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）（※）の改定のポイント

（※）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
- 政府機関等の対策基準策定のためのガイドライン

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

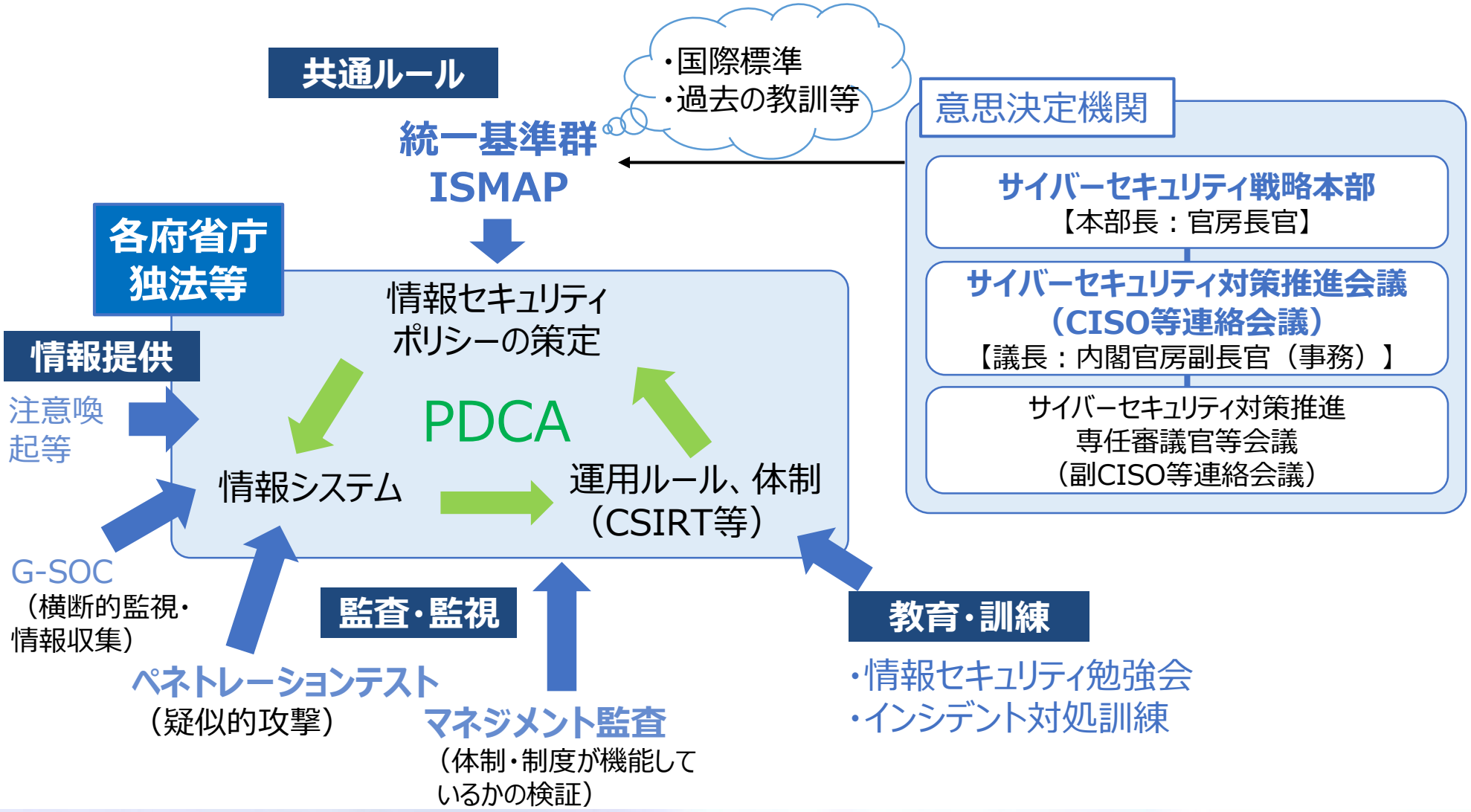
政府機関総合対策グループ

目次

目次（１．統一基準群　概要）

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

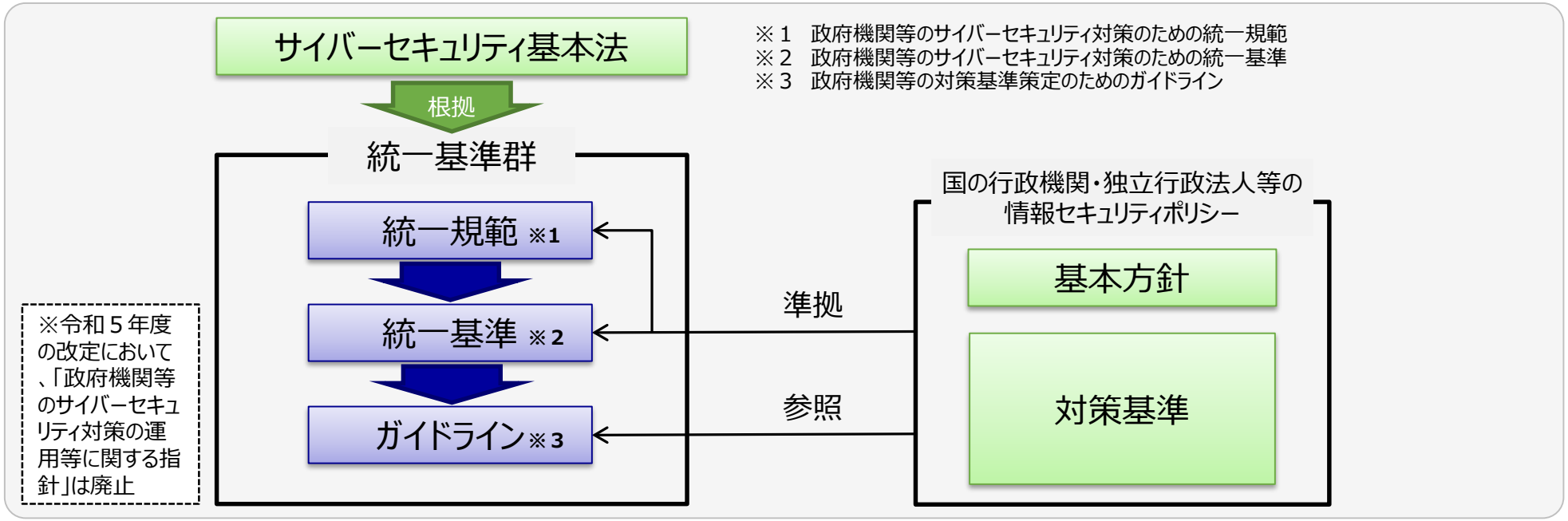


統一基準群の位置づけ

- 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。

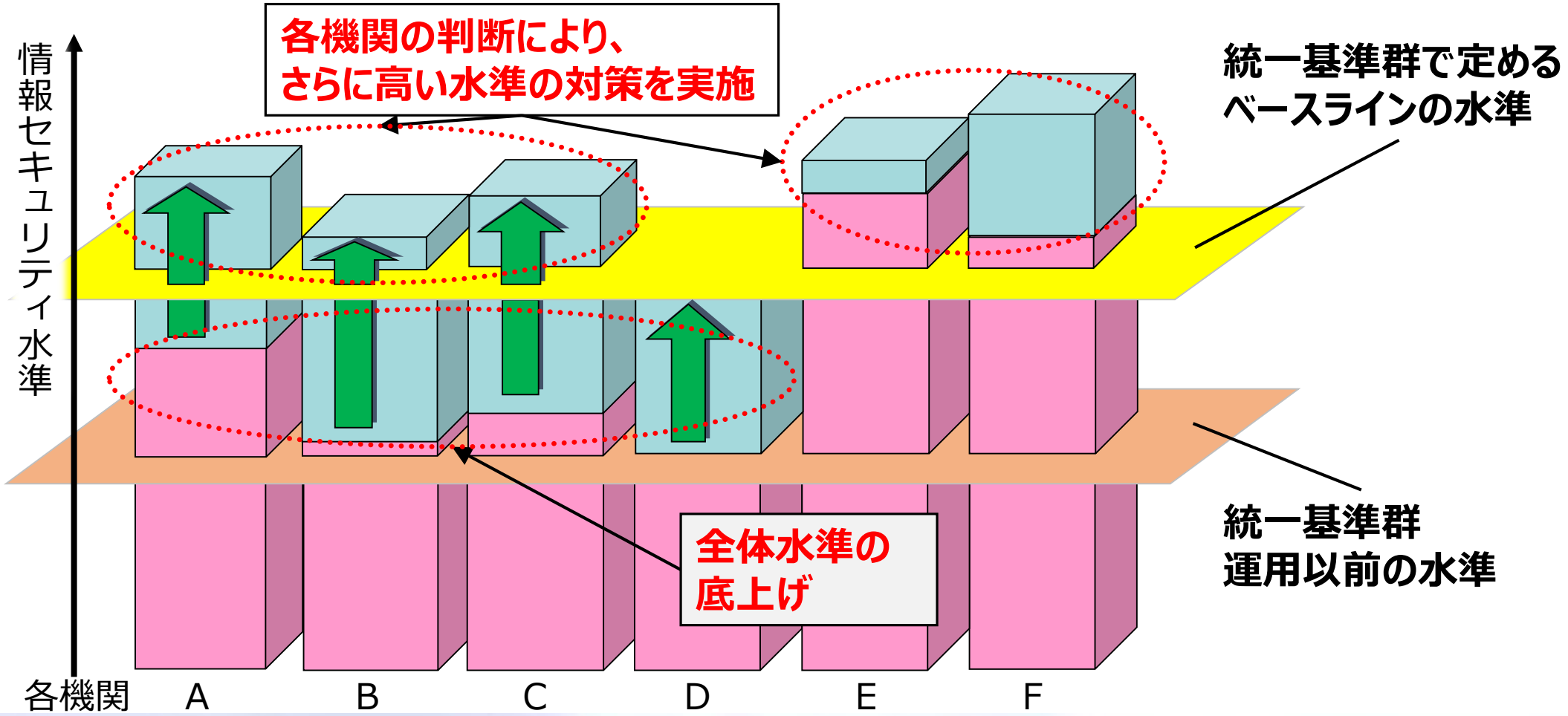
サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）
第二十六条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

