資料3

我が国における情報セキュリティの役割の見直しとその実現に向けて
ー「第1次情報セキュリティ基本計画」の策定へー

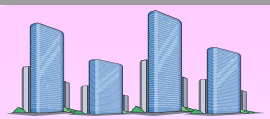
2005年12月13日

内閣官房情報セキュリティセンター（NISC）

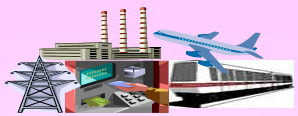
情報セキュリティ問題を巡る我が国の現状

○行政機関からの情報漏洩、国民生活･社会経済活動の基盤となる重要インフラの情報システムの停止、企業からの個人情報の漏洩等、情報セキュリティ問題は多発し複雑化する一途。

○従来からの、個別縦割り的対応、対症療法的対応を見直し、1)「全体工程表」と、2)「個別設計図」を組み合わせ、我が国の「強み」を活用した戦略的な取組みを推進することが必要。



政府機関･地方公共団体



重要インフラ

企業

個人

現状

多発し複雑化する情報セキュリティ問題

◆行政機関からの情報漏洩（複数）

等

◆航空関連システムの停止（2005.8）

◆証券取引システムの停止（2005.11）

◆原子力関連情報の漏洩（2005.6）

等

◆企業からの個人情報の漏洩（複数）

等

◆スパイウェアを利用したインターネットバンキング情報の窃取（複数）

等

個別対策の限界

対症療法的対策の限界

我が国の「強み」の活用不足

今後の取組み

●「全体工程表」（＝基本計画）と各分野の「個別設計図」（＝政府機関統一基準、重要インフラ行動計画等）を組み合わせた全体戦略が必要。

⇒ 我が国の「強み」を活用した戦略的取組みの推進

第1次情報セキュリティ基本計画（案）の全体像

～新しい官民連携モデルの構築による情報セキュリティ先進国への進展～

○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ヵ年計画として策定。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 ～

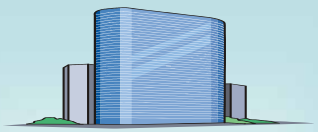
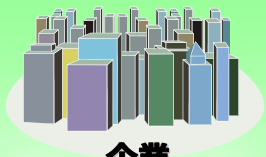
目指すべき姿

「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
［企業］：**すべての公開企業**がリスクに応じた適切な対策を実施
［重要インフラ］：IT障害の発生を**限りなくゼロ**に。
［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（案）－今後3年間の重点政策－

○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、今後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。

	政府機関・地方公共団体	重要インフラ	企業	個人
				
役割	情報セキュリティ対策の「ベストプラクティス」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報セキュリティ対策の実施	IT社会の担い手としての意識の向上
今後３年間の主な重点政策①（４領域）	◆政府機関統一基準に基づいた 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 ◆ 重要インフラ連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆政府調達における入札条件の整備 ◆ 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	◆ 情報セキュリティ教育の推進 ◆「情報セキュリティの日」の創設等広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等の環境整備
【個別設計図】	政府機関統一基準	重要インフラ行動計画	各省庁による施策	各省庁による施策

今後３年間の主な重点政策②（横断的事項）

情報セキュリティ技術戦略の推進
◆政府が活用することを前提とした技術開発実施
◆「グランドチャレンジ型」技術開発の推進

情報セキュリティ人材の育成確保
◆ 多面的・総合的能力を有する実務家の育成
◆ 情報セキュリティの資格制度を体系化

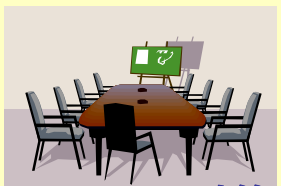
国際連携・協調の推進
◆ 国際的な安全・安心の基盤づくりへの貢献
◆ 我が国発の国際貢献

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強化及び関連基盤整備
◆ サイバー空間の安全性向上のための技術開発

「政府機関統一基準」（個別設計図①）

○政府機関全体としての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、「政府機関の情報セキュリティ対策のための統一基準」を策定。

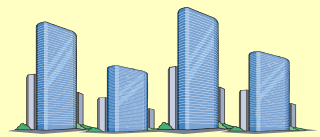
○各政府機関は本基準を踏まえて対策を実施し、内閣官房情報セキュリティセンター（NISC）が対策実施状況を検査・評価。その結果に基づき、情報セキュリティ政策会議が改善を勧告。



