへの対応などが策定されており、当該計画に基づき継続的かつ計画的に情報システムの情報セキュリティ対策の見直しを実施する必要がある。

- **遵守事項 5.2.5(1)(b)「改善指示に基づき、情報セキュリティ対策を適切に見直す」について**

  遵守事項 2.4.1(2)(c)において、統括情報セキュリティ責任者が改善の必要があると判断した措置の改善指示に基づき、情報システムセキュリティ責任者は所管する情報システムの情報セキュリティ対策を見直し、措置を講ずる必要がある。また、措置の結果については、統括情報セキュリティ責任者に報告する必要がある。

5.3 情報システムの運用継続計画

5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、地震、火災、感染症、情報セキュリティインシデント等の危機的事象発生時でも継続させる必要があり、国の行政機関においては、府省業務継続計画と情報システム運用継続計画を策定し運用している。独立行政法人及び指定法人においても、業務の特性に応じて、中期目標による指示等により、法人の業務継続計画と情報システムの運用継続計画を策定し運用している。

危機的事象発生時に情報システムの運用を継続させるためには、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を検討し、定めることが重要となる。

なお、こうした業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 統括情報セキュリティ責任者は、機関等において非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討すること。

(b) 統括情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であるかを定期的に確認すること。

(c) 統括情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直すこと。

【 基本対策事項 】

＜5.3.1(1)(a)関連＞

5.3.1(1)-1 統括情報セキュリティ責任者は、機関等の情報システムが、政府業務継続計画（首都直下地震対策）（平成 26 年３月閣議決定。以下「政府業務継続計画」という。）において情報システムの運用継続計画を整備することとされている非常時優先業務等を支える情報システムに該当するか、また、該当する場合には、当該情報システムについて、情報システムの運用継続計画が整備されているかを確認すること。

＜5.3.1(1)(b)関連＞

5.3.1(1)-2 統括情報セキュリティ責任者は、危機的事象発生時における情報セキュリティに係る対策事項及び運用規程が運用可能であるかを確認するため、以下を例とする訓練の実施を検討すること。

a) 情報システム復旧訓練

b) 情報システム切り替え訓練

5.3.1(1)-3 統括情報セキュリティ責任者は、危機的事象発生時における情報セキュリティに係る実施手順が運用可能であるかを確認するため、以下を例とする訓練の実施を検討すること。

a) 手順書確認訓練

b) シナリオ非提示型訓練

＜5.3.1(1)(c)関連＞

5.3.1(1)-4 統括情報セキュリティ責任者は、以下を全て含む事項を踏まえ、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を見直すこと。

a) 危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であるかの確認結果

b) 危機的事象発生時の対処結果

c) 情報システムの構成や利用環境、利用方法、取り扱う情報の変化

（解説）

- **遵守事項 5.3.1(1)(a)「非常時優先業務」について**

政府業務継続計画では、首都直下地震発生時に優先的に実施する業務を「非常時優先業務」とし、非常時優先業務を遂行するために必要な組織管理、庁舎管理等の事務を「管理事務」としている。非常時優先業務及び管理事務に位置付ける業務については、中央省庁業務継続ガイドライン 第３版（首都直下地震対策）等を参考にするとよい。

また、本款では、不正プログラム感染やサービス不能攻撃による情報セキュリティインシデントなど情報システム特有の危機的事象等の発生時に優先的に実施する業務を行う必要がある場合には、当該業務も非常時優先業務として取り扱うことが求められる。

独立行政法人及び指定法人においても、法人の特性に応じて、災害等の発生時に優先的に実施する業務を非常時優先業務とする必要がある。

参考：内閣府（防災担当）「国の業務継続計画」
（https://www.bousai.go.jp/taisaku/chuogyoumukeizoku/）

- **遵守事項 5.3.1(1)(a)「情報システムの運用継続計画を整備」について**

機関等における情報システム運用継続計画は、下表のプロセスで検討・整備される。詳細は、内閣官房国家サイバー統括室「政府機関等における情報システム運用継続計画ガイドライン」を参照すること。

検討作業名			検討作業の概要
1	基本方針の決定		計画の適用範囲及び基本方針を定める。
2	策定・運用体制の構築		計画の策定・運用に係る体制を構築する。
3	危機的事象の特定		計画の対象とする危機的事象を調査・検討し、特定する。
4	被害想定		危機的事象が発生した場合の情報システムの被害状況を想定する。
5	情報システムの復旧優先度の設定		
	①	非常時優先業務と情報システムの関連整理	非常時優先業務を確認した上で、対象の情報システムとの関連性を整理する。
	②	情報システムの復旧優先度の設定	非常時優先業務の目標復旧時間と、情報システム停止時の影響や代替手段を踏まえ、情報システムの復旧優先度を設定する。
6	情報システム運用継続に必要な構成要素の整理		
	①	情報システムを支える構成要素の明確化	危機的事象発生時に必要な情報システムを支える構成要素を整理する。
	②	情報システムを支える構成要素ごとの目標対策レベルの設定	情報システムを支える構成要素ごとに、情報システムの復旧優先度に応じた目標対策レベルを設定する。
7	事前対策の計画とその実施		
	①	現状の対策の確認及びリスクの評価	情報システムの構成要素ごとに、現状の対策を確認し、リスクの評価を実施し、情報システムの運用継続に係るリスクを整理する。
	②	事前対策計画の策定とその実施	リスクの評価を踏まえ、情報システムの継続能力を強化する「事前対策計画」を作成する。
8	危機的事象発生時の対応計画の検討		
	①	危機的事象発生時の体制構築	危機的事象発生時に情報システムの運用を継続させるために必要となる体制・役割を決定する。
	②	危機的事象発生時における対応計画	情報システムの運用を継続させる具体的な対応方法を対応計画として整理する。
9	教育訓練・維持改善の計画とその実施		
	①	教育訓練の計画とその実施	事前対策や危機的事象発生時の対応計画の実効性を高めるための「教育訓練計画」を作成する。
	②	維持改善の計画とその実施	情報システム運用継続計画を定期的に見直すための「維持改善計画」を作成する。

参考：内閣官房国家サイバー統括室「政府機関等における情報システム運用継続計画ガイドライン」
（https://www.cyber.go.jp/policy/group/general/itbcp-guideline.html）

- **遵守事項 5.3.1(1)(a)「危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順」について**

情報システムの運用継続を脅かす危機的事象の例として、地震、風水害等の自然災害、

火災等の人的災害・事故、停電等の社会インフラの不全、不正アクセス等の運用妨害、機器等の故障、感染症の流行による影響等が想定される。これらの危機的事象発生時に対して、業務継続計画、情報システムの運用継続計画及び情報セキュリティ関係規程のそれぞれで定める対策に矛盾があると、危機的事象発生時に職員等は一貫性のある行動をとることができない。このため、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を検討する際は、業務継続計画及び情報システムの運用継続計画と情報セキュリティ関係規程との間で整合性を確保するよう検討する必要がある。

検討が必要な対策事項、運用規程及び実施手順の例を以下に示す。なお、具体的な内容については、「政府機関等における情報システム運用継続計画ガイドライン」を参照のこと。

- 対応体制及び連絡方法に係わる対策
- 電力に係わる対策
- 空調に係わる対策
- ネットワークに係わる対策
- ハードウェア及びソフトウェアに係わる対策
- バックアップ及び復旧に係わる対策
- クラウドサービスの利用に係わる対策
- 業務継続のためにやむを得ず、以下を利用する場合の対策
  - 機関等支給以外の端末
  - 自身に付与された以外の識別コード及び主体認証情報。例えば、通常時用とは別に危機的事象発生時用の識別コード及び主体認証情報を設定し、その識別コード及びパスワードを記載した紙面を施錠された安全な保管場所に保管する。また、保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用する対策が考えられる。
- 機関等の施設の一部に帰宅困難者等を受け入れる場合の対策
  - 例えば、各執務室や各職員等の卓上の情報セキュリティ対策を含め、通常時から不特定の者の出入りを想定した対策を講ずることが考えられる。

- **遵守事項 5.3.1(1)(b)「運用可能であるかを定期的に確認」について**

情報システムの運用継続を脅かす危機的事象発生時においては、危機的事象発生時の情報セキュリティに係る対策事項、運用規程及び実施手順を整備した際には想定していなかった様々な不整合が発生し、整備した対策事項、運用規程及び実施手順が有効に機能しないことも考えられる。このため、訓練を実施することによって、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が有効に機能することを確認することが重要である。

訓練においては様々な実施内容が考えられる。実施内容については、訓練の初期段階では容易な内容とし、職員等の習熟度等に応じて、段階的に高度な内容へ引き上げるとよい。また、危機的事象発生時は訓練で扱ったとおりの事態が発生するとは限らないため、実施内容は可能な限り高度化し、どのような事態が発生しても対応できるように備

えるとよい。

なお、情報システムの運用継続計画の教育訓練を行う際は、危機的事象発生時の対策事項、運用規程及び実施手順の理解と対応能力の向上の他、対策事項、運用規程及び実施手順の有効性の確認も目的とすることが望ましい。

- **遵守事項 5.3.1(1)(c)「定期的に見直す」について**

危機的事象発生時の情報セキュリティに係る対策事項、運用規程及び実施手順の実効性の維持又は向上を図るため、定期的な見直し以外に、基本対策事項 5.3.1(1)-3 に示した事項の結果が示された場合等が発生した際に適時見直しを行うことが望ましい。

- **基本対策事項 5.3.1(1)-1「政府業務継続計画において情報システムの運用継続計画を整備することとされている非常時優先業務等を支える情報システムに該当するか、また、該当する場合には、当該情報システムについて、情報システムの運用継続計画が整備されているかを確認」について**

情報システムの運用継続計画については、危機的事象発生時においても非常時優先業務等を継続させるために、当該非常時優先業務等を支える情報システムについて整備することとされている。危機的事象の中には、不正プログラム感染やサービス不能攻撃による情報セキュリティインシデントなど情報システム特有の事象も対象として含まれる。統括情報セキュリティ責任者は、こうした情報システム特有の危機的事象発生時において早期に復旧させ継続して利用するために情報システムの運用継続計画を策定することが必要な情報システムであるとして、当該情報システムが非常時優先業務等を支える情報システムに該当すべきものかどうかについて、機関等の情報セキュリティ対策の責任者の立場から確認することが求められる。また、当該情報システムが非常時優先業務等を支える情報システムに該当すべきものである場合、情報システムの運用継続計画が整備されているかを確認し、整備されていない場合には、情報システムの運用を継続する最高責任者（各機関等において情報システム運用継続計画の策定・運用全般を統括し、最終的な責任を負う者）に対して、当該情報システムに係る情報システムの運用継続計画の整備を要請する等の対応が求められる。なお、情報システムの運用継続計画の整備対象であるかどうかについては、情報システム台帳等で網羅的に管理することが望ましい。

- **基本対策事項 5.3.1(1)-2 a)「情報システム復旧訓練」について**

実機を使い、情報のバックアップを用いて実際に情報システムを復旧する訓練を想定している。

当該訓練の初期段階では、情報のバックアップの一部を用い、情報システムの一部を復旧する訓練を実施するとよい。その後、職員等の習熟度等に応じて、情報のバックアップの全てを用い、情報システムを完全に復旧する訓練を実施する等、段階的に高度化するとよい。

- **基本対策事項 5.3.1(1)-2 b)「情報システム切り替え訓練」について**

代替機が存在する場合に、本番機から代替機への切り替えが実際に可能か確認する訓練を想定している。また、代替機から本番機への切り戻しも併せて確認することが望

ましい。

- **基本対策事項 5.3.1(1)-3 a)「手順書確認訓練」について**

  危機的事象発生時における情報セキュリティに係る実施手順書を読み合わせ、関係者間で危機的事象発生時における役割や行動について机上で確認する訓練を想定している。

  危機的事象発生時における情報セキュリティに係る実施手順が適切に機能することの確認においては、本基本対策事項を優先的に実施し、職員等の習熟度等に応じて、段階的にシナリオ非提示型訓練等の高度な訓練を実施するとよい。

- **基本対策事項 5.3.1(1)-3 b)「シナリオ非提示型訓練」について**

  訓練前に訓練シナリオを参加者に通知せず、訓練開始時に危機的事象発生時における被害状況のみを参加者に提示し、参加者に対応させる訓練を想定している。

5.4 政府共通利用型システム

5.4.1 政府共通利用型システム管理機関における対策

目的・趣旨

政府共通利用型システムは、政府共通利用型システムの管理機関と利用機関が連携して運用するものであることから、機関等の間で情報セキュリティ対策の漏れが生じないようその防止を図る必要がある。また、政府共通利用型システムを利用する一部の情報システムで情報セキュリティインシデントが生じた場合に同システムを利用する他の情報システムにも影響が及ぶ可能性等も踏まえ、政府共通利用型システムの管理機関は、政府共通利用型システム全体としての情報セキュリティマネジメントを適切に実行し、情報セキュリティ水準を適切に確保する必要がある。

このため、両機関の責任と役割分担を明確化し、情報セキュリティインシデントを認知時にこれに係る対処を連携して迅速・確実に実施できる体制にする必要がある。

遵守事項

(1) 情報セキュリティ対策に関する運用管理規程の整備

(a) 情報システムセキュリティ責任者は、政府共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用管理規程を整備し、政府共通利用型システム利用機関と十分な合意形成を行うこと。

(ア) 政府共通利用型システム管理機関と政府共通利用型システム利用機関との間の責任分界

(イ) 平常時及び非常時の協力・連携体制

(ウ) 非常時の具体的対応策

【 基本対策事項 】

＜5.4.1(1)(a)関連＞

5.4.1(1)-1 情報システムセキュリティ責任者は、政府共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用管理規程を定めること。

a) 政府共通利用型システム管理機関と政府共通利用型システム利用機関がそれぞれ責任を追うべき情報セキュリティ対策の責任分界点

b) 政府共通利用型システム及び政府共通利用型システム利用機関の情報システムにおける情報セキュリティインシデントを認知した場合の、政府共通利用型システム管理機関と政府共通利用型システム利用機関の間の情報共有や対処の方法を含む対処手順

c) 政府共通利用型システム利用機関が確保するべき管理体制や整備するべき運用規程及び実施手順

d) 政府共通利用型システムが提供するセキュリティ機能を利用する情報システムが備えるべきセキュリティ要件

e) 政府共通利用型システムが提供する機器等を利用する職員等への識別コード及

び主体認証情報の付与や管理に関する手順並びにアクセスの権限の設定に関する手順

（解説）

- **遵守事項 5.4.1(1)(a)「政府共通利用型システム」について**

統一基準 1.3「用語定義」における「政府共通利用型システム」の用語定義のとおり、政府共通利用型システムには、他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システムと、他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムがある。このうち、セキュリティ機能を提供する政府共通利用型システムついては、統一基準 7.1「情報システムのセキュリティ機能」で対策を規定する各機能のいずれかの機能を提供する情報システムが該当すると考えられる。

なお、「統一基準」の対象ではない組織のみにセキュリティ機能を提供する情報システムについては政府共通利用型システムに該当しないが、セキュリティ機能の提供先の組織や当該情報システムの特性等を踏まえて、本款の規定を参考として対策を講ずることが望ましい。

- **遵守事項 5.4.1(1)(a)「情報セキュリティ対策に関する運用管理規程」について**

この運用管理規程は、遵守事項 2.1.3(3)(a)で整備する機関等の情報セキュリティ対策に関する運用規程及び実施手順ではなく、政府共通利用型システム管理機関と政府共通利用型システム利用機関の双方が政府共通利用型システムの情報セキュリティ対策に関する共通認識を持つために必要な文書を想定している。

（以下、本節において単に「運用管理規程」と記載した場合は、これを示すものとする。）

- **遵守事項 5.4.1(1)(a)「十分な合意形成を行う」について**

政府共通利用型システムにおける情報セキュリティ対策に関する運用管理規程の整備に当たっては、政府共通利用型システム管理機関と政府共通利用型システム利用機関との十分な合意形成を行う必要があるが、当該運用管理規程の整備後に新たに政府共通利用型システムの利用を検討する機関等は、すでに定められている当該運用管理規程を理解した上で、政府共通利用型システムの利用を決定することが求められる。また、新たに政府共通利用型システムを利用する機関等との協議により、運用管理規程の修正が必要となった場合は、他の政府共通利用型システム利用機関の同意も必要となる。

- **遵守事項 5.4.1(1)(a)(イ)「非常時の協力・連携体制」について**

非常時とは、情報セキュリティインシデントや政府共通利用型システムの障害等により、政府共通利用型システム自体やセキュリティ機能を提供できなくなった場合が考えられる。このような場合に、政府共通利用型システム管理機関から政府共通利用型システム利用機関に速やかに情報提供できる体制を確保することが求められる。

- **基本対策事項 5.4.1(1)-1 a)「情報セキュリティ対策の責任分界点」について**

  統一基準各部で情報システムセキュリティ責任者が実施することを求めている対策については、政府共通利用型システムにおいても同じであるが、政府共通利用型システム利用機関においても一部実施すべき対策がある場合は、その実施の責任範囲を運用管理規程に明記し、利用機関と事前に合意する必要がある。例えば、遵守事項 6.1.1(1)(a)の端末を物理的な脅威から保護するための対策や遵守事項 8.1.3(3)(a)のテレワーク実施時における対策等については、政府共通利用型システム利用機関において実施する場合があることが想定される。

- **基本対策事項 5.4.1(1)-1 b)「政府共通利用型システム利用機関の情報システムにおける情報セキュリティインシデント」について**

  政府共通利用型システムが提供するセキュリティ機能を利用した情報システムにおける情報セキュリティインシデントを想定している。

- **基本対策事項 5.4.1(1)-1 c)「政府共通利用型システム利用機関が確保するべき管理体制や整備するべき運用規程及び実施手順」について**

  政府共通利用型システム利用機関において、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合に、政府共通利用型システムとの連携に係る調整等を政府共通利用型システム管理機関と行うために必要な体制や手順、セキュリティ機能の仕様変更等の連絡を速やかに受けるために必要な体制や手順等が考えられる。

- **基本対策事項 5.4.1(1)-1 d)「備えるべきセキュリティ要件」について**

  政府共通利用型システムが提供するセキュリティ機能の利用に際し、政府共通利用型システムのセキュリティ水準を低下させないために必要なセキュリティ要件等が考えられる。

- **基本対策事項 5.4.1(1)-1 e)「識別コード及び主体認証情報の付与や管理に関する手順並びにアクセスの権限の設定に関する手順」について**

  政府共通利用型システム管理機関が実施する場合を除き、政府共通利用型システム利用機関は当該手順に基づき、実施手順を定め、識別コード及び主体認証情報の付与や管理、アクセスの権限の設定を行う必要がある。

  なお、政府共通利用型システム利用機関において定める実施手順については、基本対策事項 5.4.2(3)-1 を参照のこと。

遵守事項

(2) 情報システム台帳及び情報システム関連文書の整備

(a) 政府共通利用型システム管理機関の統括情報セキュリティ責任者は、遵守事項2.1.2(1)(a)で整備する政府共通利用型システムに関する情報システム台帳について、政府共通利用型システム利用機関に関係するセキュリティ要件に係る事項を含めて整備すること。

(b) 政府共通利用型システム管理機関の情報システムセキュリティ責任者は、遵守事項5.2.2(1)(d)で整備する政府共通利用型システムに関する情報システム関連文書について、**政府共通利用型システム利用機関に関係する情報**を含めて整備すること。

【 基本対策事項 】

＜5.4.1(2)(a)関連＞

5.4.1(2)-1 政府共通利用型システム管理機関の統括情報セキュリティ責任者は、セキュリティ機能を提供する政府共通利用型システムに関する情報システム台帳について、以下の内容を全て含めて整備すること。

a) 当該政府共通利用型システムが提供するセキュリティ機能を利用する情報システム名
b) 上記情報システムの政府共通利用型システム利用機関名及び管理課室
c) 上記情報システムの情報システムセキュリティ責任者の氏名及び連絡先
d) 上記情報システムの利用目的

5.4.1(2)-2 政府共通利用型システム管理機関の統括情報セキュリティ責任者は、機器等を提供する政府共通利用型システムに関する情報システム台帳について、以下の内容を全て含めて整備すること。

a) 当該政府共通利用型システムが提供する機器等を利用する政府共通利用型システム利用機関名
b) 上記利用機関における当該政府共通利用型システム利用管理者の氏名及び連絡先
c) 上記利用機関において当該政府共通利用型システムで取り扱う**情報の格付及び取扱制限に関する事項**

＜5.4.1(2)(b)関連＞

5.4.1(2)-3 政府共通利用型システム管理機関の情報システムセキュリティ責任者は、政府共通利用型システムに関する情報システム関連文書のうち、政府共通利用型システム利用機関に提供した機器等に係る情報については、政府共通利用型システム利用機関の求めに応じ、必要な範囲で提供すること。

（解説）

- **遵守事項 5.4.1(2)(b)「政府共通利用型システム利用機関に関係する情報」について**

掲載すべき政府共通利用型システム利用機関に関係する情報としては、政府共通利

用型システム利用機関に端末などの機器等を提供して利用をさせている場合に、当該機器等に関する情報が考えられる。

- **基本対策事項 5.4.1(2)-2 c)「情報の格付及び取扱制限に関する事項」について**

  適切に情報セキュリティインシデント対処を行うためには、政府共通利用型システム管理機関においても、政府共通利用型システム利用機関が取り扱う情報の格付や取扱制限を把握する必要があるが、これらの事項が詳細に至る場合は、管理機関における把握は概要とし、詳細は利用機関で管理することも考えられる。この場合、情報セキュリティインシデント対処時には速やかに管理機関と詳細が共有される必要がある。

5.4.2 政府共通利用型システム利用機関における対策

目的・趣旨

政府共通利用型システム利用機関は、政府共通利用型システム管理機関が定める運用管理規程に基づき必要な体制を確保すると共に、責任と役割分担を踏まえ、適切に利用する必要がある。また、情報セキュリティインシデントを認知した際の対処においては両機関の協力が必要となることから、管理機関が定める運用管理規程に基づき情報セキュリティインシデントを認知した際の両機関の責任と役割分担を明確にしておき、対処に必要となる情報は両機関で共有されている状態にしておくことが重要である。

遵守事項

(1) 政府共通利用型システム利用機関における体制の整備

(a) 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を、最高情報セキュリティ責任者に求めること。

(b) 統括情報セキュリティ責任者は、政府共通利用型システムが提供する機器等の提供を受けこれを自機関等の職員等が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに**政府共通利用型システム利用管理者**を指名すること。

(c) 政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を、最高情報セキュリティ責任者に求めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.4.2(1)(b)「政府共通利用型システム利用管理者」について**

政府共通利用型システムの情報システムセキュリティ責任者は管理機関にて設置するものであるが、その実施すべき対策のうち、運用管理規程で定められた責任分界の範囲において、利用機関においても実施すべき対策がある場合は、利用機関に設置する政府共通利用型システム利用管理者が実施する必要がある。

遵守事項

(2) 政府共通利用型システム利用機関における情報セキュリティ対策

(a) 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムの情報セキュリティ水準を低下させることのないように、適切にセキュリティ要件を策定し、運用すること。

(b) 情報システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.4.2(2)(a)「セキュリティ機能を利用する情報システム」について**

  政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築、運用する場合は、当該情報システムに対しては、政府共通利用型システムの情報セキュリティ水準を低下させることのないように、適切にセキュリティ要件を策定し、運用するとともに、併せて 5.2「情報システムのライフサイクルの各段階における対策」も実施する必要がある。

遵守事項

(3) 政府共通利用型システム利用機関における機器等の管理

(a) 政府共通利用型システム利用管理者は、政府共通利用型システムが提供する機器等の提供を受けてこれを自機関等の職員等が利用する場合は、当該政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程及び実施手順を整備すること。

(b) 政府共通利用型システム利用管理者は、**提供を受けた政府共通利用型システムの機器等を把握するために必要な文書**を整備すること。

(c) 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、政府共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知すること。

(d) 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。

【 基本対策事項 】

＜5.4.2(3)(a)関連＞

5.4.2(3)-1 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程を踏まえ、以下の内容を全て含む情報セキュリティ対策に係る運用規程及び実施手順を定めること。

a) 政府共通利用型システムが提供する機能のうち、**自機関で利用を認める機能**

b) 政府共通利用型システムが提供する端末で**利用を認めるソフトウェア**や接続を認める機器等

c) 政府共通利用型システムにおける情報セキュリティインシデントの可能性を認知した場合の報告手順及び対処手順

d) 政府共通利用型システムにおける**業務委託サービスやクラウドサービスの利用申請**の手順

e) 政府共通利用型システムを利用する職員等への識別コードや主体認証情報の付与、アクセス権限の設定等に関する手順。ただし、政府共通利用型システム利用機関において識別コードや主体認証情報の付与、アクセス権限の設定等を行わない場合は除く。

f) **政府共通利用型システム利用機関における機器等のキッティングファイルの管理手順**

g) 前各号に掲げるもののほか、政府共通利用型システム利用機関における政府共通利用型システムの利用に係る情報セキュリティ対策に関する事項

5.4.2(3)-2 政府共通利用型システム利用管理者は、自機関の対策基準や取り扱う情報の格付等を踏まえ、政府共通利用型システムに追加のセキュリティ対策を行う必要があると認める場合は、政府共通利用型システムにおける当該**セキュリティ対策の追加的実**

施その他の措置について協議すること。

＜5.4.2(3)(b)関連＞

5.4.2(3)-3 政府共通利用型システム利用管理者は、自機関に設置している政府共通利用型システムの機器等を把握するため、以下の内容を全て含む文書を整備すること。

a) 当該機器等を管理又は利用する職員等を特定する情報

b) 当該機器等の設置場所並びにその区域のクラス及び当該設置場所の区域情報セキュリティ責任者

（解説）

- **遵守事項 5.4.2(3)(b)「提供を受けた政府共通利用型システムの機器等を把握するために必要な文書」について**

提供を受けた政府共通利用型システムの機器等を把握するために必要な文書の整備に当たっては、必要な範囲で、政府共通利用型システム管理機関が整備している情報システム関連文書の提供を受けるとよい。

- **基本対策事項 5.4.2(3)-1 a)「自機関で利用を認める機能」について**

政府共通利用型システムが提供する機能のうち、自機関で利用を認める機能については、政府共通利用型システム管理機関から提供される当該機能に講じられている情報セキュリティ対策などを確認し、当該機能で取り扱う情報等や自機関のポリシーの内容を踏まえて定める必要がある。

- **基本対策事項 5.4.2(3)-1 b)「利用を認めるソフトウェア」について**

政府共通利用型システムが標準で提供していないソフトウェアについては、遵守事項7.2.1(1)で対策を講ずることを求めている当該ソフトウェアに関する脆弱性対策が情報システムセキュリティ責任者によって実施されない可能性があるため、当該ソフトウェアの利用を認めるに当たっては、政府共通利用型システム管理機関が定める運用管理規程における責任分界に基づき、それらの対策の実施責任を事前に明確にする必要がある。

- **基本対策事項 5.4.2(3)-1 d)「業務委託サービスやクラウドサービスの利用申請」について**

政府共通利用型システムが標準で提供していない業務委託サービスやクラウドサービスを想定している。これらのサービスを利用する場合の申請や承認の手順について、政府共通利用型システム管理機関が定める運用管理規程に基づき定める必要がある。

- **基本対策事項 5.4.2(3)-1 f)「政府共通利用型システム利用機関における機器等のキッティングファイルの管理手順」について**

キッティングファイル(機器等を業務利用できる状態にするためのファイルのこと。)が最新のものとなっていない又は意図せず改変・改造された場合、キッティングに支障が生じるだけでなく、重大な情報セキュリティインシデントが発生するおそれがある。そのため、キッティングファイルは、常に最新の状態に保つとともに、使用する外部記

録媒体も含めて厳格に管理することが求められる。

- **基本対策事項 5.4.2(3)-2「セキュリティ対策の追加的実施その他の措置」について**

  政府共通利用型システム利用管理者が政府共通利用型システム管理機関と追加的実施を協議するセキュリティ対策としては、例えば、第 6 部や第 7 部で規定する各セキュリティ対策や、遵守事項 8.1.1(2)(a)で規定する職員等による規定の遵守を支援する機能の導入等が考えられる。

  なお、セキュティ対策の追加的実施について、政府共通利用型システム管理機関との協議の結果困難である場合、利用機関において講ずる代替措置の検討や取り扱う情報の見直し等を行い、運用規程及び実施手順に反映する必要がある。

第6部 情報システムの構成要素

6.1 端末

6.1.1 端末

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等に注意する必要がある。また、職員等の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。これらのリスクを考慮し職員等が利用する端末については適切なセキュリティ対策を講ずるとともに、利用を認めるソフトウェアや接続を認める機器等を定めておくことが重要である。また、物理的な端末のモバイル利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、6.4.4「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(1) 端末の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う物理的な端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で**利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない**こと。

(c) 情報システムセキュリティ責任者は、端末に**接続を認める機器等を定め、接続を認めた機器等以外は接続させない**こと。

(d) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した内容に従い、端末に対して**適切なセキュリティ対策を実施する**こと。

(e) 情報システムセキュリティ責任者は、端末において利用する**ソフトウェアに関連する公開された脆弱性について対策を実施する**こと。

【 基本対策事項 】

＜6.1.1(1)(a)関連＞

6.1.1(1)-1 情報システムセキュリティ責任者は、モバイル端末を除く物理的な端末について、**原則としてクラス２以上の要管理対策区域に設置する**こと。

6.1.1(1)-2 情報システムセキュリティ責任者は、物理的な端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定すること。

b) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意すること。

6.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずること。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定すること。

b) 不特定多数の人が出入りする場所で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付けること。

＜6.1.1(1)(b)関連＞

6.1.1(1)-4 情報システムセキュリティ責任者は、以下の全てを考慮した上で、端末で利用を認めるソフトウェアをバージョンも含め定めること。なお、特定の業務や端末のみに利用を認めるなどの条件を付す場合は、その旨を含めること。

a) ソフトウェアベンダ等のサポート状況

b) ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む。）、使用するポート、暗号化の有無

c) インストール時に同時にインストールされる他のソフトウェア

d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

6.1.1(1)-5 情報システムセキュリティ責任者は、端末に対して、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講ずること。

（解説）

- **遵守事項 6.1.1(1)(b)「利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない」について**

利用を認めるソフトウェアのリストには、市販のアプリケーションに限らず、リモートデスクトップやファイル共有サービス等の特定のポート番号を利用する OS が備えているサービス等も登録する必要がある。また、情報セキュリティリスクを低減する観点から、利用を認めるソフトウェアは極力限定することが重要である。そのため、特定の業務で利用することを条件として利用を認める場合や、特定の端末でのみ利用を認める場合等、利用を認めるソフトウェアを条件を付した状態でリストに登録する場合は、その旨を含めて登録する必要がある。

なお、リストに登録する単位については、ソフトウェアの個別の製品名やバージョン単位で列挙すると分かりやすいが、頻繁にアップデートをする必要がある製品についてはバージョンを最新版とする運用が考えられる。

- **遵守事項 6.1.1(1)(c)「接続を認める機器等を定め、接続を認めた機器等以外は接続させ**

ない」について

接続を認める機器等については、例えばUSBポートに接続するキーボードやマウス、ヘッドホンなどが考えられるが、端末を利用して行う業務等を踏まえて定めるとよい。また、外部電磁的記録媒体については、組織で認めたもの以外の接続を制限するなども考えられる。さらに、出所が不明なUSBデバイスについては、不正プログラムが組み込まれたBadUSBと呼ばれる攻撃が存在するため、接続を制限するとよい。

- **遵守事項 6.1.1(1)(d)「適切なセキュリティ対策を実施する」について**

端末を導入する際は、セキュリティ要件に従って適切なセキュリティ対策を実施する必要がある。例えば、端末を利用する際の主体認証方式や情報の暗号化等の情報セキュリティ機能が正しく実装されていることや脆弱性対策、不正プログラム対策等を実施する必要がある。また、端末において不要なポートやプロトコルが有効になっていないことを確認することや一定の無通信時間が経過した場合は当該通信セッションに係る通信を遮断する、不要な機能は無効にするなどの対策も重要である。

- **遵守事項 6.1.1(1)(e)「ソフトウェアに関連する公開された脆弱性について対策を実施する」について**

職員等が端末を利用する前に端末で利用するソフトウェアに関連する脆弱性情報を確認し、脆弱性が公開されていた場合は、セキュリティパッチを適用するなどの対策を実施する必要がある。

ソフトウェアの脆弱性については、7.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

- **基本対策事項 6.1.1(1)-1「原則としてクラス２以上の要管理対策区域に設置する」について**

クラス２より低位の区域に設置する必要がある場合は、利用者が常時監視できる場所への設置を義務付けるなど、クラス２の区域に設置する場合と同程度の安全性を確保するための代替の対策を講ずる。

- **基本対策事項 6.1.1(1)-2「物理的な端末の盗難及び不正な持ち出しを防止」について**

モバイル端末を除く物理的な端末については、設置する場所によっては、ハードディスク等の電磁的記録媒体の盗難についても注意が必要である。そのような端末においては筐体を施錠する等の対策も検討するとよい。また、モバイル端末については紛失した際のリスクを軽減するため、ハードディスク等の電磁的記録媒体を暗号化するなどの措置を講ずる等の対策も検討するとよい。

- **基本対策事項 6.1.1(1)-3「第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずる」について**

第三者による不正操作等の防止のための対策事項であるが、その他、端末の操作のロックの解除にICカード等の主体認証情報格納装置を使用し、主体認証情報格納装置

が無い状態で又は操作の無い状態が一定時間続くことで端末の操作がロックされるようにし、かつ、当該主体認証情報格納装置を執務室からの退出の確認にも利用するという方法が考えられる（これにより、利用者が執務室外にいる際には端末の操作が確実にロックできる）。

また、正規の利用者による不正操作や誤操作の防止策として、端末が備える機能のうち、利用しない機能を停止することが考えられる。停止する機能の例としては、以下が考えられる。

- 無線 LAN 等の通信用のインタフェース
- USB ポート等の外部電磁的記録媒体を接続するためのインタフェース
- マイク、ウェブカメラ（機能として不要な場合）

- **基本対策事項 6.1.1(1)-4「利用を認めるソフトウェアをバージョンも含め定める」について**

利用を認めるソフトウェアを定める際には、以下を行うことが考えられる。

- ソフトウェアベンダによるセキュリティパッチ等のサポートが提供されていることや、セキュリティベンダ等の第三者が提供するソフトウェアの脆弱性等に関する情報を確認する。
- 外部と通信を行う機能を有することが明確なもの又は外部との通信の有無について利用規約により確認できるものについては、当該機能によって使用するプロトコル（バージョンを含む。）、ポート、暗号化の有無を事前に確認する。プロトコルのバージョンについては、TLS などにおいて脆弱なバージョンを使用していないかなども確認する必要がある。
- インストール時に、他のソフトウェアのインストールの同意を求めるものについては、当該ソフトウェアの利用の可否についても併せて定める。
- ブラウザを含め個々のソフトウェアにおける機能拡張用のソフトウェア（いわゆる、プラグインやアドオン）の利用の可否についても併せて定める。

また、一度利用を認めたソフトウェアであっても、バージョンが上がった際に、旧バージョンと比べ、機能が変わることや、同時にインストールされる他のソフトウェアが追加される場合があるので、利用を認めるソフトウェアを定める際には、バージョンも含めて定めることが重要である。

- **基本対策事項 6.1.1(1)-5「端末に対して、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講ずる」について**

端末で利用を認めるソフトウェア以外のソフトウェアについて、職員等の認識不足などにより無断で利用されることを防ぐため、本基本対策事項では、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講ずることを求めている。

技術的な措置としては、以下の例が挙げられる。

- 一般の業務に従事する職員等に対しては、管理者権限を有しない、いわゆる標準ユーザのアカウントのみを付与し、標準ユーザによるソフトウェアのインストールを制限する。

- OS や製品（例えば、MDM（Mobile Device Management）ツールや IT 資産管理ソフトウェア）の機能を用いて、利用を認めるソフトウェアのみが端末にインストール可能となる設定を行う。

遵守事項

(2) 端末の運用時の対策

(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。

(b) 情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

【 基本対策事項 】

＜6.1.1(2)(a)関連＞

6.1.1(2)-1 情報システムセキュリティ責任者は、利用を認めるソフトウェアの定期的な確認においては、引き続き利用を認めるか否かを判断し、利用を認めない場合は利用を認めるソフトウェアから削除すること。

6.1.1(2)-2 情報システムセキュリティ責任者は、利用を認めるソフトウェア以外のソフトウェアについて職員等から利用申請があった場合には、当該ソフトウェアの利用を認めるか否かを判断し、利用を認める場合は利用を認めるソフトウェアに追加すること。

（解説）

- **遵守事項 6.1.1(2)(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、また、利用者の要求に柔軟に対応するため、利用を認めるソフトウェアの確認による見直しを行う必要がある。見直しを行うに当たっては、利用を認めるソフトウェアの必要性や利用を認めることによる脅威へのリスク等を踏まえた上で見直しを行う必要がある。

「定期的」以外の見直しの契機として、職員等から利用を認めるソフトウェア以外のソフトウェアの利用承認の申請（8.1.1「情報システムの利用」を参照のこと。）を受け付けたときが考えられる。申請のあったソフトウェアについて、当該ソフトウェアの必要性や利用目的、取り扱う情報の概要、要機密情報の利用の有無、その他利用することによる脅威へのリスク等を踏まえて、利用を認めるか否かを判断する必要がある。なお、民間事業者等が不特定多数の利用者に対して提供する、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、このようなクラウドサービスの利用に必要なソフトウェア（端末にインストールされるアプリケーションを含む）では、原則として要機密情報を取り扱うことはできない（4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」を参照のこと。）。

特に管理者権限を必要とするソフトウェアや他のソフトウェアを含む機器等の管理や制御を行うソフトウェアの利用を認める場合は、追加のセキュリティ対策を実施させるなど、ソフトウェアを利用することによる脅威へのリスクを低減することが重要

である。

- **遵守事項 6.1.1⑵(b)「不適切な状態にある端末を検出等した場合には、改善を図る」について**

「不適切な状態」とは、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。その他にも不正プログラム対策ソフトウェアのパターン等が最新でない、要機密情報が暗号化されていない、脆弱又は不要なプロトコルやポート、サービスなどが動作している、脆弱な初期の設定値等が是正されていない状態なども改善を図る必要がある。

なお、利用を認めるソフトウェア以外のソフトウェアが稼働している場合には、当該ソフトウェアを停止する、又は削除する必要がある。セキュリティパッチについては、7.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

遵守事項

(3) 端末の運用終了時の対策

(a) 情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.1.1(3)(a)「端末の運用を終了する際」について**

  端末を廃棄処分する場合やリース契約が終了し端末を返却する場合が考えられる。

- **遵守事項 6.1.1(3)(a)「抹消する」について**

  抹消の方法については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」を参照のこと。

  なお、運用を業務委託しているなど、調達元の機関等において抹消できない場合においては、保存されている情報の漏えいが生じないための対策を講じさせるため、情報の抹消方法及び履行状況の確認手段を、契約内容に含むようにするなどの別の手段で対策を講ずる必要がある。

6.1.2 要管理対策区域外での端末利用時の対策

目的・趣旨

テレワークの実施等により、職員等が機関等外で業務を行うことが増え、機関等が支給する物理的な端末を利用して要管理対策区域外で業務を行う場合は、盗み見や盗難・紛失などのリスクが増える。そのようなリスクに対抗するため、要管理対策区域外で機関等が支給する物理的な端末を使用する場合は、利用手順や利用の許可手続等を定め、職員等に守らせる必要がある。また、端末においても盗難、紛失、不正プログラムの感染等による情報窃取を防止するため技術的な措置を講ずる必要がある。

さらに、職員等が機関等外通信回線を用いて情報システムにリモートアクセスをする場合は、リモートアクセス特有の攻撃等に対抗するためのセキュリティ対策を実施する必要がある。リモートアクセスについては、遵守事項 8.1.3(2)を参照のこと。

なお、機関等外通信回線を用いて情報システムにリモートアクセス環境を構築する場合は、情報システムへのアクセスについて初回のアクセス要求時のみ制御を行うのではなく、アクセスの都度信用できるアクセスであるかを検証し、信用できない場合には追加の措置を講ずるなど、アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御を実施することも有効である。動的なアクセス制御については、7.3「ゼロトラストアーキテクチャ」を参照のこと。

遵守事項

(1) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。

(b) 統括情報セキュリティ責任者は、**要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）**について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する運用規程を整備すること。

(c) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する物理的な端末を**機関等内通信回線に接続することについての可否を判断**した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた**技術的な措置に関する運用規程**を定めること。

【 基本対策事項 】

＜6.1.2(1)(a)関連＞

6.1.2(1)-1 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）を用いて要保護情報を取り扱う場合の利用手順

を実施手順として、以下を例として定めること。

a) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化
b) 盗み見に対する対策（のぞき見防止フィルタの利用等）
c) **盗難・紛失に対する対策**（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
d) 利用する場所や時間の限定
e) 端末の盗難・紛失が発生した際の緊急対応手順

6.1.2(1)-2 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）を用いて要保護情報を取り扱う場合について、以下を全て含む許可手続を実施手順として定めること。

a) 利用時の許可申請手続
b) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）
c) **利用期間満了時の手続**
d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

＜6.1.2(1)(b)関連＞

6.1.2(1)-3 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を**暗号化**するための機能を検討し、要管理対策区域外で使用する物理的な端末に求める技術的な措置に関する運用規程を設けること。

a) **シンクライアント等**の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築し、利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスすること。
b) **セキュアブラウザ等**を活用した、端末に情報を保存させないリモートアクセス環境を構築し、利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスすること。
c) **ファイル暗号化等のセキュリティ機能を持つアプリケーション**を導入すること。
d) 端末に、**ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能**を設けること。
e) 上記の各号のいずれの機能も使用できない場合は、端末に**ファイルを暗号化する機能を設ける**こと。
f) ハードディスク等の電磁的記録媒体に保存されている情報を**遠隔からの命令等により暗号化消去する機能**を設けること。
g) **高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等**を使用すること。

＜6.1.2(1)(c)関連＞

6.1.2(1)-4 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線

に接続した機関等が支給する物理的な端末について、機関等内通信回線に接続する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえ、以下を例とする技術的な措置について運用規程として定めること。

a) 機関等内通信回線に接続する前に当該端末に対し、不正プログラム対策ソフトウェアを用いて検査を行うこと。
b) 機関等内通信回線に接続した当該端末が、不正な通信を行っていないか、不要なアプリケーション、サービスやポートを使用していないか確認すること。
c) 技術的な措置において不適切な状態を検知した場合は、機関等内通信回線に接続させない措置を講ずることや、機関等内通信回線から直ちに切断するなどの措置を講ずること。

（解説）

- **遵守事項 6.1.2(1)(b)「要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）」について**

要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る。）とは、モバイル端末が該当する。

- **遵守事項 6.1.2(1)(c)「機関等内通信回線に接続することについての可否を判断」について**

要管理対策区域外においてインターネットに接続した端末（支給外端末を含む。）を要管理対策区域において機関等 LAN システムに直接接続する場合、境界監視やファイアウォール等の多重防御を回避して不正プログラムが直接に機関等 LAN システム内に持ち込まれることにより、情報窃取、情報の破壊、サービス不能攻撃の踏み台になること等のリスクが高まる。このため、要管理対策区域外において機関等外通信回線に接続した物理的な端末（支給外端末を含む。）の接続の必要性がある場合には、取り得る情報セキュリティ対策、接続先となる情報システムにおいて取り扱う情報、情報セキュリティインシデント発生時の影響等を適切に評価した上で、総合的な見地から可否の判断を行う必要がある。例えば、要管理対策区域外での端末（支給外端末を含む。）の利用時に、機関等外通信回線を通じて機関等の情報システムのみにアクセスできる設定（例えば、機関等の情報システムにアクセスするためのアプリケーション以外を使用させない設定等）とし、シンクライアントや VPN とセキュアブラウザの組み合わせを用いて当該情報システムへリモートアクセスさせるような場合は、機関等外通信回線に接続して業務を行った後、機関等内通信回線へ接続する時のリスクを懸念する必要性は低下する。このように取り得る情報セキュリティ対策等を考慮して上記の判断を行うことが求められる。なお、リモートアクセスに関する対策は、遵守事項 8.1.3(2)を参照のこと。

また、テレワークやクラウド利用の拡大により、機関等外から情報システムへのアクセスが増えるにつれ、主体のなりすましによる不正アクセスなどの脅威への対策が重

要である。そのような脅威へ対抗するためには、あらゆるアクセスを信用できないものとして扱い、アクセスの都度信用情報を用いた検証によって動的なアクセス制御を行う対策が有効である。動的なアクセス制御の実装については、7.3「ゼロトラストアーキテクチャ」を参照のこと。

- **遵守事項 6.1.2(1)(c)「技術的な措置に関する運用規程」について**

インターネット等の機関等外通信回線に直接接続して業務を行った物理的な端末を機関等内通信回線に接続を行う場合には、利用可能な情報セキュリティ対策技術等を総合的に勘案の上、適切に対策を講ずる必要がある。例えば、機関等内通信回線に接続する前に不正プログラム対策ソフトウェアを用いて検査を行うことや当該端末において不正な通信を行っていないか、不要なアプリケーション、サービスやポートを使用していないかなどを確認するなどが考えられる。その際、不適切な状態を検知した場合は、機関等内通信回線に接続させない措置を講ずることや、機関等内通信回線から直ちに切断するなどの措置を講ずることも考えられる。

- **基本対策事項 6.1.2(1)-1 c)「盗難・紛失に対する対策」について**

一般的に、以下に例を挙げる状況では、盗難・紛失が発生しやすいため、要機密情報を含むモバイル端末を携行する場合には十分注意させる必要がある。特に飲酒が想定される場合は、モバイル端末は携行しないことが重要である。

  - 電車等での移動中に、モバイル端末の入ったかばん等を網棚に置き、そのまま下車する。
  - 飲酒が想定されるいわゆる宴会等でモバイル端末の入ったかばん等を置いたまま帰宅する。

- **基本対策事項 6.1.2(1)-2 c)「利用期間満了時の手続」について**

利用期間満了時は、職員等に報告を求めるよう手続に定める必要がある。特に機密性３情報等の取扱いに注意すべき情報を要管理対策区域外に持ち出す場合においては、以下を例とする管理手順を設けるとよい。

  - 利用期間満了時の連絡が無い場合は、当該利用者に確認する。
  - 利用期間の延長が必要であれば、再手続を要請する。
  - 利用期間満了前に利用が終了した際には、利用終了時に報告を求める。

- **基本対策事項 6.1.2(1)-3「暗号化」について**

機関等が支給する端末（要管理対策区域外で使用する場合に限る。）に要機密情報を保存して業務を行う場合は、端末に保存する情報を暗号化して、盗難・紛失時の情報漏えいのリスクを低減する必要がある。情報へのアクセス権を管理する方法もあるが、モバイル端末が第三者の者の手に渡った場合には、モバイル端末から取り外された内蔵電磁的記録媒体や、モバイル端末で利用していた外部電磁的記録媒体に保存されている情報を他の端末を利用して解読するなどの手段によってアクセス権管理機構を回避され要機密情報が窃取される危険性がある。このような情報の窃取への対策として、端末に暗号化機能を搭載することが有効である。

暗号化する方法としては、ファイル暗号化等のセキュリティ機能を持つアプリケー

ションを用いる方法、ハードディスク等の電磁的記録媒体又はファイル単体を暗号化するソフトウェアの導入や OS が備えている暗号化機能を使用することが挙げられる。遠隔データ消去機能を補助的な機能として組み合わせると効果的である。ハードディスク等の電磁的記録媒体を暗号化している場合であっても、端末の起動中等の復号可能な状態で盗難等に遭った場合には情報窃取されるおそれがあるため、遠隔データ消去機能と組み合わせて用いると情報窃取される可能性をより低減できる。

また、安全性を確保するためには暗号化に用いる鍵の管理が重要である。端末紛失時に端末内に鍵や、鍵を生成するために必要な全ての情報を保持していると暗号化したデータを復号されるリスクがある。

したがって、業務利用していないときはこれらを保持しないなど、鍵の漏えいリスクが低減されるような管理の仕組みを持つ以下を例とする方式を導入するとよい。

＜例＞

- 端末内の耐タンパ性を備えた TPM（Trusted Platform Module）を利用する方法
- 鍵を USB セキュリティトークンに格納して、利用時以外は端末とは別に管理する方法
- 暗号化する範囲を業務領域に限定しパスワードを入力するタイミングを業務システムへのログイン時、パスワードを基に生成した鍵を消去するタイミングをログアウト時（又はタイムアウト時）とする方法

- **基本対策事項 6.1.2(1)-3 a)「シンクライアント等」について**

端末に情報を保存させない仕組みとして、シンクライアントやリモートデスクトップと呼ばれる技術の活用が有効である。既に市場において提供されているが、外部の情報処理サービスを組み合わせてシンクライアントやリモートデスクトップ関連の製品やソリューションサービスを利用する場合には、第 4 部「外部委託」についても参照する必要がある。

＜シンクライアントの主な機能及び特徴＞

- 業務ネットワーク内の仮想デスクトップ画面を転送
- ユーザデータを端末に残さない。
- ウェブキャッシュ、接続情報、作業履歴等全てサーバ装置内に保管
- 外部情報出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

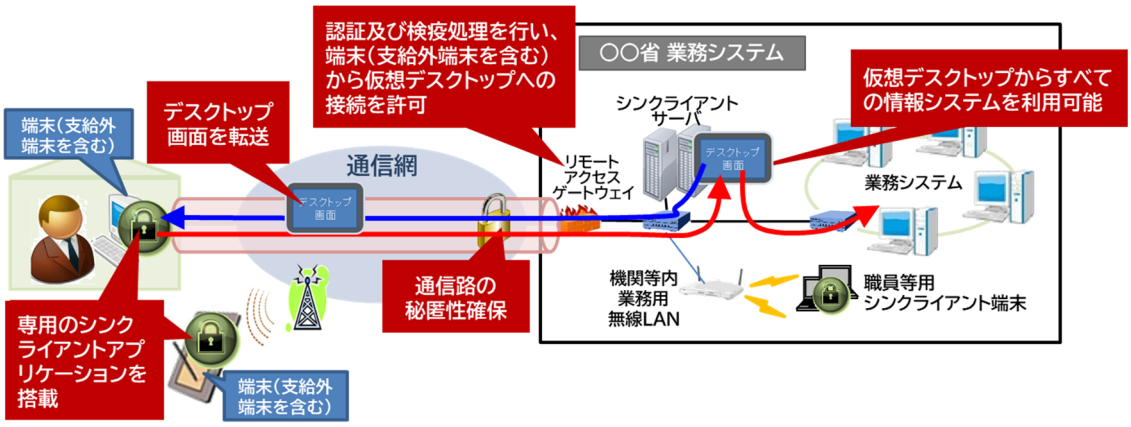


図 6.1.2-1　シンクライアントのシステム構成例

また、シンクライアントの発展形として、仮想デスクトップ環境の利用機能（ネットワーク接続や画面描画・ディスプレイ出力、キーボード・マウス入力等）のみに機能が絞り込まれたゼロクライアントやシンクライアント専用端末の利用も有効である。特にゼロクライアントは、汎用 OS や汎用ブラウザ等を搭載していないことから、不正プログラム対策やソフトウェア更新等のセキュリティ管理の負荷が軽減でき、万一端末が故障しても、端末を交換するだけですぐに利用可能になるなど、セキュリティ管理面の負荷の軽減も期待される。処理能力やコスト負担等の課題も考えられるので、それらも勘案した上で利用を検討するとよい。

- **基本対策事項 6.1.2(1)-3 b)「セキュアブラウザ等」について**

  セキュアブラウザ製品は、各種サービスと組み合わせたソリューションとして提供される場合があることから、外部の情報処理サービスを組み合わせて利用する場合は、第 4 部「外部委託」についても参照する必要がある。

  ＜セキュアブラウザの主な機能及び特徴＞

  - 端末に電子メール、ファイル閲覧等を画面転送等で行い、端末内のブラウザ等で閲覧することなどが可能。閲覧終了時に当該データを端末に残さない
  - ブラウザ終了時に閲覧に関連する情報（ウェブキャッシュ、URL、cookie 等）を消去可能
  - 外部出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

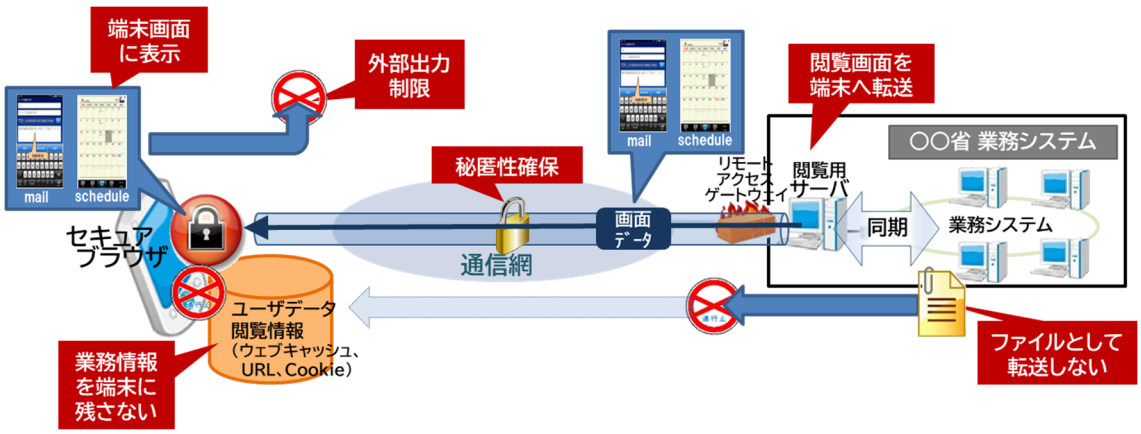


図 6.1.2-2　セキュアブラウザ活用型ソリューションのシステム構成例

- **基本対策事項 6.1.2(1)-3 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について**

  通信回線との接続環境が無い場所で業務を行うなど、やむを得ず情報を端末に保存させる必要がある場合は、セキュアブラウザやシンクライアントは利用できないことから、他の方法で安全な利用環境の提供を考える必要がある。この場合は、モバイル端末にファイル暗号化等のセキュリティ機能を持つ業務専用のアプリケーションを搭載し、アプリケーション単位で情報を暗号化するなどの方法が考えられる。当該機能を有するセキュリティソリューションが製品として民間事業者より提供されていることから、それらの活用を検討するとよい。

