

# わが国のサイバーセキュリティ戦略

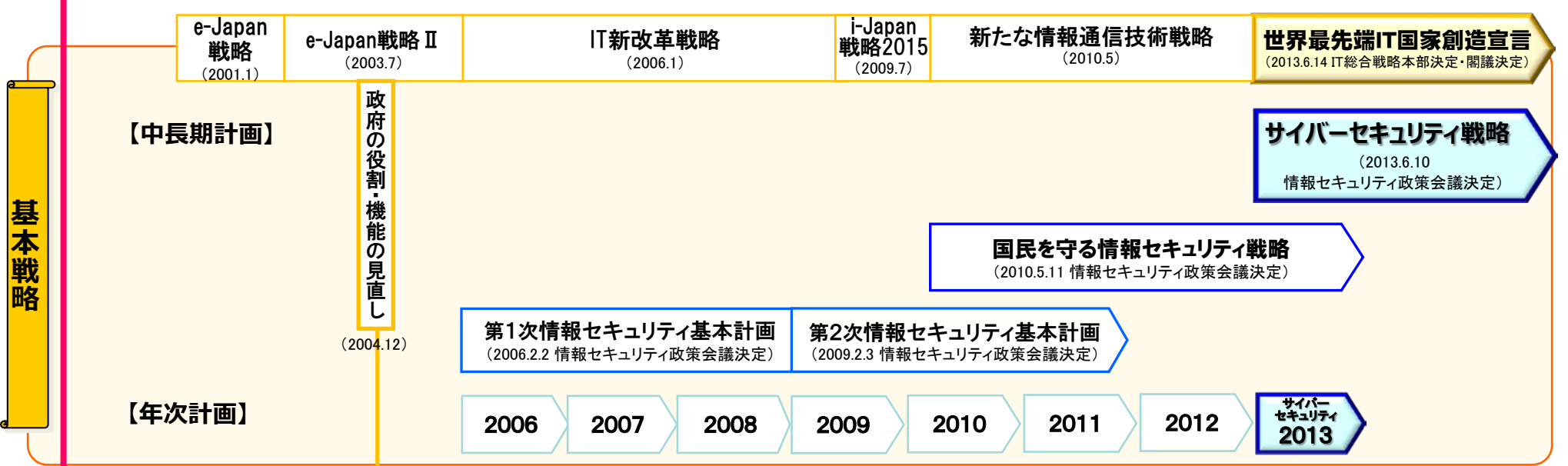
2014年7月3日

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/>

# 我が国における基本戦略・推進体制の推移



# 我が国における推進体制



## 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)

## 情報セキュリティ政策会議 (2005年5月に設置)

**議長** 内閣官房長官  
**議長代理** 情報通信技術 (IT) 政策担当大臣  
**構成員** 国家公安委員会委員長  
 総務大臣  
 外務大臣  
 経済産業大臣  
 防衛大臣  
 有識者 (7名)

閣僚が参画

重要インフラ  
専門委員会

技術戦略  
専門委員会

普及啓発・  
人材育成  
専門委員会

情報セキュリティ  
対策推進会議  
(CISO等連絡会議)

(事務局)

## 内閣官房 情報セキュリティセンター (NISC 2005年4月に設置)

**センター長**  
 (内閣官房副長官補 [事態対処・危機管理担当])  
**副センター長** (内閣審議官)  
**内閣参事官** 情報セキュリティ補佐官

政府機関・情報セキュリティ横断監視・即応調整チーム(GSOC)

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)

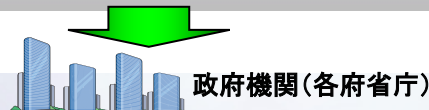
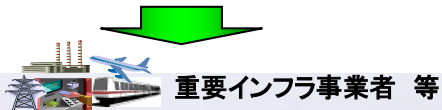
その他の  
関係省庁

### 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



# 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

重要インフラ分野からの情報連絡※件数	2012年度	2013年度	
	110	4~6月	7~9月
標的型攻撃メール等の情報提供※※件数	2012年度	2012年度	2013年度
	246	74	95

#### 【重要インフラ分野】

- 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

保護対象の多様化

- 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月デンブ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**※※

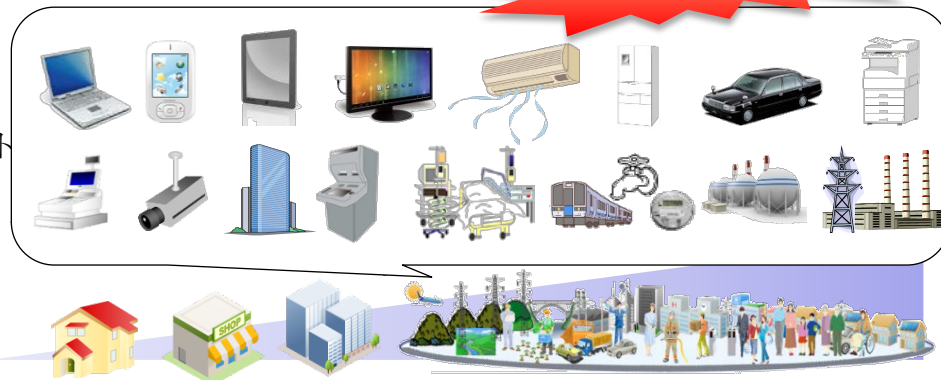


スマートメーター  
(次世代電力量計)

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)

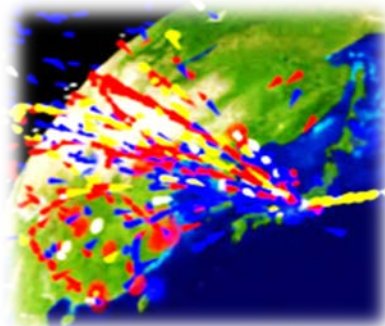
### 世界中からの多様な主体による攻撃

#### 【海外からの我が国への攻撃状況※】

グローバル化

#### 【最近の主な事例】

国家関与の可能性



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%

- 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  
→ **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  
→ **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、**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)


# IT先進国における経験


～深刻な危機に直面～




## 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見ることが可能。
- 選挙投票や確定申告等がネット上ででき、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、重点的に取り組むが進展。
- 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ることで推進。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。

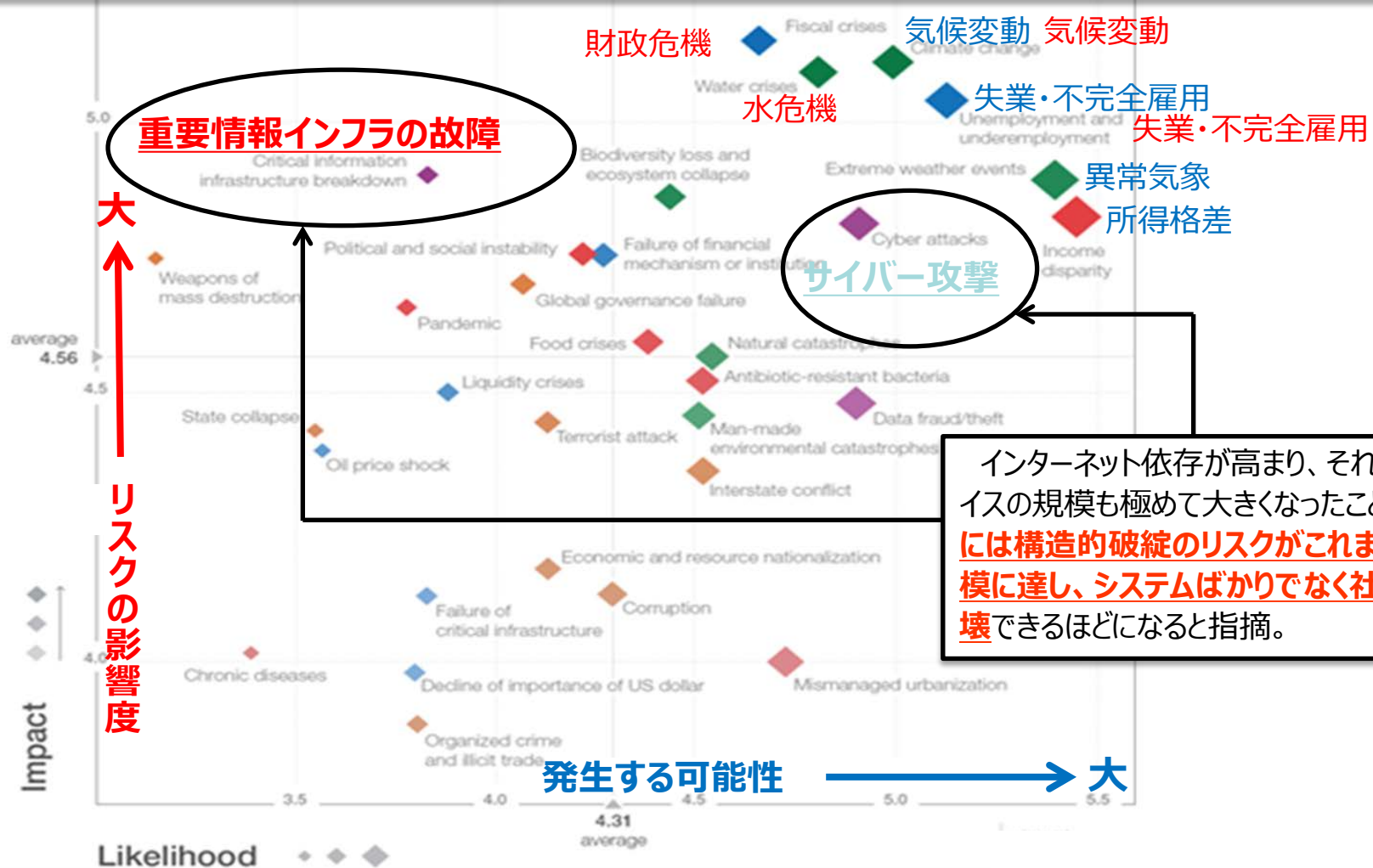
 上記について、当局は北朝鮮によるものと発表。昨年7月には、司令塔の強化など新計画を策定。

