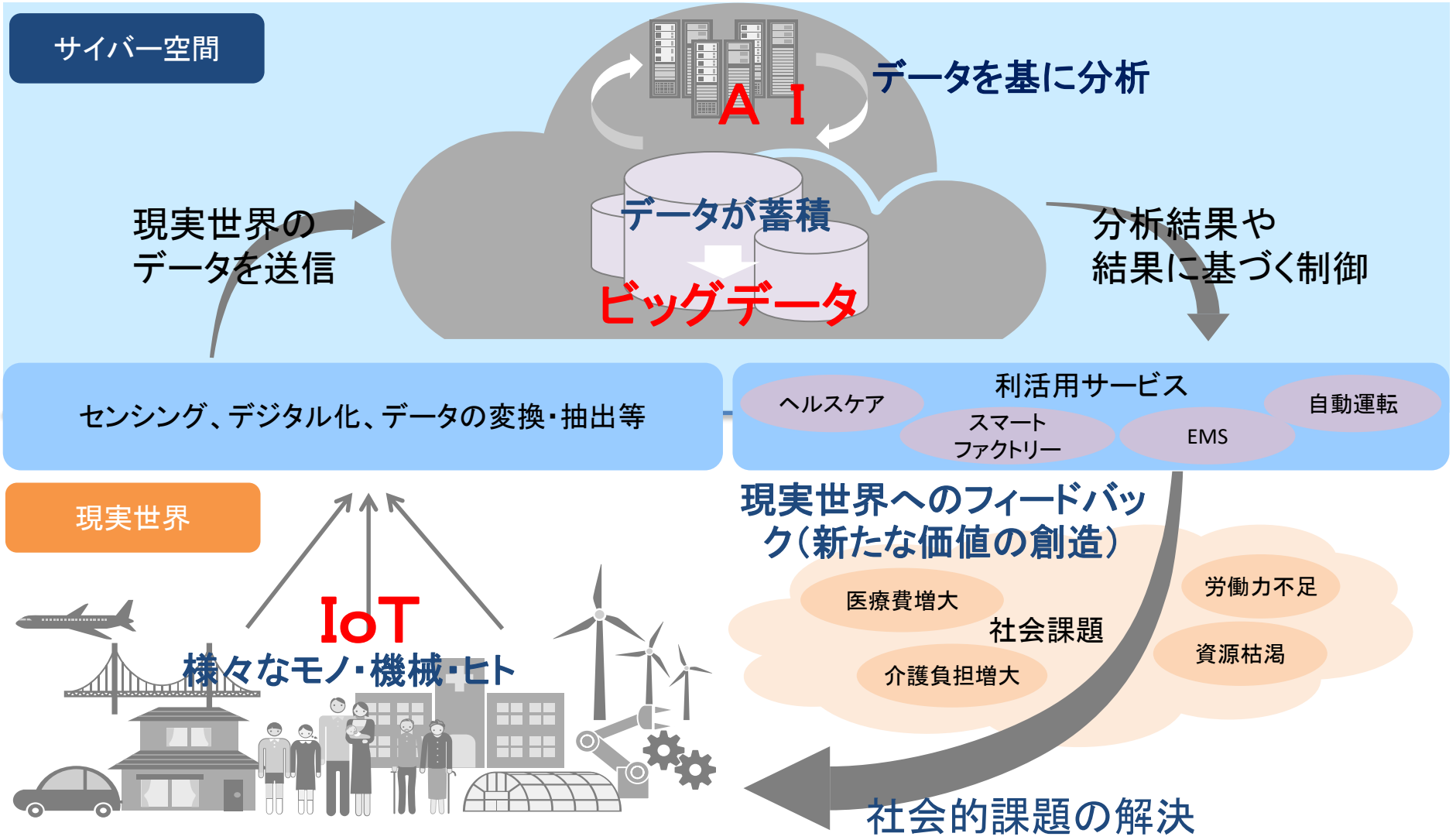
総務省

データ主導社会とサイバーセキュリティ

２０１８年1月２４日

総務省政策統括官（情報セキュリティ担当）
谷脇　康彦

データ主導社会


サイバー空間
AI
データを基に分析
現実世界の
データを送信
データが蓄積
ビッグデータ
分析結果や
結果に基づく制御
センシング、デジタル化、データの変換・抽出等
利活用サービス
ヘルスケア
スマート
ファクトリー
EMS
自動運転
現実世界
IoT
様々なモノ・機械・ヒト
現実世界へのフィードバック（新たな価値の創造）
医療費増大
介護負担増大
社会課題
労働力不足
資源枯渇
社会的課題の解決

未来投資戦略2017（17年6月）

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

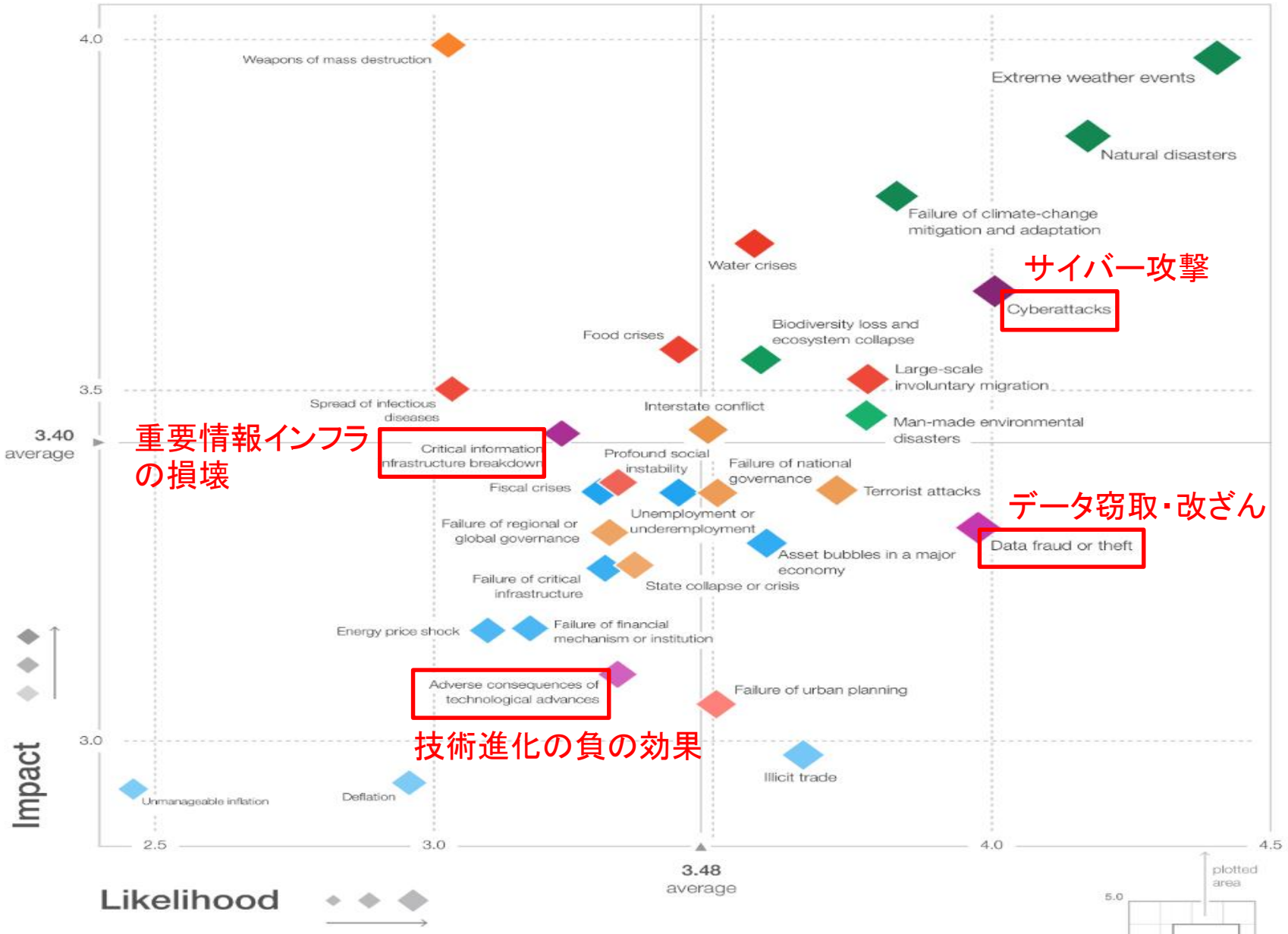
価値の最大化を後押しする仕組み

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

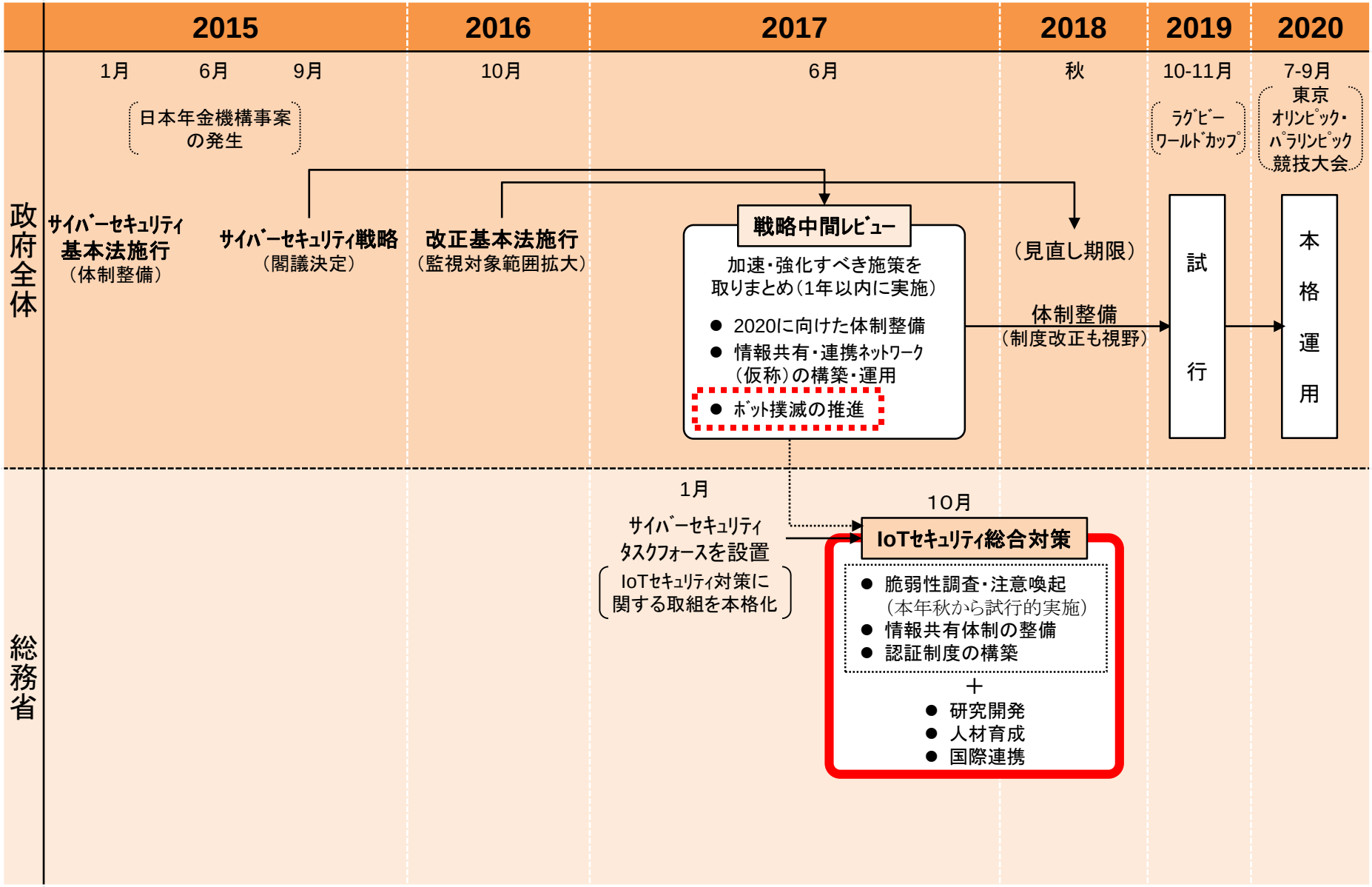
Ⅳ. 海外の成長市場の取り組み

グローバルリスクに対する評価（WEF2018）

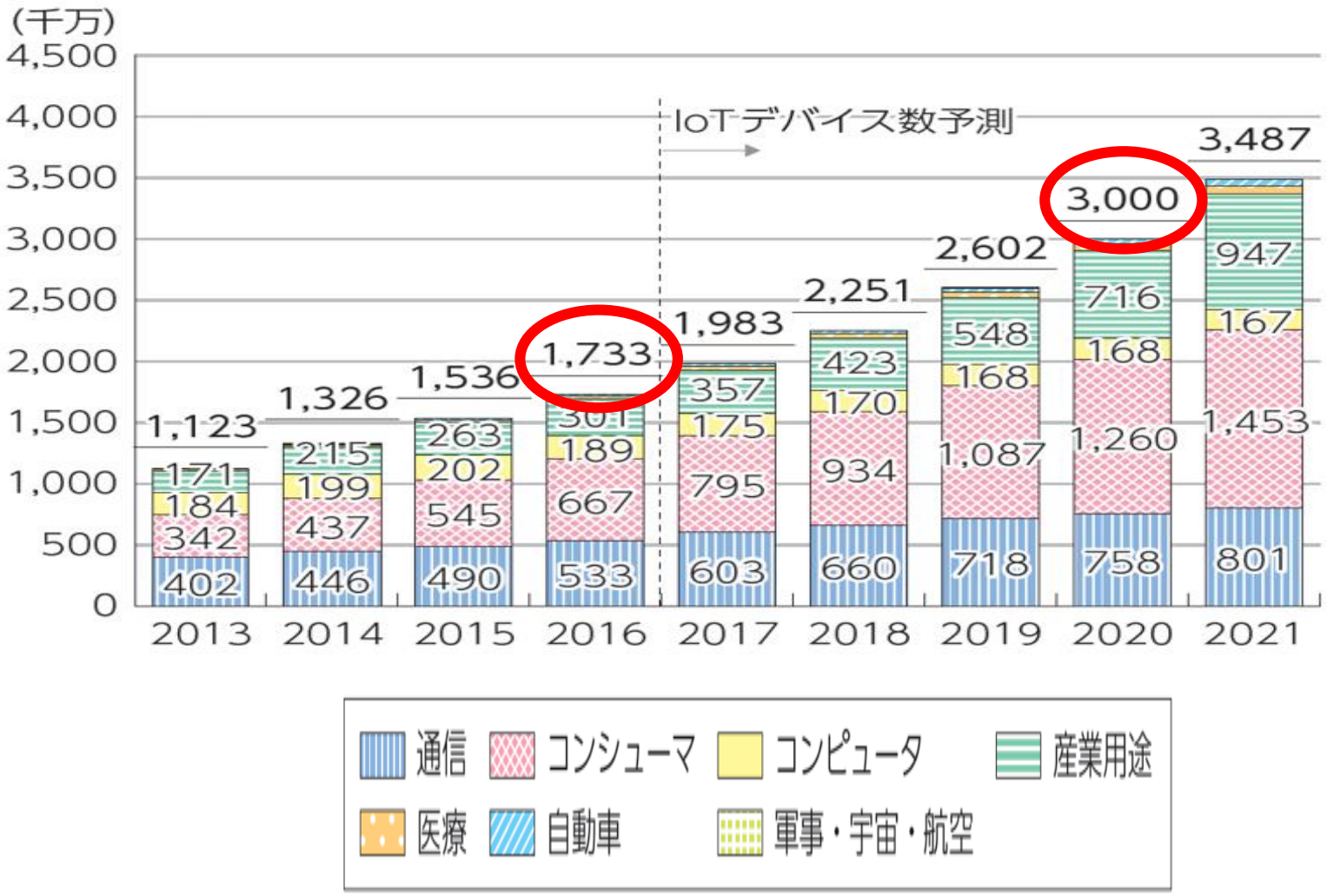


（出典）World Economic Forum “The Global Risks Report 2018 13th Edition” (January 2018)