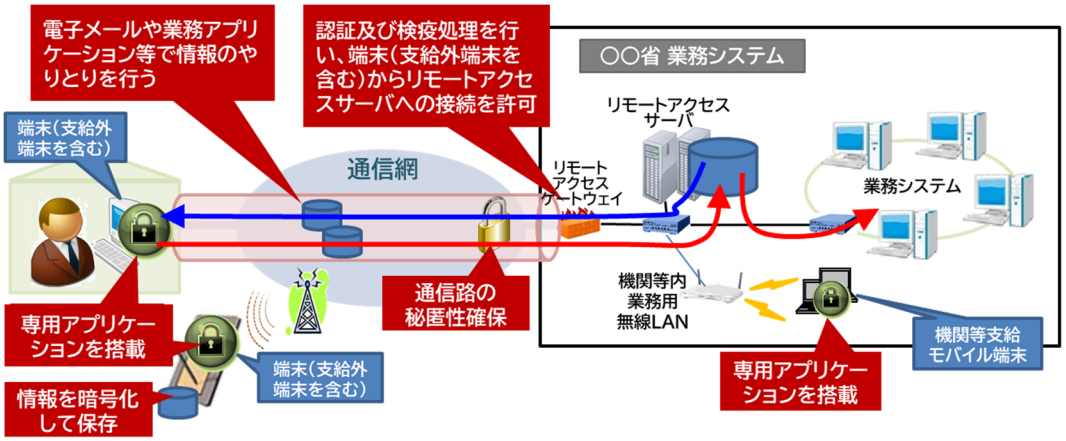


図 6.1.2-3　ファイル暗号化等セキュリティ機能を持つ

アプリケーションを活用したシステム構成例

- **基本対策事項 6.1.2(1)-3 d)「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」について**

  電磁的記録媒体全体を暗号化する機能については、例えばソフトウェアによる暗号化（Windows の BitLocker 等）やハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などが考えられる。なお、暗号化する機能として Windows の BitLocker を利用する場合は、パスワード解析への耐性を高めるため、端末起動時に追加の認証（PIN）を要求することを検討するとよい。

- **基本対策事項 6.1.2(1)-3 e)「ファイルを暗号化する機能を設ける」について**

  機関等が支給する端末（要管理対策区域外で使用する場合に限る。）のセキュリティ対策については、職員等の人的作業負担とならないようにすべきであり、職員等が講じた安全管理措置が不十分であることも考えられるため、基本対策事項 6.1.2(1)-3 a)～d)に示すシステム面で対応が取られることが望ましい。要管理対策区域外で要機密情報を取り扱う際の対策として、個々のファイルを手作業により暗号化する場合は、職員等に確実にこれを実施させることが必要となる。ただし、職員等が個々に暗号化すると、設定ミスや漏れ等が発生する可能性が高くなることから、職員等が暗号化の実施を容易にする仕組みの検討が重要である。

  例えば、職員等が確実にファイルの暗号化を実施することを容易にする仕組みとして、仮想化技術を活用した仮想ドライブを用いる方法がある。仮想ドライブの作成時に暗号化の設定を施すことにより、当該仮想ドライブに保存されるファイルの暗号化と復号を自動的に行うことができる。

- **基本対策事項 6.1.2(1)-3 f)「遠隔からの命令等により暗号化消去する機能」について**

  端末の通信機能を利用して、遠隔から端末内のデータを暗号化消去する機能であるが、通信が確立できないために遠隔からデータ消去できない場合に備え、主体認証の失敗した回数をカウントして一定数を超えた際に消去するなど特定の条件で自律的に消去する機能についても導入するとよい。

- **基本対策事項 6.1.2(1)-3 g)「高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等」について**

  一部のスマートフォンやタブレット端末用の OS において、不正プログラム対策ソフトウェアが有効な役割を果たさないと考えられ、提供されていないことがある（「（解説）遵守事項 7.2.2(1)(a)「不正プログラム対策ソフトウェア等を導入する」について」を参照のこと。）。そうした OS は多くの場合、基本対策事項 6.1.2(1)-3 d)及び f)のような高度なセキュリティ機能を標準で備えており、追加の対策を講ずることなく容易にそれらの機能を利用することができる。

  業務上の要件との兼ね合いもあるが、安全性を優先して、こうした OS を搭載する端末を積極的に利用することも考えられる。

遵守事項

(2) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策

(a) 情報システムセキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、当該端末について前条(b)の技術的な措置を講ずること。

(b) 情報システムセキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する物理的な端末を機関等内通信回線に接続させる際、当該端末について前条(c)の技術的な措置を講ずること。

【 基本対策事項 】

＜6.1.2(2)(a)(b)関連＞

6.1.2(2)-1 情報セキュリティリスクが相対的に高いと考えられる地域においては、第三者による物理的なアクセスのリスクへの対策を実施すること。

（解説）

- **遵守事項 6.1.2(2)(a)「前条(b)の技術的な措置を講ずる」について**

  職員等が機関等が支給する物理的な端末(要管理対策区域外で使用する場合に限る。)を用いて要機密情報を取り扱う場合は、遵守事項 6.1.2(1)(b)において定めた運用規程に基づき、当該端末に対して技術的な措置を講ずることが求められる。

- **遵守事項 6.1.2(2)(b)「前条(c)の技術的な措置を講ずる」について**

  テレワークなどによって要管理対策区域外の機関等外通信回線に接続した機関等が支給する物理的な端末については、機関等内通信回線に接続させる際に、遵守事項 6.1.2(1)(c)において定めた運用規程に基づき技術的な措置を講ずることが求められる。

- **基本対策事項 6.1.2(2)-1「第三者による物理的なアクセスのリスクへの対策」について**

  情報セキュリティリスクが相対的に高いと考えられる地域等においては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。このような地域等においては、例えば、使用する端末の USB ポート等を物理的にロック（塞ぐ）して封印、システム設定で端末の USB ポート等を無効にするといった対策を施した専用のモバイル端末で業務を行うとともに、端末は常時携行し、このような地域等から戻った際には、端末を工場出荷時の状態に戻すことが望ましい。

6.1.3 機関等支給以外の端末の導入及び利用時の対策

目的・趣旨

機関等の業務の遂行においては、機関等から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等や危機的事象発生時の際に、やむを得ず機関等支給以外の端末を利用して情報処理を行う場合も考えられるが、この際、当該端末の情報セキュリティ水準が対策基準を満たさないおそれがある。このため、機関等支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で、職員等に対して機関等における厳格な管理の下で利用させることが必要である。

また、機関等支給以外の端末については、端末の管理を端末の所有者が行うこととなり、機関等において管理ができないことへのリスクを勘案し、その利用の可否を判断する必要がある。利用を認めたとしても、利用の許可手続を定めるとともに、情報の取扱いについての規定や手順を整備し遵守させる必要がある。

遵守事項

(1) 機関等支給以外の端末の利用可否の判断

(a) 最高情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.1.3(1)(a)「機関等支給以外の端末の利用」について**

機関等支給以外の端末の利用とは、職員等が従事する業務で利用する機関等の情報システムから入手可能な業務に係る情報(業務上知り得る情報)、情報システムの仕様やデータ設定等に係る情報や、情報システムにおいて利用される主体認証情報（パスワード等）を機関等支給以外の端末において利用することである。ただし、機関等支給以外の端末で機関等が公表している情報を入手するなどの利用は、含まない。

- **遵守事項 6.1.3(1)(a)「求められる情報セキュリティの水準の達成の見込み」について**

機関等支給以外の端末の導入に当たっては、以下のようなリスクが想定される。

  - 不正プログラムに感染し、要機密情報が外部に漏えいする。
  - 接続先の情報システムが、機関等支給以外の端末を通じて不正プログラムに感染し、業務の継続が困難になる等の影響が生じる。

- 端末の盗難・紛失等により、要機密情報が外部に漏えいする。
- 利用者の知識不足により、利用者の意図に反して要機密情報が国外のサーバ装置等に保存され、第三者に閲覧される。
- 家族や知人の端末操作により端末内の要機密情報が外部に漏えいする。

- **遵守事項 6.1.3(1)(a)「可否を判断すること」について**

個別判断により機関等支給以外の端末の利用を認めてしまうと、「(解説) 遵守事項 6.1.3(1)(a)「求められる情報セキュリティの水準の達成の見込み」について」に記載したリスクが顕在化する可能性が高いことから、利用に当たっては、最高情報セキュリティ責任者があらかじめ統一的に判断することを求めている。利用を許可するに当たり、機関等としての利用方針を定めて、その利用方針の下、厳格な管理を行うことが求められる。

機関等支給以外の端末の利用方針として、例えば以下の事項を明確にすることが考えられる。

- 利用を許可する部局・課室等の組織の単位
- 利用を許可する職員等の条件
- 利用を許可する端末の種類（スマートフォン、携帯電話、PC 等）
- 利用を許可する端末の OS 及びそのバージョン
- 利用を許可する業務（出張時の連絡、危機的事象発生時の緊急対処業務 等）
- 利用する機能（電子メール及びウェブ閲覧に限定 等）
- 利用を許可する情報の格付（機密性１情報又は機密性２情報　等）

また、機関等支給以外の端末の利用に際して、利用する通信回線やサーバ装置等、情報システム全体として情報セキュリティを確保することが重要であることから、リモートアクセス環境や端末の安全管理措置について、システム機能として提供することも考慮すべきである。

併せて、機関等支給以外の端末の利用可否及びその利用方針について、当該事項を対策基準に記載するとともに、職員等へ周知することで機関等支給以外の端末の適切な利用が行われるようにすることも重要である。

遵守事項

(2) 機関等支給以外の端末の利用に関する運用規程等の整備

(a) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の**許可等の手続**を実施手順として定めること。

(b) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。

(c) 統括情報セキュリティ責任者は、**要機密情報を取り扱う機関等支給以外の端末**について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を含めた安全管理措置に関する運用規程を整備すること。

(d) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を**機関等内通信回線に接続することについての可否**を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた**安全管理措置に関する運用規程**及び許可手続に関する実施手順を定めること。

【 基本対策事項 】

＜6.1.3(2)(a)関連＞

6.1.3(2)-1 統括情報セキュリティ責任者は、機関等支給以外の端末を利用する際に、以下を全て含む許可等の手続を実施手順として整備し、職員等に周知すること。

a) 以下を全て含む機関等支給以外の端末利用時の申請内容

- 申請者の氏名、所属、連絡先
- **利用する端末の契約者の名義**（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の製造企業名、機種名、OS の種類及びバージョン
- 利用目的及び利用を許可する業務、取り扱う情報の概要、要機密情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- **利用する期間**

b) **利用許諾条件**

c) 申請手順

d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順

e) 利用期間満了時の利用終了又は利用期間更新の手続方法

f) **許可権限者**（端末管理責任者）

＜6.1.3(2)(b)関連＞

6.1.3(2)-2 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて要保護情報を取り扱う場合の利用手順を、以下を例とし実施手順として定めること。

a) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

b) 盗み見に対する対策（のぞき見防止フィルタの利用等）
c) **盗難・紛失に対する対策**（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
d) 利用する場所や時間の限定
e) 端末の盗難・紛失が発生した際の緊急対応手順

6.1.3(2)-3 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等支給以外の端末について、以下を例とする利用時の措置を利用手順に加え、実施手順として定めること。
a) **パスワード等による端末ロック**の常時設定
b) **OS やアプリケーションの最新化**
c) **不正プログラム対策ソフトウェアの導入**及び定期的な不正プログラム検査の実施（機関等として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含む。）
d) 機関等提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）

6.1.3(2)-4 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等支給以外の端末について、以下を全て含む禁止事項を利用手順に加え、実施手順として定めること。
a) **端末、OS、アプリケーション等の改造行為**
b) **安全性が確認できないアプリケーション**のインストール及び利用
c) **利用が禁止されているソフトウェア**のインストール及び利用（利用を禁止するソフトウェアを定める場合）
d) **許可されない通信回線サービスの利用**（利用する回線を限定する場合）
e) **第三者への端末の貸与**
f) **利用承認を得ていないクラウドサービス等への端末内の要機密情報のバックアップ**
g) 機密性３情報の取扱い

6.1.3(2)-5 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて要保護情報を取り扱う場合について、以下を全て含む許可手続を実施手順として定めること。
a) 利用時の許可申請手続
b) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）
c) **利用期間満了時の手続**
d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

＜6.1.3(2)(c)関連＞

6.1.3(2)-6 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を**暗号化**するための対策の検討のほか、端末で機密性３情報を取り扱うことができない対策についても検討し、要機密情報を取り扱う機関等支給以外の端末に求める安全管理措置に関する運用規程のうちの技術的な措置として加える

こと。

なお、可能な限り端末に情報を保存させない機能を設けることも運用規程に含めること。

a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築し、利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスすること。

b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築し、利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスすること。

c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入すること。

d) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設けること。

e) 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設けること。

f) ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設けること。

g) 高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等を使用すること。

＜6.1.3(2)(d)関連＞

6.1.3(2)-7 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を要管理対策区域で機関等内通信回線に接続することの許可手続として、以下を全て含む手続を実施手順として整備し、職員等に遵守させること。

a) 利用時の許可申請手続

b) 手続内容（利用者、目的、利用する情報、端末等）

c) 利用期間満了時の手続

d) 機関等内通信回線への接続時の手続（端末の事前検疫等）

e) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

（解説）

- **遵守事項 6.1.3(2)(a)「許可等の手続」について**

許可等の手続を定める際には、機関等支給以外の端末を用いて業務を行うことの脅威を把握し、十分なリスク評価を行った上で許可等の手続を定めるとよい。特に機関等支給以外の端末で要保護情報を取り扱うなど重要な業務に使用する場合は、利用する端末の種類や利用場所、利用する通信回線などを把握し、情報セキュリティインシデントが発生しないような使い方を遵守させることが重要である。また、機関等支給以外の端末を利用する職員等に対しても、どのような脅威が起こり得るかを理解させた上で、十分な管理を行うことを遵守させるとよい。

機関等支給以外の端末としてスマートフォンを利用する場合は、以下を参考にするとよい。

参考：総務省「スマートフォンを安心して利用するために実施されるべき方策」（スマートフォン・クラウドセキュリティ研究会最終報告）
（https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html）

- **遵守事項 6.1.3(2)(c)「要機密情報を取り扱う機関等支給以外の端末」について**

  要機密情報を取り扱う機関等支給以外の端末とは、機関等支給以外のモバイル端末と職員等の自宅で業務を行う際に用いる機関等支給以外の据え置き型端末が該当する。

- **遵守事項 6.1.3(2)(d)「機関等内通信回線に接続することについての可否」について**

  「（解説）遵守事項 6.1.2(1)(c)「機関等内通信回線に接続することについての可否を判断」について」を参照のこと。

- **遵守事項 6.1.3(2)(d)「安全管理措置に関する運用規程」について**

  機関等支給以外の端末は、日常的に職員等が業務以外の目的で利用していると考えられる。したがって、日常的にインターネット等に直接接続していると考え、機関等内通信回線に接続を行う場合には、利用可能な情報セキュリティ対策等を総合的に勘案の上、職員等に適切に対策を講じさせる必要がある。例えば、機関等内通信回線に接続する前に不正プログラム対策ソフトウェアを用いて検査を行わせることや利用を禁止しているソフトウェアがインストールされていないことを確認させるなどが考えられる。

- **基本対策事項 6.1.3(2)-1 a)「利用する端末の契約者の名義」について**

  契約者の名義の提示を求めるのは、業務に使用する端末の名義人と使用人の一致を確認するためである。端末の名義人が端末の利用に係る契約者であり、業務への使用や通信費用に係る訴訟リスクを回避するためには、利用申請時に使用人と名義人が一致していることを確認する必要がある。

  なお、名義人と使用人である申請者が同一であることを利用条件とする場合は、名義人の確認を求める必要はない。

- **基本対策事項 6.1.3(2)-1 a)「利用する端末の製造企業名、機種名、OS の種類及びバージョン」について**

  職員等が利用する機関等支給以外の端末についても、機関等が支給する端末を調達する際と同等の情報セキュリティ水準でサプライチェーン・リスクに対応することが適当である。

  機関等支給以外の端末について、製造企業名、機種名を把握し、「IT 調達に係る国等の物品又は役務の調達方針及び調達手続に関する申合せ」（関係省庁申合せ　内閣官房国家サイバー統括室）の趣旨を踏まえた対応として、内閣官房国家サイバー統括室に助言を求める。また、スマートフォンの Android OS のように製造企業によってカスタマイズされた OS がある場合や様々なバージョンが利用されている場合、機関等が許可で

きる OS、バージョンであるか、利用する情報システムの情報セキュリティ対策が対応できる端末であるかを判断する。

- **基本対策事項 6.1.3(2)-1 a)「利用する期間」について**

機関等支給以外の端末を利用する際に、利用の都度申請手続を行うと事務処理が煩雑化する可能性があるため、例えば 1 年間の利用期間を定め、包括的な許可を与えるなどして事務処理を効率化する方法も考えられる。この場合は、安全管理措置の実施状況について定期的なチェックを行うなどの対応が求められる。

- **基本対策事項 6.1.3(2)-1 b)「利用許諾条件」について**

職員等に機関等支給以外の端末の利用を許可するに当たり、以下の内容を例とした利用許諾条件を示し、許諾書にサインするなどして利用者の同意を証拠として残す必要がある。

  - 情報の格付及び取扱制限に応じた取扱いの遵守
  - 定められた安全管理措置の遵守
  - 組織による利用状況の情報収集の承諾
  - 組織による利用端末の制御及び端末の設定変更の承諾
  - 盗難・紛失時に私的な情報を含めた遠隔データ消去を行うことの承諾（職務上取り扱う情報のみ遠隔消去可能なツールを導入する場合は不要）
  - 情報セキュリティインシデントの可能性を認知した際の迅速な届出
  - 機種変更や端末交換の際の再届出の遵守
  - その他、情報システムセキュリティ責任者等の管理責任者の指示の遵守

- **基本対策事項 6.1.3(2)-1 f)「許可権限者」について**

機関等支給以外の端末の利用の許可申請においては、許可権限者である端末管理責任者の許可を得ることになるが、必要に応じて取り扱う情報の管理責任を持つ課室情報セキュリティ責任者の許可（遵守事項 8.1.1(4)(b)で規定）を同時に得る手続を定めるとよい。

- **基本対策事項 6.1.3(2)-2 c)「盗難・紛失に対する対策」について**

「（解説）基本対策事項 6.1.2(1)-1 c)「盗難・紛失に対する対策」について」を参照のこと。

- **基本対策事項 6.1.3(2)-3 a)「パスワード等による端末ロック」について**

盗難、紛失時の情報窃取を防止するために、適切な方法でパスワード等により端末をロックすることが重要である。適切でない方法による端末ロックの例としては、強固でないパスワードを設定した場合が挙げられる。このような場合、端末を窃取した者により端末ロックを解除される危険性があり、端末ロックが解除されると、基本対策事項 6.1.3(2)-6 の措置が効力を失う（暗号化している情報が自動的に復号されてしまう、リモートアクセス環境にアクセスされてしまうなど）可能性があるため、情報窃取の被害につながる。

強固なパスワードの設定方法については、「（解説）基本対策事項 7.1.1(1)-4「強固な

パスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照のこと。なお、端末ロックの機能が、主体認証の失敗した回数をカウントして一定数を超えた際に暗号化消去する機能を備えている場合には、数字のみからなる PIN（Personal Identification Number）コードを主体認証情報として用いてもよい。ただし、例えば 6 桁以上とするなどの一定の長さを要件とする必要がある。

- **基本対策事項 6.1.3(2)-3 b)「OS やアプリケーションの最新化」について**

脆弱性対策のため、OS や業務利用するアプリケーションを最新化する必要がある。私的利用するアプリケーションについても最新化することが望ましいが、基本対策事項 6.1.3(2)-6 で講ずる技術的な措置等を踏まえ、私的利用するアプリケーションが最新化されていないことによるリスクを評価した上で判断するとよい。

- **基本対策事項 6.1.3(2)-3 c)「不正プログラム対策ソフトウェアの導入」について**

携帯電話や一部のスマートフォンなど、不正プログラム対策ソフトウェアが有効な役割を果たさないと考えられている端末や OS において、不正プログラム対策ソフトウェアが提供されていない場合（「(解説）遵守事項 7.2.2(1)(a)「不正プログラム対策ソフトウェア等を導入する」について」を参照のこと。）には、事前に安全性が確認されたアプリケーションしかインストールしないようにするなどの別の方法で安全性を確保する必要がある。

- **基本対策事項 6.1.3(2)-4 a)「端末、OS、アプリケーション等の改造行為」について**

iOS における Jailbreak や Android における root 化のように、ソフトウェア等の改造が行われた端末は外部からの攻撃の的となりやすく、不正パケットの受信によって不正プログラムに感染し、端末が乗っ取られるなどの危険性が高くなる。

このような改造された端末が業務に使用されると、端末に保存された情報が漏えいするなどの情報セキュリティインシデントが発生する可能性があるため、機関等支給以外の端末を利用する際は、事前に端末、OS、アプリケーション等の改造行為を行わないことについて、職員等と事前に同意することが重要である。

モバイル端末を業務利用することを目的とした、MDM ツール等を機関等のリモートアクセス環境と組み合わせ、改造された端末を検知するなどして、システム的に改造端末の使用を回避する方法も考えられる。

- **基本対策事項 6.1.3(2)-4 b)「安全性が確認できないアプリケーション」について**

スマートフォンにおいては、専用のアプリケーション提供サイト等からオンデマンドでアプリケーションをダウンロードする利用形態が一般的であるが、不正プログラム等が混在する提供サイトの存在が懸念されるため、業務に利用する機関等支給以外のスマートフォン等においては安全性が不明なアプリケーションがインストールされた状態で利用されることがないように、例えば OS 提供事業者や通信事業者等がアプリケーションの安全性の審査を行っている信頼性の高いアプリケーション提供サイトにて提供されるアプリケーションのみに利用を限定すること等を対策にするとよい。ただし、大手の事業者であっても安全なアプリケーションを提供しているとは限らない

ので、提供サイトを運営する事業者のセキュリティ対策水準を十分見極めた上で判断することが求められる。

スマートフォンを安全に利用するための留意事項として、OS の最新化及び不正プログラム対策とともに注意喚起されているので、参考にすること。

参考：総務省「スマートフォン情報セキュリティ３カ条」（スマートフォン・クラウドセキュリティ研究会最終報告）
（https://www.soumu.go.jp/main_content/000166095.pdf）

- **基本対策事項 6.1.3(2)-4 c)「利用が禁止されているソフトウェア」について**

遵守事項 6.1.1(1)(b)の対策として、機関等支給の端末において規定される利用を認めたソフトウェアを参考に利用を禁止するソフトウェアを検討することが考えられるが、例えば私的な利用の範囲を必要以上に制限しないよう考慮する必要がある。

- **基本対策事項 6.1.3(2)-4 d)「許可されない通信回線サービスの利用」について**

ホテル等の施設や街中で提供される公衆無線 LAN サービスでは多数のユーザが容易に接続できることの利便性のため暗号化されていないことや、PSK（Pre-Shared Key/事前共有鍵）による認証方式が使用されていることがあるが、そのような状況では通信内容の盗聴や改ざん、アクセスポイントのなりすましによる情報の窃取等のおそれがあるため、業務に利用すべきではない。また、同様に有線によるインターネット接続が提供されている場合であっても接続経路や管理状況が不明である場合は業務に利用すべきではない。ただし、国外等での利用も含め、情報セキュリティ水準が不明な通信回線サービスを利用せざるを得ない場合が想定されることから、例えば、情報システムへのリモートアクセス経路において VPN 回線を設定し end-end の秘匿性を確保するなどの方法を用いるとよい。

なお、無線 LAN の利用については、総務省が公表している以下のガイドラインを参考にするとよい。

参考：総務省「公衆 Wi-Fi 利用者向け 簡易マニュアル」
（https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）

- **基本対策事項 6.1.3(2)-4 e)「第三者への端末の貸与」について**

家族や知人に私物の端末等を貸与することがあるが、その際に意図的に機密性の高い情報を閲覧したり又は誤操作により機密性の高い情報を外部に転送してしまったりすることが懸念される。

私物端末であっても業務に利用するのであれば、第三者への貸与は禁止すべきであり、それに同意できない職員等には私物端末を利用させるべきではない。

- **基本対策事項 6.1.3(2)-4 f)「利用承認を得ていないクラウドサービス等への端末内の要機密情報のバックアップ」について**

本規定はシャドーIT の抑止を目的としたものである。

なお、クラウドサービス自体の利用承認を得ている場合であっても、職員等の私的な

アカウントを用いて機関等支給以外の端末に格納された要機密情報のバックアップを取得させてはならない。

- **基本対策事項 6.1.3(2)-5 c)「利用期間満了時の手続」について**

  「(解説) 基本対策事項 6.1.2(1)-2 c)「利用期間満了時の手続」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6「暗号化」について**

  「(解説) 基本対策事項 6.1.2(1)-3「暗号化」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 a)「シンクライアント等」について**

  「(解説) 基本対策事項 6.1.2(1)-3 a)「シンクライアント等」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 b)「セキュアブラウザ等」について**

  「(解説) 基本対策事項 6.1.2(1)-3 b)「セキュアブラウザ等」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について**

  「(解説) 基本対策事項 6.1.2(1)-3 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 d)「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」について**

  「(解説) 基本対策事項 6.1.2(1)-3 d)「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 e)「ファイルを暗号化する機能を設ける」について**

  「(解説) 基本対策事項 6.1.2(1)-3 e)「ファイルを暗号化する機能を設ける」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 f)「遠隔からの命令等により暗号化消去する機能」について**

  「(解説) 基本対策事項 6.1.2(1)-3 f)「遠隔からの命令等により暗号化消去する機能」について」を参照のこと。

- **基本対策事項 6.1.3(2)-6 g)「高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等」について**

  「(解説) 基本対策事項 6.1.2(1)-3 g)「高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等」について」を参照のこと。

遵守事項

(3) 機関等支給以外の端末の利用に関する責任者の策定

(a) 情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等の業務に係る情報処理に関する**安全管理措置の実施状況を管理**する**責任者**（以下「端末管理責任者」という。）を定めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.1.3(3)(a)「安全管理措置の実施状況を管理」について**

  機関等支給以外の端末を職員等が利用するに当たって、申請時に安全管理措置の実施状況について端末を目視確認する方法や、定期的な実施状況の確認を管理者にて行うことをあらかじめ定めておく方法等、安全管理措置の確実な実施に資する実効性のある取組を行う必要がある。

- **遵守事項 6.1.3(3)(a)「責任者」について**

  機関等支給以外の端末の安全管理措置の実施状況を管理する責任者であり、PC やスマートフォン等に対して一定以上の知見を有している者がその任に当たることが望ましい。例えば、機関等 LAN システムの情報セキュリティ責任者等が考えられる。ただし、職員等の安全管理措置の実施状況について適時状況を把握することが求められるため、課室情報セキュリティ責任者が兼ねることも考えられる。

遵守事項

(4) 機関等支給以外の端末の利用時の対策

(a) 職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。

(b) 職員等は、機関等支給以外の端末を用いて要保護情報を取り扱う場合は、(2)(b)で定める利用手順に従うこと。

(c) 端末管理責任者等は、要機密情報を取り扱う機関等支給以外の端末について、(2)(c)に定める安全管理措置を講じる又は職員等に講じさせること。

(d) 職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.1.3(4)(b)「利用手順に従う」について**

職員等は、機関等支給以外の端末の利用に係る機関等全体のポリシーをよく理解し、安全管理措置を徹底し、また、利用手順に従い、情報セキュリティインシデントの回避に努めなければならない。特にスマートフォン等の利用については、その特性に応じたリスクを利用者である職員等自身もよく理解した上で利用することが求められる。

- **遵守事項 6.1.3(4)(c)「端末管理責任者等」について**

遵守事項 6.1.3(2)(c)に定める安全管理措置のうち、機関等支給以外の端末から機関等 LAN システム等の情報システムにアクセスさせる場合、当該情報システムの情報システムセキュリティ責任者が、機関等支給以外の端末に対する安全管理措置と併せて、当該情報システム側で対応すべき措置を講ずることも考えられる。

例えば、基本対策事項 6.1.3(2)-6 a)の規定を参考とし、シンクライアントを用いた機関等 LAN システムへのリモートアクセス環境を構築する場合は、端末に専用のシンクライアントアプリケーションをインストールすることに加え、サーバ装置に仮想マシンを構築することが考えられる。この場合は、機関等支給以外の端末から利用される機関等 LAN システムに知見を有している、機関等 LAN システムを管理する情報システムセキュリティ責任者が機関等支給以外の端末に対して本項を行うことが適切とも考えられる。

- **遵守事項 6.1.3(4)(c)「職員等に講じさせる」について**

基本対策事項 6.1.3(2)-6 の安全管理措置のうち、職員等が講ずることが適当な項目としては、例えば OS の機能を利用する 6.1.3(2)-6 d)の「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」や 6.1.3(2)-6 e)の「ファイルを暗号化する機能」が考えられる。

- **遵守事項 6.1.3(4)(d)「要保護情報を機関等支給以外の端末から消去する」について**

  要保護情報を消去することは必須であるが、不必要な情報及び業務用のアプリケーション等についても併せて消去することが望ましい。

6.2 サーバ装置

6.2.1 サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に機関等が利用するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・監視機能等の機能面での対策、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、7.2.3「サービス不能攻撃対策」、6.4.4「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。さらに、機関等外通信回線を経由してサーバ装置の保守作業等を行う場合は、6.4.1「通信回線」のリモートメンテナンスについての対策も遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本款での共通的な対策に加え、それぞれ本節において定める遵守事項についても併せて遵守する必要がある。

遵守事項

(1) サーバ装置の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う物理的なサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

(c) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させないこと。

(d) 情報システムセキュリティ責任者は、サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させないこと。

(e) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施すること。

(f) 情報システムセキュリティ責任者は、サーバ装置において利用するソフトウェアに

関連する公開された脆弱性について対策を実施すること。

(g) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得すること。

【 基本対策事項 】

＜6.2.1(1)(a)関連＞

6.2.1(1)-1 情報システムセキュリティ責任者は、要保護情報を取り扱う物理的なサーバ装置については、クラス２以上の要管理対策区域に設置すること。

6.2.1(1)-2 情報システムセキュリティ責任者は、物理的なサーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) 施錠可能なサーバラックに設置して施錠すること。

b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定すること。

6.2.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定すること。

＜6.2.1(1)(b)関連＞

6.2.1(1)-4 情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。

a) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

b) 同一システムを２系統で構成することによる冗長化

＜6.2.1(1)(c)関連＞

6.2.1(1)-5 情報システムセキュリティ責任者は、以下を全て考慮した上で、利用を認めるソフトウェアをバージョンも含め定めること。

a) ソフトウェアベンダ等のサポート状況

b) ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む。）、使用するポート、暗号化の有無

c) インストール時に同時にインストールされる他のソフトウェア

d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

（解説）

- **遵守事項 6.2.1(1)(c)「利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない」について**

「（解説）遵守事項 6.1.1(1)(b)「利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない」について」を参照のこと。

- **遵守事項 6.2.1(1)(d)「接続を認めた機器等を定め、接続を認めた機器等以外は接続さ**

せない」について

「(解説) 遵守事項 6.1.1(1)(c)「接続を認める機器等を定め、接続を認めた機器等以外は接続させない」について」を参照のこと。

- **遵守事項 6.2.1(1)(e)「適切なセキュリティ対策を実施する」について**

端末を導入する際と同様に、サーバ装置を導入する際も、セキュリティ要件に従って適切なセキュリティ対策を実施する必要がある。例えば、主体認証方式やアクセス制御等の情報セキュリティ機能が正しく実装されていることや脆弱性対策、サーバ装置において要安定情報を取り扱う場合及び非常時優先業務等を支える情報システムを運用する場合はサービス不能攻撃対策等を実施する必要がある。また、不要なポートが開放されていない、不要なサービスが起動していないなどの対策も重要である。

- **遵守事項 6.2.1(1)(f)「ソフトウェアに関連する公開された脆弱性について対策を実施する」について**

「(解説) 遵守事項 6.1.1(1)(e)「ソフトウェアに関連する公開された脆弱性について対策を実施する」について」を参照のこと。

- **遵守事項 6.2.1(1)(g)「適切な方法でサーバ装置のバックアップを取得する」について**

要安定情報を取り扱うサーバ装置については、情報システムにおける RTO（目標復旧時間)、RLO（目標復旧レベル）等を踏まえて、適切な方法でバックアップを取得する必要がある。そのバックアップの方法については、OS やアプリケーションなどを含むサーバ装置全体をバックアップする方法やサーバ装置の複製をバックアップとして用意する方法などが存在する。

また、バックアップを取得する際は、バックアップの世代管理、保存場所や媒体についても考慮する必要がある。バックアップの取得については、「(解説) 基本対策事項 5.2.3(1)-7 a)「適切なバックアップの取得及びバックアップ要件の確認による見直し」について」を参照のこと。

- **基本対策事項 6.2.1(1)-1「クラス２以上の要管理対策区域に設置する」について**

サーバ装置に関しては、取り扱う情報の重要性に応じて原則としてクラス３の区域に設置する。また、クラス２の区域（執務室等）に設置する場合においては、原則として常時施錠されたサーバラックに置くことが重要である。

- **基本対策事項 6.2.1(1)-4 b)「冗長化」について**

「冗長化」とは、障害や過度のアクセスが発生した場合を想定し、サービスを提供するサーバ装置を代替サーバ装置に切り替えること等により、サービスが中断しないように、情報システムを構成することである。可用性を高めるためには、サーバ装置本体だけでなく、ハードディスク等のコンポーネント単位で冗長化することも考えられる。

なお、災害等を想定して冗長化する場合には、代替のサーバ装置を遠隔地に設置することが望ましい。

- **基本対策事項 6.2.1(1)-5「利用を認めるソフトウェアをバージョンも含め定める」につ**

いて

「(解説) 基本対策事項 6.1.1(1)-4「利用を認めるソフトウェアをバージョンも含め定める」について」を参照のこと。

遵守事項

(2) サーバ装置の運用時の対策

(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による**見直しを行う**こと。

(b) 情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、**不適切な状態にあるサーバ装置を検出等した場合には改善を図る**こと。

(c) 情報システムセキュリティ責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講ずること。

(d) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行えるよう運用をすること。

【 基本対策事項 】

＜6.2.1(2)(b)関連＞

6.2.1(2)-1 情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、改善を図る場合は、作業日、作業を行ったサーバ装置名、具体的な作業内容（サーバ装置の構成等の変更、脆弱性管理、ソフトウェアのインストール等）及び作業者、正常動作を確認した者などを含む変更事項等を記録し、管理すること。

＜6.2.1(2)(c)関連＞

6.2.1(2)-2 情報システムセキュリティ責任者は、サーバ装置への不正アクセス等の情報セキュリティインシデントの発生を監視するために、以下を例とする対策を講ずること。

a) **アクセスログ等を定期的に確認する**こと。
b) IDS/IPS、WAF 等を設置すること。
c) **不正プログラム対策ソフトウェア**を利用すること。
d) ファイル完全性チェックツールを利用すること。
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認すること。
f) **ホスト型の IDS/IPS** を利用すること。
g) ユーザ、グループ、システム管理者の追加、変更の有無を確認すること。
h) 管理者、ユーザのパスワード漏えいの有無、大量のログオン失敗や、通常とは異なる時間帯やアクセス元 IP アドレスからのログインがないか確認すること。

＜6.2.1(2)(d)関連＞

6.2.1(2)-3 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置及び非常時優先業務等を支える情報システムを運用するサーバ装置について、以下を全て含む運用をすること。

a) サーバ装置全体の**適切なバックアップの取得及びバックアップ要件の確認による見直し**
b) サーバ装置の構成やソフトウェア等の設定の変更が行われた際及び定期的に、**サーバ装置が停止した際の復旧手順の確認による見直し**

（解説）

- **遵守事項 6.2.1(2)(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、定期的に利用を認めるソフトウェアの確認による見直しを行う必要がある。見直しを行うに当たっては、利用を認めるソフトウェアの必要性や利用を認めることによる脅威へのリスク等を踏まえた上で見直しを行う必要がある。特に管理者権限を必要とするソフトウェアや他のソフトウェアを含む機器等の管理や制御を行うソフトウェアの利用を認める場合は、追加のセキュリティ対策を実施させるなど、ソフトウェアを利用することによる脅威へのリスクを低減することが重要である。

- **遵守事項 6.2.1(2)(b)「不適切な状態にあるサーバ装置を検出等した場合には改善を図る」について**

「不適切な状態」とは、例えば以下の状態のことをいう。

- サーバ装置のハードウェアの構成が不正に変更されている。
- セキュリティ水準の低下を招くような設定変更がされている。
- 利用を認めるソフトウェア以外のソフトウェアがインストールされている。
- ソフトウェアのアップデート等により追加された機能において適切な設定がなされていない。
- 最新のセキュリティパッチが適用されていない。
- 不正プログラム対策ソフトウェアのパターン等が最新でない。
- 脆弱又は不要なプロトコルやポート、サービスなどが動作している。
- 不要な識別コードを無効化していない。
- 脆弱な主体認証情報を使用している。
- 管理者権限アカウントのみが存在しており、全ての作業を管理者権限アカウントで実施している。
- 時刻同期がなされていない。

利用を認めるソフトウェア以外のソフトウェアがインストールされているか否かについては、構成管理ツールを使用するほか、プロセスやその他挙動等を監視する方法もある。また、利用を認めるソフトウェアであっても、利用しない機能については無効化するなどの措置が考えられる。セキュリティパッチについては、7.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

- **基本対策事項 6.2.1(2)-2 a)「アクセスログ等を定期的に確認する」について**

不正アクセスを検知するために、サーバ装置へのアクセスに関するログのほか、サーバ装置が異常等を検出した際に出力するログ（エラーログ）を確認することも有効である。

アクセスログを確認する際は、運用管理作業の記録、管理者権限を持つ識別コードによるアクセスを検知した場合の通知等の確認により、不正なアクセスが行われた可能性を確認することも考えられる。

- **基本対策事項 6.2.1⑵-2 c)「不正プログラム対策ソフトウェア」について**

  不正プログラム対策ソフトウェアについては、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアが考えられるが、具体的には EPP（Endpoint Protection Platform）と呼ばれる製品のうち「アンチウイルス（AV)」や「次世代アンチウイルス（NGAV)」が挙げられる。そのような製品のうち NGAV については、不正プログラムの検知方法として、シグネチャにより検出するものに加え、機械学習や振舞い検知といった技術を用いた製品もある。これによって既知の不正プログラムだけではなく、未知の不正プログラムへの対応も可能となる。

  さらに EPP と組み合わせて、侵入した不正プログラムを検知する機能を持つ EDR 製品を用いると、より効果的である。EDR には、リアルタイムでエンドポイントを監視することが可能な製品もあり、EPP で検知できなかった不正プログラム等が被害を拡大させる前に対策をすることが可能となる。

  したがって、不正プログラム対策ソフトウェアを利用する場合は、情報システムで取り扱う情報や業務として行う内容等を踏まえて、必要なセキュリティ対策を検討した上で導入する製品等を選定することが望ましい。

- **基本対策事項 6.2.1⑵-2 f)「ホスト型の IDS/IPS」について**

  ホスト型の IDS/IPS は、ネットワーク型の IDS/IPS とは異なりサーバ装置に直接導入し利用することで、対象のサーバ装置で発生したイベントを監視することが可能となる。また、製品によっては不正アクセスに関する監視のみならず、操作ミスやアプリケーションで発生したエラー、ファイルやレジストリの改ざんを検知する機能を有するものも存在する。

- **基本対策事項 6.2.1⑵-3 a)「適切なバックアップの取得及びバックアップ要件の確認による見直し」について**

  「（解説）基本対策事項 5.2.3(1)-7 a)「適切なバックアップの取得及びバックアップ要件の確認による見直し」について」を参照のこと。

- **基本対策事項 6.2.1⑵-3 b)「サーバ装置が停止した際の復旧手順の確認による見直し」について**

  「（解説）基本対策事項 5.2.3(1)-7 b)「情報システムが停止した際の復旧手順の確認による見直し」について」を参照のこと。

遵守事項

(3) サーバ装置の運用終了時の対策

(a) 情報システムセキュリティ責任者は、**サーバ装置の運用を終了する際**に、サーバ装置の電磁的記録媒体の全ての情報を**抹消する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.2.1(3)(a)「サーバ装置の運用を終了する際」について**

  サーバ装置を廃棄処分する場合やリース契約が終了し返却する場合のほか、当該サーバ装置のサービス又は機能の提供を終了する場合も考えられる。

- **遵守事項 6.2.1(3)(a)「抹消する」について**

  サーバ装置の電磁的記録媒体の全ての情報を抹消する場合、サーバ装置で取り扱っていた情報だけでなく OS 領域も含めて全て抹消する必要があることに注意が必要である。

  抹消の方法については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」及び「（解説）遵守事項 6.1.1(3)(a)「抹消する」について」を参照のこと。

6.2.2 電子メール

目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する職員等が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 電子メールの導入時の対策

(a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

(c) 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。

(d) 情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。

【 基本対策事項 】

＜6.2.2(1)(a)関連＞

6.2.2(1)-1 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように以下を例とする設定をすること。

a) 送信元の電子メールサーバの IP アドレスによって中継を制限する設定

b) 送信元のメールアドレスのドメイン名によって中継を制限する設定

c) 宛先のメールアドレスのドメイン名によって中継を制限する設定

＜6.2.2(1)(b)関連＞

6.2.2(1)-2 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする職員等の主体認証を行う機能を備えること。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入すること。

＜6.2.2(1)(c)関連＞

6.2.2(1)-3 情報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

a) DMARC による送信側の対策を行うこと。DMARC による送信側の対策を行う

ためには、**SPF**、**DKIM** の**いずれか又は両方による対策を行う必要**がある。

b) DMARC による**受信側の対策**を行うこと。DMARC による受信側の対策を行うためには、**SPF、DKIM の両方による対策を行う必要**がある。

c) **DMARC ポリシーには、“p=quarantine”又は“p=reject”を設定すること**。やむをえず、”p=none”を設定する場合も設定期間が可能な限り短くなるようにする必要がある。

6.2.2(1)-4 情報システムセキュリティ責任者は、**必要に応じて、S/MIME 等の電子メールにおける電子署名**の技術による電子メールのなりすましの防止策を講ずること。

6.2.2(1)-5 情報システムセキュリティ責任者は、職員等が機関等外の者と電子メールを送受信する場合には、**政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能**を備えること。

＜6.2.2(1)(d)関連＞

6.2.2(1)-6 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。

a) **SMTP によるサーバ間通信を TLS により保護**すること。

b) **S/MIME 等の電子メールにおける暗号化及び電子署名**の技術を利用すること。

（解説）

- **遵守事項 6.2.2(1)(a)「不正な中継」について**

不正な中継が行われると、迷惑メールの送信等に悪用される問題がある。電子メールの不正な中継に起因し生じるおそれのある事象として、以下が考えられる。

- 電子メールサーバや通信回線のリソースが消費されて運用に支障をきたす。
- 不正な中継を行う電子メールサーバとして他の電子メールサーバ等から接続や電子メールの転送を拒否される。
- 迷惑メールの受信者からの苦情や問合せへの対応が必要になる。

悪用を回避するため、電子メールの不正な中継を行わないように、中継を許可する電子メールを必要最小限とする設定を電子メールサーバに行う必要がある。

特に、電子メールサーバ間で送受信する電子メールを中継するメール中継サーバが設置される場合、電子メールの不正な中継を行わない設定をメール中継サーバで必ず実施し、IP アドレスによる制限等の対策をファイアウォールによる通信制限のみに依存しないよう留意が必要である。

なお、当該設定においては、多重防御の考えに基づき、メール中継サーバを含む全ての電子メールサーバにおいて実施するとともに、設定が可能な範囲で複数の設定を行う必要がある。

さらに、送信元のメールがなりすまされていないか検証する必要がある場合には、電子メールの中継を行う電子メールサーバにおいて、電子メールのなりすまし防止対策を講ずることも考えられる。

- **遵守事項 6.2.2(1)(d)「サーバ間通信の暗号化」について**

  相手先サーバが暗号化に対応していない状況も考慮しなければならない。自らが送信側となる際には、相手先が暗号化に対応可能であることを確認し、確認が取れた場合には以降の通信を暗号化することが求められる。また、自らが受信側となる際には、相手先からの接続要求時に暗号化の機能に対応していることを示すことが求められる。

  暗号化された通信の監視については、「(解説) 遵守事項 5.2.1(3)(a)(イ)「監視するデータが暗号化されている場合は、必要に応じて復号」について」を参照のこと。

  また、電子メールクライアントと電子メールサーバ間の通信の暗号化についても併せて対応することが望ましい。

- **基本対策事項 6.2.2(1)-3「送信ドメイン認証技術」について**

  送信ドメイン認証技術の導入に当たっては、技術的な解説や導入の手順などを詳細に解説した、迷惑メール対策推進協議会による「送信ドメイン認証技術導入マニュアル」を参考にするとよい。

  参考:迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル　第 3.1 版」
  (https://www.dekyo.or.jp/soudan/aspc/report.html#dam)

  総務省による「送信ドメイン認証技術等の導入に関する法的解釈について」において、送信ドメイン認証技術の導入に当たり、電気通信事業法における法的な整理を示しており、この範囲内で実施することが可能となっている。なお、職員等が利用する電子メールシステムに機関等が送信ドメイン認証技術を導入する際には、「送信ドメイン認証技術等の導入に関する法的解釈について」は、必ずしも留意する必要はない。

  参考：総務省「送信ドメイン認証技術等の導入に関する法的解釈について」
  (https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html)

- **基本対策事項 6.2.2(1)-3 a)「DMARC」について**

  DMARC は、認証の基本的な技術は SPF や DKIM を利用しており、SPF や DKIM で認証されたドメイン名と、メールヘッダ上の送信ドメイン名が一致した場合に、なりすまされていないものと判断する。また、電子メールの受信側において SPF、DKIM の送信ドメイン認証が失敗したときの処理を送信側が指定できる。例えば、受信側で認証が失敗したときは受信を拒否させるといった処理を送信側が指定できる。さらに、認証結果を電子メールの送信側に DMARC レポートとしてフィードバックする機能を備えている。例えば、機関等になりすましたメールが送信されている状況や、受信側における SPF、DKIM の認証が成功あるいは失敗している状況を DMARC レポートの内容から分析することができる。

- **基本対策事項 6.2.2(1)-3 a)「送信側の対策」について**

  送信側の対策を行うことによって、送信側である機関等が送信した電子メールが詐称されているかどうかを受信側において確認することが可能となる。

送信ドメイン認証技術を使用した送信側の対策として、電子メールで使用するドメインを管理する DNS サーバに、受信者が電子メールの正当性を確認するための情報を登録し公開する必要がある。なお、DNS キャッシュポイズニング攻撃等により DNS レコードを偽の情報に書き換えられる可能性があるため、DNS サーバに対して DNSSEC を導入することが望ましい。

また、電子メールの送信に使用するドメイン名だけではなく、Web サイトの URL 等、機関等の使用するあらゆるドメイン名に対しても、受信者が電子メールの正当性を確認するための情報を登録し公開することが重要である。

- **基本対策事項 6.2.2(1)-3 a)「SPF」について**

SPF はネットワーク方式の送信ドメイン認証技術である。

SPF の送信側の対策としては、送信側の電子メールサーバの情報を DNS サーバに登録する必要がある。登録の際は以下の事項に留意が必要である。

- 電子メールを利用していないドメインについても、その情報を SPF レコードに登録する。(「SPF レコード」とは、SPF において、DNS サーバの TXT レコードに記述される送信側の電子メールサーバ等の情報をいう。) あわせて null MX (RFC7505) の設定をすることが望ましい。
- SPF レコードの末尾は、"~all"ではなく"-all"を記述する。
- SPF レコードは、チェックツール等で、文法的に記述間違いのないことを確認する。
- なりすましの防止策のため、ウェブによるサービス等も含め全く利用していない、又は将来にわたって利用の予定の無いドメインについては、なりすましの防止策を講ずるか、ドメイン名の登録を廃止する。
- 民間事業者等において提供されている、他の利用者と共用する電子メールサービスを利用する場合は、機関等をなりすました電子メールが、当該電子メールサービスを利用する他の利用者から送信されないような仕組みを備えていることを確認する。他の利用者と共用しない専用の IP アドレスを割り振ることが可能なサービスが提供されている場合は、当該サービスの利用を検討する。

- **基本対策事項 6.2.2(1)-3 a)「DKIM」について**

DKIM は電子署名方式の送信ドメイン認証技術である。

DKIM の送信側の対策としては、電子メールに付与する電子署名の検証に使用する公開鍵を DNS サーバに登録する必要がある。

SPF、DKIM はどちらも、電子メールが詐称されているかどうかをドメイン名単位で受信側が確認することが可能な技術であるが、DKIM はそれに加えて、電子メールが改ざんされていないことを受信側が検証することが可能となる。

また、電子メールの転送においては、SPF の場合、受信した電子メールのエンベロープ From のドメイン名から取得した SPF レコードに設定されている IP アドレスと、電子メールを転送したサーバの IP アドレスが異なるため、SPF の認証が失敗する。しかし、電子メールの最初の送信者が DKIM 署名を付与する場合は、電子メールのヘッダや本文が改変されていなければ DKIM の認証が成功する。そのため、電子メールの

転送における送信側の対策を講ずる際は DKIM を検討するとよい。

さらに、メーリングリストにおいては、SPF の場合、SPF の認証が成功したとしても、SPF で認証されたドメイン名と DMARC で認証に用いるメールヘッダ上の送信ドメイン名が一致しないため、DMARC の認証は失敗する。しかし、DKIM の場合は、メーリングリスト側でメーリングリストのドメイン名での DKIM 再署名とメールヘッダ上の送信ドメイン名の変更等を行うことで、DMARC の認証が成功する。そのため、メーリングリストの転送における送信側の対策を講ずる際は DKIM を検討するとよい。

- **基本対策事項 6.2.2(1)-3 a)「いずれか又は両方による対策を行う必要」について**

電子メールの受信側が SPF、DKIM いずれかのみを導入している可能性があるため、送信側である機関等としては SPF、DKIM の両方を導入することが望ましい。

SPF、DKIM のいずれかのみを導入する場合は、「(解説) 基本対策事項 6.2.2(1)-3 a)「DKIM」について」を参考に、SPF、DKIM の機能の違い等を踏まえた上で選択するとよい。

- **基本対策事項 6.2.2(1)-3 b)「受信側の対策」について**

受信側の対策を行うことによって、なりすましと判定した電子メールをいわゆる迷惑メールフォルダへの格納や、電子メールサーバ上での破棄等が可能となり、受信側である機関等がなりすましメールによる被害に遭うリスクを低減させることができる。

送信ドメイン認証技術による受信側の対策としては、受信した電子メールに対し送信ドメイン認証に基づくなりすまし判定を行い、なりすましと判定した場合には、受信した電子メールの DMARC ポリシーに従って受信を拒否することや隔離すること等が考えられる。また、受信した電子メールが送信ドメイン認証技術を用いておらず、送信ドメイン認証に基づくなりすまし判定が行えない場合は、受信を拒否することや、隔離し安全性を確認した上で受信すること等の対策を行うことが重要である。

なお、送信ドメイン認証技術を使用し、受信側の電子メールサーバによってなりすましと判定したとしても、送信側の設定等によっては、受信側の電子メールクライアントでは判定結果が分からない場合がある。そのため、なりすましと判定した場合には、以下を例とする電子メールの受信者への注意喚起等を行う機能の導入を検討するとよい。

  - 電子メールの件名（Subject）や本文への注意喚起文の挿入
  - 電子メールクライアントの機能によるラベリングやメッセージの表示

- **基本対策事項 6.2.2(1)-3 c)「DMARC ポリシーには、“p=quarantine”又は“p=reject”を設定すること」について**

DMARC ポリシーが”p=none”の場合、受信側に特別な処理を要求しないため、機関等になりすましたメールによって受信側が被害に遭うリスクを必ずしも低減させることができない。そのため、以下の対策を実施する必要がある。

・電子メールを利用していないドメインを“p=reject”に設定する。

・電子メールを利用しているドメインを“p= quarantine”に設定する。

・DMARC レポートを取得し、機関等が送信した電子メールが受信側において SPF、DKIM の認証に失敗するケースを確認して対策する。メーリングリスト、転送

を使用している場合は、対策が必要となる場合がある。解説「基本対策事項 6.2.2(1)-3 a)「DKIM」について」等を参照し、対策を講ずること。

・認証に失敗するケースが少ないことを確認し、“p=reject”に設定する。

なお、上記の設定は、すべての電子メールについて有効とすること。

電子メールを利用しているドメインについて、DMARC 導入当初等でやむをえず、”p=none”に設定する場合も、DMARC レポートを取得、確認のうえ、一年以内に全ての電子メールについて“p= quarantine”又は“p=reject”を設定することが望ましい。

あわせて、DMARC によって認証された電子メールの視認性を向上させる BIMI（Brand Indicators for Message Identification）を導入することが望ましい。送信側が BIMI を設定すると、受信側の BIMI に対応する電子メールクライアントに送信側のロゴの表示ができるため、正規のドメイン名を用いて機関等が送信した電子メールであることが視覚的に分かりやすくなり、類似のドメイン名を用いてなりすまされた電子メールと容易に区別できるようになる。

- **基本対策事項 6.2.2(1)-3 b)「SPF、DKIM の両方による対策を行う必要がある」について**

電子メールの送信側では SPF、DKIM のいずれかのみを導入している可能性があるため、電子メールの受信側である機関等においてはどちらでも対応できるように SPF、DKIM の両方を導入する必要がある。

- **基本対策事項 6.2.2(1)-4「必要に応じて、S/MIME 等の電子メールにおける電子署名」について**

外部に一斉送信する電子メールに、組織の電子証明書で電子署名をすることは、電子メールのなりすまし防止の観点から効果的である。

また、通常のメールについては、職員等に電子証明書を配布し、電子署名を付与することにより、電子メールクライアントによっては、同時に電子メールを自動的に暗号化することが可能となるというメリットもある。

なお、電子メールのなりすまし防止策としては、本基本対策事項の他に、送信ドメイン認証技術を利用する「基本対策事項 6.2.2(1)-3」を挙げている。

送信ドメイン認証技術はドメイン名単位で電子メールが詐称されているかどうかを確認できる。一方、S/MIME は送信者と受信者が一対一で電子メールが詐称されているかどうかを確認できる。送信ドメイン認証技術と S/MIME では、認証の対象が異なる等の違いがあり、一対一で電子メールが詐称されているかどうかの確認が必要な場合等は、本基本対策事項を検討するとよい。

- **基本対策事項 6.2.2(1)-5「政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能」について**

本基本対策事項は、職員等が遵守事項 8.1.1(5)(b)の遵守を支援する機能を設けることを求めている。

政府ドメイン名を取得できない場合については、「（解説）遵守事項 8.1.1(5)(b)「政府ドメイン名を取得できない場合」について」を参照のこと。

- **基本対策事項 6.2.2(1)-6 a)「SMTP によるサーバ間通信を TLS により保護」について**

  メールサーバ間通信である SMTP によるサーバ間通信には、データを保護する仕掛けがないことから、これを TLS により保護することが、インターネット上でのデータの盗聴及び改ざんの防止に有効である。

  ただし、相手先サーバが TLS に対応していない場合は、通常の SMTP で送受信することになる。相手先が TLS に対応しているかを確認した後に TLS 接続を確立する STARTTLS（RFC3207）を用いた SMTP サーバが普及しているが、STARTTLS は、中間者攻撃により TLS の使用を妨害されるダウングレード攻撃に弱いことが知られている。これを克服する仕組みとして MTA-STS（SMTP MTA Strict Transport Security、RFC8461）や TLSRPT（SMTP TLS Reporting、RFC8460）が普及しつつあるので、導入を検討することも考えられる。また、MTA-STS を導入した場合であっても、DNS キャッシュポイズニング攻撃等により DNS レコードを偽の情報に書き換えられることによって、STARTTLS を無効化される可能性がある。この攻撃への対策としては、DNSSEC が必須となるが、DNS キャッシュポイズニング攻撃等により DNS レコードを偽の情報に書き換えられる可能性を低減できる DANE（DNS-based Authentication of Name Entities）を導入することが考えられる。

