報道発表

平成 20 年4月 22 日
内閣官房情報セキュリティセンター（NISC）

第17回情報セキュリティ政策会議の開催について

－「セキュア・ジャパン 2008」パブコメ案の決定等－

本日4月 22 日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第17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、「セキュア・ジャパン 2008（SJ2008）」のパブリックコメント案及び「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」が決定された。

1. セキュア・ジャパン 2008 パブリックコメント案の決定

第１次情報セキュリティ基本計画に基づき、各府省庁が実施する施策の年度計画であるセキュア・ジャパンの３年目の計画としてセキュア・ジャパン 2008(案)を作成。同案では「セキュア・ジャパン 2007」に基づいた取組みへの評価と分析を踏まえ、第１次情報セキュリティ基本計画（以下、「基本計画」という。）の実現に向け「情報セキュリティ基盤の強化に向けた集中的な取組み」をまとめている。本日、同案についてパブリックコメントに付すことが決定（平成 20 年4月 22 日～5月 22 日の間）。

基本計画の最終年度として、同計画の理念を実現するため、多くのコメントが寄せられることを期待。

セキュア・ジャパン 2008（案）のポイントは以下のとおり。

- セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図る。
- 2008 年度に実施する具体的行動計画と、2009 年度の重点施策の方向性を示す。
- 総施策数 179 施策（内新規 19 施策、継続 138 施策、2009 年度の重点 22 施策）（別紙１参照）

2. 2007 年度の情報セキュリティ政策の評価等の報告

2007 年度の情報セキュリティ政策の評価等を実施し報告。評価のポイントについては、以下のとおり。

○ 総評

- 「官民における情報セキュリティ対策の底上げ」が進んだ。
- 情報セキュリティに関するリスクは依然として軽減しておらず、情報セキュリティ政策の社会的効果は十分な判断がつかない状況。
- 対策水準の更なる向上のため体制の強化、効率的な対策の推進が引き続き必要。

○ セキュア・ジャパン 2007 の実施状況について

約 9 割の施策が当初の予定どおりに実施。残りの約 1 割については、「go.jp」ドメインへの移行等全府省庁が実施することとなっているものの、一部府省庁において実施が完了しなかった施策、いわゆるウイルス罪の新設に係る刑法の改正等政府としては施策を推進しているものの、政府機関以外の理由により完了していないもの等がある。

○ 重要インフラ分野について

2007 年度中に CEPTOAR（※1）が新規追加 3 分野（医療、水道及び物流）において整備を完了したことにより、全 10 分野において CEPTOAR が整備されるなど、情報共有、連絡・連携を進めるための枠組み・体制は徐々に構築されつつある。

※1 CEPTOAR（情報共有・分析機能）：Capability for Engineering of Protection, Technical Operation, Analysis, and Response

（別紙2参照）

3. 政府機関における情報セキュリティ対策

（1） 政府機関の対策実施状況報告（2007 年度）について

○ 基本計画において「2009 年度初めには、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を目指す」と目標を設定。

○ 上記目標を達成するため、政府機関全体としての情報セキュリティ対策を推進する観点から、各府省庁の対策の実施状況を NISC において把握。

○ 2007 年度は出来る限り多くの対象に係る対策実施状況の報告を求め、約 30 万人（前年度比約 30 倍）分の報告があり、全府省庁の平均把握率（※2）は93．4％であった。

なお、次回（2008 年度）は政府機関統一基準の対象となるすべての職員（約 50 万人）を報告の対象とする予定。

○ 全府省庁の平均実施率(※3)は93．4%であった。
○ 全府省庁の平均到達率(※4)は以下のとおり。
・ 100%実施した割合:64．1%
・ 95%以上実施した割合:75．8%
・ 90%以上実施した割合:81．7%
○ 報告を分析した結果、全府省庁の平均実施率が低く、全府省庁共通の課題として以下の 3 つの項目が判明。今後、3 つの課題を中心に、平均実施率が低い項目について対策を実施していく予定。
・ 情報セキュリティ対策の教育(全府省庁平均実施率84．2%)
・ 格付け・取扱い制限に係る措置(全府省庁平均実施率89．7%)
・ 情報システムの台帳整備(全府省庁平均実施率77．9%)

(別紙3参照)

※2 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
※3 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
※4 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

(2) 政府機関における安全な暗号利用の促進(政策会議決定)

○ インターネット上でやりとりされる情報の盗聴、改ざん、なりすまし等を防ぐため、様々な暗号技術が利用されている。
○ しかし、コンピュータの性能の向上等によりそれらの暗号の安全性が相対的に低下することは不可避。
○ 現在、電子政府システムでは、電子署名等のために SHA-1(※5)及び RSA1024(※6)と呼ばれる暗号方式を広く使用しているが、上記理由により、将来的に安全性が低下するため、政府統一的な移行指針の策定が不可欠であり、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」を決定。
(なお、同移行指針は平成 20 年 2 月 4 日～3 月 7 日の間、パブリックコメントを実施し、14 件のコメントが寄せられたものの、2008 年度における検討事項に対するコメント等の理由により、文章の修正には至らなかった。)
○ 同移行指針の概要は次のとおり。
① 技術的な対応
・ 新たな暗号方式として、SHA-256(※7)及び RSA2048(※8)を採用。
・ 移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。
② 制度的な対応
・ 各府省庁において、システムの移行時期を踏まえ、必要な対応の取りま

とめ、移行手順書の整備を実施。

③ スケジュール

- 2008 年度中に新たな暗号方式へ切り替える時期を検討。
- 2010 年度から 2013 年度までの間に、各府省庁における情報システムの対応を完了。
- 総務省及び経済産業省は暗号の安全性に係る状況を監視し、内閣官房は必要な情報を速やかに各府省庁に提供。

(別紙4参照)

(参考) 米国では期限を決めて対応する方法を採用し、2010 年末以降、政府機関において、SHA-1 の新規使用を停止する方針。

※5 ハッシュ関数 SHA の一つで、与えられたデータから 160 ビットの固定長の値を生成する。

※6 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 1024 ビットとしたもの。

※7 ハッシュ関数 SHA の一つで、与えられたデータから 256 ビットの固定長の値を生成する。

※8 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 2048 ビットとしたもの。

4. 重要インフラにおける情報セキュリティ対策に係る報告

(1) 「重要インフラ連絡協議会(CEPTOAR-Council)」(仮称)創設の検討について

CEPTOAR 代表者等から構成される「検討の場」において基本的な考え方をとりまとめ、「重要インフラ連絡協議会(CEPTOAR-Council)(仮称)創設準備会」を本年 6 月を目処に設置することとした。今後、創設準備会での議論を踏まえつつ本年度中の「重要インフラ連絡協議会(CEPTOAR-Council)」(仮称)創設を目指す。

(別紙5参照)

(2) 分野横断的演習について

有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会等を通じ、シナリオ等の議論を経て、分野横断的な機能演習を実施。