※ 「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が発生させてしまうサイバー攻撃

# 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。



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。

## 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。



## サイバー攻撃の特徴（例）

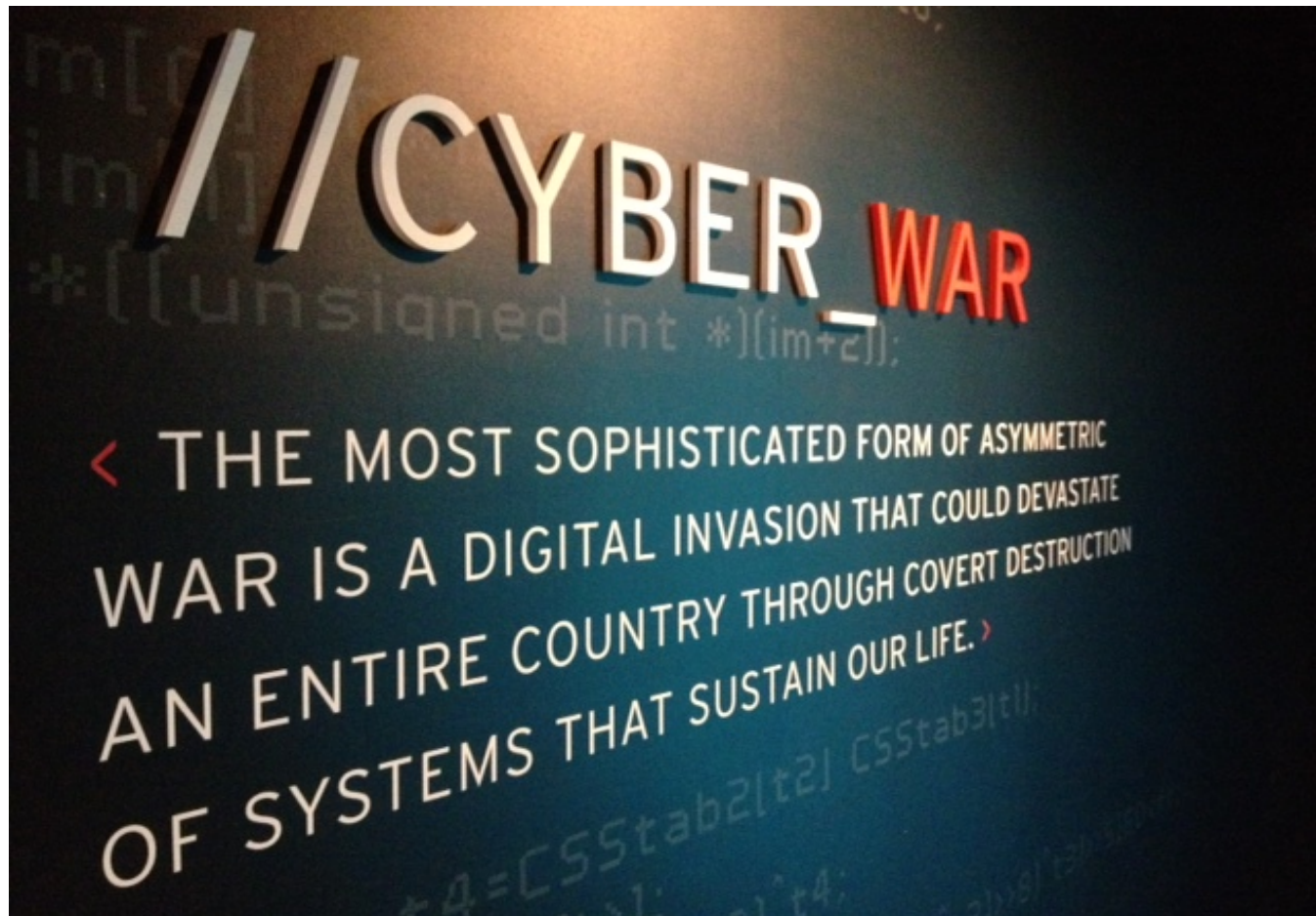
1. 非対称性(高価な兵器を必要とせず、費用がかからない)
2. 攻撃側の優位性(インターネットは拡張性があり、新技術の導入も容易)
3. 従来の抑止モデルが適用されず(攻撃者の特定が困難かつ時間を要する)
4. ソフトウェア及びハードウェア自体が脅威を内在(サプライチェーンリスク)
5. 予測の困難性(国家及び非国家主体の両方が実行者になり得る)

# サイバー攻撃と安全保障

- サイバー攻撃は**大きな脅威・リスク**。対象は**国家、企業、個人を超えて重層化・融合化**。
- 世界のどこで発生する事象であっても、直ちに我が国の平和と安全に影響を及ぼし得る。**国境の内側と外側を明確に区別することは難しい**。
- サイバー空間は、インターネットの発達により形成された仮想空間。**安全保障上も陸・海・空・宇宙に続く新しい領域だが、法的側面については議論が続いている**。
- サイバー攻撃が行われれば、政府機関から企業に至る社会の隅々にまで**深刻な影響を及ぼす**。この問題の**重要性が認識されるに至っている**。
- 日進月歩の技術進歩**を背景とするサイバー攻撃は、**攻撃の予測や攻撃者の特定が困難、攻撃の手法が多様、といった特徴あり、従来の典型的な武力攻撃と異なる点も少なくない**。そのため、**サイバー攻撃の法的位置付けについて一概に述べるのは困難**。
- これまでのところ、サイバー攻撃が「**武力攻撃**」に該当しないと位置付けられている事例が多いように見受けられる。
- 外部からのサイバー攻撃に対処するための制度的な枠組みの必要性等について、国際社会における議論にも留意しつつ、引き続き、検討が必要。

(出典)「安全保障の法的基盤の再構築に関する懇談会」報告書(2014年5月)

“最も洗練された非対称の戦争はDigital Invasionであり、これは我々の生命を維持するシステムを密かに破壊することで国全体を破壊しうるものである。”



*“International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”*

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2013)

# 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）



	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
<p><b>①</b> →</p> <p><b>「強靱な」サイバー空間（守り強化）</b></p>	<ul style="list-style-type: none"> <li>●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【14年5月】</li> <li>●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応</li> <li>●対処訓練の実施、警察・自衛隊等の関係機関の役割整理</li> <li>●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</li> </ul>	<p><b>②</b> →</p> <ul style="list-style-type: none"> <li>●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【14年5月】</li> <li>●政府機関やシステムベンダー等との情報共有の強化</li> <li>●事業継続確保のための分野横断的な演習</li> </ul>	<ul style="list-style-type: none"> <li>●スマートフォン不正アプリへの対応</li> <li>●情報セキュリティ月間【毎年2月】・“サイバーセキュリティの日”創設</li> <li>●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】</li> <li>●税制など中小企業のセキュリティ投資の促進</li> <li>●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</li> <li>●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</li> </ul>
<p><b>「活力ある」サイバー空間（基礎体力）</b></p>	<p><b>④</b> → ●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【14年5月】</p> <p><b>⑤</b> → ●研究開発戦略(2011年情報セキュリティ政策会議)の見直し【14年夏】</p>		
<p><b>⑥</b> ↓</p> <p><b>「世界を率先する」サイバー空間（国際戦略）【13年10月】</b></p>	<ul style="list-style-type: none"> <li>●日米</li> <li>●日英</li> <li>●日印</li> <li>●日露</li> <li>●日EU</li> <li>●日ASEAN</li> <li>●サイバー空間の国際規範づくり等に関する会議【平成24年10月：ソウル会議】</li> <li>●IWWN注1</li> </ul>	<ul style="list-style-type: none"> <li>●MERIDIAN注2</li> </ul>	<p>〈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</p> <p>〈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。</p> <p>●共同意識啓発活動【毎年10月】</p>
<p><b>⑦</b> ↓</p> <p><b>組織体制</b></p>	<p>●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)【方針決定:14年夏】</p>		

# 標的型メールの特徴

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等はウイルスの可能性



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

①差出人: 情報太郎 [[johou.taro@cas-go.jp](mailto: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

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

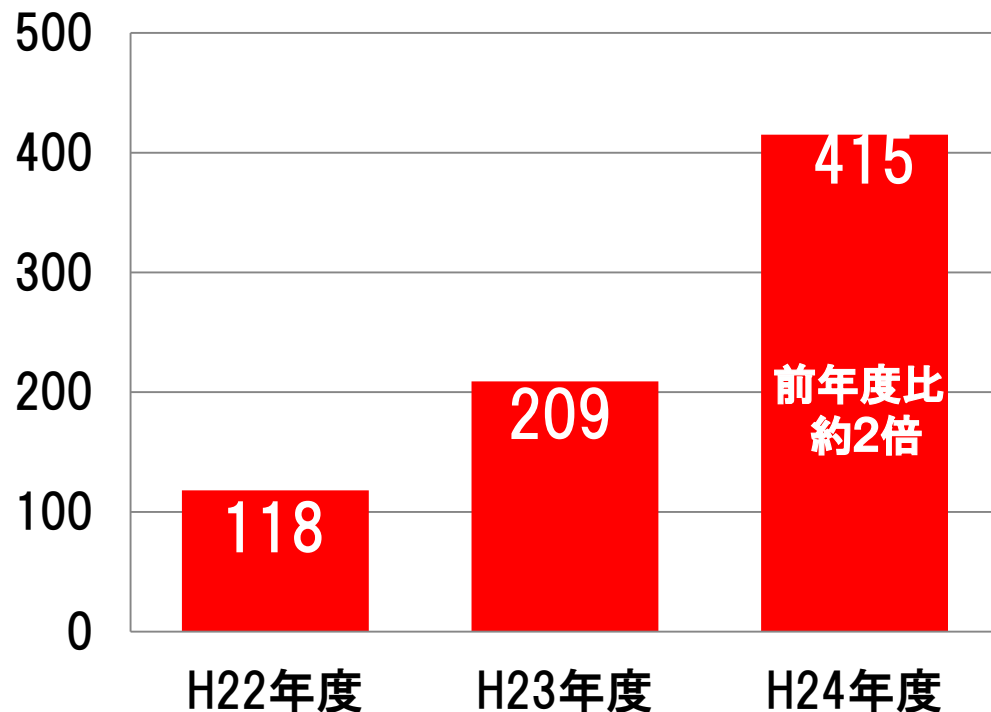


クリックすると

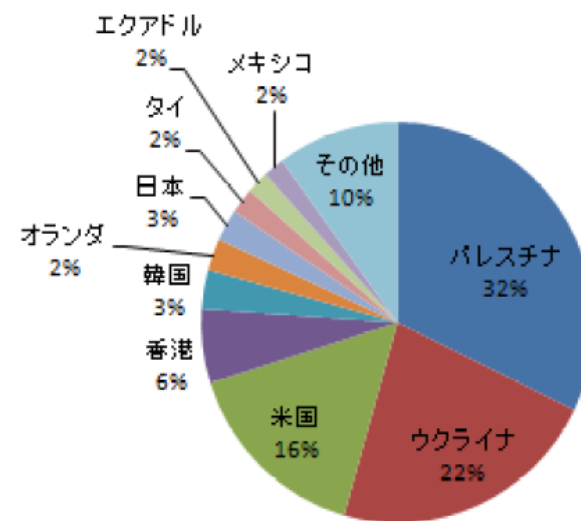
<http://10.243.23.11/詐欺/>

- 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）

## ① 初期潜入

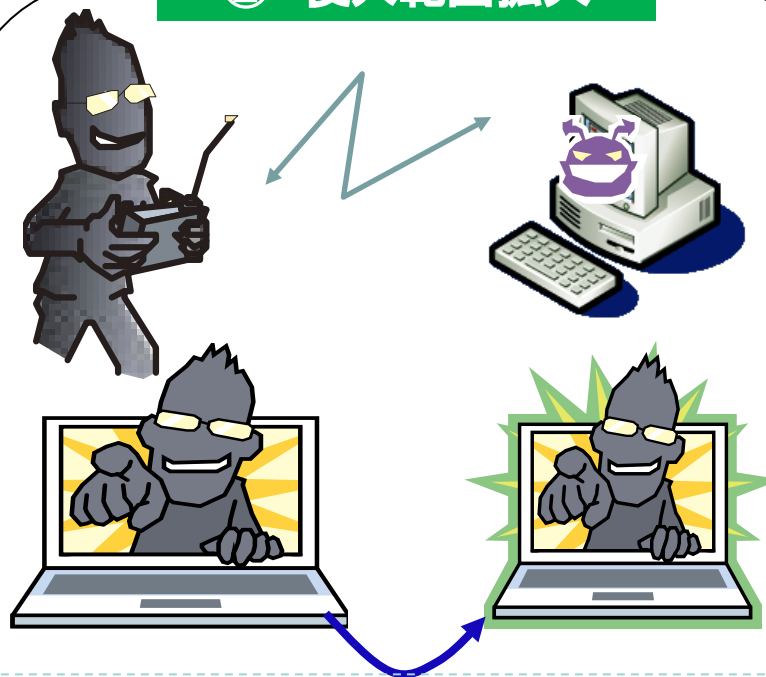


ウイルス  
対策ソフトが  
検知しない！

最初はメールの添  
付ファイルやリンク  
を開くだけ

外部(インターネット)

