NISC National Information Security Center

情報セキュリティ先進国に向けて
～第2次情報セキュリティ基本計画の目指すもの～

平成20年12月18日

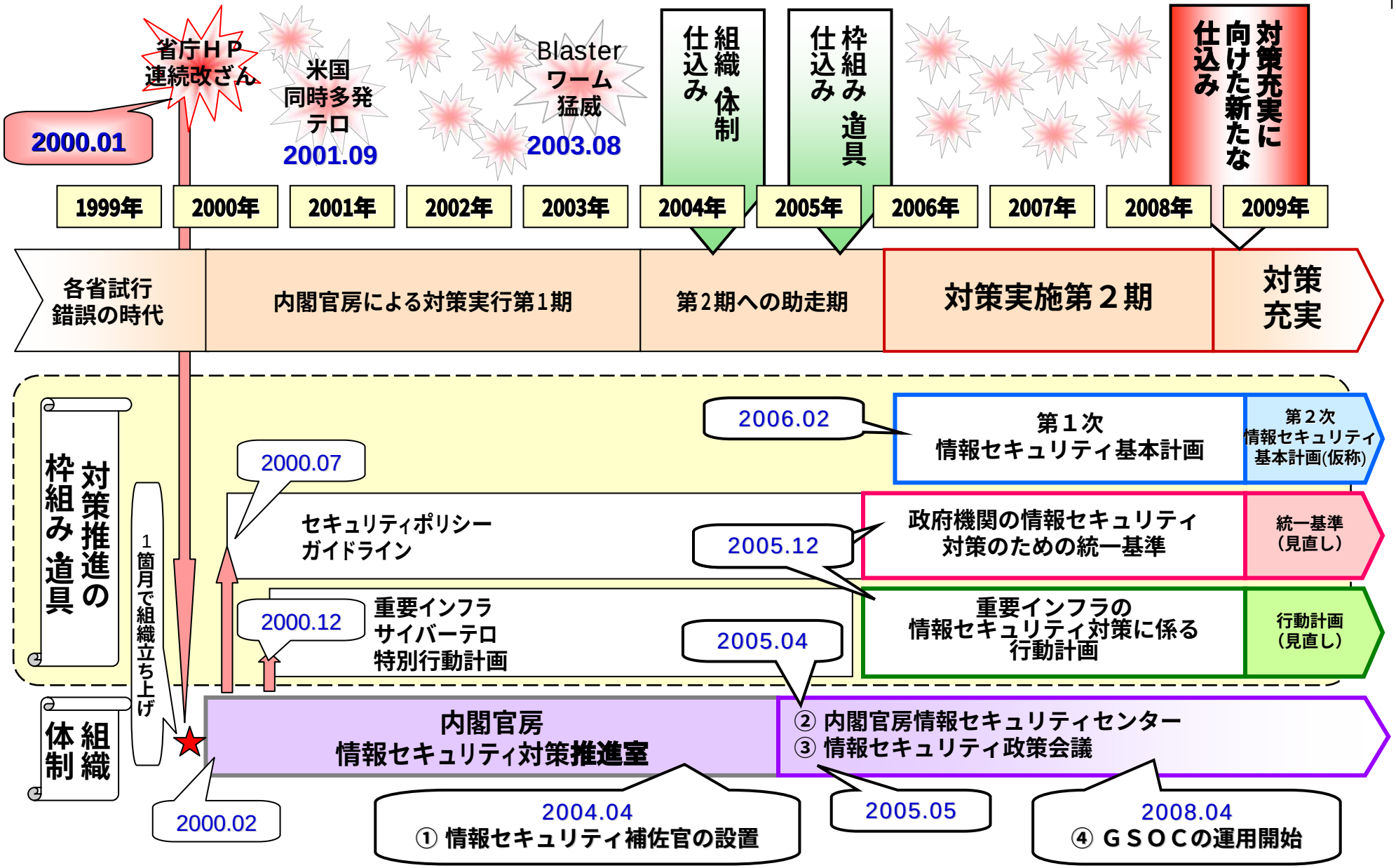
内閣官房情報セキュリティセンター（NISC）
内閣審議官　前野　陽一

http://www.nisc.go.jp

NISC National Information Security Center

これまでの取組

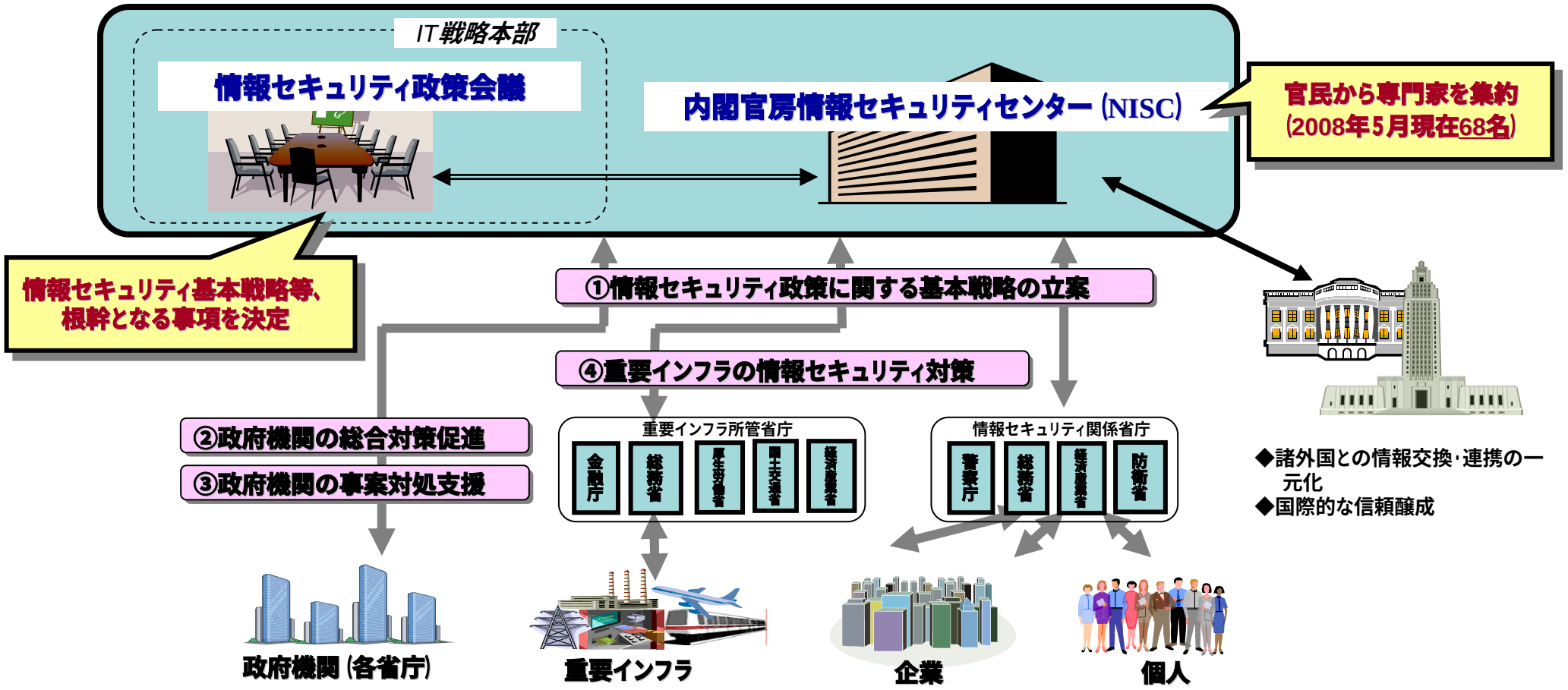
内閣官房における情報セキュリティ政策の流れ（２０００年以降の概要）



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

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



情報セキュリティ政策の構造

「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決定）

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