サイバーセキュリティ対策関連スケジュール

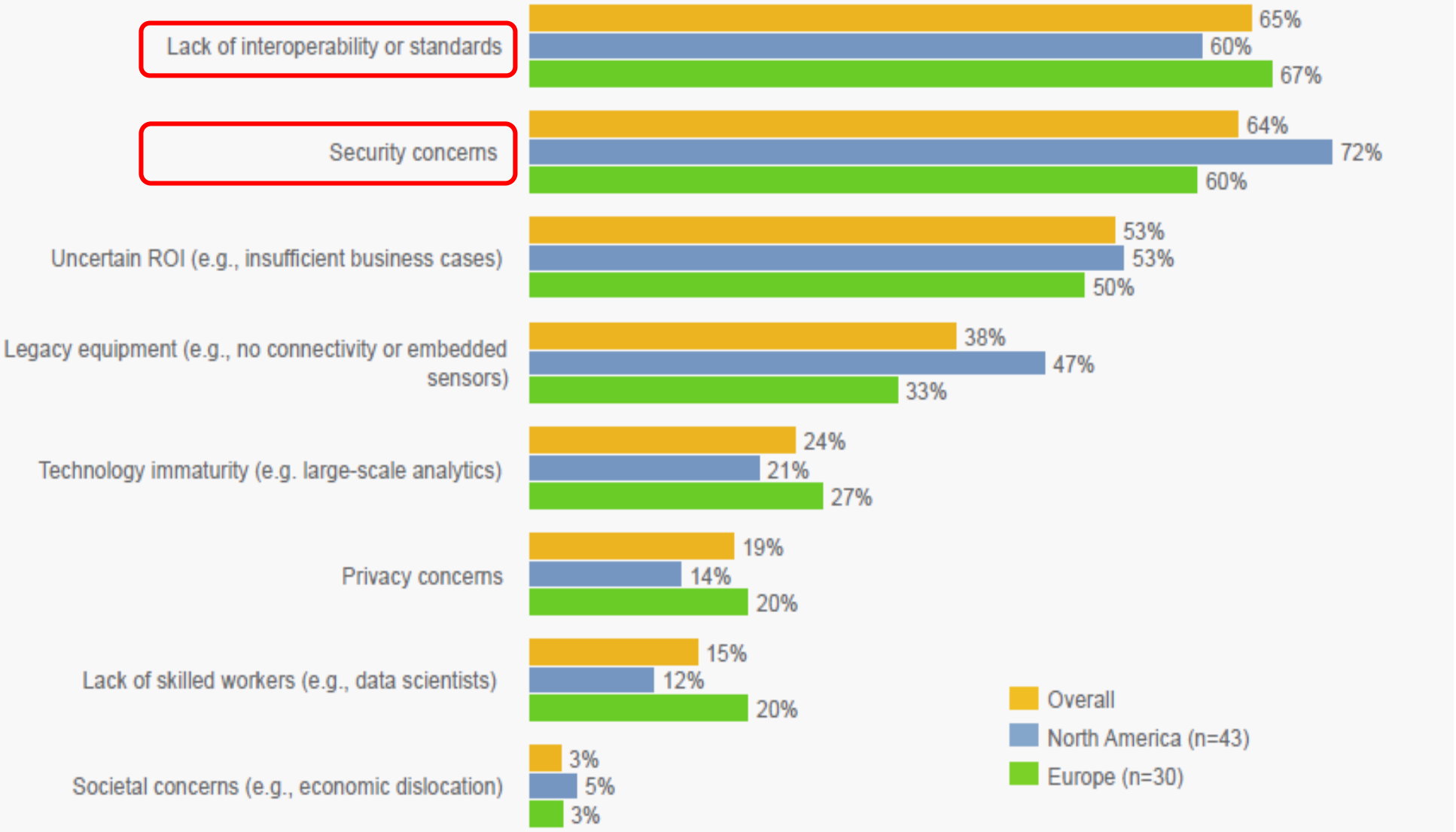


IoT機器の幾何級数的な増加



（出典）HIS Technology

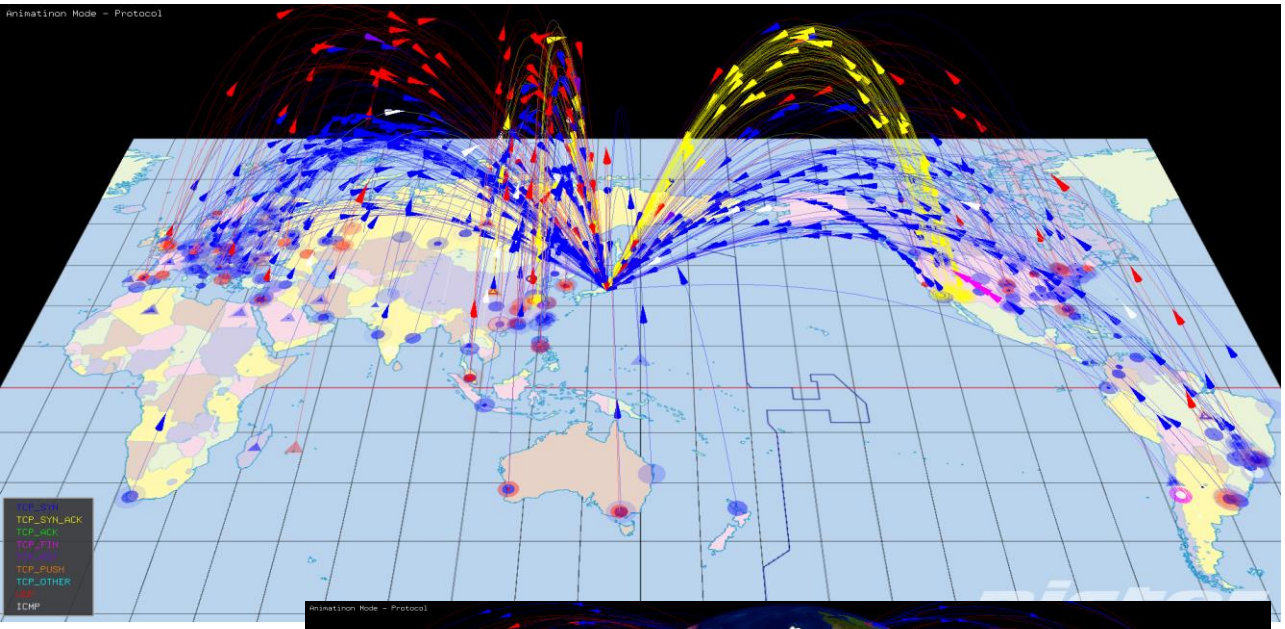
IoT普及促進の鍵となるセキュリティ

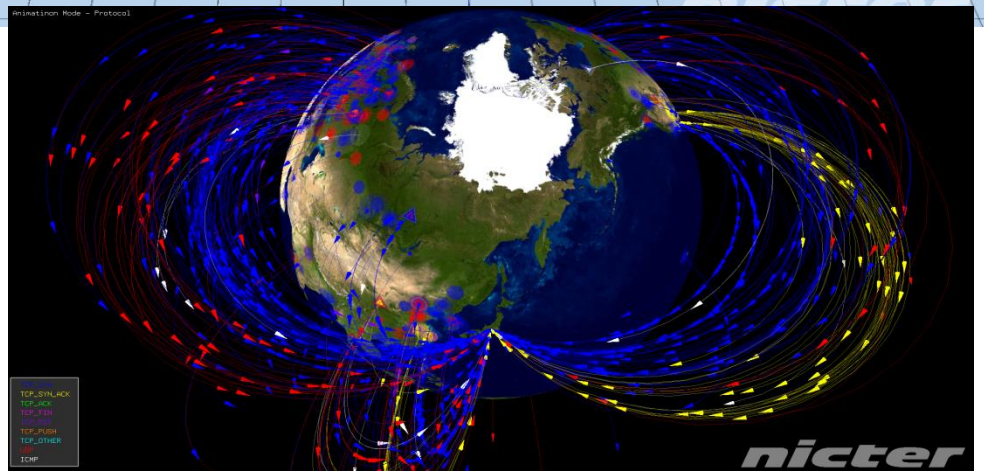


（Source)World Economic Forum, “Industrial Internet of Things : Unleashing the Protection of Connected Products and Services” (January 2015)

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。



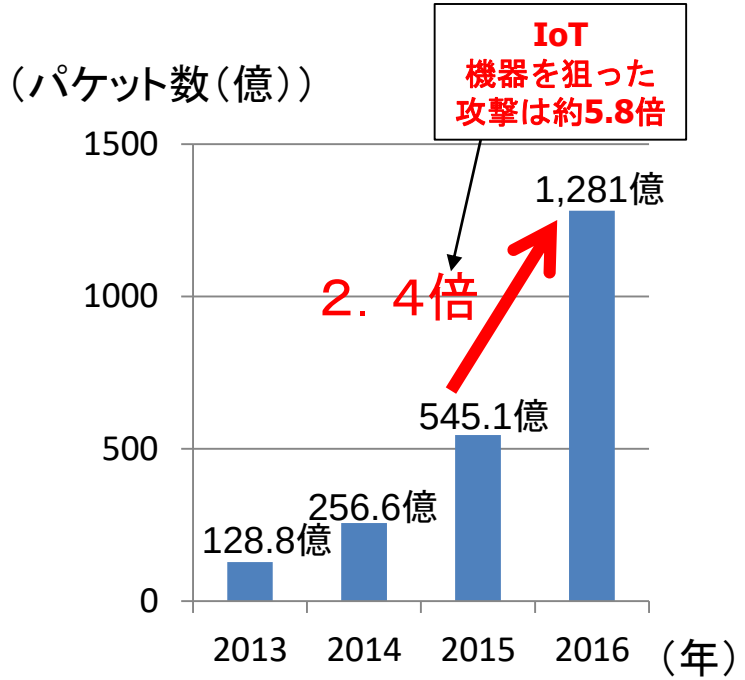


- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・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