情報セキュリティ政策会議
- 政府機関統一基準の策定
- 各府省庁の評価結果に基づき改善を勧告

政府機関統一基準
各府省庁が最低限採るべき情報セキュリティ対策を定めたもの。

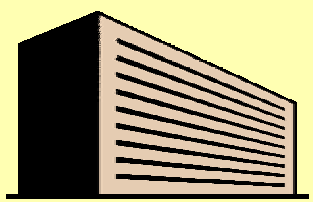
改善勧告



各府省庁
- 政府機関統一基準に基づき、省庁対策基準の見直し

策定・導入 → 運用 → 評価 → 見直し

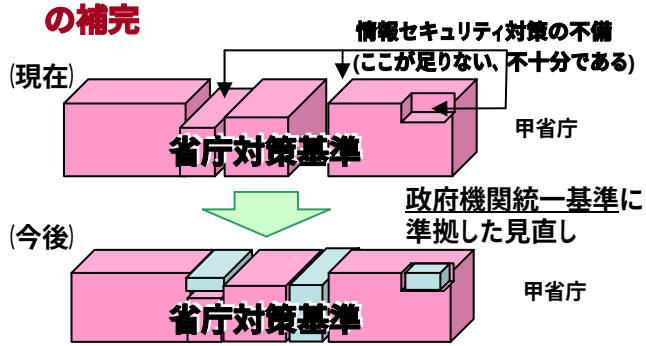
策定・導入 → 運用 → 評価 → 見直し



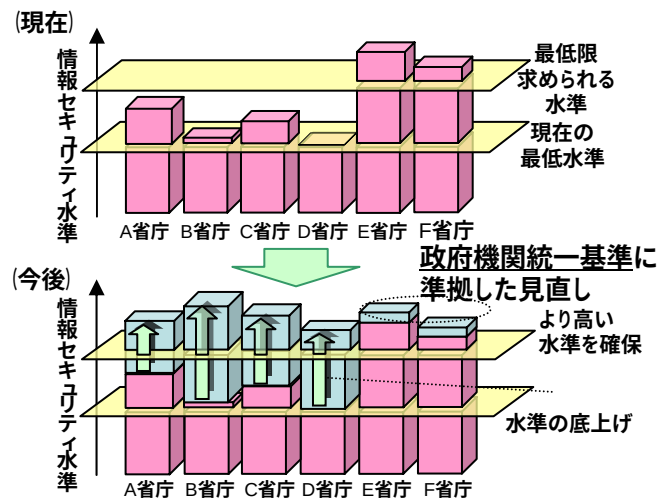
内閣官房 情報セキュリティセンター（NISC）

対策実施状況の検査・評価
NISCが各府省庁の対策実施状況を検査・評価し、その結果を情報セキュリティ政策会議が改善を勧告する。

① 政府機関統一基準による省庁対策基準の補完



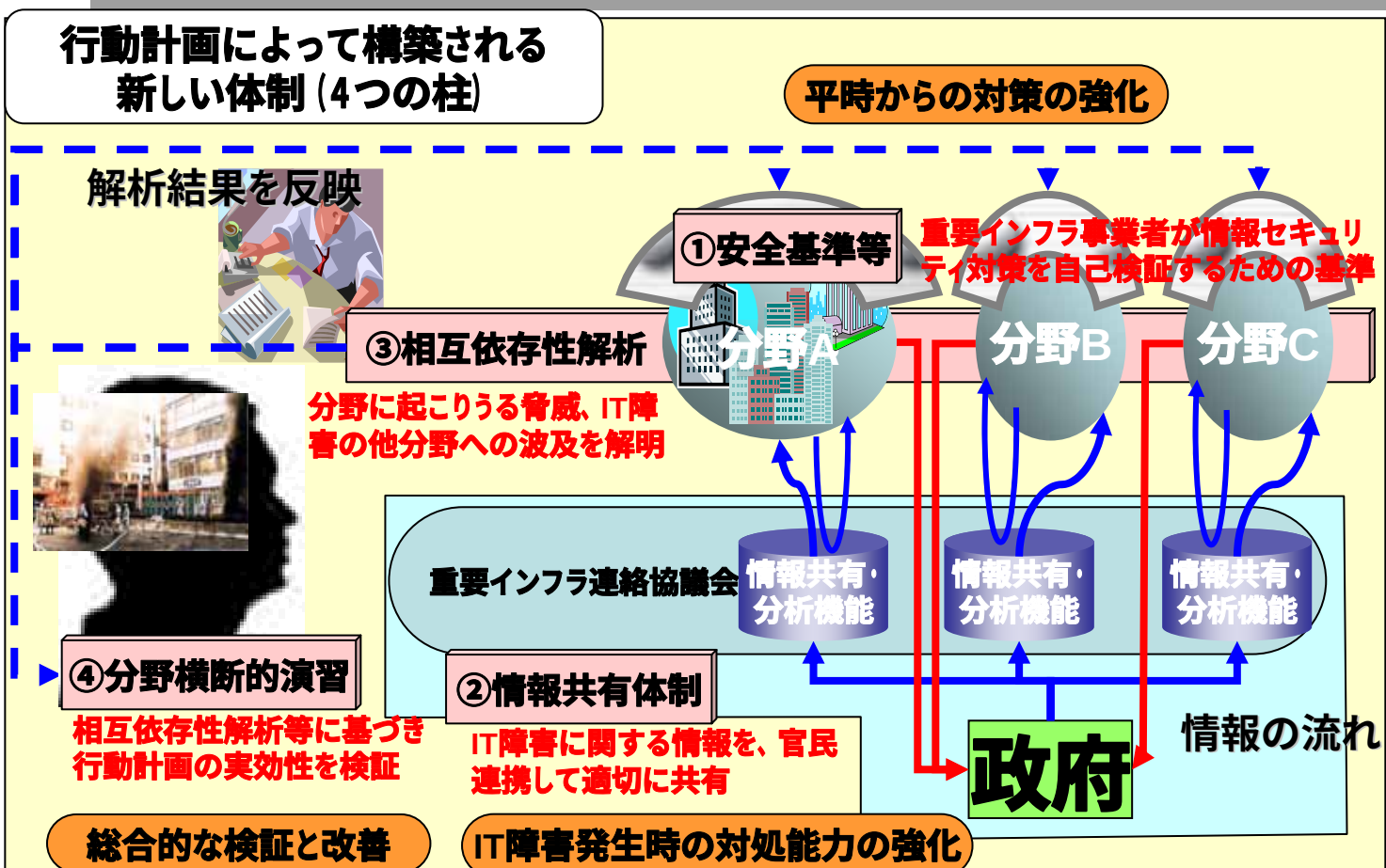
② 各府省庁の情報セキュリティ水準の向上



「重要インフラ行動計画」（個別設計図②）

○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）

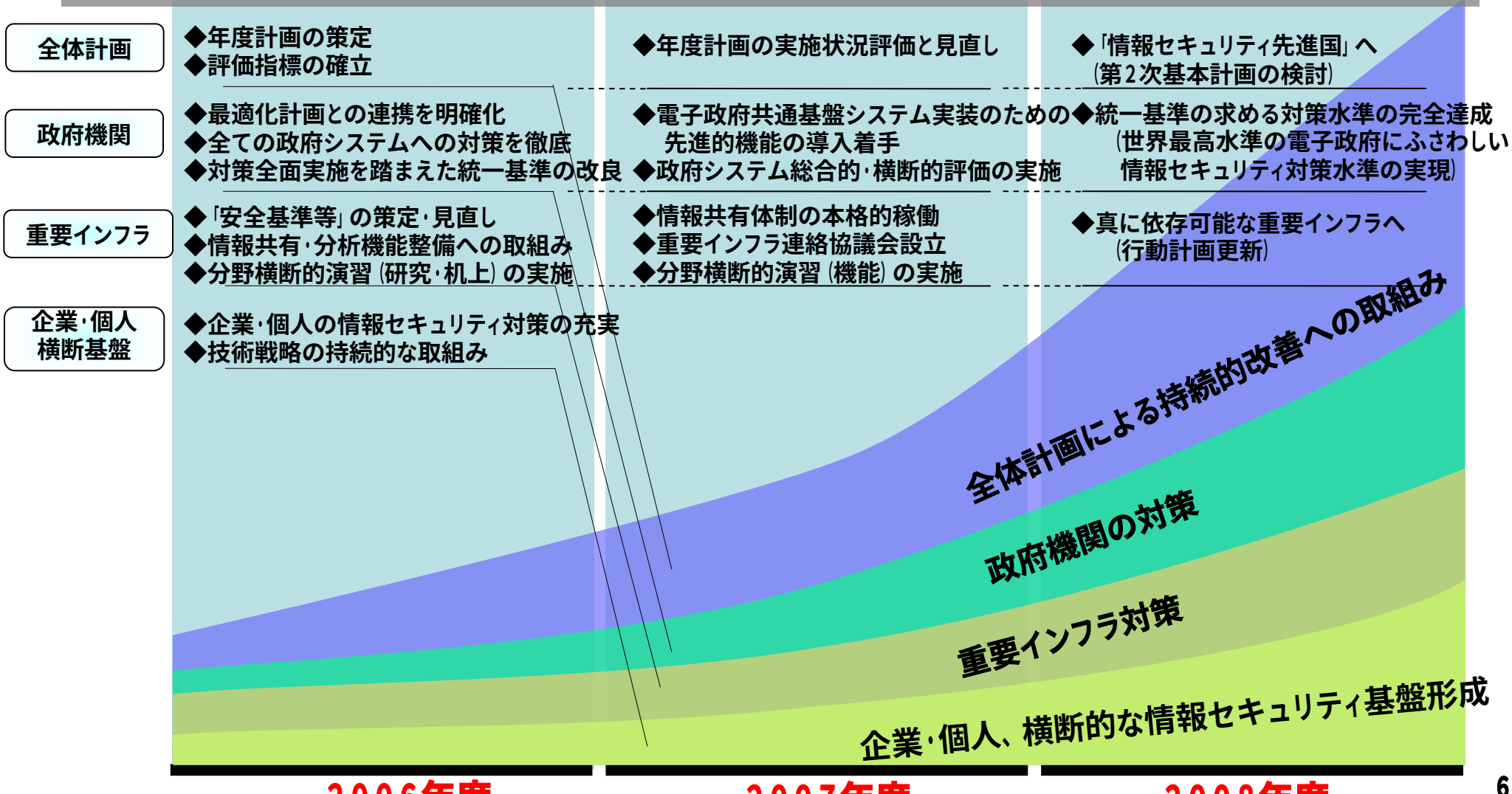
③相互依存性解析
2006年度　内閣官房にて試行を開始

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

