わが国の情報セキュリティ政策について

経済産業省 商務情報政策局
情報セキュリティ政策室
三角　育生

IT化の急速な進展

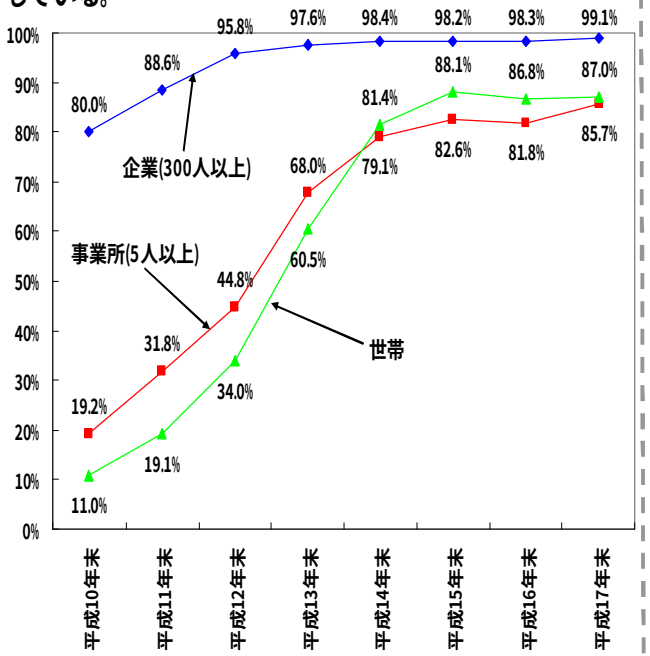
インターネットの爆発的普及等を通じて、情報技術(IT)は、ネットベンチャーやハイテク産業といった特殊な世界の出来事から、家庭での電子メール活用、職場での一人一台ＰＣなど、身近な生活の出来事に。

産業の現場でも、電子商取引の拡大、自動車の電子制御化などのように、ソフトウエア化・ネットワーク化が進展。

→ ＩＴは、産業・社会の隅々に浸透し、物理的活動等を代替

参考：世帯、事業所及び企業でのインターネット普及率

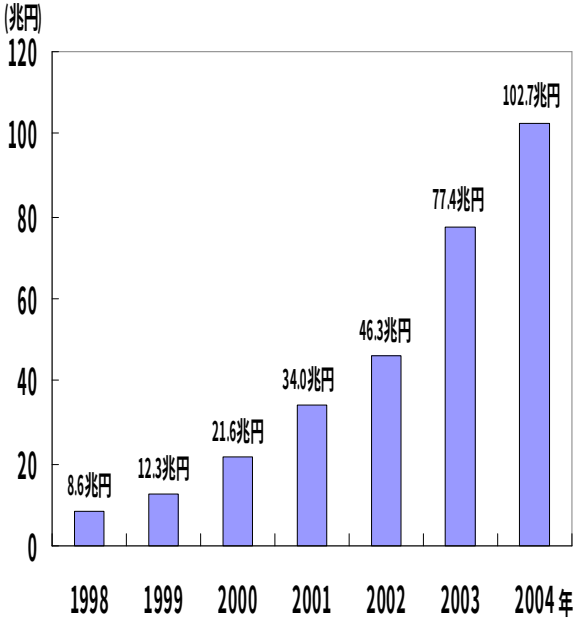
インターネットの普及率は、着実に増加してきており、特に企業においては、ほぼ全てでインターネットへ接続している。



(出典：平成１７年通信利用動向調査等)

参考：ＢｔｏＢ電子商取引の市場規模推移

ＢｔｏＢの電子商取引取引は急速に普及しており、市場規模は６年間で約１２倍となっている。

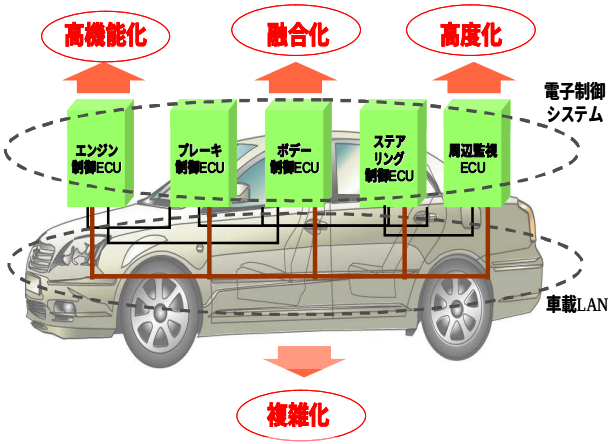


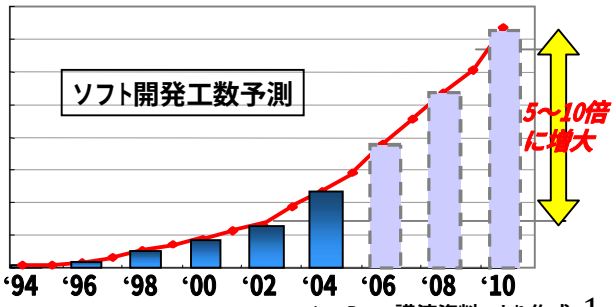
注：1999年はBtoB EC調査を行っていないため、1998年調査における予測値を使用。

(出典：電子商取引に関する実態・市場規模調査)

