資料7

NISC National Information Security Center

政府機関における情報セキュリティ問題への取組み

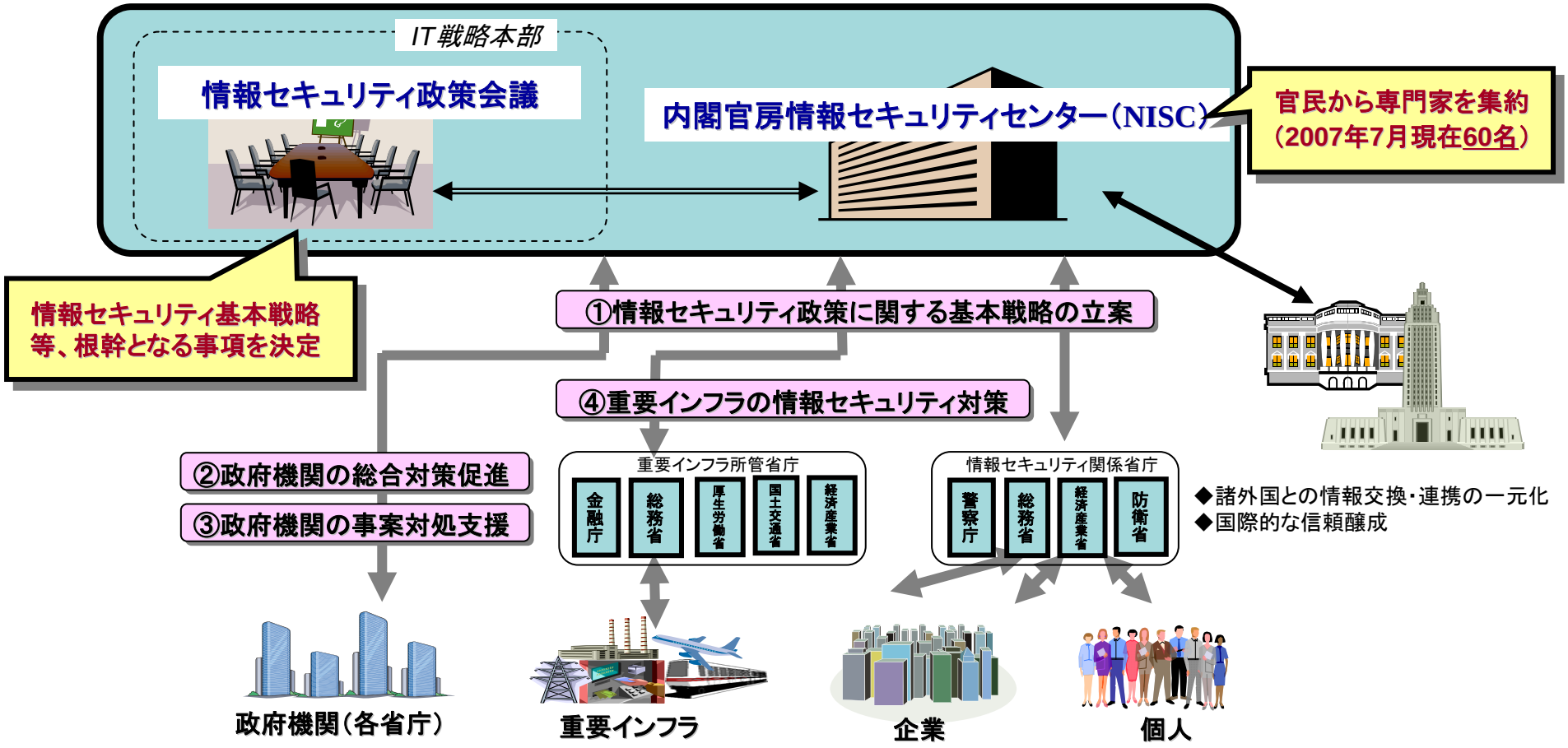
～ 政府機関統一基準に基づく対策 ～

2007年7月18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

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

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

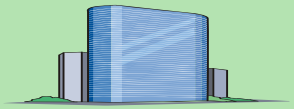
事案対処支援
- 早期警戒情報の収集・分析機能の強化
- 情報セキュリティ関係機関との連携強化　等

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

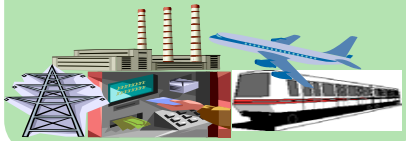
国際戦略
- 情報セキュリティに関する我が国の国際戦略の立案
- 諸外国の関係機関等との緊密な連携　等

企業　個人

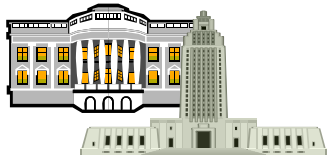
各政府組織



重要インフラ



諸外国関係機関



政府機関の情報セキュリティ対策の整合化・共通化

➢ 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。

これまでの各省庁の情報セキュリティ対策	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	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	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	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

