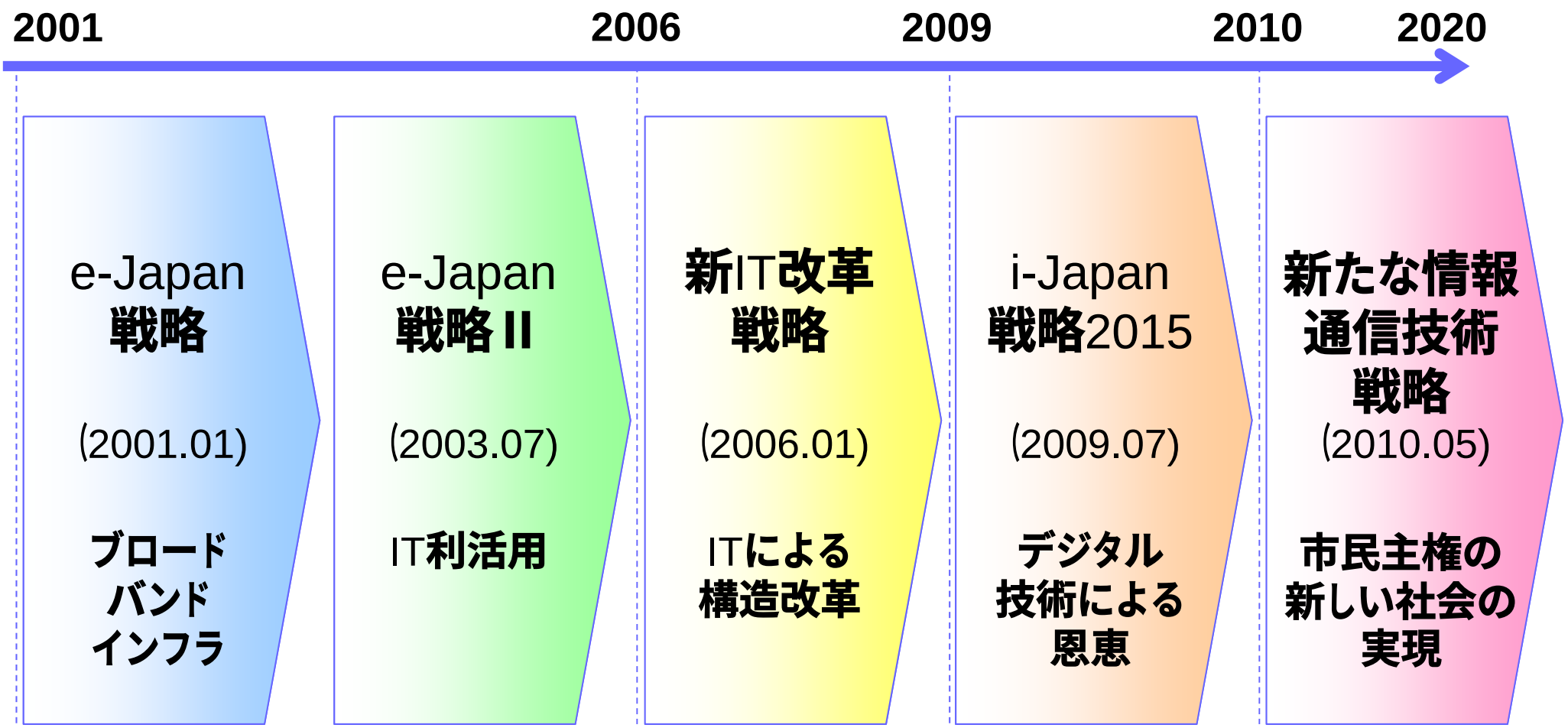
情報通信技術の新たな利活用と
サイバーセキュリティ

2013年2月1日

政府CIO
遠藤　紘一

今後の電子行政推進の方針

日本のIT戦略



情報インフラ等の整備に
ついては一定の成果

⇔

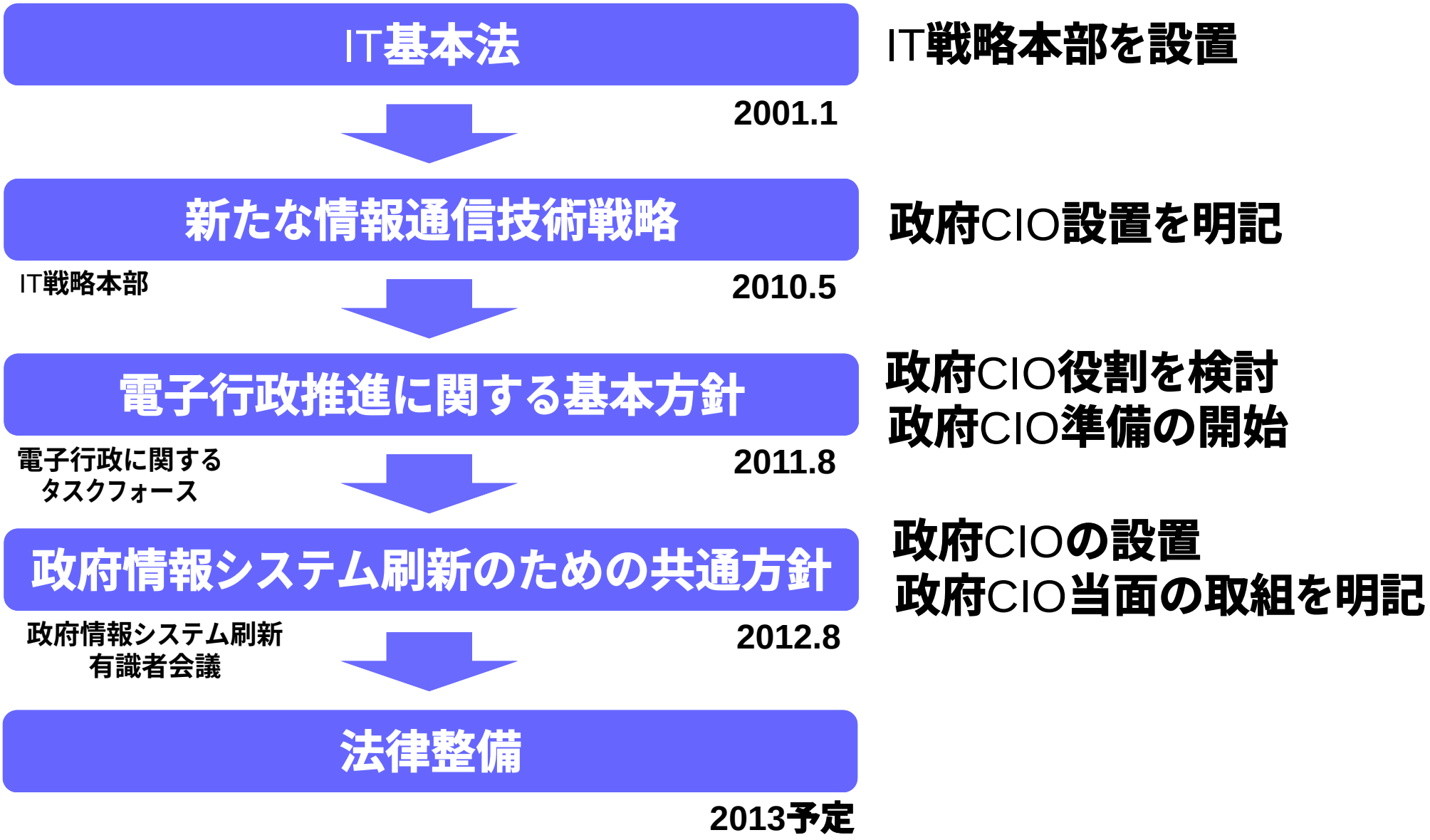
ITを活用した業務改革に
ついては課題が残存

電子行政の課題

- 現場の声の不足
  - 行政サービスのエンドユーザの声が聴けていない
  - 現場の職員がニーズなどを理解できていないことがある
- 可視化されていない
  - 分析・改善のための基礎情報が揃っていないことがある
- 縦割りの組織やシステム
  - 重複や組織間の連携ができていないものがある
    - 府省間、府省ー自治体、自治体ー自治体
- 専門家の不足

