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等を定めた「サイバーセキュリティ基本法」が2014年（平成26年）11月に成立した。2015年（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た。

同本部における検討を経て、同年9月に「サイバーセキュリティ戦略*1」が閣議決定されており、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。

その後政府は、サイバー空間とフィジカル（実）空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立する人間中心の社会を目指す方針を決定し、経済社会が、人々に豊かさをもたらし、持続的に発展するためには、その基盤であるサイバー空間のサイバーセキュリティが確保されつつ、自律的・持続的に進化・発展していく必要があるとされた。こうした認識の下、2020年東京オリンピック・パラリンピック競技大会等の国際的なイベントを控えていることを見据え、2020年（令和2年）以降の目指す姿を念頭に置きつつ、サイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後3年間の諸施策の目標及び実施方針を国内外に明確にするため、新たな「サイバーセキュリティ戦略*2」が2018年（平成30年）7月に閣議決定された。同戦略では、目指すサイバーセキュリティの在り方を「サイバーセキュリティエコシステム」と名づけ、3つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進することとしている。また、同戦略の下、2018年度（平成30年度）に実施した具体的な施策の実施状況等の年次報告と、2019年度（令和元年度）に実施する具体的な施策等の年次計画をそれぞれまとめた「サイバーセキュリティ2019*3」が2019年（令和元年）5月に本部決定された。

また、サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進し、2020年東京オリンピック・パラリンピック競技大会の開催に万全を期すため、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策を推進する必要があることから、「サイバーセキュリティ基本法の一部を改正する法律」が2018年（平成30年）12月に成立し、同法に基づいて、官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会として、新たに「サイバーセキュリティ協議会」が2019年（平成31年）4月に創設された。同協議会は、国の行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者、教育研究機関、有識者等で構成され、構成員には秘密保持義務及び協議会への情報提供の協力義務が課されることとされており、専門機関等から得られた脅威情報を戦略的かつ迅速に共有し、サイバーセキュリティの確保に取り組んでいく。

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、2017年（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。その中で2018年（平成30年）7月に、同総合対策の進捗状況及び今後の取組について

＊1　サイバーセキュリティ戦略：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf
＊2　新たな「サイバーセキュリティ戦略」：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf
＊3　サイバーセキュリティ2019：https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf

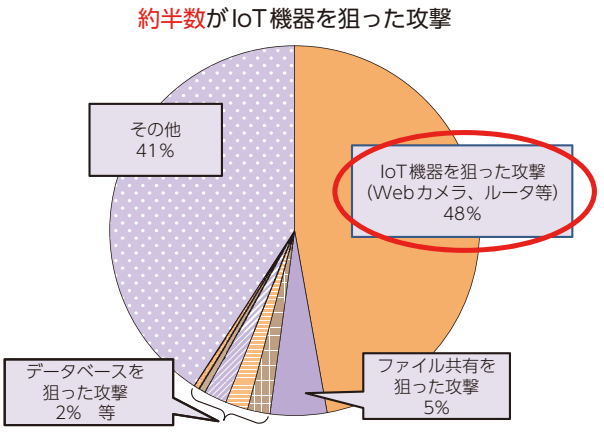
整理した「IoTセキュリティ総合対策 プログレスレポート2018[*4]」を公表したのに続き、2019年（令和元年）5月には「IoTセキュリティ総合対策 プログレスレポート2019[*5]」を公表した。

