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（※）の概要

（※）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

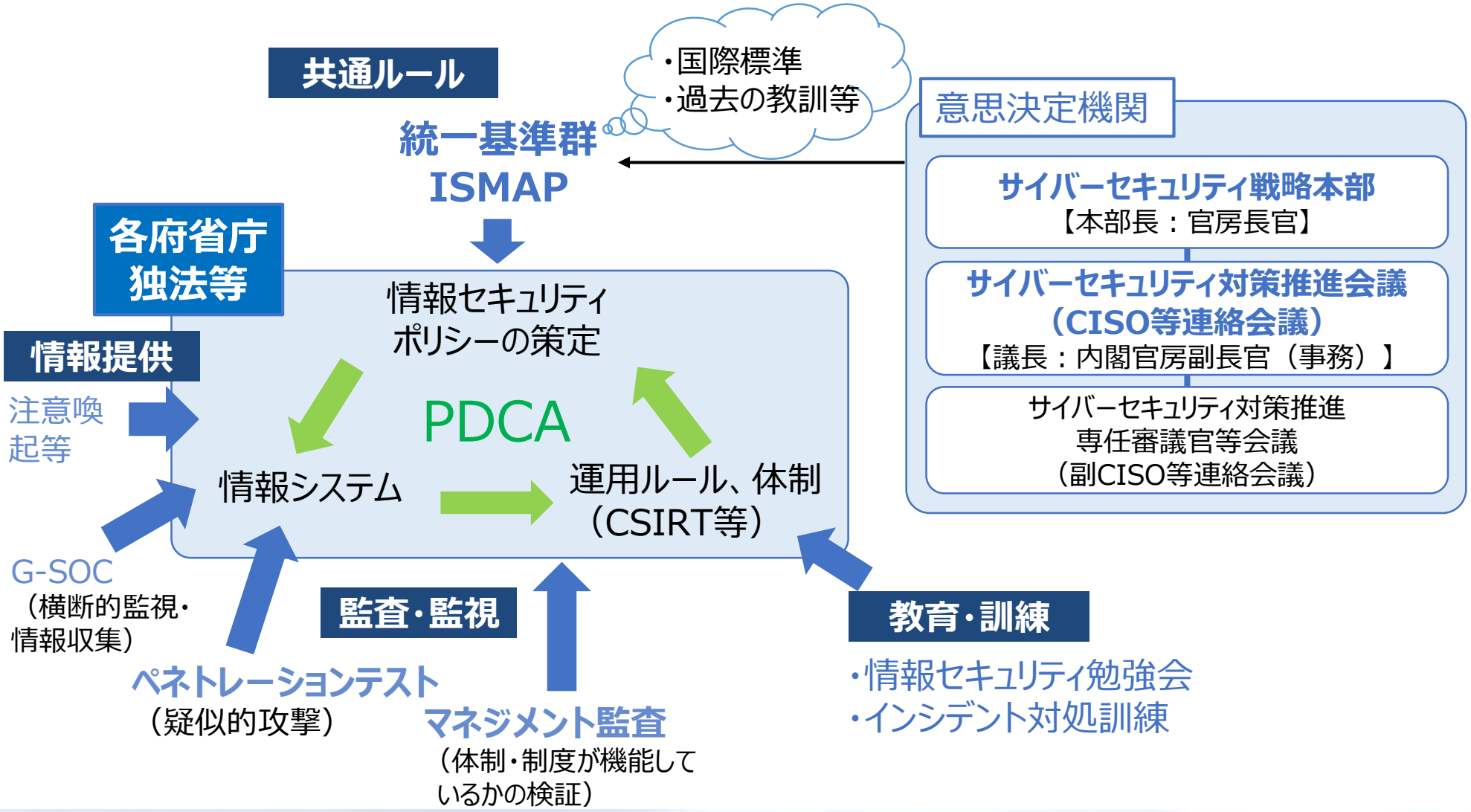
内閣官房 内閣サイバーセキュリティセンター

政府機関総合対策グループ

目次

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



政府統一基準とは

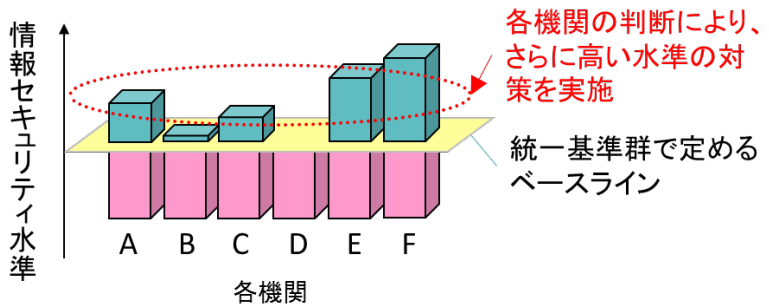
- 政府統一基準は、**サイバーセキュリティ基本法に基づく、政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み**。
- 統一基準では、**政府機関等が講ずるべき情報セキュリティ対策のベースライン**を定めている。
- 政府機関および独立行政法人等は、**政府統一基準に準拠**しつつ、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシーを策定**。これにより、政府機関等のどの組織においても、一定以上のセキュリティ対策の水準が確保されるよう図るもの。