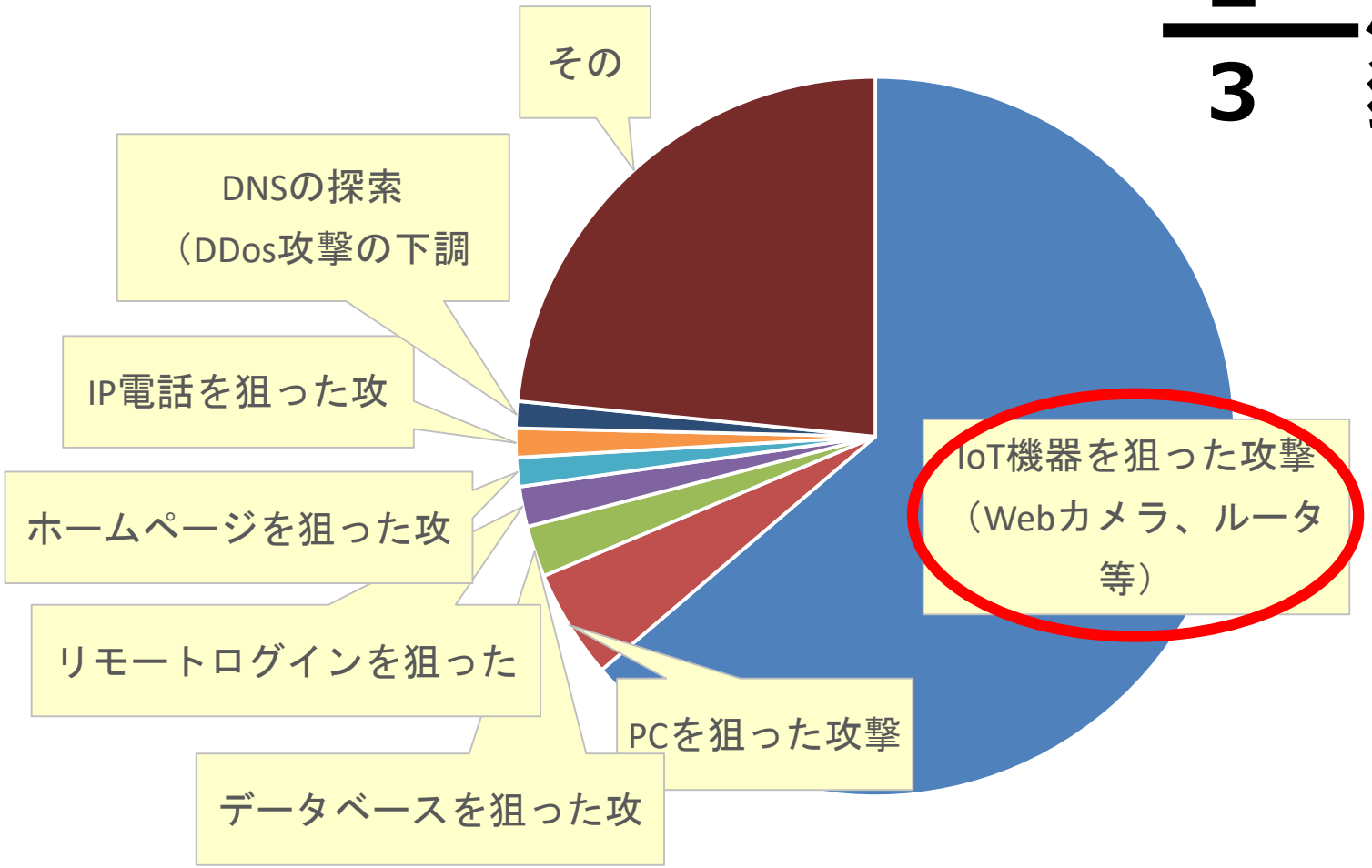
1年間で観測されたサイバー攻撃回数



サイバー攻撃の内訳（16年、NICTERによる観測）

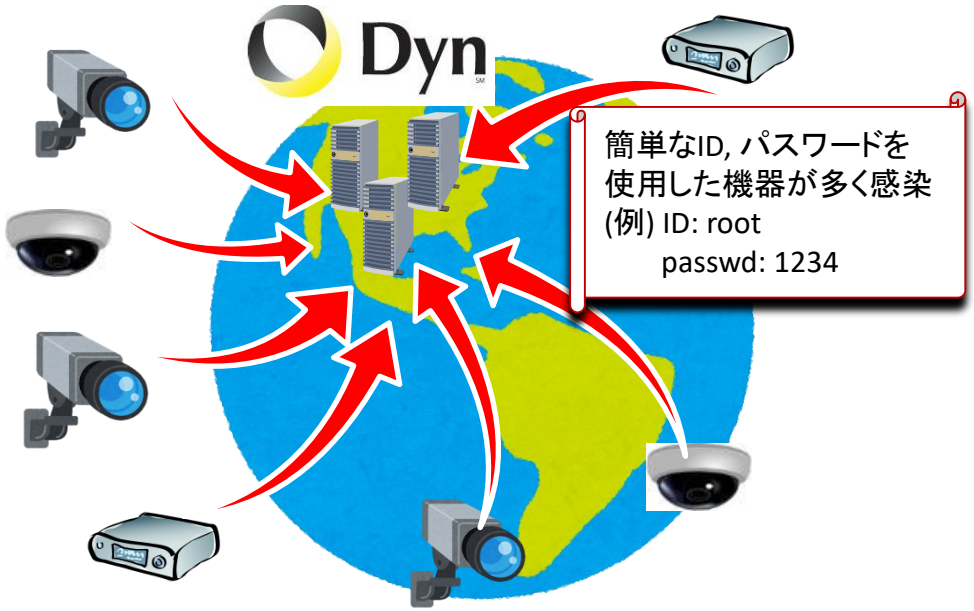
観測された全サイバー攻撃1,281億パケットのうち、

2/3がIoTを狙っている！



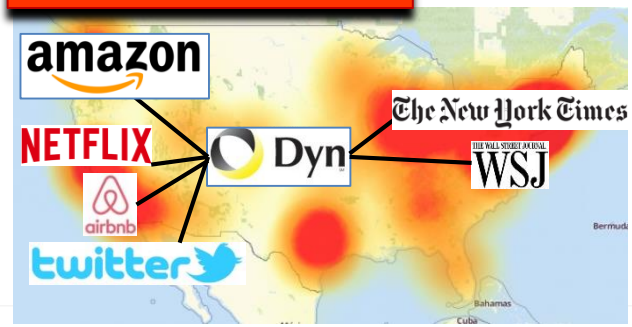
IoTによる大規模DDoS攻撃

- 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。
- 同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。



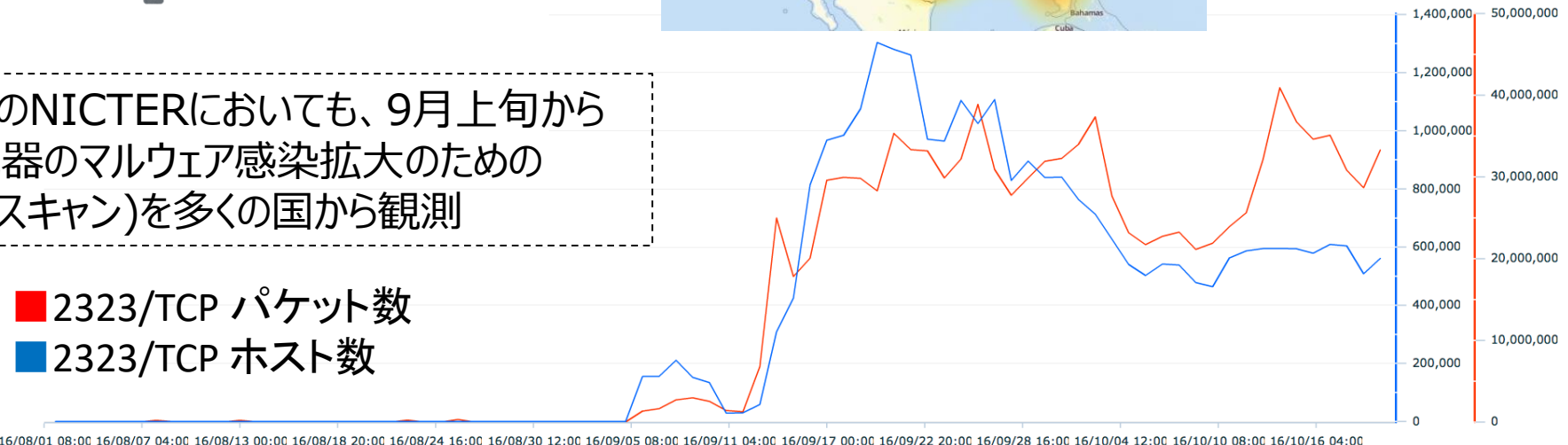
- ✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生
- ✓ 最大で1.2Tbpsに達したとの報告もあり。

システムダウンの状況

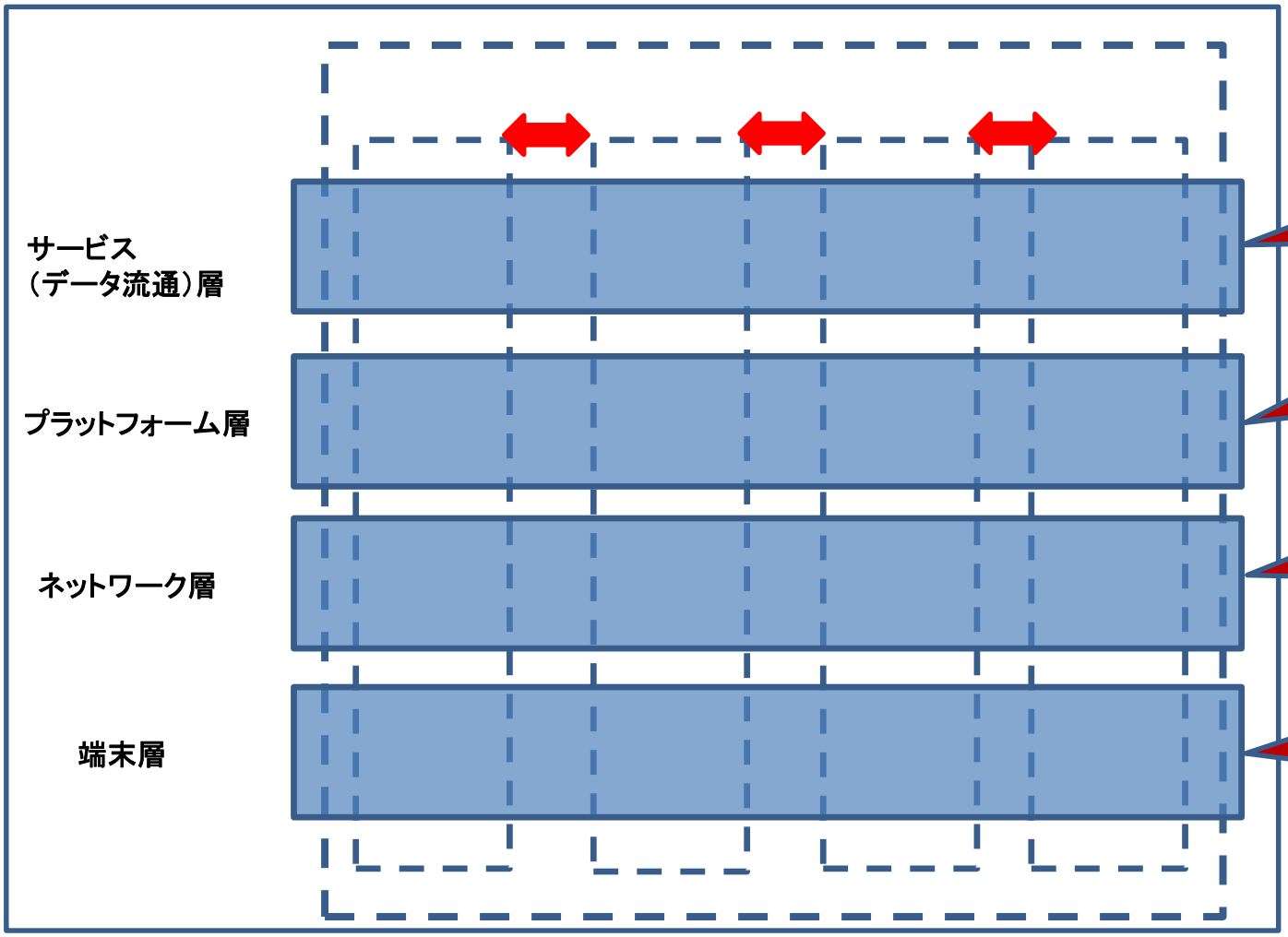


Dyn社のDNSサービスを使用した数多くのインターネットサービスやニュースサイトに影響

- ✓ NICTのNICTERにおいても、9月上旬からIoT機器のマルウェア感染拡大のための通信(スキャン)を多くの国から観測



IoTシステム（System of Systems）とサイバーセキュリティ



IoTシステムは社会基盤として機能

■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

IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策：脆弱性対策に係る体制の整備

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

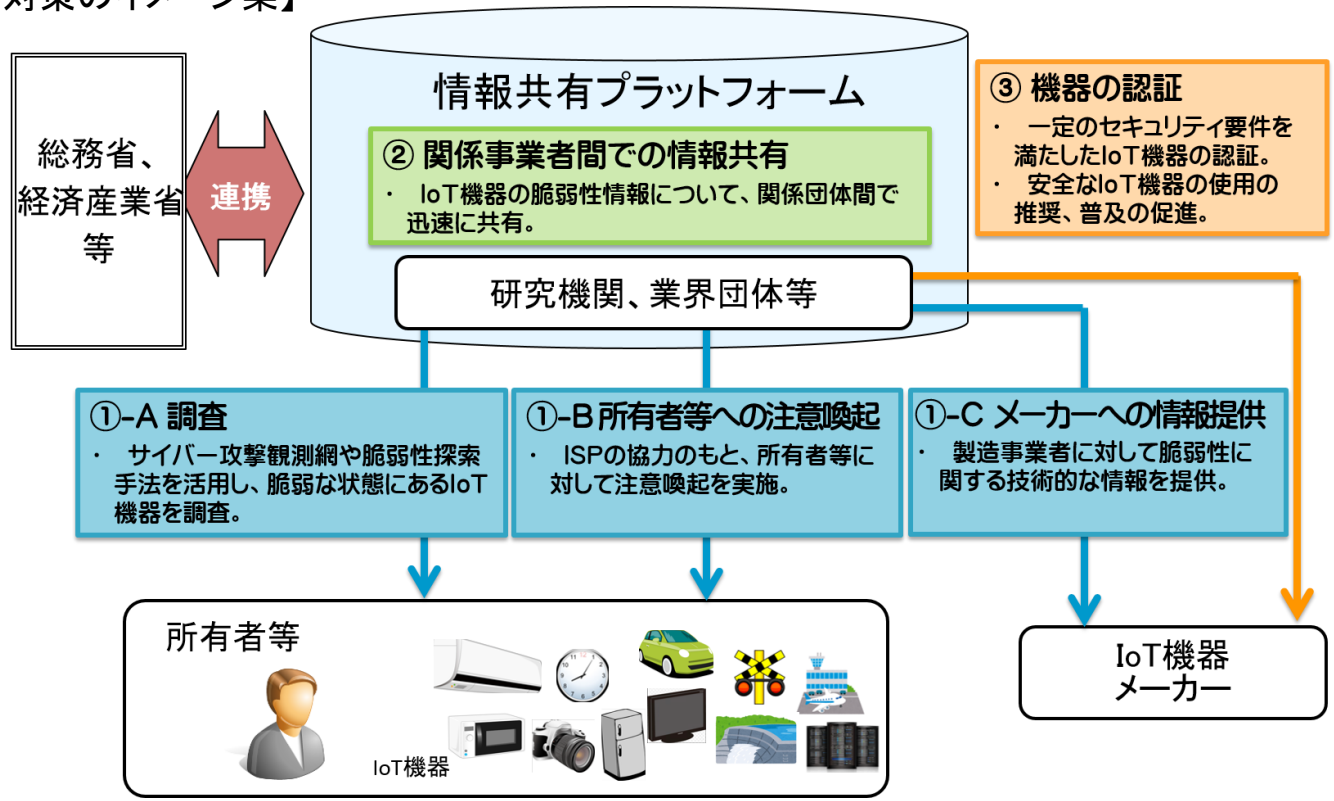
■ **利用者に対する意識啓発の実施や相談窓口等の設置**

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

脆弱性対策に係る体制の整備（脆弱性調査の実施）

■ 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

【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）。

欧米におけるIoT機器セキュリティ認証に関する動向

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(済)、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。

国家安全保障電気通信諮問委員会(NSTAC)勧告(2017年11月)

■11月16日、NSTAC(National SecurityTelecommunications Advisory Committee)は“Report to the President on Internet and Communications Resilience”(ボットネット対策勧告案)を承認。
→DHSのHPにおいて公開。

(関連部分抜粋)

