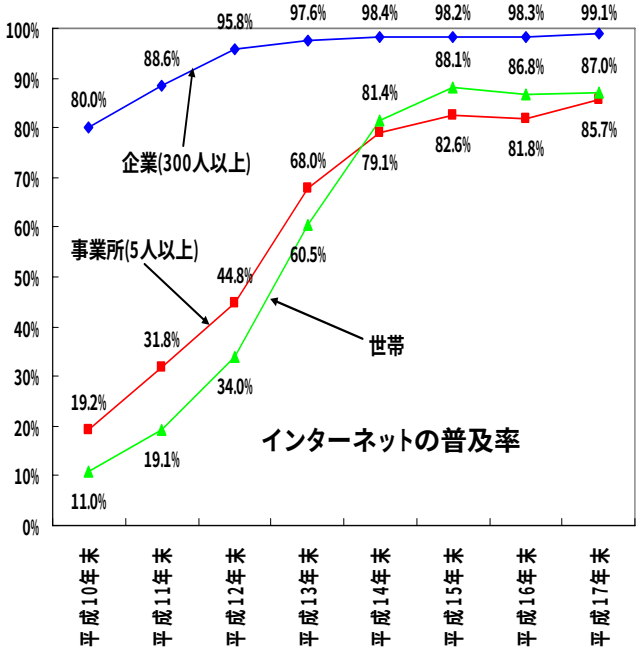
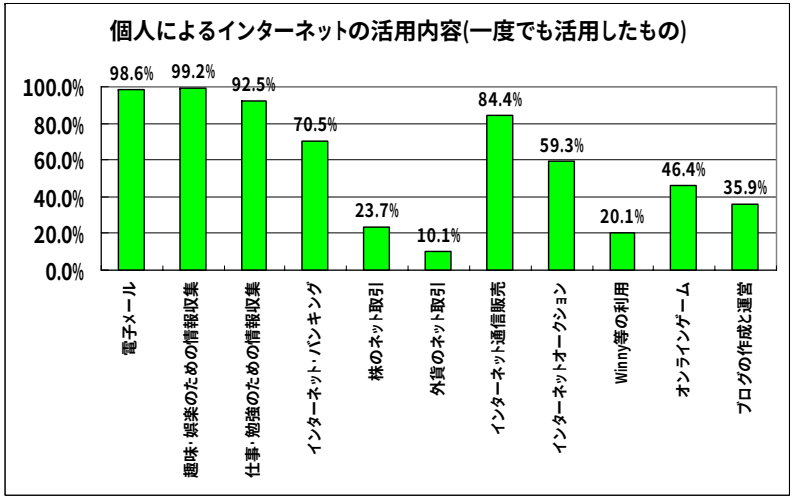
我が国の情報セキュリティ政策の動向について

経済産業省 商務情報政策局
情報セキュリティ政策室

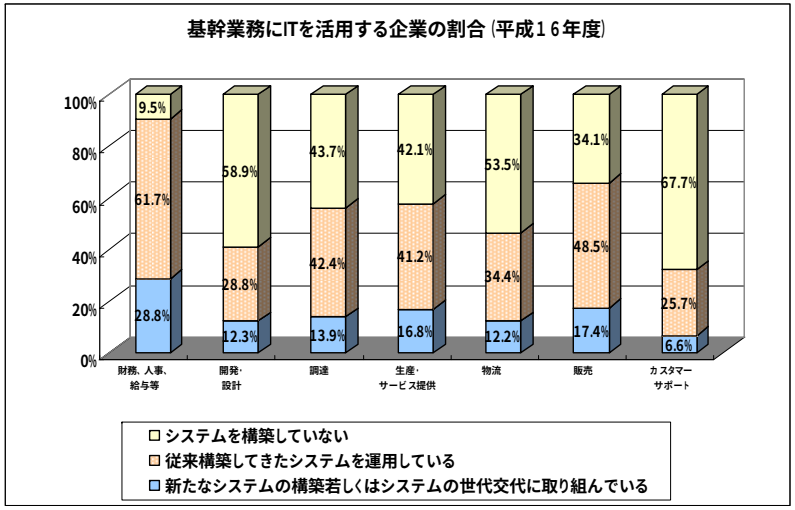
IT化の急速な進展



出所：通信利用動向調査(総務省)等

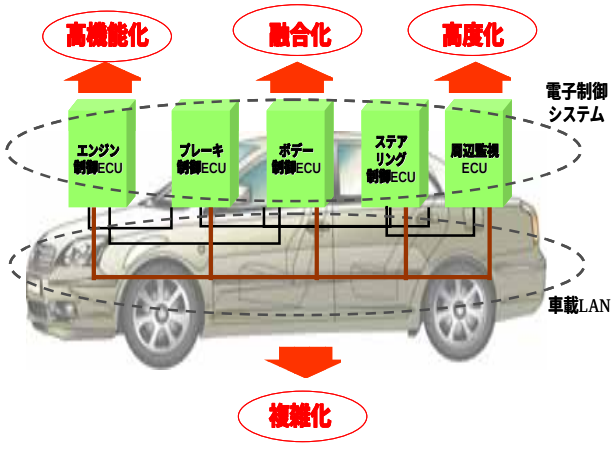


出所：情報セキュリティに関する新たな脅威に対する意識調査(2007年2月：情報処理推進機構)



出所：情報処理実態調査(経済産業省)

自動車においてソフトウェア関連のコストが占める割合は
２００２年　２０％　→　２０１５年(予測)　４０％

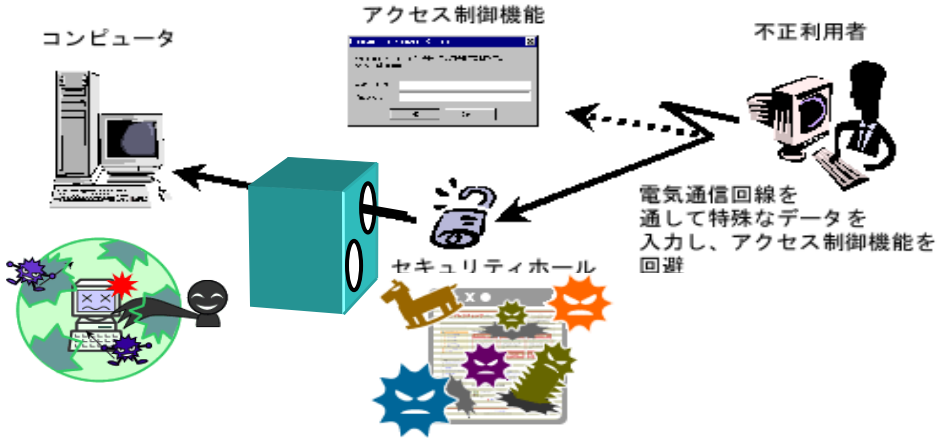


出所：ＪａｓＰａｒ　講演資料

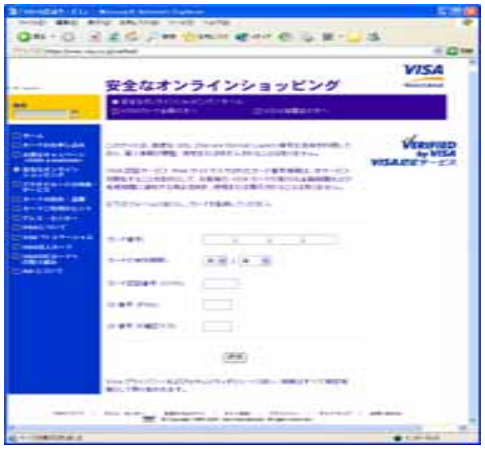
情報セキュリティに関するさまざまな脅威

【コンピュータウイルス】

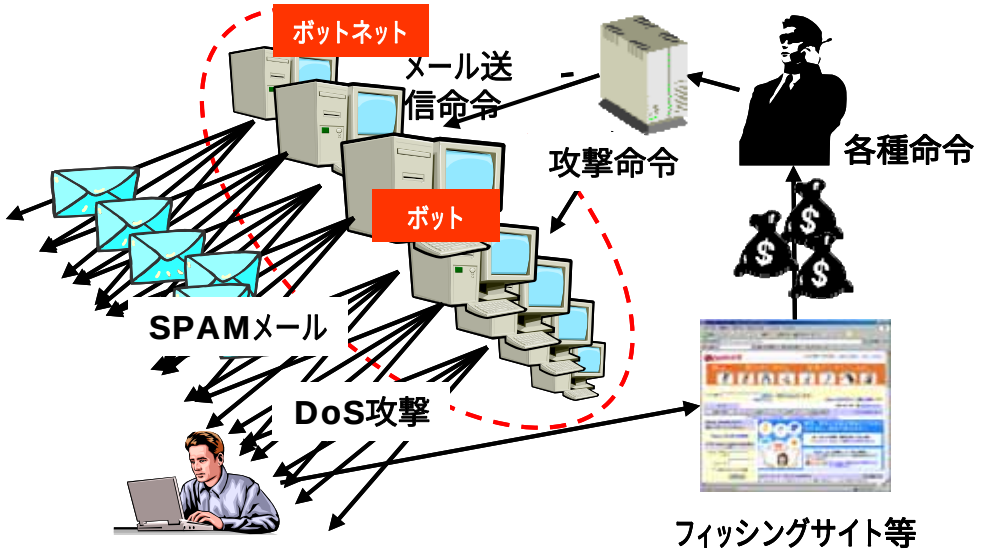
【脆弱性(安全上の問題箇所)】



【フィッシング】



【ボット】



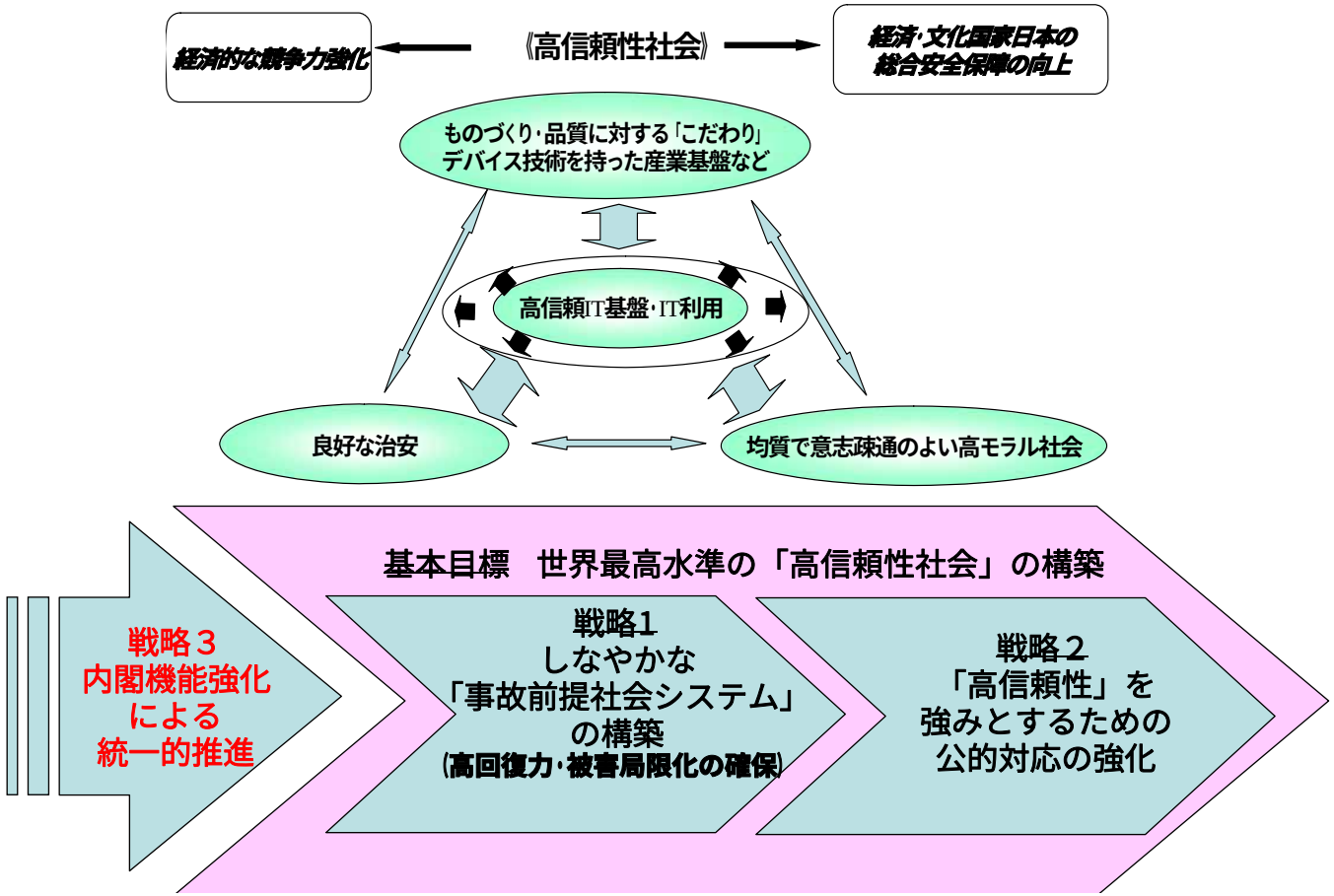
(注) ボット:「ロボット」から取られた造語で、ある種のプログラムを埋め込まれたコンピュータを指す。ボットは、攻撃者の命令に基づき、様々な活動を行う。
SPAM:公開されているWebサイトなどから手に入れたe-mailアドレスに向けて、営利目的のメールを無差別に大量配信すること。
DoS攻撃:“Denial Of Service”の略。大量のデータを送信すること等により、Webサイトが提供するサービスを妨害、停止させる行為。

我が国政府における統一的・横断的な施策推進体制の整備

「情報セキュリティ総合戦略」－産業構造審議会報告書

METI 経済産業省

- 2003年10月、経済産業大臣の諮問機関である産業構造審議会の情報セキュリティ部会において、**我が国初の総合的な情報セキュリティに関する戦略である「情報セキュリティ総合戦略」を策定。**
  - ■ 基本目標を、経済・文化国家日本の強みを活かした「世界最高水準の『高信頼性社会』の構築」と位置付け。
  - ■ その要となる「情報セキュリティ対策」について、**3つの戦略**(42の施策項目)**を提言**。



政府全体の取組み

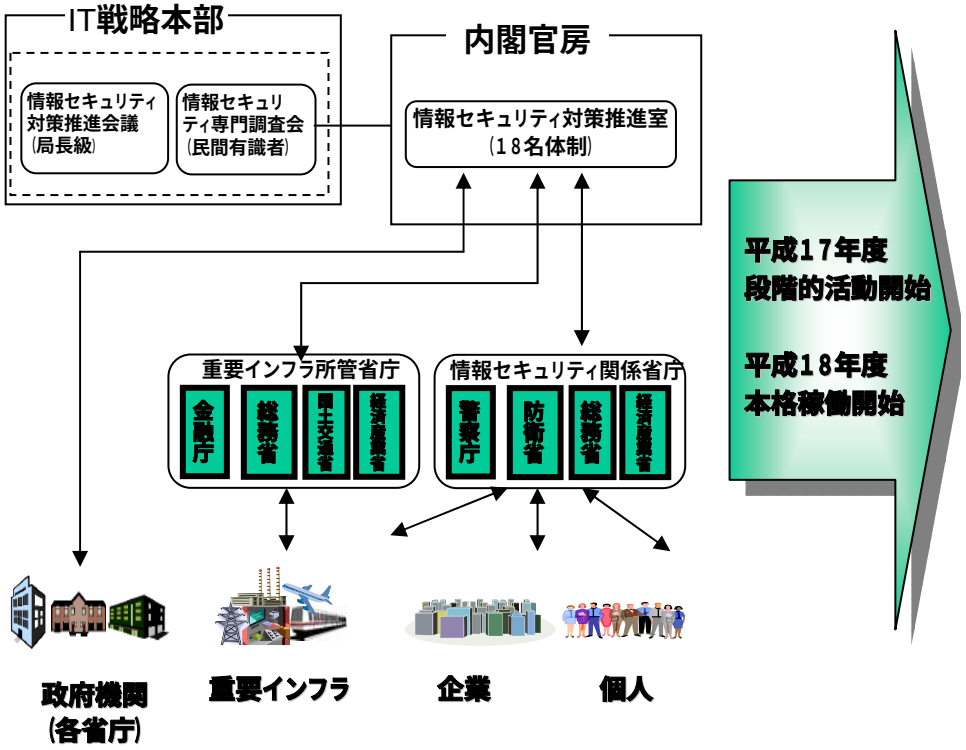
～内閣官房情報セキュリティセンター（NISC）及び情報セキュリティ政策会議の設置～

METI 経済産業省

- 「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。
  - 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(議長：内閣官房長官)」を設置。

→これまでの開催実績：2005年：7月14日(第1回)、9月15日(第2回)、12月13日(第3回)、
2006年：2月2日(第4回)、4月28日(第5回) 6月15日(第6回)、7月25日(第7回)、10月25日(第8回),
12月13日（第9回）、2007年2月2日(第10回)、4月23日(第11回)

