

情報セキュリティ政策の評価等の実施方針

2011年7月8日

内閣官房情報セキュリティセンター（NISC）

目次

はじめに.....	3
情報セキュリティ政策に係る PDCA サイクル.....	4
（ 1 ） 計画（Plan）段階.....	4
（ 2 ） 実施（Do）段階.....	4
（ 3 ） 点検（Check）段階.....	4
（ 4 ） 改善処置（Act）段階.....	5
評価等の実施方針.....	6
1 枠組み.....	6
（ 1 ） 評価指標に基づく評価等の実施.....	6
（ 2 ） 評価指標に基づくデータの把握及び評価の実施等.....	6
（ 3 ） 補完調査の実施.....	6
（ 4 ） 分析.....	7
（ 5 ） 報告.....	7
（ 6 ） 持続的な改善.....	7
（ 7 ） 年度計画等への反映.....	7
2 考え方.....	7
（ 1 ） 評価等の視点.....	7
（ 2 ） 評価等の対象.....	8
（ 3 ） 評価等の方法.....	8
（ 4 ） 政府機関等の基盤強化における評価等の方法.....	9

別添 情報セキュリティ政策領域における評価に当たり考慮すべき状況

はじめに

我が国の情報セキュリティ政策については、2006年度から2008年度までは、「第1次情報セキュリティ基本計画」¹により、2009年度からは、同計画を継続・発展させることとした「第2次情報セキュリティ基本計画」²に基づき、官民の各主体によって推進されてきた。

同計画では、計画の策定から実施、評価、評価結果を次期計画策定に反映させる基本的なサイクルと、計画期間の各年度に年度計画を定め、その評価結果を次年度計画に反映させる単年度のサイクルによって情報セキュリティ政策の持続的改善を図るPDCAサイクル³の構築を行ってきた。

こうした取組を推進する中、2009年7月の米韓における大規模サイバー攻撃事態の発生等により情報セキュリティ上の脅威が安全保障・危機管理上の問題となり得ることが明らかとなり、また、情報セキュリティ上のリスクが多様化・高度化・複雑化しそれまでの取組では情報セキュリティの確保が困難な状況が発生してきたことを受け、新たに、2010年度から2013年度を対象とした中長期計画である「国民を守る情報セキュリティ戦略」⁴（以下「戦略」という。）が策定された。

今後の取組においても、戦略策定の契機となった脅威や社会・環境の変化に的確に対応し、また、戦略等の評価を定期的に行い、必要に応じて取組内容の見直しを行うため、PDCAサイクルによる持続的改善構造を維持する必要がある。

本文書は、情報セキュリティ政策のPDCAサイクルの基本的な考え方、評価の枠組み及び方法等について取りまとめ、「すべての国民が情報通信技術を安心して利用できる環境の実現に向けた取組の評価等及び合理性を持った持続的改善の推進について」⁵に基づき、内閣官房情報セキュリティセンター（以下「NISC」という。）及び各府省庁が情報セキュリティ政策の評価等と持続的改善のための様々な取組を実施していく際に活用するためのものである。

¹ 2006年2月2日 情報セキュリティ政策会議決定。

² 2009年2月3日 情報セキュリティ政策会議決定。

³ 計画（Plan）、実施（Do）、点検（Check）、改善処置（Act）の各々の段階を経て、改めて計画（Plan）に戻る自律的な政策推進サイクルのこと。

⁴ 2010年5月11日 情報セキュリティ政策会議決定。

⁵ 2011年7月8日 情報セキュリティ政策会議決定。

情報セキュリティ政策に係る PDCA サイクル

情報セキュリティに関する取組は、情報通信技術の利用・活用のあり方や取り巻くリスクが刻々と変化することからも、持続的な改善構造を備えることにより、適時適切に見直されることが重要である。この点を踏まえ、中長期計画は基本的な PDCA サイクルを4か年として設計されており、計画期間中においても定期的に評価を行い必要に応じ見直しを行うこととされている。また、中長期計画を具体的に実行していくため、単年度の施策実施プログラムである年度計画（「情報セキュリティ 20XX」）が策定されているところ、その実施状況を社会情勢の変化とともに評価し、この評価結果を踏まえて翌年度の計画を策定するという単年度の PDCA サイクル構造を備える必要がある。

（１）計画（Plan）段階

中長期計画である「戦略」、個別設計図である「政府機関の情報セキュリティ対策のための統一基準群」⁶（以下「政府機関統一基準群」という。）、「重要インフラの情報セキュリティ対策に係る第2次行動計画」⁷、年度計画である「情報セキュリティ 20XX」等の策定が計画段階（P）⁸に当たる。

情報セキュリティ対策を取り巻く環境やリスクは刻々と変化を続けていることから、年度計画や中長期計画の策定に当たっては、そのような変化を的確に把握しておく必要がある。

（２）実施（Do）段階

中長期計画において示される取組、年度計画において示される具体的な取組の着実な推進が実施段階（D）に当たる。

（３）点検（Check）段階

中長期計画で設定された実現すべき成果目標にどの程度到達できたか、すなわち、様々な脅威に適切に対処することが可能となっているかどうか、社会・環境の変化に的確に対応できているかどうかなどといったことについて検証することが点検段階（C）に当たる。

