「IoTセキュリティ総合対策」について

平成３０年２月２８日
総務省　情報流通行政局
サイバーセキュリティ課
課長補佐　澤谷　航

本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．政府全体の取組

３．総務省の取組（IoTセキュリティ総合対策）

（1）脆弱性対策に係る体制の整備

（2）研究開発の推進

（3）民間企業等におけるセキュリティ対策の促進

（4）人材育成の強化

（5）国際連携の推進

本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．政府全体の取組

３．総務省の取組（IoTセキュリティ総合対策）

（1）脆弱性対策に係る体制の整備

（2）研究開発の推進

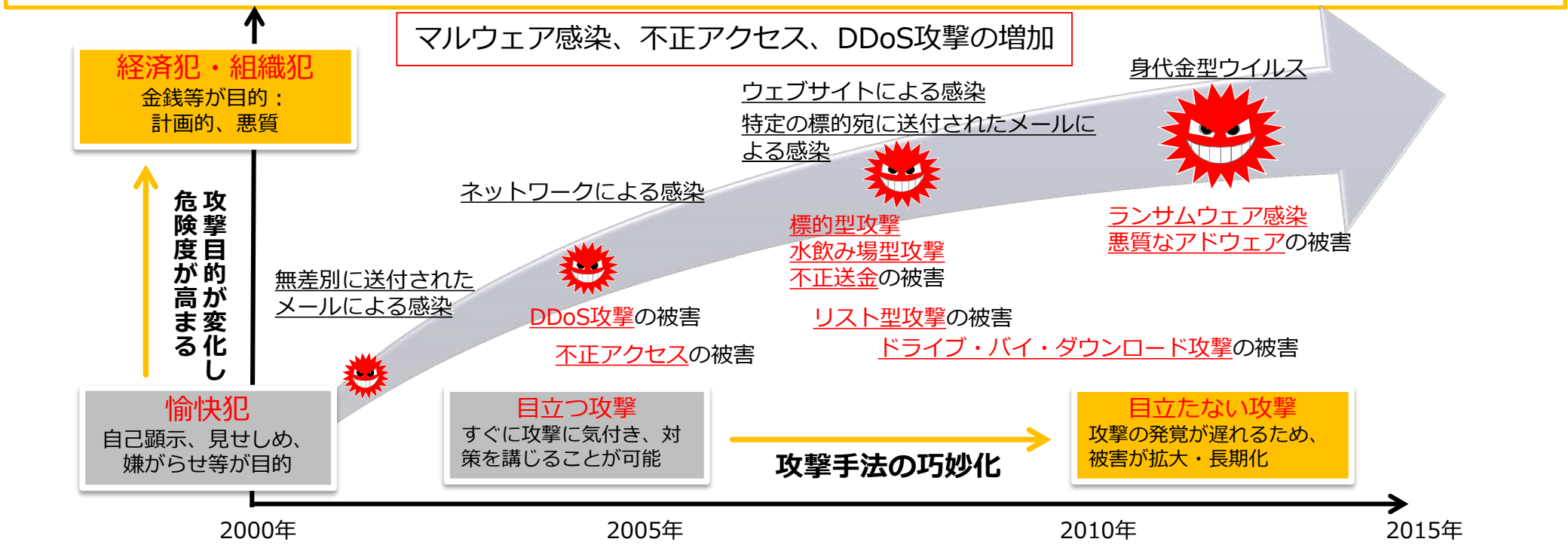
（3）民間企業等におけるセキュリティ対策の促進

（4）人材育成の強化

（5）国際連携の推進

サイバーセキュリティ上の脅威の増大

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



国内事例

2015年6月: **日本年金機構**の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出（**標的型攻撃**）

2015年10月: **金融庁**の注意喚起を装ったフィッシングサイトを確認、国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報を騙し取られる恐れ（**フィッシング攻撃**）

2015年11月: **東京五輪組織委員会**のホームページにサイバー攻撃、約12時間閲覧不能（**DDoS攻撃**）

2016年6月: **i.JTB（JTBのグループ会社）**の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（**標的型攻撃**）

2017年5月: 国内（行政、民間企業、病院等）において、**WannaCry**による被害が確認。企業内のシステム停止などの障害が発生した。（**ランサムウェア**）

