NISC National Information Security Center

# ビッグデータ時代の
# サイバーセキュリティ戦略

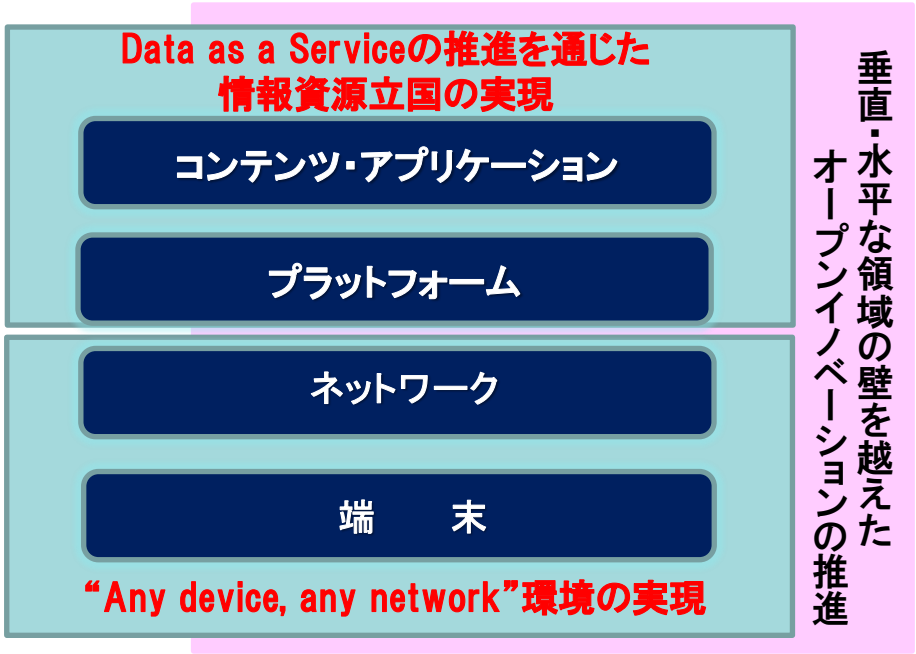
２０１４年3月14日
内閣官房情報セキュリティセンター（NISC）副センター長
内閣審議官　谷脇　康彦
http://www.nisc.go.jp/

# 新ICT戦略（世界最先端IT国家創造宣言、１３年６月）

“世界最高水準のIT 利活用社会を実現するに際して、

「ヒト」、「モノ」、「カネ」と並んで「情報資源」は新たな経営資源となるものであり、
「情報資源」の活用こそが経済成長をもたらす鍵となり、課題解決にもつながる。

ビッグデータやオープンデータに期待されるように、分野・領域を越えた情報資源の収集・蓄積・融合・解析・活用により、新たな付加価値を創造するとともに、変革のスピードを向上させ、産業構造・社会生活において新たなイノベーションを可能とする社会の構築につなげる必要がある。“



# 世界最先端IT国家創造宣言（13年6月閣議決定）

世界最高水準のIT利活用社会（情報資源立国）の実現
～5年程度の期間（2020年）で実現～

## 新産業・新サービスの創出

- オープンデータ・ビッグデータ活用の推進
- made by Japan農業の実現
- オープンイノベーションの推進
- ITやデータを活用した地域の活性化
- 次世代放送サービスによる新事業創出

## 安心・安全社会の実現

- 健康長寿社会の実現
- 世界一安全で災害に強い社会の実現
- スマートグリッドの推進
- 世界最先端の道路交通社会の実現
- 雇用形態の多様化等の実現

## ワンストップ型公共サービスの実現

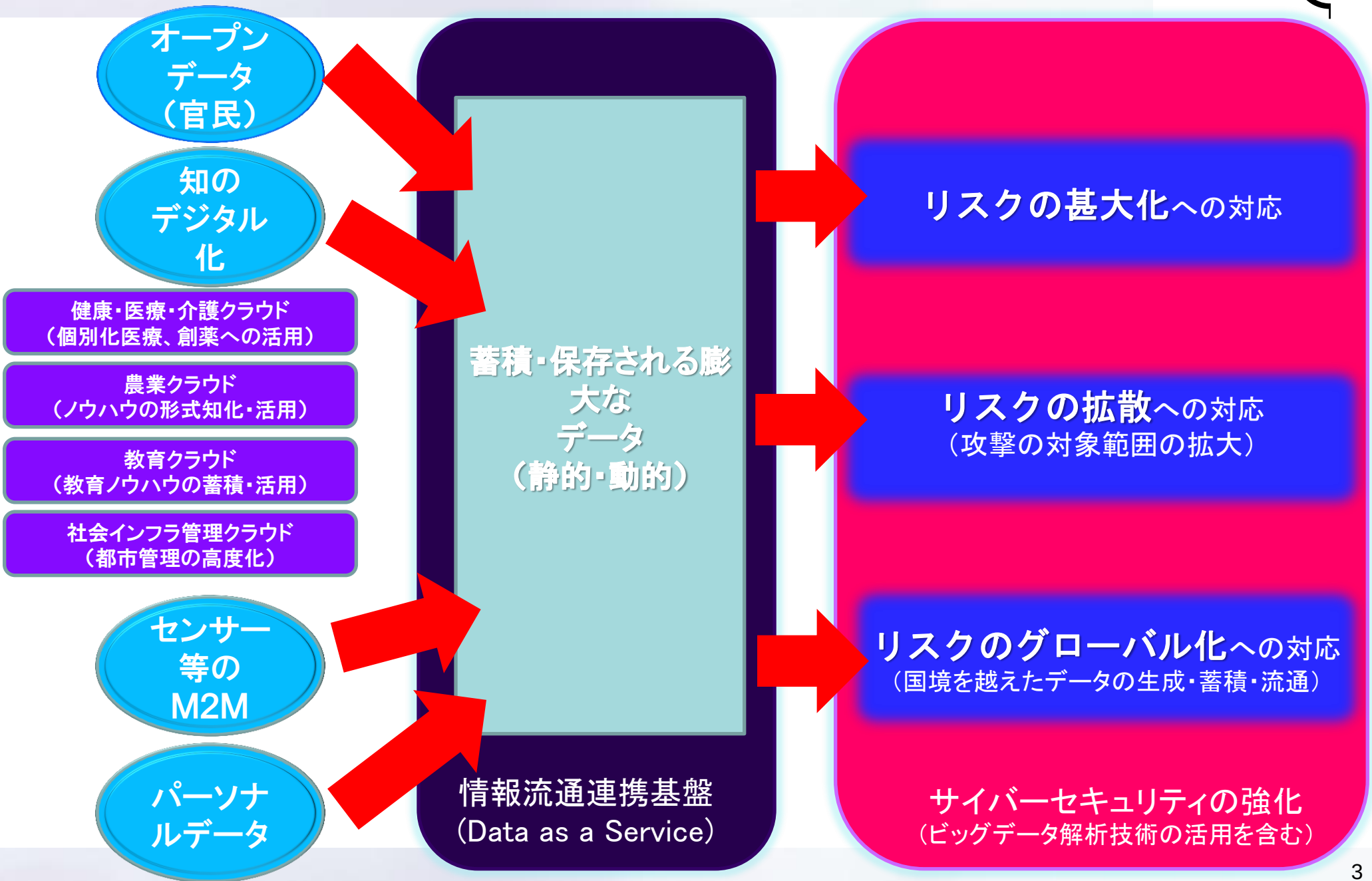
- 利便性の高い行政サービスの実現
- 国・地方の行政情報システムの改革
- 政府におけるITガバナンスの強化

- 教育環境のIT化
- 世界最高水準のITインフラ環境の確保
- サイバーセキュリティ立国の実現
- 研究開発の推進（総合科学技術会議と連携）

- 政府CIOの司令塔機能の発揮
- 定量的なKPIによる推進管理
- 規制制度改革の推進
- 分野複合的な課題解決プロジェクトの推進

（注）各施策の表記は宣言本文の趣旨を踏まえて一部修正。

# ビッグデータ時代のサイバーセキュリティ政策の重要性



# 我が国における危機①
## ～リスクの甚大化～

## 機微な情報に対する巧妙な攻撃

**【最近の主な事例】** 氷山の一角

| | |
|---|---|
| 2011.9～ | [三菱重工業、衆議院等] 標的型攻撃によるウイルス感染発覚 |
| 2012.5 | [原子力安全基盤機構] 過去数か月間の情報流出の可能性確認 |
| 2013.1 | [農林水産省] TPP情報流出に関するサイバー攻撃事案報道 |
| 2013.4 | [宇宙航空研究開発機構] サーバに対する外部からの不正アクセス発覚 |
| 2013秋頃 | [政府機関等] 特定者がウェブ閲覧により感染するゼロデイ攻撃※発覚 |
| 2014.1 | [原子力研究開発機構] ウイルス感染による情報の流出の可能性発覚 |

**【政府機関への脅威件数等】** 24時間365日（１分に２回）

| | 2010年度 | 2011年度 | 2012年度 |
|---|---|---|---|
| センサー監視等による脅威件数 ※※ | 約48万 | 約66万 | **約108万** |
| センサー監視等による通報件数 | 181 | 139 | **175** |
| 不審メールに関する注意喚起の件数 | 118 | 209 | **415** |

※ 「ゼロデイ攻撃」とは、ソフトウェアにおける未修正・未発表のセキュリティ上の脆弱性を悪用した攻撃

※※ GSOC（政府機関・情報セキュリティ横断監視・即応調整チーム）により各府省等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

## 重要インフラに対する攻撃

**【重要インフラへの攻撃件数等】** 危機の高まり

| | 2012年度 | 主な内訳 | |
|---|---|---|---|
| 重要インフラ分野からの情報連絡※件数 | **110** | 不正アクセス、DoS攻撃<br>ウイルスへの感染<br>その他の意図的要因 | 55<br>6<br>15 |

| | 2012年度 | 2013年度 4～6月 | 2013年度 7～9月 |
|---|---|---|---|
| 標的型攻撃メール等の情報提供※※件数 | **246** | **74** | **95** |

**【重要インフラ分野】** 保護対象の多様化

① 情報通信
② 金融
③ 航空
④ 鉄道
⑤ 電力
⑥ ガス
⑦ 政府・行政サービス
⑧ 医療
⑨ 水道
⑩ 物流

○ 化学
○ クレジット
○ 石油
※※※

**［参考］米国の状況** 電力、水道及び交通分野等の重要インフラに対する攻撃が、**2011年以降、17倍に増加**（2013年6月デンプシー統合参謀本部議長講演）

※ 重要インフラ事業者からNISCへの連絡　※※ 重要インフラ機器製造、電力、ガス、化学、石油の5業界・45組織から情報処理推進機構（IPA）への提供

※※※ 現在、情報セキュリティ政策会議で検討・パブリックコメント中の「重要インフラの情報セキュリティ対策に係る第3次行動計画（案）」において追加予定

# 我が国における危機②
## ～リスクの拡散・グローバル化～

## 攻撃の対象範囲の拡散

**【スマートフォンの普及等】**

国民1人1人へ

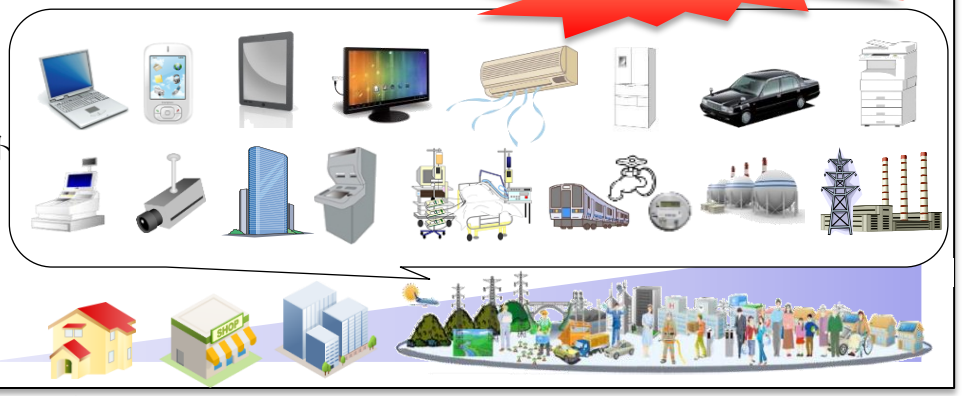
**スマートフォン**
世帯保有率が**5倍**に急増※
（2010年末：約10%→**2012年末：約50%**）

**スマートカー**
1台に搭載される車載コンピュータは**100個以上**、ソフトウェアの量は**約1000万行**※※

**スマートメーター**
**（次世代電力量計）**
電力会社による開発・導入の開始
［主な予定］
・東京：2023年度までに**2700万台**の導入完了
・関西：2023年度までに**1300万台**の導入完了

**【我が国社会全体への浸透】**

いつでもどこでも何でも



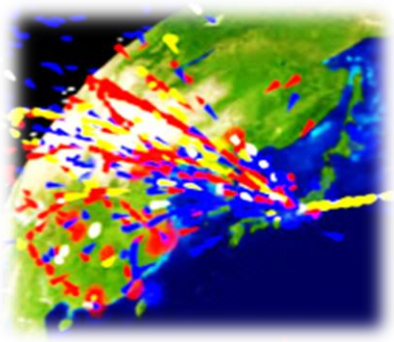
※　総務省「平成25年版情報通信白書」

※※　（独）情報処理推進機構（IPA）「自動車の情報セキュリティへの取組みガイド」（2013年8月）

## 世界中からの多様な主体による攻撃

**【海外からの我が国への攻撃状況※】**

グローバル化



| 国名（国コード） | ホスト数 | 割合 |
|---|---|---|
| 中国（CN） | 37,149 | 47% |
| 韓国（KR） | 6,005 | 8% |
| 日本（JP） | 5,820 | 7% |
| 台湾（TW） | 3,351 | 4% |
| アメリカ（US） | 3,240 | 4% |
| ロシア連邦（RU） | 2,237 | 3% |
| ブラジル（BR） | 2,123 | 3% |
| 香港（HK） | 1,608 | 2% |
| タイ（TH） | 1,504 | 2% |