3カ年の目標	すべての政府機関が「政府機関統一基準」が求める水準に	IT障害を限りなくゼロに	対策の実施状況を世界トップクラスの水準に	「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	◆ 重要インフラ行動計画 ・安全基準等の整備の推進 ・情報共有体制の強化 ・相互依存性解析 ・分野横断的演習実施	◆ 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
- 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

第2次情報セキュリティ基本計画

2005年度 | 2006年度 | 2007年度 | 2008年度 | 2009年度

評価2006 → セキュア・ジャパン2006

評価2007 → セキュア・ジャパン2007

評価2008 → セキュア・ジャパン2008

セキュア・ジャパン2009

「セキュア・ジャパン」：基本計画の遂行を確実にするため、毎年の政府の重点施策をまとめた年度計画

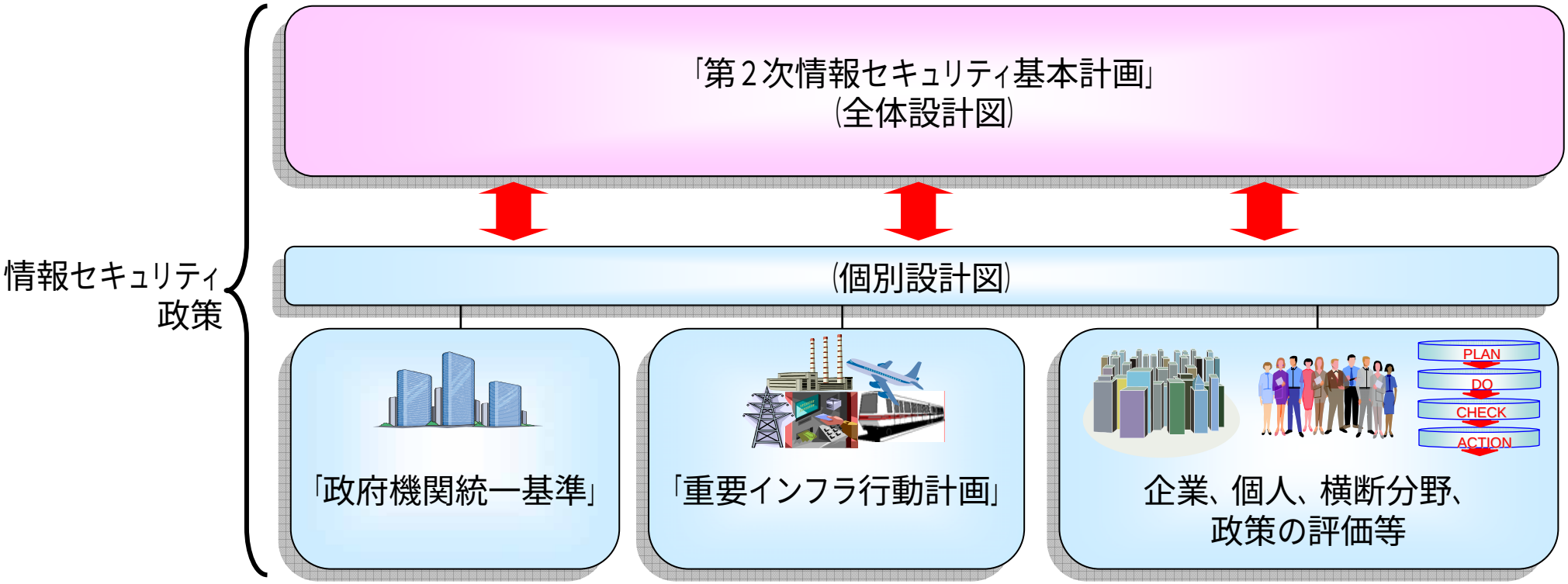
NISC National Information Security Center

