IoT 機器等へのサイバー攻撃の急増と固定電話網のＩＰ網への移行等に対する取組

― 電気通信事業法・ＮＩＣＴ法改正法 ―

千葉　翔平
（総務委員会調査室）

１．はじめに

第 196 回国会（平成 30 年常会）において、情報通信技術の進展に対応し、電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護するため、IoT 機器等に対するサイバー攻撃又はそのおそれへの対処に係る制度と、電気通信番号の管理の仕組みと電気通信業務の休止及び廃止に係る情報の整理及び公表の制度の新設等の措置を講ずる「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」が成立した（平成 30 年５月 16 日成立、平成 30 年法律第 24 号）。

本稿では、近年急激に増加している IoT 機器に対するサイバー攻撃等への対策と、交換

機の寿命等に伴うＮＴＴ東西の固定電話網のＩＰ網への移行に関する総務省や事業者等の議論を踏まえて整理された方向性等、法律案の提出の背景について概観するとともに、本法の概要と主要な国会論議を紹介する。

２．法律案の提出の経緯

（１）IoT 機器等へのサイバー攻撃の増加と機器の脆弱性調査・被害拡大防止策の検討

ア　検討の背景

パソコンやスマートフォンのような従来型のＩＣＴ端末だけでなく、自動車や家電、施設等身の回りのあらゆるものがネットワークにつながる IoT（Internet of Things：モノのインターネット）社会が到来しようとしている。インターネットに接続される IoT 機器は爆発的に増加しており、2020 年までには約 300 億台の IoT 機器がインターネットに接続されるものと見込まれ[1]、我々の生活の向上につながることが期待される。

その一方で、IoT 機器にはセキュリティ面で深刻な脆弱性を抱えたものも多数存在する。国内外において、IoT 機器を悪用した DDoS 攻撃[2]等のサイバー攻撃によりインターネットに障害が発生する事例が急増しており、特に我が国では東京オリンピック・パラリンピックが行われる 2020 年に向けて DDoS 攻撃等の脅威が高まることが想定されている[3]。

イ　機器の脆弱性調査に関する検討

平成 29 年１月から開催されている総務省のサイバーセキュリティタスクフォースは、同年 10 月に IoT 機器等の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について整理した「IoT セキュリティ総合対策」[4]を公表した。

この中では、既に設置されている IoT 機器はもとより、製造・販売された新規の IoT 機器についても新たな脆弱性を突いたサイバー攻撃が行われる可能性があるため、関係者の連携による体制を整備し、計画的かつ包括的な脆弱性調査を継続的に実施する必要があるとしている。

その際、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等について、所要の脆弱性調査と当該調査結果に基づく対策を講じる必要があり、脆弱性調査の効果を高める観点から所要の法制度の整備についても併せて検討する必要があるとされた。

ウ　被害拡大を防止するための取組に関する検討

「IoT セキュリティ総合対策」では、イで述べた機器の脆弱性調査の実施に加え、脆

---

[1] 総務省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」２頁 <http://www.soumu.go.jp/main_content/000534017.pdf>（以下、ＵＲＬの最終アクセスの日付けはいずれも平成 30 年６月 15 日。）

[2] Distributed Denial of Service attack。分散サービス拒否攻撃。Web サーバやメールサーバ等に対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能にする。第三者のコンピュータをボット（IoT 機器を外部から遠隔操作するための不正プログラム）に感染させておくなどして、攻撃者の指示によって複数のコンピュータから一斉に攻撃する例もある。

[3] 総務省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」３頁 <http://www.soumu.go.jp/main_content/000534017.pdf>

[4] 総務省ホームページ<http://www.soumu.go.jp/main_content/000510701.pdf>

弱性を有するIoT機器がサイバー攻撃の踏み台となったことが確認された場合に、被害拡大を防止するため、インターネット・サービス・プロバイダによって、当該IoT機器と乗っ取られたコンピュータ群に指令を送るＣ＆Ｃサーバとの通信を遮断する等の取組を検討する必要性が挙げられ、平成29年10月に設置された総務省「円滑なインターネット利用環境の確保に関する検討会」において検討が行われ、平成30年２月に「対応の方向性」が取りまとめられた。

「対応の方向性」では、踏み台とされている機器が接続している通信ネットワークを管理する事業者の調査や、DDoS攻撃等に関する通信等に係る情報の集積・分析等のための情報共有の結節点として第三者機関の必要性が示された。また、通信の秘密に該当する情報を取り扱うことが予定されていることに鑑み、当該第三者機関を法律上位置付ける必要があるとされた。

（２）固定電話網のＩＰ網への移行に向けた議論と法改正の必要性

ア　ＮＴＴ東西のＰＳＴＮの現状とＩＰ網への移行

ＮＴＴ東日本・西日本は一般の加入電話回線ネットワークであるＰＳＴＮ（Public Switched Telephone Networks：公衆交換電話網）を提供している。ＮＴＴ東日本・西日本の加入固定電話は、利用者宅等から電話線をメタルケーブル等で経由してＮＴＴ東日本・西日本の電話局にある交換機までつなぎ、交換機と相手の電話局内の交換機がやり取りすることで通話を成立させている（この仕組みを用いた従来の固定電話を以下「メタル電話」という。）。

近年では、中継交換機やメタルケーブルを用いずインターネットの仕組みを用いて音声をやり取りするＩＰ電話への移行や携帯電話の普及により、メタル電話は年々ユーザー数が減少している。そして、世界的にＩＰ化が進展する中で、電話のみに使われる交換機の製造をメーカーは停止しており、現在使われている交換機は2025年頃に設備維持の限界を迎えると予想されている。