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。



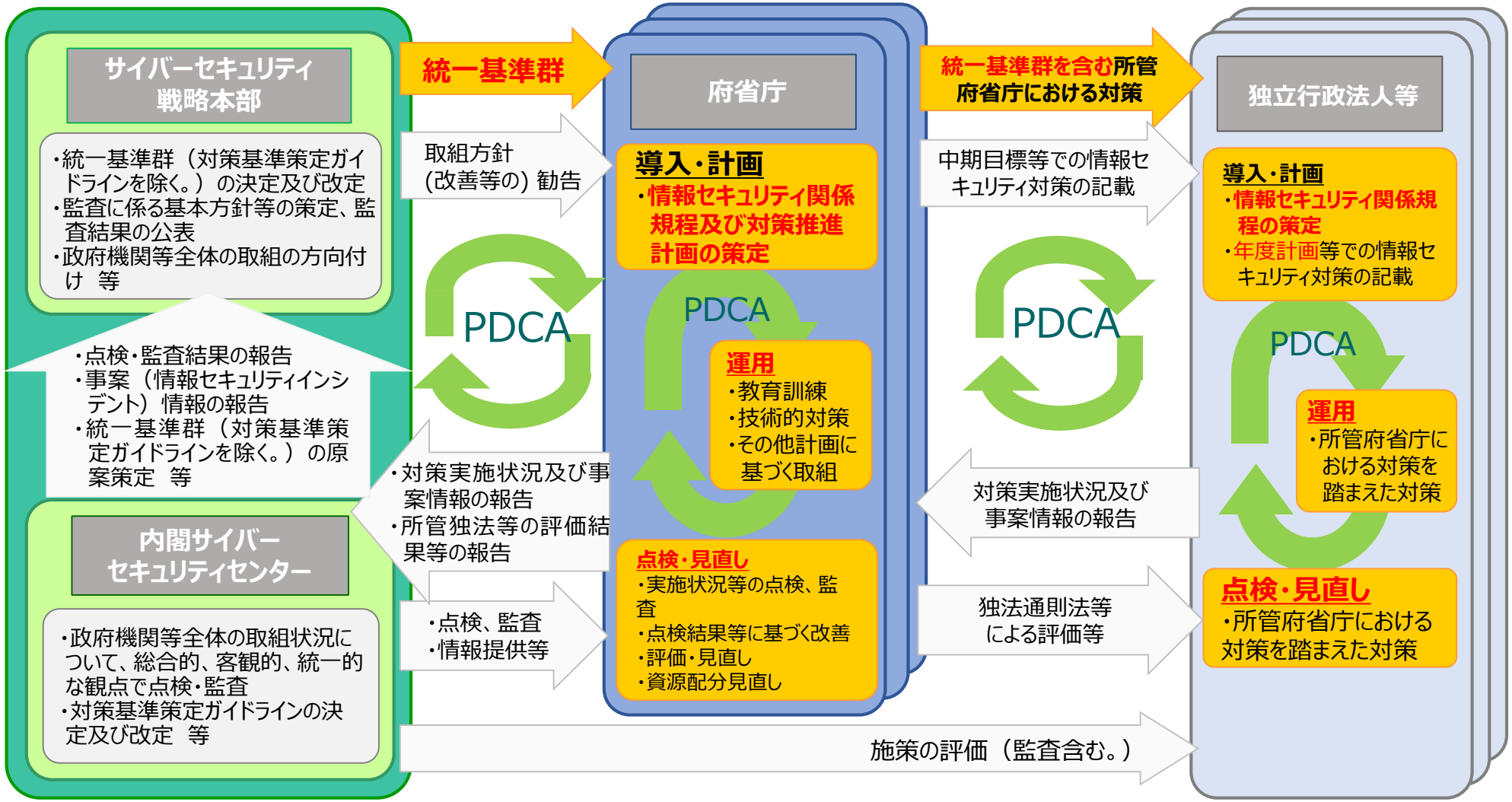
統一基準群の役割

- 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。

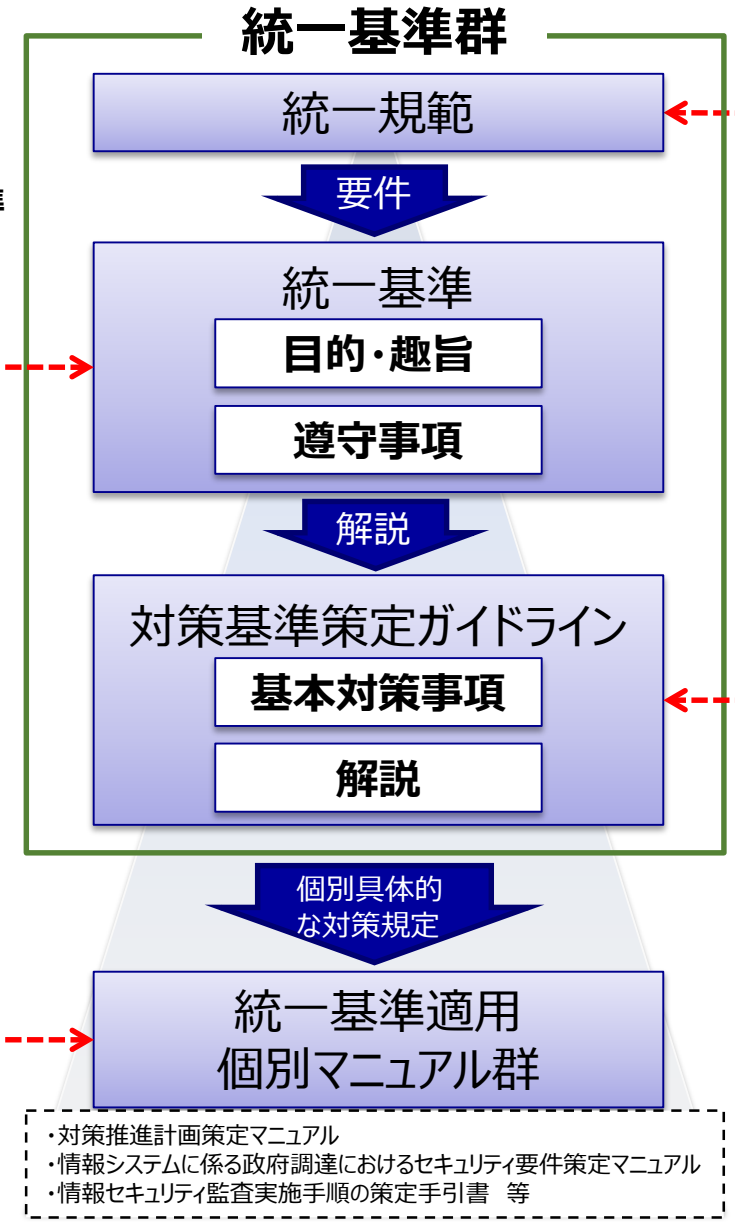


政府機関等全体における情報セキュリティのPDCAサイクル

- 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

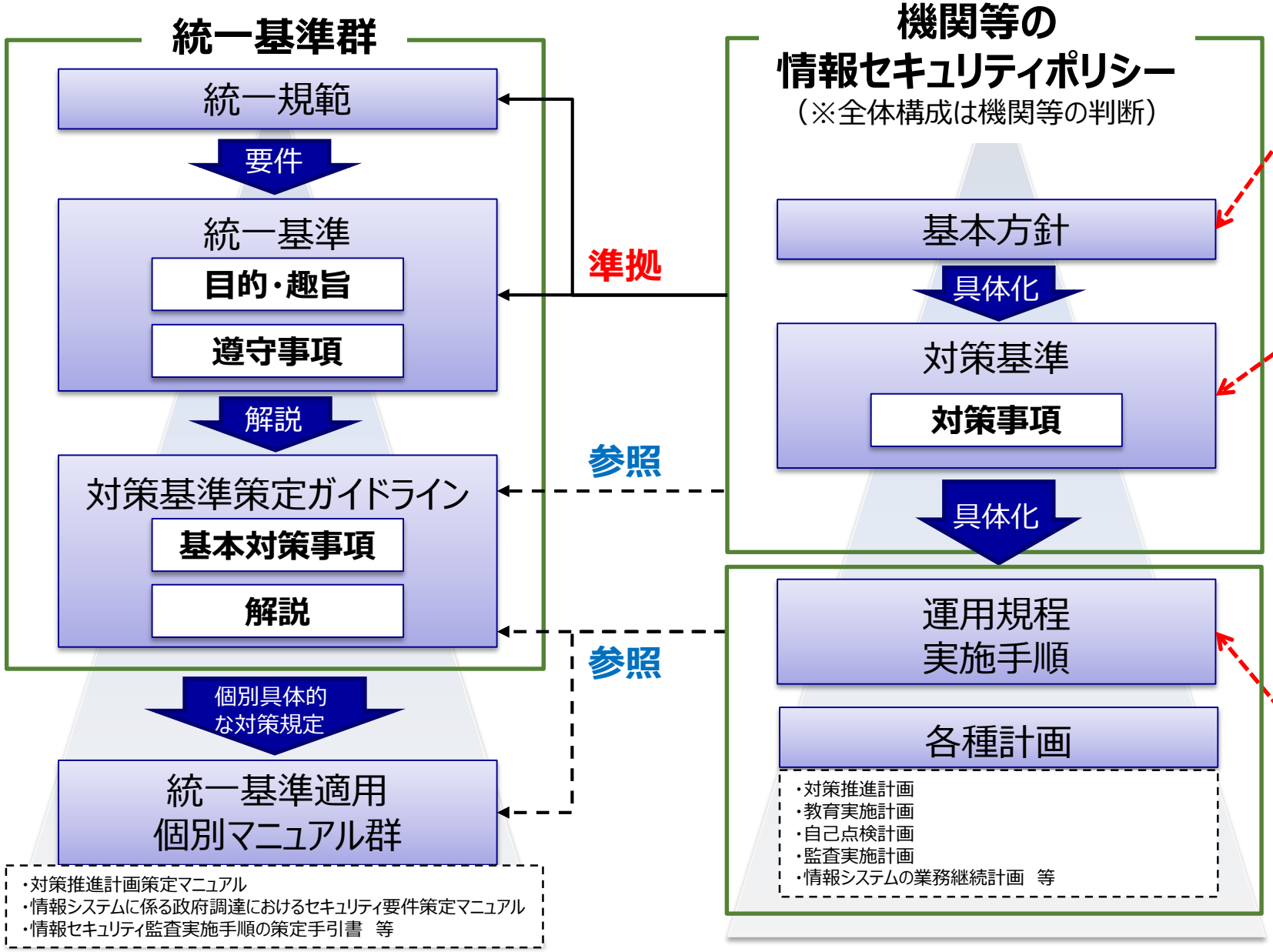
統一基準の遵守事項を満たすためにとるべき基本的な対策事項（基本対策事項）の例示とともに、対策基準の策定及び実施に際しての考え方等を解説したもの

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

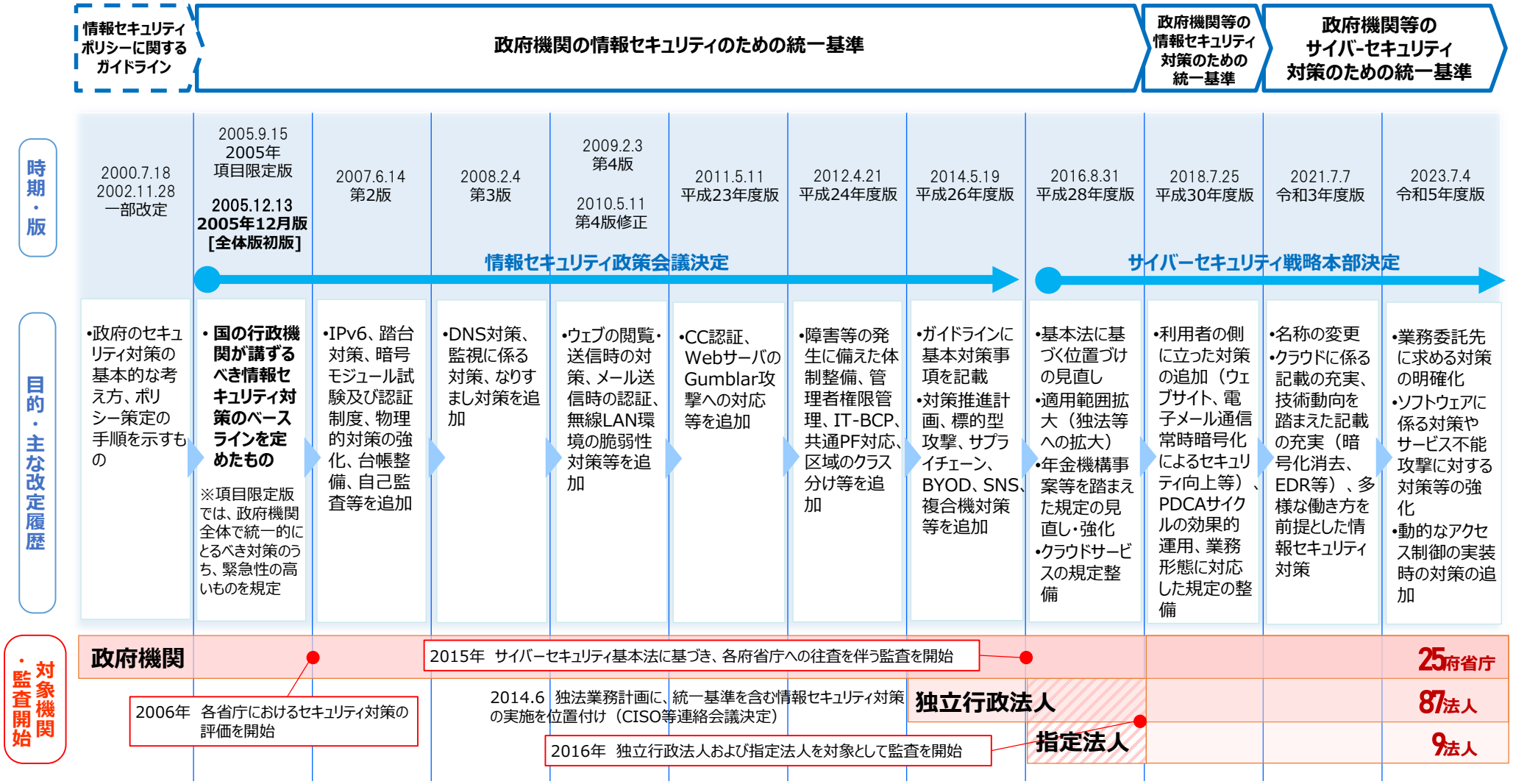
情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準
※統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように定める必要がある

【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（令和５年度版）改定のポイント（全体））

統一基準群改定の背景

- 統一基準群は、サイバーセキュリティ基本法に基づく、**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維持・向上させるための統一的な枠組み**。
- サプライチェーンの脆弱な部分を起点としたサイバー攻撃リスクが増大していることを踏まえた**業務委託先に求める対策**や**ソフトウェアに係る対策**の強化（定期的な設定の確認等）、政府機関等におけるクラウドサービスの利用拡大、最新のDDoS攻撃の特徴を踏まえたサーバ装置の冗長化等の対策強化を盛り込む等、昨今の状況を踏まえた見直しを行うもの。

業務委託（例　情報システムの保守の委託）先に求める対策の明確化 → 改定ポイント「１．情報セキュリティに関するサプライチェーン対策の強化」

- 委託先が運用するファイル共有ツールへの不正アクセスにより、当該事業者に委託していた政府機関等の情報が流出する事案が発生。サプライチェーンの複雑化に伴い、委託先などのサプライチェーンの脆弱な部分を起点としたサイバー攻撃によるリスクが増大。

クラウドサービス利用時のセキュリティ対策の明確化 → 改定ポイント「２．クラウドサービスの利用拡大を踏まえた対策の強化」

- 政府機関等におけるクラウドサービスの利用が拡大。クラウドサービスの調達時から開発、運用、廃棄に至るまでの一連のプロセスにおいてセキュリティ強化が必要。また、広報等で利用するSNS等のクラウドサービスについても、安全に利用するための対策（適切な主体認証やアクセス制御等）を確認していくことが必要。

ソフトウェアの利用時の対策の強化 → 改定ポイント「３．ソフトウェア利用時の対策の強化」

- ソフトウェア設定不備に起因する情報漏えいインシデントや、正規のネットワーク監視ソフトウェアのアップデートを通じた攻撃など、ソフトウェアを標的としたサイバー攻撃が複雑化・巧妙化。米国でも、政府機関等のソフトウェア利用時のセキュリティ対策の強化が図られており、かかる国際動向も踏まえつつ対策の強化が必要。

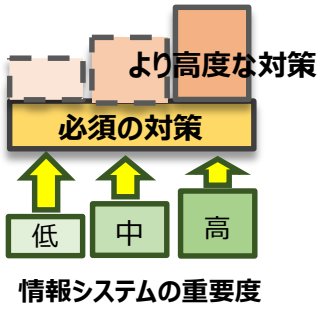
脅威・技術動向を踏まえての対策の強化 → 改定ポイント「４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化」

- 昨今、サービス不能攻撃（DDoS攻撃）が多く観測されており、ウェブサイト障害につながるおそれがあるため、これに対する対策強化が必要。また、ランサムウェア被害も多く発生しており、政府機関等においても、サイバー攻撃を受けることを念頭においた情報システムの防御・復旧やバックアップに係る対策の強化が必要。

統一基準群改定のポイント①

ポイント	詳細
1. 情報セキュリティに関するサプライチェーン対策の強化	➢ 業務委託における政府の情報を保護するため、**米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策**（※）を契約に含めるとともに、委託期間を通じた実施を求める。 （※）NISTのSP800-171を参考に、以下の８類型の対策を規定 ①インシデント等への対処能力の確立・維持、②アクセス主体の識別とアクセス制御、③ログの取得・監視、④機器等の物理的保護、⑤要員への周知と統制、⑥資産管理・リスク評価、⑦システムの完全性の保護、⑧セキュリティ対策の検証・評価・見直し
2. クラウドサービスの利用拡大を踏まえた対策の強化	➢ 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、**要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定**することを明記 （調達したい機能を有したクラウドサービスが登録されていない場合など、やむを得ずISMAPクラウドサービスリスト以外から選定する場合は、CISOの責任において、ISMAP制度で求めている要求事項や管理基準を満たしていることを確認） ➢ 要機密情報を取り扱わない場合においても、**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**。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。
3. ソフトウェア利用時の対策の強化	➢ 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記。また、重要なソフトウェア（※）について、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。 （※）端末やサーバ装置の制御、統合的な主体認証管理、資産管理、ネットワーク監視など、情報システムを制御する上でセキュリティ上の重要な機能を有しているソフトウエアをいう ➢ 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化。

