統一基準群学習資料

NISC National center of Incident readiness and Strategy for Cybersecurity

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（令和５年度版）（※）について

（※）以下の文書群を指す
- 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
- 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（令和５年度版）
- 政府機関等の対策基準策定のためのガイドライン（令和５年度版）

令和６年１月

内閣官房 内閣サイバーセキュリティセンター

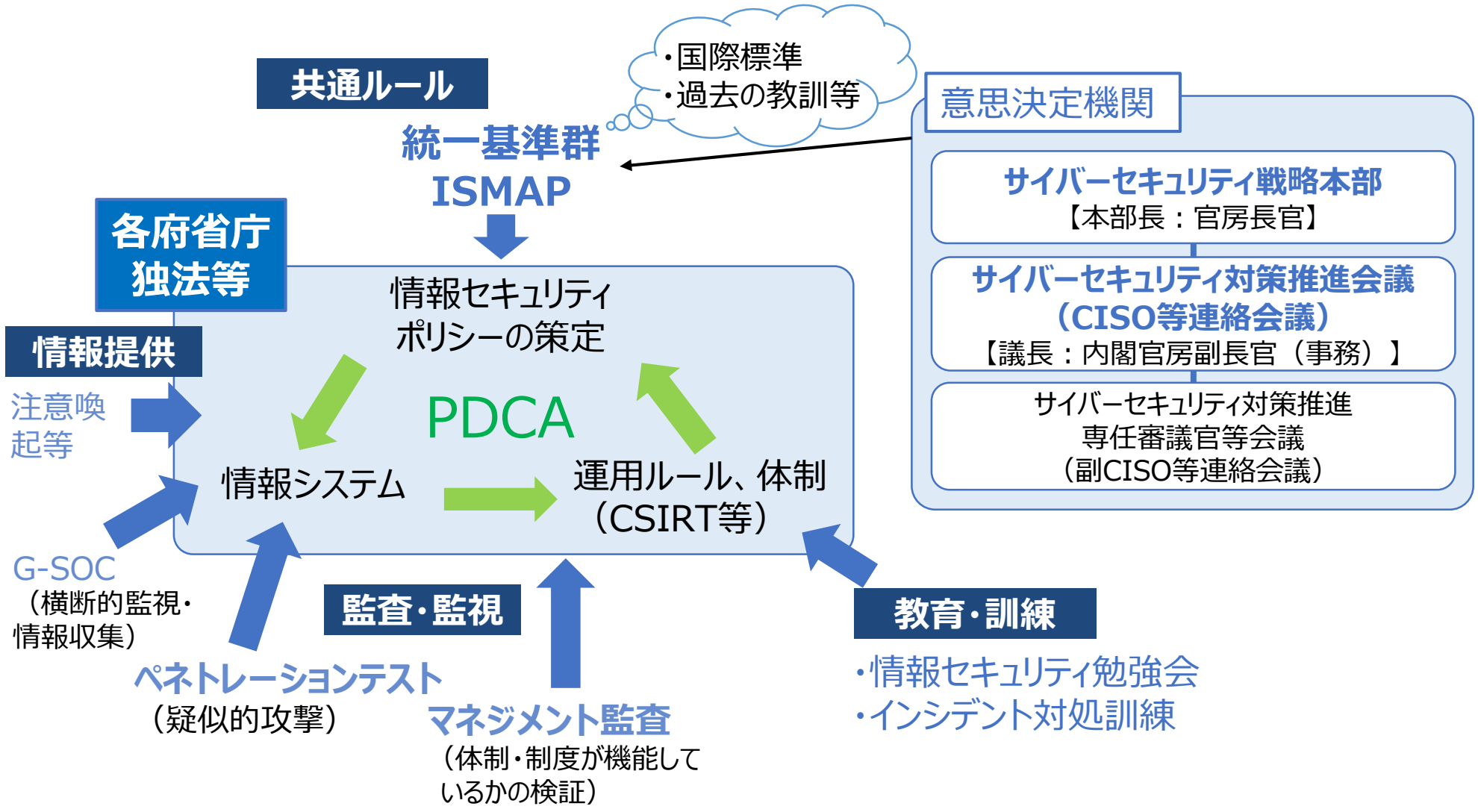
政府機関総合対策グループ

目次

目次（１．統一基準群の位置づけ･役割･文書体系 等）

政府機関等に対する情報セキュリティ対策の取り組み

- NISCにおいて、共通ルール（統一基準群）の策定、監査・監視、教育・訓練等を通して、政府機関等全体のPDCAサイクルを適切に回し、情報セキュリティ対策の総合的強化を図る

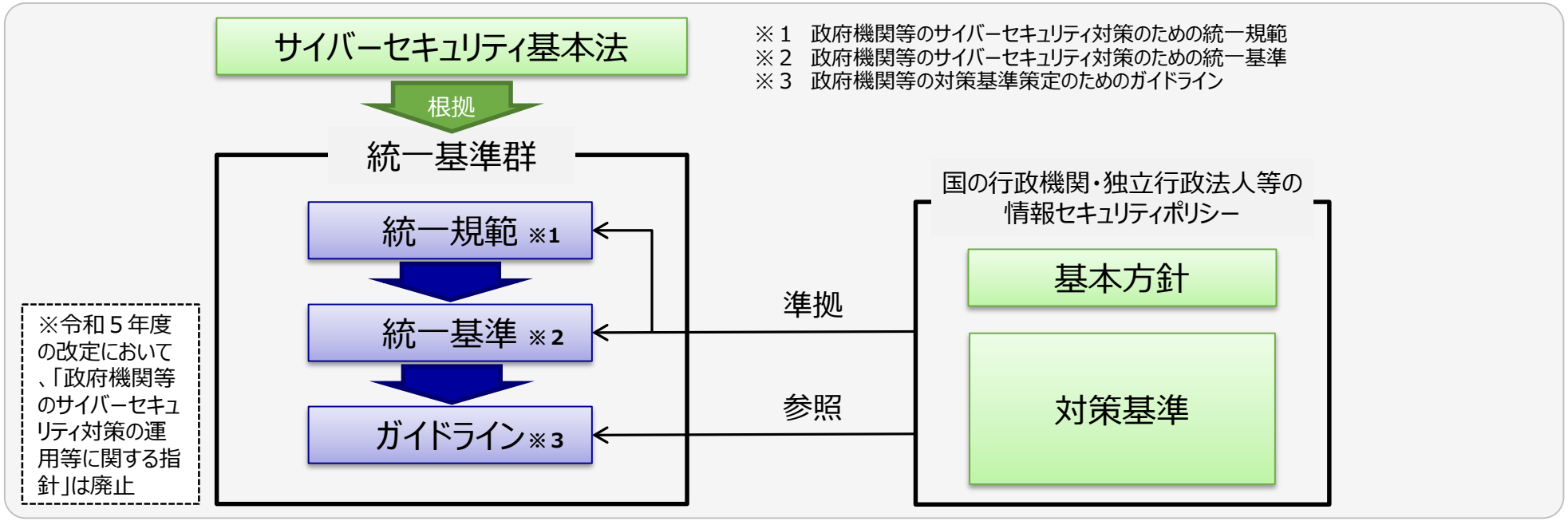


統一基準群の位置づけ

- 国の行政機関及び独立行政法人等は、統一規範及びその実施のための要件である統一基準に準拠するとともに、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情報セキュリティポリシーを策定。

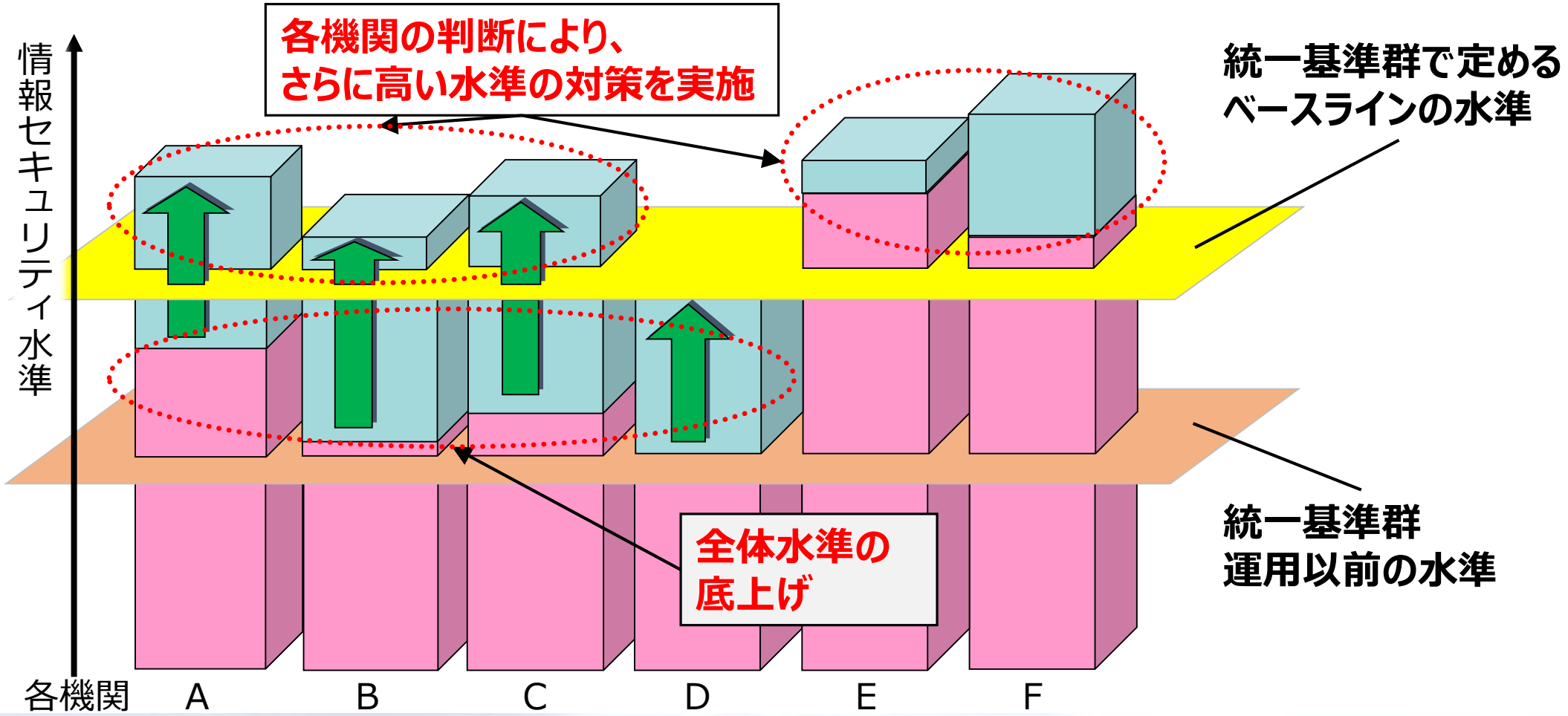
サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）
第二十六条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

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（抜粋）
第六条　機関等は、自組織の特性を踏まえ、**基本方針**及び**対策基準**を定めなければならない。
（略）
3　対策基準は、**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**定めなければならない。



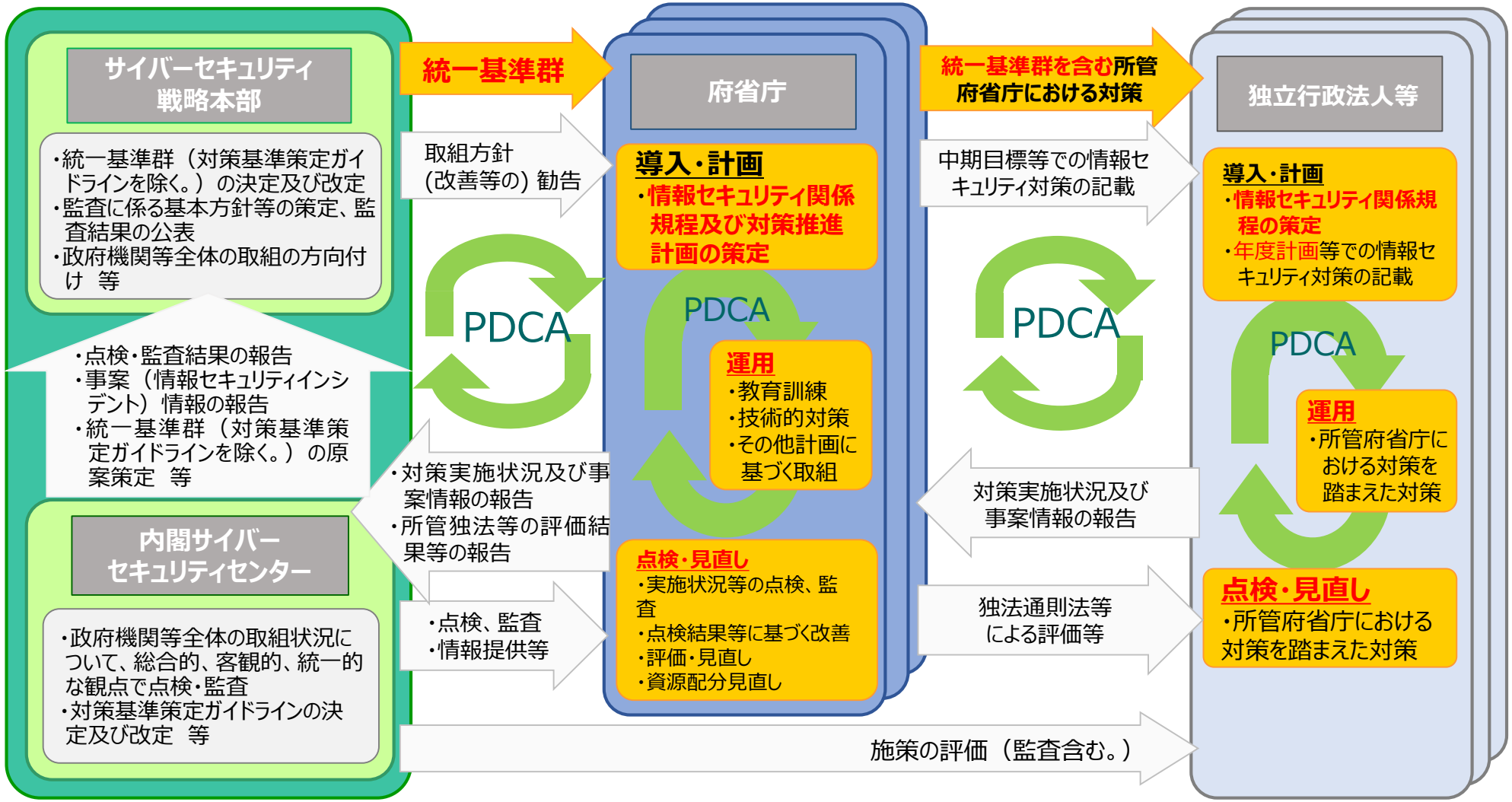
統一基準群の役割

- 統一基準群は、政府機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組み。
- 政府機関及び独立行政法人等の情報セキュリティのベースラインを示しており、各機関の判断により、さらに高い水準の対策も可能。

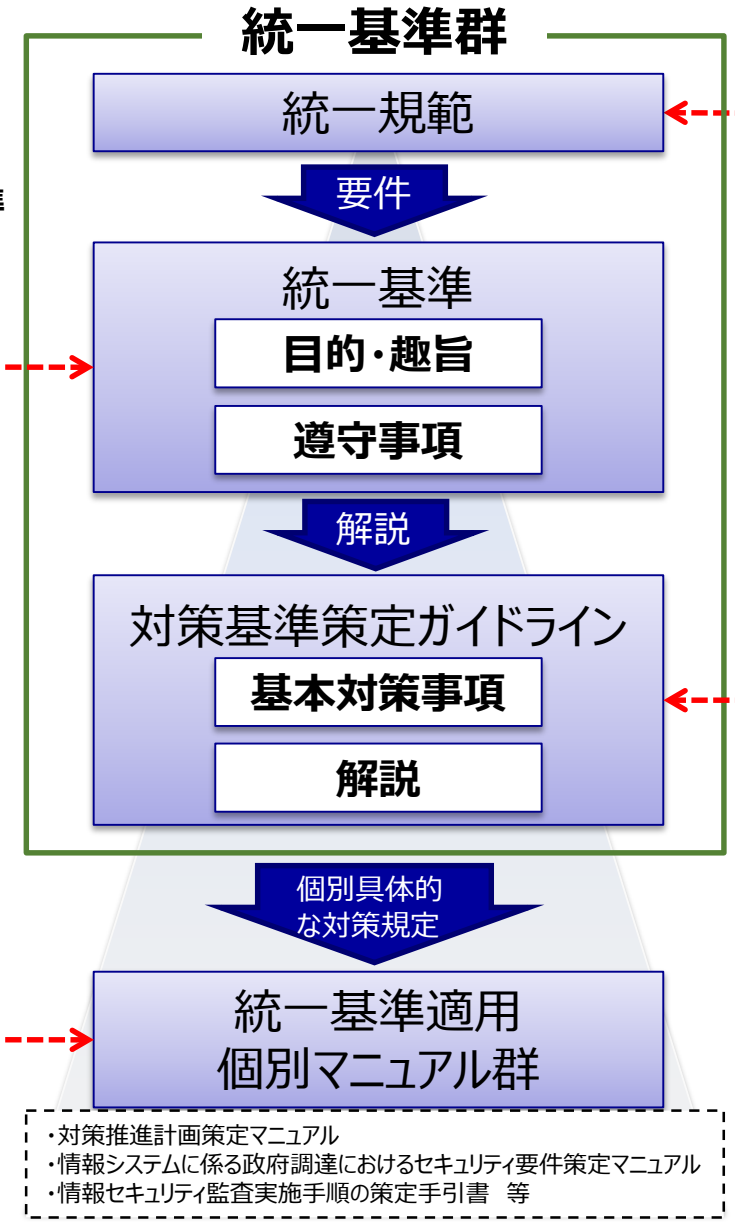


政府機関等全体における情報セキュリティのPDCAサイクル

- 統一基準群の運用により、個々の組織のPDCAサイクルや政府機関等全体のPDCAサイクルを適切に回し、政府機関等全体としての情報セキュリティを確保する。



統一基準群の文書体系



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

機関等がとるべき対策の統一的な枠組みを定めたもの

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

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（遵守事項）を規定することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的としたもの