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。

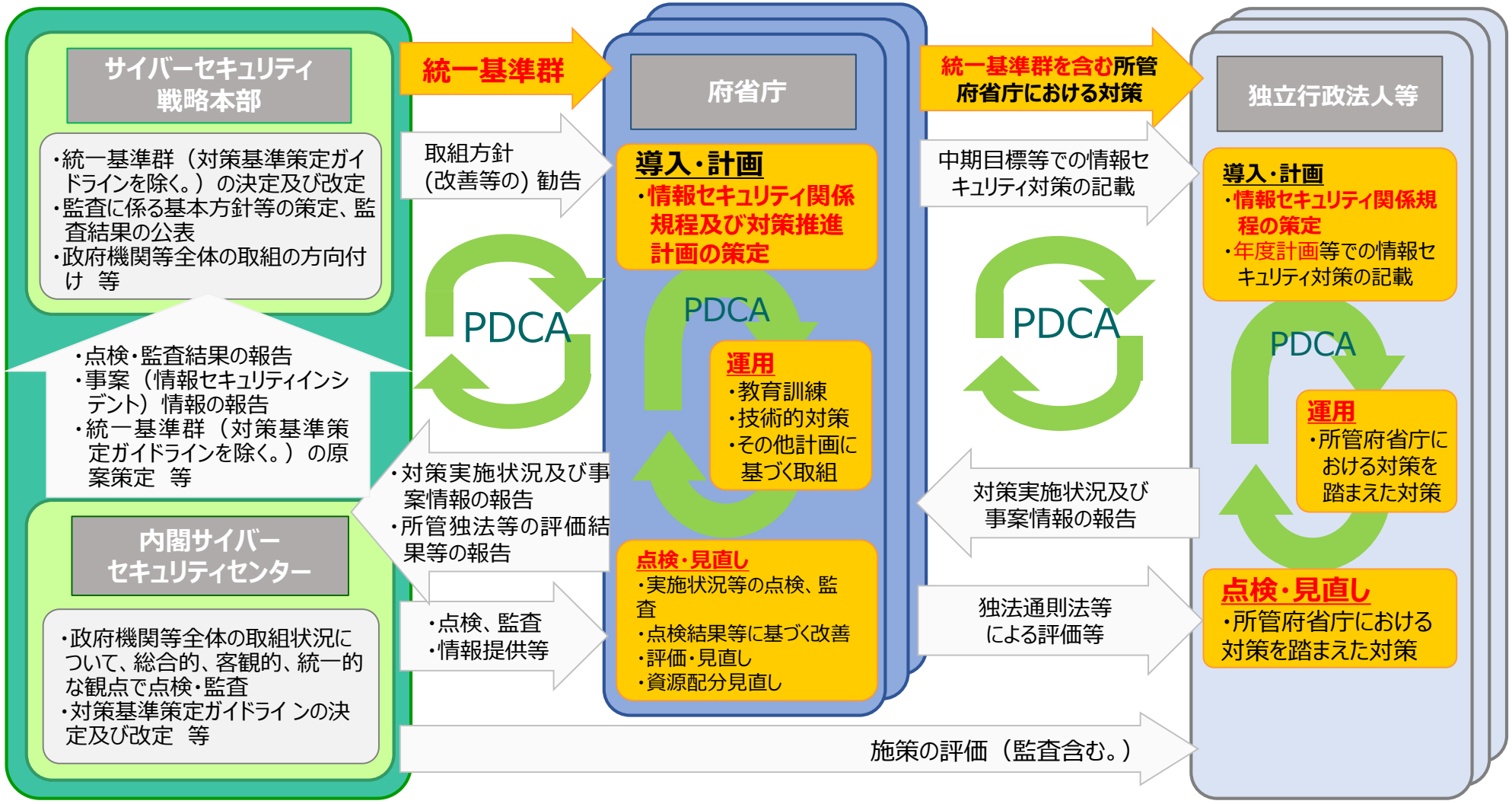
政府機関等のサイバーセキュリティ対策のための統一規範（令和５年７月４日サイバーセキュリティ戦略本部改定）（抜粋）