**【最近の主な事例】**

国家関与の可能性

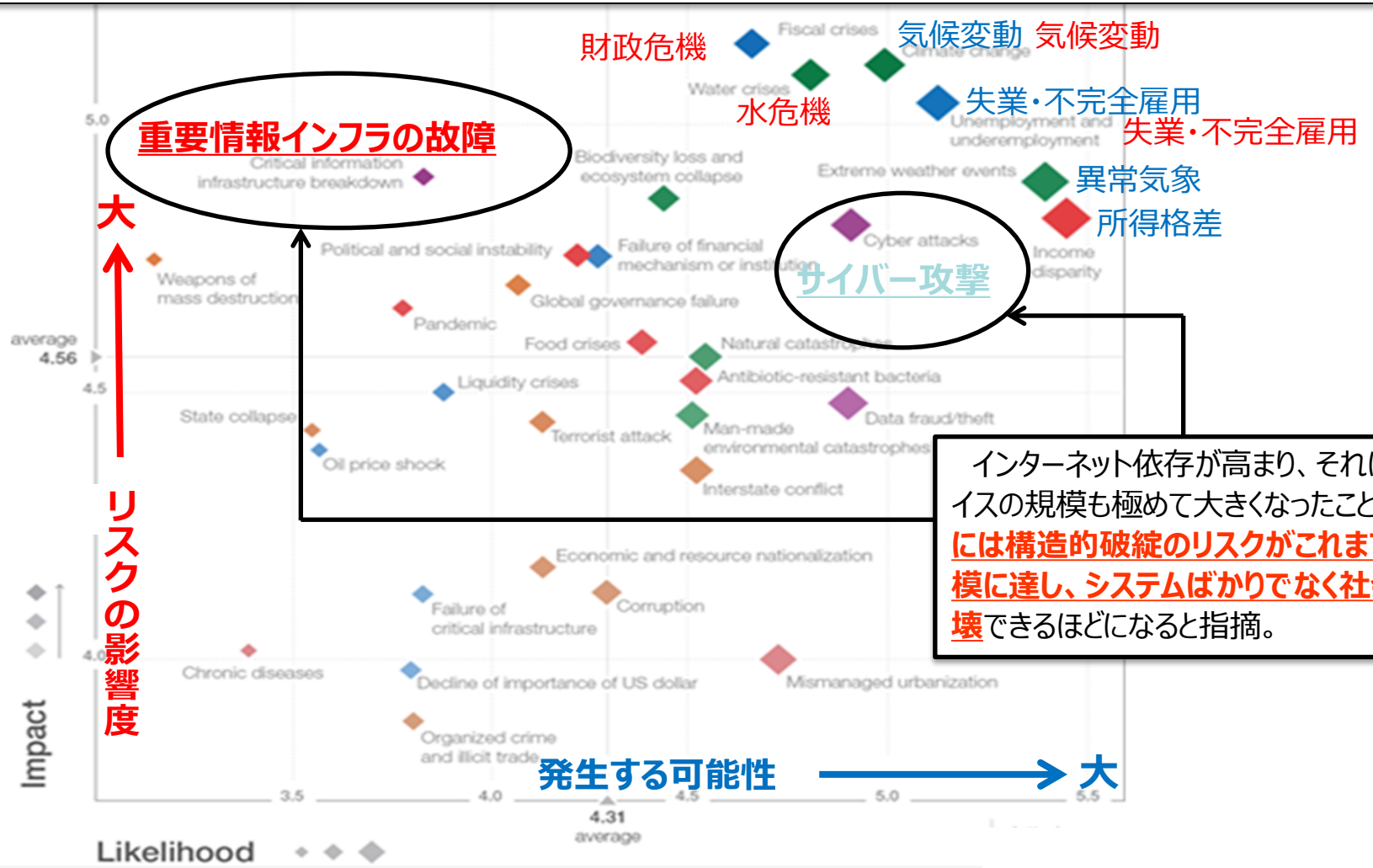
| | |
|---|---|
| 2011.3 | ［韓国］政府機関等の40のウェブサーバへのDDoS攻撃発生<br>***→ 日本の家庭用PCが踏み台となり攻撃指令サーバ化*** |
| 2013.3 | ［韓国］重要インフラに対する大規模サイバー攻撃発生<br>***→ 使用された不正プログラムが我が国でも同時期に確認*** |
| （参考） | |
| 2013.5 | ［米国］国家機密や企業機密を窃取する標的型攻撃について、<br>**外国政府・軍の関与の可能性を政府が指摘**※※ |

※　（独）情報通信研究機構（NICT）のインシデント分析システム「nicter（ニクター）」より（右図は「国別ホスト数Top10」2014年1月22日現在）

※※　ホワイトハウス「営業秘密侵害を低減するための米国政府戦略」（2013年2月）及び国防総省「年次報告書」（2013年5月）

# 世界が直面するグローバルリスク
## ～一層深刻な状況へ～

本年に入り、世界経済フォーラム（WEF）は、**今後10年間で全世界及び全産業界に重大な悪影響を及ぼす可能性が高いリスク**として、**サイバー攻撃及び重要情報インフラの故障**を位置づけ。




インターネット依存が高まり、それに繋がるデバイスの規模も極めて大きくなったことで、**2014年には構造的破綻のリスクがこれまでで最大規模に達し、システムばかりでなく社会までも破壊**できるほどになると指摘。

備考：全世界及び全産業界に対して重大な悪影響を及ぼす可能性のあるものとして抽出した31のリスクに関する今後10年間の展望について、世界各地の700名以上の専門家に対する調査結果をとりまとめたもの。「1」は「発生する可能性がないもの」又は「影響がないと思われるもの」、「7」は「大いに発生する可能性があるもの」、又は「甚大かつ破壊的な影響があると思われるもの」を示している。

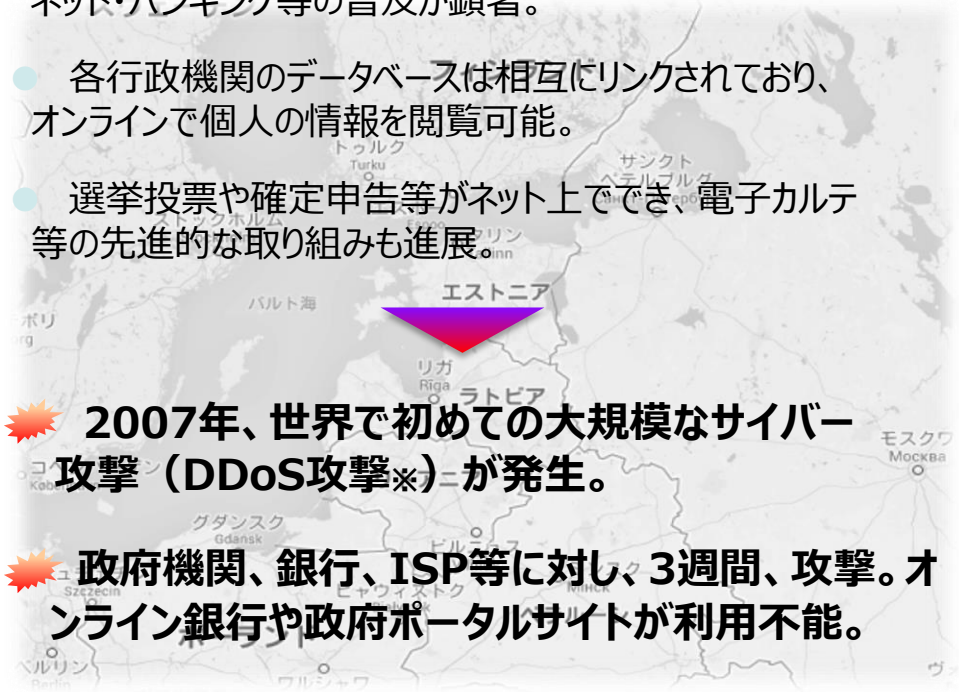
＜出典：WEF「グローバルリスク報告書2014年版」(2014年1月16日)＞

# ＩＴ先進国における経験
## ～深刻な危機に直面～

NISC

## エストニア

- IT立国を国策として進め、電子政府、電子IDカード、ネット・バンキング等の普及が顕著。
- 各行政機関のデータベースは相互にリンクされており、オンラインで個人の情報を閲覧可能。
- 選挙投票や確定申告等がネット上でき、電子カルテ等の先進的な取り組みも進展。



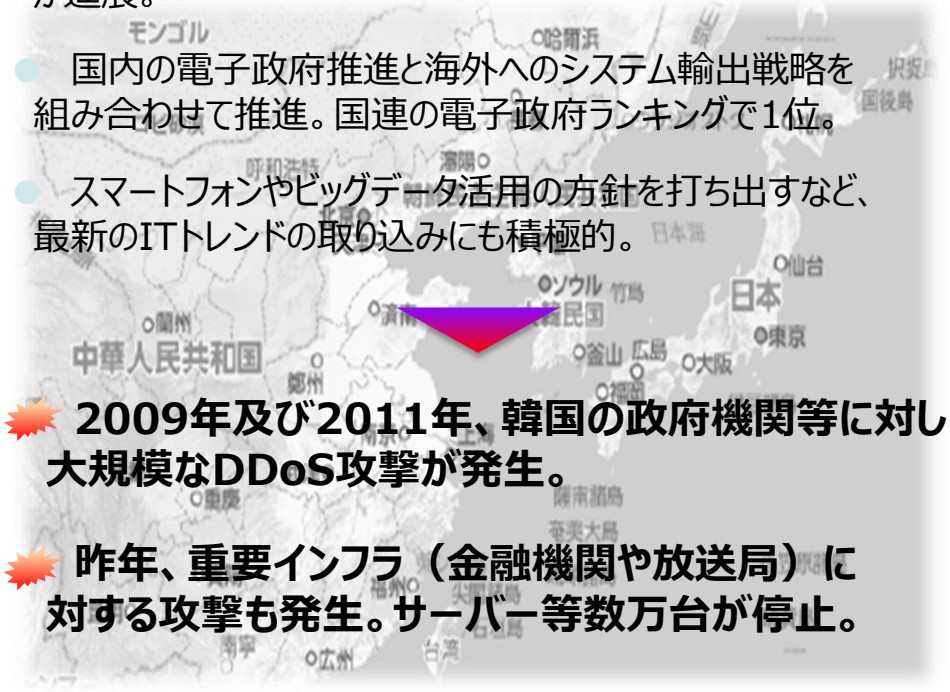

**2007年、世界で初めての大規模なサイバー攻撃（DDoS攻撃※）が発生。**

**政府機関、銀行、ISP等に対し、3週間、攻撃。オンライン銀行や政府ポータルサイトが利用不能。**

**以降、サイバー防衛の分野で国際的なイニシアティブを発揮。本年、新たな戦略を策定予定。**

## 韓国

- IT政策を国家戦略的課題と設定し、重点的に取組が進展。
- 国内の電子政府推進と海外へのシステム輸出戦略を組み合わせて推進。国連の電子政府ランキングで1位。
- スマートフォンやビッグデータ活用の方針を打ち出すなど、最新のITトレンドの取り込みにも積極的。




**2009年及び2011年、韓国の政府機関等に対し大規模なDDoS攻撃が発生。**

**昨年、重要インフラ（金融機関や放送局）に対する攻撃も発生。サーバー等数万台が停止。**

**上記について、当局は北朝鮮によるものと発表。昨年7月には、司令塔の強化など新計画を策定。**

※「DDoS（Distributed Denial of Services）攻撃」とは、遠隔操作された大量のコンピュータが一斉に特定のサーバ等にデータを送出し、通信路をあふれさせて機能を停止させ、ホームページの閲覧障害等を発生させてしまうサイバー攻撃

＜出典：外務省ウェブページ、総務省「平成25年情報通信白書」等＞

# 国家安全保障戦略（13年１２月閣議決定）

## Ⅲ　我が国を取り巻く安全保障環境と国家安全保障上の課題

### １　グローバルな安全保障環境と課題

**（4）国際公共財（グローバル・コモンズ）に関するリスク**

近年、海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。

（中　　略）

情報システムや情報通信ネットワーク等により構成されるグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

一方、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化しつつある。

我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とする観点から、不可欠である。

# サイバーセキュリティ戦略（13年6月情報セキュリティ政策会議決定）

NISC

| | 政府機関・独立行政法人等 | 重要インフラ事業者 | 企業・一般個人 |
|---|---|---|---|
| 「強靭な」サイバー空間（守り強化） | ①●機微情報を守るためのﾘｽｸ評価手法の確立・統一基準の見直し【今年度】<br>②●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応<br>●対処訓練の実施、警察・自衛隊等の関係機関の役割整理【今年度】<br>●SNS・グループメールを含む新サービスに伴う新たな脅威への対応 | ③●重要ｲﾝﾌﾗの範囲拡大や安全基準見直し等行動計画の見直し【今年度】<br>●政府機関やシステムベンダー等との情報共有の強化<br>●事業継続確保のための分野横断的な演習 | ●スマートフォン不正アプリへの対応<br>●情報セキュリティ月間【2月】・サイバー・クリーン・デー[仮称]創設<br>④●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【今年度】<br>●税制など中小企業のセキュリティ投資の促進<br>●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組<br>●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保 |
| 「活力ある」サイバー空間（基礎体力） | ⑤●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【今年度】<br>⑥●研究開発戦略（2011年情報セキュリティ政策会議）の見直し | | |
| ⑦「世界を率先する」サイバー空間（国際戦略） | ●日米【10～12月：第2回サイバー対話】<br>●日英<br>●日印<br>●日露<br>●日EU<br>●日ASEAN【9月：閣僚会議@東京】<br>●サイバー空間の国際規範づくり等に関する会議【10月：ソウル会議】<br>●IWWN注1<br>●MERIDIAN注2 | | 〈注１〉サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加<br>〈注２〉重要インフラ防護等のベストプラクティスの共有や国際連携方策等に関する意見交換。 米・英・独・日等の重要インフラ防護担当者が参加。<br>●共同意識啓発活動【10月】 |
| ⑧組織体制 | ●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組：2015年度目途） | | |

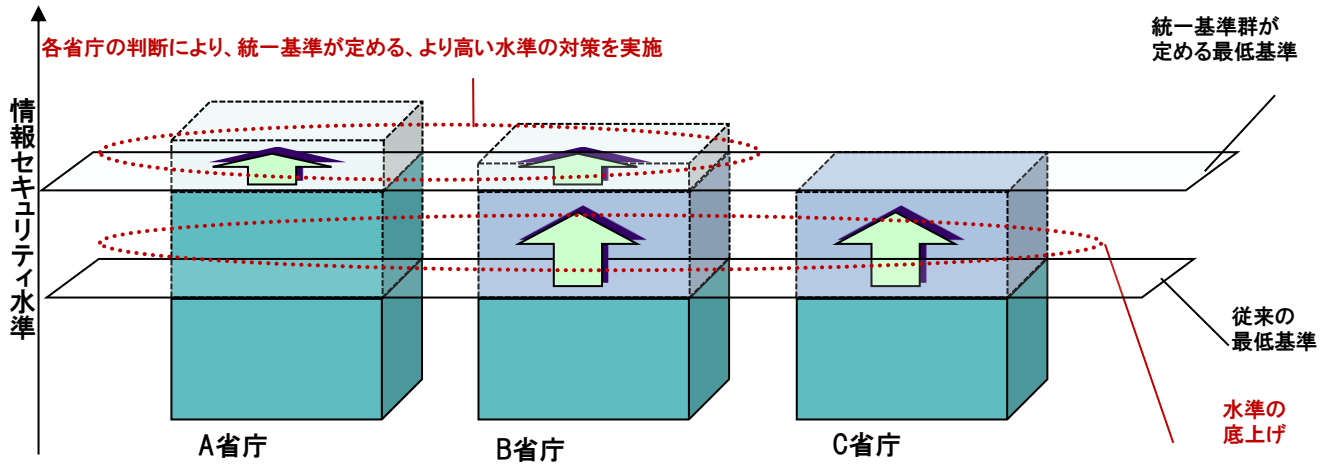
# （１）政府機関における情報等の重要度等に応じた対策の重点化

## 現行の統一基準群

〇政府機関が実施すべき対策の統一的な枠組みを構築

〇政府機関全体の情報セキュリティ水準の底上げに寄与

＜統一基準群の効果（イメージ）＞




## 課　　題

〇毎年の改定により基準が複雑化、肥大化
〇新たな脅威、技術進展、環境変化への対応が必要

〇重要な情報窃取を意図した標的型攻撃等の高度サイバー攻撃による脅威が深刻化

（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）においては、「標的型攻撃等への対処に関するリスク評価手法の確立等を通じて、政府機関における統一的な仕組みを強化する」こととされている。）

# 標的型メールの特徴

①差　出　人：情報 太郎 [johou.taro@cas-go.jp]

　宛　　先：二鋤 次郎

②件　　名：【重要】放射線量の状況

③添付ファイル：放射線量.zip

④関係各位

　いつもお世話になっております。内閣官房の〇〇〇〇です。現在の放射線量についてまとめました。添付を確認ください。
　また、添付ファイルと併せて、以下のURLもご確認ください

