重要インフラにおける
情報セキュリティ

平成18年3月23日

重要インフラ向け情報セキュリティセミナー

中央大学理工学部

土居範久

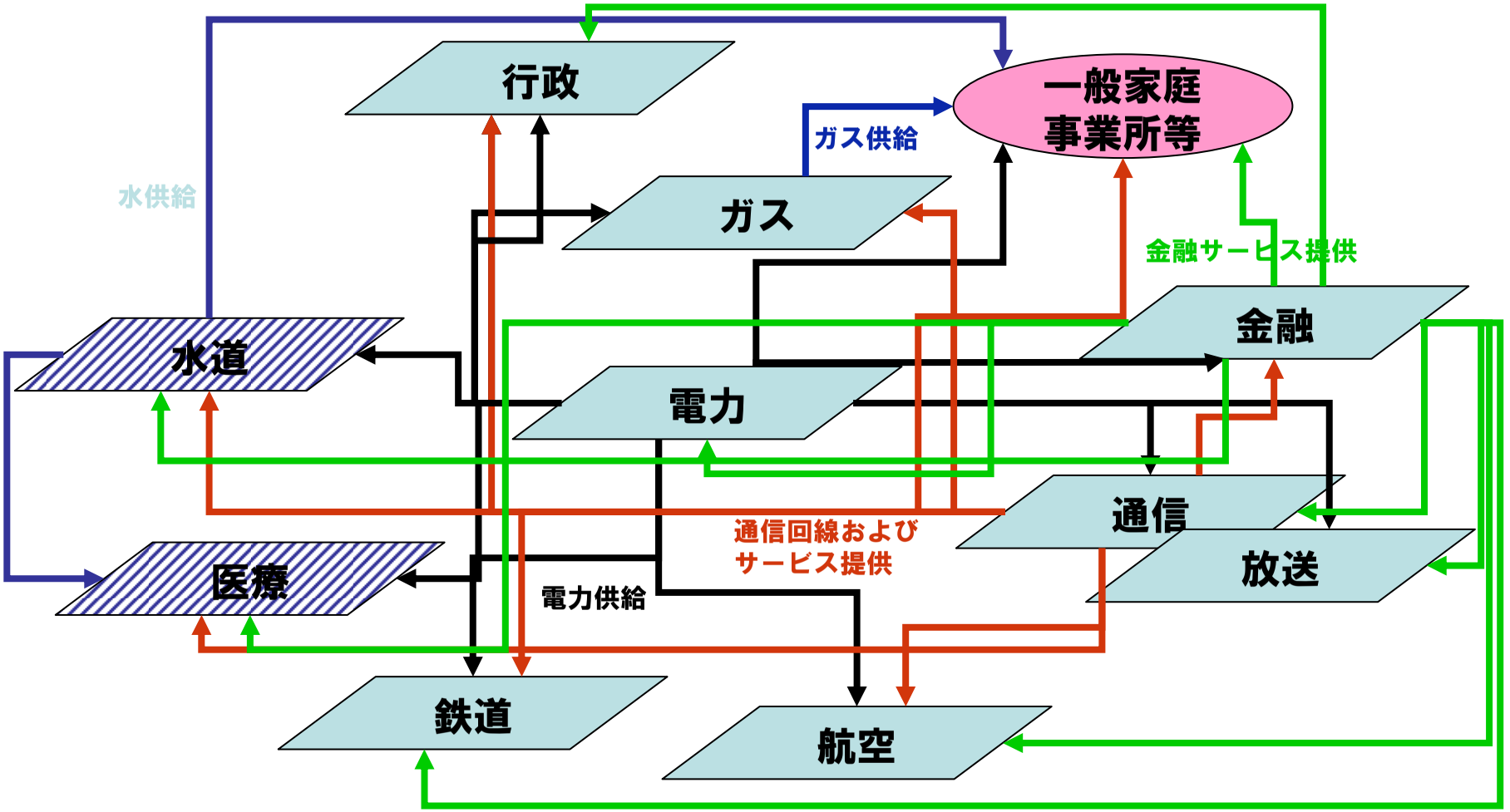
謝辞

資料を作成するにあたっては多くの方々の協力を得た．とりわけ，次の方々には貴重な資料をご提供頂いた：

山崎琢矢　内閣官房情報セキュリティセンター 参事官補佐
内閣官房情報セキュリティ対策推進室

わが国における重要インフラの相互依存性概観

－　ハザードマップ作成のベース　－

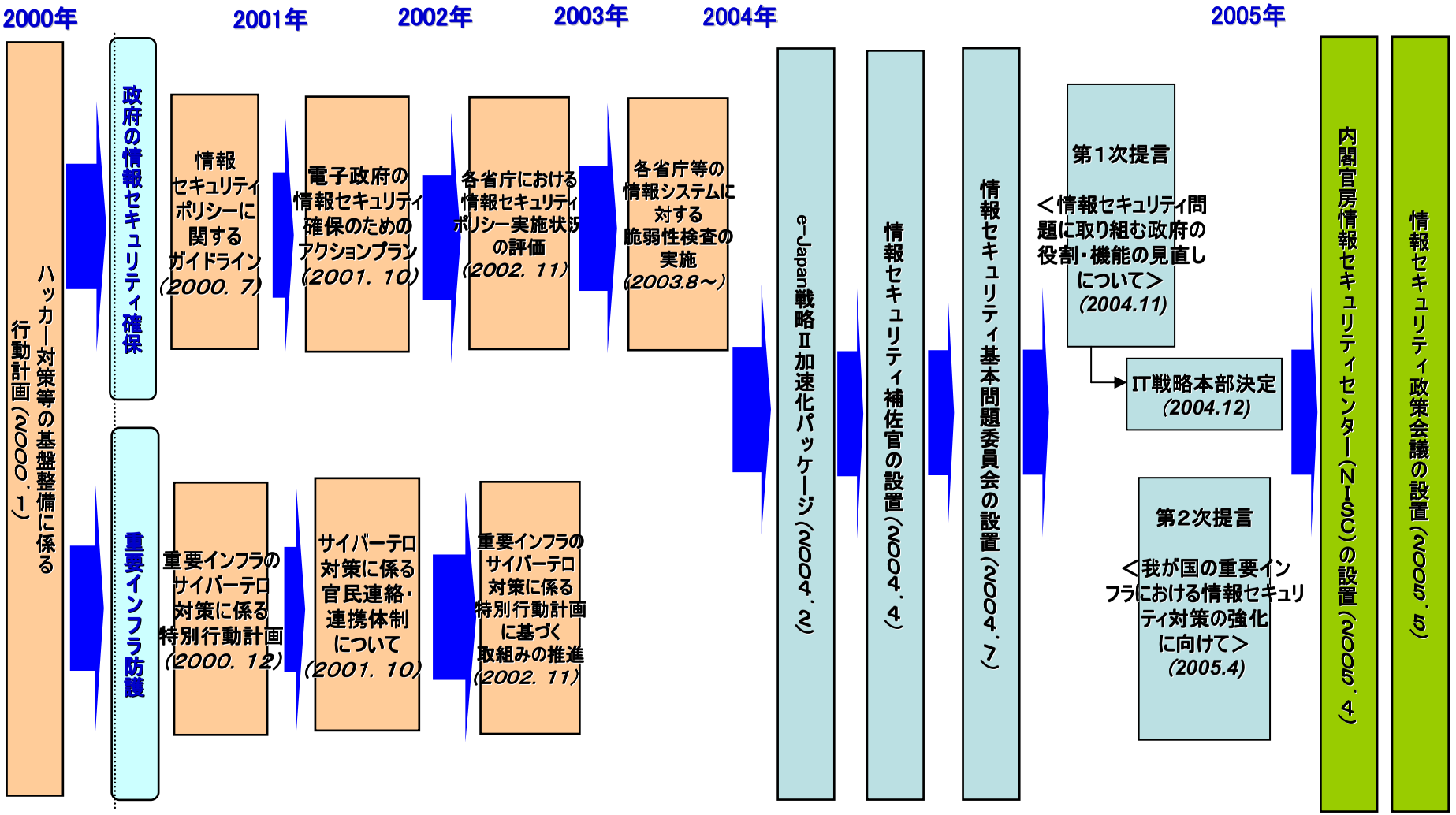


ristex「情報と社会」領域作成

