情報セキュリティ戦略元年
－　わが国の情報セキュリティ政策の現状　－

2007年2月

内閣官房情報セキュリティセンター（NISC）

■ 情報セキュリティの日

2月2日を情報セキュリティ日とする
（情報セキュリティ政策会議決定）

- **情報セキュリティ基本計画（第一次）決定** 2006.2.2

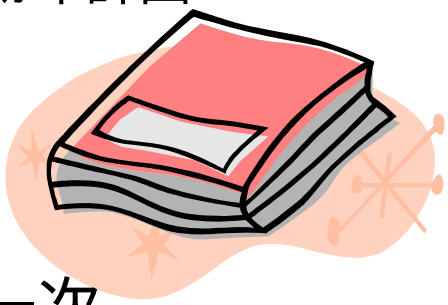
「情報セキュリティの日」はセキュアジャパン2006の133 施策の一つ

わが国の情報セキュリティ政策の構図

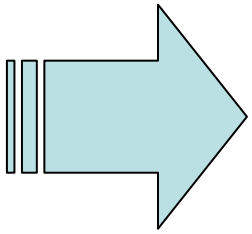
わが国の情報セキュリティ政策は

「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

(133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
- ◆重要インフラ横断的な研究的演習及び机上演習の実施
- ◆「情報セキュリティの日」の創設
- ◆‥ ‥ ‥ ‥ ‥ ‥
- ◆‥ ‥ ‥ ‥ ‥ ‥ ‥

1．政府中核機能の整備

政府全体の政策は２０００年に始まる

（内閣官房に情報セキュリティ対策推進室設置　2000年2月）

２００４年までは二つの流れ

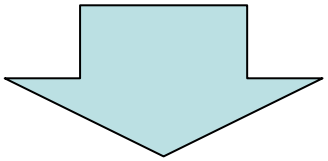
①政府機関の情報セキュリティ対策

②重要インフラの情報セキュリティ対策

２０００年の節目

◆２０００年以前　　試行錯誤の時代

- 省庁の情報セキュリティ対策は自己責任（各自で企画）
- 重要インフラ・企業・個人等に対する施策は各省ばらばら
- 総合的戦略なし



◆２０００年以降　　第一期施策時代　～　2004

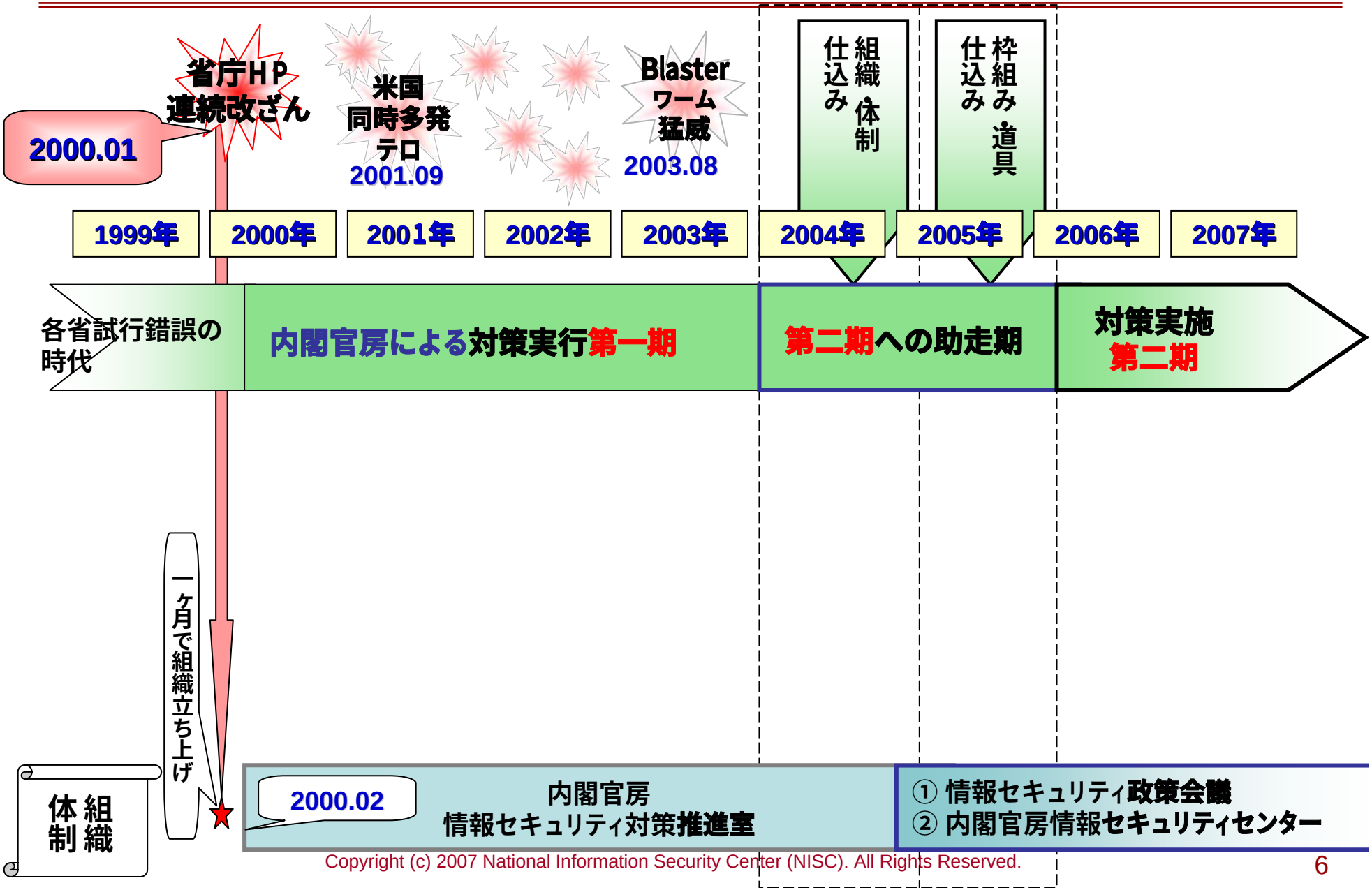
- 政府機関の情報セキュリティ対策を強化するため、２０００年７月に「セキュリティポリシー・ガイドライン」策定
- 重要インフラについて、「サイバーテロ特別行動計画」策定
- 総合的戦略は、引き続きなし

