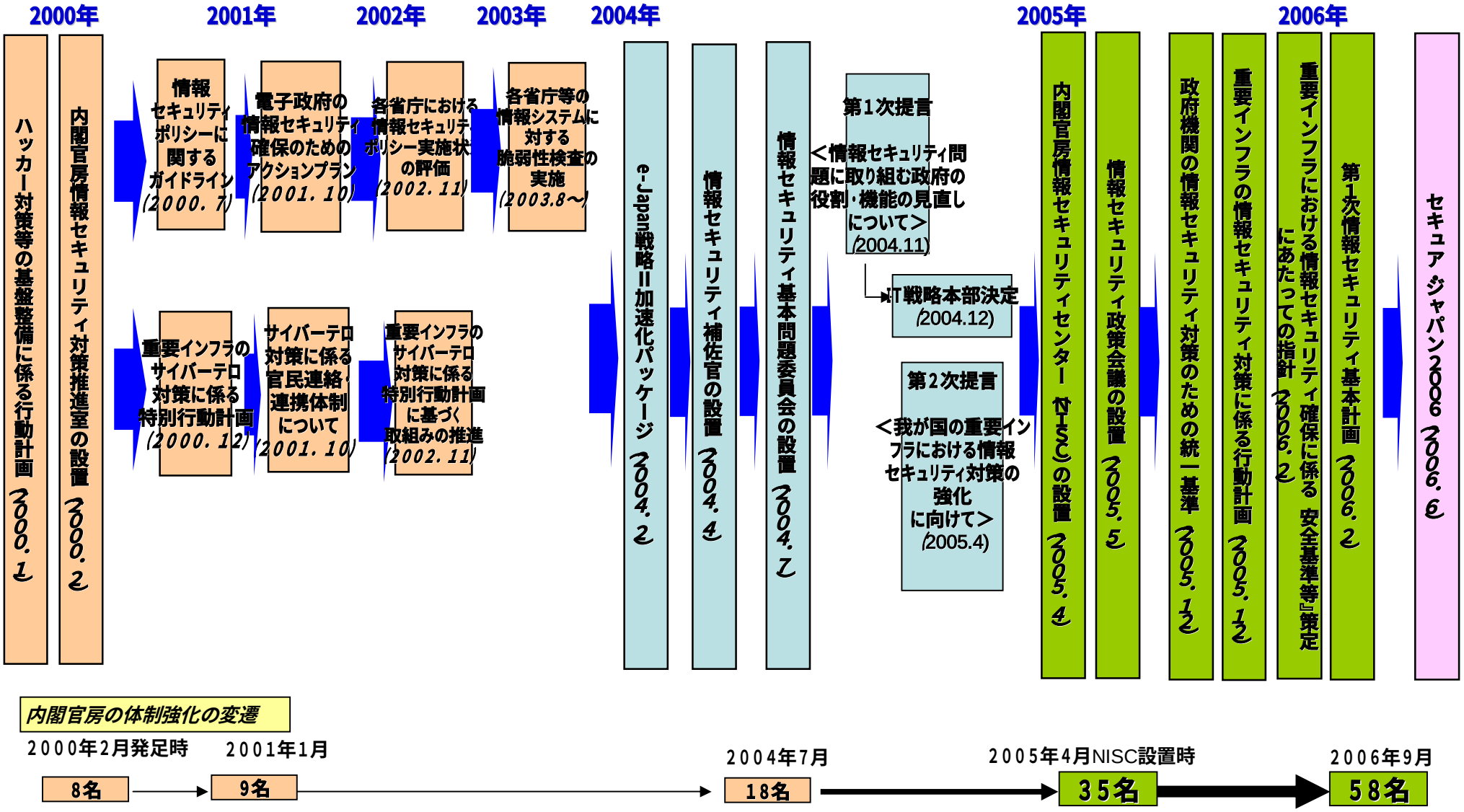
政府機関における情報セキュリティ問題への取組み
～ 政府機関統一基準を中心として ～

