

情報セキュリティ政策

2008年度の評価等に向けた「作業方針」

内閣官房情報セキュリティセンター(NISC)

2008年12月10日

# 目次

第1章 情報セキュリティ政策の評価等に向けた「作業方針」について.....	1
第2章 情報セキュリティ政策全体に関する2008年度の評価等 .....	3
第1節 情報セキュリティ政策全体に関する2008年度の取組みの評価等	
(1) 情報セキュリティ政策全体に関する2008年度の評価等の考え方 .....	3
① 評価等の視点 .....	3
② 評価等の対象 .....	4
③ 評価等の方法 .....	4
④ 関係府省庁 .....	5
第2節 情報セキュリティ政策全体に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方 .....	5
第3章 政府機関対策に関する2008年度の評価等 .....	6
第1節 政府機関に関する2008年度の取組みの評価等	
(1) 政府機関対策に関する2008年度の評価等の考え方 .....	6
① 評価等の視点 .....	6
② 評価等の対象 .....	6
③ 評価等の方法 .....	6
④ 関係府省庁 .....	9
(2) 政府機関対策に関する2008年度の補完調査の考え方 .....	9
① 補完調査項目 .....	9
② 補完調査の趣旨 .....	10
③ 補完調査の調査方法 .....	10
④ 関係府省庁 .....	10
第2節 政府機関に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方 .....	10

第4章 重要インフラ対策に関する2008年度の評価等	13
第1節 重要インフラ対策に関する2008年度の取組みの評価等	
(1) 重要インフラ対策に関する2008年度の評価等の考え方	13
① 評価等の視点(目標)	13
② 評価等の対象	13
③ 評価等の方法	13
④ 関係府省庁	14
(2) 重要インフラ対策に関する2008年度の補完調査の考え方	14
① 補完調査項目	14
② 補完調査の趣旨	14
③ 補完調査の調査方法	14
④ 関係府省庁	14
第2節 重要インフラ対策に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方	16
第5章 企業・個人対策に関する2008年度の評価等	18
第1節 企業・個人対策に関する2008年度の取組みの評価等	
(1) 企業・個人対策に関する2008年度の評価等の考え方	18
① 評価等の視点	18
② 評価等の項目(評価指標)	19
③ 評価等の方法	19
④ 関係府省庁	19
(2) 企業・個人対策に関する2008年度の補完調査の考え方	19
① 補完調査項目	19
② 補完調査の趣旨	20
③ 補完調査の調査方法	20
④ 関係府省庁	20
第2節 企業・個人対策に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方	21
第6章 横断的な情報セキュリティ基盤に関する2008年度の評価等	27
第1節 横断的な情報セキュリティ基盤に関する2008年度の取組みの評価等	
(1) 横断的な情報セキュリティ基盤に関する2008年度の補完調査の考え方	27
① 補完調査項目	27
② 関係府省庁	27

第2節 横断的な情報セキュリティ基盤に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方.....	27
---	----

今後のスケジュール .....	29
-----------------	----

## 第1章 情報セキュリティ政策の評価等に向けた「作業方針」について

我が国の情報セキュリティ政策は、「「セキュア・ジャパン」の実現に向けた取組みの評価及び合理性を持った持続的改善の推進について」（平成19年2月2日情報セキュリティ政策会議決定）及び「情報セキュリティの観点から見た我が国のあるべき姿及び政策評価のあり方」（平成19年2月2日情報セキュリティ政策会議了解）（以下、前記2文書を合わせて「枠組み文書」という。）に基づき、

- (i) 情報セキュリティ基本計画（以下「基本計画」という。）を中心とする3年単位の政策サイクル（基本サイクル）
- (ii) 基本計画の下で策定される年度計画を中心とする1年単位の政策サイクル（年度サイクル）

の2種類のサイクルによって運営されている。枠組み文書では、当該政策サイクルのもと、毎年を取組みの進捗等を点検（Check）するために、評価指標に基づく評価、補完調査、分析等（以下「評価等」という。）を行うこととしている。

また、2008年度は基本サイクルの3年目（最終年度）であることから、特に、枠組み文書に記載されている「2009年時の我が国社会の姿」（以下、「あるべき姿」という。）の達成度についても評価等を行う。

本文書は、前記2種類のサイクルの評価等を実施するための2008年度の評価等に向けた作業方針（以下「作業方針」という。）を策定するものである。

枠組み文書では、毎年、内閣官房情報セキュリティセンター（以下、「NISC」という。）が作業方針を策定し、その内容として、具体的には以下の要素を盛り込むこととしている。

- (i) 評価指標の項目及び関係府省庁
- (ii) 補完調査の項目及び関係府省庁
- (iii) 分析課題及び分析方法
- (iv) 評価等の実施に係る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

本作業方針策定後は、2009年3月頃までを目途に評価、補完調査、分析等の作業を実施し、作業の結果については、NISCを中心に2008年度の評価等に係る文書としてとりまとめるとともに、以降の政策の企画・立案（翌年度計画や次期基本計画の策定）等に活用することとなる。

なお、本作業方針の策定に当たっては、以下の2点に十分留意する。

- (i) どのような内容、スケジュールで情報セキュリティ政策の政策評価等に係る

作業を進めようとしているかという点について、国民に対する説明責任を果たすこと

(ii)内閣官房、各府省庁等の作業当事者が、計画的かつ合理的に必要な作業を進めることに資するべきものであること

## 第2章 情報セキュリティ政策全体に関する2008年度の評価等

### 第1節 情報セキュリティ政策全体に関する2008年度の評価等

#### (1) 情報セキュリティ政策全体に関する2008年度の評価等の考え方

##### ① 評価等の視点

2008年度は、第1次基本計画に基づく取組みの3年目（最終年度）として、「セキュア・ジャパン2008」（平成20年6月19日情報セキュリティ政策会議決定）において「情報セキュリティ基盤の強化に向けた集中的な取組み」を年度の重点としている。そこで、2008年度の評価等の視点として、第一に当該年度目標の達成度を測ることが重要である。第二の視点として、2008年度に限らないことではあるが、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み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欠かせない。

また、評価等の取組みは、その結果を踏まえて以降の政策の企画・立案等に活用することを企図して行うものである。本来であれば、取組みの最終年度であることから、基本サイクルに従い次期情報セキュリティ基本計画（以下、「次期基本計画」という。）に対して評価の結果を反映させるべきものである。しかしながら、次期基本計画は第1次情報セキュリティ基本計画と間隔を空けないようにするため、平成21年2月を目途に決定される予定であり、次期基本計画に反映させることは困難である。そこで、評価の結果は次期計画下における年次計画等において反映させることとする。そのため、第3の視点として、2009年度の取組み（年次計画等）の具体化等に向けた助けとする視点が必要である。

