経済産業省の
情報セキュリティ政策

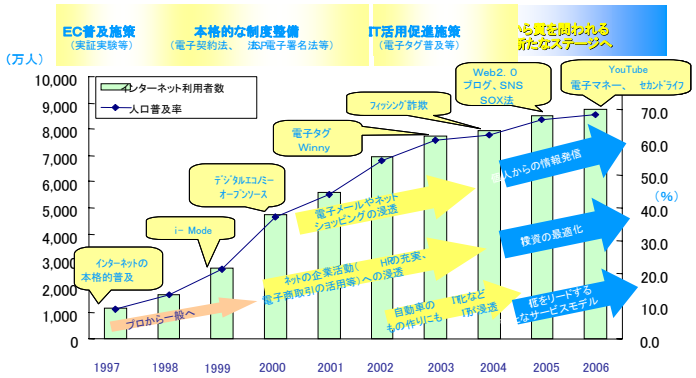
平成２２年７月
商務情報政策局
情報セキュリティ政策室

IT化の急速な進展

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：情報の爆発的増大と情報ネットワークの世界的広がり

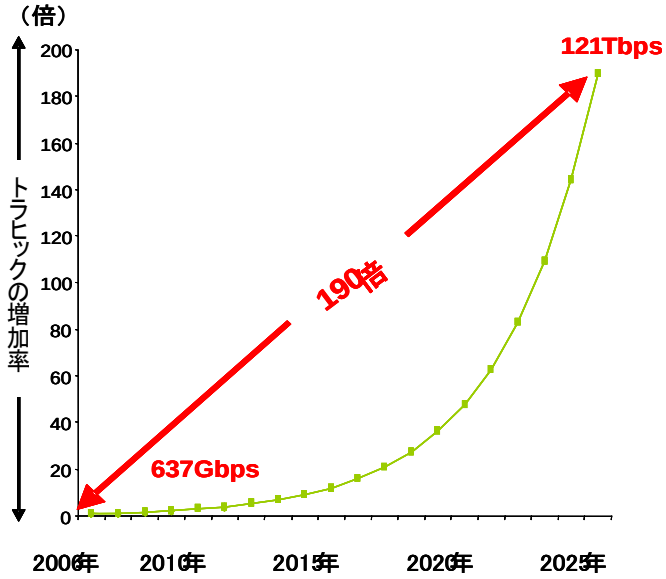
インターネットの人口普及率は、この10年で1割から7割へと着実に増加。
その普及に合わせて、ネットショッピングの普及、企業のネット活動の充実、自動車のIT化などモノ作りにもITが浸透するなど、個人・企業の双方においてITの活用が拡大。



（出典：経済産業省 産業構造審議会情報経済分科会資料（平成20年5月））

参考：インターネット内の情報流通量の推計（2006－2025）

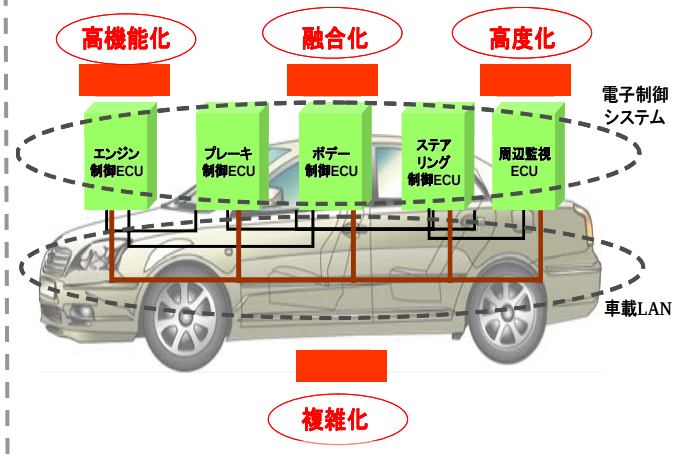
本格的なIT化に伴い、動画像の送配信や各種ITサービスが普及し、社会で扱う情報量は2025年には約200倍になると見込まれている（情報爆発）。

