政府機関と重要インフラの情報セキュリティ対策のあり方

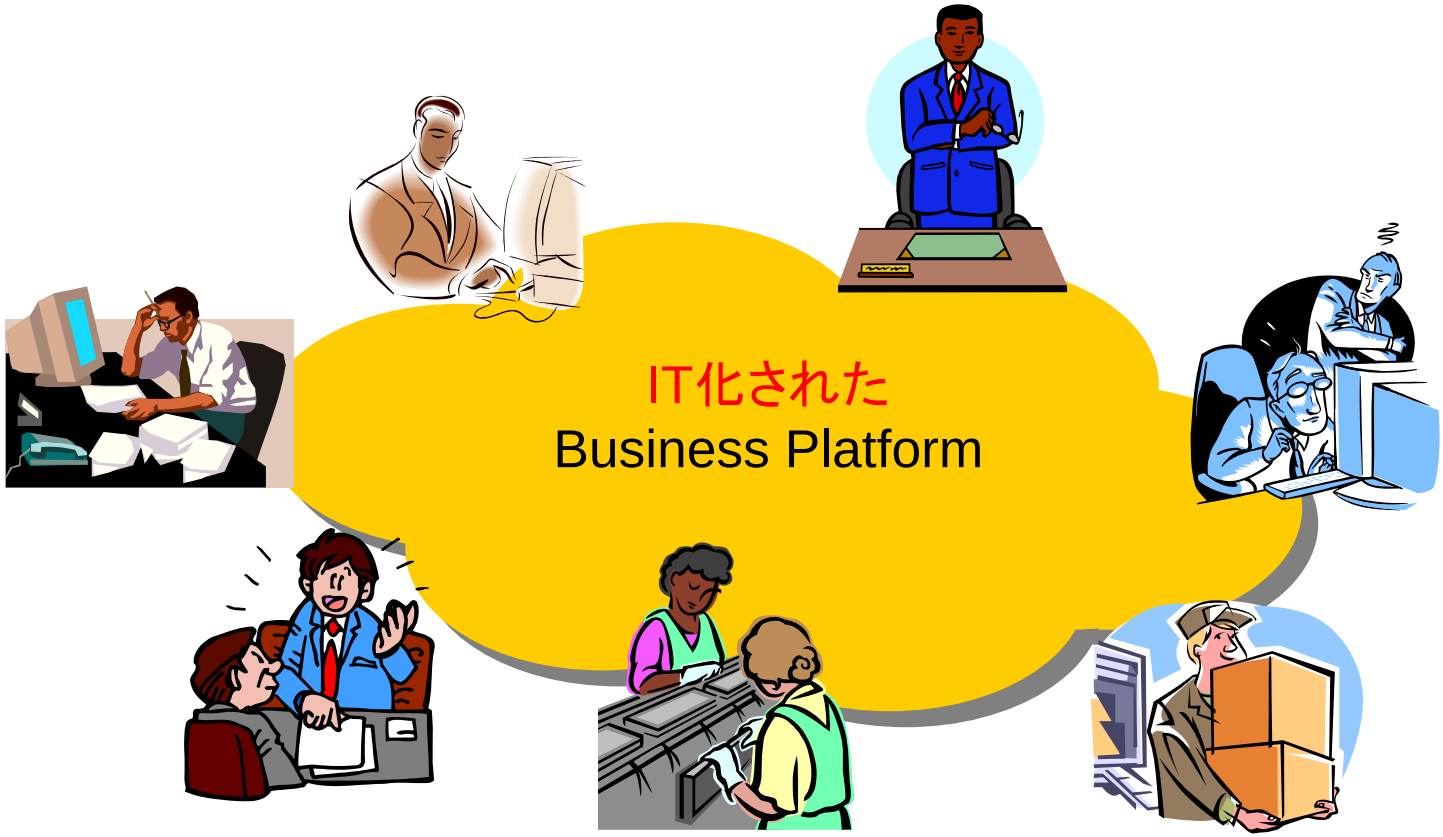
山口　英
情報セキュリティ補佐官
内閣官房情報セキュリティセンター (NISC)

概要

- 情報セキュリティ対策のありかた
- 政府の取組み
- 重要インフラ防護（CIP）と情報セキュリティ

1. 情報セキュリティ対策のあり方

なぜ情報セキュリティ管理は必要なのか



Think one day without Computers and Networks

ありとあらゆる作業はコンピュータとネットワークに依存している

システムと人間系の不協和音の解消

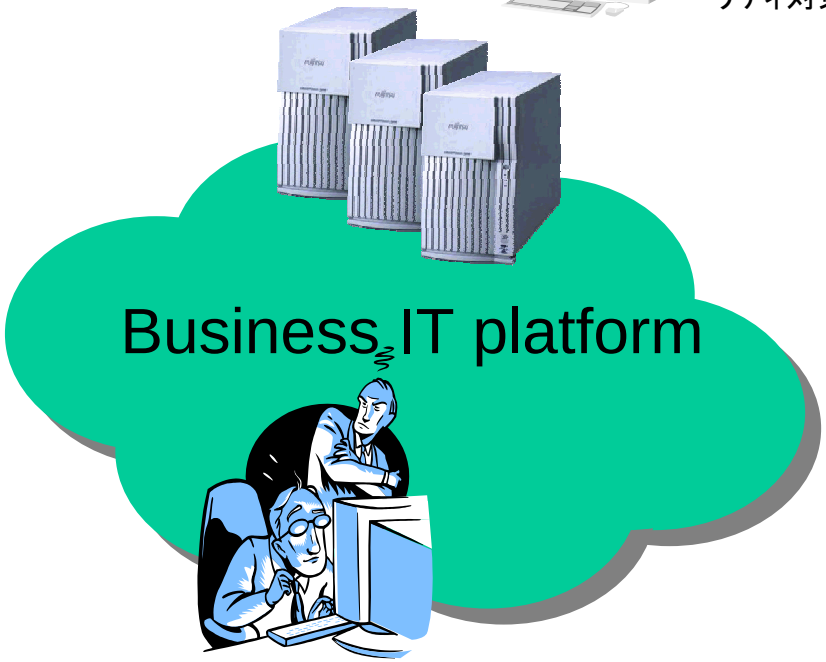
（1）急速なシステム依存の拡大
（2）人材不足に直面、素人運用拡大へ
（3）雇用の弾力化と統治機構の弱体化
（4）実効性の高い取り組みの模索
（5）実感できる「安全」

業務依存性拡大

企業・各種組織における本業での、情報通信サービス、情報処理サービスへの依存度拡大。まさに「システム止まれば売り上げこける」の状態。事業継続性確保の視点からの情報セキュリティ対策のニーズ拡大

攻撃手法・対象の変化

BOTnet等の登場により、攻撃手法が急速に高度化することによって、実害が発生する事態が拡大。民間のオンラインサービスも攻撃対象に。まさに、自分たちのビジネス・プラットフォームがねらわれ出した