⁶ 「政府機関の情報セキュリティ対策のための統一基準」の初版は、2005年12月13日 情報セキュリティ政策会議決定、現行は、「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」2011年4月21日 情報セキュリティ政策会議決定。また、「政府機関の情報セキュリティ対策のための統一基準群」とは、「政府機関の情報セキュリティ対策のための統一規範」、「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」、「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」を指す。

⁷ 2009年2月3日 情報セキュリティ政策会議決定。

⁸ 以下、PDCA サイクルの各段階について、計画段階（P）、実施段階（D）、点検段階（C）、改善処置段階（A）というように、PDCA サイクルそれぞれの頭文字を括弧内に標記する形で示す。

そのため、検証時点で明らかとなった脅威や社会・環境の変化を把握した上で、状況把握に有益な既存のデータ等（以下「評価指標」という。）の活用を原則とし、必要に応じて補完的な調査（以下「補完調査」という。）等を行い、新たに対応が必要な事項、改善が必要な事項等を抽出する。

（４）改善処置（Act）段階

点検段階（C）の結果を踏まえ、必要な取組の改善を図っていくことが改善処置段階（A）に当たる。点検段階（C）段階で抽出した事項を次の計画へ反映するように努める。

評価等の実施方針

1 枠組み

ここでは、情報セキュリティ政策のPDCAサイクルの点検段階（C）の具体的な内容のうち、評価等の枠組みに関して記述する。

以下の取組は、「すべての国民が情報通信技術を安心して利用できる環境の実現に向けた取組の評価等及び合理性を持った持続的改善の推進について」に基づき、NISCが主体的に推進するものとし、各府省庁はこれに協力するものとする。

（1）評価指標に基づく評価等の実施

中長期計画は、計画段階（P）において実現すべき成果目標を念頭に置き、実施段階（D）においてはその目標に到達すべく具体的な取組を推進するという形で設計されている。

このため、評価指標の設定に当たっては、実現すべき成果目標、すなわち、脅威と社会・環境の変化への的確な対応という観点に着目することが必要である（アウトカム指標）。また、中長期計画が上記のように設計されていることにかんがみ、適切な評価を実施するためには、年度計画において示される取組の推進状況を把握することが必要である（アウトプット指標）。

（2）評価指標に基づくデータの把握及び評価の実施等

NISCは、点検段階（C）において、各府省庁の協力を得て、評価指標に基づきデータを把握し、これに基づいて評価を実施する。

また、NISCは、効率的かつ実効的に評価等を行うため、評価手法の改善に努めるとともに、情報通信技術の利用・活用のあり方や取り巻くリスクは刻々と変化することから、各府省庁の協力を得て、必要な評価指標の見直しを行う。ただし、評価指標に基づく評価は、データ等の経年的な変化を見ることにも大きな意味があることから、設定した評価指標の見直しの際には、経年的な比較が実施可能であることに留意する必要がある。

（3）補完調査の実施

技術的に設定が可能な評価指標だけでは、必要なデータ等をすべて把握できるとは言い難い。このような場合においては、評価指標に基づく評価を実施することが困難な事項に関する状況を把握するため、補完できるデータを参照することも含めて、補完調査を実施することが必要となる。

このため、NISCは、調査テーマ・調査項目に関係の深い府省庁の協力を得て、補完調査を実施する。その実施に当たっては、取組を行う情報セキュリティ政策の性質が各々異なること、これらを取り巻く環境が異なること等を十分に考慮し、柔軟に対応を行うことが必要である。

(4) 分析

評価指標に基づいて収集したデータ、補完調査によって把握した現状等については、データや事実関係、またはそれらの変動だけからでは、その背景が十分に見えない可能性がある。

このような場合については、NISCは、把握したデータ等と具体的な取組との「隙間」を埋めるため、必要に応じて、必要な分析を行う。

(5) 報告

NISCは、前述のような取組の結果、評価指標に基づくデータ、評価の結果、補完調査の結果及び分析の結果について、情報セキュリティ政策会議に報告を行う。

(6) 持続的な改善

情報セキュリティ政策会議は、NISCからの評価等の結果に関する報告を踏まえ、「取組が不十分と認められる事項」、「更なる取組改善が期待できる事項」及び「新たに明らかになった克服や解決が必要となる事項」に対処するために必要な取組を推進する。具体的な例としては、政府機関統一基準群の活用を通じて各府省庁の効果的な対応を促すこと、各省庁の情報セキュリティ対策に係る取組を広く周知するための情報発信等を行うこと、各府省庁が情報セキュリティ政策を検討・実施する上で参考となる情報提供等を行うことなどが挙げられる。

(7) 年度計画等への反映

持続的な改善の仕組みを実効あるものとするためには、点検結果を踏まえ、必要となる対策を次年度の計画段階（P）に具体的に反映することが必要不可欠となる。

このため、情報セキュリティ政策会議は、NISCからの評価等の結果に関する報告を踏まえ、情報セキュリティ対策を推進していくために必要な施策を年度計画及び中長期計画に反映するよう努める。

