資料１－２

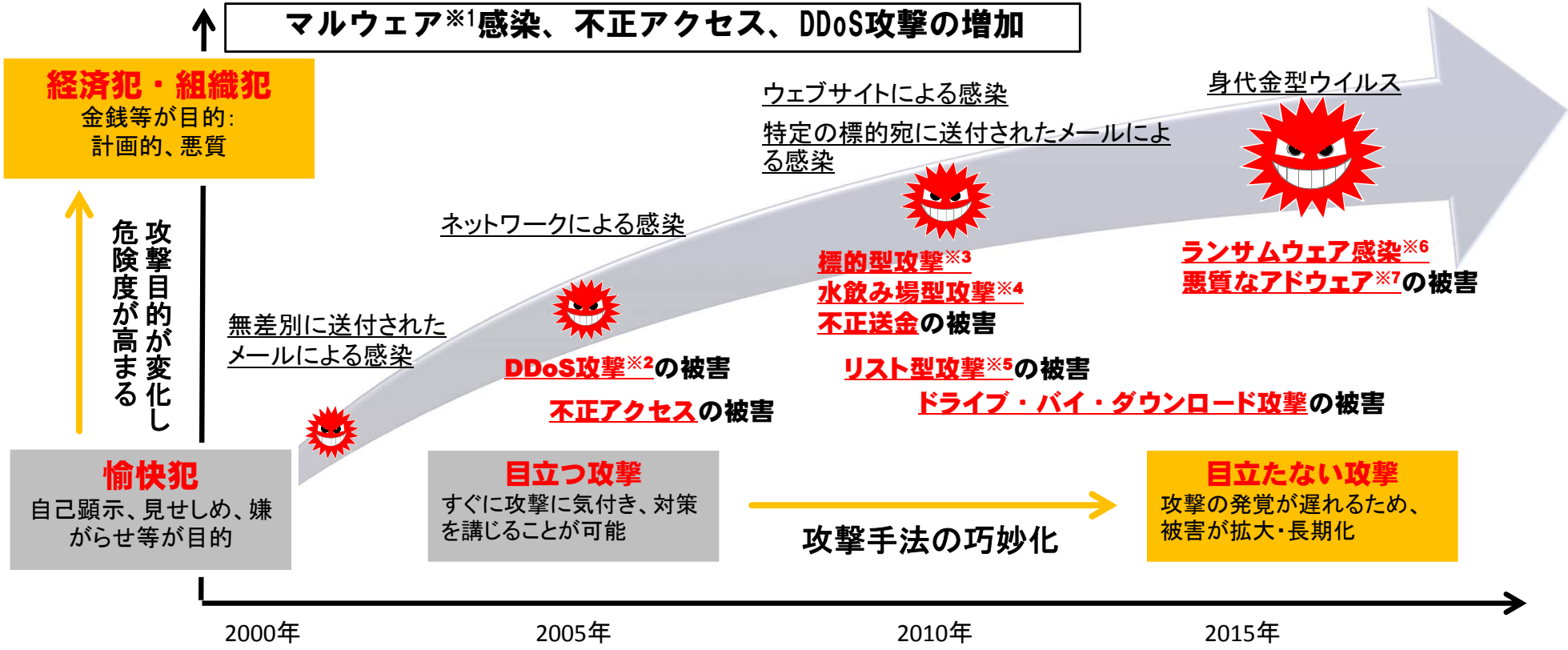
サイバーセキュリティの現状と総務省の対応について

平成29年1月30日

事務局

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。



※1 マルウェア（Malware）：Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃：分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃：機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃：標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃：不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア（Ransomeware）：身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)：広告表示によって収入を得るソフトウエアの総称。狭義には，フリーウエアと共にインストールされ，ブラウザー利用時に広告を自動的に付加するソフト

近年の大きなサイバー攻撃事案

国内事例

2013年8～9月・・・共同通信等によるニュースサイト「47行政ジャーナル」が改ざんされ、サイト閲覧者にマルウェア感染のおそれ （水飲み場型攻撃）

2014年9月・・・法務省のサーバやPCに不正アクセスがあり、法務局の情報が流出（不正アクセス）

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）

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）

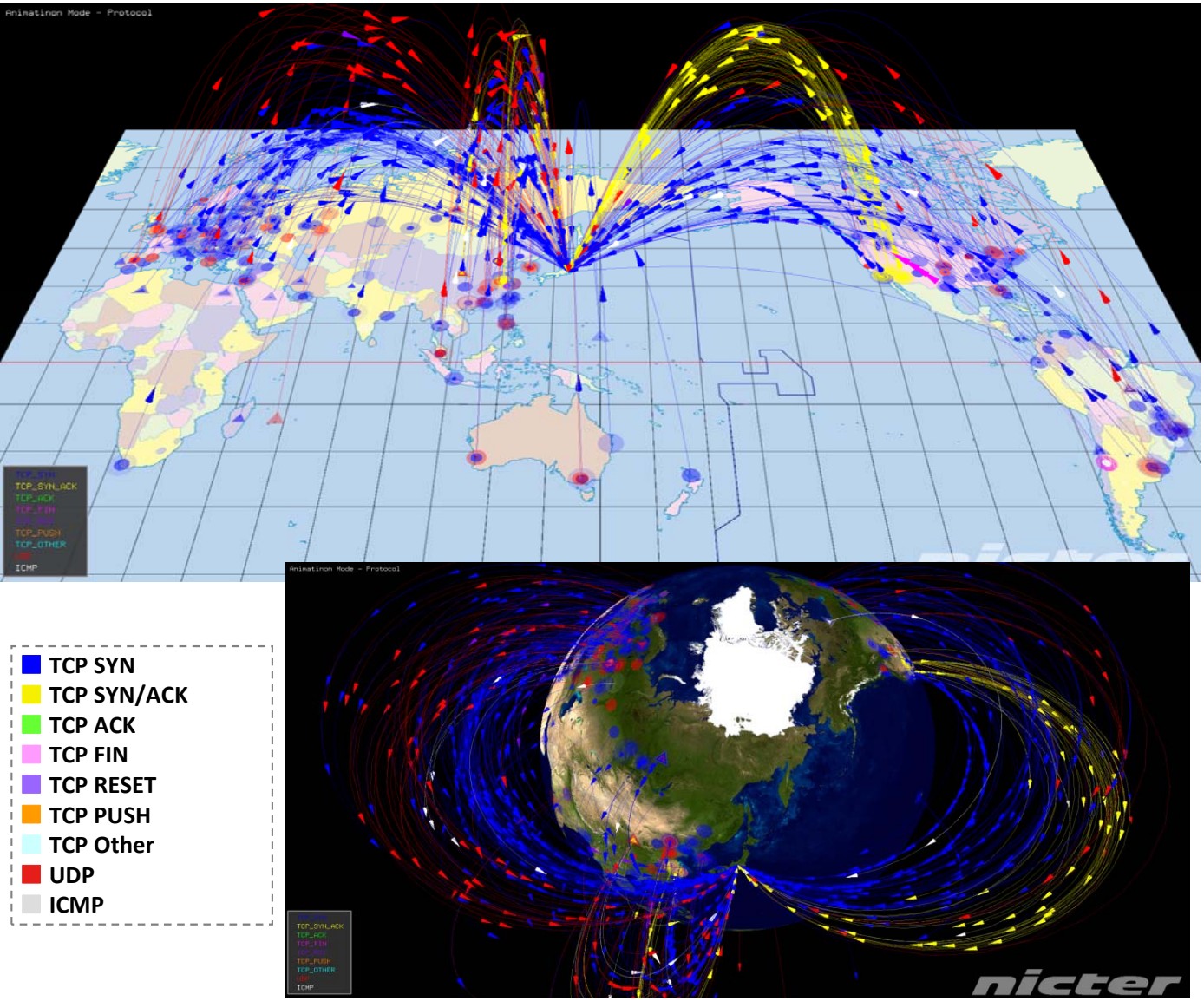
2015年6月・・・米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）

