

# 我が国のセキュリティ政策の現状と方向性

2008年3月

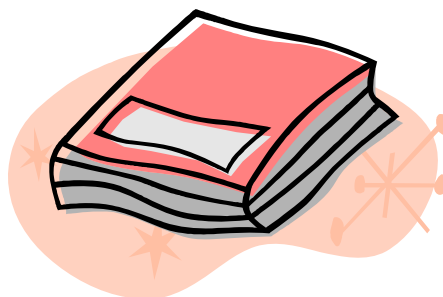
豊内 順一

内閣官房情報セキュリティセンター(NISC)

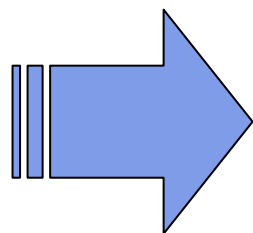
<http://www.nisc.go.jp/>

わが国の情報セキュリティ政策は  
「情報セキュリティ基本計画」に従って実施

3ヵ年計画



第一次  
情報セキュリティ基本計画



年度計画



セキュア・ジャパン2006  
セキュア・ジャパン2007  
セキュア・ジャパン2008

(159施策)

- ◆ . . . . .
- ◆ 重要インフラ横断的な研究的演習及び机上演習の実施
- ◆ 政府統一基準の見直し
- ◆ . . . . .
- ◆ **セキュアVMの開発**
- ◆ . . . . .
- ◆ . . . . .

- セキュア・ジャパン2006に基づいた取組みへの評価と分析を踏まえ、「第1次情報セキュリティ基本計画」の実現に向けた2年目の取組みをまとめる。
- セキュリティ対策を推進する体制の維持や対策が不十分な部分の底上げを含め、対策推進の安定化を図る
- 2007年度に実施する具体的行動計画と、2008年度の重点施策の方向性を示す

## ＜基本計画を実現するための取組みの底上げ＞

「第1次情報セキュリティ基本計画」(2006年度～2008年度)の実現に向け、取組みの底上げを含む二年目の取組み

## ＜2006年度末の状況認識・評価を踏まえた取組みの方向性＞

- 政府機関対策の徹底と定着に向けた取組拡充
- 取組が遅れがちな対策実施主体への対策強化
- 2006年度の取組みで不足感が目立った対策実施のための体制・人員の充実
- 国際的相互依存関係の深化などを踏まえた国際対応の本格化
- 喫緊の課題として、迅速かつ集中的に、電子政府の情報セキュリティ強化の取組みを推進

## ＜セキュア・ジャパン2007のポイントと主な具体策＞

### 政府機関情報セキュリティ対策の拡充

- 政府機関統一基準に基づくPDCAサイクルの定着化及び対策実施状況等の本格的な評価を行い、結果を公表
- 内閣官房を中心としたサイバー攻撃等に関する情報収集、分析・解析機能(GSOC)の構築

### 対策が遅れがちな主体への対策の普及

- 小中高等学校における情報セキュリティ教育を実施
- 「インターネット安全教室」等による普及啓発を実施
- 中小企業における情報セキュリティ対策の推進
- 分野横断的な重要インフラ連絡協議会創設の検討

### 情報セキュリティ基盤強化に向けた集中的な取組み

→ 2008年度の重点施策の方向性

- 政府機関における情報セキュリティ人材の重点確保
- 情報セキュリティ政策の国際展開に向けた集中的な取組み
- 電子政府のシステム設計段階からのセキュリティの確保

## 最近の情報セキュリティ上の脅威について

# 情報セキュリティを取り巻く最近の世界的な動向 (ITに起因する脅威)



## ● 攻撃の巧妙化、ビジネス化

政府機関のHPの改ざん、ウィルスの頒布等を通じた愉快犯的な行動

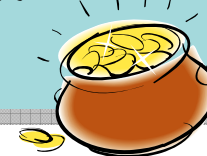
- ・全世界へのウィルスの頒布
- ・中央省庁のHP改ざん 等



社会・経済活動のICT依存の高まり

経済的利得を目的として組織化・高度化

- ・技術情報、営業秘密の流出(情報漏洩)
- ・個人情報等に関する闇市場の成立
- ・攻撃手法の売買 (Mpack等)



## 1. アンダーグラウンドエコノミーで取引された商品の内訳

ランク	商品	割合(%)	価格帯
1	クレジットカード	22	\$0.50-\$5
2	銀行口座	21	\$30-\$400
3	電子メールのパスワード	8	\$1-\$350
4	メーラー	8	\$8-\$10
5	電子メールアドレス	6	\$2/MB-\$4/MB
6	プロキシ	6	\$0.50-\$3
7	完全な個人識別情報	6	\$10-\$150
8	詐欺	6	\$10/週
9	社会保障番号	3	\$5-\$7
10	安全性が低下したUNIX Shell	2	\$2-\$10

(Source:シマンテック)

## 2. 攻撃ツールの市場(概算)

脆弱性、Exploit Code	市場価値	情報源
Exploit コード*	2200万ー 2750万円**	米国政府
インターネットエクスプローラー	660万ー 1320万円**	H.D. Moore
Vista	550万円**	Trend Micro
Microsoft エクセル	1万3200円**	eBay オークションサイト

(Source: Charlie Miller, "The Legitimate Vulnerability Marketから抜粋)

\* 特定の脆弱性を突く攻撃を可能とするプログラムコードのことを指す

\*\*1ドル=110円により計算

# 情報セキュリティを取り巻く最近の世界的な動向 (ITに起因する脅威)



## ● 攻撃のボーダレス化

ネットワークのボーダレス性を利用し、国境を越えた攻撃が行われる

- ① ボット化したPCからのDoS(サービス停止)攻撃
- ② ウェブサイトの脆弱性につけ込んだ攻撃 等

## 意図的な攻撃活動の上位発信元

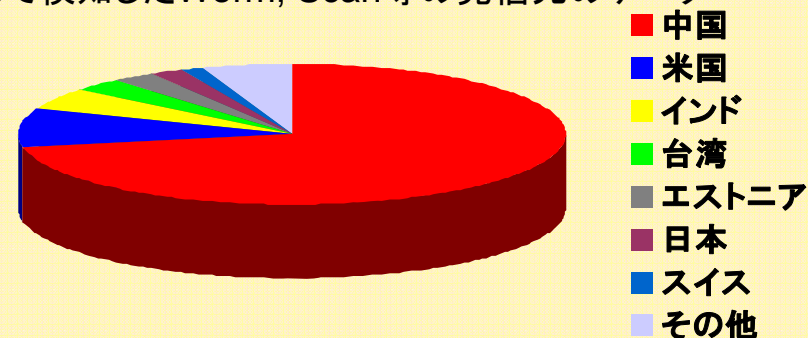
### 1. 世界向け

ランク	前期のランク	国名	割合
1	1	米国	30%
2	2	中国	10%
3	3	ドイツ	7%
4	5	英国	4%
5	4	フランス	4%
6	7	カナダ	4%
7	8	スペイン	3%
8	10	イタリア	3%
9	6	韓国	3%
10	11	日本	2%
		その他	30%

