NISC National Information Security Center

我が国のサイバーセキュリティ戦略

２０１４年１１月１８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（約６秒に１回）

	2011年度	2012年度	2013年度
センサー監視等による脅威件数 ※※	約66万	約108万	**約508万**
センサー監視等による通報件数	139	175	**139**
不審メールに関する注意喚起の件数	209	415	**381**

※ 「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）により各府省庁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

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡※件数	15	76	**133**

	2012年度	2013年度
標的型攻撃メール等の情報提供※※件数	246	**385**

＜内訳＞
- 不正アクセス、DoS攻撃 121
- ウイルスへの感染 7
- その他の意図的要因 5

【重要インフラ分野】 保護対象の多様化

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

※ NISCへの情報連絡件数のうちサイバー攻撃（意図的要因）に関するもの。 ※※重要インフラ機器製造、電力、ガス、化学、石油の5業界からIPAへ情報提供されたもの

※※※ 「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」（2014年5月19日情報セキュリティ政策会議決定）において追加

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

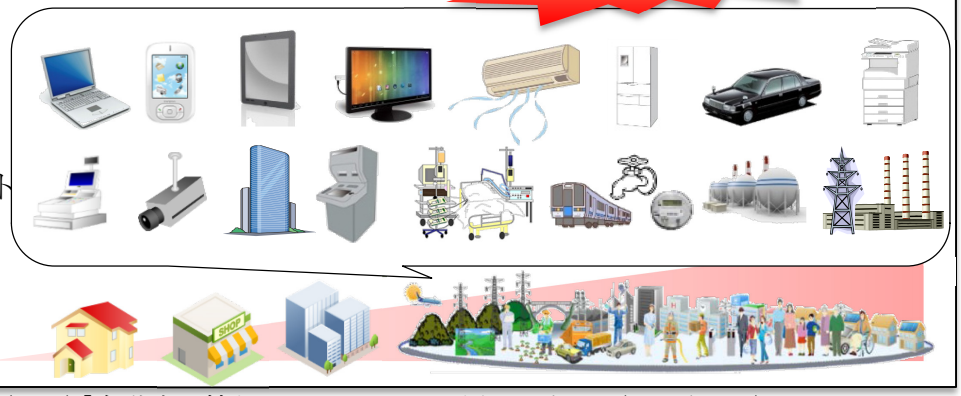
【スマートフォンの普及等】　国民1人1人へ

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%**）
携帯端末を標的とする不正サイトが**20倍**に急増※※
（2011年度末：約3千→**2013年度末：約5万7千**）

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）
各電力会社による開発・導入の開始※※※※
［主な予定］
・東京：2020年度までに**2700万台**の導入完了
・関西：2022年度までに**1300万台**の導入完了

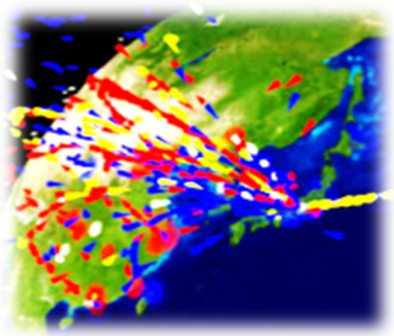
【我が国社会全体への浸透】　いつでもどこでも何でも



※　総務省「平成25年版情報通信白書」
※※　トレンドマイクロ㈱調べ（2014年4月）
※※※　（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）
※※※※　経済産業省「第14回スマートメーター制度検討会」資料（2014年3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）	26,780	41%
韓国（KR）	4,716	7%
日本（JP）	3,875	6%
アメリカ（US）	3,352	5%
台湾（TW）	2,867	4%
ロシア連邦（RU）	2,089	3%
ブラジル（BR）	1,903	3%
香港（HK）	1,665	3%
インド（IN）	1,346	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 ***→ 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4月7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。

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。

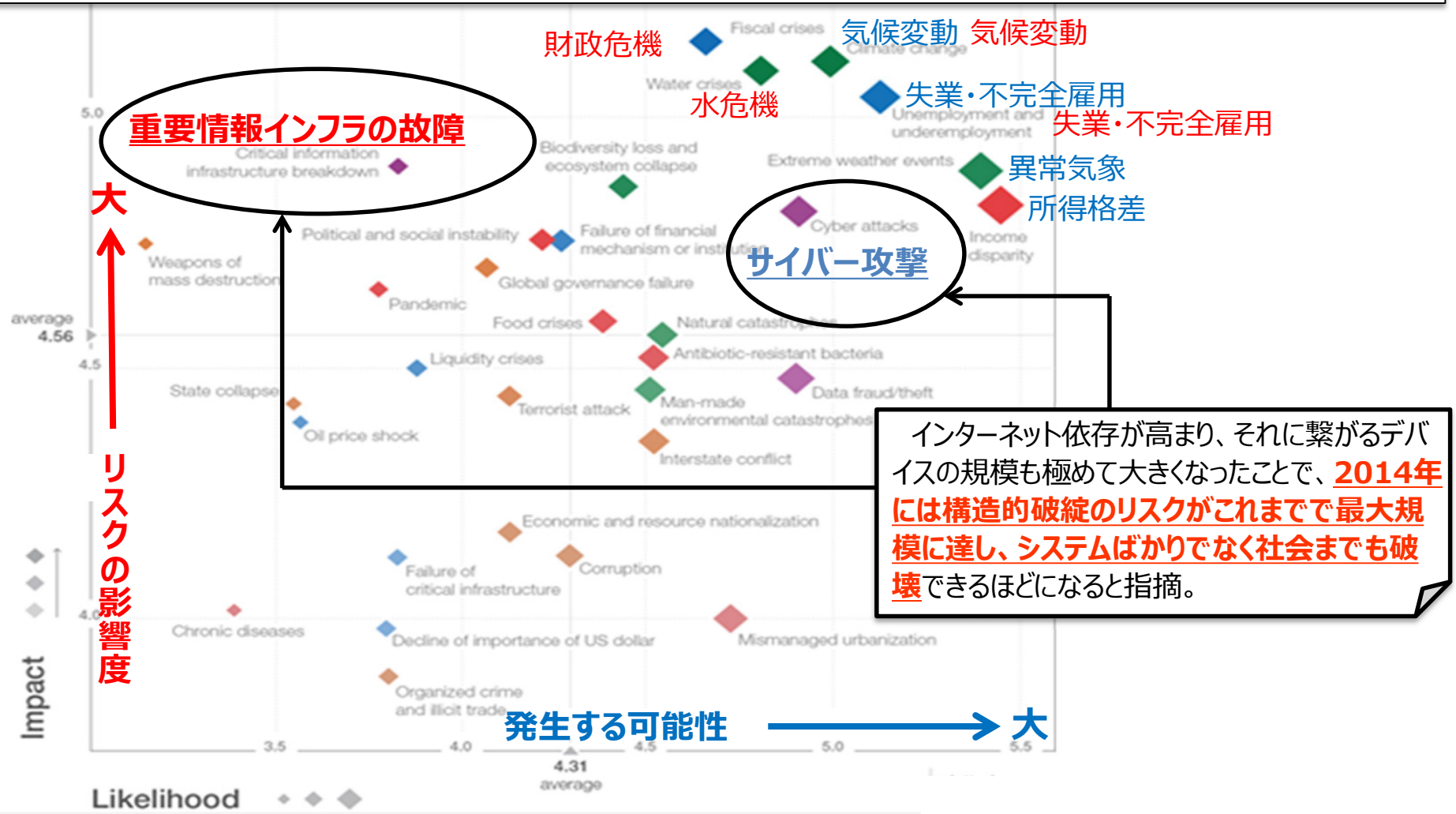
上記について、当局は北朝鮮によるものと発表。昨年7月には、司令塔の強化など新計画を策定。

※「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＞

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)＞

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。

サイバー攻撃の特徴（例）

- 非対称性（高価な兵器を必要とせず、費用がかからない）
- 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）
- 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）
- 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）
- 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）

サイバー空間と国際法の適用関係

“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)

我が国における基本戦略・推進体制の推移

NISC

省庁HP連続改ざん 2000.1
Webサーバの脆弱性への攻撃
米国同時多発テロ 2001.9
フィッシング詐欺 スパイウェア
ボットネットによる攻撃
Winny
誘導型攻撃の出現
DNSキャッシュポイズニング
米韓DDos攻撃
Gumblar猛威
制御システムStuxnet攻撃
9.18攻撃
遠隔操作ウィルス
標的型攻撃 組織的高度化
新領域としてのサイバー空間
感染PCによる不正送金
水飲場型攻撃
重要インフラへの攻撃

年度 2000 2004 2005 2006 2009 2010 2013 2015

各省における試行錯誤

サイバー攻撃への対応を中心とした対策実施時期

IT障害への対応も含めた総合的な対策基盤づくりの推進

サイバー攻撃事態発生を念頭においた危機管理等の観点からの対処態勢の整備等の取組みの重点化
「事故前提社会」への対応力強化など成熟した情報セキュリティ先進国へ向けた取組み

リスクの深刻化の進展に対応した国家安全保障・危機管理等の観点からの取組みの強化

基本戦略

e-Japan戦略（2001.1）
e-Japan戦略Ⅱ（2003.7）
IT新改革戦略（2006.1）
i-Japan戦略2015（2009.7）
新たな情報通信技術戦略（2010.5）
世界最先端IT国家創造宣言（2013.6.14 IT総合戦略本部決定・閣議決定）

【中長期計画】

政府の役割・機能の見直し（2004.12）

サイバーセキュリティ戦略（2013.6.10 情報セキュリティ政策会議決定）

国民を守る情報セキュリティ戦略（2010.5.11 情報セキュリティ政策会議決定）

第1次情報セキュリティ基本計画（2006.2.2 情報セキュリティ政策会議決定）
第2次情報セキュリティ基本計画（2009.2.3 情報セキュリティ政策会議決定）

