情報セキュリティ白書

Information Security White Paper

2018

深刻化する事業への影響：つながる社会で立ち向かえ

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2018」の刊行にあたって

2017 年は IoT、AI 等に代表される新しい IT 基盤の利活用が本格的に始まった年となりました。IoT による社会インフラ監視や物流・配車の最適制御、AI 技術による RPA（Robotic Process Automation）やセキュリティ監視、両者の融合によるスマート家電の実用化、更には仮想通貨の普及等、新しいサービスが続々と誕生しました。これらのサービスにより、私達の日常の活動はすべてサイバー空間とつながり、世界中の人々ともつながっていきます。

こうした社会を支える IT 基盤において、サイバーセキュリティが中核となるべきことは言うまでもありません。残念ながら、新しい IT 技術・利用形態の出現は、場合によっては新しい脆弱性を生み出し、それを突く攻撃が現れます。2017 年 5 月、ランサムウェア Wanna Cryptor が世界的な被害をもたらし、社会サービスが停止するという懸念が現実のものとなりました。このような被害事例を見ると、発見された脆弱性に対して適切な対処ができていないようです。

たとえ IT 基盤を頑健にしても、人間の脆弱性は恰好の標的となります。2017 年は、ビジネスメール詐欺による大規模な金銭被害が国内でも発生しました。こうした人間心理の弱点を突く詐欺的な手法による被害を防ぐことは非常に難しく、今後も大きな課題となります。更に、急速なサービスの普及・拡大はときにセキュリティ対策の遅れを生みます。2018 年 1 月、仮想通貨取引業者を狙ったサイバー攻撃により 580 億円相当の仮想通貨が流出しましたが、この事例では事業拡大のスピードにセキュリティ対策が追いつかず、また業界全体としてのセキュリティの体制も整っていませんでした。

サイバー空間とフィジカル空間がつながる社会において、サイバー攻撃は深刻な影響を及ぼすことが懸念されます。私達ひとりひとりがサイバー空間・フィジカル空間のどんなリスクに関係するのかを意識し、それぞれに対応を考える必要があります。つながりが深まれば考慮すべきリスクも増大するため、これは容易なことではありません。しかし、対応する私達もまたつながることができます。政府、セキュリティ専門家、サービス提供者、利用者を問わず、お互いに情報を共有し、学びあうことがこれまで以上に重要になってくると思います。

本白書が、多くの方々に広く利用され、見えてきた脅威やリスクに対して意識を高め、備えを実践するための一助となることを祈念します。

2018年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

2018

情報セキュリティ白書

序章

2017年度の情報セキュリティの概況

2017 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、脆弱性を悪用した攻撃や、不注意や運用不備による情報漏えいが 2016 年から継続して発生した。2017 年度になって新たに注目されたインシデントとしてはランサムウェアによる広域な被害やビジネスメール詐欺、仮想通貨取引所への不正アクセス等、事業に甚大な影響を与えかねない攻撃があった。

2017 年度前半は Apache Struts2 の脆弱性を悪用した攻撃による情報流出が相次ぎ、政府や関連組織への不正アクセスもあった。その他、国内外にてソフトウェアのアップデートを怠ったことによる被害も報告されていることから、運用改善を含め、脆弱性に対する更なる対策が必要である。

2017 年 5 月には、ランサムウェア「Wanna Cryptor」（別名 WannaCry）が世界規模で猛威を振るい、医療や交通サービス等に大きな影響を及ぼした。自己増殖機能によりネットワークを経由して感染が拡大したことが一因であるが、これも OS のアップデートを実施していれば被害は免れることができたため、適切な運用が強く望まれる。

金銭目的の攻撃については、取引先や経営者等をかたり、従業員を騙して資金を詐取するビジネスメール詐欺の被害が深刻化した。国内では 9 月に被害額が 3 億円を超える事例が発生した。

2018 年 1 月には、国内の仮想通貨取引所が不正アクセスを受け、約 580 億円相当の仮想通貨が不正流出した。更に、脆弱な機器による不正マイニングが急増する等、仮想通貨を取り巻く環境への対策が求められる。

2018 年 3 月には、政府関連組織から個人情報を委託されていた業者が無断で海外の業者に再委託していたことが発覚した。また、国外では大手 SNS で取得された個人情報が、英国の国民投票や米国の大統領選挙で不正利用された可能性があることが示唆されており、急速に成長する事業にセキュリティ対策や法制化が追いついていないという課題が明らかになった。

2017 年度は国内外で政府・組織が新しい制度に基づく施策を展開するとともに、次の施策の準備を開始した年となった。

国内では、2017 年 4 月に「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」が決定し、「サイバーセキュリティ戦略」に基づく施策の実現、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が始まった。また、人材育成においても、産業サイバーセキュリティセンターが発足し、社会インフラや産業基盤のサイバー攻撃に対する防御力を強化するための人材育成を開始した。情報処理安全確保支援士（セキスペ）登録者数は、2018 年 4 月 1 日時点で 9,181 名となった。更に、IPA では中小企業が自らのセキュリティへの取り組みを宣言する制度「SECURITY ACTION」を創設した。

10 月に経済産業省が「『Connected Industries』東京イニシアティブ 2017」、総務省が「IoT セキュリティ総合対策」を公表し、12 月には産業サイバーセキュリティ研究会が発足して対策を推進した。また、11 月には「サイバーセキュリティ経営ガイドライン」が改訂され、サイバー攻撃の検知、攻撃からの復旧への備え及びサプライチェーン対策等の取り組み等を強化した。

一方、米国では 5 月に発効した大統領令に伴って全省庁横断で対策の見直しがされた。その後米国サイバー軍を統合軍に格上げするとともに、国防権限法で要求されているサイバー戦に関する包括的な戦略を上下両院に提出した。また、NIST Cybersecurity Framework の改訂等により、サプライチェーンリスク管理が強化された。欧州では一般データ保護規則（GDPR）の施行に向け、各国におけるガイドラインの整備等が進んだ。日本では、改正個人情報保護法が 5 月から施行され、日・EU 間の相互の円滑な個人データ移転に向けた調整が行われていたが、2018 年 5 月に合意に達した。中国では 2017 年 6 月にネットワーク安全法が施行され、政府の統制が強まった。このように、海外の動向にも注意が必要である。

以上のように、2017 年度もサイバーセキュリティの脅威は継続し、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つつあるが、産学官、国内外において連携を強化し、今後ますます対策の着実な実施と強化が必要である。

2017 年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2017 年　4 月	● Apache Struts2 の脆弱性を悪用した不正アクセスによる情報流出が相次ぐ（1.2.4（1）、1.3.3（1））	● 情報処理安全確保支援士（登録セキスペ）登録開始（2.4.2） ● 「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」決定（2.1.1） ● 産業サイバーセキュリティセンター発足（2.4.1） ● 「サイバーセキュリティ人材育成プログラム」公表（2.4.1） ● SECURITY ACTION の創設（3.5）
5 月	● 世界各国で Wanna Cryptor による被害が相次ぐ（1.2.1、1.3.1）	● 改正個人情報保護法の全面施行 ● 「知的財産推進計画 2017」決定（2.2.2） ● 米国でサイバーセキュリティ強化に関する大統領令の発効（2.3.2）
6 月	● ランサムウェアを自作したとして、中学 3 年の男子生徒を不正指令電磁的記録作成等の疑いで逮捕（2.1.4）	● 「科学技術イノベーション総合戦略 2017 」「未来投資戦略 2017」決定（2.1.1、2.2.2） ● 中国でネットワーク安全法の施行（2.3.4）
7 月		● 「サイバーセキュリティ研究開発戦略」公表（2.1.1） ● ドイツで一般データ保護規則（GDPR）に対応した新ドイツ連邦データ保護法の成立（2.3.3）
8 月		● 「サイバーセキュリティ 2017」公表（2.1.1）
9 月	● 国内航空会社でビジネスメール詐欺による 3 億円を超える被害発生（1.2.5（1）、1.3.6） ● 米国の大手信用情報会社が 1 億 4,300 万人の米国顧客の個人情報が流出可能性を公表（1.1.1、1.4.1（2））	● 欧州委員会がサイバーセキュリティ法案を発表（2.3.3）
10 月	● コミュニティサイトを通じて知り合った男女 9 名が殺害される事件が発生（2.1.4） ● 仮想通貨のマイニングツールが確認される（3.1、3.3） ● 無線 LAN の暗号化規格である WPA2 の脆弱性（KRACK/KRACKs）が発見される（1.4.1）	● 「IoT セキュリティ総合対策」公表（2.1.3） ● 「Connected Industries」東京イニシアティブ 2017 発表（2.1.2） ● 「サイバーセキュリティ国際キャンペーン」月間実施（2.1.1）
11 月	● 国内における IoT 機器のウイルス感染の急増（3.1.2）	● 「サイバーセキュリティ経営ガイドライン Ver.2.0」の公開（2.1.2、2.5.1）
12 月		● 「分野横断的演習」の実施（2.1.1） ● 産業サイバーセキュリティ研究会設置（2.1.2） ● 個人情報保護マネジメントシステム JIS Q 15001 改訂（2.5.2）
2018 年　1 月	● 仮想通貨交換取引所から約 580 億円相当の仮想通貨が不正流出（3.2.1）	
2 月	● 平昌冬期オリンピック・パラリンピック競技大会の妨害を目的としたサイバー攻撃	● サイバーセキュリティ月間（2.8.1） ● 「不正競争防止法等の一部を改正する法律案」の閣議決定（2018 年 5 月 30 日公布）（2.2.2） ● 「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」公表（2.1.2）
3 月	● 日本年金機構の業務委託先が無断で海外事業者に再委託していたことが発覚（1.2.4（3）） ● SNS 上で取得された最大 8,700 万人の個人情報が米国選挙工作のため不正利用されていたことが発覚（1.2.4（3）、2.3.2（7））	● 「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」の閣議決定（2018 年 5 月 23 日公布）（2.1.3）

※ 2017 年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、DDoS 攻撃、Web 改ざん等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。表に示していない他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

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

2016年度に続き、2017年度においても多くの個人、組織でサイバー攻撃による被害が確認された。また、IoT機器やITサービスの普及、拡大による生活の利便性が向上しつつある一方で、手口の狡猾化や攻撃の容易化等、サイバー攻撃の脅威も増してきている。

2017年5月、世界中で猛威を振るったWanna Cryptorは、これまでのランサムウェアには見られなかった自己増殖機能を有していたことで大規模な感染拡大に至った。このWanna Cryptorによる騒動は、2ヵ月前に修正プログラムが公開されている脆弱性を悪用するものであり、脆弱性への対応やサプライチェーンのリスク管理等の不十分さを浮き彫りにした。2017年度は他にもビジネスメール詐欺や偽警告・偽サイト等、巧妙に人を欺き金銭を奪う被害も多数報告された。また、内部不正や不適切な運用による個人情報漏えいが継続して発生した。

本章では、2017年度に発生した主要なインシデントの概要と攻撃の手口や対策の状況、脆弱性の動向等について解説する。

1.1 2017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。2017年においても、ランサムウェア感染によるサービス停止や、大規模な情報漏えいによる深刻な事業への影響、フィッシングやビジネスメール詐欺による金銭被害、更には脆弱性のある機器を悪用した仮想通貨不正マイニング等の事案が確認されている。

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Amazon.com, Inc.等の身近なサービスをかたったフィッシングメールや、ウイルス※1感染を狙ったばらまき型メールが頻繁に確認され、更には4億円近い被害が発生したビジネスメール詐欺や580億円相当の仮想通貨が取引所から流出する等、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。

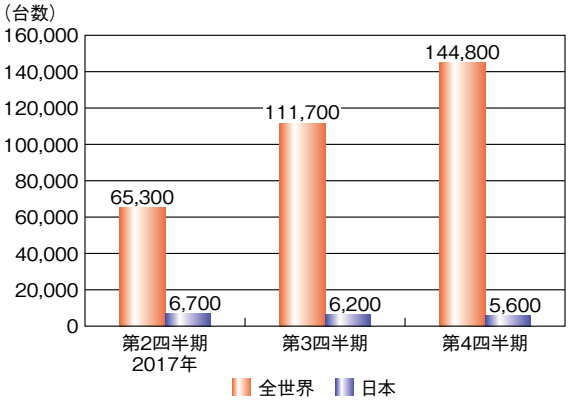
- International Business Machines Corporation（以下、IBM社）：IBM X-Force Threat Intelligence Index 2018※2
- Symantec Corporation（以下、Symantec社）：Internet Security Threat Report Volume 23※3
- Verizon Communications Inc.（以下、Verizon社）：2018 Data Breach Investigations Report※4
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2017年年間セキュリティラウンドアップ※5
- Anti-Phishing Working Group, Inc.（以下、APWG）：Phishing Activity Trends Report※6

(1) ランサムウェア被害の深刻化

2017年5月、Microsoft Corporation（以下、Microsoft社）のSMBv1（Server Message Block 1.0）の脆弱性（CVE2017-0144※7、CVE2017-0145※8）を悪用して自己増殖するランサムウェア「Wanna Cryptor」（別名WannaCry、WannaCrypt、Wcry）が世界を席巻した。トレンドマイクロ社によると、Wanna Cryptorに感染したパソコンの台数は2017年第2四半期の6万5,300台から第4四半期には14万4,800台に急増した（図1-1-1）。

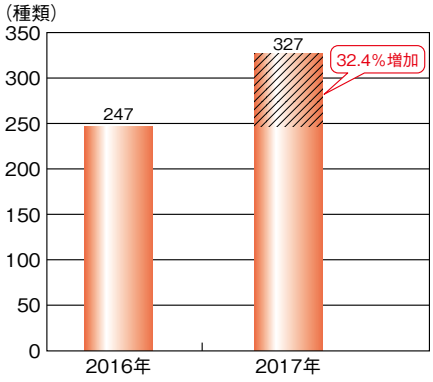
ランサムウェアは通常身代金を獲得することが目的だが、Wanna Cryptorは振込人を特定する機能を持たず、身代金による被害は比較的少なかった。一方で、これまでのランサムウェアになかった自己増殖機能を有していたために感染が拡大し、病院や鉄道等のサービスに影響が出る等、社会に大きな衝撃を与えた。

トレンドマイクロ社によれば、2016年から2017年にかけて、ランサムウェアの新種と亜種のグループ（ファミリー）



■図 1-1-1　日本と世界における Wanna Cryptor の検出台数推移
（出典）トレンドマイクロ社「2017 年年間セキュリティラウンドアップ」を基に IPA が編集

数は 32.4% 増加して 327 となる一方、攻撃の総数は 58.5% に減少し、6 億 3,100 万となった（図 1-1-2）。しかし、Wanna Cryptor や NotPetya 等の主要なランサムウェアによる攻撃により、全世界の被害額は 50 億米ドルに達しており※9、被害は深刻化している（被害については「1.2.1 ランサムウェアによる被害」、手口については「1.3.1 ランサムウェアによる攻撃」参照）。



■図 1-1-2　新たに確認されたランサムウェアファミリー数の年別比較
（出典）トレンドマイクロ社「2017 年年間セキュリティラウンドアップ」を基に IPA が編集

ランサムウェアによる被害が拡大している要因として、非常に安価に攻撃ツールやサービス（Ransomware-as-a-Service）※10 の入手や利用ができるアンダーグラウンド市場の存在が指摘されている。

Symantec 社によれば、2017 年はランサムウェア向けのツールやサービスにサイバー犯罪者が殺到、攻撃が急増したことで「市場の調整」が起こったという。例えば身代金の平均要求額は 522 米ドルで、2016 年の 1,070 米ドルの半額以下となった。またランサムウェア提供グループは淘汰され、新たなファミリーの出現は 2016 年の 98 から 2017 年の 28 に急減した。しかし、新たなランサムウェアは巧妙化を続けており、2017 年には前述の Wanna Cryptor のような自己増殖型や、ソフトウェアをインストールしないファイルレス攻撃※11 が出現した。

IBM 社によれば、同社が調査した企業の半数はランサムウェア被害を経験しており、ランサムウェアによる事業停止、身代金支払い等の被害は世界全体で 80 億米ドルを超えたという。どのような新しい攻撃があり得るかを常に把握し、必要な対策を取ることが重要である。

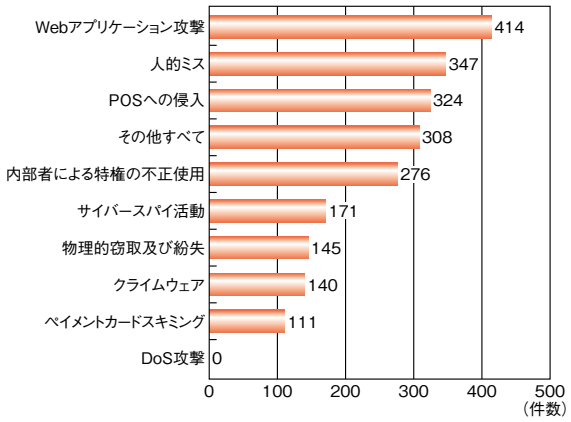
(2) 情報漏えいインシデントの状況

2017 年 10 月 2 日、米国の信用情報会社 Equifax Inc. は、不正アクセスにより 1 億 4,550 万人の米国顧客の個人情報が流出した恐れがあると公表した※12。流出した情報には社会保障番号や運転免許証番号・生年月日・住所・クレジットカード情報が含まれる。同社は原因を 2017 年 3 月に指摘された Apache Struts2 の脆弱性としており、修正プログラムを適用できていなかったため攻撃されたと考えられる。また 2017 年 12 月、データ分析会社 Alteryx, Inc. の保有する約 1 億 2,300 万件の米国の世帯情報が Amazon Web Service の設定ミスにより公開されていたことが発覚した※13。情報は匿名化されていたが、住所、家族の収入・資産、子ども等の機微情報が含まれていた。

IBM 社によると、2017 年に漏えいしたデータ件数は約 29 億件であり、2016 年度に比べて 25% 減少した。サイバー攻撃の手法がランサムウェアにシフトしたことの影響とみられるという。また、同社によれば、クラウド等の設定ミスやバックアップ事故等により公開されたデータはその 70% に上り（20 億件）、これは 2016 年に比べて 424% 増であった。

Verizon 社によると、2017 年に発生した情報漏えいインシデント 2,216 件を種別に見ると、最も件数が多い業種は「医療」で 536 件、次いで「不動産」が 338 件、「政府・自治体」が 304 件、「小売」が 169 件、「金融」が 146 件となっている。また上記の情報漏えいインシデントの攻撃方法を分類した結果によると、2017 年も「Web アプリケーション攻撃」が 414 件と最も多い（2016 年は 571 件）。2016 年に 4 位であった「人的ミス」（222 件）が 347 件で 2 位に、5 位であった「PoS への侵入」（207 件）が 3 位（324 件）となっている。一方 2016 年度に 2 位だった「サイバースパイ活動」（289 件）は 171 件に減少し、6 位となった（次ページ図 1-1-3）。

これらの情報漏えいの発生状況及び攻撃の傾向を考慮し、情報保護対策を継続的に実施する必要がある（情

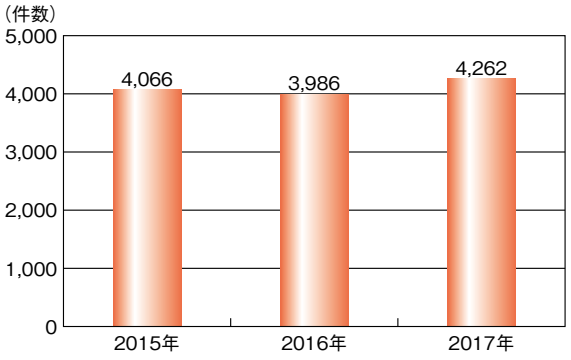


■図 1-1-3　情報漏えい事件の分類
(出典)Verizon 社「2018 Data Breach Investigations Report」を基に IPA が編集

報漏えいの被害については「1.2.4 情報漏えいによる被害」参照)。

(3)脆弱性の新たな脅威となった不正マイニング

Symantec 社によれば、2017 年に公開されたゼロデイ脆弱性の数は 4,262 件で、2016 年から約 7% の増加であった(図 1-1-4)。

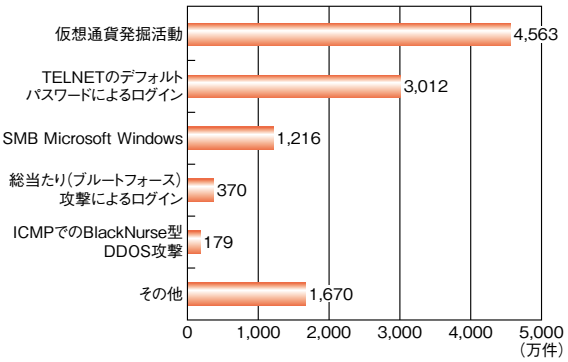


■図 1-1-4　ゼロデイ脆弱性の件数
(出典)Symantec 社「Internet Security Threat Report Volume 23」を基に IPA が編集

2017 年前半、Bitcoin 等の仮想通貨の価値が急騰した結果、セキュリティに問題のあるパソコン等を乗っ取り、仮想通貨マイニングソフトウェアを仕掛けて計算機パワーを不正に使ったマイニングを行うサイバー犯罪が急増した(仮想通貨のセキュリティに関しては「3.2 仮想通貨の情報セキュリティ」参照)。

Symantec 社によれば、2017 年にパソコン等の端末で検出されたマイニングソフトウェアは前年の 85 倍となった。また同社の観測によれば、端末でブロックしたマイニングイベント数が 2017 年 9 月以降に急増、12 月のブロックイベント数は 800 万件超となり、年初の 340 倍となった。

トレンドマイクロ社が 2017 年に観測したイベントでは、「仮想通貨発掘活動」(マイニング)(4,563 万件)、及び「TELNET のデフォルトパスワードによるログイン」(IoT 機器への不正ログイン)(3,012 万件)が上位を占めている(図 1-1-5)。

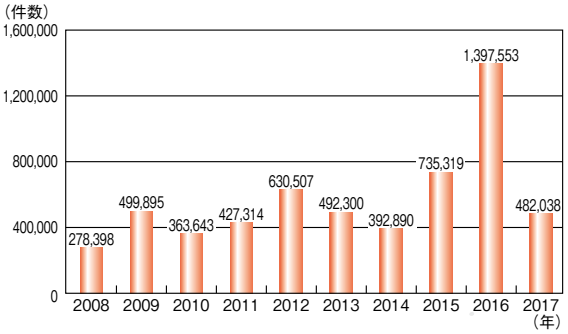


■図 1-1-5　2017 年に観測された仮想通貨マイニングと TELNET 関連活動
(出典)トレンドマイクロ社「2017 年年間セキュリティラウンドアップ」を基に IPA が編集

また、乗っ取った IoT 機器を悪用する目的に変化が見られ、DDoS 攻撃だけなく仮想通貨のマイニングにも利用されているという。不正なマイニングの悪影響は、パソコンや IoT 機器の性能の低下、あるいはその端末所有者が負担する電気料金・利用料金の増加等の形で現れるが、一般にはその原因が不正なマイニングであるとは気づかれにくい。脆弱性や適切な IoT 機器の管理に対する十分な備えが必要である(脆弱性については「1.4.2 脆弱性の状況」、IoT のセキュリティについては「3.1 IoT の情報セキュリティ」参照)。

(4)フィッシングとビジネスメール詐欺の傾向

APWG によると、2017 年のフィッシングサイトの総数は第 3 四半期までで約 48 万 2,000 件であり、2016 年と比較して減少傾向となった(図 1-1-6)。



■図 1-1-6　世界における届け出されたフィッシングサイト件数
(出典)APWG「Phishing Activity Trends Report」(2008 年～ 2017 年第３四半期)を基に IPA が作成(2017 年の数値は第３四半期までのもの)

ターゲットとなる業種は、2017 年第 2 四半期は「ペイメント（支払い）」が 45%、「金融機関」が 16%、「SaaS/Web メール」が 15%、また第 3 四半期はそれぞれ 42%、15.5%、17% となった。全体としてフィッシングサイト数は減少傾向にあるものの、トレンドマイクロ社によればフィッシングサイトに誘導される人数は減っていない。また IBM 社が指摘するように、仮想通貨取引所のウォレットを狙ったフィッシング等の詐欺も出現しており、警戒が必要である（フィッシングの被害については「1.2.5 (2) (d) フィッシングによる被害」、手口については「1.3.7 (4) フィッシングの手口と対策」参照）。

ビジネスメール詐欺の被害は拡大し続けている。トレンドマイクロ社の調査によれば、ビジネメール詐欺で最も多く詐称される役職は CEO（Chief Executive Officer：最高経営責任者）で、詐欺メールの 38.5% を占める。また最も多く標的にされる役職は CFO（Chief Financial Officer：最高財務責任者）で、詐欺メールの 15.5%を占める。例えば 2017 年 7 月、ドイツのサイバーセキュリティ機関が、組織化された偽の送金依頼により数百万ユーロの被害が出ているとして、標的となる企業に注意を喚起した※14。2018 年は、巧妙化するサイバー攻撃だけでなく、IT を巧みに悪用した詐欺にも留意することが重要である（ビジネスメール詐欺の被害については「1.2.5 (1) ビジネスメール詐欺による金銭被害」、手口については「1.3.6 ビジネスメール詐欺」参照）。

1.1.2 国内における情報セキュリティインシデント状況

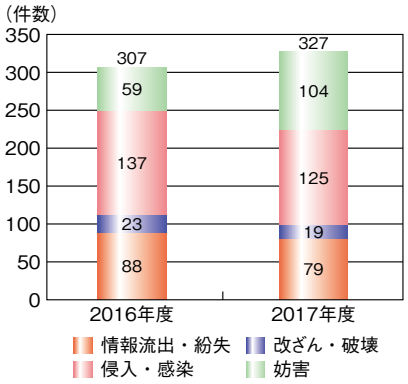
国内における情報セキュリティに関するインシデントの発生状況について、以下の報告書を参照して傾向を述べる。

- 三井物産セキュアディレクション株式会社（以下、MBSD 社）：サイバーセキュリティ事件簿※15
- トレンドマイクロ社：2017 年年間セキュリティラウンドアップ
- 一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）：インシデント報告対応レポート※16
- 日本アイ・ビー・エム株式会社（以下、日本 IBM 社）：2016 年下半期 Tokyo SOC 情報分析レポート、2017 年上半期 Tokyo SOC 情報分析レポート、2017 年下半期 Tokyo SOC 情報分析レポート※17
- フィッシング対策協議会：月次報告書※18

(1) 情報セキュリティインシデントの発生状況

MBSD 社が集計した結果によると、2017 年度に報道された情報セキュリティインシデント発生件数は 2016 年度の 307 件から 327 件に増加した（図 1-1-7）。事象別に見ると「情報流出・紛失」「改ざん・破壊」「侵入・感染」が 8.8 ～ 17.4% 減少しているのに対して、「妨害」は 76.3% と著しく増加した。

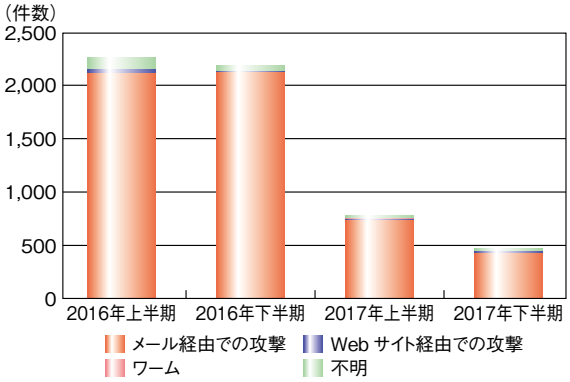
「妨害」の内容はフィッシング攻撃が多数を占めており、フィッシング対策協議会やクレジットカード会社が引き続き注意喚起を行っている（「1.2.5 (2) (d) フィッシングによる被害」参照）。



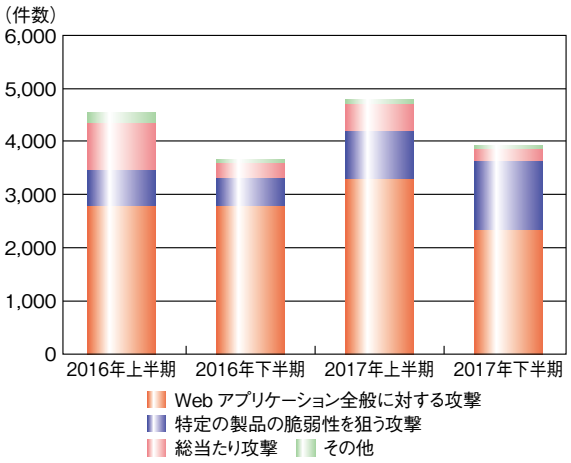
■図 1-1-7　情報セキュリティインシデントの事象分類
（出典）MBSD 社「サイバーセキュリティ事件簿」を基に IPA が作成

図 1-1-8、図 1-1-9（次ページ）は、日本 IBM 社が東京の観測拠点（Tokyo SOC）で観測したセキュリティインシデントの動向である。

半期ごとの全体的な攻撃の観測件数は減少傾向にあるが、図 1-1-8 に示すとおり、特にクライアントへの攻撃が大幅に減少している。日本 IBM 社は 2016 年度に比べてばらまき型メールによる攻撃が減少したことを要因として挙げている。一方、図 1-1-9 に示すとおり、サーバ



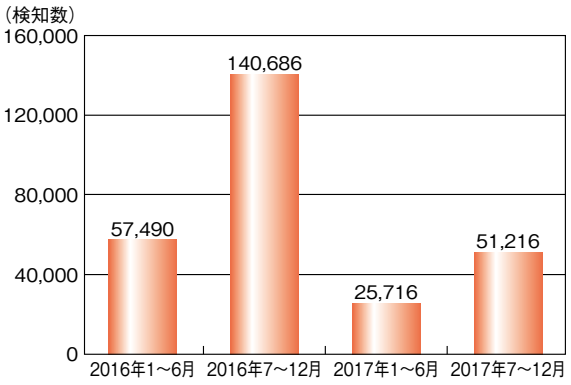
■図 1-1-8　クライアント PC を対象とした攻撃の経由元
（出典）日本 IBM 社「2017 年下半期 Tokyo SOC 情報分析レポート」を基に IPA が作成



■図 1-1-9　サーバに対する攻撃の内訳
(出典)日本 IBM 社「2017 年下半期 Tokyo SOC 情報分析レポート」を基に IPA が作成

に対する攻撃はクライアントへの攻撃に比べ、ほぼ横ばいの推移となっているが、特定の製品の脆弱性を狙った攻撃は 2017 年下半期に増加しており、そのうちの約 80%は Apache Struts の脆弱性に対する攻撃であった。

2017 年は、ばらまき型メールによる攻撃は減少したとされ、図 1-1-10 で示すように 2016 年に比べてウイルス感染を狙う不正メールの検出数が減少している。ただし、2017 年下半期に注目すると上半期の約 2 倍に増加しており、脅威は継続していると言える。

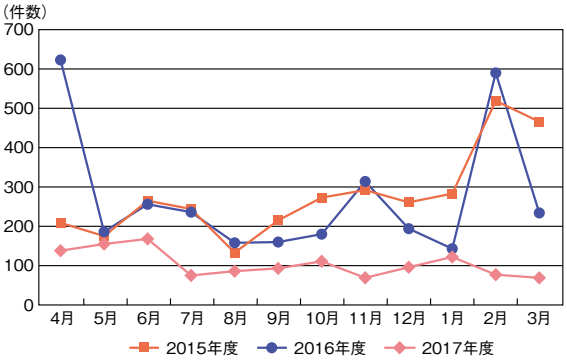


■図 1-1-10　ウイルス感染を狙う不正メールの検出数推移
(出典)日本 IBM 社「2016 年下半期 Tokyo SOC 情報分析レポート」「2017 年上半期 Tokyo SOC 情報分析レポート」「2017 年下半期 Tokyo SOC 情報分析レポート」を基に IPA が作成

2017 年上半期は、2016 年下半期に不正メールの 94.9% を占めていたランサムウェア「Locky」への感染を狙う攻撃が大幅に減少した。他方、不正送金等を狙ってインターネットバンキングの認証情報やクレジットカード情報を窃取するウイルスである「Ursnif」(アースニフ) や「Dreambot」の感染を狙うメールが継続的に確認された。下半期は、Microsoft Office の DDE (Dynamic Data Exchange) 機能を悪用して Locky への感染を狙う攻撃や数式エディタの脆弱性を悪用する攻撃等が確認され、新しい手口として注目を集めた (「1.2.5 (3) インターネットバンキングを狙った攻撃による金銭被害」「1.3.4 ばらまき型メールによる攻撃」参照)。

(2) Web サイト改ざんによる被害

2017 年度に JPCERT/CC へ報告された Web サイトの改ざん総件数は 1,259 件であった。ここ数年は 2014 年度の 3,664 件、2015 年度の 3,335 件、2016 年度の 3,274 件とわずかに減少傾向であったが、2017 年度は大幅に減少し、月別でも大きな変動はなく 100 件前後で推移した (図 1-1-11)。



■図 1-1-11　Web サイト改ざん件数推移
(出典)JPCERT/CC「インシデント報告対応レポート」(2015 年 4 月 1 日 ~ 2018 年 3 月 31 日)を基に IPA が作成

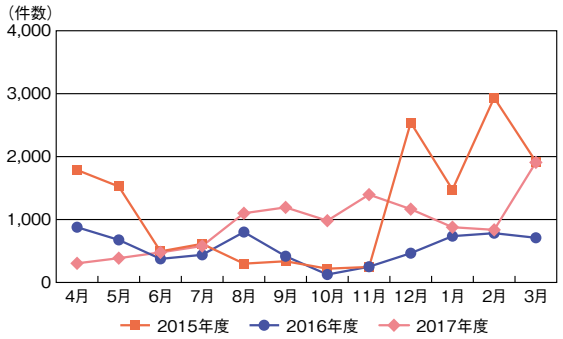
JPCERT/CC は大幅な減少の要因として、「Web サイトの改ざんを容易にするような新しい脆弱性が確認されなかったことや、ウイルスを配付する手段として、Web サイト改ざんによるドライブ・バイ・ダウンロード攻撃よりも、ファイルを添付してメールで送る方法が主流になってきていること」を挙げている。日本 IBM 社も Tokyo SOC におけるドライブ・バイ・ダウンロード攻撃の検知数は 2017 年上半期 234 件、下半期 67 件と 2016 年 1 月以降減少傾向にあると報告している。

JPCERT/CC は、Web サイト改ざんの新たな傾向について、不正に埋め込まれたスクリプトによって偽の警告を表示するサポート詐欺のサイトに転送させたり、仮想通貨の不正マイニングを実行させたりする事例を報告している。Web サイト改ざんの攻撃自体は形を変えながらも継続しており、その目的はウイルスの配布、特定の Web サイトへの誘導、仮想通貨の不正マイニング等、多岐にわたる。Web サイトの閲覧者にも被害が及ぶこともあるため、減少傾向にあるとは言え今後も継続的な対

策が必要である（「1.2.3 Web サイト改ざんによる被害」「1.2.5（2）偽警告・偽サイト等の詐欺による金銭被害」「1.3.7 偽警告・偽サイト等の詐欺」参照）。

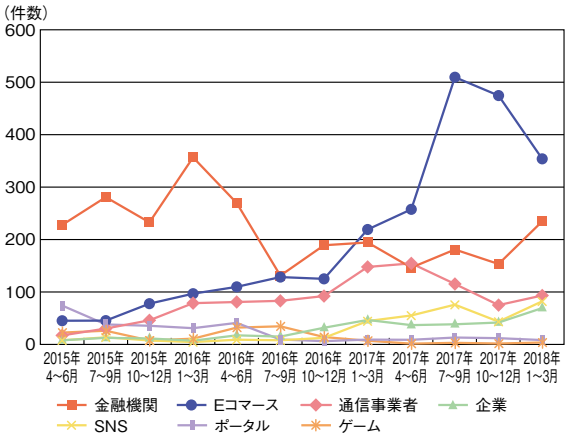
(3) フィッシングによる被害

個人情報やクレジットカード番号、銀行口座番号等の各種サービスの認証情報の詐取を目的としたフィッシング詐欺が継続している。フィッシング対策協議会への報告件数は、2017 年度は 1 万 1,205 件で 2016 年度の 6,656 件より大幅に増加した（図 1-1-12）。



■図 1-1-12 フィッシングの報告件数推移
（出典）フィッシング対策協議会「月次報告書」（2015 年 4 月～ 2018 年 3 月）を基に IPA が作成

JPCERT/CC で集計したフィッシングサイトのブランド別件数の推移を見ると、2015 年度に多かった「金融機関」をかたったフィッシングは 2016 年度に減少した。多くの金融機関でフィッシング対策が進んだことが減少の一因であると思われるが、その後は横ばいとなっており、引き続き注意が必要である。2017 年に入ると「E コマース」の件数が急増して「金融機関」を上回っており、2017 年上期には過去最多となった（図 1-1-13）。



■図 1-1-13 フィッシングサイトのブランド別件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2015 年 4 月 1 日～ 2018 年 3 月 31 日）を基に IPA が作成

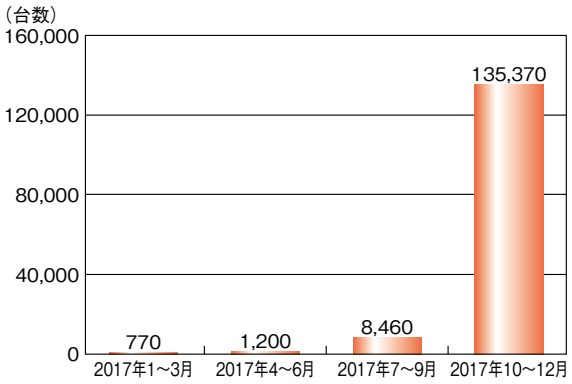
フィッシング対策協議会には Microsoft 社、Apple Inc.、Amazon.com, Inc.、LINE Corporation 等の身近なサービスをかたったフィッシングについて、繰り返し報告されている。特に 2017 年度は Apple Inc. をかたるフィッシングの報告が多く、10 月の報告の 70% を占めた。また、2017 年度になり、仮想通貨関連サービスをかたるフィッシングの報告が増え始め、2018 年に入りフィッシングメールが急増している。フィッシング対策協議会は 2017 年 11 月に仮想通貨取引所 bitFlyer、2018 年 3 月に同取引所 bitbank をかたるフィッシングに対して注意を呼びかけた※19（フィッシングについては「1.2.5（2）（d）フィッシングによる被害」「1.3.7（4）フィッシングの手口と対策」参照）。

(4) 注目された新たな脅威

2017 年度にメディア等で大きく取り上げられた脅威として「ビジネスメール詐欺」と「仮想通貨の流出」が挙げられる。ビジネスメール詐欺は米国の連邦捜査局（Federal Bureau of Investigation：FBI）が 2013 年に注意喚起しており、海外では既に被害が報告されていたが、2017 年 12 月に大手航空会社が国内のビジネスメール詐欺事例で最大となる 3 億 8,000 万円を超える被害を公表したことから、日本でも注目を集めた。また、2018 年 1 月には取引所への不正アクセスにより、過去最大級の約 580 億円分の仮想通貨が流出するというインシデントが発生した（ビジネスメール詐欺については「1.2.5（1）ビジネスメール詐欺による金銭被害」「1.3.6 ビジネスメール詐欺」、仮想通貨については「3.2 仮想通貨の情報セキュリティ」参照）。

仮想通貨に関する脅威では流出事件以外にも、仮想通貨の不正マイニングが注目された。トレンドマイクロ社の報告によれば一般のインターネット利用者に意図しないマイニングをさせるツール「コインマイナー」を拡散させる脆弱性攻撃サイトが 2017 年 5 月から急増した。また、9 月に「Coinhive」が登場し、攻撃者がこれを悪用するようになると、コインマイナー検出台数は過去最多となった。Coinhive は、Web サイト閲覧者のパソコンでマイニングを行うことで、広告の代替となる収益を Web サイトの運営者に提供するサービスであるが、この仕組みを悪用して容易に不正マイニングの実行が可能になる※20。これが不正マイニングに拍車をかけ、10 ～ 12 月の 3 ヵ月間だけで 13 万 5,370 台が検出されることとなった（次ページ図 1-1-14）。

2017 年に世界で猛威を振るったランサムウェアは、図



■図 1-1-14　日本における「コインマイナー」の検出台数推移
（出典）トレンドマイクロ社「2017 年年間セキュリティラウンドアップ」を基に IPA が編集

1-1-1（9 ページ）の Wanna Cryptor の検出台数推移に示されるように日本でも多数検出された。しかし、日本 IBM 社は Tokyo SOC での検出状況から、国内では感染を試みる攻撃の影響は限定的であり、アクセス制御により攻撃に利用される通信が成立しなかったことが一因であると推測している。他方トレンドマイクロ社がオンライン検索エンジン「Shodan」を使用し、Wanna Cryptor の感染拡大に利用されるポート 445 が露出している国内の Windows 機器の台数を確認したところ、2017 年 5 月時点でおよそ 3 万台、その後 12 月時点でおよそ 5 万台が確認された。これは現在も不要なポートを露出させたまま機器を使っている利用者が多いことを示し、Wanna Cryptor の継続的な拡散につながりかねない大きなセキュリティ上の課題であるとしている。引き続き、ランサムウェアへの警戒が必要である（ランサムウェアについては「1.2.1 ランサムウェアによる被害」「1.3.1 ランサムウェアによる攻撃」参照）。

1.2 情報セキュリティインシデント別の状況と事例

本節では、インシデント別の発生状況と、具体的な事例について述べる。

1.2.1 ランサムウェアによる被害

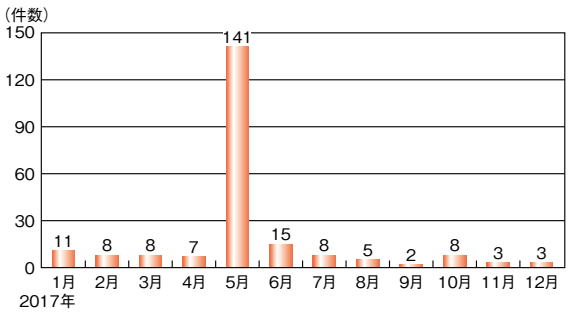
ランサムウェアとは「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、パソコン内のファイルを暗号化する、または画面ロック等によりパソコンを使用不可にするウイルスの総称である。それらの復旧を条件に身代金を支払うように促す脅迫メッセージを表示するソフトウェアであることから、ランサムウェアと呼ばれている。

2017年も様々な新しいランサムウェアが登場したが、初めてネットワークを介して感染拡大を図る自己増殖機能を持つランサムウェアが確認された。国内でも感染事例の多かった「Wanna Cryptor」を始め、「NotPetya」「Bad Rabbit」と呼ばれる自己増殖機能を持ったランサムウェアの登場が大きな話題となった。

本項では特に自己増殖型のランサムウェア被害について述べる。

(1) Wanna Cryptor による被害

2017年5月には、世界各国でWanna Cryptor（別名 WannaCry、WannaCrypt、Wcry）の感染被害が発生し、IPAでも注意喚起※21を行った。Wanna Cryptorは国内でも多数の被害が確認され、IPAにも同年5月には当該ランサムウェアに関する相談が多く寄せられた（図1-2-1）。



■図1-2-1　ランサムウェアに関する月別相談件数推移

Wanna Cryptorが猛威を振るった一因として社内ネットワークやインターネットを介して感染拡大を図る自己増殖型であったことが挙げられる。自己増殖機能を持ったランサムウェアとしてはWanna Cryptorが初めての事例であり、組織がいったんWanna Cryptorに感染してしまうと社内ネットワークを経由して感染が拡大し、社内システムに大きな影響を与える。実際に株式会社日立製作所や東日本旅客鉄道株式会社（JR東日本）等の複数の企業でWanna Cryptorの感染が社内システムに影響を与えたという事例が報告されている※22。

Wanna Cryptorの自己増殖機能は、Windowsで利用されるSMBv1と呼ばれるプロトコルの脆弱性（CVE-2017-0144）を悪用したものである（「1.3.1 (1) エクスプロイトキットの自己増殖機能による攻撃」参照）。

セキュリティベンダによると、同時期にインターネット上でSMBが有効になっていたWindows環境は全世界で50万件以上が確認されている※23が、この脆弱性については2017年3月の時点で既にWindowsの修正プログラム（MS17-010）が公開されている。Windows Updateにより最新の修正プログラムが適用されていればWanna Cryptorには感染しない状況であった。しかし、世界中で企業や個人が感染した事例が多数報告されており、Windows Updateによる修正プログラムの適用が実施されない端末が多くインターネットに接続されていることが浮き彫りになった。

(2) NotPetya による被害

2017年6月にもWanna Cryptorと同様に自己増殖機能を持ったNotPetya※24（別名 Petya、Petya亜種、GoldenEye）の感染が、ウクライナを中心に拡大した。ただし、NotPetyaの感染は同一ネットワーク内のみであり、インターネット上への自己増殖活動は確認されておらず、国内への流入は限定的であったと推察される。IPAへもNotPetyaに感染したという被害相談は寄せられていない。海外の被害事例では、デンマークの海運企業においてNotPetyaへの対応コストが約300億円に上ったと発表された※25。NotPetyaの主な初期感染経路は、ウクライナで利用されている会計ソフト「M.E.Doc」のアップデート機能を悪用した攻撃であると推察される。

(3) Bad Rabbit による被害

2017年10月には同一ネットワーク内で自己増殖する機能を持ったBad Rabbit※26の感染拡大が主にロシア等で確認された。ネットワーク内で感染を広げる手口とし

ては NotPetya と同様であり、インターネット上への自己増殖活動は行われないため、Bad Rabbit についても国内への流入は限定的であると推察される。IPA へも Bad Rabbit に関する被害相談は寄せられていない。Bad Rabbit の主な初期感染経路は、偽装した Adobe Flash Player のインストーラにより、当該ランサムウェアを配布する悪意のある Web サイトへ誘導し、そこから当該ランサムウェアをダウンロード及び実行させて感染させるというものであった。また、一般の Web サイトが改ざんされ、ランサムウェアダウンロード用の Web サイトへ誘導するコードを埋め込まれる事例が複数の国で確認され、日本でも Web サイトの改ざん被害が 1 件報告されている※27。

2017 年は自己増殖機能を持ったランサムウェアが大きな話題となったが、それ以外にも Microsoft Internet Explorer や Adobe Flash Player の脆弱性を悪用した攻撃でランサムウェアが拡散※28 されたり、従来のランサムウェアに仮想通貨を窃取する目的の機能が追加※29 されたりする等、ランサムウェアの多様化やバージョンアップは続いている。今後もランサムウェアに対する警戒が引き続き必要である。

1.2.2 サービス妨害を狙った攻撃による被害

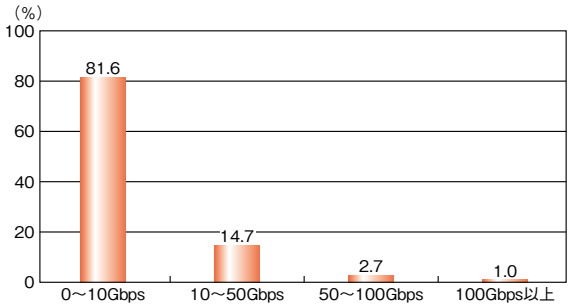
単一の発信元から Web サイトや Web サービスに対し、大量のアクセスを集中させる等してサーバやネットワークに負荷をかけたり、サーバの脆弱性を悪用したりして、正常なサービスを提供できなくする攻撃を DoS（Denial of Service）攻撃と呼ぶ。また、ルータ等の多数のネットワーク機器の脆弱性を悪用し大量の通信パケットを発生させたり、ウイルスを多数の端末に感染させ、感染した端末から同時に攻撃対象にアクセスを行わせたりする攻撃を特に DDoS（Distributed Denial of Service）攻撃という。

近年の DoS 攻撃は、特定の主義主張の表明として関係組織を攻撃すること（ハクティビズム）以外にも、金銭を脅し取ることを目的として行われている。このような状況を後押しする原因の一つとして、DDoS 攻撃請負業者による DDoS 攻撃のサービス化が挙げられる。攻撃を請け負うサービスは「booter」と呼ばれており、表向きには負荷テストを実施する代行業者を装っている。しかしながら、実際には犯罪にも利用されており、企業が DDoS 攻撃請負業者によって攻撃された事例も存在する。

更に、ウイルスの大量感染による DDoS 攻撃では、2016 年に IoT 機器を対象とした「Mirai」と呼ばれるウイルスが流行し、米国等で猛威を振るった。ネットワークに接続される機器が増加し、企業のみならず、個人でも IoT 機器を利用することが増えている。これらの機器について適切なパスワードの設定やファームウェアのアップデート等を実施し、攻撃の踏み台として悪用されないようにすることが利用者に求められている。

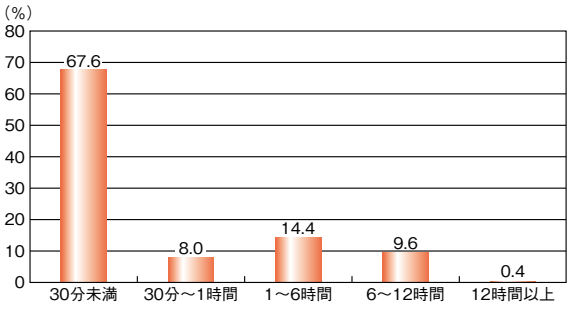
(1) DDoS 攻撃の傾向

Imperva の報告によると、2017 年第 4 四半期に観測された攻撃では、通信量が 50Gbps を超える攻撃が全体の 3.7% となり（図 1-2-2）、最大の攻撃では通信量が 335Gbps に達したという。



■図 1-2-2　2017 年第 4 四半期の DDoS 通信量の割合
（出典）Imperva「Global DDoS Threat Landscape Q4 2017※30」を基に IPA が編集

また、観測された攻撃の 67.6% は 30 分未満の攻撃となっており、極めて短期間に大量の通信が発生したとしている（図 1-2-3）。



■図 1-2-3　2017 年第 4 四半期の DDoS 攻撃期間
（出典）Imperva「Global DDoS Threat Landscape Q4 2017」を基に IPA が編集

加えて、Imperva の報告では、攻撃の対象となった企業のうち 2 回以上攻撃を受けた企業は 67.4% となっており、多くの企業が何度も攻撃に晒されたとしている。この理由としては、1 回の DDoS 攻撃を実行する費用が少なく、攻撃者は攻撃対象組織の対策を破るために様々な方法を試すことができる、ということが挙げられる。

Cisco Systems, Inc. のセキュリティ調査部門「Talos」が公開したレポート※31 によれば、中国のアンダーグラウンドマーケットで DDoS 攻撃の代行サービス市場が拡大しており、2017 年の上半期だけで 30 種類以上のサービスが見つかったとしている。サービス利用金額は 1 日で 20 人民元、1 ヵ月で 400 人民元だったという。DDoS 攻撃がサービス化していることで、攻撃のためのウイルス開発や、多数の端末の乗っ取り等の事前準備が必要なく、簡単に DDoS 攻撃を行えるようになっている。

また、2017 年 8 月には一見無害なアプリを装い、実際にはインストールされた Android 端末を DDoS 攻撃の踏み台にするアプリが多数発見された。複数のセキュリティベンダによる調査※32 の結果、Google Play 上で配信された不正なアプリが約 300 本見つかり、Google LLC はアプリの削除等の対応を行った。これらのアプリには「WireX」と呼ばれるウイルスが含まれており、アプリを一度起動させると、画面がロック状態やスリープ状態になっていてもバックグラウンドで動作する機能が実装されていた。更に、アプリがインストールされた端末間でボットネットを形成するようになっていたという。実際にこのボットネットを悪用した攻撃が、2017 年 8 月 2 日ごろから観測され、8 月 17 日に大規模な攻撃が行われたとしている。普段利用するスマートフォン等が攻撃の踏み台として悪用され、利用者が気付かないうちに攻撃に加担している可能性がある（スマートフォンのセキュリティについては「3.3 スマートフォンの情報セキュリティ」参照）。

(2) DoS 攻撃による被害事例

実際に発生した DoS 攻撃による被害事例について解説する。

(a) 金融サービスにおける被害事例

DDoS 攻撃は、Web サイトや Web サービスを利用できなくすることで、攻撃対象に対し事業機会の損失による金銭被害を与える。EC サイト等が代表的な攻撃対象となるが、近年では為替等の取引もインターネット上で行われることが主流である。常に利用できることが求められる取引所が DDoS 攻撃で停止した場合、EC サイト以上に甚大な金銭的被害が生じることが予想され、十分な備えが必要である。

2017 年 9 月に国内で FX 事業を行う複数企業の Web サイトに対し、DDoS 攻撃が行われた※33。これらの攻撃は 2 ～ 12 時間の長時間にわたり、FX 取り引きに影響が出たとされている。これらの企業では、攻撃の開始前に英文で攻撃の停止と引き換えに金銭を要求する脅迫メールが届いていたとされる。これに関しては、国内で同様の被害報告が確認されており、JPCERT/CC からも情報が公開されている※34。

海外では仮想通貨の取引所を標的とした DDoS 攻撃が観測されており、これによって仮想通貨の価格が大幅に下落したという被害が報告されている※35。

(b) 脆弱性を悪用した DoS 攻撃の被害事例

DoS 攻撃を行う際に、対象の組織が使用しているサーバソフトウェアやネットワーク機器の脆弱性を悪用し、被害を与える手口が存在する。このため、使用している製品に脆弱性が見つかった場合は速やかにアップデート等の対応を行う必要がある。

2017 年は、株式会社インターネットイニシアティブ（IIJ）や Cisco Systems, Inc. 等のルータに特定のパケットを受け付けることでサービス停止状態になってしまう脆弱性が発見され、メーカによる対応が行われた※36。これらの脆弱性を放置した場合、当該パケットを送り付けるような DoS 攻撃によって、組織内でネットワークが利用できなくなる、あるいはインターネットから Web サイトを閲覧できなくなるといった被害が想定される。

2016 年には、IoT 機器を狙ったウイルスである Mirai により、Twitter や Amazon 等の Web サイト、Web サービスが停止するという被害が発生した※37。2016 年の被害では、利用が拡大していたネットワークカメラ等の IoT 機器で、出荷時からログイン用のパスワードが固定され利用者によって変更ができなかったり、利用者が初期設定のパスワードのまま変更せずに利用していたりといった仕様や設定不備を悪用され感染が広まったとされる。

2017 年にはこのようなウイルスによる深刻な被害の報告はないが、いくつかの企業から Mirai の亜種が日本国内で感染拡大しているとの報告※38 や、ネットワーク通信を行う車載機器に Mirai の亜種が感染していることが確認されたとの報告※39 がある。海外でも Mirai の亜種の拡大が報告されており、大学に対し 54 時間にわたって DDoS 攻撃が行われた事例がある※40。このような報告から、Mirai の脅威はまだ収束しておらず、引き続き警戒が必要である（Mirai の亜種については「3.1.1 多様化する IoT のセキュリティ脅威」参照）。

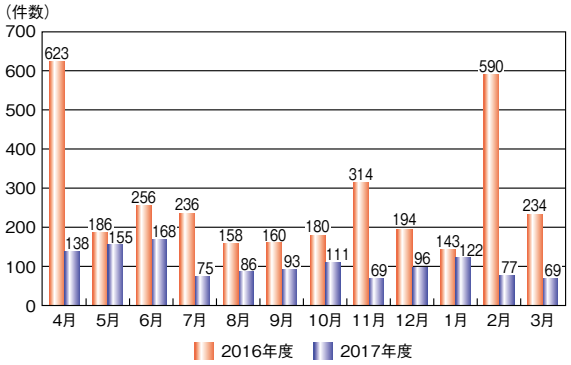
1.2.3 Webサイト改ざんによる被害

Web サイト改ざんの被害件数は、2016 年度に比べると減少しているが、2017 年度も継続して確認されている。

(1) Web サイト改ざんの被害状況

JPCERT/CC の報告※41 によると、2017 年度の「Web サイト改ざん」のインシデント件数は前年度と比べて減少傾向にある。2016 年度との比較を図 1-2-4 に示す。

具体的な被害としては、重大な被害を与えるランサムウェアの配布元として悪用するために改ざんされた等の事例が確認されている。



■図 1-2-4　2017 年度に報告された Web サイト改ざん件数（2016 年度比較）
(出典)JPCERT/CC「JPCERT/CC インシデント報告対応レポート」を基に IPA が作成

(2) Web サイトの改ざん事例

2017 年 6 月に WordPress のプラグイン「WP Job Manager」を使用した国内の複数の Web サイトにおいて、本プラグインの脆弱性を悪用した攻撃が確認された※42。ログイン権限のない第三者によって、画像ファイルをアップロードされ、ページが改ざんされるという被害が発生した。このような被害は閲覧者への直接的な影響はないが、修正のためのサービス一時停止や Web サイトを公開している組織への信用失墜につながる可能性がある。

2016 年 2 月から 2017 年 3 月にかけて、Web サイトが不正アクセスにより改ざんされ、ページを閲覧するとウイルスに感染するという状態で公開されていた事例が発生した※43。感染被害は不明であるが、約 1 年にわたってウイルス配布元の Web サイトとなっていた。

2017 年 8 月には、自由党の Web サイトが改ざんされる事例が発生した※44。ページごとに不正なコードが書き込まれ、海外の広告サイトや通販サイトへ転送されるようになっていた。

Web サイト改ざんの被害は、どの組織、どの個人においても起き得ることである。Web サイトを公開している組織、個人は、Web ページを改ざんされた「被害者」というだけではなく、ウイルス配布の「加害者」になる危険性もある。そうならないためにも、Web サイトで使われているプログラムやバージョン情報等を把握し、日々情報収集を行い、問題が見つかった際には修正プログラムの適用等の対策を実施することが重要である。

(3) 改ざんした Web サイトによるウイルス配布

2017 年度は 2016 年度と比較して、Web サイトの改ざんの件数は減少傾向にある。その理由として、ウイルス配布の手段として、メールの添付ファイルが主流になってきているためと推察される。しかし、Web サイトが改ざんされ、ウイルス配布に悪用される事例も継続して発生している。

2017 年 10 月には、「Bad Rabbit」と呼ばれるランサムウェアの被害が発生した(「1.2.1 (3) Bad Rabbit による被害」参照)。国内の企業においても、Web サイトが改ざんされ、偽の Adobe Flash Player のインストーラをダウンロードさせることで、Bad Rabbit に感染させる事例が報告された※27。ファイアウォールのアクセス制御の設定が不十分だったこと、SSH※45 の脆弱性が残存していたことが、Web サイトを改ざんされた原因であると被害企業は発表している。

(4) 偽の警告を表示する Web サイトへのリダイレクト

2017 年度に増加している被害として、改ざんした Web サイトから不正な Web サイトへリダイレクト（自動転送）させ、ウイルスに感染したという偽の警告を表示することによって、偽のサポート窓口への電話を促す事例が確認された。偽警告には Microsoft 社をかたるものもあり、偽のサポート窓口に電話させ、遠隔操作ソフトのインストールをさせる、不要なサポート料金を支払わせる、クレジットカード情報等を騙し取る等の手口が確認されている※46。このような電話に誘導する手口は頻繁に変わり、また巧妙化している。そのため、現在どのような被害が流行っているのか等の情報を収集し、被害に遭わないように注意することが重要である（手口については「1.3.7 (1) 偽警告の手口と対策」参照)。

1.2.4 情報漏えいによる被害

2017 年度も情報漏えいによる被害が多発している。本項では、外部からの攻撃、内部者の不正、不適切な運用の三つの要因による漏えい被害の状況について述べる。

(1) 外部からの攻撃による情報漏えい

管理や対策が不十分なサーバの脆弱性を狙った、外部からの不正アクセスによる情報漏えい被害が発生している。被害の中には、氏名や生年月日、電話番号、メールアドレス等の情報だけでなく、パスワードやクレジットカード情報まで窃取された事例もある。

ジャパン・フード & リカー・アライアンス株式会社の事例では、連結子会社である東洋商事株式会社が運営している通販サイト「東商マート」が外部からの SQL インジェクション攻撃を受け、氏名、住所、電話番号、メールアドレス等の情報、最大 4 万 9,468 件（クレジットカード情報 2 件を含む）が流出した可能性がある※47。

ぴあ株式会社の事例では、ぴあ株式会社が運営を受託している公益社団法人ジャパン・プロフェッショナル・バスケットボールリーグ（以下、B.LEAGUE）のチケットサイト、及びファンクラブ受付サイトのサーバ環境が Apache Struts2 の脆弱性を悪用した不正アクセスを受け、氏名、電話番号、生年月日、ログイン ID、パスワード、メールアドレス等、最大 15 万 4,599 件（クレジットカード情報 3 万 8,695 件を含む）が流出した可能性がある※48。公表された内容によると、ぴあ株式会社は、2017 年 3 月 10 日に IPA から発信された注意喚起（2017 年 3 月 8 日公表）※49 により Apache Struts2 に脆弱性が存在することは認識していたが、ぴあ株式会社がサイト開設と運営を再委託した企業に対して発注時に提示した資料及び運用ガイドラインに基づき、B.LEAGUE のチケットサイト及びファンクラブ受付サイトのサーバ上にクレジットカード情報は保管されていない、と認識していた。しかし、2017 年 3 月 17 日ごろから Twitter 上でクレジットカード情報の不正利用に関する複数の書き込みが確認され、外部の調査会社による調査の結果、2017 年 3 月 7 ～ 15 日の間に Apache Struts2 への攻撃による Web サーバ及びデータベースサーバへの不正アクセスの痕跡が確認され、情報流出が発覚した。

ぴあ株式会社の発表によれば、発注時に提示した資料及び運用ガイドラインに反して、B.LEAGUE のチケットサイトのデータベース上及びファンクラブ受付サイトの通信ログ上に情報が不適切に保存されていたという。再発防止策として Apache Struts2 のバージョンアップを実施するとともに、すべての現行システムとその運用に対するガイドラインの見直しと安全点検、監視の強化を進めるとしている。

2017 年は、ぴあ株式会社の他にも Apache Struts2 の脆弱性を悪用した攻撃による情報流出の被害が複数確認されている。

ジェネシス・イーシー株式会社の事例では、運営するストア構築パッケージ「Genesis-EC」を導入している複数の Web サーバが不正アクセスを受け、クレジットカード番号、有効期限、セキュリティコード等、最大 9,458 件が流出した可能性がある。また、外部の調査会社が調査した結果、サーバ内に 2009 年 3 月以前に顧客が利用したクレジットカード番号、有効期限、セキュリティコード、カード名義人名、及び電話番号等、最大 4,581 件が不適切に保管され、流出した可能性があることが判明した※50。

GMO インターネット株式会社の事例では、同社が運営するサイト売買仲介サービス「サイト M&A」がサイバー攻撃を受け、会員情報等、1 万 4,612 件が流出した可能性がある※51。流出した情報は、アマゾンジャパン合同会社が運営する「Kindle ストア」で 2017 年 11 月 1 日昼ごろまで電子書籍として販売されていた※52。

国立大学法人大阪大学（以下、大阪大学）の事例では、管理している教育用計算機システムが不正アクセスを受け、ID、氏名、所属、同大学発行のメールアドレス、入学年度、学籍番号等、最大 8 万 1,107 件（最大約 3,586 件の人事情報、給与情報等を含む）が流出した可能性がある※53。公表された内容によると、2017 年 5 月 18 日～ 7 月 4 日の間に、教職員の ID を利用した教育用計算機システムへの不正ログインによりシステム内部に不正プログラムを仕掛けられ、同システムの管理者 ID が盗まれたことで利用者情報が漏えいした。また、学内グループウェアにおいても教職員の ID を利用した不正ログインにより、当該教職員のメールに含まれる個人情報が漏えいした可能性があることが判明した。再発防止策として、アカウント情報の適正管理について改めて周知徹底するとともに、パスワードルールを強固にした上ですべての利用者のパスワード変更を実施した。

その他、外部からの不正アクセスにより情報漏えいが発生した主な事例を表 1-2-1（次ページ）に示す。

(2) 内部者の故意による情報漏えい

IPA が発表する「情報セキュリティ 10 大脅威」では、

組織名	公表日	被害内容
総務省	2017 年 4 月 13 日	政府統計の総合窓口「e-Stat」の一つの機能である「地図による小地域分析（jSTAT MAP）」が Apache Struts2 の脆弱性を悪用した不正アクセスを受け、登録情報約２万 3,000 件及び、利用者がアップロードしたデータが流出した可能性がある※54。
国立研究開発法人 情報通信研究機構	5 月 2 日	同機構が作成した音声対話研究用のソフトウェア開発キット「MCML 音声インタラクション SDK」を外部の研究者等に提供する公開サーバが Apache Struts2 の脆弱性を悪用した不正アクセスを受け、利用者の ID、メールアドレス、暗号化されたパスワード情報等、最大 378 件が流出した可能性がある※55。
国土交通省	6 月 6 日	「土地総合情報システム」の一つの機能である「不動産取引価格アンケート回答（電子回答）」サイトが Apache Struts2 の脆弱性を悪用した不正アクセスを受け、最大 4,335 件の回答者情報、及び最大 19 万 4,834 件の売買等に関わる所有権移転登記情報（登記名義人の名称を除く）が流出した可能性がある※56。
大阪大学医学部附属病院	6 月 26 日	同大学の医学系研究科 博士課程の学生が使うフリーメールアカウントへの不正アクセスにより、患者の氏名、年齢、ID、病気の状態、治療の状況、検査内容・数値等、最大 220 件が流出した可能性がある※57。
株式会社マネースクウェア・ジャパン	7 月 17 日	同社のホームページがサイバー攻撃を受け、利用者の氏名、メールアドレス、ID 番号等、最大約 2,500 件が流出した可能性がある※58。
東京メトロポリタンテレビジョン株式会社	10 月 4 日	同社のホームページサーバがサーバ内プログラムの脆弱性を悪用した不正アクセスを受け、メールアドレス、ニックネーム、最大約 37 万件（氏名約 1,270 件を含む）が流出した可能性がある※59。
株式会社ほくやく・竹山ホールディングス	10 月 11 日	同社の連結子会社である株式会社アドウイックの医療機関用待ち時間短縮システム「シマフクロウ・シリーズ」の Web サイトのサーバが不正アクセスを受け、氏名、診察券番号、電話番号、メールアドレス、一部の生年月日、予約日と時間、最大 59 万 7,452 件が流出した可能性がある※60。

■表 1-2-1　不正アクセスによる情報漏えいの主な事例

「内部不正による情報漏えい」が 4 年にわたって取り上げられており※61、内部者の故意（以下、内部不正）による情報漏えいは継続して大きな脅威として認識されている。

内部不正は、持ち出された秘密情報の他社による盗用や別犯罪への利用等により、組織の信用や利益に直接影響を与える重大な脅威である。また、内部不正によって漏えいした情報が個人情報であった場合、当該個人の安全や財産を脅かす事態にも発展しかねない。

以下に、内部不正の事例及び対策等を紹介する。また、表 1-2-2 に 2017 年度に報道された国内での内部不正事件の主な事例を示す。

(a) 状況と事例

内部不正は、行為者自身の金銭的欲求や特定個人への強い関心等が動機となることが多い。しかし内部不正の要因が、必ずしも行為者自身の欲求だけが動機とは言えない事例も見受けられる。

2017 年 6 月に株式会社佐賀銀行（以下、佐賀銀行）は、元行員が在職中に高額預金者の個人情報 169 件を持ち出したことを公表した※62。当該元行員は 2016 年に犯した現金窃盗事件等で逮捕及び懲戒免職されており、持ち出した個人情報はそのときの共犯者であるヤミ金業者へ提供された疑いがある。当該元行員には多額の借金があり、公判で一連の事件での共犯者であるヤミ金業者から脅迫されていたと主張した。本事例で漏えいした個人情報は大量ではなかったが、佐賀銀行では 5 月に情報漏えいが発覚して以降、高額預金者による解約、他行への預金の移し替え等が相次ぎ、2017 年末までにその総額は 10 億円を超えた※63。

表 1-2-2 の事例 4 も、行為者達が同僚であったときに発生した業務上のトラブルから行為者間での脅迫行為に至り、内部不正にまで発展している。

前述のように事業に大きな悪影響を与える事例が発生する一方で、適切な対策により実質的な情報漏えいを防いだ事例もある。2018 年 1 月、DMG 森精機株式会社は、2017 年 8 月に子会社に勤務する営業担当従業員が、自社製品の据付情報（客先納入製品の機種・機番・納入時期）約 300 社分を印刷して持ち出したことを公表した※64。同社のリスク管理システムが事態を直ちに検知してすべての印刷物が迅速に回収されたため、外部への情報漏えいはなかったと考えられている。