2006年11月7日

内閣官房情報セキュリティセンター（NISC）
内閣参事官　伊 藤 毅 志

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

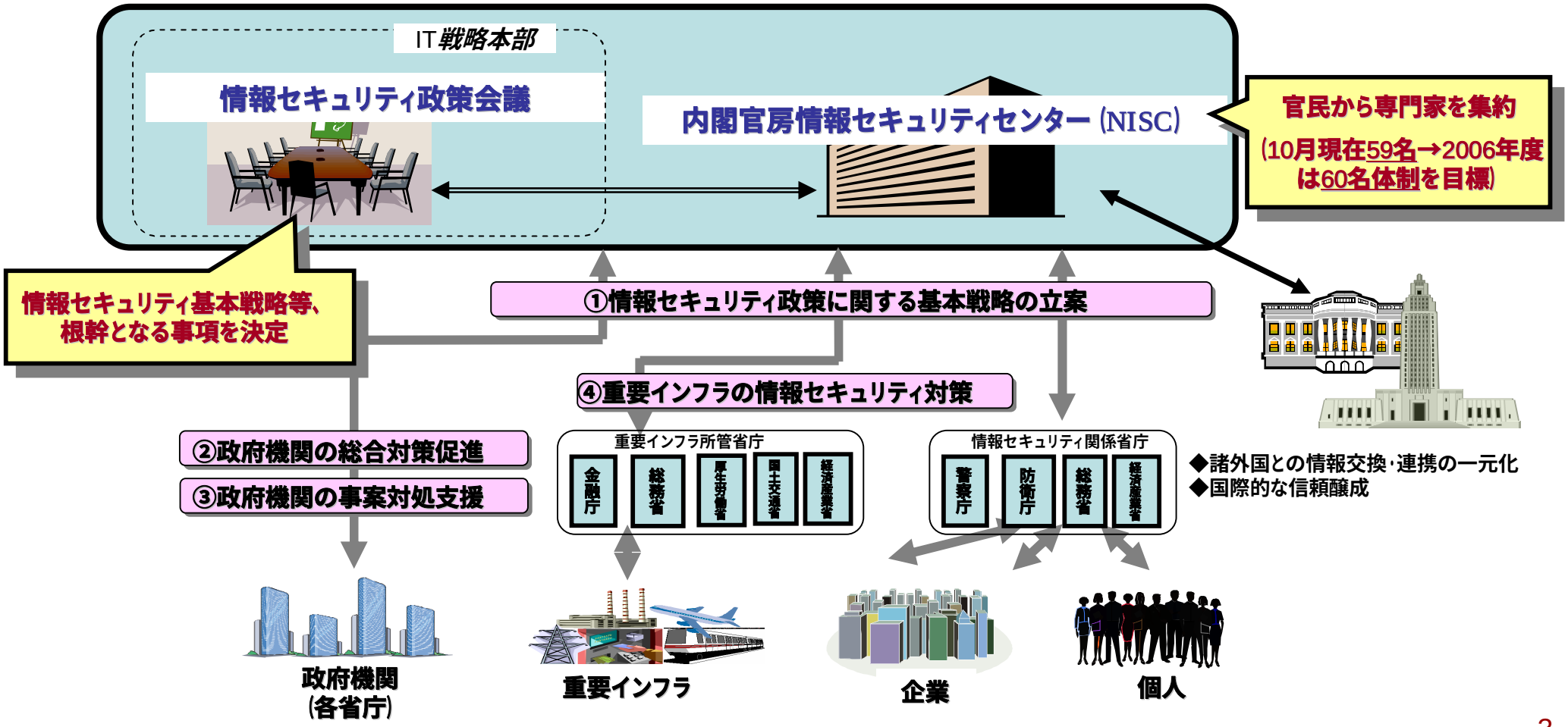


内閣官房の体制強化の変遷

2000年2月発足時 8名 → 2001年1月 9名 → 2004年7月 18名 → 2005年4月NISC設置時 35名 → 2006年9月 58名

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。



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

情報通信技術（IT）担当大臣

構成員

国家公安委員会委員長
防衛庁長官
総務大臣
経済産業大臣
江畑 謙介　　拓殖大学客員教授／軍事評論家
小野寺 正　　ＫＤＤＩ(株) 代表取締役社長
金杉 明信　　日本電気（株）取締役副会長
野原 佐和子　　(株) 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

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

「第1次情報セキュリティ基本計画」と「セキュア・ジャパン2006」

「第1次情報セキュリティ基本計画」（2006年2月2日 情報セキュリティ政策会議）

2006～2008年度の3ヵ年計画。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」の構築を目指す。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
目標	2009年度初めには すべての政府機関が 「政府機関統一基準」が 求める水準に	2009年度初めには IT障害を限りなくゼロに	2009年度初めには 対策の実施状況を 世界トップクラスの水準に	2009年度初めには 「IT利用に不安を感じる」 個人を限りなくゼロに
重要政策の各実施領域の	◆ 政府機関統一基準に基づく各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能整備 ◆ 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 ◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 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
【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

重要政策の横断的な

- 情報セキュリティ技術戦略の推進
- 情報セキュリティ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

2005年度 → 2006年度 → 2007年度 → 2008年度 → 2009年度

「セキュア・ジャパン2006」

① 2006年度の実施計画　（133施策）
～「官民におけるセキュリティ対策の体制の構築」

② 2007年度の重点施策の方向性　（26施策）
～「官民におけるセキュリティ対策の底上げ」

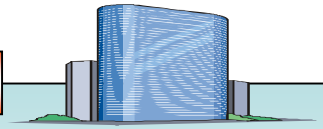
セキュア・ジャパン2007

セキュア・ジャパン2008

「セキュア・ジャパン2006」の具体的施策①

対策実施4領域における情報セキュリティ対策の強化

1　政府機関・地方公共団体



【 目　標 】 **政府機関について、2008年度までに政府機関統一基準のレベルを世界最高水準のものとし、かつ、2009年度初めにはすべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指す。**

【主な施策】
- ○ 「政府機関統一基準」に基づくPDCAサイクルの確立・試行的評価の実施及び結果の公表　*（内閣官房及び全府省庁）*
- ○ 各府省庁における情報の外部持ち出し及び私物パソコンの業務使用に関する厳格な管理　*（全府省庁）*
- ○ 高セキュリティ機能を実現する次世代OS環境の開発　*（内閣官房、内閣府、総務省及び経済産業省）*
- ○ 政府機関に対するサイバー攻撃等に関する情報収集、分析・解析機能の強化　*（内閣官房）*
- ○ 地方公共団体における情報セキュリティポリシーの策定・見直しの促進　*（総務省）*　等

