第5節 サイバーセキュリティ対策の推進

1 サイバーセキュリティ対策に関する取組方針の検討

1 政府の取組

世界的規模で深刻化するサイバーセキュリティ上の脅威の増大を背景として、我が国におけるサイバーセキュリティ政策の基本理念を定め、国や地方公共団体をはじめとする関係主体の責務等を明確化するとともに、サイバーセキュリティ政策に係る政府の司令塔機能を強化し、経済社会の発展や国民の安全・安心な暮らしを実現するため、平成26年11月、第187回国会（臨時会）において「サイバーセキュリティ基本法」が成立した。

平成27年1月、同法に基づき、サイバーセキュリティ政策に係る政府の司令塔として、内閣の下にサイバーセキュリティ戦略本部が新たに設置され、それまでIT総合戦略本部の下で情報セキュリティ政策会議が担っていた、官民における統一的・横断的な情報セキュリティ対策の推進機能は、より強力な権限が付与された形で、法律上の根拠を持つサイバーセキュリティ戦略本部が担うこととなった。

同本部における検討を経て、同年9月に新たな「サイバーセキュリティ戦略」[*1]が閣議決定された。同戦略では、監視対象の拡大等、「政府機関全体としてのサイバーセキュリティを強化するため、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化」や、「実践的な訓練・演習の実施等の取組」等を推進することが掲げられている。

平成29年7月、最新の脅威動向等を踏まえて、現行のサイバーセキュリティ戦略のレビューが行われ、「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　－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）として取りまとめられた。その中では、今後1年以内を目処に加速・強化すべき施策として、「ボット撲滅の推進」、「情報共有・連携ネットワーク（仮称）の構築・運用」、「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態勢の整備」等が掲げられた。

2 総務省の取組（サイバーセキュリティタスクフォース）

総務省においては、平成29年1月から、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、同年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」を取りまとめ、公表した。同総合対策では、「(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推進」、「(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。

2 サイバーセキュリティ対策の強化

1 組織に対する取組

昨今、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事業者等を狙ったサイバー攻撃はますます巧妙化する傾向にあり、機密情報の漏えい等の被害は甚大なものとなっている。組織を標的としたサイバー攻撃への対策については、攻撃手法の解析が困難であることや攻撃を受けた後の対応が確立されていないこと、情報システム担当者等の対応能力が不足していることが指摘されているなど、十分とは言えない状況である。このような状況を踏まえ、総務省では平成25年度より、サイバー攻撃への対応能力の向上を図り、組織の実際のネットワークを模した大規模仮想LAN環境下で実機を操作しながら、サイバー攻撃によるインシデント発生時の一連の対処方法を体験する実践的サイバー防御演習「CYDER」（CYber Defense Exercise with Recurrence）を実施している。

平成28年度には、サイバー防御演習の質の向上や継続的・安定的な運用を実現するため、演習の実施主体を国

＊1　サイバーセキュリティ戦略：http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf

立研究開発法人情報通信研究機構（NICT）に変更した。全国11都市で開催した演習には、1,539名の受講者が参加した。

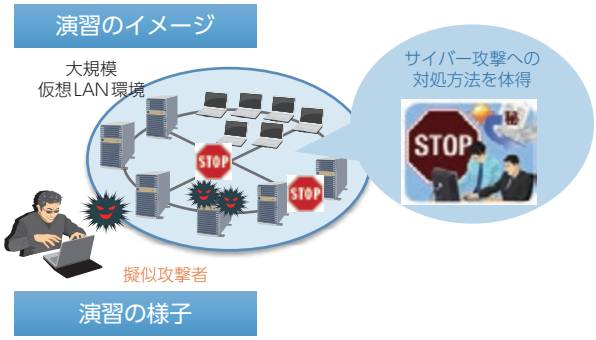
平成29年度からは、平成29年4月にNICTに組織した「ナショナルサイバートレーニングセンター」において、セキュリティ人材育成の取組（CYDER、サイバーコロッセオ、SecHack365）を実施している。

CYDERは、平成29年度、全国47都道府県で全100回の演習を実施し、3,009名が受講した。平成30年度からは、重要インフラ事業者向けのコースを新設し、金融、交通インフラ、医療、教育研究機関等向けにそれぞれ最適化したシナリオを用いて演習を行うなど、さらなる内容の充実を図ることとしている。（図表6-5-2-1）。