海外事例

2015年4月: **フランスのテレビネットワーク TV５ Monde** がサイバー攻撃を受け、放送が一時中断（**標的型攻撃**）

2015年6月: **米国の人事管理局（OPM）**が不正にアクセスされ、政府職員の個人情報が流出（**不正アクセス**）

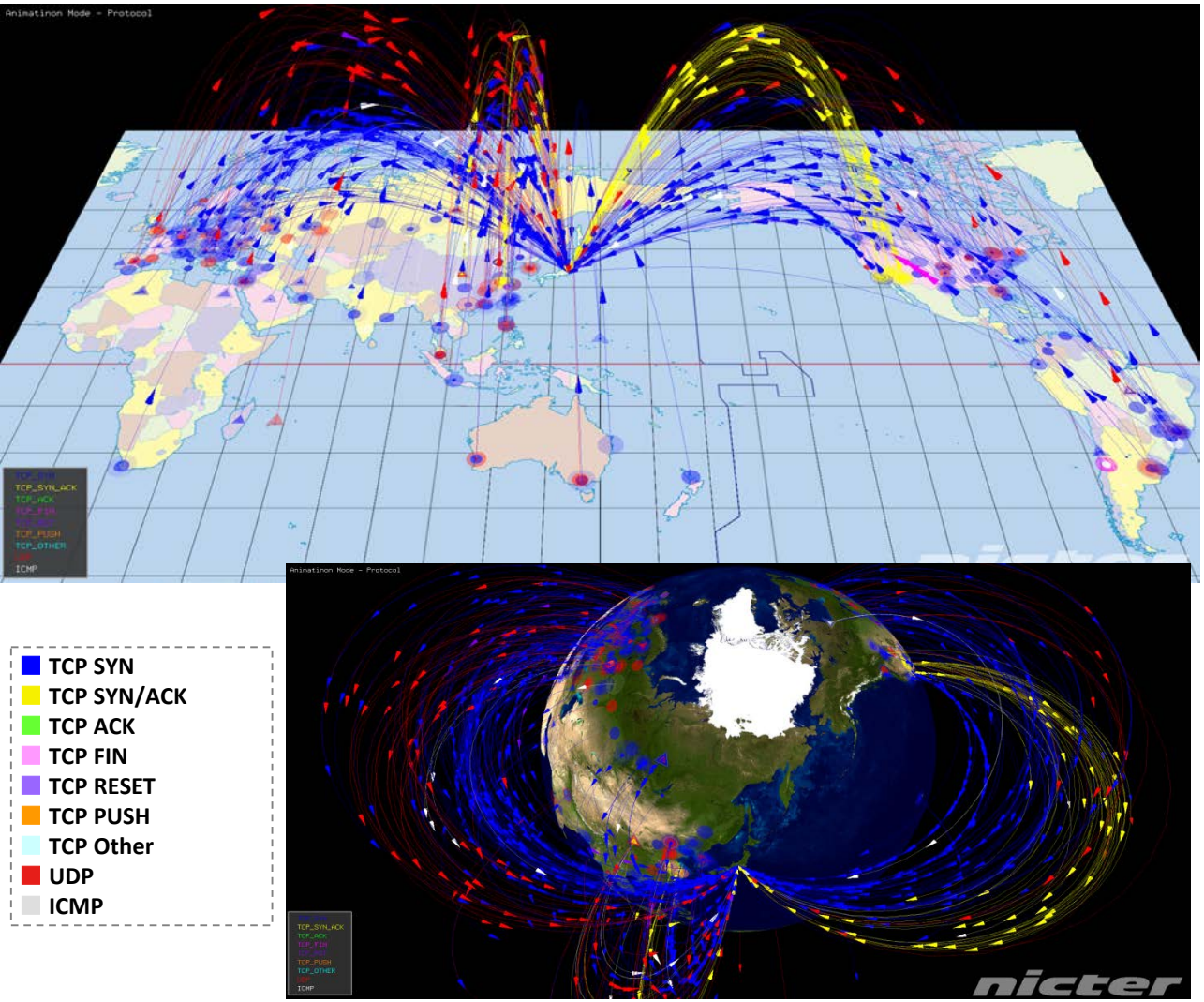
2015年12月: **ウクライナの電力会社**のシステムがマルウェアに感染し、停電が発生（**標的型攻撃**）

2016年10月: **米国のDyn社**のDNSサーバが大規模なDDoS攻撃を受け、同社の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（**DDoS攻撃**）

2017年5月: 世界各国（アメリカ、イギリス、中国、ロシア等）で**WannaCry**の感染被害が発生。行政、民間企業、医療等の多くの組織に影響を及ぼした。（**ランサムウェア**）

サイバー攻撃の状況（NICTERによる観測）

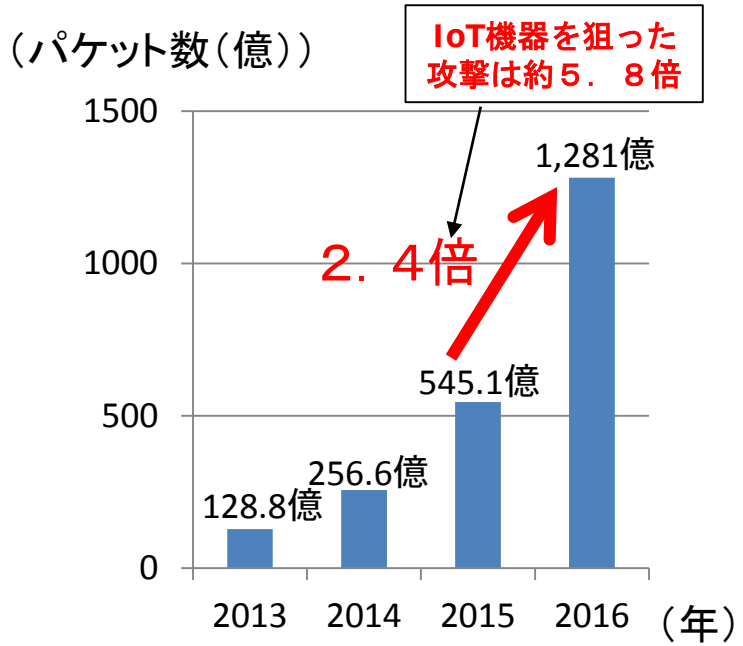
➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレスブロック30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。



