資料　3
科学技術・学術審議会　研究計画・評価分科会
安全・安心科学技術委員会（第９回）H19．６．12

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

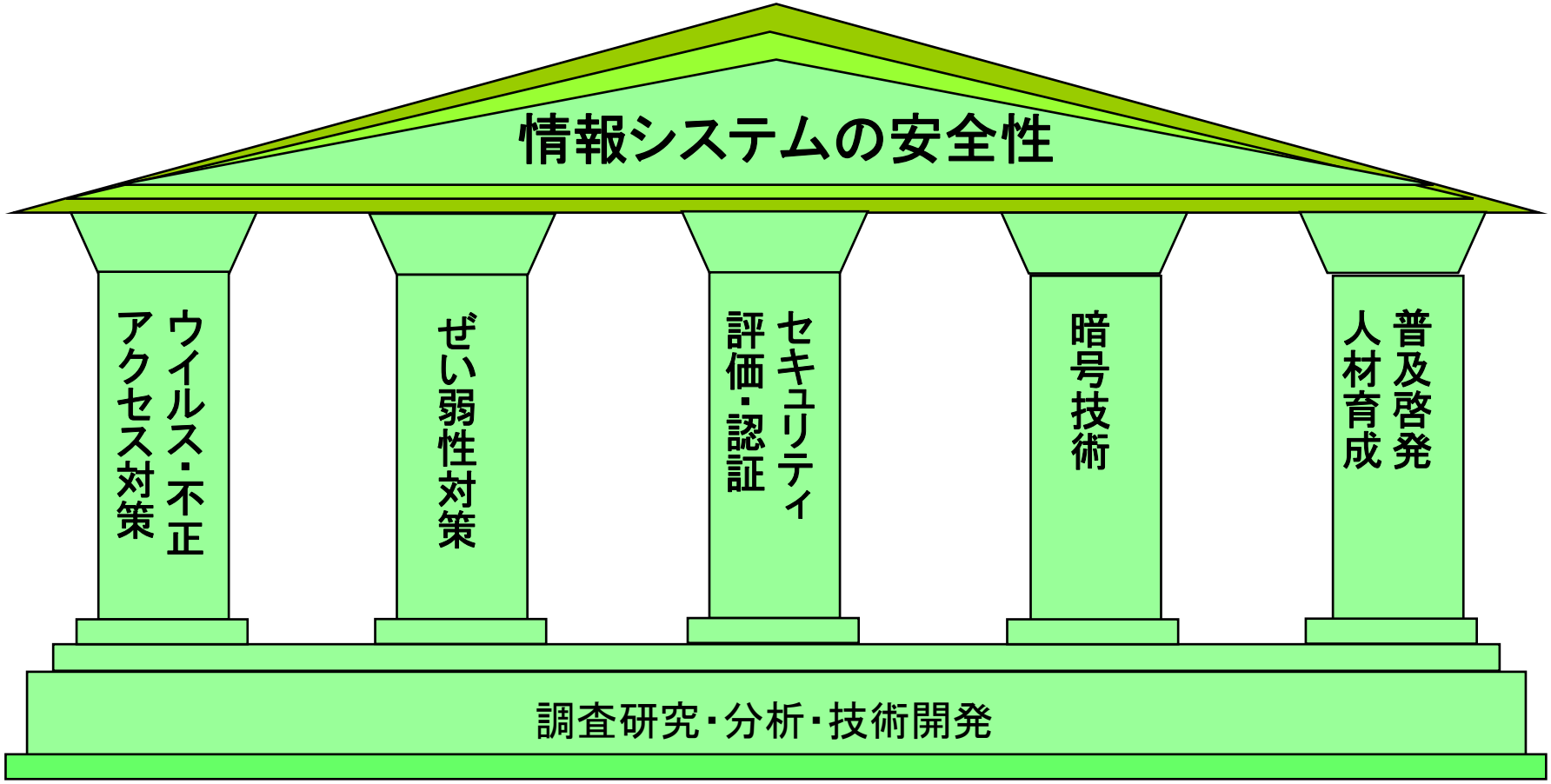
セキュリティセンターの活動について

平成19年6月12日

独立行政法人 情報処理推進機構（IPA）
セキュリティセンター
三角育生

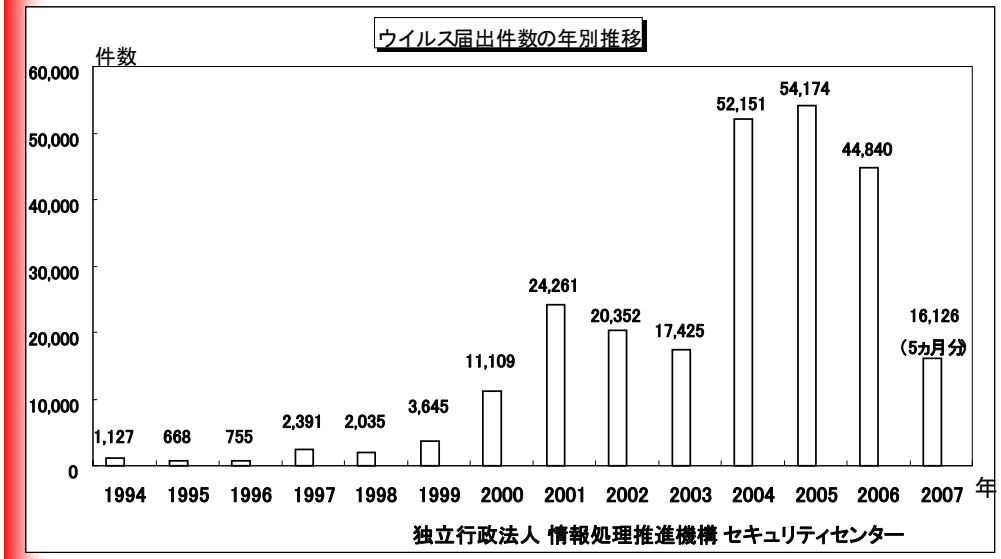
http://www.ipa.go.jp/security/

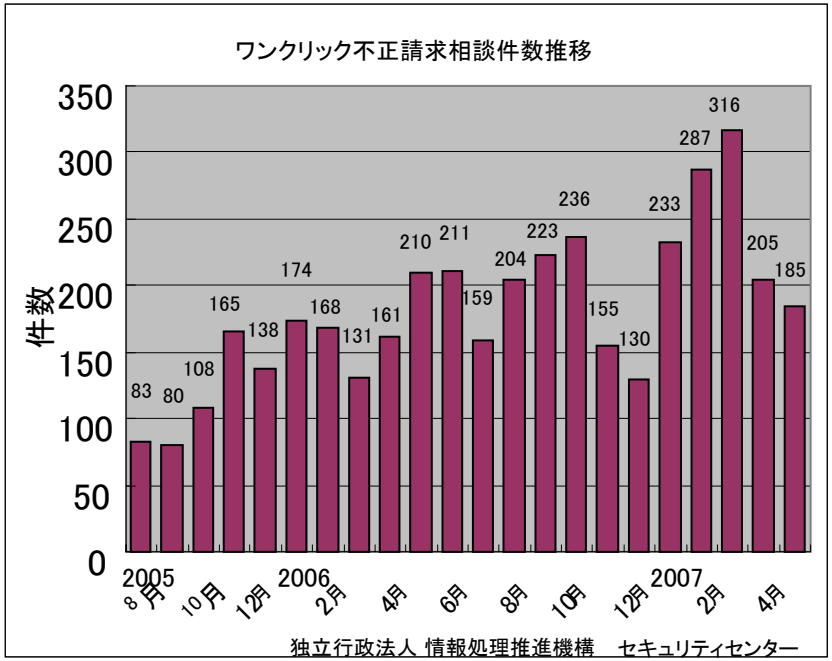
