



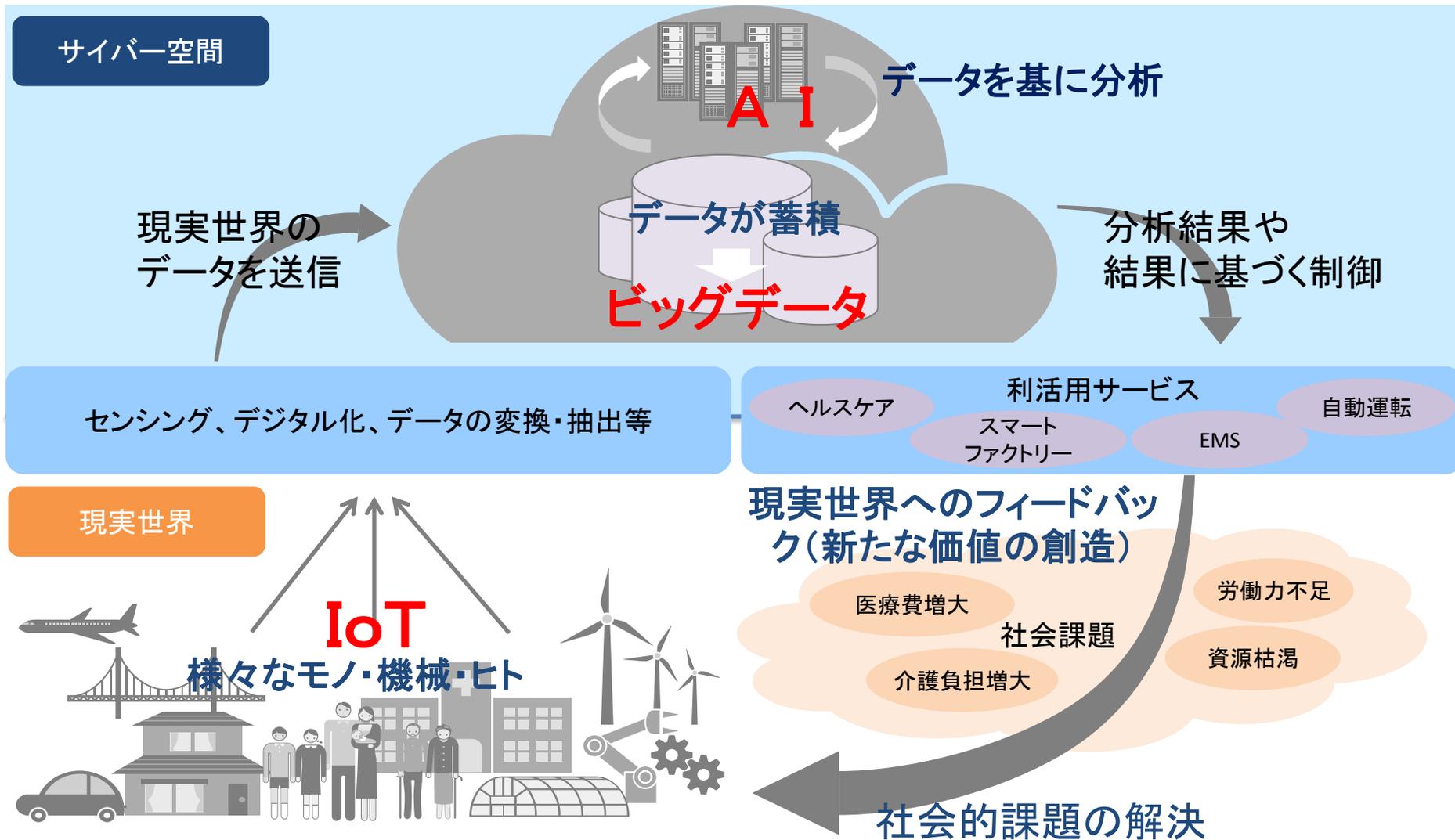
総務省

データ主導社会とサイバーセキュリティ

2018年3月9日

総務省政策統括官（情報セキュリティ担当）

谷脇 康彦



I. Society 5.0に向けた戦略分野

1. 健康寿命の延伸

- ・データ利活用基盤の構築
- ・保険者・経営者による「個人の行動変容の本格化」
- ・遠隔診療、AI開発・実用化
- ・自立支援に向けた科学的介護の実現
- ・革新的な再生医療等製品等の創出促進、医療・介護の国際展開の推進

2. 移動革命の実現

- ・世界に先駆けた実証
- ・データの戦略的収集・活用、協調的領域の拡大
- ・国際的な制度間競争を見据えた制度整備

3. サプライチェーンの次世代化

- ・データ連携の制度整備
- ・データ連携の先進事例創出・展開

4. 快適なインフラ・まちづくり

- ・インフラ整備・維持管理の生産性向上

5. FinTech

II. Society 5.0に向けた横割課題

価値の源泉の創出

1. データ利活用基盤・制度構築

- ・公共データのオープン化
- ・社会のデータ流通促進、知財・標準の強化

2. 教育・人材力の抜本強化

- ・世界に先駆けた実証
- ・データの戦略的収集・活用、協調的領域の拡大
- ・国際的な制度間競争を見据えた制度整備

3. イノベーション・ベンチャーを生み出す好循環システム

価値の最大化を後押しする仕組み

1. 規制の「サンドボックス」の創設

2. 規制改革・行政手続簡素化・IT化の一体的推進

3. 「稼ぐ力」の強化

4. 公的サービス・資産の民間開放

5. 国家戦略特区の加速的推進

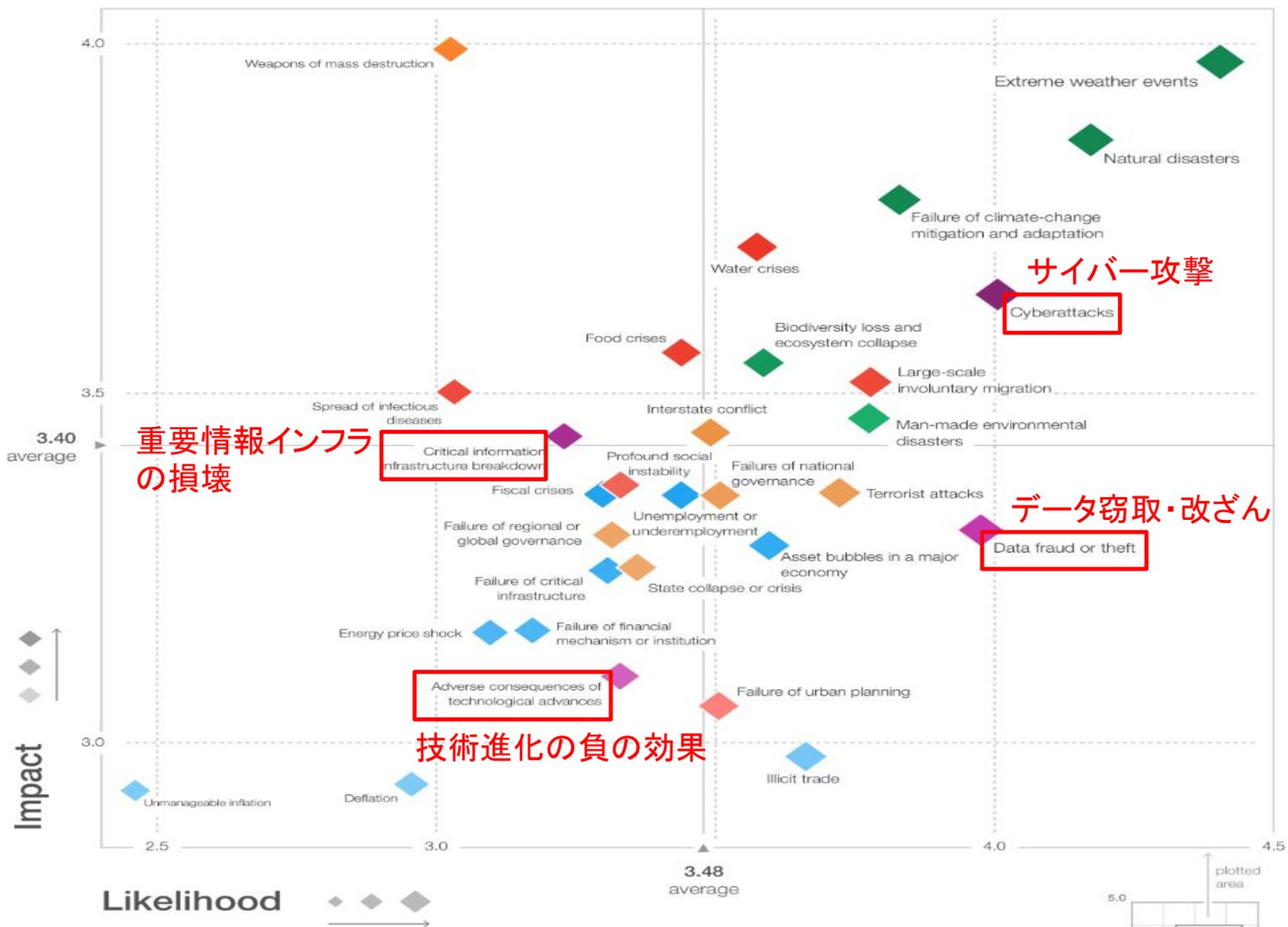
6. サイバーセキュリティ

7. シェアリングエコノミー

III. 地域経済好循環システムの構築

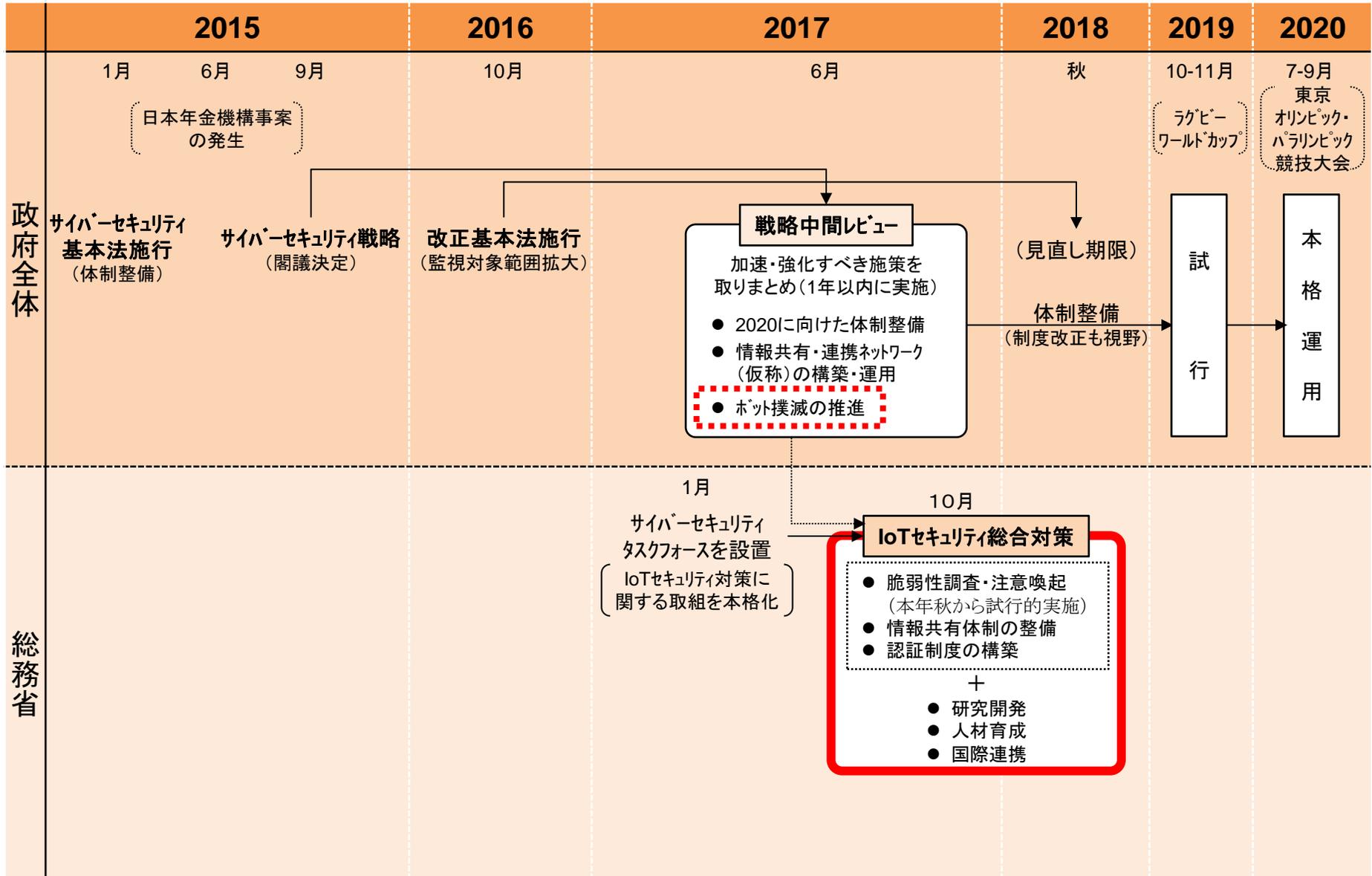
IV. 海外の成長市場の取り組み

グローバルリスクに対する評価(WEF2018)