政府CIOによる一貫した戦略の推進

政府CIO設置に向けた取組



電子行政推進に関する基本方針

電子行政のこれまでの反省をもとに、今後の取り組みを整理。
その中核としての政府CIOを明記。

政府CIOの役割

- 電子行政に関する戦略等
  - 電子行政に関する戦略等について、明確かつ迅速な決定と責任の下、統率力・調整力をもって企画・立案・推進
  - オープンガバメント等、府省横断的に取り組むべき施策の推進
- 政府全体のIT投資の管理
  - 政府全体として、IT投資の全体最適を実現
- その他
  - 地方、民間との連携
  - IT人材の確保・育成、広報等

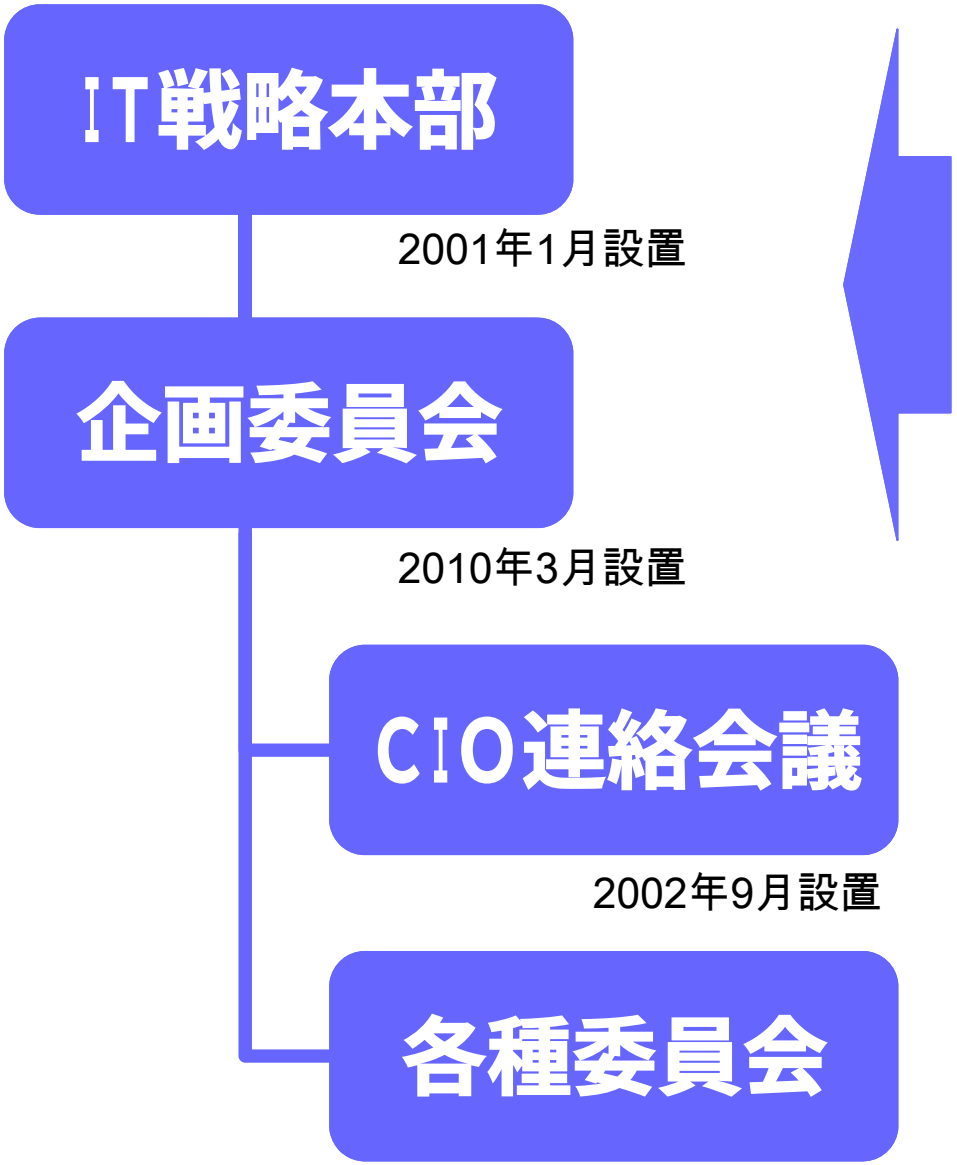
政府情報システム刷新のための共通方針(提言)

政府情報システムは行政運営の中核をなす基盤であり、行政を改革するエンジン

政府CIOの下、情報システムの刷新とITガバナンス強化を通じて、「ITを活用した行政機能向上とトータルコスト低減の両立」を目指す

政府CIOの設置を提言し、実現（2012年8月10日）

電子政府推進体制



2012年8月10日
政府CIO
政府CIO室

ＩＴ戦略本部の本部員は、
政府ＣＩＯに協力

視点

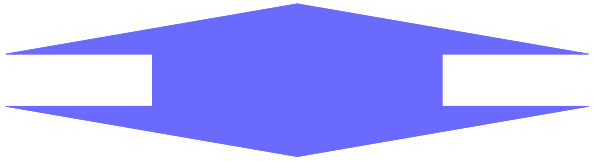
民間視点での改革を推進

利用者の視点

業務改革の視点

情報技術の視点

競争力の視点



電子行政

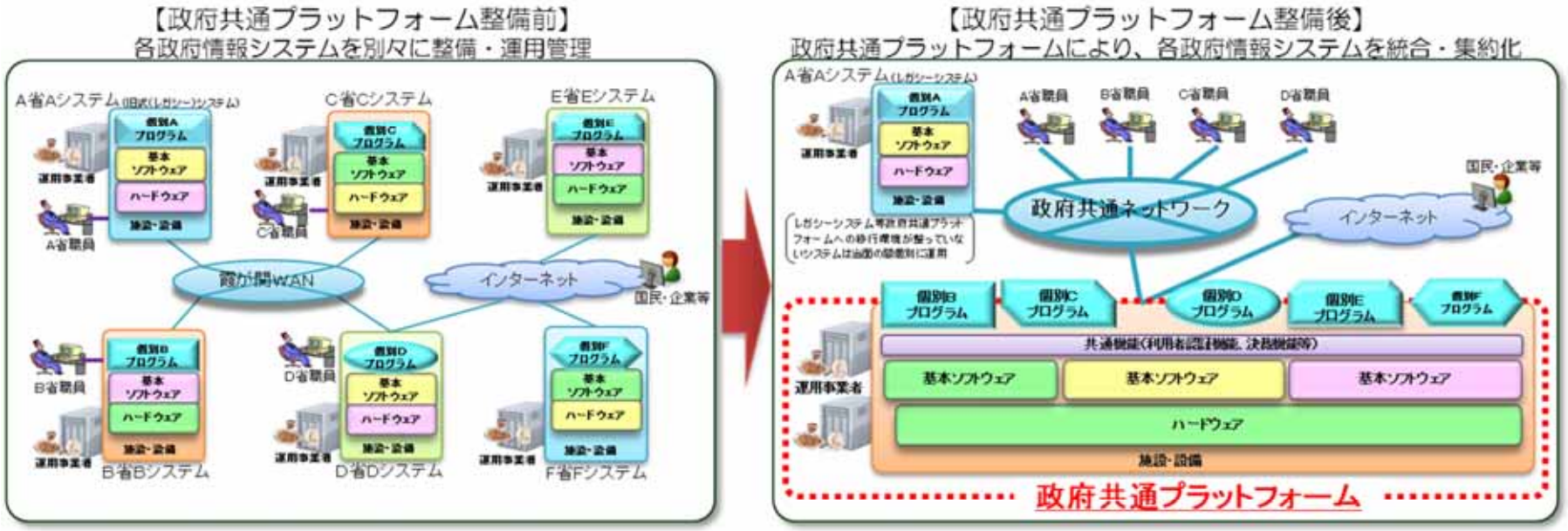
We are the change leaders !!