政府機関等の対策基準策定のためのガイドライン

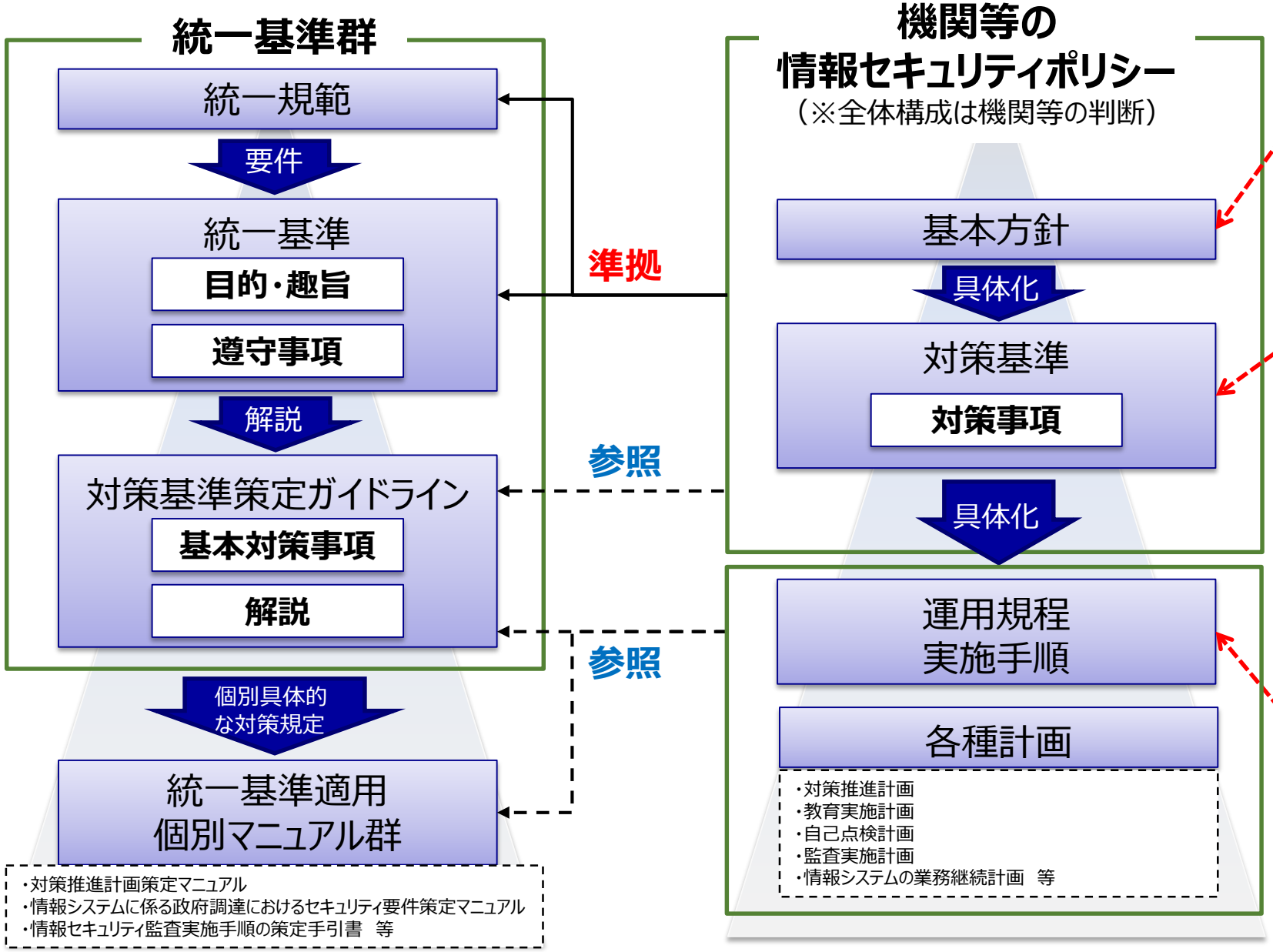
統一基準の遵守事項を満たすためにとるべき基本的な対策事項（基本対策事項）の例示とともに、対策基準の策定及び実施に際しての考え方等を解説したもの

統一基準適用個別マニュアル群

機関等において具体的な運用規程や実施手順を定める際の参考資料や個別の情報システムのセキュリティ要件等を検討する時等に利用されるもの

※令和５年度の改定において、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」は廃止

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



情報セキュリティ対策の目的、対象範囲等の情報セキュリティに対する基本的な考え方を定めたもの

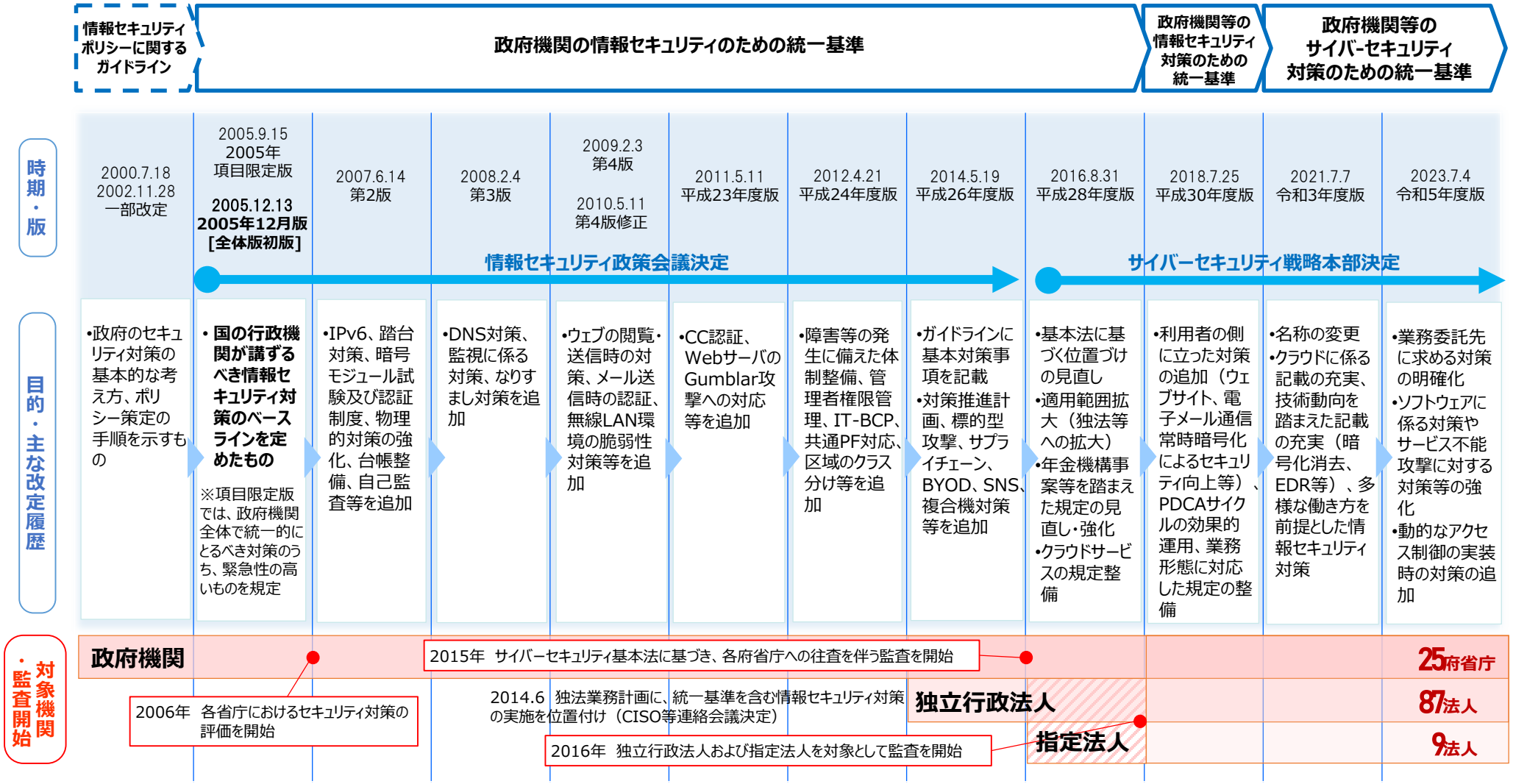
情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準
※統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように定める必要がある

【運用規程】
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

【実施手順】
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

【参考】統一基準群の変遷

➢ 2005年に現在の統一基準の基となる「政府機関の情報セキュリティのための統一基準」（初版）を策定。以後、サイバーセキュリティをめぐる動向等を踏まえ、必要なセキュリティ対策の基盤を着実に進化させることを目指し、概ね２年に一度、改定を行っている。



目次（２．統一基準群に定められている内容）

統一基準の目次構成（概要図）

第１部
総則

目的、適用範囲、用語定義　等

＜セキュリティに係る組織的・横断的取組＞

第２部
組織のガバナンス
マネジメント

体制、資産管理（台帳）、教育、インシデント対応、自己点検、
監査、独法・指定法人に係る対策　等

第３部
情報の取扱い

情報の格付・取扱制限、区域　等

第４部
外部委託

業務委託

クラウドサービス
- 要機密情報取扱い有
- 要機密情報取扱い無

機器等の調達

＜情報システムに係るセキュリティ対策＞

第５部
情報システムの
ライフサイクル

情報システムの分類

情報システムのライフサイクル
- 企画・要件定義
- 調達・構築
- 運用・保守
- 更改・廃棄
- 見直し

情報システムの運用継続

政府共通利用型システム

第６～８部
各構成要素や
シーンに応じた
セキュリティ対策

- 第6部　情報システムの構成要素
- 第7部　情報システムのセキュリティ要件
- 第8部　情報システムの利用

統一基準の目次構成（第１部～第４部）

部	部のタイトル	主な規定内容
1	総則	➢ 目的、適用範囲、用語定義
2	情報セキュリティ対策の基本的枠組み	➢ 導入・計画、運用、点検、見直し ✓ 組織・体制の整備、資産管理、対策基準・対策推進計画の策定 ✓ 情報セキュリティ対策の運用、教育、情報セキュリティインシデントへの対処 ✓ 自己点検、情報セキュリティ監査 ✓ 対策基準・対策推進計画の見直し ➢ 独立行政法人・指定法人に係る対策
3	情報の取扱い	➢ 情報のライフサイクルの各段階（作成、入手、利用、保存、提供、運搬、送信、消去、バックアップ）における対策 ➢ 情報を取り扱う区域の管理
4	外部委託	➢ 業務委託 ✓ 業務委託 ✓ 情報システムに関する業務委託 ➢ クラウドサービス ✓ 要機密情報を取り扱う場合 ✓ 要機密情報を取り扱わない場合 ➢ 機器等の調達

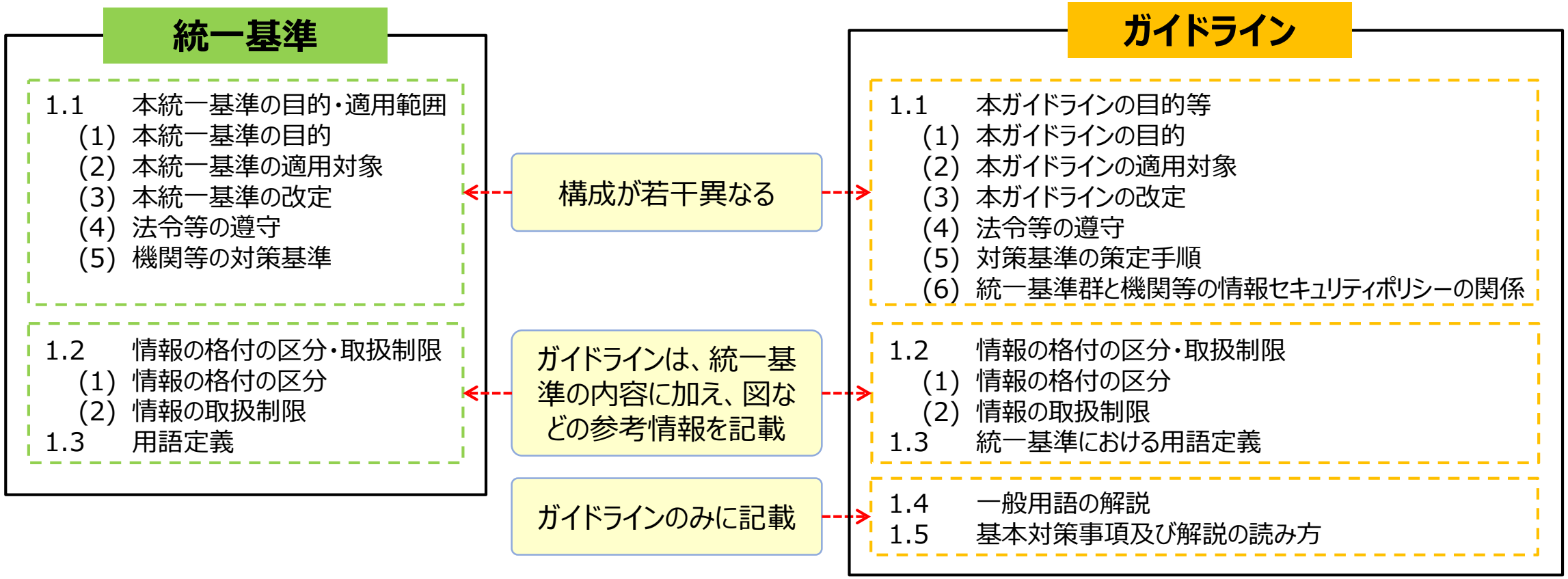
統一基準の目次構成（第５部～第８部）

部	部のタイトル	主な規定内容
5	情報システムのライフサイクル	➢ 情報システムの分類 ➢ 情報システムのライフサイクルの各段階（要件定義・構築・運用・更改・廃棄）における対策 ➢ 情報システムの運用継続計画 ➢ 政府共通利用型システム
6	情報システムの構成要素	➢ 端末、特定用途機器（IoT機器を含む）、通信回線の対策 ➢ サーバ装置、電子メール、ウェブ、DNS、データベースの対策 ➢ 情報システムの基盤を管理又は制御するソフトウェアの対策 ➢ アプリケーション・コンテンツの対策
7	情報システムのセキュリティ要件	➢ 情報システムのセキュリティ機能 ✓ 主体認証、アクセス制御、権限管理、ログ管理、暗号・電子署名、監視 ➢ 情報セキュリティの脅威への対策 ✓ ソフトウェア脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策 ➢ ゼロトラストアーキテクチャ
8	情報システムの利用	➢ 端末、電子メール、Web会議、クラウドサービスなどの情報システムの利用時の対策 ➢ ソーシャルメディアサービスによる情報発信時の対策 ➢ テレワーク実施時の対策

統一基準の目次構成（第１部　総則）

部	部のタイトル	主な規定内容
1	総則	➢ 目的、適用範囲、用語定義
2	情報セキュリティ対策の基本的枠組み	➢ 導入・計画、運用、点検、見直し ✓ 組織・体制の整備、資産管理、対策基準・対策推進計画の策定 ✓ 情報セキュリティ対策の運用、教育、情報セキュリティインシデントへの対処 ✓ 自己点検、情報セキュリティ監査 ✓ 対策基準・対策推進計画の見直し ➢ 独立行政法人・指定法人に係る対策
3	情報の取扱い	➢ 情報のライフサイクルの各段階（作成、入手、利用、保存、提供、運搬、送信、消去、バックアップ）における対策 ➢ 情報を取り扱う区域の管理
4	外部委託	➢ 業務委託 ✓ 業務委託 ✓ 情報システムに関する業務委託 ➢ クラウドサービス ✓ 要機密情報を取り扱う場合 ✓ 要機密情報を取り扱わない場合 ➢ 機器等の調達

第１部　総則



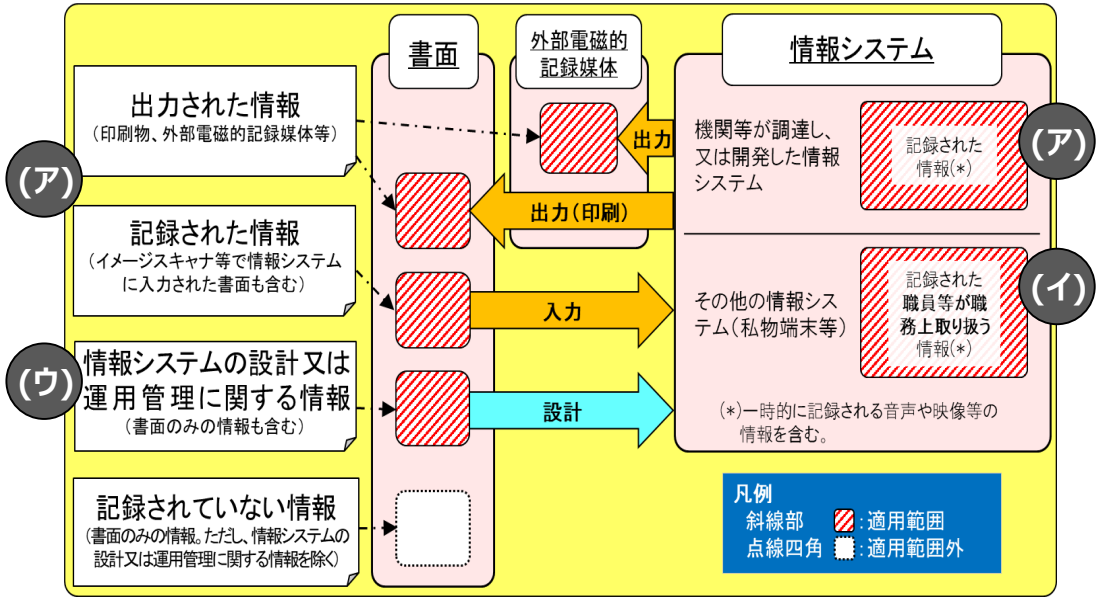
基本的には、ガイドラインは統一基準＋αの内容が記載されている。
ただし、「1.1」だけは構成が若干異なるので、統一基準・ガイドラインの両方を確認するとよい。

1.1(2) 統一基準の適用対象

1.1 本統一基準の目的・適用範囲
(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。

統一基準の適用対象となる「情報」の範囲

参考：ガイドライン 1.3 図1.3-2



(イ)の「その他のシステム」の例
- 私物端末
- 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

適用範囲外の情報の例
- 私物端末において職務上取り扱わない情報
- 記録されていない書面のみの情報

1.2(1) 情報の格付の区分

	格付の区分	分類の基準
機密性	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られる法人（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
完全性	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。）
可用性	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。）

要機密情報

要保全情報

要安定情報

いずれか一つでも該当する場合

要保護情報

【参考】秘密文書(機密性３)・不開示情報(機密性２)について

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

行政文書の管理に関する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：ガイドライン 1.3【参考２】機密性３情報について

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

格付の区分	分類の基準
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られる法人（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