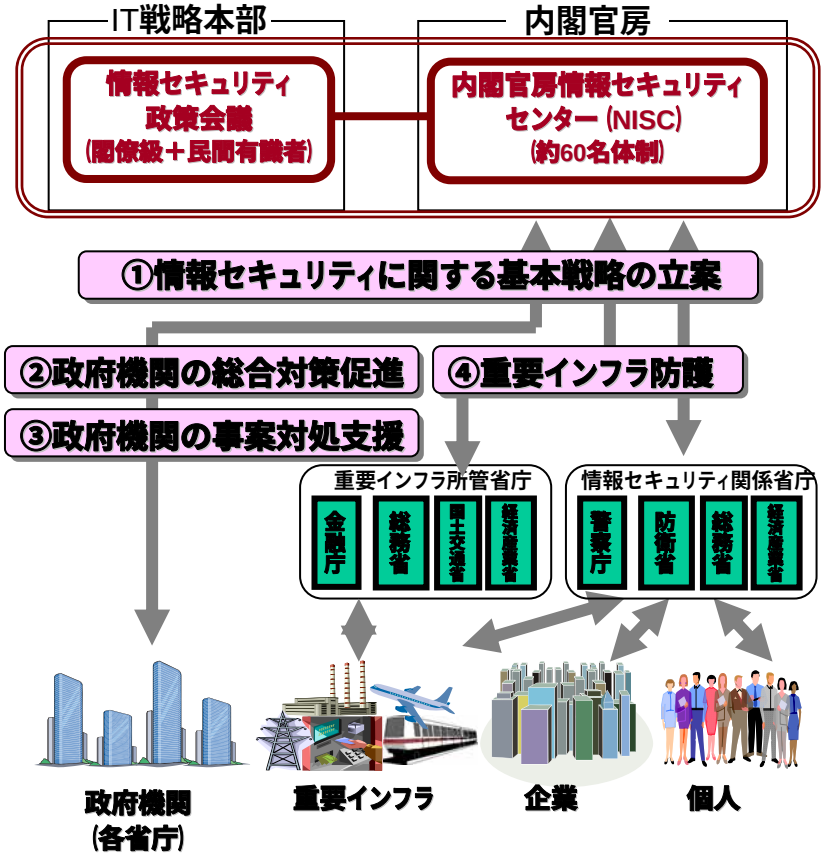
＜旧体制＞



平成17年度 段階的活動開始

平成18年度 本格稼働開始

＜新体制＞



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（イノベーション）

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

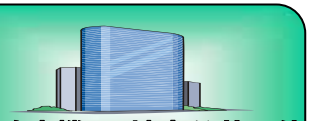
江畑 謙介	拓殖大学客員教授／軍事評論家
小野寺 正	KDDI(株) 代表取締役 社長兼会長
黒川 博昭	富士通株式会社代表取締役社長
野原 佐和子	(株) イプシ・マーケティング研究所代表取締役社長
前田 雅英	首都大学東京教授
村井 純	慶應義塾大学教授

（有識者構成員は、五十音順。敬称略）

「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2007」等の位置づけ

「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

目標


政府機関・地方公共団体


重要インフラ


企　業


個　人

重要政策横断的な


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

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

「セキュア・ジャパン2006」

① 2006年度の実施計画
～「官民におけるセキュリティ対策の体制の構築」

② 2007年度の重点施策の方向性
～「官民におけるセキュリティ対策の底上げ」

報告

評価
2006

「セキュア・ジャパン2007」（案）

① 2007年度の実施計画（159施策）
～「官民におけるセキュリティ対策の底上げ」

② 2008年度の重点施策の方向性（24施策）
～「セキュリティ基盤強化に向けた集中的取組み」

報告を受け止める形で政策会議として現状を認識・評価

セキュア・ジャパン2008

報告

評価
2007

今後のスケジュール

・4月23日から約1ヶ月間のパブリックコメントを経た後、6月の政策会議（予定）において最終決定

政府機関統一基準

（2005年12月13日　第3回情報セキュリティ政策会議決定）

METI 経済産業省

● 世界最先端のIT(情報技術)国家にふさわしい情報セキュリティ水準を目指して、統一基準を運用

各府省庁の現状	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（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ガイドライン等を今後多数作成（重要なものは年内目途）
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

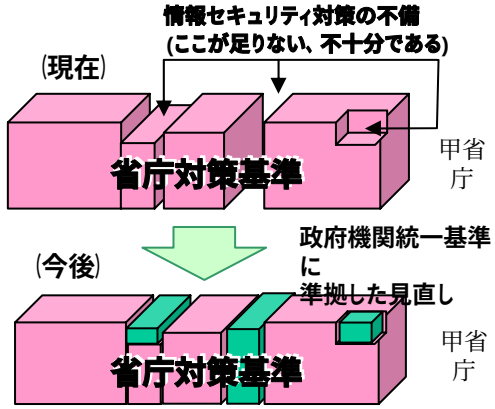
穴が埋まる

本質的原因

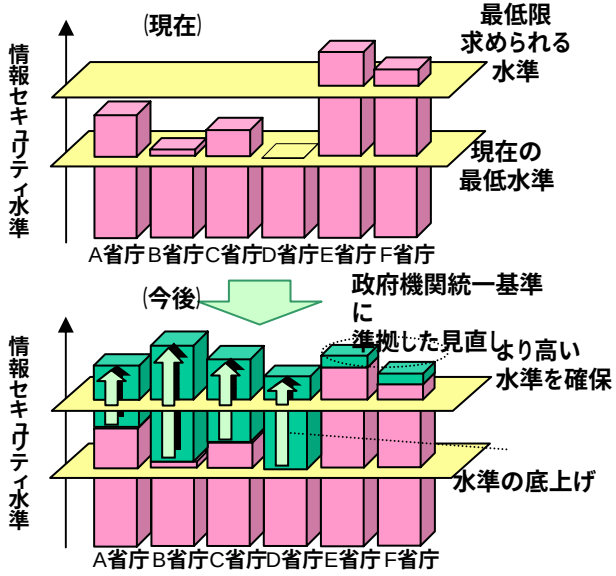
迅速・的確

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



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

(2006年7月25日情報セキュリティ政策会議資料)

METI 経済産業省

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 ・アンチウィルスソフトの運用状況
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 ・ウェブサーバ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18年3月末時点

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

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%

各省庁からの対策実施状況報告(2006年度)の概要①

(2007年4月23日情報セキュリティ政策会議資料)

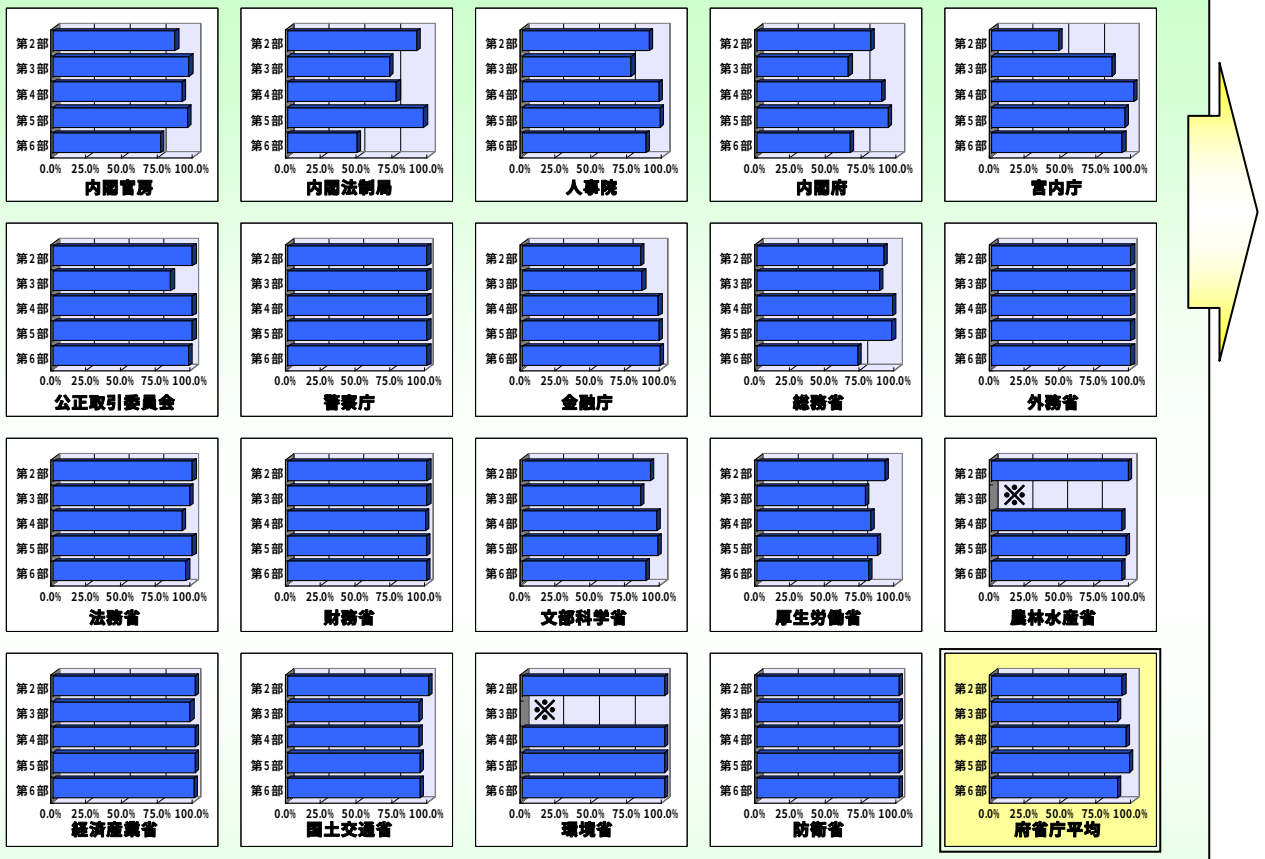
METI 経済産業省

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	31.2 %
(独自の調査を含める場合)	(98.2 %)
経済産業省	100.0 %
国土交通省	100.0 %
環境省	40.7 %
(独自の調査を含める場合)	(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○部の集計 (実施率の算出例)

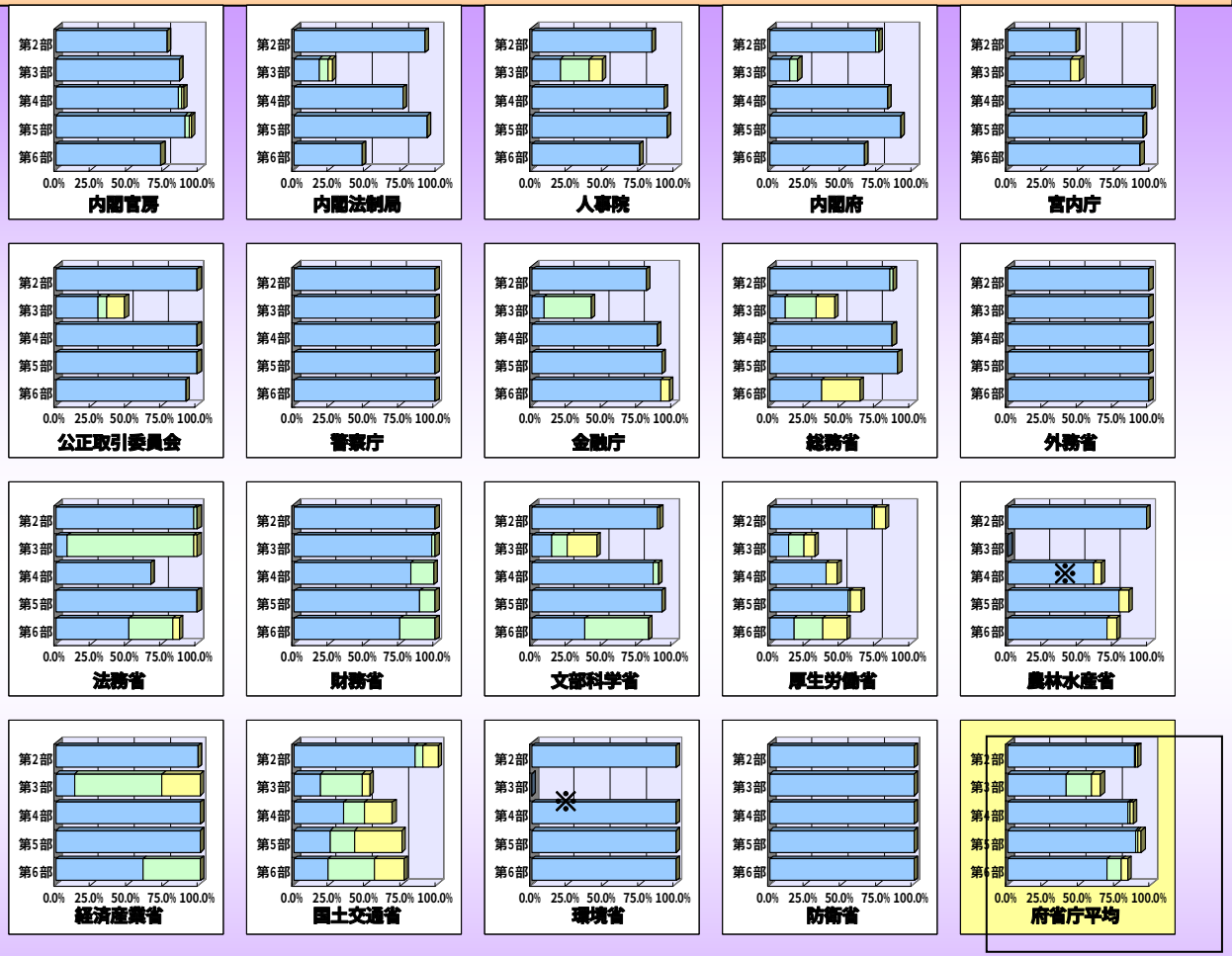
	実施状況	割合	実施率
遵守事項 (a)	2人中1人実施	50%	割合の単純平均 75%
遵守事項 (b)	100人中75人実施	75%	
遵守事項 (c)	10人中10人実施	100%	

各省庁からの対策実施状況報告(2006年度)の概要②

(2007年4月23日情報セキュリティ政策会議資料)

METI 経済産業省

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)



※：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)

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

「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）

METI 経済産業省

●２０００年１２月に策定された**「重要インフラのサイバーテロ対策に係る特別行動計画」**は、増大するサイバーテロの脅威から7つの重要インフラ分野の防護のための初めての官民協力の枠組みについて規定。

●その後の各重要インフラ分野におけるIT利用の飛躍的進展とITへの依存度の増大、重要インフラ間相互の依存性の増大等の変化を踏まえ、**「重要インフラの情報セキュリティ対策に係る基本的考え方」（２００５年９月１５日　情報セキュリティ政策会議決定）**に基づき、新たな行動計画を策定。

対象分野・脅威の見直し

基本的考え方	行動計画
➢ 重要インフラ分野として、医療・水道・物流を加えた１０分野を設定 ➢ 想定する脅威を、「サイバー攻撃」に加えて、人為的ミス等の「非意図的要因」、「自然災害」へと拡大	➢ 重要インフラ分野として１０分野*を指定し、具体的対象事業の範囲を設定 ➢ 想定する脅威及び各分野別重要システムを例示

新たな体制の構築

１．情報セキュリティ水準の向上

➢ 技術的基準及び運用基準についての「安全基準・ガイドライン」の策定・見直し等を実施	➢ ２００５年度中に、内閣官房情報セキュリティセンターは「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を策定 ➢ 各分野は、上記指針を踏まえて、必要又は望ましい情報セキュリティ対策の水準を２００６年９月を目処に「安全基準等」に明示するよう努力

２．情報共有体制の強化

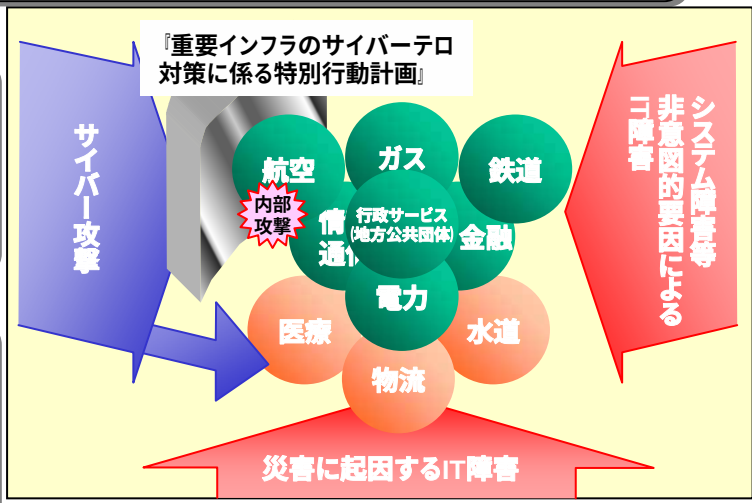
➢ 情報提供体制の整理・強化、情報充実・質の向上 ➢ 「情報共有・分析センター」（仮称）等の各分野内情報共有機構の創設 ➢ 重要インフラ横断的な情報共有の推進（「重要インフラ連絡協議会（仮称）の設立等）	➢ IT障害発生時における連絡体制等、官民の情報共有、連絡・連携の仕組みについて具体的に規定 ➢ ２００６年度末まで**に各重要インフラ分野ごとに「情報共有・分析機能（CEPTOAR）」の整備を推進 ➢ 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の設立の場を内閣官房に設置

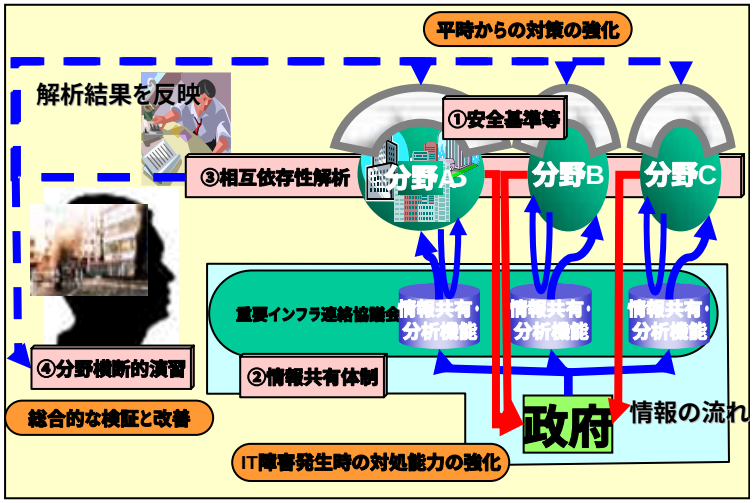
３．相互依存性解析

➢ 内閣官房情報セキュリティセンターを中心に重要インフラ分野横断的な状況把握（相互依存性解析等）を実施	➢ 相互依存性解析の効果・実施の流れを記載 ➢ 内閣官房情報セキュリティセンターを中心に、２００６年度から相互依存性解析を試行

４．分野横断的演習の実施

➢ 想定脅威に対応した具体的脅威シナリオの類型を元に、毎年度、重要インフラ分野横断的な演習を実施	➢ ２００６年度に「研究的演習」、「机上演習」、２００７年度に「機能演習」を段階的に実施 ➢ 内閣官房において「演習実施計画」を立案、内閣官房の監修の下、各重要インフラから参加する形態で実施



