総務省のIoT機器を含む端末設備のセキュリティ対策について

総務省 総合通信基盤局 電気通信事業部
電気通信技術システム課
中山　貴博

近年、インターネットから操作可能な家電やスマートメータ等の利用が進む中、様々な分野においてIoT（Internet of Things）の普及が進んでおり、IoTサービスが国民生活に深く浸透しつつある一方、IoT機器に感染するマルウェア「Mirai」による大規模DDoS攻撃等により、インターネットに障害を及ぼす事案も増加している。今後普及していく様々なIoTサービスを誰もが安心して安定的に利用できるネットワーク環境を確保するため、総務省では、電気通信事業法上の観点からIoT機器を含む端末設備のセキュリティ対策について検討を行ってきた。本稿では本検討の背景や検討結果について概略を述べる。

1.検討の背景

民間調査会社（HIS Technology）の推定によれば、2015年時点でIoTデバイスの数は約154億個、2020年までには約2倍の約304億個まで増大すると予測されている。IoTの普及に伴い、IoT機器を踏み台とするサイバー攻撃も増加している。このように、近年サイバー攻撃等によりインターネットに重大な支障が発生する事例が増加していることを踏まえて総務省が開催した、「円滑なインターネット利用環境の確保に関する検討会」において、2018年2月、電気通信事業におけるこれらの障害への対処を促進するための「対応の方向性」が取りまとめられた。