## ② 侵入範囲拡大



遠隔操作により、システムの内  
部に侵入し、乗っ取りを拡大

組織内ネットワーク

## ③ 情報窃取



重要情報の窃取や  
システム破壊も





# 標的型メール攻撃に対する教育訓練(平成25年度)

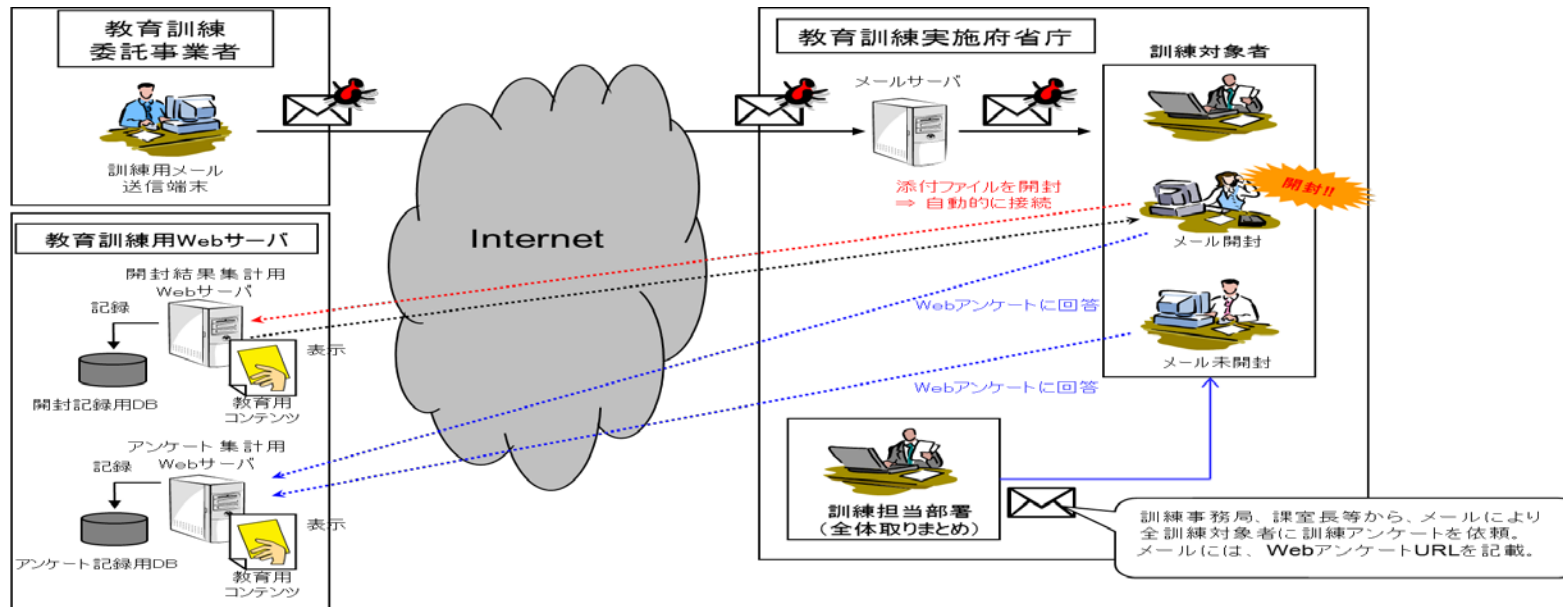
【目的】 標的型メール攻撃に関する教育・意識啓発のため、標的型メールを模擬メールを通じて“ヒヤリハット”を経験することで注意を深め、同攻撃に対し適切な対処を身につけることを目的。

【訓練概要】 標的型メール攻撃を模擬した訓練メールを2回職員に送付(加えて、希望府省庁にはやりとり型の訓練メールを送付)し、職員が不注意に開封するなどした場合に訓練用に設けたWebサイトに誘導。職員の不審メールへの対応状況を把握及びWeb教育コンテンツによる事後教育を実施。

【訓練対象者】 18府省庁 約18万人の職員(去年は19府省庁 約12万人)

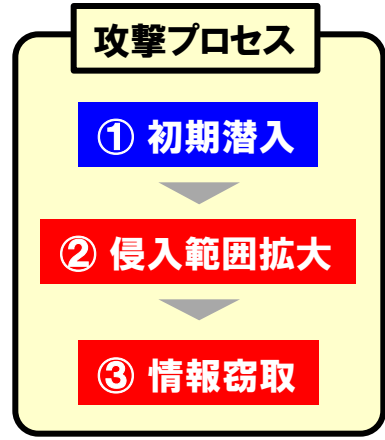
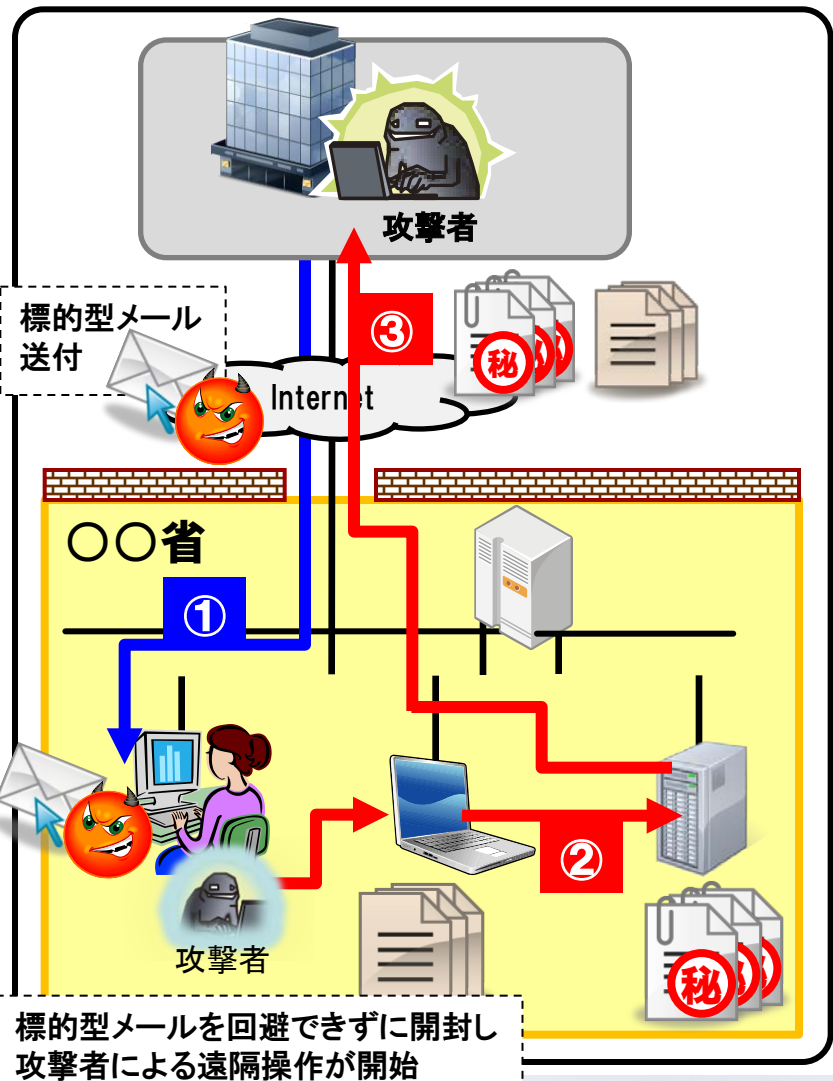
【訓練実施期間】 8月～12月の5カ月間を設定

【訓練結果】第一回目 10.1% 第二回目 16.3% やり取り型訓練 19.2%



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)



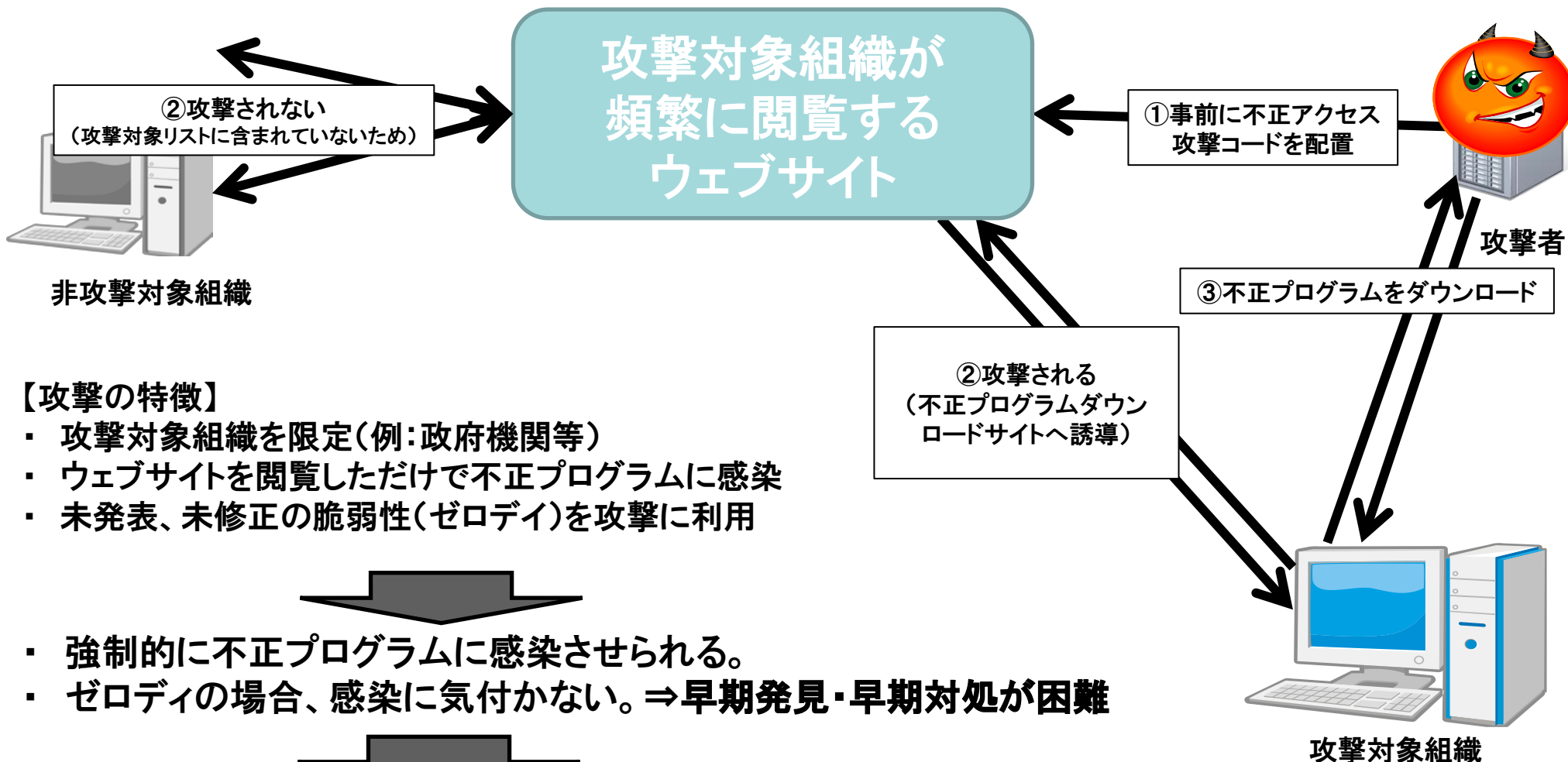
政府機関の情報セキュリティ対策のための統一管理・技術基準で対策を規定

**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	<ul style="list-style-type: none"> <li>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</li> <li>機器乗っ取りをしづらいシステム設計</li> </ul>
攻撃の兆候を監視し、早期に発見・検知する	<ul style="list-style-type: none"> <li>攻撃(主に攻撃失敗)の痕跡を残す</li> <li>攻撃者の侵入を発見・検知するためのトラップ(罠)を設置</li> <li>上記の継続的な監視</li> </ul>

