我が国の情報セキュリティ政策の現在と今後

平成２２年１月２３日

経済産業省 商務情報政策局
情報セキュリティ政策室
黒田俊久

企業に対する情報セキュリティ政策の背景

経済産業省 Ministry of Economy, Trade and Industry

我が国産業の競争力強化

● ＩＴを基盤とした情報の利活用は競争力の源泉

↓

競争力強化を阻害する情報セキュリティに係る要因

しかし、企業の情報資産に対する脅威は増大の一途
⇒　事件・事故が多数発生

↓

情報セキュリティ基本計画に位置づけ

● 第二次情報セキュリティ基本計画にて「情報セキュリティガバナンスの確立」を位置づけ［２００９年２月　情報セキュリティ政策会議（議長：内閣官房長官）で決定］
※情報セキュリティガバナンス：情報セキュリティの観点からガバナンスの仕組みを構築・運用

【 第二次情報セキュリティ基本計画 】（計画期間　2009年度～2011年度）
（http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf）

● 企業における情報セキュリティ対策の推進は、政府、重要インフラ、個人における対策とともに４本柱の一つ。
● 「政府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目指して最大限の努力を行う」
● 企業に係る第一の情報セキュリティ政策として「情報セキュリティガバナンスの経営の一環としての認識の定着とそれに応えられるツールの存在」を位置づけ。

「第2次情報セキュリティ基本計画」に基づく取組み－今後3年間の重点政策－

経済産業省 Ministry of Economy, Trade and Industry

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	◆情報セキュリティガバナンス確立の促進 ◆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）

主な重点政策②（横断的事項）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

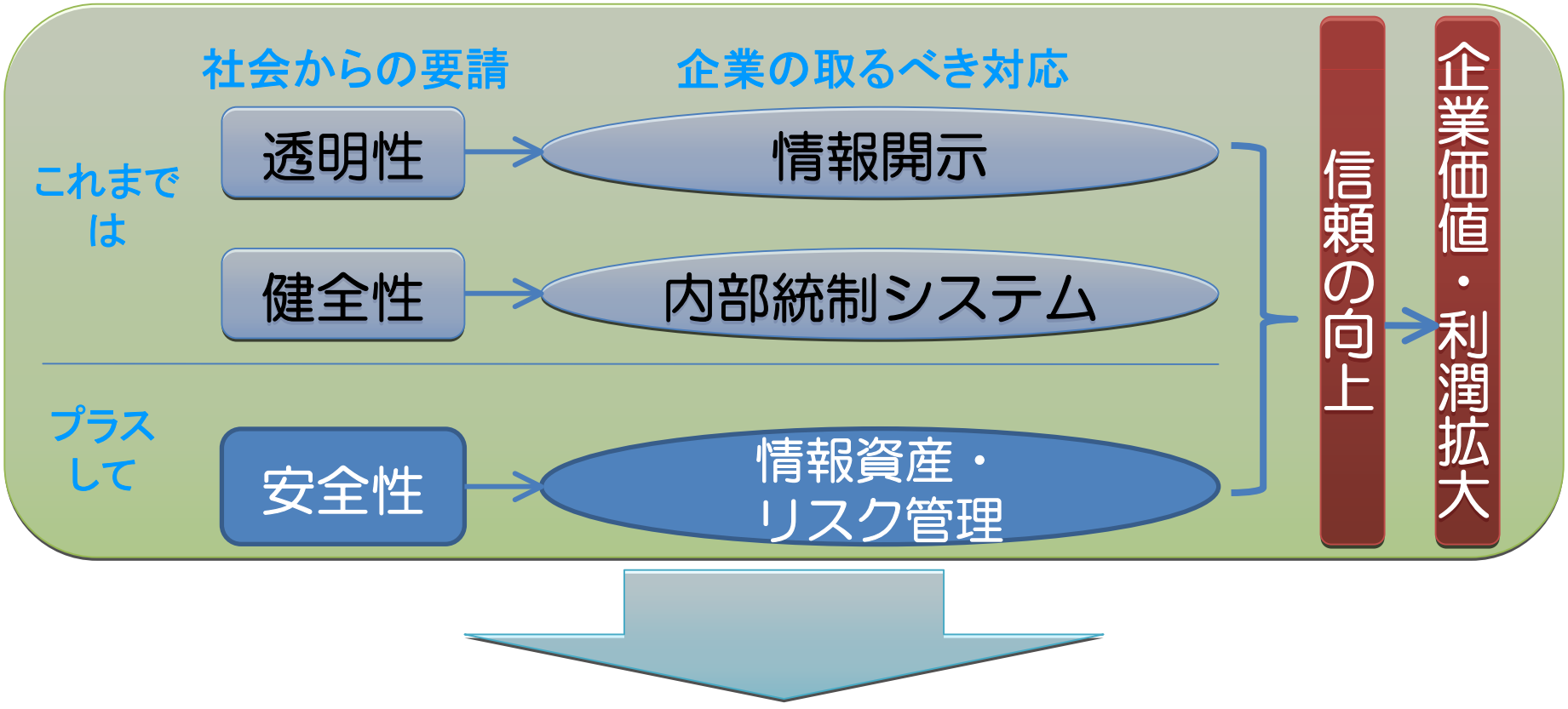
情報セキュリティ人材の育成確保
◆ 政府機関における人材の育成・確保
◆ 保有するスキルの見える化の推進