2 考え方

(1) 評価等の視点

中長期計画では、実現すべき成果目標に到達するよう具体的な取組を推進するという形で設計されている。

そのため評価等の視点としては、中長期計画に示された実現すべき成果目標、すなわち、様々な脅威に適切に対処することが可能となっているかどうか、社会・環境の変化に的確に対応できているかどうかなどについて、年度計画において示される取組の推進状況を把握しつつ、検証するという視点が重要となる

また、情報セキュリティ政策は社会の現状を踏まえて企画・立案し、社会に対してプラスの影響を及ぼすことを意図して実施するものであることから、情報セキュリティに係る様々な動向（当該年度の情報セキュリティ政策の取組の結果によるもの及びそうでないも

のの双方を含む)を測るという視点も必要である。

(2) 評価等の対象

評価等は、中長期計画及び年度計画の見直しに資することを目的として実施するものであるところ、情報セキュリティ上のリスクが多様化・高度化・複雑化し、また、情報セキュリティを取り巻く環境が刻一刻と変化する中、これらに迅速かつ的確に対応するためには、取組の詳細にわたる部分についてのみではない俯瞰的な改善に備えておく必要がある。したがって、評価等は、中長期計画及び年度計画に基づき設定した情報セキュリティ政策領域(表1)を対象として、総括的に実施するものとする。

表1 情報セキュリティ政策領域⁹

1	大規模サイバー攻撃事態への対処態勢の整備等
2	新たな環境変化に対応した情報セキュリティ基盤の強化
(1)	国民生活を守る情報セキュリティ基盤の強化
	政府機関等の基盤強化
	重要インフラの基盤強化
	その他の基盤強化
(2)	国民・利用者保護の強化
	普及・啓発活動の充実・強化
	個人情報保護の推進
	サイバー犯罪に対する態勢の強化
(3)	国際連携の強化
(4)	技術戦略の推進等
	情報セキュリティ関連の研究開発の戦略的推進等
	情報セキュリティ人材の育成
(5)	情報セキュリティに関する制度整備
(6)	その他

(3) 評価等の方法

年度計画に基づく取組の進捗状況及び別添「情報セキュリティ政策領域における評価に当たり考慮すべき状況」に示す評価指標に基づき、データを把握しつつ評価を実施する。

ただし、評価等の実施に当たっては、主体の特性に応じた検討が必要であり、具体的な例としては、企業・個人に係る情報セキュリティ政策の領域については、環境整備等の間接的な働きかけを行うことが政府の施策の中心であること、他の主体に係る取組を始めと

⁹ 本表は、2010年度の情報セキュリティ政策領域に準拠して策定したものであり、2011年3月11日に発生した東日本大震災を踏まえた情報セキュリティ政策等については、今後の見直しにより評価対象としていく。

する多様な要因の影響を受ける可能性が高いことなどを踏まえ、主体全体としての評価等を総合的な視点から行うことが必要となる。

また、情報セキュリティ人材の育成や国際連携の強化など、評価指標を設定することが必ずしも容易ではない主体も存在する。そのため、これらの情報セキュリティ領域については、必要に応じて政府機関をはじめとする各主体による調査を実施し、これをもって点検段階（C）の仕組みとして活用していくこととする。

（４）政府機関等の基盤強化における評価等の方法

情報セキュリティ政策会議は、これまでの政府機関の情報セキュリティ対策への取組について、実施状況などを数次にわたり精査し、その結果を公表し、政府機関の取組を促してきた。

情報セキュリティ政策会議は、これらの成果を踏まえ、情報セキュリティガバナンスの確立に向けた組織・体制の強化を図ることを目的に、情報セキュリティ政策会議 第24回会合（2010年7月22日）において、各政府機関の「最高情報セキュリティ責任者」（以下「CISO」という。）相互の緊密な連携の下、政府機関における情報セキュリティ対策の推進を図る「情報セキュリティ対策推進会議（最高情報セキュリティ責任者等連絡会議）」（以下「CISO等連絡会議」という。）を設置したところである。

また、政府全体としてのPDCAサイクルの定着と浸透を確実なものとするため、情報セキュリティ政策会議の下に設置された「情報セキュリティ報告書専門委員会」¹⁰において、2009年9月11日に「情報セキュリティ報告書専門委員会報告書」を策定しており、各政府機関においては、当該報告書に基づき、「情報セキュリティに係る年次報告書」（以下「情報セキュリティ報告書」という。）を作成することとなった。ここで、各政府機関において作成された情報セキュリティ報告書については、CISO等連絡会議の下に設置された「最高情報セキュリティアドバイザー等連絡会議」での審議を経て、CISO等連絡会議に報告を行うこととしている。

さらに、NISCにおいて、各政府機関の情報セキュリティ対策の実施状況に係る評価等を行い、「政府機関における情報セキュリティに係る年次報告」として取りまとめ、CISO等連絡会議において決定を行い、「情報セキュリティ政策会議」に報告することとなっている。本報告は、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすものと位置づけられ、情報セキュリティの維持・確保にも配慮しつつ公表していくこととしている。