こうした状況を踏まえ、平成22年11月、ＮＴＴ東日本・西日本は2020年頃から、ＰＳＴＮからＩＰ網への移行を開始し、2025年頃に移行を完了する考え方を公表した[5]。この中では、銀行ＡＴＭや電子商取引等に利用されているＩＮＳネット（ディジタル通信モード）等利用の減少が見込まれるサービスについて、提供を終了する考えを示した。

平成27年11月、ＮＴＴは「「固定電話」の今後について」[6]を公表した。この中では、現在利用されているメタル電話については、ＩＰ網へ移行後も基本的な通話等の音声サービスは利用可能とする一方 、ＰＳＴＮ特有の機能である優先接続機能（事業者識別番号をダイヤルしなくとも中継事業者を選択できる機能。マイライン。）等について、ＩＰ網移行後は具備しないこととしている。

また、事業者等を変更しても電話番号を継続して利用できる「番号ポータビリティ」

---

[5] 東日本電信電話株式会社・西日本電信電話株式会社「ＰＳＴＮのマイグレーションについて～概括的展望～（2010年11月２日）」<https://www.ntt-east.co.jp/release/detail/pdf/20101102_01_01.pdf>

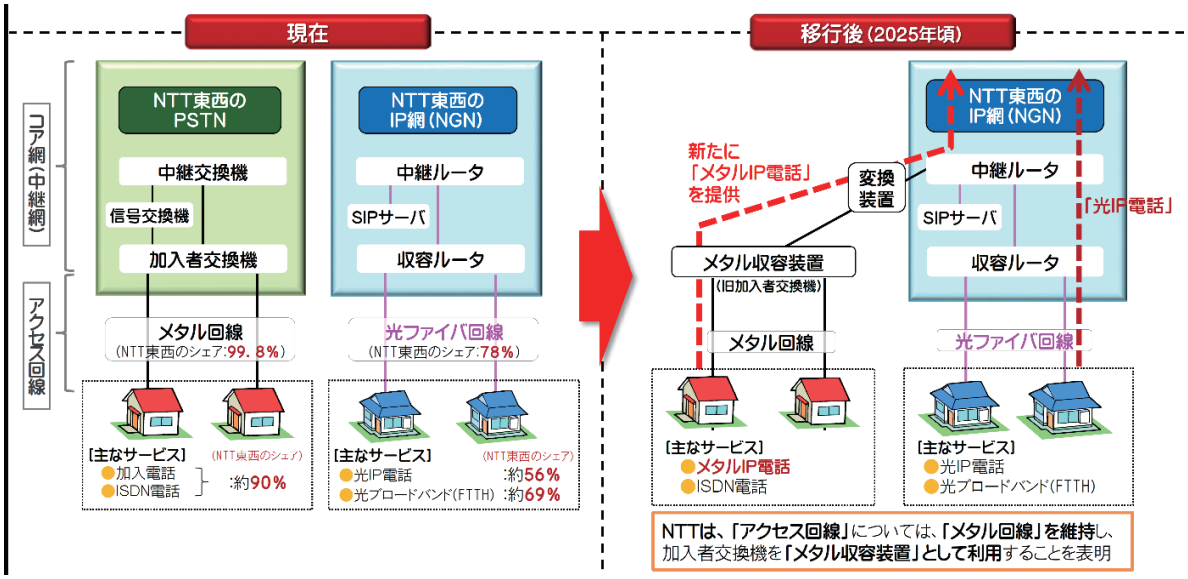
[6] ＮＴＴホームページ<http://www.ntt.co.jp/news2015/1511jwbw/xddh151106d_01.html>

について、現在の固定電話では、ＮＴＴ東日本・西日本のメタル電話の新規契約時に取得した番号のみ持ち運ぶことのできる「片方向番号ポータビリティ」であるが、ＩＰ網移行後は、「ＮＴＴ東日本・西日本と他の事業者間」及び「ＮＴＴ東日本・西日本以外の事業者間」で番号を持ち運ぶことのできる「双方向番号ポータビリティ」を実現する考えを示した。

平成 28 年２月、総務大臣は情報通信審議会に固定電話網の円滑な移行の在り方について諮問を行った。諮問を受けて情報通信審議会電気通信事業政策部会電話網移行円滑化委員会（主査：一橋大学大学院商学研究科　山内弘隆教授）では、事業者等を交え、ＰＳＴＮのＩＰ網への移行工程・スケジュール、ＩＰ網への移行に向けた電話番号の管理の在り方等について議論が行われ、平成 29 年３月に移行後のＩＰ網のあるべき姿を示す一次答申[7]が、同年９月に円滑な移行の在り方を示した二次答申[8]が示された。

スケジュールに関しては、2021 年初頭に事業者間でＩＰ接続を開始し（ＩＰ－ＩＰ接続）、2024 年初頭に従来のメタル電話からメタル回線を用いたＩＰ電話（メタルＩＰ電話）へのサービス移行（契約切替え）、2025 年初頭に移行完了と整理された。

図表１　移行のイメージ



（出所）総務省資料より抜粋

イ　総務省情報通信審議会における議論の詳細

（ア）電気通信番号の管理の仕組みに関する検討

これまで音声通話を疎通させる番号管理の機能はＮＴＴ東日本・西日本の交換機が担ってきたため、2021 年から開始されるＩＰ－ＩＰ接続に向け、新しい番号管理の方法が議論された。二次答申では、①ＩＰ－ＩＰ接続に対応した番号管理の実効性・継続性

