資料10

サイバーセキュリティに関する総務省の取組

総務省政策統括官
（情報通信担当）
南　俊行

平成28年3月31日

本年度の成長戦略を踏まえた取組

「日本再興戦略」改訂2015（平成27年6月30日閣議決定）

第二　３つのアクションプラン
一．日本産業再興プラン
４．世界最高水準の IT 社会の実現
（３）新たに講ずべき具体的施策
ｉ）国民・社会を守るサイバーセキュリティ
④ サイバーセキュリティの確保に向けた基盤強化（技術力の強化・産業育成、人材育成）
ア）技術力の強化・産業育成
（略）今後の成長産業と見込まれるIoT分野に係るセキュリティの確保は、我が国経済の成長の核となる。このため、国が推進する**IoTシステムに係る事業について、本年度末を目途に、総合的なセキュリティガイドラインを策定する**。
イ）人材育成
（略）**2020年東京オリンピック・パラリンピック競技大会の開催も見据え、高度な実践的人材の育成を強化する**。このため、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、**実践的なサイバー演習環境をクラウド環境で整備する**。

① IoTセキュリティガイドラインの策定

法人会員1800社以上が参加するIoT推進体「IoT推進コンソーシアム」（会長：村井純慶大教授）の下、IoTセキュリティWGが設立され、総務省及び経済産業省が共同事務局となり、必要なガイドラインを策定中。

② セキュリティ人材の育成強化

国の行政機関等を対象にした実践的なサイバー防御演習（CYDER（サイダー））について、演習の更なる強化を図る観点から、NICTに演習を担わせること等を内容とする法案を本国会に提出。

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、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。）
■ 技術開発、利活用、政策課題の解決に向けた提言等を実施。

※法人会員1820社加盟（平成28年3月時点）

総　会
■ 会長
■ 副会長
運営委員会

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　執行役員兼ＣＥＯ

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機器のネット接続に関するガイドラインの検討等

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

※本年1月21日に設置

機器製造・管理SWG
議題１
「IoT機器等の設計・製造・構成・管理に求められるセキュリティガイドライン」を検討

ネットワークSWG
議題２
「IoT機器の通信ネットワークへの接続に係るセキュリティガイドライン」を検討

総務省と経済産業省が共同で事務局となり、機器の設計・製造及びネットワークの接続等に関する統合セキュリティガイドラインを本年５月末までに策定予定。

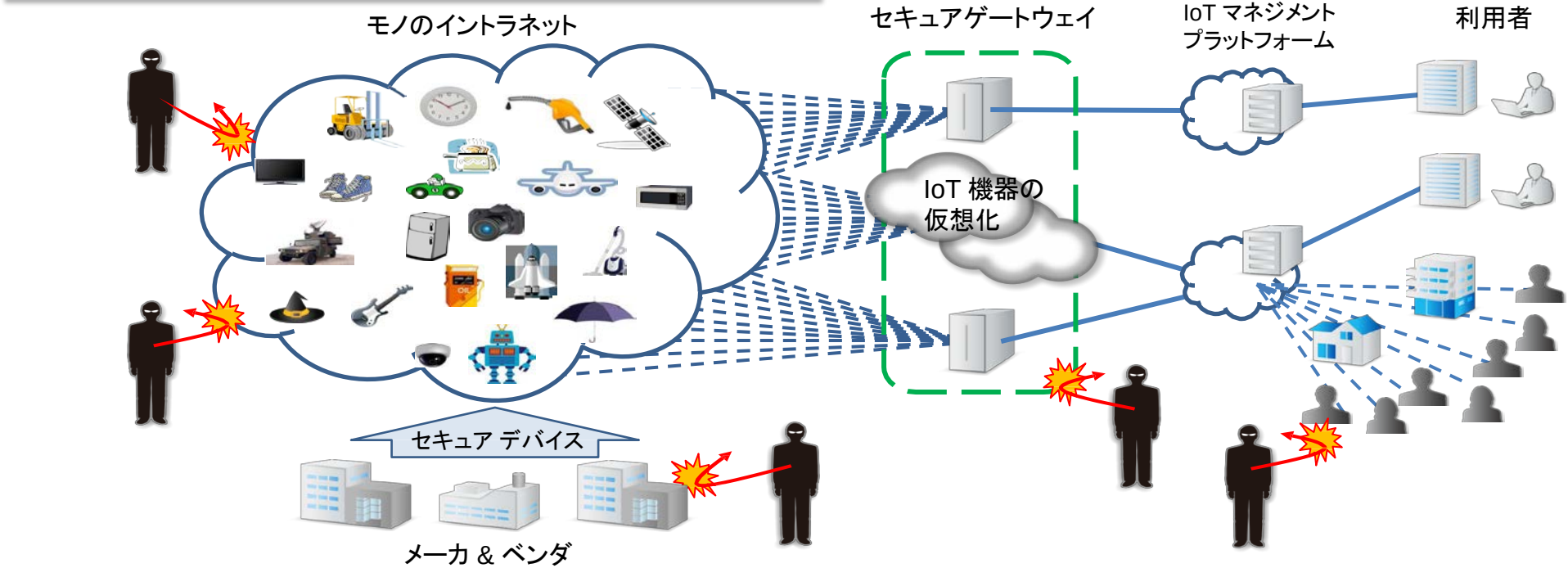
IoTセキュリティガイドラインのイメージ

- IoT時代には、通信ネットワークに接続される機器数の急速な増加が見込まれている（IHS社は、全世界のIoT機器の数は、2013年に約158億個であるが、2020年には約530億個となると予測）。
- インターネットに接続されるIoT機器の中には、機器の物理的な制約等の理由により、十分にセキュリティを確保できないまま、ネットワークに接続されるケースも想定される。
- こうした状況のなか、IoT時代においても、通信ネットワークのセキュリティを確保するため、機器の種類、機能に応じたネットワーク接続の在り方についてガイドラインを本年5月末までに取り纏める予定。