(b) 有効な対策

IPA が公開している「組織における内部不正防止ガイドライン※73」では、内部不正対策として 10 の観点から 30 項目の対策を提示している。経済産業省が公開している「秘密情報の保護ハンドブック※74」にも、従業員及び退職者向けの情報漏えい対策例が記載されている。

事例番号	報道時期	行為者（発覚時）	概要
1	2017 年 5 月	元従業員	株式会社スタッフサービスの元従業員が、自分が立ち上げた人材派遣業の営業に利用するため、過去 3 年にわたり在職中に登録者の個人情報（氏名や住所、電話番号、メールアドレス等）1 万 5,368 名分を持ち出した。同社は元従業員のパソコンから情報を回収した※65。
2	2017 年 6 月	職員	熊本県荒尾市の男性職員が、過去 3 年にわたり住民情報システムを不正使用して職員の個人情報を取得していた。不正取得した情報を利用して女性職員にストーカー行為を行い、懲戒免職処分を受けた。市長、副市長が監督責任を取って減給処分となった※66。
3	2017 年 6 月	契約社員	ゲーム会社である株式会社 Aiming の契約社員が、自社開発スマートフォンゲームの利用者アカウント約 70 個を不正取得し転売した。同社員は懲戒解雇され、詐欺等の容疑で逮捕された※67。
4	2017 年 6 月	職員 退職者	日本年金機構職員と無職男性（同職員の元上司で社会保険庁職員 OB）が共謀し、過去 5 年にわたり個人情報が印刷された書面計 558 枚を持ち出した。職員は懲戒免職され、窃盗と加重収賄で逮捕された。地裁で懲役 3 年、執行猶予 4 年、追徴金 7 万 5,000 円の判決を受けた。機構内の情報漏えい防止検査で、当該職員の机から無職男性宛の郵便物が見つかったことから判明した※68。
5	2017 年 8 月	元従業員	千葉県東金市の会社員が 2016 年 7 月に数回にわたり、当時勤務していた土木建築会社から貸与されていたパソコンを不正に操作し、同社が営業秘密として管理する顧客データをクラウドサービス上へコピーし持ち出した。会社員が同年 7 月に退社後、同社役員が貸与していたパソコンを調べたところ「データどろぼう」というファイルが見つかり、同年 12 月に警察へ相談した。 会社員は 2017 年 8 月に不正競争防止法違反（営業秘密侵害）の疑いで書類送検された。会社員は同年 7 月から元同僚男性が設立した同業他社で掛け持ちして働くようになり、「同業他社への移籍を見越してデータを盗んだ」等と容疑を認めているという※69。
6	2017 年 9 月	委託先 派遣社員	株式会社ビューカードがコールセンター業務を委託した企業の派遣社員が、クレジットカード番号等の個人情報を印刷し外部に持ち出した。持ち出したクレジットカード情報を利用して商品を不正に購入した容疑により逮捕された※70。
7	2017 年 11 月	元従業員	株式会社ゼネテックの元従業員が、取引情報を無断で社外へ持ち出した。同社は事態把握後、警察へ通報し、告訴手続きを取った※71。
8	2018 年 2 月	従業員	株式会社レオガーデンの営業職従業員が、顧客情報を含むデータ（資金計画書、建築図面等の業務書類のほか、事業計画書、同社保有物件データ等）約 2 万 6,000 人分を、第三者に提供する目的で不正に持ち出した。社内定期点検により、外部オンラインストレージへのアップロードが判明した。同社は当該従業員を懲戒解雇し、不正競争防止法違反により刑事告訴予定である※72。

■表 1-2-2　2017 年度に報道された内部不正事件（報道または公表事例を基に IPA が作成）

DMG 森精機株式会社の事例では、同社のリスク管理システムが「どのような資料を何枚印刷したか等」の記録に基づきアラームを発したものと推測される。表中の事例 8 のように、「情報漏えい行為につながり得る兆候がないか」を定期的に監査することも、内部不正の早期検知及び実質的な情報漏えい防止に有効であると考えられる。

また、内部不正に至る要因が個人的な欲求だけではなく職場での人間関係や行為者の私生活でのトラブルに端を発する場合もある。佐賀銀行の事例では、再発防止策として閉店後の行員の再入店等を禁止した。また、佐賀県内の別の金融機関は当該事例を踏まえ、職員を対象にした定期的な面談に力を入れるようになったという※63。経済産業省が発行した「秘密情報の保護ハンドブック」に記載されているように、コミュニケーションを取りやすい職場環境を整備すること等により、トラブルを相談する心理的負担を減らすことも有効と考えられる。

(3) 不適切な運用による情報漏えい

Web サイトにおける提供対象外機能やファイルのアクセス制限なし公開、使用ソフトウェアの脆弱性放置、個人情報を提供した委託先の不適切な管理等の不適切な運用による情報漏えいも発生している。

(a) 状況と事例

2018 年 3 月に日本年金機構がデータ入力を委託した株式会社 SAY 企画（以下、SAY 企画）が、契約に反し無断で業務を中国の関連事業者へ再委託していたことが発覚した※75。本件では、委託先である SAY 企画が当初契約を大幅に下回る人員体制で業務を実施していたことや、日本年金機構が契約違反である業務再委託を把握した後も SAY 企画へ業務を委託し続けていたことが報道されており※76、委託元、委託先の双方で不適切な運用がなされていたと考えられる。なお中国の関連事業者への外部監査の結果、データ入力に利用された申告書の氏名部分のみを切り出した画像データは適切に破棄されたという。本件に関連し、日本年金機構は SAY 企画に対し 3 年間の競争参加資格停止及び資格停止期間経過後、業務改善が十分に図られたと年金機構が判断するまで、競争入札への参加制限を実施した。

また海外では、2018 年 3 月に、SNS プラットフォーム

である Facebook 上で取得された個人情報が不正利用されたことが報道された※77。報道によると本件では、2014 年に Facebook 上のアプリでのアンケートに同意の上回答した 27 万人及びその友達を含む最大 8,700 万人の個人情報を取得した研究者が、当該個人情報を Facebook, Inc. の情報管理ポリシーに反して調査会社である Cambridge Analytica と共有した。Facebook, Inc. は 2014 年に友達の情報取得を制限する API の仕様変更を実施した※78 が、制限なく情報を取得できる旧 API 及びそれを利用するアプリは 1 年後まで利用可能な状態にあった。2015 年に事態を把握した Facebook, Inc. は、当該アプリの公開を停止し研究者へ情報の削除を求めたが、実際には情報は削除されておらず、当該情報は英国の欧州連合離脱是非を問う国民投票や 2016 年の米国大統領選挙での世論形成に利用された可能性があるとも報道されている（不正流用とその影響については「2.3.2 (7) 個人情報保護・世論誘導に対する規制強化の可能性」参照）。

2017 年度に報道された不適切な運用による情報漏えいのうち、その他の国内と海外の主な事例を表 1-2-3 に示す。表に挙げた事例の原因を見ると、委託先での契約違反（事例 1、2）、設定不備や作業の失念（事例 3、6、7、8、9）、仕様についての認識誤り（事例 4）、法令違反（事例 5）等、業種や事業規模、あるいはデータの種別に関わらず、事業遂行上の作業で発生し得る事象が原因となっている。

(b) 有効な対策

Web サイト等における不適切な運用を防ぐためには、IPA が提案する「日常における情報セキュリティ対策※88」や発行資料※89 に記載された対策の実施が有効であると考えられる。

個人情報等の秘密情報の管理や処理を委託する場合は、委託先が適切に情報を管理するルールを設けて

事例番号	報道時期	概要
1	2017 年 4 月	株式会社ぴあが運営を受託していたプロバスケットボールリーグ「B.LEAGUE」のチケットサイト及びファンクラブ受付サイトが不正アクセスを受け、クレジットカード情報を含む個人情報が流出した。ぴあ社の再委託先である株式会社ききょう屋ソフトと株式会社ホットファクトリーは、発注仕様及び運用ガイドラインと異なり、データベース及び通信ログにクレジットカード情報を不適切に保持していた※48。
2	2017 年 4 月	高知大学医学部附属病院の委託先従業員が、システム障害対応において遠隔操作でシステムログデータを収集した際、収集データに患者の個人情報が含まれていた。遠隔操作に利用したノートパソコンを紛失したことにより、情報漏えいが発覚した。同大は委託契約により情報を作業場所以外へ持ち出すことを禁じていたが、契約に反し収集データをノートパソコンに保存して外部に持ち出していた※79。
3	2017 年 6 月	米国共和党から業務委託を受けていた Deep Root Analytics、TargetPoint Consulting, Inc.、Data Trust の 3 社が収集した米国有権者の個人情報 1 億 9,800 万人分が、自由に閲覧可能な状態になっていることをセキュリティベンダが発見した。これらの個人情報は 12 日間にわたって、アクセス制限がまったくなされない状態でクラウドサービス上に保存されていた※80。
4	2017 年 6 月	株式会社メルカリが運営する Web サービスで、5 時間以上にわたり個人情報が他者から閲覧できる状態になっていた。コンテンツキャッシュに利用する CDN プロバイダの切り替えに際し、株式会社メルカリ側でキャッシュサーバの動作仕様について認識誤りがあり、本来対象ではないデータが CDN にキャッシュされていた※81。
5	2017 年 7 月	スウェーデンの運転免許証、警察・軍関係の機密を含むデータベースに、管理を委託された IBM Sweden の再委託先であるチェコの現地技術者が自由にアクセスできる状態となっていた。 当該データベースの管理は IBM Sweden が受注したが、コスト軽減のためにチェコにサーバを移転し、現地企業に管理を再委託していた。この再委託に際し、スウェーデン政府のセキュリティクリアランス※82 チェックが実施されていなかった※83。
6	2017 年 8 月	旅行会社である株式会社エイチ・アイ・エスの Web サイトから、ツアー申込者最大 1 万 1,975 人分の個人情報が流出した。Web サイト更新に伴う旧サイトでの予約データ移行において、誤って公開領域に予約データを残置したことが原因であった。第三者が当該データをダウンロードしていた※84。
7	2017 年 9 月	株式会社宮地商会が運営する音楽教室のセキュリティシステムにおいて、入力された個人情報が過去 7 ヵ月にわたり Web 上で閲覧可能な状態になっていた。関係者以外には非公表であったシステムの管理者用ページが検索エンジンの検索対象として表示され、閲覧可能になっていた※85。
8	2017 年 10 月	Dell Inc. が、アフターサポート用 Web サイトのドメイン更新を失念し、当該ドメインが 1 ヵ月程度の間、マルウェアをホスティングしているサイトへリダイレクトされていた。Dell Inc. は、ドメイン失効は一時的で当該期間中にマルウェアがユーザのデバイスへ転送されたとは考えていないとしている※86。
9	2018 年 1 月	株式会社ミクシィ・リクルートメントが提供する求人情報サイト「Find Job!」において、アクセス権限設定不備により、2017 年 5 月 12 日から同年 12 月 25 日の間、特定条件を満たすことで、アクセス権限を持たずとも外部から一部の求職者の履歴書情報を閲覧できる状態にあった。求職者の履歴書を参照できる URL を直接入力した場合に、求職者の Web 履歴書が閲覧できる状態にあった※87。

■表 1-2-3　2017 年度に報道された不適切な運用による情報漏えい（報道または公表事例を基に IPA が作成）

いるかの確認や、情報管理状況の報告や監査等によるチェックが重要である。特に委託する秘密情報が大量である場合は、委託先の管理不備等により情報漏えいが発生すると、事業への影響や金銭的損失が甚大なものになるため、ルールの確認と不断のチェックが必要である。

また Facebook の事例のように、第三者が利用可能なオープン API で情報を提供する場合は、「Need to Know の原則」を踏まえ、意図しない情報提供が発生しないよう、アクセス制御に十分な配慮が必要である。

1.2.5 金銭被害

ビジネスメール詐欺、偽警告・偽サイト等による詐欺、インターネットバンキングを狙った攻撃による被害の状況について述べる。

(1)ビジネスメール詐欺による金銭被害

巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらす攻撃をビジネスメール詐欺(Business E-mail Compromise:BEC)という(手口については「1.3.6 ビジネスメール詐欺」参照)。

FBI の統計※90 によると、2013 年 10 月から 2016 年 12 月までに、米国インターネット犯罪苦情センター(Internet Crime Complaint Center:IC3)に報告されたビジネスメール詐欺の被害件数は 2 万 4,345 件(米国内:2 万 2,292 件、米国外:2,053 件)、被害総額は約 22 億米ドル(米国内:約 16 億米ドル、米国外:約 6 億米ドル)であり、国際法的執行機関や金融機関等、複数の情報源から IC3 に報告されたデータを含めると、被害件数は 4 万 203 件、被害総額は 53 億 289 万 448 米ドルに上る。この統計は全米 50 州と 131 ヵ国から報告されたものである。ビジネスメール詐欺は、世界各地で大きな金銭被害をもたらす脅威となっている。

日本でも、2014 年以降、被害が増加傾向にあり※91、脅威の高まりを受け 2016 年ごろから金融機関や一部の都道府県警等が注意を呼びかけてきた※92。2017 年には本格的にビジネスメール詐欺が広がる兆しが出てきたという※93。また、セキュリティベンダが国内法人のセキュリティ担当者 1,361 人に実施したアンケートによると、2016 年度に 13.4% の組織がビジネスメール詐欺のメールを受信し、7.4% の組織が金銭被害を経験していた※94。ここでは、2017 年 12 月に国内で報じられた日本航空株式会社(以下、JAL)の事例とスカイマーク株式会社(以下、スカイマーク)の事例を紹介する。JAL の事例は金銭被害を受け、スカイマークの事例は金銭被害を免れた。

(a)JAL の事例※95

2017 年 12 月 20 日、JAL が 2 件のビジネスメール詐欺により、約 3 億 8,400 万円(347 万 880.64 米ドル)の被害を受けたことを発表した。2 件のうち 1 件は JAL の米国にある貨物事務所の地上業務委託料(約 2,400 万円)の被害、もう 1 件は JAL が米国の金融会社からリースしている航空機のリース料(約 3 億 6,000 万円)の被害である。

いずれも本来の取引先とは別のメールアドレスから、送金先口座変更を伝える偽の電子メールが JAL に届き、それを信じた担当者が、香港の銀行に開設された偽の口座へ送金してしまい被害に遭った。

JAL の事例の概要を表 1-2-4 に、被害別の経緯を図 1-2-5(次ページ)、図 1-2-6(次ページ)に時系列で示す。

JAL は再発防止策として、次の対策を講じたとしている。

- JAL グループ内の情報共有
  詐欺被害の経緯や犯行の手口等の詳細を共有する。
- 口座情報確認や登録手続きの厳格化
  取引先への送金先口座を変更する際は担当部門と出納部門の双方で事実確認を徹底する。

	貨物地上業務委託料の被害	航空機リース料の被害
被害額	21 万 5,999.61 米ドル(約 2,400 万円) ※ 2017 年 7 月と 8 月分の貨物地上業務委託料	325 万 4881.03 米ドル(約 3 億 6,000 万円) ※航空機 3ヵ月分のリース料
送金日	2017 年 8 月 24 日、9 月 7 日	2017 年 9 月 29 日
送金を行った部署	JAL 米国支店 航空貨物事業所	JAL 本社 財務部
送金先口座	香港の銀行に開設された偽の口座(航空機リース料の送金先とは別口座) ※正規の口座は香港以外	香港の銀行に開設された偽の口座(貨物地上業務委託料の送金先とは別口座) ※正規の口座は香港以外
口座変更連絡の送信元	本来の取引先とは別のメールアドレス	本来の取引先とは 1 文字違いのメールアドレス ※画面上は取引先担当と同一の名前とメールアドレスが表示された。

■表 1-2-4 JAL の事例の概要

2017 年 8 月	【貨物地上業務委託料に関する偽メール】 ① JAL の米国にある貨物事業所に、本来の取引先とは別のメールアドレスから、地上業務委託料の送金先口座変更を伝える偽のメールが届いた。 ②メールアドレスが異なることを不審に思い、JAL の米国の担当者が本来の取引先のメールアドレスを宛先に付け加えて、口座の変更は本当かを尋ねるメールを送信した。 ③それに対し、本来の取引先のメールアドレスから本当だとする返信があった。 ※本来の取引先のメールアドレスから届いたのか、画面表示上、本来の取引先のメールアドレスを偽装していたのかは報道から確認できなかった。
8 月 24 日と 9 月 7 日 （米国時間）	【貨物地上業務委託料の偽口座への送金】 JAL の担当者は、7 月分と 8 月分の貨物地上業務委託料として、香港の銀行に開設された偽の口座へ 2 回にわたり、計 21 万 5,999.61 米ドル（約 2,400 万円）を送金した。
11 月 10 日	【貨物地上業務委託料の被害届提出（海外）】 JAL が米国現地警察へ貨物業務委託料の被害届を提出した。
12 月 6 日	【貨物地上業務委託料の被害届提出（海外）】 JAL が FBI へ貨物業務委託料の被害届を提出した。
12 月 19 日	【貨物地上業務委託料の被害届提出（海外）】 JAL が香港警察へ貨物業務委託料の被害届を提出した。
12 月 20 日	【貨物地上業務委託料の詐欺被害公表】 JAL は一連の手続きが区切りを迎えたことでビジネスメール詐欺の被害を発表した。

■図 1-2-5　JAL の貨物地上業務委託料被害事例の経緯

(b) スカイマークの事例[※96]

2017 年 12 月 21 日、スカイマークにも JAL と同様の電子メールが 2 度にわたって届いていたことが報じられた。

1 度目は、2016 年 6 月に実在する海外の取引先担当者の名前で、送金先変更のメールがスカイマークに届いた。それを信じたスカイマークの担当者が指定された香港の口座に 40 万円を送金したが、既にその口座は凍結されており被害を免れた。口座が凍結されていることを不審に思ったスカイマークの担当者が取引先に確認したところ、送金先変更の事実はなく電子メールは偽物だと判明した。この件についてスカイマーク社内で注意喚起が行われた。

2 度目は、2017 年 10 月に 1 度目のメールとは別の実在する海外の取引先担当者の名前で、送金先変更のメールがスカイマークに届いた。変更後の海外の送金先に 200 万円余りを送金するよう請求するものだった。1 度目の件で既に注意喚起が行われていたため、スカイマークの担当者が不審に思い、取引先へ送金先変更の電子メールについて確認した。その結果、詐欺と分かり被害を免れることができた。

2017 年 9 月 25 日	【航空機リース料に関する偽メール】 JAL 本社財務部に、取引先である米国の金融会社のものと 1 文字違いのメールアドレスから、航空機リース料の送金先口座変更を伝える偽のメールが届いた。 取引先担当者と同一の名前とメールアドレスが表示されていた。 その前に送られていた正規の請求書の「訂正版」として、送金先を偽の口座に変更した PDF ファイルが添付されていた。 支払い期日が 4 日後と迫っており、支払わないと航空機が使用できなくなる恐れがあった。 JAL 本社財務部担当者は記載された口座へ日本から送金できるか確認したが、口座情報は精査しなかった。
9 月 29 日	【航空機リース料の偽口座への送金】 JAL 本社の担当者は香港の銀行に開設された偽の口座に、3 ヵ月分の航空機リース料 325 万 4881.03 米ドル（約 3 億 6,000 万円）を送金した。 複数人で送金をチェックしたが詐欺と見抜けなかった。
数日後	【航空機リース料の詐欺被害】 送金先口座（偽の口座）から、何者かにより航空機リース料の全額が引き出された。
10 月 7 日	【航空機リース料の詐欺被害発覚】 10 月に JAL へ米国の金融会社から航空機リース料の支払い督促があったことを受け、JAL は航空機のリース料の送金先が変わっていないことを知り、詐欺被害が発覚した。
ー	【航空機リース料の詐欺被害の社内調査】 JAL の社内調査に対し、担当者は「リース機のため、支払いが遅れると止められる恐れがあり、（変更口座の）確認前に支払いを優先した」と説明した。
11 月 2 日	【航空機リース料の被害届提出（国内）】 JAL が警視庁品川警察署へ航空機リース料の被害届を提出した。
11 月 7 日	【航空機リース料の被害届提出（海外）】 JAL が香港警察へ航空機リース料の被害届を提出した。
12 月 20 日	【航空機リース料の詐欺被害公表】 JAL は一連の手続きが区切りを迎えたことでビジネスメール詐欺の被害を発表した。

■図 1-2-6　JAL の航空機リース料被害事例の経緯

(c) JAL とスカイマークの事例のまとめ

JAL とスカイマークの事例はともに、実在する取引先の担当者をかたり、巧妙に送金先口座の変更を促すものであった。JAL は詐欺を見抜くことができず、多額の被害に遭い、スカイマークには結果的に金銭被害はなかったが、一度は騙されて送金まで行っていた。攻撃者は、狙った組織の担当者を騙すために、何らかの方法で、取り引きや請求に関する情報や、関係している従業員のメールアドレスや氏名等を入手していた可能性がある。

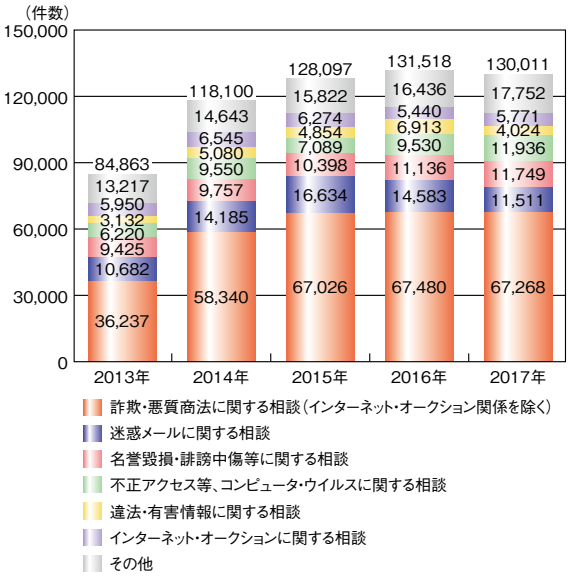
ビジネスメール詐欺は、攻撃者にとって多額の収益が

見込めることから、今後も脅威は続くと思われ、注意が必要である。

(2) 偽警告・偽サイト等の詐欺による金銭被害

2017 年においても前年からインターネットを悪用した詐欺が継続しており、従来の手口に加えて、いくつかの新しい手口等も確認されている。

警察庁の発表によると、2017 年の警察における「詐欺・悪質商法に関する相談（インターネット・オークション関係を除く）」の相談件数は 6 万 7,268 件（前年比 0.3% 減）となっている。これは、サイバー犯罪等に関する相談件数全体の約半数を占める割合である（図 1-2-7）。



■図 1-2-7　サイバー犯罪に関する相談件数の推移
（出典）警察庁「平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について[※97]」を基に IPA が編集

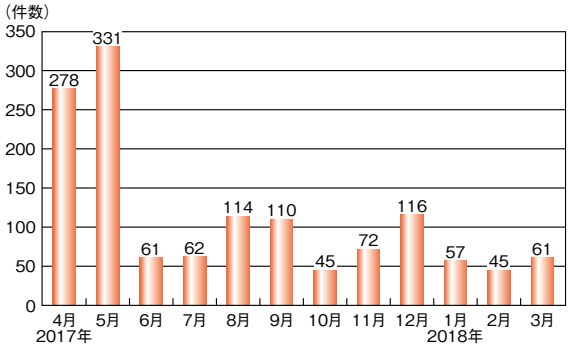
インターネット利用は幅広い年代に浸透しているため、インターネットを悪用した詐欺は誰でも遭遇し得る脅威となっている。また詐欺の手口も巧妙化しているため、十分な注意が必要である（具体的な手口については「1.3.7 偽警告・偽サイト等の詐欺」参照）。

(a) 偽警告による被害

2017 年度に IPA に寄せられたウイルス・不正アクセス関連の相談の中で最も多かったのは、前年度に引き続き、「偽警告（別名：サポート詐欺）」に関する相談であった。

「偽警告」とは、パソコンで Web サイトを閲覧していると、突然、「ウイルスが検出された」といった偽の警告画面が表示され、画面に記載された電話番号に電話をかけると保守サポート契約締結等による金銭を要求される手口である。

2016 年度から高止まりをしていた相談件数には変化が見られ、2017 年 6 月に急激な減少が確認された（図 1-2-8）。減少の要因としては、米国の連邦取引委員会（Federal Trade Commission：FTC）が、「サポート詐欺」への対策として「Operation Tech Trap」と名付けたキャンペーンによる詐欺業者の摘発[※98]で被害自体が低減したことが一因と考えられる。また、IPA が 4 月に[※99]、警視庁が 5 月に[※100]それぞれ、動画による偽警告の啓発コンテンツを公開したことで、相談をせずとも被害者自らが対処可能となった等の理由も考えられる。



■図 1-2-8　偽のウイルス検出の警告画面に関する月別相談件数推移

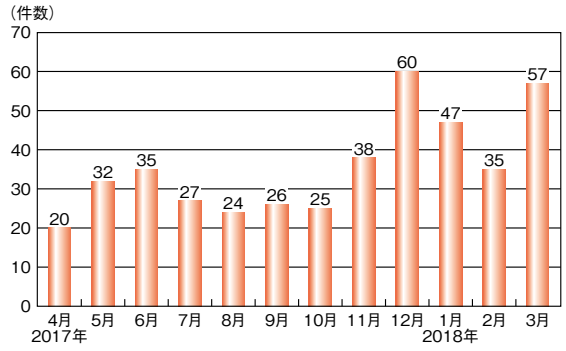
なお、一般企業や公共団体の提供する Web サイトを閲覧している際に警告画面が表示された、という偽警告に関する相談が IPA に複数寄せられた。これは不正アクセス等により、当該 Web サイトが偽の警告画面を表示するサイトへリダイレクトするように改ざんされたことによるものと考えられる。2016 年度に比べ相談は減少しているものの、特に不審さを感じない Web サイトからの偽警告被害が確認できている等、今後も偽警告への警戒が必要と言える。

(b) 偽セキュリティソフトによる被害

「偽セキュリティソフト」とは、Web サイトの閲覧中に突然「あなたのシステムに問題がある」等の警告メッセージを表示し、その問題を解決する手段と称して、システムメンテナンスやセキュリティに関する有償のソフト購入に誘導し、金銭を騙し取る手口である。

IPA に寄せられる相談件数は、2016 年度以降は月に 30 件弱程度で推移していたが、2017 年 12 月及び 2018 年 3 月に相談件数が倍化した（次ページ図 1-2-9）。

相談件数が倍化した 2017 年 12 月頃より、有償のソフトを購入させた後の画面で、認証（アクティベート[※101]）のために電話するように促された、という相談が寄せら

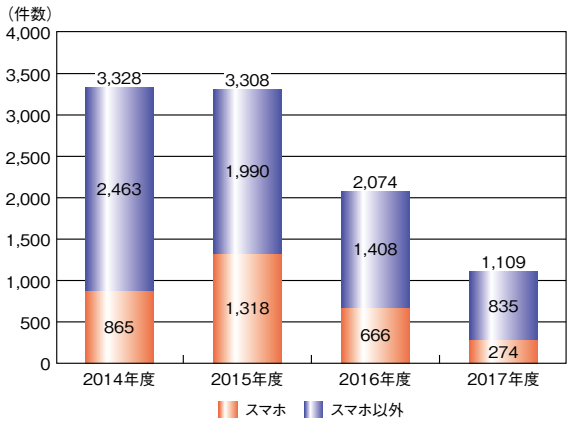


■図 1-2-9　偽セキュリティソフトの警告画面に関する月別相談件数推移

れ始めた。相談によれば電話をかけると偽警告の手口と同様、遠隔操作による対応を持ちかけられ、更に問題が見つかったとして年間サポート契約等に誘導されるという。有償のソフトの購入に加え、サポート契約料の支払いとして二重に金銭を詐取される被害ともなり得るため注意が必要である。

(c) ワンクリック請求による被害

2017 年度に寄せられたワンクリック請求に関する相談件数は、前年度比 46.5%減と大幅な減少となった（図 1-2-10）。



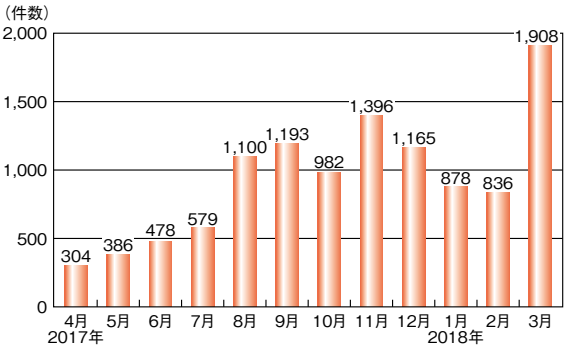
■図 1-2-10　ワンクリック請求に関する年別相談件数推移

「ワンクリック請求」とは、アダルトサイトで動画再生に必要な手続きと称して、HTA（HTML Application）ファイルをダウンロード、実行するように促し、実行したパソコンに一方的に有料サービスに会員登録されたかのように偽って、アダルトサイトの請求画面を繰り返し表示させ、金銭を詐取する手口である。

なお、請求画面が繰り返し表示されるようになってしまった人が解決を模索し、インターネット検索で見つけたワンクリック請求に関する「無料相談」「返金可能」をうたう探偵業者に依頼をした結果、何も解決されないにもかかわらず調査料を支払わされたという相談が消費生活センターに寄せられている※102。そのような被害者心理につけ込む手口にも注意が必要である。

(d) フィッシングによる被害

「フィッシング」とは実在する企業をかたったメールを送り「第三者によるアクセスを確認したのでパスワードを変更した。下記 URL からログインして変更し直して欲しい」等の文言で、メールの URL リンクから偽の Web サイト（フィッシングサイト）に誘導し、そこで個人情報等を入力させて詐取する手口である。攻撃者に誘導される偽の Web サイトは、実在する Web サイトに酷似しているため、一目で偽物だと判断がしにくい。フィッシング対策協議会に寄せられた報告によると、2017 年度前半から件数は増加傾向にあり、特に 2018 年 3 月は 1,908 件と大きく増加した（図 1-2-11）。

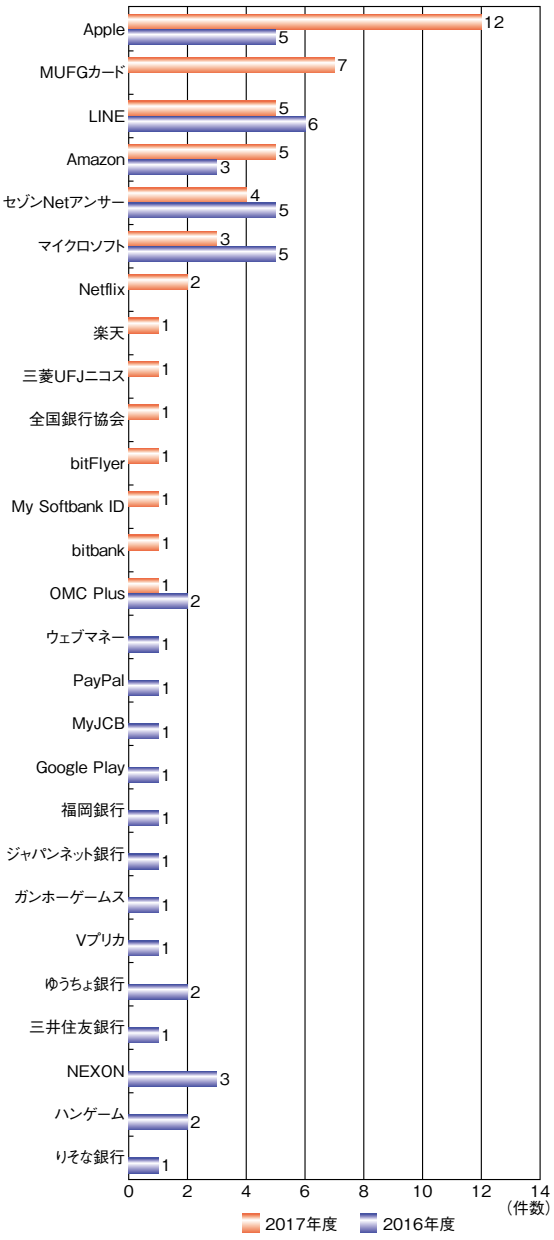


■図 1-2-11　フィッシング対策協議会に寄せられた報告件数推移
（出典）フィッシング対策協議会の月次報告書※103 を基に IPA が作成

フィッシングの手口では、銀行やカード会社等の金融機関をかたるものが多かったが、2017 年度は Apple Inc. をかたるフィッシングメールが増加した（図 1-2-12）。その要因としては、Apple サービスの利用者が多いことや、クラウドやメール、アプリ購入等の複数のサービスと連携していることから、攻撃者にとって効率が良い、利用価値が高い等が考えられる。また、日本のビットコイン取引所（bitFlyer 等）をかたるフィッシングメールの報告もある。今後もこのような新たなサービスをかたるフィッシングメールの出現にも注意が必要である※104。

(e) 偽サイトによる被害

2017 年 12 月、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center：JC3）より、インターネットショッピングに関する詐欺サイト対策の発



■図 1-2-12　フィッシング対策協議会によるサービス別注意喚起の件数
(出典)フィッシング対策協議会の緊急情報一覧※105を基に IPA が作成

表があった。JC3 から、米国に本拠を置く世界最大のフィッシング対策の国際機関 APWG（Anti-Phishing Working Group）等に対し詐欺サイトの URL 情報 1 万 9,834 件を提供したという※106。

この詐欺サイトの一種である偽 EC サイトは、見た目もよくある EC サイトのようなつくりとなっており、検索サイトで上位に表示される等、あたかも本物の EC サイトであるかのような細工がされている。しかし、実際には検索サイトから訪れたユーザが会員登録を済ませ、購入手続きをしても商品は届かず、そのことを問い合わせても回答が得られない等、会員登録時の個人情報やクレジットカード番号、あるいは商品の購入代金を詐取する等を目的とした偽サイトとなっている。

新たな手口として、2017 年 7 月「警察庁」の偽サイトが確認された※107。この手口では警察庁を装い「幼児猥褻や動物虐待」等の違法サイトを閲覧したとして、Web サイト閲覧者に違反金 2 ～ 5 万円を iTunes カードで支払うよう要求する。トレンドマイクロ社によると、7 月 27 日前後から 30 日までの間、警察庁の偽サイトへの国内利用者からのアクセス 2,500 件以上を、同社のセキュリティソフトでブロックしたという※108。

(3) インターネットバンキングを狙った攻撃による金銭被害

警察庁の統計によると、2017 年のインターネットバンキングを狙った攻撃による不正送金の被害額は約 10 億 8,100 万円、被害件数も 425 件となり、被害額は 2016 年、件数は 2015 年から継続して減少傾向にある。特に発生件数については前年と比べ、大きく減少している（表 1-2-5）。

年	被害件数	被害額（約）
2013 年	1,315 件	14 億 600 万円
2014 年	1,876 件	29 億 1,000 万円
2015 年	1,495 件	30 億 7,300 万円
2016 年	1,291 件	16 億 8,700 万円
2017 年	425 件	10 億 8,100 万円

■表 1-2-5　不正送金の被害件数と被害額
(出典)警察庁発表※109を基に IPA が作成

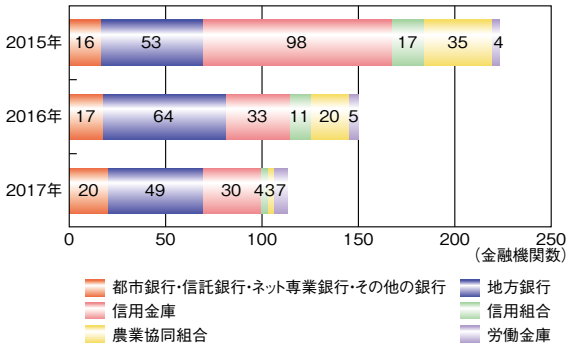
2017 年は、インターネットバンキングの不正送金の機能を持ったウイルス「DreamBot」が、実在の企業をかたるばらまき型メールによって広く拡散された※110（手口については「1.3.4 ばらまき型メールによる攻撃」参照）。

特に 2017 年 10 月以降、感染が拡大しているとして JC3 や警察庁が注意を呼びかけた※111。このような注意喚起や感染チェックサイト※112 の提供といった被害防止に向けた取り組みが、被害減少の要因の一つとして考えられる。

一方で、インターネットバンキングの電子決済サービスを利用して仮想通貨取引所に対して不正に送金を行う、といった新たな手口が確認されている。また、仮想通貨アカウントへの不正アクセスによる不正送金被害も発生する等、仮想通貨関連被害への対策も必要となっている（仮想通貨のセキュリティについては「3.2 仮想通貨の情報セキュリティ」参照）。

2016 年に不正送金の被害を受けた金融機関数は

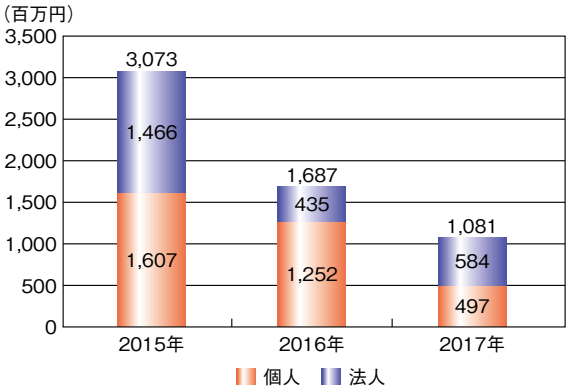
150 機関であったが、2017 年には 113 機関に減少している。被害金融機関の内訳は、「都市銀行･信託銀行･ネット専業銀行・その他の銀行」が 20 行、「地方銀行」が 49 行、「信用金庫」が 30 金庫、「信用組合」が 4 組合、「農業協同組合」が 3 組合、「労働金庫」が 7 金庫である（図 1-2-13）。



■図 1-2-13　被害金融機関数の推移
（出典）警察庁「平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について[※97]」を基に IPA が編集

口座種別（法人・個人）ごとの被害額では、2016 年に比べ法人口座では増加したものの、個人口座では大きく減少している（図 1-2-14）。被害額の減少は、不正送金に使用された IP アドレス等に対する監視が強化されたことによるものと考えられる。

警察庁によると、被害を受けた個人口座名義人及び法人口座のいずれも約 6 割がワンタイムパスワードや電



■図 1-2-14　口座別の被害額の推移
（出典）警察庁「平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

子証明書を利用していなかった。また、仮想通貨交換業者等への不正アクセスによる不正送金被害の約 8 割で ID・パスワードによる認証のみしか提供されていない、または提供されていても被害者が利用していない等の理由で 2 段階認証を利用していなかった。

仮想通貨取り引きを含め、不正送金被害に遭わないためには、各金融機関や仮想通貨交換業者が提供・推奨しているセキュリティ対策（ワンタイムパスワード、電子証明書、2 段階認証等）を利用することが重要である。また、併せてウイルス感染への対策や不正送金に関する被害事例・手口の情報収集も実施すべきである。

1.3 攻撃・手口の動向と対策

本節では、2017 年度に確認されたサイバー攻撃の手口を中心に解説する。

1.3.1 ランサムウェアによる攻撃

2017 年に世界中で感染を広げ、大きな注目を浴びた「Wanna Cryptor」と呼ばれるランサムウェアを取り上げて解説する。Wanna Cryptor は、ファイルを暗号化して身代金を要求するという基本的な手口は従来のランサムウェアと同様だが、ネットワークを介して他の端末に感染を広げる自己増殖機能を持っている点が従来と異なる。Wanna Cryptor の自己増殖は、組織のネットワーク内だけでなく、インターネット上の端末でも行われ、世界中で感染を大きく広げる一因となった。

(1) エクスプロイトキットの自己増殖機能による攻撃

Wanna Cryptor の自己増殖機能は厳密にはランサムウェア自体の機能ではなく、「EternalBlue」と呼ばれるエクスプロイトキット※113 の機能である。EternalBlue は Microsoft 社製品の SMBv1※114 と呼ばれるプロトコルの脆弱性（CVE-2017-0144）を悪用し、SMBv1 が利用する特定ポートを公開している端末に対してネットワークを介して攻撃パケットを送出することで感染拡大を図る。Wanna Cryptor の事例においては、攻撃パケットが組織内等の同一ネットワーク内のみではなく、インターネット上の端末へも送出された。そのため、一般利用者のパソコンでも Wanna Cryptor に感染してしまったという相談が IPA に複数寄せられた。家庭内にルータを設置しておらず、パソコンが直接インターネットに接続している（グローバル IP アドレスが割り当てられている）等、Wanna Cryptor に感染してしまう環境要因（図 1-3-1）を満たすパソコンがインターネット上に多く存在していたといえる。

(2) Wanna Cryptor の事例から学ぶ対策

Wanna Cryptor は、ネットワークを介した自己増殖機能による攻撃で世界中に感染が拡大した。この事例から学ぶ有効な対策について述べる。

■図 1-3-1　Wanna Cryptor に感染してしまう三つの環境要因
（出典）IPA「WannaCryptor の相談事例から学ぶ一般利用者が注意すべきセキュリティ環境※115」

(a) 脆弱性への対策

エクスプロイトキットを使用した攻撃では、端末の OS や利用しているソフトウェアの脆弱性を悪用した攻撃を仕掛ける。脆弱性が発見され、提供元から修正プログラムが公開された場合は、修正プログラムを速やかに適用することが対策となる。実際に Wanna Cryptor の事例で悪用された脆弱性については、2017 年 3 月の時点で Windows の修正プログラム（MS17-010）が公開されており、この修正プログラムが適用されていれば、攻撃を防ぐことができる状況だった。

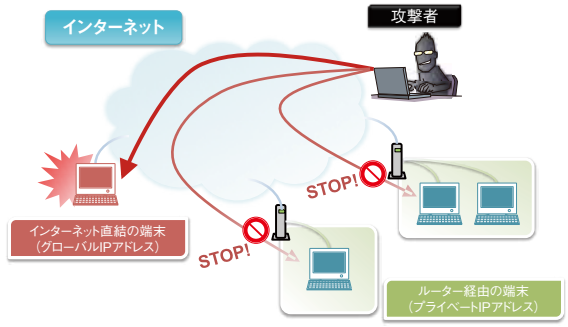
(b) 通信制御による対策

システム環境によっては即時の修正プログラム適用ができない等、脆弱性への対策が難しい場合等も考えられる。EternalBlue による攻撃は、EternalBlue が送出する不正な攻撃パケットを端末が受け付けてしまうことで成立する。そのため、通信経路上等で適切に通信制御を行うことも対策となる。一例として、通信経路上もしくは各端末上のファイアウォールによって攻撃パケットをブロックすることが挙げられる。また、一般利用者においては Wanna Cryptor の特徴であるインターネットを介した攻撃に対し、ルータを設置してインターネットからパソコンに直接アクセスできない環境とすることが有効な対策となる（次ページ図 1-3-2）。

(3) 基本的な対策の重要性

Wanna Cryptor はエクスプロイトキットによる自己増殖が特徴的であったが、メール等の他の経路でランサムウェアに感染することも十分考えられる。以下のような基本的なウイルス対策を実施することも重要である。

- セキュリティソフトを導入し、定義ファイルを常に最新



■図 1-3-2　ルータ経由でインターネットに接続することでパソコンを外部の攻撃から守る
（出典）IPA「Wanna Cryptor の相談事例から学ぶ一般利用者が注意すべきセキュリティ環境」

の状態に保つ。

- メールの添付ファイルや本文に記載された URL、SNS にアップロードされているファイルや掲載されている URL を不用意に開かないように注意する。

また、ランサムウェアに感染した場合、提示された要求どおりに金銭を支払っても暗号化されたファイルを復号できる保証はない。万が一、感染してしまった場合を想定した対策としてはファイルのバックアップが有効であり、以下を推奨する。

- 重要なファイルは定期的にバックアップを取得する。
- バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する。
- バックアップに使用する装置・媒体は複数用意する。
- バックアップの妥当性（バックアップが正常に取得できているか、現状のバックアップ手法がランサムウェアに対して有効か）を定期的に確認する。

なお、ランサムウェア対策情報を提供している Web サイト「The No More Ransom Project[※116]」にて、特定のランサムウェアによって暗号化されたファイルを復号するツールが提供されている。

1.3.2 DDoS攻撃

DDoS 攻撃では、複数のコンピュータや IoT 機器が同時に攻撃対象のサーバに対して大量のパケットを送信することで、サーバの処理能力を飽和させたり、ネットワーク帯域を枯渇させたりする手口が用いられる。

(1) DDoS 攻撃の手口

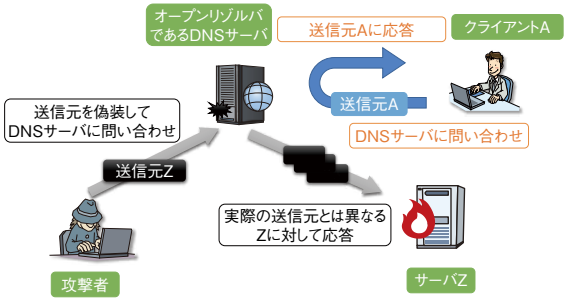
DDoS 攻撃では、標的に対して大量の通信を行う必要がある。これを実現するための手法は複数存在する。Imperva の報告[※117]では、2017 年の下期にはリフレクター攻撃やマルチベクトル型攻撃の増加が観測されたという。この二つの攻撃手法について解説する。

(a) リフレクター攻撃

リフレクター攻撃は、脆弱性等の問題のあるサーバやネットワーク機器を悪用し、送信元を偽装した問い合わせを問題のあるサーバやネットワーク機器に送り付けることで、それらの機器から偽装された送信元に対し応答パケットを送り付ける手法である。

DNS サーバや NTP サーバは、問い合わせに対し自動的に応答を行う。組織が管理する DNS サーバや NTP サーバは一般的に組織内の機器のみに応答するよう設定されているが、設定不備等により外部からの問い合わせに対しても応答してしまうものが存在する。

特に不特定の通信元からの問い合わせに応答する DNS サーバを「オープンリゾルバ」と呼ぶ。このような外部からの問い合わせに応答してしまうサーバが DNS リフレクター攻撃に悪用される（図 1-3-3）。



■図 1-3-3　DNS リフレクター攻撃のイメージ

実際の DNS リフレクター攻撃においては、複数のオープンリゾルバへ一斉に問い合わせることで、より大量の応答パケットを攻撃対象に送り付けることが多い。

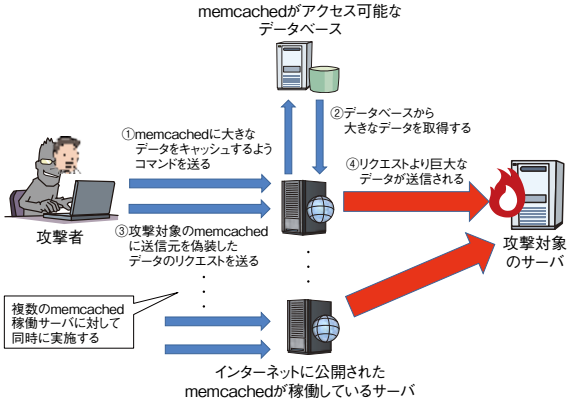
また、NTP サーバを悪用したリフレクター攻撃でも、同様に攻撃の通信を増幅する手口が存在する[※118]。NTP サーバソフトウェア「ntpd」（4.2.7p26 以前のバージョン）には、状態を確認する機能である「monlist」に脆弱性が存在し、monlist を利用した問い合わせを送信すると、その NTP サーバが過去に通信した端末、最大 600 台分の IP アドレスを応答する。この脆弱性を NTP リフレクター攻撃に悪用すると、条件次第では 234Byte の通信をおよそ 200 倍にまで増幅できるという[※119]。

2018 年 2 月 28 日に発生した DDoS 攻撃により、GitHub が断続的に接続できなくなる被害が発生した[※120]。

これは後の調査でアクセス制限設定に不備がある「memcached」が稼働するサーバを悪用されたことが原因であると判明した。

memcachedは、データベースからWebアプリケーションへの応答をキャッシュし、データベースへの問い合わせを減らすことでWebサイトの応答性向上を目的としたソフトウェアである。そのため、本来であればインターネットから直接memcachedにリクエストが送られない環境で使用されることが前提となっている。しかし、memcachedがインターネットからのリクエストを無制限に受け付けてしまう状態で運用されたサーバが多数存在し、攻撃者によってDDoS攻撃の踏み台として悪用された※121。

攻撃者はまず、memcachedに多数の大きなデータをキャッシュさせるためのコマンドを送る。次に、攻撃者が送信元を攻撃対象のIPアドレスに偽装したリクエストを送ることで、攻撃対象に対し、キャッシュされたデータが送信される。これにより、攻撃者が送信したリクエストよりも大きなデータが、攻撃対象に送信される(図1-3-4)※122。セキュリティベンダによれば、リクエストに対して5万倍もの大きさに増幅された通信を確認したという※123。



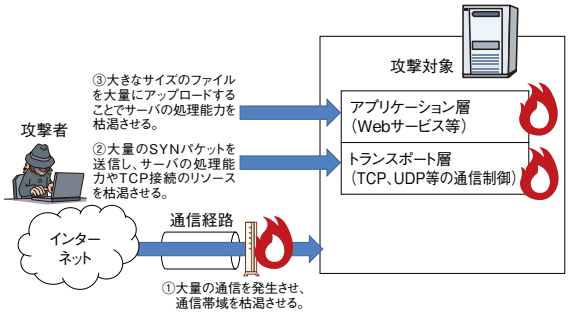
■図1-3-4 「memcached」を悪用して攻撃を増幅する手口

(b) マルチベクトル型攻撃

Impervaの報告では、2017年第3四半期に発生した攻撃の70%以上がマルチベクトル型の攻撃であったとされている。マルチベクトル型攻撃では、ネットワークにおける複数の階層(レイヤ)やサーバのサービスを標的として、同時に攻撃が行われる。図1-3-5は、マルチベクトル型攻撃の例※124である。

①前述のリフレクター攻撃によって、攻撃対象のネットワーク帯域を枯渇させる。

②ボットネットを使用して、攻撃対象のサーバに対し大量のSYNパケットを送信させ、サーバが受付可能なTCP接続のリソースやサーバの処理能力を枯渇させる。



■図1-3-5 マルチベクトル型攻撃の例

③ Webアプリケーションに対し、サイズの大きいファイルをPOSTすることで、サーバのメモリやCPU等の処理能力を枯渇させる※125。

このように複数の手法を組み合わせて攻撃を行うことにより、攻撃者は攻撃対象の弱点(ネットワーク帯域の狭さ、サーバの処理能力の弱さ等)を見つけることができる。弱点が見つかると、弱点を狙った効率的な攻撃が行われる。

(2) DDoS攻撃への対策

攻撃対象にされてしまった場合の対策について解説する。対策は、被害に遭わないための対策と攻撃に加担しないための対策の二つに分けられる。

(a) 被害に遭わないための対策

前述のマルチベクトル型攻撃のように、近年のDoS攻撃は攻撃対象の弱点を探りながら攻撃が行われるため、多層的な対策が必要となる。例えば、攻撃対象側の対策として、異常な量のSYNパケットや巨大なサイズのパケットをフィルタすることで、サービスの停止を防ぐことも対策の一つである。

しかし、DDoS攻撃では攻撃の際に大量の通信が発生するため、組織内にトラフィックが流入した時点で影響が発生する。これを防ぐためには、ISP(Internet Service Provider:インターネットサービスプロバイダ)が提供するDDoS対策サービスを利用し、組織に流入する前に攻撃と思われる通信を遮断することで、インターネット回線の帯域が枯渇しないようにする等の対策が必要である。

また、近年では様々な企業からクラウド型のDDoS対策サービスが提供されている。このサービスではWebサイトへのアクセスをプロキシとなるクラウドサービス経由

とすることで、ネットワークへの攻撃をクラウドで遮断する。こうしたサービスを利用することも対策の一つである。

(b) 攻撃に加担しないための対策

DDoS 攻撃では、ウイルスに感染した多数の端末を遠隔操作して、一斉に通信を発生させる場合がある。このような攻撃の踏み台にされることを防ぐためには、OS やアプリケーション、セキュリティソフトを最新の状態に保つことが、基本的な対策として有効である。更に、初期設定や安易なパスワードを設定している機器を乗っ取るウイルスもあるため、IoT 機器を使用する場合は、初期設定のパスワードを使用せず、複雑なパスワードに変更する等の対策が必要である。

また、前述のリフレクター攻撃では、オープンリゾルバとなっている DNS サーバやルータ等が悪用される。オープンリゾルバの問題が存在する原因としては、DNS サーバやルータの設定不備のほかに、ソフトウェアやファームウェアに脆弱性が存在することが原因の場合がある。対策としては、設定を見直し、組織外からの問い合わせに応答しないようにするほか、ソフトウェア等を最新の状態にアップデートすることも必要である。

組織が行う対策としては、組織内にある様々な端末やサーバが攻撃に加担していないか、通信を監視して確認することが必要である。例えば、Web サーバ等は外部からのリクエストを受け付けることはあっても、サーバから外部に向けて接続を行うことは少ないと考えられる。こうしたサーバから外部に向けた通信が頻繁に発生していることを確認した場合、ウイルス感染を疑って調査、対処した方が良い。

また、組織内の端末の通信量が、他の端末や過去のログのそれと比較して急増した場合等は攻撃の踏み台となっている可能性があり、確認が必要である。

1.3.3 ソフトウェアの脆弱性を悪用する攻撃

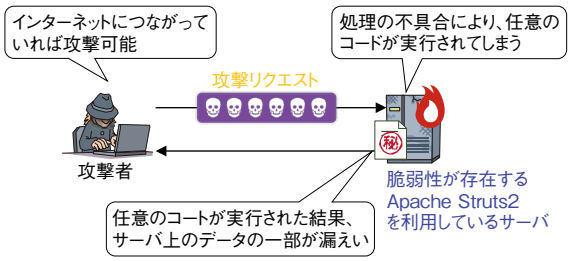
2017 年は、多くの Web サーバで使われている Apache Struts2 や、多くの利用者を持つ Windows に存在する既知の脆弱性を狙った攻撃が報告された。また、IoT 機器の脆弱性を探索するアクセスが頻繁に観測された。本項では、Apache Struts2 と Windows、IoT 機器等の脆弱性を標的とした攻撃の手口と対策について解説する。

(1) Apache Struts2 の脆弱性を悪用した攻撃

Apache Struts2 は、Web アプリケーション開発に用いられる Java フレームワークである。

2017 年は前年に引き続き Apache Struts2 の脆弱性を悪用する攻撃が確認された。総務省や B.LEAGUE サイト等、多くの個人情報を保有する Web サイトが攻撃に遭い、個人情報が漏えいした可能性があると報告された(「1.2.4 (1) 外部からの攻撃による情報漏えい」参照)。2017 年に IPA で注意喚起を行った Apache Struts2 の脆弱性 CVE-2017-5638 ※49、及び CVE-2017-9805 ※126 を悪用した攻撃の手口を以下に示す。

攻撃者はインターネットを通じて、脆弱性が存在する Apache Struts2 を利用しているサーバに対し攻撃を行う。攻撃者が細工した攻撃リクエストを送信すると、サーバ上で任意のコードが実行される。その結果、サーバ上に存在するデータを取得することが可能となる(図 1-3-6)。



■図 1-3-6　Apache Struts2 の脆弱性を悪用した攻撃イメージ

各脆弱性の概要は以下のとおりである。

- CVE-2017-5638 の脆弱性
  この脆弱性は、ファイルアップロード時の通信処理に使用している Jakarta Multipart parser の処理の不具合に起因している。この不具合により、細工した通信の Content-Type に含まれた任意の文字列がコードとして解釈されてしまう。
- CVE-2017-9805 の脆弱性
  この脆弱性は、REST プラグインが XML 通信をソフトウェアで扱うための文字列に復元する際、信用できない情報でも復元してしまう不具合に起因している。この脆弱性を悪用した攻撃は、対象となる Web サーバで REST プラグインが使用されていることが前提となる。

上記はいずれも、脆弱性が存在する Web サーバに対して、攻撃者が細工した通信を行うだけで悪用が可能なため、攻撃は容易である。攻撃された場合、情報の窃取、特定ファイルの操作、Web アプリケーションの

操作妨害等の被害が想定される。

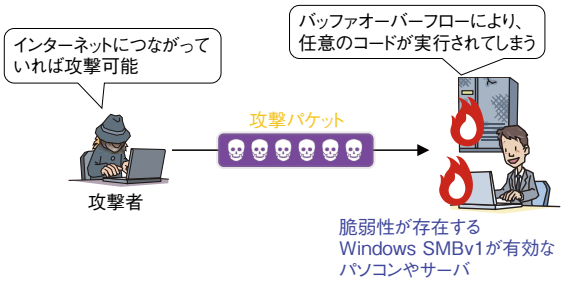
攻撃は最新の脆弱性だけではなく、既知の脆弱性を解消するアップデートが遅れているWebサーバが狙われる場合も多いと考えられる。Apache Struts2等、フレームワークのアップデートは、動作しているWebアプリケーションに不具合が発生する等の理由から即時の対応が難しい場合がある。そのため、Webサーバの運営者は、脆弱性が発見された場合に備えて計画的なバージョンアップの実施が必要である。何らかの理由によりバージョンアップまでに時間を要するような場合は、一時的にIPS※127やWAF※128等で防御する方法もある。

(2) Windowsの脆弱性を悪用した攻撃

2017年はWindowsの脆弱性を狙った攻撃やランサムウェアが相次いで確認されたことで話題となった。

ここでは、Wanna Cryptor等の数多くのウイルスで悪用された攻撃ツール「EternalBlue」について解説する。

EternalBlueは、Windows SMBv1サーバが特定のパケットを処理する際の不具合に起因し、攻撃パケットによりバッファオーバーフローが発生することで、リクエストに含まれた任意のコードが実行されてしまう脆弱性を悪用する攻撃ツールである(図1-3-7)。



■図1-3-7 EternalBlueを悪用した攻撃イメージ

2017年4月14日、悪意のあるハッカー集団により、インターネット上にEternalBlueを含む攻撃ツールが公開された。これにより他のハッカーへ広まったと考えられる。国内では、4月19日よりEternalBlueの攻撃と見られるアクセスが継続的に確認されている※129。

また、5月中旬に世界規模で感染が確認されたWanna Cryptorは、その感染拡大にEternalBlueを用いた。しかし、EternalBlueが悪用する脆弱性を解消する修正プログラムは、同年3月14日にはMicrosoft社より公開されていた。何らかの理由で修正プログラムを適用できていなかった端末がWanna Cryptor感染等の被害に遭うこととなった(Wanna Cryptorについては「1.2.1 (1) Wanna Cryptorによる被害」「1.3.1 ランサムウェアによる攻撃」参照)。

Microsoft社はWindowsの利用者に対し、定期的に修正プログラム等を提供している。修正プログラムが公開された際は、利用者には速やかな適用が求められる。

(3) IoT機器を対象とした攻撃

ネットワークに接続されたIoT機器としては、家庭用のルータ、テレビ、エアコン、Webカメラや、普及しつつあるスマートスピーカー等がある。こうした機器に脆弱性が存在すると、攻撃者による乗っ取りや個人情報の窃取、他のサーバ等を攻撃する際の踏み台等に悪用される可能性がある。2017年は、Webカメラやルータの脆弱性が公表された後、その脆弱性を標的としたと思われるアクセスが観測された※130。日本国内のIPアドレスを送信元とする、TCPの23番ポート(TELNETで使用)へのスキャンが増加しており、2017年11月半ばのピーク時には、1時間あたり約2.4万件のアクセスが確認されている。

製品の脆弱性の公表及び修正プログラムの配布がされた場合でも、一般家庭のIoT機器利用者が自ら進んで情報を確認したり、修正プログラムを適用したりすることは多くないと見られる。このような修正未対応の製品のTELNETや、開発者がメンテナンス用に割り当てているプライベートポートを探すためのアクセスが観測されたと考えられる。

脆弱性が存在するIoT機器が発見されれば、ウイルス感染により攻撃に利用される。攻撃はDDoS攻撃だけでなく、情報窃取や機器破壊等、多様化している(詳細は「3.1 IoTの情報セキュリティ」参照)。このような攻撃及び攻撃のための事前調査からIoT機器を安全に保つための対策を以下に示す。

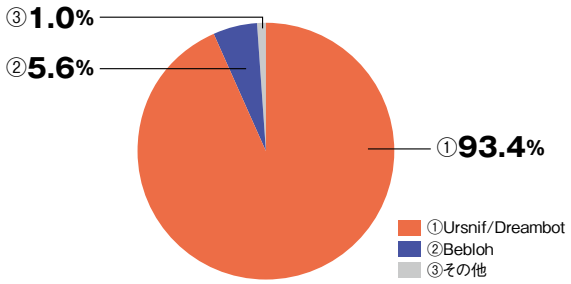
- 製品開発者が行うべき対策
  - 各組織が公開しているIoT機器の開発ガイドライン等を基に対策を実装する。
- メーカ(販売者)が行うべき対策
  - 製品に関連する脆弱性が報告された場合、速やかに修正プログラムを公開する。
  - 製品の問題や、安全に運用するための注意点等の情報を製品利用者に提供し、対策を促す。
- 製品利用者が行うべき対策
  - メーカが提供する、製品の問題や安全に運用するための注意点等の情報を確認した上で使用する。
  - IPAが公開している「JVN iPedia※131」や脆弱性

情報の通知メール等から、脆弱性が公表されていないか確認する。
- メーカが修正プログラムを公開した場合は、速やかに修正プログラムを適用する。
- 攻撃者に脆弱性を悪用されるリスクを低減するため、製品を利用するにあたって問題がなければ、インターネットから直接 IoT 機器にアクセスできないようにする。

1.3.4 ばらまき型メールによる攻撃

特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的とした日本語のメールを本項では「ばらまき型メール」と呼ぶ。

日本 IBM 社によると、2017 年 1 月 1 日～ 6 月 30 日の間に検知した、件名や添付ファイル名に日本語を利用するメールで感染するウイルスのうち 93.4% が、不正送金を狙ってインターネットバンキングのアカウント情報を窃取するウイルス「Ursnif※132」、またはその亜種「DreamBot※133」であったという（図 1-3-8）。なお、セキュリティベンダによっては、Ursnif と DreamBot を区別していないため、出典の中で特段の区別がなされていない場合は、以降、「Ursnif/DreamBot」と記載する。



■図 1-3-8　件名や添付ファイル名に日本語を利用するメールで感染するマルウェアの割合
（出典）日本 IBM 社「2017 年上半期 Tokyo SOC 情報分析レポート※134」を基に編集

JC3 は、日本を標的とした攻撃が大量に確認されたとして、2017 年 3 月、DreamBot に関する注意喚起情報を公開した※110。また、警察庁によると、DreamBot を用いてインターネットバンキングのユーザ ID・パスワードを盗み取る事案が 10 月に急増したという※135。12 月には、DreamBot の感染拡大を確認したとして、JC3 が不正送金の被害について改めて注意を呼びかけた※136（関連する警察の活動については「2.1.4 (1) (c) 不正送金対策」参照）。

日本は、Ursnif/DreamBot への感染を狙った攻撃において、2017 年に最も標的とされた国の一つであり※137、国内で観測された手口は巧妙化を続けている。

(1) ばらまき型メールの手口の動向

攻撃者がばらまき型メールを送信してからウイルスに感染させるまでの手口を解説する。

(a) メールのセキュリティ対策を回避する手口

IPA のサイバー情報共有イニシアティブ（Initiative for Cyber Security Information sharing Partnership of Japan：J-CSIP）によると、ばらまき型メールを用いた攻撃を継続的に受けていた組織で着信状況を観測したところ、従来の攻撃では、ばらまき型メールの攻撃者は、宛先が存在するかしないかにかかわらず、攻撃者の送信先リストに載っていると思われるメールアドレスに対して送信する傾向があった。しかし、今回観測された攻撃では、宛先が実在するメールアドレスのみに送信した攻撃が確認された。このことから、攻撃者が送信エラーとなった宛先を削除する等して、送信先リストをメンテナンスし、実在する相手に絞って送信を試みている可能性がある※138。

DreamBot への感染を狙ったばらまき型メールには、従来、悪意のあるファイルが添付されたものが多く確認されていたが、2017 年 9 月以降、メール本文中に悪意のあるファイルをダウンロードさせるための URL を記載する攻撃が新たに確認された。これは、指定された拡張子の添付ファイルの削除等を行うメールフィルタリング機能を回避することが狙いと推測される。

実際、いくつかの組織で、メール本文中に URL を記載する手口となってから、こうしたばらまき型メールが検知できず、数十～数百通単位で、組織内に流入したケースが報告されている※138。

(b) 本物のメールと信じ込ませる手口

パロアルトネットワークス株式会社によると、Ursnif による攻撃を分析する中で、攻撃に用いられたスパムボットネットを発見し、そこから配信されるメールを分析したところ、日本を含む複数の国が標的となっていた※139。すべての言語のメールに共通して、「写真」「注文」「請求」「お知らせ」「配達」等の単語が確認できたという（表 1-3-1）。攻撃者は、国や地域によらず受信者が開封しやすい題材を選択し、日本を含む各国の言語のウイルスメールを作成していると考えられる。

これらの単語は、JC3 が 2017 年に注意喚起情報として公開したメールの件名や本文でも確認でき※140、繰り

標的	ポーランド	イタリア	スペイン	ドイツ	オーストラリア	日本
メールで頻出する単語	Zejęcie	Foto	Foto	Foto	Photo	写真
	Oferta	D'ordine	Orden	Bestellung	Order	注文
	Faktura	Fattura	Factura	Rechnung	Invoice	請求
	Powiadomienie	Notifica	Notificación	Versandbenachrichtigung	Notification	お知らせ
	Dostawa	Recapito	Entregar	-	Delivery	配達

■表 1-3-1　標的と電子メールの特徴
（出典）パロアルトネットワークス株式会社「銀行を狙うトロイの木馬：日本の感染者を踏み台に世界中に攻撃を行う、Ursnif による配信ネットワークが明らかに※139」を基に IPA が作成

返し使用されていることがうかがえる。

一方、実在する企業や組織をかたり、送信元アドレスや本文の日本語にも不自然さを感じさせない、更に巧妙なばらまき型メールも確認されている。2016 年 6 月ごろより宅配事業者が、2017 年 9 ～ 10 月ごろより金融事業者（銀行やクレジットカード会社）が詐称されている※141。

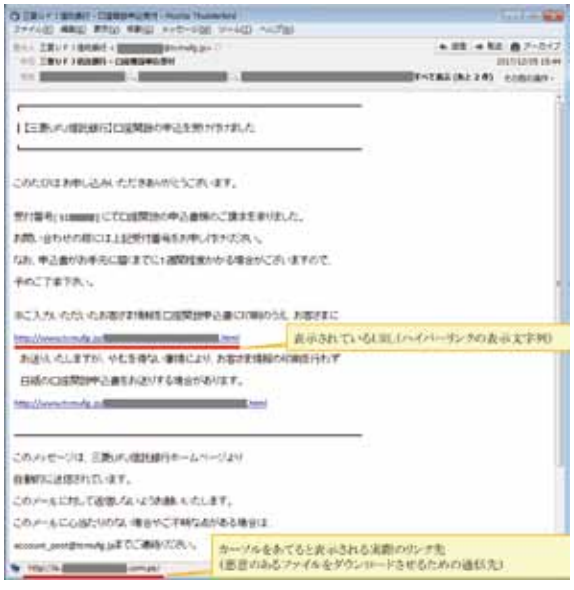
特に、12 月に確認された「カード利用のお知らせ」という件名のばらまき型メール（図 1-3-9）では、従来、テキスト形式のメールを用いていたところを、詐称する企業の実際のメールを真似て HTML 形式にする等の偽装が行われている。詐称された楽天カード株式会社は「楽天カードが実際にお客様に送信するメールと酷似し、見た目上は違いがわからない巧妙な偽メールが発信されております。」と注意喚起※142 を行っている。

(c) ウイルスに感染させる手口

悪意のある URL あるいは添付ファイルを介して、最初にダウンローダに感染させ、そのダウンローダが不正接続先にアクセスして DreamBot 本体をダウンロード、自動実行する。