【年次計画】

2006 2007 2008 2009 2010 2011 2012 サイバーセキュリティ2013 サイバーセキュリティ2014

推進体制

内閣官房 情報セキュリティ対策推進室（2000.2設置）

① 内閣官房情報セキュリティセンター（NISC）（2005.4 設置）
② 情報セキュリティ政策会議（2005.5 設置）
③ GSOC（2008.4 運用開始）
④ CYMAT（2012.6 設置）

NISCの機能強化等

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）

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、化学、クレジット、石油）
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

協力

庶務協力５省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- 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）


重要インフラ事業者　等


政府機関（各府省庁）


企業


個人

「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）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	②●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③●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【2014年5月】 ④●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略）	⑤●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●国際戦略の策定【2013年10月】 ⑥●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

「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）

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）	①②●機微情報を守るためのリスク評価手法の確立【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③●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【2014年5月】 ④●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
⑤「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】	●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
⑥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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

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

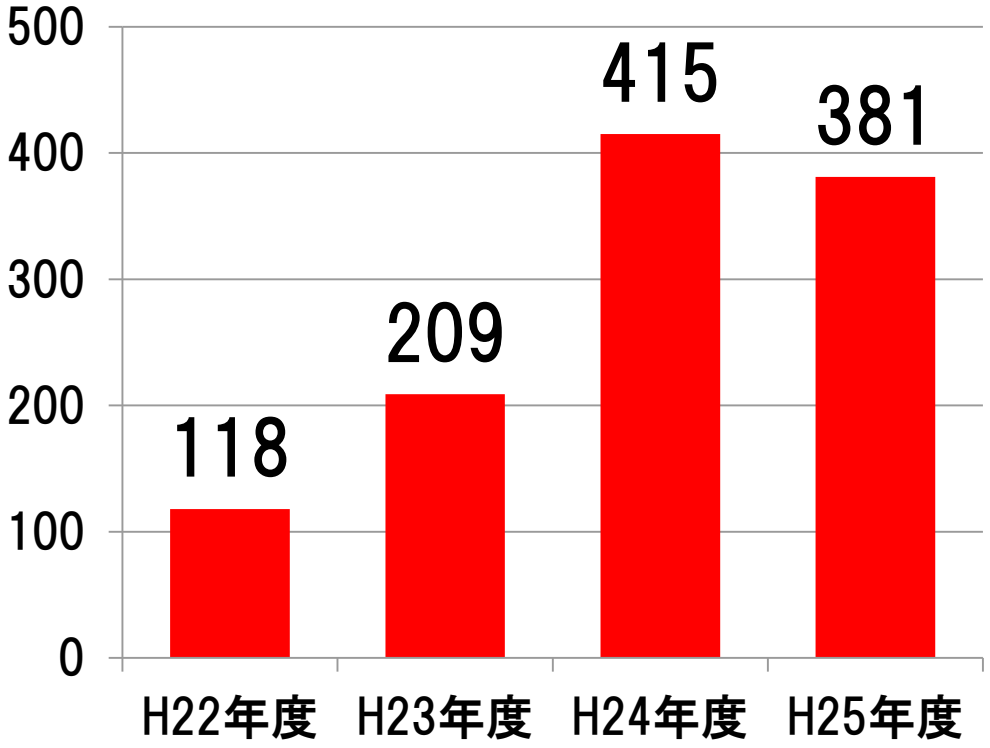
⑤リンク先表示

全く別のアドレスに偽装可能

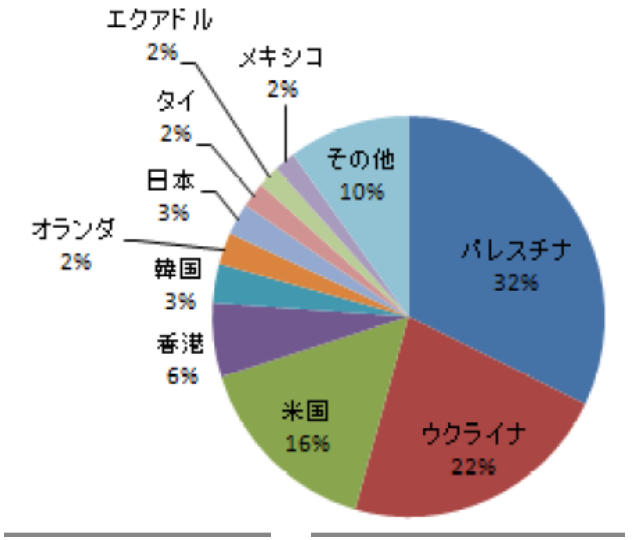
増加する標的型メール攻撃

○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）

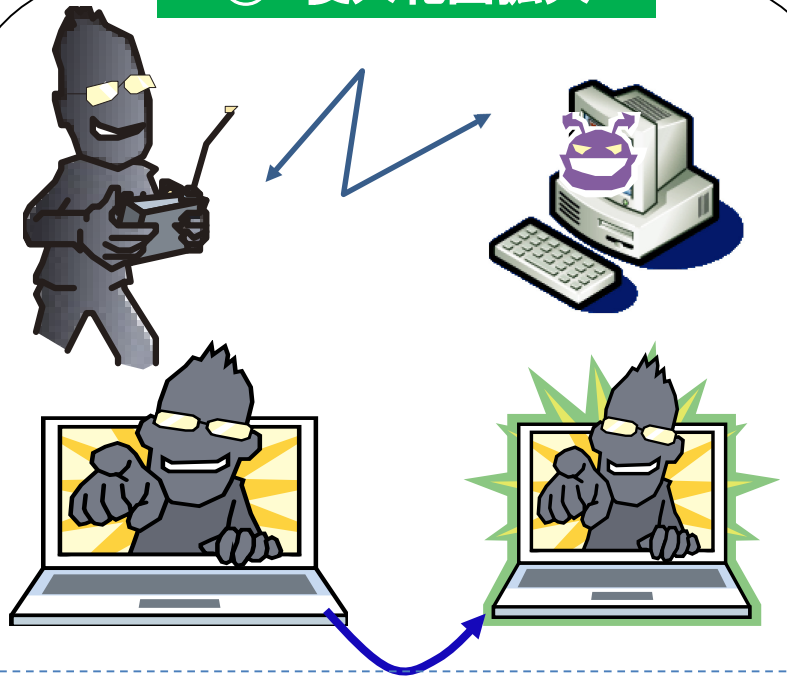
標的型メール攻撃の攻撃プロセス

① 初期潜入

ウィルス
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

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

③ 情報窃取

重要情報の窃取やシステム破壊も

外部（インターネット）

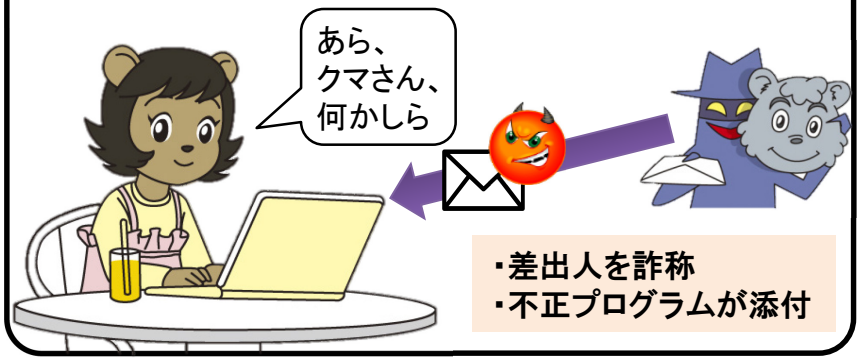
組織内ネットワーク

様々な標的型攻撃

○標的型攻撃は、初期潜入し、遠隔操作により侵入範囲を拡大し、情報窃取等を行うもの
○初期潜入段階において、端末を不正プログラムに感染させるために種々の手口が使われている