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）

サイバー攻撃の状況（NICTERによる観測）

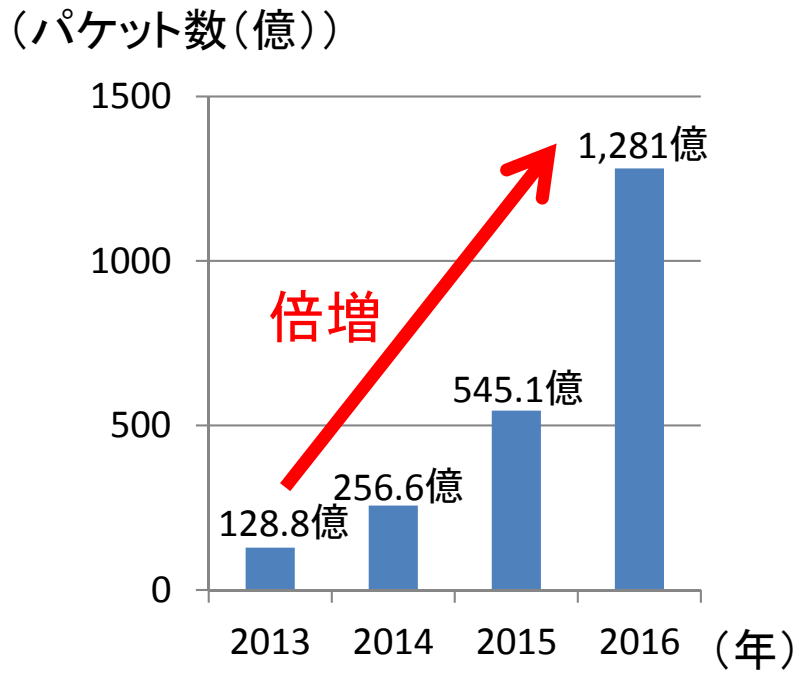
➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレスブロック30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。