内閣官房を中心とした情報セキュリティ政策の取り組み

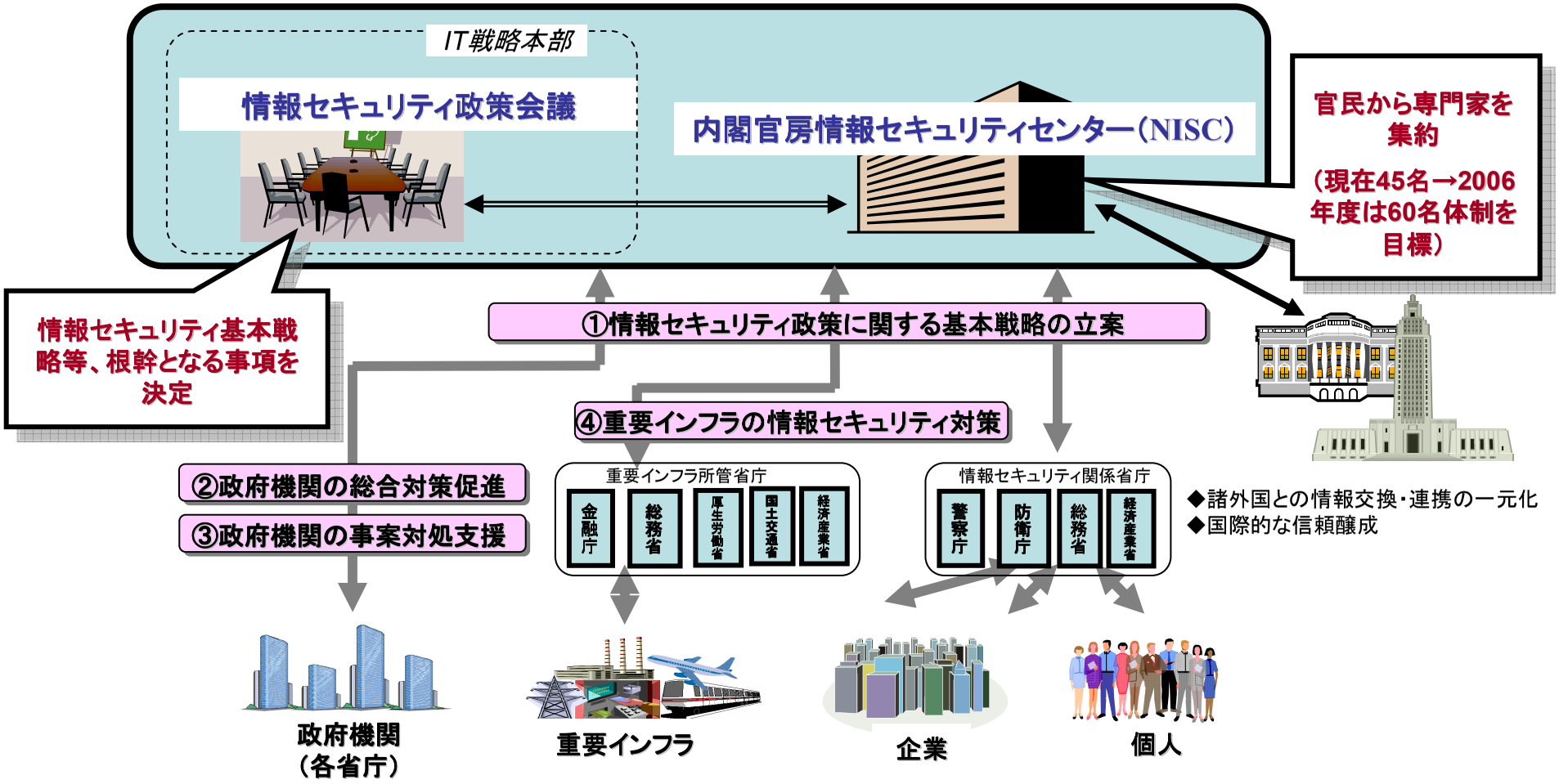
1. 政府中核機能の整備

現在までの内閣官房における情報セキュリティ政策の流れ

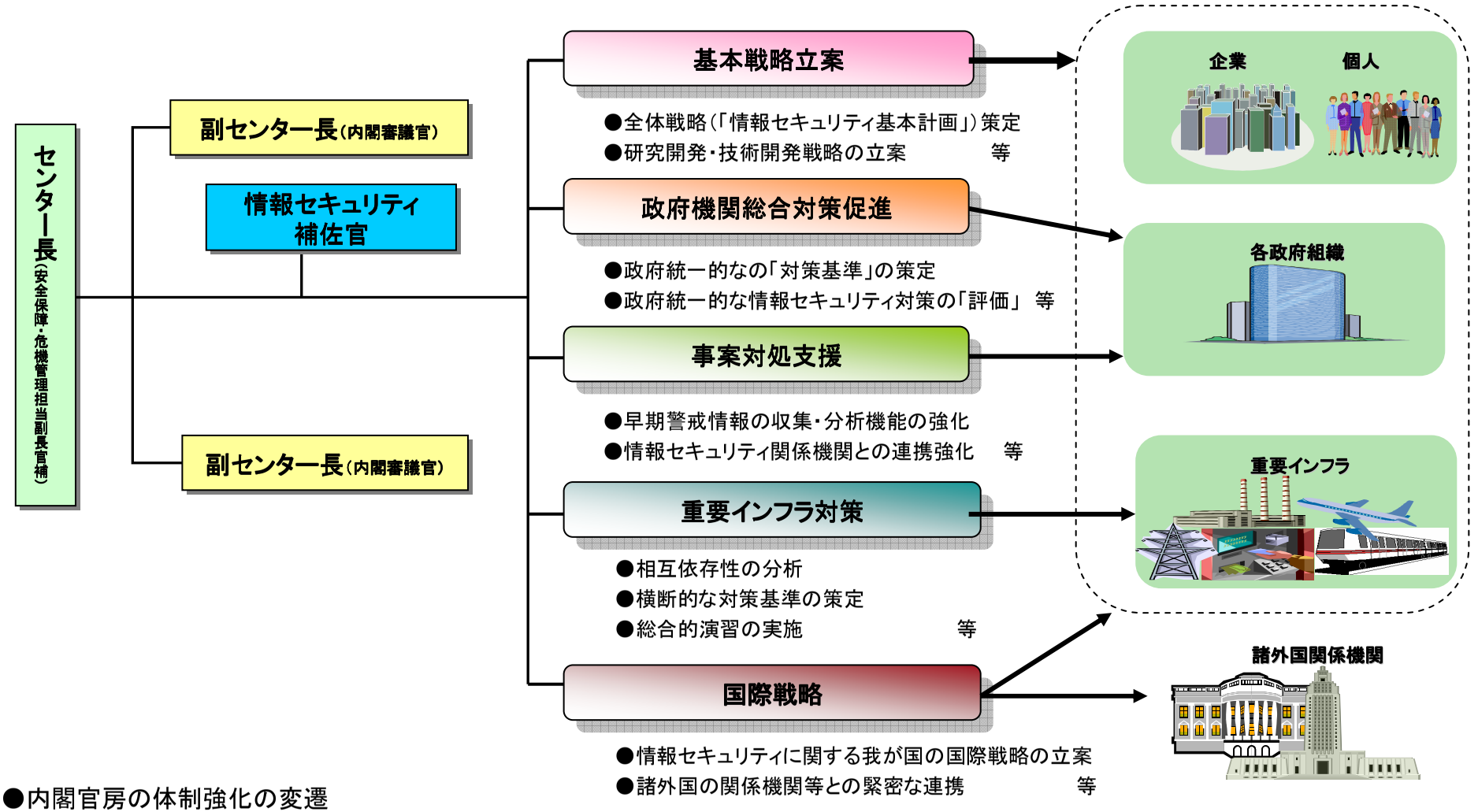


情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）の設置

- 「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

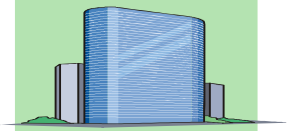