2 サイバーセキュリティ対策の強化

1 IoT等に関する取組

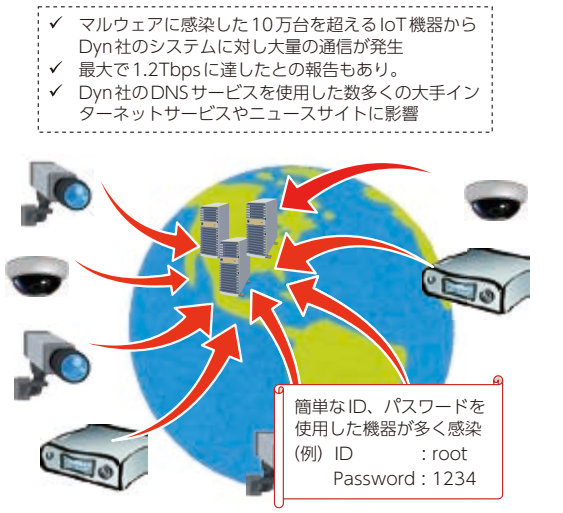
社会基盤としてのIoT化が進展する一方で、IoT機器については、管理が行き届きにくい、ウイルス駆除ソフトのインストールなどの対策が困難、利用者等においてインターネットにつながっている意識が低いなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。情報通信研究機構（NICT）が運用するサイバー攻撃観測網（NICTER）が2018年（平成30年）に観測したサイバー攻撃パケット、2,121億パケットのうち、約半数がIoT機器を狙ったものであるという結果が示されている（図表4-5-2-1）。実際に、米国では、2016年（平成28年）10月、マルウェアに感染したIoT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4-5-2-2）。

図表4-5-2-1　NICTERによる観測結果



＊1　NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。
＊2　IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

図表4-5-2-2　「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、「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－」、「IoTセキュリティ総合対策」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、総務省は、「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（平成30年）3月に国会へ提出、同改正法は同年5月に公布、同年11月に施行された。

同改正法に基づき、2019年（平成31年）2月より、NICTによるサイバー攻撃に悪用されるおそれのある機器の調査及び電気通信事業者による利用者への注意喚起を行う取組「NOTICE」を実施している。

また、「円滑なインターネット利用環境の確保に関する検討会」による「対応の方向性」（2018年（平成30年）2月20日とりまとめ）に基づき、以下の取組を実施している。

一点目は、情報共有に係る制度整備と共有の促進であり、上述の改正法により改正された電気通信事業法に基づき、2019年（平成31年）1月に、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関である「認定送信型対電気通信設備サイバー攻撃対処協会」として、一般社団法人ICT-ISACを認定した。

二点目は、電気通信事業者の取り得るDDoS攻撃等の防止措置であり、2018年（平成30年）9月、「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」において、DDoS攻撃に係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

＊4　IoTセキュリティ総合対策 プログレスレポート2018：http://www.soumu.go.jp/main_content/000566458.pdf
＊5　IoTセキュリティ総合対策 プログレスレポート2019：http://www.soumu.go.jp/main_content/000623344.pdf

で、ユーザーに対して注意喚起を行うといった手法等について、通信の秘密やプライバシーとの関係等を踏まえ、取組の実施に向けての条件や留意点等を整理した。

三点目は、IoT機器を含む端末設備のセキュリティ対策であり、今後製品化されるIoT機器がパスワード設定の不備等によりサイバー攻撃に悪用されないようにする対策として、2019年（平成31年）3月にIoT機器の技術基準にセキュリティ対策を追加する端末設備等規則を改正し、2020年（令和2年）4月に施行となる。

四点目は、2017年（平成29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り、情報通信ネットワーク安全・信頼性基準を改正[*6]し、インターネットの経路設定時の人為的ミスの防止等大規模なインターネット障害発生時に有効な対策についての規定を整備した。

2　人材育成に関する取組

我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、その育成は喫緊の課題である。サイバーセキュリティ戦略（2018年（平成30年）7月27日閣議決定）においても「産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化していく。」と言及されているとおり、政府一丸となってサイバーセキュリティ人材の育成に取り組んでいる。

巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、2017年（平成29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、サイバーセキュリティ人材育成の取組（CYDER、サイバーコロッセオ、SecHack365）を積極的に推進している。

CYDERは、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対象とした実践的サイバー防御演習である。受講者は、組織の情報システム担当職員として、チーム単位で演習に参加し、組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験する。2018年度（平成30年度）は、全国47都道府県で全107回の演習を実施し、2,666名が受講した。2019年度（令和元年度）も同規模で実施予定である（図表4-5-2-3）。