参考：電子制御システムの進化

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％

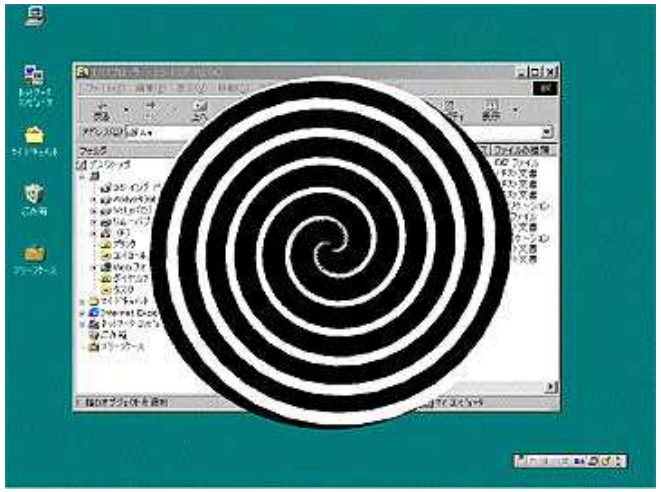




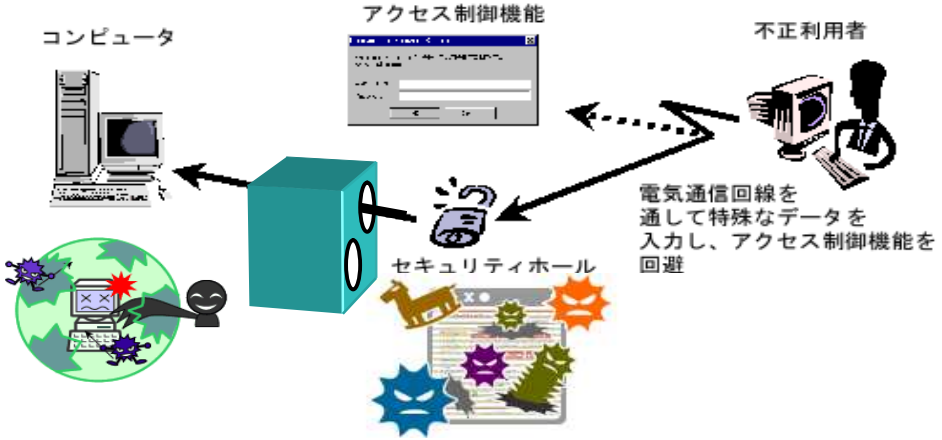
JasPar 講演資料 より作成

(参考)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】

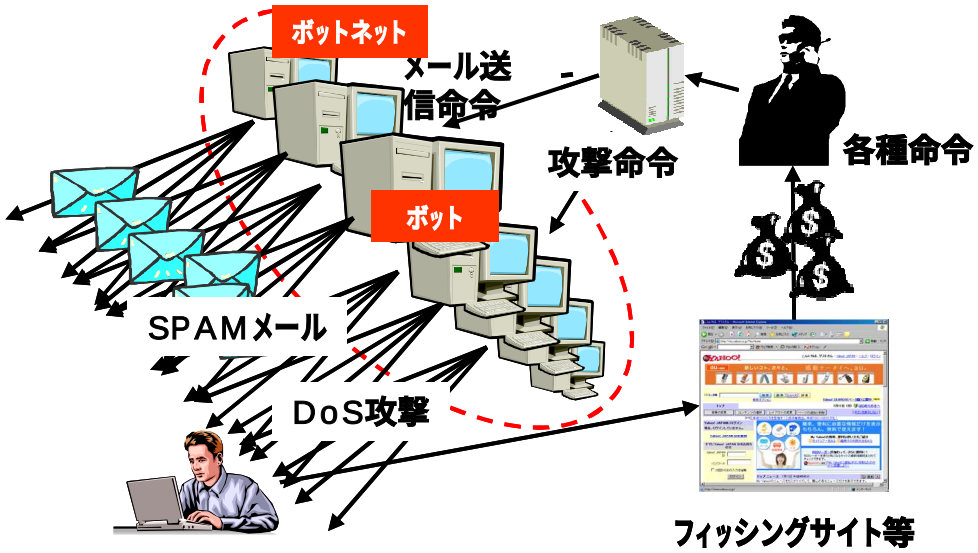


【脆弱性(安全上の問題箇所)】



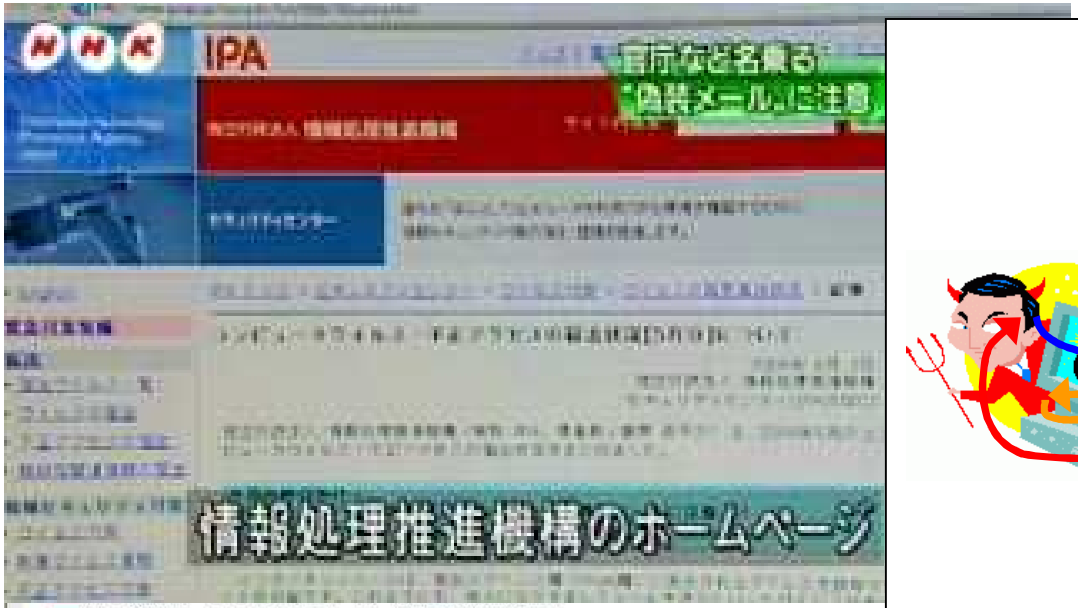
【フィッシング】

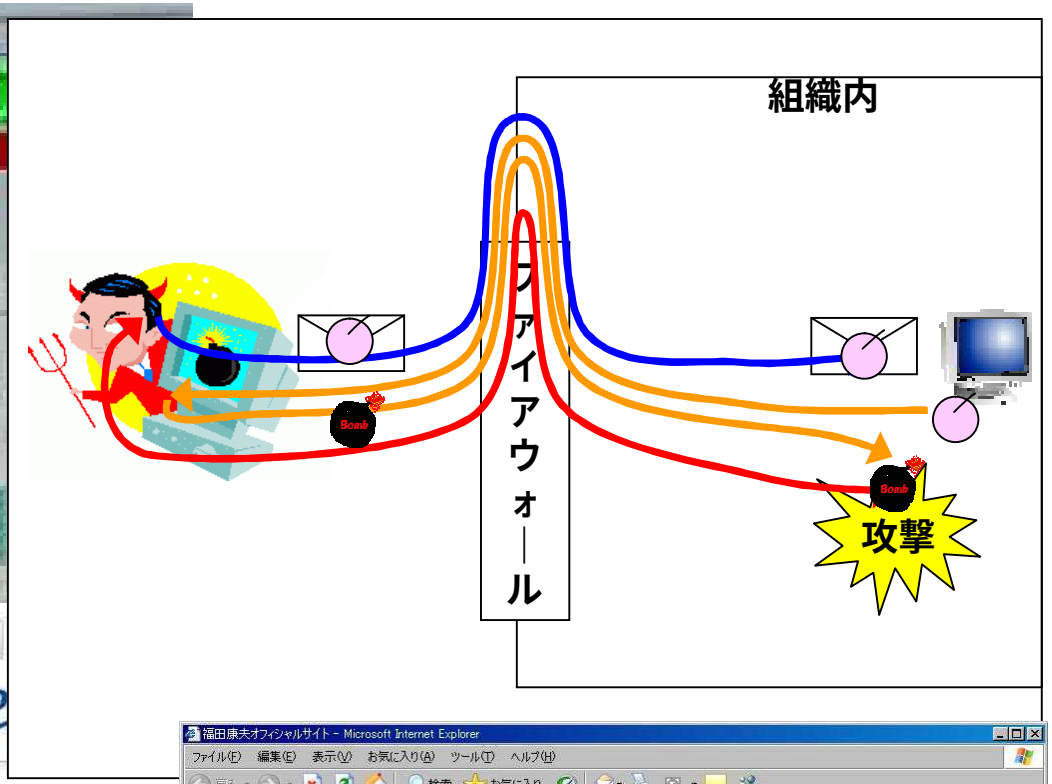
【ボット】



(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。

（参考）新たな脅威





ニュース

米国務省への不正侵入、MS Officeの脆弱性から

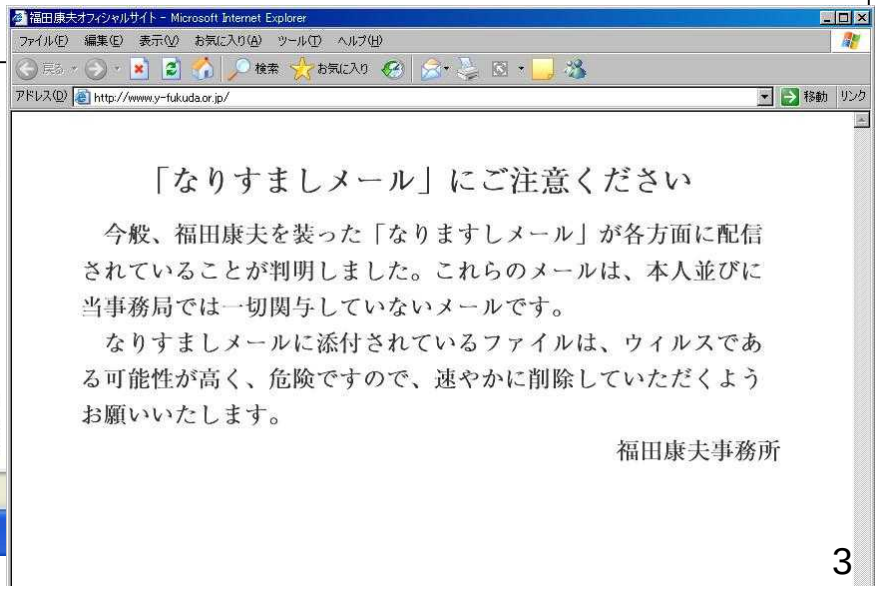
職員が謎のメールを開いたことが不正侵入につながり、米政府の省庁は、北朝鮮によるミサイル発射が懸念される中、緊迫した数週間をインターネットアクセスなしで乗り切る羽目に陥った。

2007年04月19日 15時53分 更新

ワシントン（Associated Press）

昨夏、米国務省の国内外のコンピュータを狙った不正侵入が発生したのは、同省アジア支局の職員が謎のメールを開いて以降のことだった。ハッカーらはこのメールを介して、密かに米政府の