・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

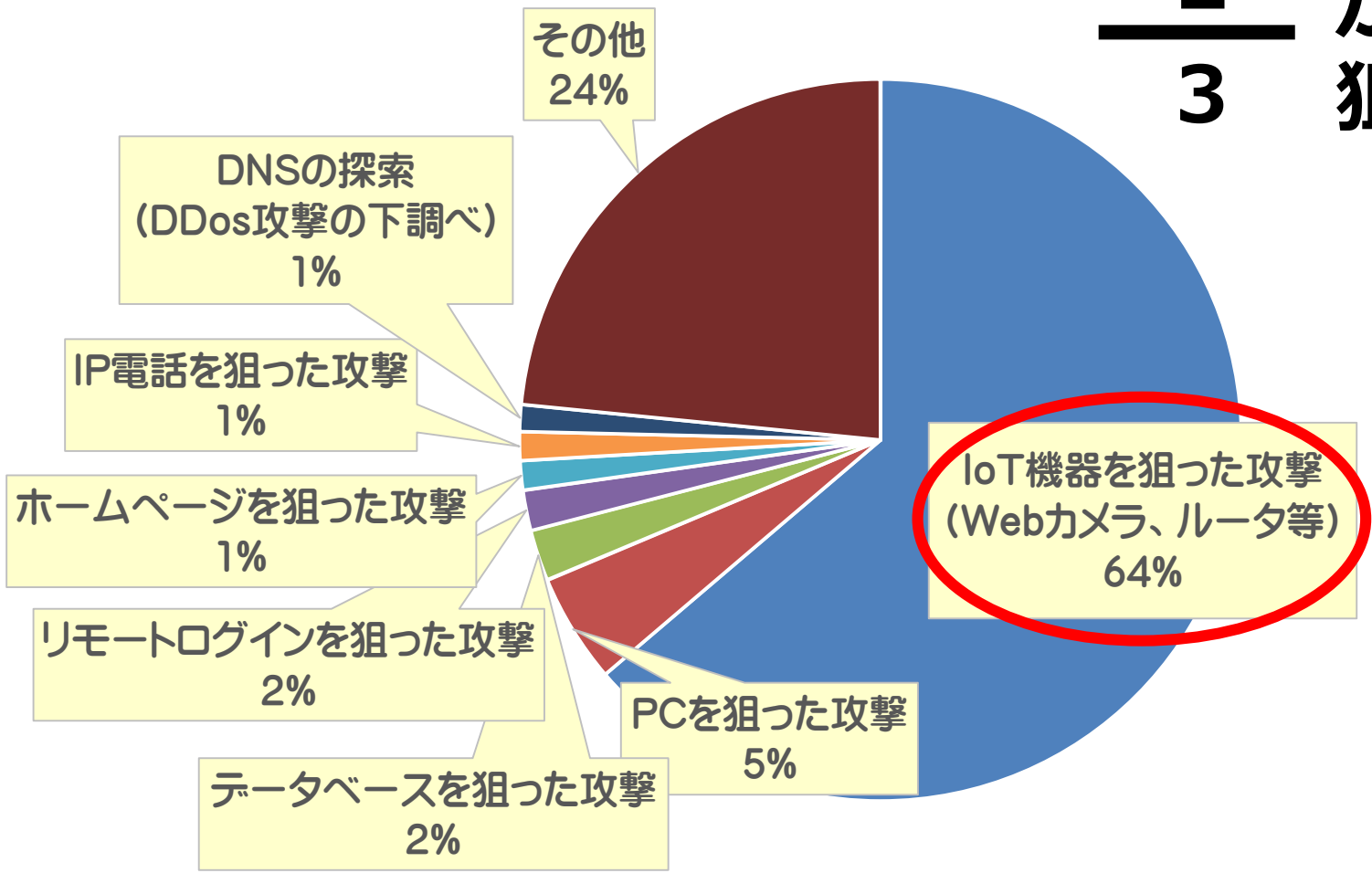
１年間で観測されたサイバー攻撃回数



サイバー攻撃の内訳（2016年、NICTERによる観測）

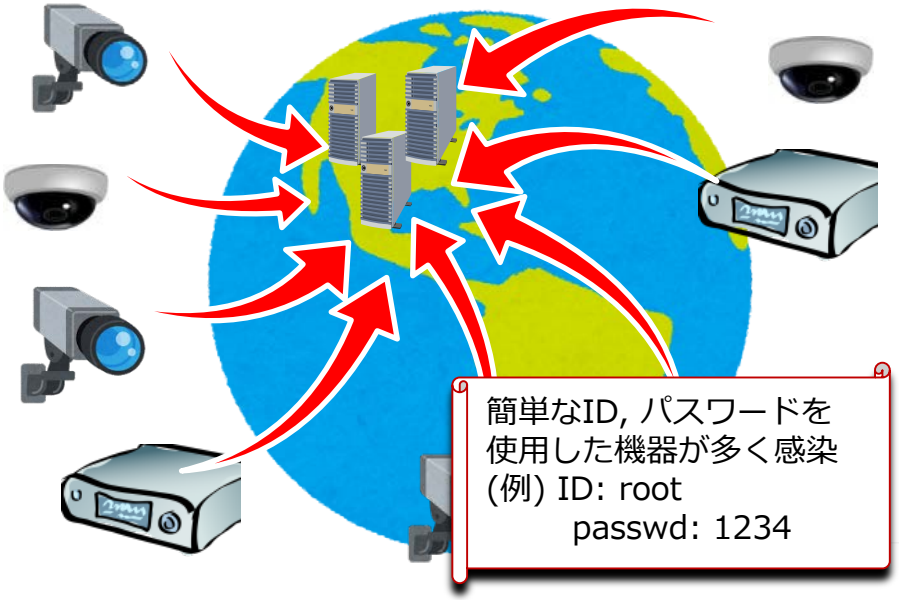
観測された全サイバー攻撃1,281億パケットのうち、

2/3 がIoTを狙っている！



IoTによる大規模DDoS攻撃について

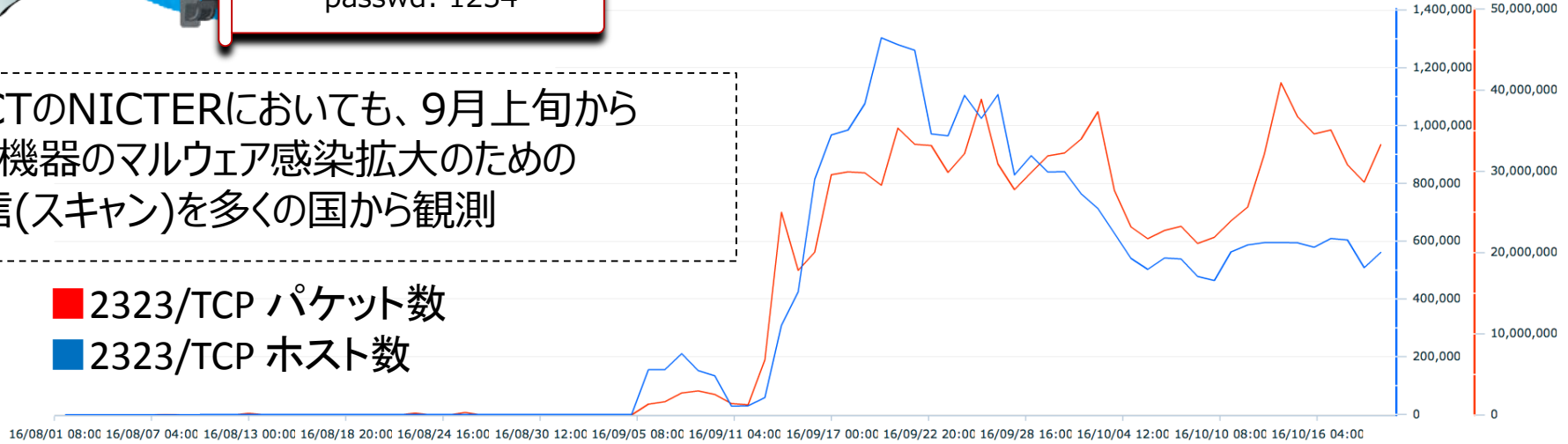
- **2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が２回発生。**
- **同社からDNSサービスの提供受けていた企業のサービスにアクセスしにくくなる等の障害が発生。**
- **サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。**



