総務省
Ministry of Internal Affairs and Communications

総務省におけるサイバーセキュリティ政策の最新動向

平成29年2月3日

総務省 情報流通行政局 情報セキュリティ対策室

山田　隆裕

講　演　内　容

1. ｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威と政府全体の取組

2. IoTにおけるｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威

3. IoTｻｲﾊﾞｰｾｷｭﾘﾃｨ ｱｸｼｮﾝﾌﾟﾛｸﾞﾗﾑ 2017

講　演　内　容

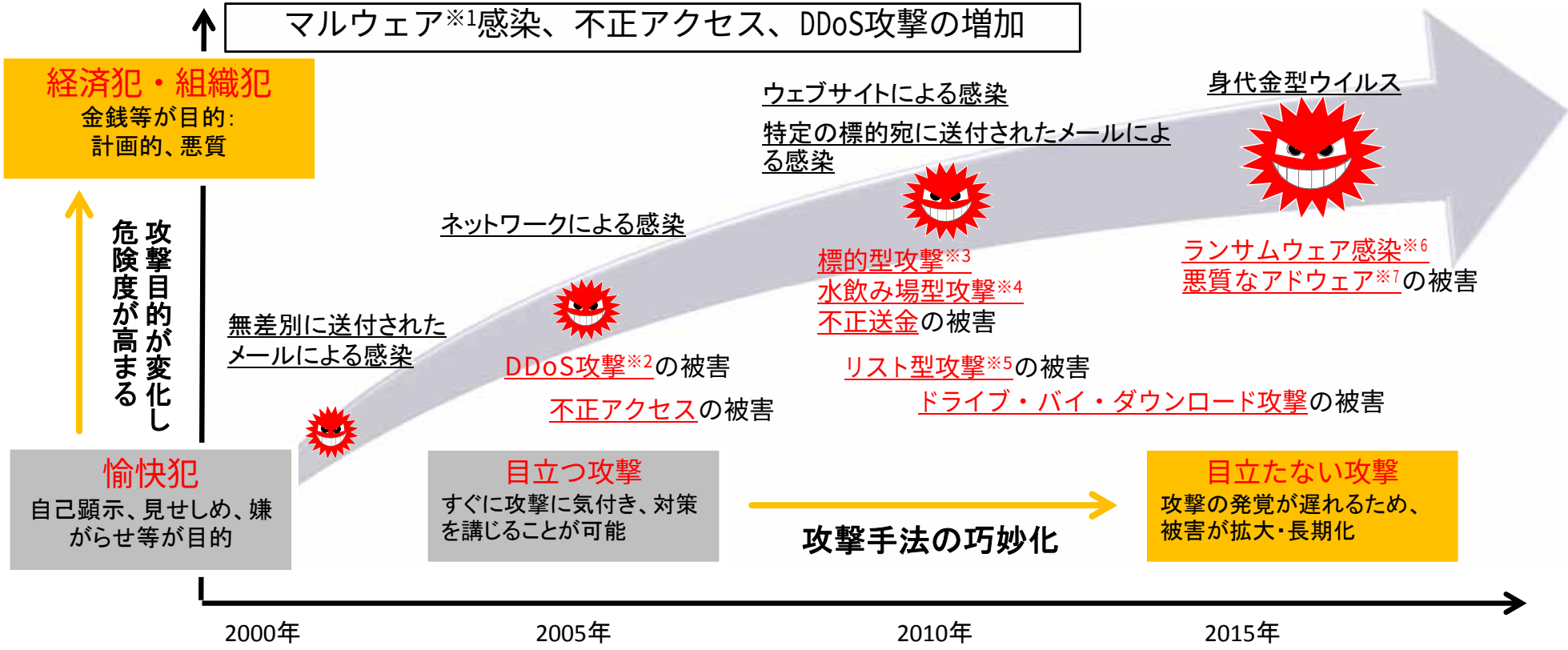
1. ｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威と政府全体の取組

2. IoTにおけるｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威

3. IoTｻｲﾊﾞｰｾｷｭﾘﾃｨ ｱｸｼｮﾝﾌﾟﾛｸﾞﾗﾑ 2017

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）

サイバーセキュリティ政策の経緯

省庁ＨＰ連続改ざん 2000.1
Webサーバの脆弱性への攻撃
米国同時多発テロ 2001.9
フィッシング詐欺 スパイウェア
ボットネットによる攻撃
Winny
DNSキャッシュポイズニング
誘導型攻撃の出現
米韓ＤＤｏＳ攻撃
Gumblar猛威
制御ｼｽﾃﾑStuxnet攻撃
9.18攻撃
韓国大規模障害
遠隔操作ウィルス
水飲み場型攻撃
標的型攻撃 組織的高度化
米国での中国軍関係者起訴・指名手配
感染PCによる不正送金
米国ｿﾆｰ(SPE)
年金機構情報流出

○今後の重要な環境変化
- オリンピック・パラリンピック東京大会
- マイナンバー利用開始
- IoTの広がり　等
  （スマートメーター、自動走行システム等）

年度 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017

試行錯誤 | DoS攻撃、コンピュータウイルス対策 | リスクゼロ社会 | 「事故前提社会」でのリスクベース対策 | 国家安全保障・危機管理としてのサイバーセキュリティ　高度なサイバー脅威に対し、積極的な対処が求められる時代に

e-Japan 戦略 (2001.1.22)
e-Japan 戦略Ⅱ (2003.7.2)
IT新改革戦略 (2006.1.19 IT戦略本部決定)
i-Japan 戦略2015 (2009.7.6)
新たな情報通信技術戦略 (2010.5.11 IT戦略本部決定)
世界最先端ＩＴ国家創造宣言 (2013.6.14 閣議決定,2014.6.24改訂、2015.6.30改訂、2016.5.20改訂)

参考：IT利活用

基本戦略
第１次 情報ｾｷｭﾘﾃｨ基本計画 (2006.2.2 政策会議決定)
第２次 情報ｾｷｭﾘﾃｨ基本計画 (2009.2.3 政策会議決定)
国民を守る情報ｾｷｭﾘﾃｨ戦略 (2010.5.11 政策会議決定)
ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2013.6.10 政策会議決定)
サイバーセキュリティ基本法公布 (2014.11.12)
新・ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2015.9.4 閣議決定)