スタート　Microsoft PowerPoint...　ITmedia News：米国...



「なりすましメール」にご注意ください

今般、福田康夫を装った「なりますしメール」が各方面に配信されていることが判明しました。これらのメールは、本人並びに当事務局では一切関与していないメールです。

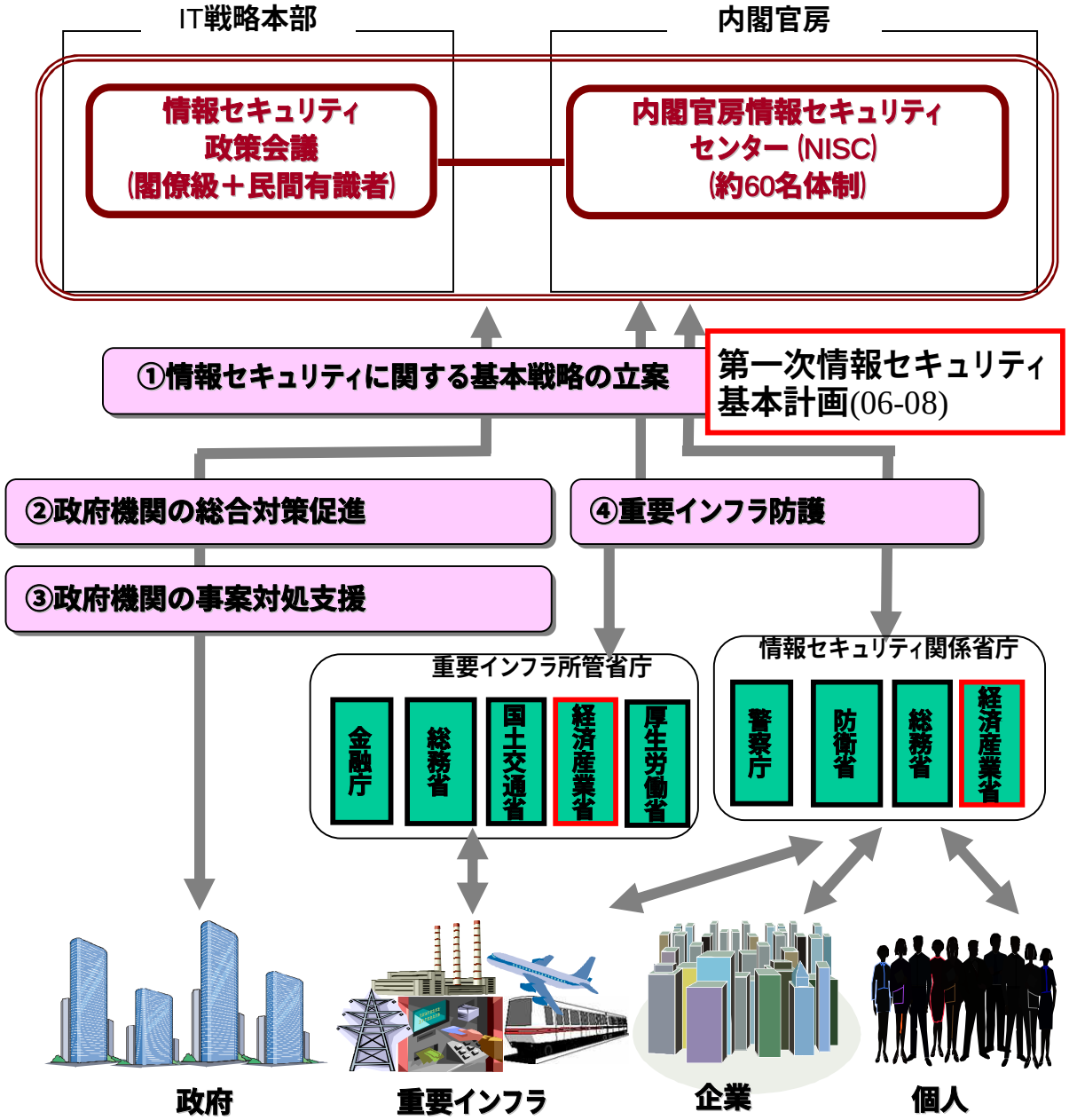
なりすましメールに添付されているファイルは、ウィルスである可能性が高く、危険ですので、速やかに削除していただくようお願いいたします。

福田康夫事務所

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



議長

内閣官房長官

議長代理

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）代表取締役社長兼会長
黒川 博昭　富士通（株）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）

経済産業省施策の概要

「グローバル情報セキュリティ戦略」

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、2007年5月、次の3つの戦略からなる「グローバル情報セキュリティ戦略」を取りまとめた。

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

【委員長】

寺島　実郎	(財) 日本総合研究所会長／(株) 三井物産戦略研究所所長

【委員】(50音順、敬称略)

