参考資料２

情報セキュリティ政策

２００７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）

２００７年１０月３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

我が国の情報セキュリティ政策は、情報セキュリティ政策の評価等の枠組み文書[1]（以下「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）、及び(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、毎年の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。本文書は、２００７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（ＮＩＳＣ）が作業方針を策定することとしており、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なる。

(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、２００８年３月頃までを目途に評価、補完調査、分析等の作業がなされ、作業の結果については、内閣官房情報セキュリティセンターを中心に２００７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、作業方針の策定にあたっては、作業方針が、(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、及び(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に十分留意する。

---

[1] 本文書では、「「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）」の２文書を合わせて「情報セキュリティ政策の評価等の枠組み文書」とする。

第２章　情報セキュリティ政策全体に関する２００７年度の評価等

（1）情報セキュリティ政策全体に関する２００７年度の評価等の考え方

①　評価等の視点

２００７年度は、第１次基本計画に基づく取組みの２年目であることから、２００６年度の取組みを踏まえた「官民における情報セキュリティ対策の底上げ」が年度の重点とされている。そこで、２００７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ということが重要である。

また、２００７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・立案され、また社会に対して影響を及ぼすことを意図して実施されるものである。このことから、第二の視点として、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。

さらに、第三には、評価等の取組みは、作業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ねらいの一つとして行われるものである。したがって、２００７年度の評価等においては、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、２００７年度の評価等の視点として、以下の３つを設定する。

(i)　２００７年度の重点である「官民における情報セキュリティ対策の底上げ」の達成度を測る視点
(ii)　情報セキュリティに係る２００７年度の様々な動向を測る視点
(iii)　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、(i)２００７年度の年度計画である「セキュア・ジャパン２００７」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が必要である。

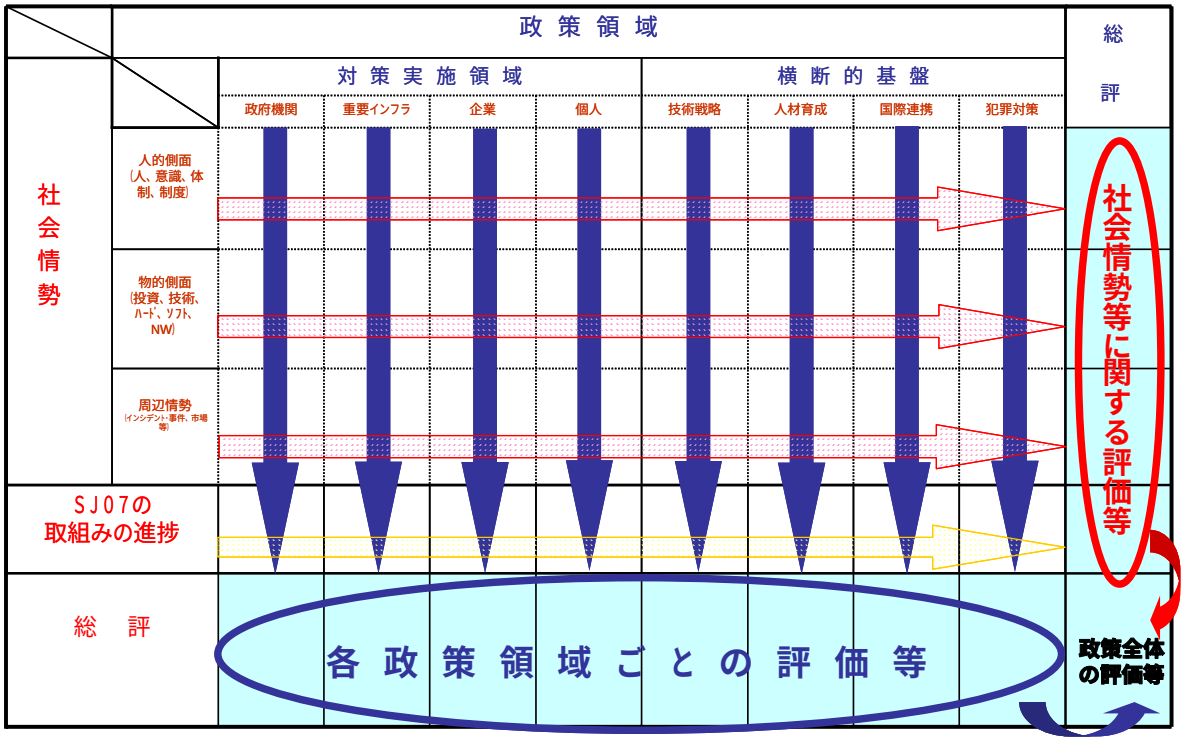
また、(ii)施策を進めた結果、情報セキュリティに係る動向にどのような変化が見られたかという点についても見ることが不可欠である。