・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

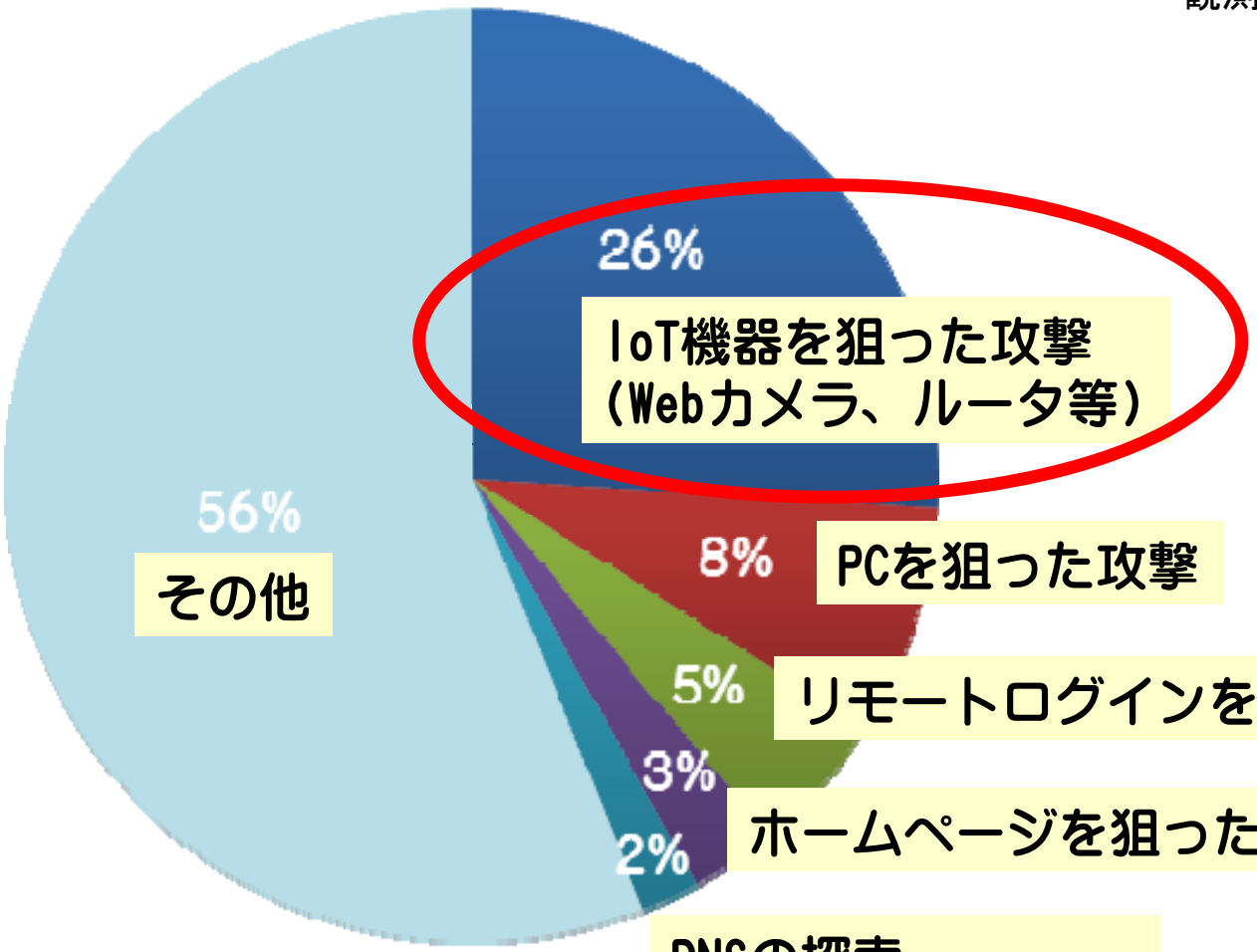
・色：パケットごとにプロトコル等を表現

１年間で観測されたサイバー攻撃回数



NICTで観測されたサイバー攻撃の対象

観測したサイバー攻撃の内訳（2015年）

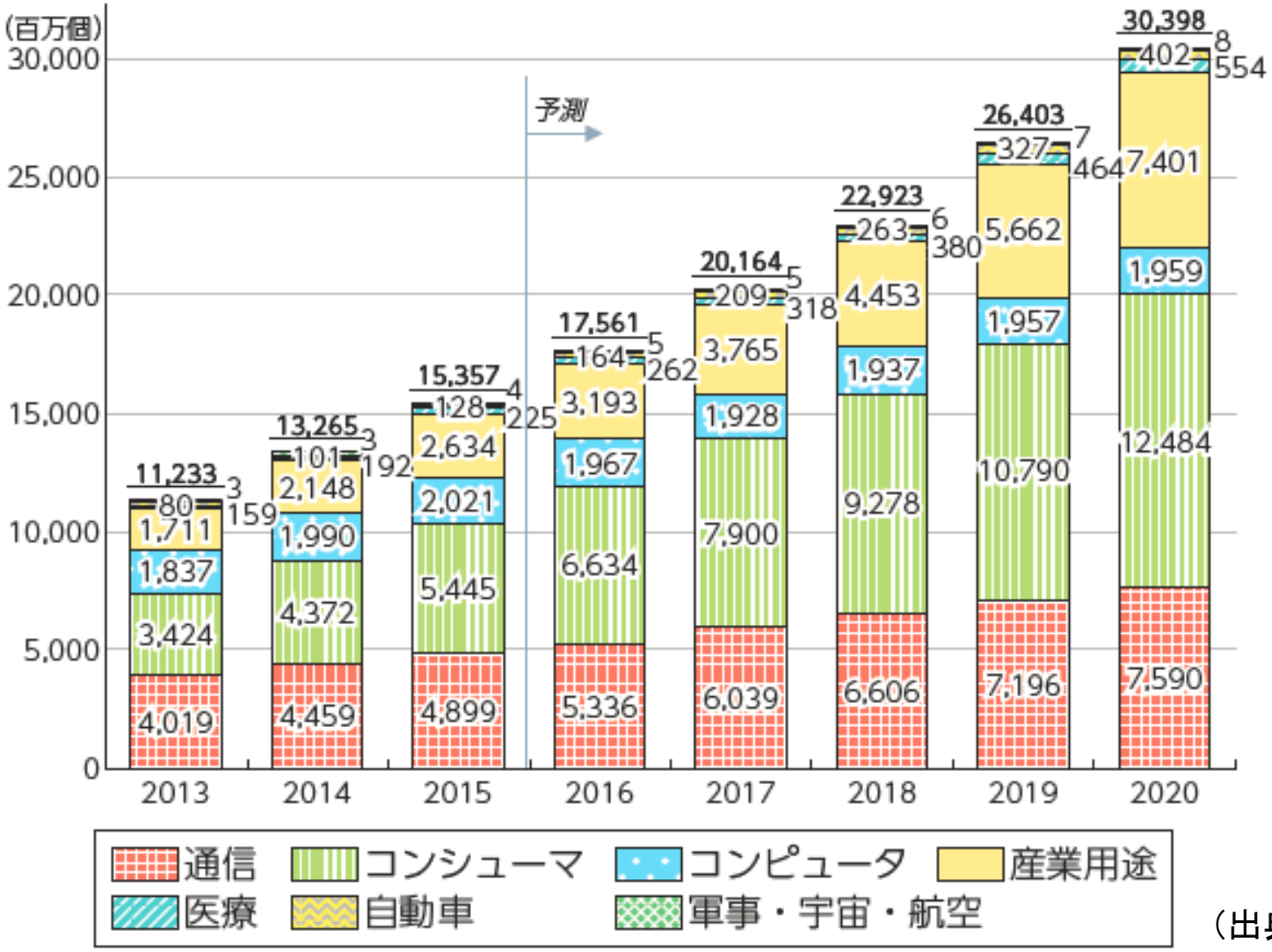


観測された全サイバー攻撃545.1億パケットのうち、

1/4がIoTを狙っている！

IoT機器の推移と普及分野

- IHS Technology の推定によれば、2015年時点でインターネットにつながるモノ（IoTデバイス）の数は154億個であり、2020年までにその2倍の304億個まで増加するとされており、そのうち、約4割が消費者向けのものである。

