

情報セキュリティの観点から見た
我が国社会のあるべき姿及び政策の評価のあり方

【第2版】

～「セキュア・ジャパン」の実現に向けた
情報セキュリティ政策のPDCAサイクルの確立へ～

2010年5月11日

情報セキュリティ政策会議了解

目 次

はじめに	1
1 . 基本認識	1
2 . 本文書の構成	2
第 1 章 IT 安心利用環境の構築に向けた情報セキュリティ政策に 関する P D C A サイクル	3
第 1 節 第 2 次基本計画の基本的な改善構造	3
第 2 節 P D C A サイクルによる持続的改善の実施	3
(1) 計画 (P l a n) 段階	3
(2) 実施 (D o) 段階	4
(3) 点検 (C h e c k) 段階	4
(4) 改善処置 (A c t) 段階	5
第 2 章 評価等のあり方	6
第 1 節 評価等に関する基本的枠組み	6
1 . 成果 (アウトプット) 評価指標と結果 (アウトカム) 評価指標	6
2 . 評価指標に基づく評価と補完調査	6
3 . 分析	7
4 . 報告	8
5 . 具体的な作業方針の策定	8
6 . まとめ	8
第 2 節 評価等 (総論) ~ 我が国全体としての評価指標について	9
第 3 節 評価等 (各論)	9
1 . 考え方	9
(1) 対策実施四領域	9
(2) 対策実施四領域以外の分野	10
2 . 対策実施四領域に関する評価指標	11
(ア) 政府機関・地方公共団体	11
(イ) 重要インフラ	12
(ウ) 企業	12
(エ) 個人	13
第 3 章 評価等の結果を受けた持続的改善のあり方	14
第 1 節 評価指標等を用いた持続的改善のあり方 (基本的考え方)	14

第2節 持続的改善の方法	14
1. 次期計画への反映	14
2. 持続的な改善のための取組み推進	14

図 表

- 図1：情報セキュリティ政策のPDCAサイクルの計画段階（P）
- 図2：情報セキュリティ政策のPDCAサイクル
- 図3：評価指標に基づく評価及び状況把握のための補完調査
- 図4：評価指標等を用いた持続的改善

別 添

- 別添1：『第2次情報セキュリティ基本計画』（抄）
- 別添2：『情報セキュリティ報告書専門委員会報告書
～能動的な政府機関の情報セキュリティ対策のために～』（抄）
- 別添3：『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』（抄）
別紙：重要インフラサービスと検証レベル
- 別添4：企業・個人における情報セキュリティの評価指標

はじめに

1. 基本認識

我が国の国民生活・社会経済活動のITへの依存度の深化にともない、ITを安全・安心に活用するための取組み、すなわち情報セキュリティ問題への取組みを抜本的に強化する必要があるとの認識の下、戦略的思考に基づく我が国の取組みの体系的な中長期計画として「第1次情報セキュリティ基本計画」¹（以下「第1次基本計画」という）が策定された。

情報セキュリティ問題への取組みは、ITの利用・活用のあり方や取り巻く環境が刻々と変化することからも、一度定めた計画に基づき取組みを進めるだけでは不十分であり、一定期間毎に時宜に見合った見直し、PDCAサイクル²の構築が不可欠である。第1次基本計画では3か年を計画期間とし、計画策定から実施、評価、評価結果を次期計画策定へ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へ反映させる単年度のサイクルをもって情報セキュリティ政策の持続的改善を図る構造としていた。このようなPDCAサイクルによる持続的改善構造をもつ第1次基本計画の下、官民各主体によって、2006年度から2008年度の3か年にわたり様々な取組みが進められた。これにより、政府機関・地方公共団体、重要インフラ、企業、個人の各主体における対策の進展と、情報セキュリティ技術戦略の推進、情報セキュリティ人材育成・確保、国際連携・協調の推進、犯罪の取締り及び権利利益の保護・救済といった横断的な基盤の形成のための各種施策が実施されたところである。

こうした3か年の取組みの後の課題やITを基盤とした社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するため、2009年度以降を念頭に置いた「第2次情報セキュリティ基本計画」³（以下「第2次基本計画」という）が策定された。今後3か年の取組みにおいても、第1次基本計画同様にPDCAサイクルによる持続的改善構造を引き続き維持し、IT利用を取り巻く環境の変化に対応する必要がある。そのため、第2次基本計画の下、情報セキュリティ政策におけるPDCAサイクルを推進するために必要となる要素、手段、個別取組みの改善と政策全体の見直しの体系についてとりまとめを行う。本文書は、情報セキュリティ政策会議決定文書「「セキュア・ジャパン」の実現に向けた取組み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」に基づいて、内閣官房情報セキュリティセンター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み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 PDCAサイクルとは、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。

³ 2009年2月2日 情報セキュリティ政策会議決定。

2．本文書の構成

本文書でとりまとめる持続的改善の取組みが目指す我が国社会のあるべき姿については、第2次基本計画に示された内容を参照することとし、本文書第1章では、IT安心利用環境の構築に向けて情報セキュリティ政策のPDCAサイクルを構築することが重要であることを前提に、情報セキュリティ政策におけるPDCA各段階で必要となる諸点、第2次基本計画における対応について述べた。これを受けて第2章では、点検(Check)段階で必要となる評価指標の設定や、評価指標の設定が容易でない場合等に行う補完調査、分析等について述べている。さらに、以上を踏まえて第3章においては、改善処置(Act)段階として評価指標等を活用した持続的改善のあり方について述べている。

第1章 IT安心利用環境の構築に向けた情報セキュリティ政策に関するPDCAサイクル

第1節 第2次基本計画の基本的な改善構造

情報セキュリティの取組みは、ITそのものの利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もってその変化に即し、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、第2次基本計画は基本的なPDCAサイクルを3か年として設計され、計画期間中であっても環境変化が生じた場合には見直しを行うこととしている。また、第2次基本計画を具体的に実行していくために、単年度毎の施策実施プログラムを「年度計画（セキュア・ジャパン20XX）」として策定し、その実施状況を社会情勢の変化とともに評価し、この評価を踏まえ翌年度の計画策定を行う単年度のPDCAサイクルを実施する構造をもつ。

こうしたプロセスにより、情報セキュリティ政策そのものについて政策の取組みの計画作成から実施、評価、評価結果の翌年度施策実施プログラムへの反映、第2次基本計画の基本目標である『IT安心利用環境の構築』に向けた情報セキュリティ問題への取組みを行う。

第2節 PDCAサイクルによる持続的改善の実施

PDCAサイクルによる持続的改善の実施において、PDCAの各々の段階における必要な諸点と第2次基本計画での対応について述べる。

(1) 計画（Plan）段階

計画段階（P）⁴は、中長期計画である第2次基本計画とその個別設計図である『政府機関の情報セキュリティ対策のための統一基準』⁵（以下「政府機関統一基準」という。）と『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』⁶（以下「第2次行動計画」という。）の策定、年度計画であるセキュア・ジャパン20XXの策定がこれにあたる。第2次基本計画では基本理念や施策の方向性を定め、年度計画では具体的な実施施策を定める。個別設計図では各分野での取組みの計画や対策実施項目を定めている。策定にあたっては、その時点での課題やリスクを明らかにし、それらに対して適切な対策を継

⁴ 以下、PDCAの各段階について、計画段階は「計画段階（P）」、実施段階は「実施段階（D）」、点検段階は「点検段階（C）」、改善処置段階は「改善処置段階（A）」というように、PDCAの文字を後ろに付ける形で標記する。

⁵ 初版 2005年12月13日 情報セキュリティ政策会議決定、第4版改定 2009年2月3日 情報セキュリティ政策会議決定。

⁶ 2009年2月3日 情報セキュリティ政策会議決定。

続的に実施することで、目標とする時期までにリスクを受容可能な水準に管理（解消・低減）することを念頭に置いて設計する必要がある。また、計画による取組みを推進することにより、社会がどのようになるべきと考えられるのかをあるべき姿として明示し、その姿へ向かった取組みがなされなければならない。

第2次基本計画では、計画策定時における現状の認識と、計画に基づく3か年の取組みを進めることで、我が国の姿が計画期間終了後にどのようになっているかを2012年の姿⁷（以下「あるべき姿」という。）として記述し、それらを施策の方向性として取りまとめている。

ただし、取り巻く環境やリスクは常に変化することからも、必ずしも計画策定時点の認識のままではない。そのため、それら現状の認識は年度計画の評価等において、又は、次期計画策定に際して見直しを実施していく必要がある。

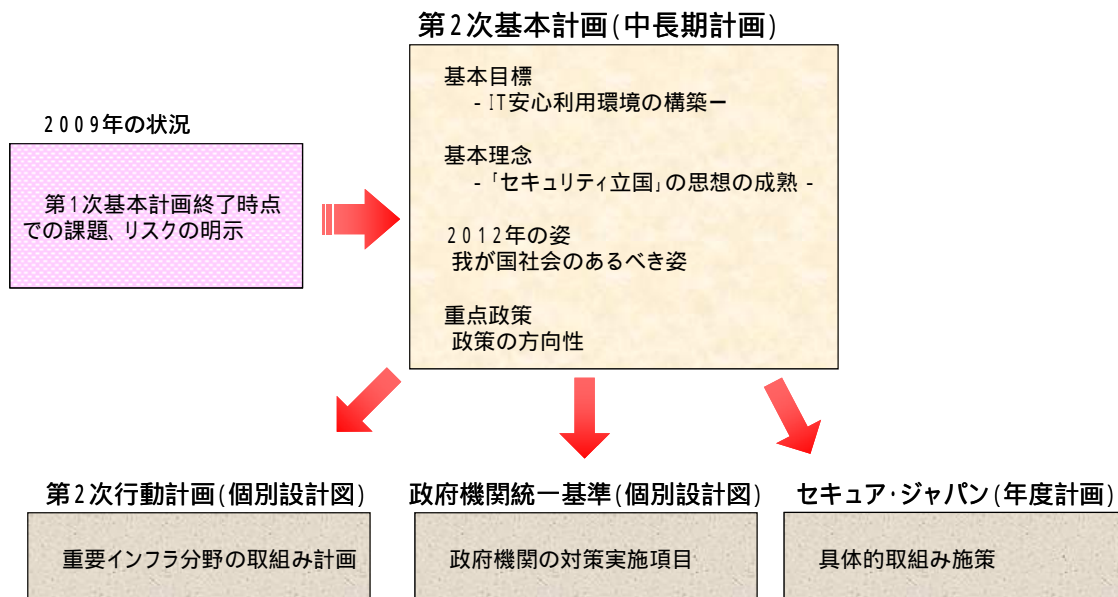


図 1 情報セキュリティ政策のPDCAサイクルの計画段階（P）

(2) 実施（Do）段階

実施段階（D）は、第2次基本計画において示されたあるべき姿、施策の方向性の具体的実現のために策定される年度計画をもって、その着実な推進が求められる。

(3) 点検（Check）段階

点検段階（C）は、第2次基本計画終了後の2012年当初に、想定した姿

⁷ 第2次基本計画 第2章第2節 2012年の姿の項（別添1）を参照。

にどの程度到達できたか、その時点での取り巻く環境やリスクが許容できる水準にあるかを点検できることが必要である。また、年度計画のサイクルでは、1年ごとに着実に第2次基本計画が示すあるべき姿へと進んでいることが目標であり、これを点検できることが必要である。

そのためには、設定可能な評価指標等を活用し、必要に応じて補完調査等を行い、目標への到達度を測ることとする。また、評価指標や補完調査に基づく状況把握及び分析等のほか、その時点の取り巻く環境や新たに明らかになったリスク等の把握も行う必要がある。

(4) 改善処置 (Act) 段階

改善処置段階 (A) は、前項の点検段階 (C) の結果を踏まえ、必要な取り組みの改善を図っていく。単年度の改善では、取り組みが不十分と認められる事項、更なる改善が期待される事項及び新たに明らかになったリスクに対処するために必要な施策を次年度計画へ反映するように努めることとする。また、第2次基本計画の最終年度にあたっては、点検段階 (C) の結果を踏まえ、必要な施策の方向性及び実現しようとするあるべき姿を次期計画へ反映するよう努めることとする。こうした反映作業については、年度計画への反映は毎年行われるとともに、基本計画への反映は、原則、3年に一度行われることとなる。

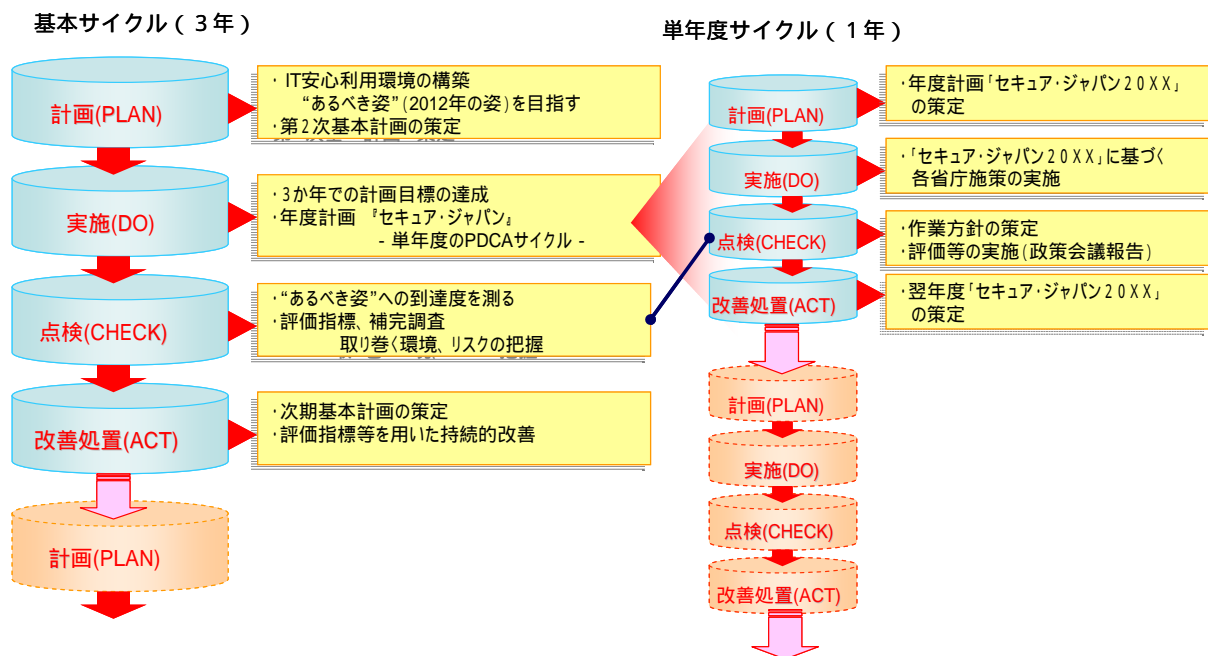


図 2 情報セキュリティ政策のPDCAサイクル

第2章 評価等のあり方

第1節 評価等に関する基本的枠組み

ここでは、第1章第2節(3)に基づき、情報セキュリティ政策のPDCAサイクルの点検段階(C)の具体的な内容となる評価等の枠組みに関して記述する。

情報セキュリティ政策会議は、ITを安心して利用できる環境の構築に向け、以下のとおり、情報セキュリティ対策に関する評価指標に基づく評価やこれを補完して状況を把握するための調査等を図ることとする。

また、これらの取組みは、「「セキュア・ジャパン」の実現に向けた取組み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(2007年2月2日情報セキュリティ政策会議決定)」に基づき、内閣官房情報セキュリティセンター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. 成果(アウトプット)評価指標と結果(アウトカム)評価指標

第2次基本計画は、計画段階(P)においては、第1章で述べたように、計画が目標とする時点における我が国社会のあるべき姿を念頭に置き、そして実施段階(D)においては、社会がその姿に近づいていくよう具体的な各種施策を実施するという形で設計されている。このため、評価指標群の設定に当たっては、個々の具体的な施策がどういう成果をあげているのかという「成果(アウトプット)を測る視点」と、社会が実際にどの程度その姿に近づいているのかという「結果(アウトカム)を測る視点」の二つの視点に配慮する必要がある。これを踏まえると、点検段階(C)のための指標は、

(i) 成果評価指標：政府の施策を中心にIT安心利用環境の構築に向けて様々な取組みが推進されている状況で、こうした取組みの成果がどの程度出ているのかを測るための指標、

() 結果評価指標：各種の取組みを実施した結果として、社会がどのようになったかを測るための指標

という二種類に大別して設定することが望ましい。

2. 評価指標に基づく評価と補完調査

内閣官房情報セキュリティセンターは、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。しかし、情報セキュリティ政策のPDCAサイクルにおける点検段階(C)は、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しきれるとは言えないため、固定的な指標に基づく評価のみでは把握できることに限界がある。