⑤http://www3.cas.go.jp/mapserch/ ⇒ 表示は偽装できます！

クリックすると

http://10.243.23.11/詐欺/

**①差出人のアドレスを確認**

@より右側が省庁ドメイン（.go.jp）でない

**②件名で開封を急がせる**

「重要」「緊急」などを付加

**③添付ファイルの確認**

アイコンを文書のように偽装
・.exe等はウィルスの可能性

放射線量.doc.exe

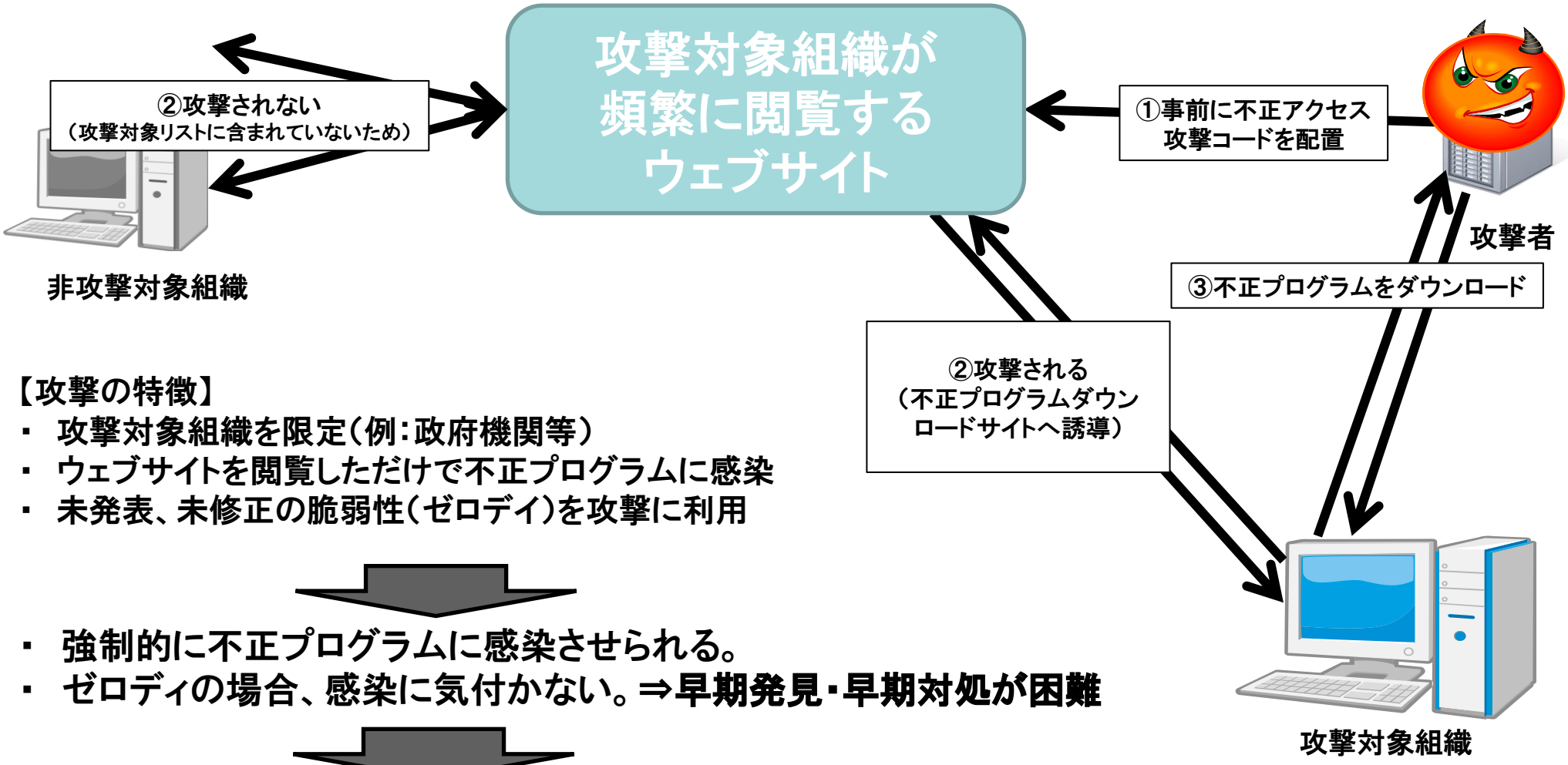
**④メール本文は本物のコピー**

・発信者に送信したかを確認

**⑤リンク先表示**

全く別のアドレスに偽装可能

# 水飲み場攻撃による特定の攻撃対象への攻撃




【攻撃の特徴】
- 攻撃対象組織を限定（例：政府機関等）
- ウェブサイトを閲覧しただけで不正プログラムに感染
- 未発表、未修正の脆弱性（ゼロデイ）を攻撃に利用

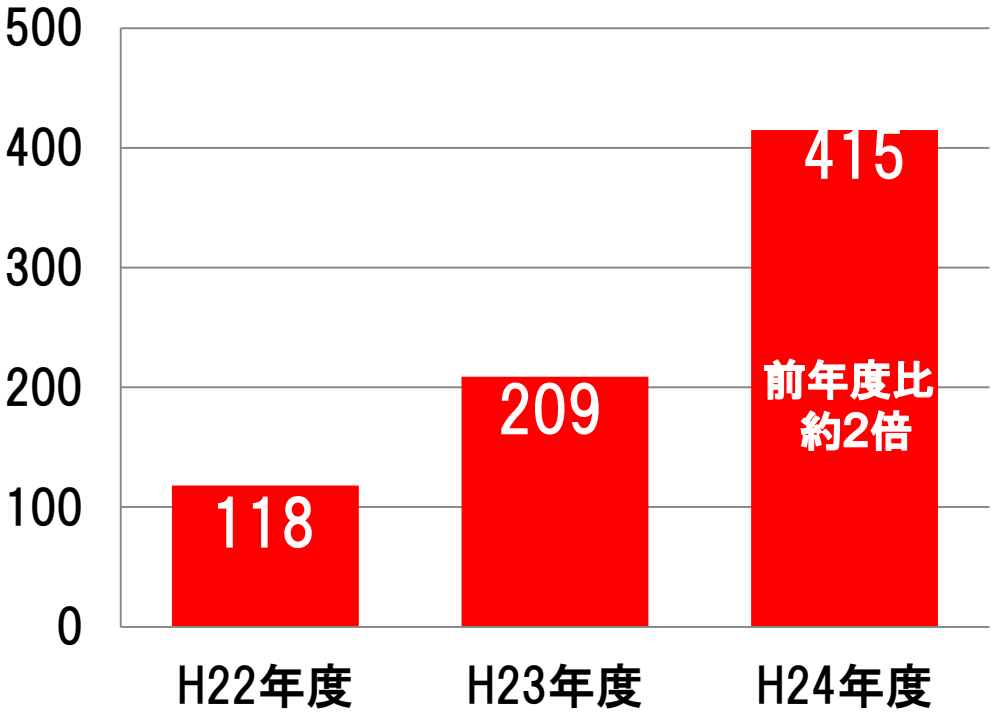
- 強制的に不正プログラムに感染させられる。
- ゼロディの場合、感染に気付かない。⇒**早期発見・早期対処が困難**

- 従来のセキュリティ対策に加え、定期的なネットワーク監視がより重要。
- 関係機関間の情報共有・相互連携が極めて重要。

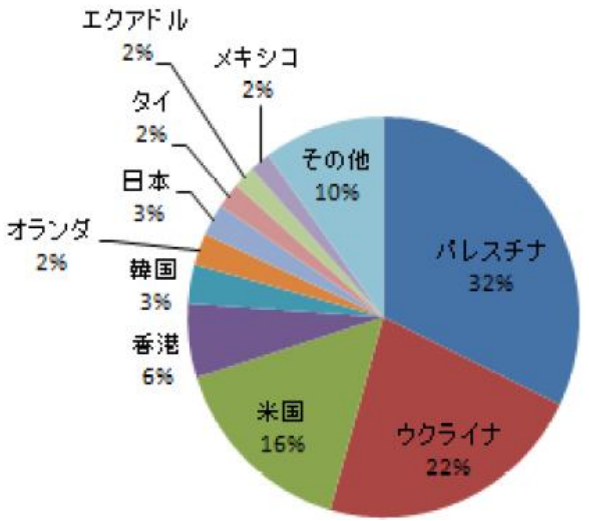
# 増加する標的型メール攻撃

○機密情報などの窃取を目的としたサイバー攻撃
○年々増加し、手口も巧妙化（組織的な攻撃の可能性）
○感染後の通信の接続先は、ほとんどが海外。

政府機関等への標的型メールに関する
注意喚起の件数の推移



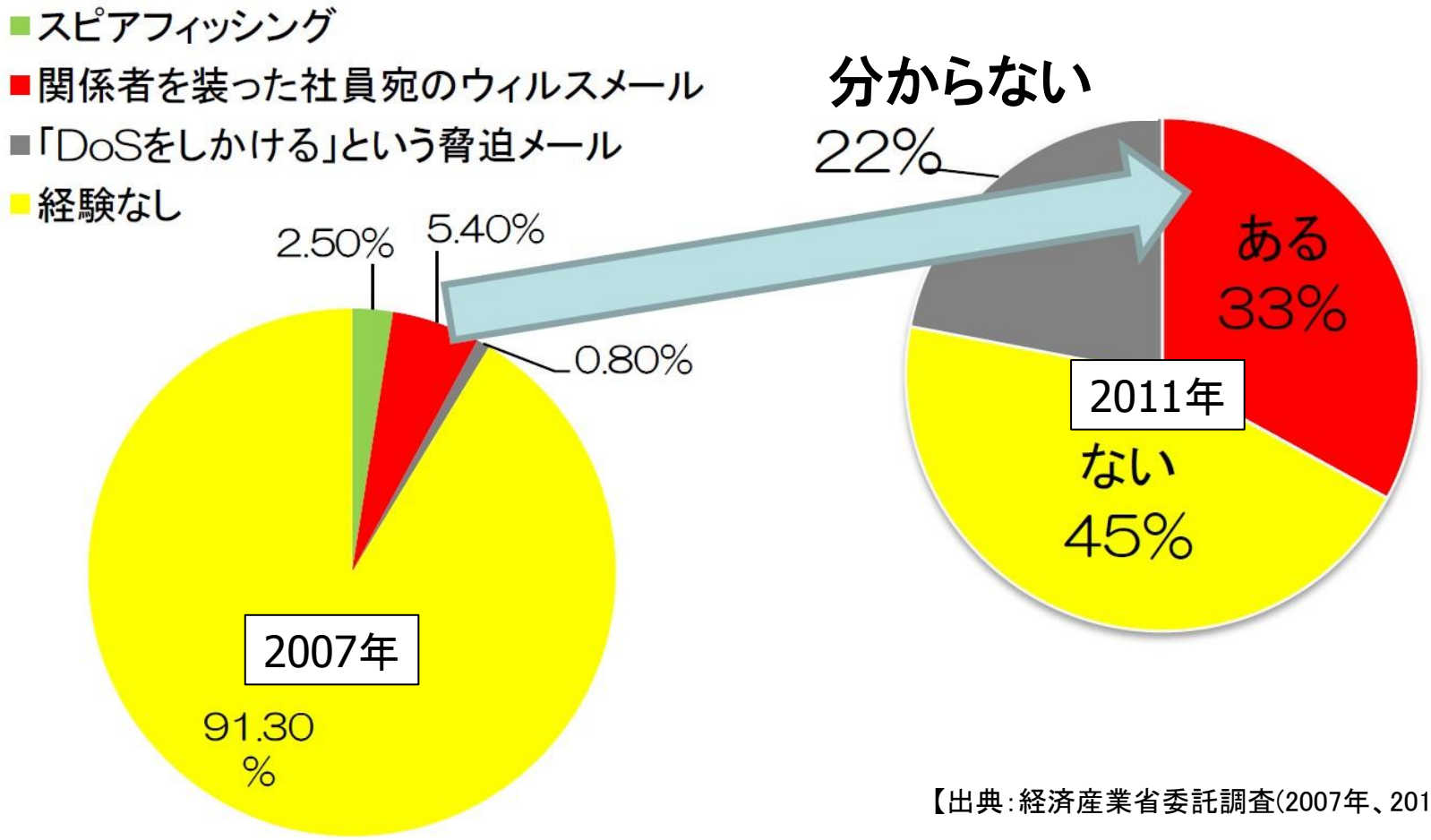

H25年中の標的型メール攻撃に使用された
不正プログラム等の接続先




出典：警察庁（H26年2月）

# 標的型メール攻撃を受けた経験

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%



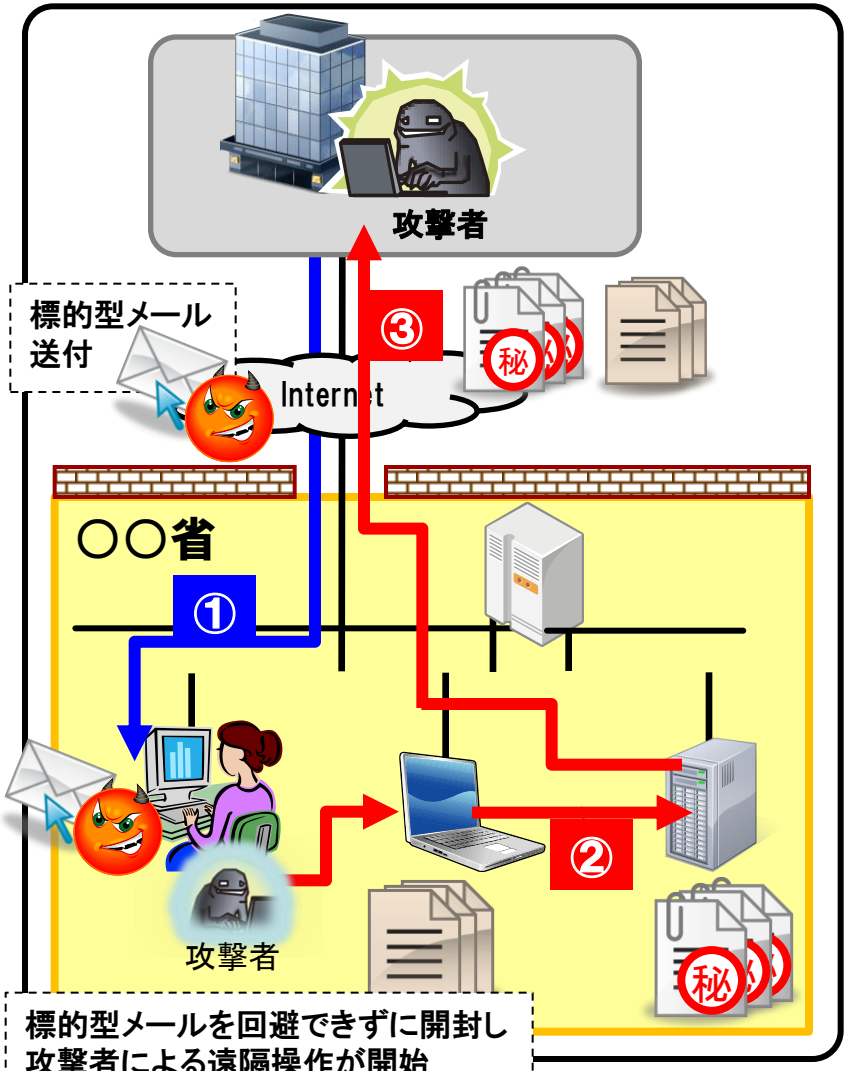

【出典：経済産業省委託調査(2007年、2011年)】

# 高度サイバー攻撃（標的型攻撃）対処のための対策実施

NISC

標的型メールを開封し、省内システムが不正プログラムに感染したとしても、攻撃者が**最終目的（重要な情報の窃取やシステム破壊）を達成する前まで**に、攻撃の兆候を監視・検知又は攻撃を防御し、対処する。

## 標的型攻撃（典型的なモデル）




**攻撃プロセス**

① 初期潜入

② 侵入範囲拡大

③ 情報窃取

政府機関の情報セキュリティ対策のための統一管理・技術基準で対策を規定

**情報システム内部の設計対策**

統一管理・技術基準の上乗せ対策

| 対策目的 | 対策方針 |
|---|---|
| 攻撃を遮断し、侵入範囲の拡大を防止する | • 攻撃者にとってハッキング技術を用いた内部探索をしづらいシステム設計<br>• 機器乗っ取りをしづらいシステム設計 |
| 攻撃の兆候を監視し、早期に発見・検知する | • 攻撃（主に攻撃失敗）の痕跡を残す<br>• 攻撃者の侵入を発見・検知するためのトラップ（罠）を設置<br>• 上記の継続的な監視 |

# ダッシュボードに基づきCISOが承認・決定する事項

**ダッシュボードに基づき CISOが承認・決定する事項**

自府省庁において**重点的に守るべき業務・情報**が妥当かどうか

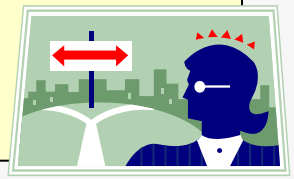
現状の情報システムの**対策状況等**

**計画内容**（優先順位付け、進捗状況、資源配分等）

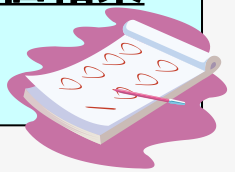
**ダッシュボードの記載内容**

情報セキュリティ推進の目標・計画に照らして進捗状況を可視化し、CISOへのリスク評価結果等の報告及び対策導入計画の提案に用いるもの。

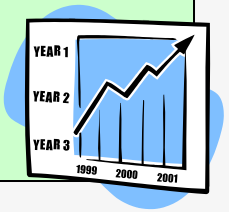
**①重点的に守るべき業務・情報**
- 重点的に守るべき業務・情報を評価
- 脅威事象発生時の影響　等