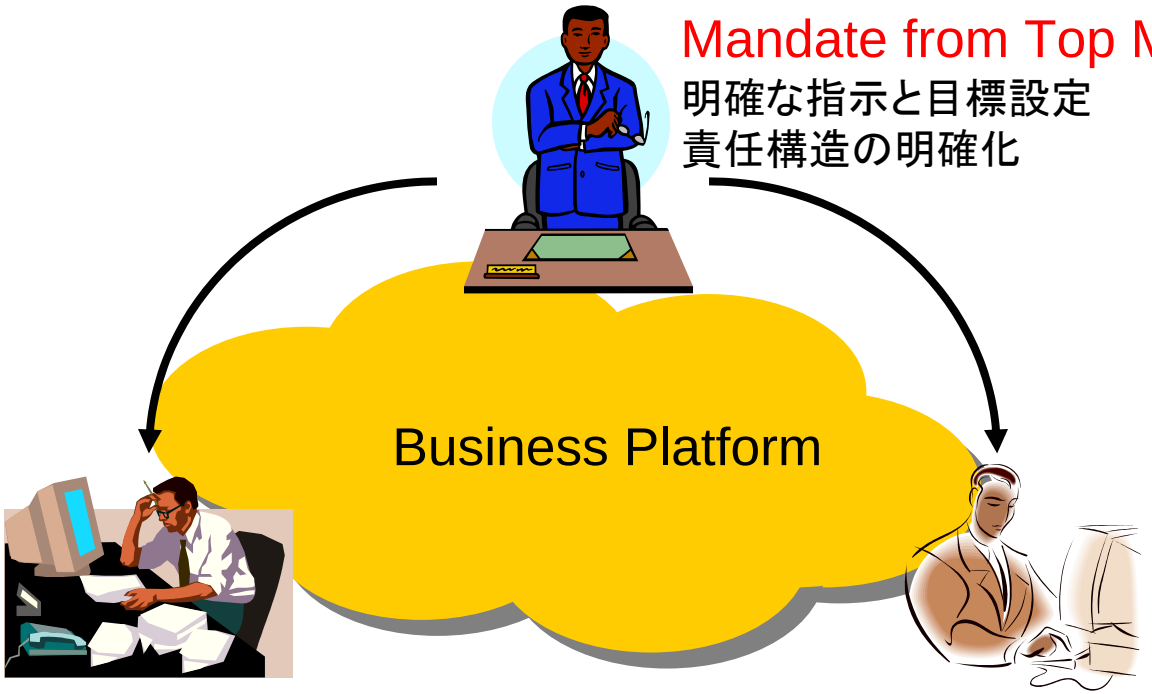
高度IT人材不足

情報システムの高度化、情報セキュリティ対策の推進、事業継続性確保について、取り組み不十分。取り扱う情報に見合う人材が不足

組織内部構造の変化

雇用環境の変化に、組織内での統治構造が対応しきれてなく、結果として情報漏洩などのリスクが高まる

セキュリティ対策推進のありかた（1）



Mandate from Top Management

明確な指示と目標設定
責任構造の明確化

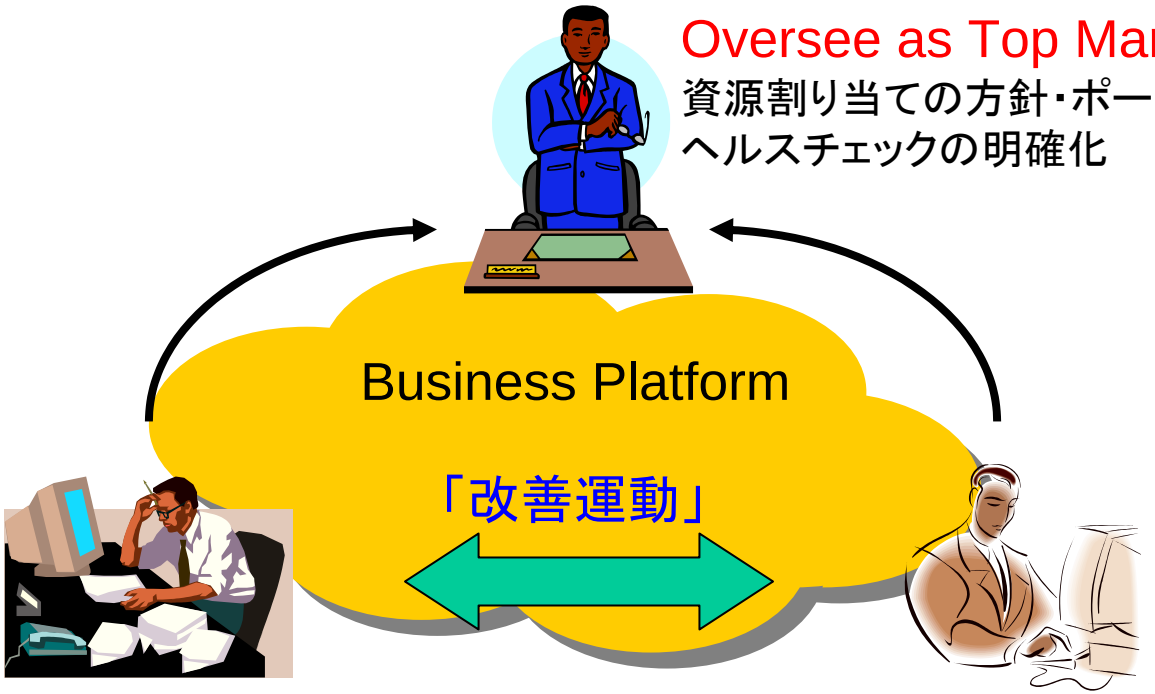
Business Development & Operation

情報通信システム基盤への依存
情報力の活用
利益率の最大化

IT Security Expert