[7] 総務省ホームページ<http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000216.html>
[8] 総務省ホームページ<http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000230.html>

の確保、②番号の移転に係る適正な管理の確保、③番号資源[9]の公平かつ効率的な利用の確保の３つの観点から課題が整理され、次の点についての制度的対応が必要であるとされた。

> ①　ＩＰ－ＩＰ接続に対応した番号管理の実効性・継続性を確保するため、電気通信番号を利用する事業者についての
> ・　ＥＮＵＭ方式[10]に対応した「番号解決」及び番号移転に対応した「発番管理」の実施義務
> ・　事業の休廃止又は譲渡等の場合における円滑な地位の「承継」を可能とする仕組み[11]
> ②　卸電気通信役務により番号利用事業者が発番事業者と異なる場合に、卸先事業者における番号制度上の義務の履行の徹底を図るよう電気通信番号の適正な管理を確保するための仕組み
> ③　電気通信番号を利用するサービスの継続性に配慮しつつ、指定された電気通信番号の公平かつ効率的な利用を図るための
> ・　電気通信番号の利用状況や電気通信番号に係る義務の履行状況を一定期間ごとに確認する仕組み
> ・　電気通信番号が一定期間利用されていない場合や電気通信番号に係る義務が履行されていない場合は番号利用に関する取消し等の処分を可能とする仕組み等

そして、これらの制度的な対応は、事業者に対して新たな義務を課し、又はその権利を制限する内容が含まれることとなるため、電気通信事業法（昭和 59 年法律第 86 号）に規定することも含め、適切な制度設計を総務省において検討することが適当であるとされた。

（イ）電気通信業務の休廃止に係る情報の整理・公表

先述のとおり、ＮＴＴ東日本・西日本は、ＩＰ網への移行に伴い、ＩＰ網での提供が困難なサービスや利用減少が見込まれるサービスについて、提供を終了する考えを示した。情報通信審議会の議論の中では、これらのサービスの中には現時点で一定規模の利用者が存在しているものや国民生活に広く利用されているものがあるため、サービス終了時期の早期公表や周知の在り方等の利用者保護の確保が課題となった。

一次答申・二次答申では、他の事業者によって十分に提供されないような電気通信サービスを終了しようとする場合について、現行の電気通信事業法では、事業の休廃止について一律に事後届出制が適用される規律となっている[12]こと等を踏まえ、利用者利益の保護の必要性が高いと考えられるサービスに関し、その廃止・移行に係る取組（例えば、

---

[9] 電気通信番号の指定・使用状況は、指定率については携帯電話・ＰＨＳ（070/080/090 番号）が約 90%、10 桁の着信課金（0120 番号）が約 99%と逼迫しているが、実際の使用率は、携帯電話・ＰＨＳが約 70%、10 桁の着信課金が約 55%となっている（平成 29 年３月末時点、二次答申（前掲注８）64 頁）。

[10] E.164 Number Mapping 方式の略。インターネットのＩＰアドレス問合せの技術を応用して、番号に対応する接続先の情報を取得するための標準規格。

[11] 現在は、発番事業者が引き継ぎたい電気通信番号の指定に係る廃止の届出を行うとともに、他の事業者が当該電気通信番号の指定を受けるための申請を行うことによって、総務大臣が同じ電気通信番号を指定するといった運用上の対応を行っている（二次答申（前掲注８）12 頁）。

[12] 電気通信事業法第 18 条第１項

契約切替えに係る周知・案内、メタルＩＰ電話の料金・提供条件の確定、代替サービスに係る情報提供等）をあらかじめ行政が確認し、整理・公表するためのルールの導入について、電気通信事業法に規定することも含め、適切な制度設計を総務省において検討することが必要とされた。

以上のような経緯の下、政府は、平成 30 年３月６日に「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」（閣法第 33 号）を閣議決定し、国会に提出した。

同法律案は、衆議院においては、同年４月 12 日に附帯決議を付して総務委員会で、同月 17 日に本会議でそれぞれ賛成多数で可決された。参議院においては、４月 19 日に総務委員会においてＮＴＴ霞ヶ関ビルに法律案審査のための視察が行われ、５月 15 日に総務委員会、同月 16 日に本会議でそれぞれ賛成多数で可決された。

３．本法の概要

（１）IoT 機器等に対するサイバー攻撃等への対処

ア　第三者機関を中心とした情報共有

改正後の電気通信事業法では、サイバー攻撃を行うマルウエア感染機器やそれらに指令を出すサーバへの対処を促進するため、電気通信事業者が必要な情報共有を行うに当たり中心となる第三者機関（認定送信型対電気通信設備サイバー攻撃対処協会）を総務大臣が認定することとしている。認定送信型対電気通信設備サイバー攻撃対処協会は電気通信事業者が設立した一般社団法人であり、その業務はおおむね次のとおりである[13]。

① 会員である電気通信事業者の委託を受けて、その事業者の電気通信設備等が送信型対電気通信設備サイバー攻撃[14]の送信先であることが特定され、（その業務上記録している通信履歴の電磁的記録により）当該送信型対電気通信設備サイバー攻撃の送信元の電気通信設備が特定されたとき、当該他の電気通信事業者に対し、当該通信履歴の電磁的記録を証拠として当該電気通信設備を送信元とする送信型対電気通信設備サイバー攻撃又はそのおそれへの対処を求める通知を行う。