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２００７」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、２００７年９月頃（上半期調査）及び２００８年２月頃（下半期調査）の２回実施する。

次に、２００６年度の評価等の検討手法に準じ、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３章　政府機関対策に関する２００７年度の評価等

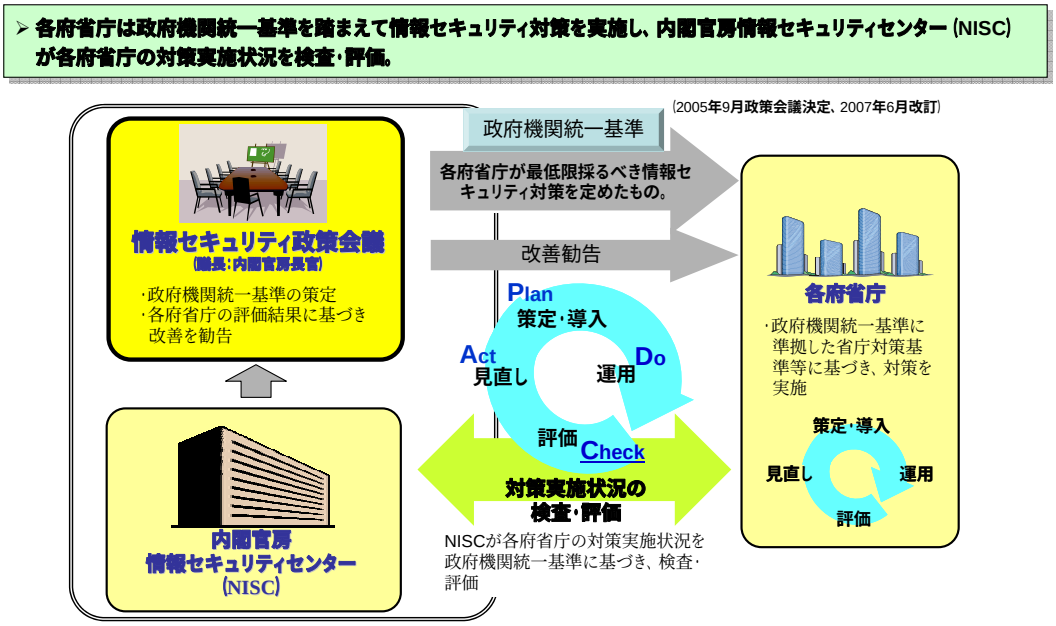
（１）政府機関対策に関する２００７年度の評価等[2]の考え方

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



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。

③　評価等の方法

[2] 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

(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１年間においては、次の重点検査を行う。

○ メールサーバ【新規調査】

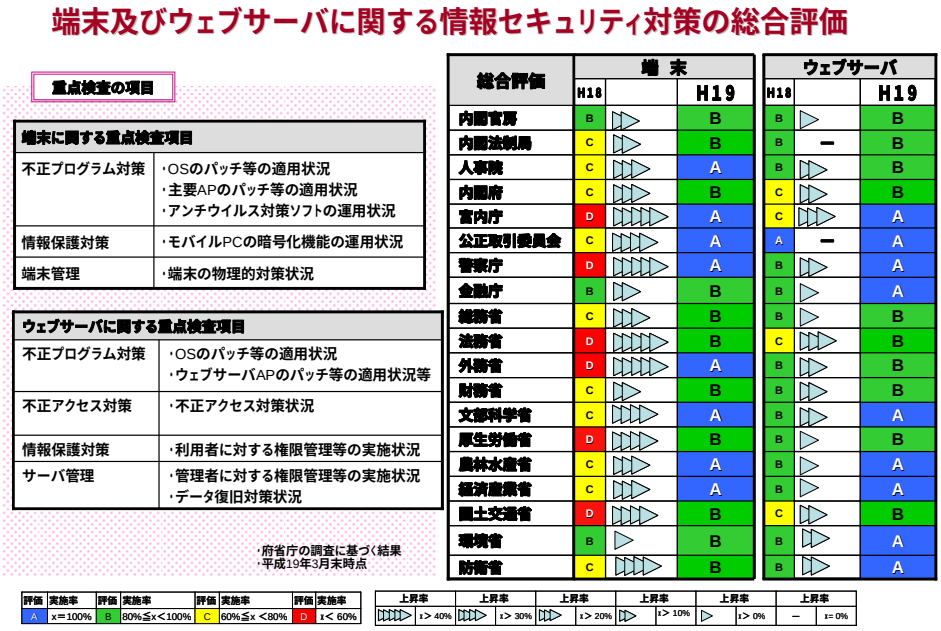
（２００７年９月から実施し、１１月に各府省庁から内閣官房情報セキュリティセンター（ＮＩＳＣ）へ結果を提出。１２月に公表予定。）