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、補完情報を参照することも含めて、補完的な調査（以下「補完調査」という。）を実施することが必要となる。このため、内閣官房情報セキュリティセンターは、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、取組みを行う情報セキュリティ対策の実施主体（政府機関・地方公共団体、重要インフラ、企業、個人）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⁸。

ここで、政府機関については対策実施主体としても、また、問題の理解・解決を促進する主体としても重要な役割を果たしており、他の様々な主体の模範となることが期待されていることから、指標に基づく評価及びそのための情報収集、状況把握のための補完調査において、他の主体よりも率先し、積極的な役割を果たすとともに、特に、政府機関自身の状況等に関する補完調査については、政府機関の間で柔軟に協力を行いつつ効果的に調査を実施することが期待される。

なお、リスクは日々変化が生じうることから、2009年度時点に設定した評価指標のみでリスクの変化も含めてすべてを把握しきれるとは必ずしも言えない。このことを踏まえ、点検段階（C）では、その時点ごとの評価指標項目について、より充実し、時宜に合った指標となるよう、内閣官房情報セキュリティセンターが、必要に応じて各府省庁の協力を得て必要な見直しや追加を行う。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、設定した指標の見直しの際には、経年的な比較がまったくできなくなるような見直しとならないよう留意することが必要である。

3．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、またそれらの変動だけからは、背景等が十分に見えな可能性もある。また、特に結果評価指標に関して顕著なことであるが、情報セキュリティ政策の具体的取組みと指標に基づいて把握できたデータ等との間の因果関係・相関関係が明らかではない場合も想定される。

このような場合には、内閣官房情報セキュリティセンターは、把握したデータ等と具体的な取組みとの間の「隙間」を埋めるため、必要に応じて分析を行う。

⁸ 例えば、政府機関の状況の把握に比べて、企業や個人に関する状況把握はより間接的なものとならざるを得ないことや、政府機関は企業総体や個人総体に比べて母集団の規模が小さいことから、相対的に状況把握が容易であることを勘案することなどが挙げられる。

4．報告

内閣官房情報セキュリティセンターは、上記のような取組みの結果、評価指標に基づくデータ、評価の結果及び補完調査によって把握した現状について、原則、毎年度第一回目の情報セキュリティ政策会議に報告を行う。また、分析結果についても、これらとともに、情報セキュリティ政策会議へ報告を行うこととする。

5．具体的な作業方針の策定

評価指標に基づく評価、補完調査及び分析等（以下「評価等」という。）の実施については、スケジュール等に関して計画性を持った上で各府省庁が協力を行いつつ、効率的に行うことが不可欠である。そのため、内閣官房情報セキュリティセンターは、指標に基づく評価等を実施するための作業方針（以下「作業方針」という。）を毎年度策定する。作業方針は、その年度における評価等に関する方針やスケジュールを定めると同時に、翌年度の年度計画や次期の基本計画の策定のための方針ともなるものである。具体的には、(i)評価指標の項目・関係府省庁、(ii)補完調査の項目・関係府省庁、(iii)分析課題及び分析方法、(iv)評価等のスケジュールその他評価等を実施する上で必要となる事項が盛り込まれる。これに基づき、内閣官房情報セキュリティセンターは、各府省庁の協力を得つつ評価等の作業を進める。

6．まとめ

3か年を計画期間とする基本計画や年度計画であるセキュア・ジャパンの策定過程の関係で整理を行うと、評価等に関する過程は以下の通りとなる。

第一に、内閣官房情報セキュリティセンターは、毎年度可能な限り速やかに、作業方針を策定する。

第二に、内閣官房情報セキュリティセンターは、作業方針に基づき、各府省庁の協力を得つつ、評価指標に基づき必要なデータ等の収集及び補完調査を行う。

第三に、内閣官房情報セキュリティセンターは、収集したデータに基づく評価等、補完調査による状況の把握及び必要に応じた分析を行い、年度末までを目途にとりまとめを行う。

なお、内閣官房情報セキュリティセンターは、評価等を通じて明らかになったリスクや姿の変化の把握及び変化を踏まえた評価指標の見直し・追加についてもこの時期に行う。

また、基本計画の計画期間（3か年）の最終年度では、それまでの評価等及び当該年度の収集したデータに基づく評価等、補完調査による状況の把握及び必要

に応じた分析を基に、基本計画策定時に示されたあるべき姿への到達度についても評価等を行う。

第四に、内閣官房情報セキュリティセンターは、原則、翌年度開催される当該年度第一回目の情報セキュリティ政策会議において、評価指標に基づくデータ及び評価等の結果について報告を行う。

第2節 評価等（総論）～我が国全体としての評価指標について

情報セキュリティ政策における実施施策は、基本計画に定めた方向性に従って毎年度定められるセキュア・ジャパンに基づき実施される。したがって、我が国全体としての成果（アウトプット）評価は、個々の施策の成果を見るための指標に基づく評価の積み上げによって、総体としてなされるものであると言える。

結果（アウトカム）評価に関しては、例えば我が国の経済発展が進んでいるか（GDP成長率等）、我が国が発信元となって新たなIT文化が現れているかといった我が国全体を大きな視点で見た状況に、それらだけでは情報セキュリティ面の寄与が不明であることから、例えば国民がIT利用に安心を感じているか、情報セキュリティに関するIT障害の発生が減少しているか、といった情報セキュリティ面の取組みの結果という要素等を併せ考えるという手法で見ることが考えられる。しかし、実際には情報セキュリティ面の取組みの結果は、様々な主体ごとの取組み結果の積み上げで見ることがあることから、我が国全体の成果評価指標同様、積み上げによって我が国総体として評価をなす必要があると考えられる。

つまり、成果評価、結果評価ともに我が国全体としての評価は、評価指標各論で行う主体ごとの指標に基づく評価や、必要に応じてなされる現状把握のための補完調査といった要素も加味しながら、総合的かつ分析的になされるべきである。

以下では、分野・主体の特徴に着目しつつ、評価指標各論に関して記述することとする。

第3節 評価等（各論）

1. 考え方

評価指標各論は、対象とする分野・主体に基づいて、以下のとおり大きく2つに分ける。

（1）対策実施四領域

情報セキュリティ政策の主対象である対策実施四領域（対策実施機関としての政府機関・地方公共団体、重要インフラ、企業、個人）については、情報セキュリティ政策に係るPDCAサイクルの基本要素として重点的に評価指標

を設定する⁹。この指標は、第2次基本計画の対象分野の中から、特に注目したい部分について一定期間ごとの状態をみるために重点的に選択し、基本計画の全体領域を隈なく覆うものでは必ずしもない。

なお、評価等に当たっては、主体の特性に応じた検討が必要であり、例えば、企業・個人の領域については、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みをはじ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である。

(2) 対策実施四領域以外の分野

上記対策実施四領域以外の分野（例：横断的な基盤の形成四領域など）については、例えば情報セキュリティ人材育成や国際対応など、評価指標を設定することが必ずしも容易ではない。したがって、これらの分野は、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。

なお、基本計画においては、具体的な施策の実施プログラムを「年度計画（セキュア・ジャパン20XX）」として策定するとともに、その実施状況とともに評価し、公表を行うこととされている¹⁰。内閣官房情報セキュリティセンターは、これに基づき、年度計画のすべての施策について、その進捗状況を半年ごとに把握することとしていることから、これも点検段階（C）の仕組みとして活用していくこととする。これらは、基本計画全体の成果評価指標として貢献できる性格を有するとともに、個々の進捗状況の把握結果は個別の分野において結果評価指標を補完するものである。

以上を踏まえ、以下では、対策実施四主体の評価指標について述べることとする。

⁹ なお、地方公共団体に関しては、政府機関そのものではなく、重要インフラの一分野として様々な取組みを進めており、評価指標についても重要インフラの中の一部として見ることとする。

¹⁰ 第2次情報セキュリティ基本計画69頁（第4章第3節（1）「年度計画」の策定とその評価等を参照。

2. 対策実施四領域に関する評価指標¹¹

(ア) 政府機関・地方公共団体¹²

(評価指標の考え方とその活用の枠組み)

政府機関における情報セキュリティ対策は、(i)各府省庁が政府機関統一基準に準拠した省庁対策基準に基づくP D C Aサイクルを持続的に進め、また(ii)各府省庁の対策実施状況の評価や政府機関統一基準の適時・適切な見直しといった要素も含め、政府全体として情報セキュリティ対策の状況を見るP D C Aサイクルが推進されることが基本となっている。そのため、内閣官房情報セキュリティセンターは、各府省庁と政府全体の2つのP D C Aサイクルが確実かつ自律的に回っていることを確認するとともに、それらの改善に活用が可能な評価指標を設定する。

(「情報セキュリティに係る年次報告書」に係る評価)

第2次基本計画では、それぞれの政府機関において「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。)を作成することとしている。作成された情報セキュリティ報告書は、最高情報セキュリティ責任者が情報セキュリティ政策会議の下に設置されている「情報セキュリティ対策推進会議」等の場において報告し、公表される。また、各政府機関における情報セキュリティ対策のバランスを確保するとともに、一層の充実・向上を推進する観点から、内閣官房情報セキュリティセンターは、各政府機関が作成した情報セキュリティ報告書に係る評価等を行い、その結果を情報セキュリティ政策会議に報告することとしている。

情報セキュリティ報告書については、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」において、情報セキュリティ報告書作成のためのガイドライン、政府機関における評価等の考え方等が示されており(2009年9月11日とりまとめ)(別添2)これに基づき、2011年度までに段階的に取組みを完全実施する。

そのため、2011年度からは、各府省庁の情報セキュリティ対策の評価は情報セキュリティ報告書に係る評価等にプロセスを一本化する。

(補完調査)

例えば、突発的なIT障害など緊急時対応等の対策については、現時点で

¹¹ 第2次基本計画に掲げられる2012年の姿と評価指標の関係については、評価指標は、本来的には実際の状況が姿にどの程度近付いたかを測るためのものである。しかし、実際は指標化が困難な項目が存在し、また、例えば指標化したとしても企業や個人に関する指標はデータ等の収集が容易ではないというように、主体毎に状況が異なっている。したがって、こういった点について柔軟に対応を行うことが不可欠であり、姿の各要素、各項目と指標との関係は全てが1:1対応となるわけでは必ずしもない。これらの課題については、例えば指標総体として姿総体を見ることや、分析を加えた上で他の指標の結果から当該姿の項目の状況を判断すること、さらに補完調査で補うことなどの方法で対応を行うべきである。

¹² 脚注9を参照。

はそれに対応する指標がとり難いものが存在することから、こういった分野に関しては、必要に応じて補完調査をもって状況把握を行い、分析を通じて課題点を明らかにする。

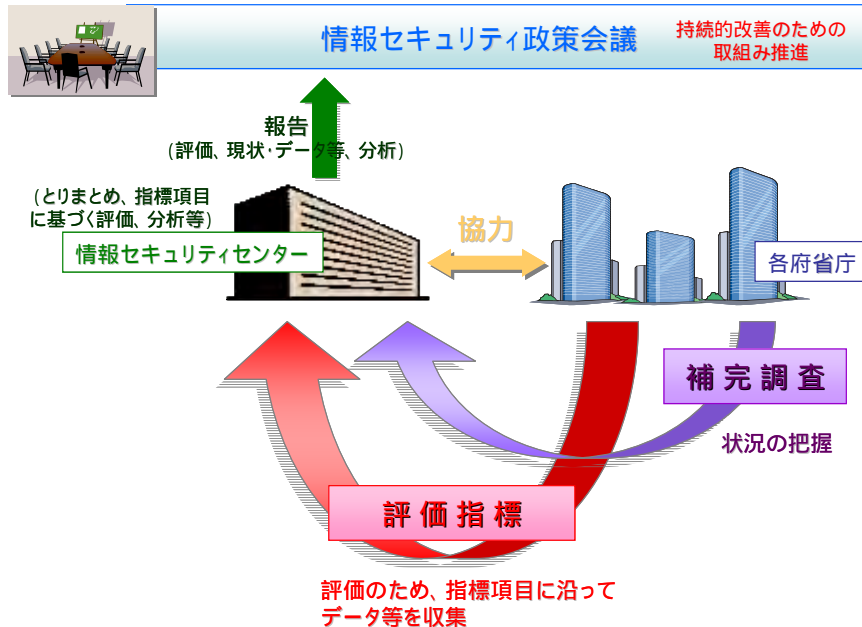


図 3 評価指標に基づく評価及び状況把握のための補完調査

(イ) 重要インフラ

重要インフラの情報セキュリティ対策については、第2次基本計画及びその具体的取組みについて定めた「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」(以下「第2次行動計画」という。)に従って、官民の緊密な連携の下で、情報セキュリティ対策の強化を目指しているところである。

重要インフラ分野では、第2次行動計画に基づく取組みを着実に進め、また継続的に取組みを改善していくために、その進捗状況についての評価・検証を行うこととしている。対策実施四領域の重要インフラにおける点検段階(C)は、第2次行動計画に示された評価・検証の枠組みに従って行う。別添3として、第2次行動計画における評価・検証と見直しについて添付する。(『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』 評価・検証と見直し)

(ウ) 企業

企業の対策実施領域においては、政府の役割は、(i)政策により、各主体の情報セキュリティ意識を高めること、(ii)各主体が自主的に行う情報セキュリティ対策を支援するなど環境を整備すること、である。言い換えると、

この対策実施領域が政府機関、重要インフラといった他の対策実施領域に比べて巨大な母数を抱え、かつ、多種多様な主体の集合体であるために一律の対策を設定することが困難であること等を踏まえ、企業に対しては、環境整備等の間接的な働きかけを行い、各主体が自律的・継続的に取り組んでいくよう対策を促していくことが、政府の施策の中心となる。

したがって、この対策実施領域における評価指標に関しては、すべての主体にわたる詳細な調査を行うよりは、いくつかの既存のデータを収集し、それぞれのデータの特性を考慮しつつ企業全体の傾向を分析する方法により実態を把握することが適当であり、このように対策の浸透の度合いを評価する。

ただし、政策の直接的な作用として対策の浸透が図られたのかについては、その因果関係・相関関係を明確にすることは容易ではない。そのため、評価にあたっては、対策の浸透度合いの実態を把握するとともに、脅威等の周辺情勢や或いは経済状況の変化に伴うIT投資全体の推移の影響等も勘案し、総合的かつ分析的に行う。

具体的な指標に関しては、個人に関する指標とともに、別添4として添付する。

(エ) 個人

個人の対策実施領域においては、企業と同様に、環境整備や広報啓発・情報発信等を行い、各主体が自律的・継続的に取り組んでいくよう対策を促していくことが、政府の施策の中心となる。

したがって、この対策実施領域における評価指標に関しては、すべての主体にわたる詳細な調査を行うよりは、いくつかの既存のデータを収集し、それぞれのデータの特性を考慮しつつ個人全体の傾向を分析する方法により実態を把握することが適当であり、このように対策の浸透の度合いを評価する。

個人分野での取組みの対象は巨大な母数を抱える多種多様な主体の集合体である。実態の把握にあたっては、広報啓発・情報発信等を中心とした施策の効率化へ向けた改善等に資するため、既存データの収集において可能なものについては属性(例えば、性別、職業、年齢、IT利用・活用の習熟度・経験等)ごとの実態を把握する必要がある。

具体的な指標に関しては、企業に関する指標とともに、別添4として添付する。

第3章 評価等の結果を受けた持続的改善のあり方

第1節 評価指標等を用いた持続的改善のあり方（基本的考え方）

ここでは、第1章第2節（4）に基づき、情報セキュリティ政策のPDCAの改善処置段階（A）すなわち評価指標に基づく評価や補完調査に基づく状況把握及び分析等の結果を受けた持続的改善のあり方について述べることとする。

点検段階（C）の結果を受けて情報セキュリティ水準を向上させるには、

（i）点検の結果を踏まえ、どのような対策を引き続き又は新たに行うべきか検討を行い、次期の計画段階（P）に必要な内容を反映すること、

（ ）点検の結果を踏まえ、対策実施主体の取組みの持続的な改善が進むよう情報セキュリティ政策会議が必要な取組みを推進すること

の二点が検討されるべきである。

なお、評価等の結果やそれを踏まえた次の段階の取組みを我が国におけるあらゆる主体が目にすることで、「気付き」を促し、その結果、自身の情報セキュリティ対策の見直しや再確認等につながり、情報セキュリティ水準向上に向けた取組みがより促進されることが期待される。

第2節 持続的改善の方法

1．次期計画への反映

持続的改善の仕組みを実効あるものとするためには、上記のとおり、点検結果を踏まえ、必要な対策を次期の計画段階（P）に具体的に反映することが不可欠である。このため、情報セキュリティ政策会議は、内閣官房情報セキュリティセンターからの評価等の結果に関する報告を踏まえ、取組みが不十分と認められる事項、更なる改善が期待できる事項及び新たに明らかになったリスク、に対処するために必要な施策を、年度計画及び基本計画に反映するように努めることとする。