A. メール

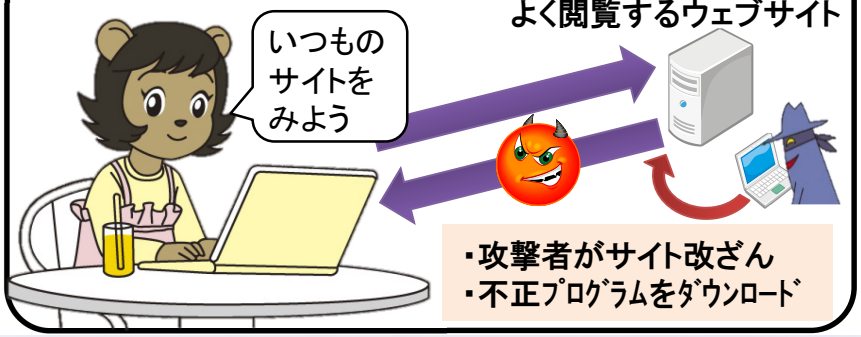
よく知っている人からのメールだと思って添付ファイルを開いてしまうと・・・



・差出人を詐称
・不正プログラムが添付

B. ウェブ閲覧（水飲み場型）

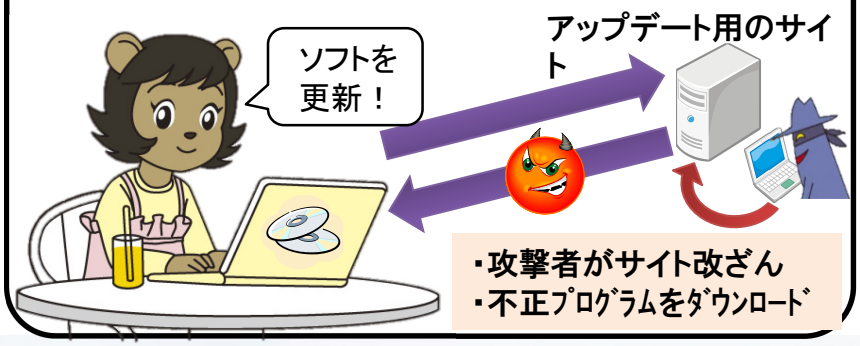
いつも閲覧しているウェブサイトにアクセスすると・・・



・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

C. ソフトウェアアップデートを悪用

ソフトウェアのアップデート機能を使用すると・・・



・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

多重防御を備えたシステム構築が重要

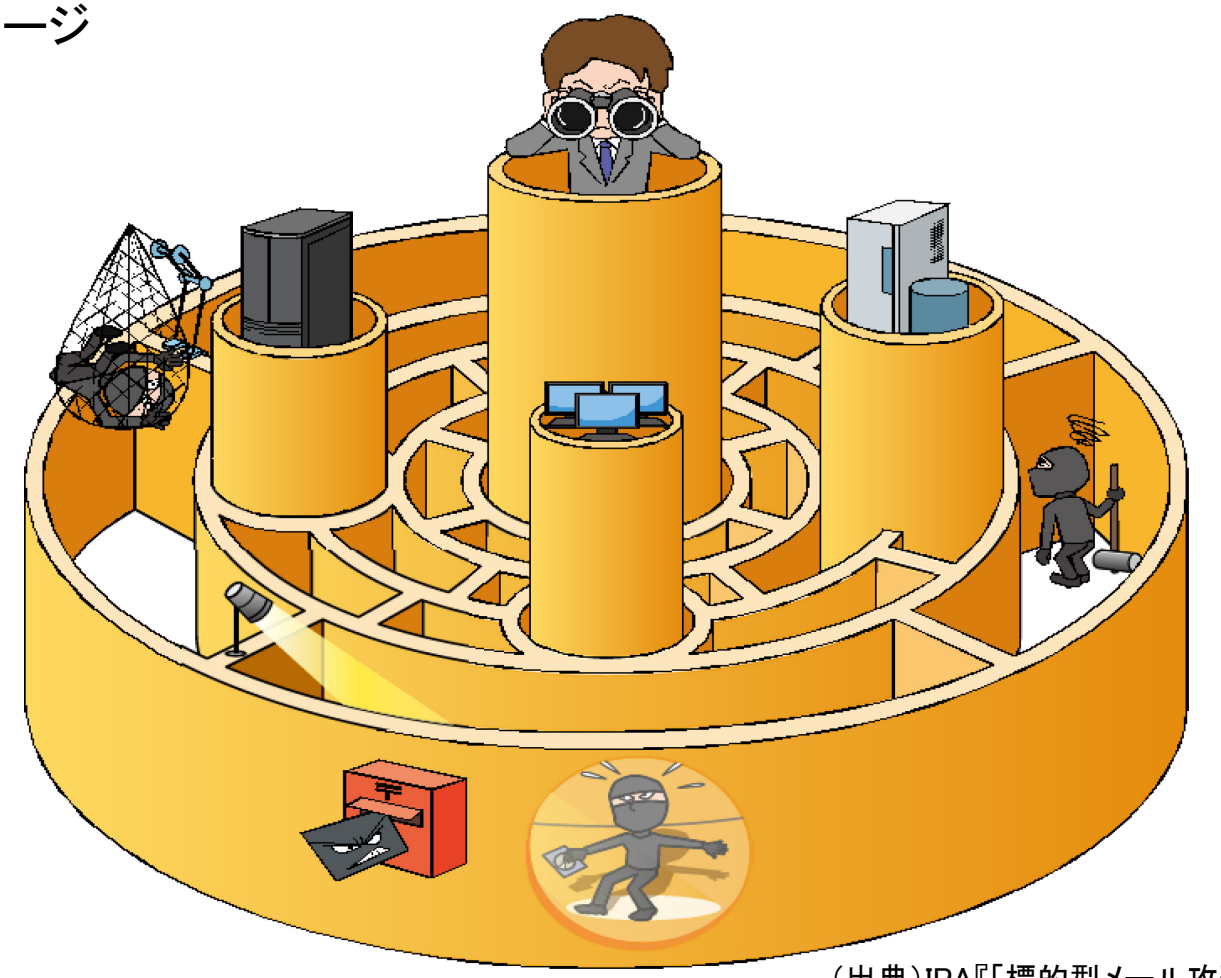
○ 侵入を100%防ぎ続けることは困難。侵入されても被害を抑える対策実施が重要。
○ 単独の対策に頼らない多重防御を備えたシステム構築が重要。

■多重防御を備えたシステムのイメージ

重要なものを重点的に守る

第2、第3の壁を作って攻撃を拡げにくくする

侵入されていないか見張る



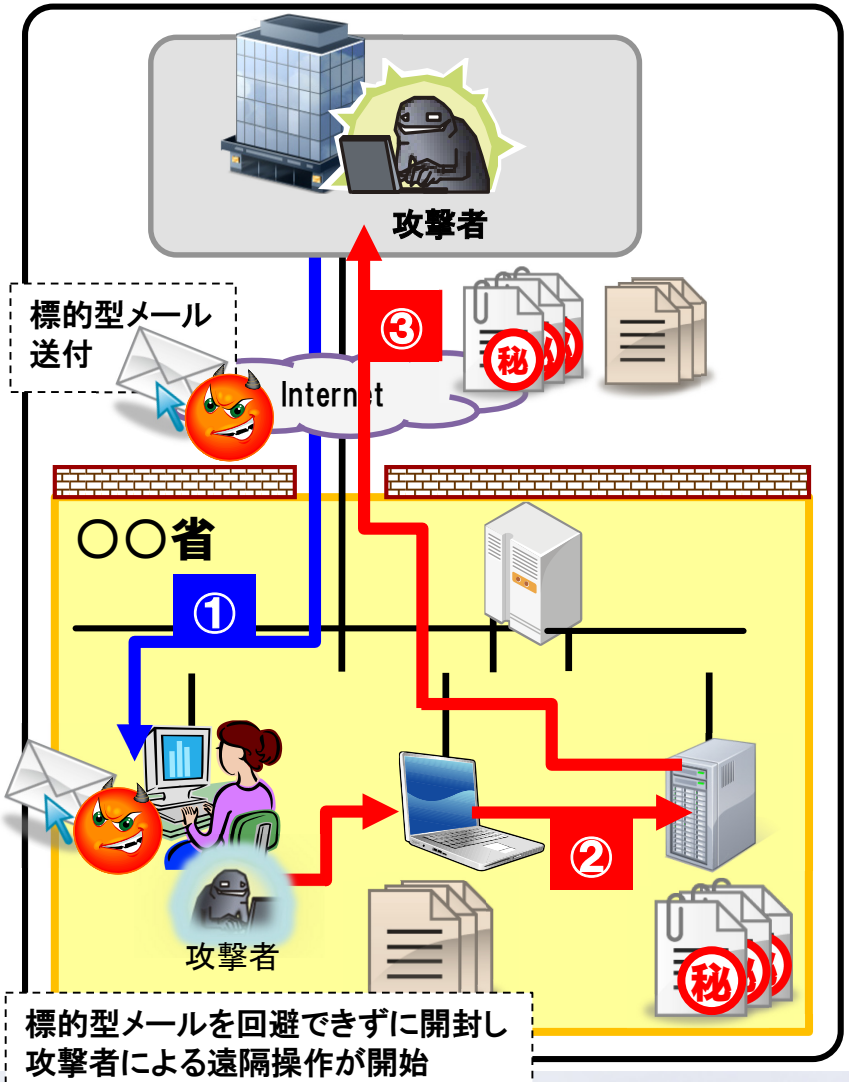
パスワードだけでは
盗まれます！

（出典）IPA『「標的型メール攻撃」対策に向けたシステム設計ガイド』

高度サイバー攻撃（標的型攻撃）対処のための対策実施

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

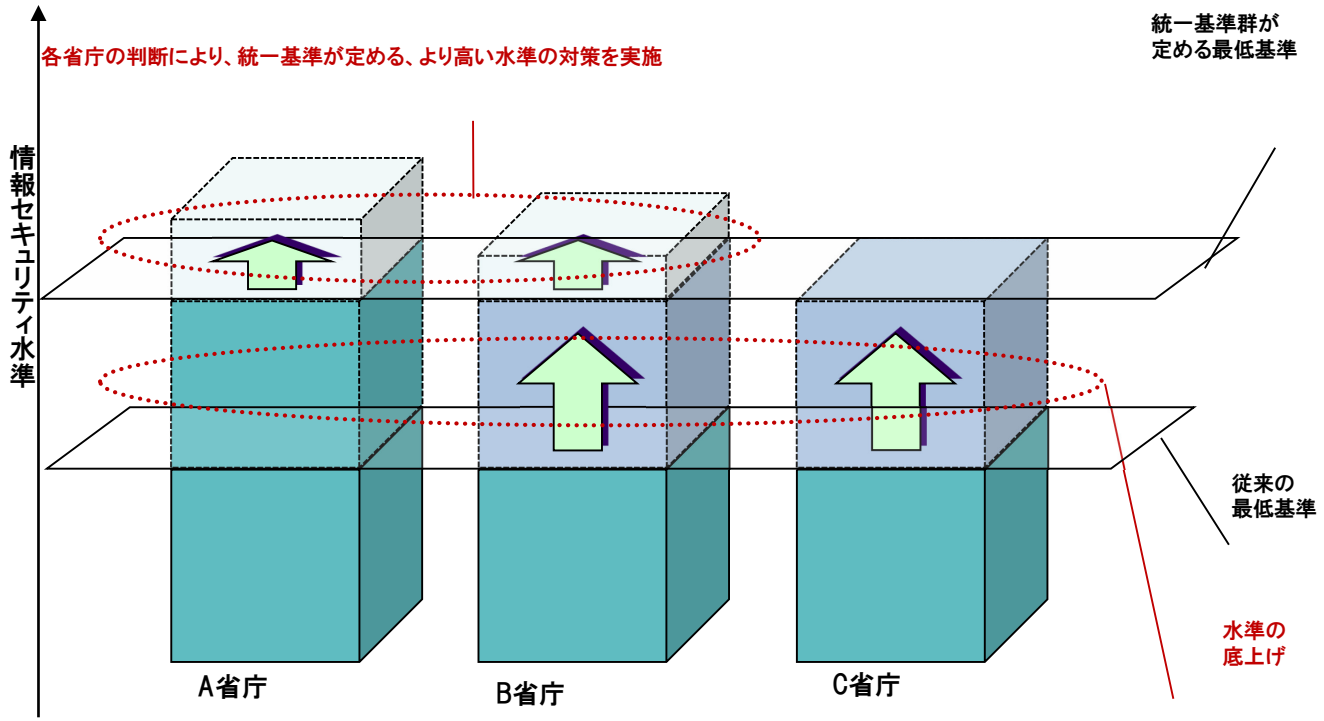
対策目的	対策方針
攻撃を遮断し、侵入範囲の拡大を防止する	• 攻撃者にとってハッキング技術を用いた内部探索をしづらいシステム設計 • 機器乗っ取りをしづらいシステム設計
攻撃の兆候を監視し、早期に発見・検知する	• 攻撃（主に攻撃失敗）の痕跡を残す • 攻撃者の侵入を発見・検知するためのトラップ（罠）を設置 • 上記の継続的な監視