# 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】

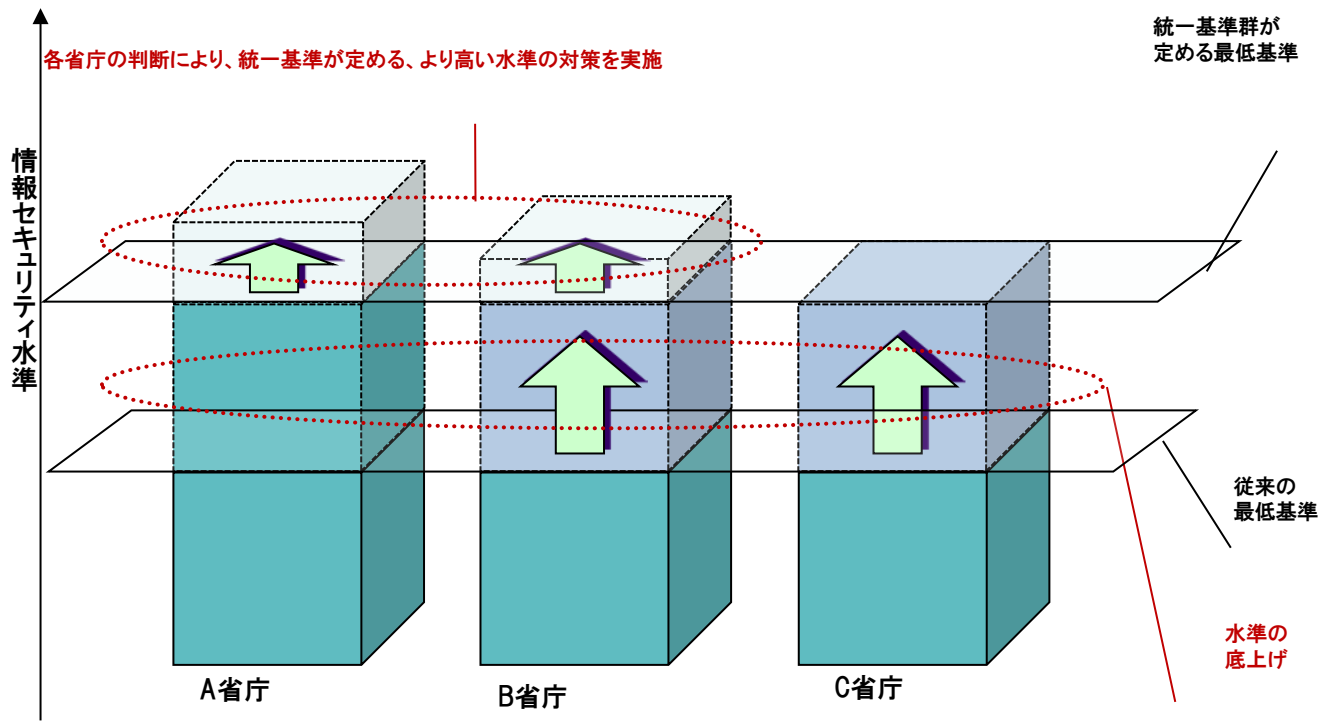
- ・ 攻撃対象組織を限定(例:政府機関等)
- ・ ウェブサイトを閲覧しただけで不正プログラムに感染
- ・ 未発表、未修正の脆弱性(ゼロデイ)を攻撃に利用

- ・ 強制的に不正プログラムに感染させられる。
- ・ ゼロデイの場合、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。

- 政府機関が実施すべき対策の統一的な枠組みを構築
- 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)>



## ◆毎年の改定により基準が複雑化・肥大化・形骸化

### 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、守られやすい基準に見直し。

## ◆脅威の高度化・多様化や技術進展などの環境変化

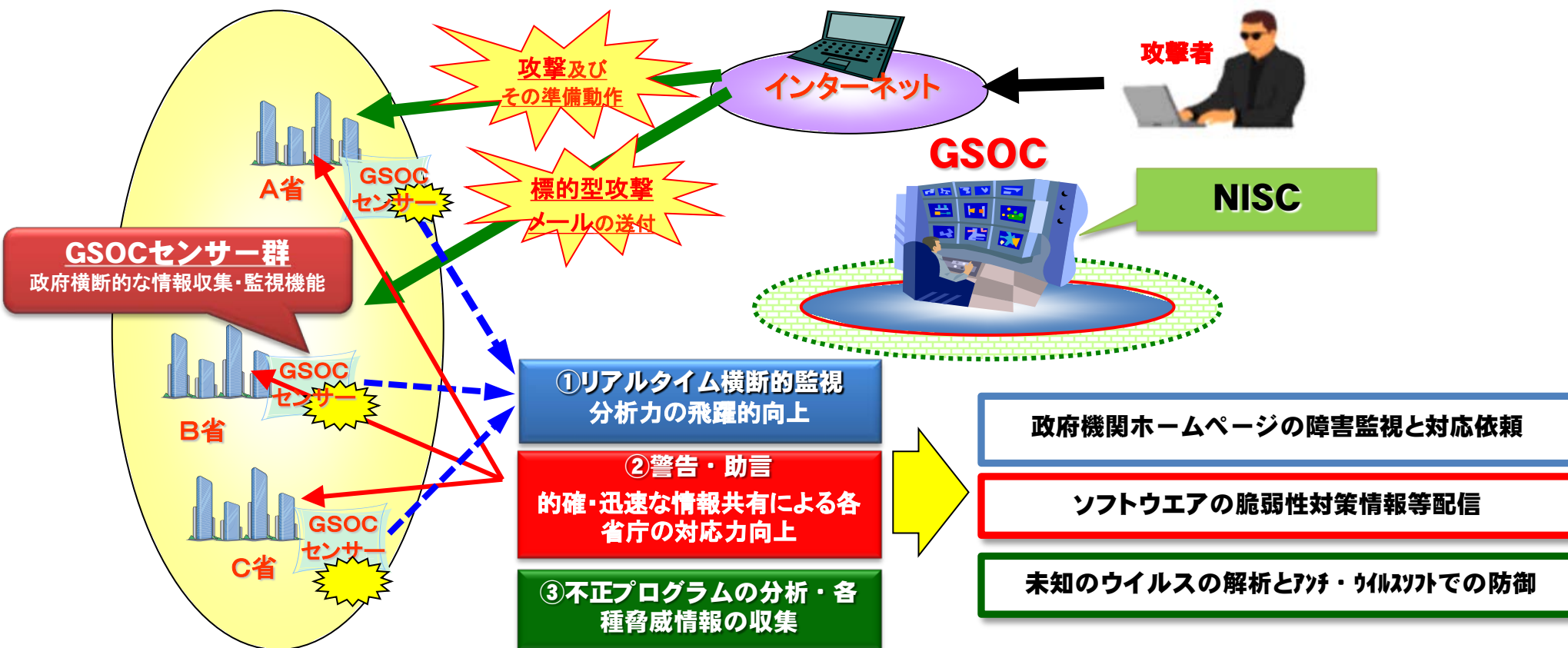
#### ◆新たな脅威・技術への対応

- 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。

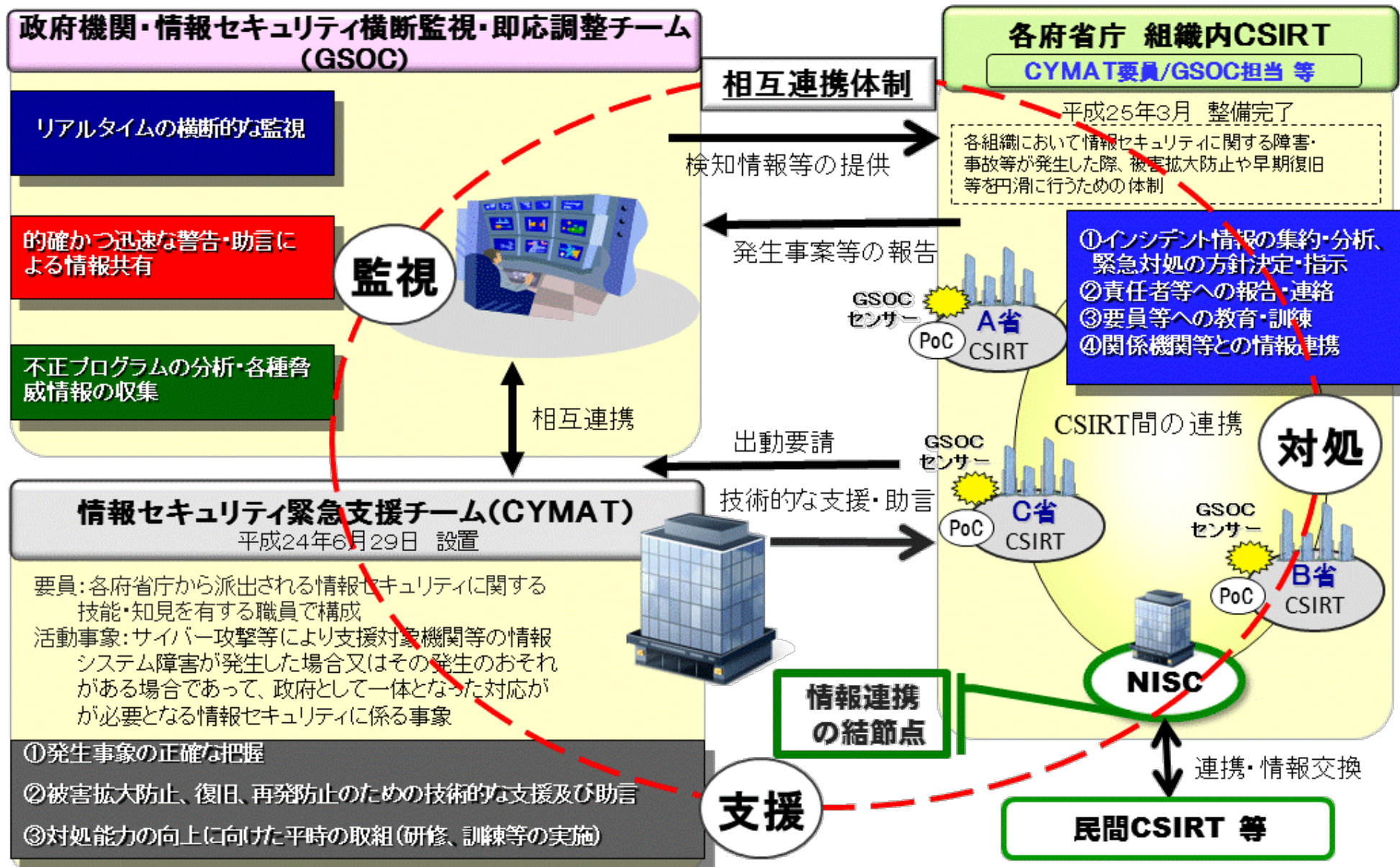
# GSOC (ジーソック)

【Government Security Operation Coordination team … 政府機関・情報セキュリティ横断監視・即応調整チーム】

- 平成20年4月 GSOCの運用開始 (8時間運用)
- 平成21年1月 24時間対応開始
- 平成25年4月 現行GSOCシステム運用開始
- 平成29年(2017年) 次期システムへ移行



# 政府におけるサイバーセキュリティ確保体制



# 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

(2014年5月、情報セキュリティ政策会議決定)

## 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サービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する

### 重要インフラ(13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
- クレジット
  - 石油
  - 化学

### 重要インフラ所管省庁(5省庁)

- 金融庁 [金融]
- 総務省 [情報通信、行政]
- 厚生労働省 [医療、水道]
- 国土交通省 [航空、鉄道、物流]
- 経済産業省 [電力、ガス、クレジット、石油、化学]