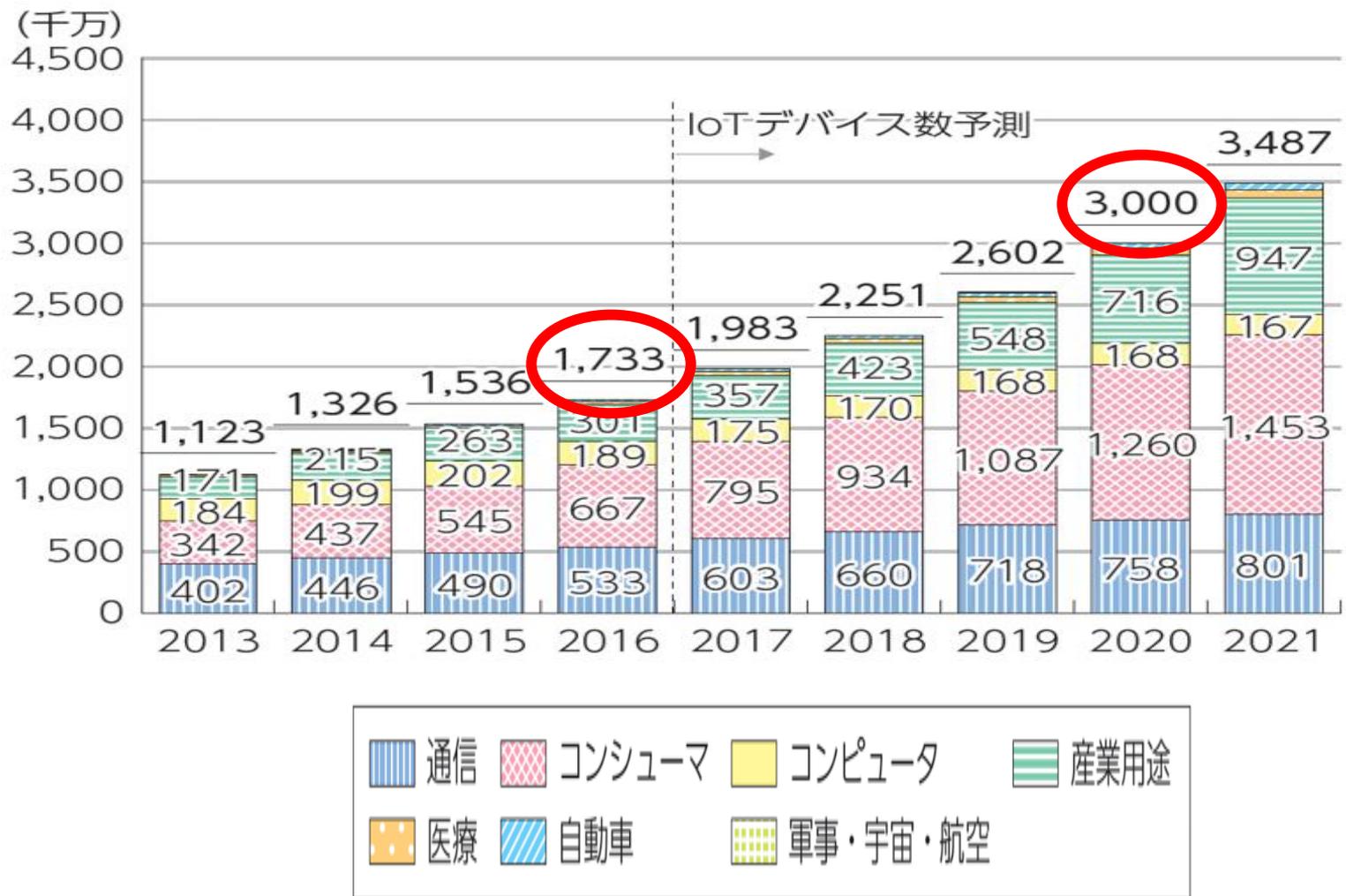


(出典) World Economic Forum "The Global Risks Report 2018 13th Edition" (January 2018)

サイバーセキュリティ対策関連スケジュール



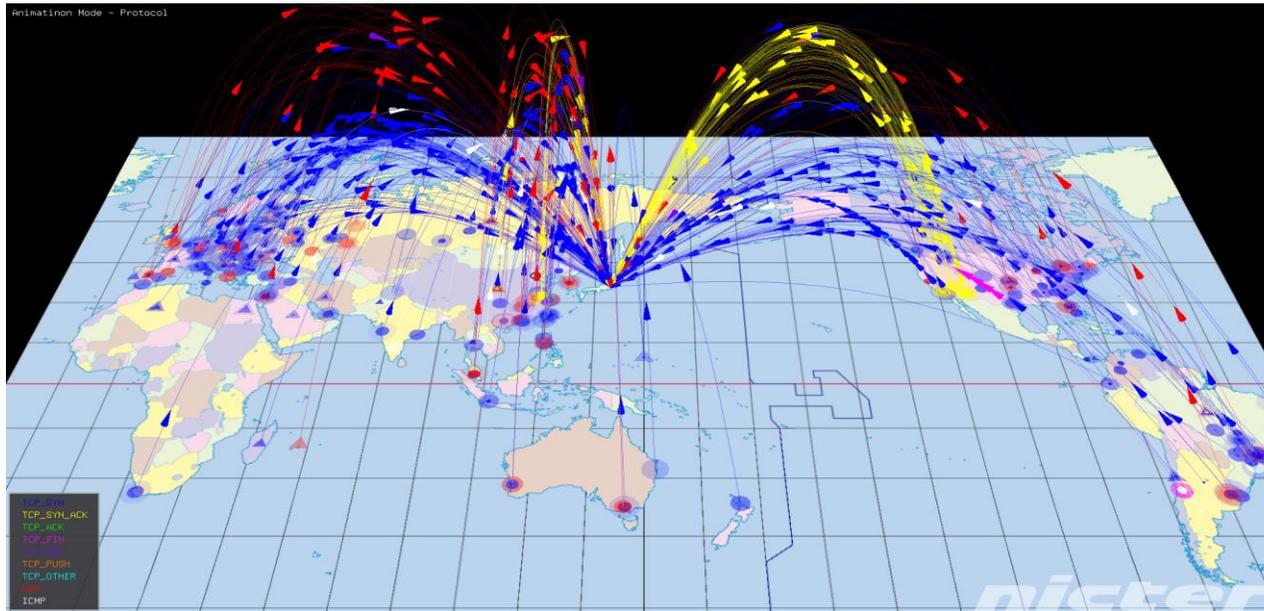
IoT機器の幾何級数的な増加



(出典) HIS Technology

IoT機器を狙った攻撃が急増(NICTERによる観測)

- ▶ 国立研究開発法人 情報通信研究機構(NICT)では、未使用のIPアドレスブロック30万個(ダークネット)を活用し、グローバルにサイバー攻撃の状況を観測。

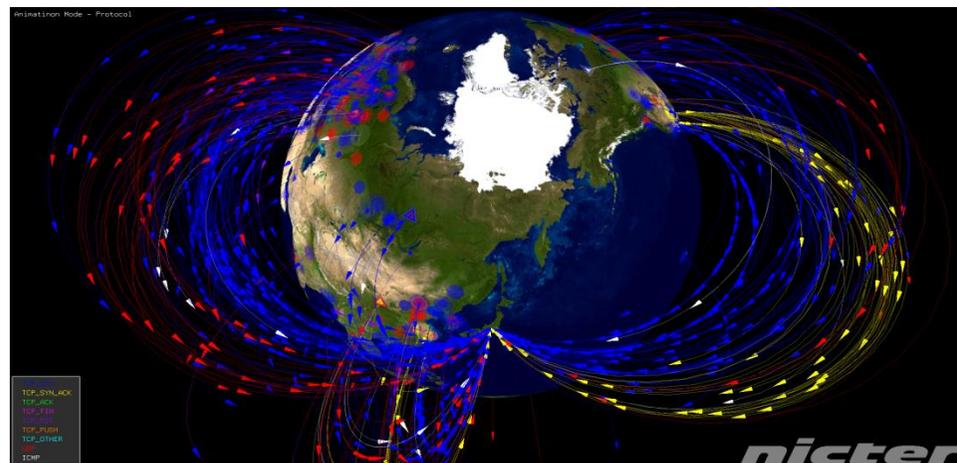
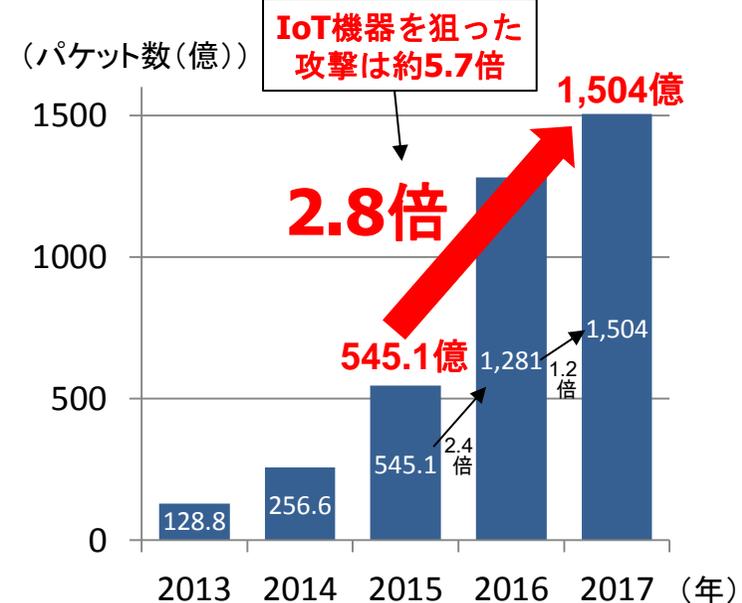


- ・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化
- ・色:パケットごとにプロトコル等を表現

NICTERで1年間に観測されたサイバー攻撃回数

・2年間で2.8倍

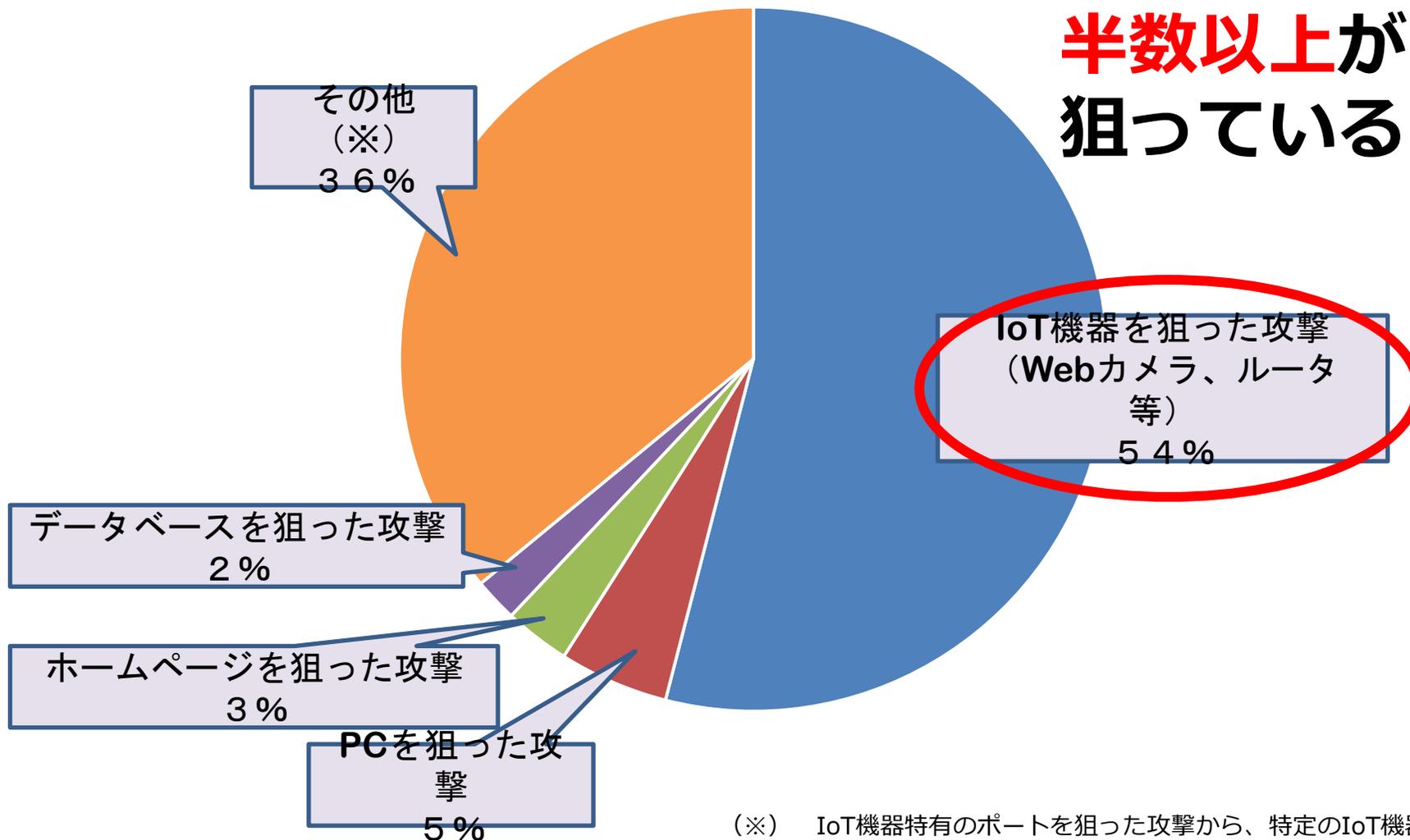
(2015年→2016年:2.4倍、2016年→2017年:1.2倍)



■ TCP SYN
■ TCP SYN/ACK
■ TCP ACK
■ TCP FIN
■ TCP RESET
■ TCP PUSH
■ TCP Other
■ UDP
■ ICMP

観測された全サイバー攻撃1,504億パケットのうち、

半数以上がIoTを 狙っている！



(※) IoT機器特有のポートを狙った攻撃から、特定のIoT機器の脆弱性を狙ったより高度な攻撃も観測されるようになっており、単純にポート番号だけから分類することが難しいIoT機器を狙った攻撃が「その他」に含まれている。

