NISC

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１１月２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

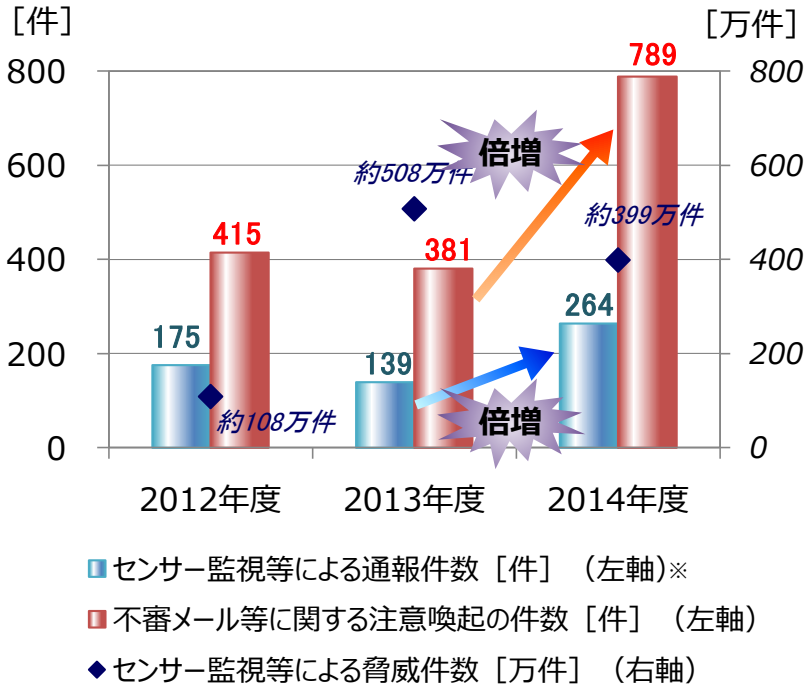
http://www.nisc.go.jp/

リスクの深刻化

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）

リスクの拡散

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

リスクのグローバル化

～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「Cybercalophate」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。

