



National center of Incident readiness and
Strategy for Cybersecurity

我が国のサイバーセキュリティ戦略

2015年3月20日

内閣サイバー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
- 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月デンブ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

【我が国社会全体への浸透】

いつでもどこでも何でも



スマートフォン

世帯保有率が**6倍**に急増※
 (2010年末:約10%→**2013年末:約63%**)
 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



※ 総務省「平成25年版情報通信白書」
 ※※ トレンドマイクロ(株)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)

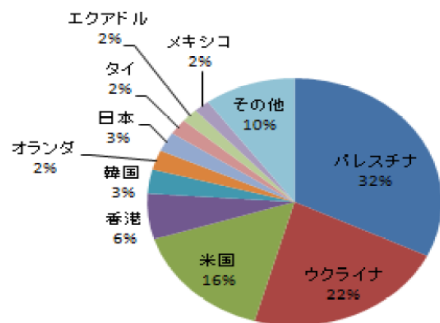
世界中からの多様な主体による攻撃

【海外からの我が国への攻撃状況※】

グローバル化

【最近の主な事例】

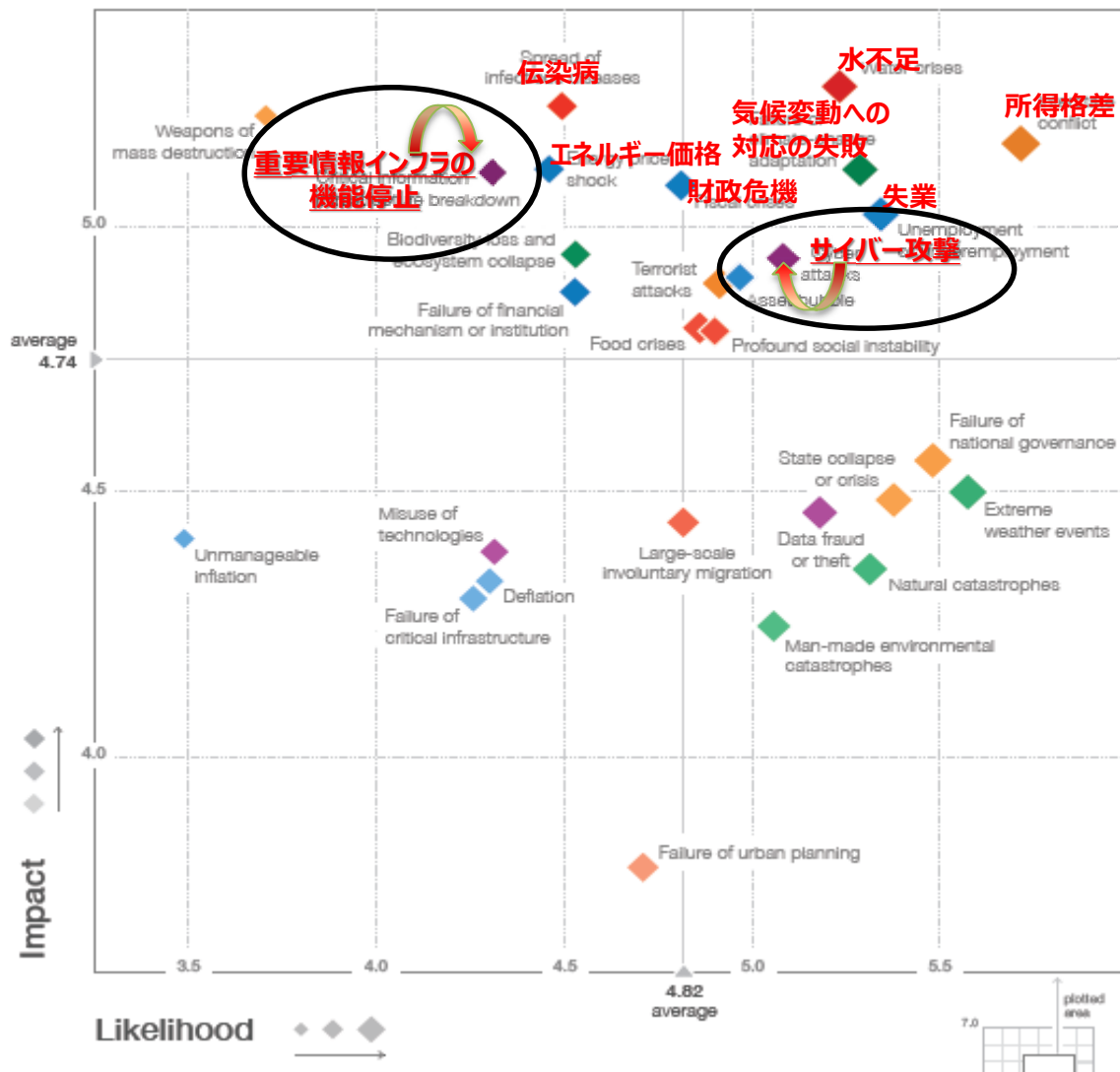
国家関与の可能性



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
(備考)	
2014.12	【米国】SPE社に対するサイバー攻撃が発生。米国政府は北朝鮮に責任ありとし、 国家安全保障上の問題として対応 。

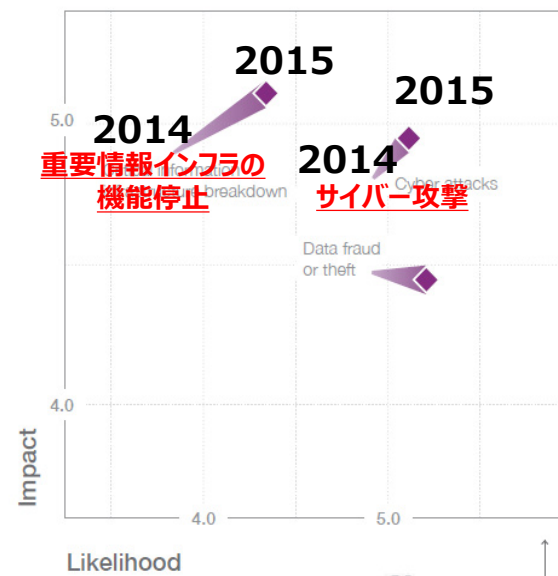
※ 警察庁(2014年2月)

世界が直面するグローバルリスク



“大規模サイバー攻撃のリスクは、発生確率、発生時の影響度のいずれの側面からみても平均的リスクを上回る。これはサイバー攻撃がますます洗練化されていることに加え、インターネットに接続されるモノが急増し、企業によってクラウドにより多くの機微性を有するパーソナルデータを蓄積されるようになってきていることによるものである。”

Technological Risks 2014 → 2015



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28のリスクに関する今後10年間の展望について、世界各地の約900名の専門家に対する調査結果をとりまとめたもの。

(Source)World Economic Forum “Global Risks 2015 : 10th edition”

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)

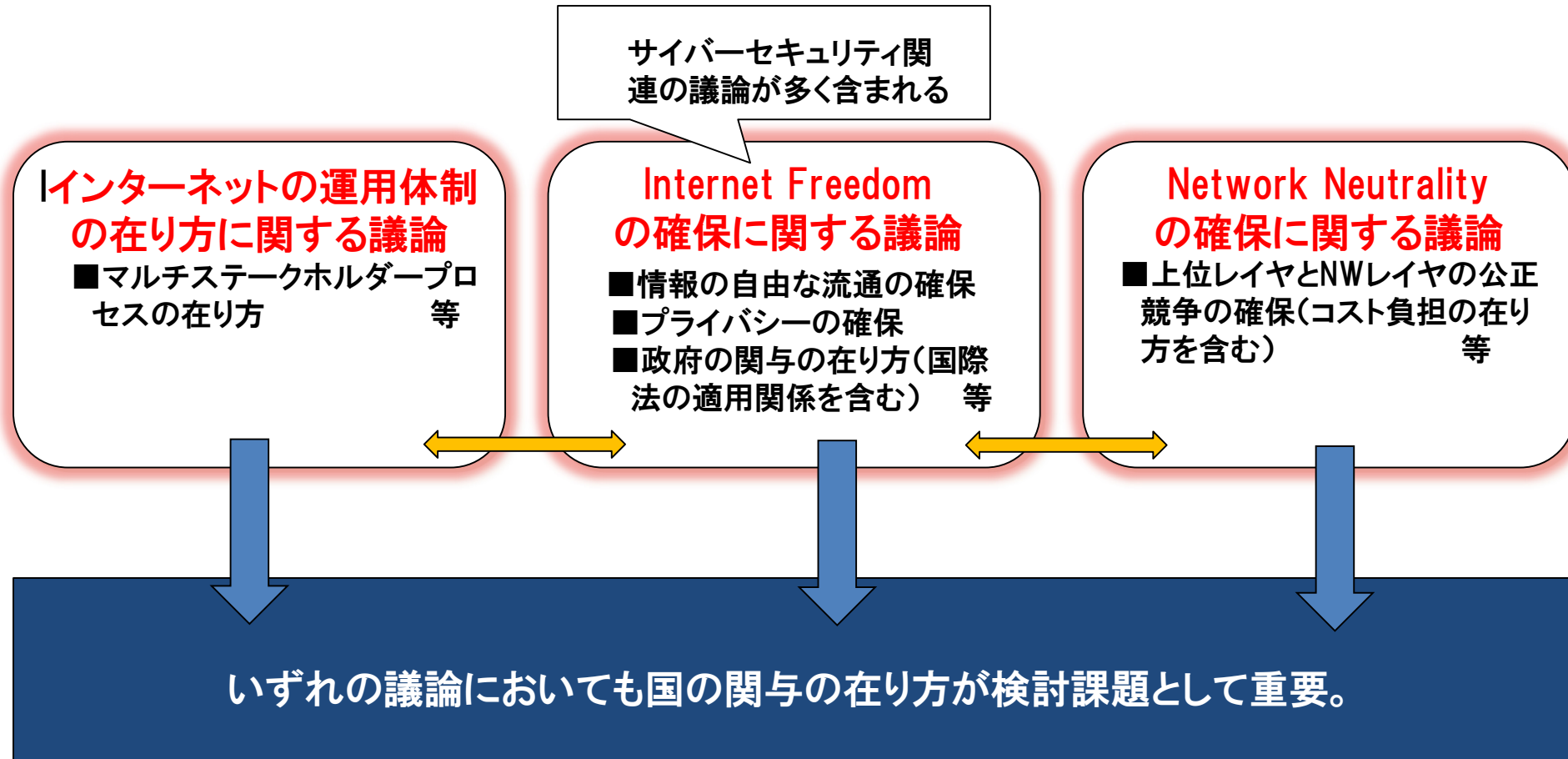
情報システムや情報通信ネットワーク等により構成されるグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

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。

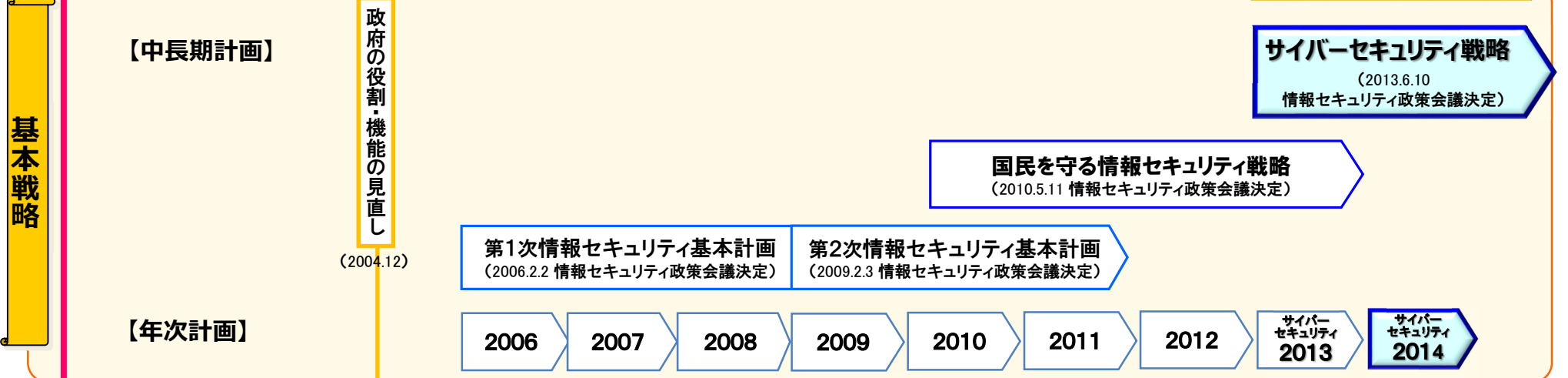
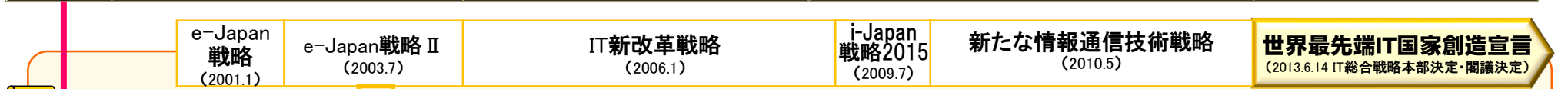
我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とする観点から、不可欠である。