日時:2008 年 2 月 6 日(水) 13:00～18:30

目的:大規模なサイバー攻撃発生時における情報提供及び情報連絡機能の検証

参加者:政府(NISC 及び重要インフラ所管省庁)、重要インフラ事業者(10 分野)、CEPTOAR(7 分野11CEPTOAR)及び関係機関等から約 120 名

(別紙6参照)

(3) 安全基準等の浸透状況等に関する調査について

2006 年度に策定・見直しを行った安全基準等の浸透状況等の調査を実施した結

果、調査対象範囲における概ね全ての事業者等に認知されている（認知率：97．9%）ものの、内規の見直しを予定していない事業者も 3 割以上存在（31．5%）することが確認された。今後、安全基準等に基づく内規の見直しの推進等につとめていく予定。

具体的な調査内容は以下のとおり。

- 分野の安全基準について認知されているか
- 情報セキュリティの確保に関する内規等を制定しているか
- 分野の安全基準に基づき、自社の内規等の見直しを実施しているか　等

（別紙7参照）

（4） 指針の見直しについて

○ 「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」は、各重要インフラ分野における安全基準等の策定・改定を支援することを目的として 2006 年 2 月に策定。

○ 「1 年ごと及び必要に応じて適時に、本指針の見直しを推進する」こととしており、2007 年度も指針の見直しを実施。

○ 4つのアプローチで分析・検証を行い指針の見直しを行った結果、2006 年 9 月の安全基準等の策定、見直しから 1 年経過した時点で、内規見直しを終えることができた事業者等は半数程度に留まっていると推定されること等から、今回は指針の改定は行わず、指針の周知と実態把握に努めることが適当と認められた。ただし、独自に見直しを実施している分野もあることから、独自の見直しを行う場合等に活用してもらうため指針の見直しの要点を参考資料として周知。

4 つのアプローチは以下のとおり。

- 定常的な IT 障害の発生状況の分析
- 「相互依存性解析」の成果
- 関連文書の検証
- 社会的条件（環境）の変化の検証

（別紙8参照）

（5） 情報共有・分析機能（CEPTOAR）の整備について

○ 行動計画で掲げられた全 10 分野で 14 の CEPTOAR の整備が完了。

○ 昨年 4 月より運用開始している既存 7 分野に加え、新規 3 分野（医療、水道及び物流）は 2008 年 4 月より運用を開始。

○ 既存分野は、2007 年度に情報共有訓練及び官民連携による分野横断的演習に参加。

（別紙9参照）

(6) 相互依存性解析について

○ 有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる相互依存性解析検討会を設置し、検討会等で、「相互依存性解析における視点(考え方のポイント)」を整理しつつ、「動的相互依存性解析」を実施。

○ 解析の結果、「情報通信分野(通信)は他の7分野」と、「電力分野は他の 10 分野」と、「水道分野は他の 8 分野」と相互依存性があることが明確になるとともに、電力・水道のサービスの停止・低下において時間経過に伴う状況の変化等によりIT障害が発生する場合があることが判明。

○ 今後の課題としては、「「周辺システム」から「重要システム」へのデータの送受信に係る分野間の関係性」について、IT 障害につながる可能性等を検討する必要があるのではないかと考えられる。

(別紙10参照)

【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#seisaku17)

□ 「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)

「第1次情報セキュリティ基本計画」の概要と「セキュア・ジャパン2008」（案）の位置づけ

NISC

「第1次情報セキュリティ基本計画」（2006年2月2日　情報セキュリティ政策会議）

2006～2008年度の3ヵ年計画。全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築を目指す。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
3ヵ年の目標	すべての政府機関が「政府機関統一基準」が求める水準に	IT障害を限りなくゼロに	対策の実施状況を世界トップクラスの水準に	「IT利用に不安を感じる」個人を限りなくゼロに
各実施領域の重要政策	◆ 政府機関統一基準に基づく各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能の整備 ◆ 連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等

横断的な重要政策：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の育成確保／国際連携・協調の推進／犯罪の取締り、権利利益の保護救済

次期基本計画

2005年度 → 2006年度 → 2007年度 → 2008年度 → 2009年度

「セキュア・ジャパン2006」	評価2006	「セキュア・ジャパン2007」	評価2007	「セキュア・ジャパン2008」	評価2008	SJ 2009
① 2006年度の実施計画（133施策） ～「官民におけるセキュリティ対策の体制の構築」 ② 2007年度の重点施策の方向性（26施策） ～「官民におけるセキュリティ対策の底上げ」		① 2007年度の実施計画（159施策） ～「官民における情報セキュリティ対策の底上げ」 ② 2008年度の重点施策の方向性（24施策） ～「情報セキュリティ基盤の強化に向けた集中的な取組み」		① 2008年度の実施計画（157施策） ～「情報セキュリティ基盤の強化に向けた集中的な取組み」 ② 2009年度の重点施策の方向性（22施策） ～「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」		

「セキュア・ジャパン」：基本計画の遂行を確実にするため、毎年の政府の重点施策をまとめた年度計画

別紙1－1

7

「セキュア・ジャパン2008」（案）のポイント

- 「セキュア・ジャパン2007」に基づいた取組みへの評価と分析を踏まえ、「第１次情報セキュリティ基本計画」の実現に向けた3年目（最終年度）の取組みをまとめる。
- セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図る。
- 2008年度に実施する具体的行動計画と、2009年度の重点施策の方向性を示す。

＜基本計画を実現するための取組みの底上げ＞

－「第1次情報セキュリティ基本計画」（2006年度～2008年度）の実現に向け、取組みの底上げを含む三年目（最終年度）の取組み

＜2007年度末の状況認識・評価を踏まえた取組みの方向性＞

➢現行の対策推進体制や対策枠組み、技術水準に照らし限界点に達していると考えられる諸点について、ブレークスルーをもたらす方法を検討

➢中長期にわたり取り組むべき方策、加速化が必要な方策、迅速かつ集中的な取組みが必要な方策を強力に推進

➢これまでに整備されてきたツール・体制といった取組基盤を活用し、情報セキュリティ政策の社会的効果（アウトカム）を発現

重点

取組みの方向性

＜「セキュア・ジャパン2008」のポイント＞

電子政府等の情報セキュリティ強化のための総合的な取組み

【主な具体策】
- 「政府機関統一基準」に基づくPDCAサイクルの定着・本格的な評価の推進及び結果の公表
- 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（SBD）ための方策の強化
- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の本格運用・能力強化