  なお、SMTP による電子メール転送は複数のサーバを経由することがあり、最終的な受信先のサーバまでの通信が全て保護されることは必ずしも保証されない点に留意しなければならない。確実に保護するべきデータは、電子メールの送信者があらかじめ暗号化等の対策を行った上で送信する必要がある。

- **基本対策事項 6.2.2(1)-6 b)「S/MIME 等の電子メールにおける暗号化及び電子署名」について**

  S/MIME は電子メール自体に暗号化等を行うものであり、電子メールクライアント側で処理されるセキュリティ機能である。このため、送受信する相手側の電子メールクライアント側も S/MIME に対応している必要がある。

6.2.3 ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。さらに、ウェブサーバにおけるウェブアプリケーションについては、6.6「アプリケーション・コンテンツ」を参照のこと。

遵守事項

(1) ウェブサーバの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用すること。

(b) 情報システムセキュリティ責任者は、ウェブサーバからの不用意な情報漏えいを防止するための措置を講ずること。

(c) 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を行う主体を限定すること。

(d) 情報システムセキュリティ責任者は、インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。

【 基本対策事項 】

＜6.2.3(1)(a)関連＞

6.2.3(1)-1 情報システムセキュリティ責任者は、ウェブサーバが備える機能のうち、必要な機能のみを利用するために、以下を全て含むウェブサーバの管理や設定を行うこと。

a) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とすること。

b) ディレクトリインデックスの表示を禁止すること。

c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限すること。

d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持すること。

＜6.2.3(1)(b)関連＞

6.2.3(1)-2 情報システムセキュリティ責任者は、ウェブサーバからの不用意な情報漏えいを防止するために、以下を全て含むウェブサーバの管理や設定を行うこと。

a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かないこと。

b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除すること。

c) ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

＜6.2.3(1)(c)関連＞

6.2.3(1)-3 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を担当するアカウントの限定として、以下を全て含むウェブサーバの管理や設定を行うこと。

a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えないこと。

b) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除すること。

6.2.3(1)-4 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。

a) ウェブコンテンツの更新の際は、**専用の端末**を使用して行うこと。

b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限すること。

c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、**情報セキュリティを確保した管理**を行うこと。

＜6.2.3(1)(d)関連＞

6.2.3(1)-5 情報システムセキュリティ責任者は、通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を全て含むウェブサーバの実装を行うこと。

a) **TLS 機能を適切に用いる**こと。

b) TLS 機能のために必要となるサーバ証明書には、**利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局**（証明書発行機関）により発行された電子証明書を用いること。

c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された**「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定**すること。

（解説）

- **基本対策事項 6.2.3(1)-1 a)「CGI 機能」について**

CGI 機能において、外部からの文字列に基づいて実行されるスクリプト等は脆弱性の原因となり易い部分であり、細心の注意を払って脆弱性の無いスクリプト等のみを設置しなければならない。そのため、本基本対策事項は、サーバに設置するスクリプト等は必要最低限のものに限定することを求めている。

- **基本対策事項 6.2.3(1)-1 b)「ディレクトリインデックスの表示を禁止する」について**

ウェブサーバの機能であるディレクトリインデックスの表示機能とは、ウェブサイトの公開対象となるディレクトリが、ファイル名を指定しない形式の URL（すなわち、例えば「https://exmaple.go.jp/directory_name/」の形式）又は「index.html」等の所定

のファイル名を指定した形式の URL によってアクセスされたときに、当該ディレクトリに存在するファイル名の一覧を自動的に生成して表示する機能である。万が一、公開するつもりのないファイルがディレクトリに混入していた場合、ディレクトリインデックス機能が有効であると、外部から容易にそのファイル名を見つけられてしまい、アクセスされてしまう。本来、公開対象のディレクトリには、非公開にすべきファイルが混入していてはならないところであるが、念のため、本基本対策事項は、ディレクトリインデックスの表示機能を無効にすることを求めている。

- **基本対策事項 6.2.3(1)-1 c)「不要な機能を制限する」について**

  不要な機能の典型的な例としては、管理者画面の機能が挙げられる。ウェブコンテンツ作成ツールや CMS（Content Management System）には、コンテンツを編集する管理者向けのログイン画面を有するものがある。このログイン画面がインターネットから閲覧可能であると、管理者のパスワードを破って不正にログインされ、ウェブサイトのコンテンツを改ざんされるリスクを生じさせる。管理者画面は、機関等内からのアクセスのみを許可し、インターネットからの利用を制限することを求めている。その他の不要な機能として制限すべき例として、アクセス解析の機能がインターネットから閲覧できるようになっている場合等が挙げられる。

- **基本対策事項 6.2.3(1)-4 a)「専用の端末」について**

  ウェブコンテンツを管理する端末では、ウェブコンテンツの管理に関係する作業のみを行い、その作業に関係の無いウェブサイトを閲覧しない、セキュリティ対策が不十分な USB メモリを利用しないなど、情報セキュリティを確保した運用をする必要がある。また、ウェブサーバのみでなく、ウェブコンテンツを管理する専用の端末においても、不正プログラム対策やソフトウェアに関する脆弱性対策を行うことが重要である。

- **基本対策事項 6.2.3(1)-4 c)「情報セキュリティを確保した管理」について**

  ウェブコンテンツを更新する際の主体認証情報について、パスワードを設定する場合は「（解説）基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照し強固なパスワードを設定する、多要素主体認証方式で主体認証を行う機能を設けるなどにより、情報セキュリティを確保することが求められる。また、ウェブコンテンツの更新に利用する識別コードや主体認証情報は、他の情報システムの認証で使用しているものを使い回さない、ウェブコンテンツを更新する者以外に知らせない、複数の更新を実施する者で共有しないなどの情報セキュリティを確保した管理が求められる。

- **基本対策事項 6.2.3(1)-5 a)「TLS 機能を適切に用いる」について**

  ウェブサーバに TLS 機能を搭載することにより、利用者が当該ウェブサーバのサイトを「https://」で始まる URL でアクセスできるようになる。「https://」で始まる URL のページ（以下「セキュアページ」という。）へのアクセスは、ブラウザからウェブサーバへの入力及びウェブサーバからブラウザへの出力が自動的に暗号化されて送受信される。

  盗聴による情報の漏えいを防止するには、盗聴を防ぐべき情報を出力するウェブペー

ジがセキュアページとなっている必要がある。また、盗聴を防ぐべき情報を利用者に入力させるウェブページを設ける場合には、入力された情報の送信先となる URL がセキュアページとなっていることが必要であり、かつ、利用者に情報を入力させるウェブページ(入力欄が設置されている画面)自体もセキュアページとなっている必要がある。

ウェブサーバに TLS 機能を搭載することは、当該ウェブサーバが正当なサーバである（偽のサーバでない。）ことを確認できる手段を利用者に提供することにもなる。利用者は、当該サイトを「https://」で始まる URL でアクセスし、エラーなく正常に表示されたことで、当該サーバが当該ドメイン名の正当なサイトのものであると確認することができる。

なお、TLS で配信されるページにおいて、TLS を使わないコンテンツが含まれていると、利用者がフィッシング等の被害に合うリスクがあるため、TLS で配信されるページにおいて、TLS を使わないコンテンツを含めてはならない。また、TLS 機能を用いるに当たっては、使用するバージョンの脆弱性に関する最新の情報も踏まえ、適切に使用する必要がある。

従来、サービス利用者の個人に関する情報を保護することが特に求められていたが、さらに今日では、全ての情報について、インターネット上の通信経路において第三者による盗聴や改ざんから守り、国民や外部組織が不利益を被らず安心して利用できるようにすることが求められている。このための対策として、ウェブサイト全体に対する TLS 適用が有効であり、本対策は、外国の政府機関や民間企業のウェブサイトにおいても取組が進められている。

利用者が「http://」から始まる URL を入力した場合であっても常に TLS でアクセスさせるためには、以下の全ての対策を実施するとよい。

- ブラウザからの TLS を使わないアクセス要求に対しては、TLS によるサービスへ自動的にリダイレクトする。
- HSTS（HTTP Strict Transport Security：RFC6797）を用いて、上記のリダイレクト以降の要求は全て TLS にすることをブラウザに伝達する。

- **基本対策事項 6.2.3(1)-5 b)「利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局」について**

TLS 機能を用いるには、ウェブサーバ側に「サーバ証明書」と呼ばれる電子証明書の設置が必要であり、サーバ証明書はそれを発行する「認証局」から取得する必要がある。

本基本対策事項は、サーバ証明書をどの認証局から取得するかの選択において、「利用者が事前のルート証明書のインストールを必要とすることなくその正当性を検証できる認証局」を選択することを求めている。それ以外の認証局を選択した場合、利用者のウェブブラウザには、サーバ証明書の正当性検証ができないことを示す警告やエラー画面が表示されることになる。この警告やエラー画面は、事前に当該認証局の自己署名証明書をブラウザにルート証明書としてインストールすることによって解消することができる。しかし、一般に、利用者によるルート証明書のインストールは安全に行うことが容易でないものであり、利用者に危険を伴うルート証明書のインストールを強い

るのはそもそも避けるべきことである。そのため、本基本対策事項は、利用者にルート証明書のインストールを求めなくても、警告やエラー画面が現れることなく、正常にTLS 通信ができるよう、適切に認証局を選択してサーバ証明書を取得することを求めている。

なお、ウェブサーバの利用が機関等内の管理された端末からのアクセスに限定されている場合には、対象となる全ての端末に対して事前に安全な方法でルート証明書をインストールすることも可能であるから、そのような管理がなされている場合には、当該ウェブサーバで使用するサーバ証明書として、機関等で独自に用意した認証局から発行されたものを用いることができる。

- **基本対策事項 6.2.3(1)-5 c)「「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定」について**

CRYPTREC が発行している「TLS 暗号設定ガイドライン」は、TLS 通信での安全性と相互接続性のバランスを踏まえた TLS サーバの設定方法を示すものである。

このガイドラインでは、「高セキュリティ型」、「推奨セキュリティ型」、「セキュリティ例外型」の 3 段階の設定基準に分けて、各々の要求設定が示されており、どの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みてサーバ管理者が選択するものとされている。

「推奨セキュリティ型」は、利用例に「電子申請等、企業・国民と役所等との電子行政サービスを提供する場合」とあるように、一般的な利用形態で使うことを想定した設定基準であり、安全性又は相互接続性についての特段の要求がなければ選択することが強く勧められている。

他方、「高セキュリティ型」は、情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に悪影響を及ぼすと予想される情報を、安全性を優先して TLS 通信を行うような場合に選択すべき設定基準である。また、「セキュリティ例外型」は、システム等の制約上、安全性が低いプロトコルの利用を全面禁止することが現実的ではなく、安全性上のリスクを受容してでも当該プロトコルを継続利用せざるを得ないと判断される場合にのみ採用すべき設定基準である。

ガイドラインは、巻末に付録として「チェックリスト」を提供しており、ここに、設定基準ごとに満たすべき要求設定として「プロトコルバージョン設定」、「サーバ証明書設定」、「暗号スイート設定」の具体的な基準が示されているので、これに従うことで、容易に適切な TLS 設定を行うことができる。

情報システムセキュリティ責任者は、TLS を導入するシステムの特性に応じて、どの設定基準が相応しいかを決定し、その設定基準に対応する要求設定に従ったサーバ設定を、「チェックリスト」を活用して確認するなどして、適切に行うことが求められる。

また、ガイドラインは、サーバ証明書の作成・管理について注意すべきことや、委託先のサーバ（PaaS/SaaS）を利用する場合の注意点を示し、また、「さらに安全性を高めるために」として、HTTP Strict Transport Security（HSTS）の設定有効化その他を推奨している。これらについても併せて検討することが望ましい。

参考：CRYPTREC「TLS 暗号設定ガイドライン」（CRYPTREC GL-3001-3.1.1）
（https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.1.1.pdf）

6.2.4 ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS：Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールで使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、機関等が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバの適切な管理が必要である。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある（SaaS 系のクラウドサービスを利用する場合を除く）。

遵守事項

(1) DNS の導入時の対策

(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

(b) 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

(c) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

【 基本対策事項 】

＜6.2.4(1)(a)関連＞

6.2.4(1)-1 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システムの名前解決を提供するコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。

a) コンテンツサーバを冗長構成にすること。

b) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行うこと。

c) ISP 等が提供するマネージド DNS サービスや DDoS 対策サービスを利用すること。

d) UDP 及び TCP の両方でサービスを提供すること。

＜6.2.4(1)(b)関連＞

6.2.4(1)-2 情報システムセキュリティ責任者は、**機関等外からの名前解決の要求に応じる必要性**があるかについて検討し、必要性がないと判断される場合は必要であれば機関等内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずること。

a) キャッシュサーバの設定でアクセス制御を行うこと。

b) ファイアウォール等でアクセス制御を行うこと。

6.2.4(1)-3 情報システムセキュリティ責任者は、**DNS キャッシュポイズニング攻撃**から保護するため、以下を例とする措置を講ずること。

a) **ソースポートランダマイゼーション**機能を導入すること。

b) **DNSSEC 検証**を有効にすること。

＜6.2.4(1)(c)関連＞

6.2.4(1)-4 情報システムセキュリティ責任者は、機関等内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする**当該コンテンツサーバで管理する情報の漏えいを防止するための措置**を講ずること。

a) 外部向けのコンテンツサーバと別々に設置すること。

b) ファイアウォール等でアクセス制御を行うこと。

（解説）

- **基本対策事項 6.2.4(1)-1 a)「冗長構成」について**

コンテンツサーバは、冗長構成にすることが一般的である。その際には、ネットワーク障害等を考慮して各々のコンテンツサーバをそれぞれ異なるネットワークに配置する、災害等を考慮して物理的に離れた建物や遠隔地に設置するなど、情報と情報システムに要求される可用性の確保に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用等も、遠隔地への設置による冗長化の措置の例である。

また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。

- **基本対策事項 6.2.4(1)-2「機関等外からの名前解決の要求に応じる必要性」について**

不特定の DNS クライアントからの名前解決の要求に応じるキャッシュサーバはオープンリゾルバと呼ばれる。オープンリゾルバは、存在しないホスト名の名前解決の問合せを大量に送信することで当該ホスト名の名前解決に関係する DNS サーバの過負荷を狙うランダムサブドメイン攻撃（DNS 水責め攻撃）や、送信元 IP アドレスを偽った問合せを大量に送信することで応答を攻撃対象に送り付け、サービス不能の状態にすることを狙う DNS リフレクター攻撃といったサービス不能攻撃等の踏み台として悪用される危険性がある。そのため機関等で利用するキャッシュサーバが機関等外からの名前解決の要求に応じる必要性があるか検討する必要がある。

- **基本対策事項 6.2.4(1)-3「DNS キャッシュポイズニング攻撃」について**

  DNS キャッシュポイズニング攻撃とは、DNS のキャッシュサーバに偽の応答をキャッシュさせることで、利用者のアクセスを攻撃者が用意したサイト等に誘導する攻撃である。この攻撃により、例えば、利用者は正しい URL のウェブサイトに接続しているつもりでも、偽の情報により不正なウェブサイトに誘導されるといった被害を受ける可能性がある。

  なお、DNS キャッシュポイズニング攻撃対策として、名前解決における IP フラグメンテーションの発生を回避するため、コンテンツサーバ及びキャッシュサーバの UDP メッセージサイズの上限を 1,232 バイトに設定することが望ましい。

  参考：DNS flag day 2020
  （https://www.dnsflagday.net/2020/index-ja.html）

- **基本対策事項 6.2.4(1)-3 a)「ソースポートランダマイゼーション」について**

  ソースポートランダマイゼーションとは、キャッシュサーバからコンテンツサーバへの問合せに使用される UDP ポート番号をランダム化する技術である。UDP ポート番号をランダム化することにより、攻撃者がキャッシュポイズニング攻撃を行う際に UDP ポート番号の推測を困難にすることができ、攻撃の成功確率を低下させることが可能となる。

  なお、キャッシュサーバからコンテンツサーバへの問合せにおいて、通信経路上のファイアウォールにてネットワークアドレス変換（NAT）処理が行われる場合、UDP ポート番号が推測可能な形に変換されてしまうことのないように留意が必要である。

- **基本対策事項 6.2.4(1)-3 b)「DNSSEC 検証」について**

  DNSSEC では、コンテンツサーバによって応答に電子署名が追加され、キャッシュサーバがその署名を検証することで、応答が改ざん等されているか確認することができる。DNSSEC は、公開鍵暗号技術を用いるため、その導入には情報の提供側であるコンテンツサーバと情報の問合せ側であるキャッシュサーバの双方に対応が必要となる。国民等への信頼できるサービスの提供と、機関等の情報セキュリティ向上の観点から、政府ドメイン名を管理するコンテンツサーバにおける DNSSEC 署名、及び機関等のキャッシュサーバに対する円滑な DNSSEC 検証の導入が望ましい。

- **基本対策事項 6.2.4(1)-4「当該コンテンツサーバで管理する情報の漏えいを防止するための措置」について**

  コンテンツサーバにおいて、機関等内のみで使用する名前の解決を提供する場合、内部のみで使用している名前情報を機関等外の者が取得できないようにすることを求めている。

遵守事項

(2) DNS の運用時の対策

(a) 情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報について**サーバ間で整合性を維持**すること。

(b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理する**ドメインに関する情報が正確であることを定期的に確認**すること。

(c) 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

【 基本対策事項 】

＜6.2.4(2)(b)関連＞

6.2.4(2)-1 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。

a) コンテンツサーバと DNS ルートサーバのそれぞれの当該ドメインに関する情報が正しく同一であること。

b) コンテンツサーバとホスト（ホスティングサービス等のホストを含む。）のそれぞれの当該ドメイン（サブドメインを含む。）に関する情報が正しく同一であること。

＜6.2.4(2)(c)関連＞

6.2.4(2)-2 情報システムセキュリティ責任者は、キャッシュサーバにおいて、ルートヒント（DNS ルートサーバの情報が登録されたファイル等）の更新の有無を定期的（３か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持すること。

6.2.4(2)-3 情報システムセキュリティ責任者は、キャッシュサーバにおいて DNSSEC を利用する場合、電子署名を検証する起点となる DNSSEC トラストアンカーを最新の状態に保つため、自動更新機能を有効にする又は更新の有無を定期的（３か月に一度程度）に確認すること。

（解説）

- **遵守事項 6.2.4(2)(a)「サーバ間で整合性を維持」について**

  複数台のコンテンツサーバでドメインに関する情報を保有し管理する場合に、各コンテンツサーバ間でドメインに関する情報の整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバで管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバが管理するドメインに関する情報も更新するといった方法が考えられる。

  なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG（Transaction Signature）の利用等が考えられる。

- **遵守事項 6.2.4(2)(b)「ドメインに関する情報が正確であることを定期的に確認」につい**

て

ドメイン名に関する情報には、機関等が当該ドメイン名の委任元（親ゾーン）の登録機関（レジストリ・レジストラ）に登録する情報（以下本解説において「登録情報」という。）と機関等のコンテンツサーバに設定・管理する情報（以下本解説において「設定情報」という。）の２種類が存在する。いずれの情報も利用者のウェブサイトのアクセスや電子メールの送受信において参照されるため、正確性を保つことが重要である。

① 登録情報に関する対策

ドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加されることで、利用者のアクセスが不適切なウェブサイト等に誘導されるドメイン名ハイジャックと呼ばれる攻撃が知られている。このような攻撃への対策として、登録機関に情報を登録する際のなりすましの防止、登録機関が提供する各種ロックサービスの利用等が挙げられる。

なりすましの防止としては、第三者に容易に推測できるパスワードを利用しない、パスワードの使い回しをしないなどの対策に加え、二段階認証やクライアント証明書等、登録機関が提供する追加の認証手段の利用等が挙げられる。

登録機関が提供する各種ロックサービスとしては、JP ドメイン名（政府ドメイン名を含む。）については、意図しない登録情報の変更を制限するためのレジストリロックサービスや意図しないドメイン名の移転を防ぐための指定事業者変更ロックサービスが利用可能な場合があるため、当該サービスの利用を検討してもよい。

ドメイン名を廃止する場合には、登録機関にドメイン名の廃止申請を行い、当該ドメイン名が確実に廃止されていることを確認するとともに、当該ドメイン名に関する機関等のコンテンツサーバの設定情報を確認し、削除することが重要である。これに加えて、ドロップキャッチ（ドメイン名の登録期限が切れたタイミングで、第三者がそのドメイン名を新たに取得してしまうこと。）対策の観点から、当該ドメイン名を利用しなくなった後でも一定期間（少なくとも１年以上）ドメイン名登録を継続することや、可能な限りウェブサイトからのリンクを解除することなどが求められる。

② 設定情報に関する対策

設定情報については、コンテンツサーバの設定誤りや削除漏れ、不正な改ざん等が発生していないかを定期的に確認することにより、正確性を保つことが重要である。具体的には、以下を例とする情報の記述内容等を確認することが求められる。

- ホストの IP アドレス情報を記述する A（AAAA）レコード
- 送信先電子メールサーバ名を記述する MX レコード
- 電子メールの送信者が詐称されていないかを受信者側で認証するために必要な、SPF レコード等を記述する TXT レコード
- 当該ホストにおいて、ホスティングサービス等を利用する際に記述する CNAME レコード
- サブドメインの名前解決のために問い合わせるべきコンテンツサーバを指定する NS レコード

なお、電子メールにおけるなりすまし防止の観点からも、管理するドメイン名の SPF レコード等を記述する TXT レコードの内容が正確であるか否かを確認する必要がある。また、ホスティングサービス等の利用終了後に残ったままになっている設定情報を利用して意図しないウェブサイト等を公開されてしまうサブドメインテイクオーバー・NS テイクオーバーと呼ばれる攻撃を避けるため、当該ウェブサイト等の利用を終了する場合には、当該ホスティングサービス等の利用開始時に設定した CNAME や NS レコードを全て削除・修正することが重要である。

加えて、クラウドサービスによっては、使用中のサービスにテイクオーバー可能な DNS 設定がないかを利用者において確認できるツールを公開している場合もあるので、そのようなツールを活用することも有用である。

6.2.5 データベース

目的・趣旨

本款における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び職員等の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.4.4「IPv6 通信回線」、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

(1) データベースの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

(b) 情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

(c) 情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

(d) 情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

(e) 情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

【 基本対策事項 】

＜6.2.5(1)(a)関連＞

6.2.5(1)-1 情報システムセキュリティ責任者は、必要に応じて情報システムの管理者とデータベースの管理者を別にすること。

6.2.5(1)-2 情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

6.2.5(1)-3 情報システムセキュリティ責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること。

＜6.2.5(1)(c)関連＞

6.2.5(1)-4 情報システムセキュリティ責任者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。

a) 一定数以上のデータの取得に関するログを記録し、警告を発すること。

b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発すること。

＜6.2.5(1)(d)関連＞

6.2.5(1)-5 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。

6.2.5(1)-6 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。

a) ウェブアプリケーションファイアウォールの導入

b) データベースファイアウォールの導入

＜6.2.5(1)(e)関連＞

6.2.5(1)-7 情報システムセキュリティ責任者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

（解説）

- **遵守事項 6.2.5(1)(b)「データベースに格納されているデータにアクセスした利用者を特定」について**

一般的に、データベースの使用形態は図 6.2.5(1)-1 のように、データベースから見たアクセス主体が「人間の利用者」となる場合と、「中間アプリケーションサーバ」となる場合の２つのモデルに分けられる。中間アプリケーションサーバを利用するモデルでは、中間アプリケーションサーバ用にデータベースアクセス用のアカウントを作成して運用する構成となるのが通常である。この構成では、データベースのログにはアクセス主体が中間アプリケーションサーバとして記録されることになるため、不正な操作が行われた場合に実際には誰が操作をしたものかをデータベースのログのみからでは特定できない可能性がある。そのため中間アプリケーションサーバにおいて、データベースの利用者とデータベースへの操作要求とを紐づけてログを取得し、利用者を特定できるようにする必要がある。

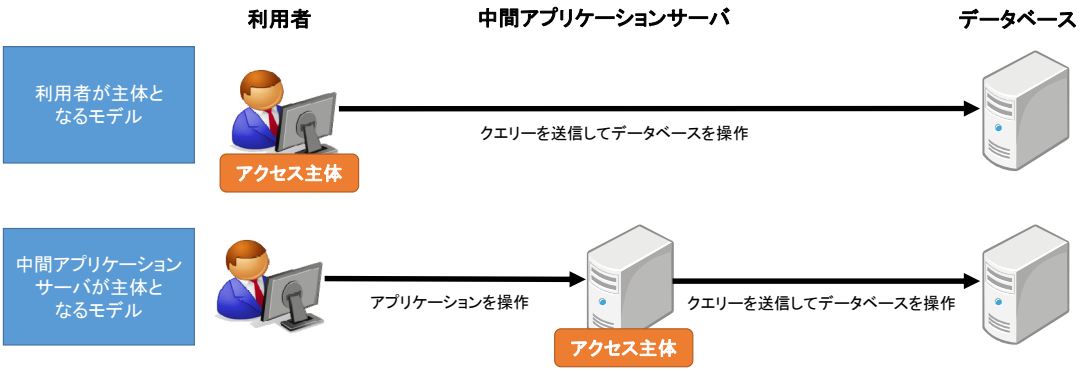


図 6.2.5(1)-1　データベース利用形態モデル

- **遵守事項 6.2.5(1)(c)「データの不正な操作を検知」について**

  通常業務では取り扱わないような大量のデータを取得することや業務時間外にデータの操作を行う等の不正な操作を、SIEM や UEBA（User and Entity Behavior Analytics）等を導入することによってシステム的に検知する方法を用いるとよい。なお、データベースのログを目視によって確認する方法も考えられるが、人手に依存する方法は確認漏れ等が発生する可能性があり望ましくない。

  データの不正な操作が発生したときの影響や操作ログの量等を踏まえて、システム的に検知する方法か人手に依存する方法かを選択するとよい。

- **遵守事項 6.2.5(1)(e)「適切に暗号化」について**

  データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット・デメリットがあるため、適切な方式を選択することが望ましい。

- **基本対策事項 6.2.5(1)-1「情報システムの管理者とデータベースの管理者を別に」について**

  データベースの管理者は、データベースに格納されるデータの管理、アカウント・権限の管理、ネットワーク環境の構成等の管理を行う。多数の管理者権限を保持するアカウントを奪取された場合、甚大な被害を受けるおそれがあるため、重要な情報を管理するデータベースの管理者の特権を他の管理者と分掌することが望ましい。

- **基本対策事項 6.2.5(1)-3「権限の不適切な付与」について**

  業務の遂行、データベースの運用・管理等をするに当たって不必要なデータに対するアクセス権の付与のほか、他のアカウントに対して権限を付与する権限の付与等がある。

6.3 複合機・特定用途機器

6.3.1 複合機・特定用途機器

目的・趣旨

機関等においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は、機関等内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、機関等においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システムが利用されている。これらの特定用途機器がインターネットに接続する機能を備える、いわゆる IoT 機器となっている場合が多くある。例えばネットワークカメラシステムの構成要素である機器のうちインターネットに接続する機能を備えるカメラや、環境モニタリングシステムの構成要素である機器のうちインターネットに接続する機能を備えるセンサーが挙げられる。近年、IoT 機器の脆弱性をついた攻撃が数多く発生しており、IoT 機器が踏み台となって他の情報システムへの攻撃に利用されるなど、社会的問題となってきている。このため、これらの機器に対する情報セキュリティ対策が必要となる。

したがって、複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講ずることが重要である。

遵守事項

(1) 複合機

(a) 情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。

(b) 情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。

(c) 情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

【 基本対策事項 】

＜6.3.1(1)(a)関連＞

6.3.1(1)-1 情報システムセキュリティ責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。

＜6.3.1(1)(b)関連＞

6.3.1(1)-2 情報システムセキュリティ責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施すること。
b) 複合機が備える機能のうち利用しない機能を停止すること。
c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用すること。
d) 複合機をインターネットに直接接続しないこと。
e) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行うこと。
f) 利用者ごとに許可される操作を適切に設定すること。

＜6.3.1(1)(c)関連＞

6.3.1(1)-3 情報システムセキュリティ責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、委託先との契約時に委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

（解説）

- **基本対策事項 6.3.1(1)-1「「IT 製品の調達におけるセキュリティ要件リスト」を参照」について**

遵守事項 5.2.1(3)(c)及び基本対策事項 5.2.1(3)-9 に規定されている「IT 製品の調達におけるセキュリティ要件リスト」には、複合機について一般的に想定される「セキュリティ上の脅威」が記載されているため、それらが自身の運用環境において該当する場合には対抗する必要がある。当該リストには、「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

なお、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、利用環境や複合機に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

- **基本対策事項 6.3.1(1)-2 a)「適切なセキュリティ設定」について**

自身の利用環境における脅威に対抗するために、運用前に複合機のセキュリティ機能の設定値が適切な値となっていることを確認する必要がある。例えば、管理者パスワードが初期設定のままでないか、イメージスキャナで複合機内部に保存したデータへのアクセス制御設定が適切であるかなどを確認する必要がある。

- **基本対策事項 6.3.1(1)-2 b)「利用しない機能を停止」について**

  運用において必要としていない機能が利用者の意図に反して動作していた場合、セキュリティ対策が不十分になっていることが考えられる。対策が不十分である場合は、情報セキュリティインシデントが発生するおそれがあるため、複合機が備える機能を把握し、運用上不必要な機能については、運用前に停止した状態にする必要がある。また、脆弱性が指摘されている通信プロトコルについても停止すべきである。

- **基本対策事項 6.3.1(1)-2 c)「操作パネルで利用者認証が成功した者のみ印刷が許可される機能」について**

  複合機の設置環境によっては、印刷された文書が第三者に閲覧される可能性がある。そのような場合には、印刷の際に複合機内部に一旦データを保存し、複合機本体の操作パネルで主体認証に成功した者だけが印刷できるように設定するなどの対策を講ずる必要がある。

- **基本対策事項 6.3.1(1)-2 e)「ファイアウォール等の利用により適切に通信制御を行う」について**

  トナー残量の通知や遠隔地からの状態監視等の遠隔保守サービス等を利用する場合には、インターネットを介して外部と通信する必要が生じる。その際には必要最小限の通信のみを許可するようにする必要がある。また、ファイアウォール等の通信制御を行うための機器に例外的な設定を行う場合には、その設定によって脆弱性が生じないようにする必要がある。

- **基本対策事項 6.3.1(1)-2 f)「利用者ごとに許可される操作を適切に設定する」について**

  様々な機能を備えている複合機では、利用者ごとに許可される操作権限の管理が重要である。例えば、ファクシミリで受信したデータを複合機内部に保存する場合のデータの読み出し権限等を適切に設定していない場合には、情報の漏えいにつながる可能性がある。

- **基本対策事項 6.3.1(1)-3「別の手段で対策を講ずる」について**

  内蔵電磁的記録媒体の全領域完全消去機能を備えていない複合機については、調達元の機関等において内蔵電磁的記録媒体の全ての情報を抹消することが困難であるため、委託先と情報の抹消サービスを契約するなどの情報の漏えいへの対策を講ずることが必要となる。

遵守事項

(2) IoT 機器を含む特定用途機器

(a) 情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、**当該機器の特性に応じた対策を講ずる**こと。

【 基本対策事項 】

＜6.3.1(2)(a)関連＞

6.3.1(2)-1 情報システムセキュリティ責任者は、特定用途機器の特性に応じて、以下を全て含む対策を講ずること。ただし、使用している特定用途機器の機能上の制約により講ずることができない対策を除く。

a) 特定用途機器について、**主体認証情報を初期設定から変更**した上で、適切に管理すること。

b) 特定用途機器にアクセスする**主体に応じて必要な権限を割り当て、管理**すること。

c) 特定用途機器が備える機能のうち**利用しない機能を停止**すること。

d) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットに接続させず、インターネットに接点を有する情報システムに接続する場合は、当該特定用途機器がインターネットに接続されないように適切に通信制御を行うこと。

e) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により**適切に通信制御を行う**こと。

f) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、**バージョンアップやセキュリティパッチの適用**、アクセス制御等の対策を講ずること。

g) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視すること。

h) 特定用途機器を使用しない場合は、**特定用途機器の電源をオフ**にすること。

i) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消すること。

（解説）

- **遵守事項 6.3.1(2)(a)「当該機器の特性に応じた対策を講ずる」について**

例えば、テレビ会議システム、IP 電話システム等は機関等 LAN システムを経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。また、これら情報システムを構成する機器が内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。このような脅威に対抗するために、情報システムや端末、サーバ装置に対して定

められた遵守事項や基本対策事項を参考にして、IoT 機器を含む特定用途機器の対策を講ずる必要がある。

特定用途機器の導入時に注意すべき点として、特定用途機器の導入後にサポートが適切に行われるかどうかという点や、特定用途機器の設定を適切に変更できるかどうかという点が挙げられる。

サポートが適切に行われなかったり、設定を適切に変更できなかったりする等の場合、必要なセキュリティ対策を講ずることが困難になる可能性がある。そのため、導入時にサポートの提供や設定変更が可能な範囲や IoT 機器の使用期間全般に渡ってファームウェアやドライバーの更新が保証されることについて仕様に盛り込むなどして、必要なセキュリティ対策を講ずることができる特定用途機器を調達する必要がある。

IoT 機器等については、2025 年３月に、セキュリティ要件適合評価及びラベリング制度（JC-STAR）の運用が開始されている。詳細については、「(解説) 基本対策事項 4.3.1(1)-2「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」について」を参照のこと。また、セキュリティ対策に係るガイドラインや手引書が公表されていることから、必要に応じて参考にするとよい。

参考：IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン」
（http://www.iotac.jp/wg/security）
（https://www.soumu.go.jp/main_content/000428393.pdf）

参考：情報処理推進機構（IPA）「IoT 開発におけるセキュリティ設計の手引き」
（https://www.ipa.go.jp/security/iot/iotguide.html）

参考：情報処理推進機構（IPA）「ネットワークカメラシステムにおける情報セキュリティ対策要件に関するチェックリスト　第２版」
（https://www.ipa.go.jp/security/jisec/about/knowledge/nw-camera.html）

- **基本対策事項 6.3.1(2)-1 a)「主体認証情報を初期設定から変更」について**

特定用途機器の一部の機種は、遠隔保守や外部ネットワークからの機能利用を目的として、インターネット回線等の通信回線を経由して、特定用途機器へログインする機能を有しているものがあるが、この機能を悪用したサイバー攻撃の手法が存在する。具体的には、工場出荷時に設定される初期のパスワードを変更せずに運用している特定用途機器を標的とし、一般によく使われる初期の識別コードとパスワードの組合せを用いて辞書攻撃を行い、不正なログインを試行するものである。特定用途機器の運用保守等のために、インターネット回線等の通信回線を介してログインを行う必要がある場合は、このような攻撃を受けることを想定して、特定用途機器の運用開始前に初期設定されているパスワード等の主体認証情報を「(解説) 基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照し強固なパスワード等に変更することが重要である。

また、管理者アカウントに対して不正なログインが行われた場合の影響は一般アカウントと比較して大きくなることが考えられるため、管理者アカウントの主体認証は多要素主体認証方式等の強固な認証技術を用いることが望ましい。

- **基本対策事項 6.3.1(2)-1 b)「主体に応じて必要な権限を割り当て、管理」について**

特定用途機器の導入及び運用においては、設定変更などを行う管理者権限と、状態の確認や閲覧等を行うだけの一般権限のアカウントを別にして使い分けることで、内部不正や誤操作の防止につながる。さらに管理者権限の利用を許可するアクセス元を制限するといった他の対策と複合的に組み合わせることによって、悪意のある第三者によって設定変更されたり攻撃に利用されたりする可能性を低減することが可能である。

- **基本対策事項 6.3.1(2)-1 c)「利用しない機能を停止」について**

「(解説) 基本対策事項 6.3.1(2)-1 a)「主体認証情報を初期設定から変更」について」にも示すとおり、インターネット回線等の通信回線を経由して特定用途機器へ不正なログインを試行する攻撃手法においては、Telnet のような汎用のプロトコルを利用したサービスが標的とされることがある。インターネット上には、グローバルアドレスに対してポートスキャンを行いレスポンスを返すサービスや、特定用途機器の情報を公表しているサイトが存在しており、そのようなサイトにセキュリティの弱いサービスや特定用途機器が登録されてしまうと、サイバー攻撃を企図する者の標的となるおそれがある。

このような攻撃手法への対抗策として、特定用途機器が備える機能を把握し、Telnet サービスや FTP サービス等のうち利用していないものは全て停止し、不正なログイン試行を無効化することが重要である。また、必要のある場合を除き、遠隔から起動する機能についても停止することが重要である。

なお、特定用途機器の中にはサービスや遠隔から起動する機能の停止などの設定を変更することができないものも存在するため、導入に当たっては、係る設定を変更できることを仕様に盛り込むといったことを検討するとよい。一方で、代替の特定用途機器がなかったり、既に導入済みで更改まで使用を継続しなければならない場合も考えられる。そういった場合には適切に通信制御を行う等の対策を講ずることが重要である。

- **基本対策事項 6.3.1(2)-1 e)「適切に通信制御を行う」について**

特定用途機器への不正アクセスが生じると、不正プログラムへの感染、不正操作、情報窃取等の不正行為が行われるおそれがある。そのため、特定用途機器への通信制御を適切に実施し、不正アクセスを防止するとともに、不正行為が行われた場合の被害範囲を限定するなどの対策を行うことが重要である。

特定用途機器への通信制御は、例えば以下の方法により実施することが考えられる。

- 特定用途機器に実装されている通信制御機能を有効にする。
- 接続しているファイアウォール等で通信制御を行う。
- ルータ等を利用して、特定用途機器に直接グローバル IP アドレスを割り当てない。

- **基本対策事項 6.3.1(2)-1 f)「バージョンアップやセキュリティパッチの適用」について**

  特定用途機器のソフトウェアの脆弱性を放置すると、脆弱性を悪用されるおそれがあることから、脆弱性が公表された場合は、ソフトウェアのバージョンアップやセキュリティパッチの適用により脆弱性対策を速やかに講ずることが重要である。特定用途機器の機種によっては、脆弱性対策が困難なものがあることに留意が必要である。そのような特定用途機器がサイバー攻撃の踏み台にされるなどし、意図せず攻撃に加担してしまう可能性も考えられる。このような問題を回避するためには、特定用途機器の導入に当たって、ベンダがセキュリティパッチを提供していること、ベンダが外部から報告を受けた脆弱性に対応するだけでなく開発時に利用したライブラリ等の脆弱性についても対応可能な体制となっていること等を仕様に盛り込むことを検討するとよい。
  また、運用保守の委託先に対して、運用している特定用途機器の脆弱性に対応する必要があることを認識させること、さらに、特定用途機器のバージョンアップやセキュリティパッチの適用手順、実施に当たってのサービスへの影響を把握させることも重要である。

  調達元の機関等で対処できないような機器の場合には、特定用途機器の調達に当たって保守契約締結の必要性等について検討することも重要である。

- **基本対策事項 6.3.1(2)-1 h)「特定用途機器の電源をオフ」について**

  使用していない特定用途機器をインターネットに接続した状態で放置した場合、気が付かない間に特定用途機器が乗っ取られてしまい、不正利用される可能性がある。特に長期休暇中等の長期間に渡って放置した場合は、特定用途機器のソフトウェアに関する新たな脆弱性が発見された場合にセキュリティパッチ等による対策が遅れることや、不正な主体認証の試行が多く繰り返されること等によって、不正利用される可能性が高まることが考えられる。

  そのため、特定用途機器を使用しない場合は特定用途機器の電源をオフにすることによって、不正アクセス等のサイバー攻撃を受ける機会を減らすことや、既に受けていたとしても悪用される時間を少なくすることが重要である。

6.4 通信回線

6.4.1 通信回線

目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

(1) 通信回線の導入時の対策

(a) 情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた**適切な回線種別を選択**し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。

(b) 情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

(c) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

(d) 情報システムセキュリティ責任者は、職員等が**通信回線へ情報システムを接続する際に**、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。**機関等内通信回線へ機関等支給以外の端末を接続する際**も同様とする。

(e) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**が接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

【 基本対策事項 】

＜6.4.1(1)(a)(b)関連＞

6.4.1(1)-1 情報システムセキュリティ責任者は、**通信回線を経由した情報セキュリティインシデント**の影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限、**拠点等の地理的事情**に応じて、以下を例とする通信経路の分離を行うこと。

a) 外部等との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離すること。
b) 通信が必要な単位でセグメントを分割し、セグメント間の通信を必要最小限とするアクセス制御を行うこと。
c) 他の情報システムから独立した専用の通信回線を構築すること。

＜6.4.1(1)(c)関連＞

6.4.1(1)-2 情報システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、TLS、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。

＜6.4.1(1)(d)関連＞

6.4.1(1)-3 情報システムセキュリティ責任者は、機関等内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。

a) 情報システムの MAC アドレス等の端末を一意に識別できる情報により接続機器を識別すること。
b) クライアント証明書により接続機器の認証を行うこと。

＜6.4.1(1)(e)関連＞

6.4.1(1)-4 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。

a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設けること。
b) 通信回線及び通信回線装置を冗長構成にすること。
c) 端末等が情報システムと通信可能な代替手段を整備すること。

（解説）

- **遵守事項 6.4.1(1)(a)「適切な回線種別を選択」について**

通信回線に利用する物理的な回線（通信事業者の回線・公衆無線 LAN 回線 等）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ対策が異なることから、適切な回線を選択することが求められる。

例えば、通信経路の破壊等による可用性への影響を回避することを目的として仮想的な通信回線を複数の通信経路により構築する場合、物理的にも分離された通信経路上にそれぞれ仮想的な通信回線を構築しなければ、本来求められる可用性の維持に関する要件を満たすことにはならない。

- **遵守事項 6.4.1(1)(d)「通信回線へ情報システムを接続する際に」・「機関等内通信回線**

へ機関等支給以外の端末を接続する際」について

要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む。）を要管理対策区域で機関等内通信回線に接続することについては、本項に加えて、遵守事項 6.1.2(1)(c)及び遵守事項 6.1.3(2)(d)にて、接続することの可否の判断、可と判断する場合における安全管理措置に関する規定及び許可手続を求めている。

- **遵守事項 6.4.1(1)(e)「要安定情報を取り扱う情報システム」について**

要安定情報を取り扱う情報システムについては、「（解説）基本対策事項 5.2.1(3)-7「要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システムについて」を参照のこと。

- **基本対策事項 6.4.1(1)-1「通信回線を経由した情報セキュリティインシデント」について**

情報セキュリティ対策が十分でない端末等から侵入すると、悪意ある攻撃者は、機関等内通信回線に接続している端末やサーバ装置、通信回線装置などの機器等の脆弱性を含めた情報を収集し、侵入可能な端末等からアクセスが可能な通信経路を用いて侵入範囲の拡大（ラテラルムーブメント：横方向の侵害）を行う。

通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするためには、通信回線の構成や特性、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限、拠点等の地理的事情に応じて、例えば拠点などのセグメントごとに通信回線を分離することや、拠点などのセグメント間における通信を必要最小限にするためのアクセス制御をする、いわゆるマイクロセグメンテーションの観点を踏まえた対策が重要である。

- **基本対策事項 6.4.1(1)-1「拠点等の地理的事情」について**

地方の拠点や海外の拠点などは、情報セキュリティ責任者による管理が行き届きにくく、情報セキュリティ対策が十分でない場合がある。このため例えば、国外の拠点等から当該情報システムに対して直接通信する必要性がない場合は、相互に直接通信ができないよう通信経路を分離し情報セキュリティインシデントが発生した際に、他の拠点等へ影響を及ぼさない構成にするなどを検討するとよい。

- **基本対策事項 6.4.1(1)-1 a)「外部等との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築」について**

セグメント間のラテラルムーブメントを困難にする観点から、内部ネットワークと他のセグメントとの間に DMZ を構築することで、仮に外部から侵入されても、アクセスが可能な範囲を限定的にすることも考えられる。

- **基本対策事項 6.4.1(1)-1 b)「セグメント間の通信を必要最小限とするアクセス制御を行う」について**

通信が必要な単位でセグメントを分割し、他のセグメントとの間に次世代ファイアウォール等を設置することや仮想ネットワーク技術を活用する等により、セグメント間の通信を必要最小限とするアクセス制御を行うことが考えられる。

- **基本対策事項 6.4.1(1)-1 c)「専用の通信回線を構築」について**

  リスクを検討した結果、他の情報システムと共通的な通信回線を利用すると情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするなどの構成を採用することが考えられるが、過剰なセキュリティ要件とならないように、閉鎖的な通信回線とする必要性を見極めることが重要である。例えば、通信回線を VLAN 等で論理的に分割し、分割された論理的な通信回線ごとに情報セキュリティを確保することで十分要件を満たすのであれば、費用や維持管理の面でメリットがある。このように情報セキュリティ以外の観点とのバランスをとって要件を定めることが重要である。

- **基本対策事項 6.4.1(1)-4 b)「通信回線及び通信回線装置を冗長構成にする」について**

  高い可用性が求められる情報システムを構築する場合は、大規模災害の発生を想定し、通信回線を冗長構成にすることが望ましい。また、機関等の施設から外部に敷設する通信回線の管路についても、例えば、異なる通信事業者が敷設した通信回線による複数の経路で構築することで、災害を受けた際に復旧にかかる時間が短縮されるなどの効果が期待される。

遵守事項

(2) 機関等外通信回線の接続時の対策

(a) 情報システムセキュリティ責任者は、機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

(b) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の不正な通信の有無を監視するための措置を講ずること。

(c) 情報システムセキュリティ責任者は、保守又は診断のために、機関等外通信回線から機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保すること。

(d) 情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。

【 基本対策事項 】

＜6.4.1(2)(a)関連＞

6.4.1(2)-1 情報システムセキュリティ責任者は、機関等内通信回線に、インターネット回線や公衆通信回線等の機関等外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。

a) ファイアウォール、WAF、プロキシやリバースプロキシ、次世代ファイアウォール等により通信制御を行うこと。

b) 通信回線装置による特定の通信プロトコルの利用を制限すること。

c) IDS/IPS により不正アクセスを検知及び遮断すること。

d) 不審なメールの受信や不審なウェブサイトへのアクセスを遮断すること。

e) サンドボックス型の標的型攻撃対策をすること。

6.4.1(2)-2 インターネット回線等の機関等外通信回線を用いたクラウドサービスへのアクセスがある場合、クラウドサービスへのアクセスを可視化し、適切な利用を把握するための対策を検討すること。

＜6.4.1(2)(b)関連＞

6.4.1(2)-3 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の不正な通信の有無を監視するため、以下を例とする監視を行うこと。

a) 機関等外と通信回線で接続している箇所における外部からの不正アクセスの監視

b) 不正プログラム感染や踏み台に利用されること等による機関等外への不正な通信の監視

c) 不正プログラム等の感染による拡大防止のため、機関等内通信回線の機器等に

おける不審な通信の監視

6.4.1(2)-4 情報システムセキュリティ責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定め、監視記録を保存し、適切に保護、管理すること。

＜6.4.1(2)(c)関連＞

6.4.1(2)-5 情報システムセキュリティ責任者は、機関等外通信回線からの保守又は診断のための機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスのセキュリティ確保のために、以下を全て含む対策を講ずること。

a) リモートメンテナンスを行う主体の認証において多要素主体認証を用いること。
b) リモートメンテナンスを行う端末等を制限するアクセス制御
c) 主体認証によるアクセス制御
d) 通信内容の暗号化による秘匿性の確保
e) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにすること。

（解説）

- **遵守事項 6.4.1(2)(c)「リモートメンテナンス」について**

インターネット等の外部ネットワークである機関等外通信回線から機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスについては、職員等が業務アプリケーション等のみへアクセスできるリモートアクセスとは違い、インターネット等の外部ネットワークから機関等内通信回線へのアクセスが前提となることを想定している。インターネット等の外部ネットワークから機関等内通信回線に接続された機器等に対して直接アクセスが可能な場合、インターネット等の外部ネットワークから攻撃を受ける可能性が高くなり、悪意ある攻撃者からのなりすまし等による不正アクセスを受けると、当該機器を踏み台に利用するなどして、他の機器等への被害が拡大するおそれがある。

したがって、インターネット等の外部ネットワークから機関等内通信回線へ接続した機器に対してリモートメンテナンスをする場合は、主体に対して強固な認証技術を用いることやアクセスする端末を限定するなど十分な情報セキュリティを確保する必要がある。

なお、機関等内通信回線に接続した機器等に対して行われるリモートメンテナンスについては、職員等が直接行うリモートメンテナンスのみならず、業務委託として行うリモート運用やリモート保守も含まれることに注意が必要である。また、機関等内通信回線に接続した機器等に対してインターネット等の外部ネットワークから直接接続して行うリモート監視についても同様の情報セキュリティを確保するための措置を講ずることが重要である。

業務委託として行うリモート運用やリモート保守に関しては、4.1「業務委託」の遵守事項も併せて遵守する必要があるため、参照すること。

- **遵守事項 6.4.1(2)(d)「契約時に取り決めておく」について**

  公衆通信回線サービスを使用する場合においては、回線の利用規約等に記載されているセキュリティレベルやサービスレベルを合意した上で当該回線を選択する必要がある。役務提供契約で通信回線を利用するなど、機関等において直接回線を調達しない場合については、通信回線に求めるセキュリティレベル及びサービスレベルについて、役務提供事業者と合意形成する必要がある。

- **基本対策事項 6.4.1(2)-1「外部からの不正アクセスによる被害を防止する」について**

  機関等内通信回線に、インターネット等の外部ネットワークを接続する場合は、外部からの攻撃による脅威から情報システムや情報を守るため、通信回線に対して必要な対策を講ずる必要がある。必要な対策としては、外部からの不正なアクセス等による侵入を防ぐための対策（入口対策）のみならず、侵入されてしまったとしても情報を外部へ漏えいさせないための対策（出口対策）が重要である。入口対策としては、外部からの攻撃や侵入に対する通信を制御及び遮断するため、ファイアウォール、WAF、リバースプロキシ、IDS/IPS などを利用することが有効である。出口対策としては、外部から侵入させてしまったとしても情報を外部へ漏えいさせないために、ファイアウォールやプロキシ、IPS、次世代ファイアウォールなどを用いて外部への通信を制限及び遮断することが有効である。さらに、入口対策と出口対策の両方で有効なサンドボックス型の標的型攻撃対策を利用することも考えられる。情報システムセキュリティ責任者は、インターネット等の外部ネットワークと接続する場合は、外部からの不正アクセスによる被害を防止するため入口対策と出口対策の両方の対策が含まれるよう必要な対策を組み合わせて講ずる必要がある。

  なお、外部からの不正アクセスによる被害を防止するため対策については、通信回線で行う入口対策や出口対策のほか、端末やサーバ装置等に対して行う内部対策も重要であるため、7.2.4「標的型攻撃対策」を参考に必要な対策を実施することが重要である。

- **基本対策事項 6.4.1(2)-1 a)「次世代ファイアウォール」について**

  次世代ファイアウォールは、機関等内通信回線に接続した端末やサーバ装置等が、インターネット等の外部ネットワークと通信する際に、出口対策として外部ネットワークと通信できるアプリケーションを制限するために有効である。例えば、機関等において許可していないファイル共有サービスにファイルをアップロードしようとする通信を遮断することなどが可能となる。

- **基本対策事項 6.4.1(2)-1 d)「不審なメールの受信や不審なウェブサイトからのアクセスを遮断する」について**

  不審なメールの受信を遮断する手段としては、電子メールフィルタリングのスパムフィルタ機能などが考えられる。また、不審なウェブサイトへのアクセスを遮断する手段としては、ウェブサイトフィルタリングや URL フィルタリングなどの機能が考えられる。これらのような手段を組み合わせて、外部からの不正アクセスによる侵入を防止するとよい。

- **基本対策事項 6.4.1⑵-1 e)「サンドボックス型の標的型攻撃対策」について**

サンドボックスとは、攻撃されても影響を与えない仮想環境を用意し、不審なファイル等を仮想環境にて動作させ異常がないかを分析するものである。サンドボックス型ではない標的型攻撃対策では、不正プログラムの検出方法として主にシグネチャを用いて検出するが、シグネチャに登録されていない不正プログラムや未知の不正プログラムに関しては、検出できない問題があった。そこで、サンドボックス型の標的型攻撃対策として、不審なファイル等の動作等を隔離された仮想環境において確認し、ファイルの動作等に異常がないかの確認を行うことで、未知の不正プログラムに対してもその挙動において判断することが可能となる。したがって、外部からの不正アクセスによる被害を防止するための対策として、サンドボックス型の対策を検討するとよい。

- **基本対策事項 6.4.1⑵-2「クラウドサービスへのアクセスを可視化し、適切な利用を把握するための対策」について**

インターネット回線等の機関等外通信回線を用いてクラウドサービスへアクセスを許可している場合、どの主体がどのような端末を用いてどのようなクラウドサービスへアクセスし、取り扱う情報に対してどのような操作を行ったか等のクラウドサービスを利用する状況を把握することが重要である。クラウドサービスの利用状況を把握することで、情報セキュリティインシデントの可能性を把握することや、未然に防止することが可能となるため、適切な利用を把握するための対策を検討する必要がある。

適切な利用を把握するための対策としては、CASB 等の“クラウドサービスの利用度の可視化”や“アクセス制御”などの機能を持つ製品や SASE などの利用を検討することが考えられる。

- **基本対策事項 6.4.1⑵-3 a)「外部からの不正アクセスの監視」について**

外部からの不正アクセスを監視する場合、ファイアウォールのログを監視するだけでは外部からの正常な通信と異常な通信を全て区別することはできない。そこで、IDS/IPS や WAF によって監視することが重要である。

また、外部へ公開しているウェブサーバ等に関しては、外部から短い間隔での大量の認証要求が発生するなどの通常とは異なる現象を監視することも重要である。

- **基本対策事項 6.4.1⑵-3 b)「機関等外への不正な通信の監視」について**

機関等内通信回線から機関等外への不審な通信を監視する場合は、ファイアウォールやプロキシ、次世代ファイアウォールなどを監視することが有効である。ただし、ファイアウォールについては、機関等内から機関等外へ特定のポート等を用いた通信は監視することができるものの、多く使われる HTTPS 等の通信について監視することは困難である。そのため次世代ファイアウォール等を用いてアプリケーションごとの不正な通信の有無を監視することが有効である。また、プロキシ等による外部への通信の成功の可否を監視することも考えられる。監視する例としては、不正なウェブサイトへのアクセスや通常通信しないアドレスとの通信、通常よりも多い頻度での通信の観測などが考えられる。

- **基本対策事項 6.4.1(2)-3 c)「機器等における不審な通信の監視」について**

  悪意ある攻撃者により機関等内通信回線へ侵入された場合、攻撃者は機関等内通信回線に接続されている端末やサーバ装置、通信回線装置などの機器等の脆弱性を含めた情報を収集する。そのため、機関等内通信回線の中で普段は起こり得ない機器同士の通信が発生してないかなど監視をすることが有効である。