■図 1-3-9　楽天カード株式会社をかたったばらまき型メールの例

- URL を使った手口
  メール本文中に悪意のある URL を記載する手口は、前述のとおり、指定された拡張子の添付ファイルの削除等を行うセキュリティソフトやスパムメール対策のフィルタリング等による検知を回避することを狙ったものと推測されるが、受信者に URL をクリックさせる工夫もなされている。例えば、HTML 形式のメールで、詐称した組織の正規の URL が表示されているが、そのリンク先には悪意のあるファイルをダウンロードさせるための通信先が設定されている攻撃を確認した（図 1-3-10）。



■図 1-3-10　三菱 UFJ 信託銀行をかたったばらまき型メールの例

- Microsoft Office の脆弱性を悪用する手口
  DreamBot ダウンロードのための不正通信を発生させる過程で、Microsoft Office の文書ファイルの脆弱性 CVE-2017-0199※143 や CVE-2017-11882※144 を悪用する攻撃も確認されている。CVE-2017-11882 を悪用

した攻撃では、修正プログラムの公開から約 1 週間という短い期間で攻撃に転用されていた。

(2) ばらまき型メールへの対策

ばらまき型メールの攻撃者は、今回紹介した DreamBot 等のウイルスに感染させる確率を上げるために様々な細工を施しており、常に新たな手口で攻撃してくる可能性がある。セキュリティソフトの活用、スパムメール対策、メール受信者の自己防衛等の対策を実施し、多層的な防御を行うことが重要である。

(a) 一般利用者における対策

次に示す基本的な対策は、今回紹介したばらまき型メール以外の攻撃に対しても有効であり、徹底することを推奨する。

- セキュリティソフトを導入する
  ウイルスであると判断できずに添付ファイル等を開いてしまっても、セキュリティソフトが検知・検疫し、被害を免れられる可能性がある。セキュリティソフトを常に最新に保つことも重要である。
- 不用意にメールの指示に従わない
  受信したメールに疑問や不審感を抱いた場合は、送信者となっている企業や組織の公式サイトでばらまき型メールに関する注意喚起が公開されていないかを確認するか、当該メールの送付有無を問い合わせてみる。真偽が分からない段階では、メールへの返信、添付ファイルの開封、本文中に記載されている URL へのアクセスは避けるべきである。
  ばらまき型メールに関する注意喚起情報は JC3、警察庁、セキュリティベンダや金融機関等が公開している。日頃から最新の動向を確認し、よく使われている件名や手口等を知っておくことで、不審なメールに対する注意力を向上させることができる。
- OS やソフトウェアのバージョンを常に最新に保つ
  適宜、修正プログラムを適用し、既知の脆弱性を解消しておくことで、脆弱性を悪用した攻撃が成功する確率を下げることができる。

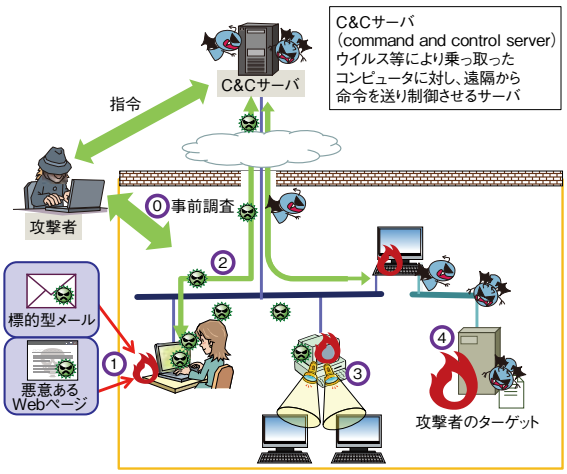
(b) 組織・企業における対策

組織・企業におけるばらまき型メールに対する対策は、「1.3.5 (4) 標的型攻撃への対策」で述べている内容と基本的には同じである。不審なメールを受信した際の報告窓口を設ける等の組織体制の整備、ウイルス感染を想定した利用者の教育と訓練、またシステムでの対策として、特定のファイル形式について実行許可・禁止の設定をする、不正通信のログの監視と管理を行う、等の対策が重要である。

1.3.5 標的型攻撃

標的型攻撃とは、ある特定の企業や組織を狙って行われるサイバー攻撃である。不特定多数の相手に対して無差別にウイルスメールやフィッシングメールを送信する攻撃等とは異なり、標的型攻撃は特定の企業や組織が保有している機密情報の窃取やシステム・設備の破壊・停止を目的として行われる。また、標的型攻撃は長期間継続して行われることが多く、攻撃者が標的とする組織の内部に数年間潜入して活動していたと考えられる事例も日本国内で確認されている※145。

IPA では過去の標的型攻撃の事例等から、標的型攻撃の流れを五つの段階に分けてとらえている(図 1-3-11)。



0 [事前調査]
ターゲットとなる組織を攻撃するための情報を収集する。

1 [初期潜入段階]
標的型メールや、Webサイト閲覧を通してウイルスに感染させる。

2 [攻撃基盤構築段階]
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い、新たなウイルスをダウンロードする。

3 [システム調査段階]
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を基に新たな攻撃を仕掛ける。

4 [攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

■図 1-3-11　標的型攻撃の流れ
(出典)IPA「標的型サイバー攻撃の脅威と対策※146」を基に編集

「事前調査」の段階では、標的とする企業・組織や業界の情報を収集する。公開されている情報を収集するだけではなく、標的とする組織と他の組織がやり取りするメールの盗聴、もしくはなりすまし等により情報を収集す

ることもある。

次の「初期潜入段階」では、攻撃者が「事前調査」で得た情報を基にして、標的とする組織の端末にウイルスを感染させようと試みる。手口としてよく用いられるのは、ウイルスを添付したメールを標的とする組織の人間に送付する手法である。このメールは「標的型攻撃メール」と呼ばれる。

標的型攻撃メールに使用されるメールの文面は、標的とする組織に合わせて作成したものが用いられることが多い。また、ウイルスが検出されることを回避するために、パスワードを設定した圧縮ファイルにウイルスを格納してメールに添付する※147といった細工がなされることもある。

「初期潜入段階」で標的の内部に侵入した攻撃者は、「攻撃基盤構築段階」に移る。攻撃者は感染端末の遠隔操作を可能にするために、遠隔操作ウイルス（Remote Access Trojan：RAT）に感染させることを試みる。遠隔操作を長期的かつ継続的に行えるように、複数のRATに感染させる場合もある。遠隔操作ウイルスに感染させる手口として、「ダウンローダ」と呼ばれる、別のウイルスを外部からダウンロードする機能を持つウイルスが「初期潜入段階」で用いられることが多い。

「システム調査段階」に入ると、攻撃者は先に感染させた遠隔操作ウイルス等を用いて、侵入した組織のネットワークを攻撃するために必要なツールや別のウイルスを送り込む。送り込んだツールやウイルスを用いて、攻撃者はネットワーク構成の把握、管理者権限の奪取、目的とする情報の探索等を行う。

「攻撃最終目的の遂行段階」では、攻撃者は目的とする情報の窃取等を行う。また、目的を遂行した攻撃者が、侵入した端末内でファイルを暗号化して使用不能にするウイルス（ランサムウェア）を実行したという事例も確認されている※148。これは身代金による金銭が目的ではなく、情報窃取の痕跡を発見しにくくする目的によるものと推察される。

標的型攻撃は、以上のような流れで行われる。海外では、情報の窃取を目的とした攻撃以外に、工場や発電所のような生活インフラに含まれる施設の停止を目的とした攻撃も確認されている※149。

(1) 標的型攻撃の傾向

標的型攻撃による被害は2011年に複数の重工業メーカ等が攻撃対象となった事件以降、継続して発生しているが、2017年については、国内で標的型攻撃による大きな被害が発生したという情報は公開されていない。

しかし、2016年の秋ごろから、国内の組織に対して標的型攻撃メールが送信されていることがJPCERT/CCから公表されている。2017年にも、前年と同一の攻撃者によると思われる国内組織への攻撃が公表されている※150。標的型攻撃は今後も継続して行われると考えられ、常に対策を講じておくことが必要である。

(2) 標的型攻撃メールの手口

標的型攻撃メールは非常に巧妙に偽装されているだけでなく、本物のメールを基に作成されていることもある。受信者が不審に思わないように、特定の企業・組織でよく用いられる言葉を件名やメール本文に用いる等の細工が施されるものも多いため、開封を完全に防ぐのは難しい。しかし、標的型攻撃メールに関する訓練・教育や、組織的・システム的な対応によって開封リスクの低減、もしくは開封した（ウイルスに感染した）際の被害リスクの低減は可能である。ここでは、標的型攻撃メールで用いられる手口の事例を紹介する。

(a) 件名や本文の内容による騙しの手口

攻撃者は、標的型攻撃メールの受信者が違和感を覚えずにメールを開封させるように仕向けるため、日常の業務で使用される件名や内容を用いたメールを作成することが多い。また、標的とする企業・組織や業界で使われる言葉を用いた手口も確認されている。

2017年1月、独立行政法人日本学術振興会※151をかたった標的型攻撃メールが日本国内の複数組織に対して送信された。公開されている注意喚起情報によると、このメールには「【H 29 科研費】繰越申請について」という件名が使用され、本文も日本学術振興会が行っている科学研究費助成事業に関する内容となっている※152。攻撃者は日本学術振興会が実際に行っている事業内容をメールに記載することで、受信者が標的型攻撃メールであることに気付きにくくさせている。

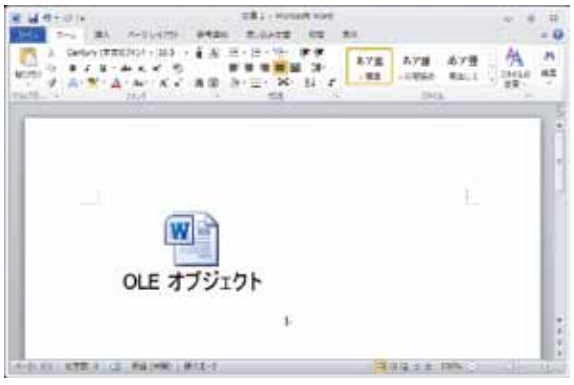
なお、標的型攻撃メールの件名や本文には一般公開情報が流用されることが多いが、非公開の情報（組織内部の人間しか知らない情報等）が用いられることもある。

(b) 添付ファイルの手口

標的型攻撃メールの添付ファイルは、攻撃であると気付かれにくくするために、巧妙な細工が施されることが多い。例えば、アイコンの偽装、RLO（Right-to-Left Override）等による拡張子の偽装、ショートカット（LNK）

ファイル（以下、LNK ファイル）の悪用、Microsoft Office の脆弱性・マクロ機能・OLE（Object Linking and Embedding）オブジェクトの悪用等がある。これらの手口は 2016 年に引き続き、2017 年にも確認されている。以下では、2017 年に確認された三つの手口について紹介する。

- LNK ファイルを悪用する手口
  一般には LNK ファイルの危険性はあまり認識されていないが、スクリプトと呼ばれる命令を埋め込むことで、実行ファイルと同等の動作をさせることが可能である。JavaScript や VBScript のスクリプトが埋め込まれた LNK ファイルが過去の標的型攻撃では多く用いられてきたが、2017 年には Windows PowerShell（以下、PowerShell）のスクリプトを用いた攻撃が複数確認された。
- Microsoft の OLE オブジェクトを悪用する手口
  Microsoft の OLE とは、あるアプリケーションで作成されたオブジェクトを、別のアプリケーションでも使用できるようにする技術である。OLE を利用したオブジェクトを「OLE オブジェクト」と呼ぶ。
  OLE を悪用すると、Microsoft Office の文書ファイルに悪意のあるプログラムやウイルス等をオブジェクトとして埋め込むことが可能になる。標的型攻撃メールに添付された文書ファイルを開き、OLE オブジェクトとして埋め込まれたウイルスをクリックして実行するとウイルスに感染してしまう、という手口が確認されている（図 1-3-12）。



■図 1-3-12　OLE オブジェクトを埋め込んだ Word ファイルの例

- ファイルストレージサービスを悪用した手口
  標的型攻撃メールはウイルスを添付して標的に送りつける場合が多いが、ファイルストレージサービスを用いた事例も確認されている※153。
  2017 年に国内で確認された標的型攻撃の事例では、標的型攻撃メールの本文中にファイルストレージサービスの URL リンクが記載されたものがあった。この URL リンクから圧縮ファイルをダウンロードすることが可能となっており、この中にウイルスが格納されていた。メールにウイルスを添付せず、受信者にダウンロードさせる形を取ることで、メールの配送経路上におけるウイルスチェックを回避しようとしたものと考えられる。

(3) 国内の標的型攻撃事例

「初期潜入段階」において使用される標的型攻撃メールでは、圧縮ファイルの中に実行ファイルを格納したものや、文書作成ソフトの脆弱性を悪用するファイルが添付されたものが一般的とされている。

しかし、2015 年ごろから、先に紹介した LNK ファイルを悪用する手口等の、従来とは異なる攻撃手法を用いた攻撃も観測されている。そのような事例のうち、2017 年に国内で観測されたものを紹介する。

(a) アメリカ学会をかたる標的型攻撃

2017 年 7 月、アメリカ学会をかたるなりすましメールが関係者に対して送信されているという注意喚起が同組織の Web サイトに掲載された※154。

後日、セキュリティベンダが当該なりすましメールの詳細な情報を紹介しており、それによると、送信されたなりすましメール（標的型攻撃メール）の本文中に、正規のファイルストレージサービスの URL リンクが記載されていたという※153。また、メール本文中では、受信者に対してこの URL リンクからファイルをダウンロードするように指示がなされていた（図 1-3-13）。

■図 1-3-13　不審メール（一部抜粋）
（出典）株式会社ラック「PowerShell Empire を利用した標的型攻撃※153」

この URL リンクからダウンロードされる圧縮ファイルの中には 2 種類のファイルが入っており、それぞれリッチテキスト（RTF）ファイルとアイコンが偽装された LNK ファイ

ルとなっていた。以下では、二つのファイルのうち、LNKファイルの挙動を紹介する。

上記のLNKファイルを実行すると、攻撃者の管理するサーバから悪意のあるファイルがダウンロードされる。ダウンロードされるファイルはPowerShellのスクリプトで、これが攻撃者の管理する外部のサーバと不正な通信を行う。

注目すべき事項は、このとき実行されるスクリプトがディスク上に保存されずに、「端末のメモリ上でのみ使用される」という点である。ファイルとしてディスク上に保存・作成されないため、セキュリティソフトのファイルスキャン等で検出することが難しくなっている。

このような、攻撃対象の端末上に極力痕跡を残さず、また、メモリ上でのみ悪意のあるファイルを動作させる攻撃は「ファイルレス攻撃」や「ファイルレス活動」と呼ばれる※155。実行ファイルが添付されたメールへの対策が進んだ組織に対する攻撃方法として、今後も本事例のような手口が多く用いられることが予想される。

(b) リモートアクセスツールとランサムウェアを用いた標的型攻撃

2017年7月、セキュリティベンダから、日本を攻撃対象としていると思われるランサムウェア「ONI」を確認したという情報が公開された※156。この情報には以下の内容が記載されていた。

- ONIは「GlobeImposter」と呼ばれるランサムウェアの亜種である。
- GlobeImposterは高度なシステム侵入の一環で使用されたことがある。

同年11月には、上記のONIが日本国内の組織に対する標的型攻撃で証拠隠滅のために用いられたと思われる事例が公表された※148。

本事例の「初期潜入段階」では、標的型攻撃メールに悪意のある文書ファイルが添付されて、標的となる組織に送信される。文書ファイルを開いてマクロが有効化されると、「Ammyy Admin」と呼ばれる、正規のリモートアクセスツールが端末に送り込まれる。攻撃者はこれを足掛かりにして、標的となる組織のネットワーク内に侵入する。

「システム調査段階」では、攻撃者は侵入したネットワークの内部で活動範囲を拡大させる。その際に、ランサムウェア「Wanna Cryptor」にも使用された脆弱性攻撃ツール「EternalBlue」が悪用された可能性があるとされている(EternalBlueについては「1.3.3 (2) Windowsの脆弱性を悪用した攻撃」参照)。攻撃者は複数の端末を侵害し、最終的にドメインコントローラ、Active Directoryサーバを掌握する。

「攻撃最終目的の遂行段階」では、目的とする情報を窃取した後、攻撃者はドメイン内の各端末でログの削除とONIの配布を行う。単純にログを削除するだけにとどまらず、ランサムウェアを用いて調査を妨害したと思われる点が、これまでに確認されている標的型攻撃とは異なっている。

(4) 標的型攻撃への対策

標的型攻撃への対策例を以下に示す。

(a) 利用者向けの対策

標的型攻撃への対策としては、複数の対策を組み合わせて防御する、多層防御が有効であるとされている。その一要素として、「利用者の注意力」も重要になっている。

- 不審メールに対する注意力の向上

  標的型攻撃メールでは、標的とする企業・組織に関係している人物のメールアカウントを攻撃者が侵害してメールを送信するものや、組織固有の用語等をメール本文中で用いて不自然さをなくそうとするもの等、受信者を騙すために巧妙な手口が用いられることがある。しかし、送信元メールアドレスに無料で取得できるフリーメールアドレスが使用されている等、不審であると気付きやすいメールも存在する。

  不審なメールと気づきやすい一例として、メールソフトが表示する送信者の名前の偽装がある。送信者の情報を確認する際は、表示されている送信者名ではなく、メールアドレスが正しいかどうかを確認することで偽装が分かる場合がある。身に覚えのないメールアドレスから送信されている場合、添付ファイルは開かないようにすべきである。前述のとおり、フリーメールアドレスであった場合も要注意である。

  受信したメールが本物かどうかを確認したい場合、送信者に問い合わせるのは有効な方法である。ただし、メール本文や署名欄に記載されている連絡先に問い合わせるのは、攻撃者によって用意されたメールアドレス等の可能性があるためこれを避け、信頼できる正しい問い合わせ先を別途確認した上で問い合わせすべきである。

  また、関係する企業・組織のWebサイトで「不審メー

ルの送信を確認している」といった注意喚起情報が発信されていないか確認することも有効である。

- マクロ機能の危険性の周知
  Microsoft Office のマクロ機能とは、Microsoft Office 製品に搭載されている VBA と呼ばれるプログラミング言語によって、特定の操作を自動化する機能である。マクロ機能は便利だが、この機能を悪用して、不正なプログラムを文書ファイル内に仕込むことも可能である。マクロ機能はデフォルトでは無効になっているが、多くの組織でマクロ機能は広く利用されており、マクロを有効化している利用者がいる可能性もある。
  マクロ機能は標的型攻撃メールだけでなく、ばらまき型メールでもウイルス感染の手口として多く用いられているため、不用意に「コンテンツの有効化」（マクロの有効化）を行わないように注意が必要である。マクロの有効化は、ファイルの入手元が信頼できるかを確認する等、安全性を確保してから行うべきである。
- ファイルストレージサービス等を使用した手口の周知
  業務において外部のファイルストレージサービスを使用する可能性がある場合、そのようなサービスを用いた攻撃が存在する、という事実を周知しておくべきである。また、正規のファイルストレージサービスではなく、攻撃者が用意したと思われるサーバを使用し、メール本文中に当該サーバの URL リンクを記載して、受信者にファイルをダウンロードさせる手口も、2017 年に観測されたばらまき型メールで用いられているため、注意が必要である。
- Microsoft OLE オブジェクトの危険性の周知
  OLEオブジェクトを悪用する手口も標的型攻撃メール、ばらまき型メールで用いられるようになっており、その手口について、IPA が注意喚起の資料※157 を公開した。この資料で紹介している手口では、文書ファイルの中にアイコンのような画像が埋め込まれており、これをダブルクリックすると領収書が確認できるという一文が記載されている。これに従って操作すると埋め込まれた不正な OLE オブジェクトが実行され、ウイルスに感染させられてしまう。
  このような、文書ファイルに不正な OLE オブジェクトを埋め込み、言葉巧みに実行させることでウイルスに感染させる手口も存在することを、利用者に周知しておくことが重要である。
- 脆弱性放置の危険性の周知
  前述した EternalBlue のように脆弱性を悪用してウイルス感染及び感染拡大を図る手口が確認されている。適切な対処をせずに脆弱性が放置されていると、攻撃者による侵入やその後の攻撃を容易にさせてしまう危険性がある。
  公開されたセキュリティ更新プログラムは適宜適用し、脆弱性を解消するよう周知、徹底しておくことが重要である。

(b) 組織体制による対策

利用者が標的型攻撃メール等の不審なメールを受信した際の連絡窓口が組織内に周知されていることも、標的型攻撃対策の一つとして重要である。連絡窓口が周知されていない場合、利用者がどこに連絡をすれば良いか分からず、結果として組織が攻撃を受けていることに気付くのが遅れてしまう可能性がある。また、外部からの情報提供によって組織が標的型攻撃を受けていることに気付く事例もあるが、その場合も、外部からの連絡を受ける窓口が重要となる。

組織内部・外部における適切な連絡体制の整備、セキュリティインシデントの調査、分析、セキュリティの教育・啓発活動の実施等を行う組織・体制のことを CSIRT（Computer Security Incident Response Team）と呼ぶ。セキュリティインシデントの未然防止、もしくはインシデント発生時の迅速な対応を行うために、CSIRT やそれに準ずる体制を組織内に設置することは有効な手段となる。

また、組織内外から得られるインシデント関連情報を集約し、最高情報セキュリティ責任者（Chief Information Security Officer：CISO）や担当役員が連携してインシデントに対応する体制を整備することも重要である（企業経営陣のセキュリティへの参画については「2.5.1 情報セキュリティと経営」参照）。

(c) ウイルス感染を想定した訓練と教育

組織内に CSIRT 等の体制を整えるだけでなく、実際のインシデント発生時に適切な対応ができるように、対応能力を維持・向上させる取り組みが必要となる。

例えば、利用者向けの取り組みでは、疑似的な標的型攻撃メールを利用者に送信して、不審メールへの対応能力を高める訓練（標的型攻撃メール訓練）がある。

訓練を通じて、不審メールを受信した場合に着目すべき箇所の再確認や、不審メールを受信した際、または受信した不審メールの添付ファイルを開いてしまった（ウイルスに感染した）際に必要となる対処の再確認等を行う。このような訓練を定期的に実施することで、利用者の対

応能力を維持・向上させる。

また、先に紹介したMicrosoft Officeのマクロ機能やOLEオブジェクトを用いた標的型攻撃メールのような、具体的な攻撃手口を利用者に事前に周知することも、対応能力の向上に有効である。

(d)システムによる対策

システムで実施すべき対策の例を以下に示す。

- 不審なメールを確保できる仕組みの確立
  メールの添付ファイルをウイルスとして検知した場合、当該ファイルを削除、無害化、もしくはメールそのものをブロックするセキュリティ製品やサービスが存在する。セキュリティ製品やサービスがこのような対処を行った場合、ウイルスの通信先情報やメールの送信元アドレスが確認できず、攻撃の詳細な情報が得られずに今後の対策に活用できない可能性がある。
  そのため、例えば、ウイルスを検知した場合、自動的に削除するのではなく、システムの管理者だけがアクセス可能な場所に隔離する等の仕組みを確立する。そして、隔離されたウイルスをCSIRT等で解析することで、ウイルスが不正な通信を行うドメインの情報を取得し、これを組織内のプロキシに設定することで不正な通信の検出、遮断に利用することができる。
- ファイルの実行防止
  あらかじめ、システムや実行ポリシーで、利用者の環境で実行可能なファイルを制限(ホワイトリスト化)しておくことで、ウイルスへの感染を防止する。ホワイトリストによる制限の実施が難しい場合、利用者の環境で実行することが望ましくないファイルの種類をシステムや実行ポリシーで制限(ブラックリスト化)する。
  悪用されることの多いスクリプトファイル(.jsや.ps1等)のような、通常利用しないであろうファイルの実行を禁止することで、ウイルスへの感染を防止する。
- 保護ビューの設定
  Microsoft Office製品(Office 2010以降)とAdobe Acrobat Readerには、安全ではない可能性がある場所から入手したファイルを読み取り専用の状態で開く「保護ビュー※158」と呼ばれる機能が備わっている。この機能を有効にしておくことで、例えば、悪意のあるMicrosoft OLEオブジェクトを文書ファイルに埋め込む手口の攻撃や、文書ソフトの脆弱性を悪用する攻撃等の実行を防げる可能性がある。
- PowerShellの実行の制限
  ファイルレス攻撃の初期潜入段階では、PowerShellのスクリプトが悪用されるケースが多く確認されている。また、近年では、PowerShellのスクリプトは標的型攻撃メールだけでなく、ばらまき型メールでも多く悪用されている。普段の業務でPowerShellを使用することがない場合、PowerShellの実行をシステムによって制限することが対策として有効である。
- 通信ログの取得と監視
  ウイルスに感染した場合、ウイルスの侵入経路、感染範囲の特定、C&C(Command and Control)サーバへの通信の有無等を調査する必要がある。組織内の通信ログ等が適切に取得できていない場合、上記の調査が困難となる。調査時点から過去に遡って不正通信等の調査を行うために、必要な各種ログを一定期間保存することが望ましい。
  また、通信ログを定期的に監視して、組織内の端末からC&Cサーバへ不正通信が発生していないか等をチェックし、早期にウイルスを発見するため、SOC(Security Operation Center)を設置することが望ましい。自組織での運用が困難である場合は、SOCサービス事業者の提供するサービスを利用することも可能である。

以上のように、標的型攻撃への対策は多層防御の考え方に基づき、利用者の不審メールに対する注意力の向上、インシデント発生時に適切な対応ができる組織体制の構築、システムによる各種対策等の複数の観点で実施していくことが重要である。

1.3.6 ビジネスメール詐欺

ビジネスメール詐欺は、巧妙な騙しの手口を駆使した偽のメールを組織・企業に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらすソーシャルエンジニアリング※159の手法を応用した攻撃である。攻撃の準備として、企業内の従業員等の情報が狙われたり、情報を窃取するウイルスが使用されたりすることもある※160。

2017年4月、IPAはJ-CSIP※161の活動から得られた情報を基に、実際に国内企業や海外関連企業、あるいはその取引先が受けた攻撃について、攻撃者とのメールのやり取りや、メールに仕掛けられた様々な騙しの手口を公開し、注意喚起した※162。その後も国内組織への攻撃を確認したため、2017年7月と2018年1月のJ-CSIPの活動報告の中で、具体的な手口を公開した※163。

このように、ビジネスメール詐欺は国内でも複数の攻撃が確認され大きな脅威となっており、今後ますます注意が必要な状況である。ここでは、ビジネスメール詐欺の手口と対策について解説する。

(1)ビジネスメール詐欺の五つのタイプ

IC3[※90]やトレンドマイクロ社[※164]では、ビジネスメール詐欺の手口を主に五つのタイプに分類している。

(a)タイプ1:取引先との請求書の偽装

「偽の請求書詐欺(The Bogus Invoice Scheme)」や、「サプライヤー詐欺(The Supplier Swindle)」「請求書偽装の手口(Invoice Modification Scheme)」等と呼ばれ、海外の企業との取り引きを行っている企業が主に被害に遭う傾向がある。

この手口では、請求に関わるやり取りをメール等で行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等を送り付け、振り込みをさせる。

攻撃者は取り引きに関係するメールのやり取りを何らかの方法によって事前に盗聴し、取り引きや請求に関する情報や、関係している従業員のメールアドレスや氏名等を入手していることもある(図1-3-14)。

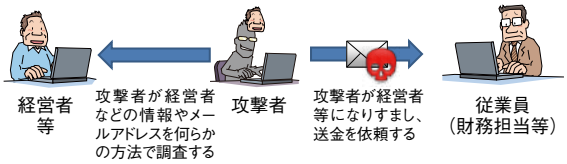
■図1-3-14　取引先との請求書の偽装の例
(出典)IPA「【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口[※162]」

(b)タイプ2:経営者等へのなりすまし

「CEO詐欺(CEO Fraud)」や、「企業幹部詐欺(Business Executive Scam)」「なりすまし詐欺(Masquerading)」「金融業界送金詐欺(Financial Industry Wire Frauds)」等と呼ばれ、企業の財務部等の金銭管理を行う部門が被害に遭う傾向がある。

この手口では、攻撃者が企業の経営者や企業幹部等になりすまし、企業の従業員に攻撃者の用意した口座へ振り込みをさせる(図1-3-15)。

事前に攻撃者は何らかの方法によって、企業の経営者等のメールアドレスを調べ、より本物らしくなりすましを行う場合もある。

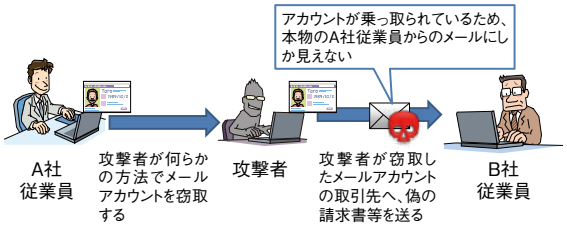


■図1-3-15　経営者等へのなりすましの例
(出典)IPA「【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口」

(c)タイプ3:窃取したメールアカウントの悪用

この手口では、攻撃者が従業員のメールアカウントの情報を何らかの手段を用いて窃取し、乗っ取る。その後、そのメールアカウント(従業員)と取引実績のある別の企業の担当者へ、攻撃者の用意した口座に差し替えた偽の請求書等をメールで送り付け、振り込みをさせる(図1-3-16)。

メールの受信者側から見ると、正当な相手を送信元としたメールであるため、攻撃であると気付きにくい。

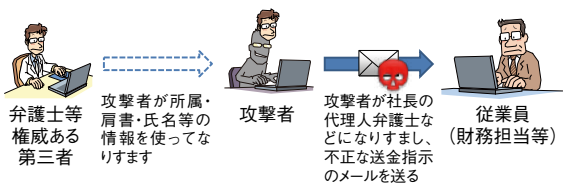


■図1-3-16　窃取したメールアカウントの悪用の例
(出典)IPA「【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口」

(d)タイプ4:社外の権威ある第三者へのなりすまし

この手口では、攻撃者が弁護士や法律事務所といった社外の権威ある第三者になりすまし、企業の財務担当者等に対してメールを送信し、攻撃者の用意した口座への振り込みをさせる(図1-3-17)。

例えば、攻撃者は企業の社長の代理人弁護士になりすまし、緊急を要する機密案件であるとその企業の担当者に伝え、秘密裏かつ迅速に対応するよう圧力をかけて送金を促す。

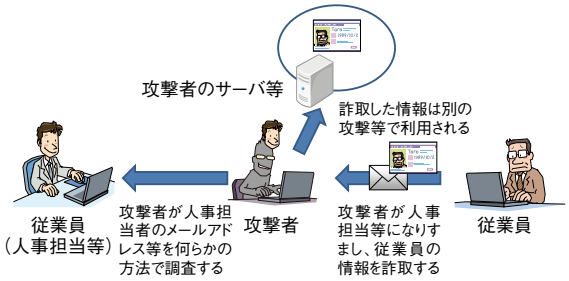


■図1-3-17　社外の権威ある第三者へのなりすましの例
(出典)IPA「【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口」

(e) タイプ 5：詐欺の準備行為と思われる情報の詐取

この手口は、攻撃者がビジネスメール詐欺の標的とする企業の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、他の従業員の個人情報等を詐取するもので、不正な送金要求の前段階として行われることがある（図 1-3-18）。

詐取された情報は、攻撃者のサーバ等に送られ、別の攻撃等に悪用されることがある。この手口はタイプ 1 ～ 4 と異なり、金銭の詐取ではなく、今後何らかの攻撃を行うための情報を得ることが目的と考えられる。



■図 1-3-18　詐欺の準備行為と思われる情報の詐取の例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口」

(2) ビジネスメール詐欺の騙しの手口

ビジネスメール詐欺で用いられる騙しの手口は様々であるが、ここでは J-CSIP の活動から得られた情報を基に、実際に使われた具体的な手口の一部を紹介する。ここで紹介する手口を組み合わせて巧妙に攻撃を仕掛けてくる場合があるため、注意が必要である。

(a) 偽の口座へ振り込ませる手口

攻撃者が用意した偽の口座へ振り込ませる手口として、次のようなものを確認している。

- 請求書に誤りがあったと連絡し、偽の口座が書かれた請求書を送付して支払いを要求する。
- 銀行口座が国の監査を受けているため振り込みができないという理由をつけて偽の口座への支払いを要求する。
- 為替レートの問題があり、新たな口座を開設したと理由をつけて偽の口座への支払いを要求する。
- 既に支払い済みの金銭は返金したと虚偽の申告をして再送金して欲しいと偽の口座への支払いを要求する。
- 経営者等になりすまして「緊急かつ秘密の案件」と称し、送金を要求する。

(b) メールの引用部分改変の手口

メールのやり取りの中で、攻撃者に都合が悪く矛盾のある引用部分を改変する手口を確認している。

- 引用部分にある過去メール本文の一部を削除または改変する。
- 引用部分にある過去メールの From/To/Cc のメールアドレスの一部を削除または改変する。

(c) メールアドレスのなりすましの手口

攻撃者は標的とした人物を騙すため、本物の取引先等のメールアドレスに似せた偽のメールアドレスを使い、「メールアドレスの見た目」によるなりすましを行う手口を確認している。攻撃者がなりすましに使う偽のメールアドレスの作り方には次のような特徴がある。

①メールアドレスを 1 文字入れ替える。
②メールアドレスに 1 文字追加する。
③メールアドレスを 1 文字削除する。
④メールアドレスの一部を誤認しやすい文字に置き換える（例：m（M）→ rn（RN））。
⑤フリーメールサービスを使い、もっともらしいメールアドレスを作る。

例えば、本物のメールアドレスが「alice@company-a.com」である場合、攻撃者がどのようなメールアドレスをなりすましに使うかを、図 1-3-19 に示す（ここではフリーメールのドメインを「freemail.com」としている）。

■本物のメールアドレス		alice @ company-a . com
■偽物のメールアドレス	①	alice @ compnay-a . com
	②	alice @ companys-a . com
		aalice @ company-a . com
	③	alice @ comp ny-a . com
	④	alice @ cornpany-a . com
	⑤	alice-company-a @ freemail.com

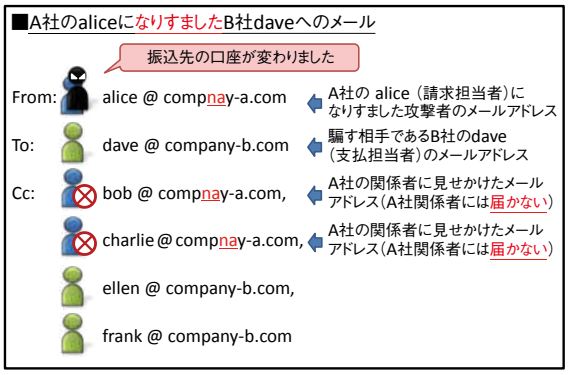
■図 1-3-19　攻撃者によるメールアドレスのなりすましの例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口」

(d) 同報メールアドレスの改変の手口

受信者に本物のメールであると錯覚させ、なりすましメールの発覚を遅らせるため、攻撃者がメールの To（宛先）や Cc（同報先）に設定するメールアドレスを細工して、あたかも複数の担当者にも同報でメール送信がされているかのように見せかける手口を確認している。

例えば、図 1-3-20（次ページ）のように攻撃者が A 社の請求担当者「alice」になりすまし、B 社の支払担当者

「dave」へ偽のメールを送った際に、A 社関係者の同報メールアドレスを部分的に改変し、多数の取引関係者に対して同報されているように錯覚させる。



■図 1-3-20　攻撃者による同報メールアドレスの改変の例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口」

この例では、A 社の他の担当者も Cc で同報されているように見えるが、実際には届いていない。すなわち、B 社（騙す相手）の担当者にのみ届いているため、A 社側はなりすましメールが送信されていることに気付くことができない。

更に、Cc にある B 社の同僚（ellen、frank）のメールアドレスも改変されたケースを確認している。その場合、実際にメールを受信したのは B 社の dave（騙す相手）一人のみとなる。

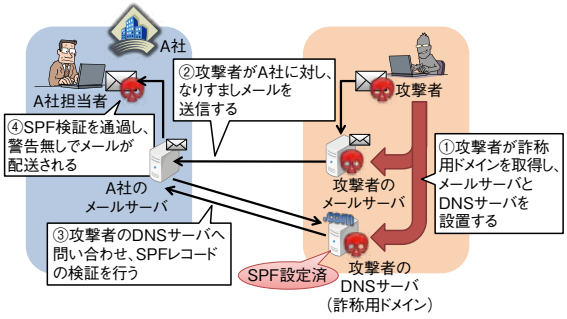
(e) 詐称用ドメインの取得と悪用の手口

攻撃者がなりすましを行う企業のものとよく似た「詐称用ドメイン」を取得し、なりすましメールが正当なメールサーバから送信されたものであるかのように偽装（送信ドメイン認証技術による警告対象となることを回避）する手口を確認している。

- SPF（Sender Policy Framework）※165 を悪用する手口

  攻撃者は、詐称用ドメインの DNS 情報に SPF レコードを設定し、受信側の SPF 検証を通過（Pass）させる。受信サーバ側は送信されたメールのドメイン名を基に、取得した DNS サーバの SPF レコードと送信元メールサーバの IP アドレスとの整合性が確認できれば送信ドメインを認証し、警告なしでメールを配信してしまう場合がある。

  攻撃者によって詐称用ドメインが取得され、DNS サーバに当該ドメインの SPF レコードが設定された場合に、なりすましメールが配送される流れを図 1-3-21 に示す。



■図 1-3-21　SPF レコード設定済みの詐称用ドメインによるなりすましメールの配送の例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口」

- DKIM（DomainKeys Identified Mail）※166 を悪用する手口

  攻撃者は、詐称用ドメインの DNS 情報に DKIM レコードを設定し、なりすましメール送信の際に電子署名を付加することで、受信側の DKIM 検証を通過（Pass）させる。DKIM 検証の際、受信側で電子署名が照合できれば送信ドメインを認証し、警告なしでメールを配信してしまう場合がある。

送信ドメイン認証技術（SPF や DKIM）を悪用する手口では、攻撃者が詐称用ドメインを取得後、短期間のうちに DNS やメールサーバの設定を実施し、なりすましメールを送信する傾向が見られた。不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられる。あるいは、詐欺がうまく進みそうな場合に、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動を取っている可能性もある。

(f) 送信元を偽装して攻撃者に返信させる手口

送信元（From）メールアドレスを本物のメールアドレスに偽装し、返信先（Reply-To）メールアドレスを攻撃者のメールアドレスにするという手口を確認している。

メールの仕組み上、送信元（From ヘッダ）は、メールを送信する側が任意の内容に指定（偽装）できる。メール受信者のメール表示画面には、この From ヘッダの内容が「送信者」として表示されるため、あたかも本物のメールアドレスから送信されたメールのように見える。そのメールの返信先（Reply-To ヘッダ）に、攻撃者のメールアドレスが設定されていた場合、返信メールの作成画面では Reply-To ヘッダに設定されたメールアドレスが宛先となるため、この時点で気付くことができなければ、攻撃

者とメールをやり取りしてしまうことになる。

例えば、攻撃者が企業の経営者（CEO）を詐称し、財務責任者（CFO）を騙そうとする際、次のような設定を行っていた。

- メールの送信元（From ヘッダ）には、本物の CEO の名前やメールアドレスを設定する。
- メールの返信先（Reply-To ヘッダ）には、攻撃者のメールアドレスを設定する。

(3) ビジネスメール詐欺への対策

ビジネスメール詐欺の被害に遭わないようにするためには、ビジネスメール詐欺について理解するとともに、不審なメール等への意識を高め、組織内の体制を強化しておくこと等が重要である。

(a) ビジネスメール詐欺の周知徹底

ビジネスメール詐欺は、企業間のビジネスがメールに依存している（メールを信頼している）点を逆手に取った巧妙な騙しの手口であり、その手口を知らなければ、攻撃であることを見破り、被害を防止することは困難である。

まず、全従業員（海外関連企業を含む全グループ企業の従業員）に詐欺の手口について周知徹底し、ビジネスメール詐欺への意識を高めておくことが重要である。

特に、送金処理に関係する担当者等がビジネスメール詐欺の脅威についてよく理解し、攻撃に気付くことができれば、金銭被害を未然に防ぐ可能性が高まる。また、社内だけでなく、取引先等に対しても、ビジネスメール詐欺への注意を促すことも有効である。

(b) 組織内外での情報共有

ビジネスメール詐欺に限らず、メールは多くのサイバー攻撃の入口でもあり、一人ひとりが注意を払うべきである。メールを確認している中で、普段とは異なる言い回しや表現の誤りがある等、不審な兆候が見られた場合、CSIRT 等の適切な部門に報告できる体制を整え、その情報を組織内外で共有することも重要である。

ビジネスメール詐欺の場合、自組織だけではなく、取引先に被害が及ぶことがある。取引先と情報を共有することにより、サプライチェーン全体のビジネスメール詐欺への耐性を高めることができる。

自組織を詐称したビジネスメール詐欺を確認した場合や自組織が被害に巻き込まれた場合等に、取引先全体や、警察、金融機関へ報告し、一般に向けても注意喚起を行うといった体制を整えておくことで、更なる被害拡大を防ぐことが可能となる。

(c) 送金処理のチェック体制強化

ビジネスメール詐欺による被害防止のためには、送金時のチェック体制を強化することが特に重要である。

例えば、突然の振込先の変更や、急な送金の依頼といった、通常とは異なる対応を求められた場合は、ビジネスメール詐欺を疑い、別の担当者とダブルチェックを行うことや、信頼できる方法で入手した連絡先に、電話や FAX 等のメールとは異なる手段で事実を確認するといったように、二重三重のチェックを行う体制とすることが必要である。

(d) 類似ドメインへの対応

ビジネスメール詐欺の攻撃者は、自組織や取引先のドメイン名に似た詐称用のドメインを取得し、攻撃を行うことがあるため、定期的に、自組織に似たドメイン名が取得されていないかを確認し、不審なドメインが取得されていた場合、必要であれば注意喚起を行う。併せて、取引先等に対しても、不審なドメインが取得されていないか確認することを促すことが望ましい。

(e) ウイルス・不正アクセス対策

ビジネスメール詐欺では、攻撃や被害に至る前に、何らかの方法（メールの内容やメールアカウントの情報を窃取するウイルスの感染、メールサーバへの不正アクセス等）で攻撃者によってメールが盗み見られている場合がある。そのため、次のような基本的なウイルス対策・不正アクセス対策が重要である。

- 不審なメールの添付ファイルは開かない。
- セキュリティソフトを導入し、最新の状態を維持する。
- OS やアプリケーションの修正プログラムを適用し、最新の状態を維持する。
- パスワードを「できるだけ長く」「複雑で」「使い回さない」ものとする※167。
- 社外からアクセス可能なメールサーバがある場合、不審なログイン等のアクセスを監視する。

特に、Office 365 や G Suite のようなクラウド型サービスを利用している場合は、フィッシングメール等により従業員のアカウント情報（ユーザ ID・パスワード）が騙し取られることで、企業内の情報（メールやクラウド上に保存したファイル等）を窃取されたり、ビジネスメール詐欺だけでなく、標的型攻撃等の深刻なサイバー攻撃に悪用された

りすることも考えられる※168。そのため、2 要素認証等の対策により、第三者による不正ログインを防ぐことが重要である。

また、メールアカウントが乗っ取られている可能性がある場合、迅速にパスワードを変更するとともに、不正な転送設定がされていないかを確認する等の対応を行う必要がある。

1.3.7 偽警告・偽サイト等の詐欺

インターネット上のサービスを利用する人の不安や焦りに付け込み、金銭や情報を騙し取る詐欺の手口はますます巧妙化している。ここでは「偽警告」「偽セキュリティソフト」「ワンクリック請求」「フィッシング」「偽サイト」の手口と対策について紹介する。

(1) 偽警告の手口と対策

偽警告の手口では、パソコンで Web サイトを閲覧していると、突然「ウイルスが検出された」といった文言で偽の警告画面が表示される。そして画面に表示された電話番号に電話をかけるよう誘導し、電話をかけると修復作業や保守サポート契約締結等を持ちかけ金銭を要求する。ここでは 2017 年に新たに確認された手口と、その対策について述べる。

(a) 新たな偽警告の手口

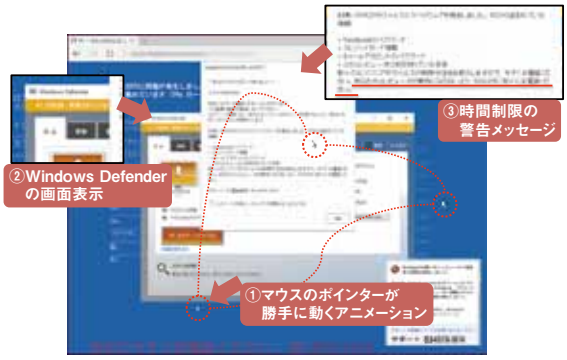
IPA では、2017 年 3 月に、マウスのポインターが勝手に動くアニメーションや Microsoft 社の URL にアクセスしているアドレスバーの画像を表示させる等の新たな偽警告の手口を確認した。確認した画面例を基に、この手口の五つの特徴について説明する。

①マウスのポインターが勝手に動くアニメーション

偽警告の画面が表示されると、Web ブラウザの画面上でマウスのポインターが移動するアニメーションが表示される。実際のマウスのポインターは非表示となり、マウスのポインターが勝手に動いている（パソコンが制御できない）と錯覚させる狙いがあると推察される（図 1-3-22）。

② Windows Defender の画面表示

Windows OS に標準搭載されている、マルウェア対策機能を持つ Windows Defender の偽の画面が Web ブラウザ上に表示される。Windows Defender が起動して、脅威が検出された（Microsoft 社の本物の警告）と錯覚させる狙いがあると推察される（図 1-3-22）。



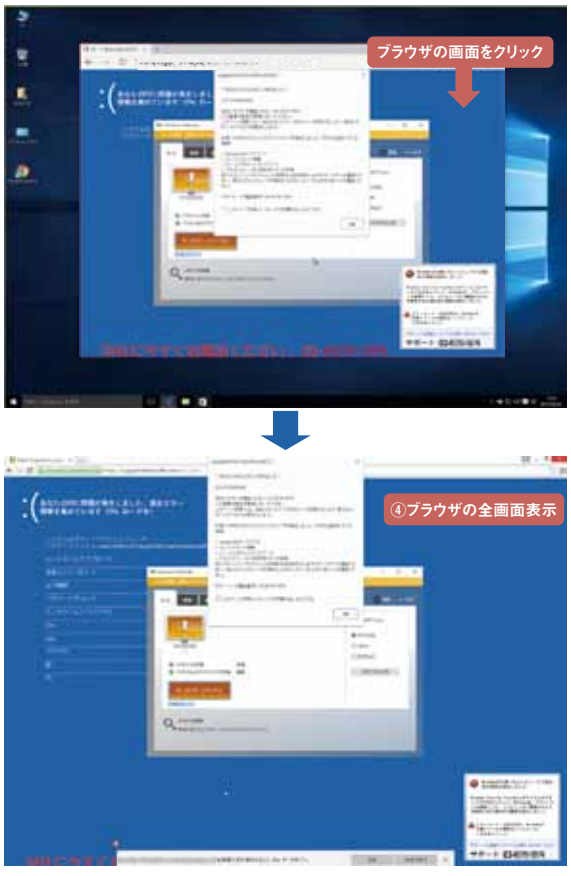
■図 1-3-22　狡猾な細工がされている偽警告画面の例

③時間制限を設けた警告メッセージ

「5 分以内に」電話をかけるようにという警告メッセージが表示される。事象を調べたり、誰かに相談したりする時間を与えずに電話に誘導する狙いがあると推察される（図 1-3-22）。

④ Web ブラウザの全画面表示

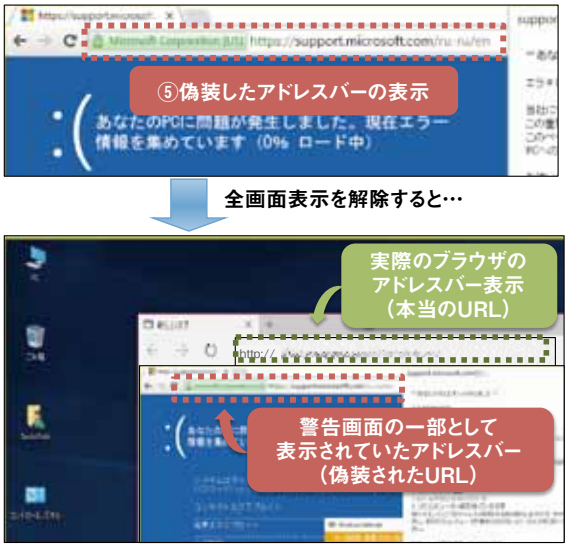
Web ブラウザの画面をクリックすると、全画面表示に切り替わる。全画面表示ではデスクトップのアイコンやタスクバーが全画面表示の後ろに隠れ、消失したように見える（図 1-3-23）。



■図 1-3-23　全画面表示になる Web ブラウザの画面例

⑤偽装したアドレスバーの表示

Web ブラウザが全画面表示に切り替わると、その画面上部に偽装されたアドレスバーが表示される。このアドレスバーには Microsoft 社の正規の URL（support.microsoft.com）が表示されているが、Web ブラウザ内のコンテンツ（画像が表示されているだけ）であり、実際にアクセスしている URL ではない。Windows Defender の画面と同様に警告が本物であると誤認させる狙いがあると推察される（図 1-3-24）。



■図 1-3-24　偽装された URL と本当の URL の画面例

(b) 対策

どの Web サイトに偽の警告を表示する仕掛け（当該サイトへ遷移するリダイレクト等）がされているかを、利用者が事前に見抜くことは困難であり、偽の警告画面を表示させないようにすることは難しい。ただし、偽警告の手口で表示される警告画面は、電話をかけさせるための根拠のない「騙し」に過ぎないため、警告の内容は鵜呑みにせず、画面を閉じるだけで問題ない。しかし、その手口は巧妙であるため、偽警告の具体的な手口を知り、冷静な対処と決して電話をかけないことが有効な対策となる。

偽警告の警告画面でポップアップメッセージが繰り返し表示される等、通常の操作で画面を閉じることができない場合は、Windows のタスクマネージャーから対象の Web ブラウザを選択して「タスクの終了」をクリックするか、もしくはパソコンの再起動を行う等で画面を消すことができる。

IPA では、実際に確認した画面のサンプルとともにその手口を紹介している※169。また、2017 年 4 月に手口と対策を紹介する動画※99 を公開しているので、参考にしていただきたい。

(2) 偽セキュリティソフトの手口と対策

偽セキュリティソフトは、Web サイト閲覧者に「ファイルが壊れている」「ウイルスが検出された」等の警告画面を Web ブラウザに表示し、それらを解決するためには「有償のセキュリティソフトが必要である」と、オンライン上での購入を迫る手口である。ここでは 2017 年に新たに確認された手口と、その対策について述べる。

(a) 新たな偽セキュリティソフトの手口

Web ブラウザに表示された警告画面の誘導に従い有償ソフトウェアの購入手続きを終えた後、当該ソフトの認証（アクティベート）が必要であるという理由で電話をかけるよう促される手口が確認された（図 1-3-25）。案内通りに電話をかけると遠隔操作ソフトをインストールするように誘導され、パソコンを遠隔操作される。更に、パソコンに問題があるため、その対処費用または今後のサポート契約料として等、追加の金銭支払いを要求される。

■図 1-3-25　アクティベートするための電話を案内する画面例

(b) 対策

Web サイト閲覧中に表示されるパソコンの不調やウイルス感染を示唆するような警告画面は、一般的な Web サイトで表示されるコンテンツと同じであり使用しているパソコンが異常な状態にあることを示すものではない。この手口についても、IPA の情報発信等※170 を通じて警告が単なる脅しであることを知り、安易に購入や電話をしないように注意していただきたい。もし誤って購入してしまった場合は、各自治体の消費生活センター※171 等、公的な機関に連絡していただきたい。また、偽セキュリティソフトの手口で誘導されたソフトをパソコンにインストールしてしまった場合は、システムの復元、またはパソコンの初

期化を行い、該当ソフトの影響を取り除くことを推奨する。

(3) ワンクリック請求の手口と対策

ワンクリック請求は、有料サービスへの登録が完了したと偽って、登録料等の名目で金銭を騙し取る手口である。Windows OS のパソコンを狙った手口では、アダルトサイトで動画再生に必要な手続き等と称して HTA（HTML Application）ファイルのダウンロード、実行を促す。HTA ファイルを実行するとパソコンに登録が完了したとして、請求画面が表示されるようになる。請求画面はパソコンの再起動や「閉じる」ボタンのクリックで一時的に消えるが、数分後に再び表示される等、請求画面が消せない状態になる。

(a) ワンクリック請求被害者を狙う詐欺

警視庁によると、「請求をやめさせることができます」「十分に返金が可能です」等とうたう探偵業者と契約してトラブルとなるケースが確認されている。探偵業者が被害金の返還請求等を行うことはなく、適当に作成した報告書を依頼者に送り付け、契約を履行したと主張し、契約料や解約料として金銭を詐取するという※172。ワンクリック請求の手口だけでなく、その被害者心理につけ込んだ詐欺行為にも注意が必要である。

(b) 対策

ワンクリック請求への対策として、アダルトサイトでは利用規約等の注意事項を確認せずに再生ボタン等をクリックしない、またプログラムのインストールを確認するメッセージが表示された場合は不用意にインストールしないことが肝要である。請求画面が出たとしても、慌てて支払いをしたり、相手へ連絡したりしないことが最良の対策となる。

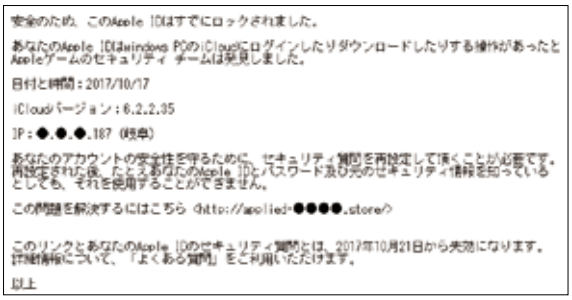
また、探偵業者は弁護士等の資格がないため、そのような業者へ相談や契約をしても、ワンクリック請求で支払ってしまった金銭を取り戻すことはできない。ワンクリック請求の契約に関する相談は、各自治体の消費生活センター等、公的な機関に連絡していただきたい※102。

(4) フィッシングの手口と対策

フィッシングとは、正規の企業等をかたった電子メール等を用いて正規の Web サイトにそっくりのサイトに誘導し、ID・パスワード、クレジットカード番号等を入力させ詐取する手口である。ここでは 2017 年に新たに確認された手口と、その対策について述べる。

(a) 金融機関以外をかたるフィッシングメールの増加

2017 年度は Apple Inc. をかたるフィッシングメールが増加した。Apple サービスのユーザ数が多いこと、また、クラウドやメール、アプリ購入等の複数のサービスと連携していること等から、攻撃者にとって効率が良く利用価値が高い、等が増加の要因であると推察される。IPA に寄せられた Apple をかたったフィッシングに関する相談では、「Apple ID のセキュリティ質問を再設定してください」「Apple ID のアカウントが無効になっています」「Apple ID がリセットされました」等、様々なメール文面で巧みにフィッシングサイトへ誘導する手口が確認されている（図 1-3-26）。中には iPhone を初めて買った直後で真偽を判断できず、フィッシングサイトへアクセスし、ID、パスワード、氏名、クレジット番号等を入力してしまったケースも見られた（図 1-3-27）。


安全のため、このApple IDはすでにロックされました。

あなたのApple IDはWindows PCのiCloudにログインしたりダウンロードしたりする操作があったとAppleゲームのセキュリティ チームは発見しました。

日付と時間：2017/10/17

iCloudバージョン：6.2.2.35

IP：●.●.●.187 (韓国)

あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂くことが必要です。再設定された後、たとえあなたのApple IDとパスワード及び元のセキュリティ情報を知っているとしても、それを使用することができません。

この問題を解決するにはこちら <http://applied-●●●●.store/>

このリンクとあなたのApple IDのセキュリティ質問とは、2017年10月21日から失効になります。詳細情報について、「よくある質問」をご利用いただけます。

以上

■図 1-3-26　Apple をかたるフィッシングメール例
（出典）フィッシング対策協議会「Apple をかたるフィッシング※173」

(b) 対策

フィッシング対策協議会の「利用者向けフィッシング詐欺対策ガイドライン※174」では下記のような行動を取るように説明している。

- 最新のフィッシング手口に関する情報に関心を持ち、予備知識を得ておく。
- 金融機関が行わないこと（ネット上で第 2 暗証をすべて入力させる等）を把握しておく。

フィッシング対策協議会の Web サイトでは、その時点で流行っているフィッシング事例について注意喚起を行っている※105。また、フィッシングメールでかたられた企業等が自組織の Web サイト上で注意喚起を行っている場合もあるので、これらの情報を確認していただきたい。

フィッシングサイトに情報を入力してしまった場合、情報を取り戻すことはできない。パスワードが盗まれたのであれば至急パスワードを変更する必要がある。なお 2 段階認証※175 を設定しておくことで、万が一パスワードが

■図 1-3-27　Apple をかたるフィッシングサイトの画面例
（出典）フィッシング対策協議会「Apple をかたるフィッシング」

詐取された場合でも第三者による不正ログインを防ぐことができる。クレジットカード番号であれば、カード会社に番号変更等の手続きのための連絡を行う必要がある。

(5) 偽サイトの手口と対策

詐欺行為を目的としたサイトがインターネット上には多数存在する。ここでは、2017 年 12 月に JC3 より注意喚起[※176] が行われた偽 EC サイト、及び 2017 年 8 月に警察庁より注意喚起[※107] が行われた偽警察庁サイトを挙げ、偽サイトの手口と、その対策について述べる。

(a) 偽サイトの手口

偽 EC サイトでは、利用者が商品を購入しても届けない、会員登録時の個人情報やクレジットカード番号等を窃取する、等の詐欺が行われる。商品が届かない等から不審に思い、偽 EC サイトにあるメールアドレスに問い合わせをしても、回答はないことがほとんどである。また、偽 EC サイトは検索サイトにて商品名等で検索をした場合、上位に表示されるような細工がされていることがあるため、誤ってアクセスしてしまう可能性が高く注意が必要である。

また 2017 年 7 月には新たな手口として、警察庁の偽サイトが確認された（図 1-3-28）。

■図 1-3-28　警察庁偽サイトの画面例
（出典）警察庁「警察庁サイトを装う偽サイトについて[※107]」

警察庁を装ったサイトを表示し、「幼児猥褻や動物虐待」等の違法サイトを閲覧したとして、違反金 2 ～ 5 万円を iTunes カードで支払うよう要求する手口である。セキュリティベンダの報告[※108] によると、Web ブラウザの全画面表示の機能を利用し、Web ブラウザのタブや URL 表示、右上の「閉じる」ボタン、「縮小」ボタン、Windows のタスクバー等すべてを偽装するという非常に巧妙な手口が使われたという。Web ブラウザ上のアドレスバーには警察庁サイトの URL（www.npa.go.jp）が表示されているように見えるため、利用者は警察庁の正規サイトであると誤解する可能性がある。

(b) 対策

JC3 は偽 EC サイトへの対策として、オンラインショッピングをする際の注意点について、Web サイトで説明しているので参考にしていただきたい[※176]。以下にその要約を示す。

- ドメイン及び URL アドレス
  - 自分が意図していない Web サイトに転送されてい

ないか。
  - URL の TLD（トップレベルドメイン）※177 が、「.top」「.xyz」「.bid」等、見慣れない文字列になっていないか。
- サイト運営者・連絡先
  サイトに事業者の名称、住所、電話番号、代表者または責任者氏名が記載されているか。
- サイトの日本語
  不自然な日本語の記載はないか。
- 暗号化通信
  ログイン、会員登録、支払情報入力時等に、Web ブラウザ上部のアドレスバーに鍵のマーク（https:// ～）があるか。
- 決済方法
  支払方法の説明と実際の決済画面とで、対応可能な支払い方法が異なっていないか。

上記に当てはまるサイトは、偽 EC サイトの可能性が高いと判断できる。ただし、事業者や代表者の情報が記載されている偽 EC サイトもあるため、少しでも不審を抱いた場合は利用を控えるか、国民生活センター等※178 へ相談いただくことを推奨する。

警察庁の偽サイトに関しては、Web サイトを通じて警察が金銭等を要求することはなく、同様な Web サイトが表示されても絶対に送金等をしないように警察庁から注意喚起※107 が行われている。警察等の法執行機関の権威を悪用しようとする手口※179 は度々出現するものであるため、今後も十分な注意が必要である。

(6) おわりに

インターネット上での様々な詐欺について、その手口と対策を説明した。今後も新たな手口で金銭や個人情報等が狙われると予想される。利用者においては、これらの手口があることを知っていただき、万一そのような場面に遭遇した場合に冷静に行動できるようにしていただきたい。特に Web サイト閲覧中に「警告」や「請求」等が表示されても、すぐに支払いをしたり、相手に電話をかけたりすることは避けるべきである。それらの真偽の判断が難しい場合は、IPA や国民生活センター等の公的窓口へ相談していただきたい。

また、セキュリティソフトには、偽サイトを含む問題のある一部のサイトへのアクセスをブロックする機能を有している場合がある。そのような機能を有効化し活用することも対策の一つとなる。

1.4 情報システムの脆弱性の動向

本節では、ソフトウェア製品の脆弱性の動向や、ソフトウェア製品及びWebアプリケーションの脆弱性対策について概説する。

1.4.1 脆弱性対策情報の登録状況

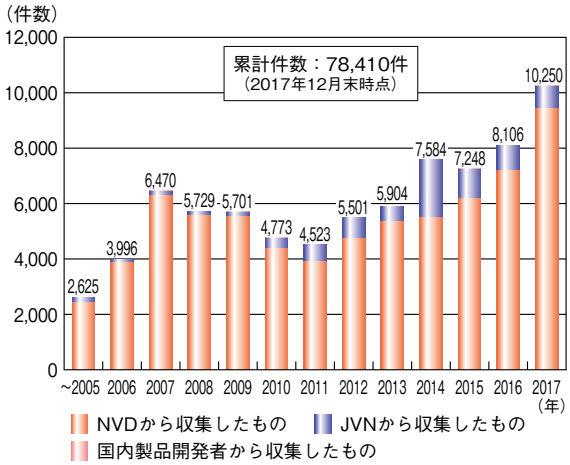
IPAは、脆弱性対策情報データベース「JVN iPedia※131」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2017年12月末までに登録されたJVN iPediaの脆弱性対策情報の傾向を分析する。

(1) JVN iPediaへの登録状況

JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007年4月25日から公開している。

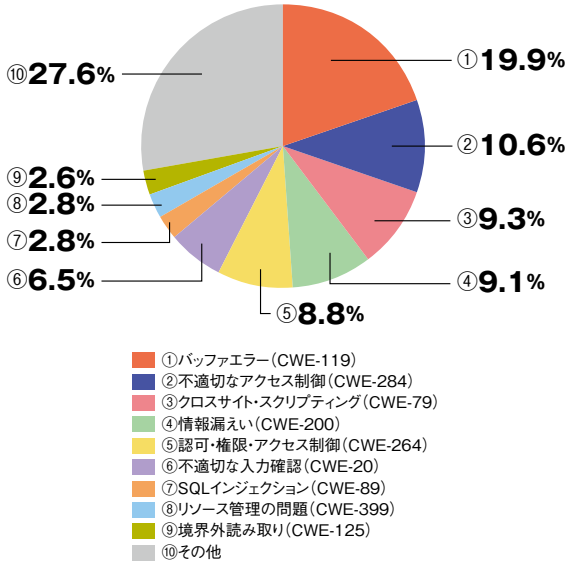
- 脆弱性対策情報ポータルサイトJVNで公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（National Institute of Standards and Technology：NIST）の脆弱性データベース「NVD※180」で公開された脆弱性対策情報

JVN iPediaの登録情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した日付で年ごとにまとめると、2011年を境にして増加傾向となっており、2014年はAndroidアプリの脆弱性対策情報が多く登録されたため7,584件と登録件数が増加した。更に2017年はNVDで公開された脆弱性対策情報の件数が増加したため、登録件数が1万250件に達している（図1-4-1）。増加の理由としては、発見される脆弱性の増加に加え、脆弱性を登録するための共通識別子であるCVE（Common Vulnerabilities and Exposures）※181の採番機関（CVE Numbering Authority：CNA）※182になるための認定基準が緩和され、CNAが増加したことが一因として挙げられる。The MITRE Corporationによると、2016年12月に47社※183だったCNAは、2017年11月には81社※184と約1.7倍となっている。このCNAの増加によって、多くの脆弱性情報にCVEが紐付けられ、NVDに登録公開される脆弱性の件数増加につながった可能性がある。



■図1-4-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

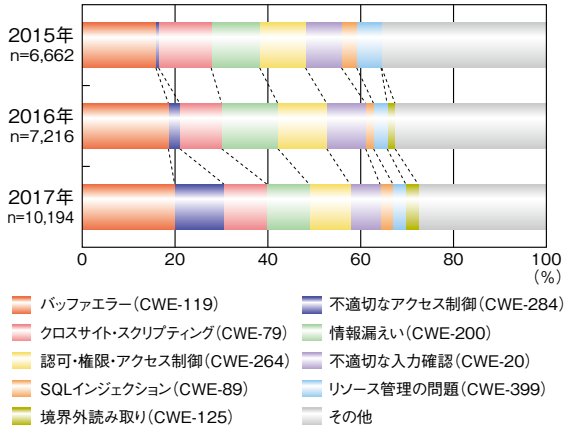
公表された脆弱性対策情報を共通脆弱性タイプ一覧（Common Weakness Enumeration：CWE）※185で分類すると、2017年は、「バッファエラー」が最多の19.9%、「不適切なアクセス制御」が10.6%、「クロスサイト・スクリプティング」が9.3%、「情報漏えい」が9.1%と続いている（図1-4-2）。



■図1-4-2 JVN iPediaにおけるソフトウェア製品の脆弱性対策情報の問題種別割合（2017年、n=10,194）
（出典）JVN iPediaの登録情報を基にIPAが作成

最も多かった「バッファエラー」に分類される脆弱性を悪用されると、製品開発者が意図していないメモリ領域への不正アクセスにより任意のコードが実行され、プログラムが異常終了したり、攻撃者にコンピュータを乗っ取られたりする可能性がある。

2015 年から 2017 年にかけての割合の変化を見ると、「不適切なアクセス制御」「境界外読み取り」の割合が増加している一方、「情報漏えい」や「不適切な入力確認」の割合は 2016 年に増加したものの、2017 年には減少に転じている（図 1-4-3）。それ以外の CWE 別の割合は前年と同様の傾向となっている。

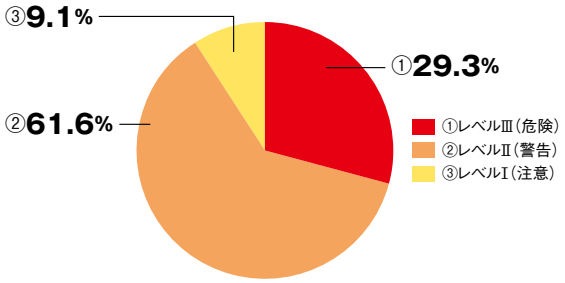


■図 1-4-3　JVN iPedia におけるソフトウェア製品の脆弱性対策情報の問題種別割合（2015 ～ 2017 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

JVN iPedia では、共通脆弱性評価システム（Common Vulnerability Scoring System：CVSS）※186 により、それぞれの脆弱性の深刻度を公開している。深刻度は、CVSS v2 の基本評価基準（Base Metrics：BM）の数値を基に評価したレベルⅠ、レベルⅡ、レベルⅢの 3 段階があり、数値が大きい程深刻度が高い。深刻度のレベルごとに想定される脅威は以下のようになる。