統一基準群改定のポイント②

ポイント	詳細
4. サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化	➢ サイバー攻撃を受けることを念頭においた**情報システムの防御に係る対策**や**情報システムの復旧のための対策**を講ずる。 （情報システムへの監視機能やクラウドサービスの管理者権限を有する主体などの厳格な主体認証が必要な場合における多要素主体認証の導入、情報セキュリティインシデント発生に備えた情報システムの復旧手順の整備や適切なバックアップの取得、バックアップ要件・復旧手順の見直しなど） ➢ 昨今のサービス不能攻撃（DDoS攻撃）を踏まえ、**専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策**や、サービス不能攻撃を受けることを想定した**監視方針の策定や脅威情報の収集等の対策**を講ずる。 ➢ クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、**情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策**を規定
5. 組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保	➢ 監査等から得られた**組織横断的**に改善が必要な事項について、**進捗状況を定期的にCISOに報告**し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。 ➢ 所管独法等の情報セキュリティ対策を支援するため、**府省庁側に必要な体制を整備する**。独法等は専門的知見を要する事項等について**所管省庁等へ助言を求める**。 ➢ **情報システムの重要度の考え方を導入**。全ての情報システムに求める必須の対策に加えて、基幹業務システムなどより**重要度の高い情報システムについては、リアルタイムにログ分析を行う機能の導入などの高度な対策**を求める。 

統一基準（令和５年度版）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

※令和５年度の改定において、第６部と第７部はそれぞれ入れ替えを行った。

・R3 第7部 情報システムの構成要素⇒R5 第6部へ
・R3 第6部 情報システムのセキュリティ要件⇒R5 第7部へ

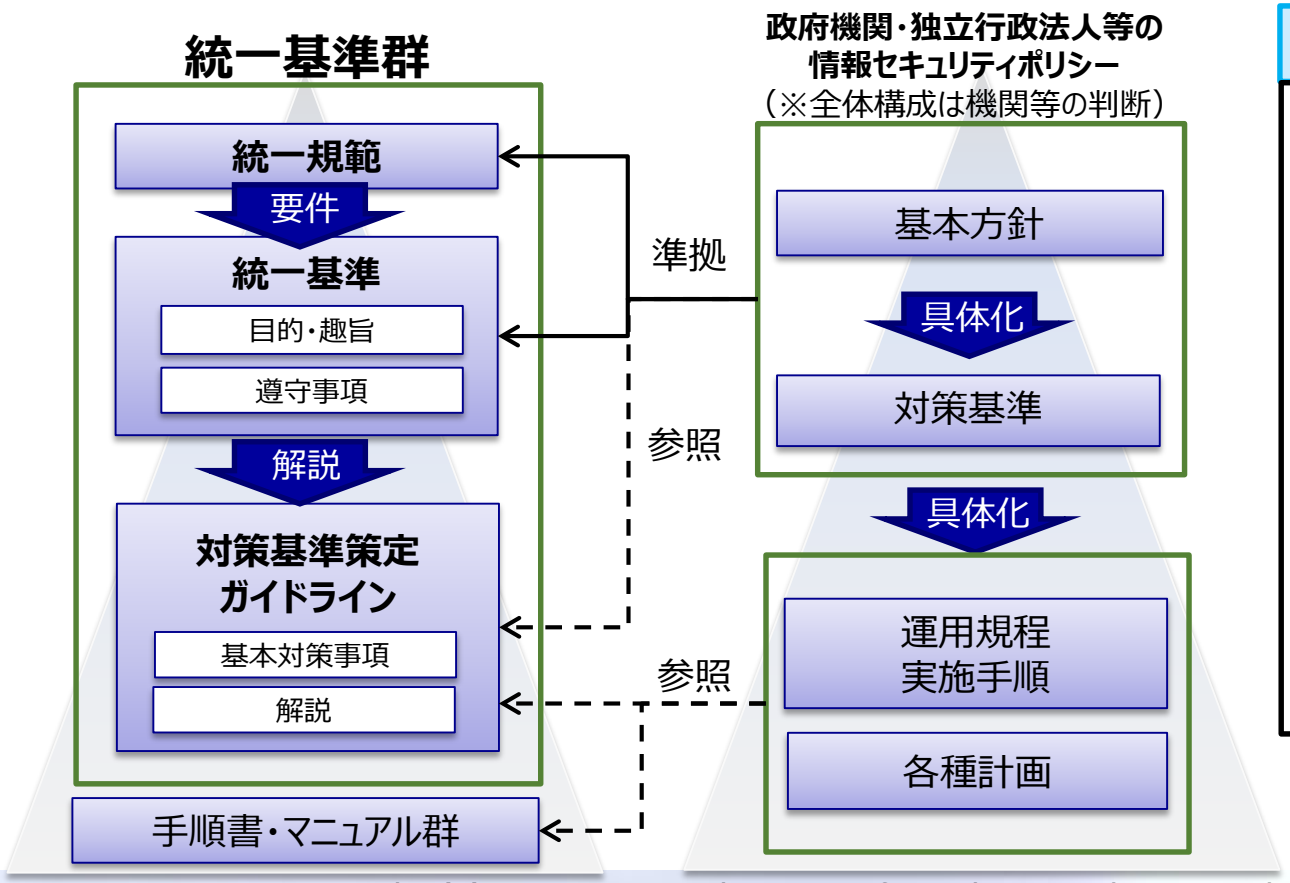
第６～８部
各構成要素やシーンに応じたセキュリティ対策

- 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

第１部　総則（改定のポイント）

- 第１部は、統一基準の目的・適用範囲、情報の格付け区分、用語定義など、対策を講ずる前提となる事項を定めるもの。
- 今般、**統一基準群の文書体系を簡潔にするため運用指針を廃止**、これに伴う修正が発生。また、**統一基準の適用対象となる情報に係る解説や法令の追記など、内容を読み解くための解説**を追加した。

統一基準群（令和５年度版）文書体系



改定のポイント

（１）　統一基準群の文書体系の見直しに伴う修正

- ４つの文書で構成していた「統一基準群」について「運用指針」を削除し、構成を簡素化。
- 所管省庁による独法等への関与など運用指針に記載されていた内容は、統一規範ないし統一基準に取り込む。

（２）　用語に係る解説の拡充

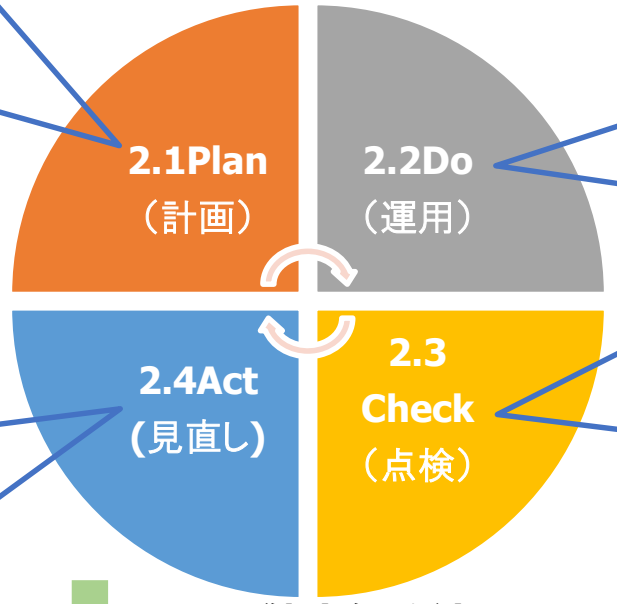
- 統一基準の適用対象に関する解説や、情報公開法など関連する法令の記載等を追加。

（３）　用語定義の見直し・追加

第２部　情報セキュリティ対策の基本的枠組み（改定のポイント）

- 第2部は、情報セキュリティ対策の基本的枠組みとして、組織のマネジメントのフレームワークを規定。PDCAサイクルに基づき、「2.1導入・計画」「2.2運用」「2.3点検」「2.4見直し」の順で、遵守事項・基本対策事項等を規定している。
- **組織全体での情報システム等の資産管理、リスクの評価と対応、継続的な見直し・改善がPDCAサイクルを通じて定着**するよう係る記載を充実。また、**独法等への関与や横断的な課題の横展開**など、**組織的な対応・ガバナンスを強化。**

改定のポイント



- **所管独法等の情報セキュリティ対策への府省庁CISO等の関与**（基本対策事項2.1.1(1)-1,(4)-1）
- **自組織の情報資産の的確な把握、管理**（2.1.2資産管理）
- 自己点検、監査（本部監査含む）や脅威動向等を踏まえた**リスク評価の実施**(遵守事項2.1.3(1))
- **対策推進計画の位置づけ明確化**（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）（遵守事項2.1.3(4)）

- ある情報システムで発生したインシデントが他の情報システムでも発生する可能性を検討することを遵守事項に盛り込むことで、**組織全体を俯瞰したインシデント対応に係る対策を強化**（遵守事項2.2.4(2)）

- **リスク評価に変化が生じた場合の対策基準や対策推進計画の見直しをCISOに義務付け**（遵守事項2.4.1(1)）
- 本部監査等の結果を踏まえ、**横断的に改善が必要な課題について機関等内の横展開及び措置結果のCISOへの報告**を規定（遵守事項2.4.1(2)(c)）

- 自己点検項目には、最新の脅威動向や情報セキュリティ監査の結果等を踏まえる事が重要であることから、これを明示（(解説)遵守事項2.3.1(1)(a)）
- 情報セキュリティ監査の対象の選定の考え方や監査の方法を提示（(解説)基本対策事項2.3.2(1)-1 b)、c)）
- 併せて、監査結果に応じて策定する**改善計画に係る定期的な進捗状況の最高情報セキュリティ責任者への報告を盛り込み**（遵守事項2.3.2(3)）

2.5 独立行政法人及び指定法人（新設）

2.5 独立行政法人及び指定法人（改定のポイント）

➢ 独立行政法人及び指定法人の情報セキュリティ対策について、これまで「運用指針」に記載していた内容を統一規範に集約。あわせて所管省庁・それに対応する独法等の取組について、遵守事項・基本対策事項をまとめた節を新たに設置した。

1. 統一規範

a. 所管省庁側
- 所管独法等に、必要に応じ自らのポリシーを当該法人がポリシーを定める際に参照するよう求める。
- 主務大臣は、独法等中期目標等に統一基準に基づいて定められ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とともに、業務の実績等に関する評価に情報セキュリティ対策の実施状況を含める。

b. 独法等側
- 所管省庁から、当該省庁のポリシーの参照を求められた時はこれに応じ、必要に応じて自らのポリシーに反映させる。

2. 統一基準

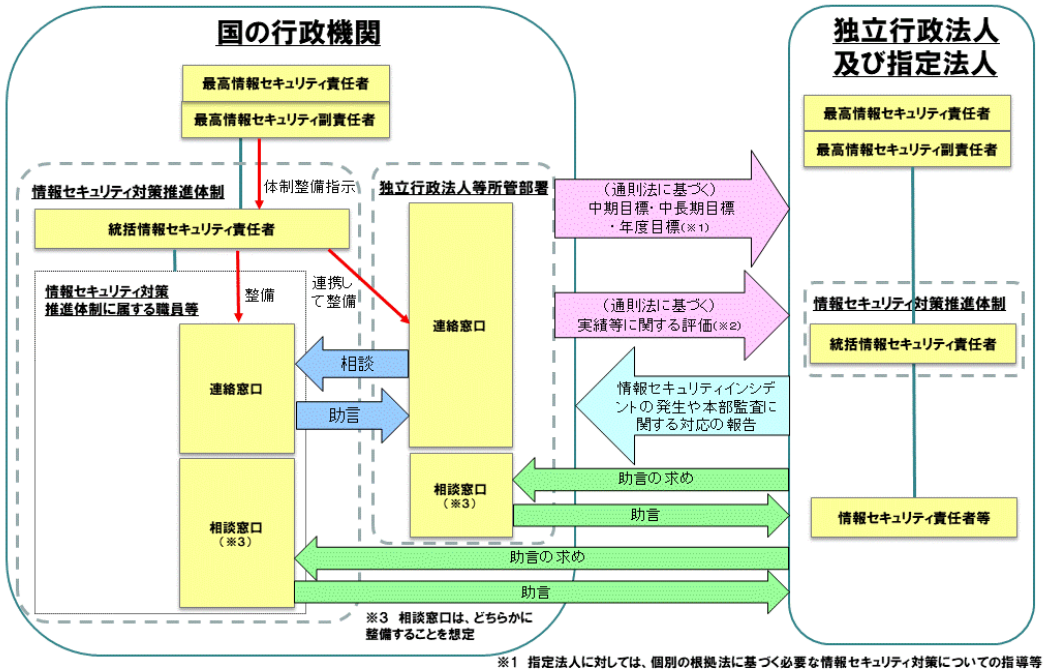
a. 所管省庁側
- CISOは、所管する独法等の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備を指示（遵守事項2.5.1(1)）
- 統括情報セキュリティ責任者は、**独法等の情報セキュリティ対策を適切に推進するために必要な体制（※）**として、法人所管部署等の関係部署及び所管法人等に必要な助言等を行うための窓口を当該法人所管部署等の関係部署と連携して整備（基本対策事項2.5.1(1)-1）

（※）独法等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に必要な体制など

b. 独法等側
- CISOは**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、所管省庁へ助言を求める。（遵守事項2.5.1(2)）

（※）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、「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

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図



※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

【参考】第２部　情報セキュリティ対策の基本的枠組み（目次レベルの変更点①）

NISC

令和３年度版

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　対策基準・対策推進計画の策定
    - 2.1.2(1)　対策基準の策定
    - 2.1.2(2)　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の再発防止・教訓の共有

第5部　情報システムのライフサイクル
- 5.1.1　情報システムに係る台帳等の整備
  - (1)　情報システム台帳の整備

令和５年度版

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　新設
    - (2)　対策基準の策定
    - (3)　運用規程及び実施手順の策定　新設
    - (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　新設
    - (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

情報セキュリティ対策における資産管理の重要性に鑑み、情報システム台帳の整備をR3 5.1.1から移設
※統一規範にも資産管理の規定を盛り込み

リスク評価の実施を明確に規定

R3 2.2.1(1)の一部規定を整理した上で新設

R3 2.2.4(2)の一部規定を整理した上で新設

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

【参考】第２部　情報セキュリティ対策の基本的枠組み（目次レベルの変更点②）

令和３年度版

- **第2部　情報セキュリティ対策の基本的枠組み**
  - 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)　情報セキュリティ関係規程等の見直し
      - (2)　対策推進計画の見直し

令和５年度版

- **第2部　情報セキュリティ対策の基本的枠組み**
  - 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　新設
      - (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　新設
    - 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