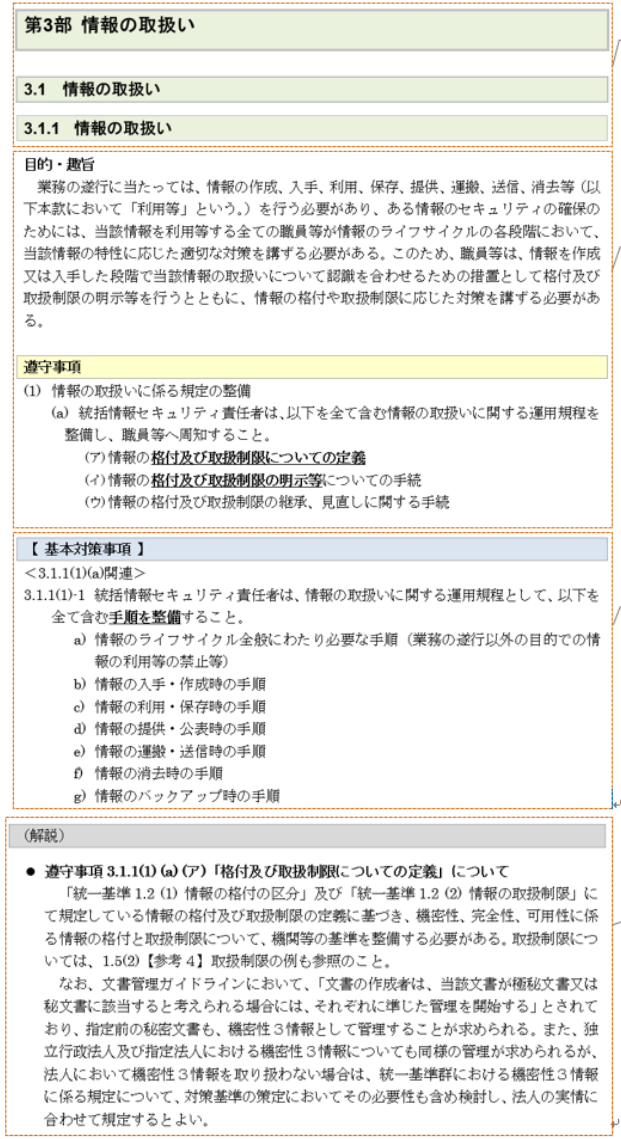
情報公開法及び独法等情報公開法における不開示情報の類型は次のとおり示されている

参考：ガイドライン 1.3【参考３】機密性２情報について

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】ガイドライン 1.5 基本対策事項及び解説の読み方

◆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

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。

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

（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。

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。

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。

3.1.1(1)の遵守事項に対応した基本対策事項を掲示

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。

基本対策事項について

◆”以下を例とする”の場合

【 基本対策事項 】
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。

◆ “～を全て含む”の場合

【 基本対策事項 】
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
（以下略）

基本対策事項が複数の事項から構成される場合は、主要な事項のみを含むべき事項として示している。

◆基本対策事項が規定されていない場合

【 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。

基本対策事項について

◆「基本セキュリティ対策」と「追加セキュリティ対策」

【 基本対策事項 】
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)-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。

統一基準の目次構成（第２部　情報セキュリティ対策の基本的枠組み）

部	部のタイトル	主な規定内容
1	総則	➢ 目的、適用範囲、用語定義
2	情報セキュリティ対策の基本的枠組み	➢ 導入・計画、運用、点検、見直し ✓ 組織・体制の整備、資産管理、対策基準・対策推進計画の策定 ✓ 情報セキュリティ対策の運用、教育、情報セキュリティインシデントへの対処 ✓ 自己点検、情報セキュリティ監査 ✓ 対策基準・対策推進計画の見直し ➢ 独立行政法人・指定法人に係る対策
3	情報の取扱い	➢ 情報のライフサイクルの各段階（作成、入手、利用、保存、提供、運搬、送信、消去、バックアップ）における対策 ➢ 情報を取り扱う区域の管理
4	外部委託	➢ 業務委託 ✓ 業務委託 ✓ 情報システムに関する業務委託 ➢ クラウドサービス ✓ 要機密情報を取り扱う場合 ✓ 要機密情報を取り扱わない場合 ➢ 機器等の調達

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
(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
(2) 情報セキュリティ委員会の設置
(3) 情報セキュリティ監査責任者の設置
(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
(5) 最高情報セキュリティアドバイザーの設置
(6) 情報セキュリティ対策推進体制の整備
(7) 情報セキュリティインシデントに備えた体制の整備
(8) 兼務を禁止する役割

2.1.2　資産管理
(1) 情報システム台帳の整備

2.1.3　情報セキュリティ関係規程の整備
(1) リスク評価の実施
(2) 対策基準の策定
(3) 運用規程及び実施手順の策定
(4) 対策推進計画の策定

2.2　運用

2.2.1　情報セキュリティ関係規程の運用
(1) 情報セキュリティ対策の運用
(2) 違反への対処

2.2.2　例外措置
(1) 例外措置手続の整備
(2) 例外措置の運用

2.2.3　教育
(1) 教育体制の整備・教育実施計画の策定
(2) 教育の実施

2.2.4　情報セキュリティインシデントへの対処
(1) 情報セキュリティインシデントに備えた事前準備
(2) 情報セキュリティインシデントへの対処
(3) 情報セキュリティインシデントに係る情報共有
(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

2.3　点検

2.3.1　情報セキュリティ対策の自己点検
(1) 自己点検計画の策定・手順の準備
(2) 自己点検の実施
(3) 自己点検結果の評価・改善

2.3.2　情報セキュリティ監査
(1) 監査実施計画の策定
(2) 監査の実施
(3) 監査結果に応じた対処

2.4　見直し

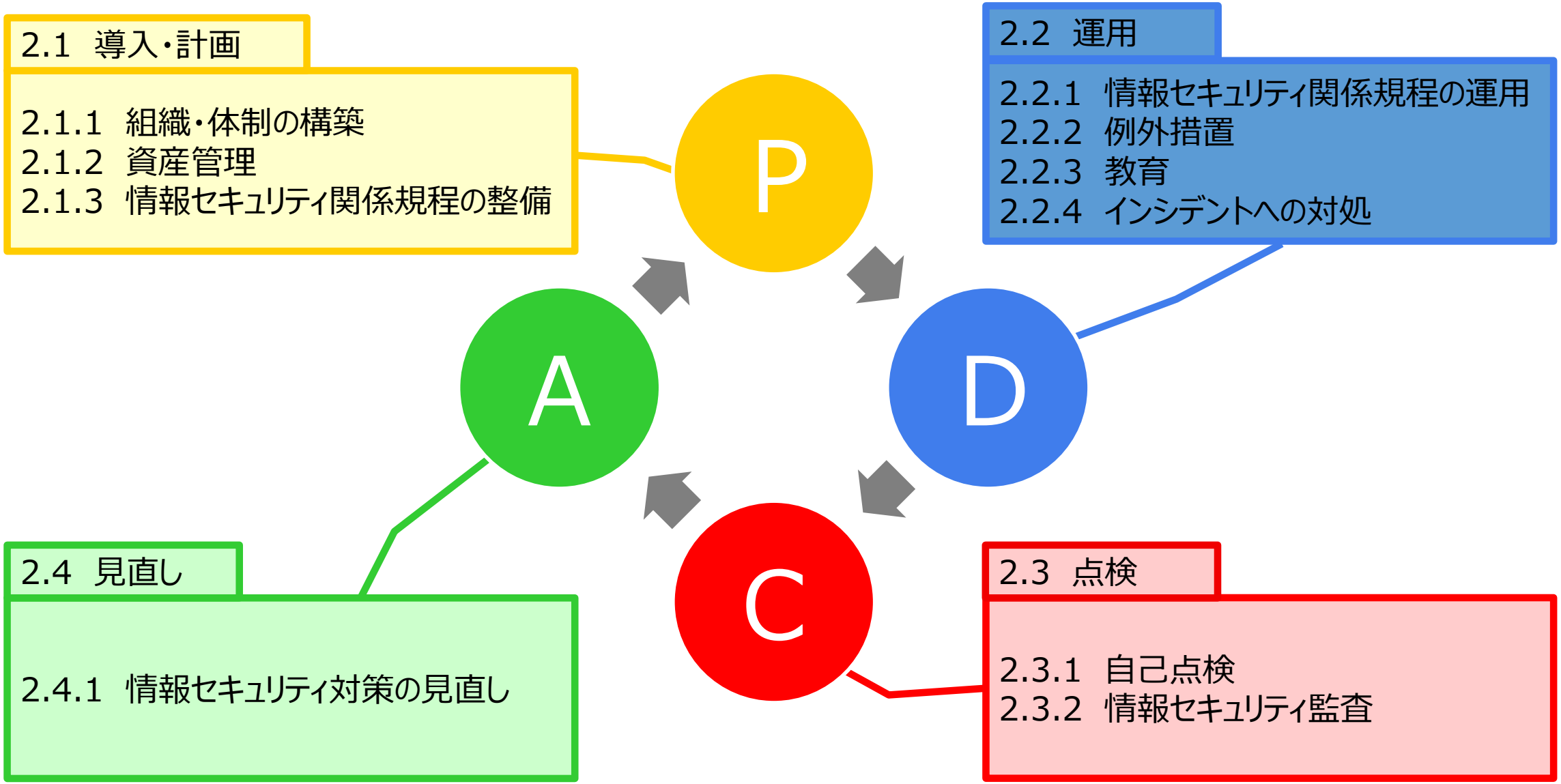
2.4.1　情報セキュリティ対策の見直し
(1) 情報セキュリティ対策の見直し
(2) 情報セキュリティ関係規程等の見直し
(3) 対策推進計画の見直し

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
(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
(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

2.1～2.4　導入・計画、運用、点検、見直し

情報セキュリティマネジメントのフレームワーク

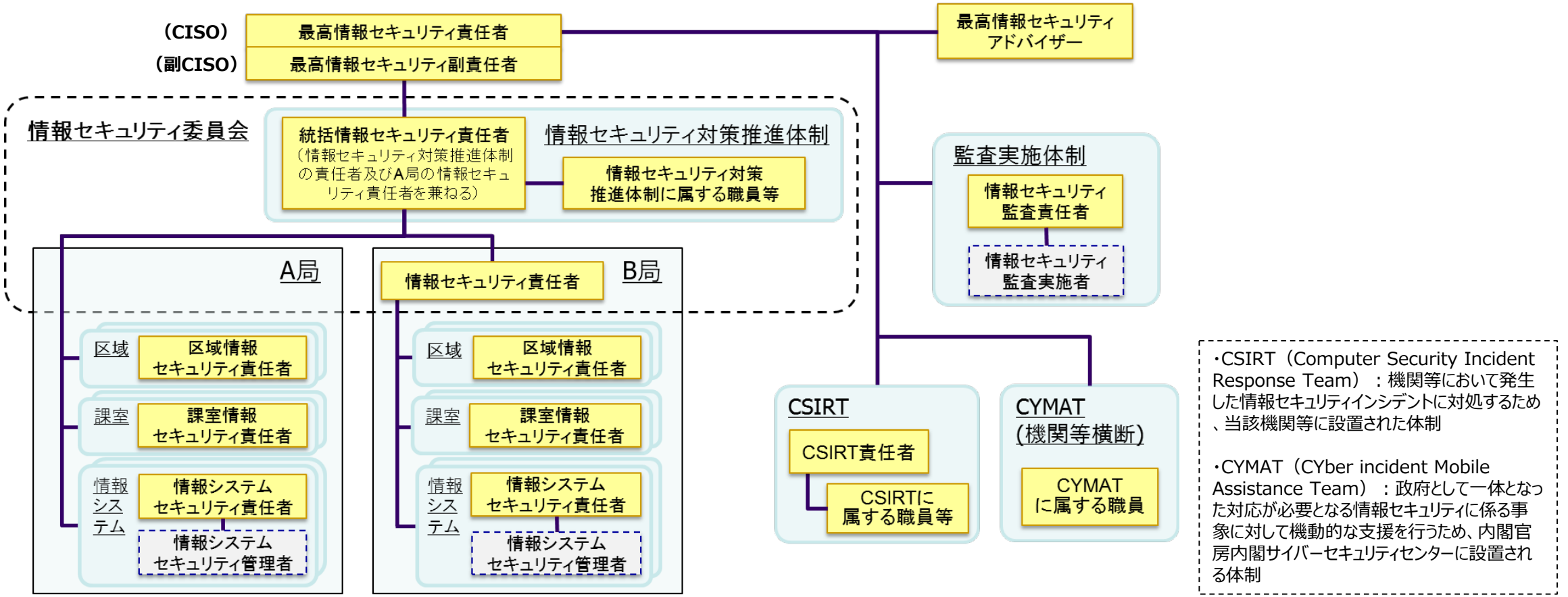


2.1.1 組織・体制の整備

情報セキュリティ対策は、それに係る全ての職員等が、職制およ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。これらの権限と責務を明確にした組織・体制を整備すること。

P
2.1 導入・検討
2.1.1 組織・体制の構築
2.1.2 資産管理
2.1.3 情報セキュリティ関係規程の整備

機関等における組織・体制の構築例



・CSIRT（Computer Security Incident Response Team）：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

・CYMAT（CYber incident Mobile Assistance Team）：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、内閣官房内閣サイバーセキュリティセンターに設置される体制

2.1.2 資産管理

自組織の資産を把握するため、情報システム台帳を整備すること。
資産が十分に把握できていない場合、対策を講じられていない資産が存在する、網羅的な対策が講じられない、インシデント発生時に情報収集に時間を要してしまいインシデントへの対処が遅れてしまう。

P
2.1 導入・検討
2.1.1 組織・体制の構築
2.1.2 資産管理
2.1.3 情報セキュリティ関係規程の整備

情報システム台帳

統括情報セキュリティ責任者

整備

以下の内容を全て含めること。

1. 情報システム名
2. 管理課室
3. 当該情報システムセキュリティ責任者の氏名及び連絡先
4. システム構成
5. 接続する機関等外通信回線の種別
6. 取り扱う情報の格付及び取扱制限に関する事項
7. 当該情報システムの設計・開発、運用・保守に関する事項
8. 情報システムの利用目的
9. 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
10. 連携する情報システム及び連携内容

さらに、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、以下の内容も全て含めること。

11. 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）
12. クラウドサービス等の提供者の名称
13. 利用期間
14. クラウドサービス等の概要
15. ドメイン名
16. 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
17. 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）
18. 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
19. サービスレベル

2.1.3 情報セキュリティ関係規程の整備

情報セキュリティ水準の維持・総合的にリスクを低減させるため、
対策基準や**運用規程**、**実施手順**、**対策推進計画**を定めること。
これらを定めるためには、**リスク評価**を実施し、その結果等を踏まえること。

P
2.1 導入・検討
2.1.1 組織・体制の構築
2.1.2 資産管理
2.1.3 情報セキュリティ関係規程の整備

最高情報セキュリティ責任者

実施

情報セキュリティ委員会

審議

- 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

勘案

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や発生時の損失等を分析

リスク評価

踏まえる

リスク評価については、以下を参照
- ガイドラインの（解説）遵守事項
  2.1.3(1)(a)「リスクを評価する」について

定める

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定めること

対策基準

具体化

- 運用規程
- 実施手順

統括情報セキュリティ責任者

定める

対策推進計画

NISC「対策推進計画策定マニュアル」を参考に定めるとよい

盛り込む

- 教育、自己点検
- 情報セキュリティ監査等を踏まえた取組
- 所管する独法等に関する取組　等

リスク評価の実施・対策基準等を定める際は、**機関等の目的**・**業務**・**取り扱う情報**や、
リスク評価・**自己点検**・**情報セキュリティ監査**・**本部監査の結果**等を踏まえることが重要

2.2.3 教育

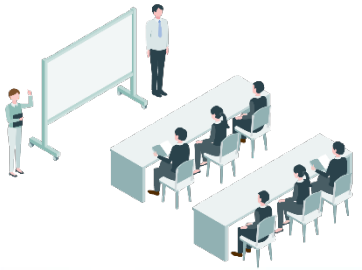
全ての職員等が、情報セキュリティ関係規程への理解を深め、情報セキュリティ水準を向上させるために、計画的に情報セキュリティ教育を実施すること。

D
2.2 運用
2.2.1 情報セキュリティ関係規程の運用
2.2.2 例外措置
2.2.3 教育
2.2.4 インシデントへの対処

教育に係る責任者の役割等

対象者	役割
統括情報セキュリティ責任者	職員等の役割に応じて教育内容を検討 対象者、手段及び実施時期等の教育実施計画を策定 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(CISO)に報告 等
課室情報セキュリティ責任者	職員等に対して教育の実施を周知 教育を受講しない者に対して受講を勧告 受講状況を確認するなどして、積極的に受講を促す 等
職員等	毎年度最低1回は教育を受講 着任又は異動後は、3か月以内に受講

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**、幅広い角度から教育内容を検討すること。



2.2.4 情報セキュリティインシデントへの対処

情報セキュリティインシデントが発生した場合は、最高情報セキュリティ責任者等の幹部に早急にその状況を報告するとともに、幹部の指揮の下で、被害拡大防止、復旧、再発防止等の対処を迅速かつ的確に行うこと。

D
2.2 運用
2.2.1 情報セキュリティ関係規程の運用
2.2.2 例外措置
2.2.3 教育
2.2.4 インシデントへの対処

情報セキュリティインシデントへの対処イメージ

事前準備
報告・対処手順、緊急連絡網の整備、訓練等による対処手順の適切性の確認

インシデント発生時
- 職員が可能性を認知
- 報告窓口へ報告
- CSIRTによる評価
- CISOへの報告
- 対処・連絡

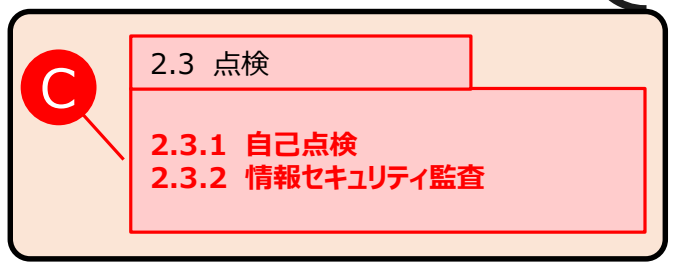
CSIRT（Computer Security Incident Response Team）：機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制

再発防止
原因の調査や再発防止策の検討、再発防止のための措置の指示

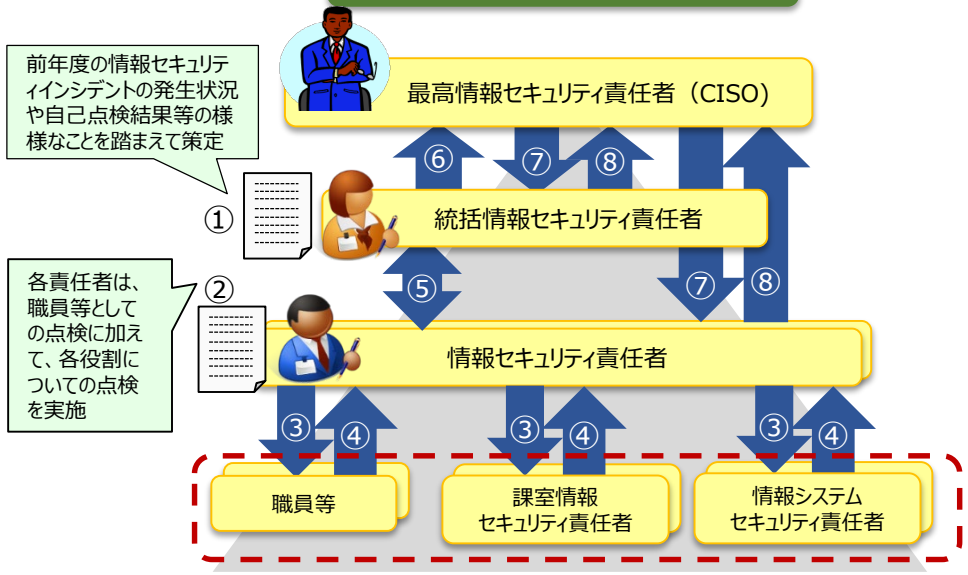
体制・手順等へフィードバック

2.3 点検

- 2.3.1 自己点検は、職員等が自らの役割に応じて対策事項を実施しているかどうかを確認するだけでなく、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。
- 2.3.2 情報セキュリティ対策の実効性を担保するために、自己点検に加えて、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。