メールサーバは外部等と電子メールを送受信するためのサーバであり、不正プログラムや不正アクセス等により要保護情報が流出するなどのおそれがある。このことから重点検査として基本遵守事項の実施状況を検査する。

○ 端末・ウェブサーバ【継続調査】

（２００８年２月から実施し、５月に各府省庁から内閣官房情報セキュリティセンター（ＮＩＳＣ）へ結果を提出。７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大幅な改善が図られているが、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検査を行う。

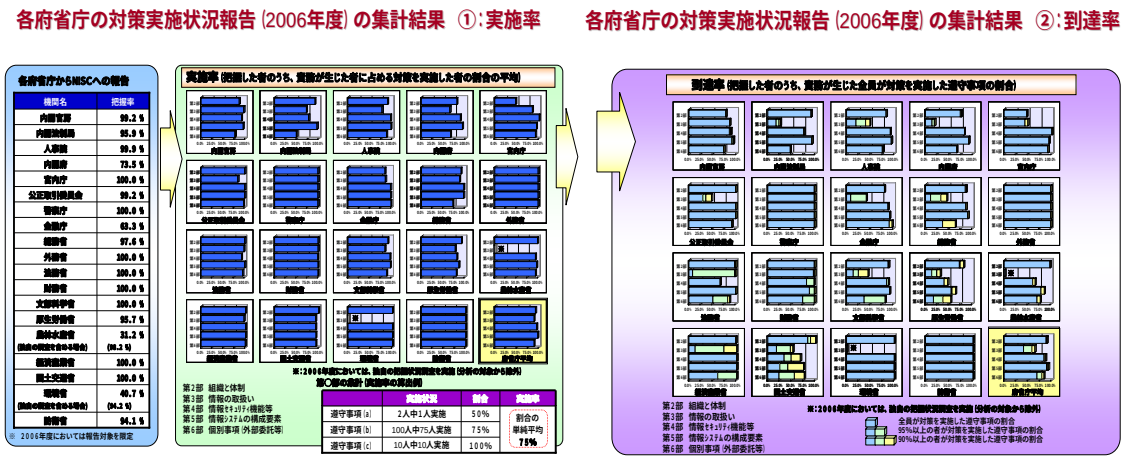


［重点検査の具体的イメージ］

(イ)対策実施状況報告

（２００７年１１月から実施し、２００８年２月末に各府省庁から内閣官房情報セキュリティセンター（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、２００６年度に実施した評価手法を基本とし、効率化を図りつつ対象を拡大して評価を行う（原則として全ての行政事務従事者を対象とする）。

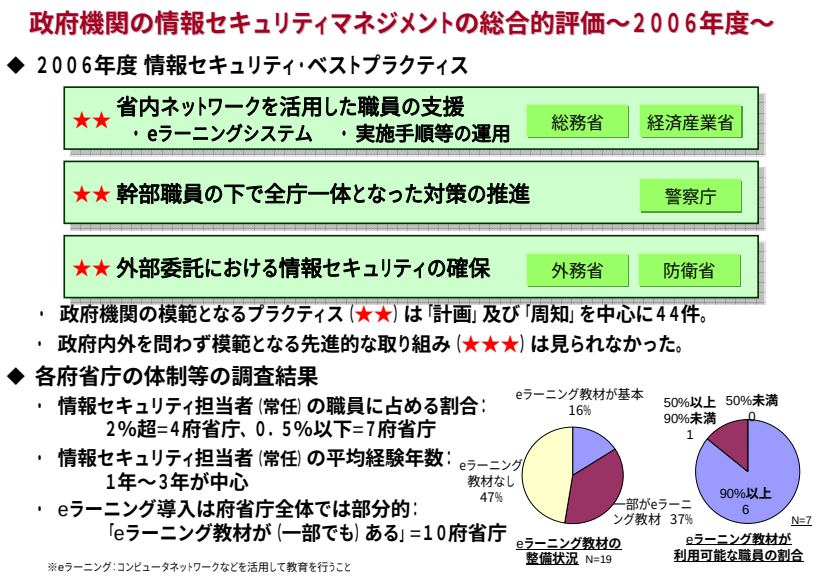


［対策実施状況報告の具体的イメージ］

(ウ)情報セキュリティマネジメントの総合評価

（２００８年２月から実施し、５月に各府省庁から内閣官房情報セキュリティセンター（ＮＩＳＣ）へ結果を提出。７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かつ効果的に行われているかを評価するため、「計画」「周知」「実施」「評価と改善」の各段階にわたる４５の評価指標に基づき、各府省庁の情報セキュリティマネジメントに関する評価を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。