このため、政府機関の評価等については、「政府機関における情報セキュリティ報告書に係る年次報告書」にて実施することとする。

¹⁰ 2009年2月3日 情報セキュリティ政策会議決定。

別添

情報セキュリティ政策領域における評価に当たり考慮すべき状況

情報セキュリティ政策分野	情報セキュリティ政策内容	評価に当たり考慮すべき状況
1 大規模サイバー攻撃事態への対処態勢の整備等	2009年7月に米韓において発生したような大規模なサイバー攻撃事態が、今後我が国においても発生する可能性があること等を踏まえ、国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれのあるサイバー攻撃事態（大規模サイバー攻撃事態）の発生時における対処態勢の整備、及び「重要インフラの情報セキュリティ対策に係る第2次行動計画」等に基づく官民情報共有体制を活用した平素からの情報収集・共有体制の強化を図る。取組の推進に当たっては、未然防止等の観点から平素からの取組を行う部局と、大規模サイバー攻撃事態発生時の対処を行う部局との十分な連携を図り、総合的な対処に努める。	<ul style="list-style-type: none"> ・ 大規模サイバー攻撃事態等発生時の初動対処に係る訓練等の実施状況 ・ サイバー攻撃による被害発生、拡大の防止のための情報集約・共有等の実施状況 ・ サイバー攻撃の主体・方法等に関する情報収集・分析の実施状況 ・ サイバー攻撃に対する各種訓練及び研修の実施状況 ・ 官民連携の活動状況及び諸外国関係機関との連携状況
2 新たな環境変化に対応した情報セキュリティ政策の強化	<p>(1)国民生活を守る情報セキュリティ基盤の強化</p> <p>政府機関等の基盤強化</p>	<p><u>最高情報セキュリティ責任者(CISO)の機能強化</u> 最高情報セキュリティ責任者(CISO)連絡会議の設置や最高情報セキュリティ・アドバイザー連絡会議の設置等を通じて、各省庁のCISOの機能強化を図る。また、各府省庁のCISOが情報セキュリティ報告書を作成し、公表を行うことにより、自ら問題意識を持って情報セキュリティ対策の改善を図る。</p> <p><u>政府横断的な情報収集・分析システム(GSOC)の充実・強化</u> 2008年度に本格運用を開始し政府機関情報システムの24時間監視を行っているGSOCについて、緊急時における連絡体制や関係連携機関との連携強化等による情報収集能力、攻撃等の分析・解析能力強化等により、政府全体としてサイバー攻撃等に対する緊急対応能力を向上させる。</p> <p><u>政府機関情報システムの効率的・継続的な情報セキュリティ対策の向上</u> 政府機関のサーバ集約化等を通じて、情報システムのスリム化や運用効率化を一層推進し、情報セキュリティ対策の向上・効率化を図る。また、各省庁の情報セキュリティ対策の評価を通じて、取組の持続的な改善を図る。</p>
		<ul style="list-style-type: none"> ・ 情報セキュリティ対策推進会議(CISO等連絡会議)の審議状況 ・ 最高情報セキュリティアドバイザー等連絡会議の審議状況 ・ 各府省庁における情報セキュリティ報告書の作成、公表状況 ・ サイバー攻撃に対する対応状況 ・ サーバ集約化計画(公開ウェブサーバ及びメールサーバ)の進捗状況 ・ 重点検査の検査結果 ・ 対策実施状況の検査結果 ・ 政府機関における情報セキュリティ教育の実施状況 ・ 「中央省庁における情報システム運用継続計画ガイドライン」の策定と、各府省庁での計画策定及び運用の状況 ・ 電子メール利用における送信ドメイン認証技術導入の進捗状況

