



政府機関における情報セキュリティ問題への取組み

～ 政府機関統一基準に基づく対策 ～

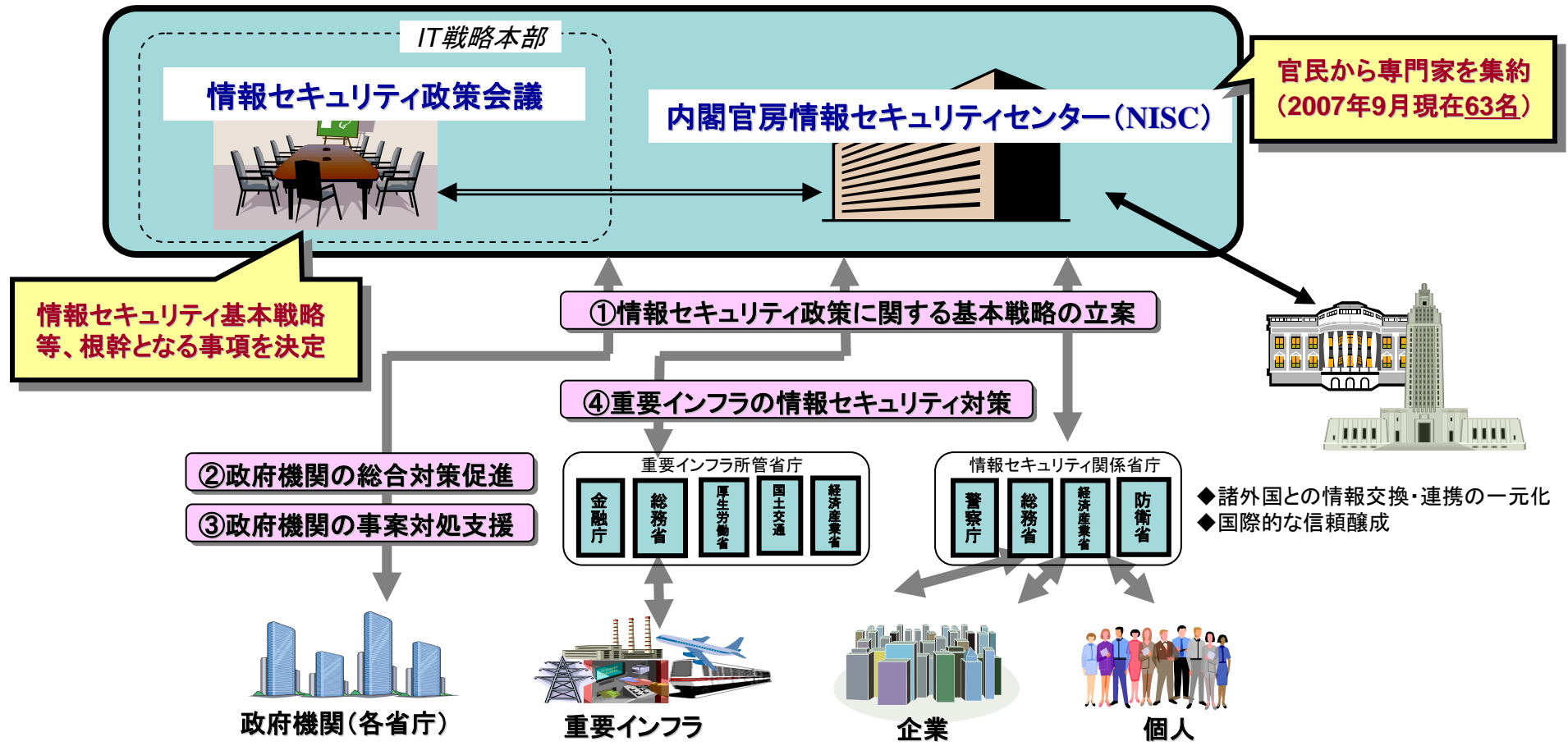
2007年9月27日

内閣官房情報セキュリティセンター

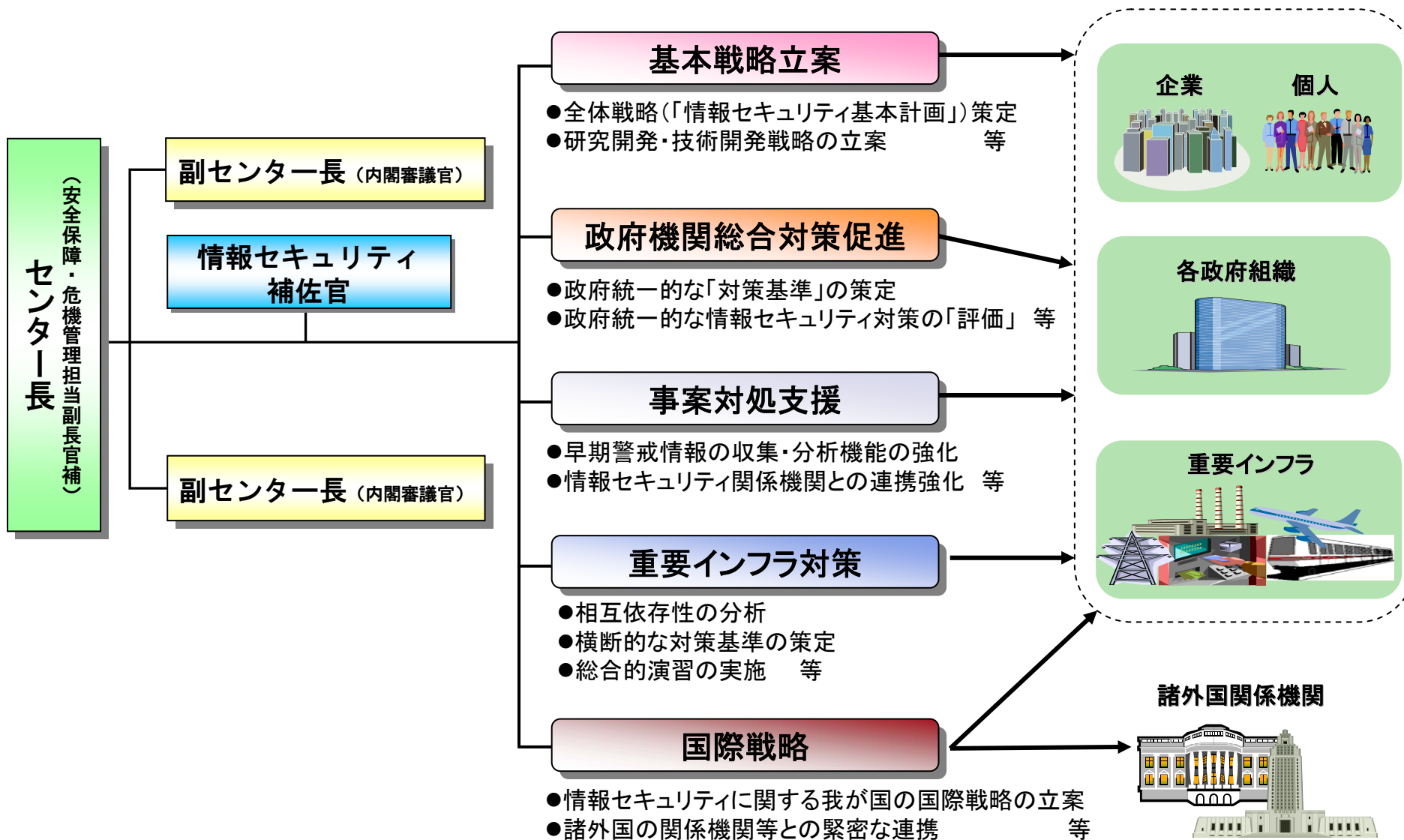
情報セキュリティ政策会議及び 内閣官房情報セキュリティセンター(NISC)の設置



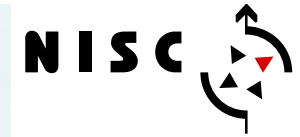
- ▶ 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」(2004年12月7日IT戦略本部決定)を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備
 - ▶ 2005年4月25日、内閣官房情報セキュリティセンター(NISC: National Information Security Center)を設置
 - ▶ 2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」(議長:内閣官房長官)を設置