統一基準群（政府機関セキュリティポリシーのベースライン）

○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）＞



統一基準群の改定（14年5月、情報セキュリティ政策会議決定）

現行の統一基準群の課題と改定の方向性

◆ 新たな脅威への対応のための基準の追加

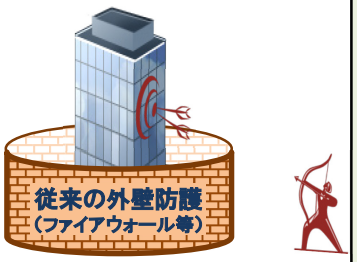
◆ 不明確で分かりにくい基準の明確化

主な改定内容（※）

◆ 標的型攻撃への対策

➢ 標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずる。

標的型攻撃のイメージ



・特定の組織の情報に狙い
・従来の外壁防護を無効化

内部対策の強化が重要

◆ サプライチェーン・リスクへの対策

➢ 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防止のため、厳正な管理を要求。

◆ 分かりやすく、守られやすい基準

➢ 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。

（現行の統一基準における規定の例）

行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。

ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に　報告することができない場合は、定められた　報告手順に従って、最高情報セキュリティ責任者に報告すること。

（見直し案）

行政事務従事者は、情報セキュリティインシデントを認知した場合には、各府省庁の報告窓口に速やかに連絡し、指示に従うこと。

（※「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。）

高度サイバー攻撃対処のための取組等（14年6月、CISO等連絡会議決定）

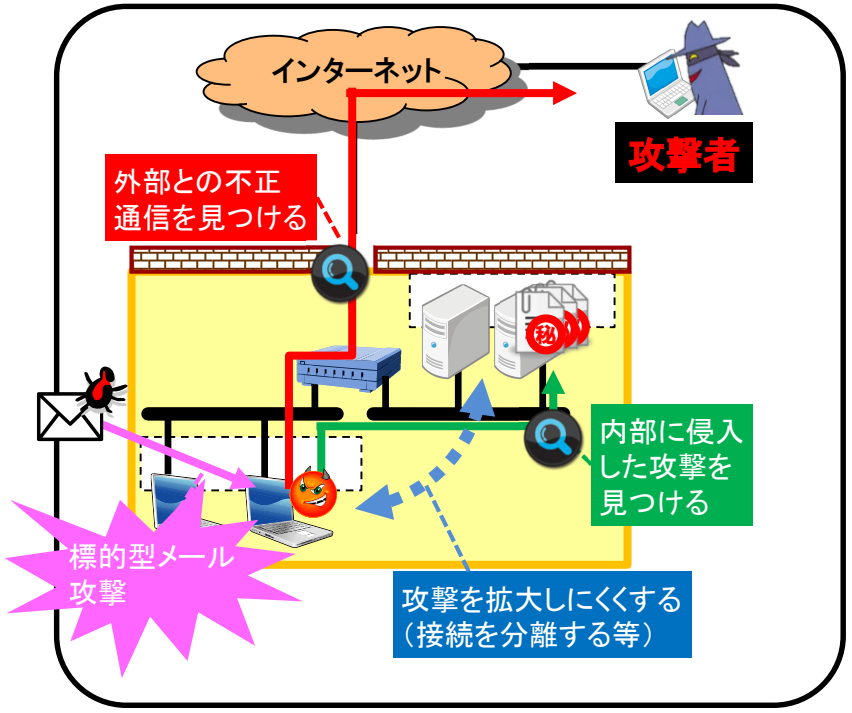
高度サイバー攻撃対処のための取組

◆ 取組の概要

- 高度サイバー攻撃の脅威から重要な業務・情報を取り扱う情報システムを守るため、それらを特定し、対象となる情報システム内部に侵入した攻撃の発見・遮断を目的とした対策を、計画的・重点的に実施する取組を今年度から本格的に実施する。

（平成26年6月25日　情報セキュリティ対策推進会議）

情報セキュリティ対策の概要（例）



独立行政法人における情報セキュリティ対策の推進

◆ 独立行政法人におけるセキュリティ対策の推進

- 独立行政法人がサイバー攻撃の標的となっている事例が複数判明
- 独立行政法人においても、政府の重要な情報を扱う場合は、政府機関と同等の情報セキュリティ対策を講ずることを決定

（平成26年6月25日　情報セキュリティ対策推進会議）

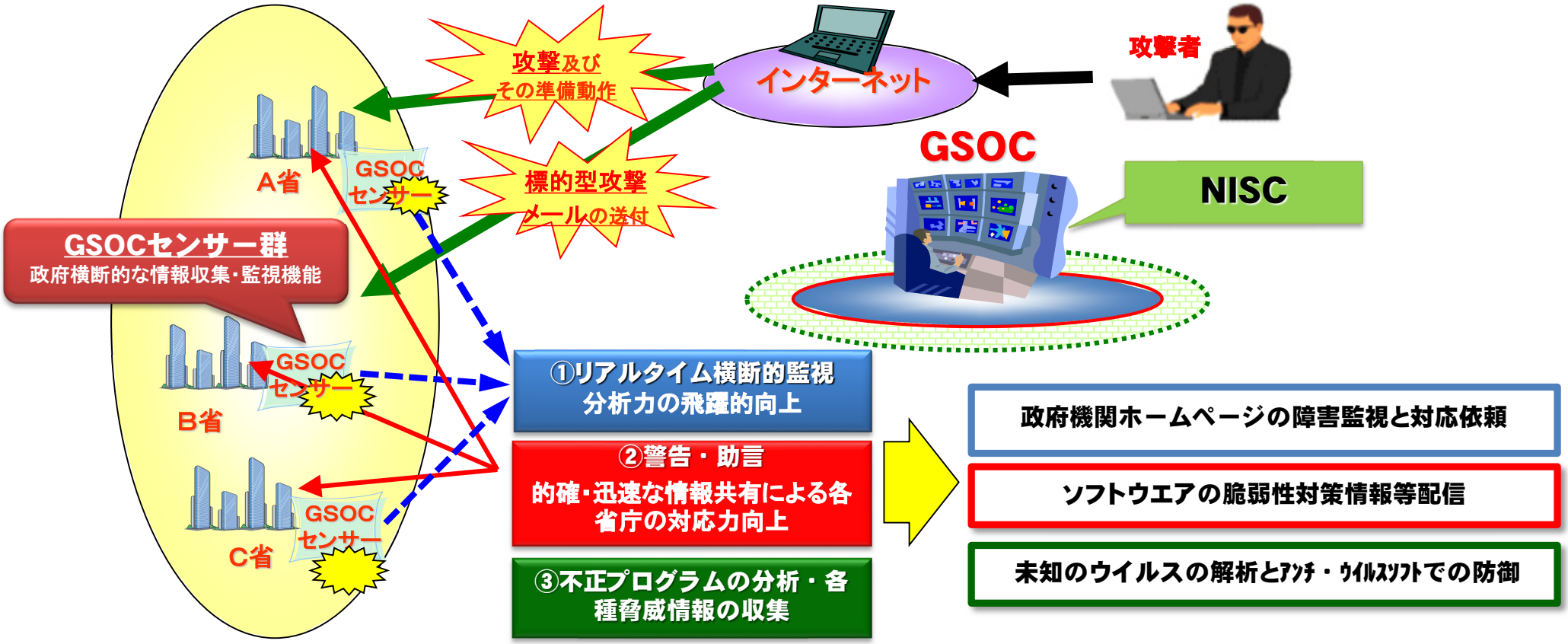
独法及び主務省庁が一体となって対策を推進

1. 業務計画の中で情報セキュリティ対策を位置付け
   - 統一基準群を踏まえた情報セキュリティ対策を独法にも適用
2. 連絡体制構築により、迅速な情報連絡・共有
   - 経営管理層への情報展開、判断による迅速な対応
3. 業務評価の際にフォローアップし、対策を着実に推進
   - 対策の実効性確保のための推進力