池上　徹彦	(独) 産業技術総合研究所理事
和泉　法夫	日本SGI(株) 代表取締役社長
今井　秀樹	中央大学教授／(独) 産業技術総合研究所情報セキュリティ研究センター長
江崎　浩	東京大学大学院教授
大木　栄二郎	工学院大学教授
岡村　久道	弁護士
黒川　博昭	富士通(株) 代表取締役社長
古池　進	松下電器産業(株) 代表取締役副社長
志方　俊之	帝京大学法学部教授
関口　和一	日本経済新聞社産業部編集委員兼論説委員
田島　優子	弁護士
土居　範久	中央大学教授
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
藤山　知彦	三菱商事(株) 国際戦略研究所所長
細川　泰秀	(社) 日本情報システム・ユーザー協会(JUAS)専務理事
山口　英	奈良先端科学技術大学院大学教授
山下　徹	(株) NTTデータ代表取締役社長

経済産業省の情報セキュリティ対策（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

企業等の情報セキュリティガバナンスの確立促進

企業が情報セキュリティの観点から、内部統制（情報管理、情報改ざん防止など）の仕組みを構築するときのガイドラインを策定することなどにより、企業の情報セキュリティ対策を促進

内部不正、システム設定ミス等

サーバー

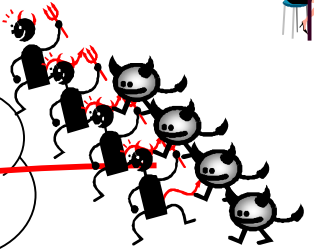
PC

ルーター

インターネット

ウイルス、不正アクセス等

セキュリティ上の弱点、システム障害等



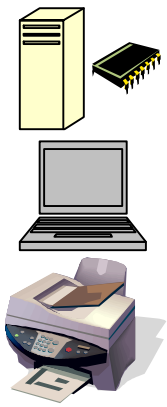
技術的対策の推進

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

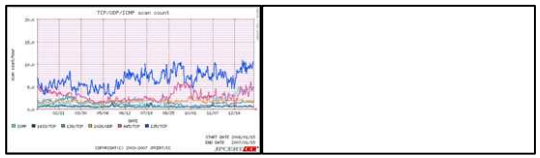
新たな脅威に対応するため、情報セキュリティに係る技術開発及び研究開発を実施



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

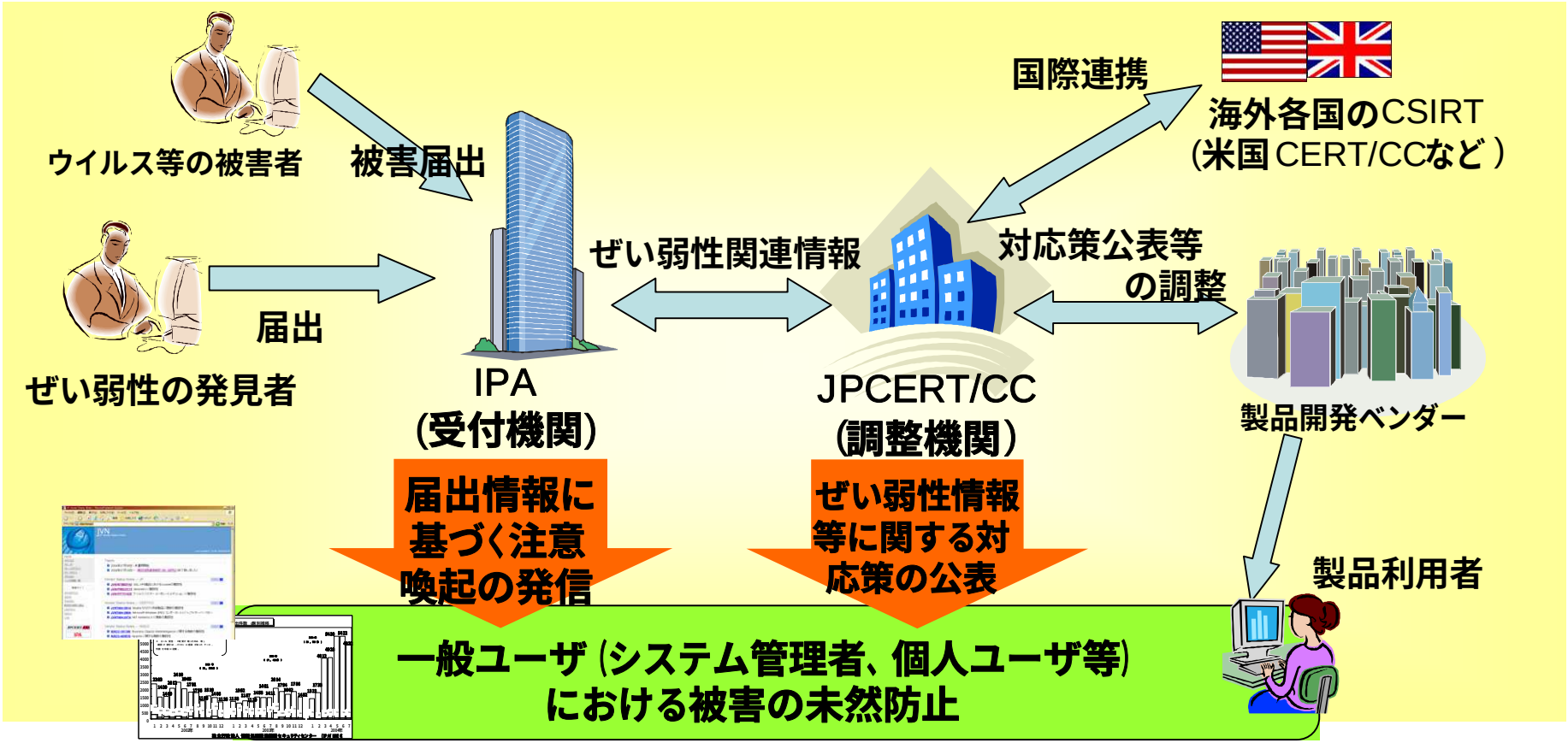


早期警戒体制の整備　～コンピュータセキュリティ早期警戒体制の整備･運用～

METI 経済産業省

- 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
- 未公表のセキュリティ上の弱点（ぜい弱性）情報を米英日のCSIRT（注）間で共有する国際連携体制を整備
- ぜい弱性情報は、届出制度の運用開始後、約3年4ヶ月で1，710件を受領（2007年11月末現在）

（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弱点･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　～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)

収集検体総数	4,821,952
駆除ツール反映検体数	5,604
駆除ツールダウンロード回数	226,670

(2007.10.31時点)

早期警戒体制の整備　～変化への対応－分析機能強化～

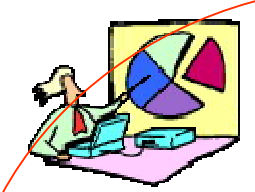
METI 経済産業省

ここの強化が必要！

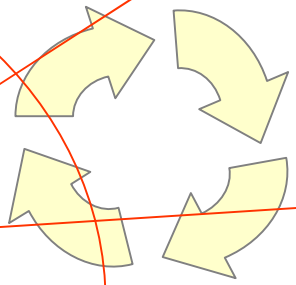
ITを利活用した経済活動

利便性＜＝安全･安心

IT社会基盤の変化
(制度、インフラ等)