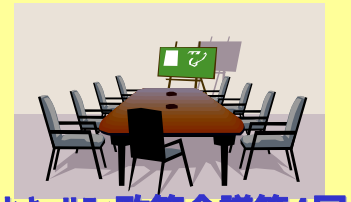


*情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流
**新規追加分野についてはCEPTOAR整備に関する基本的合意を２００６年度末までに完了し、２００７年度に実際の整備を行うことを目指す。

重要インフラにおける安全基準等の策定・見直し状況 (2006年12月13日情報セキュリティ政策会議資料)

METI 経済産業省

重要インフラ所管省庁の協力を得て、「安全基準等」策定・見直し状況の調査を行った結果、以下の通り、策定・見直しがなされつつあることを確認 (2006年11月現在)



情報セキュリティ政策会議第4回会合 (2006年2月2日)

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を決定

重要インフラ

必要な又は望ましい情報セキュリティ対策の水準について「安全基準等」に明示

分野	安全基準等の名称【発行主体】	策定・見直し状況
情報通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等 (関連する告示を含む) 情報通信ネットワーク安全・信頼性基準【総務省】 電気通信分野における情報セキュリティ確保に係る安全基準 (第1版)【ISeCT】(※1)	実施済
	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン【日本放送協会 (NHK)、(社) 日本民間放送連盟】	実施済
金融	金融機関等におけるセキュリティポリシー策定のための手引書【FISC】(※2) 金融機関等コンピュータシステムの安全対策基準・解説書【FISC】 金融機関等におけるコンティンジェンシープラン策定のための手引書【FISC】	実施済
航空	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン【国土交通省】 航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン【国土交通省】	実施済
鉄道	鉄道分野における情報セキュリティ確保に係る安全ガイドライン【鉄道事業者等】	実施済
電力	電力制御システム等における技術的基準・運用基準に関するガイドライン【電気事業連合会】	実施済
ガス	製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン【(社) 日本ガス協会】	実施済
政府・行政サービス	地方公共団体における情報セキュリティポリシーに関するガイドライン【総務省】	実施済
医療	医療情報システムの安全管理に関するガイドライン【厚生労働省】	見直し中 (※3)
水道	水道分野における情報セキュリティガイドライン【厚生労働省】	実施済
物流	物流分野における情報セキュリティ確保に係る安全ガイドライン【国土交通省】	実施済

(※1) ISeCT:電気通信分野における情報セキュリティ対策協議会　(※2) FISC: (財) 金融情報システムセンター
(※3) 今年度中に見直し完了予定

(参考)「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」と政府機関統一基準との関係

重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（2006 年2 月）

5．本指針を踏まえた安全基準等策定若しくは見直しへの期待

本指針は、個々の重要インフラ分野及び重要インフラ事業者等において、既にどのような安全基準等が定められているかについて考慮していないため、本指針に記載した全ての項目を既に包含した安全基準等を持つ重要インフラ分野又は重要インフラ事業者等も存在し得る。
ただし、本指針は、あくまで最低限の情報セキュリティ対策が講じられるよう安全基準等の策定若しくは見直しを支援するために策定されたものであることから、個々の安全基準等においては、より高度な情報セキュリティ水準の実現を目指し、本指針に示された項目を満たすだけでなく、一層高度かつ網羅的な安全基準等となるよう、随時検討がなされることを期待する。
このような観点からは、各種規格をはじめとする国内外のベストプラクティスを積極的に参考にしていくとともに、別途決定する「政府機関の情報セキュリティ対策のための統一基準」及び関連文書を適宜参照することが望ましい。

「重要インフラ事業者等」とは、「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」及び「物流」の各分野に属する事業を営む者のうち、「重要インフラの情報セキュリティ対策に係る行動計画（2005 年12 月13 日高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議決定）別紙1 の「対象となる事業者」に指定された者及びこれらの者から構成される団体を指す。

経済産業省施策の概要と
今後の方向性について

経済産業省の情報セキュリティ施策（概要）

METI 経済産業省

企業等

継続的な普及広報活動

個人

組織的対策の推進

企業等のマネジメント面での情報セキュリティ対策の推進

企業が情報セキュリティマネジメント等を適切に実施することにより、組織内の内部からの情報漏洩、不正アクセス等を防止

内部不正、システム設定ミス等

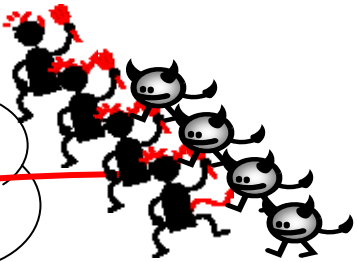
PC

サーバー

ルーター

インターネット

ウイルス、不正アクセス等



安全上の問題箇所システム障害等

技術的対策の推進

セキュリティ評価の推進

IT製品等の安全性に係る評価制度等を整備し、安全な製品の普及を図ることにより、IT製品の安全上の問題箇所等に起因する不正アクセス等を防止

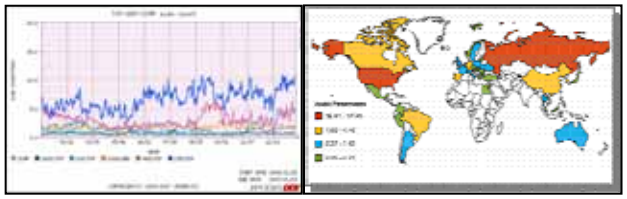
技術開発・研究開発の実施

新たな脅威に対応するため、情報セキュリティに係る技術開発及び研究開発を実施

早期警戒体制の整備

情報セキュリティの確保を図るために不可欠な情報の収集・分析・提供

脅威（ウイルス、不正アクセス等）に関する情報を早期に収集・分析し、その脅威に対する対策情報等を迅速に提供することにより、被害の拡大を抑制



経済産業省施策の今後の方向性

産業構造審議会情報セキュリティ基本問題委員会報告書

グローバル情報セキュリティ戦略

～我が国経済社会が直面し続ける「変化と挑戦」を支える基盤としての情報セキュリティ政策の飛躍～

情報セキュリティ政策の経緯

METI 経済産業省

■黎明期：一部業務へのIT導入

■愉快犯の能力誇示
■限定的被害

■過渡期：インターネットとPCの爆発的普及

■被害の大規模化
■攻撃手段の情報入手が容易に

・中央省庁ホームページ改ざん事件('00)
・官公庁サイト攻撃('01)
・航空管制システム障害による全面運航停止('03)
・金融機関ATMサービス障害('04)
・東京証券取引所のシステム障害('05)

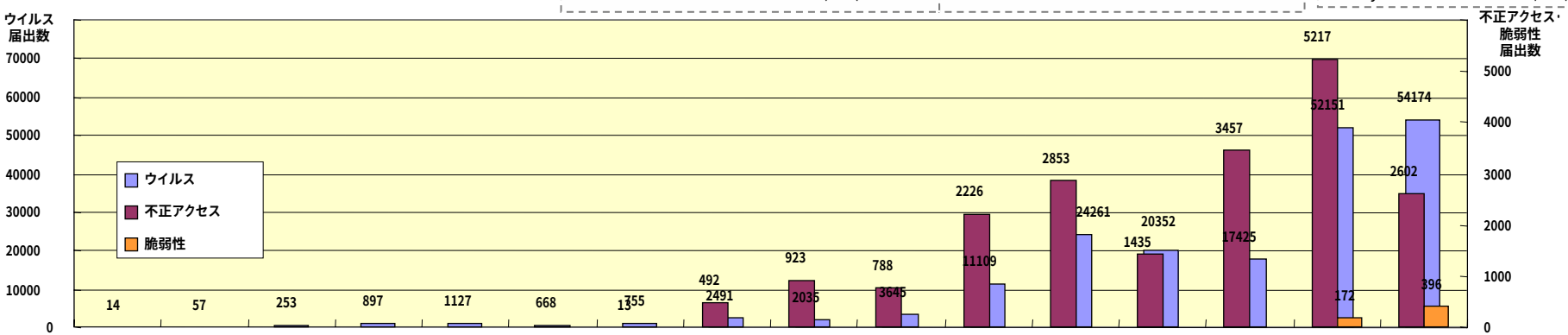
■ソフトウエア脆弱性問題の顕在化
■ウイルスの機能高度化

・脆弱性悪用型ウイルス（Nimda）登場('01)
・Webサーバの脆弱性をついた攻撃が頻発('02)
・脆弱性利用ウイルス（Slammer)により韓国インターネットインフラが全面停止('03)

■発展期

■脅威の高度化
■経済的利得を目的とした事件

・ボットによる大規模被害が報告('04)
・政府・企業からの情報漏洩多発('04)
・フィッシング詐欺・スパイウエアが社会問題化('05)
・Winny等を介した情報漏洩('05)



■コンピュータウイルス対策基準策定（METI）
■コンピュータウイルス対策室設置（IPA）
■情報システム安全対策基準改訂（METI）
■情報セキュリティセミナー開始（IPA）
■コンピュータ不正アクセス対策基準策定（METI）
■JPCERT/CC設立（METI/JIPDEC）
■情報セキュリティ政策室設置（METI）
■情報セキュリティセンター設置（IPA）
■電子署名及び認証業務に関する法律施行
■暗号技術評価委員会CRYPTREC（MIC/METI）
■情報セキュリティ対策推進室設置（内閣官房）
■電子政府情報セキュリティ基盤技術開発事業（METI/IPA）
■不正アクセス行為の禁止等に関する法律施行
■ITセキュリティ評価・認証制度創設（METI/IPA）
■電子政府の情報セキュリティ確保のためのアクションプラン策定（IT戦略本部）
■情報セキュリティマネジメントシステム適合性評価制度創設（METI/JIPDEC）
■緊急対応支援チームNIRT設置（内閣官房）
■インターネット定点観測システム開発（METI/JPCERT/CC）
■情報セキュリティ監査制度創設（METI）
■情報セキュリティ管理基準・監査基準（METI）
■インターネット安全教室開始（METI）
■情報セキュリティ総合戦略策定（METI）
■脆弱性関連情報届出制度創設（METI/IPA）
■電力サイバーテロ対策等促進事業（METI）
■企業における情報セキュリティガバナンスのあり方に関する研究会（METI）
■フィッシング対策協議会設立（METI）
■セキュア・ジャパン（政策会議）
■第一次情報セキュリティ基本計画（政策会議）
■情報セキュリティ政策会議設置（IT戦略本部）
■内閣官房情報セキュリティセンター（NISC）設置

METI－IPAの体制整備
ウィルス対策等の対処療法的対応

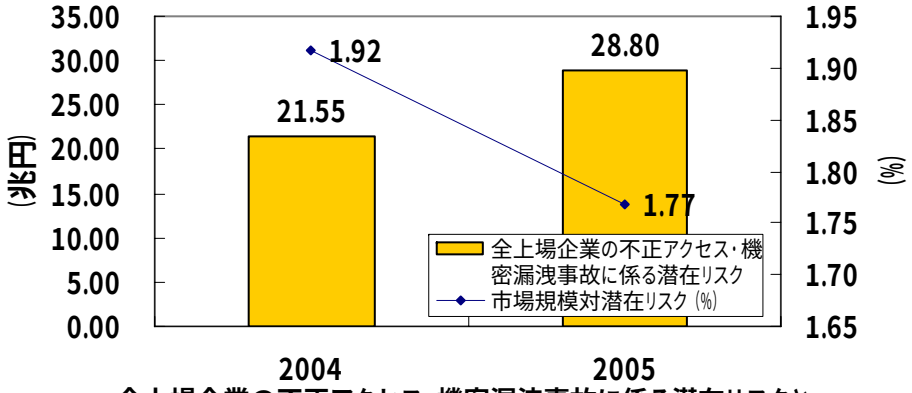
METI－IPAの体制強化
基盤となる基準、制度等の整備

内閣官房による調整機能整備
総合的な対策のための基準、制度の整備

内閣官房の体制強化
政府横断的な対策実施

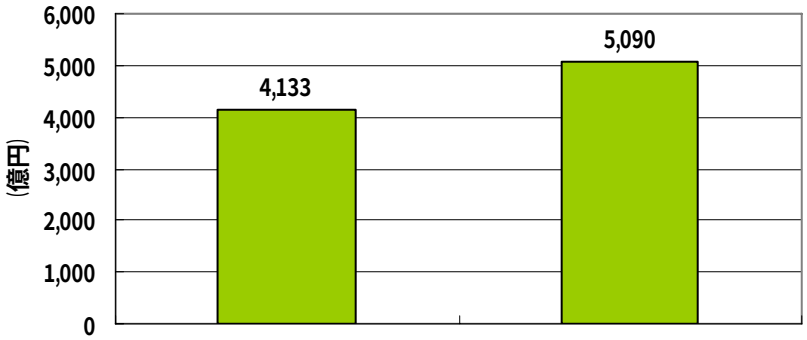
情報セキュリティに関する脅威の傾向

■情報セキュリティ事故が企業価値に与える影響が無視できなくなってきている
　◇H17年の全上場企業の不正アクセス・機密漏洩事故に係る潜在リスクは約２９兆円
■経済的利得を目的とした危険性の高い脅威が増大
　◇H18年の日本におけるオンライン詐欺被害額は1304億円と推計（ブロードバンド推進協議会）
　◇H17年の米国におけるフィッシング被害は9億2900万ドルと推計（Gartner）
■無差別的な攻撃に加え、特定の者を対象とする攻撃が増加



全上場企業の不正アクセス・機密漏洩事故に係る潜在リスクと潜在リスクに対する情報セキュリティ市場規模の比率

世界銀行資料、内閣府資料、経済産業省委託調査より推計



我が国における情報セキュリティ市場規模

経済産業省委託調査

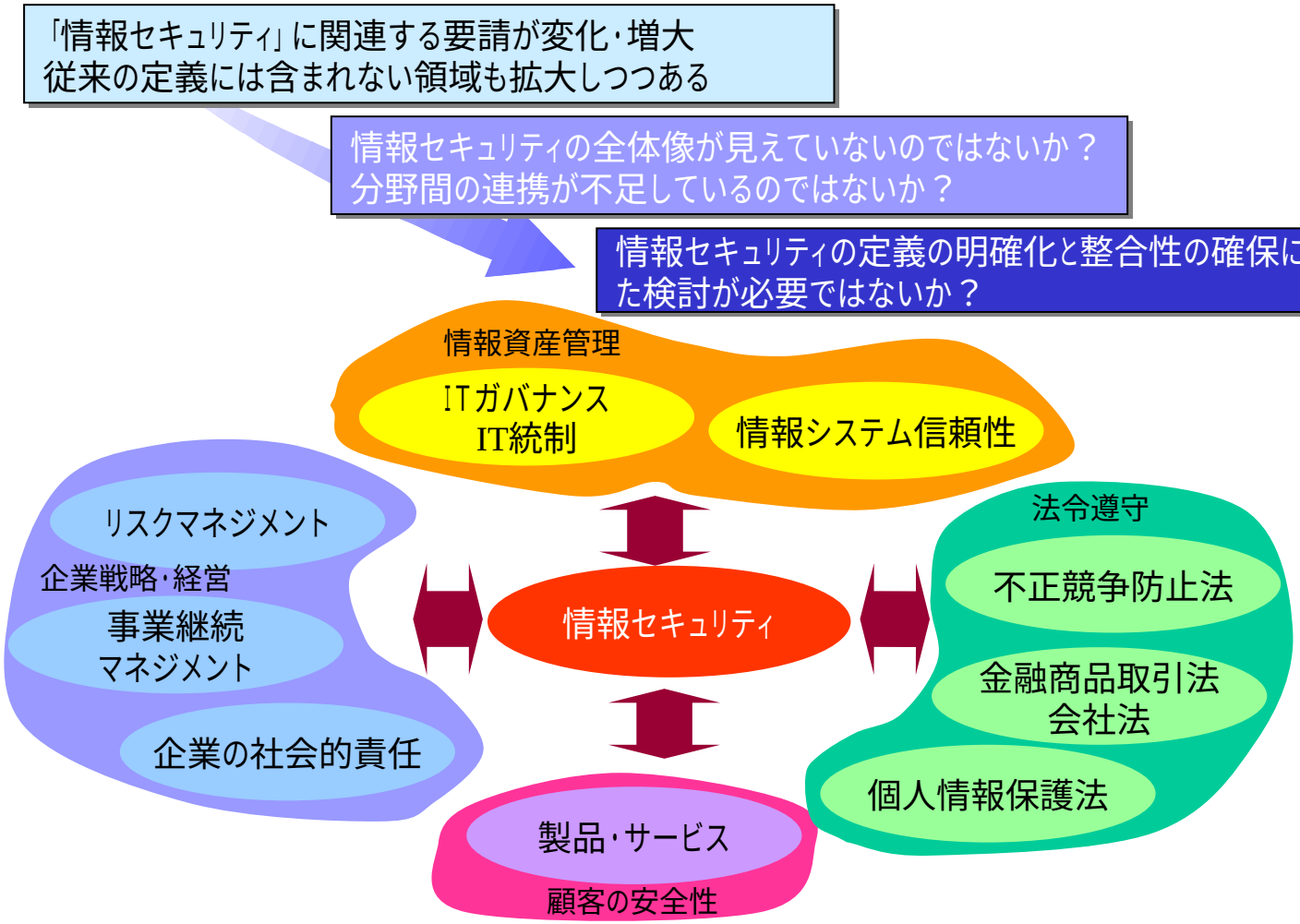
防衛庁を騙ったウイルス付きメールに対する注意喚起

平成１７年頃より、特定の政府機関、内閣官房、外務省、防衛庁、警察庁、経済産業省等を狙ったウイルス（スピア型ウイルス）が顕著に増加。大量拡散を目的としていないことから、ウイルス対策ソフトにも検出されない。感染した場合、情報漏洩や、外部からPCをコントロールされる恐れ。
企業においても同様の傾向があるものと推定されるが、被害は明らかになっていない。