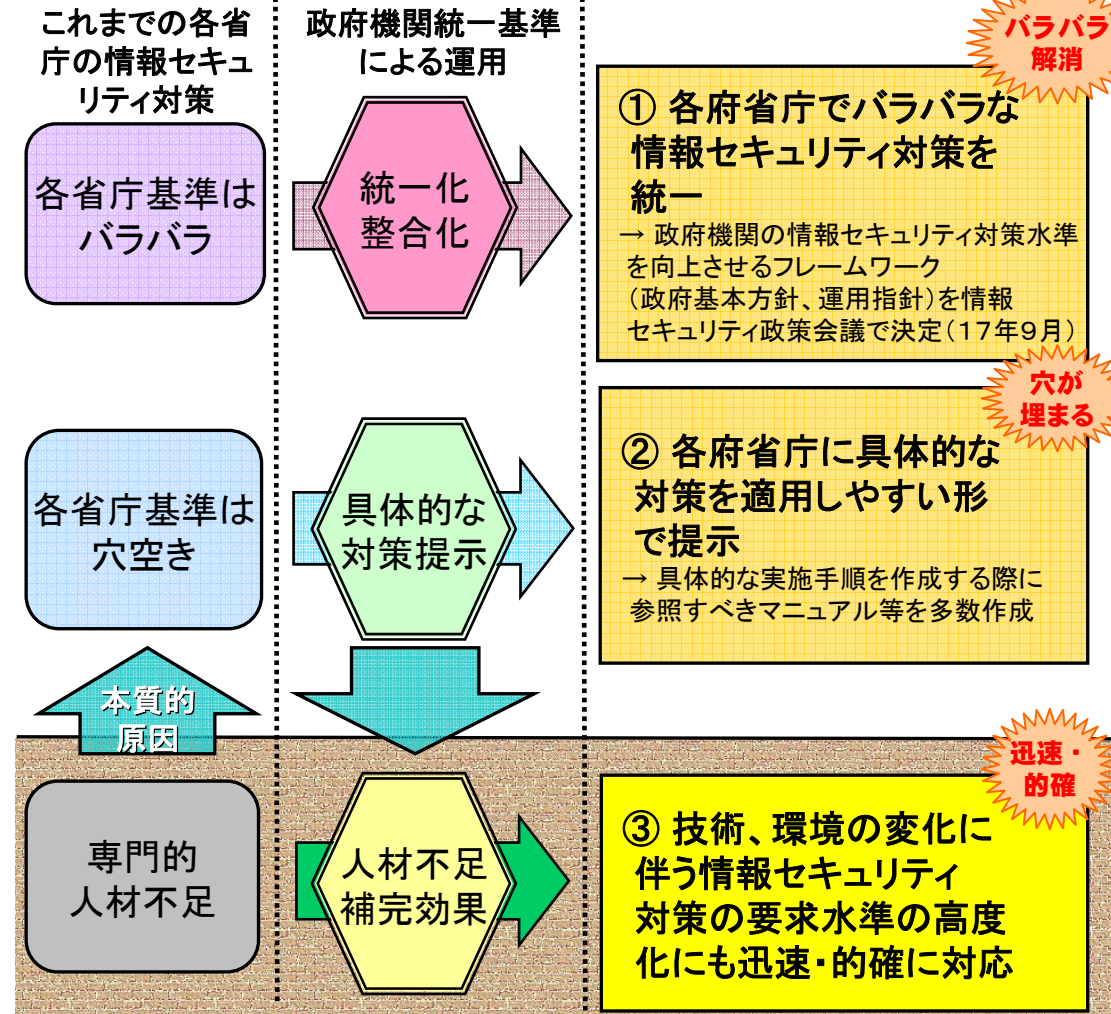
内閣官房情報セキュリティセンター(NISC)の機能・体制



政府機関の情報セキュリティ対策の統合化・共通化

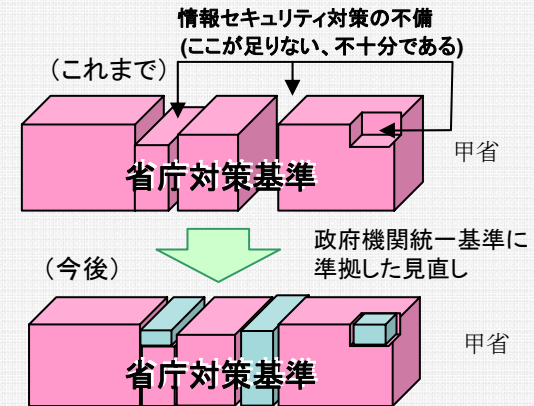


➤ 各府省庁の**情報セキュリティ対策の統合化・共通化**を促進し、政府機関全体としての情報セキュリティ水準の向上を図る。

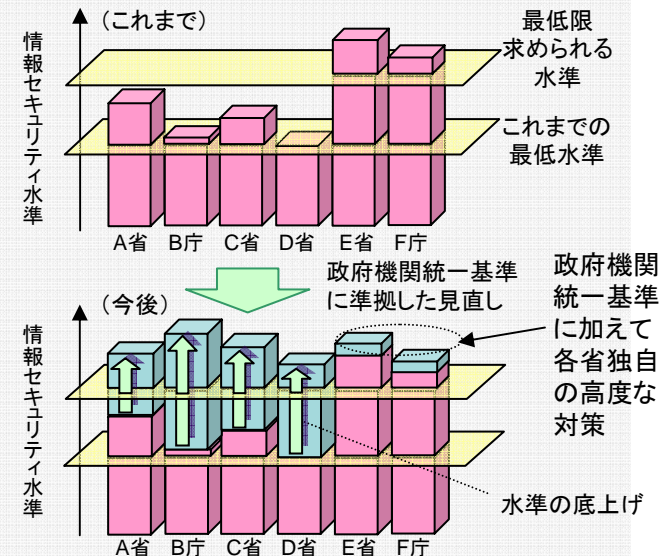