- **基本対策事項 6.4.1(2)-5 a)「多要素主体認証を用いる」について**

  多要素主体認証については、基本対策事項 7.1.1(1)-2 及び「(解説)遵守事項 8.1.3(2)(b)「リモートアクセスに対し多要素主体認証を行うこと」について」を参照のこと。

- **基本対策事項 6.4.1(2)-5 b)「端末等を制限するアクセス制御」について**

  機関等外通信回線からのリモートメンテナンスを行う場合、主体のなりすましなどによる不正アクセス等のリスクが高まる。そのため、強固な主体認証による対策のみならず、リモートメンテナンスを行う端末等を制限し、不正アクセス等の脅威に対抗するための措置を講ずる必要がある。リモートメンテナンスを行う端末等を制限する方法としては、証明書を用いた端末等の認証のほか、事前に端末等を一意に識別できる情報を登録し認証する方法などが考えられる。なお、端末等を一意に識別できる情報を用いる場合、MAC アドレスなどの偽装や情報窃取が容易な情報だけを用いてはならない。

遵守事項

(3) 通信回線の運用時の対策

(a) 情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及び**アクセス制御の設定の確認及び見直しを行う**こと。

(b) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の**不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをする**こと。

(c) 情報システムセキュリティ責任者は、保守又は診断のために、機関等外通信回線から機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認による見直しをすること。

(d) 情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。

【 基本対策事項 】

＜6.4.1(3)(c)関連＞

6.4.1(3)-1 情報システムセキュリティ責任者は、機関等外通信回線から保守又は診断のためのリモートメンテナンスに関する以下を全て含む事項について、定期的な確認による見直しを行うこと。

a) リモートからのアクセスが必要な主体

b) リモートメンテナンスを行う端末

c) ファイアウォール等の通信制御のための機器に例外的な設定を行った場合の設定

（解説）

- **遵守事項 6.4.1(3)(a)「アクセス制御の設定の確認及び見直しを行う」について**

機関等内通信回線にインターネット等の外部ネットワークを接続する場合は、経路制御及びアクセス制御の設定を定期的な確認により見直すことが重要である。特にファイアウォールや WAF、次世代ファイアウォールなどの通信を制御する機器等の設定に関しては、機関等の業務の変化やクラウドサービス、テレワークといった情報システムの利用環境の変化等により、通信の内容が変化することを踏まえて、適切に設定を見直す必要がある。

また、アクセス制御の設定の見直しにより、設定条件を変更又は設定の不備を修正する場合は、情報システムセキュリティ責任者が指名した監督者の監視の下で設定変更等を実施することや、機械的なチェック機能を設けるなど設定や修正によるミス等を防止するための対策を行うことが重要である。なお、設定変更を行う場合は、当該通信

回線に接続されている情報システムの情報システムセキュリティ責任者にも事前の連絡及び結果を通知する必要がある。

- **遵守事項 6.4.1(3)(b)「不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをする」について**

  通信内容については、機関等の業務の変化やクラウドサービス、テレワークといった情報システムの利用環境の変化等により変化することが考えられる。そのような変化に応じて、監視対象や監視方法などが適切であるか定期的な確認により見直しを行う必要がある。見直しの結果、監視対象や監視のための設定、監視方法などに不備があった場合は、修正することが求められる。

6.4.2 通信回線装置

目的・趣旨

インターネット等の外部ネットワークからアクセス可能な通信回線装置においては、ソフトウェアの脆弱性を悪用された不正アクセスの被害を受ける可能性がある。そのため、通信回線装置におけるソフトウェアの脆弱性対策は、迅速かつ適切に対処することが求められる。また、通信回線装置は端末やサーバ装置などの経路制御やアクセス制御に用いるため、情報システムの構築時からリスクを十分検討し、必要なセキュリティ対策を実施しておく必要がある。さらに運用時においても、脅威動向の変化等に応じた継続的な対策を実施することが重要である。

遵守事項

(1) 通信回線装置の導入時の対策

(a) 情報システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないようにすること。

(b) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めること。

(c) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。

(d) 情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。

【 基本対策事項 】

＜6.4.2(1)(a)関連＞

6.4.2(1)-1 情報システムセキュリティ責任者は、第三者による通信回線及び物理的な通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。

a) 要管理対策区域に設置すること。

b) 物理的な通信回線装置を施錠可能なラック等に設置すること。

c) 機関等の施設内に敷設した通信ケーブルを物理的に保護すること。

d) 物理的な通信回線装置の操作ログを取得すること。

＜6.4.2(1)(b)関連＞

6.4.2(1)-2 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

（解説）

- **遵守事項 6.4.2(1)(b)「ソフトウェアに関する事項」について**

  通信回線装置としての機能や動作を明確にするとともに、ソフトウェアの脆弱性に関する対策を確実なものとするために、通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。通信回線装置の更新ソフトウェアの提供を受けた際は、更新ソフトウェアに脆弱性を解決するための修正が含まれている可能性があるため、更新内容を確認し修正された脆弱性についての影響度と緊急度を判断し、影響度や緊急度に応じて更新ソフトウェアを適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。ただし、更新ソフトウェアに新たに機能が追加されるなど通信に影響を与えるような更新がなされる場合は、適用することへの影響を十分に考慮し、切り戻しに備えてバックアップを用意するなどの対策を講じた上で適用する必要がある。

- **遵守事項 6.4.2(1)(c)「適切なセキュリティ対策を実施する」について**

  機関等内通信回線にインターネット等の外部ネットワークを接続する場合は、不正アクセス等のリスクを低減するためのネットワーク構成等を構築する必要がある。また、通信回線装置を設定する際は、当該通信回線装置を提供している提供者が提示している推奨設定や業界標準、ベストプラクティス等を参照し、通信回線装置の各種設定を行い、設定の不備等がないようにする必要がある。

- **遵守事項 6.4.2(1)(d)「ソフトウェアに関連する公開された脆弱性について対策を実施する」について**

  通信回線装置の利用を開始する前に通信回線装置で利用するソフトウェアに関連する脆弱性情報を確認し、脆弱性が公開されていた場合は、セキュリティパッチを適用するなどの対策を実施する必要がある。

  ソフトウェアの脆弱性については、7.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

遵守事項

(2) 通信回線装置の運用時の対策

(a) 情報システムセキュリティ責任者は、通信回線装置の運用・保守に関わる作業等により**通信回線装置の設定変更等を実施する場合**は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

(b) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**を構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

(c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講ずること。

【 基本対策事項 】

＜6.4.2(2)(c)関連＞

6.4.2(2)-1 情報システムセキュリティ責任者は、通信回線装置が動作するために必要な**ソフトウェアの状態を定期的に調査**（脆弱性の確認を含む。）し、許可されていないソフトウェアがインストールされているなど、**不適切な状態**にある通信回線装置を認識した場合には、改善を図ること。

（解説）

- **遵守事項 6.4.2(2)(a)「通信回線装置の設定変更等を実施する場合」について**

通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報システムセキュリティ責任者が指名した監督者の監視の下で設定変更等を実施することや、機械的なチェック機能を設けるなど設定変更等によるミス等を防止するための対策を行うことが重要である。なお、設定変更を行う場合は、当該通信回線に接続されている情報システムの情報システムセキュリティ責任者にも事前の連絡及び結果の通知を行う必要がある。

- **遵守事項 6.4.2(2)(b)「要安定情報を取り扱う情報システム」について**

要安定情報を取り扱う情報システムについては、「(解説) 基本対策事項 5.2.1(3)-7「要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システム」について」を参照のこと。

- **基本対策事項 6.4.2(2)-1「ソフトウェアの状態を定期的に調査」について**

通信回線の重要性、想定される脅威及び機器の特性等から調査の必要性及び調査の間隔を検討する必要がある。例えば、基幹回線等の重要な通信回線を構成する機器、ファイアウォールのようにインターネット等と直接接続されている機器、頻繁にソフトウェアがアップデートされるような機器等は、ソフトウェアの脆弱性等の調査の必要性が高く、より短期間に繰り返し調査を実施することが考えられる。また、そのよう

な重要な通信回線を構成する機器に関しては、脆弱性に関する情報を製品ベンダや脆弱性情報提供サイト等から通知を受け取るようにするとともに、内閣官房国家サイバー統括室やJPCERT/CC、情報処理推進機構（IPA）等からの注意喚起も参照し、常に確認できるようにする必要がある。必要性が低いと判断された機器についても、利用するソフトウェア等の脆弱性が報告された場合や、通信回線の構成変更が発生した場合に随時調査することが望ましい。

- **基本対策事項 6.4.2(2)-1「不適切な状態」について**

  不適切な状態とは、許可されていないソフトウェアがインストールされている、ソフトウェアの脆弱性が公開されているが適切な対策が取られていない、定められたソフトウェアが動作するための設定が適切でないなどの状態のことを指す。

遵守事項

(3) 通信回線装置の運用終了時の対策

(a) 情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての**情報を抹消するなど適切な措置**を講ずること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.4.2(3)(a)「情報を抹消するなど適切な措置」について**

抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。通信回線装置内にも、設定情報や通信ログ等の情報が保存されていることから、サーバ装置及び端末と同様に運用終了時に留意が必要である。

通信回線装置は通信事業者からリース提供されることがあり、その場合は通信回線の運用終了に伴い通信事業者に装置を返却することになるため、通信回線装置の初期化の手順等本項を遵守するための方法について、通信事業者に確認する必要がある。

6.4.3 無線 LAN

目的・趣旨

無線 LAN は、有線の通信回線及び通信回線装置において想定される脅威に加え、電波を利用するために有線と比較して通信の傍受等が容易であることに起因する脅威への対策が必要である。

なお、本款の遵守事項の他、6.4.1「通信回線」及び 6.4.2「通信回線装置」において定める導入時の対策に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 無線 LAN 環境導入時の対策

(a) 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

＜6.4.3(1)(a)関連＞

6.4.3(1)-1 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、情報システムの分類に基づき、以下の対策を講ずること。

【基本セキュリティ対策】以下を全て含む対策を講ずること。

a) **無線 LAN 通信の暗号化**

b) 無線 LAN 回線利用申請手続の整備

c) **無線 LAN 機器の管理**手順の整備

d) **来訪者等に提供する無線 LAN によるインターネット接続回線**と業務で使用する機関等 LAN システムの分離

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とする対策を講ずること。

e) **IEEE 802.1X による無線 LAN へのアクセス主体の認証**

（解説）

- **基本対策事項 6.4.3(1)-1 a)「無線 LAN 通信の暗号化」について**

暗号化方式として、例えば WPA3 Enterprise（Wi-Fi Protected Access 3 Enterprise）や WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式を選択することが考えられる。WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信を妨害できたりするという脆弱性が報告されており、利用してはならない。他の暗号化方式においても同様の問題が起こる可能性があ

るため、最新の情報に従い適切な方式や設定値を選択することが求められる。

- **基本対策事項 6.4.3(1)-1 c)「無線 LAN 機器の管理」について**

  無線 LAN 機器の管理については、以下の例が考えられる。

  - 無線 LAN 機器の電波出力・周波数チャンネル等の管理
  - 無線 LAN 機器のファームウェア等の更新作業
  - 管理外の無線 LAN アクセスポイント、端末の検出及び除去

  なお、無線 LAN 回線を構築する場合は、以下を参考にするとよい。

  参考：総務省「国民のためのサイバーセキュリティサイト」の「職場での対策」、「システムを“利用”する人向けの対策」にある「安全な無線 LAN の利用」のページの解説
  （https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/03/）

- **基本対策事項 6.4.3(1)-1 d)「来訪者等に提供する無線 LAN によるインターネット接続回線」について**

  機関等の無線 LAN 環境を来訪者等に提供する場合、来訪者等が機関等 LAN システムに侵入することによって、情報の漏えいや改ざんなどが行われる可能性がある。そのため、来訪者等に提供する無線 LAN と機関等 LAN システムをルータ等の通信回線装置によって論理的に分離する対策等が考えられる。

  なお、来訪者等に向けた無線 LAN によるインターネット接続回線を提供する際には以下を参考にするとよい。

  参考：総務省「無線 LAN ビジネスガイドライン」
  （https://www.soumu.go.jp/main_content/000620877.pdf）

  参考：総務省「公衆 Wi-Fi 提供者向け セキュリティ対策の手引き」
  （https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）

- **基本対策事項 6.4.3(1)-1 e)「IEEE 802.1X による無線 LAN へのアクセス主体の認証」について**

  IEEE 802.1X 認証については、機関等 LAN システム等の無線 LAN において要機密情報を扱う場合は、高度な情報セキュリティ対策を要求する情報システムに該当する場合に限定せず、導入することが望ましい。

  IEEE 802.1X 認証で用いられる EAP の規格について、脆弱性が指摘されている EPA-MD5 や LEAP 等の認証方式もあるため、利用する規格についてセキュリティ上問題が無いか確認する。

  また、偽のアクセスポイントを利用した攻撃等へ対抗するためにも相互認証に対応した規格を利用すること。また、認証に用いる識別符号（識別コード及びパスワード、電子証明書等）の安全な配布方法と運用手順についても整備する。

6.4.4 IPv6 通信回線

目的・趣旨

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷されている。IPv6 通信プロトコルでは、グローバル IP アドレスによるパケットの直接到達性などを考慮する必要があり、設定不備によっては運用者が意図しない IPv6 通信が通信ネットワーク上で動作し、結果として、不正アクセスの手口として悪用されるおそれもある。このため、必要な対策を講じていく必要がある。

遵守事項

(1) IPv6 通信を行う情報システムに係る対策

(a) 情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択すること。

(b) 情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、IPv6 通信による情報セキュリティ上の脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

【 基本対策事項 】

＜6.4.4(1)(b)関連＞

6.4.4(1)-1 情報システムセキュリティ責任者は、以下を全て含む IPv6 通信による情報セキュリティ上の脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

a) グローバル IP アドレスによる直接の到達性における脅威

b) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

c) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

d) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

（解説）

- **基本対策事項 6.4.4(1)-1 a)「グローバル IP アドレスによる直接の到達性における脅威」について**

IPv6 通信を想定して構築する情報システムにおいて、グローバル IP アドレスによる通信パケットの直接到達性における脅威に対抗するために、以下を例に対策を講ずることが考えられる。

- 不正な機器からの経路調査コマンド（traceroute 等）への応答の禁止
- ICMP エコー要求への応答の禁止

- 許可した宛先からのみアクセス可能とするなどの経路制御の設定
- サービス不能攻撃の検知及びフィルタ

- **基本対策事項 6.4.4(1)-1 b)「不正アクセスの脅威」について**

IPv6 の特徴として、アドレスが長いこと、アドレスの省略形が複数パターン存在して一意に定まらない可能性があること、端末が複数の IP アドレスを持つこと等が挙げられる。このため、複雑なアクセス制御の設定が必要になり、設定不備等による不正アクセスにつながるリスクが想定される。

対策としては、外部ネットワークとの通信において、OSI 基本参照モデルのネットワーク層（第３層）及びトランスポート層（第４層）を中心にフィルタリングを行う機能及び断片化された通信の再構築を行う機能を適切に設定すること等、通信機器を流れる通信そのものを制御することが挙げられる。

なお、IPv6 通信を想定して構築する情報システムにおいて、IPv6 のログを取得し、分析する場合は、IPv6 アドレスでは桁数が大幅に増えること等から、IPv6 対応のログの解析ツールを利用することで、IPv6 アドレスの読み間違い等の運用上の作業ミスを軽減するための対策を検討することが望ましい。

- **基本対策事項 6.4.4(1)-1 c)「共存させる際の処理考慮漏れに起因する脆弱性」について**

IPv6 通信プロトコルに対応している端末やサーバ装置には、多様な IPv6 移行機構（デュアルスタック機構、IPv6-IPv4 トンネル機構等）が実装されている。それらの IPv6 移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用に当たっては、セキュリティホールの原因をつくらないよう十分な検討と措置を講ずる必要がある。

例えば、デュアルスタック機構を運用する場合には、IPv4 のプライベートアドレスを利用したイントラネットの情報システムであっても外部ネットワークとの IPv6 通信が可能となるため、デュアルスタック機構を導入したサーバ装置及び端末を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4 トンネル機構を運用する場合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間の IPv6 通信が既設の IPv4 ネットワークを使って可能となるため、機関等のネットワークが外部から攻撃される危険性がある。管理されたサーバ装置及び端末以外のトンネル通信を当該 IPv4 ネットワークに設置されたファイアウォールにて遮断するなど、不適切な IPv6 通信を制御する対策を行う必要がある。

- **基本対策事項 6.4.4(1)-1 d)「IPv6 アドレスの取扱い考慮漏れに起因する脆弱性」について**

IPv4 のみに対応する機器及びソフトウェアが IPv6 ネットワーク上で動作する際、システム内部での IP アドレスの取扱いが IPv4 に依存している場合、IPv6 アドレスが取り扱えない、又はバッファオーバーラン等を引き起こす可能性があるというリスクを認識し、これが無いことを確認するなどが挙げられる。統合認証システムや、システム間連動を行うようなアプリケーションでは、IPv4/IPv6 が混在した状況でも適切なシステム連携を行う必要がある。

また、IPv4 対応システムが IPv6 アドレスに対応するため、IPv6／IPv4 コンバータ等が使用される場合がある。このような場合、内部からは個別の IPv6 アドレスを特定できないため、通信ログの取得やパケットフィルタリング等の機能を実装し運用する際等において留意が必要である。

遵守事項

(2) 意図しない IPv6 通信の抑止・監視

(a) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、**IPv6 通信を抑止するなどの措置**を講ずること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.4.4(2)(a)「IPv6 通信を抑止するなどの措置」について**

複数の機関等の間及び機関等内のみで利用する情報システムについて、通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する必要がある。ただし、当該端末等の OS や OS のバージョン等によって IPv6 通信の機能を停止することが推奨されていない場合は、当該端末等の IPv6 通信の優先度を IPv4 より低くする等、当該端末等の OS や OS のバージョン等において推奨される設定を行う必要がある。

IPv6 通信を想定していない通信回線においては、ファイアウォールや IDS/IPS 等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能なサーバ装置及び端末においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該サーバ装置及び端末への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、サーバ装置及び端末と外部のネットワークとの間に情報システムの利用者や情報システムの運用管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないようサーバ装置及び端末を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。

なお、「政府情報システムに係る IPv6 対応の取組について」（2011 年 11 月 2 日各府省情報化統括責任者（CIO）連絡会議決定）において IPv6 対応の取組を進めることが確認されているが、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を抑止又は遮断するための措置を講ずる必要がある。

6.5 ソフトウェア

6.5.1 情報システムの基盤を管理又は制御するソフトウェア

目的・趣旨

情報システムの基盤を管理又は制御するソフトウェアは、情報システムを制御する上でセキュリティ上の重要な機能を有している。そのようなソフトウェアは悪用や不正アクセスされた場合、被害が広範囲に及ぶ可能性がある。したがって、情報システムの基盤を管理又は制御するソフトウェアを利用する端末やサーバ装置、通信回線装置等及びソフトウェア自体において、必要なセキュリティ対策を実施する必要がある。

本款では、情報システムの基盤を管理又は制御するソフトウェアを利用する場合に求めるセキュリティ対策として、7.1「情報システムのセキュリティ機能」で求めている対策から特に必要と考えられるものを示しており、本款以外に 7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理、7.1.4「ログの取得・管理」で定めるログの取得に係る遵守事項についても併せて遵守する必要があるが、情報システムの基盤を管理又は制御するソフトウェアの機能や仕様等を踏まえて、適切な対策を講ずることが重要となる。

また、当該ソフトウェアを利用する際の操作ミスや設定不備などを防ぐためには、当該ソフトウェアの利用者や管理者が利用するソフトウェアを利用するための手順を整備することも重要である。さらに、情報システムの基盤を管理又は制御するソフトウェアを悪用した攻撃を防ぐにはソフトウェアの脆弱性対策が特に重要となる。当該ソフトウェアに関係する脆弱性に関する情報を製品ベンダや脆弱性情報提供サイト等からの通知を受け取るようにするとともに、公開された脆弱性についての影響度と緊急度に応じてセキュリティパッチ等を適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。脆弱性対策については、7.2.1「ソフトウェアに関する脆弱性対策」を参照し確実な対策を実施することが重要である。

遵守事項

(1) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

(a) 情報システムセキュリティ責任者は、情報セキュリティの観点から**情報システムの基盤を管理又は制御するソフトウェア**を導入する**端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置**を講ずること。

(b) 情報システムセキュリティ責任者は、**利用するソフトウェアの特性を踏まえ**、以下の全ての実施手順を整備すること。

(ア) 情報システムの基盤を管理又は制御するソフトウェアの**情報セキュリティ水準の維持に関する手順**

(イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した**情報セキュリティインシデントを認知した際の対処手順**

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.5.1(1)(a)「情報システムの基盤を管理又は制御するソフトウェア」について**

情報システムの基盤を管理又は制御するソフトウェアは、端末やサーバ装置、ネットワークなどを管理又は制御するための権限を用いてアクセスが可能な機能を有しているソフトウェアを想定しており、当該ソフトウェアが悪用された場合、被害が広範囲に及ぶリスクが高くなる。また、当該ソフトウェアにおいて要機密情報が取り扱われる場合は、当該ソフトウェアを保護することで情報を守る必要がある。したがって、情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及び当該ソフトウェア自体については、必要な措置を講ずる必要がある。なお、情報システムの基盤を管理又は制御するソフトウェアについては、以下のソフトウェアが考えられる。

- 端末やサーバ装置、通信回線装置等を制御するソフトウェア
- 統合的な主体認証を管理するソフトウェア
- ネットワークを制御・管理するソフトウェア
- 資産を管理するソフトウェア
- 監視に関連するソフトウェア
- 情報システムのセキュリティ機能として使用するソフトウェア

- **遵守事項 6.5.1(1)(a)「端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置」について**

情報システムの基盤を管理又は制御するソフトウェアを導入する場合、当該ソフトウェア自体を保護するのみならず、当該ソフトウェアを動作させる端末、サーバ装置、通信回線装置等も保護する必要がある。当該ソフトウェアを保護するための対策としては、以下の各款における規定内容が有効であるため、それぞれに示される対策を行う必要がある。

- 7.1.1「主体認証機能」
- 7.1.2「アクセス制御機能」
- 7.1.3「権限の管理」
- 7.1.4「ログの取得・管理」
- 7.2.1「ソフトウェアに関する脆弱性対策」

特に情報システムの基盤を管理又は制御するソフトウェアを導入する端末やサーバ装置、通信回線装置等及び当該ソフトウェア自体の管理者権限を有する識別コードについては、なりすましによって不正アクセスによる被害を受けた場合、被害が広範囲に及ぶ可能性があることから、原則として多要素主体認証を用いることを検討するとよい。さらに、当該ソフトウェアへのアクセスは必要最小限となるよう、ネットワークセグメントを分離したアクセス制御や当該ソフトウェアのアクセスは認めた主体のみがアクセス可能となるよう制限する他、他のソフトウェアやサービスと連携する機能を有している場合の適切な認証をするなど、アクセス権限を最小限にし、不正なアクセス

がないことを監視するなどの措置も有効である。

- **遵守事項 6.5.1(1)(b)「利用するソフトウェアの特性を踏まえ」について**

  情報システムの基盤を管理又は制御するソフトウェアは、端末やサーバ装置、通信回線装置などを管理又は制御するための権限を用いてアクセスが可能な機能を有しているものを想定しており、そのようなソフトウェアを悪用された場合、被害が広範囲に及ぶリスクが高くなる。

- **遵守事項 6.5.1(1)(b)(ア)「情報セキュリティ水準の維持に関する手順」について**

  情報システムの基盤を管理又は制御するソフトウェアは、情報システムの構成要素を管理又は制御する上で重要な機能を有しているため、セキュリティに関する設定などに関しては不備がないように管理することが重要である。そのため、当該ソフトウェアが管理又は制御する情報システム全体のセキュリティ水準を保つための設定や構成に関しては、文書にすることが重要である。さらに、ソフトウェアを安全に使用及び管理するため、情報システム全体に影響を及ぼすような重要な操作や情報セキュリティに関する設定や構成を変更する際の手順も整備することが重要である。なお、情報システム全体に影響を及ぼす操作や設定変更等を実施する際は、監督者の指揮の下で実施するなどの対策も含めるとよい。

- **遵守事項 6.5.1(1)(b)(イ)「情報セキュリティインシデントを認知した際の対処手順」について**

  情報セキュリティインシデントを認知した際の対処手順に関しては、ソフトウェアの個別の事情に合わせて検討する必要がある。情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアにおいて情報セキュリティインシデントを認知した際は、機関等で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処する必要がある。また、情報セキュリティインシデントが発生すると、当該ソフトウェアが管理又は制御する権限を用いて他の機器等に対して不正なアクセスがなされる等が発生し、被害が広範囲に及ぶ可能性がある。したがって、利用するソフトウェアの仕様や機能等を踏まえて情報セキュリティインシデントを認知した際の対処手順を整備する必要がある。

  なお、統括情報セキュリティ責任者が整備する対処手順（「(解説)遵守事項 2.2.4(1)(b)「対処手順」について」を参照のこと。）が、当該ソフトウェアの事情に応じた内容で整備されているならば、個別に整備しなくても構わない。

遵守事項

(2) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

(a) 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施すること。

(ア) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(イ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

【 基本対策事項 】

＜6.5.1(2)(a)(ア)関連＞

6.5.1(2)-1 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するため、権限設定やアクセス制御、セキュリティ設定が適切であるか定期的な確認をすること。

＜6.5.1(2)(a)(イ)関連＞

6.5.1(2)-2 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアにおいて、脅威や情報セキュリティインシデントを迅速に検知し、対応するため、以下の全ての対策を実施すること。

a) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順に基づく教育の実施

b) 情報セキュリティインシデントを認知した際の対処手順に基づく訓練

（解説）

- **基本対策事項 6.5.1(2)-1「定期的な確認をする」について**

情報システムの基盤を管理又は制御するソフトウェアを管理するための権限や当該ソフトウェアを利用できる識別コードなどについては、適切な付与であることを継続的に確認する必要がある。特に、アクセスが不要となった識別コードは、すみやかに削除又は無効化するなどの対策をする必要がある。また、当該ソフトウェアのセキュリティ設定についても正しく設定されているか定期的に確認する必要がある。例えば、当該ソフトウェアのバージョンアップ等を行った際は、新たな機能が追加されるなどのセキュリティに関する設定が変更になっていないかなどを確認するとよい。

- **基本対策事項 6.5.1(2)-2 a)「情報セキュリティ水準の維持に関する手順に基づく教育の実施」について**

情報システムの基盤を管理又は制御するソフトウェアは、情報システムの構成要素を管理又は制御する上で重要な機能を有しているため、ソフトウェアを安全に使用及び管理する必要がある。当該ソフトウェアを初めて運用管理する職員等や重要な操作を行う職員等に対しては、ソフトウェアの情報セキュリティ水準の維持に関する手順に基づき教育を実施することが重要である。

- **基本対策事項 6.5.1⑵-2 b)「情報セキュリティインシデントを認知した際の対処手順に基づく訓練」について**

  情報システムの基盤を管理又は制御するソフトウェアにて制御又は管理している機器等において、情報セキュリティインシデントが発生した場合に備えて、当該ソフトウェアを利用した対処手順等を定期的に確認する必要がある。対処手順の訓練の方法としては、机上における訓練の他、実機を用いた訓練などの方法があり、どのような手段を用いて確認するかは、対処手順を整備してからの経過時間、対処に係る訓練の度合い等を踏まえて決めるとよい。なお、対処手順に基づく訓練について、2.2.4「情報セキュリティインシデントへの対処」又は 5.3「情報システムの運用継続計画」において他の訓練と一緒に実施している場合は、個別に実施する必要はない。

6.6 アプリケーション・コンテンツ

6.6.1 アプリケーション・コンテンツの作成・運用時の対策

目的・趣旨

機関等では、情報の提供、行政手続、意見募集等の行政サービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。機関等は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を業務委託する場合については、4.1「業務委託」についても併せて遵守する必要がある。

遵守事項

(1) アプリケーション・コンテンツの作成に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための運用規程を整備すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.6.1(1)(a)「アプリケーション・コンテンツ」について**

  行政サービスは、アプリケーションプログラムやウェブコンテンツ等を用いて国民等に提供されている。特にウェブコンテンツでは、機関等以外が提供するコンテンツ（以下「外部コンテンツ」という。）を組み込むことによって、容易に様々な機能を提供することが可能となるが、機関等において外部コンテンツの信頼性を担保することは不可能であることから、このような利用方法には注意が必要である。例えば、外部コンテンツが事前に通知されることなく変更されてしまい、行政サービスの利用者の意図に反して利用者の個人に関する情報が取得される可能性がある。また、外部コンテンツに不正プログラムが組み込まれ、行政サービスの利用者がそれに感染する被害が生じることも考えられる。そのため、ウェブコンテンツでは外部コンテンツを利用しないことが望ましいが、必要があって利用する場合には、これらの脅威に対して適切なセキュリティ対策を実施することが求められる。

- **遵守事項 6.6.1(1)(a)「機関等外の情報セキュリティ水準の低下を招く行為を防止する」について**

  国民等が機関等によって提供される行政サービスを利用する場合、行政サービスの利用によって、利用者の端末が不正プログラムに感染しやすい状況を強制することや、

利用者個人の情報が利用者の意図に反して第三者に提供させられるといった状況を作り出すことは避けなければならない。機関等は、機関等外の情報システム利用者の情報セキュリティ水準を低下させないように留意して、行政サービスのためのアプリケーション・コンテンツを提供する必要がある。

- **遵守事項 6.6.1(1)(a)「運用規程を整備」について**

  統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供に関する運用規程の整備に当たり、遵守事項 6.6.1(2)以降において規定した事項を含める必要がある。

遵守事項

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについてのセキュリティ要件を定め、仕様に含めること。

(b) 職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に掲げる内容を**調達仕様に含める**こと。

【 基本対策事項 】

＜6.6.1(2)(a)関連＞

6.6.1(2)-1 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが**不正プログラムを含まない**ことを確認するために、以下を全て含む対策をセキュリティ要件として仕様に含めること。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いて検査を行い、不正プログラムが含まれていないことを確認すること。

b) 業務委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

6.6.1(2)-2 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが**脆弱性を含まない**ように開発することをセキュリティ要件として仕様に含めること。

6.6.1(2)-3 情報システムセキュリティ責任者は、実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、**実行プログラムの形式でコンテンツを提供しない**ことをセキュリティ要件として仕様に含めること。

6.6.1(2)-4 情報システムセキュリティ責任者は、電子証明書を用いた署名等、提供するアプリケーション・コンテンツの**改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与える**ことをセキュリティ要件として仕様に含めること。

6.6.1(2)-5 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツの利用時に、**脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する**などの**情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求する**ことがないよう、アプリケーション・コンテンツの提供方式を定めて開発することをセキュリティ要件として仕様に含めること。

6.6.1(2)-6 情報システムセキュリティ責任者は、**サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能**がアプリケーション・コンテンツに組み込まれることがないよう、以下を全て含む開発をすることをセキュリティ要件として仕様に含めること。

a) 機関等外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。**必要があって当該機能を含める場合**は、当該機関等外へのアクセスが

情報セキュリティ上安全なものであることを確認すること。

b) 本来のサービス提供に必要のない**機関等外へのアクセスを自動的に発生させる機能**を含めないこと。

（解説）

- **遵守事項 6.6.1(2)(b)「調達仕様に含める」について**

例えば、機関等が何らかのキャンペーンとして啓発コンテンツを提供する際に、その作成を広告会社等に業務委託する場合は、情報システム部門以外の職員等がその業務委託の調達仕様を定めることになると考えられる。このような場合でも、機関等外の情報セキュリティ水準を低下させないよう、前項に掲げるセキュリティ要件を調達仕様に含めることが求められる。

- **基本対策事項 6.6.1(2)-1「不正プログラムを含まない」について**

不正プログラムを含まないようにすべきものは、機関等外の利用者の端末にインストールさせるプログラムの他、利用者に閲覧させるウェブサイトのウェブページも含む。

- **基本対策事項 6.6.1(2)-2「脆弱性を含まない」について**

脆弱性は、アプリケーションプログラムが動作する OS や利用する開発言語によって様々な種類のものが存在する。例えば、C 言語によって開発されたアプリケーションプログラムにバッファオーバーフローの脆弱性を意図せず埋め込む可能性があり、脆弱性が原因で利用者の端末上で任意のプログラムを実行される可能性がある。したがって、脆弱性を埋め込ませない、セキュアコーディングとコードの正常性を担保するテストを実施する必要がある。脆弱性が含まれないことを確認するための手段として、ソースコード診断等があり、開発するアプリケーション・コンテンツに応じて脆弱性診断を行うことを検討するとよい。なお、脆弱性診断については、「（解説）基本対策事項 7.2.1(1)-1「脆弱性診断を実施」について」を参照のこと。

- **基本対策事項 6.6.1(2)-3「実行プログラムの形式でコンテンツを提供しない」について**

実行プログラムの形式とは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。本基本対策事項に違反する例としては、会議資料等のプログラムではない文書を提供する際に、自己展開式圧縮ファイル作成ソフトウェアを用いて拡張子が「.exe」の圧縮ファイルを作成してこれを配布する行為が典型例として挙げられる。多数に及ぶ会議資料等のファイルを 1 個のファイルとして提供する必要がある場合には、拡張子「.zip」等の形式の圧縮ファイルを作成して配布すればよい。

なお、電子メールの添付により文書等を配布する場合については、「（解説）基本対策事項 8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について」を参照のこ

と。

実行プログラムの形式は、不正プログラムがその感染手段として悪用することが多いため、基本的に開かないようにしなければならない。それにもかかわらず、機関等が日頃から実行プログラムの形式でのコンテンツ提供を行う場合、機関等の職員等だけでなく、一般の行政サービスの利用者に対しても、実行プログラムの形式のファイルを開くことに慣れさせてしまうことになり、利用者の情報セキュリティ水準を低下させてしまうことになる。そのため、本基本対策事項は、実行プログラムの形式でのコンテンツ提供をしないよう求めている。

なお、機関等が行政サービスのためにアプリケーションプログラムを提供する必要がある場合等、「実行プログラムの形式以外にコンテンツを提供する手段がない」場合は、実行プログラムの形式で提供してもよいが、基本対策事項 6.6.1(2)-4 に従った措置を講ずる必要がある。

- **基本対策事項 6.6.1(2)-4「改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与える」について**

改ざん等がなく真正なものであることを確認できる手段としては、電子証明書を用いた電子署名が有効である。

利用者に提供するものがアプリケーションプログラムである場合は、「コードサイニング証明書」と呼ばれる電子証明書を用いてアプリケーションプログラムに署名を施すことがこれに該当する。利用者はアプリケーションプログラムに施された署名を確認することで、改ざんがないことを確認でき、さらに、そのアプリケーションプログラムの提供者が機関等であることを確認できる。なお、電子署名が使用できない場合は、プログラムのハッシュ値を取得し、そのハッシュ値をウェブサイト等において提供する手法も考えられる。なお、ハッシュ値を取得する際に使用するハッシュ関数については、SHA-256 などいくつか種類があるため、利用者が確認する際に判断できるように使用したハッシュ関数についても提供する必要がある。

利用者に提供するものが文書ファイルである場合は、文書ファイルに対応するアプリケーションが備える電子署名機能を利用することができる。文書ファイルは、原則として電子署名を施すことが望ましいが、文書ファイルの形式によっては、電子署名を施すアプリケーションが提供されていない場合があるが、こうした場合は TLS により通信路を保護したウェブページから当該電子ファイルをダウンロードするとともに、アプリケーションプログラムと同様にハッシュ値を用いて改ざんされていないことを確認することができるようにする等の対応が求められる。

提供するコンテンツがウェブサイト上にある場合には、TLS を用いた「https://」で始まる URL のウェブページとすることができる。これにより、利用者は現在閲覧しているウェブページが「https://」で始まる URL のウェブページであることを目視確認の上で、そこからリンクをクリックするなどしてファイルをダウンロードする手順を踏むことにより、当該ファイルは、暗号化された通信によって改ざんなくダウンロードされることになる。TLS を用いる際に、機関等のサーバ証明書を用いれば、当該サイトが機関等のものであることを確認できる。

コンテンツを電子メールで提供する場合には、S/MIME 等の電子署名の技術を用いることで、電子メールが配送途中で改ざんされていないこと及び発信者が機関等であることを確認できる。

- **基本対策事項 6.6.1⑵-5「脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する」について**

行政サービスを提供する情報システムの提供において、当該情報システムを利用するために、機関等外の事業者等が作成した汎用のソフトウェアやミドルウェアのインストールが利用者の端末で必要となる場合がある。この場合、利用者は機関等から指示されたソフトウェアを自身の端末にインストールせざるを得ないが、指定されるソフトウェア（又はソフトウェアバージョン）のサポート期間が過ぎているなどの理由により脆弱性が存在するものであると、利用者の情報セキュリティ水準を機関等が低下させることになる。したがって、脆弱性が存在するバージョンの OS の利用やソフトウェアのインストールを機関等が暗黙又は明示的に要求することにならないよう、利用者に使用を求めるソフトウェアのサポート状況を考慮した上で、アプリケーション・コンテンツの提供方式を定めて開発しなければならない。

具体的には、当該行政サービスを提供するシステムが準備された時点では脆弱性が発見されていなくても、運用開始後に発見されることがある。そのとき、利用者が迅速に当該脆弱性を回避できるようになっている必要がある。例えば、当該行政サービスを利用するために、第三者が提供している汎用のソフトウェアのインストールを必要としていたとする。このとき、当該ソフトウェアに脆弱性が発見され、それを修正した新バージョンのソフトウェアが公開された場合に、当該新バージョンのソフトウェアをインストールすることで当該行政サービスに不具合等が生じて利用が不可能になるような事態が発生すると、利用者は、当該ソフトウェアを新バージョンに更新することができなくなる。結果として、機関等の行政サービスが利用者の脆弱性回避を妨げることになってしまう。こうしたことが起きないよう、行政サービスを提供するシステムは、第三者の汎用ソフトウェアの併用を前提とする場合は、当該汎用ソフトウェアが新バージョンに置き換わっても、正常に動作するように設計する必要がある。予期せず不具合が発生する事態が発生した場合にも、行政サービスを提供するシステムを修正することができるよう、迅速に新バージョンのソフトウェアに対応することを保守契約に盛り込んでおくことが望ましい。

また、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても、他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にする必要がある。そのためには、例えば、２種類以上のウェブブラウザ又は同一製品の異なるバージョンが動作するように、情報システムの構築時に配慮し、その動作確認を行うことが考えられる。

なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、ソフトウェアの配布前に情報が公開された状態又は試用版ソフトウェアが配布され動作検証可能な状態にあれば、前もって利用可能か否かを検証するなど、その後に公開が想定されるバージョンにも対応できるよう、構

築時に配慮することが望ましい。

- **基本対策事項 6.6.1⑵-5「情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求する」について**

  行政サービスを提供する情報システムを利用するために、利用者の端末にインストールされているソフトウェア（機関等が直接提供していないソフトウェア（例えば、端末の OS やウェブブラウザ等））の設定変更を必要とするとき、その設定変更が情報セキュリティ水準の低下を招くものである場合、そのような設定変更を要求してはならない。必要があって利用者に設定変更を求めるときは、その OS やブラウザの標準設定（初期設定）に変更することのみを求めることとし、当該設定によって情報セキュリティ水準を低下させないことが前提である。

- **基本対策事項 6.6.1⑵-6「サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能」について**

  これに該当する典型的な例は、機関等のウェブサイトを構成する各 HTML ファイルの中に、機関等外のサイト（例として広告事業者の広告提供サーバ）のコンテンツを見えない形又は見える形で組み込むことで、機関等のウェブサイトの閲覧者のアクセス履歴を当該広告サーバへ自動的に送信する、いわゆる「トラッキング処理」を行う機能である。このとき、当該広告提供サーバが HTTP の cookie 機能を用いて閲覧する利用者に識別番号を付番している場合は、アクセス履歴等の、サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が、本人の意思に反して当該広告提供サーバを運営する第三者に提供されることになるので、本基本対策事項はこのような機能がアプリケーション・コンテンツに組み込まれることがないようにすることを求めている。

  また、トラッキング処理ではなくとも、例えば、利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能も、「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」に該当し得る。

  なお、対象はウェブサイトの HTML ファイルに限られず、アプリケーションプログラムを提供する場合に、そのプログラムに含まれ得る機能についても同様である。

- **基本対策事項 6.6.1⑵-6 a)「必要があって当該機能を含める場合」について**

  機関等外へのアクセスを自動的に発生させる機能を含める必要がある場合の例としては、ソーシャルメディアとの連携機能を提供するためのボタン（ボタン画像の他、ボタン押下の機能等を提供するプログラムを含む。）等を機関等のウェブページ上に設置する場合が挙げられる。万が一、機関等外のウェブサイトが提供するプログラムに不正なコードが含まれていると、当該プログラムを使用した機関等のウェブサイトが利用者に危険をもたらすことになるため、その安全性が確認できているボタン等のみを使用することが求められる。これはウェブページ等のコンテンツに限らず、機関等が提供するアプリケーションプログラムにおいても同様である。

- **基本対策事項 6.6.1⑵-6 b)「機関等外へのアクセスを自動的に発生させる機能」につい**

て

機関等外へのアクセスを自動的に発生させる機能とは、例えば、機関等が提供するウェブページの HTML ファイルに、<script src=”https://機関等外のサイト/foo.js”>等の記述があり、機関等外のウェブサイトからプログラムを読み込んで実行する機能が該当する。もし、機関等外のウェブサイトが提供するプログラムに不正なコードが含まれる場合、当該プログラムを使用した機関等のウェブサイトが利用者に危険をもたらすことになるため、そのような機能をウェブページに含めることは可能な限り避けるべきである。具体的には、当該ファイルを当該機関等ウェブサイトのサーバ上に置いて提供することで解決できる。これはウェブページ等のコンテンツに限らず、機関等が提供するアプリケーションプログラムにおいても同様である。

遵守事項

(3) アプリケーション・コンテンツの開発時の対策

(a) 情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類の**ウェブアプリケーションの脆弱性を排除するための対策**を講ずること。

【 基本対策事項 】

＜6.6.1(3)(a)関連＞

6.6.1(3)-1 情報システムセキュリティ責任者は、以下を全て含むウェブアプリケーションの脆弱性を排除すること。

a) **SQL インジェクション脆弱性**
b) **OS コマンドインジェクション脆弱性**
c) **ディレクトリトラバーサル脆弱性**
d) **セッション管理の脆弱性**
e) **アクセス制御欠如と認可処理欠如の脆弱性**
f) **クロスサイトスクリプティング脆弱性**
g) **クロスサイトリクエストフォージェリ脆弱性**
h) **クリックジャッキング脆弱性**
i) **メールヘッダインジェクション脆弱性**
j) **HTTP ヘッダインジェクション脆弱性**
k) **eval インジェクション脆弱性**
l) **レースコンディション脆弱性**
m) **バッファオーバーフロー及び整数オーバーフロー脆弱性**
n) **サーバサイドリクエストフォージェリ（SSRF）脆弱性**

6.6.1(3)-2 情報システムセキュリティ責任者は、**ウェブアプリケーションを運用段階へ移行する前**に情報システムの分類に基づき、以下の対策を実施すること。

【基本セキュリティ対策】開発したウェブアプリケーションに対して脆弱性診断の実施を検討すること。

【追加セキュリティ対策】高度な情報セキュリティ対策が要求される情報システムで実行するウェブアプリケーションに対して、脆弱性診断を実施すること。

（解説）

- **遵守事項 6.6.1(3)(a)「ウェブアプリケーションの脆弱性を排除するための対策」について**

ウェブアプリケーションの開発時には、既知の種類のウェブアプリケーションの脆弱性を排除するための対策が求められる。脆弱性を排除したウェブアプリケーションを実装する方法の詳細については、情報処理推進機構（IPA）による「安全なウェブサイトの作り方」や OWASP の ASVS（Application Security Verification Standard：ア

プリケーションセキュリティ検証標準）を参照することも考えられる。

参考：情報処理推進機構（IPA）「安全なウェブサイトの作り方 改訂第７版」
（https://www.ipa.go.jp/security/vuln/websecurity/about.html）

参考：OWASP「Application Security Verification Standard」
（https://owasp.org/www-project-application-security-verification-standard/）

OWASP「Application Security Verification Standard」については、以下の邦訳も参考にするとよい。

参考：情報処理推進機構（IPA）「情報システム開発契約のセキュリティ仕様作成のためのガイドライン～Windows Active Directory 編～」
（https://www.ipa.go.jp/digital/model/ug65p90000001ljh-att/000087453.docx）にある、「参考例　OWASP アプリケーションセキュリティ検証標準 4.0」

また、ウェブアプリケーションを開発する際に脆弱性を含まないように開発したとしても、開発者の気付かない脆弱性が存在してしまう可能性がある。そのようなリスクが考えられるため開発したウェブアプリケーションについては、脆弱性対策の状況を確認するために脆弱性診断を行うことが考えられる。脆弱性診断には、ソースコード診断、ウェブアプリケーション診断等の種類があり、必要に応じて脆弱性診断を使い分けて実施する必要がある。

さらに、高度な情報セキュリティ対策が要求される情報システムにおいてウェブアプリケーションを構築する場合は、脆弱性診断を実施することが求められる。なお、脆弱性診断については、「（解説）基本対策事項 7.2.1(1)-1「脆弱性診断を実施」について」を参照のこと。

- **基本対策事項 6.6.1(3)-1 a)「SQL インジェクション脆弱性」について**

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されることや、データベース内の情報を盗まれるなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 b)「OS コマンドインジェクション脆弱性」について**

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のコマンドを呼出しできる構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。この

ような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、ウェブアプリケーションプログラムの処理において、OS コマンドを使用しないようにし、OS コマンドの実行が可能な関数等の使用を避けることが考えられる。また、OS コマンドを使用する必要がある場合は、実行するコマンド文字列の検証処理を追加し、想定するコマンド文字列以外は実行できない仕組みとするなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 c)「ディレクトリトラバーサル脆弱性」について**

  ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 d)「セッション管理の脆弱性」について**

  ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的擬似乱数生成器（CSPRNG）で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

- **基本対策事項 6.6.1(3)-1 e)「アクセス制御欠如と認可処理欠如の脆弱性」について**

  ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりすまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 f)「クロスサイトスクリプティング脆弱性」について**

  ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラ

ムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を全て含む対策が考えられる

- HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
- URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
- SCRIPT 要素の内容を動的に生成しないようにする。
- スタイルシートを任意のサイトから取り込める仕様を排除する。
- 全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

- **基本対策事項 6.6.1(3)-1 g)「クロスサイトリクエストフォージェリ脆弱性」について**

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに前記 e)の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害（具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害）が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

- **基本対策事項 6.6.1(3)-1 h)「クリックジャッキング脆弱性」について**

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性

を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

- **基本対策事項 6.6.1(3)-1 i)「メールヘッダインジェクション脆弱性」について**

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

- **基本対策事項 6.6.1(3)-1 j)「HTTP ヘッダインジェクション脆弱性」について**

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 k)「eval インジェクション脆弱性」について**

ウェブアプリケーションのプログラムを作成する言語が、「eval」、「JavaScript」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 l)「レースコンディション脆弱性」について**

ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者

が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

- **基本対策事項 6.6.1(3)-1 m)「バッファオーバーフロー及び整数オーバーフロー脆弱性」について**

  ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、バッファオーバーフロー脆弱性等が生じない言語を採用した場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

- **基本対策事項 6.6.1(3)-1 n)「サーバサイドリクエストフォージェリ（SSRF）脆弱性」について**

  インターネット等の外部に公開したウェブアプリケーションから、本来は外部から到達できない領域にある任意の送信先に対して、リクエストを送ることが可能な仕様になっている場合がある。このような欠陥のことを一般的に「サーバサイドリクエストフォージェリ脆弱性」と呼ぶ。この脆弱性を悪用されると、インターネット等の外部に公開されているウェブアプリケーションをとおして、任意の送信先に対して不正なコマンド等を実行することができ、不正に操作される被害等が生じる可能性がある。

  この脆弱性を排除するには、インターネット等の外部に公開したウェブアプリケーションにおいて外部からのリクエストの送信先を限定するため、ドメインなどの許可リストを利用してホワイトリスト化するなどの対策が考えられる。送信先を限定することが困難な場合は、リクエストの入力規則を慎重に設計する等の対策が考えられる。

  また、外部に公開したウェブアプリケーションとの通信が必要なセグメントと通信の必要のないセグメントを分離する等の対策も有効である。

- **基本対策事項 6.6.1(3)-2「ウェブアプリケーションを運用段階へ移行する前」について**

  ウェブアプリケーションの脆弱性を悪用されると、ウェブアプリケーションで取り扱う情報の漏えいやウェブアプリケーションに入力する情報の窃取などが発生する可能性がある。そのため、脆弱性を排除するようにウェブアプリケーションの開発をする必要があるが、開発時には想定できなかった脆弱性が存在する可能性もある。そのため、ウェブアプリケーションで行われる業務や取り扱う情報等を踏まえて、ウェブアプリケーションの脆弱性診断を実施する必要がある。

基本セキュリティ対策として、開発した全てのウェブアプリケーションについては、運用段階へ移行する前に当該ウェブアプリケーションを用いて行われる業務や取り扱う情報等を踏まえて脆弱性診断の実施の必要性を検討し、実施する必要がある場合はウェブアプリケーション診断等を行うこと。なお、インターネットからアクセス可能なウェブアプリケーションについては、脆弱性診断を実施することが望ましい。

追加セキュリティ対策として、高度な情報セキュリティ対策が要求される情報システムにおいて実行するウェブアプリケーションについては、運用段階へ移行する前に脆弱性診断を行う必要がある。実施すべき脆弱性診断については、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、構築する情報システムの構成等によって利用する脆弱性診断を使い分ける必要があるが、最低限ウェブアプリケーション診断は実施することが求められる。

なお、脆弱性診断については、デジタル庁が公表している以下のガイドラインを参考にするとよい。

参考：デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」
（https://www.digital.go.jp/resources/standard_guidelines/）

遵守事項

(4) アプリケーション・コンテンツの運用時の対策

(a) 情報システムセキュリティ責任者は、利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

(b) 情報システムセキュリティ責任者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずること。

(c) 情報システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずること。

【 基本対策事項 】

＜6.6.1(4)(a)関連＞

6.6.1(4)-1 情報システムセキュリティ責任者は、利用者に強制する OS やソフトウェア等のサポート状況や脆弱性情報等を確認し、サポートが終了する又は脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなど情報セキュリティ水準を低下させる設定変更等を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

（解説）

- **遵守事項 6.6.1(4)(b)「定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずる」について**

情報システムセキュリティ責任者は、運用中のアプリケーション・コンテンツにおいて脆弱性対策の状況を確認する手段として、アプリケーション・コンテンツで使用しているソフトウェア等における脆弱性に関する情報が公開されていないかを確認する方法の他、ウェブアプリケーションを標的とした攻撃手法の確認や専用ツールを用いて脆弱性診断を行うことや、事業者が提供するサービス等を利用して脆弱性診断を行うなどの方法も考えられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、運用中の変化等に応じて脆弱性診断を使い分ける必要がある。

なお、脆弱性診断については、「(解説) 基本対策事項 7.2.1(1)-1「脆弱性診断を実施」について」を参照のこと。

アプリケーション・コンテンツの脆弱性が発覚した場合は、適切な対応を速やかに進めることが求められる。脆弱性は、脆弱性診断等により発覚する以外に、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号)」を踏まえた「情報セキュリティ早期警戒パートナーシップ」の活動により、調整機関から通知されることもある。「情報セキュリティ早期警戒パートナーシップ」の活動から通知された場合を含め、アプリケーション・コンテンツの脆弱性が発覚した場合は、「情

報セキュリティ早期警戒パートナーシップガイドライン」に説明されている脆弱性関連情報への対処に沿った対応を行うこと。「情報セキュリティ早期警戒パートナーシップ」については、以下の告示及びガイドラインを参照するとよい。

参考：経済産業省「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号）」
（https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf）

参考：経済産業省「受付機関及び調整機関を定める告示（平成 31 年経済産業省告示第 19 号）」
（https://www.meti.go.jp/policy/netsecurity/vul_institutions.pdf）

参考：情報処理推進機構（IPA）「情報セキュリティ早期警戒パートナーシップガイドライン」
（https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html）

- **遵守事項 6.6.1(4)(c)「改ざんを検知するための措置を講ずる」について**

  情報システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツの改ざんを検知するため、ウェブアプリケーションやウェブコンテンツを更新するたびにハッシュ値等を保存し、定期的に比較するなどの措置を講ずることが考えられる。

- **基本対策事項 6.6.1(4)-1「サポートが終了する又は脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する」について**

  情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツを運用する際は、当該アプリケーション・コンテンツの利用者に対して強制する OS やブラウザ等のソフトウェア等のサポート状況や脆弱性情報を確認し、利用を強制するソフトウェア等のサポートが終了する又は脆弱性が存在することが発覚した場合、利用者の情報セキュリティ水準の低下を招かぬように対策を講じなければならない。

6.6.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

機関等では、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を用意し、国民等の利用に供している。これらの国民等に提供するサービス（クラウドサービスを含む）は通常インターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の機関等のものであると確認できることが重要である。また、機関等になりすましたウェブサイトを放置しておくと、機関等の信用を損なうだけでなく、国民等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

遵守事項

(1) 政府ドメイン名の使用

(a) 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を取得できない場合を除き政府ドメイン名を情報システムにおいて使用すること。

(b) 職員等は、機関等外向けに提供するウェブサイト等の作成を業務委託する場合においては、機関等に適するドメイン名を使用するよう調達仕様に含めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.6.2(1)(a)「実際の機関等提供のものであることを利用者が確認できる」について**

政府ドメイン名は、株式会社日本レジストリサービスが定める「属性型（組織種別型）・地域型 JP ドメイン名登録等に関する規則」に基づき、その登録資格は日本国の政府機関、各省庁所轄研究所、独立行政法人、特殊法人（特殊会社を除く。）に限られるとされていることから、日頃から機関等が政府ドメイン名を用いることを徹底することにより、なりすましが発生しても、機関等外の者がウェブサイト等の真偽を見分けることが容易なものとすることができる。

仮に政府ドメイン名以外を使用した場合には、そのサイトの使用を終了した後も、当該ドメイン名を不正に利用されないように登録管理を一定期間（少なくとも 1 年以上）維持しなければならないが、そのような管理の必要がないことも、政府ドメイン名を用いることの利点の一つである。ただし、ホスティングサービス等を用いてそのサイトを公開した場合、公開時に設定した当該政府ドメイン名に関する DNS 設定を、終了時に削除する必要があることに注意が必要である。DNS 設定が残ったままになっている場合、その設定を第三者に利用され、使用を終了した政府ドメイン名を使って意図しないウェブサイト等を公開されてしまうサブドメインテイクオーバー・NS テイクオーバー