なお、こうした反映作業については、年度計画への反映は毎年行われるとともに、基本計画への反映は、原則、3年に一度行われることとなる。

2．持続的な改善のための取組み推進

情報セキュリティ政策会議は、内閣官房情報セキュリティセンターから評価指標に基づくデータ及び評価等の結果について報告を受け、これを踏まえて、取組みが不十分と考えられる事項、更なる改善が期待できる事項及び新たに明らかになったリスクに関し、各府省庁が効率的かつ効果的な対応を行うことができるよう、必要な取組みを推進することとする。具体的には、例えば内閣官房情報セキ

セキュリティセンターに対し、各府省庁へのノウハウの提示といった支援を講ずるよう求めること、政府機関統一基準の活用を通じて各府省庁の効果的な対応を促すこと、各府省庁の情報セキュリティに関する取組みをPRするための情報発信を行うこと、各府省庁が政策を検討・実施する上で参考となる情報提供を行うことなどが挙げられる。

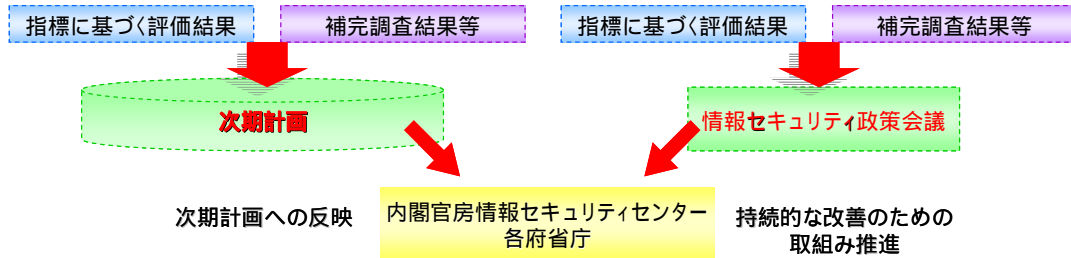


図 4 評価指標等を用いた持続的改善

別添

『第 2 次情報セキュリティ基本計画』(抄)

第 2 章 第 2 次情報セキュリティ基本計画における基本的考え方と 2012 の姿

第 2 節 2012 年の姿

以下においては、第 2 次基本計画に基づく取組みを 3 年間進めることで、我が国の姿が計画期間終了後の 2012 年においてどのような姿となっているか述べる。ここにおいても、2009 年の状況と同様、対策実施 4 領域及び横断的な基盤 4 分野の枠組みにのっとり述べる。なお、情報を預ける側の主体については便宜的に「対策実施 4 領域」の という形で記述する

(1) 対策実施 4 領域

政府機関・地方公共団体

[政府機関]

今後、行政分野への IT の活用により、国民の利便性の向上と行政運営の簡素化、効率化、高度化等を推進していく中で、安全で安心な電子政府に対する国民からの関心はより高まり、情報セキュリティに対する要求は一層高度なものとなっていく。このため、政府機関は、国内外の様々な組織にとって模範となるような情報セキュリティ対策を実施し、国民からの信頼に応えることができる安全かつ安心で効率的な行政運営、行政サービスの提供を行うことが可能な情報セキュリティ水準を確保していくことを目指して最大限の努力を行う。

このような将来像を目指すためのマイルストーンとして、第 2 次基本計画の下で、政府機関においては 2012 年時点で以下のような「姿」を実現することを目標として、関係者は今後の取組みを進めていく。

第一は、『政府機関における情報セキュリティガバナンス¹の確立に向けた組織・体制の強化』である。2012 年には、全ての政府機関において能動的に情報セキュリティ対策に取り組む体制を確立するとともに、政府全体を通じて情報システムに情報

¹ 本基本計画において、政府機関に関して目指す情報セキュリティガバナンスとは、政府機関における内部統制の一環として、情報セキュリティ対策が効果的に推進されるような内部統制を確立することを意味する。

セキュリティ対策が適切に組み込まれる仕組みを構築することにより、政府機関における情報セキュリティガバナンスの確立に向けた合理的な取組みが進展している。こうした体制の下で、政府機関において、情報セキュリティ人材の育成・確保等に向けた対策が計画的に推進され、適切な情報セキュリティ対策を適時に行うための取組みが、予算面の対応も含め進んでいる。また、技術面の知見を蓄積・活用する仕組みの構築も推進されている。

第二には、『政府機関における事後対応力の強化』である。2012年においては、各政府機関が保有する情報システムの災害・障害時の対応方針が、当該情報システムが支えている行政の優先度や重要性等に基づいて決定され、必要なシステムについては事業継続計画が策定されているなど、事後対応にも十分配慮した対策が進展している。また、万が一、事故等が発生した場合に備え、緊急時の対応及び復旧を念頭においた関係機関の連携体制の強化が図られている。

[地方公共団体]

第2次基本計画の下で、政府は各々の地方公共団体において、また幅広い行政分野全体において、望ましい情報セキュリティ対策が実施されることを目指して最大限の努力を行う。

結果、情報セキュリティに関連して、地方公共団体が直面する社会の状況は、2012年には以下のようになっていると考えられる。多くの地方公共団体においては、人口減少や厳しい財政状況の下、セキュリティも含めた情報システムに対する投資を現行水準で維持することは、容易ではなくなりつつある。このため、地域間での取組みの連携など、一定のコストで必要な機能やセキュリティを効率的に確保する手法が積極的に模索されている。地方公共団体の行政分野は相当幅広いものであることから、望ましい情報セキュリティの確保が様々な分野において強く求められていることに加えて、地方分権の進展によって、地方公共団体が自ら、情報セキュリティへの取組みをより一層積極的に行うことが望まれている。

2012年のこのような社会において、地方公共団体の情報セキュリティの取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『地方公共団体の規模によらず、また幅広い行政事務全般にわたっての情報セキュリティ対策の進展』である。2012年には、国、地方を問わず、官、民、NPO等が小規模な市町村も含めた地方公共団体の取組みを応援するべく協力体制を構築しつつある。こうした体制の下、地方公共団体では規模に応じた対策が進展し、

様々な制約によって対策が遅れている小規模な自治体を含め、おおむね全ての地方公共団体で望ましい対策が実施されている状況にある。また、特に、小規模な地方公共団体の対策促進のためには、効率的な取組み手法が確立されることが望ましいところ、成果が実証されている取組みを効率的に実施する手法が確立しつつある。さらに、複数地方公共団体間での対策の連携など、限られたリソースの下で効率的な取組みを進める手法が積極的に模索されている。

また、2012年には、国家行政組織と地方公共団体の担当組織の間での個別の関係も踏まえながら、地方公共団体独自では手が届きにくい分野においても、情報セキュリティに係る取組みが進展している。

第二に、『情報セキュリティの観点から地域で行われる活動の活発化』である。2012年には、地方公共団体が、情報セキュリティの観点から地域で行われる活動を促進できる環境が構築されている。結果、地域において、情報セキュリティ対策推進の中核を担うことができるような知識を有する人材が育つ土壌ができてきている。

重要インフラ

政府は重要インフラの領域については、第2次行動計画を別途策定し、重要インフラ事業者等がとることが望ましい自主的な対策と、内閣官房を中心とした政府及び関係機関等において実施することが望ましい施策からなる体系的な枠組みを整理している。政府は、第2次行動計画に示された官民連携の枠組みによって、重要インフラにおけるIT障害²の発生を限りなくゼロにすることを目指し、重要インフラにおけるIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう重要インフラを防護するとともに、重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図る。

重要インフラ分野の情報セキュリティ対策は、第2次行動計画にまとめられているとおり、重要インフラ事業者等の自主的な取組みを含むものであり、2012年における姿を設定して重要インフラ事業者等に義務的な取組みを求めることは適当でない。そのため、実現が期待される将来像を示す事によって、重要インフラ事業者等をはじめとした関係主体の取組みの方向性を示すこととする。

なお、第2次行動計画に基づく情報セキュリティ対策に取り組む関係主体は「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標として取組みを進めることとしており、政府はこの目標の下、以下の将来像の実現に向けて最大限の努力を行う。

² 第2次行動計画においては、「IT障害」を「重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、ITの機能不全が引き起こすもの」と定義している。

第一に、『政府機関や重要インフラ事業者等の主体的な取組み及び連携の確立』である。情報セキュリティ対策に取り組む各関係主体は、各々守るべき重要インフラサービスと維持すべきサービスレベルを踏まえて、自らがなすべき必要な対策を理解している。各関係主体は自らの置かれている状況を正しく認識しており、自らの活動目標を主体的に定めている。各関係主体は各々必要な取組みを進めており、これについて定期的に自己検証を行っている。また、他の関係主体の活動状況を把握し、互いに自主的な協力をすることができる。

関係主体はIT障害発生時の対応において、IT障害の規模に応じて、誰がどのような情報を集積しているか、誰とどのような情報を共有すべきか、また自らは何をなすべきかを理解している。自らの自主的な対応に加えて、必要に応じて他の関係主体と連携を図り統制の取れた対応を取ることができる。

第二に、『IT障害に関する情報共有の価値の普遍化』である。重要インフラ事業者等においては、いわゆる「情報セキュリティガバナンス」という考え方が十分に浸透し、情報セキュリティ対策は単に情報システムの保守運用の観点からだけでなく、企業経営の観点からも検討が必要であることを理解しており、システムの保守と企業経営のそれぞれの責任者が適切に関与する体制を有するようになっている。また、情報セキュリティ対策の対外的な説明に努めている。また、社会基盤の情報セキュリティ対策の強化のためには可能な限り情報共有するという姿勢が積極的に評価される価値観が醸成されている。

この体制において、重要インフラ事業者等は自らの事業におけるIT障害の発生は隠すべきものではなく、事業者等内の対策に取り組む関係者間で共有すべきものであるという認識を有している。対策に取り組む関係者はIT障害の発生状況等の情報を把握できており、必要に応じて当該情報を分野毎のセプターやセプターカウンシル等の第1次行動計画の下で構築された情報共有の枠組みを通じて外部の関係主体と共有し、公式又は非公式の連携を行うようになっている。

第三に、『環境変化への機敏な対応体制の常備化』である。政府の諸施策、関係主体間のリスクコミュニケーション、国際連携・協調等を通じて、重要インフラの情報セキュリティ対策に資する国内外の多様な情報が内閣官房に寄せられるようになっている。内閣官房はこれを踏まえて関係主体との連携を図り、より効果的な対策を進めるための総合調整機能を発揮している。

特に、特異重大な脅威やIT障害に係るリスクについての認識が得られ、これへの対処が重要インフラ事業者等だけでは困難な場合は、内閣官房、重要インフラ専門委員会、セプターカウンシルの連携によって、解決策の検討とその実現に向けた調整が速やかに実施されるようになっている。

企業

第2次基本計画の下で、政府は企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指して引き続き最大限の努力を行う。

結果、情報セキュリティに関連して、企業が直面する社会は、2012年には以下のようになっていると考えられる。

いわゆる「団塊の世代」の退職などを受けて労働力人口は減少しており、事業活動の更なるIT化によって効率的で労働生産性が高いビジネス運営モデルへの転換が始まっている。このため、経営管理のITへの依存度が更に高まり、情報セキュリティが経営に占める重要性も高まってきている状況にある。また、海外の拠点も十分に活用しながら効率的なビジネス運営を行う必要が更に高まり、且つグローバル化に伴う世界規模での最適生産のために企業活動の細分化、専門化がさらに進展し、海外へのアウトソーシング、直接投資が拡大している。このため、特に関係の深い東アジア地域はもとより、例えばインド、中東地域においても情報セキュリティ対策を徹底し、日系企業にとって安全・安心なビジネス拠点として確保していく必要性が認識され始めている。加えて、我が国経済はグローバルなサプライチェーンマネジメント網の中へ入り、国内企業における情報セキュリティ対策は当然に不可欠のものとなってきている。とりわけ、モノ作りをはじめとして強い国際競争力を有する中小企業における対策推進が喫緊の課題となっている。

2012年のこのような社会において、企業の情報セキュリティの取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『情報セキュリティガバナンス³の経営の一環としての認識の定着と、それに応えられるツールの存在』である。2012年には、企業における情報セキュリティ対策の重要性を経営層も含めて十分に認識するとともに、対策推進のために必要な体制も構築されており、情報セキュリティは財務統制などと並ぶ経営上の重要な要素となっている。情報資産の活用度によって、企業ごとに情報セキュリティガバナンスの重要性が変化することから、情報資産の活用度の高い企業においては、経営層も含めて情報セキュリティ対策の重要性を理解しており、外部監査などを通じて社内のセキュリティ対策について十分に状況を把握している。また、対策にあたっては、コストや利便性とのバランスなども極めて重要であることから、こうした諸要素に配慮がなされた製品やサービスが利用可能となるとともに、対策を促進するための様々な活動が政府や情報関連事業者などの対策支援主体によって積極的になされている。

³ 本基本計画において、企業に関して目指す情報セキュリティガバナンスとは、企業経営の一環として、情報セキュリティ対策を適切に実施することを意味する。

第二に、『「事故前提社会」への対応力強化に向けた緊急対応体制・事業継続性確保等の進展』である。2012年には、企業における情報セキュリティ対策自体の事前の対策が進むとともに、規模が大きい企業や、事業活動における情報セキュリティの重要性が大きい企業を中心に、事後対応の準備も進みつつある。

第三に、『大企業から中小企業にわたった、各企業における適切な対策の進展』である。2012年には、情報セキュリティ対策の進展が十分ではなかった中小企業向けの対策ツールの提供が進むなど、企業の事業規模を問わず、適切かつ必要な対策が行われつつある。

第四に、『国を問わず、日系企業の進出先における情報セキュリティ対策の進展』である。2012年には、海外のビジネス拠点において、顧客情報の漏えいをはじめ、様々な情報セキュリティ上の問題が生じないことが重要であることについて、政府、日系企業が十分に意識し、対策が始まっている。また、我が国政府と海外ビジネス拠点の政府間でもこうした取組みの重要性を共有し、官民も連携を行いながら、企業が安全・安心にITを活用できる環境整備のための取組みを進めている。

個人

第2次基本計画の下で、政府は「IT利用に不安を感じる」とする個人を限りなくゼロにすることを目指して引き続き最大限の努力を行う⁴。

結果、情報セキュリティに関連して、個人が直面する社会は、2012年には以下のようになっていると考えられる。

教育機関や企業におけるITの利用・活用の急速な広がりもあり、青少年から高齢者までの広範な世代がコンピュータに関する知識を有している。これを受けて、個人の日常生活におけるコンピュータの利用は特別なことではなくなっており、大部分の世帯が、ブロードバンド・インターネットサービスを活用している。そして、これに対応するように、情報家電、ゲーム機をはじめとする様々な機器がネットワークに接続できるようになり、人々の生活に密着した多種多様なサービスが広範に提供されている。また、より一層のインターネットを基盤としたサービスの拡大が進むとともに、2011年の地上デジタル放送への完全移行や、ネットワーク機能が強化された新たな移動体通信サービスの広がりにより、様々な双方向サービスが普及し始めている。

⁴ 当該目標は、IT基本法第22条のIT安心利用環境を個人の領域において具体化する趣旨である。個人がITを利用するに際して、リスクに対して鈍感になり、結果、IT利用に不安を感じなくなることを目指すという趣旨ではない。

携帯電話等の人々の生活の中にあるネットワーク利用端末も、より高性能化している。

2012年のこのような社会において、個人が以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『セキュリティ意識の向上を伴う個人のIT利用の拡大』である。個人は、ネットワークサービスをパソコンや携帯電話、テレビ、ゲーム機等から積極的に利用するようになり、生活がよりITに依存するようになっている。同時に、多くの個人は、パソコンだけではなく、組込み型システムを内蔵する携帯電話や家電製品等に関する情報セキュリティ上のトラブルについても認知するようになり、高信頼性を保証する製品が高い人気を持つようになっている。そして、仮にトラブルが発現しても、ベンダー等から提供される情報に基づいて適切に対応できる個人が多数となっている。

第二に、『サービス提供側と利用側である個人の互いにバランスのとれたセキュリティ意識の向上』である。サービス利用時に、個人情報やプライバシー情報を提供しなければならぬ状況が増加し、サービスを運営する企業・組織においては、こうした個人に係る情報の保護についての関心が高まっている。そして、サービスにおける個人情報利用方針、情報保護レベル等のリスクを明示することも始まっている。他方、個人の側では、リスクに関する情報の非対称性、すなわちサービス利用者とサービス提供者の間でのリスクに関する情報量の格差の存在にもかかわらず、情報を提供する利点とリスクを理解した上で、情報提供の可否を判断できる者が増えてきている。

第三に、『リスクを理解しても対策を行わない個人等に関する対応の開始』である。サービス利用におけるリスクを理解した上でも、対策を行わない個人は、一定数存在し続ける。また、情報弱者も一定数存在し続けると考えられる。これに対応するために、サービス提供者、製品提供者は、互いに協力して利用者任せの情報セキュリティ管理を廃し、より責任を持った形でサービスや製品を提供することが取組みの第一歩であると認識し始めている。