今年度の取組

- 政府横断での取組
  - 電子行政の戦略整備
  - 共通プラットフォームの構築
  - マイナンバー制度・企業コードの検討
  - 電子行政オープンデータ戦略の推進
- IT ガバナンス
  - 府省の中期計画の策定とレビュー
  - ゲートウェイレビューの試行
  - ガイドライン等の改定と整備
- 人材・体制
  - 政府CIO室の強化
  - CIO補佐官プール制の検討
- 外部機関との連携、広報
- 情報セキュリティ対策の推進

取組内容①　～政府共通プラットフォーム～

- 「新たな情報通信技術戦略」（H22.5.11高度情報通信ネットワーク社会推進戦略本部決定）に基づき整備。
- 現在各府省が別々に整備・運用している政府情報システムを可能なものから順次これに統合・集約化し、政府情報システム全体の運用コストの削減等を図る。
- 平成24年度中（25年3月）の運用開始を目指し、平成24年12月現在、テスト作業、運用管理規程案の策定作業等を実施中。



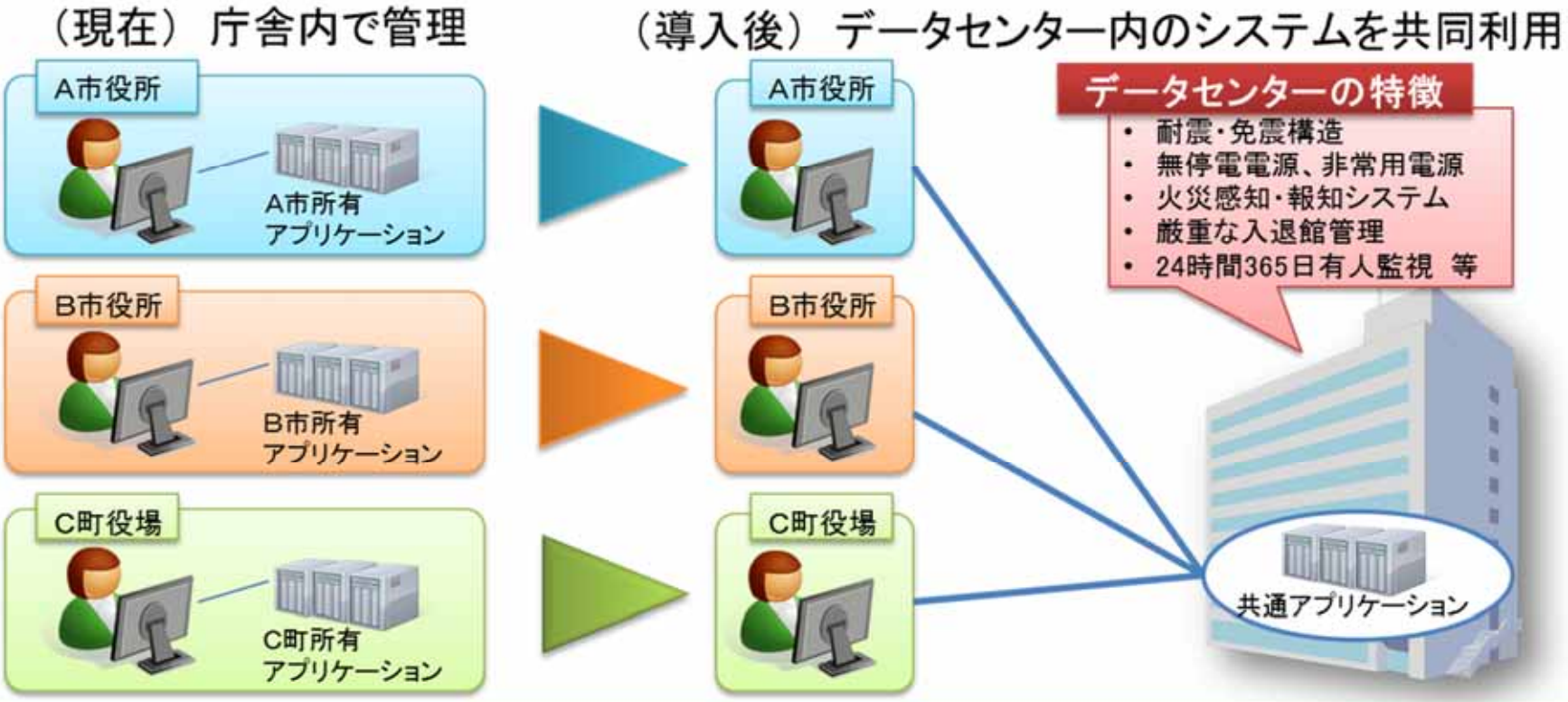
＜政府共通プラットフォームによる主な効果＞

- ハードウェア、通信ネットワーク等の共用
  ⇒　仮想化技術の活用等によるサーバマシン等ハードウェアの台数削減、通信ネットワークの多重敷設の削減
- ＯＳ・ミドルウェア等の基盤ソフトウェアの共通化
  ⇒　システム動作環境の標準化、ライセンス一括購入等による経費削減
- 運用管理の一元化
  ⇒　運用管理業務負担の軽減、外部委託システム運用要員の削減
- 共通的な機能の統一化
  ⇒　システム開発経費削減、共通的業務フローによる業務の標準化　　等

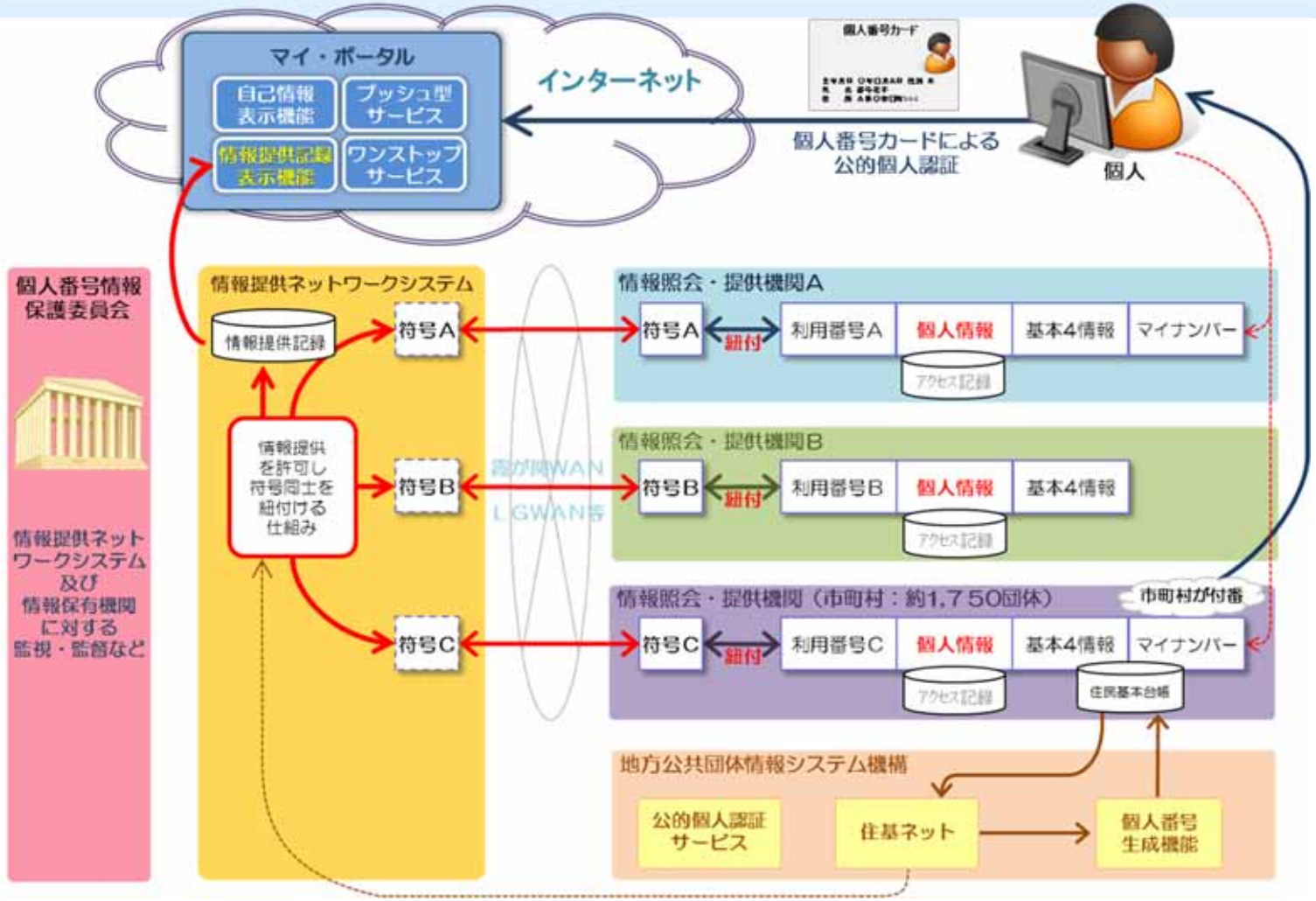
取組内容②　～自治体クラウド～

自治体クラウドとは

- 地方公共団体が情報システムを自分たちの庁舎で保有・管理することに代えて、外部のデータセンターにおいて保有・管理し、ネットワークを経由して利用できるようにする取組み
  ➡ 所有から利用へ
- 複数の地方公共団体の情報システム共同化による割り勘効果、災害に強い情報システムの構築等を実現　➡ 共同化・集約化