各府省庁の対策の統一化・整合化と水準の向上

① 政府機関統一基準による省庁対策基準の補完



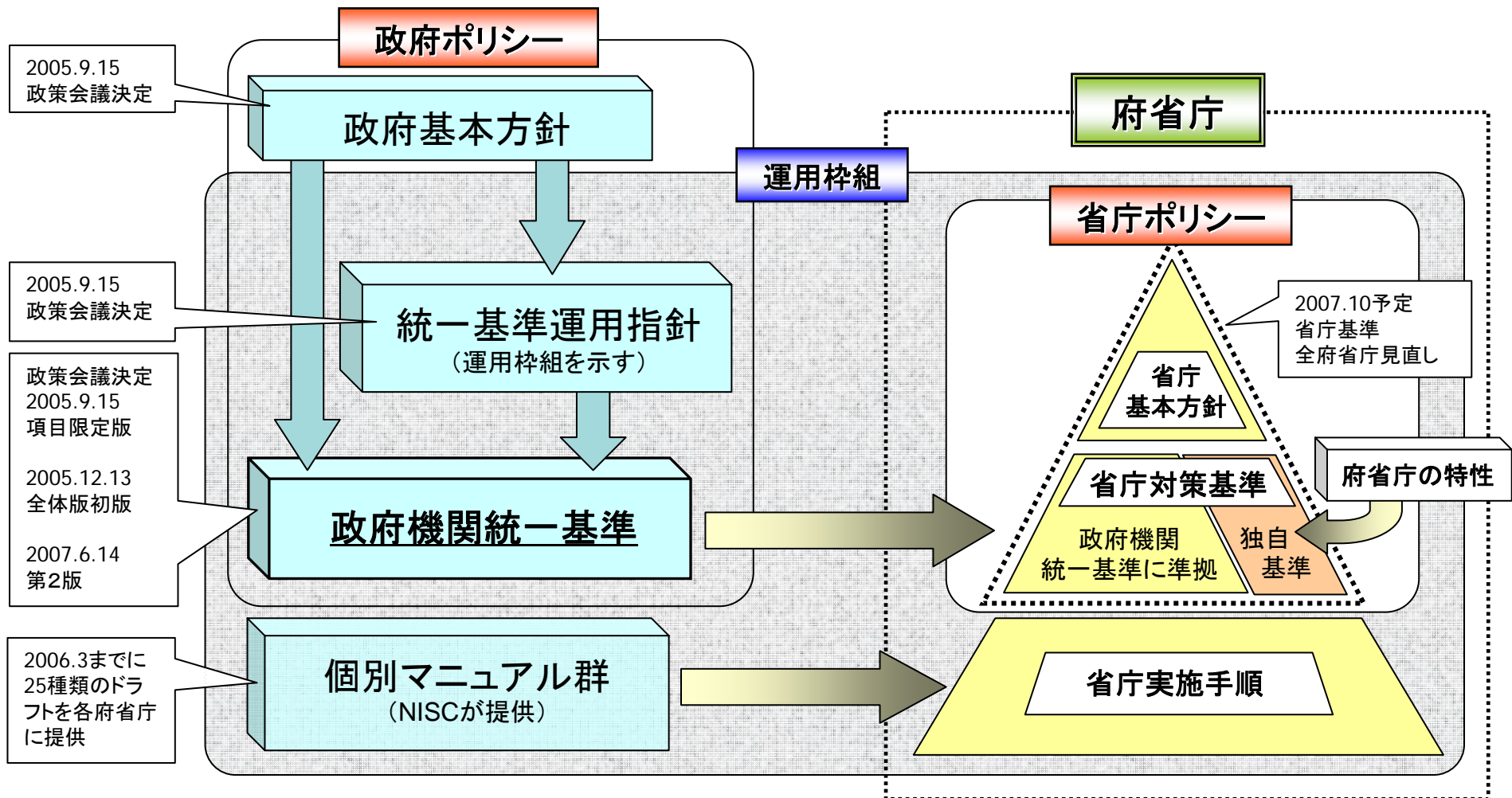
② 各府省庁の情報セキュリティ水準の向上



政府機関の情報セキュリティ対策の枠組み(1)



➤ 政府全体としての情報セキュリティ水準の向上を図るため、「政府機関の情報セキュリティ対策のための統一基準」(政府機関統一基準)を策定 (2005年12月策定、2007年6月改訂)