サイバーコロッセオは、東京2020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担当者の育成を図るための実践的サイバー演習である。大会本番を忠実に再現した仮想のネットワーク環境上で、実機を操作しながら、本格的な攻防戦等を繰り返し実施するものであり、平成29年度は74名が受講した。平成30年度以降も、さらなる内容の充実を図るとともに、参加人数についても段階的に規模を拡大し、最終的には約220人のセキュリティ担当者等を育成する予定である。

SecHack365は、未来のセキュリティイノベーターの創出に向けて、25歳以下のICT人材を対象に、NICTの持つ実際のサイバー攻撃関連データを活用し、第一線で活躍する研究者・技術者が、セキュリティ技術の研究・開発を1年かけて継続的かつ本格的に指導するプログラムである。平成29年度は39名が1年間のプログラムを修了した。平成30年度以降も、さらなる内容の充実を図ることとしている。

図表6-5-2-1　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）



CYDER 演習風景

2 個人に対する取組

ICTが国民の社会経済活動のあらゆる領域に普及・浸透していることに伴い、これらのサイバー空間を標的とした攻撃が近年の大きな社会的脅威となっている。具体的には、スマートフォン、タブレット端末等の急速な普及、ソーシャルメディア、クラウドサービス等の利用の拡大とともに、これらを狙った悪質なマルウェアが増加しているほか、利用者が気づかないうちにマルウェアに感染しているなど攻撃手法が巧妙化している。

このように、利用者が自身でマルウェアの感染を認識し自律的に対応することが困難になっている現状に対応するため、総務省では平成25年度より、インターネット・サービス・プロバイダ（ISP）やセキュリティベンダー等と連携して、マルウェア感染による被害未然防止等を行う官民連携プロジェクト（ACTIVE：Advanced Cyber Threats response InitiatiVE）に取り組んできたところであり、平成30年度からは、一般社団法人ICT-ISACにおいて本取組を実施している。

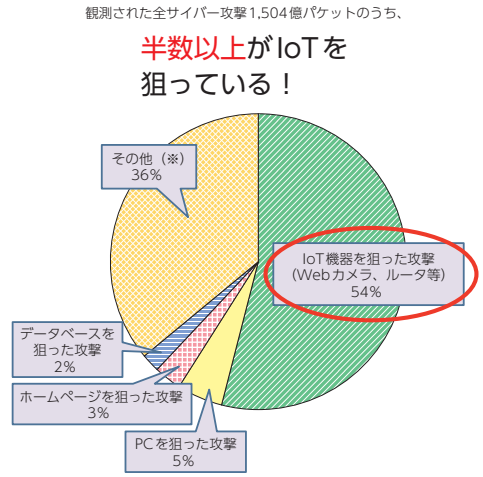
また、電気通信事業者による通信の秘密等に配慮した新たな対策や取組の在り方について検討を行うことを目的として、平成25年11月から「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」[*2]を開催し、平成27年9月に第二次とりまとめを公表した。本とりまとめを踏まえ、同年11月には、インターネットの安定的な運用に関する協議会において「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第4版）」[*3]が公表された。

＊2　電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会：http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/
＊3　電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第4版）：https://www.jaipa.or.jp/topics/2015/11/post.php

3 IoTに関する取組

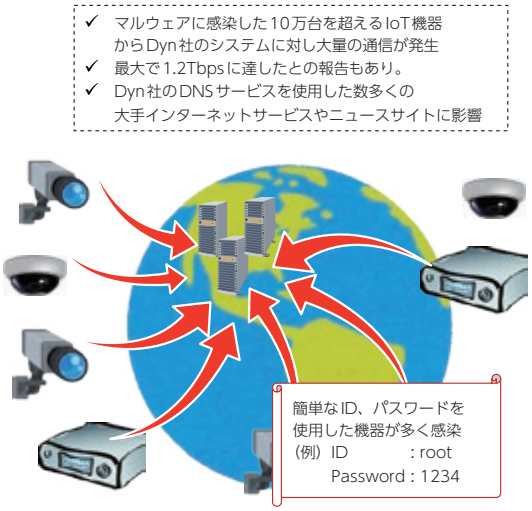
社会基盤としてのIoT化が進展する一方で、IoT機器については、管理が行き届きにくい、ウイルス駆除ソフトのインストールなどの対策が困難、利用者等においてインターネットにつながっている意識が低いなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。NICTが運用するサイバー攻撃観測網（NICTER）が平成29年に観測したサイバー攻撃パケット、1,504億パケットのうち、半数以上がIoT機器を狙ったものであるという結果が示されている（図表6-5-2-2）。実際に、米国では、平成28年10月、マルウェアに感染したIoT機器が踏み台となり、大規模なDDoS攻撃が発生し、一部サイトにアクセスできなくなる等の障害が発生した（図表6-5-2-3）。