**②情報システムの対策実施状況・リスク評価結果**
- 情報システムの対策実施状況
- 現状についてのリスク評価結果　等



**③次年度以降の対策導入計画**
- 次年度の対策導入計画の概要（投資計画含む）
- 次年度以降の対策実施の推移（グラフ）
- 対策実施までの間の応急策　等



# 統一基準群改定案のポイント

## 現行の統一基準群の課題

◆毎年の改定により基準が複雑化・肥大化・形骸化

◆脅威の高度化・多様化や技術進展などの環境変化

## 改定の方向性(※)

◆統一基準群の実効性の向上

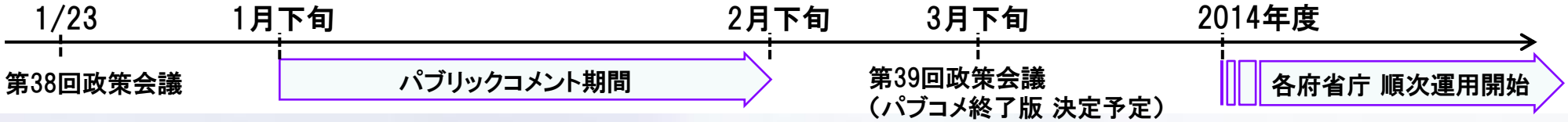
- 各府省庁が直面する情報セキュリティリスクを踏まえてCISO自らの判断で目標や実施計画を策定し、これに基づく対策の実施・評価・点検や、計画の見直しを行うよう求めることで、府省庁独自のPDCAサイクルによる自律的対策強化を図る。
- 定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人毎の遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく、守られやすい基準作りを目指す。

◆新たな脅威・技術への対応

- 標的型攻撃から守るべき重点業務・情報を特定し、攻撃の早期検知や、侵入後の活動を困難化するため、内部対策をリスクに応じて計画的に講ずる。
- 情報システムの構築等の外部委託の際、委託先における不正機能の混入などを防止するための管理体制を求める。
- 私物スマートフォン等の業務使用について、責任者の設置及び安全管理措置の規定により、厳格な管理を求める。
- SNS、グループメールサービス等の利用に際して責任者の設置、なりすまし防止対策の実施、機密情報の取り扱いの禁止等を求める。
- USBメモリ等について、ウイルス混入や紛失等の脅威に対抗するための利用手順を定めるよう求める。
- 複合機等のネット接続機器について、国際規格への適合や適切な設定等、必要な対策を講ずるよう求める。

(※「サイバーセキュリティ戦略」(平成25年6月情報セキュリティ政策会議決定)において決定された事項を踏まえ検討。)

## スケジュール(予定)



# 社会保障・税番号制度の導入に向けたロードマップ

2013年（H25年）　2014年（H26年）　2015年（H27年）　2016年（H28年）　2017年（H29年）

**制度構築**

- 番号法案提出
- 番号法整備法案提出
- 地方公共団体情報システム機構法案提出
- 内閣法等の一部を改正する法律案提出
- 法案成立
- 政省令等の整備
- 番号通知
- 個人番号カードの交付
- 順次、個人番号の利用開始

【2016年1月から利用する手続のイメージ】
○社会保障分野
・年金に関する相談・照会
○税分野
・申告書・法定調書等への記載
○災害対策分野
・要援護者リストへの個人番号記載
※ただし、事前に条例の手当てが必要

- 委員国会同意
- 特定個人情報保護委員会設置
- 委員国会同意
- 委員国会同意
- 委員会規則
- 情報提供ネットワークシステム、マイ・ポータルの運用開始
- 情報保護評価指針作成（情報保護評価SWG⇒委員会）
- 特定個人情報保護評価の実施・承認等
- 情報提供ネットワークシステム等の監査
- 2017年1月より、国の機関間の連携から開始し、2017年7月を目途に、地方公共団体との連携についても開始

**システム構築**

- システム要件定義・調達
- 調査研究
- 工程管理支援業務
- 設計
- 開発・単体テスト
- 総合運用テスト

**広報・広聴**

- 番号制度に関する広報・広聴

# マイナンバー法に基づく検討事項

行政手続きにおける特定の個人を識別するための番号の利用等に関する法律
（2013年5月31日法律第27号）

附則

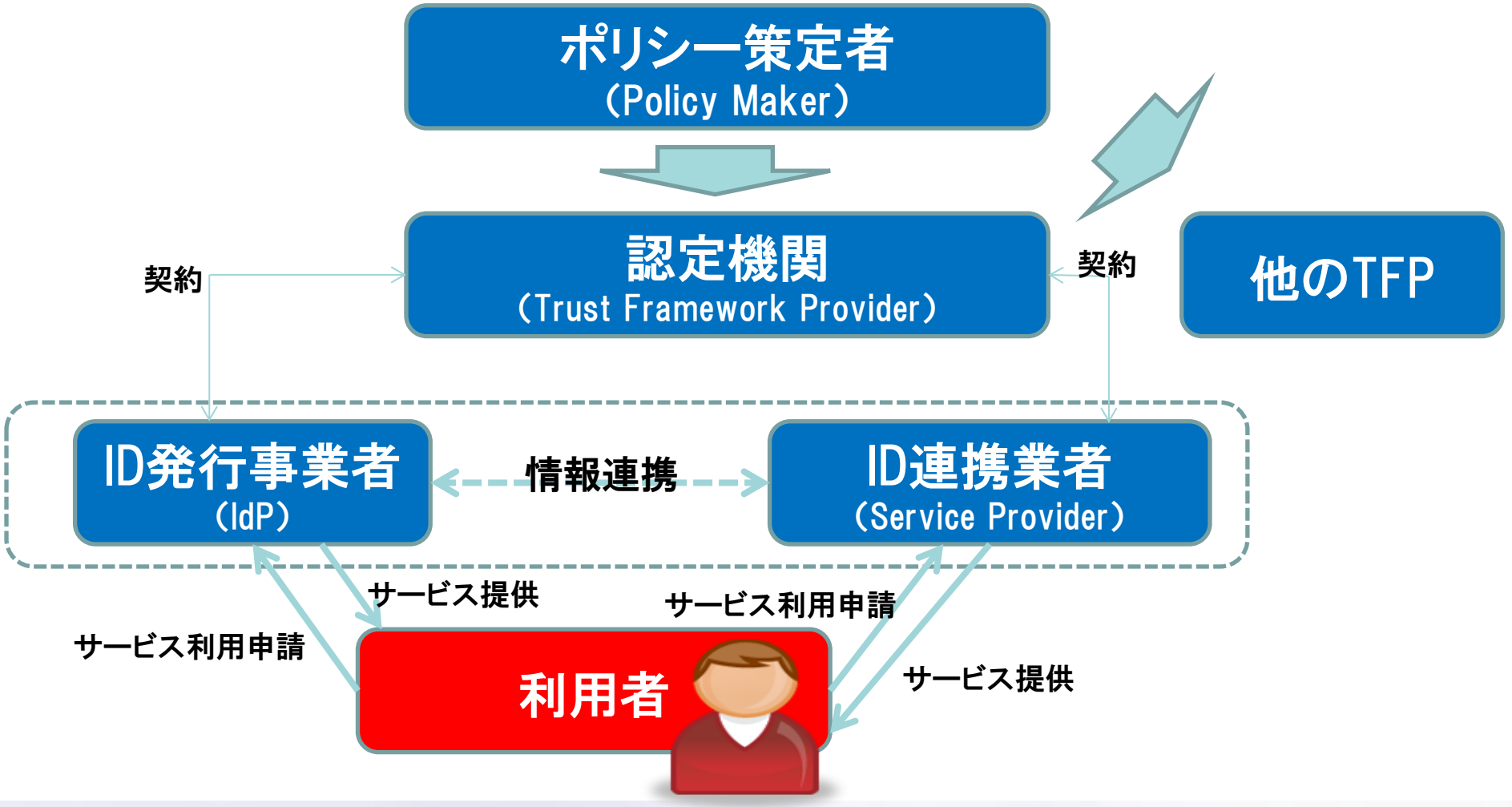
第6条　政府は、**この法律の施行後3年を目途**として、この法律の施行の状況等を勘案し、個人番号の利用及び情報提供ネットワークシステムを使用した**特定個人情報以外の情報の提供に情報提供ネットワークシステムを活用**することができるようにすることその他この法律について検討を加え、必要があると認めるときは、その結果に基づいて、国民の理解を得つつ、**所要の措置を講ずる**ものとする。

⇩

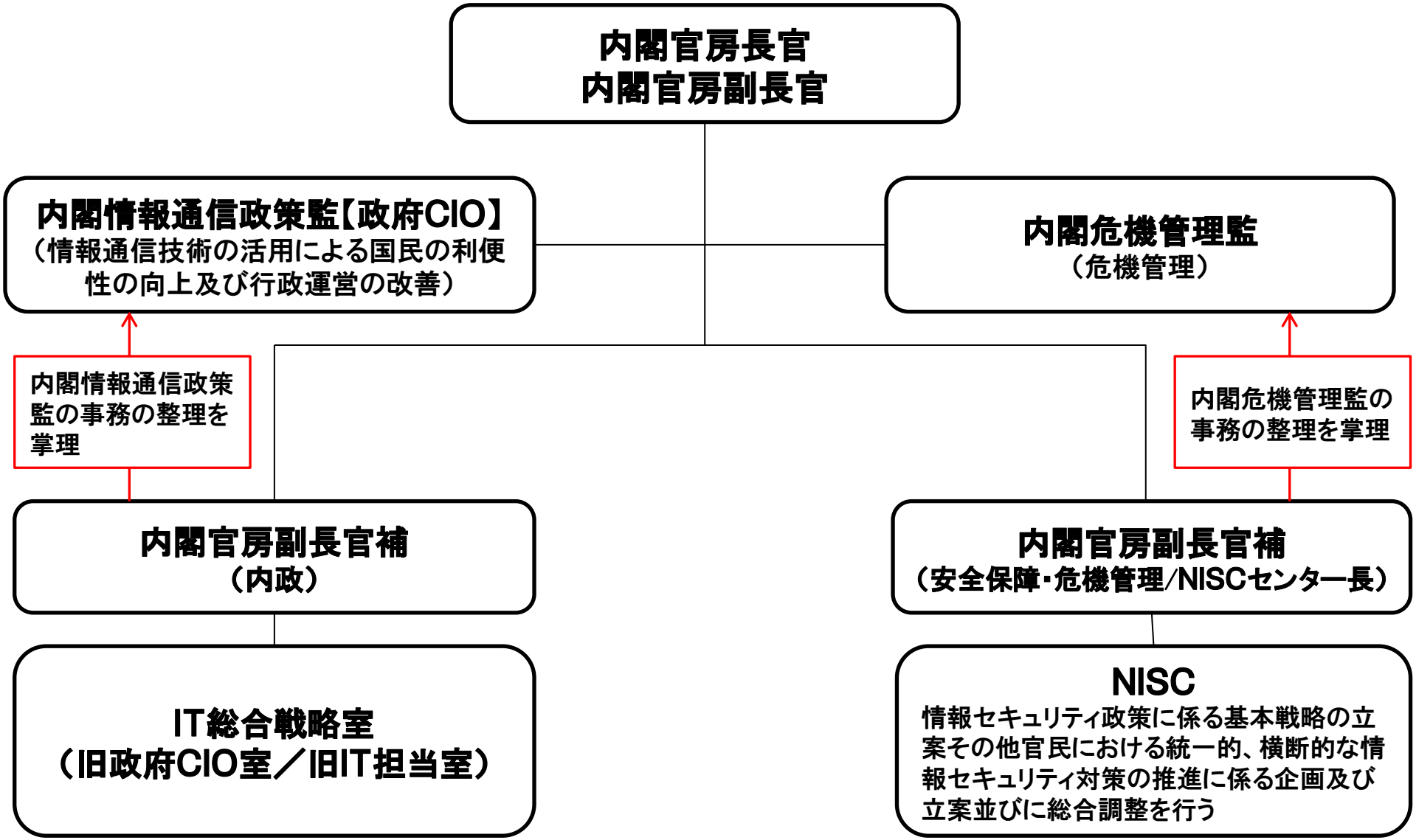
マイナンバーの利用範囲の拡大（例えば官民連携）について検討予定。

# トラストフレームワークの確立に向けて（新IT戦略）

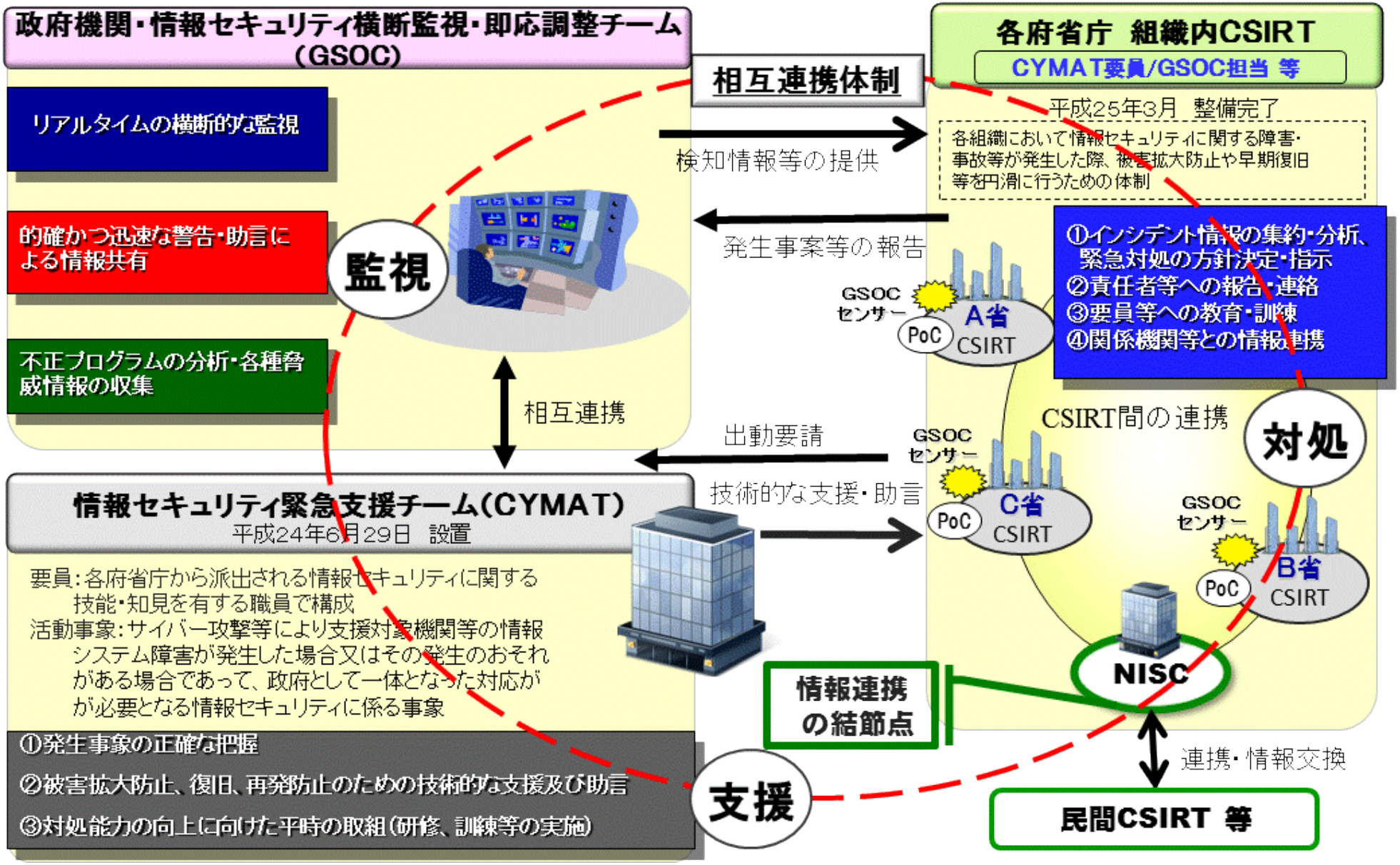
“電子行政サービスにおける認証の在り方を含め、スマートフォンやタブレット等を通じたITの活用を念頭に、本人確認手続き規定の類型化を図り、**契約締結や役務の利用に係る利用者の利便性向上とプライバシー保護、本人確認の正確性との担保との両立を図るオンライン利用を前提とした本人確認手続き等の見直しについて検討**する。”