リスク評価に変化が生じた場合の対策基準や対策推進計画の見直しをCISOに義務付け

独法等の情報セキュリティ対策に係る府省庁・独法等の取組
※統一規範にも関連する改定を実施

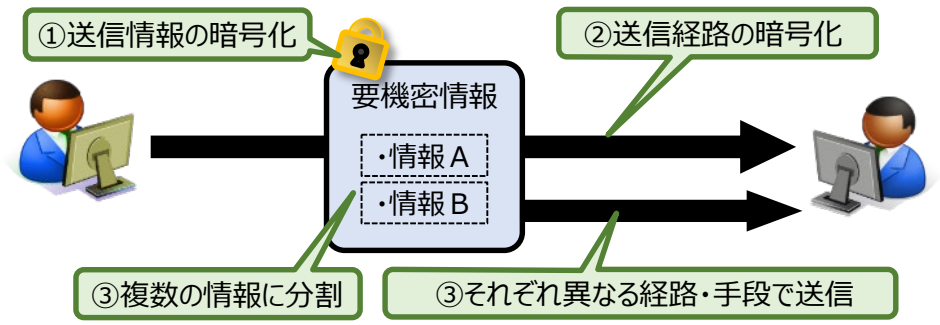
※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

第３部　情報の取扱い（改定のポイント）

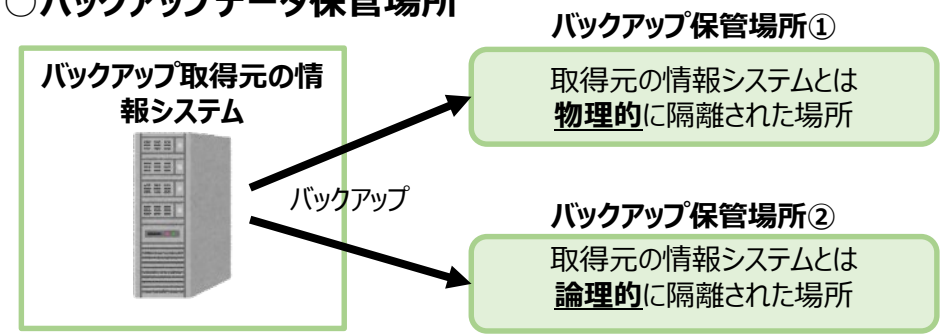
「第３部　情報の取扱い」とは？

➢「第３部　情報の取り扱い」では、統一基準群における情報を適切に取り扱うための対策を定めたものとなっており、情報のライフサイクルに応じた取り扱いと情報を取り扱う区域についての対策を規定している。

○要機密情報を送信する際の対策例



○バックアップデータ保管場所



改定のポイント

（１）情報の送信方法の明示

- 機関等外通信回線を用いて要機密情報を送信する場合に講ずる情報漏えい対策が、送信する情報自体の暗号化（例えば、パスワード付ZIPファイル）のみだと誤解されないよう、**送信経路の暗号化の対策を明示**（基本対策事項3.1.1(6)-3 b))

（２）情報の抹消方法の整理

- 従来箇条書きであった抹消方法について、**抹消方法及び注意点等を見直した上で、表として整理**（解説3.1.1(7)(b)）

（３）情報のバックアップ保管場所の明示

- ランサムウェア対策における、情報システムや情報と、バックアップが同時に破壊されないためのバックアップ保管場所の記載が解説のみとなっていたため、**当該バックアップ保管場所を基本対策事項に明示**（基本対策事項3.1.1(8)-2）

【参考】第３部　情報の取扱い（目次レベルの変更点）

令和３年度版

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
3.1.1(1)　情報の取扱いに係る規定の整備
3.1.1(2)　情報の目的外での利用等の禁止
3.1.1(3)　情報の格付及び取扱制限の決定・明示等
3.1.1(4)　情報の利用・保存
3.1.1(5)　情報の提供・公表
3.1.1(6)　情報の運搬・送信
3.1.1(7)　情報の消去
3.1.1(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
3.2.1(1)　要管理対策区域における対策の基準の決定
3.2.1(2)　区域ごとの対策の決定
3.2.1(3)　要管理対策区域における対策の実施

令和５年度版

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
3.1.1(1)　情報の取扱いに係る規定の整備
3.1.1(2)　情報の目的外での利用等の禁止
3.1.1(3)　情報の格付及び取扱制限の決定・明示等
3.1.1(4)　情報の利用・保存
3.1.1(5)　情報の提供・公表
3.1.1(6)　情報の運搬・送信
3.1.1(7)　情報の消去
3.1.1(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
3.2.1(1)　要管理対策区域における対策の基準の決定
3.2.1(2)　区域ごとの対策の決定
3.2.1(3)　要管理対策区域における対策の実施

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

機関等外通信回線を使用した情報の送信方法について、送信経路全般の暗号化の対策を明示（基本対策事項）

従来箇条書きであった抹消方法や注意点を、機関等が情報の抹消方法を適切に選択できるよう、表によって整理（解説）

ランサムウェアによるインシデントを想定した、バックアップの保管場所を明示（基本対策事項）

第４部　外部委託（改定のポイント）

- 第４部は、**業務委託、クラウドサービスの利用、機器等の調達**など、機関等外の者に情報システムの開発・運用・保守等を担わせたり、機関等の情報を取り扱う業務を実施させる場合といった**サプライチェーンの情報セキュリティ対策**について定めている。
- 業務委託に伴い必要な対策について、**機関等が実施すべき事項**と、**委託先に求める対策を区分して整理**を行ったほか、クラウドサービスの利用拡大を踏まえ**「外部サービス」を「クラウドサービス」に絞った記載に見直し、ISMAP原則利用の考え方に基づいた対策へと改定**

4.1 業務委託

- 4.1.1 業務委託
- 4.1.2 情報システムに関する業務委託

＜業務委託の例＞
- 情報システムの開発及び構築業務
- 情報システムの運用業務
- プロジェクト管理支援業務
- 調査・研究業務（調査、研究、検査等）
- 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の利用（ホスティングサービス 等）

4.2 クラウドサービス

- 4.2.1 クラウドサービスの選定
- 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

- 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

＜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

4.3 機器等の調達

- 4.3.1 機器等の調達

＜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

改定のポイント

（１）業務委託で機関等が実施する対策と、委託先に求める対策を整理
- 委託先の情報セキュリティ対策は通常直接管理できないところ、委託先に取り扱わせる情報を適切に保護する観点から、機関等において実施・確認すべき事項と、委託先に求める事項を区分して明確化

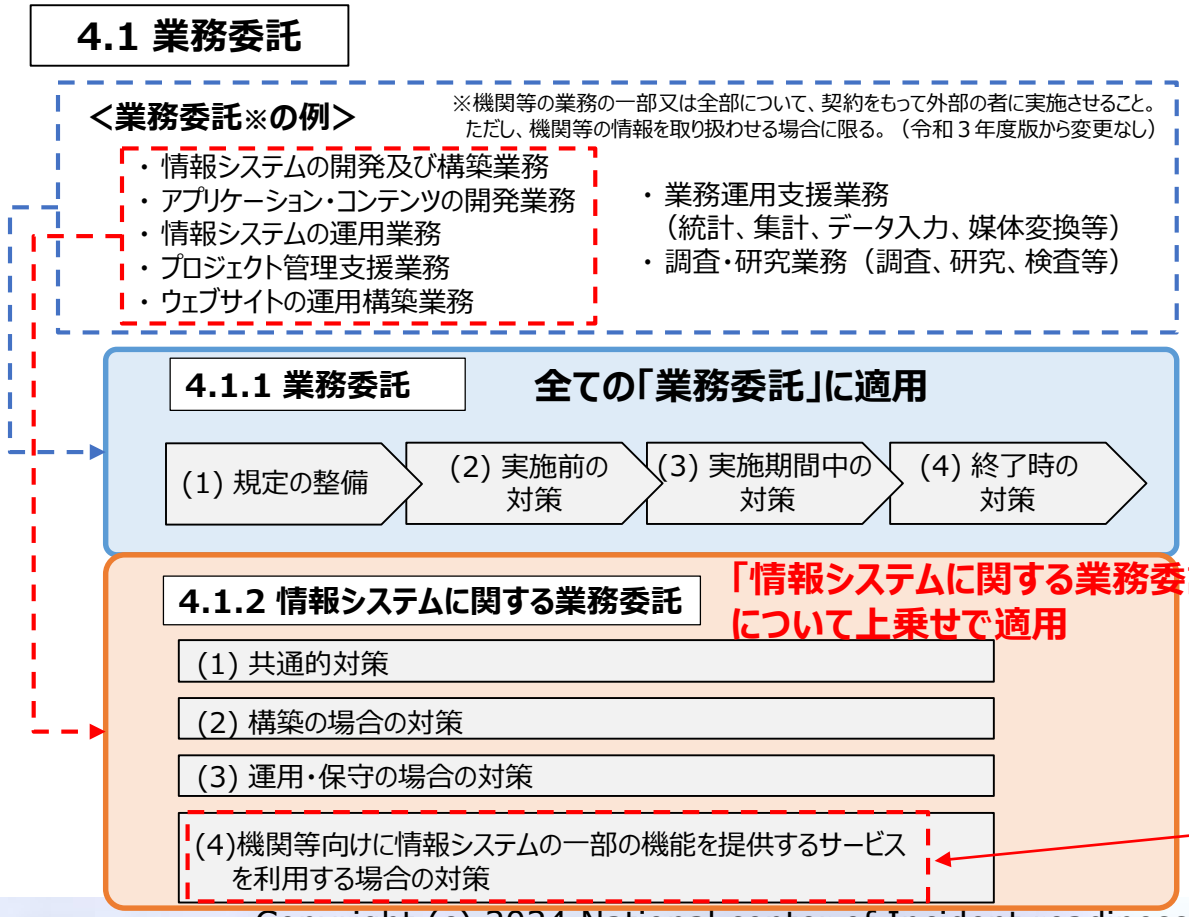
（２）クラウドサービスに絞った記載への見直し
- クラウドサービスにSaaSが含まれることを明確にした上で、従前の外部サービスのうちクラウドサービスに絞った記載に見直すとともに、原則としてISMAP等クラウドサービスリストから選定することを記載

（３）機器等の調達におけるサプライチェーン・リスク対応の明確化
- 特にサプライチェーン・リスクに対応する必要があると判断されるソフトウェアをはじめとする機器等の調達に関して、「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」に基づく措置を講ずることを明確化

4.1 業務委託（改定のポイント）

「4.1　業務委託」とは？

- 情報システムの開発、運用・保守、プロジェクト管理支援などのシステム関連業務、業務運用支援（統計、集計、データ入力等）、調査・研究など様々な業務について、機関等外の者に業務委託するケースは多く存在する。
- これら業務委託を行うに当たって委託先に提供した情報が適切に保護されるよう、業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、機関等において実施すべき対策・委託先に求めるべき対策をそれぞれ規定している。



改定のポイント

- 委託先に情報の適正な取扱いを求めるため、委託先に実施を求める対策を具体化（基本対策事項4.1.1(3)-1）
- 「業務委託」のうち「情報システムに関する業務委託」に着目し、情報システムの構築・運用等を業務委託する際に委託先に求める対策を集約しつつ拡充（遵守事項4.1.2(1)～(3)）
- 令和３年度版の統一基準における「外部サービス（クラウドサービス以外）」について、「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」（業務委託サービス）として再定義し、必要な対策を整理（遵守事項4.1.2(4)）

令和３年度版における「外部サービス（クラウドサービス以外）」
・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　等

4.1 業務委託（委託先に実施を求める対策の具体化）

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

具体例の提示

- 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

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

(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）
  - 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

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

※青字・下線は、遵守事項・基本対策事項に追加した内容

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

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（改定のポイント）

- 従来あった「外部サービス」を「クラウドサービス」と「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」に分離し、それぞれに必要な対策に再整理
- クラウドサービスの選定については、ISMAP原則利用の考え方を明確化。またクラウドサービスの利用開始から廃棄に至るまでの一連のプロセスにおけるセキュリティ対策を、それぞれの役割に応じて整理、拡充

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。

<クラウドサービスの例>

- 仮想サーバ、ストレージ、ハイパーバイザ等提供サービス（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サービス
- 検索サービス、翻訳サービス、地図サービス

要機密情報を取り扱う場合

- **4.2.1 クラウドサービスの選定**
- **4.2.2 クラウドサービスの利用**

要機密情報を取り扱わない場合

- **4.2.3 クラウドサービスの選定・利用**

令和3年度　外部サービス（クラウドサービス以外）

- 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　等

4.1.2(4)へ

改定のポイント

- クラウドサービスに一般的なSaaSが含まれることを、用語定義において明記
- 独法等がISMAP制度の対象となり、また、ISMAP-LIUの運用も開始されたことから、クラウドサービスは「原則としてISMAP等クラウドサービスリストから選定」するように見直し（4.2.1(2)(c)）
- クラウドサービスを利用した情報システムの導入時、運用時、終了時の対策に分けて記載されていた運用規程の整備を役割に基づき集約（4.2.2(1)）
- クラウドサービスを利用した情報システムにおいて、クラウドサービス管理者の役割において実施すべきクラウドサービス利用に係るライフサイクル全般の対策を整理（4.2.2(2)～(5)）
- 要機密情報を扱わない場合でも、職員等による申請と許可権限者による承認のプロセスを明確化（4.2.3(2)）

4.3 機器等の調達（改定のポイント）

「4.3　機器等の調達」とは？

- 調達する機器等において必要なセキュリティ機能が装備されていない、製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合、情報システムに必要なセキュリティ水準が担保されず、取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。
- そのため、サプライチェーン・リスクへの対応を含めた機器等の選定基準の策定や納入時の確認・検査手続等を整備することが必要である。

令和３年度　統一基準（第５部）

第5部　情報システムのライフサイクル
- 5.1　情報システムに係る文書等の整備
  - 5.1.1　情報システムに係る台帳等の整備
    - （1）　情報システム台帳の整備　→ 2部へ移設
    - （2）　情報システム関連文書の整備
  - 5.1.2　機器等の調達に係る規定の整備
    - （1）　機器等の調達に係る規定の整備
- 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）　情報システムのセキュリティ要件の策定
    - （3）　情報システムの構築を業務委託する場合の対策　→ 4部へ移設
    - （4）　情報システムの運用・保守を業務委託する場合の対策　→ 4部へ移設
  - 5.2.2　情報システムの調達・構築
    - （1）　機器等の選定時の対策
    - （2）　情報システムの構築時の対策
    - （3）　納品検査時の対策

・・・

4.3.1 へ

4.3 機器等の調達

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。

4.3.1 機器等の調達

(1)機器等の調達に係る規定の整備

特にサプライチェーン・リスクに対応する必要があると判断されるソフトウェアを具体化

＜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

改定のポイント

- 基本的には、第5部にあった機器等の調達に係る対策を4.3節に集約したもの。
- サプライチェーン・リスクへの対応として、機器等の調達に関して「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」に基づき、必要な措置を講ずることを規定（基本対策事項4.3.1(1)-1）
- 同申し合わせ別紙２「ソフトウェア」のうち、特にサプライチェーン・リスクに対応する必要があると判断されるソフトウェアを具体化（解説4.3.1(1)-1 b)）