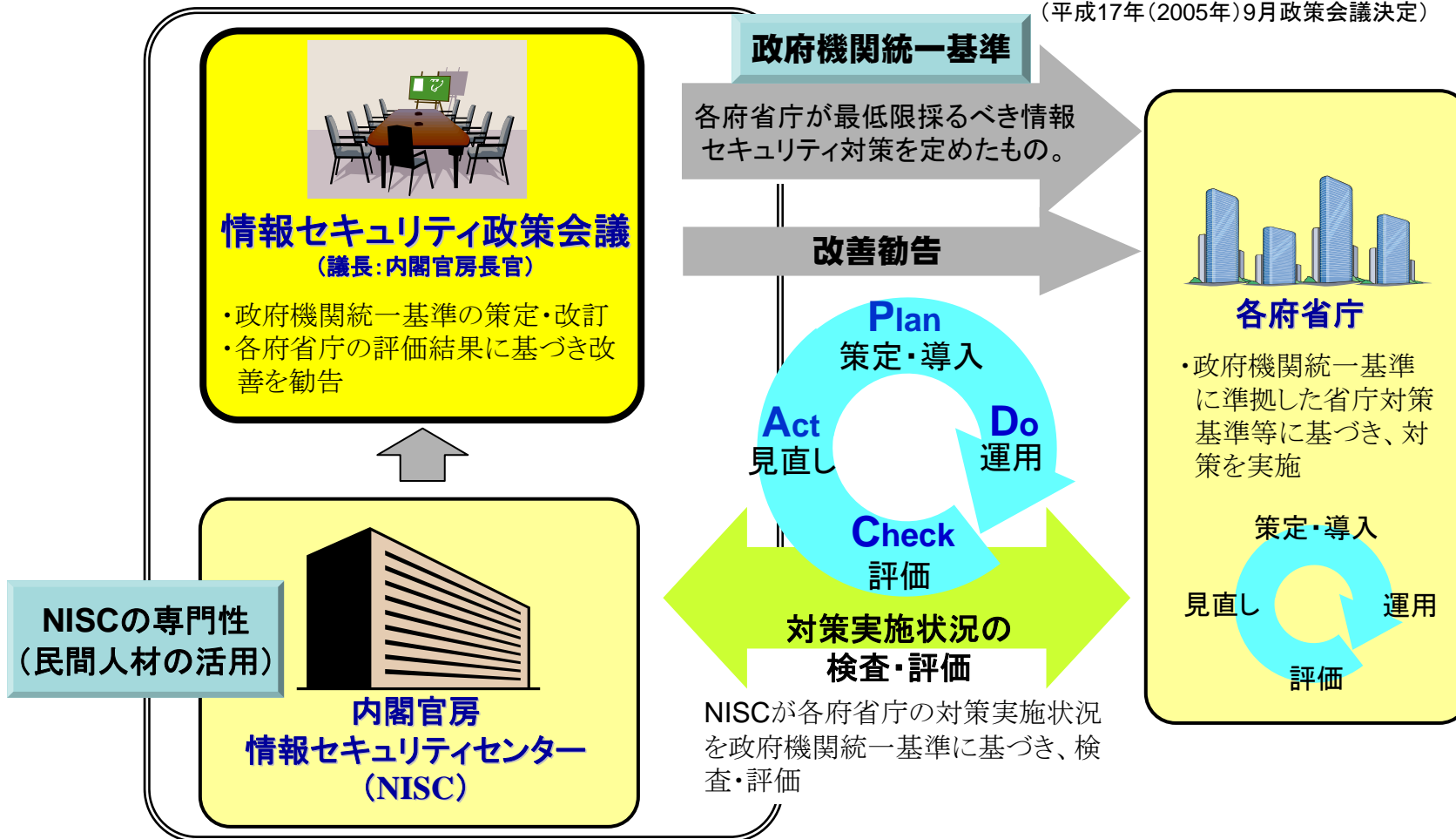


政府機関の情報セキュリティ対策の枠組み(2)