情報通信システム基盤構築と運用
カスタマの満足度向上
リスク低減への飽くなき挑戦

セキュリティ対策推進のありかた（2）

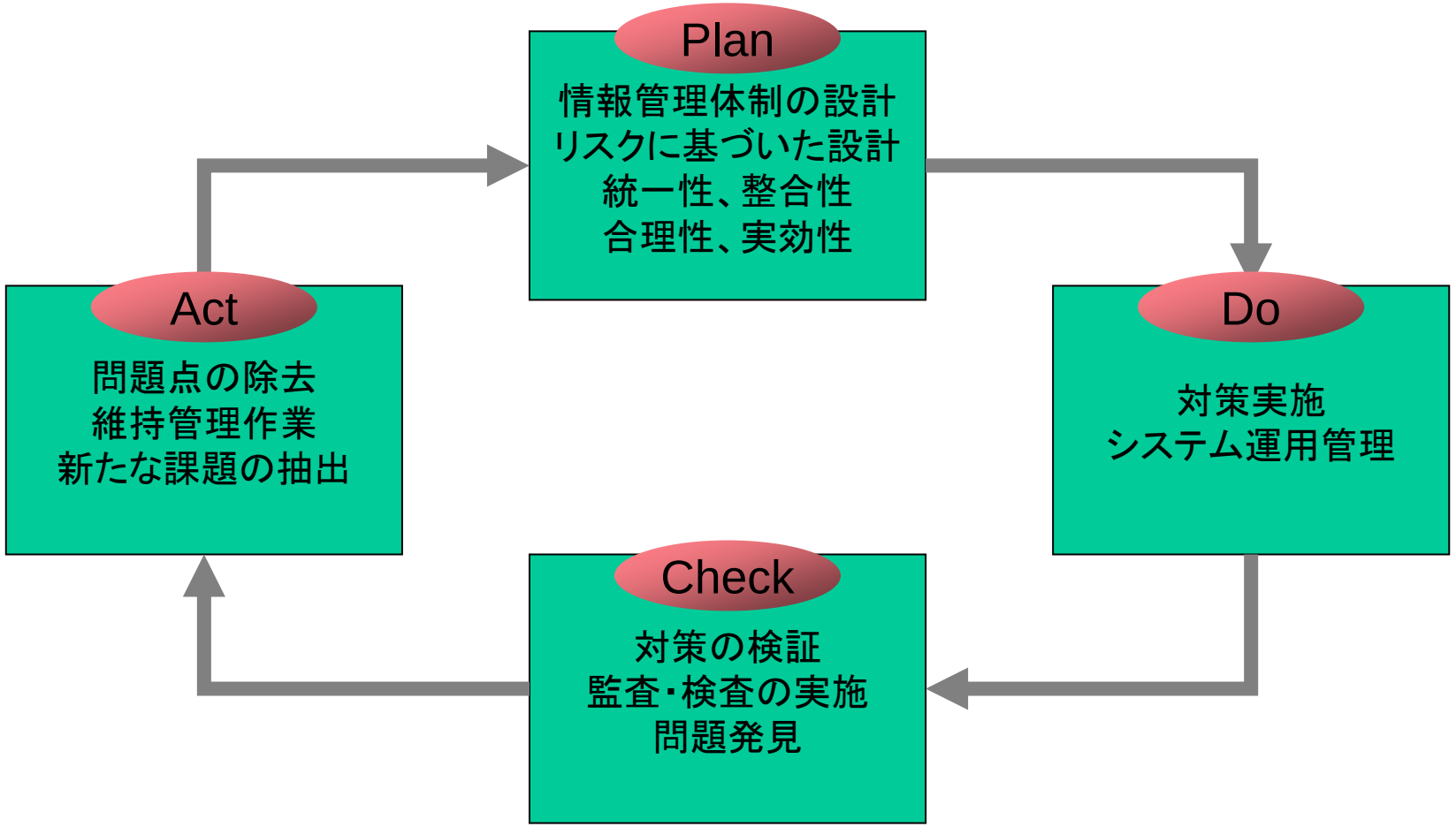


Oversee as Top Management
資源割り当ての方針・ポートフォリオ管理
ヘルスチェックの明確化

Business Development & Operation
本当のカスタマ
本当の現場

IT Security Expert
道具を知り、使いこなす専門家
現場に対する直接コンサルタント

PDCAサイクル：合理性確保



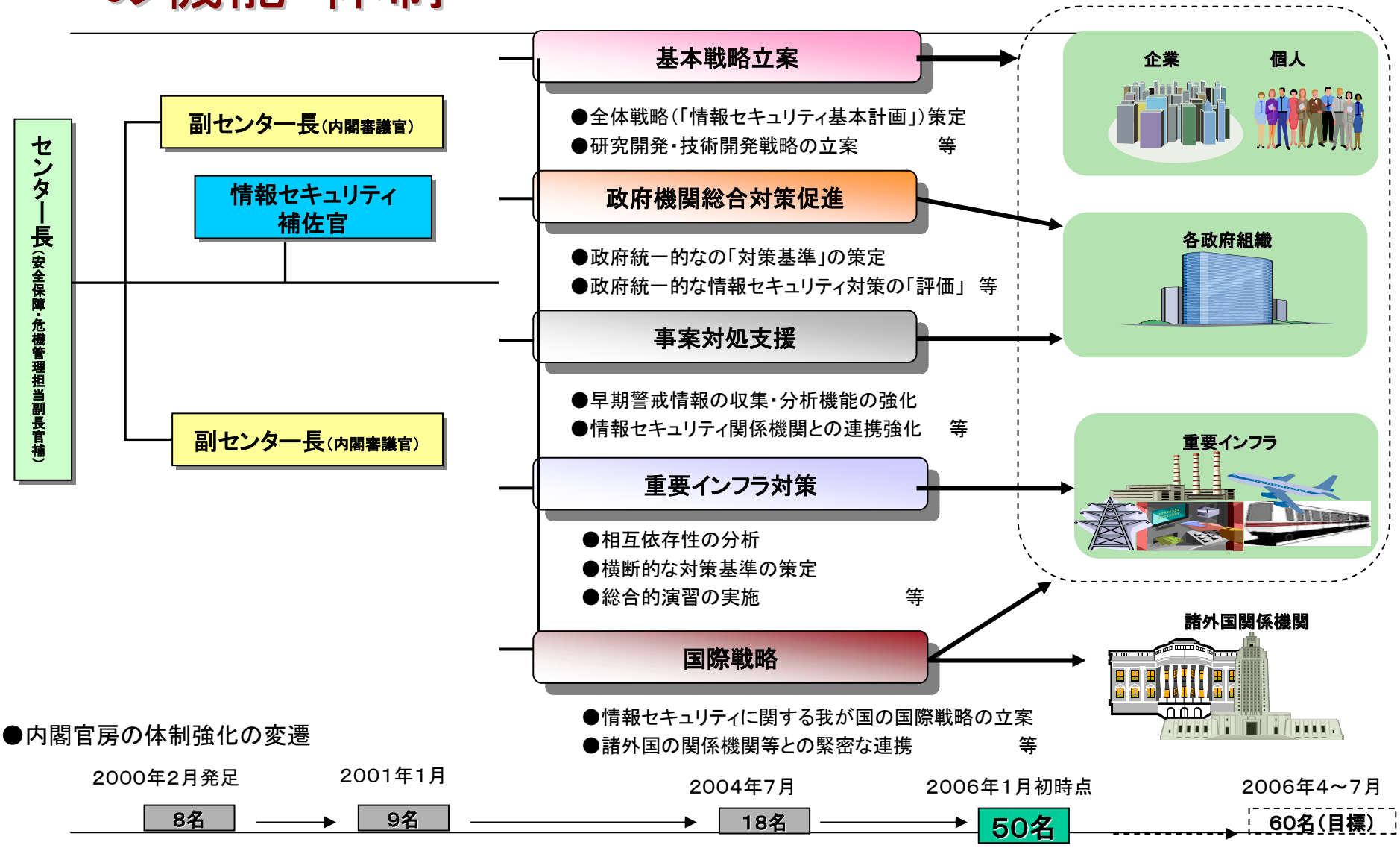
情報セキュリティの特質から “P” の弾力化必須
→新たな脅威が顕在化する時は予見できない