# 政府CIOとの関係



# （2）GSOC/CYMAT/CSIRTの連携強化



# （３）①重要インフラに関する新たな「行動計画」の策定

## 官民連携による重要インフラ防護の推進

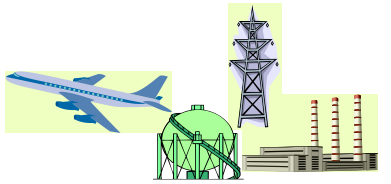
重要インフラにおけるIT障害が国民生活、社会活動に重大な影響を及ぼさないことを目指す

①予防的な対策と再発防止対策の両側から対処（具体的には、安全基準の整備、情報共有体制の強化など。）

②重要インフラ事業者等における情報セキュリティ対策の浸透状況や急速な技術進展等を踏まえたPDCAの促進

**重要インフラ（10分野）**

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流



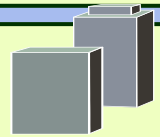
NISCによる
調整・連携

**重要インフラ所管省庁（5省庁）**

- 金融庁 [金融分野]
- 総務省 [情報通信分野、行政分野]
- 厚生労働省 [医療分野、水道分野]
- 国土交通省 [航空分野、鉄道分野、物流分野]
- 経済産業省 [電力分野、ガス分野]

**関係機関等**

- 情報セキュリティ関係省庁
- 事案対処省庁
- その他関係機関



## 重要インフラの情報セキュリティ対策に係る第2次行動計画

**重要インフラの範囲等を検討し、今年度に新たな「行動計画」を策定**

### （1）安全基準等の整備・浸透

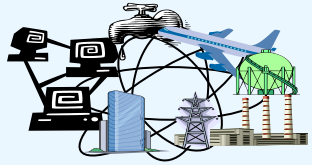
重要インフラ各分野に横断的な「指針」に基づいて、「安全基準」等の浸透を図る

### （2）情報共有体制の強化

情報の共有により、個々の主体による孤立した対応から、社会全体としての対応を促進

### （3）重要インフラ防護対策の向上

#### ①共通脅威分析



複数分野に共通する潜在的な脅威の分析

#### ②分野横断的演習

防護対策向上のための課題抽出

# （３）②「第３次行動計画（案）」の概要

## これまでの取組み

### 重要インフラ

「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの※」との定義　　※サイバーセキュリティ戦略（平成25年6月10日　情報セキュリティ政策会議決定）より抜粋

### 環境の変化

- IT依存度の高まり　→　システム障害時の影響の広範囲化・対応の困難化
- 複雑化・巧妙化するサイバー攻撃

### 行動計画の意義

重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画(注)　　（参考）第1次行動計画（平成17年12月13日 情報セキュリティ政策会議決定）
第2次行動計画（平成21年2月3日　情報セキュリティ政策会議決定）

（注）日本再興戦略-JAPAN is BACK-（平成25年6月14日閣議決定）及びサイバーセキュリティ戦略において今年度内に新たな行動計画を策定する方針を決定

## 重要インフラの情報セキュリティ対策に係る第２次行動計画

### 主な施策

1. 安全基準等の整備及び浸透
2. 情報共有体制の強化
3. 共通脅威分析
4. 分野横断的演習　　等

### 主な課題

社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在

1. 重要インフラ事業者等のPDCAサイクルとの整合に基づく指針の見直し
2. 大規模IT障害発生時の対応体制の明確化
3. 演習・訓練に係る関係主体の連携の在り方の模索
4. 環境変化・脅威に適切に対応するための取組
5. 広報公聴、国際連携の強化に追加すべき基盤強化に資する取組　　等

第２次行動計画の基本的な骨格を維持しつつ、
第２次行動計画の課題等を踏まえた修正・補強

## 重要インフラの情報セキュリティ対策に係る第３次行動計画（案）

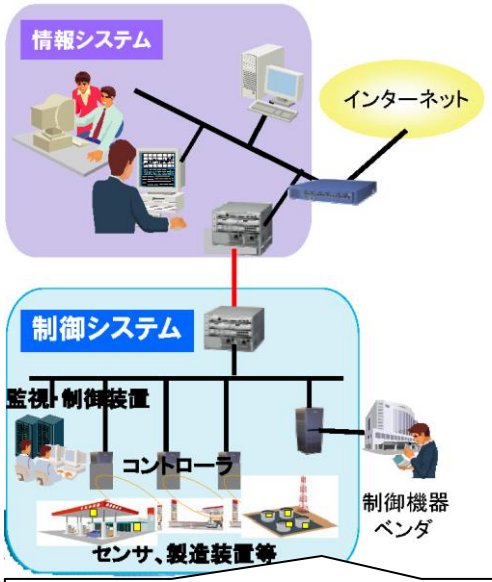
### 施策群の構成と主要なポイント

| | |
|---|---|
| **1．安全基準等の整備及び浸透** | 対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求 |
| **2．情報共有体制の強化** | 平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化 |
| **3．障害対応体制の強化** | 関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化 |
| **4．リスクマネジメント** | 重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援 |
| **5．防護基盤の強化** | 関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　　等 |

**◆ 重要インフラ分野を現行の10分野から13分野に拡大（化学、クレジット及び石油の各分野を追加）**
**◆ 行動計画の要点として、「経営層に期待する在り方」等を示すとともに、PDCAサイクルに基づく事業者等の対策例とこれに関連する国の施策を一覧化**
**◆ 客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施**

＜今後の予定＞ パブリックコメント（１月下旬～２月中旬頃）を行った上で、次回会合にて決定いただく予定

# 制御システムの普及




## 従来

制御システムは事業者毎に固有の仕様部分が多く、詳細な内部仕様等を把握できない限り、外部からの攻撃は難しいものであった。

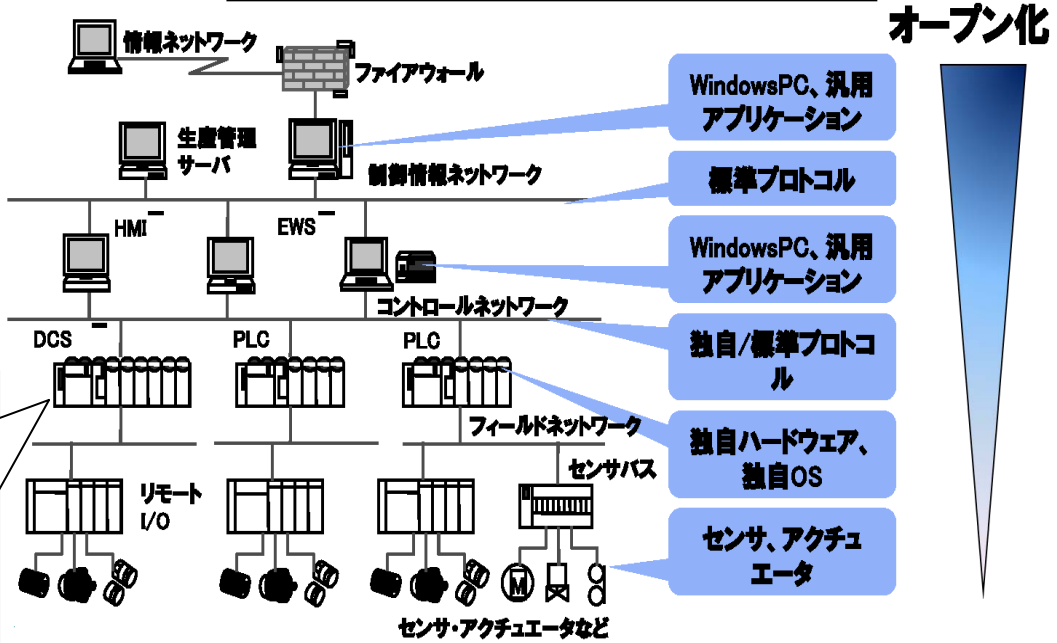
## 最近の状況

○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
○ 外部ネットワークにも接続されるようになっている。
○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。

○ 生産の自動化や、フィードバック制御による入力値の自動制御等、様々な用途で工数の軽減や正確性の向上を目的に利用。
○ 最近は、一般的な情報システムが接続するオフィスネットワークから、制御情報系ネットワーク、制御ネットワークを介して、制御システムのコントローラやセンサーまでを間接的に接続するような構成が多い。

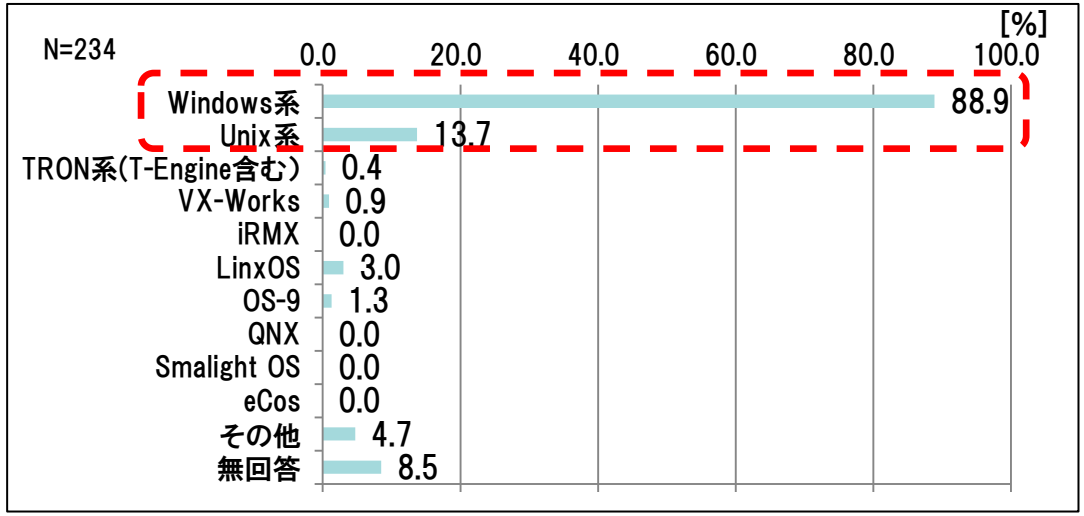
○ アプリケーション等が動作する上層のレイヤではWindowsのパソコン等のクライアント端末や汎用アプリケーション、標準プロトコルを利用。
○ 実際の制御に関わる下層部分は独自のプロトコルやハードウェア、OSが利用される割合が高く、固有の仕様により構成。
○ オープン化が上層部から徐々に進行。

## オープン化が進む制御システムの構成

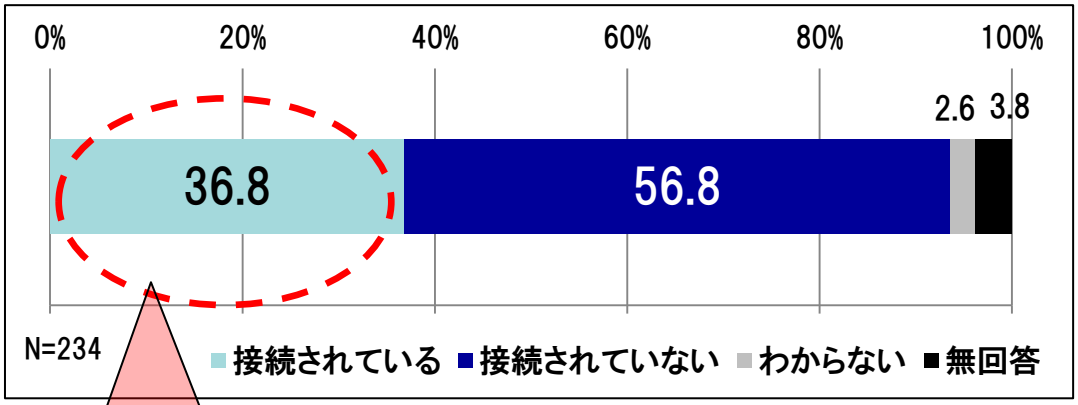



【出典：独立行政法人情報処理推進機構「制御システムセキュリティ国際標準の現状と日本の取組み」（2011年11月18日）http://www.ipa.go.jp/files/000025094.pdf】

# 各種製造装置における汎用IT技術の利用状況

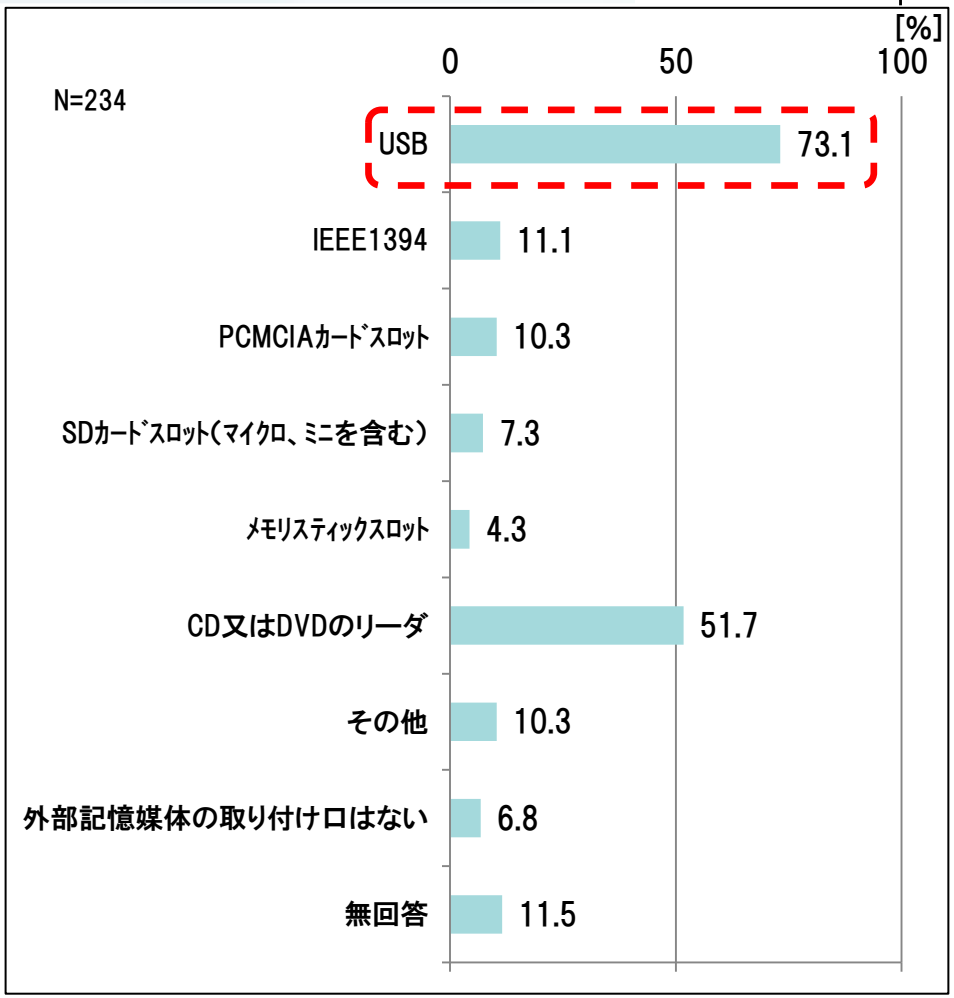



プラント設備でのOSの利用状況（端末）




外部ネットワークとの接続

このうちインターネット接続が43%
リモートメンテナンス回線接続が55%




プラント設備での外部メディアの取り付け口の有無

【出典：経済産業省「工業用装置等における汎用IT技術応用に起因する驚異と対策に関する実態調査事業　報告書」（平成21年３月）」】

# 制御システムに関するセキュリティ強化の取組

**技術研究組合制御システムセキュリティセンター**(CSSC:Control System Security Center)**の設立（2012年３月）**

○ 制御システムのセキュリティを高める技術の研究開発
　～ 防御、減災、回復
○ 制御機器の安全性の検証
　～ サイバー攻撃の再現
　～ 機器やシステムが守るべき基準作り（国際標準化）
　～ 組合員の製造する制御機器の安全性の検証、認証
○ 模擬プラントを使った人材育成・普及啓発
　～ 経営者の意識改革、～ 現場の人材教育、運用法の改善