以上より、2008年度の評価等の視点として、以下の3つを設定する。

- (i) 2008年度の重点である「情報セキュリティ基盤の強化に向けた集中的な取組み」の達成度を測る視点
- (ii) 情報セキュリティに係る2008年度の様々な動向を測る視点
- (iii) 次期基本計画の下での2009年度の取組みの具体化等に向けた助けとする視点

## ② 評価等の対象

情報セキュリティ政策全体の評価等という観点からは、以下の2点が重要である。

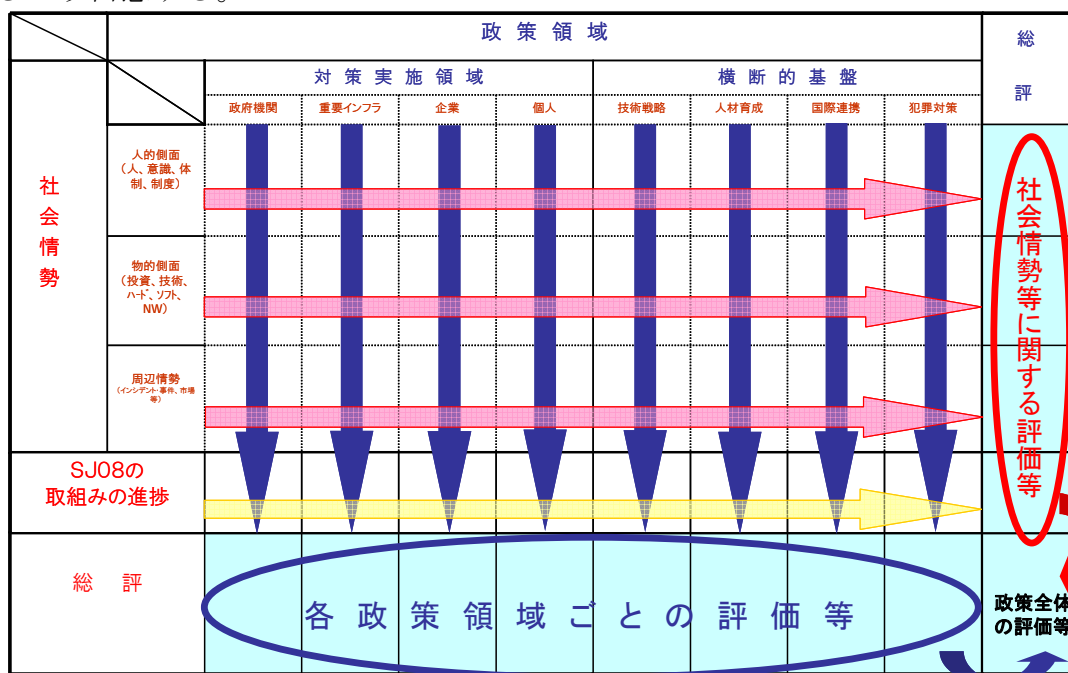
- (i) 2008年度の年度計画である「セキュア・ジャパン2008」に基づく施策の進捗に関する評価等を内閣官房及び全府省庁を対象として行うこと
- (ii) 施策を進めた結果、情報セキュリティに係る動向にどのような変化が見られたかという点についても見ること

なお、この際、例えば突発的な新しいリスクの発生など、施策の推進と必ずしも対応関係にないような動向の変化が見られる可能性もある。施策との関連性についても考慮しながら評価等に係る作業を進める必要がある。

## ③ 評価等の方法

まず、「セキュア・ジャパン2008」に基づく取組みの進捗については、「進捗状況調査」によって把握する。当該調査は、2008年9月頃（上半期調査）及び2009年2月頃（下半期調査）の2回実施する。

次に、以下の検討枠組みを活用して、評価等を行う。ここでは、上記の進捗状況調査の結果も活用しながら、取組みの進捗や、その結果見られた社会情勢の変化、政策領域ごとの状況を分析するとともに、定性的な評価を行う。その上で、情報セキュリティ政策全体としての評価等を定性的に行うこととする。なお、作業に当たっては可能な限り数値やデータを加味し、幅広い視点から評価等がなされるよう留意する。





#### ④ 関係府省庁

情報セキュリティ政策は、内閣官房と全府省庁が協力しながら進められていることから、政策全体の評価等における関係府省庁は、内閣官房及び全府省庁となる。

#### 第2節 情報セキュリティ政策全体に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方

情報セキュリティ政策全体に関する「あるべき姿」は、「ITを安心して利用可能な環境（IT安心利用環境）が実現されていること」である。しかし、その達成度を測ることが可能な単一の指標を設定することは困難であるため、新たな指標は設定しない。そのため、IT安心利用環境の実現状況については、各対策実施主体及び横断分野における「あるべき姿」の達成度や各施策の実施結果、関係する指標等を総合的・網羅的に用いることにより、評価を行う。

## 第3章 政府機関対策に関する2008年度の評価等

### 第1節 政府機関に関する2008年度の取組みの評価等

#### (1) 政府機関対策に関する2008年度の評価等<sup>1</sup>の考え方

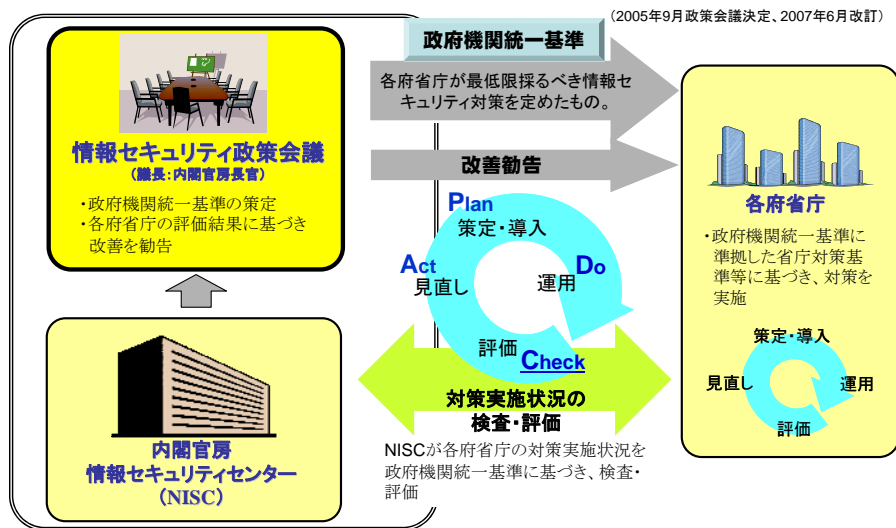
##### ① 評価等の視点

政府機関対策に関する情報セキュリティ対策の評価等は、各府省庁個別及び政府全体という政府機関の情報セキュリティ対策に係る2つのPDCAサイクルが着実に定着しているか確認を行うという視点に基づいて行う。