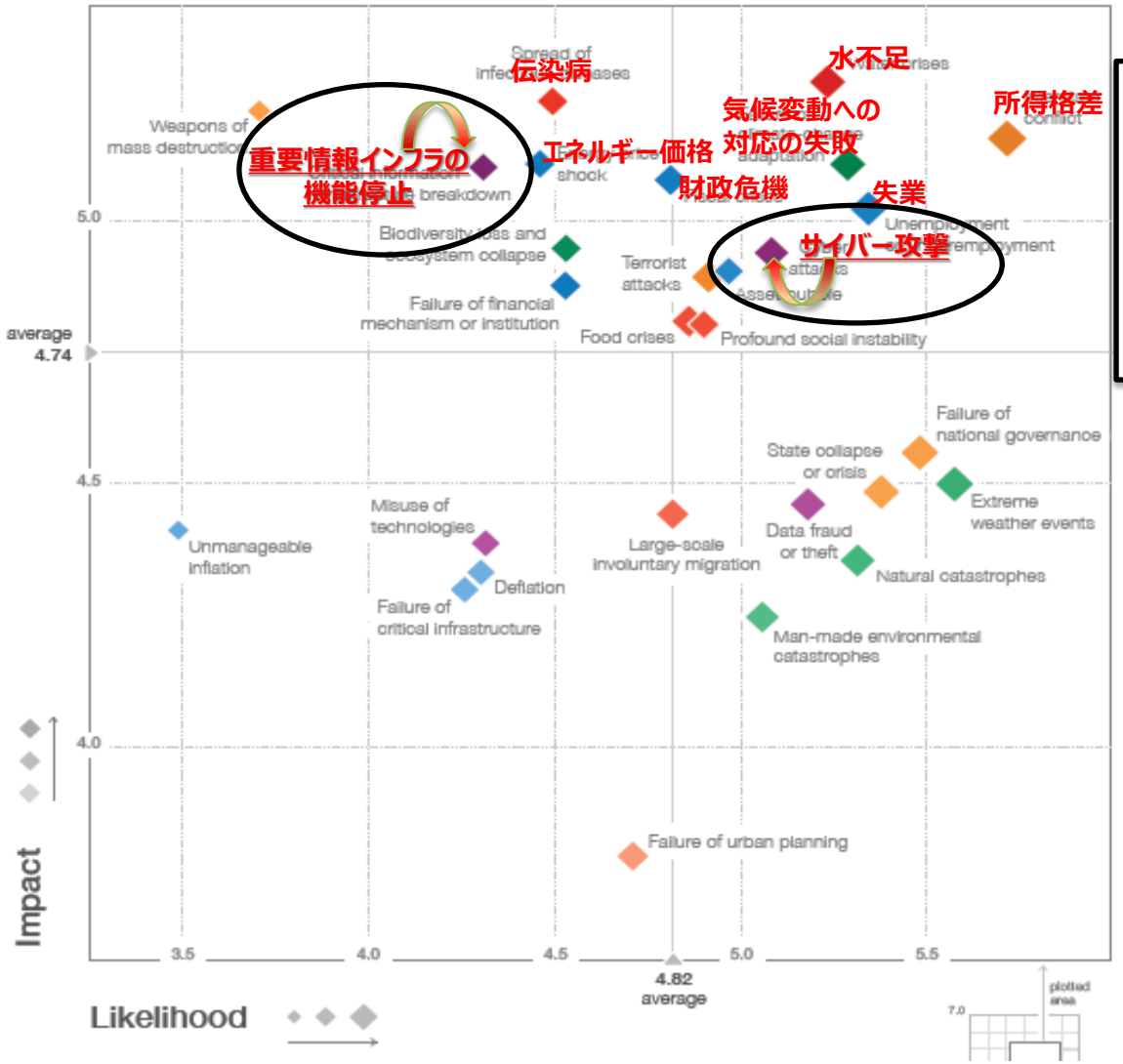
○ イラン核問題6か国協議会場（2015年5月中旬）

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 。

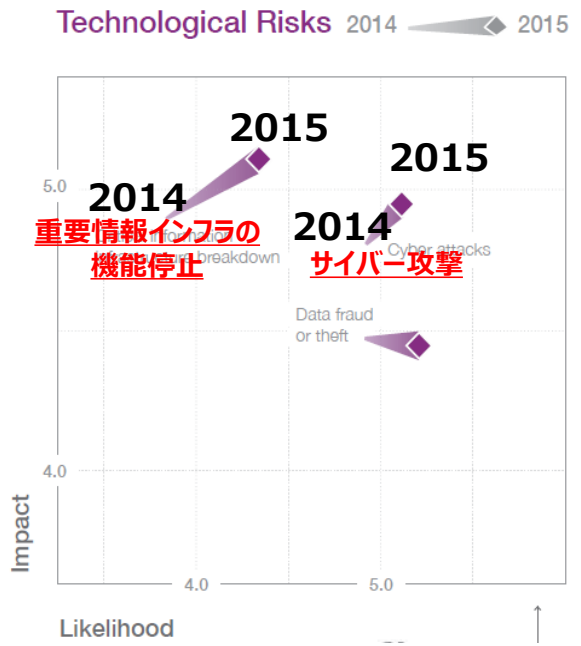
○ 米国人事管理局（2015年6月上旬）

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た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。"



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）

NISC

	施行前		施行後
政府の推進体制	内閣 IT戦略本部（本部長：総理大臣） NSC（議長：総理大臣） 情報セキュリティ政策会議 ← IT本部長決定 情報セキュリティセンター ← 総理大臣決定	法律・政令で設置根拠を明確化	内閣 IT戦略本部 ↔ 緊密連携 ↔ NSC サイバーセキュリティ戦略本部（本部長：内閣官房長官） 内閣サイバーセキュリティセンター(NISC) 基本法 政令(官房組織令)
各省への権限	各省との合意に基づく取組 ・各府省等による自主的な監査 ・事案発生時、必要に応じ、解析等の協力を実施	権限強化	サイバーセキュリティ基本法に根拠を持つ権限 ・政府機関への第三者(本部・NISC)による監査 ※ ※ マネジメント監査とシステムへの擬似的攻撃を実施 ・重大な事案発生時における原因究明調査 ※※ ・政府機関からの資料等提出義務、本部長による勧告権 ※※
基本戦略	「サイバーセキュリティ戦略」 （平成25年６月情報セキュリティ政策会議決定）	格上げ	基本法に基づく新たな「サイバーセキュリティ戦略」 （IT戦略本部・NSCへ意見聴取の上、平成２７年９月、閣議決定・国会報告）