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

出典: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

- ✓ 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



本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．政府全体の取組

３．総務省の取組（IoTセキュリティ総合対策）

（1）脆弱性対策に係る体制の整備

（2）研究開発の推進

（3）民間企業等におけるセキュリティ対策の促進

（4）人材育成の強化

（5）国際連携の推進

サイバーセキュリティ推進体制

平成26年11月に成立した「サイバーセキュリティ基本法」に基づき、平成27年1月、内閣にサイバーセキュリティ戦略本部が設置され、同年9月、日本年金機構の年金情報流出の事案も踏まえた新たな「サイバーセキュリティ戦略」を閣議決定。同本部を司令塔として、事務局を担う内閣サイバーセキュリティセンター（NISC）の調整の下、関係省庁が連携した政府横断的サイバーセキュリティ推進体制を整備し、本戦略を推進。

内閣

内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
有識者（７名；10名以下）

閣僚が参画

遠藤　信博　日本電気株式会社代表取締役会長
小野寺　正　ＫＤＤＩ株式会社代表取締役会長
中谷　和弘　東京大学大学院法学政治学研究科教授
野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎　情報セキュリティ大学院大学教授
前田　雅英　日本大学大学院法務研究科教授
村井　純　慶應義塾大学教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ補佐官

政府機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞
金融庁　（金融機関）
総務省　（地方公共団体、情報通信）
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　（鉄道、航空、物流）

＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

警察庁（サイバー犯罪・攻撃の取締り）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

サイバーセキュリティ戦略中間レビュー（平成29年7月13日サイバーセキュリティ戦略本部決定）

2020年及びその後を見据えたサイバーセキュリティの在り方について（案）
－サイバーセキュリティ戦略中間レビュー－

資料3-1

■ 現行戦略策定後の脅威動向等の認識を踏まえ、加速・強化すべき施策を取りまとめ、急ぎ対応が必要と考えられるものから実施（必要な制度面の見直し等を含む。）。
■ 今後は、本レビューを踏まえ、　（必要な制度面の見直しも含め）可能な施策から段階的に実施（1年以内）

脅威等の変化

IoT機器を踏み台にしたサイバー攻撃の顕在化

ボット（注）撲滅の推進

■ 効率的かつ効果的な対策につなげるため、官民が連携し、実態の把握、対策の実施・周知、再発防止・環境改善を一体的に実施
- 政府内に体制を構築して継続的かつ広範な実態調査ができるよう、必要な法的整理
- 電気通信事業者等の協力を得た利用者等の特定・注意喚起等の対策の実施、周知（必要な技術的・制度的枠組の構築）
- 迅速な対処の協力の要請（製造事業者・販売事業者等）
- 諸外国との連携を促進し、協調した対策を実施。

（注）ここでは、IoT機器等を外部から遠隔操作するための　不正プログラムを指している。

省庁・分野を越えた情報共有の必要性

情報共有・連携ネットワーク（仮称）の構築・運用

■ 官民が連携し、迅速な集約・分析、効果的な対策の共有を行う情報連携体制を構築することにより、サイバー攻撃の被害及び被害拡大を防止
- 効果的な情報連携体制を構築する制度整備。
  - ✓ 情報へアクセス権限を有する民間事業者の責務、官側の役割等
  - ✓ 情報提供を行う際の阻害要因に対処
- 情報提供者にとって提供しやすく、かつ利用者にとって対策しやすい情報の抽出及び環境の整備。
  - ✓ 事案に応じた提供内容をあらかじめ設定し、対策に効果的な内容を適切なタイミングで共有。

2020年東京オリンピック・パラリンピック競技大会に向けた抜本的対策を見据えた取組の必要

2020年東京オリンピック・パラリンピック競技大会に向けた体制の整備

■ サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の構築（2018年度末目途）
- 組織委員会に対する適切な助言・支援が行えるよう、東京オリンピック競技大会・東京パラリンピック競技大会推進本部との連携等、制度的枠組の検討。
- 一定程度の専任要員（計画的に訓練）
- 200人以上の技術者等（重要サービス事業者、セキュリティ事業者等）との連携態勢。

■ セキュリティ情報センターの構築
- 安全に係る情報を集約、分析・評価を行い、関係機関等に対し必要な情報を随時提供

■ リスクマネジメントの促進
- 横断的リスク評価（2018年度までに全分野で実施）に基づくマネジメントを強力に推進
- 特に影響度が大きい重要サービス事業者について、鳥瞰図的な把握及び検証、リスクの確認及び対策を推進

経済社会の活力の向上及び持続的発展

- 安全なIoTシステムの創出による国際競争力の強化（国際標準化）［関係分野の用語・設計・開発等の概念を共通化する国際標準の策定］
- セキュリティに係るビジネス環境の整備［セキュリティ規格に関する要件の策定、セキュリティに係る損害保険の普及の支援］