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・救済のための基盤整備の推進

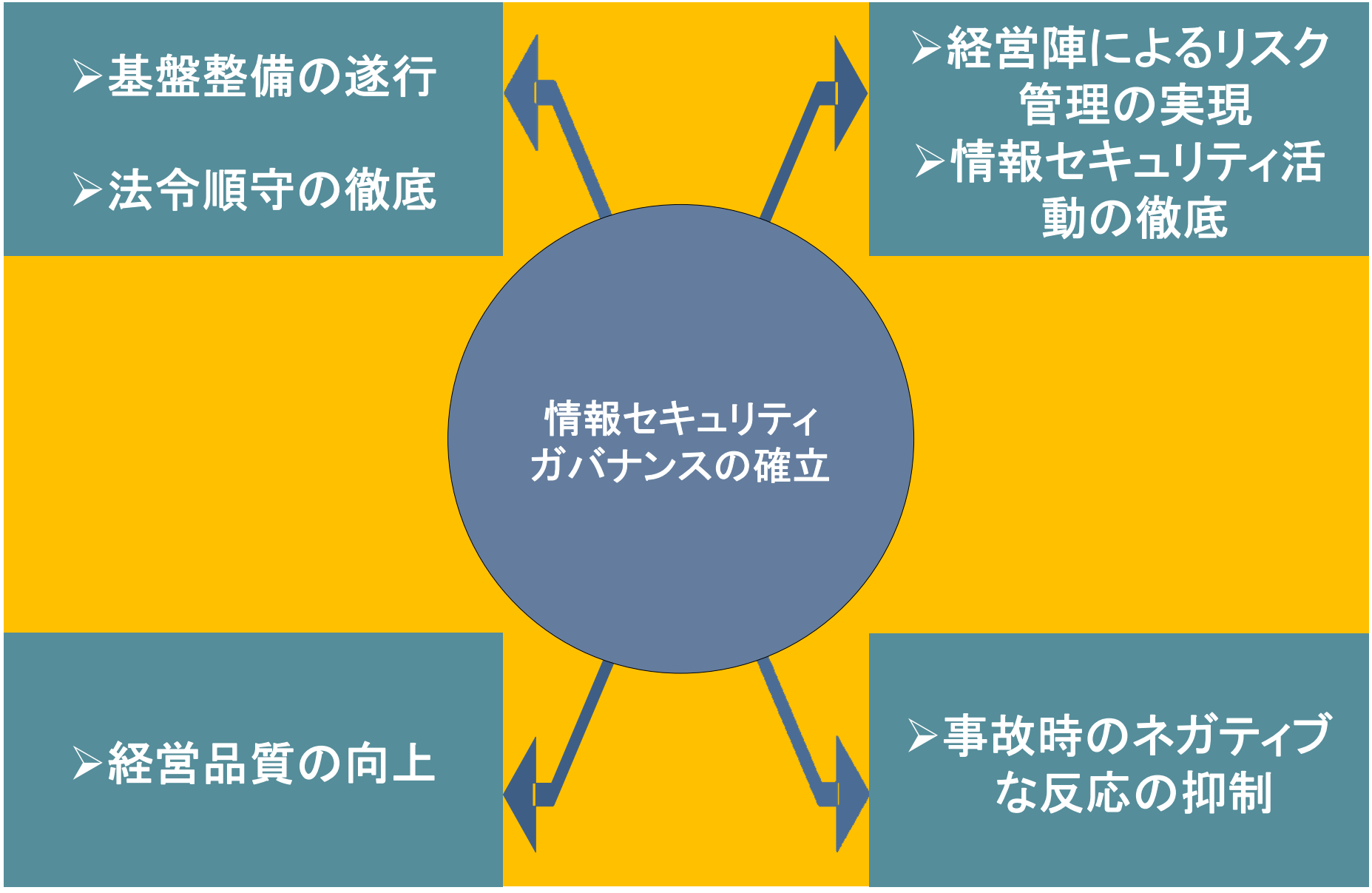
※その他、対策支援主体（「情報セキュリティ対策を実施する主体」の取組みを支援する主体）の取組みも促進する。

企業に必要なガバナンス活動



今後、企業のガバナンス活動に必要となる、経営者による情報セキュリティ上のリスクマネジメント及び改善活動を「情報セキュリティガバナンス」としてまとめたガイダンスを策定

情報セキュリティガバナンスの確立により期待される効果



情報セキュリティガバナンスとは何か

経済産業省 Ministry of Economy, Trade and Industry

定義

- 様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組み）を構築・運用する取組み

情報セキュリティガバナンスの適用対象

- 個別企業、連結ベースの企業グループ、さらにバリューチェーンを形成する企業グループ
  - ITガバナンスモデル（**ISO/IEC38500 企業のITガバナンス**）を参考

経緯

- 2005年3月「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」報告書において、「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義
- 2005年度から、構築支援ツールとして、**「情報セキュリティベンチマーク」**、**「情報セキュリティ報告書モデル」**、**「事業継続計画策定ガイドライン」**を作成し、普及展開を図る
- 2008年度には、「Direct, Monitoring, Evaluate, Report, Oversee」のフレームワークとして構築し、**「情報セキュリティガバナンス導入ガイダンス」**としてまとめた
- 今後、更なる普及展開を図るため、実践的なガイダンス策定、**国際標準化活動支援**（ISO/IEC JTC1 SC27での27014策定）等の活動を行っていく予定

情報セキュリティガバナンスの確立のための施策

経済産業省 Ministry of Economy, Trade and Industry

企業経営者の抱えている課題を解決するための施策

これまでの経緯

企業の情報セキュリティに関する制度等

- 2001年 情報セキュリティマネジメントシステム（ISMS）適合性評価制度」開始（(財)日本情報処理開発協会(JIPDEC)）
- 2003年 情報セキュリティ監査制度開始（NPO日本セキュリティ監査協会（JASA））
- 2005年 情報セキュリティ対策ベンチマークのサービス開始（（独）情報処理推進機構（IPA））
- 2008年 民間の情報セキュリティ格付機関設立

