「IoTセキュリティ総合対策」とその進捗状況及び今後の取組みについて

総務省　サイバーセキュリティ統括官室 参事官補佐　相川（あいかわ）　航（わたる）

1. はじめに

近年、ビッグデータ、AI（人工知能）、IoT（Internet of Things：モノのインターネット）等の新たな情報通信技術が様々なパラダイムシフトを生み出している。その中でも、IoTシステムは、これまで個別分野ごとに進められてきたICT化を越えて、異なる分野のデータ連携を実現する結果、現実空間とサイバー空間を緊密に連携させたデータの生成・収集・活用等を通じて、社会課題の解決をもたらす社会基盤として機能していくことが期待されている。

このように社会基盤としてのIoTシステムの発展に大きな期待が寄せられる一方で、IoT機器については、ウィルス駆除ソフトのインストールなどの対策が困難、利用者等においてインターネットにつながっているという意識が低いなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。

例えば米国においては、2016年10月、マルウェア「Mirai」に感染した10万台を超えるIoT機器が踏み台となり、Dyn社のDNSサーバに対する大規模なDDoS攻撃が発生し、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障害が発生した。

こうしたIoT機器に関連するサイバー攻撃の増加は、国立研究開発法人情報通信研究機構（NICT）が運用しているサイバー攻撃観測網（NICTER）でも観測されている。NICTERで観測されたサイバー攻撃に関係するパケット数は、545億パケット（2015年）から1504億パケット（2017年）と、2年間で2.8倍に増加し、また、2017年に観測されたパケットの半数以上はIoT機器を狙ったものであるという結果が示されている。

2. 政府及び総務省における検討

IoT分野のセキュリティ対策の重要性の高まりを受け、総務省では、2017年より、セキュリティ分野の有識者で構成される「サイバーセキュリティタスクフォース」（座長：安田 浩 東京電機大学学長）を開催し、2017年10月に、IoTに関するセキュリティ対策の総合的な推進に向けて取り組むべき課題を整理した「IoTセキュリティ総合対策」を公表した。また、2018年7月27日にはその進捗状況と今後の取組みについて整理した「IoTセキュリティ総合対策プログレスレポート2018」を作成・公表した。折しも、同日、政府全体の新たな「サイバーセキュリティ戦略」が閣議決定されたが、同戦略にも「IoTセキュリティ総合対策」における様々な取組みが位置付けられている。以下では「IoTセキュリティ総合対策」の概要と、具体的な施策の進捗状況及び今後の取組みについて、主要なものを中心に紹介したい。

3.「IoTセキュリティ総合対策」の進捗状況と今後の取組み

「IoTセキュリティ総合対策」では、(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) 国際連携の推進の5つの観点から、今後取り組むべき具体的な施策をまとめている（**図1**）。

(1) 脆弱性対策に係る体制の整備

IoT機器の脆弱性については、機器の①設計・製造段階、②販売段階、③設置段階、④運用・保守段階、⑤利用段階のライフサイクル全体を見通した対策が必要であることから、各段階において適切な対応を行うことが必要である。

例えば、①の設計・製造段階においては、セキュリティ・バイ・デザインの考え方を踏まえて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つつ、意識啓発・支援を実施する必要がある。本件は、2017年12月よりIoT推進コンソーシアムのIoTセキュリティ WGにおいて検討が開始され、2018年7月に「IoT機器のセキュリティ対策に関する検討の方向性」がまとめられたところであり、セキュアなIoT機器の認証について、求めるセキュリティ要件、認証手段、基準・規格に適合している旨の表示の仕組み等の論点の具体化を図ることとされた。

加えて、情報通信審議会IPネットワーク設備委員会において、情報通信ネットワークの安全・信頼性を確保するため、DDoS攻撃の原因となるIoT機器がマルウェアに大量感染する事態を防止すること等を目的として、IoT機器を含む端末設備の技術基準に最低限のセキュリティ対策を追加するこ

■図1.　IoTセキュリティ総合対策

とについて、2018年6月に第1次報告案が取りまとめられた。今後は同報告案の意見募集の結果を踏まえ、IoT機器等の端末設備の最低限のセキュリティ対策（アクセス制御機能、アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能、ファームウェアの更新機能等）について取りまとめた上、関係省令等の改正など所要の手続きを進めていく。

一方で、上記の①～⑤のようなライフサイクル全体を見通した対策に加え、既に設置されているIoT機器や製造・販売された新規のIoT機器についても新たな脆弱性が発見され、こうした脆弱性を突いたサイバー攻撃が行われる可能性がある。総務省では、2017年9月より、一般社団法人ICT-ISAC、国立大学法人横浜国立大学等と連携し、国民生活や社会経済活動に直接影響を与える可能性がある重要IoT機器と、家電製品などのサイバー攻撃の踏み台となってネットワークに悪影響を及ぼすおそれのある機器の双方について脆弱性調査を行い、2018年7月に結果を公表した。