年次計画
SJ2006 SJ2007 SJ2008 SJ2009 JS2010 JS2011 JS2012 CS2013 CS2014 CS2015 CS2016
SJ：セキュアジャパン　JS：情報セキュリティ　CS：サイバーセキュリティ

政府機関対策
情報セキュリティポリシーに関するガイドライン (2000.7 情報ｾｷｭﾘﾃｨ対策推進会議決定)
政府機関の情報セキュリティ対策のための統一基準
第1版 (2005.12.13 政策会議決定)
第2版 (2007.6.14 政策会議決定)
第3版 (2008.2.4 政策会議決定)
第4版 (2009.2.3 政策会議決定)
平成23年度版 (2011.5.11 政策会議決定)
平成24年度版 (2012.4.21 政策会議決定)
平成26年度版(2014.5.19 政策会議決定)
平成28年度版(2016.●.● 戦略本部決定)

重要ｲﾝﾌﾗ対策
重要インフラのサイバーテロ対策に係る特別行動計画 (2000.12 情報ｾｷｭﾘﾃｨ対策推進会議決定)
重要インフラの情報セキュリティ対策に係る行動計画 (2005.12.13 政策会議決定)
重要インフラの情報セキュリティ対策に係る第2次行動計画 (2009.2.3 政策会議決定)
重要インフラの情報ｾｷｭﾘﾃｨ対策に係る第3次行動計画 (2014.5.19 政策会議決定)
重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ (2016.3.31 政策会議決定)

組織体制
内閣官房 情報セキュリティ対策推進室 (2000.2設置)
内閣官房情報セキュリティセンター (2005.4 設置)
情報セキュリティ政策会議 (2005.5 設置)
GSOC (2008.4 運用開始)
CYMAT (2012.6 設置)
内閣官房内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ (2015.1設置)
サイバーセキュリティ戦略本部 (2015.1設置)

我が国における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

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（平成27年1月9日　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　ｻｲﾊﾞ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
オリパラ担当大臣
有識者（7人）※

閣僚が参画

※　遠藤　信博　日本電気株式会社代表取役執行役員社長
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　首都大学東京法科大学院教授
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

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

緊密連携

その他の関係省庁

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
文部科学省（セキュリティ教育）　等

協力

（事務局）内閣サイバーセキュリティセンター（NISC）

（平成27年1月9日　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）、国家安全保障局次長を兼務）

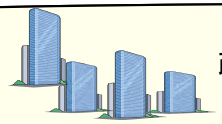
政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）

協力

閣僚本部員5省庁

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


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基本法の概要（平成28年改正後）

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民１人１人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置（第24条）

■所掌事務等（第25条）

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査等の実施

■組織等（第26条～第29条）

⇒内閣官房長官を本部長として、副本部長（国務大臣）、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、総理が指定する国務大臣、有識者本部員で構成

■事務の委託（第30条）

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

■資料提供等（第31条～第36条）

第Ⅴ章．罰則

■罰則（第37条）

⇒戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

新たな「サイバーセキュリティ戦略」について（全体構成）　平成27年9月4日 閣議決定

1 サイバー空間に係る認識

- サイバー空間は、「無限の価値を産むフロンティア」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「連接融合情報社会（連融情報社会）」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって**「経済社会の活力の向上及び持続的発展」**、**「国民が安全で安心して暮らせる社会の実現」**、**「国際社会の平和・安定及び我が国の安全保障」**に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から先手へ　／　②受動から主導へ　／　③サイバー空間から融合空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出
安全なIoT活用による新産業創出

■セキュリティマインドを持った企業経営の推進
経営層の意識改革、組織内体制の整備

■セキュリティに係るビジネス環境の整備
ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組
事業者の取組促進、普及啓発、サイバー犯罪対策

■重要インフラを守るための取組
防護対象の継続的見直し、情報共有の活性化

■政府機関を守るための取組
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保
警察・自衛隊等のサイバー対処能力強化

■国際社会の平和・安定
国際的な「法の支配」確立、信頼醸成推進

■世界各国との協力・連携
米国・ASEANを始めとする諸国との協力・連携

横断的施策

■研究開発の推進
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■人材の育成・確保
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

「サイバーセキュリティ2016」の概要について

サイバーセキュリティ戦略に基づく２期目の年次計画として、2016年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

- IoT（Internet of Things）に係る大規模な事業に対し、企画・設計段階からセキュリティを確保するために必要な働きかけを引き続き実施【内閣官房】
- IoT推進コンソーシアムを通じてIoTセキュリティガイドラインを策定し、対策を推進【総務省及び経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバーセキュリティ経営ガイドラインの普及【経済産業省】
- 情報開示の推進とインセンティブの検討【内閣官房】
- 金融業界横断的な演習を実施【金融庁】
- ICT分野の情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 企業育成等、セキュリティの成長産業化【経済産業省】
- 著作権法におけるソフトウェア製品等の解析（リバースエンジニアリング）に関する適法性を明確化【文部科学省】
- IoTシステムのセキュリティ認証制度にかかる評価・検討【経済産業省】

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

- IoTに関する攻撃を含む攻撃観測網の強化【総務省】
- 民間の取組主体と協力し、サイバーセキュリティに関する普及啓発を実施【内閣官房】
- 地方公共団体における緊急時対応の支援【総務省】
- 一般財団法人日本サイバー犯罪対策センターとの連携【警察庁】

■重要インフラを守るための取組

- 「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従った検討【内閣官房及び重要インフラ所管省庁等】
- 重要インフラ対策の中核を担う人材育成や技術開発を行う体制を強化【経済産業省】

■政府機関を守るための取組

- 統一基準群の改定及び各府省庁の情報セキュリティポリシーの整備促進【内閣官房】
- 試行的な監査の結果を踏まえた各府省庁に対する監査及び厚生労働省（日本年金機構を含む）に対する施策の評価の実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保

- 対処機関における情報収集・分析機能及び対処能力向上【警察庁、法務省、防衛省、関係各省】
- 社会インフラへのサイバー攻撃に関する任務保証の観点からの知見向上・関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 国際的な情報発信の強化【内閣官房、外務省、関係各省】
- 国際法・規範の議論と法執行の国際連携の両面から、サイバー空間への法の支配の確立に積極的に関与【内閣官房、外務省、関係各省】
- ASEAN等における能力構築を政府一体的に支援【内閣官房、外務省、関係各省】