Source: シマンテック

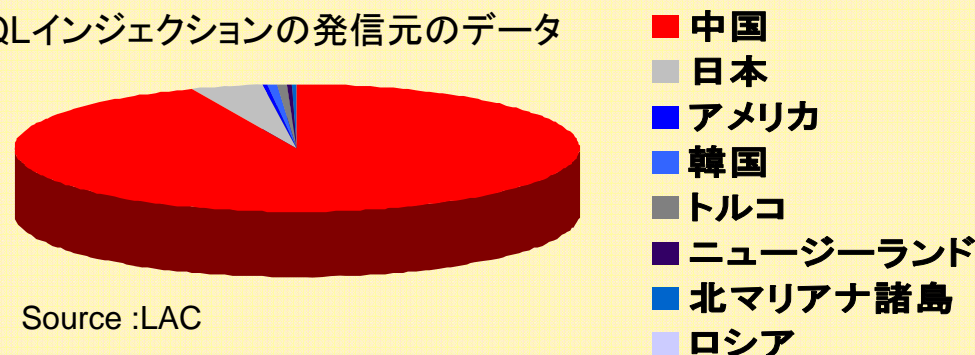
### 2. 日本向け

① IDSで検知したWorm, Scan等の発信元のデータ



Source : 不正侵入検知システムにおける不正なアクセスの検知分析(警察庁)

② SQLインジェクションの発信元のデータ



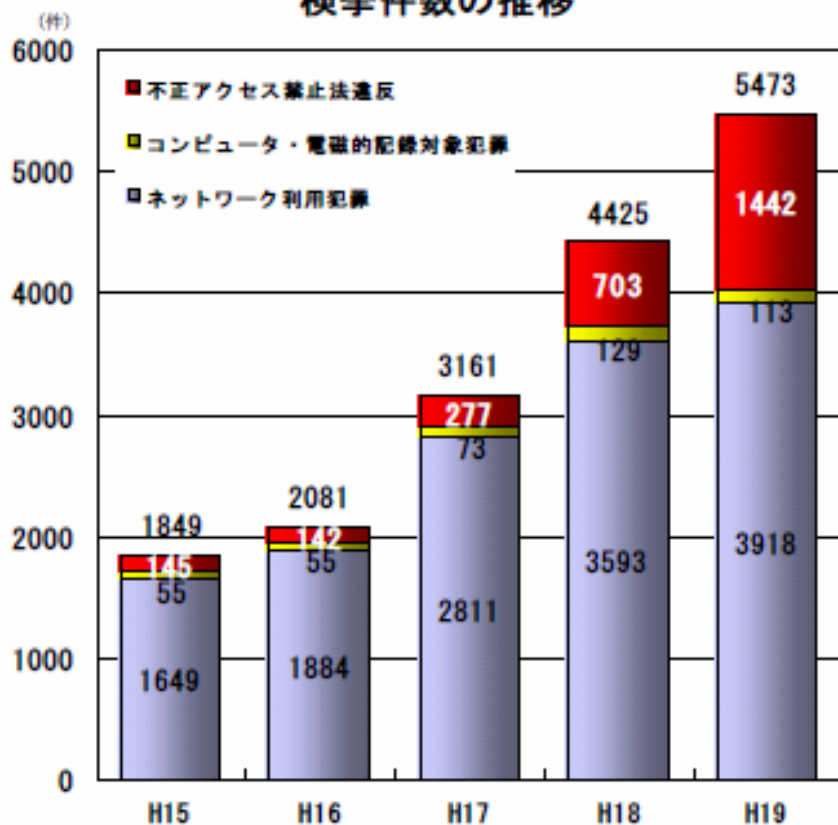
Source : LAC

# サイバー犯罪の増加



2007年中のサイバー犯罪の検挙件数は5,473件で前年(4,425件)より23.7%増加

検挙件数の推移



不正アクセス行為の認知件数の推移

区分	年次	平成15年	平成16年	平成17年	平成18年	平成19年
認知件数 (件)		212	356	592	946	1,818
海外からのアクセス		35	37	53	37	79
国内からのアクセス		158	303	487	855	1,684
アクセス元不明		19	16	52	54	55

不正アクセス行為後の行為の内訳

区分	年次	平成18年	平成19年
インターネット・オークションの不正操作 (件)		593	1,347
オンラインゲームの不正操作		257	246
インターネットバンキングの不正送金		39	113
情報の不正入手		14	55
ホームページの改ざん・消去		32	25
不正ファイルの蔵置		5	1
不明		2	0
その他		4	31