出典：IPA情報セキュリティ対策ベンチマーク（http://www.ipa.go.jp/security/benchmark/）

制度・規定・ガイダンス等

- 2001年 ISMS国際標準規格 ISO/IEC 17799:2000 に対応したISMS認証基準策定（JIPDEC）
- 2003年 情報セキュリティ管理基準、監査基準（経済産業省告示）
- 2005年 情報セキュリティ報告書モデル、事業継続計画（BCP）策定ガイドライン

（企業が公表した情報セキュリティ報告書の例）

- 2006年 財務報告書に係るＩＴ統制ガイダンス　（J-SOX対応版）
- 2008年 情報セキュリティ管理基準、監査基準（改正）、ITサービス継続ガイドライン
- 2009年 中小企業の情報セキュリティガイドライン（IPA）

事業継続計画（BCP）策定ガイドライン

情報セキュリティガバナンスの確立のための施策

経済産業省 Ministry of Economy, Trade and Industry

今回の取組

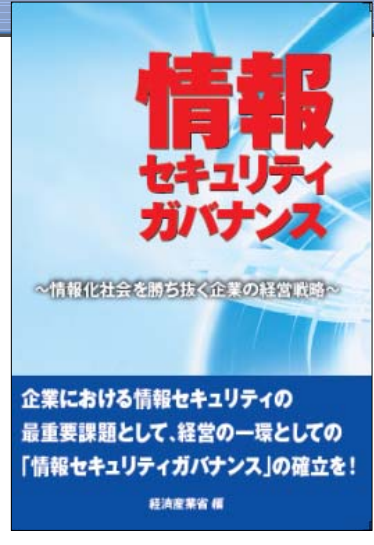
企業の情報セキュリティを確立する上で解決されていない課題（例）

（1）経営層が情報セキュリティの観点から何をすべきか不明確
（2）ＩＳＭＳを実装しようとしても法令との関係が分からない
（3）業務委託先での情報漏えい対策等の実施方策が分かりにくい
（4）実施状況の「見える化」のため信頼できる民間格付け機関が必要

課題に対応して今年策定したガイダンス類

（1）情報セキュリティガバナンス導入ガイダンス
（2）情報セキュリティ関連法令の要求事項集
（3）アウトソーシングに関する情報セキュリティ対策ガイドライン
（4）情報セキュリティ格付を実施する各種機関の運営に関する一般要求事項

企業のセキュリティガバナンスに関する一連のガイダンス類の普及展開フェーズへ



（参考）情報セキュリティガバナンス関連施策の全体像

経済産業省 Ministry of Economy, Trade and Industry

目的／担当	機密性の確保（情報漏洩対策等）	完全性の確保（情報改ざん対策等）	可用性の確保
経営者	情報セキュリティガバナンス導入ガイダンス（＊１） 情報セキュリティの観点からガバナンスの仕組みを構築・運用		
	情報セキュリティ報告書モデル（2005年）		
管理者	情報セキュリティマネジメントシステムの国際標準（ISMS）（2001年～） 自社の情報セキュリティ対策の適正な改善メカニズム（PDCAサイクル）の構築		
	情報セキュリティ関連法令の要求事項集（＊２） 情報セキュリティ対策に必要な法令を遵守するための情報提供		
		情報セキュリティ対策ベンチマーク（2005年）	
	アウトソーシングに関する情報セキュリティ対策ガイダンス（＊３）	財務報告に係るIT統制ガイダンス（2006年）	事業継続計画（ＢＣＰ）策定ガイドライン（2005年）、ITサービス継続ガイドライン（2007年）
外部機関	情報セキュリティ監査（2003年）等		
	情報セキュリティ格付（情報セキュリティ格付を実施する各種機関の運営に関する一般要求事項（＊４））		

（1）経営層が情報セキュリティの観点から何をすべきか不明確

（2）ISMSを実装しようとしても法令との関係が分からない

（3）業務委託先での情報漏えい対策等の実施方策が分かりにくい

（4）企業の情報セキュリティ対策実施状況の「見える化」が不十分

（＊ 今回策定した文書、（１）～（４）企業経営者の抱える課題）

（2）情報セキュリティ関連法令の要求事項集

経済産業省 Ministry of Economy, Trade and Industry

策定の背景

- 個人情報保護法や金融商品取引法等の法令からも情報セキュリティ対策の実施が要求。
- 企業の情報セキュリティ対策担当はIT担当部署であることが多いが、必ずしも法制度に詳しいわけではないため、情報セキュリティ対策がコンプライアンスとの矛盾を引きおこすリスクが存在する
- しかし、情報セキュリティと法令遵守の関係についてまとめた文書は存在しない。

企業が情報セキュリティ対策を実施する際に、法令遵守上、注意が必要な要求事項を示し、企業において効率的・効果的な情報セキュリティ対策・法令遵守を後押しすることが必要

主な論点

- 会社法　内部統制と情報セキュリティの関係、情報セキュリティ体制の不備による経営者の責任
- 個人情報保護法　「情報セキュリティ対策」と個人情報保護法への対応の違い、委託時の委託元の責任
- 不正競争防止法　「秘密として管理」していたことが認められる要件
  従業員が作成、取得した秘密情報について、企業は営業秘密としての保護を受けられるか
- 労働法　従業員による情報セキュリティ事件・事故を防ぐために、雇用関係上、講じるべき措置
  従業員の電子メールの内容を企業がモニタリングする際の法的な留意点
  企業は従業員の私用メールを禁止する規程を設けることはできるか　等