新たな影響分析･
予防的対策



サービス･製品･ビジネス
モデルの変化

社会経済変化の分析

悪意･意図的な
新たな脅威･攻撃

攻撃意図の解析

継続的な普及広報活動

経済産業省
Ministry of Economy, Trade and Industry

Check PC！キャンペーン

独立法人 情報処理推進機構

IPA

NPO 日本ネットワークセキュリティ協会

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association
JNSA

財団法人 日本情報処理開発協会

Japan information processing
JIPDEC
Development Corporation

○セミナーの実施
(一般企業を対象)
・経営者向け
・企業の担当者向け
・企業の一般社員向け
2006年度は全国30ヶ所以上で開催。

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

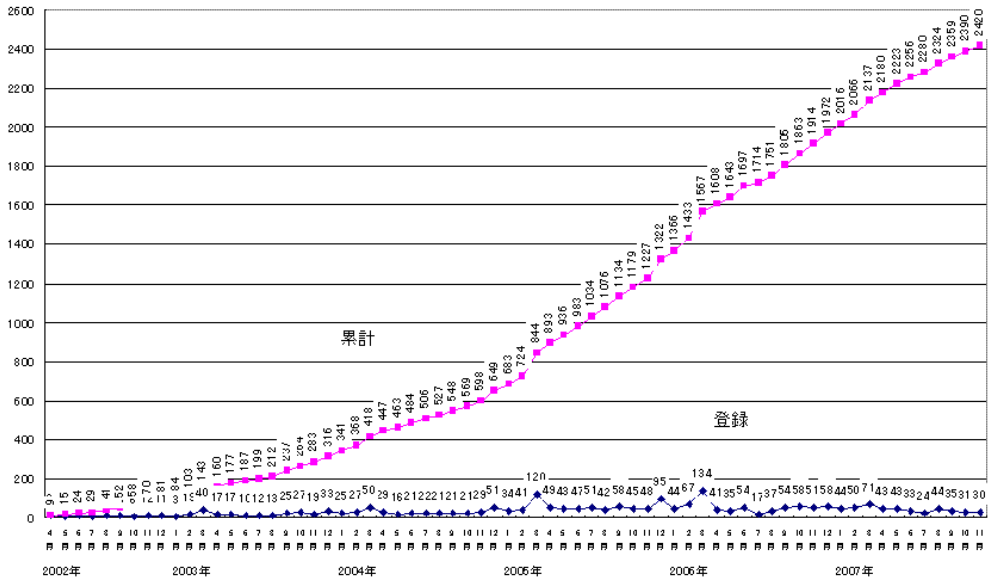
METI 経済産業省

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

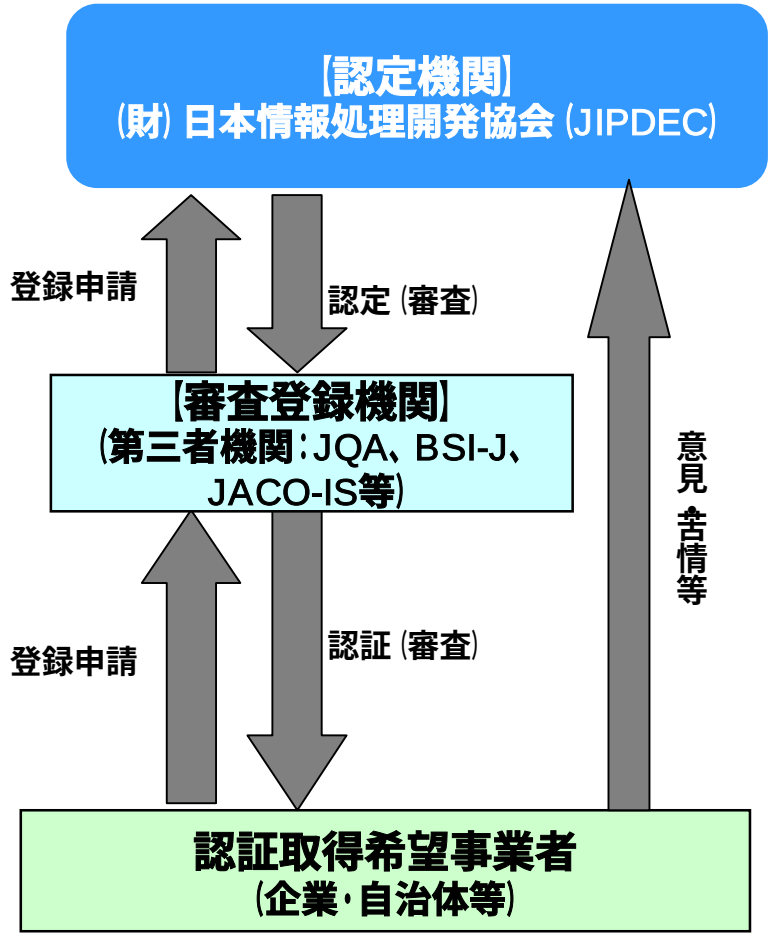
- 本制度は、企業における組織面での情報セキュリティ対策が適切に行われているかどうかについて、第三者機関が国際規格（ISO/IEC 27001等）に基づき、客観的に評価・認証する制度。
- （財）日本情報処理開発協会（JIPDEC）が2002年4月より制度を運用。
- 認証取得事業者数は、2007年12月7日現在で2,420件）。

ISMS認証取得事業者数の推移

（2007年12月7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～

METI 経済産業省

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。「日本セキュリティ監査協会」（ＪＡＳＡ）にて、監査の質の向上のための取り組み。
  - **今年度末を目途にJIS Q 27001に対応した「情報セキュリティ管理基準」の改訂を予定。**

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

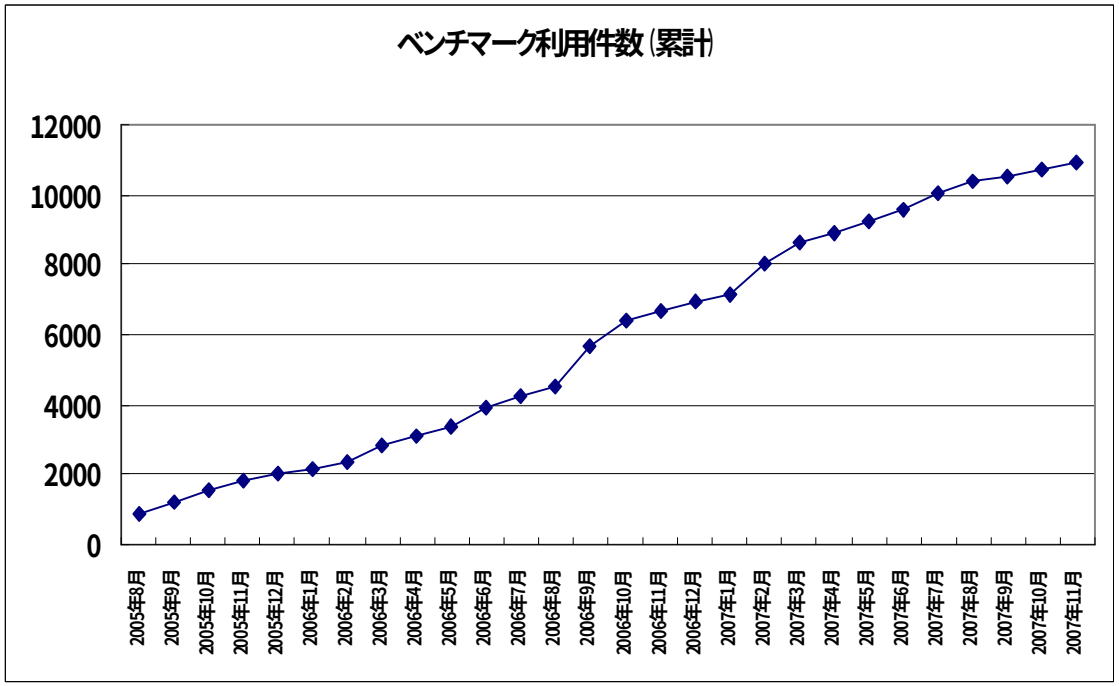
http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