取組内容③　～番号制度～



システム間の連携を図るため、国民にナンバーを付ける番号制度を準備中

税と社会保障の情報連携等、国民に利便性の高いサービスの提供を目指すとともに、行政だけでなく抜本的な社会の効率化を目指す

まとめ

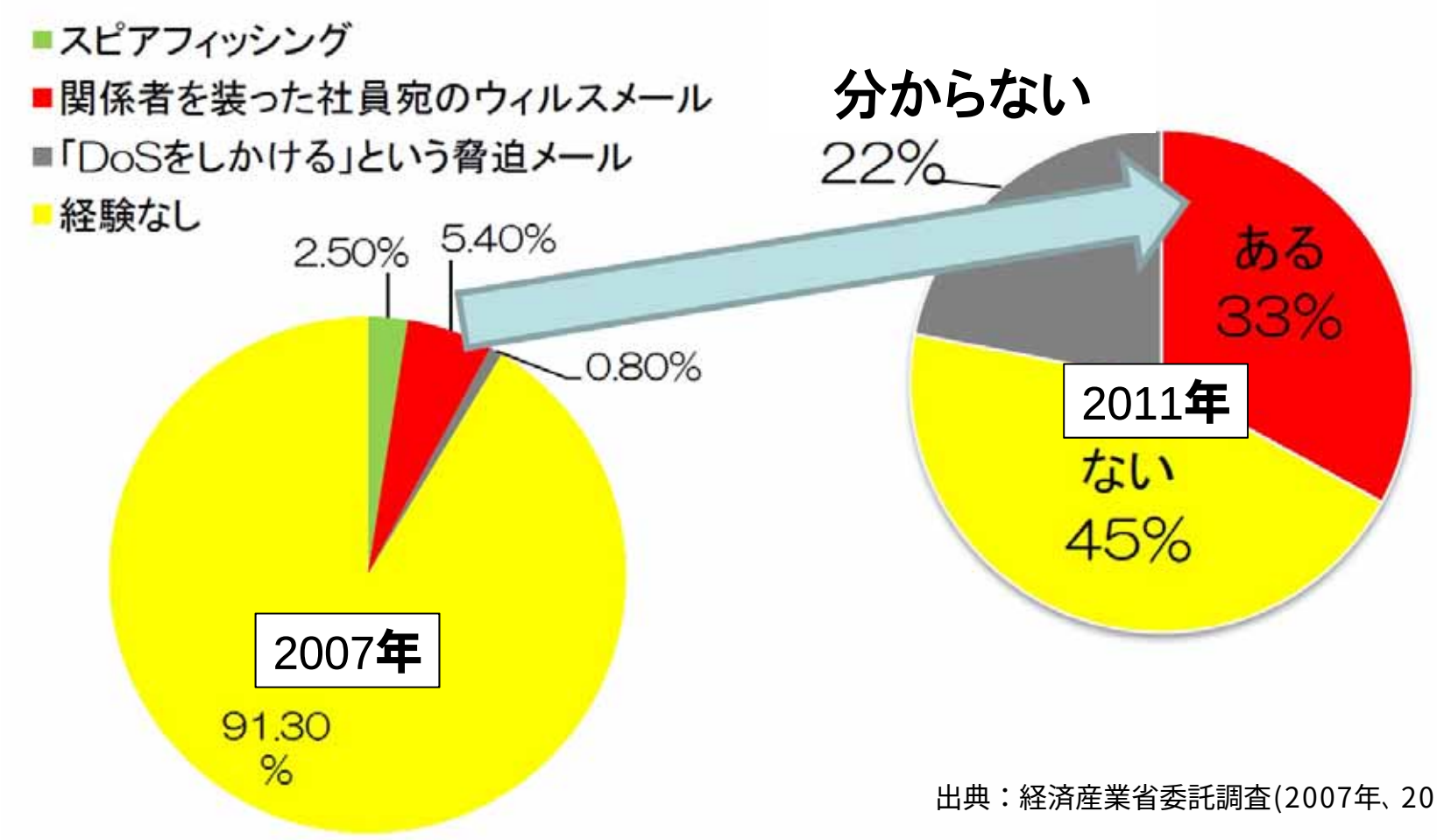
システム検討の前にやることがある。
業務の標準化と共通化である。

行政改革と情報システムという視点で、国民が成果を実感できる電子行政を目指して、関係の皆様とともに改革に取組んでいきたい。

サイバーセキュリティはなぜ大切か

最近のサイバー攻撃等（攻撃数）

標的型とみられるサイバー攻撃を受けたことがある（企業）
2007年 5.4% → 2011年 33%



出典：経済産業省委託調査(2007年、2011年)

