

政府機関の情報セキュリティ対策のための統一規範 (案)

平成23年4月21日
平成24年4月26日改定
平成26年 月 日改定
情報セキュリティ政策会議決定

- 第一章 目的及び適用対象（第一条—第二条）
- 第二章 政府機関の情報セキュリティ対策のための基本指針（第三条—第四条）
- 第三章 政府機関の情報セキュリティ対策のための基本対策（第五条—第二十三条）
- 附則

第一章 目的及び適用対象

（目的）

第一条 本規範は、政府機関の情報セキュリティを確保するため、政府機関のとるべき対策の統一的な枠組みを定め、各政府機関に自らの責任において対策を図らしめることにより、もって政府機関全体の情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第二条 本規範の適用対象とする政府機関は、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第二十号）第三条第二項に規定する機関若しくはこれらに置かれる機関（以下「府省庁」という。）とする。

2 本規範の適用対象とする者は、府省庁において行政事務に従事している国家公務員その他の府省庁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「行政事務従事者」という。）とする。

3 本規範の適用対象とする情報は、行政事務従事者が職務上取り扱う情報であって、情報処理及び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。

第二章 政府機関の情報セキュリティ対策のための基本指針

(リスク評価と対策)

第三条 各府省庁は、府省庁の保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じなければならない。

2 各府省庁は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直さなければならない。

(府省庁情報セキュリティ文書)

第四条 各府省庁は、当該府省庁の特性を踏まえ、当該府省庁における情報セキュリティ対策の基本的な方針（以下「府省庁基本方針」という。）及び情報セキュリティ対策基準（以下「府省庁対策基準」という。）を定めなければならない。府省庁基本方針及び府省庁対策基準（以下「府省庁ポリシー」という。）の呼称は各府省庁で独自に定めることができる。

2 府省庁基本方針は、情報セキュリティを確保するため、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なければならない。

3 府省庁対策基準は、別に定める政府機関の情報セキュリティ対策のための統一基準（以下「政府機関統一基準」という。）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。

4 各府省庁は、前条第一項の評価の結果を踏まえ、府省庁ポリシーの評価及び見直しを行わなければならない。

第三章 政府機関の情報セキュリティ対策のための基本対策

(管理体制)

第五条 各府省庁は、情報セキュリティ対策を実施するための組織・体制を整備しなければならない。

2 各府省庁は、最高情報セキュリティ責任者 1 人を置かななければならない。

3 最高情報セキュリティ責任者は、府省庁対策基準等の審議を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置かななければならない。

4 最高情報セキュリティ責任者は、本規範にて規定した当該府省庁における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。

5 最高情報セキュリティ責任者は、自らの所掌する事務を政府機関統一基準に定める責任者に分掌させることができる。

(対策推進計画)

第六条 最高情報セキュリティ責任者は、第三条第一項の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めなければならない。

2 各府省庁は、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。

3 最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行わなければならない。

（例外措置）

第七条 各府省庁は、府省庁ポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を府省庁ポリシーの中で定めなければならない。

（教育）

第八条 各府省庁は、行政事務従事者に対し、自覚をもって府省庁ポリシーに定めた情報セキュリティ対策を実施するために、情報セキュリティに関する教育を行わなければならない。

（情報セキュリティインシデントへの対応）

第九条 各府省庁は、情報セキュリティインシデント（JIS Q 27001:2006における情報セキュリティインシデントをいう。以下同じ。）に対処するため、必要な措置を定め、実施しなければならない。

2 情報セキュリティインシデントを認知した者は、府省庁ポリシーに定める報告窓口に連絡しなければならない。

3 府省庁ポリシーに定める責任者は、情報セキュリティインシデントの報告を受け又は認知したときは、必要な措置を講じなければならない。

（自己点検）

第十条 各府省庁は、情報セキュリティ対策の自己点検を行わなければならない。

（監査）

第十一条 各府省庁は、府省庁対策基準が政府機関統一基準に準拠し、かつ実際の運用が府省庁対策基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。

（情報の格付）

第十二条 各府省庁は、取り扱う情報に、機密性、完全性及び可用性の観点に区別

して、分類した格付を付さなければならない。

- 2 各府省庁は、府省庁間での情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。

(情報の取扱制限)

第十三条 各府省庁は、情報の格付に応じた取扱制限を定めなければならない。

- 2 各府省庁は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。
- 3 各府省庁は、府省庁間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。

(情報のライフサイクル管理)

第十四条 各府省庁は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施しなければならない。

(情報を取り扱う区域)

第十五条 各府省庁は、府省庁が管理する庁舎又は府省庁外の組織から借用している施設等府省庁の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施しなければならない。

(外部委託)

第十六条 各府省庁は、情報処理に係る業務を外部委託（約款による外部サービスを利用し、行政事務を遂行する場合を含む。）する際には、必要な措置を定め、実施しなければならない。

- 2 各府省庁は、外部委託を実施しようとするときは、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。
- 3 各府省庁は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。

(情報システムに係る文書及び台帳整備)

第十七条 各府省庁は、所管する情報システムに係る文書及び台帳を整備しなければならない。

(情報システムのライフサイクル全般にわたる情報セキュリティの確保)

第十八条 各府省庁は、所管する情報システムの企画、調達・構築、運用・保守、

更改・廃棄及び見直しの各段階において情報セキュリティを確保するための措置を定め、実施しなければならない。

(情報システムの運用継続計画)

第十九条 各府省庁は、所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案しなければならない。

2 各府省庁は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認しなければならない。

(暗号・電子署名)

第二十条 各府省庁は、府省庁における暗号及び電子署名の利用について、必要な措置を定め、実施しなければならない。

(インターネット等を用いた行政サービスの提供)

第二十一条 各府省庁は、インターネット等を用いて行政サービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施しなければならない。

(情報システムの利用)

第二十二条 各府省庁は、情報システムの利用に際して、行政事務従事者に情報セキュリティを確保するために行わせる必要な措置を定め、実施しなければならない。

(政府機関統一基準への委任)

第二十三条 本規範に定めるもののほか、本規範の実施のための手続その他その執行について必要な細則は、政府機関統一基準で定める。

附則

第一条 内閣官房情報セキュリティセンターは、統一規範に基づいた府省庁の情報セキュリティ対策について必要な範囲で検査し、評価する。

2 内閣官房情報セキュリティセンターは、毎年度前項の評価を取りまとめて情報セキュリティ政策会議に報告し、その概要を公表するものとする。

第二条 情報セキュリティ政策会議は、統一規範決定後一年後を目途として、新たな脅威の発生や府省庁における運用の結果を踏まえて検討し、その結果に基づいて必要な措置を講ずる。

第三条 政府機関の情報セキュリティ対策の強化に関する基本方針（平成17年9月15日情報セキュリティ政策会議決定）は廃止する。

附則（平成26年〇月〇日情報セキュリティ政策会議決定）

第一条 統一規範は、情報セキュリティ政策会議決定後から施行する。

第二条 情報セキュリティ政策会議は、統一規範の実施結果を踏まえ、必要があると認めるときは、その結果に基づいて必要な措置を講ずる。