2019

情報通信エンジニア

更新研修テキスト

一般財団法人 日本データ通信協会

目次

第Ⅰ部
ネットワークの技術課題に対する総務省の取り組み

1章 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ついて

1.1 はじめに

第196回通常国会において、平成30年5月16日、「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」（同年法律第24号。以下「本法律」という。）が成立し、同年5月23日に公布された。

本法律は、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、①電気通信事業者によるサイバー攻撃への対処に係る制度の新設、②電気通信番号計画及び電気通信番号計画に係る制度の新設、③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などを行うものである。

今回、この中から、①について概要を紹介する。

1.2 経緯と背景

国民生活及び社会経済活動の基盤となっているインターネットにおいて、近年国内外で大規模なサイバー攻撃が繰り返し行われ、多数のマルウェアに感染した端末によるDDoS攻撃等で大規模な通信障害が発生する事例も生じている。

インターネットにおける通信障害を引き起こすようなサイバー攻撃の脅威の増大に対して次のような対処が有効と考えられる。

- 電気通信事業者による攻撃先への通信の遮断
- マルウェア感染端末の利用者への注意喚起
- マルウェア感染端末とC&C（Command and Control）サーバ等との間の通信の遮断

このような対処を行うためには、マルウェア感染端末やC&Cサーバ等を特定し、それらの管理者が利用している電気通信事業者にマルウェア感染端末やC&Cサーバ等のIPアドレス、ポート番号、タイムスタンプ等（以下「IPアドレス等」という。）の情報を提供することが必要となる。しかし、DDoS攻撃等の送信元は多数の電気通信事業者に分散するため、個々の電気通信事業者が個別に情報提供を行うことは非常に困難となることが想定される。また、IPアドレス等の情報は通信の秘密に該当することから慎重な取扱いが必要とされる。

こうした状況を受けて、インターネットの円滑な利用環境を確保するための方策を検討するため、総務省では平成29年10月から「円滑なインターネット利用環境の確保に関する検討会」を開催した。同検討会では、通信ネットワークを保護する目的で行

われる情報共有を促進する観点から、情報共有の結節点として適切に情報を取り扱う第三者機関を法律上に位置づけ、第三者機関における通信の秘密を含む情報の収集、分析、共有等の枠組みを明確化する必要があることが提言された。

また、IoT機器を悪用したサイバー攻撃への対処に向けて、政府内においては各省が協調・連携し、官民連携による「ボット撲滅」に向けた体制を構築し、対策を推進することが目指されている。「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。）においては、内閣サイバーセキュリティセンター、警察庁、総務省、経済産業省、民間企業等が協調・連携し、官民連携による「ボット撲滅」に向けた体制を構築し、対策を推進すること、政府内に体制を構築して継続的かつ広範な実態調査ができるよう必要な法的整理を行うこととされた。さらに、総務省において開催するサイバーセキュリティタスクフォースが取りまとめた「IoTセキュリティ総合対策」においては、IoT機器の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検討する必要があることが提言された。

これらを受けて、電気通信事業法（昭和59年法律第86号）及び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）の改正が行われた。

1.3 改正の概要

1.3.1 電気通信事業者間のサイバー攻撃に関する情報共有を促進するための制度整備（電気通信事業法の一部改正）

電気通信事業法の改正では、電気通信事業者間の情報共有及びそれによるサイバー攻撃への対処を促進する観点から、情報共有の結節点となる第三者機関を総務大臣が認定する制度を新たに設けている。

また、電気通信事業者は電気通信役務の提供を業務としており、特にサイバー攻撃により電気通信役務の提供に支障が生じることを防止すべき立場にあることから、様々な形態が存在するサイバー攻撃のうち、電気通信事業者の情報共有の対象として、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（C&Cサーバ等の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を「送信型対電気通信設備サイバー攻撃」と定義している。具体的には、攻撃先の通信設備に負荷をかけることで障害を発生させるDDoS攻撃のほか、自動的に攻撃先の端末をマルウェアに感染させてその機能を停止させるランサムウェアなども含まれる。

さらに、第三者機関として認定を受ける者については、その業務に鑑み、電気通信事業者が設立した一般社団法人であることが求められている。また、送信型対電気通信設備サイバー攻撃の送信元に関する情報提供を行う者は、当該一般社団法人の社員である電気通信事業者であって、その利用者の電気通信設備が送信型対電気通信設備サイバー攻撃を行うことを禁止する旨の技術的条件を定めるとともに、提供条件において情報提供を行うことを定めることが求められている。

第Ⅲ部
情報セキュリティ分野

1章　情報セキュリティ対策

近年における無線ネットワークとクラウド型サービスの普及とともに、今後はパソコンやスマートフォンといった従来のICT端末だけでなく、情報家電、センサーやロボットなどのさまざまなIoT機器が広く社会に浸透していくことが想定される。もはや情報通信ネットワークは日常生活に欠かすことのできない社会基盤といえる。

