政府機関等の情報セキュリティ対策のための統一規範（案）

平成 28 年８月 31 日
平成　年　月　日改定
サイバーセキュリティ戦略本部決定

第一章　目的及び適用対象

（目的）

第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十五条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む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組織は、次の各号に掲げるとおりとする。

一　国の行政機関　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百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

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　政府機関等の情報セキュリティ対策のための基本方針

（リスク評価と対策）

第三条　機関等は、自組織の目的等を踏まえ、第十条に定める自己点検の結果、第十一条に定める監査の結果、法に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、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　機関等は、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。

（情報セキュリティ文書）

第四条　機関等は、自組織の特性を踏まえ、基本方針（機関等における情報セキュリティ対策の基本的な方針をいう。以下同じ。）及び対策基準（機関等における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をいう。以下同じ。）を定めなければならない。基本方針及び対策基準（以下「ポリシー」という。）の呼称は機関等で独自に定めることができる。

２　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　対策基準は、別に定める政府機関等の情報セキュリティ対策のための統一基準（以下「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　国の行政機関は、必要に応じて、所管する独立行政法人及び指定法人に対して、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こととする。

５　独立行政法人及び指定法人は、前項の求めに応じることとする。

６　機関等は、前条第一項の評価結果を踏まえ、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　政府機関等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　機関等は、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　機関等は、最高情報セキュリティ責任者１人を置かなければならない。

３　最高情報セキュリティ責任者は、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機関等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、統一基準に定められた自らの担務を、統一基準に定める責任者に担わせることができる。

（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　機関等は、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　機関等は、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定めなければならない。

（教育）

第八条　機関等は、職員等が自覚をもってポリシーに定められた情報セキュリティ対策を実施するよう、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　機関等は、情報セキュリティインシデント（JIS Q 27000:2014 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、適正な体制を構築するとともに、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の可能性を認知した者は、ポリシーに定める報告

窓口に報告しなければならない。
３　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に関して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　機関等は、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　機関等は、対策基準が本規範及び統一基準に準拠し、かつ実際の運用が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　機関等は、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　機関等は、機関等間での情報の提供、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　機関等は、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　機関等は、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　機関等は、機関等間での情報の提供、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　機関等は、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　機関等は、自組織が管理する又は自組織以外の組織から借用している施設等、自組織の管理下にあり、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　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。

２　機関等は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、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　機関等は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。
４　機関等は、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　機関等は、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　機関等は、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　機関等は、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　機関等は、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　機関等は、自組織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　機関等は、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　機関等は、情報システムの利用に際して、情報セキュリティを確保する

ために職員等が行わなければならない必要な措置を定め、実施させなければならない。

（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必要な要件は、統一基準で定める。

附則

政府機関の情報セキュリティ対策のための統一規範（平成 23 年４月 21 日情報セキュリティ政策会議決定）は廃止する。