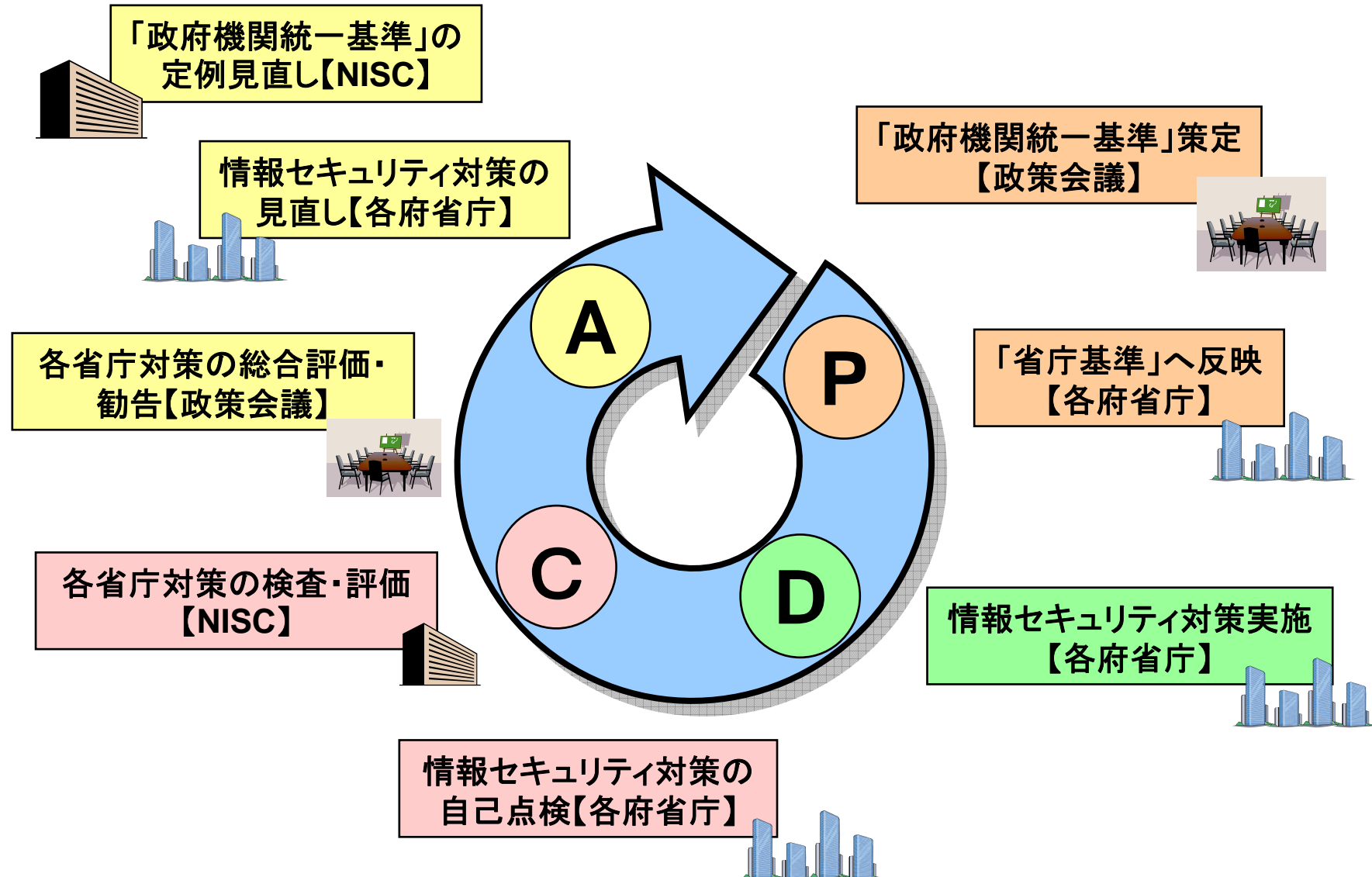
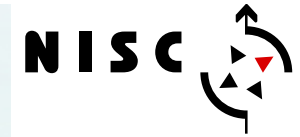


各府省庁は政府機関統一基準を踏まえて情報セキュリティ対策を実施し、**内閣官房情報セキュリティセンター(NISC)が各府省庁の対策実施状況を検査・評価**

(平成17年(2005年)9月政策会議決定)



「政府機関統一基準」に基づくPDCAサイクル



第1部 総則

第2部 組織と体制の構築

- 組織・体制の確立(各責任者等の権限と責務の明確化等)
- 情報セキュリティ対策の教育
- 情報セキュリティ対策の自己点検
- 見直し
- 違反と例外措置
- 障害等の対応
- 情報セキュリティ対策の監査

第3部 情報についての対策

- 情報の格付け
- 情報の取扱い(利用・保存・移送・提供・消去)

第4部 情報セキュリティ要件の明確化に基づく対策

- 情報セキュリティ機能
 - 主体認証、アクセス制御、権限管理、証跡管理、情報保証、暗号・電子署名
- 脅威対策
 - セキュリティホール対策、不正プログラム対策、サービス不能攻撃対策
- 情報システムのセキュリティ要件
 - 情報システムの設計・構築・運用等