国民が安全で安心して暮らせる社会の実現

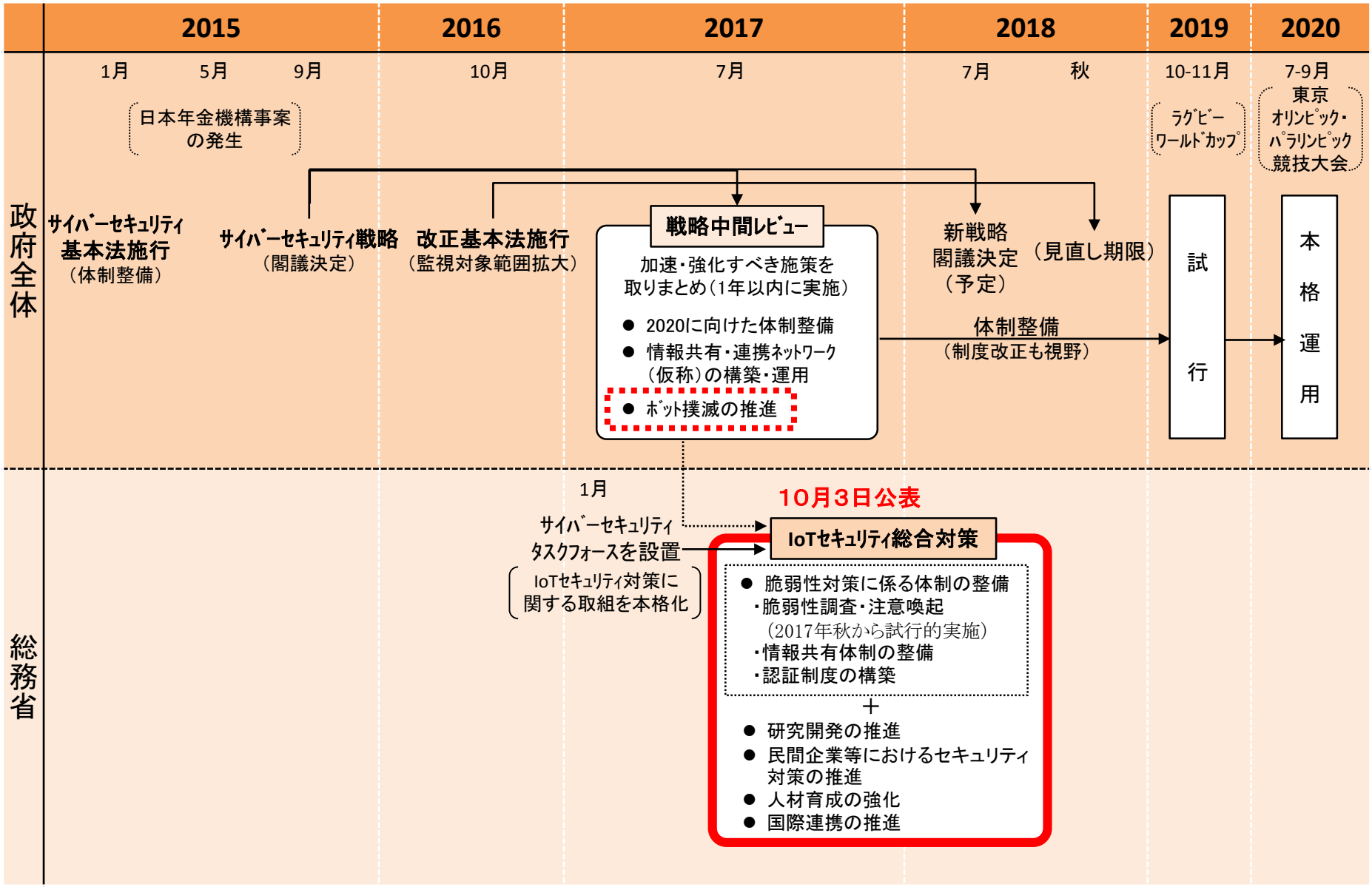
- 深刻度判断基準の策定等によるサイバー攻撃対処態勢の強化［コンティンジェンシープラン策定の支援］
- 政府機関・独法等における効率的・効果的防護体制の再構築［検知精度・対処能力等の監視能力の向上、情報システムの侵入耐性診断時の自衛隊能力の活用］
- 地方公共団体におけるセキュリティ対策向上［セキュリティ人材・体制の確保充実の支援］
- 大学等における情報セキュリティ対策の向上［大学等の相互協力による取組、情報システムの侵入耐性診断実施支援］
- サイバー犯罪・サイバー攻撃対策の強化
- 普及啓発・情報発信［迅速な情報発信・相談対応のための取組強化］

国際社会の平和・安定及び我が国の安全保障

- 組織・分野 横断的な取組等による我が国の安全の確保
- 国立研究開発法人における先端技術の防護のための情報セキュリティ対策の強化
- 海外の多様な主体との多層的な連携の強化
- サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