【参考】第４部　外部委託（目次レベルでの変更点）

令和３年度版

第4部　外部委託
- 4.1　業務委託
  - 4.1.1　業務委託
    - (1)　業務委託に係る規定の整備
    - (2)　業務委託に係る契約
    - (3)　業務委託における対策の実施
    - (4)　業務委託における情報の取扱い

第5部　情報システムのライフサイクル
- 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
    - (3)　情報システムの構築を業務委託する場合の対策
    - (4)　情報システムの運用・保守を業務委託する場合の対策

第５部

第4部　外部委託
- 4.2　外部サービスの利用
  - 4.2.1　要機密情報を取り扱う場合
    - (1)　外部サービスの利用に係る規定の整備
    - (2)　外部サービスの選定（クラウドサービスの場合）
    - (3)　外部サービスの選定（クラウドサービス以外の場合）
    - (4)　外部サービスの利用に係る調達・契約
    - (5)　外部サービスの利用承認
    - (6)　外部サービスを利用した情報システムの導入・構築時の対策
    - (7)　外部サービスを利用した情報システムの運用・保守時の対策
    - (8)　外部サービスを利用した情報システムの更改・廃棄時の対策
  - 4.2.2　要機密情報を取り扱わない場合
    - (1)　外部サービスの利用に係る規定の整備
    - (2)　外部サービスの利用における対策の実施

第5部　情報システムのライフサイクル
- 5.1　情報システムに係る文書等の整備
  - 5.1.2　機器等の調達に係る規定の整備
    - (1)　機器等の調達に係る規定の整備

第５部

令和５年度版

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　新設
    - (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）　新設
    - (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

業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、機関等において実施すべき対策・委託先に求めるべき対策をそれぞれ規定

従来、各箇所に規定されていた、情報システムに関する業務委託の規定を集約

(1)：R3 4.1.1(2)の一部規定を移設
(2)：R3 5.2.1(3)を移設
(3)：R3 5.2.1(4)を移設
(4)：R3「外部サービス(クラウドサービス以外)」を再定義し、必要な対策を整理

- クラウドサービスを利用した情報システムの導入時、運用時、終了時の対策に分けて記載されていた運用規程の整備を役割に基づき集約
- クラウドサービスを利用した情報システムにおいて、クラウドサービス管理者の役割において実施すべきクラウドサービス利用に係るライフサイクル全般の対策を整理

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

基本的には、第5部にあった機器等の調達に係る対策を集約

第５部　情報システムのライフサイクル（改定のポイント）

- 第５部は、機関等において所管する情報システムの企画・要件定義、調達・構築、運用・保守、更改・廃棄、見直しまでの情報システムの**ライフサイクルにおいて情報システムセキュリティ責任者の役割において留意すべき事項**を取りまとめたもの。情報システムの構成要素やセキュリティ機能にかかる対策（第４部、第６部、第７部）との繋ぎとなる部である。
- **高度な情報セキュリティ対策が要求される情報システムを判別するための基準である「情報システムの分類基準」の考え方を導入。分類基準に応じたセキュリティ対策を、「基本セキュリティ対策」と「追加セキュリティ対策」に区分。**（5.1を新設）
- また、他省庁が整備運用するシステムを共通利用するケースを念頭に、**「5.4 政府共通利用型システム」を新設。**

表5.1.1-1　情報システムの分類基準（例）

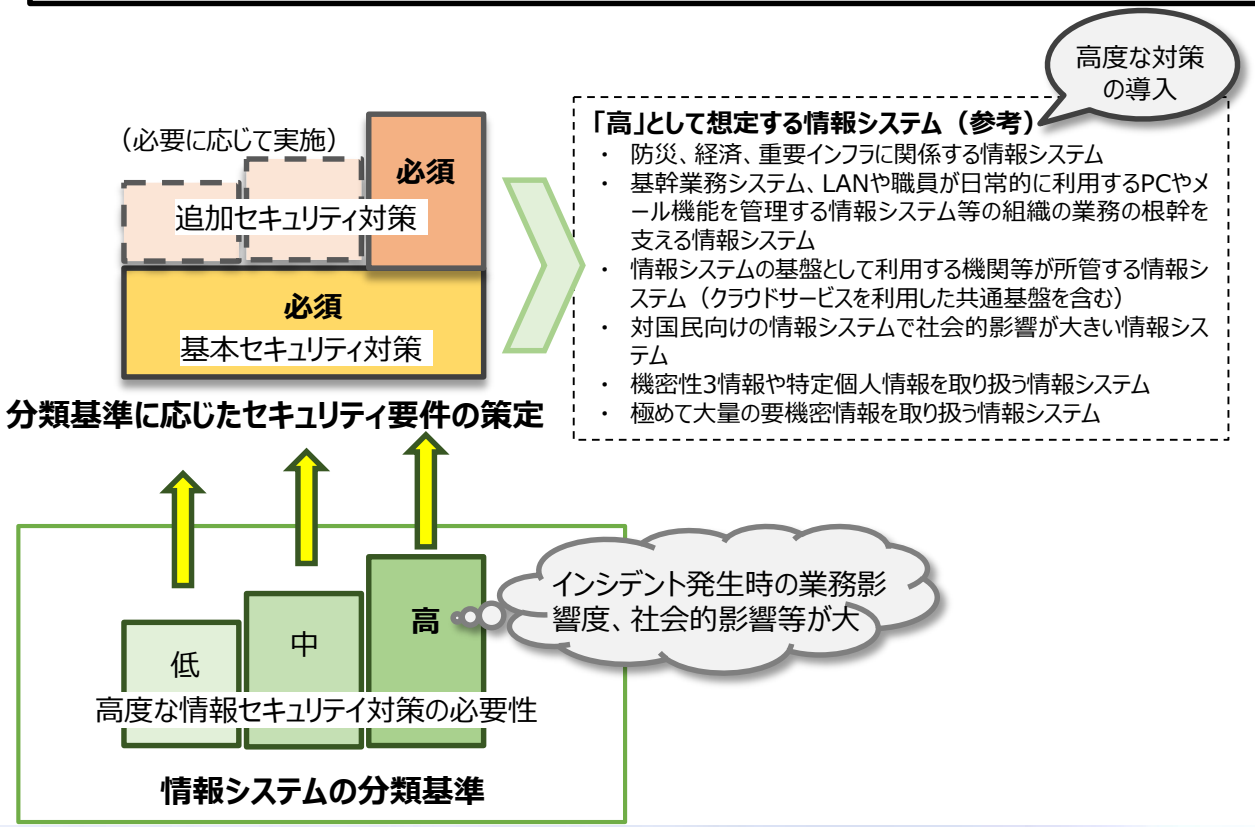
	判断基準
高	• 国家安全保障及び治安関係の業務を行う場合 • 機密性の高い情報を取り扱う場合並びに情報の漏洩及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱う場合 • 番号制度関係の業務を行う場合等、個人情報を極めて大量に取り扱う業務を行う場合 • 機能停止等の場合、機関等の業務遂行に著しい影響を及ぼす場合 • 運営経費が極めて大きい場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：高」に分類される他の情報システムに影響を与える場合
中	• 「情報システムの重要度：高」を除く要保護情報を取り扱う場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：中」に分類される他の情報システムに影響を与える場合
低	• 「情報システムの重要度：高、中」を除く全て

表5.1.1-2　具本的な対策事項を実施させるための判断基準（例）

情報システムの重要度	基本セキュリティ対策	追加セキュリティ対策
高	必須	必須
中	必須	必要に応じて実施
低	必須	必要に応じて実施

5.1 情報システムの分類（改定のポイント）

- 情報システムを取り巻く脅威動向や、インシデント発生時の業務影響度、社会的影響、取り扱う情報、機関等の組織特性等によって、通常のシステムと比してより**高度な情報セキュリティ対策が必要となる情報システム**が存在する。
- このため、**高度な情報セキュリテイ対策が要求される情報システムを判別するための基準（情報システムの分類基準）を統括情報セキュリティ責任者が策定**するとともに、それに基づく各情報システムの分類と、分類基準に応じたセキュリティ対策の実施を求める。
- 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については、ベースラインとして**全てのシステムに必ず求める対策事項（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）の実施**を求める。



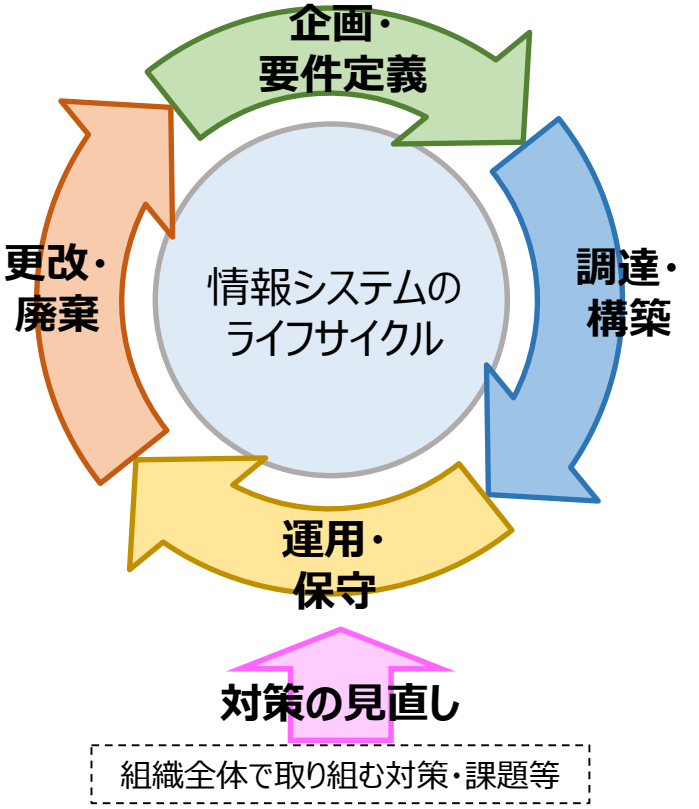
改定のポイント

- 統括情報セキュリティ責任者は情報システムの分類基準（遵守事項5.1.1(1)(a)）及び、分類基準に応じた具体的な対策事項を整備（遵守事項5.1.1(2)(a)）
- 情報システムの構築・更改時や情報システムで取り扱う情報に変更が発生した場合などに、統括情報セキュリティ責任者は、情報システムセキュリティ責任者に対して分類基準に基づいた分類を実施させ、実施した結果を報告させる。（遵守事項5.1.1(3)(a)）
- 統括情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた情報セキュリティ対策の具体的な対策事項を定期的な見直しや、分類基準に基づく適切な分類が行われているかを定期的に確認する。（遵守事項5.1.1(4)）

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(改定のポイント)

「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」とは？

- 5.2では、情報システムのライフサイクルの各段階（企画・要件定義、調達・構築、運用・保守、更改・廃棄）で必要となる情報セキュリティ対策や留意すべき事項を定めている。
- 情報システムを新規に構築又は更改する際は、5.1に示す分類基準に基づいて**情報システムを分類の上、当該分類に応じた具体的な対策事項をセキュリティ要件として要件定義への盛り込み**を求めることで、情報システムの企画・要件定義段階からの**ライフサイクルを通じたセキュリティ対策の浸透**を図る。



改定のポイント

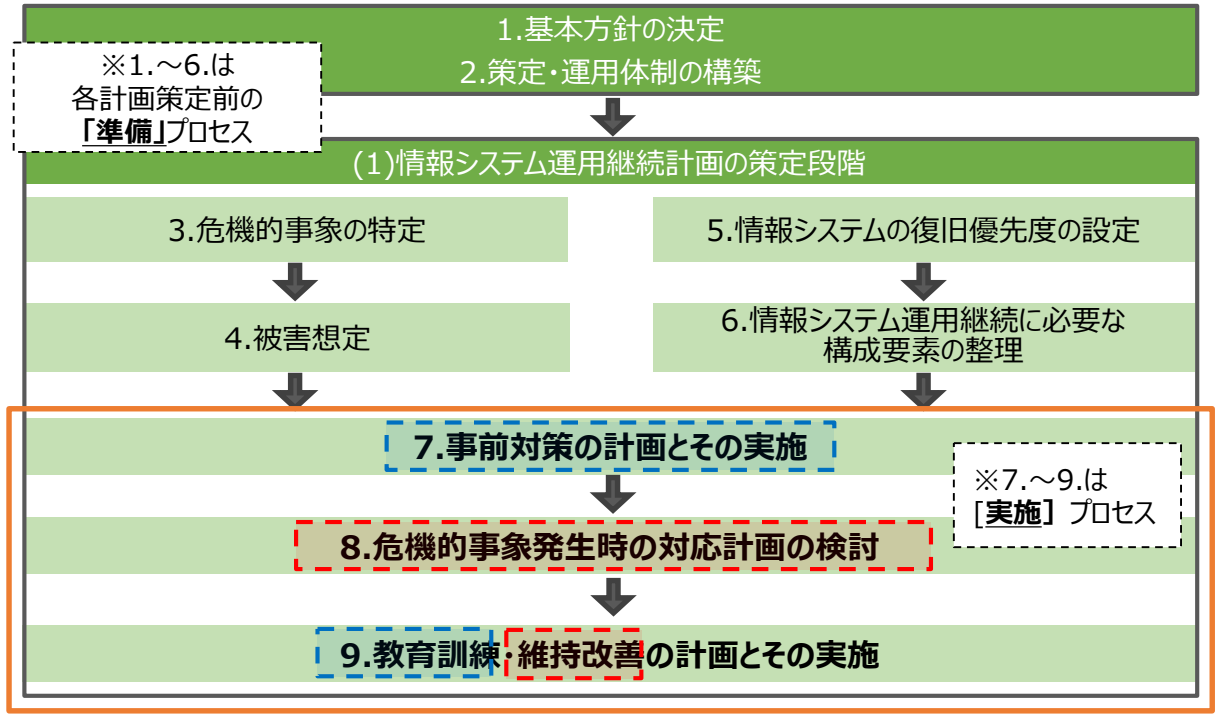
- 情報システムセキュリティ責任者による、5.1に示す**分類基準に基づく分類の実施と、当該分類に応じたセキュリティ要件の策定**（遵守事項5.2.1(2)(a)，5.2.1(3)(a)）
- 情報システムのセキュリティ要件に「不正プログラム対策」「可用性に関する対策」「ネットワーク構成に関する対策」を追加（遵守事項5.2.1(3)(a)）
- **設定ミスや不備の防止対策**として、機器やソフトウェア等の推奨設定や業界標準、ベストプラクティス等を参照し、各種設定を行うことを追加（基本対策事項5.2.2(1)-1c)）
- **非常時の運用継続**を図るために、システムが停止した際の復旧手順の整備、適切なバックアップの取得やバックアップ要件の見直し、停止した際の復旧手順の確認・見直しに関する対策を追加（遵守事項5.2.2(1)(e), 5.2.3(1)(e) ）
- ライフサイクルを通じて、**機器やソフトウェア等における脆弱性対策やアカウント等を見直すための対策を追加**。利用するソフトウェアのセキュリティ維持に関する手順の整備（基本対策事項5.2.2(1)-6 e)）、納品時の確認・検査事項の具体化（不要な識別コードの削除、初期値設定されている主体認証情報の削除、不要なポートが開放されていない等の確認）（基本対策事項5.2.2(2)-1）、過剰なアクセス権限の付与がないか等の運用時の適宜の見直しなどを追加（基本対策事項5.2.3(1)-4）