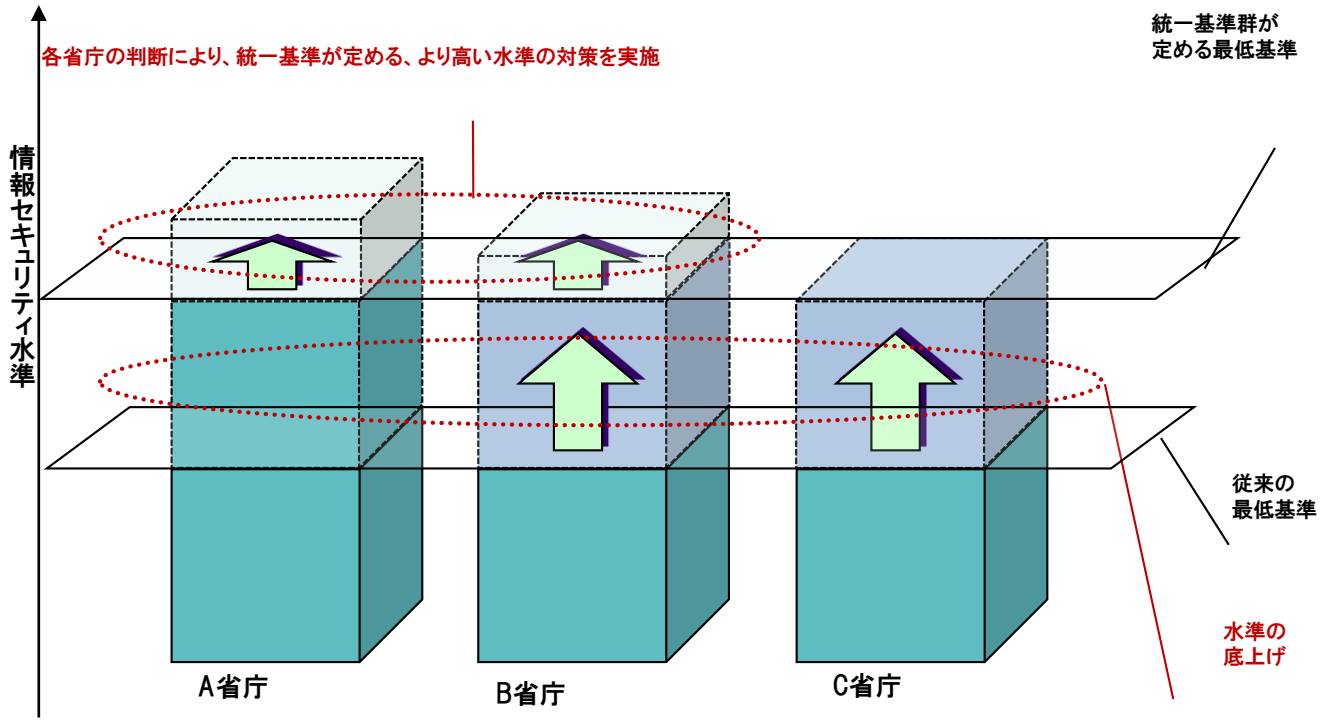
統一基準群（政府機関セキュリティポリシーのベースライン）

○政府機関が実施すべき対策の統一的な枠組みを構築

○政府機関全体の情報セキュリティ水準の底上げに寄与

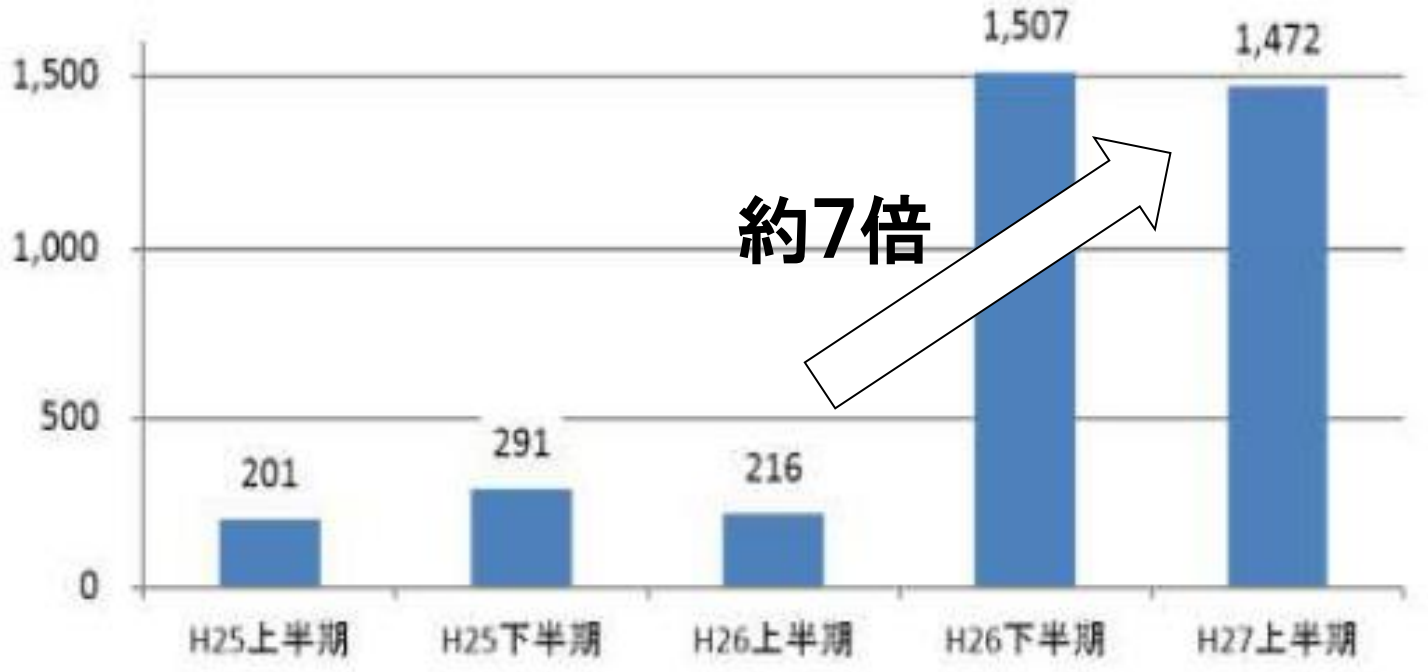
○標的型攻撃対策に力点。

＜統一基準群の効果（イメージ）＞



増加する標的型メール攻撃

○非公開メールアドレスに対する攻撃が全体の約９割。
○多くの攻撃において送信元メールアドレスを詐称（攻撃対象の事業者等や実在する事業者等のメールアドレス）
○ばらまき型の攻撃が大半。



【警察が把握した標的型メール攻撃の件数】

（出典）警察庁「平成27年上半期のサイバー空間をめぐる脅威の情勢について」（2015年9月）

標的型メールの特徴

①差　出　人：情報 太郎 [johou.taro@cas-go.jp]

　宛　　先：二鋤 次郎

②件　　名：【重要】放射線量の状況

③添付ファイル：放射線量.zip

④関係各位

　いつもお世話になっております。内閣官房の〇〇〇〇です。現在の放射線量についてまとめました。添付を確認ください。
　また、添付ファイルと併せて、以下のURLもご確認ください

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

クリックすると

http://10.243.23.11/詐欺/

①差出人のアドレスを確認

@より右側が省庁ドメイン（.go.jp）でない

②件名で開封を急がせる

「重要」「緊急」などを付加

③添付ファイルの確認

アイコンを文書のように偽装

・.exe等はウィルスの可能性

放射線量.doc.exe

④メール本文は本物のコピー

・発信者に送信したかを確認

⑤リンク先表示

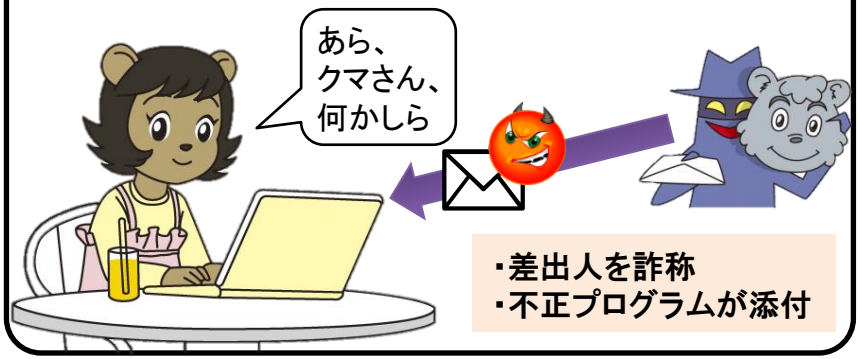
全く別のアドレスに偽装可能

様々な標的型攻撃

〇標的型攻撃は、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
〇初期潜入段階において、端末を不正プログラムに感染させるために種々の手口が使われている