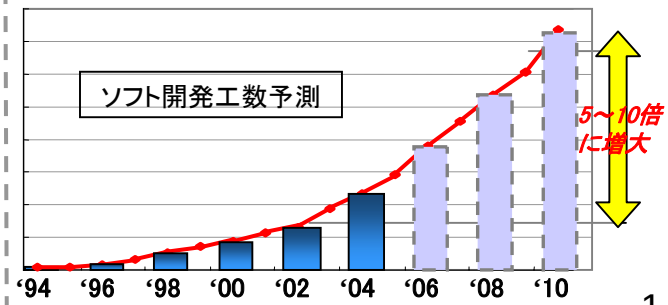


（出典：経済産業省 産業構造審議会情報経済分科会資料（平成20年5月））

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

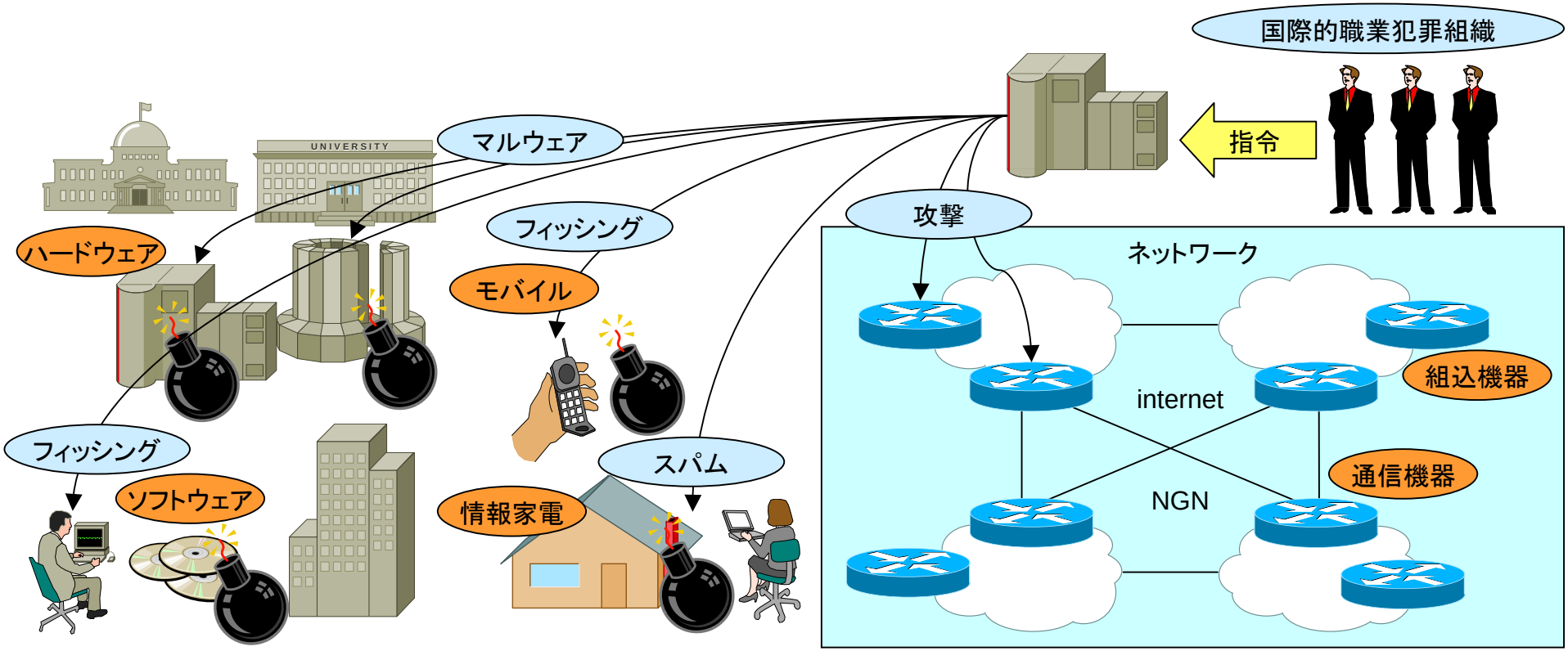
情報システムに関する脅威の構造

経済産業省
Ministry of Economy, Trade and Industry

- 経済システムと情報システムが密接にからみあうことで、リスクがどこにあるのか、どれくらいあるのか、識別・評価が極めて困難になっている
- 情報窃盗、マルウェア製造等の不正行為をビジネスとする職業犯罪組織の出現