「第２次情報セキュリティ基本計画」の下での政策推進
及び
「第２次情報セキュリティ基本計画（案）」について

全体設計図である「第2次情報セキュリティ基本計画」、分野単位の個別設計図

○情報セキュリティ政策は、情報セキュリティ問題全般に関する全体設計図である「第２次情報セキュリティ基本計画」と、分野別の個別設計図の組み合わせで推進する。

○このような組み合わせに基づくことで、個別分野縦割り的対応を排し、我が国全体として分野横断的・政策領域横断的な視点を持って、複雑化する情報セキュリティ問題への的確な対応を進める。



「第2次情報セキュリティ基本計画」(パブリックコメント案)に係る検討の経緯

・2007年12月　「次期情報セキュリティ基本計画」の策定へ向け、「基本計画検討委員会(委員長:東京大学須藤修教授)」を設置　(第15回情報セキュリティ政策会議決定)。

・2008年1月より、「基本計画検討委員会」による検討を実施(計16回、延べ48時間)。

・途中、関係者からのヒアリングを実施(8団体、1関係委員会、2政府機関)。

　日弁連／全国市長会(藤沢市)／経団連／重要インフラ専門委員会／日本商工会議所／消費者団体(主婦連合会、東京都地域婦人団体連盟、全国消費者団体連絡会、日本消費生活アドバイザーコンサルタント協会)／ 政府機関(国交省・外務省)

・第18回 情報セキュリティ政策会議(6月18日開催)において、「基本計画検討委員会」がとりまとめた「次期情報セキュリティ基本計画に向けた第1次提言」を報告。

・ 第1次提言報告後、約一ヶ月間のパブリックコメントを経た後、各論部分を検討するために、委員会の検討を7月から再開。以下のような分野についての検討を行った。

　政府機関・地方公共団体、重要インフラ、企業・個人、横断的な情報セキュリティ基盤など

・ 今回の政策会議(12月10日)における、「第2次情報セキュリティ基本計画」のパブリックコメント案のとりまとめを目指して案文を作成。

「次期情報セキュリティ基本計画に向けた第１次提言」(2008年6月19日)の概要

第１次情報セキュリティ基本計画 (2006年度～2008年度)

- 我が国の情報セキュリティ政策の立ち上げ
- 「気付きを与える」ための戦略
- 官民各主体のITの安心・安全な利用へ向けた取組み

『情報セキュリティ立国』の思想

『ジャパン・モデル』の確立・世界への展開 (高品質・高信頼性・安心安全)

『情報セキュリティ先進国』の実現

目指すべき結果：情報セキュリティ上の問題がない水準

継続

- 情報セキュリティ上の問題がない水準は目指す
- 各主体最大限の尽力は更に進める
- 対策の推進、水準の向上

発展

- 具体的取組みの持続的な推進
- 「事故前提社会」への対応力強化
- 合理性に裏付けられたアプローチの実現

第２次情報セキュリティ基本計画 (仮称)