と呼ばれる攻撃を受ける可能性がある。

政府ドメイン名を用いるべき場合の例を以下に示す。

- 機関等の地方出先機関や在外公館等が組織の紹介サイトを提供する場合

  「.go.jp」で終わるドメイン名は、運営主体が日本国政府及び政府に関係する機関であることを示すものとして、閲覧者に理解される。サーバを国外に設置している場合であっても、当該サーバのホスト名として「.go.jp」で終わるドメイン名を設定することは可能である。
- 機関等が主催する講演会等に係るウェブサイトの提供において、参加者の登録をオンラインで行うために、ウェブサイト上で閲覧者に個人情報を入力させる場合
- 機関等が広報活動として期間限定でキャンペーンサイトを広告会社に制作させ提供する場合

  一時的に提供するウェブサイトを構築する場合や、広告会社に制作からサーバ管理までを委託する場合であっても、政府ドメイン名を用いるべきである。サーバが広告会社管理のもので、サーバに割り当てられた IP アドレスが機関等外のものであっても、そのホスト名として政府ドメイン名を用いることはできる。

  なお、政府ドメイン名を用いて一時的に提供するウェブサイトを終了する場合、サブドメインテイクオーバー・NS テイクオーバーによる攻撃を防止するため、提供開始時に設定した当該政府ドメイン名に関する DNS 設定を、終了時に削除する必要があることに注意が必要である。

- **遵守事項 6.6.2(1)(a)「政府ドメイン名を取得できない場合」について**

政府ドメイン名を使用しない場合は、機関等を装ったなりすましの脅威があることを十分に理解し、国民に対して当該ドメイン名が機関等のものであることの真偽を見分けられるようにすることが重要である。また、政府ドメイン名以外のドメイン名は、ドメインの廃止後に第三者に取得され、悪用されるリスクがあることから、当該ドメインを利用しなくなった後でも当面の間、登録を継続することや再利用することができない URL 等を用いるなどの対策が必要となり、利用を終了した後もリスクが存在することを十分に理解した上で、使用することを検討すること。

本対策における政府ドメイン名を取得できない場合とは、特段の理由により政府ドメイン名が使えない場合も含めたものである。

政府ドメイン名を取得できない場合の例を以下に示す。

- 指定法人が政府ドメイン名を登録する資格を持たない場合

  この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。
- 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用する場合

  高等教育機関向けのドメイン名とは、高等教育機関及び学校法人等が登録できるドメイン名（ac.jp）を指す。高等教育機関向けのドメイン名を取得するため

の要件は、政府ドメイン名の要件とは異なるものの、取得可能な機関が高等教育機関に限られていることから、高等教育機関向けのドメイン名を使用することは、なりすまし等の特定の脅威に対する対策として一定の効果があると考えられる。

- 遵守事項 8.1.2(1)に掲げるソーシャルメディアによる情報発信を行う場合

  ソーシャルメディアによる情報発信を行う場合は、当該ソーシャルメディアの機関等のアカウントが、実際の機関等のものであると認識できるようにするため、なりすまし対策を講ずる必要がある。ソーシャルメディアのなりすまし対策については、基本対策事項 8.1.2(1)-2 を参照のこと。

なお、高等教育機関向けのドメイン名を使用する場合は、あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断すること。

国の行政機関に属する教育機関については、従前より統一基準において政府ドメイン名の使用を求めてきているが、その性格が「職員の養成や研修」という点において国の行政機関の行政事務の一環としてとらえることができ、政府ドメイン名を用いることが適当である。

一方、独立行政法人や指定法人である教育機関については、これら教育機関で勉学を行う国民の目から見れば、国の行政関係機関というよりも教育の場としての性格が強いと考えられ、使用するドメイン名については、情報セキュリティ確保の観点と、ウェブサイトの利用者側の視点の両面から考慮する必要がある。また、例えば、教育機関に所属する学生が政府ドメイン名のメールアドレスを使用するとした場合、メールを受信した者にとっては、メールの送信者が機関等の職員であると誤解する可能性もあり、このような点も考慮する必要がある。

そのため、独立行政法人や指定法人である教育機関においては、これら自組織の特性及び情報セキュリティ確保の観点を踏まえた上で、どちらのドメイン名を使用するべきか比較考慮し、判断する必要がある。

政府ドメイン名の取得は可能であるが、例外として政府ドメイン名以外を使用する場合の例と留意事項を以下に示す。

- 限定的な公開により提供する場合

  広く国民に提供することを目的とせず、特定の者や特定の用途など限定的な公開により提供する場合は、なりすましサイト等を作成する悪意ある第三者により、国民が不正なサイトへ誘導されるリスクが低くなると考えられる。ただし、長期的に公開する場合や提供するウェブサイト等を用いて個人情報を取得するなど機関等の信用が必要となる場合は、政府ドメイン名を使用しないことによるリスクを十分に評価する必要がある。

  なお、このような方法を用いる場合は、利用した URL が第三者によって悪用されないようにすることが重要である。

- 災害等により機関等の公式ウェブサイト等による情報発信が困難となった場合

  迅速に国民に対して情報提供するための代替手段として、政府ドメイン名を

使用しないウェブサイト等から情報発信することが想定される。

いずれの場合も、運用を終了する際には、ドメイン名等が悪用されないよう適切な措置を講ずる必要がある。

- **遵守事項 6.6.2(1)(b)「機関等に適するドメイン名を使用するよう調達仕様に含める」について**

  機関等外向けのウェブサイトを構築する場合に、情報システム部門以外の職員等がウェブサイトの構築業務を業務委託することが考えられる。このような場合でも、情報セキュリティ水準の低下を招かないよう、例えば、国の行政機関であれば政府ドメイン名の使用を調達仕様に含めることが求められる。

遵守事項

(2) 不正なウェブサイトへの誘導防止

(a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して**機関等のウェブサイトになりすました不正なウェブサイト**へ誘導されないよう対策を講ずること。

【 基本対策事項 】

＜6.6.2(2)(a)関連＞

6.6.2(2)-1 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイトに対して、以下を例とする**検索エンジン最適化措置（SEO 対策）**を講ずること。

a) **クローラからのアクセスを排除しない**こと。

b) **cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする**こと。

c) **適切なタイトルを設定する**こと。

d) **不適切な誘導を行わない**こと。

6.6.2(2)-2 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、**不審なサイトへのアクセスを防止するための対策**を講ずること。

6.6.2(2)-3 情報システムセキュリティ責任者は、機関等のウェブサイトなどになりすました**不審なウェブサイト等が存在していることの連絡を受け付ける体制を整備する**とともに、**不審なウェブサイトに対し必要な措置を講ずる**こと。

（解説）

- **遵守事項 6.6.2(2)(a)「機関等のウェブサイトになりすました不正なウェブサイト」について**

機関等外の者が、機関等の名前をタイトルに掲げるなどして、機関等のウェブサイトと誤認されかねないウェブサイトを作成することがあり、これを完全に防ぐことはできない。本来ならば、利用者は当該サイトの URL 中のドメイン名が政府ドメイン名であるかを確認することで、機関等のウェブサイトかを確認できるところであるが、検索サイト等を利用して機関等名で検索して訪れる利用者も多いことから、検索サイトで検索したときに、正規の機関等サイトが検索結果の上位に現れるようになっていることが望ましい。通常は、特別な対策をすることなく、そのような結果になることがほとんどであるが、正規の機関等サイトの側で、不適切な設定になっている場合や、コンテンツが適切に構成されていない場合に、検索サイトで、正規の機関等サイトが最上位に現れないことや、適切な表示がなされないことがある。本条はそのような事態を防止するための措置を講ずることを求めている。

- **基本対策事項 6.6.2(2)-1「検索エンジン最適化措置（SEO 対策）」について**

正規のウェブサイトが検索サイトで上位に現れるように正規のウェブサイト側で工

夫を施すことを、一般に「検索エンジン最適化」又は「SEO 対策」と呼ぶ。本基本対策事項は、機関等サイトにおいても一般的な検索エンジン最適化の措置を講ずることを求めている。

- **基本対策事項 6.6.2⑵-1 a)「クローラからのアクセスを排除しない」について**

一般に、検索サイトは、ウェブクローラと呼ばれる自動的にウェブサイトのリンクをたどって全てのページを巡回するプログラムを、自ら稼働させることによって収集したHTML データを用いて検索機能を実現している。そのため、検索サイトのクローラからのアクセスを拒否する設定をしている場合、当該サイトは検索サイトの検索結果に現れなくなることがある。そのような設定は、ウェブサイトの「/robots.txt」のファイルの記述で簡単にできるものであるため、誤ってクローラからのアクセスを拒否する設定にしてしまう状況が想定される。通常、このファイルを設定する必要はないため、何ら記述しないでおくことが望ましい。

- **基本対策事項 6.6.2⑵-1 b)「cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする」について**

一般に、検索サイトが自ら稼働させるウェブクローラは、HTTP の cookie 機能に対応していない。そのため、cookie 機能を無効に設定したブラウザで閲覧したときに、正常に表示されないウェブページは、検索サイトの検索結果に正常に表示されない事態が起きる。通常のウェブサイトの構成では、cookie 機能を無効にしても正常に表示されるものであるが、一部の CMS には、cookie を無効にして閲覧すると「cookie を有効にしてください」とだけ記述したエラー画面を表示するものがあり、そのような CMS を用いてウェブサイトを構成すると、前述の事態が生じる。実際に、過去に一部の機関等サイトでそのような事態が発生したことがあるため、ウェブサイトの構築を業務委託する場合を含め、注意が必要である。

- **基本対策事項 6.6.2⑵-1 c)「適切なタイトルを設定する」について**

一般に、検索サイトの検索結果には、当該ページのタイトル（HTML 中の TITLE 要素で設定される文字列）が見出しとして表示され、利用者はこれを頼りにサイトを訪れることから、機関等サイトにおいても、ページのタイトルに機関等の名称を含めるなど、適切なタイトルを設定することが重要である。

その他の対策として、HTML 中の H1 要素や H2 要素を適切に記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。機関等サイトにおいても、H1 要素や H2 要素を適切に記述することで、検索結果の上位に現れやすくすることができる。また、HTML 中のメタタグ（「description」や「keywords」等）に概要やキーワード等を記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。機関等サイトにおいても、メタタグを適切に記述することで、検索結果の上位に現れやすくすることができる。

- **基本対策事項 6.6.2⑵-1 d)「不適切な誘導を行わない」について**

一般に、HTML 中に見えない文字等でページ内容に関係のないキーワードを過剰に

記述するなどして、当該ページへのアクセスを無用に誘う行為（「SEO スパム」等と呼ばれる。）は、不適切な行為として検索サイトからペナルティを科され、検索結果の上位に表示されなくなることがある。機関等のウェブサイトにおいて、故意にそのような行為が行われることは考えにくいが、コンテンツの作成を業務委託した場合に、委託先が独自判断で行うことも想定されるため、そのようなコンテンツを作成しないよう注意が必要である。

- **基本対策事項 6.6.2(2)-2「不審なサイトへのアクセスを防止するための対策」について**

  不審なサイトを確認した場合は、機関等のウェブサイト等において注意喚起を行うなどの対応を図るとともに、必要に応じて自組織や内閣官房国家サイバー統括室等の関係部門に状況を報告する。特に悪質な場合は、誤って当該サイトにアクセスすることを防止するため、検索サイト業者に対して検索結果に表示されないよう依頼する、機関等 LAN システムからアクセスできないよう当該サイトに対してフィルタを設定する、といった対策が考えられる。

- **基本対策事項 6.6.2(2)-3「不審なウェブサイト等が存在していることの連絡を受け付ける体制を整備する」について**

  機関等のウェブサイトなどになりすました不審なサイトは、主に外部からの通報によって把握する場合が多い。そのため、ウェブサイト等のアプリケーション・コンテンツを提供する場合は、不審なウェブサイト等を発見した場合の外部からの通報窓口などを用意することが望ましい。また、警察や内閣官房国家サイバー統括室、JPCERT/CC などの公的機関や専門機関、職員等からの通報についても定められた連絡先を用意するとよい。定められた連絡先としては、情報セキュリティインシデントの可能性を認知した際の報告窓口や CSIRT などが考えられる。また、公的機関等からの通報があることを踏まえて、公的機関等との関係を整理するとよい。

- **基本対策事項 6.6.2(2)(a)-3「不審なウェブサイトに対し必要な措置を講ずる」について**

  不審なウェブサイトについて通報を受けた場合は、そのサイトが正規のサイトではない場合、警察への通報・連絡をするとともに、JPCERT/CC やフィッシング対策協議会などに正規でないサイトを閉鎖するための支援を要請するなどの措置を講ずることが考えられる。また、そのような正規でないサイトを把握した場合、当該ウェブサイトの利用者が正規でないサイトへ誘導されないよう、機関等のウェブサイトや SNS 等を使用し通知するなどの措置を講ずることも考えられる。

  なお、フィッシング対策については、フィシング対策協議会が公開している「フィッシング対策ガイドライン」を参考にするとよい。

  参考：フィッシング対策協議会「フィッシング対策ガイドライン」
  （https://www.antiphishing.jp/report/guideline/）

遵守事項

(3) アプリケーション・コンテンツの告知

(a) 職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

(b) 職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

【 基本対策事項 】

＜6.6.2(3)(a)関連＞

6.6.2(3)-1 職員等は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示すること。また、短縮 URL を用いないこと。

6.6.2(3)-2 職員等は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

＜6.6.2(3)(b)関連＞

6.6.2(3)-3 職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の全ての措置を講ずること。

a) 告知するアプリケーション・コンテンツを管理する組織名を明記すること。

b) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記すること。

（解説）

- **遵守事項 6.6.2(3)(b)「機関等外の者が提供するアプリケーション・コンテンツを告知する」について**

機関等外の者が提供するアプリケーション・コンテンツを告知する場合、告知を開始した時点では、当該アプリケーション・コンテンツが、告知した URL 等の誘導先に確かに存在していても、将来にわたりその誘導先に意図したアプリケーション・コンテンツが存在し続けるとは限らない。誘導先のドメイン名等が放棄された場合には、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、機関等外の者が提供するアプリケーション・コンテンツを機関等が告知する場合には、誘導先の有効性を保つことが求められる。

- **基本対策事項 6.6.2(3)-1「URL 等を用いて直接誘導」について**

URL を用いた直接誘導に該当する例としては、ウェブサイトにハイパーリンクを設

ける場合のほか、電子メールに URL を記載して告知する場合、印刷物に URL を表示して誘導する場合等が挙げられる。URL「等」としているのは、例えば、ホスト名（FQDN 形式での表記）もこれに該当するものとする趣旨である。

- **基本対策事項 6.6.2(3)-1「検索サイトで指定の検索語を用いて検索することを促す方法」について**

  印刷物やテレビ CM により告知する際に、URL 等の文字列が長すぎると、利用者にその全部を入力させることが困難であることから、検索サイトで検索するよう検索語を指定して促す方法が広く普及している。

  しかし、この誘導方法では、偽サイトや別のサイトに誘導されてしまうリスクを否定できない。検索結果の上位に目的の誘導先が現れない可能性があるだけでなく、検索サイトの広告部分に悪意あるサイトを出現させる攻撃手法も想定され、利用者が検索サイトの広告部分を誘導先として解釈してしまうおそれがある。

  また、アプリケーション・コンテンツの告知を広告代理店に委託している場合、広告代理店が検索連動型広告と呼ばれる検索サイトの広告枠を購入し、検索結果の画面に表示される広告部分を直接クリックすることなどを用いて目的の誘導先に誘導する方法が用いられることがある。この広告部分を利用して誘導する方法が広告代理店によって頻繁に用いられると、検索結果の画面に表示される広告部分を正規の誘導先として利用者が解釈するようになると考えられ、広告部分に攻撃者による偽サイトが現れることのリスクを無視することはできなくなる。したがって、機関等がアプリケーション・コンテンツを告知する場合には、検索サイトの検索画面に表示される広告枠を購入して誘導する方法を用いないようにすることが望ましい。なお、検索サイトに限らず、名称や存在等を広く周知することを目的とし、利用者の主体的な検索等による誘導を前提としないディスプレイ広告等については、この限りでない。

- **基本対策事項 6.6.2(3)-1「間接的な誘導方法を用いる場合」について**

  間接的な誘導方法を用いて機関等の提供するアプリケーション・コンテンツを告知する場合は、当該誘導方法による誘導の状況を適時確認するなどして、不正な又は不適切なウェブサイトへ誘導されてしまう可能性が高い状況になっているか否かを確かめることが望ましい。

- **基本対策事項 6.6.2(3)-1「URL 等と一体的に表示する」について**

  アプリケーション・コンテンツの告知は URL 等を用いて直接誘導することを原則とするが、間接的な誘導方法を用いたい場合があることも想定されることから、その場合に実施すべき措置として、間接的な誘導方法と一体的に URL 等を表示することを求めている。

- **基本対策事項 6.6.2(3)-1「短縮 URL を用いない」について**

  短縮 URL を提供する民間事業者のサービスは、将来にわたり永続的に運営が保証されるものではなく、いずれサービスが消滅し、ドメイン名が放棄されれば、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、やむを得ない場合を除き、短縮 URL を用いるべきでな

い。やむを得ない場合の例としては、ソーシャルメディアにおいて URL を告知する場合に、当該ソーシャルメディアが強制的に所定の短縮 URL を用いてしまう場合が挙げられる。

- **基本対策事項 6.6.2(3)-2「アプリケーション・コンテンツの内容に係る記述を当該バーコードと一体的に表示」について**

  印刷物等でアプリケーション・コンテンツを告知する際に、URL 等の表示に代わるもの又は URL 等と一体的に表示するものとして、二次元コード等を用いて誘導する方法がある。この方法は、特にスマートフォンや携帯電話の利用者にとって利便性が高く、機関等においても用いられるようになってきている。

  しかしながら、二次元コード等のみを単体で表示した場合、それがどこへ誘導するものであるかが、利用者にとって必ずしも明確でない場合がある。そこで、本基本対策事項では、当該二次元コード等がどこへ誘導するものであるかを、当該二次元コード等と一体的に表示することにより利用者に明示することを求めている。

  「アプリケーション・コンテンツの内容に係る記述」の例としては、誘導先の URL 等や、誘導先のアプリケーション・コンテンツの内容を示す記述が考えられる。

- **基本対策事項 6.6.2(3)-3「告知する URL 等の有効性を保つために以下の全ての措置を講ずる」について**

  この措置を講ずるための対策事項 a)及び b)について、具体的な記載例を以下に示す。

  - このウェブサイトは○○協会が運営しており、○○省が運営しているものではありません。
  - このウェブサイトのアドレスについては、○○年○○月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、御自身で御確認ください。

第7部 情報システムのセキュリティ要件

7.1 情報システムのセキュリティ機能

7.1.1 主体認証機能

目的・趣旨

情報又は情報システムへアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、機関等の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(1) 主体認証機能の導入

(a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の**識別**及び**主体認証**を行う機能を設けること。

(b) 情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、**オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること**。

(c) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、**主体認証情報の漏えい等による不正行為を防止するための措置**及び**不正な主体認証の試行に対抗するための措置**を講ずること。

【 基本対策事項 】

＜7.1.1(1)(a)関連＞

7.1.1(1)-1 情報システムセキュリティ責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入すること。

a) **知識**（パスワード等、利用者本人のみが知り得る情報）による認証

b) **所有**（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

c) **生体**（指紋や静脈等、本人の生体的な特徴）による認証

7.1.1(1)-2 情報システムセキュリティ責任者は、情報システムの主体認証方式として、２つ以上の主体認証方式を組み合わせる**多要素主体認証方式**等の導入を検討すること。特に、機関等内通信回線へリモートアクセスを必要とする主体やインターネット回線等

の機関等外通信回線から直接アクセスが可能なクラウドサービス等の管理者権限を有する主体、重要な情報システムにおいて情報セキュリティインシデントに繋がる恐れのある強い権限を有する主体など、**厳格な主体認証が必要な場合**は、原則として多要素主体認証方式等の強固な認証技術を用いること。。

7.1.1(1)-3 情報システムセキュリティ責任者は、ウェブブラウザを介した主体認証機能を設けるに当たっては、主体認証方式として、**フィッシング耐性を有する方式**の導入を検討すること。

7.1.1(1)-4 情報システムセキュリティ責任者は、主体認証情報としてパスワードを使用し、主体認証情報を付与された主体自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、**強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること**を利用者に守らせる機能を設けること。

＜7.1.1(1)(c)関連＞

7.1.1(1)-5 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。

a) 原則として、機器等において**初期値として設定されている識別コードを使用しない**こと。
b) **不要な識別コードを無効にする**こと。

7.1.1(1)-6 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を全て含む方法を用いて適切に管理すること。

a) 主体認証情報を送信又は保存する場合には、その内容を暗号化すること。
b) 主体認証情報に対するアクセス制限を設けること。
c) 主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認すること。

7.1.1(1)-7 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。

a) 当該主体認証情報及び対応する識別コードの利用を停止する機能
b) 主体認証情報の再設定を利用者に要求する機能

（解説）

- **遵守事項 7.1.1(1)(a)「識別」について**

識別のための機能が実装されていない情報システムにおいて主体認証を行う場合（例えば、識別コード自体が存在せず、主体認証情報の検証のみで主体認証を行う場合）は、例外措置として判断し、主体を識別しないことによる影響を勘案の上、必要に応じて代替又は追加の措置を講ずる必要がある。

- **遵守事項 7.1.1(1)(a)「主体認証」について**

情報セキュリティ水準と情報システムの利便性等を考慮し、主体認証機能の運用に係る以下の要件の実装要否を情報システムの導入時に考慮するとよい。

- 正当な主体以外の主体認証を受諾しないこと。(誤認の防止)
- 正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。(誤否の防止)
- 正当な主体が容易に他の主体に主体認証情報の付与(発行、更新及び変更を含む。以下本款において同じ。)及び貸与ができないこと。(代理の防止)
- 主体認証情報が容易に複製できないこと。(複製の防止)
- 情報システムセキュリティ責任者の判断により、ログインを個々に無効化できる手段があること。(無効化の確保)
- 必要時に中断することなく主体認証が可能であること。(可用性の確保)
- 新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。(継続性の確保)
- 主体に付与した主体認証情報を利用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。(再発行の確保)

なお、生体認証に用いる認証方式によっては、誤認の防止や誤否の防止とならない可能性があるため、そのような認証方式を用いる場合は、複数の認証方式を採用するなどを検討し、情報システムの導入時に考慮することが望ましい。例えば、生体認証として顔認証や指紋認証を用いる場合、認証精度は製品等によって異なる。顔認証の場合、製品によっては、顔の経年の変化や髪型が変わった場合などにより認証できない可能性があるので注意が必要である。また、機関等支給以外の端末をやむを得ず主体認証に利用する場合は、6.1.3「機関等支給以外の端末の導入及び利用時の対策」を参照し、必要な措置を講ずることに留意が必要である。

- **遵守事項 7.1.1(1)(b)「オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること」について**

本項は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する際に、利用者本人であることを確認するための認証機能を適切に実装することを求めるものである。

オンライン手続におけるリスク評価に当たっては、サイバー攻撃等の脅威から生じ得る不正な認証の成功に加え、事業目的の遂行、公平性、ユーザビリティ／アクセシビリティ、プライバシー保護等の多面的な観点から要件を選定する必要がある。リスク特定の際は、主に以下４つのプロセスに係る代表的なリスクをもとにシステム個別のリスクを抽出すると良い。

①主体認証情報（認証器）の登録
②主体認証（当人認証）の実施
③主体認証情報（認証器）の盗難・紛失時の対応
④停止アカウントの回復

特に「④停止アカウントの回復」に関しては、採用している当人認証手法よりも強い強度を持った方法で実施しない場合、攻撃の起点とされやすいため、注意する必要がある。

次に、抽出されたリスクが顕在化した時の影響を判断する。判断に関しては、以下の観点から実施すると良い。

①申請者が対象手続等によって得られる権利権益等の侵害

②プライバシーの重大な侵害

③犯罪や攻撃への悪用

一方、これらは対象手続において個人等が申請・届出等を行う際の本人確認を対象としているため、リスクの影響範囲は、攻撃や侵害を受けた特定の利用者やアカウント等に限定されることを前提としている。情報システムの特性上、リスクの影響範囲が多数の利用者又は関係者に及ぶ場合には、さらに異なる観点からの影響評価が必要である点に注意が必要である。

なお、認証方式の選択に当たっては、適切なセキュリティ確保と普及を妨げない利便性とを両立させることが重要である。その際は、特定のリスクのみに着目せず、様々な観点でリスクを評価した上で認証方式を決定する必要がある。認証方式の選択においては、以下を参考にするとよい。

参考：デジタル庁「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」

（https://www.digital.go.jp/resources/standard_guidelines/）

参考：デジタル庁「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン 解説書」

（https://www.digital.go.jp/resources/standard_guidelines/）

- **遵守事項 7.1.1(1)(c)「主体認証情報の漏えい等による不正行為を防止するための措置」について**

主体認証情報の漏えい等が発生すると、悪意ある第三者によってなりすましによる不正アクセスをされ、情報の窃取や踏み台にされるなどのリスクが発生する。主体認証情報の漏えいしたアカウントを悪用されると、情報セキュリティ対策を無効にされることや、情報を窃取するために使用する不正プログラム等を導入される可能性がある。したがって、誰もが知っている機器等において初期値として設定されている識別コードは原則として利用しない措置を講ずることが重要である。また、開発時に使用した識別コードや一時的に利用したテスト用の識別コード等を運用時においても有効にしていた場合、そのような識別コードが何らかの手段によって攻撃者に渡り、悪用される可能性も高くなる。したがって、不要となった識別コードは無効にすることが有効である。

- **遵守事項 7.1.1(1)(c)「不正な主体認証の試行に対抗するための措置」について**

主体認証機能に対する不正を防止するための機能として、以下を例とする機能を設

けることを検討することが重要である。

- 不正にログインしようとする行為を検知又は防止する機能

  特定の識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を正当な主体や情報システムの運用担当者等に通知し、一定期間当該端末（又は識別コード）からのログイン操作受付を停止する機能を指す。当該識別コードによる情報システムへの以後のログインを無効にすることも考えられる。この機能により、不正なログインの試行の有無等について、正当な主体や情報システムの運用担当者等がその状況を確認するとともに、一定程度不正ログイン等を防止することができる。

- リスクがあると判断したときに追加の認証を要求するリスクベース認証による機能

  リスクベース認証では、例えば、リモートから情報システムにログインする際に使用する端末の IP アドレスを確認し、特定の範囲以外からのアクセスであった場合は追加の認証を行うことや、登録済みのデバイス以外からのアクセスであった場合は追加の認証を行うなど様々な方法が考えられる。ただし、当該機能を実装する場合は、特定のリスクを判断するための情報の収集が必要になることや、実装する際のコストが高くなる可能性があるため、当該機能が必要となるリスク等を検討した上で実装することが望ましい。

- 情報システムへのログイン時に本来の主体へメッセージを通知する機能

  不正アクセスが行われた際に、早期に発見し、対処を可能とするため、ログインが行われたことを本来の主体へ電子メールなどで通知する機能を指す。

  通知メッセージの内容として、以下の例が考えられる。

  - 情報システムに対してログインが行われたこと
  - 正当なログインとの区別を容易とするため、ログイン時刻、IP アドレスなどから求めた端末のおおよその場所、端末の種別、ブラウザの種類等

- **基本対策事項 7.1.1(1)-1 a)「知識」について**

端末によっては、例えばパスワード以外にも、自分のみが知る「パターン」を主体認証情報として扱うケースがあるが、これも「知識」に分類される。

- **基本対策事項 7.1.1(1)-1 b)「所有」について**

「所有」による認証の例を以下に示す。

- マイナンバーカード
- 耐タンパ性を有する USB トークン、IC カード
- スマートフォンの SMS で送信されるワンタイムパスワード又は、音声電話を利用した認証

  利用するスマートフォンの SIM カードに設定された電話番号が所有の対象
- Authenticator 等の認証アプリに保存された秘密鍵で生成するトークン

  アプリに保存されている秘密鍵が所有の対象

- **基本対策事項 7.1.1(1)-1 c)「生体」について**

生体情報による主体認証を用いる場合には、その導入前に、この方式特有の他人受入率（本人を他人と誤って認証してしまう確率）と本人拒否率（本人の認証が受け入れられない確率）の課題があるため、誤認の防止や誤否の防止とならない可能性がある生体による主体認証を用いる場合は、多要素主体認証の一つとして利用することを考慮して情報システムを設計する必要がある。

- **基本対策事項 7.1.1(1)-2「厳格な主体認証が必要な場合」について**

厳格な主体認証が必要な場合の具体的な例は、以下のとおり。

- VPN 等を用いて機関等外通信回線から情報システムにリモートアクセス可能な主体（管理者権限の有無によらない。）
- クラウドサービス等の管理機能へアクセス可能な管理者権限を有する主体
- ウェブコンテンツ等を管理・更新することが可能な管理者権限を有する主体
- 侵害されると深刻・広範囲に影響がある情報システムや組織の業務の基幹となる情報システムにおける重要なサーバ装置等の管理者権限を有する主体
- Active Directory ドメイン管理サーバのドメイン管理権限を有する主体
- 機微な情報を管理する情報システム、組織の基幹となる重要な業務システム等において情報セキュリティインシデントに繋がる恐れのある強い権限を有する主体

- **基本対策事項 7.1.1(1)-2「多要素主体認証方式」について**

主体認証を行う情報システムにおいて、厳格な主体認証が必要な場合や 1 つの主体認証方式のみで行う認証の強度におけるリスクが許容できない場合には、2 つ以上の主体認証方式を用いて認証を行う多要素主体認証方式（一部の 2 段階認証と呼ばれる方式を含む。）を導入する必要がある。

主体認証方式は、一般に、異なる認証方式を組み合わせた方が、強度が高くなる。異なる認証方式を組み合わせた多要素主体認証方式であれば、例えば仮にパスワード（知識）が露呈してしまっても、IC カード（所有）又は指紋（生体）等の残りの主体認証情報が他者の手に渡らない限り、不正なログインを防ぐことができる。

また、通常の運用時は単一の主体認証を実施するケースであっても、認証の要求時に、アクセス元の IP アドレス、アクセスする時間帯、位置情報等が通常のアクセスとは異なる特徴が確認された場合は、不正ログインのリスクが高まったと判断して多要素主体認証を行う方法も考えられる。

2 段階認証の例として、利用者の携帯電話の電話番号や利用者の電子メールアドレスに対してワンタイムパスワードを送信して利用者に入力させる方法やスマートフォン等への認証要求を利用した認証方式などがあるが、AiTM（Adversary in The Middle）と呼ばれる高度なフィッシング攻撃（正規の認証画面へのアクセスに対するプロキシサーバとして機能し、正規の認証画面によく似たコンテンツをリアルタイムに表示するフィッシングサイト上で認証を行わせることで、2 段階認証済の cookie を窃取する攻撃）により、2 段階認証を突破されてしまう可能性がある。また、スマートフォン等への認証要求を利用した認証方式については、不正な認証要求に対して誤って許可を

してしまう多要素認証疲労攻撃等に対しては脆弱であり、スマートフォン等の SMS や音声を使用した認証方式においては、SIM スワップ攻撃等に対して脆弱であるため、2 段階認証を突破されてしまう可能性がある。したがって、これらの 2 段階認証は、上記リスクを評価し、情報システムにおいてリスクを受容できるか判断した上で利用する必要がある。

なお、多要素主体認証方式の代表例として FIDO 認証がある。FIDO 認証は、端末等のデバイス側で生体情報等を用いた認証を行った上で、デバイスに保管された秘密鍵を用いた公開鍵暗号方式によりサーバ側で端末認証を行う仕組みである。したがって、FIDO 認証は多要素主体認証方式に該当する。デバイスの紛失等のリスクを評価した上で利用する必要があるが、デバイスの紛失等が生じた場合であっても、秘密鍵を OS 等のプラットフォームの機能を介して複数のデバイス間で同期することによって認証を可能とする、「マルチデバイス対応 FIDO 認証資格情報（マルチデバイス FIDO クレデンシャル）」と呼ばれる仕組みも登場している。本方式はフィッシング耐性を有するが、プラットフォーマーのアカウントが侵害された場合、当該サービスのアカウントも侵害されてしまうこと等を考慮する必要がある。

- **基本対策事項 7.1.1(1)-3 「フィッシング耐性を有する方式」について**

ウェブブラウザを介した主体認証機能が、パスワードを用いた認証方式で実現されている場合、フィッシング攻撃によってパスワードを窃取されてしまう危険性があり、2 段階認証を用いたとしても、「（解説）基本対策事項 7.1.1(1)-2「多要素主体認証方式」について」で述べたように、AiTM 型のフィッシング攻撃によって、2 段階認証も突破されてしまう危険性がある。これに対して、フィッシング耐性のある認証方式は、AiTM 型のフィッシング攻撃に対しても耐えるものであり、偽サイト上で誤って認証を開始しようとしても、認証が成功しない仕組みを実現するものである。

フィッシング耐性のある認証方式は、ウェブブラウザに組み込まれた仕組みを用いることなしには実現できないものであり、ウェブサーバ側の工夫だけでは実現できないことに留意が必要である。W3C Web Authentication（WebAuthn）は、フィッシング耐性のある認証方式の一つであり、今日の主要ブラウザに標準で組み込まれている。WebAuthn は、「検証者名バインディング」と呼ばれる手法により、あらかじめ登録したウェブサイトにアクセスしたときにしか認証が成功しない仕組みを実現している。

フィッシング耐性のある認証方式には、WebAuthn のほかにも、マイナポータルで用いられているような、独自のウェブブラウザ拡張機能によって検証者名バインディングに相当する仕組みを実現する方法もある。フィッシング耐性のある認証方式として WebAuthn 以外の独自の方法を用いる場合には、検証者名バインディングに相当する仕組みが適切に実装されたブラウザ拡張機能を用いる必要がある。

- **基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について**

強固なパスワードの要件を一律に定めることは困難であるが、少なくとも、一般的に知られる単語 1 つを用いたものや、キーボードの並び順（「qwertyuiop」等）をなぞったものは、たとえそこに数字や記号を付加しようとも、脆弱であり、設定を許すべきで

はない。他方、ランダムに生成されたパスワードは、適切な長さであれば、強固なものとなる反面、利用者の記憶を要する場合には必ずしも強制できない面がある。利用者が記憶しやすいランダム生成の強固なパスワードの例としては、ランダムに複数の単語（例えば、10 万語の辞書から 3 語、2 万語の辞書から 4 語など）を選んでつなげたものなどが考えられる。そのようなパスフレーズを用いたパスワードを設定する際は、可能な限り桁数を増やして安全性を高める必要がある。

強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を利用者に守らせる機能を実現するには、ランダム生成を支援する機能を提供することや、利用者が入力したパスワード候補に対して、適切なパスワードチェッカー（パスワードの強度を評価するソフトウェア）を用いて、脆弱と判断された候補を拒否する機能を設けることなどが考えられる。ただし、既存のパスワードチェッカーの中には、単語 1 つやキーボードの並び順に数字や記号を付加しただけで合格としてしまう不完全なものも散見されるので、注意が必要である。適切なパスワードチェッカーの例としては、過去に流出が報告されているパスワード文字列と同じものを不合格と判定するものなどが挙げられるが、これに限られない。

また、設定可能なパスワードについては、以下のような第三者に安易に推測可能なパスワードを使用させないための機能を設けることが重要である。

- 識別コードと同じパスワード
- 端末名やサーバ装置名、組織名等の安易な情報を含んだパスワード
- ソフトウェアや通信回線装置などの初期値として設定されているパスワード
- インターネット等において掲載されている「よく使われるパスワード」などの一覧と一致するパスワード
- 年月日等の日付の組み合わせから想定される数字列（例：0321, 2021, 202204, 20220401,etc）
- 上記に関して、一部の文字を似たような文字に変換しただけのパスワード（例 S→$、O→0 等）
- 上記の組み合わせ
- 有名な言葉などを用いたパスフレーズ

これらのうち、機能として設けることができないものに関しては、注意喚起するなどの対策を講ずることも考えられる。

さらに、端末やサーバ装置においてパスワードに設定できる桁数等を制限する機能を一元的に管理するための仕組みを用いる場合、利用者に守らせる制限の内容を変更した場合は、新規に登録する識別コードに対してのみ制限の内容を適用するのではなく、既存の識別コードに対しても同様の制限を適用するため、パスワードを再設定させるようにするなどの対策を講ずる必要がある。

また、利用者にパスワードの定期的な変更を求めることは、利用者の利便性を低下させ、利用者が強度の低い安易なパスワードを設定しやすくなるなど、結果的に主体認証機能の安全性を低下させる懸念があるため、実施しないことが望ましい。何らかの理由により必要があって実施する場合は、その理由に応じた適切なタイミングと方法で実施する必要がある。

なお、本解説は情報システムや情報へのアクセス主体を特定するための主体認証情報を設ける際の解説となるが、情報自体を暗号化する場合は、「（解説）基本対策事項 3.1.1(6)-2 a)「運搬する情報を暗号化する」について」を参照のこと。

- **基本対策事項 7.1.1(1)-5 a)「初期値として設定されている識別コードを使用しない」について**

  端末やサーバ装置、通信回線装置などで使用されている初期値として利用可能な識別コード（Administrator、root、admin 等）は、誰もが識別コードを知っているため不正アクセスの標的となる可能性が高い。そのため、そのような識別コードは無効化し、新たに別の識別コードを用意することが望ましい。やむを得ず、そのような識別コードを使用する場合は、強固な認証技術を用いることが重要である。

- **基本対策事項 7.1.1(1)-5 b)「不要な識別コードを無効にする」について**

  情報システムを構築した際、情報システムを構築する際に使用する識別コードやテスト用の識別コードなどを登録している可能性がある。そのような識別コードが残っていると不正に利用される可能性もあるため、運用開始前までに削除又は無効化するなど、利用できないようにする必要がある。

遵守事項

(2) 識別コード及び主体認証情報の管理

(a) 情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び**主体認証情報を適切に付与**し、管理するための措置を講ずること。

(b) 情報システムセキュリティ責任者は、主体が**情報システムを利用する必要がなくなった場合**は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。

【 基本対策事項 】

＜7.1.1(2)(a)関連＞

7.1.1(2)-1 情報システムセキュリティ責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下遵守事項 7.1.1(2)(a)において同じ。）すること。また、識別コードを情報システムにアクセスする者に交付する際には、身分証明書等による本人確認を行うこと。

7.1.1(2)-2 情報システムセキュリティ責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずること。

a) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

b) 主体への識別コードの付与に関する記録を消去する場合の情報セキュリティ責任者からの事前の許可

7.1.1(2)-3 情報システムセキュリティ責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合、主体以外の者が設定する主体認証情報は**強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を設定**し、主体へ**安全な方法で主体認証情報を配布する**よう、措置を講ずること。

7.1.1(2)-4 情報システムセキュリティ責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、主体以外の者が設定した主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。なお、主体認証情報の変更を確認できる機能がある場合は、変更日時を確認し変更がなされない(使用していない)識別コードについては無効にするなどの措置を講ずること。

7.1.1(2)-5 情報システムセキュリティ責任者は、知識による主体認証方式を用いる場合には、**他の情報システムで利用している主体認証情報を設定しない**よう主体に注意を促すこと。

7.1.1(2)-6 情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず**共用識別コードを付与する必要がある場合**には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する実施手順を整備し、その実施手順に従って利用者に付与すること。

＜7.1.1(2)(b)関連＞

7.1.1(2)-7 情報システムセキュリティ責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずること。

a) 当該主体の**識別コードを無効にする**こと。

b) 当該主体に交付した主体認証情報格納装置を返還させること。

c) 無効化した識別コードを他の主体に新たに発行することを禁止すること。

（解説）

- **遵守事項 7.1.1(2)(a)「主体認証情報を適切に付与」について**

情報システムにおいて認証機能を統合している場合、各機器等の管理者権限を持つローカルアカウントは通常の運用では未使用となるが、その場合においてもデフォルトパスワードのままにせず、設定するパスワードについても同一の値にしないといった措置を講ずる必要がある。

なお、主体認証が必要となる場面が多岐にわたるような情報システムの場合、認証連携を適切に用いることにより、業務の効率化を図ることも考えられる。

- **遵守事項 7.1.1(2)(b)「情報システムを利用する必要がなくなった場合」について**

情報システムの利用者に対して付与した識別コードの中には、識別コードを付与しても利用しない主体がいる可能性がある。また、人事異動等によって情報システムへアクセスする必要がなくなった識別コードをそのままにしている可能性がある。そのような識別コードを残していると不正に利用される可能性もあるため、不要な識別コードは定期的に確認し、無効にするなどの対処を講ずる必要がある。

- **基本対策事項 7.1.1(2)-3「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を設定」について**

強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等については、「（解説）基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照のこと。

- **基本対策事項 7.1.1(2)-3「安全な方法で主体認証情報を配布する」について**

利用者以外の者（情報システムの管理者等）が主体認証情報を設定する場合には、以下を例とする方法で、当該主体認証情報を安全な方法で利用者に配布する必要がある。

  - 本人の電子メールアドレスに対し、必要に応じて、暗号化を施すことにより、主体認証情報を送付する。この際、暗号化された主体認証情報が添付された電子メールに復号するための鍵を同時に付すのではなく、復号するための鍵は、別の方法を用いて送信することが望ましい。
  - 本人の電子メールアドレスに対して主体認証情報を入手するためのウェブサイトを送付し、別の方法を用いてパスワードを送付、当該パスワードによる認証の上で当該ウェブサイトから主体認証情報をダウンロードする。

- 本人の住所に対して主体認証情報を運搬する。

- **基本対策事項 7.1.1⑵-5「他の情報システムで利用している主体認証情報を設定しない」について**

  複数の情報システムにおいて共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に利用されるというリスクが発生する。機関等の管理下にない情報システムからの漏えいを防止することは不可能であるため、このような情報システムから主体認証情報が漏えいした場合の機関等の情報システムへの影響について考慮する必要がある。対策の例としては、他の情報システムで利用している主体認証情報を機関等の情報システムに設定しないよう注意喚起を表示する、識別コードを情報システム側で割り当てることで識別コードの共通利用を防止する、といった方法が考えられる。

- **基本対策事項 7.1.1⑵-6「共用識別コードを付与する必要がある場合」について**

  共用識別コードは、その利用履歴だけでは利用者を特定できないため、不正な利用の検知が難しく、また情報セキュリティインシデントが発生した場合の真相究明の支障となる可能性がある。この点を踏まえ、やむを得ず、共用識別コードを利用する場合には、利用者を特定するための以下を例とする仕組みを講ずる必要がある。

  - 当該情報システムにおける別途の認証手段を併用する
  - 入退室管理装置等の物理的認証手段を併用する
  - 第三者による承認を得てから利用する（その際、共用識別コードを使用したことが通知される仕組みも併せて設けること。）。

  また、共用識別コードの主体認証情報は、悪用されないために主体認証情報を知る者を限定するなどの措置を講ずる必要がある。普段は共用識別コードを利用しない職員等が共用識別コードを使用する場合は、一時的に利用する主体認証情報を設定することなどの対策も有効である。

- **基本対策事項 7.1.1⑵-7 a)「識別コードを無効にする」について**

  識別コードの付与を最小限に維持するため、退職等により不必要となった識別コードについては、これを無効にする必要がある。また、本人からの届出による場合のほか、登録した識別コードに異常がないことを確認する目的で、定期的に不要な識別コードが存在しないことを確認することが望ましい。

7.1.2 アクセス制御機能

目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

遵守事項

(1) アクセス制御機能の導入

(a) 情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

(b) 情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

【 基本対策事項 】

＜7.1.2(1)(a)関連＞

7.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、情報システムの分類に基づき、以下の対策を実施すること。

【基本セキュリティ対策】以下を例とするアクセス制御機能の要件を定めること。

a) 利用時間や利用時間帯によるアクセス制御

b) 同一主体による複数アクセスの制限

c) IP アドレスによる端末の制限

d) ネットワークセグメントの分割によるアクセス制御

e) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討すること。

f) 認証・認可の統合管理基盤を用いたアクセス制御

g) アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御

＜7.1.2(1)(b)関連＞

7.1.2(1)-2 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件の定期的な確認による見直しをすること。

（解説）

- **基本対策事項 7.1.2(1)-1「主体の属性、アクセス対象の属性に基づくアクセス制御」について**

  具体的な手法としては、端末や共有フォルダ上のファイルやフォルダ（ディレクトリ）に対する許可属性のリストであるアクセス制御リスト（ACL： Access Control List）が挙げられる。ACL では例えば、アクセス対象の所有者／所有者の属するグループ／全利用者といったアクセス主体に対して、読み取り／書き込み／実行の権限を設定する。

  ただし、一般的な情報システムでは、利用者が適切なアクセス制御の設定を行っても、システムの管理者は全てのファイルやフォルダへアクセス可能である。実際に、運用保守の担当者が、管理者権限相当のアクセス権限を行使して、機密性の高い情報を不正に閲覧するといった事案も確認されている。そのため、アクセス対象が要機密情報等の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等されないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。

- **基本対策事項 7.1.2(1)-1 d)「ネットワークセグメントの分割によるアクセス制御」について**

  業務や取り扱う情報の性質・量に応じて、重要な情報に攻撃が到達しないよう、情報システムの重要な情報を取り扱う部分を他の情報システムやインターネットから分離するといった対策をとる必要がある。特に、情報システムの管理を行う部分を独立したネットワークセグメントとし、これをインターネットから切り離すことは、攻撃の拡大阻止の観点から有効である。同時に、ネットワークセグメント分割の意義を損なうことのないよう、各システムで取り扱うことができる情報についてルール化し、職員等に徹底することも重要である。また、他の情報システムやインターネットから論理的に分離をする際は、必要最小限の IP アドレスやプロトコルが通信できるように制御し、許可しない通信に関しては拒否するなどの対策も重要である。

  なお、遵守事項 5.2.1(3)(a)(オ)において、構築する情報システムのネットワーク構成に関する要件について定めることを求めているが、本基本対策事項は、その際に併せて検討し、情報システムのネットワーク構成の要件を決定するとよい。

- **基本対策事項 7.1.2(1)-1 e)「ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御」について**

  ファイル自体にセキュリティ機能を組み込むことで、ファイルに対する閲覧、編集、印刷等の操作を制御する技術（DRM（Digital Rights Management）や IRM（Information Rights Management）として知られるデジタル著作権管理技術）を利用することも考えられる。この技術を利用したファイルは暗号化されるため、ファイルを利用するには、ファイルに記録された情報へのアクセスを制御するサーバで主体認証を受け、正当な主体として認識されること及びファイルへのアクセス権限が付与されていることが必要となる。そのため、第三者がファイルを閲覧しようとしても、主体

認証を受け、正当な主体として認識されない限り当該ファイルの内容を参照することはできず、ファイルに記録された情報の漏えいを防止することができる。

また、ファイル利用時には、利用者はファイルの暗号化・復号を意識することなく、付与されたアクセス権限に従った閲覧、編集、印刷等の操作を行えるため、利便性が損なわれることはない。

- **基本対策事項 7.1.2(1)-1 f)「認証・認可の統合管理基盤」について**

認証・認可の統合管理基盤とは、それぞれの情報システムにおいて行っている識別コード、主体認証情報、主体の属性等の管理やそれらを使用した主体認証機能及びアクセス制御機能を一元的に実施することを実現するためのものである。そのような基盤を用いてアクセス制御を行うことで、それぞれの情報システム間の整合性を確保しつつ、職員等の異動や機器の交換等による変化に合わせて、常に正しいアクセス制御を実現することができる。

- **基本対策事項 7.1.2(1)-1 g)「動的なアクセス制御」について**

クラウドサービスの利用拡大やテレワークの推進等により、情報システムの利用における業務環境等が変化することで、新たな脅威や攻撃経路などが増大する。このような脅威に対抗するためには、初回のアクセス要求時のみ制御を行うのではなく、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装することが有効である。

動的なアクセス制御については、7.3「ゼロトラストアーキテクチャ」を参照のこと。

- **基本対策事項 7.1.2(1)-2「アクセス制御の要件の定期的な確認による見直し」について**

主体の属性、アクセス対象の属性に基づくアクセス制御の要件については、機関等の業務の変化やクラウドサービス、テレワークといった情報システムの利用環境の変化等により、アクセス制御のセキュリティ要件が変化することを踏まえて、定期的な確認による見直しをする必要がある。

また、アクセス制御の要件の見直しにより、アクセス制御の設定の変更等を実施する場合は、情報システムセキュリティ責任者が指名した監督者の監視の下で設定変更等を実施することや、機械的なチェック機能を設けるなどの設定や修正によるミス等を防止するための対策を行うことが重要である。なお、アクセス制御の見直しを行う場合は、アクセス権限の付与は必要最小限の範囲に限ることを原則とすることが重要である。

7.1.3 権限の管理

目的・趣旨

情報システムのアクセス制御機能を適切に運用するためには、主体から対象に対するアクセスの権限を適切に設定することが必要である。その際、アクセス権限は最小権限の付与とするため、全てにアクセスできないことを前提に、アクセスの必要がある主体に対してのみ権限を付与し、アクセスの必要のない主体に対しては権限を与えないことを原則とすることが重要である。また、情報に対して権限を付与する場合も同様に、知る必要のある主体に対してのみ権限を付与し、知る必要のない主体に対しては権限を与えないことを原則とすることが重要である。なお、権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。

また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報のみならず特権アクセスが可能な情報等の漏えい、改ざん、さらには情報システムや情報を破壊することを目的とした不正プログラムによって業務継続への影響もあり得る。また、これらの不正アクセスや不正プログラム等を検知又は防止するための設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

遵守事項

(1) 権限の管理

(a) 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずること。

(b) 情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

(c) 情報システムセキュリティ責任者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認すること。

【 基本対策事項 】

＜7.1.3(1)(a)関連＞

7.1.3(1)-1 情報システムセキュリティ責任者は、初期値として利用可能な管理者権限を有する識別コードには、管理者権限を付与しない又は無効化にすること。

＜7.1.3(1)(b)関連＞

7.1.3(1)-2 情報システムセキュリティ責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、また、管理者による権限の濫用や作業ミスを防ぐため、以下を例とする措置を講ずること。

a) 業務上必要な場合に限定すること。

b) 必要最小限の権限のみ付与すること。

c) 同一の者が権限の付与と権限の執行を兼ねないようにすること。

d) 管理者権限を行使できる端末をシステム管理者等の専用の端末とすること。

7.1.3(1)-3 情報システムセキュリティ責任者は、管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させないこと。

（解説）

- **遵守事項 7.1.3(1)(b)「内部からの不正操作や誤操作を防止するための措置」について**

  権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、複数名による主体認証操作がなければ、その処理自体を完遂できない「デュアルロック機能」や「ワークフロー機能」を導入することが考えられる。

  その他の情報システムについては、操作ログを取得することや、確認画面を表示することなどの措置が考えられる。

- **遵守事項 7.1.3(1)(c)「不要なアクセス権限が付与されていないか定期的に確認する」について**

  主体から対象に対するアクセス権限については、人事異動等による主体の業務の変化等に応じて適切に付与する必要がある。特に管理者権限を付与した主体については、情報セキュリティインシデントの発生防止の観点等から管理者権限の付与が不要になった時点で権限を変更するなどの対策を実施する必要がある。また、保守やメンテナンスなどを実施するため、特定の主体に対して一時的に付与した権限については、必要な作業等が終了したら確実に権限の付与を削除する必要がある。したがって、このようなアクセス権限の付与が適切に行われているかを定期的に確認する必要がある。

- **基本対策事項 7.1.3(1)-1「初期値として利用可能な管理者権限を有する識別コード」について**

  初期値として利用可能な管理権限を有する識別コードとは、例えば、Administrator、root、admin などが考えられるが、そのような識別コードは誰もが知っているため不正アクセスの標的となる可能性が高い。そのため初期値として利用可能な管理権限を有する識別コードは無効化することが望ましい。やむを得ず利用する場合においても、管理者権限を付与しない又は権限を最小限にするなどの措置を講ずることを検討することが考えられる。

- **基本対策事項 7.1.3(1)-2 b)「必要最小限の権限のみ付与」について**

  必要最小限の権限のみ付与とは、権限が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な権限を付与することにより、当該権限を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。

  本対策の例として、システムを通常操作するユーザにおいては、あらかじめ実行できるプログラムやアクセス可能な領域を限定した権限を付与し、管理作業をするときに限定して管理者権限を利用することを可能とする方式（Unix 系システムにおける sudo

等）が考えられる。

特に核心的な強い権限（アカウント管理者、権限管理者等）は常時付与せず、権限の執行が必要となった時に権限有効化申請を都度実施のうえ、承認を受けたうえで執行することが望ましい。

7.1.4 ログの取得・管理

目的・趣旨

情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

(1) ログの取得・管理

(a) 情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

(b) 情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じて**ログを取得する目的**を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの**保存期間**、要保護情報の観点でのログ情報の取扱方法等について定め、適切にログを管理すること。

(c) 情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に**点検又は分析**する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

【 基本対策事項 】

＜7.1.4(1)(b)関連＞

7.1.4(1)-1 情報システムセキュリティ責任者は、所管する情報システムの特性に応じて想定される脅威を分析し、分析事象・観点を見極めた上で、ログとして取得する必要のある情報項目を定め、管理すること。

7.1.4(1)-2 情報システムセキュリティ責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の**時刻を同期**させ、ログに時刻情報も記録されるよう、設定すること。

7.1.4(1)-3 情報システムセキュリティ責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、**ログ情報の保全方法**を定めること。

＜7.1.4(1)(c)関連＞

7.1.4(1)-4 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、情報システムの分類に応じて以下の対策を実施すること。

【基本セキュリティ対策】以下を例とする当該作業を支援する機能を導入すること。

a）ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化機能

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とする当該作業を支援する機能の導入を検討すること。

b）リアルタイムでのログの調査・分析を行うための機能

（解説）

- **遵守事項 7.1.4(1)(b)「ログを取得する目的」について**

情報システムにおけるログは、情報セキュリティインシデント発生時や情報セキュリティインシデントの予兆となる現象を特定する際に重要な役割を果たすほか、情報セキュリティインシデント対応及びサイバー脅威の分析においても重要な材料となることから、ログを取得する目的を明確にしたうえで、必要なログを取得・保存し適切に保護、管理する必要がある。

ログを取得する目的は、情報システムの特性（取り扱われる情報、接続されるネットワーク、設置環境、利用者等）や想定される脅威に応じ、当該情報システムでどのような事象を検知すべきか、そのためにはどのような情報をどう分析する必要があるかを見極めた上で設定し、目的を実現するために取得すべきログ情報やその保存期間等を検討する必要がある。

また、ログの取得に当たっては、IoC やアノマリ（異常値）の検知に資する情報が含まれるよう留意する必要がある。

不正アクセス、DoS 攻撃、内部不正による情報漏洩、マルウェア感染等の脅威に対する分析事象・観点の設定方法、必要な情報・分析などについては、デジタル庁「政府情報システムにおける脅威の検知・対応のためのログ取得・分析導入ガイドブック」に例示があるため、参考にするとよい。

参考：デジタル庁「政府情報システムにおける脅威の検知・対応のためのログ取得・分析導入ガイドブック」
（https://www.digital.go.jp/resources/standard_guidelines）

- **遵守事項 7.1.4(1)(b)「保存期間」について**

保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、情報セキュリティインシデント対応やサイバー脅威の分析の必要性も踏まえ、関連するガイドラインや想定されるリスクに基づき設定することが望ましい。標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、ログの長期保存にはコストがかかるため、費用を抑える観点から、直近のログはすぐに調査可能なハードディスク等のオンラインの電磁的記録媒体に保存し、それ