② 会員である電気通信事業者の電気通信設備等が送信型対電気通信設備サイバー攻撃の送信先であることが特定され、（その業務上記録している通信履歴の電磁的記録により）当該送信型対電気通信設備サイバー攻撃の送信元の電気通信設備が合理的に特定できないとき、当該事業者から通信履歴の電磁的記録の提供を受け、送信型対電気通信設備サイバー攻撃の送信元の電気通信設備を合理的に特定するための調査及び研究を行うとともに、その成果の普及を行う。

③ このほか、送信型対電気通信設備サイバー攻撃に対処する電気通信事業者を支援す

---

[13] 改正後の電気通信事業法第 116 条の２第２項

[14] 情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち、送信先の電気通信設備の機能に障害を与える電気通信の送信（当該電気通信の送信を行う指令を与える電気通信の送信を含む。）により行われるもの（改正後の電気通信事業法第 116 条の２第１項第１号）。

る。

①の通知と②で取り扱う通信履歴の電磁的記録は、電気通信事業者の取扱中に係る通信とみなし、検閲の禁止と通信の秘密の保護の規定[15]を適用し、これらの業務に従事する者は電気通信事業に従事する者とみなして秘密保持義務の規定[16]を適用することとしている[17]。

イ　ＮＩＣＴによる機器の脆弱性調査

国立研究開発法人情報通信研究機構（ＮＩＣＴ：National Institute of Information and Communications Technology）は、国立研究開発法人情報通信研究機構法（平成11年法律第162号）を設置根拠とし、「情報の電磁的流通及び電波の利用に関する技術の研究及び開発、高度通信・放送研究開発を行う者に対する支援、通信・放送事業分野に属する事業の振興等」を総合的に行う[18]情報通信分野における公的研究機関である（総務省所管）。サイバーセキュリティ関係では、コンピュータネットワーク上で発生する様々な情報セキュリティ上の脅威を可視化して把握し、対策を導出するためのシステム等の技術研究や公開を行っている[19]。

改正後の国立研究開発法人情報通信研究機構法では、業務の特例として、平成36年３月31日までの５年間、次の業務を行うこととされている[20]。

①　特定アクセス行為（後述）を行い、通信履歴等の電磁的記録を作成すること。

②　特定アクセス行為に係る電気通信の送信先の電気通信設備が電気通信事業者若しくは電気通信事業者の利用者であるときは、当該電気通信事業者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと[21]。

③　①、②に附帯する業務

「特定アクセス行為」は、ＮＩＣＴの端末設備等を送信元とし、（アクセス制御機能を有する特定電子計算機である）電気通信設備等を送信先とする電気通信の送信を行う行為であって、当該電気通信設備に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号[22]（不正アクセス行為から防御するために必要な基準として総務省令で定める基準を満たさないものに限る。）を入力して当該電気通信設備等を作動させ、当該ア

---

15 電気通信事業法第３条、第４条

16 電気通信事業法第４条第２項

17 改正後の電気通信事業法第164条第４項、第５項

18 国立研究開発法人情報通信研究機構法第４条参照

19 平成28年常会では国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律（平成28年法律第32号）が成立し、ＮＩＣＴの業務に、その研究等の成果の普及として行うサイバーセキュリティに関する演習その他の訓練等の業務が加えられた。これを受けて、従来総務省が主催していた実践的サイバー防御演習（ＣＹＤＥＲ：CYber Defense Exercise with Recurrence）を平成28年度より規模を拡大してＮＩＣＴが主催している。

20 改正後の国立研究開発法人情報通信研究機構法附則第８条第２項

21 電気通信事業者への通知業務は、認定送信型対電気通信設備サイバー攻撃対処協会に委託することができる（改正後の国立研究開発法人情報通信研究機構法附則第８条第３項）。

22 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第２条に規定する識別符号であり、ＩＤとパスワード等を指す。

クセス制御機能により制限されている特定利用をし得る状態にさせる行為とされている[23]。

ＮＩＣＴが①～③の業務を行う場合には、特定アクセス行為は不正アクセス行為の禁止等に関する法律第２条第４項第１号に規定される不正アクセス行為から除外される[24]。

（２）電気通信番号の管理の仕組みと電気通信業務の休廃止に係る情報の整理・公表

ア　電気通信番号計画及び電気通信番号使用計画

従前、電気通信番号については改正前の電気通信事業法第 50 条第１項の規定に基づき、総務省令である電気通信番号規則によって基準が定められてきた。

改正後の電気通信事業法では、総務大臣が番号ごとの使用条件や指定可能な番号数等を記載した「電気通信番号計画」を作成・公表することとされた[25]。番号を使用する電気通信事業者は、電気通信番号計画に記載された使用条件の遵守や使用を希望する番号数等を記載した「電気通信番号使用計画」を作成し、総務大臣の認定を受け、番号の指定を受けることとなる[26]。

電気通信事業者の電気通信番号の使用がこの認定を受けた電気通信番号使用計画に適合していないと認めるときは、総務大臣は当該事業者に番号の使用等に関する是正命令を行うことができ、事業者がこの命令に違反したとき等には認定を取り消すことができることとされている[27]。

イ　電気通信業務の休廃止に係る情報の整理及び公表の制度

電気通信事業者は電気通信事業の一部又は全部を休廃止しようとするときは利用者に対してその旨を周知し[28]、休廃止した際には遅滞なくその旨を総務大臣に届け出る[29]こととされている。