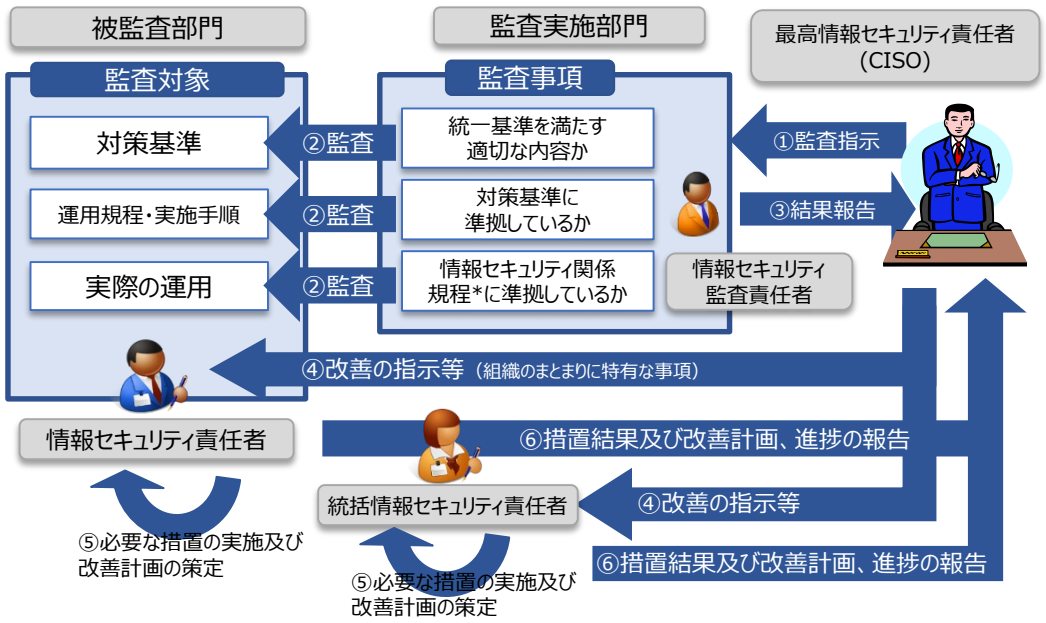


2.3.1 自己点検の流れ（例）



① 年度自己点検計画の策定
② 職員等ごとの自己点検票の作成、実施手順の整備
③ 実施の指示
④ 実施結果の報告
⑤ 結果の分析・評価
⑥ 評価結果の報告
⑦ 全体の評価及び改善指示
⑧ 改善結果の報告

2.3.2 情報セキュリティ監査の実施イメージ



（＊）「情報セキュリティ関係規程」･･･ 対策基準及び実施手順を総称したもの

2.4.1 情報セキュリティ対策の見直し

情報セキュリティに係る重大な変化等を踏まえてリスクを評価し、対策基準・対策推進計画・運用規程・実施手順を適時見直すこと。

A 2.4 見直し
2.4.1 情報セキュリティ対策の見直し

対策基準・対策推進計画の見直しのイメージ

最高情報セキュリティ責任者(CISO)

見直し結果・措置の結果を報告

定期的に見直す

情報セキュリティに係る重大な変化等を踏まえる

見直す

リスク評価に変化が生じた場合
(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)

対策推進計画

対策基準

総合的に評価

- 情報セキュリティの運用
- 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

情報セキュリティ委員会

審議

運用規程・実施手順の見直しのイメージ

統括情報セキュリティ責任者

踏まえる

見直しを指示

措置の指示

情報システムセキュリティ責任者　等

見直す

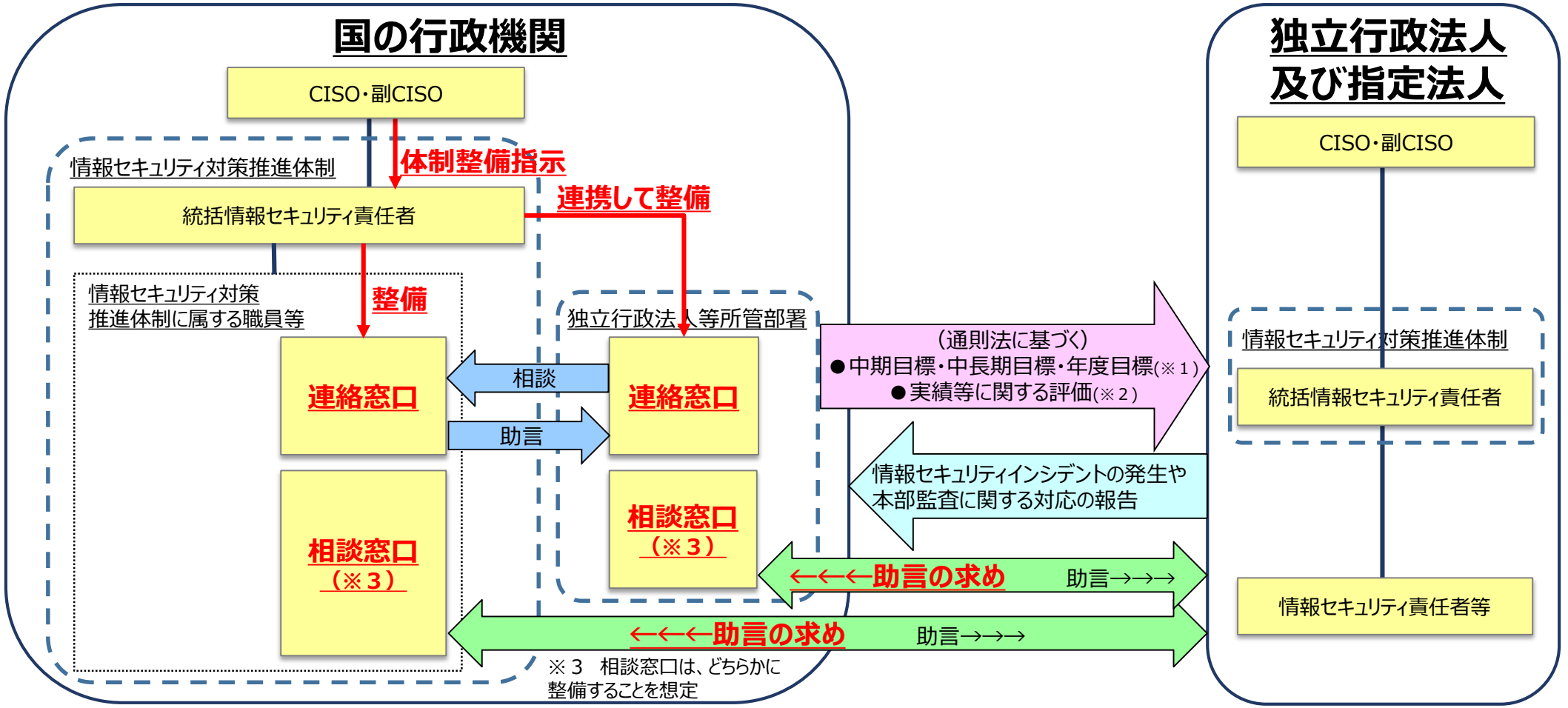
運用規程
実施手順

措置の実施

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

2.5 独立行政法人及び指定法人

国の行政機関は、所管する法人に助言を行うための窓口を整備すること。
独立行政法人・指定法人は、情報セキュリティ関係規程や対策推進計画を改定する場合等に、所管省庁へ助言を求めること。



参考：ガイドライン
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

※1 指定法人に対しては、個別の根拠法に基づく必要な情報セキュリティ対策についての指導等
※2 指定法人に対しては、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

統一基準の目次構成（第３部　情報の取扱い）

部	部のタイトル	主な規定内容
1	総則	➢ 目的、適用範囲、用語定義
2	情報セキュリティ対策の基本的枠組み	➢ 導入・計画、運用、点検、見直し ✓ 組織・体制の整備、資産管理、対策基準・対策推進計画の策定 ✓ 情報セキュリティ対策の運用、教育、情報セキュリティインシデントへの対処 ✓ 自己点検、情報セキュリティ監査 ✓ 対策基準・対策推進計画の見直し ➢ 独立行政法人・指定法人に係る対策
3	情報の取扱い	➢ 情報のライフサイクルの各段階（作成、入手、利用、保存、提供、運搬、送信、消去、バックアップ）における対策 ➢ 情報を取り扱う区域の管理
4	外部委託	➢ 業務委託 ✓ 業務委託 ✓ 情報システムに関する業務委託 ➢ クラウドサービス ✓ 要機密情報を取り扱う場合 ✓ 要機密情報を取り扱わない場合 ➢ 機器等の調達

3.1　情報の取扱い

3.1.1　情報の取扱い

(1) 情報の取扱いに係る規定の整備
(2) 情報の目的外での利用等の禁止
(3) 情報の格付及び取扱制限の決定・明示等
(4) 情報の利用・保存
(5) 情報の提供・公表
(6) 情報の運搬・送信
(7) 情報の消去
(8) 情報のバックアップ

3.2　情報を取り扱う区域の管理

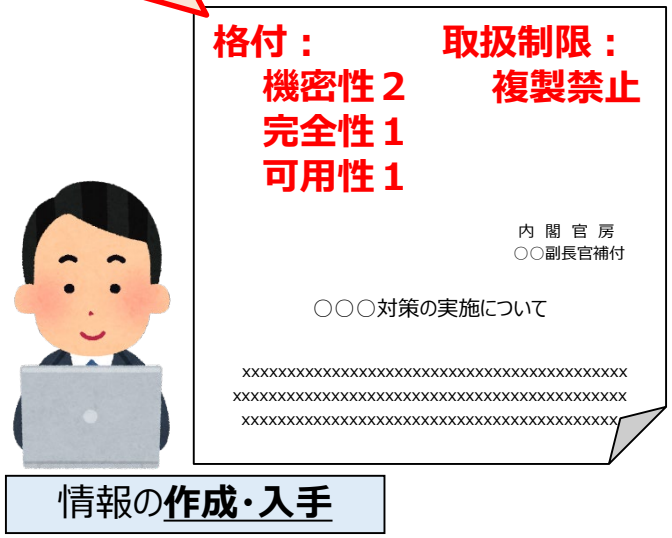
3.2.1　情報を取り扱う区域の管理

(1) 要管理対策区域における対策の基準の決定
(2) 区域ごとの対策の決定
(3) 要管理対策区域における対策の実施

3.1.1 情報の取扱い

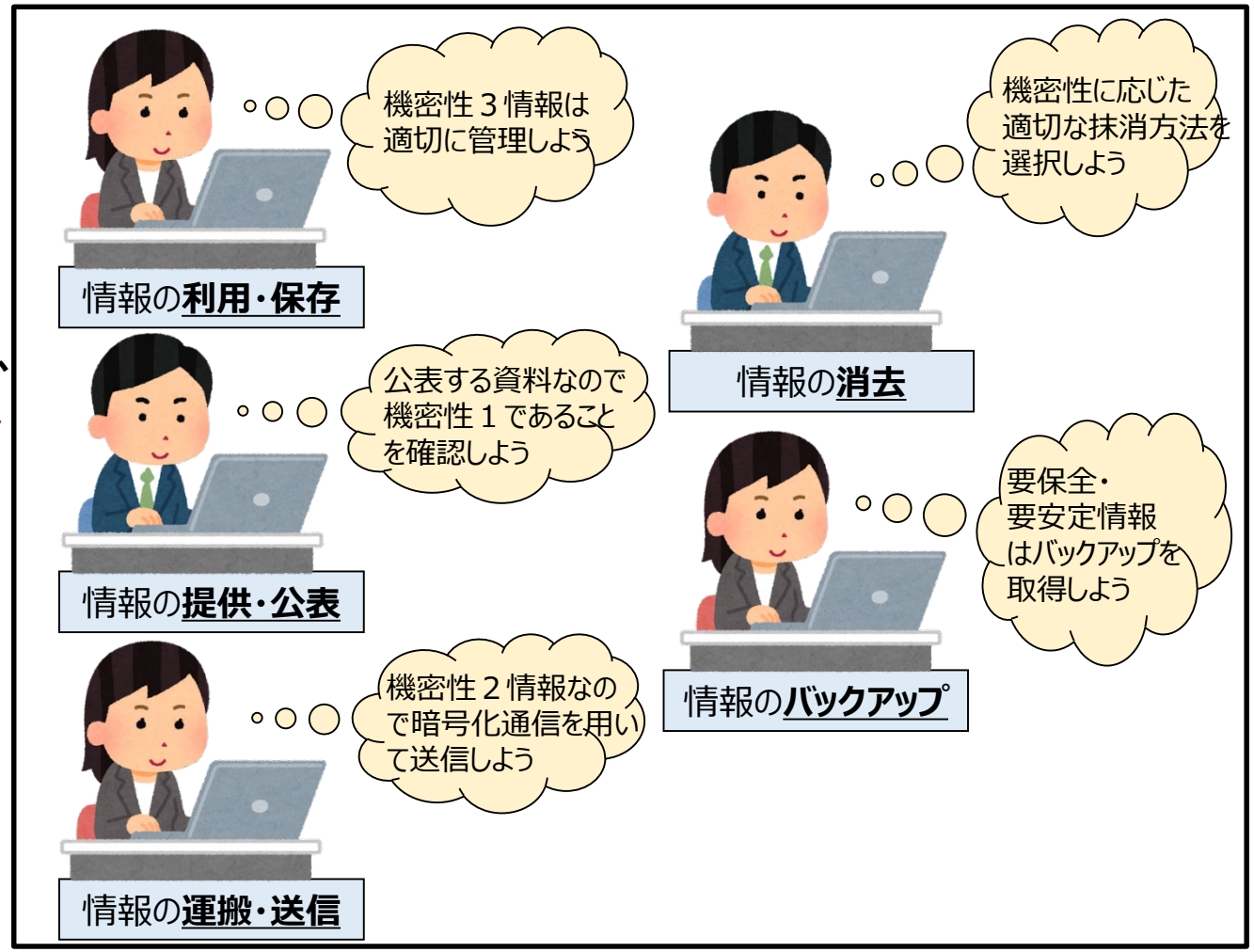
情報を作成・入手した段階で、格付及び取扱制限の明示を行うこと。
また、利用・保存、提供・公表、運搬・送信、消去、バックアップを行う場合は、明示された格付及び取扱制限に応じて、適切に情報を取り扱うこと。

作成・入手した段階で、格付及び取扱制限の明示を行う



情報の**作成・入手**

情報の利用シーンと、明示された格付・取扱制限に応じて情報を取り扱う



3.2.1 情報を取り扱う区域の管理

執務室、会議室、サーバ室等の情報を取り扱う区域の特性に応じて、区域ごとにクラスを割り当て、それぞれのクラスごとに物理的な対策や入退管理の対策等を講ずること。

統括情報セキュリティ責任者

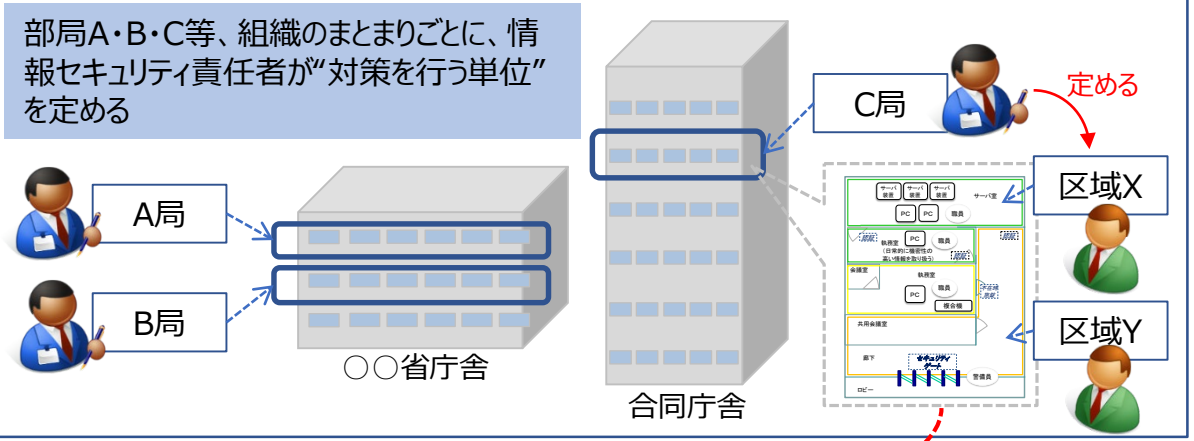
- クラスの区分の定義の整備
- クラス区分ごとの対策基準の整備

クラス	クラスの区分の定義（例）
クラス３	立入りを厳格に制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	行政事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対象区域

情報セキュリティ責任者

- 施設及び環境に係る対策を行う単位ごとの区域を定める

部局A・B・C等、組織のまとまりごとに、情報セキュリティ責任者が“対策を行う単位”を定める



区域情報セキュリティ責任者

- 管理する区域へのクラスの割当て
- 立入りを制限するための物理的対策・入退管理対策の決定と実施
- 扉の開閉・施錠等に係る実施手順の整備

統一基準の目次構成（第４部　外部委託）

部	部のタイトル	主な規定内容
1	総則	➢ 目的、適用範囲、用語定義
2	情報セキュリティ対策の基本的枠組み	➢ 導入・計画、運用、点検、見直し ✓ 組織・体制の整備、資産管理、対策基準・対策推進計画の策定 ✓ 情報セキュリティ対策の運用、教育、情報セキュリティインシデントへの対処 ✓ 自己点検、情報セキュリティ監査 ✓ 対策基準・対策推進計画の見直し ➢ 独立行政法人・指定法人に係る対策
3	情報の取扱い	➢ 情報のライフサイクルの各段階（作成、入手、利用、保存、提供、運搬、送信、消去、バックアップ）における対策 ➢ 情報を取り扱う区域の管理
4	外部委託	➢ 業務委託 ✓ 業務委託 ✓ 情報システムに関する業務委託 ➢ クラウドサービス ✓ 要機密情報を取り扱う場合 ✓ 要機密情報を取り扱わない場合 ➢ 機器等の調達

第４部　外部委託

4.1　業務委託

4.1.1　業務委託
(1) 業務委託に係る運用規程の整備
(2) 業務委託実施前の対策
(3) 業務委託実施期間中の対策
(4) 業務委託終了時の対策

4.1.2　情報システムに関する業務委託
(1) 情報システムに関する業務委託における共通的対策
(2) 情報システムの構築を業務委託する場合の対策
(3) 情報システムの運用・保守を業務委託する場合の対策
(4) 機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

4.2　クラウドサービス

4.2.1　クラウドサービスの選定（要機密情報を取り扱う場合）
(1) クラウドサービスの選定に係る運用規程の整備
(2) クラウドサービスの選定
(3) クラウドサービスの利用に係る調達
(4) クラウドサービスの利用承認