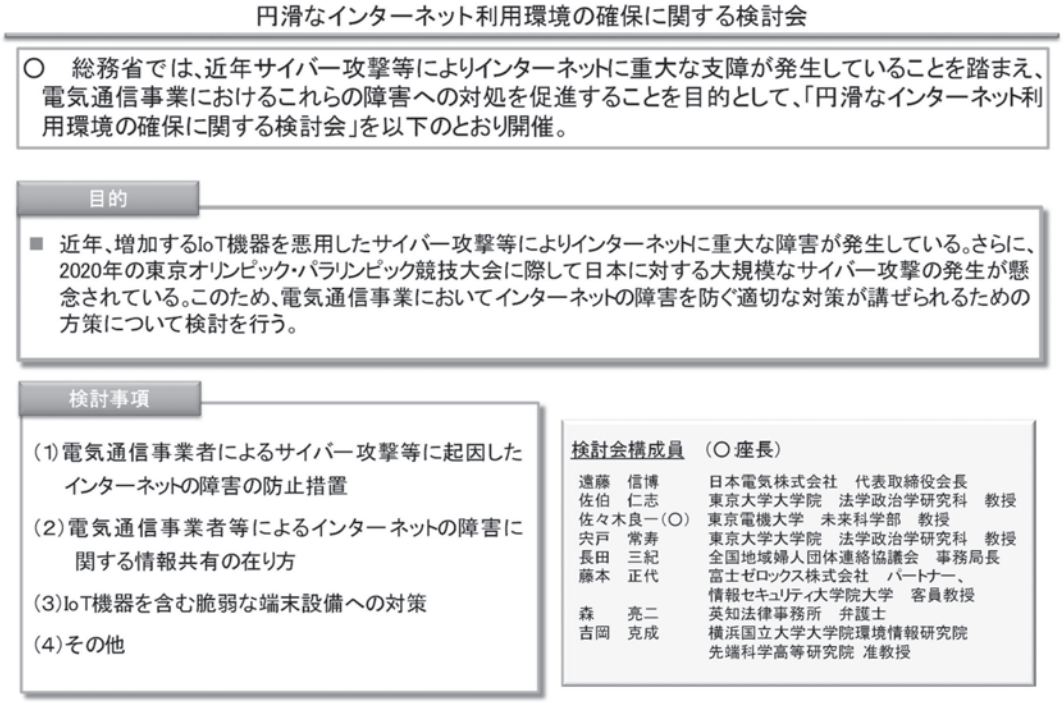

図1　円滑なインターネット利用環境の確保に関する検討会概要

「円滑なインターネット利用環境の確保に関する検討会」により取りまとめられた「対応の方向性」の概要は図2及び図3のとおりである。

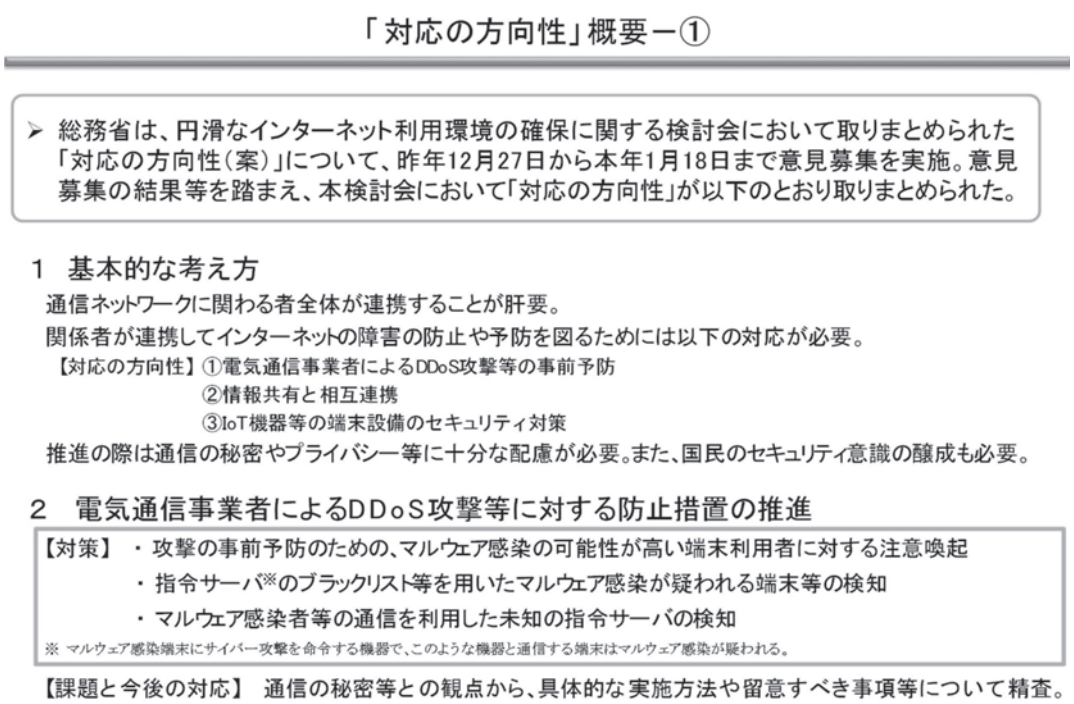

図2　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要①

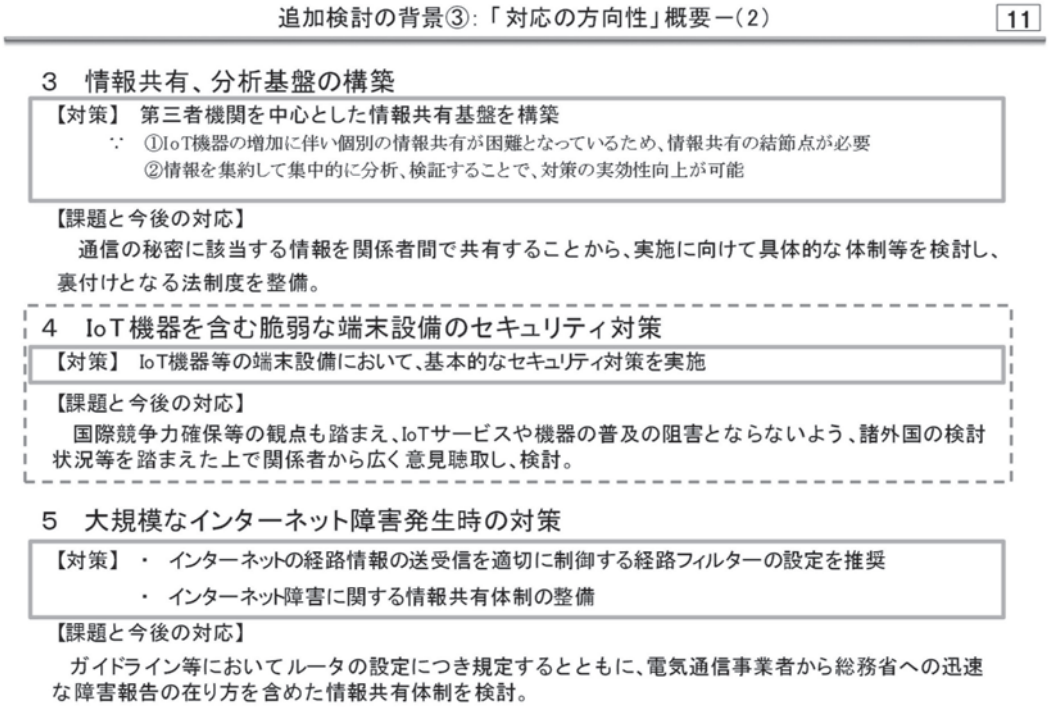

図3　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要②

このうち、「IoT機器を含む脆弱な端末設備のセキュリティ対策」については、IoT機器等の端末設備において、基本的なセキュリティ対策を実施すべきとして、具体的な検討にあたっては、国際競争力確保等の観点も踏まえ、IoTサービスや機器の普及の阻害とならないよう、諸外国の検討状況等を踏まえた上で関係者から広く意見聴取し、検討することとされた。こうした結論を踏まえ、どのような対策が有効か、技術的な観点から専門的な検討を行うため、情報通信審議会情報通信技術分科会IPネットワーク設備委員会（以下「委員会」という。）において検討を実施した。

2.端末設備の接続の技術基準と端末機器の基準認証制度について

IoT機器に関連する電気通信事業法における制度として、利用者が接続する端末設備の接続の技術基準と、その技術基準に適合していることを認証する端末機器の基準認証制度がある。本節では、これらの制度について概略を説明する。