改正後の電気通信事業法ではこれに加え、利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務に係る電気通信業務の休廃止については、あらかじめ総務大臣に届け出なければならず[30]、総務大臣はこの届出に関して作成・取得した情報等を整理し、これをインターネット等により公表する[31]ものとされた。

また、第一種・第二種指定電気通信設備[32]を設置する事業者が、他の事業者に貸し出し

---

23 改正後の国立研究開発法人情報通信研究機構法附則第８条第４項第１号
24 改正後の国立研究開発法人情報通信研究機構法附則第８条第７項
25 改正後の電気通信事業法第 50 条第２項
26 改正後の電気通信事業法第 50 条の２第１項
27 改正後の電気通信事業法第 50 条の９第４号、第 51 条
28 電気通信事業法第 18 条第３項、改正後は第 26 条の４第１項
29 電気通信事業法第 18 条第１項
30 改正後の電気通信事業法第 26 条の４第２項
31 改正後の電気通信事業法第 26 条の５
32 電気通信事業法第 33 条、第 34 条は第一種指定電気通信設備（都道府県ごとに 50％超のシェアを占める加入者回線を有する電気通信事業者が設置する電気通信設備のうち、総務大臣が指定したもの）、第二種指定電気通信設備（業務区域ごとに 10％超の端末シェアを占める伝送路設備を有する電気通信事業者が設置する電気通信設備のうち、総務大臣が指定したもの）を設置する事業者について接続約款に関して総務大臣の認定を受けなければならないこと等を定めている。平成 30 年６月現在、第一種指定電気通信設備を設置する事業者はＮＴＴ東日本・西日本、第二種指定電気通信設備を設置する事業者はＮＴＴドコモ、ＫＤＤＩ、ソフトバンク、沖縄セルラーである。

ている設備の機能を休廃止しようとするときは、あらかじめ、当該機能を利用する事業者に対し、その旨を周知させなければならないこととした[33]。

４．主要な国会論議

（１）第三者機関を中心としたサイバー攻撃の情報共有の意義と実効性

ア　第三者機関を中心としたサイバー攻撃の情報共有の意義

本法では、総務大臣がサイバー攻撃の送信元の情報を通信事業者間で共有する業務を行う第三者機関を認定する仕組みを設けており、その意義が問われた。

これに対し政府参考人から、「送信元の情報共有等は、サイバー攻撃の対処のために有用でございますが、多数の電気通信事業者が関係し、情報共有を行うことが煩瑣となるため取組が進んでいない」ため、「情報共有を行う第三者機関を総務大臣が認定する制度を設けまして、サイバー攻撃の送信元に関する情報の効率的な共有を促すことにより、電気通信事業者が連携してサイバー攻撃に円滑に対応することを促進していく」旨の答弁があった[34]。

イ　第三者機関として念頭に置かれている法人と信頼性・公平性

本法で第三者機関の要件として一般社団法人であることを求めている[35]理由と特定の法人を認定することを念頭に置いているかという点について問われた。これに対しては、政府参考人から、「通信の秘密に該当する情報の取扱いにつきましては、原則として利用者からの同意の取得が必要であり、本法律の情報共有におきましては、電気通信事業者に対して、利用者との契約などにおきまして、利用者からの同意を取得することを求めて」おり[36]、「一般社団法人におきましては、これを社員であります電気通信事業者の遵守する要件として定款で定めることにより担保することが可能であるということから、情報共有を行う第三者機関は一般社団法人を対象」とした旨答弁があった。また、現時点ではＩＣＴ分野のサイバーセキュリティに関する情報収集、調査、分析等の活動を実施している一般社団法人ＩＣＴ－ＩＳＡＣを念頭においているが、「第三者機関の認定に関しましては、特定の法人に限られるものではなく、要件を満たす一般社団法人から申請等があれば対応していきたい」と述べている[37]。

第三者機関の信頼性と公平性については、政府参考人は、「総務大臣の認定に際しまして、業務を適正かつ確実に行うのに必要な要件といたしまして、まず一点目としましては、サイバー攻撃に関する知識、能力を有すること、それから二点目としましては、業務運営に必要な財政的基礎を有すること、さらに、業務を円滑に行うための業務の実施の方法が定められていることを確認することで確保」する旨説明している。また、「第三者機関の業務運営が不適切であると認める場合に関しましては、総務大臣は、立入検査のほか業務の改善や業務の全部又は一部の停止を命じることが可能」であると述べてい

---

[33] 改正後の電気通信事業法第 33 条の２、第 34 条の２
[34] 第 196 回国会参議院総務委員会会議録第８号 19 頁（平 30.5.15）
[35] 改正後の電気通信事業法第 116 条の２第１項
[36] 改正後の電気通信事業法第 116 条の２第２項
[37] 第 196 回国会衆議院総務委員会議録第９号 18 頁（平 30.4.12）

る[38]。

ウ　情報共有への参加促進

サイバー攻撃への対処を網羅的に行うため、情報共有への電気通信事業者の参加促進にどのような措置を講じるか問われた。これに対し、政府参考人より、「情報共有の枠組みには幅広い通信事業者の方に参加いただくことが重要」であり、総務省としては「更に情報共有の重要性を説明し、より幅広い電気通信事業者の方の参加を促していきたい」旨の答弁がなされた。また、「サイバー攻撃の対処におきましては、通信事業者以外のセキュリティーベンダー、製造事業者等とも連携していくことが重要」であり、「具体的には、マルウエア、機器の脆弱性に関わる情報につきまして、第三者機関の業務として利用者への注意喚起を適切に行っていくといった業務のためにも、セキュリティーベンダーからサイバー攻撃を行うマルウエアに関する情報の提供ですとか、製造業者からはマルウエアに感染しやすい機器の情報、こういった情報の提供を受けることが必要」と述べている[39]。