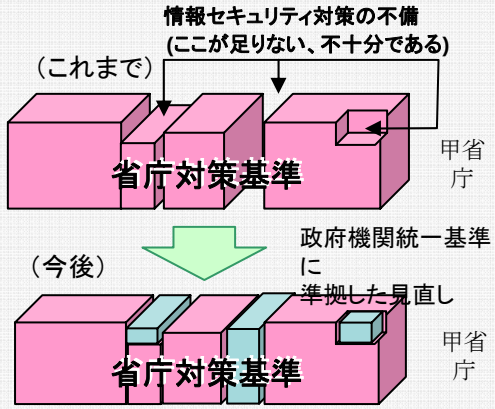
バラバラ解消

穴が埋まる

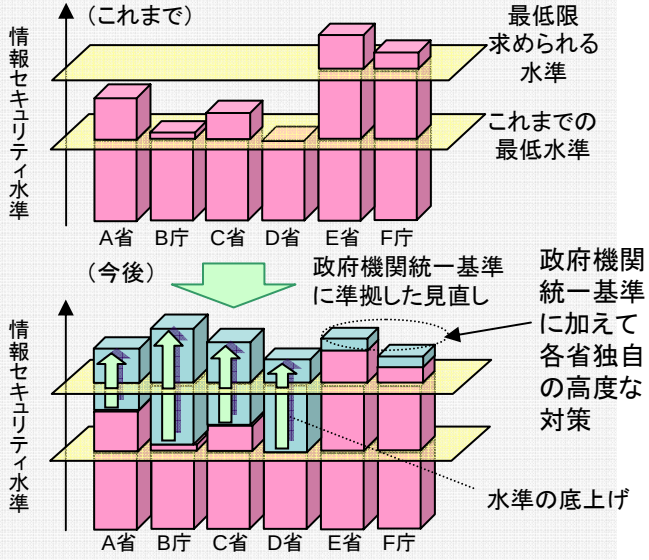
迅速・的確

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

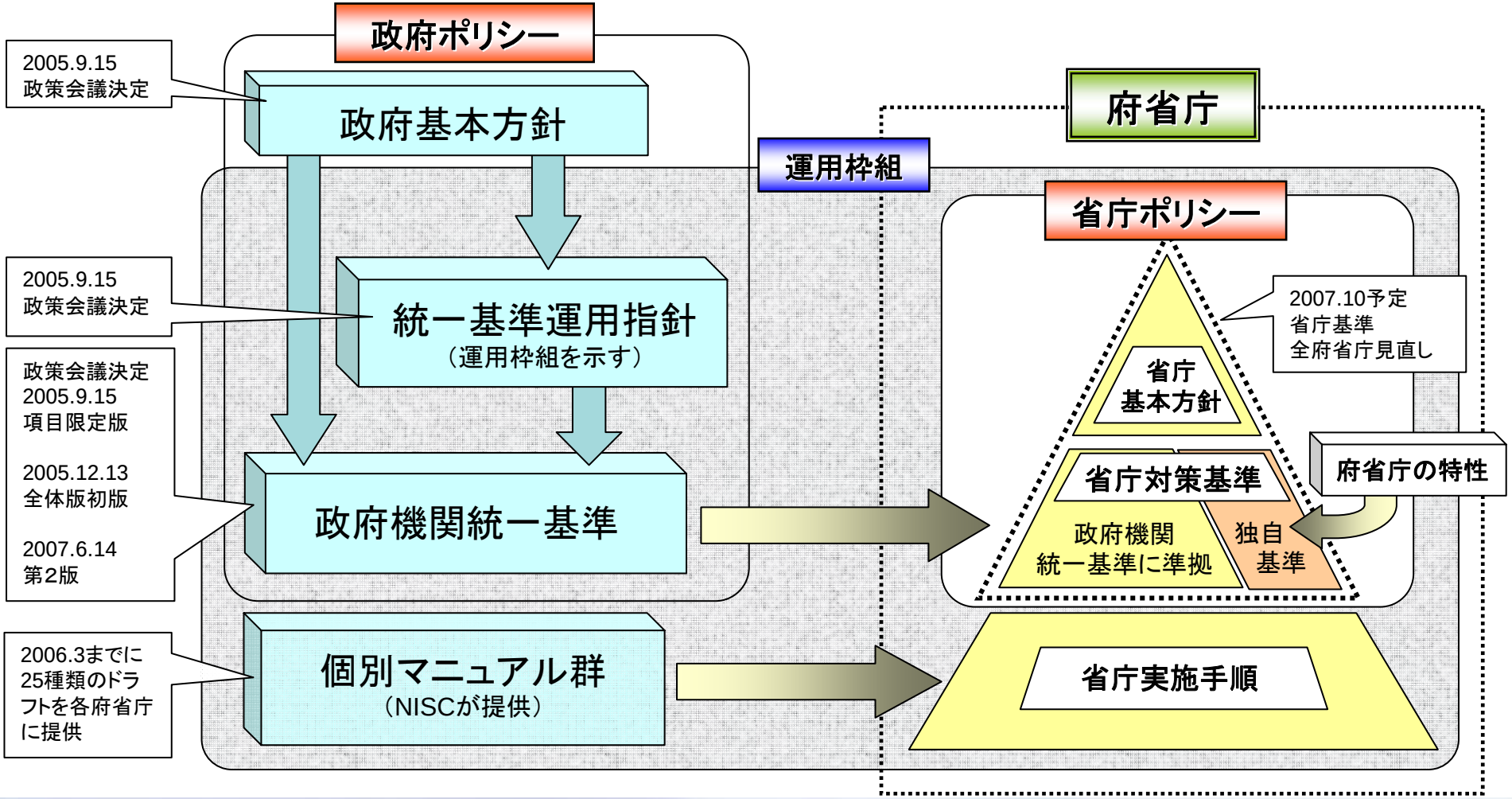