中期的取組みを必要とする課題への集中的な取組み

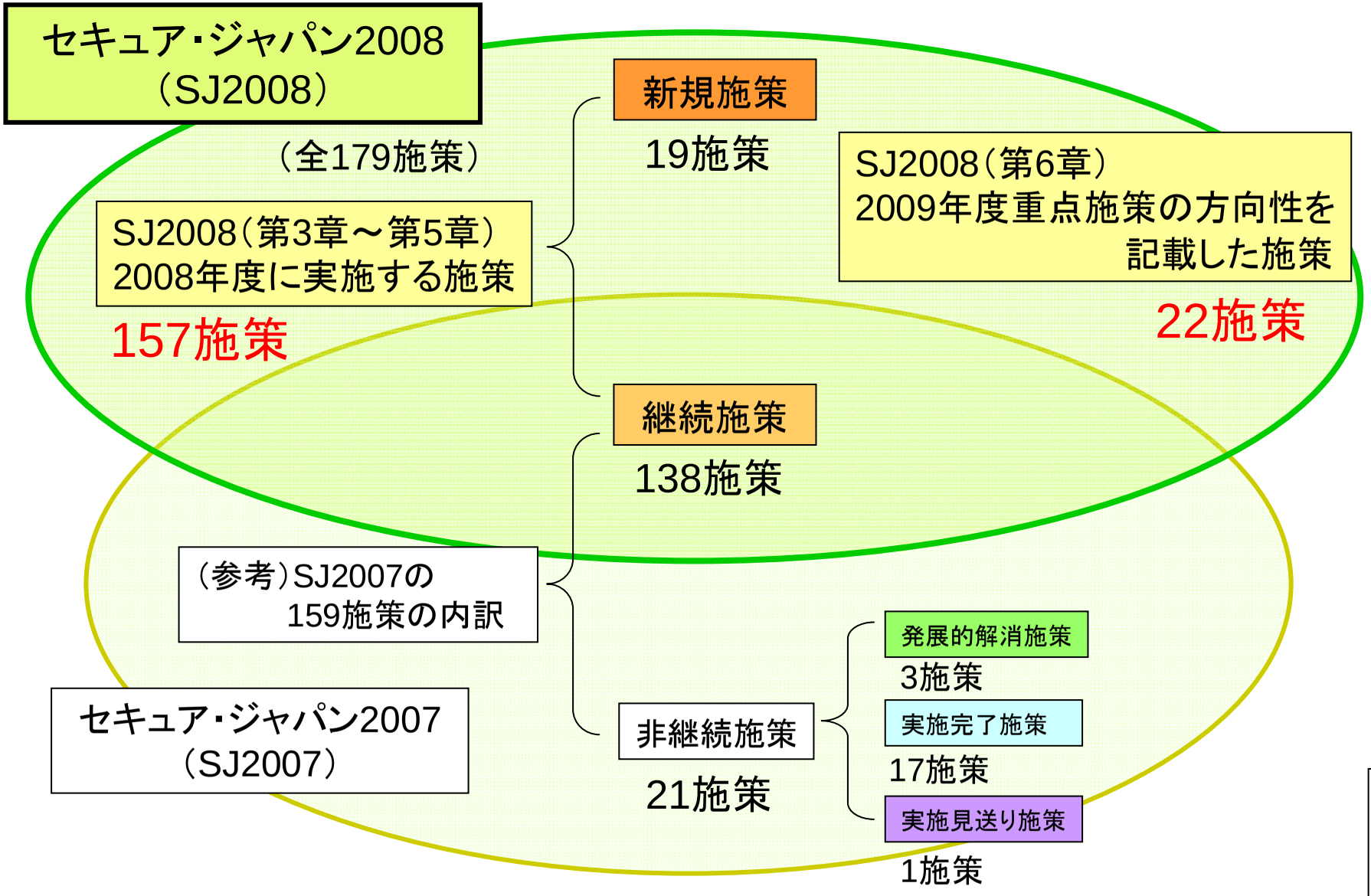
【主な具体策】
- 長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」のテーマの検討
- アジア地域における情報セキュリティ政策会合の創設
- 分野横断的な情報共有促進のための「重要インフラ連絡協議会(仮称)」創設の促進

持続的な対策の推進体制の構築に向けた基盤整備

【主な具体策】 *→ 2009年度の重点施策の方向性*
- 情報セキュリティ人材の重点確保
- 各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討

