

我が国政府の情報セキュリティ問題への取組みについて  
- 内閣官房の取組みを中心として -

---

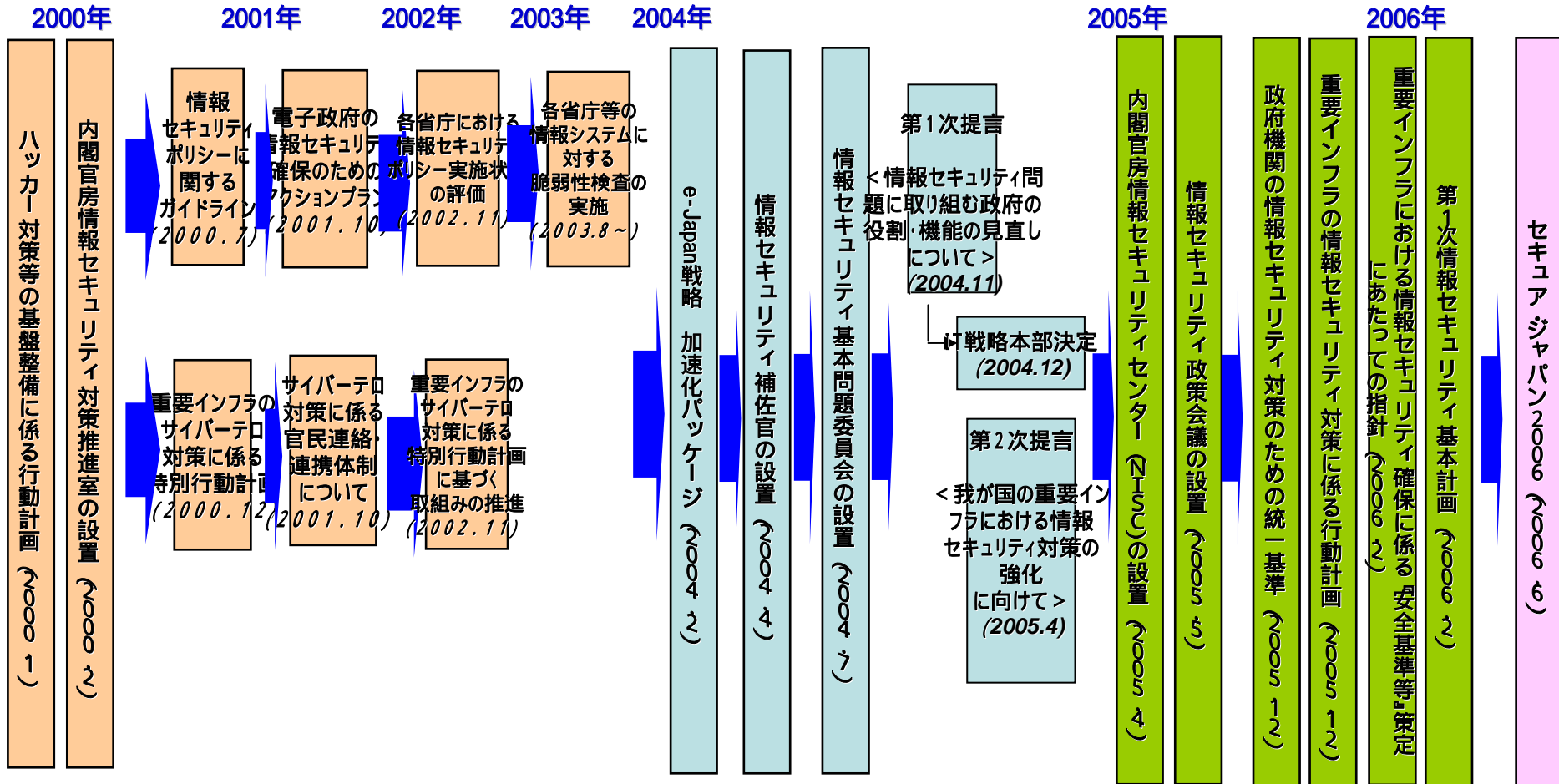
平成18年8月3日

内閣官房情報セキュリティセンター(NISC)