### 関係機関等

- 情報セキュリティ関係省庁
- 事案対処省庁
- 防災関係府省庁
- 情報セキュリティ関係機関
- サイバー空間関連事業者

NISCによる  
調整・連携

## 重要インフラの情報セキュリティに係る第3次行動計画

### 安全基準等の整備・浸透



重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

### 情報共有体制の強化



IT障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

### 障害対応体制の強化



官民が連携して行う演習等の実施によるIT障害対応体制の総合的な強化

### 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評価を含む包括的なマネジメントの支援

### 防護基盤の強化



広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開



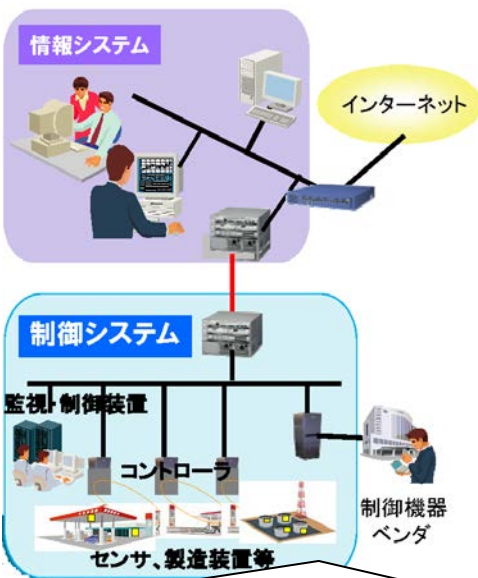
# 制御システムの普及

## 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

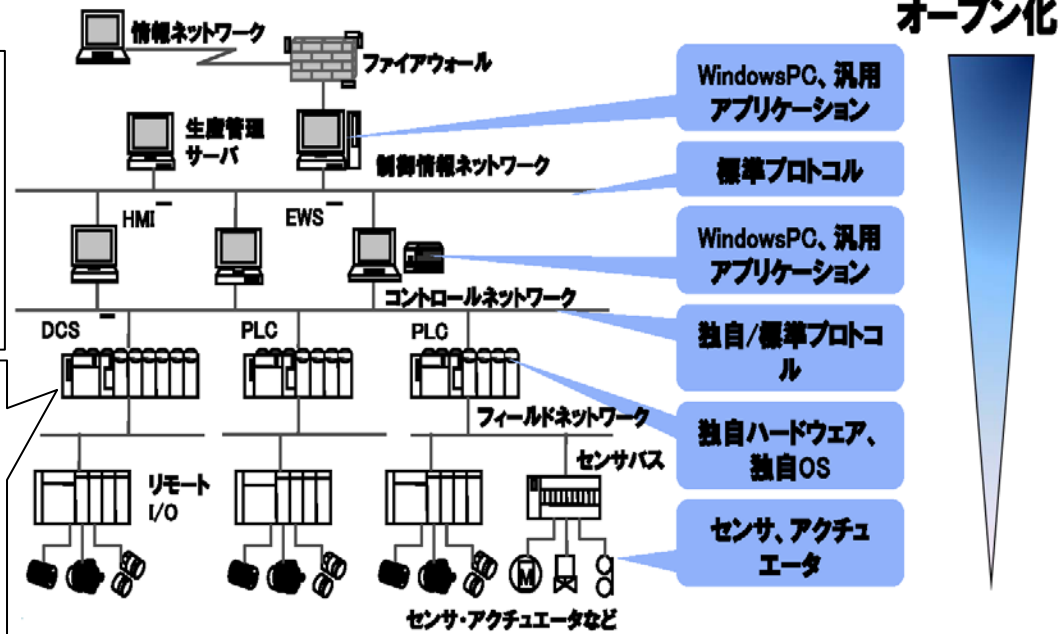
- 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
- 外部ネットワークにも接続されるようになっている。
- このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。



- 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。
- 最近では、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>】

## 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するためには、
- 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

IT人材106万人(SE80万人)

## 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

### 【需要】経営層の意識改革

#### ○組織の経営層

- ・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。

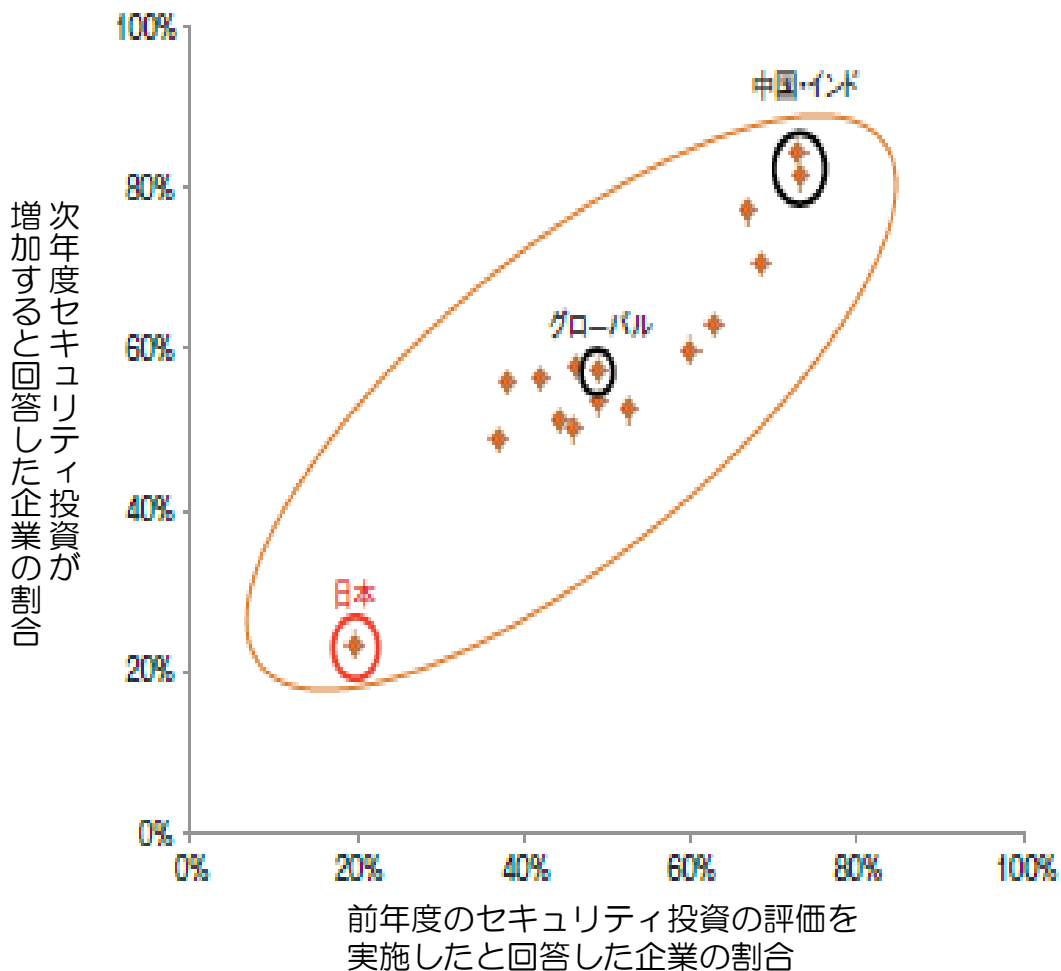
#### ○実務者層のリーダー層

- ・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

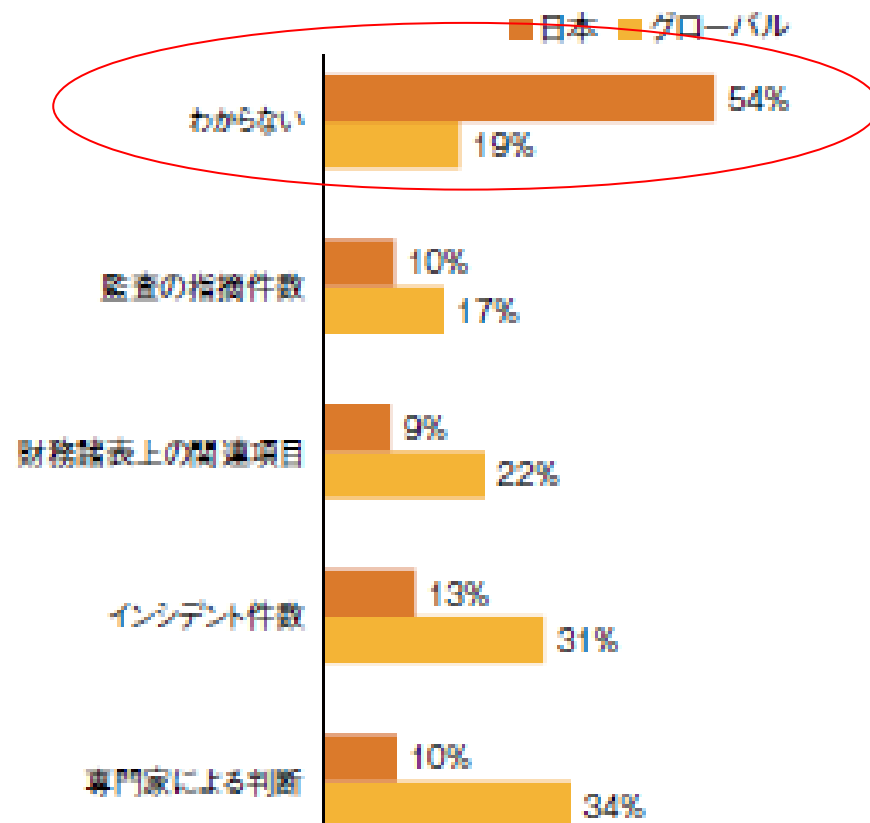
### 【供給】人材の「量的拡大」と「質的向上」

- IT技術者等に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。
- 高度な専門性及び突出した能力を有する人材の発掘・育成を推進するとともに、実社会での活躍を促進。
- グローバル水準の人材の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。
- 政府機関は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。
- 教育機関(初等中等教育機関含む)の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。

セキュリティ投資と投資効果の相関

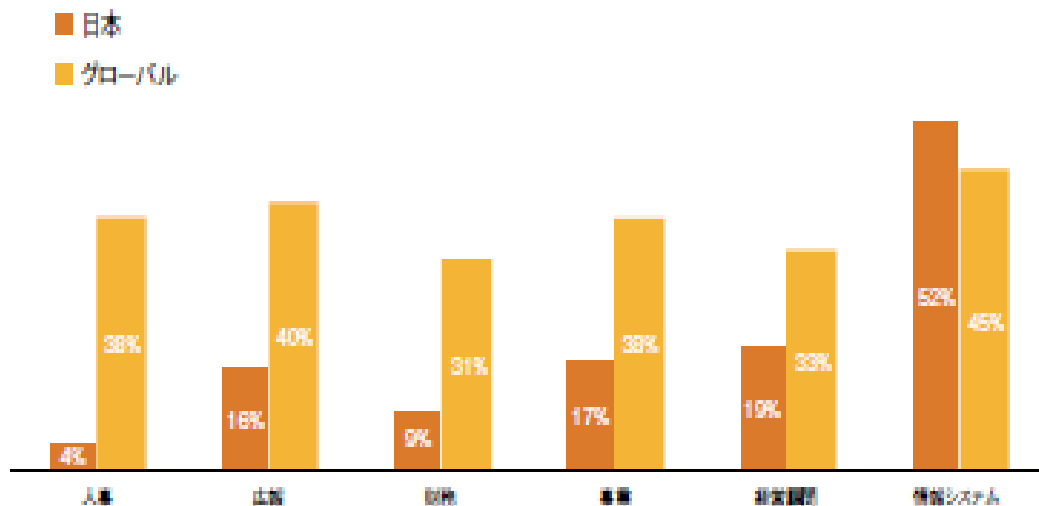


セキュリティ投資の効果測定方法

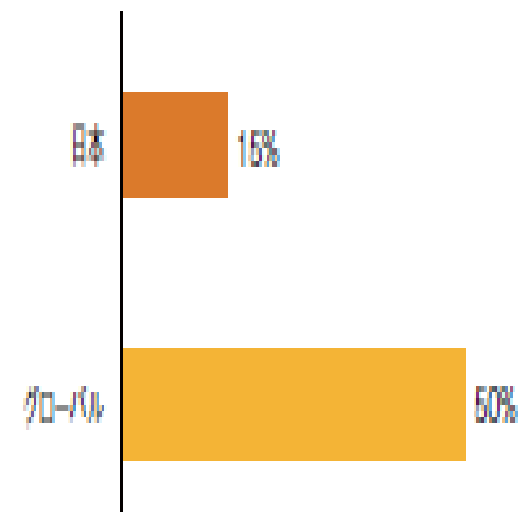


(出典) プライスウォーターハウス「グローバル情報セキュリティ調査2014」(14年2月)

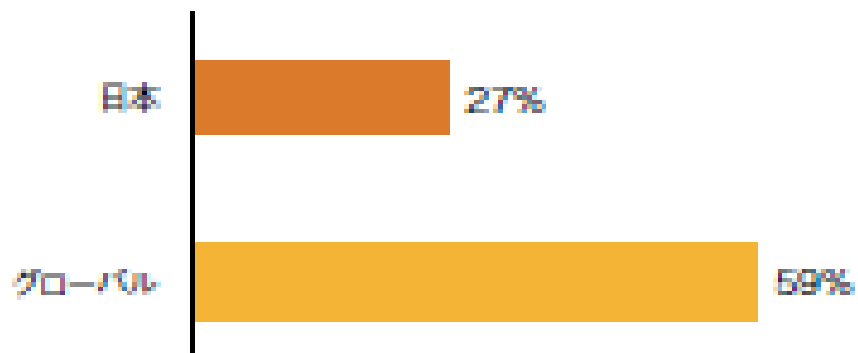
インシデントレスポンスに関与している部門



業界内でセキュリティ情報について連携している企業



積極的にセキュリティ対策を推進する経営幹部がいる企業



(出典)プライスウォーターハウス「グローバル情報セキュリティ調査2014」(14年2月)