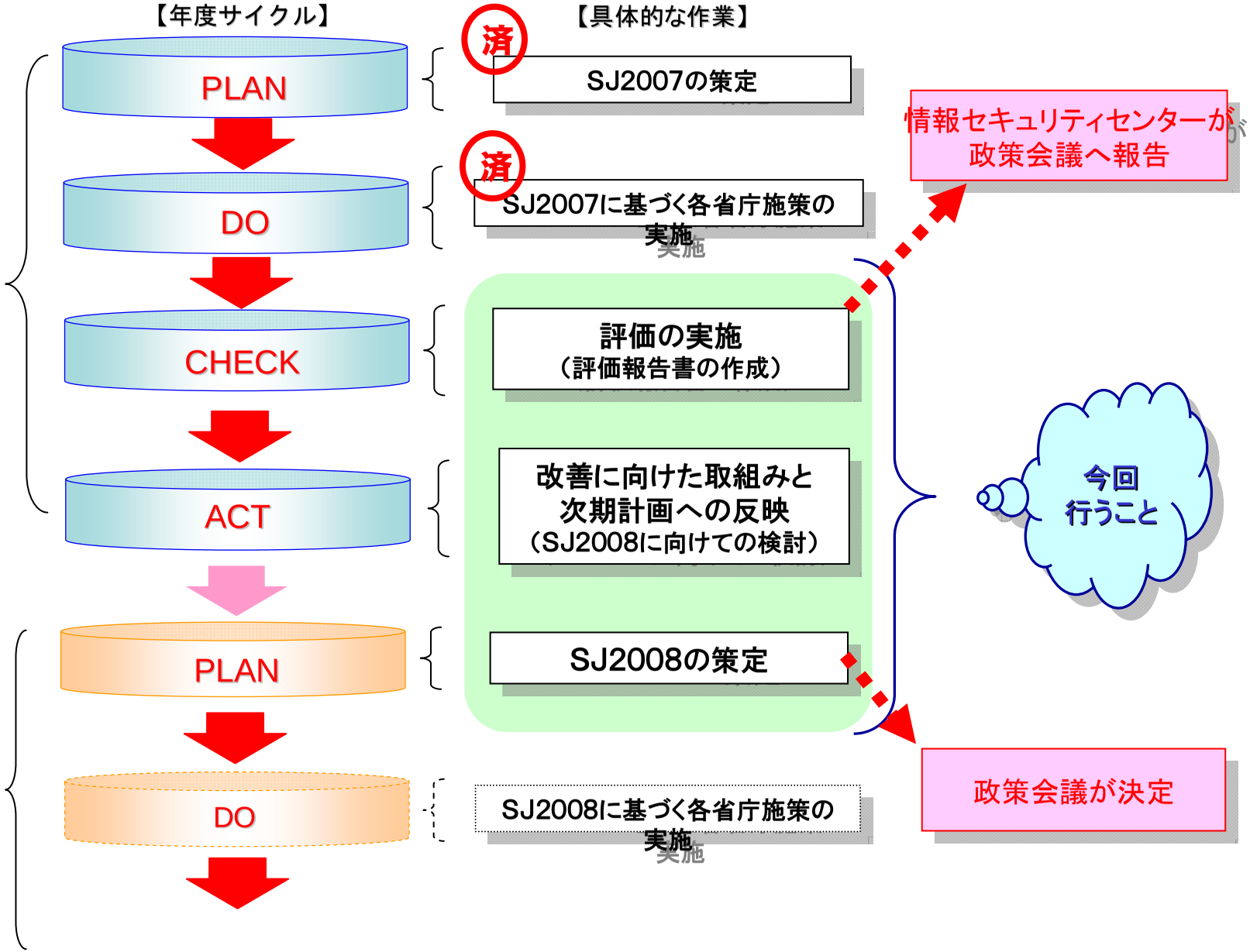
別紙１－２

「セキュア・ジャパン2008」（案）に記載された施策の内訳



別紙1－3

情報セキュリティ政策のPDCAサイクルと2007年度の評価等、SJ2008の関係



別紙2－1

2007年度の評価等における評価・分析のポイント①
（情報セキュリティ政策全体）

○ 情報セキュリティ政策全体（総評）

・官民の情報セキュリティ対策のための体制維持、対策推進の安定化へ向けた取組みが懸命に進められた。
・各対策実施領域の取組み状況に一定の進展があり、「官民における情報セキュリティ対策の底上げ」も進んだものと考えられる。
・情報セキュリティに関するリスクの大幅な軽減はみられず、情報セキュリティ政策の社会的効果は十分な判断がつかない状況。
・現行技術水準の限界もあると考えられ、対策水準の向上には体制の強化、効率的な対策の推進が引き続き求められる。

○2007年度の取組み及び取組みを受けた現状の評価等

- SJ2007に盛り込まれた取組み
  第一次基本計画及びSJ2007の目標に掲げられる「4つの基本方針」に対する取組み

（1）官民各主体の共通認識の形成
⇒官民各主体の共通認識の強化
・政府機関の持続的改善構造による対策推進意識の高まり
・重要インフラ10分野CEPTOAR整備完了、安全基準等の見直し、官民連携による分野横断的演習、相互依存性解析、情報共有体制の強化へ向けた継続的な取組み等を通じた対策推進意識の高まり
・教育拠点、教育ツールの整備、教育事業者団体の業界横断的な連携体制の構築等、官民における人材育成に係る意識の浸透

（2）先進的技術の追求
⇒先進的技術の追求の継続
・政府全体として情報セキュリティ分野へ重点投資を進める環境の整備
・ボットを使ったサイバー攻撃等の課題を解決する技術等、課題解決型の技術開発の推進

（3）公的対応能力の強化
⇒政府機関対応体制の確立の推進
政府機関に対するサイバー攻撃等に関する横断的な情報収集・分析・情報共有を行うための体制（GSOC※）整備開始
※Government Security Operation Coordination Team

（4）連携・協調の推進
⇒連携協調へ向けた活動の開始、NISCを結節点とした連携（各主体間の横断的連携はこれから）
国際協調・貢献に関する基本方針の策定を受けた本格的な活動の開始
重要インフラ10分野CEPTOARの連携、情報共有体制CEPTOAR－Council（仮称）の創設へ向けた検討等

- SJ2007の取組みの状況と成果
  2007年度の一年間の取組みの状況と成果としては、
  1）各主体における情報セキュリティ意識の維持・強化
  2）対策実施領域ごとの具体的取組みの着実な推進
  3）横断的な情報セキュリティ基盤分野における具体的取組みの着実な推進
  4）情報セキュリティ推進体制の維持・強化と持続的改善構造に基づく政策の推進　、であったと言える。

2007年度の評価等における評価・分析のポイント⑧（1）
（「セキュア・ジャパン2007」に盛り込まれた施策の実施状況）

○施策の実施状況

A	：予定どおり施策を推進することができた施策	・・144施策（90．6%）
B＋	：年度内には完了していないが、着実に取組みを進めており、数ヶ月以内には完了する施策	・・・　1施策（0．6%）
B	：予定どおり推進することができなかったが、今後も取組みを続けることにより最終的には施策を推進することができる施策	・・12施策（7．5%）
C	：予定どおり施策を推進することはできず、今後の見通しも立たない施策	・・・　1施策（0．6%）
―	：予定どおり施策を推進することができなかったが、その理由が政府機関の事情によるものではない施策	・・・　1施策（0．6%）

「A」とされた施策について

144施策（90．6%）について予定どおり施策を推進。内5施策については施策は推進するも、体制・人員に関して課題があるため、継続的な推進に当たって解決が必要であることが、作業の進捗や各省へのヒヤリング等から明らかになった。これら5施策については、政府機関の対策実施に関する取組みであり、政府機関の情報セキュリティ対策推進のための、体制や人員の不足が課題であることがうかがえる。

施策は推進されたが、体制・人員に関して課題があり、継続的な推進に当たって解決が必要な5施策

- ・各政府機関でのPDCAサイクルの定着
- ・政府全体でのPDCAサイクルの定着
- ・対策実施状況に関する評価等
- ・情報セキュリティマネジメントに関する評価等
- ・情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施

「B＋」とされた施策について

各府省庁で「IT人材育成・確保実行計画」を作成をしており、数ヶ月以内には全府省庁で完了する見込み。

2007年度の評価等における評価・分析のポイント⑧（2）
（「セキュア・ジャパン2007」に盛り込まれた施策の実施状況）

「B」とされた施策について

情報資産台帳の整備や「go.jp」ドメインへの移行など全府省庁が実施すべき施策であったものの、一部府省庁で実施が完了しなかったものが6施策、その他、刑事共助条約の締結等、施策を推進したものの年度内に完了できなかったものが6施策となっている。

全府省庁が実施すべき6施策
- ・各府省庁の情報システムの一元的把握
- ・政府機関のドメイン名であることが保証されるドメイン名の利用の促進
- ・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等の活用
- ・情報セキュリティ監査制度の活用
- ・安全性・信頼性の高いIT製品等の利用推進
- ・入札条件等の見直し

その他の6施策
- ・電子政府認証ガイドライン利用の推進
- ・「情報システムの信頼性向上に関するガイドライン」の活用・普及
- ・政府機関における安全な暗号利用の推進体制等の検討
- ・地方公共団体における情報セキュリティ対策の手引きの作成
- ・客観的な高度IT人材評価メカニズムの構築
- ・中央当局制度 を活用した国際捜査共助の迅速化

「C」とされた施策について

本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査について、既存OS環境でのセキュリティレベルの向上や現在開発中の高セキュリティ機能を実現する次世代OS環境の開発（セキュアVM）の成果をかんがみると、施策実施は不要と判断した。

「－」とされた施策について

刑法等の改正（「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」）で、政府機関の事情以外の理由により完了しなかったものが1施策となっている。