政府機関に係る対策実施指標は2009年度において「政府機関の情報セキュリティ対策のための統一基準の基本遵守事項について、『実施率を100%』、『把握率を100%』」とすることを目標とする。

#### 政府機関の情報セキュリティ対策の枠組み

各府省庁は政府機関統一基準を踏まえて情報セキュリティ対策を実施し、内閣官房情報セキュリティセンター(NISC)が各府省庁の対策実施状況を検査・評価。



##### ② 評価等の対象

内閣官房及び全府省庁(19機関)を評価等の対象とする。

<sup>1</sup> なお、評価等のうち、補完調査の考え方に関しては(2)において記述する

### ③ 評価等の方法

#### (ア) 重点検査

「政府機関の情報セキュリティ対策のための統一基準」において必須として実施すべき事項とされている基本遵守事項の実施状況の中でも特に重要な事項に着目し、効率化を図りつつその実施状況を重点的に検査する。今後2008年度末までに、次の重点検査を行う。

#### ○ 端末・ウェブサーバ・メールサーバ【継続調査】

(2008年7月から実施し、12月に各府省庁からNISCへ結果を提出。2009年2月に公表予定。)

端末・ウェブサーバについては、前2回の重点検査を通じて実施率100%の府省庁が半数となり、大幅な改善が図られている。また、メールサーバについては、前回検査において端末・ウェブサーバと同水準の対策状況であった。このため、端末・ウェブ・メールサーバのそれぞれについて、経年比較を行い、水準が維持・改善されているかについて把握する観点から、基本遵守事項の実施状況を検査する。

#### 電子メールサーバに関する情報セキュリティ対策の総合評価



重点検査の項目		電子メールサーバ		(参考) 端末	(参考) ウェブサーバ
電子メールサーバに関する重点検査項目		平成19年9月末		平成19年3月末	平成19年3月末
不正プログラム対策	・OSのセキュリティパッチ適用状況(アップデートの状況) ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況(アップデートの状況) ・電子メールコンテンツに対する不正プログラム対策の状況	内閣官房	B	B	B
サーバ管理	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況 ・時刻同期機能の動作	内閣法制局	B	B	B
不正アクセス対策	・不正中継対策の状況	人事院	A	A	B
情報保護対策	・電子メールの受信に係わる利用者に対する認証等の実施状況	内閣府	B	B	B
		宮内庁	B	A	A
		公正取引委員会	B	A	A
		警察庁	A	A	A
		金融庁	A	B	A
		総務省	B	B	B
		法務省	B	B	B
		外務省	B	A	B
		財務省	A	B	B
		文部科学省	A	A	A
		厚生労働省	A	B	B
		農林水産省	A	A	A
		経済産業省	A	A	A
		国土交通省	B	B	B
		環境省	A	B	A
		防衛省	A	B	A

・府省庁の調査に基づく結果  
・平成19年9月末時点

評価	実施率	評価	実施率	評価	実施率
A	x=100%	B	80%≤x<100%	C	60%≤x<80%
				D	x<60%

2

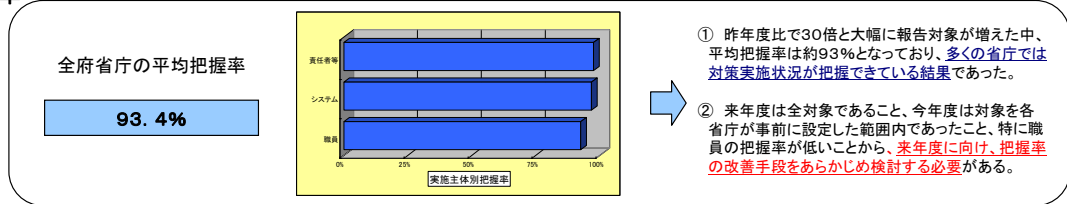
[重点検査の具体的なイメージ]

## (イ)対策実施状況報告

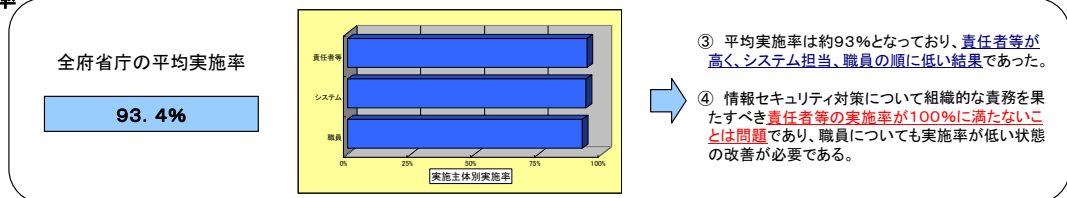
(2008年6月から実施し、2009年2月末に各府省庁からNISCへ結果を提出。4月に公表予定。)

政府機関における情報セキュリティ対策の実施状況を把握・分析するため、各府省庁の情報セキュリティ対策の実施状況について、2007年度に実施した評価手法を基本とし、6月にNISCから示した方針に基づき各省庁において効率化を図りつつ対象を拡大して評価を行う(全ての行政事務従事者を対象とする)。

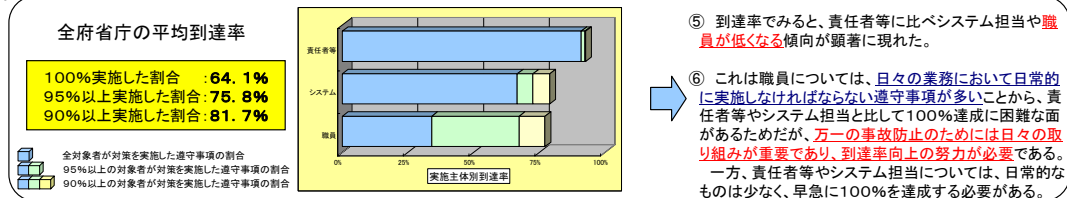
### 1 把握率



### 2 実施率



### 3 到達率



[対策実施状況報告の具体的イメージ]

## (ウ)情報セキュリティマネジメントの総合評価

(2008年8月から実施し、2009年1月に各府省庁からNISCへ結果を提出。4月に公表予定。)

各府省庁における情報セキュリティ対策に関するマネジメントが、計画・実施・評価・改善のいわゆるPDCAサイクルの各段階で確実に効果的に行われているかを評価するため、「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」(平成19年2月2日情報セキュリティ政策会議了解)における、「計画」「周知」「実施」「評価と改善」の各段階にわたる評価指標に基づき、各府省庁の情報セキュリティマネジメントの実施状況について、2006年度に実施した評価

