政府機関等の対策基準策定のためのガイドライン
（令和７年度版）

令和７年７月１日

令和８年６月 12 日 一部改定

内閣官房 国家サイバー統括室

改定履歴

以下に、「政府機関等の対策基準策定のためのガイドライン（令和７年度版）」の改定履歴を記載する。

改定年月日	改定内容
令和７年７月１日	初版発行
令和７年９月５日	一部改定
令和８年６月 12 日	一部改定

目次

第1部 総則

1.1 本ガイドラインの目的等

(1) 本ガイドラインの目的

政府機関等の対策基準策定のためのガイドライン（以下「本ガイドライン」という。）は、国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）が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。以下「統一基準」という。）の規定を遵守するための対策基準を策定する際に参照するものであり、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、対策基準の策定及び実施に際しての考え方等を解説するものである。これにより、機関等が、本ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて対策基準を定められるようにすることを目的とする。

(2) 本ガイドラインの適用対象

本ガイドラインの適用対象は、統一基準の「1.1(2) 本統一基準の適用対象」に定めるものとする。

> 参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）
> (2) 本統一基準の適用対象
> (a) 本統一基準において適用対象とする者は、全ての職員等とする。
> (b) 本統一基準において適用対象とする情報は、以下の情報とする。
> (ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）
> (イ) その他のシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）であって、職員等が職務上取り扱う情報
> (ウ) (ア)及び(イ)のほか、機関等が調達し、又は開発したシステムの設計又は運用管理に関する情報
> (c) 本統一基準において適用対象とする情報システムは、本統一基準の適用対象となる情報を取り扱う全ての情報システムとする。

(3) 本ガイドラインの改定

情報セキュリティの水準を適切に維持・向上させていくためには、脅威の変化や技術の進展を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、本ガイドラインの規定内容については、環境の変化に応じて適宜内容の見直

しを行い、必要に応じて項目の追加やその内容の充実等を図ることによって、規定内容の適正性を将来にわたり維持することとする。

機関等においては、本ガイドラインが更新された場合には、その内容をそれぞれの対策基準に適切に反映させることが期待される。

なお、本ガイドラインは、国の行政機関と協議の上、内閣官房国家サイバー統括室において決定する。

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、本ガイドラインのほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本ガイドラインでは、あえて関連法令等の遵守について明記していない。また、情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。

(5) 対策基準の策定手順

機関等は、基本方針に基づき、統一基準に定める遵守事項等の規定を満たすよう、具体的な対策基準を策定する必要がある。

本ガイドラインに規定される基本対策事項は、遵守事項を満たすためにとるべき基本的な対策事項の例示であり、遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講ずる必要がある。

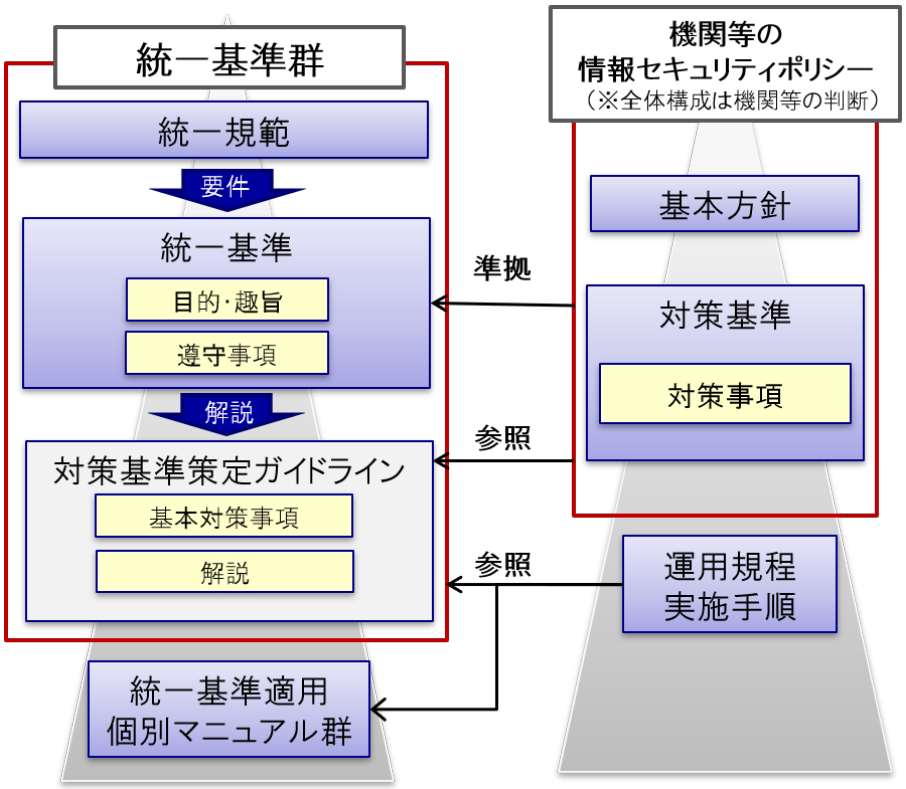
したがって、本ガイドラインにおいて遵守事項に対応する基本対策事項が規定されている場合は、具体的な対策事項を対策基準に定める必要がある。ただし、機関等の規模、情報システムの構成、取り扱う情報の内容・用途等の特性によって、達成すべき情報セキュリティの水準やとるべき具体的な対策は異なり得ることから、基本対策事項に記載された対策とは別の対策により、基本対策事項と同等以上の情報セキュリティ水準が確保できると判断される場合は、当該対策事項を対策基準に定めてよい。

なお、対策基準の構成としては、統一基準と本ガイドラインと同様に、遵守事項と対策事項を分けて記載する方法や、対策事項のみを記載する方法などが考えられるが、機関等の状況に応じてよりよい構成とすることが望ましい。

(6) 統一基準群と機関等の情報セキュリティポリシーの関係

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。以下「統一規範」という。）及び統一基準と本ガイドラインの関係は図 1.1-1 のとおりであり、これらを総称して、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（以下「統一基準群」という。）と呼ぶ。また、統一基準群と機関等の情報セキュリティポリシーの関係についても、併せて図 1.1-1 に示す。

図 1.1-1 統一基準群と機関等の情報セキュリティポリシーの関係について



1.2 情報の格付の区分・取扱制限

統一基準 1.2 において定義されている情報の格付の区分・取扱制限を以下に再度掲載する。

(1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、本統一基準の遵守事項で用いる格付の区分の定義を示す。

なお、機関等において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本統一基準の遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。また、他機関等へ情報を提供する場合は、自組織の対策基準における格付区分と本統一基準における格付区分の対応について、適切に伝達する必要がある。

機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性２情報	国の行政機関における業務で取り扱う情報のうち、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。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、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。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情

	報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 　別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

格付の区分	分類の基準
完全性２情報	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

(2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを職員等に確実に行わせるための手段をいう。

職員等は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。機関等は、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある。

【参考１】 統一基準の適用対象とする情報について

統一基準において、適用対象とする情報は次のように規定されている。

参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）

(b) 本統一基準において適用対象とする情報は、以下の情報とする。

(ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）

(イ) その他のシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）であって、職員等が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、機関等が調達し、又は開発したシステムの設計又は運用管理に関する情報

(イ)の「その他のシステム」とは、「職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム」<u>以外</u>のシステムを示しており、例えば、私物端末や民間事業者等の他の組織が運用するシステム、ソーシャルメディアなどが広く含まれる。

【参考２】 機密性３情報について

文書管理ガイドラインにおいて、秘密文書は次のように規定されている。

参考：文書管理ガイドラインの「第 10 秘密文書等の管理」（抄）

2 特定秘密又は重要経済安保情報以外の公表しないこととされている情報が記録された行政文書のうち秘密保全を要する行政文書（特定秘密である情報又は重要経済安保情報を記録する行政文書を除く。以下「秘密文書」という。）の管理

(1) 秘密文書は、次の種類に区分し、指定する。

極秘文書 秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書

秘文書 極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書

前述のとおり、本統一基準における機密性３情報に係る記載は「文書管理ガイドラインに定める秘密文書としての取扱いを要する情報」（「秘密文書」は、「文書管理ガイドライン」において、特定秘密又は重要経済安保情報以外の公表しないこととされている情報が記録された行政文書のうち秘密保全を要する行政文書（特定秘密である情報又は重要経済安保情報を記録する行政文書を除く。）と定義されている。）を前提としているため、機関等が独自に格付の定義を変更又は追加する場合は、本統一基準における格付との差異について把握し、対策基準に適切に反映することが求められる。

なお、機密性３情報の取扱いに係る本統一基準の遵守事項には、独立行政法人及び指定法人における職員等を対象とした規定が存在するが、これは独立行政法人及び指定法人

の職員等が文書管理ガイドラインの対象外であることから必要な規定を特に追加したものである。国の行政機関の職員等による秘密文書の管理においては、もとより文書管理ガイドラインの規定が優先的に適用されるため統一基準上に規定はないが、実質的に独立行政法人及び指定法人の職員等と同等の対策が求められている。

【参考３】 機密性２情報について

情報公開法及び独法等情報公開法における不開示情報の類型は次のとおり示されている。

参考：不開示情報の類型

1) 個人に関する情報で特定の個人を識別できるもの等。ただし、法令の規定又は慣行により公にされている情報、公務員や独立行政法人等の役職員等の職に関する情報等は除く。
2) 法人等に関する情報で、公にすると、法人等の正当な利益を害するおそれがあるもの、非公開条件付の任意提供情報であって、通例公にしないこととされているもの等
3) 公にすると、国の安全が害されるおそれ、他国との信頼関係が損なわれる等のおそれがあると行政機関の長が認めることにつき相当の理由がある行政文書に記録されている情報
4) 公にすると、犯罪の予防、捜査等の公共の安全と秩序の維持に支障を及ぼすおそれがあると行政機関の長が認めることにつき相当の理由がある行政文書に記録されている情報
5) 国の機関、独立行政法人等及び地方公共団体の内部又は相互の審議、検討等に関する情報で、公にすると、率直な意見の交換が不当に損なわれる等のおそれがあるもの
6) 国の機関、独立行政法人等又は地方公共団体等が行う事務又は事業に関する情報で、公にすると、その適正な遂行に支障を及ぼすおそれがあるもの

参考：総務省「情報公開法制の概要」
（https://www.soumu.go.jp/main_sosiki/gyoukan/kanri/jyohokokai/gaiyo.html）

【参考４】 取扱制限の例

取扱制限は、情報の機密性、完全性、可用性等の内容に応じた情報の取扱方法を具体的に指定するものであるから、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たすために適切に明示等する必要がある。以下の例のように、代表的な取扱制限を指定してもよい。例えば「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」等と記載しても目的を果たせると考えられる。

機密性についての取扱制限の定義の例

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配布について	配布禁止、配布要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可

取扱制限の種類	指定方法
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

上記の指定方法の意味は以下のとおり。

「○○禁止」

当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。

「○○要許可」

当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。

「暗号化必須」

当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。

「○○限り」

当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「○○課内限り」「○○会議出席者限り」等、参照を許可する者が分かるように指定する。

「○月○日まで○○禁止」

○月○日まで複製を禁止したい場合、「○月○日まで複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

例えば、上記の「○○要許可」は、「○○する行為を禁止するが、許可を得ることにより○○することができる」という意味を持たせている。取扱制限は、このように、職員等にとって簡便かつ分かりやすい表現を採用することが望ましい。

完全性についての取扱制限の定義の例

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

情報の保存期間の指定の方法は、以下のとおり。

保存の期日である「年月日」又は期日に「まで保存」を付して指定する。

例）令和〇〇年７月 31 日まで保存

例）令和〇〇年度末まで保存

完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。

例）年度内保存文書用共有ファイルサーバに保存

例）３か年保存文書用共有ファイルサーバに保存

可用性についての取扱制限の定義の例

取扱制限の種類	指定方法
復旧までに許容できる時間について	〇〇以内復旧
保存場所について	〇〇において保存

復旧許容時間の指定の方法は以下のとおり。

復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。

例）１時間以内復旧

例）３日以内復旧

可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、端末のファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。

例）課室共有ファイルサーバ保存必須

例）各自 PC 保存可

1.3　統一基準における用語定義

統一基準 1.3「用語定義」において定義されている用語を以下に再度掲載する。

【あ】

● 「アプリケーション・コンテンツ」とは、機関等が開発し提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。

● 「運用規程」とは、対策基準に定められた対策内容を個別の情報システムや業務において運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。

【か】

● 「機関等」とは、国の行政機関、独立行政法人及び指定法人をいう。

● 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。

● 「機関等内通信回線」とは、一つの機関等又は政府共通利用型システム管理機関が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該機関等の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。機関等内通信回線には、専用線や VPN 等物理的な回線を機関等が管理していないものも含まれる。

● 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部電磁的記録媒体等の総称をいう。（参考：図 1.3-1）

● 「業務委託」とは、機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において機関等の情報を取り扱わせる場合に限る。

● 「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。

● 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。

参考：「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」（抄）
- IaaS（Infrastructure as a Service）
  利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。
- PaaS（Platform as a Service）
  IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。
- SaaS（Software as a Service）
  利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。

● 「クラウドサービス管理者」とは、クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う機関等の職員等をいう。

● 「クラウドサービス提供者」とは、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。

● 「クラウドサービス利用者」とは、クラウドサービスを利用する機関等の職員等又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。

【さ】

● 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。また、物理的なハードウェアを有するサーバ装置を「物理的なサーバ装置」という。

● 「CYMAT（サイマット）」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情

報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房国家サイバー統括室に設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。

● 「CSIRT（シーサート）」とは、機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。

● 「GSOC（ジーソック）」とは、24 時間 365 日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房国家サイバー統括室に設置される体制をいう。Government Security Operation Coordination Team（政府機関情報セキュリティ横断監視・即応調整チーム）の略。なお、GSOC には、政府機関を対象とした「第一 GSOC」と独立行政法人及び指定法人を対象とした「第二 GSOC」がある。

● 「実施手順」とは、対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順や手続をいう。

● 「情報」とは、統一基準の「1.1(2) 本統一基準の適用対象」の(b)に定めるものをいう。（参考：図 1.3-2）

参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）

(b) 本統一基準において適用対象とする情報は、以下の情報とする。

(ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）

(イ) その他のシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）であって、職員等が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、機関等が調達し、又は開発したシステムの設計又は運用管理に関する情報

● 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機関等が調達又は開発するもの（管理を外部委託しているシステムや政府共通利用型システムを含む。）をいう。（参考：図 1.3-1）

参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）

(c) 本統一基準において適用対象とする情報システムは、本統一基準の適用対象となる情報を取り扱う全ての情報システムとする。

● 「情報セキュリティインシデント」とは、JIS Q 27000:2019 における情報セキュリティインシデントをいう。

> 参考：JIS Q 27000:2019（抄）
> ・ 情報セキュリティインシデント
> 望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
> ・ 情報セキュリティ事象
> 情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

● 「情報セキュリティ関係規程」とは、対策基準、運用規程及び実施手順を総称したものをいう。

● 「情報セキュリティ対策推進体制」とは、機関等の情報セキュリティ対策の推進に係る事務を遂行するため、当該機関等に設置された体制をいう。

● 「職員等」とは、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の管理対象である情報及び情報システムを取り扱う者をいう。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

● 「政府共通利用型システム」とは、他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、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及び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をいう。なお、政府共通利用型システムを構築・運用する機関等を「政府共通利用型システム管理機関」といい、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・運用する機関等及び政府共通利用型システムが提供する機器等を利用する機関等を「政府共通利用型システム利用機関」という。

● 「政府ドメイン名」とは、.go.jp で終わるドメイン名のことをいう。日本国の政府機関、独立行政法人、特殊法人（特殊会社を除く。）が登録（取得）することができる。

【た】

● 「対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。

● 「対策推進計画」とは、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。

● 「端末」とは、情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機関等が調達又は開発するもの以外を指す「機関等支給以外の端末」がある。また、機関等が調達又は開発した端末と機関等支給以外の端末の双方を合わせて「端末（支給外端末を含む。）」という。さらに、物理的なハードウェアを有する端末を「物理的な端末」という。

● 「通信回線」とは、複数の情報システム又は機器等（機関等が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機関等の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機関等が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

● 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。

● 「特定用途機器」とは、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特有の構成要素であって、通信回線に接続する機能を備えている又は内蔵電磁的記録媒体を備えているものをいう。

【は】

● 「本部監査」とは、サイバーセキュリティ基本法第 26 条第１項第２号に基づきサイバーセキュリティ戦略本部が実施する監査をいう。

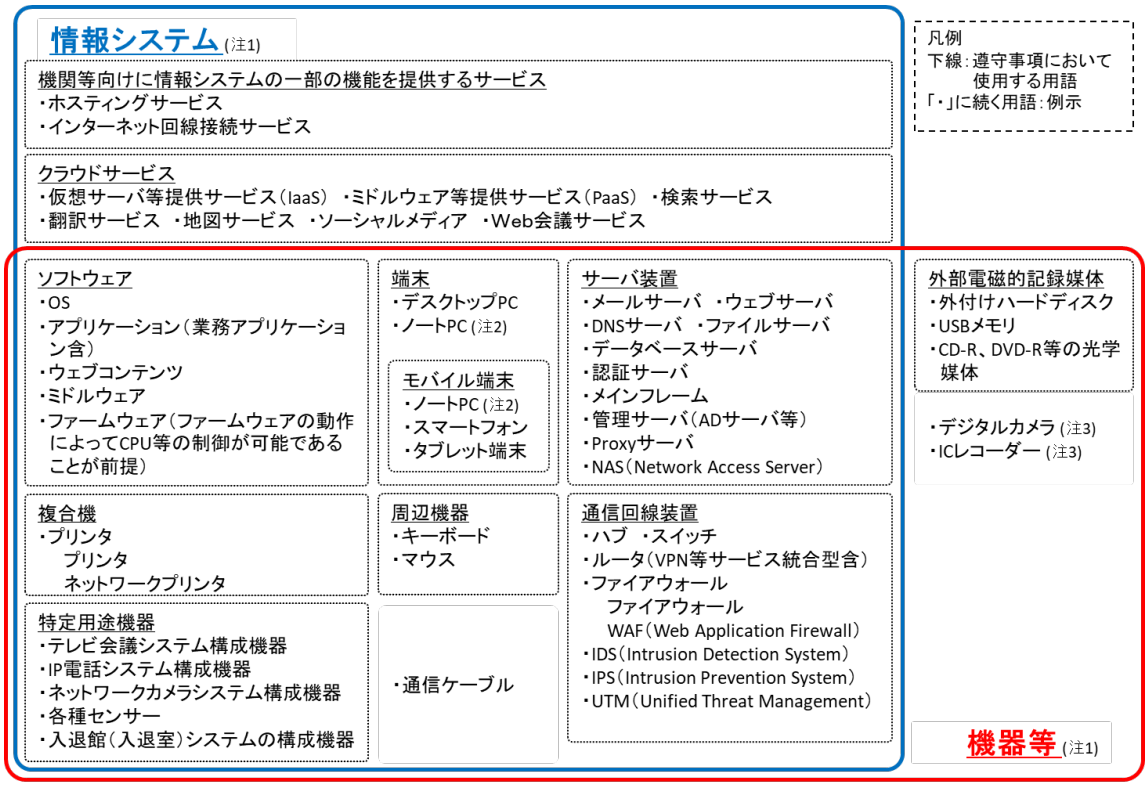
【ま】

● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

【や】

● 「要管理対策区域」とは、機関等の管理下にある区域（機関等が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設

及び執務環境に係る対策が必要な区域をいう。



注1）「機器等」の定義には、情報システムの個々の構成要素は含まれているが、情報システム自体は含まれていない。
注2）いわゆるノートPCのうち、業務上の必要に応じて移動させて使用することを目的としたものはモバイル端末に分類される。利用場所が決まっているものはモバイル端末に含まれないことに注意。
注3）ICレコーダーやデジタルカメラ等の機器は、使用形態によって特定用途機器や外部電磁的記録媒体等の特性を備えることから、使用形態に基づく特性を踏まえ、関連する遵守事項及び基本対策事項を参照の上、適切な対策を講ずることが必要。