中央省庁ホームページ連続改ざん

◆２０００年1月　中央省庁ホームページ連続改ざん！

- ➢ 政府のコンピュータシステムの管理の悪さが顕在化
- ➢ 実はWebサーバ書換え可能にとどまらない問題だった
- ➢ この時、攻撃者にもっとハックされていたら？
- ➢ 1ヶ月後に内閣官房情報セキュリティ対策推進室立ち上げ

内閣官房における情報セキュリティ政策の流れ



2004 - 2005 政策体系の見直し　第二期への助走期

◆ 社会基盤としてのITと、それへの脅威の増大

- DoS攻撃などサイバー攻撃の増大、さらにはサイバーテロの脅威
- 人為的なミスやハードウェア障害など非意図的要因
- 地震･台風などの自然災害

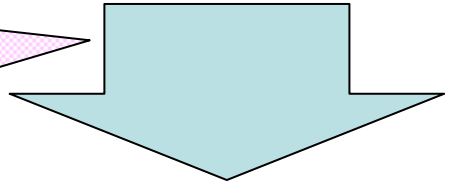
◆ IT障害の大規模化や国民生活や経済活動への直接的な打撃

- 航空管制システムのダウンによる２１５便の欠航 (2003.3)
- 県警交通管制システムの障害による市内１２８ヶ所の信号機障害 (2003.12)
- 医療系コンピュータ･プログラムのミスにより、本来、移植可能な腎臓移植待機　患者が移植出来ず (2004.1)
- などなど　‥　‥

2004 - 2005 政策体系の見直し

- **社会基盤としてのITと、それへの脅威の増大**
  - 生活のあらゆる部分にITが浸透。脅威も質的に変化、量的に増大。
- **IT障害の大規模化や国民生活や経済活動への直接的な打撃**
  - 重要インフラに対する脅威は、サイバーテロだけではない。
- **政府機関の情報セキュリティ対策の不十分さが再び顕在化**
  - ポリシー作って実行伴わず。そもそもポリシーもばらばら。