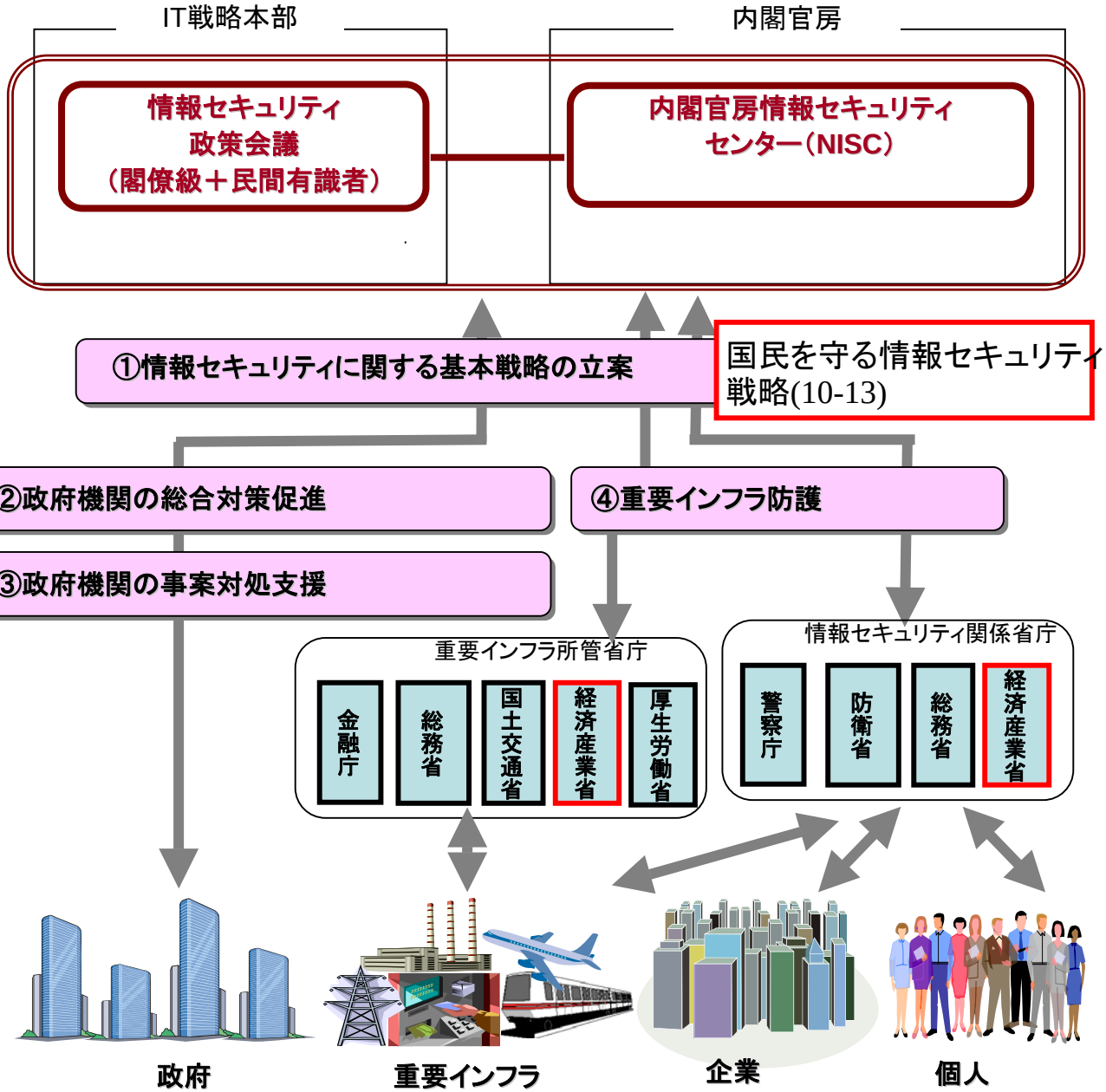
↓

- 思いつき、その場しのぎの情報セキュリティ対策を止め、システムの相互関係を分析し、効果的に弱点を補強する、総合的・根本的な情報セキュリティ対策が求められている



脅威：ボット、フィッシング詐欺、ID窃盗、スパムメール、ウェブ改ざん、暗号危殆化、分散サービス不能攻撃。