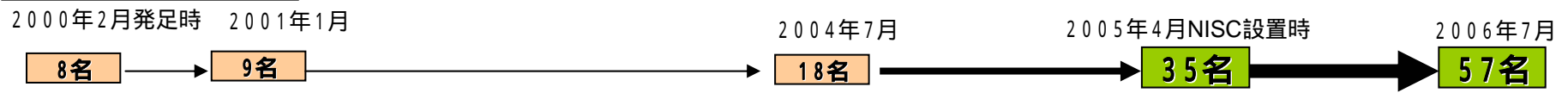
# 1. 政府中核機能の整備

---

# 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

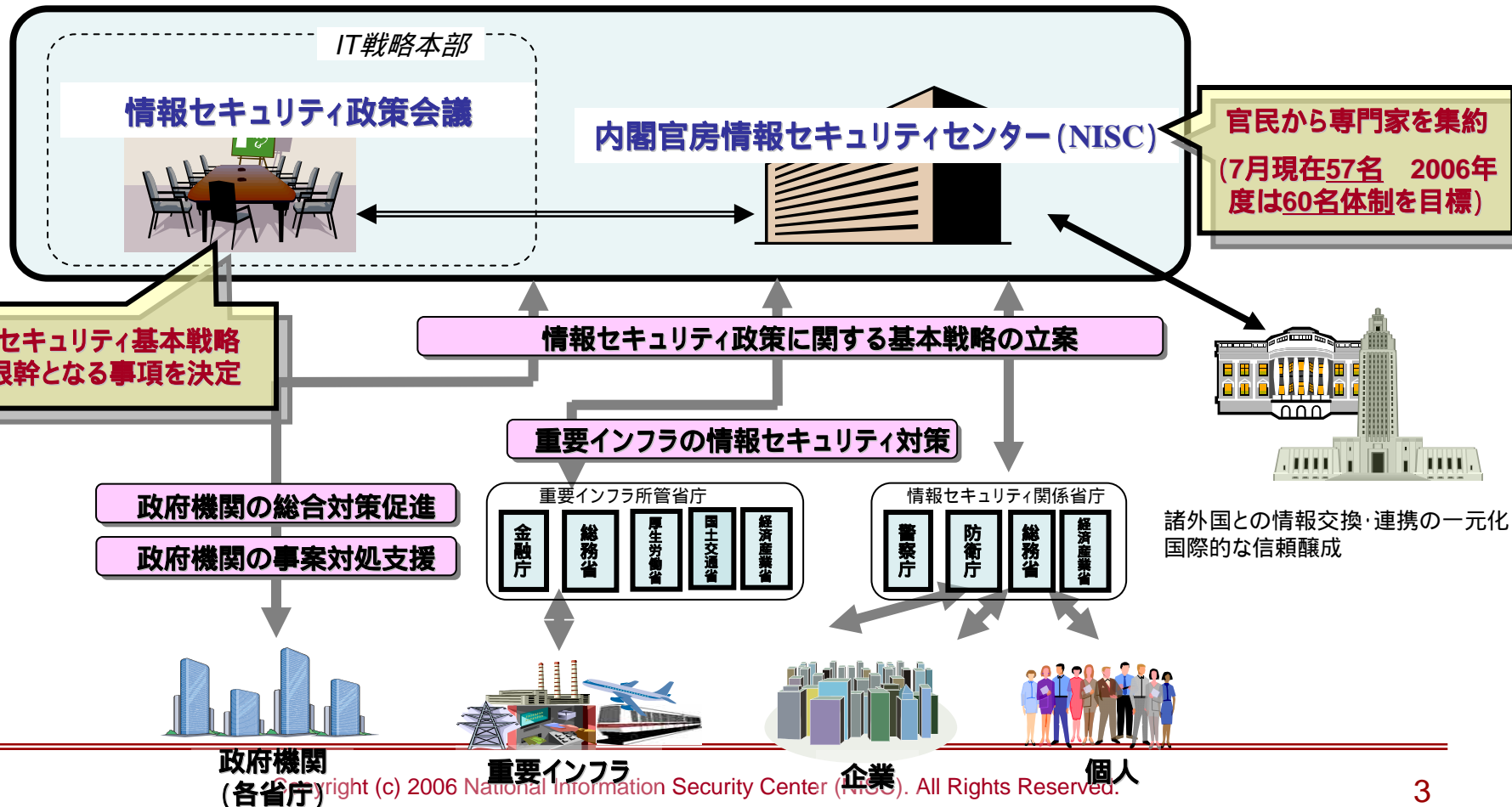


## 内閣官房の体制強化の変遷



# 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

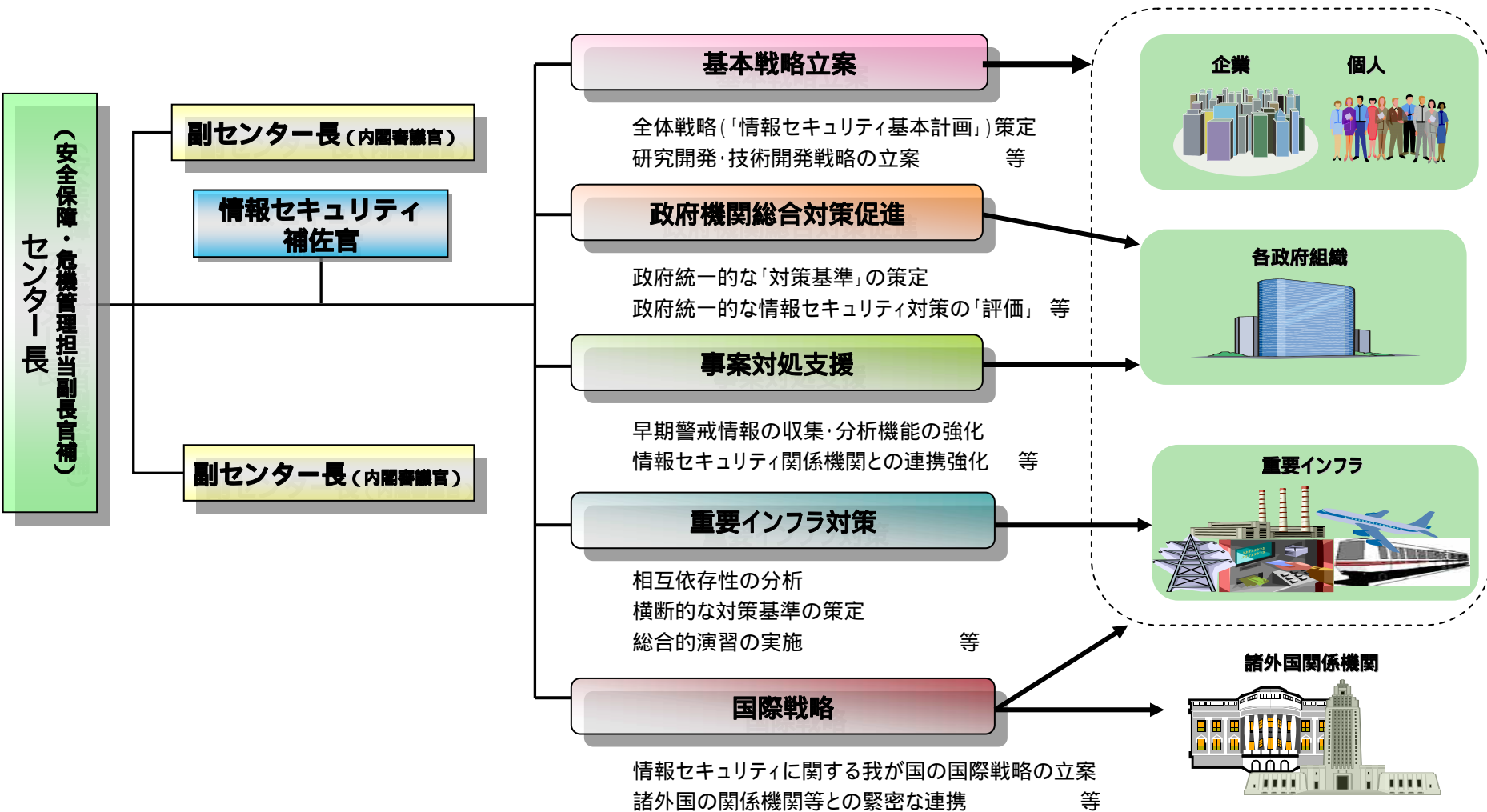
野原 佐和子        (株)イプシ・マーケティング研究所代表取締役社長

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



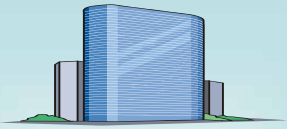
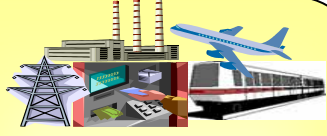


## 2 第1次情報セキュリティ基本計画関連

---

# 「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、今後3年間、政府は「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	 重要インフラ	 企業	 個人
役割	情報セキュリティ対策の「ベストプラクティス」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報セキュリティ対策の実施	IT社会の担い手としての意識の向上
今後3年間の 主な重点政策 (4領域)	政府機関統一基準に基づいた各省庁の評価 サイバー攻撃等への緊急対応能力の強化	情報共有・分析機能の整備 重要インフラ連絡協議会の設置 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 情報セキュリティ監査等第三者評価制度の活用推進 コンピュータウイルス等への対応体制の強化	情報セキュリティ教育の推進 「情報セキュリティの日」の創設等広報啓発の強化 ユーザーフレンドリーなサービスの提供等の環境整備