情報を預ける側の主体

第2次基本計画の下、社会全体で、合理性に裏付けられたアプローチを追求する中で、政府は、対策情報を預ける側の主体も含めて社会全体が情報セキュリティに係る自身の問題を主体的に考えられるようになることを目指して最大限の努力を行う。結果、情報を預ける側の主体に関して、我が国は2012年には以下のようになっていると考えられる。

第一に、『情報を預ける側の主体全体としての意識の向上』である。啓発活動やモデル契約書の提供などを通じて、当該情報を電子情報として預けることの必要性和万が一の場合のリスクの許容性について、個々の主体が無意識にある程度の注意を払うようになっている。

第二に、『対策知識が十分でなくとも情報を預ける際に安全が確保される技術的発展の実現』である。技術の発展により、意識的な対策をとらなくても預けた情報が保護されるようになっている。[参照：「(2) 情報セキュリティ技術戦略の推進」の2012年の姿]

(2) 横断的な情報セキュリティ基盤

情報セキュリティ技術戦略の推進

社会全体のITへの依存度が高まり、情報セキュリティの対象範囲と重要性が大幅に増すなか、政府は、第2次基本計画の下で、我が国の情報セキュリティ関連技術の研究開発が、世界で最も効果的・効率的に進められる体制となることを目指して最大限の努力を行う。結果、情報セキュリティに関連して、研究開発・技術開発の面で、社会は2012年には以下のようになっていると考えられる。

2012年にはNGN⁵(次世代ネットワーク)やIPv6⁶の普及が進み、固定通信と移動通信の融合が進むとともに、認証、課金処理、権利管理、顧客管理などの機能コンポーネントが連携した安全なポータルが実現して、キャリア以外のサードパーティのサービスの提供が増加している。また、地上波も含めた全てのテレビ放送がデジタルに移行し、通信と放送の融合のメリットを活かしたデータ放送や双方向サービスが広く利用されている。その結果、SaaS⁷やASP⁸をはじめとするネットワーク上のサービスは、企業向け・個人向けともますます多様化し、サービス間の連携による高付加価値化も進んでいる。

このような背景の中、企業では業務の効率化と再構築のために、積極的に電子会議や勤務管理、旅費精算などのネットワーク上のサービスを活用している。生活者も場所や端末の種別などを意識することなく、多種多様なサービスを享受している。オフィスや家庭においては、パソコンや情報家電、ゲーム機などに加えて、照明機器やエアコンといった白物家電も、ホームサーバを経由してネットワークに接続されるよう

⁵ Next Generation Network の略。

⁶ Internet Protocol version 6 の略。

⁷ Software as a Service の略。

⁸ Application Service Provider の略。

になっている。

こうして、利用者の利便性が向上する反面、不正アクセスなどセキュリティの脅威も増大し、計算機や情報のみならず国民の生活全体を如何に守るかが、大きな関心事となっている。また、ネットワーク経由で提供されるサービスが普及し、相互連携するようになることは、業務情報やプライバシー情報、あるいは認証情報などがどこに保管され、どのように流れているかを把握することや、障害発生時の原因の切り分けが困難になることを意味する。このような環境の中で、信頼性の高い製品やサービスをリーズナブルなコストで提供することの重要さが、ますます増している。

さらに、生活の中にITが溶け込むことで、日常的にITを利用する若年層や高齢層が増加し、個人が情報セキュリティ上のリスクにさらされる可能性が高まっている。そのため、機能や自由度の制約と引き換えに、事前に十分検証された情報セキュリティ対策が施されて、安全・安心に使えるタイプの機器が、一つの商品のジャンルとして確立されている。

2012年のこのような社会において、技術戦略の情報セキュリティの取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

具体的には、第一には、『利用者による情報セキュリティ対策が不要な端末や情報家電の提供』である。これまでも、ウィルス対策ソフトや脆弱性修正プログラムなどの手法によるセキュリティ対策や、利用者に情報セキュリティの重要性を認知させる取組みなどが行われてきた。2012年には、啓発活動による利用者の意識の向上への取組みは引き続き継続しつつ、利用者に負担を与えずにセキュリティを確保するとともに、高齢者らの、認識力の衰えなどによるミスや誤認があっても情報セキュリティ上のリスクを防ぐという観点から、例えば出荷段階から情報セキュリティの設定が適切になされ、アクセシビリティに関する規格標準等に配慮した安全で安心な機器やソフトウェア等が提供されている。

第二に、『設計段階からセキュリティを作り込む開発手法の普及と定着』である。2012年には、情報セキュリティは、信頼性や性能のようなソフトウェアやシステムの品質と同じく、設計段階から考慮すべき要素であると広く認識されている。効率的に安全なソフトウェアを開発する手法の確立と、その手法を用いた開発を重ねることによるノウハウと人材の蓄積により、情報セキュリティ対策をすべき対象範囲の拡大への対応や、妥当なコストで脆弱性や重大な欠陥の事前の回避が可能となっている。また、そのことが、例えば、携帯電話やICカードなどの組込み系のような、日本企業が先進的な機器やサービスを提供している分野の製品の重要な付加価値要因となり、国際競争力の源泉となっている。

第三に、『リスクの形式的な表記法や、リスクの評価方式の共通化』である。この

共通化により、ソフトウェアや情報システムのセキュリティに関するリスク情報の迅速な共有が促進されている。また、共通化は、新たな脅威の危険性の客観的な評価や、効率的に安全なソフトウェアを開発する手法の確立や、情報セキュリティ対策の合理性の判断などに大きく寄与している。

情報セキュリティ人材の育成・確保

第2次基本計画の下で、社会全体のIT依存度の高まりを受けて情報セキュリティ人材の重要性が社会で十分に認識され、その業務が魅力的なものとして、優秀な人材が官民を問わず情報セキュリティ分野にすすんで集まることを目指して、政府をはじめ、各主体が種々の取組みを展開する。結果、情報セキュリティに関連して、人材育成・確保の面で、社会は2012年には以下のようになっていると考えられる。

第一に、『政府機関におけるセキュリティ人材のニーズの高まりと対応の開始』である。政府機関においては、情報セキュリティ上の脅威の増加を背景に、情報セキュリティを支える人材に対するニーズや、人材の重要性に関する認識がよりいっそう高まっている。そうした意識の高まりを受けて、政府機関において必要となる情報セキュリティに携わる人材を育成・確保するためのロードマップが描かれるとともに、そのロードマップに従った情報セキュリティ人材の育成・確保が積極的に推進されている。

第二に、『民間企業におけるセキュリティ人材のニーズの高まりと対応の開始』である。民間企業においても、業務効率化のためITへの依存度が更に高まり、もはや企業経営の重要な一部となっている情報セキュリティ対策において、ITの進歩にも対応することのできる情報セキュリティ専門家へのニーズが高まっている。このニーズに対して、政府は情報セキュリティ人材に係る環境整備・基盤整備を行うことで、企業における情報セキュリティ人材の育成・確保を推進している。

第三に、『情報セキュリティに関する能力向上に係る環境整備の進展』である。民間を含めた情報セキュリティ部門においては人材を募る際の要件として、資格の保有を要件や考慮要素とする例も一部で見られ始めている。このように、情報セキュリティ業務に携わる人材が能力を高めることに係る環境整備が行われ始めている。さらに、情報セキュリティ業務に携わる人材の側から見ると、資格保有等によるキャリアアップの道筋が見えやすくなることで、能力を高めることに対するインセンティブが生じている。他方、情報セキュリティに携わる人材を雇用する官民の組織においては、かけがえのない人材として、情報セキュリティに携わる人材を育成する意識が芽生えつつある。

国際連携・協調の推進

第2次基本計画の下で、グローバルなIT安心利用環境を実現するための取組みが国際的に進められているなか、政府は、我が国の官民連携を中心とした取組みが世界最先端・最高のベストプラクティスとして世界に貢献することを目指して最大限の努力を行う。

このような状況下において、情報セキュリティに関連して我が国が直面する世界の状況は、2012年には以下のようになっていると考えられる。ITは世界中で人々の生活にますます浸透し、利用者は国境を気にすることなく様々なコミュニケーションを行っている。結果、ITは、あらゆる主体にとって従来よりも劇的に低いコストで、国境と関係なく革新（イノベーション）をもたらす道具であるとの認識が飛躍的に広まっている。一方で、ITは、悪意ある者が低いコストでグローバルな活動を行うことも可能としている。また、ITを活用した大規模な情報蓄積、業務管理の実現によって、無知や事故がもたらす影響も大規模なものとなり、国境を越えた影響も大きくなっている。

重要インフラの領域においては、規制緩和による事業者間の競争圧力、消費者からの利便性向上の要請を受け、情報システムを利用した事業管理のみならず、消費者との取引においても、ITの利用・活用は更に拡大している。国境を越えるサービスを提供する重要インフラ事業者は、国境を越えた主体間の依存性、接続性の他、複数国の情報セキュリティ政策を考慮に入れる必要性も高まっている。このような状況に対応するため、我が国は、早期から対応を行ってきた他国政府と協力し、事業継続性確保のための最新のベストプラクティスを、国内環境に合致する形で還元するべく努力を行っている。また、第2次行動計画を中心とした我が国の官民連携体制について、その優れた点を世界に発信していく取組みを行うなど、国内外の取組みの有機的な連携を進めている。

企業の領域においては、グローバル化に伴う企業活動の細分化、専門化が更に進展し、海外へのアウトソーシング、直接投資が拡大している。製品・サービスは、少なからぬ部分がITを活用したグローバルなサプライチェーンを経て製造、提供されている。経済活動は国家の領域を超えて行われており、世界における情報セキュリティ対策の推進という観点から、グローバル企業の果たす役割は拡大している。

なお、近年のコーポレートガバナンスの要請や会計監査に関する統制の強化に見られるように、企業の経済活動に一定の規制・統制が要求される場合、情報セキュリティの領域においても相応の規制・統制が求められる可能性は否定できない。しかし、政府は、企業の事業活動のグローバル化を支援・促進することを重要な課題として捉え、情報セキュリティに関する国境を越えた政府間の連携、官民の連携を通じて、情

報セキュリティに関する規制・統制が過度なものとならないよう適切に調整を行うことにより、企業が安全・安心にITを活用できる環境整備を実施する努力を継続している。

個人の領域においては、世界各国で、ITを利用・活用する人口が若年層を中心に増加している。世界の個人ユーザーは、ITを活用して無限大の知識にアクセスすることが可能となり、個人が国家の領域を超えて、自由に社会的、文化的、政治的活動を行うことが容易になっている。一方で、ITの利用・活用が急拡大する国においては、ITの抱えるリスクについて無防備なユーザーが急増することとなり、これに対応するためにITの利用・活用に対する規制の声が急速に高まることも考えられる。このような状況下で、我が国は、自由と統制のバランス、官民のバランスの取れた情報セキュリティ政策をグローバルに展開する努力を継続している。

このように、ITの普及は、世界的に個々の主体の自由な発想・活動を更に促進し、新たな創造や革新を可能としていく。一方で、ITは、その利便性を維持するために、政府が最低限果たすべき役割の重要性を高めていく性質を有する。

2012年には世界がこのような状況となることを認識しながら、情報セキュリティの国際連携・協調面の取組みが、以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『グローバル化へ対応し、世界と連動した政策の実施』である。政府は、情報セキュリティに係る国内の政策が、企業をはじめとする個々の主体のグローバルな活動にも影響を与えることを理解している。そして、各国政府、国際機関の動向を十分に注視し、必要な要素を我が国の政策に反映する取組みを行っている。同時に、我が国のベストプラクティスと言える政策が、関係の深い国・地域、ひいてはグローバルに採用され、我が国の主体が国内で進める情報セキュリティの取組みを以て、グローバルに必要とされる取組みを進めていると言える環境作りをしている。このように、我が国では、国内外の取組みが有機的に連動している。

第二に、『アジアにおける情報セキュリティ分野の取組みへのイニシアティブの発揮』である。第1次基本計画同様、内閣官房情報セキュリティセンターはPOCとしての機能を強化し、情報セキュリティ政策・オペレーションに関する国際的な情報連携の要としての活動を行っている。特に、欧米の機関との関係において、情報セキュリティに関するアジアの玄関としての地位を確立するとともに、アジアにおける情報セキュリティ先進国として位置付けられている。

第三に、『情報セキュリティ文化の醸成へ向けたグローバルレベルでの貢献』であ

る。情報セキュリティの推進には、情報セキュリティの政策担当者や情報セキュリティが事業の信頼に直結する企業のみならず、より広い政策分野の担当者やIT利用者全体の意識向上が不可欠である。このため、我が国政府は、国際機関や他国政府と協力しながら、グローバルレベルでの情報セキュリティ意識の向上のための取組みを行っている。

犯罪の取締り及び権利利益の保護・救済

第2次基本計画の下で、政府は、犯罪の取締り及び権利利益の保護・救済が進むことによりサイバー空間が安全にかつ安心して利用できるものとすることを目指して引き続き最大限の努力を行う。

このような努力を進めるなか、我が国が直面する社会の状況は、2012年には以下のようになっていると考えられる。

ITは、国民生活の利便性を向上させ、社会経済基盤として機能している。このため、サイバー犯罪や権利利益の侵害がひとたび発生すると、国民に直接かつ深刻な影響が及びかねない状況となっている。このような状況の中、サイバー犯罪もその手口を一層高度化・多様化させており、サイバー空間の安全性・信頼性を維持するためには、犯罪の取締りを的確に推進していくことが不可欠な状況となっている。

このため、サイバー犯罪の取締りが強力に進められている。

また、国民の間では、サイバー犯罪の未然防止や被害拡大防止、情報流出対策等の重要性に対する意識が従来以上に高まっており、個人、社会の両面から積極的に犯罪抑止や情報セキュリティへの取組みが行われている。

さらに、各種情報セキュリティ技術の開発・普及が進み、サイバー空間の安全性・信頼性を向上させるための選択肢も増加している。

2012年のこのような社会において、サイバー犯罪の取締りや権利利益の保護・救済に関する取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『犯罪の取締りの一層の強化』である。サイバー空間の安全・安心が確保されるためには、サイバー犯罪を迅速かつ的確に検挙するとともに、犯罪抑止のための対策を進めていくことが大前提となる。このため、政府は、犯罪の取締りのための施策を強力に推進している。あわせて、増大するサイバーテロの脅威に備えるための基盤整備についても推進している。

第二に、『対策に向けた意識の高揚と知識の充実』である。犯罪や権利利益の侵害に強いIT社会を構築するためには、国民一人ひとりが被害に遭わないための知識を身に付け、それを実践することが大切である。このため、政府は、効果的な広報啓発の推進に努めている。

第三に、『権利利益の保護・救済のための基盤の整備』である。国民が安全にかつ安心してサイバー空間を利用するためには、サイバー空間上で権利利益が保護されていることが不可欠である。政府は、基本的人権に十分配慮しつつ、サイバー空間の権利利益の保護・救済のための基盤の整備に向けて引き続き努めている。

**『情報セキュリティ報告書専門委員会報告書
～能動的な政府機関の情報セキュリティ対策のために～』(抄)**

第 1 部 情報セキュリティ報告書作成のためのガイドライン

目的

政府機関においては、第 1 次情報セキュリティ基本計画の下、すべての政府機関において、政府機関の情報セキュリティ対策のための統一基準（以下、「政府機関統一基準」という。）が求める水準の対策を実施していること等を目指して、各府省庁の PDCA サイクル及び情報セキュリティ政策会議による評価・勧告を中心とした政府機関全体の PDCA サイクルという 2 階層の PDCA サイクルを構築し、情報セキュリティ対策を促進するため様々な取組を推進してきた。第 2 次情報セキュリティ基本計画においては、この取組を定着、浸透させ、すべての府省庁が能動的に情報セキュリティ対策に取り組む体制の確立を目指し、各府省庁が情報セキュリティ報告書を作成し、公表することとしている。

情報セキュリティ報告書の作成及び公表は、各府省庁における情報セキュリティ対策の取組状況等について明らかにし、国民への説明責任を果たすことにより、行政事務全般について国民からの信頼を向上させることを目的とする。また、情報セキュリティ報告書を作成する過程において、各府省庁が改めて自らの情報セキュリティ対策について見直しを行い、更なる向上が図られる効果を期待する。

第 1 部においては、各府省庁の情報セキュリティ報告書の記載内容のバランスを確保する観点から、各府省庁が情報セキュリティ報告書を作成するためのガイドラインとして、情報セキュリティ報告書の作成から公表までの手順、情報セキュリティ報告書への記載事項の具体的項目等を示している。

なお、本ガイドラインに示す、情報セキュリティ報告書の作成から公表までの手順及び記載事項の具体的項目については、政府機関全体における情報セキュリティ対策の浸透・定着、技術や環境の変化等を踏まえ、必要に応じて、NISC において見直すものとする。

