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

平成 28 年８月 31 日
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、政府機関について、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 28 年８月 31 日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。）及び政府機関の情報セキュリティ対策のための統一基準（平成 28 年８月 31 日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。）に基づく府省庁対策基準の策定及びその運用等のために必要な事項、並びに独立行政法人等（独立行政法人及び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 13 条に定める指定法人。以下同じ。）における情報セキュリティマネジメント等に関して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、本指針及び府省庁対策基準策定のためのガイドライン（平成 28 年８月 31 日内閣官房内閣サイバーセキュリティセンター。以下「対策基準策定ガイドライン」という。）の総称をいい、統一規範、統一基準及び本指針の原案は、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。）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（以下「戦略本部」という。）において決定する。また、対策基準策定ガイドラインは、府省庁と協議の上、NISC において決定する。

なお、NISC は、新たな脅威の発生や府省庁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、全ての府省庁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、府省庁が準拠できるよう、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。
(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採るべき基本的な対策事項の例示、考え方等を解説することを目的として策定する。

３　府省庁における情報セキュリティマネジメント

(1)　導入・計画

①　府省庁基本方針の策定

府省庁は、情報セキュリティ対策の目的、対象範囲等、情報セキュリティに

対する基本的な考え方を示した府省庁基本方針を定める。

府省庁基本方針の策定に当たっては、対象となる情報、情報システム、組織（者）、場所・区域の範囲及びその境界について、外部委託の観点も含めて明確にするとともに、対象範囲外においては、他の主体により情報セキュリティ対策が講じられていることを確認するなどにより、その境界が妥当であることを確認することが重要である。

なお、府省庁基本方針は、情報セキュリティに対する基本的な方向性を決定付けるものであることから、頻繁に更新される性質のものではないことに留意する必要がある。

② 府省庁対策基準の策定

府省庁は、府省庁基本方針に基づき、統一規範及び統一基準に準拠して府省庁対策基準を定める。府省庁対策基準には、統一基準の規定を遵守するための対策事項について、対策基準策定ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて定めることとする。また、脅威の変化等に迅速に対応するために政府機関共通の情報セキュリティ対策が個別に決定されている場合にはそれを反映する。

③ 対策推進計画の策定

府省庁は、最高情報セキュリティ責任者の指揮の下、情報セキュリティに係るリスク評価の結果を踏まえ、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。）を策定する。対策推進計画は、教育訓練、情報システムに対する技術的な対策を含め、府省庁における情報セキュリティに関する一連の取組をふ瞰できるものとする。

(2) 運用

府省庁は、対策推進計画に基づき、行政事務従事者に対する教育訓練を実施し、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。）の浸透を図るとともに、情報システムに対する技術的な対策を強化するなど、情報セキュリティに関する取組を実施する。

(3) 点検・見直し

府省庁は、対策推進計画に基づく取組について、年度ごとに実施状況を把握し点検するとともに、必要に応じて見直しや改善を行う。

府省庁は、情報セキュリティ対策について、その適正性を確保するため、情報セキュリティ対策の実施状況、効果及び対策実施の結果としての情報セキュリティの状態を点検することが必要である。

なお、点検は客観的な視点から行なわれていると認められることが重要であり、このため点検対象の部門や者から独立した組織又は部門による監査を含めることが必要である。

点検の結果、求める情報セキュリティ水準が達成されていないと判断された場合又は情報セキュリティ対策の実施状況や効果が不十分であると判断された場合は、それについて、再発防止を考慮した改善を実施しなければならない。改善においては、府省庁対策基準等の改正、教育による府省庁対策基準等の周知徹底、情報システムや機器の更新、情報セキュリティの重要性に係る啓発等の措置を講ずることとなる。改善措置の結果については、意図した目的が達成されていることを確認する必要がある。

最高情報セキュリティ責任者は、対策推進計画に照らして自府省庁の情報セキュリティマネジメントの状況を総合的に評価し、情報セキュリティに係る取組をより一層推進するため、今後の情報セキュリティマネジメントの方向性、資源配分の見直しを行う。

また、府省庁は、本部監査（法第 25 条第１項第２号に基づく監査をいう。以下同じ。）において助言された事項についても、優先順位を検討した上で、必要に応じて上記(1)から(3)のプロセスに則り情報セキュリティ対策の見直しや改善を行う。