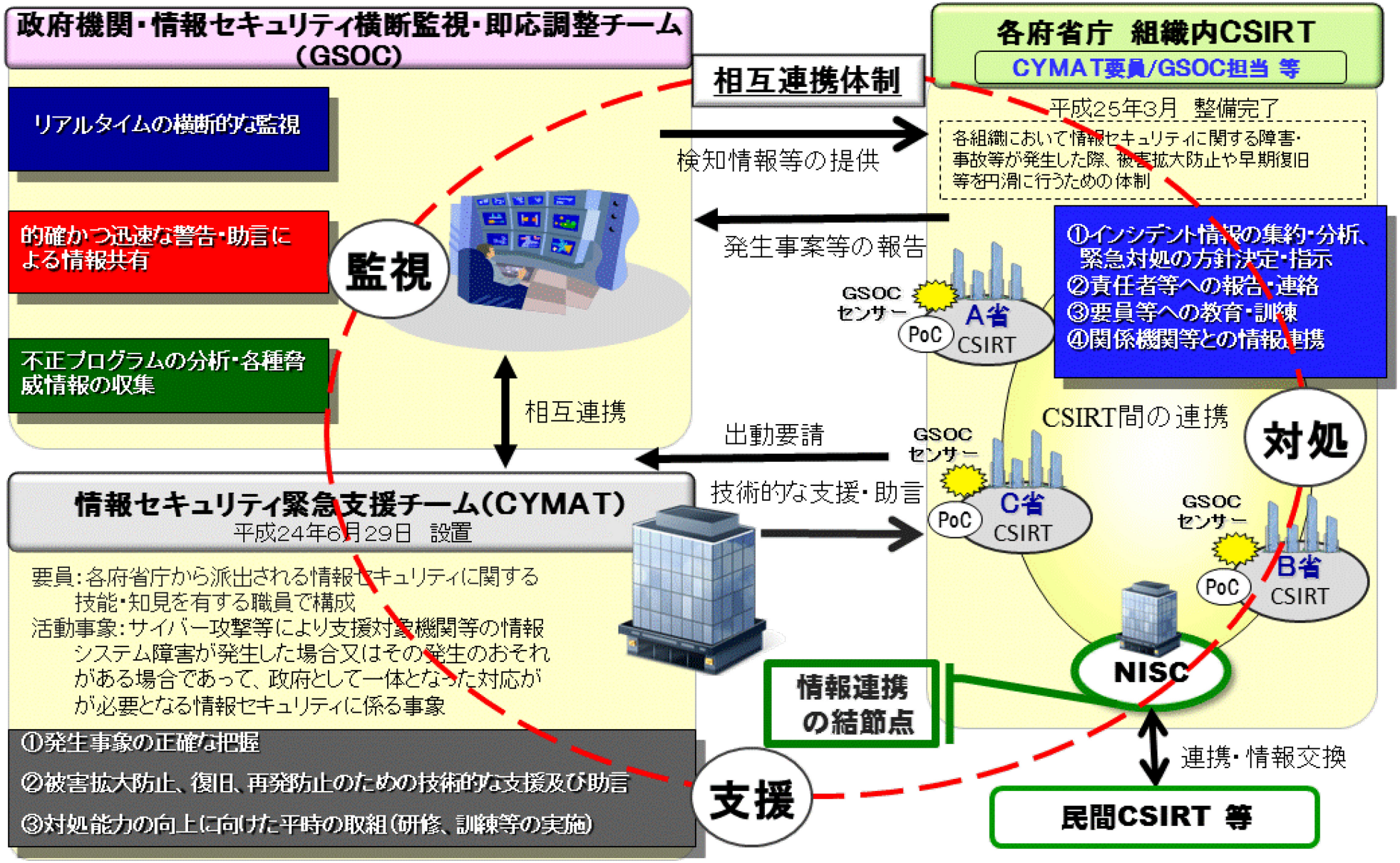
GSOC（ジーソック）

【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



「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）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	② ●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③ ●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【2014年5月】 ④ ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
⑤ 「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】	●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
⑥ 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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

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

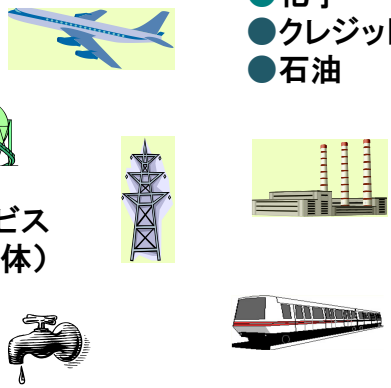
（2014年5月、情報セキュリティ政策会議決定）

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
- 化学
- クレジット
- 石油



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

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

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・演習・訓練間の連携によるIT障害対応体制の総合的な強化

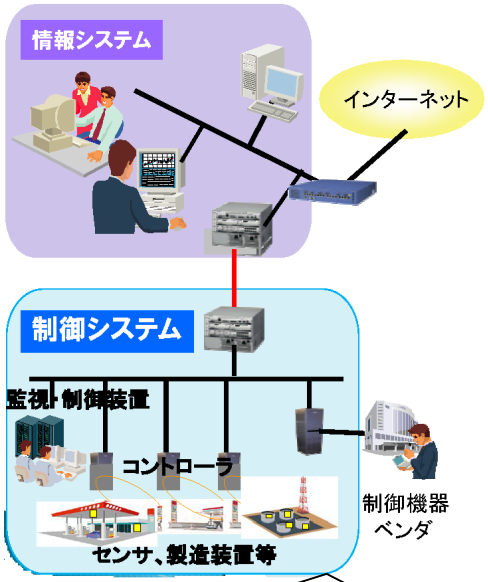
リスクマネジメント

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。

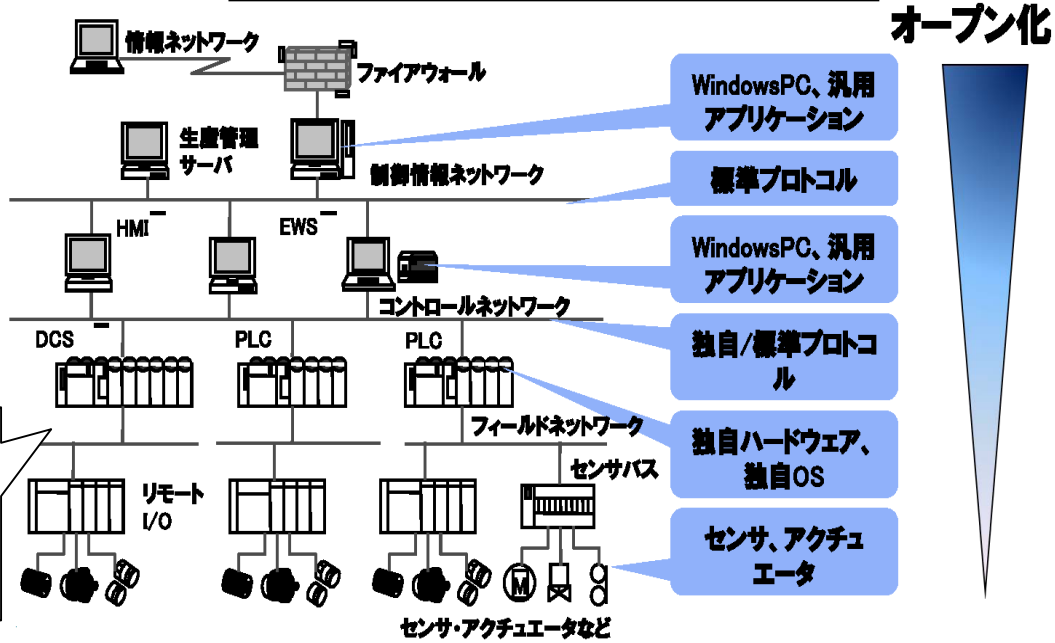
最近の状況

○ 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」（平成25年6月情報セキュリティ政策会議）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	②●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③●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【2014年5月】 ④●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
⑤「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】⑥	●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

新・情報セキュリティ人材育成プログラム（１４年５月、情報セキュリティ政策会議決定）

NISC

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） *IPA調べ

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

○**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。

企業等における情報漏えいインシデントの動向

○企業等における情報漏えいインシデントについて、全体の件数自体は減少しているが、**不正アクセスを原因とする大規模な被害**が急増。

2013年個人情報漏えいインシデント

	2013年データ	2012年データ
漏えい人数	931万2543人	972万65人
漏えい件数	1333件	2357件
想定損害賠償総額	2020億6575万円	2132億6405万円
一件当たりの漏えい人数	7385人	4245人
一件当たり平均想定損害賠償額	1億6024万円	9313万円
一人当たり平均想定損害賠償額	2万7675円	4万4628円

件数は減少

被害が大規模化

インシデントの規模トップ10

No.	漏えい人数	業種	原因
1	400万人	情報通信業	不正アクセス
2	169万2496人	情報通信業	不正アクセス
3	47万人	卸売業，小売業	不正アクセス
4	42万6000人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24万3266人	情報通信業	不正アクセス
6	17万5297人	情報通信業	設定ミス
7	15万0165人	卸売業，小売業	不正アクセス
8	12万0616人	金融業，保険業	管理ミス
9	10万9112人	情報通信業	不正アクセス
10	9万7438人	情報通信業	不正アクセス

