

我が国のサイバーセキュリティ戦略

2015年9月17日

内閣サイバーセキュリティセンター（NISC）副センター長

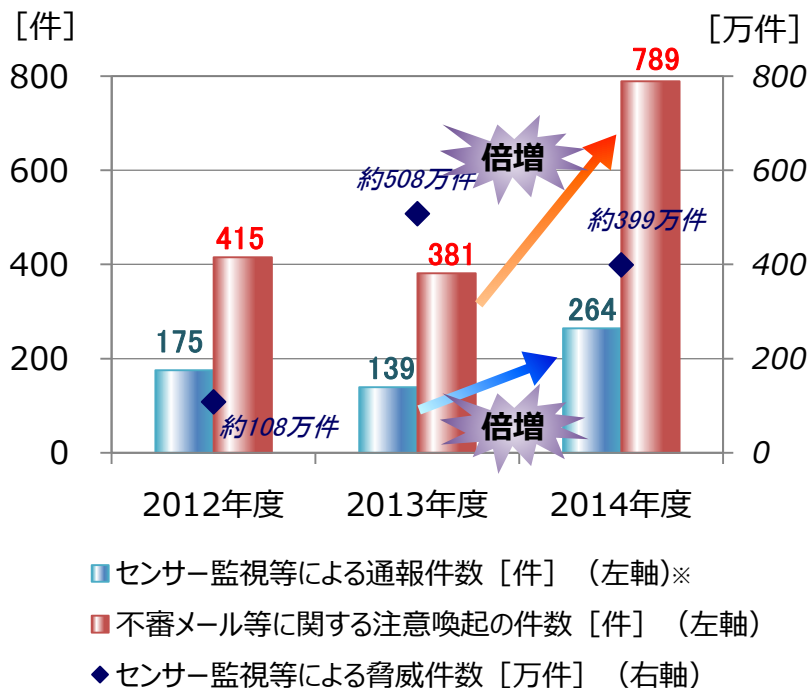
内閣審議官 谷脇 康彦

<http://www.nisc.go.jp/>

政府機関等における情勢

- **標的型攻撃の脅威が深刻化**しており、最近では日本年金機構が個人情報の流出を発表（2015年6月）。

【政府機関への脅威件数等】



※ 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。

【外部からの攻撃に係る2014年度の特徴】

以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、標的型メールによる脅威が一層深刻化。

- センサー監視等による**通報件数は前年度から倍増**（264件）、そのうち**約4割は標的型メール**（標的型メールの通報件数は前年度比約3倍に増加）。
- 不審メール等の**注意喚起件数は前年度から倍増**（789件）。
- センサー監視等による**脅威件数は約399万件**。
（約8秒毎に1回脅威を認知。前年度より減少したのは、GSOCシステムの能力向上によって、軽微なものの判別対象からの除外を含め、脅威の識別精度が向上したことによるもの。脅威そのものは一層深化。）
- 文書作成ソフト等の**未知の脆弱性を利用した攻撃**や、不正通信の接続先にクラウド上のサーバが利用される等、**認知・防御が困難に**。

（出典）NISC「サイバーセキュリティ政策に係る年次報告（2014年度）」（2015年7月）

PC



多くの職場・家庭に普及し、インターネットに接続
(2014年末：PC普及率 78.0%、インターネット普及率 82.8%)

※2015年版情報通信白書(総務省)

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

～海外のサイバー攻撃事案(2014年8月以降、報道ベース)～

○ JPモルガン・チェース(2014年8月中旬)

2014年8月、サイバー攻撃が行われ、顧客の名前、住所、電話番号、電子メールアドレス及びユーザー関連の内部情報が流出したことが明らかとなった。サイバー攻撃は、ウクライナをめぐる西側諸国によるロシアへの金融制裁に対する報復としてロシア政府の関与した可能性もあるとのFBI捜査官の見解もある。

○ ソニー・ピクチャーズ・エンターテインメント(2014年11月下旬)

2014年11月、「平和の守護者(Guardians of Peace)」を名乗る組織が、システムに侵入し、同社の数千に及ぶ社内文書や未公開の4作品を含む5作品の同社映画全編の違法コピーがオンライン上に流出。米国政府は、12月19日、当該サイバー攻撃を北朝鮮政府による犯行とし、翌月2日、大統領令を発出し追加的な経済制裁を実施。

○ 保険会社アンセム(2015年2月上旬)

2015年2月、同社に対するサイバー攻撃により、8,000万人分に及ぶ新旧加入者や従業員の個人情報が盗まれた。氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えいしたが、クレジットカードや医療記録などの情報は流出した形跡はないとしている。なお、攻撃者は米国人事管理局(OPM)(後述)へのサイバー攻撃を行った中国人民解放軍ハッカー部隊であるとの可能性も指摘されている。

○ フランスTV5モンド(2015年4月上旬)

2015年4月8～9日、フランス国営テレビTV5モンドは、イスラム国に所属すると主張するグループ「Cybercaliphate」によってTVチャンネル、Web、FaceBookが乗っ取られ、イスラム国の犯行を主張するメッセージが表示されていた。4月10日、フランス国防省は、調査の結果、軍の機密情報が漏えいすることはなかったと発表した。

○ ドイツ連邦委議会(2015年5月上旬)

2015年5月15日、ドイツ連邦議会(下院)のサーバにサイバー攻撃を受け、約2万台のパソコンが外部から自由に操作できる状態となった。メルケル首相の下院事務局のパソコンも感染。情報機関のトップは、手法が極めて巧妙であることからロシアの関与を示唆している。少なくとも5人の議員のパソコンからデータ流出が確認されており、それ以外の情報も流出するおそれがあるとしている。

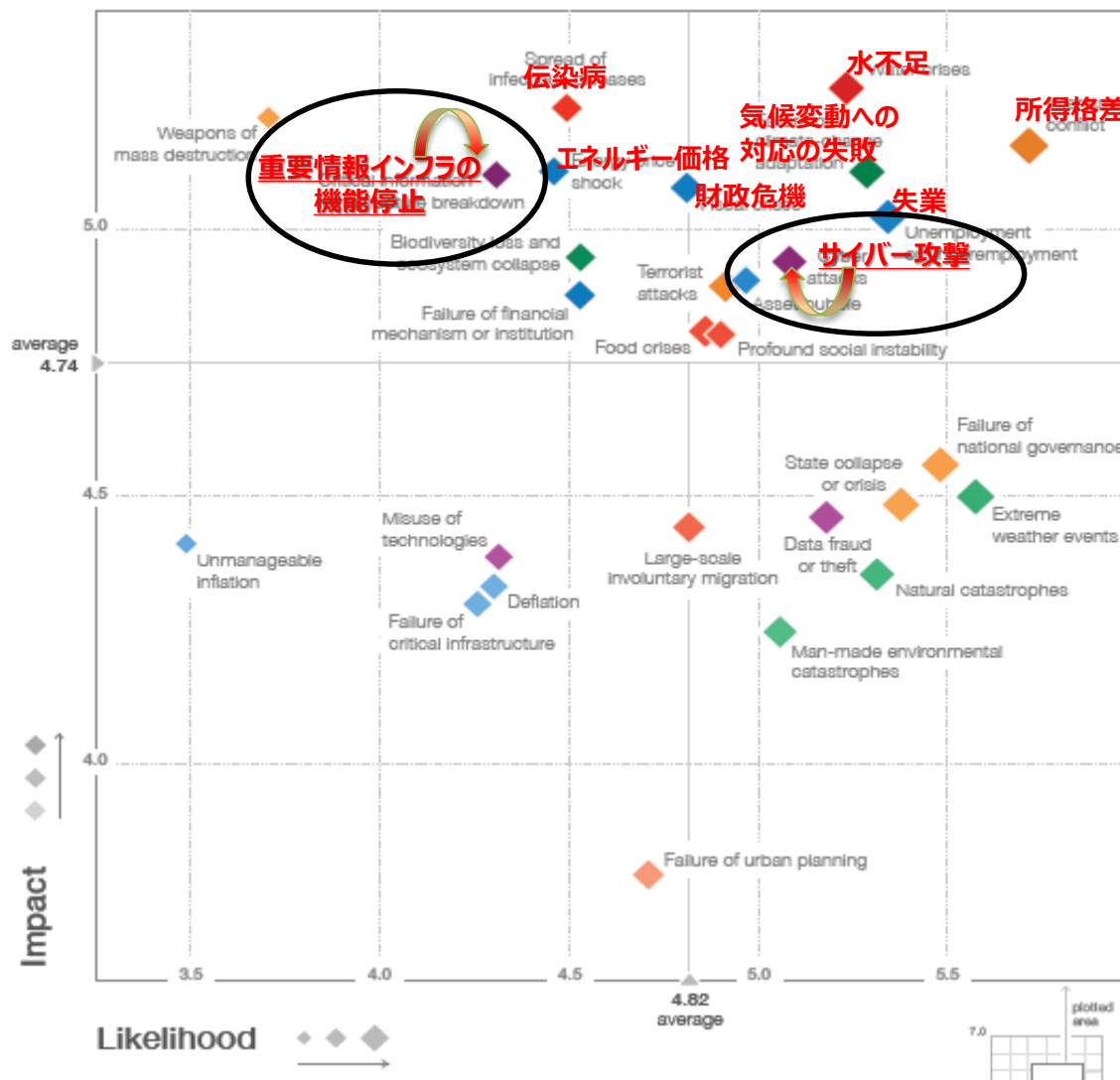
○ イラン核問題6か国協議会場(2015年5月中旬)

2015年5月12日、スイス当局はイランの核問題をめぐる6か国協議がジュネーブのホテルで行われた際、サイバー攻撃が行われた可能性があり、それに関連するホテルの家宅捜査及びITシステムやソフトウェアの差し押さえを行ったと報道されている。イスラエルの関与が疑われているが、イスラエルは根拠のないものであると否定している。

○ 米国人事管理局(2015年6月上旬)

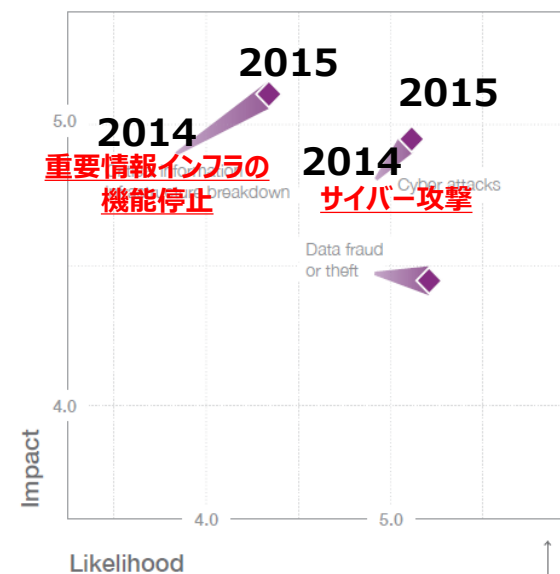
2015年6月4日、米国人事管理局は、システムが侵入され、2,210万件の職員及び元職員の個人情報が流出したと発表。同局は、情報流出による影響を調べているが、人事管理局や内務省だけでなく、ほぼすべての連邦政府機関に及ぶとされる。さらに数百万人の職員の情報が流出していた可能性もあるとしている。専門家の見解では、中国人民解放軍のハッカー部隊である「ディープ・パンダ」と呼ばれる組織が今回の攻撃及び保険会社アンセムへの攻撃を実施したとされている。