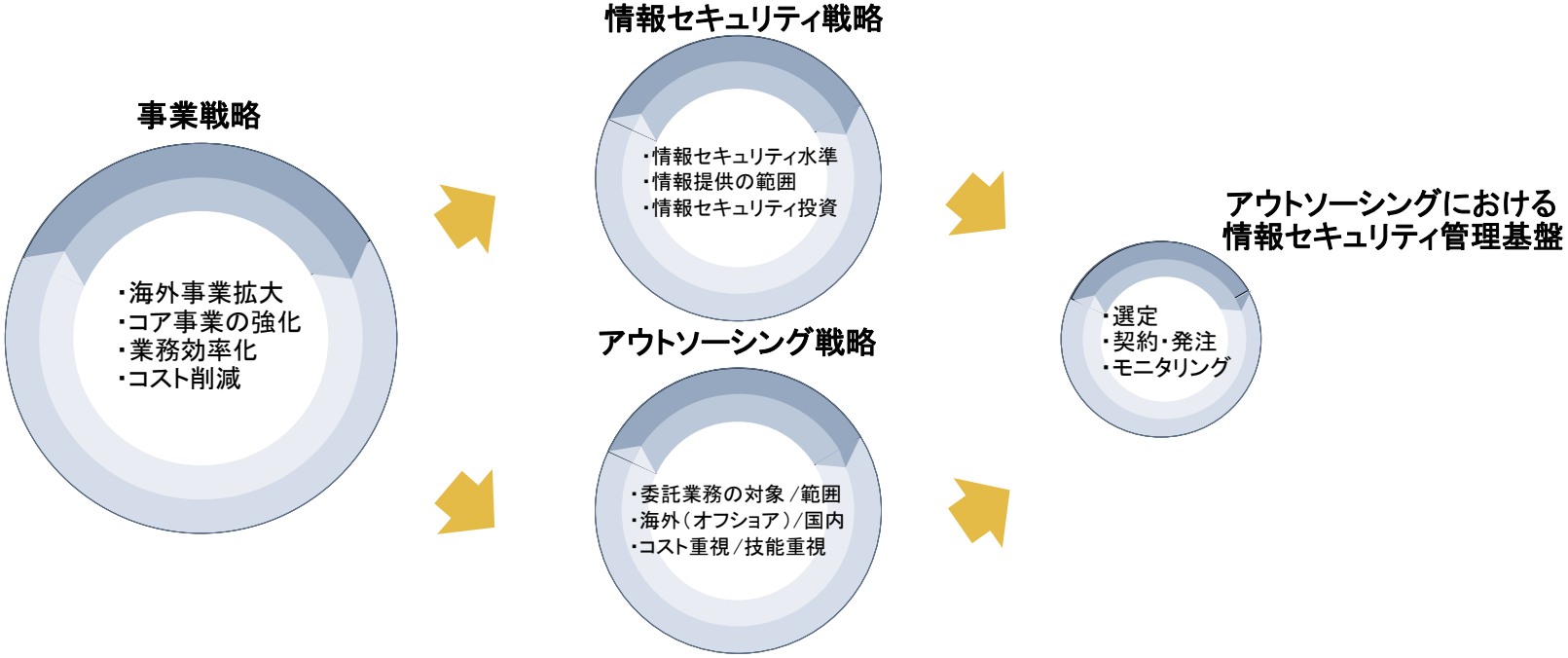
（3）アウトソーシングに関するガイダンス

経済産業省 Ministry of Economy, Trade and Industry

策定の背景

- 企業の管理が及びにくいアウトソーシング先において発生する事件・事故が多く報告
  - 個人情報の取り扱いにおける事故等の報告1,829件のうち704件、実に4割近くがアウトソーシング先、代理店、子会社、協力会社、提携先等で発生
- 企業活動のグローバル化の進展とともに、アジアを中心とした海外アウトソーシングの利用が拡大
  - 企業が保有する技術情報等を海外企業に預託する際の漏えいリスク等、新たな種類のリスクが発生
- しかしながら、情報セキュリティを単独で捉えるのではなく、事業戦略、アウトソーシング戦略との関係の中で考えることが重要

アウトソーシングに係るリスクを正しく把握し、情報セキュリティを十分に確保する手法を示し、情報漏えい等の事故の発生を抑制することが必要



（4）情報セキュリティ格付を実施機関の運営要求事項

経済産業省 Ministry of Economy, Trade and Industry

策定の背景

- 各企業が積極的に情報セキュリティ対策に取り組むためには「企業における情報セキュリティ対策の実施が当該企業の価値の向上につながるような市場メカニズムを働かせる」ことが必要
- 信頼性向上を目指した情報セキュリティの取組状況開示が有効だが、実施状況を詳細に公表することは、情報セキュリティ対策の問題点を明らかにしてしまう危険性がある

情報セキュリティ対策の詳細を明らかにせず、対策の実施状況のみを開示する方法として「情報セキュリティ格付け」が有効であり、その社会的位置付けを明確にし、格付け結果の公平性を担保するため「情報セキュリティ格付」に対する規律が必要

主な内容

- 民間組織による情報セキュリティ格付の信頼性を高めるために、情報セキュリティ格付機関において満たすべき行動規範的要件を多面的観点から整理・検証
- 海外の情報セキュリティ格付に関連する機関との連携等の可能性を踏まえ、必要に応じ国際標準の枠組みも視野に入れる

情報セキュリティガバナンス普及展開体制

経済産業省
Ministry of Economy, Trade and Industry

内閣官房 情報セキュリティセンター	経済産業省	（独）情報処理推進機構
政府全体の情報セキュリティ戦略である第二次情報セキュリティ基本計画に「企業の情報セキュリティ」位置付け	制度、ガイドライン等の整備	経済産業省が整備する各種ガイダンス類を具体的に適用するために必要な手順書を策定、中小企業への普及推進、情報セキュリティ対策ベンチマークの普及等（以下の団体等と適宜連携）