IPAセキュリティセンター



ウイルス･不正アクセス対策

- 経済産業省の告示に基づき届出受付･情報発信
- 相談対応及び調査研究

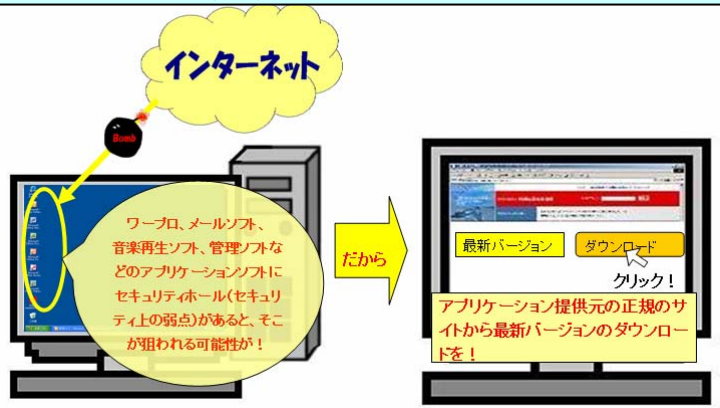




ウイルス・不正アクセス対策

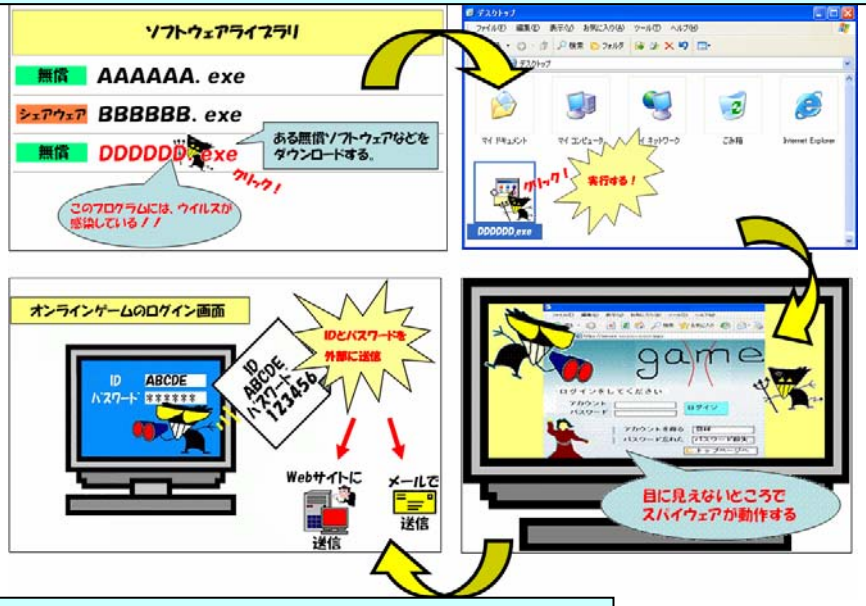
2007年6月公表

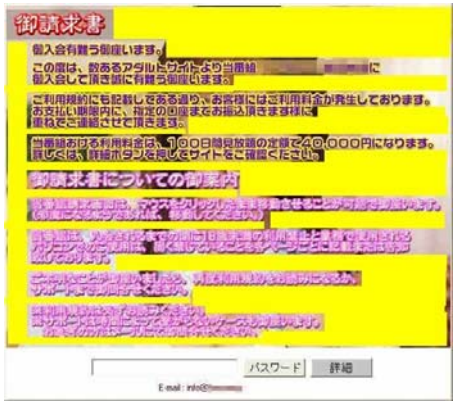
今月の呼びかけ：
「そのアプリケーションソフトには、セキュリティホールはありませんか？」
―セキュリティホール対策は、オペレーティングシステム(OS)だけではない！ ―