サイバーコロッセオは、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大会関連組織のセキュリティ担当者等を対象者とした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し、2018年度（平成30年度）は延べ137名が受講した。さらに、2018年度（平成30年度）からは、講義形式によりセキュリティ関係の知識や技能を学ぶコロッセオカレッジを開設し延べ347名が受講した。2019年度（令和元年度）も、さらなる内容の充実や受講機会の拡大を図りながら大会関連組織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・開発等を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。2017年度（平成29年度）は10歳から24歳の39名が、2018年度（平成30年度）は12歳から24歳の46名が1年間のプログラムを修了した。2019年度（令和元年度）以降も、育成プログラムの質の向上を図りつつ、同規模で実施予定である。

また、特に人口減少が急速に進む地方において、サイバー攻撃に対処可能な人材の育成・確保は大きな課題となっていることから、2018年（平成30年）12月からサイバーセキュリティタスクフォースの下に「サイバーセキュリティ人材育成分科会」を開催した。同分科会の取りまとめも踏まえ、地域におけるサイバーセキュリティ人材育成のエコシステムの構築に向け、地域の中小企業や自治

図表4-5-2-3　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

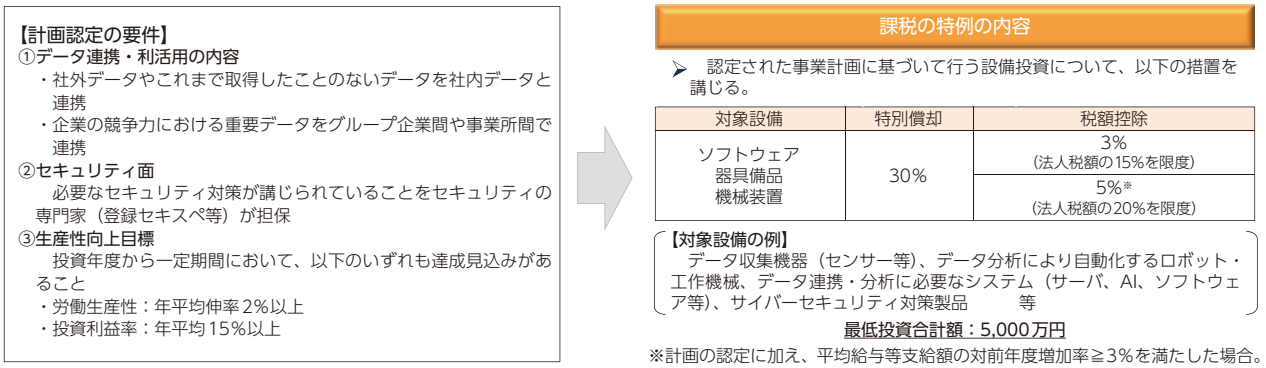
＊6　2019年（平成31年）3月26日公布、同年4月1日施行

体等のサイバーセキュリティに関する意識向上や取組を促進するための研修等、地域のサイバーセキュリティ人材の育成に取り組むこととしている。

3　民間企業等のセキュリティ対策の促進に関する取組

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、2018年度（平成30年度）税制改正において、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）を創設し、説明会等を通じて同税制の周知を行い、活用を促進した（図表4-5-2-4）。

図表4-5-2-4　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



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（平成29年）12月より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」を開催し、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（平成30年）6月8日に「情報開示分科会報告書」を公表した。

同報告書を踏まえ、2018年度（平成30年度）に企業のサイバーセキュリティ対策に関する情報開示を行うに当たって参照可能な手引きの策定に着手した。なお、手引きの策定・公表は2019年度（令和元年度）早期を予定している。

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（平成29年）12月の日ASEAN情報通信大臣会合[*7]の合意に基づき、2018年（平成30年）9月に日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN Japan Cybersecurity Capacity Building Centre）をタイ・バンコクに設立した。現在、同センターにおいてASEAN各国の政府機関及び重要インフラ事業者を対象にCYDER等を継続的に実施している。