5.3 情報システムの運用継続計画（改定のポイント）

「5.3　情報システムの運用継続計画」とは？

- 情報システム運用継続計画は、「中央省庁業務継続ガイドライン第３版（首都直下地震対策）」において、「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」に基づき策定することとされている。また、当該計画は、統一基準群における機関等の情報セキュリティ体制とは別の体制において策定される。
- 統一基準群においては、情報システム運用継続計画を策定する体制と連携し、情報セキュリティ関係規定で定める事項と矛盾がないよう、整合性を確保する規定が設けられている。

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（第３版）
図1.2-1 情報システム運用継続計画策定・運用の流れ（一部抜粋）

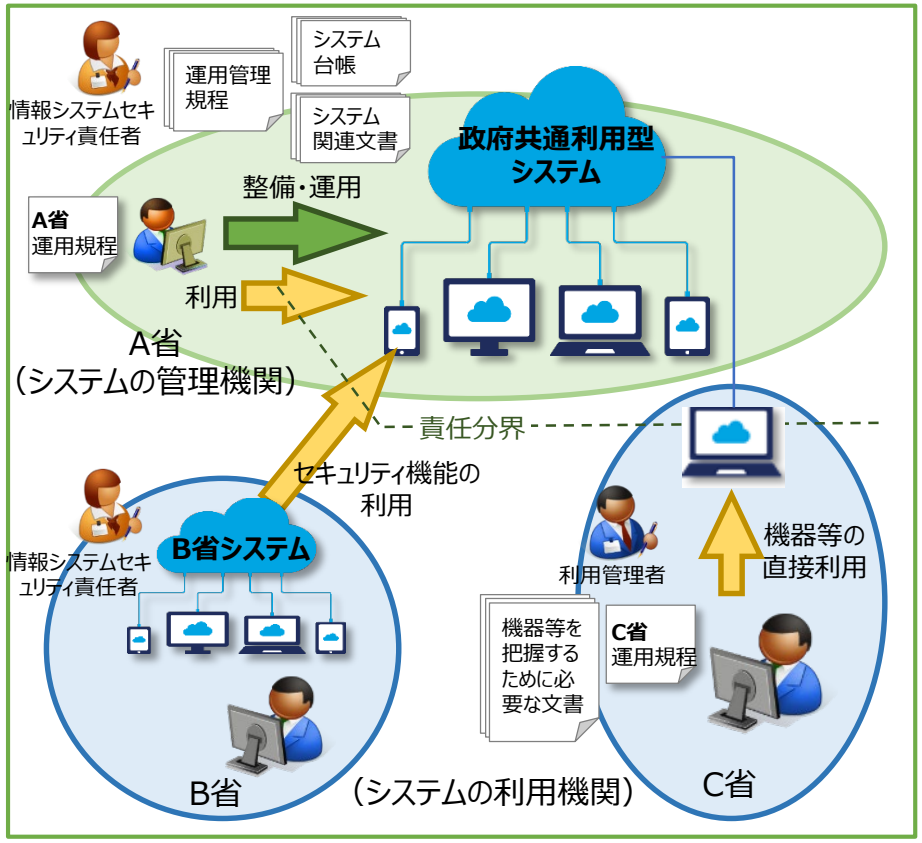


改定のポイント

- 統一基準群（令和３年度版）では、情報システム運用継続計画の「実施」プロセスの一部のみ、関連する規定が設けられている（青点線部）
- **対応計画や維持改善（見直し）の検討を追加（赤点線部）**することで、情報システム運用継続計画の実施プロセスと統一基準群の規定の整合性を強化（遵守事項5.3.1(1)(a),(c)）
- 情報システム運用継続計画の実効性を高めるために訓練が重要であるという考えのもと、**情報システム復旧訓練等、具体的な訓練を規定**（基本対策事項5.3.1(1)-1、-2）
- 情報システムの構成や取り扱う情報の変化等、**見直しを行う際に踏まえる事項を規定**（基本対策事項5.3.1(1)-3）

5.4 政府共通利用型システム（改定のポイント）

- これまで統一基準では、政府共通プラットフォームを念頭に置いた「基盤となる情報システム」についてセキュリティ上留意すべき事項等を運用指針及びガイドラインにおいて示してきた。
- 他省庁が整備したシステムの利用が広がっていること、また、システムの利用形態が従来の定義には収まりきれないことから「政府共通利用型システム」として新たに定義した上で、当該システムの管理機関と利用機関の責任分界やそれぞれに必要となる対策等について、節を新設して整理。



令和３年度版

基盤となる情報システム：他の機関等と共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

令和5年度版

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

- 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
- 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

改定のポイント

- 「政府共通利用型システム」の管理機関は、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する（5.4.1(1)）
- 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（5.4.2(1)(a)及び(c)並びに5.4.2(2)）
- 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する（5.4.2(1)～(3)）

【参考】第５部　情報システムのライフサイクル（目次レベルの変更点）

NISC

令和３年度版

- 第5部　情報システムのライフサイクル
  - 5.1　情報システムに係る文書等の整備
    - 5.1.1　情報システムに係る台帳等の整備
      - (1)　情報システム台帳の整備
      - (2)　情報システム関連文書の整備
    - 5.1.2　機器等の調達に係る規定の整備
      - (1)　機器等の調達に係る規定の整備
  - 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)　情報システムのセキュリティ要件の策定
      - (3)　情報システムの構築を業務委託す
      - (4)　情報システムの運用・保守を業務
      - の対策
    - 5.2.2　情報システムの調達・構築
      - (1)　機器等の選定時の対策
      - (2)　情報システムの構築時の対策
      - (3)　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

R5 2.1.2資産管理へ

R5 4.3.1 機器等の調達へ

R5 4.1.2 情報システムに関する業務委託へ

令和５年度版

- 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　新設
    - 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　新設
      - (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　新設
    - 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

- 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」の考え方を導入
- ベースラインとなる「基本セキュリティ対策」と、より高度な「追加セキュリティ対策」の考え方を導入

5.1.1において整備した、「情報システムの分類基準」に基づいた分類を実施

従来の「情報システムの構築時の対策」に加え、「情報システム関連文書の整備」を移設

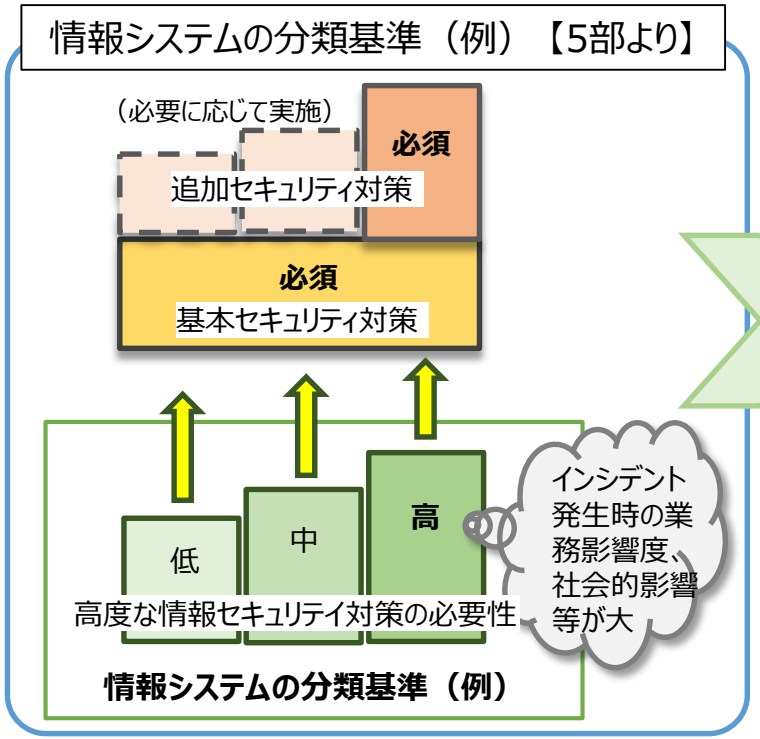
※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

他省庁が整備したシステムの利用が広がっていることや、システムの利用形態が従来の定義に収まらなくなってきたことから「政府共通利用型システム」を新たに定義し、管理側と利用側の責任分界やそれぞれに必要な対策を整理

第６・7部　情報システムの構成要素、情報システムのセキュリティ要件（改定のポイント）

- 「第６部　情報システムの構成要素」は、令和3年度版第7部に該当。**端末、サーバ装置、複合機・特定用途機器（IoT機器を含む）等といった情報システムの主たる構成要素毎に実施すべき対策**を規定。
- 「第7部　情報システムのセキュリティ要件」は、令和3年度版第6部に該当。**主たるセキュリティ機能における対策や、代表的な脅威への対応の他、ゼロトラストアーキテクチャに関する対策を加え、それぞれ実施すべき対策**を規定。
- 「情報システムの分類基準（5部参照）」に対応し、第6部・第7部の基本対策事項のうち**対策水準に段階が考えられるものについて、「基本セキュリティ対策」と「追加セキュリティ対策」とレベル分け**。
- 併せて、最新の脅威や技術の動向を踏まえ、所要の改定を盛り込み。

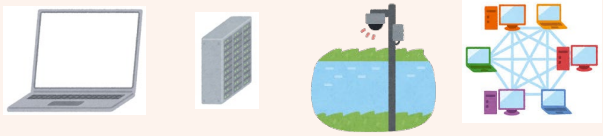
情報システムの分類基準（例）【5部より】



第6部 情報システムの構成要素

構成要素毎の実施すべき対策を規定

基本対策事項を「基本セキュリティ対策」と「追加セキュリティ対策」にレベル分け（２項目）



6.1 端末　6.2サーバ装置　6.3複合機・特定用途機器　6.4通信回線　6.5ソフトウェア　6.6アプリケーション・コンテンツ

第7部 情報システムのセキュリティ要件

機能・観点毎に実施すべき対策を規定

基本対策事項を「基本セキュリティ対策」と「追加セキュリティ対策」にレベル分け（１０項目）

7.1 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・・・）

7.2 情報セキュリティへの脅威への対策
（ソフトウェア脆弱性対策、DDoS対策・・・）

7.3 ゼロトラストアーキテクチャー

【参考】「基本セキュリティ対策」「追加セキュリティ対策」として区分した基本対策事項（一覧）①

	基本対策事項	
	基本セキュリティ対策	**追加セキュリティ対策**
6.4.3　無線LAN	6.4.3(1)-1 情報システムセキュリティ責任者は、無線LAN技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、情報システムの分類に基づき、以下の対策を講ずること。	
	以下を全て含む対策を講ずること。 a)無線LAN通信の暗号化 b)無線LAN回線利用申請手続の整備 c)無線LAN機器の管理手順の整備 d)来訪者等に提供する無線LANによるインターネット接続回線と業務で使用する機関等LANの分離	基本セキュリティ対策の実施に加えて、以下を例とする対策を講ずること。 e)IEEE 802.1Xによる無線LANへのアクセス主体の認証
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	6.6.1(3)-2 情報システムセキュリティ責任者は、ウェブアプリケーションを運用段階へ移行する前に情報システムの分類に基づき、以下の対策を実施すること。	
	開発したウェブアプリケーションに対して脆弱性診断の実施を検討すること。	高度な情報セキュリティ対策が要求される情報システムで実行するウェブアプリケーションに対して、脆弱性診断を実施すること。
7.1.2 アクセス制御機能	7.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、情報システムの分類に基づき、以下の対策を実施すること。	
	以下を例とするアクセス制御機能の要件を定めること。 a)利用時間や利用時間帯によるアクセス制御 b)同一主体による複数アクセスの制限 c)IPアドレスによる端末の制限 d)ネットワークセグメントの分割によるアクセス制御 e)ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御	基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討すること。 f)認証・認可の統合管理基盤を用いたアクセス制御 g)アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御

【参考】「基本セキュリティ対策」「追加セキュリティ対策」として区分した基本対策事項（一覧）②

	基本対策事項	
	基本セキュリティ対策	**追加セキュリティ対策**
7.1.4 ログの取得・管理	7.1.4(1)-4 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、情報システムの分類に応じて以下の対策を実施すること。	
	以下を例とする当該作業を支援する機能を導入すること。 a)ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化機能	基本セキュリティ対策の実施に加えて、以下を例とする当該作業を支援する機能の導入を検討すること。 b)リアルタイムでのログの調査・分析を行うための機能
7.1.6 監視機能	－	7.1.6(1)-4 情報システムセキュリティ責任者は、情報システム運用時の監視において、SOCやNOC等のセキュリティ監視を専門の外部事業者に業務委託することを検討すること。
7.2.1 ソフトウェアに関する脆弱性対策	7.2.1(1)-1 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に以下の対策を実施すること。	
	インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、その他のサーバ装置、端末及び通信回線装置については、情報システムの分類や保有する情報、システム特性等を踏まえ、脆弱性診断を実施を検討すること。	サーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、脆弱性診断の実施に当たっては、ペネトレーションテスト、TLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施を検討すること。
	－	7.2.1(1)-5 情報システムセキュリティ責任者は、情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計を行うこと。
	－	7.2.1(1)-6 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の運用時に、定期的な脆弱性診断（ペネトレーションテスト、TLPT等の高度な脆弱性診断を含む）の実施を検討すること。

【参考】「基本セキュリティ対策」「追加セキュリティ対策」として区分した基本対策事項（一覧）③

	基本対策事項	
	基本セキュリティ対策	**追加セキュリティ対策**
7.2.2 不正プログラム対策	－	7.2.2(1)-7 情報システムセキュリティ責任者は、EDRソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染した装置を早期にネットワークから切り離す機能の導入を検討すること。
7.2.3 サービス不能攻撃対策	7.2.3(1)-2 情報システムセキュリティ責任者は、以下を例とするサービス不能攻撃への対策を実施すること。	
	以下を例とする対策を実施すること。 a)サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入 b)サーバ装置、端末及び通信回線装置及び通信回線の冗長化	基本セキュリティ対策に加え、以下を例とする対策を検討すること。 c)インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 d)コンテンツデリバリーネットワーク（CDN）サービスの利用
	－	7.2.3(1)-9 情報システムセキュリティ責任者は、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合は、必要に応じて、CSIRT等の関係者に通知すること。
7.2.4 標的型攻撃対策	－	7.2.4(1)-5 情報システムセキュリティ責任者は、以下を例とする内部対策及び出口対策を行うこと。 a)プロキシサーバ等により、C&Cサーバ等への不正な通信を監視し、遮断する。 b)情報システムの管理者が利用する情報システム管理用の専用端末を用意し、他のセグメントと分離した運用管理セグメントを構築し、当該セグメントにシステム管理用の専用端末を接続する。 c)認証サーバに管理者権限でログインできる端末をシステム管理用の専用端末に制限する。 d)一般利用者が利用する端末間でのファイル共有機能を停止する又は一般利用者が利用する端末間の直接通信を遮断する。