○IoT端末セキュリティガイドラインの策定-----商務省は端末セキュリティを確保するため、任意の端末認証や独立した検査の役割・可能性について検討すべき。

・NSTACは特定のセキュリティポリシーの認証のためのUnderwriters Lab (UL)の設立を検討すべきである旨、過去に提言。NSTACは、国際標準に基づく産業界主導のIoT端末認証が有益であるとの結論を支持。

○連邦、州、国際的なセキュリティ要件の調和の追及-----国際的には、欧州、日本、中国、その他の国でIoT端末認証と検査の開発を視野に入れている。米国政府は、継続的な相互運用可能なIoTセキュリティ標準の確保に努めるべき。

○SDN/ネットワークスライス/仮想化-----ネットワークスライス技術を使えば、一つの物理レイヤーを複数の仮想網に分け、通信事業者が多様なユーザーに多様なサービスを提供可能で、フィルタリング、ルーティング、プロトコル制御等が可能。

米国・ボットネット対策に関する報告書案（2018年1月）（1/2）

■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 Agaist 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

米国・ボットネット対策に関する報告書案（2018年1月）（2/2）

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---NISC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）政府調達の具体化が必要。

5つのゴールを達成するための23の行動計画を整理

IoTサイバーセキュリティ改善法案（米国、2017年8月）

“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。

欧州ネットワーク情報セキュリティ機関(ENISA)の提言(2017年11月)

■ENISによるIoTの定義

“IoTとは、相互に接続されたセンサーやアクチュエータで構成される、意思決定を可能とするcyber-physical ecosystemである。”

■IoTセキュリティを向上させるためのハイレベルの勧告

1. IoTセキュリティに関する取り組みや規制の調和の促進
2. IoTセキュリティの必要性に関する意識啓発の推進
3. IoTに関するセキュアなソフト・ハード開発のライフサイクルガイドラインの策定
   - ”security & privacy by default”と”security & privacy by design”が基本。
   - IoTにおけるサイバーリスクは”context-dependent”であることに留意。
4. IoTエコシステムを縦断する相互運用性に関するコンセンサスの醸成
   - 相互運用可能なセキュリティを確保するためのオープンな枠組みの促進
   - 相互運用可能な枠組みのセキュリティに関する透明性の確保
   - 相互運用性に関するラボラトリーやテストベッドへのオープンでアクセス可能な環境の促進
5. IoTセキュリティのための経済的・行政的なインセンティブの育成
   - 認証やラベリングのような枠組みは、IoTセキュリティの理解と透明性の確保を促す。
6. セキュアなIoT製品・サービスのライフサイクル管理の確立
   - セキュリティ更新はIoTの文脈において重要な事項。これは提供約款に基づき、サポート終了までの間、消費者が特別な知識や金銭的な負担をすることなく提供されることが必要。
7. IoTのステークホルダー間の責任(liability)の明確化

(注)ENISA(European Union Agency for Network and Information Security), “Baseline Security Recommendations for IoT : in the context of Critical Information Infrastructures” (November 2017)

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

運営委員会　（15名）

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	三菱電機株式会社　代表執行役	須藤　修	東京大学大学院　教授
越塚　登	東京大学大学院　教授	堂元　光	日本放送協会　副会長
小柴　満信	JSR株式会社　社長	徳田　英幸	慶應義塾大学大学院　教授
齊藤　裕	株式会社日立製作所　副社長	野原　佐和子	イプシ・マーケティング研究所　社長
坂内　正夫	情報通信研究機構　理事長	程　近智	アクセンチュア株式会社 会長
志賀　俊之	産業革新機構　会長(CEO)	林　いづみ	弁護士
篠原　弘道	日本電信電話株式会社　副社長	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

先進的ﾓﾃﾞﾙ事業推進ＷＧ（IoT推進ラボ）
先進的なﾓﾃﾞﾙ事業の創出、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

2017年12月より検討

協力　協力

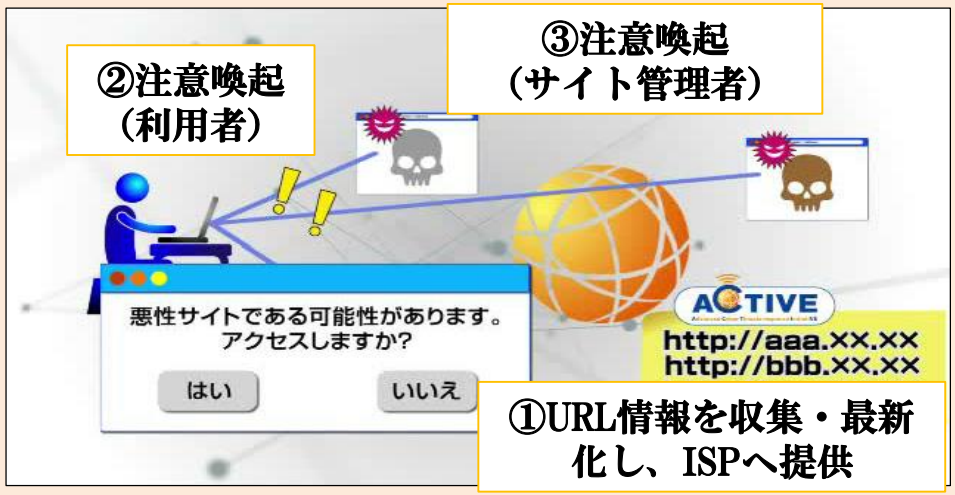
総務省、経済産業省　等

ウィルス感染被害予防対策“ACTIVE”

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

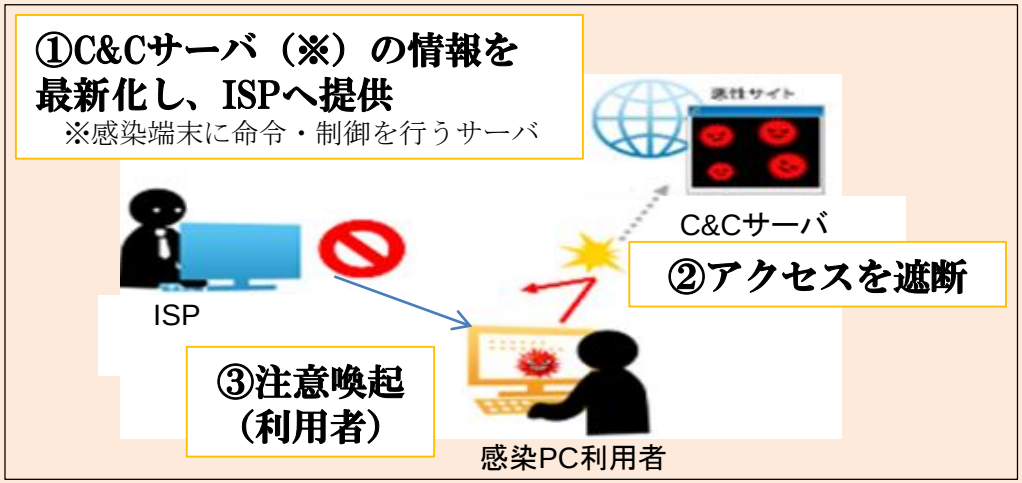


①マルウェア配布サイトのURL情報を最新化し、ISPへ提供。

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2017年10月までに約2億5,728万件の遮断実績）

③ 感染PC利用者に注意喚起。

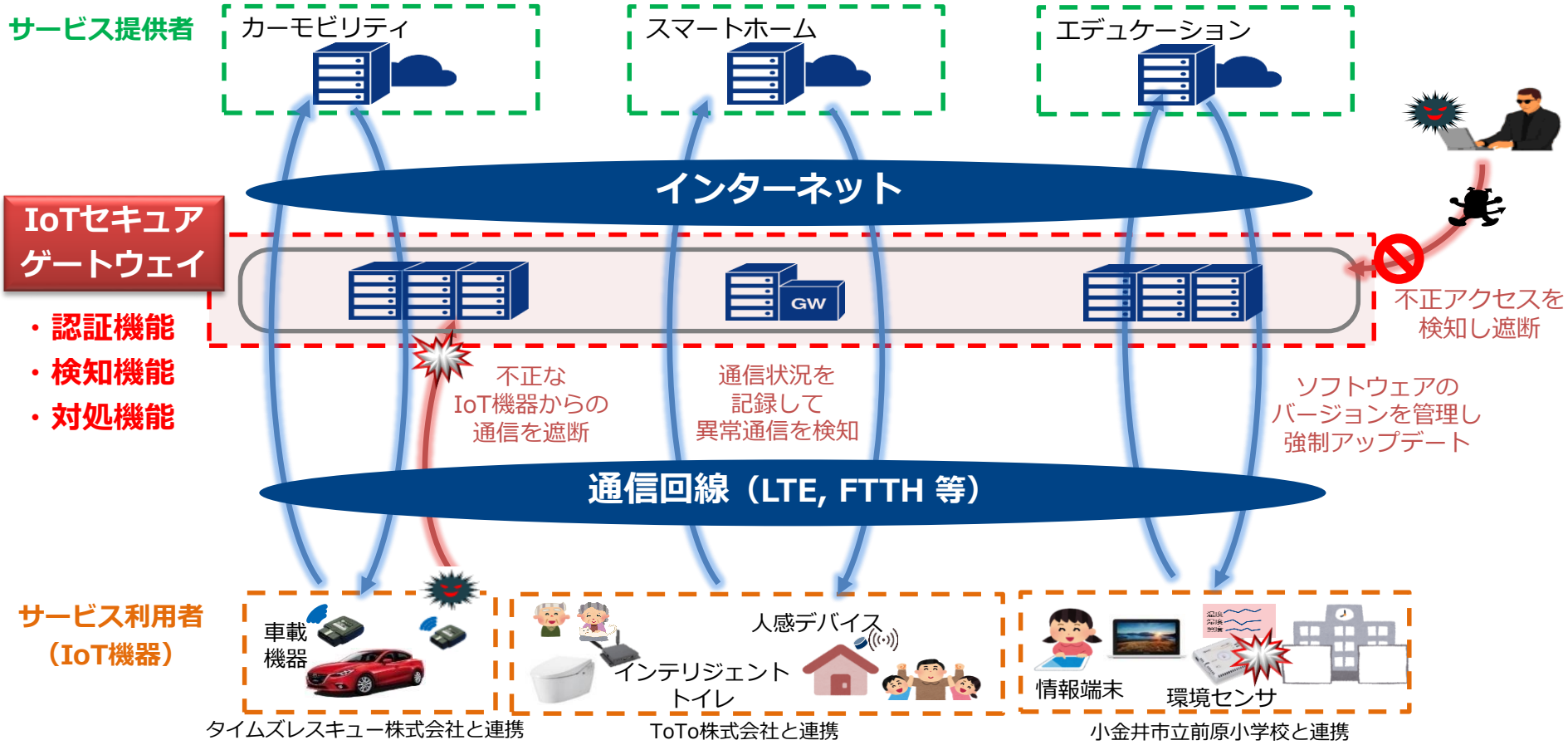
○ 実施期間：平成25～29年度

IoTセキュアゲートウェイの実証実験

- 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））



IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策：研究開発の推進

■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

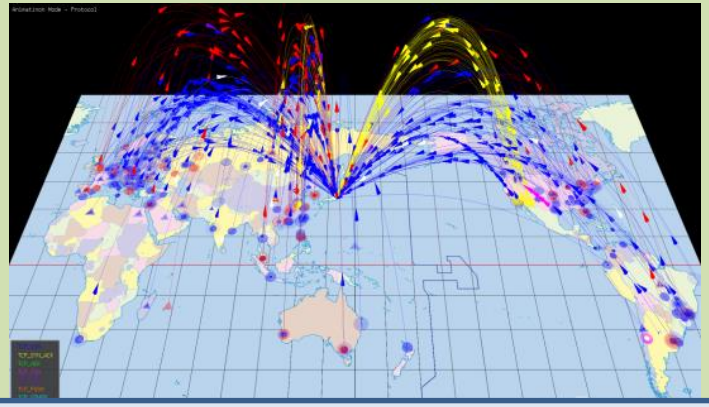
サイバー攻撃の検知・解析を自動化するような、AIを活用したサイバー攻撃検知・解析技術の研究開発を推進。

情報通信研究開発機構（NICT）におけるサイバーセキュリティ技術

■ 国立研究開発法人 情報通信研究機構（NICT）では、研究開発の一環として、サイバーセキュリティ技術の成果展開を実施。無差別攻撃型（マルウェア）対策技術については、多くの自治体に導入が進むとともに、年金機構に対しても使用された標的型攻撃対策についても、早期導入に向けた取り組みを推進。

◆NICTER（ニクター）【無差別型攻撃対策】

- ダークネット（未使用IPアドレス）への通信をセンサーで観測することで、サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化。
- 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、マルウェアに感染した自治体へアラートを提供。