■世界各国との協力連携

- G7伊勢志摩サミットにおいて立ち上げが決定された「サイバーに関するG7作業部会」を通じ、G7各国との政策協調及び実務的な協力を強化【内閣官房、外務省】
- 二国間協議や多国間協議を通じたASEANや米国等、世界各地域のパートナーとの連携の更なる強化【内閣官房、外務省、関係各省】

横断的施策

■研究開発の推進

- 政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術やサイバーセキュリティ関連情報の大規模集約技術の研究開発を行う【総務省】
- IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会を支える研究開発等の実施【経済産業省】
- 戦略的イノベーション創造プログラム（SIP）の枠組みにより、制御・通信機器の真正性／完全性確認技術を含む研究開発を行う【内閣府】

■人材の育成・確保

- 「新・情報セキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成総合強化方針」に基づく施策を促進【内閣官房】
- 「情報処理安全確保支援士」の創設に係る必要な制度整備を行うとともに、制度の普及を図る【経済産業省】
- サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）等を通じサイバーセキュリティ人材育成を行う【総務省】

推進体制

- 東京オリンピック・パラリンピック競技大会を見据えたリスク評価、対処体制の構築、総合的分析機能の強化、関係機関との協力体制の整備等【内閣官房】

講　演　内　容

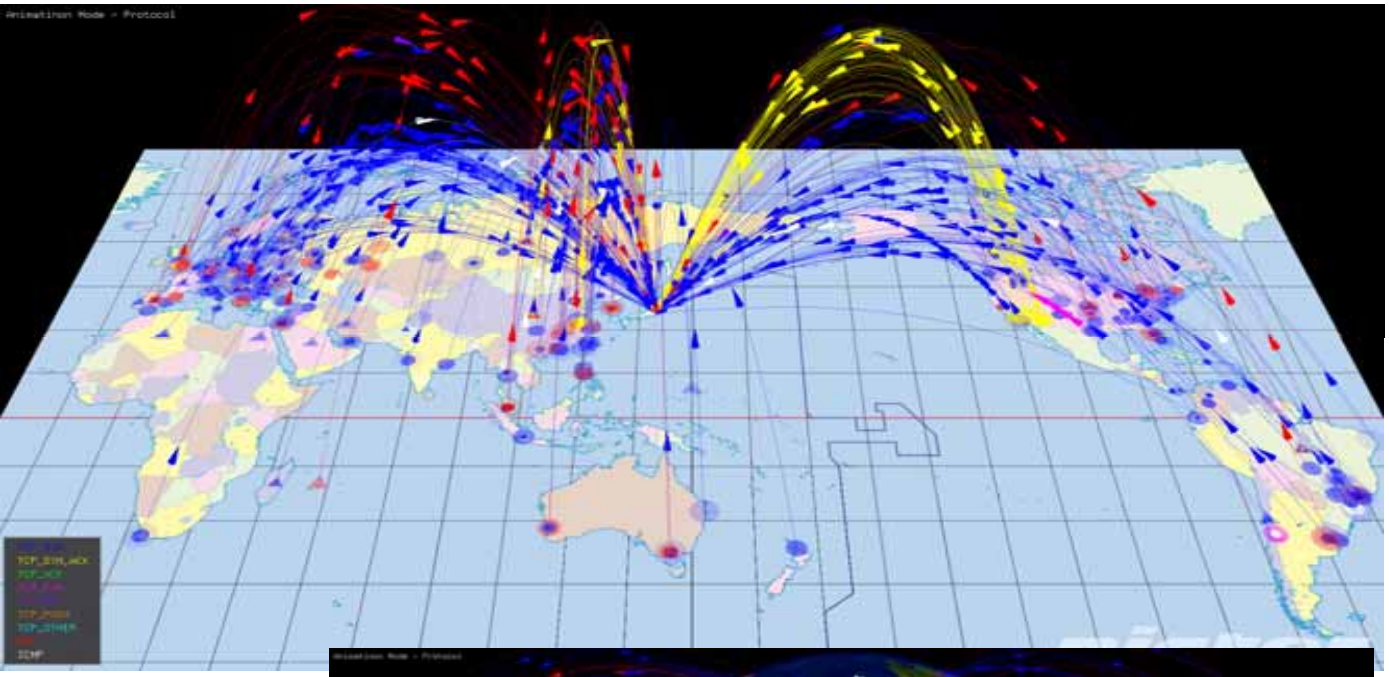
1. ｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威と政府全体の取組

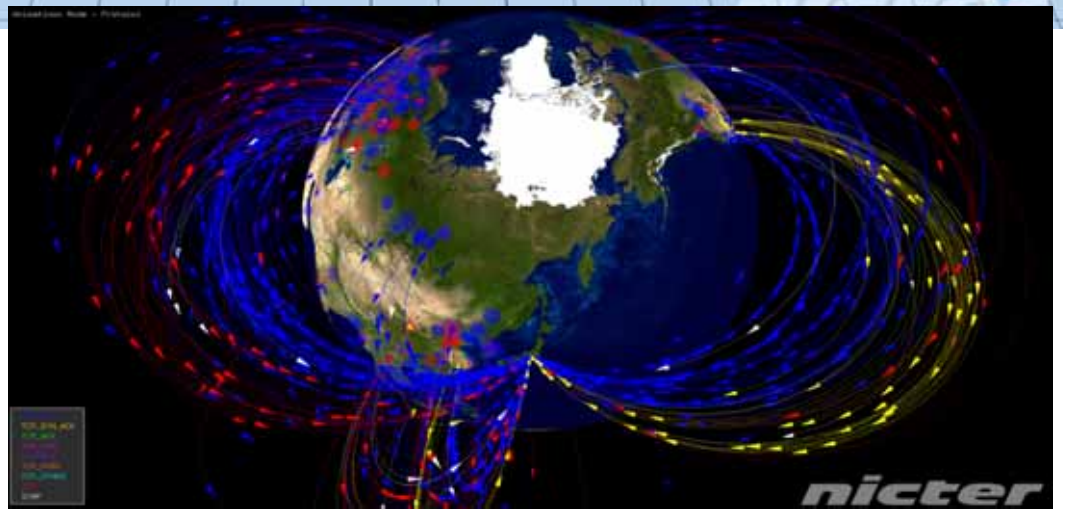
2. IoTにおけるｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威