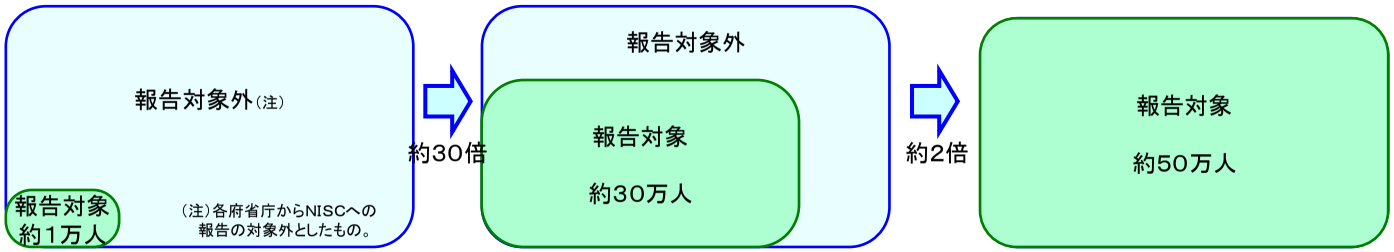
政府機関の対策実施状況報告（2007年度）の概要

1　対策実施状況報告の実施目的

政府機関の情報セキュリティ対策は、「2009年度初めには、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を目指す」（第1次情報セキュリティ基本計画）ことが目標とされている。
この**目標を達成するため、政府機関全体としての情報セキュリティ対策を推進する観点から、各府省庁の対策の実施状況をNISCにおいて把握**。

2　2007年度の報告の範囲

2007年度は、目標達成のための中間地点と位置づけ、**2008年度に全ての対象を報告することを明確化**するとともに、2007年度は**できるかぎり多くの対象に係る対策実施状況の報告を求めた（前年度比約30倍）。**
（2007年度の報告対象については組織の規模や繁忙期等に配慮し、各府省庁から事前に提示された対象範囲とした。）



3　報告の概要及び2008年度に向けた課題

報告の概要
- 政府機関全体で約30万人分の対策実施状況について報告があった。これを分析した結果、各府省庁が報告対象とした者のうち状況が把握できた者の割合を示す把握率は全府省庁平均で約93%、実施率は全府省庁平均で約93%、到達率については、100%の職員が実施した遵守事項の割合では約64%、90%の職員が実施した遵守事項の割合では約82%であった。
- 一定の成果が見られるが、なお不十分な点があり、第一次基本計画の最終年度に向けて、取り組むべき課題が依然として残っている。

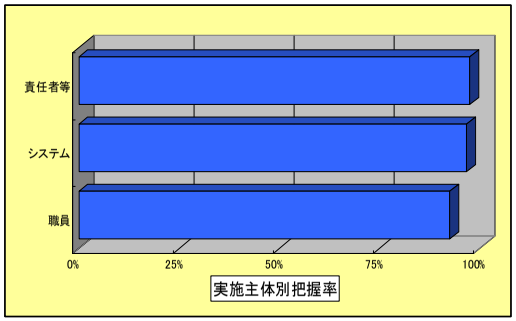
2008年度に向けた課題
- 第1次基本計画の目標を達成するためには、政府全体として「情報セキュリティ対策の教育」、「格付け・取扱い制限に係る措置」、「情報システムの台帳整備」等の課題が残っている。これらのほとんどについては、前回（2006年度）からの課題でもあり、改善に向けた取組みを加速する必要がある。
- 一方、前回（2006年度）に課題とされた「安全区域内における職員識別の徹底」等については、各府省庁とも改善がみられている。
- 今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、NISCにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

政府機関の対策実施状況報告(2007年度)の評価結果【実施主体ベース】

1 把握率

全府省庁の平均把握率

93.4%



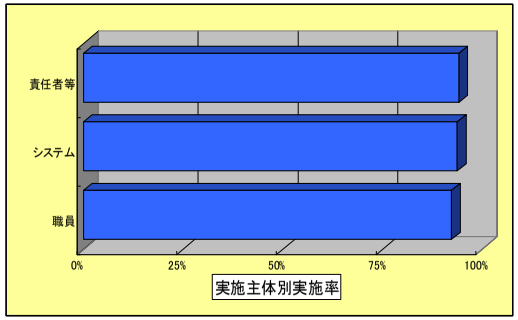
① 昨年度比で30倍と大幅に報告対象が増えた中、平均把握率は約93%となっており、多くの省庁では対策実施状況が把握できている結果であった。

② 来年度は全対象であること、今年度は対象を各省庁が事前に設定した範囲内であったこと、特に職員の把握率が低いことから、来年度に向け、把握率の改善手段をあらかじめ検討する必要がある。

2 実施率

全府省庁の平均実施率

93.4%



③ 平均実施率は約93%となっており、責任者等が高く、システム担当、職員の順に低い結果であった。

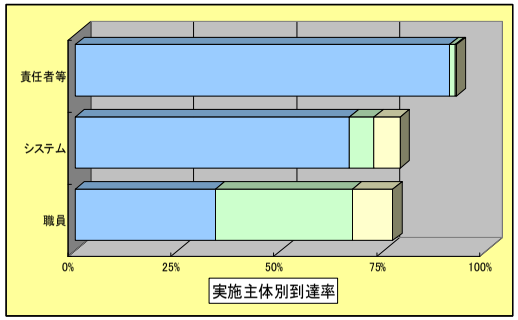
④ 情報セキュリティ対策について組織的な責務を果たすべき責任者等の実施率が100%に満たないことは問題であり、職員についても実施率が低い状態の改善が必要である。

3 到達率

全府省庁の平均到達率

100%実施した割合　:64.1%
95%以上実施した割合:75.8%
90%以上実施した割合:81.7%

全対象者が対策を実施した遵守事項の割合
95%以上の対象者が対策を実施した遵守事項の割合
90%以上の対象者が対策を実施した遵守事項の割合



⑤ 到達率でみると、責任者等に比べシステム担当や職員が低くなる傾向が顕著に現れた。

⑥ これは職員については、日々の業務において日常的に実施しなければならない遵守事項が多いことから、責任者等やシステム担当と比して100%達成に困難な面があるためだが、万一の事故防止のためには日々の取り組みが重要であり、到達率向上の努力が必要である。

一方、責任者等やシステム担当については、日常的なものは少なく、早急に100%を達成する必要がある。

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

責任者等: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、情報セキュリティ監査実施者、統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者、許可権減車及び情報セキュリティ関係規程を整備した者

システム: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責任者を含む複数の者が主体となっているものを含む)、情報システムセキュリティ管理者及び権限管理を行う者

政府機関の対策実施状況報告(2007年度)の評価結果【遵守事項ベース】

政府機関全体の実施状況について特筆すべき遵守事項は次のとおり。

1 情報セキュリティ対策の教育

[統一基準2．2．1]

全府省庁の平均実施率

84．2%

遵守事項	実施率
(1)教育の実施	84．1%
(2)教育の受講	84．8%

遵守事項別実施率

①毎年度1回以上実施すべき教育の計画策定や着任・異動後3ヶ月以内に実施すべき教育の計画策定が不十分。
計画がなされていても受講状況の把握や未受講者への受講指導の徹底が不十分。

②職員による教育受講が不十分である。

2 格付け・取扱い制限に係る措置

[統一基準3．2．1～3．2．6]

