NISC

National center of Incident readiness and Strategy for Cybersecurity

知る・守る 続ける

サイバー空間をめぐる状況とサイバーセキュリティ戦略

平成28年2月
内閣サイバーセキュリティセンター（NISC）
内閣参事官　三角　育生

紙面を賑わす「サイバー」

個人情報漏えい

知的財産／ノウハウ

事業継続

…

- エストニアへの大規模サイバー攻撃（2007年5月）
- ジョージアへの大規模サイバー攻撃(2008年8月）
- 重工業・国会へのサイバー攻撃(2011年秋）
- 韓国重要インフラへのサイバー攻撃(2013年4月）
- SPEへのサイバー攻撃（2014年12月）
- フランスTV5モンド(2015年4月上旬）
- 日本年金機構(2015年6月上旬）
- 米国人事管理局(2015年6月上旬）
- ウクライナ電力網への攻撃(2015年12月）

被害規模

世界経済に対するコスト：4450億ドル以上※

西欧　950億ドル以上※

米国　1000億ドル以上※

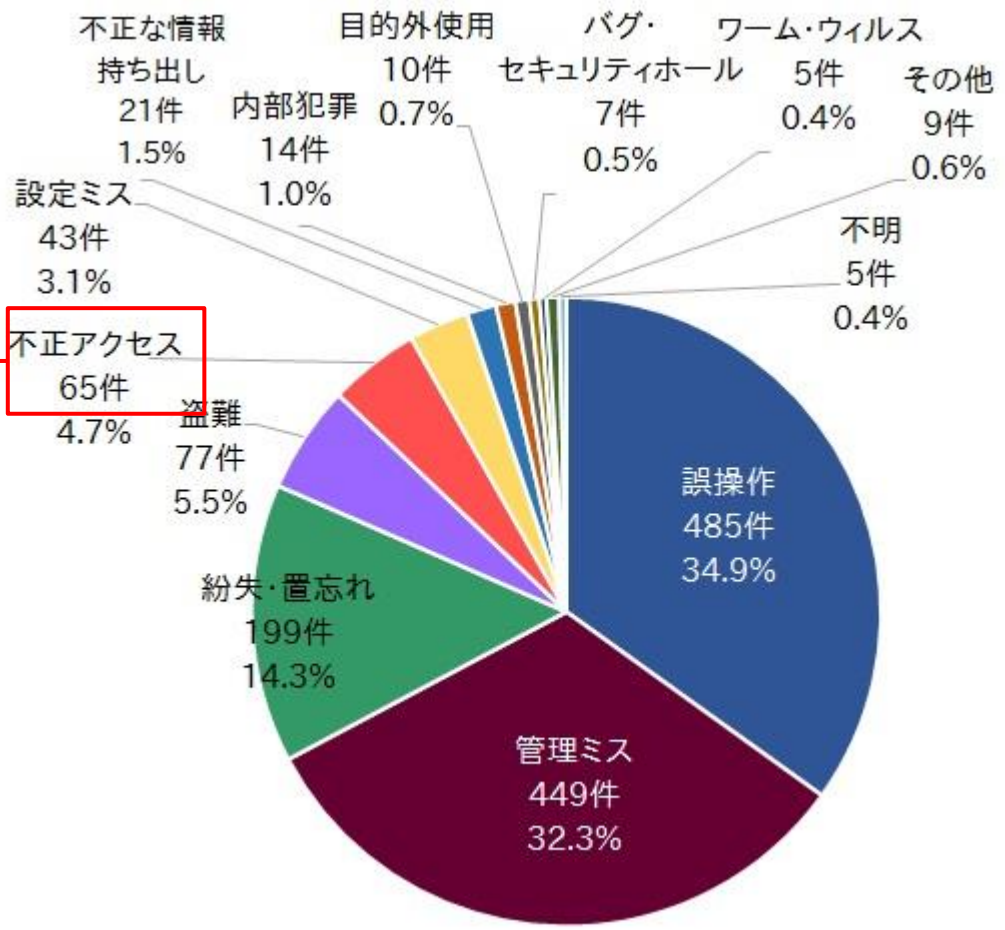
※ Cybercrime等による損失額(試算値)
Net Losses: Estimating the Global Cost of Cybercrime (June 2014, McAfee)
及び同社資料