2007年1月公表

今月の呼びかけ：「オンラインゲームのパスワードを盗むスパイウェアに注意！！」
―オンラインゲームを狙ったウイルスが大量に出回っています―





不正請求画面の例

2007年4月公表

今月の呼びかけ：
「 警告画面を無視していませんか？」
― 不正プログラムを取り込まないために、警告が出たら先に進まないこと！！ ―

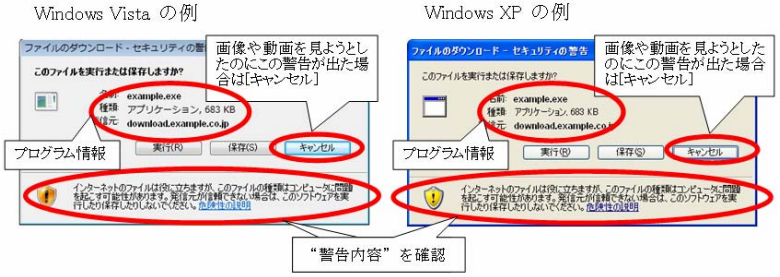
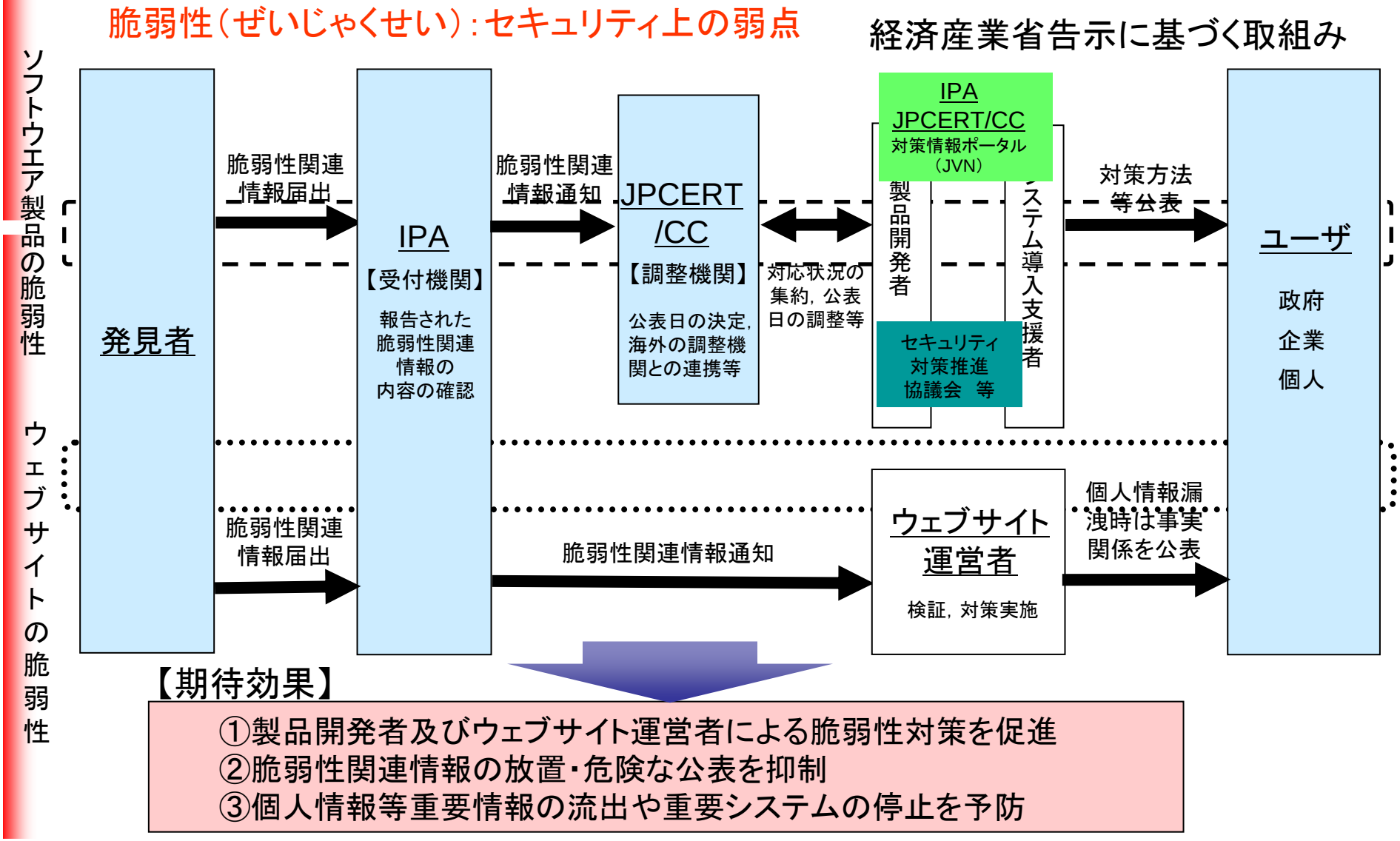
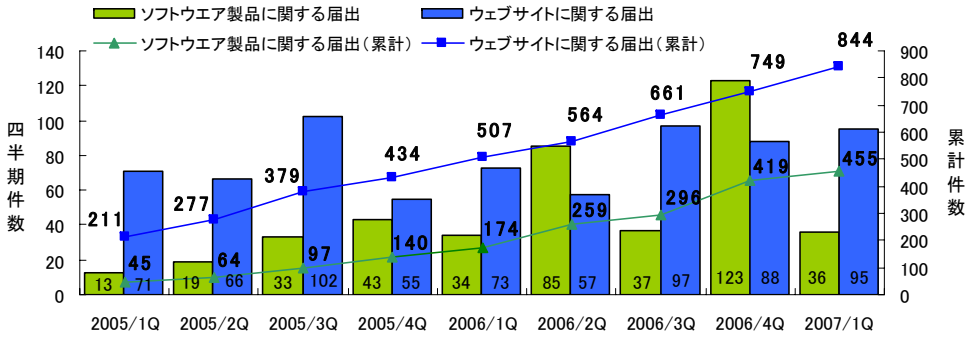