基本理念

『成熟した情報セキュリティ立国』

●より現実に即した実効的な情報セキュリティ対策●

- 冷静で迅速な対応
- 最適な水準の対策の効果的・効率的な実施
- 説明責任の明確化

ITルネサンス

世界との協調・イニシアティブの発揮

基本目標

「ITを安心して利用可能な環境」の構築

●基本目標に向けて考慮すべき諸点●

■「事故前提社会」への対応力強化

- 理解 (気付き) の推進、判断力の向上
- 事後対応への更なる注力
- 主体間の共通理解、信頼関係の構築
- 事実把握と被害拡大防止・再発防止への情報共有

■合理性に裏付けられたアプローチの実現

- 脅威の把握、リスクへの柔軟な対応
- コスト・利便性とのバランス
- 最適な「水準」に関する認識の共有
- 人的側面の対策
- 説明責任の明確化

「第1次情報セキュリティ基本計画」の成果と「第2次情報セキュリティ計画（パブリックコメント案）」の目標（目指す「姿」）

1．第1次基本計画（'06～'08年）

成果

情報セキュリティ政策の立上げ

◆関係者の「気付き」を高めた

→ P to Pソフトで情報流出の危険性

→ サイバー攻撃で情報を盗まれる危険性

→ システム障害で事業が止まる危険性

◆とりあえず政策推進の枠組みは構築

→ 政府機関の統一基準に基づく対策と評価

→ 重要インフラ事業者間の情報共有体制

→ 日米、日ASEANで情報交換を行う枠組み

◆（問題が生じないための）事前対策の取組みはある程度進展

→ 但し、日々新たなリスクが生まれ、また変化している

2．第2次基本計画（'09年～'11年）

目標

政策の継続と更なる発展

◆事前対策は当たり前のことに

◆問題が生じても、冷静かつ迅速に事後対応・復旧活動を推進できる

◆情報を管理する側に加えて、情報を預ける側も取組みの対象に

「第２次情報セキュリティ基本計画（案）」の構造

第１章

第１次情報セキュリティ基本計画の下での取組みと２００９年の状況

1. **第１次情報セキュリティ基本計画の下での取組み**　（第１次基本計画の考え方などについて記述）
2. **２００９年の状況**　（第１次基本計画の下で様々な取組みを進めた結果、どのような状況となっているか考察）

第２章

第２次情報セキュリティ基本計画における基本的考え方と２０１２年の姿

1. **第２次情報セキュリティ基本計画の基本的考え方**　（第２次基本計画の考え方などについて、適宜第１次基本計画と比較しながら記述）
2. **２０１２年の姿**　（第２次基本計画の下で様々な取組みを進めた結果、計画期間後にどのような姿となると考えているか記述）

第３章

今後３年間に取り組む重点政策

1. **対策実施４領域における取組みの推進と政策目的の着実な実現**　（政府・地方公共団体、重要インフラ、企業、個人について記述）
2. **横断的な情報セキュリティ基盤の強化と発展**　（技術、人材、国際、犯罪対策などについて記述）

第４章

政策の推進体制と持続的改善の構造について

1. **政策の推進体制**
2. **他の関係機関等との関係**
3. **持続的改善構造の構築**

「第２次情報セキュリティ基本計画（パブリックコメント案）」の全体像　［1］

○「第２次情報セキュリティ基本計画（パブリックコメント案）」は、情報セキュリティ問題全般に係る中長期計画（全体設計図）として、今後の我が国の取組みに関する、1）基本的考え方と、2）重点政策の方向性を提示。

○具体的には、２００９年度～２０１１年度までの３カ年計画として策定。これまで同様、本計画に基づいた年度ごとの推進計画である「セキュア・ジャパン」を策定するとともに、年度ごとの取組み状況や社会変化などに関する評価等を行う予定。

第１次基本計画からの「発展」と「継続」

1. **具体的取組みの持続的な推進、新たな課題への政策的対応**
   （第１次基本計画で構築した取組みの各種枠組みを持続的に活用）

2. **「事故前提社会」への対応力強化**
   （十分な事前対策の取組みにも関わらず、万が一問題が生じた場合を考えて準備を怠らない）

3. **合理性に裏付けられたアプローチの実現**
   （情報資産の価値、リスクの大きさに応じた合理的（最適）な水準の対策を実現）

「第２次情報セキュリティ基本計画（パブリックコメント案）」の全体像　［2］

第２次基本計画の基本的考え方

●基本目標　→　「ITを安心して利用できる環境」の構築
（第１次基本計画と同様。IT基本法第２２条の実現）

●取組みにあたっての基本理念　→　「セキュリティ立国」の思想の成熟　（IT時代の力強い「個」と「社会」の確立へ）
（目指す「姿」は、最適な水準の取組みとセキュリティの実現であり、絶対的な無謬性の追求ではない　→　絶対的な無謬性から脱却するには国民や社会全体の意識改革も不可欠）

●基本目標の実現に向けた取組み　→　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」＋（対策実施側のみならず）情報提供側も視野に入れた取組みの推進
（第１次基本計画の下では、対策実施主体及び対策支援主体による「新しい官民連携モデル」を追求。状況変化を踏まえ、新たに情報提供側も視野に入れた取組みを推進）

「第２次情報セキュリティ基本計画（パブリックコメント案）」の全体像　［3］

第２次基本計画の下で取組みを行う政策領域

●**課題の把握から事前対策、事後対応まで視野に入れた取組み**
（事前対策のみならず、万が一問題が生じた場合も視野に入れて事後対応の準備を進める）

●**技術面での対応から制度面、人的側面の対応まで視野に入れた取組み**
（技術開発から人材育成のような側面まで幅広く取組みを進める）

●**国内における対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取組み**
（IT利用・活用においては国境を越えるのは当然となっており、国内の取組みと国際的な取組みを有機的に結びつけた取組みとする）

●**国民の日常生活や経済活動といった個別主体に関係の深い領域から、安全保障や文化といった我が国全体に関係の深い領域にまで対応した取組み**
（情報セキュリティ問題は相当程度幅が広いことに鑑み、様々な観点から柔軟かつ領域横断的に取組みを進める）

「第2次情報セキュリティ基本計画（パブリックコメント案）」に基づく取組み－今後3年間の重点政策－

NISC

主な重点政策①（4領域）3年間の

政府機関・地方公共団体	重要インフラ	企業	個人
◆能動的に情報セキュリティ対策を推進する体制確立 （最高情報セキュリティアドバイザー設置、年次報告書の報告・公表） ◆事業継続性確保の検討、サイバー攻撃等への緊急対応能力強化	◆情報共有体制の強化 ◆重要インフラ連絡協議会の設置 ◆分野横断的な演習、共通脅威分析の実施	◆情報セキュリティ監査等第三者評価制度の活用推進 ◆対策容易化のためのツール提供 ◆中小企業の対策促進 ◆コンピュータウィルス等への対応体制の強化	◆学校や地域における教育モラル等の教育の推進 ◆個人の質問対応を行えるようなサポータの育成 ◆サービス提供事業者や対策支援主体によるリスク情報等の個人への適切な提供促進
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