2000年2月発足	2001年1月	2004年7月	2005年12月初時点	2006年4～7月
8名 →	9名 →	18名 →	45名 ⇢	60名（目標）

「第１次情報セキュリティ基本計画（仮称）」に向けた検討

- 本年末を目処に、情報セキュリティ問題を俯瞰した中長期の戦略としての「第１次情報セキュリティ基本計画（仮称）」（案）を情報セキュリティ政策会議にて策定予定。→パブリックコメントを実施した上で最終決定
- 「第１次情報セキュリティ基本計画（仮称）」の審議に資するため、以下の３つの専門委員会を設置。
  - セキュリティ文化の醸成に関する方策の検討→**セキュリティ文化専門委員会**
  - 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についての検討→**技術戦略専門委員会**
  - 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の検討→**重要インフラ専門委員会**

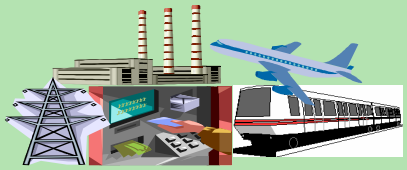
「第１次情報セキュリティ基本計画（仮称）」
情報セキュリティ問題を俯瞰した中長期の戦略

政府組織



- 高水準の情報セキュリティ対策への適応と高い事業継続性確保
- 国民から預託された情報に対する信頼感の高い取り扱い
- 国際的な信頼醸成
- バランスある技術投資の実施
- 透明性の確保