図 a：Windows Vista/Windows XP でのファイルのダウンロードの警告画面

脆弱性関連情報流通の基本枠組み
「情報セキュリティ早期警戒パートナーシップ」



ぜい弱性対策



2004年7月～2007年3月末

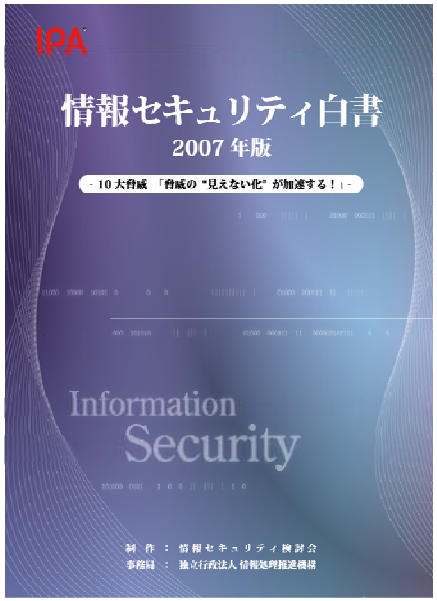
		累計件数
ソフトウエア製品	届出	455件
	脆弱性公表	170件
ウエブサイト	届出	844件
	修正完了	456件

安全なウエブサイトの作り方

セキュア･プログラミング講座

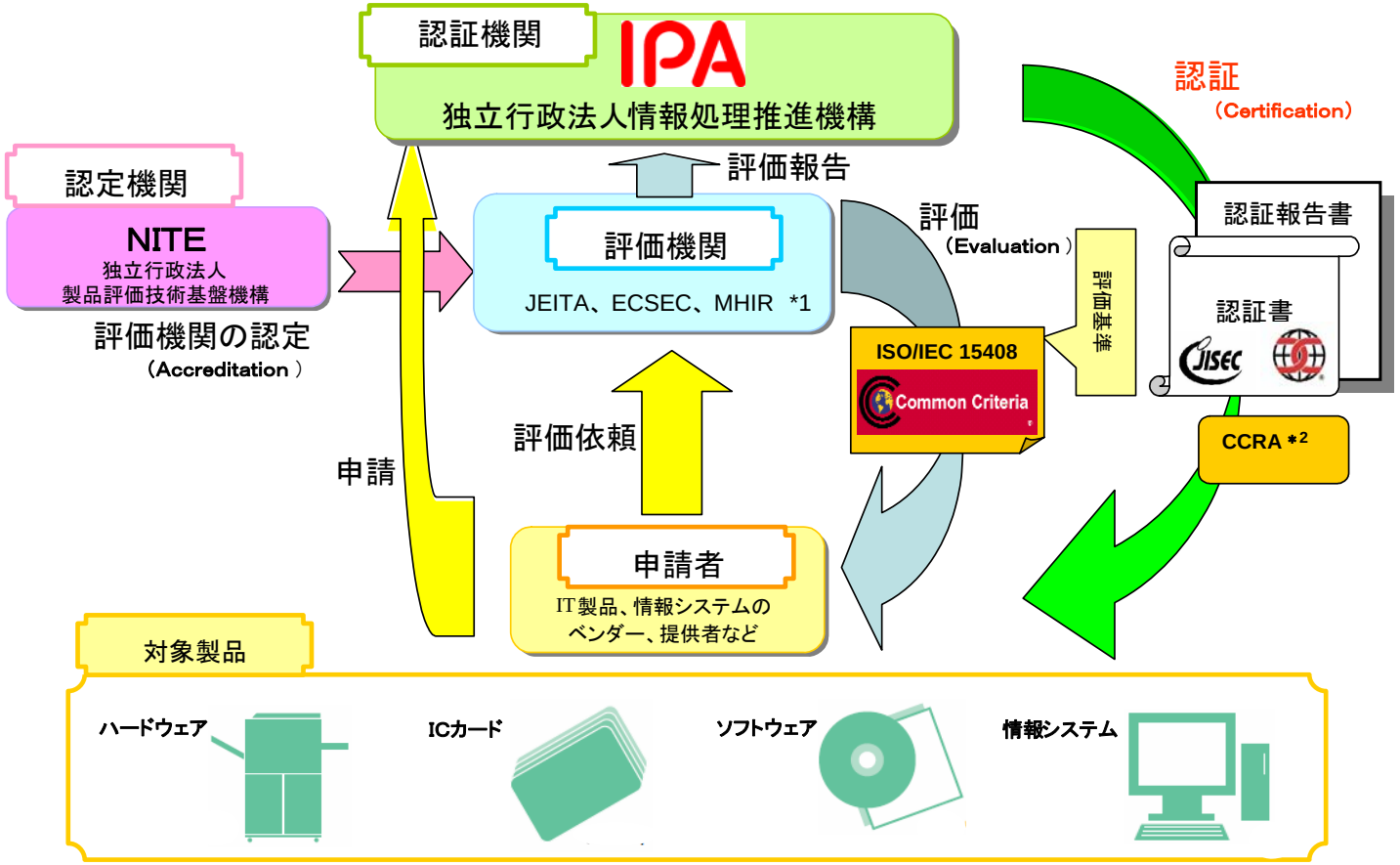
組込みシステムのセキュリティ

…



ITセキュリティ評価・認証制度

・国際標準ISO/IEC 15408 (CC:Common Criteria、JIS X 5070)に基づいてIT製品(ソフトウェア、ハードウェア)や情報システムを評価・認証する制度