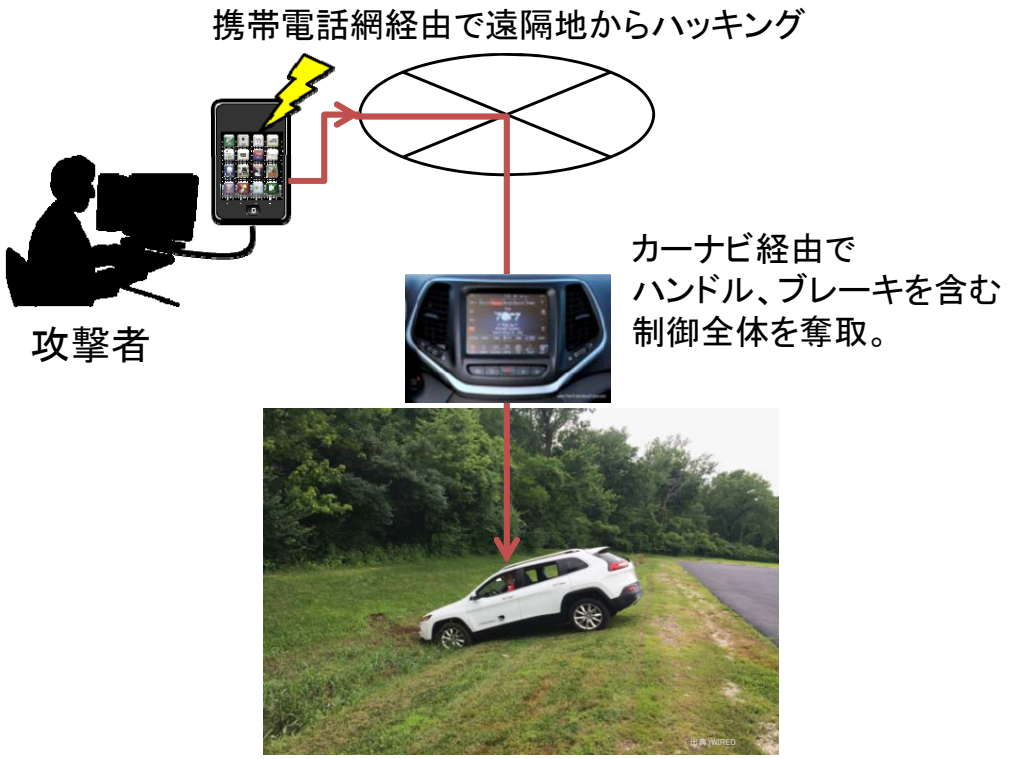


（出典）IHS Technology

IoTセキュリティ対策の必要性について

IoTでは、これまで接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングによる遠隔操作



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。
（ID, パスワードなどの初期設定が必要）

IoT機器がサイバー攻撃の対象として狙われやすい理由

○ IoT機器は、その性質から、サイバー攻撃の対象として狙われやすい状況にある。一般的なIoT機器特有の性質は下記のとおり。

① 脅威の影響範囲・影響度合いが大きい

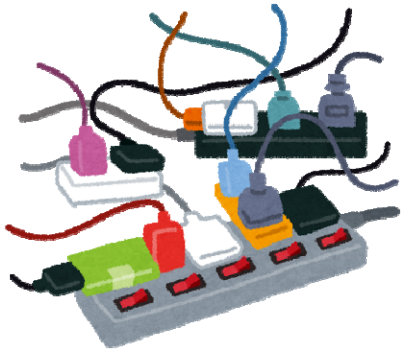
② IoT機器のライフサイクルが長い

③ IoT機器に対する監視が行き届きにくい

④ IoT機器側とネットワーク側の環境や特性の相互理解が不十分である

⑤ IoT機器の機能・性能が限られている

⑥ 開発者が想定していなかった接続が行われる可能性がある



IoTセキュリティガイドライン（Ver1.0）の策定

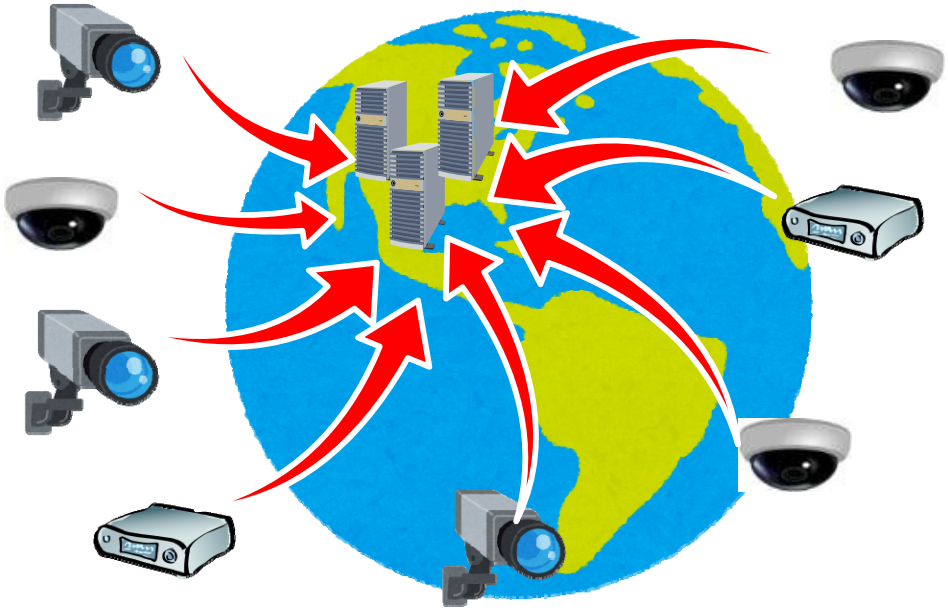
- 2016年1月より、「IoT推進コンソーシアム」において、IoT機器の設計・製造及びネットワークの接続等に関するセキュリティガイドラインを検討。
- 本ガイドラインは、IoTのセキュリティを確保するための「機器メーカ、サービス提供者などを対象にした5つの指針」及び「一般利用者を対象にしたルール」を分野横断的に定めたものであり、「IoT推進コンソーシアム、総務省及び経産省」の3者連名で、7月5日に公表。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	IoTのリスクを認識する	• 守るべきものを特定する • つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	• 出荷・リリース後も安全安心な状態を維持する • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る

今後、利用シーンを考慮した分野別の対策、官民連携によるセキュリティ対策の検討が必要

IoTによる大規模DDoS攻撃について

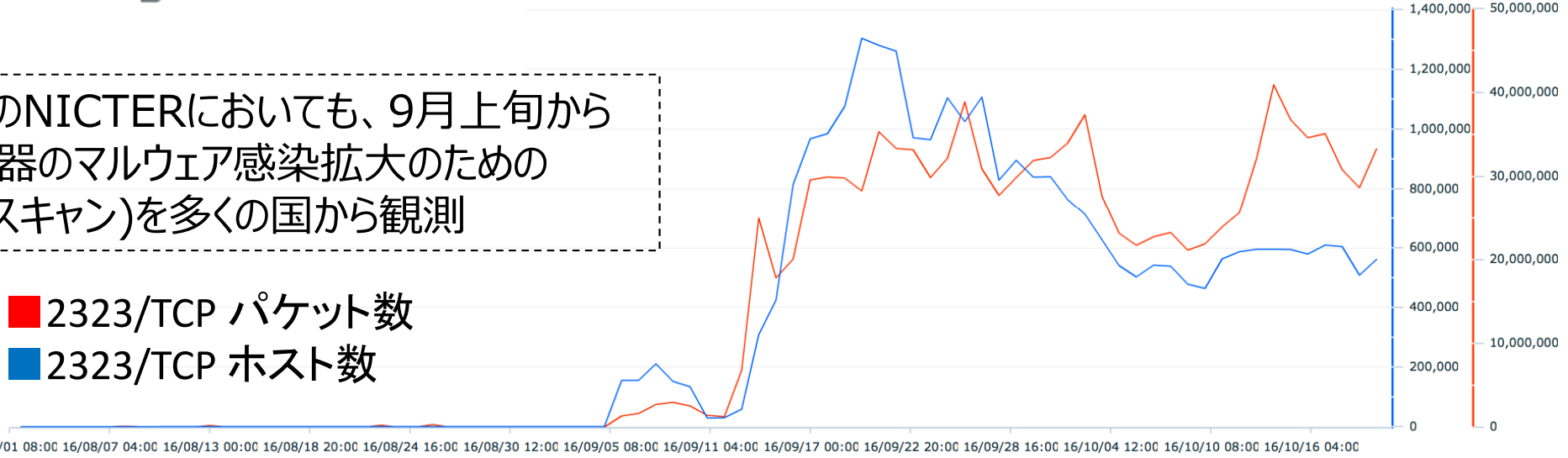
- 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。
- 同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。
- サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。



- ✓ 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。

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



IoTサイバーセキュリティ アクションプログラム2017

■ 総務省では、2020年東京オリンピック・パラリンピック競技大会を3年半後に控え、IoT機器・サービスが急速に普及する中、IoT時代に対応したサイバーセキュリティを早急に確立すべく、2017年に、関係府省・団体・企業等との緊密な連携の下、下記のサイバーセキュリティ施策を実施