図 1.3-1　「情報システム」、「機器等」及びその関係

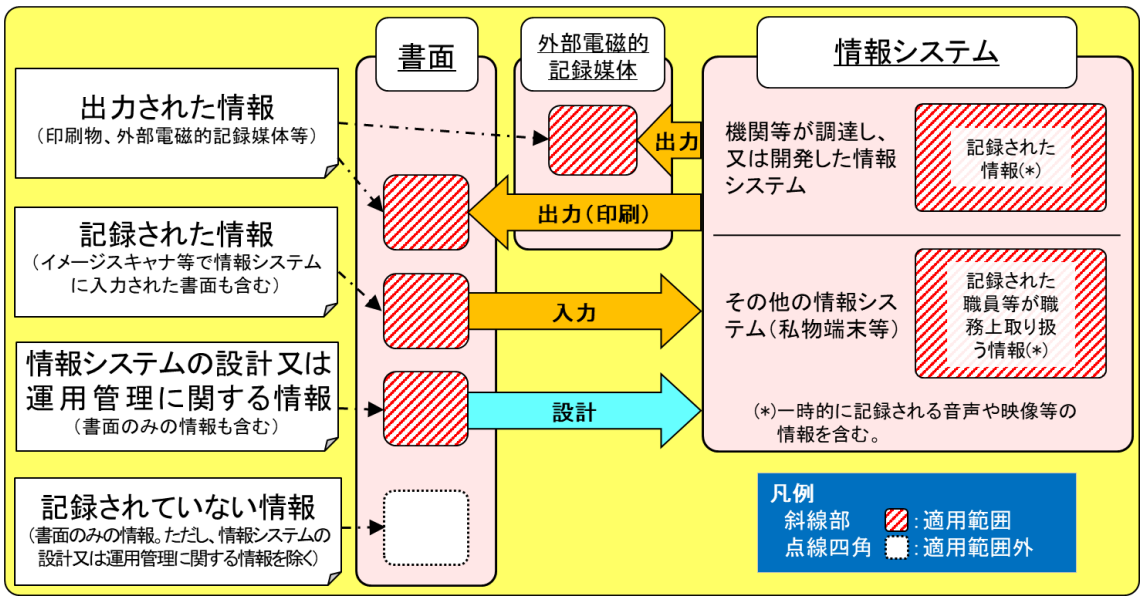


図 1.3-2　統一基準において適用対象とする情報の範囲

1.4 一般用語の解説

留意すべき一般用語を以下に解説する。

【あ】

● 「アクセス制御」とは、情報又は情報システムへのアクセスを許可する主体を制限することをいう。

● 「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

● 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。

● 「暗号化」とは、第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。

● 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に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し、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、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）などがある。

● 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。

● 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

● 「運用監視暗号リスト」とは、CRYPTREC が発行する「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）」において、危殆化等により推奨すべきではないが、互換性維持のために継続利用を容認するものをいう。

【か】

● 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。

● 「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

● 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。

● 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、電子的方式、磁気的方式その他人の知覚によっては認識する

ことができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

● 「業務継続計画」とは、機関等において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。

● 「共用識別コード」とは、複数の主体が共用するために付与された識別コードをいう。原則として、一つの識別コードは一つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。

● 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

● 「サービス不能攻撃」又は「DoS（Denial of Service）攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。また、この DoS 攻撃を複数の拠点から一か所に対して行う攻撃は、DDoS（Distributed Denial of Service）攻撃と呼ばれ、攻撃元が複数に分散しているために防御側の対処が困難な攻撃として知られている。

● 「識別」とは、情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

● 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

● 「次世代ファイアウォール」とは、従来のファイアウォール製品が備えていた、IP アドレスやポート番号によるアクセスの可否を判断する機能だけでなく、通信内容を確認しアクセスの可否を制御する機能等（アプリケーションフィルタリング、ペイロードの検査等）を備えたファイアウォール製品をいう。

● 「シャドーIT」とは、所属する組織の承認を得ずに、職員等がソフトウェア、サービス等を業務利用することをいう。

● 「主体」とは、情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。

● 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、

すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。

- 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

- 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

- 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

- 「推奨候補暗号リスト」とは、CRYPTREC 暗号リストにおいて、安全性及び実装性能は確認されているが、利用実績や普及見込みが十分ではないものをいう。

- 「セキュリティパッチ」とは、発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

- 「ゼロデイ攻撃」とは、ソフトウェアの脆弱性が発見された直後の、脆弱性を解消する手段が公開されておらず、ソフトウェアが脅威にさらされている状態を悪用した攻撃をいう。

- 「ソーシャルメディア」とは、インターネット上において、ブログ、ソーシャルネットワーキングサービス（SNS）、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。

- 「送信ドメイン認証技術」とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン名単位で確認する技術をいう。具体的な技術としては、SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）が挙げられる。

- 「ソフトウェア」とは、サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

【た】

● 「耐タンパ性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。

● 「テレワーク」とは、情報通信技術（ICT：Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。

● 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

● 「電子政府推奨暗号リスト」とは、CRYPTREC 暗号リストにおいて、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストをいう。

● 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

● 「電子メールサーバ」とは、電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。

● 「ドメインネームシステム（DNS）」とは、クライアント等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について回答を行うシステムである。

● 「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.cyber.go.jp というウェブサイトの場合は、cyber.go.jp の部分がこれに該当する。

【な】

● 「名前解決」とは、ドメイン名やホスト名と IP アドレスを変換することをいう。

【は】

● 「ファイアウォール」とは、アクセス制御ポリシーに基づきネットワーク間のアクセスを制御するゲートウェイをいう。

● 「フィッシング」とは、悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メール等を送りつけ、受け取った者にその電子メール等に記載された URL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為をいう。

● 「複合機」とは、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機器をいう。

● 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）、不正なサイトへ誘導を行うスクリプト、利用者のブラウザやアドインの脆弱性を悪用する悪意のあるスクリプト等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

● 「不正プログラム定義ファイル」とは、不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。

● 「踏み台」とは、悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

● 「ペネトレーションテスト」とは、情報システムに対して疑似的な攻撃を実施し、実際に侵入できるかどうかの観点で検証を行う脆弱性診断の手法をいう。その中でも、情報システムごとに脅威分析を行い、個別にカスタマイズしたシナリオに基づき現実の脅威を再現した上で、より実戦的に行う「脅威ベースのペネトレーションテスト」は「TLPT（Threat-Led Penetration Testing）」と呼ばれる。

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「無線 LAN」とは、IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad 等の規格により、無線通信で情報を送受信する通信回線をいう。

● 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

● 「ユーティリティプログラム」とは、設定の自動化ツールなど、実行が容易ではあるがその影響がシステム全体に影響するようなものをいう。

【ら】

● 「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。

● 「リスクベース認証」とは、ユーザの情報システムへのアクセス状況を記録し、通常のアクセス状況と異なるアクセス要求があった際に、リスクの有無を判断して追加の認証を要求する仕組みのことをいう。

● 「ルートヒント」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合は

ルートヒントも変更される。ルートヒントの情報は InterNIC（Internet Network Information Center）のサイトから入手可能である。

【A～Z】

● 「CGI（Common Gateway Interface）」とは、ウェブブラウザから送信された文字列を、スクリプト等のプログラムへの入力パラメータとして受け取り、当該スクリプト等をウェブサーバ上で実行するための仕組みをいう。

● 「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

● 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の２種類に分けることができる。

● 「DNSSEC トラストアンカー」とは、DNSSEC 検証を行う際の、信頼の連鎖の起点情報をいう。

● 「EDR（Endpoint Detection and Response）」とは、端末やサーバ装置（エンドポイント）における活動を可視化し、不正プログラムの検知や記録、攻撃遮断などの対処といった機能を提供する製品をいう。

● 「IDS（Intrusion Detection System）」とは、システムやネットワークを監視し、不正なアクセスを検知して管理者への通知を行う製品をいう。不正なアクセスの検知後、アクセスの遮断等防御措置を行う「IPS（Intrusion Prevention System）」と合わせ「IDS/IPS」と総称される場合がある。

● 「IoC（Indicator of Compromise）」とは、システムに対する攻撃発生やどのようなツールが使われたかなどを明らかにする手がかりとなる情報をいう。例として、不正アクセス元・先又は不審な通信元・先の IP アドレス、ドメイン名、URL、ポート番号、マルウェアのファイル名やハッシュ値、不審なログイン試行、ネットワークトラフィックの異常など、サイバー攻撃や不正アクセスの痕跡等が挙げられる。セキュリティ侵害インジケータ、侵害の痕跡等とも呼ばれる。

● 「IoT（Internet of Things）機器」とは、従来インターネットに接続していなかったが、インターネットに接続する機能を備えるようになった機器をいう。

● 「IPv6 移行機構」とは、物理的に一つのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。

例えば、サーバ装置及び端末並びに通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。

● 「MAC アドレス（Media Access Control address）」とは、機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組合せによって表される。

● 「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。

● 「SASE（Secure Access Service Edge）」とは、ネットワーク機能及びネットワークセキュリティ機能を単一のクラウドサービスによって一元的に提供する製品をいう。

● 「SBOM（Software Bill of Materials：ソフトウェア部品表）」とは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストをいう。SBOM には、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができる。

● 「SIEM（Security Information and Event Management）」とは、セキュリティ関連のログを分析・監視することを目的とし、ログの一元管理、異常の自動検出機能を有する製品をいう。

● 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。

● 「WAF（Web Application Firewall）」とは、ウェブサーバと外部との通信を監視して、ウェブアプリケーションの脆弱性を悪用した攻撃を検知し、遮断することでウェブアプリケーションを保護する製品をいう。

● 「Web 会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム等）は含まれない。

1.5　基本対策事項及び解説の読み方

本ガイドラインの第２部以降に記述する遵守事項に対応した基本対策事項及び解説を参照するに当たり、留意すべき点を以下に示す。なお、以下の抜粋は、紙面の関係上、実際の記載内容から一部の文や規定を削除しているので、実際の記載内容は本文を確認すること。

また、本ガイドラインの解説に記載のウェブサイトのアドレスは、令和７年７月８日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

◆第２部以降の基本的な記述構成

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

統一基準の部・節・款の番号を掲示。
本例では、第３部 3.1 節 3.1.1 款についてのガイドラインを示している。

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。

3.1.1 の目的・趣旨及び3.1.1(1)の遵守事項を掲示。
3.1.1(1)では遵守事項は(a)のみ。
遵守事項は、条(数字)項(アルファベット)号(カタカナ)単位で掲示。

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) の遵守事項に対応した基本対策事項を掲示。

（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、1.5(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。

3.1.1(1)の遵守事項及び対応する基本対策事項について解説している。

◆基本対策事項の個別対策事項が“以下を例とする”として例示されている場合

【 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

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

複数の方法が考えられる基本対策事項については、具体例を示している。

◆基本対策事項の個別対策事項について、“～を全て含む”として例示されている場合

【 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

基本対策事項が複数の事項から構成される場合は、主要な事項として全て行うべき事項を示している。

◆基本対策事項が規定されていない場合

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

遵守事項が具体的な対策事項となっている場合は、基本対策事項を定めていない。
この場合は、遵守事項の解説を参照し、対策基準を定めることになる。

◆基本対策事項が基本対策事項 5.1.1(2)-1 で規定する「追加セキュリティ対策」に該当する場合

【 基本対策事項 】

＜7.2.2(1)(b)関連＞

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。

「追加セキュリティ対策」に該当する対策は、文頭に【追加セキュリティ対策】と示している。

【 基本対策事項 】

＜7.2.3(1)(a)関連＞

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

「基本セキュリティ対策」と「追加セキュリティ対策」に該当する対策が混在する場合は、それぞれの対策の文頭に【基本セキュリティ対策】又は【追加セキュリティ対策】と示している。

第2部 情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1 組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての職員等が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に最高情報セキュリティ責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、最高情報セキュリティ責任者は、統一基準に定められた自らの担務を、最高情報セキュリティ副責任者その他の統一基準に定める責任者に担わせることができる。

遵守事項

(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置

(a) 機関等は、機関等における情報セキュリティに関する事務を統括する**最高情報セキュリティ責任者**1人を置くこと。

(b) 機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する**最高情報セキュリティ副責任者**1人を必要に応じて置くこと。

【 基本対策事項 】

＜2.1.1(1)(a)関連＞

2.1.1(1)-1 最高情報セキュリティ責任者は、次に掲げる事務を統括すること。ただし、e) は独立行政法人又は指定法人を所管する国の行政機関に限る。

a) **情報セキュリティ対策推進のための組織・体制の整備**
b) 対策基準の決定、見直し
c) 対策推進計画の決定、見直し
d) **情報セキュリティインシデント**に対処するために必要な指示その他の措置
e) **所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制**の整備の指示
f) 情報セキュリティ監査の結果を踏まえた改善計画の策定等の必要な措置の指示
g) 前各号に掲げるもののほか、情報セキュリティに関する重要事項

（解説）

- **遵守事項 2.1.1(1)(a)「最高情報セキュリティ責任者」について**

最高情報セキュリティ責任者は、機関等における情報セキュリティ対策の推進の責任者であり、機関等全体の情報セキュリティ対策を推進するため、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することが求められることから、国の行政機関においては局長（官房長）級以上の職員が想定される。その際には、国内外の情報セキュリティに関連する動向を注視するとともに、有益な最新の技術の活用を検討するなど、先手を打って必要な対策をとることが重要である。

最高情報セキュリティ責任者は、情報セキュリティに関する機関等全体の方向付けを行う事務について自ら直接関与すべきであることから、統一基準では、対策基準及び対策推進計画を決定するとともに、重大な情報セキュリティインシデントが発生した場合には、それに対処するための必要な指示その他の措置を行うこととしている。加えて、統括情報セキュリティ責任者からの情報セキュリティ関係規程に係る運用状況や機関等で共通的な課題及び改善すべき点に係る報告、情報セキュリティ監査責任者からの監査結果報告等を踏まえ、機関等における情報セキュリティ対策がより適切に推進されるよう、対策基準及び対策推進計画を見直すことも求められる。

なお、国の行政機関に置かれる最高情報セキュリティ責任者においては、所管する独立行政法人及び指定法人に関し、当該法人を所管する部署との適切な連携や当該部署への必要な助言等を通じて、当該法人の情報セキュリティ対策が適切に推進されるようにすることについても、役割として求められる。

- **遵守事項 2.1.1(1)(b)「最高情報セキュリティ副責任者」について**

最高情報セキュリティ副責任者は、最高情報セキュリティ責任者からの委任（最高情報セキュリティ責任者が自ら行うべき重要事項を除き、事務を任せること。この場合、最高情報セキュリティ責任者から委任された事務について定め、最高情報セキュリティ責任者へ報告することが求められている事項について、その報告先を最高情報セキュリティ副責任者とする場合も定めておくことが望ましい。ただし、任命及び監督の責任は、最高情報セキュリティ責任者に残る。）に基づき、最高情報セキュリティ責任者を助けて、機関等の情報セキュリティ対策に係る事務を総括整理する役割を担う。

このため、最高情報セキュリティ副責任者には、機関等において情報セキュリティ対策について一定程度の専門性を有するとともに、最高情報セキュリティ責任者を助け、組織全体として整合性の取れた方針等の策定、人的資源及び予算等の計画的で持続可能な投入等を実施していく役割が求められることから、国の行政機関においては原則として最高情報セキュリティ責任者に次ぐ官職の職員を充てることが想定される。

なお、国の行政機関に置かれる最高情報セキュリティ副責任者においては、最高情報セキュリティ責任者を助けて、所管する独立行政法人及び指定法人に関し、当該法人を所管する部署との適切な連携や当該部署への必要な助言等を通じて、当該法人の情報セキュリティ対策が適切に推進されるようにすることについても、役割として求められる。

- **基本対策事項 2.1.1(1)-1 a)「情報セキュリティ対策推進のための組織・体制の整備」について**

  機関等の情報セキュリティ体制のイメージを【図 2.1.1-1】に示す。各組織において、当該体制の具体化を検討する際には、内閣官房国家サイバー統括室「サイバーセキュリティ人材フレームワーク（同活用の手引き）」を活用し、各責任者・管理者等の具体的な役割や実施すべきタスク、必要な知識・スキルを明確化することが有効であると考えられる。

  参考：内閣官房国家サイバー統括室「サイバーセキュリティ人材フレームワーク」
  （https://www.cyber.go.jp/council/csjinzai/index.html）

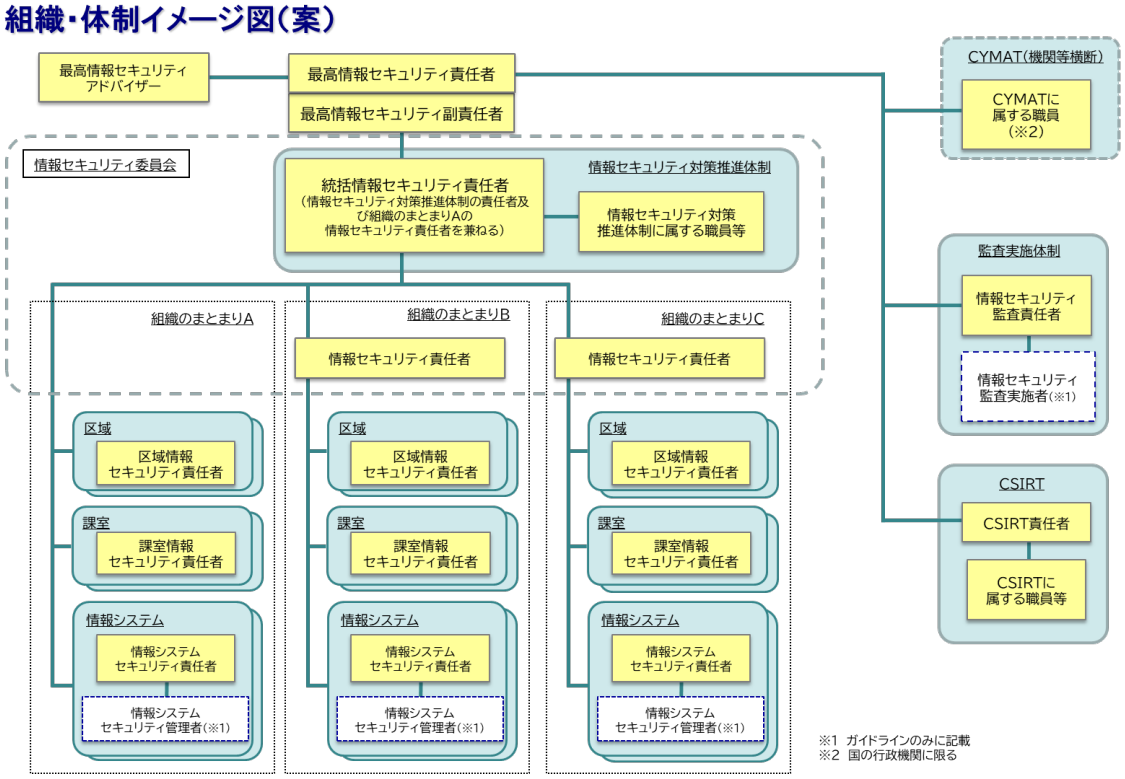


図 2.1.1-1　機関等の情報セキュリティ体制のイメージ

- **基本対策事項 2.1.1(1)-1 d)「情報セキュリティインシデント」について**

情報セキュリティインシデントについては、統一基準 1.3「用語の定義」（本ガイドライン 1.3「統一基準における用語定義」）に示すとおりであるが、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものとして、実際に業務等への影響は顕在化していないものの、そのおそれがある場合を含むことに留意が必要である。情報システムに関する情報セキュリティインシデントとしては、以下の例が考えられる。

- 要機密情報が含まれる電子メールの機関等外への誤送信
- 要機密情報が保存された記録媒体の紛失や盗難
- 端末の不正プログラム感染
- 機関等外からのサーバ装置、端末への不正侵入
- 機関等外からのサービス不能攻撃等による情報システムの停止

- **基本対策事項 2.1.1(1)-1 e)「所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制」について**

独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備には、以下の内容が考えられる。

（導入・計画）

- 独立行政法人を所管する主務大臣が独立行政法人通則法（平成 11 年法律第 103 号）第 29 条第 1 項の規定により指示する同項の中期目標、第 35 条の 4 第 1 項の規定により指示する同項の中長期目標又は第 35 条の 9 第 1 項の規定により指示する同項の年度目標に、統一基準群に基づいて定めたポリシーに従って情報セキュリティ対策を講ずる旨を盛り込むために必要な体制
- 所管する指定法人に対する個別の根拠法に基づいた、必要な情報セキュリティ対策についての指導等を行うために必要な体制

（評価）

- 独立行政法人を所管する主務大臣が行う独立行政法人通則法に基づく業務の実績等に関する評価（情報セキュリティ対策の実施状況に関する部分に限る。）を行うために必要な体制
- 所管する指定法人に関し、個別の根拠法に基づく、情報セキュリティ対策の実施状況に関する評価を行うために必要な体制