- 経営層の意識改革や、橋渡し人材等幅広い階層における人材育成・確保の継続的な促進
- 研究開発等の推進

サイバーセキュリティ戦略の推進



本日の講演内容

1．サイバーセキュリティ上の脅威の現状

2．政府全体の取組

3．総務省の取組（IoTセキュリティ総合対策）

（1）脆弱性対策に係る体制の整備

（2）研究開発の推進

（3）民間企業等におけるセキュリティ対策の促進

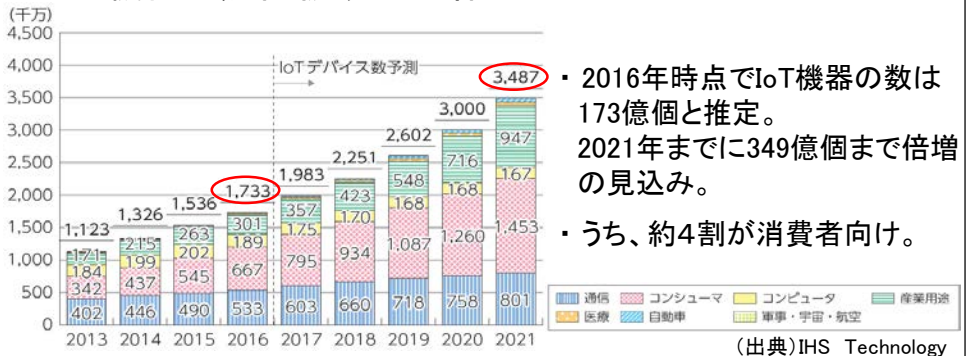
（4）人材育成の強化

（5）国際連携の推進

IoTセキュリティ総合対策（全体像）（平成29年10月3日　公表）

現状

○IoT機器の幾何級数的な増加

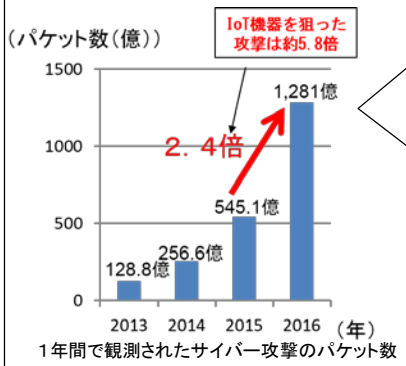


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

・うち、約4割が消費者向け。

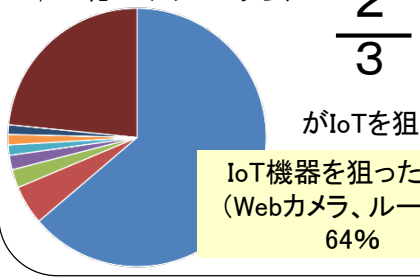
（出典）IHS　Technology

○IoT機器を狙った攻撃が急増



1年間で観測されたサイバー攻撃のパケット数

観測された全サイバー攻撃
1,281億パケットのうち、

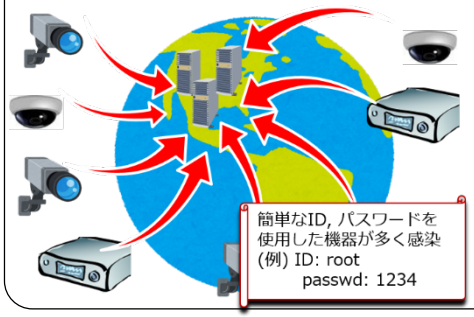


$\frac{2}{3}$

がIoTを狙っている！

IoT機器を狙った攻撃
（Webカメラ、ルータ等）
64%

○IoT機器を踏み台にした大規模攻撃が発生



・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。

対策

IoTセキュリティ総合対策

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）

（1）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）

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**

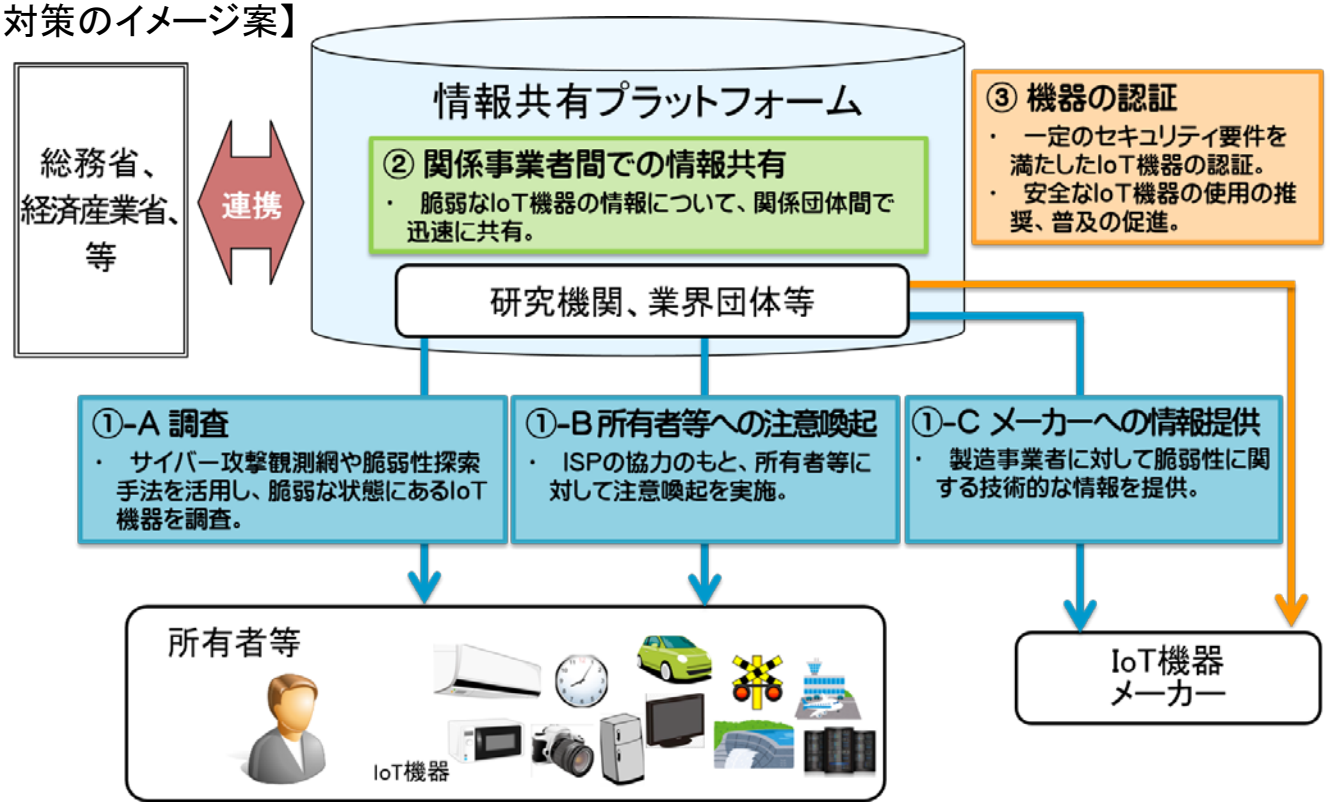
ID/パスワード設定、ファームウェアのアップデート、Wi-Fi設定の3点を中心とした利用者への意識啓発の実施、利用者からの相談窓口や、脆弱性が見つかった場合の関係機関との調整窓口の設置。