情報セキュリティに関連する要請の変化・増大～広がりの兆候～

■情報セキュリティに関連する要請の変化・増大

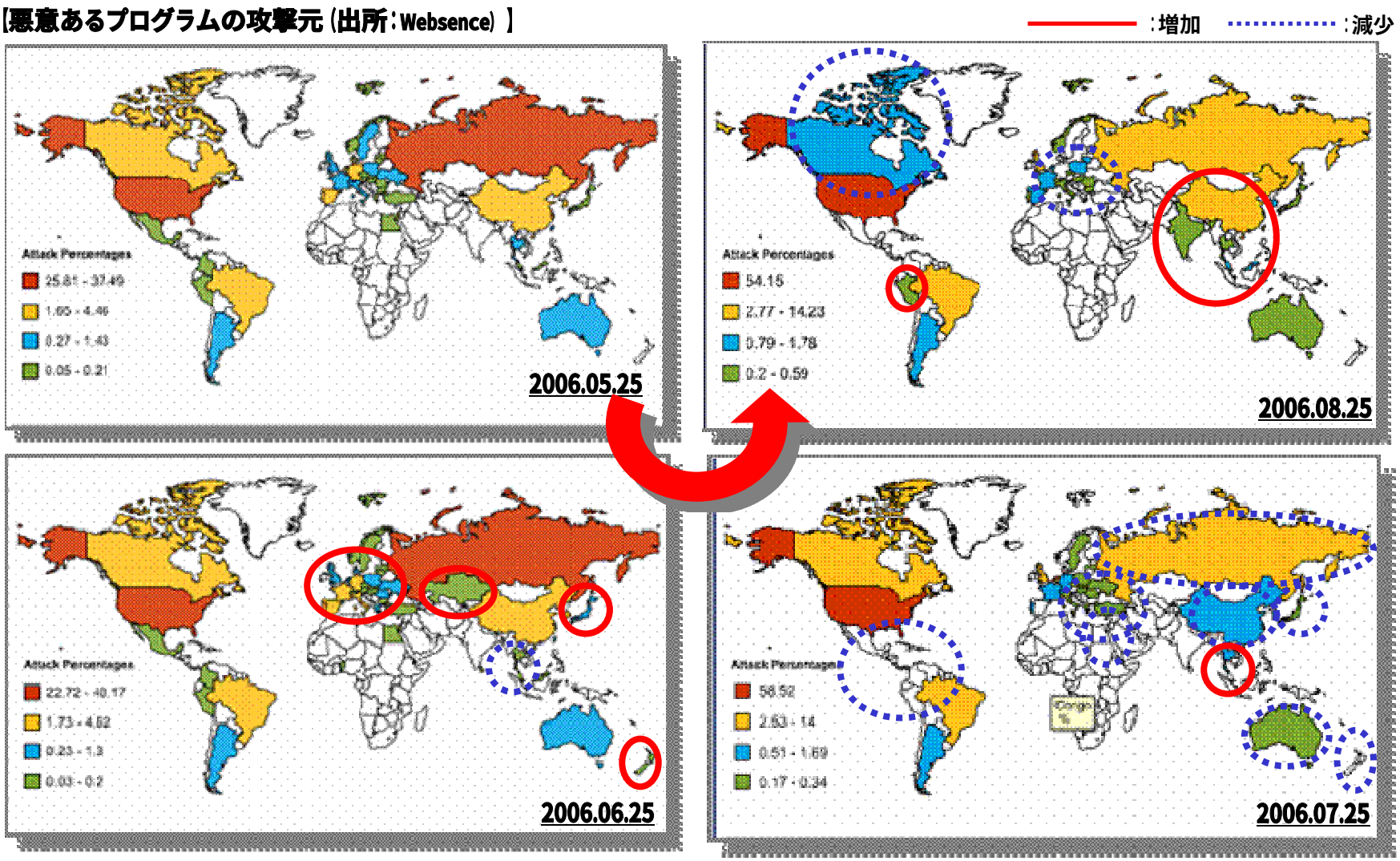
ー情報セキュリティ対策が法令遵守の観点、企業経営・戦略の観点、顧客の安全性などの観点からも求められるようになってきていることに加え、信頼性等、従来の情報セキュリティの定義（機密性（Confidentiality）、完全性（Integrity）、可用性（Availability））には含まれない領域も徐々に拡大



攻撃側における国境を越えた活動

■ 例えば、ウィルス等の悪意のあるプログラムの攻撃元を時系列で見ると、攻撃元の地域は頻繁に変化していること、すなわち、国境を越えた活動が活発に行われていることが分かる。

【悪意あるプログラムの攻撃元（出所：Websence）】



「グローバル情報セキュリティ戦略」の概要①

METI 経済産業省

ITが国内外の経済社会システムに融合化し、情報セキュリティに関する脅威も国際化傾向にある中、産業構造審議会情報セキュリティ基本問題委員会は、次の3つの戦略(60の施策項目)からなる「グローバル情報セキュリティ戦略」を取りまとめ。

戦略1　我が国を真に「情報セキュリティ先進国」とするための取組み

戦略2　国際化する脅威に対応し、我が国の国際競争力を強化していく観点からの情報セキュリティ政策のグローバル展開

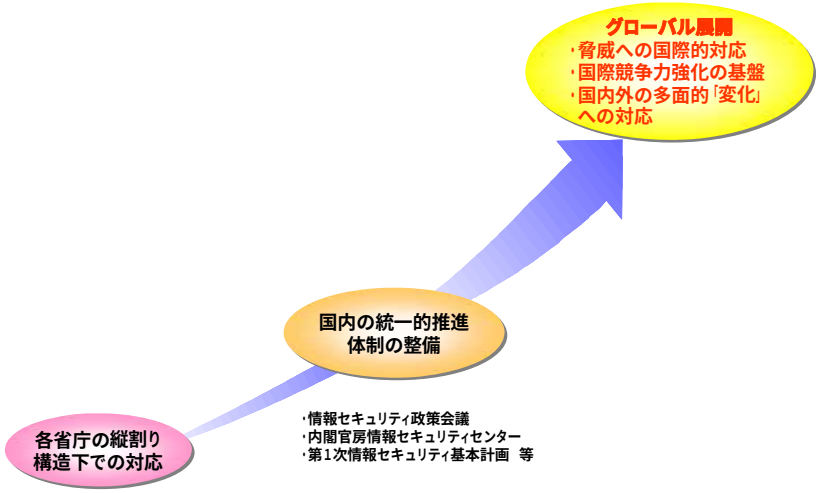
戦略3　国内外の変化に対応するためのメカニズムの確立

これまでの経緯と本戦略の位置付け

○政府の施策が縦割り構造での独自対応となっている等の問題意識の下、産業構造審議会情報セキュリティ部会は、「世界最高水準の『高信頼性社会』実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」という基本目標の下、「内閣機能強化による統一的推進」等を掲げた「情報セキュリティ総合戦略」を2003年に策定。

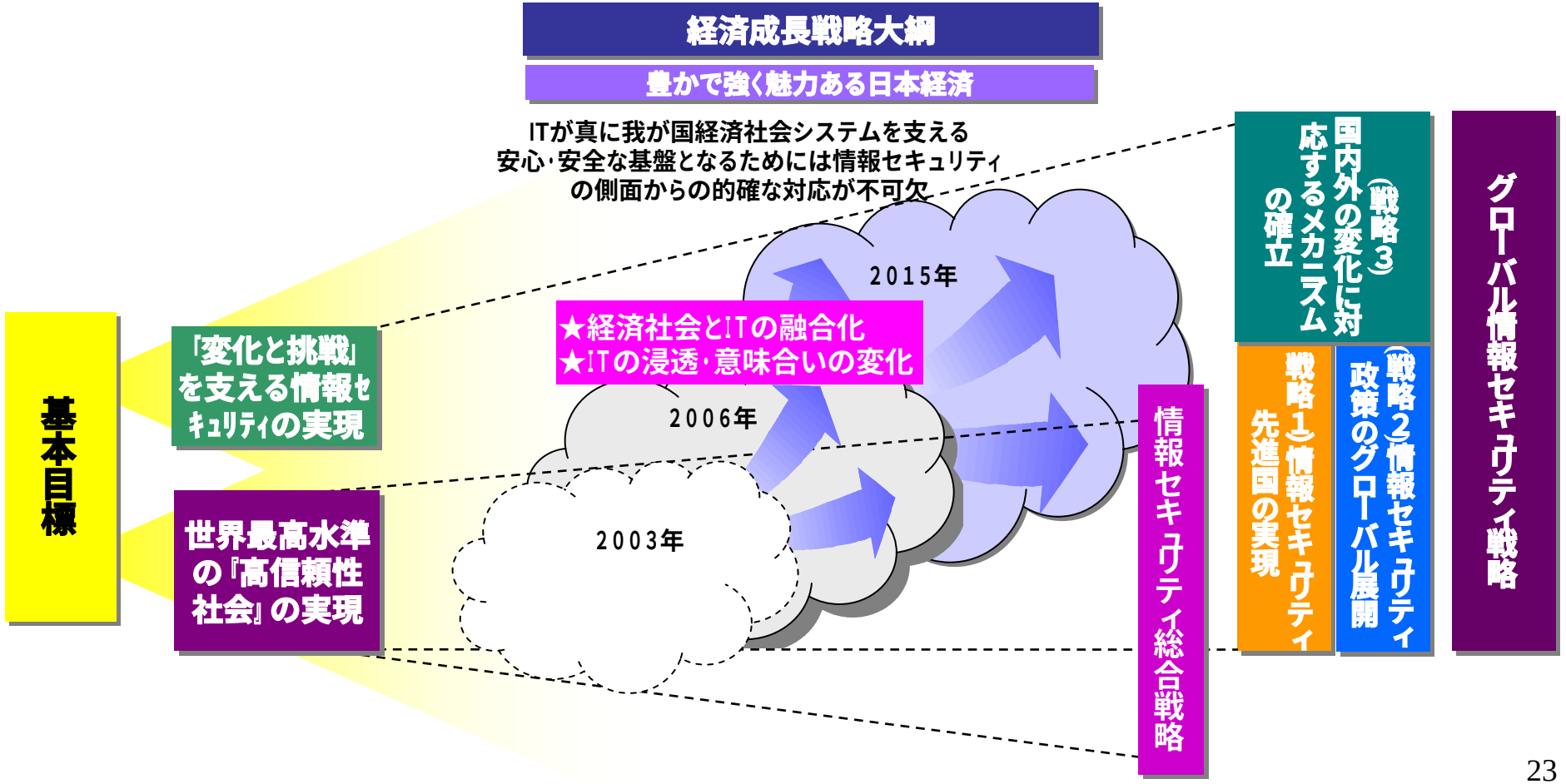
○現在、内閣官房情報セキュリティセンター(以下、「NISC」という)及び情報セキュリティ政策会議(以下、「政策会議」という)が設置され、政策会議で「第1次情報セキュリティ基本計画」が決定される等、国内の統一的推進体制の整備が進展中。

○国際化する脅威への対応に加え、我が国の国際競争力強化基盤を整備し、かつ、国内外で経済社会が直面し続けるであろう多面的「変化」に的確に対応していくため、2007年5月、産業構造審議会情報セキュリティ基本問題委員会は、新たな戦略として「グローバル情報セキュリティ戦略」を取りまとめ。



「グローバル情報セキュリティ戦略」の概要②

■総合戦略で掲げた「世界最高水準の『高信頼性社会』の構築」は引き続き重要な基本目標
■経済社会システムの構造の多面的「変化」に迅速かつ適切に対応し、「経済成長戦略大綱」の掲げる「豊かで強く魅力ある日本経済」を実現するという「挑戦」の歯車を円滑に機能させるため、情報セキュリティ政策の基本目標に「『変化と挑戦』を支える情報セキュリティの実現」を追加



「グローバル情報セキュリティ戦略」の概要③

METI 経済産業省

戦略1：情報セキュリティ先進国の実現

➢ 現状の課題及び発生しつつある問題を踏まえた、「第1次情報セキュリティ基本計画(2006年2月情報セキュリティ政策会議決定)」の具体的方向性(真に「情報セキュリティ先進国」になること)に向けた対策

(対策の例)
○各種基準等に基づくPDCAサイクルを通じた政府機関・重要インフラの対策の加速化
○情報セキュリティの面で質の高い製品・サービスを政府機関が積極的に調達し、その取組みを企業に示すことにより、我が国全体の情報セキュリティレベルを牽引
○業務効率化・知財管理強化等に資する情報セキュリティ対策をベストプラクティス事例集として提供
○中小企業向け簡易チェックツールの作成等を通じた中小企業の対策の底上げ
○IT製品に係る販売時の安全設定促進や「安心・安全」マーク等の検討　等

戦略2：情報セキュリティ政策のグローバル展開

➢ 情報セキュリティに関する脅威の国際化傾向に対応するための国際連携強化
➢ 経済社会システムに深く組み込まれたITのセキュリティを、グローバルに確保するための基盤の構築
➢ 我が国企業・製品等が適切に評価される国際的な基盤の整備

(対策の例)
○多面的・重層的な政策対話・情報交換等を通じた国際連携・協力の推進
○ソフトウェア等の脆弱性の重要度・優先度をユーザが的確に判断するための国際的な基準の整備
○国境を越えたサイバー攻撃の抑制に向けた国際連携体制の構築
○国境を越えて提供されるWebサービスを利用する際に確認すべき事項やサービス提供事業者が具備すべきセキュリティ上の要件等に関するガイドラインの作成
○我が国の技術及び組織管理面での取組みについて国際標準化を推進
○海外の情報セキュリティ関連規制に係る情報収集・提供　等

戦略3：国内外の変化に対応するメカニズムの確立

➢ 国内外の多面的「変化」に的確に対応していく体制の整備

(対策の例)
○関連データ等の収集、国際比較、計量的分析、分析結果の発信等を行うための中核組織として、国内関係機関に情報セキュリティ分析部門(仮称)を創設
○情報セキュリティ分析部門(仮称)等と国内外の関係機関との協力関係構築
○政府統計等の調査項目の充実　等

情報セキュリティ政策の広がりの一例

～システム管理基準　追補版～

→次のプレゼンテーションで

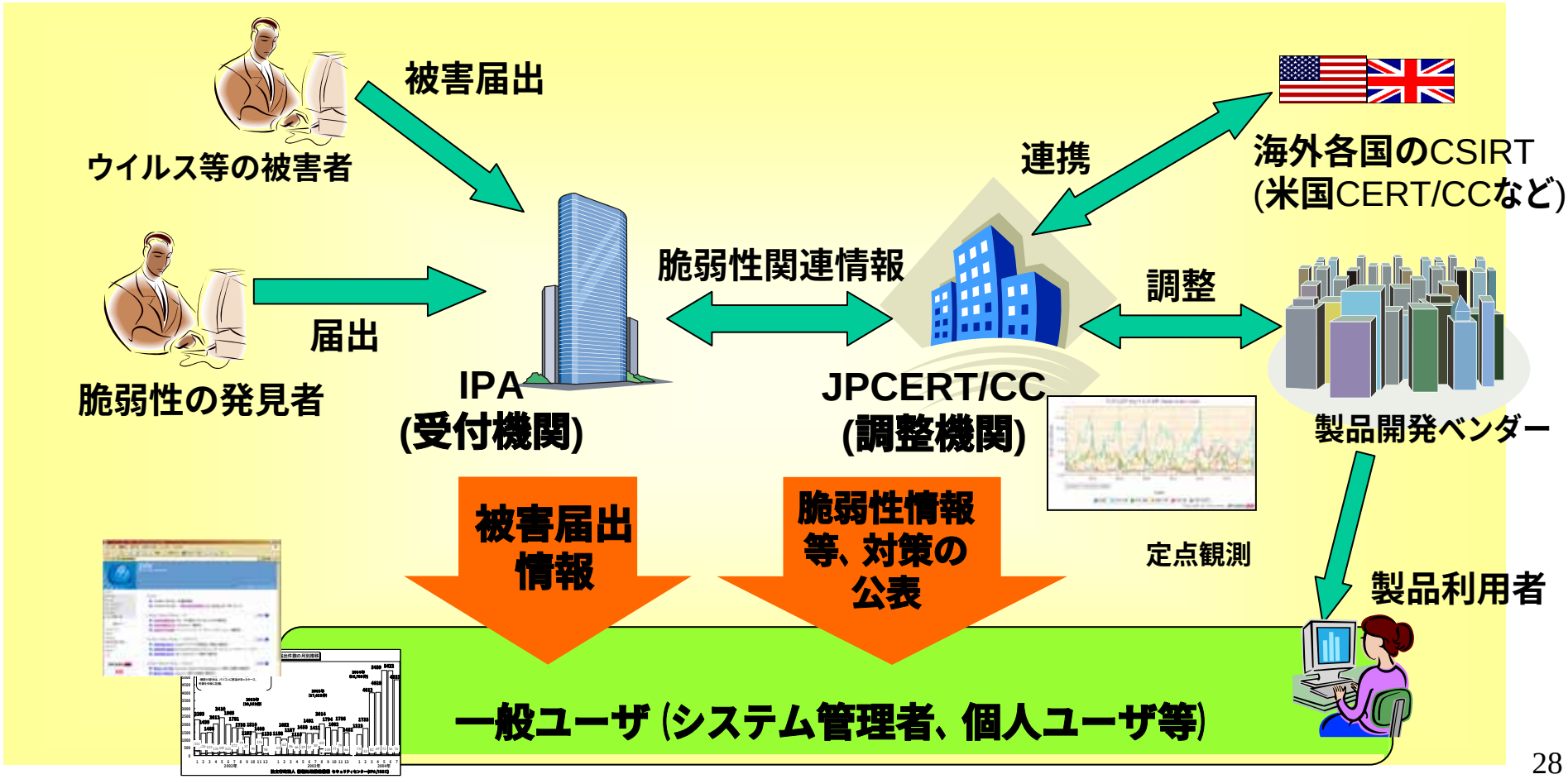
＜参考資料＞
経済産業省の情報セキュリティ施策の紹介

早期警戒体制の整備

早期警戒体制の整備①～ウィルス、不正アクセス、脆弱性等～

- 関係機関の効果的な連携により、情報セキュティ上の問題発生を抑制
- 未公表の脆弱性情報を米英日のCSIRT（注）間で共有する国際連携体制を整備
- 脆弱性情報は、届出制度の運用開始後、約2年10ヶ月で1346件を受領（本年5月2日現在）
- 制度運用により、未対応の脆弱性情報の公表サイトが活動を停止

（注）CSIRTとは、「Computer Security Incident Response Team」の略で、情報システムの運用におけるセキュリティ上の問題に関する報告を受け、その調査、対応活動などを行う組織の一般名称。JPCERT/CCは日本におけるＣＳＩＲＴ。