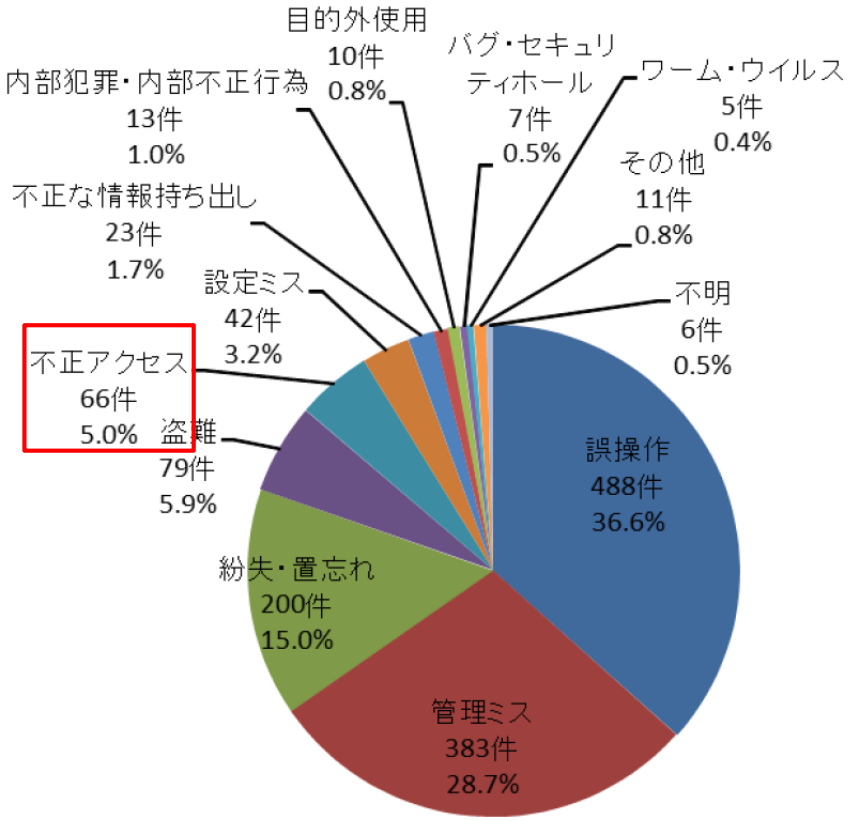
情報通信業が多い

2013年は不正アクセスが急増！

100万人以上！

大規模な漏えいの上位を占める不正アクセス

2013年原因別インシデント数



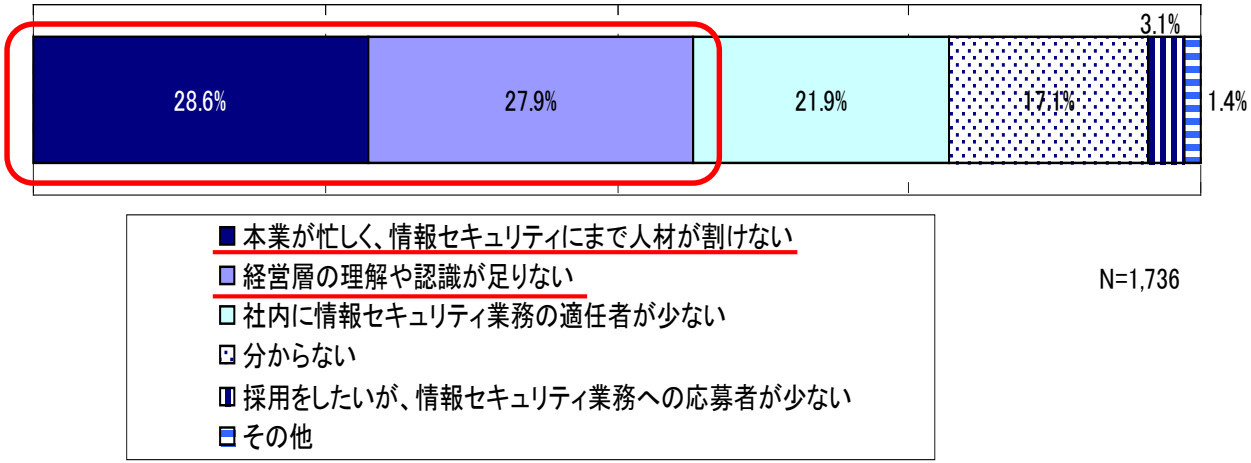
出典：2013年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～（日本ネットワークセキュリティ協会（JNSA））

2013年1月1日～12月31日の1年間にインターネットニュース等で報道されたインシデントの記事、組織から公表されたインシデントのプレスリリース等をもとに集計。想定損害賠償額については、JNSAが開発したモデルを用いて推定。

企業等における情報セキュリティ対策の現状

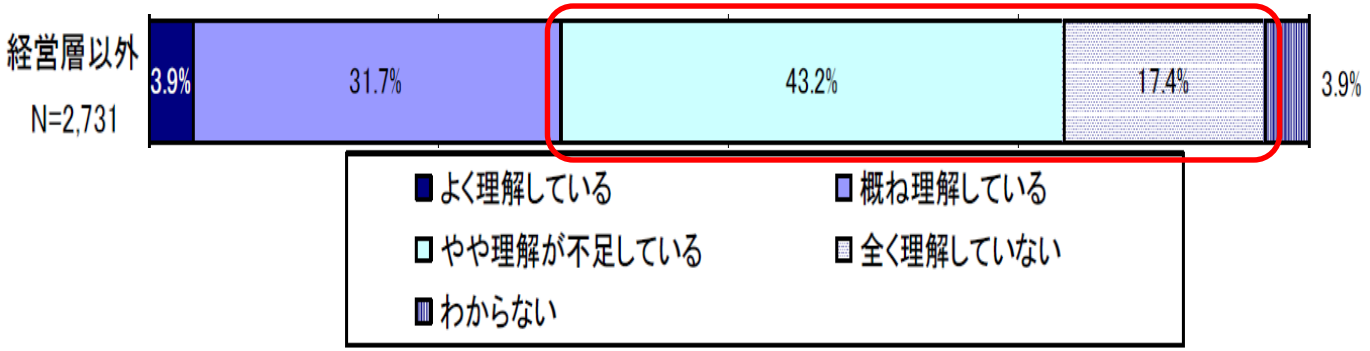
○企業では**情報セキュリティに関する業務に従事する人員が不足**。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

人材不足の原因（社内向け業務）



企業経営層の情報セキュリティに対する理解度

（経営層以外からの回答）



出典：独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012年4月

米証券取引委員会(SEC)「企業財務部門開示ガイダンス」

「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ると考えられる場合には、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。

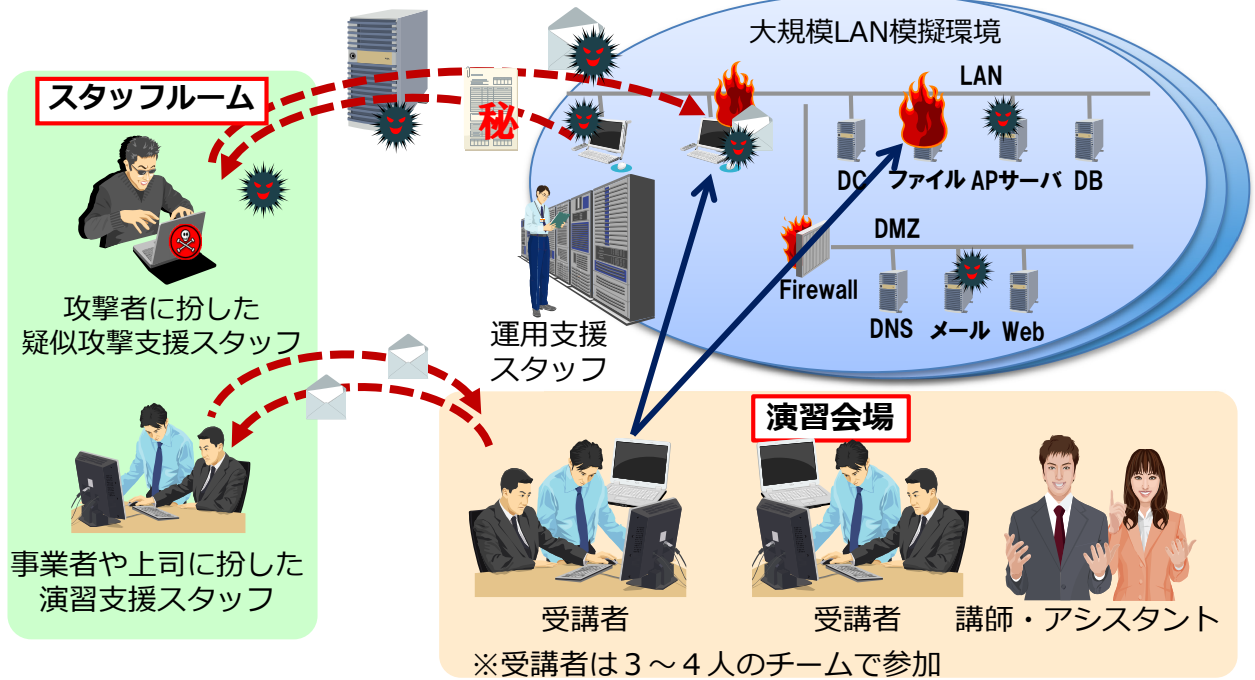
＊1 Management's Discussion and Analysis of Financial Condition and Results of Operations：経営者による財政状態及び経営成績の検討と分析。米国では、SECが投資家への情報提供の一環として企業に開示を要求している。

（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充実

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

iパス	◆ **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)**
基本情報技術者試験(FE) 応用情報技術者試験(AP)	◆ 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)**

※ IPA プレス発表「i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)iパスは 平成26年5月7日以降、i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。**(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。

新・情報セキュリティ普及啓発プログラム（14年７月、情報セキュリティ政策会議決定）

NISC

背景

・若年層から高齢者までの**あらゆる世代**、個人・家庭・職場・公共施設などの**あらゆる場面**、国民1人1人の日常生活や社会経済活動等の**あらゆる活動**にサイバー空間が拡大・浸透。

・オリンピック・パラリンピック東京大会が開催される2020年を見据え、我が国として情報セキュリティ水準の向上が急務。

課題

国民1人1人や企業が自ら具体的な情報セキュリティ対策を進んで実行できるよう、以下の課題への対応が必要

○一般利用者等における認識の更なる醸成　○地域における普及啓発活動の活性化　○主体的な普及啓発の促進

今後の取組方針

基本的な考え方

国民全体の情報セキュリティへの関心・理解度・対応力の強化・増進を図る

推進体制

産学官民の多様な主体で構成する**協議会形式の場**を設け、国民運動として普及啓発活動を推進していく体制を構築。
各主体が自律的に取り組める環境を整備し、国民1人1人に身近な地域との連携を推進。