*1 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

*2 Common Criteria Recognition Arrangement 、CC承認アレンジメント

ーCC承認アレンジメント(CCRA*)ー

*:Commom Criteria Recognition Arrangement

2007年5月現在

(認証国:CAP*1)

アメリカ　オーストラリア　ニュージーランド　日本

イギリス　オランダ

- 国際標準ISO/IEC15408セキュリティ評価基準(Common Criteria)に基づいて評価・認証した認証製品を12ヵ国間で、相互に承認
- 日本は、2003年10月に参加
- さらに、12ヵ国が認証製品を受入
- 我が国IT製品の国際競争力強化に必須

ドイツ　ノルウェー

フランス　カナダ　スペイン　韓国

受入れ

(受入国:CCP*2)

フィンランド　ギリシャ　イタリア　イスラエル　スウェーデン　オーストリア

トルコ　ハンガリー　チェコ　シンガポール　インド　デンマーク

*1 CAP : Certificate authorising participants　*2 CCP: Certificate consuming participants

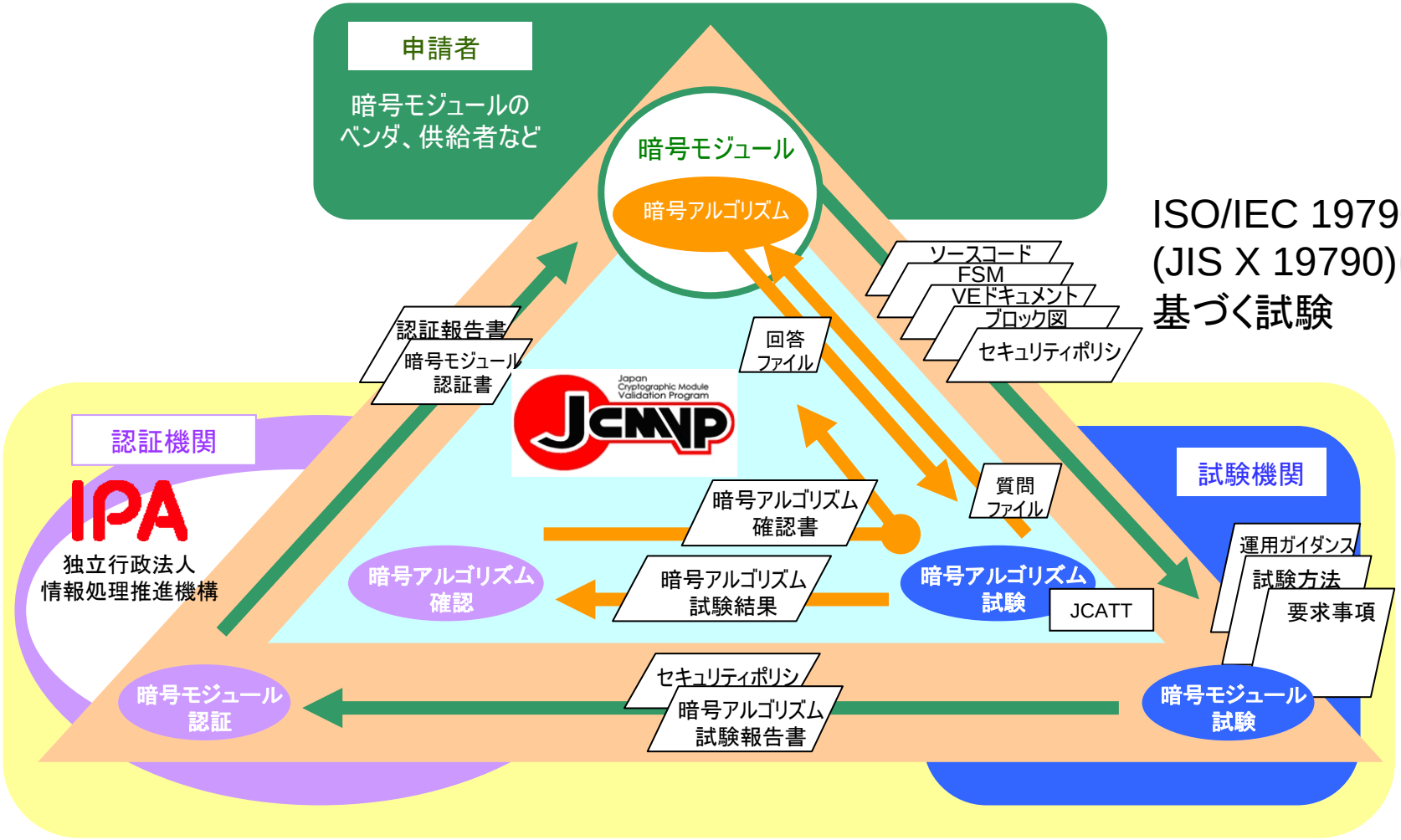
電子政府推奨暗号リスト

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。

暗号モジュール試験及び認証制度

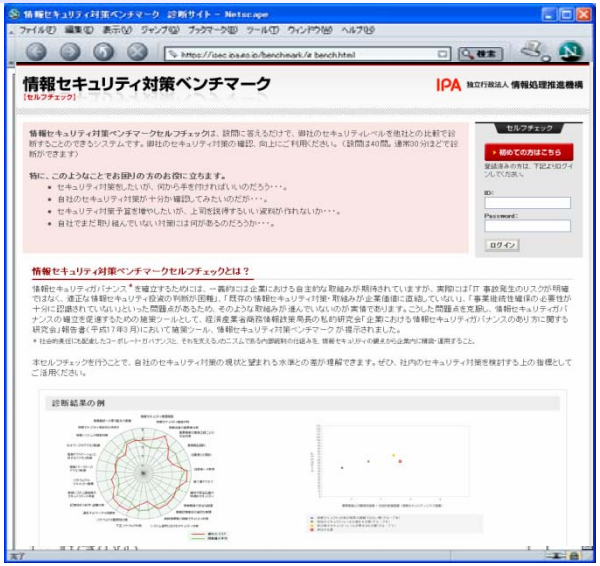