2　重要インフラ

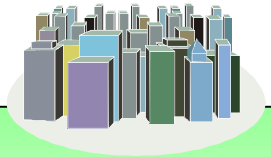
【 目　標 】 **2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロにすることを目指す。**

【主な施策】
- ○ 各重要インフラ分野における情報セキュリティ確保に係る「安全基準等」の策定・見直し　*（重要インフラ所管省庁）*
- ○ 「安全基準等」の策定状況の把握及び評価　*（内閣官房）*
- ○ 情報共有体制整備と機能強化　*（内閣官房及び重要インフラ所管省庁）*
- ○ 各重要インフラ分野の依存関係を可視化できる仕組みの構築及びこれに基づく相互依存性解析の試行的実施　*（内閣官房）*
- ○ 重要インフラ横断的な研究的演習及び机上演習の実施・各分野サイバー演習間の連携

（内閣官房及び重要インフラ所管省庁）　等

「セキュア・ジャパン2006」の具体的施策②

対策実施4領域における情報セキュリティ対策の強化（続き）



3 企 業

【 目 標 】 2009年度初めには、企業における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することを目指す。

【主な施策】
- ○ 企業における情報セキュリティガバナンスの確立促進 *（経済産業省）*
- ○ 政府調達において競争参加者に入札条件等として求めるセキュリティ対策レベルの検討 *（内閣官房、総務省、財務省及び全府省庁）*
- ○ 情報セキュリティ関連制度と内部統制制度等との整合性確保 *（内閣官房、金融庁及び経済産業省）*
- ○ 情報セキュリティ関連リスクに対する定量的評価手法の検討 *（経済産業省）*
- ○ 情報通信セキュリティ人材を育成するための研修事業への支援 *（総務省）* 等

4 個 人

【 目 標 】 2009年度初めには、「IT利用に不安を感じる」とする個人を限りなくゼロにすることを目指す。

【主な施策】
- ○ 小中学校における情報セキュリティ教育の推進 *（文部科学省）*
- ○ 「インターネット安全教室」の充実・強化と全国での継続的開催 *（経済産業省及び警察庁）*
- ○ 保護者・教職員向け啓発講座（e－ネットキャラバン）の全国規模での実施 *（総務省及び文部科学省）*
- ○ 「情報セキュリティの日（2月2日）」の創設 *（内閣官房、警察庁、総務省、文部科学省及び経済産業省）*
- ○ IPv6によるユビキタス環境構築に向けたセキュリティの確保 *（総務省）* 等

「セキュア・ジャパン2006」の具体的施策③

横断的な情報セキュリティ基盤の形成

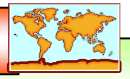
1　情報セキュリティ技術戦略の推進

【主な施策】
- ○ 長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」のテーマ検討　*（内閣官房及び内閣府）*
- ○ 高い情報セキュリティ保証レベル（EAL6）を満足する情報システムの試作　*（防衛庁）*　等

2　情報セキュリティ人材の育成・確保

【主な施策】
- ○ 情報セキュリティ関連の高等教育機関における多面的・総合的能力を有する人材の育成　*（文部科学省）*
- ○ 情報セキュリティに関する資格制度の体系化等のための検討　*（内閣官房、総務省、文部科学省及び経済産業省）*　等

3　国際連携・協調の推進



【主な施策】
- ○ 多国間の枠組み等における国際連携・協力の推進　*（内閣官房及び全府省庁）*
- ○ ベストプラクティスの国際的な発信・普及　*（内閣官房及び全府省庁）*　等

4　犯罪の取締り及び権利利益の保護・救済

【主な施策】
- ○ サイバー犯罪の取締り強化のための技能水準の向上、体制の強化・整備、捜査・解析用資機材の充実・強化　*（警察庁）*
- ○ 高度なネットワーク認証基盤実現のための技術開発　*（総務省）*　等

政策の推進体制等

1　政策の推進体制、他の関係機関等との連携

【主な施策】
- ○ 内閣官房情報セキュリティセンター（NISC）の強化　*（内閣官房）*
- ○ 情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施　*（全府省庁）*
- ○ 関係機関等（IT戦略本部、経済財政諮問会議、総合科学技術会議等）との連携強化　*（内閣官房及び内閣府）*　等

2　持続的改善構造の構築

【主な施策】
- ○ 「セキュア・ジャパン2006」の評価の実施及び公表　*（内閣官房）*
- ○ 政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等　*（内閣官房）*
- ○ 情報セキュリティ対策に関する評価指標の確立　*（内閣官房、総務省及び経済産業省）*　等

「セキュア・ジャパン2006」の具体的施策④

○2006年度の体制の構築を受け継ぎ、2008年度に向けての確かな道筋を確立すべく、**「官民における情報セキュリティ対策の底上げ」**を重点として、2007年度に推進する施策の方向性を提示。

2007年度：官民における情報セキュリティ対策の底上げ

模範となる領域の情報セキュリティ対策の底上げ

- ○ 政府機関でのPDCAサイクルの定着と本格的評価の推進
- ○ 政府機関に対するサイバー攻撃等に対する機能の強化
  (GSOC (Government Security Operation Coordination team) の本格稼動)
- ○ 重要インフラ分野間の動的依存性解析、機能的演習の推進　等

取組みが遅れがちな主体の対策の底上げ

- ○ 政府機関の情報に係るポータルサイトの充実・整備
- ○ 分かりやすく実用的な教育コンテンツの作成・配布
- ○ サイバー犯罪の情勢を反映した被害防止対策の推進　等