以降はテープや光ディスク等の長期保存に適した外部電磁的記録媒体に保存する方法も考えられる。オンラインの電磁的記録媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

- **遵守事項 7.1.4(1)(c)「点検又は分析」について**

  情報システムの特性等に応じて、点検・分析の頻度や分析の精度を高める必要がある場合には、ログを分析するための製品である SIEM などを導入することや監視事業者への委託を検討することが考えられる。

- **基本対策事項 7.1.4(1)-2「時刻を同期」について**

  具体的な実装例としては、ログを取得する機器のシステム時刻を、タイムサーバを用いて同期する方法がある。タイムサーバは、NTP（Network Time Protocol）や SNTP（Simple Network Time Protocol）等の方式により、ネットワーク上のクライアント機器に対して、時刻を提供する。例えば、公開 NTP サービスを用いる方式や組織内にタイムサーバを設置し、サーバ装置・端末・通信回線装置をタイムサーバに時刻同期するよう設定する方式が挙げられる。後者については、タイムサーバを複数利用することにより、時刻の精度や冗長性を高めることができる。

  また、機器によっては明示的に設定を行わないとログに出力する時刻が現地時間とならない場合があるため注意が必要である。

- **基本対策事項 7.1.4(1)-3「ログ情報の保全方法」について**

  取得したログ情報に対する不正な消去、改ざん及びアクセスを防止するためのログ情報の保全方法として、以下の例が考えられる。

  - ログ収集サーバにログを転送し保存する。ログ収集サーバの管理者を他のサーバ等の管理者と異なる者とし、他の管理者によるログ情報の消去や改ざんが行われないようにする。
  - ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保管する。
  - ログを書き換え不能な外部電磁的記録媒体（DVD-R 等）に書き出して保管する。

- **基本対策事項 7.1.4(1)-4 a)「自動化機能」について**

  ログとして取得する項目数、利用者数等が多くなるにつれて、ログの量は膨大になり、システム担当者等がログを目視することによって問題（又はその予兆）を検出するのは、困難を極める。システム自体に実装される機能や各種運用管理ツールを組み合わせ、ログの点検・分析・通知が自動的に実行されるなど、ログ管理作業を支援する仕組みを構築することが望ましい。

- **基本対策事項 7.1.4(1)-4 b)「リアルタイムでのログの調査・分析を行うための機能」について**

  リアルタイムでのログの調査・分析を行うための機能を具備する製品については、SIEM などが考えられる。

SIEM を利用することにより、端末、サーバ装置、通信回線装置等の様々なログを組み合わせた相関分析を行うことができ、特定のログ分析だけでは検知できなかった異常が検知できるだけでなく、リアルタイムで自動的に異常を検出できるようになるため、情報セキュリティインシデントへの対処開始に要する時間が短縮できる。

ただし、SIEM 等によるリアルタイムでのログの調査・分析を行うための機能を情報システムに実装する場合、導入だけでなく、運用・保守の業務負荷等が増大することから、高度なセキュリティ対策が必要となる情報システム、情報システムを利用して行う業務等を勘案し、導入を判断することが望ましい。

また、収集したログを SIEM 等のシステムで一元的に保存する場合は、許可された管理者のみがアクセスできるようアクセス制御を施すことが望ましい。

また、SIEM 等によるリアルタイムでのログの調査・分析を行うための機能を実装しない場合、ファイアウォール、IDS/IPS、EDR、NDR（Network Detection and Response）等のセキュリティ対策機器やソフトウェアに加え、SOC（Security Operation Center）や NOC（Network Operations Center）等での監視を実施するなどの対策を講ずることを検討するとよい。

7.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズム及び鍵長に加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズム又は鍵長が危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された**「電子政府推奨暗号リスト」に基づき**、情報システムで使用する暗号及び電子署名の**アルゴリズム及び鍵長**並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

(c) 情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な**公的な公開鍵基盤が存在する場合はそれを使用する**など、目的に応じた適切な公開鍵基盤を使用するように定めること。

【 基本対策事項 】

＜7.1.5(1)(a)関連＞

7.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、**暗号モジュールを交換**することが可能な構成とすること。

b) **複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択**することが可能な構成とすること。

c) 選択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、**「暗**

号モジュール試験及び認証制度」に基づく認証を取得している製品を選択すること。

d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納すること。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮すること。

＜7.1.5(1)(b)関連＞

7.1.5(1)-2 情報システムセキュリティ責任者は、職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、情報システムで使用するアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを、「電子政府推奨暗号リスト」に基づき定めること。

7.1.5(1)-3 情報システムセキュリティ責任者は、基本対策事項 7.1.5(1)-2 で定めた事項の運用方法について、以下を全て含めて実施手順として定めること。

a) 暗号化及び電子署名に使用するアルゴリズム又は鍵長が危殆化した場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

b) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

（解説）

- **遵守事項 7.1.5(1)(b)「「電子政府推奨暗号リスト」に基づき」について**

職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長を定めることが原則である。

しかし、職員等が利用するソフトウェアや連携する他の情報システム側が「電子政府推奨暗号リスト」に記載されたアルゴリズム又は鍵長に対応していない等の場合は、利用実績が不十分であること、また、今後の普及が見込めない可能性があることによる影響を踏まえた上で、「推奨候補暗号リスト」に記載されたアルゴリズム及び鍵長を利用するとよい。

なお、「運用監視暗号リスト」に記載されたアルゴリズム及び鍵長は互換性維持以外の目的での利用をしてはならない。また、互換性維持の目的であったとしても、暗号が解読される等のリスクが考えられるため、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長への移行を検討する必要がある。

参考：CRYPTREC「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（CRYPTREC LS-0001-2022R2）
（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf）

- **遵守事項 7.1.5(1)(b)「アルゴリズム及び鍵長」について**

  「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」に掲載されている暗号技術を利用する際に、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致しない鍵長を用いた場合には、「電子政府推奨暗号リスト」の暗号技術を利用しているとは見なしていないことに留意が必要である。

  参考：CRYPTREC「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（CRYPTREC LS-0003-2022R1）
  （https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf）

- **遵守事項 7.1.5(1)(c)「公的な公開鍵基盤が存在する場合はそれを使用する」について**

  保健医療福祉分野の公開鍵基盤（HPKI）のように特定の分野における公的な PKI が存在し、その使用が求められる場合に、当該 PKI を使用することが考えられる。

  また、政府機関及びその職員が申請・届出等手続において電子署名を行う際には政府認証基盤（GPKI）を使用することが考えられる。

- **基本対策事項 7.1.5(1)-1 a)「暗号モジュールを交換」について**

  暗号モジュールは、暗号化、電子署名、ハッシュ関数等の暗号に関連した機能を提供するソフトウェアの集合体又はハードウェアとして定義される。選択した暗号化アルゴリズム又は鍵長が将来危殆化することを想定し、暗号モジュールの交換が可能な構成とすることを、情報システムの設計段階から考慮する必要がある。

  また、事前に暗号モジュールのアプリケーションインタフェースを統一することなどを考慮する必要がある。

- **基本対策事項 7.1.5(1)-1 b)「複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択」について**

  選択したアルゴリズム又は鍵長が将来危殆化することを想定し、危殆化していない他のアルゴリズム及び鍵長へ直ちに変更できる機能と併せて、暗号利用モード等との組合せ等により脆弱性の顕在化が認められない安全なプロトコルを選択できる機能も、あらかじめ情報システムに設けておく必要がある。

- **基本対策事項 7.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について**

  アルゴリズム及び鍵長自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する擬似乱数に偏りが生じるなどの理由で擬似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生じるなどの理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがあることから、これらを確認するには、ISO/IEC 19790 に基づく「暗号モジュール試験及び認証制度」が利用可能である。

- **基本対策事項 7.1.5(1)-1 d)「耐タンパ性」について**

JIS X 19790（ISO/IEC 19790）の規定によると、耐タンパ性は以下の３つの機能から構成される。

- タンパ検出
  暗号モジュールのセキュリティを危殆化する試みがなされたことの、暗号モジュールによる自動的な判定
- タンパ証跡
  暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、観察可能な表示
- タンパ応答
  暗号モジュールがタンパを検出したときにとる自動的な動作

また、暗号モジュールを利用する環境等に応じ、セキュリティレベルが１から４まで設定されている。セキュリティレベル１は、最小限の物理的保護を要求している。セキュリティレベル２では、タンパ証跡メカニズムの追加を要求している。セキュリティレベル３では、除去可能なカバー及びドアに対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。セキュリティレベル４では、囲い全体に対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。

なお、タンパ検出及びタンパ応答は、タンパ証跡の代わりにはならない。

暗号モジュールの耐タンパ性に関わるセキュリティレベルは、情報システムが取り扱う以下の特性を踏まえて選択することが望ましい。

- 暗号化又は復号する情報の特性
- 電子署名が付与される情報の特性

- **基本対策事項 7.1.5(1)-1 e)「安全性に実績のあるプロトコル」について**

情報システムで暗号を用いるとき、暗号アルゴリズム及び鍵長の適切な選択に加え、暗号プロトコル（暗号アルゴリズム及び鍵長をどのように用いるかの手順）が適切なものとなっている必要がある。一般に、情報システムを新規に構築するときに、独自の暗号プロトコルを設計することは、その安全性について十分に検証されないときは、期待される安全性が確保されていない可能性がある。安全な暗号プロトコルの設計は高度な専門性を有する者以外には容易なことではないため、可能な限り、独自の設計を避け、既に広く利用実績のある著名な暗号プロトコルを用いることが求められる。

なお、必要とする機能を実現する暗号プロトコルとして既存のものが存在しない場合はこの限りでないが、独自に暗号プロトコルを設計するときは、その安全性に関して十分に検証する必要がある。

- **基本対策事項 7.1.5(1)-1 e)「長期的な秘匿性」について**

情報システム上で機微な情報のやり取りを行う場合、情報を暗号化して通信しても、その暗号文が悪意ある第三者等に傍受され、将来の解読に備えて長期間にわたり保管されるという脅威が想定される。この場合に、前方秘匿性を有しない暗号プロトコルを用いた結果、公開鍵暗号の鍵交換で使用した秘密鍵（以下本解説において「秘密鍵」と

いう。）が将来破られることになれば、過去に遡って全ての暗号文が解読されてしまうことになる。「前方秘匿性」とは、秘密鍵に対して乱数を付加することで、毎回異なる秘密鍵を使ったセッション鍵の共用により、秘密鍵が破られた場合でも乱数が破られなければ、過去に遡った暗号文が解読される可能性を低減することができる性質のことをいう。なお、TLS で使う暗号スイートの中では、DHE（Ephemeral DH）及び ECDH（Ephemeral ECDH）方式が前方秘匿性を有している。

そのため、長期の機密性を確保する必要のある機微な情報のやりとりを行う情報システムを構築するときは、前方秘匿性を実現する暗号プロトコルの採用を検討し、必要かつ可能であれば、採用することが求められる。

- **基本対策事項 7.1.5(1)-3 a)「アルゴリズム又は鍵長が危殆化」について**

暗号化や電子署名に用いられる暗号アルゴリズム及び鍵長は、年月が経つにつれ、情報システムの処理能力の向上や新たな暗号解読技法の考案等によって、アルゴリズム及び鍵長の設計当初の強度を失い、結果として、安全性を保てなくなる。

暗号アルゴリズム及び鍵長の強度には理論上の強度及び実装上の強度が存在する。理論上の強度の低下は情報システムの処理能力の向上や暗号解読法の考案によるところが大きく、実装上の強度の低下はサイドチャネル攻撃等の攻撃技術によるところが大きい。サイドチャネル攻撃の例として、実装時に暗号アルゴリズム及び鍵長の動作に伴う消費電力や暗号モジュールから漏えいする電磁波等の付加的な情報を悪意ある第三者等が知り得る場合には、実装上の強度は極端に低下する可能性がある。

- **基本対策事項 7.1.5(1)-3 b)「管理手順を定めること」について**

暗号化された情報の復号又は電子署名の付与に用いる鍵（以下本解説において「鍵」という。）の管理手順として、CRYPTREC が発行している「暗号鍵管理システム設計指針（基本編）」や「暗号鍵設定ガイダンス」を参照しつつ、以下の視点を含む鍵のライフサイクルを考慮した管理手順を策定するとよい。また、暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、適切に管理する必要がある。

  - 鍵の生成
    適切な暗号モジュールの内部において、その値を推定することが困難である乱数又は擬似乱数に係る処理を通じて生成し、かつ利用者以外の者が入手できないことを保証する仕組みを備える必要がある。
  - 鍵の配送
    鍵の受取先と事前に対面等で確認し合うなどにより、受取先の正当性に係る十分な確証が得られない限り、オンライン上での鍵の配送を行うべきではない。鍵を配送する際は、受取先のなりすまし対策等、配送先が確実であることを保証するとともに当該鍵に係る情報が適切に保護される仕組みを備える必要がある。
  - 鍵の保管
    鍵は、例えば HSM 等の保存装置又は記録媒体等に適切に保護された環境で保管され、第三者等による窃取の防止に加え、改ざんからの保護、検知及び回復を実現する仕組みを備える必要がある。

- 鍵の利用
  鍵はその運用期限が有効な限り、当該鍵へのアクセスが取扱いの許可されたものだけに限定されるよう可用性が確保され、かつ適切に実装された上で利用する必要がある。
- 鍵の期限切れ
  有効期限を過ぎた鍵は使用を停止し、適切な手段で取り除かれる必要がある。
- 鍵の更新
  鍵の有効期限が終了した後も運用を継続する場合、鍵としての継続性を維持するため、基本的に有効期限の終了前に古い鍵のパラメータを基に、新たな鍵を生成することが望ましい。
  なお、古い鍵は適切に廃棄する必要がある。
- 鍵の失効
  鍵の漏えいによる危殆化や、鍵を利用していた職員等が組織から離れることに伴う鍵の登録抹消等により、そのコピーやバックアップが存在する場合も含め、有効期限前の鍵の利用を適切に停止する必要がある。
- 鍵の廃棄
  特別な理由を除き、不要となった鍵の情報はそのコピーやバックアップが存在する場合も含め、有効期限後に適切な物理的又は電磁気学的な消去方法を用いて確実に消去する仕組みを備える必要がある。

参考：CRYPTREC「暗号鍵管理システム設計指針（基本編）」（CRYPTREC GL-3002-1.1）
（https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.1.pdf）

参考：CRYPTREC「暗号鍵設定ガイダンス」（CRYPTREC GL-3003-1.0.1）
（https://www.cryptrec.go.jp/report/cryptrec-gl-3003-1.0.1.pdf）

遵守事項

(2) 暗号化・電子署名に係る管理

(a) 情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の全ての措置を講ずること。

(ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。

(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズム又は鍵長の危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図ること。

【 基本対策事項 】

＜7.1.5(2)(a)(ア)関連＞

7.1.5(2)-1 情報システムセキュリティ責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。

a) 信頼できる機関による電子証明書の提供

b) 機関等の窓口での電子証明書の提供

（解説）

- **基本対策事項 7.1.5(2)-1 a)「信頼できる機関による電子証明書の提供」について**

例えば、信頼できる機関のサイトから、利用者が電子署名を検証するための電子証明書をダウンロードできるように環境を整備する方法である。利用者はダウンロードした電子証明書を端末に取り込み、それを基に署名検証を行う。

- **基本対策事項 7.1.5(2)-1 b)「機関等の窓口での電子証明書の提供」について**

機関等において、利用者に電子署名を検証するための電子証明書を電磁的記録媒体で配布する方法である。利用者は電磁的記録媒体経由で電子証明書を端末に取り込み、それを基に署名検証を行う。

7.1.6 監視機能

目的・趣旨

情報システムにおける情報セキュリティインシデントや不正利用等の速やかな認知や、情報セキュリティ対策の実効性を確認するためには、適切に監視機能を実装し、運用することが重要である。また、監視機能の実装に当たっては、情報システムの特性や当該情報システムで取り扱う情報の格付等を踏まえて、監視対象や監視内容を定める必要がある。

遵守事項

(1) 監視機能の導入・運用

(a) 情報システムセキュリティ責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、**監視機能を実装**すること。

(b) 情報システムセキュリティ責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用すること。

(c) 情報システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直すこと。

【 基本対策事項 】

＜7.1.6(1)(a)(c)関連＞

7.1.6(1)-1 情報システムセキュリティ責任者は、監視のために必要な機能について、**以下を例とする機能**を調達仕様書等に明記すること。

a) 機関等外と通信回線で接続している箇所における外部からの不正アクセスやサービス不能攻撃を監視する機能

b) 不正プログラム感染や踏み台に利用されること等による機関等外への不正な通信を監視する機能

c) 端末等の組織内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能

d) 機関等内通信回線への端末の接続を監視する機能

e) 端末への外部電磁的記録媒体の挿入を監視する機能

f) サーバ装置等の機器の動作を監視する機能

g) **ネットワークセグメント間の通信を監視**する機能

7.1.6(1)-2 情報システムセキュリティ責任者は、暗号化された通信データを**監視のために復号することの要否**を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を調達仕様書等に明記すること。

＜7.1.6(1)(b)関連＞

7.1.6(1)-3 情報システムセキュリティ責任者は、情報システムのセキュリティ監視について、以下の内容を全て含む**監視手順**を定め、適切に監視運用すること。

a) 監視するイベントの種類や重要度

b) 監視体制

c) 監視状況の報告手順や重要度に応じた報告手段

d) 情報セキュリティインシデントの可能性を認知した場合の報告手順
e) 監視運用における情報の取扱い（機密性の確保）

7.1.6(1)-4 **【追加セキュリティ対策】**情報システムセキュリティ責任者は、情報システム運用時の監視において、SOC や NOC 等の**セキュリティ監視を専門の外部事業者に業務委託**することを検討すること。

（解説）

- **遵守事項 7.1.6(1)(a)「監視機能を実装」について**

監視機能により監視を求められる対象やイベントは、情報システム及び取り扱う情報の格付や取扱制限等を考慮して必要性を見極める必要がある。職員等による情報窃取等の不正な動作を監視し、これらの不正な動作を検知・防止する内部脅威対策機能を備えた DLP の仕組みの導入を検討してもよい。

監視の対象やイベントとしては、以下が考えられる。また、監視の対象やイベントについては、新たな脅威の出現、運用の状況等により、定期的に見直す必要がある。

- クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信（基本対策事項 4.2.2(1)-4）
- クラウドサービス上の情報システムが利用するデータ容量や稼働性能（基本対策事項 4.2.2(1)-4、4.2.2(1)-12）
- 利用するクラウドサービスの不正利用（基本対策事項 4.2.2(1)-8）
- サーバ装置上での情報セキュリティインシデントの発生を監視する必要がある場合は、当該サーバ装置（遵守事項 6.2.1(2)(c)）
- 機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内で送受信される通信内容（遵守事項 6.4.1(2)(b)）
- 情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作（遵守事項 7.1.3(1)(b)）
- 要安定情報を取り扱う情報システムについて、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線（遵守事項 7.2.3(1)(c)）
- C&C サーバ等への不正な通信（基本対策事項 7.2.4(1)-5）

なお、監視に係る運用管理機能要件の策定の際には、イベント情報を効率的に活用できるようにするため、当該情報を収集する際のデータ形式については、その標準化の動向を踏まえ、一般的に用いられる見込みのある形式をとることが望ましい。

- **基本対策事項 7.1.6(1)-1「以下を例とする機能」について**

ここに例示した監視機能について、情報システムの構成を踏まえ、それぞれに監視対象となる脅威が存在するかどうかを検討し、脅威が存在すると判断した場合には、その全てを監視対象とすることが望ましい。

- **基本対策事項 7.1.6(1)-1 g)「ネットワークセグメント間の通信を監視」について**

異なるネットワークセグメントを接続する通信回線装置において、異なるネットワークセグメント間の通信を監視することにより、攻撃者による侵入範囲の拡大（ラテラル

ムーブメント：横方向の侵害）の試み等検知することを想定している。

- **基本対策事項 7.1.6(1)-2「監視のために復号することの要否」について**

  監視のために復号することの要否については、個人情報等の取り扱う情報の特性によって判断するとよい。

- **基本対策事項 7.1.6(1)-3「監視手順」について**

  情報システムのセキュリティ監視を行う体制を特別に設けずに、情報システムの運用を行う体制にてセキュリティ監視を行うことも考えられる。

  監視によりプライバシーを侵害する可能性がある場合は、対象となる関係者への説明等の手順についても機関等として定めておく必要がある。

- **基本対策事項 7.1.6(1)-4「セキュリティ監視を専門の外部事業者に業務委託」について**

  24 時間 365 日のセキュリティ監視の必要がある場合、セキュリティ監視を専門の外部事業者に業務委託することが考えられる。当該業務を外部事業者に請け負わせることは、「業務委託」に該当することから、4.1「業務委託」の規定を遵守する必要がある。さらに、機関等内通信回線に接続した機器等に対してインターネット等の外部ネットワークから直接接続してリモート監視を行わせる場合は、遵守事項 6.4.1(2)(c)も遵守する必要がある。また、外部事業者の選定に際しては、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監視・運用サービスに係る部分）を活用することが考えられる。

7.2 情報セキュリティの脅威への対策

7.2.1 ソフトウェアに関する脆弱性対策

目的・趣旨

機関等の情報システムに対する脅威としては、第三者が情報システムに侵入し機関等の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、個人情報等の重要な情報の漏えい等が発生した場合、国民生活に多大な影響を及ぼすとともに機関等に対する社会的な信用が失われる。

このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが多く見受けられる。したがって、機関等の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

(1) ソフトウェアに関する脆弱性対策の実施

(a) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

(b) 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施すること。

(c) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的及び適時に確認すること。

(d) 情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

【 基本対策事項 】

＜7.2.1(1)(a)関連＞

7.2.1(1)-1 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に以下の対策を実施すること。

【基本セキュリティ対策】インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置に対し脆弱性診

断を実施すること。また、その他のサーバ装置、端末及び通信回線装置については、情報システムの分類や保有する情報、システム特性等を踏まえ、脆弱性診断の実施を検討すること。

【追加セキュリティ対策】サーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、脆弱性診断の実施に当たっては、ペネトレーションテスト、TLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施を検討すること。

＜7.2.1(1)(a)(c)関連＞

7.2.1(1)-2 情報システムセキュリティ責任者は、対象となるソフトウェアの脆弱性に関して、以下を全て含む情報を適宜入手すること。

a) 脆弱性の原因
b) 影響範囲
c) 対策方法
d) 脆弱性を悪用する不正プログラムの流通状況

7.2.1(1)-3 情報システムセキュリティ責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

7.2.1(1)-4 情報システムセキュリティ責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認すること。

7.2.1(1)-5 情報システムセキュリティ責任者は、情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計を行い、実行可能な運用体制を構築・維持すること。

＜7.2.1(1)(c)関連＞

7.2.1(1)-6 【追加セキュリティ対策】情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の運用時に、定期的な脆弱性診断（ペネトレーションテスト、TLPT等の高度な脆弱性診断を含む。）の実施を検討すること。

7.2.1(1)-7 情報システムセキュリティ責任者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くすること。

＜7.2.1(1)(d)関連＞

7.2.1(1)-8 情報システムセキュリティ責任者は、ネットワーク境界にある通信回線装置や認証サーバ、要機密情報を保有するサーバ等のサイバーセキュリティリスクが高い機器等に対しては、原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずること。リスク評価結果を踏まえ措置を講じないと判断した場合には、リスク評価結果の記録を残すこと。

7.2.1(1)-9 情報システムセキュリティ責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、サイバー攻撃の高度化・自動化等の技術や脅威の動向を踏まえ、迅速な対策が必要であるかどうかを見極めた上で、以下の全ての事項について判断すること。

a) 対策の必要性
b) 対策方法。この際、自動でソフトウェアを更新する機能を有するIT資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法をあらかじめ決定すること。

c) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法

d) 対策方法又は回避方法が情報システムに与える影響。迅速な対策が必要である場合は情報システムの運用を一時停止することも検討すること。

e) 対策の実施予定時期

f) 対策試験の必要性

g) 対策試験の方法

h) 対策試験の実施予定時期

7.2.1(1)-10　情報システムセキュリティ責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認すること。

7.2.1(1)-11　情報システムセキュリティ責任者は、脆弱性対策を実施する場合には、少なくとも以下の全ての事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

a) 実施日

b) 実施内容

c) 実施者

7.2.1(1)-12　情報システムセキュリティ責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手し、完全性を検証すること。

（解説）

- **遵守事項 7.2.1(1)(b)「公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策」について**

対策としては、データ実行防止機能（DEP、Exec-Shield）の有効化、特定のメモリ上の実行権限の削除等の対策を実施すること等が挙げられる。

- **遵守事項 7.2.1(1)(c)「サーバ装置、端末及び通信回線装置上で利用するソフトウェア」について**

情報システムの構築時に、ソフトウェアを効率的に開発するために使用するソフトウェアフレームワークやソフトウェア部品が情報システムに組み込まれて納入される場合があることについても考慮する必要がある。当該フレームワークや部品についても脆弱性対策の状況を定期的に確認することが求められる。これを確実に実施するためには、対象とするソフトウェアの管理簿を作成することが望ましい。また、これらのソフトウェアには外部から入手するもののみでなく、機関等が自ら開発するもの及び委託により開発するものについても含まれる。

- **遵守事項 7.2.1(1)(c)「定期的及び適時に確認」について**

定期的に加え、脆弱性を悪用する不正プログラムの流通が確認されたり、当該脆弱性を悪用した被害が多く発生している等の重大な脆弱性が公開された場合には、適時、当該脆弱性の対策状況を確認する必要がある。

- **基本対策事項 7.2.1(1)-1「インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置」について**

  インターネットから攻撃を受ける可能性のあるサーバ装置、端末及び通信回線装置を想定している。グローバル IP アドレスが付与されているサーバ装置等は直接インターネットから到達可能なため、対象とする必要がある。また、グローバル IP アドレスを直接付与されていない場合であっても、静的 NAT（Network Address Translation）により実質的にグローバル IP アドレスを付与されているものと同じと考えられる場合は、これも対象とする必要がある。

- **基本対策事項 7.2.1(1)-1「脆弱性診断を実施」について**

  OS や各種サーバ、ファイアウォール等の通信回線装置等における脆弱性対策の状況を効率的に確認する方法として、専用ツールを用いて機関等自らが脆弱性診断を行ったり、事業者が提供するサービス等を利用して脆弱性診断を行うことが挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。

  ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。

  プラットフォーム診断では、OS や各種サーバ、ファイアウォール等を対象に、テスト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に 1 回診断を実施するなど、定期的に実施することが望ましい。

  ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信するなどの方法によって、SQL インジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ましい。診断の項目等については、OWASP の ASVS を参考にするとよい。

  なお、事業者が提供するサービス等を利用して脆弱性診断を行う場合には、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うち脆弱性診断サービスに係る部分）を活用することが考えられる。また、脆弱性診断の種別や対象範囲、事業者が提供するサービス等の検討に当たっては「政府情報システムにおける脆弱性診断導入ガイドライン」を参考にするとよい。

  開発を伴わない情報システムの導入を行う場合（パッケージ製品をプログラム開発

なしのパラメータ変更のみで利用する場合やSaaSサービスを利用する場合）やクラウドサービス等で利用者側の脆弱性診断が禁止されている場合については、ベンダから当該製品やサービスに関する脆弱性診断の実施結果等の証跡を徴求し、脆弱性対策が行われていることを確認する必要がある。また、証跡の徴求も困難な場合については、自組織の対策基準に基づきリスク評価を行った上で利用する必要がある。

参考：デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」
（https://www.digital.go.jp/resources/standard_guidelines/）

- **基本対策事項 7.2.1(1)-1「ペネトレーションテスト、TLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断」について**

  事業者が提供するサービス等を利用してペネトレーションテストを行う場合には、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うちペネトレーションテスト（侵入試験）サービスに係る部分）を活用することが考えられる。

- **基本対策事項 7.2.1(1)-2「情報を適宜入手」について**

  情報システムを構成するサーバ装置、端末及び通信回線装置上で利用するソフトウェアの脆弱性に関する情報は、製品ベンダや脆弱性情報提供サイト等を通じて適時調査を行う必要がある。自動アップデート機能を持つソフトウェアの場合には、当該機能を利用して、定期的に脆弱性に関連する情報が報告されているかを確認する方法で差し支えないが、自動アップデート機能の対象範囲を把握し、対象範囲外のソフトウェアについては適時調査を行う必要がある。例えば、ウェブアプリケーションの開発にソフトウェアフレームワークを利用する場合があるが、そのようなソフトウェアフレームワークは自動アップデートが行えないのが通常であるため、脆弱性の有無について適宜調査を行う必要がある。

  入手した脆弱性に関連する情報及び対策方法に関しては、脆弱性対策を効果的に実施するために、他の情報システムセキュリティ責任者と共有することが望ましい。

- **基本対策事項 7.2.1(1)-2 d)「脆弱性を悪用する不正プログラムの流通状況」について**

  脆弱性が既知になると、インターネット上の情報交換コミュニティ等を通じて、その脆弱性を悪用する方法が考案され、その悪用方法を機械的に実行するための不正プログラム（exploitコードとも呼ばれる。）が作られ、次第に広まっていく。この「脆弱性を悪用する不正プログラム」が流通している段階に入ると、脆弱性が攻撃されるリスクが格段に高まると考えられる。脆弱性を悪用する不正プログラムが世の中に流通していることが確認された場合には、速やかに当該の脆弱性について対処することを検討する必要がある。

- **基本対策事項 7.2.1(1)-3「サポート期間を考慮」について**

  利用するソフトウェアのサポート期間が過ぎた場合、それ以降はセキュリティ関連の脆弱性を修正するためのセキュリティパッチは、原則としてソフトウェアベンダか

ら提供されなくなる。したがって、情報システムのライフサイクルを考慮し、少なくとも情報システムの次期改修までは対策用ファイルの提供が継続されるソフトウェアを選定する必要がある。

また、情報システムは特定のソフトウェアバージョンに依存しないよう設計することが望ましいが、情報システムの中には、特定のソフトウェアバージョンに強く依存する場合がある。この場合には、ソフトウェアをバージョンアップすることが困難となるが、新しいバージョンのソフトウェアでしか対処できない脆弱性が発生したときに、情報システムの停止という最悪の事態も想定される。したがって、情報システムが特定のソフトウェアバージョンに依存せざるを得ない場合には、当該ソフトウェアのサポート期間を考慮して情報システムの更改について検討する必要がある。

- **基本対策事項 7.2.1(1)-3「サポートが受けられないソフトウェア」について**

ソフトウェアベンダによるサポートや他の事業者によるサポートサービスが一切受けられないものを対象としている。ソフトウェアベンダの製品ロードマップの見直し等により、サポートの打ち切りが突然予告されることもあり得るため、利用するソフトウェアのサポート期間に関する情報を適時入手し、ソフトウェア更改やサポート事業者の切替え等の対策が適切に講じられるよう考慮することが望ましい。

- **基本対策事項 7.2.1(1)-4「ソフトウェアのバージョン等を把握」について**

ソフトウェアのバージョン等の把握については、「(解説) 基本対策事項 5.2.2(1)-3 b)・基本対策事項 5.2.2(1)-5 b)「機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等」について」及び「(解説) 基本対策事項 5.2.2(1)-3 c)「ソフトウェアを動作させるために用いられる他のソフトウェア」について」を参照のこと。

例えば、外部から入手した脆弱性情報が世の中で大きな被害をもたらしているような緊急性の高い場合には、情報システムにおける該当する脆弱性の有無の確認を運用保守業者に作業を委託するのみでなく、情報システムセキュリティ責任者自らも情報セキュリティ関連文書を参照し確認することが望まれる。

- **基本対策事項 7.2.1(1)-5「情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計」について**

ソフトウェアに関する脆弱性対策では、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用される対策用ファイルが提供され次第、情報システムを構成する機器等に速やかに対策用ファイルを適用することが重要である。

一方で、情報システムの運用という観点では、情報システムの安定稼働を重視する場合、対策用ファイルを適用した場合の影響有無の調査・検証が必要であり、対策用ファイルの適用までの期間が長期化するだけでなく、対策用ファイルがほとんど適用されないといった状況が発生してしまうことは珍しくない。

しかしながら、不正アクセス、ランサムウェア等のサイバー攻撃において、ソフトウェアに関する脆弱性を悪用する手法は一般的であり、対策用ファイルの未適用は重大な情報セキュリティインシデントを引き起こす要因となっている。高性能 AI の悪用などのサイバー攻撃の高度化、自動化等を踏まえると、セキュリティパッチの速やかな

適用は非常に重要である。

そのため、情報システムの新規構築、更改時において、サーバ装置、端末、通信回線装置等の情報システムを構成する機器等へのセキュリティパッチ等の対策用ファイルの適時の適用を前提とした運用設計（パッチマネジメント（管理））を行う必要がある。また、サイバー攻撃の高度化、自動化等の状況を踏まえ、必要に応じて運用設計を見直し、脆弱性対策の強化を図る必要がある。

セキュリティパッチ等の対策用ファイルの適用を前提とした運用設計を行うためには、設計段階において以下を例とする内容を検討し、定めることが重要である。

- 情報システムの構成要素であるサーバ装置、端末、通信回線装置と、それぞれの機器等が利用するソフトウェア（ファームウェア含む。）の把握・管理
- セキュリティパッチ等の対策用ファイルの適用基準
- 対策用ファイルを適用した場合の影響有無の調査・検証手順

特に「セキュリティパッチ等の対策用ファイルの適用基準」は、製品、セグメント、脆弱性の深刻度等のセキュリティリスクを踏まえた判断基準を事前に定めておくことで、セキュリティリスクが高い場合にセキュリティパッチ等の対策用ファイルの適用を速やかに実施できる運用を構築し、即時適用してセキュリティ対策を優先する場合と影響調査・検証を必要とする安定稼働を優先する場合を明確にすることができる。

また、脆弱性の深刻度については、共通脆弱性評価システム「CVSS」や Microsoft 社の「深刻度評価システム（Security Update Severity Rating System）」などを活用することが考えられる。

- **基本対策事項 7.2.1(1)-6「定期的な」について**

定期的な脆弱性診断を実施する頻度については、少なくとも 1 年に 1 回程度以上とし、さらに機能追加などの変更が行われた時に実施することが望ましい。

- **基本対策事項 7.2.1(1)-8「サイバーセキュリティリスクが高い機器等」について**

例えば、NAS（Network Attached Storage）において、認証情報を不正に入手される可能性がある脆弱性が公表された際には情報漏えい等のリスクが高まることが考えられる。

- **基本対策事項 7.2.1(1)-9 b)「自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェア」について**

IT 資産管理ソフトウェアには OS やその他アプリケーションのセキュリティパッチを管理する機能を持つものがあり、サーバ装置及び端末に導入されたソフトウェアの種類やバージョンの管理と併せて統合的に管理を行うことができる。

- **基本対策事項 7.2.1(1)-9 c)「一時的な回避方法」について**

ソフトウェアにおいて脆弱性が顕在化した際に、ソフトウェアベンダが対応するまでの間は、当該ソフトウェアの利用を禁止する、当該ソフトウェアベンダが公開した緩和策を実施する、脆弱性が関係する機能を無効化する、ファイアウォール、WAF 等により当該ソフトウェアへの通信を制限するなどの対応が必要となる。

しかし、これらの対応によって業務に著しく悪影響を与えることが想定される場合

は、事前に必要な措置を講じておくことが求められる。例えば、ブラウザは業務上利用せざるを得ないケースが多いが、異なるソフトウェアベンダが提供する複数のブラウザを、端末に事前に導入することで、業務継続性を維持しつつ、脆弱性を悪用した攻撃を受けるリスクを低減することができる。複数のブラウザを導入することは、情報システムのコスト増加を招く可能性があるが、一方のブラウザを常時利用するとともに、他方を緊急時のインターネットへのアクセス手段として利用するなど、用途を分ける方法も考えられる。また、ログ出力の設定を確認し、対応が完了するまでの期間、出力されたログの監視を強化するなどの対応も考えられる。

- **基本対策事項 7.2.1(1)-9 f)「対策試験」について**

  「対策試験」とは、脆弱性対策の実施による情報システムへの影響の有無を確認するために、事前に試験用の情報システムを用いて試験することが想定される。

- **基本対策事項 7.2.1(1)-12「対策用ファイル」について**

  入手した対策用ファイルに悪意のあるコードが含まれている可能性を考慮し、対策用ファイルは信頼できる方法で入手する必要がある。

  信頼できる方法としては、OS やソフトウェアの開発元が提供するパッケージ管理システムや自動アップデート機能のほか、ソフトウェアの開発元等が公開するウェブサイトからダウンロードする方法が挙げられる。また、入手した対策用ファイルが改ざんされていないこと等の完全性の検証を開発元等が公開したハッシュ値と入手した対策ファイルのハッシュ値を比較する等により行う必要がある（検証が自動的に行われるものを含む。）。

7.2.2 不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(1) 不正プログラム対策の実施

(a) 情報システムセキュリティ責任者は、サーバ装置及び端末に**不正プログラム対策ソフトウェア等を導入する**こと。

(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

(c) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

【 基本対策事項 】

＜7.2.2(1)(a)関連＞

7.2.2(1)-1 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の導入に当たり、**既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する**ソフトウェアを導入すること。

7.2.2(1)-2 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

7.2.2(1)-3 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その**定義ファイルが常に最新の状態となるように構成する**こと。

7.2.2(1)-4 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

7.2.2(1)-5 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象とした検査を実施するように構成すること。

＜7.2.2(1)(b)関連＞

7.2.2(1)-6 情報システムセキュリティ責任者は、想定される全ての**感染経路を特定**し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による**感染拡大の防止**等の必要な対策を行うこと。

7.2.2(1)-7 **【追加セキュリティ対策】**情報システムセキュリティ責任者は、**EDR ソフトウェ**

ア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

＜7.2.2(1)(c)関連＞

7.2.2(1)-8 情報システムセキュリティ責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

a) 不正プログラム対策ソフトウェア等の導入状況

b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

（解説）

- **遵守事項 7.2.2(1)(a)「不正プログラム対策ソフトウェア等を導入する」について**

メインフレームシステムや一部のスマートフォンなど、不正プログラム対策ソフトウェアが有効な役割を果たさないと考えられている OS において、不正プログラム対策ソフトウェアが提供されていないことがあるが、そのような場合は、取り扱う情報の格付や情報システムの特性に応じ、不正プログラム対策ソフトウェアをインストールせずに利用できる不正プログラム対策の技術や運用を検討するとよい。

- **基本対策事項 7.2.2(1)-1「既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する」について**

既知の不正プログラムについては、不正プログラム対策ソフトウェアベンダにより、その不正プログラムに関するシグネチャが対策ソフトの定義ファイルに反映されることにより感染を防止することができる。一方で、標的型攻撃等の攻撃手法においては、不正プログラムのソースコードを部分的に改変する亜種や、ソフトウェアの新たな脆弱性を突く不正プログラムなど、不正プログラム対策ソフトウェア等の検知を回避しようとする攻撃が多く見られる。

このような未知の不正プログラムの検知及び感染防止への対応として、ソフトウェアの脆弱性への適切な対策に加えて、シグネチャにより検知する方式以外の手法を用いる製品やサービスを導入することの重要性も高まっている。例えば、必要に応じ以下の検知方式を複数組み合わせて多重防御を行うことにより、攻撃にスクリプト等を使用するファイルレスマルウェア対策としても効果が期待できるなど、不正プログラムの検知精度を向上させることで、端末及びサーバ装置に対する不正プログラム感染リスクの低減を図ることも可能となる。

  - シグネチャに依存せずに OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式（振る舞い検知方式）
  - シグネチャ方式では未対応の亜種を検知しやすい方式（機械学習検索方式）
  - 仮想環境内で検査対象ファイルを実行し、不正な動作を検知する方式（サンドボックス方式）

なお、不正プログラム対策ソフトウェア等の選定に当たっては、ソフトウェアの稼働

によって端末及びサーバ装置への負荷が増加し、業務に影響を与えるおそれがあること等も勘案した上で判断する必要がある。

- **基本対策事項 7.2.2(1)-3「定義ファイルが常に最新の状態となるように構成する」について**

  インターネットに接続されていないサーバ装置や端末の定義ファイルを最新の状態にするため、一時的にインターネット接続が必要となる場合は、当該サーバ装置及び端末を定義ファイルの更新時にインターネットに接続することのリスクや取り扱う情報の格付等を勘案して、定義ファイルの更新の頻度や方法を検討する必要がある。

- **基本対策事項 7.2.2(1)-6「感染経路を特定」について**

  不正プログラムの感染経路には、電子メール、ウェブ等のネットワーク経由のほか、不正プログラムに感染したモバイル端末の機関等支給回線への直接接続や外部電磁的記録媒体の経由及びソフトウェアサプライチェーン攻撃も考えられる。

  不正プログラム対策ソフトウェア等は、製品ごとに検知方式や不正プログラム定義ファイルの提供時期及び種類が異なる。また、不正プログラム対策ソフトウェア等は現存する全ての不正プログラムを検知及び除去できるとは限らないほか、不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害を低減させるため、感染経路において、異なる定義ファイルを用いる不正プログラム対策製品を組み合わせる、又は定義ファイルパターンマッチングやふるまい検知等の異なる技術を用いる製品を組み合わせることにより、どれか一つの不具合で、その環境の全てが不正プログラムの被害を受けることのないようにすることが望ましい。例えば、電子メールサーバに導入する不正プログラム対策と端末に導入する不正プログラム対策について、それぞれ異なる検知技術を用いる製品を導入すること等が考えられる。

- **基本対策事項 7.2.2(1)-6「感染拡大の防止」について**

  ネットワークを経由した感染拡大の防止策としては、以下の例が挙げられる。

  - OS やアプリケーションに関するセキュリティパッチ及び不正プログラム定義ファイルについて最新化されていない端末をネットワークに接続させない仕組みの導入
  - 通信に不正プログラムが含まれていることやサンドボックス方式で検知した不正プログラムが行う通信を検知したときに、その通信をネットワークから遮断する仕組みの導入
  - リモートメンテナンスツール、リモートデスクトッププロトコル、SMB 共有等の悪用を防止するため、不要なツールの削除やポートの変更等

- **基本対策事項 7.2.2(1)-7「EDR ソフトウェア」について**

  不正プログラム対策ソフトウェア等の EPP のような不正プログラムへの感染防止に特化した製品とは異なり、端末やサーバ装置（エンドポイント）の活動を監視し、不正プログラム等の検知や対処を行うなど、不正プログラム等に感染した後の対処に有効である EDR ソフトウェア等を利用し、複数台にわたって統合的に監視を行うことで、

感染した装置を早期にネットワークから切り離す仕組みを導入することができる。ただし、一般的に EDR ソフトウェアは導入後の運用・保守段階において、専門的な知識を持った人材による膨大なログの分析が必要になることから、マネージドセキュリティサービス（Managed Security Service：MSS）と呼ばれる、ログ分析等を行う SOC 業務を委託できるサービスの利用なども検討するとよい。

7.2.3 サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、機関等の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている。

遵守事項

(1) サービス不能攻撃対策の実施

(a) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

(b) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**については、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

(c) 情報システムセキュリティ責任者は、**要安定情報を取り扱う情報システム**については、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

【 基本対策事項 】

＜7.2.3(1)(a)関連＞

7.2.3(1)-1 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置について、**サービス不能攻撃に対抗するための以下の機能**を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

a) パケットフィルタリング機能
b) 3-way handshake 時のタイムアウトの短縮
c) 各種 Flood 攻撃への防御
d) アプリケーションゲートウェイ機能

7.2.3(1)-2 情報システムセキュリティ責任者は、以下を例とするサービス不能攻撃への対策を実施すること。

【基本セキュリティ対策】以下を例とする対策を実施すること。

a) サービス不能攻撃の影響を排除又は低減するための専用の**対策装置**やサービスの導入
b) サーバ装置、端末及び通信回線装置及び通信回線の**冗長化**

【追加セキュリティ対策】基本セキュリティ対策に加え、以下を例とする対策を検討すること。

c) インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

d) コンテンツデリバリーネットワーク（CDN）サービスの利用

＜7.2.3(1)(b)関連＞

7.2.3(1)-3 情報システムセキュリティ責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。

7.2.3(1)-4 情報システムセキュリティ責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。

＜7.2.3(1)(c)関連＞

7.2.3(1)-5 情報システムセキュリティ責任者は、特定した監視対象について、監視方針及び監視方法を定めること。

7.2.3(1)-6 情報システムセキュリティ責任者は、監視対象の監視記録の保存期間を定め、監視記録を保存すること。

7.2.3(1)-7 情報システムセキュリティ責任者は、監視対象の平常時の負荷の状況を把握し、監視においてこれを著しく逸脱したと判断する目安を定めること。

7.2.3(1)-8 情報システムセキュリティ責任者は、監視において、前項で定めた目安を超える負荷の状況が確認された場合は、サービス不能攻撃の可能性が排除される場合を除き、速やかに遵守事項 2.2.4(1)(a)で定める報告手順に基づき CSIRT に報告すること。

7.2.3(1)-9 **【追加セキュリティ対策】**情報システムセキュリティ責任者は、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合は、必要に応じて、CSIRT 等の関係者に通知すること。

（解説）

- **遵守事項 7.2.3(1)「要安定情報を取り扱う情報システム」について**

  要安定情報を取り扱う情報システムについては、「(解説) 基本対策事項 5.2.1(3)-7「要安定情報を取り扱う情報システム及び非常時優先業務等を支える情報システム」について」を参照のこと。

- **基本対策事項 7.2.3(1)-1「サービス不能攻撃に対抗するための以下の機能」について**

パケットフィルタリング機能は、通信パケットのヘッダ部に含まれる情報（送信元及び送信先の IP アドレス、ポート番号、通信プロトコル等）を条件として、パケットの許可/遮断を行う機能である。これにより、攻撃に利用されている IP アドレスが明らかになっている場合、攻撃を遮断することが可能である。

3-way handshake 時のタイムアウトの短縮は、TCP 通信時に用いられる 3-way handshake の一連の通信（通信の可否確認、通信の可否応答、通信セッションの確立）

の上限時間を短縮することにより、DDoS 攻撃によって大量の通信セッションが同時に確立されサーバ等の CPU やメモリ等のリソースがひっ迫することを防止する方法である。

各種 Flood 攻撃への防御は、3-way handshake の仕組みを悪用した SYN Flood や ACK Flood、DNS 通信において問い合わせパケットに比べて応答パケットのサイズが大きくなることを悪用した DNS Flood 等に対する防御である。具体的な方法として、帯域制限機能により特定の IP アドレスからの一定時間内の通信数の上限を設定する、アラート機能によりサーバ等の CPU やメモリ等のリソースひっ迫を検知し攻撃を遮断する・一時的にリソースを増強する等があげられる。

アプリケーションゲートウェイ機能は、パケットフィルタリング機能で用いるヘッダ部の情報のみならず、通信の本体部（ペイロード部）を条件として、パケットの許可/遮断を行う機能である。

- **基本対策事項 7.2.3(1)-2 a)「対策装置」について**

  WAF、IDS/IPS、UTM（Unified Threat Management）、DDoS 攻撃対策専用アプライアンス製品等が考えられる。

- **基本対策事項 7.2.3(1)-2 b)「冗長化」について**

  冗長化の例としては、サービス不能攻撃が発生した場合に備え、サービスを提供するサーバ装置、端末、通信回線装置又は通信回線について、負荷を分散させる、又はそれぞれ代替のものに切り替えるなどにより、サービスを継続することができるように情報システムを構成することが考えられる。

  なお、代替のものへの切替えについては、サービス不能攻撃の検知及び代替サーバ装置等への切替えが許容される時間内に行えるようにする必要がある。

- **基本対策事項 7.2.3(1)-2 c)「インターネットに接続している通信回線」について**

  情報システムに対してサーバ装置、端末及び通信回線装置に係るサービス不能攻撃の対策を実施しても、機関等外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者に確認した上で、サービス不能攻撃発生時の対処手順や連絡体制を整備する必要がある。

- **基本対策事項 7.2.3(1)-2 c)「サービス不能攻撃に係る通信の遮断等」について**

  DDoS 攻撃はボットからの攻撃によって実施されることが多いため、ボットに感染している端末等が多い国やドメインからの通信を拒否することによっても DDoS 攻撃の影響を緩和することが可能であり、特に国内のみからアクセスを受ける情報システムであれば有効であるため、正規の通信への影響も考慮しつつ実施を検討してもよい。また、同一の IP アドレスからのしきい値を超えた大量のリクエストを遮断する機能がオプションとして提供されている場合は、その利用について検討するとよい。

- **基本対策事項 7.2.3(1)-2 d)「コンテンツデリバリーネットワーク（CDN）サービス」について**

  DDoS 攻撃によるパケットが大量に送り込まれインターネット接続回線の帯域が消

費されると、正当なユーザも Web サイトにアクセスできなくなる状況が発生する。コンテンツデリバリーネットワーク（Contents Delivery Network）は、世界中に配置されたキャッシュサーバを利用して Web サイトのコンテンツを配信するというサービスであり、元来は Web サイトのレスポンス向上を目的としたサービスであるが、DDoS 攻撃で大量にアクセスがあった場合も、接続先がキャッシュサーバに分散されるため、攻撃の影響を軽減する効果が期待できる。また、CDN 機能がオプションとして提供されているクラウドサービスやクラウド型 WAF サービスに本機能が含まれている場合もあることから、それらの利用についても検討するとよい。なお、コンテンツデリバリーネットワーク（CDN）サービスを利用する場合は、元の配信コンテンツを格納しているオリジンサーバへ直接アクセスされることを防ぐため、オリジンサーバの IP アドレスを隠蔽する必要がある。

- **基本対策事項 7.2.3(1)-4「攻撃への対処を効率的に実施できる手段」について**

対処例としては、サービス提供に利用している通信回線がサービス不能攻撃により過負荷状態に陥った場合においても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保することが挙げられる。具体的には、管理者が当該装置を操作するためのサーバ装置、端末及び通信回線を、サービス提供に利用しているものとは別に用意することが挙げられる。

また、サービス不能攻撃に伴い、機関等の自己管理ウェブサイトの閲覧障害が発生した場合においても、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力回避すべきである。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼし得るような重要情報については、広報担当とも協力するなどして、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなどの必要な措置を考慮するとよい。

- **基本対策事項 7.2.3(1)-5「監視方針及び監視方法」について**

インターネットからアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する必要がある。

「監視方針」については、監視対象の特性を踏まえて、監視する時間を定め、監視により認知した異常の程度の段階に応じた対応の優先度や情報共有範囲、対応時間帯（24 時間 365 日対応、平日の日中のみ対応等）　等を定めることが考えられる。

「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握や、システムの構成要素に対する負荷の定量的な把握（CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等）がある。監視方法は多種多様であるため、当該情報システムの構成等の特性に応じて適切な方法を選択する必要がある。

- **基本対策事項 7.2.3(1)-6「監視対象の監視記録の保存期間を定め、監視記録を保存」について**

サーバ装置、端末、通信回線装置及び通信回線を監視している場合、監視対象の状態

は一定ではなく変動することが一般的である。そのため、時間変動、曜日変動、週変動、月変動、季節変動等を監視対象の変動を把握するという目的に照らした上で記録の保存期間を定め、一定期間保存する。

- **基本対策事項 7.2.3(1)-8「サービス不能攻撃の可能性が排除される場合を除き」について**

  サービス不能攻撃の可能性が排除される場合として、情報システムのメンテナンスのために一時的に一部機能等を制限した場合や、一時的にアクセスが集中することが考えられるコンテンツをウェブサイトに掲載した場合などが考えられる。

- **基本対策事項 7.2.3(1)-9「脅威動向等の脅威情報を収集」について**

  脅威動向等の脅威情報の収集については、内閣官房国家サイバー統括室等からの注意喚起等のほか、セキュリティベンダが提供している脅威情報の提供サービスを活用することも考えられる。

7.2.4 標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織の情報システム内に何らかの手法で不正侵入・潜入し、権限の奪取等を通じて侵入範囲を拡大、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されることもあり、完全に検知及び防御することは困難との前提に立った対策が必要である。

標的型攻撃への対策としては、情報システム内部への侵入を低減する対策（入口対策）に加え、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる（内部対策）、及び外部との不正通信を検知して対処する対策（出口対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

なお、近年は、組織に対する直接的な攻撃だけでなく、委託先等の関連組織への間接的な攻撃も確認されており、より幅広い対策の検討が求められる。

遵守事項

(1) 標的型攻撃対策の実施

(a) 情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

(b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。

【 基本対策事項 】

＜7.2.4(1)(a)関連＞

7.2.4(1)-1 情報システムセキュリティ責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 不要なサービス機能やアプリケーションを削除又は停止すること。

b) 不審なプログラムが実行されないよう設定すること。

c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限すること。

d) サービスは原則「標準ユーザ」の権限で実行すること。

7.2.4(1)-2 情報システムセキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行う。

a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させないこと。また、接続する外部電磁的記録媒体を事前に特定すること。

b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査すること。

c) サーバ装置及び端末について、自動再生（オートラン）機能や自動実行機能を無

効化すること。

d) サーバ装置及び端末について、使用を想定しないUSBポートを無効化すること。

e) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入すること。

＜7.2.4(1)(b)関連＞

7.2.4(1)-3 情報システムセキュリティ責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を全て含む対策を行うこと。

a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定すること。また、インターネットに接続する必要がある場合は、必要最小限のプロトコルやポートのみに限定し、インターネットに接続する必要がない場合はインターネット分離を行うこと。

b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずること。

7.2.4(1)-4 情報システムセキュリティ責任者は、端末の管理者権限アカウントについて、以下を全て含む対策を行うこと。

a) 不要な管理者権限アカウントを削除すること。

b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定すること。

7.2.4(1)-5 【追加セキュリティ対策】情報システムセキュリティ責任者は、以下を例とする内部対策及び出口対策を行うこと。

a) プロキシサーバ等により、C&C サーバ等への不正な通信を監視し、遮断すること。

b) 情報システムの管理者が利用する情報システム管理用の専用端末を用意し、他のセグメントと分離した運用管理セグメントを構築し、当該セグメントにシステム管理用の専用端末を接続すること。

c) 認証サーバに管理者権限でログインできる端末をシステム管理用の専用端末に制限すること。

d) 一般利用者が利用する端末間でのファイル共有機能を停止する又は一般利用者が利用する端末間の直接通信を遮断すること。

（解説）

- **遵守事項 7.2.4(1)(a)「標的型攻撃」について**

第６部から第８部の各款における規定内容は、標的型攻撃への対策としても有効であるため、各款にそれぞれに示される対策を標的型攻撃への対策の観点からも行う必要がある。

- **遵守事項 7.2.4(1)(a)「入口対策」について**

  標的型攻撃の手法として代表的なものは「標的型メール」であり、攻撃者は攻撃対象の組織や個人の情報を入念に調査し情報を収集した上で、攻撃対象が疑念を抱かないよう巧妙に偽装したメールにより攻撃を仕掛けてくる。情報システムセキュリティ責任者には、不審な電子メールへの対策として基本対策事項 8.1.1(2)-2 に例示された対策の導入が求められるが、これら攻撃メールを完全に検知及び防御することは困難であることから、システム的な抑止機能の導入だけでなく、不審な電子メールの添付ファイルを実行しない、記載された URL リンクをクリックしないといった基本的な情報セキュリティ対策を職員等に意識づけるための教育や定期的な注意喚起を組織全体として実施することが重要である。