“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



基本戦略

推進体制

2015年1月
内閣サイバーセキュリティセンター発足

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<ul style="list-style-type: none"> ●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】 	<ul style="list-style-type: none"> ●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 	<ul style="list-style-type: none"> ●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
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<ul style="list-style-type: none"> ●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】 ●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】 		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<ul style="list-style-type: none"> ●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… ●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) 	<p>〈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。</p>	
<p>⑥</p> <p>組織体制</p>	<ul style="list-style-type: none"> ●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) ●共同意識啓発活動【毎年10月】 		

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<p>●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】</p> <p>●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応</p> <p>●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</p> <p>●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】</p>	<p>●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】</p> <p>●政府機関やシステムベンダー等との情報共有の強化</p> <p>●事業継続確保のための分野横断的な演習</p> <p>●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</p>	<p>●スマートフォン不正アプリへの対応</p> <p>●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】</p> <p>●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】</p> <p>●税制など中小企業のセキュリティ投資の促進</p> <p>●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</p> <p>●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</p>
---	--	---	--

<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<p>●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】</p> <p>●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】</p>		
--	---	--	--

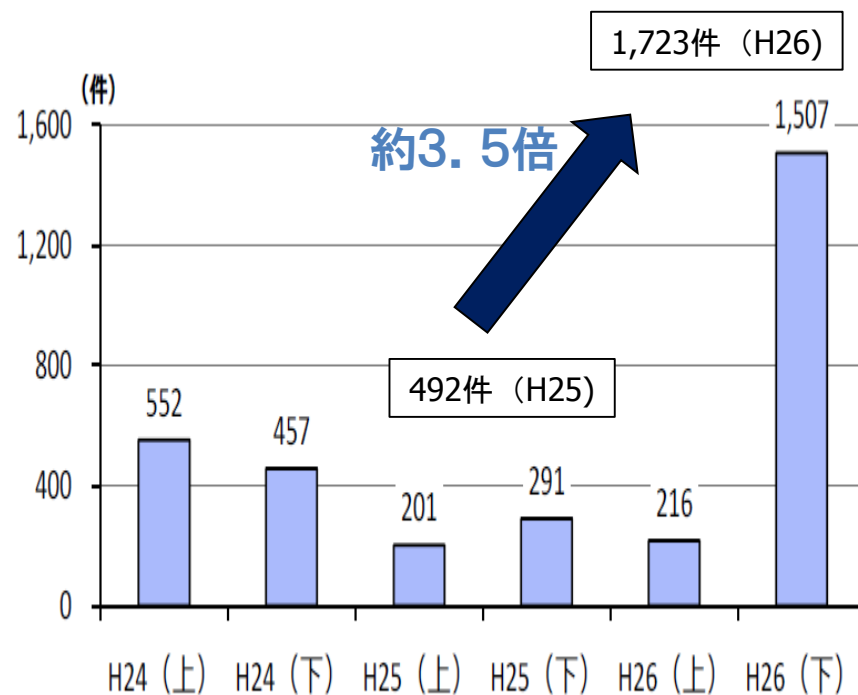
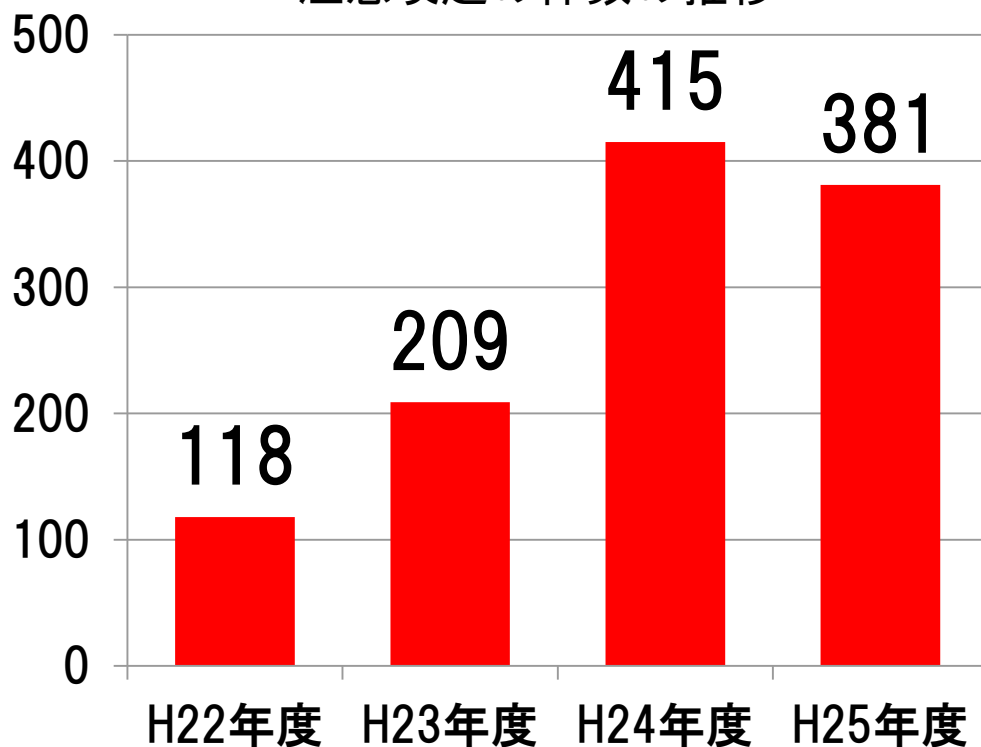
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<p>●日ASEAN【2009年～：日ASEAN政策会議^{注1}(2014年10月・東京)】等</p> <p>●日米【2013年～：日米サイバー対話(2014年4月・ワシントンDC)】等</p> <p>●日英【2012年～：日英サイバー協議】</p> <p>●日印【2012年～：日印サイバー協議】</p> <p>●日EU、日仏、日イスラエル、日エストニア、日豪、日露…</p> <p>●サイバー空間の国際規範づくり等に関する会議【2011年～：次回(2015年4月・オランダ・ハーグ)】</p> <p>●IWWN^{注2}(2014年5月・東京)</p> <p>●MERIDIAN^{注3}(2014年11月・東京)</p>		<p>〈注1〉日・ASEAN情報セキュリティ政策会議。各国局長級が参加。</p> <p>〈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。</p> <p>〈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。</p> <p>●共同意識啓発活動【毎年10月】</p>
---	--	--	--

<p>⑥</p> <p>組織体制</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)</p>		
-----------------------------	---	--	--

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）
- ばらまき型の攻撃が減少。

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



警察が把握した標的型メール攻撃の件数

出典：警察庁（H27年3月）

企業におけるサイバー攻撃の手口(IPA調査)

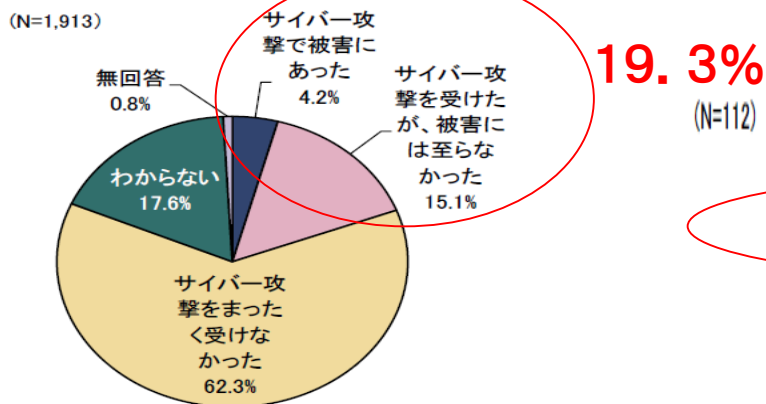


図 3.5-1 サイバー攻撃の遭遇経験

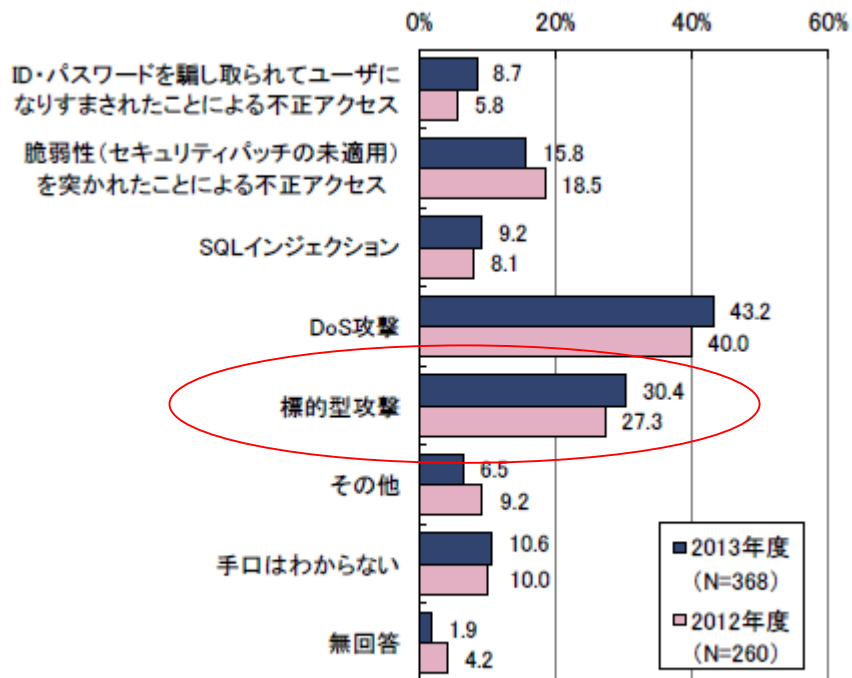


図 3.5-5 サイバー攻撃の手口 (2012 年度調査との比較)