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”

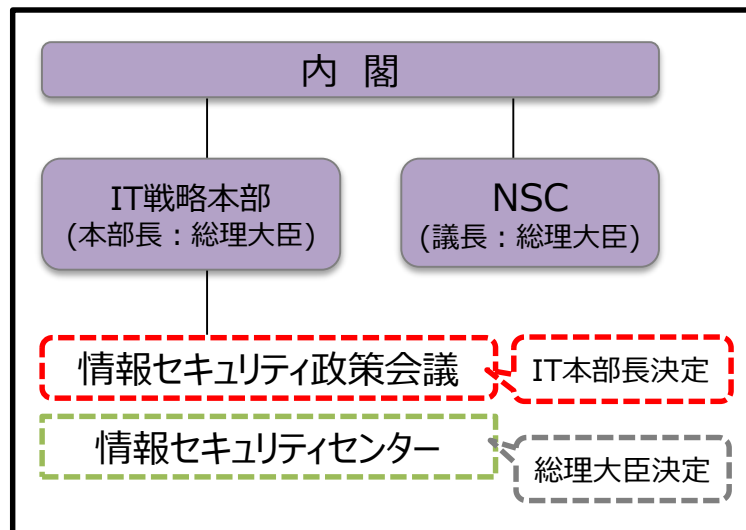
サイバーセキュリティ基本法の施行（2015年1月）



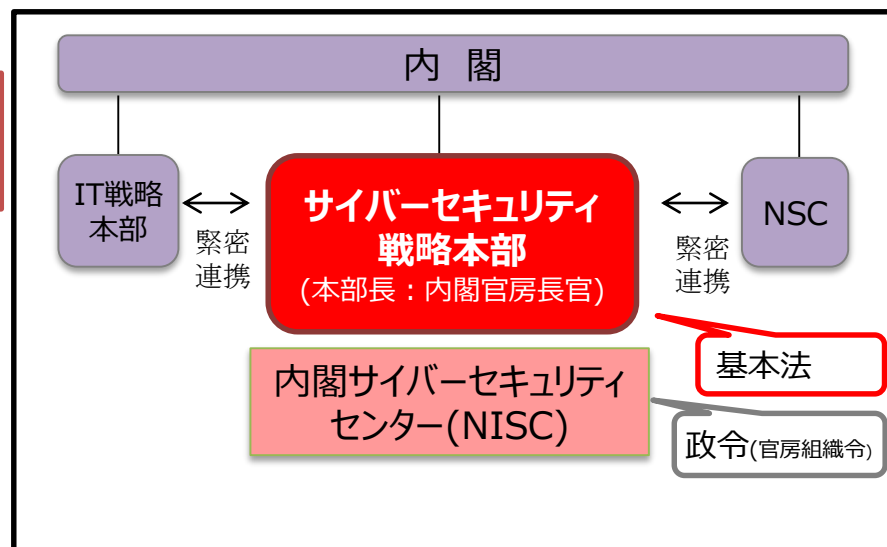
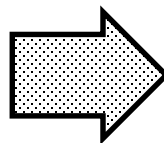
施行前

施行後

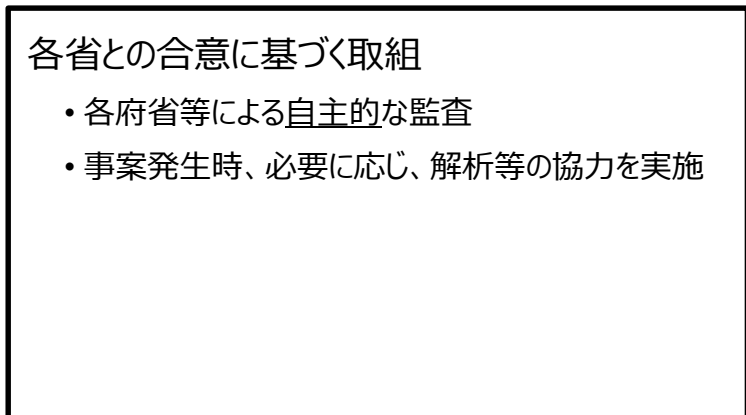
政府の推進体制



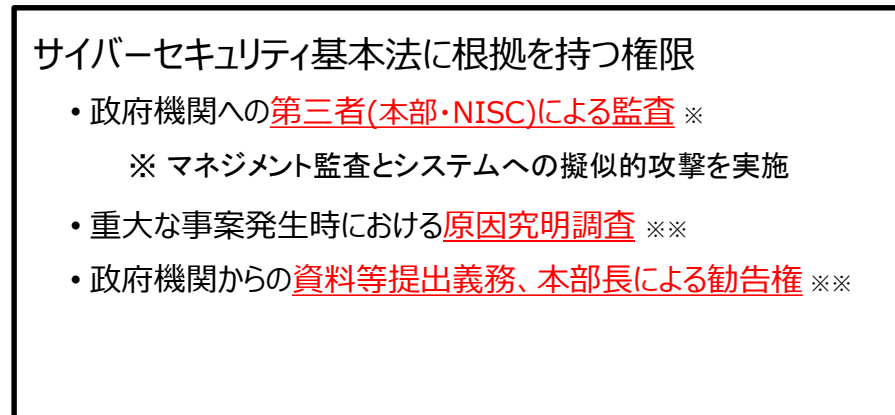
法律・政令で
設置根拠を
明確化



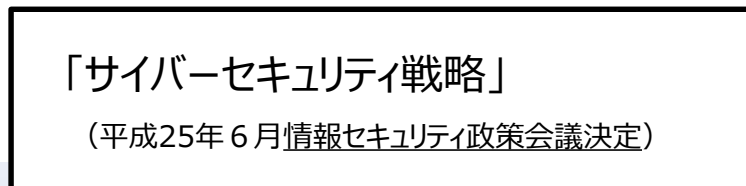
各省への権限



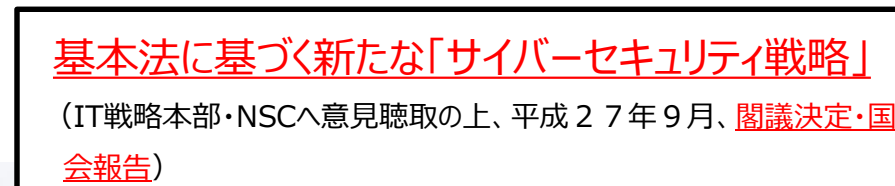
権限強化



基本戦略

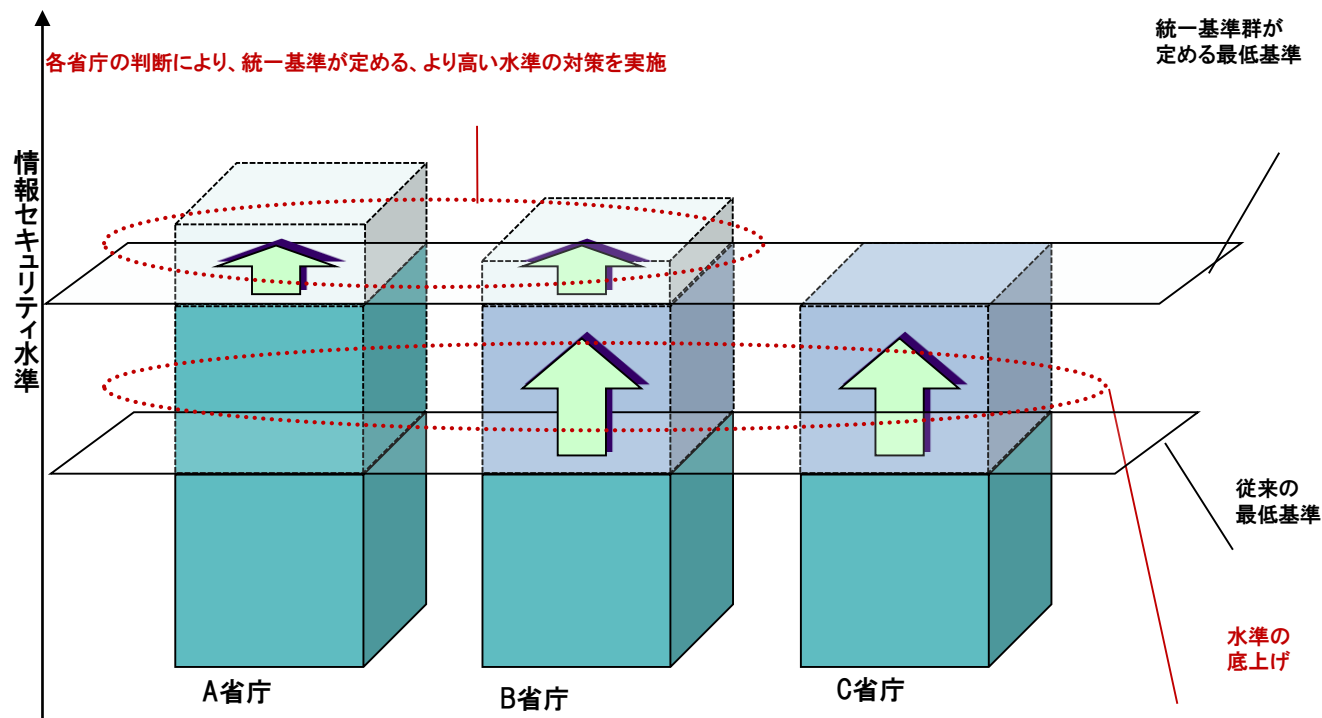


格上げ



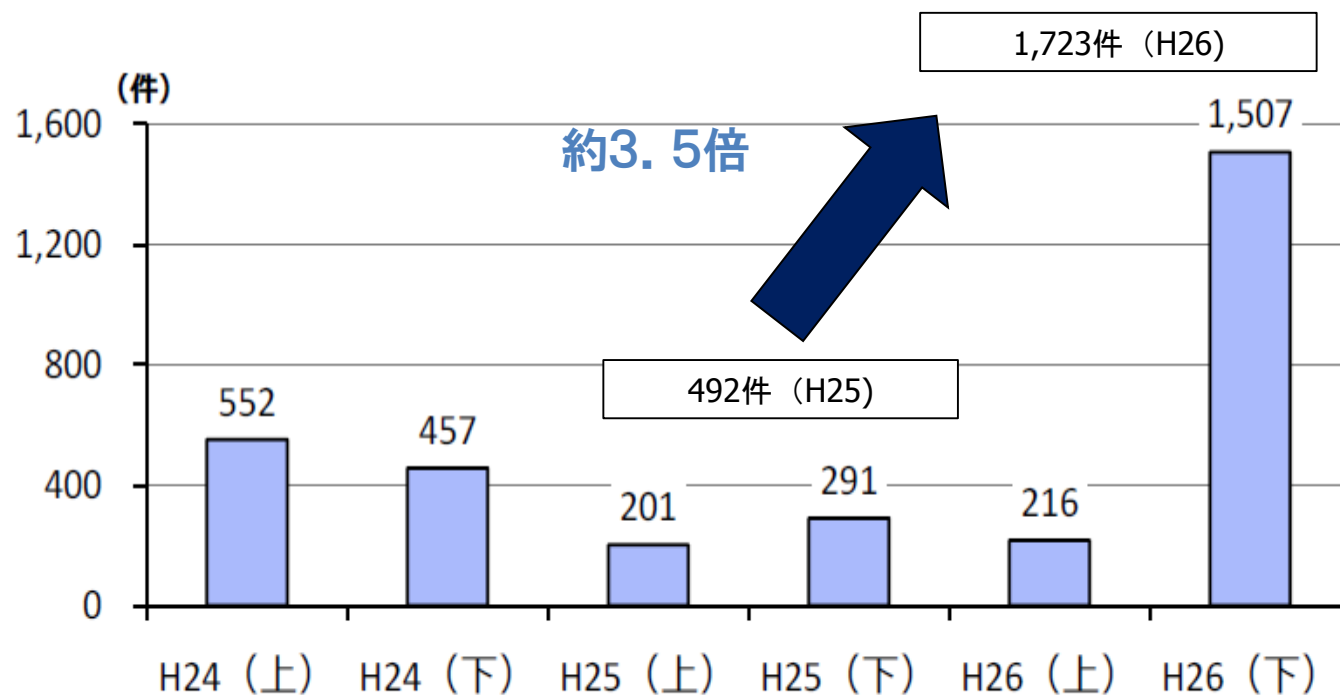
- 政府機関が実施すべき対策の統一的な枠組みを構築
- 政府機関全体の情報セキュリティ水準の底上げに寄与
- 標的型攻撃対策に力点。