  ただし、上記のような入口対策を講じても組織内部への侵入の可能性はなお残ることから、内部対策の実施及び職員等が被害を受けた可能性を認知した際の機関等内での連絡体制を日頃から周知することも重要である。

- **基本対策事項 7.2.4(1)-1 b)「不審なプログラムが実行されないよう設定する」について**

  具体的な設定手段としては、あらかじめ利用するアプリケーションを登録してそれ以外のアプリケーションの実行を拒否するよう設定する、通常のアプリケーションでは利用しないメモリ空間を利用しようとしたアプリケーションを不審と判定して実行を拒否するソフトウェアを利用する、情報システムにおいて不正プログラムの起動又は動作を拒否する手法を導入するなどが挙げられる。

  なお、これらを導入する場合には、業務で利用するアプリケーションに影響が及ぶ可能性があるため、事前に検証する必要がある。

- **基本対策事項 7.2.4(1)-2 c)「自動再生（オートラン）機能や自動実行機能を無効化」について**

  標的型攻撃に用いられる手段として、自動再生（オートラン）機能を悪用するものがあり、例えば、不正プログラムを格納した USB メモリを端末に接続させることにより、不正プログラムを実行させるという手法が想定される。

  自動再生（オートラン）機能を無効にすることで、この機能を悪用する手段による被害に遭うリスクを低減することができる。

- **基本対策事項 7.2.4(1)-2 d)「USB ポートを無効化」について**

  物理的に又はシステム的に USB ポートを利用できない状態にすることで、USB メモリ等の外部電磁的記録媒体を接続することによって生じる情報セキュリティインシデントの発生を抑止できる。

- **基本対策事項 7.2.4(1)-2 e)「組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービス」について**

  外部電磁的記録媒体のポートへの接続や利用を制御及び管理するため、以下のような機能を持つ製品やサービスが市場に提供されている。

  - 端末の USB ポートのインタフェースを無効化し、外部電磁的記録媒体を含む全ての機器を利用不可とする。

- USB ポートに接続された機器のうち、全ての外部電磁的記録媒体を利用不可とする。
- 利用を認める外部電磁的記録媒体を一元管理するサーバに事前に登録しておき、登録されていない外部電磁的記録媒体の利用不可とする。
- 利用を認める外部電磁的記録媒体の個体識別情報（製品番号等）と利用者の組合せを一元管理するサーバに事前に登録しておき、組合せ以外での利用を不可とする。
- 外部電磁的記録媒体の接続の際における、利用者、出力日時、出力ファイル名等のログを自動的に取得する。

- **基本対策事項 7.2.4(1)-3「情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバ」について**

悪意ある第三者等は、入口対策を突破して内部への侵入に成功すると、外部から遠隔指令を出して内部侵入の範囲を拡大しつつ、目的の達成を目指すと想定される。その目的としては、重要情報の窃取や破壊が想定され、したがって、識別コード及びアクセス権限を集中管理する認証サーバ、又は、情報が集中的に保存されるファイルサーバは、攻撃対象となる蓋然性が高いと考えられる。これら重要サーバには、特に注意して情報セキュリティ対策を講ずる必要がある。

- **基本対策事項 7.2.4(1)-3 b)「管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策」について**

管理者権限を狙う攻撃としては、機械的にパスワードを変えながら連続してログイン試行する攻撃が考えられる。このような攻撃を受けることを想定した対策としては、以下に挙げるものが考えられる。

- 連続でのログイン失敗回数に上限値を設け、この上限値を超えた場合は、次回ログイン試行までに一定の期間（例：15 分）ログイン試行を受け付けないようにシステム等で設定する。
- ログイン失敗ログを取得し、その取得内容を継続的に監視することにより、大量のログイン失敗を検知する仕組みを導入する。

- **基本対策事項 7.2.4(1)-4 b)「容易に推測できないもの」について**

「（解説）基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照のこと。

- **基本対策事項 7.2.4(1)-5「内部対策」について**

内部対策は、内部に侵入してしまった攻撃を想定し、これを早期検知して対処するための対策や侵入範囲の拡大（ラテラルムーブメント：横方向の侵害）の困難度を上げるための対策などが考えられる。具体的には、基本対策事項 7.2.4(1)-3 及び 4 並びに 7.2.4(1)-5 b)から d)の対策のほか、多要素主体認証方式の導入や基本対策事項 7.1.3(1)-1 の管理者権限に係る対策、基本対策事項 7.2.2(1)-7 の EDR ソフトウェア等を利用した端末やサーバ装置（エンドポイント）の監視、基本対策事項 6.4.1(2) -3 の機関等内通信回線の機器等における不審な通信の監視などが考えられる。また、高い管理者権限ア

カウントに似せたトラップアカウントを端末等に設定しておき、当該トラップアカウントを用いた攻撃者のログイン行為等を検知する対策も有効であるが、認証失敗のログを収集し、これを監視できる体制とする必要がある。さらに、侵入範囲の拡大の手法の一つとして、ActiveDirectory のようなディレクトリサービスが攻撃対象とされる事例も多く、当該サービスを提供するサーバ装置に対する脆弱性対策や上記の対策が特に重要であるほか、当該サービスの管理専用端末を用意するといった対策も検討するとよい。

- **基本対策事項 7.2.4(1)-5「出口対策」について**

  出口対策として、基本対策事項 7.2.4(1)-5 a)の対策のほか、基本対策事項 6.4.1(2)-3 の機関等外への不正な通信の監視などが考えられる。

- **基本対策事項 7.2.4(1)-5 a)「不正な通信を監視し、遮断」について**

  本対策を有効とするため、プロキシサーバの導入に当たっては、ウェブブラウザのプロキシ設定を有効にし、ファイアウォールにおいて、内部（ユーザセグメント）から外部（インターネット）への通信の遮断ルール（ファイアウォールポリシー）を適切に設計・設定することにより、端末から直接インターネットへの通信（プロキシサーバを経由しない通信）ができないようにする必要がある。また、プロキシサーバにおけるアクセス制御リストを適切に設計・設定する必要がある。

  プロキシサーバの認証機能を有効にした場合は、当該認証失敗ログ等を分析することにより、不正な通信を調査・発見できることがある。

  なお、不正な通信の監視、遮断について、NDR 製品を活用することも考えられる。

- **基本対策事項 7.2.4(1)-5 d)「端末間でのファイル共有機能を停止」について**

  OS が Windows である端末間でファイルやフォルダを共有するための機能である「ファイル共有機能」について、内部に侵入した悪意ある第三者等によって侵入範囲を拡大するために悪用されることを防ぐため、本機能を停止することが望ましい。なお、「管理共有機能」（C$、D$、ADMIN$等）も停止することが望ましい。

7.3　ゼロトラストアーキテクチャ

7.3.1　動的なアクセス制御の実装時の対策

目的・趣旨

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の機関等外通信回線と組織内ネットワークである機関等内通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な政府情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。

ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装する場合に特に必要な対策について記載する。

動的なアクセス制御の機能を実装する場合は、本款以外に 7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理に係る遵守事項についても併せて遵守する必要があるが、既存の情報システムの構成に動的なアクセス制御を実装する場合は、既存の情報システムの構成やアクセス制御に用いるソフトウェアなどを見直していくことが重要となる。

遵守事項

(1) 動的なアクセス制御における責任者の設置

(a) 統括情報セキュリティ責任者は、複数の情報システム間で**動的なアクセス制御**を実装する場合は、**複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者**として、情報システムセキュリティ責任者を選任すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.1(1)(a)「動的なアクセス制御」について**

  本節における動的なアクセス制御とは、特定のアクセスに対して、セッションが確立していない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。

- **遵守事項 7.3.1(1)(a)「複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者」について**

  機関等において動的なアクセス制御を実装する場合は、複数の情報システム間で動的なアクセス制御を実装する場合がある。その場合、複数の情報システムに対して横断的な対策を実施しなければならず、複数の情報システムセキュリティ責任者が連携して対応する必要がある。したがって、複数の情報システムセキュリティ責任者の中から複数の情報システム間の横断的な対策の企画・推進・運用に関する事務を統括する責任者として、情報システムセキュリティ責任者を選任することが有効である。

遵守事項

(2) 動的なアクセス制御の導入方針の検討

(a) 情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。

【 基本対策事項 】

＜7.3.1(2)(a)関連＞

7.3.1(2)-1 情報システムセキュリティ責任者は、**動的なアクセス制御の対象とする情報システムの範囲や優先度を検討**し、動的なアクセス制御の対象とする情報システムを特定すること。

7.3.1(2)-2 情報システムセキュリティ責任者は、特定した情報システムの利用形態等を基に以下を例とする区分で**情報システムのリソースを識別する**こと。

a) ユーザアカウント
b) 機器
c) アプリケーション
d) データ

7.3.1(2)-3 情報システムセキュリティ責任者は、**識別したリソースを基にアクセスパターンを整理**すること。

7.3.1(2)-4 情報システムセキュリティ責任者は、整理した**アクセスパターンに対するリスク評価**を実施し、動的なアクセス制御を実装するアクセスパターンを特定すること。

（解説）

- **基本対策事項 7.3.1(2)-1「動的なアクセス制御の対象とする情報システムの範囲や優先度を検討」について**

動的なアクセス制御の実装においては、組織内ネットワーク上に存在する全ての情報システムを対象とすることが望ましいが、全ての情報システムを対象とする場合、リソースの識別やアクセスパターンの特定、リスク評価の実施など多くの時間を要することが想定される。このため、動的なアクセス制御の対象とする情報システムの範囲や優先度を検討し、動的なアクセス制御の対象とする情報システムを特定することが重要である。

なお、動的なアクセス制御の対象とする情報システムについては、5.1 節で定める高度な情報セキュリティ対策が求められる情報システムを判別するための分類に基づき検討することも考えられる。また、機関等 LAN システムのような機関等内で共通的に利用される情報システムを優先的な動的なアクセス制御の対象とすることで、機関等全体の情報セキュリティ水準の向上を図ることが可能となる。

- **基本対策事項 7.3.1(2)-2「情報システムのリソースを識別する」について**

情報システムのリソースとは、情報システムを構成（当該情報システムを利用する機

器等を含む。）する機器、アプリケーション、利用アカウント、データ等の情報資産を指す。情報システムにおけるリソースの識別については、情報システムの調達仕様書や設計書等における情報システムの構成図や利用形態等を参照しつつ、情報システムへアクセスする際に利用するリソースについて整理する必要がある。

また、情報システムの利用形態によっては、複数の情報システム間で連携するアプリケーションなどが存在する場合もある。そのような形態が存在する場合、それぞれの情報システムで連携するアプリケーションや、アプリケーションが利用する認証用アカウント、アクセストークン、証明書、証明書発行に用いる認証情報、アクセス対象のデータ等のリソースを識別する必要がある場合があることに留意が必要である。

表 7.3.1-1 は、リソースを識別するに当たり、ユーザアカウント、機器、アプリケーション、データを区分した例示である。このような区分を参考に、情報システムに対してどのようなものが存在するか整理する必要がある。

表 7.3.1-1　リソースを識別する区分例

リソース	属性		リソース例
	属性例	属性値の例	
ユーザアカウント	所属	部局名、課室名、委託先名	機関等 LAN システム内ディレクトリサービスのユーザアカウント、クラウド型メールサービスのログインアカウント、（特定の）システムユーザアカウント
	役職	部局長、課室長、係長、主査、係員	
	権限種別	利用者、管理者、運用者	
機器	機関等支給の有無	機関等支給、機関等支給以外	PC、タブレット端末、スマートフォン、サーバ装置、複合機、特定用途機器、通信回線装置
	用途	事務用、運用・保守用、開発用	
	場所の使用制限等	要管理対策区域（庁舎や契約するデータセンター等）、要管理対策区域外（持ち出し先、自宅等）	
	ネットワーク所属情報	機関等 LAN システム内端末、インターネット接続端末	

リソース	属性		リソース例
	属性例	属性値の例	
	クライアントアプリケーション	Web ブラウザ、アプリケーション名	
アプリケーション	種別	機関等 LAN システム内情報システム上のアプリケーション、クラウドサービス	機関等 LAN システム内ディレクトリサービス、クラウド型メールサービス
	実行基盤	サーバ名、クラウドサービス（PaaS、IaaS）名	
	実行環境	本番環境、開発環境	
データ	格付	機密性〇、完全性〇、可用性〇	特定プロジェクトの要機密情報、機関等 WEB ページ公開用コンテンツ
	取扱制限	〇〇限り、〇〇禁止、〇〇要許可	
	操作の制限	管理者：フルコントロール可能 一般職員：参照のみ	

- **基本対策事項 7.3.1⑵-3「識別したリソースを基にアクセスパターンを整理」について**

動的なアクセス制御の実装に向けて、対象とする情報システムにおいて考えられるリソース及び当該リソースへのアクセスパターンを漏れなくリスト化する必要がある。ここで整理したアクセスパターンのリストは、動的なアクセス制御の制御対象の単位となり、組織内ネットワーク上の情報システムのリソースを保護するための基礎情報となるものである。なお、リソースやアクセスパターンは運用していく中で当初に想定していたものから変化していくため、変化に応じて見直しをする必要があることに注意が必要である。

アクセスパターンの整理に当たっては、情報システムの利用形態に基づき識別される各リソースに対して、どのようなアクセスが考えられるかといった点を考慮し検討する必要がある。その際、ある文脈でアクセス先であったリソースが、別の文脈ではアクセス元として、さらに別のリソースへアクセスを行う場合もあることに留意が必要である。例えば、あるユーザが、ある機器にログインし、当該機器を用いてアプリケーション A にアクセスを行い、アプリケーション A は、さらに別のアプリケーション B にアクセスを行う、という点を考慮する必要がある。

検討の中で、識別したリソースに不足があった場合は、新たなリソースとして識別する必要もある。識別した全てのリソースについて、このようなアクセスパターンを列挙することで、対象となる情報システム全体のアクセスパターンを整理することができる。

アクセスパターンを整理する具体例として、例えば機関等 LAN システムのような機関等内で共通的に利用される情報システムにおいて、当該情報システムへアクセスする方法として、職員等が自組織のドメインユーザアカウントで端末にログインし、当該端末を用いて庁舎内の要管理対策区域内から機関等内通信回線を用いてファイルストレージシステムに保存された要機密情報にアクセスする場合や、職員等が端末を用いて、公衆回線経由で、クラウド型メールサービスに、クラウド用認証アカウントを用いてログインしアクセスする場合、等が想定される。このように、情報システムの利用形態からリソースに着目し、アクセスパターンを整理する。

アクセスパターンの整理についての例示として、表 7.3.1-2 に「職員が端末を用いてインターネット経由でクラウド型電子メールサービスへのアクセスする」パターンと「職員が VPN 経由で機関等 LAN システム上のファイルストレージシステム上のデータにアクセスする」パターンを示す。アクセスパターンを整理する場合は、それ以外にも考えられる各リソースの組み合わせを用いて整理することが求められる。

表 7.3.1-2　アクセスパターンの特定例

アクセスパターン		リソースアクセス		アクセス元	アクセス先
		項番	項目		
A	職員が端末を用いてインターネット経由でクラウド型電子メールサービスへのアクセスする。	1	OS ログインアカウントの認証	職員	クラウドディレクトリサービス上のユーザオブジェクト
		2	クラウド型メールサービスの認証	職員	クラウド型メールサービスの ID プロバイダ
		3	端末からクラウド型メールサービスへのアクセス	端末	クラウド型メールサービス
B	職員が VPN 経由で機関等 LAN システム上のファイルストレージシステム上のデータにアクセスする。	1	OS ログインアカウントの認証	職員	ディレクトリサービス上のユーザオブジェクト（キャッシュされたログオン情報）
		2	端末から VPN 装置へのアクセス	端末	VPN 装置

アクセスパターン		リソースアクセス		アクセス元	アクセス先
		項番	項目		
		3	端末からファイルストレージシステムへのアクセス	端末	ファイルストレージシステム

- **基本対策事項 7.3.1(2)-4「アクセスパターンに対するリスク評価」について**

アクセスパターンに対するリスク評価については、整理した全てのアクセスパターンに対して想定される脅威に基づき、脅威事象が発生する可能性及び脅威事象が負の影響をもたらす可能性を推定することによって行う。想定される脅威は、係わるリソースの持つ属性や状態に依存して発生するものもあることに留意が必要である。

例えば、職員等が端末の WEB ブラウザを用いてインターネット経由で機関等が契約するクラウドサービス上の要機密情報を参照するようなアクセスパターンを想定した場合、攻撃者が当該職員の認証情報を不正利用し当該サービスにアクセスするリスクが高いと評価することが考えられる。この場合、インターネット経由でのアクセスか、機関等 LAN システム経由でのアクセスか、といった情報は、職員が使用する機器をリソースとして捉えた場合に、当該機器リソースの「所属ネットワーク情報」という属性の値の違いから判別される。

動的なアクセス制御を実装するアクセスパターンの優先度や範囲については、リスク評価の結果を踏まえ、当該リスクを低減するための費用対効果の観点などから決定することが考えられる。

なお、具体的なリスク評価の手法や考え方については「(解説) 遵守事項 2.1.3(1)(a)「リスクを評価する」について」を参照のこと。

遵守事項

(3) 動的なアクセス制御の実装時の対策

(a) 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成すること。

(b) 情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

【 基本対策事項 】

＜7.3.1(3)(a)関連＞

7.3.1(3)-1 情報システムセキュリティ責任者は、動的なアクセス制御を実現するための構成について検討すること。

7.3.1(3)-2 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、動的なアクセス制御に活用する以下を例とするリソースの信用情報を整理すること。

a) ユーザアカウント
b) 機器
c) アプリケーション
d) データ

7.3.1(3)-3 情報システムセキュリティ責任者は、リソースの信用情報の変化に応じてアクセス制御ポリシーを作成すること。

＜7.3.1(3)(b)関連＞

7.3.1(3)-4 情報システムセキュリティ責任者は、リソースの信用情報を収集する頻度・機会について定めること。

7.3.1(3)-5 情報システムセキュリティ責任者は、リソースの認証・認可において、アクセス制御ポリシーに基づき、セッションが確立してない操作ごとにアクセス制御を行うこと。

（解説）

- **遵守事項 7.3.1(3)(a)「リソースの信用情報」について**

リソースの信用情報とは、リソースから収集する情報のことで、リソースの性質や特性に係わる属性情報(例:ユーザアカウントの権限種別､機器の所属ネットワーク情報)や状態情報（例：ユーザアカウントの識別コードや主体認証情報の漏えい状況、機器のセキュリティパッチ適用状況等）のことを指し、当該リソースをアクセス元、アクセス先とするアクセス制御において、アクセス可否の判断等に使用するものである。

- **基本対策事項 7.3.1(3)-1「動的なアクセス制御を実現するための構成」について**

動的なアクセス制御を実現するためには、新しい情報システムの導入や既存の情報システムの改修も踏まえ、対象とする情報システム上のリソースの信用情報を収集可能とし、当該信用情報を活用することでリソースへのアクセス制御を行うことを可能

とするようなシステム構成を検討する必要がある。具体的な構成を検討するに当たっては、リソースから情報を収集するための製品やソリューション、それらを用いてアクセス制御を行うための製品やソリューションを検討し、それぞれの製品やソリューションが連携可能であるか確認することが重要である。

表 7.3.1-3 は、リソースへの情報セキュリティ対策機能や当該対策が有効に機能し、リソースが信頼できるものであるかを検討する機能を有するソリューションの一部を示すが、他の製品やソリューション等も有効であるため検討するとよい。また、これらの製品やソリューションの活用については、想定されるリスクや費用対効果等を踏まえ検討することが望ましい。

表 7.3.1-3　有効な機能や当該機能を有するソリューションの例

リソース	有効な機能の例	ソリューションの例
ユーザアカウント	識別コード・主体認証情報の保護機能	IDaaS （Identity as a Service）、IGA （Identity Governance & Administration）
機器	機器（エンドポイント）の脅威からの保護機能	EPP 、EDR、MDM、MAM（Mobile Application Management） ZTNA（Zero Trust Network Access）、SWG（Secure Web Gateway）、CASB

- **基本対策事項 7.3.1(3)-2「リソースの信用情報を整理」について**

ユーザアカウント、機器、アプリケーション、データに係るリソースの信用情報としては、表 7.3.1-4 に掲げるようなものが挙げられる。動的なアクセス制御に活用する信用情報については、リスク評価の結果、リスクが高いと評価したアクセスパターンにおいて、そのリスクを低減させるためにどのリソースのどのような信用情報を活用すればアクセスの安全性が高められるかを整理することで求められる。

例えば、リスク評価の結果、不正な主体認証のリスクが高いと考えられるアクセスパターンにおいて、アクセス元の機器がリスクの懸念されるリソースとなる場合、当該機器が信用できるものであるかを判断するためには、表 7.3.1-4 で掲げるような端末における標準設定がなされていることや、不正プログラムの検知状況等の情報が必要であるとし、これらを動的なアクセス制御に活用する信用情報として整理することが考えられる。

表 7.3.1-4　リソースの信用情報の例

リソース	信用情報の例
ユーザアカウント	属性（所属する部局や役職等）
	主体認証情報の漏えい有無（脅威インテリジェンスとの突合結果）
	多要素主体認証の実施有無
	アクセスの時間帯

リソース	信用情報の例
	主体認証の失敗回数
機器	利用しているアプリケーションや OS の種類及びバージョン
	セキュリティパッチの適用状況
	端末における標準設定がされているか（クライアント証明書導入有無、ディレクトリ管理機能で管理される機関等ドメインへの参加有無、不正プログラム対策ソフトウェアの導入有無等）
	不正プログラムの検知状況
	機器が接続しているネットワーク種別（機関等 LAN システム、インターネット等）
	IP アドレス
	地理情報
アプリケーション	アプリケーションのセキュリティ状態
	アプリケーション実行環境（サーバ基盤等）のセキュリティ状態
	アプリケーションの第三者機関による安全性評価（CASB における安全性評価等）
	機関等におけるアプリケーションの利用許可状況
データ	情報の格付及び取扱制限
	情報の形式（実行プログラム形式、文書形式、圧縮形式等）
	情報の量

また、このようなリソースの信用情報を蓄積する情報基盤として、ID とアクセスの管理（Identity and Access Management：IAM）と呼ばれる仕組みや、資産管理を行う仕組みを導入することについて検討するとよい。

- **基本対策事項 7.3.1(3)-3「リソースの信用情報の変化」について**

動的なアクセス制御の実装に当たっては、リソースの信用情報は時間の経過に伴い刻々と変化する。そのため、リソースの信用情報を用いたアクセスの検証は、初回のアクセス要求時だけでなく、セッションが確立してない操作ごとに都度検証することが必要となる。

このようなリソースの信用情報の変化については、例えば、端末で利用している OS やアプリケーションの脆弱性が見つかった場合や機関等内通信回線からのアクセスではなく機関等外通信回線を利用してアクセスするなど、時間の経過に伴いリソースの属性や状態が変化し、リスクが発生する可能性が変化した状態のことをいう。

なお、このようなリソースの信用情報の変化に伴うリスクを相関的に検出する機能を有するソリューションとして、SIEM や UEBA 等があり、これらのソリューションに連携可能な情報を組み合わせることで、リソースの信用状況の変化を動的なアクセス制御に活用する可能性についても必要に応じて検討するとよい。

表 7.3.1-5　リソースの信用情報の変化例

リソース区分	変化前	変化後
ユーザアカウント	主体認証情報の漏えいや、管理されていない識別コードなし	主体認証情報が漏えい、異動に伴う不要な識別コードあり
機器	最新バージョンの OS やアプリケーション利用	脆弱なバージョンの OS やアプリケーション利用
アプリケーション	安全性が確認されたアプリケーション	問題点が発見されたアプリケーション

- **基本対策事項 7.3.1(3)-3「アクセス制御ポリシーを作成する」について**

アクセス制御ポリシーとは、動的なアクセス制御を行うに当たり、アクセス先のリソースに対してアクセス元のリソースに許容されるアクセスや処理を、アクセス元の権限等の情報に基づいて規定するルールである。アクセス制御ポリシーの作成に当たっては、リソースの信用情報や、基本対策事項 7.3.1(2)-3、基本対策事項 7.3.1(2)-4 で検討したアクセスパターンとそのリスク評価結果、機関等が定めた情報セキュリティ関係規程、アクセス制御ポリシーに基づき連携する製品やサービス等を踏まえて作成することが望ましい。

アクセス制御ポリシーに基づくアクセス制御のイメージとしては、アクセス元、アクセス先のリソースの信用情報がベースラインとして定義した表 7.3.1-6 が考えられる。この表に掲げるような要件に全て準拠していれば、他の認証要素による確認を追加で要求せずリソースへのアクセスを許可するようなことが考えられる。さらに、アクセスする際の検証の結果が表 7.3.1-7 のようにベースラインに一部準拠していないものの、非準拠部分がアクセスとして認めている内容であれば他の認証要素による確認を追加で要求することや、表 7.3.1-8 のように非準拠部分がアクセスとして認めていない内容であればアクセスを拒否することが考えられる。また、アクセス制御ポリシーが流出した場合、悪意のある第三者等によって重要な情報へのアクセス権を持つアカウントを推測される可能性がある。そのため、第三者等への流出を防止する等、適切に管理する必要がある。

表 7.3.1-6　ベースラインに全て準拠し多要素主体認証を不要とする例

リソース		リソースの信用情報
アクセス元	ユーザアカウント	主体認証情報が漏えいしていない
		主体認証の失敗回数が既定回数以内
	機器	既知の脆弱性のない OS バージョン
		端末の標準設定がされている
		機関等 LAN システムからのアクセス
アクセス先	アプリケーション	機関等において利用を許可したアプリケーション
	データ	格付や取扱制限に準拠したアクセス

表 7.3.1-7　インターネット経由のアクセスは認めているがベースラインを満たさないため多要素主体認証を追加で要求する例

リソース		リソースの信用情報
アクセス元	ユーザアカウント	主体認証情報が漏えいしていない
		主体認証の失敗回数が既定回数以内
	機器	既知の脆弱性のない OS バージョン
		端末の標準設定がされている
		インターネットからのアクセス
アクセス先	アプリケーション	機関等において利用を許可したアプリケーション
	データ	格付や取扱制限に準拠したアクセス

表 7.3.1-8　インターネット経由かつ端末の標準設定がされていない端末からのアクセスは認めておらずアクセスを拒否する例

リソース		ベースラインとする診断内容
アクセス元	ユーザアカウント	主体認証情報が漏えいしていない
		主体認証の失敗回数が既定回数以内
	機器	既知の脆弱性のない OS バージョン
		端末の標準設定がされていない
		インターネットからのアクセス
アクセス先	アプリケーション	機関等において利用を許可したアプリケーション
	データ	格付や取扱制限に準拠したアクセス

- **基本対策事項 7.3.1(3)-4「信用情報を収集する頻度・機会」について**

動的なアクセス制御において活用するリソースの信用情報については、セッションが確立してない操作ごとに都度検証する際に利用される。したがって、リソースの信用情報を収集する頻度や機会を適切に定めることで、情報セキュリティ対策が有効に機能し、リソースが保護され信用できるものであるかを確認できるようにする必要がある。

リソースの信用情報を収集する頻度・機会については、可能な限りセッションが確立してない操作ごとに都度検証することが望ましいが、システムの負荷や、想定されるリスクの受容可能期間、是正措置実施後の最新の信用情報を収集する待ち時間等に鑑みて、業務効率に影響を与えないようにすることも検討する必要がある。

ただし、リソースの信用情報の収集頻度が著しく低い場合は、適切なリスクの判断ができなくなる可能性がある。例えば、機器に対する脆弱性対策として、セキュリティパッチが未適用と判明した機器からのアクセスを遮断するような動的なアクセス制御を行う場合、セキュリティパッチ適用状況を収集する頻度が低いと、セキュリティパッチが未適用と判明した機器からのアクセスを遮断するまでの間に、振る舞い検知や UEBA や SIEM などによるリソースへのアクセス状況の特異性の評価など、他の施策による対応依存度が高まることについて、留意が必要である。

7.3.2 動的なアクセス制御の運用時の対策

目的・趣旨

テレワークの拡大やクラウド・バイ・デフォルト原則によって、リソースの利用形態は日々変化していることを踏まえ、動的なアクセス制御の運用時には、実装時に検討した対策内容が正しく機能しているかどうか確認し、必要に応じてアクセス制御ポリシーを見直すことが重要である。また、動的なアクセス制御の前提となるリソースの信用情報を収集する中でリスクが検出された場合は、当該リスクを低減するための措置が必要となる。

本款では、機関等が動的なアクセス制御を運用する場合に特に必要な対策についてのみ規定するため、本款以外に 7.1.1「主体認証機能」で定める識別コード・主体認証情報の管理、7.1.2「アクセス制御機能」で定めるアクセス制御の適切な運用、7.1.3「権限の管理」で定める権限の管理に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 動的なアクセス制御の実装方針の見直し

(a) 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しをすること。

【 基本対策事項 】

＜7.3.2(1)(a)関連＞

7.3.2(1)-1 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、アクセスパターンやアクセス先のリソースの変化があった場合は、変化が影響する箇所に対し再度リスク評価を行い、アクセス制御ポリシーの見直しをすること。

7.3.2(1)-2 情報システムセキュリティ責任者は、基本対策事項 7.3.2(1)-1 による見直しによりアクセス制御ポリシーを変更した場合、変更の履歴を記録し、点検を実施すること。

（解説）

- **基本対策事項 7.3.2(1)-1「変化が影響する箇所に対し再度リスク評価を行いアクセス制御ポリシーの見直しをする」について**

  アクセスパターンの変化として、例えばテレワークの拡大等を背景として、これまで機関等 LAN システムからアクセスしていたオンプレミスの情報システムを、クラウドサービス上へ移行する等の変化が想定される。

  アクセスパターンの変化の他にリソースの重要度及びリソースの追加、廃止、取り扱いレベル等の変化によって、これまで想定されなかった新たなリスクが想定される場合は、リスク評価の結果やアクセス制御ポリシーについて見直しが必要となる。

遵守事項

(2) リソースの信用情報に基づく動的なアクセス制御の運用時の対策

(a) 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.2(2)(a)「リソースの信用情報の収集により検出されたリスクへ対処」について**

動的なアクセス制御の運用においては、リソースの信用情報の収集により、新たなリスクを検出する機会が増加することが想定される。これら検出したリスクに対し、動的なアクセス制御で許容する範囲に是正する目的で、日常的な対処を行うことが必要となる。

このような収集によって検出したリスクに対する対処は、管理者・利用者それぞれにおいて行われる必要がある。管理者として行う対処の具体例は、ユーザアカウントの主体認証情報の利用状況の特異点を確認する中で検出された、主体認証情報の漏えいが疑わしいユーザアカウントについて、セキュリティ担当者にエスカレーションし、追加の調査の実施を依頼するような対処が挙げられる。利用者として行う対処の具体例は、動的なアクセス制御によって抵触したセキュリティパッチ未適用や不適切なネットワークへの接続などの事柄に対する是正措置として、セキュリティパッチの適用作業や適切なネットワークへの再接続を実施するような対処が挙げられる。

また、こうしたリスクへの対処に際して、一時的に当該リソースを利用する職員等による情報システムへのアクセスが不可となる影響が想定されるため、事前に職員等への連絡手段や、職員等からの問い合わせ窓口を用意するとともに、利用者に対して動的なアクセス制御で抵触した事柄の是正措置を動的なアクセス制御を提供するシステムによって明示できるようにすることが望ましい。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

目的・趣旨

職員等は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する規定を整備し、職員等は規定に従って利用することが求められる。

なお、機関等が支給する端末（要管理対策区域外で使用する場合に限る）に係る規定の整備については遵守事項 6.1.2(1)、機関等支給以外の端末に係る規定の整備については遵守事項 6.1.3(2)をそれぞれ参照すること。

遵守事項

(1) 情報システムの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する実施手順を整備すること。

(b) 統括情報セキュリティ責任者は、**USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順**を定めること。

(c) 統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めること。

【 基本対策事項 】

＜8.1.1(1)(a)関連＞

8.1.1(1)-1 統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する**以下を例とする実施手順を定める**こと。

a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順

b) 端末（支給外端末を含む。）の利用のうち、情報セキュリティに関する手順

c) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順

d) 識別コードと主体認証情報の取扱手順

e) 暗号と電子署名の利用に関する手順

f) 不正プログラム感染防止の手順

g) アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為の防止に関する手順

h) ドメイン名の使用に関する手順
i) Web 会議サービス利用時の手順
j) クラウドサービスを利用した機関等外の者との情報の共有時の手順

＜8.1.1(1)(b)関連＞

8.1.1(1)-2 統括情報セキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順として以下の事項を全て含めて定めること。

a) 職員等は、国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体、又は遵守事項 8.1.1(b)に規定する実施手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体を使用すること。
b) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。
c) 要機密情報が記録された外部電磁的記録媒体を要管理対策区域外に持ち出す場合は、外部電磁的記録媒体に格納する情報を暗号化する、又は主体認証機能や暗号化機能等を備えるセキュアな外部電磁的記録媒体を利用すること。
d) 要機密情報は保存される必要がなくなった時点で速やかに削除すること。
e) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行うこと。
f) 外部電磁的記録媒体の利用者が利用内容を貸出簿等に記録すること。

＜8.1.1(1)(c)関連＞

8.1.1(1)-3 統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続として、以下を全て含む手続を規定し、職員等に遵守させること。

a) 利用時の許可申請手続
b) 手続内容（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）
c) 利用期間満了時の手続
d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

（解説）

- **遵守事項 8.1.1(1)(b)「USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順」について**

USB メモリ等の外部電磁的記録媒体に関する対策は、情報システムの構成等によって様々であると考えられるが、基本対策事項 8.1.1(1)-2 及び「【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について」を参照しつつ、①端末等の不正プログラム感染、②盗難・紛失等による情報漏えい、③バックドアの埋め込み等のサプライチェーン・リスク、といった脅威に対抗するための実施手順を定める必要がある。また、職員等は当該手順に従う必要がある（遵守事項 3.1.1(4)(e)を参照のこと。）。

なお、USB メモリ等の外部電磁的記録媒体の管理に際しては、実施手順の整備のほか、組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するために OS に備わる機能を使用することや製品やサービスの導入も有効である（基本対策事項 7.2.4(1)-2 e)を参照のこと。）。

- **基本対策事項 8.1.1(1)-1「以下を例とする実施手順を定める」について**

a)～f)、i)及び j)は、それぞれ遵守事項 8.1.1(3)～(8)、(9)及び(10)において、職員等を名宛人とした対策事項が規定されている。同様に、g)は遵守事項 6.6.1(1)において、また、h)は遵守事項 6.6.2(1)において対策事項が規定されている。本基本対策事項では、これら規定内容を包含する形で、機関等の実施手順等を定めることを求めている。

なお、統一基準及び本ガイドラインの規定内容を、対策基準に含めて定めることで代替しても差し支えない。

- **基本対策事項 8.1.1(1)-2 a)「国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体」・「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」について**

USB デバイスの設計上の脆弱性を悪用するなどして、USB デバイスのファームウェアを不正に書き換えることによる攻撃手法が確認されている。例えば、悪意のある者が、端末を不正プログラムに感染させることを目的に USB メモリのファームウェアを書き換え、当該 USB メモリを攻撃対象者や不特定多数の者等に配ることが考えられる。当該 USB メモリは、USB ポートに挿入されると不正プログラムを自動的に実行し、端末が不正プログラムに感染してしまう。このようなファームウェアを書き換えられた USB デバイスは、不正プログラム対策ソフトウェア等では検出できない場合もあることから、出所が明らかでありかつ適切な取扱いがなされている外部電磁的記録媒体以外のものの使用については禁止する必要があり、遵守事項 8.1.1(1)(b)で規定する実施手順に基づく管理がなされた外部電磁的記録媒体を使用すべきである。

機関等で使用される外部電磁的記録媒体について、機関等が自組織以外の組織（以下、本解説において「他組織」という。）と、当該他組織が支給する外部電磁的記録媒体を用いて情報の受け渡しをする必要がある場合は、遵守事項 8.1.1(1)(b)に規定する実施手順に定めることとしている対策が、当該他組織において講じられることを担保する必要がある。他組織が機関等である場合は、統一基準群の適用対象であり、上記は担保されるが、他組織が機関等外の組織の場合は、これを契約により遵守させる必要がある。「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」の例としては、委託事業の成果物を外部電磁的記録媒体に記録した形で受け取るケースが想定される。

なお、業務の都合上、やむを得ず本基本対策事項で定める媒体以外の外部電磁的記録媒体から情報を受け取らざるを得ない場合は、例外措置として判断し、不正プログラム感染のリスク等を勘案の上、安全確保のために必要な措置を講ずる必要がある。

- **基本対策事項 8.1.1(1)-2 c)「格納する情報を暗号化する」について**

「（解説）基本対策事項 3.1.1(6)-2 a)「運搬する情報を暗号化する」について」を参

照のこと。

- **基本対策事項 8.1.1(1)-2 c)「セキュアな外部電磁的記録媒体」について**

  「(解説) 基本対策事項 3.1.1(6)-2 c)「セキュアな外部電磁的記録媒体」について」を参照のこと。

- **基本対策事項 8.1.1(1)-2 e)「不正プログラム対策ソフトウェアによる検疫・駆除」について**

  外部電磁的記録媒体に対する不正プログラム対策としては、端末等に導入した不正プログラム対策ソフトウェア等を利用し、USB メモリ等に対して直接検査を実施することが考えられる。機関等内通信回線への感染のリスクを低減させるための更なる対策として、いわゆるサンドボックスとなる緩衝環境や機器等を導入し、端末等に接続する前に検疫・駆除を行うといった方法も考えられる。

- **基本対策事項 8.1.1(1)-2 f)「貸出簿等に記録する」について**

  外部電磁的記録媒体の盗難・紛失が発生した場合に原因を追跡するために、保管場所から外部電磁的記録媒体を取り出す際や保管場所に返却する等の際に貸出簿等に利用状況を記載することが重要である。また、盗難・紛失が発生したことを速やかに把握するために、適宜貸出簿等の内容を確認するとよい。

  貸出簿等の記載事項としては、利用者及び所属、利用開始日時、利用終了日時、機器名、利用する場所、利用目的といったものが考えられる。

- **基本対策事項 8.1.1(1)-3 b)「手続内容」について**

  USB メモリ等の外部電磁的記録媒体を利用する際、実施手順に従い貸出簿等に記録することが求められており (基本対策事項 8.1.1(1)-2 f)を参照のこと。)、また利用時に許可が必要な場合は、許可手続に従い手続内容の記載が求められている (基本対策事項 8.1.1(1)-3 b)を参照のこと。)。手続内容が貸出簿等に記録する内容と重複する場合は、業務の効率化の観点から、例えば、貸出簿に一意に識別できる貸出番号の項目を追加し、参照することで手続内容の記載を省略するといった運用が考えられる。

【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について

USB メモリ等の外部電磁的記録媒体に関連する脅威（①②③）及び脆弱性（箇条書き）としては、以下が想定される。

① 端末等の不正プログラム感染
- 利用者、用法等が不明な物が使用されている。
- 外部電磁的記録媒体を接続した際に自動的にプログラムが実行される。
- 不正プログラム対策ソフトウェアによる検疫・駆除を行っていない。

② 盗難・紛失等による情報漏えい
- 利用者、用法等が不明な物が使用されている。
- 運搬の際等に暗号化等の安全管理措置がなされていない。
- 不要な要機密情報が保存されている。

③ バックドアの埋め込み等のサプライチェーン・リスク
- 製造元、製造過程が不明な物が使われる。

上記の脅威及び脆弱性に対しては、表 8.1.1-1 に掲げる対策が想定される。

表 8.1.1-1　USB メモリ等の外部電磁的記録媒体に関する対策の例

脅威	対策	対策の種類	関連する基本対策事項
①不正プログラム感染	主体認証機能や暗号化機能を備える外部電磁的記録媒体を導入する。	調達時の対策	5.2.1(3)関連
	不正プログラムの検疫・駆除機能を備える外部電磁的記録媒体を導入する。	調達時の対策	5.2.1(3)関連
	情報を暗号化するための機能を備えたソフトウェアを導入する。	調達時の対策	5.2.1(3)関連 7.1.5 関連
	外部電磁的記録媒体の検疫・駆除機能を備える不正プログラム対策ソフトウェアを導入する。	調達時の対策	7.2.2(1)関連
	サーバ装置及び端末の自動再生（オートラン）機能や自動実行機能を無効にする。	技術的な設定	7.2.4(1)-2 c)
	サーバ装置及び端末において使用を想定しない USB ポート等を無効にする。	技術的な設定	7.2.4(1)-2 d)
	外部電磁的記録媒体の使用前に、不正プログラム対策ソフトウェアや外部電磁的記録媒体に備わる機能による不正プログラムの検疫・駆除を行う。	利用時の対策	8.1.1(1)-2 e) 8.1.1(8)関連

脅威	対策	対策の種類	関連する 基本対策事項
②情報漏えい	運搬の際等に主体認証機能や暗号化機能の利用等の安全管理措置を講ずる。	利用時の対策	3.1.1(6)-2 c) 8.1.1(1)-2 c)
	要機密情報は保存される必要がなくなった時点で速やかに削除する。	利用時の対策	8.1.1(1)-2 d)
③サプライチェーン・リスク	安全と考えられる製造元、製造過程の製品を調達する。	調達時の対策	4.3.1 関連
①②③共通	使用可能な媒体の制限や利用方法等に関する手順を定める。	管理対策	8.1.1(1)-2
	組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。	管理対策 調達時の対策	7.2.4(1)-2 e)

遵守事項

(2) 情報システム利用者の規定の遵守を支援するための対策

(a) 情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

【 基本対策事項 】

＜8.1.1(2)(a)関連＞

8.1.1(2)-1 情報システムセキュリティ責任者は、機関等外のウェブサイトについて、職員等が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) ウェブサイトフィルタリング機能

b) 事業者が提供するウェブサイトフィルタリングサービスの利用

8.1.1(2)-2 情報システムセキュリティ責任者は、職員等が不審な電子メールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) 受信メールに対するフィルタリング機能

b) 受信メールをテキスト形式で表示する機能

c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアントの導入

d) 受信メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能

（解説）

- **遵守事項 8.1.1(2)(a)「職員等による規定の遵守を支援する機能」について**

職員等が対策基準に定めた規定を守ることを前提としつつ、情報システムの仕組みとして、情報セキュリティインシデントが発生しにくい利用環境を職員等に提供することにより、組織全体のセキュリティ水準を確保することを求める規定である。例えば、基本対策事項に示したとおり、閲覧するとウイルス感染被害に遭うことが判明しているサイトや受信した電子メールをフィルタリングして閲覧不可にすることで被害を回避するなどが考えられる。

これ以外にも、例えば、職員等のパスワードを他者に知られないようにするために、入力したパスワードの文字列がアスタリスク等により非表示となる機能を設けることが考えられる。また、職員等が意図しない相手に電子メールを送信することをシステム的に抑止する対策として以下のような機能を情報システムに導入すること等も考えられる。

- 送信者の電子メールアドレスのドメイン名以外のドメインのアドレスが宛先アドレスに含まれる場合に警告を表示するなど、入力された宛先アドレスをチェックして警告する機能
- To、Cc、Bcc に入力された宛先アドレスの数が設定数以上になっているときに警告する機能
- 添付ファイルがある場合に警告する機能
- 送信メールの件名、本文、添付ファイルにあらかじめ設定した文字列が含まれる場合に警告する機能
- 送信者が送信指示を行った後、あらかじめ設定された時間だけ送信を保留することにより、送信者が誤送信に気が付いた場合に、送信を取り消すことができる機能

- **基本対策事項 8.1.1⑵-2 b)「テキスト形式で表示する機能」について**

いわゆるフィッシング等の脅威が想定される外部からの電子メールを受信する情報システムを対象とした規定である。HTML 形式の電子メールは、その形式の特徴が悪用され、本文中の URL を偽装した電子メールを送ることにより、フィッシング行為や不正プログラムを埋め込んだウェブサイトへの誘引行為に利用されている。フィッシング等の被害に遭うリスクが想定される場合には、テキスト形式や RTF（Rich Text Format）形式等の URL 偽装のリスクの無い形式で表示することが望ましい。

- **基本対策事項 8.1.1⑵-2 d)「実行プログラム形式のファイルを削除等する」について**

実行プログラム形式のファイルとは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。実行プログラム形式のファイルは、不正プログラムを感染させる手段として標的型攻撃等に悪用されることが多いことから、特に電子メールに添付された実行プログラム形式のファイルについては、職員等がこれを開くことができないよう、システム的に抑止する機能を導入することを基本対策事項としている。ファイルを削除等する機能の例としては、電子メールの中継サーバにおいて、中継する電子メールの全てを検査して、実行プログラム形式のファイルが添付ファイルとして含まれている場合にはその添付ファイルを削除する機能が挙げられるほか、中継サーバでの削除に代えて、電子メールを受信した端末側で該当する添付ファイルを開けないようにする機能等が想定される。

また、実行プログラム形式のファイルは、「.zip」、「.lzh」等の圧縮形式のファイルの内部に含められることがあり、職員等が圧縮形式のファイルを展開し、展開後に現れる実行プログラム形式のファイルを開いてしまうことにより、不正プログラムに感染する事態も想定されることから、圧縮形式のファイルの内部に含められた実行プログラム形式のファイルも削除等の対象とする必要がある。

なお、パスワードを用いて暗号化された圧縮形式のファイルについては、当該ファイル中に不正プログラムが含まれるか否かの検疫を行えないことが考えられるため、不正プログラムに感染するリスクがより高まることが想定される。そのため、パスワード

を用いて暗号化された圧縮形式のファイル中に実行プログラム形式のファイルが含まれるか否かを技術的に検査できない場合には、暗号化された圧縮形式のファイル自体を添付ファイルから削除等する機能の導入を考慮する必要がある。圧縮形式のファイル中のファイルの検査をする機能を導入する代わりに、暗号化の有無にかかわらず圧縮形式のファイルの全てを削除等する措置を用いてもよい。

これらファイル削除等の機能の導入は、職員等に一定の不便をもたらすことになり得るが、これを実施せず、開いてよいファイルか否かを職員等に添付ファイルの拡張子を個々に確認させる方法を代用策とした状態では、標的型攻撃等を企図した電子メールの添付ファイルを誤って開いてしまう危険性を十分に抑制することは困難であることから、これをシステム的に抑止する機能の導入が推奨される。

また、マクロ付きファイルや、ファイル内に書かれた指示に従うことでプログラムが実行されるファイルによって不正プログラムに感染するリスクを低減するために、基本対策事項 8.1.1(8)-3 に規定する対策を検討するとよい。

遵守事項

(3) 情報システムの利用時の基本的対策

(a) 職員等は、業務の遂行以外の目的で情報システムを利用しないこと。

(b) 職員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機関等の情報システムを接続しないこと。

(c) 職員等は、機関等内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。

(d) 職員等は、業務の遂行において、利用が認められていないソフトウェアを利用しないこと。また、当該ソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。

(e) 職員等は、接続が許可されていない機器等を情報システムに接続しないこと。

(f) 職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

(g) 職員等は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、課室情報セキュリティ責任者の許可を得ること。

(h) 職員等は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しないこと。

【 基本対策事項 】

＜8.1.1(3)(f)関連＞

8.1.1(3)-1 職員等は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。

a) スクリーンロックの設定

b) 利用後のログアウト徹底

c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

（解説）

- **遵守事項 8.1.1(3)(a)「業務の遂行以外の目的で情報システムを利用しない」について**

本規定の脅威の例としては、意図せず悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染することが想定される。

- **遵守事項 8.1.1(3)(b)「接続許可を与えた通信回線以外」について**

機関等内通信回線であっても機関等外通信回線であっても、許可を得ていない通信回線に接続してはならない。モバイル端末を持ち出した際に接続する通信回線については、機関等内通信回線以外の利用となり、盗聴等の脅威が増大することから、許可されていない通信回線への接続は回避すべきである。ただし、出張先等で利用する通信回線が未定の場合は、事前の許可が難しいことから、回線の種別（通信事業者の回線・公衆無線 LAN 回線等）で管理すること等も考えられる。

なお、機関等支給以外の端末についても、本項と同等の対策を講ずることが望ましい。

- **遵守事項 8.1.1(3)(c)「接続許可を受けていない情報システム」について**

  要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む。）を機関等内通信回線に直接接続することについては、それぞれの情報システムについての接続許可を決定する前に、そもそもこのような接続を業務上認める必要があるのかどうかについて、その是非を判断することを遵守事項 6.1.2(1)(c)及び遵守事項 6.1.3(2)(d)で求めている。

- **遵守事項 8.1.1(3)(d)「情報システムセキュリティ責任者の承認を得る」について**

  職員等が、許可を得て、機関等支給以外の端末で業務を行う場合にも本規定が適用される。

  なお、承認を得る際には、ソフトウェアの必要性や利用目的、取り扱う情報の概要、要機密情報の取扱いの有無、製品名、バージョン、入手方法（ソフトウェアの入手元となる URL、事業者名等）、入手可能な場合には利用規約等を添付して、情報システムセキュリティ責任者に申請することが望ましい。

- **遵守事項 8.1.1(3)(e)「接続が許可されていない機器等」について**

  出所不明の USB デバイス（例えば、無料で配布される USB デバイス）やセキュリティ管理が不十分な私物のスマートフォン等が情報システムに接続されることが許容されていると、不正プログラム感染等のリスクが高まることから、情報システムへ接続可能な機器等（又は接続を禁止する機器等）をあらかじめ定めておくとよい。

  「（解説）基本対策事項 8.1.1(1)-2 a)「国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体」・「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」について」も参照のこと。

- **遵守事項 8.1.1(3)(g)「許可を得る」について**

  遵守事項 8.1.1(1)(c)において、USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合についての統括情報セキュリティ責任者が定めた許可手続の実施を求めている。外部電磁的記録媒体の利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、定められた手順に従って、適切に措置する必要がある。

- **遵守事項 8.1.1(3)(h)「利用承認を得ていないクラウドサービスを利用しない」について**

  本規定はシャドーIT の抑止を目的としたものである。

  クラウドサービスを利用して要機密情報を取り扱う場合は、遵守事項 4.2.1(4)において利用承認を得たクラウドサービスを利用する必要がある。また、クラウドサービスを利用して要機密情報を取り扱わない場合は、遵守事項 4.2.3(2)において利用承認を得たクラウドサービスを利用する必要がある。

遵守事項

(4) 端末（支給外端末を含む）の利用時の対策

(a) 職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

(b) 職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(ア) 機関等が支給する端末（要管理対策区域外で使用する場合に限る） 機密性3情報、要保全情報又は要安定情報

(イ) 機関等支給以外の端末 要保護情報

(c) 職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、定められた措置を講ずること。

【 基本対策事項 】

＜8.1.1(4)(c)関連＞

8.1.1(4)-1 職員等は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する端末を要管理対策区域で機関等内通信回線に接続する場合には、定められた技術的な措置を講ずること。

8.1.1(4)-2 職員等は、要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を要管理対策区域で機関等内通信回線に接続する場合には、以下を全て含む措置を講ずること。

a) 定められた安全管理措置を講ずること。

b) 課室情報セキュリティ責任者の許可を得ること。

（解説）

- **遵守事項 8.1.1(4)(a)「定められた利用手順」について**

職員等に対して、遵守事項 6.1.2(1)(a)及び遵守事項 6.1.3(2)(b)において統括情報セキュリティ責任者が定めた利用手順の遵守を求めている。取り扱う情報の格付や取扱制限に応じて、適切に情報処理を行うことが求められる。

- **遵守事項 8.1.1(4)(b)「許可を得る」について**

職員等に対して、遵守事項 6.1.2(1)(a)及び遵守事項 6.1.3(2)(b)において統括情報セキュリティ責任者が定めた許可手続の実施を求めている。利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、これらについても定められた手順に従う必要がある。

- **基本対策事項 8.1.1(4)-1「定められた技術的な措置」について**

職員等に対して、遵守事項 6.1.2(1)(c)において統括情報セキュリティ責任者が定めた

技術的な措置を講ずることを求めている。

- **基本対策事項 8.1.1(4)-2 a)「定められた安全管理措置」について**

  職員等に対して、遵守事項 6.1.3(2)(d)において統括情報セキュリティ責任者が定めた安全管理措置を講ずることを求めている。

遵守事項

(5) 電子メール・ウェブの利用時の対策

(a) 職員等は、要機密情報を含む電子メールを送受信する場合には、それぞれの機関等が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。

(b) 職員等は、機関等外の者と電子メールにより情報を送受信する場合は、政府ドメイン名を取得できない場合を除き、当該電子メールのドメイン名に政府ドメイン名を使用すること。

(c) 職員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

(d) 職員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

(e) 職員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

(f) 職員等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の全ての事項を確認すること。

(ア) 送信内容が暗号化されること

(イ) 当該ウェブサイトが送信先として想定している組織のものであること

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(5)(a)「送受信」について**

「送受信」には電子メールの「転送」が含まれる。したがって、職員等が受信する目的で機関等支給以外の電子メールサービスの電子メールアドレスに要機密情報を含む電子メールを転送することは、やむを得ない理由により許可を得ている場合を除き、認められない。許可にあっては、転送する電子メールの内容やその理由により、個別に判断する必要があり、機関等支給以外の電子メールサービスで受信することのリスクを踏まえた上で、転送先の電子メールアドレスが正しいことを確認する必要がある。特に、自動転送については、許可を受けている場合であっても、当該電子メールに含まれる情報の格付及び取扱制限にかかわらず行われるため、遵守事項 3.1.1(6)に規定されている要機密情報の送信についての遵守事項に違反しないように留意が必要である。

- **遵守事項 8.1.1(5)(b)「政府ドメイン名を取得できない場合」について**

政府ドメイン名を使用しない場合のリスク等は、「（解説）遵守事項 6.6.2(1)(a)「政府ドメイン名を取得できない場合」について」を参照のこと。

本対策における政府ドメイン名を取得できない場合とは、特段の理由により政府ドメイン名が使えない場合も含めたものである。

政府ドメイン名を取得できない場合の例を以下に示す。

- 指定法人が、政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。
- 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用すると判断する場合。
  - 併せて、「(解説)遵守事項 6.6.2(1)(a)「政府ドメイン名を取得できない場合」について」を参照のこと。
- 電子メールを受信する機関等外の者が、職員等から送信された電子メールであることを認知できる場合（政府ドメイン名又は本解説上記に基づき取得したドメイン名が使用できない場合に限る。）。

- **遵守事項 8.1.1(5)(c)「不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する」について**

「不審な電子メール」とは、受信する覚えのない電子メールであって、電子メール本文中に URL が記載されているもの、実行形式や文書形式のファイルが添付されているもの等が該当する。こういった電子メールについて、むやみに URL のリンク先や添付ファイルを開かないことも重要であるが、開かなかった場合でも他の者が同種の電子メールを受信することも考えられるため、情報提供を行うことも重要である。定められた連絡先としては、CSIRT や当該電子メールを扱う情報システムの情報システムセキュリティ責任者等が考えられる。

- **遵守事項 8.1.1(5)(d)「情報セキュリティに影響を及ぼすおそれのある設定変更を行わない」について**

以下を例とするブラウザのセキュリティ設定項目について、変更すると悪意のあるソフトウェアが端末において実行されること等により、情報の漏えいや、他のサーバ装置及び端末を攻撃することを引き起こすことも考えられるため、変更が可能であったとしても勝手に変更しないようにする必要がある。