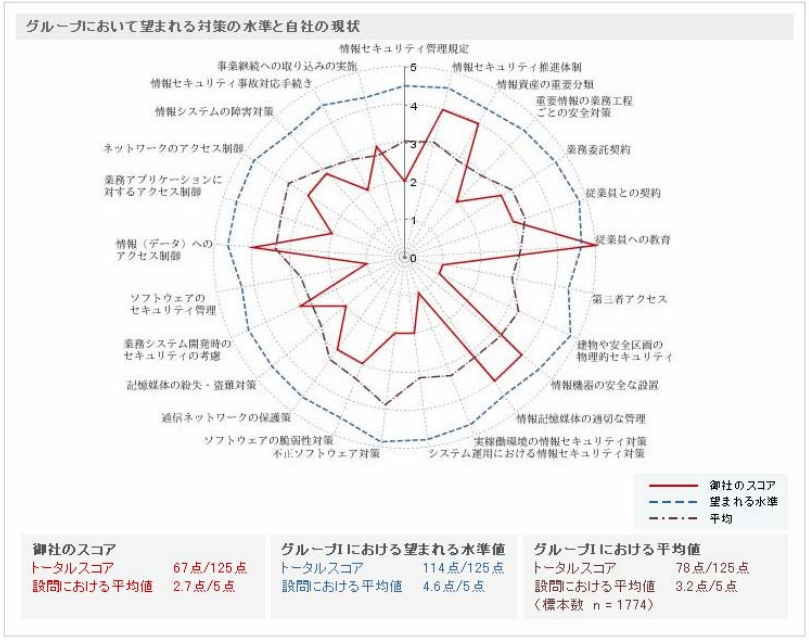
ISO/IEC 19790
(JIS X 19790)に
基づく試験

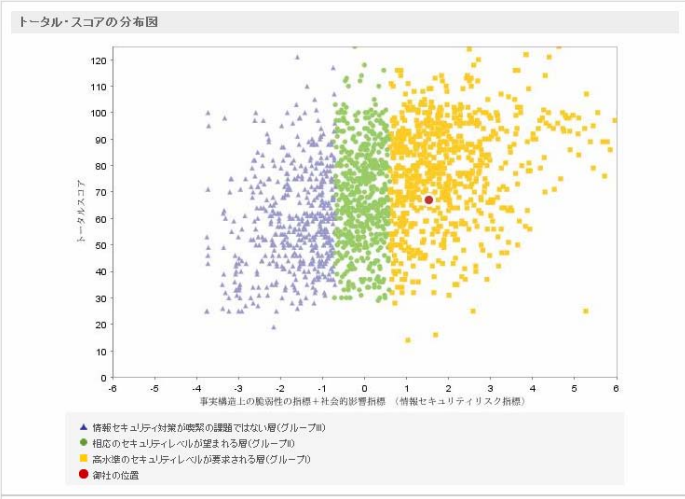
情報セキュリティ対策ベンチマーク（自己診断テスト）

セルフチェックに有用な指標

- セルフチェックにより、自社の現状と望まれる水準との差を把握して、自社と同じタイプの企業群の取組状況に基づく指標と推奨される取り組みを提示。
- Web上で自社の現状を入力すると、結果を表示







調査研究・技術開発

- 広域インターネットトラフィック観測技術
- ぜい弱性情報提供技術
- 暗号評価技術
- LSI回路解析技術
- 組込みシステムのセキュリティ関連技術
- 不正プログラム・罠サイト情報提供技術

等

情報セキュリティ分析機能

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（2007年5月）
　グローバル情報セキュリティ戦略

戦略3：国内外の変化に対応するメカニズムの確立
　情報セキュリティ分析部門（仮称）の創設

「豊かで強く魅力ある日本経済」の実現を情報セキュリティの側面から支援していく観点から、NISC を始めとする国内関係機関や諸外国の関係機関と連携等しつつ、国内外に散逸している関連データや研究結果を幅広く収集等し、データの国際比較、収集等したデータについての計量的な手法等に基づく分析、分析結果の国内外への情報発信等を行うための核となる組織として、IPA やJPCERT/CC 等の国内関係機関に情報セキュリティ分析部門（仮称）を創設する。