全府省庁の平均実施率

89．7%

遵守事項	実施率
(1)情報の作成と入手	87．3%
(2)情報の利用	96．6%
(3)情報の保存	87．7%
(4)情報の移送	86．3%
(5)情報の提供	90．6%
(6)情報の消去	96．5%

遵守事項別実施率

③情報の作成と入手時において、情報の格付けの実施や格付けの明示等の実施が不十分である。

④ 情報の移送、情報の提供時において、管理者に対して行うべき許可申請、届出が不十分である。

3 情報システムの台帳整備

[統一基準4．3．1(5)]

全府省庁の平均実施率

77．9%

⑤ 情報システムが扱う情報や当該情報の格付けを含む事項を記載した情報システムの台帳整備が不十分。

4 安全区域内における職員識別の徹底

[統一基準5．1．1(4)]

全府省庁の平均実施率

93．2%

⑥ 安全区域内における職員識別の徹底については、昨年度は課題とされたが、昨年に比べ、安全区域内の職員識別の徹底について改善がみられる。

○ 今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、NISCにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

別紙3－3

「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」の決定について

NISC

経　　緯

第16回情報セキュリティ政策会議（H20.2.4）

○　政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針（案）について審議を実施、パブリックコメントに付すことを決定。

○　その際、構成員から「移行した暗号自体の安全性の監視も重要である」等の意見もあり、パブリックコメントとともに検討することとした。

■　実　施　期　間　：　平成20年２月４日（月）　～　平成20年３月７日（金）

■　パブリックコメント総数　：　14件【内訳　企業・団体・大学　：　14件、　個人　：　0件】

■　施策実施にあたっての配慮・要望として、民間との協調や2008年度の具体的検討に当たっての要望等について意見の提出あり。

パブリックコメント等の結果

・　2008年度における検討事項に対するコメント等の理由により、文章の修正に至らず。

・　移行した暗号自体の安全性の監視について、指針に追加。

【修正個所：3(3)カ】

（新）　総務省及び経済産業省は、**現在使用しているSHA-1及びRSA1024並びに新たに使用するSHA-256及びRSA2048**の安全性について監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

（旧）　総務省及び経済産業省は、SHA-1及びRSA1024の安全性について監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

移行指針の概要

①技術的な対応【政府認証基盤とそれに依存する各府省庁の情報システム】

○　相互運用性確保のため、新旧暗号方式の双方に対応し、適切な時期に暗号方式を切り替える運用を可能に。

○　新たな暗号方式として、SHA-256及びRSA2048を採用。

○　移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。

②制度的な対応

○　各府省庁において、システムの移行時期を踏まえ必要な対応の取りまとめ、移行手順書の整備等を実施。

③スケジュール

○　【内閣官房、総務省、法務省、経済産業省等】新たな暗号方式へ切り替える時期等を2008年度中に検討。

○　【内閣官房、総務省等】相互接続の技術要件、緊急避難対応等について2008年度中に検討。

○　【各府省庁】2010年から2013年までの間に、各情報システムの対応を完了。

○　【内閣官房、総務省、経済産業省】安全性の状況を監視し、必要な情報を速やかに各府省庁に提供。

17

別紙4

◆CEPTOAR-Council創設に向けた検討の場のとりまとめ資料

◆「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設についての基本的な考え方

- 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の目的や活動等についての基本的な考え方を明らかにするとともに、創設に向けた方向性を示すことにより、「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の円滑な創設を目指すために、CEPTOAR-Council創設に向けた検討の場参加者の意見を内閣官房情報セキュリティセンターがとりまとめたもの。

◆「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設に向けた検討の場」における2007年度活動の概要

- 創設準備会での検討に活用されることを想定し、活動の概要をまとめたもの。

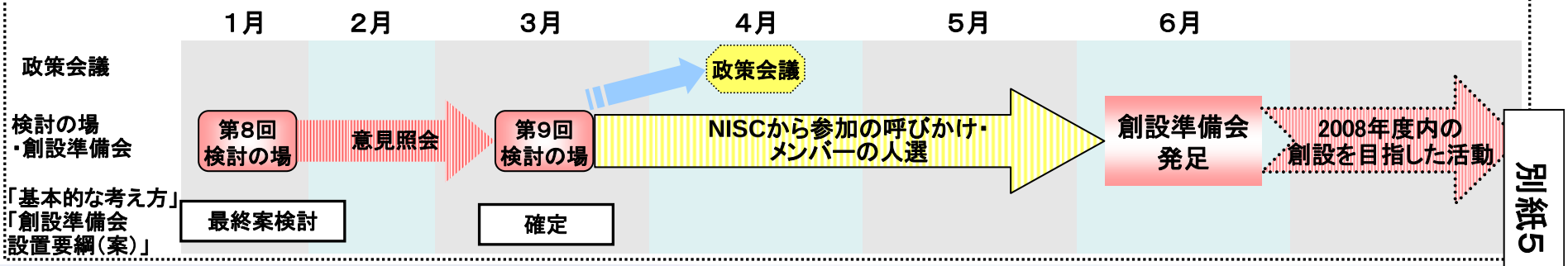
◆「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設準備会設置要綱（案）

- 「基本的な考え方」で設置することとされた創設準備会の設置要綱（案）。

◆2008年度の方針

◆「基本的な考え方」、「創設準備会設置要綱（案）」をもとに、2008年6月を目処に創設準備会を設置し、2008年度内の「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設を目指す。

＜「基本的な考え方」「創設準備会設置要綱（案）」のとりまとめ及び今後の想定スケジュール ＞



別紙5

2007年度分野横断的演習の概要

1．日時　2008年2月6日（水）　13:00～18:30

2．場所　（株）三菱総合研究所　2階セミナー室　他（千代田区大手町）

3．参加者

（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

（CEPTOAR：7分野11CEPTOAR）
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

（関係機関）

（分野横断的演習検討会有識者）
大林慶應義塾大学教授（座長）ほか、検討会有識者

4．概要

官民の連絡・連携体制の機能と、IT障害発生時の対応能力の向上等を図るため、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野のCEPTOAR等の協力を得て、相互依存性解析の知見を踏まえつつ、想定される具体的な脅威シナリオの類型をもとにテーマを設定し、分野横断的な演習を実施した。

全体の総括と今後の方向性

- 異なる分野からの参加者が顔を見合わせずに行う方法をとることで、機能演習として、より現実の状況に近い形での演習を実施できた。
- 「NISC、所管省庁、CEPTOAR、重要インフラ事業者からなる情報共有の仕組み」の検証において、事業者とNISCを両端とした情報の流れが想定通り機能することが確認された。
- サイバー攻撃に対する早期警戒情報の提供等を通じて、緊急時におけるサービスの維持・早期復旧のために事業者が必要とする情報の具体的内容の示唆が得られた。
- 緊急時に、サービスの維持・早期復旧と並行して情報連絡・情報提供を如何に行うかという課題や、実際に情報連絡・情報提供を行う際の、運用上の具体的課題が明らかになった。
- 事前情報の提供を端緒とした情報共有が、緊急時の情報共有にとって有効であることが明らかになった。
- 演習のパターンの検討、機能演習実施のためのシナリオへの反映、課題討議、演習の実施というステップを通じ、次年度以降の演習の方向性に関する示唆が得られた。