(ア)端末設備の接続の技術基準の考え方

電気通信事業法における「端末設備」とは、電気通信回線設備(図4のONU)の一端に接続される電気通信設備であって、一の部分の設置の場所が他の部分の設置の場所と同一の構内等であるものをいい、図4の例では、無線LANルータ、電話機、スマートTV、PC、スマートフォンの総体が端末設備となる。

電気通信事業法では、電気通信事業者の電気通信回線設備に接続して使用する端末設備について、次の事項を確保するものとして総務省令に定める技術基準に適合することを求めている。

- 電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること
- 電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること
- 電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界を明確であるようにすること

また、電気通信回線設備を設置する電気通信事業者以外の者が設置する端末設備以外の電気通信設備を「自営電気通信設備」といい、その接続の技術基準として、端末設備に係る技術基準が準用されている。

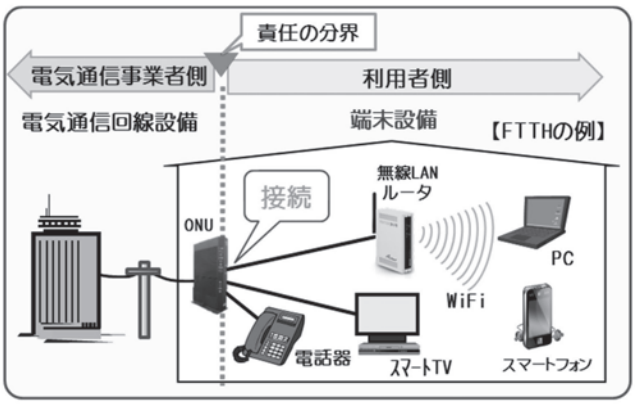

図4　利用者が接続する端末設備

(イ)端末設備の接続と技術基準の確保

電気通信事業者は、利用者から端末設備をその電気通信回線設備に接続すべき旨の請求を受けたとき、その接続が(ア)の技術基準に適合しない場合等を除き、その請求を拒むことができないとされている(電気通信事業法第52条)。