（その他）

- 所管する独立行政法人及び指定法人の求めに応じた情報セキュリティ対策に関する助言を行うために必要な体制

なお、これらの体制の整備には所管する独立行政法人及び指定法人の所管部署が適切な対応を行うため、当該法人所管部署に対して、機関の情報セキュリティを統括する立場等から、情報セキュリティに関する専門的知見等を踏まえた必要な助言を行うための連絡窓口を情報セキュリティ対策推進体制に置くことや、当該法人が所管省庁へ情報セキュリティ対策に関する助言を求める際の相談窓口を当該法人所管部署又は情報セキュリティ対策推進体制に置くことが考えられる。

遵守事項

(2) 情報セキュリティ委員会の設置

(a) 最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする**情報セキュリティ委員会**を置くこと。

【 基本対策事項 】

＜2.1.1(2)(a)関連＞

2.1.1(2)-1 情報セキュリティ委員会の委員長及び委員は、最高情報セキュリティ責任者が情報セキュリティ対策推進体制及びその他の業務を実施する部局の代表者から指名すること。

2.1.1(2)-2 情報セキュリティ委員会は、次に掲げる事項を審議すること。

a) 対策基準

b) 対策推進計画

c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

（解説）

- **遵守事項 2.1.1(2)(a)「情報セキュリティ委員会」について**

最高情報セキュリティ責任者は、横断的な事項を審議するため、情報セキュリティを推進する情報セキュリティ対策推進体制及び各部局（部門）の代表者から構成される委員会を設置する。

委員長及び委員は、最高情報セキュリティ責任者の指名によるが、最高情報セキュリティ責任者自らが委員長を兼ねてもよい。

委員会は、各部門間の意見調整を図り情報セキュリティ対策と組織の方針を整合的なものとする機能を持つことから、組織全体としての方向付けを要する対策基準及び対策推進計画を審議事項とする必要がある。その他の審議事項については、機関等の実態に応じて柔軟に運用すればよいが、例えば、遵守事項 2.1.1(6)に規定する情報セキュリティ対策推進体制に担わせる具体的な役割や、その役割に基づく情報セキュリティ対策の推進状況の確認・評価に係る事項を審議することが考えられる。

また、委員会の配下に実務を担当する下位委員会を設置し、実務レベルの詳細な事項を調整することで、委員会の運営を効率化することも考えられる。

遵守事項

(3) 情報セキュリティ監査責任者の設置

(a) 最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、**情報セキュリティ監査責任者**１人を置くこと。

【 基本対策事項 】

＜2.1.1(3)(a)関連＞

2.1.1(3)-1 情報セキュリティ監査責任者は、命により次の事務を統括すること。

a) 監査実施計画の策定

b) 監査実施体制の整備

c) 監査の実施指示及び監査結果の最高情報セキュリティ責任者への報告

d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（解説）

- **遵守事項 2.1.1(3)(a)「情報セキュリティ監査責任者」について**

機関等における情報セキュリティ対策は、最高情報セキュリティ責任者の指揮の下で推進することとなるが、最高情報セキュリティ責任者は、自らが決定した情報セキュリティ対策が適切に実施されているか否かを正しく把握する必要がある。そのため、最高情報セキュリティ責任者は、情報セキュリティ監査責任者にその実施状況等の確認を行わせることにより、情報セキュリティ対策の実効性を確保しようとするものである。

なお、情報セキュリティ監査責任者は、組織のまとまりごとの情報セキュリティに関する事務を担う情報セキュリティ責任者よりも職務上の上位の者を置くことが望ましいものの、その場合に最高情報セキュリティ責任者や統括情報セキュリティ責任者と同一となるなど、監査業務の独立性の確保の観点から問題となる可能性がある場合には、必ずしも情報セキュリティ責任者よりも職務上の上位の者である必要はない。監査に関する事務の統括に当たっては、独立性を確保するため、偏向を廃し、常に公正かつ客観的な判断に努めることに留意して、情報セキュリティ監査責任者を置く必要がある。

情報セキュリティ監査責任者は、情報セキュリティ対策が適切に実施されているか否かを監査し、その結果について最高情報セキュリティ責任者に的確に報告しなければならない。

情報セキュリティ監査責任者は、これら監査事務を効率的に実施するため、担当者（監査実施者）を置き、必要に応じて外部組織を活用するなど、監査実施体制の整備を行う。また、遵守事項 2.1.1(8)(a)(イ)において、監査を受ける者とその監査を実施する者は兼務しないこととされているため、監査実施計画の策定時において、監査実施者の指定に配慮する必要がある。

なお、機関等の実情に応じて、監査責任者を補佐する立場として監査副責任者を独自

に設置してよい。監査を受ける者が監査責任者である場合などにおいては、監査副責任者が監査責任者に代わることにより、監査の独立性を確保することが考えられる。

遵守事項

(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置

(a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、**情報セキュリティ責任者**1人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する者として、**統括情報セキュリティ責任者**1人を選任すること。

(b) 情報セキュリティ責任者は、遵守事項3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する**区域情報セキュリティ責任者** 1人を置くこと。

(c) 情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する**課室情報セキュリティ責任者**1人を置くこと。

(d) 情報セキュリティ責任者は、**所管する情報システム**に対する情報セキュリティ対策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、当該情報システムの企画に着手するまでに選任すること。

【 基本対策事項 】

＜2.1.1(4)(a)関連＞

2.1.1(4)-1 統括情報セキュリティ責任者は、命を受け、次の事務を統括すること。ただし、f) は独立行政法人又は指定法人を所管する国の行政機関に限る。

a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定
b) 情報セキュリティ対策に関する運用規程・実施手順の整備及び見直し並びに**運用規程・実施手順**に関する事務の取りまとめ
c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
d) 例外措置の適用審査記録の台帳整備等
e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
f) 独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制における連絡や相談等の窓口の整備
g) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

2.1.1(4)-2 情報セキュリティ責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。

a) 定められた区域ごとの区域情報セキュリティ責任者の設置
b) 課室の課室情報セキュリティ責任者の設置
c) 情報システムごとの情報システムセキュリティ責任者の設置
d) 情報セキュリティインシデントの原因調査、再発防止策等の実施
e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備
f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

＜2.1.1(4)(b)関連＞

2.1.1(4)-3 区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び環

境に係る情報セキュリティ対策に関する事務を統括すること。

＜2.1.1(4)(c)関連＞

2.1.1(4)-4 課室情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括すること。

＜2.1.1(4)(d)関連＞

2.1.1(4)-5 情報システムセキュリティ責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。

2.1.1(4)-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の管理業務において必要な単位ごとに**情報システムセキュリティ管理者**を置くこと。

（解説）

- **遵守事項 2.1.1(4)(a)「情報セキュリティ責任者」について**

最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能となる組織のまとまりごとに、その対策を委ねた方が効率的であることから、取りまとめの責任者として、情報セキュリティ責任者を設置する。情報セキュリティ対策の運用が可能なまとまりとしては、国の行政機関においては、部局（内局、外局、地方支分部局等、附属機関）ごとが想定されることから、情報セキュリティ責任者は局長級職員（組織のまとまりの長）又は当該職員の直接的な指示が及ぶ当該職員に次ぐ官職の職員を充てること等が想定される。独立行政法人及び指定法人においては、法人の組織構成によるが、例えば、役員を除く職員等の中で最も高位の職にある者が長となる組織のまとまりごととすることが想定される。

情報セキュリティ責任者は、最高情報セキュリティ責任者の委任に基づき、所管する組織の情報セキュリティ対策を推進及び運用するため、組織内の体制整備及び事務を行う。

機関等における情報セキュリティ確保のための体制の整備に当たっては、機関等の業務形態やその組織の有する実情を踏まえ、組織全体として情報セキュリティマネジメントが機能する体制整備を行うことが重要であり、以下のような場合には、特に情報セキュリティ責任者の役割が重要である。

例えば、国立研究開発法人等の研究開発機関においては、業務形態や組織の態様が比較的一様な事務的業務を行う一般の行政機関とは異なり、管理部門と研究部門という異なる形態の部門が存在するが、情報セキュリティの観点からは、組織全体としての統一的なセキュリティの確保が求められる。これらの研究開発機関においては各研究部門の長は、情報セキュリティ責任者として役割を担うことが想定されるが、研究内容に関する立場と同様に、情報セキュリティ対策についても情報セキュリティ責任者として各研究者に対してリーダーシップを発揮することが重要である。また、このような研究開発機関における情報セキュリティ対策推進体制においては、各研究部門を含む組織全体の情報セキュリティの対策状況をタイムリーに把握し、必要に応じて課題への機敏な対応が可能となるように、各研究部門との連携体制を構築することが必要となる。

情報セキュリティ対策推進体制と各研究部門を相互に連携させるとともに、各研究部門内の情報セキュリティ対策を指揮する立場にあるのが情報セキュリティ責任者である各研究部門の長であり、その役割に期待されるところは大きいといえる。

- **遵守事項 2.1.1(4)(a)「統括情報セキュリティ責任者」について**

最高情報セキュリティ責任者は、自らの事務及び最高情報セキュリティ副責任者の事務を補佐させるため、組織のまとまりごとに設置する情報セキュリティ責任者のうちから１人を統括情報セキュリティ責任者として選任することから､情報セキュリティ責任者のうち、職務上の最上位の者又は府省庁において情報セキュリティを所掌する情報セキュリティ責任者を充てることが想定される。

統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの委任（最高情報セキュリティ責任者が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、最高情報セキュリティ責任者に残る。）に基づき機関等の情報セキュリティ対策について総合調整する事務を担うとともに、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する役割を担う。例えば、対策基準や対策推進計画の案の作成を担うことが想定される。

- **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**

情報セキュリティ責任者は、所管する組織のまとまりの情報セキュリティ対策のうち施設及び環境に係る対策について、定められた区域ごとにその対策を推進する責任者として区域情報セキュリティ責任者を指名する。

区域情報セキュリティ責任者は、所管する区域について規定された対策の基準に従い、自ら対策を定めそれを実施する。また、区域情報セキュリティ責任者は、その役割の性質上、施設の管理者が兼任することが想定される。定める単位としては、以下の例が考えられる。

- 単一の課室が利用する執務室及び会議室を管理する場合は、課室情報セキュリティ責任者
- 情報システムが設置された部屋（サーバ室等）を管理する場合は、情報システムセキュリティ責任者
- ロビー、廊下等を管理する場合は、施設等の管理に関する部門の責任者

なお、基本対策事項 3.2.1(1)-1 で後述するクラス１は、施設管理の観点から行う措置が、情報セキュリティ上の対策と同等であれば、施設の管理者が指定されていることをもって、区域情報セキュリティ責任者を設置しているとみなしてよい。

- **遵守事項 2.1.1(4)(c)「課室情報セキュリティ責任者」について**

情報セキュリティ責任者は、課室又はこれと同等の組織単位内の情報の取扱い及び情報セキュリティ対策の責任者として、課室情報セキュリティ責任者を設置する。課室情報セキュリティ責任者は、情報の取扱い等に関して、その是非を判断する役割を担うため、課室長又はそれに相当する者であることが望ましい。

- **遵守事項 2.1.1(4)(d)「所管する情報システム」について**

所管する情報システムとは、企画・要件定義から公開・廃棄までの情報システムのラ

イフサイクル全般における事務の責任を主に負っている情報システムを想定しており、政府共通利用型システム利用機関から見た政府共通利用型システムは該当しない。しかし、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より、政府共通利用型システムの責任範囲が定められている場合は、その範囲において、所管する情報システムと見なして対策を実施する必要がある。

- **遵守事項 2.1.1(4)(d)「情報システムセキュリティ責任者」について**

  情報セキュリティ責任者は、情報システムごとの情報セキュリティ対策及び運用の責任者として、情報システムセキュリティ責任者を指名する。

  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ライフサイクル全般にわたって適切に情報セキュリティ対策を実施することが求められる。このため、情報セキュリティ責任者は、所管する新規の情報システムについて企画に着手するまでに情報システムセキュリティ責任者を選任しなければならない。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システム、特定部門における個別業務システム等、機関等の全ての情報システムについて、情報システムごとにセキュリティ対策の運用の責任の所在を明確にすることが重要である。また、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にする必要がある。

  なお、政府共通利用型システム利用機関においては、当該情報システムを所管するものではないため、情報システムセキュリティ責任者の選任は不要であるが、当該情報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務の責任者として、「政府共通利用型システム利用管理者」を置く必要がある。「政府共通利用型システム利用管理者」については、遵守事項 5.4.2(1)(b)を参照のこと。

  情報システムセキュリティ責任者は、情報セキュリティ対策の技術的事項について補佐する者（基本対策事項 2.1.1(4)-6 で定める情報システムセキュリティ管理者）をデータベース、アプリケーション等の装置・機能ごとに、必要に応じて置き、技術的対策の実効性を確保することが望ましい。

- **基本対策事項 2.1.1(4)-1 b)「運用規程・実施手順」について**

  付録(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」を参照のこと。

- **基本対策事項 2.1.1(4)-6「情報システムセキュリティ管理者」について**

  情報システムセキュリティ管理者は、情報システムセキュリティ責任者が定めた手順や判断された事項に従い、所管する情報システムのセキュリティ対策を実施する。

遵守事項

(5) 最高情報セキュリティアドバイザーの設置

(a) 最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を**最高情報セキュリティアドバイザー**として置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。

【 基本対策事項 】

＜2.1.1(5)(a)関連＞

2.1.1(5)-1 最高情報セキュリティ責任者は、以下を例とする最高情報セキュリティアドバイザーの業務内容を定めること。

a) 機関等全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者及び最高情報セキュリティ副責任者への助言
b) 情報セキュリティ関係規程の整備に係る助言
c) 対策推進計画の策定に係る助言
d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
e) 情報システムに係る技術的事項に係る助言
f) 情報システムの設計・開発を外部委託により行う場合に**調達仕様に含めて**提示する情報セキュリティに係る要求仕様の策定に係る助言
g) 職員等からの日常的な相談対応
h) 情報セキュリティインシデントへの対処の支援
i) **情報システムの分類**に応じた情報セキュリティ対策に係る助言
j) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（解説）

- **遵守事項 2.1.1(5)(a)「最高情報セキュリティアドバイザー」について**

最高情報セキュリティ責任者は、情報セキュリティに関する技術的事項等について自ら及び最高情報セキュリティ副責任者への助言等を含む機関等の情報セキュリティ対策への助言、支援等を行う者として最高情報セキュリティアドバイザーを置く。

最高情報セキュリティアドバイザーは、機関等における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち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）及び実務経験を有する者である必要がある。

設置に際しては、機関等の実情に応じて、例えば、国の行政機関の最高情報セキュリティアドバイザーが、その外局、地方支分部局等や所管する独立行政法人等の最高情報セキュリティアドバイザーを兼務することも考えられる。

なお、外部人材のみならず機関等内の職員等を充ててもよい。この場合、当該職員等が情報セキュリティ責任者やその他の責任者を兼務してもよい。

- **基本対策事項 2.1.1(5)-1 f)「調達仕様に含めて」について**

  調達仕様に含めるとは、調達仕様書や契約書に記載することを求めており、本統一基準群において同じである。

- **基本対策事項 2.1.1(5)-1 i)「情報システムの分類」について**

  遵守事項 5.1.1(1)(a)で整備を求め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である情報システムの分類基準に基づく分類を示している。

遵守事項

(6) 情報セキュリティ対策推進体制の整備

(a) 最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制を整備し、その役割を規定すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。

【 基本対策事項 】

＜2.1.1(6)(a)関連＞

2.1.1(6)-1 最高情報セキュリティ責任者は、以下を全て含む情報セキュリティ対策推進体制の役割を規定すること。

a) 情報セキュリティ関係規程及び対策推進計画の策定に係る事務
b) 情報セキュリティ関係規程の運用に係る事務
c) 例外措置に係る事務
d) 情報セキュリティ対策の教育の実施に係る事務
e) 情報セキュリティ対策の自己点検に係る事務
f) 情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

（解説）

- **遵守事項 2.1.1(6)(a)「機関等の情報セキュリティ対策推進体制を整備」・基本対策事項 2.1.1(6)-1「情報セキュリティ対策推進体制の役割を規定する」について**

機関等の情報セキュリティ対策を推進するためには、組織横断的に施策を取りまとめて推進する情報セキュリティ対策推進体制が必要であり、本項では、そのような体制とその役割を組織として明確にすることを求めている。

情報セキュリティ対策推進体制の基本的な役割は、本基本対策事項各号に定める事項を基本とし、組織の特性等に応じ、その他必要な事項を追加するなどして規定する必要がある。その他にも、以下の例の事項を役割として担うことが考えられる。

- 情報セキュリティ委員会の運営に係る事務
- 本部監査への対応に係る事務
- 内閣官房国家サイバー統括室から発出される事務連絡や調査依頼事項等への対応に係る事務

また、「(解説) 遵守事項 2.1.1(4)(a)「統括情報セキュリティ責任者」について」に記載のとおり、統括情報セキュリティ責任者が機関等の情報セキュリティ対策について総合調整する事務を担っていることから、情報セキュリティ対策推進体制は、統一基準において統括情報セキュリティ責任者の役割として規定されている事項に係る実務を含む事務を担う体制として位置付けるとよい。

さらに、遵守事項 7.2.1(1)(c)において情報システムセキュリティ責任者に求めている脆弱性対策の状況の定期的な確認を支援するために、ソフトウェアに関する脆弱性情

報の公開状況を確認し、情報システムセキュリティ責任者と情報共有を行うなど、情報システムの情報セキュリティ対策を推進するための事務を担うことなども考えられる。

- **遵守事項 2.1.1(6)(b)「情報セキュリティ対策推進体制の責任者」について**

  「（解説）遵守事項 2.1.1(6)(a)「機関等の情報セキュリティ対策推進体制を整備」・基本対策事項 2.1.1(6)-1「情報セキュリティ対策推進体制の役割を規定する」について」において記述しているとおり、情報セキュリティ対策推進体制は、統括情報セキュリティ責任者が担う実務を中心とした事務を遂行するための体制として機能させることを想定している。そのため、本項で定める責任者として、統括情報セキュリティ責任者を充てることが考えられる。ただし、実際の組織構成等に応じて統括情報セキュリティ責任者以外の者を充てることを妨げるものではない。

遵守事項

(7) 情報セキュリティインシデントに備えた体制の整備

(a) 最高情報セキュリティ責任者は、**CSIRT** を整備し、その役割を明確化すること。

(b) 最高情報セキュリティ責任者は、職員等のうちから **CSIRT に属する職員等**として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、機関等における情報セキュリティインシデントに対処するための責任者として **CSIRT 責任者**を置くこと。また、**CSIRT 内の業務統括及び外部との連携等を行う職員等**を定めること。

(c) 最高情報セキュリティ責任者は、**情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制**を整備すること。

(d) 最高情報セキュリティ責任者は、**CYMAT に属する職員**を指名すること。（国の行政機関に限る。）

【 基本対策事項 】

＜2.1.1(7)(a)関連＞

2.1.1(7)-1 最高情報セキュリティ責任者は、以下を全て含むCSIRTの役割を規定すること。

a) 機関等に関わる情報セキュリティインシデント発生時の対処の一元管理

- **機関等全体における情報セキュリティインシデント対処の管理**
- 情報セキュリティインシデントの可能性がある事案の報告受付
- 機関等における情報セキュリティインシデントに関する情報の集約
- 所管する独立行政法人及び指定法人における情報セキュリティインシデントに関する情報の集約（当該法人を所管する国の行政機関に限る。）
- 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化

b) 情報セキュリティインシデントへの迅速かつ的確な対処

- 報告を受けた事案が情報セキュリティインシデントであるか否かの評価
- 被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
- 内閣官房国家サイバー統括室への連絡（国の行政機関に限る。）
- 独立行政法人及び指定法人から所管する国の行政機関への連絡
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- 他の機関等への情報セキュリティインシデントに係る情報の共有
- 情報セキュリティインシデントへの対処に係る**専門的知見の提供、対処作業の実施**

2.1.1(7)-2 最高情報セキュリティ責任者は、**実務担当者を含めた実効性のある CSIRT 体制**を構築すること。

2.1.1(7)-3 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する**外部の専門家等による必要な支援を速やかに得られる体制**を構築すること。

2.1.1(7)-4 最高情報セキュリティ責任者は、機関等全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の**役割分担を規定**すること。

（解説）

- **遵守事項 2.1.1(7)(a)「CSIRT」について**

機関等の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、当該機関等が、最高情報セキュリティ責任者等の幹部の指揮の下、情報セキュリティインシデントへの対処を一元的に管理し、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備する必要がある。

一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRT は、時々刻々と明らかになる情報を基に、状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で最高情報セキュリティ責任者等の幹部に状況を報告する。

- **遵守事項 2.1.1(7)(b)「CSIRT に属する職員等」について**

CSIRT に属する職員等は、機関等における情報セキュリティインシデントを認知した際、最高情報セキュリティ責任者の指揮の下、これに対処する職員等であることから、最高情報セキュリティ責任者に対して適切に状況を報告し、最高情報セキュリティ責任者の指示を受け適切に対処できる必要がある。