警察庁広報資料「平成19年中のサイバー犯罪の検挙状況等について」より抜粋

警察庁発表

# サイバー攻撃による脅威事例



## ソフトウェア等の脆弱性を狙った新たなサイバー攻撃の出現

### ゼロデイ攻撃 (zero-day attack)

ゼロデイ攻撃とは、OSやアプリケーションのセキュリティホールを修正するパッチが提供される以前に、そのホールを突いて攻撃を行うこと。

2006.5 Wordにゼロデイ攻撃 ~日本の政府機関を攻撃か

2006.8 一太郎を狙うゼロデイ攻撃 ~日本のユーザーがターゲットに

2007.8 Windowsに深刻な脆弱性 ~ゼロデイ攻撃が発生

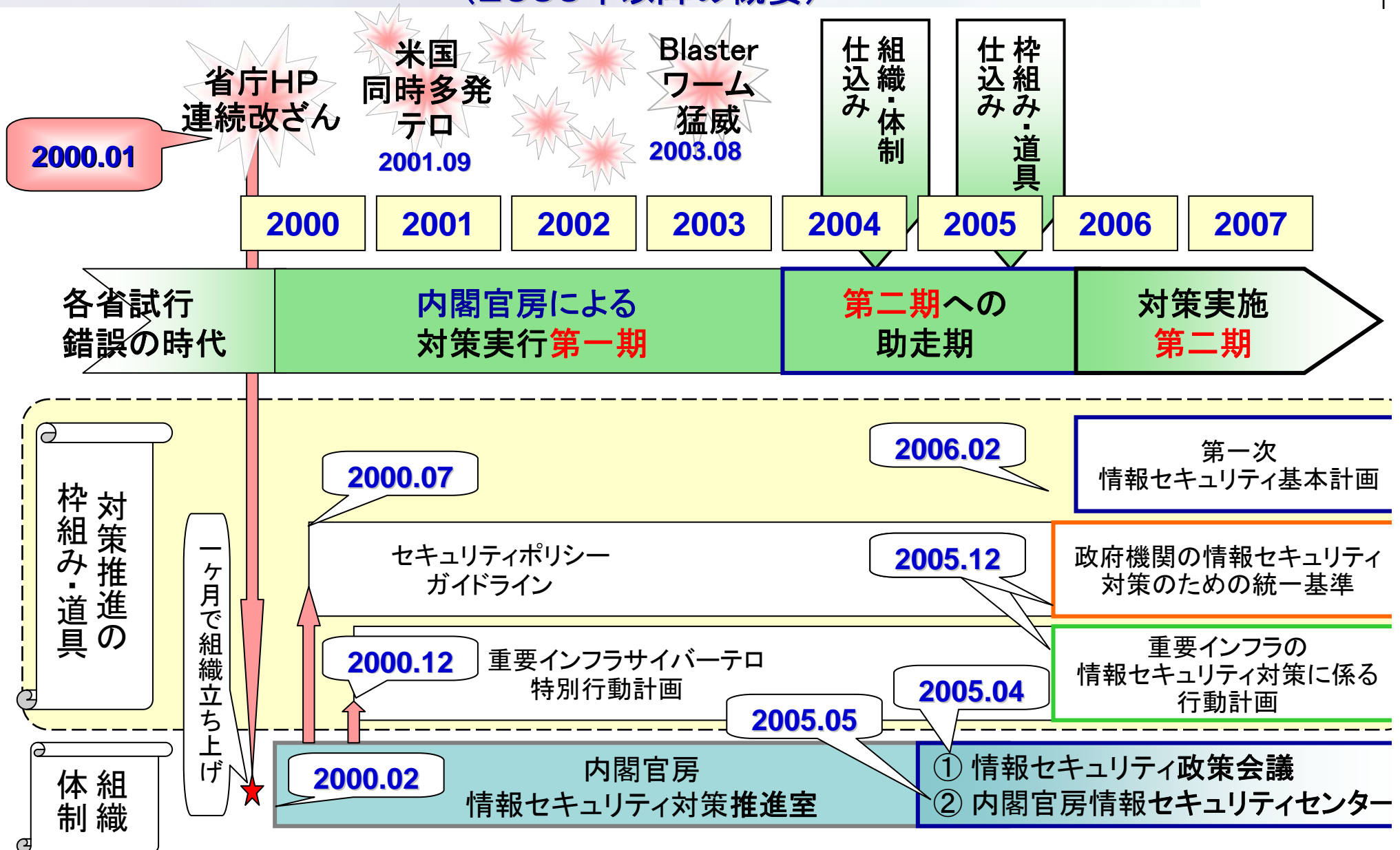
### 脆弱性関連情報の四半期別届出件数の推移



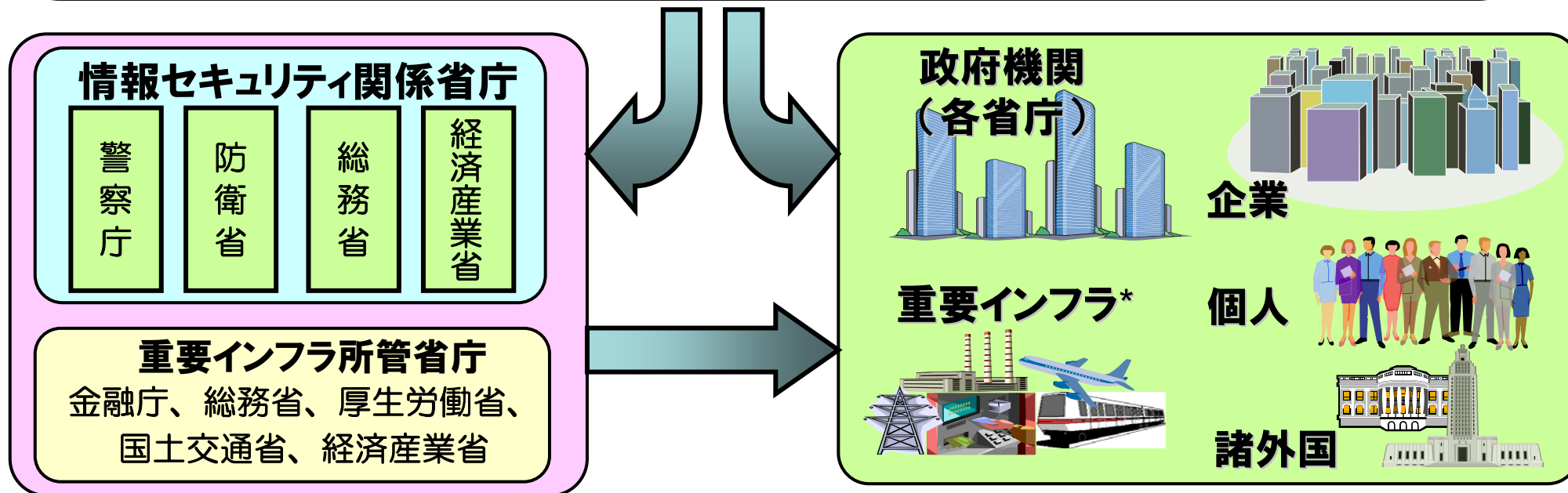
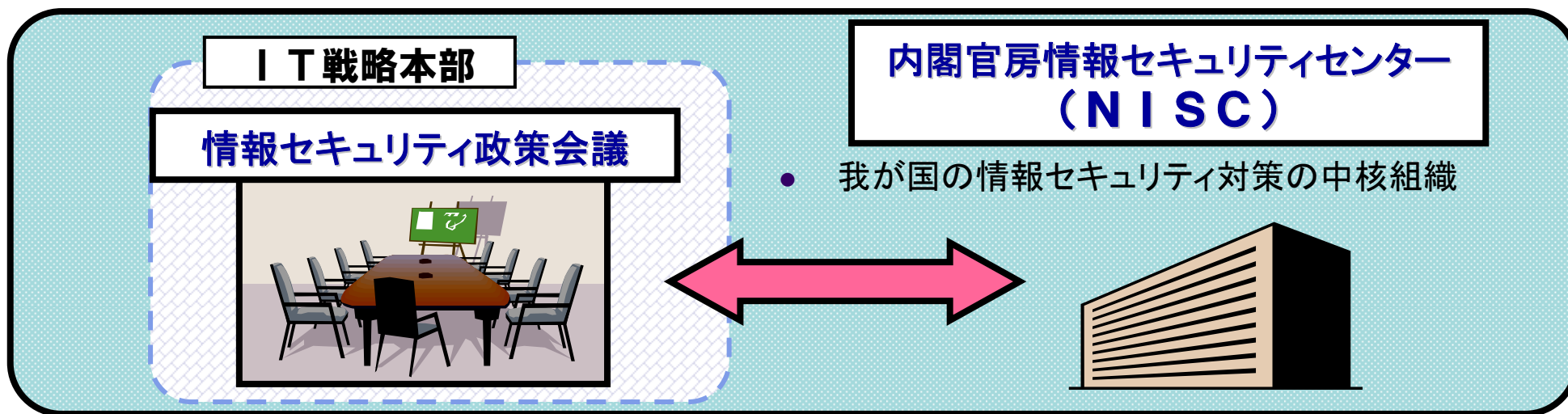
IPA、JPCERT/CC:ソフトウェア等の脆弱性関連情報に関する届出状況[2007年度 第3四半期(7月~9月)より抜粋]

## 政府中核機能の整備

# 内閣官房における情報セキュリティ政策の流れ (2000年以降の概要)



# 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



\*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)

# 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

内閣府特命担当大臣(科学技術政策)