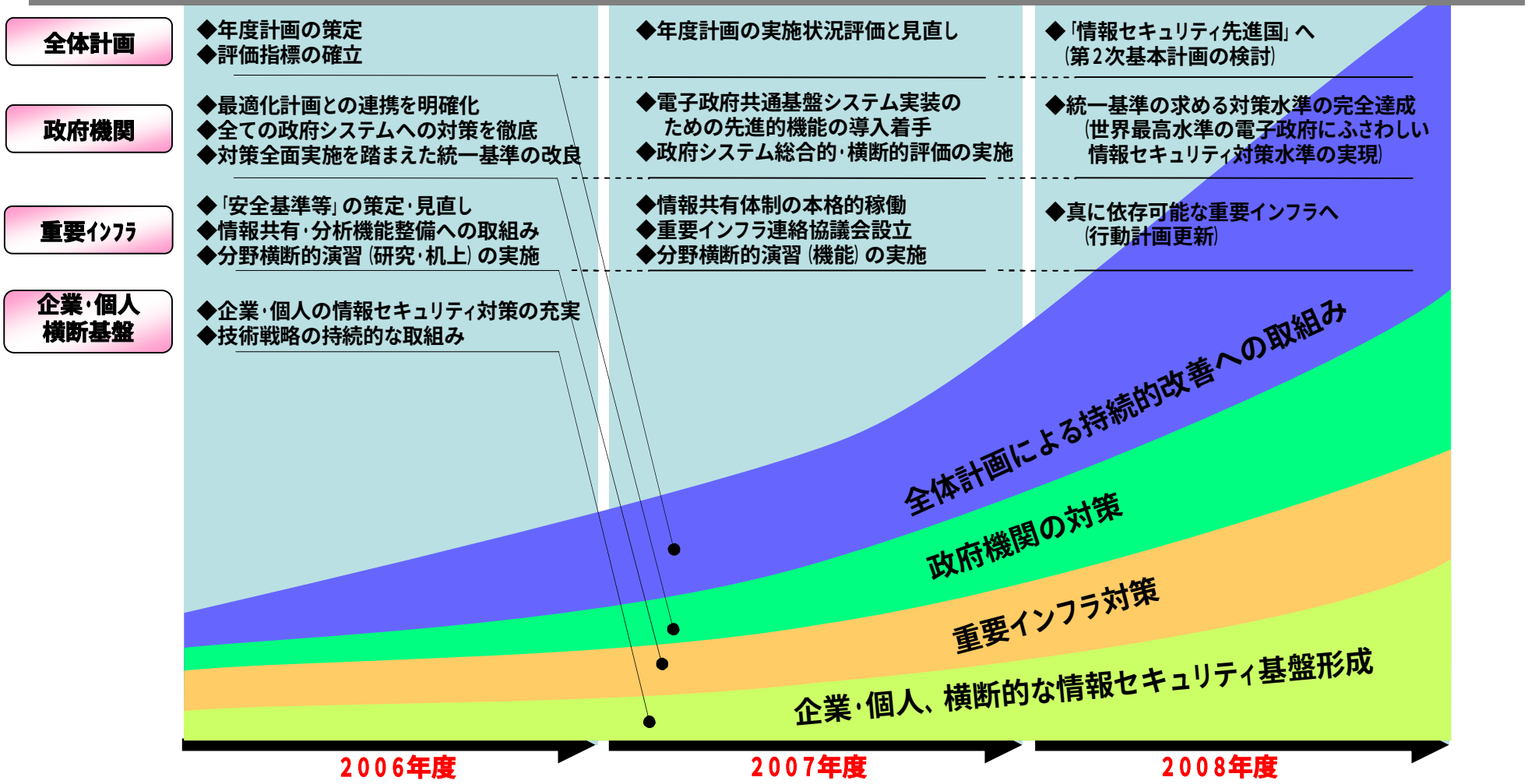
横断的な情報セキュリティ基盤の底上げ

- ○ 「情報セキュリティ対策白書（仮称）」の作成・発行
- ○ 情報セキュリティ教育者、専門家の育成・訓練とキャリアパスの構築に向けた戦略の検討
- ○ 高セキュリティ機能を実現する次世代OS環境の部分的成果の実証利用と機能拡大に向けた開発
- ○ サイバー犯罪に対する捜査能力の総合的底上げ　等