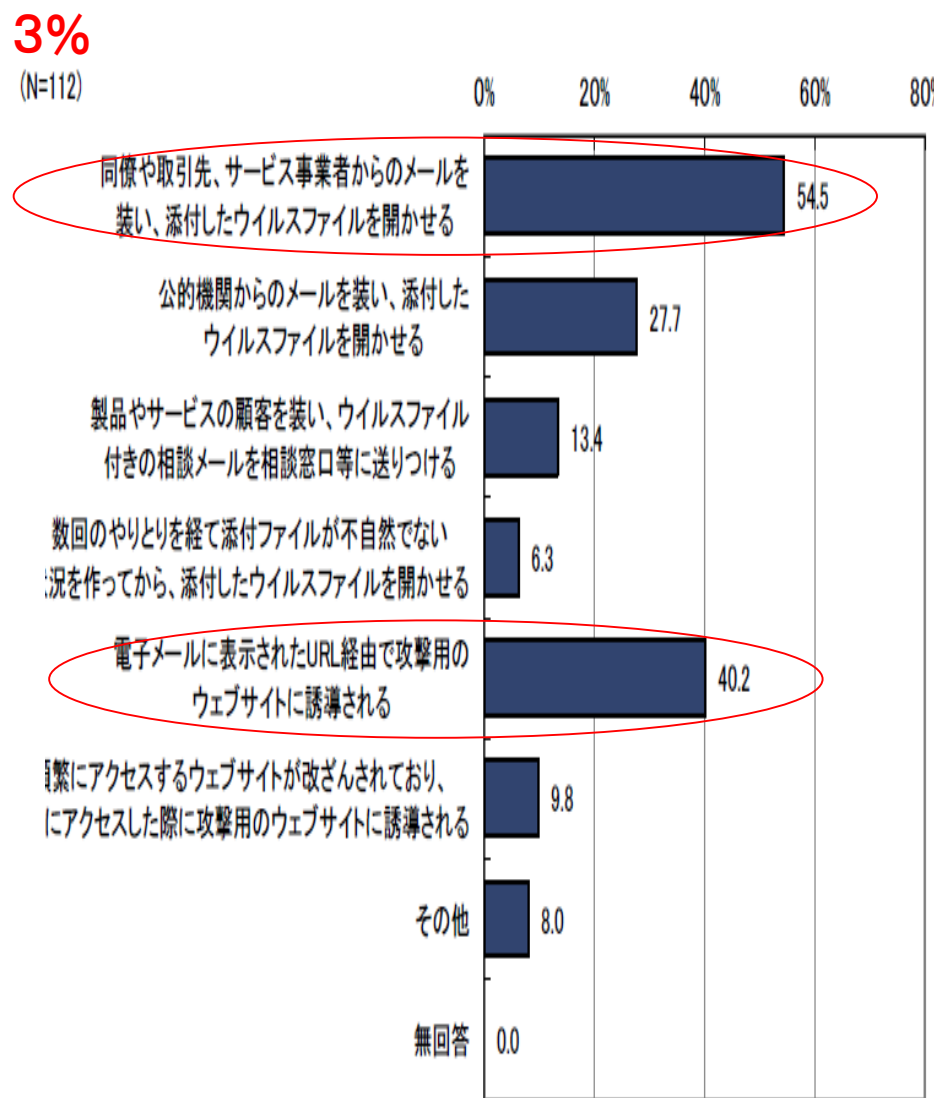


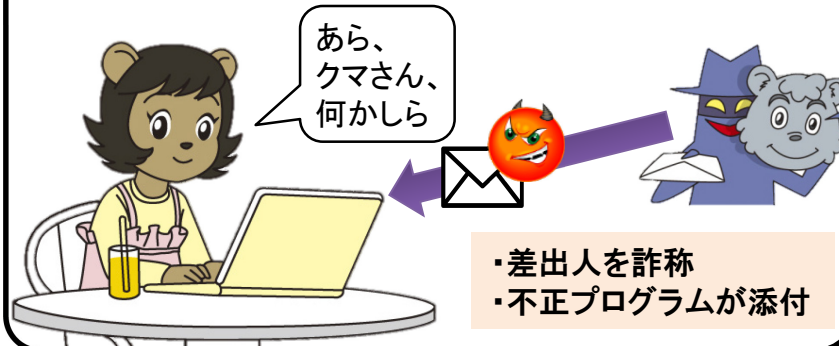
図 3.5-9 標的型攻撃の具体的な手口

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

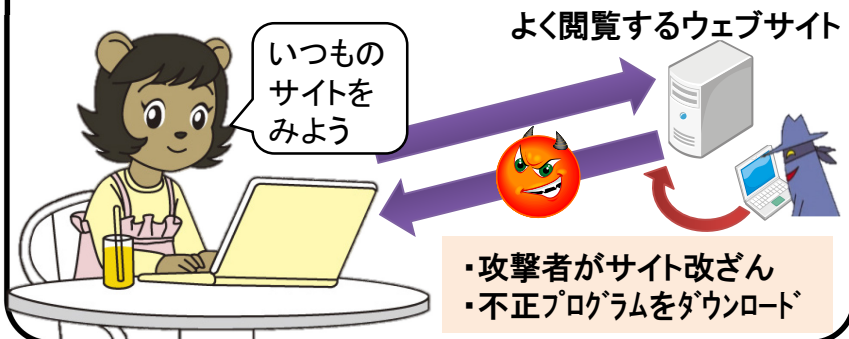
A. メール

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・・・



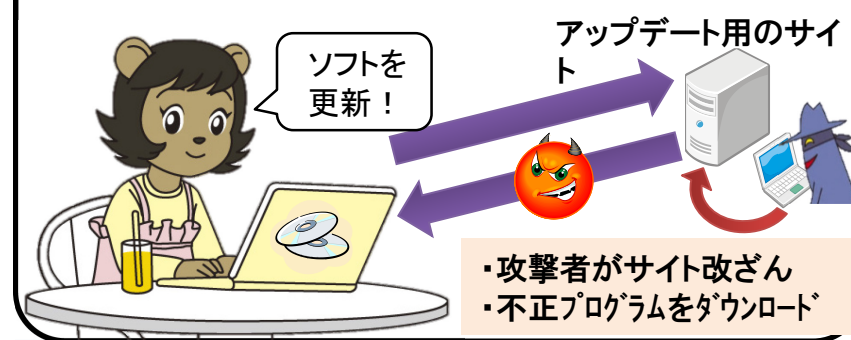
B. ウェブ閲覧（水飲み場型）

いつも閲覧しているウェブサイトへアクセスすると・・・



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・・・



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。

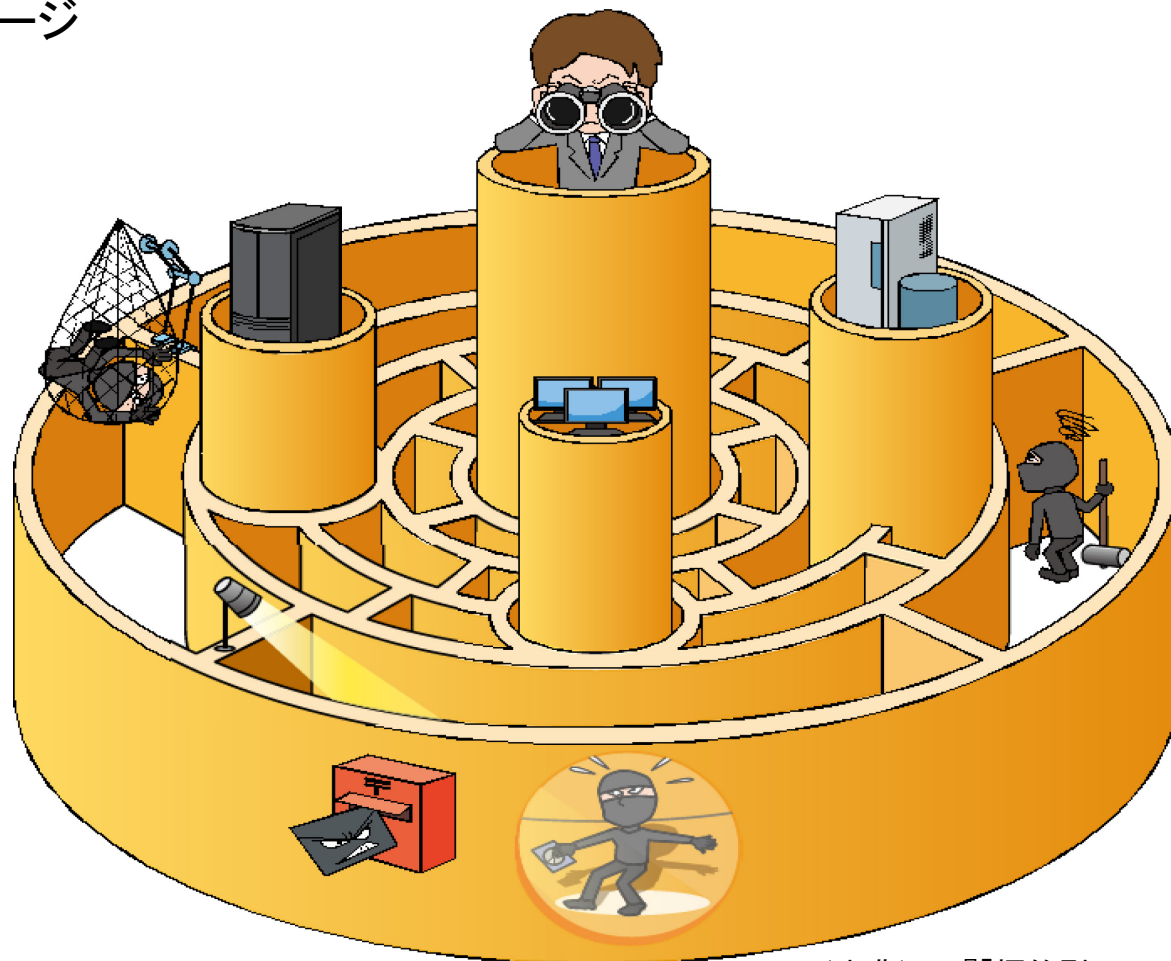
■ 多重防御を備えたシステムのイメージ

重要なものを重点的に
守る

第2、第3の壁を作って
攻撃を拵げにくくする

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！

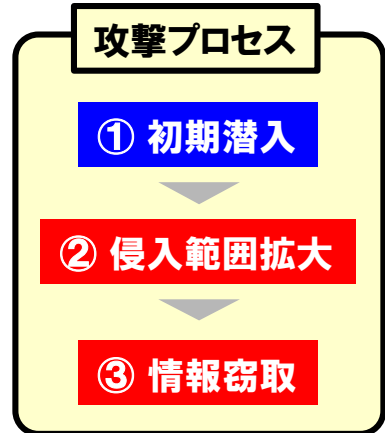
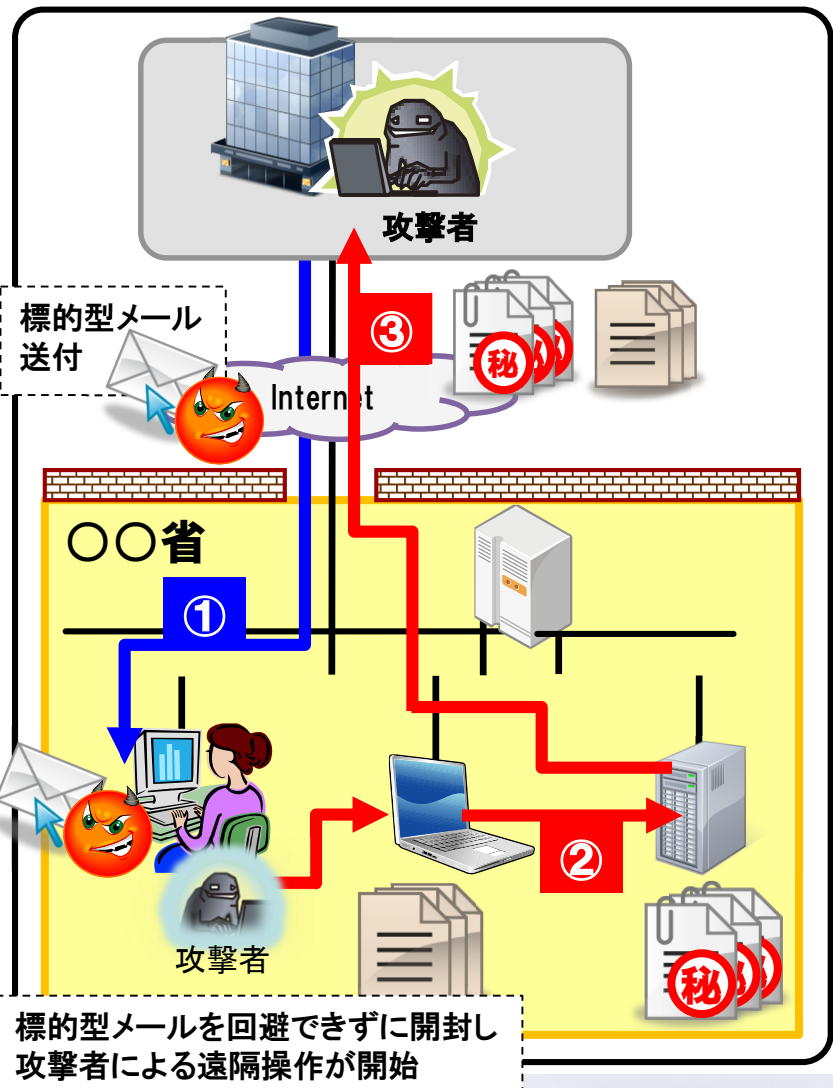


(出典)IPA『「標的型メール攻撃」対策
に向けたシステム設計ガイド』

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)