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

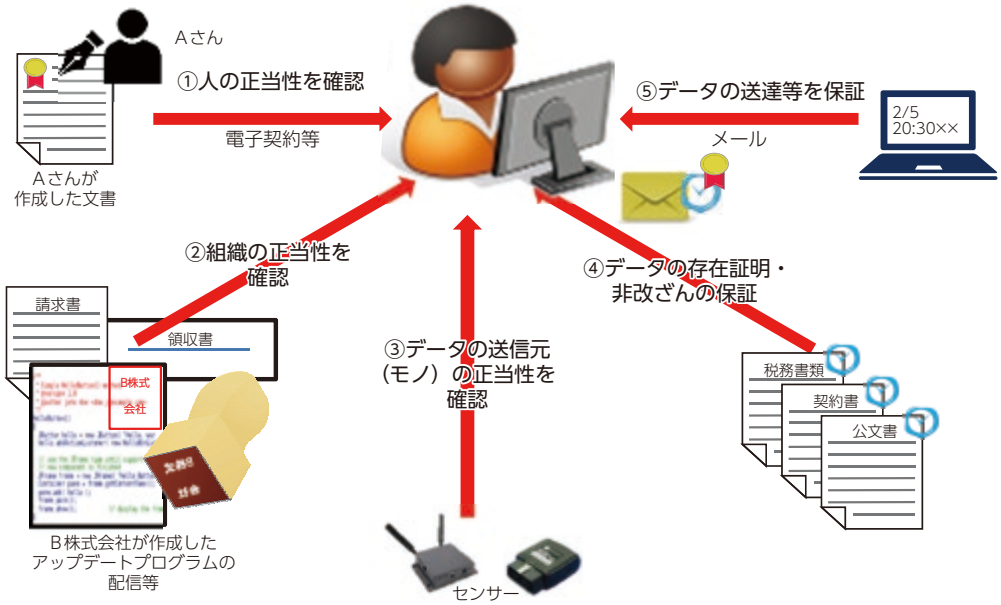
5　トラストサービスに関する取組

サイバー空間の自由で安心・安全なデータの流通を実現するためには、データの信頼性を確保する仕組みとして、データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠であることから、「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、次のようなトラストサービスに関する現状や制度的課題について検討を行っている（図表4-5-2-5）。

①人の正当性を確認できる仕組み（電子署名）
②組織の正当性を確認できる仕組み（組織を対象とする認証、ウェブサイト認証）
③IoT機器等のモノの正当性を確認できる仕組み
④データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）
⑤データの送達等を保証する仕組み（eデリバリー）

こうしたトラストサービスについては、EUでは2016年（平成28年）7月に発効したeIDAS（electronic Identification and Authentication Services）規則により、電子署名、タイムスタンプ、eシール等のトラストサービスについて包括的に規定しているところであり、国際的な相互運用性の確保の観点からも、我が国としてのトラストサービスの在り方について検討が必要である。

図表4-5-2-5　トラストサービスのイメージ



政策フォーカス

IoTセキュリティ対策の推進

1　背景等

IoT機器が普及する一方で、IoT機器を狙ったサイバー攻撃は近年増加傾向にある。センサーやウェブカメラなどのIoT機器は、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、サイバー攻撃に狙われやすい特徴を持っており、サイバー攻撃に悪用されるおそれがある。諸外国においては、IoT機器を悪用した大規模なサイバー攻撃（DDoS攻撃）によりインターネットに障害が生じるなど、深刻な被害が発生していることから、我が国においても2020年オリンピック・パラリンピック東京大会などを控え、対策の必要性が高まっている。

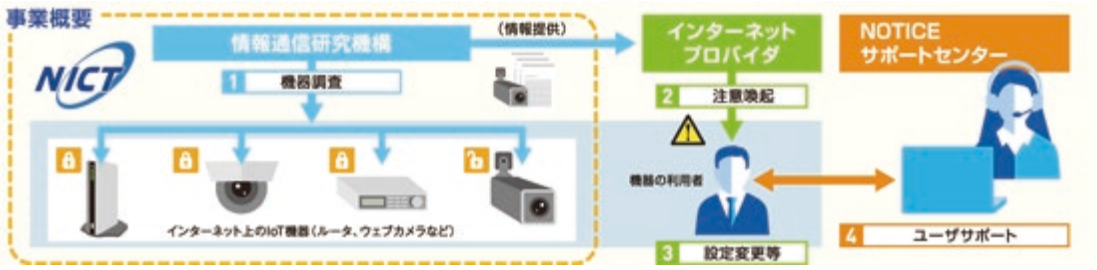
このような状況を踏まえ、総務省では、①現在使用されているIoT機器の対策、②今後販売されるIoT機器の対策を実施している。