情報セキュリティ政策分野	情報セキュリティ政策内容	評価に当たり考慮すべき状況
	<p><u>政府機関における安全な暗号利用の推進</u> 政府機関で使われている電子政府推奨暗号について、移行指針に従って暗号の着実な移行を進める。また、電子政府推奨暗号の安全性を継続的に監視・調査し、安全性が低下した暗号については速やかに代替となる暗号への移行を進めるための計画を策定するとともに、急激な安全性の低下に備え、あらかじめ緊急避難的な対応(コンティンジェンシープラン)を検討する。</p>	<ul style="list-style-type: none"> ・ 移行指針に規定する要件への適合状況 ・ 緊急避難的な対応(コンティンジェンシープラン)の策定状況 ・ 対策実施状況の検査結果
	<p><u>クラウドコンピューティング技術における情報セキュリティの確保等</u> 情報システムの統合・集約化等を可能とするクラウドコンピューティング技術について、電子行政へ効率的に活用するため必要となる情報セキュリティ確保方策を検討する。 また、先進的なセキュリティ対策事例を踏まえ、政府機関においてもテレワークの環境整備を推進する。</p>	<ul style="list-style-type: none"> ・ 政府機関統一基準群の改定状況(マニュアル類の整備状況を含む) ・ 総務省による「政府共通プラットフォームのセキュリティポリシー」の策定状況
	<p><u>政府機関の情報セキュリティ対策のための統一基準の見直し</u> 現行の政府機関統一基準の定着を図るとともに、情報通信技術や環境の変化を踏まえ、政府機関統一基準の見直しを適時に行い、新たな情報セキュリティ上の脅威に対応する。</p>	<ul style="list-style-type: none"> ・ 政府機関統一基準群の改定状況(マニュアル類の整備状況を含む) ・ 関係団体との連携状況
	<p><u>政府機関情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築</u> 情報システムに係る政府調達について、企画段階から情報セキュリティ対策を適切に組み込む方策を検討し、情報システムに組み込むべき情報セキュリティ要件を定める。 また、情報セキュリティに係る評価・認証取得が必要となる情報セキュリティ要件の明確化を図ること等により、当該評価・認証を受けた製品の活用が促進されるよう取り組む。</p>	<ul style="list-style-type: none"> ・ 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定と、各府省庁での普及・活用状況 ・ 「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の策定と、各府省庁での実施状況 ・ 対策実施状況の検査結果
	<p><u>社会保障・税の共通番号制に対応した情報セキュリティ対策の検討</u> 社会保障・税の共通番号制の検討に際し、プライバシーポリシーの下で適切な情報セキュリティ対策が講じられるよう、課題の抽出及び解決方策の検討を行う。</p>	<ul style="list-style-type: none"> ・ 社会保障・税の共通番号制に係る検討会等における情報セキュリティ対策の検討状況
	<p><u>地方公共団体、独立行政法人等における情報セキュリティ対策の促進</u> 政府機関統一基準等の見直し等を行うとともに、地方公共団体、独立行政法人等における情報セキュリティ対策の一層の推進を図る。</p>	<ul style="list-style-type: none"> ・ 「独立行政法人等の情報セキュリティ対策の現状調査」の検査結果

情報セキュリティ政策分野	情報セキュリティ政策内容	評価に当たり考慮すべき状況
	<p>重要インフラの基盤強化</p> <p>重要インフラの関係主体は、「重要インフラの情報セキュリティ対策に係る第2次行動計画」に基づいて、重要インフラサービスの維持に努め、また、IT障害発生時の迅速な復旧等を確保することに努めることとする。これに加え、最近の環境変化を踏まえ、国民生活に重大な影響を及ぼすおそれのある重要インフラに対する情報セキュリティ上の脅威に的確に対応する。</p> <p>(「分野横断的な官民連携体制」の強化)</p> <p>各重要インフラサービスの情報通信技術に対する依存性が高まり、重要インフラサービスにおける情報セキュリティ上の脅威も高度化、多様化していること等を踏まえ、官民の役割分担を明確にした上で、官民の緊密な連携の下、重要インフラ分野の情報セキュリティ対策を強化するため、以下の事項に重点的に取り組む。</p> <ul style="list-style-type: none"> ・ 情報共有体制の強化 ・ 「セクターカウンシル」の活動促進 ・ 「安全基準等」の整備浸透 ・ 重要インフラ防護対策の向上 ・ 事業継続計画（BCP）の充実 ・ 重要インフラ分野における国際連携の推進 	<ul style="list-style-type: none"> ・ 重要インフラ事業者等の取組の検証については、検証レベルを逸脱したIT障害等の発生状況を把握 ・ 政府機関等による施策の検証については、安全基準等の整備及び浸透状況を調査 ・ 情報共有体制については、共有情報の動向を調査 ・ 共通脅威分析については、分析に協力した重要インフラ事業者等の意向を調査 ・ 分野横断的演習については、参加規模と参加者の意向を調査 ・ 環境変化への対応については、情報発信やリスクコミュニケーションの現状を把握
	<p>その他の基盤強化</p> <p>マルウェア対策等の充実・強化等マルウェアへの感染対策等を強化するため、情報セキュリティインシデントへの対応能力の維持・向上や利用者への普及・啓発といったコンピュータ等の情報セキュリティ対策を強化するとともに、情報セキュリティ脅威の収集解析システム等の充実や、利用者・ISP9等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。</p> <p>また、マルウェア対策としての検体解析等を行う際のリバースエンジニアリングやダウンロードの適法性を明確化するための措置を速やかに講じる。さらに、脆弱性関連情報の速やかな流通により、不正アクセス等の未然防止に引き続き取り組む。</p> <p>クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化クラウドコンピューティングを利用したサービスを構築・運用・利用するための情報セキュリティ要件に関するガイドライン、クラウドコンピューティング技術の適用が見込まれる分野ごとの情報の取扱い等に関するガイドライン等を検討、策定する。</p> <p>IPv6 対応に関する情報セキュリティ確保方策</p> <p>IPv6 対応における情報セキュリティ上の課題に適切に対応するため、検証環境の活用等により、具体的な情報セキュリティ課題の抽出や人材育成等を実施し、円滑な移行を図る。</p>	<ul style="list-style-type: none"> ・ インシデント報告関連件数（JPCERT/CC インシデント報告対応レポート：JPCERT/CC） ・ 安全なサーバ数（ICT 基盤に関する国際比較調査：総務省） ・ コンピュータウイルス・不正アクセスの届出状況（情報処理推進機構） ・ 脆弱性関連情報の届出状況（情報処理推進機構） ・ SaaS 利用に伴う外部への支払い費用（情報処理実態調査：経済産業省） ・ SaaS 利用に関する SLA の状況（情報処理実態調査：経済産業省） ・ クラウドサービスの利用状況（通信利用動向調査：総務省） ・ クラウドサービスを利用しない理由（通信利用動向調査：総務省） ・ IPv6 普及・高度化推進協議会における検討・推進状況