1. サイバーセキュリティタスクフォースの開催

✓ IoT/AI時代のサイバーセキュリティに関する基盤・制度、人材育成、国際連携のあり方等、包括的な政策推進についてICT関係部署の司令塔の役割を担うサイバーセキュリティタスクフォースを開催、必要な施策を検討・実施

2. IoT機器セキュリティ対策の実施

✓ IoTによる大規模サイバー攻撃が発生する中、脆弱性のあるIoT機器を把握し、その機器の管理者に注意喚起を行うとともに、IoTセキュアゲートウェイの実証を行うなど、今後の抜本的なIoT機器セキュリティ対策を確立

3. セキュリティ人材育成のスピードアップ

✓ 2016年度内に、2020年オリパラ東京大会に向けた演習（「サイバーコロッセオ」）及びセキュリティ競技大会（「サイバーコロッセオ×SECCON」）を実施するとともに、引き続きサイバー防御演習を実施し、セキュリティ人材を発掘・育成

✓ ナショナルサイバートレーニングセンター（仮称）をNICTに組織し、サイバー防御演習を47都道府県に拡大、東京大会に向けた演習の強化、若手セキュリティエンジニアの育成（新規）を実施（2017年度政府予算案）

4. 総務大臣表彰制度の創設

✓ 企業・団体等サイバーセキュリティ対応の最前線（現場）において優れた功績を挙げている個人・団体を顕彰する総務大臣表彰制度を創設

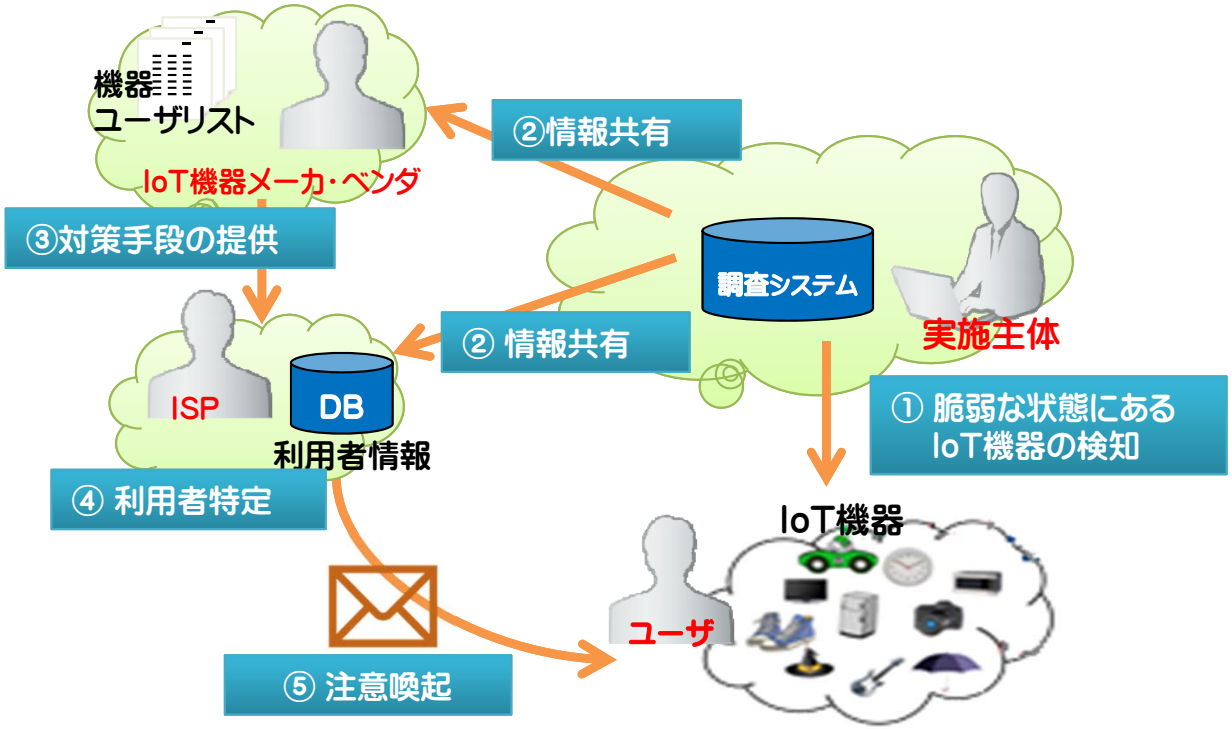
5. 国際連携の推進

✓ ASEANにおけるサイバー防御演習の拡大（現在2ケ国）、セキュリティコンテストの実施に向けて、関係各国との連携体制を強化し、サイバーセキュリティ能力の向上及びセキュリティ人材の国際交流に貢献