第5部 情報システムの構成要素についての対策

- 安全区域
- アプリケーション(共通、電子メール、ウェブ)
- 電子計算機(共通、端末、サーバ)
- 通信回線(共通、庁内、庁外)

第6部 個別事項についての対策

- 機器等の購入
- ソフトウェア開発
- 府省庁支給以外の情報システム(私物PC等)による情報処理の制限
- 外部委託
- 府省庁外での情報処理(情報の持ち帰り等)の制限
- その他

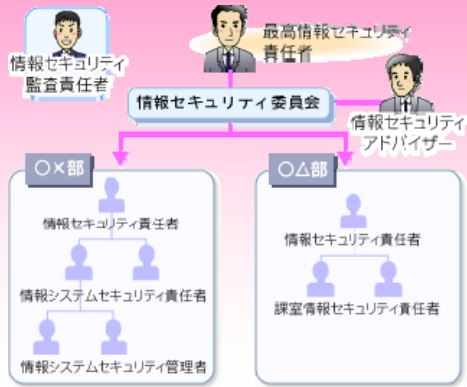
☆ 対策レベル: 「基本遵守事項」(必須の対策事項)と「強化遵守事項」(重要なシステムにおいて必要性を判断して取り入れる対策事項)

(参考) 政府機関統一基準の概要①

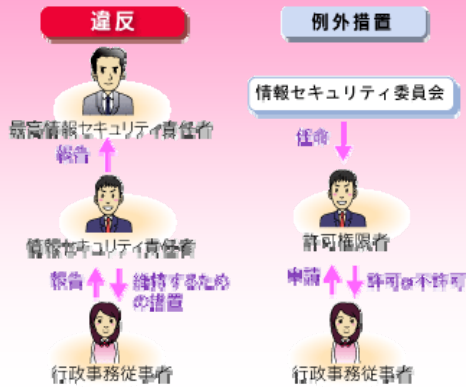


第1部 総則(政府機関統一基準の位置付け、用語定義等)

第2部 組織と体制の構築 遵守事項数:88(基本:85、強化:3)



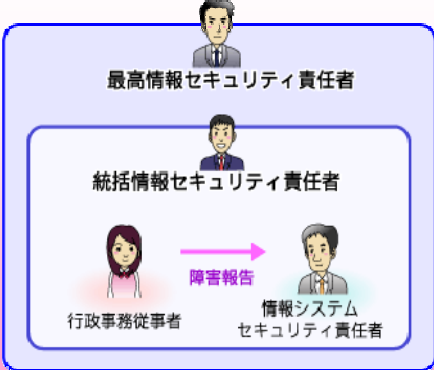
【組織・体制の確立・役割の分離】



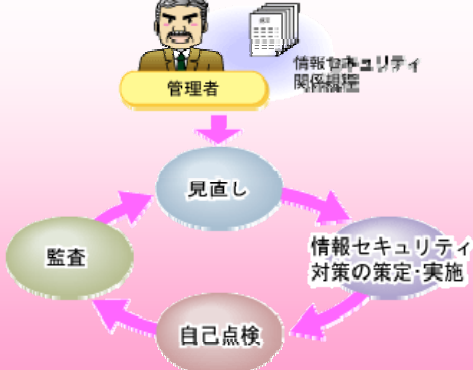
【違反の対応と例外措置の適用】



【情報セキュリティ対策の教育】



【障害等の対応】



【自己点検・監査・見直し】

(参考) 政府機関統一基準の概要②

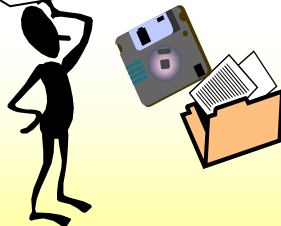
第3部 情報についての対策

※ 主に情報システムの利用者が実施する対策
 遵守事項数: 45(基本:41、強化: 4)

格付けに応じて対策を実施(第4~6部も同様)

【情報の格付け】

機密性、完全性、可用性のレベル
 取扱制限の有無

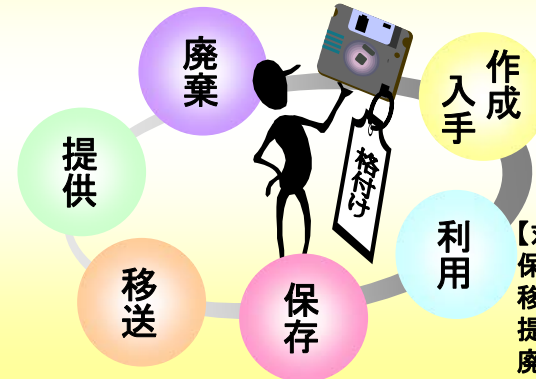


【格付けの明示】



どの程度の保護が必要かを決定 情報の利用者における意識の共有

【情報のライフサイクルに則した対策】



【対策の内容】
 保存: 適切な媒体管理
 移送: 情報の暗号化
 提供: 許可・届出
 廃棄: 確実な抹消 等

第4部 情報セキュリティ要件の明確化に基づく対策

※ 主に情報システムの管理者が実施する対策
 遵守事項数: 129(基本:89、強化:40)