主体 情報提供

自身の有する情報を預ける主体 （新たな課題として、関係機関等が協力しながら取組みを検討・推進）

横断的事項）主な重点政策②）3年間の

情報セキュリティ技術戦略の推進
- ◆セキュリティ対策を埋め込んだ機器の開発促進
- ◆「グランドチャレンジ型」技術開発の推進

情報セキュリティ人材の育成確保
- ◆政府機関における人材の育成・確保
- ◆保有するスキルの見える化の推進

国際連携・協調の推進
- ◆世界の脅威動向を把握するための官民連携確立
- ◆アジアにおける知恵の結集と水準の向上

犯罪の取締り、権利利益の保護救済
- ◆犯罪取締りのための基盤整備の推進
- ◆権利利益の保護・救済のための基盤性の推進

情報セキュリティ人材育成における背景

情報セキュリティ人材育成を巡る背景

産業界からの要望

◆産・学・官連携による安定的・継続的な人材の育成・確保

➔官民ともに高度なセキュリティ人材が不足していることからの要望

◆情報セキュリティ人材に対するキャリアパスの明確な提示

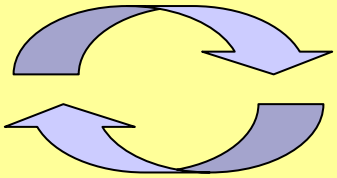
➔情報セキュリティ人材のモチベーションを確保するための要望

◆国際的に通用する高度IT人材の育成

➔産業界におけるニーズが多い、国際競争力を持った人材確保のための要望

等

要望



フィードバック

政府における様々な取り組み

◆先導的ITスペシャリスト育成推進プログラム

➔高度セキュリティ人材育成プログラムを開発・実施する拠点の形成

◆情報通信人材研修事業支援制度

➔情報通信分野の専門的人材育成のための研修事業に対する助成

◆ファカルティ・ディベロップメントの支援

➔教員の能力向上のための、各大学等におけるファカルティ・ディベロップメントの取り組み支援

◆IT人材評価メカニズムの構築、情報処理技術者試験の改革

➔ITスキルを体系的に整理した共通キャリア・スキルフレームワークの作成及び、それとの整合性を確保する情報処理技術者試験の見直し

等

第2次情報セキュリティ基本計画における取り組み

➔産業界からの要望や政府における様々な取り組み等の背景を受けて、社会におけるニーズを満たす事のできる情報セキュリティ人材育成・確保の取り組みを推進

第2次情報セキュリティ基本計画における情報セキュリティ人材の育成・確保の概要

NISC

情報セキュリティ人材について目指すべき「姿」

情報セキュリティ人材の重要性が社会で十分に認識され、その業務が魅力的なものとして、優秀な人材が官民を問わず情報セキュリティ分野にすすんで集まる社会

上記「姿」に向けて、様々な取り組みを実施

人材の育成・確保について、今後3年間で取り組む重点政策

1. 政府機関における人材の育成・確保及び職員の意識啓発
2. 企業における情報セキュリティ人材の育成・確保
3. 情報セキュリティ人材が保有するスキルの見える化の推進

個人における重点政策のうち、人材に関連する項目の例

1. 情報セキュリティ教育の強化・推進
2. 個人の底上げに向けたより効果的な普及・啓発活動の実現地域の情報セキュリティ対策の担い手の育成支援

地方公共団体における重点政策のうち、人材に関連する項目の例

1. 小規模な地方公共団体も含めた合理的・自主的な情報セキュリティ対策の促進
2. 地方公共団体の取組みを応援する主体の強化
3. 地域の情報セキュリティ対策の担い手の育成支援

第2次情報セキュリティ基本計画における「人材の育成・確保」に関する施策(1)

第1次基本計画下での施策：「多面的・総合的能力を有する実務家・専門家の育成」

→人材の育成には成果が出るまでに必要となる期間が長く、成果は未だ明確になっていない
→他方、人材育成の施策に対するニーズは依然として存在する

第2次計画では → 官民のフレームワーク・資格試験等を活用して、人材育成施策を継続して実施

○企業における情報セキュリティ人材の育成・確保

(前略)

環境の進化に柔軟に対応できる人材や企業のマネジメント全体を俯瞰した上で判断できるスキルを持った人材などの育成・確保も必要不可欠である。その際には、情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び**民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。**

(中略)

また、**技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定**や**専門家コミュニティへの支援**を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。(後略)

第2次情報セキュリティ基本計画における「人材の育成・確保」に関する施策(2)

第1次基本計画下での施策：「情報セキュリティに関する資格制度の体系化」

→「人材育成・資格制度体系化専門委員会」報告書にて、体系化を実施
→他方、保有するスキルを業務と結びついた形で明確にできる仕組みへのニーズが存在

第2次計画では → 保有するスキル等を外部に対して明確にできる仕組みを構築

◯情報セキュリティ人材が保有するスキルの見える化の推進

（前略）

実際の業務において求められるスキルを明確にするとともに、人材が保有するスキルが外部からわかりやすくするための政策を実施する。例としては、情報セキュリティ資格制度・教育制度と業務において求められるスキルや情報セキュリティ人材の目指すキャリアパスの関係を見えやすくするための取組みや、共通キャリア・スキルフレームワーク：ITSS や民間の人材育成における各種有効なフレームワークの活用により、保有するスキルを外部に明示できる仕組みを構築する取組みが挙げられる。