企業等における情報漏えいインシデントの動向

個人情報漏えいインシデント

	2013年	2012年
一件当たりの漏えい人数	7031人	4245人
一件当たり平均想定被害賠償額	1億926万円 被害が大規模化	9313万円

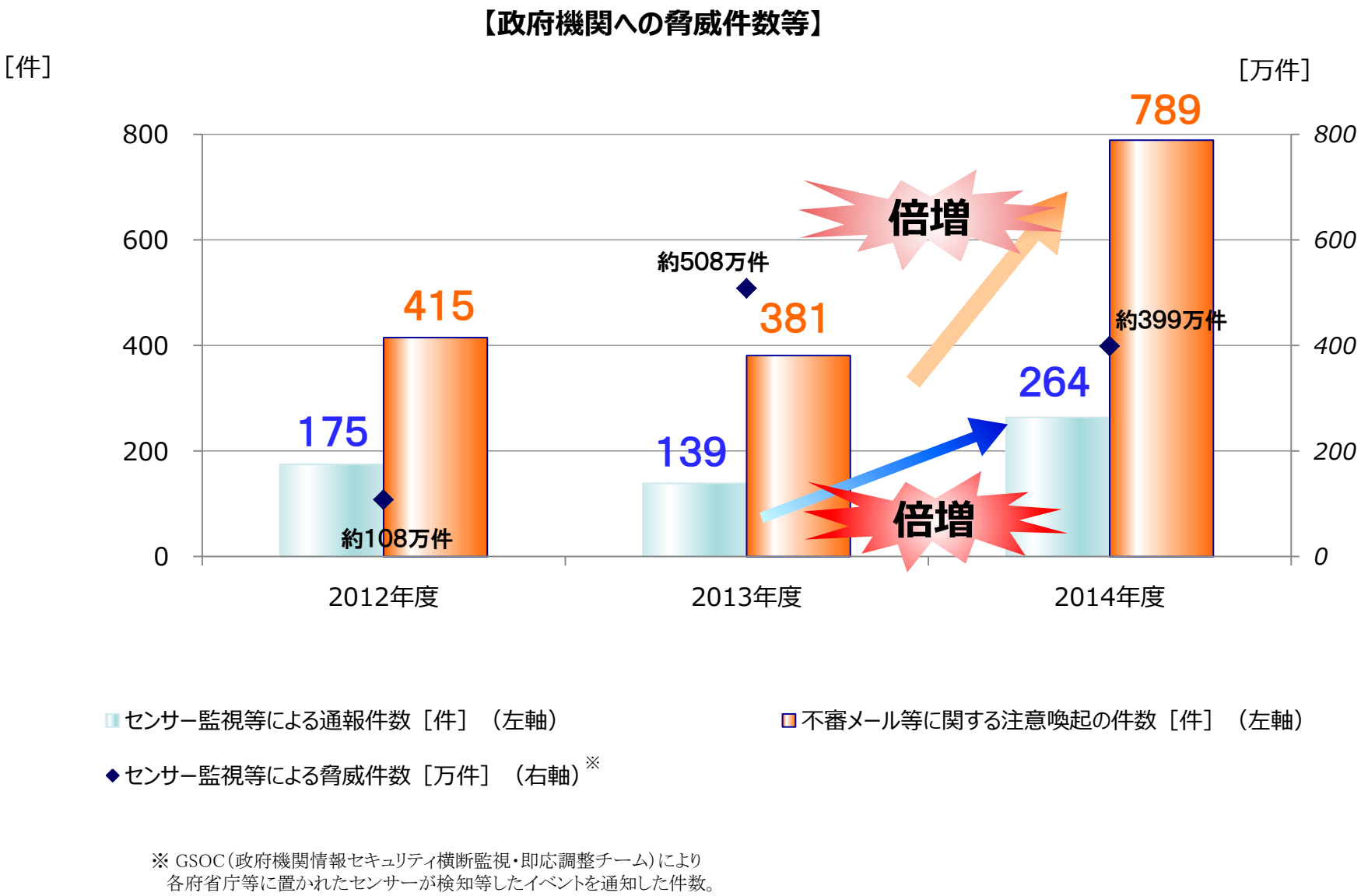
2013年は
大規模漏えい事件トップ10のうち7件の原因が
不正アクセス



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。

リスクの深刻化 （政府機関等の状況）



※ 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を通知した件数。

リスクの拡散

スマートフォン

世帯保有率が4年間６倍に急増
（2010年末：9.7%→2014年末：64.2%）

※2015年版情報通信白書（総務省）

自動車

一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

※自動車の情報セキュリティへの取組みガイド（2013.8 IPA）

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］
・東京：2020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

サイバーセキュリティ基本法の概要

§1　**目的**　：　総合的・効果的に施策を推進
➡　持続的発展／安全安心／国際社会の平和・安全保障

§2　**サイバーセキュリティ**　：
電磁的方式により記録等される情報の漏洩・滅失・毀損の防止等／ネットワーク等の安全性・信頼性の確保のために必要な措置が講じられ・維持管理されていること

§3　**基本理念**　：　情報の自由な流通、国民一人一人の認識・自発的対応、活力ある経済社会、国際的協調、IT基本法の理念配慮、国民の権利

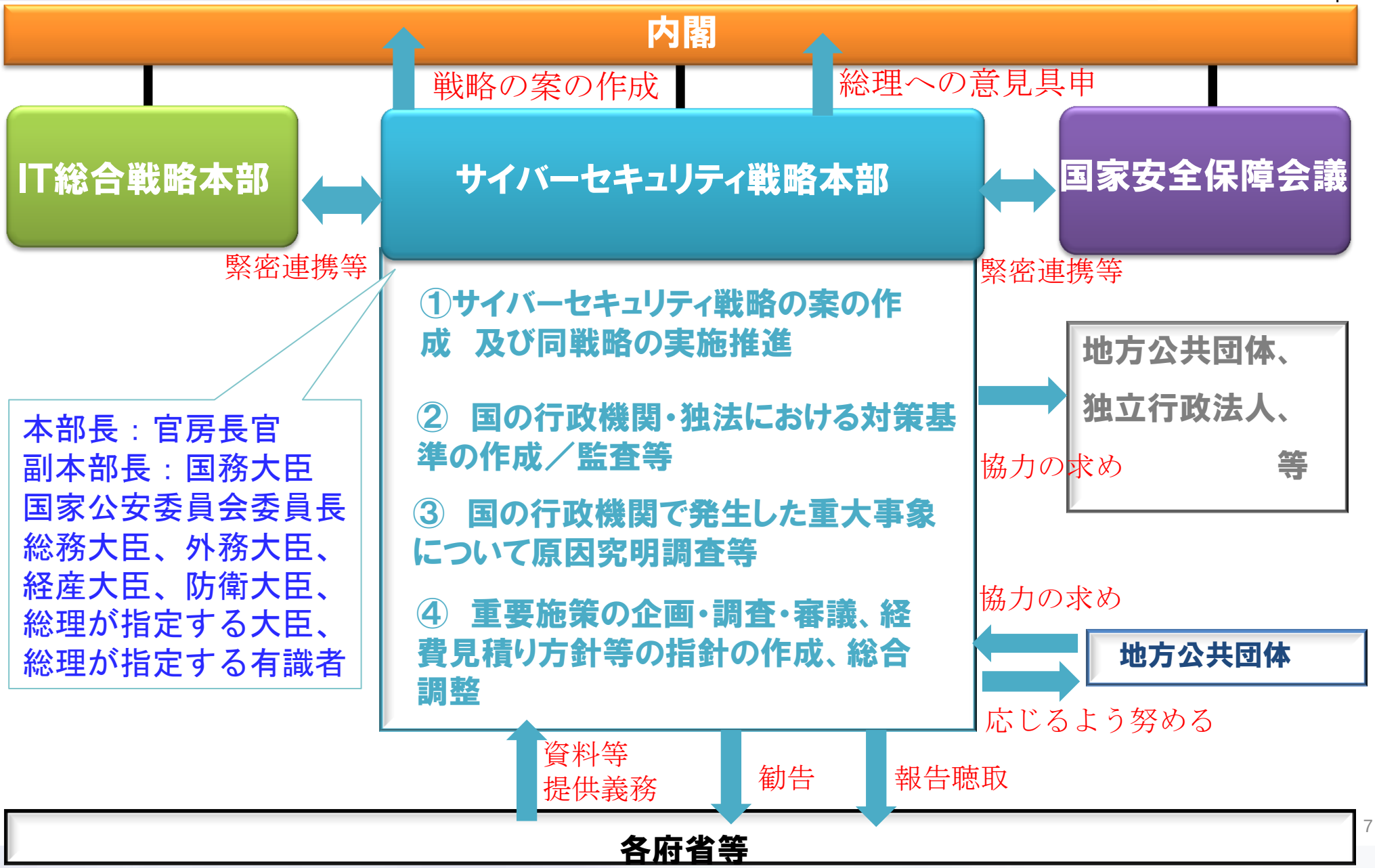
§4～　各主体の責務/努力　等

§12　**サイバーセキュリティ戦略の閣議決定・国会報告**

§13～　**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、
重要社会基盤事業者等におけるサイバーセキュリティの確保、等