IoTシステムは社会基盤として機能

サービス
(データ流通)層

プラットフォーム層

ネットワーク層

端末層

- データの真正性確保のための対策強化
- 暗号化技術の高度化

- 異なるシステム間のセキュリティ対策の運用基準の共通化
- 異なるシステム間の情報共有体制の強化

- ネットワーク脆弱性への対策(5GやLPWAを含む)
- SDN/NFVに係るセキュリティ対策

- IoT端末※の脆弱性の管理・検知・切り離し(ハードウェア脆弱性を含む)

※既設端末と新設端末に分けた対策が必要。

- 脆弱性対策に係る体制の整備
- 研究開発の推進
- 民間セキュリティ投資の促進
- 人材育成の強化
- 国際連携の推進

脆弱性対策に係る体制の整備

- ・ IoT機器の脆弱性についてライフサイクル全体(設計・製造、販売、設置、運用・保守、利用)を見通した対策が必要。
- ・ 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- ・ セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

人材育成の強化

- ・ 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

民間企業等におけるセキュリティ対策の促進

- ・ 民間企業等のサイバーセキュリティに係る投資を促進。
- ・ サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

国際連携の推進

- ・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証(関係府省と連携)

ライフサイクル全体を見通した対策

設計・製造段階

■ セキュリティ・バイ・デザイン等の意識啓発・支援の実施

セキュリティ・バイ・デザインの考え方を踏まえ設計された機器に**認証マークを付与**し、当該認証マークの付された機器の使用を推奨すること等について検討を行い、意識啓発・支援を実施。

販売段階

■ 認証マークの付与及び比較サイト等を通じた推奨

一定のセキュリティ要件を満たしているIoT機器に対する認証マークの付与や、比較サイト等を通じた**利用者が容易に認証取得の有無等を確認できる仕組み**の構築について検討。

設置段階

■ IoTセキュアゲートウェイ

IoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組について実証を進めるとともに、セキュリティ評価や実際の導入を進める仕組みの検討。

運用・保守段階

■ セキュリティ検査の仕組み作り

継続的な安全性を確保するためのセキュリティ検査の仕組み作り(**機器の脆弱性に係る接続試験を行うテストベッドの構築**を含む)と、対策が不十分なIoT機器への対応の検討。

■ 簡易な脆弱性チェックソフトの開発等

IoT機器の利用者が簡易にその**脆弱性をチェックできるソフトを開発して配布する取組**や、脆弱性を調査する民間サービスの実施を促進する取組の検討。

利用段階

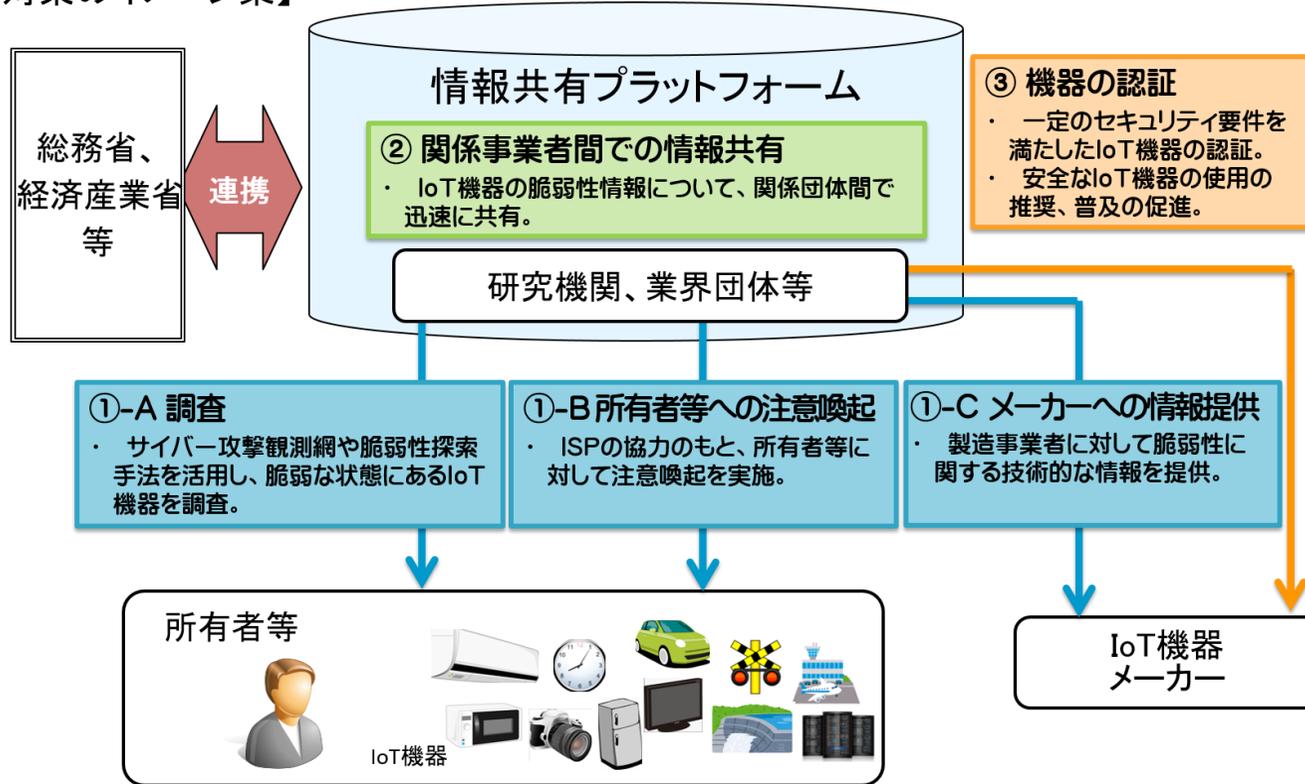
■ 利用者に対する意識啓発の実施や相談窓口等の設置

ID/パスワード設定、ファームウェアのアップデート、Wi-Fi設定の3点を中心とした**利用者への意識啓発**の実施、利用者からの**相談窓口**や、脆弱性が見つかった場合の関係機関との**調整窓口**の設置

- 重要IoT機器に係る脆弱性調査
- サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査

NICT法等改正法案を今国会に提出予定

【対策のイメージ案】



○脆弱なIoT機器の実態調査、所有者等への注意喚起

- IoT機器の調査を実施し、脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を実施。

○IoT機器の脆弱性情報の関係事業者間での共有

- IoT機器の製造事業者等が脆弱性に迅速に対応することを可能とするため、IoT機器の脆弱性情報を関係事業者間で共有する仕組みを構築。

■ 被害拡大を防止するための取組の推進

- 脆弱性を有するIoT機器が踏み台となったことが確認された場合、ISPによるC&Cサーバとの通信制御の実施を推進するとともに、当該取組を促進するための方策について検討(年度内を目途に方向性)。

■ IoT機器に関する脆弱性対策に関する実施体制の整備

- IoT機器に対する脆弱性対策を実施する体制(IoTセキュリティ対策センター(仮称))のあり方について検討(年度内を目途に結論)。

- I o T 機器などを悪用したサイバー攻撃の深刻化を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、パスワード設定に不備のあるIoT機器の調査等を追加（5年間の時限措置）する等を内容とする国立研究開発法人情報通信研究機構法の一部改正案を提出予定。

サイバー脅威の深刻化

- ・ IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。
- ※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性

- ・ パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

- ・ NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進。

情報通信研究機構法の改正

サイバーセキュリティ戦略本部

(中長期計画) 意見聴取

総務大臣

(中長期計画認可)

情報通信研究機構

- ・ パスワード設定に不備のある機器に係るIPアドレス等を提供

②情報提供

第三者機関

- ※ 改正後の電気通信事業法に規定する第三者機関に委託

電気通信事業者

①機器調査

- ・ パスワード設定に不備のある機器（その機器に係るIPアドレス）を特定

※ 総務大臣が調査の実施計画を認可

③注意喚起

- ・ パスワード設定に不備のある機器に係る利用者を特定し、設定変更の注意喚起



- ※ 平成30年度予算(案)を活用しつつ、サポート体制整備等を実施予定

インターネット上のIoT機器

機器の利用者

攻撃者

米 国

- 2017年1月、**商務省**タスクフォースはIoTに関する**グリーンペーパー**「IoTの進展の推進」を公表。
- **同年5月**、トランプ大統領が**大統領令**「サイバーセキュリティ強化のための大統領令」に署名。**ボットネット対策**も主要な項目の一つとして位置づけ。
- 同年6月、**商務省電気通信情報局 (NTIA)**がボットネット対策に関する意見募集を開始(同年9月、結果を取りまとめ公表)。
 - ※ **セキュリティ要件を満たしたIoT機器の認証制度の導入について多数の意見が提出。**
“信頼できる第三者機関が独立した試験・評価を通じて商品が安全で基準に適合していると証明することで、商品の購入決定を助ける可能性がある一方、こうしたプログラムは、脅威環境が継続的に進化していくために成功裏に実施することが難しいことが多いとの意見があった。”
- **大統領令を踏まえ、2018年1月に中間報告の公表(次頁参照)、同年5月に最終報告書**を取りまとめる予定。

欧州

- 2017年9月、**欧州委員会**は**サイバーセキュリティ強化に向けた政策パッケージ**を公表。現在の欧州ネットワーク情報セキュリティ機関(ENISA)を強化する「EUサイバーセキュリティ庁」の創設を提言するとともに、「**ICTサイバーセキュリティ認証に関する規則案**」を公表。
 - ※ **ICT製品・サービスが既知の脆弱性を有しない最新のソフトウェアを具備し、安全なソフトウェア更新のためのメカニズムを備えている場合に認証(認証の取得は任意)。**
 - ※ **認証は適合性評価機関が発行、最大3年間有効(更新可)。**
 - ※ **各加盟国は国家認証監督機関を指名。発行された認証はすべての加盟国で有効。**

- 米国政府は「ボットネットその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性を強化に関する報告書案」(※)の意見招請手続を開始(締め切りは2月12日)。
- 本報告書は、本年5月に大統領に報告される予定。

(※)“A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats” (Draft for Public Comment, jan. 5, 2018)

■ ボットネット対策の6つの主要テーマ

1. 自動化・分散化した攻撃は**グローバルな問題**。
2. **効果的なツール**は存在するが、広く利用されていない。
3. 製品は**ライフサイクル**のすべての段階でセキュアでなければならない。
4. **教育及び啓発**が必要。
5. **市場インセンティブ**が不完全。
6. 自動化・分散化した攻撃は、**エコシステム全体**に関わる課題。



■ 5つのゴール(目標)

- Goal 1 適応可能、持続可能かつ安全な技術市場環境の実現に向けた**明確な道筋の明確化**
- Goal 2 進化する脅威に動的に対応するための**インフラのイノベーションの促進**
- Goal 3 ネットワークの**エッジにおけるイノベーションの促進**による、悪意ある行為の防止、検出、影響の緩和
- Goal 4 国内外のセキュリティ、インフラ、運用技術の**各コミュニティ間の連携の構築**
- Goal 5 エコシステム全体にわたる**啓発・教育**の強化

エコシステムの技術的側面

- **インフラ**-----共同防御(shared defence)アプローチが重要。
- **企業ネットワーク**---NISTフレームワークの普及・実装が必要。
- **エッジ機器**-----製造販売者は既知のセキュリティ上の欠陥を有する製品の出荷は不可、セキュリティ更新機能を実装、最良の慣行を採用(例:ハードコードされたパスワード不可、運用に不必要なソフトウェアの機能の停止)、保証期間内のセキュリティ更新サービスの提供が必要。
- **家庭・小規模事業ネットワーク**---消費者向け製品は可能な限りセキュアに設計、セキュリティ自動更新機能の実装、製品運用に必要な知識の最小化

エコシステムの政策的側面

- 規制は直ぐに時代遅れとなり、イノベーションを阻害し、消費者の利益を制約。
米国政府は、**産業界主導のアプローチとコンセンサスベースの標準が重要**と認識。
- **国際的な連携**が重要。よりセキュアな製品を生み出す市場インセンティブを創出するため、**(セキュアなIoT機器の)政府調達の実体化**が必要。



5つのゴールを達成するための**23の行動計画**を整理

“Internet of Things Cybersecurity Improvement Act of 2017” (S.1691)(提案者: Sen. Warner (D-VA))

■ 連邦政府がIoT機器を調達する場合のセキュリティ要件を定める目的。

■ 法案の内容

- ・製造業者に対し、機器がpatchable(脆弱性へのパッチ適用可能)、業界標準の適用、変更できない(hard-coded)パスワードの使用不可、既知の脆弱性を含まないことを要求。
- ・機器がハード、ソフト、ファームウェアの既知の脆弱性を含んでいないことに加え、脆弱性を認知した場合には速やかに当該政府機関に届けることを約した書面の提出を製造業者に要求。
- ・各政府機関において、それぞれ保有するIoT機器の目録の作成を要求。
- ・IoT機器のセキュリティ確保のため、ネットワーク分離、セキュリティ水準の管理機能、多要素認証、端末の切り離し等を可能とするゲートウェイなどの方策を政府において検討。
- ・IoT機器の脆弱性について研究者が製造業者と共有するためのガイドラインを政府において策定。

