

平成 20 年 12 月 10 日
内閣官房情報セキュリティセンター (NISC)

第19 回情報セキュリティ政策会議の開催について

－「第2次情報セキュリティ基本計画」パブリックコメント案の決定等－

本日、「情報セキュリティ政策会議」(議長:内閣官房長官)の第19 回会合が開催され、その概要は以下のとおり。

なお、本会合では、「第 2 次情報セキュリティ基本計画」(案)、「政府機関の情報セキュリティ対策のための統一基準(第4版)」(案)及び「重要インフラの情報セキュリティ対策に係る第2次行動計画」(案)についてパブリックコメントに付すことが決定された。

1. 「第2次情報セキュリティ基本計画」下での政策推進について

我が国の情報セキュリティ政策は、情報セキュリティ問題全般に関する全体設計図である「第2次情報セキュリティ基本計画」(以下、「第2次基本計画」という。)と、分野別の個別設計図の組み合わせで推進。

この組み合わせにより、個別分野縦割りの対応を排し、我が国全体として主体横断的・分野横断的な視点を持って、複雑化する情報セキュリティ問題への的確な対応を推進。

また、本会合において、

「第 2 次情報セキュリティ基本計画」(案)

「政府機関の情報セキュリティ対策のための統一基準(第 4 版)」(案)

「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」(案)

について、本日から約 1 ヶ月間(平成 20 年 12 月 10 日～平成 21 年 1 月 13 日)にわたり、広く国民から意見を募集(パブリックコメント)することが決定。政策の受益者である国民にとって意味のある情報セキュリティ政策を取りまとめるため、多くの意見をいただけることを期待しております。

今後、寄せられたコメント等をもとに、さらなる検討を行い、来年 2 月を目途に決定する予定。

(1) 「第2次情報セキュリティ基本計画」(案)について

現在の我が国の情報セキュリティ政策における基本計画である「第1次情報セキュリティ基本計画」(平成18年2月2日情報セキュリティ政策会議決定)(以下、「第1次基本計画」という。)は、平成18年度から平成20年度までの3年間計画であるため、平成21年度以降の次期基本計画を定めるべく、「基本計画検討委員会」を設置。同委員会において、平成20年1月16日の第1回会合から計16回、次期基本計画の理念や目標、各論等についての検討、関係者・団体からのヒアリング等を実施するとともに、その結果などを取りまとめ、「第2次基本計画」(案)を策定。本日、情報セキュリティ政策会議において同案についてパブリックコメントに付すことを決定。

「第2次基本計画」(案)は、「第1次基本計画」における成果を踏まえ、政策の継続と更なる発展を目標に、今後の我が国の情報セキュリティに係る取組みについての「基本的な考え方」と「重点政策の方向性」を提示。

なお、これまで同様、本基本計画に基づいた年度ごとの推進計画である「セキュア・ジャパン」を策定するとともに、年度ごとの取組みの状況や社会的変化などに関する評価を行う予定。

(「第1次基本計画」の成果例)

第1次基本計画の成果:「情報セキュリティ政策の立上げ」

- 関係者の「気付き」を高めた
 - (例) →Winny に代表される P2P ソフトウェアによる情報流出の危険性
 - サイバー攻撃により情報を盗まれる危険性
 - システム障害で事業が止まる危険性
- 政策推進の枠組みを構築
 - (例) →政府機関の統一基準の基づく対策と評価
 - 重要インフラ事業者間での情報共有体制
 - 日米、日 ASEAN で情報交換を行う枠組み
- 事前対策の取組みが進捗

(「第2次基本計画」(案)の目標)

「政策の継続と更なる発展」

- 具体的取組みの持続的な推進と新たな課題への政策的対応
第1次基本計画の下で構築した基盤(枠組み)を活用して、具体的取組みを機能させる。
- 「事故前提社会」への対応力強化
事前予防の継続的な推進に加え、事後対応力の強化を図る。
- 合理性に裏付けられたアプローチの実現
情報資産の重要度とリスクの評価(アセスメント)に基づいて合理的(適切)な水準の対策を実施。

〔第2次基本計画〕(案)のコンセプト)

- 基本目標:「ITを安心して利用できる環境」の構築
- 基本理念:IT時代の力強い「個」と「社会」の確立
- 取組み方法:「新しい官民連携モデル」+情報提供側も視野に入れた取組みの推進

〔第2次基本計画〕(案)実施後の我が国社会の姿)

情報セキュリティに対する絶対的な無謬性の追求から脱却し、十分な事前対策を行ったとしても、事故が起こりうる場合があることを念頭に置いた取組みを進めることの重要性が国民に認知され、万一の事態でも各主体の事前準備や冷静かつ適切な対応により、事業継続性の確保や事後対応がなされる。また、主体ごとに、許容可能な範囲内にリスクを管理する形で、効果的・効率的に情報セキュリティ対策が実施されている。こうしたことの前提としては、一人一人が、また社会全体が理性的かつ主体的に考えられること(すなわち、IT時代の力強い「個」と「社会」の確立)が不可欠であり、このような状況の実現に向けて進展が見られている。

〔第2次基本計画〕(案)の主な施策)

○ 各政府機関が自発的に取組みを推進するための仕組みの構築

各政府機関に、最高情報セキュリティ責任者を補佐する専門的知見を持つ最高情報セキュリティアドバイザーの設置を義務化するとともに、これらの専門家の指示やアドバイスが組織全体に迅速かつ確実に反映できる仕組みを構築する。また、情報セキュリティ対策に関する説明責任を果たすため、それぞれの情報システムの現状を把握した上で、情報セキュリティに対する考え方、情報セキュリティ対策に係る目標や計画及びその実績と評価などについて客観的指標を積極的に活用して記述した「情報セキュリティに係る年次報告書」(情報セキュリティ報告書)を作成する。その際、報告書の客観性を確保する観点から、最高情報セキュリティアドバイザーがその作成に参画する。また、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、公表する。

○ リソース不足に負けない中小企業の情報セキュリティ対策の推進

人員、予算、ITインフラなど、主にリソース不足から対策が遅れがちである中小企業の情報セキュリティ対策が促進されるよう、様々な対策の中から適切な対策を容易に選択できるような環境を整備する。例えば、適切な情報セキュリティレベルを測るために活用される情報セキュリティベンチマークを引き続き改善し、自社の情報セキュリティレベルを客観的評価として提示するための統一的なチェックリストの開発、普及を図る。

また、中小企業のセキュリティ対策を促進するためには、簡便かつ安価なセキュリティ対策ツールを提供するなどの効果的な取組みが必要であるため、SaaSやAS

Pなどの活用の促進及びこれらサービス提供事業者における情報セキュリティ対策基準の提示・啓発などの取組みを行う。

○ 我が国のイニシアティブにより One-Asia の実現へ

アジアにおける脅威に対応し、情報セキュリティ対策の強化のための連携を推進するべく、以下の三つの取組みを実現することを目指す。

第一に、人のつながりの必要性を認識し、アジアにおける脅威動向の把握・分析を我が国とともに行う専門家・研究者を積極的に養成する。第二に、現在、国際機関や国際フォーラム等で議論されているアジアにおける共同の脅威動向の把握機能創設のための取組みに対し、我が国にとっても大きなメリットのある形で支援を行う。第三に、我が国は第1次基本計画期間中に構築した米国、欧州との連携を更に強化し、ベストプラクティスの共有や共同の取組みを通じて得られた教訓、情報をアジア地域に積極的に還元していく。