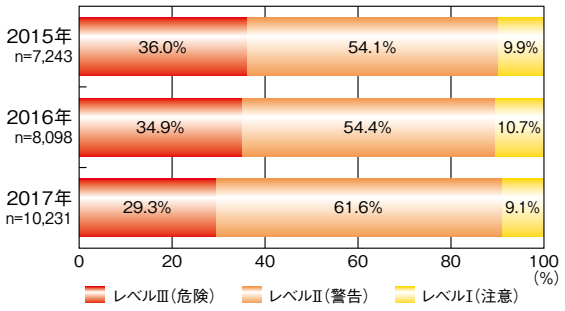
- 深刻度 レベルⅢ（危険）BM 7.0 ～ 10.0
  リモートからシステムを完全に制御されるような場合や大部分の情報が漏えいするような脅威等。
- 深刻度 レベルⅡ（警告）BM 4.0 ～ 6.9
  一部の情報が漏えいするような場合やサービス停止につながるような脅威等。
- 深刻度 レベルⅠ（注意）BM 0.0 ～ 3.9
  攻撃するために複雑な条件を必要とする脅威等。

公表された脆弱性対策情報を CVSS v2 の深刻度のレベルで分類すると、2017 年はレベルⅢが 29.3%、レベルⅡが 61.6%、レベルⅠが 9.1% となっている（図 1-4-4）。



■図 1-4-4　JVN iPedia における脆弱性対策情報のレベル割合（2017 年、n=10,231）
（出典）JVN iPedia の登録情報を基に IPA が作成

2015 年以降の CVSS v2 の深刻度のレベルの割合を年別に見ると、レベルⅡとレベルⅢで全体の 90%程を占めており、サービス停止につながるレベルⅡ以上の脆弱性が多数登録されている。最も危険なレベルⅢは、2016 年の 34.9% から 2017 年の 29.3% と減少しているものの、件数で見ると増加している（図 1-4-5）。これらの脆弱性による被害を未然に防ぐためには、製品開発者はソフトウェアの企画・設計段階から、セキュアコーディング※187 を含めたセキュリティ対策を講じる必要がある。



■図 1-4-5　JVN iPedia における脆弱性対策情報のレベル割合（2015 ～ 2017 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

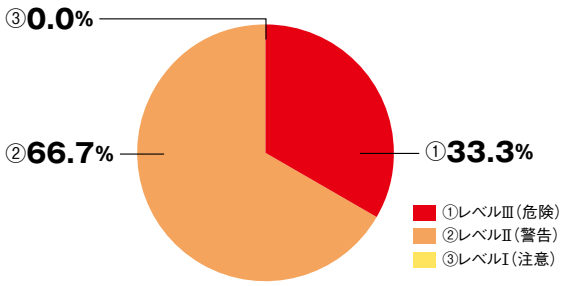
(2) Apache Struts2 の脆弱性対策情報について

2017 年 9 月、米国の大手信用情報会社が「約 1.4 億人に及ぶ顧客の氏名やクレジットカード情報等が流出した可能性がある」と公表した※188。同社の情報によると、2017 年 3 月に公開された Apache Struts2（CVE-2017-5638）の脆弱性が悪用されたことが分かっている※189。この脆弱性を修正する更新プログラムは、2017 年 3 月に Apache Software Foundation（ASF）からセキュリティ情報「S2-045」として公表されており※190、IPA でも同月に緊急対策情報を発信している※49（国内の被害事例は「1.2.4（1）外部からの攻撃による情報漏えい」参照）。

JVN iPedia では、2017 年 1 月から 12 月までに Apache Struts2 に関する脆弱性対策情報を 15 件登録した。

登録した15件のうち10件がサービス停止につながるレベルⅡ（警告）となっており、更にうち5件がCVSS v2で最も高いレベルⅢ（危険）に分類されている（図1-4-6）。いずれの脆弱性も悪用された場合、深刻な影響を受ける可能性がある。

Apache Struts2のように広く利用されるソフトウェアフレームワークの脆弱性が公開された場合、それを使って構築されたWebサイトは攻撃者に狙われやすく、情報漏えい等の被害を受ける可能性がある。そのため、システム管理者は、日頃からベンダの情報やセキュリティベンダの脆弱性情報を収集し、修正プログラムが公開された場合には速やかに適用する等、脆弱性対策を行うことが重要である。



■図1-4-6　JVN iPediaに登録されたApache Struts2の脆弱性対策情報のレベル割合（2017年、n=15）
（出典）JVN iPediaの登録情報を基にIPAが作成

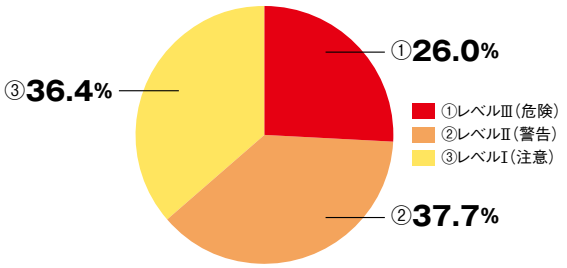
（3）2020年に予定されている主要な製品の公式サポート終了について

2020年初頭にMicrosoft Corporation（以下、Microsoft社）が提供しているWindows 7とWindows Server 2008の延長サポートが終了する[※191]。これらの製品は既にメインストリームサポートを終了しているため、仕様変更や新機能等は提供されないが、脆弱性やバグを解消する修正プログラムは提供され続けてきた。しかし、2020年に延長サポートの終了を迎えることで、脆弱性が発見されても修正プログラムが提供されなくなり、利用者は脆弱性対策を行うことができなくなる。

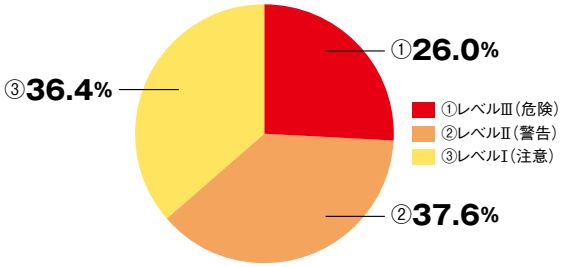
2017年の1月から12月までにJVN iPediaへ登録されたWindows 7とWindows Server 2008の脆弱性対策情報を深刻度のレベルで分類すると、Windows 7では231件中26％の60件（図1-4-7）、Windows Server 2008では242件中26%の63件（図1-4-8）がレベルⅢ（危険）となっている。2017年時点でも200件以上の脆弱性情報が発見されていることから、今後も深刻度がレベルⅢに分類される脆弱性対策情報が多数公開される可能性がある。

システム管理者は自組織で利用している製品のサポートが終了していないか、あるいは終了の予定がないかを確認する必要がある。また、終了が既に公表されている製品については、ベンダがサポートするバージョンや代替製品への移行を検討することを推奨する。

なお、2020年にはWindows 7とWindows Server 2008の他にも、Microsoft社が提供するOffice 2010[※192]やAdobe Systems Inc.が提供するAdobe Flash Player[※193]のサポートも終了を迎える。これらの製品についても移行の計画等を検討する必要がある。



■図1-4-7　JVN iPediaに登録されたWindows 7の脆弱性対策情報のレベル割合（2017年、n=231）
（出典）JVN iPediaの登録情報を基にIPAが作成



■図1-4-8　JVN iPediaに登録されたWindows Server 2008の脆弱性対策情報のレベル割合（2017年、n=242）
（出典）JVN iPediaの登録情報を基にIPAが作成

（4）今後の展望

JVN iPediaへ登録された脆弱性対策情報の件数は、2017年12月の時点で7万8,000件を超え、今後も更なる増加が見込まれる。しかし、開発者やシステム管理者が、これらの膨大な情報の中から必要な情報を収集して管理するのは困難である。これを受けて、IPAでは2018年2月に新バージョンのJVN iPediaを公開し、膨大なデータ量に対するアクセスのレスポンス強化や、JVN iPediaの検索機能においてCVSS v3値情報の取得が可能になる等の機能強化を行っている。JVN iPediaの利用が促進され、組織のセキュリティ対策に役立てられることを期待している。

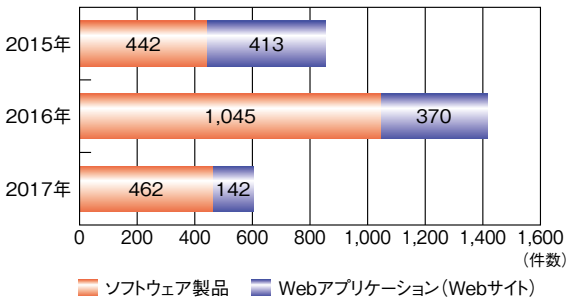
また昨今は、多くのメディアやニュースサイトで、Apache StrutsやWPA2等の影響範囲の広い脆弱性

情報が取り上げられている。しかし、脆弱性の対策情報や回避策に言及せず、脆弱性が発見されたという事実だけが報じられることも少なくない。そのため、利用者は JVN iPedia を利用して自組織内における脆弱性の影響や深刻度等を把握するとともに、開発ベンダから提供される修正プログラムや更新情報を日々収集することが望まれる。

1.4.2 脆弱性の状況

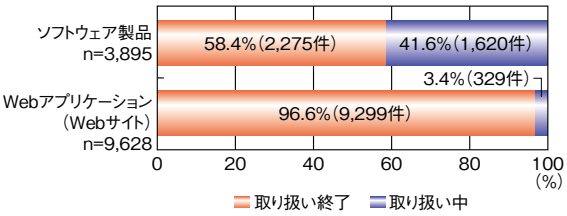
ソフトウェア製品や Web アプリケーション（Web サイト）の脆弱性を悪用した攻撃による情報漏えい、及び Web ページの改ざん等が継続して発生している。2017 年の特徴として、CMS※194 やアプリケーションプラットフォーム等のソフトウェア製品に重大な脆弱性が発覚し、脆弱性を悪用した被害が多く発生した。例えば CMS の脆弱性悪用では、世界で 150 万ページもの Web サイトの改ざんが発生したという※195。

2017 年に、脆弱性情報流通に関する公的な枠組みである「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）に基づき IPA に届け出された脆弱性関連情報※196 の件数は、ソフトウェア製品が 462 件、Web アプリケーション（Web サイト）が 142 件、合計 604 件であった。2016 年の届出件数（1,415 件）と比較すると、ソフトウェア製品（組み込み機器を含む）に対する届出、Web アプリケーション（Web サイト）に対する届出ともに約 4 割に減少した（図 1-4-9）。



■図 1-4-9　脆弱性関連情報の種類別の届出状況（2015 年～2017 年）
（出典）パートナーシップの届出状況を基に IPA が作成※197

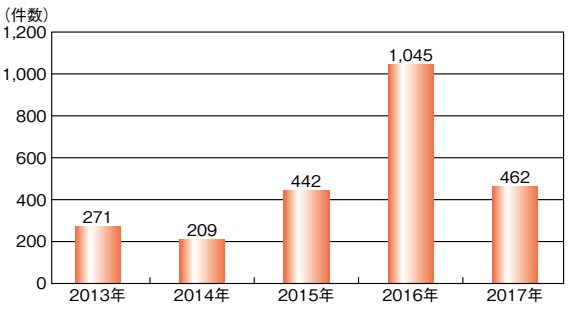
パートナーシップの開始時点（2004 年 7 月 8 日）からの届出件数を累計すると、ソフトウェア製品は 3,895 件、Web アプリケーション（Web サイト）は 9,628 件、合計 1 万 3,523 件に上る。これらの届出のうち IPA での取り扱いが終了※198 した届出は、ソフトウェア製品 2,275 件（58.4%）、Web アプリケーション（Web サイト）9,229 件（96.6%）という状況である（図 1-4-10）。ソフトウェア製品については、取り扱いを終了していない届出が多い。この状況を改善するため、「情報システム等の脆弱性情報の取扱いに関する研究会」において、製品開発者と連絡が取れない届出や Web サイト運営者が対応しない届出への対応方法に関して、パートナーシップの制度及び運用の見直しが行われている（パートナーシップの動向は「1.4.2 (4) 脆弱性情報の取り扱いに関する取り組み」参照）。



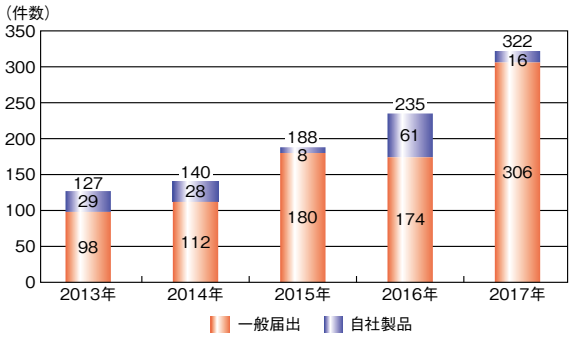
■図 1-4-10　脆弱性関連情報の種類別の届出状況（2017 年末までの累積）
（出典）パートナーシップの届出状況を基に IPA が作成

(1) ソフトウェア製品の脆弱性

2016 年は届出が急増した年であったが、2017 年の届出件数は 2015 年と同程度の 462 件（図 1-4-11）となり、届出件数はいったん落ち着きを見せた。一方、パートナーシップで取り扱った届出のうち、2017 年に JVN で公表された件数（図 1-4-12）は 322 件となり、パートナーシップが開始されてから最大となった。これは、2017 年の届出に加え、届出が急増した 2016 年やそれ以前の届出が、2017 年になって公表されるというケースが多く見られたためである。なお、製品開発者自身が、自社製品に関する脆弱性関連情報を届け出し、JVN 公表に至った件数は 16 件であり、2016 年の 61 件を大きく下回った。2017 年の JVN 公表件数において、自社製品に関する公表の割合は 5.0% となり、これは 2015 年とほぼ同じである。



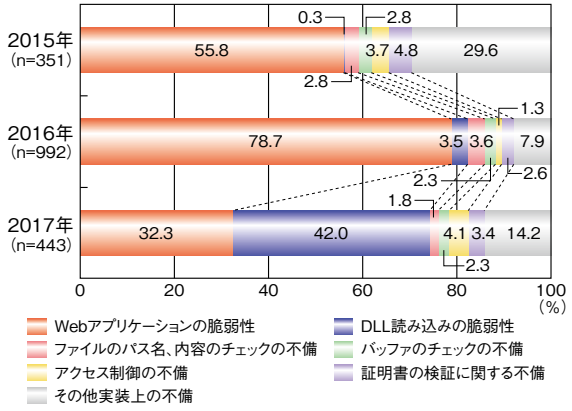
■図 1-4-11　パートナーシップに届け出されたソフトウェア製品の脆弱性の届出件数の推移
（出典）パートナーシップの届出状況を基に IPA が作成



■図 1-4-12　ソフトウェア製品の脆弱性について JVN 公表された届出件数の推移
(出典)パートナーシップの届出状況を基に IPA が作成

(a)パートナーシップに届け出されたソフトウェア製品の脆弱性の傾向

図 1-4-13 は、過去 3 年間のパートナーシップで取り扱った届出(「不受理」を除く)において、脆弱性の種類別に傾向を示したものである。2015 年、2016 年は「Web アプリケーションの脆弱性」が最も大きな割合を占めているのに対し、2017 年は「DLL 読み込みの脆弱性」が急増し、全体の 42.0% を占めている。



■図 1-4-13　脆弱性の種類別にみた届出の割合
(出典)パートナーシップの届出状況を基に IPA が作成

DLL 読み込みの脆弱性とは、実行時に DLL ファイルを読み込んで動作するアプリケーションにおいて、同一フォルダに細工された DLL ファイルが置かれていた場合に、アプリケーションがそのファイルを読み込んでしまうという問題である。結果として、DLL ファイルに記述された任意のコードが実行される可能性があるため、アプリケーションが不要な DLL ファイルを読み込まないように対策する必要がある。

2017 年に多く届け出されたこの脆弱性は、いずれも Windows アプリケーションのものであり、Windows OS の「アプリケーションと同一のフォルダから優先的に DLL ファイルを読み込む」という動作を悪用している。この脆弱性は、Windows 固有の問題ではないが、2010 年以前から Windows アプリケーションを中心に確認されてきた。パートナーシップの届出の傾向からも、Windows のアプリケーションに多数の DLL 読み込みの脆弱性が存在していると推測される。製品開発者は、開発したアプリケーションが実行時に不要な DLL ファイルを読み込む動作をしていないか今一度確認していただきたい。

この届出状況を受け、IPA は本脆弱性に関する注意喚起※199 を行った。具体的な攻撃シナリオや利用者側で実施可能な対策についても公開しているので、ぜひ参考にしていただきたい。

(b)緊急対策情報と脅威の動向

IPA では、多くの利用者が影響を受けるセキュリティ対策情報を「重要なセキュリティ情報」として公表しているが、その中でも特に影響度が高く、問題を悪用した攻撃が確認されているものを「緊急対策情報」として公表している。2017 年に緊急対策情報として公表した情報は、19 件であった(次ページ表 1-4-1)。

2017 年には、ランサムウェアによる被害と、ミドルウェアや CMS の脆弱性を悪用した攻撃による情報漏えい等の被害が大きな話題となった。以下にそれぞれの緊急対策情報、及び脆弱性情報について記載する。

ランサムウェアについては、2017 年も被害が世界中で発生した。ランサムウェアには、数多くの種類や亜種が確認されているが、中でも Wanna Cryptor、NotPetya(別名 Petya、Petya 亜種、GoldenEye)、Bad Rabbit 等が代表的である。これらは自己増殖機能を持つワーム型という特徴があり、感染拡大による被害が予想されたことから、IPA では、緊急対策情報や注意喚起を公表し、警戒を呼びかけた。それらには、感染による影響、感染経路、対策等の情報を掲載したが、その後も次々に詳細な挙動が明らかとなったため、段階的に緊急対策情報の更新を行った。特に Petya 亜種については、IPA にて検証を行い、感染後に OS の起動に必要な領域を書き換え、コンピュータを使用不可にする挙動や、同一ネットワーク内に感染拡大を試みる挙動を確認したため、検証結果を追記している。

従来のランサムウェアは、ファイルを暗号化して身代金を要求するという挙動が一般的であったが、昨今では、感染手法や感染後の挙動に様々な改良が加えられており、今後も日々進化していくと考えられる。感染しないための対策として、不審なメールの添付ファイルを開かないことや、OS 等のソフトウェアを最新の状態に保つことはも

公表日（2017 年）	タイトル
2 月 6 日	WordPress の脆弱性対策について
3 月 8 日	Apache Struts2 の脆弱性対策について（CVE-2017-5638）
3 月 9 日	更新：「SKYSEA Client View」において任意のコードが実行可能な脆弱性について（JVN#84995847）
3 月 15 日	Microsoft 製品の脆弱性対策について（2017 年 3 月）
3 月 21 日	更新：Apache Struts2 の脆弱性対策について（CVE-2017-5638）（S2-045）（S2-046）
4 月 12 日	Microsoft 製品の脆弱性対策について（2017 年 4 月）
5 月 10 日	Microsoft 製品の脆弱性対策について（2017 年 5 月）
5 月 14 日	世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
5 月 15 日	更新：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
5 月 17 日	更新：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
6 月 14 日	Microsoft 製品の脆弱性対策について（2017 年 6 月）
6 月 15 日	WordPress 用プラグイン「WP Job Manager」におけるアクセス制限不備の問題について（JVN#56787058）
6 月 28 日	感染が拡大中のランサムウェアの対策について
6 月 29 日	更新：感染が拡大中のランサムウェアの対策について
6 月 30 日	更新：感染が拡大中のランサムウェアの対策について
9 月 13 日	Microsoft 製品の脆弱性対策について（2017 年 9 月）
10 月 11 日	Microsoft 製品の脆弱性対策について（2017 年 10 月）
10 月 17 日	Adobe Flash Player の脆弱性対策について（APSB17-32）（CVE-2017-11292）
11 月 29 日	Microsoft Office の脆弱性（CVE-2017-11882）について

■表 1-4-1　2017 年に公表したソフトウェア製品の緊急対策情報
（出典）IPA による重要なセキュリティ情報の公表データ※200 を基に作成

ちろん、IPA や各セキュリティベンダが公開する情報等を適切に収集し、警戒を怠らないことが求められる。また、万が一、ランサムウェアに感染してしまった場合は、IPA の「情報セキュリティ安心相談窓口※201」等を活用していただきたい（対策については「1.3.1 ランサムウェアによる攻撃」参照）。

ミドルウェアや CMS については、WordPress や、Apache Struts2 の脆弱性が公開され、IPA では、これらの脆弱性について、それぞれ 2 月 6 日と 3 月 8 日に緊急対策情報を公表した。特に Apache Struts2 への攻撃は、情報の公開から実際に攻撃が発生するまでの間隔が非常に短く、製品開発者の脆弱性情報の公開方法や利用者の修正対応の課題が浮き彫りとなった。Apache Struts2 の脆弱性は、リモートからサーバ上で任意のコードを実行されるというものであり、この脆弱性情報が公開された 3 月 6 日から、2 日足らずで攻撃が行われた事例が確認されている※202。また、この時点では、製品の公式サイトからアナウンスが行われていなかったとされており※203、利用者側では脆弱性情報を知り得なかった可能性もある。今後もこの事例のように、情報の公開から短い間隔で攻撃が行われることが予想されるため、製品開発者、製品利用者双方において速やかな対応が求められる。

このような状況を受けて、情報の公開方法を変更した事例も存在する。例えば前述した WordPress の脆弱性では、対策バージョンの提供と脆弱性情報の公開を、期間をずらして行っている。これは、脆弱性情報公開の前に対策を行う猶予期間を利用者に与えるためとされている。また、Joomla! という CMS では、重要なセキュリティ修正が含まれる対策バージョンの公開に先駆けて、事前にリリース予告を行っている。利用者は、自身が使用している製品の更新情報が、どのような公開形式を取っているか把握し、深刻な脆弱性が含まれる場合は、速やかにアップデートを行うことが求められる。

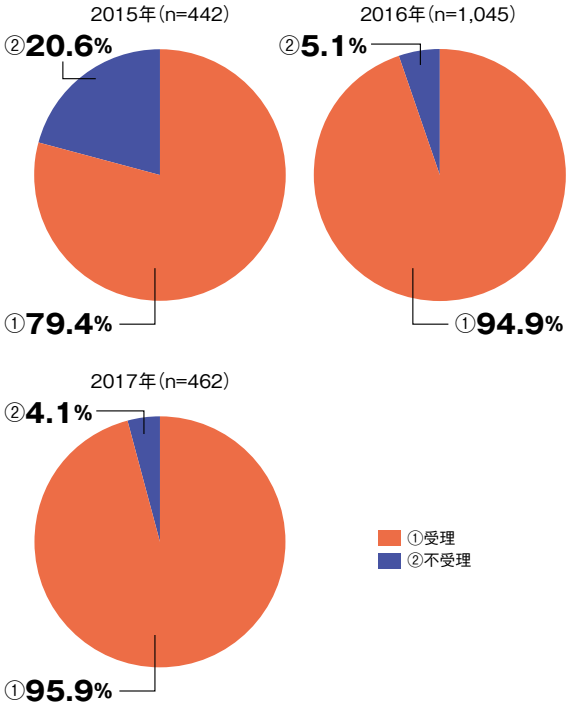
(c) 不受理となる届出の傾向

図 1-4-11（前々ページ）に示したとおり、発見者の協力により、2017 年も多くの届出があった。しかし、JVN で対策情報を公表する一方で、パートナーシップの脆弱性の定義等に合致せず、不受理となる届出も一定数存在する（図 1-4-14）。

IPA では、パートナーシップにおける脆弱性の定義について、理解を深めてもらうことを目的として、「脆弱性情報」に関する考え方を紹介するページを公開した※204。発見者は、ぜひこのページを参考にして、引き続きパートナーシップにご協力いただきたい。

(2) Web アプリケーション（Web サイト）の脆弱性

中国の脆弱性情報のポータルサイト「WooYun※205」において、SQL インジェクションの脆弱性が存在する日本の Web サイトの情報が約 400 件投稿されていることが確認されたことを受け、IPA は 2017 年 1 月、安全な Web サイトの運営及び維持管理のために、脆弱性の再



■図 1-4-14　不受理となったソフトウェア製品の脆弱性の届出の割合
(出典)パートナーシップの届出状況を基に IPA が作成

点検と改修を促すよう注意を呼びかけた※206。

SQL インジェクションの脆弱性は、古くから知られている脆弱性であり、IPA では 2008 年にも SQL インジェクション攻撃に対する注意喚起※207 を行ったが、2017 年においても、対策がなされていない Web サイトが相当数存在していると考えられる。

(a) SQL インジェクションの脆弱性

SQL インジェクションの脆弱性とは、データベースへの命令文である SQL 文の組み立て方法に問題があり、悪意あるリクエストによって、不正な SQL 文が生成・実行され、データベースを不正利用されるという問題である。この問題を悪用する攻撃を「SQL インジェクション」と呼ぶ。インジェクション(injection)は「注入」という意味である。

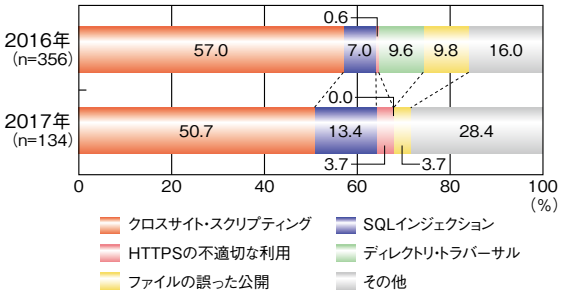
SQL インジェクションにより、データベースを直接操作され、データベース内に格納された営業秘密等の機密情報や個人情報が漏えいする、情報が消去・改ざんされる、等の被害が発生する可能性がある。個人情報やクレジットカード情報を格納したデータベースと連携している Web サイトの場合、SQL インジェクションによる情報漏えい等により事業継続の面で大きな影響を受ける恐れもあり、特に注意が必要となる。

SQL インジェクションの脆弱性は、不正な SQL 文の生成・実行による問題であることから、その解消には、正しい SQL 文を生成することが求められる。

対策としては、プレースホルダという変数を使って構成した SQL 文の雛形を事前に作成し、その変数に外部から渡される値を機械的に当てはめるバインド機構を利用する方法がある。その中でも、変数に当てはめる処理をデータベースエンジン側で行う静的プレースホルダを利用することが、セキュリティの観点から安全であることが知られているが、データベースエンジンによってはサポートしていない場合もある。他の手法としては、SQL 文にとって特殊な意味を持つ記号文字をエスケープ処理する方法があるが、データベースエンジンの種類や設定ごとにエスケープすべき特殊文字が異なる、といった問題点がある。アプリケーションのプログラミング言語によってはデータベースの種別に応じたエスケープ処理を行うメソッドもあるが、処理に不備があるものもある等、十分な対策を行うことは必ずしも容易ではない。Web サイト運営者は環境の特性を把握した上で対応する必要がある。

(b) パートナーシップから見る SQL インジェクションの脆弱性の現状

2017 年にも Web サイトにおける様々な種類の脆弱性がパートナーシップに届け出された。SQL インジェクションの脆弱性の届出は、2017 年に受け付けた届出のうち、不受理を除いたものの中で、13.4%を占めており、クロスサイト・スクリプティング(50.7%)に次いで 2 番目に多かった。2016 年の SQL インジェクションの脆弱性の届出は 7.0%であり、その割合は増加している(図 1-4-15)。



■図 1-4-15　Web サイトにおける脆弱性の種類別割合
(出典)パートナーシップの届出状況を基に IPA が作成

以下では、2017 年に取り扱った案件について紹介する。

- SQL インジェクションの脆弱性の探知
  SQL インジェクションの脆弱性による被害は、SQL 文の組み立てに悪影響を及ぼす値を外部から挿入され

ることで生じる。パートナーシップに報告されるSQLインジェクションの脆弱性の届出では、URLの誤入力やフォームの入力項目の誤記入等により、想定されないリクエストがWebアプリケーションに送信された後のWebサイトの挙動が、当該Webサイトにおける通常の挙動とは異なるものとなったことを脆弱性の発見の契機としているものが多い。

例えば、表示されるエラーメッセージがSQLインジェクションの脆弱性が存在するかどうかを判断する要素となる場合がある。具体的には、エラーメッセージの内容に、実行エラーを起こしたSQL文の情報等が含まれることがあり、これらの情報を基に脆弱性の有無を推測できる。

2017年に受け付けたSQLインジェクションの脆弱性の届出の7割が、リクエストを送信した後に表示されたエラーメッセージについて記載しており、脆弱性の発見に関する重大な契機となっていることがうかがわれる。

また、2017年に受け付けた届出の中には、検索エンジンでエラーメッセージを構成する文字列を検索することで、SQLインジェクションの脆弱性が疑われるWebサイトを発見した事例が複数見られた。

データベースエンジンや連携するWebアプリケーションのプログラミング言語・ライブラリの種類によっては、特有のエラーメッセージを表示するものがある。エラーメッセージが出力されたWebページが検索エンジンに登録されている場合、エラーメッセージ中の文字列をキーワードとして検索することで、SQLインジェクションの脆弱性が疑われるWebサイトが探知されてしまう可能性がある。

なお、SQLに関するエラーメッセージの中には、機微な情報が含まれることもある。情報が漏えいしているWebページにアクセスした場合には、Webサイト運営者がアクセス履歴の調査をする際にトラブルとなる可能性もある。

- エラーメッセージへの対処

  前述のとおり、エラーメッセージの情報がSQLインジェクションの脆弱性の発見とその悪用を容易にしてしまう可能性がある。また、SQLインジェクションの脆弱性が存在しなかったとしても、表示されるエラーメッセージは攻撃者にとって攻撃や他の脆弱性発見等への有用な情報となり得る。このため、SQLインジェクションの脆弱性への予防的対策としてエラーメッセージを表示しない、または、表示する内容を制限して必要最小限となるように設定することが有効である。また、エラーメッセージの中にデータベースに格納している情報の一部が表示され、外部に漏えいすることもあるため、エラーメッセージの表示を抑制することは情報漏えい対策にもなる。

  Webアプリケーションの種類やバージョンによっては、デフォルトの設定で、発生したエラーの詳細な情報をWebサイトに表示するようになっており、設定を変更しなければならない場合もある。そのため、Webサイトの公開前に設定を確認しておくことが望ましい。

  パートナーシップにおいて2017年に修正の完了が確認されたSQLインジェクションの脆弱性の案件のうち、発見者からの届出の中にエラーメッセージに関する記載のあったものについては、その70%以上がエラーメッセージの表示に関する対策を併せて行っている。しかし、エラーメッセージの対策はあくまで次善策であり、SQLインジェクションの脆弱性が存在する場合は、脆弱性それ自体を解消することが必要である。脆弱性を修正せず、エラーメッセージの表示の対処のみを行ったとしても、検索エンジンにキャッシュ等の形式で情報が残っている場合や、第三者のWebサイト等にエラーメッセージに関する情報が投稿された場合等は、それらの事業者が情報の削除に応じない限り、脆弱性の発見が容易な状況が継続してしまう恐れがある。

- SQLインジェクションの脆弱性の対策

  SQLインジェクションの脆弱性は、脆弱性の存在が発覚した後に設計レベルから修正することが難しく、パートナーシップにおいても取り扱いが長期化する傾向にある。他の脆弱性も同様であるが、安全なWebサイトの維持管理を行うにあたり、脆弱性の原因自体を解消する根本的な対策を、システム設計・構築の段階で実装することが重要である。一方で、根本的対策に漏れが生じることも否定できない。根本的対策に加え、エラーメッセージの抑制等の対策を併せて採用する等、複合的対策を検討することも必要である。

(3) ソフトウェアに組み込まれた製品の動向

ソフトウェア製品やWebアプリケーション（Webサイト）と同様に、ソフトウェアが組み込まれた機器（以下、組み込み機器）においても脆弱性が存在する場合がある。

(a) 組み込み機器の脆弱性の届出傾向

「1.4.2 (1) ソフトウェア製品の脆弱性」の図1-4-11 (54

ページ）に示した 2017 年のソフトウェア製品の届出総数 462 件のうち、組み込み機器の届出は 64 件で、13.9% を占めている。年ごとの届出件数の推移を見ると、2014 年以前は 20 件程度で推移していたが、2015 年 67 件、2016 年 160 件、2017 年 64 件と近年は届出が増加している。また、組み込み機器の届出のうち、「情報家電（Web カメラ等の消費者向け家電）」の割合が 2015 年より増加し、2017 年は約半数（48.4%）を占めた（表 1-4-2）。

年	組み込み機器の届出		
	件数	内）情報家電	
		件数	割合
2012 年	18	0	0%
2013 年	21	2	9.5%
2014 年	27	3	11.1%
2015 年	67	13	19.4%
2016 年	160	58	36.3%
2017 年	64	31	48.4%

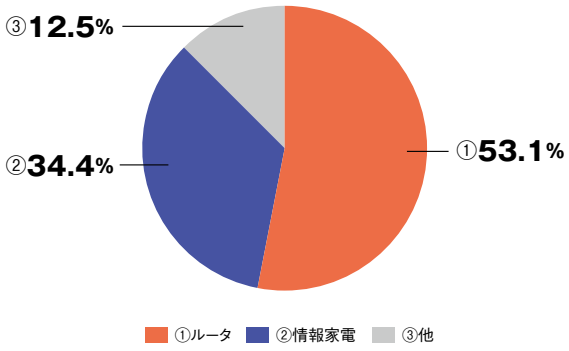
■表 1-4-2　組み込み機器の脆弱性の届出件数の推移
（出典）パートナーシップの届出状況を基に IPA が作成

2017 年に公表された組み込み機器の対策情報は 32 件あった。製品種類別では「ルータ」が 17 件で 53.1%、次いで「情報家電」が 11 件で 34.4% を占めた（図 1-4-16）。

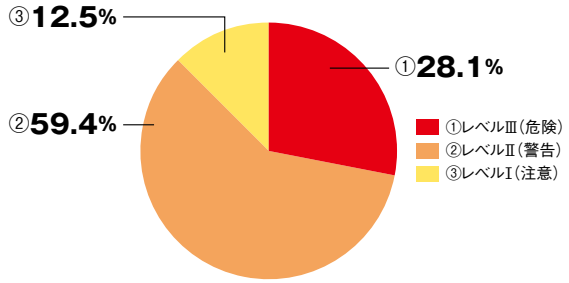
このうち、CVSS v2 基本値[※208] が危険（7.0 ～ 10.0）とされたものは 9 件あり、組み込み機器として公表された総数の約 3 割を占めている（図 1-4-17）。

(b) 危険な組み込み機器の脆弱性の事例

2017 年に公表された報告事例として、株式会社プリンストンが提供する Wi-Fi ストレージの「デジ蔵 ShAirDisk」における PTW-WMS1 の脆弱性（JVN#98295787[※209]）がある。本件は遠隔の第三者に root 権限で当該製品



■図 1-4-16　組み込み機器の脆弱性対策情報の製品種類
（2017 年、n=32）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-4-17　組み込み機器の脆弱性対策情報のレベル割合
（2017 年、n=32）
（出典）JVN iPedia の登録情報を基に IPA が作成

にログインされ、任意の操作を実行される可能性があることから CVSS v2 基本値が 10.0（危険）と評価された。また、消費者にとって身近な製品である、シャープ株式会社の掃除ロボット家電「COCOROBO」にセッション管理不備の脆弱性（JVN#76382932[※210]）、株式会社アイ・オー・データ機器が提供する複数のネットワークカメラ製品に OS コマンドインジェクションの脆弱性（JVN#46830433[※211]）が発見された。これらは最新のファームウェアにアップデートすることで問題を回避できる。

(c) 組み込み機器における脆弱性対策の課題

今後、IoT の普及によって組み込み機器は情報通信以外にも医療や自動車等の様々な分野に浸透すると考えられ、それらの機器の脆弱性は従来のソフトウェア製品と比べてより直接的に人の生命・身体に影響を及ぼす可能性が高まる。また、掃除ロボット等の情報家電は、IT に詳しくない所有者の利用も予想される。このような情報家電、あるいは医療や自動車等の組み込み機器は、利用者に情報セキュリティを含めた高い IT リテラシーを求めることが難しい製品といえる。製品開発者には、脆弱性のないソフトウェアを提供することがまず求められるが、潜在的な脆弱性まで考えると現実的には難しい。そのため、脆弱性が発見された場合の対応手段を準備しておくことも重要である。例えばファームウェアの自動アップデート機能を設けることで、利用者に操作を要求せずに発見された脆弱性への対策を適用することが可能となる。このような方策が組み込み機器の企画・設計段階で検討されることが望まれる。

(4) 脆弱性情報の取り扱いに関する取り組み

脆弱性情報の公表は製品開発者だけでなく、様々な組織・企業が行うようになった。また、公表のみではなく、脆弱性情報の発見や流通についてもより積極的な活動が行われている。以下に、脆弱性情報の流通に関する

動向、及び公的機関が行う脆弱性情報の流通の枠組みである「情報セキュリティ早期警戒パートナーシップ」の動向について記載する。

(a) 脆弱性情報の流通に関する動向

脆弱性情報の流通について、形態ごとにその動向を記載する。

- 脆弱性情報の流通のためのサービス

  脆弱性情報の公表に関する取り組みは年々活発化している。これまでは社内システムの監視やインシデント対応を行うCSIRTの必要性が認識され、企業において活発に設立が行われてきた。加えて2017年はIoTの普及に伴い、PSIRT（Product Security Incident Response Team）設立の必要性も高まっている※212。このような、CSIRT、PSIRTといった脆弱性情報流通のためのスキームが増加していることから、情報流通についての取り組みが活発になっていると考えられる。HackerOne※213によると、HackerOneが実施したバグバウンティプログラム※214のうち、テクノロジー分野からの参加が占める割合は減少傾向にあるが、その中でIoT機器に関するプログラムは増加している※215。一方、テクノロジー以外の分野の参加は、2014～2015年に28%であったものが2016～2017年では41%と増加している。バグバウンティプログラム「BugCrowd」においては2016年と比較して支払い金額が2倍以上、平均金額が1.5倍※216となっており、このようなサービスが普及し、また脆弱性情報の重要性が高まっている様子がうかがえる。

- 脆弱性報奨金制度

  IoTの普及によるPSIRTの必要性の高まりから、脆弱性情報の重要性の高まりを伺う事ができる。これとともに、前述のような第三者が提供するバグバウンティプログラム（プラットフォーム）の利用だけでなく、より積極的に独自の脆弱性報奨金制度を運用する組織も増えることが予想される※212。しかしながら、脆弱性報奨金制度については、独自の脆弱性判断のルールや報奨金の金額等、運用設計の難しさがあり、製品開発者と発見者間での以下のようなトラブルも発生している。組織で脆弱性報奨金制度を開始したが、具体的な脆弱性のルールを決めていなかった。その組織の製品開発者が、脆弱性を報告した発見者と事後に交渉を行った結果、交渉内容に納得できなかった発見者が報奨金の受け取りを拒否し、脆弱性情報及び製品開発者との交渉内容を一般に公開した※217。その後、製品開発者は報奨金制度のポリシー※218を公開し、併せて発見者に対する声明を公開している※219。

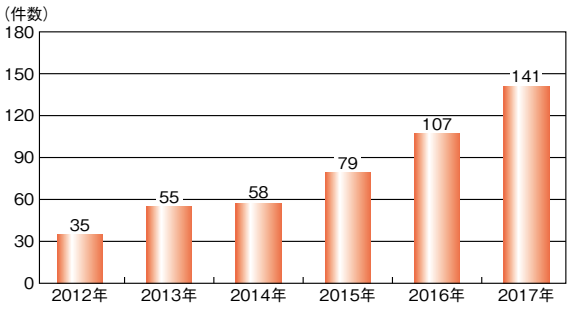
  このようなトラブルを回避するためにも、報奨金額や報奨金支払いの対象だけでなく、脆弱性情報の取り扱い方針等についてもあらかじめ設計・公表し、発見者と齟齬が発生しないようにしておく必要がある。独自の設計に不安がある場合、まずは第三者の提供するバグバウンティサービスを利用することで、一部の設計負担の低減を期待できる。例えば、HackerOneはプログラムに参加する組織のためにマニュアルを公開している※220。

- 脆弱性発見のイベント

  DEFCONと呼ばれるセキュリティイベントにおいて「余興」として実施されたことから普及したCTF（Capture the Flag）は、参加者同士でコンピュータへの侵入等の技術を競い合うというものである。

  世界的にCTFは活発化しており、CTF TIME※221によればイベントの実施数は年々増加している（図1-4-18）。

  日本では、SECCON（Security Contest）やCODE BLUE等のセキュリティ関連イベント・カンファレンスで実施されている。2014年からは参加者を女性に限定したCTF for Girlsコミュニティが発足し、CTFのみでなくCTFに関するワークショップ等も実施している。このようなオープンなCTFに加え、近年は社内限定のCTFを実施する企業も増え、脆弱性の知見を持ったセキュリティ人材の底上げに活用されている様子がうかがえる。

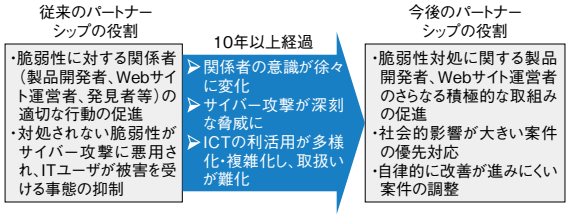


■図1-4-18　CTFの開催件数の推移
（出典）CTF TIMEを基にIPAが作成

(b) 情報セキュリティ早期警戒パートナーシップについて

日本には、脆弱性情報の届出を受け付ける公的な制度である情報セキュリティ早期警戒パートナーシップが存在する。このパートナーシップは経済産業省の告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程※222」

（以下、告示）に基づいた「情報セキュリティ早期警戒パートナーシップガイドライン」に則り運用されている。このガイドラインを取りまとめた「情報システム等の脆弱性情報の取扱いに関する研究会」は、パートナーシップ運用開始から 10 年が経過し、求められる役割も変化している（図 1-4-19）として、2016 年度の活動で制度について、以下の七つの変更を実施した。



■図 1-4-19　パートナーシップに求められる役割の変化
（出典）IPA「『情報セキュリティ早期警戒パートナーシップガイドライン - 2017 年版』の改訂に伴う運用変更について※223」

①届出取り扱い順序の変更

受付順序によらず、脆弱性による影響が大きい届出を優先的に扱う。これにより社会への影響が大きい脆弱性が迅速に対応され、社会的被害が低減することを期待する。

②発見者と製品開発者の直接調整を選択肢として提示

脆弱性情報の受付や対処について自律的な対応を期待できる製品開発者や Web サイト運営者については、発見者から当該製品開発者・Web サイト運営者に直接届け出る形も有効とする。これにより、パートナーシップが調整を必要とする脆弱性に注力できる体制になることを期待する。

③製品開発者との連携強化

脆弱性対応に積極的な製品開発者をパートナーシップの「優良製品開発者（仮）」に選定し、②の対応を可能とする。これが他の製品開発者に対脆弱性への適切かつ迅速な対処・公表に取り組む動機付けとなることを期待する。

④発見者との連携強化

パートナーシップへの届出実績を有する発見者を「実績ある発見者」に選定し、彼らとの意見交換等を通じて連携を強化する。これによって得られる発見者のニーズがパートナーシップに活かされること等を期待する。

⑤届出様式の変更

届出の記入項目を追加／変更する。これによる、関係者による脆弱性情報の把握の円滑化、及び関係者間の脆弱性に関する調整の円滑化を期待する。

⑥取り扱い終了条件の変更

パートナーシップへの届出件数が増大し、すべての届出に対して一律の対応を取ることが難しくなったため、これまでの取り扱い終了条件に加え、以下 3 点を新たに追加する。これにより、パートナーシップに求められる社会的な役割が効率的に果たされることを期待する。

ソフトウェア製品の追加条件

- 脆弱性による影響が小さい※224 場合、製品開発者への届出情報通知をもって取り扱い終了とすることを可能にする。
- 製品開発者の Web サイト等で脆弱性対策情報が公表された場合は JVN で公表せず取り扱い終了とすることを可能にする。

Web アプリケーションの追加条件

- Web サイト運営者の応答有無にかかわらず、脆弱性の影響が小さい場合、Web サイト運営者への届出情報通知をもって取り扱い終了とすることを可能にする。

⑦重要インフラ事業者への優先情報提供※225 の条件更新

優先的な情報提供を受ける基盤保有事業者（重要インフラ事業者）について、以下の条件を満たす必要がある旨を明確化する。これにより、脆弱性による国民の日常生活に必要不可欠なサービスへの被害が低減することを期待する。

- 情報を提供された当該事業者の中で秘密情報管理を徹底すること
- 事業者自身の委託先（システム構築事業者、セキュリティベンダ等）各社において、秘密情報管理を徹底すること
- JPCERT/CC から優先的に提供される情報は当該基盤を保護する目的に対してのみ利用することを徹底すること

以上を踏まえた運用の変更については、発見者へ説明会を実施している。このような関係者の協力により、より迅速に脆弱性情報が流通し、脆弱性による被害が低減することが期待される。

COLUMN

未成年者をサイバー犯罪の加害者や被害者にさせないために

2017年6月、ランサムウェアを作成した14歳の男子中学生が不正指令電磁的記録作成・保管の疑いで逮捕されました。供述によると、犯行の動機は身代金を目的としたものではなく、力試しや知名度向上等、興味本位や自己顕示によるものが大きいようです。また、12月にはコンピュータウイルスを作成し、提供したとして9歳の小学生が不正指令電磁的記録提供等の非行内容で児童相談所に通告され、このウイルスを利用する目的でダウンロードした9歳と11歳の小学生も児童相談所に通告されました。この小学生達の動機は「友達を驚かせたかった」「いたずらに使えるかもしれないと思った」だったといいます。他にも広告収入を目的にウイルスの作成方法をインターネット上に公開したり、仮想通貨の不正入手を目的としてウイルスを作成したりといった犯行で、いずれも17歳の高校生が逮捕されています。

国家公安委員会、総務省及び経済産業省が公表した「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況*」によると、2017年の不正アクセス禁止法違反の検挙件数は648件（前年比146件増）、検挙人員は255人（前年比55人増）でした。特に気になるのは不正アクセス禁止法違反に係る被疑者の年齢で、「14～19歳」が92人（36.1%）と最も多く、更に不正アクセス行為の動機は「好奇心を満たすため」が193件（32.2%）と最も多くなっています。これらのことから、ちょっとしたイタズラ気分でサイバー犯罪に手を染めてしまう未成年が増えていると言えます。

警察庁が公表した「平成29年におけるSNS等に起因する被害児童の現状と対策について**」によると、SNSに起因する犯罪の被害児童数は増加傾向にあり、2017年は過去最多となっています。また、フィルタリングの利用の有無が判明した被害児童のうち8割強が契約当時からフィルタリングを利用しておらず、その理由について保護者は「特に理由はない」と回答しています。

未成年者がサイバー犯罪の加害者や被害者となっている原因としては、スマートフォンの普及に伴って所有率が増加していることもありますが、それに反してスマートフォンやSNSの適切な利用方法を学ぶ機会があまりないことも大きな要因と考えられます。

スマートフォンやSNSは非常に便利であり、上手に活用すると生活を豊かにしてくれるツールになりますが、使い方を間違えると危険なツールともなり得ます。例えるなら、火や包丁、車のようなもので、使い方を間違えれば自分を含めて周りの人たちを傷つけることになり、最悪、命を落とすことにもなりかねません。

未成年者がサイバー犯罪に巻き込まれないよう、スマートフォンやSNSを利用する際には利便性だけに目を向けるのではなく、どのようなことが問題となるのか、危険なことはないのかといったことについて学校や家庭で学ぶ機会が増えていくことが望まれます。

* http://www.meti.go.jp/press/2017/03/20180322004/20180322004-1.pdf〔参照 2018-06-14〕

** https://www.npa.go.jp/safetylife/syonen/H29_sns_shiryo.pdf〔参照 2018-06-14〕

1.5 情報セキュリティ対策の状況

企業や、政府、地方公共団体、教育機関、一般利用者の情報セキュリティの対策状況について、IPA による調査結果及び公表されている資料等を参考に述べる。

1.5.1 企業・政府及び地方公共団体等法人における対策状況

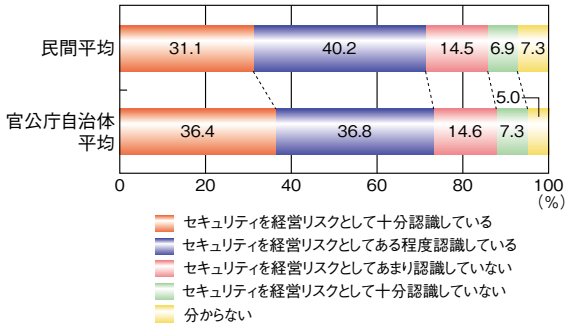
企業・政府及び地方公共団体等法人の情報セキュリティ対策状況について、以下の資料を基に述べる。

- トレンドマイクロ社：法人組織におけるセキュリティ実態調査 2017 年版※94（国内民間企業 1,100 社、官公庁自治体 261 団体を対象に調査。以下、トレンドマイクロ社調査）
- IPA：IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査※226（国内の IT システム・サービス提供企業 620 社、ユーザ企業 499 社を対象に調査）
- 総務省：地方自治情報管理概要～電子自治体の推進状況（平成 29 年度）～※227

(1) 法人における対策状況

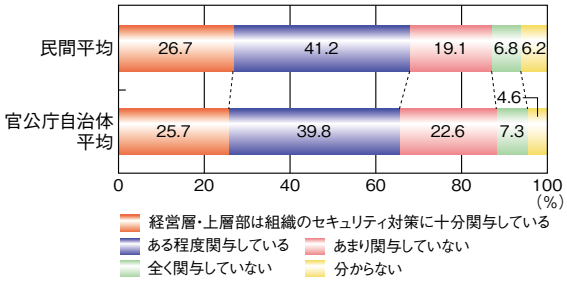
企業・政府及び地方公共団体等法人の技術的、組織的なセキュリティ対策の実施状況について、トレンドマイクロ社調査を基に述べる。

まず、情報セキュリティに関する法人経営層のリスク認識について概観する。調査結果では、「民間平均」（企業平均）と「官公庁自治体平均」（政府及び地方公共団体等の平均）とで大きな違いは見られなかった（図 1-5-1）。「セキュリティを経営リスクとして十分認識している」と「セキュリティを経営リスクとしてある程度認識している」を合計すると、「民間平均」は 71.3%、「官公庁自治体」は 73.2%とともに高い割合となった。



■図 1-5-1　経営層のリスク認識
（出典）トレンドマイクロ社調査を基に IPA が作成

経営層のセキュリティに対する関与についても同様の傾向が見られる（図 1-5-2）。「経営層・上層部は組織のセキュリティ対策に十分関与している」と「経営層・上層部は組織のセキュリティ対策にある程度関与している」を合計すると、「民間平均」が 67.9%、「官公庁自治体平均」が 65.5% と 2 ポイント程度の違いしかない。



■図 1-5-2　経営層のセキュリティに対する関与
（出典）トレンドマイクロ社調査を基に IPA が作成

次に、企業・政府及び地方公共団体等法人における技術的対策の実施状況について述べる。トレンドマイクロ社の調査では、クライアント端末、サーバの OS やアプリケーションに対して発行された修正プログラムの適用について、「クライアント端末で OS の修正プログラムを公開時に適用している」（63.1%）、「クライアント用アプリケーションの修正プログラムは公開時に適用している」（61.8%）、「組織内サーバで OS の修正プログラムを公開時に適用している」（61.1%）、「組織内向け業務アプリケーションの修正プログラムは公開時に適用している」（59.5%）、「公開サーバで OS の修正プログラムを公開時に適用している」（59.8%）、「公開サーバでサーバ用ソフトの修正プログラムを公開時に適用している」（57.7%）と、いずれも実施率は 6 割前後にとどまっている。

修正プログラムの適用は、OS やミドルウェア等の基盤ソフトウェアの脆弱性に対する攻撃の防御対策の基本である。また脆弱性情報が公開されてからその脆弱性を突く攻撃が観測されるまでの期間が短くなっているため、サーバ、クライアント端末を問わずシステムが受ける影響の確認を迅速に行う等、修正プログラム適用の早期化が望まれる。

また、WAF、IPS/IDS 等のよく知られている技術的対策については、「Web アプリケーションファイアウォールを使っている」（69.4%）、「IPS/IDS、UTM あるいは次

世代ファイアウォールを使っている」(68.1%)、「情報漏えい対策製品を使っている」(53.1%) と、5 ～ 7 割程度の採用となっていた。これらの対策は、適切なリスク分析のもとに実施することが望ましい。

続いて、企業・政府及び地方公共団体等法人における組織的対策実施状況を述べる。トレンドマイクロ社の調査によると、組織的対策実施状況は「重要な情報の定義がされ棚卸が徹底されている」(28.1%)、「重要な IT システム、ネットワーク、サービス構成の文書化、見直しが徹底されている」(29.7%)、「セキュリティポリシーの文書化見直しが徹底されている」(35.3%)、「セキュリティ・情報監査が定期的に行われている」(40.5%)、「インシデント対応プロセスの文書化、見直しが徹底されている」(43.4%)、「従業員向けインターネット利用ガイドラインの文書化・見直しが徹底されている」(38.6%) であり、標準的と思われる組織的対策の実施率は、前述の技術的対策のそれに比べ、総じて低い。

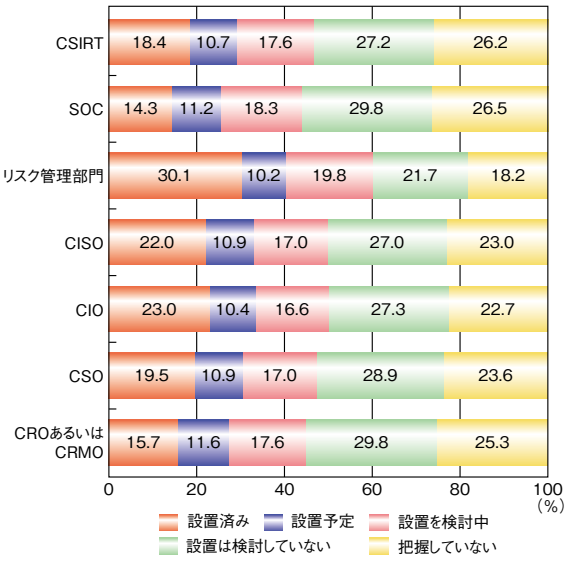
組織の状況は変化するため、組織的対策の有効性を保つには、定期的な対策の実施と見直しが欠かせない。情報資産の棚卸しや、ネットワーク・サーバの構成の変更を管理し、変更によって生じるセキュリティ上の問題点がないか確認することが求められる。技術面の対策も、この問題に対応して適切に実施すべきである。

次に、企業・政府及び地方公共団体等法人におけるセキュリティ担当組織とセキュリティ関連役職者の設置状況についての調査結果を図 1-5-3 に示す。「CSIRT」については、「設置済み」「設置予定」「設置を検討中」を合計すると 46.7% であった。調査対象には、従業員規模においても業種においても様々な企業が含まれていることを考えると、比較的高い率であると考えられる。また「リスク管理部門」については、「設置済み」「設置予定」「設置を検討中」を合計すると 6 割を超え、「CISO」についても約半数が「設置済み」「設置予定」「設置を検討中」のいずれかである。

今後は、設置の有無だけではなく、これらの担当組織、セキュリティ関連役職者の役割・機能やその適切さ、有効性等、その活動を充実させることが課題となると考えられる。

(2) IT システム・サービスの業務委託における対策状況

ここでは、企業のセキュリティ対策に関して、特に課題として認識されつつあるサプライチェーン上のセキュリティについて述べる。企業には、自組織内だけにとどまらず、サプライチェーン上のビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策が求められている。



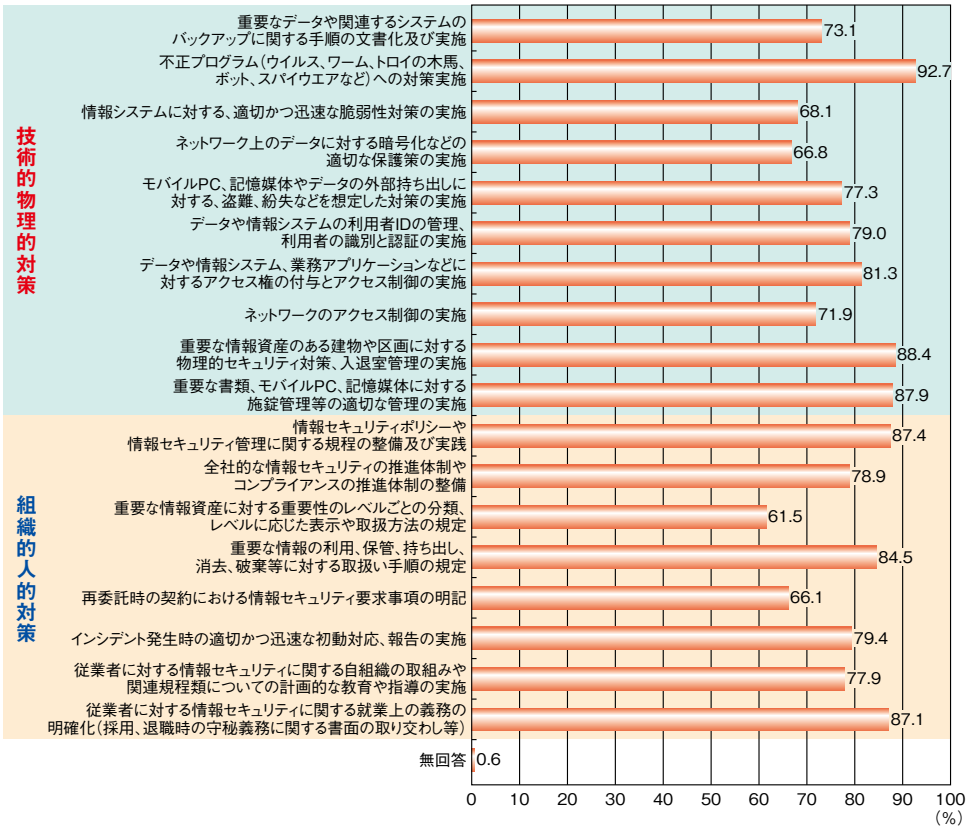
CSIRT(Cyber Security Incident ResponseTeam)
SOC(Security Operation Center)
CISO(Chief Information Security Officer、最高情報セキュリティ責任者)
CIO(Chief Information Officer、最高情報責任者)
CSO(Chief Security Officer、最高セキュリティ責任者)
CROあるいはCRMO(Chief Risk OfficerあるいはChief Risk Management Officer、最高リスク管理責任者)

■図 1-5-3　法人におけるセキュリティ関連組織・役割設置状況
(出典)トレンドマイクロ社調査を基に IPA が作成

以下では、IPA の「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」(以下、IPA 調査) を基に、IT システム・サービスの業務委託先企業 (受託企業) を主な対象として、情報セキュリティ対策実施状況、実施体制等について述べる。なお、業務委託の契約と実施状況チェックの詳細については「2.5.1 (2) サプライチェーンリスク管理の強化」を参照されたい。

図 1-5-4 に、受託業務において最低限実施している情報セキュリティ対策の調査結果を示す。

「情報システムに対する、適切かつ迅速な脆弱性対策の実施」(68.1%) と 7 割に満たない。脆弱性対策の実施は、稼働中のシステムやサービスへの影響を考慮しなければならないため、迅速な対応が困難な場合があることに起因していると考えられる。しかし、「1.5.1 (1) 法人における対策状況」で述べたように、脆弱性には早期の対応が必要である。委託先は、脆弱性情報の収集に努めるとともに、脆弱性を発見した、あるいは脆弱性の報告を受けた場合の対応方法について、委託元と事前に取り決めておくことが重要である。特に脆弱性対応のためにサービス停止や縮退運転をする場合は、委託



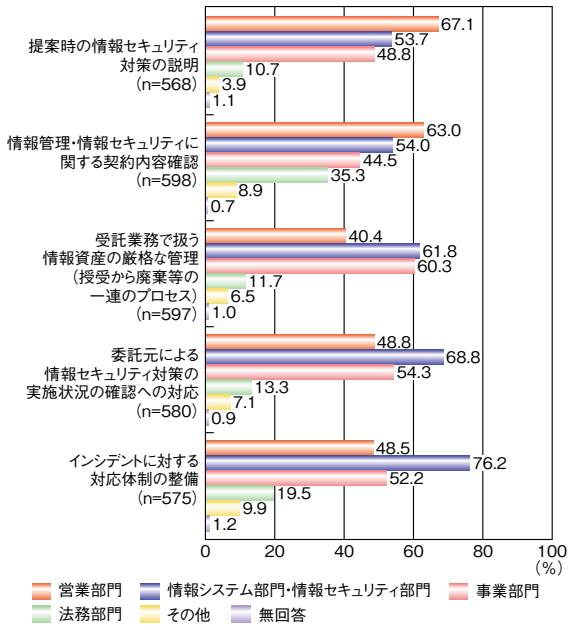
■図 1-5-4　受託業務において最低限実施している情報セキュリティ対策（n=620）
（出典）IPA 調査を基に作成

元は委託先の報告に対して速やかに業務への影響を判断し、両者が協力して対応することが望ましい。

全体をとおして最も実施率が低いのは「重要な情報資産に対する重要性のレベルごとの分類、レベルに応じた表示や取扱方法の規定」（61.5%）である。委託元が提供する情報の重要性レベルを指定しない場合、認識齟齬等により委託先で適切な取り扱いができずに情報漏えいが発生したり、逆に過剰な管理で委託先の負担が大きくなったりする可能性がある。委託先は情報資産のレベルに応じた管理方法をあらかじめ規定しておき、委託元と重要性のレベルや管理方法を調整することが望ましい。

次に、情報セキュリティの取り組みの所管部門についての調査結果を図 1-5-5 に示す。

営業部門は、「提案時の情報セキュリティ対策の説明」（67.1%）や「情報管理・情報セキュリティに関する契約内容確認」（63.0%）を実施する割合が高いため、委託先となる企業の営業部員は図 1-5-4 に示したような対策について自社はどのような状況なのかを把握することが望ましい。なお、委託先の IT 企業へのインタビューによると、業務委託においては、委託元あるいは委託先が所有する契約書フォーマットを基に作成することが多いとのこと



■図 1-5-5　受託業務における情報セキュリティの取り組みの所管部門
（出典）IPA 調査を基に作成

であった。このことから、委託先の法務部門は自社の契約書フォーマットに情報セキュリティに関する項目が漏れていないかを再点検するとともに、契約締結に当たって委託元の契約書フォーマットが利用される場合は、情報

セキュリティに関するリスクを考慮した内容であることを事前に確認していただきたい。情報システム部門・情報セキュリティ部門は、全項目が 50% 以上であるが、特に「インシデントに対する対応体制の整備」が 76.2% と高い。しかし、インシデントの被害最小化・早期解決では、情報システム部門・情報セキュリティ部門は、営業部門、事業部門、法務部門とも連携し、事態の収拾にあたる必要がある。委託先企業は、このことを十分に認識した上で、有事に備えた体制を整えておくことが望まれる。

(3) 地方公共団体における対策概況

総務省は、継続的に地方公共団体の情報セキュリティ対策の実施状況を調査し、「地方自治情報管理概要」の中で毎年公表している。ここでは、この調査結果に基づき、地方公共団体の情報セキュリティ対策の実施状況の変化について述べる。

表 1-5-1 は、対策項目に関して、都道府県及び市区町村の実施率を一覧にまとめたものである。2017 年度と 2016 年度の実施率の差も併せて記載している。

2016 年度に比べ、全体的な傾向に大きな違いは見られない。基本的な個別対策（「情報セキュリティの責任者や管理者等の任命の有無」「サーバ室等の入退室管理を行っている」等）は、都道府県・市区町村ともに高い実施率となっている。他方、調査・分析・計画等の

対策実施率（都道府県は 47、市区町村は 1,741）							
	対象項目	都道府県	市区町村		対象項目	都道府県	市区町村
	情報セキュリティの責任者や管理者等の任命の有無	100.0% (0.0 ポイント)	98.1% (+1.1 ポイント)		不正プログラムへの対策ソフトウェアの導入や定義ファイルのアップデート	100.0% (0.0 ポイント)	100.0% (0.0 ポイント)
(A)	緊急時対応計画を整備	93.6% (-4.3 ポイント)	49.7% (-7.9 ポイント)		重要なデータのバックアップを取得	100.0% (0.0 ポイント)	99.7% (+0.2 ポイント)
	情報資産の重要度に応じて、保管やアクセス、持ち出しについて規定	100% (-)	85.4% (-)		機器や外部記録媒体を廃棄する際、重要なデータを抹消	100.0% (0.0 ポイント)	99.0% (+0.8 ポイント)
	情報資産について、機密性、完全性及び可用性により分類	70.2% (-)	44.6% (-)		重要なデータへのアクセス制限（権限設定、認証）を実施	100.0% (0.0 ポイント)	98.6% (+1.4 ポイント)
(A)	主要な情報資産について調査及びリスク分析を行っている	63.8% (+6.4 ポイント)	36.2% (+1.9 ポイント)		許可されていないソフトウェアの導入を禁止	100.0% (0.0 ポイント)	96.4% (+2.0 ポイント)
	サーバ室等の入退室管理を行っている	100.0% (0.0 ポイント)	98.9% (+0.3 ポイント)		重要な情報システムのアクセスログを保存し、検査	97.9% (0.0 ポイント)	90.1% (+2.9 ポイント)
	サーバ等への停電や免震対策を実施している	100.0% (-)	98.4% (-)		重要なデータを暗号化し保存	80.9% (+12.8 ポイント)	42.9% (+4.2 ポイント)
	重要情報を含む紙媒体を適切に管理している	100.0% (0.0 ポイント)	96.6% (+1.6 ポイント)	(C)	委託事業者に対し、情報漏えい防止策を契約等により義務付けている	93.6% (-6.4 ポイント)	87.4% (-11.7 ポイント)
	CD-R、USB メモリ等によるデータの持ち出し、持ち込みを制限している	97.9% (-)	95.3% (-)	(C)	情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	89.4% (-)	53.8% (-)
	クラウドサービスやデータセンターを利用している	89.4% (-)	82.1% (-)	(B,C)	情報システムの運用等の委託事業者に対する指導・監査を実施している	59.6% (-10.6 ポイント)	36.5% (-12.5 ポイント)
	情報セキュリティ研修を職員に対して実施している	100.0% (0.0 ポイント)	86.8% (+6.1 ポイント)	(C)	機密性、完全性及び可用性等についてサービス規約（SLA）に定め、委託事業者に対し定期的に報告することを定めている	48.9% (-)	22.5% (-)
(B)	緊急時対応訓練を実施している	68.1% (+8.5 ポイント)	22.8% (+2.7 ポイント)				

（A）の項目は対策実施手順・ポリシーの策定や調査・分析・計画などの項目。（B）の項目は監査や評価に関わる項目。（C）の項目は IT サプライチェーンのセキュリティリスク管理に関わる項目（本文参照）。
1 行目の値は 2017 年度の値。2 行目の括弧付きの数値は 2016 年度の値との差。「ー」記号の項目は、2017 年度新規追加された項目か、2016 年度と内容の変更があった項目。

■表 1-5-1　地方公共団体における主な情報セキュリティ対策状況（2017 年度）
（出典）総務省「地方自治情報管理概要～電子自治体の推進状況（平成 29 年度）～」を基に IPA が作成

項目（表 1-5-1 の（A）の項目）や監査・評価に関する項目（表 1-5-1 の（B）の項目）は、都道府県・市区町村のいずれか、もしくは両方で実施率が低い。

また、IT サプライチェーンのセキュリティリスク管理に関する項目（表 1-5-1 の（C）の項目）は総じて実施率が低いことに加え、2016 年度から継続して調査した項目は実施率の低下が目立つ。昨今、IT システムの構築、運営や IT サービスを委託事業者から調達する際に、委託事業者における対策の不備等によって発注者側で発生するセキュリティ上の問題に注目が集まっている。地方公共団体における委託でも、IT サプライチェーンリスクを管理する対策の実施は、改善の余地が大きいと言える。

1.5.2 教育機関における対策状況

企業、政府機関や地方公共団体と同様に、教育機関においても、情報セキュリティインシデントが多数発生している。教育機関におけるインシデントと、教育機関の取り組みについて述べる。