CSIRT に属する職員等には、情報セキュリティ、情報システム等に関する知識及び技能を持つ者並びに機関等のネットワーク構成や個別システムの情報システムセキュリティ責任者及び管理者を把握している者を含めることが求められる。CSIRT が設置された部門において、求められる知識や技能等を有する者が不足している場合には、CSIRT が設置された部門以外の職員等を CSIRT に属する職員等として充てることも考えられる。

また、CSIRT に属する職員等には、上述した技術的な対処の外、発生した情報セキュリティインシデントの影響の大きさによっては、対外的な対応も必要となることから、広報を担当する職員等を CSIRT に含めておくことも考えられる。

なお、他の部門の職員等を CSIRT に属する職員等として充てる場合には、職務命令として CSIRT に係る職務を兼任させるなど、当該職員等が支障なく活動できるよう留意する必要がある。

- **遵守事項 2.1.1(7)(b)「CSIRT 責任者」について**

CSIRT 責任者とは、情報セキュリティインシデントの対処に係る責任者であり、情報セキュリティインシデントに関する全般的な対応が求められる。ただし、重大な情報セキュリティインシデントが生じ、最高情報セキュリティ責任者自らが、情報セキュリティインシデントへ対処する必要があるときには、その指揮監督の下で必要な対応を

行うこととなる。

- **遵守事項 2.1.1(7)(b)「CSIRT 内の業務統括及び外部との連携等を行う職員等」について**

  CSIRT 内の業務統括及び外部との連携等を行う職員等は、CSIRT 責任者の指揮の下、CSIRT の業務や連絡を一元的に管理し統括する機能を担う。ここでいう職員等は、一人の職員等に制限するものではなく、いわゆる総括班のような位置付けで複数名置くことが望ましい。

- **遵守事項 2.1.1(7)(c)「情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制」について**

  CSIRT 責任者が情報システムを所管している場合、当該情報システムの情報セキュリティインシデントを認知した際、２つの役職が利害相反関係にあることから、最高情報セキュリティ責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。

  これを避けるため、例えば、CSIRT 責任者には情報セキュリティ責任者以外の者を充てる、最高情報セキュリティ責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途 CSIRT 責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保する必要がある。

- **遵守事項 2.1.1(7)(d)「CYMAT に属する職員」について**

  CYMAT は、国の行政機関の情報セキュリティに関する知識及び技能を有する職員で構成する体制であり、サイバー攻撃等により支援対象機関で情報セキュリティインシデントを認知した場合であって、政府として一体となった対応が必要となる情報セキュリティインシデントを取り扱う。CYMAT の主な機能は以下のとおりである。

  - 発生事象の正確な把握
  - 被害拡大防止、復旧、再発防止のための技術的な支援及び助言
  - 対処能力の向上に向けた平常時の取組（研修、訓練等の実施）

  CYMAT に属する職員には、CYMAT 要員及び CYMAT 研修員がある。CYMAT 要員になるために、セキュリティに関する特定の資格は求めていないものの、情報セキュリティ、情報システム等に関する基礎的な知識を有する者を充てることが望ましい。また、CYMAT 研修員については、将来 CYMAT 要員になる候補者として活動することが期待される職員で、情報セキュリティ、情報システム等といった分野に関心を持ち、内閣官房国家サイバー統括室等が提供する研修に参加し、研さんに励むことができる職員が望ましい。

  CYMAT 要員に対しては、内閣官房の併任辞令を発令することで、内閣官房の予算を措置することにより内容の充実した訓練・演習の機会を提供している。また、CYMAT 研修員に対しても研修の機会を提供していることから、国の行政機関においては、組織内でのインシデントレスポンスに当たる職員の育成という観点からも、CYMAT 要員又は CYMAT 研修員として内閣官房国家サイバー統括室に登録することが望ましい。

- **基本対策事項 2.1.1(7)-1 a)「機関等全体における情報セキュリティインシデント対処の**

管理」について

情報セキュリティインシデントへの対処に当たっては、「検知／連絡受付」、「トリアージ（情報セキュリティインシデントであるか否かの評価、優先度付け等）」、「インシデントレスポンス（応急措置の実施、原因調査、復旧、再発防止等）」、「報告／情報公開（報道発表等の対外対応）」といったプロセスが必要となる。

「機関等全体」とは、国の行政機関における CSIRT においては、外局、地方支分部局等を含み、独立行政法人及び指定法人における CSIRT においては、法人の組織構成によるが、例えば、支部、地方組織等を含む組織の全てを意味する。CSIRT には、上記のプロセス全体について、機関等内外の関係組織と連携・調整を図り、状況を把握し、適宜幹部等への報告を行うとともに、迅速かつ的確な対処が行われるように当事者部局への指示・勧告・助言を行うことが求められる。

- **基本対策事項 2.1.1(7)-1 b)「専門的知見の提供、対処作業の実施」について**

機関等において、サイバーセキュリティや情報セキュリティインシデントへの対処に係る専門組織や専門知識を持った職員等を有する場合は、それらの組織・職員等の CSIRT への組み込み、又は情報セキュリティインシデント発生時に連携できる体制の構築を行うことが望ましい。

- **基本対策事項 2.1.1(7)-2「実務担当者を含めた実効性のある CSIRT 体制」について**

CSIRT 体制には、情報セキュリティインシデント対処における最高情報セキュリティ責任者への早急な状況報告、被害拡大防止及び復旧のための対策の実施を果たし得るよう、実務担当の職員等（例えば、国の行政機関においては、課長補佐以下の者）を複数含める必要がある。

また、CSIRT は、最高情報セキュリティアドバイザー等から情報セキュリティインシデントへの対処の支援が円滑に受けられるような体制とすることが望ましい。

- **基本対策事項 2.1.1(7)-3「外部の専門家等による必要な支援を速やかに得られる体制」について**

外部の専門家等による必要な支援を迅速に得られる体制の構築の例としては、情報セキュリティインシデント発生時にそうした事案への対処に精通した専門家を速やかに派遣してもらうための契約を事業者と結ぶこと等が挙げられる。

- **基本対策事項 2.1.1(7)-4「役割分担を規定」について**

情報セキュリティインシデント発生時に、関係者が速やかに必要な対処を行えるように、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局（広報担当部局、調達担当部局、サイバーセキュリティ専門部局等）の役割分担をあらかじめ定めておくことが望ましい。ただし、役割分担は、情報セキュリティインシデントの種類や規模、影響度合い等によって変更されることも考えられるため、発生の頻度が比較的高いと考えられる情報セキュリティインシデントを想定した役割分担をあらかじめ定めておき、必要に応じて役割分担を再設定することも考えられる。

遵守事項

(8) 兼務を禁止する役割

(a) 職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア) 承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う許可権限者

(イ) 監査を受ける者とその監査を実施する者

(b) 職員等は、承認等を申請する場合において、自らが許可権限者であるときその他許可権限者が承認等の可否の判断をすることが不適切と認められるときは、当該**許可権限者の上司又は適切な者**に承認等を申請し、承認等を得ること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.1(8)(b)「許可権限者の上司又は適切な者」について**

事前に例外の規定として定めることが求められ、規定された本来の許可権限者をもって承認等の判断をすることが適切ではない場合としては、以下がある。

- 申請する者と承認等する者が同一の場合
- 申請する者が承認等する者の上司である場合

承認等の申請を「許可権限者の上司」にする例として、情報セキュリティ責任者等よりも高位の者が承認等を申請する場合は、上司である最高情報セキュリティ責任者が原則、承認等の判断をすることが考えられる。

承認等の申請を「適切な者」にする例として、最高情報セキュリティ責任者と同等以上の職位の者が承認等を申請する場合は、適切な者として最高情報セキュリティ責任者が原則、承認等の判断をすることが考えられる。

いずれの場合であっても、最高情報セキュリティ責任者による判断が難しいと想定される承認等の申請（技術的な事項等）の場合は、規定された本来の許可権限者が承認等の判断することは差し支えないが、申請する者と承認等する者が同一であってはならないことに留意が必要である。

また、情報セキュリティインシデントの認知時において緊急を要する対処等の必要性に備えて、通常とは異なる例外的な承認等の手続を定めることも検討する必要がある。

2.1.2 資産管理

目的・趣旨

機関等において情報セキュリティ対策を検討する際に、自組織の資産の状況を把握することが重要である。資産の把握が不十分な状況では、把握できていない資産が存在することによる対策の漏れや、網羅的な対策がなされず情報システムに脅威が存在し続ける可能性がある。さらに、情報セキュリティインシデントが発生した際、資産が正しく管理されていないと情報セキュリティインシデントに対応するための情報収集に時間を要するなど、情報セキュリティインシデントへの対処が遅れる等の可能性がある。

このため機関等においては、自組織の資産の全容を把握するために必要な事項を整理し、職員等が資産を把握しやすいように、資産台帳として情報システム台帳を整備しておく必要がある。

遵守事項

(1) 情報システム台帳の整備

(a) 統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

【 基本対策事項 】

＜2.1.2(1)(a)関連＞

2.1.2(1)-1 統括情報セキュリティ責任者は、以下の内容を全て含む台帳を整備すること。

a) 情報システム名
b) 管理課室
c) 情報システムセキュリティ責任者の氏名及び連絡先
d) 情報システムの構成
e) 情報システムに接続する機関等外通信回線の種別・用途
f) 情報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
g) 情報システムの設計・開発、運用・保守に関する事項
h) 情報システムの利用目的
i) 情報システムの分類基準に基づいて実施した情報システムの分類結果
j) 連携する情報システム及び連携内容

また、民間事業者等が提供するクラウドサービス等を利用して情報システムを構築する場合は、前述の a)～j)に加え、以下を全て含む内容についても台帳として整備すること。

k) クラウドサービス等の名称（クラウドサービスの場合、必要に応じて機能名までを含む。）
l) クラウドサービス等の提供者の名称
m) 利用期間
n) クラウドサービス等の概要
o) ドメイン名
p) クラウドサービス等で取り扱う情報の格付及び取扱制限に関する事項

q) 情報の暗号化に用いる鍵の管理主体（機関等管理かクラウドサービス等の提供者管理か。）
r) クラウドサービス等で取り扱う情報が保存される国・地域
s) サービスレベル

（解説）

- **遵守事項 2.1.2(1)(a)「情報システム台帳に整備する」について**

統括情報セキュリティ責任者は、自組織の資産の全容を把握するため、情報システムセキュリティ責任者が所管する、それぞれの情報システム台帳を統合して、自組織の全ての資産（業務委託によるものを含む。）が把握できる情報システム台帳を整備することが想定される。

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係る情報システム台帳に記載する情報や資料を適切に管理するため、例えば、情報システムごとに最終更新日を記載するなどして、台帳に記載する情報や資料の作成日又は最終更新日を記録し、更新等があった場合には、統括情報セキュリティ責任者へ速やかに報告することが求められる。これに加えて、統括情報セキュリティ責任者は時期を定め、定期的に情報システム台帳の記載事項の変更の有無を調査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が所管する情報システムに係る台帳の記載については、他の責任者等（例：課室情報セキュリティ責任者）と連携して、所管する「情報システム」及び「機器等」（図 1.3-1 参照）について、情報システム関連文書を活用するなどして、必要となる事項を網羅する必要がある。

具体的には以下の例が考えられる。

- 情報システム台帳に記載する事項について、情報システム関連文書に記載がある場合、情報システム関連文書の該当箇所を情報システム台帳に明記する。
- 課室で独自に調達し、情報システム台帳に記載した情報システムの管理下にない機器等（例：端末、サーバ装置（NAS（Network Attached Storage））、外部電磁的記録媒体）について、情報システム台帳に「課室で管理する機器等一式」の項目を設けて記載する。

政府共通利用型システムに係る情報システム台帳については、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が整備する必要があるが、政府共通利用型システム利用機関に設置している機器等を把握するために必要な文書については、政府共通利用型システム利用管理者と共有することが求められる。

- **基本対策事項 2.1.2(1)-1 d)「情報システムの構成」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事項を含める必要がある。

- **基本対策事項 2.1.2(1)-1 e)「機関等外通信回線の種別・用途」について**

  当該事項については、リスク評価の結果等を踏まえた適切な情報セキュリティ対策を講ずるために必要な情報であるだけでなく、情報セキュリティインシデント（標的型攻撃やサービス不能攻撃等）発生時にも有用な情報となる

  通信回線について、次の項目を記載することが求められる。

  - 種別
    光回線（有線回線の例）、モバイル回線（無線回線の例）
  - 用途
    情報システムのリモート保守用回線、情報システムへの外部アクセス用回線、外部公開サーバへのアクセスを受けるための回線等

  以下は、必要に応じて記載を検討することが望ましい。

  - 回線サービス名
  - 事業者名
  - 利用期間
  - ネットワーク帯域

- **基本対策事項 2.1.2(1)-1 g)「設計・開発、運用・保守に関する事項」について**

  当該情報システムの設計・開発、運用・保守に関する事項の記載は、実施責任者又は実施担当組織、業務委託した場合には委託先及び委託先の責任範囲等に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。

  なお、情報システムに関する業務委託に係る事項を記録する際は、以下の項目を記録することが望ましい。

  - 契約責任者等（当該情報システムの請負業務の履行状況を実質的に理解する者であり、契約行為の責任者や情報システムセキュリティ責任者等が考えられる。）
  - 担当部署名
  - 業務委託する業務
  - 業務委託において取り扱う情報の格付及び取扱制限に関する事項
  - 情報システムに関する業務委託の範囲
  - 業務委託先名称（法人番号を含む。）
  - 契約期間
  - 情報セキュリティ対策の実施内容及び管理体制
  - 再委託先に係る事項

- **基本対策事項 2.1.2(1)-1 i)「情報システムの分類基準に基づいて実施した情報システムの分類結果」について**

  当該事項については、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分類基準に基づいて実施した情報システムの分類結果と、結果に応じて追加セキュリティ対策の実施をしたかを判断するための情報である。情報システムの

分類基準については、5.1「情報システムの分類」について参照のこと。

- **基本対策事項 2.1.2(1)-1 j)「連携する情報システム及び連携内容」について**

  当該事項については、各情報システムが他の情報システムや政府共通利用型システムと連携する場合、アプリケーションの修正や更改等において留意すべきことを把握するために必要となる。具体的には、他の情報システムの名称や政府共通利用型システムの名称等及び連携する内容について記載する必要がある。

- **基本対策事項 2.1.2(1)-1「民間事業者等が提供するクラウドサービス等を利用して情報システムを構築する場合」について**

  機関等として独自の情報システム基盤を設けずに、クラウドサービス等を利用して情報システムを構築し運用する場合は、利用するサービス名や契約事業者等の事項を記載したサービス契約に係る書類を適切に管理することが重要である。これらの書類を集約し、容易に参照できるようにすることをもって台帳整備に代えることも考えられるが、この場合は、当該書類に基本対策事項 2.1.2(1)-1 で示した内容が全て網羅されているか確認し、不足する場合は補足資料を作成し、これも集約する必要がある。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台帳を整備することも考えられる。

- **基本対策事項 2.1.2(1)-1 q)「情報の暗号化に用いる鍵の管理主体」について**

  クラウドサービスの利用においては、情報の暗号化に用いる鍵の管理をする主体を明確にする必要がある。利用するクラウドサービスの形態及び仕様によっては、暗号鍵の管理をクラウドサービス提供者自身によって行っているサービスも存在し、クラウドサービス提供者がクラウドサービス利用者の情報を復号できてしまう可能性もある。また、クラウドサービスの利用を終了する際に、クラウドサービスで取り扱った情報の廃棄方法として、暗号化消去等も考えられるが、暗号化に用いた鍵の管理を確実に実施していることを確認する必要がある。そのため、利用するクラウドサービスにおいて暗号鍵の管理主体を事前に把握する必要がある。

- **基本対策事項 2.1.2(1)1- r)「クラウドサービス等で取り扱う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、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、利用するクラウドサービスにおける情報が保存されている国や地域を把握する必要がある。

- **基本対策事項 2.1.2(1)-1 s)「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の品質保証が定められ、また、利用するサービスの組み合わせやオプションの利用などによりサービスの品質保証を受けられる構成が定まっている場合がある。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おそれがあるため、クラウドサービスのサービスレベルについて事前に把握する必要がある。把握が望ましいサービスレベルは以下が考えられる。また、これらの情報は、クラウドサービス等を含めた情報システム全体の情報として把握することにより、特に危機的事象発生時における対応に有用な情報となることが想定される。

- サービス提供時間
- 障害発生時の復旧許容時間
- 災害対策の要否や内容

2.1.3 情報セキュリティ関係規程の整備

目的・趣旨

機関等の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、機関等として遵守すべき対策の基準を、情報セキュリティに係るリスク評価の結果等を踏まえた上で定めるとともに、計画的に対策を実施することが重要である。

また、対策基準に定められた対策を実施するためには具体的な運用規程や実施手順を定める必要があるが、それらが整備されていない、又は内容に漏れがあると、対策が適切に実施されないおそれがあることから、その場合には、最高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に運用規程等の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

(1) リスク評価の実施

(a) 最高情報セキュリティ責任者は、機関等の目的等を踏まえ、自己点検の結果、情報セキュリティ監査の結果、本部監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.3(1)(a)「リスクを評価する」について**

対策基準や対策推進計画を定めるに当たっては、情報セキュリティを取り巻く様々な脅威や、機関等の業務、取り扱う情報及び保有する情報システムの特性等を踏まえた上で、リスク評価を行うことが重要である。リスク評価は、リスク分析の成果に基づき、いかなるリスクへの対応が必要か、講ずべき対策の優先順位はどうするかなどについて意思決定を支援することを目的に実施するものである（図 2.1.3-1 参照）。機関等の業務、取り扱う情報及び保有する情報システムの特性に応じてリスクは異なることから、機関等における情報セキュリティを確保するためには、リスク評価を実施し、対策基準に定めるべき対策事項等を決定することが重要である。

リスク評価手法については、機関等の情報セキュリティに係るマネジメント能力の成熟度や機関等の置かれた環境に応じた適切な手法を選ぶとよい。

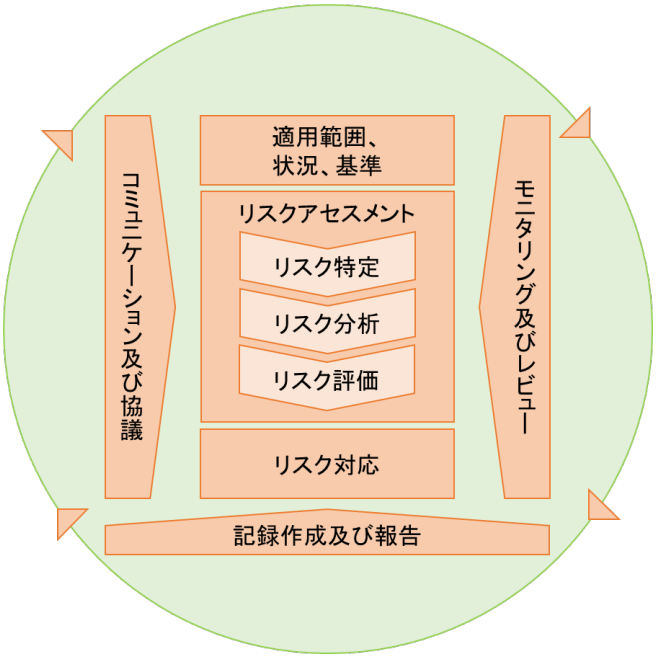


図 2.1.3-1　リスクマネジメントプロセスのイメージ図（JIS Q 31000:2019 による）

以下では、国際標準や国内のガイドライン等に基づいたリスク評価手法の例を解説する。一連のリスク評価手法のプロセスは以下のとおり。

① リスク基準の決定
② リスク特定
③ リスク分析
④ リスク評価
⑤ リスク対応

① リスク基準の決定

リスク基準は、リスクの重大性を評価するための目安とする条件であり、本解説におけるリスク評価の対象となるリスクは、情報セキュリティに係るリスクとする。情報セキュリティリスクとは、情報の機密性、完全性、可用性が損なわれる事象の可能性である。

リスク基準は、事象の影響度と発生頻度の組み合わせで表現されることが多い。一例として、影響度を"非常に高い／高い／中間／低い／非常に低い"、発生頻度を"非常に高い／高い／中間／低い／非常に低い"などと各々分類し、両者のマトリクスで結果を整理しリスク基準を決定する方法等がある。

② リスク特定

リスク特定とは、組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し、認識することである。リスク特定を実施するための方法として、保有する資産に着目する方法と、発生する可能性がある事象に着目する方法がある。