○ 官民の緊密な協力によるサイバー犯罪の根絶へ

法執行機関における取締り体制の強化、技能の向上、国際協調の推進等の基盤強化を一層推進する。

また、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強いIT社会構築のための官民連携に向けた取組みを推進する。

さらに、国民がサイバー犯罪の被害者とならないよう、犯罪の被害状況や手口、具体的な対策の方法等に関する広報啓発を一層推進する

(別紙 1-1-1～1-1-8 参照)

(2) 「政府機関の情報セキュリティ対策のための統一基準」改訂(案)について

政府機関における情報セキュリティ対策の統一的な基準である「政府機関の情報セキュリティ対策のための統一基準」については、技術や環境の変化等を踏まえ、必要に応じて見直しを行うこととしており、今回は、最近の事案の検証結果や現行の基準で対応していない新たな脅威へ対応するため見直しを実施。

なお、今回の改訂は、これまでの政府機関対策を通じて得られた知見等に基づき、政府機関統一基準のあり方について検討を行った結果も反映している。

今回の改訂の概要は以下のとおり。

- ① 第2次情報セキュリティ基本計画を踏まえた対応
最高情報セキュリティアドバイザーの設置を義務化
- ② 技術・環境の変化への対応
 - ・ ウェブの閲覧・送信時の危険性への対応

- ・ 電子メールのボット被害の危険性への対応
- ・ 無線 LAN 環境の脆弱性への対応
- ③ 実務に即した遵守事項の見直し等
 - ・ 基本編と情報システム編への分割
 - ・ 順守事項の集約
 - ・ 政府機関統一基準解説書の記述の明確化 等

今回の改訂により、政府機関における情報セキュリティ対策に係る PDCA サイクルの各プロセスにおけるマネジメントが強化されるとともに、電子メールの送受信やウェブの閲覧・送信時に係るセキュリティが向上することにより、政府機関の情報セキュリティのより一層の向上が見込まれる。

今後、必要に応じて統一基準を見直すことにより、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現し、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。

(別紙 1-2 参照)

(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」(案)について

官民の緊密な連携の下、重要インフラの情報セキュリティを強化することを目的とした、「重要インフラの情報セキュリティ対策に係る行動計画」(平成 17 年 12 月 13 日情報セキュリティ政策会議決定)については、平成 18 年度から平成 20 年度までの 3 年間の計画であるため、平成 21 年度以降の行動計画を定めるべく、重要インフラ専門委員会において検討を実施。

検討の結果を、重要インフラ防護に責任を有する政府と重要インフラ事業者等が自主的な取り組みを進めるに当たっての共通の行動計画とすべく、「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。)として取りまとめた。

(「第2次行動計画」(案)のポイント)

- 引き続き、「重要インフラにおける IT 障害の発生を限りなくゼロにすること」を目指すとともに、「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」を目標とする。
- 新たに、分野ごとに重要インフラサービスの検証レベルを設定して着実に改善を実施。
- 第1次行動計画において設定した施策の4つの柱(※)のほかに、新たに「環境変化への対応」を5つ目の柱に掲げ、変化に対する察知能力の向上と機敏な対応に取り組む。

(「第2次行動計画」実施後の我が国社会の姿)

- IT 障害は発生しないか、発生しても国民生活や社会経済活動に重大な影響を与えるような事態には至らない。

- 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。また、自らのおかれている状況を正しく認識するとともに、自らの活動目標を主体的に定めている。これにより、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うとともに、主体間で、自主的な協力が行われている。
- 「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、社会基盤の情報セキュリティを強化するためには、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。

すなわち、「安心があたりまえ」な「誰もが安心できる社会基盤」が実現されている。

※： 4つの柱とは、①安全基準等の浸透、②情報共有体制の強化、③共通脅威分析、④分野横断的演習を指す。

(別紙 1-3-1～1-3-3 参照)

2. 情報セキュリティ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、「第 1 次基本計画」と、それに基づく年度計画である「セキュア・ジャパン」により推進されているが、それら政策の進捗度合い等について毎年評価を実施することとしている。評価にあたっては、毎年、評価を行う際の評価指標、補完調査の項目、関係府省庁等を定めた作業方針を策定することとしており、「2008 年度の評価等に向けた「作業方針」」を政策会議に報告。

本年度の作業方針は、第 1 次基本計画の最終年度として、以下の2つの視点を設定。

- 「第 1 次基本計画」に掲げる政策について、全般の成果を測るとともに、次期基本計画における課題を明らかにする視点。
- 平成 20 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」に係る各種施策の達成度を図るとともに、情報セキュリティに係る動向を分析し、平成 21 年度の重点設定に資する視点。

なお、本作業方針に基づく評価結果については、「セキュア・ジャパン2009」(仮称)策定時に基礎資料として活用し、政策に反映させる。

(別紙2参照)

3. 「セキュア・ジャパン2008」の進捗状況(上半期)について

本年度の年度計画である「セキュア・ジャパン 2008」について、上半期の進捗状況について報告。

本年度中に実施することとなっている全 157 施策について進捗状況の内訳は下記のとおりであり、政府として実施すべき施策については、ほぼ全て年度内(又は予定内)に実施できる

目処が立っており、概ね順調に進捗している。

(進捗状況内訳)

- | | |
|-----------------------|-------------|
| ・「既に実施済み」 | 22 施策(14%) |
| ・「実施中であり、年度内に完了予定」 | 122 施策(78%) |
| ・「実施はまだであるが、年度内に完了予定」 | 10 施策(6%) |
| ・「年度内に実施できるか不明」 | 3 施策(2%) |

(別紙3参照)

4. その他報告事項について

(1) 平成21年度情報セキュリティ関連予算概算要求について

各府省庁における平成21年度予算の概算要求のうち、情報セキュリティに関係しているものは298億円であり、平成20年度の当初予算(299億円)と比較して-1億円、0.3%減となっている。

(別紙4-1参照)

(2) 電子政府の情報セキュリティを企画・設計段階から確保するための方策に係る検討状況について

行政情報システムにおける情報セキュリティ対策を考慮したライフサイクル管理の強化の実現を目標とし、経験・知見を有する有識者やベンダーを交えた検討会を設置。

平成20年度末を目途に一次報告書を取りまとめる予定。

(別紙4-2参照)

(3) 2008年度分野横断的演習について

IT 障害発生時における重要インフラサービスの維持・早期復旧、事業継続等に向けた課題抽出を目的として、2008年度分野横断的演習を実施。概要については、以下のとおり。本演習で得られた成果は、官民の情報共有体制の強化策の検討に役立てるとともに、各事業者において情報セキュリティ対策の向上に向けた取組みに活用されることを期待。

(開催概要)

- ・ 開催日時 平成20年12月1日(月) 12:30~18:30
- ・ 参加者数 136名(プレイヤー、事務局の合計)
- ・ 実施方法 詳細シナリオは事務局のみが把握しているという、現実に近い設定の下、分野ごとに小部屋に分かれ、メール、電話、Web ページを用いて情報交換を実施。

(別紙4-3-1~4-3-3参照)

(4) 平成 20 年度情報セキュリティの日について

昨年度に引き続き、2月2日の情報セキュリティの日の前後に、情報セキュリティの日功労者表彰を実施予定。

また、情報セキュリティの日の前後約 1 ヶ月間に各種関連行事を積極的に開催予定。
(別紙 4-4 参照)