手法を基本として効率化を図りつつ評価を行う。

政府機関の情報セキュリティマネジメントの総合評価～2006年度～

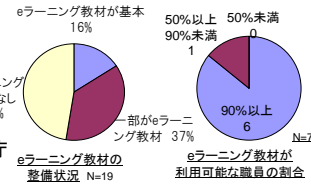
◆ 2006年度 情報セキュリティ・ベストプラクティス

★★ 省内ネットワークを活用した職員の支援 ・eラーニングシステム ・実施手順等の運用	総務省	経済産業省
★★ 幹部職員の下で全庁一体となった対策の推進	警察庁	
★★ 外部委託における情報セキュリティの確保	外務省	防衛省

- ・ 政府機関の模範となるプラクティス(★★)は「計画」及び「周知」を中心に44件。
- ・ 政府内外を問わず模範となる先進的な取り組み(★★★)は見られなかった。

◆ 各府省庁の体制等の調査結果

- ・ 情報セキュリティ担当者(常任)の職員に占める割合:  
2%超=4府省庁、0.5%以下=7府省庁
- ・ 情報セキュリティ担当者(常任)の平均経験年数:  
1年～3年を中心
- ・ eラーニング導入は府省庁全体では部分的:  
「eラーニング教材が(一部でも)ある」=10府省庁



※eラーニング:コンピュータネットワークなどを活用して教育を行うこと

[情報セキュリティマネジメントの総合評価の具体的なイメージ]

④ 関係府省庁

内閣官房及び全府省庁（19機関）が関係府省庁となる。

①重点検査	7月開始 → (12月回収) → 2月公表
②マネジメント評価	8月開始 → (1月回収) → 4月公表
③実施状況報告(自己点検)	6月開始 → (2月回収) → 4月公表

(2) 政府機関対策に関する2008年度の補完調査の考え方

① 補完調査項目

- (i) 強化遵守事項等の実施状況の調査（重点検査時に実施）
- (ii) 各府省庁の情報セキュリティ対応体制、監査の実施状況等の調査
- (iii) 社会的に問題となった情報セキュリティ上の課題に対応するための緊急調査（緊急事態の発生時に実施）

## ② 補完調査の趣旨

(i)の強化遵守事項等の実施状況調査については、強化遵守事項の適用状況や電子メールに関する規模、迷惑メール対策、暗号化メールの利用状況等、情報セキュリティ対策上重要な事項に関する状況の把握等を行い、今後の政府機関統一基準の見直し等に反映することを趣旨とする。

(ii)の各府省庁の情報セキュリティ対応体制、監査の実施状況等の調査は、情報セキュリティ担当者の経験年数、eラーニング導入状況、障害等への対応訓練の実施状況等2006年度の情報セキュリティマネジメントの総合評価において調査した項目を基本に、監査の実施状況も加え、各府省庁における十分な情報セキュリティ対策の実施に向けた課題の抽出・分析を行うことを趣旨とする。

(iii)の緊急調査は、DNSキャッシュポイズニングの脆弱性への対応等、社会的に問題となった情報セキュリティ上の突発的事項に関する政府横断的な課題への迅速な対応等のために行うことを趣旨とする。

## ③ 補完調査の調査方法

各府省庁の負担にならないよう、原則、重点検査やマネジメント評価で調査する項目に補完調査項目を追加する形で実施する（ただし、緊急調査は緊急事態の発生時に必要な項目について行う。）。

## ④ 関係府省庁

内閣官房及び全府省庁（19機関）が関係府省庁となる。

### 第2節 政府機関に関する「2009年時における我が国のあるべき姿」の達成度に関する評価等の考え方

第1次情報セキュリティ基本計画の最終年度として、以下の点について評価等を行う。

#### ① 政府機関統一基準とそれに基づく評価・勧告によるPDCAサイクルの構築

情報セキュリティ対策の強化のためには、政府機関における情報セキュリティ

対策の基準である政府機関統一基準の水準を世界最高のものとするとともに、それに基づく評価・勧告によるP D C Aサイクルが適切に機能する必要がある。

そのため、内閣官房において、政府機関統一基準の見直しを毎年行い、最新の技術や環境の変化を踏まえたものへと改訂を行うとともに、評価・勧告の枠組みによるP D C Aサイクルが機能しているかを評価するため、第1節のとおり重点検査、対策実施状況報告、マネジメントの総合評価等を引き続き実施し、その結果について経年比較を行う。

#### ② 政府機関・中長期的なセキュリティ対策の強化・検討

中長期的なセキュリティ対策の強化に向けて、政府機関全体が互いに協力することによる施策、例えばセキュリティ要求仕様の政府横断的な検討や、次世代電子政府構築の際の各種システム共通基盤的なセキュリティ機能の導入などに向けた検討が必要である。

そのため、政府機関（調達元）とベンダー（調達先）がどのように協業出来るかについて幅広く議論を行うための検討会を立ち上げるとともに、オンライン利用拡大行動計画（平成20年9月12日IT戦略本部決定）に基づき、電子政府の持続に応じたセキュリティ確保策、ユーザビリティ向上方策について、政府横断的なガイドラインを策定することに向け、電子政府ガイドライン作成検討会を設置し、政府機関横断的に検討を行っている。

中長期的なセキュリティ対策に強化に向けて、このような取組みを持続的に継続することが必要であり、2008年度末に、改めて政府横断的な検討状況の進展について把握を行う。

#### ③ サイバー攻撃等に対する政府機関における緊急対応能力の強化

政府機関の間で緊急対応を行う体制の整備については、政府横断的な情報収集、サイバー攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うためのG S O Cの整備・運用状況に関して確認を行う。

#### ④ 政府機関職員における人材育成

政府機関における人材育成については、各省庁において、I T人材・確保実行計画が策定されているところであり、情報セキュリティマネジメントの総合評価において、当該計画に基づき情報セキュリティに関する専門性の高い人材の活用や育成が計画的に進んでいるかを確認するとともに、総務省が実施している「情報システム統一研修」の情報セキュリティ関連カリキュラムの実施状況等を経年的・俯瞰的に見ることにより最終的な成果を把握し、「あるべき姿」と比較することによりその達成度を測る。