2008年度（基本計画の最終年）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。



2．政府機関の情報セキュリティ対策の枠組み

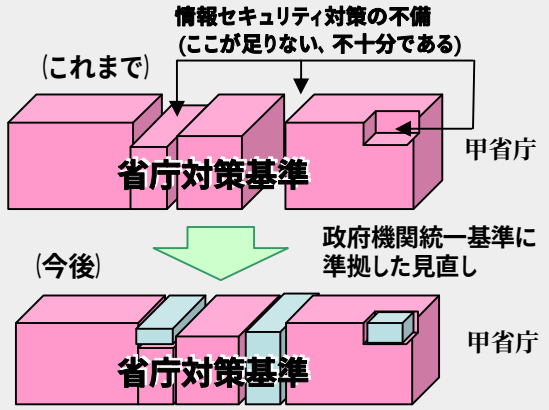
政府機関統一基準とは

●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ため、昨年9月に情報セキュリティ政策会議決定

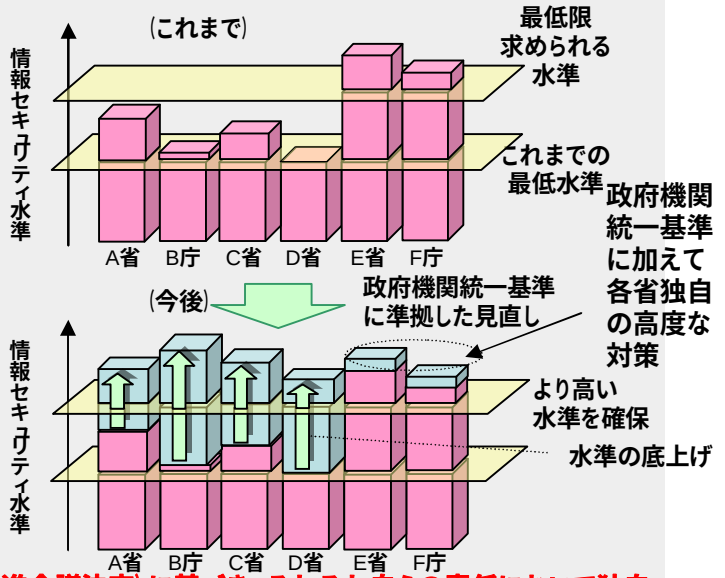
各府省庁の現状	政府機関統一基準による運用	
各省庁基準はバラバラ	統一化 整合化	バラバラ解消 ① 各府省庁でバラバラな情報セキュリティ対策を統一 → 政府機関の情報セキュリティ対策水準を向上させるフレームワーク（政府基本方針、運用指針）を情報セキュリティ政策会議で決定（17年9月）
各省庁基準は穴空き	具体的な対策提示	穴が埋まる ② 各府省庁に具体的な対策を適用しやすい形で提示 → 具体的な実施手順を作成する際に参照すべきマニュアル等を多数作成
本質的原因 専門的人材不足	人材不足補完効果	迅速・的確 ③ 技術、環境の変化に伴う情報セキュリティ対策の要求水準の高度化にも迅速・的確に対応