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。

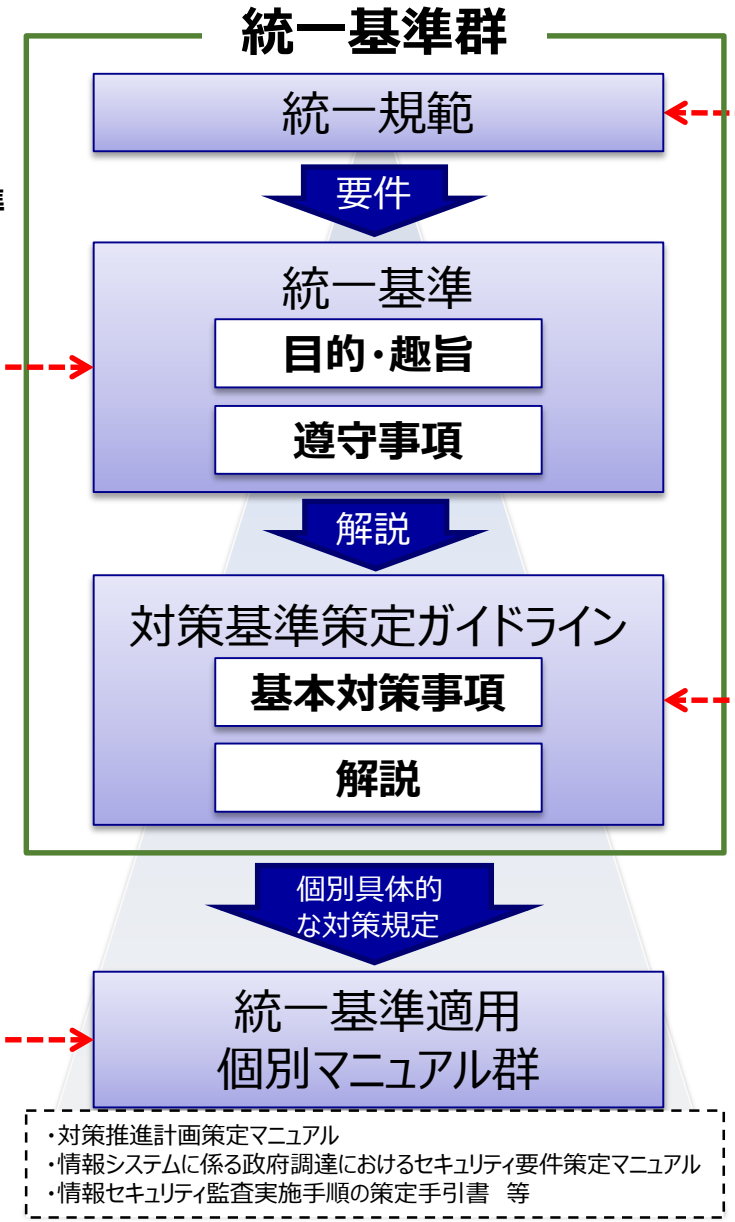


政府機関等全体における情報セキュリティのPDCAサイクル

- 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。



政府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

目次

今般改定の背景

- 政府統一基準群（※）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**。（※）統一規範、統一基準、ガイドラインで構成される文書群をいう。
- 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。

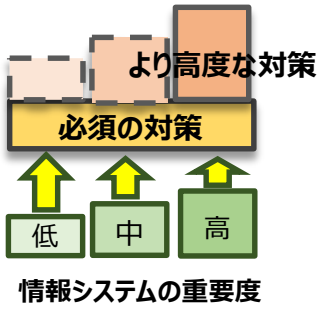
脅威・技術動向を踏まえての対策の強化 → 改定ポイント「４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化」

- 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。

政府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。

政府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。 

（参考）これまでの政府統一基準群の改定内容

■　サイバーセキュリティ基本法（平成26年法律第104号）第26条第１項第２号に基づき、国の行政機関等のサイバーセキュリティに関する対策の基準を作成。サイバーセキュリティを巡る動向等を踏まえ、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年に一度改定している。

サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター設置
（平成27年１月）

平成28年度版（平成28年８月31日サイバーセキュリティ戦略本部決定）

- 政府機関に加えて、**独立行政法人及び指定法人を適用対象に**。
- 独立行政法人等において、情報セキュリティ対策が適切に講じられるよう、対策基準等の策定、体制の構築、対策実施状況の評価等を含む**情報セキュリティマネジメントの強化**に主眼を置いた規定を追加。
- 日本年金機構における情報流出事案をはじめとする情報セキュリティインシデントの発生状況やサイバー攻撃の動向等を踏まえ、**CSIRT体制構築等**の事前準備、**標的型攻撃等による不正プログラム感染を前提とする情報システムの防御策強化**に係る規定の追加。

平成30年度版（平成30年７月25日サイバーセキュリティ戦略本部決定）

- 国民が安心して安全にウェブサイト等を通じて行政サービスを利用できるよう、**利用者側に立った対策の追加**。
- 政府機関等の**自律的な能力向上のためのPDCAサイクルの効果的運用**に係る規定を整備。
- モバイル端末の利用について、一定の安全対策を講じた場合には、**端末をネットワーク接続して業務を行うことを可能とする規定**を新設。

令和３年度版（令和３年７月７日サイバーセキュリティ戦略本部決定）

- 政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、**クラウドサービス利用者側として実施すべき対策や考え方**に係る記載を追加。
- 政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえ、CDN※１サービスやEDR※２等の**より強固なセキュリティ対策**について記載。
- **多様な働き方を前提とする場合に必要な情報セキュリティ対策**について、政府機関等が実施すべき対策の水準を明確化。

※１：CDN（Contents Delivery Network）
※２：EDR（Endpoint Detection and Response）

（参考）政府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

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