また、利用者は、適合表示端末機器(技術基準に適合している旨の表示(図5、いわゆる技適マーク)が付された機器)を接続する場合等を除き、電気通信事業者による接続の検査を受け、技術基準に適合する端末設備と認められなければ、当該設備を使用できないとされている(電気通信事業法第69条)。

さらに、利用者は、端末設備を電気通信回線設備に接続するとき、適合表示端末機器をプラグジャック方式等により接続する場合を除き、これに係る工事を工事担任者に行わせ、又は実地に監督させる必要がある(電気通信事業法第71条)。

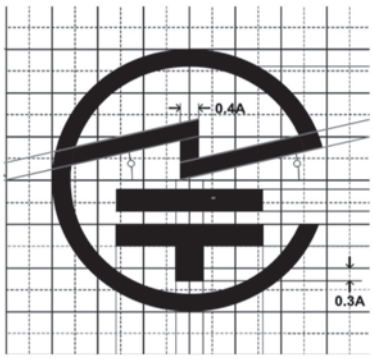

図5　技術基準に適合している旨の表示(電気通信事業法の認証では「A」又は「T」の記号が付される。)

（ウ）端末機器の基準認証制度

端末機器の基準認証制度とは、事業用電気通信設備に接続して使用される端末機器やその設計について、接続の技術基準に適合していることを登録認定機関等が認定する制度であり、

－端末機器を1台毎に認定する技術基準適合認定

－端末機器の設計を認証する設計認証

－製造者等が技術基準に適合していることを自ら確認し、総務省に届け出る技術基準適合自己確認

のいずれかの方法により認定等を取得することができる。認定等を取得した機器は図5の表示を付すことができ、当該表示が付された機器は適合表示端末機器となる。

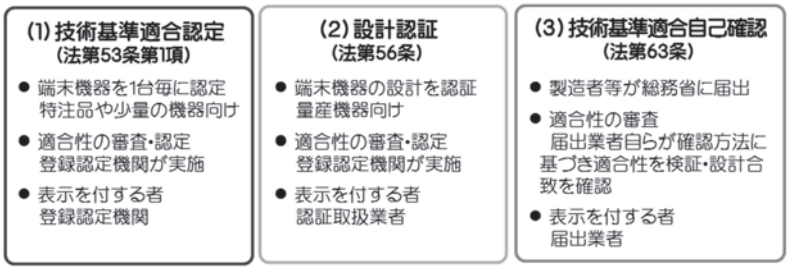

図6　技術基準適合認定等の取得方法

3.IoT機器を含む端末設備のセキュリティ対策について

近年、Webカメラやルータ等のIoT機器が乗っ取られ、インターネットに障害を及ぼすようなDDoS攻撃等のサイバー攻撃に悪用される事案が増加している。

一方、情報通信ネットワークの安全・信頼性を確保するために、電気通信事業法においては、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさない等を原則とする端末設備の接続の技術基準が定められている。

委員会では、そのような制度の枠組みの中で、大規模DDoS攻撃等のサイバー攻撃を抑止するため、IoT機器を含む端末設備がマルウェアに大量感染しないこと等を目的とするセキュリティ対策を技術基準に追加することについて検討を行った。

以下では、これらの検討をとりまとめた情報通信審議会一部答申「IoTの普及に対応した電気通信設備に係る技術的条件」（平成30年9月、以下「一部答申」という。）を基に説明する。

