情報セキュリティ白書

Information Security White Paper

2017

広がる利用、見えてきた脅威：つながる社会へ着実な備えを

IPA 独立行政法人情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

序章

2016年度の情報セキュリティの概況

2016 年度に起きた情報セキュリティに関する主なインシデントや実施された政策・制度について概況を述べる。

インシデントについては、標的型攻撃、Web 改ざん等、2015 年度からの攻撃が継続するとともに、ランサムウェアや IoT 機器の脆弱性を悪用した DDoS 攻撃等の新たな脅威により世界規模のインシデントが発生した。

2015 年度に大規模な個人情報流出で注目された標的型攻撃は、国内では旅行会社グループ企業、大学関連施設、一般社団法人日本経済団体連合会（経団連）、地方公共団体等が攻撃され、年間を通じて被害が報告された。

ソフトウェアの脆弱性を悪用した攻撃も多発した。Web サイト構築・運用で広く利用されている WordPress や Apache Struts2 の脆弱性を突いた攻撃の被害が相次いだ。広く普及している Adobe Flash Player の脆弱性や、OpenSSL の既知の脆弱性を狙った攻撃も報告された。脆弱性に対する更なる対策が必要である。

ランサムウェアの被害は日本国内でも急増し、被害報告件数は過去最大となった。ランサムウェアの販売や、ランサムウェアによる攻撃のサポート等を行う Web サイトの存在が明らかになっており、今後も十分な警戒が必要である。

DDoS 攻撃についても国内外で被害が継続した。捕鯨やイルカ漁に対する抗議やリオデジャネイロオリンピック開催への抗議等のハクティビズムによる攻撃に加え、EC サイトへの攻撃によりサービスが停止する等、金銭的被害も報告された。

また、2016 年度の新たな脅威として、IoT 機器の脆弱性を悪用した DDoS 攻撃が注目された。2016 年 9 月、「Mirai」ウイルスが 15 万台以上のネットワークカメラやホームルータ等に感染し、史上最大規模の DDoS 攻撃が発生した。脆弱性を持つ IoT 機器は世界中で放置されている可能性があり、早急な対策が求められる。

更に、国家レベルのサイバー攻撃については、米国政府が 2016 年 12 月、大統領選挙においてサイバー攻撃を含む妨害が行われたと断定し、深刻な事態となった。

2016 年度は国内外で政府・組織が新しい制度に基づく施策を開始した年でもあった。国内では、改正サイバーセキュリティ基本法及びその関連法制等が施行され、独立行政法人・指定法人の監査・監視が強化された。また、セキュリティ人材育成のための新たな資格制度が開始され、2017 年 4 月 1 日に 4,172 名の情報処理安全確保支援士（登録セキスペ）が登録された。更に「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」「サイバーセキュリティ戦略」等に基づく重要インフラセクターの情報共有やサイバー演習が本格化し、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リスク評価も開始された。

IoT のセキュリティについては、政府が本格的な取り組みの方針を表明し、産学官連携の枠組みによりセキュリティガイドラインを整備するとともに、世界的な動向を見すえて、米国や欧州との IoT セキュリティ分野の連携を推進した。

企業においては、「サイバーセキュリティ経営ガイドライン」の普及や、CISO や CSIRT の設置等により、経営層のセキュリティ対策への参画が着実に進展した。2017 年 2 月には中小企業や情報セキュリティの関係団体が、中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言を発表した。今後の取り組みが期待される。

海外でも、米国のサイバーセキュリティフレームワークの普及、EU の NIS 指令の施行等による重要インフラ防御の政策が進展した。EUではまた、一般データ保護規則（GDPR）の施行に向けガイドラインの整備等が進んだ。国内では、個人情報保護委員会が、改正個人情報保護法の 2017 年 5 月の施行に向けてガイドラインを整備した。日本は IoT、重要インフラ防御、個人情報保護等の分野で各国と連携しつつ、サイバーセキュリティ対策を進める必要がある。

以上のように、2016 年度もサイバーセキュリティの脅威は継続し、対策は着実に進んだものの、多数のインシデントが発生した。新しい IT 基盤を悪用した脅威も現実になり、今後ますます対策の強化が必要である。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

IoT 等の新しい技術の普及、重要インフラの IT 化等で IT の利用場面が大きく拡大しつつある中、サイバー攻撃の脅威は少しも衰えていない。2015 年度に引き続き、2016 年度は、標的型攻撃事案が旅行会社等の企業、大学等の研究機関で発生し、大規模な情報流出の危機が継続した。

金銭を狙うサイバー攻撃では、ランサムウェアの被害が急増し、国内外で問題となった。Adobe Flash Player や Web サイトを構築するためのソフトウェア等の脆弱性を突く攻撃も継続した。更に、脆弱な IoT 機器を乗っ取るウイルス「Mirai」により過去最大規模の DDoS 攻撃が発生し、IoT 機器のセキュリティ対策の不備が深刻な問題であることが明らかになった。