② 各府省庁の情報セキュリティ水準の向上



政府機関の情報セキュリティ対策の枠組み(1)

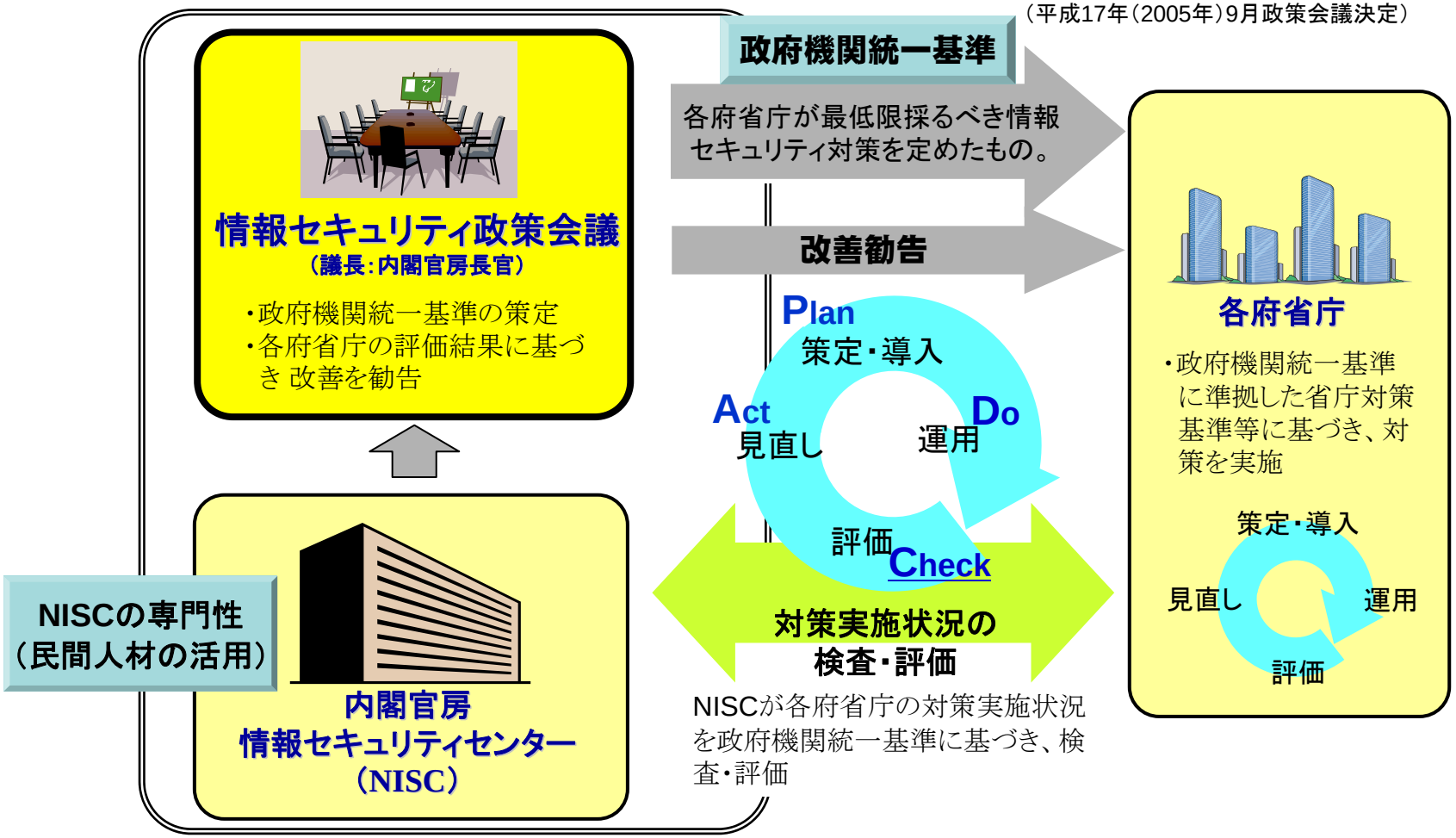
➢ **政府全体としての情報セキュリティ水準の向上を図る**ため、**「政府機関の情報セキュリティ対策のための統一基準」(政府機関統一基準)**を策定(2005年12月策定、2007年6月改訂)