・端末設備の接続の技術基準にセキュリティ要件を追加する必要性について

近年増加しているマルウェア「Mirai」等による大規模DDoS攻撃を抑止するためには、ネットワークを提供する電気通信事業者、ネットワークの利用者、IoT機器のそれぞれで対応を行うことが重要となる。以下にそれぞれの対応の概略を説明する。

○電気通信事業者における対応

大規模DDoS攻撃については、電気通信事業者による対応が期待されることは言うまでもない。しかしながら、電気通信事業者は、電気通信事業法第4条に基づき、その取扱中に係る通信の秘密は侵してはならないとされていることから、原則として、通信内容を確認することは不可能である。このため、仮にIoT機器からの大量通信が発生した場合であっても、通信内容を確認して正常な通信なのか、DDoS攻撃に加担しているものであるか判別することができない。また、マルウェア感染したIoT機器のみの通信を止めることについても、技術面から困難であるため、電気通信事業者が取り得る対応も制約がある状況となっている。

なお、本年5月に成立した「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」により、電気通信事業者によるセキュリティ対策を強化するため、電気通信事業者による情報共有体制などの新たな取組みが導入されることとなっている。

○利用者における対応

大規模DDoS攻撃に対処する上では、IoT機器の利用者における対応も重要である。しかしながら、例えば機器メーカ等がソフトウェアの更新を呼びかけたとしても、技術的に対策が難しい、利用者が更新に気づかない等の理由で全ての利用者に対応を求めることは容易ではない。

更に、DDoS攻撃の踏み台となっている機器は、必ずしもその利用者に直接の被害が及ぶわけではないことから、IoT機器が目的どおり動作している限り、そもそも利用者は攻撃の踏み台となっていることを認知することが難しいという課題も存在する。

実際に過去の事例では、利用者に注意喚起を行った後、脆弱性のある機器の約8割に対処が行き届くのに約3年を要したものもあった。

以上のことから、利用者における対応についても限界がある状況となっている。

○IoT機器における対策

現在のIoT機器に対するサイバー攻撃は、グローバルIPアドレスを有する機器を対象として、セキュリティ上の不適切な設定や利用者に認知されていない脆弱性等を悪用したサイバー攻撃が多い。平成28年10月に、米国を中心に大手インターネットサービスの障害を引き起こしたマルウェア「Mirai」の事例では、本来不要な通信機能のアクセス制御のため、主に工場出荷時のID/パスワードをそのまま使用していたIoT機器が数多く乗っ取られ、大規模DDoS攻撃が行われた。このような事例でも、IoT機器において比較的に簡易なセキュリティ対策を行うことで大半の攻撃を防ぐことが可能である。

また、アクセス制限がない機器、ハードコーディングされたID/パスワードを持っている機器、既知の脆弱性が埋め込まれている機器等が出荷された場合には、その脆弱性を事後に修正することは困難なものとなる。そのため、出荷前に必要な対策を講じることが有効であると考えられる。

以上を踏まえ、一部答申においては、IoT機器を含む端末設備に対するセキュリティ対策として、電気通信事業法の枠組みの中で、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった端末設備の接続の技術基準の原則の範囲内において、その技術基準にセキュリティ要件を追加することが適当とされた。

なお、当該セキュリティ要件は、電気通信事業法の観点からIoT機器のマルウェア大規模感染を防止することを目的としているものであり、IoTセキュリティを確保するためには、これらの対策だけでは不十分であることに留意する必要がある。

・IoTセキュリティ対策に関する国内外の動向

IoTセキュリティ対策については、現在、欧米等においても議論が活発に行われているところである。

米国においては、「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」に関する報告書が取りまとめられた。当該報告書では、IoTセキュリティに関し、初期設定及び自動ソフトウェアの更新機能などの重要性を指摘するとともに、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要であるとして、今後、具体的な施策の検討が行われていくことが見込まれる。