エ　通信の秘密と網羅的なセキュリティの関係性

第三者機関が通信の秘密を扱うこととなる点について、政府参考人は「第三者機関が取り扱う情報につきましては、通信の秘密に該当するところ、通信の秘密に該当する情報の提供は原則として同意が必要」と考えており、「本法律案におきましては、電気通信事業者に対して、利用者との契約などで情報共有につきまして情報提供先も含めて利用者の同意を取得することを求めて」おり、「当該同意の範囲を超えて第三者機関が情報の提供を行った場合は、情報共有の業務を行う者の守秘義務違反及び通信の秘密の侵害に該当することと」なる旨説明している[40]。

また、ＩＣＴ－ＩＳＡＣを構成しているのは電気通信事業者だけではないが、第三者機関として仮にＩＣＴ－ＩＳＡＣが認定された場合、電気通信事業者以外の者が通信の秘密に当たる情報に触れることになるのか指摘があり、政府参考人から、「ＩＣＴ－ＩＳＡＣ全体ということではなくて、今回の第三者機関が取り扱う情報に関する電気通信事業者の方々に限定した形で運用を図るということを想定している」と答弁があった[41]。

総務省は、上述のとおり通信の秘密に該当する情報の取扱いについては、原則として利用者からの同意の取得が必要と答弁しているが、この原則の例外が問われ、政府参考人は「通信当事者の同意がない場合であっても、法令行為、正当業務行為、正当防衛又は緊急避難に該当する場合は違法性が阻却される」という考えを示した。また、正当業務行為については「電気通信事業者が電気通信役務の提供等の業務を行うために必要であって、目的の正当性、行為の必要性等を満たす行為」であり、「具体的には、料金請求のために通話時間を確認したりとか宛先を確認したりルーティングをする場合」等が当たると述べている[42]。

---

[38] 第196回国会参議院総務委員会会議録第８号22頁（平30.5.15）
[39] 第196回国会参議院総務委員会会議録第８号19頁（平30.5.15）
[40] 第196回国会参議院総務委員会会議録第８号12頁（平30.5.15）
[41] 第196回国会参議院総務委員会会議録第８号13頁（平30.5.15）
[42] 第196回国会参議院総務委員会会議録第８号６頁（平30.5.15）

これに対し、通信の秘密に該当する情報の取扱いについてユーザーの同意が取得できない場合等が、サイバー攻撃に対する防御の穴になると考えられる旨の指摘があり、政府参考人は、利用者の同意の取り方に関して、「個別での同意というのが原則でございますが、例えば包括的なものでの同意ですとか、そこら辺の約款的なものを作って関係事業者との関係でそういったものを進めていくとか、いろいろな施策」もあり、「サイバーアタックの状況等を踏まえながら、円滑にこういったものに対してどう対応できるかと、電気通信事業者の意見も聞きながら具体的な対応策」を考えていく旨答弁している[43]。

（２）ＮＩＣＴによるIoT機器の脆弱性調査とセキュリティ対策強化のための人材等確保

ア　脆弱性調査の主体、対象

IoT 機器の脆弱性調査を行う主体をＮＩＣＴとした理由が問われた。これに対し、政府参考人から、「ＮＩＣＴはサイバー攻撃の観測を行うなどサイバーセキュリティー分野に深い知見を有しているということ、また、本調査におきましてはインターネット上でパスワード設定に不備のある機器の特定を行うことから、その調査主体は国民の信頼を得られるものとする必要があること、こういった理由から今回ＮＩＣＴに行わせることとした」旨説明があった[44]。

調査の対象となるIoT機器については、「具体的には、ウエブカメラ、ルーター、センサー」等が想定されるとしている[45]。

ＮＩＣＴが取得する情報については、総務省より「直ちに個人情報というわけではございませんけれども、当然、ＮＩＣＴ法に基づく秘密保持義務、あるいは実際にこの業務をＮＩＣＴが行う場合の実施計画を総務大臣が認可を行うこととしておりますので、その過程で適切な管理がなされるよう、私どもとしても最大限の留意をしてまいりたい」という説明があった[46]。

なお、当該調査は５年間の時限措置とされているが、この理由として、「過去に実施したパソコンのマルウエア感染駆除の取組（中略）サイバークリーンセンターという取組でございますけれども、平成18年度から22年度まで実施しましたこの５年間で、マルウエアの感染率が２％から0.6％に減少したという実績が出ており（中略）、５年間程度の実施期間で一定の成果を得ることができる」という考えを示している。加えて、「改正法の施行後３年後に、施行の状況に関する検討を行うこととしており[47]（中略）この取組の進捗状況や、また目まぐるしく変わってまいりますサイバー攻撃の態様、こうしたものの変化を踏まえて、業務の実施期間あるいは行うべき業務」等について検討を行う旨説明があった[48]。

---

43 第196回国会参議院総務委員会会議録第８号７頁（平30.5.15）
44 第196回国会参議院総務委員会会議録第８号19頁（平30.5.15）
45 第196回国会衆議院総務委員会議録第９号16頁（平30.4.12）
46 第196回国会参議院総務委員会会議録第８号17頁（平30.5.15）
47 附則第６条
48 第196回国会衆議院総務委員会議録第９号19頁（平30.4.12）