産学官による連携、各組織における施策の着実な実践等により、セキュリティ対策の更なる強化が求められる。

本章では、2016 年度に発生した主要なインシデントやその手口、対策の状況について解説する。

1.1 2016年度に観測されたインシデント状況

情報セキュリティインシデントは世界各国で発生しており、その規模や影響は年々拡大している。2016 年においても、大規模な情報漏えい、サイバー攻撃を許すきっかけとなるスパムメールや脆弱性の放置、フィッシングサイト、またランサムウェアやビジネスメール詐欺等の金銭被害に直結する事象が確認されている。

国内においても、ランサムウェアが検出された機器の台数が最大となり、Apple Inc. や Microsoft Corporation（以下、Microsoft 社）等の身近なサービスをかたったフィッシングサイトが増加する等、サイバー攻撃の脅威が増している。

1.1.1 世界における情報セキュリティインシデント状況

世界における情報セキュリティインシデントの発生状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

- IBM Corporation（以下、IBM 社）：IBM X-Force Threat Intelligence Index 2017※1
- Symantec Corporation（以下、Symantec 社）：Internet Security Threat Report, Volume 22※2
- Verizon Communications Inc.（以下、Verizon 社）：2017 Data Breach Investigations Report 10th edition※3
- Black Duck Software（以下、Black Duck 社）：2017 Open Source Security and Risk Analysis Report※4
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2016 年 年間セキュリティラウンドアップ※5
- NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）：NRI Secure Insight 2017※6
- Anti-Phishing Working Group, Inc.（以下、APWG）：Phishing Activity Trends Report※7

(1) 情報漏えいインシデントの状況

2016 年 4 月、パナマの法律事務所である Mossack Fonseca から流失した、1,150 万件の租税回避に関する文書、並びに関与する 21 万 4,000 社の企業名や首脳等の著名人の情報（日本在住者・企業約 400 を含む※8）が公開された。2016 年 12 月には、米国 Yahoo! が 2013 年に 10 億人、2014 年に 5 億人のアカウント情報が情報漏えいしたことを公表し、単一組織からの漏えい件数としては過去最悪となった。

IBM 社によると、漏えいしたデータ件数は、2014 年は約 10 億件、2015 年は約 6 億件と減少し、2016 年は約 40 億件と急増した。Symantec 社でも、2014 年は約 12.2 億件、2015 年は約 5.6 億件と減少し、2016 年に約 11.2 億件と、2016 年に再び増加したと報告している。

Symantec 社によると、情報漏えいインシデントが発生

第2章
情報セキュリティを支える基盤の動向

2016 年度は、改正サイバーセキュリティ基本法及びその関連法制等が施行され、政府機関や独立行政法人等のセキュリティ監視・監査の強化、セキュリティ人材育成に向けた新たな試験・資格制度が始まった。

このほか政府においてはサイバーセキュリティ戦略に基づく重要インフラ防御施策や、IoT セキュリティに関するガイドラインの策定や国際連携の推進、改正個人情報保護法施行に向けたガイドラインの整備等、対策の着実な実践が始まっている。

海外においては、米国のトランプ政権の誕生、欧州における個人データ保護法制の強化等があり、日本は各国と協調しつつ、サイバーセキュリティ対策を進める必要がある。本章では、情報セキュリティの取り組みを支える基盤の状況と最新の動向について解説する。

2.1 日本の情報セキュリティ政策の状況

高度化するサイバー攻撃から、我が国が保有する機密情報を守り、国際競争力の確保及び発展につなげるには、情報セキュリティ対策への取り組みを強化していく必要がある。本節では、政府が推進する情報セキュリティ政策の状況を述べる。

2.1.1 政府全体の政策動向

政府は、2016 年 1 月 22 日に閣議決定された第 5 期「科学技術基本計画※1」において、物理空間（現実社会）とサイバー空間を一体化した超スマート社会の実現に向けた取り組みである「Society 5.0」を推進すると明記した。一体化の促進により国民生活や経済活動において、より利便性・生産性が高まることが期待される。一方で、国境を越えたセキュリティ脅威の高まりや被害の深刻さにも留意しなければならない。政府は 2020 年を一つの節目ととらえ、サイバー空間のセキュリティ確保のため多くの施策に積極的に取り組んでいる。

(1) サイバーセキュリティ戦略本部の動向

我が国のサイバーセキュリティに関わる政策や方針は、サイバーセキュリティ戦略本部で策定される。同戦略本部の事務局である内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity:NISC）は、関連府省庁等と連携し、「サイバーセキュリティ戦略※2」「政府機関の情報セキュリティ対策のための統一基準群※3」「重要インフラの情報セキュリティ対策に係る行動計画※4」等の策定、並びにサイバーセキュリティに関わる施策、国際連携、国民への普及啓発等を推進し、また行政機関等への監査や調査、助言等を実施している。