【本件に関する問合せ先】

内閣官房情報セキュリティセンター(NISC)
山口補佐官、関参事官、安部参事官補佐
電話 03-3581-3768(センター代表)

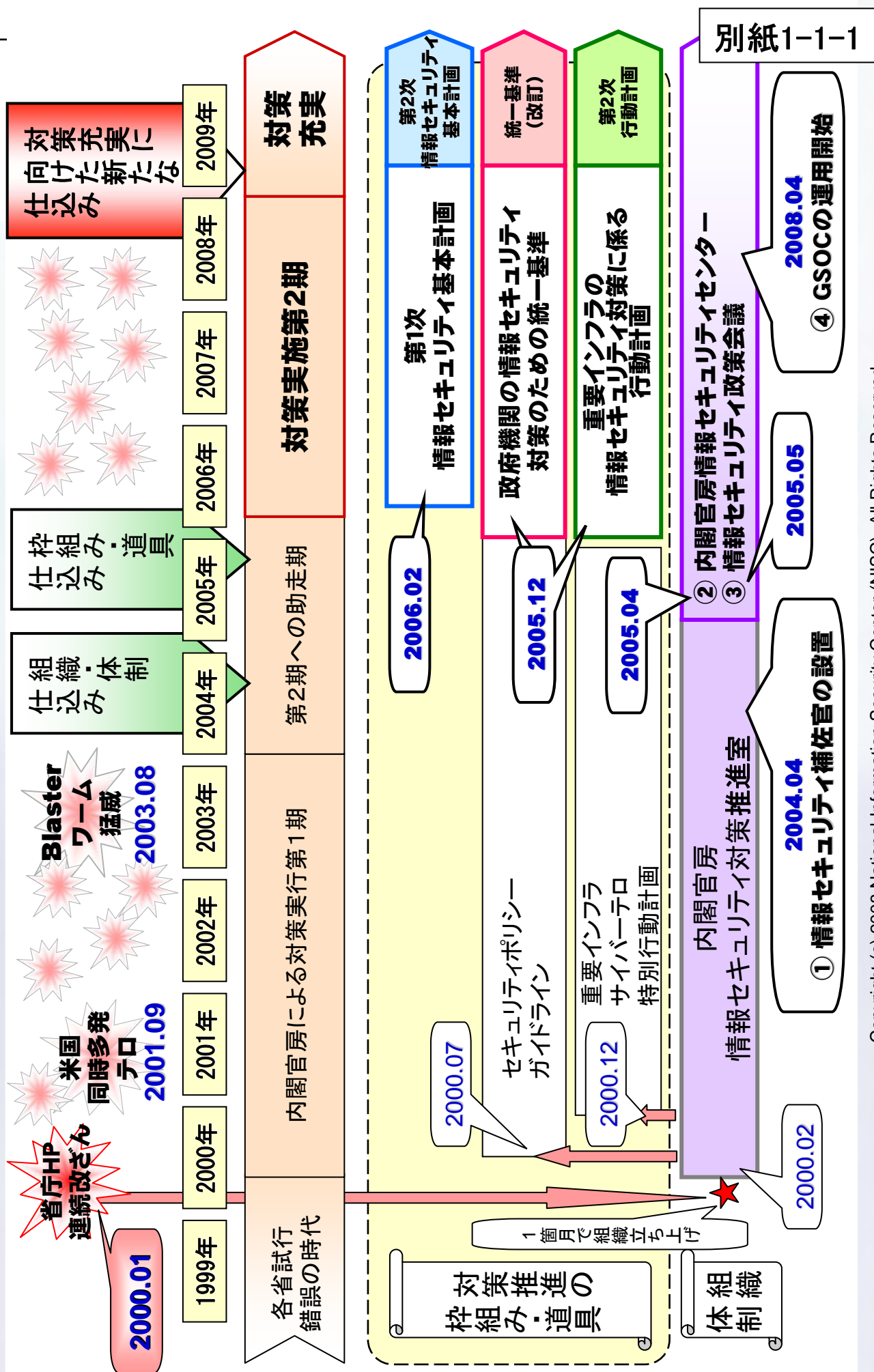
※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいて公表します。

(<http://www.nisc.go.jp/conference/seisaku/index.html#seisaku19>)

※ 「情報セキュリティ政策会議」は、平成 17 年5月 30 日のIT戦略本部決定によって設置されました。

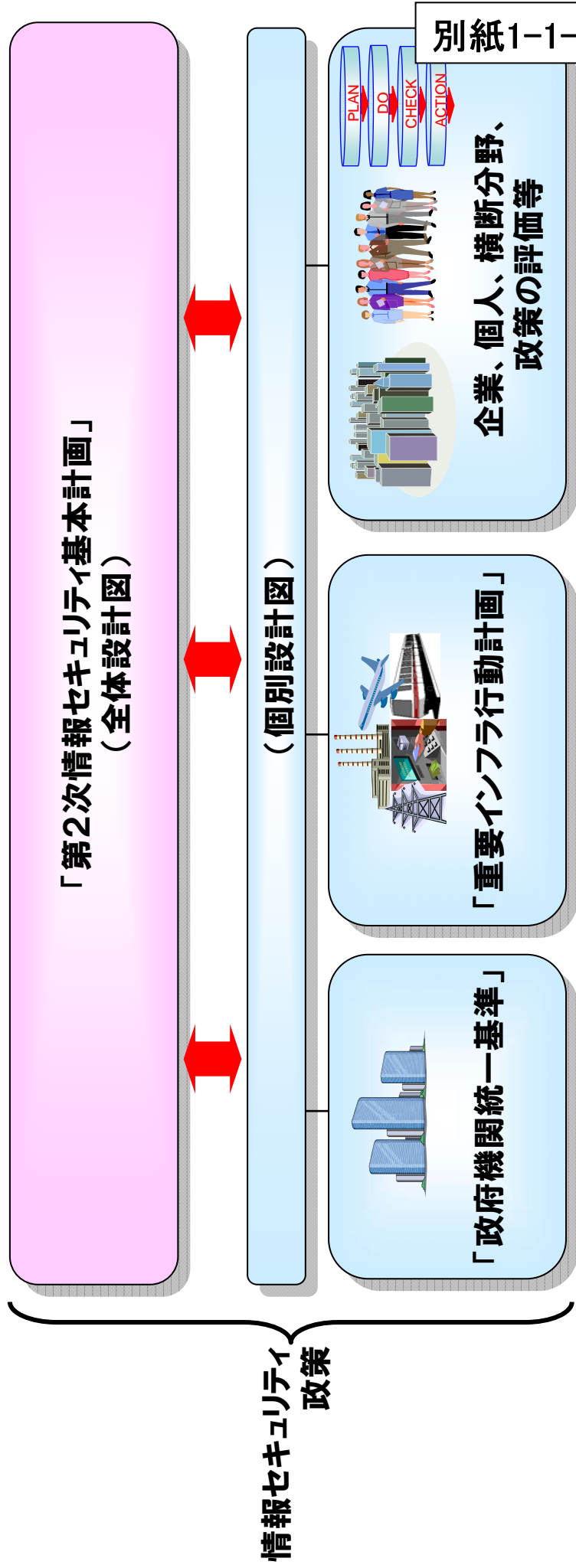
(<http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf>)

内閣官房における情報セキュリティ政策の流れ(2000年以降の概要)