【情報システムにおいてセキュリティ機能の必要性を検討】

- 主体認証機能
- アクセス制御機能
- 権限管理機能
- 証跡管理機能
- 保証のための機能
- 暗号・電子署名に係る機能

【様々な脅威による影響を検討】

- セキュリティホール対策
- 不正プログラム対策
- サービス不能攻撃対策

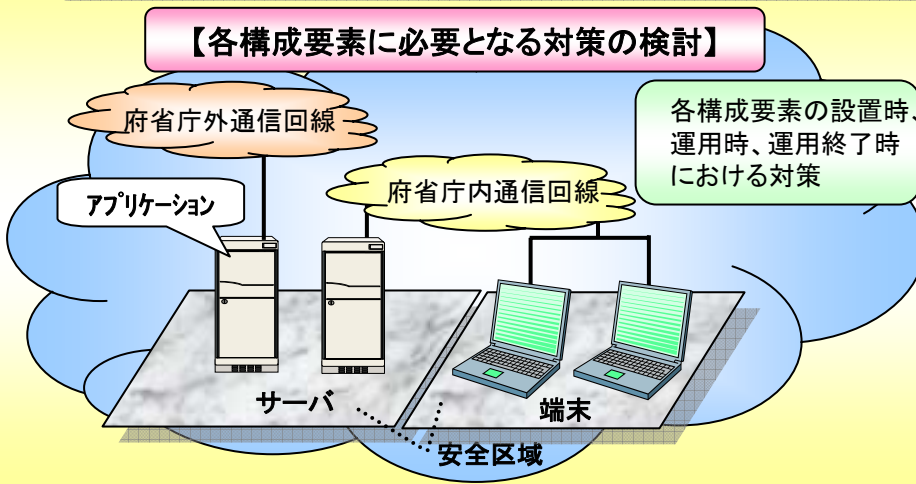
【情報システムのセキュリティ要件に係る検討】

情報システムのライフサイクル(計画、設計、構築、運用、監視、移行、廃棄、見直し)に則し、セキュリティの観点から考慮すべき要件

(参考) 政府機関統一基準の概要③

第5部 情報システムの構成要素についての対策

※ 主に情報システムの管理者が実施する対策
 遵守事項数:126(基本:82、強化:44)



【各構成要素に必要となる主な対策】

- 電子計算機等を設置する安全区域
立入り・退出の管理、身分証明書の提示等
- 電子計算機(端末、サーバ)
電子計算機関連文書の整備、モバイルPCの取扱い等
- アプリケーション(電子メール、ウェブ)
電子メールの不正な中継の禁止、特殊文字の無害化等
- 通信回線(府省庁内通信回線、府省庁外通信回線)
不適切な接続の禁止、通信状況の確認・分析等

各構成要素に必要となる対策を列挙

↓
 検討漏れによる不備の防止

第6部 個別事項についての対策

※ ④、⑤については、主に情報システムの利用者が実施する対策
 遵守事項数: 74(基本:70、強化: 4)

① 機器等の購入に係る対策

- 【脅威】セキュリティ対策に不備がある製品の購入 等
 【対策】機器等の選定基準の整備
 機器等の納入時の確認 等

② 外部委託に係る対策

- 【脅威】委託先の不適正な情報管理による情報漏えい 等
 【対策】委託先の選定基準の整備
 委託先に適用する対策の整備 等

③ ソフトウェア開発に係る対策

- 【脅威】開発したソフトに脆弱性が存在する 等
 【対策】ソフトウェア開発手順の整備
 設計レビューの実施 等

④ 庁舎外での情報処理に係る対策

- 【脅威】行政情報を保存したモバイルPCの紛失 等
 【対策】庁舎外での情報処理に係る手続の整備
 安全管理措置規定の整備 等

⑤ 私物パソコンの利用に係る対策

- 【脅威】ウイルスに感染した私物パソコンの利用による情報漏えい 等
 【対策】私物パソコンの公務利用に係る手続の整備
 安全管理措置規定の整備 等

⑥ その他

- 府省庁外の情報セキュリティ水準の低下を招く行為の防止
- 事業継続計画(BCP)との整合的運用の確保