IoTセキュリティフレームワークの実証実験

- ✓ 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。

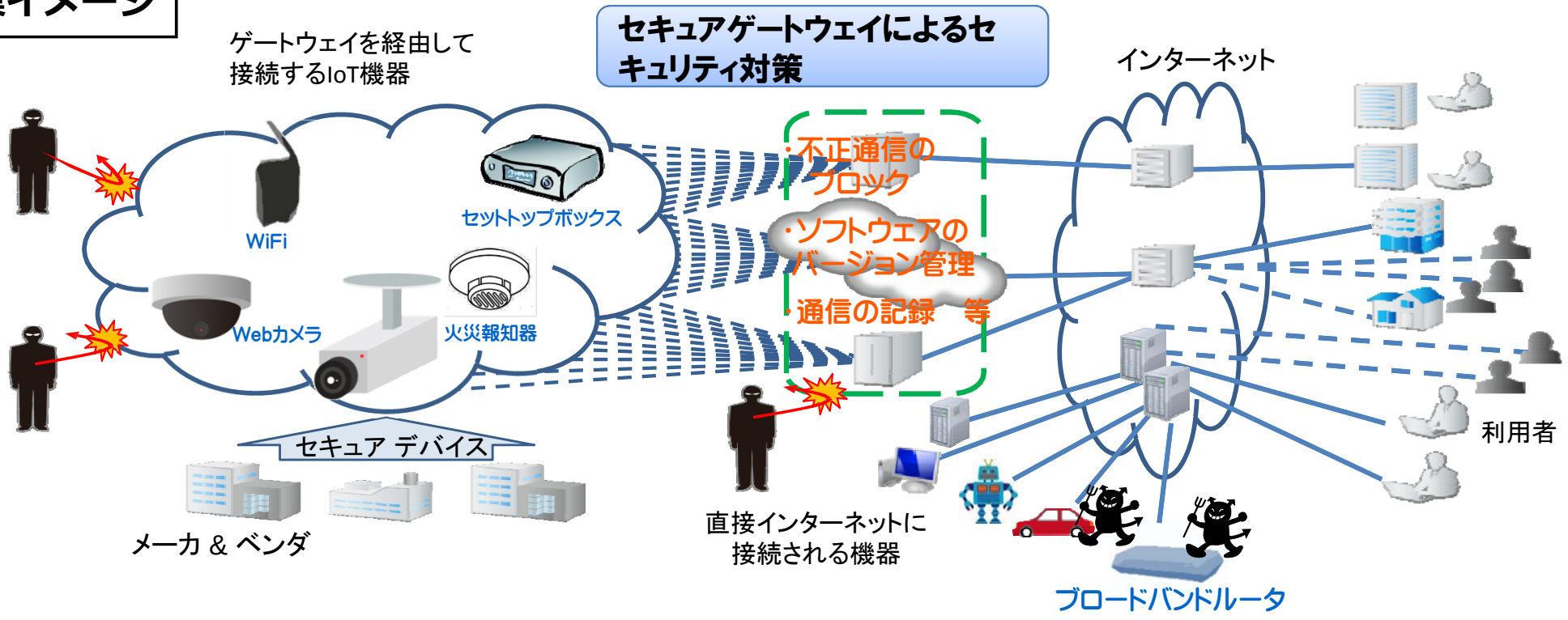
④ 利用者特定
　ISP事業者が当該機器の利用者を特定。

⑤ 注意喚起
　ISP事業者がユーザに対して注意喚起を実施。

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及び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、総務省・経済産業省・IoT推進コンソーシアムにおいて平成28年7月に策定した「IoTセキュリティガイドライン」も踏まえ、IoT機器とインターネットの境界上にセキュアなゲートウェイを設置し、低機能なIoT機器のセキュリティを確保するための取組に関する実証・検証を実施。

事業イメージ



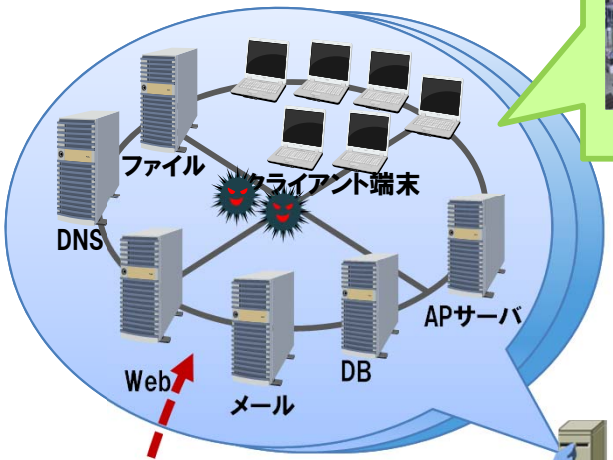
実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

（サイダー　サイバー　防御　反復演習）

- 総務省では、平成25年度から国の行政機関や重要インフラ事業者を主な対象として実践的サイバー防御演習を実施。
- 今般、サイバー攻撃の脅威の深刻化を踏まえ、NICTの技術的知見等を活用し、演習を拡大・強化。

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

都内（品川）

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）

これにより、演習の質の向上や継続的・安定的な運用を実現。

→　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27年度は官公庁、重要インフラ事業者など、約80組織、約200人が演習に参加

2020年東京オリンピック・パラリンピック開催に向けたサイバー演習による人材の育成

概要

2020年東京オリンピック・パラリンピック競技大会関連組織のセキュリティ関係者が、大会開催時を想定した模擬環境で攻撃・防御双方の実践的な演習を行うことにより、高度な攻撃に対処可能な高度な能力を有するサイバーセキュリティ人材の育成を行う。また、関係組織が一体となった演習を実施することで個々の組織の強化だけでなく、組織間の連携も強化する。

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

「ナショナルサイバートレーニングセンター（仮称）」構想

概要

○　IoTの普及や、2020年東京オリンピックパラリンピック競技大会を控え、サイバーセキュリティの確保を担う人材※の育成に早急に取り組むため、情報通信研究機構(NICT)に「ナショナルサイバートレーニングセンター（仮称）」を組織し、下記取組を実施。(2017年度政府予算案)

※　国内セキュリティ技術者約26.5万人のうち約16万人が能力不足、更に約８万人が不足しているとされる。
（「サイバーセキュリティ戦略」（平成27年９月））

・官公庁、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実践的なサイバー防御演習

⇒ *47都道府県で演習を実施し、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*

・若手セキュリティエンジニアの育成

⇒ *セキュリティ対策技術を開発できる国内の若手人材の育成を新規に開始*

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（仮称）」でプラットフォーム化

国際会議等を活用した各国との連携強化

多国間連携

- ✓ 日・ASEAN情報セキュリティ政策会議（NISC、経済産業省と連携）
  総務省施策の紹介やASEAN各国とのJASPERによる連携の推進。
- ✓ APEC-TEL SPSG（セキュリティ・繁栄分科会）
- ✓ APTサイバーセキュリティフォーラム
- ✓ 国際サイバー会議

二国間連携

- ✓ 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EUサイバー対話　等
- ✓ インドネシア、マレーシア、シンガポール、フィリピン、タイ等とのNICTER Web Premiumを中心とした連携
- ✓ ミャンマー、ベトナムにおけるODA案件の形成、タイ等におけるCYDER演習による連携

ITU関連

- ✓ ITU-T SG17（セキュリティ）
  - ・ 日本からの標準化寄書取りまとめ等。（国内のTTCセキュリティ専門委員会と連携）
  - ・ 標準化提案活動の推進（ITS、IoT、クラウドにおけるセキュリティ等）
- ✓ ITU関連会合
  - ・ ITU全権会議（ITUの役割強化等）、ITU-D（途上国対応等）、APT（アジア太平洋向け研修・フォーラム対応等）等におけるサイバーセキュリティ議題

ASEANとの連携

● **日・ASEANサイバーセキュリティ協力に関する閣僚政策会議**（2013年9月東京）
- セキュリティをテーマとする日・ASEANで初の閣僚レベルの会議
- 我が国からの提案に基づき、次のプロジェクトを連携して勧めることで合意

①JASPER（ジャスパー）(Japan-ASEAN Security Partnership)

i）PRACTICE（プラクティス）：我が国及び連携国に設置したセンサーにて、サイバー攻撃発生の予兆を検知するためのプロジェクト

ii）DAEDALUS（ダイダロス）：連携国内のPCからのウィルス感染が疑われるトラフィックが観測された場合に、連携国に警告を送付するプロジェクト

②ASEANサイバーセキュリティ人材育成イニシアティブ

● **日・ASEAN情報セキュリティ政策会議**
- 情報セキュリティを担当する局長級の会議。2009年に第１回を開催し、2016年10月20日・21日、第9回を日本（東京）で開催。