## 構成員

国家公安委員会委員長

総務大臣

経済産業大臣

防衛大臣

江畑 謙介 拓殖大学客員教授／軍事評論家

小野寺 正 KDDI株式会社代表取締役社長

黒川 博昭 富士通株式会社代表取締役社長

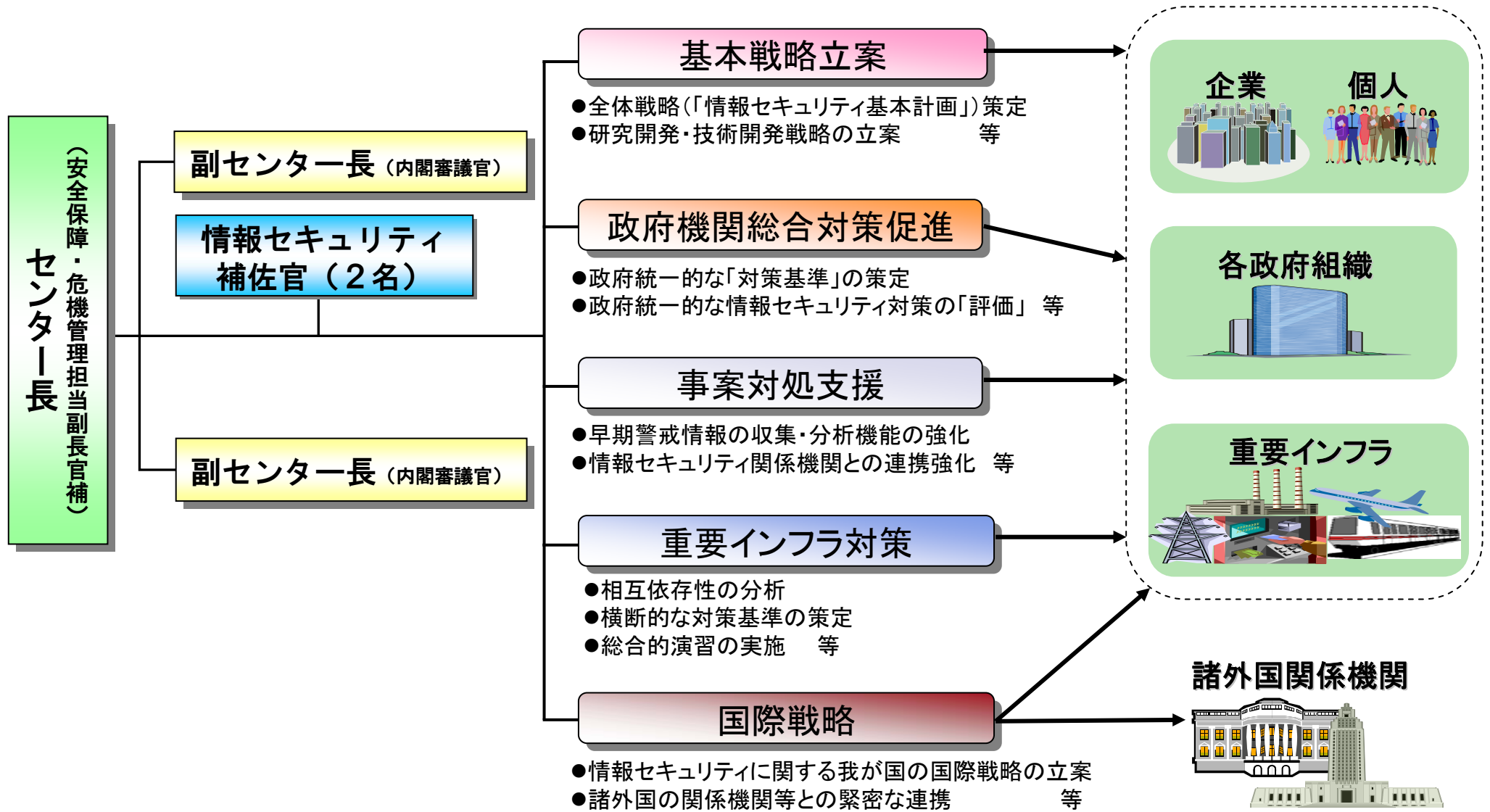
野原 佐和子 株式会社イプシ・マーケティング研究所代表取締役社長

前田 雅英 首都大学東京教授

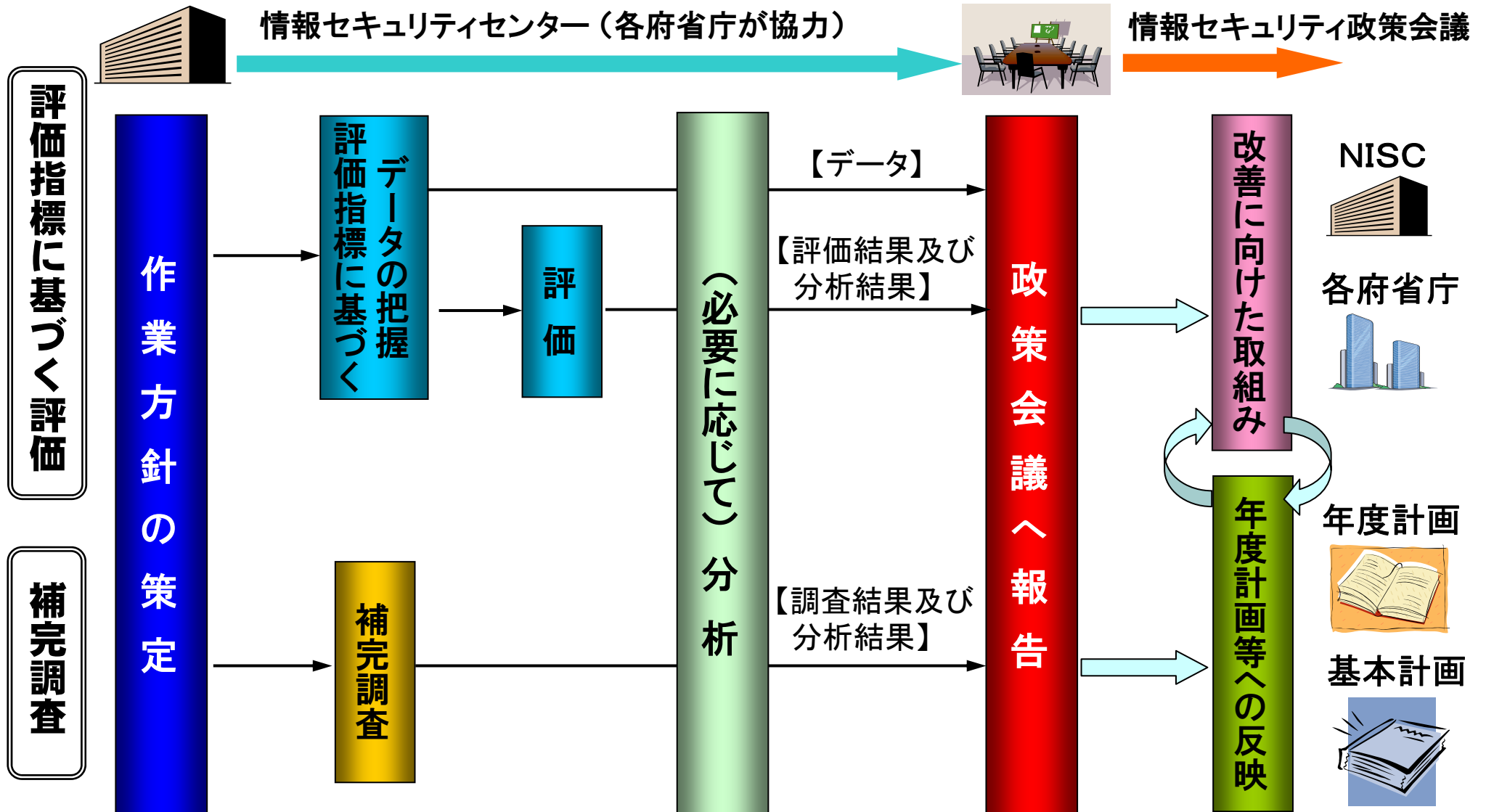
村井 純 慶應義塾大学教授

*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*