602自治体に導入済み（平成28年10月時点）

◆NIRVANA改（ニルヴァーナ・カイ）【標的型攻撃対策】

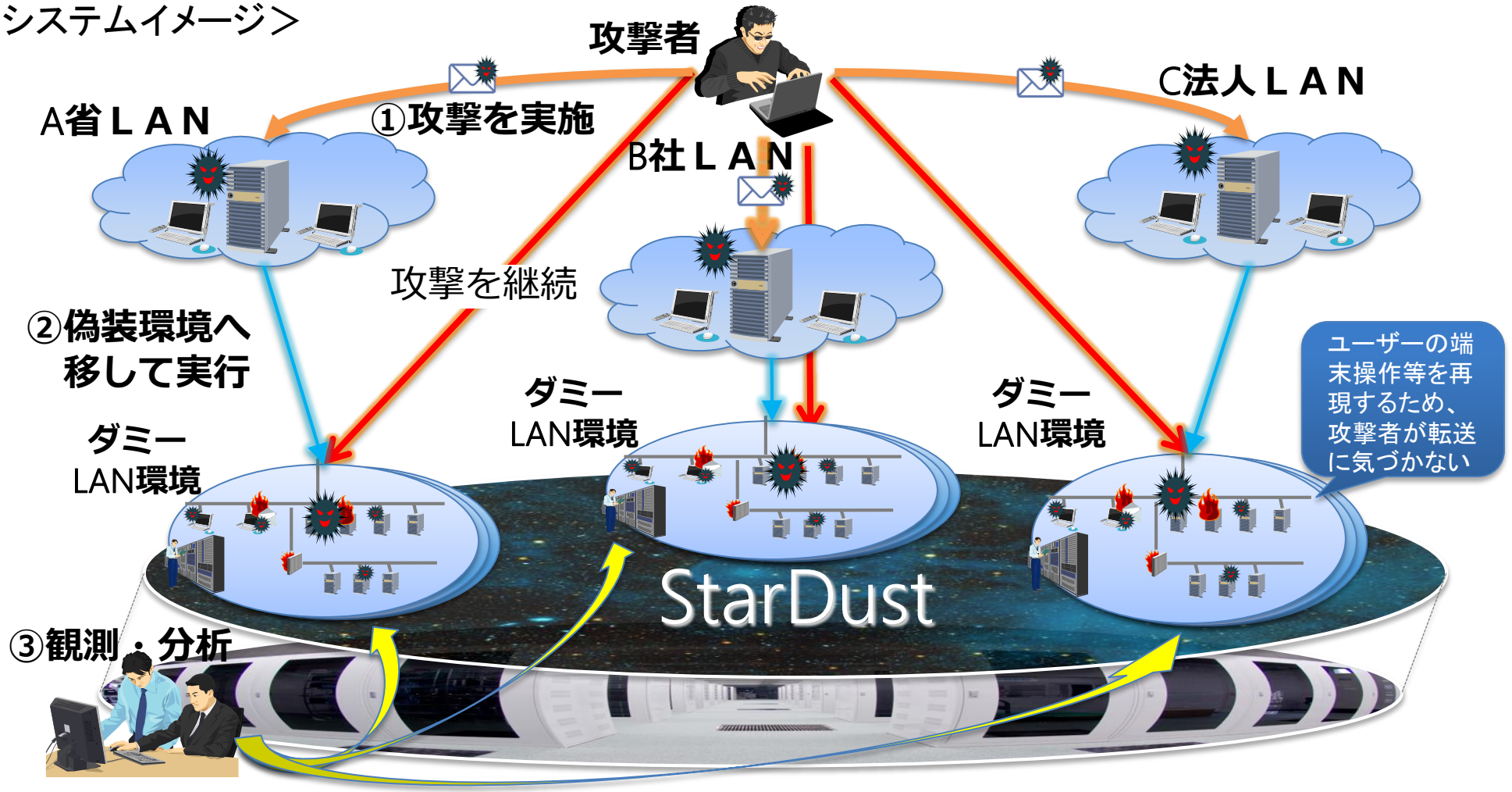
- NICTERの技術を応用し、組織内にセンサーを設置して組織内の通信状況をリアルタイムに可視化するとともに、本技術について2015年6月から技術移転開始。
- さらに、本技術と組み合わせ、ネットワーク内での異常検知時に通信を自動遮断する技術等を開発中。

技術移転を開始（平成27年6月）

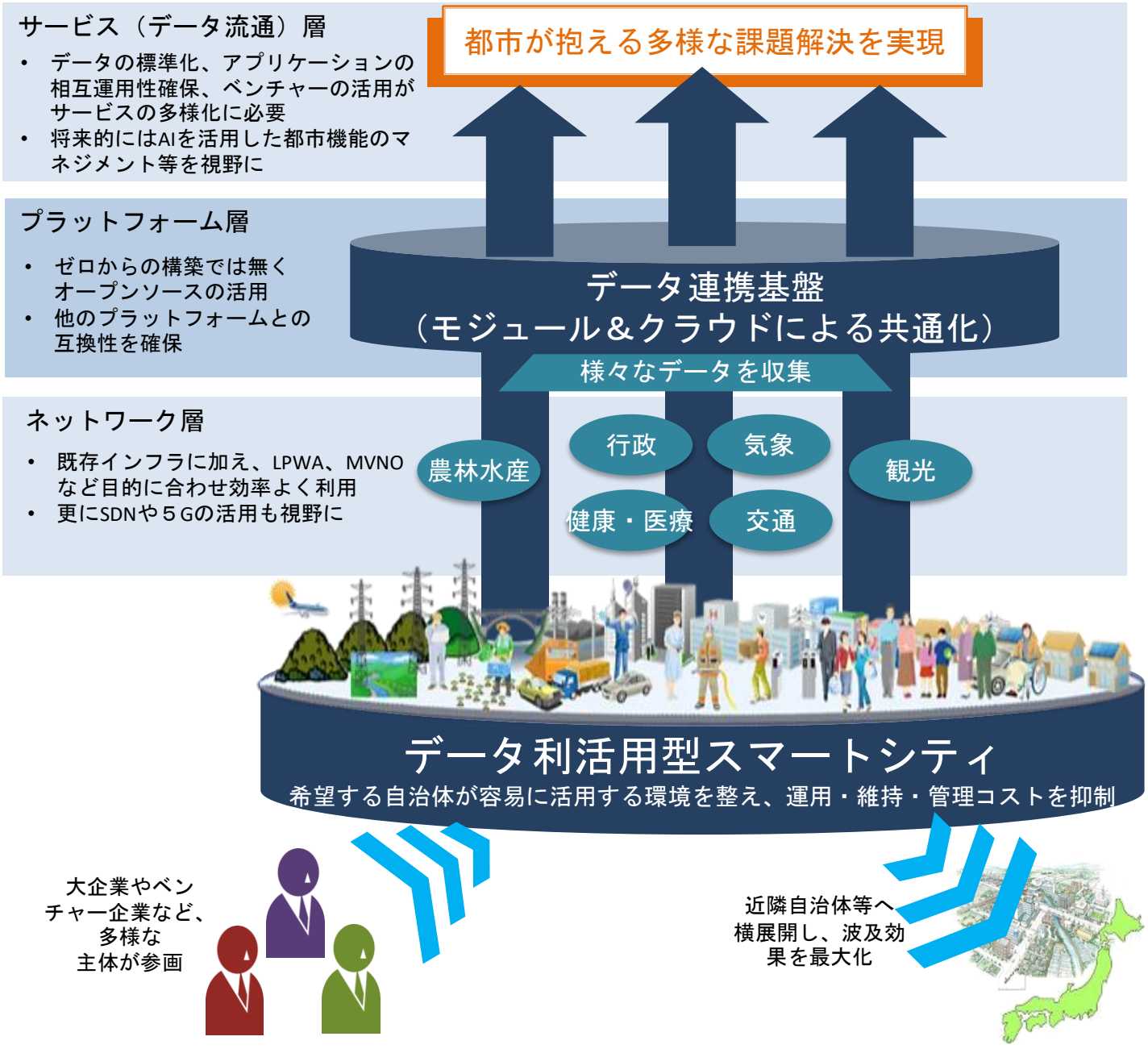
サイバー攻撃誘引基盤（STARDUST）

■ 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



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

IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策：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。

企業におけるサイバー攻撃被害の状況

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)

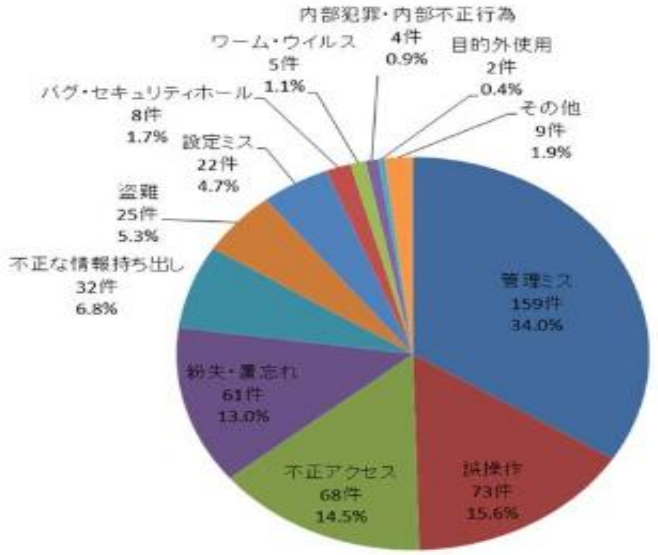


図 4-8：漏えい原因比率（件数）

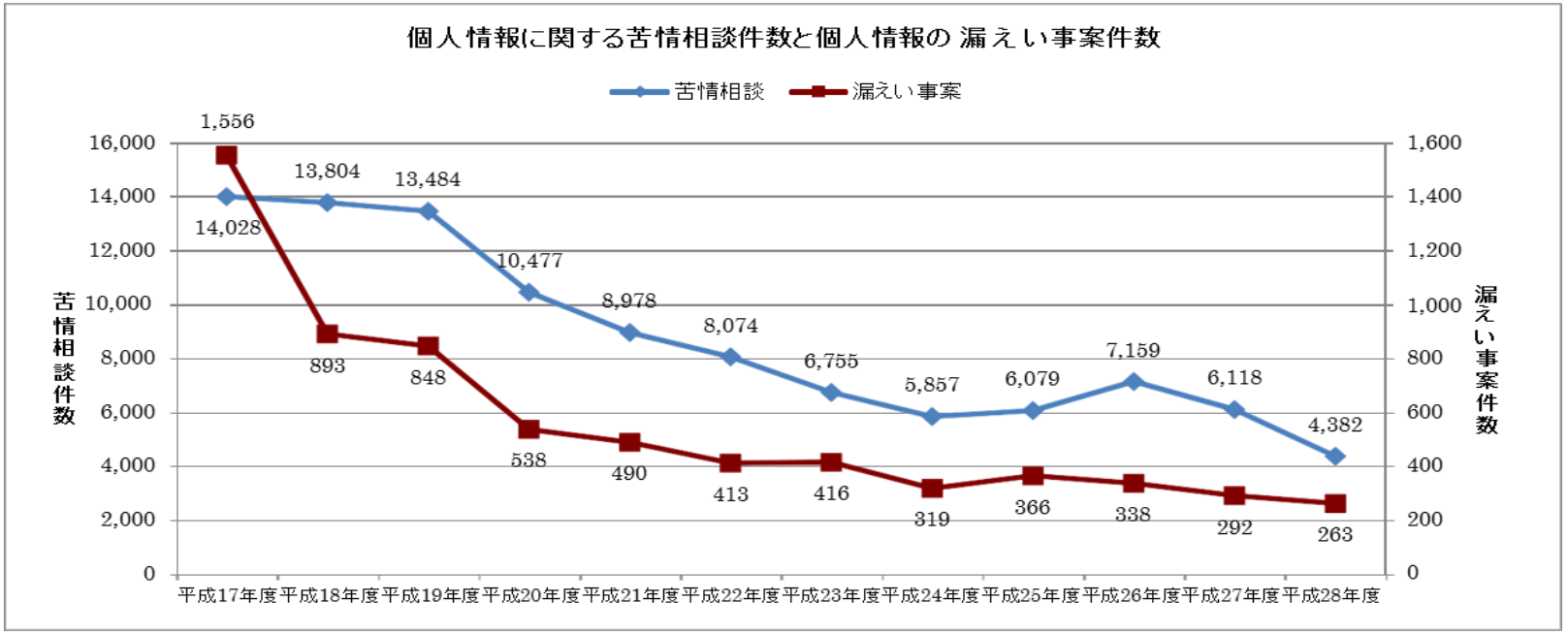
表 4-2：インシデント・トップ 10

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)

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

【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）

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、送状番号	不正アクセス（設定ミスによるファイル蔵置）
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）