イ　調査等についての国民への周知

この調査について、国家機関による国民生活への介入といった国民の不安をどのように解消していくかが問われた。政府参考人からは、総務省において、「ＮＩＣＴ、電気通信事業者、あるいは消費者庁などの関係機関と協力をしながら、ユーザーの皆様に対しまして、IoT 機器のパスワード設定を適切なものにすることについて啓発活動をまず行うとともに、ＮＩＣＴがパスワード設定に不備のある機器の調査を行い、該当するユーザーには電気通信事業者から注意喚起を行うことについて積極的な周知活動を行う」旨の答弁があった。また、「ユーザーへの丁寧な対応を行うとともに、この取組の実効性を確保する観点から、サポートセンターを新たに設置をいたしまして、パスワードの設定変更の方法が分からないユーザーの皆様に対しても電話などによる御案内を差し上げる」旨説明している[49]。また、「サポートセンターの設置につきましては、啓発活動あるいは周知活動も含めまして、平成 30 年度予算の IoT セキュリティ総合対策の推進、これ約６億円[50]でございますけれども、この一部を用いて措置をする予定」と答弁があった[51]。

ウ　IoT 機器自体のセキュリティ向上の必要性

認証手段等 IoT 機器自体のセキュリティを高める必要性が問われた。これに対し、政府参考人からは、「これから製造、販売されるものにつきましては、（中略）設計・製造段階からセキュリティー対策を講じていく、また一定のセキュリティー要件を講じているものについては認証制度を適用する、こういったことを含めて考えてまいりたいと思っておりますけれども、既に設置されている IoT 機器につきましてはこういったことが難しいことから」、ＮＩＣＴによる脆弱性調査を行うこととした旨答弁があった[52]。さらに、外部から IoT 機器にアクセスする際などに必要となる認証について、「例えばパスワードの代わりに生体認証などを用いる規格の標準化が民間で進められているなど、よりセキュアな認証方式の導入あるいは活用ということが期待されるところでございまして、引き続き」総務省としてもこうした認証関連の動向についても注視していく旨述べている[53]。

エ　サイバーセキュリティ対策強化のための人材確保・体制強化

サイバーセキュリティ分野の人材確保と予算等のＮＩＣＴの体制強化について問われた。野田総務大臣は、「これまでＮＩＣＴにおいては、その有する技術的知見等を生かしてサイバーセキュリティー分野の研究開発や人材育成（中略）具体的にはサイバー攻撃の状況をリアルタイムに把握して分析するシステム、nicter と言っていますが、の開発を始めとする研究開発に取り組んでいるほか、国の行政機関、地方公共団体、重要インフラ事業者等に対する実践的なサイバー防御演習、ＣＹＤＥＲ等のセキュリティー人材の育成を行っており、これからも本法案によって新たに追加される IoT 機器の調査の業務を含め、更に取組の強化を行うこととして」おり、「総務省としては、サイバーセキュ

---

[49] 第 196 回国会参議院総務委員会会議録第８号２頁（平 30.5.15）
[50] 平成 30 年度総務省所管予算の概要８頁<http://www.soumu.go.jp/main_content/000542301.pdf>
[51] 第 196 回国会参議院総務委員会会議録第８号３頁（平 30.5.15）
[52] 第 196 回国会参議院総務委員会会議録第８号 17 頁（平 30.5.15）
[53] 第 196 回国会参議院総務委員会会議録第８号 21 頁（平 30.5.15）

リティー上の脅威に対抗するため、ＮＩＣＴにおける先進的な研究の成果を最大限に活用していく（中略）ために必要な予算の確保に」努めると答弁している[54]。そして、2020年の東京オリンピック・パラリンピック等に向け、「内閣サイバーセキュリティセンター始め関係府省と連携しつつ、（中略）１日も早く政府一丸となってこのことについては対応していかなければならない」と述べている[55]。

（３）固定電話網のＩＰ網への移行に向けた番号管理・サービス休廃止に関する課題

ア　電気通信番号の指定数と使用数の乖離の原因

電気通信番号の指定数と使用数の乖離が生ずる原因は何か問われた。これに対し、政府参考人から、現在の電気通信番号の指定について、事業者が総務省に申請する際に今後のサービス展開等を見込んで、中長期に必要となる番号の数を算出し、総務省に需要数を提出しており、総務省はそれらの状況等を確認した上で番号があれば指定してきたと説明があった。そして、「事業者のサービスの普及が当初の予定どおり進まないような場合には、国が指定した番号数と実際に使用されている番号数に乖離が生じ（中略）、また、現行制度では、事業者が国から受けた番号に関しましては使用期限がないということから、使用しなくなった番号の返上は事業者が任意で行うということから、現在、長期間未使用となっている番号が」あり、再配分のために本法律案を国会に提出したと答弁している[56]。

イ　ＩＰ網移行後の番号管理に係る事業者の負担軽減

ＩＰ網へ移行後の固定電話の双方向番号ポータビリティ実現には番号管理の仕組みの構築が必要とされているが、中小企業においても対応が可能となるよう配慮すべきではないか問われた。政府参考人からは、「情報処理技術の進展、ＩＰ網移行に伴う汎用的な機器の導入などにより、ＮＴＴの交換機による現在の仕組みに比べましてコストを大幅に低廉化する見通しが得られて」おり、情報通信審議会の答申では、「規模の大きくない事業者につきましては大手の事業者が構築する番号データベースを借りることも可能とするような提言」があった旨答弁があった[57]。