（1）教育機関におけるインシデント

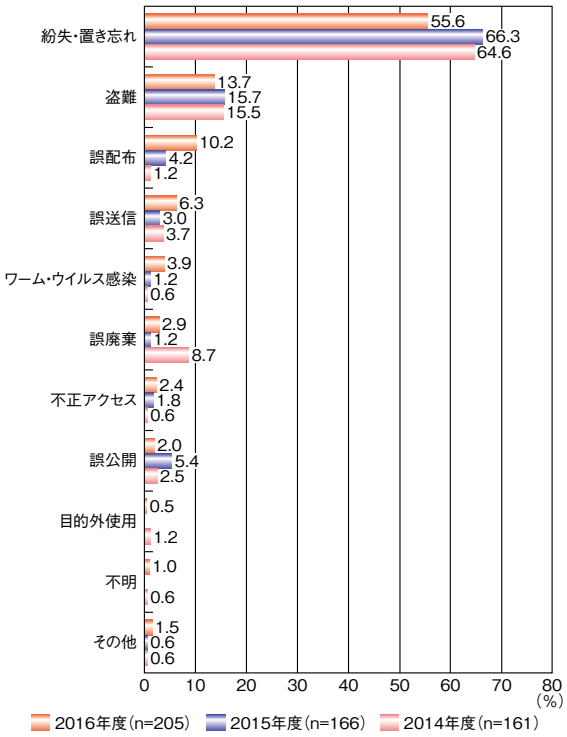
教育ネットワーク情報セキュリティ推進委員会（Information Security for Education Network：ISEN）の調査報告書※228によると、2016 年度に教育機関において発生したセキュリティインシデント数は、205 件に上った（2015 年度は 167 件、2014 年度は 168 件※229）。教育機関におけるセキュリティインシデントの原因別割合を図 1-5-6 に示す。最も割合が高いのは「紛失・置き忘れ」（2016 年度は 55.6%）であり、「盗難」（2016 年度は 13.7%）が続いている。この傾向は過去 3 年間同じである。

次に、2017 年度の主なセキュリティインシデントを表 1-5-2（次ページ）に示す。インシデントのインパクト等から、大学の事例を挙げている。

他にも、青山学院大学（学校法人青山学院）では、2017 年 12 月 2 日に外部に不審なメールを継続的に送信していたことから、緊急措置として全教員のパスワードを初期パスワードに変更（初期化）したという事案が発生している※238。

大学以外でもセキュリティインシデントは発生している。2017 年 4 月 25 日、鹿児島県の私立高校において、自校生徒 1,300 人の氏名、住所、奨学金等に関する情報が流出、Web サイトに掲載されたと報道された※239。

また 2018 年 4 月 4 日、前橋市教育委員会は、教育



■図 1-5-6 教育機関におけるセキュリティインシデントの種類別事故発生比率
（出典）ISEN の調査報告書※228 を基に IPA が作成

情報ネットワークが不正アクセスを受け、市立小・中・特別支援学校の全児童生徒の個人情報や、給食費徴収のための児童・教職員の口座情報が流出した可能性が高いと発表した※240。不正アクセスの対象となった人数は 4 万 7,839 人に上るという※241。

教育機関はいろいろな人がいろいろな用途で IT を使う。セキュリティに関して企業のようなガバナンスが利きにくいが、これらの事例を参考にして対策の見直しや周知、セキュリティ意識向上に努めていただきたい。

（2）教育機関の取り組み

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 2018 年 4 月 4 日、次期サイバーセキュリティ戦略骨子を示した※242。その中で「大学等における安全・安心な教育・研究環境の確保」を挙げ、大学においてもサイバーセキュリティ対策は経営上の重要課題と位置付け、組織的・計画的に取り組むことが必要、としている。大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（National Institute of Informatics：NII）は 2017 年 10 月、その足掛かりともなる高等教育機関の情報セキュリティ対策のためのサンプル規程集を改訂した※243。大学等の高等教育機関においても、組

公表日	大学名	概要
2017 年 5 月 11 日	共立女子大学・共立女子短期大学 （学校法人共立女子学園） 立教大学（学校法人立教学院）	大学の講師が学生の個人情報が格納されているノートパソコンを紛失した※230。
6 月 28 日	大阪工業大学（学校法人常翔学園）	大学の非常勤講師が学生の個人情報を格納した USB メモリを紛失した※231。
6 月 26 日	大阪大学	学生が利用するフリーメールに個人情報が記載されたファイルが送信されており、2017 年 6 月 7 日から 10 日までに当該アカウントへの不正アクセスが計 6 回記録されていた※232。
10 月 20 日	国立大学法人島根大学	附属図書館の Web サーバ上のアンケート管理システムで入力された個人情報が外部から閲覧可能な状態になっており、8 月下旬に不正アクセスの痕跡が発見された※233。
12 月 13 日	大阪大学	2017 年 5 月 18 日～ 7 月 4 日の間に、システムに不正ログインされ、システム管理者 ID が盗まれたことにより、個人情報が漏えいした※53（「1.2.4（1）外部からの攻撃による情報漏えい」参照）。
12 月 27 日	国立大学法人新潟大学	パソコン 1 台がランサムウェアに感染し、端末内のデータが暗号化された※234。
2018 年 1 月 9 日	国立大学法人新潟大学	Web サイトが不正アクセスにより改ざんされた※235。
3 月 8 日	学校法人中部大学	パソコン及びファイルサーバがランサムウェアに感染し、端末内のデータが暗号化された※236。
3 月 16 日	公立大学法人新潟県立看護大学	教職員 1 人のアカウントが不正利用され、同大学から約 37 万件の迷惑メールが送信された※237。

■表 1-5-2　大学における主なセキュリティインシデント

織全体のセキュリティポリシー策定・セキュリティマネジメントが求められており、積極的な対応が望まれる。

また文部科学省は、2016 年 9 月より「教育情報セキュリティ対策推進チーム」を設置し、地方公共団体が設置する学校（小学校、中学校、義務教育学校、高等学校、中等教育学校及び特別支援学校）における情報セキュリティの考え方について検討してきた。このチームでの検討を踏まえて、「教育情報セキュリティポリシーに関するガイドライン※244」が 2017 年 10 月に公表された。

本ガイドラインは、学校において情報セキュリティポリシーの策定や見直しを行う際の指針となるものとして、学校における当該ポリシーの考え方及び内容について解説している。特に、学校では教職員以外にも児童生徒が情報システムを利用する等、地方公共団体の他の行政事務と異なる点を考慮して策定されている。本ガイドラインの読者は学校のセキュリティ責任者、情報セキュリティポリシー策定の担当者を想定している。ポリシーの例文は市立の小学校や中学校等を対象とし、読者が参考にしやすい記述となっている。

情報セキュリティについては以下の六つを基本的な考え方として、具体的な対策基準を策定できるようにまとめられている。

- 情報セキュリティの組織体制を確立すること
- 児童生徒による機微情報へのアクセスリスクへの対応を行うこと
- インターネット経由による標的型攻撃等のリスクへの対応を行うこと
- 教育現場の実態を踏まえた情報セキュリティ対策を確立させること
- 教職員の情報セキュリティに関する意識の醸成を図ること
- 教職員の業務負担軽減及び ICT を活用した多様な学習の実現を図ること

地方公共団体の学校だけでなく、国立校・私立校等も、本ガイドラインを参考にしてセキュリティ対策や意識向上の取り組みを具体化し、実践することが望まれる。

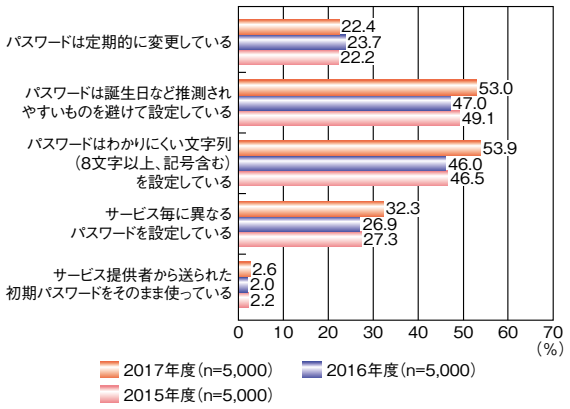
1.5.3 一般利用者における対策状況

IPA が実施した「2017 年度情報セキュリティの脅威に対する意識調査※245」を基に、一般利用者の情報セキュリティ対策の実施状況について述べる。

(1) ID・パスワードの管理状況

ID・パスワードは、様々なサービスを利用する際の本人認証に広く利用され、攻撃者に窃取されると、情報の覗き見・流出やなりすまし、金銭的な被害等を引き起こす。パスワードの設定状況の調査結果によると、「パスワードは誕生日など推測されやすいものを避けて設定している」割合は、53.0% と 2016 年度から 6 ポイント高くなっている。また、「パスワードはわかりにくい文字列（8

文字以上、記号含む）を設定している」割合も7.9ポイント高くなっている（図1-5-7）。パスワードの設定状況について世代を問わず改善が見られた。



■図1-5-7　パスワードの設定状況
（出典）IPA「2017年度情報セキュリティの脅威に対する意識調査」を基に作成

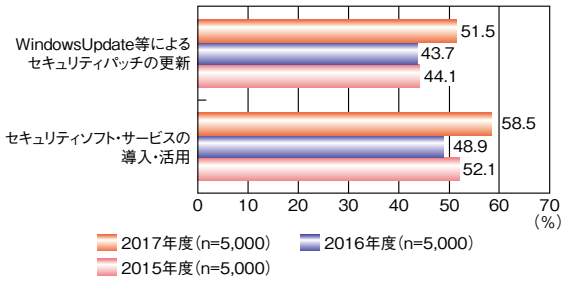
パスワードはできるだけ長く、推測されにくいものとし、他のサービスで使い回さないことが肝要である。また、利用サービスにおいて2段階認証が提供されている場合は、不正ログイン対策として積極的に設定することが推奨される※246。

(2) パソコン利用者における対策状況

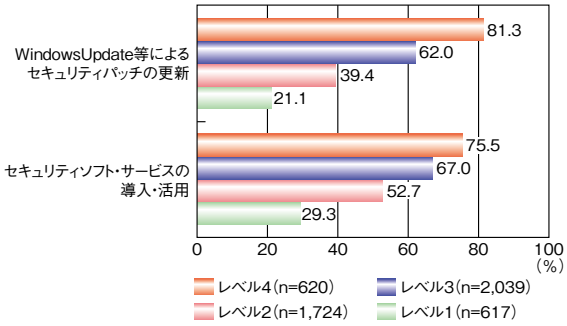
パソコンは多くの個人や企業に利用されていることから、インターネットバンキングの認証情報等の窃取を狙ったものや、ランサムウェアによりパソコンやファイルを利用できなくさせるもの等、個人、法人を狙った様々な攻撃が確認されている。このような攻撃による被害を防ぐためには、適切なセキュリティ対策を行う必要がある。

パソコンのセキュリティ対策状況の調査結果によると、「WindowsUpdate等によるセキュリティパッチの更新」（51.5%）や「セキュリティソフト・サービスの導入・活用」（58.5%）等の対策は半数以上が実施している（図1-5-8）。しかし、パソコン利用の習熟度レベル別※247で見ると、「WindowsUpdate等によるセキュリティパッチの更新」は最もレベルの高いレベル4で81.3%、最も低いレベル1で21.1%と習熟度によって対策の実施率に大きな差がある（図1-5-9）。また、「セキュリティソフト・サービスの導入・活用」もレベル4で75.5%、レベル1で29.3%と、その差は同じように大きい。

このように習熟度レベルの低いパソコン利用者は、様々な脅威や攻撃への対策が不十分な状況にあり、習熟度レベルの高いパソコン利用者に比べ被害に遭う可能性が高いと言える。そのため、家庭内または企業内において習熟度レベルの低いパソコン利用者がいる場合は、習熟度レベルの高いパソコン利用者が積極的にサポートする等、全体でセキュリティレベル及び意識を高めることが重要である。



■図1-5-8　パソコンのセキュリティ対策状況
（出典）IPA「2017年度情報セキュリティの脅威に対する意識調査」を基に作成



■図1-5-9　習熟度レベル別のパソコンのセキュリティ対策状況
（出典）IPA「2017年度情報セキュリティの脅威に対する意識調査」を基に作成

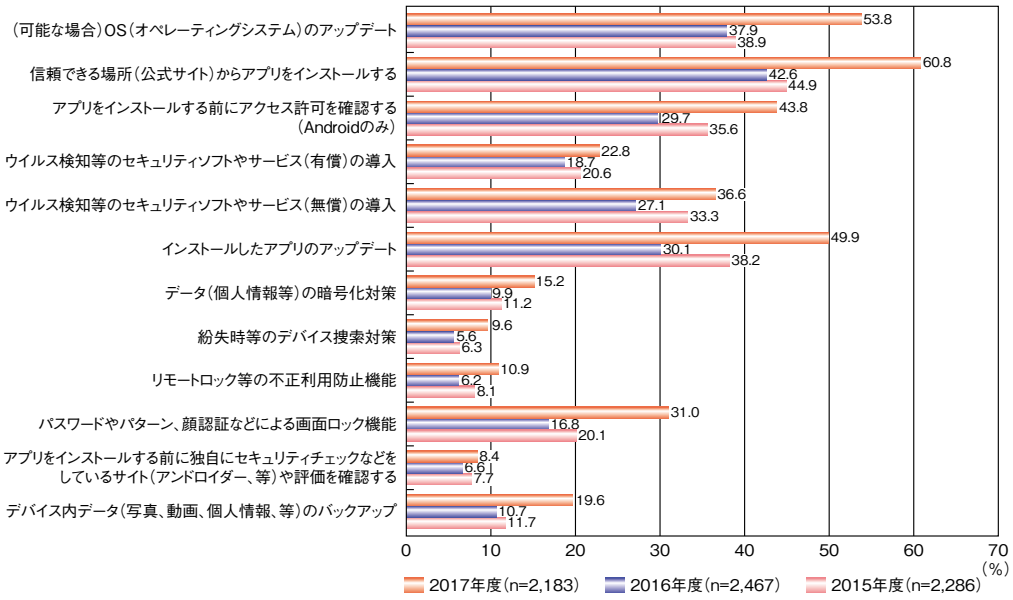
(3) スマートデバイス利用者における対策状況

スマートデバイス（スマートフォン、タブレット端末）の利用率増加とともに、スマートデバイスからのインターネット利用時間も増加している※248。利用率が増加することで、スマートデバイスを狙う脅威が増え、また利用時間が増加することで脅威に遭遇する可能性も高くなると考えられるため、被害を防ぐには適切なセキュリティ対策が重要となる。

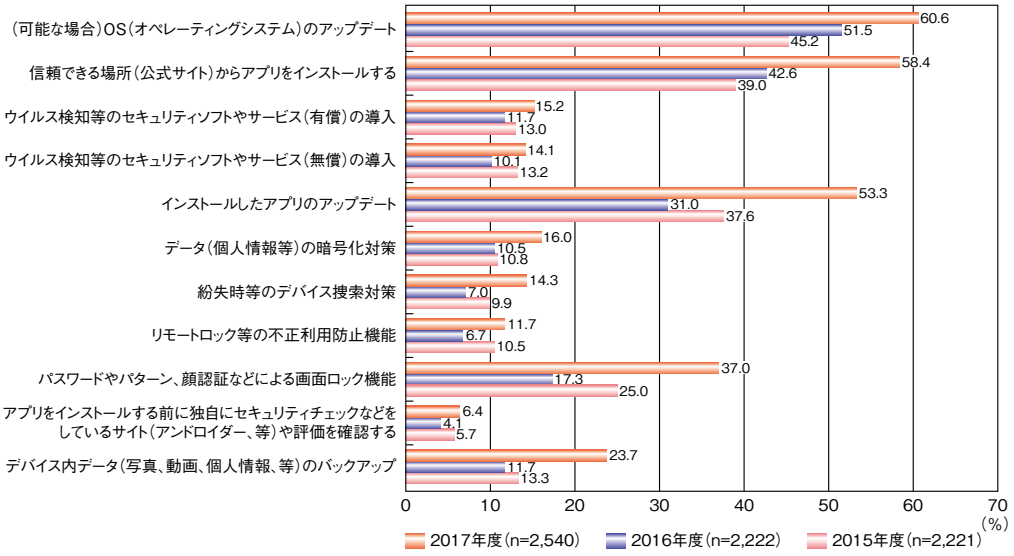
ここでは、調査結果（次ページ図1-5-10、次ページ図1-5-11）を基にスマートデバイス利用者のセキュリティ対策について述べる。

(a) セキュリティソフトの導入状況

セキュリティソフトやサービスの導入率は、Android利用者では有償が22.8%、無償が36.6%であり、2016年度より向上している。iOSでは有償が15.2%、無償が14.1%であり、こちらも2016年度より向上している。



■図 1-5-10　Android 利用者のセキュリティ対策状況
(出典)IPA「2017 年度情報セキュリティの脅威に対する意識調査」を基に作成



■図 1-5-11　iOS 利用者のセキュリティ対策状況
(出典)IPA「2017 年度情報セキュリティの脅威に対する意識調査」を基に作成

セキュリティソフトやサービスを導入すると、不正アプリや危険な Web サイトへのアクセス等が検知・ブロックされ、様々な脅威や攻撃からスマートデバイスを保護できる可能性が高まる。

(b) OS やアプリのアップデート状況

Android、iOS ともに OS やインストールしたアプリのアップデート実施率は 2016 年度より向上している。

2017 年は Android で 829 件[※249]、iOS で 366 件[※250]と 2016 年より多くの脆弱性が JVN iPedia に登録されている。これらの脆弱性の中には、2017 年 9 月に公開された「BlueBorne[※251]」と呼ばれる Bluetooth の実装における複数の脆弱性のように、適切に対処しなければスマートデバイスを乗っ取られる可能性のある危険な脆弱性が含まれている。

このような脆弱性を放置したままにスマートデバイスを利用し続けることは危険であるため、OS のアップデート（修正プログラムの適用）によって脆弱性を解消することが重要である。ただし、Android の場合はアップデートの提供可否や提供時期がメーカや端末によって異なるので、注意が必要である。

なお、OS だけでなくアプリも同様に、脆弱性が発見さ

れ、それを修正したバージョンが公開された際には、公式マーケット等からアップデートすることが推奨される。定期的にOSやアプリのアップデート情報を確認し、OSやアプリを最新の状態に保つことが重要である。

(c)不正利用防止機能の導入状況

スマートデバイスを物理的な不正利用から防止する機能については、パスワードやパターン、顔認証等による画面ロック機能の利用がAndroid、iOSともに3割を超え、2016年度の2割弱より大きく向上した。

画面ロック機能により、スマートデバイス紛失時の第三者による保存情報（プライベートな写真や友人の連絡先等）の覗き見や不正利用を防ぐことができる。また、気づかないうちに勝手に操作され、不正アプリや遠隔監視アプリ等をインストールされること（結果として、機微情報を窃取されたり、プライバシーを侵害されたりする被害につながる）への対策ともなる。万が一に備えて不正利用防止のために、適切な対策を実施しておくことが重要である。

(d)インストール時のアクセス許可の確認状況

Android利用者を対象にした調査では、アプリをインストールする前にアクセス許可（パーミッション）を確認すると回答したのは43.8%であった。2016年度の調査から14.1ポイント向上し、約4割の利用者がアクセス許可を確認している。信頼できる場所（公式マーケット等）からアプリをインストールする利用者はAndroid、iOSともに2016年度より向上し、約6割が信頼できる場所からアプリをインストールしている。

公式マーケットではアプリの審査が行われているが、巧妙に審査をすり抜けて不正アプリが配信される事例も発生している※252。公式マーケットにあるアプリだからすべて安全と考えるのではなく、アプリの必要性やアプリのアクセス許可の内容や評価等をしっかりと確認し、不用意にアプリをインストールして、不正アプリによる被害に遭うことがないように気を付けることが重要である。

COLUMN

次は東京　オリンピックを狙ったサイバー攻撃に備えを

2018 年 3 月 18 日、平昌オリンピック・パラリンピック冬季競技大会が無事に閉会しました。サイバー攻撃による大きな混乱は起きなかったものの、開会式中にサイバー攻撃によってプレスセンターの IP テレビシステム等に障害が発生し、その攻撃への対処として組織委員会がネットワークを遮断したことで、公式 Web サイトが一時的にアクセス不能に陥り、情報の閲覧やチケットの印刷ができなくなったといいます※。

前回の夏季大会である、2016 年リオデジャネイロオリンピック・パラリンピック競技大会では、大会の妨害を狙った大規模な DDoS 攻撃だけでなく、偽のチケットサイトやフィッシングによる金銭や個人情報の詐取の被害も発生しました。

オリンピックのような大イベントは、金銭や個人情報を狙う攻撃者にも絶好の機会となります。2 年後に迫った 2020 年東京オリンピック・パラリンピック競技大会でも、大会自体の妨害だけでなく、金銭や個人情報を狙ったサイバー攻撃が発生する可能性が高いといえます。

自国でのオリンピック開催は、一生のうちで何度もない大イベントです。自分の目で観戦するつもりで購入したオリンピックのチケットが、もし偽のチケットサイトのものだったら、金銭的な被害に遭うだけでなく、スタジアムで観戦するはずだった競技を自宅でテレビ観戦するという辛い体験をすることになってしまいます。

「サイバーセキュリティ対処調整センター」（政府オリンピック・パラリンピック CSIRT）が 2018 年度末に設置予定である等、政府機関やライフライン事業者によるサイバー攻撃への対策強化は着実に図られていますが、一般の方々も、オリンピックを契機としたサイバー攻撃に対して「自己防衛」するための備えが必要ではないでしょうか。

オリンピックを悪用した偽のチケットサイトやフィッシングへの対策は、現行の偽サイトやフィッシングへの対策と、共通する部分が多くあります。偽サイトへの対策としては、表示している Web サイトのドメインが公式サイトのドメインであるか確認すること、フィッシングへの対策としては、最新のフィッシングの手口を知っておくこと等が重要です。「1.3.7（4）フィッシングの手口と対策」及び「1.3.7（5）偽サイトの手口と対策」で詳しく解説していますので、ぜひご一読ください。

※Yonhap News：(Olympics) PyeongChang organizers cyber-attacked during opening ceremony　http://english.yonhapnews.co.kr/news/2018/02/10/0200000000AEN20180210000500320.html〔参照 2018-06-07〕

※1 「マルウェア」等の用語が使われ、読者を混乱させる可能性があるため、本白書では特に断りのない限り、また文献引用上の正確性を期する必要のない限り、総称して「ウイルス」と表現する。
※2 IBM 社：IBM X-Force Threat Intelligence Index 2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN〔参照 2018-06-05〕
※3 Symantec 社：2018 年インターネットセキュリティ脅威レポート https://www.symantec.com/ja/jp/security-center/threat-report〔参照 2018-06-05〕
※4 Verizon 社：Tales of dirty deeds and unscrupulous activities. https://www.verizonenterprise.com/verizon-insights-lab/dbir/〔参照 2018-06-05〕
※5 トレンドマイクロ社：2017 年年間セキュリティラウンドアップ セキュリティの常識を覆すサイバー犯罪の転換期 https://resources.trendmicro.com/jp-docdownload-form-m051-web-asr.html〔参照 2018-06-05〕
※6 APWG：Phishing Activity Trends Report http://www.antiphishing.org/resources/apwg-reports/〔参照 2018-06-05〕
※7 JVN iPedia：JVNDB-2017-001843 複数の Microsoft Windows 製品の SMBv1 サーバにおける任意のコードを実行される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-001843.html〔参照 2018-06-05〕
※8 JVN iPedia：JVNDB-2017-001844 複数の Microsoft Windows 製品の SMBv1 サーバにおける任意のコードを実行される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-001844.html〔参照 2018-06-05〕
※9 Cybersecurity Ventures：Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017 https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/〔参照 2018-06-05〕
※10 Ransomware-as-a-Service（RaaS）：身代金請求ウイルスであるランサムウェアを提供する不正活動を支援するサービスの一つ。
※11 ファイルレス攻撃：ハードディスクにファイルを残さず悪意のあるコードをメモリや OS のレジストリ等に埋め込むことで不正な活動を行う攻撃。
※12 ITmedia エンタープライズ：Equifax の情報流出は「人為ミスと技術的失敗」、前 CEO が証言 http://www.itmedia.co.jp/enterprise/articles/1710/04/news051.html〔参照 2018-06-05〕
※13 Fortune：Data Breach Exposes 123 Million U.S. Households http://fortune.com/2017/12/22/experian-data-breach-alteryx-amazon-equifax/〔参照 2018-06-05〕
※14 U.S. News & World Report：German Firms Lost Millions of Euros in 'CEO Fraud' Scam: BSI https://www.usnews.com/news/technology/articles/2017-07-10/german-firms-lost-millions-of-euros-in-ceo-fraud-scam-bsi〔参照 2018-06-05〕
※15 http://www.mbsd.jp/casebook_index.html〔参照 2018-06-05〕
※16 https://www.jpcert.or.jp/ir/report.html〔参照 2018-06-05〕
※17 日本 IBM 社：Tokyo SOC Report https://www.ibm.com/blogs/tokyo-soc/〔参照 2018-06-05〕
※18 フィッシング対策協議会：月次報告書 一覧 https://www.antiphishing.jp/report/monthly/〔参照 2018-06-05〕
※19 フィッシング対策協議会：bitFlyer をかたるフィッシング（2017/11/06） https://www.antiphishing.jp/news/alert/bitflyer_20171106.html〔参照 2018-06-05〕
フィッシング対策協議会：bitbank をかたるフィッシング (2018/03/07) https://www.antiphishing.jp/news/alert/bitbank_20180307.html〔参照 2018-06-05〕
※20 トレンドマイクロ社：不正広告により、仮想通貨発掘ツールが拡散される http://blog.trendmicro.co.jp/archives/16904〔参照 2018-06-05〕
※21 IPA：更新：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html〔参照 2018-05-11〕
IPA：IPA に寄せられているランサムウェアの相談について～ WannaCryptor の感染防止のために今すぐ Windows Update を～ https://www.ipa.go.jp/security/anshin/mgdayori20170515.html〔参照 2018-05-11〕
※22 日経 xTECH：国内襲い始めた WannaCry、日立や JR 東など 600 カ所 2000 端末で感染 http://tech.nikkeibp.co.jp/it/atcl/column/14/346926/051500971/〔参照 2018-05-11〕
※23 トレンドマイクロ社：ランサムウェア「WannaCry ／ Wcry」のワーム活動を解析：侵入／拡散手法に迫る http://blog.trendmicro.co.jp/archives/14920〔参照 2018-05-11〕
※24 IPA：感染が拡大中のランサムウェアの対策について https://www.ipa.go.jp/security/ciadr/vul/20170628-ransomware.html〔参照 2018-05-11〕
IPA：IPA に寄せられているランサムウェアの相談について～ WannaCryptor の感染防止のために今すぐ Windows Update を～ https://www.ipa.go.jp/security/anshin/mgdayori20170515.html〔参照 2018-05-11〕
※25 Forbes JAPAN：身代金ウイルスで「損失額 300 億円」デンマークの海運企業が発表 https://forbesjapan.com/articles/detail/17381〔参照 2018-05-11〕
※26 IPA：感染が拡大中のランサムウェア「Bad Rabbit」の対策について https://www.ipa.go.jp/security/ciadr/vul/20171026-ransomware.html〔参照 2018-05-11〕
※27 アイカ工業株式会社：アイカホームページ再開のお知らせ（弊社ホームページに対するサイバー攻撃について【最終報】） http://www.aica.co.jp/news/corporate/20171120_04.pdf〔参照 2018-05-11〕
※28 ZDNet Japan：ランサムウェア「GandCrab」、2 種類のエクスプロイトキットで拡散 --Malwarebytes 報告 https://japan.zdnet.com/article/35114045/〔参照 2018-05-11〕
※29 トレンドマイクロ社：ランサムウェア「CERBER」に新たな機能追加。ビットコインを窃取 http://blog.trendmicro.co.jp/archives/15664〔参照 2018-05-11〕
※30 Imperva：GLOBAL DDOS THREAT LANDSCAPE Q4 2017 https://www.incapsula.com/ddos-report/ddos-report-q4-2017.html〔参照 2018-05-11〕
※31 Cisco Systems, Inc.：Booters with Chinese Characteristics: The Rise of Chinese Online DDoS Platforms http://blog.talosintelligence.com/2017/08/chinese-online-ddos-platforms.html〔参照 2018-05-11〕
※32 ITmedia エンタープライズ：Android 端末を踏み台にした DDoS 攻撃発生 Google Play に 300 本の不正アプリ http://www.itmedia.co.jp/enterprise/articles/1708/29/news052.html〔参照 2018-05-11〕
※33 日経 xTECH：ネット金融狙う DDoS 攻撃が続く、脅迫型による被害も明らかに http://tech.nikkeibp.co.jp/it/atcl/news/17/092202316/〔参照 2018-05-11〕
※34 JPCERT/CC：Phantom Squad を名乗る攻撃者からの DDoS 攻撃に関する情報 http://www.jpcert.or.jp/newsflash/2017092101.html〔参照 2018-05-11〕
※35 CoinPost：Bittrex も被害に、DDoS 攻撃がもたらす仮想通貨取引所への影響 http://coinpost.jp/?p=10029〔参照 2018-05-11〕
※36 JVN iPedia：JVNDB-2017-000071 SEIL シリーズルータにおけるサービス運用妨害 (DoS) の脆弱性 http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-000071.html〔参照 2018-05-11〕
JVN iPedia：JVNDB-2017-001619 Cisco cBR シリーズ コンバージドブロードバンド ルータにおけるサービス運用妨害 (DoS) の脆弱性 http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-001619.html〔参照 2018-05-11〕
※37 YOMIURI ONLINE：「IoT 乗っ取り」攻撃でツイッターなどがダウン http://www.yomiuri.co.jp/science/goshinjyutsu/20161028-OYT8T50051.html〔参照 2018-05-11〕
※38 株式会社インターネットイニシアティブ：日本国内における Mirai 亜種の感染状況 (2017 年 12 月) https://sect.iij.ad.jp/d/2018/01/091843.html〔参照 2018-05-11〕
JPCERT/CC：Mirai 亜種の感染活動に関する注意喚起 https://www.jpcert.or.jp/at/2017/at170049.html〔参照 2018-05-11〕
※39 INTERNET Watch：街中のクルマ数万台がボットに感染、IoT ボット「Mirai」が走りながらサイバー攻撃！ 仮想通貨取引所への DDoS は利ざや稼ぎが目的か？ https://internet.watch.impress.co.jp/docs/event/1092497.html〔参照 2018-05-11〕
※40 Imperva：New Mirai Variant Launches 54 Hour DDoS Attack against US College https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html〔参照 2018-05-11〕
※41 JPCERT/CC：インシデント報告対応レポート https://www.jpcert.or.jp/ir/report.html〔参照 2018-05-11〕
※42 IPA：WordPress 用プラグイン「WP Job Manager」におけるアクセス制限不備の問題について (JVN#56787058) https://www.ipa.go.jp/security/ciadr/vul/20170615-jvn.html〔参照 2018-05-11〕
※43 Security NEXT：1 年以上にわたりサイトが改ざん状態、閲覧でマルウェア感染のおそれ - 大阪硝子工業会 http://www.security-next.com/080303〔参照 2018-05-11〕
※44 朝日新聞デジタル：自由党のホームページ改ざん 不正アクセス、数日前から https://www.asahi.com/articles/ASK815HLVK81ULBJ00M.html〔参照 2018-05-11〕
※45 SSH（Secure Shell）：暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコル。
※46 Microsoft 社：テクニカル サポート詐欺から身を守る https://support.microsoft.com/ja-jp/help/4013405/windows-protect-from-tech-support-scams〔参照 2018-05-11〕
※47 ジャパン・フード & リカー・アライアンス株式会社：当社連結子会

社通販サイトへの不正アクセスによる個人情報流出の可能性についてのお知らせ　http://contents.xj-storage.jp/xcontents/AS07889/3be70c75/24fd/4569/8a5a/3fbebfd1a74e/140120170413441363.pdf〔参照 2018-05-11〕
※ 48 ぴあ株式会社：ぴあ社がプラットフォームを提供する B.LEAGUE チケットサイト、及びファンクラブ受付サイトへの不正アクセスによる、個人情報流出に関するお詫びとご報告　http://corporate.pia.jp/news/files/security_incident20170425.pdf〔参照 2018-05-11〕
※ 49 IPA：更新：Apache Struts2 の脆弱性対策について (CVE-2017-5638)(S2-045)(S2-046)　https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html〔参照 2018-05-11〕
※ 50 ジェネシス・イーシー株式会社：不正アクセスによるカード情報流出に関するお知らせとお詫び　http://www.genesis-ec.com/20170829.html〔参照 2018-01-23〕
※ 51 GMO インターネット株式会社:サイト M&A（サイト売買仲介サービス）ご登録会員様情報流出のお詫びとお知らせ　https://www.gmo.jp/info/alert/index171030.php〔参照 2018-05-11〕
※ 52 日経 xTECH：GMO インターネットから漏えいの個人情報、Amazon の電子書籍として販売される　http://tech.nikkeibp.co.jp/it/atcl/news/17/110102579/〔参照 2018-05-11〕
※ 53 大阪大学：不正アクセスによる個人情報漏えいについて　http://www.osaka-u.ac.jp/ja/news/topics/2017/12/13_01〔参照 2018-05-11〕
※ 54 総務省：地図による小地域分析（jSTAT MAP）における不正アクセス　http://www.soumu.go.jp/menu_news/s-news/01toukei09_01000023.html〔参照 2018-05-11〕
※ 55 国立研究開発法人情報通信研究機構：Apache Struts2 の脆弱性を悪用した不正アクセスについて https://www.nict.go.jp/info/topics/2017/05/170502-1.html〔参照 2018-05-11〕
※ 56 国土交通省：「土地総合情報システム」における不正アクセスおよび情報流出の可能性について http://www.mlit.go.jp/report/press/totikensangyo05_hh_000129.html〔参照 2018-05-11〕
国土交通省：「土地総合情報システム」における不正アクセス及び情報流出の調査結果について　http://www.mlit.go.jp/report/press/totikensangyo16_hh_000152.html〔参照 2018-05-11〕
※ 57 産経 WEST:患者220人の個人情報漏洩か　阪大医師の個人メールサーバーに中国から不正アクセス　http://www.sankei.com/west/news/170626/wst1706260075-n1.html〔参照 2018-05-11〕
中小企業情報セキュリティ .COM：医員のメールが不正アクセスを受け患者の情報 220 件流出　大阪大学　https:// 中小企業情報セキュリティ .com/%E5%8C%BB%E5%93%A1%E3%81%AE%E3%83%A1%E3%83%BC%E3%83%AB%E3%81%8C%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%82%92%E5%8F%97%E3%81%91%E6%82%A3%E8%80%85%E3%81%AE%E6%83%85%E5%A0%B1220/〔参照 2018-05-11〕
※ 58 株式会社マネースクウェア・ジャパン：サイバー攻撃によるお客様情報の漏えいの可能性について　https://www.m2j.co.jp/info/newsdetail.php?id=1329〔参照 2018-05-11〕
株式会社マネースクウェア・ジャパン：（差替え版）サイバー攻撃によるお客様情報の漏えいについて（7 月 26 日付追加情報）　https://www.m2j.co.jp/info/newsdetail.php?id=1334〔参照 2018-05-11〕
※ 59 東京メトロポリタンテレビジョン株式会社：弊社ホームページに対する不正アクセスによる個人情報流出の可能性について　http://s.mxtv.jp/company/press/pdf/press2017_510001.pdf〔参照 2018-05-11〕
※ 60 株式会社ほくやく・竹山ホールディングス：お客様情報の流出に関するお詫びとお知らせ　http://www.hokutake.co.jp/pdf/news/news_291011-1.pdf〔参照 2018-05-11〕
※ 61 IPA：情報セキュリティ 10 大脅威 2015　https://www.ipa.go.jp/security/vuln/10threats2015.html〔参照 2018-05-11〕
IPA：情報セキュリティ 10 大脅威 2016　https://www.ipa.go.jp/security/vuln/10threats2016.html〔参照 2018-05-11〕
IPA：情報セキュリティ 10 大脅威 2017　https://www.ipa.go.jp/security/vuln/10threats2017.html〔参照 2018-05-11〕
IPA：情報セキュリティ 10 大脅威 2018　https://www.ipa.go.jp/security/vuln/10threats2018.html〔参照 2018-05-11〕
※ 62 佐賀銀行：お客さま情報漏洩の報告とお詫びについて　http://www.sagabank.co.jp/oshirase/000885.php〔参照 2018-05-11〕
※ 63 佐賀新聞 LiVE：佐銀多額窃盗事件、元行員に判決　信用回復の手だて地道に　http://www.saga-s.co.jp/articles/-/163454〔参照 2018-05-11〕
※ 64 DMG 森精機株式会社：弊社社員による製品据付情報持出しについて　https://www.dmgmori.co.jp/corporate/news/pdf/20180129_information.pdf〔参照 2018-05-11〕
※ 65 株式会社スタッフサービス・ホールディングス／株式会社スタッフサービス：ご登録者様の個人情報等の流出に関するお詫びとご報告　http://www.staffservice.co.jp/nt-files/nr_170509.html〔参照 2018-05-11〕
産経ニュース：スタッフサービス元社員、個人情報持ち出す　1 万 5 千人分、該当者に謝罪　http://www.sankei.com/affairs/news/170509/afr1705090033-n1.html〔参照 2018-05-11〕
※ 66 日本経済新聞：市職員、住民情報使いストーカー　熊本・荒尾 https://www.nikkei.com/article/DGXLZO17646150U7A610C1CC1000/〔参照 2018-05-11〕
※ 67 株式会社 Aiming：『剣と魔法のログレス いにしえの女神』の不正アクセスの件　https://aiming-inc.com/ja/news/2017/0621-%e3%80%8e%e5%89%a3%e3%81%a8%e9%ad%94%e6%b3%95%e3%81%ae%e3%83%ad%e3%82%b0%e3%83%ac%e3%82%b9-%e3%81%84%e3%81%ab%e3%81%97%e3%81%88%e3%81%ae%e5%a5%b3%e7%a5%9e%e3%80%8f%e3%81%ae%e4%b8%8d%e6%ad%a3%e3%82%a2/〔参照 2018-05-11〕
※ 68 日本年金機構：元日本年金機構職員の逮捕について　http://www.nenkin.go.jp/oshirase/press/2017/201706/20170629.files/20170629.pdf〔参照 2018-05-11〕
日本経済新聞：年金機構元職員らに猶予刑　個人情報持ち出し、大阪地裁　https://www.nikkei.com/article/DGXMZO27950280090320 18AC8000/〔参照 2018-05-11〕
産経新聞：年金情報 400 人分持ち出しか　機構の元上司と元部下を逮捕　漏洩規模は過去最大　https://www.sankei.com/west/news/170629/wst1706290087-n1.html〔参照 2018-05-11〕
サイバーセキュリティ .com：個人情報 400 件流出か - 日本年金機構の元職員二人を逮捕　https://cybersecurity-jp.com/news/16344〔参照 2018-05-11〕
※ 69 千葉日報：元経理が営業秘密盗む　千葉県警初、容疑で書類送検　https://www.chibanippo.co.jp/news/national/431243〔参照 2018-05-11〕
※ 70 株式会社ビューカード：会員様の個人情報の漏洩に関するお詫びと今後の対応について (2017 年 9 月 28 日）　https://www.jreast.co.jp/card/caution/notice170928.html/〔参照 2018-05-11〕
※ 71 株式会社ゼネテック：お詫びとご報告　http://www.genetec.co.jp/topics/862/〔参照 2018-05-11〕
※ 72 千葉日報：資金計画書など流出　顧客情報 2 万 6 千人分　船橋の不動産業　https://www.chibanippo.co.jp/news/national/477703〔参照 2018-05-11〕
※ 73 IPA：組織における内部不正防止ガイドライン（日本語版）第 4 版　https://www.ipa.go.jp/files/000057060.pdf〔参照 2018-05-11〕
※ 74 http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〔参照 2018-05-11〕
※ 75 日本年金機構：年金からの所得税の源泉徴収について　資料 2 委託業者の契約違反の内容及び当該事業者に対する措置等について　http://www.nenkin.go.jp/oshirase/press/2018/201803/20180320 01.files/20180320 01.pdf〔参照 2018-05-11〕
※ 76 日経新聞：年金過少支給は 20 億円　https://www.nikkei.com/article/DGKKZO28584830W8A320C1EE8000/〔参照 2018-05-11〕
※ 77 The New York Times：How Trump Consultants Exploited the Facebook Data of Millions　https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html〔参照 2018-05-11〕
日経新聞：フェイスブック情報流出　データ主導時代の副作用　https://www.nikkei.com/article/DGXMZO28347810Q8A320C1000000/
※ 78 開発者ニュース：The New Facebook Login and Graph API 2.0　https://developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login〔2018-05-11〕
※ 79 国立大学法人高知大学：個人情報を含むノートパソコン紛失のお詫び　https://www.kochi-u.ac.jp/information/2017042600011/〔参照 2018-05-11〕
※ 80 CNN.co.jp：米有権者 2 億人の個人情報流出、共和党の委託企業から　https://www.cnn.co.jp/tech/35102994.html〔参照 2018-05-11〕
UpGuard, Inc.：The RNC Files: Inside the Largest US Voter Data Leak　https://www.upguard.com/breaches/the-rnc-files〔参照2018-05-11〕
GIZMODE：GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters　https://gizmodo.com/gop-data-firm-accidentally-leaks-personal-details-of-ne-1796211612〔参照 2018-05-11〕
※ 81 株式会社メルカリ：Web 版のメルカリにおける個人情報流出に関するお詫びとご報告※ 6/23 追記あり　https://about.mercari.com/press/news/article/20170622_incident_report/〔参照 2018-05-11〕
株式会社メルカリ：CDN 切り替え作業における、Web 版メルカリの個人情報流出の原因につきまして　http://tech.mercari.com/entry/2017/

06/22/204500〔参照 2018-05-11〕
※ 82 セキュリティクリアランス：秘密にすべき情報を扱う職員に対して、その適格性を確認すること。
※ 83 CSO FROM IDG：Sweden leaks its military secrets, national driver database in IBM outsourcing deal https://www.cso.com.au/article/625148/sweden-leaks-its-military-secrets-national-driver-database-ibm-outsourcing-deal/〔参照 2018-05-11〕
※ 84 株式会社エイチ・アイ・エス：国内バスツアーサイトからのお客様情報流出について https://www.his.co.jp/material/pdf/n_co_20170822.pdf〔参照 2018-05-11〕
※ 85 株式会社宮地商会（宮地楽器）：お客さまの氏名・メールアドレスの情報流出について http://www.miyajimusic.com/pdf/info20170905.pdf〔参照 2018-05-11〕
※ 86 Krebs on Security：Dell Lost Control of Key Customer Support Domain for a Month in 2017 https://krebsonsecurity.com/2017/10/dell-lost-control-of-key-customer-support-domain-for-a-month-in-2017/〔参照 2018-05-11〕
※ 87 株式会社ミクシィ・リクルートメント：システム設定不備による Web 履歴書情報への外部アクセスの可能性について https://www.mixi-recruitment.co.jp/news/2018/0109/01.html〔参照 2018-05-11〕
※ 88 IPA：日常における情報セキュリティ対策 https://www.ipa.go.jp/security/measures/everyday.html〔参照 2018-05-11〕
※ 89 IPA：企業（組織）における最低限の情報セキュリティ対策のしおり+1 https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf〔参照 2018-05-11〕
IPA：安全なウェブサイトの構築と運用管理に向けての 16 ヶ条 ～セキュリティ対策のチェックポイント～ https://www.ipa.go.jp/security/vuln/websitecheck.html〔参照 2018-05-11〕
※ 90 IC3：Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam https://www.ic3.gov/media/2017/170504.aspx〔参照 2018-05-11〕
※ 91 日本経済新聞：企業狙う振り込め詐欺 https://www.nikkei.com/article/DGKKZO04776090S6A710C1CR8000/〔参照 2018-05-11〕
※ 92 日本経済新聞：そのメールは詐欺だ! 手口が「進化」、対策は 3 つ https://www.nikkei.com/article/DGXMZO25037790V21C17A2000000/〔参照 2018-05-11〕
※ 93 日経 xTECH：ビジネスメール詐欺の被害が国内でも続出、銀行が注意喚起 http://tech.nikkeibp.co.jp/it/atcl/column/14/346926/102401175/〔参照 2018-05-11〕
※ 94 トレンドマイクロ社：法人組織におけるセキュリティ実態調査 2017 年版 | 資料ダウンロード https://appweb.trendmicro.com/doc_dl/select.asp?type=1&cid=236〔参照 2018-05-11〕
※ 95 日本経済新聞：アドレス1字違い見逃す 日航 3.8 億円メール詐欺被害 https://www.nikkei.com/article/DGXMZO24979150S7A221C1EA5000/〔参照 2018-05-11〕
朝日新聞デジタル：JAL が振り込め詐欺被害 「航空機リース料」信じる https://www.asahi.com/articles/ASKDN66QBKDNUTIL04Y.html〔参照 2018-05-11〕
日経 xTECH: JAL が「信じ込んでしまった」手口とは、振り込め詐欺で 3.8 億円被害 http://tech.nikkeibp.co.jp/it/atcl/column/14/346926/122001256/〔参照 2018-05-11〕
Aviation Wire：JAL、詐欺被害 3 億 8000 万円 777 リース料や貨物委託料送金 http://www.aviationwire.jp/archives/136855〔参照 2018-05-11〕
産経ニュース：日本航空が“振り込め”詐欺被害に 航空機リース料名目で 3 億 8 千万円 http://www.sankei.com/affairs/news/171220/afr1712200056-n1.html〔参照 2018-05-11〕
YOMIURI ONLINE：JAL3.8 億円詐欺被害 ビジネスメールに割り込み偽請求 http://www.yomiuri.co.jp/science/goshinjyutsu/20180109-OYT8T50178.html〔参照 2018-05-11〕
※ 96 産経ニュース：スカイマークにも偽メール 2 回 200 万円超を請求 日航 3 億円被害 http://www.sankei.com/affairs/news/171221/afr1712210033-n1.html〔参照 2018-05-11〕
日経 xTECH：スカイマークにも振り込め詐欺、1 度信じたが金銭被害は免れる、ANA は「メールは確認されていない」 http://tech.nikkeibp.co.jp/it/atcl/news/17/122102902/〔参照 2018-05-11〕
※ 97 警察庁：平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf〔参照 2018-05-11〕
※ 98 Federal Trade Commission：FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams https://www.ftc.gov/news-events/press-releases/2017/05/ftc-federal-state-international-partners-announce-major-crackdown〔参照 2018-05-11〕
※ 99 IPA：安心相談窓口だより 被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開～ 2016 年度の偽警告に関する相談件数は昨年度の 7.7 倍に～ https://www.ipa.go.jp/security/anshin/mgdayori20170411.html〔参照 2018-05-11〕
※ 100 警視庁：サポート詐欺にだまされないで!!（第 1 弾） https://www.youtube.com/watch?v=MsXbBr9D2sw〔参照 2018-05-11〕
※ 101 アクティベート:ソフトウェアを有効にし、利用できる状態にすること。
※ 102 独立行政法人国民生活センター:「アダルトサイトとのトラブル解決」をうたう探偵業者にご注意! http://www.kokusen.go.jp/news/data/n-20161215_1.html〔参照 2018-05-11〕
※ 103 フィッシング対策協議会：2018/03 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/201803.html〔参照 2018-05-11〕
※ 104 フィッシング対策協議会：bitFlyer をかたるフィッシング (2017/11/06) https://www.antiphishing.jp/news/alert/bitflyer_20171106.html〔参照 2018-05-11〕
※ 105 フィッシング対策協議会：緊急情報一覧 https://www.antiphishing.jp/news/alert/〔参照 2018-05-11〕
※ 106 警察庁：日本サイバー犯罪対策センターによるインターネットショッピングに係る詐欺サイト対策について https://www.npa.go.jp/cyber/policy/pdf/20171221.pdf〔参照 2018-05-11〕
※ 107 警察庁：警察庁サイトを装う偽サイトについて http://www.npa.go.jp/cyber/pdf/caution201708.pdf〔参照 2018-05-11〕
※ 108 トレンドマイクロ社：警察を偽装したネット詐欺を国内で新たに確認 http://blog.trendmicro.co.jp/archives/15600〔参照 2018-05-11〕
※ 109 警察庁：平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf〔参照 2018-05-11〕
警察庁：平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf〔参照 2018-05-11〕
警察庁：平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf〔参照 2018-05-11〕
警察庁：平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf〔参照 2018-05-11〕
警察庁：平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf〔参照 2018-05-11〕
※ 110 JC3：インターネットバンキングマルウェア「DreamBot」による被害に注意 https://www.jc3.or.jp/topics/dreambot_cm.html〔参照 2018-05-11〕
※ 111 JC3：インターネットバンキングの不正送金の被害に注意 https://www.jc3.or.jp/topics/dreambot.html〔参照 2018-05-11〕
警察庁：インターネットバンキングに係るコンピュータウイルス DreamBot に関する注意喚起 http://www.npa.go.jp/cyber/policy/20171211.html〔参照 2018-05-11〕
※ 112 JC3：DreamBot・Gozi 感染チェックサイト https://www.jc3.or.jp/info/dgcheck.html〔参照 2018-05-11〕
※ 113 エクスプロイトキット：攻撃者が脆弱性を悪用した攻撃を行うために使用するツール。
※ 114 SMBv1（Server Message Block 1.0）：ネットワークを介して端末間でファイルやプリンタ等を共有する際に利用されるプロトコル。
※ 115 https://www.ipa.go.jp/security/anshin/mgdayori20170713.html〔参照 2018-05-11〕
※ 116 The No More Ransom Project：https://www.nomoreransom.org/ja/index.html〔参照 2018-05-11〕
IPA：ランサムウェア対策特設ページ https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html〔参照 2018-05-11〕
※ 117 Imperva：Global DDoS Threat Landscape Q3 2017 https://www.incapsula.com/ddos-report/ddos-report-q3-2017.html〔参照 2018-05-11〕
※ 118 JPCERT/CC：ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起 https://www.jpcert.or.jp/at/2014/at140001.html〔参照 2018-05-11〕
※ 119 井澤志充：NTP を使った DDoS について https://www.slideshare.net/yizawa/ntp-ampattack〔参照 2018-05-11〕
※ 120 GitHub Inc.：February 28th DDoS Incident Report https://githubengineering.com/ddos-incident-report/〔参照 2018-05-11〕
※ 121 アカマイ・テクノロジーズ合同会社：MEMCACHED を利用した UDP リフレクション DDOS https://blogs.akamai.com/jp/2018/03/aa.html〔参照 2018-05-11〕
※ 122 トレンドマイクロ社:GitHub に 1TBps 超の攻撃、「memcached」を利用する新たな DDoS 手法を解説 http://blog.trendmicro.co.jp/

archives/17116〔参照 2018-05-11〕
※ 123 アカマイ・テクノロジーズ合同会社：MEMCACHED を利用した 1.3TBPS の DDOS 攻撃　https://blogs.akamai.com/jp/2018/03/memcached13tbpsddos.html〔参照 2018-05-11〕
※ 124 Imperva：The Top 10 DDoS Attack Trends　https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf〔参照 2018-05-11〕
※ 125 Imperva：Ginormous POST Flood Spells BIG Trouble for Hybrid DDoS Protection　https://www.incapsula.com/blog/post-flood-hybrid-ddos-protection.html?_fsi=DsYSEHcw〔参照 2018-05-11〕
※ 126 IPA:Apache Struts2の脆弱性対策について(CVE-2017-9805)(S2-052)　https://www.ipa.go.jp/security/ciadr/vul/20170906-struts.html〔参照 2018-05-11〕
※ 127 IPS（Intrusion Prevention System：侵入防止システム）：不正アクセスを検知し、必要に応じて通信を遮断する装置。
※ 128 WAF（Web Application Firewall）：主に Web アプリケーションへの攻撃を防御する装置。
※ 129 警察庁：攻撃ツール「Eternalblue」を悪用した攻撃と考えられるアクセスの観測について　https://www.npa.go.jp/cyberpolice/important/2017/201705151.html〔参照 2018-05-11〕
※ 130 国立研究開発法人情報通信研究機構：ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19)　http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf〔参照 2018-05-11〕
※ 131 https://jvndb.jvn.jp/〔参照 2018-05-11〕
※ 132 Ursnif（アースニフ、別名：Gozi、Snifula、Papras 等）：日本国内において、2016 年 3 月より観測されている、インターネットバンキングの情報を窃取し、不正送金を行うウイルス。
※ 133 DreamBot：日本国内において、2016 年 12 月ごろより観測されているウイルスで、Tor を用いた通信機能を持たせた Ursnif の亜種。
※ 134 https://www.ibm.com/blogs/tokyo-soc/wp-content/uploads/2017/09/tokyo_soc_report2017_h1.pdf〔参照 2018-05-11〕
※ 135 警察庁：インターネットバンキングに係るコンピュータウイルス DreamBot に関する注意喚起　https://www.npa.go.jp/cyber/policy/20171211.html〔参照 2018-05-11〕
※ 136 JC3：インターネットバンキングの不正送金の被害に注意　https://www.jc3.or.jp/topics/dreambot.html〔参照 2018-05-11〕
※ 137 日本 IBM 社：日本に迫る金融系マルウェア Ursnif 攻撃キャンペーンの波　https://www.ibm.com/blogs/security/jp-ja/ursnif-campaign-waves-breaking-on-japanese-shores/〔参照 2018-05-11〕
※ 138 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017 年 10 月～ 12 月]　https://www.ipa.go.jp/files/000063812.pdf〔参照 2018-05-11〕
※ 139 パロアルトネットワークス株式会社：銀行を狙うトロイの木馬：日本の感染者を踏み台に世界中に攻撃を行う、Ursnif による配信ネットワークが明らかに　https://www.paloaltonetworks.jp/company/in-the-news/2017/unit42-trojan-horses-aiming-at-banks.html〔参照 2018-05-11〕
※ 140 JC3：犯罪被害につながるメール INDEX 版　https://www.jc3.or.jp/topics/vm_index.html〔参照 2018-05-11〕
※ 141 日本 IBM 社：日本に迫る金融系マルウェア Ursnif 攻撃キャンペーンの波　https://www.ibm.com/blogs/security/jp-ja/ursnif-campaign-waves-breaking-on-japanese-shores/〔参照 2018-05-11〕
JC3：犯罪被害につながるメール INDEX 版　https://www.jc3.or.jp/topics/vm_index.html〔参照 2018-05-11〕
※ 142 楽天カード株式会社：フィッシングの被害からお客様を守るために　https://www.rakuten-card.co.jp/guide/securityinfo/〔参照 2018-05-11〕
※ 143 IPA：Microsoft 製品の脆弱性対策について (2017 年 4 月)　https://www.ipa.go.jp/security/ciadr/vul/20170412-ms.html〔参照 2018-05-11〕
※ 144 IPA：Microsoft Office の脆弱性 (CVE-2017-11882) について　https://www.ipa.go.jp/security/ciadr/vul/20171129_ms.html〔参照 2018-05-11〕
※ 145 株式会社ラック：CYBER GRID VIEW Vol.2　https://www.lac.co.jp/lacwatch/pdf/20160802_cgview_vol2_a001t.pdf〔参照 2018-05-11〕
※ 146 https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔参照 2018-05-11〕
※ 147 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2016 年 4 月～ 6 月]　https://www.ipa.go.jp/files/000053922.pdf〔参照 2018-05-11〕
※ 148 サイバーリーズン・ジャパン株式会社：ランサムウェア「ONI（鬼）」ランサムウェアを利用し、日本企業への侵入の痕跡を消去　https://www.cybereason.co.jp/blog/ransomware/1830/〔参照 2018-05-11〕
※ 149 McAfee LLC：Updated BlackEnergy Trojan Grows More Powerful　https://securingtomorrow.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/〔参照 2018-05-11〕
※ 150 JPCERT/CC:PowerSploitを悪用して感染するマルウエア(2017-02-10)　https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html〔参照 2018-05-11〕
※ 151 http://www.jsps.go.jp/〔参照 2018-05-11〕
※ 152 辻伸弘：日本学術振興会を騙った標的型攻撃メール 調査メモ　http://csirt.ninja/?p=1103〔参照 2018-05-11〕
※ 153 株式会社ラック：PowerShell Empire を利用した標的型攻撃　https://www.lac.co.jp/lacwatch/people/20170807_001352.html〔参照 2018-05-11〕
※ 154 アメリカ学会：緊急不審メール情報ーアメリカ学会を語ったなりすましのメール（「富士山会合提言」というメールは決して開けないでください）　http://www.jaas.gr.jp/blog/2017/07/post-284.html〔参照 2018-05-11〕
アメリカ学会：続　緊急不審メール情報ーアメリカ学会を語ったなりすましのメール（「アーミテージ・ナイ報告」「富士山会合」というメールの添付ファイルは決して開けないでください）　http://www.jaas.gr.jp/blog/2017/07/post-285.html〔参照 2018-05-11〕
※ 155 マカフィー株式会社：高度化するファイルレス攻撃に対処せよ　https://blogs.mcafee.jp/post-e8b5〔参照 2018-05-11〕
トレンドマイクロ社：より高度な「ファイルレス活動」を実現した一連のマルウェアを確認　http://blog.trendmicro.co.jp/archives/15653〔参照 2018-05-11〕
※ 156 Cylance Japan 株式会社：日本をターゲットにした GlobeImposter の亜種（”ONI” の正体）　https://www.cylance.com/ja_jp/blog/jp-oni-ransomware-globeimposter.html〔参照 2018-05-11〕
※ 157 IPA：文書ファイルの新たな悪用手口に関する注意点　https://www.ipa.go.jp/files/000060949.pdf〔参照 2018-05-11〕
※ 158 Microsoft 社：保護ビューとは　https://support.office.com/ja-jp/article/%E4%BF%9D%E8%AD%B7%E3%83%93%E3%83%A5%E3%83%BC%E3%81%A8%E3%81%AF-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653〔参照 2018-05-11〕
※ 159 ソーシャルエンジニアリング：なりすまし等を行い、騙す相手（人間）の心理的な隙やミスに付け込んで情報を盗む技術。
※ 160 トレンドマイクロ社：多額の損失をもたらすビジネスメール詐欺「BEC」- 脅威データベース　https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3151/billiondollar-scams-the-numbers-behind-business-email-compromise〔参照 2018-05-11〕
Trend Micro Incorporated：Tracking Trends in Business Email Compromise (BEC) Schemes　https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf〔参照 2018-05-11〕
Kaspersky Lab：Nigerian phishing: industrial companies under attack　https://ics-cert.kaspersky.com/reports/2017/06/15/nigerian-phishing-industrial-companies-under-attack/〔参照 2018-05-11〕
※ 161 J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan（サイバー情報共有イニシアティブ）の略称。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策につなげていく取り組み。
※ 162 IPA：【注意喚起】偽口座への送金を促す “ビジネスメール詐欺” の手口　https://www.ipa.go.jp/security/announce/20170403-bec.html〔参照 2018-05-11〕
※ 163 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017 年 4 月～ 6 月]　https://www.ipa.go.jp/files/000060948.pdf〔参照 2018-05-11〕
IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017 年 10 月～ 12 月]　https://www.ipa.go.jp/files/000063812.pdf〔参照 2018-05-11〕
※ 164 トレンドマイクロ社：多額の損失をもたらすビジネスメール詐欺「BEC」- 脅威データベース　https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3151/billiondollar-scams-the-numbers-behind-business-email-compromise〔参照 2018-05-11〕
※ 165 IPA：なりすましメール撲滅に向けた SPF（Sender Policy Framework）導入の手引き　https://www.ipa.go.jp/security/topics/20120523_spf.html〔参照 2018-05-11〕
※ 166 一般財団法人インターネット協会：DKIM（Domainkeys Identified Mail）　http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/〔参照 2018-05-11〕
※ 167 IPA：不正ログイン対策特集ページ　https://www.ipa.go.jp/security/anshin/account_security.html〔参照 2018-05-11〕
※ 168 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017

年７月～９月］ https://www.ipa.go.jp/files/000062172.pdf〔参照 2018-05-11〕
※ 169 IPA：安心相談窓口だより 偽警告で、また新たな手口が出現～パソコンが正常に操作できなくなったと錯覚させる多数の狡猾な細工～ https://www.ipa.go.jp/security/anshin/mgdayori20170329.html〔参照 2018-05-11〕
※ 170 IPA：安心相談窓口だより 「その警告表示はソフトウェア購入へ誘導されるかも知れません」～ Yes. Ok. クリック前に 一呼吸 https://www.ipa.go.jp/security/txt/2015/02outline.html〔参照 2018-05-11〕
※ 171 独立行政法人国民生活センター：全国の消費生活センター等 http://www.kokusen.go.jp/map/index.html〔参照 2018-05-11〕
※ 172 警視庁：詐欺被害の解決・返金をうたう探偵業者 http://www.keishicho.metro.tokyo.jp/kurashi/higai/tantei_trouble.html〔参照 2018-05-11〕
※ 173 フィッシング対策協議会：Apple をかたるフィッシング (2017/10/23) https://www.antiphishing.jp/news/alert/apple_20171023.html〔参照 2018-05-11〕
※ 174 フィッシング対策協議会：資料公開： 利用者向けフィッシング詐欺対策ガイドラインの改訂について https://www.antiphishing.jp/report/guideline/consumer_guideline2017.html〔参照 2018-05-11〕
※ 175 2 段階認証：ID、パスワードの認証に追加して、追加の認証コード等による確認を行うことで不正ログインを防ぐ仕組み。
※ 176 JC3：詐欺サイト等悪質なショッピングサイトに関する注意喚起 https://www.jc3.or.jp/topics/malicious_site.html〔参照 2018-05-11〕
※ 177 TLD（トップレベルドメイン）：インターネット上で使用されるドメイン名において、末尾部に配置される「com」や「jp」「org」等といった文字列のこと。
※ 178 国民生活センター越境消費者センター：悪質な通販サイトにご注意! https://www.ccj.kokusen.go.jp/aksht_kikk〔参照 2018-05-11〕
※ 179 CNET Japan：日本語表示に対応したモバイル版ランサムウェアを初確認 https://japan.cnet.com/article/35079658/〔参照 2018-05-11〕
※ 180 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔参照 2018-05-11〕
※ 181 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/CVE.html〔参照 2018-05-11〕
※ 182 The MITRE Corporation：CVE Numbering Authorities https://cve.mitre.org/cve/cna.html〔参照 2018-05-11〕
※ 183 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs) https://cve.mitre.org/news/archives/2016/news.html〔参照 2018-05-11〕
※ 184 The MITRE Corporation：SAP Added as CVE Numbering Authority (CNA) https://cve.mitre.org/news/archives/2017/news.html〔参照 2018-05-11〕
※ 185 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/CWE.html〔参照 2018-05-11〕
※ 186 IPA：共通脆弱性評価システム CVSS 概説 https://www.ipa.go.jp/security/vuln/CVSS.html〔参照 2018-05-11〕
※ 187 JPCERT/CC：セキュアコーディング https://www.jpcert.or.jp/securecoding/〔参照 2018-05-11〕
※ 188 Equifax, Inc.：Equifax Announces Cybersecurity Incident Involving Consumer Information https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628〔参照 2018-05-11〕
※ 189 Equifax, Inc.：Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832〔参照 2018-05-11〕
※ 190 Apache Software Foundation：Apache Struts 2 Documentation (S2-045) https://cwiki.apache.org/confluence/display/WW/S2-045〔参照 2018-05-11〕
※ 191 日本マイクロソフト株式会社：ご存じですか？ OS にはサポート期限があります! https://www.microsoft.com/ja-jp/atlife/article/windows10-portal/eos.aspx〔参照 2018-05-11〕
※ 192 日本マイクロソフト株式会社：Windows 7 & Office 2010 2020 年サポート終了 https://www.microsoft.com/ja-jp/business/windows/endofsupport.aspx〔参照 2018-05-11〕
※ 193 Adobe Systems Inc.：Flash & The Future of Interactive Content https://theblog.adobe.com/adobe-flash-update/〔参照 2018-05-11〕
※ 194 CMS（Content Management System）：Web サイトを構築し、コンテンツ（Web ページ、テキストや画像等）を統合的に管理するシステム。
※ 195 トレンドマイクロ社：2017 年第 1 四半期セキュリティラウンドアップ https://www.trendmicro.com/content/dam/trendmicro/global/ja/security-intelligence/research-reports/sr/sr-2017q1/2017q1sr0602.pdf〔参照 2018-05-11〕
※ 196 脆弱性関連情報：脆弱性に関する情報であり、「脆弱性情報」「検証方法」「攻撃方法」のいずれかに該当する情報である。（参考：IPA：脆弱性関連情報の届出受付 https://www.ipa.go.jp/security/vuln/report/index.html〔参照 2018-05-11〕）
※ 197 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況 [2017 年第 4 四半期（10 月～ 12 月）] https://www.ipa.go.jp/files/000063751.pdf〔参照 2018-05-11〕
※ 198 ソフトウェア製品の取り扱い終了は、「不受理」「脆弱性でない」「脆弱性対策情報公表済み」「公表せずに製品開発者が利用者ごとに個別で対策を実施済み」であることを指す。Web アプリケーションの取り扱い終了は、「不受理」「脆弱性でない」「連絡不可能」「修正完了」「IPA による注意喚起実施済み」であることを指す。
※ 199 IPA：【注意喚起】Windows アプリケーションの利用における注意 https://www.ipa.go.jp/security/ciadr/vul/20170928_dll.html〔参照 2018-05-11〕
JPCERT/CC でも、DLL 読み込みの脆弱性に関する情報を公開している。JPCERT/CC：Windows アプリケーションの DLL 読み込みに関する脆弱性について https://www.jpcert.or.jp/tips/2017/wr172001.html〔参照 2018-05-11〕
※ 200 IPA：重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html〔参照 2018-05-11〕
※ 201 https://www.ipa.go.jp/security/anshin/〔参照 2018-05-11〕
※ 202 GMO ペイメントゲートウェイ株式会社：再発防止委員会の調査報告等に関するお知らせ https://corp.gmo-pg.com/newsroom/pdf/170501_gmo_pg_ir-kaiji-02.pdf〔参照 2018-05-11〕
※ 203 Lukasz Lenart：[ANN] Apache Struts 2.5.10.1 GA with Security Fixe Release https://lists.apache.org/thread.html/c744d564201a388dbfa9c1b426d49ded34b4903863a87af905e75bd7@%3Cannouncements.struts.apache.org%3E〔参照 2018-05-11〕
※ 204 IPA：脆弱性関連情報として取り扱えない場合の考え方の解説 https://www.ipa.go.jp/security/vuln/report/notice/handling_notaccept.html〔参照 2018-06-14〕
※ 205 http://wooyun.org/〔参照 2018-05-11〕
※ 206 IPA：【注意喚起】SQL インジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を https://www.ipa.go.jp/security/announce/website_vuln.html〔参照 2018-05-11〕
※ 207 IPA：SQL インジェクション攻撃に関する注意喚起 https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html〔参照 2018-05-11〕
※ 208 IPA: 脆弱性の深刻度評価の新バージョン CVSS v2 への移行について https://www.ipa.go.jp/security/vuln/SeverityLevel2.html〔参照 2018-05-11〕
※ 209 JVN：JVN#98295787: ワイヤレスモバイルストレージ「デジ蔵 ShAirDisk」PTW-WMS1 における複数の脆弱性 https://jvn.jp/jp/JVN98295787/index.html〔参照 2018-05-11〕
※ 210 JVN：JVN#7638293: ロボット家電 COCOROBO におけるセッション管理不備の脆弱性 https://jvn.jp/jp/JVN76382932/index.html〔参照 2018-05-11〕
※ 211 JVN：JVN#46830433: アイ・オー・データ製の複数のネットワークカメラ製品に複数の脆弱性 https://jvn.jp/jp/JVN46830433/index.html〔参照 2018-05-11〕
※ 212 株式会社アイ・ティ・アール：ITR Market View：サイバー・セキュリティ・コンサルティング・サービス市場 2017 https://www.itr.co.jp/report/marketview/M17001000.html〔参照 2018-05-11〕
※ 213 HackerOne：脆弱性情報の公開と、バグ発見者への報奨金プログラムを提供するプラットフォーム。
※ 214 バグバウンティプログラム：「脆弱性報奨金制度」等とも呼ばれ、企業等が一般に対して脆弱性やバグに報奨金をかけ、発見者に対し報奨金を支払う制度。
※ 215 HackerOne：THE HACKER-POWERED SECURITY REPORT 2017 https://www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf〔参照 2018-05-11〕
※ 216 bugcrowd：The 2017 State of Bug Bounty https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/〔参照 2018-05-11〕
※ 217 Kevin Finisterre：Why I walked away from $30,000 of DJI bounty money https://regmedia.co.uk/2017/11/16/whyiwalkedfrom3k.pdf〔参照 2018-05-11〕
※ 218 DJI：DJI Bug Bounty Program Policy https://security.dji.com/policy?lang=en_US〔参照 2018-05-11〕
※ 219 DJI：DJI To Offer 'Bug Bounty' Rewards For Reporting Software Issues https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues〔参照 2018-05-11〕