## 「CF Disclosure Guidance」とは

- サイバーセキュリティ・リスク及びサイバーインシデントに関わる開示義務に関する、SEC企業財務部門の見解の記述をガイドする文書。
- サイバーセキュリティが、当該企業の事業に重要な影響を与える場合に、財務リスクなどと同様に開示を要求し得る、新たなビジネスリスクとして識別している。
- ただし、企業に法的義務を課すSECのルールや規則とは異なり、企業に新たな開示義務を課すものではない。
- また、SECはガイダンスの内容について、承認／非承認のいずれも行っていない。

右記の6項目に関して、サイバーセキュリティ・リスクやインシデントに関する、開示概要を示している

### リスクファクター

- 企業のサイバーインシデントに関するリスクが、当該企業への投資を、投機的或いは危険なものにし得るファクターの中で最も重要なリスクファクターである場合に、その開示をする必要がある。

### MD&A \*1

- サイバーセキュリティ・リスク及びサイバーインシデントに関わる費用やその他の影響が、企業経営、資産流動性、財務状況等に重大な影響を与えられられる場合には、それらについてMD&Aの中で開示する必要がある。

### 事業内容

- サイバーインシデントが、企業の製品、サービス、顧客や取引先との関係や競合状況に重大な影響を与える場合には、当該企業の「事業内容」の中でそれについて開示する必要がある。

### 法的手続

- 企業或いはその子会社が、サイバーインシデントに関わる法的手続を保留されている場合には、その訴訟に関わる情報を、当該企業の「法的手続に関する情報開示」の中で開示する必要がある。

### 財務諸表の開示

- 潜在的或いは実際のインシデントの性質や大きさにより、サイバーセキュリティ・リスクやサイバーインシデントは当該企業の財務諸表に広範な影響を与える可能性があることを開示する必要がある。

#### サイバーインシデントの発生前段階及び発生事後段階

- 企業が取り組んだインシデント回避対策コスト（発生前段階）や顧客とのビジネス関係を維持するために顧客に提供した費用または損失等（発生事後段階）を考慮する。

### 開示規制及び手続き

- 企業は、開示規制及び手続きの有効性に関する結論を開示する必要がある。

\*1 Management's Discussion and Analysis of Financial Condition and Results of Operations : 経営者による財政状態及び経営成績の検討と分析。米国では、SECが投資家への情報提供の一環として企業に開示を要求している。  
(出所) NTTデータ

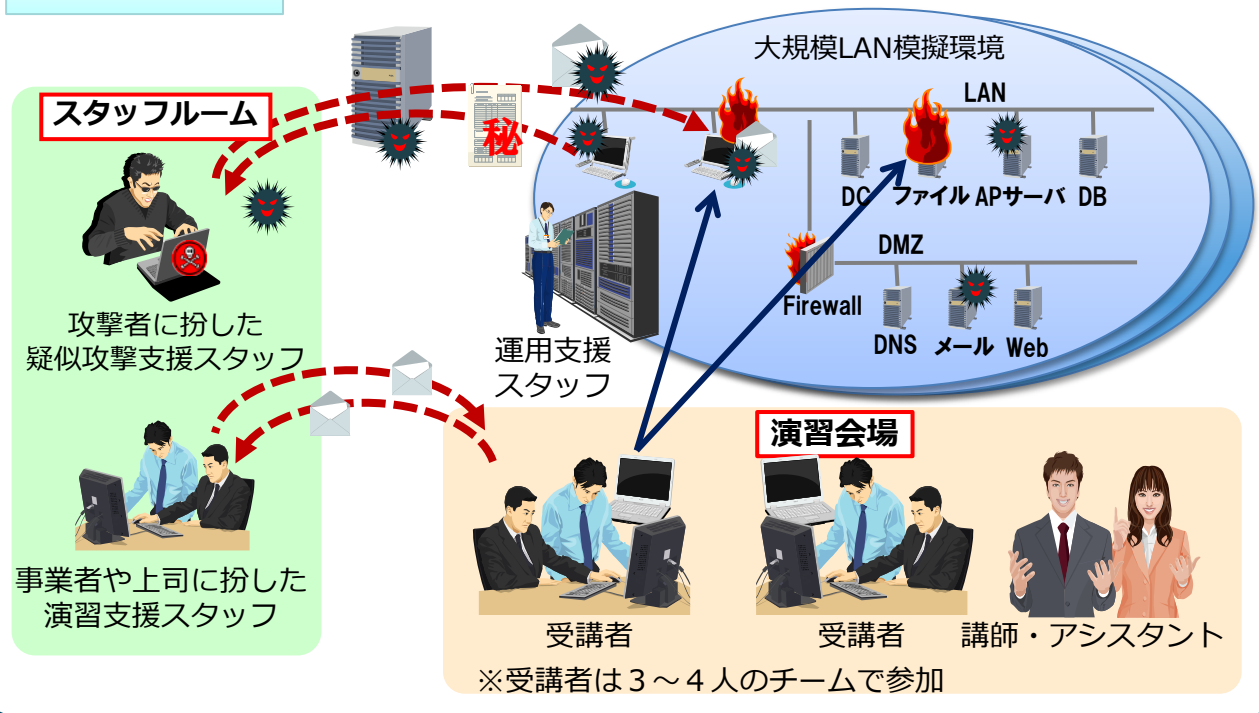
# CYDER (CYber Defense Exercise with Recurrence)



【総務省】

- 官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力向上のため、実践的なサイバー防御演習を実施。
- 職員数千人規模の組織内ネットワークを模擬した大規模環境による、官公庁を対象としたサイバー演習は日本初。
- LAN管理者の能力向上に寄与すると共に、演習で得られた知見を基に防御モデルを確立し広く展開していく予定。
- 「サイバー攻撃解析・防御モデル実践演習」(H24～H29)の一環として実施し、平成25年度は10回実施。

## 演習イメージ



## 昨年度演習実績

開催回	開催日
第1回	H25/9/25(水), 26(木)
第2回	H25/10/16(水), 17(木)
第3回	H25/11/13(水), 14(木)
第4回	H25/12/12(木), 13(金)
第5回	H26/1/15(水), 16(木)
第6回	H26/1/29(水), 30(木)
第7回	H26/2/12(水), 13(木)
第8回	H26/2/25(火), 26(水)
第9回	H26/3/3(月), 4(火)
第10回	H26/3/6(木), 7(金)

## 昨年度演習参加者

省庁(法務省、防衛省等)や独立行政法人、民間事業者などから  
計33組織、292名が参加

(注)総務省作成資料

## 所要経費

平成24年度補正予算額 15.2億円の内数  
平成26年度予算額 4.5億円の内数

情報処理技術者試験の全試験区分において、「情報セキュリティ」に関する出題の強化・拡充を実施

## パス

基本情報技術者試験 (FE)  
応用情報技術者試験 (AP)

◆ 情報セキュリティに関する出題比率の大幅な引き上げ(2倍)

◆ 午前試験において「中分類11 セキュリティ」の出題比率を引き上げ  
◆ 午後試験において「情報セキュリティ分野」を選択問題から必須問題に変更

## 高度試験

◆ 午前Ⅰ試験(共通知識)、午前Ⅱ試験において「中分類11 セキュリティ」の出題比率を引き上げ  
◆ ITストラテジスト試験(ST)、プロジェクトマネージャ試験(PM)においては、午前Ⅱ試験の出題範囲に新たに「中分類11 セキュリティ」を追加(高度全区分で出題)

すべての社会人	情報処理技術者(ベンダ側/ユーザー側)									
 ITを活用する社会人に求められる基礎知識 (IP)	高度な知識・技能	ITストラテジスト試験 (ST)	システムアーキテクト試験 (SA)	プロジェクトマネージャ試験 (PM)	ネットワークスペシャリスト試験 (NW)	データベーススペシャリスト試験 (DB)	エンベデッドシステムスペシャリスト試験 (ES)	情報セキュリティスペシャリスト試験 (SC)	ITサービスマネージャ試験 (SM)	システム監査技術者試験 (AU)
	応用的知識・技能	応用情報技術者試験 (AP)								
	基本的知識・技能	基本情報技術者試験 (FE)								

※ IPA プレス発表「パス(ITパスポート試験)をはじめとする情報処理技術者試験の出題構成の見直しについて」 <http://www.ipa.go.jp/about/press/20131029.html>

(注)パスは平成26年5月7日以降、パス以外は26春試験から適用



○ ITを利用する企業(ユーザー企業)における情報セキュリティ人材不足を解消するために、IT人材の国家試験である情報処理技術者試験に組織のセキュリティポリシーの策定等に必要となる知識を問う試験区分「情報セキュリティマネジメント試験」を創設。(本年夏から検討着手。平成28年度(2016)からの開始を目指す。)

(注)経済産業省資料を基にNISC作成。

サイバーセキュリティ戦略（H25年6月策定）において示された、「活力ある」サイバー空間の構築（産業活性化、研究開発）を目指し

- サイバー攻撃の検知・防御能力の向上
- 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
- ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発 等

を推進する観点から、「**情報セキュリティ研究開発戦略**」を改定

## 情報セキュリティ研究開発の推進方針

### 1. サイバー攻撃の検知・防御能力の向上

研究開発における実際のサイバー攻撃情報等の重要性に鑑み、分散しているサイバー攻撃情報等の共有のための組織等の連携強化、可能な範囲・方法・条件で研究者等へ政府の有する標的型攻撃等の検体等の提供等を検討。

### 2. 社会システム等を防護するためのセキュリティ技術の強化

社会システム等を構成する制御システム等のセキュリティ技術の研究開発にあたっては成果の早期実用化が重要であることに鑑み、国際標準化・認証制度につながるよう推進。

### 3. 産業活性化につながる新サービス等におけるセキュリティ研究開発

産業活性化・国際競争力の強化の観点から、今後発展が期待されるICT利用分野で企画・研究開発・設計段階等上流工程からセキュリティ品質を組み込み等の取組みを促進。

### 4. 情報セキュリティのコア技術の保持

暗号等の基礎研究をはじめ情報セキュリティのコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり、大学・公的研究機関等の役割も含めて維持・強化。

### 5. 国際連携による研究開発の強化

サイバーセキュリティに係る高度な技術の研究開発に向け、各国が「強み」を有する技術を組み合わせて発展させるなどのため、研究者受け入れを含め国際連携を推進。

## 研究開発の効果・成果を高めるための方策等

1. 研究成果の**社会還元**の推進：事業化等に向けて研究者等を支援するための環境整備
2. 必要な研究開発**リソースの確保と柔軟性確保**
3. 情報セキュリティ技術と**社会科学、経営学など他分野との融合**：技術のみならず安全保障・危機管理、経済学、経営学、心理学等の研究者とも連携した取組みを促進

