NISC National Information Security Center

情報セキュリティ政策について
ー重要インフラ保護政策を中心としてー

2008年2月

内閣参事官　関　啓一郎

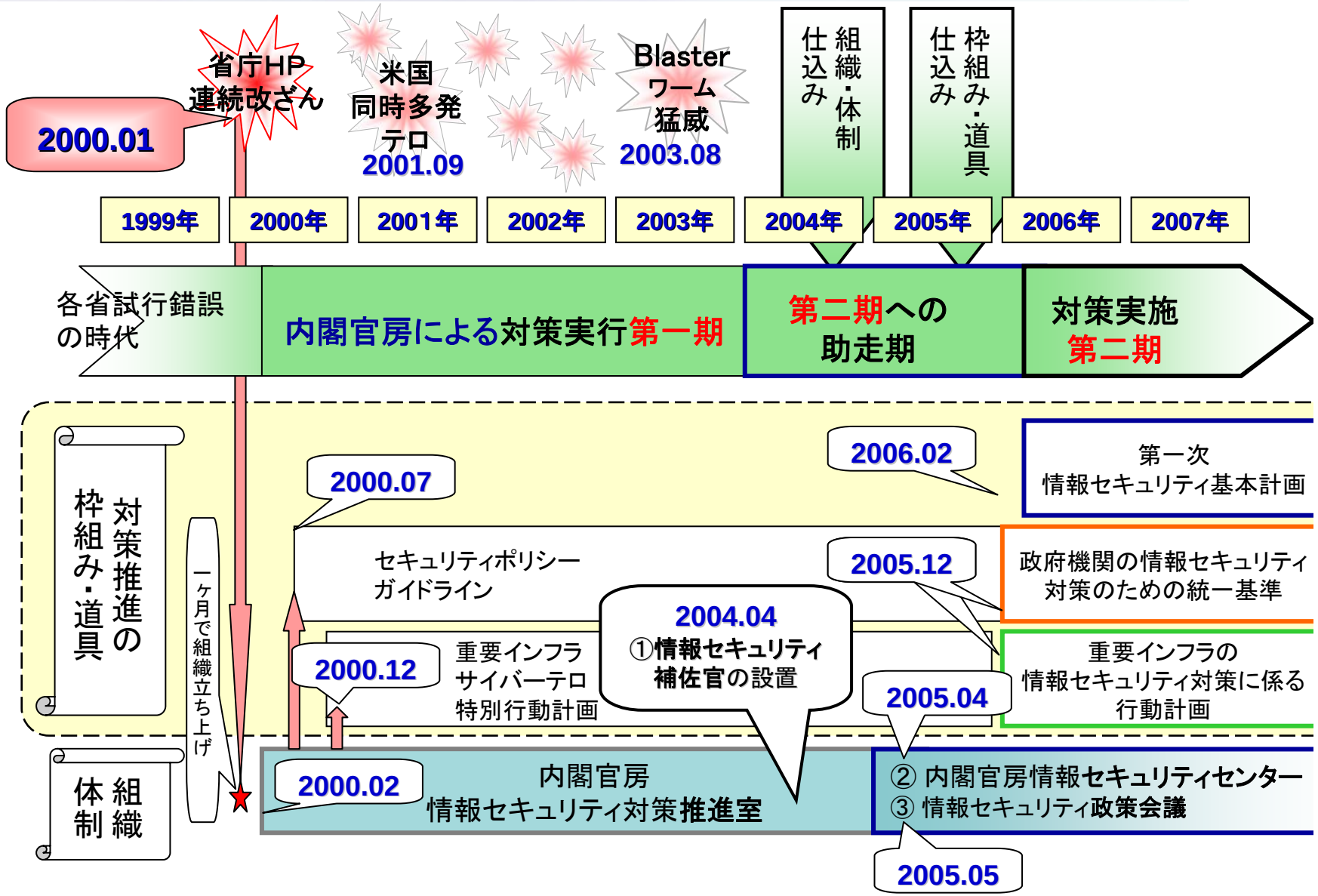
内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