- 2008年度以降は、本年度までの結果から得られた知見等を踏まえ、想定される具体的な脅威シナリオ等、諸条件を元に研究課題として検証すべきテーマを設定し、重要インフラ事業者、CEPTOAR、所管省庁、NISCがプレーヤーとして参加し、テーマに応じた最適な演習手法（机上演習、機能演習など）による、より実践的な演習を実施。
- 情報共有体制については、実施細目、情報提供の迅速化、提供される事前情報の信頼性など、多くの課題が明らかになったことから、円滑な情報共有の推進のために、見直しを検討する必要がある。

別紙6－2

「安全基準等の浸透状況等に関する調査」の概要

◆目的・位置づけ

「セキュア・ジャパン２００７」に基づき、２００６年度に策定・見直しを行った各重要インフラ分野における安全基準等（２００７年度に見直し前の安全基準等であることに注意）について、事業者等にどの程度浸透しているか、また事業者等が安全基準等に対して準拠しているかを把握するために行う調査。

安全基準等は随時見直しがなされるものであり、また着実にその浸透を図るべきものであることから、定期的に本調査を実施し、継続的に浸透状況等の把握を行う。

◆調査概要

調査対象範囲	：調査対象とする事業者等の範囲は重要インフラ所管省庁が決定
調査方法	：以下いずれかを重要インフラ所管省庁が選択 ①既存調査を活用　②ＮＩＳＣ案に準じて実施
調査基準日	：２００７年内に調査基準日を設定（②ＮＩＳＣ案に準じて実施 の場合、２００７年１０月１日現在）
アンケートの発出・回収	：重要インフラ所管省庁が配布・回収（配布・回収方法は分野ごとに決定）
分野毎の集計	：集計方法については、重要インフラ所管省庁が選択 ⅰ重要インフラ所管省庁で集計、ⅱＮＩＳＣで集計
全体集計・とりまとめ	：ＮＩＳＣが実施

◆実施時期（②NISC案に準じて実施 の場合）

調査期間	：２００７年１０月～２００７年１２月（集計は２００８年１月まで）
とりまとめ	：２００７年度中

◆調査内容（NISC案）

２００６年度に策定・見直しを行った安全基準等の浸透状況等

- 分野の安全基準について認知されているか
- 情報セキュリティの確保に関する内規等を制定しているか
- 分野の安全基準に基づき、自社の内規等の見直しを実施しているか（予定を含む）　等

まとめ

- **重要インフラ事業者等における情報セキュリティ対策の実施状況を分野横断的な調査により初めて把握**
- **2006年2月の指針の策定を受け、各分野における安全基準等の策定・見直しが着実に浸透していることが推定**

① 安全基準等の整備の状況に関する事項
- 各分野の安全基準等について、調査対象範囲における概ね全ての事業者等に認知されていることが推定
- 大半の事業者等が内規を制定済であるとともに、約7割の事業者等で内規見直しが実施・予定されていることが推定
- 安全基準等の策定・見直し（2006年9月）から1年間にて、約半数の事業者等で内規見直しを実施済と推定
- 一方で、内規見直しを予定していない事業者等も3割近く存在することが推定

② 安全基準等に対する準拠状況に関する事項
- 今回初めて自己点検、演習・訓練、内部監査、外部監査の実施状況について調査
- 本調査を継続して行う中で、これらの事項を引き続き確認していく
- より従業員数の多い事業者等において、概ね実施率が高い傾向にあることが推定

- これらの結果を踏まえ、今後も継続的に調査を実施し、安全基準等の浸透状況等の傾向を把握する
- 加えて、指針の周知及び安全基準等に基づく内規の見直しの推進、並びに的確な情報把握のための調査の改善に努める

