政府機関等の情報セキュリティ対策の運用等に関する指針（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

１　本指針の目的

本指針は、サイバーセキュリティ基本法（平成 26 年法律第 104 号。以下「法」という。）第 25 条第１項第２号に定める国の行政機関、独立行政法人（独立行政法人通則法（平成 11 年法律第 103 号）第２条第１項に規定する法人をいう。以下同じ。）及び指定法人（法第 13 条に規定する指定法人をいう。以下同じ。）（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の運用に関して、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）における政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）及び政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の案の策定、政府機関等の対策基準策定のためのガイドライン（NISC 決定。以下「対策基準策定ガイドライン」という。）の策定、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の運用並びに複数の機関等で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。以下「基盤となる情報システム」という。）に関する情報セキュリティ対策の運用のために必要な事項を定めるものである。

２　統一基準群の策定

統一基準群は、統一規範、統一基準、本指針及び対策基準策定ガイドラインの総称をいい、統一規範、統一基準及び本指針の原案は、NISC が策定し、サイバーセキュリティ対策推進会議（平成 27 年２月 10 日サイバーセキュリティ戦略本部長決定）を経てサイバーセキュリティ戦略本部において決定する。また、対策基準策定ガイドラインは、国の行政機関と協議の上、NISC において決定する。

なお、NISC は、新たな脅威の発生や機関等における運用の状況を定期的に点検した結果を踏まえ、次の点に留意の上、原案の策定を行う。

(1)　統一規範及び統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策を包含するものとし、責任体制、実施体制及び対策内容について、機関等が準拠できるよう、実状を踏まえるとともに、国際的な基準等との整合性に配慮の上、策定する。統一基準には、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（以下「遵守事項」という。）を規定

する。

(2) 対策基準策定ガイドラインは、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（以下「基本対策事項」という。）を例示するとともに、機関等による対策基準の策定及び実施に際しての考え方等を解説することを目的として策定する。基本対策事項は遵守事項に対応するものであるため、機関等は対策基準策定ガイドラインを参照し、基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要があるものである。

3 独立行政法人及び指定法人の情報セキュリティ対策に係る主務大臣等の責務

(1) 導入・計画

独立行政法人を所管する主務大臣は、独立行政法人通則法（平成 11 年法律第 103 号）第 29 条第１項の規定により指示した同項の中期目標、第 35 条の４第１項の規定により指示した同項の中長期目標又は第 35 条の９第１項の規定により指示した同項の年度目標に、統一基準群に基づいて定め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こととする。指定法人に対しては、個別の根拠法に基づき、当該指定法人を所管する国の行政機関が必要な情報セキュリティ対策についての指導等を実施する。

(2) 評価

独立行政法人を所管する主務大臣は、独立行政法人通則法に基づく業務の実績等に関する評価の際に、情報セキュリティ対策の実施状況に関しても評価を行い、評価結果を公表する。指定法人を所管する国の行政機関は、当該指定法人に対して、個別の根拠法に基づき、情報セキュリティ対策の実施状況に関して評価を行う。

独立行政法人及び指定法人の情報セキュリティ対策に係る評価の結果に関しては、NISC においても確認し、必要に応じてこれら法人を所管する国の行政機関に対して助言等を行う。

4 共通的に使用する情報システムにおける情報セキュリティ対策

基盤となる情報システムについては、これを使用する各機関等の情報システムと連携して運用管理を行うものであることから、各機関等の間での情報セキュリティ対策の遺漏防止を図る必要がある。また、基盤となる情報システムと連携する一部の情報システムにおける情報セキュリティインシデントが他の情報システムに影響を及ぼす可能性等も踏まえ、情報セキュリティマネジメントを適切に実行し、情報システム全体としての情報セキュリティ水準を適切に確保しなければならない。

このため、基盤となる情報システムの整備・運用管理を行う機関等及び基盤となる情報システムと連携する情報システムを管理する機関等（以下「整備・運用管理機関等」という。）は、基盤となる情報システムの運用管理を行う体制を整備するに当たっては、各機関等の責任と役割分担を明確化するとともに、情報セキュリテ

ィ対策を確実かつ迅速に調整・実施できる体制にする必要がある。

また、整備・運用管理機関等は、基盤となる情報システムの情報セキュリティを確保するための方策等について包括的に定めた文書を整備するに当たっては、それぞれのポリシーとの関係について検討し、適切な運用管理が行われるよう、以下の事項等を整理するものとする。

・各機関等の間の責任分界
・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　等

以上の検討・実施に当たっては、各機関等の間での十分な合意形成を図るとともに、情報セキュリティ対策の円滑かつ迅速な実施に支障を来さないように留意する必要がある。

なお、基盤となる情報システムの情報セキュリティ対策を共通的に行うため、基盤となる情報システムを整備し、運用管理を行う機関等は、当該基盤となる情報システムと連携する情報システムを管理する機関等と協議の上、基盤となる情報システムの情報セキュリティについて、各機関等が定めるそれぞれのポリシーの定めにかかわらず、共通的な規程を定めることができるものとする。

附則　政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（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。