NISC National Information Security Center

政府中核機能の整備

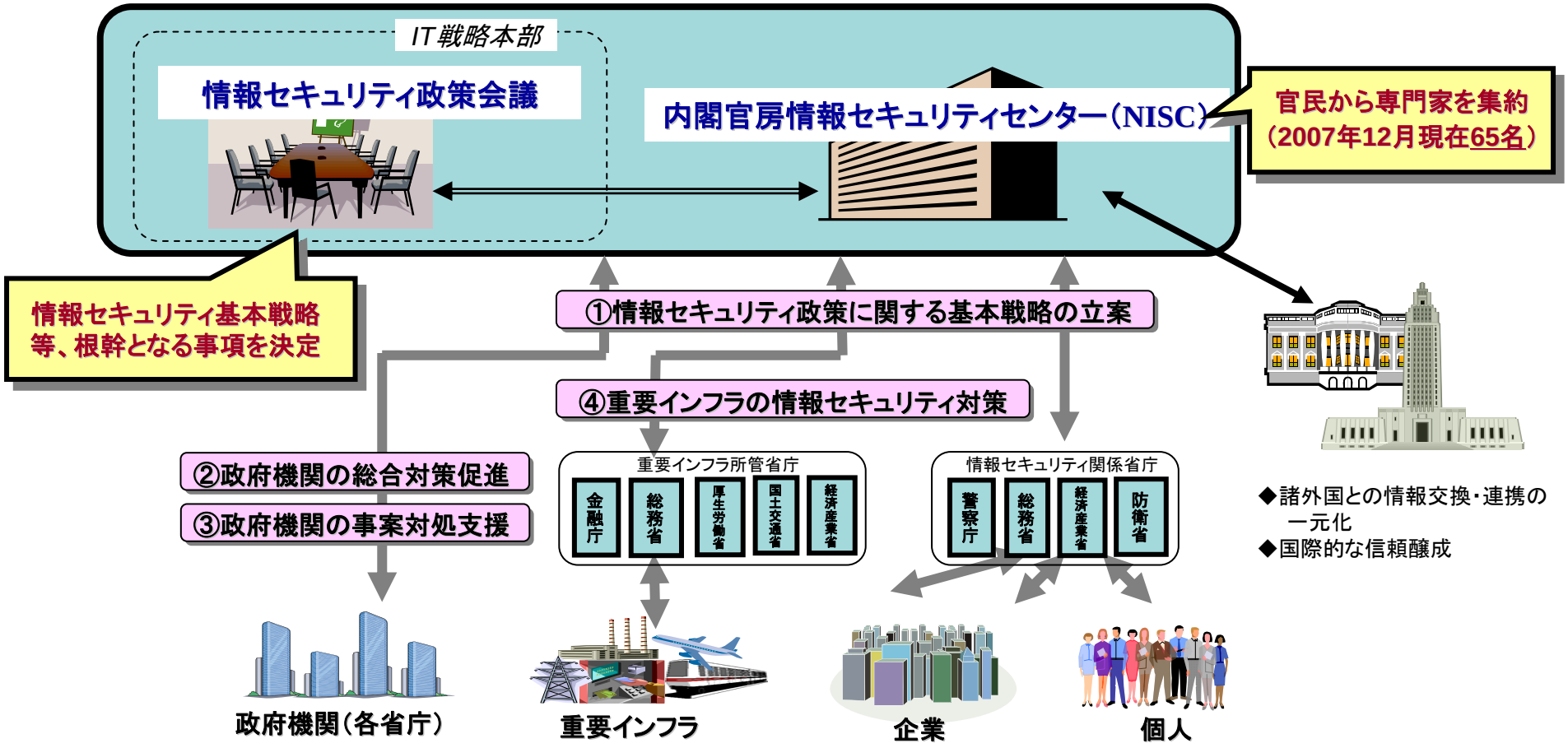
内閣官房における情報セキュリティ政策の流れ（2000年以降の概要）



情報セキュリティ政策会議及び内閣官房情報セキュリティセンター(NISC)の設置

NISC

- 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」(2004年12月7日IT戦略本部決定)を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備中
  - **2005年4月25日、内閣官房情報セキュリティセンター(NISC:National Information Security Center)を設置**
  - **2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」を設置**



情報セキュリティ政策会議の構成

議長

内閣官房長官

議長代理

内閣府特命担当大臣（科学技術政策）

構成員

国家公安委員会委員長

総務大臣

経済産業大臣

防衛大臣

江畑 謙介	拓殖大学客員教授／軍事評論家
小野寺 正	KDDI株式会社代表取締役社長
黒川 博昭	富士通株式会社代表取締役社長
野原 佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田 雅英	首都大学東京教授
村井 純	慶應義塾大学教授

このほかの国務大臣も必要に応じ会議に出席し意見を述べることができる

内閣官房情報セキュリティセンター(NISC)の機能・体制

センター長（安全保障・危機管理担当副長官補）

副センター長（内閣審議官）

情報セキュリティ補佐官（２名）

副センター長（内閣審議官）

基本戦略立案

●全体戦略(「情報セキュリティ基本計画」)策定
●研究開発・技術開発戦略の立案　等

政府機関総合対策促進

●政府統一的な「対策基準」の策定
●政府統一的な情報セキュリティ対策の「評価」 等

事案対処支援

●早期警戒情報の収集・分析機能の強化
●情報セキュリティ関係機関との連携強化　等

重要インフラ対策

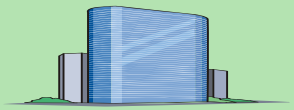
●相互依存性の分析
●横断的な対策基準の策定
●総合的演習の実施　等

国際戦略

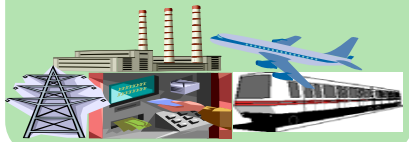
●情報セキュリティに関する我が国の国際戦略の立案
●諸外国の関係機関等との緊密な連携　等

企業　個人

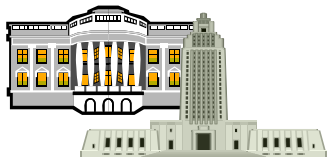
各政府組織



重要インフラ



諸外国関係機関



「第1次情報セキュリティ基本計画」の全体像
ーセキュア・ジャパンの実現に向けてー

NISC

○ 情報セキュリティ問題全般に関する**中長期計画(「全体工程表」)**として、
1)我が国が情報セキュリティ問題に取り組む際の**基本理念**と、2)**重点政策の方向性**を提示
○ **2006年度から2008年度までの3か年計画**として策定。2006年度から、本計画に基づいた年度ごとの推進計画を策定

基本理念

1 経済国家日本の基盤としての情報セキュリティ
2 安全・安心を求める、より良い国民生活実現のための情報セキュリティ
3 新たな安全保障確保の観点からの情報セキュリティ

＜捉えるべき視点＞

◆ 我が国の経済基盤(商取引)の1／4はITに依存
◆ 8000万人のインターネットユーザを抱える世界最大のブロードバンド大国
◆ 災害対策等安全・安心に対する国民ニーズの高まり
◆ ITに起因する新しい安全保障への脅威と、我が国の「強み」の再認識

今後3年間の取組み

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」の構築
～ 内閣官房情報セキュリティセンター(NISC)を中心に、全主体が参加して実行 ～

目指すべき姿

「情報セキュリティ先進国」への進展

【政府機関】:**すべての政府機関**が「政府機関統一基準」が求める水準の対策を実施
【重要インフラ】:IT障害の発生を**限りなくゼロ**に。
【企業】: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
【個人】:「IT利用に不安を感じる」とする個人を**限りなくゼロ**に

「第1次情報セキュリティ基本計画」を実現する個別設計図

「第1次情報セキュリティ基本計画」2006～2008年度の3ヵ年計画。

年度計画：セキュア・ジャパン

2005年度 | 2006年度 | 2007年度 | 2008年度 | 2009年度

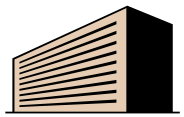
「セキュア・ジャパン2006」 → 評価2006 → 「セキュア・ジャパン2007」 → 評価2007 → セキュア・ジャパン2008

	政府機関・地方公共団体	重要インフラ	企　業	個　人
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
個別設計図	政府機関統一基準	重要インフラ行動計画	内閣官房・各省庁による施策	内閣官房・各省庁による施策

横断的な重要政策

- **情報セキュリティ技術戦略の推進**
  - 技術戦略専門委員会報告書
- **情報セキュリティ人材の育成確保**
  - 人材育成・資格制度体系化専門委員会報告書
- **国際連携・協調の推進**
  - 我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み
- **犯罪の取締り、権利利益の保護救済**
  - 内閣官房・各省庁による施策