- 資産ベースのアプローチ

情報、情報を取り扱う情報システム、情報システムの脆弱性、情報システムへの

脅威を特定し、リスク評価を実施する手法。

- 事象ベースのアプローチ
  情報の機密性、完全性、可用性が損なわれる事象とその結果を特定し、リスク評価を実施する手法。

③ リスク分析

リスク分析とは、特定したリスクに対し、リスクの原因を特定して以下の事項を分析し、リスクのレベルを決定することである。

- 守るべき資産（情報、情報を取り扱う情報システム等）の価値
- その資産に影響を及ぼすおそれのある事象の影響度と発生頻度
- 既存の管理策の有効性

④ リスク評価

リスク評価とは、リスク分析の結果から、対応が必要なリスクを決定し、その優先順位を決定することである。

⑤ リスク対応

リスク対応とは、リスク評価の結果、優先順位が高いリスクから対応方針を決定することである。対応方針は主に以下の４つの方法があり、どのような方針を選択するかは、目的、リスク対応が新たに生み出すリスクの有無、費用対効果等を踏まえ、最善の対応を選択することが望ましい。

- リスク低減：リスクに対して対策基準に定めるべき対策事項を決定する。
  リスク低減には、①影響度の低減 ②発生頻度の低減 ③影響度及び発生頻度の低減の３つの低減策がある。
- リスク回避：リスクを生じさせる活動を開始又は継続しないことを決定することにより、リスクを回避する。
- リスク移転：一つ以上の他者とリスクの全部又は一部を共有する。（契約によるリスクの分散及び保険加入等による金銭面でのリスク対策を含む。）。
- リスク保有：情報に基づく意思決定により、リスクを保有する。

リスクアセスメントに関しては、以下の文献が参考となるので紹介する。

参考：JIS Q 31000:2019 リスクマネジメント－指針

参考：ISO/IEC270005 ISO/IEC27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks 情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティ

参考：JIS Q31010:2022 リスク マネジメント－リスクアセスメント技法（IEC31010:2019,Risk management-Risk assessment techniques）

参考：National Institute of Standards and Technology（NIST、米国国立標準技術研究所）Special Publication 800-30 revision1
（https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000balw.pdf）

参考：ISO/IEC27001 情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項

参考：内閣官房国家サイバー統括室「機能保証のためのリスクアセスメント・ガイドライン 1.0 版」
（https://www.cyber.go.jp/policy/group/cyber/policy.html）

遵守事項

(2) 対策基準の策定

(a) 最高情報セキュリティ責任者は、**情報セキュリティ委員会における審議を経て、統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように対策基準を定める**こと。また、対策基準は、機関等の業務、取り扱う情報、保有する情報システムに関するリスク評価の結果及び**対策基準や対策推進計画の見直し結果を踏まえた上で定める**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.3(2)(a)「情報セキュリティ委員会における審議を経て、統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように対策基準を定める」について**

  対策基準の策定に当たっては、あらかじめ、情報セキュリティ委員会において審議を行うとともに、情報セキュリティの知見を持つ者に意見を求めるなどして、規定内容の網羅性や妥当性等について確認した上で決定することが望ましい。

  また、対策基準は、「統一基準 1.1(5)機関等の対策基準」に記載されている内容に基づき、リスク評価の結果を踏まえ、定期的に見直しの必要性を確認するなど常に最新の状況に適合させることが重要である。

- **遵守事項 2.1.3(2)(a)「対策基準や対策推進計画の見直し結果を踏まえた上で定める」について**

  対策基準等の見直し結果を踏まえ、情報セキュリティ委員会において審議を行うとともに、情報セキュリティの知見を持つ者に意見を求めるなどして、規定内容の網羅性や妥当性等について確認した上で決定することが望ましい。

遵守事項

(3) 運用規程及び実施手順の策定

(a) 統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する運用規程（本統一基準で最高情報セキュリティ責任者が整備すべきとされている場合を除く。）及び実施手順（本統一基準で整備すべき者を別に定める場合を除く。）を整備し、運用規程及び実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告すること。

(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における雇用の開始、終了及び人事異動時等に関する管理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 2.1.3(3)(a)「運用規程（本統一基準で最高情報セキュリティ責任者が整備すべきとされている場合を除く。）及び実施手順（本統一基準で整備すべき者を別に定める場合を除く。）を整備」について**

  統一基準で整備を求めている運用規程及び実施手順は、付録(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」に整理している。

- **遵守事項 2.1.3(3)(a)「運用規程及び実施手順に関する事務を統括」について**

  統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する運用規程及び実施手順について、監査結果を通じて、対策基準に従って整備されていないことを把握した場合には、整備すべき者に対して指導することが想定される。

  また、統括情報セキュリティ責任者は、情報セキュリティ関係規程について自己点検や監査の結果、例外措置の申請状況等を通じ、課題又は問題点について把握し得ることから、運用規程及び実施手順の整備主体が、特定の部門の情報セキュリティ責任者に係るものであったとしても、同種の課題又は問題点の有無を他の部局等に確認することも想定される。

- **遵守事項 2.1.3(3)(b)「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に関する管理の運用規程」について**

  着任又は異動した職員等に対して実施する情報セキュリティ対策に係る教育や人事異動により管理者権限を必要とする職員等が交代する場合の権限設定の変更、職員等の退職等により識別コードを使用する必要がなくなった場合の識別コードの停止に関する運用規程等が想定される。

遵守事項

(4) 対策推進計画の策定

(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、**対策推進計画**を定めること。

【 基本対策事項 】

＜2.1.3(4)(a)関連＞

2.1.3(4)-1 最高情報セキュリティ責任者は、対策推進計画に、機関等の業務、取り扱う情報及び保有する情報システムに関する**リスク評価の結果を踏まえた全体方針**並びに以下に掲げる**取組の方針・重点**及びその実施時期を全て含むよう定めること。ただし、e)は独立行政法人又は指定法人を所管する国の行政機関に限る。

a) 情報セキュリティに関する教育
b) 情報セキュリティ対策の自己点検
c) 情報セキュリティ監査及び過年度の監査結果（本部監査の結果を含む。）を踏まえた取組
d) **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**
e) **所管する独立行政法人及び指定法人のセキュリティ対策の評価及びその推進に資するための取組**
f) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.1.3(4)-2 最高情報セキュリティ責任者は、「対策推進計画策定マニュアル」（内閣官房国家サイバー統括室）を参照して対策推進計画を定め、少なくとも１年に１回、策定した対策推進計画の総合評価を実施し、その結果等からの対策推進計画の見直しを踏まえて、次年度の「全体方針」及び「個別の取組の方針・重点等」を定めること。

（解説）

- **遵守事項 2.1.3(4)(a)「対策推進計画」について**

対策推進計画は、情報セキュリティ対策に関する一連の取組を対象とした全体計画であり、情報セキュリティ対策に関する取組の全体方針のほか、基本対策事項 2.1.3(4)-1 に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を設定し、情報セキュリティ対策を組織的・継続的に改善し、総合的に推進するために定めるものである。

対策推進計画は、機関等が組織として、種々の情報セキュリティ対策をいかなる考え方や方向性に基づいて進めていくのかといった一連の取組全体の大枠について、最高情報セキュリティ責任者があらかじめ総合的に定めるものであり、個々の取組の実施に当たって詳細計画が必要となる場合は、対策推進計画に則して、それぞれの取組の責任者がその権限の下に詳細計画を策定する。

参考：内閣官房国家サイバー統括室「対策推進計画策定マニュアル」

（https://www.cyber.go.jp/pdf/policy/general/sakutei-manual.pdf）

- **基本対策事項 2.1.3(4)-1「リスク評価の結果を踏まえた全体方針」について**

  情報セキュリティ対策は、情報セキュリティを取り巻く様々な脅威、機関等の業務、取り扱う情報及び保有する情報システムの特性等を踏まえ、目的達成の成否等に影響を与える情報セキュリティに係るリスクの分析・評価を行った上で、対策の方針や優先度を判断し、計画的に推進することが重要である。また、情報セキュリティ対策については、限られた予算や人的資源を最大限に活用して、対策全体としての方向付けを行った上で対策基準に策定した個々の対策を実施していくことも重要である。

  全体方針としては、例えば、優先的に対応すべき脅威や優先的に対策を講ずるべき対象を設定し、それらへの対応を重点として掲げることが考えられる。

  また、自組織の目的等を踏まえ、情報セキュリティ対策の自己点検、情報セキュリティ監査、本部監査の結果等を考慮した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講ずることが求められる。

  リスク評価の具体的な進め方については、「（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。

- **基本対策事項 2.1.3(4)-1「取組の方針・重点」について**

  本基本対策事項に掲げる情報セキュリティ対策に関する個々の取組の方針・重点は、全体方針を踏まえ、例えば、情報セキュリティに関する教育において、特定の脅威（例：標的型攻撃、サプライチェーン・リスク）、特定の対象（例：業務の内容や役職に応じた者）、特定の内容（例：対策基準の改正点）を掲げることが考えられる。

- **基本対策事項 2.1.3(4)-1 d)「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」について**

  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としては、政府全体としての取組のほか、機関等において独自に推進している技術的な対策を含めることが望ましい。技術的対策には、情報システムを構成する機器等の更新等の投資による対策も含まれる。

- **基本対策事項 2.1.3(4)-1 e)「所管する独立行政法人及び指定法人のセキュリティ対策の評価及びその推進に資するための取組」について**

  所管する独立行政法人及び指定法人のセキュリティ対策の評価及びその推進に資するための取組については、「（解説）基本対策事項 2.1.1(1)-1 e)「所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制」について」、「（解説）遵守事項 2.5.1(1)(a)「所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備」について」及び「（解説）基本対策事項 2.5.1(1)-1「情報セキュリティ対策が適切に推進されるために必要な体制として、当該法人所管部署等の関係部署及び所管する法人等に必要な助言等を行うための窓口を、当該法人所管部署等の関係部署と連携して整備」について」を参考にするとよい。

2.2 運用

2.2.1 情報セキュリティ関係規程の運用

目的・趣旨

機関等は、対策基準に定められた対策を実施するために定める具体的な運用規程及び実施手順を適切に運用する必要がある。

情報セキュリティ関係規程の運用において、当該規程に係る課題及び問題点を含む運用状況を適時に把握することが重要である。

遵守事項

(1) 情報セキュリティ対策の運用

(a) 情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行すること。

(b) 情報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、職員等から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告すること。

(c) 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.1(1)(a)「最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行」について**

  情報セキュリティ対策推進体制の役割については、遵守事項 2.1.1(6)(a)及び基本対策事項 2.1.1(6)-1 において規定しているが、本項では、情報セキュリティ対策推進体制が規定された役割に従って事務を遂行すべきことを示している。

  当該事務の内容としては、例えば、情報セキュリティ関係規程の運用状況の適時の把握、情報セキュリティ関係規程に関する教育や訓練の実施、自己点検による情報セキュリティ関係規程の遵守状況の調査及び問題点の改善が考えられる。また、情報システムの脆弱性に係る情報や外部のインシデント情報等の情報セキュリティ対策に有用となる情報を入手するとともに、それらを関係機関と共有することも、対策の運用において重要な対応である。

遵守事項

(2) 違反への対処

(a) 職員等は、情報セキュリティ関係規程への重大な違反を知った場合は、**情報セキュリティ責任者にその旨を報告**すること。

(b) 情報セキュリティ責任者は、**情報セキュリティ関係規程への重大な違反**の報告を受けた場合及び自らが重大な違反を知った場合には、**違反者及び必要な者**に**情報セキュリティの維持に必要な措置**を講じさせるとともに、統括情報セキュリティ責任者を通じて、**最高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 2.2.1(2)(a)「情報セキュリティ責任者にその旨を報告」について**

機関等において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉するための事項である。一般的に、機関等においては、違反を知った者はこれを報告する義務が課されており、情報セキュリティ関係規程への違反については、各規定の実施に責任を持つ情報セキュリティ責任者に報告することとなる。本項は、職員等から情報セキュリティ責任者への直接の報告を必須とするものではなく、重大な違反等の有無を情報セキュリティ責任者が確実に認識できるようにすることを求めている。

なお、職員等は、自ら違反した場合に限らず、他の職員等が違反している場合においても、迅速な是正措置を促す理由から、当該職員等への助言に加えて情報セキュリティ責任者に報告するなど適切に対応することが求められる。また、情報セキュリティ関係規程に係る課題及び問題点を認識した場合についても、情報セキュリティ責任者に報告することが望ましい。

- **遵守事項 2.2.1(2)(b)「情報セキュリティ関係規程への重大な違反」について**

情報セキュリティ関係規程への重大な違反とは、当該違反により機関等の業務に重大な支障をきたすもの又はその可能性のあるものをいう。例えば、機密性の極めて高い情報を保存した端末を、許可無く要管理対策区域外に持ち出してしまった場合等が考えられる。

情報セキュリティ責任者は、機関等において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉し、被害の未然防止又は拡大防止のための措置を適切に講じさせるとともに、再発防止に関する取組を進めることが求められる。

- **遵守事項 2.2.1(2)(b)「違反者及び必要な者」について**

情報セキュリティ関係規程への重大な違反があった場合には、違反者自身が対策を講ずることは当然であるが、それ以外の「必要な者」として措置を義務付けられるのは、情報システムセキュリティ責任者、課室情報セキュリティ責任者及び区域情報セキュリティ責任者等の当該規程の実施に責任を有する者が挙げられる。情報システムの運

用者や担当者、委託先等とも協力し、情報セキュリティを維持するために必要な措置を講ずる必要がある。

- **遵守事項 2.2.1(2)(b)「情報セキュリティの維持に必要な措置」について**

  重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、早期解決、拡大防止等の対処を行う。拡大防止としては、情報セキュリティ関係規程について再周知の徹底が考えられる。

- **遵守事項 2.2.1(2)(b)「最高情報セキュリティ責任者に報告」について**

  報告を受けた最高情報セキュリティ責任者は、その内容、結果、業務への影響、社会的評価等を確認し、機関等全体として再発防止を徹底するなど、適切に対応する必要がある。

  また、統括情報セキュリティ責任者は、同様の違反が多発している可能性の有無を考慮し、違反の原因について分析し、必要に応じて情報セキュリティ関係規程の見直しを含めた対策を検討する必要がある。

2.2.2 例外措置

目的・趣旨

例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が業務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

遵守事項

(1) 例外措置手続の整備

(a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査し、許可する者（以下本款において「許可権限者」という。）及び審査手続を定めること。

(b) 統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

【 基本対策事項 】

＜2.2.2(1)(a)関連＞

2.2.2(1)-1 最高情報セキュリティ責任者は、例外措置について以下を全て含む手順を定めること。

a) 例外措置の許可権限者

b) 事前申請の原則その他の申請方法

c) 審査項目その他の審査方法

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置により生じる情報セキュリティ上の影響と対処方法
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

＜2.2.2(1)(b)関連＞

2.2.2(1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、統括情報セキュリティ責任者へ定期的に報告すること。

a) 審査した者の情報（氏名、役割名、所属、連絡先）

b) 申請内容

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間

- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

c) 審査結果の内容

- 許可又は不許可の別
- 許可又は不許可の理由
- 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を許可した期間
- 許可した措置内容（講ずるべき代替手段等）
- 例外措置を終了した旨の報告方法

（解説）

- **遵守事項 2.2.2(1)(a)「例外措置の適用の申請を審査し、許可する者」について**

例外措置の適用の申請を受けた際に適切な審査が実施できるように、許可権限者を定め、審査手続を事前に整備する必要がある。情報セキュリティ関係規程の誤った解釈や恣意的な例外運用を防止するために、例えば、情報セキュリティ関係規程を策定した者を許可権限者に充てることが考えられる。申請の内容に応じて、適切な許可を与えられる者を許可権限者として定めておくことが重要である。

遵守事項

(2) 例外措置の運用

(a) 職員等は、定められた審査手続に従い、許可権限者に規定の**例外措置の適用を申請**すること。ただし、業務の遂行に緊急を要し、当該規定の趣旨を十分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。

(b) 許可権限者は、職員等による**例外措置の適用の申請**を、定められた審査手続に従って**審査**し、許可の可否を決定すること。

(c) 許可権限者は、例外措置の申請状況を台帳に記録し、**統括情報セキュリティ責任者に報告**すること。

(d) 統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた**情報セキュリティ関係規程の追加又は見直しの検討**を行い、最高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 2.2.2(2)(a)「例外措置の適用を申請」について**

職員等は、定められた審査手続に従い例外措置の適用を申請し、許可を得てから例外措置を講ずることが原則であるが、業務の遂行に緊急を要するなどの場合であって、情報セキュリティ関係規程の規定内容とは異なる代替の方法を直ちに採用すること又は規定された対策を実施しないことが不可避のときは、事後速やかに届け出る必要がある。

職員等は、例外措置の適用を希望する場合には、当該例外措置を適用したときの情報セキュリティ上の影響を検討、分析する必要がある。その上で、例外措置の適用が必要であると判断した場合は、その影響を低減させるための補完措置を提案し、適用の申請を行う必要がある。

- **遵守事項 2.2.2(2)(b)「例外措置の適用の申請」・「審査」について**

許可権限者は、例外措置の適用の申請を適切に審査しなければならない。審査に当たっては、申請内容の情報セキュリティ関係規程の該当箇所、期間、措置内容等が、申請する理由と照らして必要最小限の内容となっているか確認した上で、例外措置の適用を許可した場合の情報セキュリティ上の影響と、不許可とした場合の業務遂行等への影響を評価し、その判断を行う必要がある。

例外措置の適用期間が長期にわたる場合等においては、例外措置の実施によるリスクが変化する可能性を踏まえ、定期的に当該措置の適用状況等を許可権限者において把握することも重要である。

- **遵守事項 2.2.2(2)(c)「統括情報セキュリティ責任者に報告」について**

  統括情報セキュリティ責任者は、許可権限者から例外措置の適用状況の報告を受ける。これは、次項で情報セキュリティ関係規程の追加又は見直しの検討を行うためである。

- **遵守事項 2.2.2(2)(d)「情報セキュリティ関係規程の追加又は見直しの検討」について**

  例外措置の適用が多い状況は、例外とはみなせないと考えるべきである。その場合には、代替手段の導入を含め、情報セキュリティ関係規程の見直しを検討する必要がある。

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が職員等に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての職員等が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

また、機関等における近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

遵守事項

(1) 教育体制の整備・教育実施計画の策定

(a) 統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。

(b) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すこと。

【 基本対策事項 】

＜2.2.3(1)(a)関連＞

2.2.3(1)-1 統括情報セキュリティ責任者は、職員等の役割に応じて**教育すべき内容を検討**し、教育のための資料を整備すること。

2.2.3(1)-2 統括情報セキュリティ責任者は、**職員等が毎年度最低１回は教育を受講**できるように、教育実施計画を立案するとともに、その実施体制を整備すること。

2.2.3(1)-3 統括情報セキュリティ責任者は、職員等の着任又は異動後に、**３か月以内に受講**できるように、その実施体制を整備すること。

（解説）

- **基本対策事項 2.2.3(1)-1「教育すべき内容を検討」について**

教育の内容については、最新の脅威動向を考慮した上で、組織において想定すべき脅威や機関等の実状や情報セキュリティインシデントの発生状況等、情報セキュリティ環境の変化、前回の教育の実施状況の分析、評価の結果、自己点検の結果、情報セキュリティ監査の結果等を踏まえ、幅広い角度から検討し、受講者の役割、責任及び技能に適したものにする必要がある。

さらに、教育の内容は、職員等が対策内容を十分に理解できるものとする必要があり、そのためには、網羅的な資料ではなく、理解すべき事項に限定した資料を教育に用いるべきである。例えば、情報セキュリティ関係規程の教育資料の作成においては、遵守事項を遵守すべき者ごとに整理し、職員等が遵守する必要のない事項は、含まないように配慮すべきである。

また、違反の抑止効果を期待することを目的に、ウェブサイトの閲覧に係るログを取得していることや、必要に応じて当該ログを調査することがあること等の情報システムの運用ルールを職員等の教育内容に含めることも考えられる。

このような教育内容の検討に加えて、教育実施後に簡単なテストを実施することにより受講者の理解度を把握したり、受講者にアンケートを記入してもらったりすることで、次回開催のテーマや現在の教育方法等についての改善を検討することも考えられる。

なお、情報セキュリティ対策推進体制を含む情報セキュリティ関係部署の者やCYMAT 及び CSIRT に属する職員等に対して、情報セキュリティに関する知識及び技能を向上させるため、研修及び実務を模擬した訓練を実施することも有効である。訓練内容や実施結果の評価等について、最高情報セキュリティアドバイザーの助言を受けることも有用である。より高度な技能の習得や将来的な脅威への対応等を求めた訓練を実施する場所等においては、外部の専門事業者に委託することにより訓練を実施してもよい。