セキュアジャパン2007（案）　情報セキュリティ政策会議（2007年4月23日）

2008年度の重点施策の方向性

　情報セキュリティ分析部門（仮称）の創設

　諸外国の機関とも連携等しつつ、国内外の関連データや研究結果を幅広く収集、分析等するため、国内の関係機関に情報セキュリティ分析部門（仮称）の創設を図る。

情報セキュリティ事象被害調査（2006．11公表）

- コンピュータ･ウイルス被害

  アンケート調査：5,500企業あて送付
  1,206社から有効回答　（21.9%)

  モデルを用いた推計

- 不正アクセス（SQLインジェクション）及びWinnyを介した情報漏えい被害

  ヒアリング等による事例研究（計10社）

情報セキュリティ事象被害調査の結果（ウイルスによるシステム停止）

2005年度のケース

	中小企業 （従業員300名未満）	大手・中堅企業 （従業員300名以上）
被害額	約4．3百万円／社	約130百万円／社

- ウイルス被害による直接の復旧コストは大きくない
- 一旦、ウイルス被害により電子商取引システムや重要システムが停止すると、大きな売上減が発生

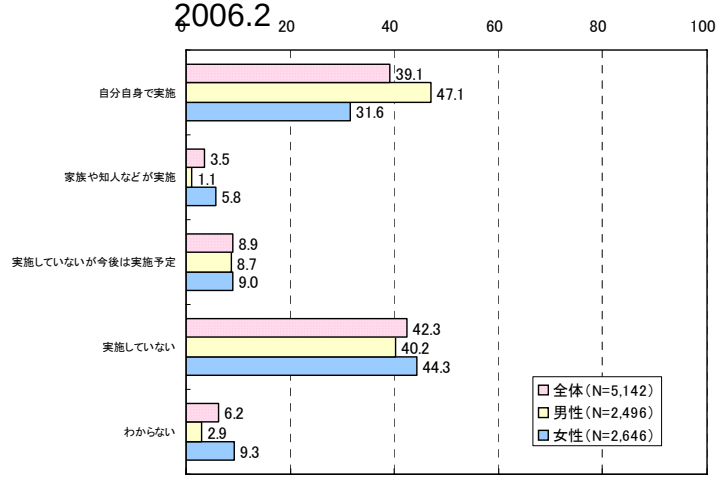
（参考）回答企業　1,206社のうち

復旧コスト発生のあった企業数	中小企業	95社
	大手・中堅企業	110社
売上減のあった企業数	中小企業	35社
	大手・中堅企業	46社

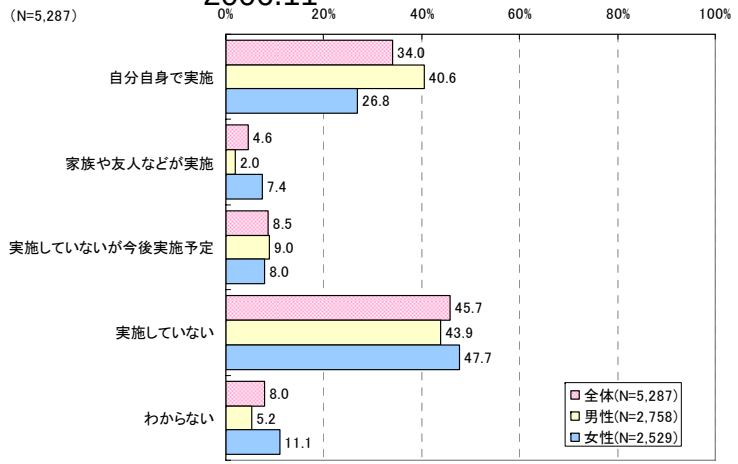
情報セキュリティに関する新たな脅威に対する意識調査

パスワードの定期的な更新　[PC保有者全体／性別]