評価指標に基づく評価等の基本的な枠組み



情報セキュリティセンター（各府省庁が協力）

情報セキュリティ政策会議

評価指標に基づく評価

補完調査

作業方針の策定

データの把握
評価指標に基づく

評価

補完調査

（必要に応じて）分析

【データ】

【評価結果及び分析結果】

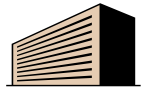
【調査結果及び分析結果】

政策会議へ報告

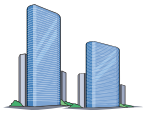
改善に向けた取組み

年度計画等への反映

NISC



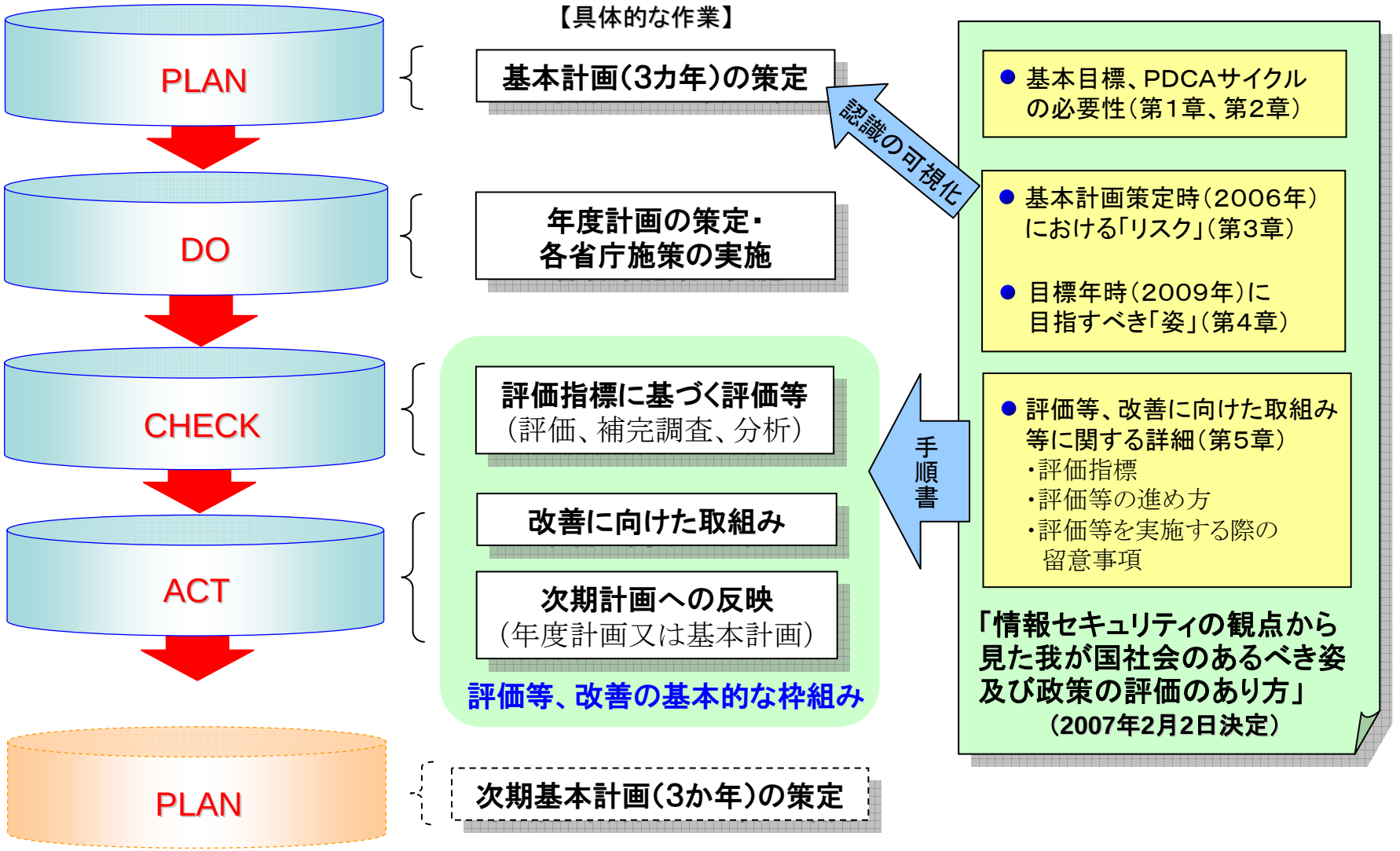
各府省庁



年度計画

基本計画

情報セキュリティ政策のPDCAサイクル



システムトラブルによる混乱（新聞報道等による）

2003．　3　東京航空交通管制部で航空管制システムがダウンし、122便が欠航、721便に遅れ

2003．11　三井住友銀行でシステム障害、振り込み処理が不能に

2003．12　福岡県警で交通管制システムに障害、128台の信号機が制御不能となり、道路が大渋滞

2004．　1　日本臓器移植ネットワークでプログラムミス、6人が臓器移植を受けられず

2005．11　東京証券取引所で大規模システム障害、全銘柄の取引停止へ

2006．　9　NTT東西の光ファイバを利用したIP電話で通話が出来ないなどの障害が発生

2006．10　ソフトバンクモバイルでシステムトラブル、携帯電話の契約受付を2日間停止

2007．　5　全日空で搭乗手続システムがダウン、130便が欠航、306便に遅れ

2007．10　自動改札システム（PASMO等）トラブル、首都圏の約660駅で計4,400台の自動改札機が使用不能となり約260万人が影響

情報セキュリティを取り巻く最近の世界的な動向（ITに起因する脅威）

NISC

- 攻撃のボーダレス化

ネットワークのボーダレス性を利用し、国境を越えた攻撃が行われる。
①ボット化したPCからのDOS（サービス停止）攻撃
②ウェブサイトの脆弱性につけ込んだ攻撃　等

意図的な攻撃活動の上位発信元

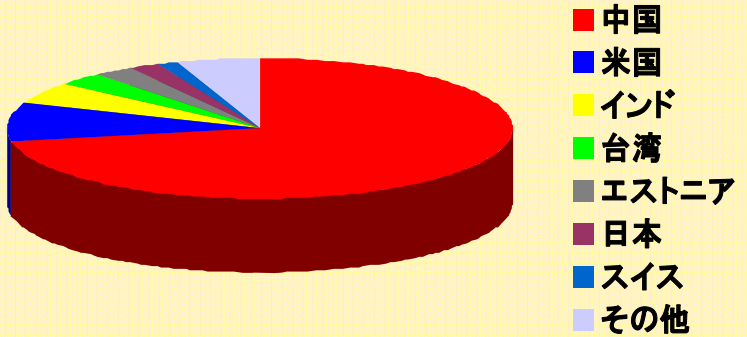
1. 世界向け

ランク	前期のランク	国名	全体に占める割合
1	1	米国	30%
2	2	中国	10%
3	3	ドイツ	7%
4	5	英国	4%
5	4	フランス	4%
6	7	カナダ	4%
7	8	スペイン	3%
8	10	イタリア	3%
9	6	韓国	3%
10	11	日本	2%
		その他	30%