重要インフラ



- 依存可能な基盤としての機能提供
- 検証可能な機能設計と事業継続性確保
- 重要インフラ相互間の連携と協力

企業　　**個人**

- 「セキュリティ文化」の参加者としての積極的な取り組み
- 個人情報保護問題やプライバシー問題に対するコンセンサスの形成

◆ 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

情報セキュリティ基本問題委員会
第１次提言
（2004.11.16）

情報セキュリティ基本問題委員会
第２次提言
（2005.4.22）

セキュリティ文化専門委員会
セキュリティ文化の醸成に関する方策の検討

技術戦略専門委員会
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についての検討

重要インフラ専門委員会
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の検討

2. 政府機関・重要インフラの対策

「政府機関の情報セキュリティ対策のための統一基準（2005年項目限定版）」（2005.9.15）

●各府省庁の情報セキュリティ対策の整合化・共通化を促進し、**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べく、「政府機関の情報セキュリティ対策のための統一基準」とその運用枠組みを政策会議決定**（2005年9月15日）。

●今後、各府省庁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。**

ポイント

1. 政府機関統一基準の策定と省庁対策基準の見直し（水準の底上げ）
各府省庁の情報セキュリティ対策の整合化・統一化と、その水準の斉一的な引き上げ

2. 各府省庁の対策実施状況の検査と評価に基づくPDCAサイクルを確立
第三者の視点で内閣官房情報セキュリティセンター（NISC）が検査・評価し、当該評価結果を基に情報セキュリティ政策会議が勧告→見直し

3. 政府機関統一基準の対策項目の具体化（個別ガイドライン群の策定）
各府省庁における具体的なレベルでの対策実施を支援するための個別ガイドライン群の策定
（例：webサーバ設置、モバイルPC管理等）

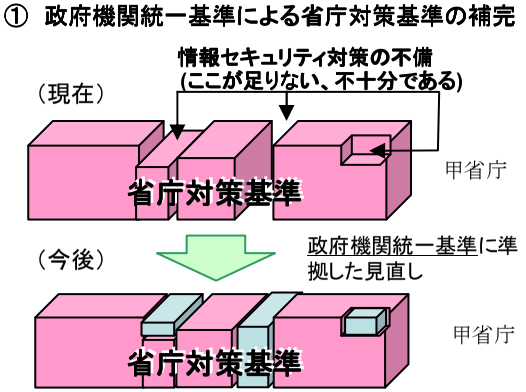
今回策定した文書

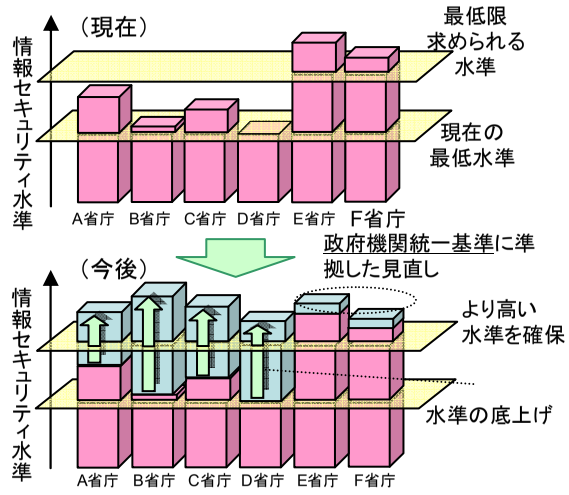
政府機関統一基準（2005年項目限定版）
「政府機関の情報セキュリティ対策のための統一基準」
各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために、各府省庁が採るべき情報セキュリティ対策を定めたもので、緊急性の高いものを中心に取りまとめ

＜盛り込まれた内容の例＞
- ●情報の格付け及び取扱制限に関する基準を明示する手順の整備
- ●情報の持ち出し等の制限事項の強化
- ●一定の情報システムに対するアクセス制御・ログ管理機能の導入
- ●サービス不能攻撃（DoS攻撃）対策の実施
- ●省庁ネットワークに対する不用意な接続の禁止
- ●外部委託先が遵守すべき事項等を含めた契約書の取り交わし