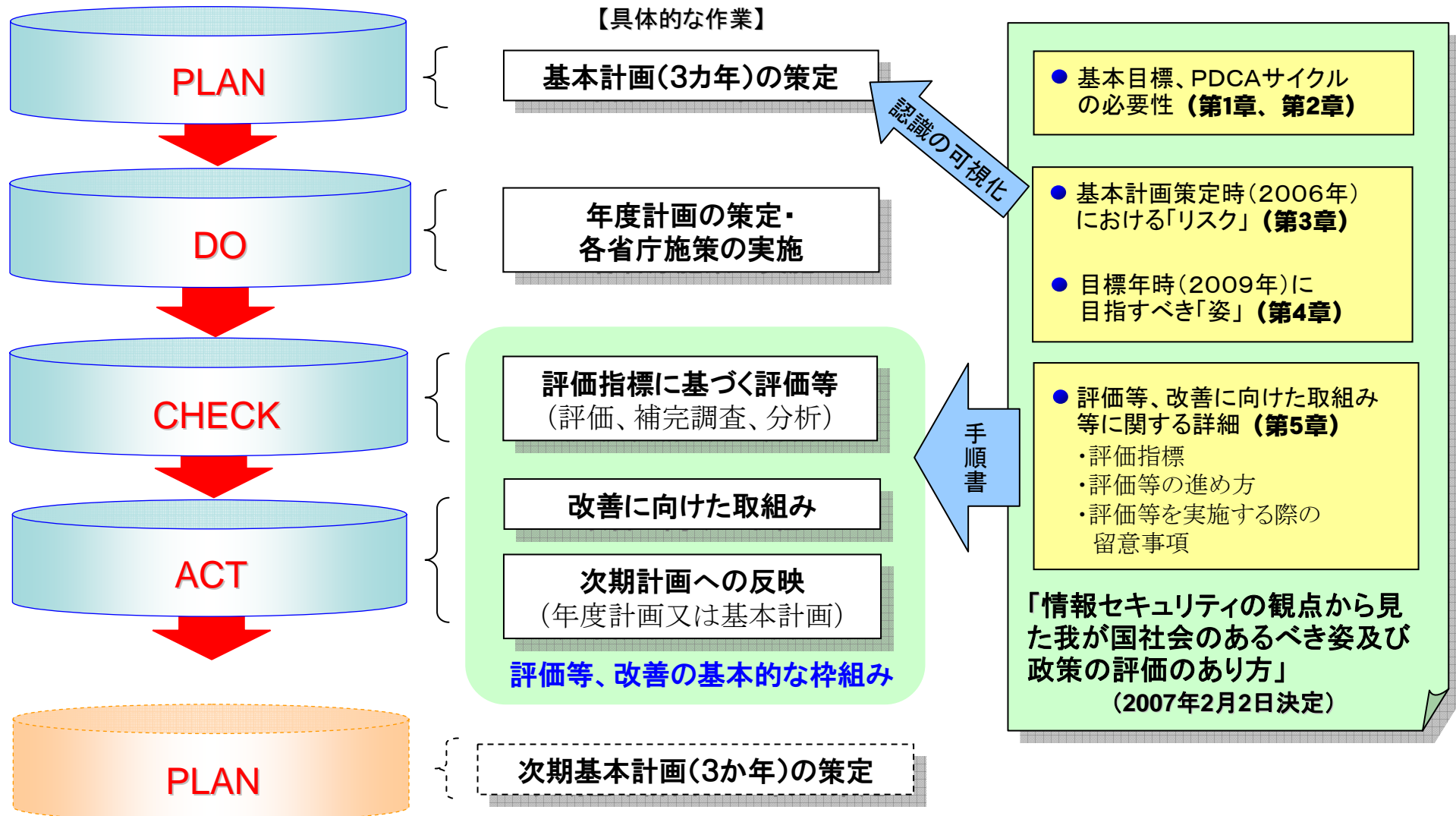
# 内閣官房情報セキュリティセンター(NISC)の機能・体制



# 評価指標に基づく評価等の基本的な枠組み

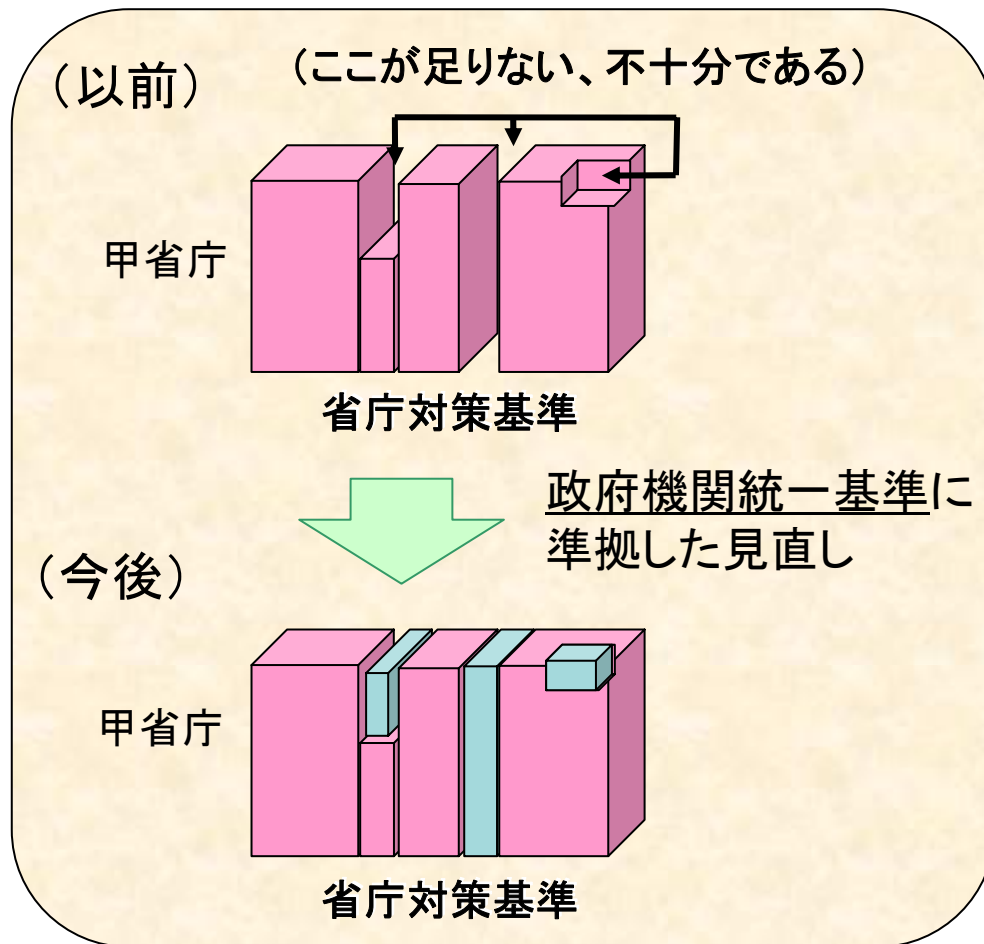


# 情報セキュリティ政策のPDCAサイクル

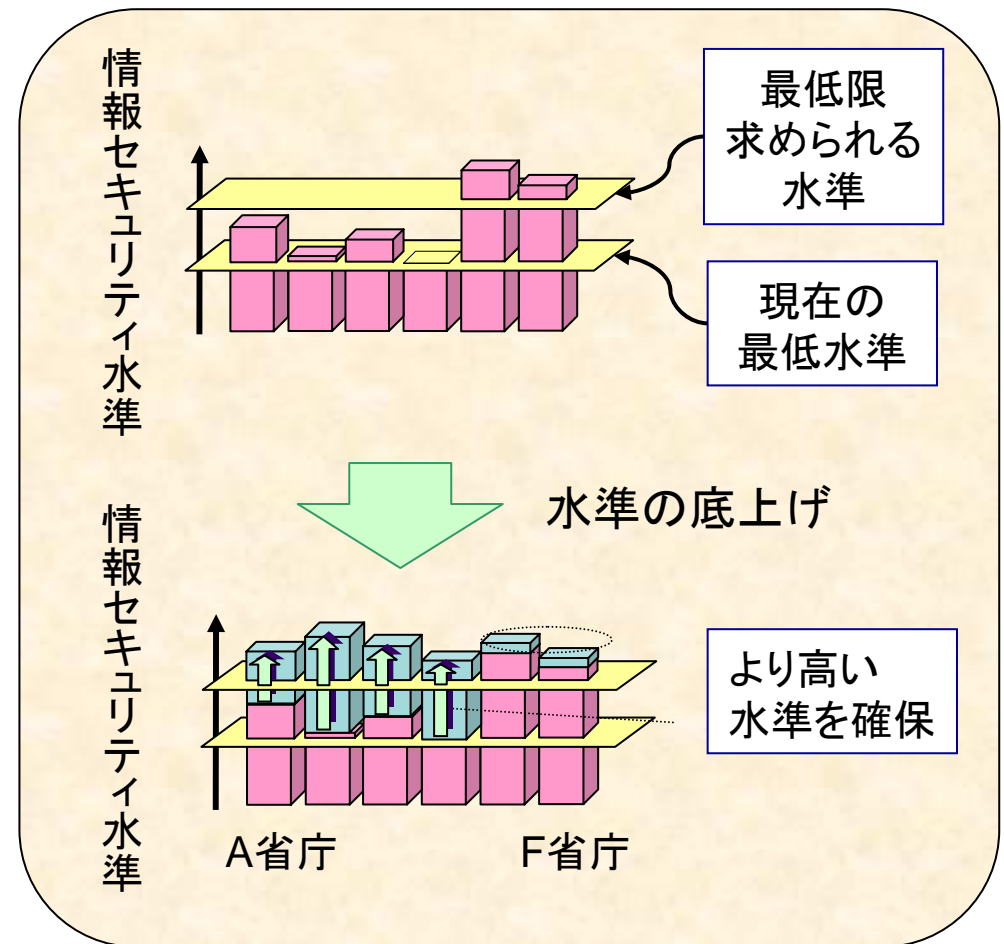


## 内閣官房における個別の取組み

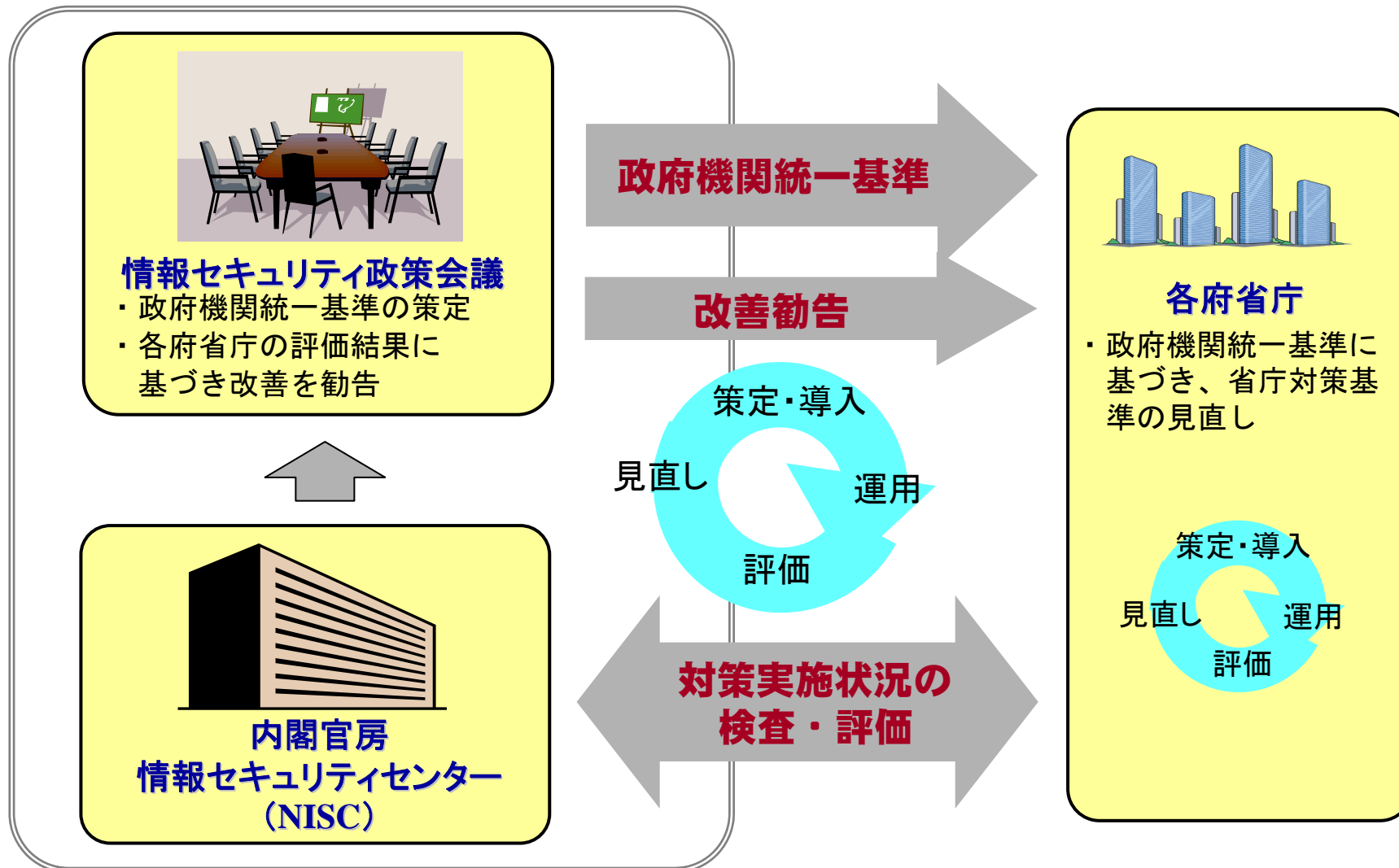
## ① 政府機関統一基準による省庁対策基準の補完



## ② 各府省庁の情報セキュリティ水準の向上



# 「政府機関統一基準」の運用



# 2007年度第1回重点検査の評価結果

## ～端末及びウェブサーバに関する情報セキュリティ対策の総合評価～



### 重点検査の項目

端末に関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・主要APのパッチ等の適用状況 ・アンチウイルス対策ソフトの運用状況
情報保護対策	・モバイルPCの暗号化機能の運用状況
端末管理	・端末の物理的対策状況