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～



- 「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。

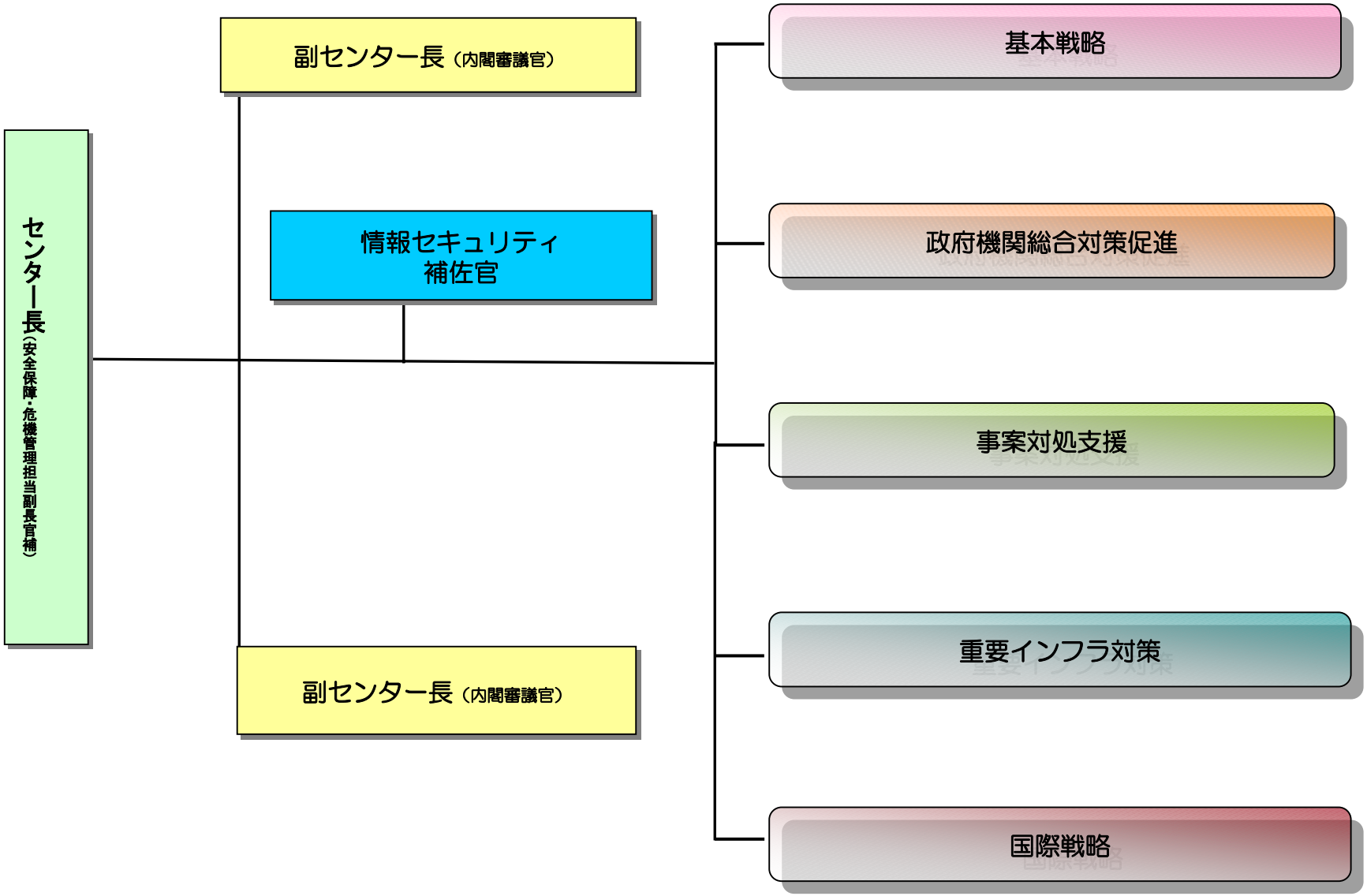
  2005年4月25日、内閣官房情報セキュリティセンター（NISC；National Information Security Center）を設置。