４　独立行政法人等における情報セキュリティマネジメント

(1)　導入・計画

法第 25 条第１項第２号に基づき作成する独立行政法人等におけるサイバーセキュリティに関する対策の基準は統一基準群を指すものとする。独立行政法人等は、３(1)に掲げる府省庁における情報セキュリティマネジメントの導入及び計画を踏まえ、対策基準等（以下「独法等ポリシー」という。）を策定する。

また、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、対策基準等に基づき、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。指定法人においては、個別の根拠法に基づき、所管府省庁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)　運用

独立行政法人等は、３(2)に掲げる府省庁における情報セキュリティマネジメントの運用を踏まえ、独法等ポリシーの浸透を図るとともに、情報セキュリティに関する取組を実施する。

また、独立行政法人等は、被害の拡大防止等の観点から、情報セキュリティインシデントに関する情報を迅速かつ有効に活用するため、所管府省庁との間の情報連絡体制を構築する。情報セキュリティインシデント対処の際には経営判断が求められる場合もあることから、この情報連絡体制は、実務者クラスと並行して、所管府省庁管理職及び当該法人役員クラスにも情報セキュリティインシデントに関する情報及び対処状況が周知される体制とする。所管府省庁は、情報共有体

制を通じて、情報セキュリティインシデント発生時の NISC への情報提供、NISC からの注意喚起等、双方向の円滑な情報連絡を図る。

(3)　点検・見直し

独立行政法人等は、３(3)に掲げる府省庁における情報セキュリティマネジメントの点検及び見直しを踏まえ、年度ごとに実施状況を把握し点検するとともに、必要に応じて見直しや改善を行う。

また、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。府省庁は、所管の指定法人に対しても、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。係る評価結果に関しては、NISC においても確認し、必要に応じて所管府省庁に対して助言等を行う。

また、独立行政法人等は、本部監査において助言された事項についても、優先順位を検討した上で、必要に応じて上記(1)から(3)のプロセスに則り情報セキュリティ対策の見直しや改善を行う。

５　情報セキュリティ対策の改善の在り方

(1)　府省庁への情報セキュリティ対策の点検

情報セキュリティ対策は、一過性のものではなく、継続的な取組が必要であることから、客観的に比較検証することが可能な判断基準による点検を実施することが重要である。

情報セキュリティ対策の実施状況の点検は、府省庁の責任において行われることが原則であるが、政府機関全体として、これを更に効果的かつ効率的に実施するため、戦略本部及び NISC は、統一基準群に基づき府省庁が定める情報セキュリティ関係規程等の整備状況及び対策の実施状況並びに府省庁の情報セキュリティマネジメントの状況について、総合的、客観的及び統一的な視点で、定期的に、又は必要に応じて点検及び本部監査を実施する。

(2)　独立行政法人等の情報セキュリティ対策の監査

独立行政法人等は、本部監査を受けるとともに、監査結果を所管府省庁に報告する。

(3)　監査結果の検証及び公表

戦略本部は、(1)及び(2)の監査結果により情報セキュリティ対策の実施等に係る課題を把握し、それを踏まえた府省庁及び独立行政法人等（以下「政府機関等」という。）の全体の取組の方向性を取りまとめ、その概要を公表するものとする。