ウェブサーバに関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・WEBサーバAPのパッチ等の適用状況等
不正アクセス対策	・不正アクセス対策状況
情報保護対策	・利用者に対する権限管理等の実施状況
サーバ管理	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況

・府省庁の調査に基づく結果  
・平成19年3月末時点

総合評価	端末		ウェブサーバ	
	H18		H18	H19
内閣官房	B	▶▶▶	B	B
内閣法制局	C	▶▶▶	—	B
人事院	C	▶▶▶▶	▶▶▶	B
内閣府	C	▶▶▶▶▶	▶▶▶	B
宮内庁	D	▶▶▶▶▶▶	▶▶▶▶	A
公正取引委員会	C	▶▶▶▶▶	—	A
警察庁	D	▶▶▶▶▶▶	▶▶▶▶	A
金融庁	B	▶▶▶	▶▶▶	A
総務省	C	▶▶▶▶	▶▶▶	B
法務省	D	▶▶▶▶▶▶	▶▶▶▶	B
外務省	D	▶▶▶▶▶▶	▶▶▶▶	B
財務省	C	▶▶▶▶	▶▶▶▶	B
文部科学省	C	▶▶▶▶▶	▶▶▶▶	A
厚生労働省	D	▶▶▶▶▶	▶▶▶▶	B
農林水産省	C	▶▶▶▶▶	▶▶▶▶	A
経済産業省	C	▶▶▶▶▶	▶▶▶▶	A
国土交通省	D	▶▶▶▶▶▶	▶▶▶▶	B
環境省	B	▶▶▶▶	▶▶▶▶	A
防衛省	C	▶▶▶▶▶	▶▶▶▶	A

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x=100%	B	80% ≤ x < 100%	C	60% ≤ x < 80%	D	x < 60%

上昇率		上昇率		上昇率		上昇率		上昇率		上昇率	
▶▶▶▶▶	x > 40%	▶▶▶▶	x > 30%	▶▶▶	x > 20%	▶▶	x > 10%	▶	x > 0%	—	x = 0%

# 2007年度第2回重点検査の評価結果

## ～電子メールサーバに関する情報セキュリティ対策の総合評価～



### 重点検査の項目

電子メールサーバに関する重点検査項目	
不正プログラム対策	<ul style="list-style-type: none"> <li>OSのセキュリティパッチ適用状況（アップデートの状況）</li> <li>電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況）</li> <li>電子メールコンテンツに対する不正プログラム対策の状況</li> </ul>
サーバ管理	<ul style="list-style-type: none"> <li>電子メールサーバの管理者に対する認証等の実施状況</li> <li>電子メールサーバの障害等の発生時における復旧対策の状況</li> <li>時刻同期機能の動作</li> </ul>
不正アクセス対策	<ul style="list-style-type: none"> <li>不正中継対策の状況</li> </ul>
情報保護対策	<ul style="list-style-type: none"> <li>電子メールの受信に係わる利用者に対する認証等の実施状況</li> </ul>

・府省庁の調査に基づく結果  
 ・平成19年9月末時点

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x=100%	B	80% ≤ x < 100%	C	60% ≤ x < 80%	D	x < 60%

総合評価	電子メールサーバ	(参考) 端末	(参考) Webサーバ
	平成19年9月末	平成19年3月末	平成19年3月末
内閣官房	B	B	B
内閣法制局	B	B	B
人事院	A	A	B
内閣府	B	B	B
宮内庁	B	A	A
公正取引委員会	B	A	A
警察庁	A	A	A
金融庁	A	B	A
総務省	B	B	B
法務省	B	B	B
外務省	B	A	B
財務省	A	B	B
文部科学省	A	A	A
厚生労働省	A	B	B
農林水産省	A	A	A
経済産業省	A	A	A
国土交通省	B	B	B
環境省	A	B	A
防衛省	A	B	A

## 1 現状と課題

- ①電子政府システムでは電子署名等の為に暗号が使用されており、SHA-1及びRSA1024を広く使用
- ②これらの方式は、安全性の低下が指摘されており、**より安全な暗号方式への移行が必要**
- ③より安全な暗号方式への移行にあたっては、情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため、**政府統一的な移行指針を策定することが必要。**

## 2 暗号の移行指針(案)の概要

### ①技術的な対応

【政府認証基盤とそれに依存する各府省庁の情報システム】

- 相互運用性確保のため、新旧暗号方式の双方に対応し適切な時期に暗号方式を切り替える運用を可能に
- 新たな暗号方式として、SHA-256及びRSA2048を採用
- 移行完了前に安全性低下の影響が発生する場合に備え緊急避難的な対応も想定