組合員18社（2013年５月17日現在）
ユーザ企業、制御ベンダ、セキュリティベンダ等

【出典：技術研究組合制御システムセキュリティセンター
http://www.css-center.or.jp/pdf/about_CSSC_ppt.pdf】

○ 制御システムセキュリティの国際標準に基づく評価・認証機関設立
　日本国内で制御関連デバイスのセキュリティ評価について、パイロット認証等の実施を経て体制を確立し、CSSCを中心とした制御システムのセキュリティに関する評価・認証機関の設立を目指す。

○ 制御システムセキュリティ評価・認証の利活用に向けた検討
　CSSCによる制御システムのセキュリティに関する評価・認証を受けたシステムの導入を推進するための制度整備を進める。

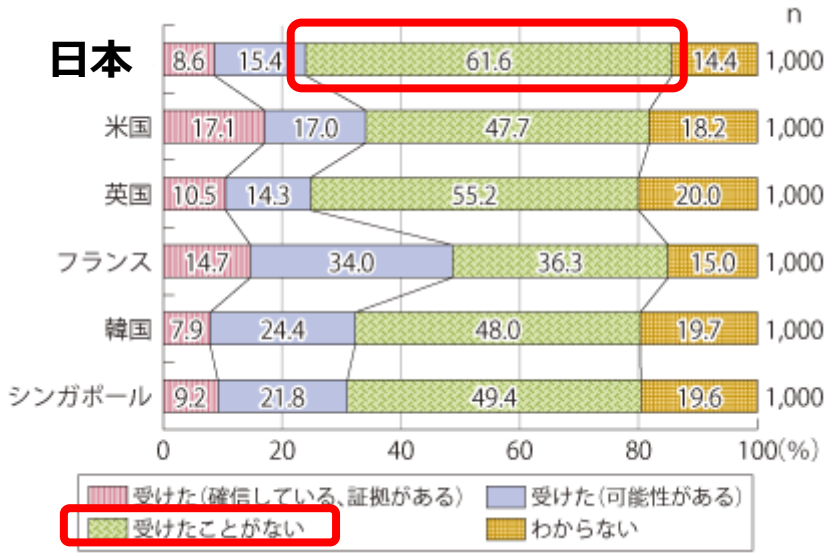
○ 制御システムセキュリティに関する研究開発
　CSSCが宮城県多賀城市に構築したテストベッド施設を中核として、制御システムのセキュリティ検証方法及び第三者による評価・認証方法に関する研究開発に取り組み、日本発の技術的基盤を確立する。

○ 制御システムセキュリティに係る人材育成
　CSSCのテストベッド施設を活用し、制御システムセキュリティに係る人材育成のための研修等を実施する。

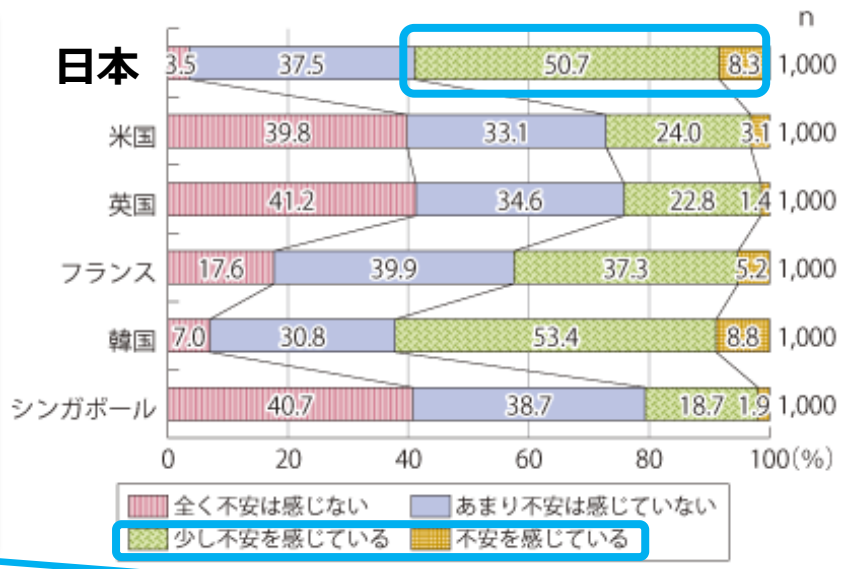
# （４）①普及啓発プログラムの改定

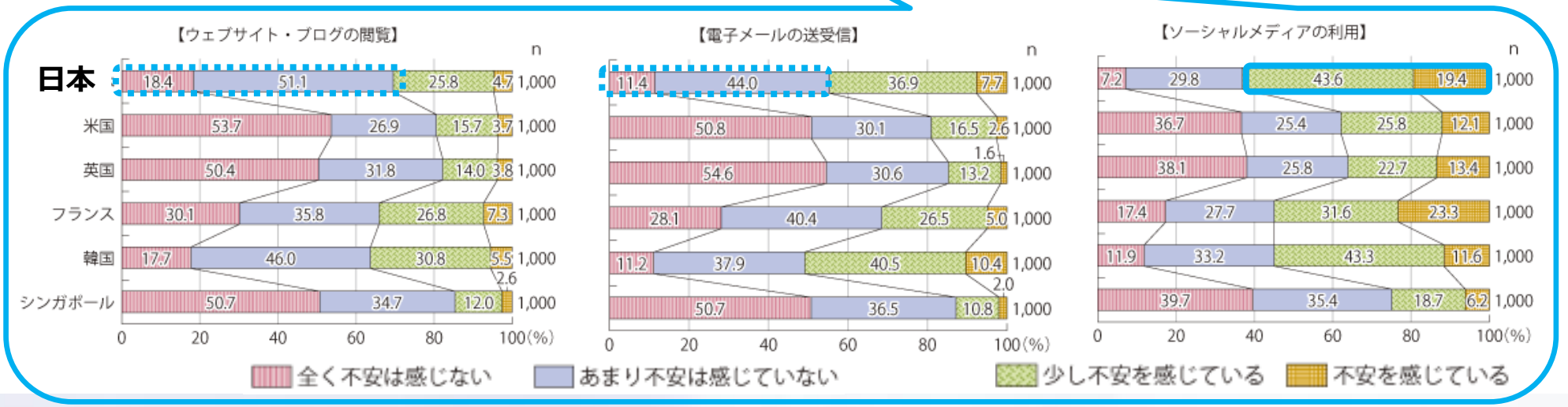
● 諸外国と比べ、情報セキュリティ被害の経験は少ないが、ソーシャルメディアの利用を中心にインターネット利用への不安感は高い。他方、ウェブサイトや電子メール等に関しては高くない。

## 情報セキュリティ被害の経験




## インターネット利用への不安感

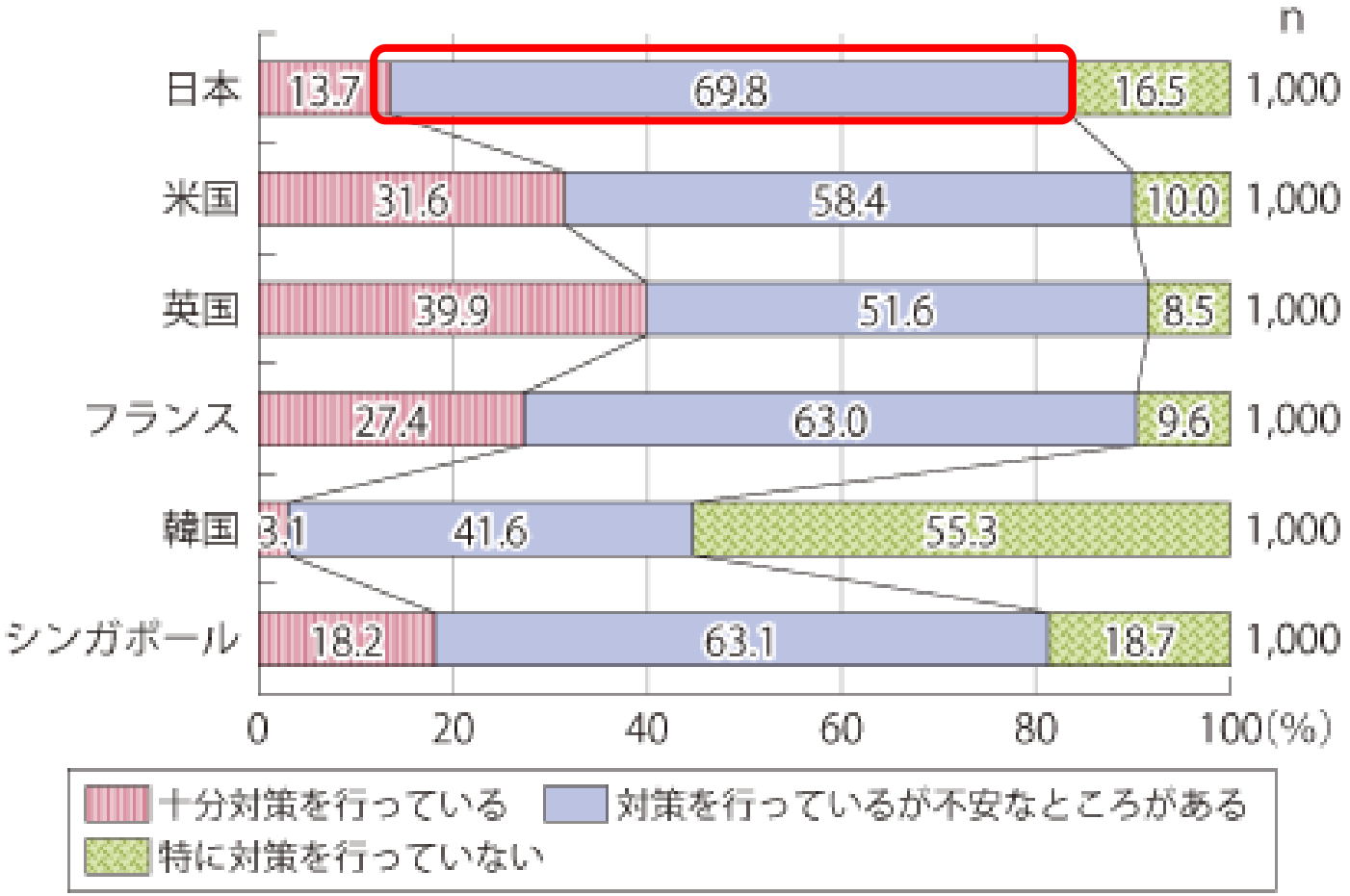



【出典】平成25年情報通信白書

# （４）②普及啓発プログラムの改定

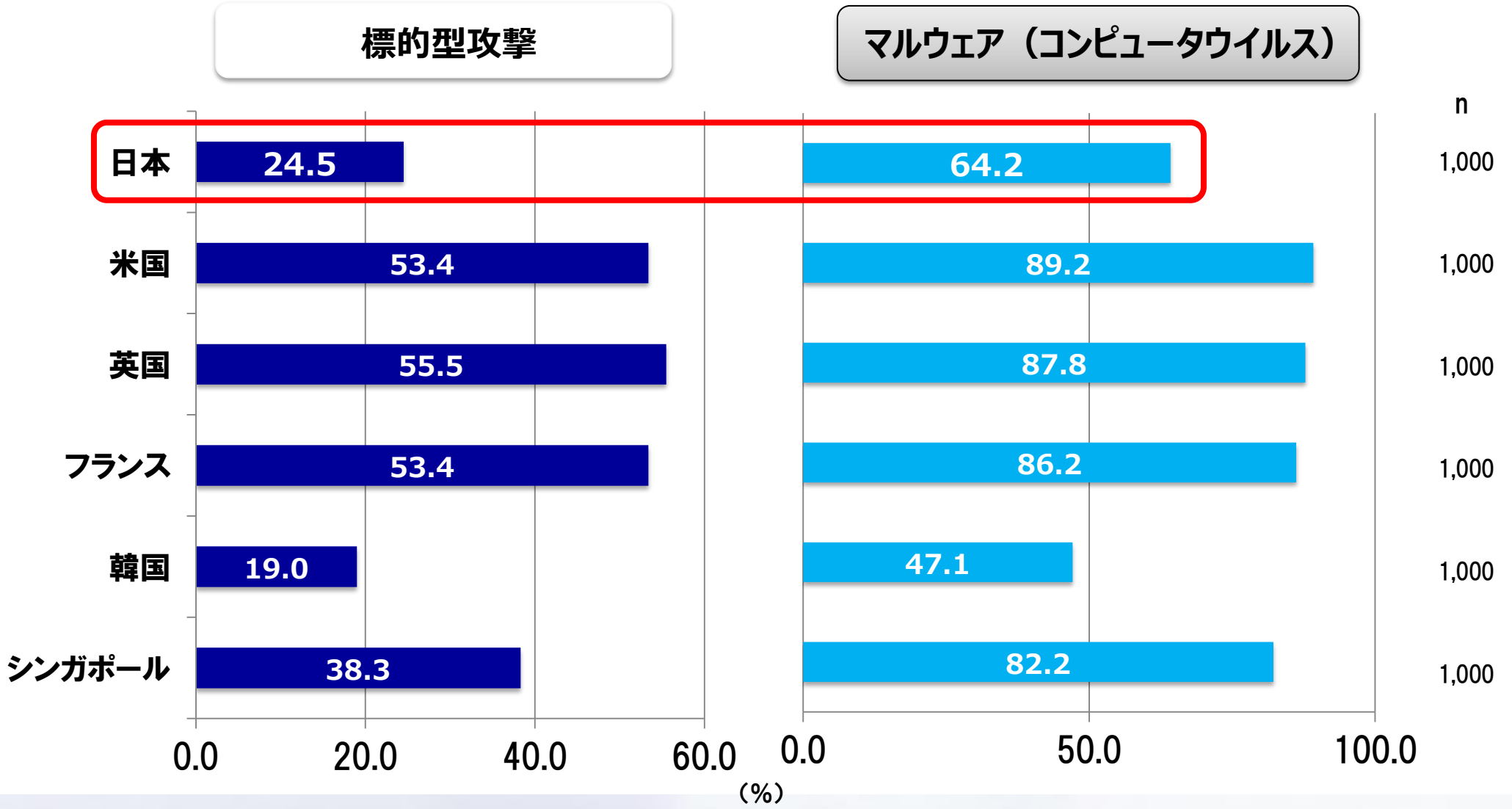
- 日本の利用者は約７割が情報セキュリティ対策を講じているが、不安を抱えている。