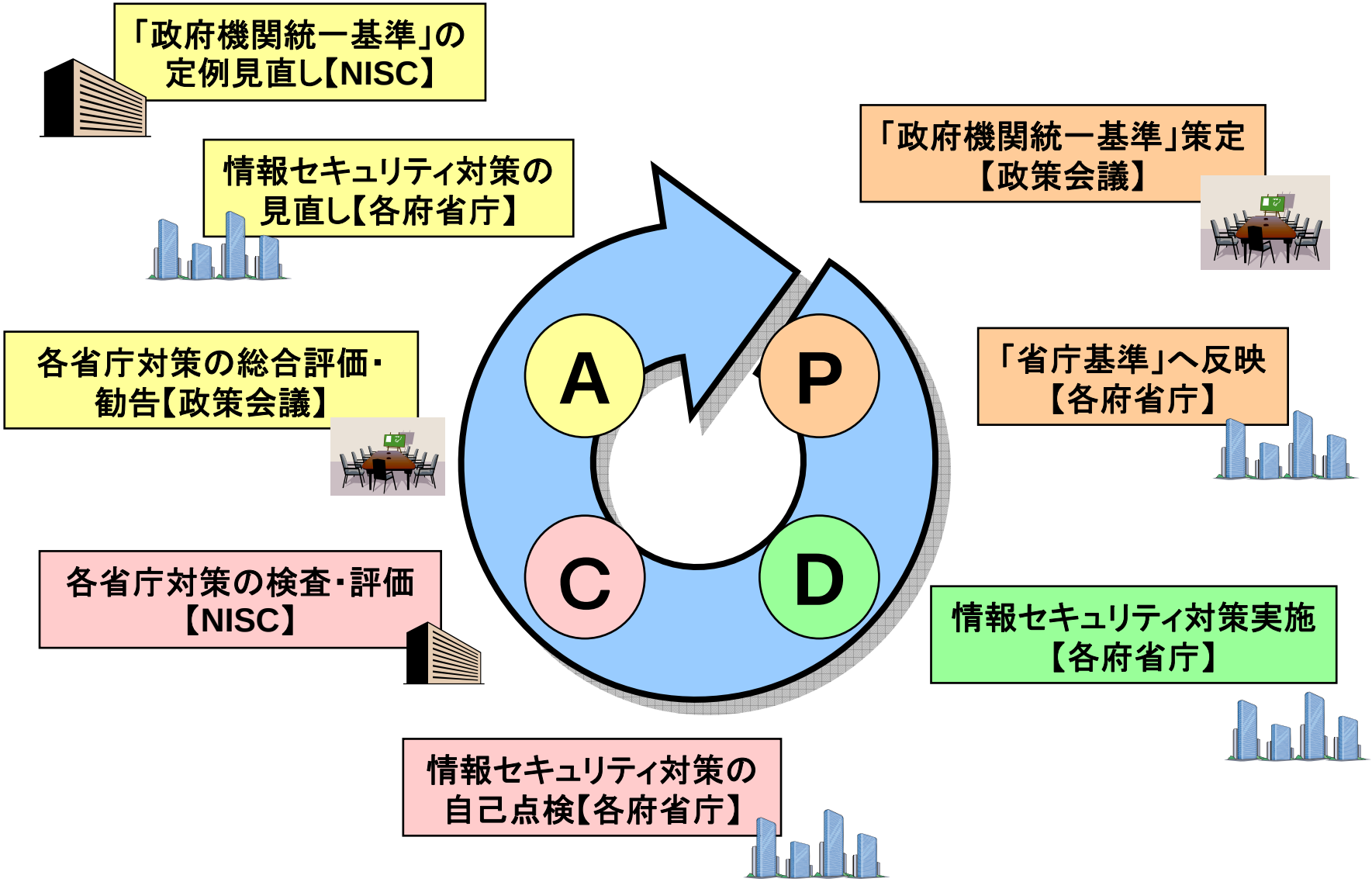
政府機関の情報セキュリティ対策の枠組み(2)

➢ 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



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）
- ○ 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）

各府省庁からの対策実施状況報告(2006年度)の概要

【報告の概要】 報告内容 ：政府機関統一基準の基本遵守事項について、**責務が発生した場合の対策の措置状況**等

報告対象 ：・ 情報セキュリティ責任者等、**情報セキュリティに係る役割を担う者**
・ **本府省庁課長相当職以上**の行政事務従事者(地方支分部局を含む。)
・ **電子申請ｼｽﾃﾑ**、**文書管理ｼｽﾃﾑ**、**府省庁LAN**及び**最適化対象ｼｽﾃﾑ**(個別府省業務・ｼｽﾃﾑ)