企業の経営課題としてのサイバーセキュリティ

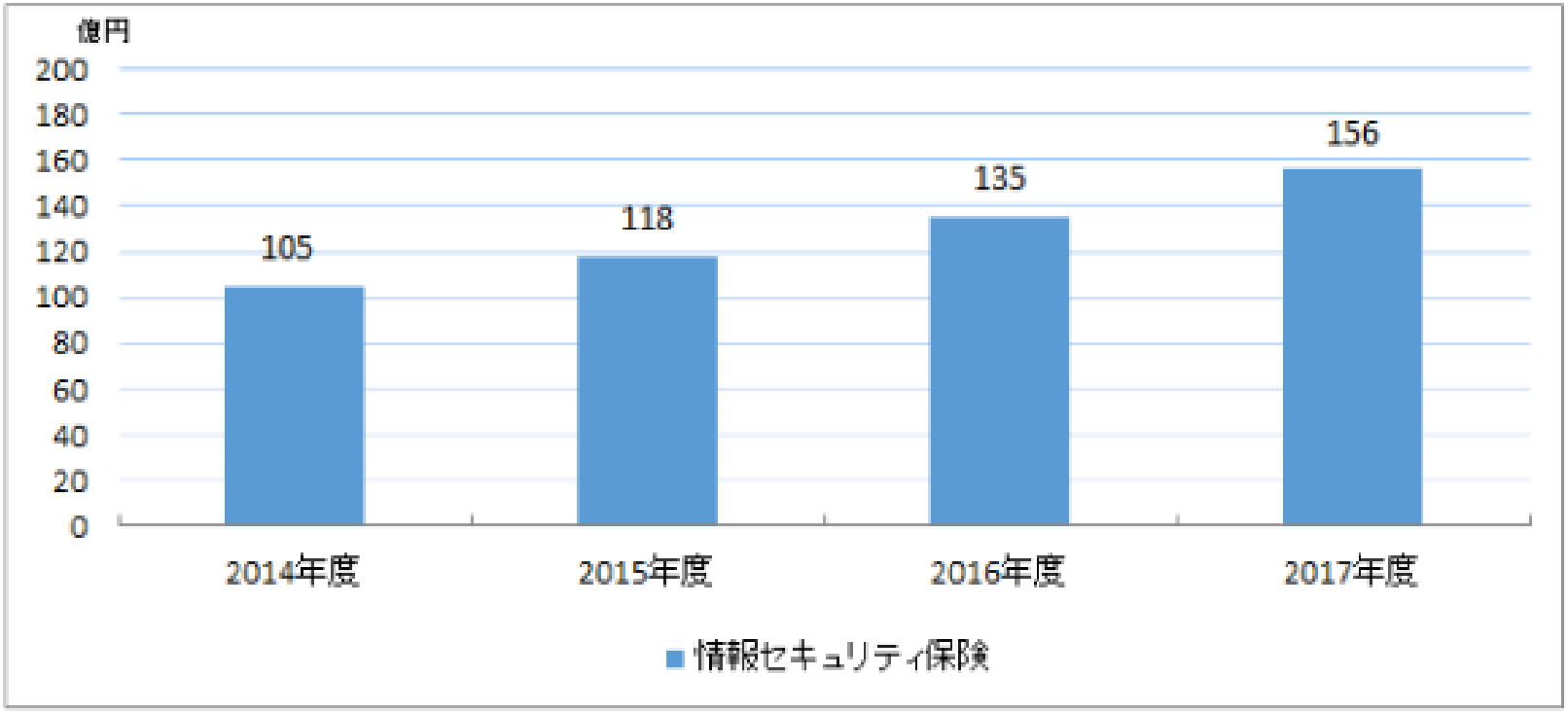
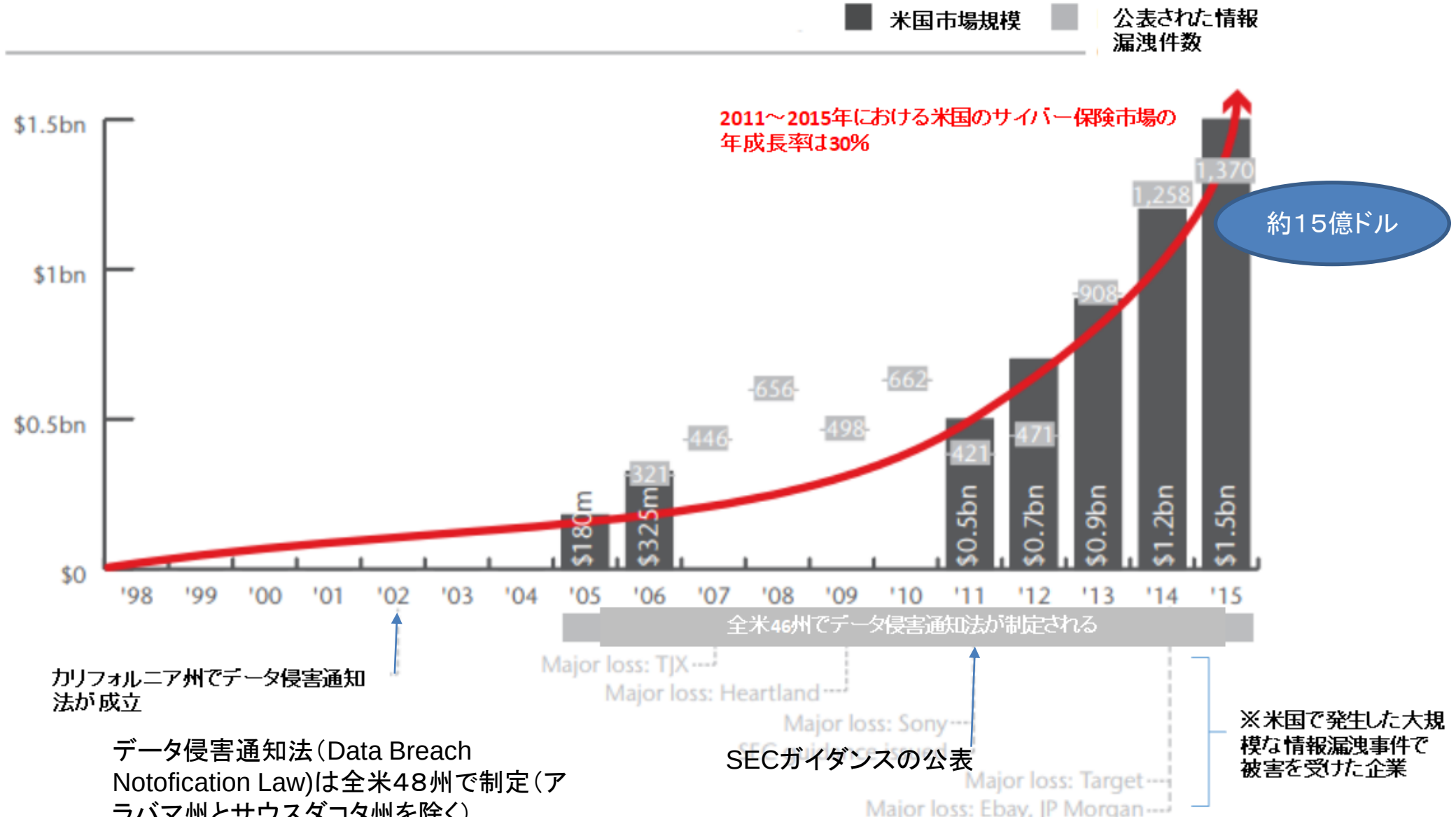


図 25　国内情報セキュリティ保険市場推移

（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



（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）

IoT普及促進税制（コネクテッド・インダストリーズ税制）の創設

○ **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≧３％を満たした場合。

IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策：人材育成の強化

■実践的サイバー防御演習（CYDER）の充実

国の行政機関・地方自治体及び重要インフラ事業者などを対象とした実践的サイバー防御演習を引き続き推進するとともに、新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツの開発を継続的に実施。

■2020年東京大会に向けたサイバー演習の実施

2020年東京大会開催時を想定したサイバー攻撃を模擬し、大会組織委員会のセキュリティ担当者を中心に、攻撃側と防御側の手法の検証及び訓練を行う環境を整備した事業について、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図るとともに、大会終了後に、同システムによる演習の実施により得られた知見、ノウハウを活用する方策について併せて検討。

■若手セキュリティ人材の育成の促進

若年層のICT人材に対し、集中的な研修を行うとともに、海外派遣による経験等を通じて、サイバーセキュリティのコア技術を開発できるような人材、あるいは、そのような技術力を生かしてリスクを許容し、積極的に起業ができるような人材の育成方策を検討し、そうした人材に対する支援の枠組みの構築を促進。

■IoTセキュリティ人材の育成

IoTセキュリティに関するスキルを獲得するための教材作成や研修体制の整備、各種調査のデータの共有、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等を行うための総合的な対策を産学官の連携により推進するための環境整備に向けた検討を行う必要がある。

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）

■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

⇒ *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年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成

⇒ *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）*

■若手セキュリティエンジニアの育成

⇒ *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）*

実践的な防御演習

東京大会に向けた人材育成

若手セキュリティエンジニアの育成

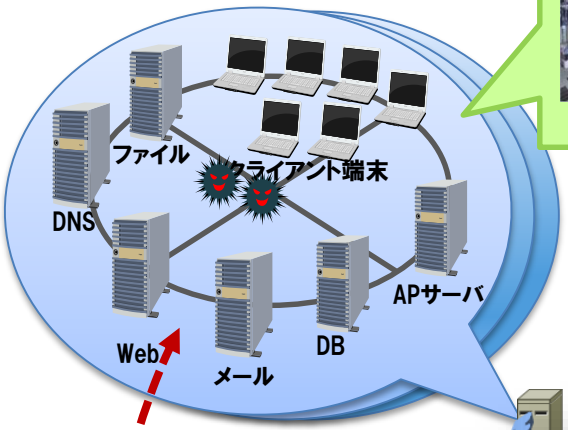
「ナショナルサイバートレーニングセンター」でプラットフォーム化

実践的サイバー防御演習

CYDER: CYber Defense Exercise with Recurrence）

演習のイメージ

大規模仮想LAN環境
（NICT「StarBED」により実現）



石川県能美市

研究開発用の
新世代超高速通信網
NICT「JGN」

仮想ネットワークに
対して疑似攻撃を実施
（実際の不正プログラムを使用）

疑似攻撃者

サイバー攻撃への対処方法を体得

演習会場

演習の特徴

- **サイバー攻撃が発生した場合の被害を最小化するための一連の対処方法**（攻撃を受けた端末の特定・隔離、通信記録の解析による侵入経路や被害範囲の特定、同種攻撃の防御策、上司への報告等）**を体得**
- **150台の高性能サーバを用いた数千人規模の仮想ネットワーク環境**（国の行政機関や大企業を想定）**上で演習を実施**
- **我が国固有のサイバー攻撃事例を徹底分析し、最新の演習シナリオを用意**

平成２８年度の実施内容

技術的知見を有するNICTを実施主体とするため、NICTへの業務追加を行う法改正を実施。

（平成28年4月20日成立、5月31日施行）

→ **地方自治体等に対象を拡大し、全国11地域において、約1500人に実施**

平成29年度の実施予定

演習規模を拡大し、全国47都道府県において約3000人に対し実施予定。

2020東京大会に向けたサイバー演習

cyber colosseo

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

攻防戦によるサイバー演習

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

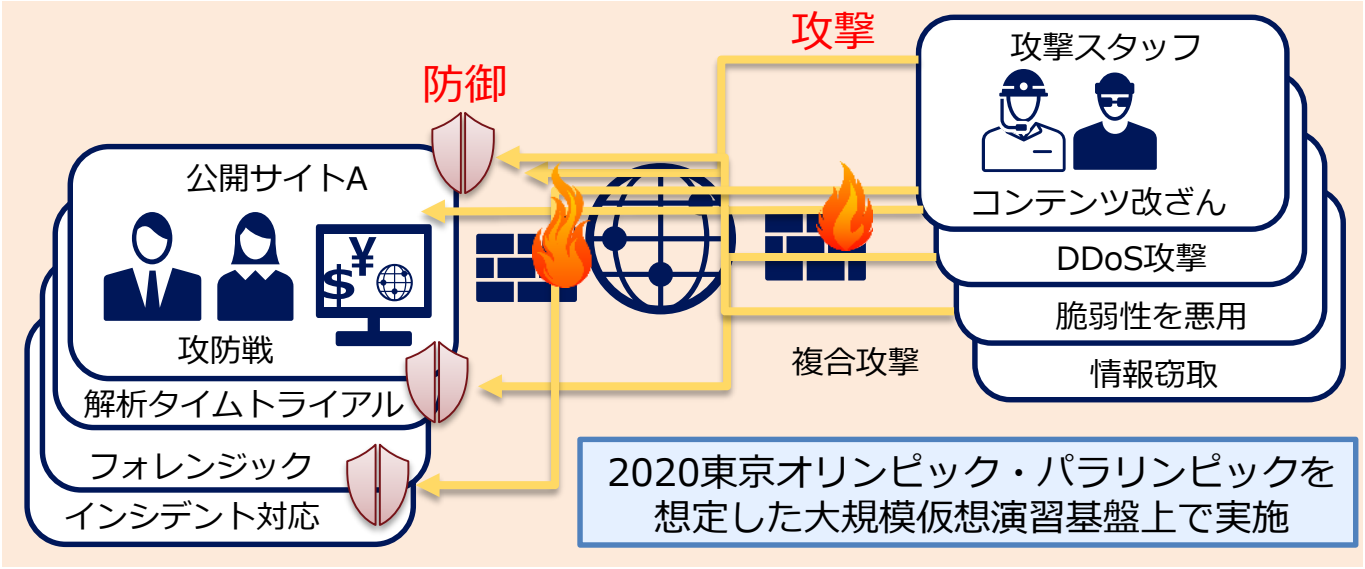
演習シナリオイメージ

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）

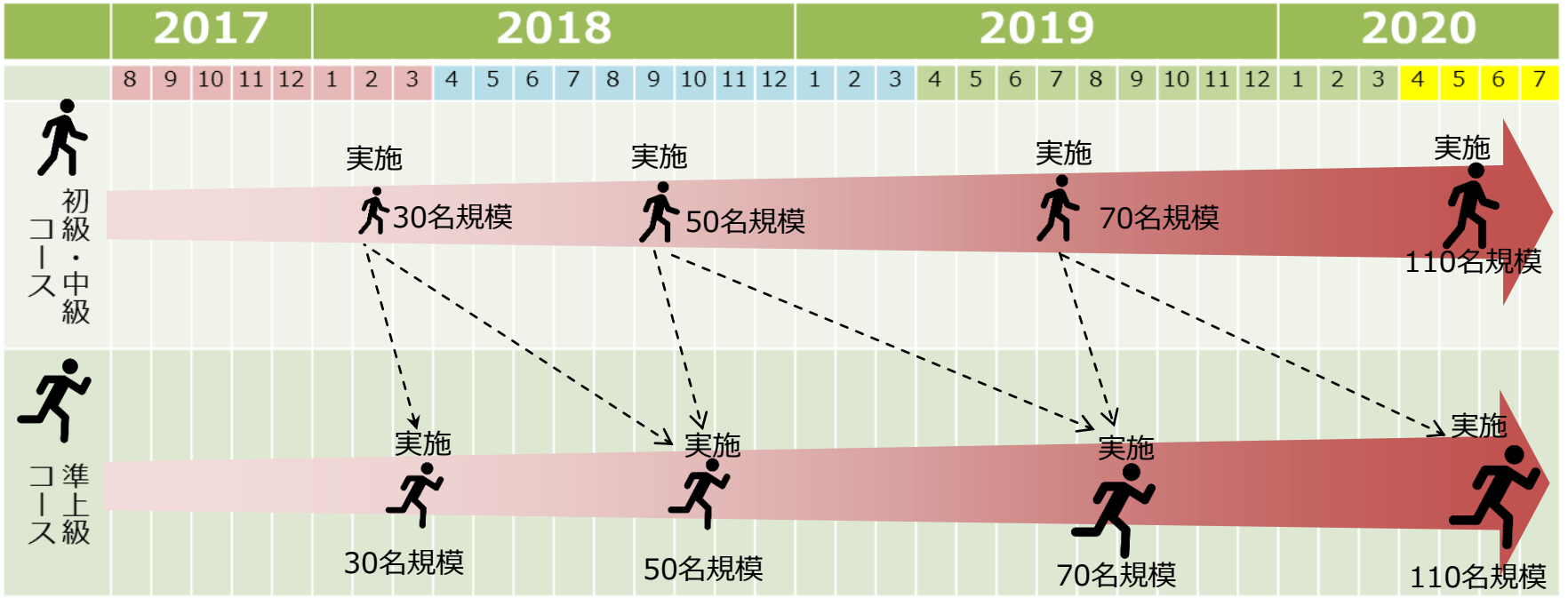


サイバーコロッセオの実施スケジュール

○　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。

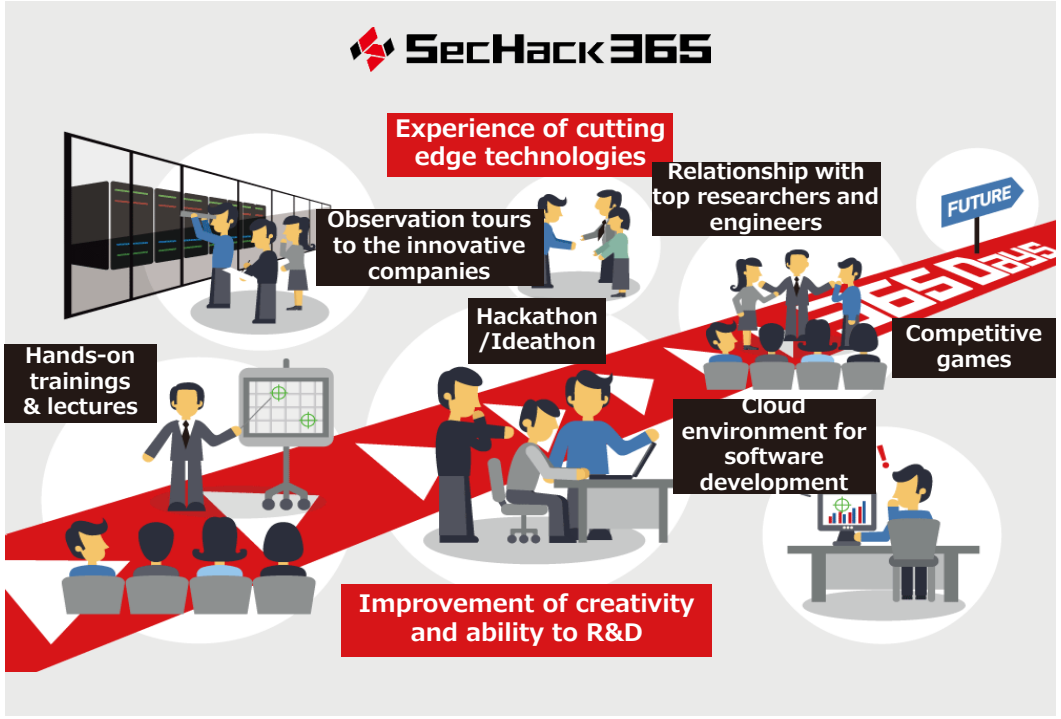
○　**演習受講者は、サイバーコロッセオ演習会場（NICTイノベーションセンター（大手町））に集合**し、仮想のネットワーク環境の上で、実際の機器やソフトウエアの操作を伴って、**本格的な攻防戦等を繰り返し実施**。