<統一基準群の効果(イメージ)>



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。



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)

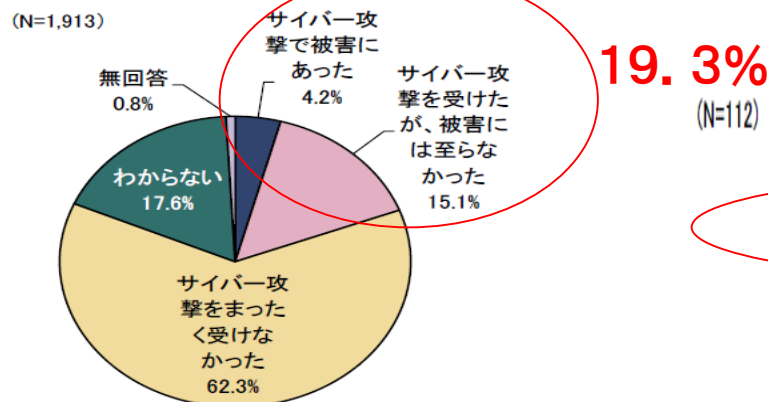


図 3.5-1 サイバー攻撃の遭遇経験

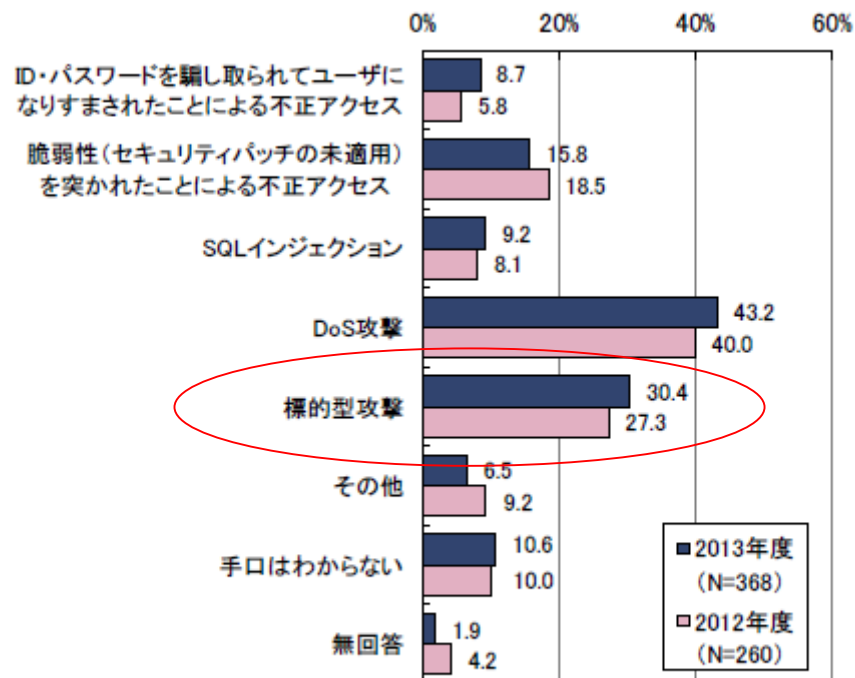


図 3.5-5 サイバー攻撃の手口 (2012 年度調査との比較)

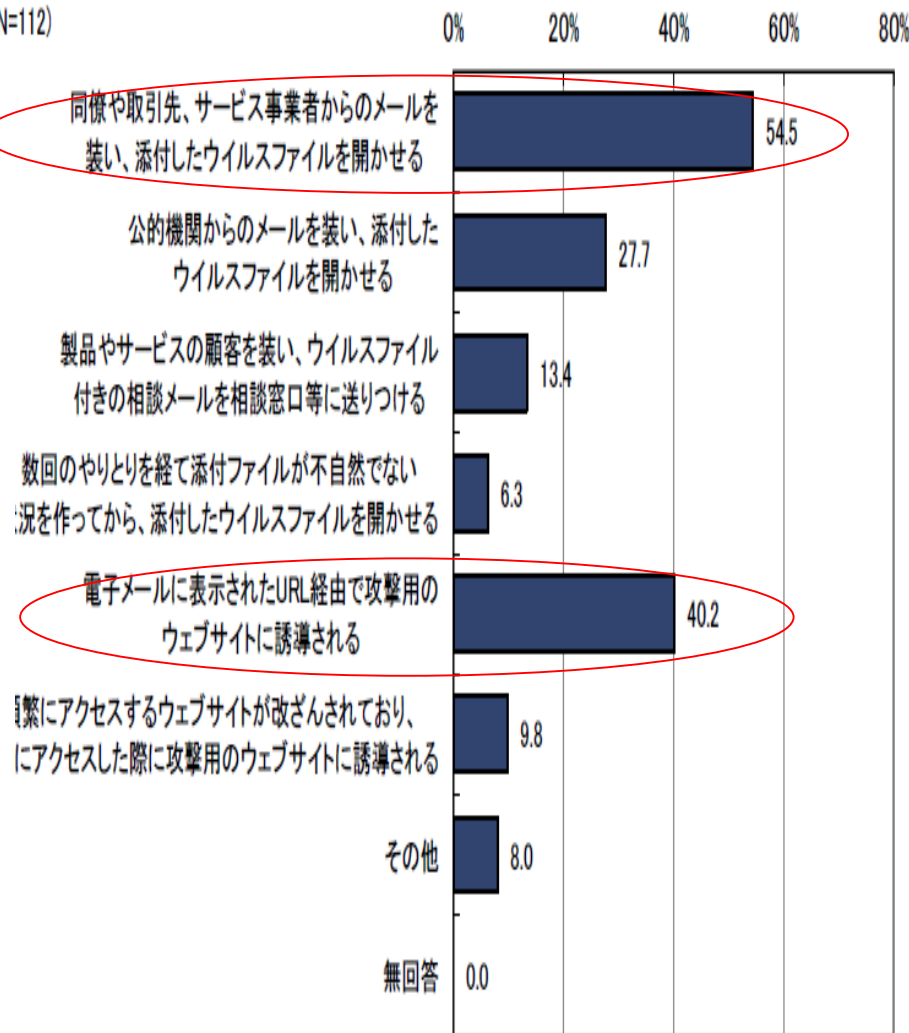


図 3.5-9 標的型攻撃の具体的な手段

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

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



クリックすると

<http://10.243.23.11/詐欺/>

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

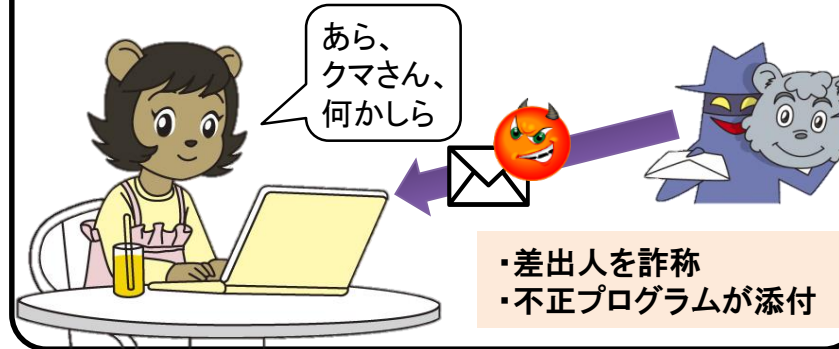
全く別のアドレスに偽装可能

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

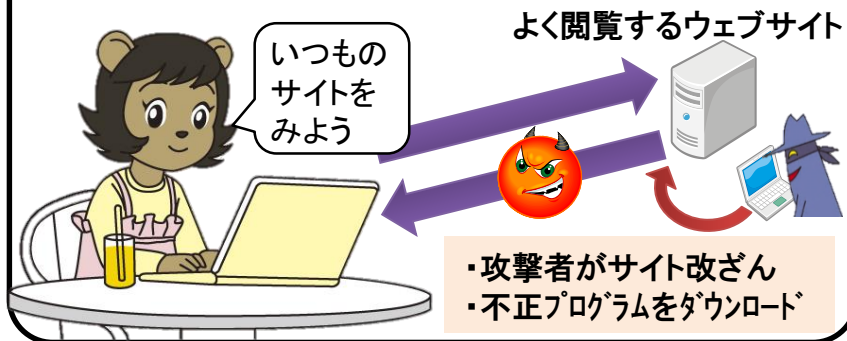
A. メール

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...



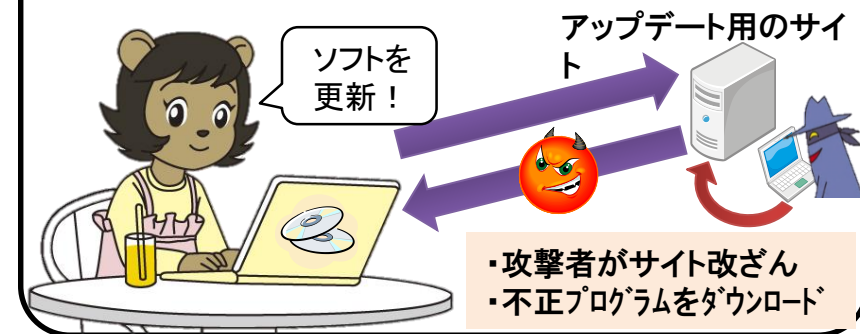
B. ウェブ閲覧（水飲み場型）

いつも閲覧しているウェブサイトへアクセスすると...



