

情報セキュリティ政策の評価等の実施方針
(第2版) (案)

2012年 月 日

内閣官房情報セキュリティセンター (NISC)

目次

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

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

I 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。

II 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）で抽出した事項を次の計画へ反映するように努める。

Ⅲ 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もある。

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 |
| ① | 政府機関等の基盤強化 |
| ② | 重要インフラの基盤強化 |
| ③ | 情報セキュリティ産業の振興 |
| ④ | その他の基盤強化 |
| (2) | 国民・利用者保護の強化 |
| ① | 普及・啓発活動の充実・強化 |
| ② | 個人情報保護の推進 |
| ③ | 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 |
| ① | 情報セキュリティ関連の研究開発の戦略的推進等 |
| ② | 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 |
| 3 | 東日本大震災を踏まえた情報セキュリティ政策 |
| 4 | 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

⁹ 本表は、最新の情報セキュリティ政策分野に準拠して策定したものであり、情報セキュリティを取り巻く脅威や社会・環境の変化に伴い新たな政策が立案されれば、必要に応じて本表の見直しを行い評価対象としていく。

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し、「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付けられ、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」により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 | (1) 対処態勢の整備 | ○大規模サイバー攻撃事態における政府の初動対処態勢の整備 ○官民連携の推進 | ・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 ・サイバー攻撃事態への対処に資する情報の集約・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) 平素からの情報収集・共有体制の構築強化 | ○サイバー攻撃に対する防衛分野での体制の強化 ○サイバー犯罪の取締り ○サイバー攻撃への対処に係る国際連携の強化 ○対処に資する情報の収集・分析・共有体制の強化 ○サイバー攻撃等に関する諸外国等との情報共有体制の構築・強化 | |
| 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 | (1) 国民生活を守る情報セキュリティ基盤の強化 | ①政府機関等の基盤強化 | ○サイバー攻撃等に関する情報収集・分析結果等の情報共有の実施状況 |
| | | ○政府横断的な情報収集・分析システム (GSOC) の充実・強化 | ・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 ・情報セキュリティ報告書に関する評価項目等の改善状況 ・年次報告の作成、公表状況 |
| | | ○最高情報セキュリティ責任者 (CISO) の機能強化 | ・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 ・脆弱性検査の実施状況 ・標的型メール攻撃に係る教育訓練の実施状況 ・東日本大震災による情報システムへの影響に関する分析・評価の状況 ・各府省庁における情報システム運用継続計画の策定及び内閣官房による評価手法の検討状況 ・認証ガイドラインに基づく助言等の実施状況 ・政府機関における情報セキュリティ教育の実施状況 ・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 |
| | | ○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 | ・移行指針に規定する要件への適合状況 ・緊急対応計画の発動要件の策定状況 |
| | | ○政府機関における安全な暗号利用の推進 | ・クラウドコンピューティングを踏まえた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) ・「政府共通プラットフォーム」における情報セキュリティ確保方策の検討状況 |
| | | ○クラウドコンピューティングにおける情報セキュリティの確保等 | |

| 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 |
|--------------|----------------------|--|---|
| | | ○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 | ・リスク・マネジメント手法の検討及び取りまとめ状況 ・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） ・独立行政法人等との連携状況 |
| | | ○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 | ・「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」の各府省庁における活用・普及状況 |
| | | ○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 | ・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 |
| | | ○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 | ・独立行政法人等における情報セキュリティ対策の実施状況 ・独立行政法人における送信ドメイン認証技術導入の進捗状況 |
| | ②重要インフラの基盤強化 | ○情報共有体制の強化 | ・重要インフラ事業者等の取組の検証における検証レベルを逸脱したIT障害等の発生状況 ・政府機関等による施策の検証における安全基準等の整備及び浸透状況 |
| | | ○「セプターカウンスル」の活動促進 | ・重要インフラ分野における共有情報の動向 ・共通脅威分析における分析に協力した重要インフラ事業者等の意向 ・分野横断的演習における参加規模と参加者の意向 ・環境変化への対応における情報発信やリスク・コミュニケーションの現状 |
| | | ○「安全基準等」の整備浸透 | |
| | | ○重要インフラ防護対策の向上 | ・技術戦略専門委員会等における情報セキュリティ産業を活性化する方策の検討状況 |
| | | ○制御システムに関する情報セキュリティ上の課題への対応 | |
| | | ○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 | | |
| | ③情報セキュリティ産業の振興 | ○情報セキュリティ産業の振興 | ・技術戦略専門委員会等における情報セキュリティ産業を活性化する方策の検討状況 |
| | ④その他の基盤強化 | ○スマートフォンに関する情報セキュリティ確保方策 | ・スマートフォンの利用状況（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） ・スマートフォンに必要だと思うセキュリティ対策（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） |
| | | ○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 | ・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対応、SNSに関する情報セキュリティ確保方策 | ・IPv6普及・高度化推進協議会における検討・推進状況 ・ソーシャルメディアの利用時におけるなりすまし防止等の周知状況 |