### ②制度的な対応

- 各府省庁において次を実施
  - ・ システムの移行時期を踏まえ、必要な対応の取纏め
  - ・ 移行手順書の整備

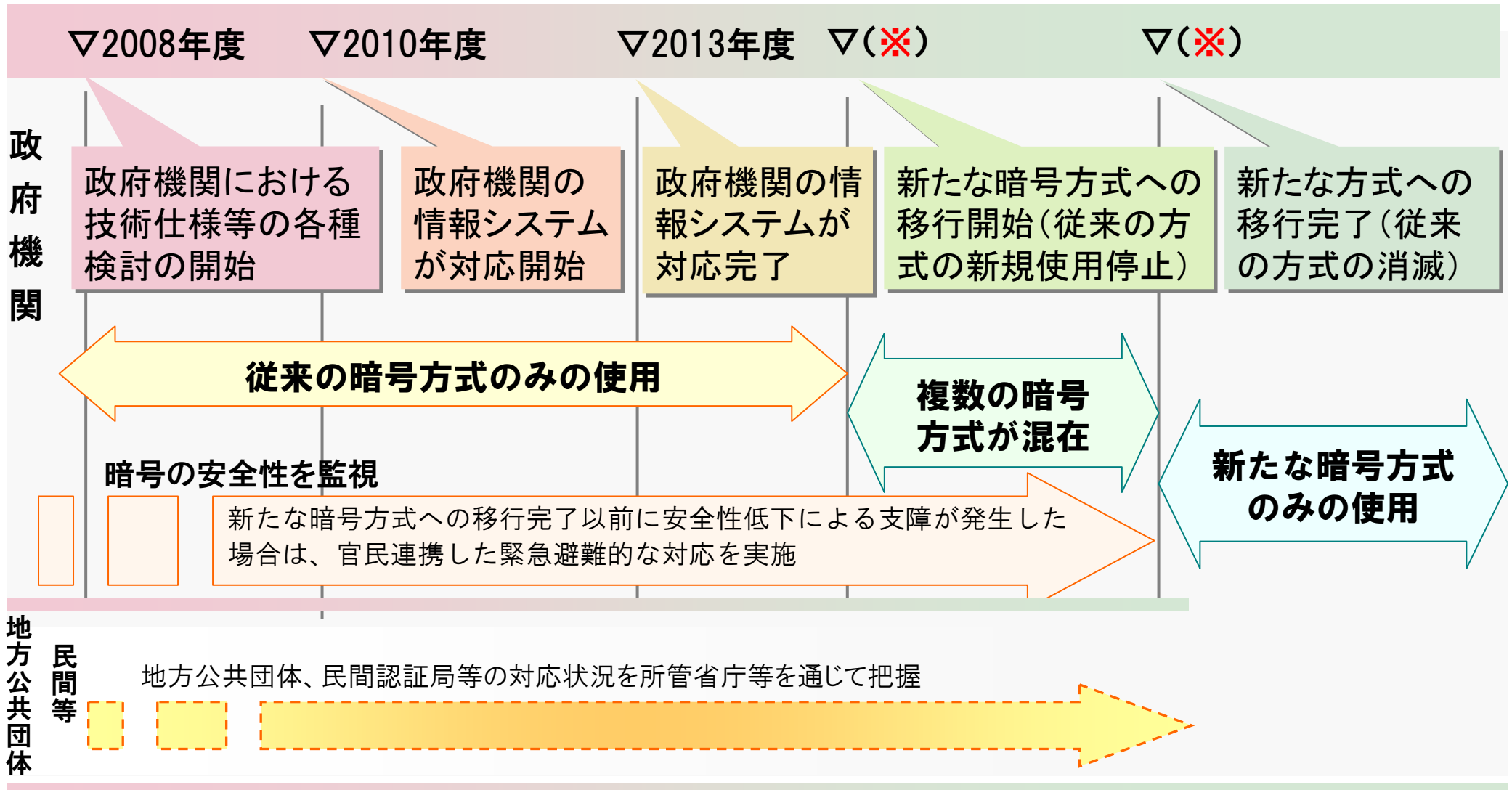
### ③スケジュール

- 内閣官房、総務省、法務省、経済産業省等  
新たな暗号方式へ切替る時期等を2008年度中に検討
- 内閣官房、総務省等  
相互接続の技術要件、緊急避難対応等について、2008年度中に検討。
- 各府省庁  
2010年から2013年の間に各情報システムの対応完了
- 内閣官房、総務省、経済産業省  
安全性の状況を監視し、必要な情報を速やかに各府省庁に提供。

# 移行指針(案)に基づく暗号方式の移行完了までのスケジュール



(※):関係機関との調整を図りながら、  
2008年度中に時期を検討



- 2008年度に、内閣官房にてセキュアVMの評価試験を実施
- 評価ポイント
  - ・政府のニーズにマッチするか？ ユースケースに照らし合わせて検証  
セキュリティ機能のみならず、保守・運用支援機能まで考慮
  - ・不足する機能を補う、既存製品、他の技術などの検討
  - ・実用化への課題洗い出し(政府向けのみならず、一般利用までをスコープに)
- アウトプットの活用(予定)
  - ・政府調達端末ガイドラインにインプット
  - ・セキュアVMの次期研究開発フェーズにおける課題の提案

## 次期基本計画の検討

# 「基本計画検討委員会」の設置について



## 1. 検討のための専門委員会の設置

- ・第1次基本計画は、2008年度が最終年度
- ・官民の各種取組み、技術革新や制度改正等を含めた社会環境の変化等の把握  
→ 2009年度からの情報セキュリティ政策の在り方・方向性について検討を行うため  
情報セキュリティ政策会議の下に、「基本計画検討委員会」を設置

## 2. 「次期情報セキュリティ基本計画(仮称)」に向けた検討スケジュール(案)

平成19年12月12日	第15回情報セキュリティ政策会議(委員会設置決定)
平成20年1月16日	第1回委員会～以後、数回開催
2～3月	産業界、消費者、府省等の関係者からのヒアリング ワークショップ開催等の意見インプット機会の設定
4月	「第一次提言」(仮称)(政策会議)
6、7月頃	検討再開～以後、数回開催
12月頃	「第2次基本計画(仮称)」(案)(政策会議)、パブコメ募集
平成21年1月	パブコメ締切
2月	「第2次基本計画(仮称)」決定(政策会議)

## 基本計画検討委員会の構成



<b>委員長</b>	須藤 修	東京大学大学院情報学環・学際情報学府教授
<b>委員</b>	有賀 貞一	株式会社CSKホールディングス代表取締役
	井川 陽次郎	読売新聞東京本社論説委員
	井上 雅博	ヤフー株式会社代表取締役社長
	笥 捷彦	早稲田大学理工学術院教授
	木内 里美	大成建設株式会社社長室理事情報企画部長
	重木 昭信	株式会社NTTデータ代表取締役副社長執行役員
	下村 正洋	NPO日本ネットワークセキュリティ協会事務局長
	神保 謙	慶應義塾大学総合政策学部専任講師
	関 正樹	関彰商事株式会社代表取締役社長
	高橋 伸子	生活経済ジャーナリスト
	富永 新	日本銀行金融機構局考査役兼企画役システム関連考査担当総括
	中尾 康二	テレコム・アイザック推進会議委員 (KDDI株式会社情報セキュリティフェロー)
	深谷 聖治	東日本旅客鉄道株式会社総合企画本部システム企画部長
	満塩 尚史	環境省情報化統括責任者 (CIO) 補佐官 (各府省情報化統括責任者 (CIO) 補佐官等連絡会議情報セキュリティワーキンググループリーダー)
	宮地 充子	北陸先端科学技術大学院大学情報科学研究科教授
三輪 信雄	総合警備保障株式会社参与	
安富 潔	慶應義塾大学大学院法務研究科 (法科大学院)・法学部教授	
和貝 享介	監査法人トーマツ	

このほかに情報セキュリティ政策会議有識者構成員 (その代理人を含む) も必要に応じ会議に出席し意見を述べることができる。

## 1. 「情報セキュリティ政策」の意義・目的・範囲

- 事前予防、問題発生時の対応体制、事後復旧の在り方など、「情報セキュリティ政策」の射程距離(めざすもの)をどのように設定するか。

→ 現行の情報セキュリティ対策の枠組みの限界

## 2. 状況変化と現状認識

- この間、社会はどう変化したか(ビジネス、個人の利用状況、技術革新の動向等)

→ ネット接続ゲーム機等の普及、攻撃ツールの充実／流通

## 3. 対象分野の設定

- 第1次基本計画の欠落部分(例えば地域、中小企業、安全保障の視点、重要インフラの範囲等)の検討

→ 人材・スキル不足、対策継続インセンティブの必要性

## 4. 推進体制・その他

- 国際動向・諸外国の政策との整合性、各国の参考事例等の採否 等

→ NISCのPOC化は完。提案・推進フェーズへ(OECD, APEC, Meridian(CIIP)、...)



おつかれさまでした

## 我が国のセキュリティ政策の現状と方向性

2008年3月19日

内閣官房情報セキュリティセンター(NISC)

<http://www.nisc.go.jp>