統一基準の構成	記載内容(抜粋)
第2部　組織と体制	管理体制の確立、ｾｷｭﾘﾃｨ教育、自己点検、監査
第3部　情報の取扱い	情報の格付け、情報の作成・利用等取扱いに係る対策
第4部　情報ｾｷｭﾘﾃｨ機能等	ﾕｰｻﾞ認証機能、ﾛｸﾞ管理機能、暗号・電子署名、不正ﾌﾟﾛｸﾞﾗﾑ対策
第5部　情報ｼｽﾃﾑの構成要素	安全区域、端末・ｻｰﾊﾞ、ｱﾌﾟﾘｹｰｼｮﾝ(ﾒｰﾙ・ｳｪﾌﾞ)に係る対策
第6部　個別事項	機器等購入、外部委託、庁舎外情報処理、私物ﾊﾟｿｺﾝ利用に係る対策

①実施率・②到達率による分析

【把握した主な課題】

今後、改善が求められる事項

行政事務従事者

第3部　情報の取扱い
○ 情報の格付け・取扱制限に係る措置

第5部　情報ｼｽﾃﾑの構成要素
○ 安全区域内における職員識別の徹底

情報セキュリティ責任者等

第2部　組織と体制
○ 情報セキュリティ教育及び情報セキュリティ監査の実施

第4部　情報セキュリティ機能等
○ 電子署名の付与に必要な機能の導入

第6部　個別事項
○ 外部委託先のアクセス範囲等に係る基準の整備

統一基準の導入初年度であり、十分な実施状況ではないが、課題は明確にされた。

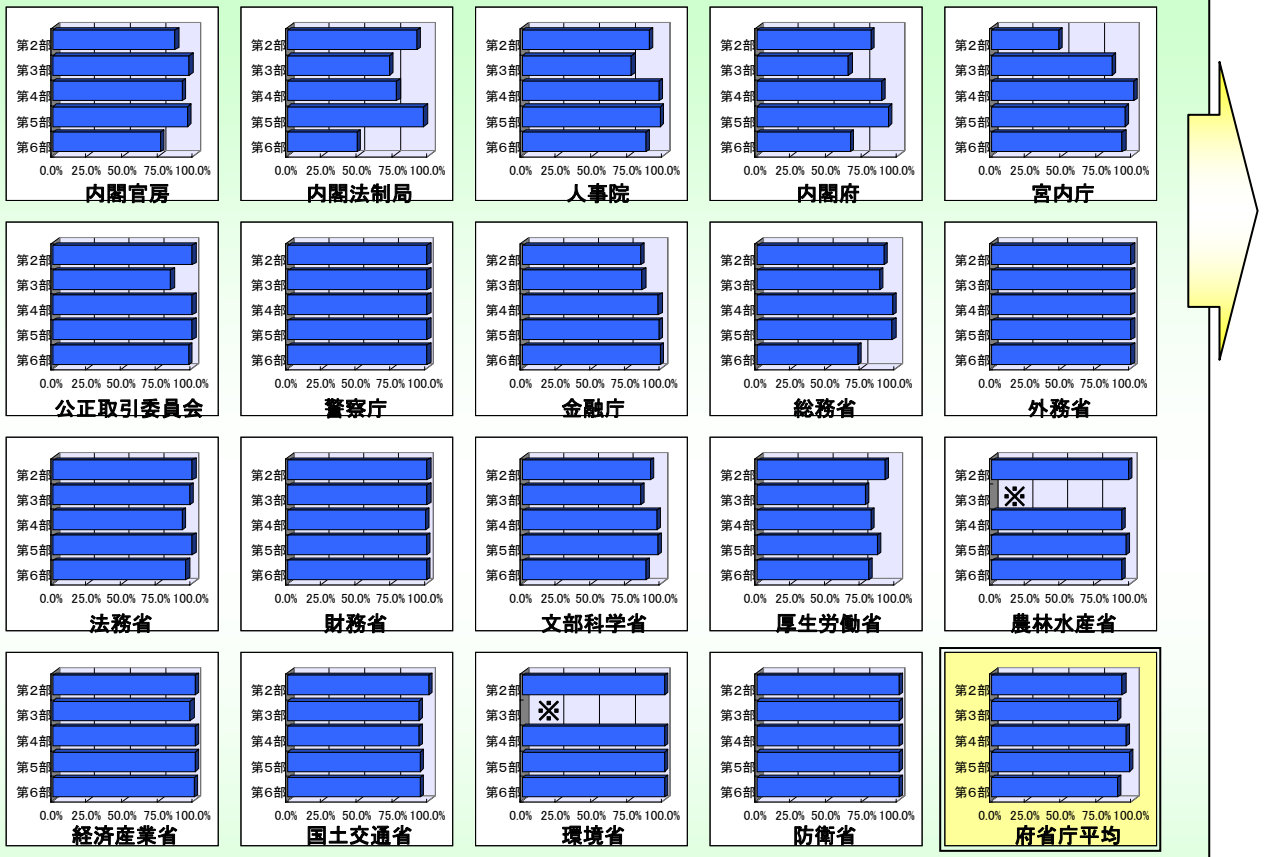