A. メール

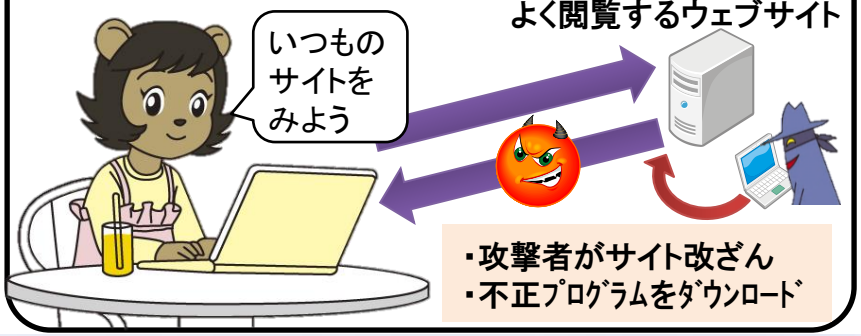
よく知っている人からのメールだと思って添付ファイルを開いてしまうと・・・



・差出人を詐称
・不正プログラムが添付

B. ウェブ閲覧（水飲み場型）

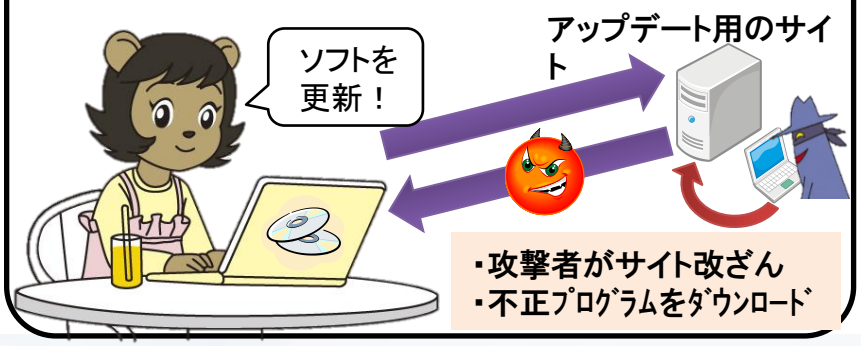
いつも閲覧しているウェブサイトにアクセスすると・・・



・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

C. ソフトウェアアップデートを悪用

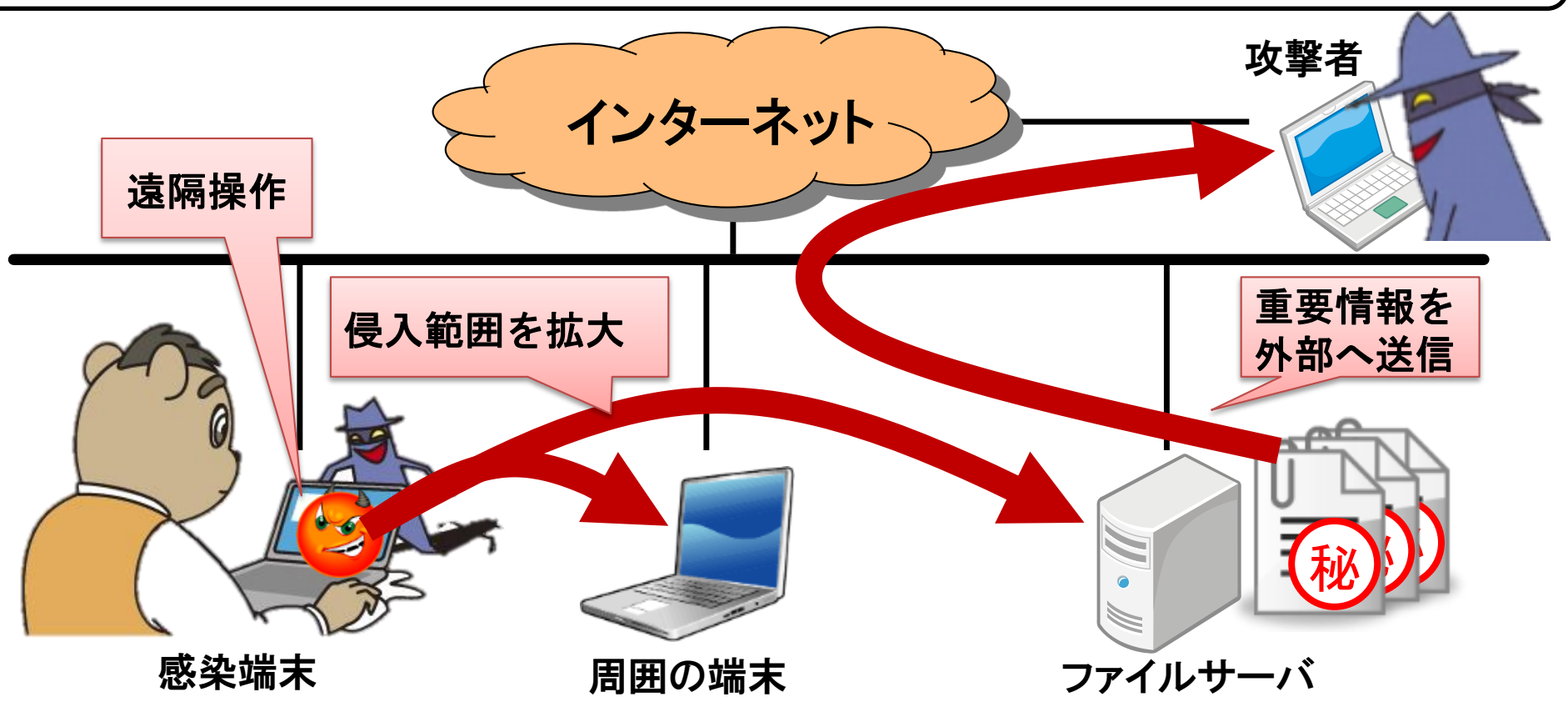
ソフトウェアのアップデート機能を使用すると・・・



・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

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