Source: シマンテック

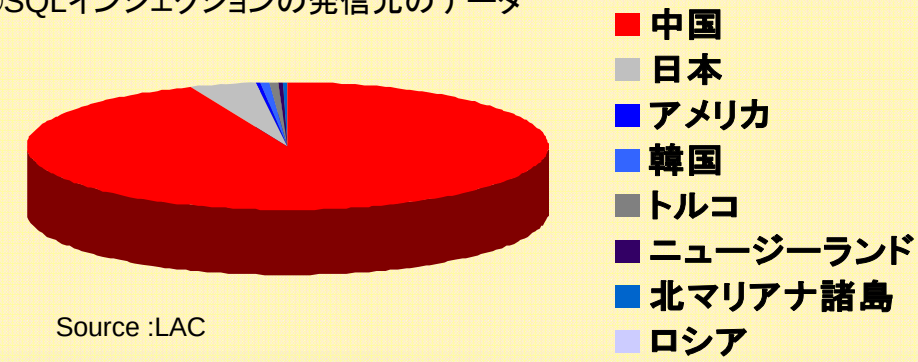
2. 日本向け

①IDSで検知したWorm, Scan等の発信元のデータ



Source : 不正侵入検知システムにおける不正なアクセスの検知分析(警察庁)

②SQLインジェクションの発信元のデータ



Source :LAC

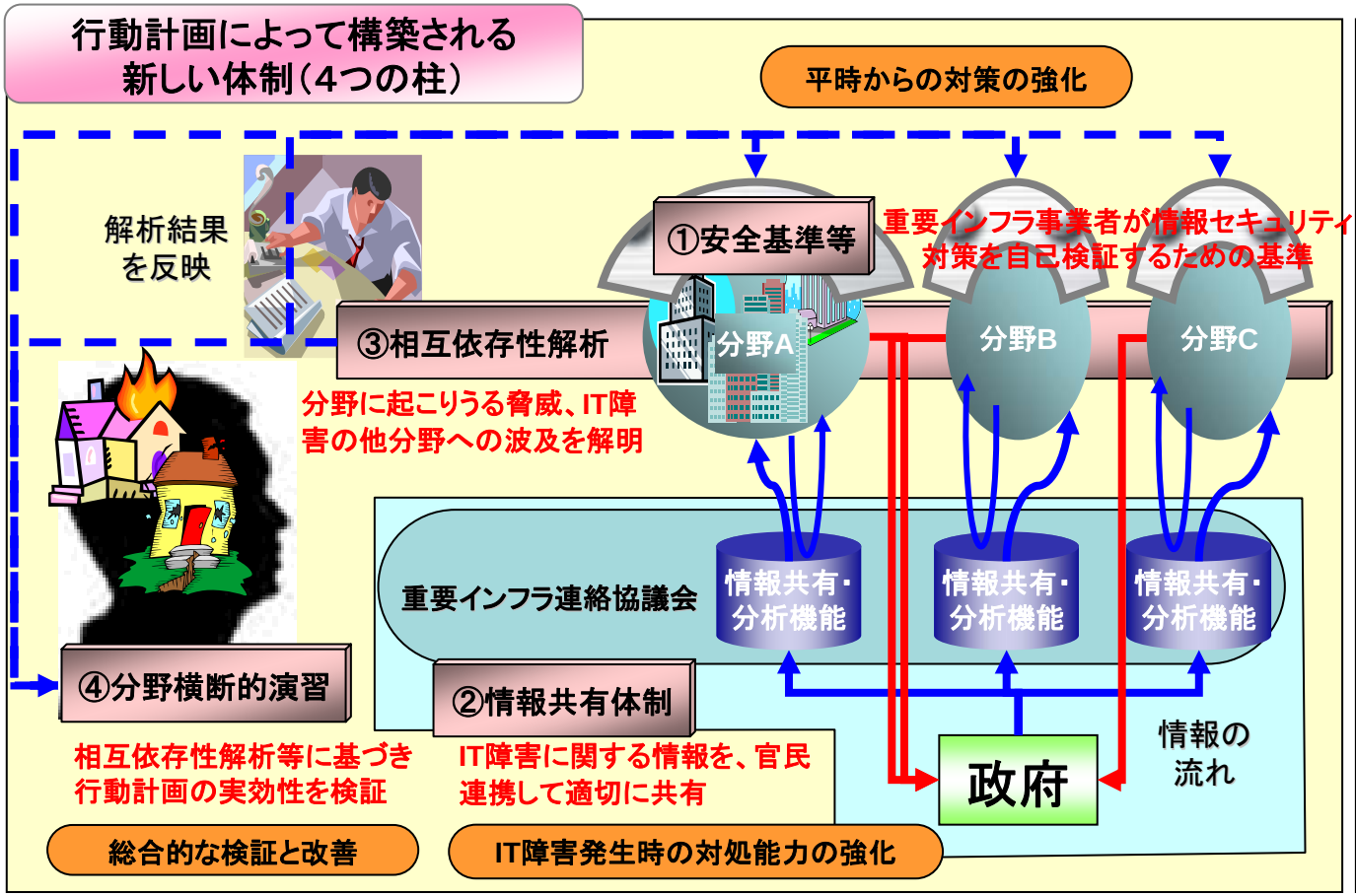
NISC National Information Security Center

重要インフラ保護に関する取組み

個別設計図としての「重要インフラ行動計画」

○ 我が国の重要インフラ（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）横断的な情報セキュリティ水準の向上を図るための「個別設計図」として、「重要インフラの情報セキュリティ対策に係る行動計画」を策定

○ 1）サイバー攻撃のみならず、2）非意図的要因、3）災害に起因する、「ITの機能不全が引き起こすサービスの停止や機能の低下等」（IT障害）から重要インフラを防護



①安全基準等
2006年　内閣官房にて指針策定
2006年9月を目途に各分野にて安全基準等の策定・見直しを努力

②情報共有体制
2006年度末までに、各分野にて情報共有・分析機能を整備（医療、水道、物流は整備に関する基本的合意を2006年度末までに完了）

③相互依存性解析
2006年度　内閣官房にて試行を開始

④分野横断的演習
2006年度　内閣官房にて「研究的演習」、「机上演習」を実施
2007年度　内閣官房にて「機能演習」を実施

本行動計画の実施により、官民が連携した、新しい重要インフラ防護体制の構築へ

「重要インフラの情報セキュリティ対策に係る行動計画」の概要

● 2000年12月に策定された「重要インフラのサイバーテロ対策に係る特別行動計画」は、増大するサイバーテロの脅威から7つの重要インフラ分野の防護のための初めての官民協力の枠組みについて規定していた
● その後の各重要インフラ分野におけるIT利用の飛躍的進展とITへの依存度の増大、重要インフラ間相互の依存性の増大等の変化を踏まえ、**「重要インフラの情報セキュリティ対策に係る基本的考え方」（2005年9月15日情報セキュリティ政策会議決定）**に基づき、新たな行動計画を策定