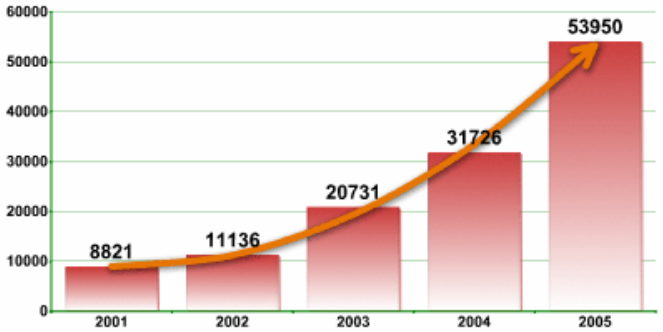
早期警戒体制の整備②～ボットの問題と被害の実例～

ボットの概要

■ウイルスのように感染し、攻撃者の命令に基づき、あらかじめ埋め込んだボットプログラム等を実行
■多数のボットが連携（ボットネット）することで、攻撃元を偽装し、対策を取りにくくすることが可能
■攻撃方法の複合化・高度化と、攻撃者の組織化・分業化の相乗効果により、被害の拡大が進む
■JPCERT/CC・Telecom-ISAC合同調査の結果(平成１６年度調査)
・未知種が一日70種も登場する一方、ウイルスに比較して変種が多く、対策ソフトをすり抜けるボットプログラムが多数存在することから、総合的対策が必要。
・**1台のコンピュータ（1IPアドレス）に対して、ボット化させるための攻撃が一日あたり平均758回ある（約2分に1回の割合）**

ボット被害の拡大

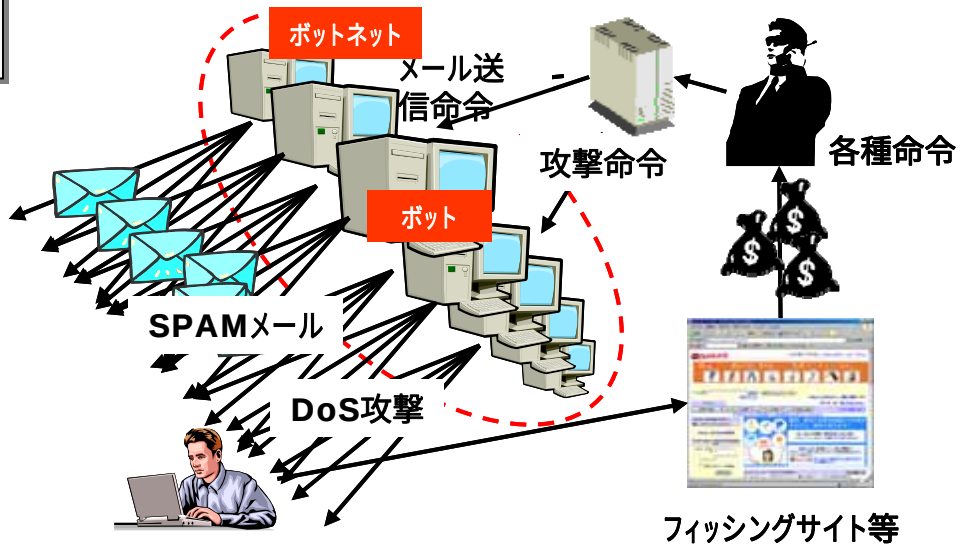
◆米国最大手のISP（AOL）によれば、スパムメールの75%（推定15億通/日）がボットから送信されている(2005年)
◆shadowcrewと呼ばれるボット運営組織は、米・英・露・西・伯に4000人のメンバーを擁し、クレジット詐欺等により数百万ドルを稼ぐ
◆ボットで1800万通／日のスパムメールを送信していた者が韓国で逮捕



発見された悪意のあるプログラムの種類（増加分の殆どはボット）
Kaspersky Lab 調査

ボットの高度化・凶悪化

◆米マイクロソフトによれば、米連邦政府の2000台以上のPCがrootkitと呼ばれる高度な秘匿技術を用いたボットに感染（2006年）
◆米国を中心にユーザの銀行口座情報を盗むボットMetaFisherの大規模な感染が発覚（2006年）

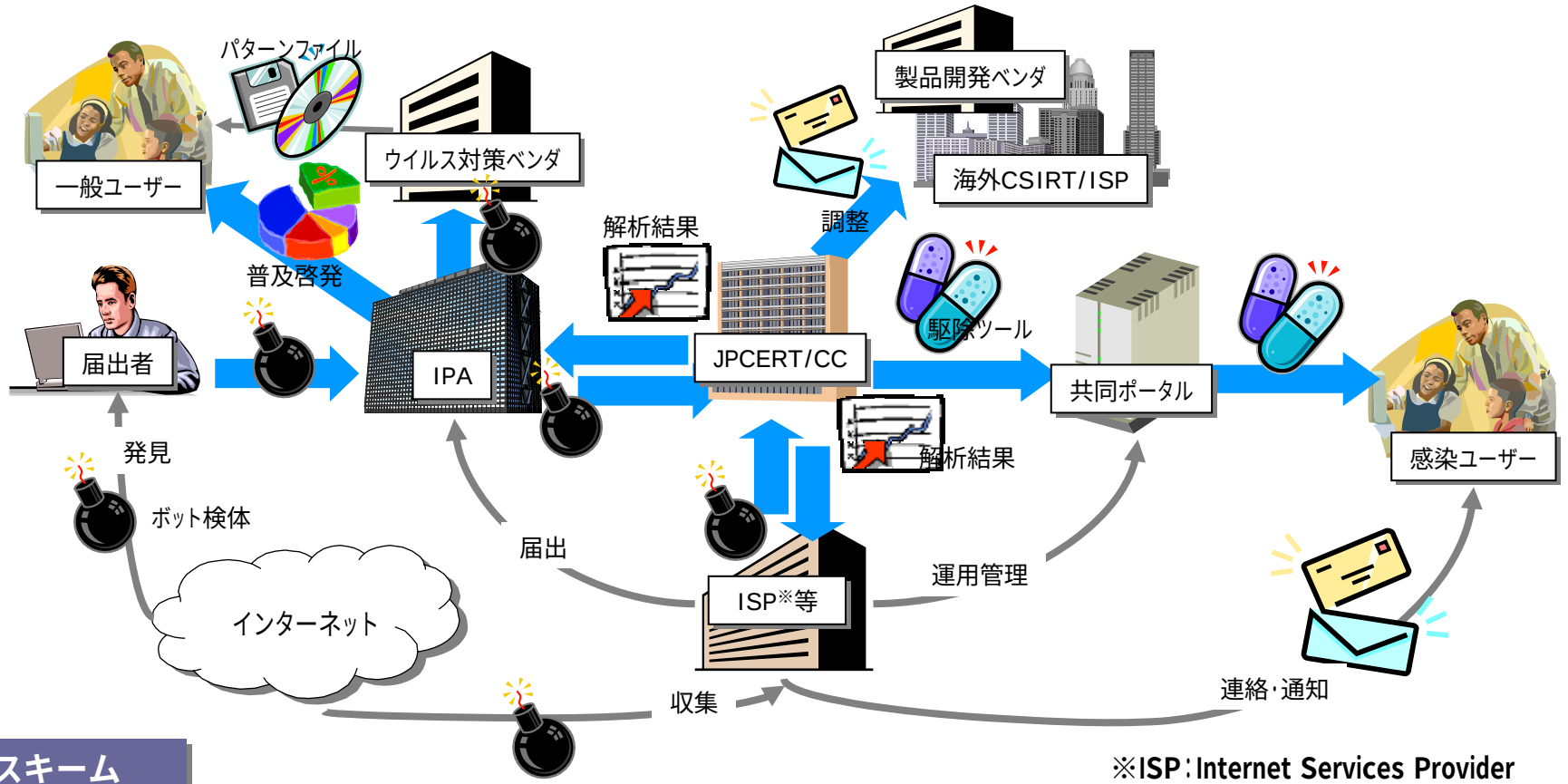


早期警戒体制の整備③～ボット対策推進事業～

METI 経済産業省

目的

管理の不十分なコンピュータにユーザの知らない間にボットが設置されることで、DDoS攻撃、迷惑メールの送信、金銭詐取などが大規模かつ組織的に行われる事例が発生しており、ボットの感染防止、駆除及び被害の局限化等が急務。



※ISP：Internet Services Provider

スキーム

■IPAに届け出窓口を設置すると共に、セキュリティベンダと連携してウイルスソフト等による対策も実施。(予防策)
■JPCERT/CCはISP等と連携し、ボットの検体を入手、解析することで挙動を分析し、駆除ツールを作成する(感染後対策)。必要に応じて、国内外のISP等と連携してネットワークの遮断等を行う。

早期警戒体制の整備④～サイバークリーンセンターの創設～

METI 経済産業省

•平成18年12月12日に、経済産業省・総務省連携プロジェクトであるボット対策プロジェクトの専用ポータルサイト「サイバークリーンセンター」を開設。一般ユーザ向けに、ボットを駆除するための対策情報等の提供を開始している。(http://www.ccc.go.jp)

普及広報活動

経済産業省が実施する主な普及広報活動

METI 経済産業省

経済産業省 Ministry of Economy, Trade and Industry

	独立法人　情報処理推進機構	NPO　日本ネットワークセキュリティ協会	財団法人　日本情報処理開発協会
実施	IPA	NPO 日本ネットワークセキュリティ協会 Japan Network Security Association JNSA	Japan information processing JIPDEC Development Corporation
取組	情報セキュリティセミナー 	インターネット安全教室 	セキュリティキャンプ 
対象	企業の**経営者、システム管理者、端末利用者** (2006年度：全国30ケ所以上で開催、約7,000名が参加)	一般のインターネット、PCの利用者 (2003年からで47都道府県、208ケ所開催。累計参加者17,000名超)	大学生、高校生等若年層（将来のIT業界を担う人材） (満22歳未満の者を毎年約30名選出し、合宿形式で実習)

普及広報活動～Check PC！ キャンペーン～

METI 経済産業省

経済産業省は、平成19年1月22日～3月31日の約2ヶ月間、タレントの白石美帆さんをキャンペーンキャラクターとして、一般利用者・事業者向けに情報セキュリティ対策の重要性を訴える「CHECK　PC！」キャンペーンを実施。
（昨年に続き、今回キャンペーンは2回目）

○「CHECK PC！」キャンペーン開始式の開催

1月22日、甘利経済産業大臣より白石美帆さんを「情報セキュリティ広報大使」に任命。

○「CHECK PC！」キャンペーンの専用ホームページ開設

白石美帆さんが情報セキュリティ対策をわかりやすく説明する、という形式の専用ホームページを開設し、情報セキュリティの基礎知識のほか、WEBムービー、クイズ、チェックリスト等を掲載。
（ホームページアドレス　http://www.checkpc.jp/ ）

○情報セキュリティ対策の重要性を訴えるテレビCM、新聞広告等の実施

白石美帆さんが情報セキュリティ対策の重要性を訴えるテレビCMを1月23日から民放各社において、約2週間放映するとともに、新聞広告を掲載。

○リーフレット、ポスターの配布

本キャンペーンのリーフレット（50万枚）、ポスター（1万枚）を企業、関係団体、書店等を通じて配布。

組織的対策の推進

組織的対策の推進（全体像）

■ 情報セキュリティに関する事件・事故の原因は、運用・管理上の不備によるもの、内部からの情報漏えい・侵害行為などの**内部要因によるものも多い**。このため、技術的側面からのみだけでなく、**組織的側面からの対応**が必要。現在以下のような施策を実施。

■ **情報セキュリティマネジメントシステム（ISMS）の促進：**

✓組織のセキュリティ対策が一定の基準を満たしているかを客観的に評価をするための、国際標準（ISO/IEC 27001等）に則した第三者機関による認証制度を促進。

■ **情報セキュリティ監査制度の推進：**

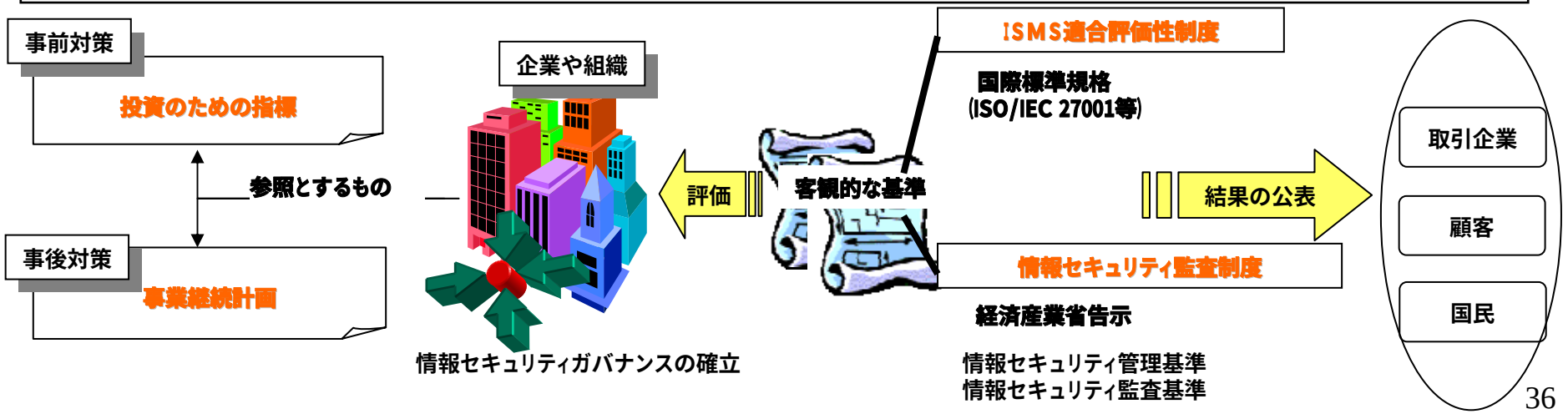
✓個々の企業に即した対策を促進するため、独立した専門家が組織のセキュリティ対策を、客観的に定められた国の基準に基づいて監査（保証または助言）する制度を推進。

■ **情報セキュリティガバナンスの確立：**

✓企業の組織運営の中で、必要な情報セキュリティに係る投資が行われておらず、またどの程度対策を行えばよいかわからない現状を踏まえ、平成17年3月に以下のツールを策定。これらのツールを活用して、企業の組織内で情報セキュリティを確保させる「情報セキュリティガバナンス」の確立を促進。

①情報セキュリティ対策ベンチマーク
②情報セキュリティ報告書モデル
③事業継続計画策定ガイドライン

■ **J－SOX法における「ITへの対応」に関する検討**



組織的対策の推進～ISMS（Information Security Management System）適合性評価制度～

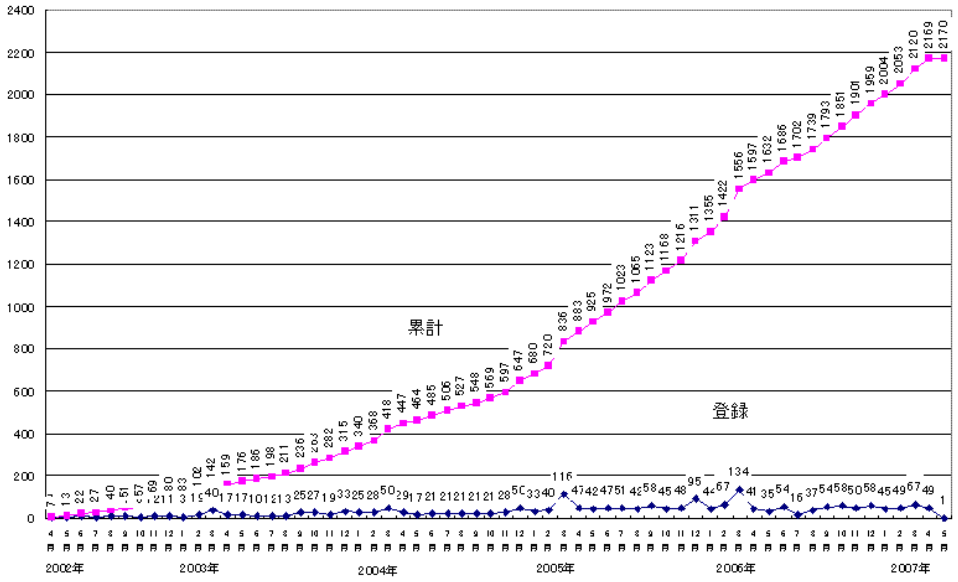
METI 経済産業省

http://www.isms.jipdec.jp/

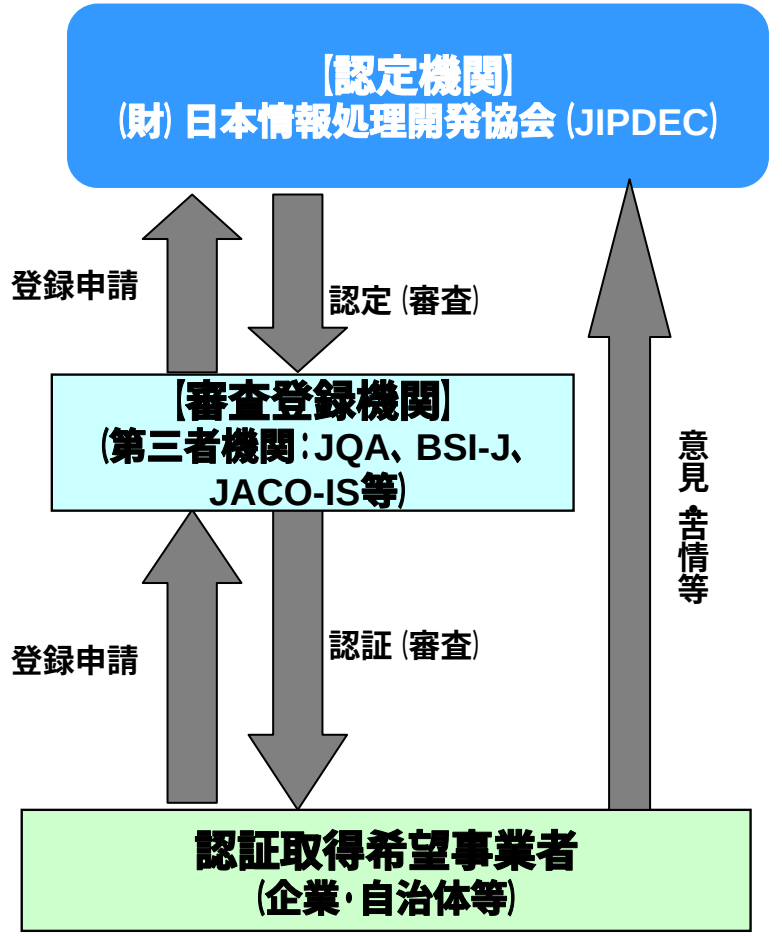
- 本制度は、企業における組織面での情報セキュリティ対策が適切に行われているかどうかについて、第三者機関が国際規格（ISO/IEC 27001等）に基づき、客観的に評価・認証する制度。
- （財）日本情報処理開発協会（JIPDEC）が2002年4月より制度を運用。
- 認証取得事業者数は、2007年5月18日現在で2,170件）。