このような情報通信ネットワークの高度化に伴い、生活の利便性が高まる一方で、政府機関や企業などへの標的型攻撃や、個人のPCに対するさまざまな手口で仕掛けられるコンピュータウイルスは、手口がますます巧妙になり、サイバー攻撃の脅威も増しつつある。情報通信ネットワークを安心して利用するためにも、情報セキュリティについて適切に対策を講じることが不可欠である。

本章では、近年発生が顕著化している攻撃手法とその対策を紹介する。

1.1 セキュリティ脅威の傾向

インターネットサービスの進展やSNS、スマートフォンの普及に伴い、サイバー攻撃などの言葉が飛び交うようになり、情報セキュリティを取り巻く問題や環境が多様化している。近年では、被害がすべてのユーザに一様に降りかかるものではなく、攻撃者の意図や自組織の環境により、攻撃対象を特定した攻撃も増えている。

IPA（独立行政法人情報処理推進機構）は、2017年において社会的影響の大きかった個人向けおよび組織向けのセキュリティ上の脅威をそれぞれ選出している[1]。

上位に選出された脅威の中から、特に注意すべきものを以下にピックアップする。

●インターネットバンキングやクレジットカード情報の不正利用

2016年と同様、個人向けの脅威でトップである。ウイルス感染やフィッシング詐欺により、利用者からインターネットバンキングの認証情報などを窃取し、本人になりすまして不正送金される被害が及んだ。不正送金による被害件数と被害額は2016年より減少したものの、新たに仮想通貨利用者を狙う攻撃が確認された。クレジットカード不正使用の被害額については2016年の2倍近くに増加した。ウイルス感染の対処方法については、1.5節にて紹介する。

●標的型攻撃による情報流出

2016年と同様、組織向けの脅威でトップである。従来から主要な攻撃の1つであるが、企業や官公庁などでの被害が継続して発生している。ソーシャルエンジニアリング（人の行動のミスなどにつけ込む手口）を使った攻撃で、組織内部の情報の窃取を狙っ

たものである。標的型攻撃の攻撃手法や対策については、1.2節にて紹介する。

●ランサムウェアを使った詐欺・恐喝

2016年と同様、個人／組織向けの脅威で2位である。ランサムウェアと呼ばれる悪意あるプログラムによってPC内のファイルが閲覧・編集できない形に勝手に暗号化され、ファイル復元の身代金として、利用者に金銭を要求する攻撃である。2017年はOSの脆弱性を悪用した自己増殖型のランサムウェアの感染が世界的に広がった。ランサムウェアの攻撃手法や対策については、1.3節にて紹介する。

●ビジネスメール詐欺による被害

組織向けの脅威で3位である。ビジネスメール詐欺は、取引先などになりすまして企業の財務担当者や人事担当者などをだまし、攻撃者の用意した口座へ送金させたり、従業員の個人情報などを窃取する詐欺の手口を使った攻撃である。

企業間のビジネスがメールに依存している点を逆手に取った狡猾なだましの手口であり、代表的な手口としては、取引先との請求書の偽装、経営者や社外の権威ある第三者（弁護士など）などへのなりすまし、窃取したメールアカウントの悪用などが確認されている。地組織や取引先のメールアドレスやドメイン名に似せた詐称用のメールアドレスやドメイン名などが使われる場合もあり、受信者は攻撃者からの偽のメールを本物のメールとして取り扱ってしまう。メールは多くのサイバー攻撃の入口でもあることから、メールを確認する際は日頃から注意を払う必要がある。

以上のセキュリティ脅威に加えて、最近、ネットワークカメラやモバイルルータなどのIoT機器を狙ったサイバー攻撃が急増している。IoTの情報セキュリティについては、1.4節にて紹介する。

1.2 標的型攻撃

(1) 概要

標的型攻撃とは、特定の組織をターゲットとして、その取引先や関係者、公的機関などを語ってマルウェア※1や不正なリンクが埋め込まれたメール（標的型攻撃メール）を送信することで、相手をだまし、組織の機密情報を盗むことを目的とする手法である。実在する組織のメールアドレスに偽装したメールアドレスが用いられる場合もあるため、被害者は攻撃や被害に気づきにくい。組織内部に侵入したウイルスは、外部の攻撃者と通信を行いながら、攻撃を加える。

2017年には、攻撃者が情報窃取などの目的を遂行した後、侵入した端末をランサムウェアによって暗号化して使用不能にし、情報窃取の痕跡を発見しづらくするといった事例が国内で確認されている。

(2) 攻撃の手法

標的型攻撃メールの件名や本文の内容は、組織内部の関係者しか知らない情報など