§24～　**サイバーセキュリティ戦略本部**

サイバーセキュリティ戦略本部の機能・権限（イメージ）



「内閣サイバーセキュリティセンター」の設置

サイバーセキュリティ戦略本部
（本部長：内閣官房長官）

戦略本部に関する事務：内閣官房副長官補

事務局

内閣サイバーセキュリティセンター（注1）
（センター長：内閣官房副長官補（事態対処・危機管理担当））

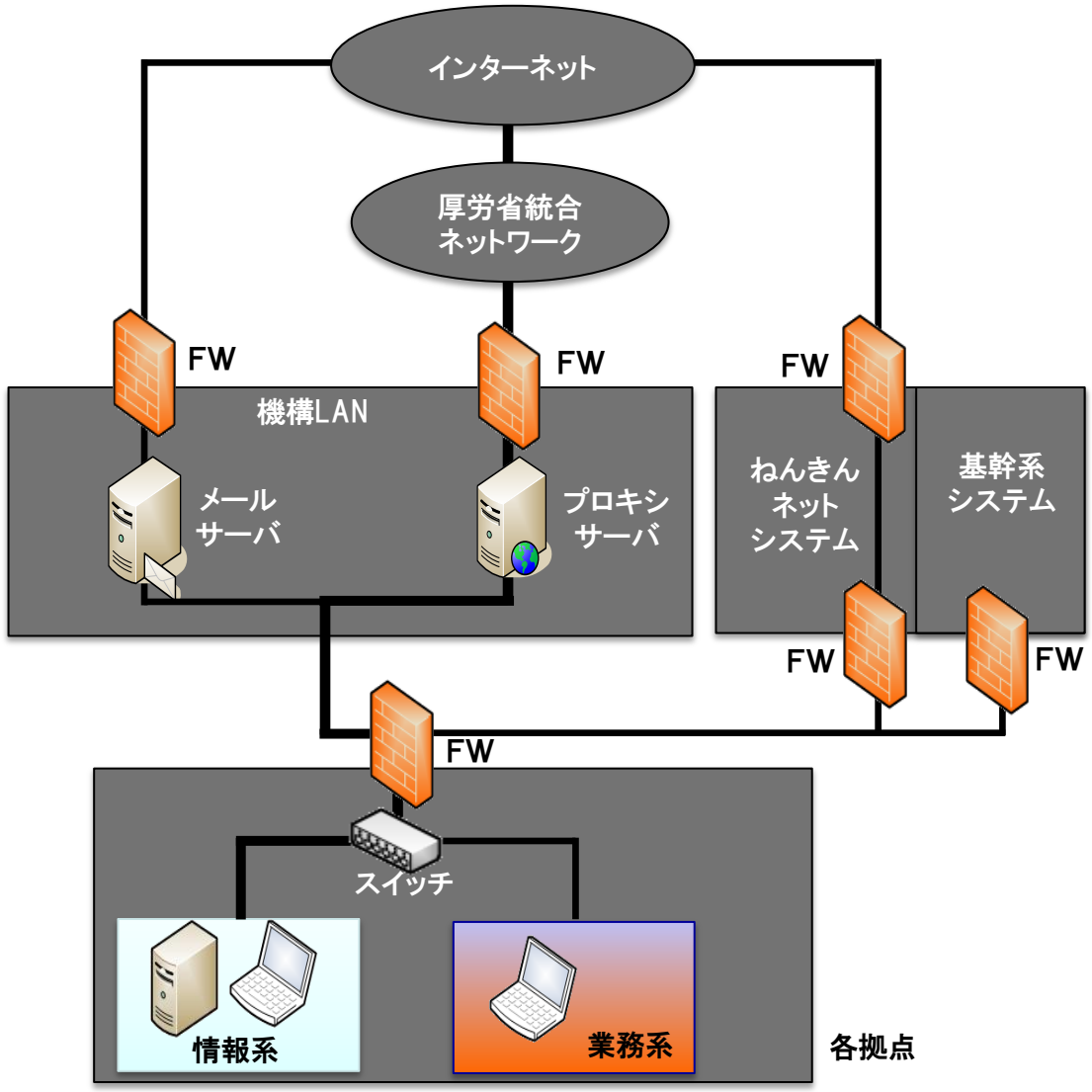
● 内閣サイバーセキュリティセンターの所掌事務

① ＧＳＯＣ（注2）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

（注1）英名称：National center of Incident readiness and Strategy for Cybersecurity
（注2）GSOC：政府機関情報セキュリティ横断監視・即応調整チーム（Government Security Operation Coordination team）