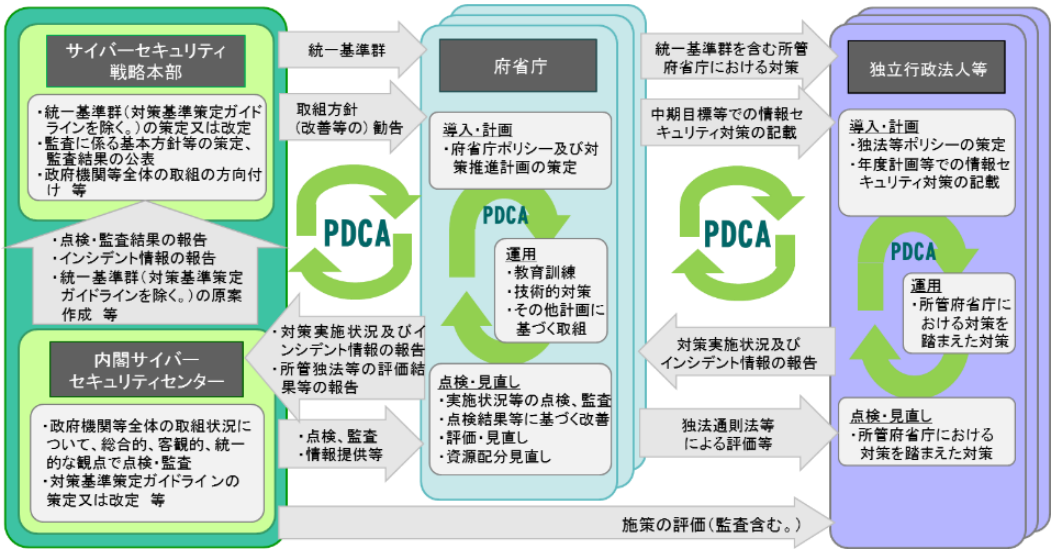

図　政府機関等における情報セキュリティマネジメントの全体像

6　情報セキュリティ対策の進め方

(1)　基本原則及び最高情報セキュリティ責任者の指揮と推進体制の確立

政府機関等の各機関における情報セキュリティの確保については、国民、企業等からの情報セキュリティ確保に関する要求や期待を踏まえた上で、自らが取り扱う情報の管理に責任を持ち、それぞれの業務や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則である。

そのためには、最高情報セキュリティ責任者は各機関における情報セキュリティ対策の推進を指揮し、その方向性を明確化するとともに、情報セキュリティ対策に必要な人員・予算等の資源配分の方針を決定する。

また、情報セキュリティ対策を効率的かつ実用的に推進するためには、取り扱う情報や業務、組織等の特性を踏まえる必要があることから、各機関において部門横断的に取り組むため、情報セキュリティ対策の推進のための組織・体制を確立する。

府省庁は、所掌の業務において機微な個人情報を含む多くの重要情報を扱っており、その適切な管理を国民から期待されていることを行政事務従事者に認識させるとともに、このような認識を日頃から所管の独立行政法人等とも共有しつつ、監督等を行っていくことが重要である。

(2)　情報セキュリティ対策の実施

政府機関等は、策定した府省庁ポリシー又は独法等ポリシーの適切な運用を通じて、一定のセキュリティ水準を確保する。また、重要な業務、情報等に対しては詳細にリスクを把握した上で情報セキュリティ対策を講ずる。

その際は、過度のセキュリティ対策の実施によってルールを潜脱する行為を招かないよう、業務要件や業務フローを考慮した上で、業務の効率・効果を高める

形で情報セキュリティ対策が講じられるようにすることが重要である。

また、政府機関等は、リスクを把握し、情報セキュリティ対策を実施する手法について、政府機関等において適用されているガイドライン等が存在する場合は、それらに沿って実施することが求められる

(3)　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

他の機関と共通的に使用する情報システム（一つの機関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。）については、これを使用する各機関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を整備・運用管理を行う機関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（以下「整備・運用管理機関」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、それぞれの府省庁ポリシー又は独法等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、各機関が定めるそれぞれの府省庁ポリシー又は独法等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。

(4)　情報セキュリティインシデントの情報共有

情報セキュリティインシデントに対し、政府機関等全体として迅速かつ的確に対処するためには、情報セキュリティインシデントに関する情報が組織内外の関係部門と適時・適切に共有されることが重要である。

そのため、府省庁は、当該府省庁又は所管する独立行政法人等における情報セキュリティインシデントの認知時には、当該情報セキュリティインシデントに係る情報を速やかに NISC に連絡するとともに、平時においても、収集した情報セキュリティインシデントに関する情報を NISC に連絡する。

独立行政法人等は、情報セキュリティインシデントについて、所管府省庁との間で緊密な情報共有を行う。

NISC は、平時から府省庁や外部の関係機関との情報共有の結節点となり、収集・集約された情報を情報セキュリティインシデントによる被害の未然防止又は拡大防止、応急措置・復旧のための措置及び再発防止に活用するため、情報元の同意を得た上で、府省庁に対して積極的な情報提供を行う。

(5)　情報セキュリティインシデントへの対処

府省庁は、情報セキュリティインシデントの認知時には、自らが設置した CSIRT（Computer Security Incident Response Team）を中心として、早急にその状況を確認し、被害の拡大防止及び応急措置・復旧のための措置を講ずる。

独立行政法人等も、情報セキュリティインシデントの認知時には府省庁と同様に、情報セキュリティインシデントへの対処を行う。

NISC は、情報セキュリティインシデントへの政府一体となった対応の中核となる機関として、府省庁間の連携・調整を行う。また、CSIRT の能力向上の支援等、府省庁へ技術的な支援及び助言を行い、府省庁の求めに応じて情報セキュリティ緊急支援チーム（Cyber Incident Mobile Assistance Team（CYMAT））による支援を行う。

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。