最近の主なサイバー攻撃の事例

○　対策をとっていると思われている企業等も被害に遭遇
○　最近は情報漏えい事案が多い

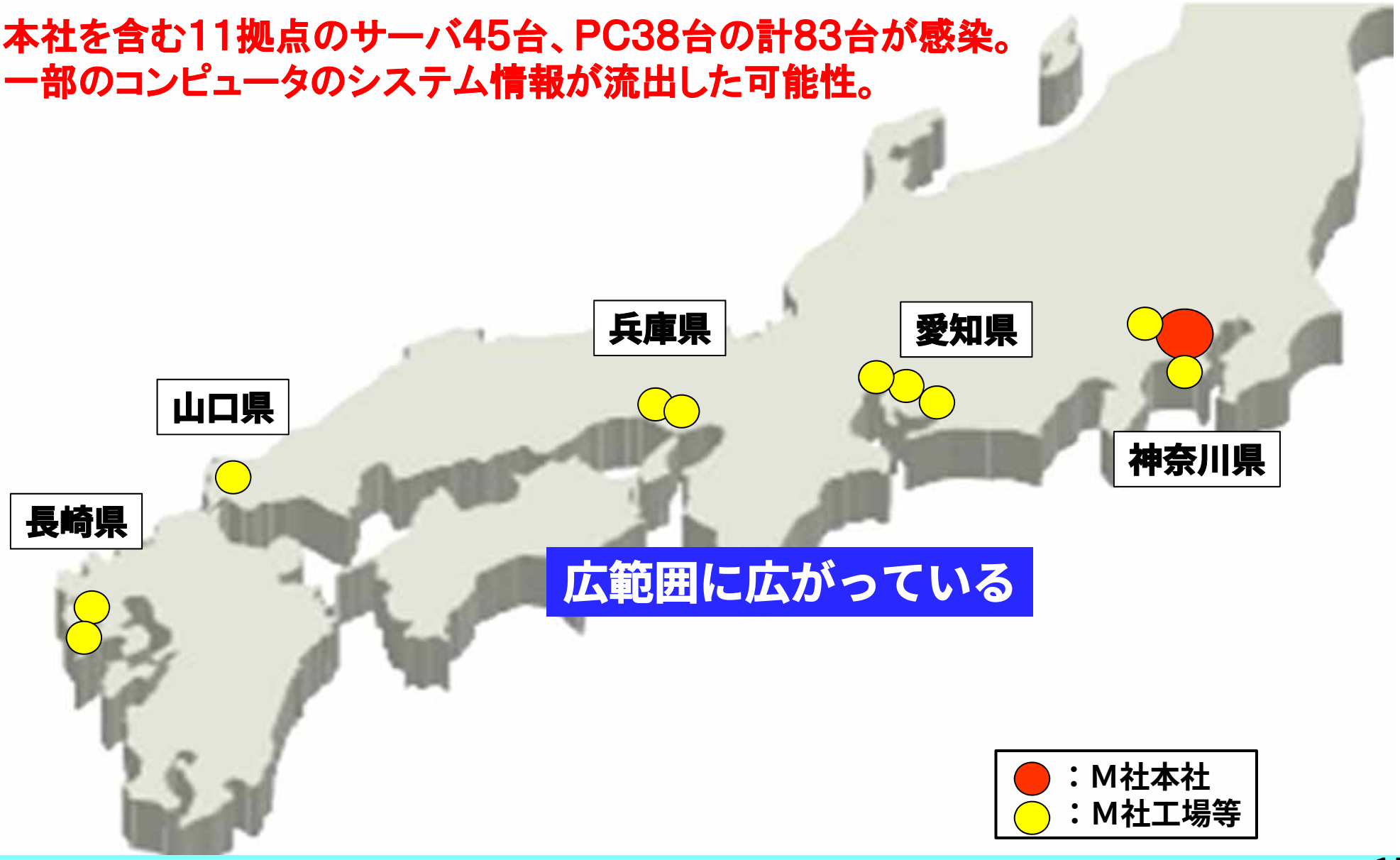
最近の主な事例

2009末	「ガンブラー攻撃」による**ウェブサイト改ざん**被害等が増加
2010．7	イランの原子力発電所への**スタックスネットによる攻撃**が判明 その後、ウラン濃縮施設への攻撃も判明し、**遠心分離機が全て停止**
2011．4	ソニー米国子会社のネットワークへの**不正侵入** 最大で7700万人分の**顧客情報が流出**
2011．9	三菱重工業、衆議院等への**標的型攻撃**によるウィルス感染発覚
2012．10	GhostShellを名乗るハッカーによる世界各国に100大学（日本の5大学を含む）への**不正アクセス及びネット上への情報掲載**
2012．11	JAXA（宇宙航空研究開発機構）における**ウイルス感染**及び**情報流出の可能性**
2012．12	JAEA（日本原子力研究開発機構）における**ウイルス感染**及び**情報流出の可能性**
2013．1．	農林水産省からの**TPP機密情報流出**に関する報道