脆弱性対策に係る体制の整備（脆弱性調査の実施）

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）。

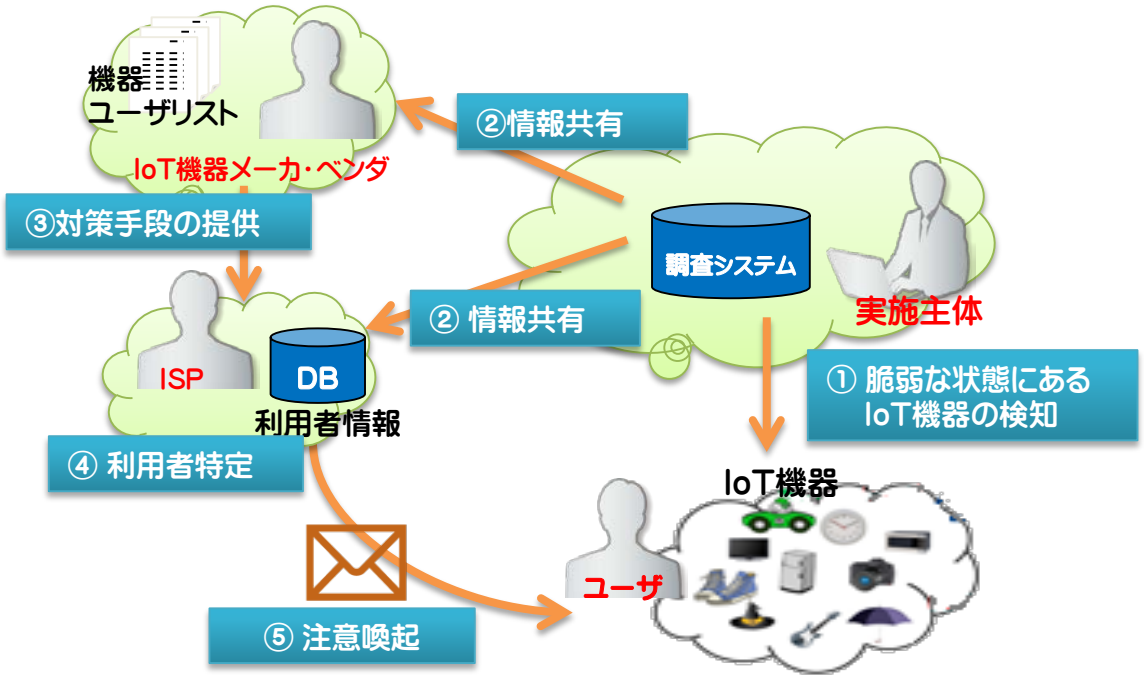
■ **IoT機器に関する脆弱性対策に関する実施体制の整備**

・ 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）。

IoT機器に関する脆弱性調査等の実施（平成29年9月5日　報道発表）

- ✓ IoT機器のセキュリティ対策は、IoT機器の性能が低く、また、IoT機器のメーカ、システム構築業者、サービス提供者等が複雑に連携して構築されており、従来のPCのようなセキュリティ対策が困難である。
- ✓ こうした課題に対処するため、ネットワーク上の脆弱なIoT機器の調査及びユーザへの注意喚起等、業界を超えたIoT機器に関するセキュリティ対策（IoTセキュリティフレームワーク）の調査・実証等を行う。

○ IoTセキュリティフレームワークのイメージ



【プロセス】

① 脆弱な状態にあるIoT機器の検知
　インターネット上をスキャンし、脆弱な状態にあるIoT機器を検知。

② 情報共有・蓄積
　①で収集した情報を蓄積し、機器メーカ・ISP事業者等に共有。

③ 対策手段の検討・提供
　IoT機器メーカ・ベンダが対策手段を検討・提供。

④ 利用者特定
　ISP事業者が当該機器の利用者を特定。

⑤ 注意喚起
　ISP事業者がユーザに対して注意喚起を実施。

（2）研究開発の推進

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。

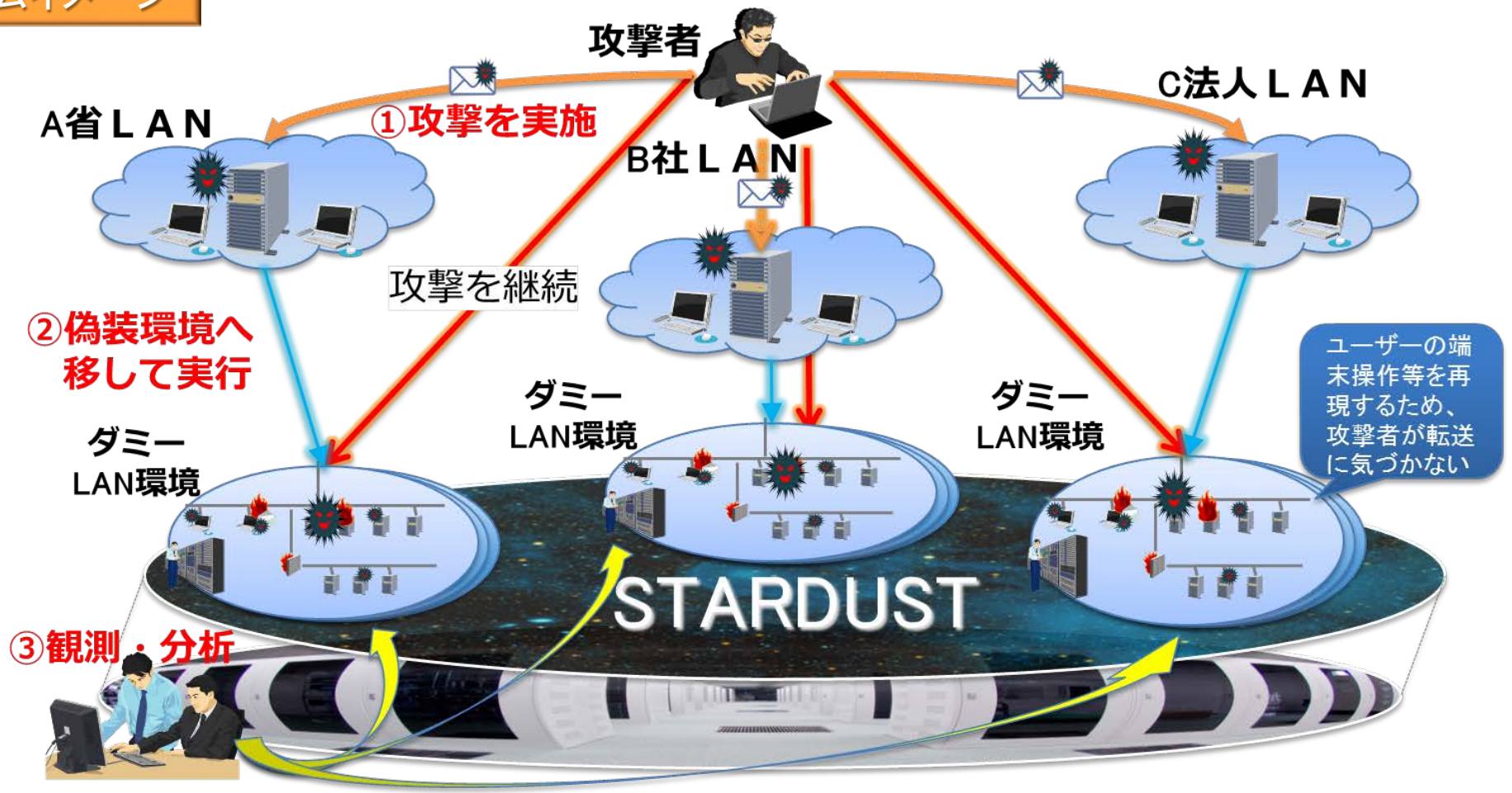
■AIを活用したサイバー攻撃検知・解析技術の研究開発

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。

サイバー攻撃誘引基盤

■ 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



（3）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）。

■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）。

IoT投資の抜本強化（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。

分科会における検討

公衆無線LANセキュリティ分科会

〇概要

公衆無線LANについては、2020年東京オリンピック・パラリンピック競技大会に向けて、観光や防災の観点から、その普及が進んでいる。しかし、公衆無線LANサービスの中には、セキュリティへの対策が十分でないものも多く、公衆無線LANサービスを踏み台にした攻撃や情報漏洩等のインシデントが発生することが考えられる。