平成27年1月9日設置

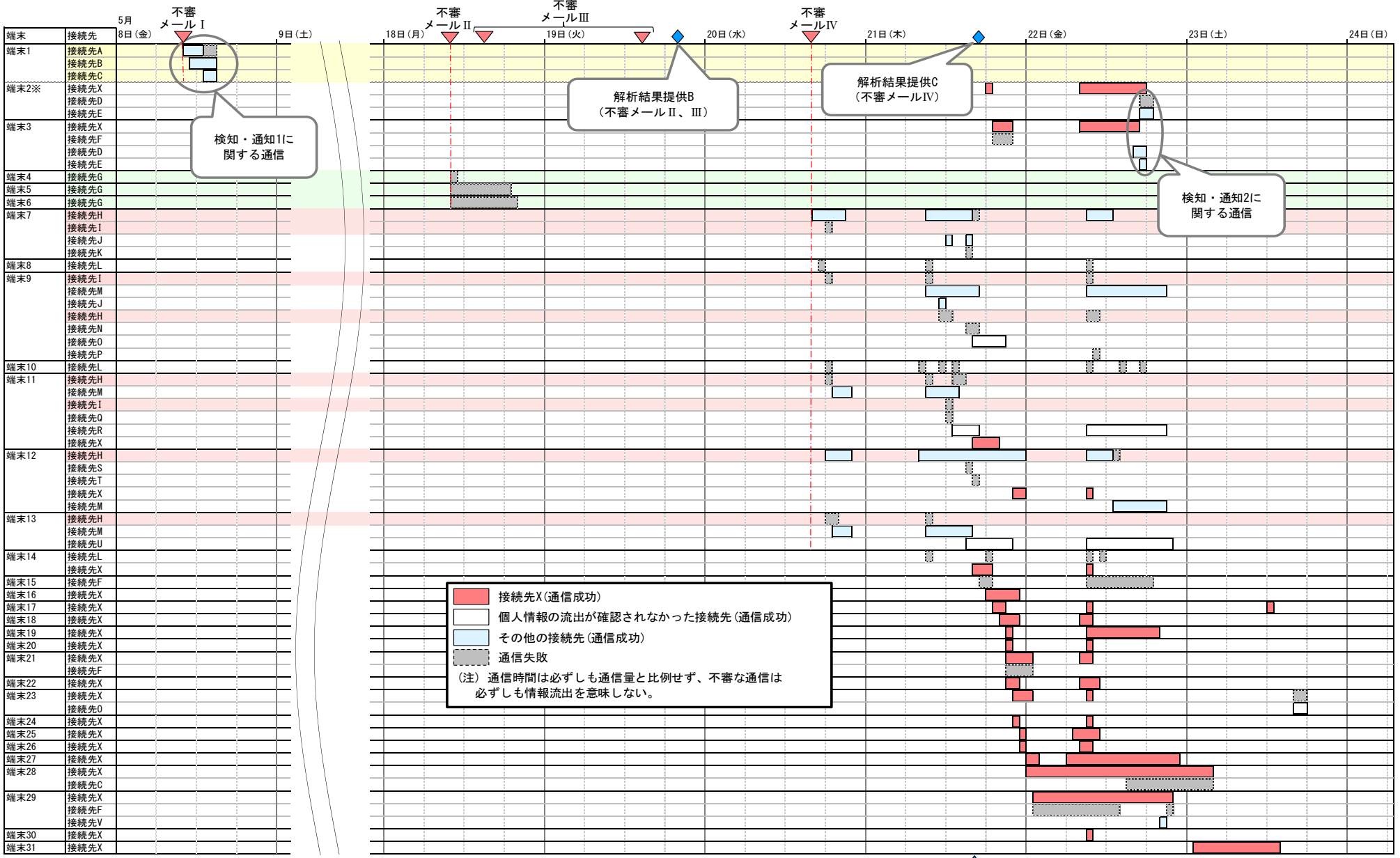
年金機構の事例①


インターネット
厚労省統合
ネットワーク
FW
FW
FW
機構LAN
メール
サーバ
プロキシ
サーバ
ねんきん
ネット
システム
基幹系
システム
FW
FW
FW
スイッチ
情報系
業務系
各拠点

年金機構の事例②

受信日	不審メールの概要	発生した不審な通信
5月8日	件名：「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先：公開メールアドレス(2)	端末1台が不正プログラムに感染、不審な通信が発生。約4時間後に端末の通信ケーブルを抜線、その後は不審な通信なし。
5月18日	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス(98)	端末3台が不正プログラムに感染、不審な通信が発生するも接続先への通信は失敗。
5月18日 ～ 5月19日	件名：厚生年金徴収関係研修資料 宛先：非公開の個人メールアドレス(20)	不審な通信は発生せず。
5月20日	件名：【医療費通知】 宛先：公開メールアドレス(3)	20日午後、端末1台が不正プログラムに感染、不審な通信が発生。数時間以内に、他の6台の端末からも不審な通信が発生。 21日から23日にかけて、合計21台の端末から国内のサーバ(接続先X)への多数の通信。

年金機構の事例③


5月
8日（金）
9日（土）
18日（月）
19日（火）
20日（水）
21日（木）
22日（金）
23日（土）
24日（日）
不審メールⅠ
不審メールⅡ
不審メールⅢ
不審メールⅣ
検知・通知1に関する通信
解析結果提供B（不審メールⅡ、Ⅲ）
解析結果提供C（不審メールⅣ）
検知・通知2に関する通信
端末
接続先
端末1 接続先A 接続先B 接続先C
端末2※ 接続先X 接続先D 接続先E
端末3 接続先X 接続先F 接続先D 接続先E
端末4 接続先G
端末5 接続先G
端末6 接続先G
端末7 接続先H 接続先I 接続先J 接続先K
端末8 接続先L
端末9 接続先I 接続先M 接続先J 接続先H 接続先N 接続先O 接続先P
端末10 接続先L
端末11 接続先H 接続先M 接続先I 接続先Q 接続先R 接続先X
端末12 接続先H 接続先S 接続先T 接続先X 接続先M
端末13 接続先H 接続先M 接続先U
端末14 接続先L 接続先X
端末15 接続先F
端末16 接続先X
端末17 接続先X
端末18 接続先X
端末19 接続先X
端末20 接続先X
端末21 接続先X 接続先F
端末22 接続先X
端末23 接続先X 接続先O
端末24 接続先X
端末25 接続先X
端末26 接続先X
端末27 接続先X
端末28 接続先X 接続先C
端末29 接続先X 接続先F 接続先V
端末30 接続先X
端末31 接続先X
接続先X（通信成功）
個人情報の流出が確認されなかった接続先（通信成功）
その他の接続先（通信成功）
通信失敗
（注） 通信時間は必ずしも通信量と比例せず、不審な通信は必ずしも情報流出を意味しない。
（凡例） 不審メールⅠに係る不正プログラムの接続先
不審メールⅡに係る不正プログラムの接続先
不審メールⅣに係る不正プログラムの接続先
不審メール受信
解析結果提供
※ 端末2は端末1の代替機（IPアドレスは同一）

標的型攻撃の特徴と対策

□ 標的型攻撃の特徴

○ **メール開封を前提**とした対策が必要
○ 初期段階での認知・対処、**侵入範囲を拡大させない**ための**システム設計・構築・運用**が重要

□ 標的型攻撃に対する情報システム防御策等の考え方

［検討対策例］

◆ システム防御策

- メールに添付された**実行形式のファイルを取り込まない・起動できないようにシステム設定**
- 既知の**脆弱性を放置しない**（アップデート、脆弱性診断等）
- **ウェブブラウザの拡張機能の必要最小限の使用**
- 侵入範囲が**拡大しにくいよう**に設定・運用
- 重要な情報に攻撃が到達しないよう、**システム分離**
  （各システムで扱える情報・できない情報につきルール化し、職員に徹底）
- **ローカル管理者権限**のパスワードを共通とする範囲の**最小限化**
- **不要な管理アカウント**の確実な**消去**
- 内部ネットワークにおける**異常を検知**する仕組みの整備

◆ インシデント対策に係る対策

- 不審メールの受信につき攻撃者が繰り返して攻撃を試みるものとして**継続的に対応**
- システム構築・運用事業者とは独立した専門性の高い事業者への依頼等、**平素からの準備**
- CISO等**権限を有する者の下**でのインシデント対応