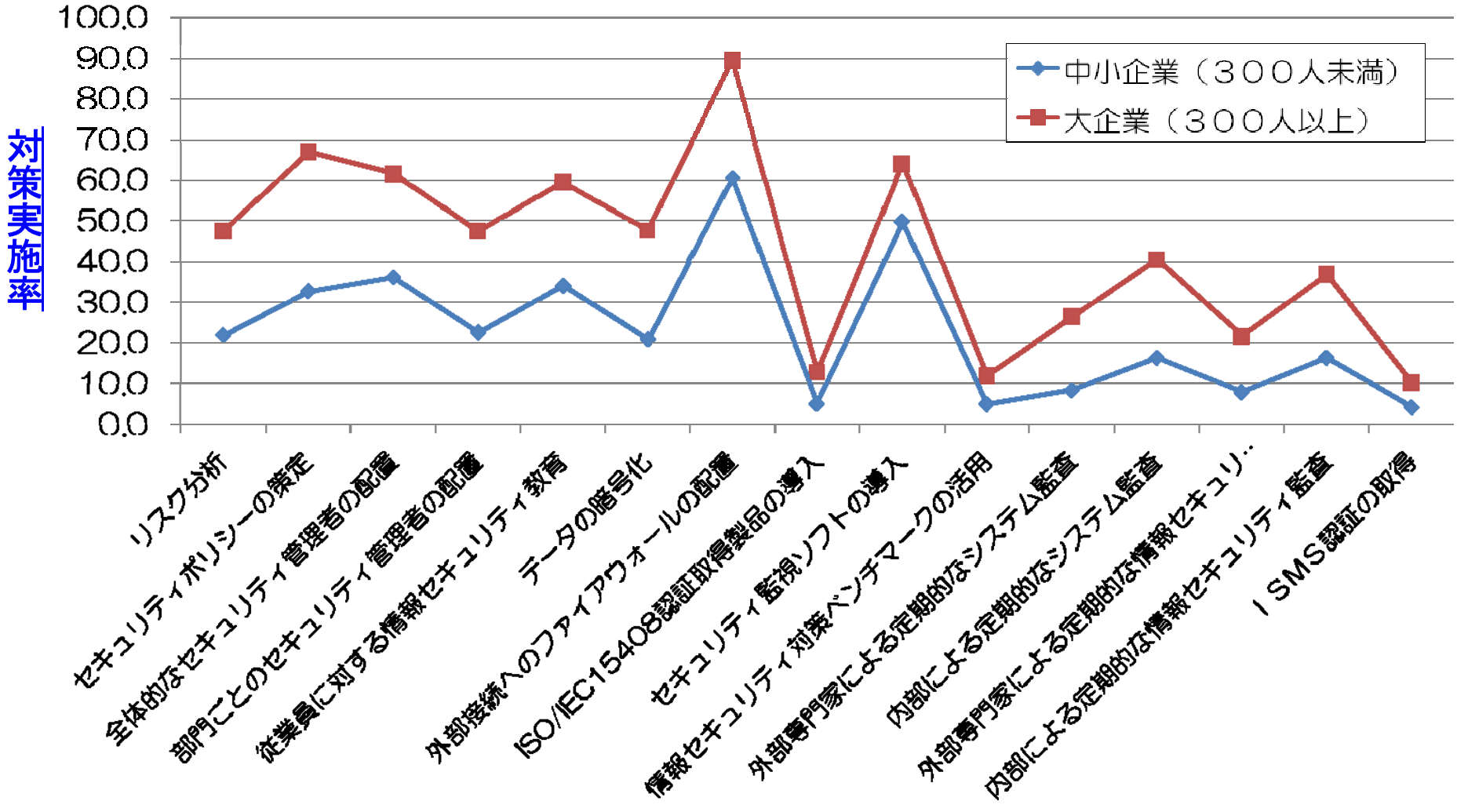
- 民間情報セキュリティ格付け機関
- 日本セキュリティ監査協会　等
- （財）日本情報処理開発協会
- ISO/IEC SC27（情報セキュリティ）
- 日本商工会議所 全国商工会連合会等

今後、企業全般に働きかけ

中小企業の情報セキュリティ対策の現状

経済産業省 Ministry of Economy, Trade and Industry

・　中小企業の情報セキュリティ対策は、大企業と比較して遅れている。



情報セキュリティ対策

経済産業省「平成20年情報処理実態調査」より

中小企業の情報セキュリティ対策促進事業

経済産業省 Ministry of Economy, Trade and Industry

スキーム

●全国の商工会議所の職員、商工会職員、全国中央会職員、エキスパートバンク登録者、ITコーディネータ、中小企業診断士等を対象とした情報セキュリティ研修を開催。

●各商工会議所の職員、商工会職員等は、情報セキュリティ対策に関する中小企業からの問い合わせに対応。

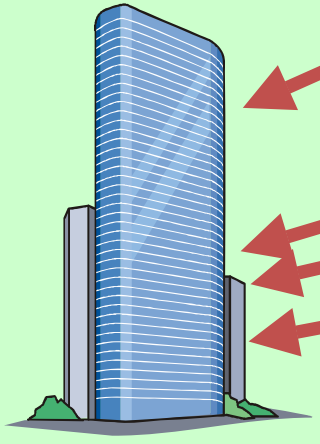
●エキスパートバンク登録者、ITコーディネータ、指導員等のITの専門家は、IT利活用の支援等を実施する際に、併せて情報セキュリティ対策の必要性について「気づき」をもたらし、中小企業の情報セキュリティ対策の実施を導く。