3. IoTｻｲﾊﾞｰｾｷｭﾘﾃｨ ｱｸｼｮﾝﾌﾟﾛｸﾞﾗﾑ 2017

サイバー攻撃の状況（NICTERによる観測）①

➢ 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。



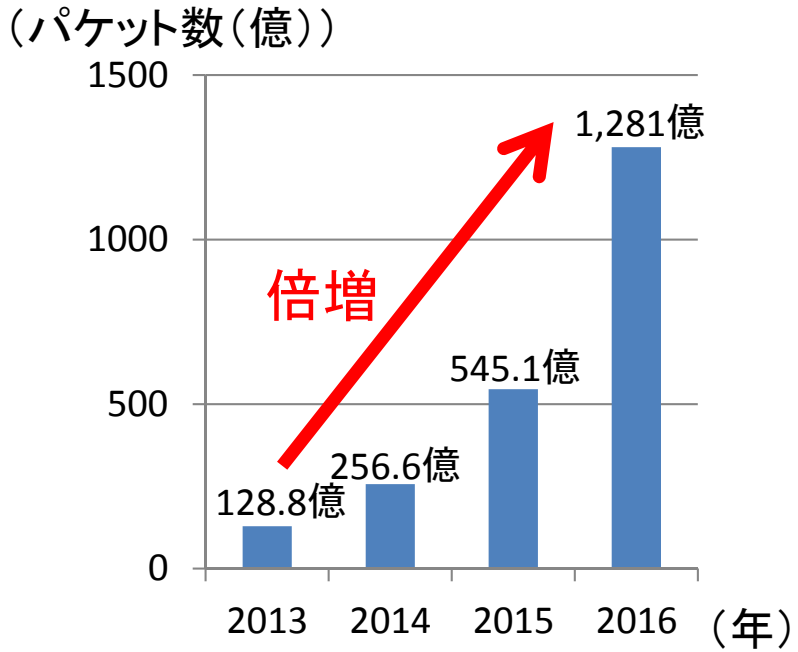


- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・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