※　本資料は報道ベースで作成

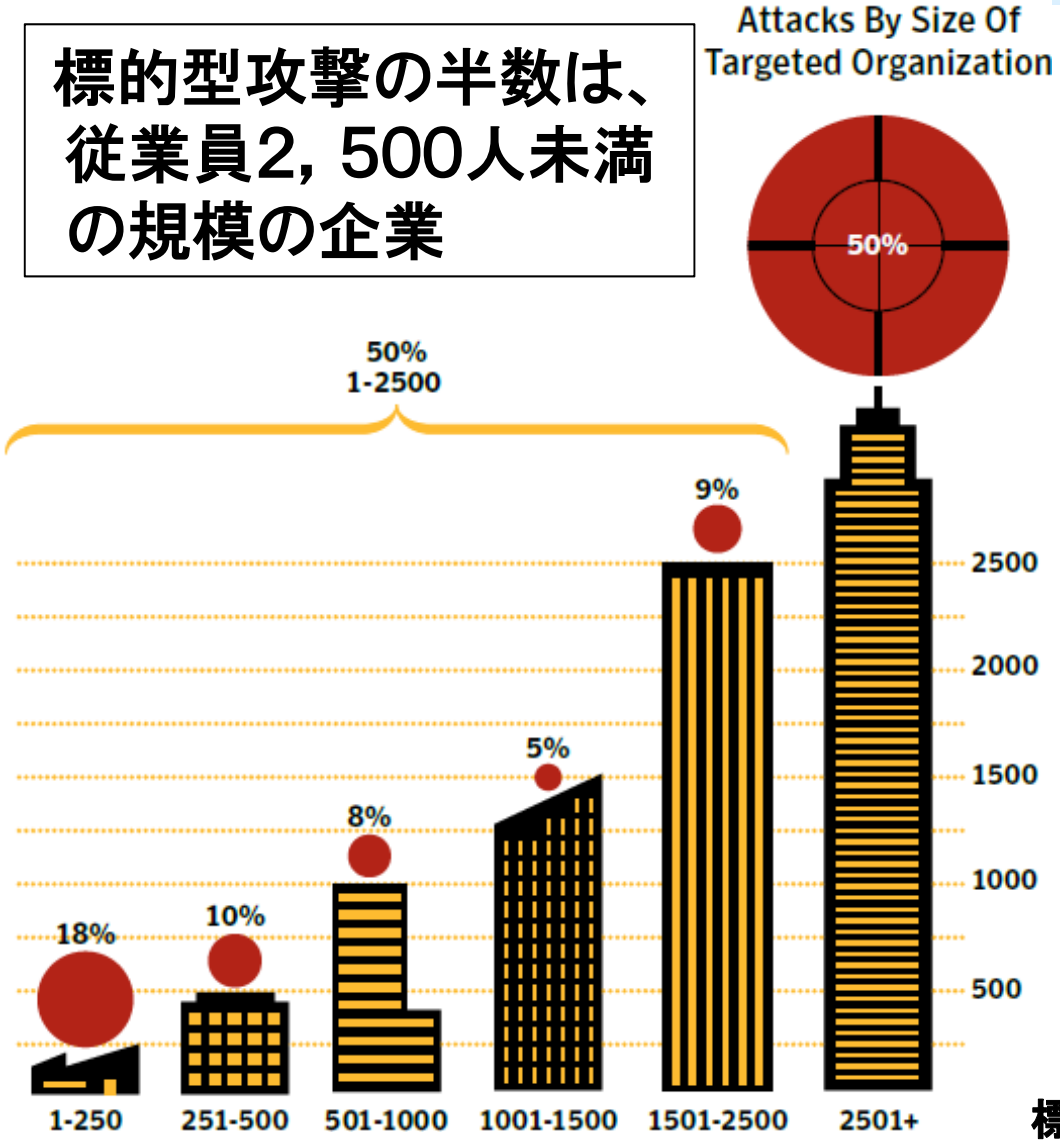
最近のサイバー攻撃の事例（M社の例）

本社を含む11拠点のサーバ45台、PC38台の計83台が感染。
一部のコンピュータのシステム情報が流出した可能性。



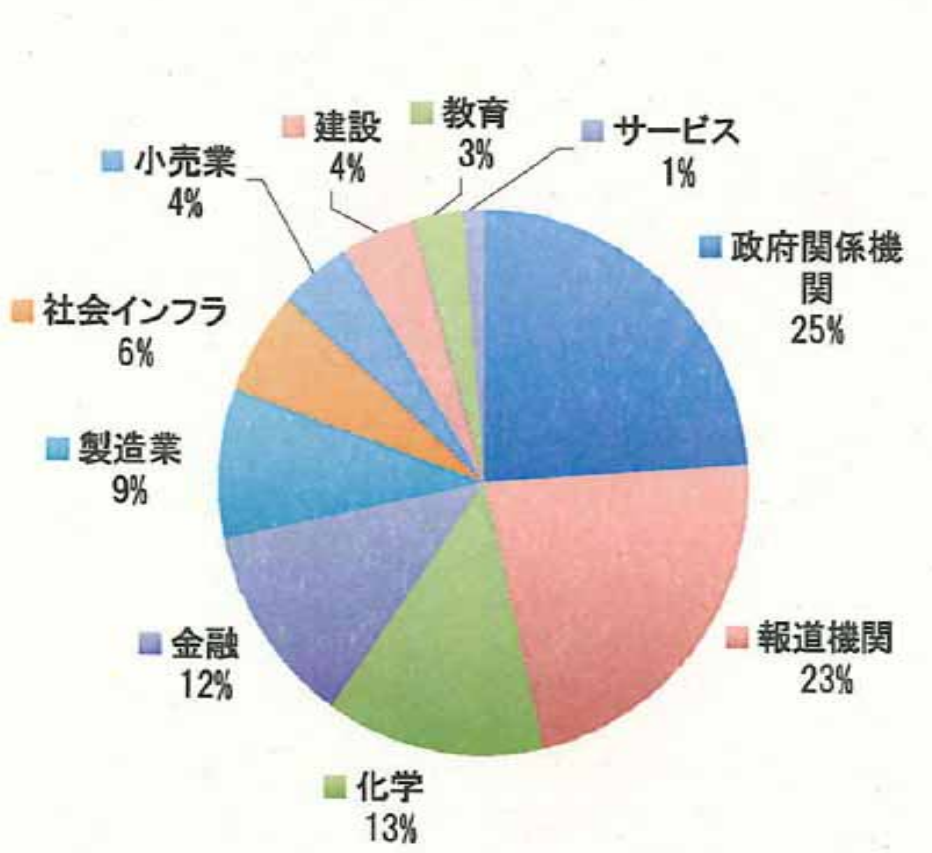
サイバー攻撃の対象企業

標的型攻撃の半数は、従業員2，500人未満の規模の企業



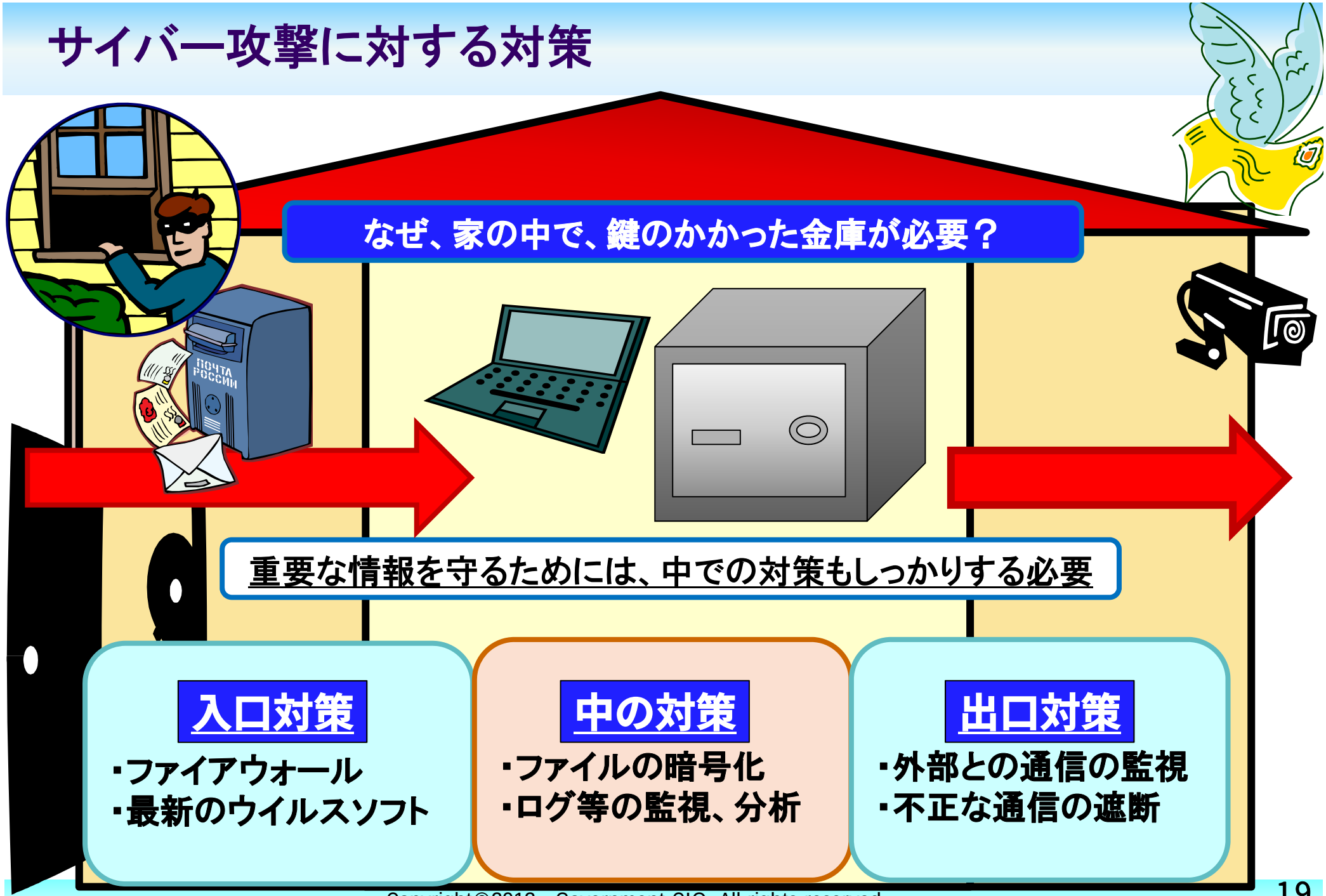
出典：INTERNET SECURITY THREAT REPORT：
2011 Trend Volume 17（2012年４月、Symantec社）

政府機関のほか、製造業企業、金融機関等様々な企業がターゲット



標的型メール攻撃のターゲットとなった組織の業務別割合
出典：2012年上半期Tokyo SOC情報分析レポート（IBM）
（東京SOC調べ　2012年１月～2012年６月）

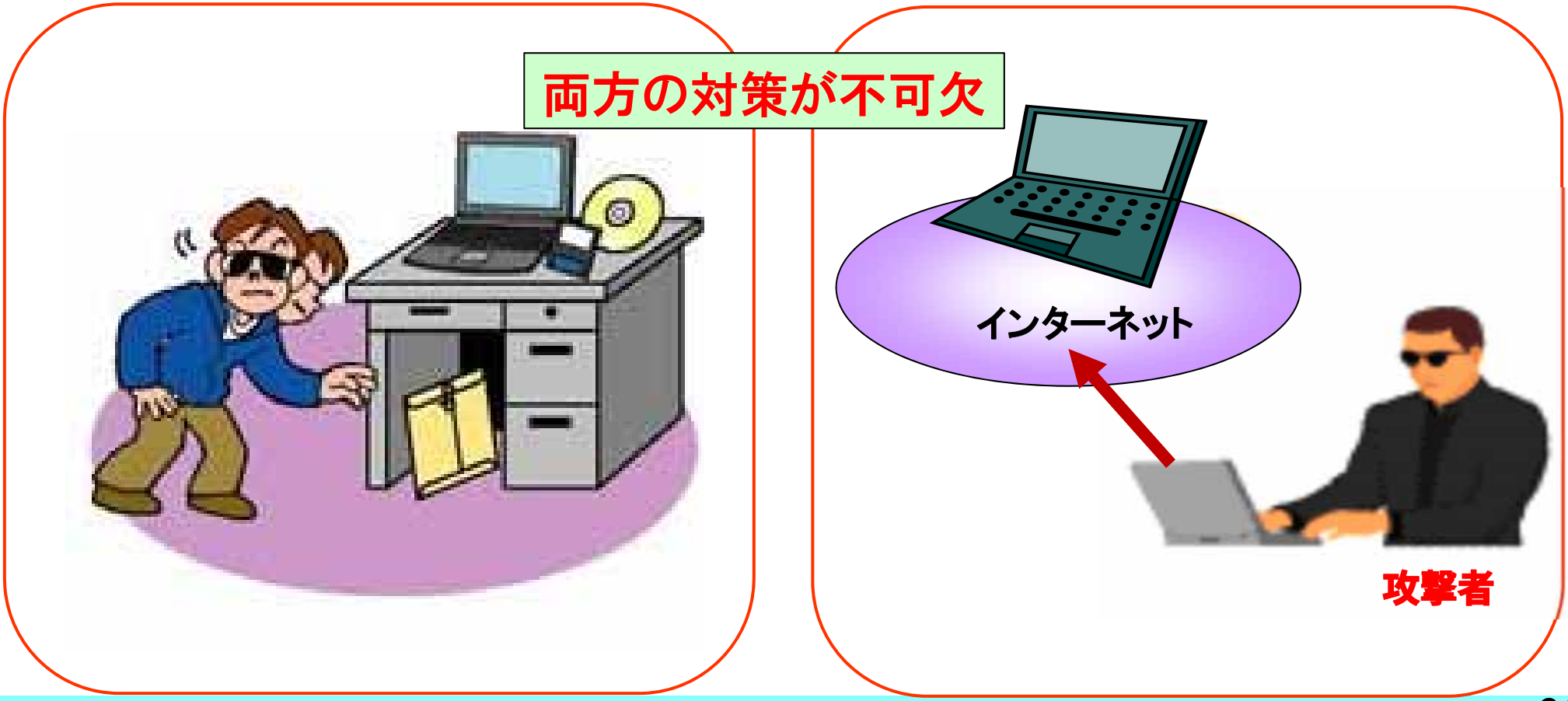
サイバー攻撃に対する対策



企業における情報漏えい

○ 「情報漏えいした」、「漏えいしたと感じた」経験がある企業は35%
○ 「国内退職者」(44%)、「海外退職者」(15%)などからも流出

【出典：日本経済新聞社による企業法務調査、2012年10月調査、主要企業326社を対象に実施。148社の回答】



情報漏えい事案（最近の事例）

○管理ミス、従業員の不注意などによる事件・事故が後を絶たない。
○多くの事故は日ごろの情報セキュリティ対策により防げると考えられる。

2012年3月6日　保険会社

保険会社は、2,555人分の顧客情報が社外に流出したと発表。
社員が顧客情報が入ったファイルを販売代理店に電子メールで送信する際に、誤ったアドレスを指定。ファイルには、保険契約者の指名や生年月日、住所、契約内容等が記録されていた。