※ 220 HackerOne：BUG BOUNTY FIELD MANUAL　https://www.hackerone.com/resources/bug-bounty-field-manual〔参照 2018-05-11〕
※ 221 CTF TIME：https://ctftime.org/〔参照 2018-05-11〕
※ 222 経済産業省：ソフトウエア製品等の脆弱性関連情報に関する取扱規程　http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔参照 2018-05-11〕
※ 223 https://www.ipa.go.jp/security/vuln/report/notice/handling_20170530.html〔参照 2018-05-11〕
※ 224 脆弱性による影響が小さい場合、パートナーシップによる取り扱いは終了しても、パートナーシップにおいて「脆弱性ではない」と判断したわけではない。Web サイト運営者、及び製品開発者に対して、攻撃が発生した場合の経営リスク等を考慮した上で対応方針を検討するよう IPA、JPCERT/CC から案内する。
※ 225 IPA：情報セキュリティ早期警戒パートナーシップガイドライン https://www.ipa.go.jp/files/000059694.pdf〔参照 2018-05-11〕
※ 226 IPA：「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」報告書について　https://www.ipa.go.jp/security/fy29/reports/scrm/index.html〔参照 2018-05-28〕
※ 227 http://www.soumu.go.jp/main_content/000542503.pdf〔参照 2018-05-28〕
※ 228 ISEN：平成 28 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版　http://school-security.jp/pdf/2016.pdf〔参照 2018-05-28〕
ISEN：平成 27 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版　http://school-security.jp/pdf/2015.pdf〔参照 2018-05-28〕
ISEN：平成 26 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版　http://school-security.jp/pdf/2014.pdf〔参照 2018-05-28〕
※ 229 2015 年度と 2014 年度のセキュリティインシデント数は「平成 28 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版」に記載されているものである。図 1-5-6 は「平成 27 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版」及び「平成 26 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版」を基に作成しているため、本文のセキュリティインシデント数と図の標本数は異なった数になっている。
※ 230 共立女子大学・共立女子短期大学（学校法人共立女子学園）：個人情報を保存したノートパソコン紛失に関するお詫び　http://www.kyoritsu-wu.ac.jp/uploads/news/news_release_2017051.pdf〔参照 2018-05-28〕
立教大学（学校法人立教学院）：個人情報の紛失に関するお詫びとお知らせ　http://www.rikkyo.ac.jp/news/2017/05/qo9edr000000mlx7.html〔参照 2018-05-28〕
※ 231 大阪工業大学（学校法人常翔学園）：学生の個人情報を保存した USB メモリ紛失について（お詫び）　http://www.oit.ac.jp/japanese/news/index.php?i=4334〔参照 2018-05-28〕
※ 232 朝日新聞デジタル：阪大生のメールに不正アクセス、患者情報漏洩の可能性　https://www.asahi.com/articles/ASK6V5TVRK6VPTIL01M.html〔参照 2018-05-28〕
※ 233 国立大学法人島根大学：本学 Web サーバからの個人情報漏えいの可能性に関する報告及び今後の対応について（お詫び）　https://www.shimane-u.ac.jp/docs/2017102000188/〔参照 2018-05-28〕
※ 234 国立大学法人新潟大学：本学医歯学総合病院管理パソコンのコンピュータウイルス感染について　https://www.niigata-u.ac.jp/news/2017/38642/〔参照 2018-05-28〕
※ 235 国立大学法人新潟大学：医歯学総合病院ホームページの改ざんについて　https://www.niigata-u.ac.jp/news/2018/38847/〔参照 2018-05-28〕
※ 236 Security NEXT：中部大でランサムウェア被害 - 不正ログイン後にインストールか　http://www.security-next.com/091067〔参照 2018-05-28〕
※ 237 公立大学法人新潟県立看護大学：メールサーバーへの不正アクセスと迷惑メールの送信について　https://www.niigata-cn.ac.jp/information/2018-0116-0852-27.html〔参照 2018-05-28〕
上越タウンジャーナル：アカウント不正利用され迷惑メール 37 万件送信 上越市の新潟県立看護大学　https://www.joetsutj.com/articles/51144748〔参照 2018-05-28〕
※ 238 日経 xTECH：青学大が全教員のパスワードを変更、不審メール送信続き緊急措置　http://tech.nikkeibp.co.jp/it/atcl/news/17/120502793/〔参照 2018-05-28〕
※ 239 産経 WEST：生徒 1300 人分の個人情報流出 鹿児島県の私立高校　https://www.sankei.com/west/news/170425/wst1704250044-n1.html〔参照 2018-05-28〕
※ 240 ITmedia：前橋市立小中学校、全児童生徒の個人情報流出 不正アクセスで　http://www.itmedia.co.jp/news/articles/1804/05/news081.html〔参照 2018-05-28〕
※ 241 前橋市：前橋市教育委員会ネットワークへの不正アクセスにより流出した可能性のある個人情報の特定について　http://www.city.maebashi.gunma.jp/sisei/532/001/p019321.html〔参照 2018-05-28〕
※ 242 NISC：次期サイバーセキュリティ戦略骨子　https://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou02.pdf〔参照 2018-05-28〕
※ 243 NII：高等教育機関における情報セキュリティポリシー策定について　https://www.nii.ac.jp/service/sp/〔参照 2018-05-28〕
※ 244 http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2017/10/18/1397369.pdf〔参照 2018-05-28〕
※ 245 https://www.ipa.go.jp/files/000062904.pdf〔参照 2018-05-28〕
※ 246 IPA：不正ログイン対策特集ページ　https://www.ipa.go.jp/security/anshin/account_security.html〔参照 2018-05-28〕
※ 247 パソコン利用者の習熟度をレベル 4 の「パソコンを組み立てたり、トラブルが起きても自分で解決できるレベルである」からレベル 1 の「パソコンの設定はお店や家族・知人に任せ、メールやホームページの閲覧をする程度で簡単な操作ならできるレベルである」までの 4 段階で自己評価したもの。「2017 年度情報セキュリティの脅威に対する意識調査」の調査票「パソコンでのインターネット利用と情報セキュリティに関するアンケート」Q3 参照（https://www.ipa.go.jp/files/000062913.pdf〔参照 2018-05-28〕）。
※ 248 総務省：平成 29 年版 情報通信白書　http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/29honpen.pdf〔参照 2018-05-28〕
※ 249 2017 年 JVN iPedia 活動報告レポートの数値を集計（2017 年 1 ～ 3 月 159 件、4 ～ 6 月 118 件、7 ～ 9 月 298 件、10 ～ 12 月 254 件）。
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 1 四半期（1 月～ 3 月）］　https://www.ipa.go.jp/files/000059090.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 2 四半期（4 月～ 6 月）］　https://www.ipa.go.jp/files/000060905.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 3 四半期（7 月～ 9 月）］　https://www.ipa.go.jp/files/000062122.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 4 四半期（10 月～ 12 月）］　https://www.ipa.go.jp/files/000063694.pdf〔参照 2018-05-28〕
※ 250 2017 年 JVN iPedia 活動報告レポートの数値を集計（2017 年 1 ～ 3 月 108 件、4 ～ 6 月 136 件、7 ～ 9 月 48 件、10 ～ 12 月 74 件）。
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 1 四半期（1 月～ 3 月）］　https://www.ipa.go.jp/files/000059090.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 2 四半期（4 月～ 6 月）］　https://www.ipa.go.jp/files/000060905.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 3 四半期（7 月～ 9 月）］　https://www.ipa.go.jp/files/000062122.pdf〔参照 2018-05-28〕
IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート［2017 年第 4 四半期（10 月～ 12 月）］　https://www.ipa.go.jp/files/000063694.pdf〔参照 2018-05-28〕
※ 251 IPA：Bluetooth の実装における複数の脆弱性について　https://www.ipa.go.jp/security/ciadr/vul/20170914_blueborne.html〔参照 2018-05-28〕
※ 252 ITmedia エンタープライズ：「Google Play」にマルウェア感染アプリ、古い脆弱性やパーミッションを悪用　http://www.itmedia.co.jp/enterprise/articles/1712/01/news070.html〔参照 2018-05-28〕
トレンドマイクロ株式会社：偽の画面を被せて不正を行うアプリ「TOASTAMIGO」、Google Play で新たに確認　https://www.is702.jp/news/2241/partner/200_k/〔参照 2018-05-28〕

第2章
情報セキュリティを支える基盤の動向

2017 年度は、世界規模のランサムウェア被害や数百億円の仮想通貨流出等、つながることの脅威が顕在化し、社会的に注目されるインシデントがいくつも発生した。国内では、このような深刻化するサイバー攻撃の脅威に立ち向かうべく、産学官が協力して現状に即したガイドラインや関連法規の整備、セキュリティ人材の育成等、国内のセキュリティ基盤の確立等に取り組んだ。

国外では、米国で大統領令が発効し全省庁で対策が見直され、中国では「ネットワーク安全法」が施行された。また EU では GDPR 発効に向けた各国の法整備等、サイバーセキュリティ対策が強化され、特にグローバルにインターネットサービスを提供する企業等に影響を与えている。

本章では、情報セキュリティの取り組みを支える国内、国外の基盤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対策の状況を述べる。

2.1.1 政府全体の政策動向

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」「政府機関等の情報セキュリティ対策のための統一基準群」「重要インフラの情報セキュリティ対策に係る行動計画」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。

本項では、2017 年度に実施された主な取り組みと次期サイバーセキュリティ戦略について述べる。

(1)「サイバーセキュリティ 2017」の策定と実施

2015 年 9 月「サイバーセキュリティ戦略[※1]」が閣議決定され、我が国が取るべき諸施策の目標や実施方針が明示された。「サイバーセキュリティ戦略」の期間は策定後 3 年間とされており、2017 年 8 月に公表された「サイバーセキュリティ 2017[※2]」は、最後の 1 年間の取り組みを示すものである。

(a)「サイバーセキュリティ 2017」の策定

「サイバーセキュリティ戦略」策定後の脅威動向等を踏まえ、加速・強化すべき施策を取りまとめ、急ぎ対策が必要なものから実施するために、NISC は 2017 年 7 月に「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−[※3]」を作成した。中間レビューでは、「サイバー空間ガバナンス」「安全でクリーンなサイバー空間」「多様な関係主体による連携と役割分担」「グローバルな連携」を方針として、段階的に実施することを決定した。

2017 年 8 月 25 日には、「サイバーセキュリティ戦略」に基づき、上記の中間レビュー結果も踏まえ、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 2017」を公表した。

(b) 主な取り組み状況

「サイバーセキュリティ 2017」に基づき実施された取り組みについて以下に述べる。

- 経済社会の活力の向上及び持続的発展

  2016 年は IoT 機器が第三者により悪用され DDoS 攻撃に利用されるという大きなインシデントが発生し、2017 年も脅威が継続している（「3.1.2 国内に広がる感染被害や DDoS 攻撃の脅威」参照）。政府は、安全な IoT システムの創出に向けて、「ボット撲滅」に向

けた官民連携による体制構築、「IoT セキュリティガイドライン※4」の普及、IoT システムのセキュリティに関わる技術開発や実証等を行った。また、企業におけるセキュリティ対策の実現には経営層の参画が引き続き重要であることから、2017 年 11 月に「サイバーセキュリティ経営ガイドライン Ver2.0※5」を発行し、経営層の意識改革を進めた。更に、経営者、事業戦略に基づくサイバーセキュリティの立案や関係者との調整を行う橋渡し人材、サイバーセキュリティを推進する実務者等の、各人材層向けの施策について官民の連携を強化し、「サイバーセキュリティ人材育成プログラム※6」の検討や育成の実施を行った（「2.1.2 (1) サイバーセキュリティ経営ガイドラインの改訂」「2.4.1 (1) 状況の変化を踏まえた新たな取り組み」参照）。

- 国民が安全で安心して暮らせる社会の実現
  内閣官房及び重要インフラ所管省庁等は、「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※7」に示されている、安全かつ持続的なサービス提供に努める、という機能保証の考え方に基づき、先進的取り組みの推進、2020 年東京オリンピック・パラリンピック競技大会を見据えた情報共有体制の強化、リスクマネジメントを踏まえた CSIRT 等の対処体制整備の推進を行った。例えば国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology：NICT）は、東京オリンピック・パラリンピック競技大会に向けた攻防戦型サイバー演習「サイバーコロッセオ」を開発し、2018 年 2 月に中級コース、3 月に準上級コースを実施した※8。政府内部のセキュリティ人材の充実については、「政府機関におけるセキュリティ・IT 人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT 人材確保・育成計画」に従い、各府省庁で体制の整備、有為な人材の確保、一定の専門性を有する人材の育成等を実施した※9。また、「橋渡し人材のスキル認定の基本的な考え方」（2017 年 9 月 5 日サイバーセキュリティ対策推進専任審議官等会議・各府省情報化専任審議官等会議合同会議決定）に基づき、橋渡し人材のスキル認定を行うための全府省庁共通の基準を定めた※10。今後各府省庁において、個々の職員の業務経験や情報システム統一研修の修了判定等を受けて認定を実施する予定である。
- 国際社会の平和・安定及び我が国の安全保障
  2017 年 10 月に「サイバーセキュリティ国際キャンペーン」月間の活動として、日・ASEAN 各国のサイバーセキュリティを取り巻く状況について各国の識者が執筆する「ウィークリーコラム」の発信や、「ネットワークビギナーのための情報セキュリティハンドブック※11」の英訳版公開等、外国人にも役に立つ情報を発信した。また、関係省庁で日・ASEAN 共同サイバーセキュリティ意識啓発活動を実施した（「2.3.1 (5) ASEAN とのサイバー連携協議」参照）。

また、上記三つの政策分野を支える府省庁横断的施策として、研究開発の推進と人材の育成・確保の取り組みを実施した。

- 研究開発の推進
  研究開発戦略専門調査会は、これまでのサイバーセキュリティに関わる研究開発の進捗と、IT 利活用の広がりやサイバー攻撃の脅威の深刻化といった環境の変化を踏まえて、2017 年 7 月「サイバーセキュリティ研究開発戦略※12」を策定し、近い将来及び中長期を見据えたサイバーセキュリティ研究開発の方向性について示した。
  また、内閣府は、「戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保」と連携し、真贋判定技術（機器やソフトウェアの真正性・完全性を確認する技術）を含めた動作監視・解析技術と防御技術の研究開発を行った※13。
- 人材の育成・確保
  「サイバーセキュリティ人材育成プログラム」等を踏まえ、NISC はサイバーセキュリティと経営の問題等を含むサイバーセキュリティ人材育成に関する方向性について議論を行い、検討結果を報告書（案）として取りまとめた※14。また、関係省庁・独立行政法人は、以下のような事業を行った。
  - 突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保を目指した「セキュリティ・キャンプ事業」
  - 人材が将来にわたって活躍し続けるための環境整備のための情報処理安全確保支援士制度の普及事業
  - 「ナショナルサイバートレーニングセンター」での若年層の ICT 人材を対象とした「若手セキュリティイノベーター育成事業『SecHack365』※15」
  - 国の行政機関、地方公共団体、重要インフラ等を対象とする実践的なサイバー防御演習「CYDER（CYber Defense Exercise with Recurrence）※16」

なお、情報処理安全確保支援士については「2.4.2 情報セキュリティ人材育成のための資格制度」、セキュリティ・キャンプ事業については「2.4.3 情報セキュリティ人材育成のための活動」を参照されたい。

(2) 重要インフラの情報セキュリティ対策強化

2017 年 4 月 18 日、サイバーセキュリティ戦略本部は、重要インフラをサイバー攻撃から防護することを目的とする「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」(以下、行動計画)を決定した。機能保証の観点から、保護対象として IT 障害に加え「サービス障害」が追記された。また「経営層の積極的な関与」のもと、これらの障害の発生を低減させ、迅速な復旧へ取り組むことが明記された。同行動計画に基づき、NISC は「安全基準等の整備及び浸透」「情報共有体制の強化」「障害対応体制の強化」「リスクマネジメント及び対処態勢の整備」「防護基盤の強化」の五つの施策を進めている。2017 年度に実施された主な活動について述べる。

(a)「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂

2018 年 4 月に「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針 (第 5 版)※17」を公表した。本指針は、各重要インフラ事業者等が情報セキュリティ対策の基準等を規定する際に、含めることが望まれる項目を整理したもので、今回の改訂では、行動計画の内容を反映している。

NISC では、本指針に従い、重要インフラ所管省庁や業界団体等が整備した情報セキュリティ対策の基準等が継続的に改善されているか、重要インフラ事業者等に浸透しているかをアンケート及びインタビューにより確認し、重要インフラ専門調査会※18 で毎年報告している。

(b)リスクアセスメントの強化

機能保証の考え方に立脚したリスクアセスメントの浸透を図るため、NISC は 2018 年 4 月、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書 (第 1 版)※19」(以下、リスクアセスメント手引書)を公表した。リスクアセスメント手引書は、2016 年 9 月に NISC から 2020 年東京オリンピック・パラリンピック競技大会の関係事業者に提供された「機能保証のためのリスクアセスメント・ガイドライン※20」(以下、オリパラ向けガイドライン) をベースに、重要インフラ事業者等における一般的なリスクアセスメントに活用できるよう見直したものである。

オリパラ向けガイドラインは、大会運営の成功に求められる事項を勘案して重要なサービスを選定し、大会期間中のサービスをいかに継続するかという点に着目している。一方、リスクアセスメント手引書は、重要インフラ事業者等の役割を総合的に勘案して優先するサービスを選定し、自組織の活動目標を踏まえてサービスを継続する点に着目している。

なお、東京オリンピック・パラリンピック競技大会に向けた第 2 回リスクアセスメントは、オリパラ向けガイドラインの手順に従い、2017 年度第 2 四半期に、東京圏(1 都 3 県) における重要サービス 20 分野を対象に実施された。大会開催までに合計 6 回のリスクアセスメントが計画されている※21。

(c)「分野横断的演習」の実施

NISC は、重要インフラ分野におけるサービス障害への対応能力の維持・向上を目的に、重要インフラ 13 分野の事業者等を対象とした「分野横断的演習」を 12 月に実施した。「『機能保証』や『サービス維持レベル』を踏まえた演習シナリオ」「組織横断的な情報伝達の有効性検証」「プレーヤーのインシデント対応状況評価」「オリパラ大会を見据えた情報共有体制の確認 (一部事業者のみ)」等、新たな取り組みも行い、参加者は過去最大の 2,647 名となった。また、2018 年 1 月に演習参加者の意見交換会を行い、他の参加事業者等と気づきや取り組み状況の共有、及び平素より情報交換が行える関係性の構築を支援した※22。

(d)「セプター訓練」の実施

重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織である「セプター」(Capability for Engineering of Protection, Technical Operation, Analysis and Response：CEPTOAR) は、セプターカウンシル総会第 10 回会合において医療 CEPTOAR の入会が認められ、13 分野 18 セプターとなった※23。

2017 年度のセプター訓練は行動計画に従い、各分野の特性を生かした模擬情報 (シナリオ) のカスタマイズ化、事前通告なしの抜き打ち訓練等で実施し、全セプターで 2,106 名が参加した※24。

(e)「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(試案)」策定

2018 年 4 月 11 日、「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準 (試案)」(以下、評

価基準）の意見募集が行われた※25。

本評価基準は、サイバー攻撃によりシステムの不具合が発生し、それが重要インフラサービス障害にまで至ってしまった場合に、その障害が社会に与えた影響の深刻さを表すものである。今回公表された評価基準は、第1段階として、発生したサービス障害の影響全体の深刻さを事後に評価するための試案である。

NISCは、この評価基準を用いて深刻度を評価・公表することにより、関係主体が共通の理解で冷静かつ適切な対応をとれるようになることを目指している。

(3) 次期サイバーセキュリティ戦略策定に向けた活動

政府は、「科学技術イノベーション総合戦略2017※26」「未来投資戦略2017※27」等で「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社会」（Society 5.0）を目指す方針を決定してきた。サイバーセキュリティ戦略本部は、次期サイバーセキュリティ戦略においても、このような「変革の潮流」を俯瞰しながらサイバーセキュリティの在り方を検討する必要があるとして、「『次期サイバーセキュリティ戦略』の骨子※28」を作成した。

本骨子では、サイバーセキュリティの基本的な在り方として、サイバー空間における安全・安心と経済発展を両立させる枠組みとなる「サイバーセキュリティエコシステム」（仮称）を目指して、「任務保証」「リスクマネジメント」「参加・連携・協働」の観点から、官民のサイバーセキュリティに関する取り組みを推進することを示した。図2-1-1に次期戦略におけるサイバーセキュリティの基本的な在り方のイメージを示す。

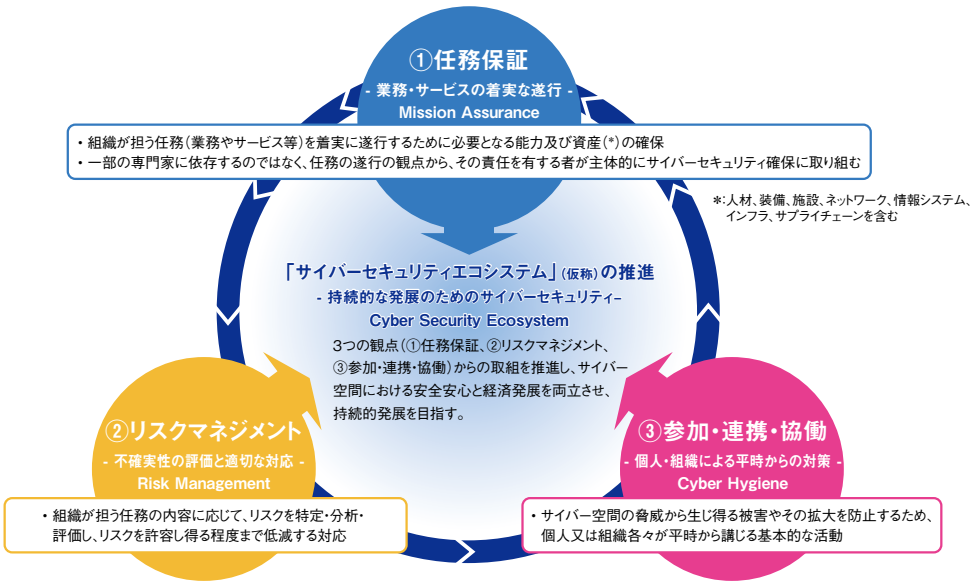
2.1.2 経済産業省の政策

経済産業省は、「サイバーセキュリティ経営ガイドライン」等の各種ガイドラインの普及、サプライチェーン全体にわたるセキュリティ対策フレームワークの検討、重要インフラを守るためのリスク分析や情報共有体制の整備等、様々な施策を実施している。

(1) サイバーセキュリティ経営ガイドラインの改訂

経済産業省とIPAは、2015年12月「サイバーセキュリティ経営ガイドライン」を発行した※29。同ガイドラインは、経営者が認識すべき3原則とCISO等に指示すべき10項目の対策がまとめられている。2016年12月の改訂では「経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である」という表現が明記された※30。経営層のセキュリティ参画の意識は企業でも高まり、同ガイドラインの周知・利用にも進展がみられたことから、2017年7月、経済産業省はIPAと協力して「サイバーセキュリティ経営ガイドライン改訂に関する研究会※31」を発足させ、本ガイドラインの改訂を議論した。その成果として2017年11月、「サイバーセキュリティ経営ガイドライン Ver2.0※32」を発行した。

本改訂では、経営者が認識すべき3原則は維持しつ



■図2-1-1　次期戦略におけるサイバーセキュリティの基本的な在り方のイメージ
（出典）サイバーセキュリティ戦略本部「『次期サイバーセキュリティ戦略』の骨子」を基にIPAが編集

つ、経営者がCISO等に対して指示すべき10の重要項目について見直しを実施した。図2-1-2に概要を示す。

主な改訂内容は以下のとおりである。

- 「指示5 サイバーセキュリティリスクに対応するための仕組みの構築」において、新たに「攻撃の検知」を含めたリスク対応体制について記載
- 「指示8 インシデントによる被害に備えた復旧体制の整備」において、新たに「サイバー攻撃を受けた場合の復旧への備え」について記載
- 「指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」に、サプライチェーンのセキュリティ対策強化に関する記載を追記するとともに類似項目を整理
- 「付録C」の参考情報に、インシデントが発生したときに組織が整理しておくべき事項を新規追加

米国のサイバーセキュリティリスク管理フレームワークであるNIST Cybersecurity Framework[※33]との整合を意識しつつ、攻撃検知、復旧の体制及びサプライチェーン対策に配慮した改訂となっている。後述する産業サイバーセキュリティ研究会のWG活動（「2.1.2(3) 産業サイバーセキュリティ研究会」参照）では、本ガイドラインの普及施策も検討されており、さらなる活用・実践が望まれる。

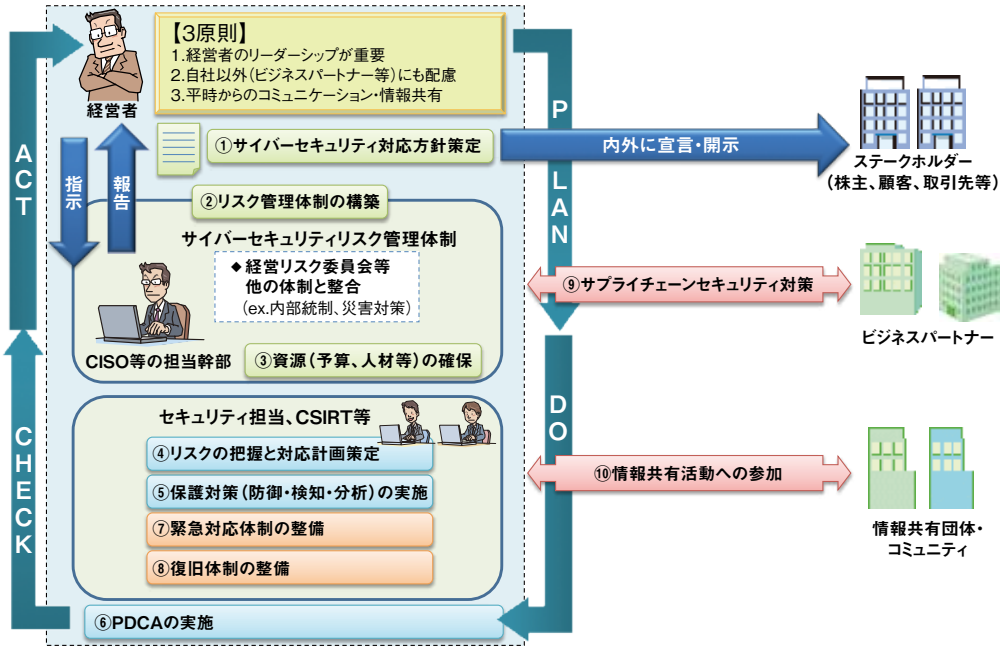
(2) Connected Industriesへの取り組み

2017年3月にドイツで開催された国際情報通信技術見本市（Centrum für Büroautomation, Informationstechnologie und Telekommunikation：CeBIT）に、安倍晋三首相、世耕弘成経済産業大臣他が出席し、目指すべき産業の在り方として「Connected Industries」の概念を提唱した[※34]。「Connected Industries」では、様々なつながりにより新たな付加価値が創出される産業社会は、以下の三つを柱とするとしている。

- 人と機械・システムが対立するのではなく、協調する新しいデジタル社会の実現
- 協力と協働を通じた課題解決
- 人間中心の考えを貫き、デジタル技術の進展に即した人材育成の積極推進

2017年度は、「Connected Industries」実現に向けて産業界の代表や有識者と世耕経済産業大臣との懇談会の開催[※35]や、産学の有識者によるシンポジウム討議[※36]により、政府・産業界の取り組みについて普及推進を図った。このうち2017年10月の第3回シンポジウムは、IoT分野の国内最大展示会であるCEATEC JAPAN 2017の一部として開催し、地域・中小企業の事例や、大手・中堅企業×ベンチャー企業の連携の事例等を取り上げた[※37]。

またCEATEC JAPAN 2017に先立ち開催された「Connected Industries」カンファレンスにおいて、



■図2-1-2　ガイドラインの3原則と重要10項目の概要
（出典）IPA「サイバーセキュリティ経営ガイドライン Ver2.0」

「『Connected Industries』東京イニシアティブ 2017※38」が発表された。これにより「Connected Industries」の考え方やアクションプランとして、五つの重点分野に政策資源を集中投入し、三つの横断的な政策も推進することで、リアルデータを巡るグローバルな競争の中での我が国の「勝ち筋」を実現することが示された。

【五つの重点取組分野】

- 自動走行・モビリティサービス
- ものづくり・ロボティクス
- バイオ・素材
- プラント・インフラ保安
- スマートライフ

【三つの横断的な政策】

- リアルデータの共有・利活用
- データ活用に向けた基盤整備
  研究開発、人材育成、サイバーセキュリティ
- さらなる展開
  国際、ベンチャー、地域・中小企業

重点取組分野にはそれぞれ推進主体（分科会）となる業界団体や推進組織があり、活動が始まっている※39。各分科会のサイバーセキュリティやデータ協調に関する検討の論点を紹介する。

①自動走行・モビリティサービス（推進主体　自動走行ビジネス検討会）

- 地図データ、国が収集した走行映像データの活用、共有データの最大化の検討
- サイバーセキュリティインシデントの情報共有体制構築（一般社団法人日本自動車工業会に構築済み）。評価環境（テストベッド）の整備（2019 年度末まで）

②ものづくり・ロボティクス（推進主体　ロボット革命イニシアティブ協議会（Robot Revolution Initiative：RRI））

- データ契約ガイドライン（2017 年 5 月発行）の検証・改訂。業界全体で共有できるデータ等の検討
- サイバーセキュリティの製造業向けガイドラインの作成検討、国際標準化の推進

③バイオ・素材（推進主体　産業競争力懇談会（Council on Competitiveness-Nippon：COCN）、一般社団法人日本化学工業協会）

- 産学官連携によるデータプラットフォームの構築。協調領域の設定
- サプライチェーン全体におけるデータの連携の在り方の検討

④プラント・インフラ保安（推進主体　プラントデータ活用促進会議）

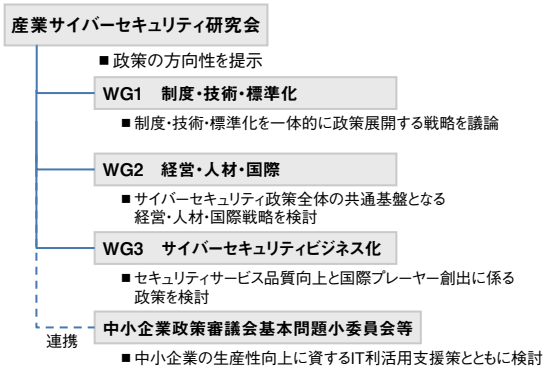
- 分野特化の秘密保持契約の締結等のためのガイドライン作成
- 分野特化のサイバーセキュリティガイドライン作成

⑤スマートライフ（推進主体　IoT 推進ラボ）

- スマートホーム市場の拡大に向けた共通ルールの検討
- スマートライフ分野のセキュリティ等に関わるガイドラインの作成検討

(3) 産業サイバーセキュリティ研究会

2017 年 12 月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」（以下、研究会）を設置した※40。同研究会は、サイバーセキュリティ政策を総合的に検討するため、三つのテーマに関するワーキンググループ（以下、WG）を設置し、中小企業政策審議会等とも連携をとる。図 2-1-3 に研究会の構成を示す。



■図 2-1-3　産業サイバーセキュリティ研究会の構成
（出典）経済産業省「産業分野におけるサイバーセキュリティ政策※41」

各 WG の概要と活動状況は以下のとおりである。

(a) WG1　制度・技術・標準化

WG1 では、産業サイバーセキュリティに関する「制度・技術・標準化を一体的に政策展開する戦略」を議論する。また IoT の進展を踏まえ、製造から供給に至るサプライチェーンごとの対策強化を図る。

このためにまず、WG1 で業界横断的な対策の枠組みの標準モデルを作成し、これに業界ごとに設置するサブワーキンググループ（以下、SWG）で検討される業界固有の要件や対策を加味して、その業界に適用される

セキュリティポリシーとする。策定されたセキュリティポリシーは、グローバルビジネスで認められるように標準化・認証機関やセキュリティ技術開発プロジェクト等と連携し、米欧等の主要な認証制度との相互承認等を提案する、としている。最初のSWGとして、2018年2月にビルSWGが活動を開始した。

WG1で検討されている標準モデルは、2018年4月に「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」として公表された（2018年5月28日までパブリックコメント募集）[※42]。

「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」では、価値創造の活動が営まれる産業社会を、以下の3層構造と六つの構成要素（組織、ヒト、モノ、データ、プロシージャ、システム）でとらえ、包括的にセキュリティ対策のポイントを整理し、それらに対応するための指針を示している。

第1層－ 企業間のつながり（従来型サプライチェーン）
第2層－ フィジカル空間とサイバー空間のつながり
第3層－ サイバー空間におけるつながり

(b) WG2　経営・人材・国際

WG2は「サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略」を検討する。

具体的には経営者の意識喚起と多様なサイバーセキュリティ人材の育成、更に国際協力基盤の整備に関する施策の検討を行う。2018年3月に第1回WGが開催され、WGの活動の方向性について確認された。

このうち経営者の意識喚起、セキュリティへの参画については、改訂された「サイバーセキュリティ経営ガイドライン」の実践をより容易にするためのプラクティス集作成、及び企業におけるセキュリティ対策が実際にどこまで実践できているかの実施状況可視化、を重点項目として進めようとしている。具体的な活動はIPAとの協力により行われる予定である。

(c) WG3　サイバーセキュリティビジネス化

WG3では、「セキュリティサービス品質向上と国際プレーヤー創出に係る政策」を検討する。

経済産業省は、2017年2～6月の間に「セキュリティ産業のビジネス化研究会」を開催し、セキュリティ産業の現状の整理と今後実施するべき政策を取りまとめた[※43]。同研究会の議論は政府調達の拡充や税制の検討等、出口政策が中心となったが、WG3はこの結果を受け、何を強化してビジネスの拡大を図るか、という供給する側の対策の検討に重点を置く予定である。2018年4月に第1回WGが開催され、「IoT（主に自動車）セキュリティ」「制御系セキュリティ」「尖った人材・技術の発掘・創出」をテーマとして活動していくことが確認された。

(4)「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」の策定

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「セキュリティサービス審査登録制度に関する検討会」を開催し、「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018年2月に公表した[※44]。本基準は、情報セキュリティサービスについて一定の品質の維持向上が図られているかどうかを第三者が客観的に判断し、結果を公開することで、利用者が必要なセキュリティサービスを容易に選定できるようにする枠組みである。

- 情報セキュリティサービス基準
  「情報セキュリティ監査サービス」「脆弱性診断サービス」「デジタルフォレンジックサービス」及び「セキュリティ監視・運用サービス」を対象とし、それぞれのサービスについて、必要な資格や仕様の明示等の技術要件、及び品質管理者の割当状況、品質管理マニュアルの整備、品質の維持・向上に関する手続き等の導入状況等の品質管理要件を、基準として定めている。
- 情報セキュリティサービスに関する審査登録機関基準
  民間企業が提供する情報セキュリティサービスの上記サービス基準への適合性について、審査及び登録を行う機関（以下、審査登録機関）に求められる事項として、審査登録機関が備えるべき公平性や、組織管理及び審査手続きにおける通則的事項を定めている。

今後、情報セキュリティサービス事業者は、情報セキュリティサービス基準に基づき技術要件、品質管理要件を整理し、一定の基準が満たされているかどうかを確認することにより、自らの組織の状況を把握し、不十分な部分を改善することができる。情報セキュリティサービスの利用者も、公開された情報を基に、要求に合った情報サービス事業者を選定できるようになることが期待される。

(5) 総務省との連携

経済産業省と総務省は2017年3月から局長級による連携チームを発足[※45]し、IoT関連の様々なテーマにつ

いて検討を行ってきたが、2018 年 5 月、同連携チームの検討成果が報告された※46。同報告から、2017 年度の新たな取り組みや制度について述べる。

- 「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)創設
  経済産業省と総務省が共同で税制改正要望を行い、「平成 30 年度税制改正の大綱」(平成 29 年 12 月 22 日閣議決定)において、一定のサイバーセキュリティ対策を講じながら行う IoT 投資に対して、優遇措置を講じる「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)が平成 30 年度に創設されることとなった※47。
- 「『情報銀行』の認定に係る指針 ver1.0(案)」の取りまとめ
  いわゆる「情報銀行」に求められる情報信託機能に関し、民間団体等による任意の認定制度の在り方を検討する目的で、2017 年 11 月に「情報信託機能の認定スキームの在り方に関する検討会」を発足し、2018 年 5 月に「『情報銀行』の認定に係る指針 ver1.0(案)」をまとめた(2018 年 5 月末まで意見募集※48)。同指針は、「情報銀行」の認定団体が制度の構築・運用に用いることを意図し、認定基準、モデル約款の記載事項、認定スキームを示している。
- 「IoT 推進コンソーシアム」での活動
  経済産業省と総務省が共同事務局を担当している「IoT 推進コンソーシアム IoT セキュリティワーキンググループ」を2017 年 12 月に開催し※49、「IoT セキュリティガイドライン ver1.0」の普及啓発や、IoT 機器のセキュリティに関する認証制度等のセキュリティ確保策について検討した。また、「IoT 推進コンソーシアム データ流通促進ワーキンググループ」のもとに設置した「カメラ画像利活用サブワーキンググループ」の活動成果である「カメラ画像利活用ガイドブック」を改訂し、ver2.0 を 2018 年 3 月に発行した※50。

2018 年度も経済産業省と総務省との連携チームは継続して検討を行い、IT 総合戦略本部等とも連携しつつ、検討結果の施策への反映を目指すとしている。

(6) J-CSIP(サイバー情報共有イニシアティブ)

経済産業省の協力のもと、IPA では 2011 年 10 月より、官民連携による標的型攻撃への対策を目的として、J-CSIP (Initiative for Cyber Security Information Sharing Partnership of Japan:サイバー情報共有イニシアティブ)を運用している。

J-CSIP は、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2018 年 3 月末日現在、IPA を情報の中継・集約点(情報ハブ)として 11 の領域(SIG※51)から 228 の企業や業界団体が J-CSIP に参加している(次ページ図 2-1-4)。2017 年 9 月には、「航空業界 SIG」「物流業界 SIG」「鉄道業界 SIG」が新たに発足した。また、2017 年 6 月、電力業界 SIG で組織改編が行われ、2017 年 3 月に設立された「電力 ISAC」及びその会員等が J-CSIP に参加した。これにより電力業界 SIG は、11 組織から 30 組織に拡大した。他の SIG も参加組織が増え、2017 年度は参加業界数、参加組織数ともに大幅増加となった。

J-CSIP は IPA を通じて、経済産業省やセプターカウンシルの C4TAP※52、一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)とも連携している。J-CSIP では、IPA と参加組織との間で秘密保持契約を締結し、主に標的型攻撃メールに関する情報共有を行っている。なお、J-CSIP の中で共有される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

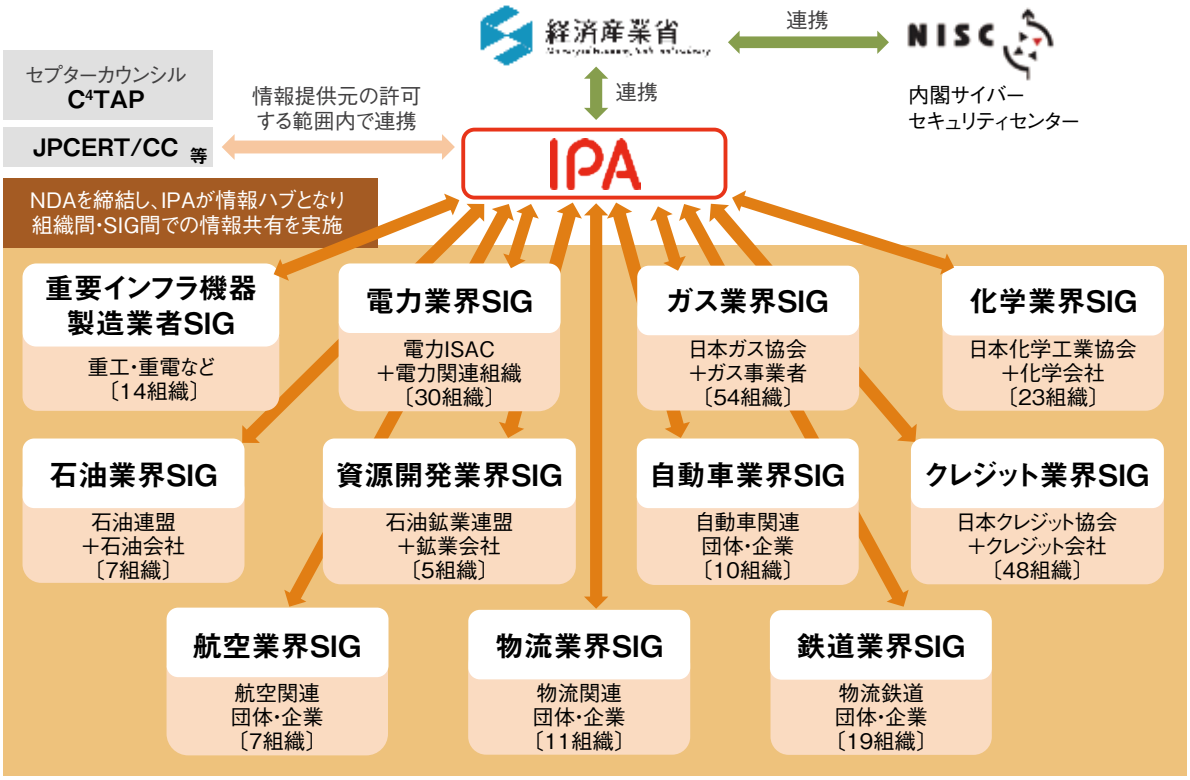
参加組織からの情報提供件数、提供を受けた情報のうち標的型攻撃メールと見なした件数(攻撃メール件数)、及びそれらを基に J-CSIP 内で情報共有を行った件数(情報共有件数)を表 2-1-1 に示す。

	2014 年度	2015 年度	2016 年度	2017 年度
参加組織からの情報提供件数	626	1,092	2,505	3,456
攻撃メール件数	505	97	177	274
情報共有件数	195	133	96	242

■表 2-1-1　J-CSIP の運用実績

2017 年度は、J-CSIP 運用開始以来、最も多くの情報提供があった。最大の要因は、2015 年 10 月ごろから国内で多く観測されるようになった「日本語のばらまき型メール」が 2017 年度も多く発生し、それらが提供されたことである(「1.2.5 (3) インターネットバンキングを狙った攻撃による金銭被害」参照)。

もう一つの要因は、2017 年 10 月ごろから観測している、プラント関連事業者を狙う英文の攻撃メールである。一連の攻撃メールの内容は常に変化を続けており、継続して多数の情報提供を受けている。特定の宛先に対して執拗に攻撃が行われている傾向があるため、これらの



■図 2-1-4　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 1 月～ 3 月］[※53]」

メールは標的型攻撃として取り扱っている。

一方、2016 年度まで観測されてきたような、日本国内の特定の業界や組織を狙う標的型攻撃メールは、J-CSIP 参加組織の中での提供件数は減少傾向にある。ただし、日本国内全体では攻撃が発生しており、IPA で入手した攻撃情報を共有したところ、同じ攻撃の痕跡（例えば同等の標的型攻撃メールの着信）が確認された事例がある。国内への標的型攻撃は依然として継続している状況であり、引き続き注意が必要である。

(7) J-CRAT（サイバーレスキュー隊）

経済産業省の協力のもと、IPA は 2014 年 7 月に J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）を発足させた。J-CRAT の目的を以下に示す。

- 攻撃に気付いた組織に対する被害拡大と再発の抑止・低減
- 標的型攻撃による諜報活動等の連鎖の遮断

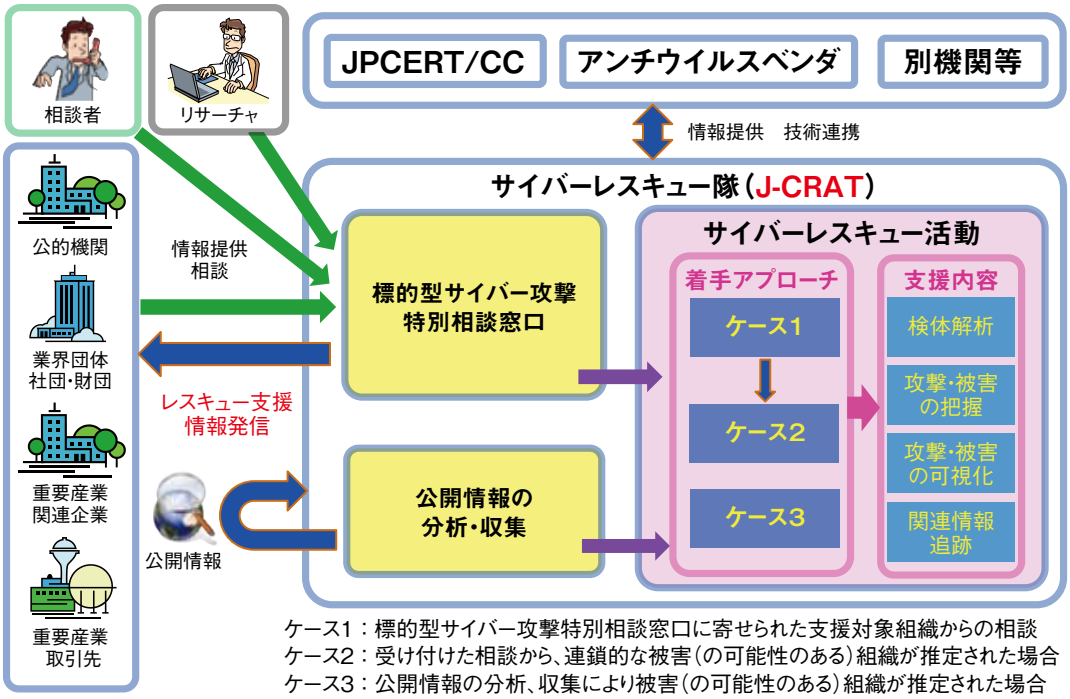
J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

窓口では、主に公的機関等の組織から、標的型攻撃メールに関する情報提供や相談を受け付けている。「公開情報の分析・収集」では、日々公開されるインターネット上の情報から、各種ウイルス[※54]情報を収集している。これまでの活動実績から、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになったため、それらの情報収集を幅広く行っている。

標的型サイバー攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応における助言を「サイバーレスキュー活動」として実施している[※55]。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、民間セキュリティ事業者への移行を前提とした助言を行っている（図 2-1-5）。

緊急を要する事案に対しては、「レスキュー支援」を行い、当該組織での対応が必要な場合は、隊員を派遣する「オンサイト支援」を行っている。それぞれの支援件数を表 2-1-2 に示す。

2017 年度の活動実績を 2016 年度と比較すると、相



■図 2-1-5　J-CRAT の活動の全体像とスキーム

	2014 年度	2015 年度	2016 年度	2017 年度
相談件数	107 件	537 件	519 件	412 件
レスキュー支援数	38 件	160 件	123 件	144 件
オンサイト支援数	11 件※	39 件	17 件	27 件

※一つの事案に対して複数回のオンサイト対応を要した場合も、1 件として集計

■表 2-1-2　J-CRAT での活動実績

談件数は減少しているが、支援件数は増加している。

J-CRAT は、活動の成果を分析レポート、及び技術レポートにまとめ公開している。「サイバーレスキュー隊（J-CRAT）技術レポート 2017※56」では、J-CRAT のレスキュー活動で実際に行っている初動対応の一部である「Windows OS 標準ツールで感染を見つける」方法を解説している。組織のシステム管理者やセキュリティ担当者が、インシデント発生時の対応や次のアクションへ進むための判断材料として、このような調査を選択できることを目標としており、手順や解説だけでなく、標的型攻撃における調査の全体像が分かる早見表やコマンドの実行例等を記載している。

J-CRAT では、これらの取り組みを通じ、被害組織におけるセキュリティインシデントに対する速やかな対応力向上や、平時における標的型攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、標的型サイバー攻撃の連鎖の解明と、攻撃の連鎖を遮断することによる被害の低減を推進していく。

2.1.3 総務省の政策

総務省は、IoT 時代に対応したサイバーセキュリティを確保するために、インターネットや公衆無線 LAN 等の通信基盤の安心・安全な利用環境の実現を目指した施策を講じている。

(1) サイバーセキュリティタスクフォース

総務省が公開した「IoT サイバーセキュリティアクションプログラム 2017※57」に基づき、IoT ／ AI 時代のサイバーセキュリティに関する基盤・制度、人材育成、国際連携の在り方等、包括的な政策の推進を目指し、2017 年 1 月にサイバーセキュリティタスクフォース※58 が発足した。

(a) IoT セキュリティ総合対策

IoT 時代のサイバーセキュリティは、安心・安全な国民生活や社会経済活動の確保の観点から重要な課題となっている。特に、IoT 機器を狙ったサイバー攻撃は年々増加傾向にあり、国際的にも攻撃された IoT 機器による深刻な被害が発生している。このような状況から早急な IoT セキュリティ対策の取り組みの必要性があるとし

て、サイバーセキュリティタスクフォースは 2017 年 4 月に「IoT セキュリティ対策に関する提言※59」を取りまとめた。

この提言の問題意識を踏まえ、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するものとして、2017 年 10 月、「IoT セキュリティ総合対策※60」(以下、総合対策)を策定した。

総合対策では、表 2-1-3 の五つの施策群において具体的な施策を示している。

施策群	具体的施策
(1) 脆弱性対策に係る体制の整備	①セキュリティ・バイ・デザイン等の意識啓発・支援の実施
	②認証マークの付与及び比較サイト等を通じた推奨
	③ IoT セキュアゲートウェイ
	④セキュリティ検査の仕組み作り
	⑤簡易な脆弱性チェックソフトの開発等
	⑥利用者に対する意識啓発の実施や相談窓口等の設置
	⑦重要 IoT 機器に係る脆弱性調査
	⑧サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査
	⑨被害拡大を防止するための取組の推進
	⑩IoT 機器に関する脆弱性対策に関する実施体制の整備
(2) 研究開発の推進	①基礎的・基盤的な研究開発等の推進
	②広域ネットワークスキャンの軽量化
	③ハードウェア脆弱性への対応
	④スマートシティのセキュリティ対策の強化
	⑤衛星通信におけるセキュリティ技術の研究開発
	⑥AI を活用したサイバー攻撃検知・解析技術の研究開発
(3) 民間企業等における セキュリティ対策の促進	①民間企業のセキュリティ投資等の促進
	②セキュリティ対策に係る情報開示の促進
	③事業者間での情報共有を促進するための仕組みの構築
	④情報共有時の匿名化処理に関する検討
	⑤公衆無線 LAN のサイバーセキュリティ確保に関する検討
(4) 人材育成の強化	①実践的サイバー防御演習（CYDER）の充実
	②2020 年東京大会に向けたサイバー演習の実施
	③若手セキュリティ人材の育成の促進
	④ IoT セキュリティ人材の育成
(5) 国際連携の推進	① ASEAN 各国との連携
	②国際的な ISAC 間連携
	③国際標準化の推進
	④サイバー空間における国際ルールを巡る議論への積極的参画

■表 2-1-3　IoT システムのセキュリティ対策に係る具体的施策
(出典)サイバーセキュリティタスクフォース「IoT セキュリティ総合対策」を基に IPA が作成

(b) 公衆無線 LAN セキュリティ分科会

2017 年 11 月、総合対策を踏まえて、公衆無線 LAN セキュリティ分科会がサイバーセキュリティタスクフォースのもとに設置された※61。

公衆無線 LAN 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て、観光や防災の観点から普及が進んでいる。しかし、公衆無線 LAN サービスの中にはセキュリティ対策が不十分なものもあり、脆弱なサービスを踏み台にした攻撃や情報漏えい等のインシデントが発生する恐れがある。このような背景から、本分科会では、公衆無線 LAN におけるセキュリティの課題と対策について検討を行い、2018 年 3 月に「公衆無線 LAN セキュリティ分科会報告書※62」を策定・公表した。

本報告書は、公衆無線 LAN の利用形態や脅威と対策の状況を踏まえて、セキュリティ対策の在り方や普及策について述べている。また、セキュアな公衆無線 LAN 環境実現に向け、国（総務省）や民間事業者が推進するべき以下の三つの観点の行動計画が示されている。

- 利用者・提供者の意識向上
- データ利活用施策との連携
- 優良事例の普及

東京オリンピック・パラリンピック競技大会に向け、これらの行動計画の実践が望まれる。

(c) 情報開示分科会

2017 年 12 月、総合対策を踏まえて、情報開示分科会がサイバーセキュリティタスクフォースのもとに設置された※63。

企業では複雑化・巧妙化するサイバー攻撃への対策強化の取り組みが進んでいるが、こうした取り組みを更に進めるためには、企業が、市場を含む第三者から適切に評価される仕組みを構築することが求められる。このような背景から、本分科会では、民間企業の情報開示に関する課題を整理し、情報開示の普及に必要な方策を検討した結果を「情報開示分科会報告書(案)※64」として取りまとめた。

(2)「サイバー攻撃(標的型攻撃)対策防御モデルの解説」の公表

総務省は、2013 年度から行っている「サイバー攻撃

対策防御モデル・実践演習の実証実験」事業の成果として、2017年7月、「サイバー攻撃（標的型攻撃）対策防御モデルの解説」を策定・公表した※65。

本解説資料は、巧妙化・複雑化し続けるサイバー攻撃への対策として、官公庁・企業が標的型攻撃に備えるべき防御モデルを推奨している。防御モデルは、「人・組織対策」と「技術的対策」から構成されている。人・組織対策は、インシデントレスポンスに関するプランニングとインシデントハンドリングから成り、インシデント発生の事前計画と計画実行について記載されている。技術的対策では、事前対策、検知、事後対策の三つのフェーズでの実施内容が記載されている。

官公庁・企業が本モデルを参考にして、標的型攻撃への対策を強化し、インシデント発生の低減やインシデントの早期終息につなげることが期待される。

(3)「テレワークセキュリティガイドライン」改版

総務省は、企業等がテレワークを実施する際に、情報セキュリティの不安を払拭し、安心なテレワークを導入・活用するための指針として、「テレワークセキュリティガイドライン」を策定・公表してきた（第1版：2004年12月、第2版：2006年4月、第3版：2013年3月）。

しかし、近年のクラウドサービスやSNSの普及を始めとする社会や技術の変化、また、無線LANの脆弱性やランサムウェア、標的型攻撃等の新たな脅威の出現等を踏まえた改訂が必要となり、2018年4月、「テレワークセキュリティガイドライン（第4版）※66」を策定・公表した。

第3版から改訂された内容としては、経営者とシステム管理者が実施すべき対策として以下の項目が追加されている。

- 経営者が実施すべき対策：
  - 社内で扱う情報を重要度に応じてレベル分けし、利用可否と、利用可の場合の取扱方法を定める。
  - 情報セキュリティ対策に適切な投資として、必要な人材・資源に必要な予算を割り当てる。
- システム管理者が実施すべき対策：
  - 情報セキュリティ保全対策の大枠
    情報のレベルに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否等を設定する。
  - ウイルスに対する対策
    ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する。
  - 重要情報の盗聴に対する対策
    端末で無線LANの脆弱性対策が適切に講じられるようにする。
  - 外部サービスの利用に対する対策
    メッセージングアプリケーションを含むSNSに関する従業員向けの利用ルールやガイドラインを整備し利用上の留意事項を明示する。
    ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用方法を禁止する。

本ガイドラインの活用により、安全なテレワーク環境の普及と、テレワークの拡大が期待される（テレワークの現状については「2.9.2（1）新しい営業秘密保護の課題」参照）。

(4) 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改正に関する政策

総務省は、サイバー攻撃の深刻化や、固定電話サービスのIP網への移行等の社会動向に対応するため、電気通信事業法の一部を改正する法案を策定した。この法案に伴い、NICTの業務にIoTセキュリティを確保する業務を追加するため、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案を策定した。

これらの法案は、第196回通常国会で可決成立し、2018年5月23日に法律第24号として公布された。

(a) 電気通信事業法改正のポイント

電気通信事業法改正のポイントは以下のとおりである※67。

- サイバー攻撃に対する通信事業者の対処の促進
  IoT機器等を悪用したサイバー攻撃等によるインターネット障害の深刻化に対し、サイバー攻撃の送信元となるウイルス感染機器等の情報を共有するための制度を整備する。これにより、通信事業者による利用者への注意喚起や、ウイルスに感染した端末・IoT機器等を遠隔制御するC&Cサーバとの通信を通信事業者がブロックすることが可能になり、大規模なサイバー攻撃等を効果的に防御できる。
- 電気通信番号に関する制度整備
  モバイル化・IoT化に伴う番号ニーズの増大による番号の逼迫や、IP網移行に対応したすべての通信事業者による番号管理の必要性に対応するため、番号の公平・効率的な使用と電話サービスの円滑な提供

を期し、使用条件を付して通信事業者に番号を割り当てるための制度を整備する。

- 電気通信業務等の休廃止に関わる利用者保護
  IP 網移行や通信設備の更改等により、INS ネット等、利用者への影響が大きい業務等の終了が予定されていることを背景として、通信事業者が業務の休廃止に伴い行う利用者周知について、行政があらかじめ確認するための制度を整備する。

(b) 国立研究開発法人情報通信研究機構法改正のポイント

IoT 機器の急激な増加に伴い、IoT 機器を踏み台とするサイバー攻撃の脅威が顕在化し、その対策が必要となっている。特に、パスワード設定に不備のある IoT 機器が多く存在しているという問題があり、その実態を把握し、対策につなげていく必要がある。このような状況を踏まえ、NICT の業務に「パスワード設定に不備のある IoT 機器の調査」等を追加（5 年間の時限措置）する。本改正により、インターネット上の機器調査でパスワード設定に不備のある IoT 機器の IP アドレスを特定し、通信事業者と連携して当該機器の利用者に設定変更を促す注意喚起を行う等の対策の実施が可能となる（図 2-1-6）。

2.1.4 警察におけるサイバー犯罪対策

2017 年度における警察の主な取り組みと、サイバー犯罪の検挙状況等について述べる。

(1) 警察における主な取り組み

2017 年度における警察の主な取り組みについて述べる。

(a) 組織基盤の強化

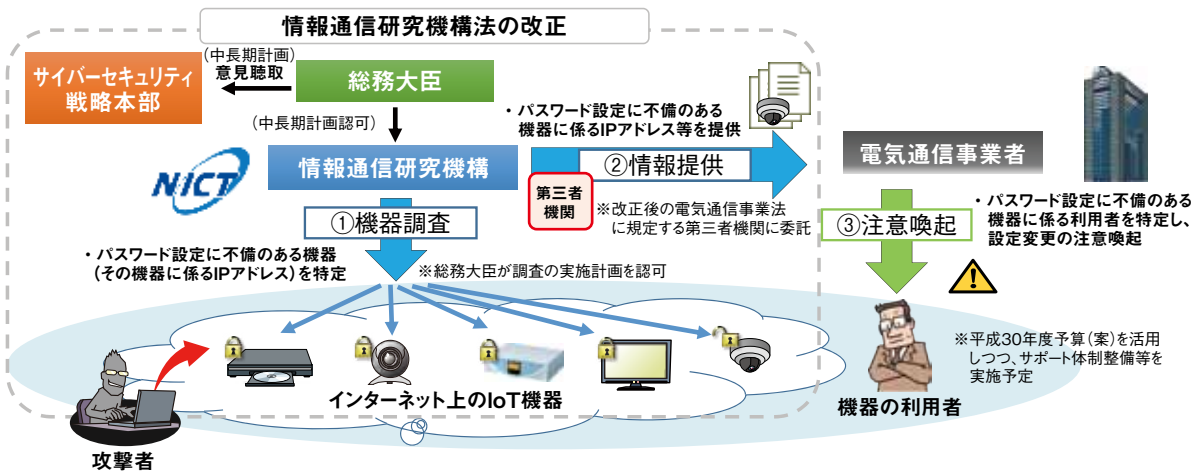
2013 年 4 月、管区警察局所在県を中心とする 13 都道府県警察の公安部または警備部に、サイバー攻撃特別捜査隊が配置された※68。サイバー攻撃に関わる情報収集や捜査活動、民間事業者等との連携によるサイバー攻撃の未然防止対策等が実施されている。

警視庁は、2017 年 4 月、特別捜査隊の人員を約 100 名に増員し、新たに「サイバー攻撃対策センター」に改組した。これにより、2020 年の東京オリンピック・パラリンピック競技大会に向け、政府機関やライフライン事業者に対するサイバー攻撃への対策強化を図る旨を発表した※69。

更に、警視庁は 2018 年 4 月、同センター、サイバー犯罪対策課及び捜査 1 課等、各部に分散するサイバー関連部署を集約することを発表した。約 500 名の捜査員によって構成され、初動捜査から解析等まで、部門横断的に連携した捜査活動が行われる※70。

(b) 情報収集・発信機能の強化

サイバー空間における情報収集等の観点から、重要な役割を果たしているのが、警察庁に設置されたサイバーフォースセンターである。同センターでは、リアルタイム検知ネットワークシステムによるインターネット観測を 24 時間体制で行っている。サイバー攻撃の予兆や実態を把握するとともに、関係情報を公開し、注意喚起する等の任務を遂行している。また、全国都道府県警察が実



■図 2-1-6　国立研究開発法人情報通信研究機構法の一部改正案
（出典）総務省「国立研究開発法人情報通信研究機構法の一部改正案について※67」を基に IPA が編集

施するサイバーテロ対策を技術的に支援している※71。

同センターは、2017年度、認証機能の弱いネットワークカメラ等※72のIoT機器を標的とした探索行為の検知、ランサムウェア「Wanna Cryptor」（別名 WannaCry）またはその亜種に感染したパソコンからの感染活動と見られるアクセスの観測等を行い、注意喚起も行っている※73。

また、警察庁は2017年6月、ポータルサイト「サイバーポリスエージェンシー※74」を開設した。同サイトにおいては、サイバーフォースセンターによる観測状況だけでなく、各都道府県警察におけるサイバー犯罪対策等の情報が発信されている。

(c) 不正送金対策

一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center:JC3）は、2017年3月より、インターネットバンキングウイルス「DreamBot」感染防止に向けた注意喚起等を実施している※75。

警察庁及び警視庁サイバー犯罪対策課は、JC3と連携し、DreamBot感染被害に関する情報交換を行う等、不正送金被害の低減に向けた活動を進めた。このような連携活動の中、警視庁は、2017年10月、DreamBotにより不正送金された現金を引き出したとして、「出し子」のまとめ役であった男を逮捕した※76。

また、2017年3月、JPCERT/CCは、インターネットバンキングにおける不正送金被害を防止するための国際的な取り組みへの協力として、警察庁に対し感染端末情報の提供を開始した※77。警察庁では、これらの情報を基に、インターネットバンキング利用者等に対して注意喚起等を行っている（インターネットバンキング被害に関しては「1.2.5 (3) インターネットバンキングを狙った攻撃による金銭被害」参照）。

(d) 悪質 EC サイト対策

一般社団法人セーファーインターネット協会（Safer Internet Association：SIA）は、2017年12月、「悪質EC サイトホットライン」を開設した。同サイトでは、悪質EC サイトにより代金を騙し取られる等の被害を受けた消費者からの通報を受け付けている※78。通報された情報はJC3と共有し、被害防止施策に活用される。

こうした中、神奈川県を始めとする20都道府県警察は、JC3からの情報に基づき、詐欺サイトに記載された代金振込先口座の名義人である日本人及び中国人の男女43人を、犯罪収益移転防止法違反（口座の有償譲渡）等の疑いで逮捕した※79（詐欺被害に関しては「1.2.5 (2) 偽警告・偽サイト等の詐欺による金銭被害」参照）。

(e) コミュニティサイト等に起因する犯罪対策

警察庁の発表によれば、2017年度上半期におけるコミュニティサイト等に起因する犯罪の被害児童数は919人に上り、過去最多となった※80。

2017年10月、神奈川県座間市内において、複数の男女を殺害した疑いがあるとして、男が逮捕された（座間事件）。容疑者は、Twitterを介し、自殺願望があった被害者らと知り合い、被害者の中には未成年者もいたとされる※81。本件は、被害者数が9名にも及ぶ重大事件であり、現在のSNS普及状況から、模倣犯による新たな被害が発生し得る危険性も認められた。2017年11月、再発防止のための閣僚会議が開催される等※82、社会に重大な影響を与えた。

2017年7月、コミュニティサイト及びアプリ運営等を行うネット事業者は、コミュニティサイトに起因する児童被害防止や、児童が安全に利用できるインターネット環境の向上を目指し、「青少年ネット利用環境整備協議会」を発足させた※83。同協議会は同年12月、座間事件を受け、SNS利用規約に自殺の勧誘禁止を明記し、自殺関連情報に的確に対応するための指針作成や、警察との連携強化を図る旨の提言を発表した※84。警察庁も同月、同協議会等と連携し、緊急性の高い自殺予告事案の認知、発信者の特定、人命救助等に取り組むべく、再発防止策を公表した※85。

青森県警察では、2017年、八戸学院大学の学生15人、青森公立大学の学生14人、弘前大学の学生15人に「サイバー防犯ボランティア」を委嘱する等、自殺予告等のネット上の有害情報の発見、犯罪被害防止の啓発活動への協力体制が構築されている※86。これらの取り組みは各都道府県警察でも継続的に行われている。

今後も、官民一体となって、コミュニティサイト等に起因する犯罪から未成年者等を守っていく必要がある。

(2) サイバー犯罪の検挙状況

2017年における、サイバー犯罪の検挙状況について述べる。

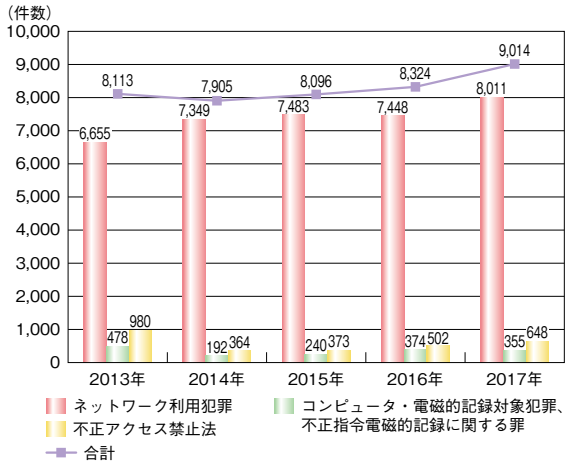
(a) サイバー犯罪検挙件数

警察庁によれば、2017年のサイバー犯罪検挙件数は9,014件であり、引き続き増加している（次ページ図2-1-7）。

インターネットバンキングに関する不正送金事案による

被害は、発生件数 425 件と、ピーク時の 2014 年と比較して 4 分の 1 以下に減少し、被害額は約 10 億 8,100 万円と、ピーク時の 2015 年と比較して約 3 分の 1 に減少した。金融機関によるモニタリングの強化、ワンタイムパスワードの導入等の対策により、被害が大幅に減少したとされる。

他方、インターネットバンキングに不正アクセスし、電子決済サービスを使用して、あらかじめ用意した仮想通貨交換業者のアカウントの円口座に、仮想通貨の購入資金として不正送金する新たな手口による被害が約 2 億 1,200 万円発生した。また、仮想通貨交換業者等への不正アクセスによる不正送信事案の認知件数は 149 件、被害額約 6 億 6,240 万円相当に上る。認知件数のうち、122 件（81.9%）では、ID・パスワードによる認証のみで、2 要素認証が利用されていなかった[※87]。仮想通貨の送金・決済に関する制度・セキュリティは整備途上にあり、警戒が必要である（「3.2 仮想通貨の情報セキュリティ」参照）。



■図 2-1-7　サイバー犯罪検挙件数推移
（出典）警察庁「平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