| 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 |
|--------------|------------------------|--|--|
| | | ○マルウェア対策等の充実・強化等 | <ul style="list-style-type: none"> ・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 ・安全なサーバ数（ICT基盤に関する国際比較調査：総務省） ・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） ・コンピュータウイルス届出状況（情報処理推進機構） ・コンピュータ不正アクセス届出状況（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） |
| | | ○情報家電、モバイル端末、電子タグ、センサーネットワーク等の情報セキュリティ確保方策 | <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 |
| | | ○中小企業に対する情報セキュリティ対策支援 | <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） |
| | | ○安全な電子商取引の推進 | <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） |
| | | ○知的財産保護の推進 | <ul style="list-style-type: none"> ・「知的財産推進計画」の進捗状況（内閣官房） |
| | ⑤内閣官房情報セキュリティセンターの機能強化 | ○NISCの総合調整機能の強化 | <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 ・各府省庁への支援に関する取組状況 ・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 |
|------------------|----------------------|---|---|
| (2) 国民・利用者保護の強化 | ①普及・啓発活動の充実・強化 | ○普及・啓発活動の充実・強化 | <ul style="list-style-type: none"> ・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） ・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必要性（不正アクセス行為対策等の実態調査：警察庁） ・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） ・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） |
| | ②情報セキュリティ安心窓口（仮称）の検討 | ○情報セキュリティ安心窓口（仮称）の検討 | <ul style="list-style-type: none"> ・被害・トラブル時に対処しなかった理由（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） ・情報セキュリティ安心相談窓口における相談対応状況（情報処理推進機構） |
| | ③個人情報保護の推進 | ○個人情報保護法の見直し | ・消費者委員会個人情報保護専門調査会の開催状況 |
| | | ○国際的なフレームワークへの対応 | ・OECD、APEC等の国際会議への出席や報告の状況 |
| ④サイバー犯罪に対する態勢の強化 | ○犯罪取締りのための基盤整備の推進 | <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） | |
| | ○犯罪抑止のための広報啓発の推進 | <ul style="list-style-type: none"> ・インターネット安全教室開催数（経済産業省） ・サイバー犯罪に関する防犯セミナー等の実施状況 ・情報セキュリティに係る政府系ウェブサイト（サイバー犯罪対策、@police）へのアクセス状況（警察庁） | |

| 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 |
|--------------|---|---|--|
| (3) 国際連携の強化 | ①米国、ASEAN、欧州等との連携強化（二国間、ASEANとの関係強化） | ○米国、ASEAN、欧州等との連携強化（二国間、ASEANとの関係強化） | ・二国間、ASEAN各国との関係構築状況 |
| | ②APEC、ARF、ITU、MERIDIAN、IWWN等国際会合を活用した情報共有体制等の強化 | ○APEC、ARF、ITU、MERIDIAN、IWWN等国際会合を活用した情報共有体制等の強化 | ・外国機関等との情報共有体制の強化状況 |
| | ③NISCの窓口機能の強化 | ○NISCの窓口機能の強化 | ・諸外国等の関係機関等との連携状況 |
| (4) 技術戦略の推進等 | ①情報セキュリティ関連の研究開発の戦略的推進等 | ○情報セキュリティ関連の研究開発の戦略的推進等 | ・研究開発戦略において選定されている重要分野の研究開発の推進状況 |
| | ②情報セキュリティ人材の育成 | ○情報セキュリティ人材の育成 | <ul style="list-style-type: none"> ・情報セキュリティ監査を行う者の資質向上を図るための教育の実施状況 ・e-ネットキャラバン開催状況（総務省、文部科学省） ・情報セキュリティの対策状況（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） ・インターネット安全教室開催数（経済産業省） ・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） ・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） |

| 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 |
|----------------------|-----------------------------|-----------------------------|---|
| | ③情報セキュリティガバナンスの確立 | ○情報セキュリティガバナンスの確立 | <ul style="list-style-type: none"> ・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（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） ・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） ・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） ・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） ・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) |
| (5) 情報セキュリティに関する制度整備 | ①サイバー空間の安全性・信頼性を向上させる制度の検討等 | ○サイバー空間の安全性・信頼性を向上させる制度の検討等 | ・各種制度の検討等の状況 |
| | ②各国の情報セキュリティ制度の比較検討 | ○各国の情報セキュリティ制度の比較検討 | ・各国の法制度に関する調査報告書作成等の進捗状況 |

| 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 |
|-----------------------|-------------------------------------|----------------------------------|--|
| 東日本大震災を踏まえた情報セキュリティ政策 | (1) 災害時に強靱な情報通信システムの構築 | ○災害時に強靱な情報通信システムの構築 | <ul style="list-style-type: none"> ・先進的な取組事例等の調査及び物理的セキュリティ対策の在り方に関する検討状況 ・リスク・マネジメント手法の検討及び取りまとめ状況 ・情報システム運用継続計画の策定及び評価手法の検討状況 ・東日本大震災による情報システムへの影響に関する分析・評価の状況 ・重要インフラ情報システムに係る対応の状況 ・重要インフラ分野間の相互依存性解析の状況 |
| | (2) 「リスク・マネジメント」、「リスク・コミュニケーション」の確立 | ○「リスク・マネジメント」、「リスク・コミュニケーション」の確立 | <ul style="list-style-type: none"> ・東日本大震災による情報システムへの影響に関する分析・評価の状況 ・リスク・マネジメント手法の検討及び取りまとめ状況 ・重要インフラ情報システムに係る対応の状況 |
| | (3) 情報システム全体の「ニュー・ディペンダビリティ」の確保 | ○情報システム全体の「ニュー・ディペンダビリティ」の確保 | <ul style="list-style-type: none"> ・情報システム全体の「ニュー・ディペンダビリティ」確保に向けた研究開発の進捗状況 |