＜ブラウザのセキュリティ設定項目の例＞

- ActiveX コントロールの実行
- Java の実行

- **遵守事項 8.1.1(5)(f)(ア)「送信内容が暗号化されること」について**

主体認証情報等を入力して送信する場合には、ブラウザの鍵アイコンの表示を確認するなどにより、TLS 等の暗号化通信が使用され、要機密情報が適切に保護されることを確認することを求める事項である。

なお、「閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合」とは、例えばウェブメール本文の入力欄に要機密情報を入力すること等を指す。

- **遵守事項 8.1.1(5)(f)(イ)「当該ウェブサイトが送信先として想定している組織のものであること」について**

ブラウザで主体認証情報等を入力して送信する場合には、ウェブサーバの電子証明

書の内容から当該ウェブサイトが想定している組織のものであることを確認することにより、適切でない送信先に当該情報を誤って送信することを回避する必要がある。

なお、ウェブサイトの閲覧時にウェブサーバの電子証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性があるため、利用を中止する必要がある。

近年において被害が広がっている「フィッシング（Phishing)」と呼ばれる悪質な行為に対しても十分警戒する必要がある。このようなフィッシングの被害を避けるためにも、本項で示す対策を実施することが重要である。

遵守事項

(6) 識別コード・主体認証情報の取扱い

(a) 職員等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

(b) 職員等は、自己に付与された識別コードを適切に管理すること。

(c) 職員等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

(d) 職員等は、自己の主体認証情報の管理を徹底すること。

【 基本対策事項 】

＜8.1.1(6)(b)関連＞

8.1.1(6)-1 職員等は、自己に付与された識別コードを適切に管理するため、以下を全て含む措置を講ずること。

a) 知る必要のない者に知られるような状態で放置しないこと。

b) 他者が主体認証に用いるために付与及び貸与しないこと。

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止すること。

＜8.1.1(6)(d)関連＞

8.1.1(6)-2 職員等は、知識による主体認証情報を用いる場合には、以下を全て含む管理を徹底すること。

a) 自己の主体認証情報を他者に知られないように管理すること。

b) 自己の主体認証情報を他者に教えないこと。

c) 主体認証情報を忘却しないように努めること。

d) 主体認証情報を設定するに際しては、推測されないものにすること。

e) 異なる識別コードに対して、共通の主体認証情報を用いないこと。

f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いないこと。（シングルサインオンの場合を除く。）

g) 情報システムセキュリティ責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。

8.1.1(6)-3 職員等は、所有による主体認証情報を用いる場合には、以下を全て含む管理を徹底すること。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。

b) 主体認証情報格納装置を他者に付与及び貸与しないこと。

c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告すること。

d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者に返還すること。

（解説）

- **遵守事項 8.1.1(6)(a)「自己に付与された識別コード以外の識別コード」について**

自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、合理的な理由が無い限り「なりすまし行為」である。仮に、悪意がなくても、他者の識別コードを使って情報システムを利用することは、許容されてはならない。例えば、何らかの障害により自己の識別コードの使用が一時的に不可能になった場合には、まず、当該情報システムを利用して行おうとしている業務について、他者へ代行処理を依頼することを検討すべきであり、仮に他者の許可を得たとしても、他者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを使って、情報システムを利用するということは制限されなければならない。

業務の停止によって重大な影響を及ぼす業務を継続させるために、他者の識別コードを使うことが不可避の場合には、例外措置の手続を行う際に本人の事前の了解に加えて、情報システムセキュリティ責任者の承認を得ることが最低限必要である。また、他者の識別コードを使用していた期間とアクセスの内容を、事後速やかに、情報システムセキュリティ責任者に報告しなければならない。情報システムセキュリティ責任者は、その理由と使用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えることが望ましい。

いずれの場合も、使用する識別コードの本人からの事前の許可を得ずに、その者の識別コードを使って、情報システムを利用することは禁止されるべきである。

- **遵守事項 8.1.1(6)(c)「管理者としての業務遂行時に限定して」について**

例えば、情報システムの OS が Windows の場合、管理者権限ありの識別コードを利用中に不正プログラムに感染等した場合、攻撃者は管理者権限を利用することが可能となるため、管理者権限なしの識別コードを利用中に不正プログラムに感染等した場合と比べ、大きな影響を及ぼすおそれがある。

そのため、電子メールの利用や Web サイトの閲覧等の、管理者権限が不要であり、不正プログラム感染等の脅威が発生する可能性が高まることは、管理者としての業務遂行時に行ってはならない。

- **基本対策事項 8.1.1(6)-1 a)「知る必要のない者に知られるような状態で放置しない」について**

多くの場合、識別コード単体は必ずしも秘密ではないが、必要以上の範囲に開示する、又は公然となるような状態で放置しないように求めている。

主体認証には、識別コードと主体認証情報の組合せが用いられる。識別コードの開示範囲を必要最小限に止めることによって、第三者が不正に主体認証を行う可能性をより低くすることができる。そのため、識別コードを適切に管理する必要がある。

- **基本対策事項 8.1.1(6)-1 b)「他者が主体認証に用いるために付与及び貸与しない」について**

情報システムセキュリティ責任者が明示的に共用識別コードとしているもの以外の

識別コードを、他の主体と共用してはならない。

- **基本対策事項 8.1.1(6)-1 c)「定められた手続に従い、識別コードの利用を停止する」について**

  識別コードを使用する必要がなくなった場合に、職員等自らが情報システムセキュリティ責任者へ届け出ること等、定められた手続に従い、識別コードを使用できない状態に変更することを求めている。ただし、例えば、人事異動等によって、職員等の識別コードが大規模に変更となる場合や、その変更を情報システムセキュリティ責任者が職員等自らからの届出によらず把握できる場合等、職員等自らの届出が不要となる条件を情報システムセキュリティ責任者が定めてもよい。

- **基本対策事項 8.1.1(6)-2 a)「自己の主体認証情報を他者に知られないように管理する」について**

  以下を例とする他者からのパスワード窃取行為に注意が必要である。

  - パスワードを入力する際に他者が周囲から盗み見する。
  - 他者が管理者を名乗ってパスワードを聞き出す。

  また、以下に挙げる行為は行うべきではない。

  - 自己のパスワードを、内容が分かる状態で付箋等に記入してモニタ、端末本体、及びその周辺に貼付する。
  - 自己のパスワードを、特段の保護をせずに平文のままテキスト形式で保存する。

  など、容易に他者に知られてしまう状態で、情報システム上に記録する。

- **基本対策事項 8.1.1(6)-2 b)「自己の主体認証情報を他者に教えない」について**

  たとえ、他者に処理を代行させる目的であっても、職員等は自己の主体認証情報を他者に教示してはならない。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関係が曖昧になり、アクセス制御、権限管理、ログ管理その他のセキュリティ対策が効果を失う可能性がある。また、教示された者にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己の主体認証情報は他者に「教えない」ことを徹底すべきである。

- **基本対策事項 8.1.1(6)-2 c)「主体認証情報を忘却しないように努める」について**

  他者が容易に見ることができないような措置（施錠して保存するなど）や、他者が見ても分からないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取る行為を禁ずるものではない。むしろ、忘れることのないように努めなければならない。

  なお、本人の忘却によって主体認証情報を初期化（リセット）する場合には、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。

- **基本対策事項 8.1.1(6)-2 d)「推測されないもの」について**

主体認証情報がパスワードである場合、パスワードに利用者の名前や利用者個人に関連する情報から簡単に派生させたもの、キーボードの並び順（「qwertyuiop」等）等、容易に推測されるものを用いてはならない。

パスワードとして設定できる文字列の長さにシステム上の上限があるなどの理由により、8 文字程度の短い文字列しか使用できない場合には、辞書に載っているような単語をそのまま用いてはならず、使用する文字種として、アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜるなどして、可能な限りランダム生成に近い文字列（※）を選び、推測されないパスワードを設定することが望ましい。

一方、設定できる文字列の長さに上限がなく、十分に長い文字列をパスワードとして設定する場合には、辞書に載っている単語を用いてよい場合もある。例えば、5 万語の辞書から 3 つの語をランダムに選び(日常の使用頻度が低めの語を選ぶ方が望ましい。)それらを繋げた文字列（その長さは、30 文字を超えることが望まれる。）をパスワードとするならば、上記※の文字列以上に「推測されないもの」となるので、この場合は辞書に載っている単語をそのまま用いてよい。また、この場合、数字や記号を織り交ぜることも必要でない。

何文字以上の文字列ならば数字や記号を織り交ぜる必要がなくなるのかは、選択した文字列のランダム性との関係で決まるため、数字や記号を織り交ぜたくないならば長めの文字列を選び、長い文字列を選びたくないならば数字や記号を織り交ぜることになる。

なお、パスワードの設定方法は、「(解説) 基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」も参照すること。

- **基本対策事項 8.1.1(6)-2 e)「共通の主体認証情報を用いない」について**

複数の識別コードを付与されている場合に、それら識別コードに対して共通の主体認証情報を用いると、一つの識別コードに対応する主体認証情報が漏えいした場合に、他方の識別コードを用いた不正アクセスを受ける危険性が高くなる。したがって、共通の主体認証情報を用いてはならない。

- **基本対策事項 8.1.1(6)-2 f)「識別コード及び主体認証情報についての共通の組合せ」について**

複数の情報システムにおいて、共通の識別コードを使用し、かつ、共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に使用されるという情報セキュリティインシデントが発生することが考えられる。したがって、複数の情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを使用しないようにしなければならない。特に、機関等支給の情報システムと機関等支給以外の情報システムとの間では、共通の識別コード及び主体認証情報を使用しないよう注意が必要である。

- **基本対策事項 8.1.1(6)-3 a)「主体認証情報格納装置を本人が意図せずに使われることの**

ないように」について

主体認証情報格納装置の例としては、建物への入退や端末ログインに必要となる IC カード等が挙げられる。所有による主体認証方式では、本人でなくとも主体認証情報格納装置を保持する者が正当な主体として主体認証されるため、他者に当該装置を使用されることがないように適切に管理する必要がある。

遵守事項

(7) 暗号・電子署名の利用時の対策

(a) 職員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム、鍵長及び方法に従うこと。

(b) 職員等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

(c) 職員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(7)(a)「定められたアルゴリズム、鍵長及び方法に従う」について**

暗号アルゴリズム及び鍵長は、ファイル単体の暗号化やハードディスク全体の暗号化、ブラウザを使う通信の暗号化等、様々な場面で利用されていることから、利用する場面ごとに適切なアルゴリズム及び鍵長を適切な方法で利用する必要がある。

情報システムセキュリティ責任者は、職員等の暗号機能の利用において、認められていないアルゴリズム及び鍵長が利用されないよう、事前に情報システムにおいて対処することが望ましい。

- **遵守事項 8.1.1(7)(b)「定められた鍵の管理手順等に従い、これを適切に管理する」について**

暗号化された情報の復号又は電子署名の付与に用いる鍵の管理手順として、情報システム共通として鍵の保存手順を定めている場合と、情報システムごとに鍵の保存手順を個別に定めている場合があるので、各情報システムに対応した手順に従うことが求められる。

- **遵守事項 8.1.1(7)(c)「鍵のバックアップ手順に従い、そのバックアップを行う」について**

暗号化された情報の復号に用いる鍵の滅失により、情報の可用性が損なわれるおそれがあることから、適切に鍵をバックアップすることを求めている。

バックアップが必要な鍵については、バックアップの取得又は第三者への鍵情報の預託に関する手順等の規定に従う必要がある。

また、バックアップしてはならない鍵や、鍵情報の複製が、その漏えいに係るリスクを高める可能性があるなどについても留意し、バックアップは必要最小限にとどめることも大切である。

遵守事項

(8) 不正プログラム感染防止

(a) 職員等は、不正プログラム感染防止に関する措置に努めること。

(b) 職員等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

【 基本対策事項 】

＜8.1.1(8)(a)関連＞

8.1.1(8)-1 職員等は、不正プログラム対策ソフトウェア等を活用し、不正プログラム感染を回避するための以下の全ての措置に努めること。

a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しないこと。また、検知されたデータファイルをアプリケーション等で読み込まないこと。

b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にすること。

d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施すること。

8.1.1(8)-2 職員等は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

8.1.1(8)-3 職員等は、不正プログラムに感染するリスクを低減する情報システム（支給外端末を含む。）の利用方法として、以下のうち実施可能な措置を講ずること。

a) 不審なウェブサイトを閲覧しないこと。

b) アプリケーションの利用において、マクロ等の自動実行機能を無効にすること。

c) プログラム及びスクリプトの実行機能を無効にすること。

d) 安全性が確実でないプログラムをダウンロードしたり実行したりしないこと。

（解説）

- **遵守事項 8.1.1(8)(a)「不正プログラム感染防止に関する措置に努める」について**

  情報システムの利用に当たっては、職員等自らが不正プログラム感染の予防に努めなければならない。また、不正プログラム対策ソフトウェア等が全ての不正プログラムを検知できるとは限らないことを念頭に入れ、不正プログラムに感染するリスクを低減するために、可能な措置の実施に努める必要がある。

- **遵守事項 8.1.1(8)(b)「通信回線への接続を速やかに切断するなど、必要な措置を講ず**

る」について

不正プログラムに感染したおそれがある情報システム（支給外端末を含む。）については、他の情報システムへの感染等の被害の拡大を防ぐ必要がある。当該情報システムを構成するサーバ装置又は端末（支給外端末を含む。）が通信回線に接続している場合には、有線の場合は回線の切断や抜去を行う、無線の場合は機器等の無線 LAN 通信機能を停止することや機器等を休止状態にすること等、有線と無線では措置が異なることに留意した上で、感染拡大を防止する措置を行うことが求められる。また、2.2.4「情報セキュリティインシデントへの対処」に定められた報告や連絡等の対処を行うことが求められる。

不正プログラムに感染したおそれのある場合の対処について、手順が規定されている場合、その内容に従う必要がある。

- **基本対策事項 8.1.1(8)-1 a)「実行プログラム形式のファイルを実行しない」について**

不正プログラムとして検知された実行プログラム形式のファイルを実行した場合には、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に相当な労力を要することとなるため、このような実行プログラム形式のファイルを実行しないよう努めなければならない。

- **基本対策事項 8.1.1(8)-1 b)「最新の状態に維持する」について**

一般的に不正プログラムはほぼ毎日のように新種や亜種が出現しているため、不正プログラム対策ソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を更新機能や更新プログラムにより最新の状態に維持することで、不正プログラム等に感染することを回避する必要がある。自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。

また、最新の状態に維持する方法としては、端末（支給外端末を含む。）ごとに利用者が自動化の設定をする方法のほか、情報システムセキュリティ責任者等が管理する端末を一括して自動化する方法もあるため、情報システムごとに定められた方法に従うこと。

- **基本対策事項 8.1.1(8)-1 c)「自動検査機能を有効にする」について**

手動による対策実施は、実施漏れや遅れが発生する可能性があるため、不正プログラム対策の中で自動化が可能なところは自動化することが望ましい。

自動検査機能の例としては、ファイルの作成や参照のたびに検査を自動的に行う機能等がある。

- **基本対策事項 8.1.1(8)-1 d)「不正プログラムの検査を実施する」について**

基本対策事項 8.1.1(8)-1 c)の自動検査機能が有効になっていたとしても、検査した時点における不正プログラム対策ソフトウェア等では検知されない不正プログラムに感染している危険性が残る。このような危険性への対策として、最新の状態にした不正プログラム対策ソフトウェア等で定期的に全てのファイルについて検査する必要がある。

- **基本対策事項 8.1.1(8)-2「外部からデータやソフトウェアをサーバ装置及び端末等に取**

り込む場合又は外部にデータやソフトウェアを提供する場合」について

「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合」には、ウェブの閲覧や電子メールの送受信等のネットワークを経由する場合だけでなく、USB メモリや CD-ROM 等の外部電磁的記録媒体を経由する場合も含む。

遵守事項

(9) Web 会議サービスの利用時の対策

(a) 職員等は、定められた利用手順に従い、**Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること**。

(b) 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

【 基本対策事項 】

＜8.1.1(9)(a)関連＞

8.1.1(9)-1 職員等は、Web 会議サービスの利用に当たり、以下を全て含む情報セキュリティ対策を実施すること。

a) **原則として、機関等が支給する端末を利用する**こと。

b) **原則として、機関等が利用を許可した Web 会議サービスを利用する**こと。

c) 利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認すること。

d) 要機密情報を取り扱う場合は、**可能な限りエンドツーエンド（E2E）の暗号化を行うこと**。

e) 要機密情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、**E2E の暗号化を利用できなくなる機能を可能な限り使用しない**こと。

＜8.1.1(9)(b)関連＞

8.1.1(9)-2 職員等は、会議に無関係な者を会議に参加させないために、以下を例とする対策を行うこと。

a) 会議室にアクセスするための**パスワード等**をかけること。

b) 会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知すること。

c) 会議を非公開設定にすること。

d) **待機室を設けて参加者と確認できた者**だけを会議室に入室させること。

e) **Web 会議の主催者が事前に登録した者**だけを会議室に入室させること。

f) なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させること。

（解説）

- **遵守事項 8.1.1(9)(a)「Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること」について**

Web 会議サービスを利用する場合、Web 会議サービスのソフトウェアで録画等を防止する設定を行っていても、ビデオカメラで撮影されれば会議内容は保存されるため、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認

する必要がある。

- **基本対策事項 8.1.1(9)-1 a)「原則として、機関等が支給する端末を利用する」について**

  Web 会議サービスの機能は多岐に渡り、機能追加も日々行われている状況にあり、要機密情報を扱う場合もあることから、原則として、機関等が支給する端末を利用するべきである。ただし、Web 会議サービスを利用する場合でも、一般に公開されたオンラインセミナー等に参加する場合など特に要機密情報を取り扱わない場合は、機関等支給以外の端末を利用してもよい。

- **基本対策事項 8.1.1(9)-1 b)「原則として、機関等が利用を許可した Web 会議サービスを利用する」について**

  Web 会議サービスは一般的にはクラウドサービスであることが考えられる。Web 会議サービスがクラウドサービスの場合は、原則として、4.2「クラウドサービス」において機関等が利用を承認した Web 会議サービスを利用する必要がある。Web 会議サービスがクラウドサービスではない場合は、原則として、機関等が利用を承認したソフトウェアを使用し、Web 会議サービスを利用する必要がある。

  なお、外国政府、企業又は団体等（以下本解説において「外部機関等」という。）からゲストアカウントなどにより、機関等が利用を承認していない Web 会議サービスを利用する場合は、Web 会議サービスにおいて実施されているセキュリティ対策が明らかではないため、Web 会議サービスで取り扱う情報が漏えいすることを前提にした上で、機関等において漏えいが許容できない情報は取り扱わない等、情報の取扱いに留意が必要である。

- **基本対策事項 8.1.1(9)-1 d)「可能な限りエンドツーエンド（E2E）の暗号化を行うこと」について**

  E2E の暗号化を行わない場合、端末からサービス提供者のサーバまで会議データは暗号化されるが、復号鍵をサービス提供者が保有しているため、会議データの復号が可能となる。このため、E2E の暗号化を行わない外部機関等との Web 会議に招待され、参加しなければならない等のやむを得ない場合を除き、要機密情報を取り扱う場合は E2E の暗号化を行うように設定する必要がある。

- **基本対策事項 8.1.1(9)-1 e)「E2E の暗号化を利用できなくなる機能を可能な限り使用しない」について**

  E2E の暗号化を行っている場合は、サービス提供者が復号鍵を保有していないため、サービス提供者のサーバ上で会議データを復号することができない。しかし、会議の録画、議事録の自動作成、自動翻訳などを行うには、サービス提供者が復号された会議データを利用する必要があるため、当該機能を利用する場合は、E2E の暗号化を利用できなくなる。従って、サービス提供者により会議データの復号が可能となることに注意が必要である。

  そのため、E2E の暗号化を利用できなくなる自動翻訳機能を利用しなければ外部機関等との Web 会議が成立しない等のやむを得ない場合を除き、要機密情報を取り扱う場合は E2E の暗号化を利用できなくなる機能を使用しないようにする必要がある。

- **基本対策事項 8.1.1(9)-2 a)「パスワード等」について**

  パスワードを用いる場合は、「(解説) 基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照すること。

- **基本対策事項 8.1.1(9)-2 d)「待機室を設けて参加者と確認できた者」について**

  正当な参加者であることを確認するための方法としては、参加者名に特定の規則を設けることや、事前に参加者名を申告させることを会議の開催前に参加者に周知し、待機室で参加者名が適切であることを確認すること等が考えられる。

- **基本対策事項 8.1.1(9)-2 e)「Web 会議の主催者が事前に登録した者」について**

  Web 会議サービスによっては、Web 会議の参加者に対してメール等で招待状を送り、その招待に応じた参加者を主催者が事前に登録を行うことで、事前に登録された参加者のみが会議に参加することが可能となる機能が存在する。利用する Web 会議サービスが当該機能を備えている場合は利用するとよい。

遵守事項

(10) クラウドサービスを利用した機関等外の者との情報の共有時の対策

(a) 職員等は、機関等外の者と**情報の共有**を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、**情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となる**ための措置を講ずること。

(b) 職員等は、機関等外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、**クラウドサービス上に保存した要保護情報を速やかに削除する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(10)(a)「情報の共有」について**

本条における「情報の共有」とは、一つの場所に保存されている同一の情報を複数の利用者が参照、更新、削除することをいう。「情報の共有」が想定しているケースは、例えば、オンラインストレージ等のファイル共有サービス上に保存した同一のファイルを複数の利用者が参照、更新、削除するケースや、進捗管理機能やファイル共有機能等を備えるいわゆるコラボレーションツール上に保存した同一のファイルを複数の利用者が参照、更新、削除するケースが挙げられる。

また、チャットツールで投稿したメッセージやメッセージに添付するファイルを削除した時に、受信側においても投稿されたメッセージやメッセージに添付されたファイルが削除される場合は、メッセージやメッセージに添付するファイルは一つの場所に保存されている同一の情報と考えられるため、このようなチャットツールの利用も「情報の共有」が想定しているケースとして挙げられる。

その一方で、例えば、電子メールサービスを利用してファイルを送信するケースや、Web 会議サービスで情報を画面に投影するケースは、情報が保存されている場所が異なるため、本条における「情報の共有」が想定しているケースに該当しない。

- **遵守事項 8.1.1(10)(a)「情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となる」について**

外部に公開しているクラウドサービスに情報を保存する場合は、誤って、インターネット上に情報を公開してしまうことが考えられ、その場合、情報漏えいによる影響が大きくなる可能性が高い。そのため、保存する情報がどの範囲の者からアクセス可能かについて、留意が必要である。

例えば、クラウドサービスに情報を保存する時に共有範囲が選択できる場合は、情報の共有を行う必要のある者のみを範囲とする必要がある。また、情報を保存するフォルダごとに共有範囲が設定されている場合は、情報の共有を行う必要のある者のみが共有範囲となっているフォルダに情報を保存する必要がある。

なお、共有範囲の設定の誤り等によって情報の共有を行う必要のない者に対してアクセスを許可したとしても、クラウドサービスに保存する情報自体を暗号化することにより、情報漏えいのリスクを低減することが可能となる。本条で定める規定と併せて、情報の格付、取扱制限等に応じてクラウドサービスに保存する情報自体を暗号化するとよい。

- **遵守事項 8.1.1(10)(b)「クラウドサービス上に保存した要保護情報を速やかに削除する」について**

保存する必要のない情報をクラウドサービス上に放置してしまうと、クラウドサービスが不正アクセス等の被害を受けた場合に、クラウドサービスから情報が漏えいする可能性がある。

削除する方法として、人手による削除は方法の一つとして考えられるが、人手による削除では削除の漏れや削除の遅れが発生する可能性があるため望ましくない。

利用するクラウドサービスが、情報の共有期間や保存期間等、期間の設定が可能であり、設定した期間を超えた場合は自動的に情報を削除する機能を備えている場合は、当該機能を利用するとよい。なお、期間の設定を行うときは、情報の共有に際して必要最小限の期間を設定することが重要である。

8.1.2 ソーシャルメディアによる情報発信

目的・趣旨

機関等においても、積極的な広報活動等を目的としたソーシャルメディアの利用が一般的になっている。しかし、民間事業者等により提供されているソーシャルメディアでは政府ドメイン名を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、機関等のアカウントを乗っ取られた場合や、利用しているソーシャルメディアが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民等に提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

また、このようなソーシャルメディアは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアは、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスであることが考えられ、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことは困難であることが一般的である。このことから、ソーシャルメディアの利用は、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとする。ソーシャルメディアを利用の際は 4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の対策を参照すること。

遵守事項

(1) ソーシャルメディアによる情報発信時の対策

(a) 統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアを利用することを前提として、以下を全て含む情報セキュリティ対策に関する**運用規程を定める**こと。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ア) 機関等のアカウントによる**情報発信**が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

(イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

(b) 職員等は、要安定情報の国民への提供にソーシャルメディアを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

【 基本対策事項 】

＜8.1.2(1)(a)関連＞

8.1.2(1)-1 統括情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を全て含む対策を手順として

定めること。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている機関等のウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示すること。

b) URL 短縮サービスは、利用するソーシャルメディアが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しないこと。

8.1.2(1)-2 統括情報セキュリティ責任者は、機関等のアカウントによる情報発信が実際の機関等のものであると認識できるようにするためのなりすまし対策として、以下を全て含む対策を手順として定めること。

a) 機関等からの情報発信であることを明らかにするために、機関等が政府ドメイン名を用いて管理しているウェブサイト内（政府ドメイン名を登録する資格を持たない機関等においては、機関等のウェブサイト内）において、利用するソーシャルメディア名と、そのソーシャルメディアにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

b) 機関等からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、機関等が運用していることを利用者に明示すること。

c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている機関等のウェブサイト上のページの URL を記載すること。

d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

8.1.2(1)-3 統括情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を全て含む管理手順を定めること。

a) パスワードを適切に管理すること。具体的には、ログインパスワードには強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用した容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

c) ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行うこと。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃

取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

8.1.2(1)-4 統括情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を全て含む対処手順を定めること。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT に報告すること。報告を受けた CSIRT は遵守事項 2.2.4(2)に従い、内閣官房国家サイバー統括室への連絡（独立行政法人及び指定法人においては所管する国の行政機関を経由）を含む適切な対処を行うこと。

（解説）

- **遵守事項 8.1.2(1)(a)「運用規程を定める」について**

運用規程を定めるに当たっては、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準を低下させることがないよう留意が必要である。機関等のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するウェブサイト等へのリンクを掲載することは、当該の投稿やウェブサイト等の内容を信頼性のあるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やウェブサイト等の内容が変更される可能性があることを考慮した上で、慎重に行う必要がある。

なお、ソーシャルメディアの利用は、クラウドサービスの利用に相当することから、4.2「クラウドサービス」の規定及び本条に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

- **遵守事項 8.1.2(1)(a)(ア)「情報発信」について**

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまうため、完全に削除することは不可能となる。このため、当該情報が公開可能な情報であるか否かについて、情報発信する前に十分に確認する必要がある。

- **基本対策事項 8.1.2(1)-3 a)「パスワードを適切に管理する」について**

パスワードの管理については、遵守事項 8.1.1(6)(d)も参照のこと。

- **基本対策事項 8.1.2(1)-3 a)「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用」について**

「（解説）基本対策事項 7.1.1(1)-4「強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること」について」を参照のこと。

- **基本対策事項 8.1.2(1)-3 a)「パスワードを知る担当者を限定」について**

  ソーシャルメディアのアカウントは、複数の担当者で利用することが一般的であり、また、担当者の異動に伴いアカウントの利用者が交代することが想定される。したがって、ログインパスワードの管理に当たっては、担当者の交代があった時点で直ちにパスワードを変更し、権限のない者がパスワードを知る状態が生じないようにすることが求められる。

8.1.3 テレワーク

目的・趣旨

働き方改革実行計画（平成 29 年 3 月 28 日　働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、職員等が業務を遂行する上で、必ずしも勤務官署に出勤する必要はなく、自宅やサテライトオフィス等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模災害時や感染症対策として勤務官署への出勤が抑制されるような状況下では、大半の職員等が勤務官署以外から業務を遂行できるようにテレワーク環境の整備が必要となる。

本款では、テレワークの実施に特に必要な対策についてのみ規定しているため、本款以外に、3.1.1「情報の取扱い」、6.1.2「要管理対策区域外での端末利用時の対策」、6.1.3「機関等支給以外の端末の導入及び利用時の対策」、6.4.1「通信回線」、6.4.2「通信回線装置」、6.4.3「無線 LAN」、7.1.6「監視機能」及び 8.1.1「情報システムの利用」の各款を参照すること。

遵守事項

(1) 運用規程の整備

(a) 統括情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策に係る運用規程を整備すること。なお、<u>原則としてテレワークは機関等が支給する端末で行うよう定めること</u>。

【基本対策事項】

＜8.1.3(1)(a)関連＞

8.1.3(1)-1 統括情報セキュリティ責任者は、以下を例とする項目について、既に機関等において整備されている運用規程に不足があれば、新たに運用規程を整備すること。

a) テレワークの実施申請及び承認並びにテレワークの実施報告
b) テレワークで取り扱うことができる情報の格付
c) テレワークで取り扱う情報の保存場所
d) 要管理対策区域外での要機密情報の取扱手続
e) テレワークに使用する端末に必要な情報セキュリティ対策
f) 機関等が支給する端末の持出手続
g) <u>例外的に機関等支給以外の端末の利用を認める場合</u>
h) 機関等支給以外の端末の利用許可手続及び安全管理措置
i) テレワーク実施可能な場所
j) テレワークに利用可能なネットワーク

（解説）

- **遵守事項 8.1.3(1)(a)「原則としてテレワークは機関等が支給する端末で行うよう定め**

ること」について

機関等支給以外の端末は、機関等が支給する端末と異なり情報セキュリティ水準を一定以上に保ち続けることが困難なため、機関等が支給する端末に比べて情報セキュリティインシデントの引き金となる可能性が高い。従って、原則としてテレワークに使用する端末は、情報セキュリティ水準の機関等によるコントロールが容易な機関等が支給する端末に限ることとし、機関等支給以外の端末の使用は控えるべきである。

- **基本対策事項 8.1.3(1)-1 g)「例外的に機関等支給以外の端末の利用を認める場合」について**

テレワークにおいては、原則として機関等が支給する端末を利用するべきであるが、大規模災害や大規模感染症対策等により勤務官署に出勤することができないが、テレワークに対応した機関等が支給する端末を持ち出していない場合等、機関等が支給する端末を用いてテレワークを行うことができない状態に陥る可能性は捨てきれない。このような場合でも業務を継続させる必要がある場合、例外的に機関等支給以外の端末をテレワークに使用することが考えられる。

機関等支給以外の端末をテレワークに使用する場合は、機関等が支給する端末でテレワークを行うよりも職員等の権限を縮小し、取り扱う情報や利用できる情報システムを制限すべきである。

また、機関等支給以外の端末の情報セキュリティ水準を均一化させるため、USB メモリ起動や光ディスク起動によるシンクライアント又は USB メモリや光ディスクで OS を起動した際のセキュアブラウザの利用も検討するべきである。

なお、私物端末であっても要機密情報を取り扱うのであれば、第三者（家族等の同居する者を含む。）への貸与は禁止すべきであり、それに同意できない職員等には業務において私物端末を利用させるべきではない。

遵守事項

(2) 実施環境における対策

(a) 情報システムセキュリティ責任者は、テレワークの実施により機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保すること。

(b) 情報システムセキュリティ責任者は、**リモートアクセスに対し多要素主体認証を行うこと**。

(c) 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じること。

(d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。

【基本対策事項】

＜8.1.3(2)(a)関連＞

8.1.3(2)-1 情報システムセキュリティ責任者は、**VPN 回線を整備して**リモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 通信を行う端末の識別又は認証
c) 利用者の認証
d) 通信内容の暗号化
e) **主体認証ログ**の取得及び管理
f) リモートアクセスにおいて**利用可能な公衆通信網の制限**
g) アクセス可能な情報システムの制限
h) **リモートアクセス中の他の通信回線との接続禁止**
i) **不正な通信の有無の監視**

＜8.1.3(2)(c)関連＞

8.1.3(2)-2 情報システムセキュリティ責任者は、リモートアクセスする端末が、許可されたものであるかどうかを確認するために、以下を例とする対策を行うこと。

a) 証明書による端末確認
b) ソフトウェア認証による端末確認

＜8.1.3(2)(d)関連＞

8.1.3(2)-3 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定するために、以下を例とする対策を行うこと。

a) 検疫ネットワークの整備
b) IT 資産管理の自動化

（解説）

- **遵守事項 8.1.3⑵(b)「リモートアクセスに対し多要素主体認証を行うこと」について**

  リモートアクセスにおけるアクセスポイントは、インターネットとの接点になるため、外部からの攻撃にさらされる可能性が高い。

  例えば、インターネット VPN 等の公衆回線網である機関等外通信回線を利用する場合は、VPN 回線装置等のアクセスポイントはインターネットとの接点を有することが考えられるため、多要素主体認証方式を用いて主体認証を行う機能を設ける必要がある。また、IP-VPN 等の閉域網をベースとしたインターネットと接点を有していない場合であっても、アクセス元が機関等外通信回線である場合は、機関等の管理外の端末等が接続される可能性があり、なりすましによる不正アクセス等の脅威が考えられるため、多要素主体認証方式を用いて主体認証を行う機能を設ける必要がある。

  なお、侵入を許してしまった場合に備えて、認証を受けた後でも、適宜再認証が必要となるようシステムを構築することが望ましい。

- **基本対策事項 8.1.3⑵-1「VPN 回線を整備して」について**

  VPN 回線には、IP-VPN 等の閉域網をベースとした回線とインターネット VPN 等の公衆回線網をベースとした回線があるが、どちらを整備する場合であっても通信内容の暗号化及びリモートアクセスする端末（又は利用者）の認証は、必ず講じておくべき措置となる。さらに、特に機密性の高い情報を取り扱う場合においては二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行う）などを考慮してもよい。

- **基本対策事項 8.1.3⑵-1 e)「主体認証ログ」について**

  運用中のサーバ装置や通信回線装置の認証ログを定期的に確認するなどして、不正アクセスが行われていないことに留意が必要である。

- **基本対策事項 8.1.3⑵-1 f)「利用可能な公衆通信網の制限」について**

  リモートアクセスの際に使用する通信回線については、適切な情報セキュリティ対策が施されている通信回線サービスに限定することが望ましいが、海外で利用する場合等においては、利用可能な通信回線サービスが限られており、通信回線サービスを制限できない。このような場合は、「通信回線サービスを限定しない」という前提条件の下、通信回線サービスの安全性や信頼性に関わらず、取り扱われる情報のセキュリティが確保されるよう、VPN 接続時の認証処理及び通信内容の暗号化等の対策を考慮する必要がある。

- **基本対策事項 8.1.3⑵-1 h)「リモートアクセス中の他の通信回線との接続禁止」について**

  リモートアクセスする端末が不正プログラムに感染した状態で、VPN 回線への接続中に、例えば直接インターネットに接続する等、VPN 回線以外の通信回線への接続が行われる場合、以下のリスクが考えられる。

  - VPN 回線と VPN 回線以外の通信回線がいわゆるブリッジ構成となり、VPN 回

線で行う通信が VPN 回線以外の通信回線に流れてしまうことによる、情報漏えい。

- プロキシサーバ等が C&C サーバ等への不正な通信を監視及び遮断が行えないことによる、リモートアクセスする端末を踏み台としたリモートアクセス先への不正アクセス。

そのため、VPN 回線への接続とインターネット等の VPN 回線以外の通信回線へ同時に接続を行う設定をリモートアクセスする端末において許可しない等によって、VPN 回線を用いたリモートアクセス中は VPN 回線以外の通信回線との接続を禁止する必要がある。

- **基本対策事項 8.1.3(2)-1 i)「不正な通信の有無の監視」について**

遵守事項 6.4.1(2)(b)を参照のこと。

遵守事項

(3) 実施時における対策

(a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等が確認するべき項目を定め、職員等に当該項目を確認させること。

(b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。

(c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。

【基本対策事項】

＜8.1.3(3)(b)関連＞

8.1.3(3)-1 職員等は、基本対策事項 6.1.1(1)-3 に示した対策のほか、以下の項目を例とする画面ののぞき見や盗聴から発生する情報漏えい対策を講ずること。

a) 背後に人が立たないよう背後に通路がない場所で壁を背にする位置に座りテレワークを行うこと。

b) Web 会議等、音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

c) 同居する者に対し知り得た情報を他人に漏らさないよう協力を求めること。

＜8.1.3(3)(c)関連＞

8.1.3(3)-2 職員等は、テレワークに情報セキュリティ対策の状況が不明又は不十分な機関等外通信回線を利用しないために、以下を例とする対策を行うこと。

a) 公衆無線 LAN を利用しないこと。

b) 宿泊施設等が提供する無料ネットワークを利用しないこと。

（解説）

- **遵守事項 8.1.3(3)(a)「テレワーク実施前及び実施後に職員等が確認するべき項目」について**

実施前に行う確認としては、

① 資産管理として、「持ち出した機器は全てそろっているか」

② 脆弱性対策として、「OS やアプリケーション等のソフトウェアが最新の状態に保たれているか」、「サポート切れのソフトウェアを利用していないか」、「自宅のネットワークルータは最新のファームウェアに更新されているか」

③ 情報漏えい対策として、「のぞき見防止フィルタが装着されているか」、「背後にのぞき見可能なスペースがないか」、「スクリーンロックは設定されているか」、「VPN 接続や https 接続（Web ベースで業務を行う場合）等により通信は暗号化されているか」、「自宅の無線ネットワークルータにより無線 LAN 通信を行う場合は WPA3 あるいは WPA2 方式を用いた暗号化通信となっているか、また、

暗号化パスワードは第三者に推測されにくいものか」

④ 不正プログラム対策として、「不正プログラム対策ソフトウェアのパターンファイルが最新の状態になっているか」、「不正プログラム対策ソフトウェアがリアルタイム検査を行うように設定されているか」

⑤ インシデント対策として、「インシデント発生時の初期対応方法を把握しているか」、「インシデント発生時の連絡先（電話番号含む。）を把握しているか」

等が考えられる。

中小企業担当者向けではあるが、総務省においてチェックリストを公表しているので参考にするとよい。

参考：「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第３版）」
（https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/）

実施後に行う確認としては、

① 不正プログラム対策として、「不正プログラム対策ソフトウェアを用いた検査を行い不正プログラムに感染していないことを確認したか」

② 資産管理として、「持ち出した機器は全てそろっているか」

③ 情報漏えい対策として、「端末に保存した情報が暗号化されているか（シンクライアントを利用している場合や、内蔵ディスク全体を暗号化している場合は除く。）」

④ どのファイルにアクセスしたか。（記録することが望ましい。）

⑤ 情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去したか。

等が考えられる。

日本ネットワークセキュリティ協会（JNSA）において、チェックリストを公表しているので参考にするとよい。

参考：日本ネットワークセキュリティ協会（JNSA）「緊急事態宣言解除後のセキュリティ・チェックリスト」
（https://www.jnsa.org/telework_support/telework_security/index.html）

- **基本対策事項 8.1.3(3)-1 c)「同居する者に対し知り得た情報を他人に漏らさないよう協力を求める」について**

自宅でテレワークを行う場合、同居する者に取り扱う情報を知られないように対策を講ずることが前提であるが、同居する者に取り扱う情報を全く知られないように業務を行うことは困難な場合がある。従って、同居する者に情報が漏れる可能性を考慮し、例えば、SNS へのアップロードをしないこと、知人との会話で話題にしないことなど、知り得た情報を他人に漏らさないよう協力を要請すべきである。

- **基本対策事項 8.1.3(3)-2「情報セキュリティ対策の状況が不明又は不十分な機関等外通**

信回線を利用しない」について

公衆無線 LAN サービスのうち無線経路の秘匿性や安全性が不明なものや接続経路の管理状況が不明な無料のインターネット接続サービス等は、通信内容の盗聴やなりすましによる情報の窃取等のおそれがあり、このような情報セキュリティ水準が不明な通信回線は原則として業務に利用すべきではない。また、宿泊施設等が当該施設の利用者に無料で開放している LAN（有線・無線を問わない。）も同様である。

当該回線を使用しなければならない場合は、VPN 接続やセキュアブラウザの利用など通信内容の暗号化等の対策を考慮する必要がある。

なお、無線 LAN の利用については、総務省が公表している以下のガイドラインを参考にするとよい。

参考：総務省「公衆 Wi-Fi 利用者向け 簡易マニュアル」
（https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）

付録

(1) 情報セキュリティ対策に関連する関連文書等

(a) 統一基準群

- 政府機関等のサイバーセキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定）
- 政府機関等のサイバーセキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定）
- 政府機関等の対策基準策定のためのガイドライン（内閣官房国家サイバー統括室決定）

(b) 統一基準関連文書

「統一基準関連文書」は、遵守事項又は基本対策事項を満たすために遵守又は参照すべき文書

第２部

- 大規模サイバー攻撃事態等への初動対処について（平成 22 年３月 19 日　内閣危機管理監決裁）　遵守事項 2.2.4(3)(b)

第４部

- 政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について（令和２年６月 30 日　サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定）　基本対策事項 4.2.1(1)-2 及び遵守事項 4.2.1(2)(c)
- 調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ（令和４年 12 月 12 日関係省庁申合せ　内閣官房国家サイバー統括室）　遵守事項 4.2.3(2)(a)
- IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ（平成 30 年 12 月 10 日関係省庁申合せ　内閣官房国家サイバー統括室）　遵守事項 4.1.1(1)(a)(イ)、遵守事項 4.2.1(2)(c)、遵守事項 4.2.3(2)(a)、基本対策事項 4.3.1(1)-1 b)及び遵守事項 4.3.1(1)(a)

第５部

- IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ（平成 30 年 12 月 10 日関係省庁申合せ　内閣官房国家サイバー統括室）　遵守事項 5.1.1(1)(a)
- 安全保障等の機微な情報等に係る政府情報システムの取扱い（令和５年７月 19 日　デジタル社会推進会議幹事会決定）　遵守事項 5.2.1(3)(a)
- IT 製品の調達におけるセキュリティ要件リスト（令和８年２月６日　経済産業省）　遵守事項 5.2.1(3)(c)

第６部

- TLS 暗号設定ガイドライン（CRYPTREC GL-3001-3.1.1）（2025 年４月 25 日

CRYPTREC）　基本対策事項 6.2.3(1)-5 c)

- IT 製品の調達におけるセキュリティ要件リスト（令和８年２月６日　経済産業省）　基本対策事項 6.3.1(1)-1

第７部

- 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）（CRYPTREC LS-0001-2022R2）（令和８年３月 30 日　CRYPTREC）　遵守事項 7.1.5(1)(b)
- 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（CRYPTREC LS-0003-2022R1）（令和４年３月　CRYPTREC）　遵守事項 7.1.5(1)(b)

(c) 統一基準適用個別マニュアル群

「統一基準適用個別マニュアル群」は、機関等において具体的な運用規程や実施手順を定める際の参考資料や個別の情報システムのセキュリティ要件等を検討する時等に利用される資料

第２部

- 対策推進計画策定マニュアル（令和７年７月１日　内閣官房国家サイバー統括室）　遵守事項 2.1.3(4)(a)
- 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書（令和７年７月　内閣官房国家サイバー統括室）　遵守事項 2.3.2(1)(a)

第４部

- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊. クラウド設計・開発編（2025 年７月１日　内閣官房国家サイバー統括室）　遵守事項 4.2.2(3)(a)
- 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（2025 年７月１日　内閣官房国家サイバー統括室）　遵守事項 4.1.1(2)、(3)及び 4.3.1(1)

第５部

- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2025 年７月１日　内閣官房国家サイバー統括室）　基本対策事項 5.2.1(3)-1
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊. クラウド設計・開発編（2025 年７月１日　内閣官房国家サイバー統括室）　基本対策事項 5.2.2(1)-1 c)
- 政府機関等における情報システム運用継続計画ガイドライン（令和７年７月　内閣官房国家サイバー統括室）　遵守事項 5.3.1(1)

第６部

- スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書（2025 年７月１日　内閣官房国家サイバー統括室）　6.1.2 款及び 6.1.3 款

(2) 情報セキュリティに関連する法律

〔法律〕

- サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- 行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）
- 独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号）
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 公文書等の管理に関する法律（平成 21 年法律第 66 号）

注）詳細については、原文を参照すること。

(3) 統一基準群で整備を求めている運用規程及び実施手順等

(a) 運用規程

最高情報セキュリティ責任者

- 情報セキュリティ対策推進体制の役割に関する運用規程(基本対策事項 2.1.1(6)-1)
- CSIRT の役割に関する運用規程（基本対策事項 2.1.1(7)-1）

統括情報セキュリティ責任者

- 情報セキュリティ対策における雇用の開始、終了及び人事異動時等の管理に関する運用規程（遵守事項 2.1.3(3)(b)）
- 情報の取扱いに関する運用規程（遵守事項 3.1.1(1)(a)）
- 要管理対策区域の対策の基準（遵守事項 3.2.1(1)(b)）
- 業務委託に係る運用規程（遵守事項 4.1.1(1)(a)）
- クラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程（遵守事項 4.2.1(1)(a)）
- クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針に係る運用規程（遵守事項 4.2.2(1)(a)）
- クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針に係る運用規程（遵守事項 4.2.2(1)(b)）
- クラウドサービスの利用を終了する際のセキュリティ対策の基本方針に係る運用規程（遵守事項 4.2.2(1)(c)）
- クラウドサービス（要機密情報を取り扱わない場合）の利用に関する運用規程（遵守事項 4.2.3(1)(a)）
- 機器等の調達に関する選定基準（遵守事項 4.3.1(1)(a)）
- 高度な情報セキュリティ対策が要求される情報システムを判別するための情報システムの分類基準に係る運用規程（遵守事項 5.1.1(1)(a)）
- 情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項に係る運用規程（遵守事項 5.1.1(2)(a)）
- 危機的事象発生時における情報セキュリティに係る運用規程（遵守事項

5.3.1(1)(a))
- 要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）についての技術的な措置に関する運用規程（遵守事項 6.1.2(1)(b)）
- 要管理対策区域外において機関等外通信回線に接続した機関等が支給する物理的な端末を機関等内通信回線に接続する際の技術的な措置に関する運用規程（遵守事項 6.1.2(1)(c)）
- 要機密情報を取り扱う機関等支給以外の端末の安全管理措置に関する運用規程（遵守事項 6.1.3(2)(c)）
- 要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を機関等内通信回線に接続する際の安全管理措置に関する運用規程（遵守事項 6.1.3(2)(d)）
- アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための運用規程（遵守事項 6.6.1(1)(a)）
- ソーシャルメディアによる情報発信時における情報セキュリティ対策に関する運用規程（遵守事項 8.1.2(1)(a)）
- テレワーク実施時の情報セキュリティ対策に係る運用規程（遵守事項 8.1.3(1)(a)）

政府共通利用型システム利用管理者
- 政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程（遵守事項 5.4.2(3)(a)）

(b) 実施手順

最高情報セキュリティ責任者
- 例外措置の適用の申請を審査する者及び審査手続に関する実施手順（基本対策事項 2.2.2(1)-1）

統括情報セキュリティ責任者
- 情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機関等関係者への報告手順（遵守事項 2.2.4(1)(a)）
- 情報セキュリティインシデントの可能性を認知した際の機関等外との情報共有を含む対処手順（遵守事項 2.2.4(1)(b)）
- 機器等の納入時の確認・検査手続（遵守事項 4.3.1(1)(b)）
- 危機的事象発生時における情報セキュリティに係る実施手順（遵守事項 5.3.1(1)(a)）
- 機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順及び許可手続（遵守事項 6.1.2(1)(a)）
- 機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続（遵守事項 6.1.3(2)(a)）
- 機関等支給以外の端末を用いて要保護情報を取り扱う場合の利用手順及び許可

手続（遵守事項 6.1.3(2)(b)）
- 要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を機関等内通信回線に接続する際の許可手続（遵守事項 6.1.3(2)(d)）
- 機関等の情報システムの利用のうち、情報セキュリティに関する実施手順（遵守事項 8.1.1(1)(a)）
- USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順（遵守事項 8.1.1(1)(b)）
- 機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続（遵守事項 8.1.1(1)(c)）

情報セキュリティ責任者
- 職員等ごとの自己点検票及び自己点検の実施手順（遵守事項 2.3.1(1)(b)）

情報システムセキュリティ責任者
- 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順（遵守事項 5.2.2(1)(e)(ア)）
- 情報セキュリティインシデントを認知した際の対処手順（遵守事項 5.2.2(1)(e)(イ)）
- 情報システムが停止した際の復旧手順（遵守事項 5.2.2(1)(e)(ウ)）
- 情報システムにおける監視手順（基本対策事項 5.2.3(1)-1、基本対策事項 7.1.6(1)-3）
- 通信回線装置が動作するために必要なソフトウェアに関する実施手順（遵守事項 6.4.2(1)(b)）
- 無線 LAN 回線利用申請手続、無線 LAN 機器の管理手順（基本対策事項 6.4.3(1)-1）
- 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順（遵守事項 6.5.1(1)(b)(ア)）
- 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順（遵守事項 6.5.1(1)(b)(イ)）
- 共用識別コードの取扱いに関する実施手順（基本対策事項 7.1.1(2)-6）
- 情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれを利用した安全なプロトコルの運用方法（遵守事項 7.1.5(1)(b)）
- リモートアクセス環境に VPN 回線を用いて接続する際の利用開始及び利用停止時の申請手続（基本対策事項 8.1.3(2)-1）

政府共通利用型システム利用管理者
- 政府共通利用型システムの利用に関する情報セキュリティ対策に係る実施手順（遵守事項 5.4.2(3)(a)）

クラウドサービス管理者
- クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順（遵守事項 4.2.2(3)(c)(ア)）
- クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順（遵守事項 4.2.2(3)(c)(イ)）
- 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順（遵守

事項 4.2.2(3)(c)(ウ))

区域情報セキュリティ責任者

- 管理区域の利用手順（基本対策事項 3.2.1(3)-1）

(c) その他

政府共通利用型システム管理機関の情報システムセキュリティ責任者

- 政府共通利用型システムに関する運用管理規程（遵守事項 5.4.1(1)(a)）

(4) 本ガイドラインにおいて「基本セキュリティ対策」「追加セキュリティ対策」として区分した基本対策事項

<table>
<tr><th rowspan="2"></th><th colspan="2">基本対策事項</th></tr>
<tr><th>基本セキュリティ対策</th><th>追加セキュリティ対策</th></tr>
<tr><td rowspan="2">6.4.3 無線 LAN</td><td colspan="2">6.4.3(1)-1 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、情報システムの分類に基づき、以下の対策を講ずること。</td></tr>
<tr><td>以下を全て含む対策を講ずること。
a) 無線 LAN 通信の暗号化
b) 無線 LAN 回線利用申請手続の整備
c) 無線 LAN 機器の管理手順の整備
d) 来訪者等に提供する無線 LAN によるインターネット接続回線と業務で使用する機関等 LAN システムの分離</td><td>基本セキュリティ対策の実施に加えて、以下を例とする対策を講ずること。
e) IEEE 802.1X による無線 LAN へのアクセス主体の認証</td></tr>
<tr><td rowspan="2">6.6.1 アプリケーション・コンテンツの作成・運用時の対策</td><td colspan="2">6.6.1(3)-2 情報システムセキュリティ責任者は、ウェブアプリケーションを運用段階へ移行する前に情報システムの分類に基づき、以下の対策を実施すること。</td></tr>
<tr><td>開発したウェブアプリケーションに対して脆弱性診断の実施を検討すること。</td><td>高度な情報セキュリティ対策が要求される情報システムで実行するウェブアプリケーションに対して、脆弱性診断を実施すること。</td></tr>
</table>

	基本対策事項	
	基本セキュリティ対策	追加セキュリティ対策
7.1.2 アクセス制御機能	7.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、情報システムの分類に基づき、以下の対策を実施すること。	
	以下を例とするアクセス制御機能の要件を定めること。 a) 利用時間や利用時間帯によるアクセス制御 b) 同一主体による複数アクセスの制限 c) IP アドレスによる端末の制限 d) ネットワークセグメントの分割によるアクセス制御 e) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御	基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討すること。 f) 認証・認可の統合管理基盤を用いたアクセス制御 g) アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御
7.1.4 ログの取得・管理	7.1.4(1)-4 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、情報システムの分類に応じて以下の対策を実施すること。	
	以下を例とする当該作業を支援する機能を導入すること。 a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化機能	基本セキュリティ対策の実施に加えて、以下を例とする当該作業を支援する機能の導入を検討すること。 b) リアルタイムでのログの調査・分析を行うための機能
7.1.6 監視機能	－	7.1.6(1)-4 情報システムセキュリティ責任者は、情報システム運用時の監視において、SOC や NOC 等のセキュリティ監視を専門の外部事業者に業務委託することを検討すること。

	基本対策事項	
	基本セキュリティ対策	追加セキュリティ対策
7.2.1 ソフトウェアに関する脆弱性対策	7.2.1(1)-1 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に以下の対策を実施すること。	
	インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、その他のサーバ装置、端末及び通信回線装置については、情報システムの分類や保有する情報、システム特性等を踏まえ、脆弱性診断の実施を検討すること。	サーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、脆弱性診断の実施に当たっては、ペネトレーションテスト、TLPT 等の高度な脆弱性診断の実施を検討すること。
	―	7.2.1(1)-6 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の運用時に、定期的な脆弱性診断（ペネトレーションテスト、TLPT 等の高度な脆弱性診断を含む）の実施を検討すること。
7.2.2 不正プログラム対策	―	7.2.2(1)-7 情報システムセキュリティ責任者は、EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染した装置を早期にネットワークから切り離す機能の導入を検討すること。

	基本対策事項	
	基本セキュリティ対策	追加セキュリティ対策
7.2.3 サービス不能攻撃対策	7.2.3(1)-2 情報システムセキュリティ責任者は、以下を例とするサービス不能攻撃への対策を実施すること。	
	以下を例とする対策を実施すること。 a) サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入 b) サーバ装置、端末及び通信回線装置及び通信回線の冗長化	基本セキュリティ対策に加え、以下を例とする対策を検討すること。 c) インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 d) コンテンツデリバリーネットワーク（CDN）サービスの利用
	－	7.2.3(1)-9 情報システムセキュリティ責任者は、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合は、必要に応じて、CSIRT 等の関係者に通知すること。
7.2.4 標的型攻撃対策	－	7.2.4(1)-5 情報システムセキュリティ責任者は、以下を例とする内部対策及び出口対策を行うこと。 a) プロキシサーバ等により、C&C サーバ等への不正な通信を監視し、遮断する。 b) 情報システムの管理者が利用する情報システム管理用の専用端末を用意し、他のセグメントと分離した運用管理セグメントを構築し、当該セグメントにシステム管理用の専用端末を接続する。 c) 認証サーバに管理者権限でログインできる端末をシステム管理用の専用端末に制限する。 d) 一般利用者が利用する端末間でのファイル共有機能を停止する又は一般利用者が利用する端末間の直接通信を遮断する。