4.2.2　クラウドサービスの利用（要機密情報を取り扱う場合）
(1) クラウドサービスの利用に係る運用規程の整備
(2) クラウドサービスの利用に係るセキュリティ要件の策定
(3) クラウドサービスを利用した情報システムの導入・構築時の対策
(4) クラウドサービスを利用した情報システムの運用・保守時の対策
(5) クラウドサービスを利用した情報システムの更改・廃棄時の対策

4.2.3　クラウドサービスの選定・利用（要機密情報を取り扱わない場合）
(1) 要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備
(2) 要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施

4.3　機器等の調達

4.3.1　機器等の調達
(1) 機器等の調達に係る運用規程の整備

4.1 業務委託

業務委託を行う際は、委託先に提供する要保護情報等を適切に保護するための情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とすること。

4.1 業務委託の全体イメージ

＜業務委託※の例＞

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

※業務委託とは？

「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。

4.1.1 業務委託 全ての「業務委託」に適用

(1) 規程の整備 → (2) 実施前の対策 → (3) 実施期間中の対策 → (4) 終了時の対策

次スライドへ

4.1.2 情報システムに関する業務委託 「情報システムに関する業務委託」について上乗せで適用

（1）共通的対策
（2）構築の場合の対策
（3）運用・保守の場合の対策
（4）機関等向けに情報システムの一部の機能を提供するサービス(※)を利用する場合の対策

※機関等向けに情報システムの一部の機能を提供するサービスとは？

機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（以下「業務委託サービス」という。）。
なお、業務委託サービスは、契約をもって外部の者に実施させる「業務委託」により提供を受けるサービスであることから、セキュリティ要件を調達仕様書に個別に記載するなどにより情報セキュリティを確保する必要がある。
＜業務委託サービスの例＞
・ホスティングサービス
・インターネット回線接続サービス

4.1 業務委託（委託先に実施を求める対策）

4.1.1 業務委託

委託先に実施を求める対策

(1)業務委託に係る規定の整備

- なし

委託元（各機関等）にて、委託判断基準、委託先の選定基準を含む規定を整備

(2) 業務委託実施前の対策

- 仕様に準拠した提案

委託元（各機関等）にて、以下を委託先の選定条件として仕様に含める

- 情報の目的外利用の禁止
- セキュリティ対策の実施及び管理
- インシデントへの対処
- 契約の履行状況の確認（定期的な報告、監査の受入れ）
- セキュリティ対策の履行が不十分な場合の対処
- サービスレベルの保証

- 契約の締結

対策の遵守方法、管理体制等の確認書の提出

- 秘密保持契約（NDA）の締結

(3) 業務委託実施期間中の対策

- 取り扱う情報の適正な取扱い（以下を契約に含める）

具体例の提示

- インシデント対処能力の確立・維持
- 情報へアクセスする主体の識別とアクセス制御
- ログの取得・監視
- 情報を取り扱う機器等の物理的保護
- 情報を取り扱う要員への周知と統制
- 脅威に対処するための資産管理・リスク評価
- システム及び情報の完全性の保護
- セキュリティ対策の検証・評価・見直し

- セキュリティ対策の履行状況の定期的な報告
- インシデントの発生、情報の目的外利用を認知した場合の対処

(4) 業務委託終了時の対策

- セキュリティ対策の実施報告を含む検収の受検
- 提供された情報の返却・廃棄・抹消

情報システムに関する業務委託の場合には、委託先の選定条件に加える

4.1.2 情報システムに関する業務委託

(1) 情報システムに関する業務委託における共通的対策

- システムに意図せざる変更が加えられないための管理体制の確保
- 委託先の資本関係・役員等の情報、実施場所、従事者の所属・専門性・国籍等の情報提供

【参考】業務委託先に実施を求める情報セキュリティ対策①

- 統一基準4.1.1(3)において、政府情報の適切な取扱いのため業務委託先に求める情報セキュリティ対策の事項を明確化
- 情報セキュリティ対策の事項は、米国国立標準技術研究所（NIST）が公表している サプライチェーンにおける情報セキュリティ対策のガイドライン（SP800-171）を参考に、8項目を規定
- 各府省の調達において、委託先に求める要件としてこれらを契約に含めることとなる

基本対策事項4.1.1(3)-1	実施内容の概要	SP800-171の関連条項
a) 情報セキュリティインシデント等への対処能力の確立・維持	**インシデントを予防し、万一の発生時に的確な対処を行うことで情報を保護できるようにする** （対策例） • 当事者及び関係者の役割を含む体制をあらかじめ定めている • インシデント対処体制、責任者、委託業務担当者から当該体制への報告フロー等の概要について、対処能力の証明として契約締結までに説明ができる • 委託期間中に情報セキュリティインシデント等の検出有無等について定期的な報告を行う など	3.6 インシデント対応
b) 要保護情報へアクセスする主体の識別とアクセスの制御	**必要な者だけが情報にアクセスできる状態を維持する** （対策例） • 主体認証やその属性ごとにアクセス制御を行い、管理者権限を持つ場合には必要最低限の権限と利用に制限した上で、ログを取得する • システム利用者及び使用機器が一意で特定されている • 強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用する、初期パスワードの変更など主体認証情報に関する対策を行う など	3.1 アクセスコントロール 3.5主体識別と認証
c) ログの取得・監視	**インシデント兆候の検知・分析と、証跡の確保を実施する** （対策例） • ログの取得プロセスの障害監視を行う • 取得したログ情報やその分析内容に応じて、不正アクセスや異常操作への対応が取れるようプロセス設計を行う • 取得したログ情報及びログ取得機能について改変・削除から保護し、ログ取得機能の管理者権限付与を最低限の対象に限定する など	3.3 監査と説明責任

【参考】業務委託先に実施を求める情報セキュリティ対策②

基本対策事項4.1.1(3)-1	実施内容の概要	SP800-171の関連条項
d) 要保護情報を取り扱う機器等の物理的保護	**適切な物理的管理策によって情報を保護する** （対策例） • 機器等の廃棄時又は再利用時にデータを抹消又は破壊する • 委託事業の実施場所について、鍵等の管理や入退室記録等、入退管理対策を行う　など	3.8 メディアの保護 3.10 物理的保護
e) 要保護情報を取り扱う要員への周知と統制	**適切な人的管理策によって情報を保護する** （対策例） • 情報セキュリティに係る業務及び責務の遂行に必要な訓練等を確実に受講させる • 委託業務に伴う情報を取り扱う従業員等の資格条件を明確化する　など	3.2 意識啓発と訓練 3.9 要員のセキュリティ
f) セキュリティ脅威に対処するための資産管理・リスク評価	**セキュリティ対策の前提となる資産の識別と、リスクの評価を実施する** （対策例） • 情報システムの変更に係る検知機能やログ解析機能を実装する • 定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時な脆弱性対策を行う　など	3.4 構成管理 3.7 メンテナンス 3.11 リスクアセスメント
g) システム及び情報の完全性の保護	**適切な技術的管理策によって情報を保護する** （対策例） • 定期的な検索等によりシステムの欠陥を適時に検出し是正する • 悪意あるコードに対する保護措置を講じる • 脆弱性に係る注意喚起の監視と対処を行う • 業務に必要な通信だけを許可し、許可していない不正な通信の発生を防止する • 不正利用防止のための職務分掌の徹底及び事後追跡のためのログの取得・管理・分析体制を整備する　など	3.13 システムと通信の保護 3.14 システムと情報の完全性
h) セキュリティ対策の検証・評価・見直し	**対策の有効性の評価と、定期的な見直しを実施する** （対策例） • システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施する • システムの欠陥の是正及び脆弱性対策等のセキュリティ対策が有効に機能していることの継続的な監視と確認を行う　など	3.12 セキュリティアセスメント

4.2 クラウドサービス

用語定義

「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。

クラウドサービスを利用する場合は、そのクラウドサービスで要機密情報（機密性２情報・機密性３情報）を取り扱うかどうかによってセキュリティ対策が異なるよ！

要機密情報を取り扱うよ!

4.2.1、4.2.2へ

要機密情報を取り扱わないよ!

4.2.3へ

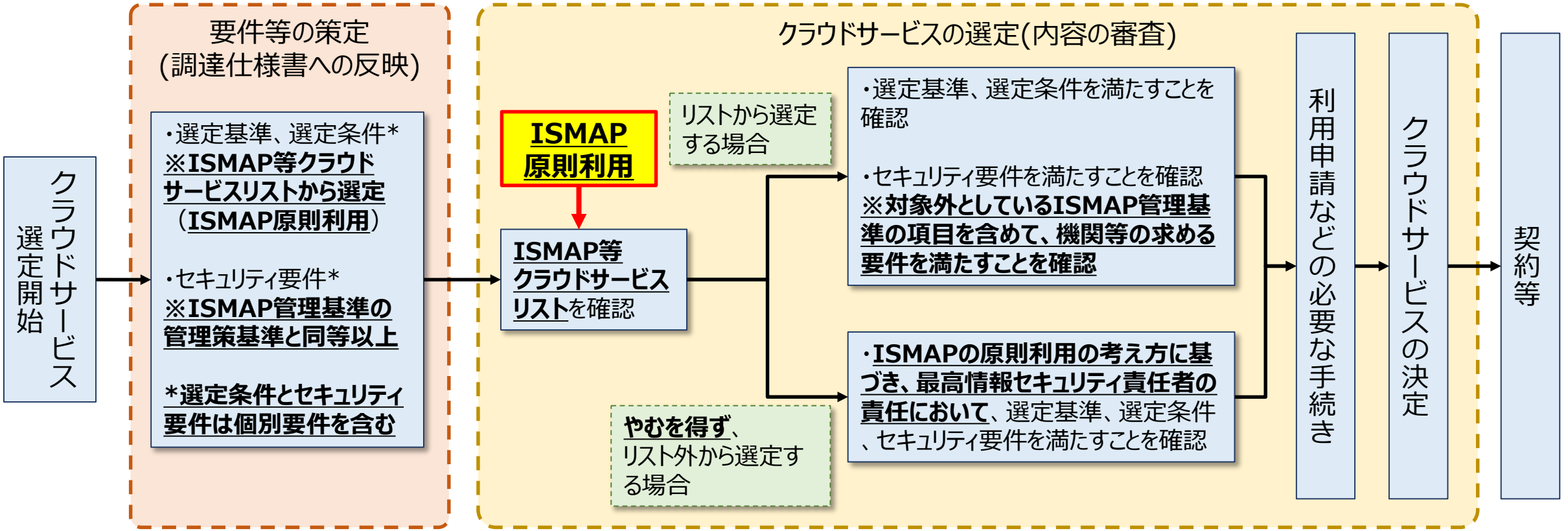
<クラウドサービスの例>

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

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

要機密情報を取り扱う場合は、原則、ISMAP／ISMAP-LIUサービスリスト（ISMAP等クラウドサービスリスト）からクラウドサービスを選定すること。
また、セキュリティ要件は、ISMAP管理基準の管理策基準が求める対策と同等以上の水準を求めること。

クラウドサービスの選定（要機密情報を取り扱う場合）のイメージ



4.2.3 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

要機密情報を取り扱わない場合であっても、利用に当たってのリスクが許容できるかを十分検討した上で、利用の可否を判断すること。
また、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずること。

考慮すべきリスクの例

- クラウドサービス提供者は、保存された情報を自由に利用することが可能である。
- 政府が利用等することで結果的に国民一般に、安全・安心なサービスであるとして推奨していると受け取られることがある。
- クラウドサービス提供者が国外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。

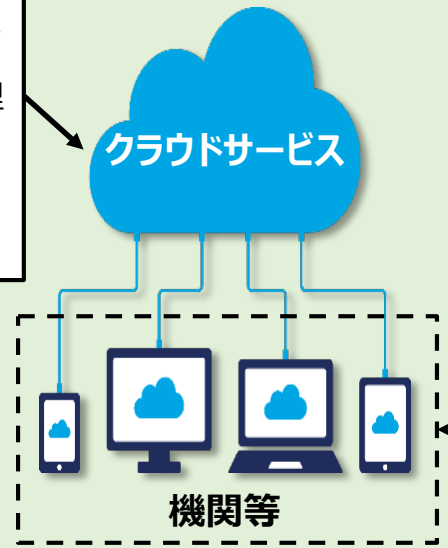
※上記以外のリスクの例は、ガイドラインの「（解説）遵守事項4.2.3(1)(a)(ア)「利用可能な業務の範囲」について」を参照

調達行為を伴わず要機密情報を取り扱わない場合においてクラウドサービスを利用等する際には、「**調達行為を伴わないＳＮＳ等の外部サービスの利用等に関する申合せ**」（※）に基づき、必要な場合において、内閣サイバーセキュリティセンターに対し、講ずべき必要な措置について、助言を求める必要があるよ。

※ガイドラインの「（解説）遵守事項4.2.3(2)(a)「利用に当たってのリスク」について」を参照

安全に利用するための対策の例

＜対策の例＞
- 管理機能に対して主体認証機能を適切に用いる
- アクセス制御の管理
- バックアップの取得
- 公開設定が正しく運用されていることを定期的に確認



＜対策の例＞
- 定期的に利用に係る注意喚起を実施
- インシデント発生時の連絡体制の整備

【参考】各種サービス・システムについて

サービス・システム名	説明	統一基準群における例
クラウドサービス ※関連する規程 4.2 クラウドサービス	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。	• 仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS） • データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS） • Web会議サービス • ソーシャルメディア • 検索サービス、翻訳サービス、地図サービス
業務委託サービス ※関連する規程 4.1.2(4) 機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策	**機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス**。 なお、業務委託サービスは、契約をもって外部の者に実施させる「業務委託」により提供を受けるサービスであることから、**セキュリティ要件を調達仕様書に個別に記載するなどにより情報セキュリティを確保する必要**がある。 また、**定型約款や規約等への同意のみで利用可能となるサービスは**、機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱うために必要なセキュリティ要件を満たすことが一般的に困難であることから、**業務委託サービスには含まれない**。	• ホスティングサービス • インターネット回線接続サービス
政府共通利用型システム ※関連する規程 5.4 政府共通利用型システム	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、以下のいずれかに該当する情報システム ① 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 ② 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	• 例示なし ＜※左記の①・②は以下が考えられる※＞ ① 他の情報システムにセキュリティ機能（主体認証機能）を提供する「職員認証サービス（GIMA）」等 ② デジタル庁が提供する「ガバメントソリューションサービス（GSS）」等

4.3.1 機器等の調達

必要なセキュリティ機能が装備されていない、機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えない等を防止するため、機器等の選定基準及び納入時の確認・検査手続を整備すること。

用語定義

- 「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。

機器等の選定基準

統括情報セキュリティ責任者

整備

機器等の選定基準

- 対策基準の該当項目を満たすために機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備する。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直す
- 必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加える
  - ✓ 機関等と調達先が連携して原因を調査・排除できる体制を整備している
  - ✓ 「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申し合わせ）に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずる
- 第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の評価項目とする

納入時の確認・検査手続

統括情報セキュリティ責任者

整備

納入時の確認・検査手続

- 受入れテスト等によって、調達時に指定したセキュリティ要件の実装状況を確認する手続を定める
- 内部監査の結果を報告させる等によって、機器等に不正プログラムが混入していないことを確認する手続を定める

情報システムセキュリティ責任者

定められた検査手続きに従い、情報セキュリティ対策に係る要件が満たされていることを確認する（遵守事項5.2.2(2)(a)）

統一基準の目次構成（第５部　情報システムのライフサイクル）

部	部のタイトル	主な規定内容
5	情報システムのライフサイクル	➢ 情報システムの分類 ➢ 情報システムのライフサイクルの各段階（要件定義・構築・運用・更改・廃棄）における対策 ➢ 情報システムの運用継続計画 ➢ 政府共通利用型システム
6	情報システムの構成要素	➢ 端末、特定用途機器（IoT機器を含む）、通信回線の対策 ➢ サーバ装置、電子メール、ウェブ、DNS、データベースの対策 ➢ 情報システムの基盤を管理又は制御するソフトウェアの対策 ➢ アプリケーション・コンテンツの対策
7	情報システムのセキュリティ要件	➢ 情報システムのセキュリティ機能 ✓ 主体認証、アクセス制御、権限管理、ログ管理、暗号・電子署名、監視 ➢ 情報セキュリティの脅威への対策 ✓ ソフトウェア脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策 ➢ ゼロトラストアーキテクチャ
8	情報システムの利用	➢ 端末、電子メール、Web会議、クラウドサービスなどの情報システムの利用時の対策 ➢ ソーシャルメディアサービスによる情報発信時の対策 ➢ テレワーク実施時の対策

第５部　情報システムのライフサイクル

5.1　情報システムの分類

5.1.1　情報システムの分類基準等の整備
（1）情報システムにおける分類のための運用規程の整備
（2）情報システムの分類基準に基づいた情報セキュリティ対策に係る運用規程の整備
（3）情報システムの分類基準に基づいた分類の実施
（4）情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用規程の見直し

5.2　情報システムのライフサイクルの各段階における対策

5.2.1　情報システムの企画・要件定義
（1）実施体制の確保
（2）情報システムの分類基準に基づいた分類の実施
（3）情報システムのセキュリティ要件の策定

5.2.2　情報システムの調達・構築
（1）情報システムの構築時の対策
（2）納品検査時の対策

5.2.3　情報システムの運用・保守
（1）情報システムの運用・保守時の対策

5.2.4　情報システムの更改・廃棄
（1）情報システムの更改・廃棄時の対策

5.2.5　情報システムについての対策の見直し
（1）情報システムについての対策の見直し

5.3　情報システムの運用継続計画

5.3.1　情報システムの運用継続計画の整備・整合的運用の確保
（1）情報システムの運用継続計画の整備・整合的運用の確保

5.4　政府共通利用型システム

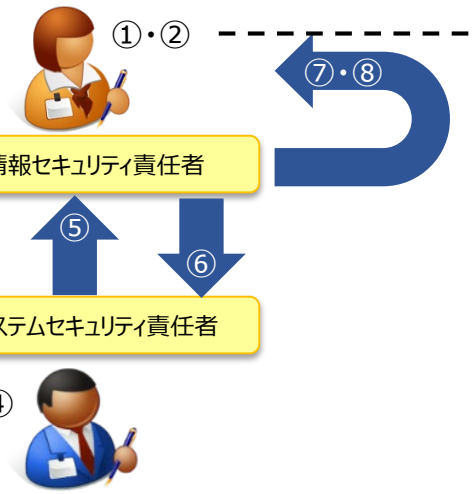
5.4.1　政府共通利用型システム管理機関における対策
（1）情報セキュリティ対策に関する運用管理規程の整備
（2）情報システム台帳及び情報システム関連文書の整備

5.4.2　政府共通利用型システム利用機関における対策
（1）政府共通利用型システム利用機関における体制の整備
（2）政府共通利用型システム利用機関における情報セキュリティ対策
（3）政府共通利用型システム利用機関における機器等の管理

5.1 情報システムの分類

自組織が所管する情報システムの分類を行うこと。
分類の結果、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は、ベースラインとして全ての情報システムに必ず求める対策（基本セキュリティ対策）に加えて、より高度な対策（追加セキュリティ対策）を求めること。