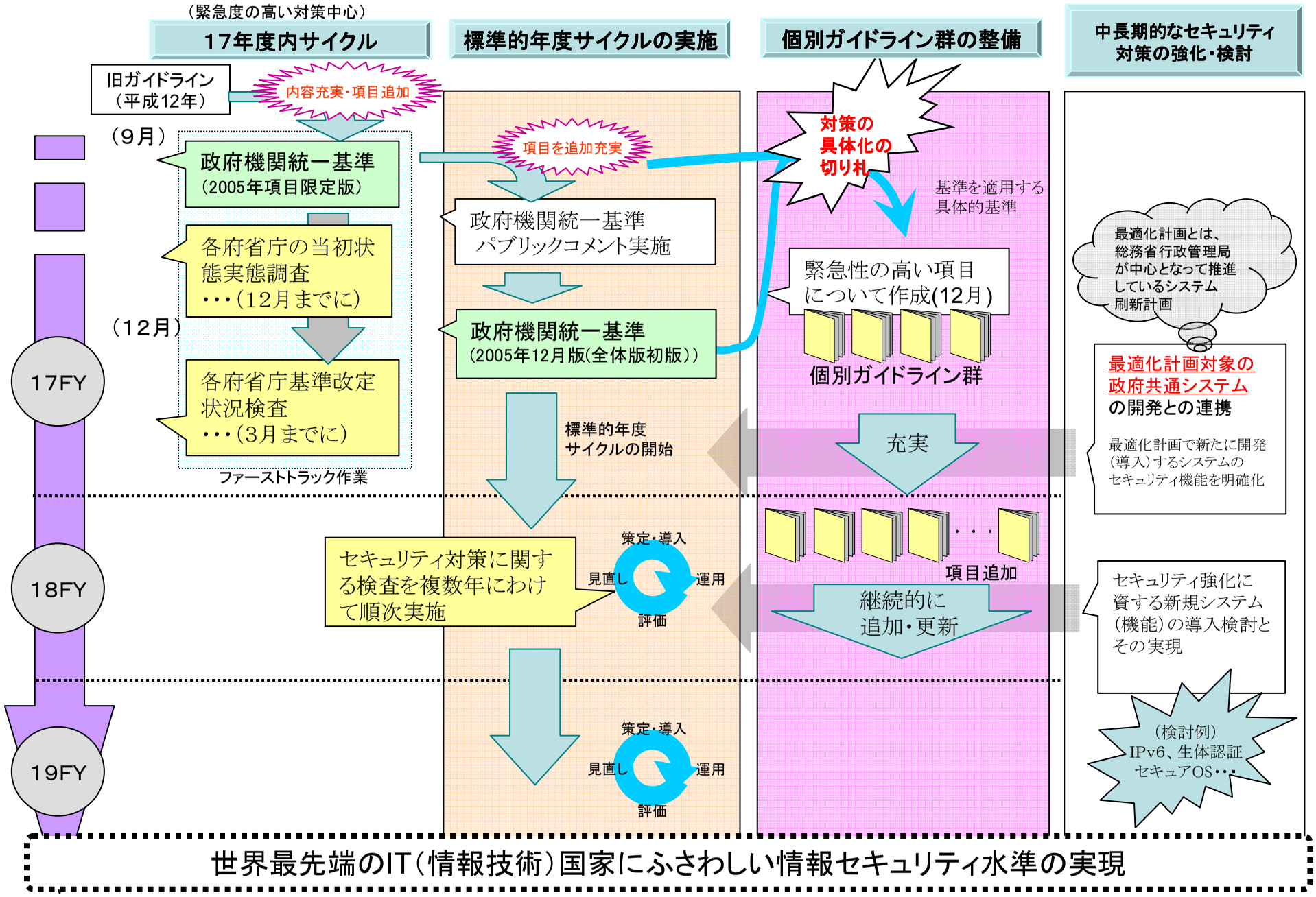
PDCAサイクルの確立
政府機関統一基準（2005年12月版(全体版初版)）の策定（年内目途）
内閣官房情報セキュリティセンターによる検査・評価（本年度内目途）

対策の具体化
具体的対策基準として個別ガイドライン群を作成





統一基準による情報セキュリティ対策の実施



世界最先端のIT（情報技術）国家にふさわしい情報セキュリティ水準の実現

「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」(2005.9.15)

●情報セキュリティ基本問題委員会第2次提言を受け、**情報セキュリティ面からの新たな重要インフラ防護の基本理念として、「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」を政策会議決定**(2005年9月15日)。

●「基本的考え方」に基づき、政策会議に設置した重要インフラ専門委員会の検討を経て、**本年12月を目処に「重要インフラの情報セキュリティ対策に係る行動計画(仮称)」を策定**する予定。

対象分野・脅威の見直し

➢重要インフラ分野として、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービスに、**新たに、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**