  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日に第１回を開催し、本年5月11日までに合計23回開催

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
小野寺 正　KDDI（株）代表取締役 社長兼会長
黒川 博昭　富士通（株）相談役
土屋 大洋　慶應義塾大学大学院准教授
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
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）

内閣官房情報セキュリティセンター(NISC)体制図＜全体像＞



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

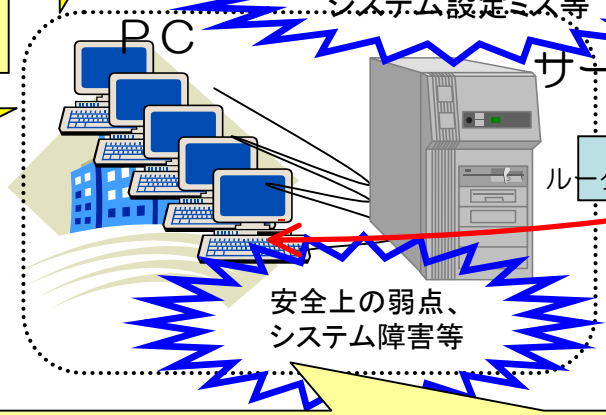
継続的な
普及広報活動

企業
（主に中小業）

個人

組織的対策の推進

内部脅威（従業員の不正・過失）による機密情報漏えい防止のためガイドライン策定等



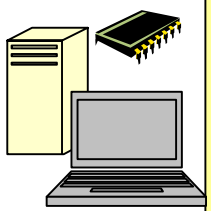
技術的対策の推進

セキュリティ評価の推進

IT製品等の安全性に係る評価認証制度による弱点の解消

技術開発の実施等

新たな脅威に対応する技術開発・研究開発、暗号対策



早期警戒体制の整備

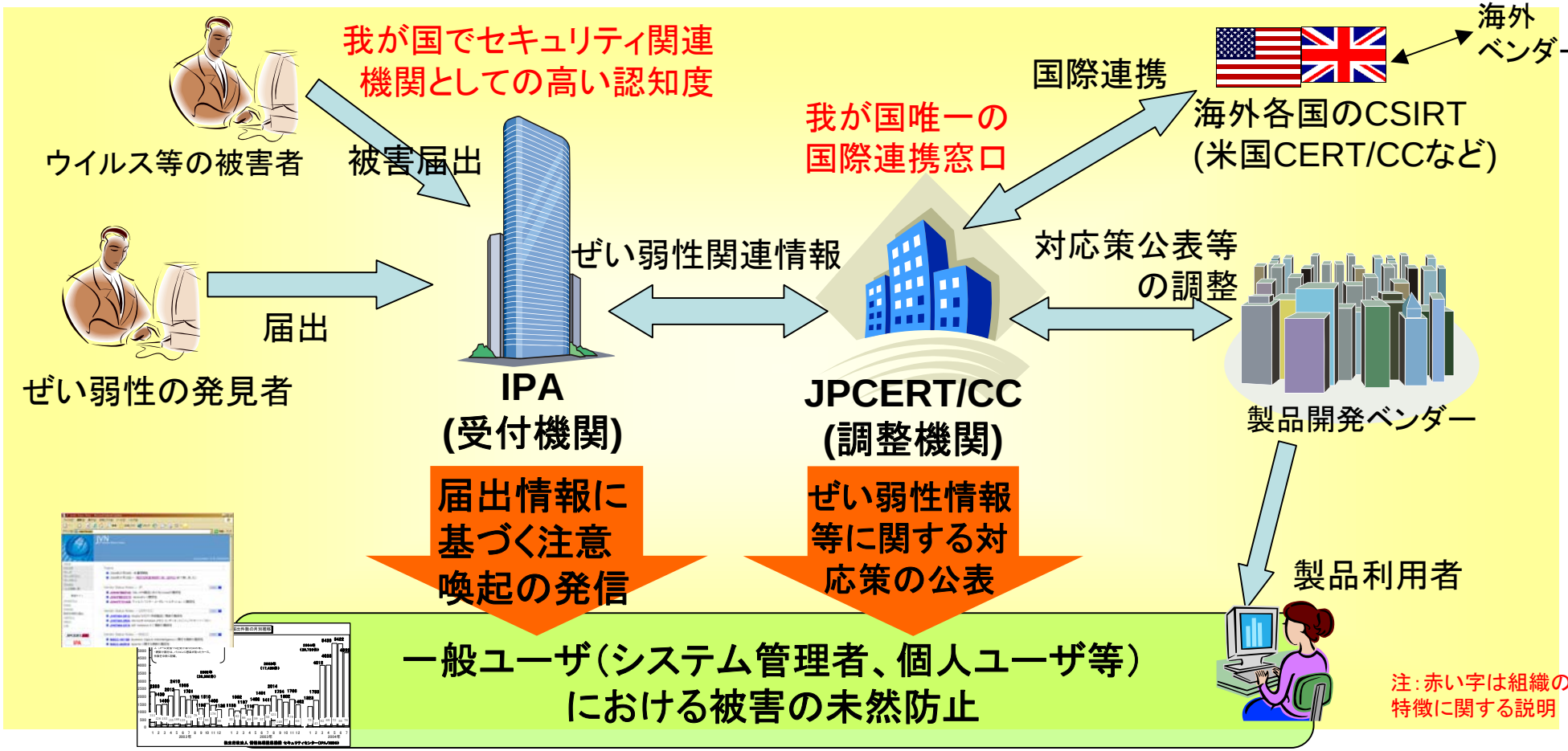
外部脅威（新しいウイルス、不正アクセス等）に関する情報を早期に収集・分析し、対策情報等を迅速提供（国際連携含む）。