情報システムの分類の流れ（例）

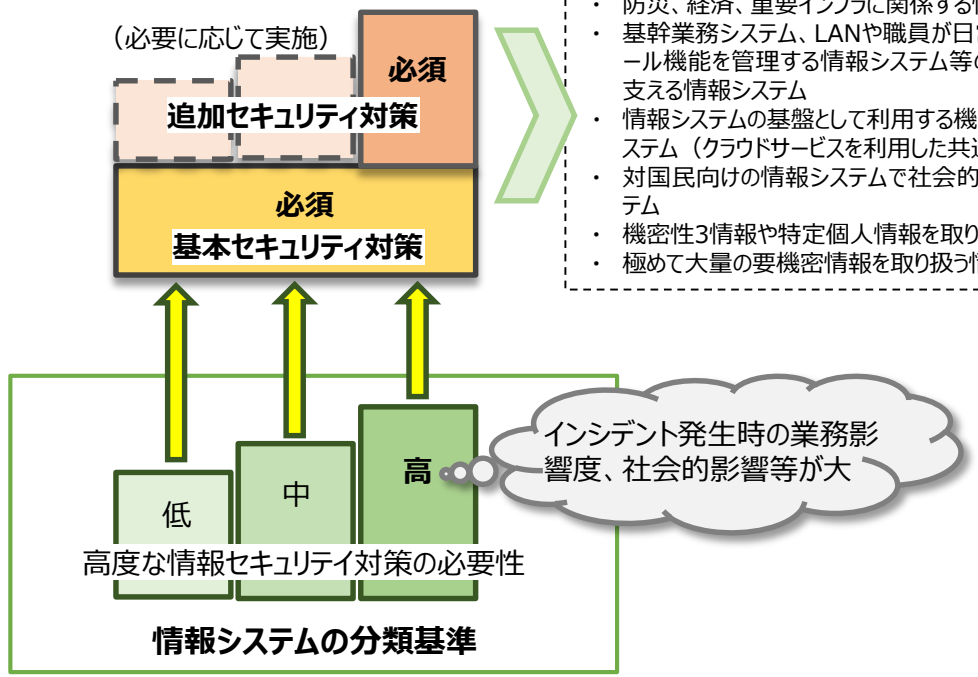


分類のイメージ（例）

情報システム名	重要度
Aシステム	中
Bシステム	高
Cシステム	低

① 情報システムの分類基準を定める
② 基本セキュリティ対策と追加セキュリティ対策を定める
③ 情報システムの分類を指示
④ 情報システムの分類を実施
⑤ 結果を報告
⑥ 必要に応じて、上位又は下位の分類への修正を指示
⑦ ①・②を定期的な確認による見直し
⑧ 情報システムの分類が適切に行われていることを定期的に確認

情報システムの分類基準・基本/追加セキュリティ対策のイメージ（例）



「高」として想定する情報システム（参考）

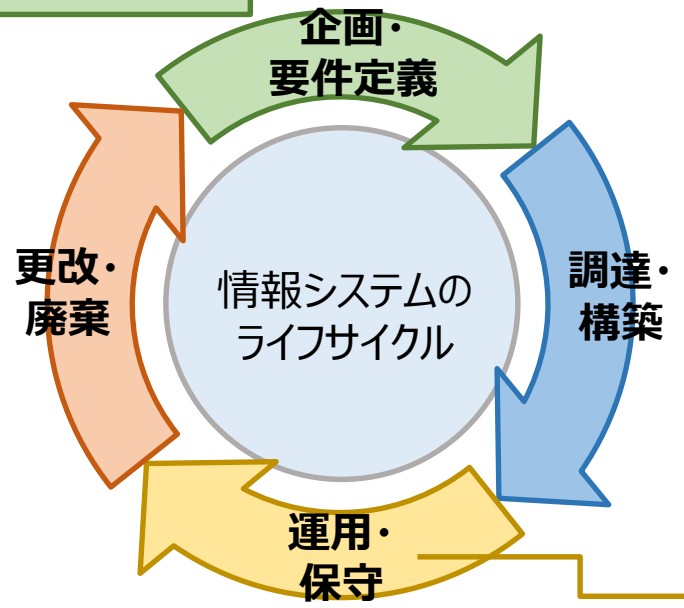
- 防災、経済、重要インフラに関係する情報システム
- 基幹業務システム、LANや職員が日常的に利用するPCやメール機能を管理する情報システム等の組織の業務の根幹を支える情報システム
- 情報システムの基盤として利用する機関等が所管する情報システム（クラウドサービスを利用した共通基盤を含む）
- 対国民向けの情報システムで社会的影響が大きい情報システム
- 機密性3情報や特定個人情報を取り扱う情報システム
- 極めて大量の要機密情報を取り扱う情報システム

5.2 情報システムのライフサイクルの各段階における対策

5.2.1

- 情報システムの分類の実施
- 分類に応じたセキュリティ要件の策定と調達仕様書等への明記
- 「SBDマニュアル(※)」の活用　等

(※)SBDマニュアル：情報システムに係る政府調達におけるセキュリティ要件策定マニュアル



5.2.2

- セキュリティ要件が適切に実装されるようにセキュリティ機能を設計
- セキュリティ要件が満たされていることを受け入れ検査の際に確認
- 情報システム台帳、情報システム関連文書の整備　等

5.2.3

- 監視を含むセキュリティ機能の運用
- 構成や設定の変更をした際、対策が有効に機能していることを確認
- 情報システム台帳、情報システム関連文書の更新
- 危機的事象発生時に対処が行えるよう、バックアップの取得や復旧手順の確認　等

5.2.4

- 更改の際、情報の移行作業における情報漏えい対策
- 廃棄の際、情報の抹消　等

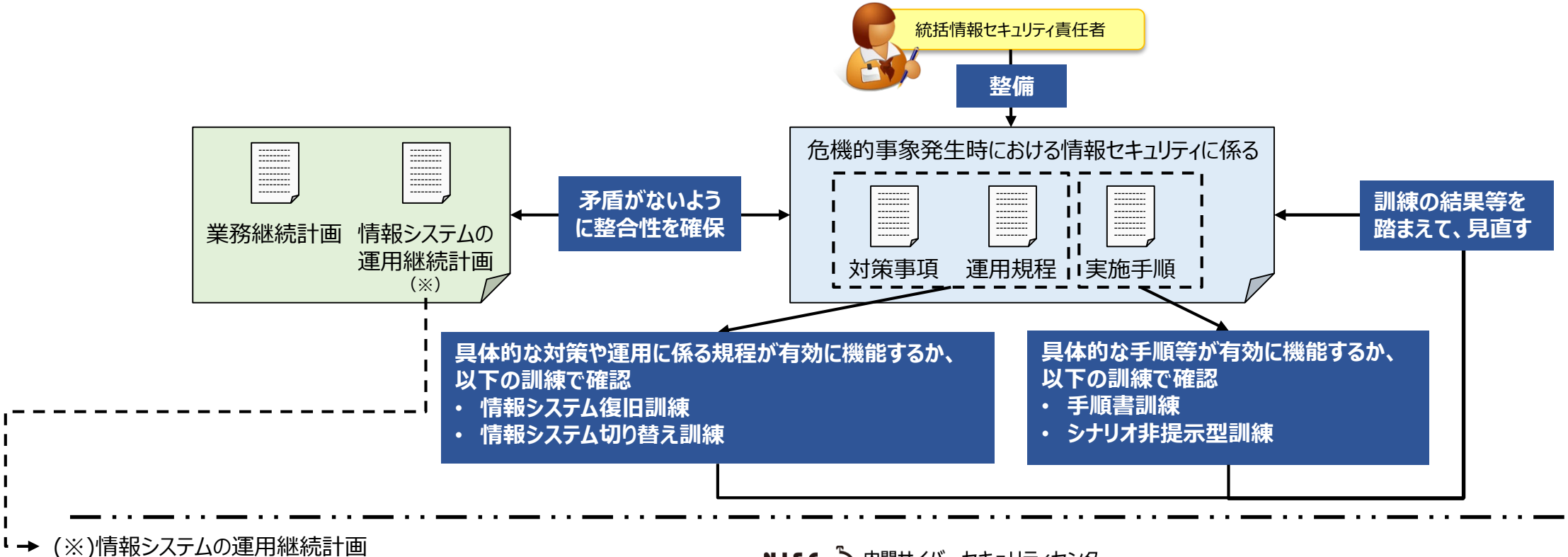
5.2.5

- 対策推進計画に基づいた対策の見直し
- 機関等内の横断的な改善指示に基づいた対策の見直し　等

対策の見直し

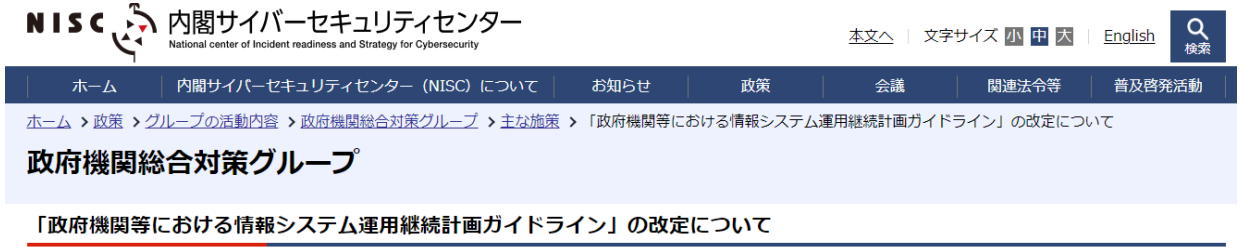
5.3 情報システムの運用継続計画

地震、火災、感染症、情報セキュリティインシデント等の危機的事象発生時でも運用を継続させる必要がある情報システムは、情報システムの運用継続計画等と整合性を確保した上で、情報セキュリティに係る対策を定めること。



(※)情報システムの運用継続計画

機関等の情報システムの運用継続計画を整備する際は、NISC「政府機関等における情報システム運用継続計画ガイドライン」に基づき、策定するとよい。
（https://www.nisc.go.jp/policy/group/general/itbcp-guideline.html）



5.4 政府共通利用型システム

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、以下のいずれかに該当する情報システム

① 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

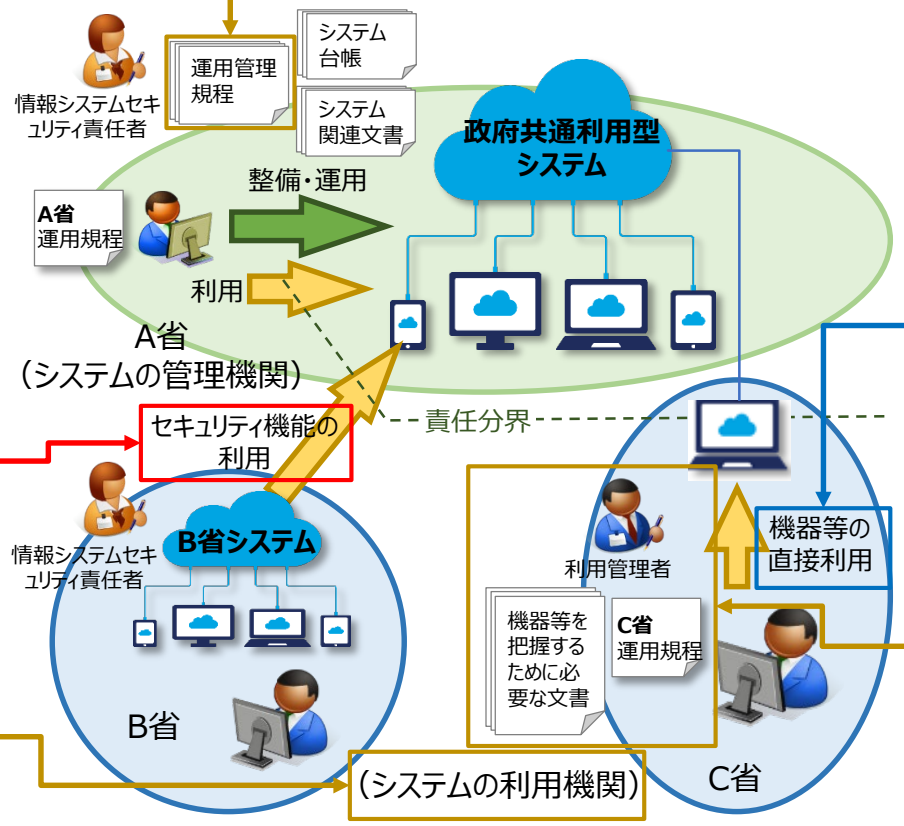
② 他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システム

- 管理機関は、管理機関と利用機関の責任分界、平常時及び非常時の協力・連携体制、非常時の具体的対応策を網羅した情報セキュリティ対策に関する運用管理規程を整備

A省側のシステムは、**①「他の機関等(B省)が整備する情報システムに対し、同情報システム(B省システム)と連携して、情報システム(B省システム)のセキュリティ機能を提供する情報システム」**に該当するため、A省側のシステムは「政府共通利用型システム」となる

※①に該当するシステムは、他の情報システムにセキュリティ機能（主体認証機能）を提供する「職員認証サービス（GIMA）」等が考えられる

- 利用機関は、管理機関が定める運用管理規程に基づき体制を整備、その他利用側でのセキュリティ対策を実施



A省側のシステムは、**②「他の機関等(C省)に機器等を提供し、他の機関等の職員等(C省の職員等)が利用する情報システム」**に該当するため、A省側のシステムは「政府共通利用型システム」となる

※②に該当するシステムは、デジタル庁が提供する「ガバメントソリューションサービス（GSS）」等が考えられる

- 提供を受ける機器等を直接利用する利用機関は、利用管理者を定め、運用規程の整備、提供を受けた機器等を把握するために必要な文書の整備、その他機器等の直接利用側でのセキュリティ対策を実施

統一基準の目次構成（第６部　情報システムの構成要素）

部	部のタイトル	主な規定内容
5	情報システムのライフサイクル	➢ 情報システムの分類 ➢ 情報システムのライフサイクルの各段階（要件定義・構築・運用・更改・廃棄）における対策 ➢ 情報システムの運用継続計画 ➢ 政府共通利用型システム
6	情報システムの構成要素	➢ 端末、特定用途機器（IoT機器を含む）、通信回線の対策 ➢ サーバ装置、電子メール、ウェブ、DNS、データベースの対策 ➢ 情報システムの基盤を管理又は制御するソフトウェアの対策 ➢ アプリケーション・コンテンツの対策
7	情報システムのセキュリティ要件	➢ 情報システムのセキュリティ機能 ✓ 主体認証、アクセス制御、権限管理、ログ管理、暗号・電子署名、監視 ➢ 情報セキュリティの脅威への対策 ✓ ソフトウェア脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策 ➢ ゼロトラストアーキテクチャ
8	情報システムの利用	➢ 端末、電子メール、Web会議、クラウドサービスなどの情報システムの利用時の対策 ➢ ソーシャルメディアサービスによる情報発信時の対策 ➢ テレワーク実施時の対策

第６部　情報システムの構成要素

6.1　端末

6.1.1　端末

（1）端末の導入時の対策
（2）端末の運用時の対策
（3）端末の運用終了時の対策

6.1.2　要管理対策区域外での端末利用時の対策

（1）機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用規程の整備
（2）機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策

6.1.3　機関等支給以外の端末の導入及び利用時の対策

（1）機関等支給以外の端末の利用可否の判断
（2）機関等支給以外の端末の利用に関する運用規程等の整備
（3）機関等支給以外の端末の利用に関する責任者の策定
（4）機関等支給以外の端末の利用時の対策

6.2　サーバ装置

6.2.1　サーバ装置

（1）サーバ装置の導入時の対策
（2）サーバ装置の運用時の対策
（3）サーバ装置の運用終了時の対策

6.2.2　電子メール

（1）電子メールの導入時の対策

6.2.3　ウェブ

（1）ウェブサーバの導入・運用時の対策

6.2.4　ドメインネームシステム（DNS）

（1）DNSの導入時の対策
（2）DNSの運用時の対策

6.2.5　データベース

（1）データベースの導入・運用時の対策

6.3　複合機・特定用途機器

6.3.1　複合機・特定用途機器

（1）複合機
（2）IoT機器を含む特定用途機器

6.4　通信回線

6.4.1　通信回線

（1）通信回線の導入時の対策
（2）機関等外通信回線の接続時の対策
（3）通信回線の運用時の対策

6.4.2　通信回線装置

（1）通信回線装置の導入時の対策
（2）通信回線装置の運用時の対策
（3）通信回線装置の運用終了時の対策

6.4.3　無線LAN

（1）無線LAN環境導入時の対策

6.4.4　IPv6通信回線

（1）IPv6通信を行う情報システムに係る対策
（2）意図しないIPv6通信の抑止・監視

6.5　ソフトウェア

6.5.1　情報システムの基盤を管理又は制御するソフトウェア

（1）情報システムの基盤を管理又は制御するソフトウェア導入時の対策
（2）情報システムの基盤を管理又は制御するソフトウェア運用時の対策

6.6　アプリケーション・コンテンツ

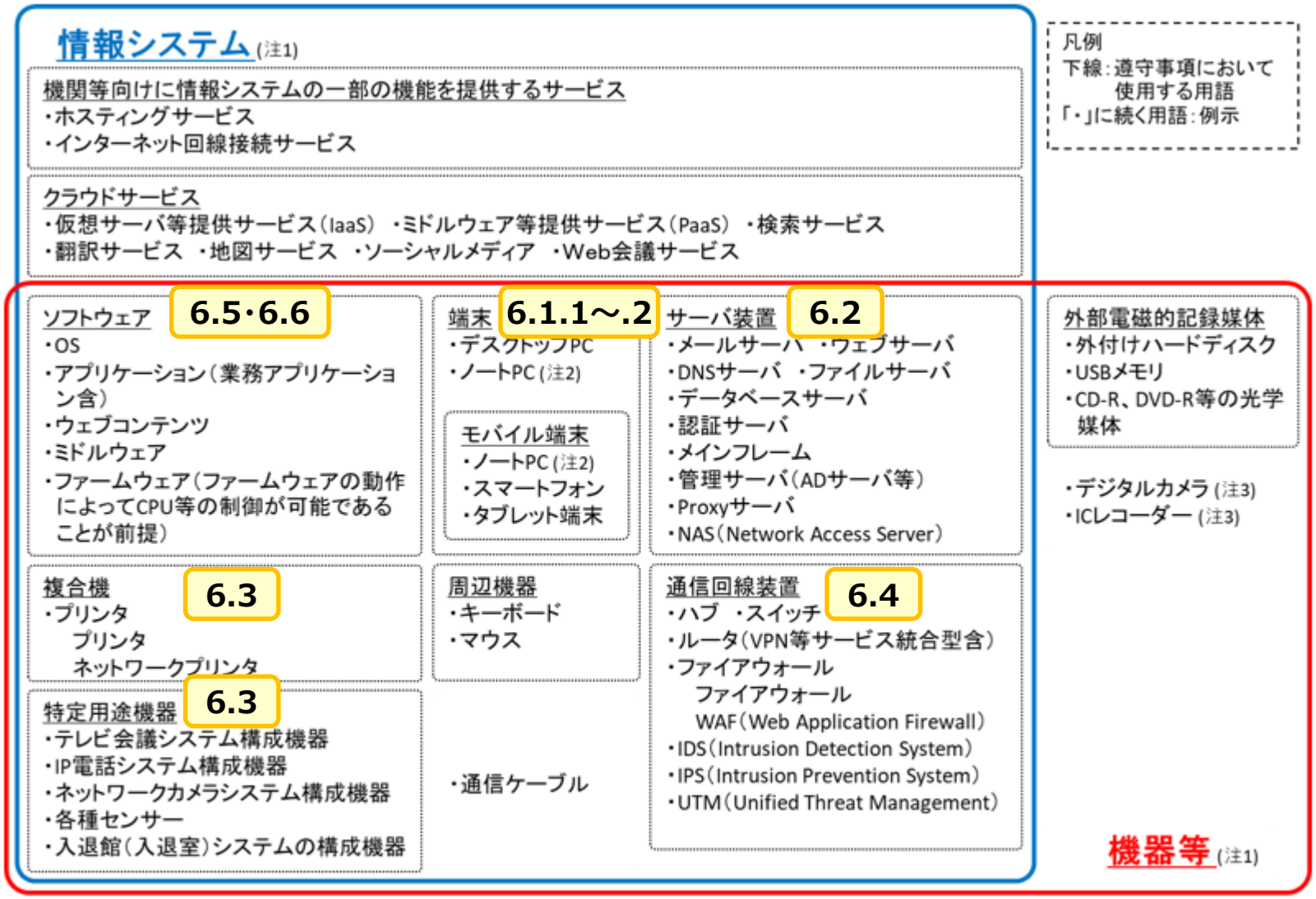
6.6.1　アプリケーション・コンテンツの作成・運用時の対策

（1）アプリケーション・コンテンツの作成に係る運用規程の整備
（2）アプリケーション・コンテンツのセキュリティ要件の策定
（3）アプリケーション・コンテンツの開発時の対策
（4）アプリケーション・コンテンツの運用時の対策