［情報セキュリティマネジメントの総合評価の具体的イメージ］

なお、端末・ウェブサーバの重点検査及び情報セキュリティマネジメントの総合評価は、公表が２００８年７月となるため、２００８年度の評価等に係る文書に内容を反映する。

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	9月開始 →（11月頭回収）→ 12月公表	2月末開始 → （5月回収） → 7月公表
②対策実施状況報告	11月頭開始 → （2月末回収） → 4月公表	
③マネジメント評価		2月末開始 → （5月回収） → 7月公表

（２）政府機関対策に関する２００７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（情報セキュリティマネジメントの総合評価時に実施）
(iii) 企業・個人との比較のための状況調査（情報セキュリティマネジメ

ントの総合評価時に実施）第５章（２）１６ページを参照

(iv) 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)については、政府機関との比較により、企業・個人が必要な対策を検討するにあたって資することを趣旨とする。第５章（２）を参照。

(iv)の緊急調査は、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４章　重要インフラ対策に関する２００７年度の評価等

（１）重要インフラ対策に関する２００７年度の評価等[3]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、取組みの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。

なお、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」ことである。そのため、対策を通じて、重要インフラ分野の情報セキュリティに係る状況が当該目標へ着実に近づいていくことを目指し、取組みのプロセス評価においては、この点を確認すべく作業を行う。

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２００７」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）[4]ごとの進捗状況を、各重要インフラ分野の協力も得つつ、内閣官房情報セキュリティセンター（ＮＩＳＣ）が把握し、とりまとめを行う。

---

3 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

4 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。

④ 関係府省庁

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２００７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、現状をより的確に把握でき、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。

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／α）
Ⅱ. 各分野における安全基準等の見直し率（B／A）

α：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（α／α´）を把握。*
α´：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、○○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. CEPTOAR（セプター）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的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的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、重要インフラ行動計画は、「進捗状況の評価・検証結果を踏まえ、３年ごと（策定から２年後、進捗状況を踏まえ１２ヶ月掛けて見直す）又は必要に応じ、見直しを行う」こととされているが、当該補完調査は、行動計画の見直しに当たって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

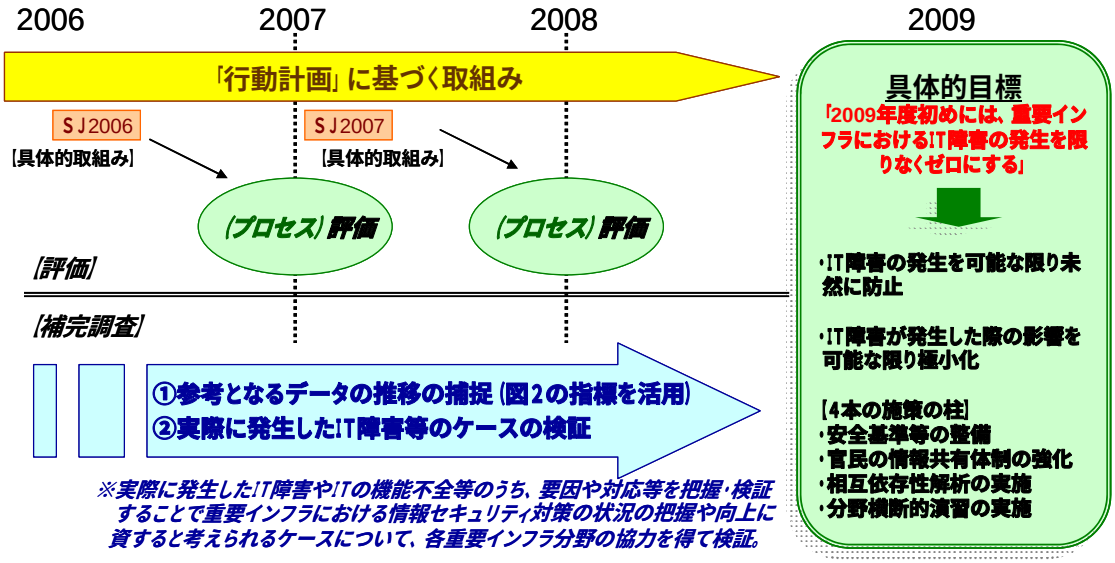
重要インフラ分野の情報セキュリティ対策の補完調査のうち、(i)参考となるデータの推移の捕捉については、各重要インフラ分野の協力も得ながら、事業者等へのアンケートその他の方法によって、データの把握・集計を行い、内閣官房情報セキュリティセンター（ＮＩＳＣ）がとりまとめる形で実施する。