(注) 政府機関については、法案は調達の責任組織であるOMB長官に措置を求めている。

IoT推進コンソーシアム

- IoT/ビッグデータ/人工知能時代に対応し、企業・業種の枠を超えて産学官で利活用を促進するため、総務省及び経済産業省の共同の呼びかけのもと、民主導の組織として「IoT推進コンソーシアム」を設立。（平成27年10月23日（金）に設立総会を開催。）
- 技術開発、利活用、政策課題の解決に向けた提言等を実施。（会員法人数3,250社（平成29年10月時点））

総会

- 会長
- 副会長

会長

村井 純 慶應義塾大学 環境情報学部長兼教授

副会長

鵜浦 博夫 日本電信電話株式会社 代表取締役社長
中西 宏明 株式会社日立製作所 執行役会長兼CEO

運営委員会 (15名)

運営委員会メンバー

委員長 村井 純 慶應義塾大学 環境情報学部長兼教授

大久保 秀之
越塚 登
小柴 満信
齊藤 裕
坂内 正夫
志賀 俊之
篠原 弘道

三菱電機株式会社 代表執行役
東京大学大学院 教授
JSR株式会社 社長
株式会社日立製作所 副社長
情報通信研究機構 理事長
産業革新機構 会長(CEO)
日本電信電話株式会社 副社長

須藤 修 東京大学大学院 教授
堂元 光 日本放送協会 副会長
徳田 英幸 慶應義塾大学大学院 教授
野原 佐和子 イプシ・マーケティング研究所 社長
程 近智 アクセンチュア株式会社 会長
林 いづみ 弁護士
松尾 豊 東京大学 准教授

技術開発WG (スマートIoT推進フォーラム)

ネットワーク等のIoT関連技術の開発・実証、標準化等

先進的モデル事業推進WG (IoT推進ラボ)

先進的なモデル事業の創出、規制改革等の環境整備

IoTセキュリティWG

- IoT機器のネット接続等に関するガイドラインの検討
- IoT機器のセキュリティ認証制度、認証されたIoT機器の普及促進のための方策の検討

データ流通促進WG

データ流通のニーズの高い分野の課題検討等

協力

協力

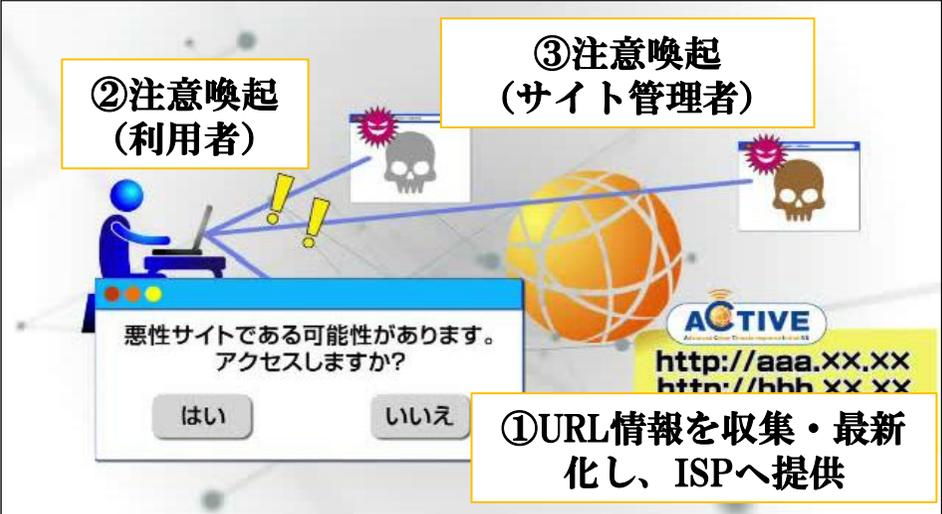
2017年12月より検討

総務省、経済産業省 等

○ 平成25年11月からインターネットサービスプロバイダ (ISP) 等との協力により、インターネット利用者を対象に、**マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト (ACTIVE) を実施。**

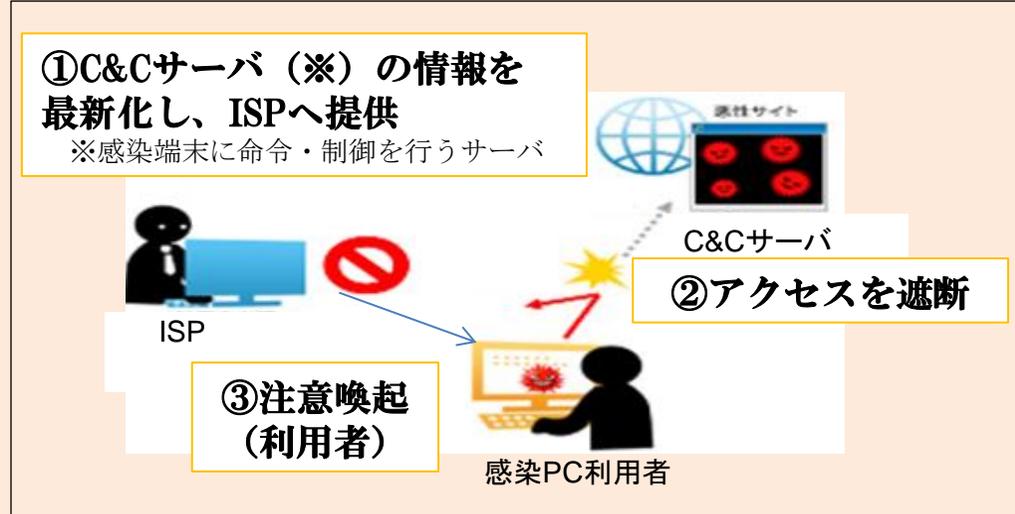
ACTIVE (Advanced Cyber Threats response Initiative) の取組

(1)マルウェア感染防止の取組



- ①マルウェア配布サイトのURL情報を最新化し、ISPへ提供。
- ②マルウェア配布サイトにアクセスしようとする利用者にISPから注意喚起。
- ③マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

(2)マルウェア被害未然防止の取組

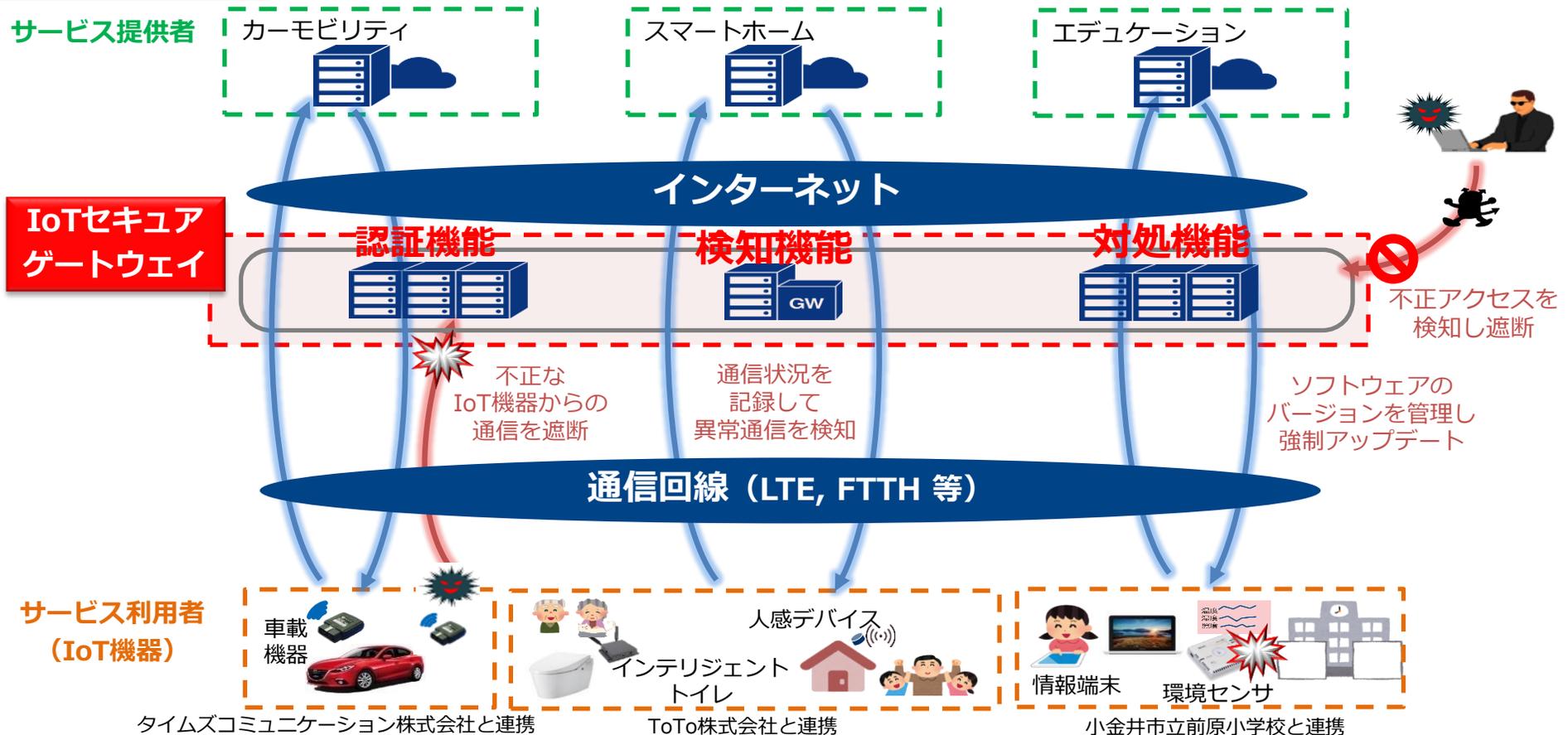


- ① C&Cサーバの情報を最新化し、ISPへ提供。
- ② 感染PC利用者からのC&Cサーバへのアクセスを遮断する。
(2016年2月から2018年1月までで約4億3616万件の遮断実績)
- ③ 感染PC利用者に注意喚起。

- IoT時代における我が国のサイバーセキュリティを確保し、我が国の経済社会の活力の向上や持続的発展に寄与するため、新たな脅威にも対応したセキュリティ対策の実証を実施
- 具体的には、IoT機器とインターネットの境界にIoTセキュアゲートウェイを設置し、その有用性に関する検証を実施

実証実験のイメージ

実施主体：NTTコミュニケーションズ株式会社、平成29年12月より実証実験を開始（平成28年度補正（2.5億円））



脆弱性対策に係る体制の整備

- ・ IoT機器の脆弱性についてライフサイクル全体(設計・製造、販売、設置、運用・保守、利用)を見通した対策が必要。
- ・ 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- ・ セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

人材育成の強化

- ・ 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

民間企業等におけるセキュリティ対策の促進

- ・ 民間企業等のサイバーセキュリティに係る投資を促進。
- ・ サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

国際連携の推進

- ・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証(関係府省と連携)

■ 基礎的・基盤的な研究開発等の推進

新たに出現する未知の標的型攻撃の挙動を早い段階で明らかにするとともに、分析結果をセキュリティ対策機関等と連携して情報共有を図ることが可能な、高度で効率的なサイバー攻撃誘引基盤(STARDUST)を構築。

■ 広域ネットワークスキャンの軽量化

膨大なIoT機器に対する広域的なネットワークスキャンを効率的に実施するため、その軽量化などの必要な技術開発を推進。

■ ハードウェア脆弱性への対応

ビッグデータやAIを活用しつつ、ハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を推進。

■ スマートシティのセキュリティ対策の強化

スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を一体的に推進。

■ 衛星通信におけるセキュリティ技術の研究開発

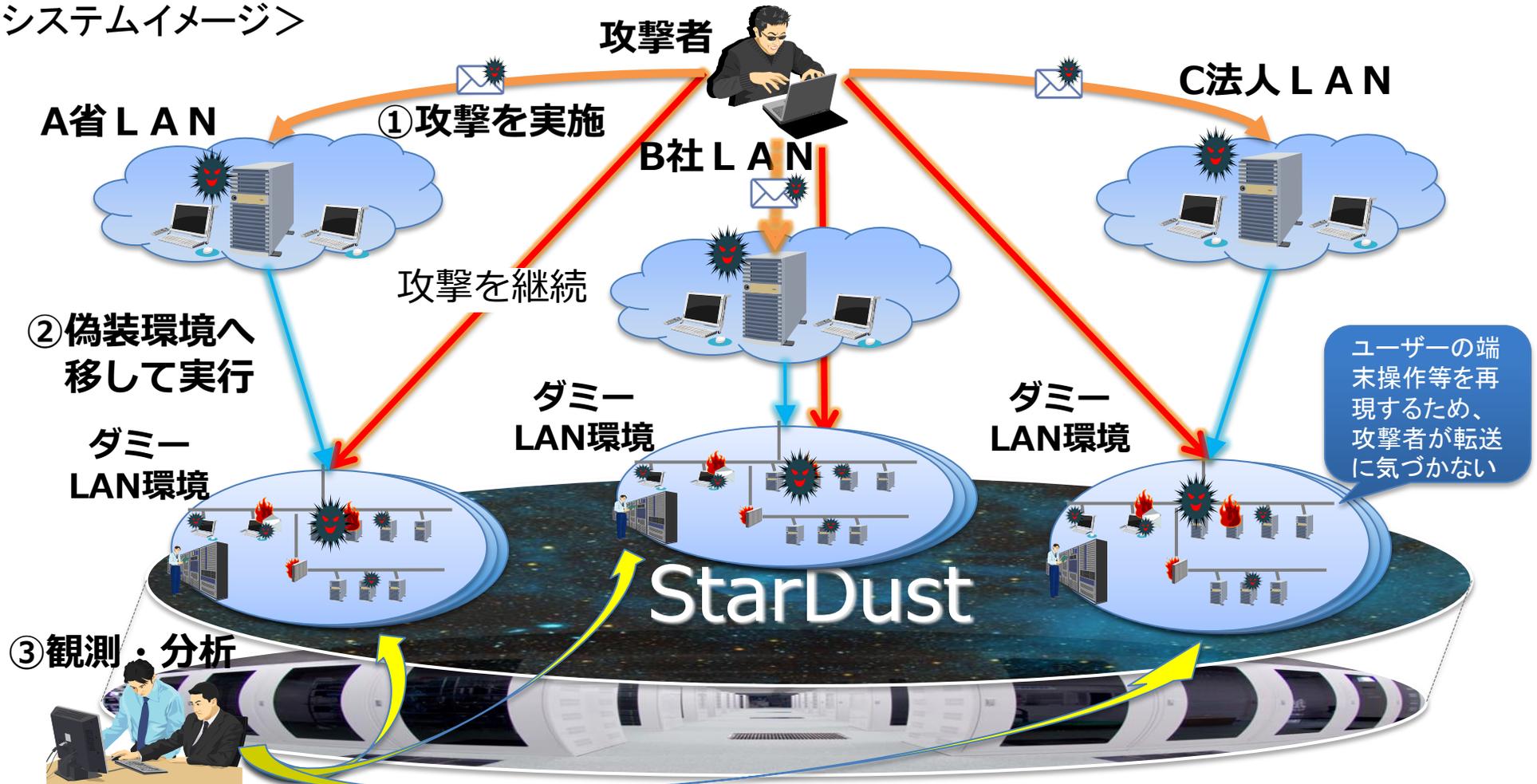
安全性を備えた衛星通信を実現するために、量子暗号技術の研究開発や高秘匿衛星光通信技術の実証を行うとともに、衛星のバックアップや高高度での中継を行うための航空機等による移動体光通信技術の研究開発を実施。