ISMS認証取得事業者数の推移

（2007年5月18日現在）



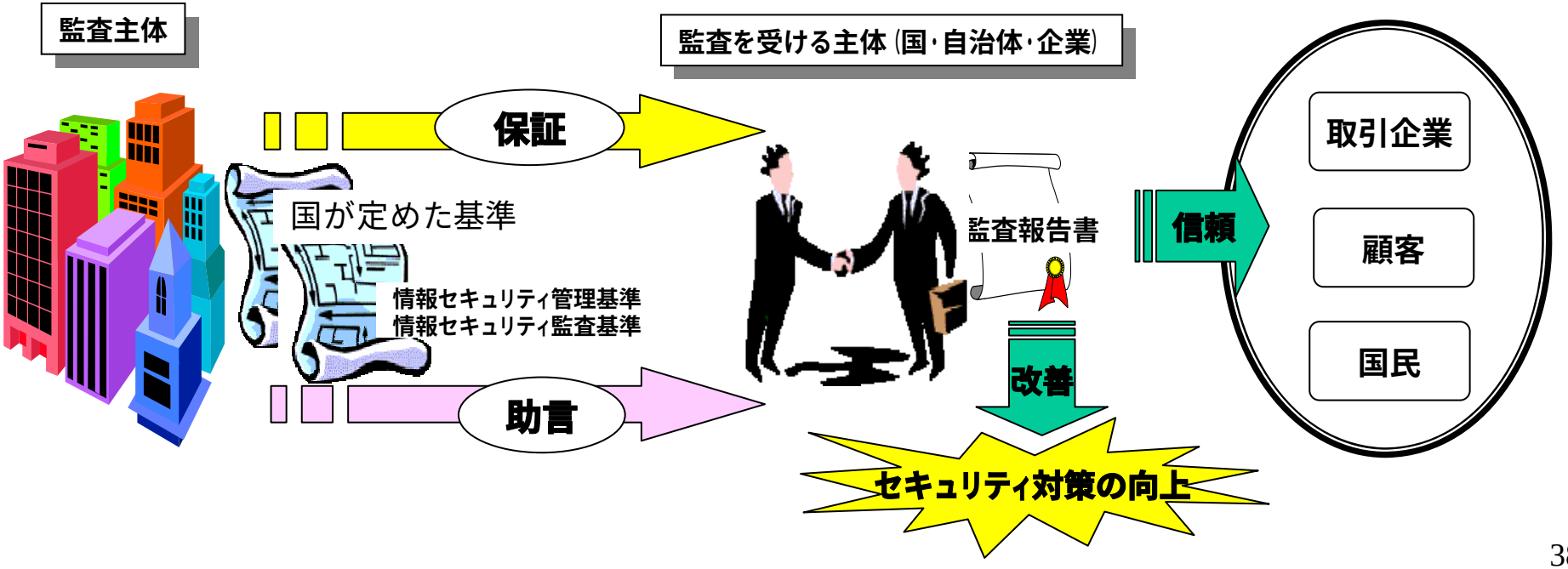
ISMS適合性評価制度スキーム概要



組織的対策の推進～情報セキュリティ監査制度～

http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

- 「情報セキュリティ監査制度」とは、企業等の情報セキュリティ対策（外部からの不正アクセス防止の設定をしているか、情報管理責任者を任命しているか等）について、客観的に定められた国の基準に基づいて、独立した専門家が評価（保証または助言）する制度。
  - ２００３年４月、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」を、経済産業省告示により公表。これに基づき、制度運用開始。
  - 監査主体は「情報セキュリティ監査企業台帳」に登録され(約500事業主体)、公表。毎年７月に更新。「日本セキュティ監査協会」（ＪＡＳＡ）にて、監査の質の向上のための取り組み。



組織的対策の推進～情報セキュリティガバナンスの確立～

METI 経済産業省

問題点

(1) IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難

✓ **投資判断のための指標**が求められているのではないか。

(2) 既存の情報セキュリティへの「対策」「取組」が企業価値に直結していない

✓ 情報セキュリティに係る取組みが、**企業価値向上**に寄与する仕組みが必要ではないか。

(3) 事業継続性確保の必要性が十分に認識されていない

✓ IT事故発生時の対応手続きを**事業継続の観点**から定めておくことが必要ではないか。

問題点を克服し、企業が情報セキュリティガバナンスの確立を促進するツール

情報セキュリティ対策ベンチマーク

- 情報セキュリティ対策のセルフチェック等に有用なベンチマークの指標を開発
- さらに、IT事故データ収集のあり方や被害想定額算出手法について調査し、ベンチマークデータと連動したリスク評価の可能性を模索

情報セキュリティ報告書モデル

- 企業のコンプライアンスや社会的責任を説明するIRの一環として、自らの情報セキュリティポリシーやそれを実現する対策の実施状況について対外的に公表する「情報セキュリティ報告書」を提唱し、そのモデル案を策定

事業継続計画策定ガイドライン

- 企業がIT事故発生時にも事業運営を継続的に維持するための事業継続計画（BCP）について、その策定手順や検討項目、事例等を紹介する「事業継続計画策定ガイドライン」を策定

企業・社会への普及方策

・情報セキュリティ格付け
・政府調達への活用
・損害保険との連携　　等

既存施策との連携

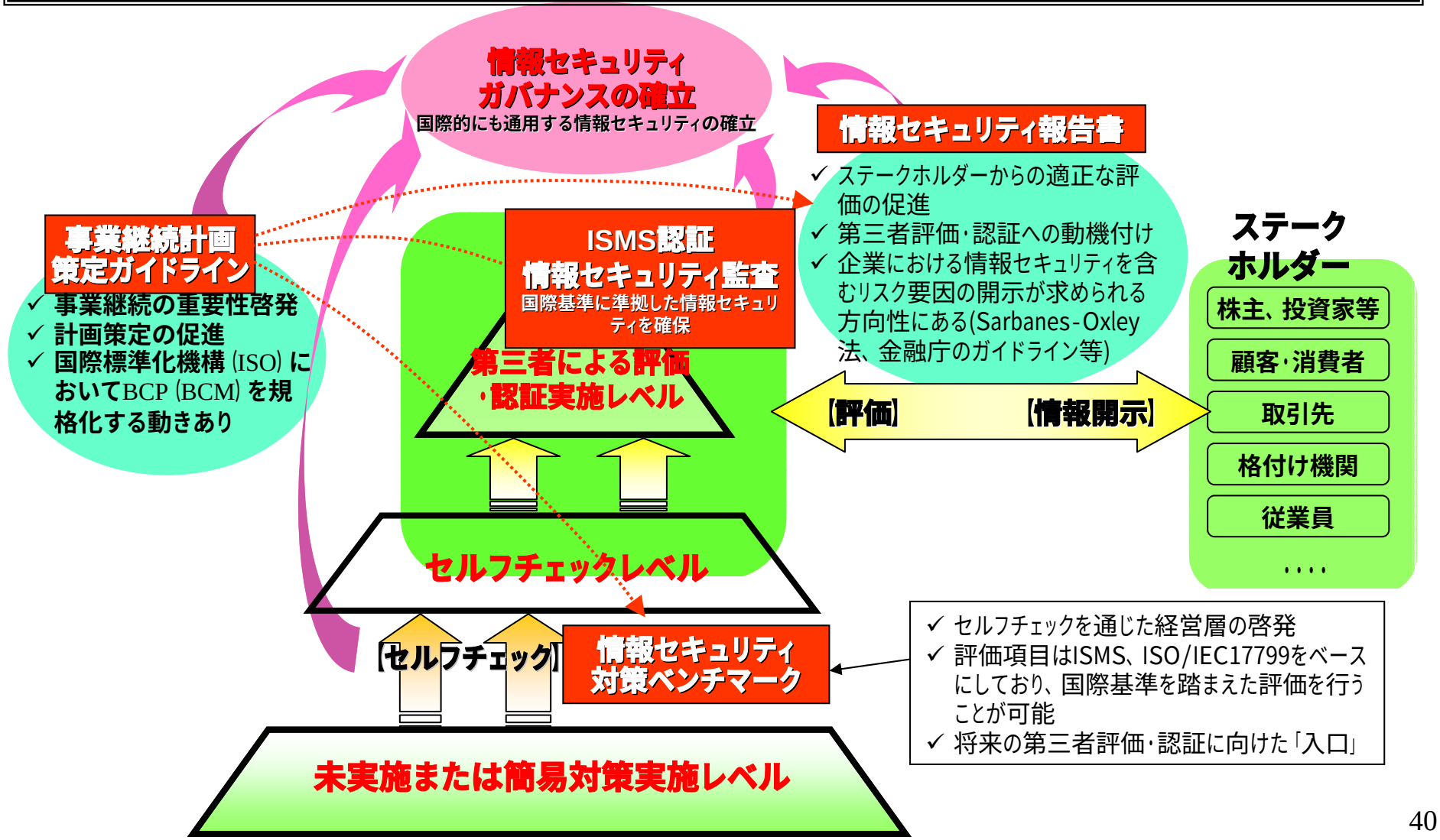
・ISMSや情報セキュリティ監査の「入口」としての活用
（セルフチェック→第三者認証・評価へ）　等

企業における情報セキュリティガバナンスの確立

http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

(参考)各ツールとISMS認証等との基本的関係

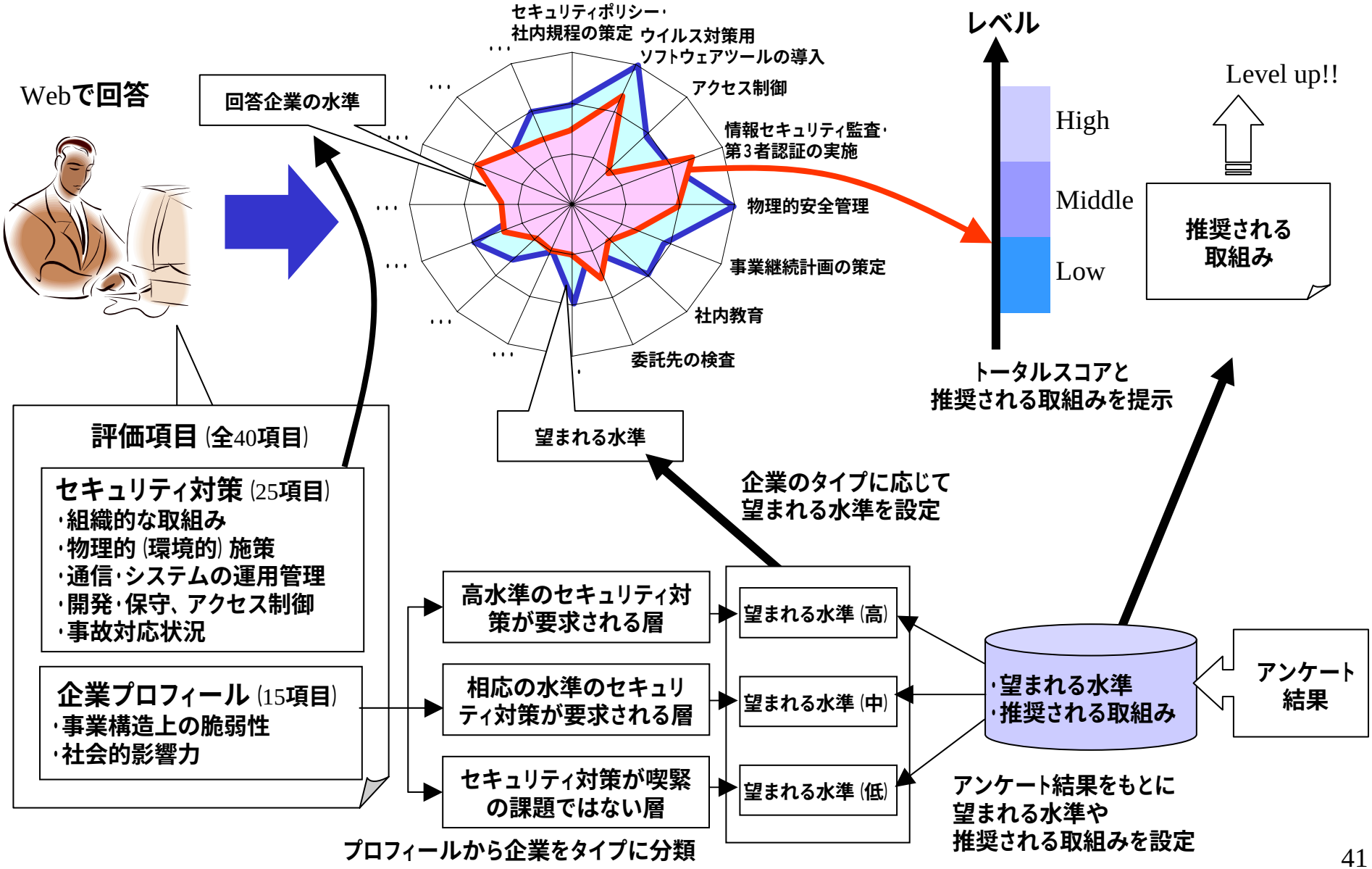
■自己評価をベースとしつつ、必要な場合は第三者による客観評価に耐えうる仕組みの構築が重要
■企業活動のグローバル化を考慮し、国際基準との整合性等にも配慮



(参考)情報セキュリティ対策ベンチマーク

METI 経済産業省

- 何をどこまで実施すべきかわからない企業に、セルフチェックによる「気づき」を促しつつ、一定の目標を提示。
- 情報セキュリティ対策の取り組み状況の結果から、レーダーチャートや全体のスコアを算出。

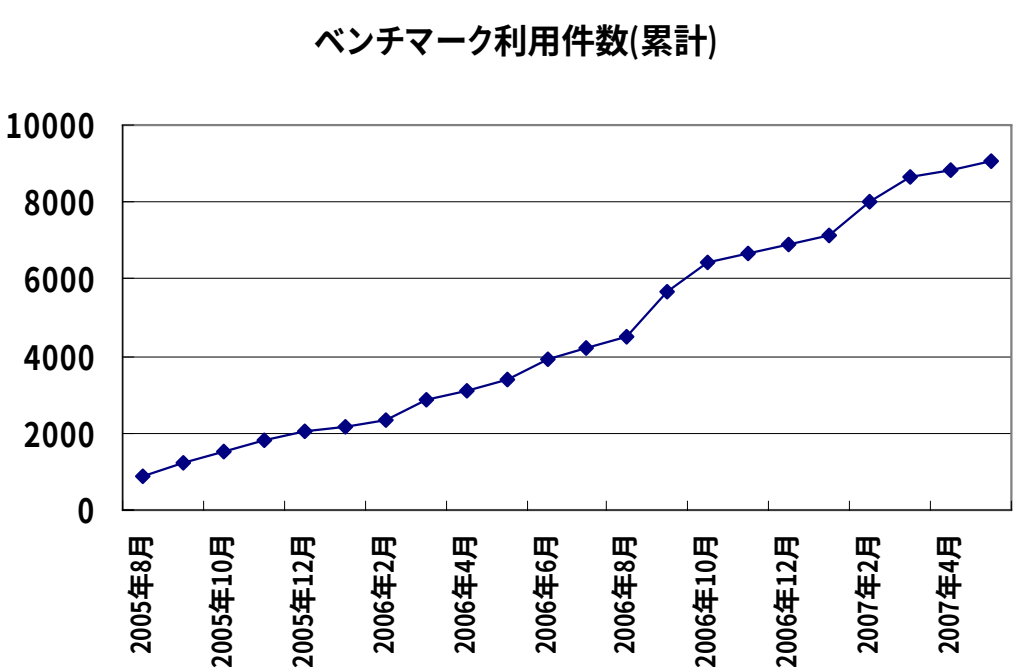


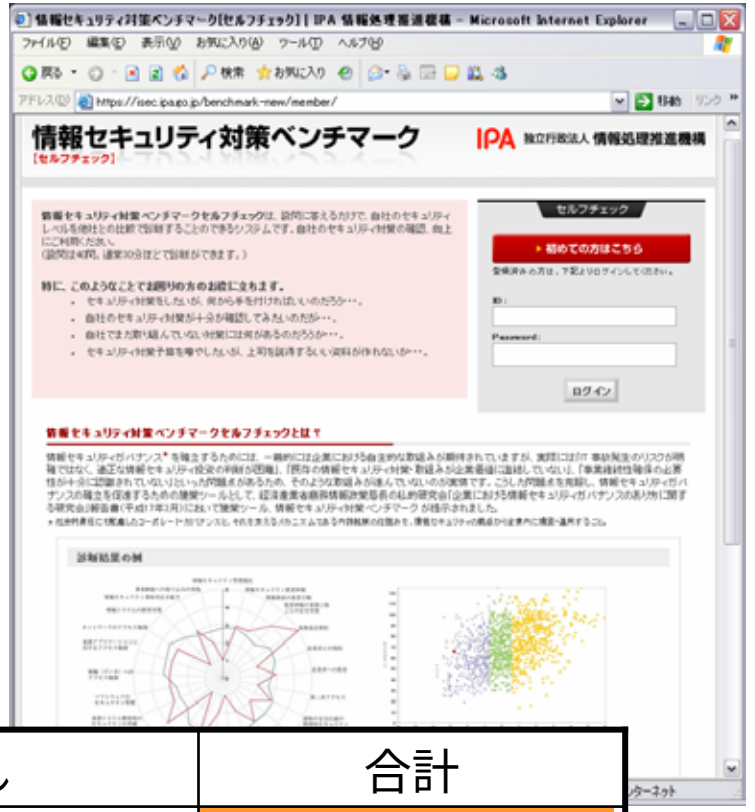
(参考)情報セキュリティ対策ベンチマークの利用状況

■(独)情報処理推進機構(IPA)において、情報セキュリティ対策ベンチマークに係るセルフチェックのWebサイトを開設　(2005年8月4日)

https://isec.ipa.go.jp/benchmark/g_bench.html

■開設以来約１年１０ケ月で約9000件のアクセス





IPAの分析用にデータを提供した者	提供無し	合計
3,567件 (39.1%)	5,558件 (60.9%)	9,125件

2007年5月21日現在

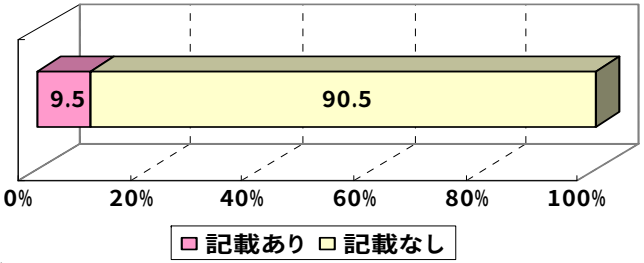
(参考) 上場企業の情報セキュリティに係る情報開示状況

METI 経済産業省

◆ 国内上場企業3,670社について、CSR報告書、環境報告書等に情報セキュリティに係る記載のある企業は、9.5% (350社) (2006年11月時点)。2005年10月時点から3.4ポイント上昇。金融機関のディスクロージャー誌を含めた影響もあるが、金融機関を除いても約2ポイントの開示率向上。
◆ 業種別で見ると、「銀行」(62.0%)「保険」(60.0%) の開示率が高く、次いで「電気・ガス」(52.%)「石油・石炭」(30.8%) 等が続く。また、開示企業 (350社) のうち、326社 (93.1%) は東証1部上場企業である。
◆ その他、情報セキュリティに関連して「個人情報保護方針」「プライバシポリシー」等がWebページに記載されているのは2,955社 (80.5%)、セキュリティポリシーやISMS等、セキュリティに対する取り組み指針等に関する記載がされているのは73社 (2.0%) である。
◆富士ゼロックス、リコーが当省モデルに基づく報告書を策定・公表。