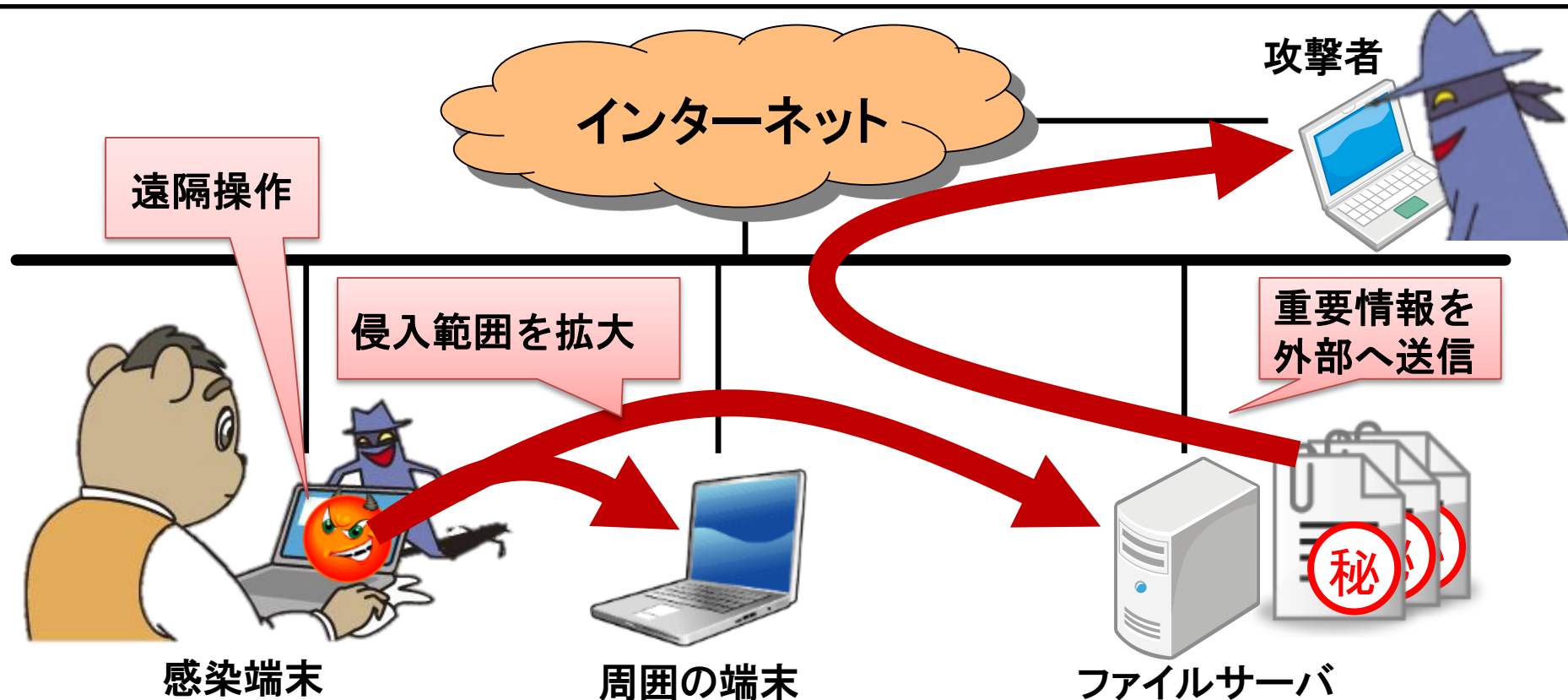
C. ソフトウェアアップデートを悪用

ソフトウェアのアップデート機能を使用すると...



標的型攻撃の攻撃プロセス

- 感染すると、攻撃者から遠隔操作される状態に
- 感染端末を拠点として、周囲の端末やサーバ等に対して侵入範囲を拡大
- 拡大の結果、重要情報にたどり着いた場合は、外部へ送信される
- 重要情報やシステムを破壊される可能性も



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。

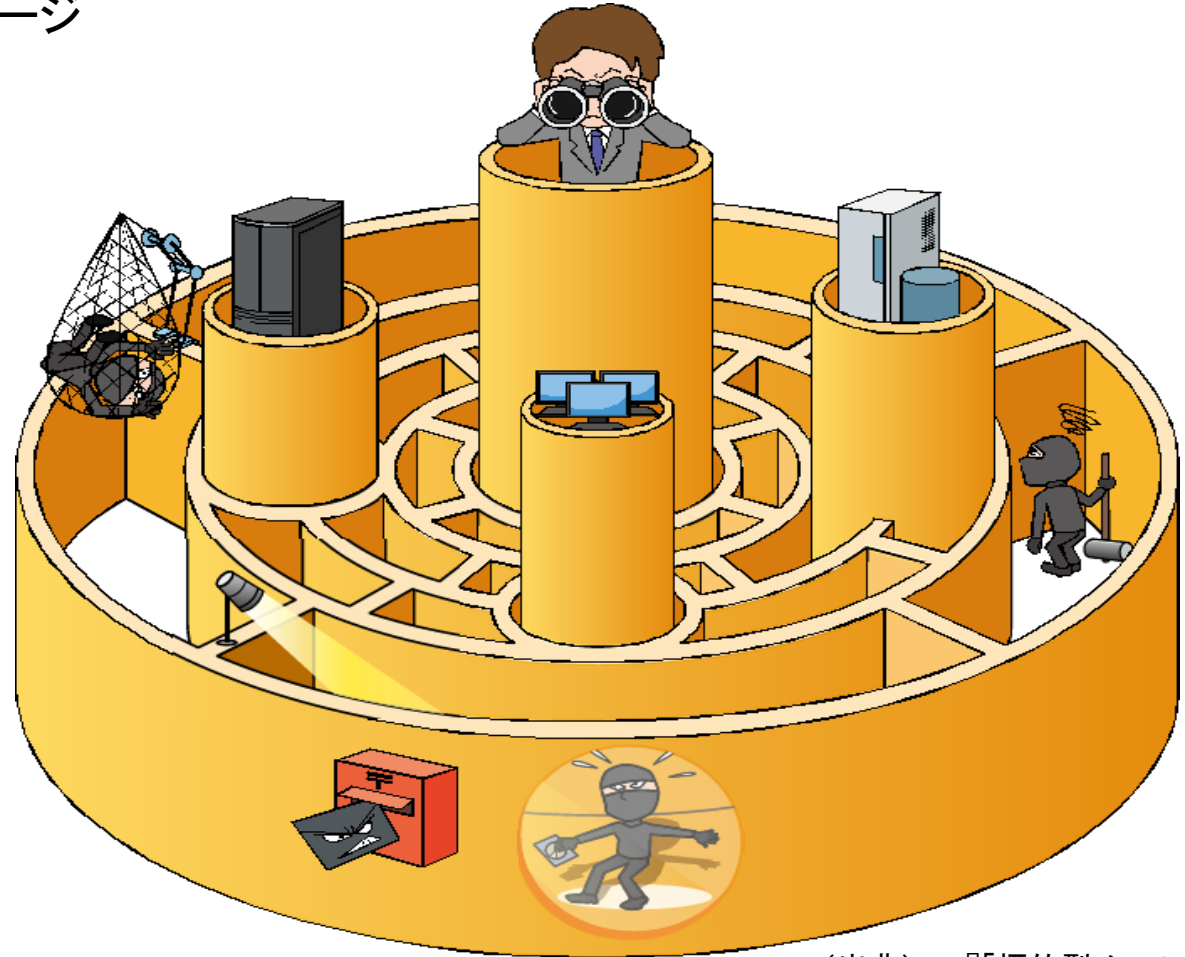
■ 多重防御を備えたシステムのイメージ

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』

年金機構事案：事案の状況と本部及びNISCの対応



● 5月8日(金)(検知・通知1)

- NISCは、厚生労働省(以下「厚労省」という。)ネットワークにおいて不審な通信を検知し、厚労省政策統括官付情報政策担当参事官室(以下「情参室」という。)に対してその旨を通知した。
- NISCは、厚労省情参室から不審な通信をした端末を特定し、LANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。(以降、厚労省情参室に対し、随時、助言等を実施。)

● 5月15日(金)(解析結果提供A)

- NISCは、厚労省情参室から5月8日に受信した不審メールⅠに関する不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月19日(火)(解析結果提供B)

- NISCは、厚労省情参室から5月18日に受信した2種類の不審メール(不審メールⅡ、不審メールⅢ)及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月21日(木)(解析結果提供C)

- NISCは、厚労省情参室から5月20日に受信した不審メールⅣ及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月22日(金)(検知・通知2)

- NISCは、厚労省ネットワークにおいて不審な通信を検知し、厚労省情参室に対してその旨通知した。
- NISCは、厚労省情参室から、機構において、不審な通信をした端末のLANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。

● 5月29日(金)

- NISCは、厚労省から、5月8日以降の経緯について5月19日に機構が警察へ相談したこと及び機構において情報流出が生じた旨の説明を受け、サイバーセキュリティ戦略本部長(官房長官)(以下「本部長」という。)に報告した。
- 本部長は、NISCから報告を受け、即時に「特定重大事象」^{注1}であるとの判断を行った。
- NISCは、厚労省の要請を受けて、厚労省と機構が行う対応を支援するため、CYMAT^{注2}を派遣した。

● 6月1日(月)

- NISCは、客観的・専門的立場から原因究明を実施するため、原因究明調査チームを設置した。
- 本部長は、サイバーセキュリティ基本法第30条第2項の規定に基づき、機構を監督する立場にある厚生労働大臣に対して、厚労省が機構に対して行ってきたサイバーセキュリティに関する監督に関する資料、情報の提供を要請した。
- 内閣官房副長官(事務)を議長とするサイバーセキュリティ対策推進会議を開催し、全府省庁に対して、システム点検と個人情報の適正管理を指示した。