新たな体制の構築

1. 重要インフラ横断的機能の強化

➢内閣官房情報セキュリティセンターを中心に、**横断的な状況把握(相互依存性解析等)を実施**

2. 情報セキュリティ水準の向上

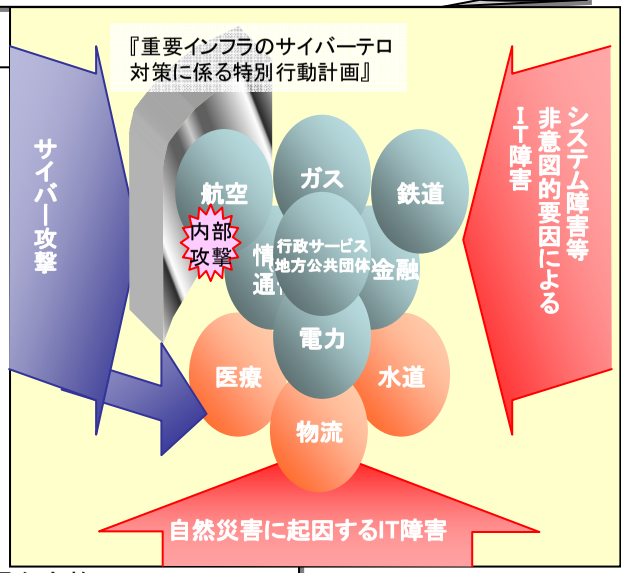
➢技術的基準及び運用基準についての**「安全基準・ガイドライン」の策定・見直し**等を実施

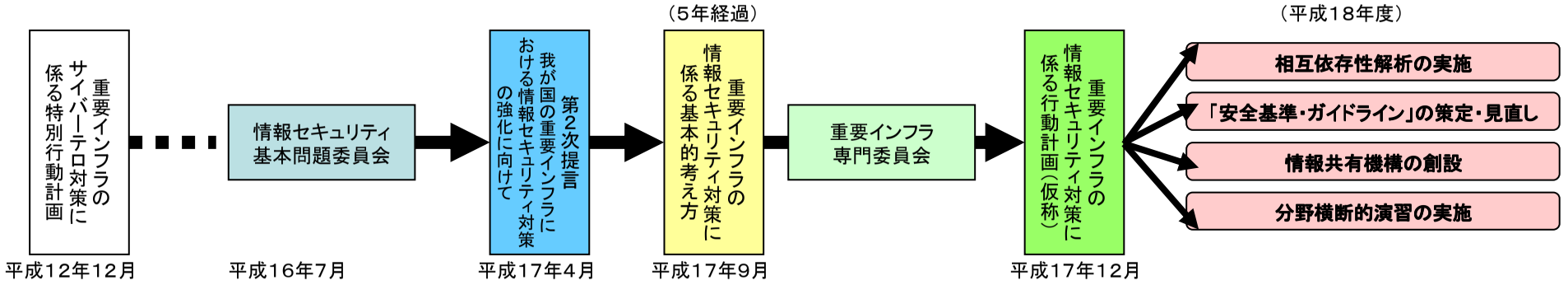
3. 情報共有・提供体制の強化

➢**「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)
➢情報提供体制の整理・強化、情報の充実・質の向上