我が国の情報セキュリティ政策の現状に対する反省

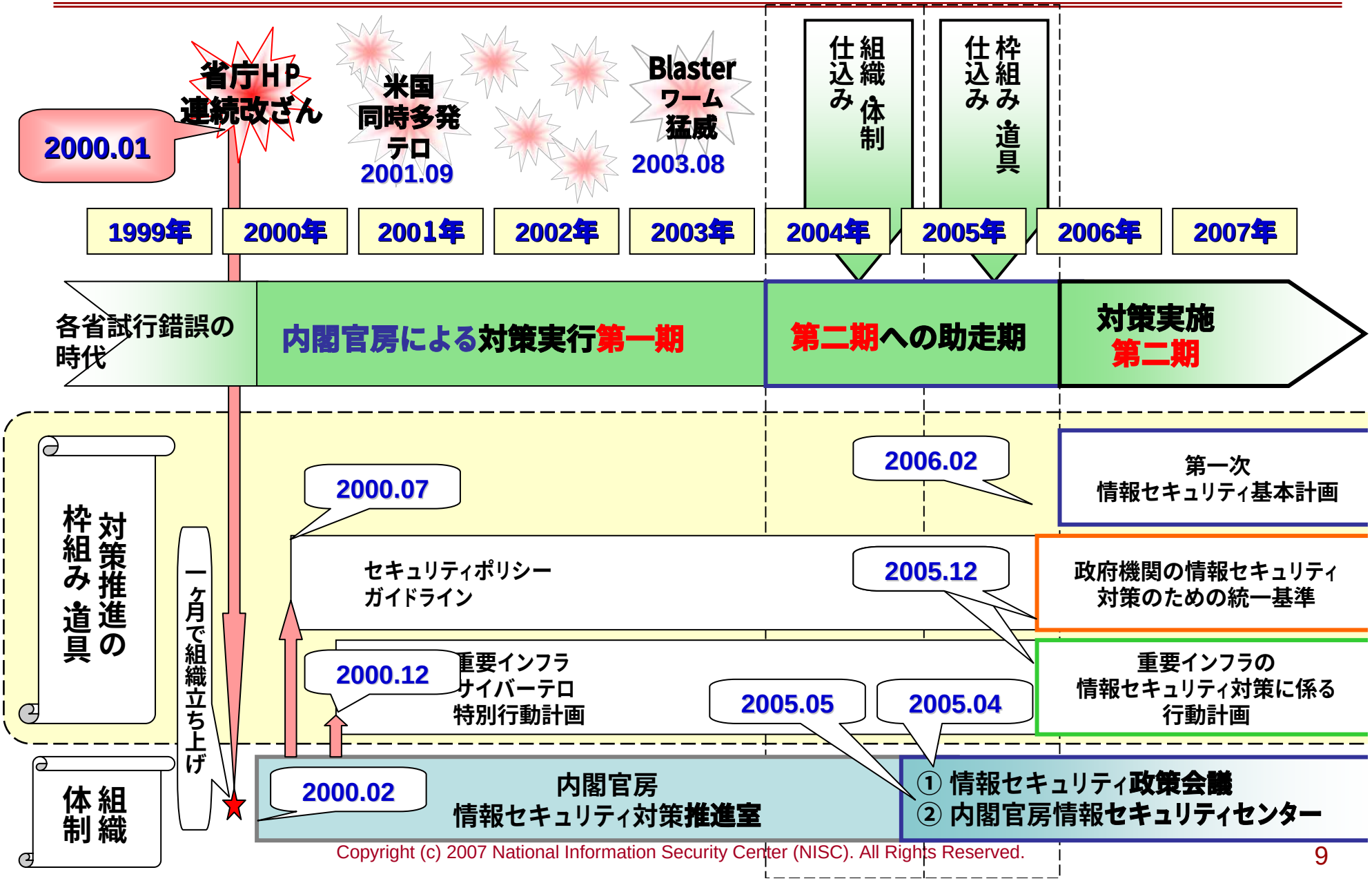


★ **基本戦略の必要性**

★ **政府・企業・個人の各レベルでの責任の所在と行動指針の提示など、本質的かつ基本的な問題の持続的検討の必要性**

★ **政府中核組織の必要性**

内閣官房における情報セキュリティ政策の流れ



組織・体制・枠組み・道具の仕込み（助走期）

2004年

e-Japan戦略Ⅱ
加速化パッケージ
（2004.2）

情報セキュリティ補佐官の
設置
（2004.4）

情報セキュリティ
基本問題委員会の設置
（2004.7）

2005年

第1次提言
＜情報セキュリティ問題に
取り組む政府の役割・機能の
見直しについて＞
（2004.11）

IT戦略本部決定
（2004.12）

第2次提言
＜我が国の
重要インフラにおける
情報セキュリティ対策の
強化に向けて＞
（2005.4）

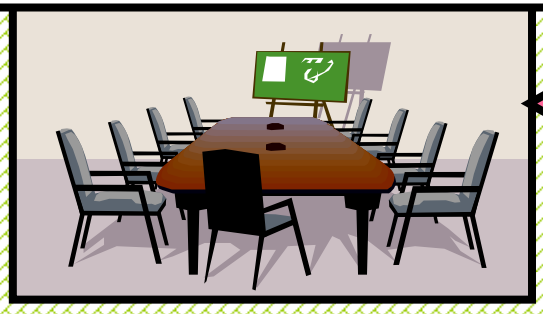
内閣官房情報セキュリティセンター（NISC）の設置（2005.4）

情報セキュリティ政策会議の設置（2005.5）

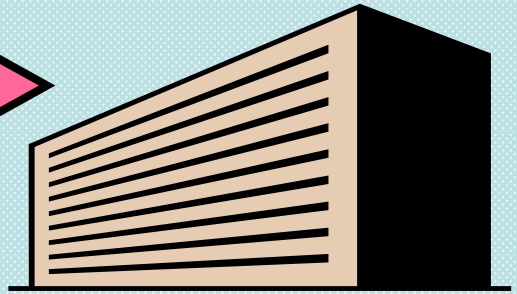
情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）の設置