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

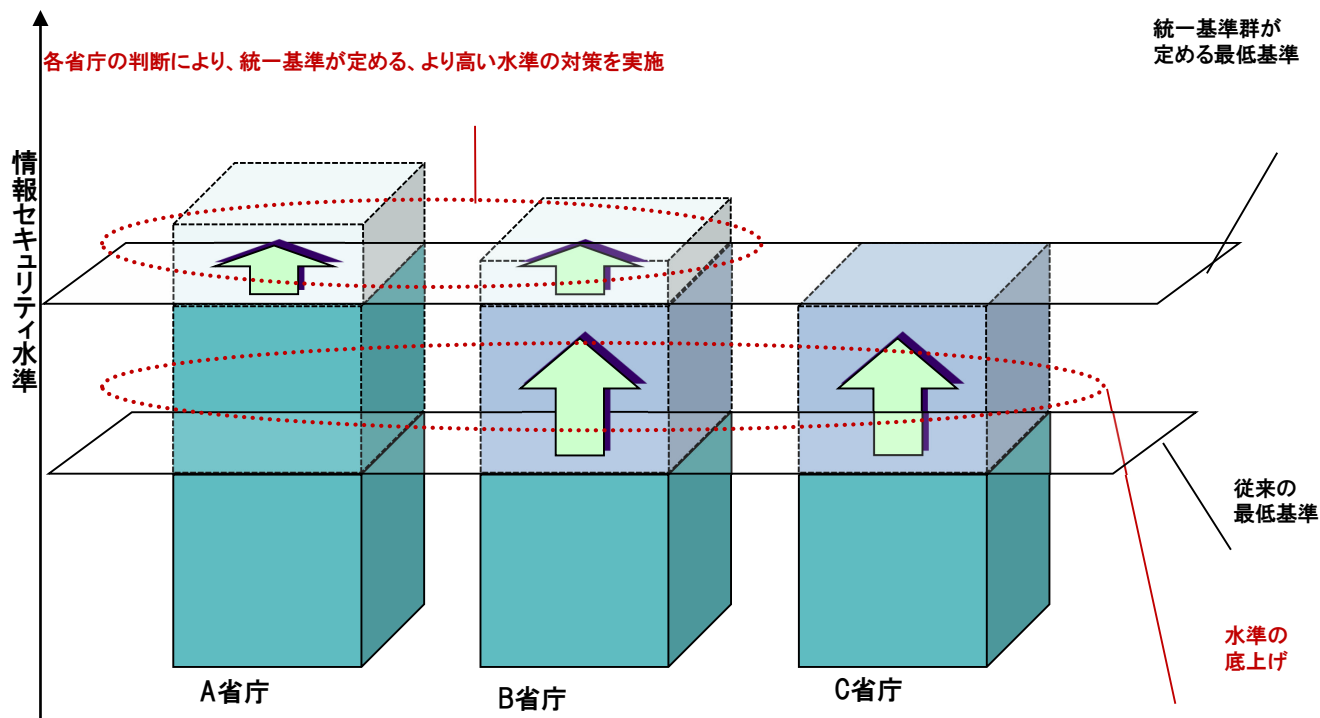
情報システム内部の設計対策

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"> 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	<ul style="list-style-type: none"> 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

- 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)>



◆ 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。



「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)

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<p>●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】</p> <p>●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応</p> <p>●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</p> <p>●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】</p>	<p>●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】</p> <p>●政府機関やシステムベンダー等との情報共有の強化</p> <p>●事業継続確保のための分野横断的な演習</p> <p>●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</p>	<p>●スマートフォン不正アプリへの対応</p> <p>●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】</p> <p>●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】</p> <p>●税制など中小企業のセキュリティ投資の促進</p> <p>●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</p> <p>●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</p>
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<p>●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】</p> <p>●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】</p>		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<p>●日ASEAN【2009年～：日ASEAN政策会議^{注1}(2014年10月・東京)】等</p> <p>●日米【2013年～：日米サイバー対話(2014年4月・ワシントンDC)】等</p> <p>●日英【2012年～：日英サイバー協議】</p> <p>●日印【2012年～：日印サイバー協議】</p> <p>●日EU、日仏、日イスラエル、日エストニア、日豪、日露…</p> <p>●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)】</p> <p>●IWWN^{注2}(2014年5月・東京)</p> <p>●MERIDIAN^{注3}(2014年11月・東京)</p>		<p>〈注1〉日・ASEAN情報セキュリティ政策会議。各国局長級が参加。</p> <p>〈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。</p> <p>〈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。</p> <p>●共同意識啓発活動【毎年10月】</p>
<p>⑥</p> <p>組織体制</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)</p>		

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

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

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・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

指針策定の背景

目指す方向

重要インフラにおけるサービスの持続的な提供

課題

IT障害の極小化／IT障害の迅速な復旧と再発防止

一義的には重要インフラ事業者等による適切かつ継続的な実施・改善が必要

～自らの情報セキュリティ対策の水準や不足を知るために、照らす規範等(安全基準等)が必要～

課題解決に向けて

国の施策として、情報セキュリティ対策の水準の維持・向上に資するガイドラインの提示

～分野ガイドラインや事業者等の内規等の策定・改訂に資する指針の提示～

* 第3次行動計画を受けた指針(改訂版)を2015年度に提示

指針(改訂版)の概要

指針の体系(以下3冊にて構成)

記載内容

指針_本編(概念)

* 改訂

具体的に何をすればよいか

I. 目的及び位置付け

II. 「安全基準等」で規定が望まれる項目

「策定の目的」、「対象範囲」、「対象とする原因」、「役割」、「公開」、「対策項目(PDCAベース)」に係る解説

指針_対策編(具現化例)

* 改訂

どの対策から行うか

I. 対策編の位置付け

II. 具体的な情報セキュリティ対策項目の例示

対策項目(PDCAベース)毎の取組や成果等の例示

指針_手引書(優先順位付け等の考え方)

* 新設

I. 目的及び位置付け

II. 情報セキュリティ対策の優先順位付け及び対応策決定のプロセス

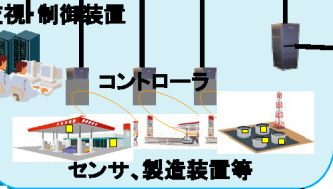
各プロセスを解説しつつ、「どのような対策をどの程度で行うか」を各事業者等が自ら定めることを推奨

制御システムの普及

情報システム

インターネット

制御システム



制御機器
ベンダ

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

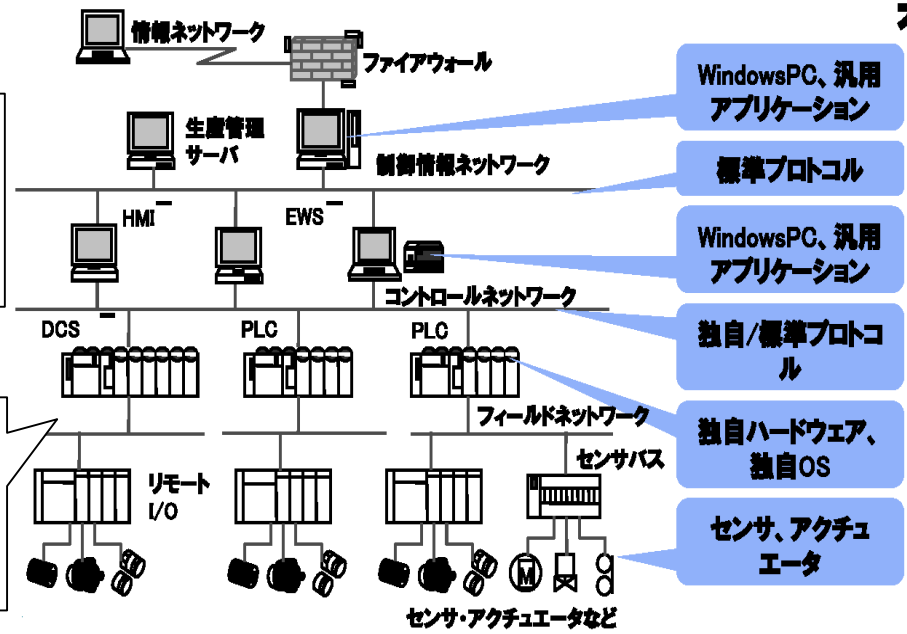
- 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
- 外部ネットワークにも接続されるようになっている。
- このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。

オープン化が進む制御システムの構成

オープン化

- 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。

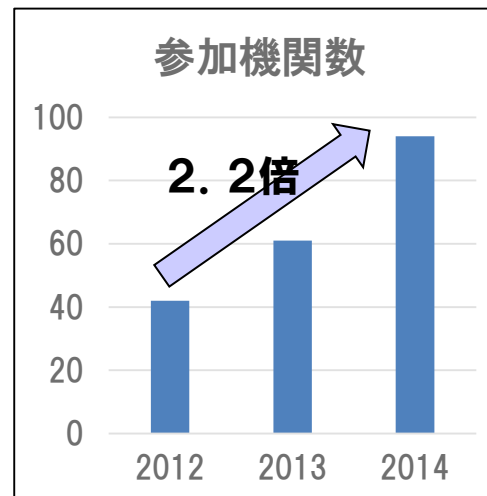
- アプリケーション等が動作する上層のレイヤではWindowsのパソコン等のクライアント端末や汎用アプリケーション、標準プロトコルを利用。
- 実際の制御に関わる下層部分は独自のプロトコルやハードウェア、OSが利用される割合が高く、固有の仕様により構成。
- オープン化が上層部から徐々に進行。



【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>】

重要インフラ分野横断的演習

	2012年度	2013年度	2014年度
参加機関	42組織 (21事業者等)	61組織 (38事業者等)	94組織 (70事業者等)
参加者	148名	212名	348名



演習の様様



意見交換会の様様

「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)

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<p>●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】</p> <p>●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応</p> <p>●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</p> <p>●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】</p>	<p>●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】</p> <p>●政府機関やシステムベンダー等との情報共有の強化</p> <p>●事業継続確保のための分野横断的な演習</p> <p>●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</p>	<p>●スマートフォン不正アプリへの対応</p> <p>●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】</p> <p>●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】</p> <p>●税制など中小企業のセキュリティ投資の促進</p> <p>●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</p> <p>●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</p>
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<p>●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】</p> <p>●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】</p>		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<p>●日ASEAN【2009年～:日ASEAN政策会議^{注1}(2014年10月・東京)】等</p> <p>●日米【2013年～:日米サイバー対話(2014年4月・ワシントンDC)】等</p> <p>●日英【2012年～:日英サイバー協議】</p> <p>●日印【2012年～:日印サイバー協議】</p> <p>●日EU、日仏、日イスラエル、日エストニア、日豪、日露…</p> <p>●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)】</p> <p>●IWWN^{注2}(2014年5月・東京)</p>	<p>●MERIDIAN^{注3}(2014年11月・東京)</p>	<p>〈注1〉日・ASEAN情報セキュリティ政策会議。各国局長級が参加。</p> <p>〈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。</p> <p>〈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。</p> <p>●共同意識啓発活動【毎年10月】</p>
<p>⑥</p> <p>組織体制</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)</p>		

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	925万2305人	972万65人
漏えい件数	1388件	2357件
想定損害賠償総額	1438億7184億円	2132億6405万円
一件当たりの漏えい人数	7031人	4245人
一件当たり平均想定損害賠償額	1億926万円	9313万円
一人当たり平均想定損害賠償額	2万7701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

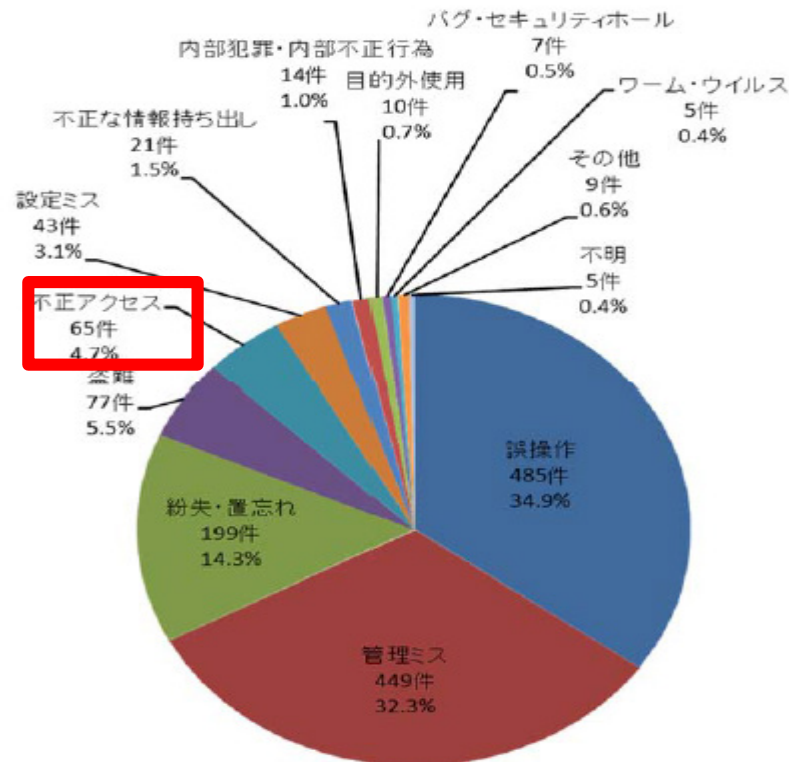
情報通信業が多い

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



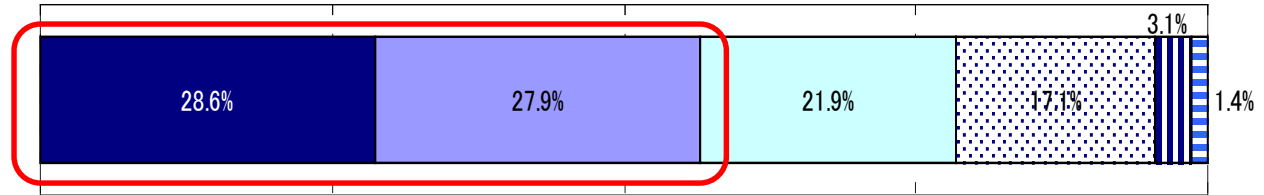
出典:2013年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～(日本ネットワークセキュリティ協会(JNSA))