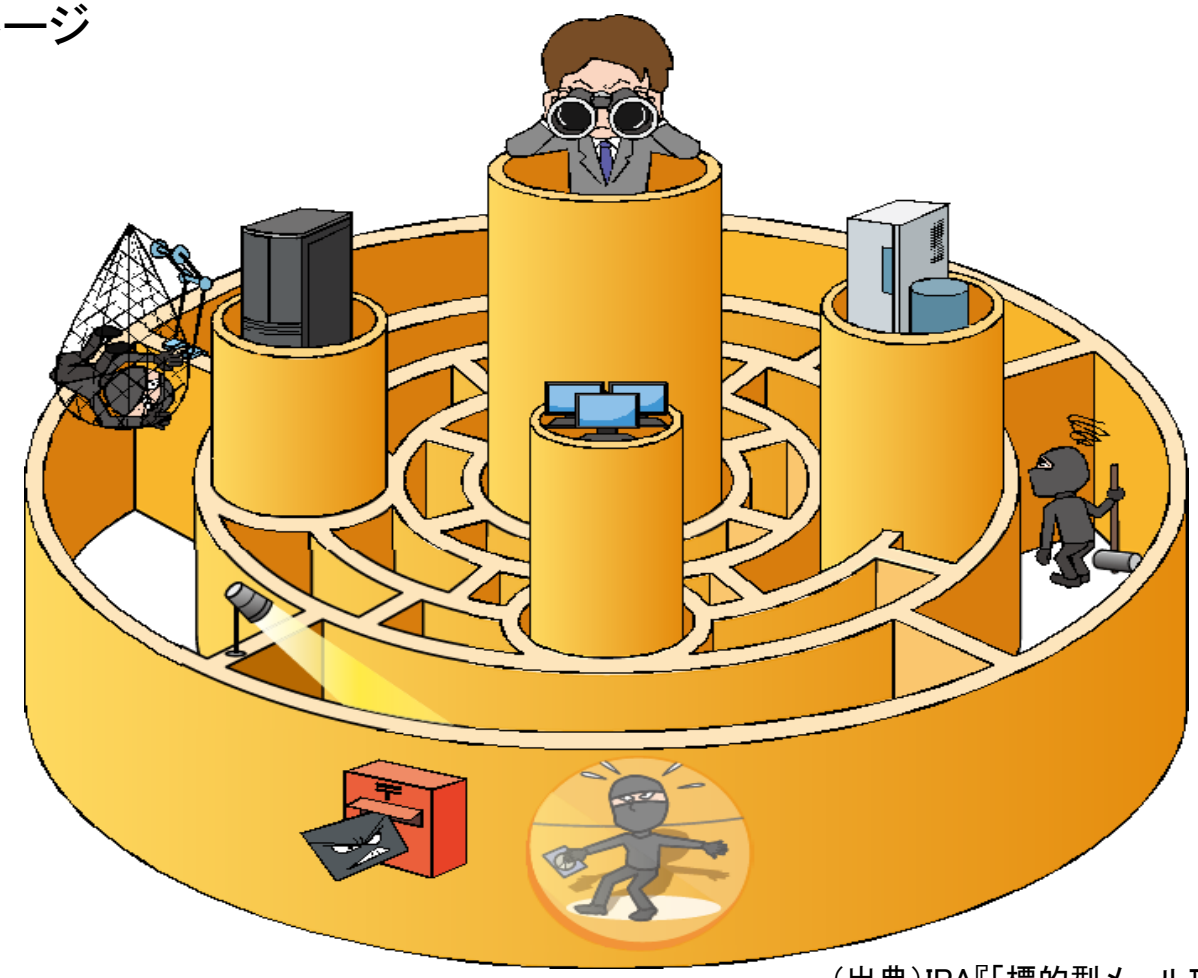
○ 侵入を100%防ぎ続けることは困難。侵入されても被害を抑える対策実施が重要。
○ 単独の対策に頼らない多重防御を備えたシステム構築が重要。

■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拡げにくくする

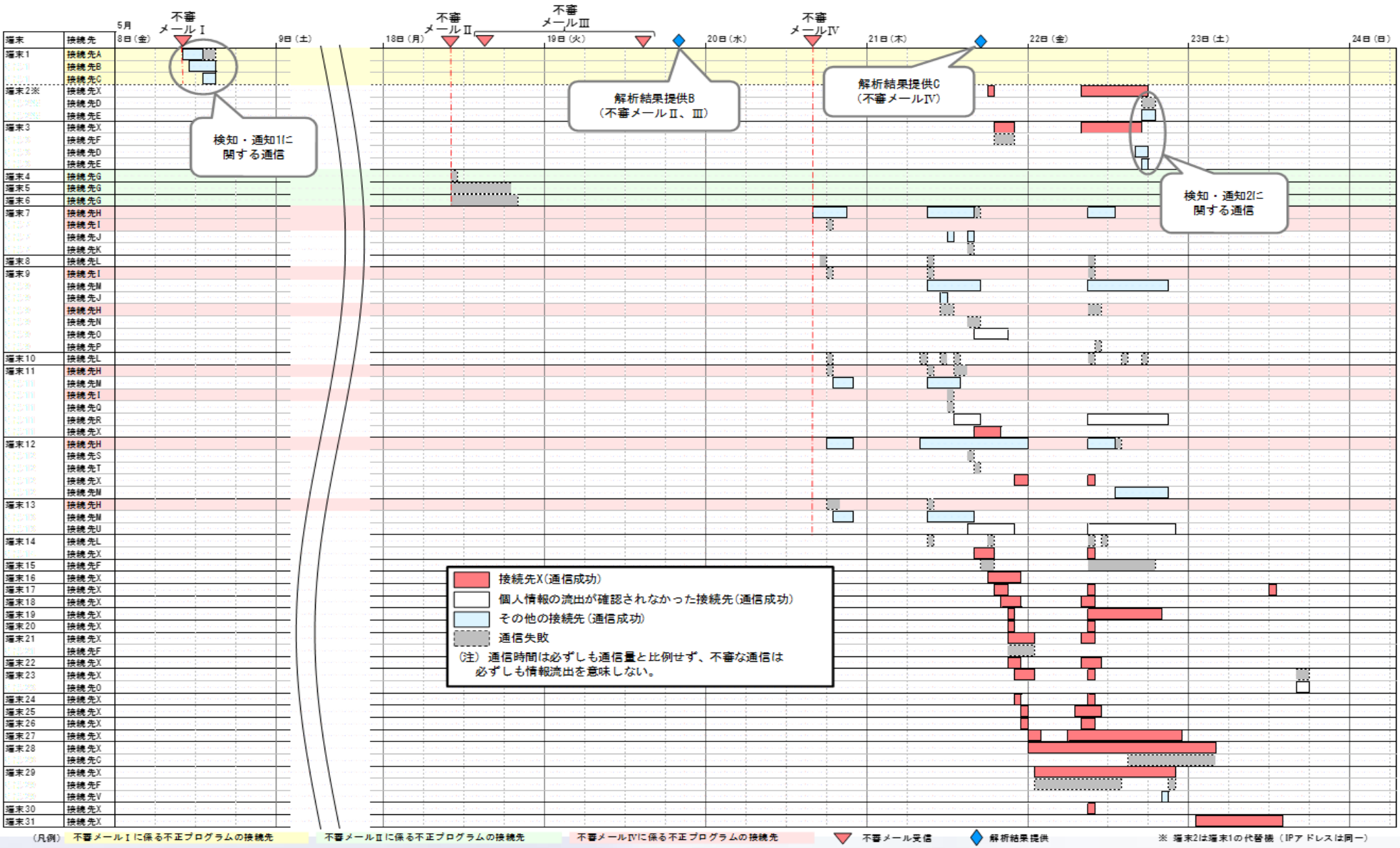
侵入されていないか見張る



パスワードだけでは
盗まれます！

（出典）IPA『「標的型メール攻撃」対策に向けたシステム設計ガイド』

年金機構事案：感染端末と不審な通信



（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）

年金機構事案：CSIRTの運用等に関する検討

	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)