ＩＴ戦略本部

情報セキュリティ政策会議



内閣官房情報セキュリティセンター
（ＮＩＳＣ）



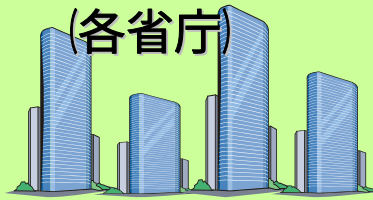
情報セキュリティ関係省庁

警察庁　防衛庁　総務省　経済産業省

重要インフラ所管省庁

金融庁、総務省、厚生労働省、
国土交通省、経済産業省

政府機関
（各省庁）

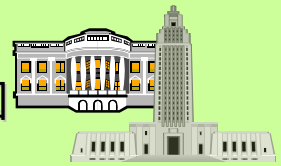


企業

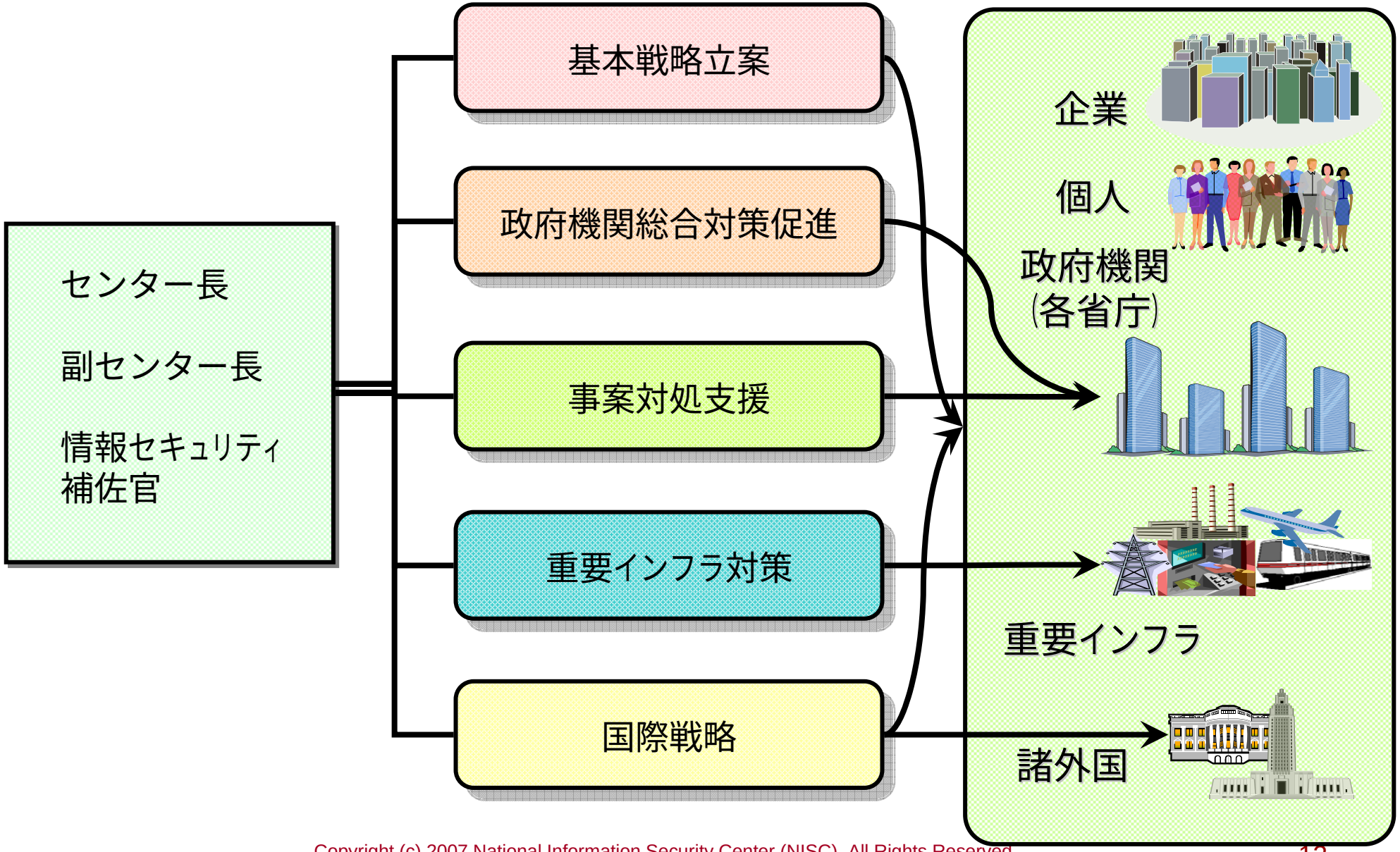
個人

重要インフラ

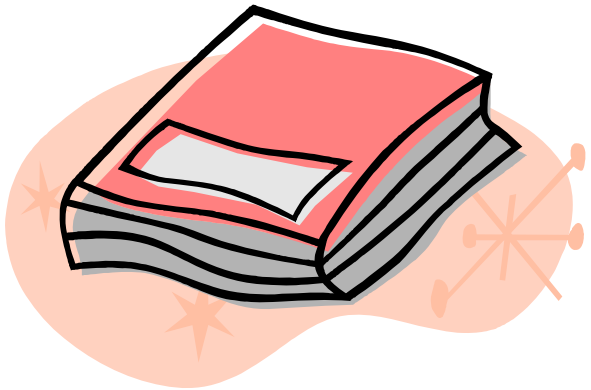
諸外国



内閣官房情報セキュリティセンター（NISC）の機能・体制



第1次情報セキュリティ基本計画について



第1次情報セキュリティ基本計画の全体像

～セキュア･ジャパンの実現に向けて～

基本理念

1. 経済国家日本の基盤としての情報セキュリティ
2. 安全・安心を求める、より良い国民生活実現のための情報セキュリティ
3. 新たな安全保障確保の観点からの情報セキュリティ

今後3年間の取り組み

官民の各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

～ 内閣官房情報セキュリティセンター（NISC）を中心に、全主体が参加して実行 ～

目指すべき姿

「情報セキュリティ先進国」への進展

【政府機関】：すべての政府機関が「政府機関統一基準」が求める水準の対策を実施

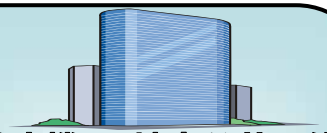
【企業】：企業の情報セキュリティ対策の実施状況を世界トップクラスの水準に

【重要インフラ】：IT障害の発生を限りなくゼロに。

【個人】：「IT利用に不安を感じる」とする個人を限りなくゼロに

「第1次情報セキュリティ基本計画」 －今後3年間の重点政策－

○ 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」の構築に向けて、
「第１次情報セキュリティ基本計画」に基づき、各種対策を強化。