このため、公衆無線LANにおけるセキュリティ上の課題を整理し、必要な対策について、検討を行う。

〇主な検討事項

・公衆無線LANのセキュリティ対策について
・セキュリティに配慮した公衆無線LANサービスの普及について

〇スケジュール

平成29年11月24日に第１回、 12月１日に第２回、12月27日に第３回、平成30年１月26日に第４回を開催。２月１日に「公衆無線LANセキュリティ分科会報告書（案）」を公表し、同月２日～21日まで意見募集を実施。年度内を目途に検討結果を取りまとめる予定。

情報開示分科会

〇概要

民間企業においては、複雑・巧妙化するサイバー攻撃に対する対策強化を進める動きが見られるようになってきており、こうした取組をさらに促進するためには、セキュリティ対策を講じている企業が市場を含む第三者から適切に評価される仕組みを構築していくことが求められている。

このため、あくまで任意の取組であることを前提としつつ、民間企業のセキュリティ対策の情報開示に関する課題を整理し、その普及に必要な方策について検討を行う。

〇主な検討事項

・情報開示する具体的な項目やその方法
・情報開示の普及の方策

〇スケジュール

平成29年12月13日に第１回、平成30年２月１日に第２回、２月27日に第３回を開催。年度内を目途に検討結果を取りまとめる予定。

（4）人材育成の強化

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。

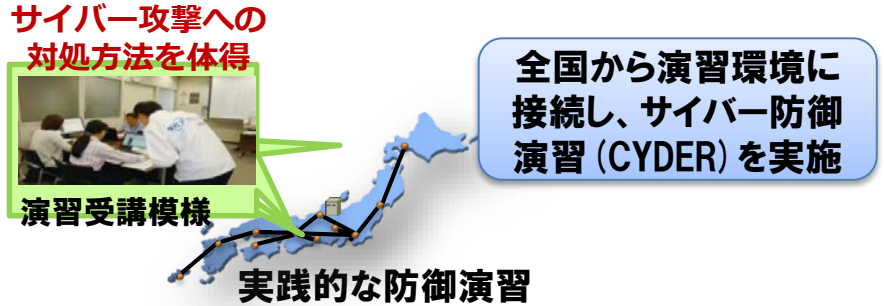
セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

○ 巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年に国立研究開発法人情報通信研究機構（NICT）に組織した「ナショナルサイバートレーニングセンター」において、下記取組を実施。

① 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、実践的な防御演習を実施 （CYDER）

② 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（サイバーコロッセオ）

③ 若手セキュリティエンジニアの育成 （SecHack365）



実践的な防御演習

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・教育コンテンツを開発

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

（5）国際連携の推進

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。

国際連携の推進

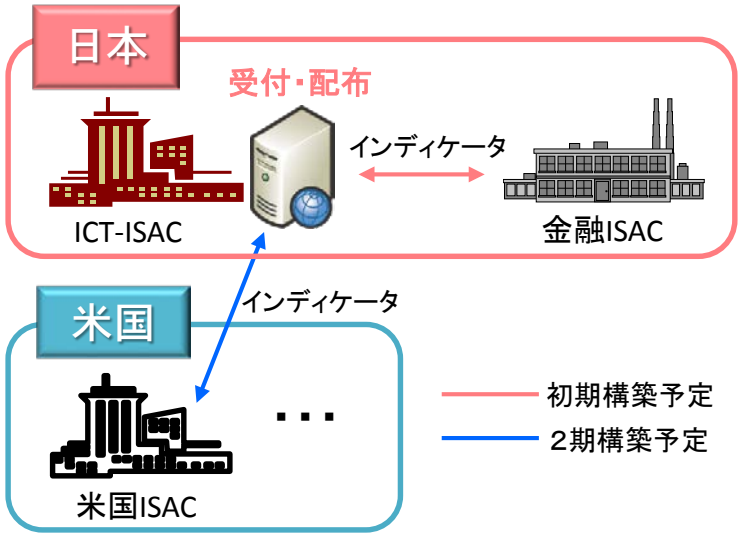
1. 情報共有

○ISAC（情報共有・分析センター）等の民間（主に情報通信業界）における国際連携を推進

- 米国ISACとのインディケータ、脅威分析情報等の共有
- ISAC連携国際ワークショップの継続的な開催（2016.11 東京）

○その他政府関係者においても情報共有を推進

- 二国間サイバー対話（2016.9日独、2016.10日英、2017.7日米 等）
- 日EU・ICT政策対話（2017.10）
- 日・ASEAN情報セキュリティ政策会議（2017.10）

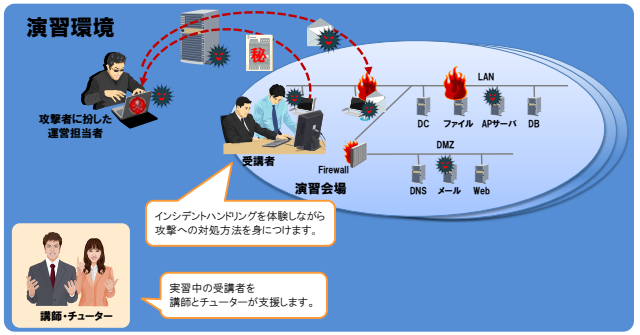


2. 能力構築

○実践的サイバー防御演習（CYDER）の海外展開を通じて、ASEAN等のセキュリティ人材育成を支援
また、人材育成を契機として、本邦企業によるSOC構築・運用等のセキュリティ事業展開を促進

- タイ（2015.11, 2017.2）、マレーシア（2017.1）
- JICA課題別研修（ASEAN向け）（2016年度～）

実践的サイバー防御演習のイメージ



ご清聴ありがとうございました