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（1/3）

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。

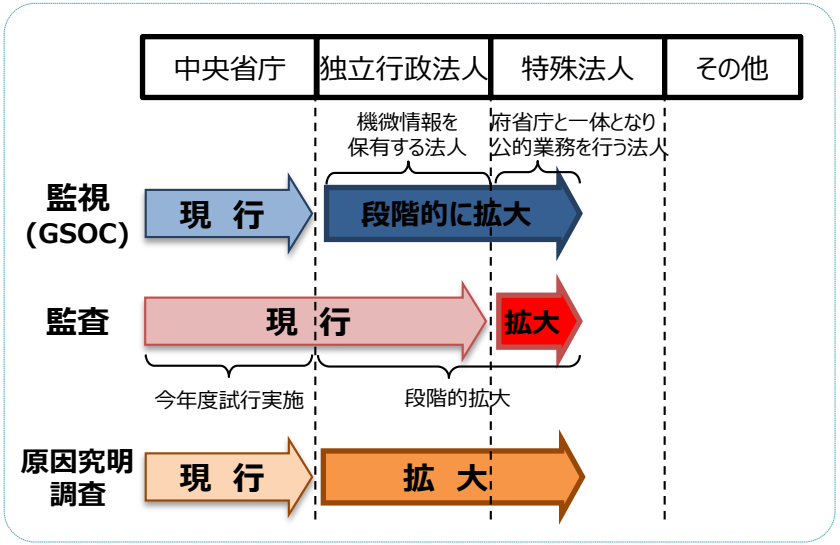
1．NISCの機能強化

■ 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

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（2/3）

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
- 初動対処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）

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(3/3)

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）

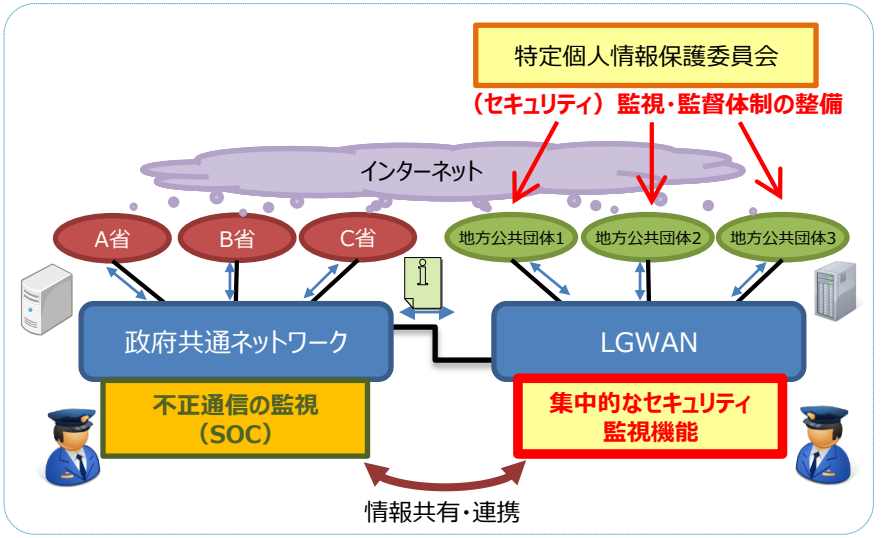
- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 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

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連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（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（各論①）