情報セキュリティ報告書の作成から公表までの手順

各府省庁の情報セキュリティ報告書作成責任部署は、最高情報セキュリティアドバイザーの積極的な関与の下、情報セキュリティ報告書（案）を作成する。

作成した情報セキュリティ報告書（案）は、最高情報セキュリティアドバイザー連絡会議（仮称）において比較・評価等を行い、同会議からの助言等を踏まえ、内容の

見直しを行う。

内容の見直し後、情報セキュリティ委員会において情報セキュリティ報告書を決定し、最高情報セキュリティ責任者が、情報セキュリティ対策推進会議等に報告した後、公表する。

情報セキュリティ報告書の構成のひな形

情報セキュリティ報告書の記載事項の具体的項目を以下、構成のひな形として列挙する。各パートは、基本的に、「項目名」₁、「目的」₂、「記載内容（必須項目・任意項目）」及び「留意事項」で構成される。

必須項目は、各府省庁が情報セキュリティ報告書を作成するに当たり、その内容を記載することが必須の事項である。

任意項目は、各府省庁が情報セキュリティ報告書を作成するに当たり、その内容を記載することが任意の事項である。

なお、情報セキュリティ報告書の作成に当たっては、以下の共通的な留意事項を参考とすること。

- ・ 情報セキュリティ報告書の作成に当たり、項目名又は記載順番の変更を行うことや、複数の項目をまとめて記載することは差し支えない。
- ・ 必須項目及び任意項目にかかわらず、各府省庁において実施した独自の情報セキュリティ対策については、積極的に記載することが望ましい。
- ・ 国民に向けて公表することにかんがみ、国民が分かりやすい記述及び構成とるように努めること。
- ・ セキュリティ脆弱性についての類推が可能となるような内容（例えば IP アドレス）や特定の製品名等については、情報セキュリティの維持・確保の観点から、記載しないよう注意すること。
- ・ 第三者組織を利用した監査等を実施した場合は、その結果を情報セキュリティ報告書の作成に積極的に活用することが望ましい。

1 最高情報セキュリティ責任者によるメッセージ及び当該年度の総括

1.1 最高情報セキュリティ責任者からのメッセージ

（目的）

各府省庁の情報セキュリティ対策の最高責任者である最高情報セキュリティ責任者から、当該府省庁における情報セキュリティ対策の取組、考え方等について、国民に対してメッセージを発信することにより、情報セキュリティ対策に関する当該府省庁の姿勢を明らかにすることを目的とする。

（記載内容）

【必須項目】

(1)最高情報セキュリティ責任者からのメッセージ

当該府省庁における情報セキュリティ対策の取組、考え方等について、最高情報セキュリティ責任者から国民へのメッセージを記載する。

(2)最高情報セキュリティ責任者名等

最高情報セキュリティ責任者の役職及び氏名を記載する。

(3)メッセージ発出年月

メッセージ発出年月を記載する。

(留意事項)

情報セキュリティ報告書は、国民に対する説明責任を果たす観点から作成することにかんがみ、一般論のみではなく、時勢を踏まえた記述を加えることが望ましい。また、最高情報セキュリティ責任者が自らメッセージを発信していることを強調するために責任者の写真を掲載すること等も考えられる。

1.2 当該年度の総括

(目的)

各府省庁における当該年度の情報セキュリティ対策を総括することを目的とする。

(記載内容)

【必須項目】

(1)当該年度の評価

当該年度の情報セキュリティ対策について、最高情報セキュリティ責任者による自己評価を記載する。

(2)翌年度の目標

翌年度重点的に取り組むべき目標を記載する。

(留意事項)

情報セキュリティ報告書に記載する以下の事項を踏まえ、最高情報セキュリティ責任者自らが評価した結果についての総括を記載すること。なお、本文と重複した内容が多くならないように、内容を引用する場合は簡潔に記載すること。

- ・ 当該年度の重点事項
- ・ 省庁対策基準に関する自己点検結果
- ・ 情報システムごとの状況
- ・ 教育・啓発
- ・ 調達・外部委託
- ・ その他取り組んだ事項
- ・ 情報セキュリティに関する障害・事故等の報告

2 報告の基本情報

(目的)

情報セキュリティ報告書が対象とする期間、組織等について明記することにより、

説明範囲を明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)府省庁の概要

所掌事務、導入している主な情報システムなどについて、府省庁の業務の全体像が分かるように、概要を簡潔に記載すること。

(2)対象とする期間

情報セキュリティ報告書の対象とする期間は原則として年度(4月1日～3月31日)とし、前年度との間で間隙が無いようにすること。ただし、関連する事項があればその前後の期間の事項を含めることも可能とする。

(3)対象とする組織

情報セキュリティ報告書の対象とする組織について簡潔に記載する。地方支分部局等も含めた全組織とすることが望ましいが、対象としない組織がある場合は、明確に記載する。なお、所管する独立行政法人等については、報告の対象外とする。

(4)対象とする情報

情報セキュリティ報告書の対象とする情報を記載する。ただし、政府機関統一基準で対象とする情報(情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。)は必須とするが、その他の情報については、必要に応じて記載すること。

(5)責任部署

情報セキュリティ報告書の責任部署名又は連絡先となる部署を明記する。担当となる係名まで記載することが望ましい。

【任意項目】

(6)府省庁の行政事務従事者数又は定員数

情報セキュリティ報告書の対象となる行政事務従事者数又は定員数を記載する。対象外となる者がいる場合は、その理由、人数等を記載する。

(7)情報システム予算額

府省庁の情報システム予算総額を記載する。

(留意事項)

図表などを用いて分かりやすく表現する工夫をすること。

3 情報セキュリティ対策の枠組み

(目的)

各府省庁の情報セキュリティ対策の体制等、情報セキュリティ対策に係る府省庁全体の枠組みが整備されていることを明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)情報セキュリティ対策に関する文書体系

府省庁にて定めている情報セキュリティ対策に関する文書（基本方針、省庁対策基準、規程類等）の概要及びそれらの文書の対応関係を記載する。府省庁の情報セキュリティ対策の枠組みの中で各文書がどのような位置付けにあるかを明記する。

(2)情報セキュリティ対策の推進体制

府省庁における情報セキュリティ対策の推進体制を記載する。府省庁の情報セキュリティ対策の枠組みの中で各責任者及び推進部署がどのような位置付けにあるかを明記する。

なお、情報セキュリティ対策に係る組織体制や推進部署の体制については、以下の事項を参考に、記載する。

・ 情報セキュリティ対策に係る組織体制

最高情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者、情報セキュリティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者、最高情報セキュリティアドバイザーなど、省庁対策基準に定める情報セキュリティ対策に係る組織体制について、その整備状況、意志決定の枠組み、役割、活動状況等を記載する。

地方支分部局等が設置されている府省庁においては、地方支分部局等における情報セキュリティ対策に係る組織体制も記載する。

また、府省庁内横断的な連絡会議等の情報セキュリティ対策に係る会議体の体制、役割（例えば、幹部への報告とその後の対応、環境変化に対する対応といった役割等）、活動状況等を記載する。

・ 情報セキュリティ対策に係る推進部署の体制

IT 部門及び情報セキュリティ対策に係る総合調整を行う具体的な推進部署名と体制、役割、活動状況等を記載する。また、推進部署の担当者の数、業務平均経験年数等を記載する。

(3)監査等

監査等について、以下の事項を参考に、実施している内容を記載する。

・ 情報セキュリティ監査計画の策定、監査報告の実施

当該年度の情報セキュリティ監査計画の概要について記載する。監査計画は、過去に実施した監査結果で明らかになった課題及び問題点を踏まえたものとなっていることが望ましい。

また、当該年度の監査報告の実施状況等（最高情報セキュリティ責任者への説明、報告等）を記載する。

- ・ 監査報告書に基づく対応の実施
監査報告書の内容を踏まえ、改善のための以下 a～e のような取組状況等を記載する。
 - a. 指摘事項に対する、最高情報セキュリティ責任者による対応実施の指示
 - b. 同種の課題及び問題点の有無について、最高情報セキュリティ責任者による確認の指示
 - c. 改善を指示された事項について、情報セキュリティ責任者による対応計画（達成可能な対応目標の設定を含む。）の作成と報告
 - d. 情報セキュリティに関する文書について、情報セキュリティ責任者による妥当性評価及び必要に応じた見直しの指示
 - e. 上記 a～d の見直し指示等に基づき、どのように対応したか
- ・ 第三者組織による監査・検査等
 - a. 監査について、客観性及び専門性をより向上するために第三者組織を利用した場合は、内部監査との関係を含めて記載する。
 - b. 情報システム脆弱性検査
情報システムに対する脆弱性検査を実施した場合は、第三者組織の利用の有無、検査対象、結果等を記載する。

【任意項目】

(4)情報セキュリティ対策の予算額

情報セキュリティ対策の予算として執行した総額、情報システム予算額に占める割合等を記載する。

(5)政府機関統一基準と省庁対策基準の差異

省庁対策基準において、政府機関統一基準に特に加えて基準としている事項等、差異として特徴的なものがある場合は、記載する。

(6)業務・システム最適化における取組の管理

各府省庁の PMO（プログラム・マネジメント・オフィス）において、業務・システム最適化の中で、情報システムの安全性・信頼性を確保するための取組を、どのように管理しているか（例えば、業務・システム最適化の企画、設計・開発段階における情報セキュリティ対策要領の作成、情報セキュリティ要件定義の作成等の管理）を記載する。

(7)情報資産台帳の整備と活用

各府省庁の PMO において、情報資産台帳を整備し、どのように活用しているかを記載する。

(8) 情報セキュリティ対策に関する文書の見直し状況

情報セキュリティ対策に関する文書の見直しの検討状況、改訂の実施状況等を記載する。

(9)業務継続計画の策定

保有する情報システムにおける、災害・障害発生時に備えた業務継続計画の策定状況を記載する。

(留意事項)

頻繁な変更が想定される事項ではないが、変更があった場合には、その点を明確に記載する。図表などを用いて分かりやすく表現する工夫をすること。

4 当該年度の重点事項

(目的)

府省庁において年度当初に当該年度の情報セキュリティ対策の重点的な取組として定めた事項の目標、実績及び評価を明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)重点事項の目標、実績及び評価

前年度の情報セキュリティ報告書で課題とした事項に加えて、当該年度当初に新たに重点的な取組と定めた事項について、測定方法と成否判断基準を含めて目標、実績及び評価を記載する。

(2)障害・事故等の再発防止状況

前年度の情報セキュリティ報告書で報告し、対策を実施している情報セキュリティに関する障害・事故等の再発防止策の取組状況を記載する。

【任意項目】

(3)年度途中で発生した重点事項

当該年度当初には重点事項としなかったが、途中で重点的に取り組むこととした事項について、理由等も含めて目標、実績及び評価を記載する。

(留意事項)

後述の「5 情報セキュリティ対策の実施状況」の記載内容と重複しないことが望ましい。

5 情報セキュリティ対策の実施状況

5.1 省庁対策基準に関する自己点検結果

(目的)

すべての行政事務従事者が省庁対策基準に準拠した運用を行っているか否かを自ら点検した結果を、府省庁において集計及び分析し報告することにより、省庁対策基準に対する準拠の全体像を明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)課題と対策

前回調査時に判明した課題とその改善対策を記載する。

(2)自己点検結果の状況

(a) 府省庁全体の把握率

各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合を主体者別に記載する。

(b) 府省庁全体の実施率

把握した者のうち、責務が生じた者に占める対策を実施した者の割合を主体者別に記載する。

(c) 府省庁全体の到達率

把握した者のうち、責務が生じた一定の割合（100%、95%、90%）

以上の者が対策を実施した遵守事項の割合を主体者別に記載する。

(3)総評

自己点検結果について分析を行い、課題の改善状況、次年度に向けた課題、全体としての傾向等を記載する。

【任意項目】

(4)特筆すべき事項

自己点検結果について特徴的な事項がある場合は記載する。

(5)特定テーマの実施率及び到達率

自府省庁として特に重要と考えている事項など特定テーマに絞って実施率、到達率、分析結果等を記載する。

(6)自己点検の計画策定、結果に基づく改善指示等の状況

当該年度の自己点検計画の概要を記載する。また、自己点検結果に基づく改善指示等の状況を記載する。

(留意事項)

原則として、【必須項目】の範囲は、省庁対策基準の全基本遵守事項とする。

自己点検において府省庁全体の把握率の母数は、回収時の全行政事務従事者とする。ただし、休職等により把握できない者を除く。

自己点検結果は、府省庁において監査を実施した後の結果を記載することにより回答の信頼性を担保する。

5.2 情報システムごとの状況

(目的)

情報セキュリティ対策が不十分な場合、情報の漏えい、改ざん、破壊等の要因となり、府省庁の業務や利用する国民・職員に特に重大な影響を及ぼす情報システムについて、対策の実施状況を明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)課題と対策

前回調査時に判明した当該システムにおける情報セキュリティ対策の課題とその改善対策を記載する。

(2)情報システムの対策状況

(a) 端末

全端末を対象に、省庁対策基準の端末に関する基本遵守事項を実施した台数の割合を記載する。

(b) 公開用ウェブサーバ

全公開用ウェブサーバを対象に、省庁対策基準の公開用ウェブサーバに関する基本遵守事項を実施した台数の割合を記載する。

(c) メールサーバ

全メールサーバを対象に、省庁対策基準のメールサーバに関する基本遵守事項を実施した台数の割合を記載する。

(3)総評

情報システムの対策状況に関して分析を行い、課題の改善状況、次年度に向けた課題、全体としての傾向等を記載する。

【任意項目】

(4)特筆すべき事項

情報システムの対策状況に関して特徴的な事項がある場合は記載する。

(5)特定システムの対策状況

障害・事故等が発生した場合に国民に重大な影響を及ぼすシステム（例えば、最適化対象システムのうち、国民の関心の高い情報システム、個人情報処理する情報システム等）について、システムごとの対策状況を記載する。

（留意事項）

特に対策状況に不備が認められない場合でも問題ない旨を記載する。

前年度、全基本遵守事項に準拠（100%）となり、システムの更新又は運用の変更等が発生せず、当該年度もその結果に変更がない場合は、記載を簡略化できる。

5.3 教育・啓発

（目的）

すべての行政事務従事者が、情報セキュリティに関する文書への理解を深め、情報セキュリティ対策を適切に実施できるようにするために取り組んでいる教育・啓発の状況を明らかにすることを目的とする。

（記載内容）

【必須項目】

(1)教育

教育について、以下の事項を参考に、実施している内容を記載する。

- ・ 教育計画の策定、教育の企画等
教育計画の概要、行政事務従事者及び情報セキュリティ対策の役割を担っている者はそれぞれの役割に応じた教育の企画や府省庁教育メニューへの組み込み等の状況について記載する。
- ・ 対象者の役割に応じた教育教材の整備
各対象者への教育教材の整備状況、情報システムの更新、セキュリティ事故の状況等を反映した教材の更新状況等を記載する。
- ・ 教育受講状況の管理
教育の受講状況を管理する仕組みや対象者ごとの受講者の割合を記載する。
また、理解度の確認、人事異動に伴う教育の実施状況について記載する。
- ・ 情報セキュリティ対策担当者の知識向上等
情報セキュリティ対策推進部署において、効果的に業務を遂行するために、担当者の情報セキュリティ対策に係る知識向上について、どのような対策を講じているかを記載する。

【任意項目】

(2)実施手順等の平易化や参照の容易化

実施手順等について、遵守事項を漏れなく含めるだけでなく、理解しやすいものとするため工夫している点について記載する。

また、日常的な参照を容易とするために工夫している点(例：府省庁内ウェブサイト等の分かりやすい場所に置いて日常的に参照可能としている等)を記載する。

(3)ひやり事案を含む障害等の事例の活用

組織内外のひやり事案を含む障害等の事例について、教育等への活用状況を記載する。(事例収集、モデル化、訓練・教育への活用)

(留意事項)

定量的に測定可能ではない項目であっても、自由に記載して構わない。

5.4 調達・外部委託

(目的)

外部委託先から情報漏えい事案等が発生した場合、府省庁の業務に対する国民の信頼が損なわれることから、調達・外部委託に係る情報セキュリティ対策の取り組み内容等を明らかにすることを目的とする。

(記載内容)

【必須項目】

(1)外部委託先の管理

外部委託先の管理について、以下の事項を参考に、実施している内容を記載する。

- ・ 調達仕様への記載事項の標準化
調達仕様に記載する情報セキュリティ対策関連事項について標準を定め、手順書やひな形に含めて示していれば、その状況等を記載する。
- ・ 契約書への記載事項の標準化
契約に記載する情報セキュリティ対策関連事項について標準を定め、手順書やひな形に含めて示していれば、その状況等を記載する。
- ・ カスタマイズを想定した調達のひな形の策定
契約の手順書やひな形は、留意点を記述する等により、案件ごとにカスタマイズして運用できるようにされていれば、その状況等を記載する。
- ・ 外部委託先の情報セキュリティ対策の履行状況等の確認
委託先における情報セキュリティ対策の履行状況を確認するための方法、情報セキュリティ対策の履行が不十分である場合の対処方法の整備状況、実際に確認している内容等を記載する。