■ AIを活用したサイバー攻撃検知・解析技術の研究開発

サイバー攻撃の検知・解析を自動化するような、AIを活用したサイバー攻撃検知・解析技術の研究開発を推進。

- NICTでは、標的型サイバー攻撃の詳細な手法を把握するため、①攻撃者が標的型メールを特定組織に送信した場合に、②不正な添付ファイル等を「あらかじめ構築した偽装環境」で実行し、③偽装環境で具体的な攻撃手段(入力コマンド等)の観測・分析が可能なシステム(StarDust)を研究開発している。

<システムイメージ>



データ利活用型スマートシティ

サービス（データ流通）層

- データの標準化、アプリケーションの相互運用性確保、ベンチャーの活用がサービスの多様化に必要
- 将来的にはAIを活用した都市機能のマネジメント等を視野に

プラットフォーム層

- ゼロからの構築では無くオープンソースの活用
- 他のプラットフォームとの互換性を確保

ネットワーク層

- 既存インフラに加え、LPWA、MVNOなど目的に合わせ効率よく利用
- 更にSDNや5Gの活用も視野に

都市が抱える多様な課題解決を実現

データ連携基盤
(モジュール&クラウドによる共通化)

様々なデータを収集

農林水産

行政

気象

観光

健康・医療

交通

データ利活用型スマートシティ

希望する自治体が容易に活用する環境を整え、運用・維持・管理コストを抑制

大企業やベンチャー企業など、多様な主体が参画



近隣自治体等へ横展開し、波及効果を最大化



対象

- 拡張可能性や持続可能性の観点から、都市全体、鉄道沿線、街区が主たる対象
- スクラッチからの開発と既存の街の再開発への導入の2種類があることに留意

計画段階

- ICT関連事業者が街づくり計画段階の初期から参画
- 自治体の首長による強いコミットメント
- 全体を統括して横串を通す自治体内の組織

構築段階

- PPP/PFIなど民間と連携したファイナンスを活用
- 地元の有志企業からの出資
- ソーシャルインパクトボンドの活用も考慮

運用段階

- 横断的なマネジメントを行う組織が鍵
- ICT企業がエリアマネジメント組織に参画し、データを利活用
- PDCAを回すことで、スマートシティのバージョンアップを図る

脆弱性対策に係る体制の整備

- ・ IoT機器の脆弱性についてライフサイクル全体(設計・製造、販売、設置、運用・保守、利用)を見通した対策が必要。
- ・ 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- ・ セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

人材育成の強化

- ・ 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

民間企業等におけるセキュリティ対策の促進

- ・ 民間企業等のサイバーセキュリティに係る投資を促進。
- ・ サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

国際連携の推進

- ・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証(関係府省と連携)

民間企業等におけるセキュリティ対策の促進

■ 民間企業のセキュリティ投資等の促進

経済産業省と連携して、企業におけるセキュリティ投資を促進するため、高レベルのサイバーセキュリティ対策に必要なシステムの構築やサービスの利用に対する**税制優遇措置**を検討。

■ セキュリティ対策に係る情報開示の促進

任意の情報開示であることを前提としつつ、関係府省と連携しながら、企業のセキュリティ対策に係る**情報開示に関するガイドライン**の策定について検討（**年度内を目途に結論**）。

→**2017年12月より分科会を設置して検討**。

■ 事業者間での情報共有を促進するための仕組みの構築

事業者間での情報共有を促進するため、**情報提供元及び共有される情報自体の信頼性を担保する仕組み**や、様々な事業者から提供された大量の情報の分析、情報の重複の排除、情報の重み付け、サイバー攻撃の全体像の把握を行った上で、**情報共有を実施する仕組み**を検討。

■ 情報共有時の匿名化処理に関する検討

情報共有に当たって、情報の秘匿性を担保する観点から、**情報の匿名化処理の導入**を検討するとともに、どのような方法で、どの程度まで情報を匿名化するべきかについての評価指標やガイドラインの整備を検討。

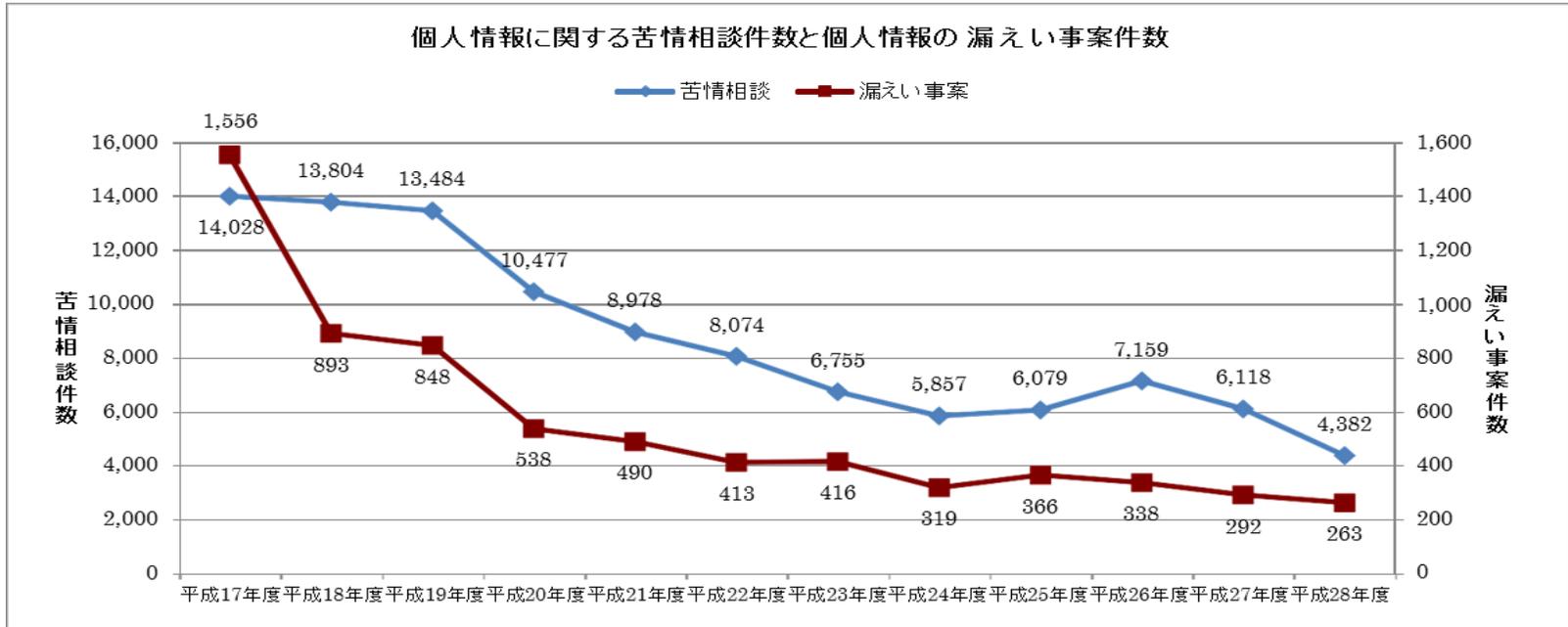
■ 公衆無線LANのサイバーセキュリティ確保に関する検討

公衆無線LANにおけるサイバーセキュリティ上の課題を整理し、今後必要な対策について検討（**年度内を目途に結論**）。

→**2017年11月より分科会を設置して検討**。

平成28年度における個人情報漏えい事案(傾向)

- 個人情報保護委員会が平成28年度の法施行状況について公表。
- 漏えい件数は減少傾向にあるものの、**漏えい人数が多い事案は増加**。



■ 個人情報の漏えい状況(公表されたもの)

漏えいした人数	平成 28 年度		平成 27 年度	
	件数	(割合)	件数	(割合)
500 人以下	145	(55.1%)	187	(64.0%)
501～ 5,000 人	53	(20.2%)	51	(17.5%)
5,001～ 50,000 人	39	(14.8%)	39	(13.4%)
50,001 人以上	22	(8.4%)	14	(4.8%)
不明	4	(1.5%)	1	(0.3%)
合計	263	(100.0%)	292	(100.0%)

電子媒体のみ	紙媒体のみ	電子媒体と紙媒体	不明
78	64	3	1
36	17	0	0
29	10	0	0
22	0	0	0
3	0	0	0
168	91	3	1

平成28年度における主な個人情報漏えい事案

■平成28年度中に事業者が公表した個人情報漏えい事案(所管府省において把握したものに限る)のうち、漏えいした個人情報が**5万件超**の事案を掲載。**(主要22件中19件がサイバー事案)**

	事業者	所管府省	公表日	漏えい人数 (最大)	漏えい情報 (主なもの)	漏えいの原因 (斜自体は報告書には無い追記事項)
1	株式会社A	A総務省	平成28年6月21日	約62万件	会員ID、会員パスワード、氏名、生年月日、性別、メールアドレス、住所、職業、電話番号、ポイント情報、決済手段区分、PAIDメンバーID	不正アクセス(ぜい弱性)
2	株式会社B	総務省	平成28年6月14日	約33万件	氏名(漢字、カタカナ、ローマ字)、性別、生年月日、メールアドレス、郵便番号、住所、電話番号、パスポート番号、パスポート取得日	不正アクセス(JTB関連)
3	株式会社C	総務省	平成28年6月22日	約98万件	注文者氏名、注文者住所、注文者メールアドレス(PC/携帯)、注文者電話番号、注文者コメント、管理者コメント、配送先氏名、配送先住所、配送先電話番号、注文金額、送料番号	不正アクセス(設定ミスによるファイル漏えい)
4	株式会社D	D総務省	平成28年4月21日	約43万件	氏名、住所、メールアドレス、電話番号等	不正アクセス(OSコマンドインジェクション)
5	株式会社E	総務省	平成28年4月22日	約64万件	氏名、住所、メールアドレス、電話番号、性別、年齢、職業	不正アクセス(OSコマンドインジェクション)
6	株式会社F	総務省	平成28年7月25日	約12万件	パスワード、メールアドレス、電話番号、住所、生年月日、氏名	不正アクセス(SQLインジェクション)
7	株式会社G	国土交通省 (観光庁)	平成28年6月14日	約678万件	氏名、性別、生年月日、メールアドレス、住所、郵便番号、電話番号、パスポート番号、パスポート取得日	外部からの不正アクセス(添付ファイル)
8	協会H	厚生労働省	平成29年2月17日	約19万人分	氏名、健康保険証の記号番号、医療機関コード、再審査を求める理由、再審査結果	紛失(誤廃棄の可能性)(FD、CD等)
9	株式会社I	経済産業省	平成28年12月2日	約42万件	氏名、性別、生年月日、年齢、職業、電話番号、メールアドレス、住所、購入履歴、ログインパスワード、一部クレジットカード情報(カード会員名、カード番号、カード有効期限)	不正アクセス(ぜい弱性)
10	公益社団法人J	経済産業省	平成29年4月25日	約15万件	住所、氏名、電話番号、生年月日、ログインID、パスワード、メールアドレス 一部クレジットカード情報(カード会員名、カード番号、有効期限、セキュリティコード)	不正アクセス(Apache Struts2 ぜい弱性)
11	株式会社K	経済産業省	平成29年3月23日	約118万件	氏名、生年月日電話番号、住所、性別、メールアドレス	不正アクセス(Apache Struts2 ぜい弱性)
12	株式会社L	経済産業省 総務省	平成29年3月10日	約40万件	メールアドレス、クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話番号、生年月日、メールアドレス、加入月	不正アクセス(Apache Struts2 ぜい弱性)
13	株式会社M	経済産業省	平成29年3月10日	36万件	クレジットカード番号、有効期限、メールアドレス	不正アクセス(Apache Struts2 ぜい弱性)
14	株式会社N	経済産業省	平成28年4月11日	約20万件	ユーザーID、パスワード、氏名、住所、電話番号、メールアドレス、生年月日の内 顧客が登録した情報、加えて、537件はクレジットカード番号、有効期限、セキュリティコード	不正アクセス
15	株式会社O	経済産業省	平成28年4月28日	約64万件	氏名、性別、住所、メールアドレス、家族に関する情報 ※漏えい項目は公表せず。	不正アクセス(ケータイキットぜい弱性)
16	株式会社P	経済産業省	平成28年4月27日	約13万件	氏名、住所、電話番号、メールアドレス、ログイン会員ID及びパスワード、クレジットカード情報(カード番号、有効期限、カード名義、セキュリティコード)うち、カード情報は7386件	不正アクセス(OpenSSL ぜい弱性)
17	株式会社Q	経済産業省	平成28年8月23日	約21万件	氏名、住所、電話番号、法人担当者名 ※漏えい項目は公表せず。	外付けハードディスクの紛失
18	株式会社R	経済産業省 総務省	平成28年8月26日	約11万件	クレジットカード情報(カード番号、カード名義、有効期限、セキュリティコード)、会員情報(メールアドレス、パスワード、氏名、住所、電話番号、その他の登録情報)	不正アクセス(ぜい弱性)
19	株式会社S	経済産業省 総務省	平成28年5月11日	約5万件	ニックネーム、メールアドレス、生年月日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正ログイン(リスト型攻撃)
20	株式会社T	経済産業省 総務省	平成28年11月29日	約58万件	ニックネーム、メールアドレス、生年月日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正アクセス(リスト型攻撃)
21	株式会社U	経済産業省	平成29年1月1日	約5万9千件	メールアドレス、氏名、生年月日、性別、住所、郵便番号、電話番号	不正アクセス(SQLインジェクション)
22	株式会社W	経済産業省	平成29年2月27日	約120万件	氏名、住所、電話番号、生年月日、メールアドレス、性別 クレジットカード番号、カード有効期限	バックアップストレージの盗難