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。

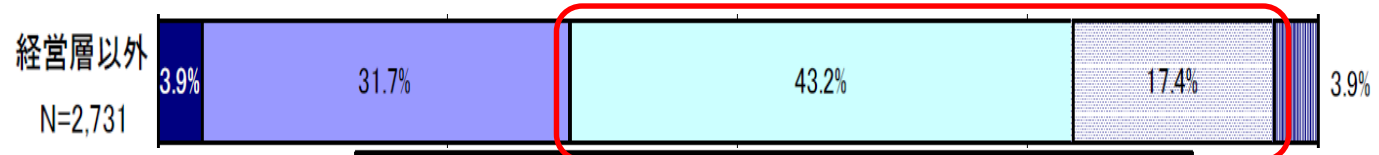
人材不足の原因 (社内向け業務)



- 本業が忙しく、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
- 社内に情報セキュリティ業務の適任者が少ない
- 分からない
- 採用をしたいが、情報セキュリティ業務への応募者が少ない
- その他

N=1,736

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)

- よく理解している
- 概ね理解している
- やや理解が不足している
- 全く理解していない
- わからない

「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

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。

いつでも・どこでも・何でも・誰でも



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。

現状

- 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**、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。
- ウィルス感染や不正アクセスによるプライバシー侵害、知的財産といった重要情報の流出など、**個人・企業等の大きな損害につながる事案**が発生。
- 様々な領域にインターネットが浸透し、**IoT(Internet of Things)**と呼ばれる状況に。サイバー攻撃の対象範囲も急速に拡散。



課題

- 利用者1人1人が情報セキュリティに関する認識を深め、**当事者意識を持って対策に取り組む自発的な活動**が促進されることが必要。
- 一方、国民全体に対す普及啓発は個々の組織・個人の活動だけでは十分な効果が見込めない。**国・地域の様々な立場の主体が重層的連携**することで相乗効果が期待できる。
- 社会に深刻な影響を及ぼす可能性のあるサイバー脅威について、**事業者の意識を高め、自発的な対策を促していく**ことが必要。

取組方針

産学官民の多様な主体で作る**協議会形式の場**を通じ、普及啓発の国民運動化を推進。

さらなる普及啓発の推進

- 情報セキュリティ月間（2月～3月18日）のさらなる推進
- 注力すべきターゲットへの普及啓発を強化
 - ・初等中等教育層
 - ・情報セキュリティを学ぶ機会が少ない層（高齢者、専業主婦等）
 - ・情報セキュリティに関心の薄い層
 - ・企業（中小企業含む）
- 親しみやすいメディア等を活用した情報発信
- 普及啓発に係る指標の検討



情報セキュリティ社会推進協議会の役割

省庁・組織間の有機的な連携

- 関係府省庁・関係機関等も協議会の議論に参画（オブザーバとして）
- 事務局を務めるNISCが、関係府省庁に対し横断的に情報共有・調整



地域における取組の促進

- 地域において草の根的に活動する団体・個人とのネットワークを形成
ボトムアップで情報を集約
- 地域のイベント情報やベストプラクティスの共有、全国的な情報発信、講師派遣等を推進
- 地域内での創意工夫を活かした産学官民連携を促進
- 地域で活躍する情報セキュリティサポーター等の活動を支援



到達目標

本協議会の活動を通じ、国民全体に自発的な取組を促すことを目指し、①**情報セキュリティに関する課題の集約化**、②**様々な主体による啓発活動の集約化と横展開**、③**活動成果を通じたグローバルな連携促進**を目指す。

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<ul style="list-style-type: none"> ●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】 	<ul style="list-style-type: none"> ●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 	<ul style="list-style-type: none"> ●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
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<ul style="list-style-type: none"> ●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】 ●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】 		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<ul style="list-style-type: none"> ●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… ●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) 	<p>〈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。</p>	
<p>⑥</p> <p>組織体制</p>	<ul style="list-style-type: none"> ●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) ●共同意識啓発活動【毎年10月】 		

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

ナレッジの創造(リアル空間へのフィードバック)



データマイニング(個人情報保護ルールの適用を含む)



情報流通連携基盤(認証基盤を含むプラットフォーム)



データ蓄積(クラウド)



ネットワーク(ユビキタス化)



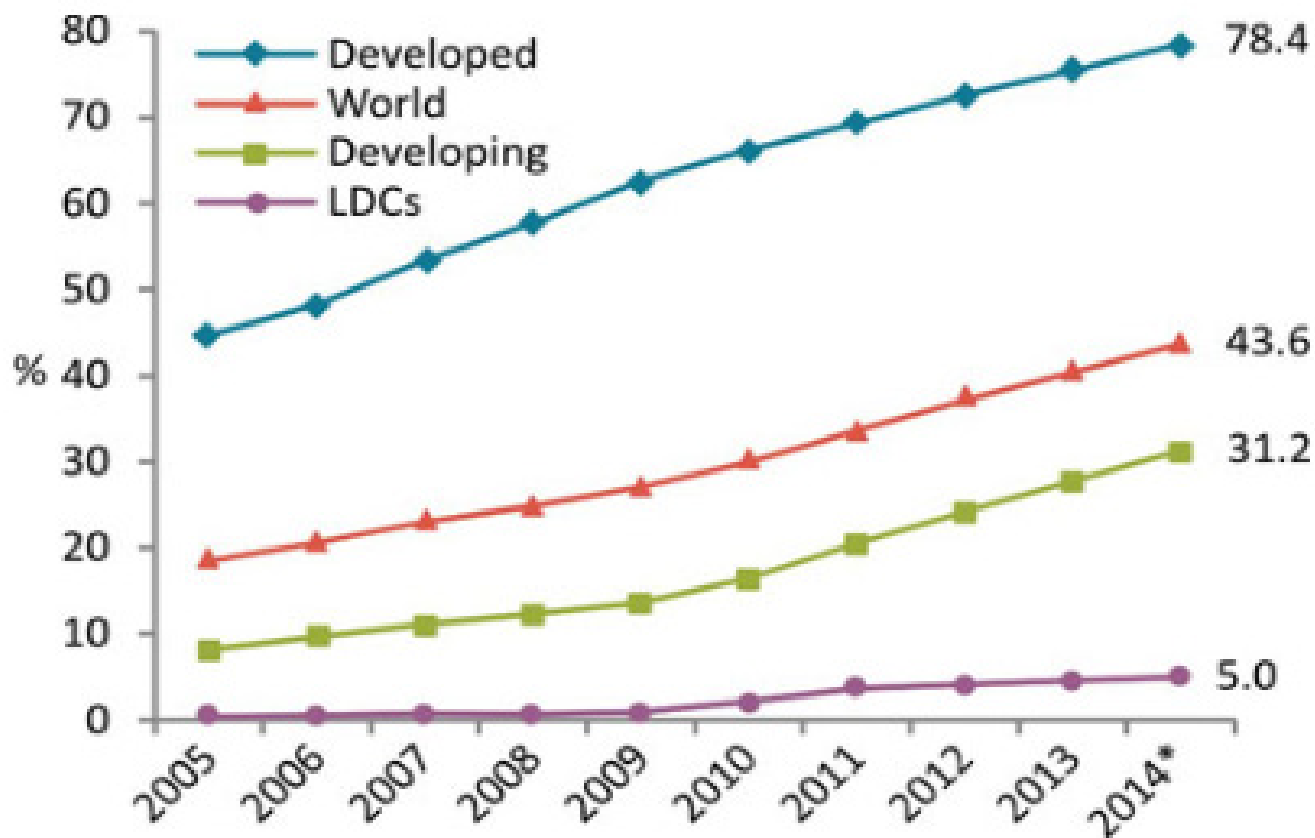
端末(センサー、アクチュエータを含む)

検討事項 (例)

- 自律・分散・協調型NW
(インターネット網に類似)
→マルチステークホルダー
による検討が必要。
- Security by Designの徹底
- 異NW間の責任分界点とイ
ンターフェースの共通化
- 端末認証の仕組み
- インシデント情報の共有体
制(連鎖の拡大への対応)
- 個人情報保護の仕組み

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<p>●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】</p> <p>●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応</p> <p>●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</p> <p>●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】</p>	<p>●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】</p> <p>●政府機関やシステムベンダー等との情報共有の強化</p> <p>●事業継続確保のための分野横断的な演習</p> <p>●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</p>	<p>●スマートフォン不正アプリへの対応</p> <p>●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】</p> <p>●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】</p> <p>●税制など中小企業のセキュリティ投資の促進</p> <p>●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</p> <p>●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</p>
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<p>●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】</p> <p>●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】</p>		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p> <p>●国際戦略の策定【2013年10月】</p>	<p>●日ASEAN【2009年～:日ASEAN政策会議^{注1}(2014年10月・東京)】等</p> <p>●日米【2013年～:日米サイバー対話(2014年4月・ワシントンDC)】等</p> <p>●日英【2012年～:日英サイバー協議】</p> <p>●日印【2012年～:日印サイバー協議】</p> <p>●日EU、日仏、日イスラエル、日エストニア、日豪、日露…</p> <p>●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)】</p> <p>●IWWN^{注2}(2014年5月・東京)</p> <p>●MERIDIAN^{注3}(2014年11月・東京)</p>	<p>〈注1〉日・ASEAN情報セキュリティ政策会議。各国局長級が参加。</p> <p>〈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。</p> <p>〈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。</p>	<p>●共同意識啓発活動【毎年10月】</p>
<p>⑥</p> <p>組織体制</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)</p>		

世界約30億人がインターネットを利用(2014年度末、推計値)



(Source) ITU “Measuring the Information Society” (October 2014)

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との国際連携の成果（2013～2014年）

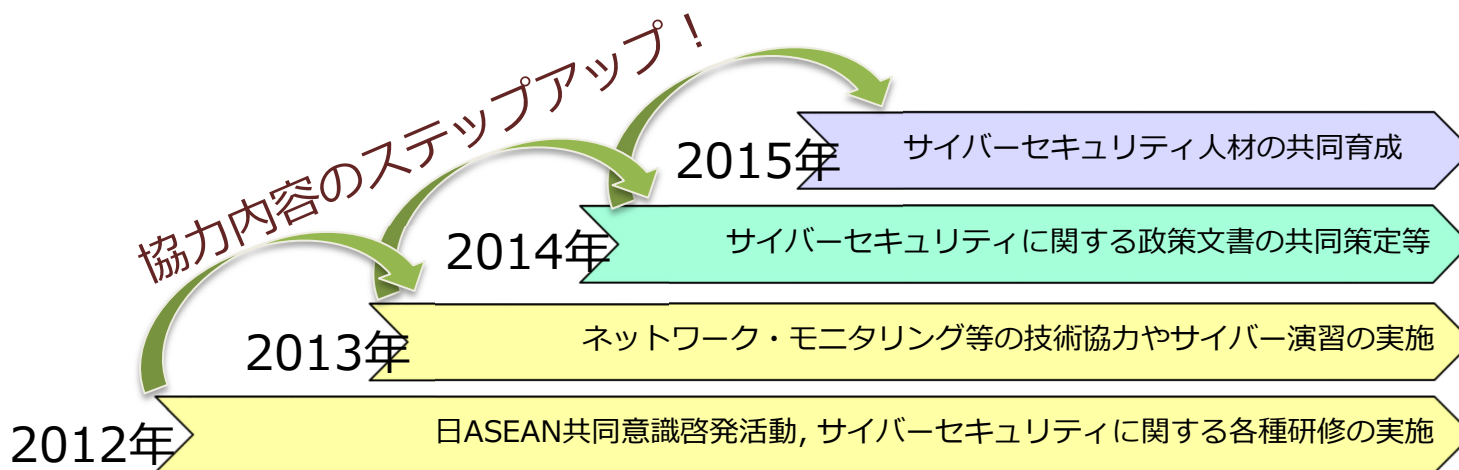


● ASEAN各国との国際会議*を主催，協力内容をステップアップ

2013年以前からの取組である日ASEAN共同意識啓発活動や各種研修，技術協力，サイバー演習等について、内容を充実・高度化させつつ継続


2014年の重点的取組として、「日ASEANにおける重要インフラ防護に関するガイドライン」を共同策定。また，サイバー犯罪対策対話によって法執行分野の能力構築支援を開始

2015年の重点的取組として，高度なスキルを有するサイバーセキュリティ人材の共同育成に向けた検討を開始



*第7回 日ASEAN情報セキュリティ政策会議(局長級) 及び第3回日ASEANシンポジウム (2014年10月7日～9日・東京)
第6回 日ASEAN政府ネットワークセキュリティワークショップ (課長級) (2014年8月27日～28日・シンガポール)
重要インフラ専門家パネル (2014年1月・東京, 2月・クアラルンプール, 5月・タイ)
第1回 日ASEANサイバー犯罪対策対話 (2014年5月・シンガポール)