- **基本対策事項 2.2.3(1)-2「職員等が毎年度最低１回は教育を受講」について**

機関等において情報セキュリティを維持するためには、職員等が常日頃から情報セキュリティの意識を持って業務を遂行する必要があり、そのためには職員等に対して継続的に教育を受講させることが重要である。本基本対策事項では、全ての職員等に対して最低限の教育を受講させることを想定して「毎年度最低１回」と規定しているが、教育の対象が広範である、繰り返し教育する必要があるなどの理由を考慮して、複数回の教育を計画することも考えられる。継続的な教育を実施するに当たっては、国の行政機関や民間企業が提供する研修プログラムや e-learning 等の活用も検討し、実施の効率性や受講のしやすさ等に配慮した上で、計画を策定するとよい。

情報セキュリティ対策推進体制を含む情報セキュリティ関係部局、CYMAT 及び CSIRT に属する職員等のセキュリティ人材に対する教育については、キャリアパスにも配慮し、十分な教育が受けられるよう、計画段階から実施内容や実施時期、手段を考慮する必要がある。

- **基本対策事項 2.2.3(1)-3「３か月以内に受講」について**

着任、異動した職員等に対しては、早期に情報セキュリティ対策の教育を受講させることも有益であり、着任後３か月以内には受講させるべきである。ただし、異動した後に使用する情報システムが、異動前と変わらないなど、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。

遵守事項

(2) 教育の実施

(a) 課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を**適切に受講**させること。

(b) 職員等は、教育実施計画に従って、**適切な時期に教育を受講**すること。

(c) 課室情報セキュリティ責任者は、**情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講**させること。また、国の行政機関における課室情報セキュリティ責任者は、**CYMAT に属する職員にも教育を適切に受講**させること。

(d) 課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告すること。

(e) 統括情報セキュリティ責任者は、**教育の実施状況を分析、評価**し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.3(2)(a)「適切に受講」について**

  課室情報セキュリティ責任者は、職員等に情報セキュリティ対策の教育を受講させる責務があり、職員等に対して教育の実施を周知するとともに、教育を受講しない者に対して受講を勧告するほか、受講状況を把握するなどして、積極的に受講を促すこと等が求められる。また、受講時間を確保するなどの職員等が受講できるための環境を整備するなどの配慮も必要である。

- **遵守事項 2.2.3(2)(b)「適切な時期に教育を受講」について**

  職員等は、教育実施計画に従って、毎年度最低１回は教育を受講することが求められる。

  着任時又は異動時の場合には、新しい職場等で、情報セキュリティ対策の教育の受講方法について課室情報セキュリティ責任者に確認することも求められる。

- **遵守事項 2.2.3(2)(c)「情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講」・「CYMAT に属する職員にも教育を適切に受講」について**

  サイバー攻撃等の情報セキュリティに対する脅威が増大している状況を踏まえ、政府機関が一体となって対処することを目的に CYMAT が整備されているほか、情報セキュリティインシデントに迅速かつ適切に対処するための組織として機関等に CSIRT が整備されている。これらに属する職員等への教育も、その責務に照らすと極めて重要である。

- **遵守事項 2.2.3(2)(e)「教育の実施状況を分析、評価」について**

  より効果的な情報セキュリティに係る教育を実施するためには、終了した教育の実

施状況を組織全体として分析、評価し、教育の実施内容や方法、対象者等を継続的に見直していくことが重要である。また、分析、評価した結果は次回の教育の実施内容や方法等のほか、自己点検の内容に活用することを報告内容に含めることも考えられる。

分析、評価の方法としては、例えば、受講者に演習問題を実施させることで理解度を定量的に把握する方法や、受講者のアンケート回答により改善点等の指摘を受ける方法が考えられる。受講者へアンケートを行う際は、改善すべき点等の有用な情報が得られるよう、具体的な質問をアンケート項目に加えるなどの工夫を考えるとよい。また、自組織において特定の運用規程及び実施手順が守られていないと考えられる場合は、当該運用規程及び実施手順に係る内容を教育に含め、教育実施前後での運用規程及び実施手順の遵守度合いを確認するといった手法で評価を行うことも考えられる。

2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

(a) 統括情報セキュリティ責任者は、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を含む機関等関係者への**報告手順**を整備し、**報告が必要な具体例**を含め、職員等に周知すること。

(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**を整備すること。

(c) 統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む**緊急連絡網**を整備すること。

(d) 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その**訓練の内容及び体制を整備**すること。

(e) 統括情報セキュリティ責任者は、情報セキュリティインシデントについて**機関等外の者から報告を受けるための窓口を整備**し、その窓口への連絡手段を機関等外の者に明示すること。

(f) 統括情報セキュリティ責任者は、**対処手順が適切に機能することを訓練等により確認**すること。

【 基本対策事項 】

＜2.2.4(1)(a)関連＞

2.2.4(1)-1 国の行政機関の統括情報セキュリティ責任者は、所管する独立行政法人及び指定法人における情報セキュリティインシデント発生が報告された際にも、自組織における情報セキュリティインシデントの場合と同様に、最高情報セキュリティ責任者や内閣官房国家サイバー統括室に速やかに報告されるよう手順を定めること。

＜2.2.4(1)(b)関連＞

2.2.4(1)-2 統括情報セキュリティ責任者は、情報セキュリティインシデント発生時の対処手順のうち、**意思決定の判断基準や決定権者、判断に応じた対応内容、緊急時の意思決定方法等**をあらかじめ定めておくこと。

＜2.2.4(1)(e)関連＞

2.2.4(1)-3 国の行政機関の統括情報セキュリティ責任者は、所管する独立行政法人及び指

定法人において発生した情報セキュリティインシデントについて、当該法人から報告・連絡を受ける窓口について定めるとともに、各法人にその窓口の連絡先を周知すること。

（解説）

- **遵守事項 2.2.4(1)(a)「報告手順」について**

報告手順として明記すべき事項としては、情報セキュリティインシデントの可能性が認知されてから最高情報セキュリティ責任者に報告するまでの具体的な手順等が考えられる。

また、情報セキュリティインシデントの可能性の報告窓口については、報告手順の中で明確にするほか、情報セキュリティ対策の教育の中で周知する、報告窓口の連絡先を執務室内に掲示するなどして、緊急時に職員等が速やかに報告できるようにする必要がある。

報告窓口を CSIRT とは異なる部門に設ける場合は、当該部門から CSIRT への報告が速やかに実施される体制にすることが求められる。

なお、政府共通利用型システム利用機関における当該政府共通利用型システムに係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にあっては、基本対策事項 5.4.2(3)-1 c)のとおり、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て、政府共通利用型システム利用管理者が実施手順を定める必要がある。

- **遵守事項 2.2.4(1)(a)「報告が必要な具体例」について**

統括情報セキュリティ責任者は、職員等に対し、情報セキュリティインシデントである可能性を認知した段階で報告を求める必要がある。例えば、不審な電子メールの添付ファイルを開く、URL リンクをクリックするなどした場合や、機密性の高い情報を保存したモバイル端末の所在が不明であるが、紛失したことや盗難されたことが確定的でない場合、平常時の情報システムの利用において確認されないはずのエラーメッセージが端末に表示された場合等が想定される。

- **遵守事項 2.2.4(1)(b)「対処手順」について**

対処手順として情報セキュリティインシデントの認知時において緊急を要する対処等の必要性に備えて、通常とは異なる例外的な承認手続を定めておくことも併せて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなことがないよう検討すること。

なお、インシデント対応自動化技術である SOAR（Security Orchestration, Automation and Response）を機関等 LAN システムのように情報セキュリティインシデント対応を一部自動化することによるメリットの大きい情報システムに導入することが考えられるが、この場合、対処手順もこれに対応したものとする必要があることに留意が必要である。また、政府共通利用型システム利用機関における当該政府共通利用型システムに係る対処手順にあっては、基本対策事項 5.4.2(3)-1 c)のとおり、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て、政府共通利用型システム

利用管理者が実施手順を定める必要がある。

- **遵守事項 2.2.4(1)(c)「緊急連絡網」について**

  統括情報セキュリティ責任者は、通常時の全ての情報セキュリティ関連の責任者及び管理者の連絡網の整備に加えて、情報セキュリティインシデントを認知した場合に速やかに対処するための「緊急連絡網」を整備する必要がある。

  緊急連絡網には、該当する職員等に支給したスマートフォンや携帯電話の番号等を記載するほか、自宅や機関等支給以外のスマートフォンや携帯電話の番号等を含むことも考えられる。また、緊急連絡網には当該情報システムに係る責任者、管理者（当該情報システムの運用・保守事業者を含む。）及びクラウドサービス事業者並びに GSOC の窓口等のほか、重大な情報セキュリティインシデントに備えて最高情報セキュリティ責任者も含める必要がある。

- **遵守事項 2.2.4(1)(d)「訓練の内容及び体制を整備」について**

  実際に情報セキュリティインシデントへの対処を模擬的に行うことにより、対処能力を向上させるために実施する訓練の内容及び体制の整備を求める事項である。

  対処能力を向上させるための訓練としては、業務の遂行のために特に重要と認めた情報システムでは、不正プログラム感染による情報漏えいやサービス不能攻撃によるシステム停止などへの対処を的確に実施できることが重要であると考えられることから、それらの情報セキュリティインシデントを想定した模擬的な対処を行う内容とすることが望ましい。

  また、実効的な訓練を実施するためには、情報システム部門だけでなく、情報セキュリティインシデントに関する報告窓口となる部門、情報セキュリティ対策推進体制や CSIRT も参加することが望ましい。

- **遵守事項 2.2.4(1)(e)「機関等外の者から報告を受けるための窓口を整備」について**

  例として、外部の者が機関等の情報セキュリティ対策の不備を発見した場合、機関等への攻撃のおそれ等を認知した場合、機関等外の者に情報セキュリティ上の脅威を与えていることを認知した場合（与えるおそれがある場合を含む。）等に、機関等外の者から連絡を受ける体制を整備することを求めている。

- **遵守事項 2.2.4(1)(f)「対処手順が適切に機能することを訓練等により確認」について**

  情報セキュリティインシデントは定常的に発生するものではないが、実際に発生した場合には、機関等の業務に大きな影響をもたらすおそれがあるため、迅速かつ的確に対処を行うことが求められる。そのため、定めた対処手順が適切に機能することを訓練等によって確認し、必要に応じて見直しを行うことが重要である。

  訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を受けて判断等を行う「ロールプレイング」、状況設定の上で手順の検証を行う「シミュレーション」といった大掛かりなもののほか、より簡易な「ウォークスルー」や「机上チェック」といった手法も存在する。CSIRT の取組状況や職員等の習熟度等に応じて、必要な訓練等を検討し実施することが望まれる。また、SOAR を導入している場合は、情報システムの保守や運用を業務委託している事業者も含め、詳細な粒度での訓練とする

ことが望ましい。

- **基本対策事項 2.2.4(1)-2「意思決定の判断基準や決定権者、判断に応じた対応内容、緊急時の意思決定方法等」について**

  例えば、機関等 LAN システム内での不正プログラム感染拡大やそれに伴う情報流出等が疑われる場合には、被害の拡大を阻止する措置を直ちに講ずることが重要である。そのような場合において、情報の重要度、情報が失われた場合のリスク、業務継続方法等を勘案した上で、調整等に時間をかけず直ちにネットワークを遮断する、特定のサーバを停止するなどの措置を講ずるため、その手続や対象範囲、判断基準、決定権者等を事前に定めておくことが考えられる。これらの基準や手続は、機関等を取り巻くサイバー攻撃事例や情報セキュリティインシデント事例を基に、適時見直すことが求められる。

遵守事項

(2) 情報セキュリティインシデントへの対処

(a) 職員等は、**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には、機関等の報告窓口に報告**し、指示に従うこと。

(b) CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

(c) CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、**最高情報セキュリティ責任者に速やかに報告**すること。

(d) CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための**応急措置の実施及び復旧に係る指示又は勧告**を行うこと。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システムセキュリティ責任者へ確認を指示すること。

(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について情報セキュリティインシデントを認知した場合には、**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、適切に対処すること。

(f) 政府共通利用型システム利用機関の情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが政府共通利用型システムに関するものである場合には、当該政府共通利用型システムの情報セキュリティ対策に係る運用管理規程に従い、適切に対処すること。

(g) CSIRT は、認知した情報セキュリティインシデントが**サイバー攻撃又はそのおそれのあるもの**である場合には、**警察への通報・連絡等**を行うこと。

(h) CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、**対処全般に関する指示、勧告又は助言**を行うこと。

(i) CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。

(j) CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。

【 基本対策事項 】

＜2.2.4(2)(d)関連＞

2.2.4(2)-1 CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、情報セキュリティインシデント対処中にあっても、必要に応じて、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局において事前に定められた役割分担を随時見直すこと。

（解説）

- **遵守事項 2.2.4(2)(a)「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には、機**

関等の報告窓口に報告」について

職員等に、情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れ等につながるため、その可能性を認知した段階で報告を求める必要がある。報告窓口に報告する内容には、情報セキュリティインシデントの防止策を無効化したり、すり抜けられたりすることにより、被害に至らないまでも蓋然性が高まった状態も含まれる。

- **遵守事項 2.2.4(2)(c)「最高情報セキュリティ責任者に速やかに報告」について**

情報セキュリティインシデントの性質上、全ての状況が判然とするまでに時間がかかるものであるため、一度の報告で完了することはまれである。例えば、未確定情報を含んだ状態で第一報として報告し、その後に第二報、第三報と続けるような、適切な頻度で報告内容を更新する報告運用が望ましい。その場合、何が確定し、何が未確定であるのかを明らかにすることが望ましい。全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

- **遵守事項 2.2.4(2)(d)「応急措置の実施及び復旧に係る指示又は勧告」について**

応急措置や復旧に当たっては、情報セキュリティインシデントが発生した情報システムの停止、ネットワークの遮断、特定のサーバの停止、職員等への注意喚起等について、被害の拡大可能性、証拠保全、業務継続等を勘案し、CSIRT 責任者の判断で指示又は勧告をする。この場合には、情報セキュリティ対策推進体制が CSIRT 責任者の指示又は勧告を支援することが望ましい。

なお、応急措置や復旧に関して、事前に決められた手順がある場合はその手順に従うことが求められる（「(解説) 基本対策事項 2.2.4(1)-2「意思決定の判断基準や決定権者、判断に応じた対応内容、緊急時の意思決定方法等」について」を参照のこと。）。

- **遵守事項 2.2.4(2)(e)「機関等で定められた対処手順」について**

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、基本対策事項 5.4.1(1)-1 b)で運用管理規程に定める対処手順に従う必要もあるが、政府共通利用型システム利用機関の影響の拡大を防止するため、政府共通利用型システム利用機関への速やかな情報共有と緊密な連携が求められる。

また、機関等で管理する情報システムの情報システムセキュリティ責任者は、情報セキュリティインシデント対処時、特にランサムウェア攻撃等を受けた直後の応急措置や復旧作業において、機器のバージョンアップ（ファームウェア更新等）や初期化、OS の再インストールを行う際にはログの保全等について留意すること。

具体的には、ログが記録されている領域を含め、現状のデータを可能な限り物理的・論理的に保全（バックアップ、スナップショット、ディスクイメージの取得等）した上で作業を開始する。特にネットワーク機器（VPN 装置、ファイアウォール等）のログは揮発しやすい、あるいはアップデートにより上書きされる可能性があるため、作業前に外部へ退避させる手順を事前に整備することが望ましい。

- **遵守事項 2.2.4⑵(g)「サイバー攻撃又はそのおそれのあるもの」について**

サイバー攻撃の例としては、不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス攻撃、サービス不能攻撃等が挙げられる。また、「そのおそれのあるもの」とは、明らかなサイバー攻撃の痕跡が発見されていなくても、単なる機器の故障や操作上の誤りではなく、サイバー攻撃により発生した情報セキュリティインシデントであることが疑われる場合のことである。

- **遵守事項 2.2.4⑵(g)「警察への通報・連絡等」について**

「通報・連絡等」の内容としては、相談、届出、告訴又は告発を想定している。

サイバー攻撃又はそのおそれがある情報セキュリティインシデントが発生した場合、当該サイバー攻撃等による被害の拡大を防止するとともに、攻撃者を追跡するため、警察が的確に初動措置を講ずる必要があることから、可能な限り速やかな通報・連絡等を求めている。

なお、その通報先は、各都道府県警察のサイバー攻撃対策部門であり、具体的には、警視庁では公安部の警視庁サイバー攻撃対策センター、道府県警察では警備部のサイバー攻撃対策担当課である。また、警察への通報に関する質問等については、警察庁サイバー警察局サイバー企画課において受け付けている。

- **遵守事項 2.2.4⑵(h)「対処全般に関する指示、勧告又は助言」について**

機関等における情報セキュリティインシデント発生時の対処として、以下のプロセスが想定される。CSIRT には、これらの対処が迅速かつ的確に行われるように、対処状況を把握し、必要に応じて指示、勧告又は助言を行うことが求められる。

- 検知／連絡受付
  - 情報セキュリティインシデントの可能性の報告受付
- トリアージ
  - 報告された情報セキュリティインシデントの可能性に関する状況確認
  - 状況確認結果に基づく情報セキュリティインシデントであるか否かの評価
  - 対処する情報セキュリティインシデントの優先順位付け(事案が多発している場合等)
- インシデントレスポンス
  - 応急措置の実施
  - 証拠保全
  - 被害規模・範囲等の特定を含む状況分析
  - 関係部局、セキュリティベンダ等の外部組織、CYMAT 等への支援要請
  - 復旧対応の実施
  - 情報セキュリティインシデントの原因調査と原因が生じた理由の究明
  - 再発防止策の検討
- 報告／情報公開
  - 最高情報セキュリティ責任者への報告
  - 内閣官房国家サイバー統括室又は所管する国の行政機関への連絡
  - 警察等の関係組織への通報・連絡・報告等

－ 報道発表等の対外対応

上記プロセスのうち、被害規模・範囲等の特定を含む状況分析は、米国 CISA（Cybersecurity and Infrastructure Security Agency）Cybersecurity Incident & Vulnerability Response Playbooks（以下、「CISA インシデント対応プレイブック」という。）に参考となる調査・分析すべきいくつかの攻撃手法をまとめた表（表 2.2.4-1 参照）があるので記載する。この表を参考に調査・分析するログ等を検討するとよい。

表 2.2.4-1　攻撃者の戦術、攻撃手法と関係するログやイベントの例（CISA インシデント対応プレイブックの Table 1: Example Adversary Tactics, Techniques, and Relevant Log and Event Data（内閣官房国家サイバー統括室訳）による）

戦術	一般的な攻撃手法	ログやイベントのソース	サイバー攻撃の痕跡
初期アクセス	・ フィッシング ・ ドライブバイ攻撃 ・ 外部公開されたアプリケーションへのエクスプロイト ・ 外部リモートサービス	・ E メール、ウェブプロキシ、サーバアプリケーションログ ・ IDS/IPS	フィッシングサーバ、リダイレクトサーバ、ペイロード（悪意のあるコードを実施するための）サーバ（ドメインや IP アドレス）、配信メカニズム（ルアー（フィッシングサイトで誘導するための疑似餌）、マクロ、ダウンローダー、ドロッパー等）、漏えいした認証情報、ウェブシェル
実行	・ コマンドとスクリプトインタプリタ ・ クライアント実行のための脆弱性悪用	・ ホストイベントログ ・ Windows イベントログ ・ Sysmon、アンチマルウェア、EDR、PowerShell ログ	コマンドやスクリプトインタプリタの呼び出し、エクスプロイト、API コール、ツール、マルウェア、ペイロード（悪意のあるコード）
永続化	・ アカウントの不正操作 ・ スケジュールされたタスク・ジョブ ・ 有効なアカウントの悪用	・ ホストイベントログ ・ 認証ログ ・ レジストリ	スケジュールされたタスク レジストリキー、オートラン（自動実行プログラム）　等
水平展開	・ リモートサービスの悪用 ・ リモートセッションハイジャック ・ ソフトウェア配布ツールの悪用	・ 内部ネットワークログ、ホストイベントログ ・ アプリケーションログ	ユーザとアプリケーション/認証情報の不一致、ワークステーションからワークステーションへの通信、インターネットへのアクセスを意図しないホストからのビーコン　等
認証情報アクセス	・ ブルートフォース ・ 認証プロセスの変更 ・ 中間者攻撃（Man-in-the-Middle）	・ 認証ログ ・ ドメインコントローラログ、ネットワークトラフィック監視	LSASS 読み込み、LSASS アクセスのコマンド又はスクリプトインタプリタ　等
C2（C&C）	・ アプリケーション層プロトコルの悪用 ・ プロトコルトンネリング	・ ファイアウォール、ウェブプロキシ、DNS、ネットワークトラフィック、クラウドアクティビティログ ・ IDS/IPS	C2 ドメイン、IP アドレス
持ち出し	・ C2 チャネルを介した持ち出し ・ 代替プロトコルを介した持ち出し	・ ファイアウォール、ウェブプロキシ、DNS、ネットワークトラフィック、クラウドアクティビティログ ・ IDS/IPS	ドメイン、URL、IP アドレス、IDS/IPS シグネチャ