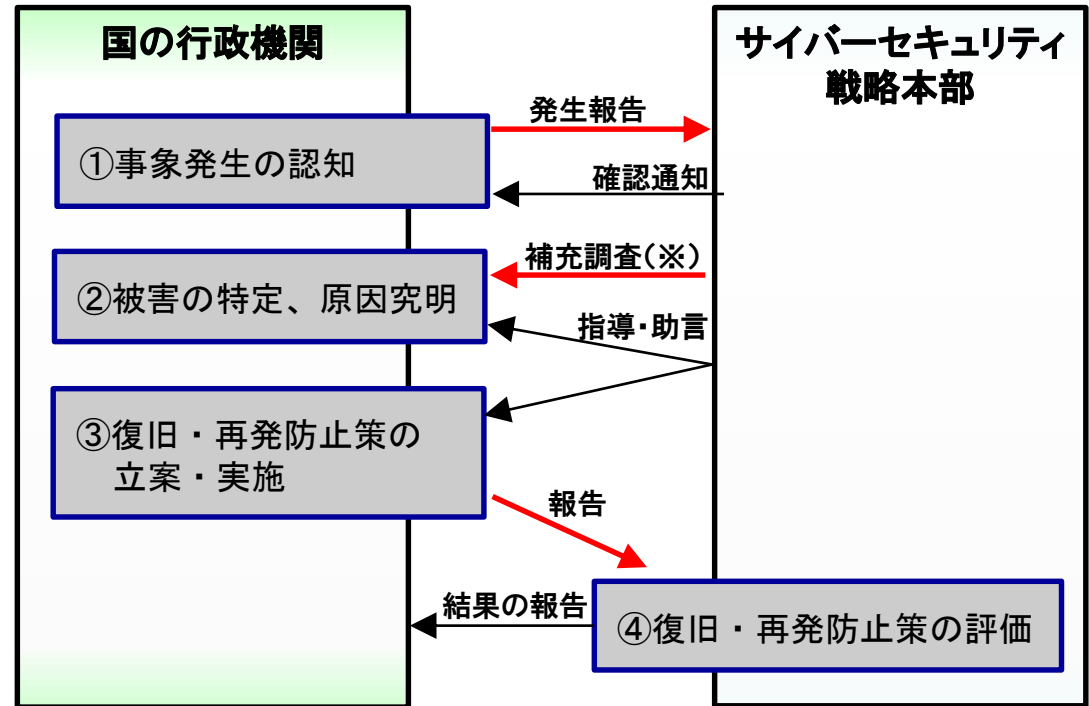
重大インシデントに係る原因究明等のプロセス

～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。

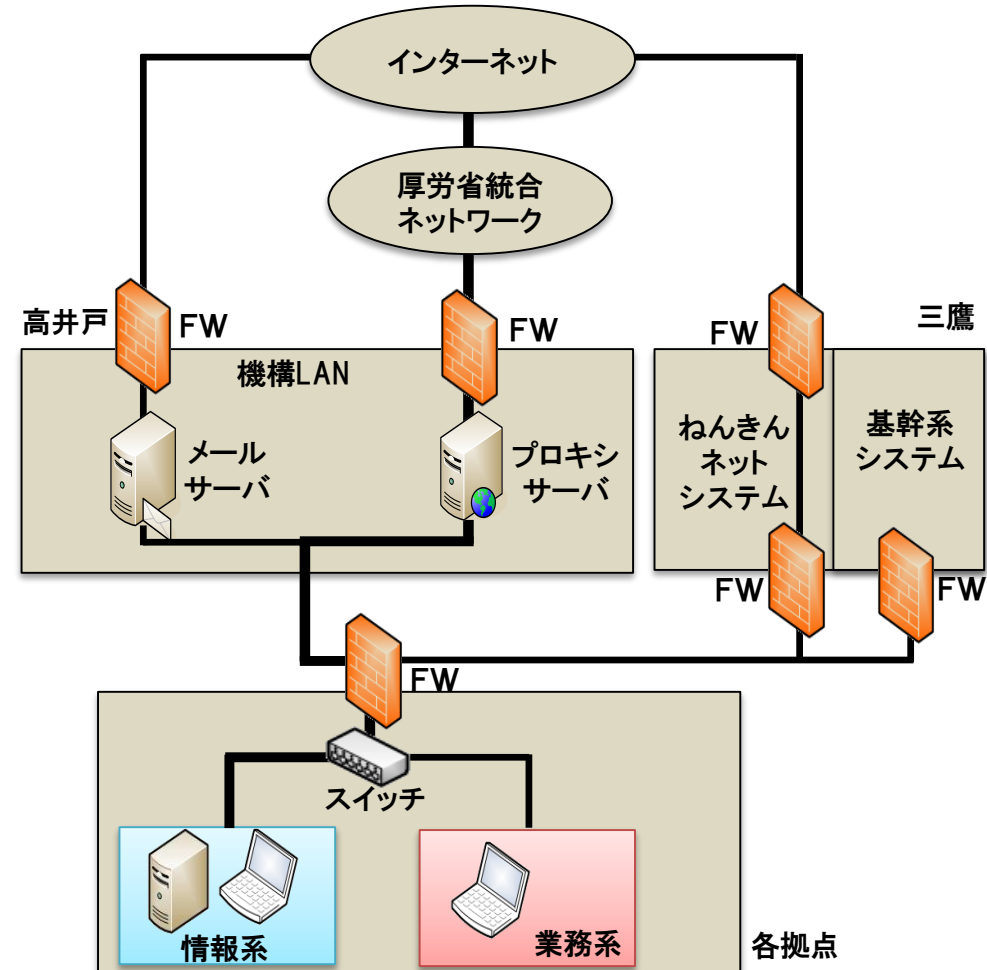
□ 原因究明調査により判明した事項①(ネットワーク構成の確認等)

- ◆ 機構のネットワークは、情報系からプロキシサーバを経由しての外部通信以外の外部通信が遮断される設定。したがって、攻撃者による外部との不審な通信については、プロキシサーバにその履歴が残る(プロキシログの解析結果は次頁参照)。

- ・ 業務系端末からの外部通信について
業務系端末から厚労省統合ネットワーク経由の外部通信は、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、NISC職員が説明どおりの設定となっていることを直接確認。

プロキシサーバに、業務系端末からの外部通信に関する履歴なし。

- ・ メール用回線等を通じた外部通信について
メール用回線及びねんきんネットシステム経由のWebアクセスは、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、NISC職員が説明どおりの設定となっていることを直接確認。



年金機構事案:事案に関する技術的検討(2/2)

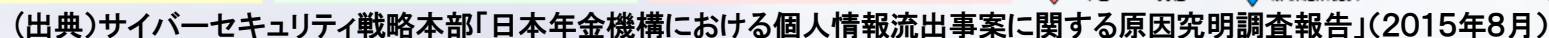
□ 原因究明調査により判明した事項②(プロキシログの解析、不審メールとの突合等)

- ◆ プロキシログの解析により、不審な通信先23件、不審な通信を行った端末31台を特定、不審メールと突合。

不審メールの番号	受信日	不審メールの概要	発生した不審な通信
I	5月8日(金)	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) リンク:商用オンラインストレージ	→ 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。
II	5月18日(月)	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) 添付ファイル:給付研究委員会オープンセミナーのご案内.lzh	→ 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。
III	5月18日(月) ~ 5月19日(火)	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) 添付ファイル:厚生年金徴収関係研修資料(150331厚生年金徴収支援G).lzh (16) リンク:商用オンラインストレージ(4)	→ 不審な通信は発生せず。
IV	5月20日(水)	件名:【医療費通知】 宛先:公開メールアドレス(3) 添付ファイル:医療費通知のお知らせ.lzh	→ 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。

- ◆ NISCでは、不審メールⅡ及び不審メールⅢに関する解析結果を5月19日夜に、不審メールⅣに関する解析結果を5月21日夕刻に、それぞれ厚労省情参室に提供しているが、これらの解析結果には不正プログラムの接続先に関する情報が含まれていた。
- ◆ 5月22日にNISCにおいて不審な通信を検知し厚労省に通知した後、機構による調査の過程で接続先Xへの多数の通信が判明した。

(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)



	NISC	厚労省	年金機構
インシデント 対処	● 政府統一基準^(注1)では、インシデントを認知したときに、CISO^(注2)やNISCに報告することを定めている。 ● 統一基準では、インシデント発生時に、CISOやNISC等への連絡のため、各府省庁において報告窓口を含む報告・対処手順を整備することとしている。	● 厚労省の情報セキュリティポリシーでは、インシデントを認知したときに、CISOやNISCに報告する旨定めている。 ● 厚労省は、報告・対処手順を整備しているが、今回のインシデントにおいて、GSOC^(注3)から連絡を受けた担当窓口から、厚労省の責任者(CISO、課長等の幹部)に報告が上がっていなかった。	● 機構のセキュリティポリシーにおいて、インシデント対処の必要性を規定し、その具体化はリスク管理一般の規程等に委ねている。 ● 当該規程において、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、サイバー攻撃を想定した具体的な対応が明確化されていない。
CSIRT ^(注4) 体制	● 政府統一基準では、CSIRTに属する職員については、「専門的な知識又は適性を有すると認められる者を選任すること」と定めている。 ● CSIRTに属する職員の選任は、各府省庁が統一基準の規定に従うこととされている。	● 厚労省のポリシーでは、CSIRTに属する職員について、「CISO、情報政策担当参事官、当該事案に係る部局の総括的な課長及び担当課室長等、CISOアドバイザを充てる」と定めている。 ● CSIRTの構成員が課室長等以上であり、実働要員(課長補佐以下の職員)が選任・指名されていなかった。	● 特殊法人である機構は、政府統一基準の直接の適用対象ではない。 ● CSIRT体制は定めておらず、セキュリティポリシーや諸規程にもその定めはない。(機構によると、平成27年7月10日からCSIRT体制の構築の検討を開始。)
個人情報を取り扱うシステムの整備等	● 「ガイドライン」^(注5)において、標的型攻撃に対する多重防御の取組は、外交・安全保障等に加え「個人にもたらされる被害」も対象としている。	● 厚労省統合ネットワークにおける標的型攻撃に対する多重防御の取組を進めていたが、機構の情報系ネットワークは、「ガイドライン」の取組の対象としておらず、標的型攻撃に対する多重防御の取組が十分でなかった。	● インターネットに接続していない業務系からインターネットに接続をしている情報系に個人情報を移して取り扱っていた。

(注1)「政府機関の情報セキュリティ対策のための統一基準」(平成26年5月 情報セキュリティ政策会議決定)

(注2) Chief Information Security Officer :最高情報セキュリティ責任者

(注3) 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

(注4) Computer Security Incident Response Team:コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織

(注5)「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成26年6月25日 情報セキュリティ対策推進会議)

(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)

□ 標的型攻撃の特徴

- ・ 標的型攻撃は巧妙化しており、使われるメールも見分けが困難。
→メール開封を前提とした対策が必要。
- ・ 攻撃者は乗っ取った端末を足掛かりとして、侵入を拡大させる。
→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

自組織の情報・システム・業務を守る目的・対策について考え、職務・職責に応じて実施することが求められる。

[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ようにアップデート等を行う。脆弱性診断を実施。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。
- 業務・情報の性質等に応じて重要な情報に攻撃が到達しないよう、システム分離。
- システム分離したときに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。等

◆ インシデント対策に係る対策

- 不審メールの受信(不正プログラム動作の可能性)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。

□ 各府省庁への情報提供が有効に機能するための対策

- ◆ NISCは、不審な通信検知後、速やかに分析を行い、インシデントの疑いのあるものは当該省庁に対して通知等を行っているが、通知や提供する不正プログラムの解析結果の重要性を当該省庁が理解し、迅速に適切な措置が取られることを前提としている。
- ◆ 今回の事案の教訓を踏まえれば、今後は、平素から各府省庁に対して、標的型攻撃を含むサイバー攻撃の本質と影響、NISCからの検知通知や不審メール等の解析結果の活用方法、対処方法等について研修や演習の機会を提供していく必要がある。
- ◆ 研修や演習の対象は、情報システム部局のみならず、独立行政法人、特殊法人等を所管する部局の幹部も対象として含めねばならない。本部は、その実施状況を年次報告等において評価し国民に説明していくことが重要である。

□ インシデントに備えた体制の強化

- ◆ 各府省庁においては、政府統一基準等に従って、CISOの指示の下、専門的な知識又は適正を有すると認められる者を選任したCSIRTを整備し、平素から要員の事案対処能力、経験の向上を図り、実践できるようにしておくことが求められている。
- ◆ NISCは、各府省庁のCSIRTが、事案発生時に実働する体制が整備・強化されるよう、事案の対応についての演習・訓練等の機会を設け、また、本部は、各府省庁において適切に体制整備がされ、実践のための必要な取組がなされているか等についても監査の対象とするなど、PDCAサイクルに基づく着実な取組を確保していく。
- ◆ 本部及びNISCは、政府統一基準等の見直しを行い、サイバーセキュリティ対策の向上を図る。