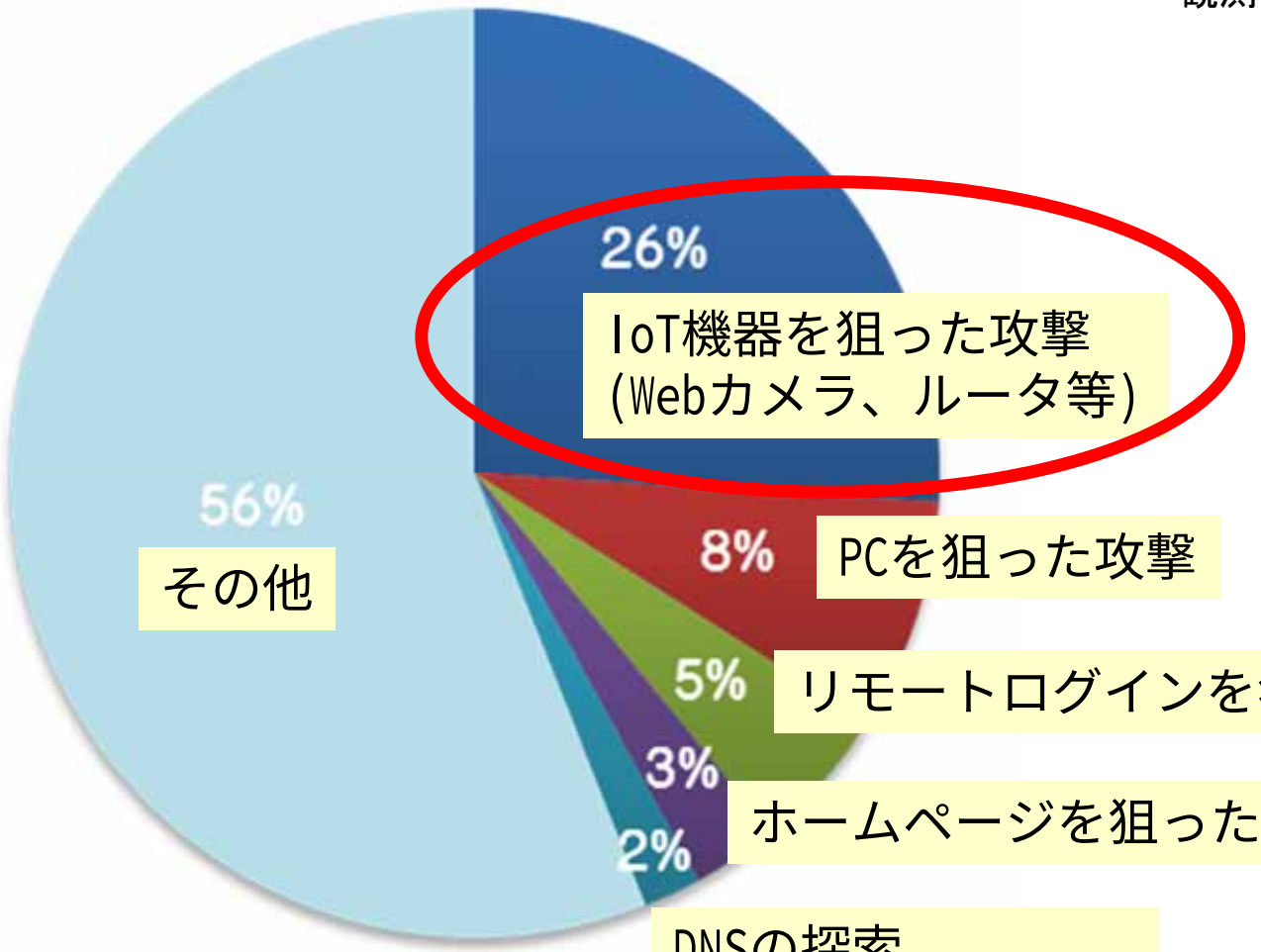
・色：パケットごとにプロトコル等を表現

１年間で観測されたサイバー攻撃に関連する通信の状況



サイバー攻撃の状況（NICTERによる観測）②

観測したサイバー攻撃の内訳（2015年）

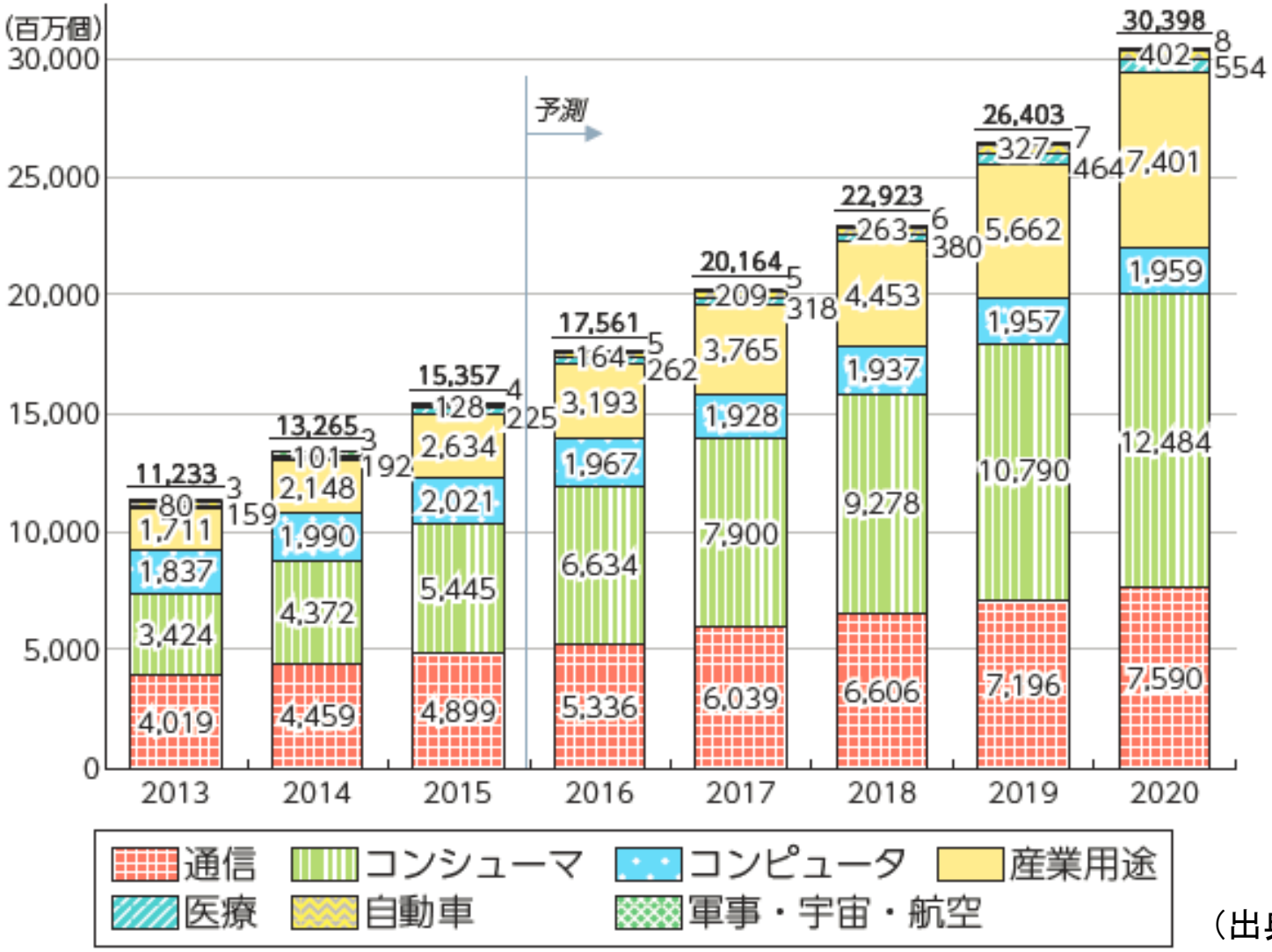


観測された全サイバー攻撃545.1億パケットのうち、

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。

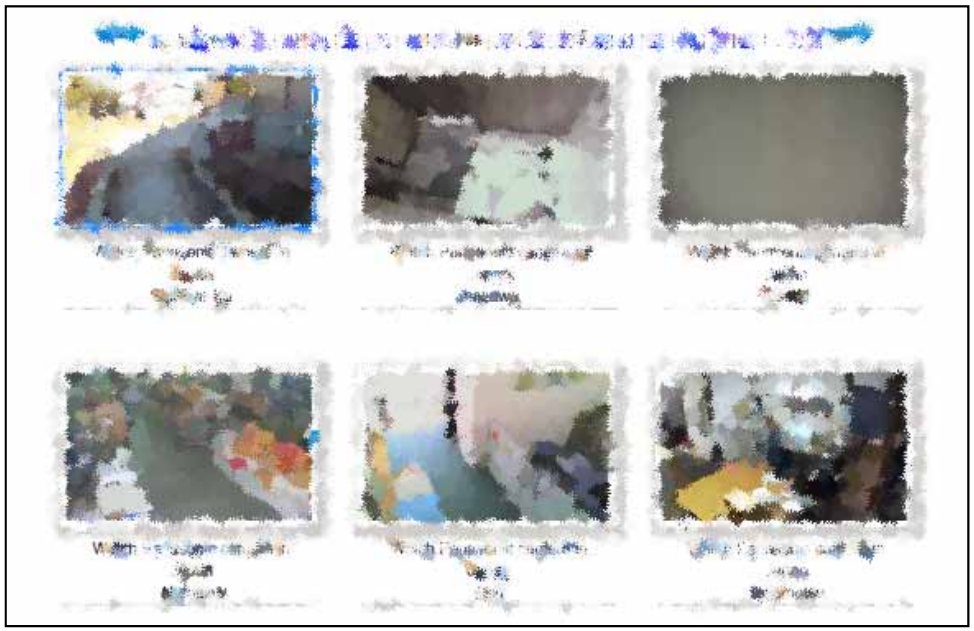


（出典）IHS Technology

IoTにおけるサイバーセキュリティ上の脅威の具体例①

ウェブカメラの事例

ネットに接続されるウェブカメラなどに外部から不正にアクセスされるおそれがあり、映像や音声がインターネット上で誰でも閲覧できる設定となっていることが判明。



複合機の事例

日本の大学等において複合機をインターネットに接続した結果、複合機に保存されたデータがインターネット上で誰でも閲覧できる設定となっていることが判明。

IoTにおけるサイバーセキュリティ上の脅威の具体例②：自動車

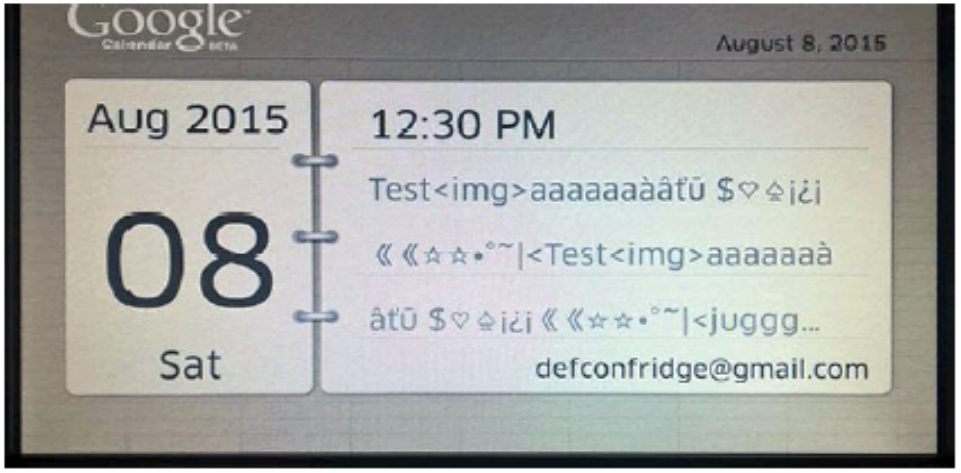
- 2015年のBlack Hat国際会議での発表によると、2014年式の自動車において、インターネットから遠隔操作を可能とする脆弱性を著名なセキュリティ研究者が発見。自宅からインターネット経由で自動車の遠隔操作に成功した。
- 脆弱性への対応として、自動車会社は140万台のリコールを発表した。

出典：Black Hat USA（2015年8月）

IoTにおけるサイバーセキュリティ上の脅威の具体例③：家電（冷蔵庫）

- 2015年、DEFCONのIoTハッキングコンテストで、スマート冷蔵庫の脆弱性が発見。
- SSL証明書の検証が正しく行われておらず、Googleアカウントが窃取可能な状態になっていた。

DEFCONで開催されたIoTハッキングコンテストで、サムスン製のスマートホームアプライアンスシリーズのスマート冷蔵庫で脆弱性が発見される。