（出典）サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」（2015年8月）

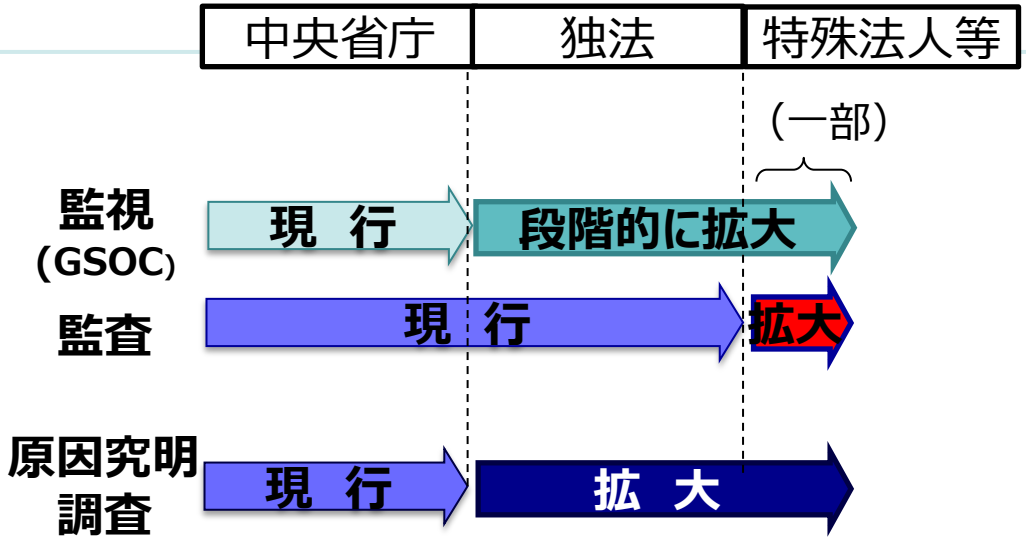
新たなサイバーセキュリティ戦略：政府機関等に係る対策①

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、所要の法改正を含め、抜本的な強化を図る。

1．NISCの機能強化

■ GSOCの大幅な機能強化

■ 業務対象の拡大等



■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）、国立研究開発法人情報通信研究機構（NICT）等

■ NISCの要員強化（高度セキュリティ人材の民間登用等）

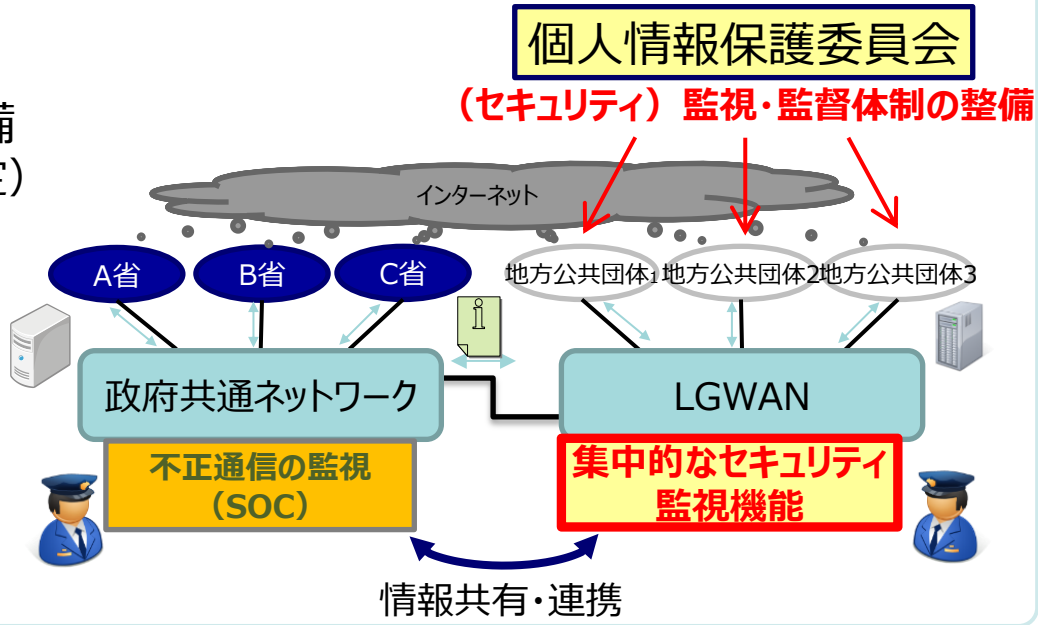
新たなサイバーセキュリティ戦略：政府機関等に係る対策②

2．政府全体の取組強化

- 政府機関における体制強化　（CSIRT体制の強化、実践的訓練）
- 攻撃リスク低減のための対策強化（インターネット接続口の集約化、多重防御、インターネットからの分離等）
- 人材・予算の確保　（専任の指揮官　等）

3．　その他の重要課題への取組強化

- 重要インフラに関する取組強化
- セキュリティ人材の育成のための演習環境の整備
  （本年度中に人材育成総合強化方針(仮称)を策定）
- 官民連携による大規模サイバー攻撃への対応
- マイナンバー制度の円滑な導入に向けた
  対策の強化
- 事案対処に関する取組強化