【出典】個人情報保護委員会「平成28年度個人情報の保護に関する法律施行状況の概要」(平成29年11月)

表 5-3：一件あたりの平均損害賠償額の経年変化

	一件あたりの 平均想定損害賠償額	(参考) 想定損害賠償総額
2005年	5億 3,935万円	約 5,329億円
2006年	4億 8,156万円	約 4,570億円
2007年	27億 9,347万円	約 2兆 2,711億円
2008年	1億 8,552万円	約 2,367億円
2009年	2億 6,683万円	約 3,890億円
2010年	7,551万円	約 1,215億円
2011年	1億 2,810万円	約 1,900億円
2012年	9,313万円	約 2,133億円
2013年	1億 6,575万円	約 1,439億円
2014年	10億 8,561万円	約 1兆 6,642億円
2015年	3億 2,192万円	約 2,527億円
2016年	6億 7,439万円	約 2,994億円

(1) 単年分析(件数)

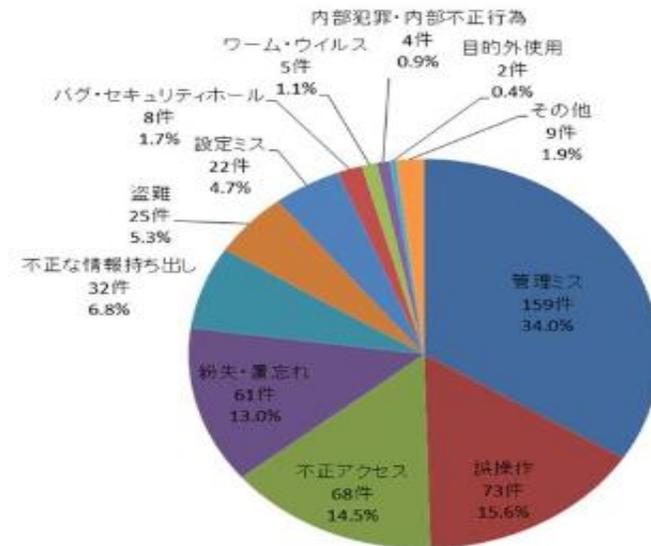


図 4-8：漏えい原因比率 (件数)

表 4-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	793万人	生活関連サービス業、娯楽業	ワーム・ウイルス
2	98万人	情報通信業	不正アクセス
3	81万人	電気・ガス・熱供給・水道業	紛失・置忘れ
4	64万人	情報通信業	不正アクセス
5	58万 9463人	情報通信業	不正アクセス
6	42万 8138人	情報通信業	不正アクセス
7	42万 1313人	卸売業、小売業	不正アクセス
8	35万人	生活関連サービス業、娯楽業	不正アクセス
9	21万 9025人	卸売業、小売業	不正アクセス
10	21万人	電気・ガス・熱供給・水道業	管理ミス

(出典)JNSA & 長崎県立大学“情報セキュリティインシデントに関する調査報告書”(2017年6月14日)

サイバー攻撃が米国に及ぼす年間の経済的損失を推計-----2016年時点
→ 570億ドル(6.1兆円)~1090億ドル(11.7兆円)
(対GDP比で0.31~0.58%)。

■サイバー攻撃の損害は攻撃を受けた企業と経済的に関連する企業にスピルオーバーし、経済に与える打撃を拡大。

- ・サイバー攻撃を受けた企業の株価の低下→他企業での(当該企業の)保有株式の資産価値の低下
- ・サイバー攻撃対策関連の支出の増大
- ・新しいICTの採用が鈍化→生産性が低下

■企業は共通する脆弱性を抱えているため、特定の脅威が企業の枠を越えて波及。共通する脆弱性の理解が不足していることがサイバー保険市場の発展を阻害。

■データの欠如や不十分な情報共有がサイバー保険市場の発展を阻害。

■サイバーセキュリティは共通財。サイバーセキュリティの欠如は他企業や国民に負の外部性をもたらす。負の外部性に関する説明不足が社会的な最適水準のセキュリティ投資を実現することを阻み、過少投資にとどまる。

■政府の果たすべき役割

- ・情報開示の推進や十台なデータ侵害企業の制裁による企業リスクの外部性の内生化
- ・サイバーセキュリティ基礎研究の推進(民間企業におけるイノベーションの促進)
- ・セキュリティ基準の普及促進
- ・情報共有の促進(ISACやISAO) 等

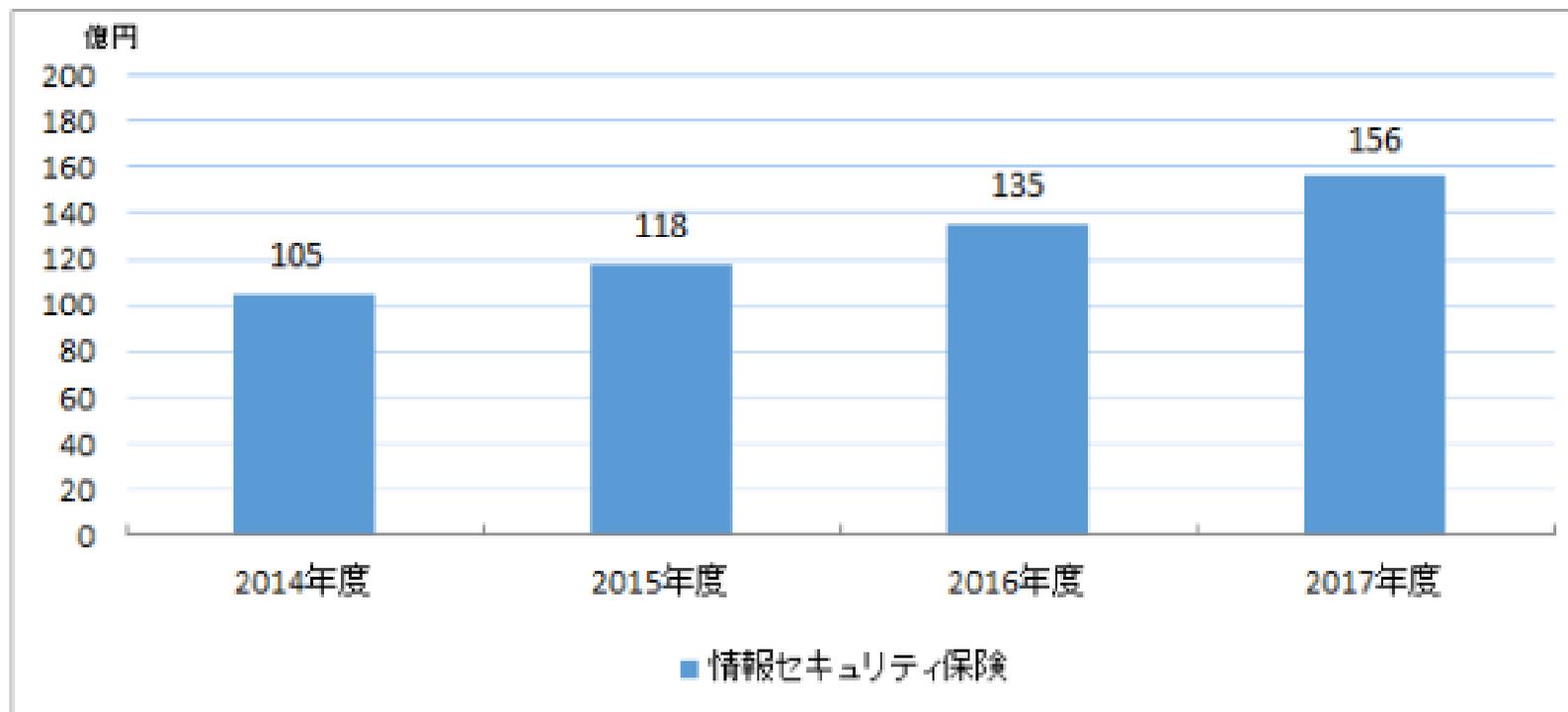


図 25 国内情報セキュリティ保険市場推移

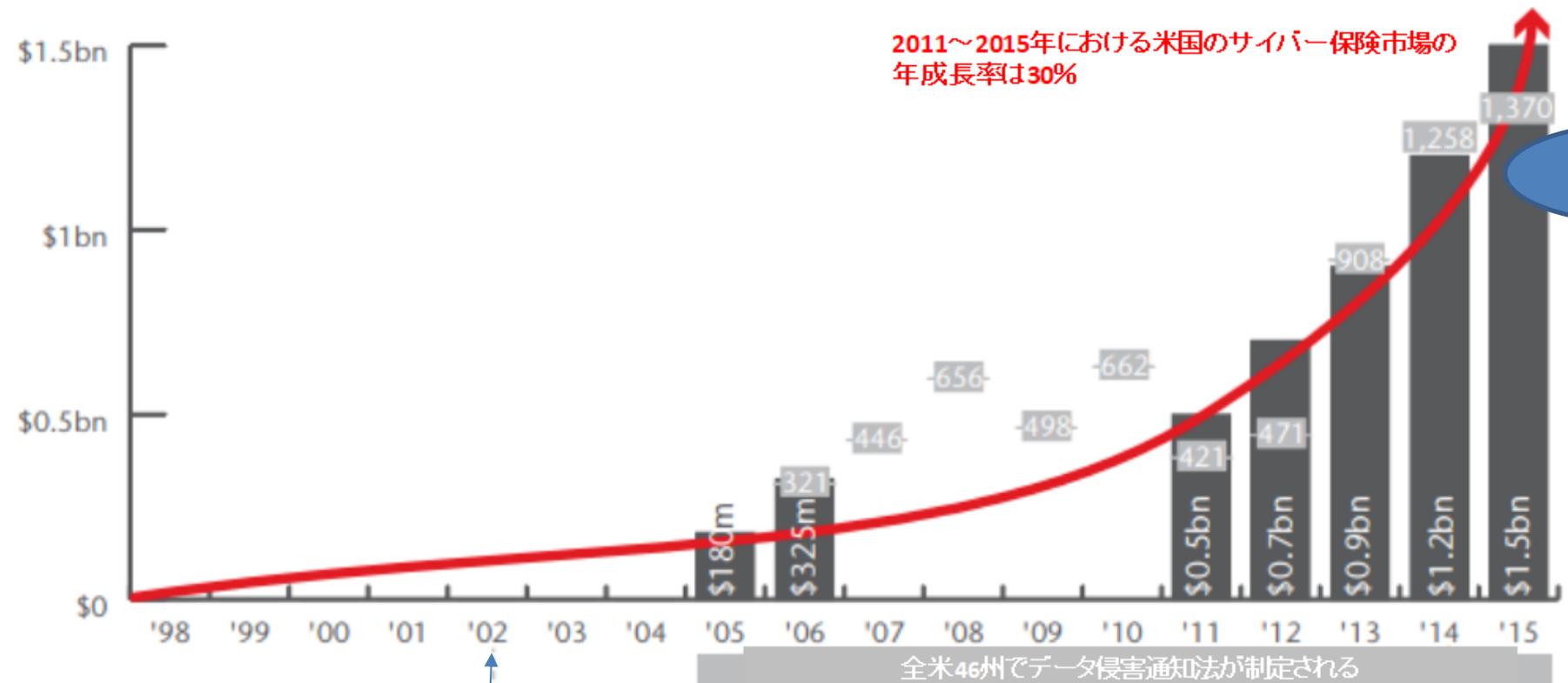
(出典)JNSA“2016年度情報セキュリティ市場調査報告書”(2017年6月)

米国におけるサイバーセキュリティ保険市場

■ 米国市場規模 ■ 公表された情報漏洩件数

2011～2015年における米国のサイバー保険市場の年成長率は30%

約15億ドル



カリフォルニア州でデータ侵害通知法が成立

データ侵害通知法 (Data Breach Notification Law) は全米48州で制定 (アラバマ州とサウスダコタ州を除く)