第2次情報セキュリティ基本計画における「個人」に関する施策

第1次基本計画下での施策：「『IT利用に不安を感じる』とする個人を限りなくゼロに」

→インターネット利用に不安を感じる個人は未だ多く存在

第2次計画では

個人がITを不安無く利用できる社会へ向けた取り組みを継続して実施

情報を預ける側の主体として、主体的に考えられる社会を目指して取り組みを実施

○ 個人に対する情報セキュリティ教育の強化・推進

ITの利用・活用には積極的であるものの、リスクの認識や情報セキュリティ対策の重要性の認識が必ずしも十分ではない**児童・生徒や保護者への教育・啓発を推進**する。**こうした観点も踏まえつつ、学校や地域における情報モラル(※)等の教育を推進**する。
また、消費者である個人が様々なサービス等の利用において生じ得るリスクを認識し、そのリスクを被害に変えないための環境を整備する。**個人に対する啓発活動**とともに、サービス提供事業者や対策支援主体によるリスク情報、対策情報の適切な提供、事故発生時の対応等の取組みを促進する。

○ 個人の底上げに向けたより効果的な普及・啓発活動の実現

個人の底上げに向け、周知・啓発活動を、関係府省庁が更に連携し、より効果的に実施できるような取組みを進めていく。また、ITに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルを効果的に上げるために、**質問への適切なアドバイスや訪問対応を行えるサポータの育成、地域団体ネットワークの実現を促進**する。

※情報モラルとは、「情報社会で適正な活動を行うための基になる考え方と態度」（高等学校学習指導要領解説　情報編）のこと。

第2次情報セキュリティ基本計画における「地方公共団体」に関する施策

第1次基本計画下での施策：「地方公共団体における情報セキュリティ確保に係るガイドラインの見直し 等」

→地域における情報セキュリティの取組みを進める観点から、地域における情報セキュリティの基盤を強化するべく、地方公共団体が活動しやすい環境が整備されることも重要

第2次計画では

地方公共団体が情報セキュリティの観点から地域で行われる活動を促進できる環境を構築

○小規模な地方公共団体も含めた合理的・自主的な情報セキュリティ対策の促進

小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行う。具体的には、対策や監査の基となる情報資産のリスク分析の実施を促進するとともに、情報セキュリティポリシーの策定等の検討や監査の実施に向けたガイドラインの見直し、業務継続計画の策定に資するガイドライン の普及などを行う。また、**人材面では、取組みを担う職員等の能力向上に向けた共同勉強会や地域セミナーの開催などを進める**。

○ 地方公共団体の取組みを応援する主体の強化

地方公共団体の対策を進めるには、取組みを応援する主体を強化することが有効である。このため、**官・民・NPOによる共同勉強会を開催するなど情報セキュリティに役立つ知見を有するあらゆる主体の協力体制を構築**するとともに、LGWAN（総合行政ネットワーク）内のポータルサイトを活用した自治体向け支援体制の強化などを進める。

○地方公共団体における、地域の情報セキュリティ対策の担い手の育成支援

地域において情報セキュリティ対策を担えるような人材の育成に際しては、地方公共団体による促進活動が有効であることから、地方公共団体のこのような活動が行いやすくなるような環境整備に取り組む。具体的には、地方公共団体が情報セキュリティをテーマとした住民向け教養講座等を開催しやすいよう、講座で活用できるような参考資料等を作成、紹介する。また、**Teaching teachers（教えることのできる人材の教育・育成）の発想に基づき、地方において人材育成が促進されるような取組み**を行う。

個別設計図としての「政府機関統一基準」とは

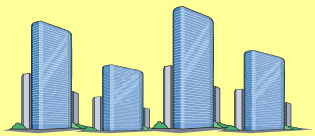
○ **政府機関全体としての情報セキュリティ水準の向上を図る**ための「個別設計図」として、**「政府機関の情報セキュリティ対策のための統一基準」**を策定

○ 各政府機関は本基準を踏まえて対策を実施し、**内閣官房情報セキュリティセンターが対策実施状況を検査・評価**。その結果に基づき、**情報セキュリティ政策会議が改善を勧告**