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



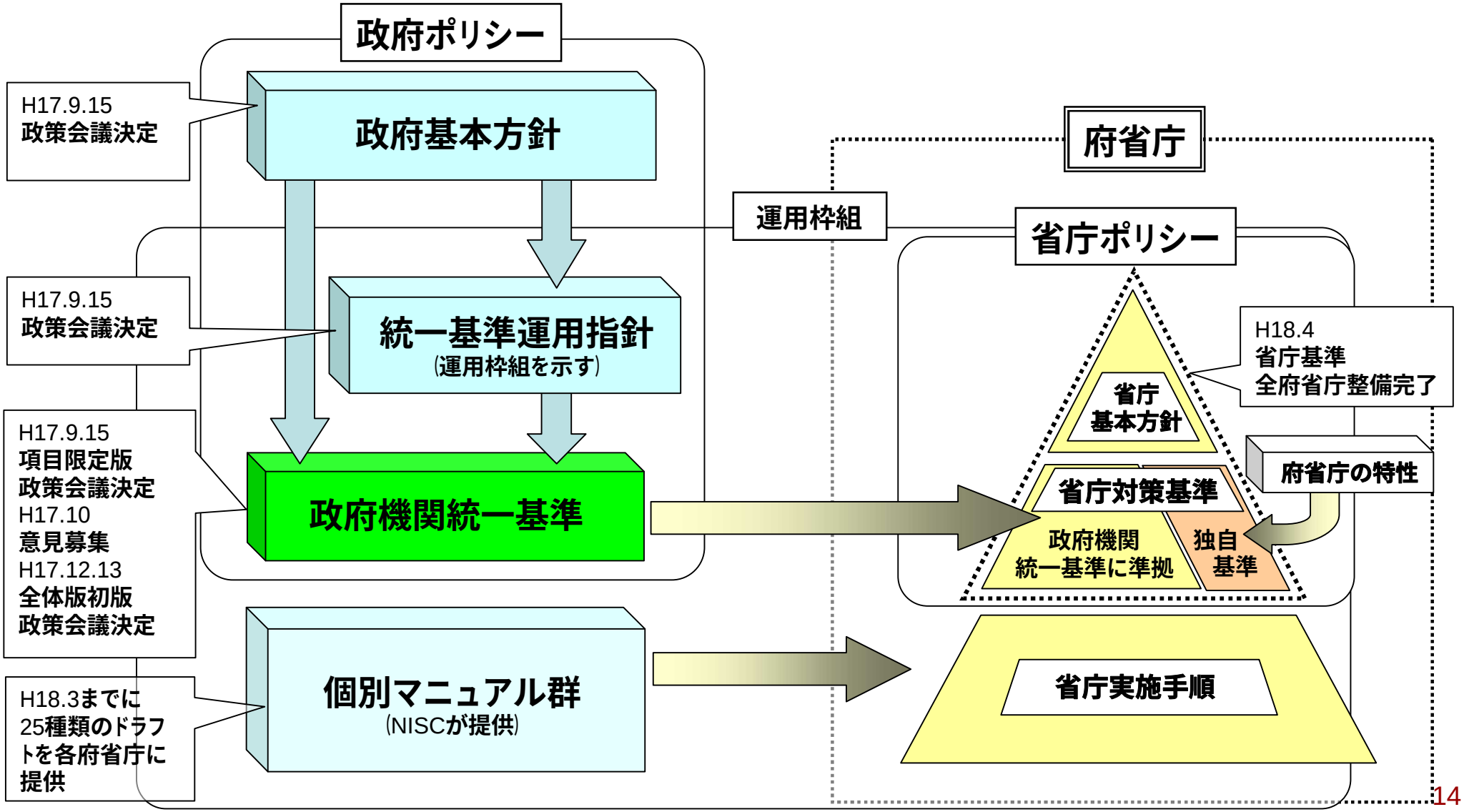
② 各府省庁の情報セキュリティ水準の向上



注）各府省庁は、これまで、「情報セキュリティポリシーに関するガイドライン」（平成12年7月14日情報セキュリティ対策推進会議決定）に基づき、それぞれ自らの責任において独自に情報セキュリティポリシーを策定し、対策を実施していた。

政府機関の情報セキュリティ対策の枠組み

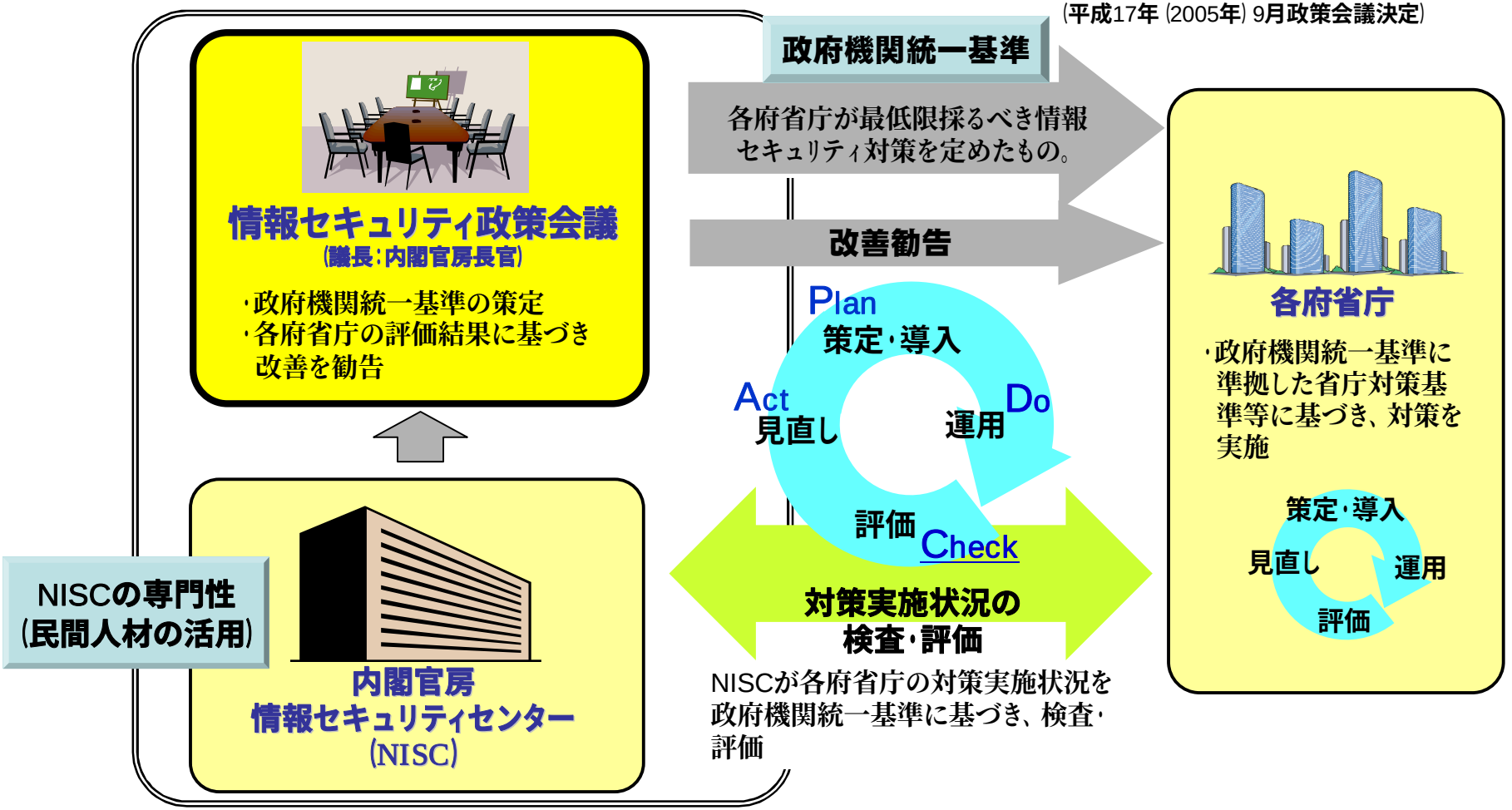
○政府全体としての情報セキュリティ水準の向上を図るため、「政府機関の情報セキュリティ対策のための統一基準」（政府機関統一基準）を策定。（平成17年（2005年）9月策定）