Major loss: TJX
Major loss: Heartland
Major loss: Sony
SECガイダンスの公表

※米国で発生した大規模な情報漏洩事件で被害を受けた企業

(出典) 中沢潔「米国におけるサイバー保険の現状」(JETRO/IPA NY、ニューヨーク便り、2017年11月)

- 一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入に対して、特別償却30%又は税額控除3%(賃上げを伴う場合は5%)を措置。
- 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用(適用期限は、平成32年度末まで)。

※ 経済産業省との共管

【計画認定の要件】

①データ連携・利活用の内容

- ・社外データやこれまで取得したことのないデータを社内データと連携
- ・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

- ・労働生産性：年平均伸率2%以上
- ・投資利益率：年平均15%以上



課税の特例の内容

- 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% (法人税額の15%を限度)
		5% ※ (法人税額の20%を限度)

【対象設備の例】

データ収集機器(センサー等)、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム(サーバ、AI、ソフトウェア等)、サイバーセキュリティ対策製品 等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率 $\geq 3\%$ を満たした場合。

脆弱性対策に係る体制の整備

- ・ IoT機器の脆弱性についてライフサイクル全体(設計・製造、販売、設置、運用・保守、利用)を見通した対策が必要。
- ・ 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- ・ セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等におけるセキュリティ対策の促進

- ・ 民間企業等のサイバーセキュリティに係る投資を促進。
- ・ サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

- ・ 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

- ・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証(関係府省と連携)

- 国の行政機関、地方公共団体、独立行政法人及び重要インフラ企業等に対するサイバー攻撃について、実践的な演習を実施([CYDER](#))
 - ⇒ 47都道府県で演習を実施し、平成29年度から演習規模を3000人まで拡大
- 2020年東京大会の適切な運営に向けたセキュリティ人材の育成([サイバーコロッセオ](#))
 - ⇒ 2020年東京大会開催時に想定される、IoTを含む高度な攻撃に対応した演習を実施(平成30年2月より本格実施)
- 若手セキュリティイノベータの育成([SecHack365](#))
 - ⇒ 高専や大学等を通じて若手人材を募集し、セキュリティの技術開発を本格指導(平成29年度から実施)



NICT「ナショナルサイバートレーニングセンター」(17年4月設立)
でプラットフォーム化

- **CYDERは、行政機関や民間企業等のセキュリティ運用者（情報システム担当者等）を対象とした体験型の実践的なサイバー防御演習。**
- **受講者は、組織の情報システム担当職員として、チーム単位で演習に参加。組織のネットワーク環境を模した環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験。**

演習のイメージ



CYDER演習会場
(大手町)

- NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用し、行政機関や民間企業の実際のネットワークを模した大規模な演習環境を構築。
- NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意。

平成29年度の実施状況

コース	主となる対象組織	開催地	開催回数	受講者数(※3)
Aコース(初級)	地方公共団体向け	47都道府県	59回	1477名
B-1コース(中級)	地方公共団体向け	全国11地域	21回	649名
B-2コース(中級)	国の行政機関、独立行政法人、指定法人(※1)、重要インフラ事業者(※2)等向け	東京	20回	883名

(※1) 特殊法人・認可法人のうちサイバーセキュリティ戦略本部が指定する法人

(※2) 情報通信、金融、航空、鉄道、電力、ガス、医療、水道、物流、化学、クレジット、石油 等

(※3) 受講者数は速報値。

全国で全100回開催、計3009名が受講

2020東京大会に向けたサイバー演習

2020年東京オリンピック・パラリンピックを想定した大規模演習基盤による演習の実施 (“サイバー・コロッセオ”)

イメージ図



具体的内容

- 大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築。
- 当該システムにより、大会開催時に想定されるサイバー攻撃を再現し、大会組織委員会のセキュリティ担当者を中心に、攻撃・防御手法の検証及び訓練を行う。

大規模な演習を実施し、2020東京大会のサイバーセキュリティを確保

サイバーコロッセオの演習内容

○ 受講者の習熟度や業務の性質等に応じて、**初級・中級コース又は準上級コースを開催。**

・ **初級・中級コース**（CSIRT（※）アシスタントレベル・CSIRTメンバーレベル）
オンライン学習（1時間程度）、機能演習（1日）

・ **準上級コース**（データ解析者レベル）
高度セキュリティ講義（1日）、機能演習（1日程度）

（演習終了後一定期間、職場等から演習環境に接続できるようにし、継続的な復習が可能）

（※）CSIRT：Computer Security Incident Response Team

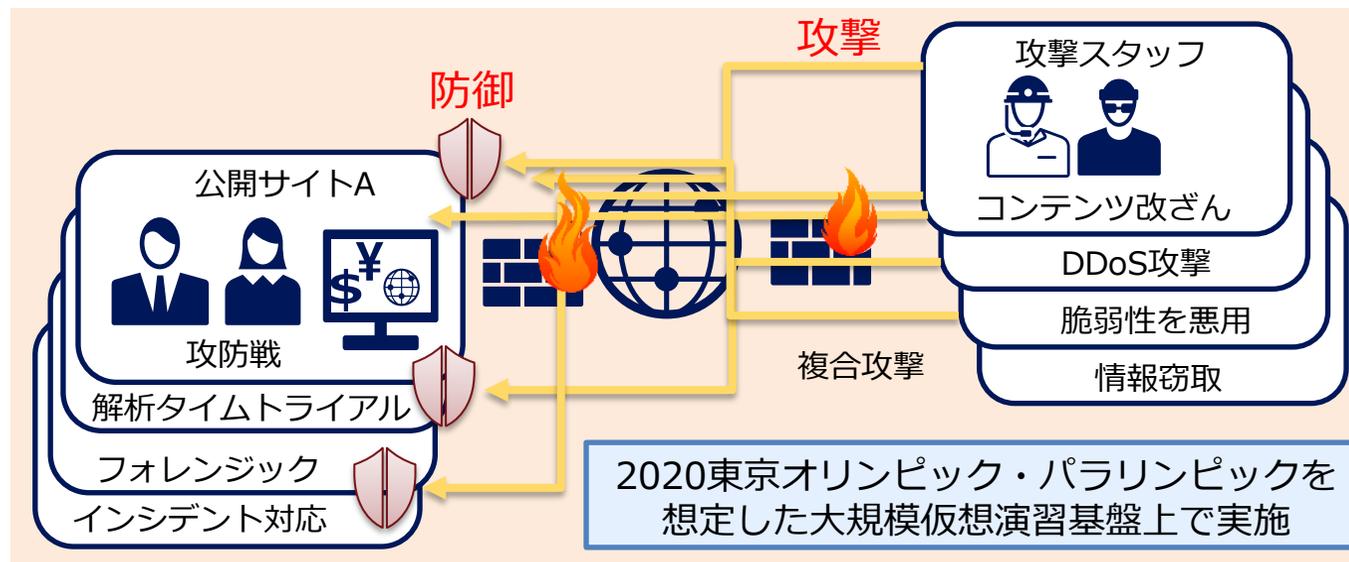
演習シナリオイメージ

受講者の習熟度や担当業務の性質等に応じた多様な実践的トレーニング・プログラムを開発・実

施。
（例）

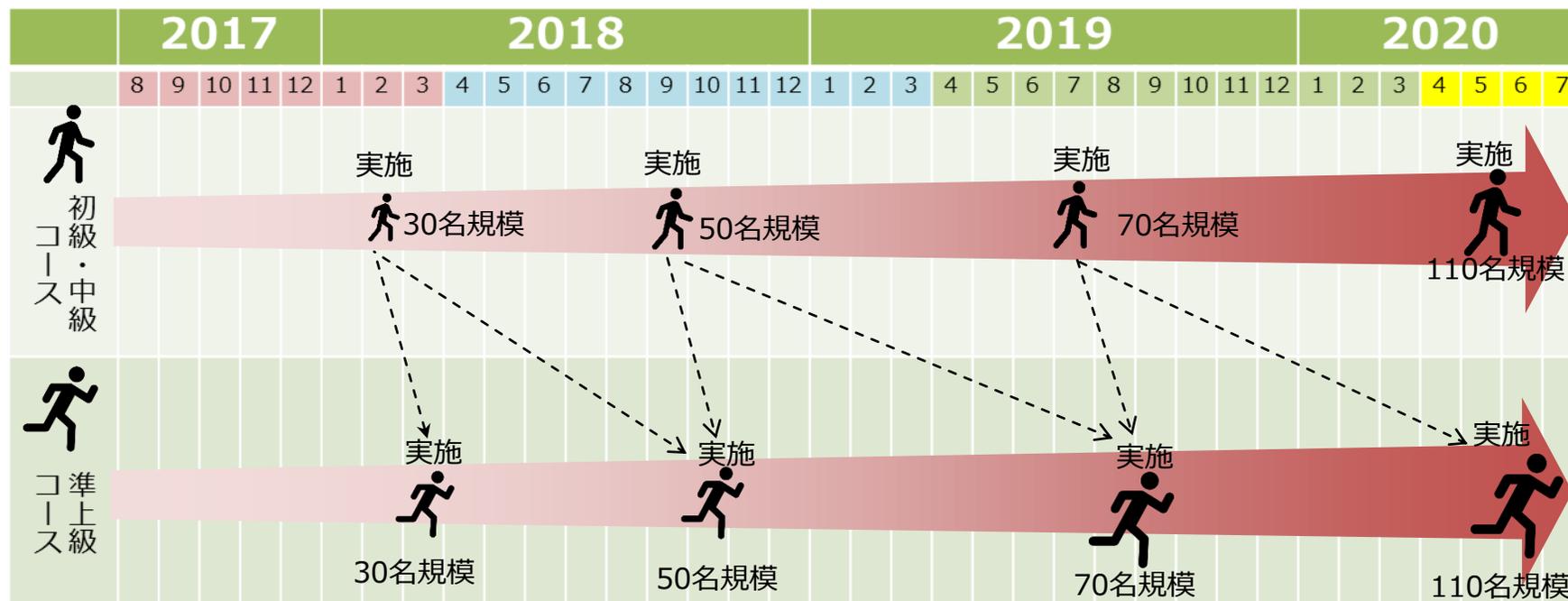
- Web系攻防戦
- ネットワーク系攻防戦
- フォレンジックチャレンジ
- 解析タイムトライアル
- インシデントレスポンス
+ BCP（※）最大化コンペ

（※）BCP：事業継続計画
（Business Continuity Plan）



サイバーコロッセオの実施スケジュール

- サイバーコロッセオは、東京大会開催までの3年間を通して継続的なトレーニングを実施。
- 回を経るごとにコンテンツを充実させていくとともに、参加人数についても段階的に規模を拡大していき、最終的には約220人のセキュリティ担当者等を育成する予定。
- 演習受講者は、サイバーコロッセオ演習会場（NICTイノベーションセンター（大手町））に集合し、仮想のネットワーク環境の上で、実際の機器やソフトウェアの操作を伴って、本格的な攻防戦等を繰り返し実施。

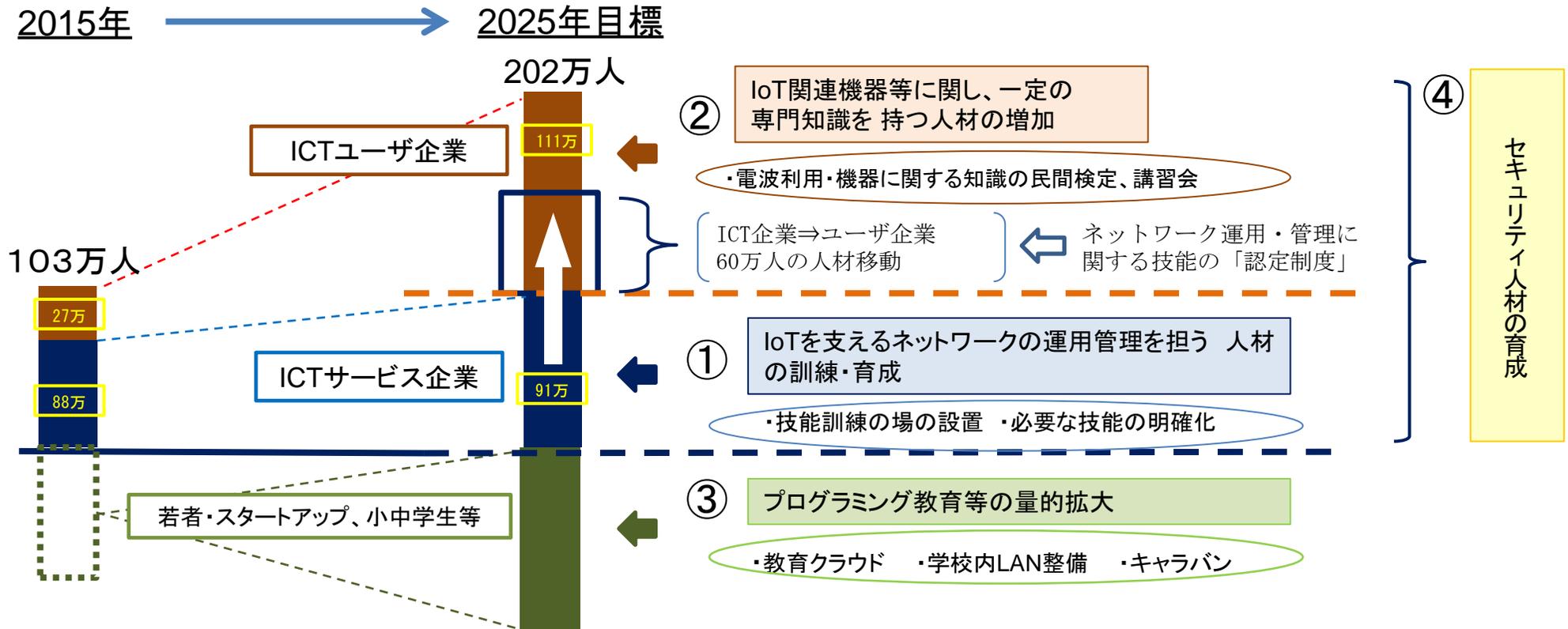


※ 目標人数は現時点において公益財団法人東京オリンピック・パラリンピック競技大会組織委員会（以下「組織委」という。）が想定する数字であり、今後、組織委側のニーズを踏まえつつ、必要に応じて見直しを行う予定。