(留意事項)

外部委託の適用範囲は、省庁対策基準で示される範囲であるが、例えば次に掲げる営業品目に該当するものに適用する。

- ・ ソフトウェア開発（プログラム作成、システム開発等）
- ・ 情報処理（統計、集計、データエントリー、媒体変換等）
- ・ 賃貸借
- ・ 調査・研究（調査、研究、検査等）

5.5 その他取り組んだ事項

(目的)

上記以外に府省庁が取り組んだ対策及び運用について、その実施状況を明らかにすることを目的とする。

(記載内容)

【任意項目】

(1)実施

業務の改善や例外措置について、以下の事項を参考に、実施している内容を記載する。

- ・ IT活用等による情報セキュリティ対策実施の自動化、強制化
情報セキュリティ対策を確実に実施するために、IT活用等により対策実施の自動化や強制をしている場合、その取組の概要を記載する。
例：外部記録媒体に格納する情報の暗号化の強制

- ・ IT活用等による情報セキュリティ対策実施状況の点検・調査の自動化
情報セキュリティ対策実施状況の点検・調査を効率的に行うために、IT活用等による自動化をしている場合、その取組の概要を記載する。
例：自己点検自動集計ツール
- ・ 例外措置件数、例外措置許可案件のリスク低減、適用期間等の検討
例外措置申請件数及び許可件数並びに許可案件のうちリスクを低減させるための代替手段等の提案が申請に含まれている割合を記載する。
また、採用した例外措置について、継続することの妥当性を適時に判断しているか、例外措置を終了するための検討や準備を行っているか（予算措置、基準への反映の要求等）等を記載する。

（留意事項）

定量的に測定可能ではない項目であっても、自由に記載して構わない。IT活用等による情報セキュリティ対策実施状況の点検・調査の自動化により、より幅広い点検等の実施ができる。

6 情報セキュリティに関する障害・事故等報告

（目的）

府省庁において、情報セキュリティに関する障害・事故等をどのように把握しているのかを明らかにするとともに、府省庁で発生し、公表した障害・事故等の概要、それに対する対応、再発防止策等を記載することにより、国民への説明責任を果たすことを目的とする。

【必須項目】

(1)情報セキュリティに関する障害・事故等の把握

府省庁において、情報セキュリティに関する障害・事故等が発生した場合に、どのように最高情報セキュリティ責任者が把握しているのかを記載する。

(2)公表した障害・事故等の概要、それに対する対応等

(a)情報セキュリティに関する障害・事故等の発生日時

府省庁として把握した日時だけでなく、実際に発生した日時を記載する。

(b)概要

当該事象により行政事務に対して、どのような影響を与えたかを含めて、事象の概要について記載する。

(c)原因

当該事象の発生原因について記載する。

(d)府省庁の対応

暫定措置及び恒久措置について記載する。

(e)原因が省庁対策基準違反によるものか否か

当該事象発生の原因が省庁対策基準違反によるものか、否かを記載する。

(f)再発防止策

当該事象の再発防止策及び情報セキュリティ報告書作成時点までの改善状況を記載する。

【任意項目】

(3)対応コスト

当該事象の発生に伴いかかった対策経費等を記載する。

(4)障害対応に係る対応手順の整備や障害・事故等が発生した際の対応訓練等

障害・事故等が発生した際の対応手順（ウイルス感染時の対応手順、情報システムの停止時の代替業務手順等）について、発生時に容易に参照できるようになっているかなど整備状況を記載する。

また、障害・事故等が発生した際の対応を想定し、訓練を実施している場合、対象システム、訓練内容、訓練にて判明した課題と改善策等を記載する。

(5)一般職員向けの注意喚起

一般職員向けの注意喚起（ウイルスについての警告、ソフトウェアの更新指示等）の実施状況（府省庁内ウェブサイトへの掲載、電子メールでの通知、文書での通達等により適時に広く周知しているか等）を記載する。

（留意事項）

(2)(a)～(f)については、原則として情報セキュリティに関する障害・事故等ごとに記載すること。ただし、同様の障害・事故等が複数ある場合は、まとめて記述しても差し支えない。

情報セキュリティに関する障害・事故等について、報道発表したものは記載しなければならないが、公表には至らない事案も含めた傾向分析等を記載することが望ましい。

原因の分析においては、省庁対策基準に反していれば違反再発防止策を記載し、それ以外の場合は、省庁対策基準の改訂の必要性について記載する。なお、事故公表直後は、事故の内容と暫定的対応措置の公表を優先する必要があるが、情報セキュリティ報告書においては、恒久的対応措置や再発防止策についても記載することが重要である。

7 情報セキュリティ対策に関する次年度の計画

（目的）

本年度の情報セキュリティ対策の総括を次年度に連続して反映させることを目的として、情報セキュリティ対策に関する次年度の計画を記載するものである。なお、本項では、政府機関統一基準において策定を求めている情報セキュリティ対策に関する計画類、情報セキュリティ報告書の中で記載した課題や目標を再掲することなどにより、次年度に実施すべき情報セキュリティ対策を概観できるようにすること

を目的としており、新たな内容の計画の策定を求める趣旨ではない。

(記載内容)

【必須項目】

(1)次年度の計画

情報セキュリティ対策に関する次年度の計画を記載する。

【任意項目】

(2) 政府機関統一基準において策定を求めている情報セキュリティ対策に関する計画類、情報セキュリティ報告書の中で記載した課題や目標以外に新たな計画類を作成した場合は、その内容を記載する。

(留意事項)

情報セキュリティ報告書の中で記載した課題や目標などの引用で差し支えない。

8 結び

(目的)

最高情報セキュリティ責任者の情報セキュリティ対策に対する考え方等を踏まえ、最高情報セキュリティアドバイザーとして、特に注力した情報セキュリティ対策の事項について、国民に対してメッセージを発信することにより、課題認識を明確にすることを目的とする。

(記載内容)

【必須項目】

(1)最高情報セキュリティアドバイザーからのメッセージ

最高情報セキュリティアドバイザーとして、特に注力した事項、課題等を記載する。

(留意事項)

最高情報セキュリティアドバイザー連絡会議(仮称)で検討された事項のうち、府省庁内に周知をしたことや、特に注力した事項を記載することも考えられる。

なお、本文と重複した内容が多くならないように、内容を引用する場合は簡潔に記載すること。

第 2 部 政府機関における評価等の考え方

目的

政府機関においては、第 1 次情報セキュリティ基本計画の下、すべての政府機関において、政府機関統一基準が求める水準の対策を実施していること等を目指して、各府省庁の PDCA サイクル及び情報セキュリティ政策会議による評価・勧告を中心とした政府機関全体の PDCA サイクルという 2 階層の PDCA サイクルを構築し、情報セキュリティ対策を促進するため様々な取組を推進してきた。第 2 次情報セキュリティ基本計画においては、この取組を定着、浸透させ、すべての府省庁が能動的に情報セキュリティ対策に取り組む体制の確立を目指し、各府省庁が情報セキュリティ報告書を作成し、公表することとしている。また、各府省庁の情報セキュリティ対策の実施状況に係る定量的評価等を行い、その結果を情報セキュリティ政策会議に報告することとしている。

「第 2 部 政府機関における評価等の考え方」においては、各府省庁の情報セキュリティ対策の一層の充実・向上を図ることなどを目的として、NISC が行う各府省庁の情報セキュリティ報告書に係る評価等の手法について記載している。

NISC は、同手法に基づき、各府省庁の情報セキュリティ報告書及び各府省庁から入手した情報セキュリティ報告書作成のための基礎資料から、政府機関全体の評価書を作成し、情報セキュリティ政策会議に報告・公表する。

位置付け

NISC は、「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方について（2007 年 2 月 2 日情報セキュリティ政策会議了解）」に基づき、各府省庁と政府機関全体の 2 つの PDCA サイクルが確実にかつ自律的に回っていることを確認するために、政府機関全体としての総合的な評価の運用に取り組んできた。

第 1 次情報セキュリティ基本計画の 3 ヶ年において、これまでの取組が徐々に浸透してきた段階であることから、これまでの取組を踏まえつつ本委員会で検討された手法に基づき、政府機関全体としての評価を行う。

なお、本評価等の考え方及び評価のプロセスは、政府機関全体における情報セキュリティ対策の浸透・定着、技術や環境の変化等を踏まえ、必要に応じて、NISC において見直すものとする。

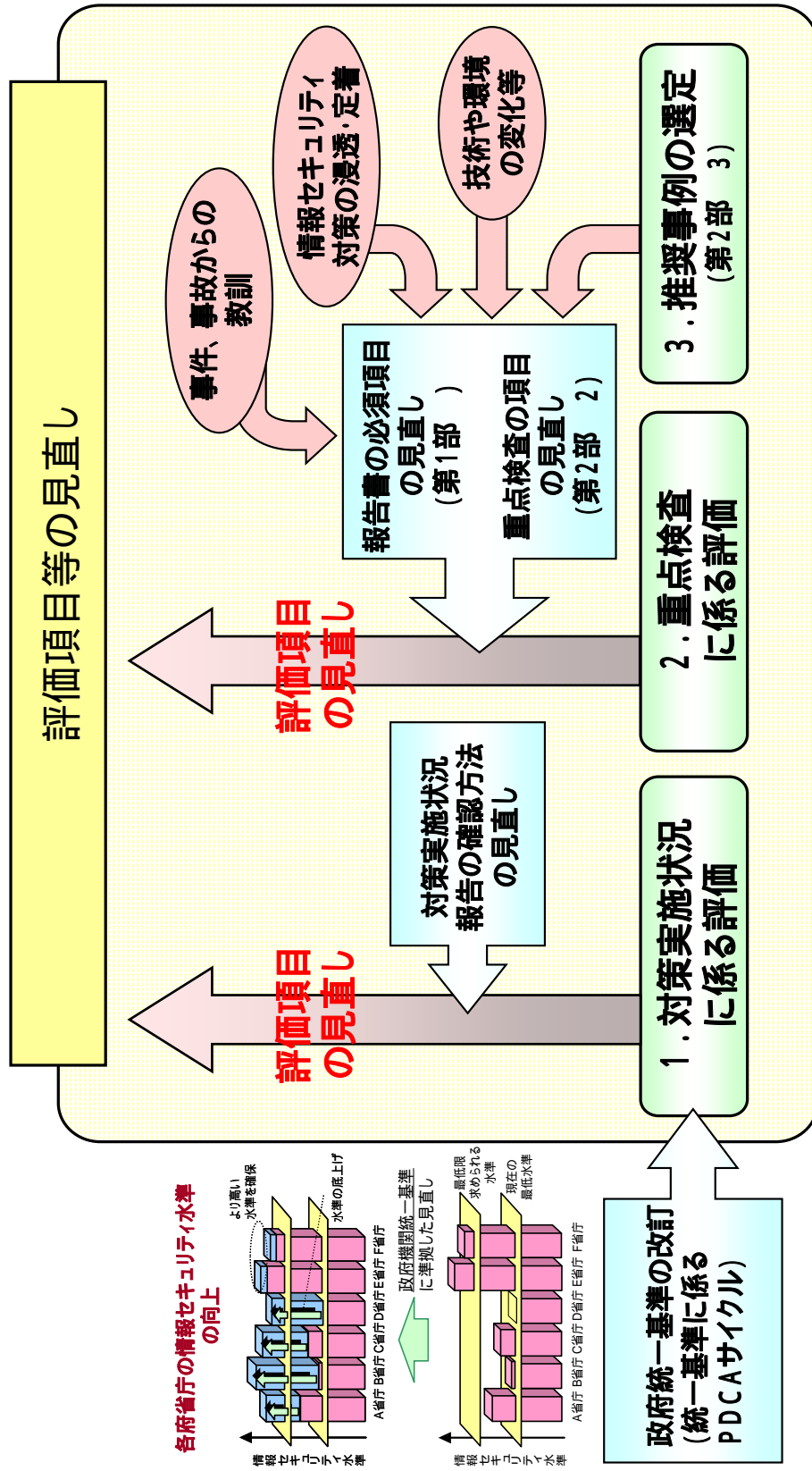


図4 評価項目等の見直し

評価等の手法に関する内容

NISC は、以下の 1 ～ 3 の各手法に基づく評価を行うとともに、各評価結果をもとに各府省庁及び政府機関全体の総合評価結果を示す。

1 対策実施状況に係る評価

(1)目的

政府機関全体の情報セキュリティ対策実施状況を継続的に把握・評価することにより、政府機関統一基準に基づく情報セキュリティ対策水準の維持・向上を図ることを目的とする。

(2)評価手法等

NISC は、「第 1 部 情報セキュリティ報告書作成のためのガイドライン 5 . 1 省庁対策基準に関する自己点検結果」について、各府省庁が情報セキュリティ報告書を作成する際に収集した基礎資料を入手し、評価を行う。

具体的に、NISC は、政府機関統一基準に準拠する省庁対策基準に基づく自己点検、監査等により把握した対策実施状況報告を各府省庁から入手し、百分率（％）で示された把握率、実施率及び到達率を集計し、政府機関全体の平均値を責任者等、システム、職員の 3 つの実施主体ごとに区分し算出する。把握率及び実施率については、各府省庁ごとに ABCD 評価を行う。また、経年度比較を行うなど改善の進捗が確認できるような形で評価を行う。

把握率、実施率及び到達率の定義は、以下のとおりである。

- ・把握率

各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合

- ・実施率

把握した者のうち、責務が生じた者に占める対策を実施した者の割合

- ・到達率

把握した者のうち、責務が生じた一定の割合（100%、95%、90%）

以上の者が対策を実施した遵守事項の割合

遵守事項については、政府機関全体の傾向を分析し、重要な課題又は継続的な課題を抽出する。なお、改善した前年度の課題があれば、記載する。

ABCD 評価の見方例は図 5 のとおりである。

評価	実施率/(把握率)	対策状況	個別対策項目についての 評価パターン例
A	100%	適切に実施すべき対策について、 すべての項目で統一基準に準拠した対策が実施 されている。	 100% 100% 100%
B	80% x < 100%	適切に実施すべき対策について、 概ねすべての項目で統一基準に準拠した対策が実施 されているが、 一部の項目で不十分なものが含ま れている。	 100% 100% 70%
C	60% x < 80%	適切に実施すべき対策について、 不備の項目が一部に見られる など、対策が遅れている。	 100% 100% 0%
D	60%未満	適切に実施すべき対策について、 不備の項目が相当数、見られる など、対策が著しく遅れている。	 100% 50% 20%

図5 対策実施状況のA B C D評価

評価方法は、例えば実施率については、対策実施状況報告の3つの実施主体者の平均実施率(項目ごとに算出した実施率の総平均値)の平均値を総合評価の実施率としている。したがって、政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は100%、すなわち“A評価”となる。

(3)評価書の内容等

NISCは、政府機関全体の対策実施状況報告に係る評価の目的、対象範囲等を記載するとともに、実施主体ごとの把握率、実施率、到達率の評価結果、課題、改善点等を評価書に記載する。

なお、参考として、各府省庁の対策実施状況報告の集計結果を添付する。

2 重点検査結果の評価

(1)目的

政府機関統一基準の基本遵守事項の中でも重要な項目及び「3 情報セキュリティ対策に係る推奨事例の選定」のプロセスで過去に選定された推奨事例の中で特に政府機関全体に浸透・定着を図るべきものについて、重点検査を行い、具体的な情報セキュリティ対策状況を把握・評価することにより、改善促進を図ることを目的とする。

(2)評価手法等

NISCは、「第1部 情報セキュリティ報告書作成のためのガイドライン」において情報セキュリティ報告書への記載を必須とした項目の中から、「第1部 5.2 情報システムごとの状況」及び「過去に選定された推奨事例の中で特

に政府機関全体に浸透・定着を図るべきもの」について、各府省庁から基礎資料を入手し、以下の 及び の評価手法等に基づき、評価を行う。

「第1部 5.2 情報システムごとの状況」に係る評価手法等

NISC は、重点検査項目に関する各府省庁の検査結果を入手し、各府省庁の実施率について、ABCD 評価を行う。その際には、経年度比較を行うなど改善の進捗が可能な限り見られるような形で評価を行う。

ABCD 評価の見方例は図6のとおりである。

評価	実施率	対策状況	個別対策項目についての評価パターン例
A	100%	適切に実施すべき対策について、すべての項目で統一基準に準拠した対策が実施されている。	 100% 100% 100% 100% 対策1 対策2 対策3
B	80% x < 100%	適切に実施すべき対策について、概ねすべての項目で統一基準に準拠した対策が実施されているが、一部の項目で不十分なものが含まれている。	 100% 100% 70% 90% 90% 90% 90% 対策1 対策2 対策3 対策1 対策2 対策3
C	60% x < 80%	適切に実施すべき対策について、不備の項目が一部に見られるなど、対策が遅れている。	 100% 100% 0% 100% 60% 50% 67% 70% 対策1 対策2 対策3 対策1 対策2 対策3
D	60%未満	適切に実施すべき対策について、不備の項目が相当数、見られるなど、対策が著しく遅れている。	 100% 50% 20% 60% 40% 0% 33% 33% 対策1 対策2 対策3 対策1 対策2 対策3