図表6-5-2-2　NICTERによる観測結果



※IoT機器特有のポートを狙った攻撃から、特定のIoT機器の脆弱性を狙ったより高度な攻撃も観測されるようになっており、単純にポート番号だけから分類することが難しいIoT機器を狙った攻撃が「その他」に含まれている。

図表6-5-2-3　「Mirai」による大規模サイバー攻撃



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

こうした状況を踏まえ、「新しい政策パッケージ」（平成29年12月8日 閣議決定）、「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　－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）等において、官民連携によるボット撲滅に向けた体制を構築して対策を推進するとともに、実態調査等ができるよう必要となる法的整理を行うこととされたところであり、総務省において、パスワード設定に不備のあるIoT機器の調査等をNICTの業務に追加することや、第三者機関が指令サーバに関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有することを可能にすること等を内容とする「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」を平成30年3月に国会へ提出し、同改正法は同年5月に公布された。

4 国際連携に対する取組

サイバー空間はグローバルな広がりをもつことから、サイバーセキュリティの確立のためには諸外国との連携が不可欠である。このため、総務省では、サイバーセキュリティに関する国際的合意形成への寄与を目的として、各種国際会議やサイバー対話等における議論や情報発信・情報収集を積極的に実施している。

また、情報通信事業者等による民間レベルでの国際的なサイバーセキュリティに関する情報共有を推進するために、ASEAN各国のISPが参加するワークショップ、日本と米国のISAC（Information Sharing and Analysis Center）が意見交換するワークショップを引き続き開催した。

このほか、ASEAN地域において、EDR（Endpoint Detection and Response）を活用した標的型攻撃対策ソリューションの適用性評価や、セキュリティガバナンスの向上に資するSD-WANの導入に向けた実証実験を実施した。また、これまで実践的サイバー防御演習（CYDER）をタイ、マレーシアで実施してきたが、2017年12月の日ASEAN情報通信大臣会合[*4]において、CYDERをはじめとするサイバーセキュリティ演習をASEANの政府機関向けに実施することで合意した。

＊4　日ASEAN情報通信大臣会合：http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000063.html

政策フォーカス

総務省におけるサイバーセキュリティ推進体制の強化

1. 総務省における推進体制の強化、改組

サイバー空間における脅威の増大に対応していくため、総務省では、2017年に政策統括官を情報セキュリティ担当として任命し、サイバーセキュリティ課及び参事官（行政情報セキュリティ担当）を新設することで、サイバーセキュリティ政策の推進体制の強化を行った。2018年度にはサイバーセキュリティ統括官を新設し、その下に３人の参事官を設置することで、更なる体制の強化を図ることとしている。

2. IoT 機器の脆弱性対策に関する実施体制の整備

インターネットがあらゆる面で国民生活や社会経済活動の基盤となる中で、近年、国内外でサイバー攻撃が頻繁に発生しており、国民生活や社会経済活動に対して大きな影響が生じている。2016年10月には、マルウェア「Mirai」に感染した10万台を越えるIoT機器が踏み台となり、米国のDyn社のDNSサーバに対する大規模なDDoS攻撃が発生し、Twitter、Netflix等のサービスが停止する等の障害が発生した。従来、これらのDDoS攻撃は、主にPC、サーバ等にマルウェアを感染させることで行われてきたが、最近では、IoT機器の普及を受け、これらを踏み台として実施されることが多くなっており、NICTが運用しているサイバー攻撃分析システム（NICTER）の観測においても、2017年に観測されたサイバー攻撃1,504億パケット（前年1,281億パケット）のうち54%（前年64%）はIoT機器を狙ったものであるなど、IoT機器を狙ったサイバー攻撃が増加している状況である。