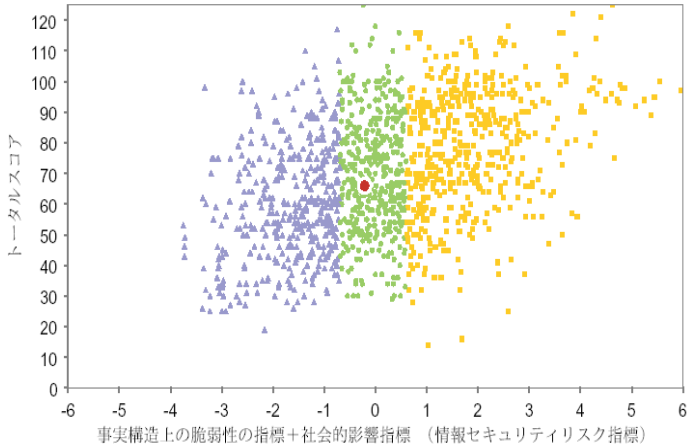
組織的対策の推進　～情報セキュリティ対策ベンチマークの利用状況～

■(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2年3ヶ月で約11,000件のアクセス





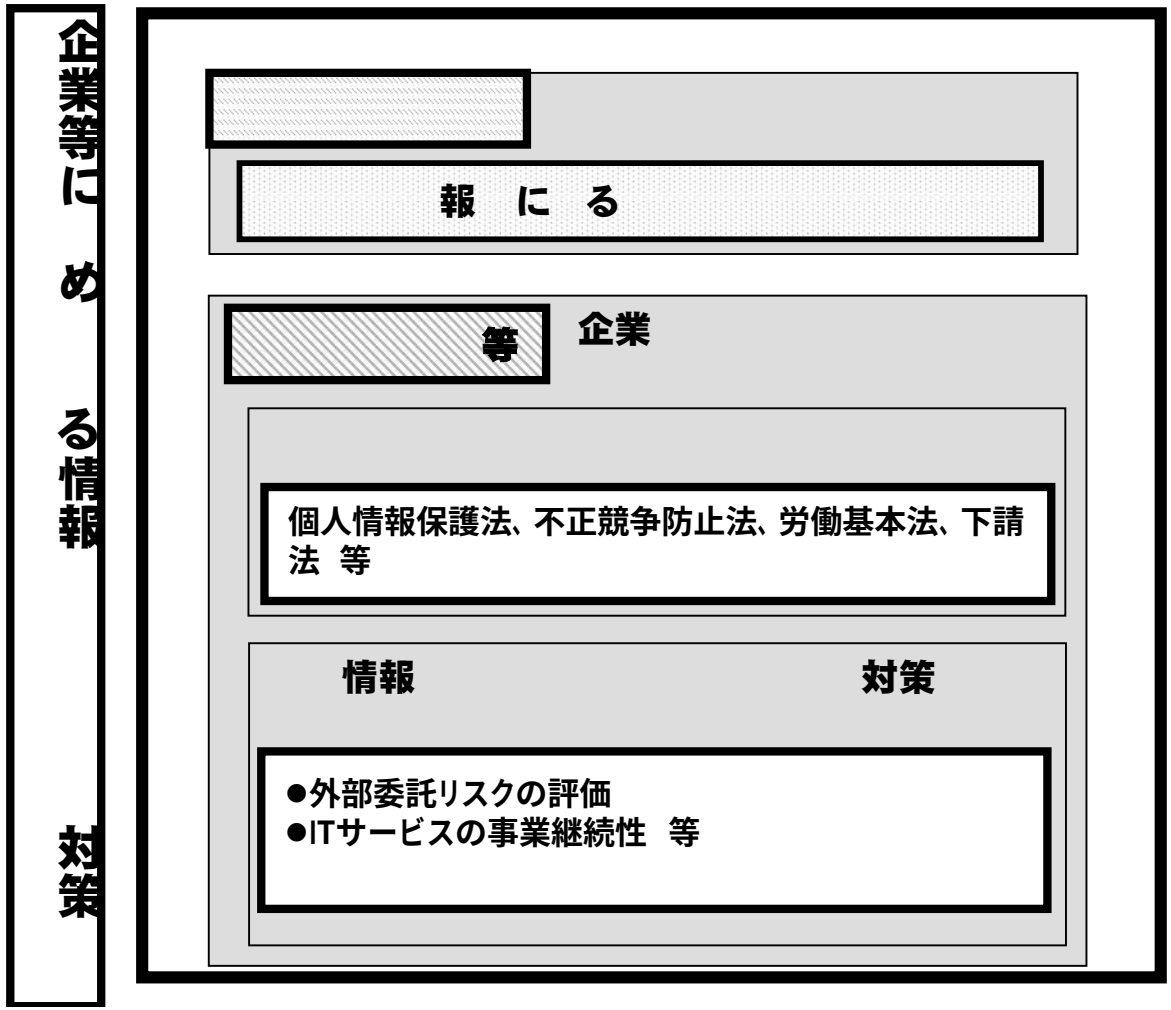
IPAの分析用にデータを提供した者	提供無し	合計
4,397 (40.3.%)	6,517件 (59.7%)	10,914件

2007年11月8日現在

情報セキュリティガバナンスの普及

METI 経済産業省

ITが浸透した企業等において、企業価値の向上、リスク管理などの目的のため、内部統制（法令遵守、情報管理等）の仕組みを情報セキュリティの観点から構築・運用することである「情報セキュリティガバナンス」の普及