対象分野・脅威の見直し

基本的考え方	行動計画
➢ 重要インフラ分野として、医療・水道・物流を加えた10分野を設定 ➢ 想定する脅威を、「サイバー攻撃」に加えて、人為的ミス等の「非意図的要因」、「自然災害」へと拡大	➢ 重要インフラ分野として10分野*を指定し、具体的対象事業の範囲を設定 ➢ 想定する脅威及び各分野別重要システムを例示

新たな体制の構築

1. 情報セキュリティ水準の向上

➢ 技術的基準及び運用基準についての「安全基準・ガイドライン」の策定・見直し等を実施	➢ 2005年度中に、内閣官房情報セキュリティセンターは「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」を策定 ➢ 各分野は、上記指針を踏まえて、必要又は望ましい情報セキュリティ対策の水準を2006年9月を目処に「安全基準等」に明示するよう努力

2. 情報共有体制の強化

➢ 情報提供体制の整理・強化、情報充実・質の向上 ➢ 「情報共有・分析センター」（仮称）等の各分野内情報共有機構の創設 ➢ 重要インフラ横断的な情報共有の推進（「重要インフラ連絡協議会（仮称）の設立等）	➢ IT障害発生時における連絡体制等、官民の情報共有、連絡・連携の仕組みについて具体的に規定 ➢ 2006年度末まで**に各重要インフラ分野ごとに「情報共有・分析機能（CEPTOAR）」の整備を推進 ➢ 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の設立に向けた検討の場を内閣官房に設置

3. 相互依存性解析

➢ 内閣官房情報セキュリティセンターを中心に重要インフラ分野横断的な状況把握（相互依存性解析等）を実施	➢ 相互依存性解析の効果・実施の流れを記載 ➢ 内閣官房情報セキュリティセンターを中心に、2006年度から相互依存性解析を試行

4. 分野横断的演習の実施

➢ 想定脅威に対応した具体的脅威シナリオの類型を元に、毎年度、重要インフラ分野横断的な演習を実施	➢ 2006年度に「研究的演習」、「机上演習」、2007年度に「機能演習」を段階的に実施 ➢ 内閣官房において「演習実施計画」を立案、内閣官房の監修の下、各重要インフラから参加する形態で実施

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の概要

重要インフラのIT障害に対する脅威の増大
相互依存性の増大
各事業分野ごとの多様性

国民生活や社会経済活動の基盤である重要インフラ

情報セキュリティ対策は、その効果が見えにくく
「何をすべきか」、「どの程度すべきか」の判断が困難

内閣官房

指針の策定

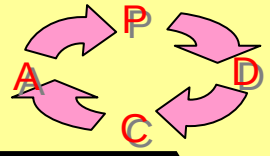
【目的】各重要インフラ分野における「安全基準等」の策定・見直しの支援

↓

分野横断的な視点から情報セキュリティ対策の実施に当たり、対処がなされていることが望ましい項目を列記

1年ごと、及び必要に応じ随時見直し

各重要インフラ分野



重要インフラ所管省庁
「強制基準」、「推奨基準」

「安全基準等」の策定・見直し
・事業分野においてその特性に応じた必要又は望ましい情報セキュリティ対策の水準を明示

情報セキュリティを取り巻く環境の変化に応じ随時見直し

重要インフラ事業者等
「対策実施基準」

事業者団体
「業界ガイドライン」

真に依存可能な基盤としての重要インフラへ向けた継続的かつ検証可能な取組みの実現

Ⅰ　目的及び位置づけ

1．重要インフラにおける情報セキュリティ確保のために
2．「安全基準等」の必要性
3．「安全基準等」とは何か
4．本指針の位置づけ
5．本指針を踏まえた安全基準等策定若しくは見直しへの期待

Ⅱ　「安全基準等」で規定が望まれる項目

1．「安全基準等」の対象範囲及び対象とする脅威
2．「安全基準等」の公開
3．具体的項目
(1)「安全基準等」策定の目的
(2) 対象範囲と想定する脅威
(3) 重要インフラ事業者等の担う役割
(4) 対策項目
① 4つの柱
ア　組織・体制及び資源の確保
イ　情報についての対策
ウ　情報セキュリティ要件の明確化に基づく対策
エ　情報システムについての対策

② 3つの重点項目
ア　IT障害の観点から見た事業継続性確保のための対策
イ　情報漏えい防止のための対策
ウ　外部委託における情報セキュリティ確保のための対策

Ⅲ　フォローアップ

(1)　本指針の見直し　（1年ごと、及び必要に応じて適時に）
(2)　「安全基準等」の継続的検証

重要インフラにおける「分野横断的演習」及び「相互依存性解析」の概要について

○ 「分野横断的演習」及び「相互依存性解析」については、2007年度は、共通/分野ごとの演習シナリオに基づく「機能演習」(※1)を実施し、技術及び組織運営上の課題事項を検証するとともに、相互依存性解析を実施して、脅威の類型や脅威と障害の因果関係、障害と事業継続の関係などについての検討の深化等を図り、動的解析を実施方法から検討し実施する。

○ 2007年度においては、行動計画を踏まえた具体的な検討のため、内閣官房情報セキュリティセンターに検討会を設置し、重要インフラ所管省庁、重要インフラ事業者、CEPTOAR等の協力を得つつ実施。検討会は、それぞれ専門的識見(※2)を有する有識者、重要インフラ所管省庁、重要インフラ事業者、CEPTOAR等により構成。

（※1） 実際の組織の指示判断系統機能を用いて模擬的に検証するための演習。

（※2） 分野横断的演習検討会については、演習コーディネーター、防災、危機管理、リスクマネジメント、BCP、複数の分野におけるシステムや機能に知見を有する研究者・専門家等。相互依存性解析検討会については、相互依存性解析、複数の分野におけるシステムや機能に知見を有する研究者・専門家等、BCP等の研究者・専門家等。