今後3年間のマイルストーン全体像

○「全体工程表」（基本計画）と「個別詳細設計図」を組み合わせ、毎年度のマイルストーンを明確にしながら、「情報セキュリティ先進国」への進展を目指す。



(参考1) 情報セキュリティに係る事故・事件の事例 (報道ベース)

	政府・地方公共団体	重要インフラ	企業・個人
情報システムの停止等	○公開されたホームページが改ざんされた。(複数) ○ホームページが集中的なアクセスを受け閲覧しにくくなった。(2005.2等)	○空港の電源設備に障害が発生したことにより、レーダー施設等の航空管制施設がダウンし、管制機能が麻痺(2005.8) ○鉄道会社のインターネット予約サービスに係るサイトが、ドメイン名失効(更新手続き漏れ)によりアクセス不能となる(2005.9) ○制御システムがあるビルの電源断により、金融機関の全国のATMが利用不能となる(2005.9) ○プログラムミスにより、一部のATMにおいて他行送金ができなくなる(2005.10) ○証券取引所の株式等の取引を扱うシステムで障害が発生し、株式等の取引が行えなかった。(2005.11)	○ウィルス対策ソフトの更新ファイルの不具合により多数の情報システムに影響が発生した。(2005.4) ○情報提供サービス関連企業の重要な基盤をなすホームページサーバがネットワークを通じて攻撃されたため、一時閉鎖を余儀なくされた。(2005.5) ○公開サーバに対して、閲覧者をウイルス感染させる意図の改ざんがなされた(2005.5) ○クレジットカード関連企業の重要な基盤をなすホームページサーバがネットワークを通じて攻撃されたため、一時閉鎖を余儀なくされた。(2005.6)
情報漏えい等	○コンピュータの盗難によりデータを紛失した(複数) ○コンピュータウイルスによるWinnyネットワークを介しての情報漏洩(複数)	○コンピュータウイルスによるWinnyネットワークを介しての情報漏洩(複数)	○コンピュータ等の盗難・紛失によるデータの紛失(複数) ○不正プログラムが入ったメールを、顧客を装って送りつけ、それを利用させることで、金融機関等に係る情報を窃取、インターネットバンキング利用者の預金が不正に引き出された(2005.7) ○不正プログラムが入ったCDを、金融機関を騙って送りつけ、それを利用させることで、金融機関等にかかる情報が盗まれた。(2005.10) ○コンピュータウイルスによるWinnyネットワークを介しての情報漏洩(複数) ○カード等情報窃取を目的に、国内銀行を騙ったフィッシングメールが送付される(2005.7) ○インターネットを介して利用者の意図せぬ不正プログラムをインストールされ、口座等に係る情報を窃取、インターネットバンキング利用者の預金が不正に引き出された(2005.7)

(参考2) 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) について

- 「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。**