全体設計図である「第2次情報セキュリティ基本計画」、分野別の個別設計図

- 情報セキュリティ政策は、情報セキュリティ問題全般に関する**全体設計図**である「**第2次情報セキュリティ基本計画**」と、**分野別の個別設計図**（例：政府機関対策における「政府機関統一基準」、重要インフラ対策における「重要インフラ行動計画」、政策の評価等の方法について定める枠組み文書）の**組み合わせで推進する**。
- このような組み合わせに基づくことで、個別分野縦割りの対応を排し、我が国全体として分野横断的・政策領域横断的な視点を持って、複雑化する情報セキュリティ問題への**的確な対応を進める**。



- ・2007年12月「次期情報セキュリティ基本計画」の策定へ向け、「基本計画検討委員会」(委員長:東京大学須藤修教授)を設置 (第15回情報セキュリティ政策会議決定)。
- ・2008年1月より、「基本計画検討委員会」による検討を実施(計16回、延べ48時間)。
- ・途中、関係者からのヒアリングを実施(8団体、1関係委員会、2政府機関)。
日弁連／全国市長会(藤沢市)／経団連／重要インフラ専門委員会／日本商工会議所／消費者団体(主婦連合会、東京都地域婦人団体連盟、全国消費者団体連絡会、日本消費生活アドバイザー・コンサルタント協会)／政府機関(国交省・外務省)
- ・第18回 情報セキュリティ政策会議(6月18日開催)において、「基本計画検討委員会」がとりまとめた「次期情報セキュリティ基本計画に向けた第1次提言」を報告。
- ・第1次提言報告後、約一ヶ月間のパブリックコメントを経た後、各論部分を検討するため、委員会での検討を7月から再開。以下のような分野についての検討を行った。
政府機関・地方公共団体、重要インフラ、企業・個人、横断的な情報セキュリティ基盤など
- ・今回の政策会議(12月10日)における、「第2次情報セキュリティ基本計画(案)」のとりまとめを旨として案文を作成。

1. 第1次基本計画('06～'08年)

成果

情報セキュリティ政策の立上げ

◆関係者の「気付き」を高めた

- P to Pソフトで情報流出の危険性
- サイバー攻撃で情報を盗まれる危険性
- システム障害で事業が止まる危険性

◆とりあえず政策推進の枠組みは構築

- 政府機関の統一基準に基づく対策と評価
- 重要インフラ事業者間の情報共有体制
- 日米、日ASEANで情報交換を行う枠組み

◆(問題が生じないための)事前対策の
取り組みはある程度進展

- 但し、日々新たなリスクが生まれ、また変化している

2. 第2次基本計画('09年～'11年)

目標

政策の継続と更なる発展

◆事前対策は当たり前のことに

◆問題が生じても、冷静かつ迅速に
事後対応・復旧活動を推進できる

◆情報を管理する側に加えて、情報を
預ける側も取組みの対象に

別紙1-1-4

第1章

第1次情報セキュリティ基本計画の下での取組みと2009年の状況

- 1 第1次情報セキュリティ基本計画の下での取組み (第1次基本計画の考え方などについて記述)
- 2 2009年の状況 (第1次基本計画の下で様々な取組みを進めた結果、どのような状況となっているか考察)

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年の姿

- 1 第2次情報セキュリティ基本計画の基本的考え方 (第2次基本計画の考え方などについて、適宜第1次基本計画と比較しながら記述)
- 2 2012年の姿 (第2次基本計画の下で様々な取組みを進めた結果、計画期間後にどのような姿となると考えているか記述)

第3章

今後3年間に取り組む重点政策

- 1 対策実施4領域における取組みの推進と政策目的の着実な実現 (政府・地方公共団体、重要インフラ、企業、個人について記述)
- 2 横断的な情報セキュリティ基盤の強化と発展 (技術、人材、国際、犯罪対策などについて記述)

第4章

政策の推進体制と持続的改善の構造について

- 1 政策の推進体制
- 2 他の関係機関等との関係
- 3 持続的改善構造の構築

○「**第2次情報セキュリティ基本計画(案)**」は、情報セキュリティ問題全般に係る中長期計画(全体設計図)として、今後の我が国の取組みに関する、**1)基本的考え方と、2)重点政策の方向性を提示。**

○具体的には、**2009年度～2011年度までの3カ年計画として策定。**これまで同様、本計画に基づいた年度ごとの推進計画である「**セキュア・ジャパン**」を策定するとともに、**年度ごとの取組み状況や社会変化などに関する評価等を行う予定。**

第1次基本計画からの「発展」と「継続」

- 1 具体的取組みの持続的な推進、新たな課題への政策的対応 (第1次基本計画で構築した取組みの各種枠組みを持続的に活用)
- 2 「事故前提社会」への対応力強化 (十分な事前対策の取組みにも関わらず、万が一問題が生じた場合を考えて準備を怠らない)
- 3 合理性に裏付けられたアプローチの実現 (情報資産の価値、リスクの大きさに応じた合理的(最適)な水準の対策を実現)

第2次基本計画の基本的考え方

- 基本目標 → 「ITを安心して利用できる環境」の構築 (第1次基本計画と同様。IT基本法第22条の実現)
- 取組みにあたっての基本理念 → 「セキュリティ立国」の思想の成熟 **(IT時代の力強い「個」と「社会」の確立へ)** (目指す「姿」は、最適な水準の取組みとセキュリティの実現であり、絶対的な無謬性の追求ではない → 絶対的な無謬性から脱却するには国民や社会全体の意識改革も不可欠)
- 基本目標の実現に向けた取組み → 官民の各主体が適切な役割分担を果たす「新しい官民連携モデル」
 + (対策実施側のみならず) **情報提供側も視野に入れた取組みの推進** (第1次基本計画の下では、対策実施主体及び対策支援主体による「新しい官民連携モデル」を追求。状況変化を踏まえ、新たに情報提供側も視野に入れた取組みを推進)

第2次基本計画の下で取り組みを行う政策領域

- 課題の把握から事前対策、事後対応まで視野に入れた取り組み
(事前対策のみならず、万が一問題が生じた場合も視野に入れて事後対応の準備を進める)
- 技術面での対応から制度面、人的側面の対応まで視野に入れた取り組み
(技術開発から人材育成のような側面まで幅広く取り組みを進める)
- 国内における対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取り組み
(IT利用・活用においては国境を越えるのは当然となっており、国内の取組みと国際的な取組みを有機的に結びつけた取組みとする)
- 国民の日常生活や経済活動といった個別主体に関係の深い領域から、安全保障や文化といった我が国全体に関係の深い領域にまで対応した取り組み
(情報セキュリティ問題は相当程度幅が広いことに鑑み、様々な観点から柔軟かつ領域横断的に取組みを進める)