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

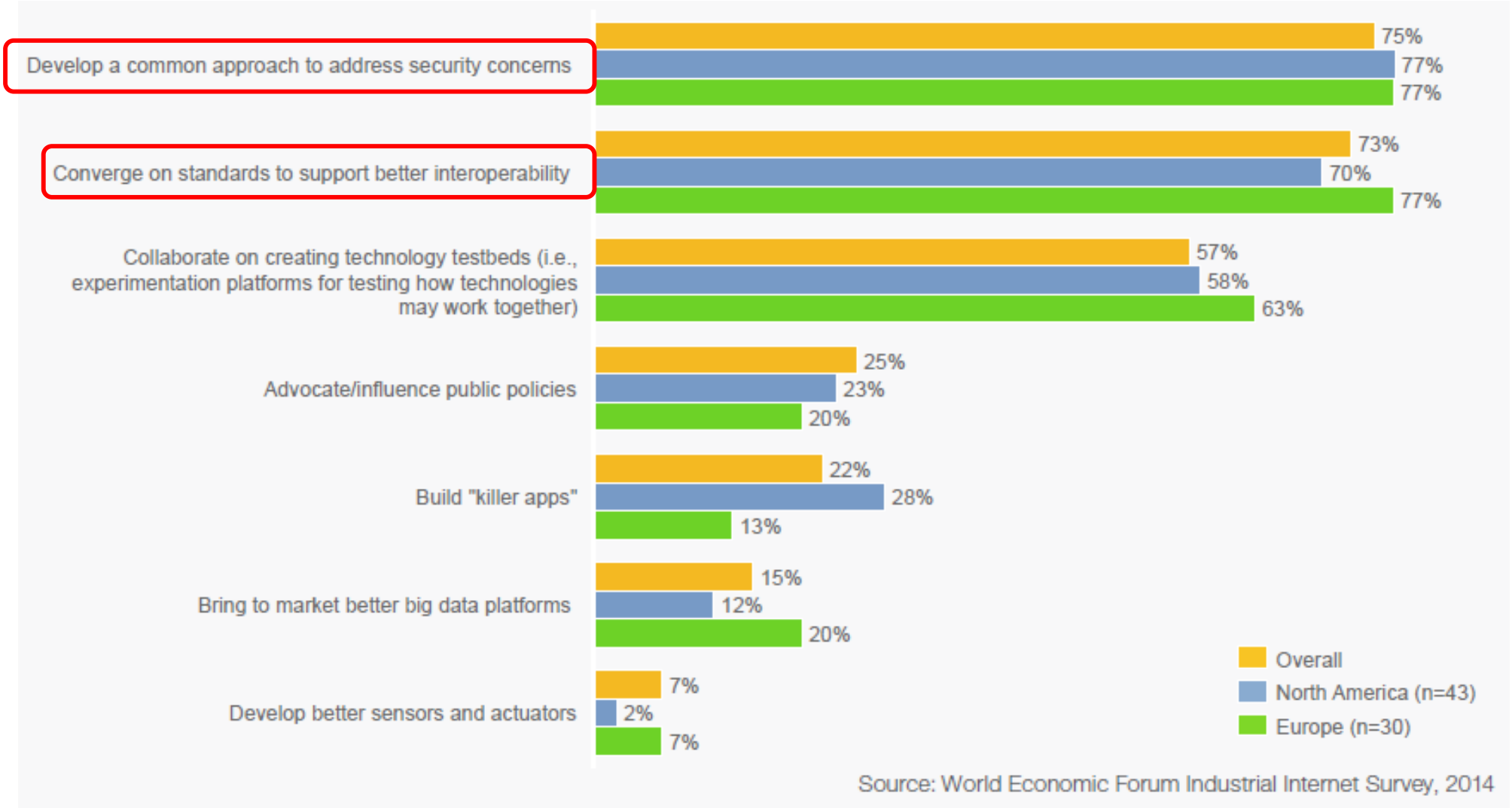
■セキュリティに係るビジネス環境の整備

- 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

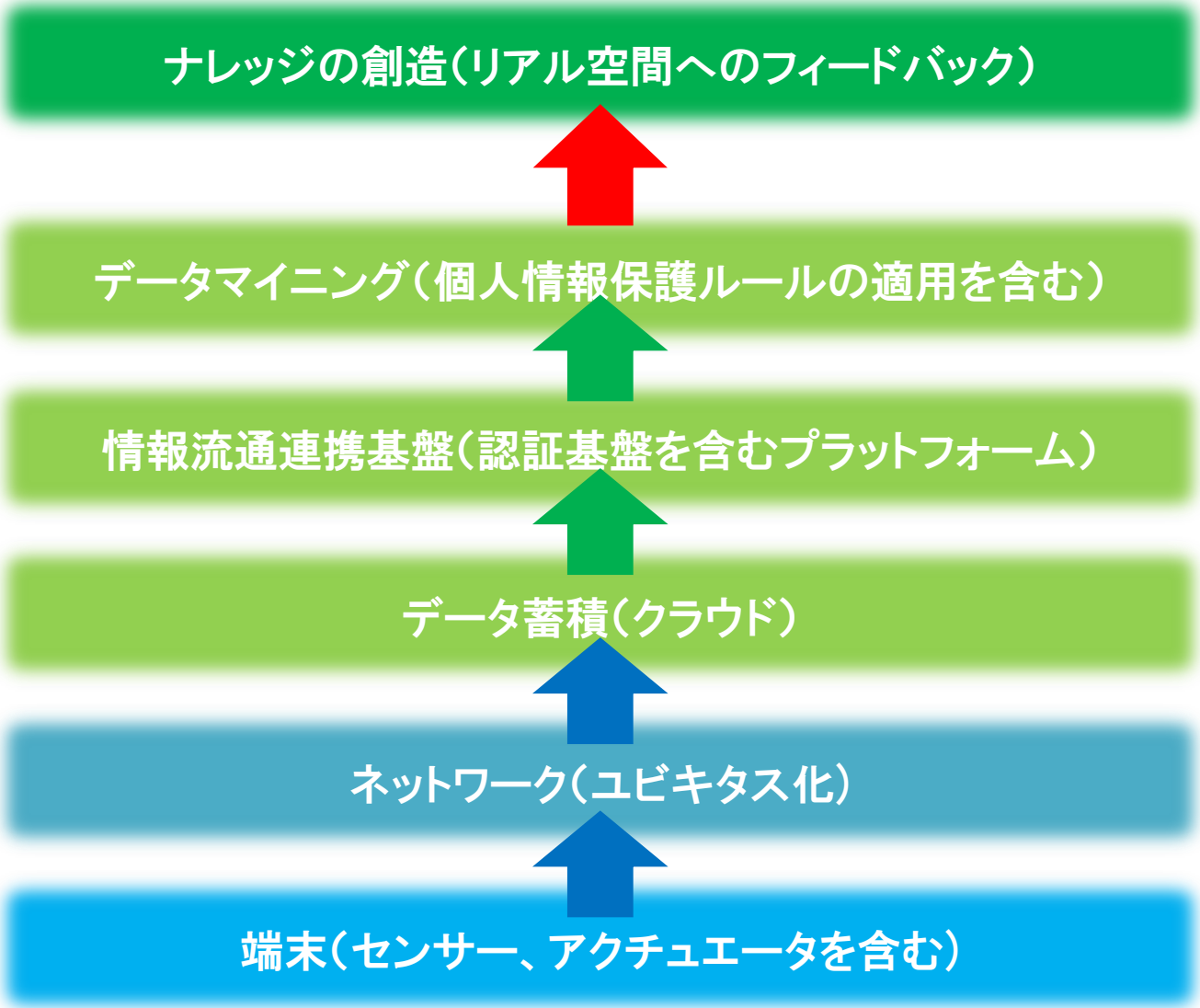
▲自動運転車の実証実験

IoT促進のカギとなるセキュリティ

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



IoTセキュリティに関する検討事項（例）



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

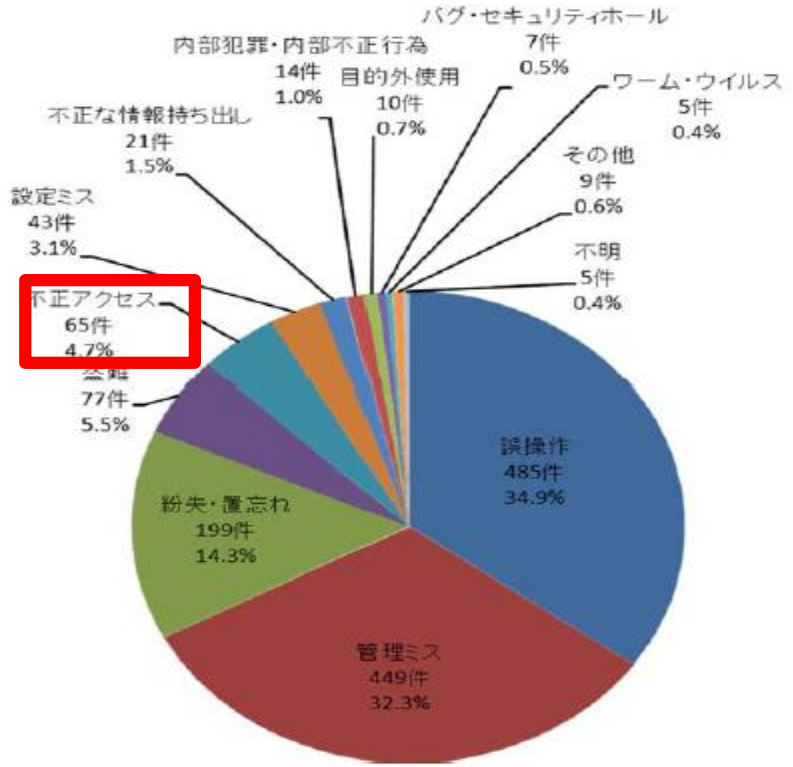
情報通信業が多い

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。

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%	
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）

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

重要インフラの情報セキュリティ対策に係る第３次行動計画

（2014年5月、情報セキュリティ政策会議決定）

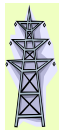
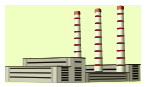
官民連携による重要インフラ防護の推進

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

重要インフラ（13分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



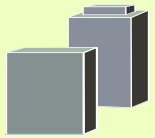



NISCによる調整・連携

重要インフラ所管省庁（5省庁）

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

関係機関等



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

重要インフラの情報セキュリティに係る第３次行動計画

安全基準等の整備・浸透

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

情報共有体制の強化

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

障害対応体制の強化

官民が連携して行う演習等の実施・演習・訓練間の連携によるIT障害対応体制の総合的な強化

リスクマネジメント

重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援

防護基盤の強化

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

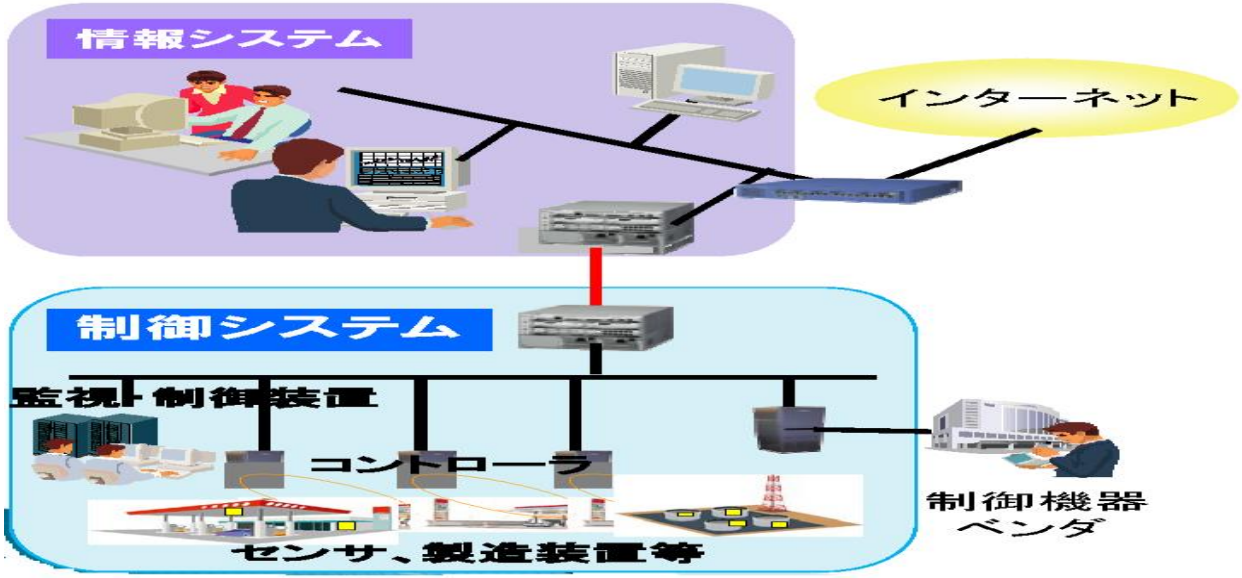
制御システムの汎用化の進展

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。



G７エネルギー相会合コミュニケ(15年5月、ハンブルグ)

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：サステイ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。*(para16)*

(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

演習の模様

意見交換会の模様

新たな「サイバーセキュリティ戦略」について（各論③）

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

国家安全保障戦略（13年１２月閣議決定）

Ⅲ　我が国を取り巻く安全保障環境と国家安全保障上の課題

１　グローバルな安全保障環境と課題

（4）国際公共財（グローバル・コモンズ）に関するリスク

近年、海洋、宇宙空間、**サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化**している。

（中　　略）

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

一方、**国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化**しつつある。

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

サイバー空間と国際法の適用関係（GGE, June 2013）

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

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

サイバー空間と国際法の適用関係(GGE, June 2015)

"In their use of ICTs, ***States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful measures, and non-intervention in the internal affairs of States****."*

*"****Existing obligations under international law are applicable to State use of ICTs*** *and States must comply with their obligations to respect and protect human rights and fundamental freedoms."*

*"****States must not use proxies to commit internationally wrongful acts using ICTs****, and should seek to ensure that their territory is not used by non-State actors to commit such acts."*

*"****The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States****, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behavior."*

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2015)

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

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）

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

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）

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

▲ 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。

NISC

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