【出典】平成25年情報通信白書

# （４）③普及啓発プログラムの改定

● 諸外国と比べ、インターネット上の脅威について、標的型攻撃やマルウェア（コンピュータウイルス）に対する認知度が低い。




【出典】平成25年情報通信白書

# （５）①人材育成プログラムの改定

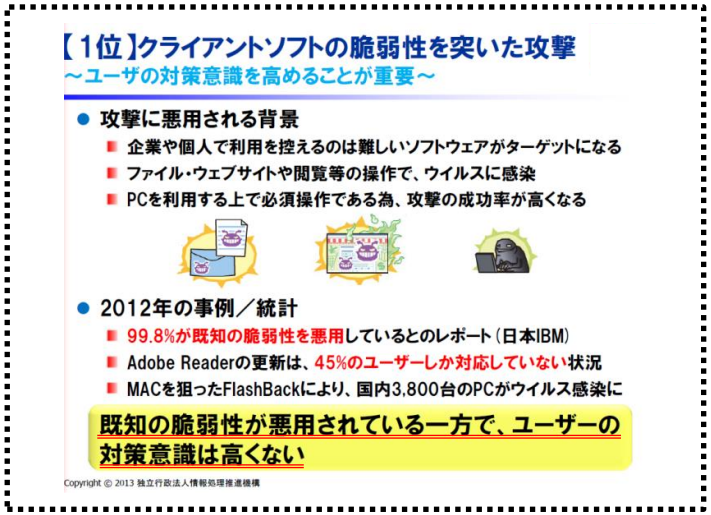
現在の
情報セキュリティ技術者
約26．5万人

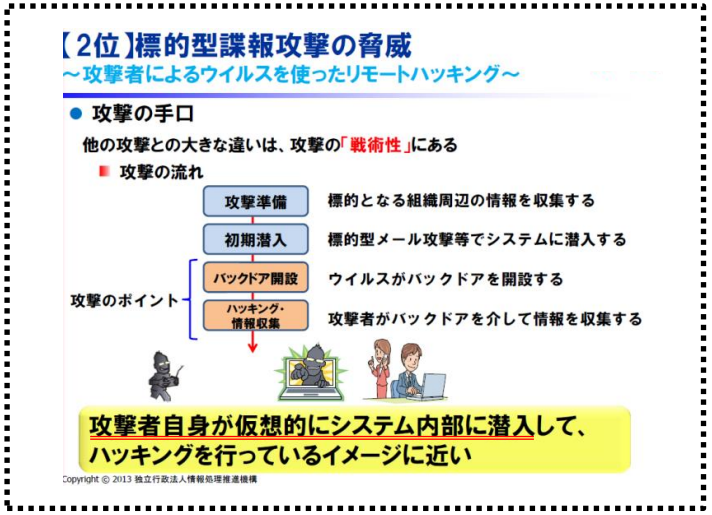
質的不足　うち約16万人の能力不足

量的不足　さらに約8万人の人材不足

と企業は感じている。
（IPA試算）

一方、ユーザーの低い対策意識やシステムの脆弱性を突いた攻撃の脅威は増加。




IPA「10大脅威」
（2013年度版）より

＊IT人材白書2013(IPA)

IT人材　国内約106万人＊
（うち約80万人がSE）

高度人材
（左のうち一部）

【対象としたセキュリティ教育】
・スキル標準の策定・資格制度等による間接的な支援
・普及啓発セミナー等の開催　等にとどまる

【対象としたセキュリティ教育】
・未踏人材 ・ enPiT・ SECCON
・セキュリティキャンプ・キャリアパス事例集
等比較的多い

# （５）②人材育成プログラムの改定

## サイバーセキュリティ戦略で示された課題

情報セキュリティに係るリスクの深刻化に対応し、情報セキュリティ水準の向上を図るためには、

○人材の量的不足の解消に向け 積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題。

○そのためには、社会全体で育成し活用するための仕組みが必要。

### 人材の量的・質的不足

情報セキュリティ従事者 約26.5万人

うち質的不足 約16万人

さらに量的不足 約8万人

⇒これら人材の雇用の受け皿も不可欠

## 取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

### 【需要】経営層の意識改革

○経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。

○製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

### 【供給】人材の「量的拡大」と「質的向上」

○実務を担うボリュームゾーンに当たる既存のIT技術者に、情報セキュリティを必須能力として位置付ける。

①技術者に情報セキュリティを意識させるための取組

②情報セキュリティ能力の評価基準・資格等の整備

③情報セキュリティの実践的スキル向上のための取組

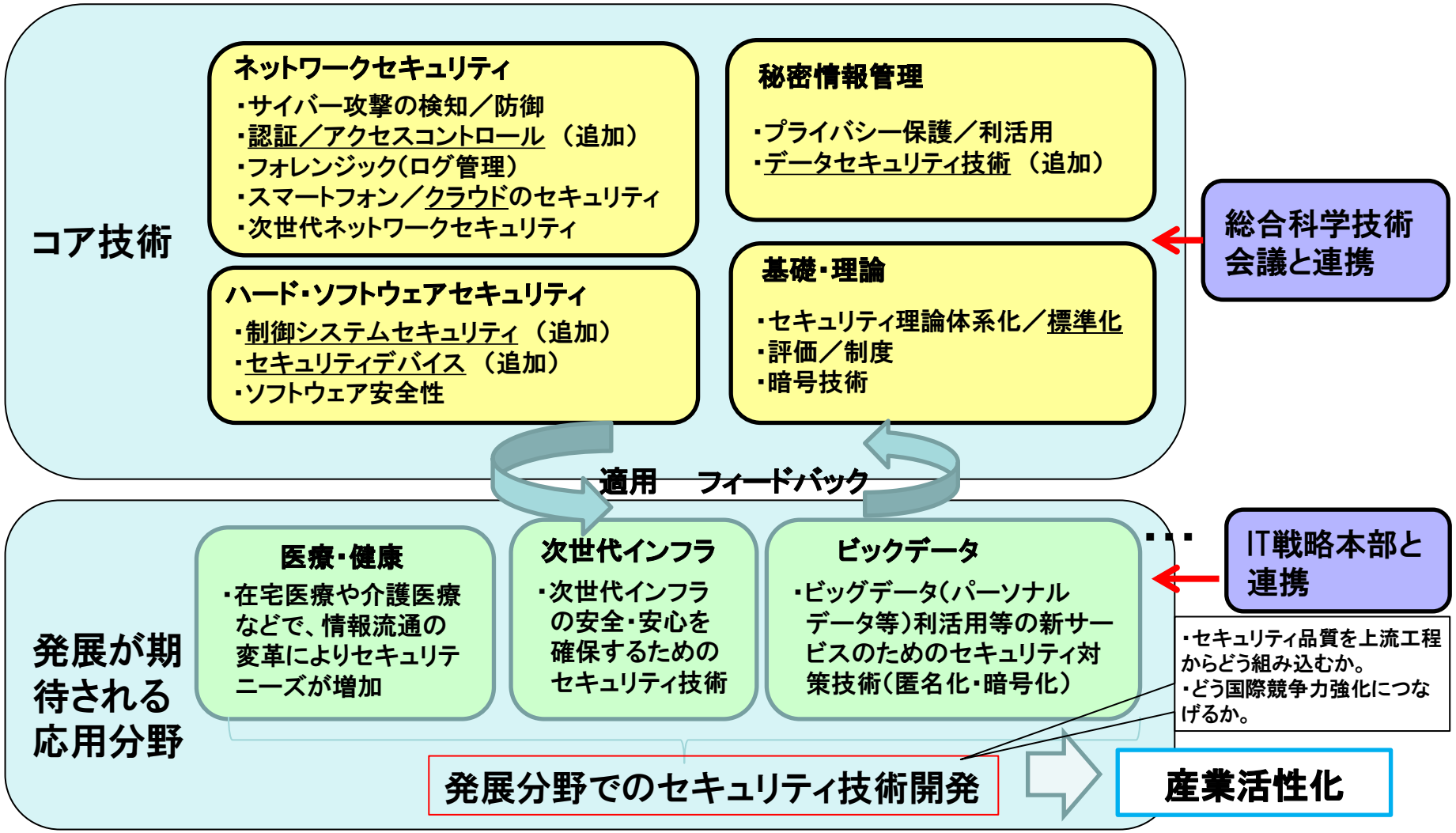
○グローバル化する脅威に対応できる、高度な人材や突出した能力を有する人材を育成・発掘。

①高度な専門性を持った情報セキュリティ人材育成のための高等教育の強化

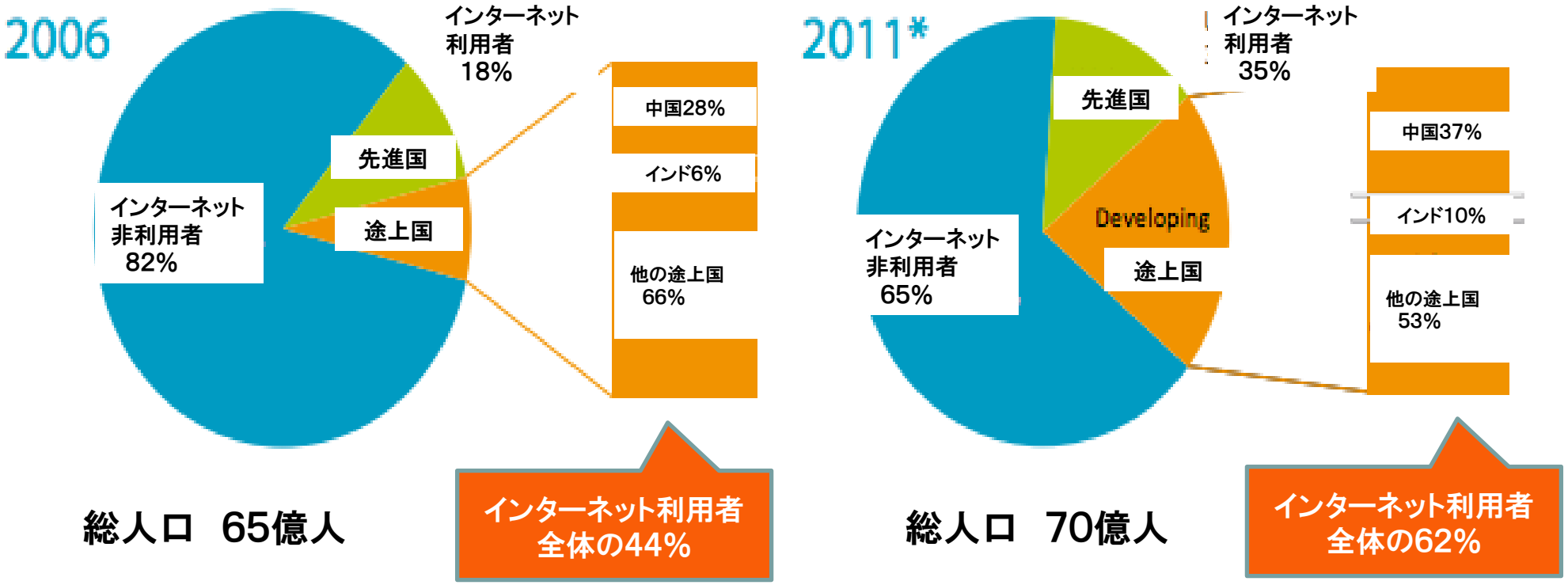
②最先端の分野で活躍する突出した人材の発掘及び更なる能力向上

○とりわけ、政府機関等においては、訓練・演習等による内部人材の育成、優秀な外部人材の登用に率先して取り組む。さらに、調達における情報セキュリティの要件化等を通じ、我が国のセキュリティ水準の向上、人材の需要喚起につなげる。

# （6）研究開発戦略の改定に向けた検討



# 世界のインターネット利用者数




＊　推計値

出典　ITU World Telecommunication / ICT Indicators database

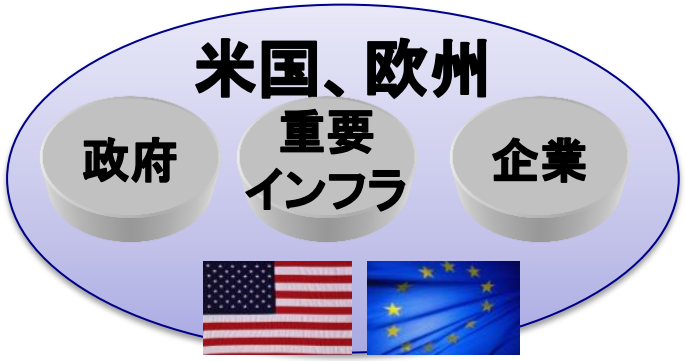
http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

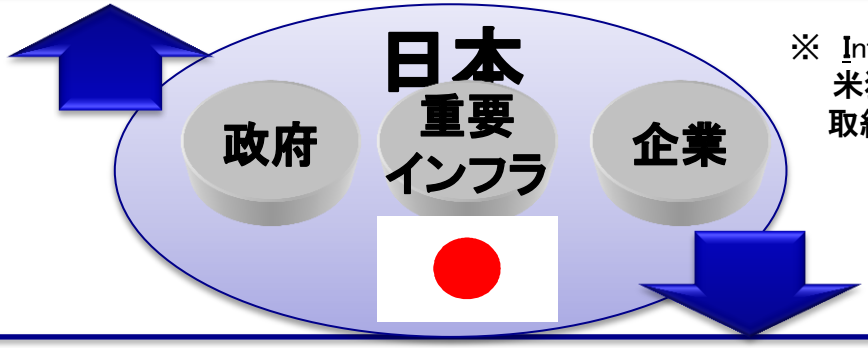
# （７）サイバーセキュリティに関する国際戦略の策定

**サイバー空間の国際的な規範形成に関する議論、最先端の知見の共有等のフェーズ**

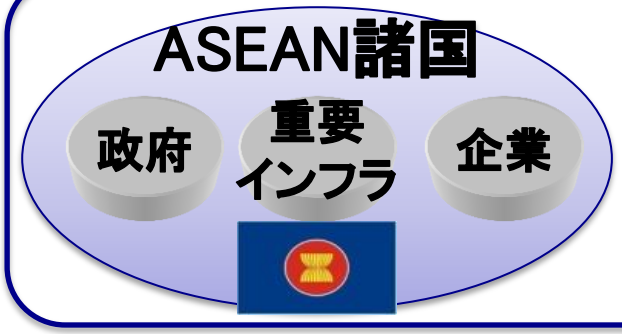
（代表例）日米サイバー対話（2013年第4四半期）
IWWN※会合
サイバー空間に関するソウル会議（2013年10月）

・官民連携等のベストプラクティス共有
・国際サイバー演習
・サイバー空間の安定的利用のための新たな国際的規範の検討　等




※ International Watch and Warning Network：
米独等の先進15カ国による、サイバー脅威対応の取組を議論する会合。国際演習等を実施。




**セキュリティレベルの底上げフェーズ**

（代表例）日・ASEAN情報セキュリティ政策会議（2013年9月閣僚会議）

・ASEAN地域のセキュリティマネジメント体制の確立、維持、改善
・セキュリティ対応組織（CSIRT※）の構築支援
・意識啓発　等

# サイバーセキュリティ国際連携取組方針（１３年１０月、情報セキュリティ政策会議決定）

## 策定方針の決定

**日本再興戦略 -JAPAN is BACK-　（平成25 年6月14 日閣議決定）（抄）**

4. 世界最高水準の IT 社会の実現　⑤サイバーセキュリティ対策の推進

世界最高水準の IT 社会にふさわしい、強靭で活力あるサイバー空間を構築するため、「サイバーセキュリティ戦略」を踏まえ、政府機関や重要インフラにおけるセキュリティ水準及び対処態勢の充実強化や国際戦略の推進等、サイバーセキュリティ対策を強力に展開する。

〇サイバーセキュリティに関する国際戦略の策定

- 我が国と戦略的に強い結び付きのある国・地域との多角的パートナーシップの強化、我が国が強みを持つセキュリティ技術の国際展開等を政府一体となって加速させるため、**今年度中に、「情報セキュリティ政策会議」において新たにサイバーセキュリティ国際戦略を策定する**とともに、来年度中に制御システム等のセキュリティの国内での評価・認証を開始し、インフラの整備・輸出等を促進する。

**サイバーセキュリティ戦略　（平成25年6月10日情報セキュリティ政策会議 決定）（抄）**

４　推進体制等　（2）評価等

本戦略に基づく各種取組施策の確実な実施及び各施策間の有機的な連携を確保する観点から、サイバーセキュリティ立国の実現に向けた中長期の目標の管理を行うとともに、本戦略に基づき、2013年度から毎年度の年次計画及び**サイバーセキュリティに関する国際戦略を策定する**。

## サイバーセキュリティ国際連携取組方針を策定

- サイバーセキュリティ政策で我が国として重視する国際連携に関する方針の明確化
- 我が国として具体的な貢献分野を訴求
- 重点的な取組地域（アジア太平洋、欧米等）を具体的に明示