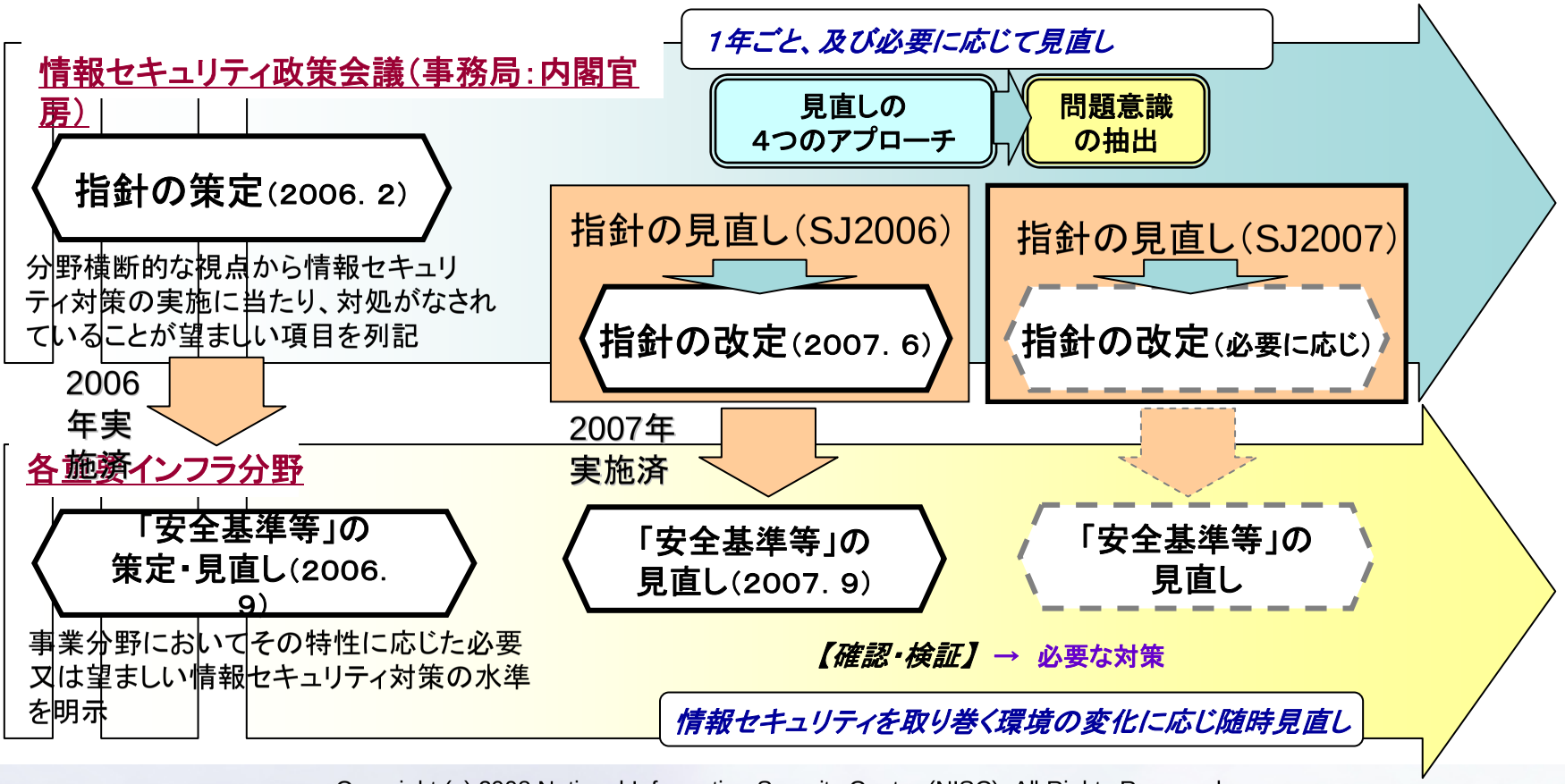
「指針の見直し」の概要

○「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（以下「指針」）は、重要インフラ分野における安全基準等の策定・改定を支援することを目的として2006年2月に策定

○その後、定常的なIT障害の発生状況の把握等を通じて、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行い、指針を改定（2007年6月14日 情報セキュリティ政策会議決定）

○「1年ごと、及び必要に応じて適時に、本指針の見直しを推進する」ことから、本年度も「指針の見直し」を実施

○昨年同様の4つのアプローチより、分析・検証を行い、情報セキュリティ対策に関する「問題意識」を抽出し、現在の指針と照らし合わせ、必要に応じて改定を実施



「指針の見直し」の観点

「指針の見直し」の方向性

◆昨年の4つのアプローチを継承し、2007年度の見直しを実施

◆昨年度実施に至らなかった「相互依存性解析」の成果を踏まえた見直しを実施

（指針より）

・内閣官房は、1年ごと、及び必要に応じて適時に、本指針の見直しを推進する

・内閣官房は定常的なIT障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行い、本指針改定のための基礎資料として整備する

・（前略）内閣官房が各重要インフラ所管省庁及び重要インフラ事業者等の協力を得て相互依存性解析を実施する際には、その結果を本指針や各重要インフラ分野における「安全基準等」の見直しの基礎資料として提供する

（「セキュア・ジャパン2007」より）

2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、指針の見直しを実施する

◆2007年度「指針の見直し」におけるアプローチ

①*定常的なIT障害の発生状況の分析*	・各重要インフラ分野に共通する横断的な対策課題の分析・検討の結果、情報セキュリティ対策の新たな観点が発見されたか
②「*相互依存性解析*」の成果	・相互依存性解析の結果を基礎資料にして、新たな「何らかの対処がなされていることが望ましい項目」をどのように活用できるか ・各分野の特性や分野の関係性によって生じる、ある分野のサービスから別の分野のサービスへの波及の状況について得られた知見をどのように活用できるか
③*関連文書の検証*	・情報セキュリティ対策の新たな観点が追加されたか。それは、重要インフラ分野に共通的な要検討事項といえるか
④*社会的条件（環境）の変化の検証*	・技術の進歩があったか（新たな脅威の発生・新たな対策の確立） ・社会的重要性に変化があったか ・IT障害の発生を未然に防止できた例から、得られる知見や教訓はあるか

※青字部分は、2007年度に新たに追加するアプローチ

CEPTOAR（セプター）（情報共有・分析機能）の整備促進

「重要インフラの情報セキュリティ対策に係る行動計画」

新規3分野（医療、水道及び物流）について、2007年度の整備を目指す

（注）重要インフラ10分野中、既存7分野（情報通信、金融、航空、鉄道、電力、ガス及び政府・行政サービス）は、2006年度末に整備済

（※）CEPTOAR（情報共有・分析機能）：**C**apability for **E**ngineering of **P**rotection, **T**echnical **O**peration, **A**nalysis and **R**esponse

「IT障害の**未然防止**、発生時の**被害拡大防止・迅速な復旧**及び**再発防止**のため、
政府等から提供される**情報**について、
適切に**重要インフラ事業者等に提供**し、**関係重要インフラ事業者等間で共有**」

⇒ 各重要インフラ事業者等の**サービスの維持・復旧能力の向上**に資する

機能・役割
- 政府からの情報提供窓口
- 関係機関、他分野CEPTOAR等との情報共有（相互の合意に基づく）

CEPTOAR（セプター）の整備状況（2007年度末）

◆行動計画で示している**全10分野14のCEPTOARが整備完了。**

◆昨年4月より運用開始している既存7分野に加え、**新規3分野（医療、水道及び物流）は、2008年4月より運用を開始。**

～各CEPTOARとも、最低限の要件（「情報取扱いルール」、「緊急時に連絡可能な窓口」）は整備～

◆**6分野（9CEPTOAR）では、障害事例分析、情勢判断等を整備。**

◆**既存分野においては、平成19年度において、情報共有訓練及び官民連携による分野横断的演習に参加。**

⇒ ***今後は、各CEPTOAR間の分野横断的な情報共有を行う「重要インフラ連絡協議会」（仮称）の創設を促進***

解析内容

2006年～2007年にわたる2年間の相互依存性解析の内容は以下のとおりである。

1. 分野間の相互依存性として、「情報通信分野（通信）は他の7分野と」、「電力分野は他の10分野と」、「水道分野は他の8分野と」相互依存性があることが明確になった。
   なお、2007年度の分野横断的演習では、「情報通信分野（通信）」との相互依存性に着目して、シナリオを検討した。
2. 相互依存性解析についての理解の共通化を図ることを目的として、相互依存性解析に必要となる視点を明確にした。具体的には、「IT障害」、「検討の範囲」、「波及」、「波及の背景となる「関係性」」、「分野の「特性」」、「重要システムとサービスの「独立性」」について整理を行った。
3. 情報通信・電力・水道の各分野が提供するサービスの停止・低下等が起きた場合、その波及を受ける分野において、時間経過に伴う状況の変化等より、下記の事象が表れる可能性があることが明らかになった。
   ① サービスに与える影響の変化
   ② 対応方針の選択
   ③ 新たな分野との関係性
4. 重要システムとサービスの独立性が、高い分野と低い分野があることが判明した。
   a. 独立性の高い分野：情報通信（放送）、鉄道、電力、ガス、医療、水道、物流の各分野
   b. 独立性の低い分野：情報通信（通信）、金融、航空、政府・行政サービスの各分野
   「重要システムとサービスの独立性（以下「独立性」という）」は、重要システムに機能不全が生じたときに、重要システムを用いずに（手作業等による代替手段により）サービスの維持・提供が可能かどうかをいう。
5. 「データの送受信」等に伴う波及に係る関係性、及び「周辺システム」を課題として整理した。（静的相互依存性解析では不明確であった関係性）
6. 相互依存性解析の結果に基づく「分野間の関係性における脅威の類型化」を実施した。
7. 「独立性」、「サービスの提供形態」という観点で、分野の分類を試みた。