- **未来のサイバーセキュリティ研究者・起業家の創出に向けて**、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導。**
- 対象者は、日本国内に居住する25歳以下の若手ICT人材（平成29年度は受講者として47名を選定。平成30年度も同程度を想定。）



IoT人材育成の必要性



(出典) 情報通信審議会 第2次答申「IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方」、IPA「IT人材白書2015」、総務省等「情報通信業基本調査報告書(平成28年3月)」等より推計

脆弱性対策に係る体制の整備

- ・ IoT機器の脆弱性についてライフサイクル全体(設計・製造、販売、設置、運用・保守、利用)を見通した対策が必要。
- ・ 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- ・ セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

人材育成の強化

- ・ 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

民間企業等におけるセキュリティ対策の促進

- ・ 民間企業等のサイバーセキュリティに係る投資を促進。
- ・ サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

国際連携の推進

- ・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証(関係府省と連携)

“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.”(サイバー空間における国家主権、平和的紛争解決等)

“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.”(国際法はサイバー空間に適用可能)

“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.”(サイバー空間における違法行為等への関与の禁止)

“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.”(サイバー空間を巡る議論における国連の主導的役割)

(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)

米国政府における攻撃元(Attribution)の特定

サイバー抑止戦略(Report on Cyber Deterrence Policy, White House, Dec. 2015)

- 1) 否定による抑止(Deterrence by denial)
- 2) コストを課すことによる抑止(Deterrence through cost imposition)

事案	攻撃発生時期	攻撃国	概要	米国政府の対応
大手企業からの機密情報窃盗	2006年～2014年	中国	人民解放軍のサイバー攻撃部隊が米国の原子力発電、鉄鋼などの大手企業のシステムに侵入し、技術や設計の機密情報を盗んだ。	2014年5月19日司法長官が記者会見において、起訴罪状を公表。中国人民解放軍のサイバー部隊である「第61398部隊」の将校ら5人を起訴。
ソニー・ピクチャーズへのサイバー攻撃	2014年11月	北朝鮮	「平和の守護神」と名乗るグループがソニー・ピクチャーズ・エンターテインメント社のコンピュータシステムを攻撃し、個人情報や未公開映画等のデータを盗んだ。	2014年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日追加的な経済制裁を実施。
銀行等、ダムへのサイバー攻撃	2011年～2013年	イラン	イラン政府の命を受けたイランのセキュリティ企業社員が米国金融機関46社にDDoS攻撃を仕掛け、またニューヨークのダム制御システムに不正にアクセス。	2016年3月24日司法省が、イラン人7人が起訴されたと発表。
Yahoo.comの情報漏えい	2014年1月～2016年12月	ロシア	2016年9月22日に米ヤフーが5億件の個人情報漏えいを公表。(2017年10月公表の30億件の漏えいとは別件)	2017年3月15日にロシア情報機関の職員等4人を起訴。
WannaCryによるサイバー攻撃	2017年5月12日	北朝鮮	150か国以上でランサムウェアの被害。英国では病院が感染し、しばらく治療ができなくなる事態に。	2017年12月19日北朝鮮の攻撃として非難。日英豪加ニュージーランドも同様に非難。

(注)各種報道に基づき作成。

優先アクション

■ プラール I 米国人、母国、米国の生き方を守る

- 米国の国境と領土を安全にする
- 脅威の出所を追及
- サイバー時代の米国の安全を維持
- 米国の回復力を促進

■ プラール II 米国の繁栄を促進

- 国内経済を活性化
- 自由、公正、相互経済関係を促進
- 研究、技術、発明、イノベーションを先導
- 米国国家安全保障基盤の推進と保護
- エネルギー支配の活用
(サイバー脅威からの保護)

■ プラール III 力を通じた平和

- 米国の競争力の優位性を取り戻す
- 能力を刷新する
軍事/防衛産業基盤/宇宙/**サイバー空間**/諜報

■ プラール IV 米国の影響力を高める

- 意欲的パートナー(途上国)への働きかけ
- 多国間フォーラムでのよりよい成果を達成
- 米国の価値感を守る

■ 地域的背景における戦略

- インド-太平洋 (北朝鮮の活動)
- 欧州 (サイバー協力強化)
- 中東 (イランの活動)
- 南部・中央アジア
- 西半球
- アフリカ

➤ **サイバー犯罪者対策**: 高度な調査ツールを使用し、不正な活動のために、オンラインマーケットプレイス、暗号通貨、その他ツールを犯罪者が使用する能力を除去。これらの**犯罪者をかくまう国に責任を取らせる**。

➤ **リスクの特定と優先順位付け**: 重要インフラのセキュリティと回復力を向上させるために、**国家安全保障、エネルギーと電力、銀行と金融、安全衛生、通信、輸送の6つの主要分野でリスクを評価**する。サイバー攻撃が致命的または多段的な影響を及ぼす可能性のある場所を評価し、それに応じて**保護活動、能力、防衛に優先順位を付す**。

➤ **政府の防衛可能なネットワークの構築**: 連邦政府の情報技術を近代化するために、**最新の商用機能、共有サービス、ベストプラクティスを使用**する。あらゆる状況下で、継続的で安全な通信とサービスの提供能力を向上させる。

➤ **サイバー犯罪者の活動阻止**: 政府は、**重要インフラ事業者が、攻撃を防止するために必要な権限、情報、能力を持つことを確保**する。**米国は、著しく悪意のあるサイバー活動を行う外国政府、犯罪者、その他の者に対して、迅速でかつ高価な代償を課す**。私たちは同盟国や友人と協力して、悪意のある行為に対する認識を深める。**より強く回復力のある重要インフラは、敵対者の目的達成に疑念を抱かせ、抑止力が強化される**。

➤ **情報の共有と検知の向上**: 米国政府は、重要インフラ事業者と協力して、**情報のニーズを評価し、また、迅速性や機密レベルなど情報共有の障壁を低減**する。また、**アトリビューション(攻撃の属性付け)能力を向上**させる。市民の自由とプライバシーの保護を考慮した上で、民間部門との協力関係を拡大し、攻撃をよりよく検出し属性付けができるようにする。

➤ **階層化防御の導入**: 米国政府は民間部門と協力して、**ネットワークレベルで既知の悪質な活動を阻止し、すべての顧客のセキュリティを向上**させる。

➤ **アトリビューション、責任、および対処の改善**: **サイバー攻撃の属性を明らかにし、迅速な対応を可能にするための能力を、維持し改善するために投資**する。

➤ **サイバーツールと専門知識の向上**: 政府の資産と重要インフラを保護し、データと情報の完全性を保護するために、様々な事案において利用される**サイバーツールを改良**する。政府機関は、このような様々な活動の範囲内で業務を行うことができる**人材を採用し、育成し、雇用を維持**する。

➤ **統合と迅速性の向上**: 米国政府の権限と手続きの**統合を向上**させ、敵対者へのサイバー対応を要求に応じて実施できるようにする。**議会と協力して、タイムリーな諜報と情報の共有、計画と運営、必要なサイバーツールの開発への継続的な妨害という課題に対処**する。

2017年12月19日 米国政府(ボサード大統領補佐官)

- ・米国はWannaCryによる大規模サイバー攻撃が北朝鮮によるものと断定。
- ・サイバーリスク上の脅威を軽減するとともに、米国を守ることでハッカーのコストを増加させるよう、政府や企業に対する協力が必要。
- ・英国、豪州、カナダ、ニュージーランド及び日本が米国の分析を精査し、米国とともに北朝鮮によるWannaCryの攻撃を非難。
- ・民間企業も同様に行動し、マイクロソフトは攻撃の出所が北朝鮮体制のサイバー関係者であることを突き止めたほか、他のセキュリティ企業もこの分析に貢献。

2017年12月19日 マイクロソフト社

- ・WannaCryと呼ばれるマイクロソフトの顧客を狙った破壊的な攻撃について、北朝鮮系ハッカーグループであるラザルスグループに責任。
- ・このグループが依拠するマルウェアの破壊を助け、顧客の感染コンピュータを掃除し、攻撃に利用されたアカウントを使用不能とするとともに、再感染防止のためウィンドウズの防御強化を実施。

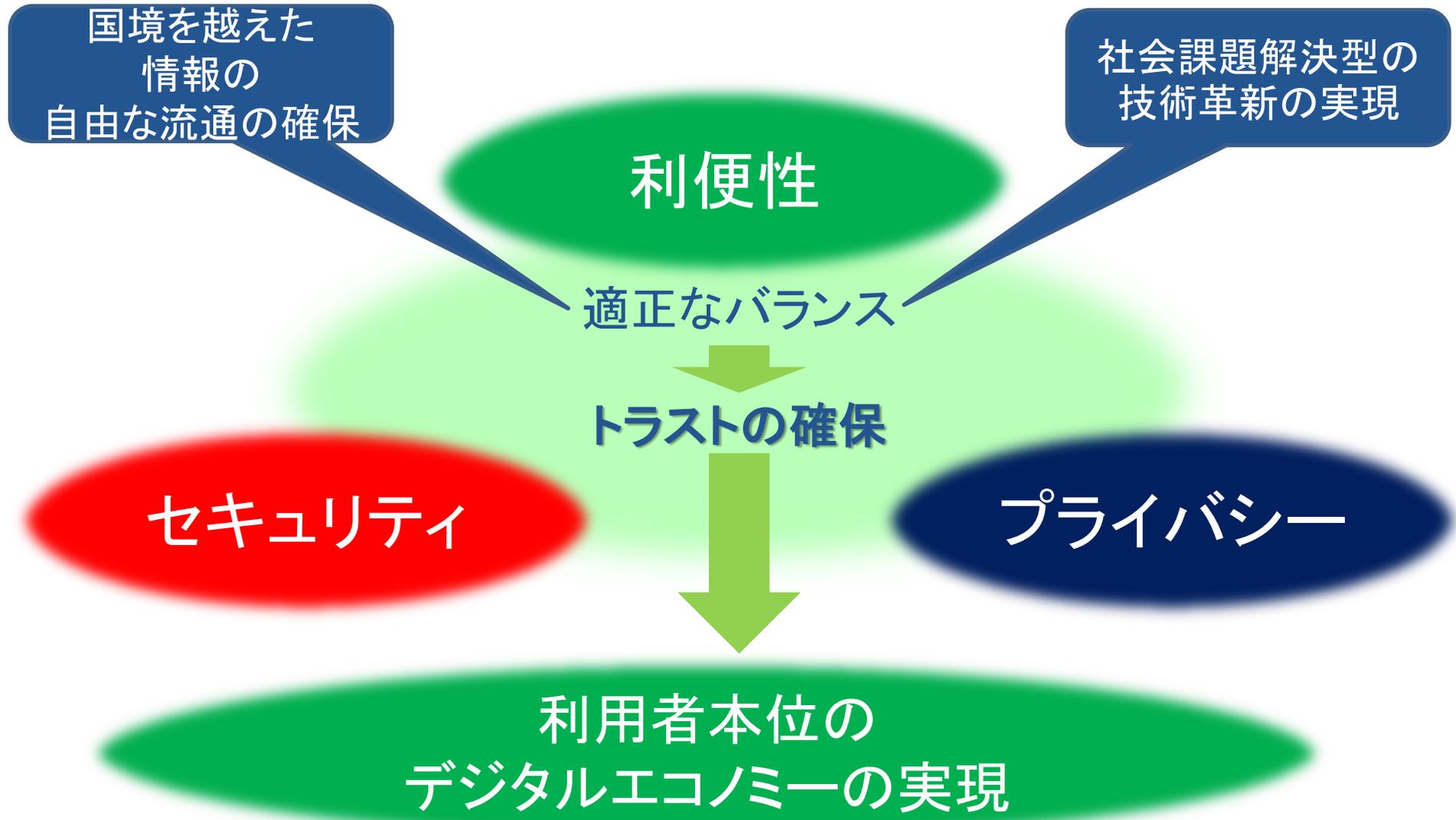
2017年12月20日(日本時間) 我が国政府(外務報道官談話)

- ・サイバー空間の安全の確保に向けた強い意志を示す今回の米国の発表を支持。
- ・我が国としてもWannaCry事案の背後に、北朝鮮の関与があったことを非難。

- **二国間ベースのサイバー政策対話**を通じた、ベストプラクティスの共有、情報共有の促進、二国間の官民連携の推進を進めることが必要。
- **サイバー空間における国際法の適用**等については、特に**有志国との連携強化**が必要。
- データローカライゼーション等の動きをけん制し、**「情報の自由な流通」**を二国間・多国間の枠組みで維持していくことが必要。
- マルチステークホルダープロセスを基盤とし、**自由で開かれたインターネットガバナンスの確保**を目指す（セキュリティ確保を理由とするサイバー空間への国家の不当な介入の防止）。

(参考) G7タオルミナ首脳コミュニケ(2017年5月)

“The recent cyber attacks hitting critical infrastructures worldwide reinforce our commitment to increased international cooperation to protect an accessible, open, interoperable, reliable and secure cyberspace and its vast benefits for economic growth and prosperity. We will work together with our partners to tackle cyber attacks and mitigate their impact on our critical infrastructures and the well-being of our societies.”



Any Question?



総務省