（アウトプットイメージ）

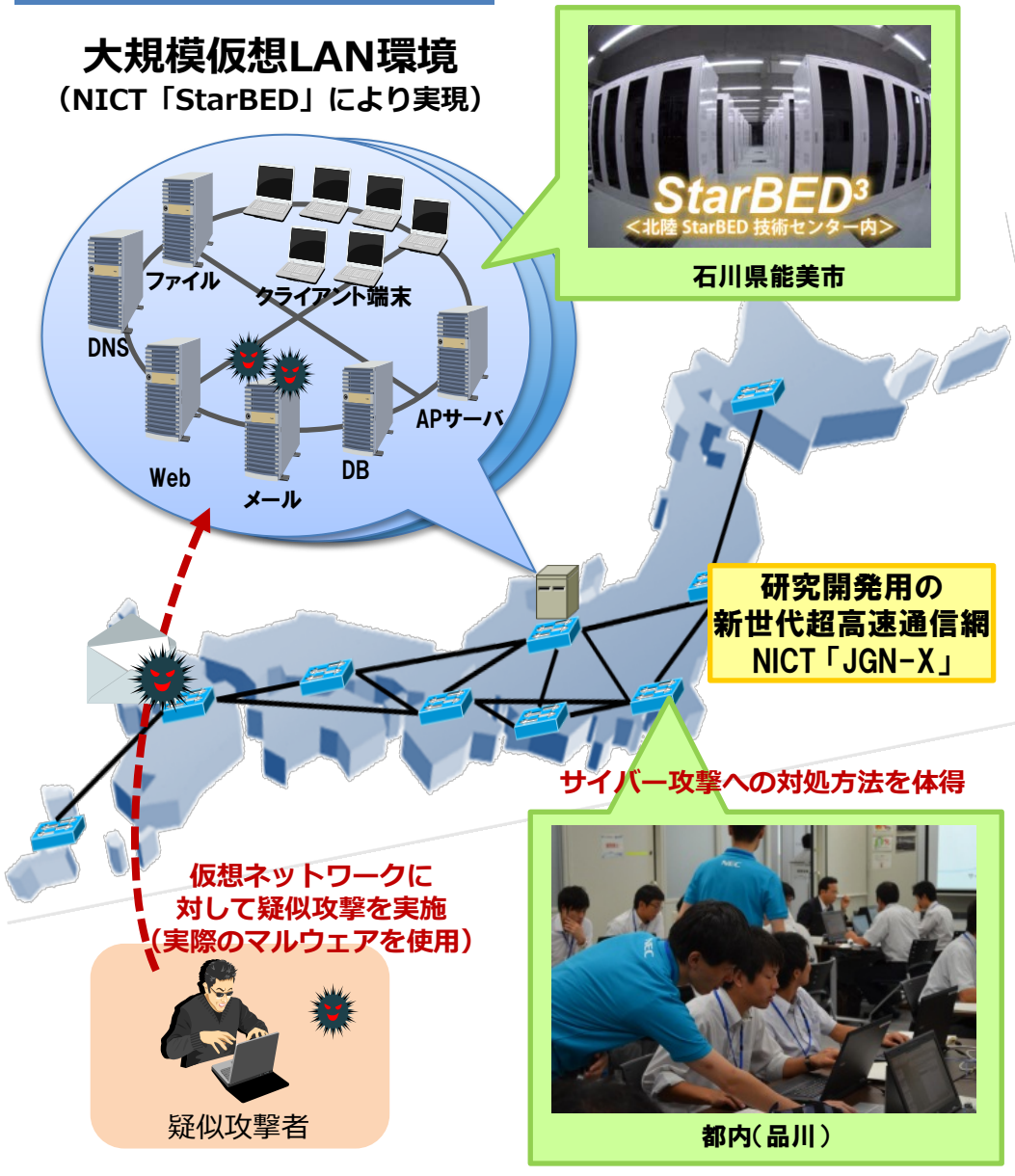
- ✓ 一定の機能を持つ機器については、脆弱性を修正するソフトウェアの自動更新を推奨
- ✓ セキュリティを十分確保できない機器については、セキュアゲートウェイを通してインターネットに接続等

IoT機器のネットワークへの接続例 （将来イメージ）



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

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、ログ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台の高性能サーバのクラウド環境による数千人規模の仮想ネットワーク**（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**（平成27年度は、年金機構への標的型攻撃を参考にしたシナリオ）**を用意**

平成27年度の実績

- **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**

→ **平成28年度は地方自治体等に対象を拡大し、500組織、1500人を目標に実施予定**

平成28年度から、技術的知見を有するNICTを実施主体とすることにより、演習の質の向上や継続的・安定的な運用を実現するための法案を本国会に提出

（注：現在は総務省が民間企業に委託して実施）

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システムの模擬環境を構築し、大会の運営に係るシステムや放送など、複数のシステムに係る攻撃・防御双方の実践的な演習を行うことにより、大会開催時に想定される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図る。

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

NICTのクラウド環境と、その演習で得られた知見を活用

具体的内容

- 大規模クラウド環境を用いて、公式サイト、大会運営のためのアドミニシステムや、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。
- さらに、当該模擬システムを活用して、大学等の教育機関とも連携し、若手セキュリティ人材の育成も行う。