【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

今後3年間の  
 主な重点政策  
 (横断的事項)

### 情報セキュリティ技術戦略の推進

政府が活用することを前提とした技術開発実施  
 「グランドチャレンジ型」技術開発の推進

### 国際連携・協調の推進

国際的な安全・安心の基盤づくりへの貢献  
 我が国発の国際貢献

### 情報セキュリティ人材の育成確保

多面的・総合的能力を有する実務家の育成  
 情報セキュリティの資格制度を体系化

### 犯罪の取締り、権利利益の保護救済

サイバー犯罪の取締り強化及び関連基盤整備  
 サイバー空間の安全性向上のための技術開発



### 3 セキュア・ジャパン2006

---

# 「第1次情報セキュリティ基本計画」の概要 と「セキュア・ジャパン2006」の位置づけ

## 「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)

([http://www.nisc.go.jp/active/kihon/pdf/bpc01\\_ts.pdf](http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf))

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
各実施領域の重要政策	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・分析機能の整備 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
横断的な重要政策	情報セキュリティ技術戦略の推進 国際連携・協調の推進		情報セキュリティ人材の育成確保 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」

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」

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

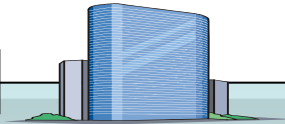
セキュア・  
ジャパン  
2008

# 「セキュア・ジャパン2006」中の具体的施策

～ 2006年度の実施計画 ～

## 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旨とする。

【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」中の具体的施策

～ 2006年度の実施計画 ～

## 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旨す。

#### 【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旨す。

#### 【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」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」中の具体的施策

～ 2006年度の実施計画 ～

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

## 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

政策の推進体制等

# 「セキュア・ジャパン2006」中の具体的施策

～ 2007年度の重点施策の方向性～

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) の本格稼働)

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