各府省庁の対策実施状況報告(2006年度)の集計結果　①:実施率

各府省庁からNISCへの報告

機関名	把握率
内閣官房	99.2 %
内閣法制局	95.9 %
人事院	99.9 %
内閣府	73.5 %
宮内庁	100.0 %
公正取引委員会	99.2 %
警察庁	100.0 %
金融庁	63.3 %
総務省	97.6 %
外務省	100.0 %
法務省	100.0 %
財務省	100.0 %
文部科学省	100.0 %
厚生労働省	95.7 %
農林水産省 (独自の調査を含める場合)	31.2 % (98.2 %)
経済産業省	100.0 %
国土交通省	100.0 %
環境省 (独自の調査を含める場合)	40.7 % (94.2 %)
防衛省	94.1 %

※　2006年度においては報告対象を限定

実施率(把握した者のうち、責務が生じた者に占める対策を実施した者の割合の平均)



※:2006年度においては、独自の把握状況調査を実施(分析の対象から除外)

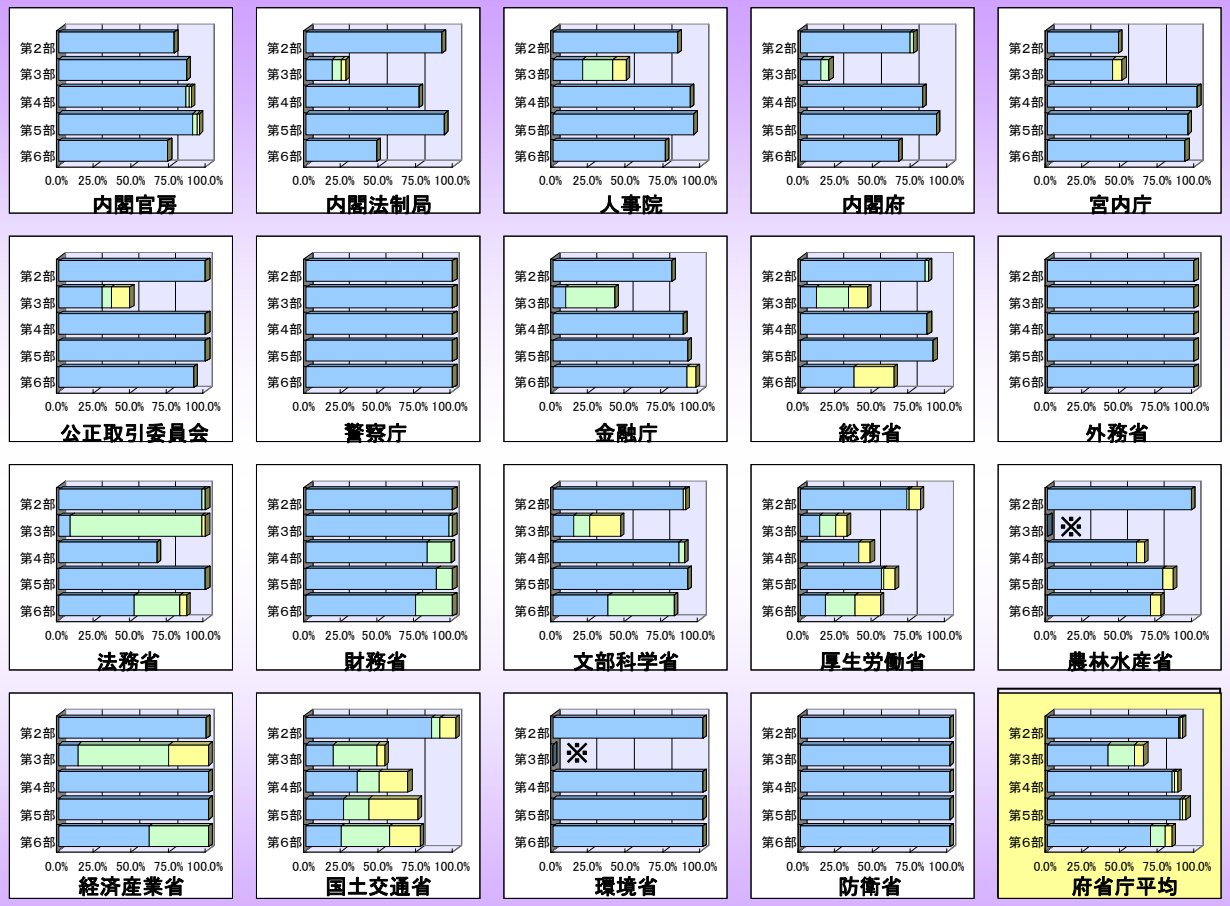
第2部　組織と体制
第3部　情報の取扱い
第4部　情報セキュリティ機能等
第5部　情報システムの構成要素
第6部　個別事項(外部委託等)