6.6.2　アプリケーション・コンテンツ提供時の対策

（1）政府ドメイン名の使用
（2）不正なウェブサイトへの誘導防止
（3）アプリケーション・コンテンツの告知

第６部　情報システムの構成要素



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。

6.1.1 端末・6.1.2 要管理対策区域外での端末利用時の対策

端末は、不正侵入などの外的要因による脅威や、不注意による不正プログラム感染や紛失などの内的要因による脅威が考えられるため、物理的・技術的な対策とともに、職員等が守るルールを整備すること。

「端末」とは？

職員等が情報処理を行うために直接操作する機器をいい、特に断りがない限り、機関等が調達又は開発するものをいう。
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。

- ✓「端末」の例：機関等が調達したデスクトップPC・ノートPC・スマートフォン・タブレット端末
- ✓「機関等支給以外の端末」の例：職員等の私物のスマートフォン

6.1.1

導入時

- セキュリティワイヤによる固定、のぞき見防止フィルタ等の物理的な脅威から保護するための対策を講ずる
- 端末に接続を認める機器を定める。また、それ以外の機器は接続させない
- 端末で利用を認めるソフトウェアを定める。また、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講ずる
- 端末で利用するソフトウェアは、セキュリティパッチ適用等の脆弱性対策を実施する

運用時

- 利用を認めるソフトウェアを定期的に確認し見直す
- 端末で利用されているソフトウェアの状態を定期的に調査。最新のセキュリティパッチが未適用、不要なプロトコルやポート、サービスが動作している等の不適切な状態の端末は改善する

運用終了時

- 端末の電磁的記録媒体（HDD・SSDなど）に保存されている情報を抹消する

6.1.2

要管理区域外での利用時

- 利用手順・許可手続を定める
- 端末に情報を保存させない機能（シンクライアントなど）又は端末に保存される情報を暗号化する機能を設ける
- 機関等外通信回線（自宅のネットワークなど）に接続された端末を、機関等内通信回線（機関等LANなど）に接続させる際の不正プログラムに感染するリスクを踏まえた技術的な措置を講ずる

6.1.3 機関等支給以外の端末の導入及び利用時の対策

業務の際は、機関等が支給する端末の利用が原則となる。
やむを得ず(※1)、職員等が所有する端末（職員等の私物のスマートフォンなど）を業務で利用する際の対策例は以下。

- 最高情報セキュリティ責任者による利用可否の判断。
- 利用手順(※2)や利用許可手続などのルールを整備。
- 安全管理措置等(※2)を講ずる。

※1
職員等が所有する端末は、機関等が求める情報セキュリティの水準を満たさない可能性があるんだ。
だから、職員等が所有する端末を業務で利用するのは、災害発生時などのやむを得ない場合に限ることが重要だよ。

※2 利用手順や安全管理措置の対策例

6.2 サーバ装置

全てのサーバ装置は、6.2.1「サーバ装置」に定める共通的な対策を行うこと。
電子メールサーバ等の個別のサーバは、共通的な対策に加えて、6.2.2「電子メール」等の個別に定める対策を行うこと。

6.2.1 サーバ装置 — 共通的な対策例

利用を認めるソフトウェアや、接続を認めた機器等を定めることなどの、端末の対策事項に加えて・・・

導入時
- サーバ装置の冗長構成など、可用性を確保すること
- サーバ装置のバックアップを取得すること

運用時
- サーバ装置を監視すること
- サーバ装置の復旧手順を見直すこと

運用終了時
- サーバ装置の電磁的記録媒体に保存されている情報を抹消すること

個別の対策例

6.2.2 電子メール
- 電子メールの不正な中継を行わないように設定すること
- 電子メールのなりすましの防止策を講ずること
- 電子メールのサーバ間通信の暗号化の対策を講ずること

6.2.3 ウェブ
- 全ての情報に対する暗号化及び電子証明書による認証の対策を講じること
- ウェブサーバが備える機能のうち、必要な機能のみを利用すること

6.2.4 DNS
- コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること
- キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること

6.2.5 データベース
- データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること
- データの不正な操作を検知できるよう、対策を講ずること

6.3 複合機・特定用途機器

複合機・特定用途機器（IoT機器を含む）は、インターネットを含む通信回線に接続することが多く、外部からの様々な脅威が考えられる。
これらの機器は情報システムの構成要素であることを認識した上で、確実に対策を講ずること。

6.3 複合機・特定用途機器
6.3.1 複合機・特定用途機器

複合機

対策例

- 調達の際、「**IT製品の調達におけるセキュリティ要件リスト**」を参照し、適切なセキュリティ要件を策定する
- 利用しない機能は**停止**する、インターネットを介して保守を行う場合は**通信制御**を行うなどの運用中の対策を講ずる
- 運用を終了する際、電磁的記録媒体に保存されている情報を**抹消**する

特定用途機器（IoT機器を含む）

特定用途機器とは？

- ネットワークカメラシステム、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特有の機器であって、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（ROMなど）を備えているもの

IoT機器とは？

- 特定用途機器の内、インターネットに接続する機能を備えるカメラやセンサー等の機器

対策例

- 主体認証情報（例：パスワード）を**初期設定から変更**する
- 機器のソフトウェアの**バージョンアップ**や**セキュリティパッチ適用**などの脆弱性対策を講ずる
- 不正なアクセスや不正な通信が行われていないかなどを**監視**する
- 機器を廃棄する際、内蔵電磁的記録媒体（ROMなど）に保存されている情報を**抹消**する

特に特定用途機器(IoT機器を含む)は、機能上の制約等によって必要な対策を講じられない可能性がある。
そのため、セキュリティ要件を策定した上で、必要な対策を講ずることが可能な機器を調達することが重要。

6.4 通信回線

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、通信を介して行われる場合が多い。そのため、情報システムの構築時からリスクを十分検討し、必要な対策を講ずること。

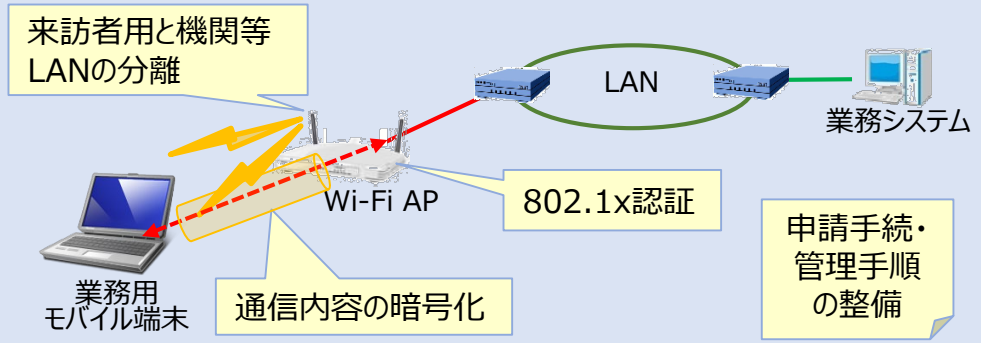
6.4.1 通信回線の対策例

- 通信が必要な単位でセグメントを分割し、セグメント間の通信を必要最小限とするアクセス制御
- 通信内容の暗号化
- 端末、サーバ装置接続時の認証
- ファイアウォール、WAF等による通信制御
- IDS/IPSにより不正アクセスの検知・遮断
- 不正通信の監視

6.4.2 通信回線装置の対策例

- 動作するために必要なソフトウェアを定める
- 利用するソフトウェアについて、セキュリティパッチ適用等の脆弱性対策を実施
- 要管理対策区域に設置する等の物理的な保護
- 運用状態を復元するために必要な情報のバックアップを取得
- 運用終了時、電磁的記録媒体に保存されている情報を抹消

6.4.3 無線LAN回線の対策例



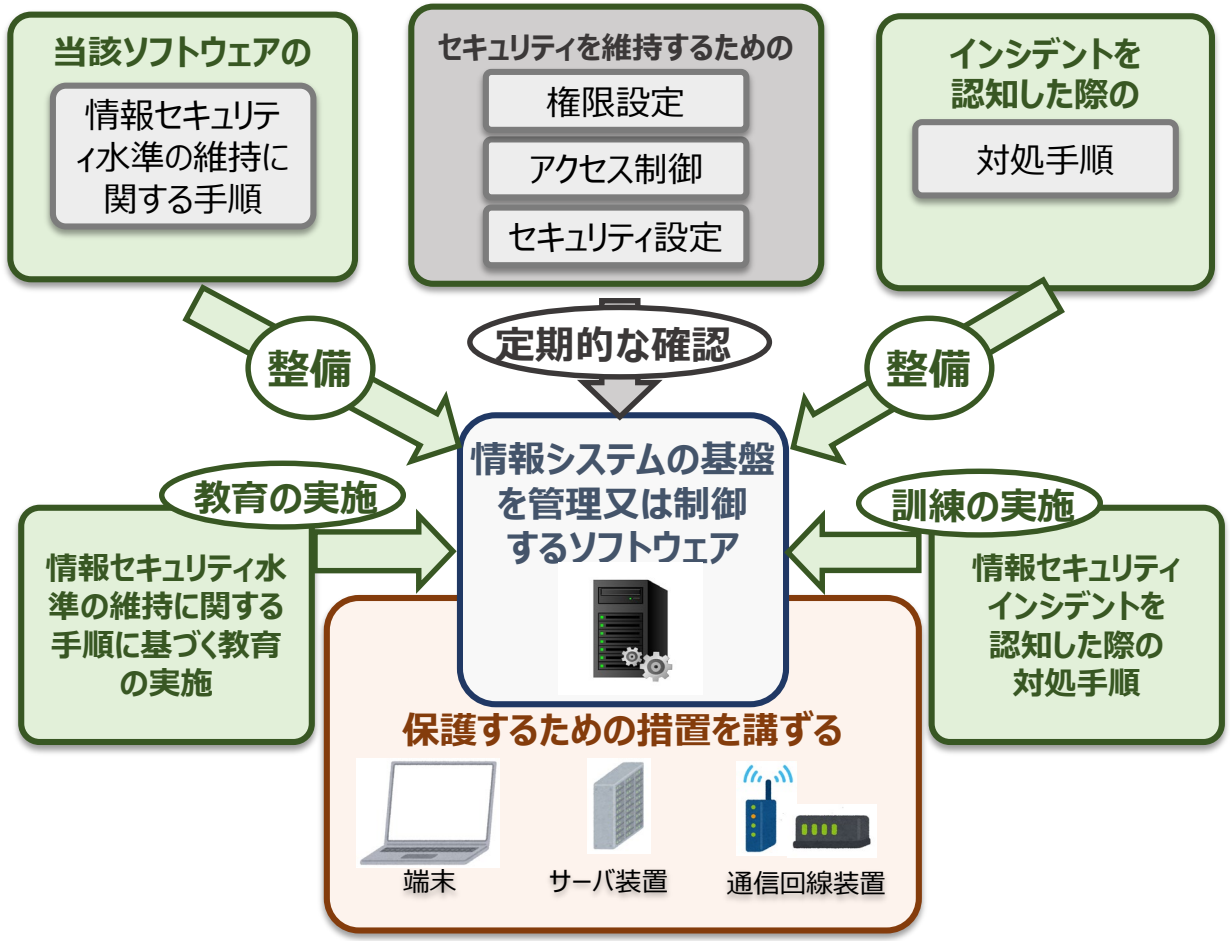
6.4.4 IPv6通信時の対策

- IPv6 Ready Logo Programに基づくPhase-2準拠製品を、可能な場合には選択する
- グローバルIPアドレスによる直接の到達における脅威への対策
- IPv4通信とIPv6通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生への対策

6.5 ソフトウェア

情報システムの基盤を管理又は制御するソフトウェア(※)は、重要な機能を有しており、悪用や不正アクセスなどがなされた場合、被害が広範囲に及ぶ可能性が高い。そのため、当該ソフトウェアを利用する際の設定不備を防ぐための手順の整備などの対策を講ずること。

6.5 ソフトウェア
6.5.1 情報システムの基盤を管理又は制御するソフトウェア



※情報システムの基盤を管理又は制御するソフトウェアとは？

端末やサーバ装置、ネットワークなどを管理又は制御するための権限を用いてアクセスが可能な機能を有しているソフトウェア。

＜例＞
- 端末やサーバ装置、通信回線装置等を制御するソフトウェア
- 統合的な主体認証を管理するソフトウェア
- ネットワークを制御・管理するソフトウェア
- 資産を管理するソフトウェア
- 監視に関連するソフトウェア
- 情報システムのセキュリティ機能として使用するソフトウェア

6.6 アプリケーション・コンテンツ

国民等の利用者が、アプリケーションやウェブサイトを利用する際に、不正プログラムに感染しやすい環境を強制されることや、不正なウェブサイトに誘導されること等がないように、作成・運用・提供における対策を講ずること。

作成時の対策例

- 脆弱なOSやソフトウェアの利用を強制させないよう、提供方式を定める
- 利用者の情報を利用者の意思に反して第三者に提供される機能（トラッキング処理）の禁止
- 脆弱性診断の実施
- SQLインジェクション・OSコマンドインジェクション等への対策

運用時の対策例

OSやソフトウェアのサポート状況を考慮し、サポート切れの際にこれらのOS等の利用を強制させることのないように、提供方式を見直す

提供

国民等

ウェブサイトのドメイン名は原則政府ドメイン名を使用する

不正なウェブサイトへ誘導させないための対策
- ✓ 検索エンジン最適化措置（SEO対策）
- ✓ 注意喚起の実施や検索サイト業者に対して検索結果に表示されないよう依頼
- ✓ 不審なウェブサイトの通報を受ける体制の整備

正規のウェブサイトへ誘導させるための対策
- ✓ 原則、URLを用いた直接的な誘導
- ✓ 間接的な誘導（検索サイトによる検索を促す方法など）の際は、URLと一緒に表示
- ✓ 二次元コードを用いる際は、誘導先の内容と一緒に表示

統一基準の目次構成（第７部　情報システムのセキュリティ要件）

部	部のタイトル	主な規定内容
5	情報システムのライフサイクル	➢ 情報システムの分類 ➢ 情報システムのライフサイクルの各段階（要件定義・構築・運用・更改・廃棄）における対策 ➢ 情報システムの運用継続計画 ➢ 政府共通利用型システム
6	情報システムの構成要素	➢ 端末、特定用途機器（IoT機器を含む）、通信回線の対策 ➢ サーバ装置、電子メール、ウェブ、DNS、データベースの対策 ➢ 情報システムの基盤を管理又は制御するソフトウェアの対策 ➢ アプリケーション・コンテンツの対策
7	情報システムのセキュリティ要件	➢ 情報システムのセキュリティ機能 ✓ 主体認証、アクセス制御、権限管理、ログ管理、暗号・電子署名、監視 ➢ 情報セキュリティの脅威への対策 ✓ ソフトウェア脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策 ➢ ゼロトラストアーキテクチャ
8	情報システムの利用	➢ 端末、電子メール、Web会議、クラウドサービスなどの情報システムの利用時の対策 ➢ ソーシャルメディアサービスによる情報発信時の対策 ➢ テレワーク実施時の対策

第７部　情報システムのセキュリティ要件

7.1　情報システムのセキュリティ機能

7.1.1　主体認証機能
（1）主体認証機能の導入
（2）識別コード及び主体認証情報の管理

7.1.2　アクセス制御機能
（1）アクセス制御機能の導入

7.1.3　権限の管理
（1）権限の管理

7.1.4　ログの取得・管理
（1）ログの取得・管理

7.1.5　暗号・電子署名
（1）暗号化機能・電子署名機能の導入
（2）暗号化・電子署名に係る管理

7.1.6　監視機能
（1）監視機能の導入・運用

7.2　情報セキュリティの脅威への対策

7.2.1　ソフトウェアに関する脆弱性対策
（1）ソフトウェアに関する脆弱性対策の実施

7.2.2　不正プログラム対策
（1）不正プログラム対策の実施

7.2.3　サービス不能攻撃対策
（1）サービス不能攻撃対策の実施

7.2.4　標的型攻撃対策
（1）標的型攻撃対策の実施

7.3　ゼロトラストアーキテクチャ

7.3.1　動的なアクセス制御の実装時の対策
（1）動的なアクセス制御における責任者の設置
（2）動的なアクセス制御の導入方針の検討
（3）動的なアクセス制御の実装時の対策