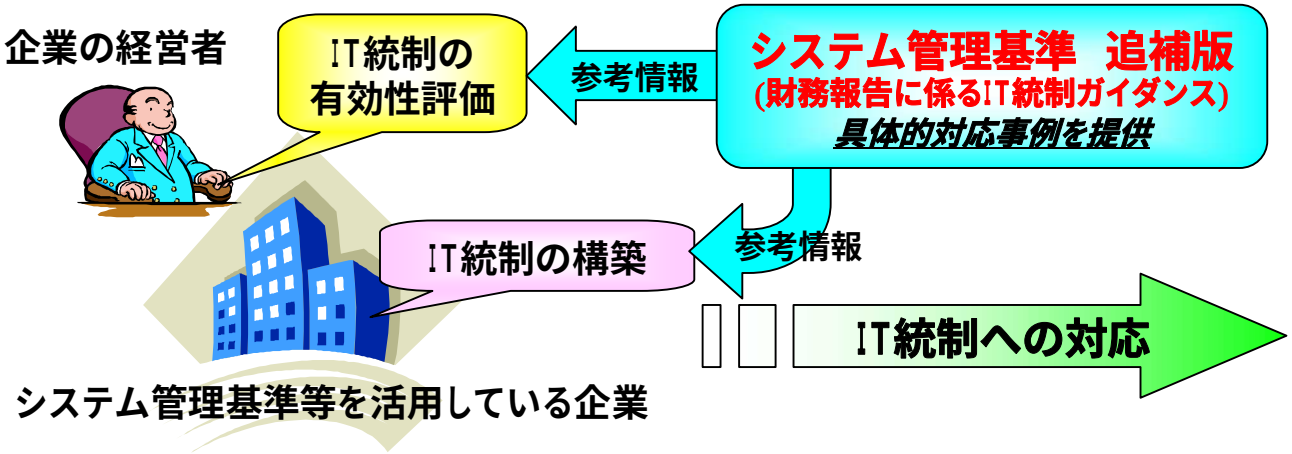


アジア標準

国際標準

組織的対策の推進　～「システム管理基準　追補版」の位置付け～

- ２００６年６月に成立した**金融商品取引法により、上場企業等は、２００８年４月以降、財務報告に係る内部統制の整備及び運用状況の有効性について評価、報告することが義務化。**
- 我が国企業の数多くの業務において、ITへの依存度が増大していることを背景に、**金融商品取引法の枠組みにおいても、「ITへの対応(→IT統制)」は内部統制の基本的要素の一つ。**
- 我が国においては、経済産業省の策定した「システム管理基準」及び「情報セキュリティ管理基準」(以下、「システム管理基準等」)が、有効な情報システム管理のための指針として広く活用されているところであるが、システム管理基準等だけではIT統制に係る詳細が不明確。
- このため、経済産業省として、「企業のIT統制に関する調査検討委員会」等を設置し、2007年３月末、**システム管理基準等を活用している企業が「ITへの対応」を行っていくための「参考情報」として、主要なケースを想定しつつ、それぞれの企業がIT統制をどのように構築し、経営者がその有効性をどのように評価するかについての具体的対応事例集である「システム管理基準　追補版(財務報告に係るIT統制ガイダンス)」を策定。**
- なお、金融商品取引法に基づき、経営者による有効性評価については、公認会計士又は監査法人がその適正性につき監査することとなっているが、本追補版はあくまでもIT統制の構築と経営者による有効性評価までを対象としていることに留意。



金融商品取引法における内部統制の６つの基本要素

1. 統制環境
2. リスクの評価と対応
3. 統制活動
4. 情報と伝達
5. モニタリング（監視活動）
6. **ITへの対応(→IT統制)**

組織的対策の推進　～「システム管理基準　追補版」の構成～

METI 経済産業省

第Ⅰ章 構成と用語について	本追補版の全体構成、各章の概要、本追補版で使用する用語について解説したもの	
第Ⅱ章 IT統制の概要について	財務報告とIT統制の関係、IT統制の意義、種類等、IT統制の基本的な概念について解説したもの	主に経営者等を想定
第Ⅲ章 IT統制の経営者評価	財務報告に係る内部統制を経営者が評価するに際して、IT統制をいかに評価すべきかのポイントを解説したもの	主に経営者等を想定
第Ⅳ章 IT統制の導入ガイダンス （IT統制の例示）	企業がIT統制を構築するため、財務情報に係るIT関連のリスクとIT統制の関係、具体的なIT統制の事例等を項目別に解説したもの	主に実務者等を想定
付録１～６	本追補版の利用にあたり参考となる情報を示したもの（本追補版と米国の関連指針等との比較表、システム管理基準と本追補版を合わせた活用方法の例、等）	

（注）本追補版の提供するものは、あくまでも、主要なケースを想定した参考情報であり、第Ⅱ・Ⅲ章を十分理解し、必要に応じて、第Ⅳ章に掲げる項目の修正・削除・追加等を行いつつ、自社の実情に合わせた運用を行っていくこと。

技術的情報セキュリティ対策推進事業（全体像）

METI 経済産業省

■　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、電子認証技術を利用した**電子署名の利用促進**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。

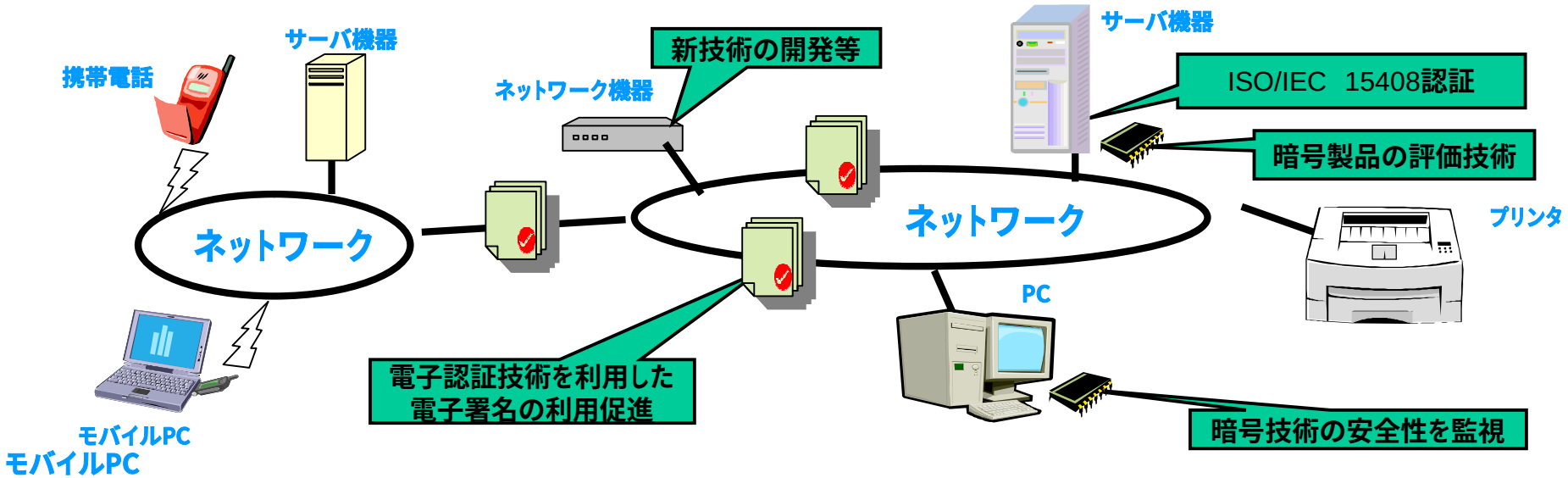
- ✓IT製品（ＯＳ、ルーター等）　：国際標準ISO/IEC15408（コモンクライテリア）に基づいた第三者評価・認証制度を推進
- ✓暗号（ＲＳＡ、ミスティー等）　：電子政府推奨暗号（平成15年2月選定）の安全性を監視
- ✓暗号製品（ＩＣカード等）　：国際標準ISO/IEC19790に基づいた第三者試験・認証制度を推進
- ✓セキュリティ評価技術の確立　：暗号モジュール（暗号製品）に係るセキュリティについての評価技術の開発を推進