1. 第2次情報セキュリティ基本計画案を踏まえた対応

1-1 政府機関におけるPDCAサイクルの各プロセスにおけるマネジメントの強化への対応

最高情報セキュリティアドバイザーの設置を義務化し、専門家の指示やアドバイザーが組織全体に迅速かつ確実に反映できる仕組みを構築。

2. 技術・環境の変化への対応

2-1 ウェブの閲覧・送信時の危険性への対応

ウェブクライアントのセキュリティ設定、ウェブサイト送信時の安全確認に係る対策を追加。

2-2 電子メールのボット被害の危険性への対応

電子メール送信時認証を基本遵守事項に変更。

2-3 無線LAN環境の脆弱性への対応

要機密情報を取り扱う無線LAN環境については、通信内容の暗号化を必要とすることを追記。

3. 実務に則した遵守事項の見直し等

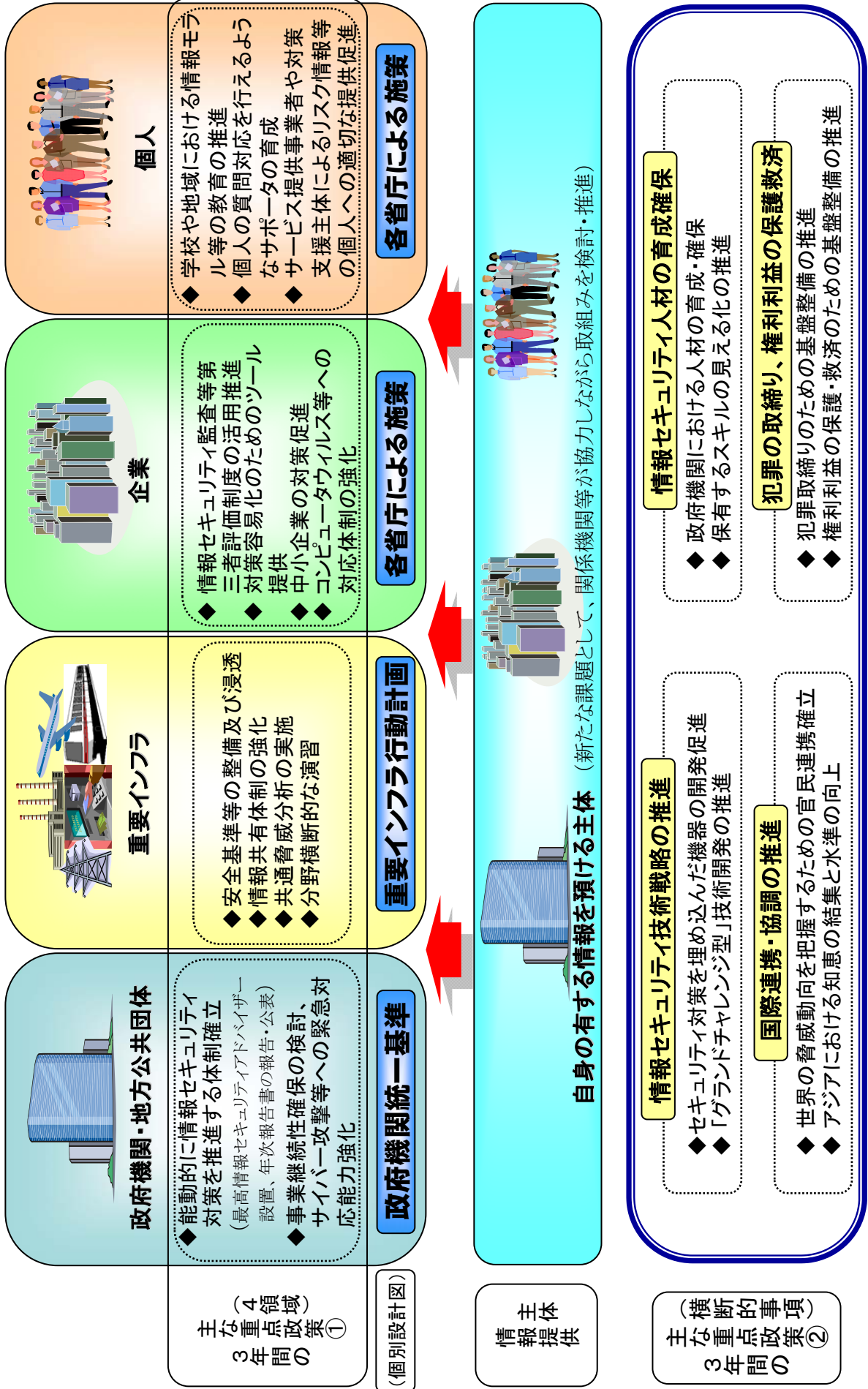
3-1 基本編と情報システム編への分割

2編分割により、省庁対策基準の決裁レベルを分けることを容易にし、より機動的な運用を可能とする。

3-2 遵守事項の集約

文書整備に係る遵守事項等を集約し、分かりやすさの向上を図る。

3-3 政府機関統一基準解説書の記述の明確化 等

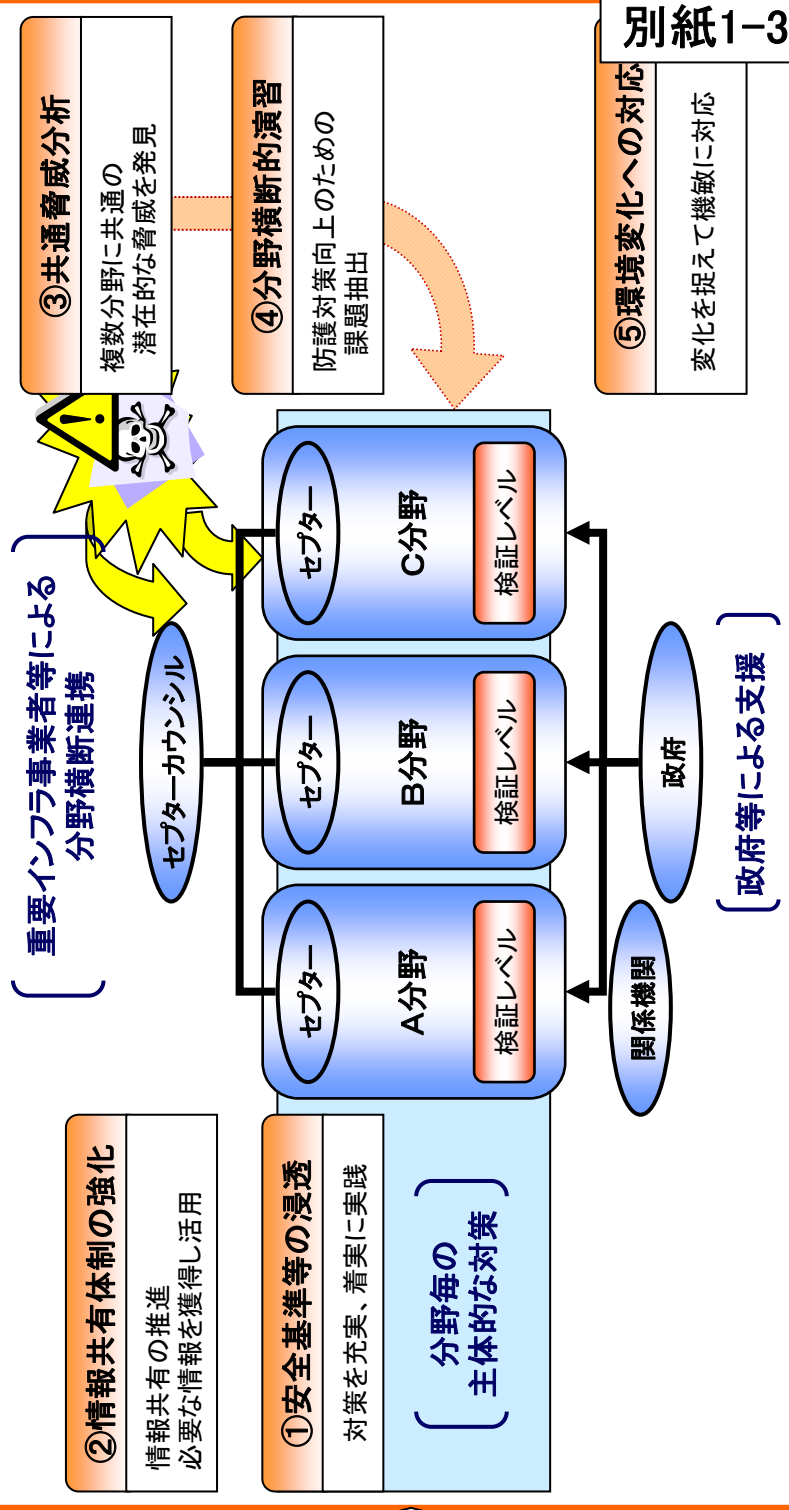


- 「重要インフラにおけるIT障害の発生を限りなくゼロにすること」を旨とする、「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標に官民が連携して重要インフラ防護に取り組む
- 新たに分野毎(*)に重要インフラサービスの検証レベルを設定して着実に改善を実施
- 第1次行動計画において設定した施策の4つの柱に「着実に改善」を添え、また経験を改善につなげるとともに、新たに「環境変化への対応」を5つめの柱に掲げ、変化に対する察知能力の向上と機敏な対応に取り組む

第1次行動計画の成果 【2006年度～2008年度】

- ①安全基準等**
 - ・重要インフラにおける情報セキュリティの確保に係る「安全基準等」策定にあたっての指針を策定、改定
 - ・各分野にて安全基準等の策定、見直し
- ②情報共有体制**
 - ・官民の情報提供・連絡の体制を整備し、情報提供・情報連絡を開始
 - ・各分野にてセブターを整備
 - ・セブターカウンシルを創設(予定)
- ③相互依存性解析**
 - ・静的相互依存性解析を実施
 - ・動的相互依存性解析を実施
- ④分野横断的演習**
 - ・研究的演習、机上演習を実施
 - ・機能演習を実施

第2次行動計画の施策の枠組み 【2009年度～2011年度】



別紙1-3-1

第2次行動計画の概要

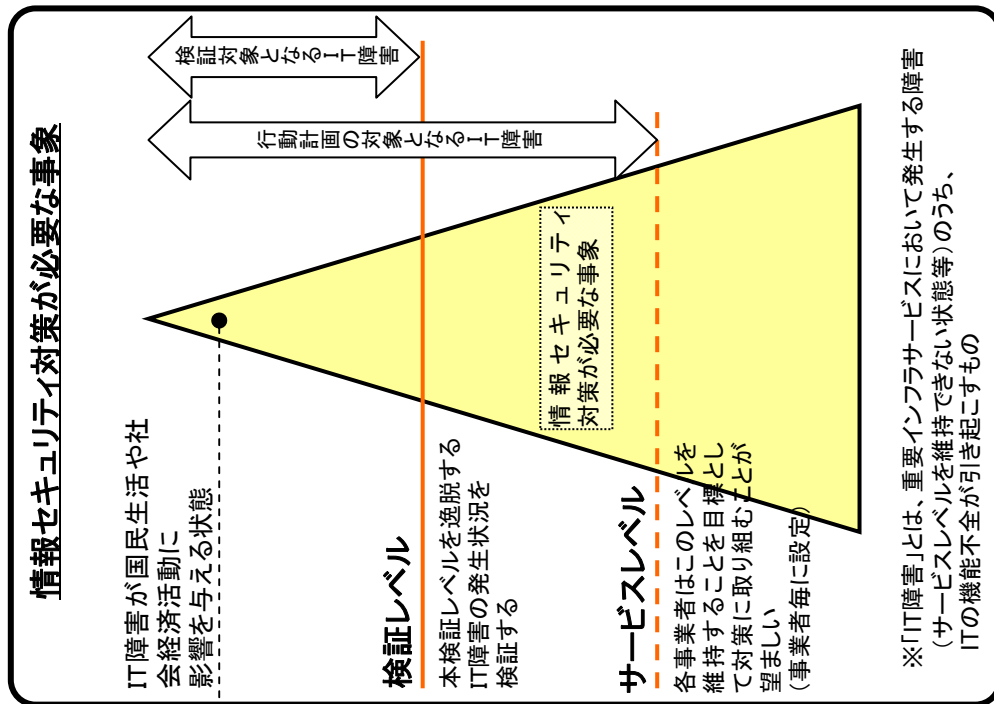


| | |
|---|--|
| ○ IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすることを目標として継続 | |
| | 第2次行動計画 (2009-2011) |