一方、欧州においては、ICT機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証すること等を目的として、「ICTサイバーセキュリティ認証に関する規則案」が公表され、引き続き欧州議会で検討が行われているところである。

機器を対象としたセキュリティ認証に係る国際標準については、政府調達機器の一部に関し、国際標準ISO/IEC15408に基づくCC(Common Criteria)認証が行われている。CC認証は、世界28カ国で受け入れられている認証制度であり、複合機の例では、他の利用者による不正な操作や通信データの盗聴・改ざん、管理機能への不正なアクセス等を脅威として想定し、識別・認証・権限付与やアクセス制御、ファームウェアに電子署名を付すといった高信頼な通信等のセキュリティ機能を保証するとともに、セキュリティ機能自体の脆弱性評定も実施している。

IoTセキュリティ対策に関する国際標準は、ISO/IEC JTC1/SC27において検討が開始されたところであり、現時点で確立しているものではない。しかし、IoTのグローバル市場への展開や国際競争力確保といった観点から、CC認証をはじめとした国際標準との整合性を図るとともに、今後も、国際的な動向の把握に努める必要がある。

また、日本からは現在、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」の内容について国際標準の議論の場に提案が行われているところであり、今後も積極的に我が国の取組みを発信していくことが重要である。

・端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

一部答申では、端末設備の接続の技術基準に追加すべきセキュリティ対策として、インターネットプロトコルを使用する端末設備であって、電気通信回線設備を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについて、大量感染を防ぐための最低限のセキュリティ要件として、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及びファームウェアの更新機能、又はそれらと同等以上の機能を具備することを要件とすることが適当であるとされた。その具体的な機能については、表1のとおりである。

表1　端末設備に最低限必要なセキュリティ要件の具体的な機能

セキュリティ要件	具体的な機能
アクセス制御機能	・電気通信回線設備を介して接続されることにより当該端末が不正に操作されないことを目的として、当該操作の前にアクセス制御を行うことが必要。
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	・アクセス制御を識別符号によって行う場合は、当該識別符号が他人から容易に推測できないものとして設定されることを目的として、当該端末の利用者に対し当該識別符号について初期値の変更を促す（二以上の識別符号の組み合わせによるものの場合は少なくとも一つの識別符号が対象。以下同じ。）若しくは識別符号の初期値について機器毎に別のものを付す、又はそれらに準じる措置を行うことが必要。
ファームウェアの更新機能	・端末に記憶されている当該電気通信の送受信の機能に係るソフトウェアの更新が可能であることが必要。当該更新は安全かつ自動で行われることが推奨されるが、IoT機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件とはしない。 ・端末への電力供給が停止した場合であっても、当該更新されたソフトウェアや変更されたアクセス制御の設定内容を維持することが必要。
同等以上の機能	・CC認証などの国際標準に基づくセキュリティ認証を取得した複合機など、上記の機能と同等以上のセキュリティ機能を有すると認められるものについては、当該セキュリティ要件を満足するものとみなす。

なお、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であり、それにより上記セキュリティ要件に関する機能が出荷時とは異なるものになることが想定される機器については、当該セキュリティ要件を適用することが馴染まないことから、本要件の規定の対象外としている。しかしながら、その場合においては、利用者においてアンチウィルスソフトを導入する等の適切な対策を行うことが求められる。

・技術基準適合認定等の対象機器の範囲

セキュリティ要件が追加された技術基準に関し、当該技術基準に係る技術基準適合認定等を求める端末機器の範囲については、インターネットプロトコルを使用する全ての機器に対し、セキュリティ対策を求めることが理想的ではあるが、より効率的かつ効果的な対策とするため、一部答申では、セキュリティ対策を行うことが効果的な機器の範囲を明確にすることが適当としている。

マルウェアに感染しているIoT機器に関する研究では、感染機器の９割以上が不明であるものの、判明している範囲では海外製品のインターネットカメラ、デジタルビデオレコーダ、ルータ等が多い。国内製品においても、ルータ、ゲートウェイ、ネットワークストレージ、太陽光パネル管理システム、電力デマンド監視システムといった機器に感染事例が見つかっているという報告がなされている。