コンピュータセキュリティ早期警戒体制の整備

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5年8月で6,148件を受領（2010年3月末現在）
- 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。



情報セキュリティに関する普及・啓発

経済産業省 Ministry of Economy, Trade and Industry

事業の概要

情報セキュリティに係る被害の防止、局限化を図るためには、一般利用者等もIT社会を構成する一員としての責任を自覚し、正しい知識と理解に基づきITを利用することが必要。そのため、コンピュータやインターネットを利用する一般利用者等の情報セキュリティリテラシーの向上を目的とした普及啓発活動を行う。

また、大企業と比較して遅れが見られる中小企業の情報セキュリティ対策レベルの向上を目指した指導事業を実施。

インターネット安全教室

家庭や学校からインターネットにアクセスする一般利用者（実際の参加者は10才台～80才台まで）を対象に、情報セキュリティに関する基礎知識を学習できるセミナーを全国各地で開催。また、平成20年度で終了した普及啓発活動「Check PC！キャンペーン」で作成したコンテンツを活用しつつ、インターネットを利用して情報セキュリティに関する基礎知識を常時学習できるサイトを運営。

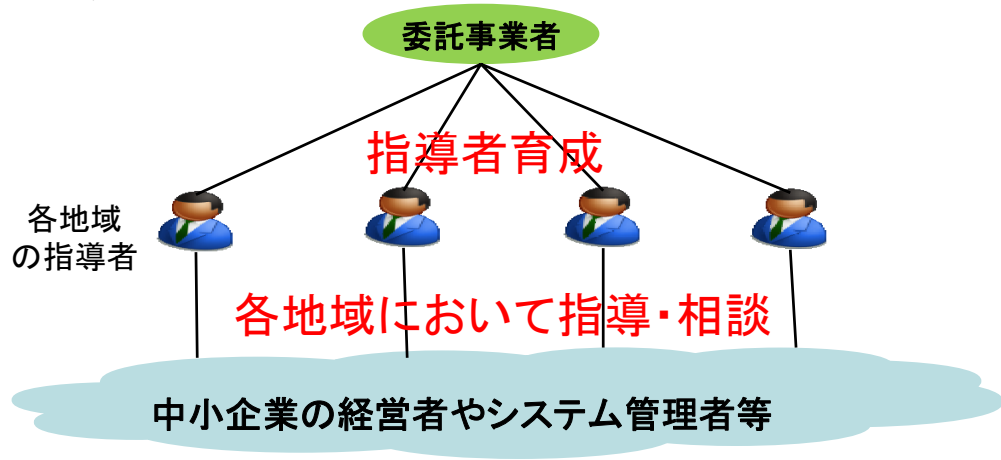
インターネットを新たに利用し始める人達への継続的啓発が必要

（参考）インターネットをここ1年半の間に利用開始した人数は、推計160万人

※2009年度情報セキュリティの脅威に対する意識調査（IPA）、平成21年通信利用動向調査（総務省）より推計

中小企業情報セキュリティ指導事業