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プ：2013年12月
- 第1回日EUサイバー協議：2014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2回日英サイバー協議：2014年11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(2014年12月)

フランス

- 日仏サイバー協議(2014年12月)

イスラエル

- 日イスラエルサイバー協議(2014年11月)


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。




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：2014年4月@ワシントン

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

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：2015年2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カ国の政府機関、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。

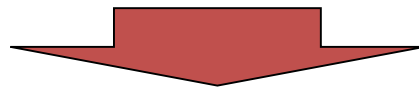
IWWN

- 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。

	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>①</p> <p>「強靱な」サイバー空間 (守り強化)</p>	<ul style="list-style-type: none"> ●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】 	<ul style="list-style-type: none"> ●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 	<ul style="list-style-type: none"> ●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
<p>③</p> <p>「活力ある」サイバー空間 (基礎体力)</p>	<ul style="list-style-type: none"> ●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】 ●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】 		
<p>⑤</p> <p>「世界を率先する」サイバー空間 (国際戦略)</p>	<ul style="list-style-type: none"> ●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… ●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) 		<p>④</p> <p>●共同意識啓発活動【毎年10月】</p>
<p>⑥</p> <p>組織体制</p>	<ul style="list-style-type: none"> ●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) 		

〈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。

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(2014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(同年11月))

オリパラ閣僚会議（議長：安倍総理） = **TOGC** (Tokyo Olympic Games Council)

オリパラ関係府省庁連絡会議（議長：杉田副長官）

セキュリティ幹事会

座長 - 内閣危機管理監

座長代理 - 内閣官房オリパラ室長、内閣官房副長官補（内政）、内閣官房副長官補（事態対処・危機管理）、
警察庁次長（シニア・セキュリティ・コマンダー）

構成員 - 内閣官房（内政・事態・NISC・内調）、内閣府（防災担当）、警察庁、金融庁、総務省、消防庁、法務省、公安調査庁、
外務省、財務省、文科省、厚労省、経産省、国交省、海上保安庁、原子力規制庁、防衛省の局長級

オブザーバー - 東京都、組織委、警視庁、東京消防庁の幹部

事務局 - 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房（内政・事態・NISC）において処理

テロ対策WT

座長 - 内閣審議官（事態、内政）

座長代理 - 警察庁審議官

※ 構成員等は今後調整

事務局 - 警察庁、国交省、防衛省の協力を得て内閣官房
（事態・内政）において処理

サイバーセキュリティWT

座長 - 内閣審議官（NISC副センター長）

座長代理 - 警察庁審議官

※ 構成員等は今後調整

事務局 - 警察庁、総務省、外務省、経産省、防衛省の協力を
得て内閣官房（NISC）において処理

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	
「強靱な」サイバー空間	<p>「政府機関統一基準群」改定 (2014/05/19)</p> <p>「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)</p> <p>「情報セキュリティ普及・啓発プログラム」改定 (2014/07/10)</p>	<p>【主な施策】</p> <ul style="list-style-type: none"> 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	<p>「情報セキュリティ研究開発戦略」改定 (2014/07/10)</p> <p>「情報セキュリティ人材育成プログラム」改定 (2014/05/19)</p>	<p>【主な施策】</p> <ul style="list-style-type: none"> 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)	<p>【主な施策】</p> <ul style="list-style-type: none"> 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	<p>サイバーセキュリティ基本法</p> <p>「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」(2014/11/25)</p>	<p>【主な施策】</p> <ul style="list-style-type: none"> 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) 	

これまでの情報セキュリティ政策の推進体制



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

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)

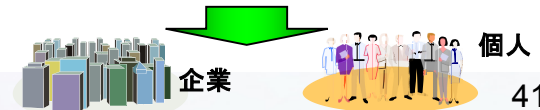
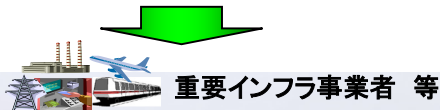
その他の
関係省庁

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



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
- ⇒ 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

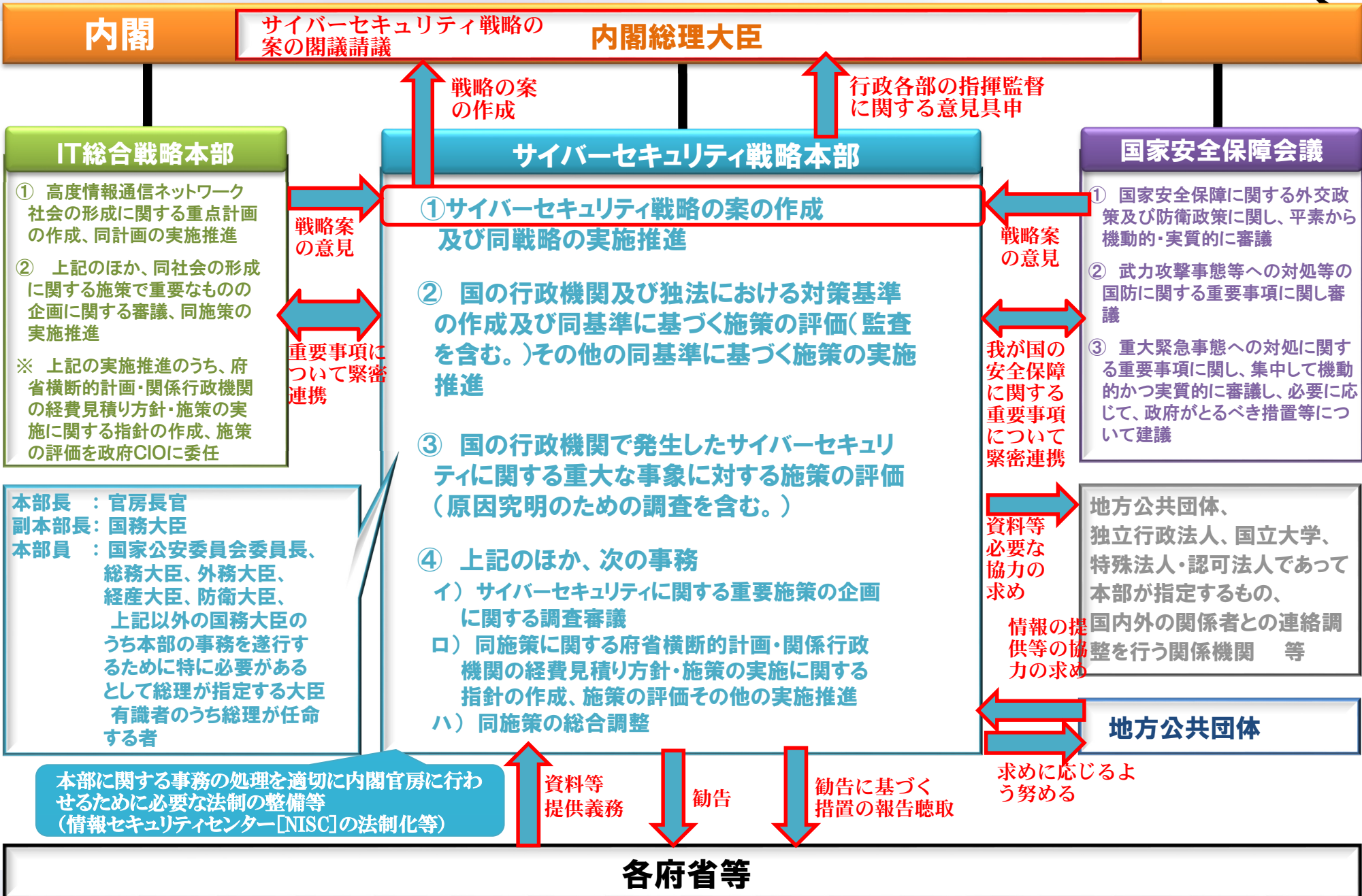
■ 検討 (第3条)

⇒ 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



1 機能強化の必要性

以下の観点から、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

- 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利活用社会」の実現が成長戦略の柱の1つ
- 国際的な連携の強化が必要な諸外国においても、積極的な体制強化を実施
- 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

2 サイバーセキュリティ基本法の制定

サイバーセキュリティ戦略本部

(本部長:内閣官房長官)

- サイバーセキュリティ戦略本部の所掌事務
 - ① サイバーセキュリティ戦略案の作成
 - ② 政府機関等の防御施策評価(監査を含む)
 - ③ 重大事象の施策評価(原因究明調査を含む)
 - ④ 各府省の施策の総合調整(経費見積り方針の作成等を含む)
- サイバーセキュリティ戦略本部に関する事務は、内閣官房副長官補が掌理

一 総合戦略本部

緊密連携

緊密連携

NISC
(国家安全保障会議)

事務局

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

3 我が国の推進体制の機能強化に向けた取組

- (1) 情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。
- (2) 内閣官房情報セキュリティセンター(NISC)を以下の組織に法制化(内閣官房組織令)する。

内閣サイバーセキュリティセンター(注)

- 内閣サイバーセキュリティセンターの所掌事務
 - ① GSOCに関する事務
 - ② 原因究明調査に関する事務
 - ③ 監査等に関する事務
 - ④ サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

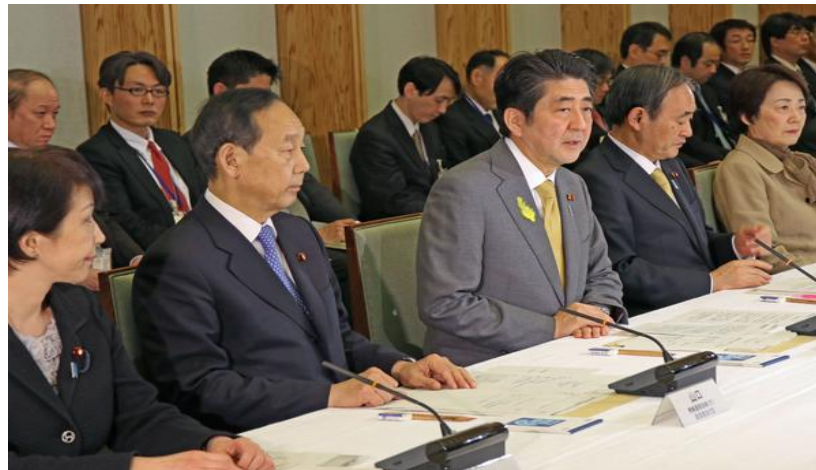
- (3) 今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

内閣サイバーセキュリティセンター発足(2015年1月9日)

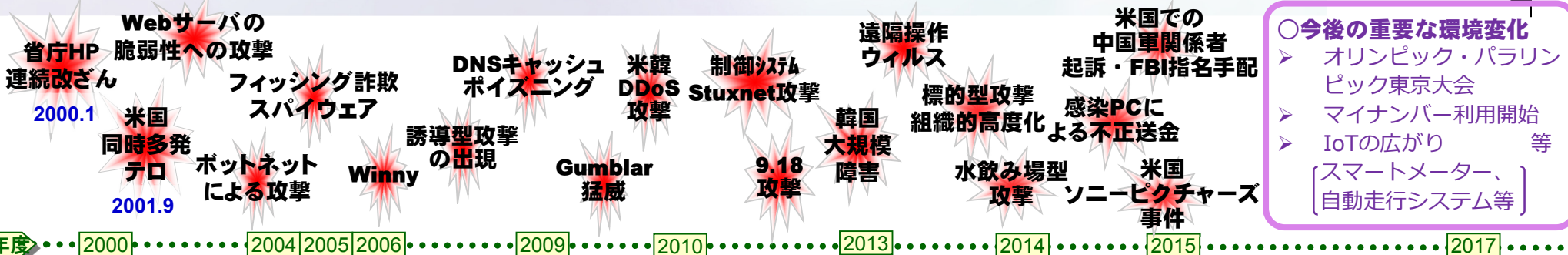


安倍総理

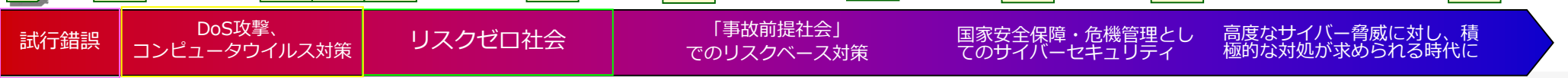
- サイバー空間は、経済成長やイノベーションを推進するために必要な場。サイバーセキュリティは**成長戦略を実現するためにも必要不可欠な基盤**。
- 他方、サイバー空間における脅威はますます深刻化。サイバー攻撃への対応は、まさに**国家の安全保障・危機管理上の重要な課題**。
- サイバーセキュリティ戦略本部は、名実ともに、我が国のサイバーセキュリティ分野の**司令塔**となるべき存在。まずは、サイバーセキュリティ施策の基本的方針について、新たな「サイバーセキュリティ戦略」を策定。
- オリンピック・パラリンピック東京大会の成功にはサイバーセキュリティの確保が必要不可欠。こうした点も見据え、我が国のサイバーセキュリティに万全を期して参りたい。