重要インフラの情報セキュリティ対策に係る行動計画

（2005年12月13日情報セキュリティ政策会議決定）

【4つの柱】

1.「安全基準等」の整備
2. 情報共有体制の構築
   (1) 官民の情報提供・連絡
   (2) CEPTOAR
   (3) CEPTOAR-Council
3. **相互依存性解析の実施**
4. **分野横断的演習の実施**

＜2006年度＞

＜Collaborationづくり＞
～官民連携の仕組みづくりに資する取組み～

＜Communicationの検証・向上＞
～官民連携の枠組みの実効性向上のための取組み～

＜2007年度以降＞

＜Functionの検証・向上＞
～官民連携体制の機能向上のための取組み～

研究的演習
演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とした演習の実施により、机上演習に向けたシナリオづくり等を行うとともに、官民連携の体制づくりへ寄与

机上演習
演習参加者が、1つのシナリオを基に会議形式で課題討議を行いながら実施し、官民の情報共有等の検証や課題の抽出などを通じて、官民連携の枠組みの実効性向上に寄与

機能的演習
各CEPTOARの整備後、共通／分野ごとの演習シナリオに基づき実施し、組織運営上及び技術上の課題事項を検証し、官民連携体制の機能的向上に寄与

※3 ※4

静的解析
重要インフラに発生しうる脅威、重要インフラにおける障害発生や復旧に係る分野間の関係を定性的に把握

動的解析
重要インフラにおける動的・障害要因の連鎖的伝搬を時系列的・定量的に把握

※3 ※4

（※3） 想定脅威、シナリオ想定のための知見。

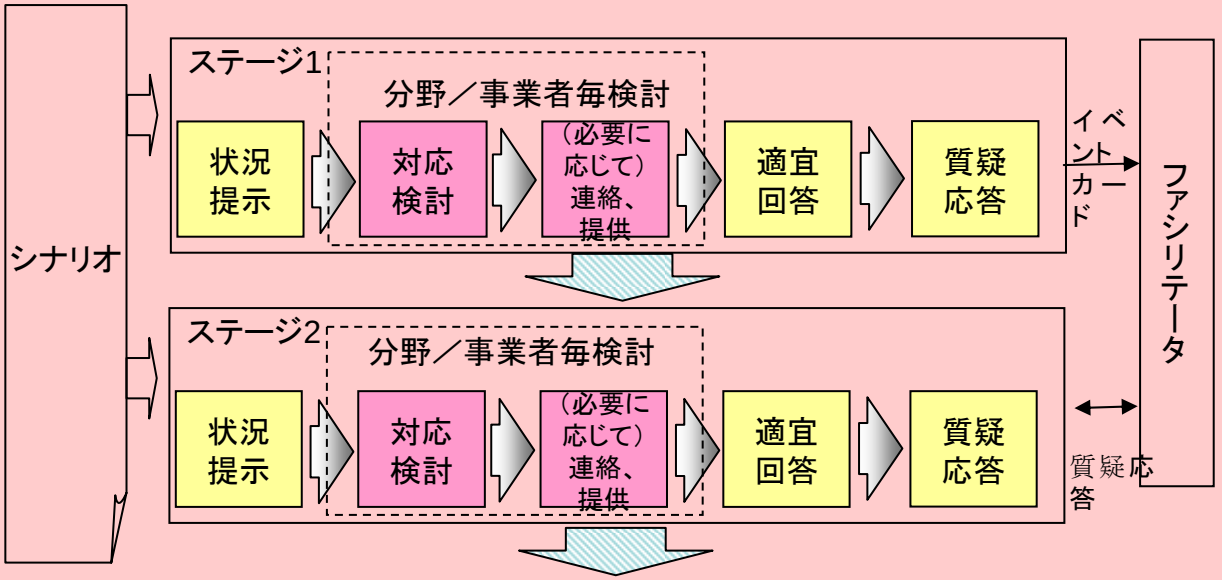
（※4） 課題の検証等を通じた次のステップでの解析の視点等提供

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、分野横断的な「機能演習」を実施

実施日時　2008年2月6日（水）

機能演習は、各ステージにおいて、以下のように進行する。
1）大部屋にて、ファシリテータは、プレイヤにシナリオに記述された状況設定を提示する
2）各部屋にて、プレイヤは分野毎または事業者毎に対応を検討する
3）各部屋にて、プレイヤは必要に応じて、他のプレイヤへ情報連絡、情報提供を行う
4）大部屋にてファシリテータは、質問を行う
5）参加者が適宜回答する、　6）参加者間での質疑応答を行う

機能演習の進行イメージ




演習風景（全体説明時）


演習風景（分散時）

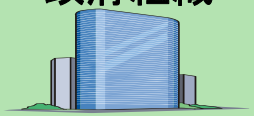
NISC National Information Security Center

第２次情報セキュリティ基本計画（仮称）の検討について

「第1次情報セキュリティ基本計画」策定時の経緯

「第1次情報セキュリティ基本計画」
（2006.2.2 情報セキュリティ政策会議決定）
情報セキュリティ問題を俯瞰した中長期の戦略

政府組織



重要インフラ

企業　個人

◆情報セキュリティに関する研究開発・技術開発の戦略的な推進

セキュリティ文化専門委員会報告書
（2005.11.17）
セキュリティ文化の醸成に関する方策

技術戦略専門委員会報告書
（2005.11.17）
情報セキュリティに係る研究開発・技術開発、その成果利用の戦略

情報セキュリティ基本問題委員会 第1次提言
（2004.11.16）
情報セキュリティ政策会議の設置
内閣官房情報セキュリティセンター（NISC）の設置

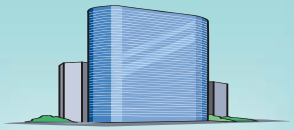
情報セキュリティ基本問題委員会 第2次提言
（2005.4.22）
重要インフラ分野における情報セキュリティ対策の強化の必要性について提言

重要インフラ専門委員会行動計画及び指針
（2005.12.13 行動計画）
（2006.2.2 安全基準等策定指針）
重要インフラの情報セキュリティ対策に係る具体的施策

「第1次情報セキュリティ基本計画」策定後の取組み

○ 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」の構築に向けて、2006年度からの3年間、政府は「第1次情報セキュリティ基本計画」に基づき、各種対策を強化

主な取組み（4領域）

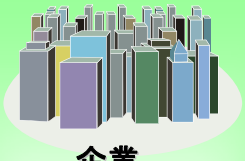


政府機関・地方公共団体

- ◆「政府機関統一基準」の策定及び見直し（H17.12.13策定、H19.6.14改訂）
- ○重点検査及び評価結果公表 (H18.7.25,H19.8.3)
- ○セキュリティマネジメントに関する評価結果公表 (H19.8.3)
- ◆ サイバー攻撃等への緊急対応能力の強化（GSOCの構築）（H19FY以降）