平成20年度から、全国各地の商工会議所に設けられた「エキスパートバンク」に登録されているIT専門家等に対してセミナー等を実施することにより、情報セキュリティ対策を促進するための知識等を習得、当該専門家等が中小企業に対して、身近な存在として直接指導・アドバイスを実施。平成21年度からは、、ITコーディネータ協会、商工会、商工会議所、全国中小企業団体、（社）中小企業診断協会とも連携。



大企業と比較して、依然として、遅れが見られ、中小企業の情報セキュリティ対策レベルの向上が必要。

組織的情報セキュリティ対策の促進

■ 情報セキュリティに係る事件・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。

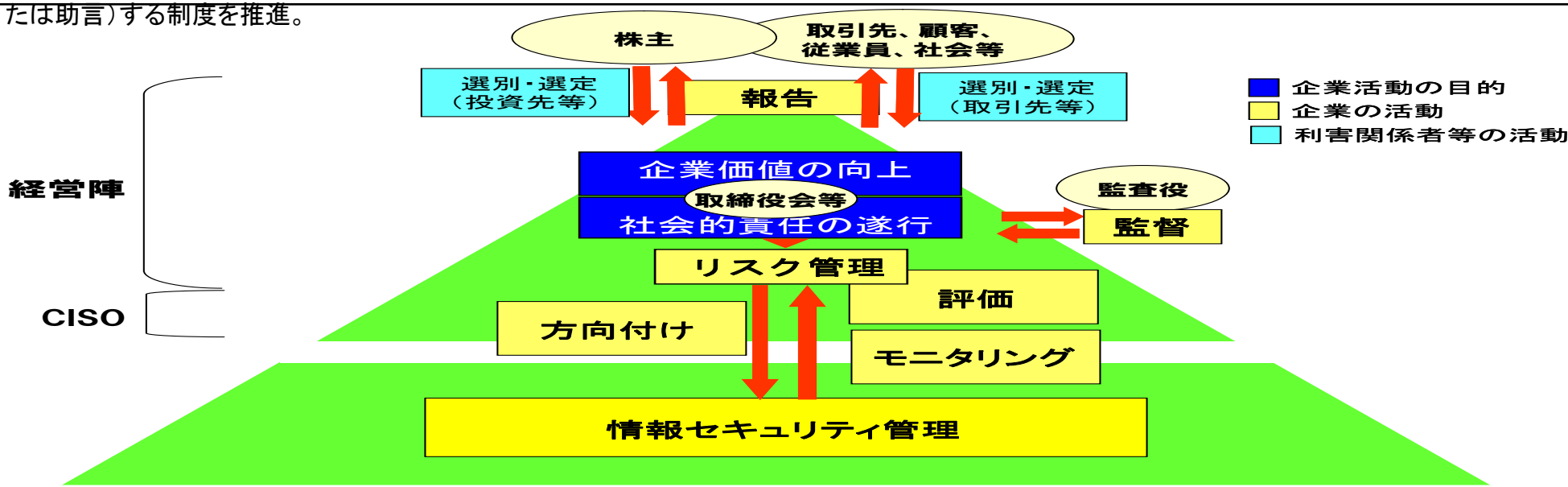
➢ **情報セキュリティガバナンスの確立：**

●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年より様々なツール等を活用して、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。

（参考）
＜平成21年＞
①情報セキュリティガバナンス導入ガイダンス：適正な情報セキュリティガバナンスを確立するために、経営陣が行うべき役割と効果について提示
②情報セキュリティ関連法令の要求事項集　：情報セキュリティ対策を実施する際の関連法令に関する考え方の提示
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ダンス：企業がアウト・ソーシングを検討する際の、アウト・ソーシング先に要求する対策等を提示
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：民間情報セキュリティ格付機関が満たすべき事項を提示