我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針

目的：深刻化が進むサイバー攻撃に備え、**政府機関等をはじめとしたサイバーセキュリティ推進体制の更なる機能強化に向けた具体的な方向性**を定めるもの。

更なる取組強化策

(1) 国が行う不正な通信の監視等の対象の拡大

(2) サイバーセキュリティに係る政府人材等の強化

(3) 大規模なサイバー攻撃に備えた官民の連携体制等の構築

(4) 重要インフラ事業者等に関する取組支援の強化

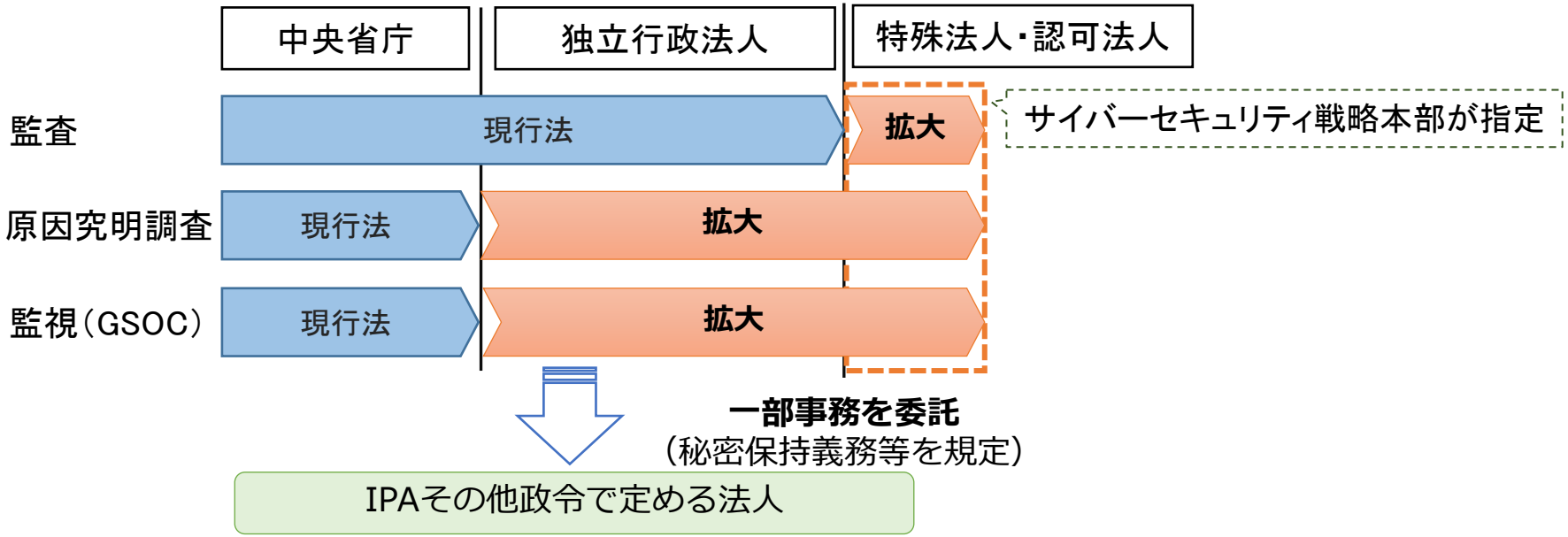
(5) マイナンバー事業の円滑な導入及び推進

(6) 東京オリンピック・パラリンピック競技大会等に向けた取組の加速化

サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案の概要（H28.2.2閣議決定）

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）等に委託

基本法



情促法

■ サイバーセキュリティ対策の強化に係る観点から、以下の規定の整備を行う。
- 本部から委託を受ける事務に係るIPAの業務追加
- 情報処理安全確保支援士制度の創設（名称独占、更新制、秘密保持義務等）
- ソフトウェアの脆弱性情報等の公表の方法・手続を整備

新たな「サイバーセキュリティ戦略」について（全体構成）

NISC

1 サイバー空間に係る認識

- サイバー空間：「**無限の価値を産むフロンティア**」である人工空間経済社会の活動基盤
- 「**連接融合情報社会（連融情報社会）**」が到来
  サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展➡「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ／②受動から**主導**へ／③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

費用から投資へ

- ■ 安全なIoTシステムの創出
- ■ セキュリティマインドを持った企業経営の推進
- ■ セキュリティに係るビジネス環境の整備

国民が安全で安心して暮らせる社会の実現

2020年・その後に向けた基盤形成

- ■ 国民・社会を守るための取組
- ■ 重要インフラを守るための取組
- ■ 政府機関を守るための取組

国際社会の平和・安定 我が国の安全保障

サイバー空間における積極的平和主義

- ■ 我が国の安全の確保
- ■ 国際社会の平和・安定
- ■ 世界各国との協力・連携

横断的施策

- ■ 研究開発の推進
- ■ 人材の育成・確保

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

新たな「サイバーセキュリティ戦略」について（各論①）

経済社会の活力の向上及び持続的発展

～費用から投資へ～

■安全なIoTシステムの創出

- 企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(SBD)の考え方に基づき、安全なIoT(モノのインターネット)システムを活用した事業を振興
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を整合的に実施するための体制等を整備
- エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドライン等を整備
- IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築(経営ガイドライン等の発信含む)
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民民間・官民間における脅威・インシデント情報の共有網の拡充

■セキュリティに係るビジネス環境の整備

- 政府系ファンドの活用等により、サイバーセキュリティ関連産業を振興(ベンチャー企業の育成等を含む)
- 中小企業等のクラウドサービス活用に有効なセキュリティ監査の普及促進
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステムのセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備

▲自動運転車の実証実験

サイバーセキュリティに関するリスク開示（有価証券報告書）

NISC

- 開示企業数は、平成21年度の52%（116社）から 平成25年度の60%（136社）へと増加。

日経業種分類				開示企業数	開示企業%	
大分野	（社数）	中分野	（社数）		中分類	大分類
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	7	5	71.4%	
D 素材	64	14 鉱業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
		35 ガス	2	2	100.0%	
合計	225		225	136		

新たな「サイバーセキュリティ戦略」について（各論②）

国民が安全で安心して暮らせる社会の実現　～2020年・その後に向けた基盤形成～

■国民・社会を守るための取組

- ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化の推進
- 攻撃を受けた端末の利用者に対する注意喚起等の推進
- 整備が進む公衆無線LAN等のセキュリティ確保のための対策検討
- 地域における普及啓発活動の促進、中小企業や地方公共団体への啓発・支援
- サイバー犯罪への対処能力・捜査能力の向上に向けた取組の強化
  (通信履歴の保存の在り方についての関係事業者における適切な取組の推進を含む)

▲双方向型の普及啓発セミナー（サイバーセキュリティカフェ）

■重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制を整備
- スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進


▲サイバー攻撃等に対する対応能力向上のための演習
（重要インフラ分野横断的演習）

■政府機関を守るための取組

- ペネトレーションテスト等を通じたセキュリティ対策を徹底、サプライチェーン・リスクへの対応、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能強化、 標的型攻撃に対する多重防御の取組加速等による防御力の強化
- マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化
- 新たなIT製品・サービスの特性を踏まえた政府統一的なセキュリティ対策の策定・推進
- 独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等への監視・監査・原因究明調査の実施等による総合的な対策強化