2　NOTICEプロジェクト（現在使用されているIoT機器への対策）

IoT機器等を悪用したサイバー攻撃の深刻化を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、パスワード設定等に不備のあるIoT機器の調査等を追加するため、国立研究開発法人情報通信研究機構法が2018年（平成30年）5月に改正され、同年11月に施行された。

上記改正法に基づき、総務省及びNICTは、20社を超えるインターネットプロバイダと連携し、サイバー攻撃に悪用されるおそれのあるIoT 機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」を2019年（平成31年）2月より実施している（図表1）。

図表1　NOTICE実施概要



「NOTICE」の実施内容は以下の通り。

1. 機器調査

NICTは総務省から認可を受けた実施計画に基づき、日本国内のグローバルIPアドレス（IPv4）によりインターネット上で外部からアクセスできるルータ、ウェブカメラ、センサーなどのIoT機器に対し、ID・パスワードを入力することができるかどうかを確認し、これらの機器に容易に推測されるID・パスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定し、当該機器の情報をインターネットプロバイダに通知する。

なお、上述の実施計画に基づき、容易に推測されるID、パスワードを外部から入力し、サイバー攻撃に悪用されるおそれのあるIoT機器を特定することは、改正法において、不正アクセス行為の禁止等に関する法律で禁止されている不正アクセス行為から除外されている。

2. 注意喚起

インターネットプロバイダは、NICTから受け取った情報を元に当該機器の利用者を特定し、電子メールなどにより注意喚起を行う。

3. 設定変更等

注意喚起を受けた利用者は、注意喚起メールやNOTICEサポートセンターのウェブサイトの説明などに従い、パスワード設定の変更、ファームウェアの更新など適切なセキュリティ対策を行う。

4. ユーザサポート

総務省が設置するNOTICEサポートセンターは、利用者からの電話、ウェブサイト（https://notice.go.jp/）からの問合せに応じ、適切なセキュリティ対策等を案内する。

なお、上記ウェブサイトにおいては、NOTICEの取組概要やIoTのセキュリティ対策に係るコンテンツを利用者向けに提供している。

今回の取組の実施にあたっては、広くIoT機器のユーザに周知し、対策の必要性について理解を得ることが不可欠である。IoT機器のセキュリティ対策の必要性や本取組の内容の広報のため、公共交通機関での広告、全国紙での広告掲載に加え、家電量販店や自治体等でのポスター掲示（図表２）を２月から実施している。また、2019年（平成31年）２月13日には、NOTICEの実施体制の強化及び周知広報を目的としたキックオフイベントを開催し、NICT、本取組に参加するインターネットプロバイダ、関係団体、関係省庁が参加した。

図表２　　周知ポスター、NOTICEキックオフイベント　集合写真

〈周知ポスター〉

〈NOTICEキックオフイベント　集合写真〉

3　IoT機器の技術基準（今後製造されるIoT機器への対策）

電気通信事業法では、電気通信事業者のネットワークに接続して使用する端末設備は、端末設備等規則（昭和60年郵政省令第31号）で定める技術基準に適合しなければならないこととされている。今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、情報通信審議会等での検討を経て、IoT機器の技術基準にセキュリティ対策を追加するための端末設備等規則の改正[*1]を行い、あわせて、改正後の端末設備等規則の運用方法や解釈等を明確化する「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」を2019年（平成31年）４月に策定・公表した。

端末設備等規則の改正概要は以下の通り。

・インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

① アクセス制御機能[※1]（例えばアクセス制限をかけてID・パスワード入力を求め、正しいID・パスワードの入力時のみ制限を解除する機能のこと）

② 初期設定のパスワードの変更を促す等の機能

③ ソフトウェアの更新機能[※1]

又は ①～③と同等以上の機能[※2]

※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。

※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証（CC認証）を受けた複合機等が含まれる。

・PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

＊1　2019年（平成31年）３月１日公布、2020年（令和２年）４月１日施行