□ 標的型攻撃のリスクを踏まえたシステムの構築、維持、運用の強化対策

- ◆ 本部及びNISCは、標的型攻撃への対処について、政府統一基準の他、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を取りまとめ、その実施を推進してきたが、その適用範囲は、国の行政機関としている。
- ◆ 今後は、大量の個人情報を取り扱うリスクの高いシステムにおいても、サイバー攻撃のリスクを踏まえたシステムの構築、維持、運用がなされるよう、各府省庁に対し多重防御の取組を加速化すべく次のような取組を促すよう対策を講じていく。
 - リスクを考慮したシステム構築を行うための基準の改善（適用範囲の拡大を含む。）
 - システムの維持運用を確実にする監査の強化
 - 特に技術的な事項について、外部から起用するCIO補佐官、CISOアドバイザーの積極的な活用
- ◆ 併せて、GSOC機能について、攻撃の手法が時々刻々巧妙化していることを踏まえ、不断の見直しを行っていく必要がある。

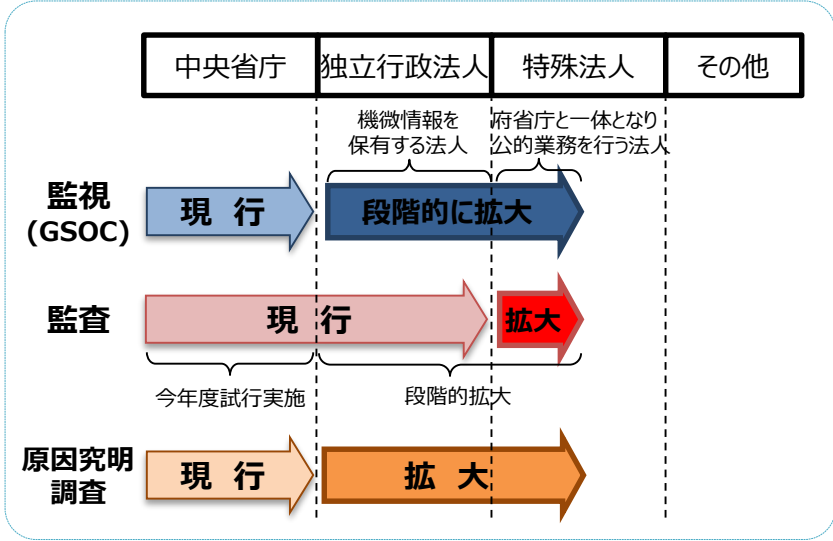
本文書は、NISCの対処能力を推知しうる情報が含まれるが、発生した事案の重大性に鑑み、可能な限り実態解明のための情報開示を行い、説明責任を果たす観点から取りまとめたものである。

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。

(注)「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に
盛り込み、積極的かつ総合的に推進する。

1. NISCの機能強化

- GSOCの大幅な機能強化
 - 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化
- 業務対象の拡大等
 - 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大（所要の法改正について速やかに検討）
- 連携推進体制の強化
 - 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携（所要の法改正について速やかに検討）
- NISCの要員強化
 - 高度セキュリティ人材の民間登用等による対処能力の一層の強化





2. 政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対応に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

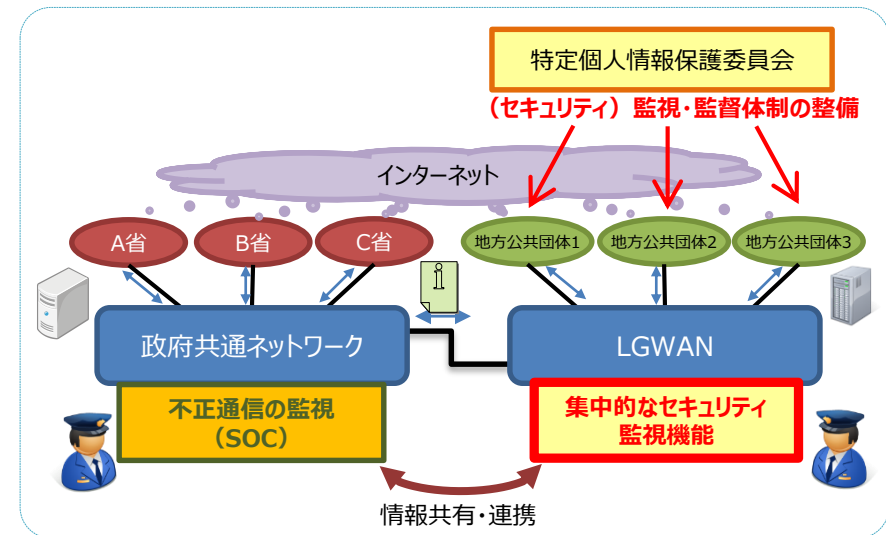
- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「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」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

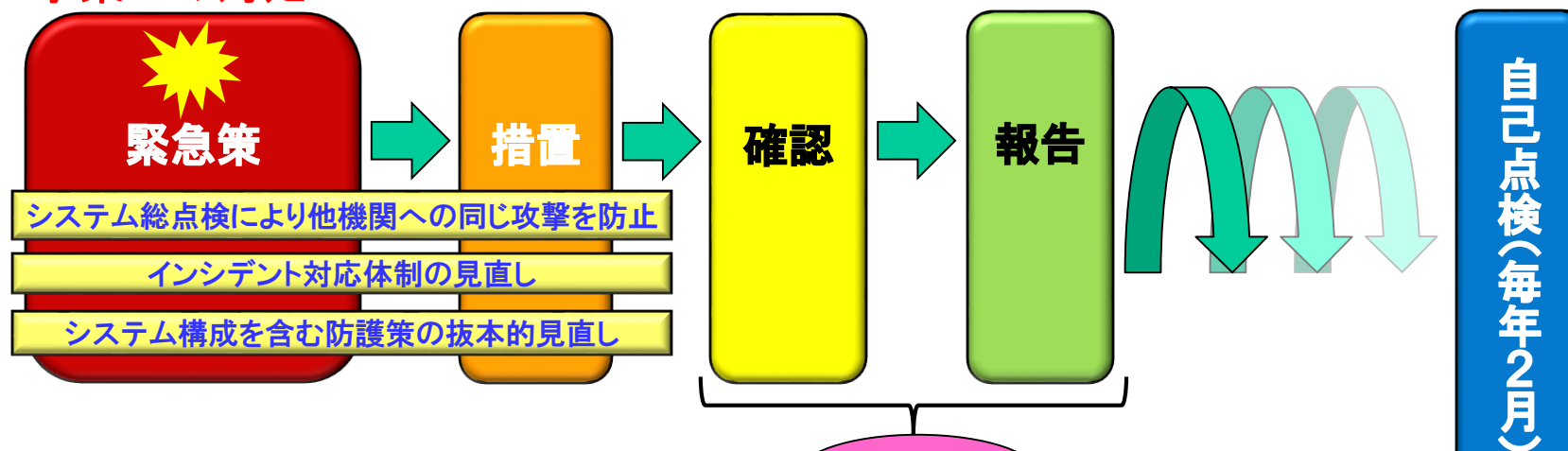
3. その他の重要課題への取組強化

- 重要インフラに関する取組強化（本年中を目途に具体策を決定）
 - ・ 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
 - ・ 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善
- 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）
 - ・ クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）
- 即応予備チームの体制整備
 - ・ 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備（法改正について速やかに検討）
- マイナンバー制度の円滑な導入に向けた対策の強化
 - ・ 特定個人情報保護委員会において、関係機関と連携して監視・監督体制を整備（本年度中を目途）
 - ・ 総合行政ネットワーク（LGWAN）について集中監視機能を設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知体制を整備
 - ・ 官民連携を実現する認証連携のための枠組みの取組方針を策定（本年中を目途）
- 事案対処に関する取組強化
 - ・ サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
 - ・ 対処機関における能力の質的・量的向上



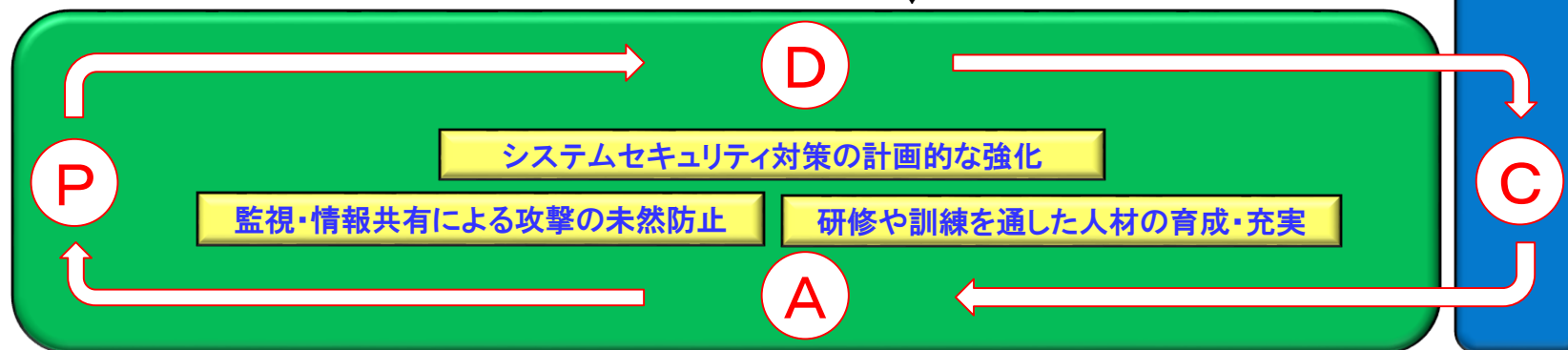
政府機関等における継続的なセキュリティ対策強化

事案への対処



課題

定常的な改善（攻撃の進化への対応）



NISCによる確認

監査によるポリシー遵守状況や体制の確認

ペネトレーションテストによるシステム防御の確認

各
年
度
の
年
次
報
告

新たな「サイバーセキュリティ戦略」について（全体構成）

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「**接続融合情報社会（連融情報社会）**」が到来同時に、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・発展させ、もって「**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**」に寄与する。

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**
安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

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**
事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

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・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的 施策

■ 研究開発の推進

攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ 人材の育成・確保

ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

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（総論）

1. サイバー空間に係る認識
2. 目的
3. 基本原則
4. 目的達成のための施策
経済社会 安全・安心 国際・安保
研究開発・人材育成
5. 推進体制

1. サイバー空間に係る認識 2. 目的 3. 基本原則

- 本戦略は、2020年オリンピック・パラリンピック東京大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示すもの。

1 サイバー空間に係る認識

- サイバー空間は「国境を意識することなく自由にアイデアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間で、経済社会の活動基盤である。
- 実空間のモノやヒトが、サイバー空間により物理的制約を超えて接続することで、実空間とサイバー空間の融合が高度に深化した「接続融合情報社会（連融情報社会）」が到来しつつある。
- 一方、国民生活・経済社会活動への重大な被害や我が国の安全保障に対するサイバー脅威も高まっている。今後、こうした脅威が更に深刻化することが予想される。

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「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」に寄与する。

本戦略の目的達成のための施策の立案及び実施に当たり、以下に示す基本原則に従う。

- ① 情報の自由な流通の確保：サイバー空間発展の基盤として、情報の自由な流通が保証された空間を維持
- ② 法の支配：実空間と同様にサイバー空間に対しても「ルールや規範」の適用を徹底
- ③ 開放性：常に参加を求める者に開かれ、新たな価値を生み出す空間として保持
- ④ 自律性：各者の主体的な行動により、悪意ある行動を抑止する自律的メカニズムを推進
- ⑤ 多様な主体の連携：様々な主体の適切な連携関係構築とダイナミックな対処策実現