●また、各商工会議所職員、商工会職員、ITコーディネータ等が、助言を求めることを可能とするコールセンターを設置。

研修会の実施

●情報セキュリティ対策に係る知識と、中小企業へのアドバイス方法に関する研究プログラムを検討。

＜各商工会議所・商工会等＞

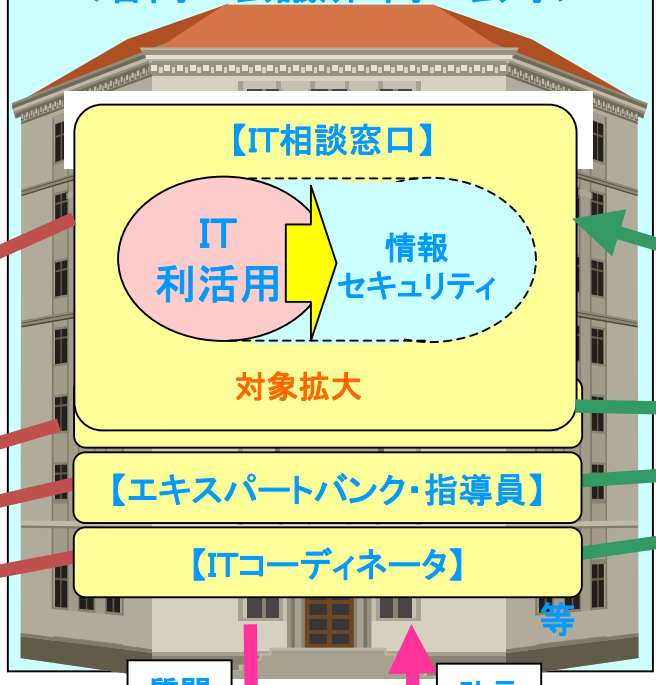


商工会議所・商工会・中央会等の職員

登録されたIT専門家

ITコーディネータ

＜各商工会議所・商工会等＞



質問

助言

IPA

＜情報セキュリティ指導に関する助言機関＞

中小企業へのアプローチ

中小企業からの情報セキュリティに関する相談に対応

情報セキュリティ対策の必要性について「気づき」をもたらす

＜中小企業＞

中小企業向け参考資料の活用

経済産業省 Ministry of Economy, Trade and Industry

- 情報セキュリティ対策のポイントを解説した各種資料を発行。
- 情報セキュリティに関する様々な脅威への対策を分かりやすく解説

- **中小企業向け情報セキュリティ対策リーフレット**
- **情報セキュリティ読本**
- **情報セキュリティ対策のしおりシリーズ**
- **CD-ROM すぐわかるウイルス対策の基礎知識**
- **知っていますか？脆弱性（ぜいじゃくせい）**
- **安全なウェブサイト運営入門**