なお、上記インシデントレスポンスにおいては、一部業務を外部事業者に請け負わせることも考えられる。このとき、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、関連する規定にも留意が必要である。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」（うちデジタルフォレンジックサービスに係る部分）を活用することが考えられる。

参考：経済産業省「情報セキュリティサービス基準」
（https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html）

参考：情報処理推進機構（IPA）「情報セキュリティサービス基準適合サービスリスト」
（https://www.ipa.go.jp/security/service_list.html）

遵守事項

(3) 情報セキュリティインシデントに係る情報共有

(a) 国の行政機関における CSIRT は、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房国家サイバー統括室に連絡すること。また、独立行政法人及び指定法人における CSIRT は、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関における CSIRT は、当該事象について速やかに、内閣官房国家サイバー統括室に連絡すること。

(b) 国の行政機関における CSIRT は、認知した情報セキュリティインシデント又は独立行政法人及び指定法人から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「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）」に基づく報告連絡を行うこと。

(c) CSIRT は、情報セキュリティインシデントに関して、機関等を含む関係機関と情報共有を行うこと。

(d) 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告を行うこと。

【 基本対策事項 】

＜2.2.4(3)(c)関連＞

2.2.4(3)-1 CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、自機関の関係する者や他の機関等と情報共有を行うこと。

（解説）

- **遵守事項 2.2.4(3)(a)「当該機関の情報システム」について**

  当該情報システムが政府共通利用型システムである場合、当該利用機関においては、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基づく必要がある。

- **遵守事項 2.2.4(3)(a)「情報セキュリティインシデントを認知した場合」について**

  情報セキュリティインシデントを認知した場合のほか、情報システムの運用・保守事業者（情報システムで利用しているクラウドサービスのクラウドサービス提供者を含む。）その他信頼性が高いと考えられる情報提供者から情報セキュリティインシデントのおそれがある情報セキュリティに係る事象の情報提供があった場合において、当該事象が重大な情報セキュリティインシデントに該当する可能性がある場合は、情報セキュリティインシデントと認知する前の段階も含むものとする。

- **遵守事項 2.2.4(3)(a)「速やかに」について**

内閣官房国家サイバー統括室への連絡の目数の目安としては、国の行政機関における CSIRT が当該情報セキュリティインシデントを認知した日から概ね 5 日以内とする。

また、独立行政法人及び指定法人においては、当該法人における CSIRT が当該情報セキュリティインシデントを認知した日から概ね 5 日以内（当該法人を所管する国の行政機関を経由）とする。

ただし、いずれの場合においても、重大な情報セキュリティインシデントと考えられる場合は直ちにとする。

- **遵守事項 2.2.4(3)(a)「内閣官房国家サイバー統括室に連絡」について**

内閣官房国家サイバー統括室への連絡内容としては、以下が考えられる。

- 情報セキュリティインシデントが発生した部署
- 公表の有無
- 他部署への被害波及の可能性
- 影響範囲（業務や国民等への影響）
- 発生日時とその内容
- サイバー脅威の分析に資する情報（機器やソフトウェアのバージョン、IoC やログ、デジタルフォレンジック結果等）
- 復旧状況及び復旧見込み

連絡方法については、「(解説) 遵守事項 2.2.4(2)(c)「最高情報セキュリティ責任者に速やかに報告」について」と同様の頻度で連絡内容を更新することが望ましく、全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

サイバー脅威が我が国の国民生活・経済活動、ひいては国家安全保障に深刻な影響を及ぼすおそれが高まる中、我が国が戦後最も厳しく複雑な安全保障環境に直面する中で、地政学的緊張を反映したサイバー空間を取り巻く情勢は、近年、一層深刻化しており、国家を背景とした組織化・洗練化されたサイバー攻撃は、我が国にとっても現に直面する安全保障上の深刻な脅威となっている。

このような厳しいサイバー安全保障情勢に柔軟かつ適切に対応していくため、「サイバーセキュリティ戦略 （令和 7 年 12 月 23 日閣議決定）において、サイバー安全保障分野における情報収集、とりわけ国家を背景としたアクター等、サイバー攻撃の攻撃者側に関する情報収集・分析能力を一層強化するとともに、国家を背景とした攻撃を含め巧妙化・高度化するサイバー攻撃からサイバー空間を守るため、司令塔の役割を担う国家サイバー統括室が中心となって、能動的サイバー防御を含む多様な手段を組み合わせることで、被害が生じる前の脅威の未然排除、事案発生後の的確な対処を含め、安全保障の観点も踏まえた実効的な防御・抑止に向けた取組を進めていくこととされている。

そのため、分析に有用なあらゆる情報を国家サイバー統括室に集約していくために、政府機関等において発生したサイバー攻撃の疑いがある情報セキュリティインシデント（例えば、不正アクセス、マルウェア感染等）が発生した際には、当該整理・分析に資する情報を収集する必要がある。ここでいう連絡を求める「IoC」は、不正アクセス

元・先の IP アドレスやマルウェアのハッシュ値等が含まれ、「デジタルフォレンジック結果」には、情報システムへの不正アクセスの方法や情報システム内での詳細な侵害状況等が含まれる。

- **遵守事項 2.2.4(3)(b)「「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）」に基づく報告連絡」について**

国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれがある緊急事態に際して政府一体となった初動対処体制をとる必要があることから、内閣官房副長官補（事態対処・危機管理担当）付等に関連情報等を迅速に報告連絡することとしている。

- **遵守事項 2.2.4(3)(c)「情報共有を行う」について**

情報セキュリティインシデントに関して、被害拡大防止のため、関連する可能性のある関係機関と情報共有を行うことが重要である。例えば、自組織で発生した情報セキュリティインシデントについて調査した結果、他の関係機関においても同様の情報セキュリティインシデントの可能性がある場合には、それらの関係機関と情報を共有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ではないと評価した場合であっても、注意喚起等が必要と考えられる場合は、同様に情報共有が重要である。

なお、国の行政機関については、情報共有に関し、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）において、「各府省庁は、その業務において得たサイバー攻撃に係る情報を、可能な限り速やかに内閣官房情報セキュリティセンターに連絡する。また、内閣官房情報セキュリティセンターは、収集・集約された情報をサイバー攻撃に対する初動対処、被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う」と記載している。

- **遵守事項 2.2.4(3)(d)「必要に応じて個人情報保護委員会へ報告を行う」について**

一定の要件に該当する個人情報・特定個人情報の漏えい等が発生した場合は、個人情報保護委員会への報告及び本人への通知が義務付けられている。報告者や報告が必要となる要件については、「個人情報の保護に関する法律」（平成 15 年法律第 57 号）又は「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年法律第 27 号）を参照すること。

なお、本遵守事項は報告を CSIRT が実施することを求めているものではない。

遵守事項

(4) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに**再発防止策を検討**し、それを報告書として最高情報セキュリティ責任者に報告すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、**再発防止策を実施するために必要な措置**を指示すること。

(c) CSIRT 責任者は、情報セキュリティインシデント対処の結果から**得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有**すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.4(4)(a)「再発防止策を検討」について**

一般に、再発防止策を定めるには、組織の体制や当該情報システムの運用管理体制や利用手順、情報システム調達時の要件定義や受入テスト結果等を踏まえて上流工程での対応状況等を遡って確認することも含め、十分な原因調査が必要となる。原因調査により、どのような要素が絡んで情報セキュリティインシデントに至ったのか、因果関係を明らかにした上で、原因から情報セキュリティインシデントの発生段階の間で、因果関係の進行を断ち切るための防護策を複数検討し、講ずることが有効である。また、対策については、情報セキュリティインシデントが発生したシステム単独で講ずるよりも、他のシステムにも同様に展開することにより（水平展開）、類似事案の発生を組織全体にわたって食い止めることが可能となる。

なお、水平展開については、自らの組織の再発防止策に限らず、他組織の事案を参照することにより、事後対処よりも先んじた未然防止が可能となり、対応コストの低減も期待される。

さらに、再発防止策は、情報システムの利用手順で対策する方法及び情報システムへの情報セキュリティ機能の実装による対策を情報システムセキュリティ責任者へ求める方法の両面から検討し、必要な対策を定めて実施する必要がある。情報システムへの情報セキュリティ機能の実装には一定の時間を要することも考えられることから、利用手順による対策を暫定的に実施し、その後、機能追加により本格的な対策を行うなど段階的な実施も考慮する必要がある。

- **遵守事項 2.2.4(4)(b)「再発防止策を実施するために必要な措置」について**

最高情報セキュリティ責任者は、情報セキュリティインシデントの再発防止策の報告を受けた場合は、その内容を確認する必要がある。

情報システムへの情報セキュリティ機能の実装等計画的に実施する必要がある再発

防止策については、対策推進計画に反映させるなどして、適切に実施させるよう取組を推進することが求められる。また、機関等全体として再発防止策を講ずることが有効と想定される場合は、機関等全体での取組を進めることも求められる。

情報セキュリティインシデントに係る再発防止策を策定する際には、デジタルフォレンジック結果や攻撃者の詳細な挙動に関する事項に基づく技術的検討を行い、機能・運用の改善点を明らかにしたうえで、再発防止策を策定することが必要である。

- **遵守事項 2.2.4(4)(c)「得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有」について**

  CSIRT 責任者には、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に対し、単に情報セキュリティインシデントの情報を共有するだけでなく、情報セキュリティインシデントの対処を踏まえ、統括情報セキュリティ責任者が定める対処手順等の改善や、個別の情報システムの情報セキュリティ水準の改善につなげられるような事項を含めて共有することが求められる。

2.3　点検

2.3.1　情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、職員等が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

(1)　自己点検計画の策定・手順の準備

(a)　統括情報セキュリティ責任者は、対策推進計画に基づき**年度自己点検計画を策定**すること。

(b)　情報セキュリティ責任者は、年度自己点検計画に基づき、**職員等**ごとの**自己点検票**及び自己点検の実施手順を整備すること。

(c)　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(1)(a)「年度自己点検計画を策定」について**

  点検を実施するに当たり、対策推進計画に基づき適切に実施するため、実施頻度、実施時期、確認及び評価の方法や自己点検項目等を定めた年度自己点検計画を策定することが求められる。

  自己点検項目の選定に当たっては、最新の脅威動向を踏まえた想定すべき脅威に鑑みた項目や、情報セキュリティインシデントの発生状況に鑑みた項目、前年度の自己点検実施率が低かった遵守事項、情報セキュリティ監査の結果を踏まえた項目、教育の実施状況の分析、評価の結果を踏まえた項目等、様々な選択肢が考えられる。

- **遵守事項 2.3.1(1)(b)「職員等」について**

  本条における「職員等」には、情報セキュリティ責任者、課室情報セキュリティ責任者及び情報システムセキュリティ責任者等、情報セキュリティ対策の体制ごとの責任者を含む。具体的にどの責任者を対象に自己点検を実施するかについては、年度自己点

検計画で策定する。

情報セキュリティ責任者や課室情報セキュリティ責任者は、自組織の情報セキュリティ対策や業務委託先に求める情報セキュリティ対策、クラウドサービスを利用する際の情報セキュリティ対策について、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、区域情報セキュリティ責任者は、所管する区域における情報セキュリティ対策について実施するなど、役割に応じて異なることに留意が必要である。

なお、情報システムセキュリティ責任者の点検は、情報システムに係る各種セキュリティ対策の実施状況等を様々な観点で実施する必要がある。例えば、ソフトウェアの脆弱性への対処状況の点検であれば、セキュリティパッチや不正プログラム定義ファイルの更新状況を把握したり、実際の文書を確認したりするなど、代替の確認方法を含めた点検が考えられる。

- **遵守事項 2.3.1(1)(b)「自己点検票」について**

職員等が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、情報セキュリティ責任者は、職員等ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することが重要である。

遵守事項

(2) 自己点検の実施

(a) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示すること。

(b) 職員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(2)(a)「自己点検の実施」について**

  自己点検は、年に２度以上の頻度で実施することが望ましい。例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては、半年に一度の頻度で実施するなどが考えられる。

遵守事項

(3) 自己点検結果の評価・改善

(a) 情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を統括情報セキュリティ責任者に報告すること。

(b) 統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を最高情報セキュリティ責任者に報告すること。

(c) 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受けること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(3)(a)「自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価」について**

情報セキュリティ責任者が自己点検の結果を分析、評価する際は、自らが担当する組織のまとまり、取り扱う情報等の特性に応じた課題や、改善すべき点があるか否かを確認する必要がある。例えば、職員等に求める安全管理措置のうち、特定の措置が実施できていないなどの課題の有無について、点検結果を分析して確認し、課題があることが判明した場合は、執務室の物理的条件、業務用システムの配備状況等の執務環境面も含めて原因分析を行う必要がある。原因分析の結果、速やかに改善すべきものがある場合は、自らの判断で措置が可能なものについては改善措置を講じた上で、その内容を含めて統括情報セキュリティ責任者へ報告することが望ましい。

また、自己点検の実施内容が、自らが担当する組織のまとまりに対して適切であったか否かについて評価を行い、その結果を報告内容に含めることも重要である。例えば、情報の運搬に係る事務が多い職場において、重要な情報を紛失するなどのインシデントが発生しているにもかかわらず、情報の運搬に係る自己点検が項目に含まれていないなど、自己点検の実施内容について改善が必要と考えられる場合は、その旨を報告内容に含め、次回の自己点検において考慮されるようにすることが考えられる。

- **遵守事項 2.3.1(3)(b)「機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価」について**

統括情報セキュリティ責任者が自己点検の結果を分析、評価する際は、機関等で共通的な課題や、改善すべき点があるか否かを確認する。例えば、複数の組織のまとまりにおいて同じ運用規程及び実施手順が守られていないことが判明した場合は、当該運用規程及び実施手順自体に問題がないか分析し、運用規程及び実施手順を見直す必要性を検討するなどして、その結果を最高情報セキュリティ責任者へ報告する。

また、自己点検の評価については、点検項目の選択の適切性や、組織のまとまりごとに適切な自己点検が実施されたか否かなどの観点で実施し、次回の年度自己点検計画の策定の際に参考にするとよい。さらに、分析、評価した結果は教育の実施内容や方法等に活用することも考えられる。

2.3.2 情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。機関等において実施する情報セキュリティ監査は、業務や情報システムへの理解度が高く、効率的に監査の深掘りができ、組織の情報セキュリティ対策の改善に係る PDCA サイクルを円滑に機能させるためにも重要である。

また、監査の結果で明らかになった課題を踏まえ、最高情報セキュリティ責任者は、情報セキュリティ責任者に指示し、必要な対策を講じさせることが重要である。

遵守事項

(1) 監査実施計画の策定

(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。

(b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定めること。

【 基本対策事項 】

＜2.3.2(1)(a)関連＞

2.3.2(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

a) 監査の目的（例：情報セキュリティ対策の実際の運用が情報セキュリティ関係規程に準拠していること等）

b) 監査の対象（例：監査の対象となる組織、情報システム、業務等）

c) 監査の方法（例：情報セキュリティ対策の運用状況を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、対策基準及び運用規程・実施手順とする。）

d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名）

e) 監査の実施時期（例：対象ごとの実施時期）

2.3.2(1)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足している場合等においては、機関等外の者に監査の一部を請け負わせること。

（解説）

- **遵守事項 2.3.2(1)(a)「対策推進計画に基づき監査実施計画を定める」について**

遵守事項 2.1.3(4)(a)に規定する対策推進計画には、監査の基本的な方針として、重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にす

る）・監査の実施時期・監査業務の管理体制等を簡潔に記載することを想定している。監査の基本的な方針の案は、情報セキュリティ監査責任者が作成することを想定している。また、情報セキュリティ監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。被監査部門に対しては、監査実施期間、監査実施者の氏名、監査対象等を含む事項を、情報セキュリティ監査責任者より事前通知し、監査の内容や範囲を事前に明確にすることが望ましい。

なお、内閣官房国家サイバー統括室の「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」は、監査実施計画の策定における考え方や計画に含めるべき内容等を具体的に示しており、これを参考に計画を策定するとよい。この他にも、経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver2.0」等にも詳細が説明されているので、併せて参考にするとよい。

参考：内閣官房国家サイバー統括室「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」
（https://www.cyber.go.jp/pdf/policy/general/R7_AuditManual.pdf）

参考：経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver2.0」
（https://www.meti.go.jp/policy/netsecurity/is-kansa/IS_Audit_Annex12.pdf）

- **遵守事項 2.3.2(1)(b)「追加の監査実施計画を定める」について**

機関等内外において注目すべき情報セキュリティインシデントが発生した場合は、機関等の実態を把握するため、追加的な監査を行い、必要な措置を講ずることが想定される。また、情報セキュリティ対策の実施内容に大きな変更が生じた場合は、その対策の実施状況を把握するために追加で監査を行うことも考えられる。このように、情報セキュリティ監査責任者は、対策推進計画に基づき策定した監査実施計画以外の事項についても、必要に応じて監査実施内容に含めることを考慮する必要がある。

- **基本対策事項 2.3.2(1)-1 b)「監査の対象」について**

監査の対象を検討する際は、以下の情報を参考に検討することが考えられる。

- 機関等内で発生した情報セキュリティインシデントの再発防止・教訓
- 機関等における教育の実施状況に関する分析・評価結果
- 機関等における自己点検結果の分析・評価結果
- 過去の情報セキュリティ監査の結果
- 本部監査の結果
- 外部の勉強会や研修で得られた知見
- 最新の脅威動向に関する情報

また、監査の対象例と監査の対象に合わせた監査内容例は以下のとおりであり、機関等の実情に応じて検討すること。

- 情報セキュリティ対策推進体制を監査対象とした場合
  最高情報セキュリティ責任者や統括情報セキュリティ責任者等が担う役割を対

象に、情報セキュリティ関係規程の運用が適切に行われていることを確認する。

対策基準に統一基準を満たすための適切な事項が定められていることを確認する。

運用規程及び実施手順が対策基準に準拠していることを確認する。

- 特定の業務を監査対象とした場合

業務に関与する部門、取り扱う情報、使用する情報システムについて、業務手順の観点から情報セキュリティ関係規程の運用が適切に行われていることを確認する。

- 特定の部門を監査対象とした場合

部門で取り扱う情報、利用する情報システムについて、当該部門の職員等により情報セキュリティ関係規程の運用が適切に行われていることを確認する。

- 特定の情報システムを監査対象とした場合

情報システムの情報セキュリティ対策について、情報セキュリティ関係規程で規定されている情報セキュリティ対策が講じられていること、及び実際に運用されていることを確認する。

- 特定の情報セキュリティ対策を監査範囲とした場合

最新のサイバーセキュリティに関する脅威動向、インシデント事例、様々な情報セキュリティ技術の普及等を踏まえ、以下に示す例のように、セキュリティリスクの高い範囲に監査を限定し、複数の情報システムへ監査を同時に実施する。

  - 情報システム関連文書の整備状況
  - インターネットに接続する認証機能での多要素主体認証の導入
  - アクセス制御機能の適切な運用
  - 管理者権限を持つ主体の識別コード及び主体認証情報に関する管理
  - ソフトウェアに関する脆弱性対策の実施
  - 情報システムの情報セキュリティに影響する各種設定情報
  - 不正アクセスへの対策状況

- **基本対策事項 2.3.2(1)-1 c)「監査の方法」について**

監査を実施するに当たっての監査技法の例を以下に示す。監査対象や監査テーマに応じて効果的な技法を実施することで監査品質を向上できるが、監査の作業負荷に留意が必要である。

- 監査対象の組織の職員等への質問（ヒアリング）
- 記録文書等やシステム設定等の査閲（レビュー）
- 執務室、サーバ室等の観察（視察）
- 監査人自らが監査対象の組織で実施される運用を試行することによる情報セキュリティ対策の運用状況の評価（再実施）
- 情報システムに対する脆弱性診断又はペネトレーションテスト

更に、必要に応じて、サーバ、端末、通信回線装置等の機器、クラウド環境を含む情報システムの情報セキュリティに関する設定情報の確認、ログ出力状況の確認などを確認することも考えられる。