我が国は、上記の5つの基本原則に従うとともに、国民の安全・権利の保障のため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として保持する。

新たな「サイバーセキュリティ戦略」について（各論①）

1. サイバー空間に係る認識
2. 目的
3. 基本原則
4. 目的達成のための施策
経済社会 安全・安心 国際・安保
研究開発・人材育成
5. 推進体制

4. 目的達成のための施策

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

IoTは成長戦略のkeyの1つ

○成長戦略進化のための今後の検討方針（平成27年1月29日産業競争力会議決定）

（略）「ロボット革命」の実現に加え、ビッグデータ、人工知能やモノのインターネット（IoT）等の急速な発展により生産・流通・販売、交通、健康・医療、公共サービス等の幅広い分野で想定される産業構造の変革に対応するため、今後のビジネスモデルの在り方を見据えた産業横断的な課題及び対応策の検討を進めるとともに、人材育成やセキュリティ対策、グローバル市場を念頭に置いた国際標準化対応などの環境整備を加速化する。

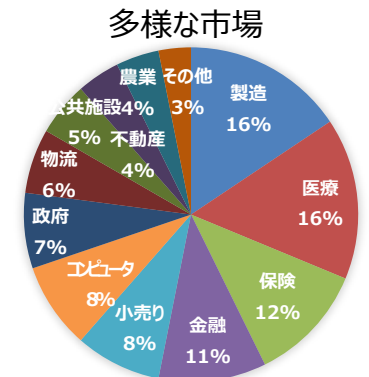
背景

- ハードウェアデバイスの進化
（センサー等の小型化・低価格化が進展）
 - 低廉・高速なインターネットの普及
 - ビッグデータ解析技術の進歩
- ↓
- あらゆるモノがネットワークでつながり、リアルタイムでのデータ化・自動制御が進展。あらゆる産業でデータの利活用、高度な判断サービスや自動制御が可能に。

市場規模・対象範囲の拡大

- 創出する経済価値：
1.9兆ドル（約228兆円）
- 全体のサービス投資：
2630億ドル（約32兆円）
- 対応製品は約250億台
（PC、スマートフォン、タブレット
以外の端末が過半数）

※ 数字は2020年時点の予測、1ドル = 120円で計算



Source: 全てGartner

諸外国も国家レベルで推進

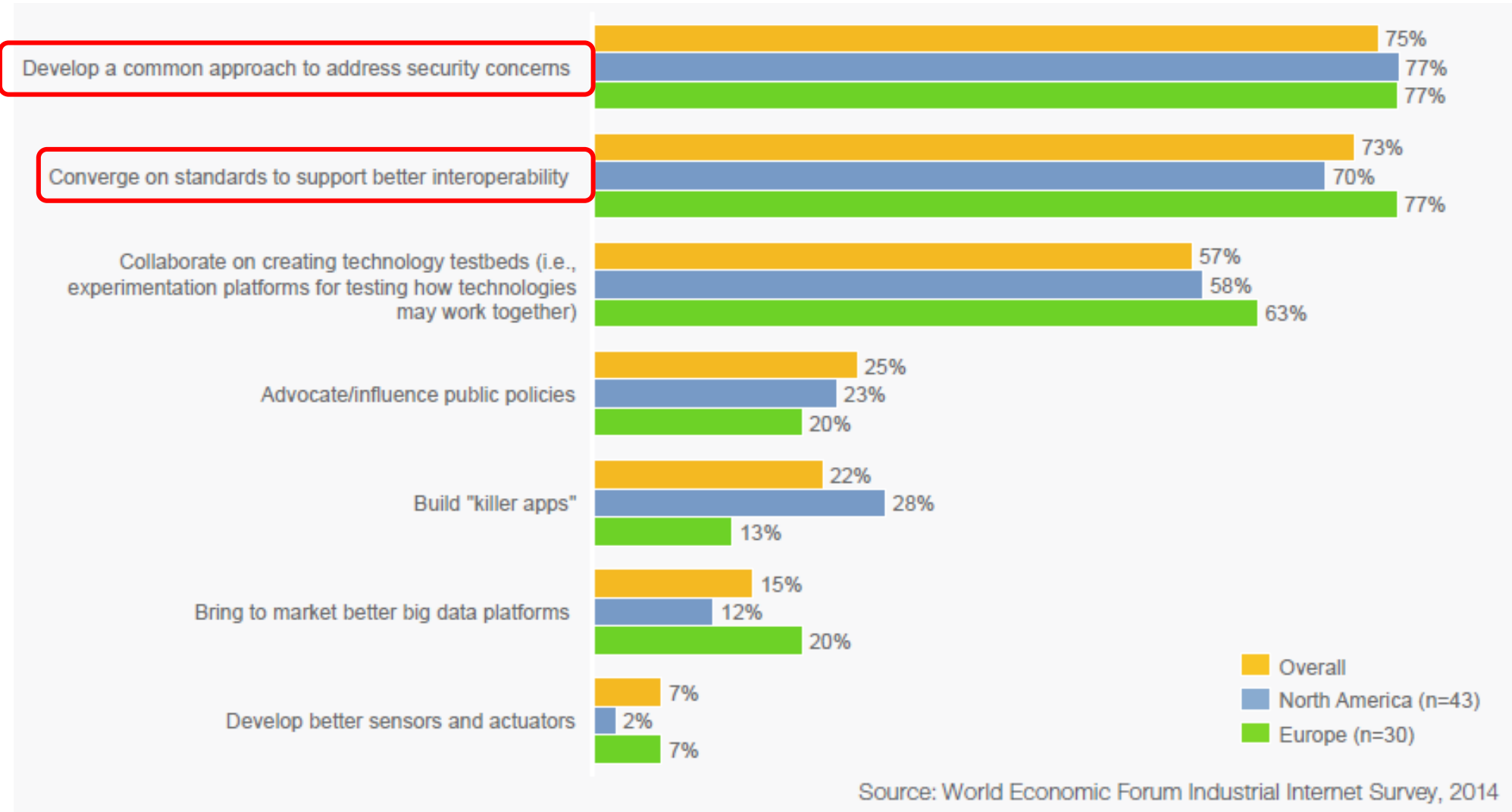


ドイツ政府は、2011年、独製造業の競争力強化のための構想“**Industry4.0**”を提示し、IoTによるさらなる効率化を国全体で強化。メルケル首相の強力なリーダーシップにより推進。



米国政府は、2012年、ビッグデータを活用し、国家の喫緊の課題解決を図るため“**BigData R&D Initiative**”を発表。民間では、GEが、「インダストリアル・インターネット」を提唱。60社以上でコンソーシアムを形成。

IoTの適用を加速させる重要なアクション ⇒ セキュリティと相互接続を促進する標準化が2大アクション



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

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

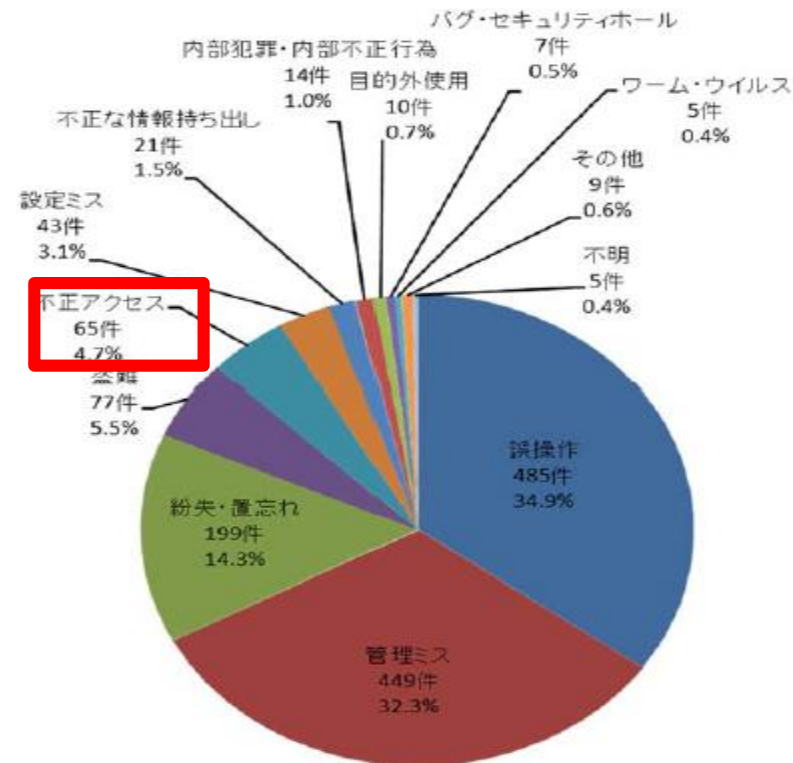
No.	漏えい人数	業種	原因
1	400万人	情報通信業	不正アクセス
2	169万2496人	情報通信業	不正アクセス
3	47万人	卸売業、小売業	不正アクセス
4	42万6000人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24万3266人	情報通信業	不正アクセス
6	17万5297人	情報通信業	設定ミス
7	15万0165人	卸売業、小売業	不正アクセス
8	12万0616人	金融業、保険業	管理ミス
9	10万9112人	情報通信業	不正アクセス
10	9万7438人	情報通信業	不正アクセス

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



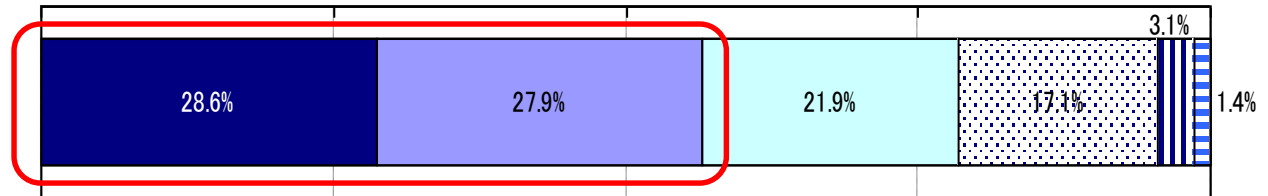
出典：2013年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～（日本ネットワークセキュリティ協会（JNSA））

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)

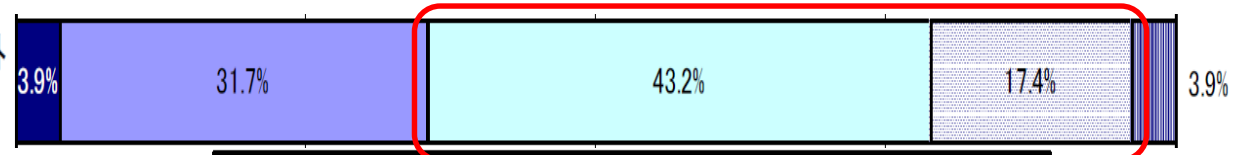


- 本業が忙しく、情報セキュリティにまで人材が割けない
- 経営層の理解や認識が足りない
- 社内に情報セキュリティ業務の適任者が少ない
- 分からない
- 採用をしたいが、情報セキュリティ業務への応募者が少ない
- その他

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
N=2,731



- 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

(経営層以外からの回答)

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)

- 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。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の14業種が100%(合計51社)。
- 繊維、パルプ・紙、鉄鋼等の4業種は0%(合計14社)。
- 素材産業全体(64社)では開示割合が32.8%と低く、原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低いと考えられる。
- サイバーセキュリティリスクの記載文書が5年間同一の企業(65社)には、その記載の仕方が包括的で意味が広く捉えられる(想定インシデント・被害が具体的でない)ものが多かった。
- 自社で発生したサイバーセキュリティインシデントを記載している企業は調査対象企業中4社と少なかった。