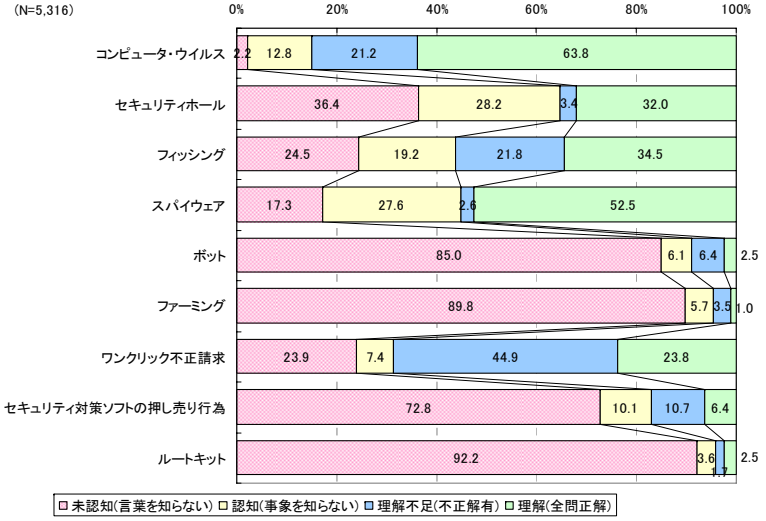
2006.2



2006.11



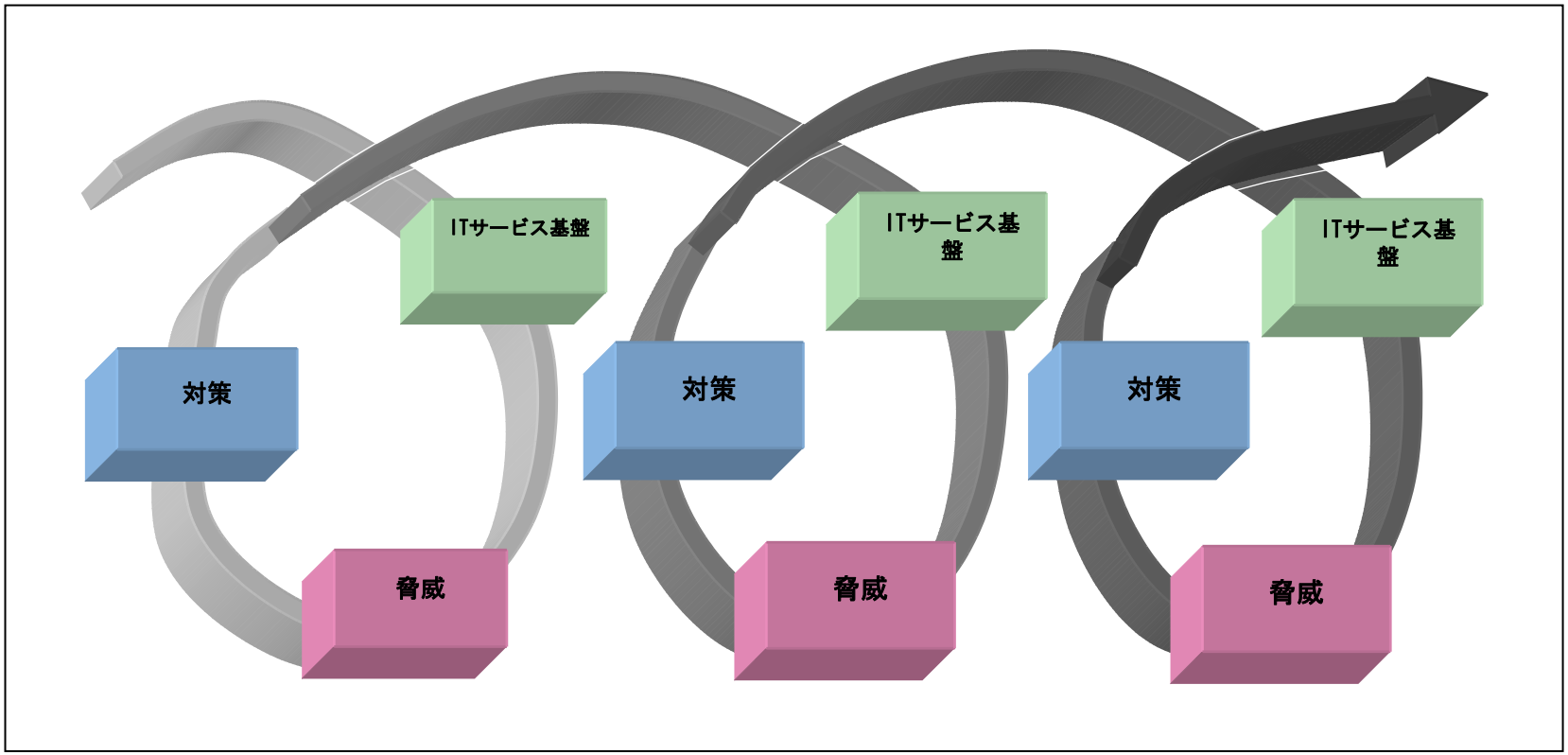
情報セキュリティに関する事象の理解度



- ウエブアンケートこれまで3回実施
  06年2月、11月、07年3月　（第3回分は公表準備中）
- 毎回5000名以上の回答（15歳以上）

情報セキュリティ水準評価指標の検討

検討モデル



バンキング・サービスでの事例

	ITサービス基盤	情報セキュリティ脅威	情報セキュリティ対策
1970年	**現金自動預入支払サービス**（キャッシュカード/ATMの利用が前提）		
		偽造キャッシュカード【偽造キャッシュカードによる預金等不正引出率】	
2002年	1日当たりの**利用限度額引上げ**（ICキャッシュカード利用が前提） 【ICキャッシュカード対応ATM設置率】		**ICカード化** 【ICキャッシュカード利用率】
		ICキャッシュカード盗難 【盗難・偽造ICキャッシュカードによる預金等不正引出率】	
2004年	1日当たりの**利用限度額引上げ**（生体認証用ICキャッシュード・ATMにおける生体認証が前提） 【生体認証対応ATM設置率】		**生体認証**導入で本人認証強化 【生体認証用ICキャッシュカード利用率】

情報セキュリティ水準評価指標の検討

- 社会における情報セキュリティ対策に係る取組みの進展度合を体系的、経年的に把握するため、「情報セキュリティ水準評価指標」の検討を実施
- ・「情報セキュリティ水準評価指標研究会」を設置し、情報セキュリティ水準評価指標を構成する個別指標の検討指針を示すモデルを提案し、このモデルを活用しつつ、具体的な指標の選定も実施。

～情報セキュリティ水準評価指標の例～

組織・人的対策	マネジメントシステム	リスク分析実施率（企業）
	教育・啓発	従業員に対する情報セキュリティ教育実施率（企業）
		情報セキュリティの必要性認識率（個人）
	監査	情報セキュリティ内部監査実施率（企業）
技術的対策	予防・制御	＜少額決済専用電子マネーの普及状況＞ 発行枚数
		ICキャッシュカード利用率
		デジタル著作権管理（DRM）技術普及率
対策リソース	情報セキュリティ投資	IT関連予算に占める情報セキュリティ投資割合（企業）
		IT関連予算に占める情報セキュリティ投資割合（政府）

独立行政法人　情報処理推進機構
セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
　文京グリーンコートセンターオフィス１６階
TEL 03（5978）7508　　FAX 03（5978）7518
電子メール　isec-info@ipa.go.jp
URL　http://www.ipa.go.jp/security/