第６部　情報システムの構成要素　改定のポイント①

6.1 端末

- 端末において、利用者にソフトウェアを自由にインストールさせないための技術的な措置を追加（6.1.1(1)-5）など、端末で利用するソフトウェアに係る対策を強化
- 端末に接続可能な機器を定めること（6.1.1(1)(c)）など、他の部に包括的に記載があるものの、特に端末において実施すべき対策について明記

6.2 サーバ装置

- 6.2.1 サーバ装置：
  - ✓ 端末と同様に、ソフトウェアに係る対策と接続可能な機器に係る対策を追加（6.2.1(1)(c)、(d)）
  - ✓ 要安定情報を取り扱うサーバ装置において、復旧手順の整備やバックアップの取得などの情報システムの復旧のための対策を強化（6.2.1(1)(g)、6.2.1(2)-3など）
- 6.2.2 電子メール：送信側・受信側共に、送信ドメイン認証技術(DMARC)による対策を必須化し、電子メールのなりすまし防止策を強化（6.2.2(1)-2）
- 6.2.3 ウェブ：ウェブサーバの導入・運用時の対策におけるベースラインの引上げ（6.2.3(1)-1などの、「以下を例とする」を「以下を全て含む」に変更）
- 6.2.4 ドメインネームシステム（DNS）：名前解決を停止させないための措置について、ISP等が提供するマネージドDNSサービスやDDoS対策サービスの利用、UDP及びTCPの両方でサービスを提供することを例示として追加（6.2.4(1)-1 c)、d)）
- 6.2.5 データベース：内部不正への対策としてデータの不正な操作を検知する方法を解説に追加（解説6.2.5(1)(c)）

第６部　情報システムの構成要素　改定のポイント②

6.3 複合機・特定用途機器

- 6.3.1(2)IoT機器を含む特定用途機器：使用しない場合は電源をオフにする（6.3.1(2)-1 h)）など、サイバー攻撃を受ける機会を減らす等のための対策を強化

6.4 通信回線

- 6.4.1 通信回線：
  - ✓ 令和３年度版は入口対策が中心であったところ、出口対策を追加（6.4.1(2)-1など）。また、通信回線の監視について、入口・出口とともに、内部ネットワークの監視に言及（6.4.1(2)-3）
  - ✓ ネットワークの監視内容や、保守・診断のためのリモートメンテナンスに係る対策を定期的に見直すことを追加(6.4.1(3)(b)、(c))
- 6.4.2 通信回線装置：従来、通信回線と一体で記載されていたが、通信回線装置自体の重要性に鑑み分離
- 6.4.3 通信回線装置：従来、遵守事項の一つであった無線LANに係る規定を款として新設

6.5 ソフトウェア

- スライド43参照

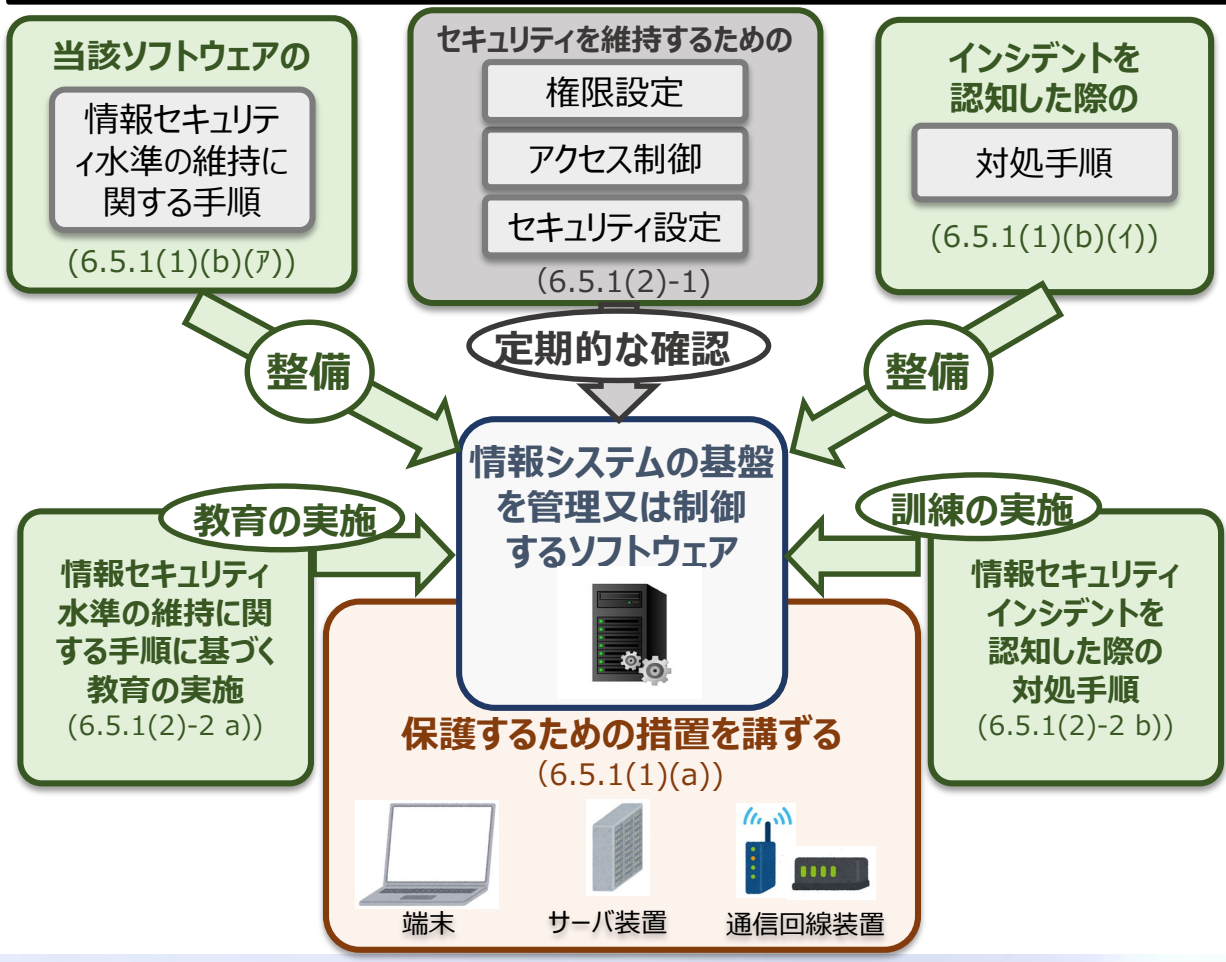
6.6 アプリケーション・コンテンツ

- 不審なウェブサイトの通報を受け付ける体制を整備することを追加（6.6.2(2)-3）
- 利用者の情報セキュリティ対策の水準の低下を招く設定変更を強制することのないよう、提供方式等を見直す対策を追加。また、定期的に脆弱性対策の状況を確認すること、ウェブアプリケーション等の改ざんを検知する措置を設けることを追加(6.6.1(4))
- 追加セキュリティ対策として、高度な情報セキュリティ対策が要求される情報システムで実行するウェブアプリケーションに対して、脆弱性診断を実施することを追加（6.6.1(3)-2）

6.5 ソフトウェア（改定のポイント）

「6.5　ソフトウェア」とは？

- 情報システムを構成する多種多様なソフトウェアのうち、端末やサーバ装置、ネットワークなどの機器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となるソフトウェアである「情報システムの基盤を管理又は制御するソフトウェア」については、情報セキュリティを確保するために必要な対策を規定。
- また、当該ソフトウェアを利用する際の操作ミスや設定不備などを防ぐための**情報セキュリティ水準の維持に関する手順等の整備**等を求める。



改定のポイント

- 情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を**保護するための措置**（管理者権限への多要素主体認証の適用、アクセス権限の最小化と不正なアクセスがないか監視するなど）（6.5.1(1)(a)）
- 当該ソフトウェアの**情報セキュリティ水準の維持に関する手順の整備**（6.5.1(1)(b)(ア)）
- 当該ソフトウェアで発生した**情報セキュリティインシデントを認知した際の対処手順の整備**（6.5.1(1)(b)(イ)）
- 当該ソフトウェアのセキュリティを維持するため、権限設定やアクセス制御、セキュリティ設定が適切であるか**定期的な確認**（6.5.1(2)-1）
- 当該ソフトウェアについて、情報セキュリティ水準の維持に関する手順に基づく**教育の実施**、情報セキュリティインシデントを認知した際の対処手順に基づく**訓練の実施**（6.5.1(2)-2 a)、b)）

【参考】第６部　情報システムの構成要素（目次レベルの変更点①）

令和３年度版

- 第7部　情報システムの構成要素
  - 7.1　端末・サーバ装置等
    - 7.1.1　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
      - (4)　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
      - (5)　機関等支給以外の端末の導入及び利用時の対策
    - 7.1.2　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
    - 7.1.3　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
  - 7.2　電子メール・ウェブ等
    - 7.2.1　電子メール
      - (1)　電子メールの導入時の対策
    - 7.2.2　ウェブ
      - (1)　ウェブサーバの導入・運用時の対策
      - (2)　ウェブアプリケーションの開発時・運用時の対策
    - 7.2.3　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
    - 7.2.4　データベース
      - (1)　データベースの導入・運用時の対策

R5 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」へ

令和５年度版

- 第6部　情報システムの構成要素
  - 6.1　端末・サーバ装置等
    - 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　新設
      - (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　新設
      - (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

※令和５年度の改定において、第６部と第７部はそれぞれ入れ替えを行った。
・R3 第7部 情報システムの構成要素⇒R5 第6部へ
・R3 第6部 情報システムのセキュリティ要件⇒R5 第7部へ

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）の対策を整理した上で、款を新設

機関等支給以外の端末の対策を整理した上で、款を新設

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

【参考】第６部　情報システムの構成要素（目次レベルの変更点②）

令和３年度版

第7部　情報システムの構成要素
- 7.2　電子メール・ウェブ等
  - 7.2.2　ウェブ
    - (1)　ウェブサーバの導入・運用時の対策
    - (2)　ウェブアプリケーションの開発時・運用時の対策
- 7.3　通信回線
  - 7.3.1　通信回線
    - (1)　通信回線の導入時の対策
    - (2)　通信回線の運用時の対策
    - (3)　通信回線の運用終了時の対策
    - (4)　無線LAN環境導入時の対策
  - 7.3.2　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

R5 6.2.3「ウエブ」へ

第6部　情報システムのセキュリティ要件
- 6.3　アプリケーション・コンテンツの作成・提供
  - 6.3.1　アプリケーション・コンテンツの作成時の対策
    - (1)　アプリケーション・コンテンツの作成に係る規定の整備
    - (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
  - 6.3.2　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

令和５年度版

第6部　情報システムの構成要素
- 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　新設
    - (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　新設
    - (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　新設
  - 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

※令和５年度の改定において、第６部と第７部はそれぞれ入れ替えを行った。
- R3 第7部 情報システムの構成要素⇒R5 第6部へ
- R3 第6部 情報システムのセキュリティ要件⇒R5 第7部へ

従来、通信回線と一体で記載されていたが、通信回線装置自体の重要性に鑑み分離

通信回線装置の分離に伴い、構成の見直し

「情報システムの基盤を管理又は制御するソフトウェア」（※）について、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を規定
（※）端末やサーバ装置の制御、統合的な主体認証管理、資産管理、ネットワーク監視など、情報システムを制御する上でセキュリティ上の重要な機能を有しているソフトウエア

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

開発時と運用時の対策を分離

第７部　情報システムのセキュリティ要件　改定のポイント①

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：クラウドサービスの管理者権限を有する主体などの厳格な主体認証が必要な場合において多要素主体認証の必須化(7.1.1(1)-2)。また、強固なパスワードとして、推測が困難なパスフレーズを用いることを例示するなど、パスワードに係る対策を強化(7.1.1(1)-3)

- 7.1.2 アクセス制御機能：アクセス制御要件の定期的な見直しを追加(7.1.2(1)-2)。また、追加セキュリティ対策として、認証・認可の統合管理基盤や動的なアクセス制御の適用を検討することを追加(7.1.2(1)-1 f)、g))

- 7.1.3 権限の管理：ISO27002の、「5.15 アクセスコントロール」の規定の内、知る必要性（need-to-know）、アクセスの必要性（need-to-use）、最小限の特権を前提とする原則の考え方を、目的・趣旨等に追加。また、必要最小限の範囲でのアクセス権限設定(7.1.3(1)(a))と定期的な見直し(7.1.3(1)(c))を盛り込み。さらに、管理者権限を有する識別コードの権限管理に係る対策を強化(7.1.3(1)-1,-3)

- 7.1.4 ログの取得・管理：追加セキュリティ対策として、ログの分析におけるSIEM導入について検討することを追加(7.1.4(1)-4)

- 7.1.5 暗号・電子署名：「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）」及び「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の文書と整合性を取り、電子政府推奨暗号リストの暗号技術を利用していると見なす条件として、従来のアルゴリズムに加えて鍵長を明示(7.1.5(1)(b)など)

- 7.1.6 監視機能：監視機能の重要性を鑑み、従来第５部に記載されていた監視に係る規定を抜き出し、新たな款として規定。また、情報システムへの監視機能導入を必須化(7.1.6(1)(a))。さらに、追加セキュリティ対策として、SOCやNOC等の監視を外部事業者に業務委託することを検討することを追加(7.1.6(1)-4)