2. 情報セキュリティ政策の概要と推進体制

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）

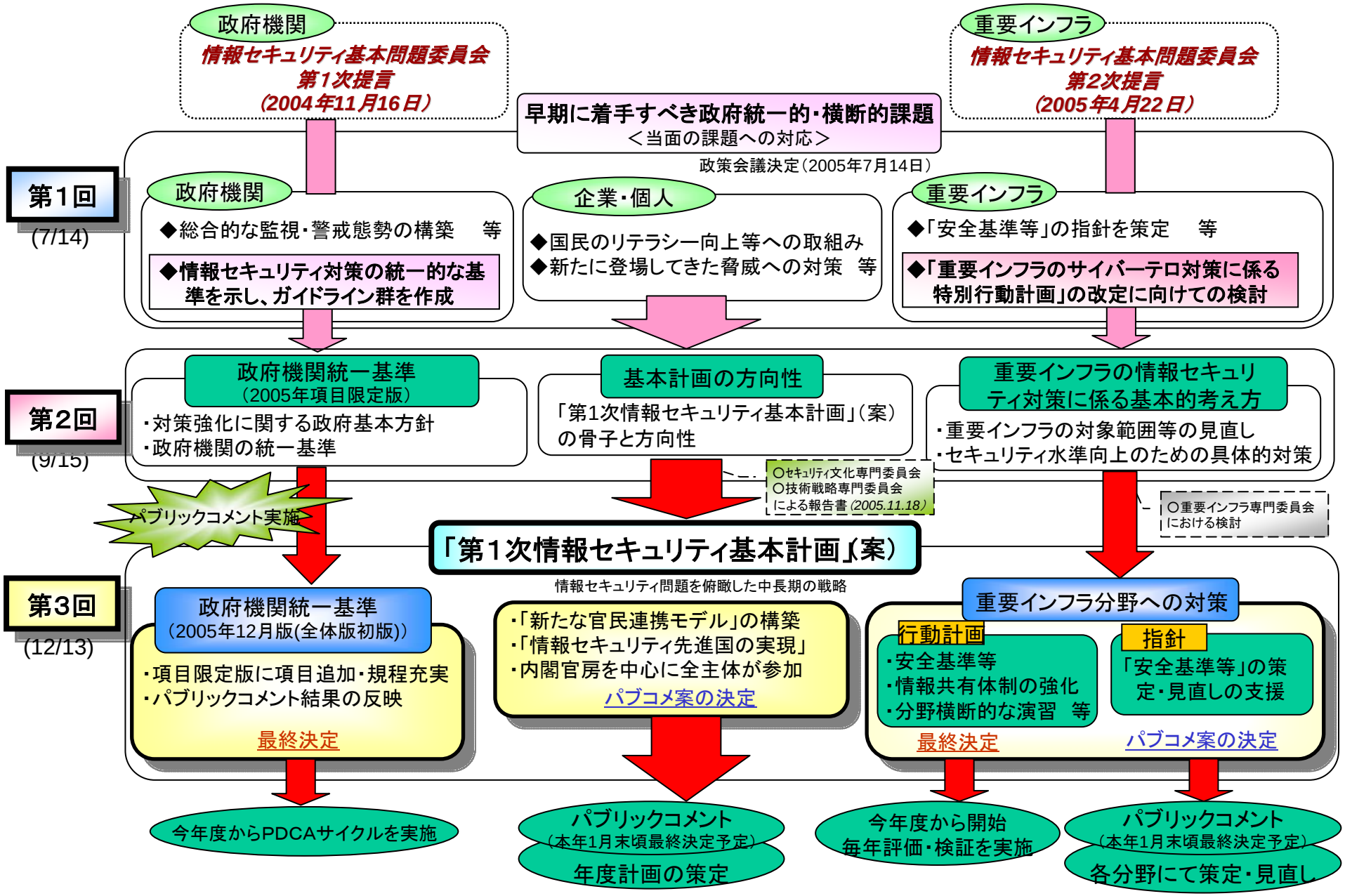
- 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（2004年12月7日IT戦略本部決定）を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備中。
  - **2005年4月25日、内閣官房情報セキュリティセンター（NISC；National Information Security Center）を設置。**
  - **2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」を設置。**