2012年7月13日　飲料メーカー

飲料メーカーのキャンペーンに応募した顧客の個人情報が流出した可能性があると発表。約95,000件の氏名や性別、メールアドレス、住所などが2月3日から7月5日まで、インターネットで閲覧できる状態だった。
個人情報の管理の委託先の担当者が個人情報のデータを個人使用パソコンに複製して保有。レンタルサーバへ移したことからインターネット検索でアクセス可能な状態になっていた。

2012年7月20日　病院

都内の病院が、患者の個人情報を記録したパソコンなどを紛失したと発表。
病院の研修医が医局に個人所有のノートパソコンとUSBメモリーを残したまま診療業務に出向き、医局に戻ったところ無くなっていた。

2012年10月3日　大学

国内の5大学のサーバーがハッキングされ、教職員らの個人情報や研究リストなどが流出した。
大学は「サーバーの弱点を突かれた。甘い管理で申し訳ない。現在、再発防止策を検討している」とした。

※ 本資料は報道ベースで作成

情報漏えいに係る損害賠償額

損害賠償額は２，５００万円以上（2012年上半期）

2012年上半期　個人情報漏えいインシデント（速報値）

漏えい人数	150万7833人
漏えい件数	952件
想定損害賠償総額	250億4314万円
一件当たりの漏えい人数	1609人
一件当たり平均想定損害賠償額	2675万円
一人当たり平均想定損害賠償額	5万9776円

出典：NPO日本ネットワークセキュリティ協会、情報セキュリティ大学院大学

情報セキュリティインシデントが経営に与える影響

○ **倒産、訴訟、信用失墜、膨大な賠償金、経営層の責任追及、行政処分、職員解雇**

ネットスーパー運営会社

○不正アクセスを受け、顧客のクレジットカード情報１万2,191件を流出。
○この分野で業界最大規模の実績を持っていたものの、約４ヶ月後に倒産。

証券会社

○約５万人分の個人情報が流出。
○約５万人に１万円相当のギフト券を送付。
損失は70億円以上であると発表。
○社長、役員の減給、謝罪会見
○金融庁による行政処分

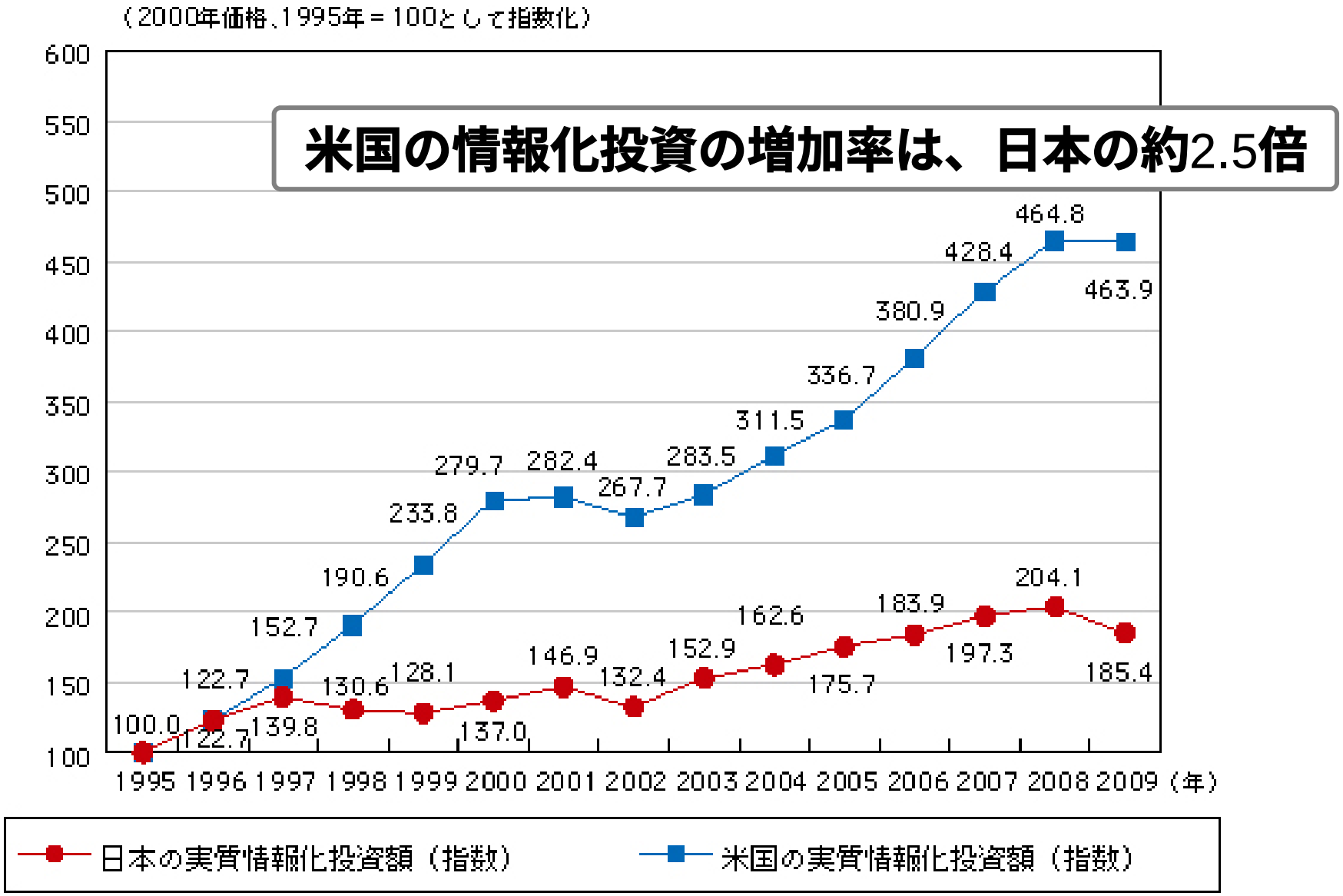
クレジット情報処理会社（米国）

○不正アクセスを受け、約4,000万件の個人情報流出。
○ハッカーによる情報搾取が原因。
○大量データ流出を受け、Visaと American Expressの２社との業務契約が打ち切りを表明したため、経営危機へ。

京都府Ｕ市

○住基台帳データ約22万人分の個人情報流出。
○アルバイト従業員が当該データを不正にコピーして名簿業者に販売、さらに他へ転売。
○漏えいしたアルバイト従業員は住民に対する違法行為と認定。
○一人あたり慰謝料１万円。