情報セキュリティ政策分野		情報セキュリティ政策内容	評価に当たり考慮すべき状況
		<p><u>情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策</u> 情報家電、モバイル端末、電子タグ、センサー等あらゆるものがネットワークに繋がった場合の情報セキュリティの確保方策として、開発者に対する検証ツールや安全性評価体制の整備等の環境整備・技術課題の解決を図るとともに新たな利用指針等を検討する。</p>	<ul style="list-style-type: none"> 情報セキュリティ技術の整理状況とマイルストーンの進捗及び報告書の作成状況
		<p><u>医療、教育分野等における情報セキュリティ確保方策</u> 医療、教育分野等において、医療・教育機関、国民等が安全・安心に情報通信技術を活用するためのガイドラインの充実等情報セキュリティ対策の推進方策について検討する。</p>	<ul style="list-style-type: none"> SaaS 利用に伴う外部への支払い費用（情報処理実態調査：経済産業省） SaaS 利用に関する SLA の状況（情報処理実態調査：経済産業省） クラウドサービスの利用状況（通信利用動向調査：総務省） クラウドサービスの利用を利用しない理由（通信利用動向調査：総務省）
		<p><u>中小企業に対する情報セキュリティ対策支援</u> 中小企業に対し、高度な情報セキュリティが確保された戦略的な情報通信技術投資を促進するための環境整備や、独立行政法人や関係機関等を活用し、情報セキュリティに係る情報提供、相談窓口の提供等の支援を行う。</p>	<ul style="list-style-type: none"> SaaS 利用に伴う外部への支払い費用（情報処理実態調査：経済産業省） SaaS 利用に関する SLA の状況（情報処理実態調査：経済産業省） クラウドサービスの利用状況（通信利用動向調査：総務省） クラウドサービスを利用しない理由（通信利用動向調査：総務省） IPA 中小企業情報セキュリティセミナー開催状況（情報処理推進機構）
		<p><u>安全な電子商取引の推進</u> クレジットカード情報等の保護のため、国際標準を踏まえた情報セキュリティ対策を推進し、電子商取引を行うウェブサイトについて、情報セキュリティ基準の策定やその準拠を推進するとともに、新たな情報漏えい防止対策等を検討する。</p>	<ul style="list-style-type: none"> BtoB EC（企業間電子取引）市場規模について（我が国情報経済社会における基盤整備：経済産業省） BtoC EC（消費者向け電子商取引）市場規模について（我が国情報経済社会における基盤整備：経済産業省）
		<p><u>知的財産保護の推進</u> 企業等の知的財産を適切に保護するため、「知的財産推進計画 2010」（2010年5月策定）に基づき、インターネット上の著作権侵害コンテンツ対策の推進、模倣品・海賊版拡散防止条約（ACTA）交渉の妥結を通じ、世界に知的財産保護の輪を広げる。</p>	<ul style="list-style-type: none"> 「知的財産推進計画」の進捗状況（内閣官房）
内閣官房情報セキュリティセンターの機能強化	<p><u>NISC の総合調整機能の強化</u> NISC において、情報セキュリティに関する高度な情報収集や分析機能の強化を実施し、専門性の向上を図るとともに、官民連携を強化する。</p>	<ul style="list-style-type: none"> 情報セキュリティ専門家の登用及び活用状況 関係府省庁との連携状況 	