(b) 主なサイバー犯罪検挙事例

2017 年度における、上記以外の注目すべきサイバー犯罪検挙事例として、次の事例が挙げられる。

- 2017 年 6 月、神奈川県警察は、ランサムウェアを自作したとして、中学 3 年の男子生徒を、不正指令電磁的記録作成等の疑いで逮捕した[※88]。
- 2017 年 9 月、警視庁は、他人が所有するポイントを悪用し、インターネット通販サービスや家電量販店から商品を騙し取った等として、中国籍の男 3 人を、詐欺等の疑いで逮捕した。被疑者らは、何らかの方法で入手した大量の個人情報を基に、サーバに不正アクセスを試みる「リスト型攻撃」を行っていたとされる[※89]。
- 2017 年 10 月、岐阜県警察は、USB 型「キーロガー」を用いて、中学校のパソコンの ID やパスワードを不正に取得したとして、無職の男を、不正指令電磁的記録供用等の疑いで書類送検した[※90]。

(3) 今後の課題

高度化するサイバー犯罪に対する、警察その他法執行機関の役割は今後ますます重要となってくる。

サイバー犯罪を予防するためには、法に従って行為者を追跡し、司法の場において相応の責任を負わせ、サイバー犯罪行為が割に合わないことを行為者自身及び社会全体に認知させる必要がある。サイバー犯罪者にとってローリスク・ハイリターンの状況にある限り、サイバー犯罪はなくならない。

特に、薬物やウイルスの売買、不正入手した仮想通貨のロンダリング等、あらゆる犯罪の温床となっているのが、インターネット上の「ダークウェブ[※91]」と呼ばれる空間である。ダークウェブでは、追跡困難な匿名通信によって、日々、犯罪に関するやり取りがなされている。警察庁の重点施策では、サイバー空間の脅威への対処に関わる研究開発の推進事項の一つとして、「Tor 等の匿名化通信の発信元の特定等に関する調査研究を実施する」としている[※92]。2018 年 1 月、警察庁は、東京オリンピック・パラリンピック競技大会が迫る中、重要インフラ等に対する大規模サイバー攻撃に備え、ダークウェブに関する初の実態調査に乗り出すとした[※93]。このような実態調査等を通じ、サイバー犯罪に対する追跡能力の更なる向上が望まれている。

2.1.5 電子政府システムの安全性確保への取り組み

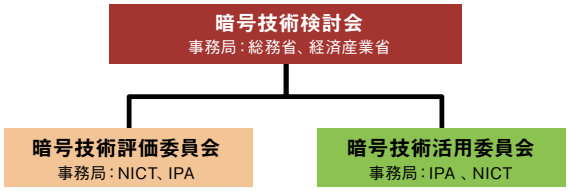
電子政府の情報セキュリティを確保するため、総務省と経済産業省は安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC では、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC 暗号リスト[※94]）の安全性を評価、監視し、暗号技術の適切な実装や運用法を調査、検討している。

(1) 2017 年度の体制

CRYPTREC は、総務省と経済産業省が運営し、政策的な判断を含む総合的な観点から電子政府の安

全性及び信頼性を確保する活動を推進する「暗号技術検討会」と、NICT、IPA が共同で運営し、主に技術的な評価を実施する委員会とで構成されている。

委員会には、暗号技術の安全性評価を中心とした技術的な検討課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図 2-1-8）。



■図 2-1-8　CRYPTREC の体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会
  CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。
- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術における技術的信頼に関する検討を担当する。傘下には、公開鍵暗号の中長期的な安全性の検証や新世代暗号に係る調査等を行う「暗号技術調査ワーキンググループ」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。

(2) 2017 年度の主な活動

2017 年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

暗号技術検討会では CRYPTREC 活動の承認、各委員会が作成する各種成果物の承認等を行っている。2017 年度は、第 1 回の暗号技術検討会において各委員会の 2017 年度活動計画の承認、第 2 回の暗号技術検討会において各委員会の活動報告、及び、以下の事項の審議が行われ、承認された。

- 64 ビットブロック暗号の注釈の変更
- 3-key Triple DES（Data Encryption Standard）の注釈の削除及び「電子政府推奨暗号」から「運用監視暗号リスト」への降格
- MISTY1 のフルラウンド攻撃への対応
- 認証暗号 ChaCha20-Poly1305 の「推奨候補暗号リスト」への追加
- 技術分類「認証暗号」の新設及び注釈の追加

(b) 暗号技術評価委員会

暗号技術評価委員会では、暗号技術についての動向調査や安全性の評価に関する検討を行っている。CRYPTREC 暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動の他、2017 年度の主な活動内容・成果は以下のとおりである。

- 64 ビットブロック暗号の安全性評価
  2016 年度に、TLS や OpenVPN 等の実プロトコルで 64 ビットブロック暗号を使ったとき、同じ秘密鍵（同一鍵）で 2^{32} ブロック以上のデータを暗号化した場合、Cookie やパスワード等の秘密情報が導出可能であるとの発表※95 があった。また、米国国立標準技術研究所（National Institute of Standards and Technology：NIST）から 64 ビットブロック暗号である Triple DES による同一鍵での暗号化上限回数を 2^{32} から 2^{20} に引き下げたガイドライン（SP800-67 rev.2）のドラフト版が公開された。このように、64 ビットブロック暗号の安全性に関する動きがあったことから、2017 年度は 64 ビットブロック暗号利用時の安全な利用方法（同一鍵での暗号化上限回数等）についての指針を検討した。またその検討結果を踏まえ、CRYPTREC 暗号リストでの 64 ビットブロック暗号の安全な利用方法に関する注釈として追加することを検討した。
- 認証暗号 ChaCha20-Poly1305 の安全性・実装性評価
  Web ブラウザ Google Chrome に標準搭載され、TLS1.3 にも採用が見込まれている認証暗号 ChaCha20-Poly1305 について、2016 年度はストリーム暗号 ChaCha20 単独での安全性評価を実施してきた。2017 年度はメッセージ認証コード Poly1305 単独での安全性評価、及び、認証暗号 ChaCha20-Poly1305 の安全性評価と実装性評価を実施し、ChaCha20-Poly1305 が安全性・実装性能ともに CRYPTREC 暗号リスト（推奨候補暗号リスト）への追

加に十分な条件を満たしているかどうかの検討を行った。また、CRYPTREC暗号リストへの新規カテゴリ（認証暗号）新設について検討した。

- ハッシュ関数SHA-1の安全性低下への対応検討
  2016年度にCRYPTREC暗号リスト（運用監視暗号リスト）記載のハッシュ関数SHA-1（Secure Hash Algorithm 1）で、実際にハッシュ値が同じになる（衝突する）二つのデータを求めることに初めて成功したとの発表[※96]があった。これを受けて、2017年度はCRYPTREC暗号リストの中でSHA-1を利用する暗号技術（DSA（Digital Signature Algorithm）、ECDSA（Elliptic Curve Digital Signature Algorithm）等）に対するSHA-1の安全性低下に伴う影響を評価した。また、CRYPTREC（暗号技術評価委員会）の既発行ガイドラインである「暗号技術ガイドライン（SHA-1）」のアップデートについて検討を行った。
- 暗号技術調査ワーキンググループの活動
  2017年度は「暗号解析評価」をテーマとして、将来、量子計算機が実用化されても安全性が保てると期待される暗号（耐量子計算機暗号）の調査・検討が行われた。この調査・検討は2017～2018年度の2年間で行い、2018年度末に調査報告書として公開予定である。また、現時点の主要な公開鍵暗号（RSA暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関してCRYPTRECが公開している「予測図」の改訂についての検討も行われた。

(c) 暗号技術活用委員会

暗号技術活用委員会では、情報セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）の整備を中心とした暗号利用に関する検討を行っている。2016年度に、今後運用ガイドラインを作成する価値がある対象や作成の課題について検討を行った。その結果を踏まえ、2017年度は以下の活動を行った。

- 「鍵管理に関する運用ガイドライン」作成に向けた活動
  2016年度に取りまとめた運用ガイドラインの候補の中で鍵管理に関するものが多数を占めており、また実際に暗号を利用する上でも鍵の正しい運用は不可欠であることから、鍵管理に関する運用ガイドラインの重要性は他と比較しても高いと考えられる。一方、鍵管理に関するガイドラインは、既に国内外を含め、いくつか発行されているが、いずれのガイドラインも広く認知され利用されているとは言い難い。これらの点を踏まえ、2017年度は、鍵管理に関する規格を網羅的に調査し、どのような体系・順番で鍵管理に関するガイドラインを作成していくのが良いか検討を行った。
- 「SSL/TLS暗号設定ガイドライン」のアップデート
  CRYPTREC（暗号技術活用委員会）の既発行運用ガイドラインである「SSL/TLS暗号設定ガイドライン」のダウンロード数は、2015年5月公開以来、14万件以上に上っている。しかし、発行時から約3年が経過し状況が変化していることから、2017年度は外部動向の追加並びにそれに対応するためのマネジメント方針の追記・修正等を行い、2018年5月「SSL/TLS暗号設定ガイドライン 第2.0版」として公開した[※97]。
  本ガイドラインの第1.0版を公開した2015年当時は、レガシーシステムや携帯電話等でSSL3.0やSHA-1証明書の利用を必要とするケースが無視できないことから、「セキュリティ例外型」を設け「早期移行を前提とした暫定的な利用継続」を認めていたが、この3年間でSSL3.0やSHA-1証明書の利用脱却が大きく進んだ。また、安全性の面からも、SSL3.0で利用するストリーム暗号RC4の利用禁止が決まったり、前述のとおりTriple DESやSHA-1の安全性が一段と低下したりしている。このため第2.0版では「セキュリティ例外型」の「安全性」について「本ガイドラインの公開時点（2018年5月）において、最低限度の安全性水準を満たしているとは言えない状況になっている。速やかな推奨セキュリティ型への移行を強く求める」と記述を変更した。

2.2 情報セキュリティ関連法の整備状況

企業及び組織には管理された秘密情報や個人情報が電子的に保存され、また、インターネットを介して様々な情報が流通している。これらの情報を保護し、有効活用を進めるため、法律面の整備が進められている。

2.2.1 サイバーセキュリティ基本法

サイバーセキュリティ基本法は、サイバーセキュリティ対策に関する国・地方公共団体の責務を規定した基本法である。2014 年に成立し、2015 年 1 月 9 日に全面施行された。この基本法に基づき、内閣官房にサイバーセキュリティ戦略本部が設置され、以後「サイバーセキュリティ戦略の立案や実施」「政府機関などにおける対策基準の作成や評価」「政府機関などで発生する重大なセキュリティ事案などの評価」等が行われることとなった。

(1) サイバーセキュリティ基本法改正の経緯

サイバーセキュリティ基本法は、2016 年に一度改正されている。2015 年に発生した日本年金機構の情報漏えい事件等を契機として、2016 年 4 月、改正法が第 190 回通常国会で成立し、同年 10 月 21 日に施行された。これまで、サイバーセキュリティ戦略本部及び NISC は、情報システムに対する不正通信の監視、重大な事象に対する原因究明調査、「政府機関の情報セキュリティ対策のための統一基準群」に基づく監査を中央省庁に対して実施してきた。この改正により、監視及び原因究明調査の対象範囲が独立行政法人及び指定法人（サイバーセキュリティ戦略本部が指定した特殊法人及び認可法人）までとなり、監査の対象範囲も指定法人にまで拡大した。また、サイバーセキュリティ戦略本部は、これらに関する事務の一部を IPA とその他政令で定める法人へ委託可能となった※98。

一方で、サイバーセキュリティ戦略本部のサイバーセキュリティ戦略中間レビュー※99 では、2020 年東京オリンピック・パラリンピック競技大会で懸念される重要インフラを狙ったサイバー攻撃への対策や、更なる官民の連携が求められている。

こうした状況を受け、2018 年 3 月 9 日にはサイバーセキュリティ基本法の改正が閣議決定された。第 196 回通常国会に同法案が提出され、改正に向けた審議が実施されているところである。

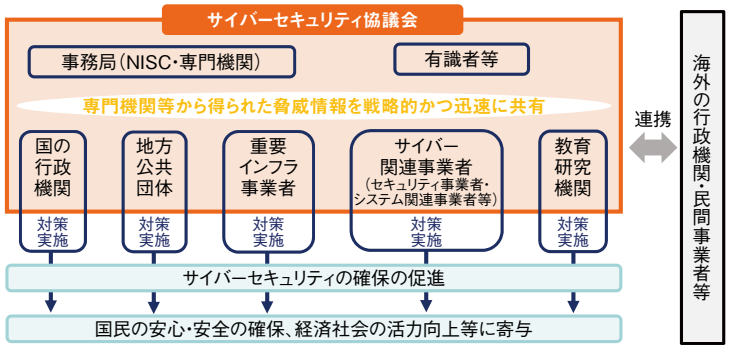
(2) 2018 年のサイバーセキュリティ基本法改正のポイント

今回のサイバーセキュリティ基本法改正のポイントは以下のとおりである。

- 「サイバーセキュリティ協議会」の設置

  サイバー攻撃に関する情報を戦略的かつ迅速に共有するため、官民の協議体である「サイバーセキュリティ協議会」（以下、協議会）を設置する。

  協議会は、NISC 及び専門機関が事務局となり、国の行政機関や地方公共団体のほか、発電所や鉄道等の重要インフラ事業者、サイバー関連事業者（セキュリティ事業者・システム関連事業者等）、教育研究機関、有識者で構成され、サイバー攻撃の兆候や事案に関する情報（ウイルスの検体、DDoS 攻撃予兆・被害情報等）を自動的に共有し、それらを迅速に分析・解析することを可能とする仕組みとする（図 2-2-1）。情報の分析・解析は IPA や NICT も協力する。サイバー攻撃情報等は、構成員を通じ関係機関等へ迅



■図 2-2-1　サイバーセキュリティ協議会
（出典）NISC「サイバーセキュリティ基本法の一部を改正する法律案※100」

速に周知し、対策の実施が促進される仕組みとする。協議会は、「政府オリンピック・パラリンピックCSIRT」の位置付けとなる「サイバーセキュリティ対処調整センター」(2018年度末設置予定)との情報交換も密に実施する※21。

- グローバル連携
  協議会は、米国を始めとする諸外国の行政機関、セキュリティ会社等とグローバルな連携を行うものとし、情報交換を始め、重要インフラのセキュリティに関するサイバー演習や、セキュリティ人材育成を実施するための基盤を整える。

改正法を根拠としたこれらのサイバーセキュリティ対策の実装により、今後も直面することが予想される新たなセキュリティ脅威に対して、迅速な状況判断と情報共有が円滑に実施されることが期待される。

2.2.2 不正競争防止法

不正競争防止法は、事業者間の公正な競争と国際約束の的確な実施を確保するため、不正競争の防止を目的として設けられた法律である。1993年の現行法成立以降、これまで8次に及ぶ改定を経ており、今回更に、最近の社会情勢を踏まえた改正法案が2018年2月27日に閣議決定され、第196回通常国会で可決成立し、同年5月30日に法律第33号として公布された。

(1)不正競争防止法改正の背景

2017年3月、モノやデータ(情報)が様々に連携して新たな付加価値を創出する「Connected Industries」の概念が政府により提唱された※101。その一つが、従来では自社で囲い込み閉じた領域で使用していたデータを、囲い込まずに事業目的に応じて積極的に市場に流通させ、横断的なデータの利活用を促すことで様々な変革を行う取り組みである。

こうした社会を実現する基盤として、安心してデータをやり取りでき、データの創出・収集・分析・管理等に対する投資に見合った適正な対価を得られる環境整備が重要となる。「知的財産推進計画2017※102」(2017年5月知的財産戦略本部決定)及び「未来投資戦略2017※103」(2017年6月閣議決定)では、安心してデータをやり取りできる環境整備のため、公正な競争実現やデータ不正利用防止の検討が求められた。

こうした背景のもと、データの不正取得や不正取得されたデータの流通を抑止し、事案発生時の被害を低減するため、不正競争防止法の改正が検討されることとなった。

(2)不正競争防止法改正のポイント

2016年12月から、産業構造審議会 知的財産分科会「営業秘密の保護・活用に関する小委員会※104」では、データ保護の在り方を中心に不正競争防止法に関わる課題について審議が行われ、2017年5月に「第四次産業革命を視野に入れた不正競争防止法に関する検討中間とりまとめ」が行われた※105。これを受け、同分科会「不正競争防止小委員会」では2017年7月から、不正競争防止法の改正に向け検討を継続し、改定すべき以下の事項を抽出した。

- データ利活用促進に向けた制度
- 技術的な制限手段による保護強化

これらの事項を踏まえ、不正競争防止法の改正が実施された。この改正により、データの利活用を阻害することなく、不正な取得・流通が抑止される、等の効果が期待される。それぞれの事項のポイントは以下のとおりである。

(a)データ利活用促進に向けた制度

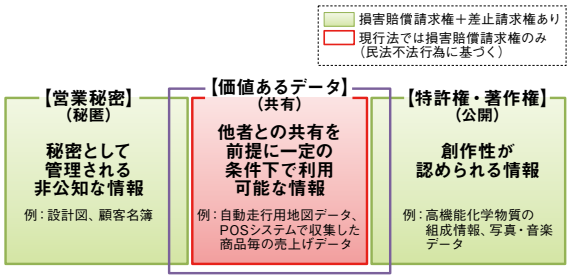
自動車走行用地図データやPOSシステムで収集した商品売り上げデータ等の「活用されることにより新たな価値を生み出すデータ」がスムーズに共有され、利活用が促進される法的枠組みを作る。現行の不正競争防止法では共有が前提となっているようなデータは不正競争防止法による保護が受けられないことから企業がデータの提供を控える等、データ利活用を抑制する要因となっていた。そこでID・パスワード等の管理を施した上で提供されるデータの不正取得・使用等を新たに不正競争行為と位置付け、これに対する差止請求権、損害賠償の特則等の民事上の救済措置を設ける。これによりデータの利活用を促進し、活用されるデータを保護する(データの不正取得等の禁止)。図2-2-2に新たなデータ保護対象の領域(赤枠内)を示す。

(b)暗号化等の技術的な制限手段の保護強化

「暗号化等の技術的制限手段が施されたもの」に対する「効果を妨げる行為(いわゆるプロテクト破り等)の範囲」が見直され、技術的制限手段による保護対象として映像、音等のコンテンツの視聴等に、電磁的記録(デー

タ）が追加された。技術的制限手段の新たな保護対象としては、各種アクティベーション方式等が例示された。

また、技術的制限手段を無効化する機器の提供等に加えて、役務の提供等も不正競争行為とされた。



■図 2-2-2　データ保護対象
（出典）経済産業省「不正競争防止法等の一部を改正する法律案（不正競争防止法、工業標準化法、特許法等）の概要資料※106」

COLUMN

えっ、私も個人情報取扱事業者!?

2017 年 5 月 30 日から、すべての事業者に「個人情報保護法」が適用されています。

個人情報保護法が 2005 年に施行された後も、取り扱う個人情報の数が 5,000 人分以下の事業者には適用されていなかったため、多くの中小企業では適用が除外されていました。そのため、個人情報保護法が適用されるようになっても、何をしたらよいのか戸惑われている中小企業の経営者や従業員の方がまだ多いようです。どのような情報が個人情報にあたるのかご存知ですか?

「氏名」「顔写真」「DNA 情報」「マイナンバー」等、「生存する個人に関する情報で、特定の個人を識別することができるもの」が個人情報です。ですから、顧客情報だけでなく、従業員情報や取引先の名刺といったものも個人情報になります。そして、自治会や同窓会等の非営利組織にも適用されるので、会員名簿等を取り扱う際は注意を払わなければなりません。

2016 年 1 月に発足した個人情報保護委員会では、個人データの漏えい等の報告を受け付けています。漏えい等事案の発生原因の多くはメールの誤送信及び書類等の誤送付や紛失といった人為的な誤りだそうです。こういった事案は事業規模の大小によらず個人情報を扱うすべての人が気を付けなければならないことですね。

個人情報保護委員会のサイトでは中小企業向けのサポートページ（http://www.ppc.go.jp/personal/chusho_support/）を開設し、説明資料や Q&A を公開しています。自治会や同窓会で会員名簿を作るときの注意事項や、個人情報保護法ヒヤリハット事例集等、個人情報を取り扱う上で発生しやすい事例の紹介もしています。ぜひ参考にしてください。

2.3 国別・地域別の情報セキュリティ政策の状況

テロリズム、思想・信条に基づく攻撃（ハクティビズム）、職業的サイバー犯罪は国境を問わず、あらゆる国・地域のシステムをターゲットに攻撃を仕掛けてくる。社会基盤のIT化が進展したことで、これらの脅威は深刻化しているが、国や地域が単独で対処することは難しく、国際連携が不可避である。本節では、国際連携に向けた状況理解のために、各国・各地域における情報セキュリティ政策について述べる。

2.3.1 国際社会と連携した取り組み

2016年度に引き続き、日本政府は2017年度も米国、欧州、イスラエル、アジア諸国とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動の中で注目すべき取り組みを紹介する。

(1) 日米のサイバー連携

2017年7月20～21日、第5回日米サイバー対話が開催された※107。大鷹正人外務省総合外交政策局審議官兼サイバー政策担当大使、国家安全保障局、NISC、内閣情報調査室、警察庁、総務省、経済産業省、防衛省等の政府関係者が参加した。米国はChristopher Painter国務省サイバー問題調整官を始め、国務省（Department of State：DoS）、国土安全保障省（Department of Homeland Security：DHS）、国防総省（Department of Defense：DoD）、連邦捜査局（Federal Bureau of Investigation：FBI）等の幅広い関係者が参加した。2016年の日米サイバー対話等のフォローアップや環境情勢認識、両国の取り組み、国際協力、能力構築支援等の幅広い協力について議論を行い、共同プレスリリース※108では、「日米防衛協力のための指針」による防衛省とDoDとのサイバー協力、NISCとDHSのサイバーインテリジェンス情報共有、IoTセキュリティ強化のためのアプローチ共有、サイバー空間の安全・自由の維持・強化等が盛り込まれた。

経済産業省とIPAは2017年9月19～26日、DHS及びDHS配下のICS-CERT（Industrial Control Systems Cyber Emergency Response Team）の専門家を招聘し、産業システムのインシデントを想定したサイバー演習を実施した※109（「2.4.1（3）産業サイバーセキュリティセンター」参照）。日米政府間協力による産業サイバー演習として初の試みである。

首脳レベルでは、2017年9月21日に安倍晋三首相とトランプ（Donald John Trump）大統領による日米首脳会談がニューヨークにて行われたが、北朝鮮に対する各国の連携が主な議題となった。2018年4月17～18日にフロリダにて行われた日米首脳会談においても北朝鮮対応と経済交渉が主要議題となり、サイバーセキュリティ政策への言及はなかった※110。サイバーセキュリティに関する日米協力は、オバマ（Barack Hussein Obama II）政権時の合意をほぼ引き継ぐ形で推移していくと思われる。

(2) EU諸国とのサイバー協議

EU諸国との主要なサイバー協議について述べる。

(a) 日EUサイバー対話

2018年3月5日、第3回日EUサイバー対話が東京にて開催された※111。日本から大鷹外務省総合外交政策局審議官兼サイバー政策担当大使を始めとする関係機関の代表者が、EUからFrancois Rivasseau欧州対外活動庁宇宙特使兼安全保障・宇宙政策課長を始めとする関係機関の代表者が出席した。協議においてはサイバーセキュリティに対する双方の戦略・政策と課題について広範な討議が行われ、サイバー犯罪対策の連携、サイバー空間における国際法や規範の遵守、不当な知的財産窃取への反対等が共同声明に盛り込まれた※112。2017年に中国が「中華人民共和国網絡安全法」（ネットワーク安全法※113）を策定し、サイバー空間への統制を強めていることへの懸念が示されたものと言える。

(b) エストニアとの連携協議

2018年1月12日、安倍首相はエストニアのJüri Ratas首相とタリンで会談し、東京オリンピック・パラリンピック競技大会を見据え、サイバー攻撃対策に関する連携強化で合意した※114。

(c) 英国とのサイバー協議

2017年8月31日、安倍首相とTheresa May首相による日英首脳会談が東京で行われ、サイバーセキュリティに関しては自由で開かれた安全なサイバー空間の実現に向け、緊密に連携することで合意した※115。

これを受け、第4回日英サイバー協議が2018年3月16日にロンドンで開催された。日本側共同議長は大鷹外務省総合外交政策局審議官、英国側の共同議長はSarah Taylor外務省サイバー政策部長が務め、両国の関係機関の代表者が参加した。協議においてはサイバーセキュリティ分野における両国の最新の取り組みや重要インフラ防護、能力構築支援について議論が行われ、会合後の共同プレスステートメントでは、安全で自由なサイバー空間の重要性の再確認、IoT機器の保護や悪意のサイバー活動への対策、能力構築への取り組み強化等が盛り込まれた※116。

(3) 欧州委員会とのGDPRに関する包括討議

EUの新たな個人情報保護規則である「一般データ保護規則(General Data Protection Regulation:GDPR)」は2018年5月から発効となり、欧州で事業を行う日本企業にも少なからぬ影響が及ぶと考えられ、準備が急がれている。影響の一つとして、日本・EU間の個人データの越境移転の問題がある。現時点で、当該データ移転について日本・EU間の包括的な取り決めはなく、データ移転を必要とする企業は個別契約でGDPRに対処する必要がある。しかし、2017年5月30日に改正個人情報保護法が施行されたことから、欧州委員会は日本との包括的取り組みの構築を急ぐことを明言し、それに向けた検討が始まっている。2017年12月14日、日本の個人情報保護委員会と欧州委員会は共同プレスステートメントを発表し、双方の制度の相違について、法改正によらない解決策を詳細化し、2018年早期の合意を目途に会談を持つこととした※117。2018年5月31日、個人データの相互移転に関する合意がなされたことが発表され、懸案がクリアされた。

(4) 日・イスラエル・サイバー協議

2017年10月5日、日・イスラエル投資協定※118が発効し、サイバーセキュリティや安全保障分野を含む二国間の投資が促進される体制が整った。イスラエルはサイバーセキュリティに関する日本の投資を歓迎し、日本を有望な市場ととらえており、民間の企業連携等が加速している。

こうした中、11月29日、東京にて第3回日・イスラエル・サイバー協議が開催された※119。日本からは、大鷹外務省総合外交政策局審議官を始め関係政府機関の代表者が、イスラエルからは、Yigal Unna首相府国家サイバー局副局長を始め、国家サイバー局、イスラエル外務省及び在京イスラエル大使館から関係者が出席し、サイバー政策や脅威の現状、人材育成・能力構築等について協議が行われた。

(5) ASEANとのサイバー連携協議

NISC、総務省、経済産業省は、2017年10月10～11日、シンガポールにて第10回日・ASEAN情報セキュリティ政策会議を開催した※120。同会議にはASEAN加盟国から経済・情報通信関係政府機関の局長・審議官等が、日本から関係省庁の審議官等が参加した。会議においては、前年の第9回で合意されたサイバー脅威等の情報連絡演習、重要インフラ防護、人材育成の取り組みの成果を確認し、更なる対策強化が議論された。具体的な強化策では日常的な情報共有の一層の促進、重要インフラ防護の先進的な取り組み事例の共有等について合意がなされた。

また外務省は、ASEAN地域の政治・安全保障フォーラムであるASEAN地域フォーラム（ASEAN Regional Forum：ARF）を通じた連携を継続している。2018年1月18日、東京にてサイバーセキュリティに関するARF会期間会合（ARF-ISM on ICTs Security）のための第1回専門家会合が開催された※121。本会合では、日本・マレーシア・シンガポールが共同議長を務め、サイバーセキュリティの環境認識や域内の各国・地域の取り組みを共有し、今後取り組むべき信頼醸成措置について議論が行われた。この成果は2018年4月25～26日、クアラルンプールにて開催されたARF-ISM on ICTs Security※122に提供された。

(6) 日インド・サイバー協議

2017年8月17日、第2回日インド・サイバー協議がニューデリーにて開催された※123。日本からは大鷹外務省総合外交政策局審議官、NISC、内閣官房内閣情報調査室、警察庁、JPCERT/CCが参加した。インド側からはSanjay Kumar Verma外務省Eガバナンス・IT・サイバー外交担当局長を始め、関係政府機関の代表者が参加した。

会議においては、自由で開かれた安全なサイバー空間の実現に向けて取り組むこと、サイバー空間にも既存国際法が適用されることが再確認された。また、企業に競争優位性を与えることを目指し、情報通信(ICT)技術による営業秘密や知的財産等の窃取・支援を実行すべきでないことが再確認された。

これらは、サイバー空間での国家主権の優越に対し、

明確に反対の立場を主張するもので、この点でインドは日米欧と共同歩調を取っており、日米欧のパートナーとして重要性を増している。

(7) セキュリティ連携に関する国際会議

2017 年 10 月 5 ～ 6 日、サイバーセキュリティに関する国際会議 Cyber3 Conference Tokyo 2017※124 が開催された。本会議は世界経済フォーラム（World Economic Forum：WEF）の協力、国内の関係政府機関、各国大使館等の後援を受けて 3 年連続で実施されるもので、第 3 回は東京オリンピック・パラリンピック競技大会後を見据えたセキュリティのあるべき姿がテーマとなった。また、会場となった慶應義塾大学による「第 5 回サイバーセキュリティ国際シンポジウム」も同時開催となり、慶應大学セッションという形で実施された。Cyber3 Conference Tokyo のセッションでは、Society 5.0（IoT 活用による超スマート社会）の実現に向けたセキュリティの課題として、過去 1 年で脚光を浴びた Fintech、AI、自動走行の安全に加え、インシデントに対するレジリエンスの強化、AI の活用、データの機密性から可用性への重点シフト、人・モノ・データの統合的な認証等が議論された。

一方、慶應大学セッションでは、同大学を含む日米英 13 大学によるセキュリティ調査・教育・演習の共同連携組織 International Cyber Security Center of Excellence（INCS-CoE）※125 の活動紹介、及び関連トピックの議論が行われた。INCS-CoE は米国 5 大学、英国の 4 大学、日本の 4 大学が参加し、2016 年 11 月に発足した組織であり、本セッションでメンバーによる活動報告が行われた。また関連トピックとして、サイバーセキュリティ・サプライチェーン、セキュリティ演習におけるグローバル連携のパネルセッションが開催され、産学官の識者による議論が行われた。INCS-CoE の活動は 2 年目に入り、グローバル連携の今後の成果が注目される。

(8) サイバー犯罪対策に関する国際連携

日本政府は INTERPOL と協力し、サイバー犯罪対策に関する国際連携を推進している。INTERPOL は 2015 年、シンガポールにイノベーション開発とトレーニングの拠点となる INTERPOL Global Complex for Innovation（IGCI）を設立したが、日本政府・企業は人材派遣や技術の提供でこれを支援している。

2018 年 2 月 19 ～ 21 日、INTERPOL のサイバー犯罪捜査演習 INTERPOL Digital Security Challenge の第 3 回がウィーンで開催された※126。今回は初めて IoT 機器が悪用されるシナリオで演習が行われたが、シナリオの策定・演習実施では毎回日本企業が貢献している。各国捜査機関のサイバー犯罪対応力の向上が期待される。

(9) 今後の海外連携

以上のように、欧米、ASEAN、インド等とのセキュリティ政策連携は着実に進展している一方、中国・ロシアとの連携協議は進んでいない。特に中国はネットワーク安全法の成立により、インターネット上の経済活動に対する国家の関与が深まることが予想される。米中貿易摩擦の懸念が深まる中、どのような連携を行うべきか、各国との協調も含めた慎重な対応が求められる。

2.3.2 米国のセキュリティ政策

2 年目に入ったトランプ政権は、2018 年 3 月に鉄鋼・アルミニウム輸入品への追加関税に関する大統領令に署名※127 する等、保護主義的な経済政策を強化している。こうした「アメリカファースト」の政策は米国内の経済界や議会を始め、内外の反発・懸念を招き、4 月には中国が米国産ワイン・豚肉等に関する報復関税を発動した※128。中国との経済摩擦は予断を許さない状況となっている。

安全保障面では、トランプ政権は北朝鮮・イラン・シリア・ロシア等に強硬な姿勢を取る一方、親イスラエルの立場を鮮明にしている。このうち北朝鮮は 2017 年 2 月から 11 月にかけてミサイル発射実験・核実験を繰り返し、米国が核攻撃の射程圏内であることを誇示した。これに対してトランプ政権は各国と連携した経済制裁を強化した※129 が、2018 年 3 月、一転して両国は首脳会談を開催することで合意した※130。

こうした中、2017 年の米国のサイバーセキュリティ政策は、5 月に発効した大統領令に基づく連邦政府のセキュリティ政策見直し、及び権限集約等によるナショナルセキュリティ戦略の強化が重点課題となった。本項では、トランプ政権のセキュリティ政策の主な動向について述べる。

(1) サイバーセキュリティ強化に関する大統領令の概要

2017 年 5 月 11 日、トランプ大統領は米国のサイバーセキュリティ強化に関する大統領令※131 に署名した。本大統領令は、1 月の就任直後の案ではサイバーセキュリ

ティに関するDoDの権限を強化する、等の施策を盛り込んでいたが、関係機関の調整が長引き、5月にようやく発効したものである。

内容は連邦政府ネットワークのセキュリティ、重要インフラのセキュリティ、国家のセキュリティの3部構成となっており、それぞれの概要を述べる（以下の記載において報告する相手が明示されていない場合は、すべて大統領への報告である）。

- 連邦政府ネットワークのセキュリティ

  連邦政府機関の長（Agency Heads）は、各組織のセキュリティ脅威に応じたリスク管理対策の実装に責任を持つ。彼らは、NIST Cybersecurity Frameworkに基づくリスク評価を行い、大統領令発効後90日以内にDHS長官、及び行政管理予算局（Office of Management and Budget：OMB）長官に報告する。

  OMB長官とDHS長官は報告を査閲し、商務長官、連邦政府一般調達局長官と協力して60日以内にリスク評価の査閲結果、及び必要な対策・予算措置・規格等の計画を併せて報告する。

  各組織の長はメール、クラウド、セキュリティ等で共有ITサービスの利用を優先する。また、連邦政府のIT刷新に関する評議会であるAmerican Technology Council[※132]の議長は関連官庁の報告を調整し、安全・頑健な統合ITアークテクチャ、共有サービスへの移行に関する実現可能性コストについて90日以内に報告する。

  ナショナルセキュリティ関連システムへの大統領令の実装については、国防長官と国家情報長官が責任を負う。

- 重要インフラのセキュリティ

  政府執行部門は重要インフラ所有者・運用者を支援し、最大の脅威に備える。

  DHS長官は、国防長官、司法長官、国家情報長官、FBI長官、その他分野別所管官庁の長と連携し、大統領令13636第9節に基づく、重要インフラ事業者への壊滅的な攻撃を想定したセキュリティ対策実施の権限と機能を特定し、その実装について当該事業者に意見を求め、180日以内に報告する。

  DHS長官は商務長官と連携し、重要インフラ事業者のセキュリティリスク管理実践の透明性に関する連邦政府の施策を調査し、90日以内に報告する。

  商務長官とDHS長官は、国防長官、司法長官、FBI長官、分野別所管官庁の長、連邦通信委員会（Federal Communications Commission）議長、及び連邦取引委員会（Federal Trade Commission）議長等の支援を受け、ボットネットや他の自動化・分散化された攻撃脅威に対するインターネットの頑健性強化、連携推進のプロセスについて240日以内に報告する。

  エネルギー省長官とDHS長官は、国家情報長官及び関係自治体と連携し、重大サイバーインシデントによる電力喪失リスクの評価、それに対する政府の準備状況と課題について調査し、90日以内に報告する。

  国防長官、DHS長官及びFBI長官は、国家情報長官の支援を受け、防衛産業とそのサプライチェーン、米軍のITプラットフォーム、システム、ネットワーク、機能に関するサイバーリスク評価について90日以内に報告する。

- 国家のセキュリティ

  オープンで相互運用性があり、高信頼で安全なインターネットの維持は効率的な通信・イノベーション・経済拡大の基盤であり、米国の政策である。国務長官、財務長官、国防長官、司法長官、商務長官、DHS長官、米国通商代表は国家情報長官と協力し、これを脅かす勢力・サイバー脅威に対抗する施策について90日以内に報告する。

  また国務長官、財務長官、国防長官、商務長官、DHS長官、司法長官はFBI長官と協力し、サイバーセキュリティの調査分析、情報共有、能力構築等の国際的な優先課題を45日以内に報告し、更に当該報告後90日以内に具体的な国際連携戦略について報告する。

  更に長期的なサイバーセキュリティ施策として、DHS長官と商務長官は、国防長官、労働長官、教育長官、連邦人事管理局（Office of Personnel Management：OPM）長官他の支援を受け、セキュリティ教育訓練プログラムを検証し、また国家セキュリティに関わる官民の人員体制強化に関するアセスメント結果を120日以内に報告する。

  国家情報長官は関係機関の支援を受け、米国のサイバーセキュリティの優位に影響する海外の体制構築について60日以内に報告する。

  国防長官、商務長官、DHS長官、国家情報長官は国家のセキュリティに関わるサイバー機能構築の範囲と十分性を検証し、150日以内に報告する。

この大統領令は、連邦の各省庁が共通のセキュリティ基準に基づきリスクアセスメントを行い、セキュリティ施策

を大統領（実質的にはDHS、OMB等）が査閲する点で、初の省庁横断的な総合施策である。オバマ政権の資産を引き継ぎつつ、政府機関やセキュリティ専門家の意見を取り入れた結果、重要インフラの重視、新しいIT基盤への移行、国際連携等の内容が盛り込まれ、内容に対しておおむね好意的な評価がされている。一方で、政策の実効性や有効性に対して疑問の声もあり、具体的な政策内容に関する見解は分かれている[※133][※134]。2017年度は本大統領令に基づく施策策定の時期となり、その実施は多くが次年度からとなる。

(2) サイバー空間のナショナルセキュリティ

2017年8月18日、トランプ大統領はTwitterで米国サイバー軍（Cyber Command）を統合軍（Unified Combatant Command）に格上げすると発表した[※135]。James Mattis国防長官の意向にも沿うものであり、米国安全保障におけるサイバーセキュリティの重要性が増したことを示している[※136]。

次いで12月18日、トランプ大統領は国家安全保障戦略に関するビジョンを発表した[※137]。このビジョンは、同大統領の「アメリカファースト」の信念が反映されたものとなっているが、サイバー空間の脅威については、「米国に対する悪意の行為者に対し、リスクを考慮の上、抑止、防御に加え、必要なら打倒する」と簡潔に述べ、以下の3点を優先課題としている。

- サイバー攻撃者の特定能力の向上、インシデント対応の迅速化
- 米国政府・重要インフラの資産・情報保護に関する機能・人材の強化
- 政府の権限・手続きの統合とタイムリーな情報共有・施策実施のためのアジリティ強化

更に2018年4月19日、トランプ大統領は2017年12月に成立した国防権限法（National Defense Authorization Act for Fiscal Year 2018[※138]）で要求されている、サイバー戦に関する包括的な戦略を上下両院に提出した[※139]。同戦略は、国家レベルの統合的なサイバーセキュリティ戦略が政府になく、米国が他国のサイバー攻撃の標的になっている、というオバマ政権時代からの議会の不満に対してホワイトハウスが初めて応えたもので、ハッキング等の攻撃オプションを含む包括的なサイバー戦争戦略である。戦略の内容は機密とされているが、どのような場合にハッキングが許容されるか、等が今後の政策議論の焦点になると予想される。

(3) 北朝鮮のサイバー脅威への対応

サイバー空間の脅威に関し、2017年に米国と最も緊張関係にあった国家は北朝鮮とロシアである。

北朝鮮は2017年2月から11月までの間、中距離弾道ミサイル発射実験・核実験を相次いで実施し、米国との緊張は一気に高まった。この間、10月には北朝鮮による韓国軍へのハッキング攻撃により米韓の軍事情報漏えいが報じられる[※140]等、北朝鮮のサイバー攻撃能力への警戒感も強まった。米国内ではサイバー戦争の可能性についてメディアが論じたが、トランプ政権は北朝鮮とのサイバー戦については発言していなかった。

12月19日、Tom Bossert国土安全保障担当補佐官は、ランサムウェア「Wanna Cryptor」（別名WannaCry）による大規模なサイバー攻撃被害について、直接的な責任は北朝鮮にある、と同国を非難した。この攻撃はLazarus Groupと呼ばれる組織が実施したとされるが、Lazarusは2014年のSony Pictures Entertainment Inc.攻撃の実行部隊であったという。Wanna Cryptorへの北朝鮮の関与は英国政府やセキュリティ専門家によっても指摘されていたが、同国が経済制裁を逃れるため、ランサムウェア攻撃を新たな資金獲得の手段としたことをうかがわせる。Bossert補佐官は北朝鮮に対する報復のオプションがあまりなく、「官民連携によるサイバー攻撃対策の更なる強化が必要」としたが、米国サイバー軍がどのように対応しているかはもちろん公表されていない。

なお2017年5月、Wanna Cryptor被害の蔓延について、Microsoft CorporationのBrad Smith社長兼CLO（Chief Legal Officer）は、悪用されたWindowsの脆弱性情報を民間に適切に公開しなかったことが原因だとして、国家安全保障局（National Security Agency：NSA）を非難した。一方NSAは必要な情報は公開している、と反論した。官民における脆弱性情報の共有は、DHSがSTIX[※141]、TAXII[※142]等の標準フォーマット利用の推進、あるいはISACs、ISAOs[※143]等の民間組織との連携を進めているが、脆弱性情報を公開したからといって効果的に攻撃が防げるとは限らないともいわれる[※144]。Wanna Cryptorの事例は、こうした体制により実効的な対策を取ることの難しさを顕在化させたといえる。

(4) ロシア疑惑と外交関係の悪化

トランプ政権は発足以来、大統領選挙へのロシアの介入というスキャンダルへの対処に苦慮している。2017年5月、司法省はRobert Mueller元FBI長官を特別検

察官に任命、同検察官はロシア疑惑の捜査を進めてきた。10月30日にはPaul Manafort元選挙対策本部長他2人（いずれもトランプ陣営）をウクライナの親ロシア派支援に関する資金洗浄他の複数の罪で起訴した※145が、トランプ大統領は彼らが選挙対策チームに入る以前の疑惑であり、政権は無関係だと主張している。更にMueller特別検察官は2018年2月16日、組織ぐるみで大統領選挙介入に関わったとしてロシア人13人、企業3社を起訴した※146。ただし、ロシアの選挙介入にトランプ陣営が関わったことを立証するのは難しい情勢である。当然ながらロシア政府は選挙介入を否定し続けている。

経済面では2018年3月2日、ロシアのクリミア半島領土化に関する国家緊急事態（2014年3月に発令された大統領令13660）がまだ継続しているとの判断により、トランプ大統領は失効時期に来た国家緊急事態の1年延長を許可する大統領令に署名した※147。ロシアへの経済制裁は更に継続する。

また、元ロシア諜報機関員に軍用の神経ガス剤が使用されたとする英国政府に同調して、トランプ大統領は3月26日、ロシア外交官60人以上を国外追放処分とした※148。ロシア政府は関与を否定したが、更に4月13日、シリア政府軍が毒ガスを利用したとして、米・英・仏によるシリア空爆が、国連の現地査察がないまま実施された。シリア政府を支援するロシアはこれを激しく非難、安全保障理事会で空爆非難決議を提出したが否決された※149。

このように表面上では米国とロシアの対立は悪化を続けている。しかし、空爆において死者が出ていない、プーチン政権を名指しで非難していない、あるいはサイバー軍が目立った対応をしていない、等で米国は決定的な対立を回避し、交渉の余地を常に残しているとの見方もある。

(5) ホワイトハウスのセキュリティ体制再編

2018年3月13日、トランプ大統領はRex Tillerson国務長官を解任し、後任にMike Pompeo CIA長官をあてると発表した※150。国際協調派のTillerson氏から対北朝鮮強硬派のPompeo氏への移行であった。次に4月10日、前出のBossert国土安全保障担当補佐官の辞任が発表された。同補佐官はサイバー戦略の専門家であるが、4月6日のHerbert Raymond McMaster国家安全保障担当補佐官の辞任に続く退任劇となった。更にその直後、Rob Joyceサイバーセキュリティ調整官の退任も発表され、トランプ政権内で積み上げられてきたサイバーセキュリティ戦略の継承に懸念が生まれた。

今後、米国国家安全保障会議（National Security Council：NSC）では対外強硬派である新任のJohn Bolton国家安全保障担当補佐官の発言力が強まり、オープンな国際協調よりも国内のセキュリティが優先される可能性、あるいはサイバーセキュリティ戦略において、報復的なオプションが取られる可能性がある※151。現政権のタカ派的性格がどのように現れるか、予断を許さない。

こうした中、Pompeo CIA長官（当時）が3月31日～4月1日に北朝鮮の金正恩委員長と直接会談したことが報じられ※152、トランプ政権が強硬路線一本槍ではないことを示した。更に4月27日、金正恩委員長と韓国の文在寅大統領が首脳会談を行う等、北朝鮮との対話ムードが急速に醸成されつつある。ただし、これは経済制裁を含む強硬姿勢の成果だとする考えもあり、また非核化に対する米朝の立場には依然として大きな開きがある※153。開催予定の米朝首脳会談の成否が対北朝鮮政策を左右することは間違いないが、硬軟織り交ぜた関係各国の粘り強い交渉が必要になると思われる。

(6) サイバーサプライチェーンに関する強化施策

ICTシステム・サービスの調達・運用に関するサプライチェーン上でセキュリティをどう確保するかは各国で重要な課題となりつつある。米国では、2018年4月16日にNIST Cybersecurity Frameworkの改訂版（v1.1）が公開されたが、主要な改訂のポイントの一つにサプライチェーンのセキュリティマネジメントがある※154。

これに先立ち、DoDは2016年10月の通達で、同省の防衛装備品調達に参加するすべての事業者（日本の事業者を含む）に対し、政府機関以外の組織及び情報システムのセキュリティ基準であるSP800-171※155を、2017年12月末までに実装することを要請した。SP800-171が求めるのは、DoDが調達事業者に対して提供する「管理された非格付け情報（Controlled Unclassified Information：CUI）」の保護で、例えば装備品の設計図等が該当する。SP800-171が求めるセキュリティ管理策は、ISO 27001/27002のそれとほぼ同等であり、ISMSを実装した企業には大きな負担とはならないが、ISMS未実装の中小企業には支援が必要となる可能性がある。なおDoDはSP800-171の実装の監査等は行わない。規格策定者の一人は、各事業者がリスク分析に基づき、必要な管理策を実装すればよいとしている。

米国政府は、DoDを皮切りに他の政府機関の調達参加事業者にもSP800-171の実装を求めていく方針で

ある（守るべきCUIは各政府機関が定義する）。従来の調達契約ではセキュリティは個別に規定されていたが、全政府機関の全調達で同じレベルのサイバーサプライチェーンセキュリティを担保したい、という意思の表れであると思われる。

(7) 個人情報保護・世論誘導に対する規制強化の可能性

2017年7月、マイクロターゲティング※156技術を持つ選挙コンサルティング企業Cambridge Analyticaによるロシアの選挙介入工作の可能性が指摘された※157。トランプ政権の元首席戦略官Stephen Bannon氏は一時同社の副社長を務めていたが、2018年3月、同社のデータアナリストChristopher Wylie氏が、選挙工作のためにFacebook, Inc.の個人情報を不正流用したことを認めた※158。この不正流用は、Cambridge大学の心理学者であるAleksandr Kogan博士が研究目的としてFacebook上で実施した性格テストに端を発する。Facebook, Inc.は、同テストで収集された個人情報がCambridge Analyticaへ流出したことが判明した2015年に契約違反としてデータ削除を求め、削除したとの回答を得たとしているが、実際には8,700万人に上る個人情報が選挙工作に利用されたという※159。

プライバシー保護の点でFacebookのAPIに問題があることは以前から指摘されていたが、同社の対応は十分ではなかった。2018年4月11日の下院公聴会でMark Zuckerburg CEOはこれまでの対応が間違いであったことを認め、謝罪した※160。また同氏はSNSに対する規制についても必要性を認めた。今後、SNSやデータ分析に対する個人情報・プライバシーの保護、更にはフェイクニュースやマイクロターゲティング等による不正な世論誘導がナショナルセキュリティの問題として議論されることとなるが、欧州においてはGDPR遵守の視点からグローバル企業への要求が厳しくなることが予想される。今後の政策動向が注目される（GDPRについては「2.3.3 (3) GDPR実施の準備状況」参照）。

2.3.3 欧州のセキュリティ政策

欧州では2018年5月9日に、「ネットワークと情報システムのセキュリティに関する指令（The Directive on security of network and information systems）」（以下、NIS指令）に基づく国内法制の整備が期限を迎えた。NIS指令に基づき、基幹インフラ等を運用する重要サービス事業者、EC・クラウド・ネット検索等のデジタルサービス事業者が遵守すべきセキュリティ施策の実践がEU加盟国に求められるが、欧州委員会（European Commission）では、更に加盟国の連携強化のための体制強化施策を打ち出している。一方、2018年5月25日にGDPRが発効したが、各国はこれに対する準備を急ピッチで行ってきた。本項では、NIS指令に対する各国の準備状況と欧州委員会の施策、GDPR発効に対する各国の準備状況について述べる。

(1) NIS指令実装の準備状況

前述のように、EU加盟国は2018年5月9日までにNIS指令を国内法に組み込み、同年11月9日までに規則を適用すべきサービス事業者を確定する義務を負っている。また、EU加盟国はCSIRTネットワークの構築及び加盟国間の情報共有連携を求められている。

EU域内では、NIS指令実装の準備は法案成立以前から開始されていた。ドイツでは、NIS指令のひな型と呼べる構造を持ったドイツITセキュリティ法（German IT Security Law）が2015年に成立していたが、更に2017年6月24日、NIS指令実装法（NIS Directive Implementation Act）が発効し、NIS指令の適用対象となる重要サービス事業者（金融・保険、医療、輸送・交通、エネルギー、IT・通信、水・食料等の分野）が確定した※161。

フランスでは、2018年2月15日、フランス国民議会がNIS指令の実装法案を承認した※162。実際の法案運用は、NIS指令の成立に尽力してきた国家情報システムセキュリティ庁（Agence Nationale de la Sécurité des Systèmes d'Information：ANSSI）が行い、国内の重要サービス事業者・デジタルサービス事業者は重大インシデントについてANSSIに報告することとなる※163。

EU離脱が決定した英国においても、NIS指令、及び後述するGDPRの遵守は不変の方針である。英国のサイバーセキュリティを統括する国家サイバーセキュリティセンター（National Cyber Security Centre：NCSC）は、EU離脱決定直後の2017年8月からNIS指令実装案を国民に示し、意見聴取を行った。結果は2018年1月に公開され※164、更に4月20日にNIS指令実装法案であるネットワーク情報システム規則（The Network and Information Systems Regulations 2018）が議会に提出された※165。

(2) 更なる EU 加盟国の連携強化施策

2017 年 9 月 13 日、欧州委員会は、加盟国のサイバーセキュリティに関する連携強化のための政策パッケージとして、サイバーセキュリティ法案を発表した※166。本法案の概要は以下のとおりである。

- 欧州ネットワーク情報セキュリティ庁（European Union Agency for Network and Information Security：ENISA）の機能強化
  ENISA は EU 加盟国の情報ネットワークセキュリティ推進の中心組織で、ナショナルセキュリティ戦略の立案、ISACs を通じた脅威情報共有、各国 CSIRT の立ち上げ等を支援しているが、NIS 指令の実装や EU 規模のサイバー犯罪等の課題に比べ、現組織は小規模であり、付与されている権限も 2020 年 6 月に失効する。このため本法案は、ENISA の業務を規定する規則である Regulation（EU）526/2013 を廃し、恒久的で強力な権限を ENISA に与えるよう提案している（ENISA を EU Cybersecurity Agency と表現）。強化される機能には、各国のセキュリティ対策能力向上の支援、汎欧州サイバーセキュリティ訓練の定期実施、脅威情報共有、EU 規模の大事故における各国協調支援等が含まれる。
- 統合的なサイバーセキュリティ認証制度
  本法案は更に、IT 製品・サービスのセキュリティレベルを認証する新たな制度を提案している。このような公的認証制度としては ISO/IEC 15408 に基づく Common Criteria（CC）があるが、CC を相互認証する国は EU 域内でも 13 ヵ国にとどまる一方、英国・フランス・ドイツ等が独自の認証制度を持つため、各制度への個別対応が負担となり、EU 市場の分断化が起こり得る。ビジネスの IT 化によるデジタル単一市場（Digital single market）の実現は EU の基本戦略であり※167、本法案はそのために、統合的な欧州サイバーセキュリティ認証フレームワーク（European Cybersecurity Certification Framework）を提唱している。本フレームワークの具体化は、加盟国の認証監督機関等の支援を受けて ENISA が行い、技術的な手続きや運用は CC 等の既存制度を活用しつつ、新たに必要なスキームについては ENISA が策定、認証するとしている※168。ただし、本フレームワークの遵守は法律で定められる場合以外は自主的なもので、一律の規制はない。
  同提案に対するパブリックコメントでは、拙速・厳格な規制への反対、柔軟性の要請等の意見が出され※169、それらに配慮した結果、厳格な適用はされない形となっている。また、EU の情報通信技術関連産業団体であるデジタルヨーロッパ（DIGITALEUROPE）は、国際的な標準・認証への産業界の密接な関与が重要との立場を表明し、「産業界の自主的な行動規範の方が信頼性が高く実施可能であり、推奨されるべきだ」との慎重な見解を示している※170。統合的な認証制度の必要性は理解されているものの、実現は容易ではないと思われる。

(3) GDPR 実施の準備状況

2016 年に成立した GDPR※171 は、EU 市民の個人データの保護に関する包括的な規則である。GDPR は個人データに関する以下の三つの役割を定義し、その権利・義務を規定している。

- データ主体（Data Subject）：個人データが表現する、あるいは関係する個人。実質は EU 市民であり、サービス間の個人データ移転を容易にするデータポータビリティ、委託した個人データを消去する忘れられる権利等、データ主体の権利が強化された。権利保護範囲は EU 域内だけでなく、個人データが移転され得る第三国にも同等の保護が求められる。
- データ管理者（Data Controller）：個人データの処理の目的と手段を決定する。GDPR では、公共の組織や、大規模な個人データ収集または大規模な個人データ処理により事業を行う企業（データ管理者）は、データ保護責任者（Data Protection Officer：DPO）を選任して GDPR の遵守状況を各国の監督機関（Supervisory Authority）に報告しなければならない。
- データ処理者（Data Processor）：データ管理者を代行してデータ処理を行う。クラウド事業者等も含まれる。データ処理者はデータ管理者、または他のデータ処理者によって選任されなければならない。

GDPR 規則の違反行為に対しては制裁金が科せられるが、顧客への情報開示を怠った場合等の制裁金は最大で事業者の全世界年間売上高の 4%、または 2,000 万ユーロのどちらか高額な方、遵守状況報告義務に違反した場合等の制裁金は最大で全世界年間売上高の 2%、または 1,000 万ユーロのどちらか高額な方、という厳しいものである。

2018 年 5 月 25 日の GDPR 発効に向けて、欧州委員会、EU 加盟国で対応の準備が進められてきた。以下ではその状況を述べる。

(a)ガイドラインの追加

欧州委員会でGDPRを策定している第29条作業部会(Article29 Working Party)は2016年12月、データポータビリティ(WP242)、DPOの責務(WP243)、越境データ処理の管理・監督(WP245)に関する三つのガイドラインを公開したが、2017年以降もGDPRの円滑な実施に向けて各種ガイドラインを改訂または公開している※172。主なものを以下に挙げる。

- データ保護影響評価に関するガイドライン(WP248)
  2017年10月改訂。高リスクが想定されるデータ処理に義務づけられるデータ保護影響評価(Data Protection Impact Assessment:DPIA)の実施ガイドラインである※173。
- データ侵害通知に関するガイドライン(WP250)
  2018年2月改訂。個人データ侵害を監督機関に通知する方法・タイミングに関するガイドラインである。更なる明確化を求めるコメントもある※174。
- 自動決定及びプロファイリングに関するガイドライン(WP251)
  2018年2月改訂。GDPRでは、個人データの自動処理(プロファイリング)による決定に対し、特定集団排除等の人権侵害の懸念から異議を申し立てる権利が認められるが、WP251はその詳細に関するガイドラインである。公表直後には欧州銀行連合(European Banking Federation)が預金者保護に必要なプロファイリングに影響しかねないとコメントする※175等、難しい運用になると思われる。
- 制裁金に関するガイドライン(WP253)
  2018年2月改訂。違反行為に対する制裁金(過料)の設定に関するガイドラインである。GDPRといえば重い制裁金というイメージが定着してしまったが、実際には罰則は違反の程度に応じた段階的なものであり、効果、抑止力を総合的に考慮して決定すべきとしている※176。
- 合意に関するガイドライン(WP259)
  2018年4月公開。個人データの委託と処理に関する合意のガイドラインである。オプトイン形式の同意の取り方について、改めて注意を促している※177。
- 透明性に関するガイドライン(WP260)
  2018年4月改訂。データ主体、データ管理者、データ処理者間の情報共有に関する透明性確保のガイドラインである。

以上のように、第29条作業部会はGDPR発効直前までガイドライン改訂・公開を継続した。それだけ実践の課題が多いということでもあり、対応する組織・企業は規則・ガイドラインの十分な理解と準備が必要である。

(b)各国の国内法整備

GDPRの施行の詳細は厳密に規定されず、加盟国の国内法に委ねられる部分があるため、対応する組織・企業はEU域内の各国法制も精査する必要がある。各国の国内法で規定しておくべき事項として、例えば以下のようなものが挙げられている※178。

- 個人データ処理の適法性
- 情報サービスに関する子供の同意
- 特別なカテゴリー(思想信条、犯歴等の機微情報)のデータ処理
- 削除権(忘れられる権利)の例外
- 自動化処理による決定に対する異議申し立ての例外
- データ管理者・処理者の権限に基づく処理
- DPIAの詳細
- 制裁金が科されない場合の罰則
- 雇用データ管理における被雇用者の権利確保

以下では、主要国の国内法整備状況について述べる。

- ドイツ
  2017年7月5日、ドイツの新しいデータ保護法(Bundesdatenschutzgesetz)が成立した。GDPRに対応した初めての国内法として、同法の改正は2016年8月から議論されてきたが、紆余曲折を経てようやく成立したものである。同法はDPOの選任義務が発生する条件、雇用者データ処理が可能となる条件、犯罪行為の調査に関する制限、被雇用者の同意が成立する条件等について規定しており※179、ドイツで事業を行う企業は内容を吟味する必要がある。
- フランス
  2017年12月13日、フランス司法省により個人情報保護に関する法案(French Data Protection Bill)が国民議会に提出された。本法案は現行のフランスデータ保護法の改訂版であり、機微情報の管理等は従来形式を踏襲しつつ、GDPRと国内法を整合させる特例を追加している。また、フランス国民のデータを扱う国外のデータ処理者にも同法は適用されるとしている※180。本法案は2018年5月14日に承認された。なお、個人情報保護の実務を担当するCNIL(Commission Nationale de l'Informatique et des Libertés)は2018年2月の時点で、GDPRの運用

は柔軟に行うとし、2018 年は、GDPR により新しく適用される規則（データポータビリティ等）については「理解する」期間として、実施を猶予するとしている※181。

- 英国

  2017 年 9 月 14 日、英国デジタル・文化・メディア・スポーツ省は GDPR 規定に対する特例、あるいは拡張を含むデータ保護法案（Data Protection Act 2018）を公開した※182。特例には、例えば個人情報の処理委託合意に対する雇用者・研究者・報道関係者等への制限緩和、国内法と整合した子供の同意年齢規定が含まれ、更に保険事業者に対する制限緩和等の修正がなされた。2018 年 5 月 23 日、同法案は承認された※183。

(4) GDPR 実施後の課題

以上のように、GDPR のガイドライン策定や主要国の国内法整備は発効ぎりぎりまで時間がかかった。それほどに GDPR 運用は複雑であるといえる。

このような状況で 2018 年 3 月、Cambridge Analytica を介した Facebook の個人情報流出事故が発覚した※184（事故の概要は「2.3.2（7）個人情報保護・世論誘導に対する規制強化の可能性」参照）。情報流出は皮肉にも、GDPR が制限し、英国が特例で認めるとしている研究目的の個人情報利用を契機として起こったが、Facebook, Inc. と Cambridge 大学の研究者、同研究者と Cambridge Analytica の契約が英国データ保護法に違反していたかはまだ明らかになっていない。少なくとも、今後 GDPR の実施において、データ処理委託に関する合意の規定が厳しく運用されることは予想できる。

例えば米国の IT 系グローバル企業は、EU 市民と非 EU 市民のデータ管理を分ける等の対策を進めている※185が、EU 地域のビジネスに加え、EU 市民の個人情報を含めたデータ利活用、データアナリティクス等の新ビジネスでは、誰とどこまで合意をすれば GDPR 違反、あるいは加盟国の国内法違反にならないか、精査が必要であり、合意に対して十分な配慮が求められる。

更に、先の NIS 指令で重要サービス事業者、デジタルサービス事業者に指定された企業は、インシデント対応で NIS 指令と GDPR の報告義務に同時に対処しなければならない可能性がある。インシデント対応についても準備が必要である。

2.3.4 中国のセキュリティ政策

2017 年 6 月 1 日、中華人民共和国網絡安全法※113,186、いわゆる「ネットワーク安全法」が施行された。同法は、中国国内のネットワーク上の個人データ保護とローカライゼーション（国内保管）、国家セキュリティ・権利侵害に関する監視等を導入するもので、サイバー空間上での国家権力の優越の方針に基づく非常に統制色の強い法制である。6 月 1 日以降も施行の細則が決まらない状態が継続しており、中国で事業を行う海外企業はその影響について懸念を抱いている。

例えば同法のデータローカライゼーション要件については、中国で収集・生成した個人データの海外移転に対して、十分なセキュリティが担保されているか評価が必要、としており、この点で欧州の GDPR と同様なデータ主体の権利保護を志向していると考えられる。しかし GDPR とは対照的に評価の詳細が明らかにならず、企業は対応に苦慮している※187。

2018 年 2 月、Apple Inc. が iCloud にある中国人ユーザの個人データを中国のデータセンターに移行した。中国のデータセンターで利用される暗号は中国政府の管理下に置かれるため、この決定は中国政府による iCloud ユーザの個人情報チェックがはるかに容易になることを意味する※188。2015 年 12 月の San Bernardino 銃乱射事件で、米国司法省からのスマートフォン暗号解除要求を拒否した※189Apple Inc. にとっては難しい決断となった。このように、ネットワーク安全法の施行により、企業は中国人顧客の人権侵害や、自社の知的財産権（ソースコード等）開示等の問題に直面する可能性があるが、中国市場に参入する多くの企業は Apple Inc. のような対応をせざるを得ないと考えられる。

これまで、中国政府による露骨な介入があったわけではなく、中国政府高官も、ネットワーク安全法は事業と顧客の安全のためであることを強調している。その一方で、ネットワーク上の言論・コンテンツに対する規制強化の動きは顕著である。2017 年 5 月 2 日、国家インターネット情報弁公室は「インターネットニュース情報サービス管理規定」を発表し※190、中国の一般利用者に向けた Web サイト、ブログ、ライブ配信等のネットニュース配信は営業許可が必要であるとし、無許可のニュース配信を禁じた。本規定は 6 月 1 日から施行された。

2018 年 4 月 21 日、習近平国家主席は、中国は社会及び経済の目標達成に向け、インターネット規制を強化すべきとの考えを示す※191 等、更なる規制強化を推進

する構えである。その背景にはSNS等で自由に情報を発信・共有する若い世代の統制に対する懸念があり、ネットワーク上のコンテンツに対する政府の取り締まり、あるいはネットワーク事業者の自主規制の動きは継続すると思われる。

一方で、中国は自国内の事業のIT化、イノベーションで世界をリードすることへの自信を深めつつある。2017年12月3～5日、浙江省烏鎮にて第4回世界インターネット大会（4th World Internet Conference）が開催され、世界各国から1,500人が参加した。同会議ではデジタルエコノミーのためのサイバー空間の共同建設、「デジタルシルクロード」の構築に向けた議論が行われ、「中国インターネット発展報告書2017」「世界インターネット発展報告書2017」が公開された※192。同会議は例年烏鎮で開催されるが、毎回サイバー空間の民間の活動を国が規制する、という中国スタイルのインターネット利用をアピールする場となっており、そのような点から醒めた評価もされている。しかし、デジタルエコノミーにおける中国市場、中国企業のプレゼンスは今や確固としたものになっており、「経済の安定はネットワークの安全があってこそ」という習近平国家主席の主張※193も説得力が増す可能性がある。

サイバー空間のガバナンスに関して、日中の政府レベルのセキュリティ協議は、2017年2月の第3回日中韓サイバー協議以降実現していない。2018年4月15日、世耕弘成経済産業大臣は、第4回日中ハイレベル経済対話※194のために来日した鍾山中華人民共和国商務部部長及び張勇中華人民共和国国家発展改革委員会副主任と会談し、日中の経済協力推進を確認するとともに、知的財産、サイバーセキュリティ、貿易管理等において公正・自由で開かれた事業環境の整備が必要である、との日本側意見を伝えた※195。一方、2018年5月9日に東京で開催された第7回日中韓サミット※196における共同宣言では、サイバー分野に関する政策協議の強化を確認するに留まった。サイバー空間のガバナンス、あるいは安全なデジタルエコノミー実現に向けた本格的な折衝、合意形成は今後の課題である。

2.3.5 アジア太平洋地域でのCSIRTの動向

本項では、アジア太平洋地域における地域CSIRTの設立と機能強化に関する動き、CSIRT間の相互連携の実態について述べる。2017年5月にランサムウェアWanna Cryptor（別名WannaCry）により引き起こされた大規模サイバー攻撃では、アジア太平洋地域の国々でも広範囲にわたって感染の事例が報告された。こうした同時多発的なインシデントへの対応においては、個々のCSIRTが役割を発揮すること、また各国及び地域全体においてCSIRT間で連携をとることが一層重要となる。

(1) CSIRTの設立・機能強化の動き

各国のCSIRTの設立、機能強化の動きについて述べる。

(a) ニュージーランド

ニュージーランドのNational CSIRTであるCERT NZ※197が2017年4月11日にビジネス・革新技術・雇用省のもとに設立され、活動を開始した※198。このCSIRTの設立は、2015年に発表されたサイバーセキュリティ戦略※199に基づいて作られた行動計画に盛り込まれていた。インシデント対応の窓口機能を、これまでのナショナルサイバーセキュリティセンター（National Cyber Security Centre：NCSC）※200から引き継ぎ、既にCSIRTの連携フォーラムであるFIRST（Forum of Incident Response and Security Teams）※201へ加入する等、国際的なCSIRTコミュニティ活動を開始している。

(b) オーストラリア

2017年10月にオーストラリア外務省より「国際サイバー連携政策」が発表された。これは2016年に首相府が策定したサイバーセキュリティ戦略※202から、主にサイバーセキュリティにおける国際連携の指針を抜き出し、詳細化してまとめたものである。この中で、インド太平洋地域においてCSIRTの発足を支援し、連携を強化していくオーストラリア政府の方針が明記されている。また、同国のNational CSIRTであるCERT Australia※203が、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）※204をとおして地域のCSIRT間連携に貢献する方針も記載されている。CERT Australiaは、2015年9月から現在まで、APCERTの議長チームを務めている。

太平洋島嶼国においてはNational CSIRTの設立が進んでいないが、この地域のサイバーセキュリティに関する組織間連携の促進を目的とした取り組みPaCSON（Pacific Cyber Security Operational Network：太平洋サイバーセキュリティオペレーションネットワーク）を

オーストラリア外務省が開始し、CERT Australia がその活動の一端を担っている。PaCSON では、太平洋島嶼国のサイバーセキュリティ担当者を招いた年次イベントの開催や、インシデント対応に活用できるツールキットの配布、ベストプラクティスの共有等をとおして、各組織が限られたリソースの中でサイバーセキュリティ対応能力を向上させられるよう支援している。

(c) サモア

南太平洋に位置するサモアが、同国初のサイバーセキュリティ戦略※205 を 2017 年 2 月に通信・情報技術省から発表した。サイバー脅威を取り除き、サイバーセキュリティを強化・促進すること等、五つの目標を掲げている。具体的な行動計画には、2019 年までに National CSIRT を設立することを盛り込んでいる。この戦略では National CSIRT について、サイバー攻撃への対処や、サイバーセキュリティの促進等の機能の他に、サイバー犯罪捜査のためのコンピュータフォレンジックやインテリジェンス機能も持たなければならないとしている。