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内閣官房情報セキュリティセンター（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取組みを進めた結果、
［1］毎年の具体的取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５章　企業・個人対策に関する２００７年度の評価等

（1）企業・個人対策に関する２００７年度の評価等[5]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目指す」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目指す」旨が掲げられている。企業・個人対策に関する２００７年度の評価等においては、各種の施策の取組みの結果、これらの目標に対して現状がどこまで近づい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、枠組み文書において明らかにした既存の各種指標[6]に基づく数値について、具体的目標の達成に向けて着実に推移しているか否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[7]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・対策の発生面」の３つの評価指標を設定し、評価を実施する。

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

---

5 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。

6 参照：別添１

7 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。

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２００６年度までのデータについては、その数値の推移から２００７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。内閣官房情報セキュリティセンター（ＮＩＳＣ）は、これら有益な既存データを有する府省庁と十分な連携を行うこととする。

○ （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）

（２）企業・個人対策に関する２００７年度の補完調査の考え方

① 補完調査項目

２００７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、セキュア・ジャパン２００７において示されているように[8]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ことで、企業・個人分野の対策をさらに進めるために必要な要点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

政府機関の負担が過度に増加することを防止する観点から、当該補完調査は、政府機関対策関連の調査・点検の際に、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。具体的には、２００８年２月に予定される端末・ウェブサーバの重点検査及び２００７年度マネジメント評価調査の際に、調査票を配布する。ただし、これらの評価結果は、２００８年度の評価等に係る文書に盛り込まれるというスケジュールである。このため、当該補完調査については、結果を２００７年度の評価等に係る文書に盛り込められるよう〆切の設定等を工夫する。

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。

---

8 参照：セキュア・ジャパン２００７　３４ページ

別添１

企業・個人における情報セキュリティの評価指標

⑴ 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

今のところ該当する既存のデータはないが、企業間の取引相手における情報セキュリティ対策の確認状況に関するデータ、事業継続計画（ＢＣＰ）の作成状況に関するデータ等の指標の追加については、今後、見直しの際に検討する。

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）

・「ＩＳＭＳ認証の取得事業者数」（日本情報処理開発協会）

・「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

a 企業に対する情報セキュリティ教育等に係る指標

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）

b 今後の検討課題

さらなる指標の追加の可否については、今後、見直しの際に検討する。

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」（JPCERT/CC）

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

a 実施体制･実施状況

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）

・「情報セキュリティを含む情報教育に関する教員向け研修を受けたことがある教員の状況」（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）

b 今後の検討課題

小学校における情報セキュリティを含む情報モラル教育を実施できる教員の存在率等の指標の追加の可否については、今後、見直しの際に検討する。

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

a 利用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）

b 今後の検討課題

その他ボット対策の実施状況等に係る指標の追加については、今後、見直しの際に検討する。

(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

a 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）

b 今後の課題

情報セキュリティ対策を行ったことによる顧客･市場等からの評価に関するデータ

等の指標の追加について、今後の見直しの際に検討する。

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ー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）

d 今後の課題

情報セキュリティ対策の維持及び改善に係る指標については、現時点で適当な指標が見あたらないことから、今後他の対策実施領域での取組みを参考にしつつ検討していくものとする。

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）

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 4641 件、回収率 48.9%（H17）
http://www.meti.go.jp/policy/it_policy/statistics/jyojitsu.htm

○ 「通信利用動向調査」（世帯編）（総務省）：有効回答数 3982 件、回収率 62.2%(H17)
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）：有効回答数 606 件、回収率 24.2%(H17)
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）
http://211.120.54.153/b_menu/houdou/18/07/06072407.htm

○ 「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 5142 件、回収率 51.4%（H17）
http://www.ipa.go.jp/security/products/products.html

○ 「国内におけるコンピュータウィルス被害状況調査」（独立行政法人情報処理推進機構）：有効回答数 1,701 件、回収率 25.9%（H17）
http://www.ipa.go.jp/security/products/products.html

第６章　横断的な情報セキュリティ基盤に関する２００７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２００７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分野が挙げられる。これら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ことも考えられる。

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。

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、ＳＪは年度計画であるセキュア・ジャパンを表し、ＳＪ０８は「セキュア・ジャパン２００８」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。