SSL証明書を正しく検証していないため、スクリーンに表示するためのGoogleカレンダーのアクセスを盗聴され、Googleのアカウント認証が窃取可能。
ファームウェアアップデートのためのサムスンのサイトへのアクセスは防御が掛っており、攻撃は失敗。



http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

出典：Pen Test Partners（2015年8月）

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セキュリティ対策の必要性

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

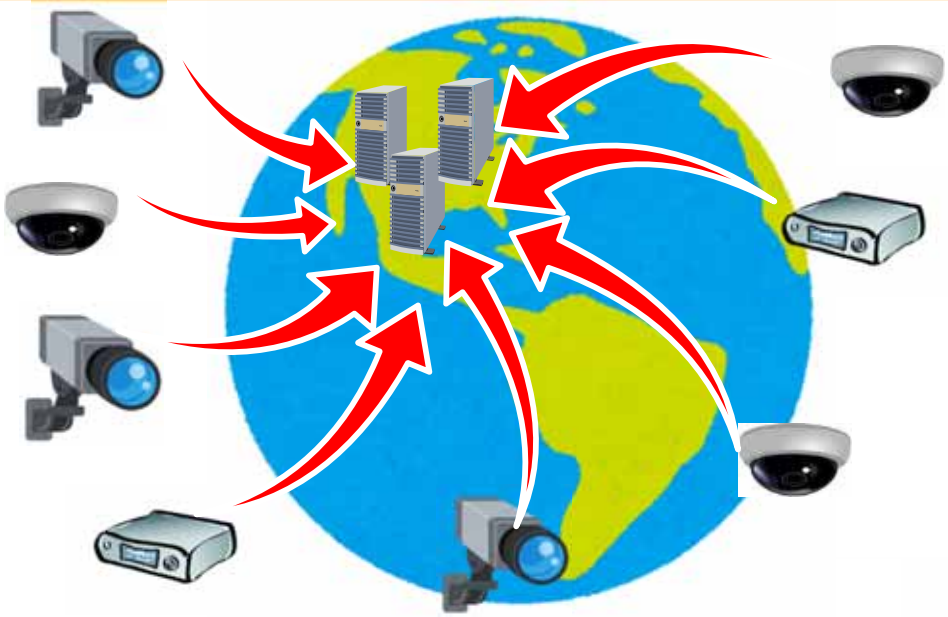
- 2016年1月より、「IoT推進コンソーシアム」において、IoT機器の設計・製造及びネットワークの接続等に関するセキュリティガイドラインを検討。
- 本ガイドラインは、IoTのセキュリティを確保するための「機器メーカ、サービス提供者などを対象にした5つの指針」及び「一般利用者を対象にしたルール」を分野横断的に定めたものであり、「IoT推進コンソーシアム、総務省及び経産省」の3者連名で、7月5日に公表。

	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

講　演　内　容

1. ｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威と政府全体の取組

2. IoTにおけるｻｲﾊﾞｰｾｷｭﾘﾃｨ上の脅威

3. IoTｻｲﾊﾞｰｾｷｭﾘﾃｨ ｱｸｼｮﾝﾌﾟﾛｸﾞﾗﾑ 2017

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

サイバーセキュリティタスクフォースの開催

趣旨

○ 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/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、サイバーセキュリティタスクフォースを開催する。