## バイ・マルチの政策対話において日本のスタンスをアピール

# ASEANにおけるICTの現状

## ASEAN ICTマスタープラン2015

2015年を目標年次としたASEAN域内のICTの発展を目的としたプラン。2011年1月に開催された、ASEAN情報通信大臣会合において策定、公表。

**情報セキュリティの促進**
- ネットワークセキュリティの共通基準の確立
- CERT(※)間協力
- データ及び情報保護のベストプラクティス共有　等

※　Computer Emergency Response Teamの略。
サイバー攻撃発生時等の連絡窓口となり、また、その際の対処を行う専門組織

### マスタープランの概要

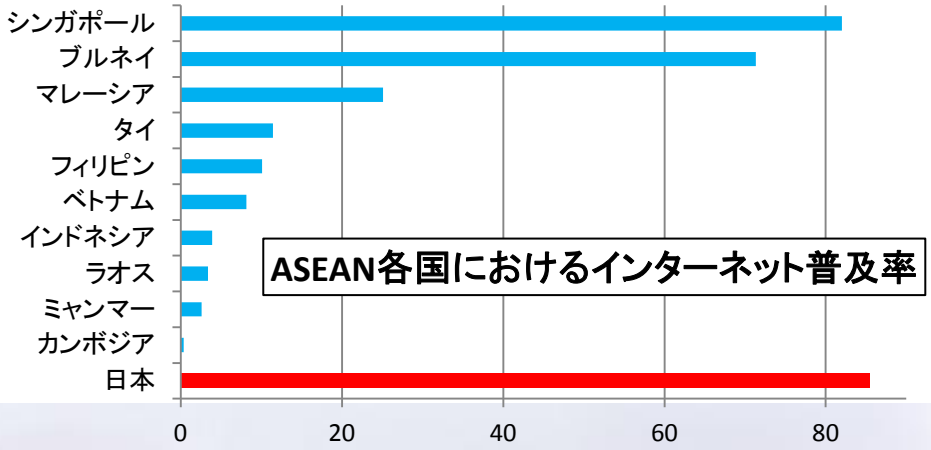
**ビジョン**
ICTによる経済の強化と変革に向けて
包括的、活気のある、統合化されたASEANの構築

**取組の柱**
1. 経済の変革
2. 人材強化と雇用
3. イノベーション

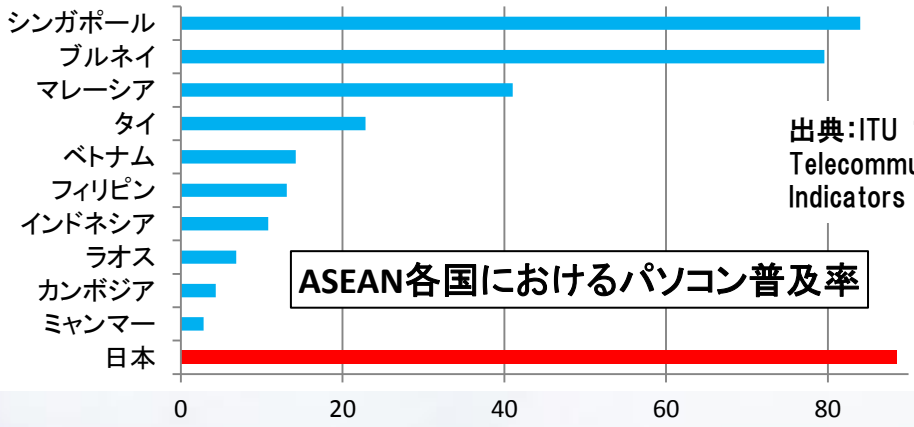
**基盤的取組**
4. インフラ開発
5. 人材開発
6. デジタルディバイドの解消

## ASEANにおけるICTインフラの現状

ASEAN各国におけるインターネット普及率とパソコン普及率については、国によって大きなばらつきがある。



ASEAN各国におけるインターネット普及率



ASEAN各国におけるパソコン普及率

出典：ITU ‘World Telecommunication/ICT Indicators database 2011’

# 国際連携に向けた政策対話の推進

## EU
●重要インフラ防護や官民の情報共有等の取組の共有、意識啓発や政策動向の意見交換
●第1回日EUｲﾝﾀｰﾈｯﾄｾｷｭﾘﾃｨﾌｫｰﾗﾑ：平成24年11月

## ロシア
●サイバーセキュリティ等安全保障・防衛分野での協力や交流の深化
●日露外相会談：本年4月

## 基本的な考え方
「情報の自由な流通の確保」という基本的な考え方の下、民主主義、基本的人権の尊重及び法の支配といった価値観を共有する国や地域とのパートナーシップ関係を多角的に構築・強化。

## イギリス
●国際規範づくり、安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護、経済・社会的側面の取組等に関する意見交換
●第1回日英サイバー協議：平成24年6月

リスクのグローバル化

## 国際戦略の策定
●多角的なパートナシップの強化や技術の国際展開等の加速化

## アメリカ
●脅威認識の共有、国際規範づくり、重要インフラ防護、防衛分野のサイバー課題等に関する意見交換
●第2回日米サイバー対話：**本年第4四半期@D.C.**

## インド
●安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護、経済・社会的側面の取組に関する意見交換
●第1回日印サイバー協議：平成24年11月

## ASEAN
●意識啓発、人材育成、技術協力、情報共有体制の構築等での連携
●サイバーセキュリティ協力に関する閣僚政策会議：**本年9月@日本**
●共同意識啓発活動の実施：**本年10月**

## 多国間・マルチステークホルダーの取組み

### サイバー空間の国際規範づくり等に関する会議
●サイバー空間における自由と安全保障の両立、開放性や透明性、マルチステークホルダーの重要性、サイバー空間における国際行動規範づくり，サイバー犯罪条約，キャパシティ・ビルディング、サイバー空間における従来の国際法や国家間関係を規律する伝統的規範の適用、信頼醸成措置等に関する対話。　●60ヵ国の政府機関，国際機関，民間セクター，NGO等が参加。　●ソウル会議：**昨年10月@ソウル**

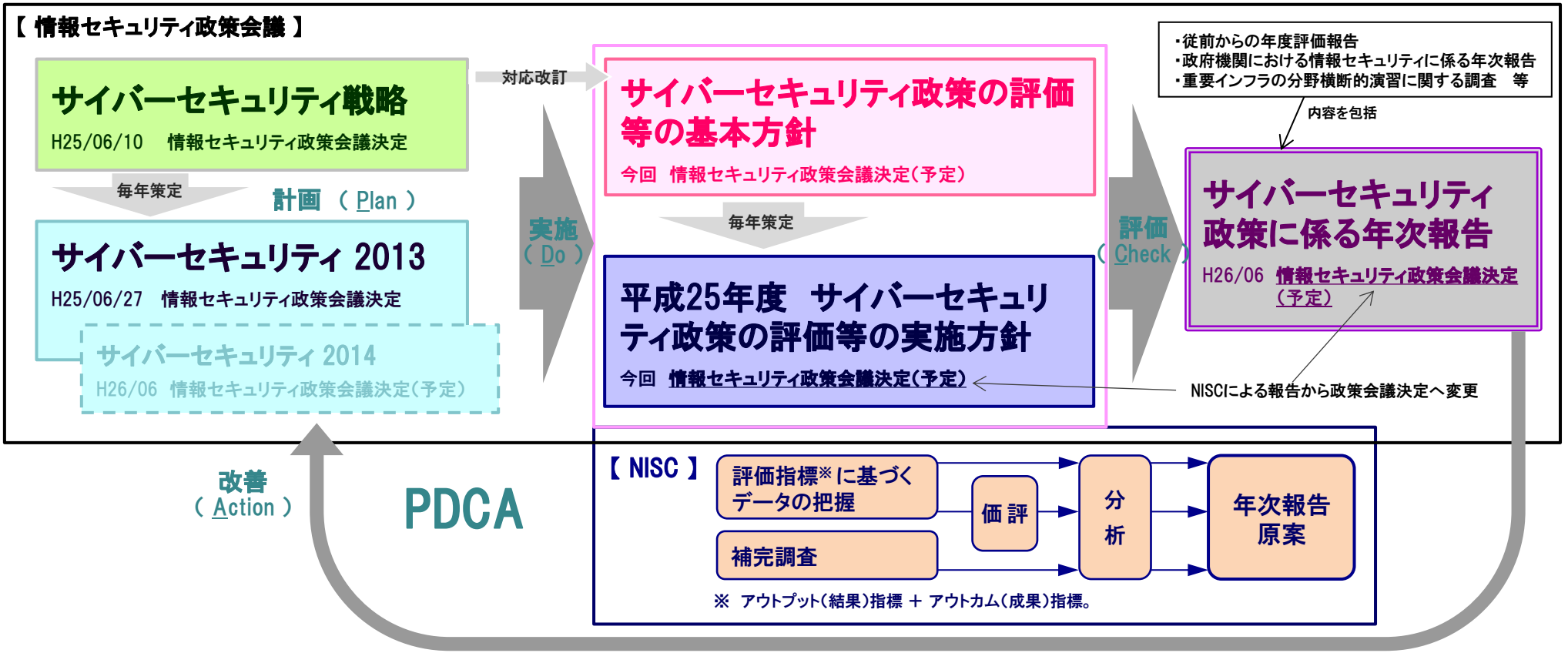
### MERIDIAN
●重要インフラ防護等のベストプラクティスの共有や国際連携方策等に関する意見交換。
●米・英・独・日等の重要インフラ防護担当者が参加。

### IWWN
●サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。
●米・独・英・日等の政府機関、CERTが参加。

# サイバーセキュリティ戦略の評価等の基本方針（２０１４年1月）

## サイバーセキュリティ政策に係る年次報告

- 従前からのNISCによる年度評価報告に代えて、情報セキュリティ政策会議が「サイバーセキュリティ政策に係る年次報告」を策定・公表することとし、「サイバーセキュリティ戦略」（平成25年6月10日情報セキュリティ政策会議決定）に対応する「サイバーセキュリティ政策の評価等の基本方針」、「平成25年度　サイバーセキュリティ政策の評価等の実施方針」を策定する。
- 年次報告には政府機関や重要インフラ事業者等における他の調査結果も可能な範囲で取り込み、包括的な内容とする。



# IT利活用セキュリティ総合戦略部会の開催

## 高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

本部長　内閣総理大臣
副本部長　情報通信技術（ＩＴ）政策担当大臣
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
内閣情報通信政策監（政府CIO）
有識者

（事務局）
**内閣官房　IT総合戦略室**
室長（政府CIO）

連携

## 情報セキュリティ政策会議

### IT利活用セキュリティ総合戦略推進部会

- IT政策担当大臣が主催。各専門委員会等の有識者から構成。
- 討議結果は、IT政策担当大臣より政策会議に報告・提言。
- IT総合戦略室の協力を得て、NISCが実施。

| | |
|---|---|
| 技術戦略専門委員会 | 研究開発戦略（本年央に見直し） |
| 普及啓発・人材育成専門委員会 | 人材育成プログラム（本年度中に改定） |
| 情報セキュリティ対策推進会議（CISO等連絡会議） | 政府機関統一基準（本年度中に改定） |
| 重要インフラ専門委員会 | 重要インフラ行動計画（本年度中改定） |

現在検討中の主な事項

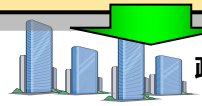
（事務局）
**内閣官房 情報セキュリティセンター（NISC）**
センター長
（内閣官房副長官補（事態））
副センター長（内閣審議官）
内閣参事官6名
情報セキュリティ補佐官
情報セキュリティ緊急支援チーム（CYMAT）

協力

協力
5省庁
- 警察庁（サイバー犯罪の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

*その他の関係省庁*
重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他
文部科学省（セキュリティ教育）　等


重要インフラ事業者　等


政府機関（各府省庁）


企業


個人

# 今後のＩＴ利活用を見据えたセキュリティ対策に関する論点

2020年オリンピック・パラリンピック東京大会の安心、安全、確実な開催のためには、
社会インフラ等における情報システム等ＩＴの利活用の促進とそのセキュリティの確保が不可欠

**技術戦略専門委員会及び普及啓発・人材育成専門委員会における取組状況等を踏まえ、下記の課題について検討する。**

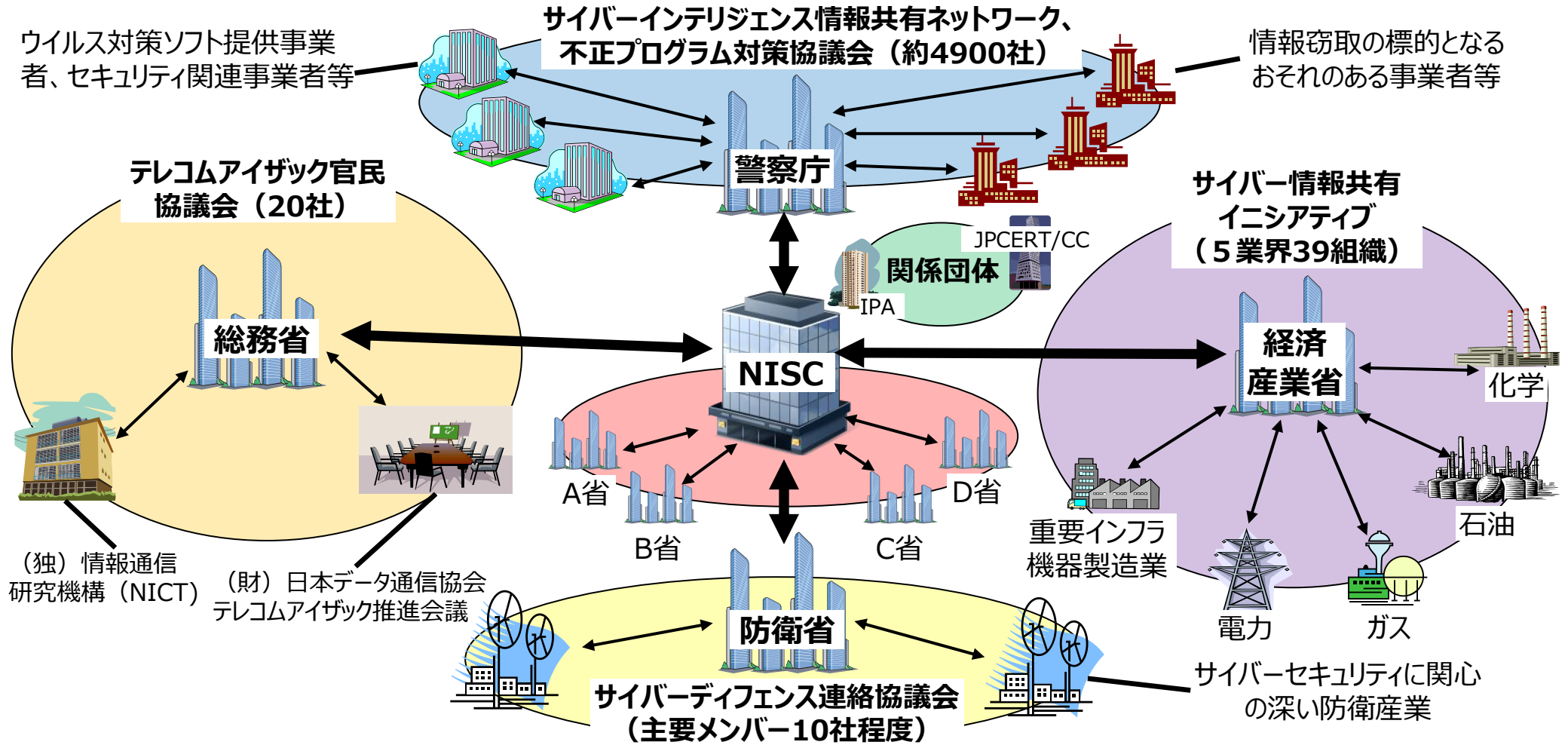
2020年に向けて新たなＩＴサービスが登場することが予想されるところ、これらの利便性向上のためには、各サービスの認証を連携させる必要があるのではないか。


様々な分野で利活用されるＩＴの安心、安全を確保するためには、サイバーセキュリティ技術研究開発・実証実験等のための投資を集中的に実施する必要があるのではないか。

新たなセキュリティ技術を支えるためには、コンピュータサイエンスを身に着けた人材の育成を強化する必要があるのではないか。

**本年夏頃を目途に提言を取りまとめる**

# 官民の情報共有の促進に向けて



# Any question?