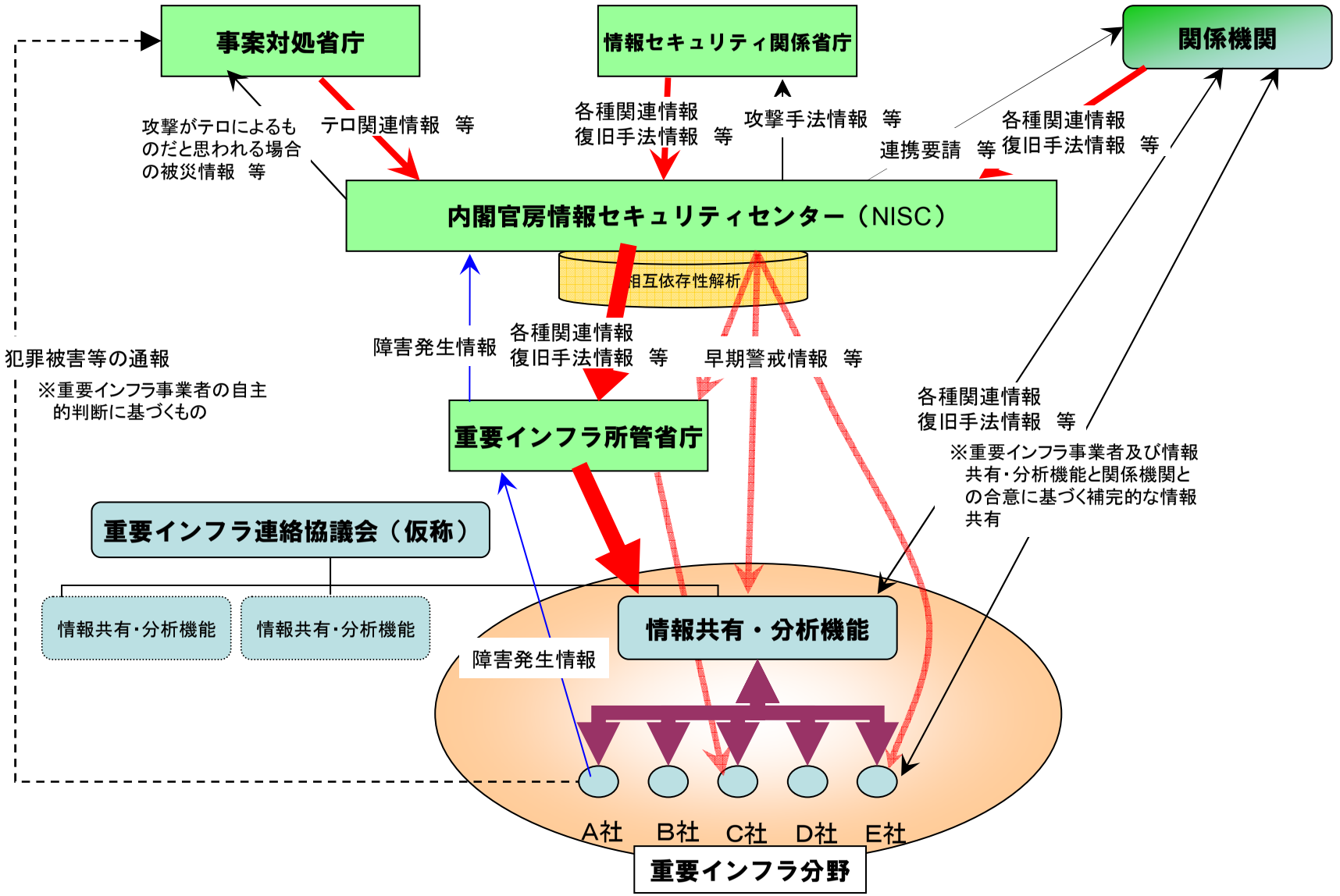
4. 分野横断的演習の実施

➢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





情報共有・提供体制の強化



3. 今後の活動(NISC)

情報セキュリティ政策会議において検討中の課題

政府機関

情報セキュリティ基本問題委員会
第1次提言
（平成16年11月16日）

重要インフラ

情報セキュリティ基本問題委員会
第2次提言
（平成17年4月22日）

早期に着手すべき政府統一的・横断的課題
＜当面の課題への対応＞
政策会議決定（平成17年7月14日）

第1回
(7/14)

政府機関

◆ 総合的な監視・警戒態勢の構築　等
◆ **情報セキュリティ対策の統一的な基準を示し、ガイドライン群を作成**

企業・個人

◆「インターネット安全教室」等、国民のリテラシー向上等への取組み
◆ フィッシング、ボットネットなど新たに登場してきた脅威への対策　等

重要インフラ

◆「安全基準・ガイドライン」の指針を9月までに策定
◆重要インフラごとの「安全基準・ガイドライン」策定
◆自治体ISAC（仮称）の創設支援　等
◆ **「重要インフラのサイバーテロ対策に係る特別行動計画」の改定に向けての検討**

第2回
(9/15)

政府機関統一基準
（2005年項目限定版）
・情報セキュリティ対策の強化に関する政府基本方針
・統一基準運用指針（スキームの提示）
・政府機関の統一基準

基本計画の方向性
・「第1次情報セキュリティ基本計画（仮称）」の骨子と方向性

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
・重要インフラの対象範囲等の見直し
・情報セキュリティ水準向上のための具体的対策
・官民の連絡・連携、情報共有体制の強化

セキュリティ文化専門委員会等での検討

項目の追加充実

基本的考え方に基づいた具体的な行動計画の策定

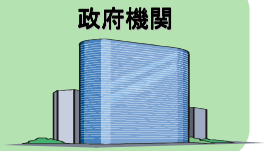
第3回
(12月)

政府機関統一基準
（2005年12月版(全体版初版)）

「第1次情報セキュリティ基本計画(仮称)」（案）
情報セキュリティ問題を俯瞰した中長期の戦略

重要インフラの情報セキュリティ対策に係る行動計画

政府機関



企業

個人

重要インフラ