現在のIoT機器に対するサイバー攻撃は、グローバルIPアドレスを有する機器へのインターネット側からの直接的攻撃が主流であり、ルータ等の直接接続される機器に感染した後、更に家庭内の機器にまで感染活動を行うものは5%程度という分析事例がある。そのため、インターネット側からアクセスし操作可能なネットワークサービス（Web管理、telnet等）を使用する機器については、特に脆弱性対策が必要と考えられる。

現状の技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しているが、上記を踏まえれば、現状においてネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、一部答申では、セキュリティ要件が追加された技術基準適合認定等の対象についても、従来と同様に電気通信回線設備に直接接続される端末機器とすることが適当としている。

なお、直接接続される機器とは、電気通信回線設備に物理的かつ技術的に直接接続可能な端末機器を指すが、その中でも恒常的に既認定機器を介して接続する機器（屋外に持ち出す等により電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器(例: 大型白物家電等)）については、今後、技術基準適合認定等の対象外とすることとされた。

ただし、この場合に利用者が認定等を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要があるとされている。

また、認定等を取得していない機器については、表1のセキュリティ要件を満たしていないおそれがある。こうした機器の乗っ取りを防ぐためには、IoT機器メーカやIoTシステム/サービス提供者等において、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」等に基づき、直接接続される既認定機器における対策も含む適切なセキュリティ対策を検討・実施していくことが必要となる。

今後、端末機器の接続が多様化することが想定される。認定等が必要な機器の範囲等については、一部答申の記載だけでは判断が難しくなる事例が出てくる可能性があることから、一部答申においては、機器メーカ等が判断できるように、ガイドライン等により明示することについて速やかに検討を開始する必要があるとされている。

・セキュリティ要件の追加に係る経過措置

端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合には、IoT機器メーカや登録認定機関等の対応を考慮して、一定の期間を設けて施行することとなるが、本件に関する改正について、その期間は1年から2年程度とすることとされている。

また、従来の制度に基づき、新制度の施行前に取得した技術基準適合認定等については、施行後も引き続き有効であり、当該認定等に基づく機器も引き続き使用することを可能とすることが適当とされている。

・技術基準適合認定等の審査方法等

登録認定機関等による技術基準適合認定については、セキュリティ要件の対象となる機器の審査が円滑に行われるよう、その審査方法や機器の審査単位等について通信事業者、機器メーカ等が参画可能な場で別途議論を行うことが適当であるとされている。

4. 今後の予定

一部答申を踏まえ、総務省では、3.のセキュリティ要件を端末設備の接続の技術基準に追加するための制度整備を行うこととしている。本制度整備による改正法令の施行後は、端末メーカ等において技術基準適合認定等を取得する場合には、セキュリティ要件にも適合する必要があることとなり、大規模DDoS攻撃等の抑止に寄与することが期待される。

また、ガイドライン等において明示することとされた、技術基準適合認定等を要する機器の範囲や端末機器の審査単位等については、今後、総務省において検討を実施し、ガイドライン等を策定・公表する予定である。こうしたガイドラインにより、端末メーカ等による技術基準適合認定等の取得に係る検討や手続が円滑に進むことが期待される。

本稿では、本年9月に取りまとめられた一部答申の内容を基にIoT機器を含む端末設備に関するセキュリティ対策について説明を行った。本文でも触れたとおり、今回検討を行ったIoT機器を含む端末設備のセキュリティ対策は、あくまで電気通信事業法の観点から大規模DDoS攻撃等を抑止するため、IoT機器のマルウェア大規模感染を防止することを目的としているものであり、個人情報の保護などのIoTセキュリティ全体を確保するためには、これらの対策だけではなく、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」等に基づき、適切なセキュリティ対策を検討・実施していくことが必要である。