新・サイバーセキュリティ戦略の策定に向けて

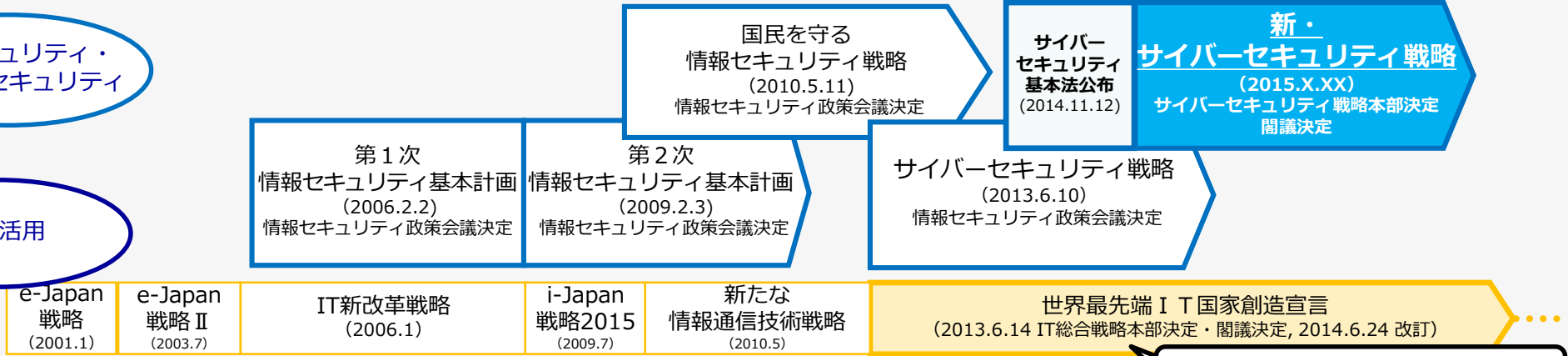


- 今後の重要な環境変化
- ▶ オリンピック・パラリンピック東京大会
 - ▶ マイナンバー利用開始
 - ▶ IoTの広がり 等
 - ▶ [スマートメーター、自動走行システム等]

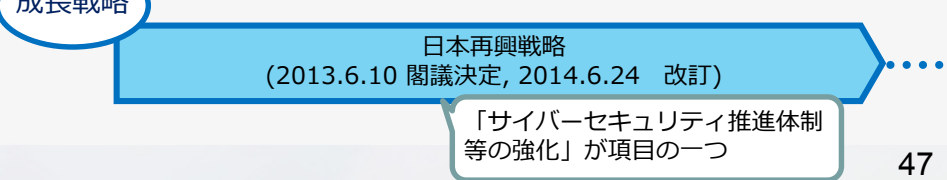
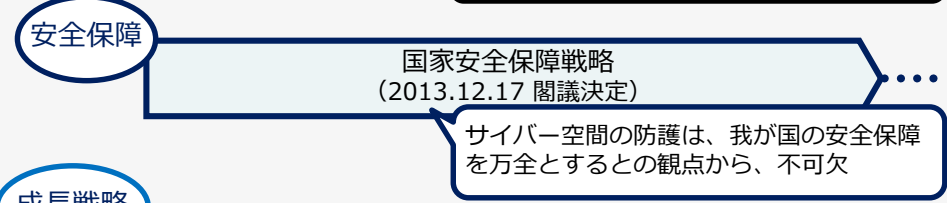


情報セキュリティ・サイバーセキュリティ

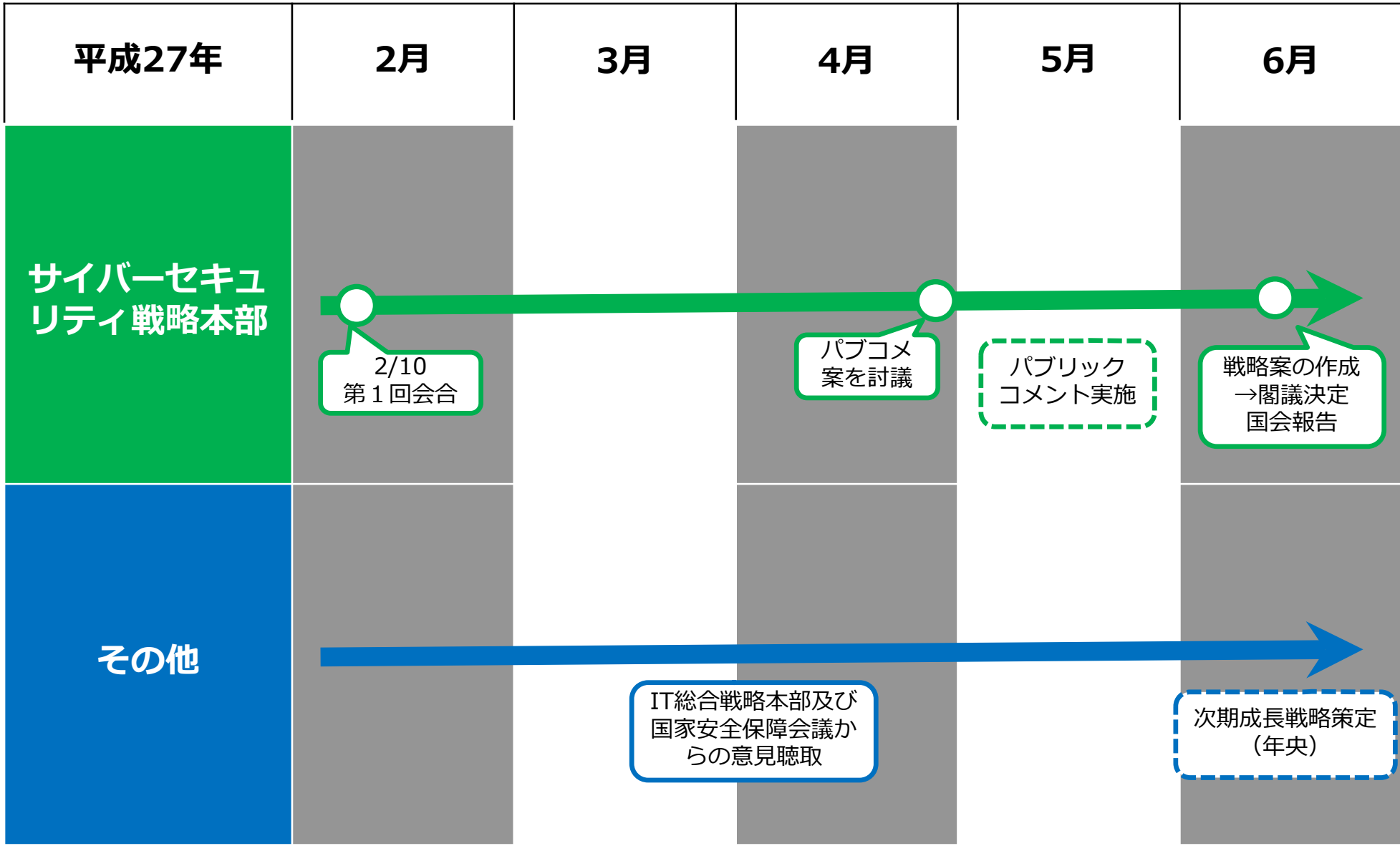
IT利活用



「サイバーセキュリティ立国」の実現が急務



新・サイバーセキュリティ戦略の策定スケジュール(案)



【全般的事項】

- ・ 今後、「サイバー空間」はどのような性質の空間として発展していくと考えるか。
- ・ サイバー空間における多様な主体間の役割分担をどのように考えていくべきか。
- ・ サイバーセキュリティ政策を推進する上で、我が国はどのような基本原則に基づくべきか。

【政策分野別事項】

- ・ サイバー空間を通じて我が国の経済・社会の持続的な発展を実現するためには、サイバーセキュリティが果たす役割や必要とされる政策をどのように考えるか。
- ・ 国民が、サイバー空間上で安全に、安心して豊かな経済社会活動を行うためにはどのような対策が必要か。
- ・ サイバー空間に係る我が国の安全保障を確保し、国際社会の平和に貢献するためには、どのような政策を追求すべきか。

【基盤的事項】

- ・ 社会全体のセキュリティ意識を高め、更にその能力を高めるためには、どのような取組が考えられるか。
- ・ 日本におけるセキュリティ人材を充実させるためには、どのような政策を推進すべきか。
- ・ 社会や技術が変化していく中、サイバーセキュリティに関する研究開発等はどのようなあり方が適切か。

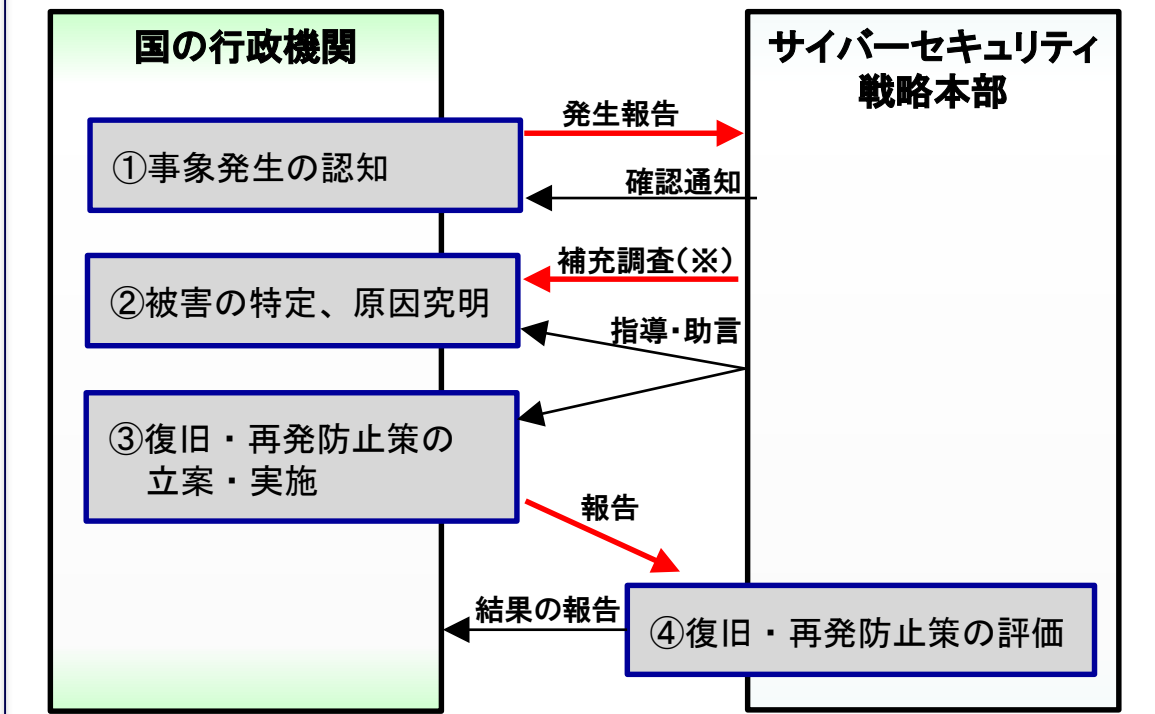
重大インシデントに係る原因究明等のプロセス

～重大事象施策評価規則(2015年2月、サイバーセキュリティ戦略本部決定)～

対象とする事象(特定重大事象)

1. 国の行政機関が運用する情報システムにおける障害を伴う事象であって、**行政事務の遂行に著しい支障**を及ぼす(おそれがある)もの
2. 情報の漏えいを伴う事象であって、**国民生活又は社会経済に重大な影響**を与える(おそれがある)もの
3. 我が国のサイバーセキュリティに対する**国内外の信用を著しく失墜**させる(おそれがある)事象(例:我が国の行政機関のサーバー等が、他国へのサイバー攻撃の踏み台とされるケース)