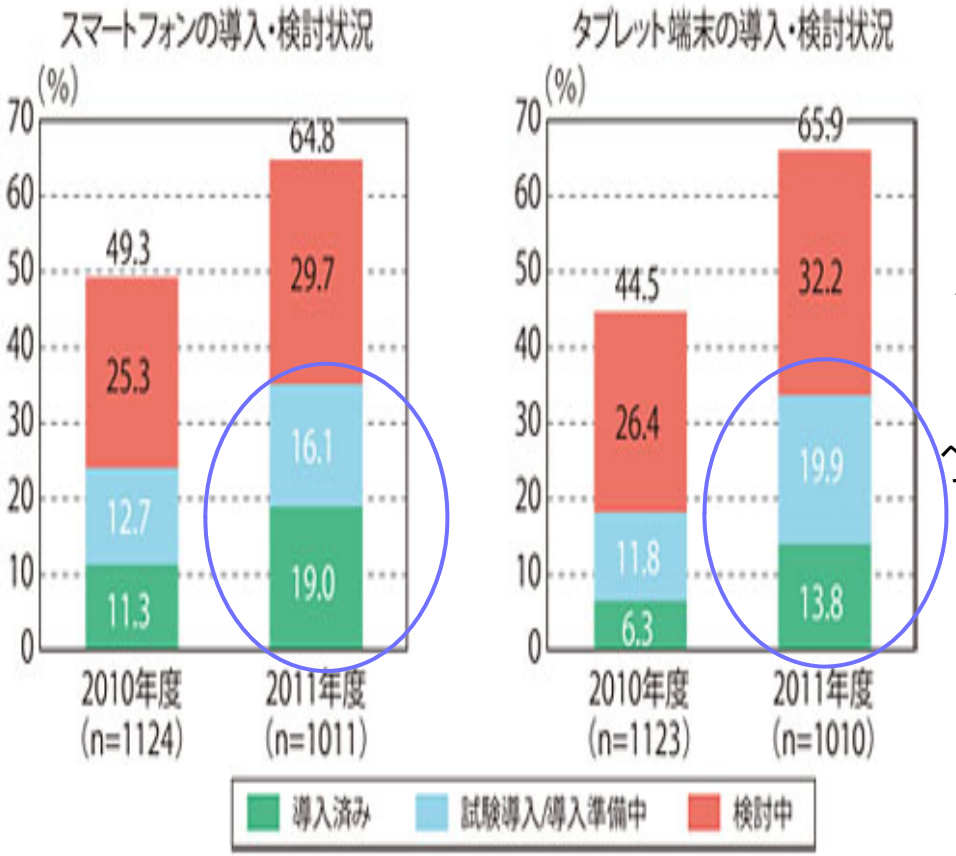
新しい情報通信技術の導入（情報化投資の日米比較）

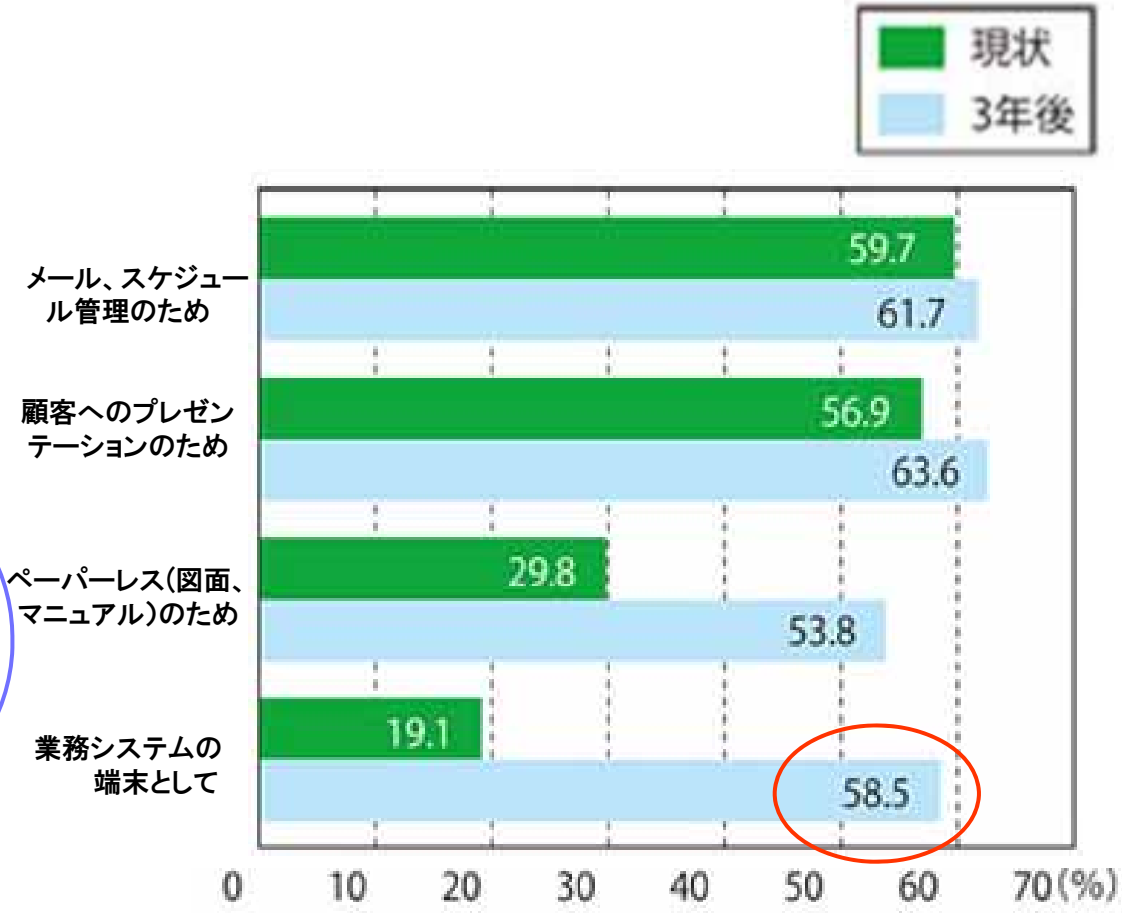


（出典）総務省「ICTの経済分析に関する調査」（平成23年）

新しい情報通信技術の導入とセキュリティの確保

企業の35.1%が既にスマートフォンを導入又は準備中





(出典　(社) 日本情報システム・ユーザ協会　企業IT動向調査2012
2011/10/29~11/21実施　4000社に郵送し1039社から回答)

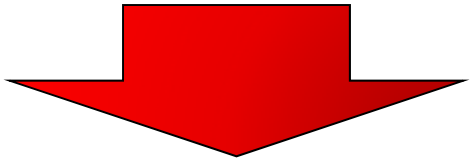
まとめ

○情報セキュリティインシデントの発生は企業経営に多大な影響

○システムの効率性　vs　情報セキュリティ

○利便性(BYOD等)　vs　情報セキュリティ

○現場(生産、営業部門)　vs　情報セキュリティ部門



セキュリティ対策は重要な経営判断
（コストと見るか、投資と見るか）

政府機関におけるサーバ集約化に関する取組①

経　緯

- 政府機関全体において多数のサーバを保有（H20年11月1日時点）
  ＊公開ウェブサーバ約1,000台、電子メールサーバ約1,900台
- 平成21年4月以降複数発生した政府機関のＨＰ改ざん事案において、関係政府機関の対応の遅れが見られた。

問題認識

- 統制なく多数のサーバを設置・運用すると、コストが増大し、**緊急時に迅速かつ的確な対応が困難**となる等**セキュリティリスクが高まる**。
- セキュリティ向上の観点、また、コスト削減の観点からも、既存の最適化等の状況を踏まえつつ、各府省庁の業務や実情に応じて、**サーバの集約化を推進**する必要がある。
- 障害・事故等発生時における**緊急連絡体制が、十分に機能していない**場合がある。

多数のサーバ

政府機関におけるサーバ集約化に関する取組②

対応方針

*情報セキュリティ政策会議決定（平成21年6月22日）

- **公開ウェブサーバ及び電子メールサーバについては、平成25年度末までに、政府機関全体として少なくとも半減することを目標とする。**
- **各府省庁においては、最適化計画の枠組みも活用し、省全体の平成22年度からの公開ウェブサーバ及び電子メールサーバに係る集約化計画を定め、情報セキュリティ政策会議に報告する。**

集約化計画

*情報セキュリティ政策会議報告（平成22年5月11日）

集約台数	H20年11月1日時点		H25年度末見込み
○ 公開ウェブサーバ：	約1,000台	→	約　550台　（約45%を削減）
○ 電子メールサーバ：	約1,900台	→	約1,000台　（約47%を削減）

【主な集約方法】
- 基盤となる情報システムのサーバに統合
- 地方の出先機関毎に設置されていたサーバを本省庁等に集約

【例　外】
- 業務との密接な連携や独自な運用が必要なサーバ
- 災害発生時等において可用性を確保する観点から負荷分散・冗長構成が不可欠なサーバ