○ 本タスクフォースは、政策統括官、情報通信国際戦略局長共催の公開の会合として立ち上げる。

体制

○ サイバーセキュリティタスクフォースは座長1名、副座長1名、委員10名で構成

○ 事務局は、情報流通行政局 情報流通振興課 情報セキュリティ対策室及び情報通信国際戦略局 情報通信政策課が行う。

議題

○ IoT/AI時代のサイバーセキュリティを支える基盤・制度（IoTなど新たな脅威への対応方策等）

○ IoT/AI時代のサイバーセキュリティを担う人材育成（産学官連携体制の構築等）

○ IoT/AI時代のサイバーセキュリティ確保に向けた国際連携（情報共有、セキュリティ技術の海外展開等）

○ その他

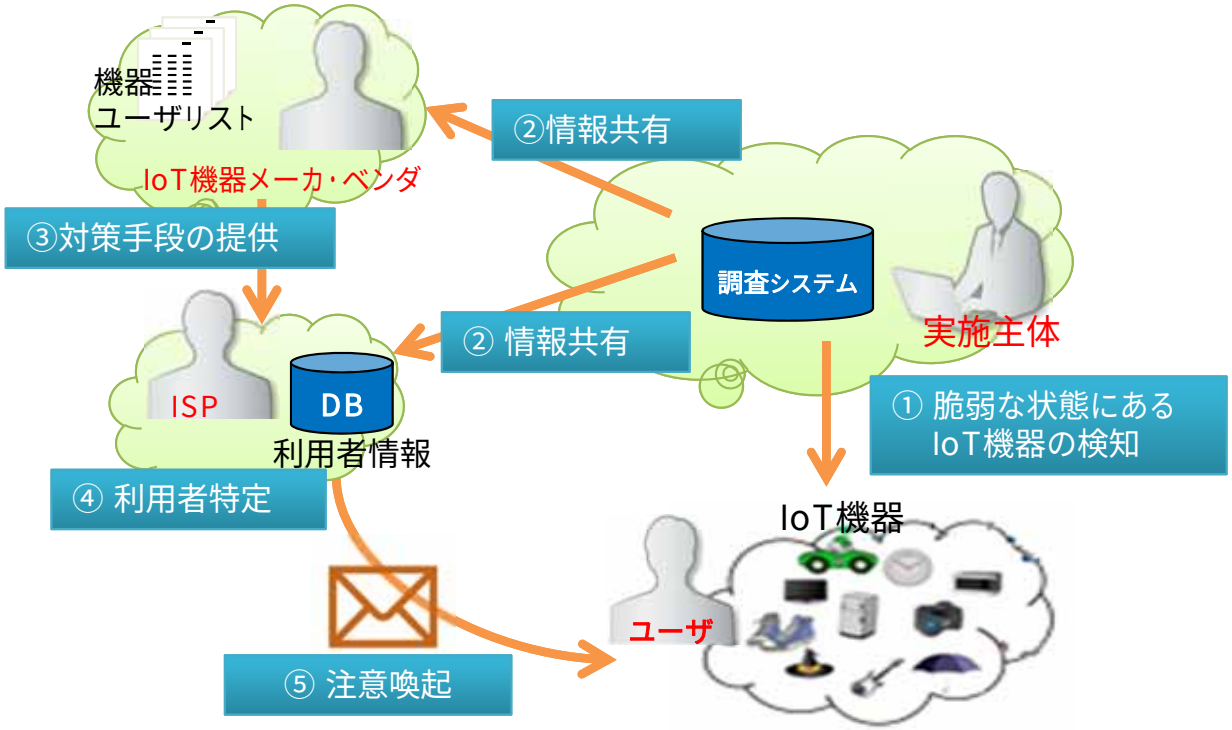
スケジュール

○ 2017年1月30日（月）に第一回タスクフォースを開催。（以降、随時開催予定）

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。

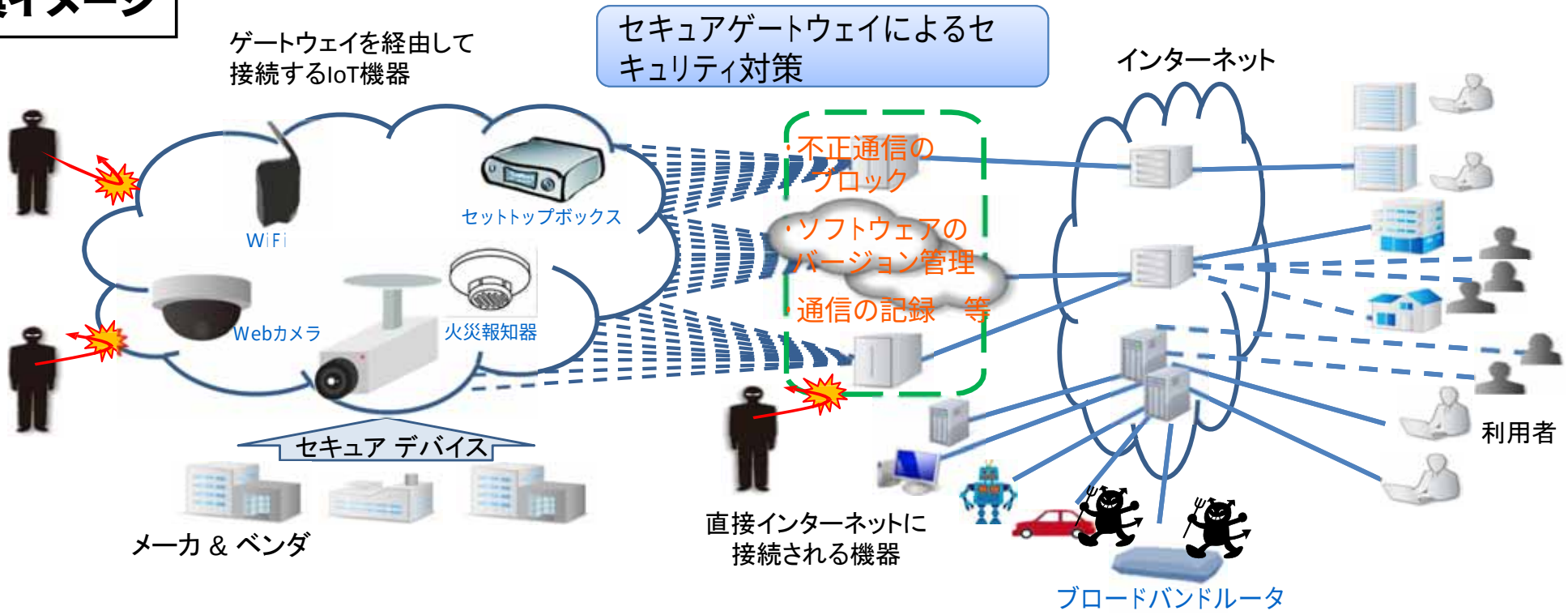
④ 利用者特定
　ISP事業者が当該機器の利用者を特定。

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。

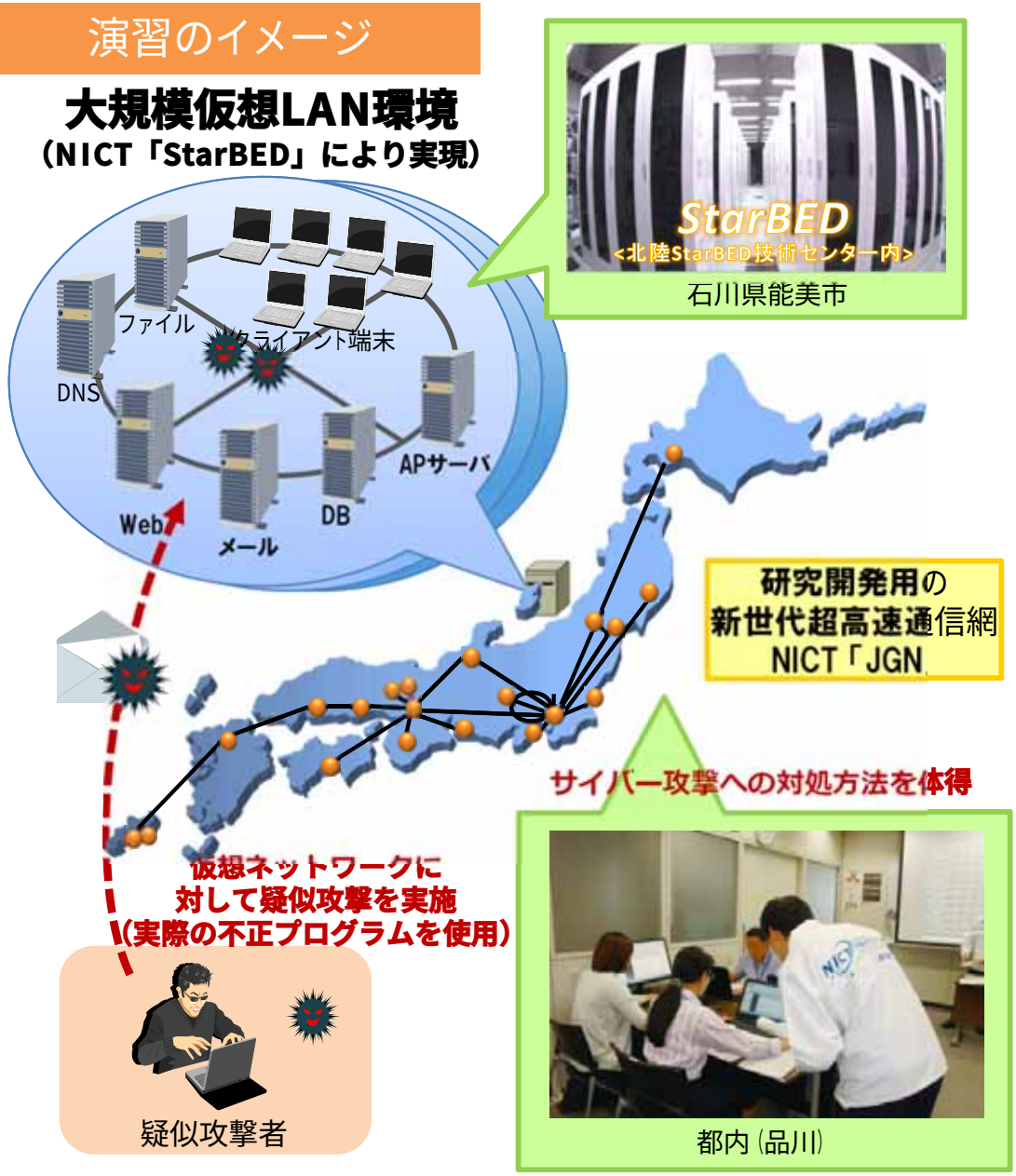
事業イメージ



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

- 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



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年東京ｵﾘﾝﾋﾟｯｸ・ﾊﾟﾗﾘﾝﾋﾟ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

総務大臣表彰制度の創設

1. 設立趣旨