こうした状況を踏まえ、総務省に設置したサイバーセキュリティタスクフォースにおいて2017年10月に「IoTセキュリティ総合対策」が策定された。「IoTセキュリティ総合対策」においては、IoT機器の脆弱性についてライフサイクル全体（設計・製造段階、販売段階、設置段階、運用・保守段階、利用段階）を見通した対策や、脆弱性調査の実施等のための体制整備に取り組むべきことが示されている。

このうち、脆弱性の調査については、サイバー攻撃に用いられやすい簡単なID及びパスワードを使用するIoT機器を特定し、機器の利用者への注意喚起、機器製造事業者への対応要請につなげる必要があることから、総務省において、パスワード設定に不備のあるIoT機器の調査等をNICTの業務に追加すること等を内容とする「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、同改正法は同年５月に公布された。

3. 民間企業等におけるセキュリティ対策の促進

（1）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）の創設

IoT産業等の関連産業等の成長を見据え、民間企業におけるセキュリティ投資を促進するため、経済産業省と共同で税制改正要望を行い、「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、支援措置を講じる「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）を2018年度に創設することとした（図表1）。

図表１　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）の概要

【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。

（2）公衆無線 LAN のセキュリティ対策の在り方に関する検討（公衆無線 LAN セキュリティ分科会）

公衆無線LANについては、2020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ところ、公衆無線LANサービスの中には、セキュリティ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月からサイバーセキュリティタスクフォースの下に設置した「公衆無線LANセキュリティ分科会」において、利便性と安全性のバランスに配慮しつつ、公衆無線LANのセキュリティ対策のあり方とセキュリティに配慮した公衆無線LANサービスの普及策について検討を行った。2018年3月22日、本分科会は報告書を取りまとめ、本報告書を踏まえ、「セキュアな公衆無線LAN環境の実現に向けた行動計画」を策定、公表した（図表２）。

図表２　「セキュアな公衆無線LAN環境の実現に向けた行動計画」の概要

１．利用者・提供者の意識向上

（国における取組）

■　Wi-Fi利用者・提供者向けマニュアル（手引き）の改定（2018年夏頃を目途）
■　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（2018年秋頃を目途に開始）
■　e-ネットキャラバン等の活動を通じた青少年・高齢者向けの周知・啓発（2018年度以降に実施）
■　「公衆無線LAN版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）

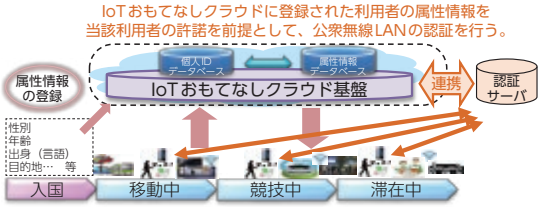
（民間事業者における取組）

■　暗号化の有無を識別可能な公衆無線LANサービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

２．データ利活用施策との連携

（国・民間事業者における取組）

■　公衆無線LANサービスとIoTおもてなしクラウドとの連携推進（2019年中を目途に実用化）



３．優良事例の普及

（国・民間事業者等における取組）

■　自治体に対する公衆無線LAN環境整備支援事業の継続的推進（2019年度まで継続）及び優良事例の普及促進（優良事例の調査・公表及びこれを踏まえた所要の政策支援については、2018年夏以降に実施）
■　デジタルスタジアムの実現に向けたセキュアな公衆無線LAN環境の整備及び公衆無線LANサービスのSSID等の情報や接続アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018年度以降に実施）

(3) 民間企業のサイバーセキュリティ対策の情報開示の在り方に関する検討（情報開示分科会）

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いるが、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、2017年12月にサイバーセキュリティタスクフォースの下に「情報開示分科会」を設置し、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った。本分科会における検討を踏まえ、2018年6月8日に「情報開示分科会報告書」を公表した（図表3）。

図表３　「情報開示分科会報告書」の概要

○　民間企業におけるセキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて、民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な対策を検討し、導入する「セキュリティ対策の好循環」が起こる環境の実現が期待される。
○　情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書（案）においては、①社内の情報共有（第一者開示）、②契約者間等の情報開示（第二者開示）、③社会に対する情報開示（第三者開示）の３つの側面に分けて整理している。