7.3.2　動的なアクセス制御の運用時の対策
（1）動的なアクセス制御の実装方針の見直し
（2）リソースの信用情報に基づく動的なアクセス制御の運用時の対策

7.1 情報システムのセキュリティ機能

情報システム及び情報システムに保存される情報に対する脅威を想定し、その脅威に対抗するために必要なセキュリティ機能を適切に導入・運用すること。

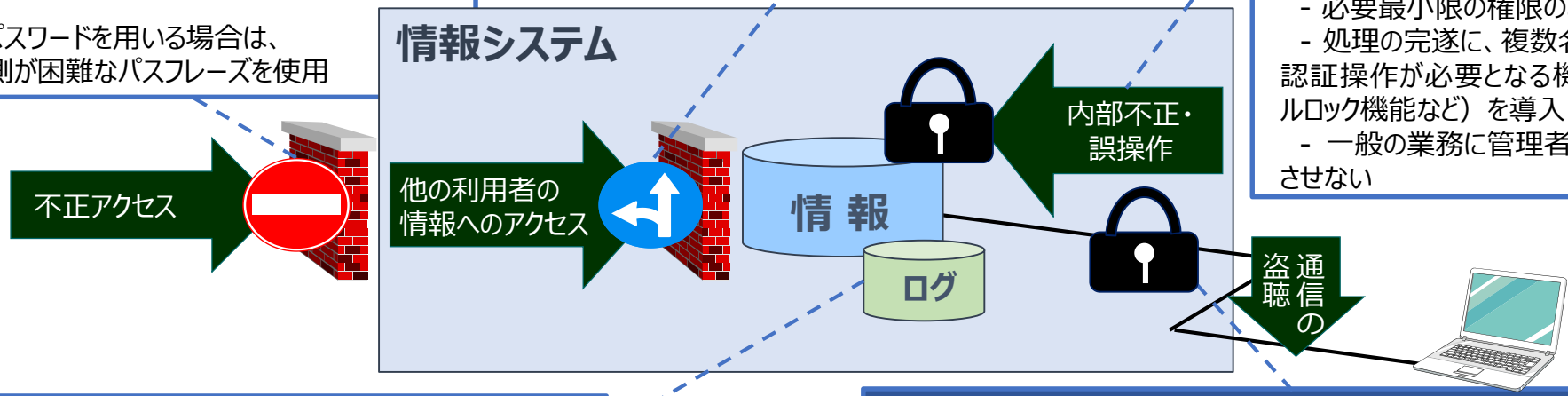
想定される主な脅威とセキュリティ機能による対策例

7.1.1 主体認証機能

・ リモートアクセスや管理者アカウントによるログインの際は、多要素主体認証方式を用いる
・ パスワードを用いる場合は、推測が困難なパスフレーズを使用

7.1.2 アクセス制御機能

・ 権限を有する者のみがアクセス制御の設定等を行うことができる機能を導入



7.1.3 権限の管理

・ 管理者権限の管理
- 必要最小限の権限のみ付与
- 処理の完遂に、複数名による主体認証操作が必要となる機能（デュアルロック機能など）を導入
- 一般の業務に管理者権限を使用させない

7.1.4 ログの取得・管理

・ 定期的にログを点検又は分析するため、ログを集計し、時系列に表示し、報告書を作成するなどの作業を自動化する機能を導入

7.1.5 暗号・電子署名

・ CRYPTREC「電子政府推奨暗号リスト」から、暗号・電子署名のアルゴリズム・鍵長、それらを利用した安全なプロトコルを決定
・ 電子署名の目的に合致する場合、GPKI(政府認証基盤)等の公的なPKIが発行する電子証明書を使用

7.1.6 監視機能

・ 外部からの不正アクセスや、内部の横方向の侵害（ラテラルムーブメント）を監視
・ SOCやNOC等のセキュリティ監視を業務委託することを検討

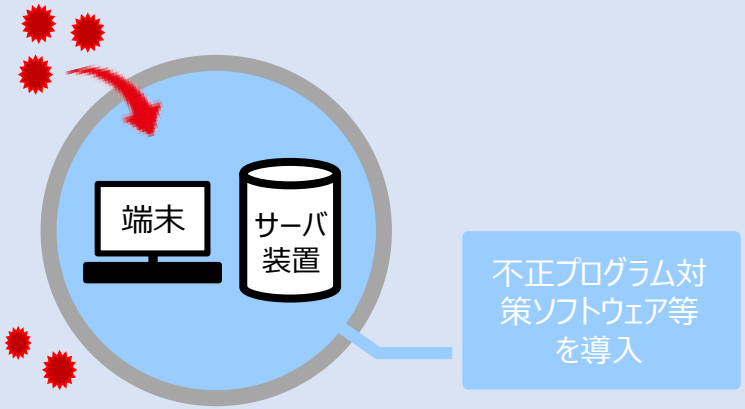
7.2 情報セキュリティの脅威への対策

情報システム及び情報システムに保存される情報に対する脅威を想定し、その脅威に対抗するために必要なセキュリティ対策を実施すること。

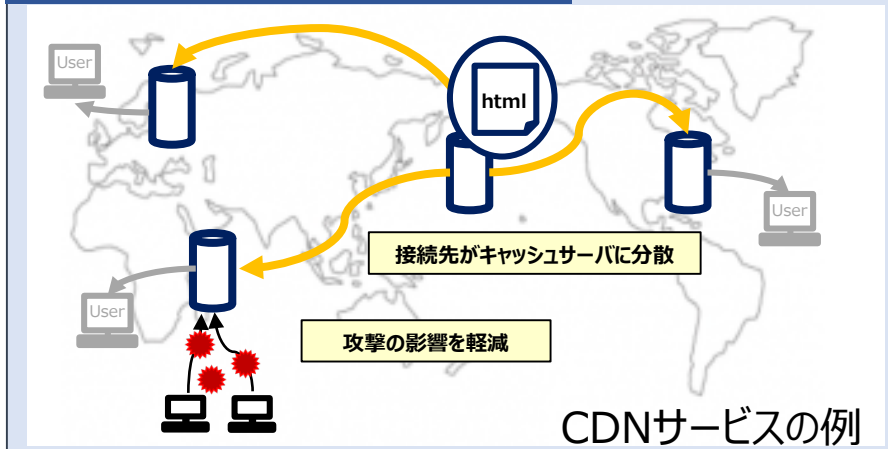
7.2.1 ソフトウェアに関する脆弱性対策

- ソフトウェア資産管理
- 脆弱性情報の収集
- 脆弱性診断
- セキュリティパッチ適用
- ゼロデイ攻撃への一時的な対処
- 脆弱性対策状況の定期的・適時の確認

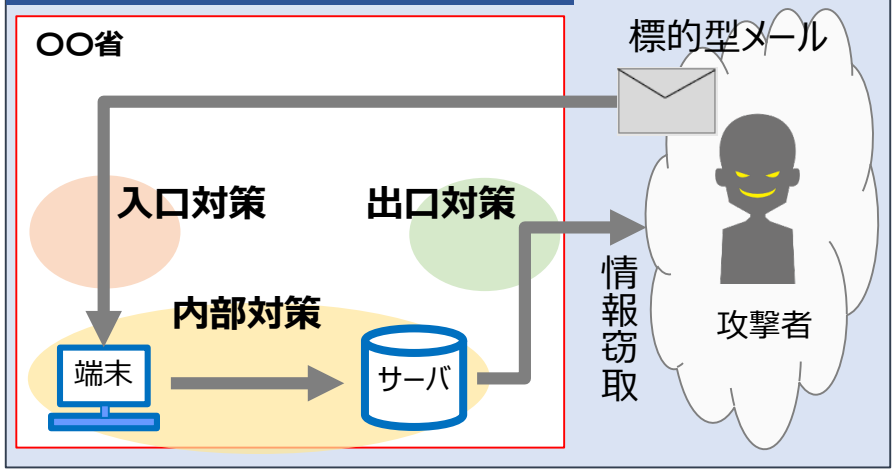
7.2.2 不正プログラム対策



7.2.3 サービス不能攻撃対策



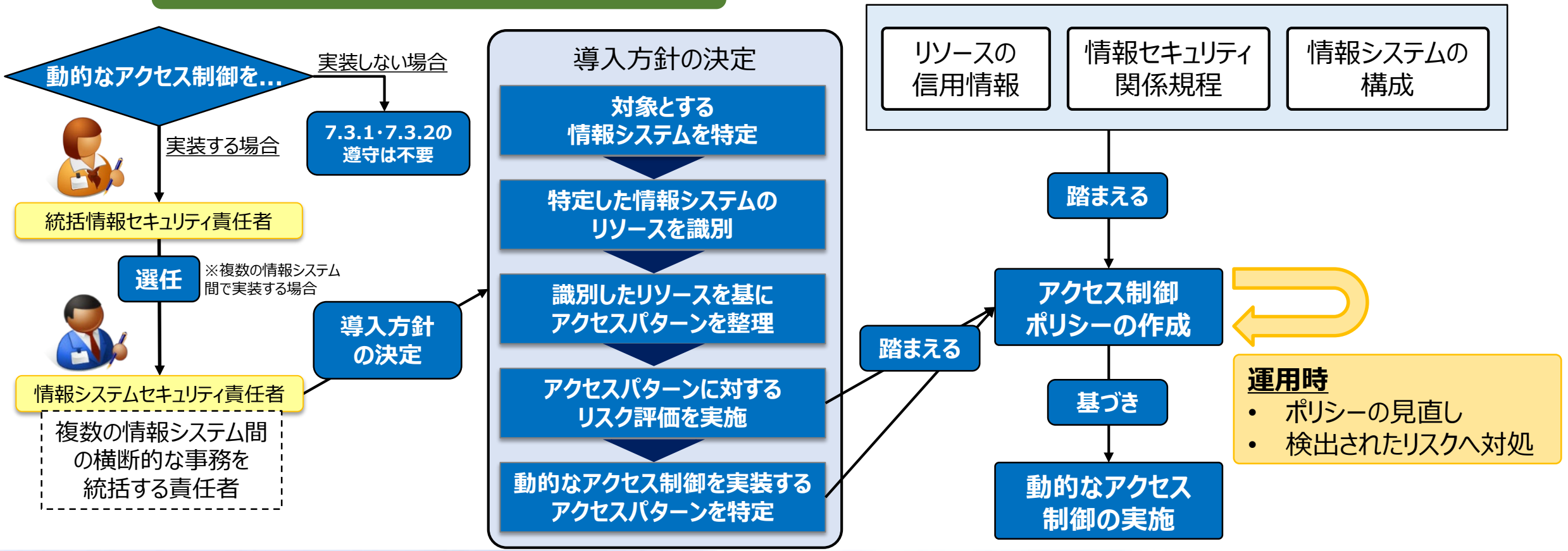
7.2.4 標的型攻撃対策



7.3.1・7.3.2　動的なアクセス制御の実装／運用時の対策

動的なアクセス制御とは？
ゼロトラストアーキテクチャに基づく情報資産の保護を行う仕組みを実現する機能の一部と考えられるものであって、特定のアクセスに対して、セッションが確立していない操作ごとに、都度、アクセス元の信用情報を動的に評価・検証し、アクセス制御を行うもの。

動的なアクセス制御の実装／運用のイメージ



統一基準の目次構成（第８部　情報システムの利用）

部	部のタイトル	主な規定内容
5	情報システムのライフサイクル	➢ 情報システムの分類 ➢ 情報システムのライフサイクルの各段階（要件定義・構築・運用・更改・廃棄）における対策 ➢ 情報システムの運用継続計画 ➢ 政府共通利用型システム
6	情報システムの構成要素	➢ 端末、特定用途機器（IoT機器を含む）、通信回線の対策 ➢ サーバ装置、電子メール、ウェブ、DNS、データベースの対策 ➢ 情報システムの基盤を管理又は制御するソフトウェアの対策 ➢ アプリケーション・コンテンツの対策
7	情報システムのセキュリティ要件	➢ 情報システムのセキュリティ機能 ✓ 主体認証、アクセス制御、権限管理、ログ管理、暗号・電子署名、監視 ➢ 情報セキュリティの脅威への対策 ✓ ソフトウェア脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策 ➢ ゼロトラストアーキテクチャ
8	情報システムの利用	➢ 端末、電子メール、Web会議、クラウドサービスなどの情報システムの利用時の対策 ➢ ソーシャルメディアサービスによる情報発信時の対策 ➢ テレワーク実施時の対策

8.1　情報システムのセキュリティ機能

8.1.1　情報システムの利用
（1）情報システムの利用に係る規定の整備
（2）情報システム利用者の規定の遵守を支援するための対策
（3）情報システムの利用時の基本的対策
（4）端末（支給外端末を含む）の利用時の対策
（5）電子メール・ウェブの利用時の対策
（6）識別コード・主体認証情報の取扱い
（7）暗号・電子署名の利用時の対策
（8）不正プログラム感染防止
（9）Web会議サービスの利用時の対策
（10）クラウドサービスを利用した機関等外の者との情報の共有時の対策

8.1.2　ソーシャルメディアによる情報発信
（1）ソーシャルメディアによる情報発信時の対策

8.1.3　テレワーク
（1）運用規程の整備
（2）実施環境における対策
（3）実施時における対策

8.1.1 情報システムの利用

職員等が情報システムを利用する際の情報セキュリティに関する実施手順を整備し、職員等への周知・徹底を図ること。

職員等への周知・徹底

実施手順を職員等に守ってもらうことは大事だけど、人間だから、うっかりミスをしちゃうよね。
ミスをしないようにシステム面でサポートする機能を導入して、ミスが起こらない仕組みを作ることが大事だよ。

情報システムの利用シーン毎の対策例

基本対策

- 利用が認められていないソフトウェアやクラウドサービスを利用しない
- 接続許可を得ていない機器を機関等LANに接続しない
- 機密性３情報が記録されたUSBメモリを持ち出す場合は許可を得る

不正プログラム感染防止

- マクロの自動実行機能を無効にする
- 感染した疑いがあるときは、通信ケーブルを抜く・無線LAN機能を停止する

電子メール・ウェブ利用時

- 外部の者と電子メールによるやり取りを行う場合は、電子メールのドメイン名に政府ドメイン名を使用する
- 不審な電子メールを受信した場合は報告を行う

Web会議サービス利用時

- 原則、エンドツーエンド(E2E)の暗号化を行う
- 待機室を設けるなど、無関係な者を会議に参加させない

識別コード・主体認証情報の取扱い

- パスワードは推測が困難なパスフレーズを使用する
- 情報システム毎に異なるパスワードを使用する

クラウドサービスによる情報共有

- 必要な者のみを共有範囲に設定する
- 不要になった情報は速やかに削除する

8.1.2 ソーシャルメディアによる情報発信

ソーシャルメディアでは政府ドメインを使用することができないため、真正なアカウントであることを国民等が理解できるよう対策を講ずる必要がある。

ソーシャルメディアは、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限って、利用を許可してね。
あと、ソーシャルメディアはクラウドサービスだと思うから、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の対策も参照してね。

ソーシャルメディア利用における対策例

- 機関等からの情報発信であることを明らかにするために、機関等が政府ドメイン名を用いて管理しているウェブサイト内において、**利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設ける**こと。
- アカウント名やアカウント設定の自由記述欄等を利用し、**機関等が運用していることを利用者に明示**すること。
- 運用しているソーシャルメディアのアカウント設定の自由記述欄において、**当該アカウントの運用を行っている旨の表示をしている機関等のウェブサイト上のページのURLを記載**すること。
- 「**認証アカウント（公式アカウント）**」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

8.1.3 テレワーク

テレワーク実施時の情報セキュリティ対策に係る規定を整備し、実施環境におけるセキュリティ対策を講じ、画面ののぞき見、盗聴などに対する実施時の対策を行うこと。

実施環境における対策

- **通信経路及びリモートアクセス特有の攻撃に対するセキュリティを確保する**
- リモートアクセスに対し**多要素主体認証**を行うこと

- リモートアクセスする端末を**許可された端末に限定**する措置を講ずること
- リモートアクセスする端末を**最新の脆弱性対策や不正プログラム対策が施されている端末に限定**すること

実施時における対策

- テレワーク実施前後に職員等が確認するべき項目を定めること

テレワーク実施**前**の確認項目

- ✓ 自宅のネットワークルータは最新のファームウェアに更新されているか
- ✓ インシデント発生時に連絡する電話番号を把握しているか

テレワーク実施**後**の確認項目

- ✓ 持ち出した機器は全てそろっているか
- ✓ 不正プログラム対策ソフトウェアを用いたスキャンを行い不正プログラムに感染していないことを確認したか
- ✓ どのファイルにアクセスしたか

目次（３．まとめ）

本資料のまとめ

- ✓ 統一基準群は、機関等（政府機関及び独立行政法人等）の情報セキュリティのベースラインを示している。

- ✓ 機関等は統一基準群を準拠・参照し、組織及び取り扱う情報の特性等を踏まえて情報セキュリティポリシーを策定している。

- ✓ 統一基準群はあくまでベースラインである。機関等の判断によって、より高い水準の対策も可能。

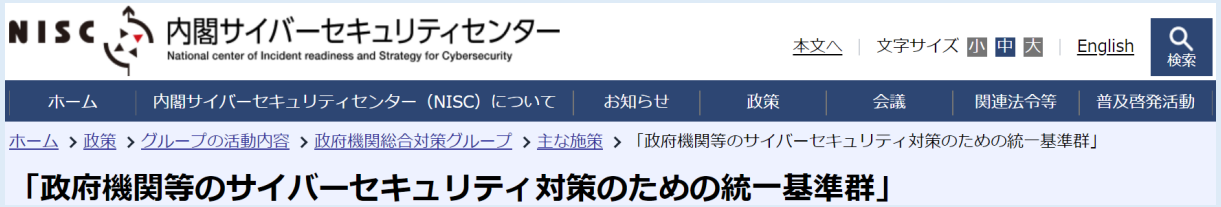
- ✓ 統一基準は全８部構成。
  - ➢ 第１部は総則。
  - ➢ 第２～４部は、セキュリティに係る組織的・横断的取組を規定。
    - 第２部は、体制・インシデント対応・監査など、主に組織のガバナンスマネジメントを規定。
    - 第３部は、情報のライフサイクルに応じた取扱いなど、主に情報の取扱いを規定。
    - 第４部は、業務委託、クラウドサービス、機器等の調達など、主に外部委託の対策を規定。
  - ➢ 第５～８部は、情報システムに係るセキュリティ対策を規定。
    - 第５部は、情報システムの要件定義・運用など、主に情報システムのライフサイクルに応じた対策を規定。
    - 第６部は、端末やサーバ装置など、主に情報システムの構成要素ごとの対策を規定。
    - 第７部は、主体認証機能やサービス不能攻撃対策など、主に情報システムのセキュリティ要件を規定。
    - 第８部は、端末の利用やテレワークなど、主に情報システムの利用時の対策を規定。

付録：統一基準群のWebページについて

統一基準群のWebページに、
- ●統一基準群のWord版やExcel版
- ●統一基準適用個別マニュアル群
- ●学習用の教材

など、統一基準群に関わる情報を掲載しているので、活用してね。

統一基準群のWebページ



URL：https://www.nisc.go.jp/policy/group/general/kijun.html

掲載情報

- **概要**
  - ✓ 統一基準群の概要
- **統一基準群**
  - ✓ 統一規範、統一基準、ガイドライン（PDF版）
  - ✓ 統一規範、統一基準、ガイドライン（Word版）
  - ✓ ガイドライン（Excel版）　統合版（PDF／Word／Excel）ZIP形式
- **統一基準適用個別マニュアル群** ← 機関等において具体的な運用規程や実施手順を定める際の参考資料や個別の情報システムのセキュリティ要件等を検討する時等に利用される資料
  - ✓ 対策推進計画策定マニュアル
  - ✓ 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
  - ✓ 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル など
- **統一基準群の教材**
  - ✓ 本資料
  - ✓ 統一基準群改定のポイント（令和５年度版）
  - ✓ サイバーセキュリティ小冊子（国の行政機関などの一般職員向けに、わかりやすくまとめた教材）←

- **統一基準群の英訳版**
  ※公開に向けて準備中
- **改定履歴**
  - ✓ これまでの統一基準群など

https://www.nisc.go.jp/