第〇部の集計(実施率の算出例)

	実施状況	割合	実施率
遵守事項(a)	2人中1人実施	50%	割合の単純平均 75%
遵守事項(b)	100人中75人実施	75%	
遵守事項(c)	10人中10人実施	100%	

各府省庁の対策実施状況報告(2006年度)の集計結果　②:到達率

到達率(把握した者のうち、責務が生じた全員が対策を実施した遵守事項の割合)



第2部　組織と体制
第3部　情報の取扱い
第4部　情報セキュリティ機能等
第5部　情報システムの構成要素
第6部　個別事項(外部委託等)

※:2006年度においては、独自の把握状況調査を実施(分析の対象から除外)

全員が対策を実施した遵守事項の割合
95%以上の者が対策を実施した遵守事項の割合
90%以上の者が対策を実施した遵守事項の割合

集計方法と結果の見方

1. 報告内容の集計 ：

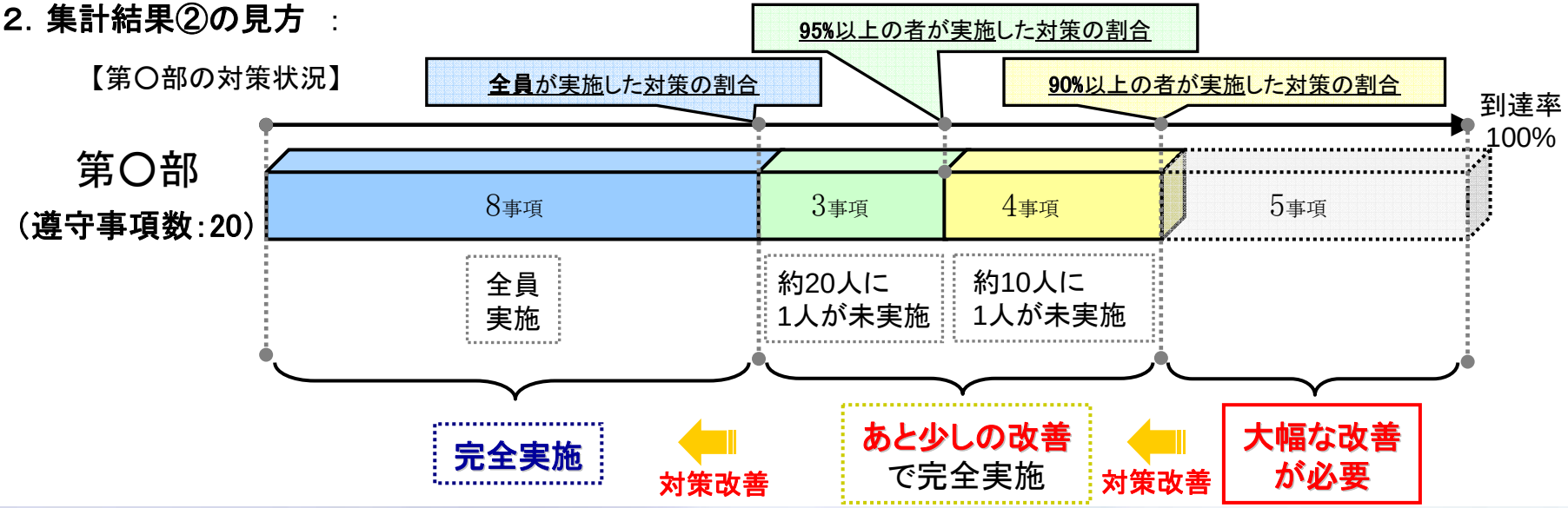
$$\text{把握率} = \frac{\Sigma(\text{各遵守事項について対策実施状況が把握できた者の数})}{\Sigma(\text{各遵守事項における報告対象者数})}$$

$$\text{実施率} = \frac{\Sigma(\text{各遵守事項について責務が生じた者に占める実施した者の割合})}{\text{責務が生じた遵守事項の数}} \qquad \text{実施率（政府平均）} = \frac{\Sigma(\text{各府省庁の実施率})}{\text{府省庁の数}}$$

$$\text{到達率} = \frac{\text{責務が生じた全員が必要な対策を実施した遵守事項の数}}{\text{責務が生じた遵守事項の数}} \qquad \text{到達率（政府平均）} = \frac{\Sigma(\text{各府省庁の到達率})}{\text{府省庁の数}}$$