中小企業の情報セキュリティ対策の底上げ

経済産業省 Ministry of Economy, Trade and Industry

- 何をするべきかを明確にするための「5分で出来る自己診断シート」の配付
- 企業の競争力強化の資する情報セキュリティ対策

経済産業省の情報セキュリティ対策（概要）

経済産業省
Ministry of Economy, Trade and Industry
METI

継続的な
普及広報活動

企業等

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

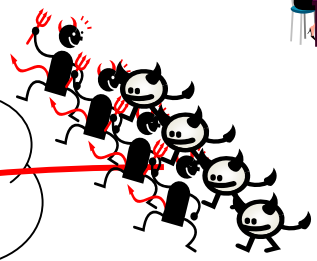
内部不正、
システム設定ミス等

サーバー

ルーター

インターネット

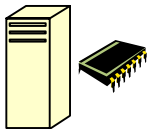
ウイルス、
不正アクセス等



個人

PC

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

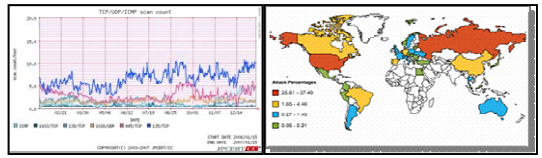
技術開発・研究開発の実施

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



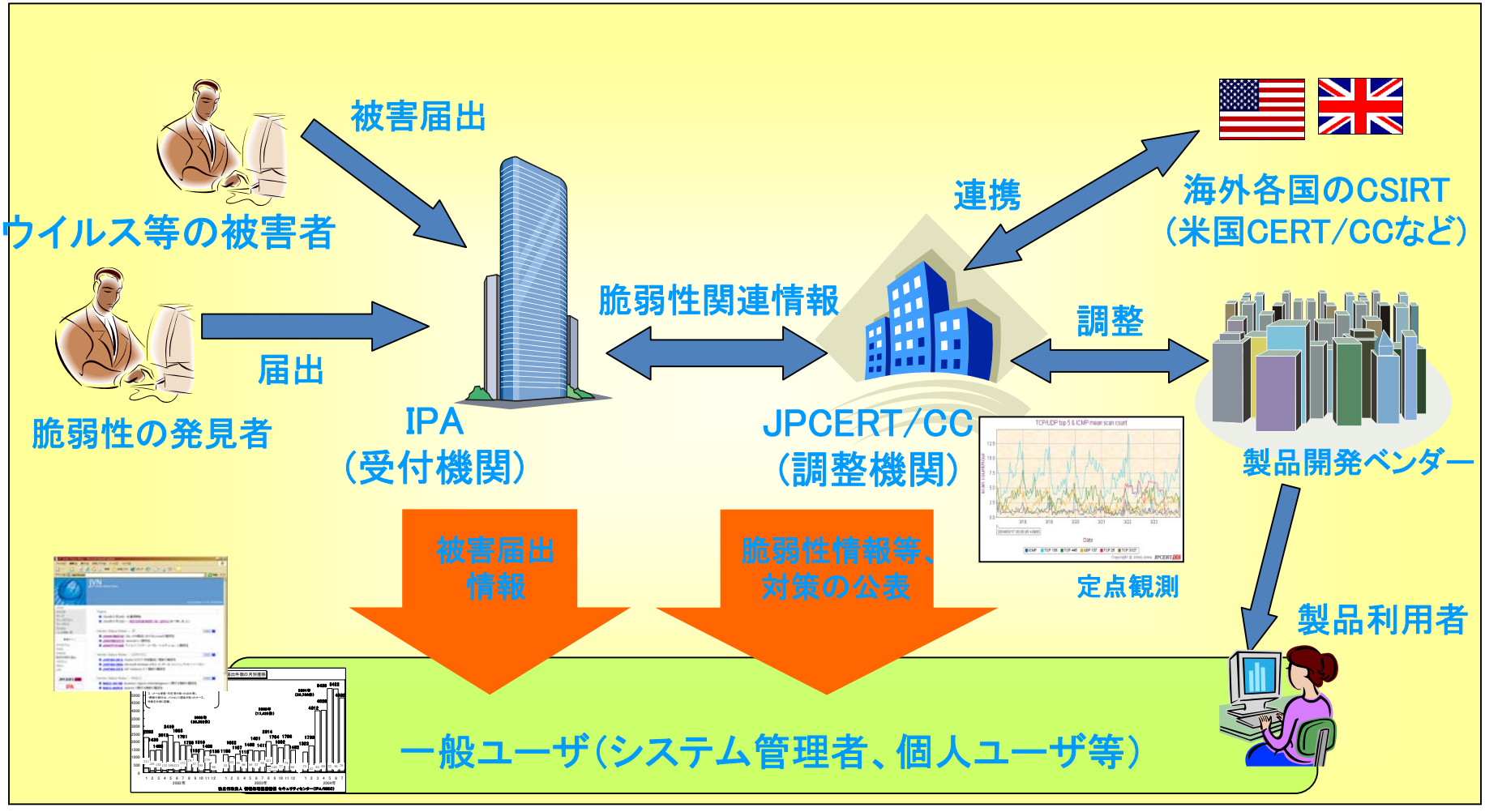
コンピュータセキュリティ早期警戒体制の整備

～コンピュータセキュリティ早期警戒体制の整備・運用～

経済産業省 Ministry of Economy, Trade and Industry

- 関係機関の効果的な連携により、情報セキュリ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3年11ヶ月で2,323件を受領（本年6月30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。