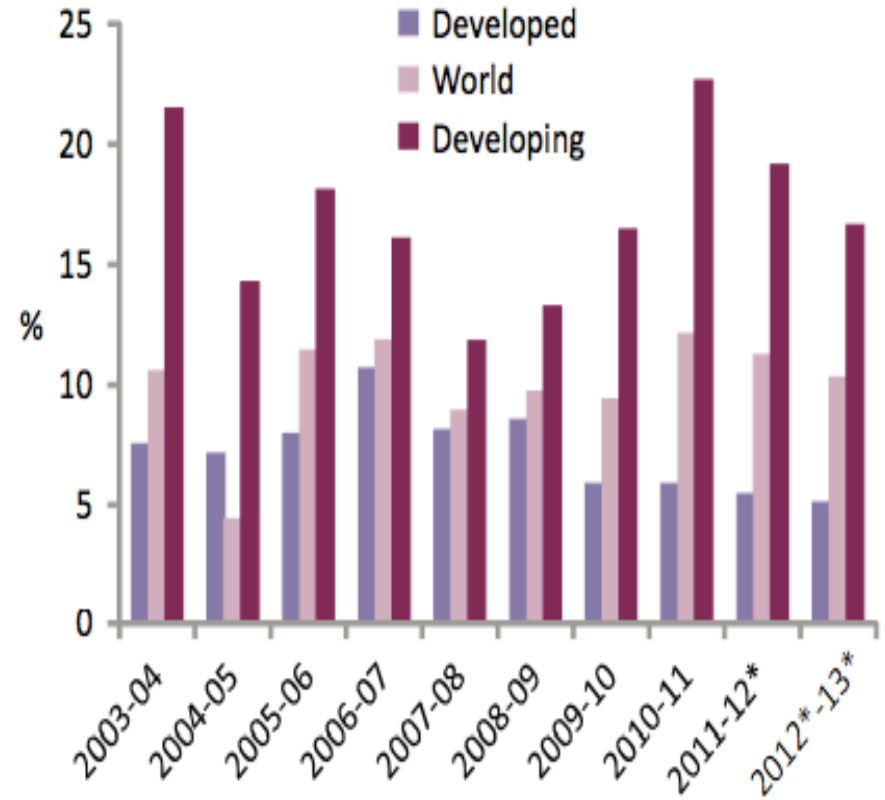
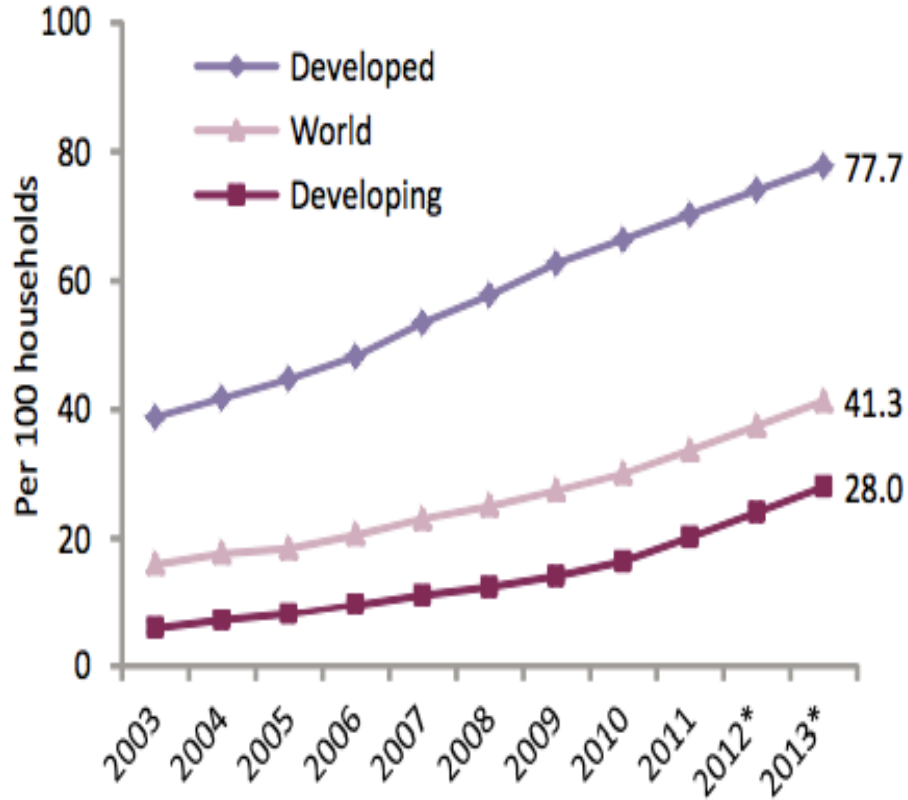
## 情報セキュリティ研究開発における16の重要分野

（※ 上記の観点を踏まえ、従来の重要分野を見直し）

<b>(1)情報通信システム全体のセキュリティの向上</b>	
①	サイバー攻撃の検知／防御
②	ID連携／認証／アクセス制御
③	ITサービスのセキュリティ(スマートフォン／クラウド等)
④	次世代ネットワークセキュリティ
<b>(2)ハード・ソフトウェアセキュリティの向上</b>	
⑤	制御システムセキュリティ
⑥	セキュリティデバイス
⑦	ソフトウェアの安全性確保
<b>(3)個人情報等の安全性の高い管理の実現</b>	
⑧	プライバシー保護／パーソナルデータ利活用のための技術
⑨	フォレンジック等を支援するためのデータ管理・追跡技術
<b>(4)研究開発の促進基盤の確立とセキュリティ理論の体系化</b>	
⑩	セキュリティ理論体系化／調査研究
⑪	標準化／評価／制度／基盤整備
⑫	暗号技術
<b>(5)発展が期待される応用分野でのセキュリティ研究開発</b>	
⑬	医療健康分野での情報流通変革に伴い必要となるセキュリティ技術
⑭	次世代インフラで必要となるセキュリティ技術
⑮	ビッグデータにおける情報の秘匿化、暗号化等のセキュリティ技術
⑯	家電、自動車のネットワーク接続で必要となるセキュリティ技術



# 世界のインターネット世帯普及率の推移



Note: \* Estimate.

Source: ITU World Telecommunication/ICT Indicators database.

(Source) ITU “Measuring the Information Society” (October 2013)

# サイバーセキュリティ国際連携取組方針（13年10月）

## 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、強靱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。

#### ○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

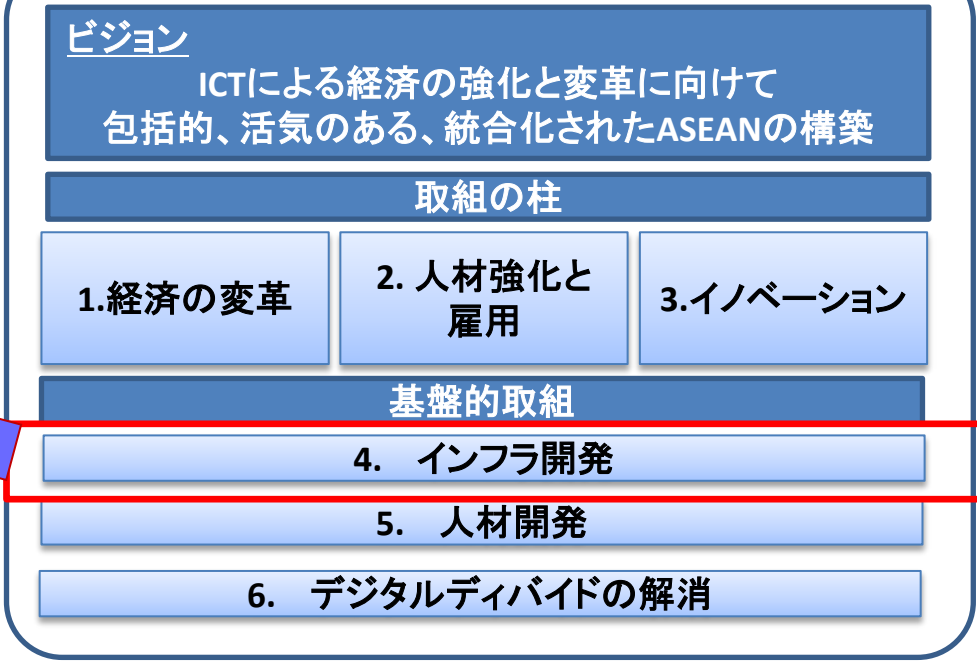
## ASEAN ICTマスタープラン2015

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

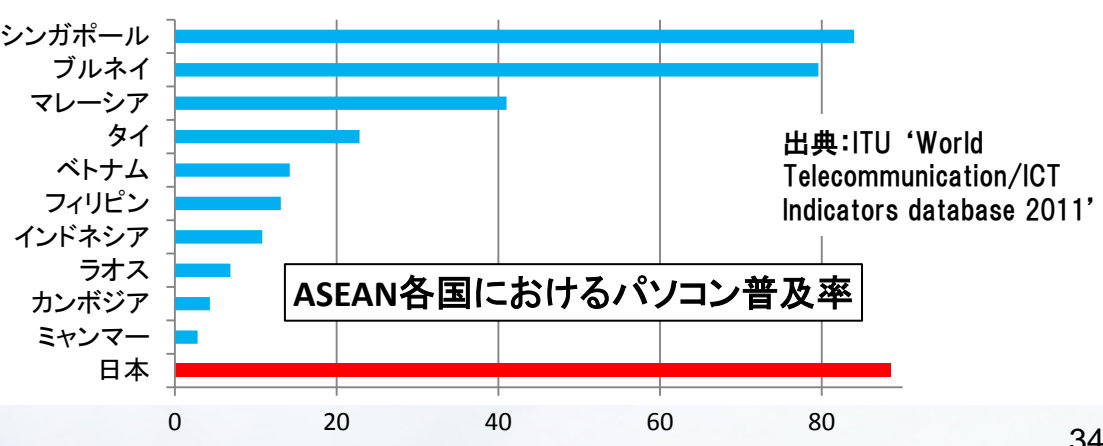
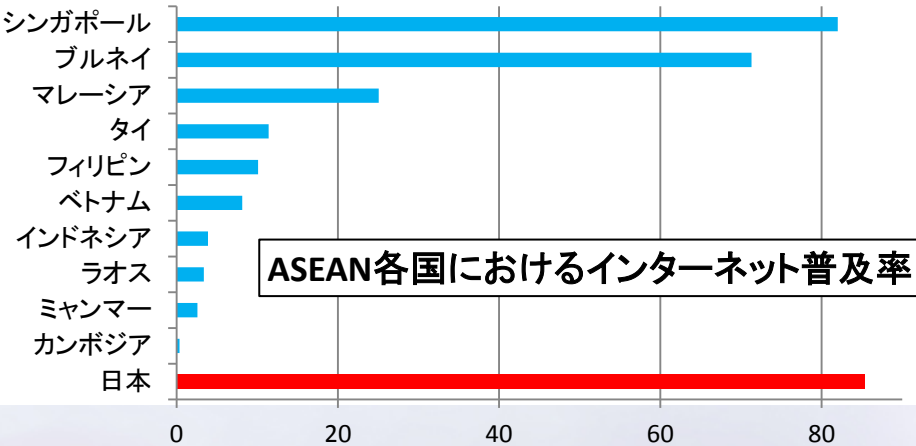
\* Computer Emergency Response Teamの略。  
 サイバー攻撃発生時等の連絡窓口となり、また、その際の対処を行う専門組織

## マスタープランの概要



## 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。



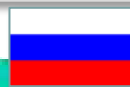
## EU

- **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



## 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

- 多角的なパートナー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4月@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：**平成24年9月@日本**
- 共同意識啓発活動の実施：**平成24年10月**



## 多国間・マルチステークホルダーの取組み

(注)エストニア、豪州、EU、フランス、イスラエル等の間でサイバー協議立ち上げに合意。

## 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カ国の政府機関、国際機関、民間セクター、NGO等が参加。
- ソウル会議：**平成24年10月@ソウル**

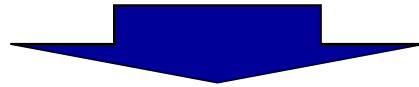
## MERIDIAN

- **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。

GCHQ(政府通信本部)に政府予算を付けて英国全体のセキュリティ対策を実施。



## ■ロンドンオリンピック公式サイトへの攻撃

- 2週間の開催期間に2億1,200万回のサイバー攻撃(公式サイト "London2012.com")。
- 全体で23億件のセキュリティイベントが発生。
- 1秒間に1万1千件のDDoS攻撃を観測・防御。

## ■開会式での電力インフラ(照明)への攻撃

- オリンピックに備えて考えられる限りの電力インフラへのサイバー攻撃対処訓練を5回実施。本番直前に攻撃情報があり、照明設備を急遽マニュアルで操作。
- わずか30秒の停電で開催国の威信が損なわれる(reputation riskへの対応が重要)。

## ■教訓

- 「ダウンタイム」は許されない。
- 品質保証は"Right First Time"と"Fail First"が原則。
- 本格システム稼働は開催の28か月前。
- 英国との協力関係(本年5月総理訪英、日英協定によるノウハウ移転、日英サイバー協議)