- **基本対策事項 2.3.2(1)-2「機関等外の者に監査の一部を請け負わせる」について**

  情報セキュリティ監査責任者は、監査を実施するに当たり、機関等内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮することが重要である。また、監査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、関連する規定にも留意が必要である。また、情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。加えて、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記載した「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査サービスに係る部分）を活用することも考えられる。

遵守事項

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告すること。

【 基本対策事項 】

＜2.3.2(2)(a)関連＞

2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

2.3.2(2)-2 情報セキュリティ監査責任者は、以下の事項を全て含む監査の実施を監査実施者に指示すること。

a) 対策基準に統一基準を満たすための適切な事項が定められていること。

b) 運用規程及び実施手順が整備されている場合、運用規程及び実施手順が対策基準に準拠していること。

c) 被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること。

（解説）

- **遵守事項 2.3.2(2)(a)「監査報告書」について**

監査報告書の作成に際しては、根拠となる監査調書を適切に作成する必要がある。監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等をつづり込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。

監査の結果は、監査報告書として文書化した上で、最高情報セキュリティ責任者へ確実に提出する必要がある。監査報告書には、対策基準に統一基準を満たすための適切な事項が定められているか、実際の運用状況が情報セキュリティ関係規程に準拠して行われているかなどの結果を記載する。さらに、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言・提案を監査報告書に含める。反対に組織として推奨すべき優れた取組等がある場合には、それらを組織全体に広めるなどの助言・提案があってもよい。

- **基本対策事項 2.3.2(2)-1「被監査部門から独立した者」について**

情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。例えば、情報システムを監査する場合に、当該情報システムの構築をした者や運用を行っている者が監査をしてはならない。また、情報の取り扱われ方に関する監査を行う場合には、当該情報を取り扱う者はその監査をしないこととする。

- **基本対策事項 2.3.2(2)-2 a)「統一基準を満たすための適切な事項が定められていること」について**

  統一基準 1.1(1)において、「情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定する」とされており、また、本ガイドラインの 1.1(1)「本ガイドラインの目的」において、「統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、対策基準の策定及び実施に際しての考え方等を解説するものである。」とされており、本ガイドラインの 1.1(5)「対策基準の策定手順」において、「本ガイドラインに規定される基本対策事項は、遵守事項を満たすためにとるべき基本的な対策事項の例示であり、遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講ずる必要がある。」とされている。これらの記述から、本基本対策事項で定める「統一基準を満たすための適切な事項が定められていること」について監査する際は、基本対策事項及び解説の記載についても参照した上で監査を実施する必要がある。

  対策基準に、統一基準を満たすための適切な事項が定められているか否かを判断する際には、機関等における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性等を踏まえ、必要な事項が対策基準に盛り込まれているか否かを確認する必要がある。このため、対策基準の策定に当たり、対策基準に各事項を盛り込んだ理由や本ガイドラインの基本対策事項との関係等について記録を残すと、監査の際に有用である。

- **遵守事項 2.3.2(2)-2 c)「実際の運用」について**

  被監査部門の職員等に対する質問や記録文書の査閲、執務室等の観察、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することも求められる。例えば、監査対象によっては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の検査、情報システムに対する侵入検査といった方法によっても確認することができる。

  なお、監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を行った場合には、その行為に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、情報セキュリティ対策の向上になり得る行為や、作業を効率的に行うことにつながる行為であるとしても、監査以外の行為を監査実施計画の中に取り込むべきではない。

遵守事項

(3) 監査結果に応じた対処

(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、**指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示**すること。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示すること。

(b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、**機関等内で横断的に改善が必要な事項**について、**必要な措置を行った上で改善計画を策定**し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。

(c) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、**自らが担当する組織のまとまりに特有な改善が必要な事項**について、**必要な措置を行った上で改善計画を策定**し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。また、措置が完了していない改善計画は、定期的に進捗状況を最高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 2.3.2(3)(a)「指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示」について**

情報システムに対する指摘事項の場合には、情報システムセキュリティ責任者等が指摘事項に対する改善計画の策定等を実施する場合があるので、指摘事項へ対応する範囲に留意し、遵守事項 2.3.2(3)(b)及び(c)でも同様に留意が必要である。

なお、指摘事項へ対応する範囲に留意すべき事項は以下が考えられる。

- 情報システムセキュリティ責任者が担当する情報システムでの改善だけでなく、機関等の対策基準や運用規程等の見直しが発生する場合には、統括情報セキュリティ責任者や情報セキュリティ責任者において改善計画を個別に策定する必要がある。
- 機関等内で横断的に改善が必要な事項、又は自らが担当する組織のまとまりに特有な改善が必要な事項では、運用規程等の見直しが発生した場合、所管する情報システムで対応が必要となる。また、遵守事項 5.2.5(1)に基づき、情報システムセキュリティ責任者が情報システムの情報セキュリティ対策の見直しを行い、その措置結果を統括情報セキュリティ責任者へ報告を行う場合、改善を実施するために複数の関係者が関与するため、責任分界を改善計画で明確にする必要がある。

- **遵守事項 2.3.2(3)(b)「機関等内で横断的に改善が必要な事項」について**

  監査報告書に記載される改善が必要な事項の内容によっては、監査を受けた部門以外の部門においても同種の課題や問題が存在している可能性がある。また、機関等内で共通的に使用している情報システムに対する改善が必要な事項については、監査を受けた部門のみで対処することが困難であると同時に、情報システムの利用部門全体に係る改善が必要な事項となる可能性がある。このような、組織全体として改善が必要な事項が確認された場合は、統括情報セキュリティ責任者がその対策に係る事務を統括することが求められる。

  なお、改善を指示されていない事項であっても、監査によって得られた教訓等を被監査組織以外にも展開し、組織全体で監査の教訓を対策に生かすことを考慮することも、組織全体の情報セキュリティを強化するために重要な取組である。

- **遵守事項 2.3.2(3)(b)「必要な措置を行った上で改善計画を策定」・遵守事項 2.3.2(3)(c)「必要な措置を行った上で改善計画を策定」について**

  改善が必要な事項の中には、緊急の措置が必要なものが存在する可能性があることから、そのような事項が確認された場合は、直ちに措置を行い、その結果を報告する必要がある。情報システムの機能改修を伴う措置等、即時の実施が困難と考えられるものについては、情報セキュリティに係るリスクを軽減させるための暫定的な措置を講ずるなどの対応を行うとともに、情報システムの改善計画を策定し、暫定的な措置の実施結果と併せて報告する必要がある。

- **遵守事項 2.3.2(3)(c)「自らが担当する組織のまとまりに特有な改善が必要な事項」について**

  遵守事項 2.3.2(3)(a)により、最高情報セキュリティ責任者から指示を受けた改善すべき事項のうち、遵守事項 2.3.2(3)(b)における「機関等内で横断的に改善が必要な事項」を除いたものを指している。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

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、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、機関等の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検・監査等の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策基準及び対策推進計画に反映することも重要である。

遵守事項

(1) 情報セキュリティ対策の見直し

(a) 最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、対策基準や対策推進計画の必要な見直しを行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(1)(a)「リスク評価に変化が生じた場合」について**

「（解説）遵守事項 2.1.3(1)(a)「リスクを評価する」について」において、対策基準や対策推進計画を定めるに当たっては、情報セキュリティを取り巻く様々な脅威や、機関等の業務、取り扱う情報及び保有する情報システムの特性等を踏まえた上で、リスク評価を行うことを示しているが、リスク評価実施時の情報セキュリティを取り巻く環境が変化した場合にはリスク評価の結果も変化するため、リスク評価に応じた対策基準や対策推進計画も見直す必要がある。

遵守事項

(2) 情報セキュリティ関係規程等の見直し

(a) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策基準について必要な見直しを行うこと。

(b) 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を踏まえて情報セキュリティ対策に関する運用規程及び実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告すること。

(c) 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を踏まえて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運用見直しについて、機関等内の職制及び職務に応じた措置の実施又は指示し、措置の結果について最高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 2.4.1(2)(a)「情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を総合的に評価」について**

機関等における情報セキュリティインシデントの発生状況、例外措置の申請状況、教育の実施状況に関する結果、自己点検や情報セキュリティ監査の結果、本部監査の結果、職員等からの相談、最新の脅威動向、セキュリティ対策技術の動向等を踏まえ、対策基準に課題及び問題点が認められるか否かなどの観点から総合的な評価を行い、対策基準について所要の見直しを行うことについて、最高情報セキュリティ責任者に求めている。

また、本部監査において助言された事項に関し、対策基準を見直す必要があるか否かを確認し、必要とされる場合には対策基準の見直しを行う。

なお、対策基準の見直しは、統一基準群の改定に合わせて実施することが考えられるが、最新の脅威動向を踏まえ、機関等全体で統一基準以上のセキュリティ対策や機関等固有のセキュリティ対策が求められる場合があるため、適宜実施できることが望ましい。

- **遵守事項 2.4.1(2)(b)「整備した者に対して規定の見直しを指示」について**

機関等における情報セキュリティインシデントの発生状況、例外措置の申請状況、自己点検や情報セキュリティ監査の結果、本部監査の結果、職員等からの相談、最高情報セキュリティ責任者からの指示、最新の脅威動向、セキュリティ対策技術の動向等を踏まえ、情報セキュリティ対策に関する運用規程及び実施手順を見直すことの必要性を

検討し、情報システムセキュリティ責任者等の運用規程及び実施手順を整備した者に、その見直しを指示することを統括情報セキュリティ責任者に求めている。

なお、策定済みの運用規程及び実施手順を見直すだけではなく、例えば、機関等内における共通のルールが存在しないため、各所属等において個別にルールを定めて運用しているなどの場合について、機関等内における共通のルールを整備するか否かを検討することも考えられる。

なお、運用規程及び実施手順の見直しは、対策基準の見直しに合わせて実施することが考えられるが、最新の脅威動向を踏まえ、機関等全体で統一基準以上のセキュリティ対策や機関等固有のセキュリティ対策が求められる場合があるため、適宜実施できることが望ましい。

- **遵守事項 2.4.1(2)(b)「見直し結果について最高情報セキュリティ責任者に報告」**

運用規程及び実施手順の見直しにより、運用規程及び実施手順の改定が行われた場合には、見直し結果である改定状況を最高情報セキュリティ責任者へ報告する。

また、運用規程及び実施手順の改定に時間を要する場合には、進捗状況や改定完了予定時期を報告することで、最高情報セキュリティ責任者が運用規程及び実施手順の策定状況を適切に把握することができる。

- **遵守事項 2.4.1(2)(c)「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運用見直し」について**

機関等における情報セキュリティ対策の見直しでは、対策基準や対策推進計画の見直しだけでなく、実際の運用についても見直しが発生する場合がある。特に、機関等内で横断的に改善が必要となるような機関等 LAN システムに関連した運用や情報システムごとに対策が異なると機関等全体の情報セキュリティ対策に影響を及ぼすものに対する措置については、改善の実施や指示等を一元的に行う必要がある。

- **遵守事項 2.4.1(2)(c)「機関等内の職制及び職務に応じた措置の実施又は指示」について**

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運用見直しに当たっては、実施者が情報セキュリティ対策推進体制であるのか、それとも課室情報セキュリティ責任者や情報システムセキュリティ責任者であるのか、更に職員等であるのかなど多岐に渡るため、措置の内容に応じて実施又は対象者への実施指示を行う必要がある。

また、措置の実施を指示するだけでなく、実施状況の把握まで必要があるかは、情報セキュリティに係る重大な影響を及ぼすかなどを勘案し、必要性を検討すること。

- **遵守事項 2.4.1(2)(c)「措置の結果について最高情報セキュリティ責任者に報告する」について**

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運用見直し措置結果に関する報告に当たっては、情報セキュリティに係る重大な影響を及ぼすかどうか、予算措置が必要となるため運用の見直しに時間を要するかどうかなど、措置の内容に応じて報告方法や報告時期などを分けることが考えられる。

遵守事項

(3) 対策推進計画の見直し

(a) 最高情報セキュリティ責任者は、**情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、本部監査等を総合的に評価**するとともに、**情報セキュリティに係る重大な変化等**を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について**定期的な見直し**を行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(3)(a)「情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、本部監査等を総合的に評価」について**

  機関等における情報セキュリティインシデントの発生状況、自己点検、情報セキュリティ監査の結果、職員等からの相談等を踏まえ、対策推進計画に加えるべき事項の有無、策定済みの計画の変更の必要があるかなどの観点から、評価を行う。

  また、本部監査において助言された事項において、対策推進計画に盛り込むべき事項がある場合は、当該事項の実施優先順位を検討した上で、適切に計画に盛り込むこととする。

- **遵守事項 2.4.1(3)(a)「情報セキュリティに係る重大な変化等」について**

  サイバー攻撃の量的な拡大や攻撃手法の高度化等による質的な変化等、計画策定時に前提としていた条件から大きく異なり、情報セキュリティに係るリスクが高まった場合や、年度途中における種々の要因により、当初の対策推進計画では課題解決が図られていない場合等を想定している。

- **遵守事項 2.4.1(3)(a)「定期的な見直し」について**

  機関等における対策推進計画は少なくとも毎年度１回の頻度で見直されることが期待される。

2.5 独立行政法人及び指定法人

2.5.1 独立行政法人及び指定法人に係る情報セキュリティ対策

目的・趣旨

独立行政法人や指定法人においても、国の行政機関の重要な情報に相当する情報が取り扱われている場合があるため、国の行政機関と同様に情報セキュリティ対策が適切に講じられる必要がある。そのためには、当該法人を所管する国の行政機関との連携による情報セキュリティマネジメントが適切に機能することが重要である。

遵守事項

(1) 独立行政法人及び指定法人を所管する国の行政機関における体制の整備

(a) 独立行政法人及び指定法人を所管する国の行政機関に置かれる最高情報セキュリティ責任者は、<u>所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備</u>を指示すること。

【 基本対策事項 】

＜2.5.1(1)(a)関連＞

2.5.1(1)-1 独立行政法人及び指定法人を所管する国の行政機関に置かれる統括情報セキュリティ責任者は、所管する独立行政法人及び指定法人の<u>情報セキュリティ対策が適切に推進されるために必要な体制として、当該法人所管部署等の関係部署及び所管する法人等に必要な助言等を行うための窓口を、当該法人所管部署等の関係部署と連携して整備</u>すること。

（解説）

- **遵守事項 2.5.1(1)(a)「所管する独立行政法人及び指定法人の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備」について**

独立行政法人を所管する主務大臣は、統一規範において、独立行政法人通則法の規定により指示する中期目標、中長期目標や年度目標に、統一基準に基づいて定めたポリシーに従って情報セキュリティ対策を講ずる旨を盛り込むことや、同法に基づく業務の実績等に関する評価の際に、情報セキュリティ対策の実施状況に関しても評価を行うことが求められている。さらに、指定法人を所管する国の行政機関は、統一規範において、個別の根拠法に基づき、必要な情報セキュリティ対策についての指導等を実施することや、情報セキュリティ対策の実施状況に関して評価を行うことが求められている。また、国の行政機関は、所管する独立行政法人及び指定法人の求めに応じて、情報セキュリティ対策に関する助言を行うことが求められる。ここでは、機関の情報セキュリティを統括する立場から、これらの目標策定や評価、指導等を当該法人所管部署が適切に行うために必要な体制を整備することを規定している。

なお、目標策定や評価においては、本部監査の結果やこれらの結果に対する各法人で

策定された改善計画の進捗状況も参考・考慮することが重要であると考えられる。また、助言の実施の一環として、当該法人から当該法人を所管する国の行政機関の情報セキュリティ関係規程の提供を求められた場合は、情報セキュリティに係る支障がある場合等を除き、これに応じることを検討することが望ましい。当該法人は、提供を受けた国の行政機関の情報セキュリティ関係規程を参考としつつ、自組織の特性等を踏まえて情報セキュリティ対策を行うことが考えられる。

- **基本対策事項 2.5.1(1)-1「情報セキュリティ対策が適切に推進されるために必要な体制として、当該法人所管部署等の関係部署及び所管する法人等に必要な助言等を行うための窓口を、当該法人所管部署等の関係部署と連携して整備」について**

  具体的には、所管する独立行政法人及び指定法人の情報セキュリティ対策に関する目標策定及び実施状況に関しての評価、指導等を当該法人所管部署が適切に行うため、当該法人所管部署に対して、機関の情報セキュリティを統括する立場等から、情報セキュリティに関する専門的知見等を踏まえた必要な助言を行うための連絡窓口を情報セキュリティ対策推進体制に置くことや、当該法人が所管省庁へ情報セキュリティ対策に関する助言を求める際の相談窓口を当該法人所管部署又は情報セキュリティ対策推進体制に置くことが考えられる。

  なお、複数の国の行政機関が当該法人を共管している場合は、共管する国の行政機関の間で連携して、代表窓口をいずれかの国の行政機関に置くなども考えられる。

遵守事項

(2) 独立行政法人及び指定法人における情報セキュリティ対策

(a) 独立行政法人及び指定法人の最高情報セキュリティ責任者は、情報セキュリティ対策を適切に推進するため、所管省庁と密接な連携を要する事項や専門的知見を要する事項について、当該法人を所管する国の行政機関へ助言を求めること。

【基本対策事項】規定なし

（解説）

- **遵守事項 2.5.1(2)(a)「所管省庁と密接な連携を要する事項や専門的知見を要する事項」について**

  所管省庁と密接な連携を要する事項や専門的知見を要する事項とは、独立行政法人及び指定法人が自らの情報セキュリティ関係規程や対策推進計画を定める場合や、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」の検討を行う場合、重大な情報セキュリティインシデントに対処する場合、本部監査の結果等を踏まえ情報セキュリティ関係規程や対策推進計画について必要な見直しを行う場合などが考えられる。

【参考 2.5.1-1】独立行政法人及び指定法人に係る情報セキュリティ体制のイメージ例

独立行政法人及び指定法人に係る情報セキュリティ体制のイメージを図 2.5.1-1 に示す。

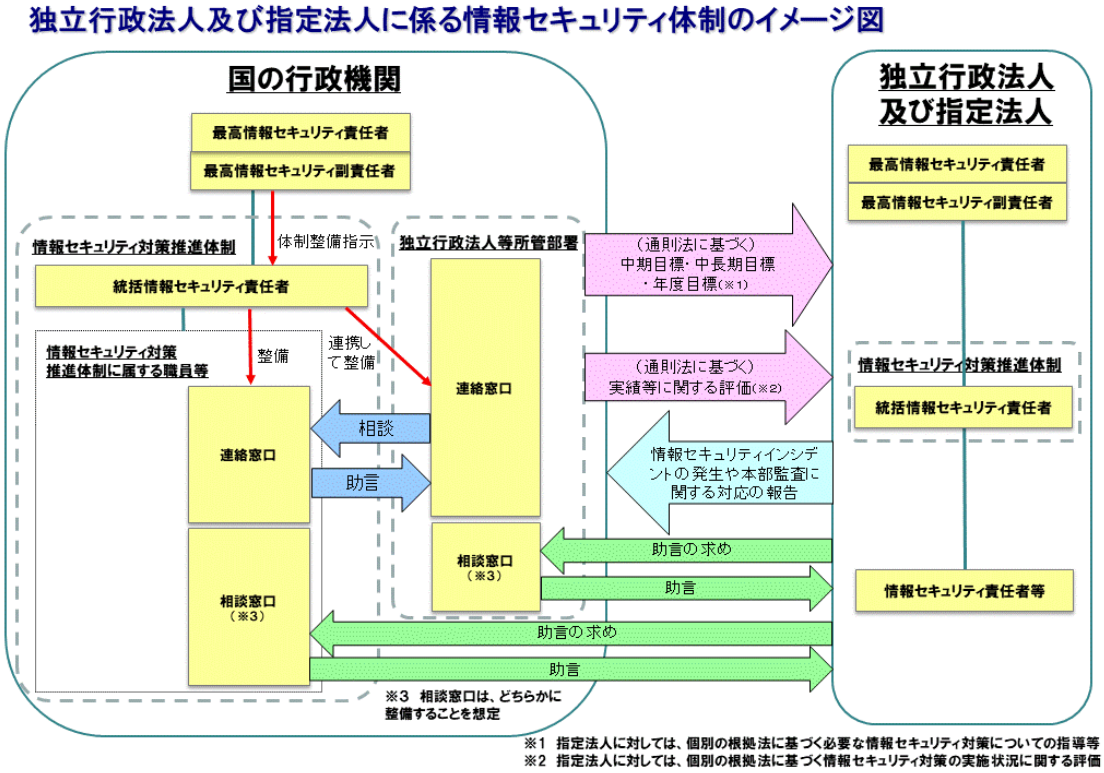


図 2.5.1-1　独立行政法人及び指定法人に係る情報セキュリティ体制のイメージ