| 総論 | <ul style="list-style-type: none"> 想定する脅威や防護すべき重要システム等の対策の範囲を設定 情報セキュリティ対策に関する官民連携の施策の枠組みを構築 |
| | 第1次行動計画 (2006-2008) |
| | <ul style="list-style-type: none"> 想定する脅威や防護すべき重要システム等の対策の範囲を設定 情報セキュリティ対策に関する官民連携の施策の枠組みを構築 |
| | 第2次行動計画 (2009-2011) |
| | <ul style="list-style-type: none"> サービシレベルと検証レベルを定義、脅威等の対象範囲を見直し アウトカムとなる「理想とする将来像」を提示 |
| | 1 安全基準等の整備及び浸透 |
| | <ul style="list-style-type: none"> 『安全基準等』策定にあたっての指針』の充実 各分野毎に「安全基準等」の継続的な改善の実施と、確実な浸透 |
| | 2 情報共有体制の強化 |
| | <ul style="list-style-type: none"> 情報セキュリティ対策に資する、共有すべき情報を整理 情報の分析等のセプターに期待される機能を示し、必要な支援を実施 分野横断的な情報共有等のセプターカウンスルに望まれる事項を提示 |
| | 3 共通脅威分析 |
| | <ul style="list-style-type: none"> 潜在的なリスクチェーンの把握等のため相互依存性解析を継続 検討対象を技術、システム、環境等に拡大した分野共通の脅威を分析 |
| | 4 分野横断的演習 |
| | <ul style="list-style-type: none"> 具体的なIT障害の発生を想定した分野横断的演習を継続的に実施 |
| | 5 環境変化への対応 |
| | <ul style="list-style-type: none"> 広く協力、支援を得るため広報公聴活動を実施 国際会合や他国機関との対話を通じた国際連携を推進 |
| | <ul style="list-style-type: none"> 分野毎にIT障害の検証レベルを設定し、また施策毎に検証指標を設定して、報セキュリティ対策の継続的な検証と改善に取り組む 指標だけでは把握しきれない状況を収集するために、補完調査を実施 3年毎又は必要に応じて行動計画を見直し |
| | 情報セキュリティ対策の柱 |
| | 評価・検証 |

別紙1-3-2

重要インフラサービスの検証レベル

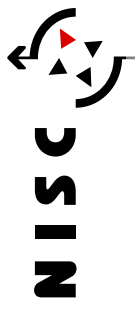
- **重要インフラ分野毎に業法上の義務的な取組みに加えて、新たに検証レベルを設定し、これを逸脱するIT障害の発生状況を毎年検証して行動計画の改善を期す**
- **重要インフラ事業者等は検証レベルによらず各々サービスレベルを定め、これを維持することを目標として対策に取り組む事が望ましい**