内閣官房情報セキュリティセンター（NISC）の機能・体制



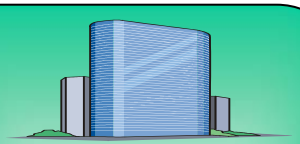
●内閣官房の体制強化の変遷

情報セキュリティ政策会議の議題全体像（第1回～第3回）



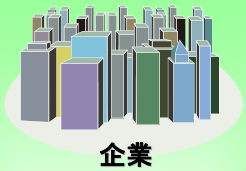
第1次情報セキュリティ基本計画（案）－今後3年間の重点政策－

○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

	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

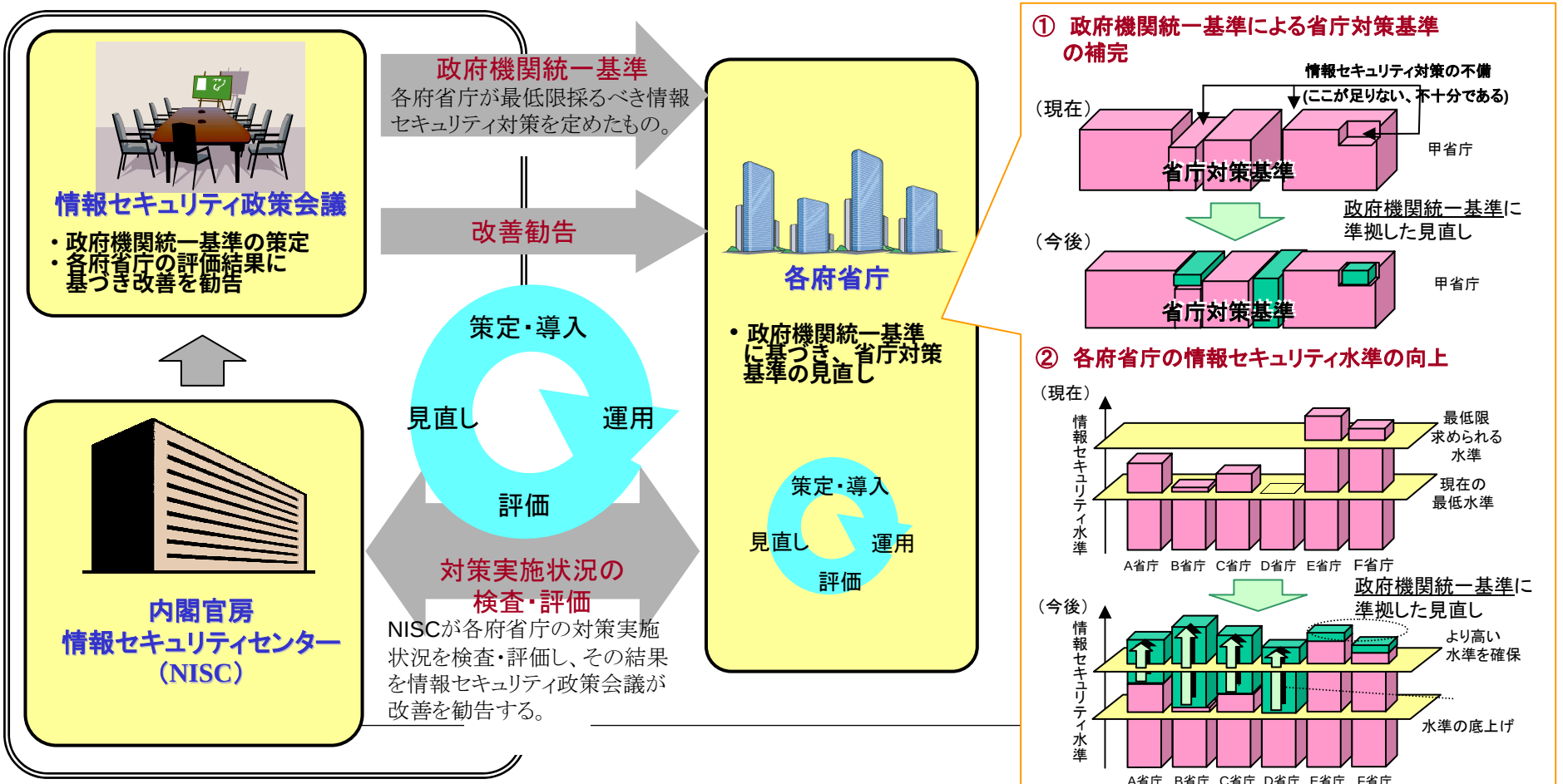
犯罪の取締り、権利利益の保護救済

◆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。

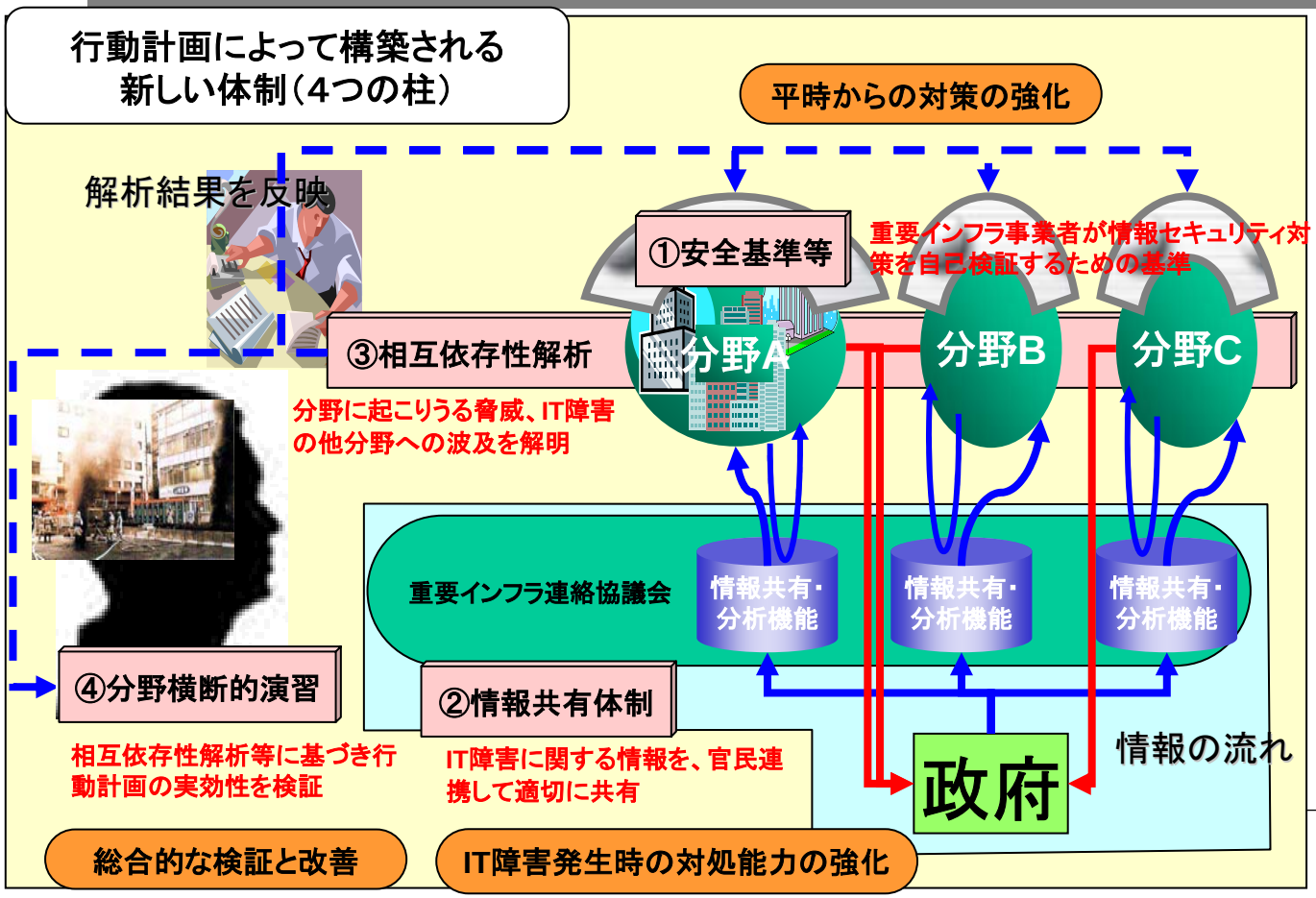
○各政府機関は本基準を踏まえて対策を実施し、内閣官房情報セキュリティセンター（NISC）が対策実施状況を検査・評価。その結果に基づき、情報セキュリティ政策会議が改善を勧告。



「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

3. 重要インフラ防護（CIP）と情報セキュリティ管理

（読売新聞：2002年4月3日報道写真）

重要インフラに関するこれまでの主な取組み

- 2000年12月
  - 『重要インフラのサイバーテロ対策に係る特別行動計画』
    - 対象とする重要インフラ分野の規定
    - 官民におけるサイバーテロ対策の5つの柱を規定
    - 定期的な行動計画の見直しを宣言
- 2001年10月
  - 『サイバーテロ対策に係る官民の連絡・連携体制について』
    - 官民の連絡体制、連絡対象、手段、対応措置、情報の取り扱いに関する基本的な考え方を策定
- 2002年3月
  - 『「重要インフラのサイバーテロ対策に係る特別行動計画」のフォローアップについて』
    - 官民における取組みの進捗状況調査の取りまとめ
    - 取組みの強化に向けた検討課題の抽出
- 2002年11月
  - 『「重要インフラのサイバーテロ対策に係る特別行動計画」に基づく取組みの推進について』
    - 重点的に取組みを行うべき事業者の範囲を当面絞り込む
    - 重要インフラにおける情報システムの現状評価
    - 検討課題への具体的方策として次の三点を推進
      - 重要インフラの情報システムに関する現状把握・検証
      - 民間重要インフラ事業者等におけるサイバーテロ対策状況の把握
      - 民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

これまでの重要インフラの保護に関する官民の取組みは、サイバーテロ対策に係る基本的な連絡・連携体制等の構築に主眼が置かれてきた。重要インフラを取り巻くその後の環境変化の下では、これまで焦点をあててきたサイバー攻撃に加え、それ以外のリスクも含めた「IT障害」に関わるリスクは増大してきているのではないか。

重要インフラにおける情報セキュリティ対策の重要性

重要インフラを巡る最近のIT障害の事例（報道ベース）

サイバー攻撃	非意図的要因（人為的ミス）等
・豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が、未処理の汚水100万リットルを河川および沿岸部に流し込んだ(2000年3月) ・SQL slammerワームが猛威を振るい、韓国では一時インターネットに障害が発生(2003年1月) ・米オハイオ州原子力発電所内のシステムにSQL slammerワームが侵入し、安全システムの一部及びプラント制御システムがダウン(2003年1月) ・米鉄道の信号システムがコンピュータウイルスに感染、ワシントン周辺3路線で列車が停止したりダイヤが乱れるなどした(2003年8月)	・大手銀行の合併に伴うシステム統合において、口座振替の未処理など大規模なシステム障害が発生、復旧に時間を要した(2002年4月) ・インターネットバンキングのサービスがデータベースサーバの障害により全面的にダウン(2003年5月) ・飛行計画情報処理システムがプログラムミスによりダウンし、200便近くが遅れるなど、航空ダイヤが全国的に混乱 (2003年3月) ・注文件数の増加により証券取引所の売買システムや株価情報システムの処理が遅延(2003年7月) ・通信制御プログラムの不具合が原因で、金融機関同士のATMをネットワークで結ぶ「統合ATMスイッチングサービス」に障害発生。全国約20の金融機関のATMで他行カードを利用した取引が不可に(2004年1月) ・航空路レーダー処理システムのトラブルでメインシステムを停止、国内便約130便に影響(2004年4月) ・ジャスダック証券取引所システムが設定ミス、プログラム不具合により停止し、取引が停止(2005年2月、4月、8月)