政府機関・地方公共団体

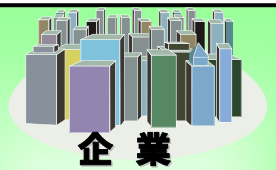
役割：情報セキュリティ対策の「ベストプラクティス」へ

【個別設計図】：政府機関 統一基準

重要インフラ

役割：国民生活・社会経済活動の基盤としての安定供給確保

【個別設計図】：重要インフラ 行動計画



企　業

役割：市場に評価される情報セキュリティ対策の実施

【個別設計図】：各省庁による施策

個　人

役割：IT社会の担い手としての意識の向上

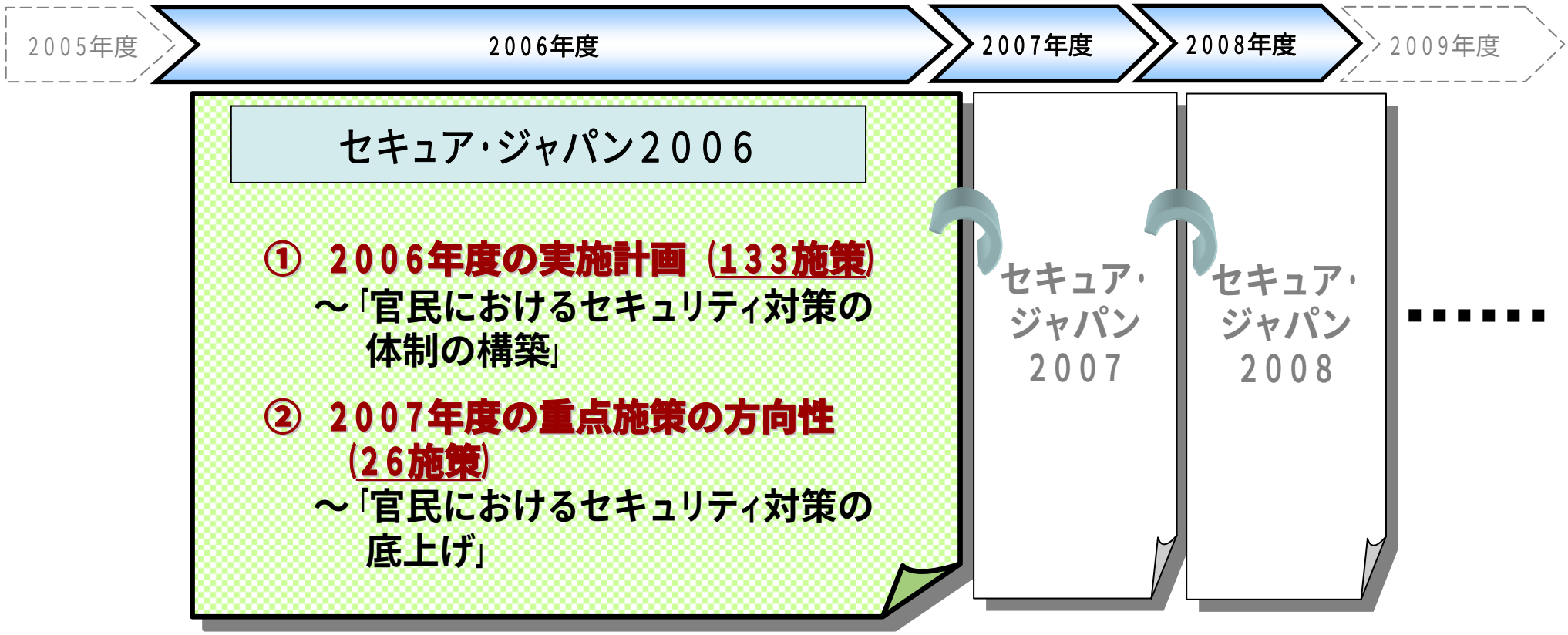
【個別設計図】：各省庁による施策

横断的事項

- 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

セキュア・ジャパン2006

「セキュア・ジャパン２００６」の位置づけ



「セキュア・ジャパン２００６」のポイント

○「第１次情報セキュリティ基本計画」（２００６年２月２日）を着実に実行に移す（「セキュア・ジャパンへの第一歩」）とともに、昨今新たに起こった問題（ウィニーを介した情報流出等）に確実に対応し、情報管理のあり方も含めた総合的な対応策を盛り込み。

○２００６年度に実施する具体的行動計画と、２００７年度の重点施策の方向性を示す。

基本計画を着実に実行に移す必要性

全体対策

基本計画策定(2006.2.2)後に起こった主な問題への対応

- Winny（ウイニー）を介した情報流出の多発
- 政府機関を狙ったサイバー攻撃の多発

対策の方向性

「セキュア・ジャパン２００６」のポイント

政府機関の情報セキュリティ対策の徹底

広く国民も含めた全主体への対策の普及

対策が遅れがちな主体の底上げ