図6 重点検査項目のA B C D評価

評価方法は、重点検査項目の各カテゴリーの平均実施率（項目毎に算出した実施率の総平均値）の平均値を総合評価の実施率としている。したがって、政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は100%、すなわち“A評価”となる。

なお、実施率は、「実際に情報セキュリティ対策を実施している対象数」を「情報セキュリティ対策を実施すべき対象数」で割った式で求められる。

過去に選定された推奨事例の中で特に政府機関全体に浸透・定着を図るべきものに係る評価手法等

検査項目に応じて、適宜、NISC において定量的又は定性的評価手法を検討する。

(3)評価書の内容等

NISC は、政府機関全体の重点検査の評価結果に基づき、対象機関や対象システム及びその数、所見等の概要を記載するとともに、重点項目に関する情報セキュリティ対策の総合評価、評価結果を受けた各府省庁の対応方針を記載する。なお、(2) に関しては、適宜、NISC において検討する。

3 情報セキュリティ対策に係る推奨事例の選定

(1)目的

各府省庁が独自に取り組んだ情報セキュリティ対策から、推奨事例を選定することにより、当該府省庁の独自性や創意工夫を評価し、モチベーションを高めるとともに、府省庁間における取組事例の共有を通じ、政府機関全体としての情報セキュリティマネジメント水準の向上を図ることを目的とする。

なお、情報セキュリティマネジメント水準の向上を図るために、選定された推奨事例は、政府機関全体への浸透状況を踏まえ、「第1部 情報セキュリティ報告書の構成のひな形」の必須項目とするとともに、「第2部 2重点検査結果の評価」の検査項目とすることにより、マネジメント水準の評価に活用する。

(2)評価手法等

最高情報セキュリティアドバイザー連絡会議（仮称）は、各府省庁の情報セキュリティ報告書に記載されている事項を相互に評価し、推奨事例候補となる取組事例をNISCに推薦する。NISCは、推薦された事例から、以下の選定基準に基づき、推奨事例を選定する。

（推奨事例選定の基準）

府省庁の模範となる工夫が見られる、参考にすべき優れた取組事例であること。

(3)評価書の内容等

NISCは、選定した推奨事例の内容、選定理由等を評価書に記載する。

『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』(抄)

評価・検証と見直し

1 行動計画の推進体制**(1) 行動計画の進捗状況の評価・検証**

第2次行動計画に基づく取組みを着実に進め、また継続的に改善させていくために、その進捗状況についての評価・検証を行う。継続的な改善においては、関係主体がそれぞれの取組みを通じて得た経験を、行動計画の関係主体の全体で共有し、それぞれがそれぞれの取組みの改善に活かせるようにすることを重視する。IT障害は回避すべきものであるが、IT障害を防いだ経験や、IT障害が発生した際に影響範囲を限定した経験は、それ自体を将来の糧として活かすべきものであることを認識することが重要である。

当然ながら、IT障害が発生させた当事者はその原因と責任の所在を把握し、自らの取組みを改善するよう努めるべきものである。しかし、第2次行動計画の評価・検証においては、原因と責任を追及することに着目するのではなく、むしろ様々な経験から将来の取組みの改善に活かせる教訓を抽出し、これを関係主体のそれぞれの取組みの改善に役立てるようにすることを主眼とする。

第2次行動計画の進捗状況の評価・検証は、個々の情報セキュリティ対策がどのような成果をあげたのかという「成果(アウトプット)を測る視点」と、社会が実際にどの程度理想とする将来像に近づいたのかという「結果(アウトカム)を測る視点」のふたつの視点で取り組む。この際、可能な限り客観的な指標を用いた検証を行った上で、評価に取り組むこととする。

なお、第2次行動計画においては、「検証」とは各々の取組みについてその進捗状況に関する客観的事実を指標として確認することとし、また、「評価」とは目標に照らしてその取組みの妥当性を見直すこととする。

「成果(アウトプット)を測る視点」からの検証は、第2次行動計画に基づく個別の情報セキュリティ対策の柱に着目して行う。第2次行動計画に基づく情報セキュリティ対策の柱は、いずれも複数の関係主体による多層構造をなしているため、検証のための指標も多様なものが考え得るが、大別して重要インフラ事業者等による対策の検証のための指標と、政府機関等による施策の検証のための指標を設定することとする。これらの検証は、重要インフラ事業者等及び重要インフラ所管省庁の協力を得て、内閣官房が行う。

個別の重要インフラ事業者等による対策の評価については、それが自主的なものである事に鑑み、基本的には事業者自らが行うこととする。また、政府機関等による施策の評価は情報セキュリティ政策会議が行うこととする。

この際、情報セキュリティ対策の柱毎の指標については、その数値自体の多寡、増減にとらわれるのではなく、その数値の意味するところを適切に解釈する事が重要である。

「結果（アウトカム）を測る視点」からの評価・検証は、第2次行動計画の目標と理想とする将来像に照らして行う。行動計画に基づく様々な情報セキュリティ対策が相互に関連して結果をなすものであることに鑑み、個別の情報セキュリティ対策に対して評価・検証を行うのではなく、情報セキュリティ対策の全体、すなわち第2次行動計画の枠組みに対して総合的かつ分析的に行うこととする。

また、行動計画の枠組みの評価を行う際には、情報セキュリティ対策の柱毎の個別の成果だけでは把握しきれない状況も適切に把握して行うことが重要である。そのため、評価に必要な補完的な情報を収集するために、補完調査を実施することとする。

対策の成果検証、施策の成果検証、補完調査は年に1度、情報セキュリティ政策会議が実施することとし、そのために必要な調査検討は重要インフラ所管省庁の協力を得て重要インフラ専門委員会で行う。

また、行動計画に基づく取組みの結果の評価は、その性質上毎年の変化を追っても直ちに改善策を検討することが困難であることから、3年に1度、情報セキュリティ政策会議で実施することとし、そのために必要な調査検討は重要インフラ所管省庁の協力を得て重要インフラ専門委員会で行う。

（2）対策の成果検証

重要インフラ事業者等は重要インフラサービスの安定的供給に一義的な責任を負うものとして、日々情報セキュリティ対策に取り組んでいる。この取組みを継続しかつ着実な改善を期すために、また重要インフラ事業者等の取組みに対する政府の支援策をより効果的なものへと改善させていくためには、互いが情報セキュリティ対策の成果を客観的に検証することが重要である。

対策の成果検証は、第2次行動計画の目標である「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を踏まえ、重要インフラの分野毎に検証対象とした重要インフラサービスについて、検証レベルを逸脱したIT障害の発生状況を検証することとする。検証対象とする重要インフラサービスと検証レベルは、「別紙 重要インフラサービスと検証レベル」に示すとおりとし、具体的な指標は、検証レベルを逸脱するIT障害事例のうち内閣官房が認知したものの10分野全体での総数とする。

なお、個別の事業者等の対策が各々の経営判断に基づく自主的な対策を含むものである以上、事業者等毎又は分野毎のIT障害の発生状況を比較して対策を評価することは不相当である。そのため、対策の評価は重要インフラ事業者等による自己評価によるものとし、各々の事業者等が自ら改善に取り組む事が適当である。また、可能であれば自己評価の実施状況を明らかにすることが望ましい。

(3) 施策の成果検証

第2次行動計画の施策は、「計画期間内に取り組む情報セキュリティ対策」に示したとおりであるが、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるための施策である。第1次行動計画期間においては、これらの施策の枠組みの構築に重点がおかれたが、第2次行動計画においてはこの枠組みの構築が計画通り完了する見込みであることを踏まえ、各施策の効果の検証に着手する。

施策の成果検証では、それぞれの情報セキュリティ対策の柱毎に、重要インフラ事業者等による情報セキュリティ対策への寄与を検証することとする。具体的な指標は以下のとおりとする。

ア) 安全基準等の整備及び浸透

「安全基準等の整備及び浸透」に期待される成果は、重要インフラ事業者等における各種の対策の更なる充実と、その着実な実践である。そのため、指針と安全基準等の項目の充実と、個別事業者等の安全基準等に基づいた取組みの確実な実施に着目した指標を設定する。具体的な指標は、指針及び参考資料に採録した対策項目数、安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の数、指針の重要インフラ事業者等による評価とする。

イ) 情報共有体制の強化

「情報共有体制の強化」により期待される成果は、関係主体間で共有する情報についての整理がなされ、情報提供、情報連絡等に必要な環境整備等が進展し、各セプター、セプターカウンシルの自主的な活動が充実強化された結果として、重要インフラ事業者等が必要な情報を享受し、活用できるようになっていることである。そのため、整備された情報共有体制と共有された情報の充実に着目した指標を設定する。具体的な指標は、内閣官房が発信した情報件数、セプター等で共有された情報件数、共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数とする。

ウ) 共通脅威分析

「共通脅威分析」に期待される成果は、指針の継続的改善及び重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供することである。

そのため、毎年度当初に、重要インフラ事業者等の必要性を勘案して策定する共通脅威分析の検討項目に対する年度末時点の達成度に着目した指標を設定する。具体的な指標は、実施した検討項目件数、各検討結果の重要インフラ事業者等による評価とする。

エ) 分野横断的演習

「分野横断的演習」に期待される成果は、重要インフラ事業者等のIT障害発生時の早期復旧手順、事業継続計画の検証などに対する貢献である。演習で得られた知見を現実のIT障害発生時の事業継続、早期復旧活動に効果的に活用できるものとするためには、より現実の状況に近い演習の実施が重要であり、それぞれの役割を担当する多くのプレイヤーの参加が望ましい。そのため、演習参加者の拡大と演習で得られた知見が、重要インフラ事業者等の取組みに貢献したかどうかに着目した指標を設定する。具体的な指標は、演習の延べ参加者数と、演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した重要インフラ事業者等の数とする。

オ) 環境変化への対応

「環境変化への対応」に挙げた施策のうち、「広報公聴活動」に期待される成果は、行動計画の枠組みについて広く国民の理解を得ることと、第2次行動計画への協力者を関係主体以外にも拡大することである。そのため、第2次行動計画の周知機会の充実に着目した指標を設定する。具体的な指標は、Webサイトのコンテンツの充実度、行動計画を紹介したセミナー等の回数とする。

また、「環境変化への対応」に挙げた施策のうち、「リスクコミュニケーション」に期待される成果は、関係主体間で互いの活動への理解の向上と、連携を図りやすい環境の醸成である。そのため、関係主体間のコミュニケーション機会の充実に着目した指標を設定する。具体的な指標は、セブターカウシルや分野横断的演習等の関係主体間のコミュニケーションの機会の開催回数とする。

カ) 調査活動の充実

これらの施策が重要インフラ事業者等の対策にどう活かされたかを把握することは重要である。内閣官房は関係主体が自主的にまとめている統計情報の収集を進めるとともに、自らの調査活動の充実を図ることとする。この際、施策の対策への効果をより高めるために、内閣官房は重要インフラ事業者等のサービスレベルの設定状況を可能な範囲で把握することとする。なお、この際、重要インフラ事業者等に過度の負担をかけないよう配慮する事が必要である。

(4) 結果の評価のための補完調査

指標を用いた成果検証は実態を捉えるために不可欠なものであるが、それは一側面を捉えるものに過ぎない。第2次行動計画の期待する結果(アウトカム)の評価をより実態に即すようにするために、指標では捉えられない側面を補完的に調査する必要がある。そのため、IT障害等の事例について補完調査を実施し、第2次行動計画に基づく施策と対策を評価するため材料を得ることとする。

補完調査は毎年1回行うこととし、調査結果を可能な範囲で公表する。

(5) 行動計画に基づく取組みの結果の評価

第2次行動計画の理想とする将来像を踏まえて、行動計画に基づく取組みの結果の評価に取り組む。

理想とする将来像に着目すると、個別の対策や施策の成果がこの結果にそれぞれの程度貢献したかを分析的に評価することは困難である。また、個別の対策や施策の成果が結果に結びつくまでには時間差があり、それぞれの取組みを一律に同じ時系列で評価することも適当ではない。そこで、第2次行動計画のどの施策や対策がどの程度貢献したかを個別に分析するのではなく、これらの総体である行動計画そのものを総合的に評価することとする。

行動計画の結果の評価では、対策の検証、施策の検証、補完調査の結果を内閣官房でとりまとめ、行動計画に基づく取組みが、全体として第2次行動計画の結果(アウトカム)の達成に適ったものであるかを評価する。この際、個別の対策や施策の及ばない面のみに着目するのではなく、むしろ全体のバランスを見た上で更に取組みを前進させるためにはどうすれば良いかという面にも着目することが重要である。

(6) 行動計画の見直し

第2次行動計画については、対策の成果、施策の成果、補完調査、評価の内容(以下「評価等」という。)を踏まえ、また、脅威、IT障害、ITを利用したサービス等に関する社会情勢等の変化等をふまえ、3年毎又は必要に応じ、見直しを行う。第2次行動計画期間においては、少なくとも策定から2年後から12ヶ月かけて見直すこととする。

特に見直しの要点となるのは、目標とそれに基づく基本的な方向性、重要インフラ事業者等の対象範囲、関係主体とすべき主体の対象範囲、対策や施策の追加や廃止、想定すべき脅威の例示、対象とすべき重要インフラサービスの範囲、サービスレベル、検証レベル、評価指標の設定等である。またこれに併せて、各用語の定義や行動計画の対象範囲についても、必要に応じて見直しを行うものとする。

第2次行動計画の見直しに際しては、各分野の特性や取組状況に配慮しつつ、事業者の取組みが自主性に基づくものであることを踏まえた検討を行うことが必要

である。また、第2次行動計画が想定し得なかった事象が発生した場合はこれに対応できるようにすることが重要である。

行動計画の見直しは重要インフラ専門委員会において行うこととし、委員会の合意を経て、情報セキュリティ政策会議で新たな行動計画を決定するものとする。

2 既存の情報共有体制との連携

緊急事態時や災害対策等においては、第2次行動計画の情報共有の枠組みの他にも、既存の情報共有体制がある。既存の情報共有体制が想定している事態のもとIT障害が発生した場合には、第2次行動計画とこれら情報共有体制との連携が望まれる。このため、内閣官房は関係する府省庁の協力を得て情報共有の円滑化に向けた検討を行うこととする。

別紙 重要インフラサービスと検証レベル

重要インフラ分野		重要インフラサービス(手続きを含む)(注)		検証レベル	
		呼称	サービス(手続きを含む)の説明 (関連する法令)	対象・水準	備考
情報通信		・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること(電気通信事業法 第2条)	・電気通信設備の故障により、役務提供の停止・品質の低下が、3万以上の利用者に対し2時間以上継続する事故が生じないこと	・電気通信事業法施行規則 第58条による
		・放送	・公衆によって直接受信されることを目的とする無線通信の送信(放送法 2条)	・ITの機能不全により、放送の停止が生じないこと	
金融	銀行	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ(銀行法 第10条1項1号) ・資金の貸付け又は手形の割引(銀行法 第10条1項2号) ・為替取引(銀行法 第10条1項3号)	・ITの機能不全により、預金の払戻しの遅延、停止が生じないこと ・ITの機能不全により、融資承諾をした貸付の実行の遅延、停止が生じないこと ・ITの機能不全により、為替(銀行振込)の遅延、停止が生じないこと	・「主要行等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合(例えば、一部のATMが停止した場合であっても同一店舗または近隣店舗の他のATMや窓口において対応が可能な場合等)を除く
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付 ・保険金等の支払審査 ・保険金等の支払い	・ITの機能不全により、保険金等の支払いに遅延、停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
	損害保険	・保険金等の支払い	・事故受付 ・損害調査等 ・保険金等の支払い	・ITの機能不全により、保険金等の支払いに遅延、停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
	証券会社 金融商品 取引所	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ ・金融商品市場の開設	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引(金融商品取引法 第2条8項1号) ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理(金融商品取引法 第2条8項2号) ・有価証券等清算取次ぎ(金融商品取引法 第2条8項5号) ・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務(金融商品取引法 第2条14項、同条16項、80条、84条)	・ITの機能不全により、預り有価証券等の売却、解約代金の払い出し等に遅延、停止が生じないこと ・ITの機能不全により、有価証券の売買又は市場デリバティブ取引等に遅延、停止が生じないこと	・「金融商品取引業者等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合(例えば、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。)を除く ・金融商品取引所等に関する内閣府令 第112条7項を参照