#### ⑤ 独立行政法人等のセキュリティ対策の改善

独立行政法人等についても、政府機関と同等水準を目指し、政府機関に概ね準じた程度までセキュリティ面での対策が進むことが必要である。そのため、独立行政法人がセキュリティポリシーを策定するための雛形を提供することにより、その対策を促進するとともに、2006年度に独立行政法人等における情報セキュリティ対策調査を実施したところである。2008年度は、2006年度調査のフォローアップを行うことにより、独立行政法人に情報セキュリティポリシーの策定、職員の教育・訓練の実施状況等、政府機関に概ね準じた程度まで情報セキュリティ対策が進んでいるかについて、各独立行政法人の業務の特殊性等に配慮しつつ把握する。



## 第4章 重要インフラ対策に関する2008年度の評価等

### 第1節 重要インフラ対策に関する2008年度の取組みの評価等

#### (1) 重要インフラ対策に関する2008年度の評価等<sup>2</sup>の考え方

##### ① 評価等の視点（目標）

重要インフラ分野における情報セキュリティ対策の評価等は、枠組み文書で定めたように、重要インフラの情報セキュリティ対策に係る行動計画（以下、「重要インフラ行動計画」とする。）において対策の向上を目的に定めた4本の施策の柱それぞれに係る取組みが着実に進んでいるかという点を測ることとなる。したがって、重要インフラ対策の評価等は、取組み（プロセス）の進捗具合を測る（プロセス評価）という視点に基づいて行う。

また、本作業に際しては、2007年度の評価において2008年度に向けた課題とされた事項についても留意することとする。

##### ② 評価等の対象

重要インフラ分野の情報セキュリティ対策の評価等は、重要インフラ行動計画の4本の施策の柱（安全基準等の整備、情報共有体制の強化、相互依存性解析の実施、分野横断的な演習の実施）に基づく取組みの進捗を対象とする。具体的には、行動計画の4本の柱に沿って、年度計画である「セキュア・ジャパン2008」に施策が盛り込まれていることから、これら施策の進捗度合いを測ることとなる。

##### ③ 評価等の方法

評価等にあたっては、4本の施策の柱それぞれについて、各年度の目標（具体的取組み）<sup>3</sup>ごとの進捗状況を、各重要インフラ分野の協力も得つつ、NISCが把握し、とりまとめを行う。

##### ④ 関係府省庁

<sup>2</sup> なお、評価等のうち、補完調査の考え方に関しては（2）において記述する

<sup>3</sup> 具体的取組みについては、重要インフラ専門委員会で検討を行うこととなる。その際、実際のIT障害の発生状況等も踏まえながら、行動計画に掲げられている取組みの着実な進捗を確保することに留意する。

内閣官房及び重要インフラ所管官庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）が関係府省庁となる。

## （２）重要インフラ対策に関する２００８年度の補完調査の考え方

### ① 補完調査項目

重要インフラ分野の情報セキュリティ対策の補完調査は、施策のプロセス評価と補完しあうことで、現状をよりの確に把握でき、より効果的な施策を効率的に企画・実施することに資する調査となるよう努力を行う。具体的には、第一に、評価を通じて把握する取組みの進捗度合いを補完するような参考データの推移を捕捉する。具体的には、下図の項目についてデータを捕捉する。

なお、下図中の１．安全基準の整備の状況については、２００７年度の評価の際の課題を踏まえて運営サイクルの調整を図り、調査時期を２００９年度の前半としているため、その評価については、２００９年度の評価に係る文書に内容を反映する。

#### 1. 安全基準等の整備の状況について

##### I. 各分野における安全基準等の認知率( $A/\alpha$ )

##### II. 各分野における安全基準等を踏まえた事業者の内規等の見直し率( $B/A$ )

$\alpha$ : 回収データ数

A: 認知していると回答した事業者等の数

B: 安全基準等を踏まえ見直しを行ったと回答した事業者等の数

※ なお、NISCにおいて検証する際の参考として、回収率( $\alpha/\alpha'$ )を把握。

$\alpha'$ : 調査協力を求めた事業者等の数

取り得る具体的調査方法も踏まえ、各分野における状況を把握する上で適切な調査範囲を設定。

例: 全事業者、OO加入者、任意抽出など。

#### 2. 情報共有体制の強化の状況について

##### I. 情報提供の件数

「実施細目」に規定する「情報提供」の件数(試験・訓練を含む。)

##### II. <sup>セブター</sup>CEPTOARを構成する事業者の数

※ なお、NISCにおいて検証する際の参考として、構成事業者の分野における位置付けを把握。

#### 3. 相互依存性解析の実施、分野横断的な演習の実施の状況について

**解析及び演習に要した年間延べ時間および延べ参加者数**

また、第二には、実際に発生したIT障害やITの機能不全等のうち、要因や対応等を把握・検証することが情報セキュリティ対策の状況のよりの確な把握や

向上に資すると考えられるケースの検証を、各重要インフラ分野の協力を得つつ行う。この際、主眼は個々の事業者等の帰責性を問うことではなく、あくまで今後の対策の企画・立案にあたって、対策による効用の極大化を実現するという点にあることに留意が必要である。この観点から、有効な分析等が進められるよう、関係府省庁や関係事業者等から十分に協力を得られるよう努力することが不可欠である。

## ② 補完調査の趣旨

上記項目に基づく補完調査は、(i)参考となるデータの推移の把握によって情報セキュリティ対策の取組みの浸透を確認し、(ii)個別のIT障害等の検証によって現実のリスクとそれに対する対応状況の変化を見ることで、重要インフラ分野の情報セキュリティ対策を進めた結果、生じた変化を重要インフラ分野総体的に把握することを可能にするものである。その上で、補完調査の結果を4本の柱に基づく施策に係るプロセス評価と組み合わせることで、2009年度の具体的目標に対して、現状がどの程度近づいたのかという点をよりの確に捉えられるようになることから、プロセス評価を効果的に補完することとなる。