情報セキュリティ政策分野	情報セキュリティ政策内容	評価に当たり考慮すべき状況
<p>(2) 国民・利用者保護の強化</p>	<p>普及・啓発活動の充実・強化</p> <p>国民・利用者が IT リスクを認識し、自ら情報セキュリティ対策を実施することを促すため、普及・啓発活動を強力に推進する。2010 年 2 月から、新たに 2 月を「情報セキュリティ月間」として定め、普及・啓発を強化したところであるが、更なる充実強化を図るため、「包括的な普及・啓発プログラム」を策定する。</p>	<ul style="list-style-type: none"> インターネット利用上の不安の有無（通信利用動向調査：総務省） インターネット利用上で感じる不安の内容（通信利用動向調査：総務省） インターネットを利用しない理由（通信利用動向調査：総務省） 情報セキュリティトラブルの重要性に対する認識（情報処理実態調査：経済産業省） 情報セキュリティに関する攻撃・脅威の認知（情報セキュリティの脅威に対する意識調査：情報処理推進機構） セキュリティに関する現在の情報源と望ましい情報源（情報セキュリティの脅威に対する意識調査：情報処理推進機構） 情報セキュリティ対策の必要性（不正アクセス行為対策等の実態調査：警察庁） 情報セキュリティに係る政府系ウェブサイトへのアクセス状況（内閣官房、警察庁、総務省、経済産業省）
	<p>情報セキュリティ安心窓口（仮称）の検討</p> <p>国民・利用者の情報セキュリティ水準を向上させるための活動を行う地域 NPO 法人等の支援を行うとともに、国民・利用者からの情報セキュリティに関する相談を受け付けるため、既存の枠組みも活用しつつ、「情報セキュリティ安心窓口（仮称）」の設置を検討する。</p>	<ul style="list-style-type: none"> 情報セキュリティサポータをとりまとめる地域団体の数（総務省） コンピュータウイルス・不正アクセスの届出状況（情報処理推進機構） 被害・トラブル時に対処をしなかった理由（情報セキュリティの脅威に対する意識調査：情報処理推進機構） 知りたいセキュリティ情報（情報セキュリティの脅威に対する意識調査：情報処理推進機構）
	<p>個人情報保護の推進</p> <p><u>プライバシー保護技術の適切な利用促進</u> 大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用を促進する。</p> <p><u>各事業分野ごとの個人情報保護に関するガイドラインの見直し</u> 企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者へ暗号化等を行うインセンティブを付与するための見直しを行う。</p>	<ul style="list-style-type: none"> 消費者庁「個人情報の保護に関する法律施行状況の概要」漏えい等の形態と暗号化等の情報保護措置の「電子媒体での漏えいにおいて情報保護措置がとられていた件数」 「個人情報の保護に関する 27 分野 40 のガイドライン」について、見直しされた件数
	<p><u>国際的なフレームワークへの対応</u> 個人情報の国際的な流通が適切かつ安全な形で行われることを促進するため、OECD (The Organizations for Economic Cooperation and Development) をはじめとして、APEC (Asia-Pacific Economic Cooperation)、EU (European Union) 等様々な場で進められている国際的な取組を踏まえ、プライバシー保護に関する越境執行協力等、国際的な協調を図っていくとともに、我が国の法制度についても国際的な理解を求め、データプライバシー保護に係る諸外国の制度と我が国の法制度との整合性に留意しつつ、我が国として必要な対応を検討する。</p>	<ul style="list-style-type: none"> OECD、APEC 等の国際会議への出席や報告の状況

情報セキュリティ政策分野	情報セキュリティ政策内容	評価に当たり考慮すべき状況
	<p><u>個人情報保護法の見直し</u> 個人情報保護法について、法改正も視野に入れた問題点についての審議を踏まえ検討を行う。</p>	<ul style="list-style-type: none"> 消費者委員会個人情報保護専門調査会の開催状況
	<p><u>サイバー犯罪に対する態勢の強化</u> <u>犯罪取締りのための基盤整備の推進</u> サイバー犯罪の取締り体制の強化を図るとともに、デジタルフォレンジックを活用したサイバー犯罪の取締り、国際協調の推進等の基盤強化を推進する。 さらに、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強い社会構築のための官民連携に向けた取組を推進する。</p>	<ul style="list-style-type: none"> 不正アクセス行為の認知件数（不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況：国家公安委員会・総務省・経済産業省） サイバー犯罪の検挙状況（サイバー犯罪の検挙状況等について：警察庁） サイバー犯罪等に関する相談状況（サイバー犯罪の検挙状況等について：警察庁）
	<p><u>犯罪抑止のための広報啓発の推進</u> サイバー犯罪抑止を図るため、国民一人一人が自らサイバー犯罪から身を守るという意識を高めるための、情報セキュリティに関する講習等の啓発活動を強力に推進する。</p>	<ul style="list-style-type: none"> サイバー犯罪に関する防犯セミナー等の実施状況 インターネット安全教室開催数（経済産業省） ウェブサイト（サイバー犯罪対策、@police）へのアクセス状況
(3) 国際連携の強化	<p>日米サイバーセキュリティ会合や日・ASEAN 情報セキュリティ政策会議等の開催を通じ、政策面における海外との連携を戦略的に強化するとともに、情報セキュリティ対策セミナーの開催等の海外 CSIRT（コンピュータセキュリティ緊急対応チーム）の構築支援等、実務面におけるネットワークの構築を図る。 また、従来の取組に加え、インターネットが急速に普及している国々の状況も踏まえつつ、新たな二国間関係の構築等に努める。</p>	<ul style="list-style-type: none"> 二国間、ASEAN 各国との関係構築状況
	<p>APEC、ARF、ITU、MERIDIAN、IWWN、FIRST（Forum for Incident Response and Security Teams）、APCERT（Asia Pacific Computer Emergency Response Teams）等、様々な分野の国際会議に積極的に参加し、外国機関等との情報共有体制を強化する。</p>	<ul style="list-style-type: none"> 外国機関等との情報共有体制の強化状況
	<p>NISC は、横断的な情報セキュリティ問題に関する国際 POC（Point of Contact）として、各国の情報セキュリティに関するベストプラクティスの共有、各国の重要インフラの情報セキュリティ対策等を含む情報セキュリティ政策全般について、諸外国等の関係機関との連携を強化する。</p>	<ul style="list-style-type: none"> 諸外国等の関係機関等との連携状況