社内の情報共有（第一者開示）…自社のセキュリティ対策について、セキュリティ対策の担当部署だけでなく、社内全体で共有すること。

・経営層の理解を深め、気づきを与えるとともに、セキュリティ対策の担当部署の現場と経営層の間を繋ぐ、いわゆる「橋渡し人材」等の育成に向けた取組を進める必要がある。

（社内の情報共有に向けた橋渡し人材等の育成）
1．人材のスキルの具体化、スキル取得のための教育コンテンツの開発・普及、スキル認定を行う仕組みを産学官により構築するための検討。
【平成30年度中を目途に方向性を整理】

契約者間等の情報開示（第二者開示）…契約の相手方等、対象を限定して自社のセキュリティ対策を開示すること。

・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。

・サイバーセキュリティ保険について、対策の実施及び開示のインセンティブとなるような割引制度の普及や、グループ全体・サプライチェーン全体で一括して加入するような保険商品の展開が期待される。

（関係者間の情報共有促進のための仕組みづくりの検討）
2．米国等におけるISAO(※)等の動向等について調査するとともに、公的支援のあり方について検討。
【平成30年度中を目途に検討結果を取りまとめ】
（※）ISAO：Information Sharing and Analysis Organization
3．セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進し、標準仕様化に向けて検討。また、企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討。　【モデル事業については平成30年度に検討】

社会に対する情報開示（第三者開示）…社会の幅広い対象に向けて、自社のセキュリティ対策を開示すること。

・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。

※①基本方針等の策定状況　②管理体制　③教育・人材育成　④社外との情報共有体制　⑤第三者評価・認証

（第三者開示の促進に向けたガイドラインの策定）
4．「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。
【平成30年秋を目途にガイドラインを策定】
5．導入予定の「コネクテッド・インダストリーズ税制」の活用状況を分析するとともに、企業のニーズ等を反映した投資促進のための政策支援のあり方について検討。【支援税制の運用にあわせて適宜実施】

4. 円滑なインターネット利用環境の確保

総務省においては、IoT機器を悪用したDDoS攻撃等によるインターネット障害を防ぐために「円滑なインターネット利用環境の確保に関する検討会」を開催し、2018年2月、「対応の方向性」を取りまとめた。この取りまとめにおける主な提言内容と、それに対する総務省の取組は以下のとおりである。

一点目は、電気通信事業者の取り得るDDoS攻撃等の防止措置である。電気通信事業者から提案された、DDoS攻撃にかかる通信のメタデータを分析し、自らの通信ネットワーク内に存在するC&Cサーバと通信している機器やC&Cサーバを検知した上で、ユーザーに対して注意喚起を行うといった手法について、通信の秘密やプライバシーとの調整を図りながら実施していくことが望ましいとされたところであり、総務省において、通信の秘密やプライバシーとの関係等について引き続き検討を進めているところである。

二点目は、情報共有に係る制度整備と共有の促進である。電気通信事業者からDDoS攻撃等にかかる通信のメタデータを収集・分析した上で電気通信事業者に提供する第三者機関を設けることで、電気通信事業者のDDoS攻撃等への対応が促進されるよう、第三者機関を法律上位置づけるべきとされたところであり、総務省において、先述のパスワード設定に不備のあるIoT機器の調査等に係るNICTの業務追加と併せて、このような機関の認定制度等を盛り込んだ「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、同改正法は同年5月に公布された*1。

三点目は、IoT機器を含む脆弱な端末設備へのセキュリティ対策である。電気通信事業者のネットワークに接続されるIoT機器を含む端末設備において、基本的なセキュリティ対策を実施するため、国際競争力確保

＊1　情報共有に係る制度整備及びパスワード設定に不備のあるIoT機器の調査等に係るNICTの業務追加に係る部分の施行日は、公布の日から起算して9ヶ月を超えない範囲内において政令で定める日となっている。

等の観点を踏まえながら更に議論を深めるべきとされたところであり、情報通信審議会において、ネットワークの安全・信頼性を確保するための端末のセキュリティ対策について、検討を行っているところである。

最後に、2017年８月に発生した大規模なインターネット障害の検証を踏まえた対策である。電気通信事業者においてインターネットの経路情報を適切に制御する技術的対策を実施するとともに、事業者間でインターネット障害に関する情報を共有する体制を整備すべきとされたところであり、情報通信審議会において、情報通信ネットワーク安全・信頼性基準（ガイドライン）の改訂や、事業者から総務省へのインターネット障害の報告の在り方について、検討を行っているところである。