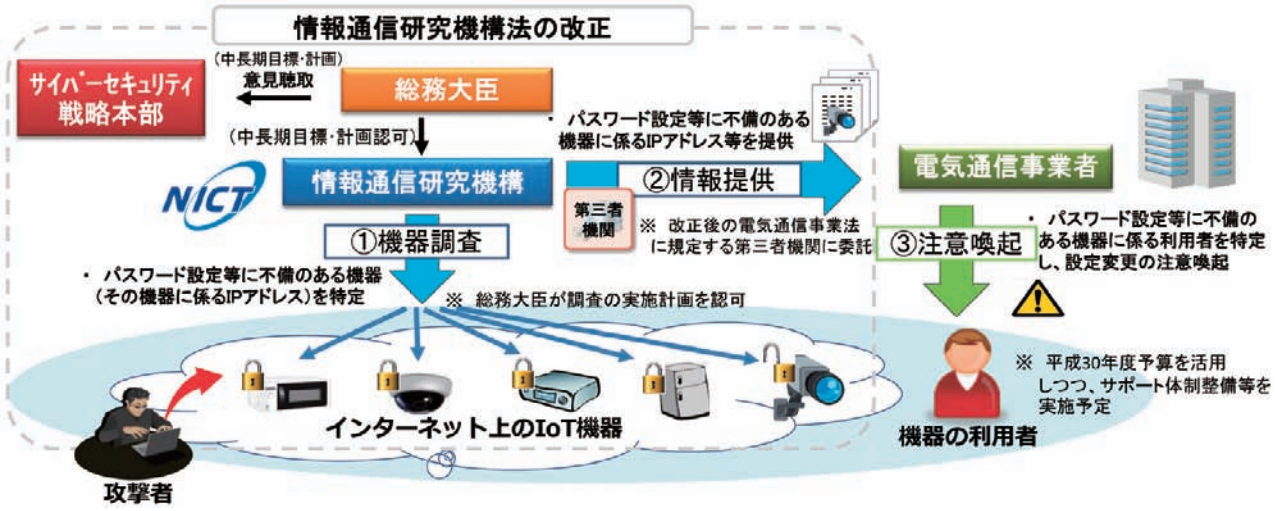
IoT機器の脆弱性調査については、5年間の時限措置でNICTの業務にパスワード設定等に不備のあるIoT機器の調査を行う業務を追加すること等を盛り込んだ「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」を2018年3月に国会へ提出し、同改正法が同年5月に成立・公布された。本法においてNICTはパスワード設定等に不備のあるIoT機器の調査を行い、当該機器のIPアドレス等の情報を通信事業者に提供し、当該事業者はこの情報をもとに利用者を特定し、パスワード設定の変更を求める注意喚起を発出することとしている（図2）。2018年度内の当該業務の開始を目指し、今後は所要の手続きを進めていく。

（2）研究開発の推進

サイバー空間における攻撃の態様は常に変化しているため、政府が支援する産学官連携による研究開発の成果を即座に反映した、最新のサイバーセキュリティ対策を実施していくことが有効となる。

これまでNICTでは、サイバーセキュリティ分野の基礎的・基盤的な研究開発を実施してきており、2017年5月には、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、その攻撃活動を長期観測することで、従来では収集が困難であった攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能にするサイバー攻撃誘引基盤（STARDUST）を開発した。今後は、サイバー攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の実証を行う研究開発環境の整備を加速する。

その他の取組みとして、膨大なIoT機器に対する広域的



■図2. 国立研究開発法人情報通信研究機構法の一部改正について

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する。また、安全性を備えた衛星通信を実現するための量子暗号技術の研究開発や、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等も推進する。

(3) 民間企業等におけるセキュリティ対策の促進

また、民間企業等におけるセキュリティ対策を促進するに当たっては、サイバーセキュリティを経営上の重要課題として取り組むことが有利となる仕組みを構築する必要がある。

まず、「平成30年度税制改正の大綱」（2017年12月22日閣議決定）において、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・利活用を通じて生産性を向上させる取組みについて、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税制優遇を措置する情報連携投資等の促進に係る税制（コネクテッド・インダストリーズ税制）が創設された。

また、公衆無線LANについては、東京2020オリンピック・パラリンピック競技大会に向けて普及が進んでいる一方、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、2017年11月、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「公衆無線LANセキュリティ分科会」を「サイバーセキュリティタスクフォース」の下に設置し、検討を行った。今後は、利用者・提供者の意識向上に向けて、Wi-Fi利用者・提供者向けマニュアル（手引き）の改定や、オンライン教育等の教育コンテンツを活用した周知・啓発、「公衆無線LAN 版安全・安心マーク」に関する周知活動の継続的な実施等に取り組むとともに、公衆無線LANの優良事例について、調査・公表し、優良事例の普及促進を図る。