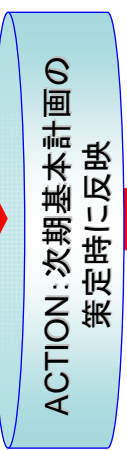
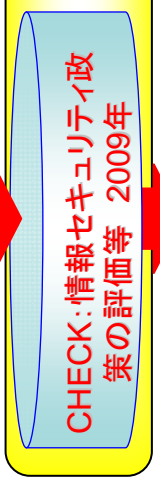
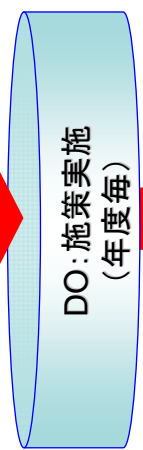
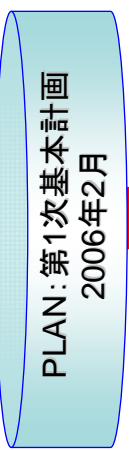
| 重要インフラ分野 | 検証レベル (一部表現を簡素化) |
|--------------------------|--|
| 情報通信 | <ul style="list-style-type: none"> ・電気通信業務の停止、品質の低下が、3万以上の利用者に対し2時間以上継続する事故が生じないこと ・放送の停止が生じないこと |
| 銀行 | <ul style="list-style-type: none"> ・預金の払戻しの遅延、停止が生じないこと ・融資承諾をした貸付の実行の遅延、停止が生じないこと ・為替(銀行振込)の遅延、停止が生じないこと |
| 生命保険 | <ul style="list-style-type: none"> ・保険金等の支払いに遅延、停止が生じないこと |
| 損害保険 | <ul style="list-style-type: none"> ・保険金等の支払いに遅延、停止が生じないこと |
| 証券会社 金融商品取引所 | <ul style="list-style-type: none"> ・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 ・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 |
| 航空 | <ul style="list-style-type: none"> ・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"> ・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 |
| ガス | <ul style="list-style-type: none"> ・供給支障戸数が30以上の供給支障事故が生じないこと |
| 政府・行政サービス (地方公共団体を含む) | <ul style="list-style-type: none"> ・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 |
| 医療 | <ul style="list-style-type: none"> ・診療録等の保存に支障が生じないこと |
| 水道 | <ul style="list-style-type: none"> ・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 |
| 物流 | <ul style="list-style-type: none"> ・貨物運送の停止や貨物の紛失が生じないこと |

別紙1-3-3

情報セキュリティ政策に関する評価について



基本計画単位 PDCAサイクル(3年単位)



・情報セキュリティ政策については、毎年評価を実施

・評価の実施に当たり毎年「評価等に向けた作業方針」を策定

・今年度は第1次基本計画の最終年度として、「2009年時における我が国社会のありべき姿」の達成度についても評価を実施

・評価の結果は、2009年度の年次計画(セキュア・ジャパン)に反映

※本来であれば次期基本計画に反映させるべきであるが、策定時期の関係上、セキュア・ジャパンに反映する。

【第1次基本計画の目標】(「2009年時における我が国社会のあるべき姿」)
IT利用促進の推進
政府機関・企業に世界最高レベルに
重要インフラのIT障害発生を限りなくゼロに
企業のセキュリティ対策を世界トップクラスに
IT利用に偏重を減じ個人を限りなくゼロに

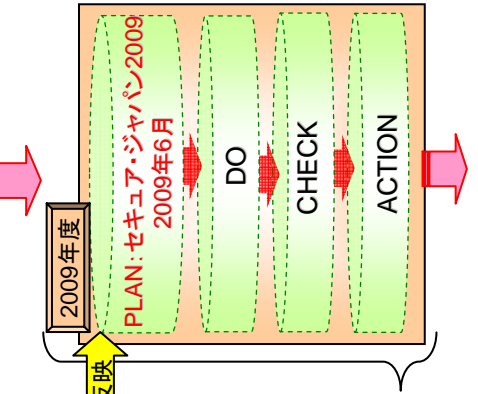
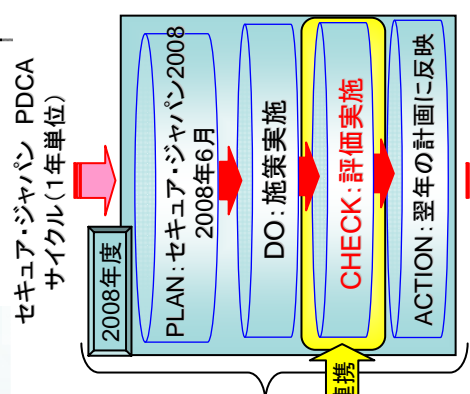
毎年、当該年度の施策実施計画であるセキュア・ジャパンを策定(毎年の実施計画にもPDCAサイクル有り)

評価を行うに当たり「作業方針」を策定(2008年12月)→評価手法、評価指標、補充調査等を定める

評価により判明した課題等を次期基本計画や年次計画の策定に反映

現在、2009年2月の策定を目指し検討中。

次期基本計画下においても、セキュア・ジャパンを策定予定



(参考)「セキュア・ジャパン2008」(全157施策)の進捗状況(上半期)の概要

- ① 「既に実施済み」
- ② 「既に具体的な検討や実施に向けた準備を進めており、年度内(又は予定内)に実施できる予定」
- ③ 「今後具体的な検討や実施に向けた作業を開始する予定だが、年度内(同上)に実施できる見込み」
- ④ 「現時点では、年度内(同上)に実施できるどうか不明」

- ... 22施策 (14%)
- ... 122施策 (78%)
- ... 10施策 (6%)
- ... 3施策 (2%)

(※ 小数点以下四捨五入)

別紙2

「セキュア・ジャパン2008」の進捗状況(上半期)について

「セキュア・ジャパン2008」の進捗状況(上半期)の概要

- ① 「既の実施済み」
... 22施策(14%)
- ② 「既に具体的な検討や実施に向けた準備を進めており、年度内(又は予定内)に実施できる予定」
... 122施策(78%)
- ③ 「今後具体的な検討や実施に向けた作業を開始する予定だが、年度内(同上)に実施できる見込み」
... 10施策(6%)
- ④ 「現時点では、年度内(同上)に実施できるどうか不明」
... 3施策(2%)

(※ 小数点以下四捨五入)

上記で「③」とされている施策について:

他の施策の実施スケジュールとの兼合いや、他の政策の検討の結果・結論等が出るまでは検討できないために上半期中においては未着手という施策もあるが、いずれの施策も実施に向けたスケジュールは立っており、全て年度内(予定内)に実施できる見込み。

上記で「④」とされている施策について:

サイバー犯罪を締結するための法律整備等の推進、刑事共助に関する条約の締結等に係る施策であり、国会審議の状況や諸外国との関係等で、明確な予定を示すことが困難。

結論

政府として実施すべき施策については、ほぼ全て年度内(又は予定内)に実施できる目途が立っており、「セキュア・ジャパン2008」は概ね順調に進捗。

別紙3

情報セキュリティ対策に関する 平成 21 年度予算概算要求について

平成 20 年 12 月 10 日
内閣官房情報セキュリティセンター

平成 21 年度予算概算要求のうち、情報セキュリティ関連のものは次のとおり。

1 要求額

○ 平成 21 年度予算概算要求額 29,821 百万円

○ 予算額推移（平成 21 年度は概算要求額）

| | 平成 17 年度 | 平成 18 年度 | 平成 19 年度 | 平成 20 年度 | 平成 21 年度 |
|------|----------|----------|----------|----------|----------|
| 当初予算 | 288 億円 | 319 億円 | 300 億円 | 299 億円 | 298 億円 |
| 補正予算 | — | — | — | — | — |
| 合 計 | 288 億円 | 319 億円 | 300 億円 | 299 億円 | 298 億円 |