情報セキュリティ政策分野		情報セキュリティ政策内容	評価に当たり考慮すべき状況
(4)技術戦略等の推進	情報セキュリティ関連の研究開発の戦略的推進等	<p>米国等の動向も踏まえ、情報セキュリティに係る研究開発を戦略的に推進するため、新たな情報セキュリティ研究開発戦略を策定する。</p> <p>インターネットを始めとする情報通信技術を利用者が活用するにあたっての脆弱性の克服や、IPv6 や、クラウドコンピューティング、情報家電、携帯端末、センサーネットワーク等の情報通信技術の環境の変化に対応した情報セキュリティ技術の開発、高度化・多様化する攻撃等に対応できる情報セキュリティ技術(「グラウンドチャレンジ型」研究開発・技術開発)の実現・普及の実現を目指す。また、情報セキュリティ脅威の実態を踏まえた、システム設計管理対策の強化・普及を図る。</p>	<ul style="list-style-type: none"> 重点テーマの研究開発の推進状況及び実用化や普及といった研究開発以降のプロセスについての進展状況
	情報セキュリティ人材の育成	<p>一般利用者の情報セキュリティ水準を底上げするため、利用者の身近で情報セキュリティ対策をサポートできる人材を育成する。</p> <p>また、共通的な人材評価・育成ツールを活用して、産学連携による実践的な人材育成手法等に基づく高度な情報セキュリティ人材を育成するとともに、このような人材を育成するためのモデル的なキャリアパスを策定、可視化し、普及等を図る。</p> <p>また、情報セキュリティ人材の中長期的な確保メカニズムの確立も視野に入れつつ、幅広い分野における情報セキュリティ人材育成に係る工程表を策定する。</p>	<ul style="list-style-type: none"> 情報セキュリティサポータの人数(総務省) インターネット安全教室開催数(経済産業省) e-ネットキャラバン開催状況(総務省・文部科学省) IPA 中小企業情報セキュリティセミナー開催状況(情報処理推進機構) 情報セキュリティスペシャリスト試験合格者数(情報処理推進機構) システム監査技術者試験合格者数(情報処理推進機構) 教員の ICT 活用指導力の状況(学校における教育の情報化の実態等に関する調査:文部科学省) 情報セキュリティ教育の実施状況(不正アクセス行為対策等の実態調査:警察庁) 従業員に対する情報セキュリティ教育の実施状況(情報処理実態調査:経済産業省)

情報セキュリティ政策分野		情報セキュリティ政策内容	評価に当たり考慮すべき状況
	情報セキュリティガバナンスの確立	事業継続計画（BCP）の策定、情報セキュリティ監査の実施や財務システム等の業務システムの入れ替え時における情報セキュリティ確保を図るため、普及・啓発活動を通じ、情報セキュリティガバナンスが経営課題として位置付けられ、経営者の意識改革が行われることを促すとともに、新たなリスクマネジメント等に関する手法の導入において情報セキュリティが明確に位置づけられるような方策を推進する。	<ul style="list-style-type: none"> ・ ISMS 認証取得組織数（日本情報経済社会推進協会） ・ ITSMS 認証取得組織数（日本情報経済社会推進協会） ・ Number of Certificates Per Country（ISMS International User Group） ・ 情報セキュリティの対策状況（事業継続計画（BCP）の作成）（情報処理実態調査：経済産業省） ・ 情報セキュリティトラブルの重要性に対する認識（情報処理実態調査：経済産業省） ・ 情報セキュリティ対策のセキュリティ向上以外の効果（情報処理実態調査：経済産業省） ・ 情報セキュリティ対策の阻害要因（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（リスク分析）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（セキュリティポリシーの策定）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（情報セキュリティ報告書の作成）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（全体的なセキュリティ管理者の配置）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（部門ごとのセキュリティ管理者の配置）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（内部統制の整備強化）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（ISO/IEC15408 認証取得製品の導入）（情報処理実態調査：経済産業省） ・ セキュリティ対策ソフト導入状況（国内における情報セキュリティ事象被害状況調査：情報処理推進機構） ・ ISO/IEC15408 に関する意識・実態（情報セキュリティ製品の調達等に関する意識調査：情報処理推進機構） ・ CC に係る税制についての意識（情報セキュリティ製品の調達等に関する意識調査：情報処理推進機構） ・ 情報セキュリティの対策状況（外部専門家による定期的な情報セキュリティ監査）（情報処理実態調査：経済産業省） ・ 情報セキュリティの対策状況（内部による定期的な情報セキュリティ監査）（情報処理実態調査：経済産業省）
	（５）情報セキュリティに関する制度整備	サイバー犯罪条約の早期締結に向けて必要な検討を進め、また、コンピュータウイルス関連の法改正等の法整備を推進するとともに、機微な情報へのアクセス権限を明確化するための方策や情報漏えい等を防止するための方策の検討等サイバー空間の安全性・信頼性を向上させる制度について積極的な検討を行う。	<ul style="list-style-type: none"> ・ 各種制度等の検討状況

情報セキュリティ政策分野		情報セキュリティ政策内容	評価に当たり考慮すべき状況
	各国の情報セキュリティ制度の比較検討	情報セキュリティに関する国際連携・協調を推進するため、各国間の法制度等の相違について分析し、課題の抽出と連携方策の検討を行う。	・ 各国の法制度に関する調査報告書作成等の進捗状況