● **日・ASEANサイバーセキュリティ協力ハブ**
- 日本の支援を通じてASEAN各国が連携してサイバー攻撃に対応する拠点をASEAN域内に構築。
- 日・ASEAN統合基金（JAIF）による約三年間の支援を予定。

PRACTICE連携国

・タイ	2013年2月～
・マレーシア	2013年3月～
・インドネシア	2013年5月～
・フィリピン	2014年1月～
・シンガポール	2014年3月～

DAEDALUS連携国

・ミャンマー	2013年10月～
・ラオス	2013年11月～
・インドネシア	2013年11月～
・フィリピン	2013年12月～
・マレーシア	2014年3月～
・タイ	2016年4月～

連携国拡大の働きかけ

ASEANにおけるサイバー脅威の認識共有、情報交換のための基盤として活用

ASEANサイバーセキュリティ人材育成イニシアティブ

①　（独）国際協力機構（JICA）専門家派遣
- 2014年７月から2年半、2名の専門家をインドネシアに派遣
- ニーズに合わせた研修を企画・立案

②　実践的サイバー防御演習（CYDER）の海外展開
- ASEAN域内でのCYDER演習実施の検討

政府職員のサイバー攻撃等への対応能力の強化

G7情報通信大臣会合 協調行動集を踏まえた取組

G7情報通信大臣会合（2016年4月）協調行動集
- NICTERにおける連携
- ISAC間の連携

情報共有 (NICTER)

主に途上国

サイバー攻撃観測・分析・対策システム（NICTER）で脅威情報を可視化
- NICTERセンサーの設置（インドネシア、タイ、マレーシア、シンガポール、フィリピン）
- NICTER Web PremiumによるASEAN地域での情報共有トライアル（2016年9月）

今後の方向性：センサー設置国の拡大、ASEAN10ヶ国での情報共有をめざす

官民連携 (ISAC)

主に先進国

民間における情報共有・分析センター(ISAC)間での情報連携を推進
- 日米会合（2016年7月）
- 日米欧ワークショップ（2016年11月）

今後の方向性：脅威情報共有の可能性を検討中

能力構築 (CYDER)

主に途上国

実践的サイバー防御演習の海外展開を通じて能力構築を支援
- タイ（2015年11月実施、2017年2月予定）、マレーシア（2017年1月実施）での演習実施
- ASEANハブの構築（2017年～）

今後の方向性：ASEANハブのフィージビリティスタディ準備中

高市総務大臣のマレーシア出張（結果概要）

2017年1月16日から18日まで、高市総務大臣が、マレーシアを訪問。サッレー通信・マルチメディア大臣との会談、情報通信分野の協力に関する覚書への署名、伊勢丹ジャパンストアの視察等を実施。

1. サッレー通信・マルチメディア大臣との会談（於：通信・マルチメディア省大臣室）

○ 日マレーシア外交関係樹立60周年となる2017年において両国間の関係を更に強化する観点から、防災ICT、**サイバーセキュリティ**、モバイル決済システム、放送コンテンツ、5G、IoTなど情報通信分野における両国間の協力を一層推進していくことを確認。

サッレー大臣との会談の模様

2. 情報通信分野の協力に関する覚書への署名（於：通信・マルチメディア省地下講堂）

○ 上記1. の会談を受け、両大臣は、総務省とマレーシア政府との間の情報通信分野の協力に関する覚書に署名。覚書は、防災ICT、**サイバーセキュリティ**、モバイル決済システム、放送コンテンツ、5G、IoTといった協力分野について、政策や規制に関する情報交換、産業連携や技術的協力の促進などを行う内容。

○ なお、本覚書は、日マレーシア首脳会談（2016年11月）において言及されたことを受け、今回、署名の運びとなった。

覚書署名式の模様

3. 伊勢丹ジャパンストアの視察

○ 2016年10月に開業した「ISETAN The Japan Store」を訪問し、総務省事業の一環で日マレーシアの放送事業者が共同製作した番組と連動した愛媛みかんのプロモーション活動のほか、日本各地の産品が販売されている現場を視察。

その他、１８日（水）に、日本人墓地献花、ICT関連施設（データセンター）視察を実施。

（参考１）2020年に向けた社会全体のICT化　アクションプラン概要

総務省「2020年に向けた社会全体のICT化推進に関する懇談会」資料より抜粋

言葉の壁をなくす

多言語音声翻訳対応の拡充

- ✓ グローバルコミュニケーション開発推進協議会中心に翻訳技術の社会実装化。
- ✓ 対応する言語や分野の拡充（医療、ショッピング、観光等分野）。

2017年までに10言語での翻訳対応拡充

情報の壁をなくす

デジタルサイネージの機能拡大

- ✓ 災害時の情報一斉配信、属性に応じた情報提供実現。
- ✓ このため、DSC※1中心に共通仕様策定、サイネージの機能を共通化。

2019年までに相互接続を可能とするシステムの実現

移動の壁をなくす

オープンデータの利活用推進

- ✓ 公共交通の運行情報等がリアルタイムに把握可能に。
- ✓ 公共交通オープンデータ協議会を中心に観光地等における社会実証。

2018年度末までに公共交通オープンデータセンターを本格稼働

日本の魅力を発信する

放送コンテンツの海外展開

- ✓ 関係省庁連携の下、BEAJ※2を中心に、放送局や権利者団体が協力しつつ推進。

2018年度までに放送コンテンツ関連海外市場売上高を2010年度の約3倍に増加

※1 DSC：一般社団法人 デジタルサイネージコンソーシアム
※2 BEAJ：一般社団法人 放送コンテンツ海外展開促進機構

高度なICT利活用

【各分野横断的なアクションプラン】

Ⅰ．都市サービスの高度化

ースマートフォンや交通系ICカード等を活用。街中や公共施設のサイネージ、商業施設や宿泊施設等において、訪日外国人、高齢者、障がい者をはじめ、誰もが、属性（言語等）や位置に応じた最適な情報やサービスを入手。