●重要インフラのサービス継続に対する情報セキュリティ上の脅威は、**サイバー攻撃に加えて、人為的ミスなどの非意図的要因や自然災害まで拡大**（上記表参照）。

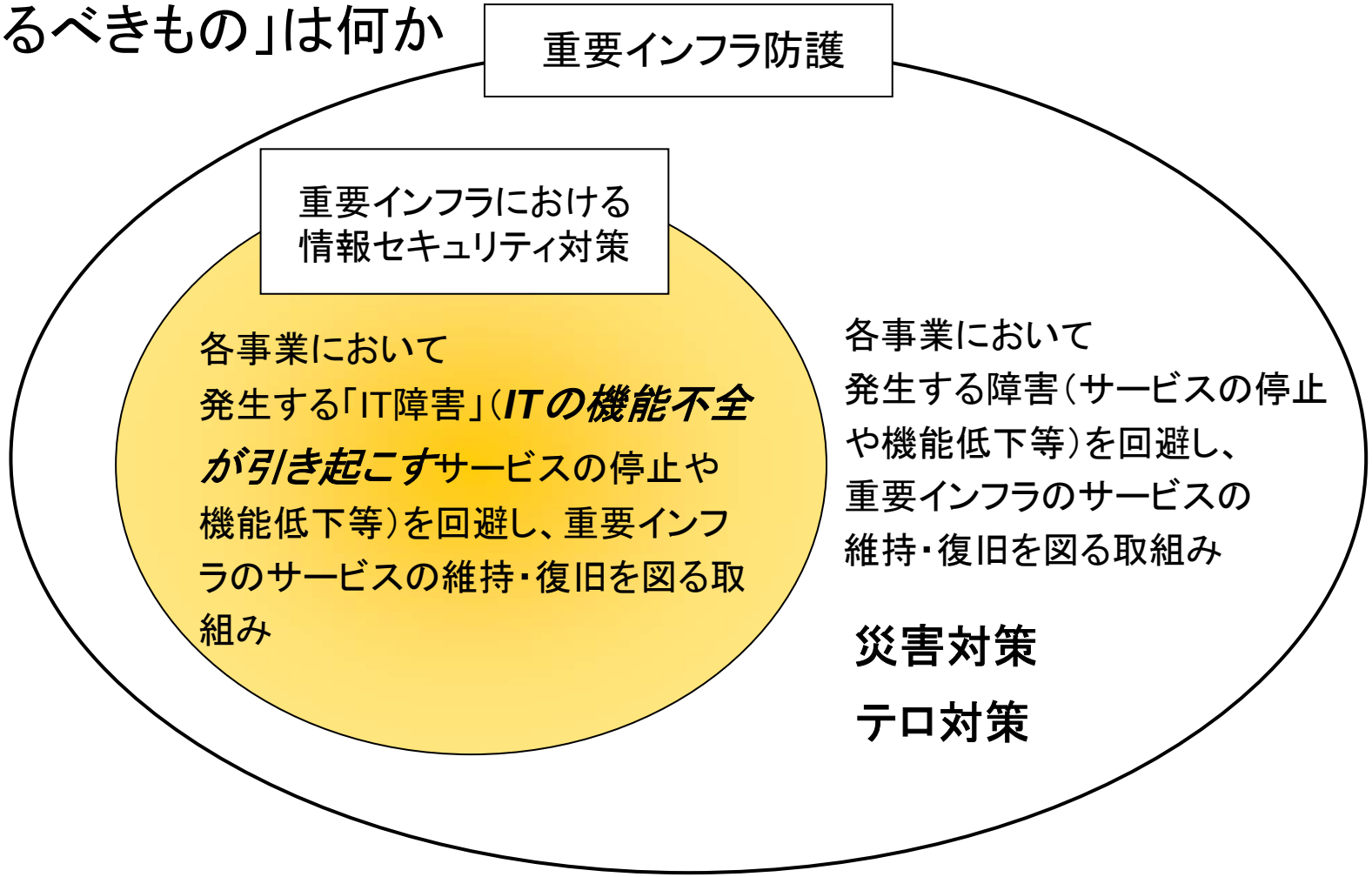
●重要インフラでは、サービス提供そのものに直接関係するシステム（**制御系システム**）及びサービス提供を側面的に支えるシステム（**情報系システム**）**の両者において、ITが年々多用**されるとともに、大規模化・複雑化。

●こうした中、**「IT障害」(※)が重要インフラのサービス停止・機能低下等に直結するリスクはもはや放置できない状況**であり、**情報セキュリティ対策の充実が必須**の課題。

（※）「IT障害」とは、重要インフラの各事業において発生する障害（サービスの停止や機能の低下等）のうち、ITの機能不全が引き起こす障害を指す用語として新たに定義。

重要インフラ防護における情報セキュリティ対策の位置づけ

「護るべきもの」は何か



問題の本質（1）

- 各事業者が持つ情報が開示されない
  - 各事業者は民間事業者（多くの場合株式会社）
  - 各事業が持つ脆弱性は、そのまま事業の脆弱性として認知
  - 脆弱性の存在を開かす経営者はいない
    - 株主に対して不利益を与える可能性がある
    - 脆弱性の存在を認知したら、当然対処しなければならない。このため、脆弱性が顕在化することはさける
    - 結局、情報は隠蔽され、開示されることはない
  - 各事業でどのようなシステムを用いているかについての情報も開示されにくい
    - 事業運営上の秘密（企業秘密）として取り扱われる
    - 結果として、どのようなシステムなのかも分からない
    - 参考）政府によるインベントリー (inventory) 作成がうまくできた例は英国NISCC (National Infrastructure Security Coordination Centre) のケースぐらいではないか…

問題の本質（2）

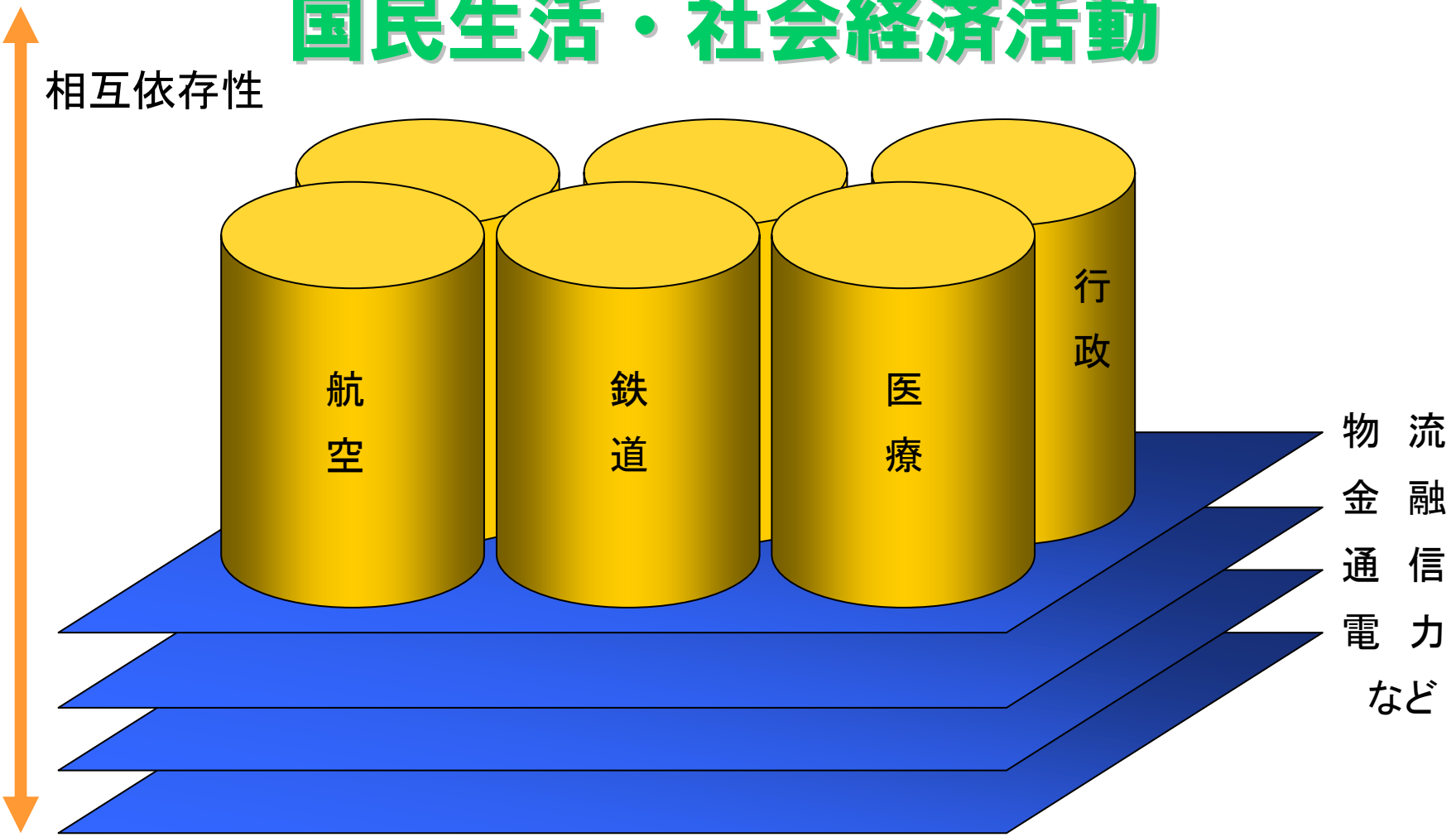
- 行政は、何でもできるわけではない
  - 重要インフラ事業の多くは認可事業である
    - 主管官庁・監督官庁が存在する
    - 監督官庁には、現状を把握する情報が集まる
  - 自由化と競争性確保が重要
    - もちろん、分野を比較すると格差が存在するのは事実
    - 護送船団方式はもはやあり得ない
  - 自主保安の原則
    - 行政による保安基準の提示＝minimum requirementの提示
    - 事業者による自助努力
  - 「検査行政」、「勧告提示」
    - 行政は事業者に対する検査を行ったり、必要に応じて勧告を出したりする
    - 明確に定義された手続きに基づき実施