（注）通常のシステム管理一般の中でセキュリティ対策を行っているなど、
情報セキュリティ関連予算のみを取り出すことが困難なものは除く。



目的

行政情報システムにおける情報セキュリティ対策を考慮したライフサイクル管理の強化の実現に向け、経験・知見を有する有識者やベンダーを交えた検討会を立ち上げ、年度末に一次報告書を取りまとめる。

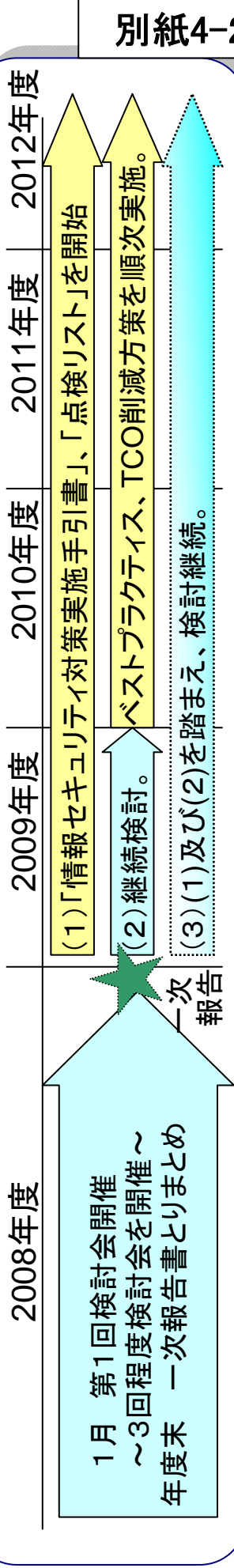
検討会メンバー

- (座長)
 - ・大学教授等
- (委員)
 - ・大手ベンダー(3名以上)
 - ・システム関連事業者関連団体内の有識者(2名以上)
 - ・府省庁CIO補佐官(2名以上)
 - (オブザーバ)
 - ・情報セキュリティ補佐官 等
 - ・関係各府省庁

検討内容

- (1) 政府機関統一基準に基づく情報システムのセキュリティ確保の進め方の検討 (情報セキュリティ対策実施手引書、点検リスト)
政府機関統一基準に基づきつつ、調達者と調達先ベンダーがどう協業できるのかについて検討を行う。
- (2) セキュリティを考慮した情報システム開発手法及び保証のあり方の検討
ベストプラクティスのとりまとめ、TCO(Total Cost of Ownership)低減のための調査等を行う。
- (3) 政府機関における情報システム関連基準のあり方の検討
上記の検討結果を踏まえ、政府調達へのプロセス組込みについて検討を行う。

スケジュール(案)



分野横断的演習の取組みについて



分野横断的演習は、IT障害発生時における重要インフラサービスにおける重要インフラサービス、セプター、重要インフラ事業者等に向けた課題抽出を目的として、重要インフラ所管省庁、セプター、重要インフラ事業者等の協力を得て、2006年度から毎年度実施。

<2006年度>
**官民連携の
 仕組みづくり**

研究的演習
 演習実施の概念、演習課題の設定、演習手法の理解等を主眼として実施。

机上演習
 脅威として災害を演習課題の設定し、会議形式の演習を実施。

重要インフラ10分野が一堂に会し、初めての分野横断的演習を実施。



机上演習状況

<2007年度>
**官民連携体制の
 機能向上**

機能演習
 脅威としてDDoS攻撃を設定し、チーム毎に個室に分かれ、メールのみを利用した演習を実施。

機能演習
 NISC、所管省庁、セプター、重要インフラ事業者等から成る情報共有の仕組みが想定通り機能することを確認。




機能演習状況

<2008年度>
**官民連携体制の
 実効性向上**

機能演習
 参加者にIT障害の発生原因を知らせないなどより現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧や事業継続等を行うべく機能演習を実施。

機能演習
 官民の情報共有、連絡連携の仕組みが、緊急時における重要インフラ事業者等のサービスの維持・早期復旧や事業継続等にとってより有益となるよう課題を抽出。



機能演習状況

別紙4-3-1

2008年度分野横断的演習の実施概要報告



松本内閣官房副長官の御出席を得て開催した2008年度分野横断的演習の実施概要は、以下の通りです。

1. 2008年度演習の目的

IT障害発生時における重要インフラのサービスの維持・早期復旧や事業継続等に向けた課題抽出

2. 検証対象

重要インフラ事業者等、セプター、関係機関、重要インフラ所管省庁及び内閣官房情報セキュリティセンターから成る情報共有の仕組み全体を対象

3. 検証課題

- (1) 緊急時の官民の情報共有、連絡・連携の仕組みの実効性確保
- (2) 平時における官民・事業者間の連絡・連携の状況
- (3) 緊急時の各主体におけるIT障害への対応要領・手順の確認
- (4) 相互依存性解析の結果
- (5) 実施細目^(注)の見直しに向けた課題の抽出

注)「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報連携に関する実施細目

4. 実施日時・場所

2008年12月1日(月) 12:30~18:30
(株)三菱総合研究所 2階セミナー室、会議室



松本内閣官房副長官挨拶



全体説明状況

5. 参加者

プレイヤ、事務局等合わせて136名が参加
主な参加機関は以下の通り

(政府)

内閣官房情報セキュリティセンター、重要インフラ所管省庁

(重要インフラ分野：10分野)

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

(セプター：10分野14セプター)

通信、放送、銀行、生保、損保、証券、航空、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流

(関係機関)

(有識者)

大林厚臣 慶應義塾大学教授(検討会座長) 他



演習状況

6. 実施方法

- (1) 各分野あるいは事業者毎に小部屋に分散し、メール、電話、Webページを用いて情報交換を実施
- (2) 詳細シナリオは、事務局のみが把握し、プレイヤにはIT障害の原因を開示せず、状況付与のみを行うという現実に近い状況で実施
- (3) 演習終了後、意見交換会を実施

7. 今後の展開

演習時のメールや電話による情報交換の内容、アンケート結果等を分析し、実施内容および検証課題の検討結果を取りまとめた後、情報セキュリティ政策会議に報告する予定。

演習で得られた成果は、官民の情報共有体制の強化策の検討に役立てるとともに、各事業者において情報セキュリティ対策の向上に向けた取り組みに活用されることが期待される。

関係省庁からの 推薦募集

- ◆ 9月下旬から10月下旬にかけて関係省庁からの推薦を募集

被表彰者の選考 及び決定

- ◆ 情報セキュリティ啓発推進委員会において被表彰者を選考
- ◆ 政策会議議長(内閣官房長官)に上申

政策会議議長に よる表彰

- ◆ 2月開催予定の情報セキュリティ政策会議に併せ、「情報セキュリティの日」功労者表彰を実施

基本的には昨年度の手続きを継承

【選考過程の透明性確保】

- 民間有識者・学識経験者等からなる「**情報セキュリティ啓発推進委員会**」において被表彰者を選考し、政策会議議長に上申。
- 被表彰者は、2月開催予定の情報セキュリティ政策会議で発表。

【普及啓発に資する活動の実施】

- **情報セキュリティの普及啓発に資する行事を政策会議として積極的に後援。**