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。



「電子署名及び認証業務に関する法律」の概要

法律の概要

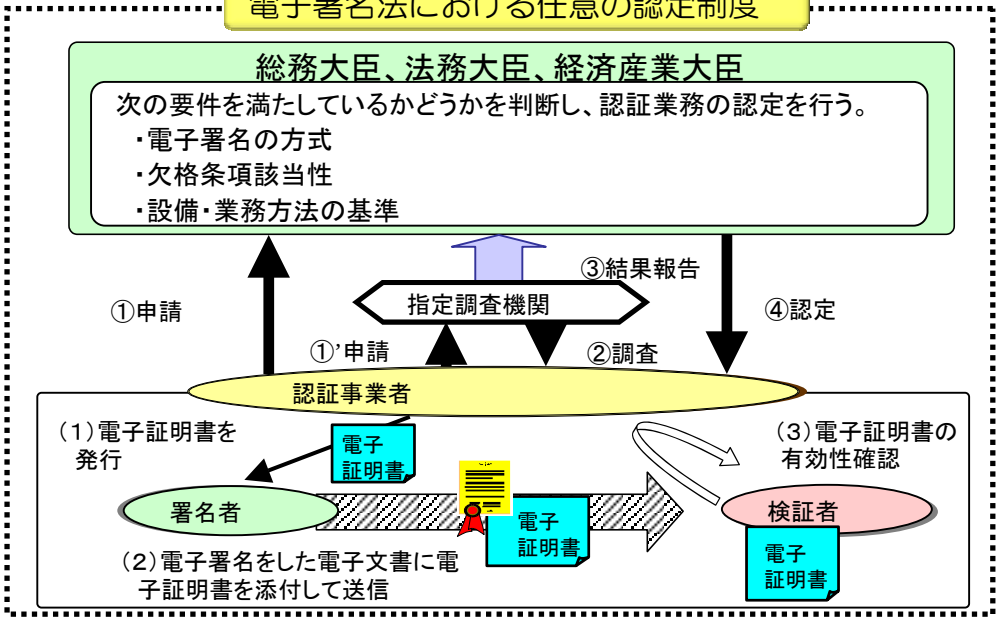
○主務大臣　：　総務大臣、法務大臣、経済産業大臣

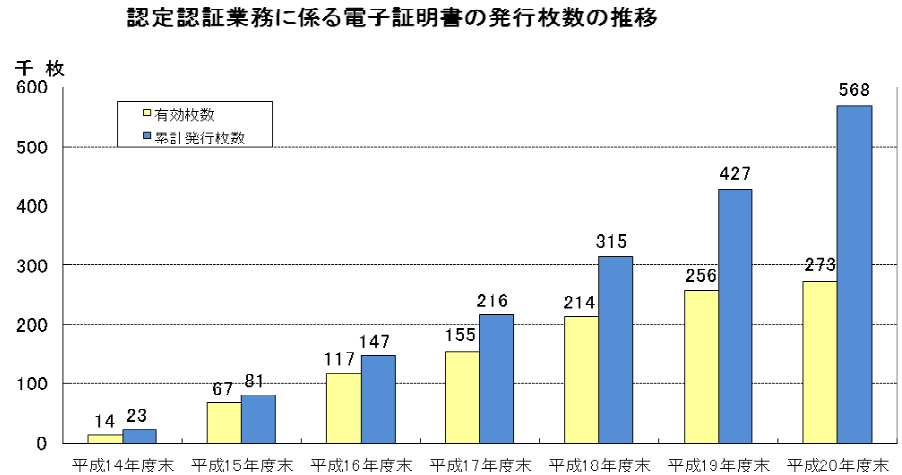
1. 電子署名の定義（第2条）
①当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
②当該情報について改変が行われていないかどうかを確認することができるものであること。

2. 電磁的記録の真正な成立の推定（第3条）
本人による一定の条件を満たす電子署名が付されている電子文書等の真正な成立の推定を規定。

3. 認定制度の創設
一定の要件を満たしている認証業務について認定を行う。

電子署名法における任意の認定制度





平成２２年度以降、必要となる措置の具体例

・認証局で使用する暗号アルゴリズムの移行に必要な制度的・技術的検討　　等