ウ　電気通信サービスの休廃止の事前届出の具体的範囲等

電気通信サービスの休廃止の総務大臣への事前届出について、改正後の電気通信事業法では実際の運用はほぼ省令に委任されているが、事前届出となる役務の範囲や代替サービス・周知方法を過度に厳格化すると新しいサービスの導入や開発が萎縮するのではないかという指摘があった。これに対し、政府参考人から、「事前届出制の対象とするサービスにつきましては、情報通信審議会の答申の趣旨に従いまして、利用者保護、それから事業者負担のバランスを考慮して、代替サービスの提供状況や利用者の範囲等を踏まえ、利用者の利益に及ぼす影響が大きいサービス、例えば、ＮＴＴ東西のＩＳＤＮ

---

[54] 第196回国会参議院総務委員会会議録第８号20頁（平30.5.15）
[55] 第196回国会参議院総務委員会会議録第８号15頁（平30.5.15）
[56] 第196回国会参議院総務委員会会議録第８号17頁（平30.5.15）
[57] 第196回国会参議院総務委員会会議録第８号20頁（平30.5.15）

サービスですとか固定電話サービス、こういったものに限る」という考えが示された。そして、「今後、事前届出制の対象とするサービスの具体的範囲、利用者への周知方法等に関しましては、（中略）審議会への諮問を経て」総務省令で定める予定であるが、「過度な負担を課すことなく、適切に利用者保護を図るものになるよう検討を進めてまいりたい」と答弁があった[58]。

エ　ＩＰ網移行後のサービスに関する課題

ＩＰ網移行後、緊急通報における回線保留機能（通報者が受話器を下ろしても指令台側が切断しない限り接続状態を維持する機能）が廃止されることについて政府としての考えが問われ、野田総務大臣より、「総務省としては、改正法に基づいて電気通信番号計画などで回線保留機能を代替する機能の具備を事業者に求めることを定めることによって、事業者による確実な対応を」図り、「今後も総務省の審議会等において警察、消防やＮＴＴによる取組の状況を継続的に確認して、取組内容が不十分な場合には改善を求めるなど適切に対応して」いく旨答弁があった[59]。

ＩＰ網移行後も既存のメタルケーブルを用いて現在の電話機を利用できるメタルＩＰ電話（図表１参照）について、いつまで提供されるのか、将来廃止された際に音声サービスのみを望む利用者に代替サービスは提供されるか問われた。政府参考人は、メタルＩＰ電話終了時期は決まっておらず、「音声のみサービスを望む利用者のニーズも踏まえながら検討が行われることは必要というふうに考えている」と答弁している[60]。

（４）省令への委任事項

改正後の電気通信事業法第 176 条の２は、「この法律に定めるもののほか、この法律を実施するため必要な事項は、総務省令で定める。」としており、この規定の趣旨及びこの規定に基づく省令規定事項として想定されている内容、このような包括的な委任規定の是非が問われた。

これに対し野田総務大臣は、「電気通信事業法の改正案では、電気通信番号計画の申請手続など多くの手続を設けており（中略）、個別の規定で総務省令への委任を定めているほかにも、必要な手続の様式などを定めることが見込まれることから、その根拠を明らかにするため（中略）、第 176 条の２を」設けた旨説明している。そして、「この規定では、法律の実施に必要な事項に限り委任することとしており、この規定に基づいて実質的に権利を制限し、義務を課す総務省令を定めることはありません。なお、本法律案では法律で定められる内容は条文で定めており、（中略）通信の秘密に直接関連する事項については総務省令の委任は行っておりません」と答弁している[61]。

---

58 第 196 回国会衆議院総務委員会議録第９号３頁（平 30.4.12）
59 第 196 回国会参議院総務委員会会議録第８号 11 頁（平 30.5.15）
60 第 196 回国会参議院総務委員会会議録第８号 12 頁（平 30.5.15）
61 第 196 回国会参議院総務委員会会議録第８号８頁（平 30.5.15）

５．おわりに

本法はこれまで概観してきたとおり、近年増加傾向にあるIoT機器に対するサイバー攻撃や固定電話網のＩＰ網への移行等に対処しようとするものである。

IoT・ＡＩに代表されるように、情報通信をめぐる技術は正に日進月歩で進化しており、社会全体もそれに応じて日々変化を続けている。これに伴い、技術を悪用したサイバー攻撃の態様も目まぐるしく変わっており、2020年東京オリンピック・パラリンピック等に向け、今後もその脅威が増大していくことは確実であろう。

国会論議の中で指摘されたように、政府にはサイバー攻撃の研究や人材確保による体制強化、電気通信事業者のみならず機器の製造事業者等各種事業者との連携の推進等、サイバーセキュリティの確保のため、不断の取組が求められる。

本法には施行後[62]３年を経過した場合の検討条項が置かれているが、電気通信事業者間のサイバー攻撃に関する情報共有や５年間の時限措置とされているＮＩＣＴによるIoT機器の脆弱性調査の効果等本法の施行状況を含め、政府によるサイバーセキュリティ施策を注視してまいりたい。

（ちば　しょうへい）

---

[62] 本法の施行期日は、総務大臣が行う法律の準備行為等については公布の日（平成30年５月23日）、電気通信番号の管理の仕組みや電気通信業務の休廃止に係る利用者保護に関する部分は公布の日から起算して一年を超えない範囲内において政令で定める日、これ以外のサイバー攻撃等への対処に係る部分等は公布の日から起算して九月を超えない範囲内において政令で定める日とされている。