重要インフラ分野	重要インフラサービス(手続きを含む)(注)		検証レベル	
	呼称	サービス(手続きを含む)の説明 (関連する法令)	対象・水準	備考
航空	<ul style="list-style-type: none"> ・ 旅客、貨物の航空輸送サービス ・ 航空交通管制業務 ・ 気象情報配信 ・ 予約、発券、搭乗・搭載手続き ・ 運航整備 ・ 飛行計画作成 	<ul style="list-style-type: none"> ・ 他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業(航空法第2条) ・ 空域の適正な利用及び安全かつ円滑な航空交通の確保(航空法第95条の2) ・ 航空機の利用に適合する予報・警報等の配信(気象業務法第14条) ・ 航空旅客の予約、航空貨物の予約 ・ 航空券の発券、料金徴収 ・ 航空旅客のチェックイン・搭乗、航空貨物の搭載 ・ 航空機の点検・整備 ・ 飛行計画の作成、航空局への提出 	<ul style="list-style-type: none"> ・ ITの機能不全により、貨客の運送に支障を及ぼす定期便の欠航が生じないこと 	
鉄道	<ul style="list-style-type: none"> ・ 旅客輸送サービス ・ 発券、入出場手続き 	<ul style="list-style-type: none"> ・ 他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業(鉄道事業法第2条) ・ 座席の予約、乗車券の販売、入出場の際の乗車券等の確認 	<ul style="list-style-type: none"> ・ ITの機能不全により、旅客の輸送に支障を及ぼす列車の運休が生じないこと 	
電力	<ul style="list-style-type: none"> ・ 一般電気事業 	<ul style="list-style-type: none"> ・ 一般の需要に応じ電気を供給する事業(電気事業法第2条、18条) 	<ul style="list-style-type: none"> ・ ITの機能不全により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと 	<ul style="list-style-type: none"> ・ 電気関係報告規則 第3条による
ガス	<ul style="list-style-type: none"> ・ 一般ガス事業 	<ul style="list-style-type: none"> ・ 一般の需要に応じ導管によりガスを供給する事業(ガス事業法第2条) 	<ul style="list-style-type: none"> ・ ITの機能不全により、供給支障戸数が30以上の供給支障事故が生じないこと 	<ul style="list-style-type: none"> ・ ガス事業法施行規則 第112条による
政府・行政サービス	<ul style="list-style-type: none"> ・ 地方公共団体の行政サービス 	<ul style="list-style-type: none"> ・ 地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの(地方自治法第2条2項) 	<ul style="list-style-type: none"> ・ ITの機能不全により、住民等の権利利益の保護に支障が生じないこと ・ 住民等の安全・安心を確保できる時間内にシステムの復旧を行うこと 	<ul style="list-style-type: none"> 例：ホームページによる各種情報提供サービスの場合 ・ 個人情報の漏えいが生じないこと ・ サービスの提供不能又は誤った内容の提供が発生した場合、概ね24時間以内にシステムを復旧し、通常どおりサービスを提供できること
医療	<ul style="list-style-type: none"> ・ 診療 	<ul style="list-style-type: none"> ・ 診察や治療等の行為 ・ 診療録及び診療諸記録類等の記録・保存 	<ul style="list-style-type: none"> ・ ITの機能不全により、診療録等の保存に支障が生じないこと 	<ul style="list-style-type: none"> ・ ITの依存度によらず、診察や治療等の行為は継続可能である ・ 保存に関しては、即時を求めるものではなく、医師法第24条2項による

重要インフラ分野	重要インフラサービス(手続きを含む)(注)		検証レベル	
	呼称	サービス(手続きを含む)の説明 (関連する法令)	対象・水準	備考
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業(水道法 第3条、15条)	・ITの機能不全により、断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと	・重大なシステム障害とは、システム停止に伴う給水への影響が大きい制御システム(浄水場の監視制御システム、ポンプ場の運転システム、水運用システム等)の障害を想定
物流	・物流	・貨物の運送及び保管	・ITの機能不全により、貨物運送の停止や貨物の紛失が生じないこと	

(注) 本行動計画の目標から、ITを全く利用していないサービスについては対象外

企業・個人における情報セキュリティの評価指標

(1) 指標に関する基本的な考え方

ア 指標のあり方

企業・個人の対策実施領域においては、政府の役割は、政策により、各主体の情報セキュリティ意識を高めること、各主体が自主的に行う情報セキュリティ対策を支援するなど環境を整備すること、である。言いかえると、この対策実施領域が政府機関・重要インフラといった他の対策実施領域に比べて巨大な母数を抱え、かつ、多種多様な主体の集合体であるために一律の対策を設定することが困難であること等を踏まえ、企業・個人に対しては、環境整備等の間接的な働きかけを行い、各主体に「気付き」を起こさせる等、IT社会の一員としての社会的責任といった観点も踏まえた形で、各主体が自律的・継続的に取り組んでいくよう対策を促していくことが、政府の施策の中心となる。

したがって、この対策実施領域における評価指標（以下「指標」という。）に関しては、すべての主体にわたる詳細な調査を行うよりは、いくつかの既存のデータを収集し、それぞれのデータの特性を考慮しつつ企業全体・個人全体の傾向を分析する方法により実態を把握することが適当であり、このように対策の浸透の度合いを評価することが必要である。

イ 指標の分類

企業・個人に係る指標は、企業全体・個人全体の傾向を分析するという観点から、企業全体・個人全体の意識、対策、被害を見る「アウトカム評価指標」、企業・個人を支援する政府の姿を見る「アウトプット評価指標」とに分けて考えることとする。

ウ 指標のソースと留意点

企業・個人に係る指標は、巨大な母集団が対象であること、調査の各主体への負担をなるべく軽減すべきであること、の観点から、状況把握に有益な既存のデータ¹の活用を原則とし、項目ごとに記載するが、このデータ一覧は、固定的なものではなく、今後定期的に、指標自体の見直しと合わせて、見直しを行っていくこととする。

¹ 「状況把握に有益な既存のデータ」とは、政府、公的機関等の保有する統計や実態調査結果のうち、内閣官房において、我が国の企業・個人における情報セキュリティの状況把握に有益と判断したデータを指す。

また、現時点では把握されていないが、政府機関等が中心となって把握していくことが望まれるデータについても今後の課題として挙げており、今後、このような関連データの把握に向けた努力が期待される。

なお、これらのデータの活用にあたっては、調査目的、調査方法、調査母集団、サンプル抽出手法及び調査時期がそれぞれ異なること、それぞれの統計と調査の質に幅があること、に留意することが必要である。

(2) 企業・個人に係るアウトカム評価指標

「アウトカム評価指標」とは、行政活動の結果として国民生活や社会生活に及ぼされる何らかの効果を計るものである。

ここでは、我が国政府の情報セキュリティ政策の結果として、各主体の対策や政府の取組みに比べると間接的であるが、何らかの効果が期待され、現象として把握できるものとして、「各主体の意識」、「各主体の対策」及び「インシデント・犯罪の発生」を企業個人に係る主なアウトカム評価指標として挙げる。ただし、これらの指標については、政府や重要インフラに係る取組み、その他多様な要因の影響を受ける可能性が高いため、企業・個人に係る取組みだけによって効果を測定するために活用するのではなく、他の主体に係る取組みも含め総合的な視点から活用していくことが望ましい。

なお、評価に際しては、これらの指標の測定時点・測定方法によっては必ずしも対象の状態を適切に把握できない場合があることに留意し、場合によってはこれらの指標以外の情報も活用する、指標の追加・見直しの検討を行うなど、柔軟に、実態の把握に努めることが必要である。

ア 各主体の意識

企業の情報セキュリティ意識に係る指標

企業全体の情報セキュリティの意識の状況を指標とする。また、可能なものについては、企業規模別の傾向の違いを把握する。

(既存のデータ)

- ・「情報セキュリティ上のトラブル(システムトラブル、不正アクセス、コンピュータウィルス、重要情報の漏えい等)の重要性の認識」
(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(トップの理解、予算等)」
(情報処理実態調査：経済産業省)

個人の情報セキュリティ意識に係る指標

個人全体の情報セキュリティの意識の状況を指標とする。また、可能なものについては個人の属性別の傾向の違いを把握する。

(既存のデータ)

- ・「インターネットを利用して感じる不安や不満、利用しない理由」

(通信利用動向調査：総務省)

- ・「インターネットにおける情報セキュリティの認知度」

(インターネットの利用実態に関する調査：総務省)

- ・「情報セキュリティに関する攻撃・脅威に対する認知状況」

(情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構)

イ 各主体の対策

企業の情報セキュリティ対策状況に係る指標

a 情報セキュリティ対策の確立に係る指標

企業全体の情報セキュリティに取り組む組織的な体制等の確立に関連するものを指標とする。また、可能なものについては、企業規模別の傾向の違いを把握する。

(既存のデータ)

- ・「リスク分析実施状況」

(情報処理実態調査：経済産業省)

- ・「情報セキュリティポリシーの策定状況」

(情報処理実態調査：経済産業省)

- ・「情報セキュリティ報告書の作成状況」

(情報処理実態調査：経済産業省)

- ・「セキュリティ管理者の配置状況」

(情報処理実態調査：経済産業省)

- ・「内部統制の整備強化」

(情報処理実態調査：経済産業省)

b 情報セキュリティ対策の導入及び運用に係る指標

企業全体の情報システムを構築・運用する場合の情報セキュリティ対策の導入及び運用の状況(教育の状況も含む)を指標とする。また、可能なものについては、企業規模別の傾向の違いを把握する。

(既存のデータ)

- ・「重要なシステムへの内部でのアクセス管理の実施状況」

(情報処理実態調査：経済産業省・通信利用動向調査：総務省)

- ・「データの暗号化実施状況」

- (情報処理実態調査：経済産業省・通信利用動向調査：総務省)
- ・「外部接続へのファイアウォールの配置状況」
(情報処理実態調査：経済産業省・通信利用動向調査：総務省)
- ・「セキュリティ監視ソフトの導入状況」
(情報処理実態調査：経済産業省・通信利用動向調査：総務省)
- ・「情報セキュリティ教育の実施状況等」
(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)
- ・「セキュリティパッチ適用」
(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)
- ・「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)
- ・「ITセキュリティ評価及び認証取得製品の導入」
(情報処理実態調査：経済産業省)

c 情報セキュリティ対策の監視及びレビューに係る指標

- 企業全体の情報セキュリティ対策の監視及びレビューの状況を指標とする。また、可能なものについては、企業規模別の傾向の違いを把握する。
(既存のデータ)
- ・「定期的な情報セキュリティ監査の実施状況」
(情報処理実態調査：経済産業省)

個人の情報セキュリティ対策状況に係る指標

- 個人全体の情報セキュリティ対策の状況を指標とする。また、可能なものについては個人の属性別の傾向の違いを把握する。
(既存のデータ)
- ・「インターネットのウィルスや不正アクセスへの対応」
(通信利用動向調査：総務省)
 - ・「インターネットにおける無線LAN等のセキュリティ対策状況」
(インターネットの利用実態に関する調査：総務省)
 - ・「情報セキュリティ対策の実施状況」
(情報セキュリティに関する脅威に対する意識調査：情報処理推進機構)

ウ インシデント・犯罪の発生

インシデント又は犯罪の被害に係る指標

インシデント又は犯罪の被害は、認知した者は申告するとしても被害を受けても気が付かない者は申告せず、全体の正確な割合が分からない、という限界はある。しかし、ここでは、企業・個人全体へのリスクの傾向を計測する観点から、企業・個人全体がインシデント又は犯罪の被害を経験した割合等を指標とする。
(既存のデータ)

- ・「情報セキュリティ上のトラブル(システムトラブル、不正アクセス、コンピュータウイルス、重要情報の漏えい等)の経験」(企業)
(情報処理実態調査：経済産業省)
- ・「インターネットを利用して受けた被害(ウイルス感染、スパムメールの中間利用・踏み台、不正アクセス、DoS 攻撃等)(ウイルス感染、不正アクセス以外は企業のみ)」
(通信利用動向調査：総務省)
- ・「過去1年間の情報セキュリティに関する被害状況」(企業)
(不正アクセス行為対策等の実態調査：警察庁)
- ・「不正アクセス行為の発生状況」
(国家公安委員会、総務省、経済産業省)
- ・「コンピュータウイルス、不正アクセス、ソフトウェア製品・ウェブサイトの脆弱性に関する情報の届出状況」
(情報処理推進機構)
- ・「情報セキュリティに関する被害やトラブルの遭遇状況」(個人)
(情報セキュリティに関する脅威に対する意識調査：情報処理推進機構)
- ・「コンピュータウイルス遭遇経験」(企業)
(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)

エ (参考指標) IT投資状況及びITを活用した経済の発展状況

IT投資状況及びITを活用した経済の発展は情報セキュリティの裏付けが伴ってなされると思料されることから、参考指標として扱うものとする。

(既存のデータ)

- ・「企業間(B to B)電子商取引の現状(国内市場規模、電子商取引化率)」
(電子商取引に関する市場調査：経済産業省)
- ・「消費者向け(B to C)電子商取引の現状(国内市場規模、電子商取引化率)」
(電子商取引に関する市場調査：経済産業省)

(3) 企業・個人に係るアウトプット評価指標

「アウトプット評価指標」とは、行政活動により提供されたモノやサービスの量等対策の浸透度を計るものである。ここでは、我が国政府の情報セキュリティ政策の浸透度に関連するものとして、「企業を支援する政府の施策」「個人を支援する政府の施

策」を企業・個人に係る主なアウトプット評価指標として挙げる。ただし、これらの指標については、政府や重要インフラに係る取組み、その他多様な要因の影響を受ける可能性が高いため、企業・個人に係る取組みだけによって効果を測定するために活用するのではなく、他の主体に係る取組みも含め総合的な視点から活用していくことが望ましい。

なお、評価に際しては、これらの指標の測定時点・測定方法によっては必ずしも対象の状態を適切に把握できない場合があることに留意し、場合によってはこれらの指標以外の情報も活用するなど、柔軟に、実態の把握に努めることが必要である。

ア 企業を支援する政府の施策

情報セキュリティガバナンスの「経営の一環としての位置付け」の確立に係る指標

企業による第三者評価制度等の利用状況を指標とする。

(既存のデータ)

- ・「情報セキュリティマネジメントシステム適合性評価制度に基づく認証取得事業者数」

(日本情報処理開発協会)

企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進に係る指標

企業による第三者評価制度等の利用状況を指標とする。

(既存のデータ)

- ・「ITセキュリティ評価及び認証制度に基づく認証取得製品数」

(情報処理推進機構)

- ・「暗号モジュール試験及び認証制度に基づく認証取得製品数」

(情報処理推進機構)

企業における情報セキュリティ人材の育成・確保に係る指標

政府等による企業に対する情報セキュリティ教育や政府等の情報セキュリティに係る資格の取得者等の状況を指標とする。

(既存のデータ)

- ・「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)

「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制の強化に係る指標

事業継続性の確保、コンピュータウィルスや脆弱性等への対応のための体制の整備状況等を指標とする。

(既存のデータ)

・「JPCERT/CCと連携しているコンピュータセキュリティ緊急対応チーム(CSIRT)の数」

(JPCERT/CC)

・「JPCERT/CCに登録している国内の製品開発ベンダー等の担当窓口の数」

(JPCERT/CC)

・「事業継続計画策定状況」

(情報処理実態調査：経済産業省)

中小企業の情報セキュリティ対策の推進に係る指標

(既存のデータ)

・「情報セキュリティセミナーの実施状況」

(情報処理推進機構)

・「SaaS利用に伴う外部への支払い費用・SLAの締結状況」(企業規模別)

(情報処理実態調査：経済産業省)

・「ASP・SaaSの利用状況」

(通信利用動向調査：総務省)

日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進に係る指標

現状、既存データによる指標の設定は難しく、年度計画における該当施策の進捗状況を成果評価として活用する。追加可能なデータがあれば、毎年度の作業方針の策定において見直しを実施する。

イ 個人を支援する政府の施策

情報セキュリティ教育の強化・推進に係る指標

個人向けの教育の機会の状況を指標とする。

(既存のデータ)

・「情報モラルなどを指導する能力を有すると回答した教員の割合」

(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)

・「インターネット安全教室参加者数(概数)」

(経済産業省)

・「e - ネットキャラバン参加者数 (概数)」

(総務省・文部科学省)

個人の底上げに向けたより効果的な普及・啓発活動の実現に係る指標

政府等による情報発信へのアクセスの状況を指標とする。

(既存のデータ)

・「情報セキュリティに係る政府系 web 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)

・「インターネットにおける情報セキュリティ脅威に関する情報・対策情報の
入手方法」

(インターネットの利用実態に関する調査 : 総務省)

・「セキュリティ情報の入手方法」

(情報セキュリティに関する脅威に対する意識調査 : 情報処理推進機構)

対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組みに係る
指標

(既存のデータ)

・「サイバークリーンセンター活動実績」

(サイバークリーンセンター : 総務省、経済産業省)