情報セキュリティ政策会議
- 政府機関統一基準の策定
- 各府省庁の評価結果に基づき改善を勧告

政府機関統一基準
各府省庁が最低限採るべき情報セキュリティ対策を定めたもの。

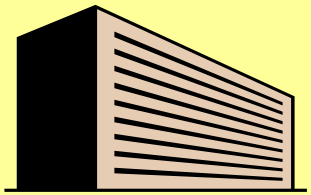
改善勧告



各府省庁
- 政府機関統一基準に基づき、省庁対策基準の見直し

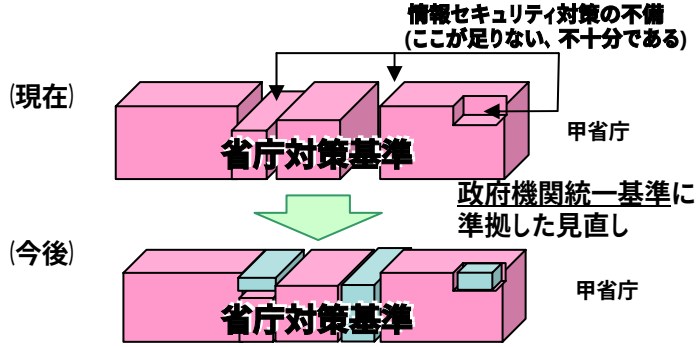
策定・導入 → 運用 → 評価 → 見直し → 策定・導入

対策実施状況の検査・評価
NISCが各府省庁の対策実施状況を検査・評価し、その結果を情報セキュリティ政策会議が改善を勧告する。

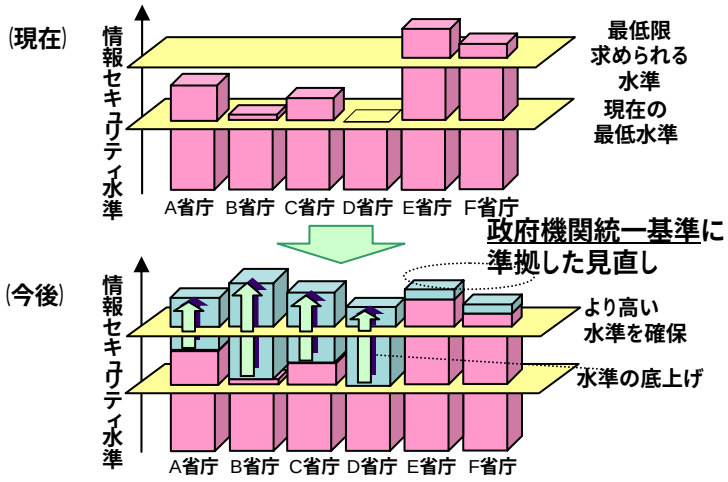


内閣官房情報セキュリティセンター（NISC）

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



「政府全体のＰＤＣＡサイクル」のための各省検査及び評価
～端末・ウェブサーバに関する重点検査（２００７年度）

NISC

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

重要インフラの情報セキュリティ対策に係る第2次行動計画(案)の全体像

NISC

○「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」を目指すとともに、**「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」**を目標に官民が連携して重要インフラ防護に取り組む

○ 新たに分野毎(*)に**重要インフラサービスの検証レベルを設定して着実に改善**を実施

○ 第1次行動計画において設定した施策の4つの柱に着実に取組み、また経験を改善につなげるとともに、**新たに「環境変化への対応」を5つめの柱に**掲げ、変化に対する察知能力の向上と機敏な対応に取り組む

※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（地方公共団体を含む）、医療、水道、物流

第1次行動計画の成果
【2006年度～2008年度】

①安全基準等
- 「重要インフラにおける情報セキュリティの確保に係る「安全基準等」策定にあたっての指針」を策定、改定
- 各分野にて安全基準等の策定、見直し

②情報共有体制
- 官民の情報提供・連絡の体制を整備し、情報提供・情報連絡を開始
- 各分野にてセプターを整備
- セプターカウンシルを創設（予定）

③相互依存性解析
- 静的相互依存性解析を実施
- 動的相互依存性解析を実施

④分野横断的演習
- 研究的演習、机上演習を実施
- 機能演習を実施

第2次行動計画の施策の枠組み
【2009年度～2011年度】

②情報共有体制の強化
情報共有の推進
必要な情報を獲得し活用

①安全基準等の浸透
対策を充実、着実に実践

分野毎の主体的な対策

重要インフラ事業者等による分野横断連携

セプターカウンシル

セプター	セプター	セプター
A分野	B分野	C分野
検証レベル	検証レベル	検証レベル

関係機関　政府

政府等による支援

③共通脅威分析
複数分野に共通の潜在的な脅威を発見

④分野横断的演習
防護対策向上のための課題抽出

⑤環境変化への対応
変化を捉えて機敏に対応

第2次行動計画の概要

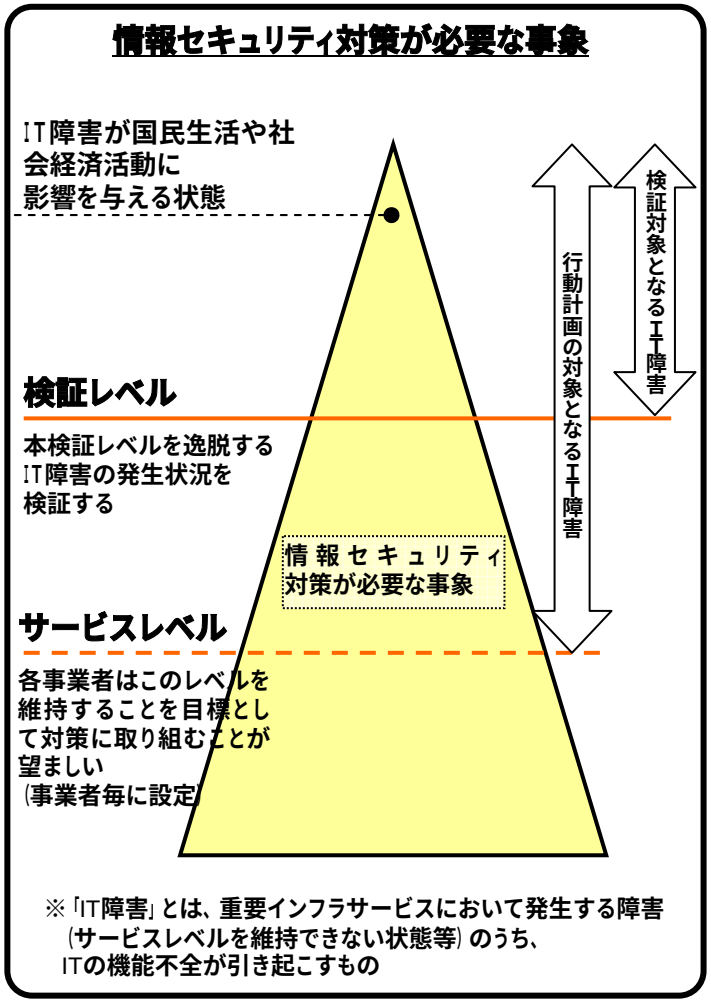
○ IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすることを目標として継続