## ロンドンとの違いも念頭に置いた検討も必要

### ■全体像の把握とリスク分析

※五輪についての全体像を把握し、リスク分析に活用

※地震、台風等我が国特有のリスクを抽出

※バランスの勘案

⇒ オリンピック関連システムだけ防御レベルを上げると他の重要システムへの攻撃が増加する弊害等も考慮

### ■技術・環境の変化への継続的な対応

※社会・経済に影響を与えるIT・環境の変化の把握

⇒ 8Kテレビ、スマートメータ等への対応

⇒ ロンドンでは、スマートフォンの出現で通信容量の見積もり変更を余儀なくされた

### ■人材の確保と育成

※質量双方の向上を見据えたセキュリティ人材の育成・確保

⇒ 2020年を見据えた若年層等の採用・育成

# わが国のサイバーセキュリティ体制の強化に向けて

(14年4月10日、自民党サイバーセキュリティ対策関係合同会議)



## 1 体制強化の必要性

～ 急速に高まるサイバー脅威への対処 ～

●安倍政権の成長戦略を確固たるものとするためには、ITの利活用等とともに、急速に高まるサイバー脅威に対処するため、**サイバーセキュリティを含む情報セキュリティの強化**について、**国自らがリーダーシップを強く発揮できる体制**への抜本的強化が必要。

## 2 体制強化に向けた基本的考え方

～ 国の主導的な役割の明確化 ～

●「インターネット前提社会」では、**民間の主導的役割等を定めるIT基本法は堅持しつつ、官民の緊密な連携を前提に、国家の安全保障、国民1人1人の認識醸成、東京オリンピック等への対策**のため、**国の主導的役割の明確化**が必要。

## 3 「サイバーセキュリティ基本法」(仮称)の制定 ～ 基本理念等の確立、司令塔の強化 ～

●**基本理念**として次を規定。

- ① **情報の自由な流通の確保**等を基本として、サイバー脅威に対し、**官民連携により能動的・積極的に対応**。
- ② **国民1人1人が情報セキュリティの認識を深化**し、被害から円滑・迅速に復旧等できる**強靱な体制を構築**。
- ③ **将来に渡りITの恵沢を享受**するため、その持続的な開発・利用による**創造的・活力ある経済社会を構築**。
- ④ **グローバルに密接な相互依存**の中、協調、規範策定、信頼醸成や能力構築支援等における**先導的な役割**。

●**国・重要インフラ事業者等の責務、関係者間の連携強化、必要な措置・行政組織の整備、基本的施策**等を規定。

●**司令塔**となる「**情報セキュリティ政策会議**」の**機能・権限**として次を規定。

- ① **サイバーセキュリティ戦略**の策定、②各府省等の対策に関する**統一基準の策定・監査**、
- ③**経費見積もり方針**等の策定、④**重大インシデントの原因究明調査**、⑤関係行政機関への**議長による勧告** 等

## 4 組織体制の強化に向けて ～ NISCの法制化等 ～

●平成27年度からの本格稼働を目指すべく、**政府において、政府機関の横断監視機能(GSOC)等を担うNISC(内閣官房情報セキュリティセンター)の法制化等**の組織体制を強化すべき。

## 第I章. 総則

### ■ 目的 (第1条)

### ■ 定義 (第2条)

⇒ 「サイバーセキュリティ」について定義

### ■ 基本理念 (第3条)

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

- ① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
- ② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築
- ③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築
- ④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
- ⑤ IT基本法の基本理念に配慮して実施
- ⑥ 国民の権利を不当に侵害しないよう留意

### ■ 関係者の責務等 (第4条～第9条)

⇒ 国、地方公共団体、重要社会基盤事業者(重要インフラ事業者)、サイバー関連事業者、教育研究機関等の責務等について規定

### ■ 法制上の措置等 (第10条)

### ■ 行政組織の整備等 (第11条)

## 第II章. サイバーセキュリティ戦略

### ■ サイバーセキュリティ戦略 (第12条)

⇒ 次の事項を規定

- ① サイバーセキュリティに関する施策の基本的な方針
- ② 国の行政機関等に
- ③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進
- ④ その他、必要な事項におけるサイバーセキュリティの確保

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

## 第III章. 基本的施策

### ■ 国の行政機関等におけるサイバーセキュリティの確保 (第13条)

### ■ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進 (第14条)

### ■ 民間事業者及び教育研究機関等の自発的な取組の促進 (第15条)

### ■ 多様な主体の連携等 (第16条)

### ■ 犯罪の取締り及び被害の拡大の防止 (第17条)

### ■ 我が国の安全に重大な影響を及ぼすおそれのある事象への対応 (第18条)

### ■ 産業の振興及び国際競争力の強化 (第19条)

### ■ 研究開発の推進等 (第20条)

### ■ 人材の確保等 (第21条)

## 第III章. 基本的施策 (つづき)

### ■ 教育及び学習の振興、普及啓発等 (第22条)

### ■ 国際協力の推進等 (第23条)

## 第IV章. サイバーセキュリティ戦略本部

### ■ 設置等 (第24条～第35条)

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

## 附則

### ■ 施行期日 (第1条)

⇒ 公布の日から施行(ただし、第II章及び第IV章は公布日から起算して1年を超えない範囲で政令で定める日)する旨を規定

### ■ 本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等 (第2条)

⇒ 情報セキュリティセンター(NISC)の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

### ■ 検討 (第3条)

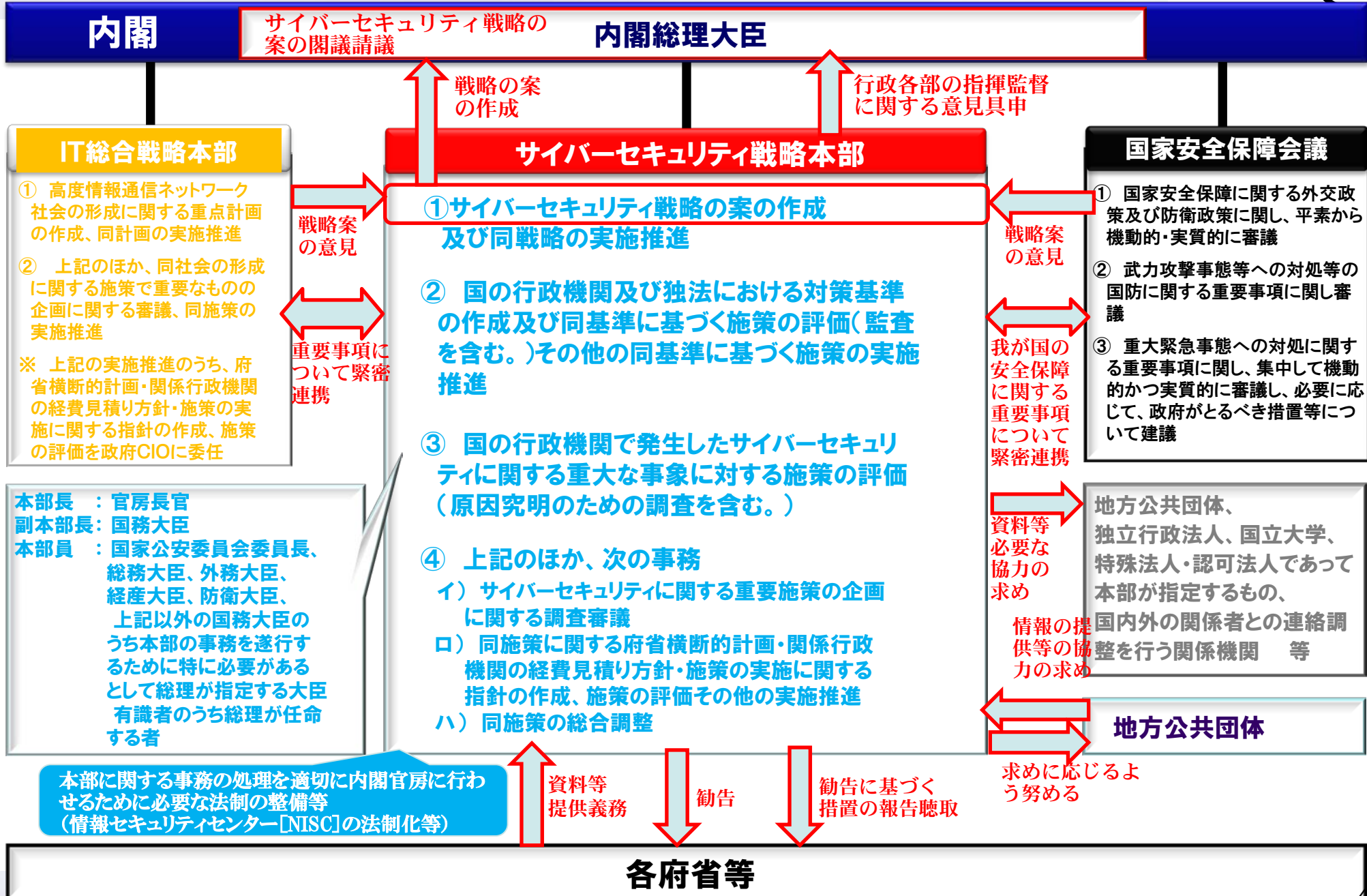
⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

### ■ IT基本法の一部改正 (第4条)

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定



# サイバーセキュリティ戦略本部の機能・権限 (イメージ) NISC



# 我が国のサイバーセキュリティ推進体制の機能強化に関する 取り組み方針（素案）（14年5月）



## 1. 機能強化の必要性

- あらゆる活動のサイバー空間への依存の高まりにより、**リスクが深刻化**（甚大化・拡散・グローバル化）
- 「**世界最高水準のIT社会**」をIT利活用においても実現することが**成長戦略**の柱の1つ

- **国際的な連携の強化が必要な諸外国**においても、積極的な**体制強化**が実施
- **2020年東京オリンピック・パラリンピックに向けた対策の強化**が必要

我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

## 2. 機能強化に向けた方針

IT社会の形成を目的とし、**民間の主導的役割等を基本理念**とする**IT基本法の基本的枠組みは今後も堅持**することが適当

**国家の安全保障・危機管理上、国の主導的役割を定め、マルチステークホルダーの相互連携によるサイバー空間の防護**が必要

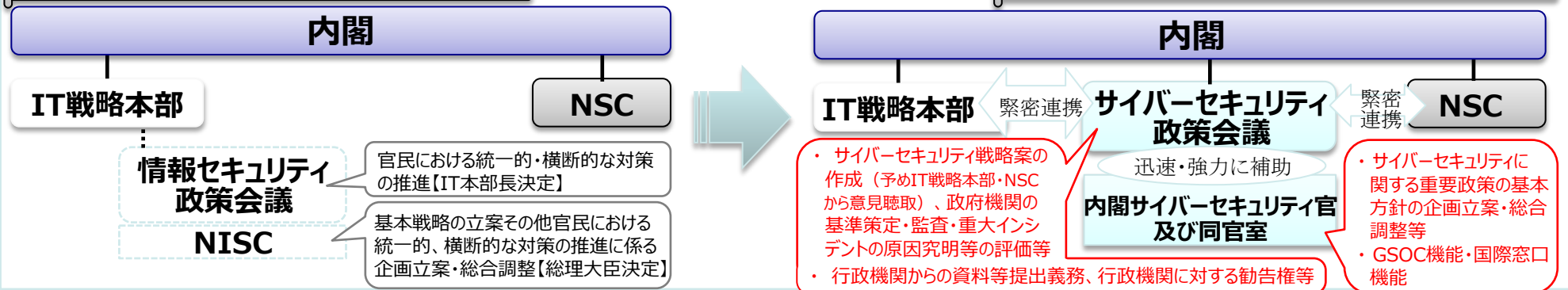
IT社会の形成及びサイバー空間の防護のための**関係者の役割を明確化**し、それが果たされるための**国の基本的施策**が必要

「サイバーセキュリティ」に関する施策を総合的かつ効果的に推進するための体制を整備することが必要

## 3. 機能強化に向けた取組

現状：法的な根拠・権限が不明確

今後：法制化し、事務・権限を明確化



2015年度を目途に「サイバーセキュリティ政策会議（仮称）」及び「内閣サイバーセキュリティ官（仮称）」へ強化

# Any question?