第７部　情報システムのセキュリティ要件　改定のポイント②

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：
  - ✓ インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置等について、運用開始時に脆弱性診断の実施を追加(7.2.1(1)-1)
  - ✓ 追加セキュリティ対策として、高度な情報セキュリティ対策が要求されるシステムは、直接インターネットから到達可能であるかなどに関わらず、運用開始時及び定期的な脆弱性診断（ペネトレーションテストやTLPT等の高度な脆弱性診断を含む）の実施を検討することを追加(7.2.1(1)-1,-6)
  - ✓ 追加セキュリティ対策として、高度な情報セキュリティ対策が要求されるシステムは、セキュリティパッチの随時の適用を前提とした運用設計を行うことを追加(7.2.1(1)-5 b))
- 7.2.2 不正プログラム対策：追加セキュリティ対策として、EDR等により端末やサーバ装置の活動を監視し、不正プログラムに感染したおそれのある端末やサーバ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を追加(7.2.2(1)-7)
- 7.2.3 サービス不能攻撃対策：⇒スライド48参照
- 7.2.4 標的型攻撃対策：追加セキュリティ対策として、高度な情報セキュリティ対策が要求されるシステムにおいて実施するべき内部対策・出口対策を具体化（プロキシサーバ等を利用した不正通信の監視・遮断など）(7.2.4(1)-5)

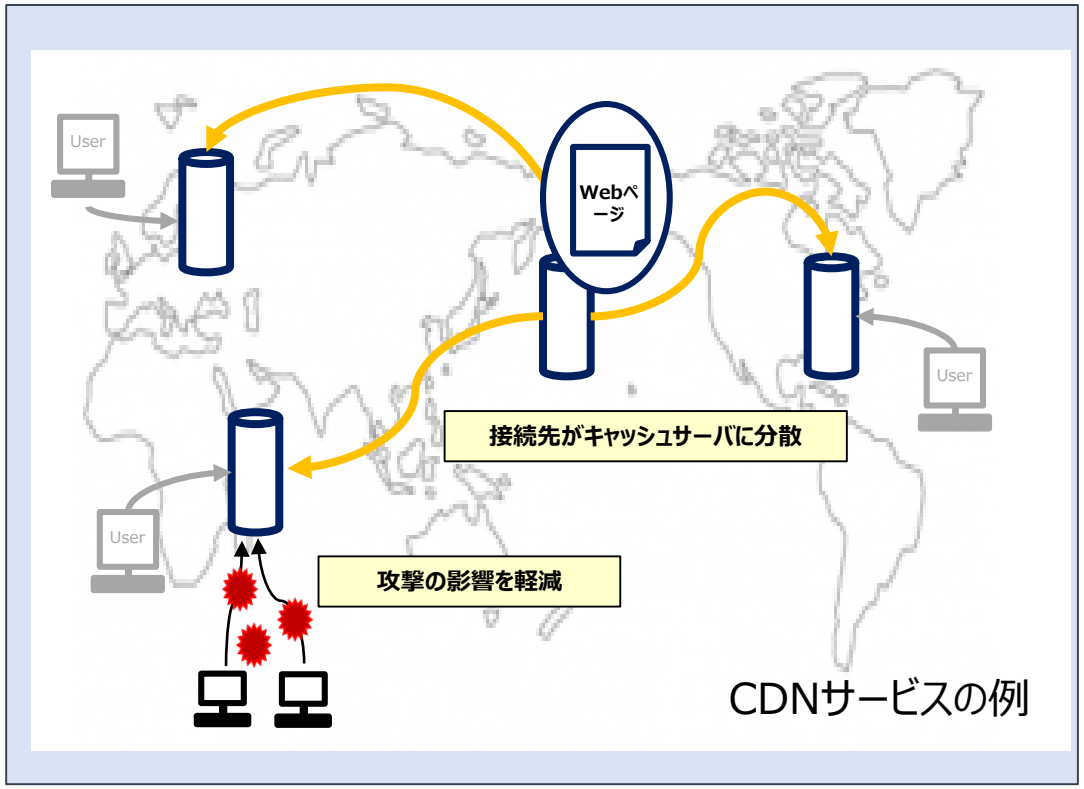
7.3 ゼロトラストアーキテクチャ

- スライド49参照

7.2.3 サービス不能攻撃対策（改定のポイント）

「7.2.3　サービス不能攻撃対策」とは？

- インターネットからアクセスを受ける情報システムのうち、要安定情報※を取り扱う情報システムに対し、サービス不能攻撃に対処するために必要な対策を規定（※「要安定情報」：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）
- 昨今の政府機関等の情報システムのインシデントを踏まえ、サービス不能攻撃の影響を排除又は低減するための対策を強化するとともに、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を強化



CDNサービスの例

改定のポイント

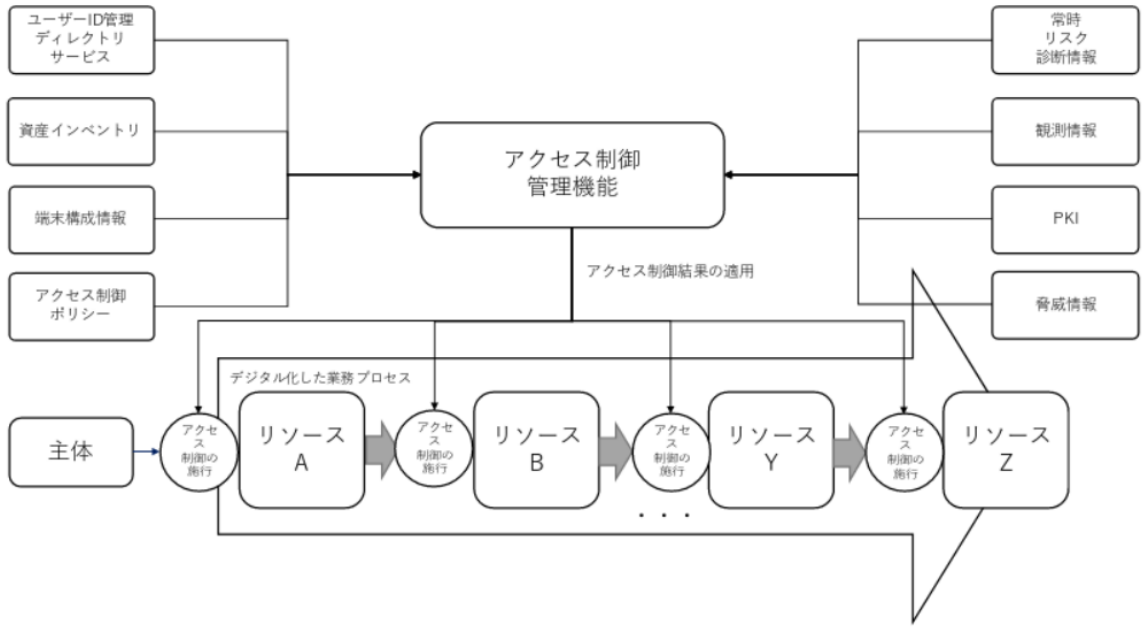
- サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入、あるいはサーバ装置や通信回線等の冗長化による対策の原則化（基本対策事項7.2.3(1)-2）
- 追加セキュリティ対策として、CDNサービスの利用や、クラウドサービス事業者等が提供するサービス不能攻撃に係る通信を遮断するサービスの利用の検討（基本対策事項7.2.3(1)-2）
- 監視によって平常時の負荷の状況を把握し、これを著しく逸脱したと判断する目安を定め、これを超えた時の対応について明記（基本対策事項7.2.3(1)-7、8）
- 追加セキュリティ対策として、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合の関係者への通知（基本対策事項7.2.3(1)-9）

7.3 ゼロトラストアーキテクチャー（改定のポイント）

「7.3　ゼロトラストアーキテクチャ」

- 「ゼロトラストアーキテクチャ」は、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。
- 本節では、ゼロトラストアーキテクチャに基づく情報資産の保護策を行う仕組みを実現する機能の一部と考えられる「動的アクセス制御」（※）を実装する場合に特に必要となる対策事項を規定。

※ 「動的なアクセス制御」とは、特定のアクセスに対して、セッションが確立してない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。



ゼロトラストアーキテクチャ概念図
（出典）ゼロトラストアーキテクチャ適用方針（デジタル庁）

改定のポイント

- 複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任（7.3.1(1)）
- 動的なアクセス制御の導入方針を定めるにあたり、動的アクセス制御の**対象とする情報システムと対象とする情報システムのリソース（ユーザーアカウント、機器等）を識別**（7.3.1(2)）
- 動的なアクセス制御の実装にあたり、リソースの信頼情報の変化に応じた**動的なアクセス制御のポリシーを作成**し、動的なアクセス制御のポリシーに基づき、**動的なアクセス制御を行う**（7.3.1(3)）
- 動的なアクセス制御の運用に際し、アクセスパターンの変化に応じて、再度リスク評価を行い、**動的なアクセス制御のポリシーを見直す**（7.3.2(1)）。また、リソースの信頼情報の収集により**検出されたリスクへ対処を行う**。（7.3.2(2)）

【参考】第７部　情報システムのセキュリティ機能（目次レベルの変更点）

令和３年度版

- 第5部　情報システムのライフサイクル
  - 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)　情報システムのセキュリティ要件の策定
    - 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

令和３年度版

- 第6部　情報システムのセキュリティ要件
  - 6.1　情報システムのセキュリティ機能
    - 6.1.1　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
    - 6.1.2　アクセス制御機能
      - (1)　アクセス制御機能の導入
    - 6.1.3　権限の管理
      - (1)　権限の管理
    - 6.1.4　ログの取得・管理
      - (1)　ログの取得・管理
    - 6.1.5　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
  - 6.2　情報セキュリティの脅威への対策
    - 6.2.1　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
    - 6.2.2　不正プログラム対策
      - (1)　不正プログラム対策の実施
    - 6.2.3　サービス不能攻撃対策
      - (1)　サービス不能攻撃対策の実施
    - 6.2.4　標的型攻撃対策
      - (1)　標的型攻撃対策の実施
  - 6.3　アプリケーション・コンテンツの作成・提供
    - 6.3.1　アプリケーション・コンテンツの作成時の対策
      - (1)　アプリケーション・コンテンツの作成に係る規定の整備
      - (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
    - 6.3.2　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

R5 6.6へ

令和５年度版

- 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　新設
      - (1)　監視機能の導入・運用
  - 7.2　情報セキュリティへの脅威への対策
    - 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　新設
    - 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

※令和５年度の改定において、第６部と第７部はそれぞれ入れ替えを行った。
・R3 第7部 情報システムの構成要素⇒R5 第6部へ
・R3 第6部 情報システムのセキュリティ要件⇒R5 第7部へ

監視機能に係る要件を7.1.6に移設した上で、原則としてすべての情報システムについて、監視のために必要な機能を備えるよう対策を強化

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

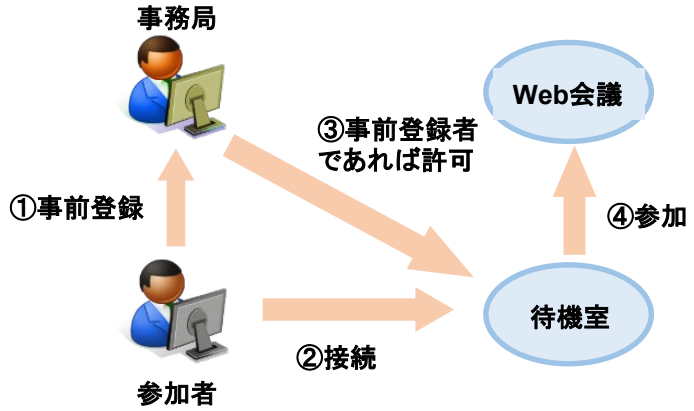
主体へのなりすましの脅威への対策の必要性の高まりを受け、ゼロトラストアーキテクチャに関わる規定を新設

第８部　情報システムの利用　（改定のポイント）

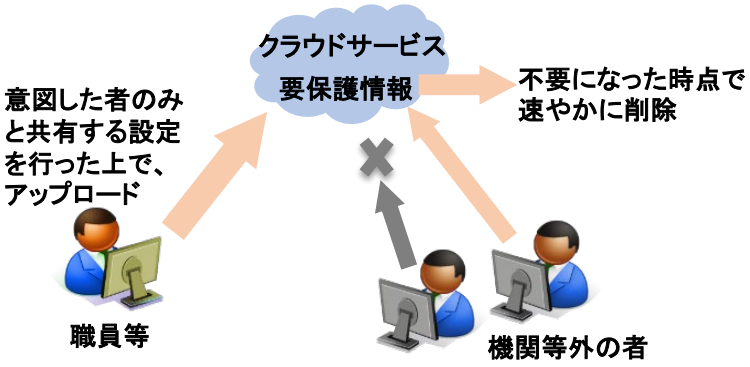
「第８部　情報システムの利用」とは？

➢「第８部　情報システムの利用」では、電子メールや端末、Web会議サービス等の情報システムを職員等が利用する際の対策や、ソーシャルメディアによる情報発信、テレワーク実施にあたっての対策を規定している。

〇Web会議に無関係な者を参加させないための対策例



〇クラウドサービスを利用した情報共有時の対策例



改定のポイント

（１）利用承認を得ていないクラウドサービスの利用の禁止

- 利用承認を得ていないクラウドサービスの利用（いわゆるシャドーIT）を明示的に禁止する規定を追加（遵守事項8.1.1(3)(h) ）

（２）Web会議サービスの利用時の対策を強化

- 事前登録制にするなど、Web会議に無関係な者を参加させないための対策の例を追加（基本対策事項8.1.1(9)-2）
- 機関等が利用を承認していないWeb会議サービスをやむを得ず利用する際の、情報の取扱いに係る留意点を解説に追加（(解説)基本対策事項8.1.1(9)-1 b)）

（３）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を追加

- オンラインストレージ等のファイル共有サービスの利用拡大を踏まえ、当該サービス利用時における情報の取扱いに係る規定を追加（遵守事項8.1.1(10) ）

【参考】第８部　情報システムの利用（目次レベルの変更点）

令和３年度版

- **第8部　情報システムの利用**
  - 8.1　情報システムの利用
    - 8.1.1　情報システムの利用
      - (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) 電子メール・ウェブの利用時の対策
      - (5) 識別コード・主体認証情報の取扱い
      - (6) 暗号・電子署名の利用時の対策
      - (7) 不正プログラム感染防止
      - (8) Web会議サービスの利用時の対策
    - 8.1.2　ソーシャルメディアサービスによる情報発信
      - (1) ソーシャルメディアサービスによる情報発信時の対策
    - 8.1.3　テレワーク
      - (1) 実施規定の整備
      - (2) 実施環境における対策
      - (3) 実施時における対策

令和５年度版

- **第8部　情報システムの利用**
  - 8.1　情報システムの利用
    - 8.1.1　情報システムの利用
      - (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　新設
    - 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

基本的対策として一体になっていた端末（支給外端末を含む）の対策を分離

機関等外の者と情報の共有を行う際、オンラインストレージ等のファイル共有サービスを利用する方法が普及していることを受け、当該サービスの利用を想定した際の職員等の留意点を規定

※赤字は、目的・趣旨、遵守事項、基本対策事項レベルで改定を行った箇所（※表現の見直しなどの軽微な修正は除く）

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