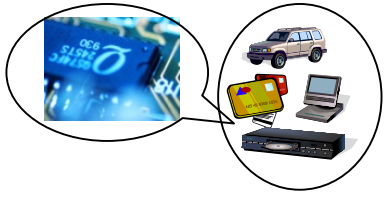
システムLSIセキュリティ評価体制の構築

経済産業省 Ministry of Economy, Trade and Industry

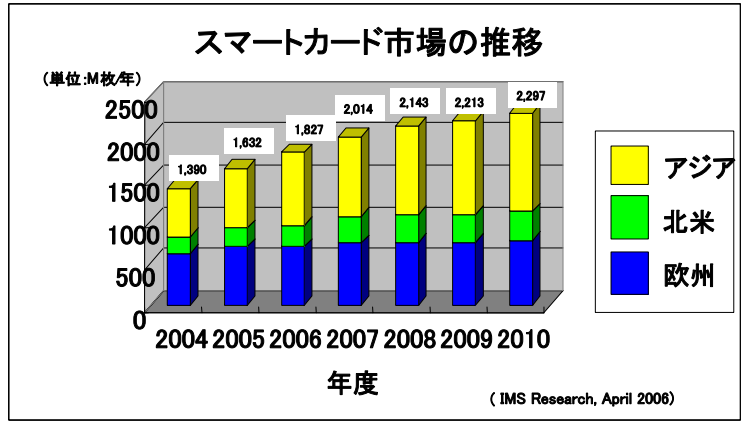
システムLSIのセキュリティ評価に関する現状

○ 国際的に組込システムの心臓部であるシステムLSIチップのセキュリティ評価はISO/IEC15408ベース

○ 現状、セキュリティ評価は、欧州が独占状態にあり、LSIチップの評価方法は、欧州の協議体の話合いで実質的に内容（どの程度の脅威への対抗が必要か）を決定。



注：スマートカードはセキュリティ機能を有するシステムLSIカード。キャッシュカード、クレジットカード、B-CASカードなどがこのカテゴリー



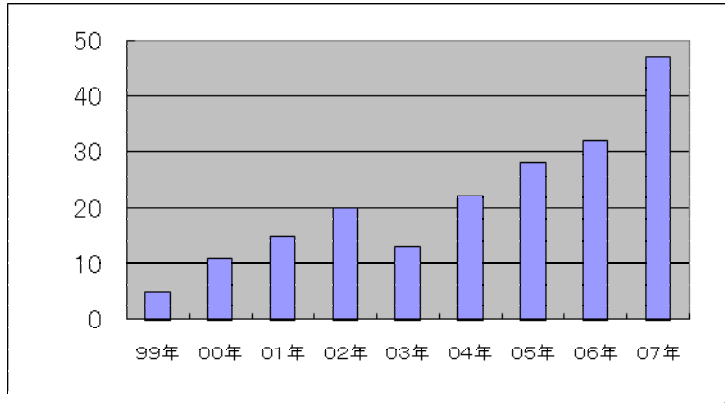
国内企業の動向

○ セキュリティ機能を有するシステムLSIチップの評価は、市場競争上、信用力のある欧州でのセキュリティ評価・認証を利用

○ 「どの程度の脅威への対抗が必要か」について共通認識が不足し、欧州での評価で不合格、再設計が要求
→市場投入の遅れ、ロスの発生

○ 設計拠点を欧州に移転せざるを得ない状況に追い込まれる可能性

スマートカードに関するCC認証件数（すべて欧州）

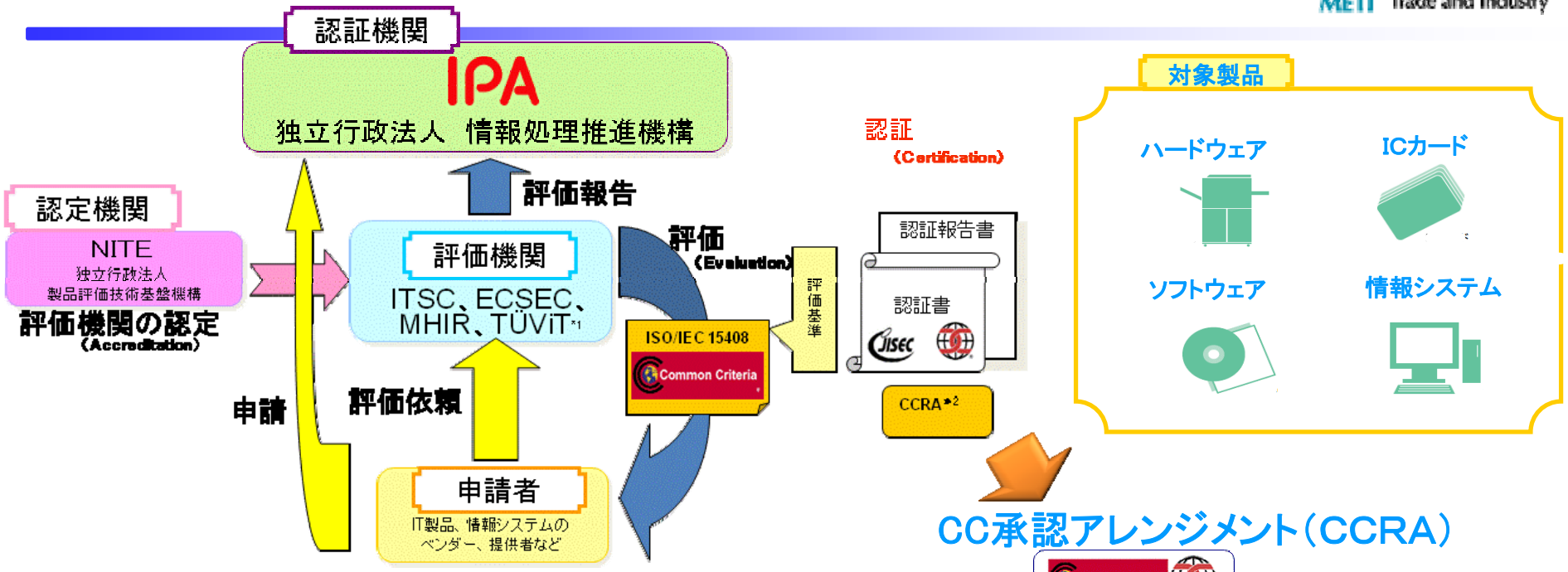


目　標

○平成23年度末までに、国際競争力のある、システムLSIチップの評価認証体制を構築し、国内で、システムLSIチップのセキュリティ評価を可能にする。
○具体的にはセキュリティ評価技術の開発及びテストセンターの整備等を行う。

（参考）ITセキュリティ評価・認証制度

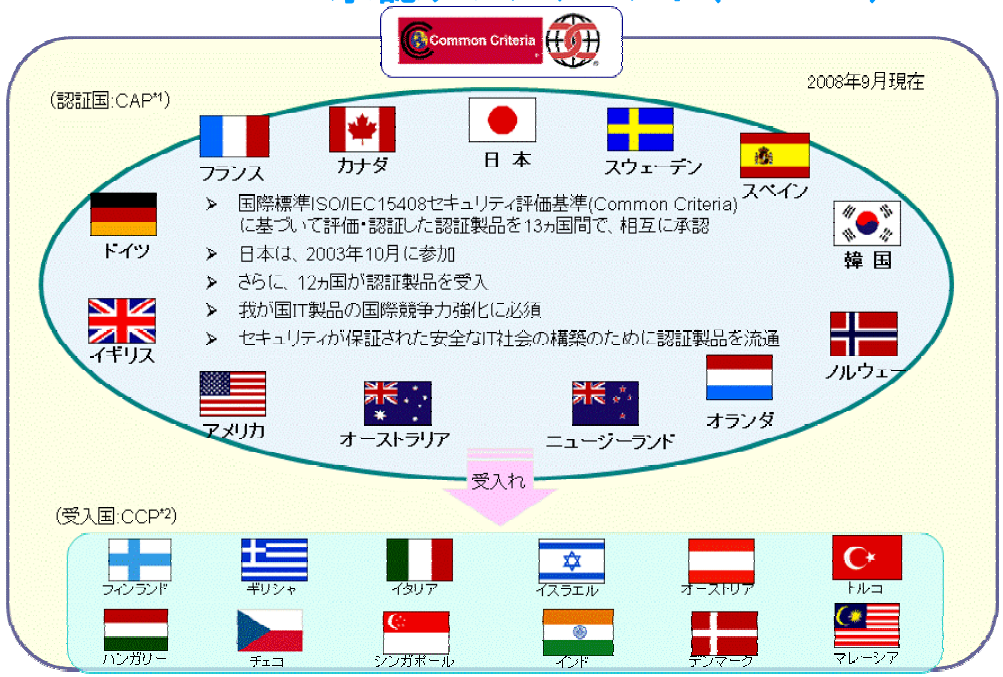
経済産業省 Ministry of Economy, Trade and Industry



*1　ITSC：有限責任中間法人ITセキュリティセンター
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
TÜViT：TÜV Informationstechnik GmbH

*2　Common Criteria Recognition Arrangement、国際相互承認協定

CC承認アレンジメント（CCRA）



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

経済産業省の主な普及広報活動

経済産業省 Ministry of Economy, Trade and Industry

www.youtube.com/user/metichannel

	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	JNSA Japan Network Security Association	JIPDEC Japan information processing Development Corporation
取組	○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。		
対象	企業で情報システムに携わる人々	一般のインターネット、PCの利用者	大学生、高校生等若年層（将来のIT業界を担う人材）

今後の進むべき方向性

課題は、ある！

ご清聴ありがとうございました。

セキュリティ施策についてのご意見・ご質問は・・・・

経済産業省商務情報政策局情報セキュリティ政策室
03－3501－1511（代表）
http://www.meti.go.jp/