重要インフラ事業者に係る取組み

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

１．安全基準等の整備及び浸透
　対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求

２．情報共有体制の強化
　平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化

３．障害対応体制の強化
　関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化

４．リスクマネジメント
　重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援

５．防護基盤の強化
　関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　　等

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

政府機関における情報集約・支援体制の枠組み

NISC

政府機関・情報セキュリティ横断監視・即応調整チーム（GSOC）

平成19年度　GSOCの整備を開始
平成20年度　整備完了、本格運用を開始
平成21年度　本格運用

リアルタイム横断的監視
（24時間対応）
分析力の向上

警告・助言
的確・迅速な情報共有による
各省庁の対応力向上

不正プログラムの分析・各
種脅威情報の収集

監視

相互連携

情報セキュリティ緊急支援チーム（CYMAT）

①発生事象の正確な把握
②被害拡大防止、復旧、再発防止のための技術的な支援及び助言
③対処能力の向上に向けた平時の取組（研修、訓練等の実施）

支援

相互連携体制

検知情報等の提供

発生事案等の報告

技術的な支援・助言

各府省庁　組織内CSIRT

GSOC センサー
A省 CSIRT
PoC

CSIRT間の連携

GSOC センサー
C省 CSIRT
PoC

GSOC センサー
B省 CSIRT
PoC

対処

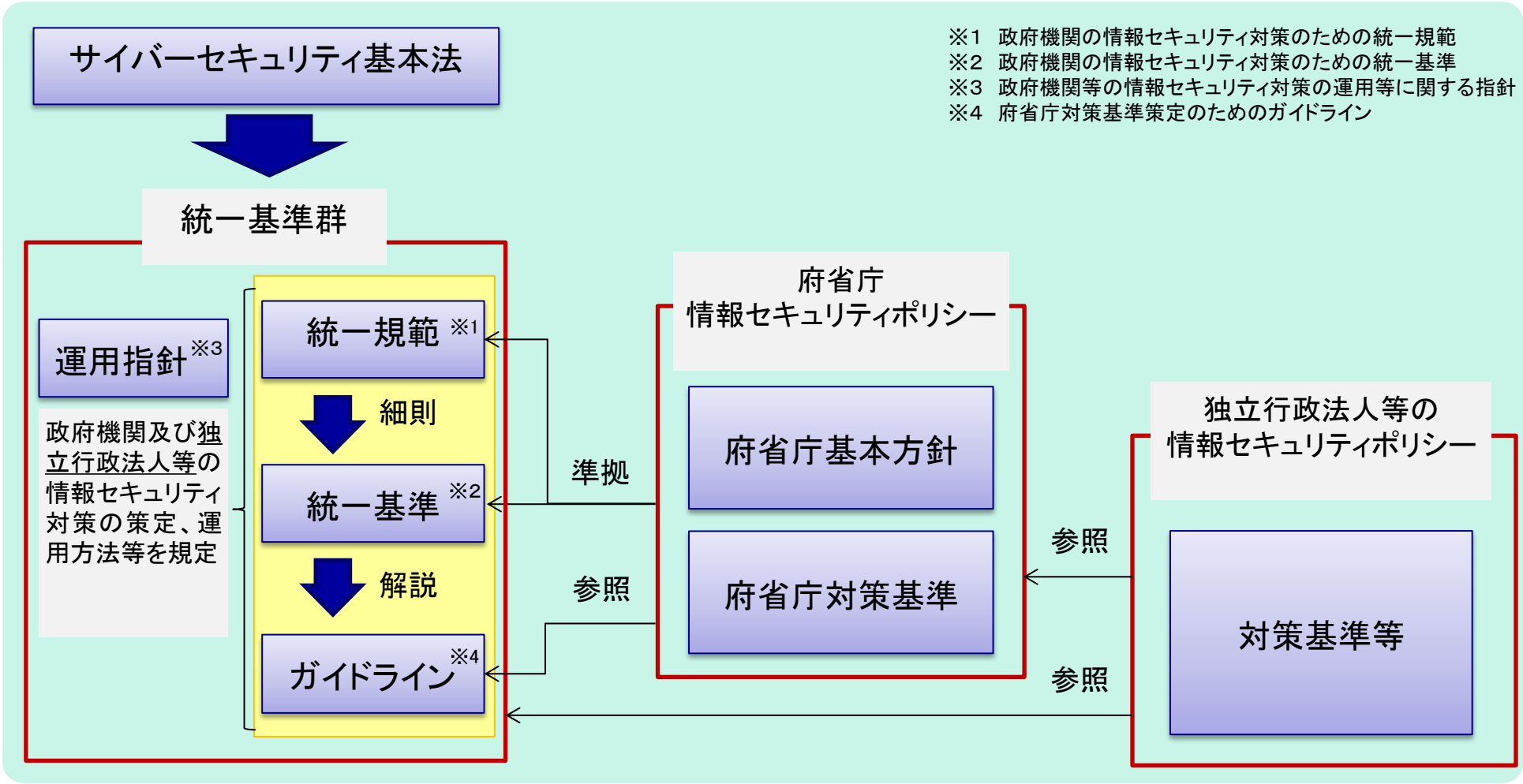
情報連携の結節点

NISC

連携・情報交換

民間CSIRT 等

政府機関の対策基準等


※1　政府機関の情報セキュリティ対策のための統一規範
※2　政府機関の情報セキュリティ対策のための統一基準
※3　政府機関等の情報セキュリティ対策の運用等に関する指針
※4　府省庁対策基準策定のためのガイドライン
サイバーセキュリティ基本法
統一基準群
運用指針※3
政府機関及び独立行政法人等の情報セキュリティ対策の策定、運用方法等を規定
統一規範※1
細則
統一基準※2
解説
ガイドライン※4
準拠
参照
参照
府省庁
情報セキュリティポリシー
府省庁基本方針
府省庁対策基準
参照
参照
独立行政法人等の
情報セキュリティポリシー
対策基準等

国の行政機関に対する監査

サイバーセキュリティ戦略本部

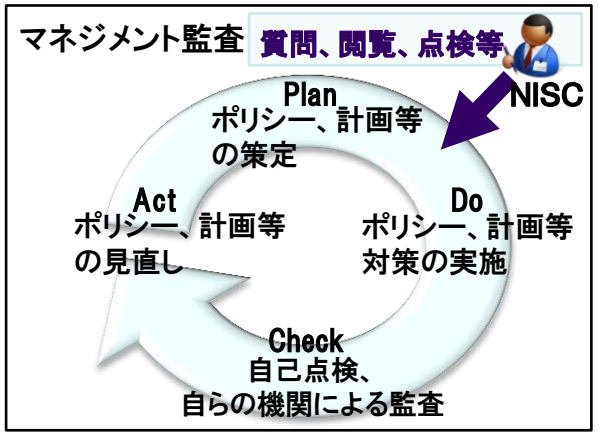
事務委任

報告等

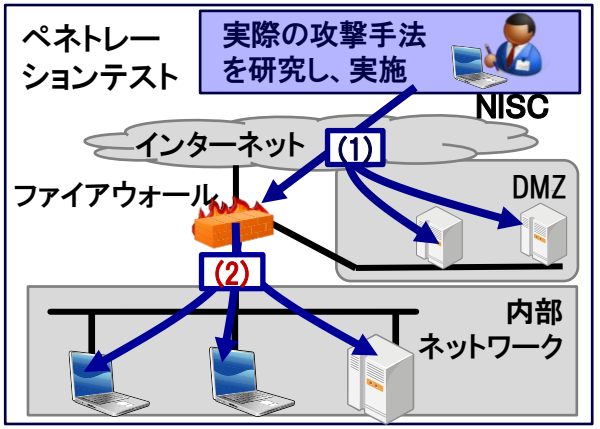
①②の二本立てで監査を実施

NISC

①セキュリティ対策強化のための体制・制度が機能しているかの検証による評価（監査）



②情報システムに対する疑似的攻撃による評価（監査）



普及啓発（サイバーセキュリティ月間等）

普及啓発プログラム

- 国民一人一人がどうしたらよいか　⇒　相談、助言等
- 地域での取組促進
- 協議会方式で
- 学ぶ機会のある人、ない人等向けの施策

新たな「サイバーセキュリティ戦略」について（各論③）

国際社会の平和・安定及び我が国の安全保障　～サイバー空間における積極的平和主義～

■我が国の安全の確保

- 警察や自衛隊を始めとする対処機関の能力の質的・量的な向上
- 安全保障上重要な先端技術(宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等)に係るサイバーセキュリティの確保
- 政府機関や重要インフラ事業者等によるサービスの持続的提供のための情報の共有・分析・対応に向けた官民連携の一層の強化