(a) サイバーセキュリティ 2016 の策定

2016 年 8 月 31 日、「サイバーセキュリティ戦略」に基づき、以下の三つの政策分野ごとに関連府省庁の具体的な取り組み方針を示した年次計画「サイバーセキュリティ 2016※5」が公表された（図 2-1-1）。

- 経済社会の活力の向上及び持続的発展
  2016 年 7 月に IoT 推進フォーラム、総務省、経済産業省により策定、公表された「IoT セキュリティガイドライン※6」や、「サイバーセキュリティ経営ガイドライン※7」の普及、「スマートメーターシステムセキュリティガイドライン※8」の電気保安規定への位置付け変更（「2.1.2 経済産業省の政策」参照）、金融業界の横断的な演習等を実施する。
- 国民が安全で安心して暮らせる社会の実現
  サイバーセキュリティに関する普及啓発、地方公共団体における緊急時対応支援、「政府機関の情報セキュリティ対策のための統一基準群」の改定、「重要インフラの情報セキュリティ対策に係る第 3 次行動計画※9」の見直し等を実施する。
- 国際社会の平和・安定及び我が国の安全保障
  サイバー脅威に関する情報収集・分析機能及び対処能力等の強化については、対象を警察庁だけでなく

第3章
個別テーマ

個別テーマとして取り上げたのは、制御システム、IoT、スマートデバイス、金融、オリンピック・パラリンピックの情報セキュリティである。いずれも重要インフラや新しい社会基盤に密接に関係するテーマであり、十分なリスク評価と情報セキュリティ対策が求められる。

新しいトピックである「3.4 金融の情報セキュリティ」では、金融等のサービスに革新をもたらすことが期待されている Fintech、特にブロックチェーンに基づく仮想通貨流通や契約自動処理のセキュリティについて解説している。

3.1 制御システムの情報セキュリティ

従来、制御システムは独立したネットワーク、独自のプロトコル、事業者ごとに異なる仕様で構築・運用されていることが多く、外部からサイバー攻撃を行うことは困難であった。しかし、近年ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだことで、制御システムがサイバー攻撃を受ける恐れが指摘されるようになり、実際にサイバー攻撃による大規模停電も発生している。本節では制御システムの情報セキュリティ動向と取り組みについて述べる。

3.1.1 制御システムの概要

制御システムは、電力・ガス・水道等の重要インフラや様々な産業分野において、生産・製造・輸送工程のオートメーション化等、多様な目的で利用されている。

業務の効率化や、企業全体での経営資産の活用（経営の最適化）のため、最近の制御システムは企業の IT システムにファイアウォール等を介してつながっていることが多い。図 3-1-1 に示すように、上位レイヤの管理システム等には UNIX 系や Windows の汎用サーバやクライアント端末が用いられ、標準プロトコルや汎用アプリケーションが利用されている。一方、下位レイヤのコントローラーやセンサー等は、独自のハードウェア、OS、プロトコル等が使われていることが多く、固有の仕様となっている。

3.1.2 制御システムのインシデント事例

2016 年 3 月、ある水道事業者の制御システムに攻撃者が侵入し、2 ヵ月程にわたって水の流量を制御するバルブの不正操作や、浄水処理に使われる化学薬品の注入量の改ざんが行われていたとの事例が報告された※1。この水道事業者の制御システムは、契約者が使用量の確認や料金のオンライン支払いを行う Web システムと直接つながっており、この Web システム（決済アプリケーション）が制御システムの IP アドレスと認証情報を平文で保存していた。攻撃者は個人情報の窃取を目的に決済アプリケーションの脆弱性を突いて侵入、内部探索により発見した IP アドレスと認証情報を用いて制御システムにアクセスし、不正操作やデータ改ざんを行ったものと見られる。バルブの不審な動作や薬品注入量の変更は迅速に検知・是正され、影響は最小限にとどめられたものの、制御システムをインターネットに接続されたシステムと安易につなぐことの危険性が改めて示された。

2016 年 12 月には、2015 年に続き、ウクライナの首都キエフ北部において、サイバー攻撃による大規模停電が発生した※2。今回は 12 月 17 日から 18 日にかけての深夜にキエフ近郊の配電所が停止し、200 メガワットの電力（キエフの夜間の電力需要量の約 5 分の 1 に相当）が配電できなくなった。電力会社 Ukrenergo の IT 担当者が不審な通信データを確認したとの報告もあって当初からサイバー攻撃が疑われていたが、その後の調査で配電所につながっている SCADA（Supervisory Control and Data Acquisition）※3 システム及びワークステーションが外部から操作されたことを示す痕跡が見つかった、と報道されている。攻撃者は 6 ヵ月間にわたってネットワーク内に潜み、システムの仕組みを調査し、権限情報を奪取して犯行に及んだと見られる※4。