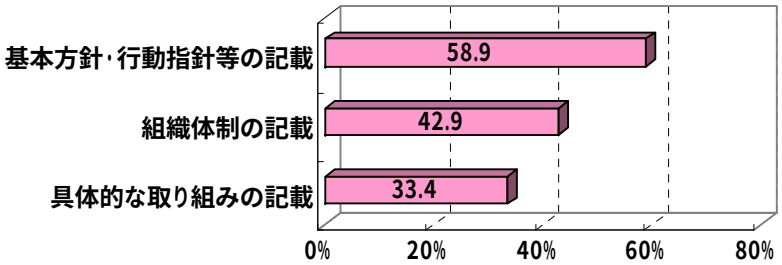
(N=3,670)

情報セキュリティに係る開示状況



(N=350)

「記載あり」の内訳



情報セキュリティに係る開示状況

出所：経済産業省調査 (2006年11月)

	調査対象	開示社数	開示率		調査対象	開示社数	開示率
情報・通信	141	8	5.7%	食料品	152	15	9.9%
通信	156	5	3.2%	石油・石炭	13	4	30.8%
電機	300	44	14.7%	繊維	87	6	6.9%
サービス	314	6	1.9%	化学	209	27	12.9%
銀行	92	57	62.0%	卸売	380	18	4.7%
保険	10	6	60.0%	ガラス・土石	71	8	11.3%
その他金融	52	9	17.3%	その他製品	110	14	12.7%
電気・ガス	25	13	52.0%	非鉄金属	39	8	20.5%
空運	6	1	16.7%	パルプ・紙	29	1	3.4%
陸運	64	1	1.6%	ゴム製品	21	3	14.3%
建設	223	10	4.5%	海運	18	5	27.8%
医薬品	49	10	20.4%	金属製品	97	4	4.1%
精密機器	48	9	18.8%	鉱業	8	0	0.0%
証券	36	3	8.3%	水産・農林	11	0	0.0%
小売	360	25	6.9%	倉庫	12	0	0.0%
機械	238	13	5.5%	倉庫・運輸関連業	30	0	0.0%
輸送用機器	105	12	11.4%	不動産	108	3	2.8%
鉄鋼	56	2	3.6%	合計	3670	350	9.5%

(参考)BCPの策定状況と国際標準化の動向

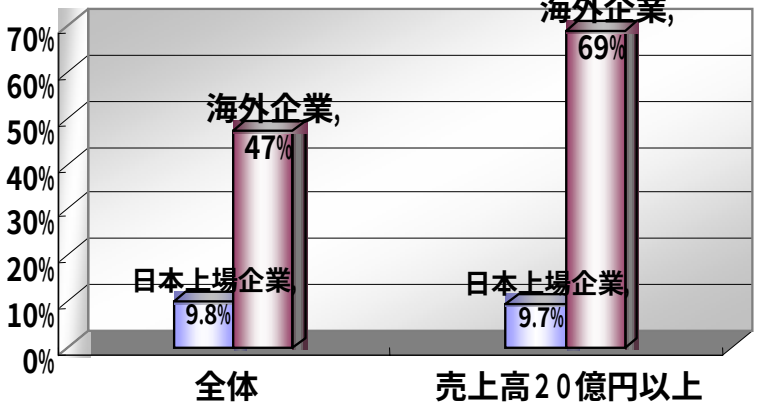
■**日本の上場企業におけるBCP策定率は１０%程度。**海外企業は４７%と比べて遅れている。

■日本はコーポレートガバナンス･CSRの一環としての導入が最も多く（７０%）、海外では既存／見込みの顧客からの要請（合計５１%）が中心。

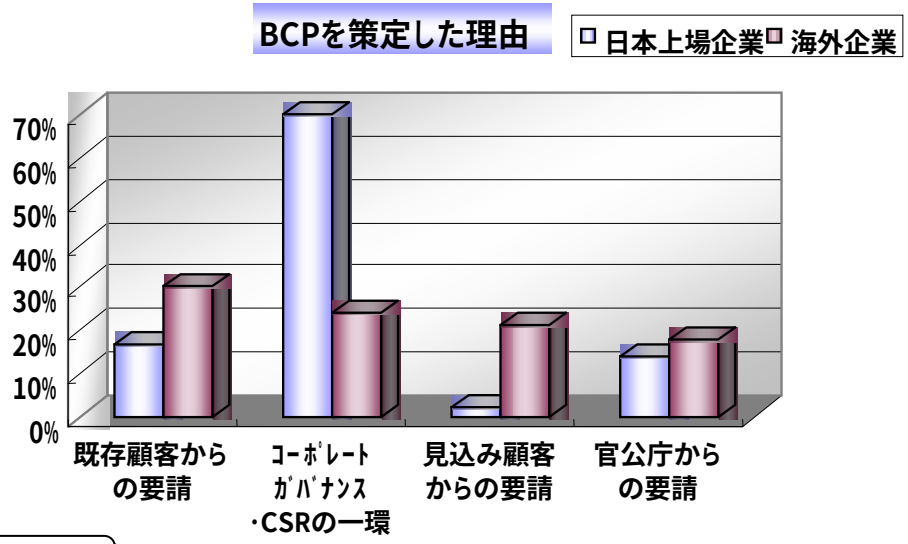
■**ＢＣＰの整備は、グローバルサプライチェーンに入るための必須条件となりつつある**（複数の業種において、日本企業は、米国を始めとする海外企業からＢＣＰ策定を求められつつある）

■**日米英の基準等（日本：経済産業省BCPガイドライン等、米国：ANSI/NFPA１６００、英国PAS５６）を元にした国際標準化の議論が活発化し、具体的な議論が進展している。**

ＢＣＰの策定状況

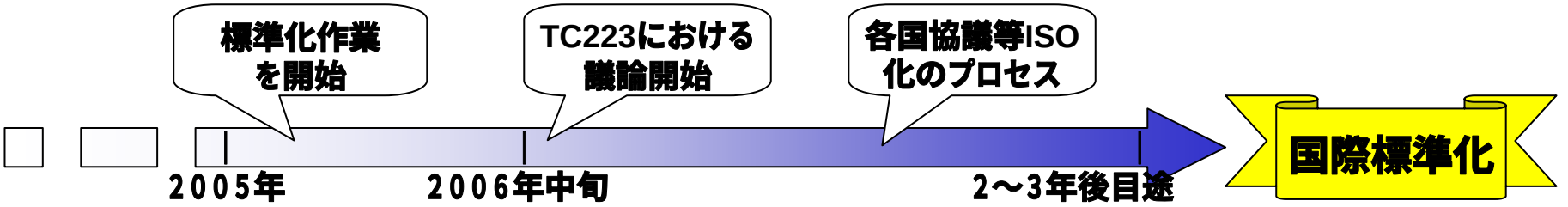


BCPを策定した理由



国際標準化のタイムスケジュール

経済産業省にISO標準化対応のためのWGを設置･対応中



技術的対策の推進

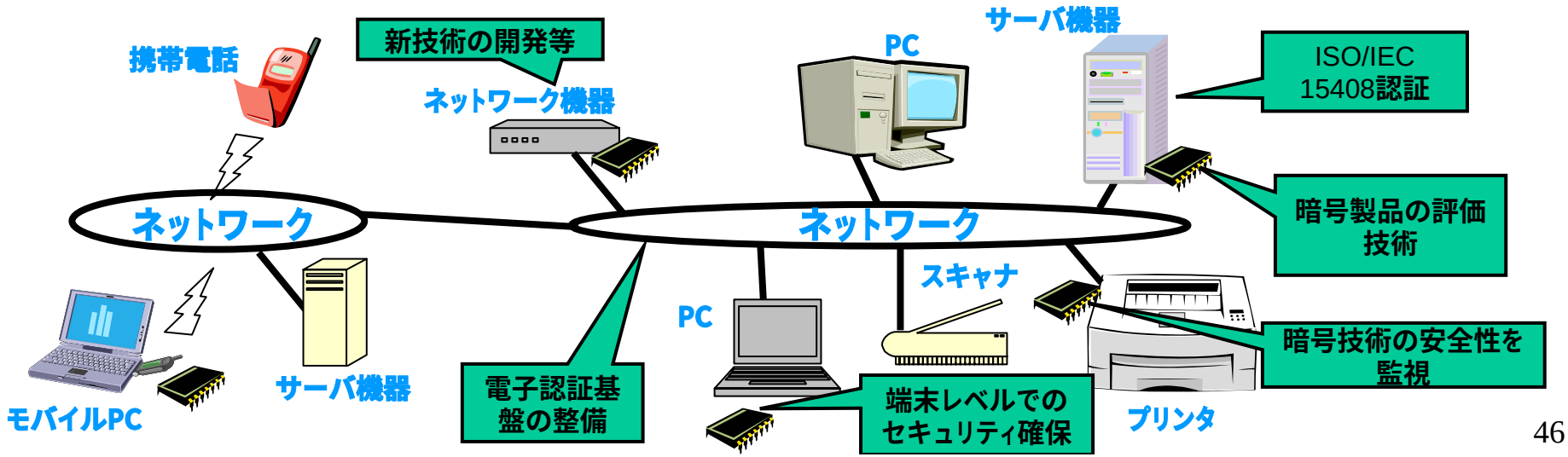
技術的対策の推進（全体像）

■　安心・安全なIT社会を実現するためには、**安全なIT製品**の社会への幅広い普及、より高度な本人認証等を実現する**電子認証基盤の整備**及びそれらを支えるための**技術開発、研究開発等**を実施することが必要。具体的には以下のような施策等を実施。

➢　**情報セキュリティ技術**についての**第三者評価等**の推進。
- ✓IT製品（ＯＳ、ルーター等）　：国際標準ISO/IEC15408に基づいた第三者評価・認証制度を推進
- ✓暗号（ＲＳＡ、ミスティー等）　：電子政府推奨暗号（平成15年2月選定）の安全性を監視
- ✓暗号モジュール等（ICカード等）　：暗号モジュール等の第三者評価・認証制度を推進
- ✓セキュリティ評価技術の確立　：情報システム、暗号モジュールに係るセキュリティについての評価技術の開発を推進

➢　情報セキュリティ技術に係る**技術開発・研究開発を推進**
- ✓アクセス制御技術、未知ウイルス予防技術等
- ✓フェイルセーフセキュリティ技術基盤整備　等

➢ 本人の確認及びやりとりされる情報が正しいことを電子的に証明する**電子認証基盤の整備**
- ➢次世代認証基盤の整備による横断的な認証基盤の実証実験
- ➢端末レベルでのセキュリティを確保するための高信頼性端末の電子認証に係る調査研究
- ➢電子認証フレームワークのあり方に係る調査研究　等