➢　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

➢　電子認証技術を利用した**電子署名の利用促進**

- ✓電子署名法制度の円滑な実施　→　認証業務に係る技術の評価に関する調査研究、利用者等に対する必要な情報提供等を行い、適切な電子署名の利用を可能とする。

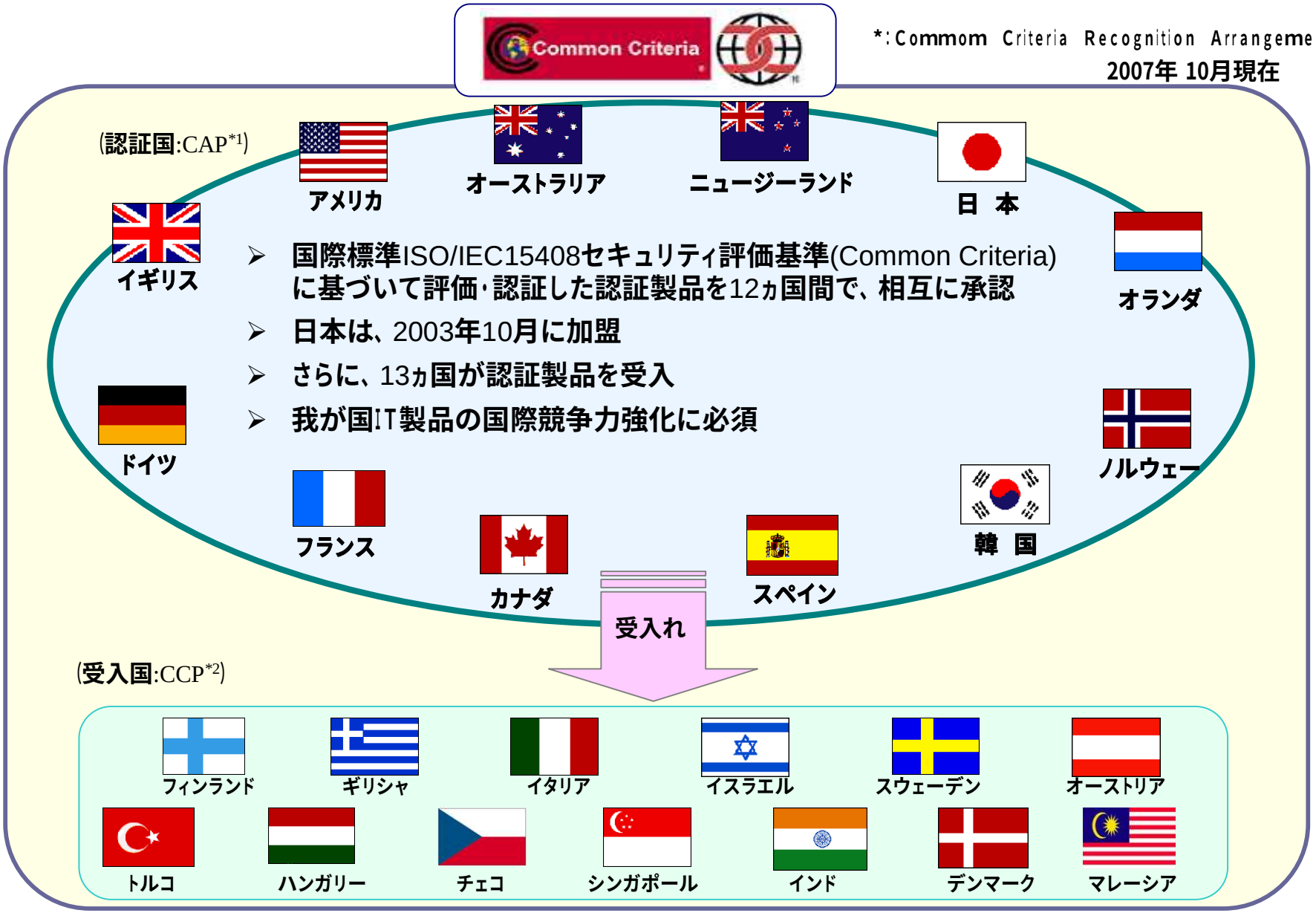


技術的対策の推進
～ITセキュリティ評価及び認証制度に係る国際相互承認協定（CCRA*）～

METI 経済産業省

*：Commom Criteria Recognition Arrangement

2007年 10月現在



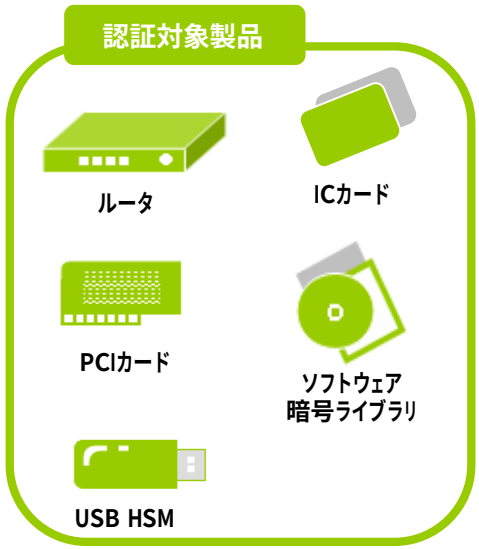
*1 CAP：Certificate authorising participants

*2 CCP：Certificate consuming participants

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）

技術的対策の推進　～電子政府推奨暗号リスト～

METI 経済産業省

平成15年2月20日 総務省 経済産業省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注2)
共通鍵暗号	64 ビットブロック暗号(注3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
共通鍵暗号	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注5)
その他	ハッシュ関数	RIPEMD-160(注6)
		SHA-1(注6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

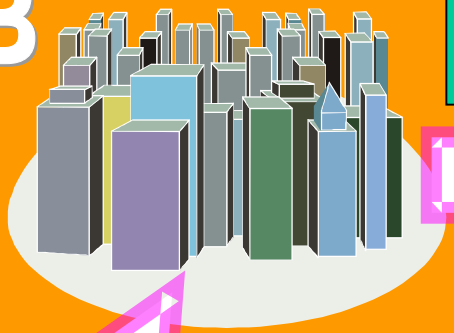
(注1)SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。
(注2)KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism) 構成における利用を前提とする。
(注3)新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビット　ブロック暗号を選択することが望ましい。
(注4)3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
1) FIPS46-3 として規定されていること
2) デファクトスタンダードとしての位置を保っていること
(注5)128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されて いる別の暗号が利用できるのであれば、そちらを使用することが望ましい。
(注6)新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット　以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が　指定されている場合には、この限りではない。
(注7)擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

技術的対策の推進　～電子署名～

METI 経済産業省

政府機関等 G

B 民間企業



② 商業登記に基づく電子認証制度の電子証明書
商業登記法第１２条の２第１項及び第３項の規定に基づき登記官が作成した電子証明書

① 電子署名法に基づく認定認証事業者による電子証明書
電子署名及び認証業務に関する法律第13条第1項に規定する電子証明書

③ 公的個人認証サービスの電子証明書
電子署名に係る地方公共団体の認証業務に関する法律第３条第１項 に規定する電子証明書

民間企業

④ 一般の
電子証明書

C 一般市民