問題の本質（3）

- 重要インフラは相互に依存している
  - Inter-dependency
  - どれかが機能停止すると、直接・間接に影響が生じる
    - 特に、電力、情報通信、金融は影響範囲が大きい
    - 社会全体から見ても、この3分野への依存度は高い
  - 単独の重要インフラにおける障害対策だけでは、問題が解決しない
    - どのインフラの、どの機能に注力して対策を行うべきか
    - 相互依存性解析が必要
      - リスクアセスメントの対象拡大
      - 合理的な解析が不在
        - » 参考）米国では2003年から研究プロジェクトが開始されている。Sandia National Lab (www.sandia.gov)では電力領域での相互依存解析研究を実施 “Critical Infrastructure Surety” initiative

各重要インフラ間の関係（私案）

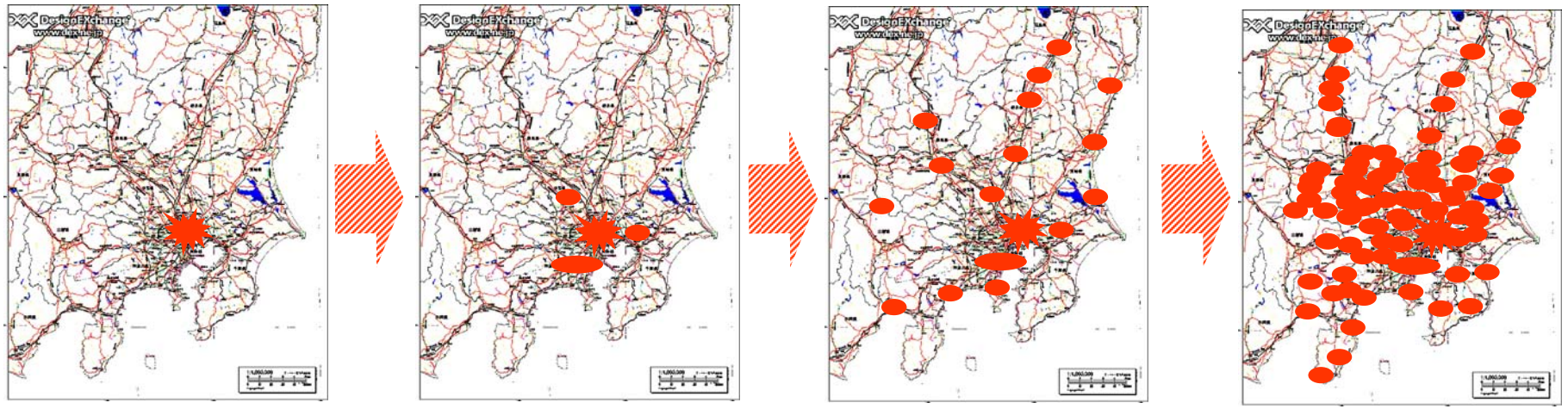
国民生活・社会経済活動



情報システムの脆弱性とそれが社会に及ぼす影響を俯瞰するツール

社会的なインシデント（大地震、テロリズム、自然災害等）が発生し、それらが情報システムに及ぼす影響をシミュレーションすることにより、情報システムの脆弱性とそれが社会に及ぼす影響を分析する

都市銀行の勘定系システムに致命的なインシデントが発生した際の時系列的被害の拡大の様子（シミュレーション）



インシデント発生

インシデント発生
1時間後

インシデント発生
12時間後

インシデント発生
24時間後

大きな影響が出ている地域

出典：JST社会技術
ミッションプログラムⅡ

問題の本質（4）

- 重要インフラが持つリスクについては、専門家しかわかり得ない状況になりつつある
  - 行政でも、その領域での問題を的確に把握するためには、専門知識を持った職員による解析が必須
  - 高い専門性が求められる