「政府機関統一基準」に基づく政府機関の情報セキュリティ対策の枠組み

○ 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）



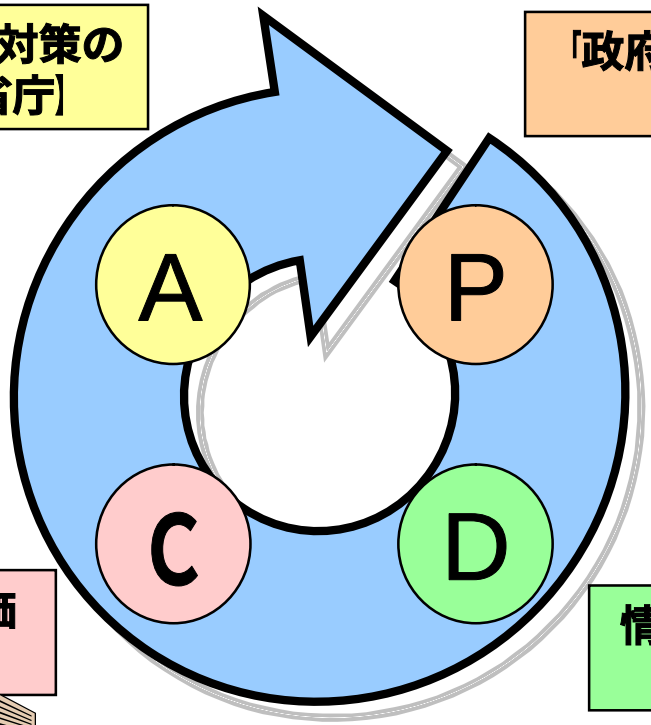
「政府機関統一基準」に基づくPDCAサイクル

「政府機関統一基準」の
定例見直し【NISC】

情報セキュリティ対策の
見直し【各府省庁】

各省庁対策の総合評価・
勧告【政策会議】

各省庁対策の検査・評価
【NISC】



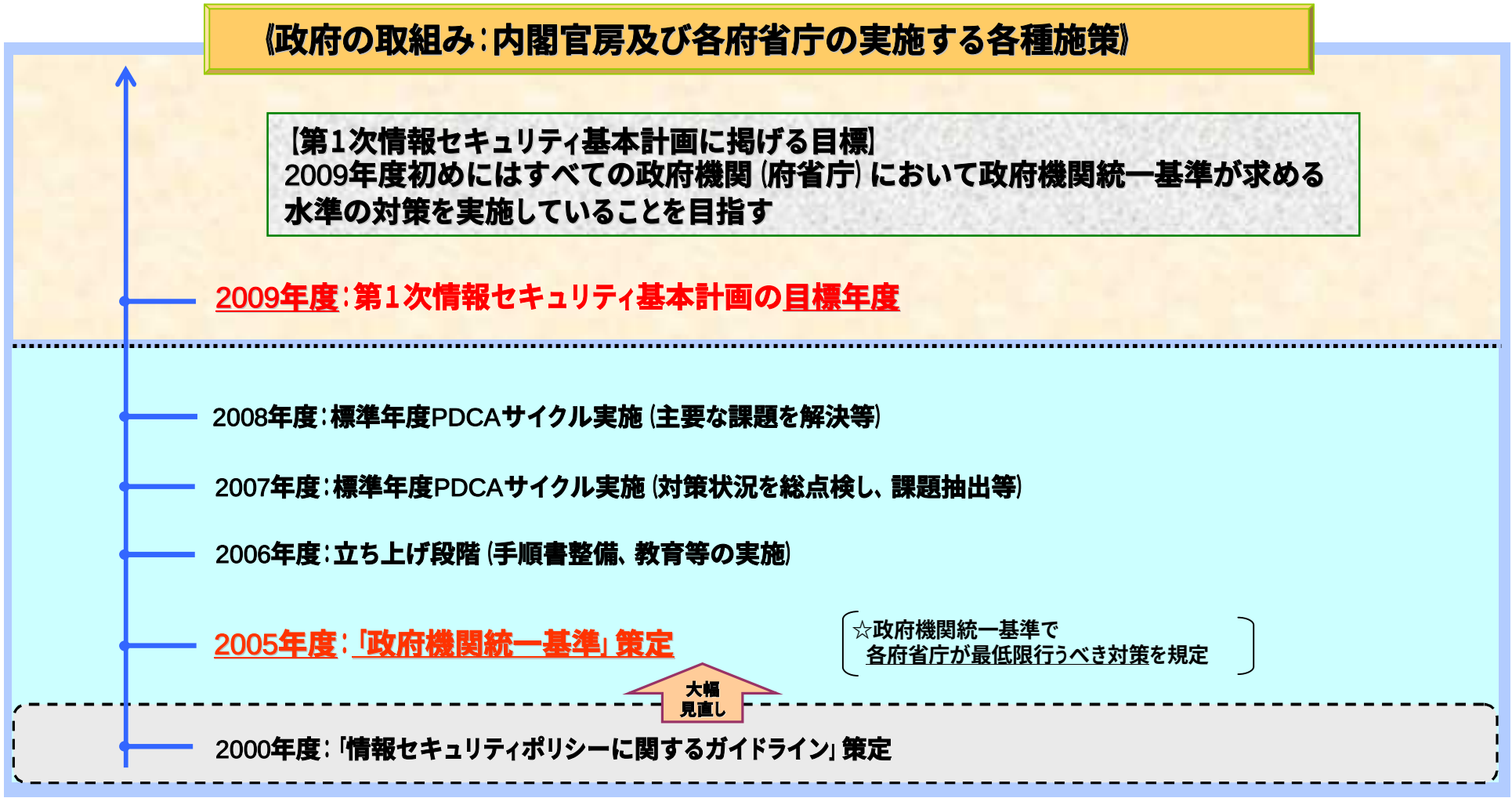
「政府機関統一基準」策定
【政策会議】

「省庁基準」へ反映
【各府省庁】

情報セキュリティ対策実施
【各府省庁】

政府機関における情報セキュリティ対策の強化 【第1次情報セキュリティ基本計画】

2009年度初めにはすべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指し、政府全体としてPDCAサイクルを確立する。