○ 地方自治体、民間企業、各種団体等におけるネットワーク環境等のサイバーセキュリティの向上を促進するため、これらの組織の現場で優れた功績があり、今後更なる活躍が期待される個人または団体（チーム）を表彰し、現場レベルでのサイバーセキュリティの向上、ひいては社会全体のセキュリティ意識の向上を図る。

2. 表彰対象

○ 地方自治体、民間企業、各種団体等の現場において、ネットワーク環境等のサイバーセキュリティ向上の観点から、特に顕著な功績があり、今後サイバーセキュリティ分野で更なる活躍が期待される個人または団体（チーム）に対し、「サイバーセキュリティに関する総務大臣奨励賞」として表彰する。

3. スキーム

○ 自薦・他薦による公募（1月18日から2月28日まで実施）、選考委員からの推薦に基づき同選考委員会で審議（3月実施予定）を行った上で、総務省が選定。

【参考】 選考委員

選考委員長： 村井 純 慶應義塾大学 環境情報学部長・教授

選考委員： ICT-ISAC、日本インターネットプロバイダー協会、テレコムサービス協会、情報通信研究機構、地方公共団体情報システム機構、日本シーサート協議会、情報処理推進機構（IPA）、JPCERT、日本ネットワークセキュリティ協会、情報処理学会、電子情報通信学会から代表者（各1名）

4. 表彰方法

○ 初年（2017年）は、毎年6月に実施している「電波の日・情報通信月間」記念中央式典で表彰。2018年以降は、サイバーセキュリティ月間におけるイベント等の場において表彰する。

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～

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

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）

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）

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～）

ご静聴ありがとうございました。