主な取組

①総合的・集中的な普及啓発施策の更なる推進

…・「情報セキュリティ月間」の期間を拡大(2月～3月18日＜サイバー訓練の日＞)し、広く国民に啓発。
・期間を問わず、ロゴマークやメディア等を活用し、国民に親しみやすい取組を推進し、取組の定着化を図る。
・国民1人1人が、サイバー空間の脅威から自ら身を守ることができるよう、国民運動として対策の実践や訓練等を促進。

②地域における取組の促進

…地域における各主体の活動や情報共有を促進。協議会形式の場を通じ、地域発産学官民連携による取組を全国的な動きに発展。

③特に注力が必要な層に対するきめ細やかな普及啓発活動の推進

…国民全体を対象とした活動に加え、特に注力が必要なターゲット（初等中等教育層、学ぶ機会が少ない層、関心が薄い層、中小企業含めた企業等）に対し、協議会形式の場も活用してきめ細やかな普及啓発を推進。

「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）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	② ●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③ ●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【2014年5月】 ④ ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略）	⑤ ●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●国際戦略の策定【2013年10月】 ⑥ ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

情報セキュリティ研究開発戦略（改定版）（14年７月、情報セキュリティ政策会議決定）

サイバーセキュリティ戦略（2013年6月策定）において示された
- ○ 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**
   - ・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
   - ・研究者等へ政府の有するサイバー攻撃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**
   - ・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進
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**
   - ・今後発展が期待されるICT利用分野で上流工程からセキュリティ品質の組込を推進
4. **情報セキュリティのコア技術の保持**
   - ・暗号等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維持・強化
5. **国際連携による研究開発の強化**
   - ・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

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
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など他分野との融合

情報セキュリティ研究開発における重要分野

（※　左記の観点を踏まえ、重要分野を整理）

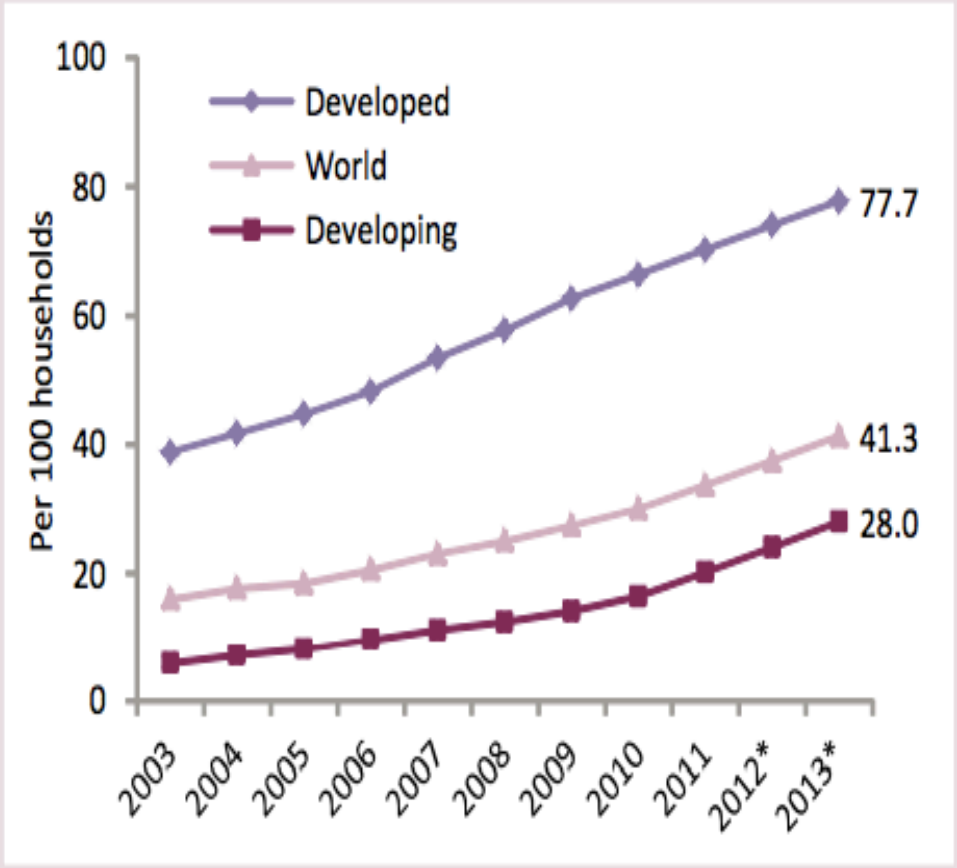
(1)情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク　等
(2)ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保　等
(3)個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用　等
(4)研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術　等
(5)発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続　等

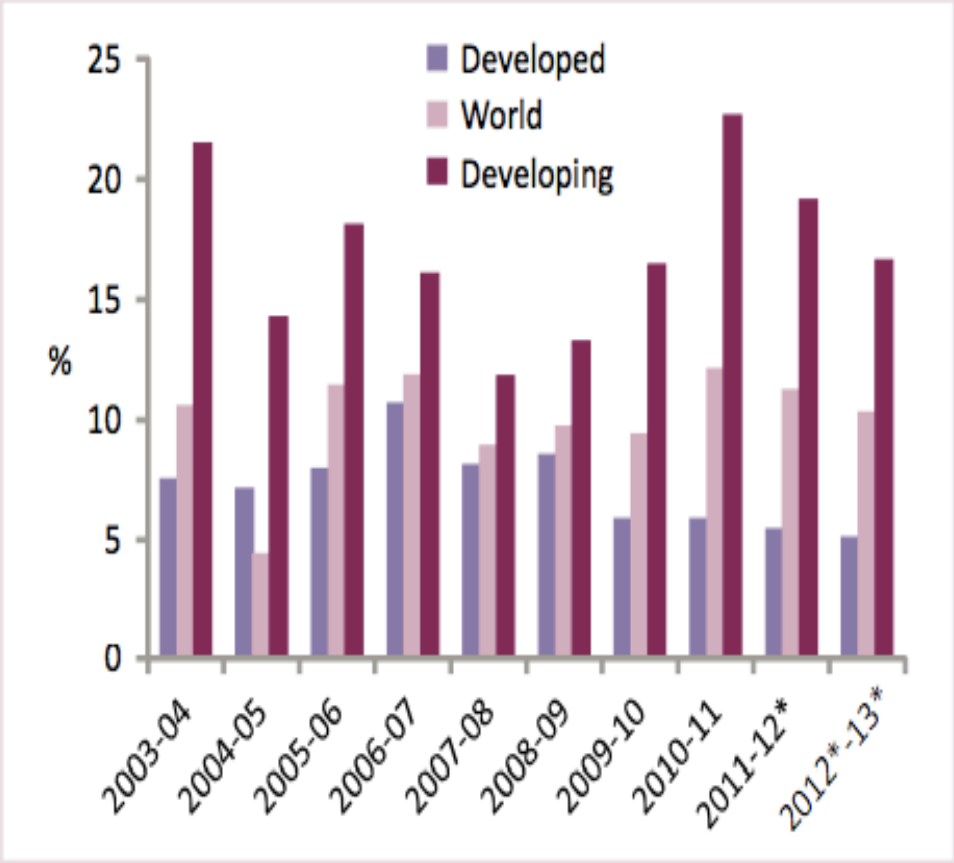
「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	② ●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③ ●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【2014年5月】 ④ ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略）	⑤ ●国際戦略の策定【2013年10月】 ⑥	●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）	〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。 〈注２〉 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。 〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。 ●共同意識啓発活動【毎年10月】
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）【継続審議中】		

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

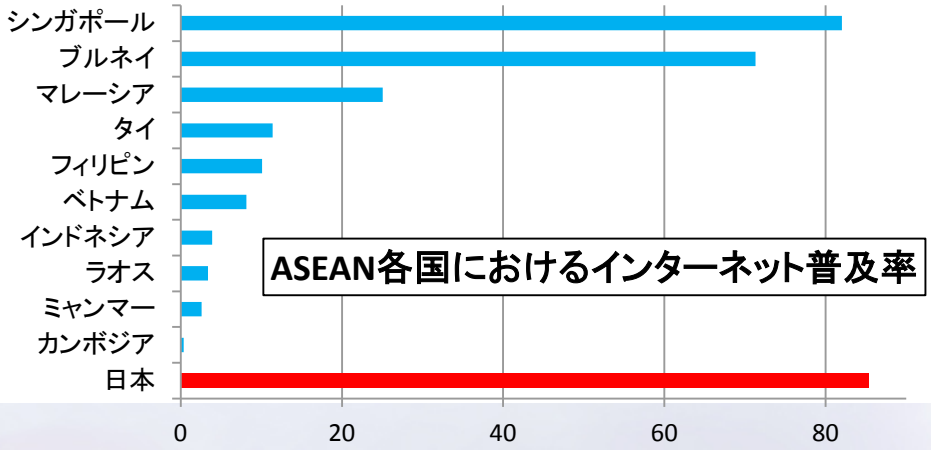
ビジョン
ICTによる経済の強化と変革に向けて
包括的、活気のある、統合化されたASEANの構築