※　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。

若手セキュリティエンジニア育成プログラム“SecHack365”

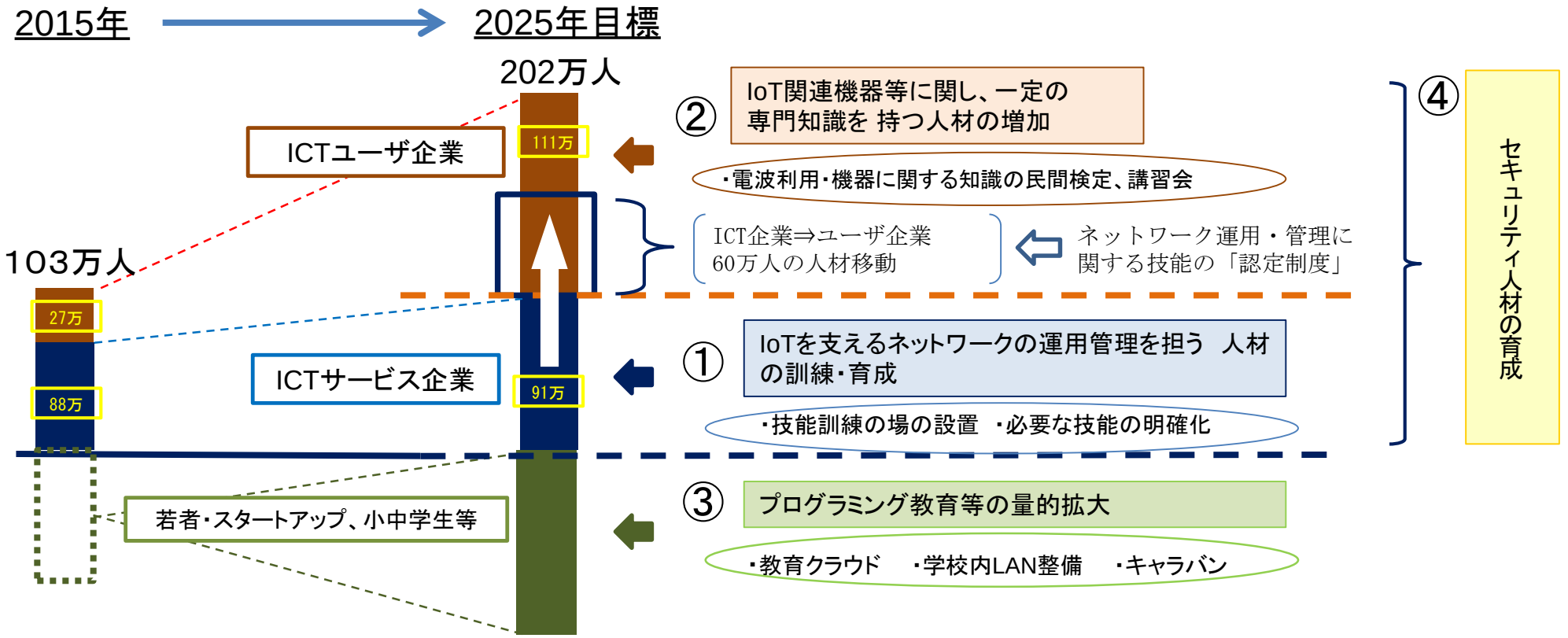
①未来のサイバーセキュリティ研究者・起業家の創出に向けて、NICTが若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導。
②NICTが、高専及び大学等と連携して若手ICT人材を公募し、自身の持つサイバーセキュリティの研究資産を活用し、実地研修及び遠隔開発による年間カリキュラムを用意。



対象者

・ 日本国内に居住する25歳以下の若手ICT人材（NICTにおける選考の結果、47名が受講）

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

頻発する重要インフラを狙ったサイバー攻撃

ハッキング対策で自動車をリコール

2015年7月、クライスラー車が乗っ取られる模様がネット上で公開。クライスラー社は該当車約140万台を自主的にリコール。

米医療機関で医療行為に支障

2016年2月、米国カリフォルニアの医療機関（Hollywood Presbyterian Medical Center）がサイバー攻撃を受け、多くのシステムがランサムウエアに感染。患者情報や検査結果等が閲覧できなくなり、一部患者は他病院に移送された。

米SPE社へのサイバー攻撃

2014年11月、米国ソニー・ピクチャーズ・エンターテイメント(SPE)社がサイバー攻撃を受け、数千に及ぶ社内文書や未公開作品を含む映画がオンライン上に流出。

米医療機関から220万件の個人情報漏えい

2015年10月3日、米国フロリダの医療機関(cancer clinic 21st Century Oncology)のシステムが不正アクセスを受け、データベースから患者と医師の個人情報が漏えい。

仏テレビ局が放送中断

2015年4月8～9日、フランスの国営放送（TV5モンド）がサイバー攻撃を受け、放送できない状態となったほか、同放送局の公式Facebookアカウントが乗っ取られた。

米金融機関から8300万件の顧客情報流出

2014年8月、JPモルガン・チェースへのサイバー攻撃により、8300万件の顧客情報が流出。

ウクライナ西部で大規模停電

2015年12月23日、ウクライナ西部で停電が発生。復旧に約6時間を要し40～70万人程度が影響を受けた。電力供給会社（Prykarpattyaoblenergo）は、「原因は遠隔操作による外部からの侵入の可能性が高い」と発表。

重要インフラの情報セキュリティ対策

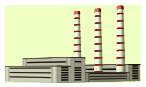
官民連携による重要インフラ防護の推進

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



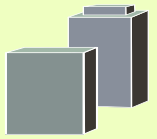



NISCによる調整・連携

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４次行動計画（１７年４月戦略本部決定）

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

重要インフラの情報セキュリティ対策に係る第四次行動計画（17年4月）

1．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

2．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系（ＩＴ）に限らず、制御系（ＯＴ）を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

3．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

① 先導的取組の推進（クラス分け）

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野（例：電力、通信、金融）において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

② オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③ リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

4．本行動計画の期間

➢ 第４次行動計画（案）はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

制御システムの汎用化の進展

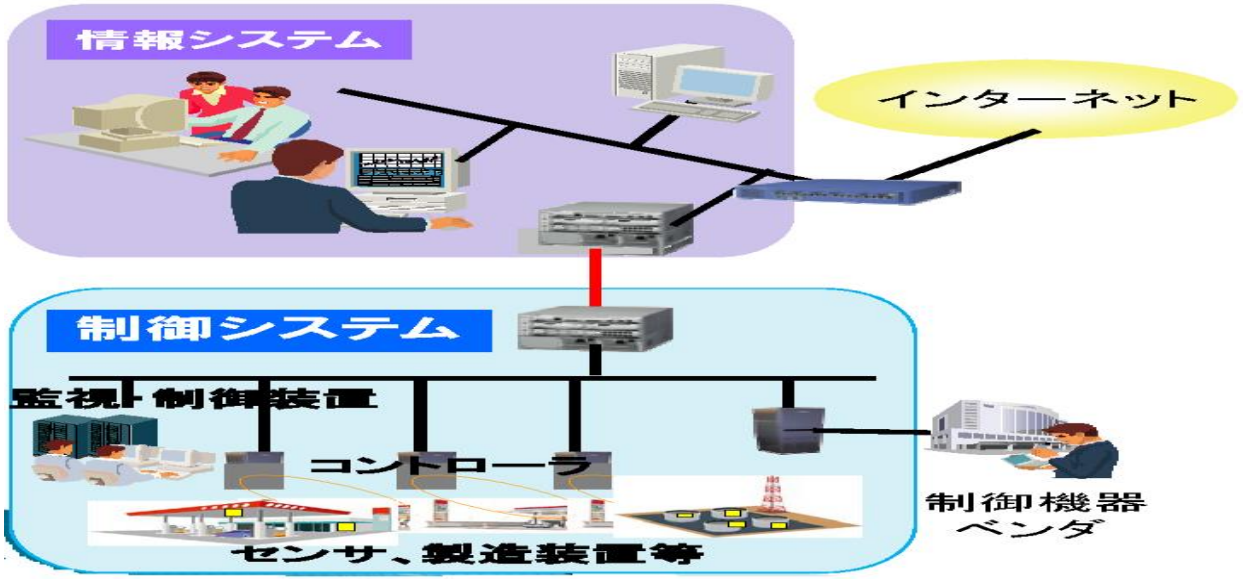
従来

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

○ 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。

IT（Information Technology）＋OT（Operation Technology）



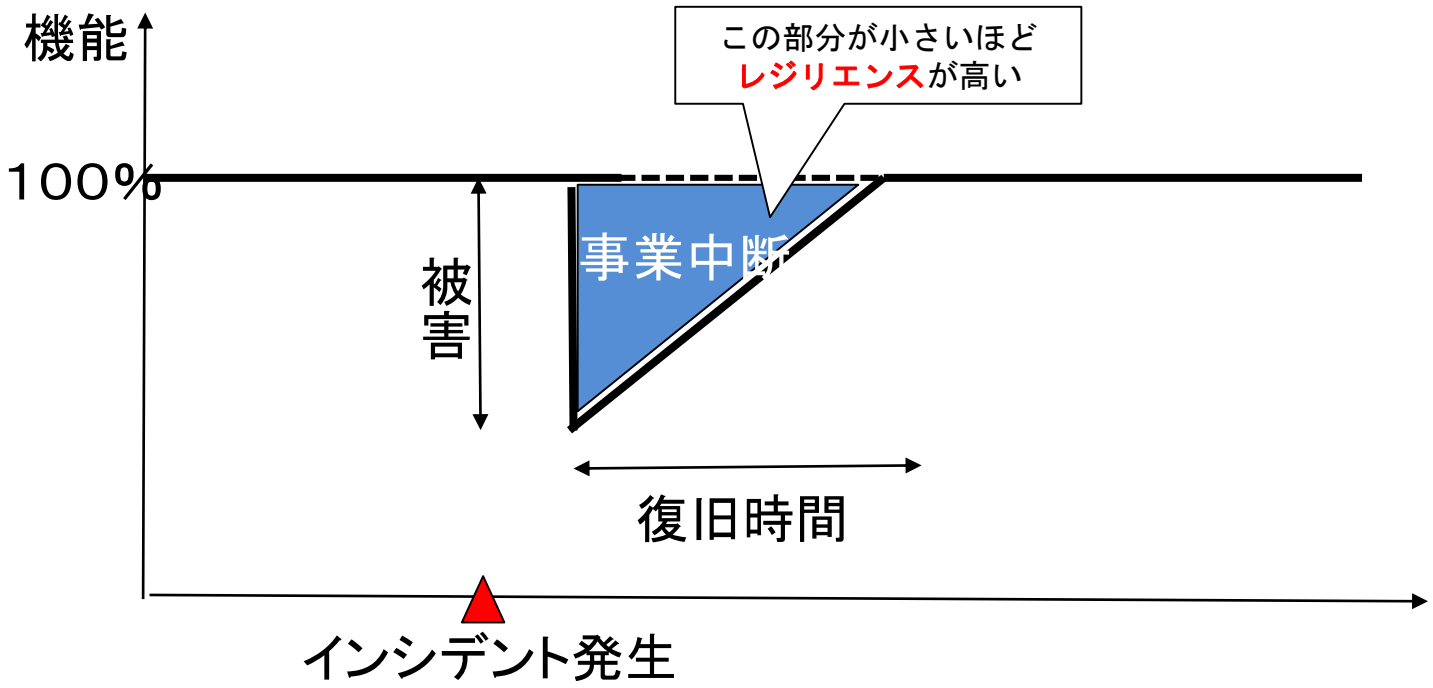
機能(任務)保障の考え方

機能保障 (Mission Assurance)

(DoDの)任務に必須の機能の性能(パフォーマンス)に不可欠な能力・資産※の継続的な機能とレジリエンスを防御・確保するプロセス

※要員、装備、施設、ネットワーク、情報及び情報システム、インフラ及びサプライチェーンを含む。

(出典)DoD "Mission Assurance Strategy" (April 2012)