また、次期重要インフラ行動計画の下での2009年度の取組みの具体化を進める際に活用できる有効なデータを把握することに資することとなる。

## ③ 補完調査の調査方法

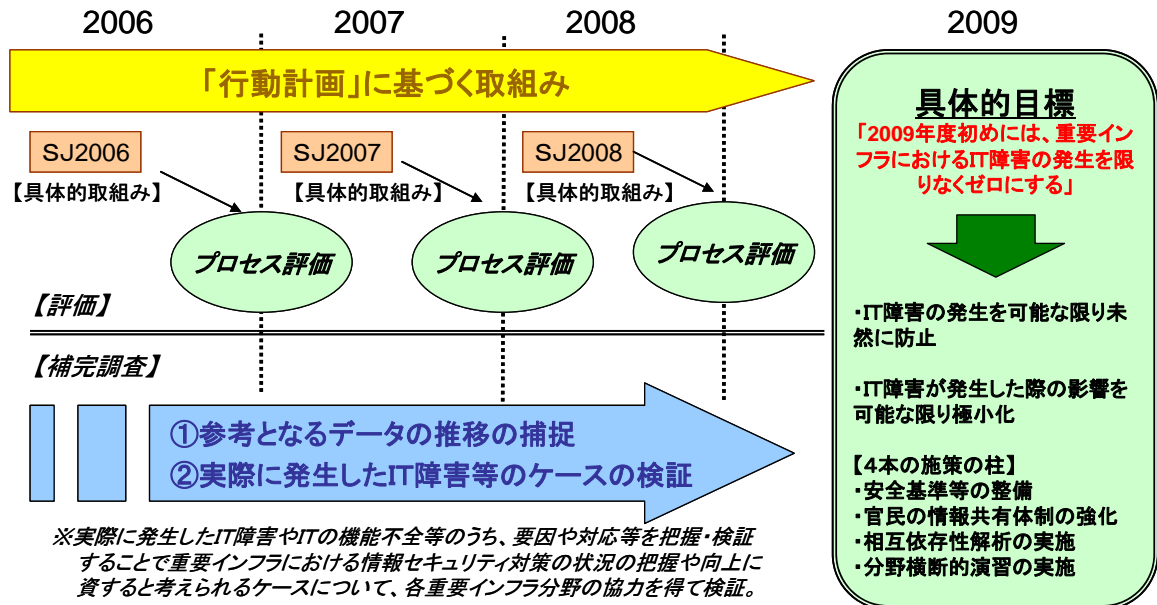
重要インフラ分野の情報セキュリティ対策の補完調査のうち、(i)参考となるデータの推移の捕捉については、各重要インフラ分野の協力も得ながら、事業者等へのアンケートその他の方法によって、データの把握・集計を行い、NISCがとりまとめる形で実施する。

また、(ii)個別のIT障害等のケースの検証については、状況の把握や対策の向上に資すると考えられるケースをNISCにおいて選択し、各重要インフラ分野の協力を得ながら、アンケートや聞き取り等の方法により進める。

## ④ 関係府省庁

評価同様、関係府省庁は内閣官房及び重要インフラ所管官庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）となる。

行動計画に基づき、09年度における「具体的目標」の達成に向けて毎年の具体的な取り組みを進めた結果、  
 [1] 毎年の具体的な取り組みが着実に予定通り進んだか評価を行う【重要インフラ対策の評価】とともに、  
 [2] ①指標に基づき、参考となるデータの推移を捕捉し、  
 ②実際に当該年度に発生したIT障害等のケースの検証を行う【補完調査】  
 その上で、これら[1][2]を総合的に見ることで、どの程度「具体的目標」に近づいたかを検証する



## 第2節 重要インフラ対策に関する「2009年時における我が国社会のあるべき姿」の達成度に係る評価等の考え方

### ① 評価等の視点（目標）

第1次基本計画の目標年度である2009年度時点での重要インフラ対策の目標は「(2009年度初めには)IT障害の発生を限りなくゼロにする」ことであり、この目標に対して、重要インフラ分野の情報セキュリティに係る状況が着実に近づいているかどうかを測ることとなる。

「2009年時における我が国のあるべき姿」に係る評価については、2006年度～2008年度の間における取組みのプロセス評価の全体を通して見ること並びに補完調査により得られたデータの推移及び補完調査による個別のIT障害等の検証の結果を総合的に見ることをもって次に掲げるところの実現状況を把握するという視点により行う。

- a) 自らの情報セキュリティ対策が十分であるか、各重要インフラ事業者等による自己検証がなされている。
- b) IT障害の未然防止、拡大防止・迅速な復旧、再発防止の3つの側面におい

て重要となる情報について、官民の各主体間で情報共有、連絡・連携がなされている。

- c) 重要インフラ分野間における I T 障害に関する相互依存関係を踏まえた重要インフラ分野での対応が適切になされている。
- d) 単にある時点において十分な対策がとられていることだけでなく、検証や見直し、さらなる強化に向けた取組み等の情報セキュリティ対策の向上に向けた取組み（すなわち P D C A サイクル）が、官民連携して継続的に行われている。

## ② 評価等の対象

重要インフラ分野の情報セキュリティ対策の評価等は、重要インフラ行動計画の 4 本の施策の柱（安全基準等の整備、情報共有体制の強化、相互依存性解析の実施、分野横断的な演習の実施）に基づく取組みの進捗を対象とする。具体的には、2008 年度が第 1 次基本計画に基づく取組みの最終年度であることを踏まえて重要インフラ行動計画の 4 本の柱に掲げられている目標に対しての進捗度合いを測ることとなる。

## ③ 評価等の方法

評価等にあたっては、4 本の施策の柱それぞれについて、2006 年度～2008 年度に得られた「進捗状況の評価」、「補完調査により得られたデータの推移」及び「補完調査による個別の I T 障害等の検証の結果」を N I S C が総合的に見ることにより行う。

## 第5章 企業・個人対策に関する2008年度の評価等

### 第1節 企業・個人対策に関する2008年度の実施状況の評価等

#### (1) 企業・個人対策に関する2008年度の実施状況の評価等の考え方

##### ① 評価等の視点

第1次基本計画においては、企業について「2009年度初めには、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旨とする」旨が、また個人について「2009年度初めには、「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旨とする」旨が掲げられている。企業・個人対策に関する評価等においては、2008年度の各種施策の取組みの結果、これらの目標へ、どれだけ近づけたかを測るという視点に立って作業を行う。

なお、評価等にあたっては、評価のあり方において明らかにした既存の各種指標<sup>4</sup>に基づく数値について、目標に対して、どの程度達成できているかという点に着目する。

##### ② 評価等の項目（評価指標）

第一に行政活動によって提供されたモノやサービスの量など、対策の浸透度を測るための指標として「アウトプット指標」を設定して作業を行う。具体的には、第1次基本計画で明らかにされている重点政策の柱<sup>5</sup>ごとに評価指標を設定し、評価等を実施する。

第二に、行政活動の結果、国民社会や社会生活に及ぼされる効果を図る指標として「アウトカム指標」を設定して作業を行う。具体的には、「意識面」、「対策面」、「インシデント発生面」の3つの評価指標を設定し、評価を実施する。

---

<sup>4</sup> 参照：別添1

<sup>5</sup> 企業については、(i)企業の情報セキュリティ対策が市場評価に繋がる環境の整備、(ii)質の高い情報セキュリティ関連製品及びサービスの提供促進、(iii)企業における情報セキュリティ人材の確保・育成、(iv)コンピュータウイルスや脆弱性等に早期に対応するための体制の強化。個人については、(i)情報セキュリティ教育の強化・推進、(ii)広報啓発・情報発信の強化・推進、(iii)個人が負担感なく情報関連製品・サービスを利用できる環境整備。