	第1次行動計画（2006-2008）	第2次行動計画（2009-2011）
総論	➢想定する脅威や防護すべき重要システム等の対策の範囲を設定 ➢情報セキュリティ対策に関する官民連携の施策の枠組みを構築	➢**サービスレベルと検証レベルを定義**、脅威等の対象範囲を見直し ➢アウトカムとなる**「理想とする将来像」を提示**
情報セキュリティ対策の柱	1　安全基準等の整備	1　安全基準等の整備及び浸透
	➢「『安全基準等』策定にあたっての指針」を策定 ➢各分野毎に上記指針を踏まえた「安全基準等」を策定・改定	➢「『安全基準等』策定にあたっての指針」の充実 ➢各分野毎に「安全基準等」の継続的な改善の実施と、確実な浸透
	2　情報共有体制の強化	2　情報共有体制の強化
	➢IT障害に対応するための、官民の情報提供・連絡の体制を整備 ➢各分野毎に「セプター（情報共有・分析機能）」を整備 ➢分野横断的な情報共有の場として「セプターカウンシル」を設立	➢情報セキュリティ対策に資する、共有すべき情報を整理 ➢情報の分析等のセプターに期待される機能を示し、必要な支援を実施 ➢分野横断的な情報共有等のセプターカウンシルに望まれる事項を提示
	3　相互依存性解析	3　共通脅威分析
	➢相互依存性解析の問題提起と実施効果等を記載 ➢内閣官房を中心に、相互依存性解析を試行	➢潜在的なリスクチェーンの把握等のため相互依存性解析を継続 ➢検討対象を技術、システム、環境等に拡大した分野共通の脅威を分析
	4　分野横断的演習	4　分野横断的演習
	➢内閣官房の企画・立案の下、各分野が参加する形態で「研究的演習」、「机上演習」、「機能演習」を段階的に実施	➢具体的なIT障害の発生を想定した分野横断的演習を継続的に実施
		5　環境変化への対応
		➢広く協力、支援を得るため**広報公聴活動**を実施 ➢国際会合や他国機関との対話を通じた**国際連携**を推進
評価・検証	➢3年毎又は必要に応じて行動計画を見直し	➢分野毎にIT障害の**検証レベルを設定**し、また施策毎に**検証指標を設定**して、情報セキュリティ対策の継続的な検証と改善に取り組む ➢指標だけでは把握しきれない状況を収集するために、**補完調査を実施** ➢3年毎又は必要に応じて行動計画を見直し

重要インフラサービスの検証レベル

○**重要インフラ分野毎に業法上の義務的な取組みに加えて、新たに検証レベルを設定**し、これを逸脱するIT障害の発生状況を毎年検証して行動計画の改善を期す

○重要インフラ事業者等は検証レベルによらず各々**サービスレベル**を定め、これを維持することを目標として対策に取り組む事が望ましい



重要インフラ分野		検証レベル （一部表現を簡素化）
情報通信		・電気通信役務の停止、品質の低下が、3万以上の利用者に対し2時間以上継続する事故が生じないこと
		・放送の停止が生じないこと
金融	銀行	・預金の払戻しの遅延、停止が生じないこと ・融資承諾をした貸付の実行の遅延、停止が生じないこと ・為替（銀行振込）の遅延、停止が生じないこと
	生命保険	・保険金等の支払いに遅延、停止が生じないこと
	損害保険	・保険金等の支払いに遅延、停止が生じないこと
	証券会社 金融商品取引所	・預り有価証券等の売却、解約代金の払い出し等に遅延、停止が生じないこと ・有価証券の売買又は市場デリバティブ取引等に遅延、停止が生じないこと
航空		・貨客の運送に支障を及ぼす定期便の欠航が生じないこと
鉄道		・旅客の輸送に支障を及ぼす列車の運休が生じないこと
電力		・供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス		・供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス（地方公共団体を含む）		・住民等の権利利益の保護に支障が生じないこと ・住民等の安全・安心を確保できる時間内にシステムの復旧を行うこと
医療		・診療録等の保存に支障が生じないこと
水道		・断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと
物流		・貨物運送の停止や貨物の紛失が生じないこと

※概要を示すため表現を簡素化しており、正確な表記は第2次行動計画（案）別紙2を参照。

第2次情報セキュリティ基本計画策定に関連した今後のスケジュール