(出典)「レジリエンス社会」をつくる研究会編 "しなやかな社会の挑戦"(2016年3月、日経BPコンサルティング)を基に一部修正。

情報共有分析センター「ISAC」を通じた事業者間連携の強化

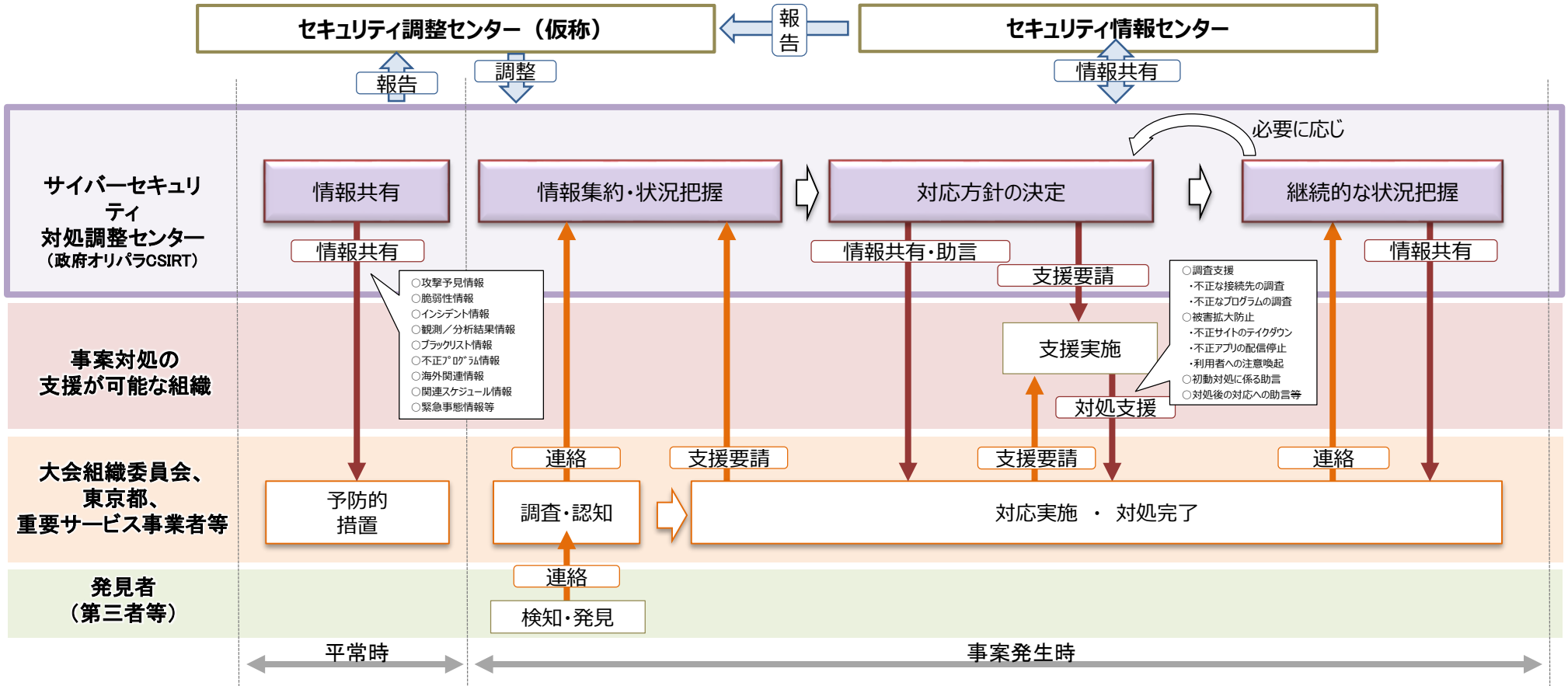
○ サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに **ISAC（Information Sharing and Analysis Center：情報共有分析センター）**が設立され活動中。

○ 国内では、**2002年に他分野に先立ち、通信分野で「Telecom-ISAC Japan」が設立**。その後、**2014年に金融分野で「金融ISAC」が設立。2017年に電力分野で「電力ISAC」が設立**。

2017年7月現在、米国では、①自動車 ②航空、③通信、④防衛産業、⑤天然ガス供給事業、⑥電力、⑦危機管理、⑧金融、⑨情報技術、⑩海運、⑪自治体、⑫国民健康、⑬石油・天然ガス、⑭不動産、⑮研究・教育、⑯小売・サービス、⑰サプライチェーン、⑱陸上輸送、⑲公共輸送、⑳輸送バス、㉑水の21分野でISACが設置・活動中。

サイバーセキュリティ対処調整センターの構築

■ サイバーセキュリティ対処調整センターを平成30年度末を目途に構築。
■センターの構築及び運用は、オリパラ推進本部の下で、オリパラ事務局と緊密に連携し、内閣サイバーセキュリティセンターが中心となって行う。（センターの運用前については、NISCがその業務を担う。）
■センターは、大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供するとともに、必要があるときには関係機関等のインシデント対処に対する対処調整を行う。
■オリパラ特措法第８条第１項の規定を踏まえ、センターは、必要があると認めるときは、大会組織委員会等に対して、サイバーセキュリティに係る情報の提供、説明その他必要な協力を求める。



IoTセキュリティ総合対策（2017年10月）

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）

IoTセキュリティ総合対策：国際連携の推進

■ASEAN各国との連携

実践的サイバー防御演習「CYDER」等の海外展開を通じたセキュリティ人材の育成支援を推進するとともに、各種会議等を通じて、我が国及びASEANにおけるサイバーセキュリティの脅威をめぐる状況やIoTセキュリティ対策に関する情報交換を行うほか、ASEAN側のニーズを踏まえつつ、ASEANにおけるIoTセキュリティ強化に向けた施策の導入・促進のための協力を推進（平成29年～平成31年の３年間で500人を目標）。

■国際的なISAC間連携

国際連携ワークショップの開催等を通じて、日本のICT-ISACと米国のICT分野のISACとの連携を強化し、通信事業者、IoT機器ベンダー、セキュリティベンダー等が、AIS（Automated Indicator Sharing）等を介して脅威情報を自動的に共有し、サイバーセキュリティ対策に活用を促進。

■国際標準化の推進

ISO/IEC（国際標準化機構/国際電気標準会議）及びITU-T（国際電気通信連合電気通信標準化部門）における、IoTシステムのセキュリティに係る国際標準化に関する活動に積極的に貢献。

■サイバー空間における国際ルールを巡る議論への積極的参画

様々なチャネルを通じて進められている、サイバー空間における国際ルール等に関する議論へ積極的に参画。

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（国連GGE、１５年６月）

"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。

米国国家安全保障戦略（サイバーセキュリティ関連）（2017年12月）

■ **ピラー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

■ **ピラー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）

■ **ピラー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

■ **ピラー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

優先アクション

➢ **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。

ランサムウェア“WannaCry”のAttribution問題

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のに、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。

サイバー空間に関する国際連携の推進

■**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。

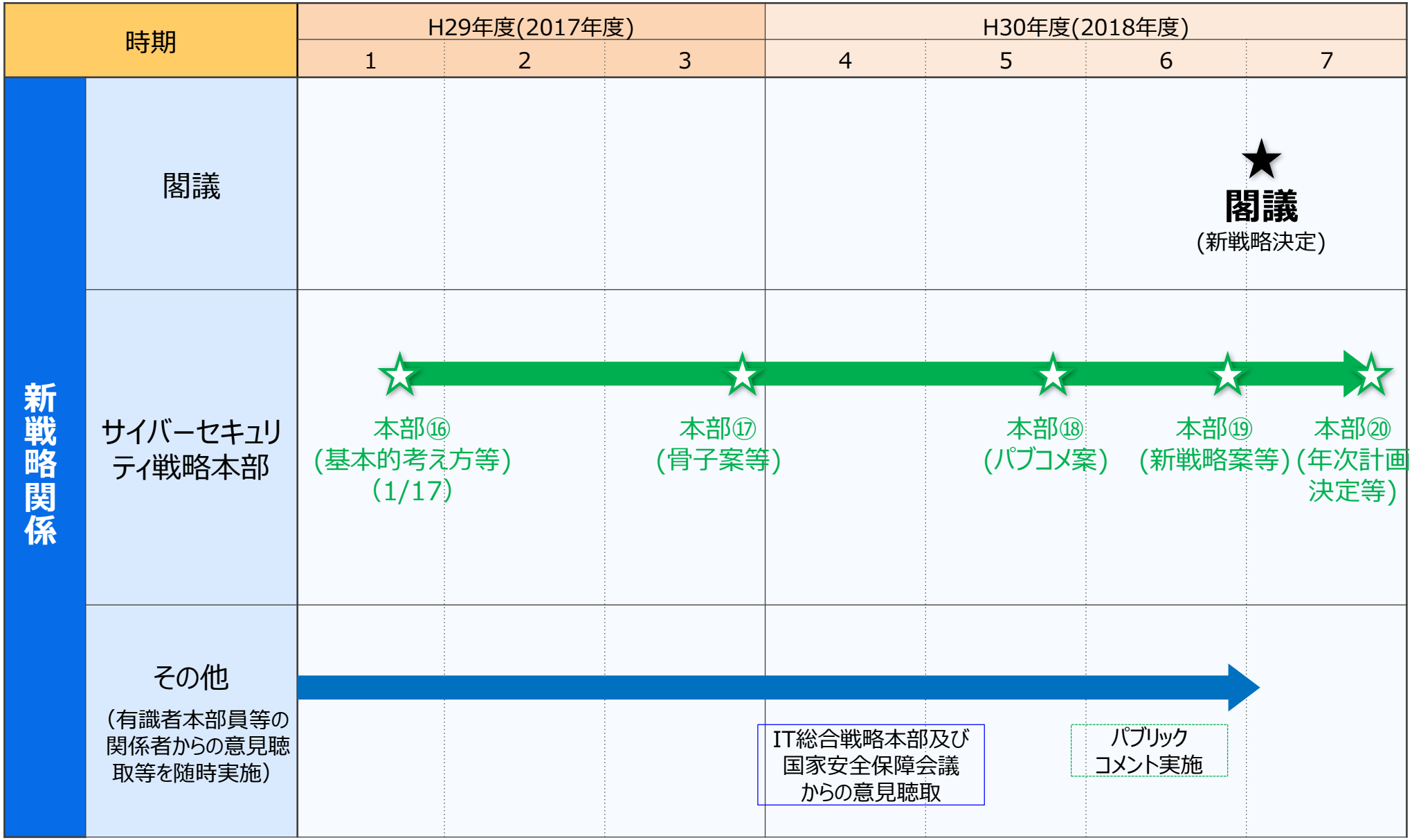
■データローカライゼーション等の動きをけん制し、**「情報の自由な流通」を二国間・多国間の枠組みで維持**していくことが必要。

■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）。

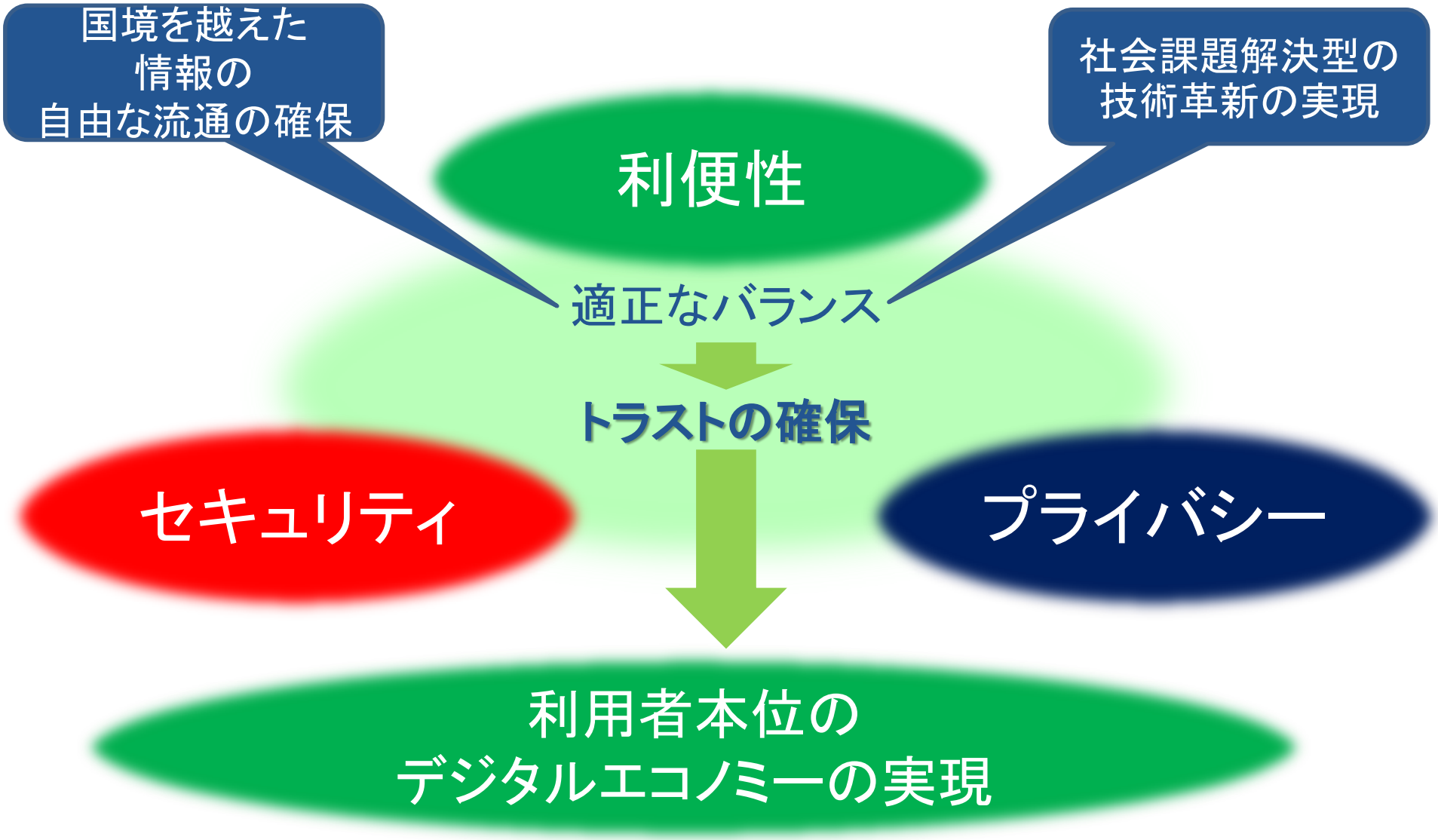
(参考）G7タオルミナ首脳コミュニケ（２０１７年５月）

“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.”

次期サイバーセキュリティ戦略の策定スケジュール（案）



デジタルエコノミーに求められる要素



Any Question?

総務省