さらに、民間企業のサイバーセキュリティ対策の取組みを促進するためには、民間企業におけるセキュリティ対策の情報開示を推進し、民間企業の経営層が自社及び他社のセキュリティ対策の現状を認識した上で、さらに必要な具体的な対策を検討し、導入するような「セキュリティ対策の好循環」が起こる環境が必要である。このため、2017年12月、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「情報開示分科会」をサイバーセキュリティタスクフォースの下に設置した。同分科会においては、セキュリティ対策の情報開示を「社内の情報共有（第一者開示）」、「契約者間等の情報開示（第二者開示）」、「社会に対する情報開示（第三者開示）」の3つの側面に分けて議論を行った。

その中で、特に、契約者間等の情報開示（第二者開示）については、契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体またはグループ全体における情報共有体制の構築の促進が必要であるとされた。また、社会に対する情報開示（第三者開示）については、事業者の規模や取組状況に応じて、セキュリティ対策の自己宣言制度や主要5項目の開示、「情報セキュリティ報告書」の作成など、段階的に対策を講じていくことが望ましいこ

とを踏まえ、今後「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表することとしている。

（4）人材育成の強化

政府全体においても、サイバーセキュリティ人材の育成は重要な課題とされており、総務省では、サイバーセキュリティ人材の育成について、2017年4月より、NICTの「ナショナルサイバートレーニングセンター」において、①国の行政機関、地方公共団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（CYDER）、②東京2020オリンピック・パラリンピック競技大会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若手セキュリティイノベーターの育成（SecHack365）の取組みを積極的に推進している。

CYDERについて、2017年度は、全国47都道府県で計3,009名（国の行政機関316名、地方公共団体1,889名、重要インフラ事業者553名、その他251名）が受講した。また、演習の運営コストの削減と効果的な演習プログラムの提供を行うためのサイバー演習自動化システム「CYDERANGE」（サイダーレンジ）を開発した。引き続き、演習プログラム・教育コンテンツの開発を継続的に行いつつ、受講者のニーズに応じた演習を実施する。

サイバーコロッセオについて、2017年度は、組織委員会のセキュリティ担当者等を対象に実施し、計74名が受講した。今後、更なる演習規模・内容の拡充を図り、より実践的なサイバー演習を実施し、最終的に約220人のセキュリティ担当者等を育成する予定である。

SecHack365について、2017年度は、39名が1年間のプログラムを修了した。SecHack365は、25歳以下のICT人材を対象に、セキュリティイノベーターの育成に取り組むものであり、引き続き、NICTの有する遠隔開発環境「NONSTOP」を活用した遠隔開発実習、集合イベントにおける座学講座やハッカソン等のプログラム内容の充実を図りつつ、セキュリティイノベーターの育成に取り組む予定である。

（5）国際連携の推進

サイバー空間は国境を越えて利用される領域であることから、サイバーセキュリティの確保のためには、国際連携の推進が不可欠であり、これまで述べた施策を含め、政府レベルや民間レベルでの国際的な連携を進めていく必要がある。また、様々なチャネルを通じて、自由、公正かつ安全なサイバー空間を実現するため、積極的に議論に参画していくことが重要である。

まず、ASEAN各国との連携については、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、サイバーセキュリティの脅威をめぐる状況や対策に関する情報交換等を推進する。2017年12月の「第12回日ASEAN情報通信大臣会合」において、「日ASEANサイバーセキュリティ能力構築センター」をタイに開設することが合意され、ASEANとのサイバーセキュリティ分野での人材育成協力を強化している。本センターはJAIF（日・ASEAN統合基金）の資金供与により実現し、2018年9月に開所し、本格的な稼働を開始した。

また、国際的なISAC（Information Sharing and Analysis Center）間の連携の推進については、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、脅威情報を共有し、サイバーセキュリティ対策に活用することを促す。さらに、ITU-T及びISO/IECにおいて、IoTのセキュリティに係るガイドラインの国際標準化活動に積極的に貢献する。

なお、2019年にはG20が我が国で開催されることを見据え、我が国はサイバーセキュリティ分野の国際協調や自由、公正かつ安全なサイバー空間を実現するための議論において主導的な役割を果たすことが求められる。

4. おわりに

本稿では紙面の都合上、「IoTセキュリティ総合対策」の進捗状況や今後の取組みについて、主要な内容に限定して紹介させていただいた。その他の部分も含めて関心がある方は、以下のHPに掲載されている「IoTセキュリティ総合対策」及び「IoTセキュリティ総合対策プログレスレポート2018」について御覧いただければ幸甚である。

▼「IoTセキュリティ総合対策」の公表（2017年10月3日）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html

▼「IoTセキュリティ総合対策 プログレスレポート2018」の公表（2018年7月27日）
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001.html