○ (各指標毎に性質を異にするため、目標については個別具体的に検討することになるが、)大まかな傾向としては、各指標を「意識に関する指標」「対策に関する指標」「インシデント又は犯罪の被害に関する指標」に分類、以下のとおり目標を設定することとする。

- ・ **意識に関する指標** …… 各統計を経年で観察し、それが増加(若しくは減少)傾向で推移することを目標とする。究極的には、ほぼ100%(若しくは0%)になることを志向する

(例)情報セキュリティ上のトラブルの重要性の認識

…… 各項目について、「非常に重要である」と回答する者の割合が増加傾向で推移することを目標とする。究極的には、ほぼ100%になることを志向する。

- ・ **対策に関する指標** …… パソコンを利用する者なら誰でも取るべき対策に関する統計については、各統計を経年で観察し、増加傾向で推移することを目標とする。究極的には、ほぼ100%になることを志向する。  
体制整備状況を表す指標については、一定規模・一定数が維持されることを目標とする

(例)ウィルス対策ソフト導入率

…… 「9割以上のパソコンに導入済」と回答する者の割合が増加傾向で推移することを目標とする。究極的には、ほぼ100%になることを志向する

(例)ISMS認証の取得事業者数

…… 取得事業者数が一定の水準で増加することを目標とする

- ・ **インシデント又は犯罪の被害に関する指標** …… 各統計を経年で観察し、減少傾向で推移することを目標とする。究極的には0%に限りなく近づくことを志向

(例)過去1年間の情報セキュリティに関する被害状況(企業)

…… 各項目について、減少傾向で推移することを目標とする、究極的には、0%に限りなく近づくことを志向する

(※ 第13回情報セキュリティ政策会議資料(平成19年8月3日開催)参照)

### ③ 評価等の方法

評価等にあたっては、上記の具体的な指標と既存のデータを活用し、数値が指標ごとに設定された具体的目標の達成に向けて推移しているか否かを把握することにより、指標ごとに評価等を行う。数値の分析においては、単年度の数値の増減にのみ着目するのではなく、数年間の数値の傾向について、社会背景等も加味する。また、評価対象期間が2007年度までのデータについては、その数値の推移から2008年度の状況を適宜合理的な範囲で推測する方法を併せて用いる。

その上で、指標ごとの評価等の内容を踏まえつつ、「企業全体」及び「個人全体」について、第1次基本計画に掲げられた目標にどこまで近づいたか評価等を行う。

### ④ 関係府省庁

関係府省庁は、内閣官房及び企業・個人の情報セキュリティ対策実施状況の把握に有益な既存データを有する府省庁となる。NISCは、これら府省庁と十分な連携を行うこととする。

## (2) 企業・個人対策に関する2008年度の補完調査の考え方

### ① 補完調査項目

2008年度の企業・個人対策の補完調査は、企業・個人の対策を推進する環境の現況について、政府機関と関わる側面から焦点を当てた調査を実施する。具体的には、以下の3点について補完調査を行う。

- (i) 電子政府の利用、活用、運用の状況に関する情報セキュリティの観点からの調査
- (ii) 政府機関が企業・個人から調達する製品・サービスに対する要求水準や選定プロセスの妥当性の確認調査
- (iii) 政府機関が企業に外部委託する際の委託先管理の適切性の確認

## ② 補完調査の趣旨

第一に、電子政府の利用、活用、運用の状況に関する補完調査については、政府機関と企業等との情報セキュリティの現状を比較できるようにすることで企業等における対策推進に貢献させる観点から、利用者である国民が電子政府のサービスを利用するに際してのトラブル発生状況について調査を行う。

第二に、調達及び外部委託については、2007年度調査に引き続き、政府機関が企業・個人から製品・サービスを調達し、また企業・個人へ外部委託する際の、情報セキュリティの観点からの取組みの進展を把握する。昨年度からの経年比較を行い、進展の度合いを把握し、企業・個人分野の対策をさらに進めるために必要な要点、課題を効率的に浮き出させることを目指す。

これら補完調査は、各府省庁の協力を得ながら実施することとなるが、関係機関に過度な負担が生じないような手法で調査を進めるよう十分に留意する。

## ③ 補完調査の調査方法

当該補完調査は、調査票を各府省庁に対して配布して調査を実施することとする。

## ④ 関係府省庁

内閣官房及び全府省庁が関係府省庁となる。ただし、当該補完調査は、大まかな状況を把握することが目的であることから、本省レベルを対象に調査を実施する。



## 第2節 企業・個人対策に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方

2008年度は、基本計画に基づく取組みの3年目（最終年度）であることから、基本計画に掲げられている目標の達成度を測ることが不可欠である。そのため、「評価のあり方」において「2009年時の我が国のあるべき姿」として「基本計画」の企業・個人分野の各政策に対応して掲げられたそれぞれの姿に対して、2008年度の時点でどれだけ近づけたかという視点での評価等を行う。評価等に当たっては、掲げられたあるべき姿に照らし、その姿への到達度を測る上で有用と思われる既存データの数値<sup>6</sup>を踏まえ、情報セキュリティに係る動向や社会的変化があるべき姿にどの程度近づけたかという点に着目して行う。

---

<sup>6</sup> 別添1に示す評価指標についてあるべき姿に照らし有用な数値データを用いる

## 企業・個人における情報セキュリティの評価指標

### (1) 企業・個人に係るアウトプット指標

#### ア 企業を支援する政府の施策

##### ① 企業の情報セキュリティ対策が市場評価に繋がる環境の整備に係る指標

企業による取引相手の情報セキュリティ対策状況確認の実施状況、情報セキュリティ報告書の作成状況、事業継続計画（BCP）の作成状況、情報セキュリティ対策の効果の認識の状況を指標とする。

(既存のデータ)

- ・「取引相手のセキュリティ対策状況確認を実施している企業の割合」(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を実施している企業の割合」(情報処理実態調査：経済産業省)
- ・「事業継続計画（BCP）の作成を実施している企業の割合」(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)

##### ② 質の高い情報セキュリティ関連製品及びサービスの提供促進に係る指標

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)

- ・「I SMS 認証の取得事業者数」(日本情報処理開発協会)
- ・「各国の ISMS 適合性評価制度認証取得数」(経済産業省)
- ・「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)

##### ③ 企業における情報セキュリティ人材の確保・育成に係る指標

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)

- ・「情報セキュリティセミナーの実施状況」(情報処理推進機構)
- ・「情報セキュリティアドミニストレータ試験合格者数」(情報処理推進機構)
- ・「テクニカルエンジニア試験（情報セキュリティ）試験合格者数」(情報処理推進機構)