2016年度中に実施地域での先行着手。2020年までに社会実装を実現。

Ⅱ．高度な映像配信サービス

ー映画館、美術館・博物館、競技場などの公共空間のデジタルサイネージ等大画面に対し、臨場感ある4K・8Kの映像配信を実現。

2016年度中に実施地域での先行着手。2020年までに全国の各地域へ展開。

世界最高水準のICTインフラ

※3 A-PAB：一般社団法人放送サービス高度化推進協会

接続の壁をなくす

無料公衆無線LAN環境の整備促進

- ✓ 無料公衆無線LAN整備促進協議会中心に、認証連携等に着手。
- ✓ 防災拠点、被災場所として想定される公的拠点約3万箇所に整備。

2015年から認証連携等に着手
2020年までに防災拠点等に整備

利用のストレスをなくす

第5世代移動通信システムの実現

- ✓ 第5世代モバイル推進フォーラムを中心に主要国・地域との国際連携を強化。
- ✓ 2017年度から5Gの社会実装を念頭に総合的な実証試験を実施。

2020年に世界に先駆けて5Gを実現

臨場感の向上、感動の共有

4K・8Kの推進

- ✓ NHKやA-PAB※3により4K・8Kの実用放送開始等に向けた試験放送を実施。

2018年に4K・8Kの実用放送開始

利用の不安をなくす

サイバーセキュリティの強化

- ✓ 実践的なサイバー防御演習を通じたサイバーセキュリティ人材の育成
- ✓ ICT-ISACを通じたICT分野全体にわたる情報共有の促進

2016年度からサイバー防御演習及び情報共有体制の拡充・強化

（参考２）ITSを発展させて実現する「Connected Car」社会

総務省「Connected Car社会の実現に向けた研究会」資料より抜粋

これまでのITS

VICS　→　渋滞情報提供
ETC　→　料金所渋滞の解消
レーダー→　追突防止
ITSスポット　→　安全情報提供
（それぞれは独立）

基本的には車がネットワークに依存しないでサービス展開

初期の自動運転機能
（車に搭載したカメラやレーダを活用）

簡単なネット接続機能
（携帯電話回線を利用して、車の位置情報等を収集・利用）

個々のITSシステムやクルマ単体でのセキュリティ対策

ＩＴＳを取り巻く世界が大きく拡大

５Ｇ、ビッグデータ、ＡＩ等の進化

「クルマ」
×
「ネットワーク」
×
「データ」
×
「AI」

将来の「Connected Car」社会

ネットとクルマがつながるのがあたりまえの世界

○たくさんのクルマのセンサーがネットに接続
→　クルマの情報を活用した新サービス創出
－IoTによるメンテナンスの提案＆予約サービス
－近くのレストラン等を提案し、自動でナビ設定　等

**車とネットワークがつながり
新たな価値やビジネスが創出される
安全・安心な「Connected Car」社会**

一方でセキュリティのリスクは増大

より高度な自動運転機能

○通信で最新の高精度地図や道路交通情報を入手し、スムースな自動運転を実現
－新規開通した道路でもすぐに自動運転が可能　等

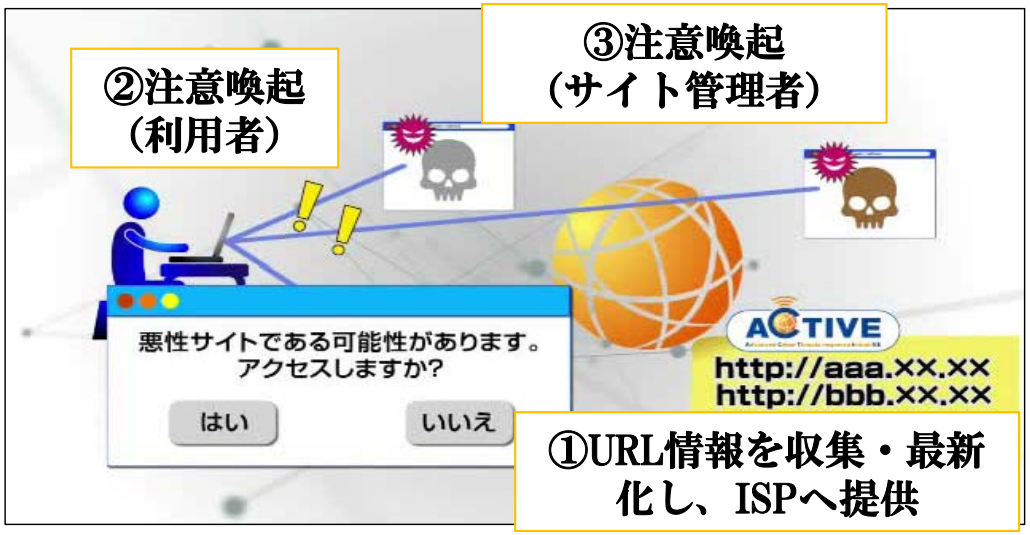
総合的なセキュリティ対策の重要性が増大

○「Connected Car」社会全体を俯瞰した総合的対策が必要
－遠隔操作・サイバーアタック対策　等

（参考３）ACTIVE（Advanced Cyber Threats response InitiatiVE）について

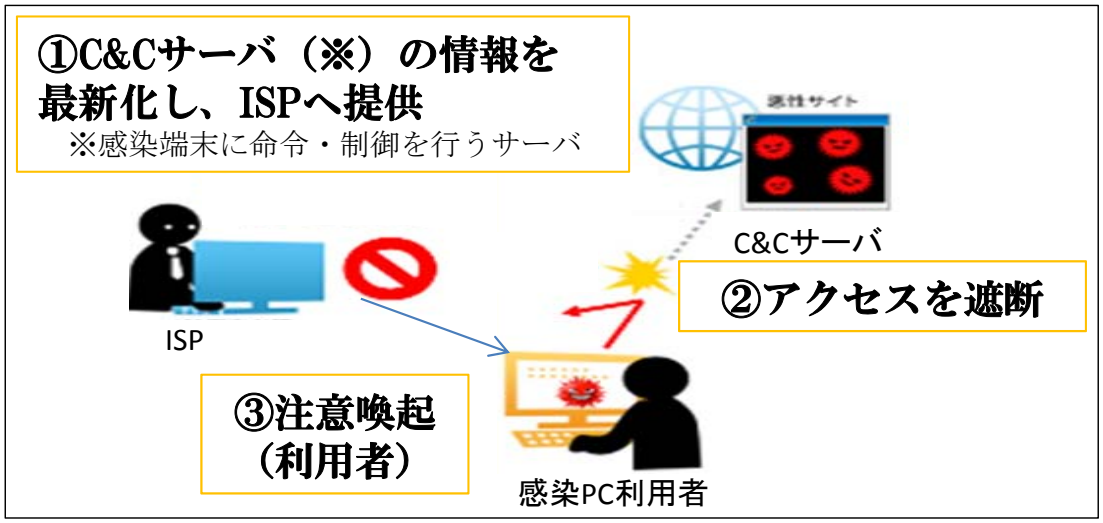
✓ 2013年１１月からインターネットサービスプロバイダ（ISP）等との協力により、インターネット利用者を対象に、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト（ACTIVE）を開始。

（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2016年12月までの11ヶ月間で約135万件の遮断実績）
③ 感染PC利用者に注意喚起。

（参考４）情報共有基盤の構築

- ✓ 国内のサイバー攻撃や脆弱性の情報を収集・分析し、通信事業者や放送事業者（ICT-ISAC）、金融機関（金融ISAC）等の関係者間で共有することで、適切な対策を促す仕組みを構築・実証。
- ✓ 情報収集から配布・適用までを自動化し、迅速な情報共有が可能。