問題の本質（5）

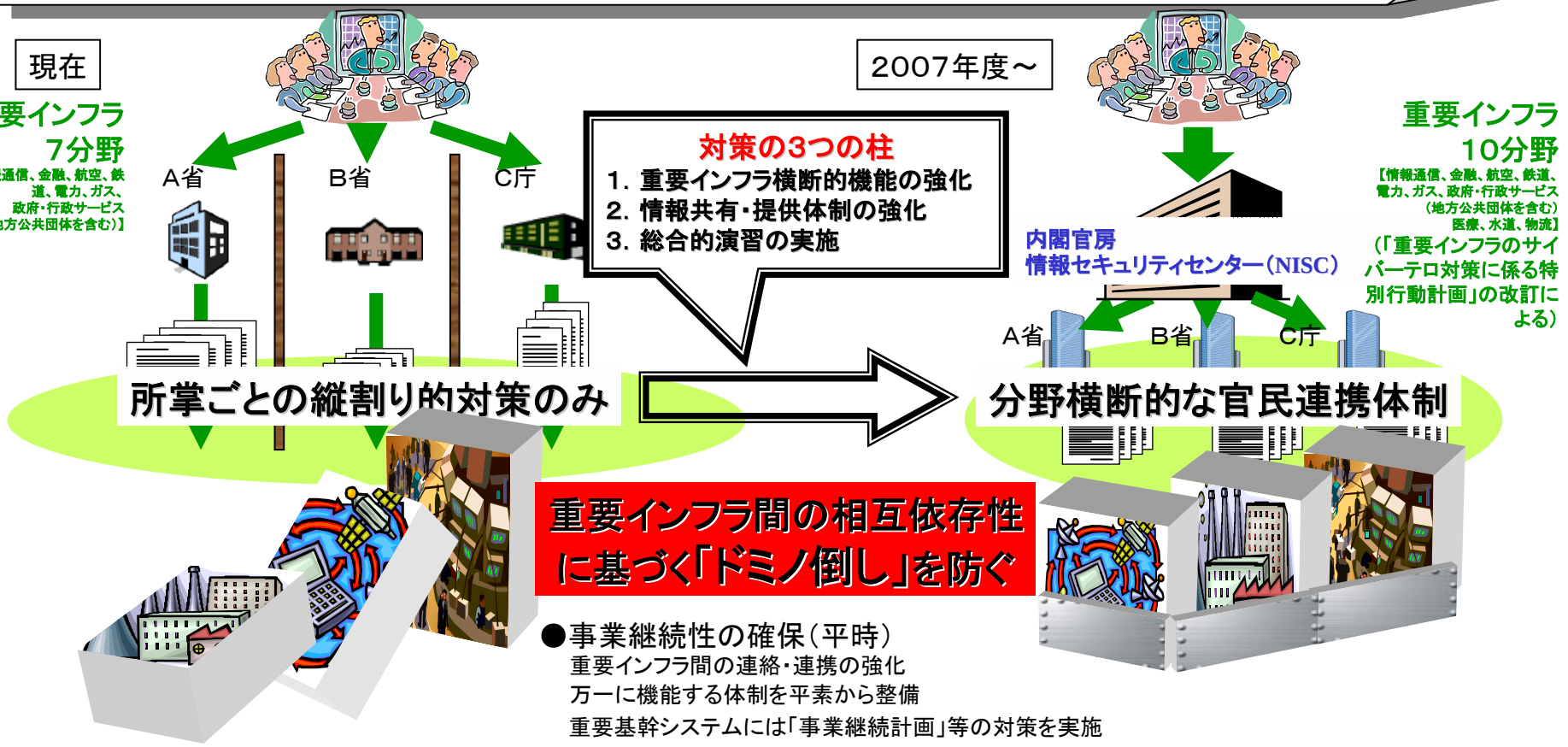
- 各分野で使われている技術は、実は似てきている
  - 過去には、各分野で使われている技術はバラバラで、かつ、一点物が多かった
  - コストダウン圧力により、汎用パッケージの利用が進む
  - 分野にかかわらず利用されているものも登場
    - たとえば、OS, middleware, 特定のパッケージ
    - 共通基盤として利用促進
    - 多くの場合、情報通信に関わる部分の共通化が進む

重要インフラにおける情報セキュリティ対策強化について

実際の事例

■サイバー攻撃により通信機能が停止した結果、株取引を含むインターネット上の金融取引が停止し、最大17億ドル（約2，100億円）の機会損失が発生 （平成12年2月：米国）

■中越地震による広域停電が小千谷市を含む地方行政ネットワークの機能停止を引き起こしたほか、非常発電用燃料供給の途絶から情報通信の障害、さらには物流機能が停止し、域内の生産活動や救急活動の停滞を招いた。（平成16年10月：新潟中越）



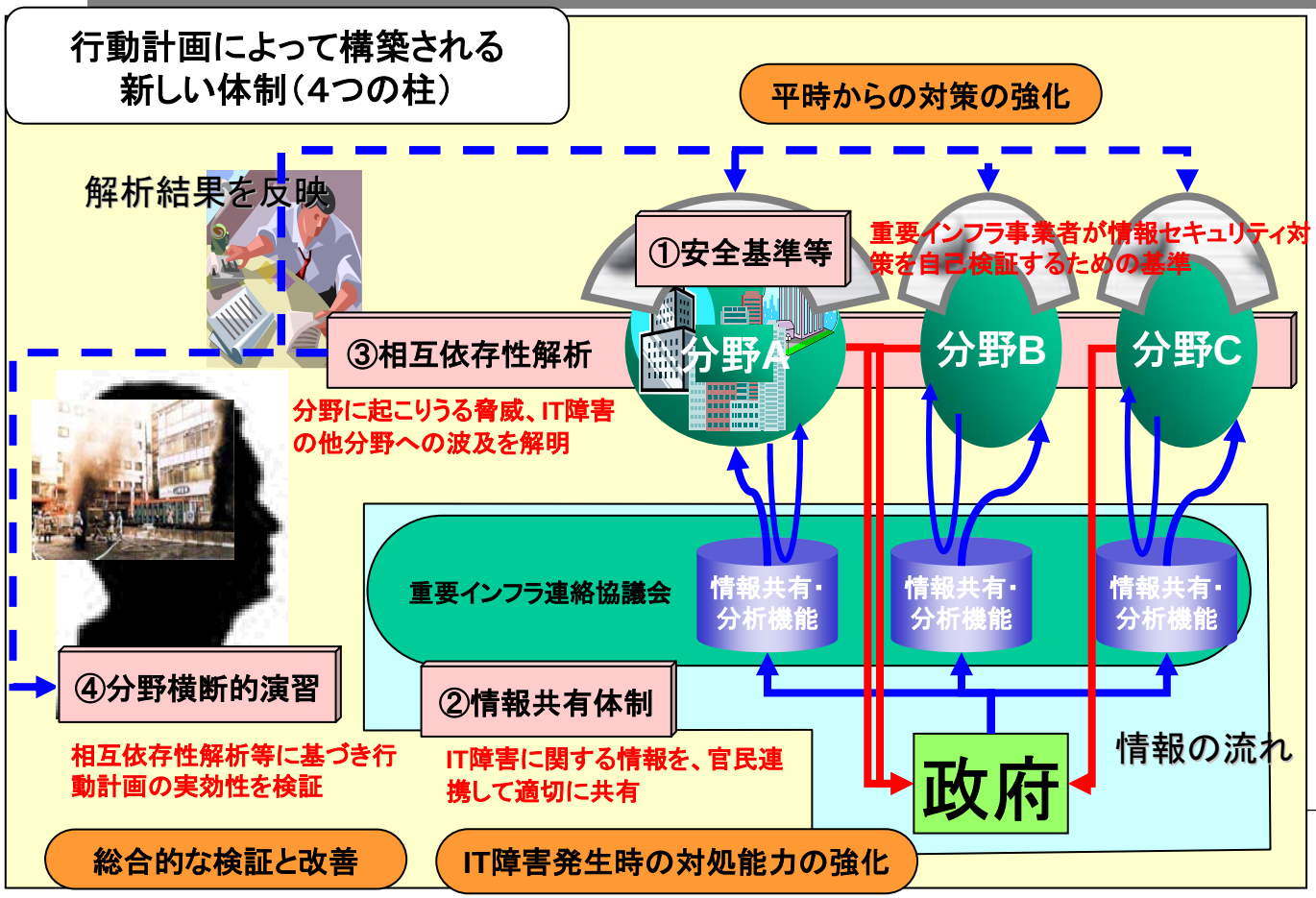
●事業継続性の確保（平時）
重要インフラ間の連絡・連携の強化
万一に機能する体制を平素から整備
重要基幹システムには「事業継続計画」等の対策を実施

●迅速な復旧の確保（障害時）
省庁間、事業者間の連携を通じた適切な優先順位付け

「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

More information

- http://www.bits.go.jp/

- 政府全体での情報セキュリティ政策についての情報
  - 第１次情報セキュリティ基本計画
  - 政府機関統一基準
  - 重要インフラにおける情報セキュリティ対策に係る行動計画
  - 会議における検討状況が分かる資料