▲日ASEAN情報セキュリティ政策会議

■国際社会の平和・安定

- 国連等におけるサイバー空間に係る国際的なルール等の形成に向けた積極的な貢献
- サイバー空間を悪用する国際テロ組織に対する国際社会と連携した対処
- 各国の能力構築(キャパシティビルディング)への積極的な協力の推進

▲我が国で開催したサイバーセキュリティに関する国際カンファレンス（Meridian Conference 2014）

■世界各国との協力・連携

- アジア大洋州　：　日・ASEAN間の協力関係の更なる深化・拡大並びに地域の戦略的パートナーとの協力・連携の強化
- 北米　：　同盟国たる米国とあらゆるレベルでの緊密な連携・対応(日米サイバー対話、インターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ等)
- 欧州・中南米・中東アフリカ　：　基本的価値観を共有する国々とのパートナーシップの構築・強化

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：２０１４年10月　等

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　等

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)等

フランス
○日仏サイバー協議(2014年12月）等

イスラエル
○日イスラエルサイバー協議（2014年11月）等

ロシア
○日露サイバー協議（2015年3月）

日中韓（2015年10月等）

リスクのグローバル化

国際連携取組方針
（１３年１０月）
●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：２０１４年4月@ワシントン　等

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　等

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。

新たな「サイバーセキュリティ戦略」について（各論④・推進体制）

横断的施策

■研究開発の推進

- 関係者間の情報・データの共有等によるサイバー攻撃の検知・防御能力の一層の向上
- 融合領域の研究促進、及び安全保障のためのコア技術(暗号技術等)の保持
- 各国が強みを有する技術を有機的に組み合わせた国際連携による研究開発の推進

▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ

■人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 初等中等教育段階からの教育の充実
  (論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実)
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進

▲ 58ヶ国が参加したセキュリティコンテスト(2014年度)

5 推進体制

- NISC対処能力の一層の強化や産学官及び関係省庁間の連携強化によるサイバー攻撃の検知・分析・判断・対処の機能強化
- 国家の関与が疑われる高度な攻撃に対し、戦略本部とNSC(安全保障)・重大テロ対策本部(危機管理)と緊密に連携
- オリンピック・パラリンピック東京大会等に向け、リスクの明確化、組織・施設・協力関係の構築・維持、十分な訓練を実施

- 戦略本部は、各年度の年次計画及び年次報告を作成するとともに、経費見積り方針を策定する。

人材

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

「新・情報セキュリティ人材育成プログラム」

人材の「需要」と「供給」の好循環を形成

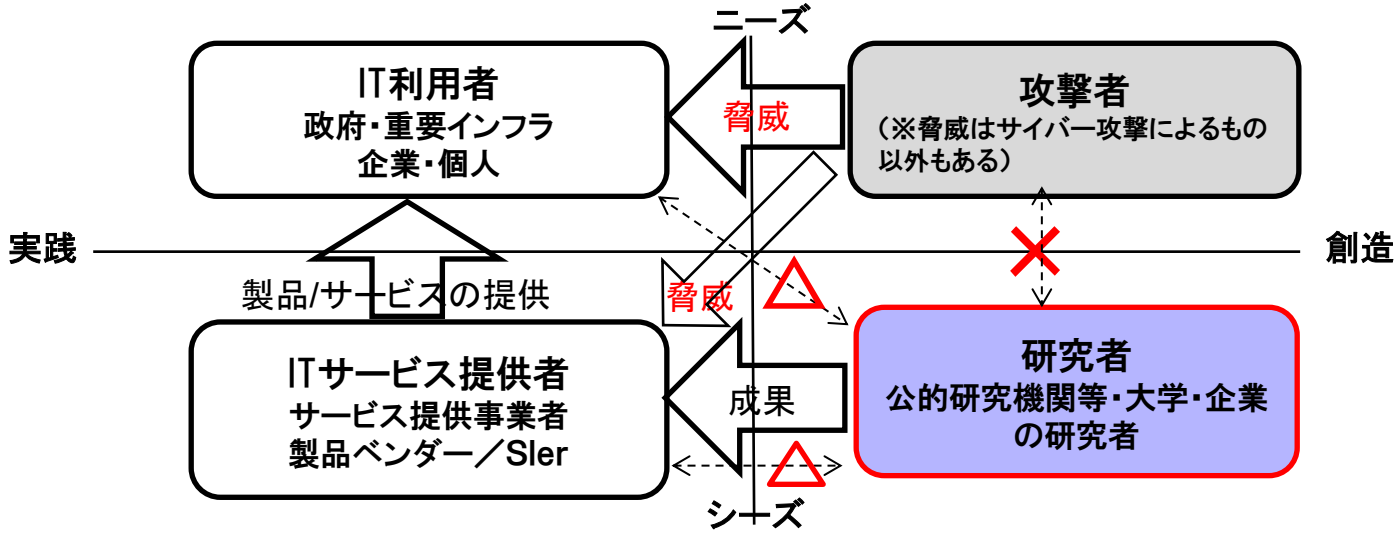
【需要】経営層の意識改革

- 組織の経営層に対する取組
- 経営層と実務者層との間のつなぎ人材

【供給】人材の「量的拡大」と「質的向上」

- 実務者層に対する取組
- グローバル水準の高度人材
- 教育等

産業／研究開発



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
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
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
4. 情報セキュリティの**コア技術の保持**
5. **国際連携**による研究開発の強化

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

(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

詳しい資料はこちら

NISCのホームページ ― http://www.nisc.go.jp/index.html

サイバーセキュリティ戦略（H27年9月4日閣議決定）
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf

我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針
（H28年1月25日本部決定） http://www.nisc.go.jp/active/kihon/pdf/cs_kyoka_hoshin.pdf

サイバーセキュリティ政策に係る年次報告（2014年度）（H27年7月23日本部決定）
http://www.nisc.go.jp/active/kihon/pdf/jseval_2014.pdf

サイバーセキュリティ関係施策に関する平成28年度予算重点化方針（H27年8月20日本部決定）
http://www.nisc.go.jp/active/kihon/pdf/yosanhoushin.pdf

日本年金機構における個人情報流出事案に関する原因究明調査結果（H27年8月20日本部決定）
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

政府統一基準、重要インフラの第3次行動計画、人材育成プログラム、研究開発戦略等については
情報セキュリティ政策会議決定 http://www.nisc.go.jp/conference/seisaku/index.html