2. 集計結果②の見方 ：

【第〇部の対策状況】

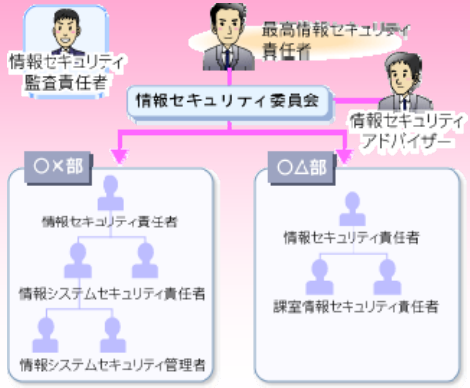


（参考） 政府機関統一基準の概要①

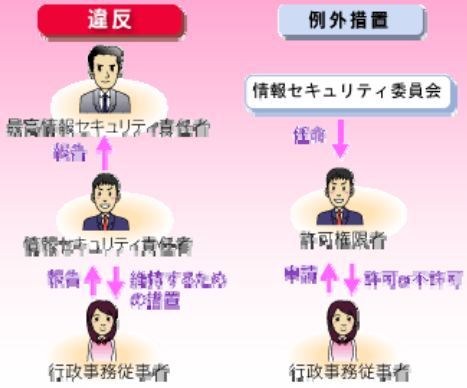
第1部　総則（政府機関統一基準の位置付け、用語定義等）

第2部　組織と体制の構築

遵守事項数：88（基本：85、強化：3）

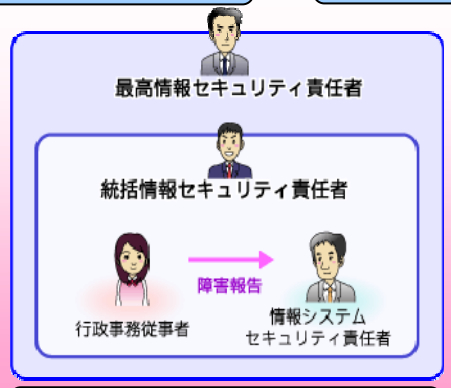


【組織・体制の確立・役割の分離】

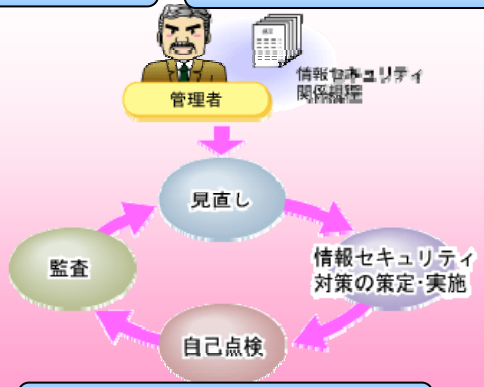


【違反の対応と例外措置の適用】

【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

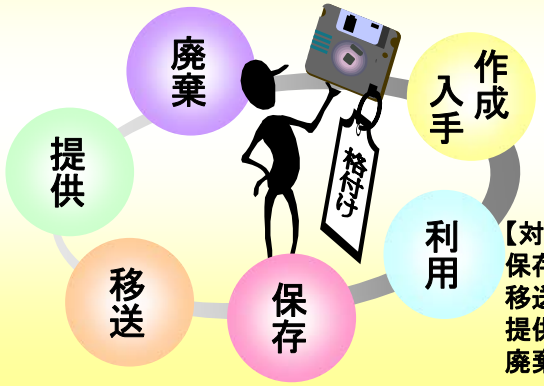
※　主に情報システムの利用者が実施する対策
遵守事項数：　45（基本：41、強化：　4）

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】　【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】

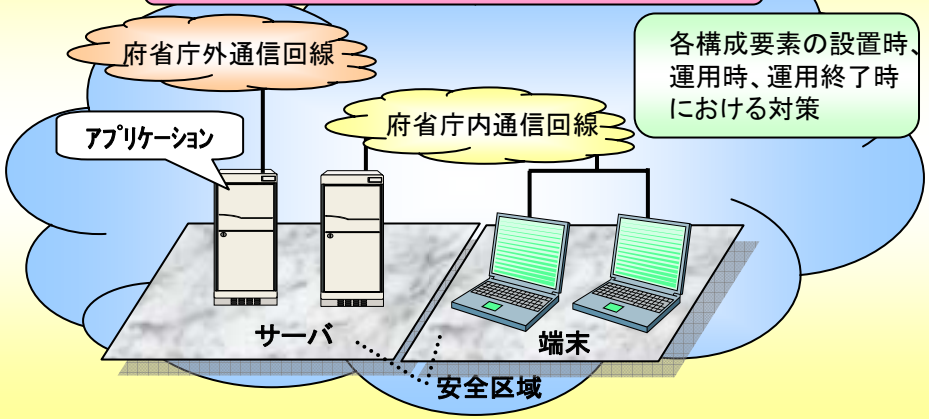
情報システムのライフサイクル（計画、設計、構築、運用、監視、移行、廃棄、見直し）に則し、セキュリティの観点から考慮すべき要件

（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対策の検討】



【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