事務処理の概要



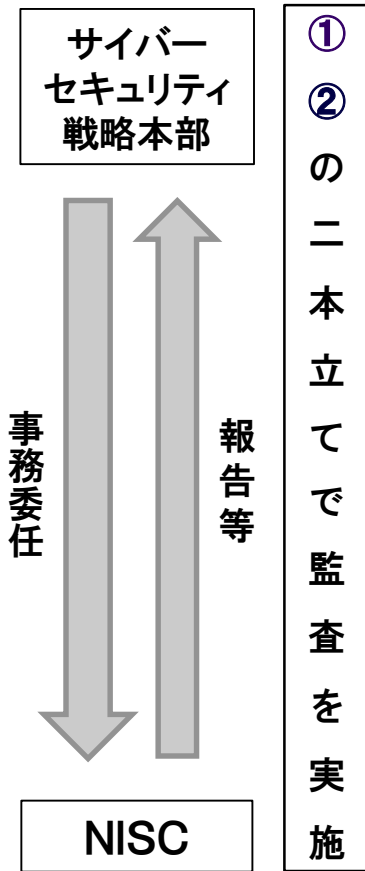
(注) — :基本法第30条に基づく資料提供等を活用

(※) デジタルデータの保全・分析といったフォレンジック調査。

補足事項

- 関係行政機関と本部は、緊密な連携を図るとともに、秘密保持に留意する。
- 本部は、評価等を踏まえ、必要に応じて勧告や政府機関統一基準群の改定等知見のフィードバックを行う。
- 迅速・柔軟な対応のため、上記の本部事務(原則として④の評価を除く)は、内閣サイバーセキュリティセンターにおいて処理。

目的: 国の行政機関におけるサイバーセキュリティ対策の強化を図ること



①
②
の
二
本
立
て
で
監
査
を
実
施

①セキュリティ向上のための体制・制度が機能しているかの検証による評価(監査)(以下「マネジメント監査」という。)

統一基準群に基づく施策の取組状況について、主に組織全体としての対策強化を続ける仕組みが有効に機能しているかどうかの観点から関係者への質問、資料の閲覧、情報システムの点検等により検証し、改善のための必要な助言等を行う。

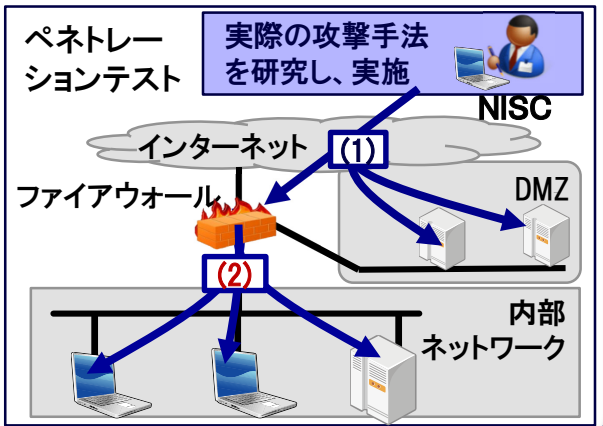
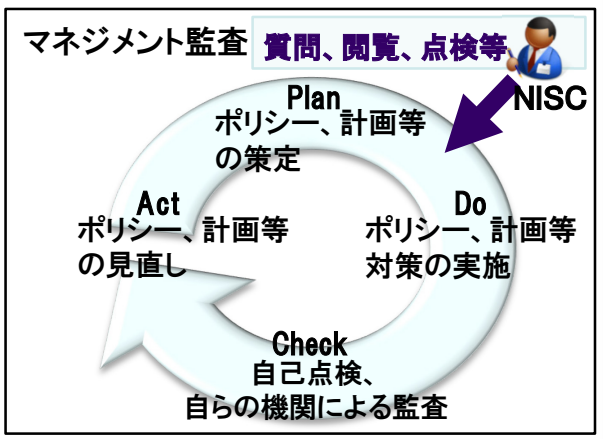
マネジメント監査の着眼点 P(計画立案)、D(実行)、C(点検)、A(見直し)の実施状況を確認するとともに、セキュリティ対策のための体制等についても確認

②情報システムに対する疑似的攻撃による評価(監査)(以下「ペネトレーションテスト」という。)

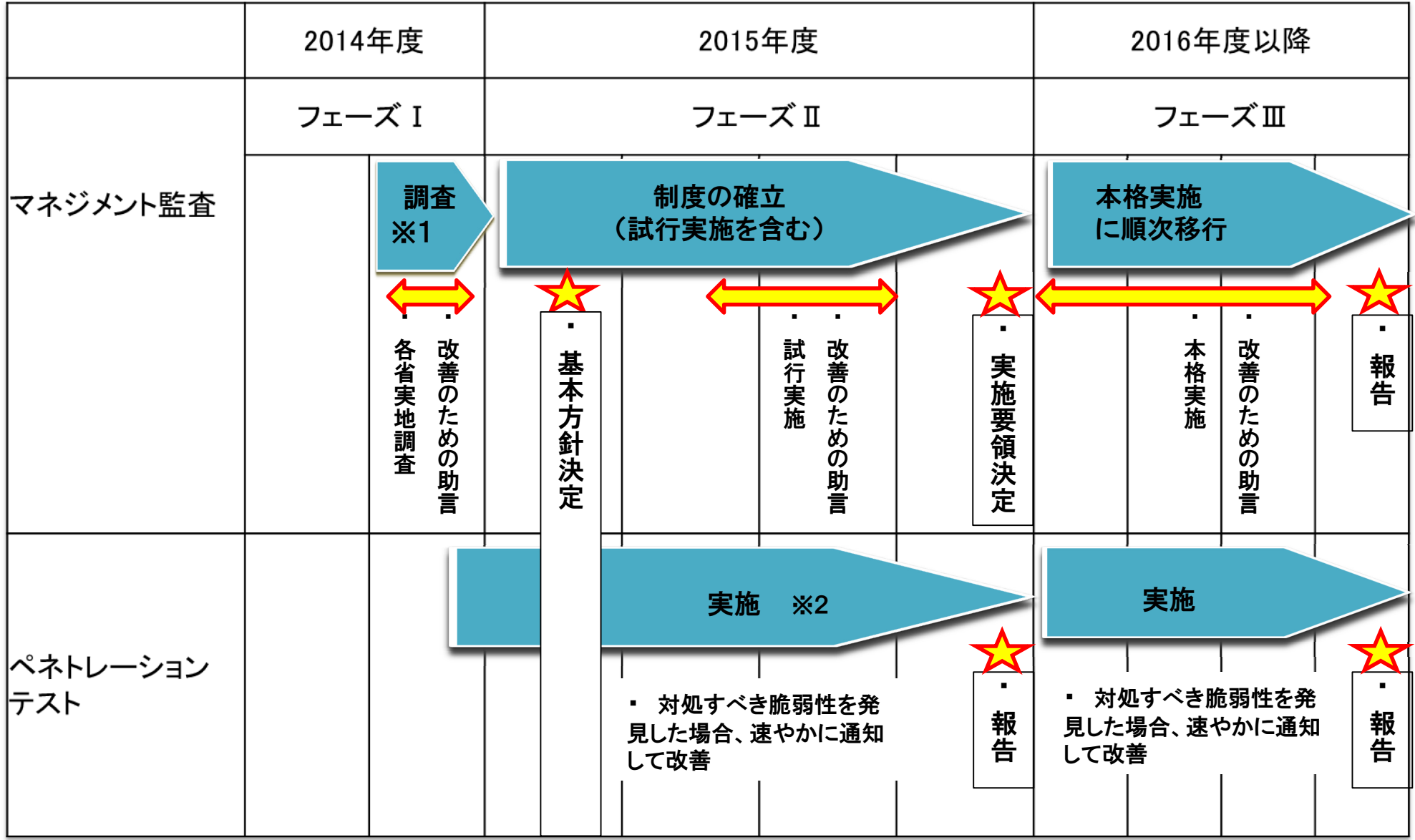
情報システムに対して、攻撃者が用いる手法で実際に侵入できるかどうかの観点から防御策の状況を検証し、改善のための必要な助言等を行う。

ペネトレーションテストの着眼点

- (1)インターネット経由での不正アクセスを想定し、問題点の有無を検証
- (2)インターネットとの境界を突破できた場合、内部ネットワークについても、問題点の有無を検証



監査実施に向けたスケジュール



※1 サイバーセキュリティ基本法の施行により、基本方針決定に向け各機関の施策の取組状況についてヒアリング等の実地調査等を実施。

※2 平成26年度補正予算及び平成27年度予算(予定)により実施。

制度整備を踏まえたNISCに関する主な検討事項

取組方針(2014年11月25日)

① GSOC機能の強化

- 新システム(2017年度～)の運用を見据えた体制、機材の整備 等

H26補正予算(7.3億円)
 ○政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)機能強化のための調査
 31百万円

H27予算(16.5億円)
 ○政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用
 649百万円

② 総合的分析機能の強化

- 諸外国の政策、サイバー攻撃の脅威情勢及び攻撃に使用された技術等の総合的な分析
- 高度な専門知識と深い知見を有する専門的人材の確保及び資質の向上

○脅威予測等総合分析の実施のためのシステム構築
 573百万円

○脅威予測等総合分析の実施
 78百万円

③ 国内外の情報集約機能の強化

- インシデント情報の集約機能や助言機能等の強化に向けた、
- 官民連携のスキーム強化・構築
 - NISC内の体制・システム整備及び能力向上

○各府省庁ネットワークに接続されているコンピュータシステムに対する侵入実験(前倒し分)
 117百万円
 ○サイバーセキュリティインシデントに係る事後調査
 7百万円
 ○脅威予測等総合分析の実施のためのシステム構築(再掲)

○各府省庁ネットワークに接続されているコンピュータシステムに対する侵入実験及び監査
 311百万円
 ○サイバーセキュリティインシデントに係る事後調査
 114百万円
 ○脅威予測等総合分析の実施(再掲)

④ 国際連携の強化

- 緊急対応関連機関とのパートナーシップ構築等による国際的な窓口機能の強化



○国際的なインシデント対応のためのCSIRT機能の構築・運用
 86百万円

⑤ 人材の育成及び登用

- 各省庁からの出向等人材を通じ、NISC内の知見・経験を各省庁に還元
- 任期付任用や人事交流の推進等による技能を備えた人材の確保

○定員増10人(任期付職員) ※H26年度措置

○定員増 ※H27年度措置



※上記のほか、サイバーセキュリティ戦略本部の運営経費やサイバーセキュリティ関連施策の実施に必要な経費(408百万円)を27年度予算に計上

■ Federal Information Security Modernization Act 2014

- ・2002年制定のFISMA法(各省にITシステムセキュリティの年次監査・報告を義務付け)の強化
- ・DHSに政府機関のサイバーセキュリティ対策(軍・インテリジェンスコミュニティ関連を除く)の監督権限を付与。

■ National Cybersecurity Protection Act of 2014

- ・DHSのNCCIC(国家サイバーセキュリティ・通信統合センター)を常設(法的権限の付与)
- ・NCCICにおいてサイバー脅威に関する官民情報を共有。

■ Cybersecurity Workforce Assessment Act of 2014

- ・DHSにおいて省内のサイバーセキュリティ人材の能力評価(3年ごと)を義務付け。同評価を基に人材強化。

■ The Border Patrol Agent Pay Reform Act of 2014

- ・DHSにおけるサイバーセキュリティ人材に係る給与水準等の設定権限を付与。

■ Cybersecurity Enhancement Act of 2014

- ・NIST(国立標準技術研究所)について、産業界主導のセキュリティ対策等の促進・支援を行う組織として位置づけ。
- ・OSTP(大統領府科学技術政策局)について、連邦政府のサイバーセキュリティ研究開発計画の策定・改定する組織として位置づけ。

オバマ米大統領演説@国土安全保障省

サイバーセキュリティに関する立法提案

✓情報共有の促進

- ・官民・民間部門内での情報共有の促進
- ・民間主導の情報共有・分析機関の組織化の推進
- ・情報共有に際してのプライバシーに係る制限の義務付け



(Source)White House HP

- 民間部門の情報共有分析組織 (ISAOs : Information Sharing and Analysis Organizations)の設立促進。
- ISAOs 設立促進のため、情報共有の在り方等の運用に関する任意基準策定のためのNPO組織創設を支援。
- DHS内のNCCICとISAOs の連携強化。

等

(注)Executive Order on Promoting Private Sector Cybersecurity Information Sharing (Feb 13, 2015)

- 国家情報長官の下に新たにサイバー脅威情報統合センター (CTIIC : Cyber Threat Information Integration Center)を設置。
- CTIICはサイバー脅威に関するインテリジェンス情報の分析・統合機能を持つ。

(注)モナコ大統領補佐官(国土安全保障及びテロ対策担当)(2015年2月10日)

✓サイバー犯罪に取り組む法執行機関の近代化

- ・ボットネットの売買に対する訴追の可能化
- ・窃取された米国民の金融情報の海外への売買の処罰化
- ・スパイウェアの売買を防止するための法執行機関の権限の拡大

✓情報漏えいに関する報告

- ・顧客データ漏えいに関する企業の顧客に対する報告義務の連邦法への統一(現在46の州法)



内閣サイバーセキュリティセンター
**National center of Incident readiness and
Strategy for Cybersecurity**