平成25年度 日経225社-業種別サイバーセキュリティ情報開示状況

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%	
		24 建設	8	4	50.0%	51.4%
E 資本 財・ その他	35	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		



- 米国企業のForm 10-Kに記載するリスク要因については連邦規則 (Regulation S-K Item 503 (c)) にて規定されており、どの企業にもあてはまるような一般的な記述ではなく、当該企業特有の内容について、具体的に分かり易く説明するよう要求されている。
- また、サイバーセキュリティリスク開示に関するガイダンスとしては、米国証券取引委員会(SEC) 企業財務局から2011年10月に発行された「CF Disclosure Guidance: Topic No. 2 Cybersecurity」(CFDG: Topic No.2)がある。同文書は、上場企業がサイバーセキュリティについて、自社特有の事実と状況を考慮しつつ、どのような場合に何を開示すべきかを判断する助けとなるガイダンスである。
- 上記に基づき、米国企業においては、サイバーセキュリティに関する自社特有の事実・状況に照らしたリスクや想定被害について詳しく開示している傾向があり、被害事例を開示する企業も見られる。
- なお、証券法は、詳細な開示によって当該企業がサイバーセキュリティ上の危険に晒されるような場合にまで開示を求めるものではないとしている。

- EUでは、現在、欧州議会において、データ保護指令の更新及び指令(Directive)から規則(Regulation)への昇格を目指した審議が行われている。

その中で審議継続中の「EUデータ保護規則案」の修正案に、上場企業のサイバーセキュリティリスク開示を求める内容も含まれている。



(修正案) 指令の詳述4に対する案

(4) ネットワーク及び情報セキュリティ(NIS)に関する情報交換や協同によるリスク回避、検知及び対応を実現するためには、協力のメカニズムは連合レベルで確立されるべきである。またメカニズムを効果的かつ包括的なものとするためには、全てのメンバー国が自国内において高いレベルのNISを実現できるような最低限の機能と戦略を有する必要がある、それはリスクマネジメント文化を推進し、最も重大なインシデントが確実に報告されるためにも、少なくとも情報インフラのしかるべき事業者にも適用されるべきである。株式市場上場企業において自主的にインシデントを財務報告書に公表するよう促進されるべきである。法的枠組みは、市民のプライバシーと完全性を保護する必要性に基づくべきである。CIWINIは本指令により事業者に拡大すべきである。

(修正案) 指令の14条第4節第1号に対する案

事業者は監督当局に報告することに加え、インシデントについて企業が自主的に財務報告書に公表することを奨励しなければならない。

理由：サイバーインシデントは、多大なる財務上の損失と多額の費用を必然的に伴う。株主や投資家は、これらの事件の結果について通知されるべきである。企業に対して、自発的にサイバーインシデントの公開を促すことにより、将来のインシデントの可能性やそのようなリスクの特質はもちろん、サイバーセキュリティ侵害を低減するためのリスク回避行動の妥当性等についての分野横断的な議論を促すこととなりうる。

新たな「サイバーセキュリティ戦略」について（各論②）

1. サイバー空間に係る認識
2. 目的
3. 基本原則
4. 目的達成のための施策
経済社会 安全・安心 国際・安保
研究開発・人材育成
5. 推進体制

4.目的達成のための施策

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

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

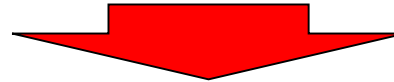
防護基盤の強化



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

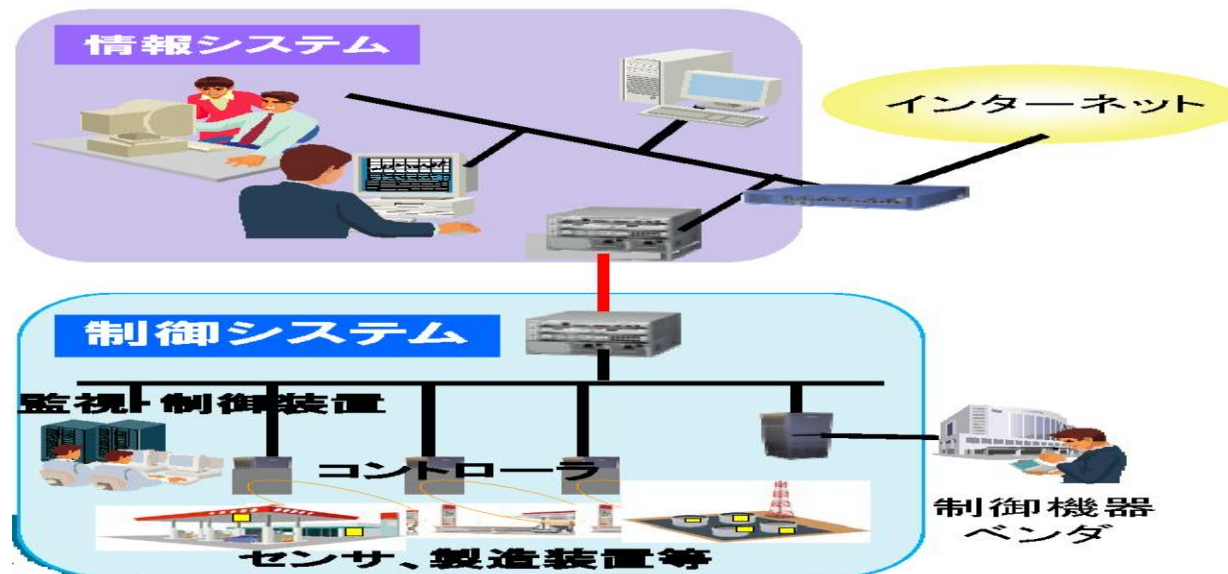
従来

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。



エネルギー部門におけるサイバーセキュリティ

- エネルギー配送システムに対するサイバー脅威は、ますます複雑で巧妙になってきている。
- エネルギーシステムは、所要のインフラやサービスを監視・コントロールする電子通信デバイスを通じ、エネルギーの生産、移動、配送を確実にするデジタルプロセスの基盤の上に構築されており、我々の経済のバックボーンとなっている。
- これらのシステムがエネルギーのバリューチェーンを越えて相互運用や相互接続を確保する必要性が、ますます増大しており、デジタルフレームワークやインフラをサポートすることが求められている。(para 9)

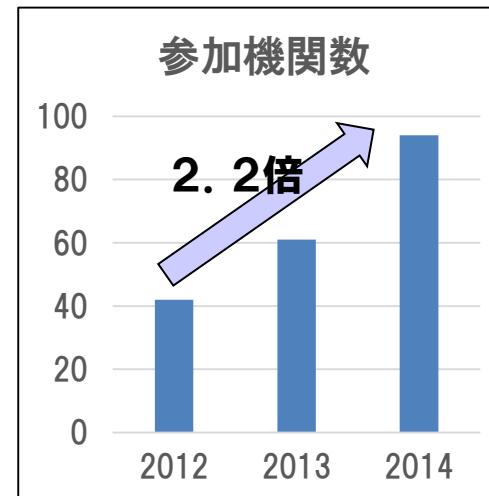
原則から行動へ：サステナブルなエネルギーセキュリティに向けたハンブルグイニシアティブ

- 我々はエネルギー部門のサイバーセキュリティを改善するために作業することをコミットする。
- この作業には、各国の異なるアプローチの分析、サイバー脅威や脆弱性を識別するための定義や方法論の交換、ベストプラクティス、サイバーセキュリティ対処能力や能力開発のための投資促進を含む。(para 16)

(Source) G7 Energy Ministerial in Hamburg Communique “G7 Hamburg Initiative for Sustainable Energy Security”(May 2015)

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

新たな「サイバーセキュリティ戦略」について（各論③）

1. サイバー空間に係る認識
2. 目的
3. 基本原則
4. 目的達成のための施策
経済社会 安全・安心 国際・安保
研究開発・人材育成
5. 推進体制

4. 目的達成のための施策

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

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)

➤ 会合の経緯・概要：

- 国連総会第一委員会が「政府専門家会合（GGE: the Group of Governmental Experts）」を設置し、国際的に新たな分野であるサイバー空間に係るグローバルなルールの在り方について議論することを決定（2001年10月）
- これまでに3会期（2004-05年、2009-10年、2012-13年）が開催され、現在は、第4会期（2014年7月-15年6月）を開催中
- 第3会期終了後、専門家会合の議論の結果を報告書として、国連総会に提出（2013年7月）。サイバー空間に国際法が適用されるとする一方で、個別具体的な国際法の参照は行わず、また必要に応じて新たな規範検討の可能性を残すことを記載。
- 第4会期のマンデートは、①現在及び潜在的な脅威、②国家の責任ある行動のための規範、ルール及び原則、③国際法の具体的適用、④信頼醸成措置の4点。

➤ **参加メンバー：**日本*、米国、英国、フランス、ドイツ、スペイン、エストニア、イスラエル、韓国、メキシコ、コロンビア、マレーシア、ケニア、ガーナ、エジプト、パキスタン、ロシア、中国、ベラルーシ及びブラジル（第4会期の議長国）の20か国

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(2015年3月)

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

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

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。

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）

1. サイバー空間に係る認識
2. 目的
3. 基本原則
4. 目的達成のための施策
経済社会 安全・安心 国際・安保
研究開発・人材育成
5. 推進体制

4. 目的達成のための施策

5. 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

■ 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



▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ



▲ 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。

- サイバーセキュリティ基本法（第25条第1項第4号）に基づき、今回初めて策定。
- サイバーセキュリティ戦略に基づき、3分野を重点分野として特定。
- 政府機関におけるサイバーセキュリティ関連予算については政府CIOと随時連携。

①IoTセキュリティの確保等

- 関係府省及び産学官の連携が基本
- 実証実験については成果の社会的還元
の道筋等を明確化
- IT利活用施策についてはセキュリティバイ
デザインの考え方を前提

③横断的施策

- 人材育成
 - ・関係府省の役割分担を明確化しつつ共
通的基盤作りを推進（産学官連携が前
提条件）
- 研究開発
 - ・「戦略的イノベーション創造プログラム
（SIP）」の枠組み等による推進等

サイバーセキュリティ戦略

1 サイバー空間に係る認識

2 目的

3 基本原則

4 目的達成のための施策

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

研究開発の推進、人材の育成・確保

5 推進体制

②政府機関対策の強化

- 政府機関の防御能力の強化（各府省）
 - ・統一基準に基づくリスク評価及び多重防御対
策を計画的に推進
 - ・重要情報を取り扱う情報システムのインターネッ
ト等からの分離、インターネット接続口の早急な
集約化等を計画的な推進
 - ・事案解明や対処のための予算を確保
 - ・攻撃前提の情報システムの防御力の強化
- GSOCシステムの検知・解析能力の強化、監視・
監査・原因究明に係る対象範囲の拡大への適切
な対応（内閣官房）
- マイナンバー制度に係るセキュリティ対策への適切
な対応（関係府省の重複を排除）

（注）所要の施策に追加的に必要な経費等については、業務・システム改革そ
他の施策の見直しによる行政の効率化等によって節減した費用等を振り向け
る。



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**