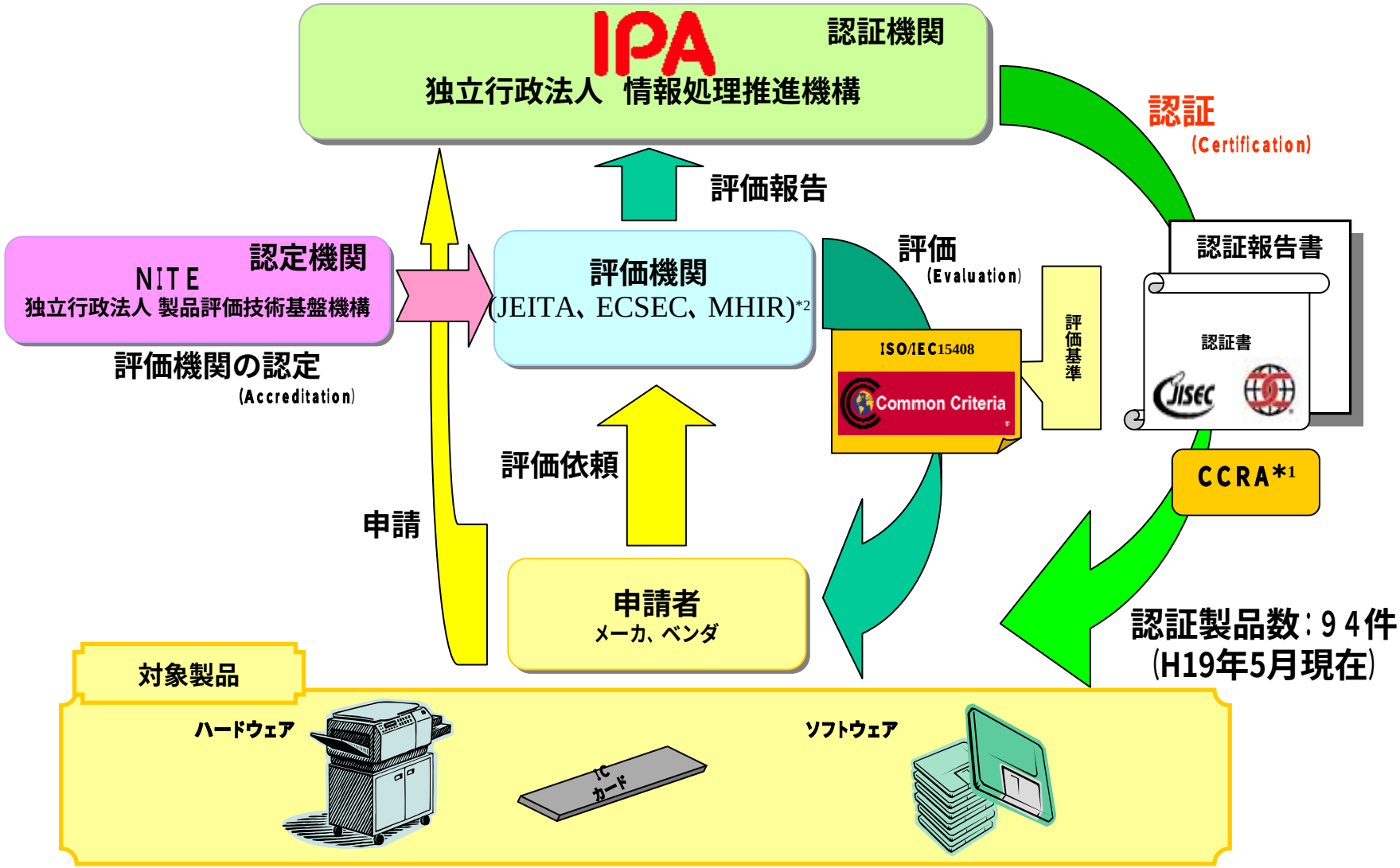


技術的対策の推進

～ITセキュリティ評価及び認証制度（IT製品等の安全性に係る国際的な評価認証制度）～

国際基準（ISO/IEC15408）に基づき、IT製品等の安全性を評価・認証する制度

http://www.ipa.go.jp/security/jisec/index.html



*1：Common Criteria Recognition Arrangement

*2 JEITA：社団法人電子情報技術産業協会、ECSEC：株式会社電子商取引安全技術研究所、MHIR：みずほ情報総研株式会社

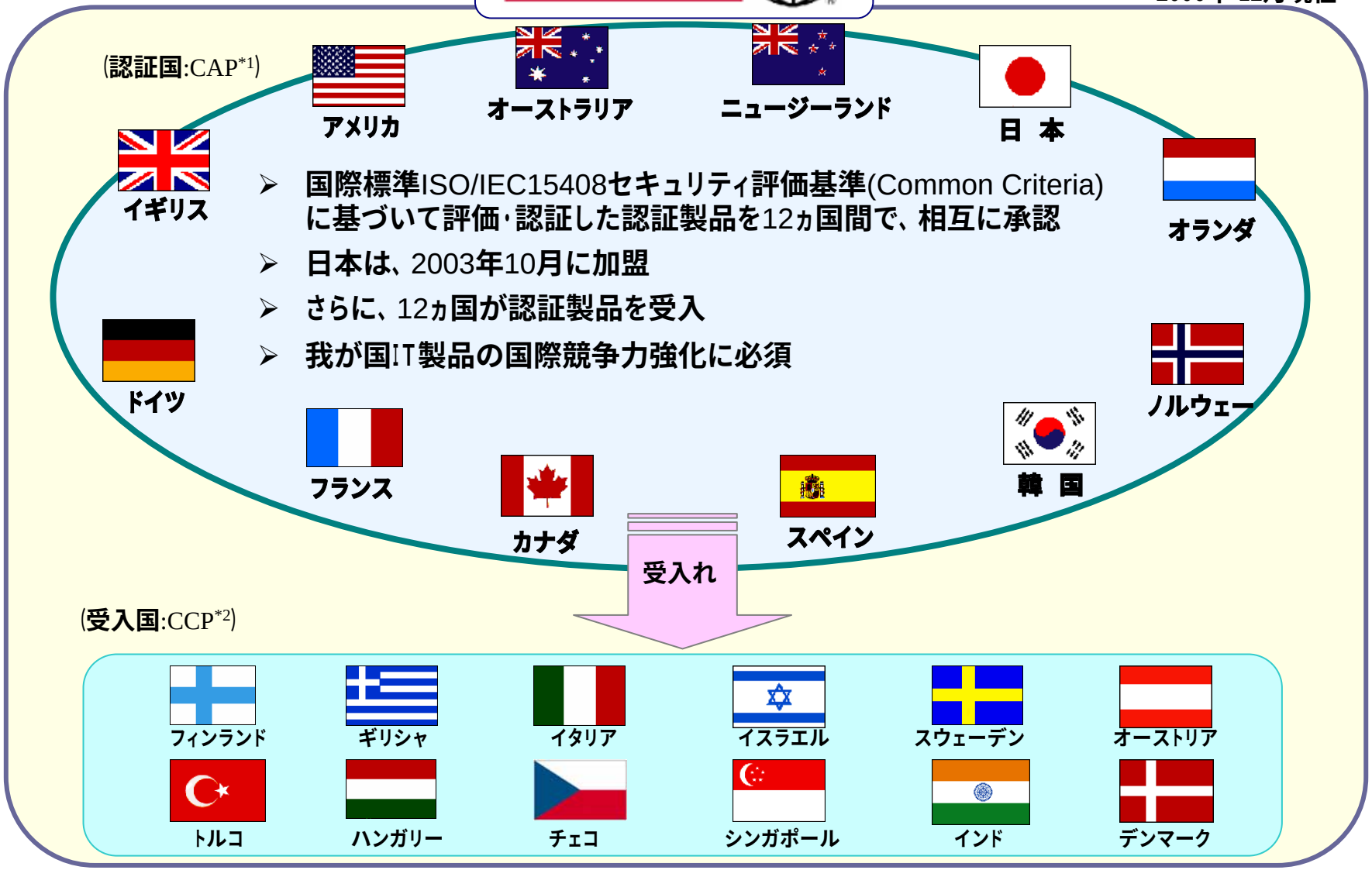
技術的対策の推進

～ITセキュリティ評価及び認証制度に係る国際相互承認協定（CCRA*）～

METI 経済産業省

*：Commom Criteria Recognition Arrangement

2006年 12月現在



*1 CAP：Certificate authorising participants

*2 CCP：Certificate consuming participants

(参考) 産業競争力のための情報基盤強化税制の創設

http://www.meti.go.jp/policy/it_policy/zeisei/

情報セキュリティ強化と国際競争力強化の観点から、高度な情報セキュリティが確保された情報システム投資を促進し、情報基盤を強化するための税制上の措置を講じる（基準取得価額に対する税額控除（10%）又は特別償却（50%）の選択適用）。

【対象企業】
すべての企業・業種

【対象資産】
平成18年4月1日から平成20年3月31日までの期間内に取得等を行う以下の投資であって、一定の金額以上のもの
①オペレーティングシステム※及びこれがインストールされたサーバー
②データベース管理ソフトウェア※及びこの機能を利用するアプリケーションソフトウェア
③ファイヤーウォール※（①または②と同時に設置されたものに限る）
＊ISO/IEC15408に基づいて評価・認証されたもの

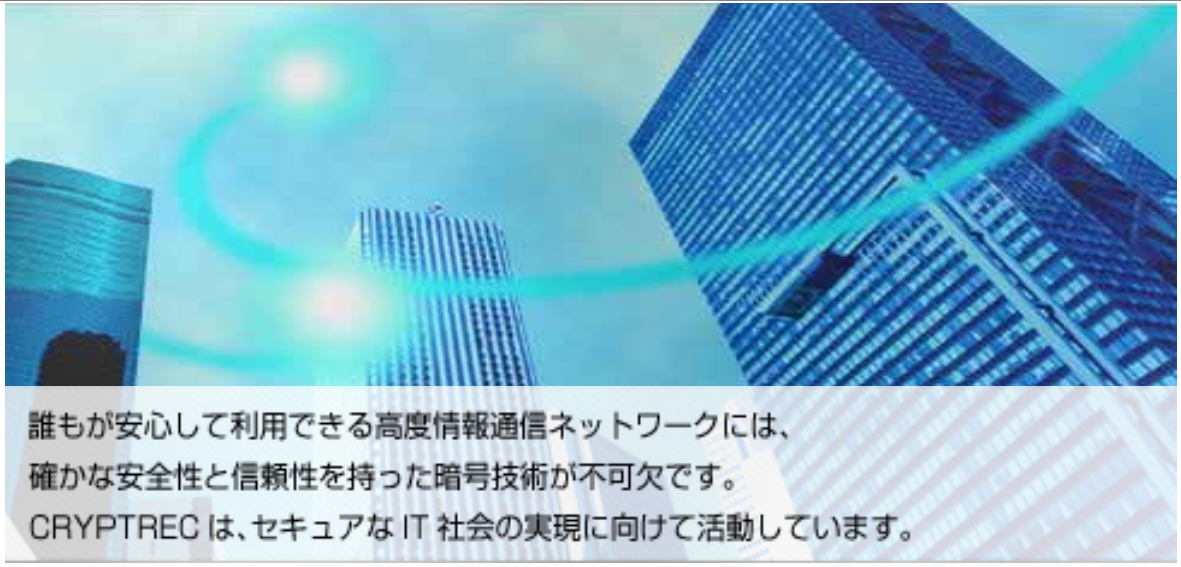
【措置内容】
下記の①，②から選択
①基準取得価格（取得価格の70%）に対する10%の税額控除
②基準取得価格（取得価格の70%）に対する50%の特別償却
※資本金1億円以下の法人については、リースの税額控除（リース費用総額の42%相当額に対する10%相当額の税額控除）が認められる。

技術的対策の推進～暗号の安全性確保等～

■電子政府推奨暗号の安全性を評価･監視し、暗号モジュール評価基準等の策定を検討するため、総務省、経済産業省、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）はCRYPTREC(Cryptography Research and Evaluation Committees)を推進。総務省と経済産業省は、CRYPTRECの評価結果を踏まえ2003年2月20日に「電子政府」における調達のための推奨すべき暗号のリスト(電子政府推奨暗号リスト)を公表。

■2003年2月28日には、行政情報システム関係課長連絡会議において、各府省が情報システムの構築に当たり暗号を利用する場合には、可能な限り、電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の「各府省の情報システム調達における暗号の利用方針」が了承された。

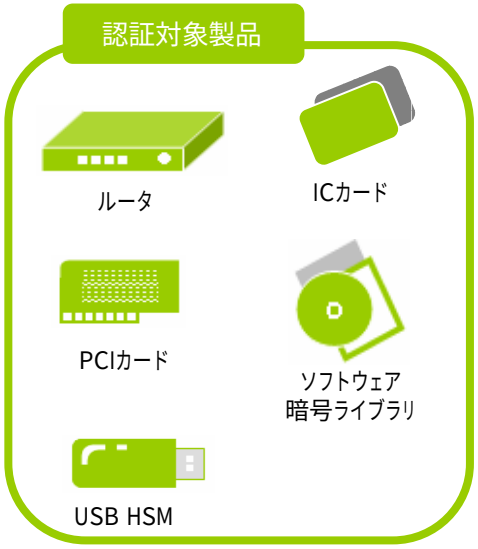
■2005年12月13日の情報セキュリティ政策会議で決定された「政府機関の情報セキュリティ対策のための統一基準」においても、「暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規(更新を含む。)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること･･･。」とされている。



技術的対策の推進
～暗号モジュール試験及び認証制度（JCMVP）～

METI 経済産業省

暗号モジュールに暗号アルゴリズムが適切に実装され、その内部に格納された暗号鍵、パスワード等の重要情報が適切に保護されていることについて、第三者機関である（独）情報処理推進機構（IPA）が、国際標準（ISO/IEC19790）に基づき試験・認証する制度。2007年4月から本格運用を開始。

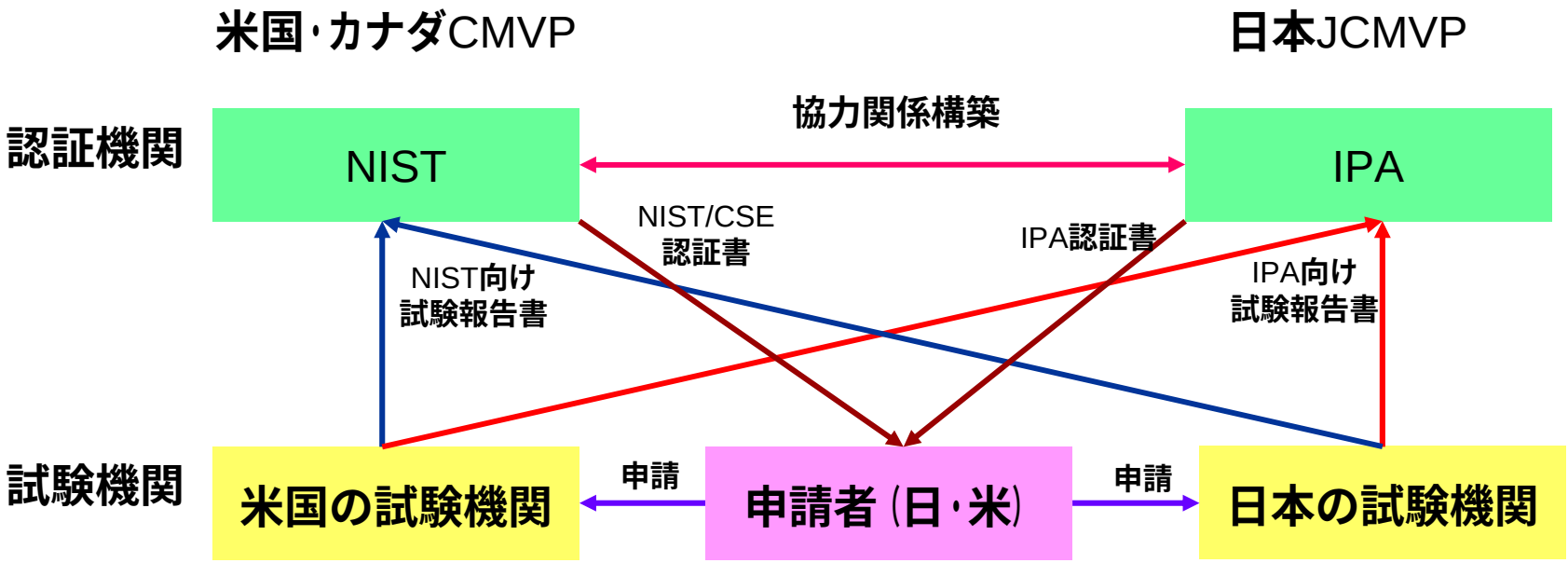


【暗号モジュール】

【試験・認証の流れ】

- ◆ 試験機関は暗号アルゴリズム試験を行い、試験結果を認証機関に提出（①～②）
- ◆ 認証機関は、試験結果により暗号アルゴリズムが適切に実装されていることが確認された場合には、暗号アルゴリズム確認書を発行（③）
- ◆ 試験機関は、暗号モジュール試験を行い、試験結果を認証機関に提出（④～⑥）
- ◆ 認証機関は、試験結果より暗号鍵、パスワード等の情報が適切に保護されていることが確認された場合には、暗号モジュール認証書を発行（⑦）

(参考)米国･カナダのCMVPとの関係



注： 1．試験機関は米国の認定機関NVLAP及び日本の認定機関NITEの両方から暗号モジュール試験機関認定を受けていることを想定。また申請者はNIST/CSE及びIPA両方に認証申請することを想定。

2．日･米の申請者は日･米どちらの試験機関に試験依頼（申請）してもよい。日本の申請者が日本の試験機関に試験依頼する場合、日本語のみで証拠資料を提出しても、JCMVPと米･加CMVPの両方から認証を得ることができる（ワンストップサービス）。

3．試験機関は試験報告書の内容につき申請者の同意を得た上でそれを認証機関に提出。

(参考)政府機関統一基準と経済産業省施策との関係①

政府機関の情報セキュリティ対策のための統一基準（2005 年12 月）

4.1.6 暗号と電子署名(鍵管理を含む)
(1) 暗号化機能及び電子署名の付与機能の導入
【基本遵守事項】
(e) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、**電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。**ただし、**新規(更改を含む。)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。**なお、複数のアルゴリズムを選択可能な構造となっている場合には、**少なくとも一つを電子政府推奨暗号リストの中から選択すること。**

電子政府推奨暗号リスト
(CRYPTREC:2003年2月)

4.2.1 セキュリティホール対策
(1) 情報システムの構築時
【基本遵守事項】
(b) 情報システムセキュリティ責任者は、電子計算機及び通信回線装置の構築又は運用開始時に、当該機器上で利用する**ソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。**

(2) 情報システムの運用時
【基本遵守事項】
(b) 情報システムセキュリティ責任者は、管理対象となる電子計算機及び通信回線装置上で利用している**ソフトウェアに関連する公開されたセキュリティホールに関連する情報を適宜入手すること。**

早期警戒体制(IPA及び JPCERT/CC)

等々

【基本遵守事項】保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項
【強化遵守事項】特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項

(参考)政府機関統一基準と経済産業省施策との関係②

政府機関の情報セキュリティ対策のための統一基準（2005 年12 月）

(注：具体的利用方法は「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書(2006年6月)」及び「情報システムの構築等におけるST評価・ST確認の実施に関する解説書(2006年6月)」で解説)

4.3.1 情報システムのセキュリティ要件
(1) システム計画・設計
【基本遵守事項】
(d) 情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、**当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書(ST: Security Target)のST評価・ST確認を受けること。**(以下、略)

【強化遵守事項】
(f) 情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、**その中から当該セキュリティ機能に関してITセキュリティ評価及び認証制度に基づく認証を取得している製品を情報システムの構成要素として選択すること。**

6.1.1 機器等の購入
(2)機器等の購入の実施における手続きの遵守
【基本遵守事項】
(d) 情報システムセキュリティ責任者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、**総合評価落札方式により購入を行う場合には、これについて、ITセキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。**

6.1.3 ソフトウェア開発
(3) ソフトウェアの設計時
【基本遵守事項】
(e) 情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、**これを実現するセキュリティ機能の設計について第三者機関による設計仕様書(ST: Security Target)のST評価・ST確認を受けること。**(以下、略)

ITセキュリティ評価及び認証制度(IPA)

(参考)政府機関統一基準と経済産業省施策との関係③

政府機関の情報セキュリティ対策のための統一基準（2005 年12 月）

ISMS適合性評価制度(JIPDEC等)
情報セキュリティ対策ベンチマーク(IPA)等

6.1.2 外部委託
（1）府省庁内における情報セキュリティ確保の仕組みの構築
【強化遵守事項】
（c）統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、**国際規格を踏まえた委託先の情報セキュリティ水準の評価方法**を整備すること。
（d）統括情報セキュリティ責任者は、**前事項の評価方法に従って**、求める情報セキュリティ要件に対する委託先の候補者の情報セキュリティ水準を確認し、**委託先の選定基準の一要素として利用する**こと。

情報セキュリティ監査等

（4）外部委託の実施における手続の遵守
【基本遵守事項】
（a）情報システムセキュリティ責任者は、**外部委託を実施する際に**、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティ侵害発生時の対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む外部委託に伴う契約を取り交わすこと。また、**必要に応じて、以下の事項を含めること。**
（ア）**情報セキュリティ監査を受け入れること。**
（イ）提供されるサービスレベルに関して委託先に保証させること。

外部委託における情報セキュリティ対策実施規程 策定手引書（2006年3月）

(注：具体的利用方法は「外部委託における情報セキュリティ対策に関する評価手法の利用の手引き(2006年5月)」で解説)

9.2.2 国際規格を踏まえた委託先の情報セキュリティ水準の評価
「**国際規格を踏まえた委託先の情報セキュリティ水準の評価方法**」としては、以下の制度を活用することが考えられる。
(1) 情報セキュリティマネジメントシステムに関する適合性評価制度
(2) 情報セキュリティ対策ベンチマーク
(3) 情報セキュリティ監査

(参考)政府機関統一基準の改訂案
(2007年4月23日情報セキュリティ政策会議資料)

1．技術･環境の変化の反映

1） 情報システムへのIPv6導入に伴う対策(6．2．3) (新規)
IPv6製品の普及に伴い、IPv4とIPv6が共存する情報システムに対する対策の追加

2） 踏み台対策(4．2．4) (新規)
府省庁の情報システムが第三者によって意図しない目的で使われること（踏み台）を防止する対策の追加

3） 暗号モジュール試験及び認証制度の利用(4．1．6)
我が国におけるISO/IEC 19790に基づく暗号モジュール試験及び認証制度の本格運用を踏まえ明記

暗号モジュール試験及び
認証制度(JCMVP：IPA)

2．実務に即した見直し等

1） 情報システム台帳の整備(4．3．1) (新規)
各府省庁が保有する情報システムについて、取り扱う情報とその格付け等を一元的に管理することを追加

2） 情報の取扱いに関する規定の見直し(1．1．3　3．2．4　3．2．5 等)
機密性2情報の範囲、情報の移送･提供等に伴う許可･届出手続を見直し

3） 情報システムの物理的対策の強化(5．1．1)
情報システムの物理的隔離及び入退出管理、盗難防止対策を強化遵守事項から基本遵守事項に変更

4） 情報セキュリティ監査体制の明確化(2．3．2)
情報セキュリティ監査実施者の位置づけ、自己点検との関係を明確化

5） 暗号化の運用管理方法の明確化(4．1．6)
暗号化の方法について、各職員が個別に選択せずに、府省庁で運用管理方法を定めることを明確化

6） その他
表現の改善等