重要インフラ

- ◆ 重要インフラ行動計画策定（H17.12.13）
- ○ 安全基準等策定指針改定（H19.6.14）
- ○ 情報共有・分析機能の整備
- ○ 重要インフラ連絡協議会（仮称）の検討の場設置（H19.3.29）
- ○ 分野横断的な演習（H19.2.7）、相互依存性解析の実施



企業

- ◆ 情報セキュリティ監査等第三者評価制度の活用推進
- ◆ コンピュータウィルス等への対応体制の強化

個人

- ◆「情報セキュリティの日」の創設等広報啓発の強化（H19.2.2）
- ◆ 情報セキュリティ教育の推進

主な取組み（横断的事項）

情報セキュリティ技術戦略の推進

- ◆ 技術戦略専門委員会報告書（H17.11.17、H19.6.29）
- ◆ 高セキュリティ機能を実現する次世代OS環境の開発（H18FY以降）

情報セキュリティ人材の育成確保

- ◆ 情報セキュリティの資格制度を体系化（H19.1.23）（人材育成・資格制度体系化専門委員会報告書）

国際連携・協調の推進

- ◆ 情報セキュリティ分野における「国際協調・貢献」の策定（H19.10.3）
- ◆ サイバーセキュリティ日米会合の開催（H19.8）

犯罪の取締り、権利利益の保護救済

- ◆ サイバー犯罪の取締りのための技能水準の向上
- ◆ デジタルフォレンジックに係る知見の集約・体系化の推進

第二次基本計画の検討について

1. 検討のための専門委員会の設置

（1） 3か年の中長期戦略「第1次情報セキュリティ基本計画」は、平成20年度（2008年度）が最終年度。

（2） 残された課題
政府機関における情報セキュリティ事故、重要インフラにおけるIT障害の発生などは後を絶たず、企業等における情報セキュリティの具体的な対策や体制作り、人材の確保といった面でも解決すべき課題が多く残されている。

（3） 専門委員会設置
第1次基本計画が最終年度を迎えるにあたり、官民における各種取組み、技術革新や制度改正等を含めた社会環境の変化などを踏まえ、平成21年度（2009年度）からの情報セキュリティ政策の在り方・方向性について検討を行うため、情報セキュリティ政策会議の下に、「基本計画検討委員会」を設置。

2. 専門委員会の構成と検討の進め方

（1） 委員構成　次ページのとおり

（2） 検討スケジュール

平成20年1月　　第1回委員会～以後、数回開催
2～3月　産業界、消費者、府省等の関係者からのヒアリング
4月頃　「第一次提言」（仮称）（政策会議）、　6、7月頃　検討再開～以後、数回開催
12月頃　「第2次基本計画（仮称）」（案）（政策会議）、パブコメ
平成21年2月　　「第2次基本計画（仮称）」決定（政策会議）

基本計画検討委員会の構成

委員長	須藤　修	東京大学大学院情報学環・学際情報学府教授
委員	有賀　貞一	株式会社CSKホールディングス代表取締役
	井川　陽次郎	読売新聞東京本社論説委員
	井上　雅博	ヤフー株式会社代表取締役社長
	筧　捷彦	早稲田大学理工学術院教授
	木内　里美	大成建設株式会社社長室理事情報企画部長
	重木　昭信	株式会社NTTデータ代表取締役副社長執行役員
	下村　正洋	NPO日本ネットワークセキュリティ協会事務局長
	神保　謙	慶應義塾大学総合政策学部専任講師
	関　正樹	関彰商事株式会社代表取締役社長
	高橋　伸子	生活経済ジャーナリスト
	富永　新	日本銀行金融機構局考査役兼企画役システム関連考査担当総括
	中尾　康二	テレコム・アイザック推進会議委員（KDDI株式会社情報セキュリティフェロー）
	深谷　聖治	東日本旅客鉄道株式会社総合企画本部システム企画部長
	満塩　尚史	環境省情報化統括責任者（CIO）補佐官 （各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
	宮地　充子	北陸先端科学技術大学院大学情報科学研究科教授
	三輪　信雄	綜合警備保障株式会社参与
	安冨　潔	慶應義塾大学大学院法務研究科（法科大学院）・法学部教授
	和貝　享介	監査法人トーマツ

このほかに情報セキュリティ政策会議有識者構成員（その代理人を含む）も必要に応じ会議に出席し意見を述べることができる。

NISC National Information Security Center

「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点

（基本計画検討委員会第一回資料より重要インフラ関係部分抜粋）

2008年1月16日（水）

※　本資料は、情報セキュリティ政策会議有識者構成員、基本計画検討委員会委員のコメントなどを取りまとめた段階のものであり、各々のコメントの中には、マクロ・ミクロの様々な視点のものが含まれている。

検討の視点（概要）　（１）

１．基本認識

○ 現在の社会環境とITが果たす役割
- ― ここ数年の社会環境の変化の特徴、
- ― ITが社会環境の変化に果たす役割の評価
- ― ITの社会における位置付け

○ 情報セキュリティ政策に関する現状認識と評価
- ― 「IT安心利用環境」の構築という第１次計画の目標をどう考えるか
- ― 確保すべき「IT安心利用環境」の変化
- ― 「IT安心利用環境」の効率的な実現に向けて政府、市場、社会規範、技術が果たす役割
- ― 情報セキュリティの定義
- ― Preparedness（準備できていること）、Response（対応）、Recovery（回復）という段階で見て、第１次計画の政策の評価

２．総論

○ 情報セキュリティ政策の理念
- ― 「費用対効果」の視点
- ― 「利便性」の視点
- ― 「不祥事」・「恥」意識から、原因究明による「再発防止」優先への転換
- ― １００％事前防止意識の払拭
- ― 「対策疲れ」と責任限界点の不存在、対策と免責の関係
- ― 「市場原理」の活用
- ― 外部不経済として他者に及ぶ影響
- ― 人的要因による問題発生に対する対策と意識作り
- ― 外部委託のメリット・デメリット
- ― 社会・産業界の円滑な活動維持に加え、国家安全保障
- ― 国際～諸外国の政策との整合性、海外の最善事例の取入れ
- ― 社会変革の予測とそれへの対応

検討の視点（概要）　（２）

○ 第2次基本計画の枠組み
- 主体（政府機関、重要インフラ、企業、個人）の分類の妥当性
- 「重要インフラ」の対象の範囲
- 「企業」の分類の要否
- 「個人」における未成年者、高齢者の扱い
- 大都市と地域の問題
- 他分野（リサイクル、防災、個人情報保護等）との整合性
- 横断的分野（技術、人材、国際、犯罪取締り及び権利利益）の妥当性