##### ④ コンピュータウィルスや脆弱性等に早期に対応するための体制の強化に係る指標

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」

## イ 個人を支援する政府の施策

### ① 情報セキュリティ教育の強化・推進に係る指標

学校等における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)

- ・「情報セキュリティに関する指導力を有すると回答した教員の割合」(学校における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)

### ② 広報啓発・情報発信の強化・推進に係る指標

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)
- ・「情報の入手経路」(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)
- ・「希望する情報提供方法」(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)

### ③ 個人が負担感なく情報関連製品・サービスを利用できる環境整備に係る指標

(既存のデータ)

- ・「無線LAN機器のセキュリティ対策の必要性に関する周知状況」(インターネットの利用実態に関する調査：総務省)
- ・「サイバークリーンセンター活動実績(ボット対策)」(サイバークリーンセンター：総務省、経済産業省)

## (2) 企業・個人に係るアウトカム指標

### ア 各主体の意識

#### ① 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。

(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)の重要性の認識」(情報処理実態調査：経済産業省)

#### ② 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。

(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言葉の認知度」(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)
- ・「情報セキュリティ対策に関する意識」(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

### ① 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。

(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)
- ・「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)

#### 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。

(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)
- ・「パッチ適用実施率」(国内におけるコンピュータウィルス被害状況調査：情報処理推進機構)
- ・「ウィルス対策ソフト導入率」(国内におけるコンピュータウィルス被害状況

調査：情報処理推進機構)

### 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。

(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)

## ② 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。

(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新たな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

### ① 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、コンピュータウィルス、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(ウィルス感染、スパムメールの中継利用・踏み台、不正アクセス、DoS攻撃等)(ウィルス感染、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」(警察庁)
- ・「コンピュータウィルス、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)
- ・「情報セキュリティ被害経験」(個人)(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)
- ・「コンピュータウィルス遭遇率」(企業)(国内におけるコンピュータウィルス

被害状況調査：情報処理推進機構)

- ・「スパイウェア遭遇率」(企業)(国内におけるコンピュータウィルス被害状況調査：情報処理推進機構)
- ・「Bot感染PC台数の国際比較」(日本のICTインフラに関する国際比較評価レポート：総務省)

## エ (参考指標)ITを活用した経済の発展状況

ITを活用した経済の発展状況は、情報セキュリティと直接関係するわけではないが、この情報セキュリティの裏付けが伴って発展が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。

- ・「企業間 (BtoB) 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 (BtoC) 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)

## (備考)既存のデータとして引用した主な調査

- 「情報処理実態調査」(経済産業省)：有効回答数 4,264 件、回収率 44.9% (H19)  
<http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html>
- 「通信利用動向調査」(世帯編)(総務省)：有効回答数 3,640 件、回収率 58.2%(H19)  
<http://www.johotsusintokei.soumu.go.jp/statistics/statistics05b1.html>
- 「通信利用動向調査」(企業編)(総務省)：有効回答数 2,158 件、回収率 75.7%(H19)  
<http://www.johotsusintokei.soumu.go.jp/statistics/statistics05b1.html>
- 「不正アクセス行為対策等の実態調査」(警察庁)  
<http://www.npa.go.jp/cyber/research/index.html>
- 「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)
- 「情報セキュリティに関する新たな脅威に対する意識調査」(独立行政法人情報処理推進機構)：有効回答数 5,000 件(H20)  
<http://www.ipa.go.jp/security/fy20/reports/ishiki01/index.html>
- 「国内における情報セキュリティ事象被害状況調査」(独立行政法人情報処理推進機構)

## 第6章 横断的な情報セキュリティ基盤に関する2008年度の評価等

### 第1節 横断的な情報セキュリティ基盤に関する2008年度の評価等

#### (1) 横断的な情報セキュリティ基盤に関する2008年度の補完調査の考え方

##### ① 補完調査項目

横断的な情報セキュリティ基盤としては、第1次基本計画に基づき、(i)情報セキュリティ技術戦略の推進、(ii)情報セキュリティ人材の育成・確保、(iii)国際連携・協調の推進、(iv)犯罪の取締り及び権利利益の保護・救済の4つの分野が挙げられる。これら横断4分野に係る補完調査については、現時点では、特段具体的な調査テーマを設定はしない。補完調査を行う必要性が生じた時点で実施を検討することとする。

具体的には、例えば、現在、人材育成に関して業界横断的な情報セキュリティ人材の育成支援体制整備が民間主導で進められており、こうした取組みが本格化する段階に至った場合には、主要な情報セキュリティ関連資格の取得者数がどの程度変化したのか調査を行うということが考えられる。また、犯罪取締りに関して、サイバー空間における犯罪動向には様々な変化が見られているが、変化が特に顕著となった場合には、こうした状況について補完調査を実施するという事も考えられる。

##### ② 関係府省庁

現時点では、具体的な補完調査項目を設定していないものの、調査項目が設定された場合には、内閣官房及び当該補完調査項目に強い関連を有する府省庁が関係府省庁となる。

### 第2節 横断的な情報セキュリティ基盤に関する「2009年時における我が国社会のあるべき姿」の達成度に関する評価等の考え方

横断分野については、過去に補完調査を実施しておらず、今年度についても今のところ補完調査を予定していない。そのため、横断4分野に関する「あるべき姿」の達成度を測る方法は、まず、第1次基本計画に掲げられている項目ごとに、セキュア・ジャパン2006～2008における各施策の実施結果（アウトプット）を取りまとめる。次に、当該結果を経年的・俯瞰的に見ることにより、各項

目における最終的な成果について把握する。最後に、当該成果と横断4分野における「あるべき姿」を比較することにより、達成度を測る。

その際、例えば「犯罪の取締り及び権利利益の保護・救済」の分野においては、サイバー犯罪の検挙状況等に関する統計を参照し、サイバー犯罪の状況の変化を考慮する、また、「情報セキュリティ人材の育成・確保」の分野においては、情報セキュリティに係る資格の合格者数（又は保有者数）の推移や資格制度そのものの変遷などから人材育成に関する状況の変化について考慮するなど、極力関係する指標等を活用し、横断4分野を取り巻く環境の変化という視点も加味する。

なお、「2007年度の情報セキュリティ政策の評価等」及び「2006年度の情報セキュリティ政策の評価等」中の「第5章 横断的な情報セキュリティ基盤における現状の評価等」における評価も参考とする。



## 今後のスケジュール

今後の具体的な作業スケジュールについては、以下の図のとおりである。なお、下図において、S Jは年度計画であるセキュア・ジャパンを表し、S J 0 9は「セキュア・ジャパン2009」を意味する。また、政策会議は、情報セキュリティ政策会議を意味する。