政府機関統一基準の構成

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）
- ○ 違反と例外措置
- ○ 情報セキュリティ対策の教育
- ○ 障害等の対応
- ○ 情報セキュリティ対策の自己点検
- ○ 情報セキュリティ対策の監査
- ○ 見直し

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

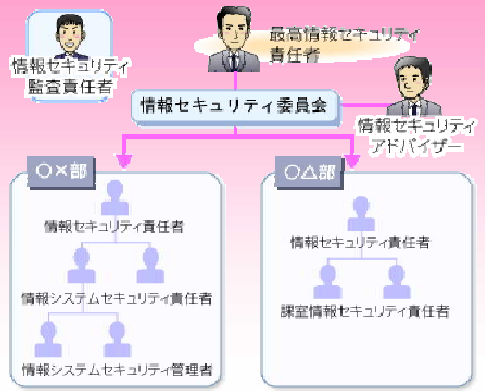
第5部　情報システムの構成要素についての対策
- ○ 安全区域
- ○ 電子計算機（共通、端末、サーバ）
- ○ アプリケーション（共通、電子メール、ウェブ）
- ○ 通信回線（共通、庁内、庁外）

第6部　個別事項についての対策
- ○ 機器等の購入
- ○ 外部委託
- ○ ソフトウェア開発
- ○ 府省庁外での情報処理（情報の持ち帰り等）の制限
- ○ 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
- ○ その他

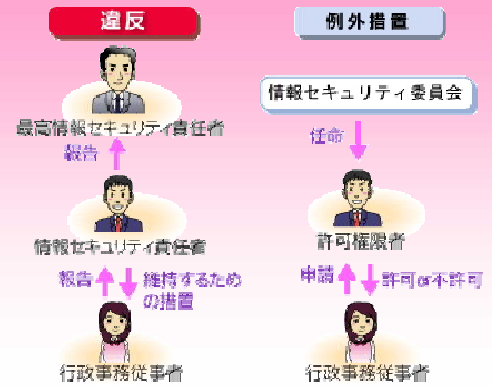
政府機関統一基準の概要①

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：84（基本：81、強化：3）

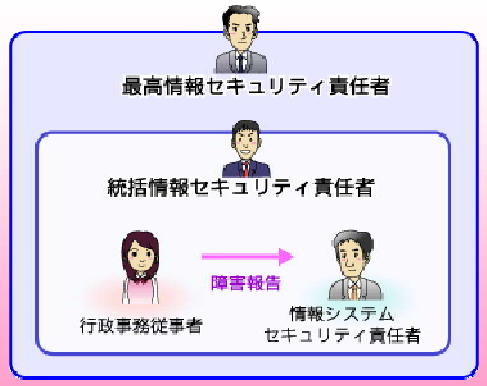


【組織・体制の確立・役割の分離】

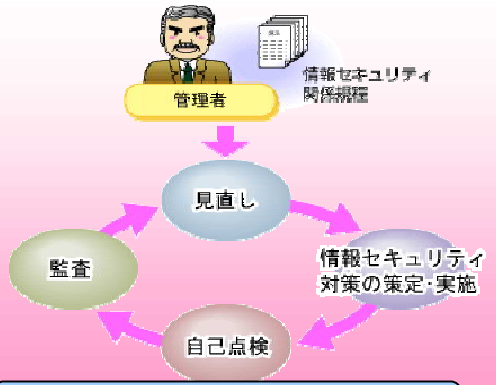


【違反の対応と例外措置の適用】

【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】

第3部～第6部　情報の適切な取扱い、情報システムに必要となる情報セキュリティ機能等

政府機関統一基準の概要②

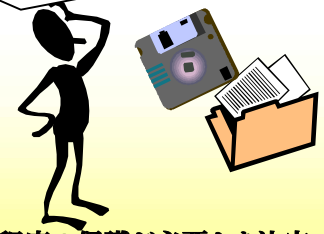
第3部　情報についての対策

※　主に情報システムの利用者が実施する対策
遵守事項数：　42（基本：38、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

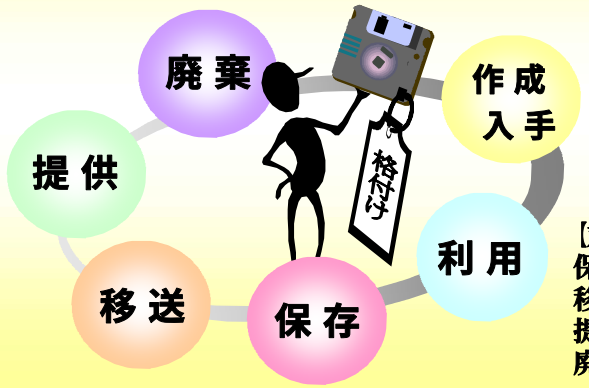


どの程度の保護が必要かを決定

【格付けの明示】

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
遵守事項数：125（基本：85、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