NISC National center of Incident readiness and Strategy for Cybersecurity

令和５年度
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（※）の改定案について

（※）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
- 政府機関等の対策基準策定のためのガイドライン

内閣官房
内閣サイバーセキュリティセンター（NISC）
令和５年４月

政府統一基準とは

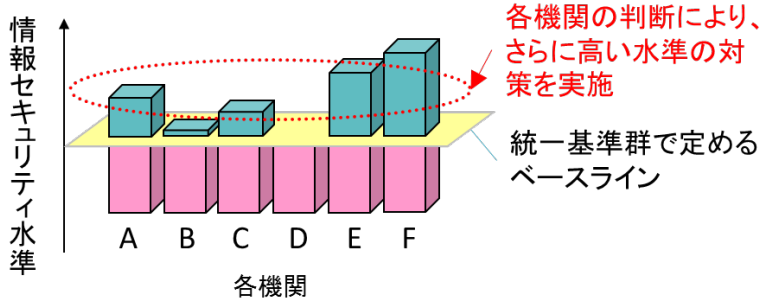
- 政府統一基準は、**サイバーセキュリティ基本法に基づく、政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み**。
- 統一基準では、**政府機関等が講ずるべき情報セキュリティ対策のベースライン**を定めている。
- 政府機関および独立行政法人等は、**政府統一基準に準拠**しつつ、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシーを策定**。これにより、政府機関等のどの組織においても、一定以上のセキュリティ対策の水準が確保されるよう図るもの。

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3年７月７日サイバーセキュリティ戦略本部改定）（抜粋）

第四条　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、別に定める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。



政府統一基準の適用対象

- 対象組織は、**国の行政機関、独立行政法人及び指定法人**（総称して、「機関等」あるいは「政府機関等」）
- 適用対象者は、**政府機関等において行政事務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の情報**（※）を取り扱う者。 ※「情報」の範囲は、規範第二条三項

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3年７月７日サイバーセキュリティ戦略本部改定）（抜粋）

（適用対象）
第二条 本規範の**適用対象とする組織は、次の各号に掲げるとおりとする。**
一 国の行政機関
二 独立行政法人 独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人
三 指定法人 法第十三条に規定する指定法人
２ 本規範の適用対象とする者は、**国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）**とする。
３ 本規範の**適用対象とする情報**は、職員等が**職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）及び情報システムの設計又は運用管理に関する情報**とする。

改定案の概要＜組織的な取組の強化＞

	現状（令和３年度版）	改定案のポイント
第２部　対策の基本的枠組み 情報セキュリティに係る組織マネジメントについて、ISO27001（情報セキュリティマネジメントシステム）を参考としたPDCAサイクル（Plan「導入・計画」、Do「運用」、Check「点検」、Act「見直し」）に沿って必要な対策を規定	○ 情報セキュリティ対策を見直した結果のCISOへの報告を規定 ○ 所管独法等の情報セキュリティ対策は各独法等が実施	➢ 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** ➢ 所管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**府省庁側の体制の整備**、独法等から府省庁側へ**助言を求めること**を明記
第４部　外部委託 機関等外の者への業務委託や外部サービス利用、機器等調達の際に、委託先等に求める情報セキュリティ対策を規定（サプライチェーンのセキュリティ対策）	○ 委託先に担保させるべき一般的な情報セキュリティ対策を規定 ○ クラウドサービスの選定において、ISMAP管理基準に沿った選定を行う ○ ソフトウェアや機器の調達においては、IT調達申合せを参考に調達	➢ 委託先に提供した政府の情報が適切に保護されるよう、業務委託契約時・実施期間中・終了時に委託先に担保させるべき情報セキュリティ対策を、**米国NISTのサプライチェーン対策を参考に具体化** ➢ 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クラウドサービスリストから選定」するように見直し** ➢ 重要なソフトウェアの調達時のサプライチェーン・リスクへの対応として**IT調達申合せに基づく対応を明記**するとともに、**サプライチェーン・リスクに対応する必要がある重要なソフトウェアを明示**

改定案の概要＜情報システムに係るセキュリティ対策の強化＞

	現状（令和３年度版）	改定案のポイント
第５部 情報システムのライフサイクル 情報システムの企画、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留意すべき事項を規定	○ 府省庁の判断により、情報システムに求めるセキュリティ対策を定めていることから、対策の程度にばらつきが生じることがある ○ 情報システムの特性に応じて、バックアップの取得や復旧訓練の実施を判断	➢ 「情報システムの分類基準」を用いた**情報システムの重要度（高・中・低）の考え方を提示**。これにより、**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事項**に加えて、**重要度の高い情報システムに対してはより高度な対策**を規定 ➢ 情報システムの復旧手順の整備、適切なバックアップの取得、バックアップ要件・復旧手順の見直し等の**情報システムの復旧対策を強化**
第６部 情報システムの構成要素 情報システムの構成要素（端末、サーバ装置、ソフトウェア等）における対策 **第７部 情報システムのセキュリティ要件** セキュリティ機能（主体認証、権限の管理、ログの管理等）の活用、脅威（脆弱性対策、不正プログラム対策等）への対策	○ ソフトウェアの運用開始時と運用中の定期的な脆弱性対策の実施を規定 ○ サービス不能攻撃に対処するための機能の有効化などの実施	➢ 運用開始時の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。あわせて、**重要なソフトウェアについては、当該ソフトウェアに係る手順の整備や設定の定期的な確認**等の情報セキュリティ水準を維持するための対策を追加 ➢ **サービス不能攻撃専用の対策装置やサービス導入あるいはサーバ装置や通信回線等の冗長化を原則化に加え**、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** ➢ **技術面での対策の最新化：** • 厳格な主体認証が必要な場合に**多要素認証方式を原則化** • 原則すべての情報システムに**監視機能**を備えるよう対策を強化 • ゼロトラストアーキテクチャに基づく情報資産の保護策の一つであり、アクセス制御の仕組みを実現する機能の一部と考えられる**「動的なアクセス制御」**の実装に必要となる対策を追加