3. 各論

○ 政府機関
- 今後どのような政府機関対策が必要か、 対策は、予算面、人員面で十分と言えるのか
- 安全保障・外交等の機密情報を扱う場合の対応、 小規模自治体の対策

○ 重要インフラ
- 事業継続のための情報セキュリティについてどう考えるか

○ 企業
- 企業における対策をどう評価するか。中小企業を対象とした対策は必要か。
- IT提供企業は、情報セキュリティ確保にどのような役割を果たすべきか。

○ 個人
- 個人に対する情報セキュリティ対策をどう評価するか。将来予想される課題をどう考えるか。

○ 技術開発

○ 人材育成

○ 国際連携・協調

○ 犯罪取締り、権利利益の保護・救済

○ その他
- 情報セキュリティ基本法は必要か。情報保護に関する法制度は必要か。外部委託における情報セキュリティ確保のための一般法制度は必要か。

情報セキュリティ政策の理念について（１）

情報セキュリティ政策の理念として検討すべきことは何か。また、戦略としてのメッセージ性は必要か。どこに置くべきか。

１.「費用対効果」の視点。

－情報セキュリティ対策の自己目的化の回避。守るべきもののコスト把握は可能か。

２.「利便性」の視点。

－利便性を過度に犠牲にすると現実から遊離しないか。利便性と情報セキュリティの均衡に関する社会的合意形成は可能か。

３.「不祥事」・「恥」意識から原因究明による「再発防止」優先への転換（後掲）。

－「事故・被害隠し」から「情報の共有」へ。隠すのではなく明らかにする方向での意識改革はできるのか。対応に取組むことが「常識」・「良いこと」である文化・社会規範の形成が必要ではないか。

４. １００％事前防止意識の払拭。

－問題発生を前提としたResponse, Recovery段階での対応の明確に意識して準備すべきではないか。

－技術革新が速いこの分野では、「完璧」を求めないという社会的合意を形成すべきではないか。むしろ、失敗しつつも進めていく対応が必要ではないか。

情報セキュリティ政策の理念について（２）

5. 何をどこまで行えば良いか。「対策疲れ」と責任限界点の不存在／対策と免責の関係。

－ベースラインの設定は可能か。リスク管理の体系化により「容認できるリスク」と「容認できないリスク」の仕分けができないか。
－計画段階で目標・達成水準の設定がなければ対策の限界がなくなるのではないか。
－情報セキュリティのレベルについての意識の共有なくして議論できないのではないか。
－ある種の免責がないと対策へのインセンティブが働かないのではないか。
－過度の責任追及は問題の隠蔽につながるという問題意識が必要ではないか。

6. 「市場原理」の活用の視点（特に企業の場合）。

－市場原理が働く領域と働かない領域の仕分けは可能なのか。

7. 外部不経済として他者（顧客・取引先等）に及ぶ影響（社会的コスト）について、どう考えるか。

8. 人間系（運用する人）の問題　［人的要因に対する対策と意識作り］。

9. 外部委託のメリット・デメリットの明確化（後掲）。

10. 社会・産業界の円滑な活動維持の面に加え、国家安全保障の視点（後掲）。

－国が守るべきもの、企業・個人のリスクに任せられないものは何か。

11. 国際の視点、諸外国の政策との整合性、海外の最善事例の取り入れ。

12. 社会変革の予測とその変革への対応という視点。

第２次情報セキュリティ基本計画の枠組みについて

第1次基本計画は、新たな官民連携の構築を掲げ、対策実施領域として、政府、重要インフラ、企業、個人の4領域と、横断的分野として、技術、人材、国際、犯罪対策・権利利益の保護の4つの枠組みを設けている。政策の継続性と環境変化への対応の間でどのような見直しが必要か。

1. どのような分野にどのような目標を設定すべきか。
2. 政府、重要インフラ、企業、個人以外の分類はあるか。
3. 重要インフラの対象拡大は必要か。対象を拡大すると別の問題が生じないか。
4. 「企業」は一括りで良いのか。
   （例）IT利用企業（一般企業）とIT提供企業（機器事業者、ソフトウェア・ASP・SaaS、通信事業者等）に分類
   一般企業をさらに大企業と中小企業に分類
5. 「個人」では、未成年者を別扱いとするべきか。高齢者はどうか。
6. 中身のある外部委託（アウトソーシング）のあり方（専門性の活用、ブラックボックス化の回避、委託先のリスク管理等）。
7. 大都市と地域の問題をどう考えるか。
8. リサイクル、防災、個人情報保護等の他分野の政策との整合性をどう取るか。
9. 横断的分野として新たに取り上げるべき分野はないか。

重要インフラにおける情報セキュリティ対策について（１）

国民生活や社会経済活動に不可欠なサービスを提供する重要インフラにおいても、情報システムは不可欠なものになっている。事業継続のための情報セキュリティについて、どのように考えるべきか。

1.「重要インフラ」というカテゴリーの範囲（事業の種類や規模等）をどのように考えるか。また、利用者（国民等）の視点からの「事業継続」をどう考えるか。

2. OECD等の場で議論されている重要情報インフラ（Critical Information Infrastructure）の概念について、我が国としてどのように対応を行っていくか。

3. 重要インフラに係る事業継続性の観点からの情報セキュリティについて、その共通課題と個別課題、及びそれに対する対応をそれぞれどう考えるか。

4. 重要インフラの情報セキュリティ対策について、部分最適と全体最適の差異はあるのか。あるとしてどのような対応が必要か。また「個々の利用者」の視点と「社会全体」の視点との差異はどうか。

重要インフラにおける情報セキュリティ対策について（２）

５．各業法でカバーしていない部分の情報セキュリティをどうすべきか。民の自主的な取組みによる成果をいかにして確保していくべきか。

６．重要インフラにおける連携体制が自律的に推進される仕組みは作れないか。

７．同一分野内では競合関係にある他社との情報共有は可能か。

８．不祥事意識・「恥の文化」の中、原因究明と再発防止対策（教訓）を１社内でなく広く共有する方法はあるか。

９．分野を超えた協力を進める上での障害は何か。

10．重要インフラ分野内での相互作用（システム障害の連鎖等）をどう考えるか。

11．問題発生に関して、調査報告を行う権限を有する体制（事故調査委員会のようなもの）は必要か。

12．経営者をはじめ組織全体として、情報セキュリティについて十分な関心を持っているか。