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

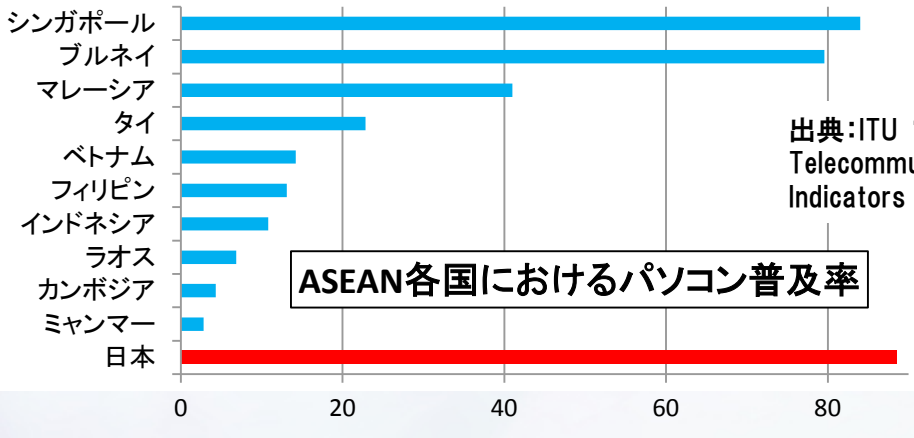
基盤的取組
4. インフラ開発
5. 人材開発
6. デジタルディバイドの解消

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2回日EU・ICTｾｷｭﾘﾃｨﾜｰｸｼｮｯﾌﾟ：２０１３年12月
●第1回日EUサイバー協議：本年10月

英国
●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、等に関する意見交換
●第1回日英サイバー協議：２０１２年6月

インド
●安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護等に関する　意見交換
●第1回日印サイバー協議：２０１２年11月

エストニア
○日エストニアサイバー協議の立上げ準備中

フランス
○日仏サイバー協議の立上げ準備中

イスラエル
○日イスラエル・サイバー協議の立上げ準備中

ロシア
○日露サイバー協議の立ち上げ予定

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。

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

米国
●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@ワシントン

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25年9月
●共同意識啓発活動の実施：２０１２年10月～

オーストラリア
○日豪サイバー協議の立上げ準備中

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。　●ハーグ会議：２０１５年4月

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」（平成25年6月情報セキュリティ政策会議）

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【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●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【2014年5月】	② ●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【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●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【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●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 ●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）	③ ●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【2014年5月】 ④ ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
⑤ 「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】	●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		●共同意識啓発活動【毎年10月】
⑥ 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）【継続審議中】		

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 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。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

サイバーセキュリティ政策に係る年次報告（2013年度）

（14年７月、情報セキュリティ政策会議決定）

- 「サイバーセキュリティ戦略」（2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度）に基づく初めての年次報告。
- 従前は個別に報告・公表してきた、政府機関等・重要インフラ事業者等における取組、各府省庁の関連施策の評価・実施状況等を1冊に集約。

年次報告 本編

年次報告 別添

＜凡例：従前の報告・公表事項等との対応＞

- 主に「201x年度の情報セキュリティ政策の評価等」として報告してきた内容
- 主に「政府機関における情報セキュリティに係る年次報告」として報告してきた内容
- 主に重要インフラ専門委員会で報告・公表してきた内容
- 本年次報告に当たって新規に設けた内容

サイバーセキュリティ2014（14年7月、情報セキュリティ政策会議決定）

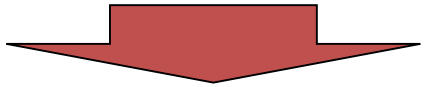
NISC

▸「サイバーセキュリティ戦略」(2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度)に基づく年次計画の2期目。

	2013	2014	2015
戦略	「サイバーセキュリティ戦略」（2013/06/10）		
年次計画	「サイバーセキュリティ2013」（2013/06/27） • 戦略に基づき、各分野で新たな方針／プログラム等を策定	「サイバーセキュリティ2014」（2014/07/10） • 新たな方針／プログラム等を踏まえ、個々の施策をより具体化して推進	
「強靭な」サイバー空間	「政府機関統一基準群」改定（2014/05/19） 「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」策定（2014/05/19） 「情報セキュリティ普及・啓発プログラム」改定（2014/07/10）	【主な施策】 • 政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し（内閣官房及び全府省庁） • 政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化（内閣官房及び総務省） • 調達時における対策の推進（内閣官房） • GSOCの抜本的強化（内閣官房及び全府省庁） • 重要インフラに関する、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化（内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁） • 新たな情報セキュリティ普及啓発プログラムの策定・推進（内閣官房及び関係府省庁） • 高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築（総務省） • 日本版NCFTAの創設に向けた検討（警察庁） • 防衛情報通信基盤(DII)の整備（防衛省） • 国家レベルのサイバー攻撃への対応の強化（内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係省庁）	
「活力ある」サイバー空間	「情報セキュリティ研究開発戦略」改定（2014/07/10） 「情報セキュリティ人材育成プログラム」改定（2014/05/19）	【主な施策】 • 情報セキュリティ研究開発戦略の研究開発の推進（内閣官房及び関係府省庁） • 新・情報セキュリティ人材育成プログラムの推進（内閣官房） • サイバー攻撃事前防止・早期対策に向けた取組の推進（総務省） • 情報セキュリティに係る競技会・演習等の実施（総務省及び経済産業省） • 情報処理技術者試験制度に関する在り方についての検討（経済産業省）	
「世界を率先する」サイバー空間	「サイバーセキュリティ国際連携取組方針」策定（2013/10/02）	【主な施策】 • サイバー空間に関する国際的な規範作りへの参画等（内閣官房、総務省、外務省、経済産業省及び関係府省庁） • サイバーセキュリティ政策に関する二国間対話の強化（内閣官房、総務省、外務省、経済産業省及び関係府省庁） • 多国間の枠組み等における国際連携・協力の推進（内閣官房、外務省及び関係府省庁） • サイバー攻撃に関する諸外国関係機関との連携の強化（警察庁及び法務省） • 諸外国とのCSIRT間連携の強化（経済産業省）	
推進体制等	「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組方針」（審議継続中）	【主な施策】 • NISCの機能強化（内閣官房） • 官民の情報共有の更なる推進（内閣官房及び関係府省庁）	

オリンピック・パラリンピック・ロンドン大会(2012)の教訓

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、電力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 Fast"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、日英ｻｲﾊﾞｰ協議)

NISCの機能強化に関する政府方針

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）

NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、**GSOCの抜本的な強化**を図るとともに、サイバー攻撃に関する**インシデントに関する情報等の集約**、サイバーセキュリティに関する**国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知**、政府機関及び独立行政法人等の**関連専門機関等に分散している各種機能の有機的な連携による動的な対応**等を強化する。その際、**国際的なインシデント対応における我が国の窓口となるCSIRT機能**の在り方についても併せて検討する。

以上を踏まえ、NISCについては、**専門職員の採用や育成等の人事管理による人材の確保**や**権限等の必要な組織体制**を整備することにより、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組するものとする。

国家安全保障戦略（平成25年12月国家安全保障会議決定・閣議決定）

サイバーセキュリティを脅かす不正行為からサイバー空間を守り、その自由かつ安全な利用を確保する。また、国家の関与が疑われるものを含むサイバー攻撃から我が国の重要な社会システムを防護する。このため、**国全体として、組織・分野横断的な取組を総合的に推進**し、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る。

そこで、**平素から、リスクアセスメントに基づくシステムの設計・構築・運用、事案の発生の把握、被害の拡大防止、原因の分析究明、類似事案の発生防止**等の分野において、**官民の連携を強化**する。また、**セキュリティ人材層の強化、制御システムの防護、サプライチェーンリスク問題への対応**についても総合的に検討を行い、必要な措置を講ずる。

さらに、国全体としてサイバー防護・対応能力を一層強化するため、**関係機関の連携強化と役割分担の明確化**を図るとともに、**サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上**及びこれらの任務を担う**組織の強化**を含む各種施策を推進する。

かかる施策の推進に当たっては、幅広い分野における**国際連携の強化**が不可欠である。このため、**技術・運用両面における国際協力の強化**のための施策を講ずる。また、**関係国との情報共有の拡大**を図るほか、サイバー防衛協力を推進する。

サイバーセキュリティ基本法の概要

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、強靭な体制の構築

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 国の行政機関等におけるサイバーセキュリティの確保

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

⇒ 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

内閣

サイバーセキュリティ戦略の案の閣議請議

内閣総理大臣

戦略の案の作成

行政各部の指揮監督に関する意見具申

IT総合戦略本部

① 高度情報通信ネットワーク社会の形成に関する重点計画の作成、同計画の実施推進

② 上記のほか、同社会の形成に関する施策で重要なものの企画に関する審議、同施策の実施推進

※ 上記の実施推進のうち、府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価を政府CIOに委任

本部長　：官房長官
副本部長：国務大臣
本部員　：国家公安委員会委員長、総務大臣、外務大臣、経産大臣、防衛大臣、上記以外の国務大臣のうち本部の事務を遂行するために特に必要があるとして総理が指定する大臣
有識者のうち総理が任命する者

戦略案の意見

重要事項について緊密連携

サイバーセキュリティ戦略本部

①サイバーセキュリティ戦略の案の作成及び同戦略の実施推進

② 国の行政機関及び独法における対策基準の作成及び同基準に基づく施策の評価（監査を含む。）その他の同基準に基づく施策の実施推進

③ 国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）

④ 上記のほか、次の事務

イ）サイバーセキュリティに関する重要施策の企画に関する調査審議

ロ）同施策に関する府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価その他の実施推進

ハ）同施策の総合調整

国家安全保障会議

① 国家安全保障に関する外交政策及び防衛政策に関し、平素から機動的・実質的に審議

② 武力攻撃事態等への対処等の国防に関する重要事項に関し審議

③ 重大緊急事態への対処に関する重要事項に関し、集中して機動的かつ実質的に審議し、必要に応じて、政府がとるべき措置等について建議

戦略案の意見

我が国の安全保障に関する重要事項について緊密連携

資料等必要な協力の求め

情報の提供等の協力の求め

地方公共団体、独立行政法人、国立大学、特殊法人・認可法人であって本部が指定するもの、国内外の関係者との連絡調整を行う関係機関　等

地方公共団体

求めに応じるよう努める

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
（情報セキュリティセンター[NISC]の法制化等）

資料等提供義務

勧告

勧告に基づく措置の報告聴取

各府省等

Any question?