(d) セクター CSIRT 設立の動き

タイでは、TB-CERT（Thailand Banking Sector Computer Emergency Response Team：タイ銀行セクター CERT）が、タイ中央銀行と ETDA（Electronic Transactions Development Agency：タイ電子取引開発機構）の支援のもとで 2017 年 10 月に新設された※206。TB-CERT では、各銀行における IT システムの安定性・安全性の向上とサイバー攻撃への対処を行う。東南アジアでは、2016 年にバングラデシュ中央銀行を始めとして、いくつかの国で不正送金被害が確認された。こうした状況から、サイバーセキュリティを確保する体制整備の必要性が改めて認識され、TB-CERT が新設されることとなった。また、スリランカやインド、台湾等においても、金融セクターが CSIRT を設立した。

更に、金融以外のセクターにおいても、学術や地方自治体等、セクターごとに CSIRT を設立する動きがアジアの複数の国において活発に見られた。

(2) アジア太平洋地域の CSIRT 間連携

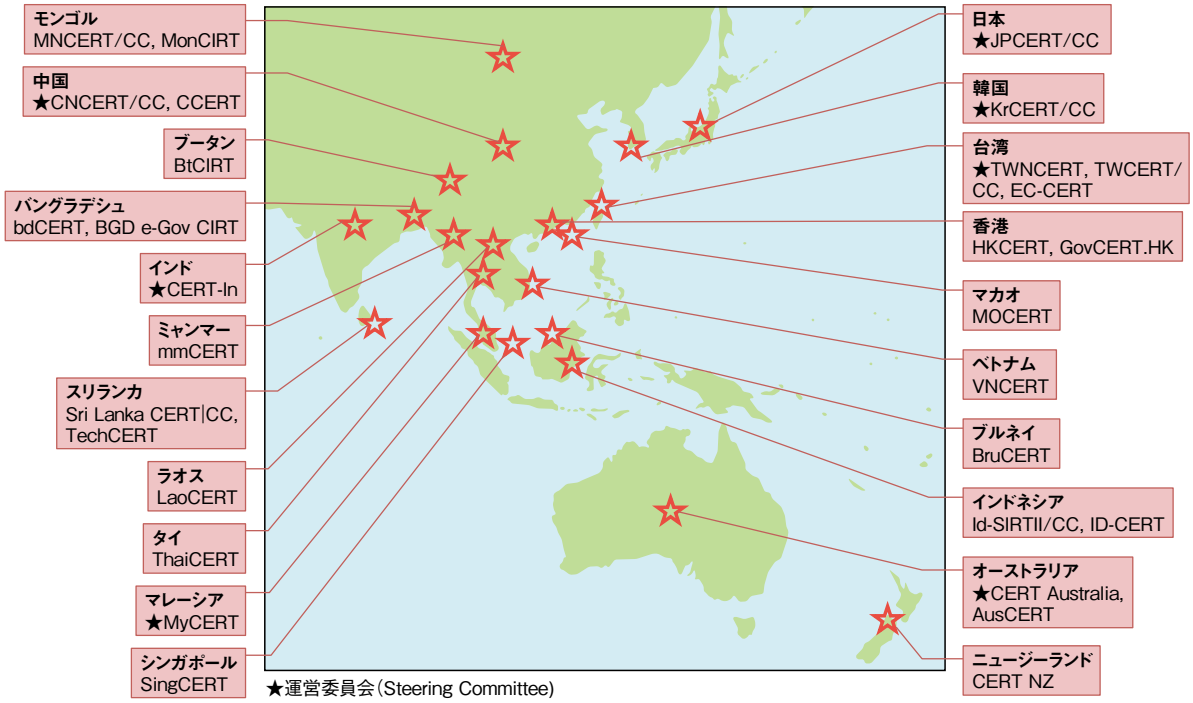
国境を越えた対応が必要なインシデントや、広範囲に存在するサイバー脅威に対応するためには、前述のような個々の CSIRT の活動に加えて、関係する CSIRT が連携する必要がある。その基礎を作るための、アジア太平洋地域の CSIRT コミュニティとして APCERT があり、地域内で発生したインシデントへの対応協力の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003 年の設立当初の参加メンバーは、12 の国・経済地域で活動する 15 チームだったが、National CSIRT の立ち上げが進んだことや、CSIRT 間での脅威情報の共有等の重要性が高まりつつあることから年々メンバーが増えている。2017 年にはバングラデシュ、ブータン、ニュージーランドから新たに 3 チームを主要メンバーであるオペレーショナルメンバーとして迎え、2018 年 5 月末現在 21 の国・経済地域の 30 チームが参加している（次ページ図 2-3-1）。

JPCERT/CC は、2003 年の APCERT 設立当初から事務局を務め、運営委員会の一員としても APCERT の組織運営を支えている。

APCERT の主な活動は、年次報告書の発行や年次会合の開催、年次サイバー演習の実施である。年次報告書は、APCERT 全体としての活動に加えて各チームの組織概要や各チームが対応したインシデントの統計等をまとめた文書で、Web サイト上で公開されている※207。

APCERT では、各チームにおけるインシデント対応体制の再確認と、CSIRT 間の連携訓練のため、アジア太平洋地域に存在するサイバー脅威を題材に取り上げて、2007 年より毎年サイバー演習を実施している。2017 年の演習は、「新たな DDoS 脅威への対応」をテーマに 3 月に実施され、ウイルスに感染しボット化した IoT 機器により引き起こされる DDoS 攻撃を想定した対応を訓練した※208。この演習は、APCERT メンバーだけでなく OIC-CERT（Organisation of The Islamic Cooperation – Computer Emergency Response Team：イスラム協力機構コンピュータ緊急対応チーム）※209 に加盟する CSIRT も招待し、合計 22 の国・経済地域から 27 チームの参加を得て行われた。

2017 年の APCERT 年次会合は、インドの CERT-In（Indian Computer Emergency Response Team）※210 が主催し 11 月にデリーで開催された。初めてサモア、トンガ、バヌアツからの参加者を迎え、地域の CSIRT ネットワークの更なる拡充に努めた。また、本会合で CERT-In が初めて運営委員会のメンバーに選出されたほか、JPCERT/CC は運営委員会及び事務局の役職に再選された。年次会合の期間中には、JPCERT/CC が APCERT メンバーを中心とした組織に呼びかけて実施している、共同ネットワーク定点観測プロジェクト「TSUBAME※211」のワークショップが併催され、前述の Wanna Cryptor のパケット観測動向に関する情報の



■図 2-3-1　APCERT オペレーショナルメンバー(2018 年 5 月末現在)

共有や、観測によって得た情報をどのようにインシデント対応に活かすかを実践的に学ぶハンズオン講習が行われた。2018 年 5 月末現在、TSUBAME プロジェクトにはアジア太平洋地域の CSIRT を中心に 21 の国・経済地域から 27 チームが参加し、観測動向を共有している。

APCERT は、アジア太平洋地域でより多くの CSIRT が連携できる環境作りを目指しており、ネパールやフィリピン、太平洋島嶼国等、APCERT に加盟していない国の CSIRT やサイバーセキュリティ関係組織とも連携を図っている。

ASPI (Australian Strategic Policy Institute：オーストラリア戦略政策研究所)[※212] が毎年公表している報告書の最新版「Cyber Maturity in the Asia Pacific Region 2017[※213]」(アジア太平洋地域におけるサイバー成熟度調査 2017 年版) では、CSIRT 機能の項目において日本が最も高い評価を獲得した。これは、APCERT や FIRST のような国際的な CSIRT コミュニティでの連携活動や、技術面での情報発信、能力構築支援等を含む JPCERT/CC の継続した取り組みを反映したものと考えられる。その他にも、オーストラリア、マレーシア、ニュージーランド、韓国が CSIRT 機能について高評価を受けている。一方で、その他のアジア太平洋各国においては CSIRT 機能の評価や国際連携のレベルに差がある状況が浮き彫りになっており、APCERT による地域での連携の役割が今後ますます重要となる。

2.4 情報セキュリティ人材の現状と育成

国内のサイバーセキュリティに関わる人材は質的にも量的にも不足しており、人材育成は各界が協力して解決すべき問題である。教育の充実、高度な人材の育成・確保、セキュリティ人材が将来にわたって活躍できる社会環境の整備等、様々な課題が挙げられている。本節では、セキュリティ人材の現状と、産学官における人材育成の取り組みについて述べる。

2.4.1 人材育成の政策と実施状況

サイバーセキュリティ戦略本部が 2017 年 4 月に公開した「サイバーセキュリティ人材育成プログラム」において、2017 年度から 2019 年度を対象期間としたサイバーセキュリティ人材の課題と在り方が検討されている。また 2017 年度の施策はサイバーセキュリティ戦略の年度計画である「サイバーセキュリティ 2017」に盛り込まれている。本項では、主にこの二つの文書に基づいて、政府の人材育成政策とその実施状況について述べる。

(1) 状況の変化を踏まえた新たな取り組み

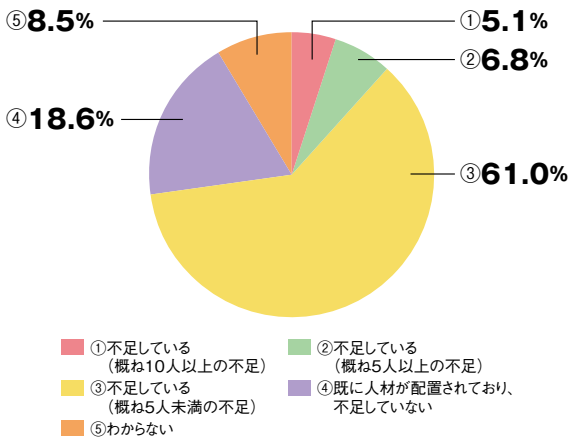
「サイバーセキュリティ人材育成プログラム」では、これまでの取り組み、すなわちサイバーセキュリティ技術人材の育成や企業経営層の意識改革による対策推進に加え、IT を利用したビジネスイノベーションへの挑戦が求められている状況に照らして、新たな取り組みが必要と指摘している（表 2-4-1）。

企業における人材の各層	新たな取り組み
企業の経営層	ビジネスにおける「挑戦」とそれに付随する「責任」としてのサイバーセキュリティに取り組むための意識改革を図る
橋渡し人材層	ビジネス戦略と表裏一体を成すサイバーセキュリティの企画・立案を行い、実務者層を指揮できる人材を育成する
実務者層	チームとなってサイバーセキュリティを推進するための人材を育成する

■表 2-4-1　企業における各層人材別の新たな取り組み
（出典）サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」を基に IPA が作成

(a) 橋渡し人材の育成

経営者自らがサイバーセキュリティをどのようにビジネスと結びつけるか具体的に企画し、実務者層を指揮し、セキュリティ対策を推進することは一般に困難である。そこで経営層の補佐役として、サイバーセキュリティの素養だけでなく、その企業の経営戦略・ビジネス戦略を理解し、セキュリティを具体的な業務課題としてとらえることができる「橋渡し人材」が必要とされている。図 2-4-1 は、橋渡し人材の充足状況について、日経 225 銘柄構成企業に対して NISC がアンケート調査を行った結果である。橋渡し人材が必要であるとした企業のうち 7 割以上が、こうした人材が不足していると回答しており、どのように育成・確保していくかが課題となっている。



■図 2-4-1　企業における橋渡し人材の充足状況
（出典）サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」を基に IPA が編集

NISC は、普及啓発・人材育成専門調査会の「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ」において、人材像の明確化、育成カリキュラムの方向性の提示等に取り組み、今後の取り組みの方向性について次期「サイバーセキュリティ戦略」に反映するとしている※214。

(b) チームとなって推進する人材の育成

IT が様々なビジネスに深く関与し重要な役割を担うようになるにつれて、サイバーセキュリティは技術だけでなく、システムやサービスの運用、組織の運営・管理といった総合的な対策によって実現することが必要になっている。サイバーセキュリティの企画・実現・運営は、従来とらえられていたような情報システム部門が単独で担うべき業務ではなく、様々な役割・専門性を持った人材が組織横断的に連携し、チームとして担うべき業務となった※6。そこで、これまでサイバーセキュリティに関する役割を与

えられなかった人材も含めて、セキュリティの知識・能力を高めてチームに参画できるよう、社会人の「学び直し」の機会創出が推進されつつある。

例えば、文部科学省の取り組み「成長分野を支える情報技術人材の育成拠点の形成（enPiT※215）」では、社会人対象の短期の学び直しプログラムを開発・実施している。また、IPA の産業サイバーセキュリティセンターでは、企業のセキュリティ対策に関わる人材を集め、模擬プラントを用いた安全性の検証や、早期復旧等のマネジメントを含む実践を体験する演習が行われている（「2.4.1(3)産業サイバーセキュリティセンター」参照）。

更に、国立研究開発法人新エネルギー・産業技術総合開発機構の「戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保」において、重要インフラ事業者の運用技術者を育成するため、カリキュラムの開発を行っている。国立大学法人名古屋工業大学において、電気、ガス、石油、化学プロセス等の重要インフラにおける安全と事業継続の観点で、事前対策としてのセキュリティ対策を適切に立案でき、サイバー攻撃によるインシデントが発生したときにはいち早く対応し、早期復旧を実現できる人材を育成するための演習を開発している※216。

(c)高度人材の育成

このほか、サイバーセキュリティ戦略本部はセキュリティ技術のイノベーション人材育成の取り組みを行うとし、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、若年層を対象に高度なセキュリティ技術を指導し、将来の研究者・起業家の育成に取り組むとしている。

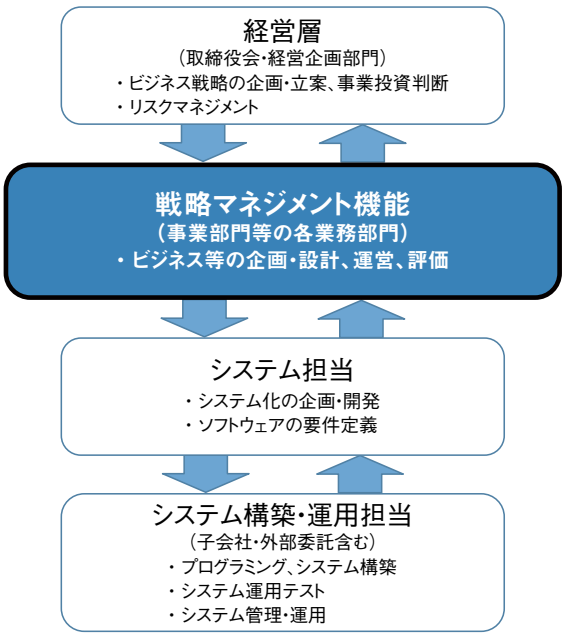
(2) 人材育成の質を高めるための新たな取り組み

「サイバーセキュリティ人材育成プログラム」では、サイバーセキュリティ人材像について産学官の認識共有が必要であり、また各施策の効果を高めるために、施策間の連携強化を促進するとしている。

前述の「サイバーセキュリティ 2017」ではこれを受け、内閣官房において施策間連携を図る「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ」を設置し、具体的な人材育成カリキュラムの策定等を行うとしている。

本ワーキンググループが主に検討する事項は、次のとおりである※217。

- 企業において育成すべき各層（経営層、戦略マネジメント機能（図 2-4-2）、システム担当、システム構築・運用担当）別の人材像やキャリアパスの明確化
  - 特に各部門におけるセキュリティを含めた戦略マネジメント機能を担う人材
  - 高度人材の定義、位置付けの整理
- 人材育成の前提となる IT の基本的知識の明確化、それを踏まえた各層別のカリキュラムの方向性
- 各省の人材育成施策に関する全体像の整理、連携策の検討推進
- カリキュラムに基づく教材の R&D 推進
- 人材育成・確保に向けた産学官連携の在り方・具体策の明確化



■図 2-4-2 「戦略マネジメント機能」担当人材の位置付け
（出典）NISC「サイバーセキュリティ人材育成の検討の方向性（案）※218」を基に IPA が作成

上記の「戦略マネジメント機能」を担う人材は、これまで橋渡し人材と呼んでいた層を想定しているが、名称は別途検討することとなっている。第 2 回会合（2017 年 9 月 14 日）の資料「サイバーセキュリティ人材育成の検討の方向性（案）」では、この層に求められる役割として、次の事項等を挙げている。

- 事業分野に関する能力・経験に加え、戦略マネジメント機能の遂行に必要となるセキュリティ知識・スキル、IT に係る基本的知識等を習得
- 事業に関するセキュリティリスクが事業利益・企業価値に与える影響を把握・分析し、経営層に適確に説明
- サプライチェーンを意識しつつ、セキュリティ要件を含めてシステム部門を指揮

これらの内容を踏まえ、今後の取り組みの方向性は、2018年夏ごろに策定する次期「サイバーセキュリティ戦略」に反映するとしている。

(3) 産業サイバーセキュリティセンター

近年、社会インフラや産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大しており、海外では、国家等からなされたとされるサイバー攻撃により社会インフラや産業基盤の安全が脅かされる事案が報告されている。このような状況のもと、我が国の経済・社会を支える社会インフラや産業基盤のサイバー攻撃に対する防御力を強化するために、2017年4月1日、IPAは、制御技術(Operational Technology：OT)と情報技術(IT)の知見を結集させたサイバーセキュリティ対策の中核拠点として、産業サイバーセキュリティセンター(Industrial Cyber Security Center of Excellence：ICSCoE)を発足させた。

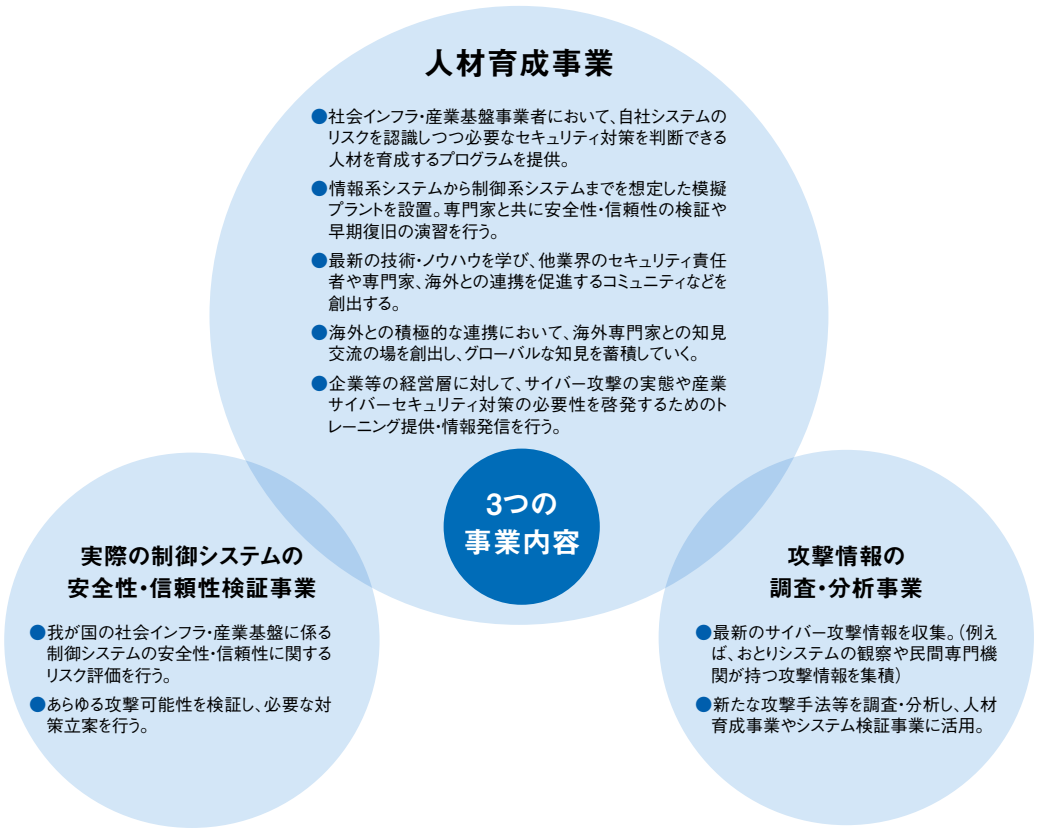
産業サイバーセキュリティセンターでは、社会インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている(図2-4-3)。ここでは、そのうち「人材育成事業」について、特徴と2017年度の実施状況を述べる。

(a) 人材育成事業の特徴

社会インフラや産業基盤のサイバー攻撃に対する防御力を強化する観点から、どのような人材が必要かについて、経済産業省が有識者・関係業界に対して行ったヒアリングによれば、あるべき人材像として以下のような特徴が挙げられた。

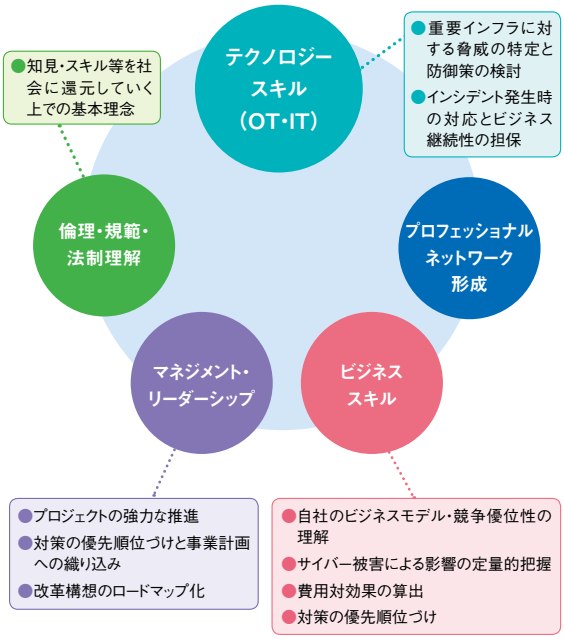
- 自社システムの安全性・信頼性を客観的に評価し、自社のサイバーセキュリティ戦略の立案や経営リスク・財務リスク等を含めて自社内幹部へ説明できる。
- 最新のサイバー攻撃のトレンドに精通し、他業界や海外の対策状況等を把握し、自社の対策立案に効果的に反映できる。
- 実装するサイバーセキュリティ対策の安全性・信頼性や必要な技術・コストを精査でき、内製化すべき対策・アウトソースすべき対策を見極めて、効率的かつ確実に導入できる。

これらを踏まえ、産業サイバーセキュリティセンターでは、社会インフラや産業基盤の運用の鍵となるOTと



■図2-4-3　産業サイバーセキュリティセンターの三つの事業内容
(出典)IPAの事業案内パンフレット※219を基に作成

IT の双方のスキルを核とした上で、サイバーセキュリティ対策の必要性を把握し、プロジェクトを強力に推進していく力の養成に重点を置くこととした（図 2-4-4）。



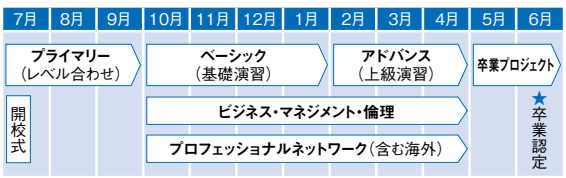
■図 2-4-4　目指すべき産業サイバーセキュリティ人材像
（出典）IPA の事業案内パンフレット

発足初年度である 2017 年度は、テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ 1 年間のトレーニングとして「中核人材育成プログラム」を 7 月に開始したほか、CEO、CIO・CISO、部門長等、責任者クラス向けのトレーニングとして 6 回の「短期プログラム」を実施した。

(b) 中核人材育成プログラム

2017 年 7 月に開講した第 1 期中核人材育成プログラムには、電力・ガス・鉄鋼・石油・化学・自動車・鉄道・放送・通信等の幅広い業界から計 76 名の受講生が参加した。

同プログラムは、図 2-4-5 に示すように、3 ヵ月程度の初歩的な「レベル合わせ」からハイレベルな「卒業プロジェクト」までを 1 年間かけて実施する。



■図 2-4-5　中核人材育成プログラムの年間カレンダー
（出典）IPA の事業案内パンフレット

カリキュラムは OT 分野の「防衛技術・ペネトレーション手法」「インシデント対応・BCP」、IT 分野の「IT セキュリティ」の 3 領域を基軸としつつ、ビジネス、マネジメントに関する実務家の講義や、米国やイスラエルの海外先進事例を学ぶ講義・演習を含む構成となっている。例えば、2017 年 9 月には、DHS の制御システムセキュリティ担当部門である ICS-CERT の専門家が来訪し、同チームが米国アイダホ国立研究所（Idaho National Laboratory）において提供しているトレーニングを同プログラムの全受講者に提供した※109。また、同年 11 月には、同年 5 月に合意された「日イスラエル・イノベーション・パートナーシップ」等に基づきイスラエルの官民有識者が来訪し、イスラエル国家サイバー局高官による同国の重要インフラサイバーセキュリティ戦略に関する講義や、イスラエル電力公社の CEO によるサイバークライシスマネジメント演習等が提供された。

第 1 期中核人材育成プログラムの受講者は 2018 年 6 月に同プログラムを修了する予定で、修了者には情報処理安全確保支援士の試験免除資格が付与される。

(c) 短期プログラム

産業サイバーセキュリティセンターでは、CEO、CIO・CISO、部門長等、責任者クラス向けのトレーニングを提供することとしているが、こうした対象者が 1 年を通じて中核人材育成プログラムに参加することは実質的に困難と判断されたことから、2017 年度は、実践演習を中心とした 2 日間の短期トレーニングの形式で提供することとした。

この短期プログラムは、OT を扱う事業領域を広く対象とし、米国のサイバーセキュリティの専門家がファシリテーターとなって机上演習を中心に実施する「業界共通トレーニング」と、業界固有の最新動向や業界別に考慮すべきセキュリティ要件や安全性要件を織り込んだ「業界別トレーニング」の二本立てとし、2017 年度はそれぞれ 3 回実施した。

- 業界共通トレーニング

  2017 年度は、2017 年 7 月、10 月及び 2018 年 3 月に実施した。米国サイバー軍等の退役軍人や重要インフラ関連企業のサイバーセキュリティ対策責任者らが講師やファシリテーターとなり、経営者の判断をサポートするためのリスク分析、迅速かつ適切な対策の提示、政府機関やマスメディアを含む会社内外の様々なステークホルダーとのコミュニケーション等、CISO がインシデント対応時に求められる役割について理解を深め、実践につなげるための講義や演習が提供され

た。演習では、2020 年東京オリンピック・パラリンピック競技大会を想定したサイバー攻撃のシナリオを基に、CISO や広報担当、事業部長等の役割を受講者が演じ、経営判断まで含めたプロセスを疑似体験することで、実践的なインシデント対応のフレームワークを学習した。

受講者は、電力、ガス、石油、化学、鉄鋼、自動車、製薬、食料品、電気機器、輸送機器、電子部品、情報通信機器等、多岐にわたる業界から集まった。

- 業界別トレーニング

2017 年度は、2017 年 8 月に「電力、不動産・ビル管理（ディベロッパー）」、同年 11 月に「自動車、FA（Factory Automation）」、2018 年 2 月に「金属・石油精製・素材（PA：Process Automation）」を対象業界として実施した。

業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだ構成とし、仮想企業を想定したシナリオ形式による実践演習を中心に進められた。演習には受講者に加え、講師としてサイバーセキュリティ専門家や監督省庁の関係者も加わった。

これらの短期プログラムの受講者からは「CISO の仕事が非常に幅広く、会社としてどう実現していくべきかを考えるきっかけとなった。社内外の関係部門との調整や、重要インフラの分野間連携の重要さに気づいた。経営層の巻き込みに努力したい。」「ドローンによる電波ジャミングや、3D プリンタによる偽造鍵による侵入といった、従来のセキュリティインシデントの概念から大きく外に広がるテーマも扱っており、セキュリティ対策に対する価値観の変化を伴う驚きがあった。」等の感想が寄せられた。

2.4.2 情報セキュリティ人材育成のための資格制度

情報セキュリティ人材に求められる IT スキル資格に関する動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業においては、上位組織が定めた情報セキュリティポリシーを部門内のメンバーに周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2015 年 10 月、「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が創設され、2016 年度春期試験より開始された。2017 年度の応募者数は 4 万 2,069 人であった[※220]。

同試験は、業種や組織を問わず、部門内で個人情報を取り扱う担当者や外部委託の担当者、情報システム担当者等を主な対象者としている。2017 年度の受験者のうち約 9 割を社会人が占めており、更に勤務先別に見ると、IT 系企業が 57.7%、非 IT 系企業が 42.3% と、非 IT 系企業が 4 割を超えている。非 IT 系企業の業種も、製造業、サービス業等、幅広い業種の人が受験していることから、広く組織の情報セキュリティを推進する人材の育成に有効な試験と考えられていることがうかがえる[※221]。

(2) 情報処理安全確保支援士

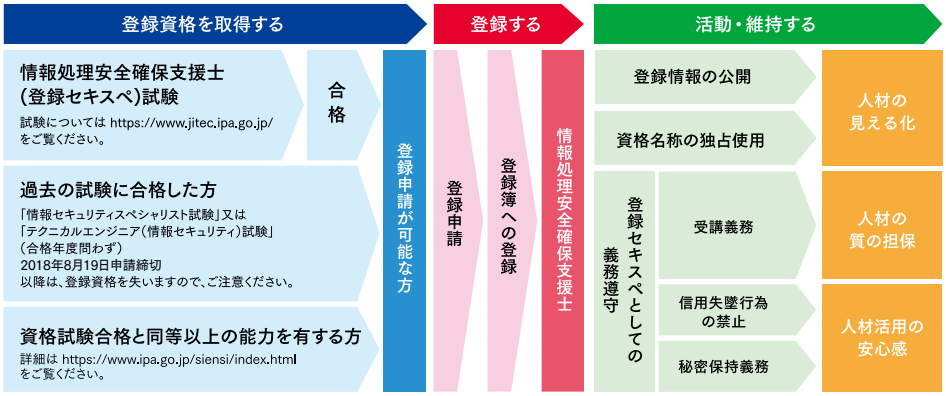
サイバー攻撃の急激な増加により、企業等におけるサイバーセキュリティ対策の重要性が高まる一方、対策を担う実践的な能力を有する人材は不足している状況である。

そこで、2016 年 10 月、「情報処理の促進に関する法律」の改正法が施行され、最新のサイバーセキュリティに関する知識・技能かつ実践的な人材に関する新たな国家資格「情報処理安全確保支援士」（以下、登録セキスペ）制度が創設された。制度の全体像を図 2-4-6（次ページ）に示す。本制度により、サイバーセキュリティ対策を担う専門人材の育成と確保を目指す。

登録セキスペは、試験合格後、登録簿に登録されることにより資格を取得できるサイバーセキュリティ分野初の名称独占資格[※223]である。登録セキスペの登録人数は、2018 年 4 月 1 日時点で 9,181 名となった[※224]。また、2017 年度試験の応募者数は 4 万 8,555 人であった[※220]。政府は、2020 年までに 3 万人の登録セキスペが誕生することを目標としている。

登録セキスペの登録者には、情報セキュリティに関する高度な知識・技能を保有する証になる、法定講習を受講することにより最新知識や実践的な能力を維持できる、といったメリットがある。登録者は毎年 1 回のオンライン講習と 3 年に 1 回の集合講習の受講が義務付けられており、受講者からは、「情報セキュリティ従事者としての倫理的責任について学べて良かった」「他業種の方のセキュリティについての目線の違いが得られ、考え方の幅が広がった」等の声が上がっている[※225]。

企業・組織においても、本資格保有者が在籍することで、提供する機能やサービスの信頼性向上、社会的評価・信頼の向上、ビジネスチャンスの拡大といったメリッ



■図 2-4-6　情報処理安全確保支援士制度の全体像
(出典)IPA「制度について※222」を基に編集

トが期待できる。内閣官房情報通信技術(IT)総合戦略室と総務省行政管理局が定めた「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第3編第6章 調達)※226」において、作業要員に求める資格等の要件を記載する一例として登録セキスペが例示されており、今後登録セキスペの配置が入札要件となる案件が増えていくことが予想される。

今後、組織における情報セキュリティ確保や、セキュリティ人材の育成・強化に、ますます登録セキスペが活用されることが期待される。

2.4.3 情報セキュリティ人材育成のための活動

情報セキュリティに関する情報共有や情報セキュリティ人材育成の場として、様々なイベントが開催されている。また、複数の大学と産業界がネットワークを形成し、セキュリティ分野の人材を育成する事業が行われている。

(1) セキュリティ・キャンプ

セキュリティ・キャンプは、22歳以下の若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘･育成する場として、一般社団法人セキュリティ・キャンプ協議会とIPAが運営している。2017年8月14～18日に東京都で14回目となる全国大会が開催され、82人が参加した※227。今回、新たに3日間連続で特定の分野を学ぶ「集中コース」が設置された。本コースでは、受講者が三つの開発テーマから一つを選択し、ハッカソン※228形式による開発演習が実施された※229。

また、主に若年層を対象としたセキュリティ・ミニキャンプもセキュリティ人材育成に関心の高い地域（近畿（神戸)／九州(福岡)／山梨／宮崎／中国(広島)／北海道(札幌)／東北(盛岡)／北陸(金沢)／沖縄／四国(徳島))で開催された※230。更に、中学生以下の若年層を対象としたジュニアキャンプ(高知)が開催された※231。

その他の活動として、過去のセキュリティ・キャンプ全国大会を修了した25歳以下の学生を対象に、キャンプ後の更なる育成の場としてセキュリティ・コアキャンプが開催されることとなり、第1回が2017年8月16日に東京で開催された※232。また、2017年に引き続き、情報セキュリティに関連する取り組みをテーマとしてプレゼンテーションを行う場を設け、優れた成果を上げた人や価値のある取り組みについて表彰するセキュリティ・キャンプアワードが2018年3月16日に東京で開催された※233。

(2) enPiT

enPiT(Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成拠点の形成）は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するため、産学協働の教育ネットワークを形成し、PBL（Problem Based Learning:課題解決型学習)等の実践的な教育を推進･普及することを目的とした事業である。2012～2016年度までは大学院生を対象とした事業「第1期enPiT」が実施され、これを踏まえ2016年度（同年度は準備期間の位置付け）から、学部生を対象とした事業「第2期enPiT(以下、enPiT2)」を開始している。

enPiT2は、ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの4分野を対象として教育プログラムを提供している。セキュリティ分野では、2017年度は大学等24校、連携企業等20社・団体が参加した。このうち、国立大学法人東北大学を中核とした14の大学が、高度化する情報セキュリティの脅威を理解し、リスクマネジメントに必要な知識、基本技術、

実践力を備えた人材を育成する Basic SecCap コースを運営しており、251 名が修了認定を取得した※234。

上記以外でも、2017 年度から、社会人を対象に情報科学技術分野を中心とする体系的かつ高度で短期の実践教育プログラムとして、enPiT-Pro が設置された※235。セキュリティ分野では、情報セキュリティ大学院大学、国立大学法人東北大学、同大阪大学、同和歌山大学、同九州大学、長崎県公立大学法人長崎県立大学、慶應義塾大学の 7 大学が、enPiT-Pro Security という教育コースを共同で運営することになった※236。

(3) SECCON 2017

特定非営利活動法人日本ネットワークセキュリティ協会（Japan Network Security Association：JNSA）は、日本における最大規模の CTF※237 大会である「SECCON 2017※238」を開催した。

2018 年 2 月 18 ～ 19 日の国際決勝大会では、102 の国と地域から参加した延べ 1,794 チーム（4,347 人）の中からオンライン予選を勝ち抜いた 12 チームと、特別招待枠 3 チームの計 15 チーム（日本から 3 チーム、台湾 4 チーム、中国 3 チーム、米国 2 チーム、韓国、ポーランド、インドネシア各 1 チーム）が集まり実力を競い合った。優勝チームは韓国の「Cykor」となり、今回で韓国のチームが 4 年連続の優勝であった※239。また、本大会では、NICT がサイバー攻撃統合分析プラットフォーム「NIRVANA 改 SECCON カスタム Mk-Ⅳ」を導入し、CTF の様子をリアルタイムで可視化して把握できるようにした※240。

SECCON 2017 ではその他、学生限定の地方大会、女性限定の CTF ワークショップ、CTF 入門者向けワークショップ、他団体と連携した大会が開催された。各イベントでは、暗号やネットワークをテーマとした講義・演習の実施、クイズ形式の CTF の実施、競技用に作成したスマートフォンゲームのチート（課金を回避する等の不正）手法を競う等、様々な取り組みが実施された※241。

(4) 産学情報セキュリティ人材育成検討会

JNSA の産学情報セキュリティ人材育成検討会は、2012 年 2 月に発足し、今後の情報セキュリティ業界を支える人材を育成するためのインターンシップの支援活動を実施している。2017 年度は、将来情報セキュリティ業界で活躍したいと考える学生に対し、インターンシップの受け入れを検討している企業との交流の場を提供する「産学情報セキュリティ人材育成交流会～インターンシップに向けて～」を 2017 年 4 月 29 日に開催した。2017 年度は企業 12 社がインターンシップを実施した※242。また、2017 年 11 月 25 日には「これからの IT 人材のキャリアを考える～サイバーセキュリティの視点から～」と題して、学生または社会人 1 ～ 2 年目程度を対象に、キャリアアップに関するセミナーを実施した※243。

(5) 産業横断サイバーセキュリティ人材育成検討会

産業横断サイバーセキュリティ人材育成検討会※244 は、「産」が「学」や「官」と連携・協調しながら様々なセキュリティ問題を自主的に乗り越えていくことを目指し、「人材育成」「情報共有」「産学連携」を推進する民間の会議体である。2017 年 4 月より、一般社団法人サイバーリスク情報センターの委員会活動に位置付く会議体に活動を移行した。同検討会には重要インフラ分野を中心とした企業 34 社が参加している。

同検討会の第一期（2015 年 6 月～ 2016 年 6 月）の成果物の一つとして「人材定義リファレンス※245」が公表され、企業におけるサイバーセキュリティ関連活動で必要な業務上の役割が示された。しかし、その役割に至るまでのキャリアパスは示されず、同検討会の参加企業においてもセキュリティ関連のキャリアパスは明確ではなかった。このようにキャリアパス具体化のニーズが見込まれたため、同検討会の人材育成 WG では、2016 年 10 月～ 2017 年 9 月までの期間（第二期中間時点）において、まず企業におけるセキュリティ人材のキャリアパスを以下の三つにモデル化した。

- ゼネラリスト：企業における（ライン）マネジメントを行う人材
- エキスパート：自社事業とセキュリティ活動をよく知り、現場と経営をつなぐ人材
- スペシャリスト：専門的技術を持った人材

既にゼネラリストとスペシャリストのキャリアパスは確立しているが、エキスパートについては、ユーザ企業内で育成すべき人材としてキャリアパスの確立が必要であると同 WG は考え、現在も検討を継続している※246。

2.5 情報セキュリティマネジメント

経済社会の活動基盤として、サイバー空間が急速に拡大している。個々の組織・企業においては経営層がリーダーシップを取り、サイバーセキュリティリスクに対処することが求められる。本節では、情報セキュリティマネジメントに関する経営層の認識や企業の取り組み、ISMS 等の情報セキュリティマネジメントの動向について述べる。

2.5.1 情報セキュリティと経営

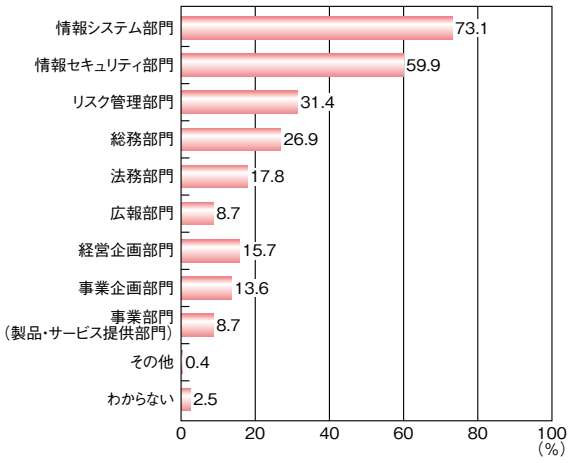
「サイバーセキュリティ経営ガイドライン※247」では「サイバーセキュリティは経営問題」であるとしており、経営者はリーダーシップを発揮して対策を進めること、自社だけでなく委託先等も含めたサプライチェーンに対してセキュリティ対策を施すこと、関係者間でセキュリティに関する情報を共有すること、の三つの原則を示している。本項では、経営者のセキュリティに関するリーダーシップを支える仕組みの実態とサプライチェーンに対するセキュリティ対策の強化について述べる（サイバーセキュリティ経営ガイドラインについては「2.1.2 (1) サイバーセキュリティ経営ガイドラインの改訂」参照）。

(1) 経営者のリーダーシップを支える仕組みの強化

セキュリティ対策推進のためには、経営者のリーダーシップが必要であるとされている。しかし、セキュリティ対策の企画・立案や、社内関係部署が必要な連携を行うためのマネジメントには、セキュリティに関する一定の専門性が必要とされるため、経営者自らがこれを実行するのは現実的でないとの指摘がある※246。そこで、セキュリティ対策を担当する CISO 等の幹部を任命することや、セキュリティ対策の策定・実施に必要な知識・業務経験を備えた複数の人員でチームを構成し※6（ここでは「セキュリティ推進チーム」と呼ぶ）、経営者を補佐すること等、経営者のセキュリティに対するリーダーシップを支える仕組みが必要となる。

IPA が 2017 年度に実施した「CISO 等セキュリティ推進者の経営・事業に関する役割調査※248」では、日本企業の CISO 等情報セキュリティ責任者及びその補佐役の役割について調べている。同調査によると、CISO 等を任命している企業の 9 割以上で、セキュリティ推進チームを設置していた。

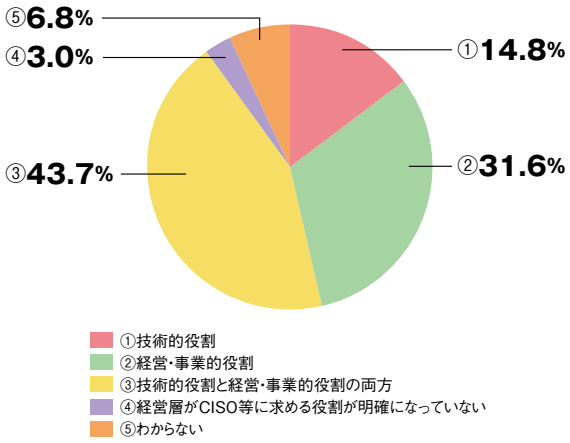
図 2-5-1 は、セキュリティ推進チームのメンバーの出身・所属部署を示している。多くは情報システム部門、セキュリティ部門であるが、リスク管理、法務、広報、経営・事業企画等幅広い業務部門からメンバーが構成されていることが分かる。



■図 2-5-1　CISO 等をサポートするメンバーの構成（n=242）
（出典）IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」を基に編集

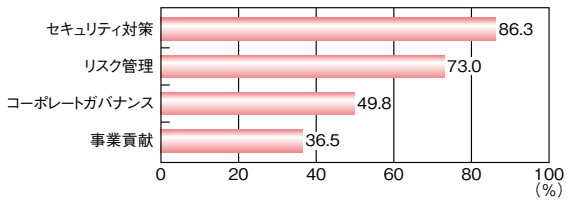
企業における IT の利用は、従来の業務効率化を目的とするものだけでなく、IT なしでは成り立たない事業（電子商取引、ネットを利用したマーケティング、クラウドサービス等）へと拡大している。今後そうした IT 依存度の高い事業が増加し、企業の収益の基盤となるにつれて、セキュリティリスクは企業経営に深刻な影響を与えるものとなる。こうしたセキュリティリスクをマネジメントするため CISO 等に求められる役割としては、技術的な対策の策定・実施だけでなく、セキュリティ関連規則の徹底等のコーポレートガバナンスや、個別事業のセキュリティリスク管理の支援が必要になる。セキュリティリスクはビジネスの継続や企業存続に支障をきたす恐れのある重大な経営リスクであり、企業におけるセキュリティへの取り組みが経営・事業に貢献するよう、主導する CISO 等の役割の重要性が認識され始めている※218。

図 2-5-2 は、経営層が CISO 等に期待している役割を調べたものである。CISO 等に、技術的役割、経営・事業に関する役割のいずれを求めるか尋ねたところ、経営・事業的役割を期待する回答は約 75% であった（「経営・事業的役割」「技術的役割と経営・事業的役割の両方」を求めるとした回答の合計）。



■図 2-5-2　経営層が CISO 等に求める役割（n=263）
（出典）IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」を基に編集

一方で、セキュリティ推進チームが担っている役割を調べたところ、経営的な役割であるコーポレートガバナンス（セキュリティガバナンス体制の構築・運営や、経営層とセキュリティ部門の間の調整等）や、事業への貢献（セキュリティ投資の事業価値最大化や、事業運営に対してセキュリティ対策が与える負荷の最小化等）を担っているセキュリティ推進チームは、半分以下であった（図 2-5-3）。



■図 2-5-3　CISO 等が担っている役割（n=263）
（出典）IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」を基に編集

このように、セキュリティ推進チームの設置は進んでいるが、その役割はセキュリティへの取り組みが経営・事業に貢献するよう主導する役割まで含んでいない場合も多いと考えられる。セキュリティ推進チームは、メンバーが備えている専門性を総合することにより、チーム全体として経営戦略や事業を深く理解し、リスク管理、法務、広報等に関する機能も提供することが求められてきている。更に、個々の事業戦略や商品設計を担う事業部門と、十分に連携することが求められる。

ただし、これらの適性を備えたチームを構成できる企業ばかりとは限らない。また個々の企業に閉じた努力で必要な人材を育成するのは簡単ではないため、業界や企業横断の活動、あるいは国レベルの取り組みとして、こうした人材を育成・供給するための試みが行われ始めている。

産業横断サイバーセキュリティ人材育成検討会におけるセキュリティ統括室、セキュリティ統括人材の検討は、業界横断の取り組みの例である[※246]。また NISC では、サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループにおいて、セキュリティチームのメンバーの人材像（特に各部署においてセキュリティを含めた戦略マネジメントを担う人材）や、人材育成のためのカリキュラムの検討を進めている[※217]。IPA では、2017 年 4 月に発足した産業サイバーセキュリティセンターにおいて、制御システムを有する企業・団体のサイバーセキュリティ対策を統括する責任者（CISO 等）向けの短期プログラムを、2017 年度に 3 回実施している（「2.4.1 (3) (c) 短期プログラム」参照）。

(2) サプライチェーンリスク管理の強化

改定された「サイバーセキュリティ経営ガイドライン Ver2.0」では、3 原則においてサプライチェーンに対するセキュリティ対策を重視している。また米国で 2018 年 4 月に改訂された NIST Cybersecurity Framework の version 1.1 では「Identify」（特定）の対策に「Supply Chain Risk Management」が追加され、同じくサプライチェーンの対策の重要性が高まっていることがうかがえる。

2017 年 7 月、スウェーデン政府が管理する国民の運転免許に関する全データベースが、委託先から再委託先に移転されたが、この再委託に際し、スウェーデン政府のセキュリティクリアランスチェックは実施されておらず、本来は閲覧の権限を持つべきではないエンジニアが自由にアクセスできる状態であった（「1.2.4 (3) 不適切な運用による情報漏えい」参照）。また、2017 年 5 月、国内企業が Wanna Cryptor の被害を報告したが、その感染源は欧州の拠点にある検査機器であった（「1.2.1 (1) Wanna Cryptor による被害」参照）。このように、サプライチェーンに関連するセキュリティの被害は既に発生している。Society 5.0 の社会では、IoT 機器等で複雑につながるサプライチェーン上のサイバーリスクが更に広がることが懸念されている。サプライチェーン全体のセキュリティリスクを把握し、対策を強化する必要がある。

(a) サイバーセキュリティ経営ガイドラインにおける対策

サイバーセキュリティ経営ガイドラインの指示 9「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」では対策例として、委託先の SECURITY ACTION（「3.5.2 (1) SECURITY

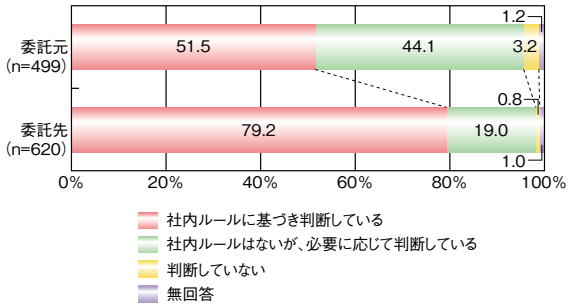
ACTION の取り組み」参照）や ISMS への取り組み状況を確認することとしている。また、「付録 A サイバーセキュリティ経営チェックシート」では、指示 9 の確認項目として以下の 3 点が示されている。

- システム管理等について、自組織のスキルや各種機能の重要性等を考慮して、自組織で対応できる部分と外部に委託する部分を適切に切り分けている。
- 委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている。
- 系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握している。

(b) IT サプライチェーンの実態調査

指示 9 の確認項目に関連して、IPA が行った IT システム・サービスの業務委託に関する調査結果について述べる。

図 2-5-4 は、委託に先立ち、情報セキュリティの観点から、業務委託／受託業務で扱う情報資産とリスクを特定し、会社として業務を委託すべきか（受託できるか）、必要な情報セキュリティ対策は何か等の判断を行っているかを尋ねた結果である。委託元、委託先とも、判断している割合（「社内ルールに基づき判断している」と「社内ルールはないが、必要に応じて判断している」の合計）は、95% 以上と高い割合となった。一方、「社内ルールに基づき判断している」割合では、委託元の回答企業で 51.5%、委託先の回答企業で 79.2% と開きがあった。



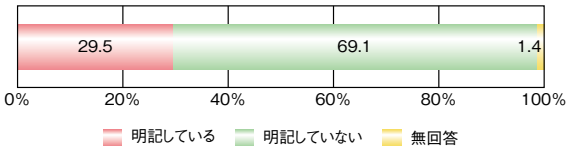
■図 2-5-4　情報資産やリスクに基づく情報セキュリティ対策の判断
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書※249」を基に編集

図 2-5-5 は、委託先選定にあたり委託先が実施すべき具体的な情報セキュリティ対策を仕様書等に明記しているかを尋ねた結果である。また、図 2-5-6 は、契約にどのような情報セキュリティに関わる要求事項を含めているかを尋ねた結果である。

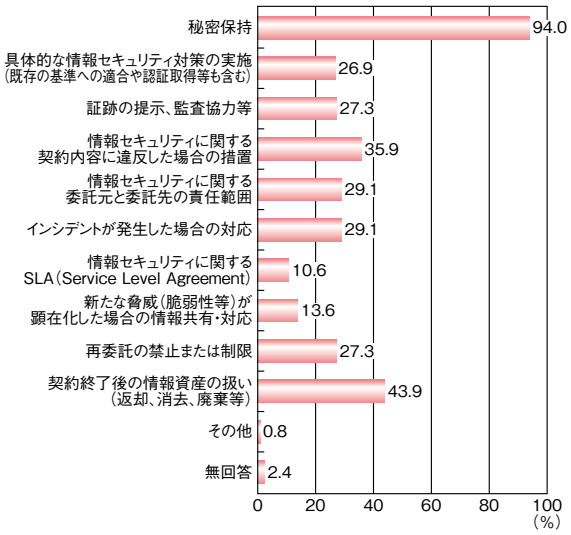
具体的な情報セキュリティ対策を仕様書に「明記している」割合は 29.5%（図 2-5-5）に、また委託先との契約に「具体的な情報セキュリティ対策の実施」を含めている割合は 26.9%（図 2-5-6）にとどまっていることから、委託元がどのような情報セキュリティ対策を求めるのか具体的に示されないまま、契約が締結される場合が多いことが分かった。また、図 2-5-6 では「秘密保持」は 94.0% とほとんどの企業で契約に含めているが、他の項目については全般的に低い割合となっている。特に「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」については 13.6% と低い割合であるが、日々脆弱性は発見され、また脆弱性を突いた攻撃及び被害が発生している。脆弱性に関する対応があいまいなまま開発や運用が進み、インシデントが発生した場合、責任分担を巡って紛争に至る場合もあり、注意が必要である。

図 2-5-7 は、委託先の情報セキュリティ対策実施状況をどのような方法で、またどのタイミングで確認しているかを、委託元に尋ねた結果である。

「チェックリストなど（自社のセルフチェック・内部監査）」は、選定時、契約時、契約期間中、契約終了時のい

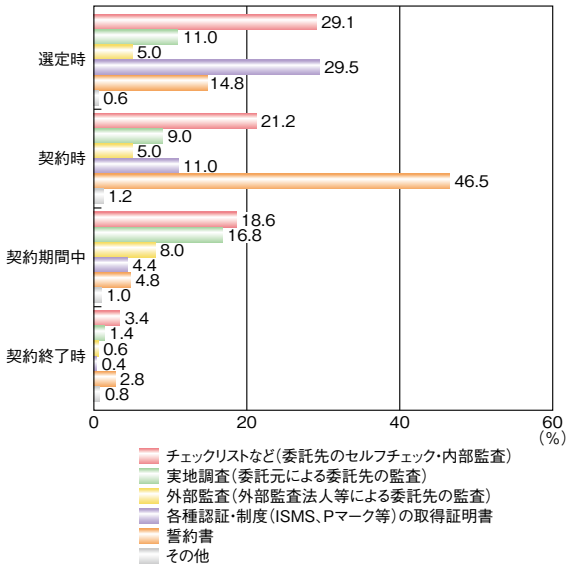


■図 2-5-5　委託先選定にあたり委託先が実施すべき具体的な情報セキュリティ対策を仕様書に明記しているか（n=499）
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」を基に編集



■図 2-5-6　委託先との契約に含める情報セキュリティに関わる要求事項（n=499）
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」を基に編集

ずれのタイミングでも上位に位置付けられている。「各種認証・制度（ISMS、Pマーク等）の取得証明書」は、選定時に確認されており、客観的な証明としてチェックリスト等に付随して提出されることが多いと思われる。契約時は、「誓約書」が最も多く、実施期間中は、「実地調査（委託元による自社（委託先）の監査）」もチェックリスト等に続いて実施されている。



■図 2-5-7　委託元による情報セキュリティ対策の実施状況の確認方法（実施タイミング別）（n=499）
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」を基に編集

情報セキュリティ対策の確認における課題として、確認にかかる委託元のコスト負担や委託先で対応する部門の負担が大きいこと、社内に十分な知見、スキルを持った人材がいないことが、委託元、委託先の両方から上位に挙げられている※249。取り扱う情報の重要度や責任範囲によって確認内容や程度は異なるが、基本的な対策項目と個別の要件に応じた対策項目を分け、基本的な対策項目については共通的な指標により客観的に評価し、複数の委託元・委託先の企業で利用できるような対策が必要である。

2017 年 12 月、経済産業省が設置した産業サイバーセキュリティ研究会においてサイバー・フィジカル・セキュリティ対策フレームワークの策定が議論され、セキュアなサプライチェーン構築のために取引先に確認すべき項目等、サプライチェーン全体のセキュリティ実現のための検討が開始された（「2.1.2（3）産業サイバーセキュリティ研究会」参照）。この検討により、調査で明確になった課題への対策を具体化することが望まれる。

2.5.2 情報セキュリティのマネジメントシステム

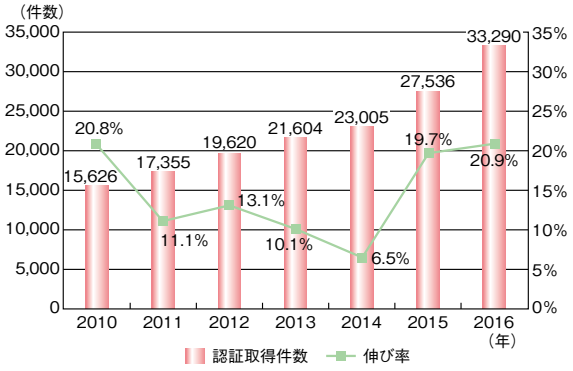
ビジネス環境の変化等により、組織が保有する情報資産の種類や資産価値も変化している。また、サイバー攻撃の手口が多様化、高度化し、それらの対策のための製品やサービスも増えている。組織はこれらの環境の変化によるリスクを見直し、情報セキュリティ対策が十分であるかを確認し、必要な処置を実施しなければならない。マネジメントシステムが推奨する PDCA（Plan-Do-Check-Act）は、これらの一連の活動を実現する方法であり、また、認証制度はマネジメントシステムの構築と運用を客観的に評価する方法として多くの組織が取り組んでいるものである。

本項では、ISMS 認証やプライバシーマーク制度等のマネジメントシステム認証の現状について述べる。

（1）情報セキュリティマネジメントシステムの国際規格 ISO/IEC 27001 の認証取得状況

サイバーセキュリティ経営ガイドラインの指示 6「サイバーセキュリティ対策における PDCA サイクルの実施」では、ISMS 等の国際標準となっている認証を活用することが対策例として挙げられている。

ISO の最新の公開情報によると、2016 年の世界の ISO/IEC 27001 認証取得件数は、2015 年と比較して 20.9% 増加の 5,754 件であり、合計で 3 万 3,290 件となっている。2010 年以降の全世界の ISO/IEC 27001 の認証取得件数とその伸び率を図 2-5-8 に示す（国際標準化の動向については「2.6.2（1）WG1（情報セキュリティマネジメントシステム）」参照）。



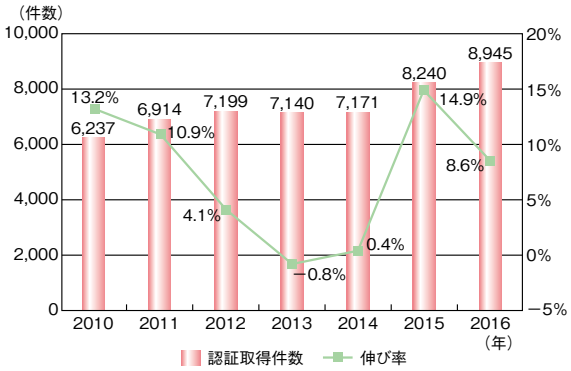
■図 2-5-8　全世界における ISO/IEC 27001 の年間認証取得件数と伸び率
（出典）ISO「ISO Survey 2016※250」を基に IPA が作成

国別の取得件数の上位 5 ヵ国は、1 位日本（8,945 件）、2 位英国（3,367 件）、3 位インド（2,902 件）、4 位中国

(2,618 件)、5 位ドイツ (1,338 件) であり、日本は常に 1 位を保っている。

上位 5 ヵ国の中で最も伸び率が高かったのは中国であり、2016 年の件数は、2015 年と比較して 78.2% 増であった。中国で 2016 年 11 月に可決し、2017 年 6 月から施行されたインターネット上の安全に関する中華人民共和国網絡安全法、いわゆる「ネットワーク安全法」により、中国のセキュリティ対策の意識が高まっていると推測される(「2.3.4 中国のセキュリティ政策」参照)。

2010 年以降の日本の ISO/IEC 27001 の認証取得件数とその伸び率を図 2-5-9 に示す。2014 年 3 月に JIS Q 27001 が改訂されたことにより、2013 年までの伸び率の減少傾向が、2014 年から増加傾向に転じ、2016 年では伸び率は低くなったが、認証取得件数は増加し続けている。



■図 2-5-9　日本の ISO/IEC 27001 の年間認証取得件数と伸び率
(出典)ISO「ISO Survey 2016」を基に IPA が作成

2016 年 8 月 1 日から開始した「ISMS クラウドセキュリティ認証」は、JIS Q 27001：2014 (ISO/IEC 27001：2013) に適合した ISMS において、その適用範囲内に含まれるクラウドサービスの提供、または利用に関して、クラウドサービス向けの国際規格である ISO/IEC 27017:2015 に規定されるクラウドサービス固有の管理策が実施されることを認証するものである。

ISMS クラウドセキュリティ認証の対象はクラウドサービスを提供している組織(クラウドサービスプロバイダ)、クラウドサービスを利用している組織 (クラウドサービスカスタマ)の両方である。なお、提供または利用するクラウドサービスの種類(IaaS、PaaS、SaaS)は問わない。

情報マネジメントシステム認定センター (ISMS Accreditation Center：ISMS-AC) が公表[※251]している ISMS クラウドセキュリティ認証の取得件数は、2018 年 5 月 11 日時点では 54 件となっており、今後も認証を取得する組織が増えることが期待される。

(2) 個人情報保護マネジメントシステム JIS Q 15001 の動向

ISMS と同じくマネジメントシステム規格を審査基準とする日本国内の制度としては、プライバシーマーク制度がある。プライバシーマーク制度は、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム−要求事項[※252]」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度である。1998 年 4 月より運用を開始し、2018 年 3 月 27 日時点でプライバシーマーク付与事業者数は 1 万 5,726 事業者となっている[※253]。

2017 年 12 月 20 日、このプライバシーマーク制度の審査基準のベース規格である JIS Q 15001 が改訂され、公開された。11 年ぶりとなる今回の改訂では、規格本文を ISO のマネジメントシステム規格と同じ構成とすることでマネジメントシステム規格としての位置付けを明確化するとともに、2017 年 5 月 30 日に全面施行された改正個人情報保護法に対応する管理策を追加した。

今回の規格改訂により、ISMS 等他のマネジメントシステムとの整合性が確保され、また要配慮個人情報や匿名加工情報といった、改正個人情報保護法で新たに規定された情報の取り扱いも明確になり、複数の規格や法律に準拠した対策を行わなければならない事業者にとって、JIS Q 15001 は理解しやすい規格となった[※254]。今回改訂された規格が、プライバシーマークの付与事業者はもちろんのこと、個人情報保護法遵守に取り組むすべての事業者の参考となることが期待される。

2.6 国際標準化活動

国際標準とは、製品や技術が国境を越えて利用されるために制定される国際的な共通規格であり、国際規格とも呼ばれる。国際標準の策定は国際標準化団体が行っており、その活動を「国際標準化活動」という。情報セキュリティに関する国際標準化は、規格が利用される領域ごとに様々な団体で行われている。

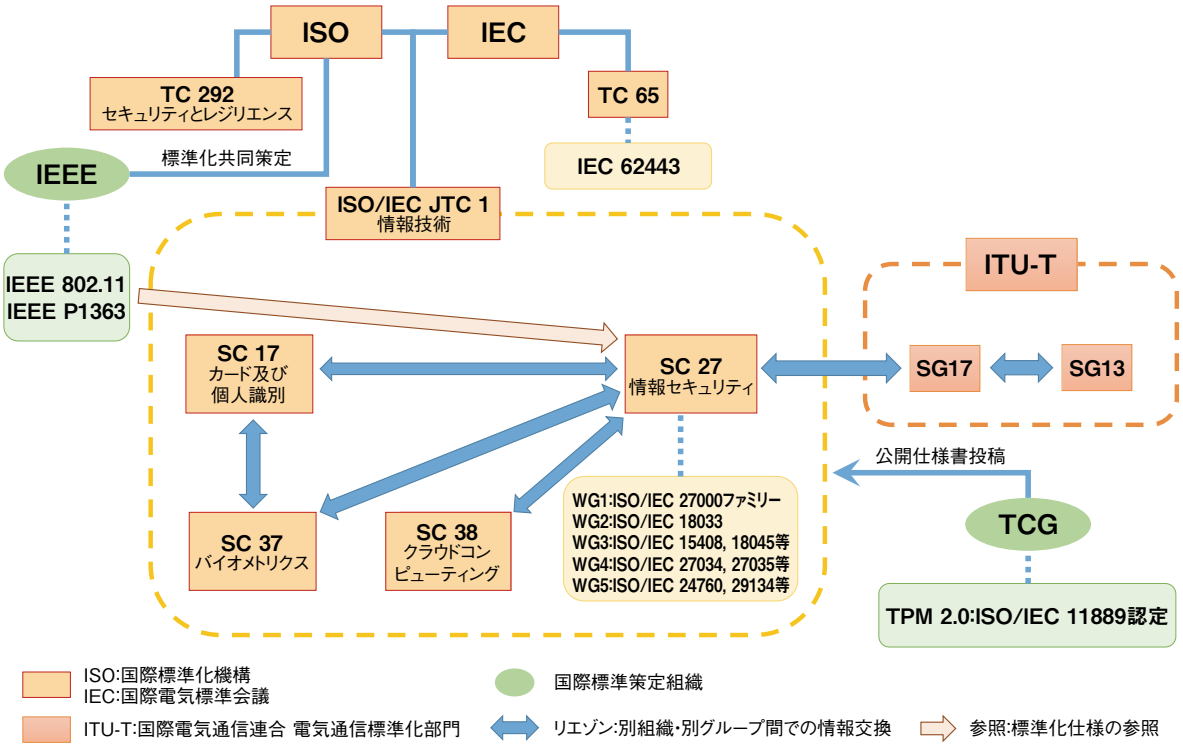
国際標準には、公的な標準化団体により所定の手続きを経て行われる「デジュール標準（de jure standard）」、いくつかの団体（企業等）が協力して自主的に作成する「フォーラム標準（forum standard）※255」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準（de facto standard）」がある。

電気製品やIT製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。また、民間の業界団体等により様々なフォーラム標準が策定されている。業界のフォーラム標準が、その後国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

2.6.1 様々な標準化団体の活動

情報セキュリティ分野に関するデジュール標準を策定する主な標準化団体として、以下に示す組織がある。また、当該デジュール標準の策定に関わる公的機関の関連を図2-6-1に示す。

- ISO（International Organization for Standardization：国際標準化機構）/IEC（International Electrotechnical Commission：国際電気標準会議）JTC 1（Joint Technical Committee 1：第一合同技術委員会）※256：情報セキュリティを含む情報技術の国際規格を策定している。コンピュータや情報分野を扱う国際標準化団体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC 1が設立された。日本国内の標準化団体としては、日本工業標準調査会（Japanese Industrial Standards Committee：JISC）がISO、IEC双方のメンバーであり、JTC 1でも活動している※257。
- ITU-T（International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）：



■図2-6-1 情報セキュリティ関連の標準化組織の相関図※261

電気通信技術に関わる国際規格を策定している。情報セキュリティに関しては SG（Study Group）17 が設置され※258、ISO や後述する IETF とともにネットワークや ID 管理等に関する標準化活動を行っている。策定した標準は ITU 勧告として定められる。

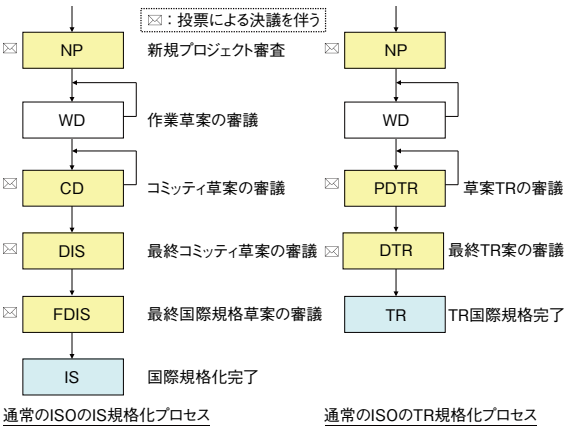
また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下のようなものがある。

- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織である IEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoT セキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加することができる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※259。標準化した技術文書は RFC（Request For Comments）として参照することができる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本に regional forum がある※260。

2.6.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27（以下、SC 27）は、ISO 及び IEC の合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会である。SC 27 は、テーマ別に五つの WG で構成される（前ページ図 2-6-1）。

ISO/IEC における標準化作業は、策定する仕様の完成度によって図 2-6-2 のような状態があり、それぞれ各国の投票によって次の段階へ進む。なお、ISO において、技術が未成熟またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書（TR：Technical Report）または技術仕様書（TS：Technical Specification）として出版する。



■図 2-6-2　ISO/IEC における文書のステータス

以下に、各 WG の活動概要を述べる。

(1) WG1（情報セキュリティマネジメントシステム）

WG1 では、情報セキュリティマネジメントシステム（Information Security Management System：ISMS）に関する国際規格として、ISO/IEC 27001（ISMS 要求事項を示す規格）及び ISO/IEC 27002（情報セキュリティ管理策及び実施の手引きを示す規格）を中心に、ISO/IEC 27001 が示す ISMS 要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001 及び ISO/IEC 27002 を土台とする分野別規格、及びその他トピックスに関する ISO/IEC 27000 ファミリー規格の国際標準化活動を実施している。

(a) ISO/IEC 27001:2013 に関する手引きや指針の国際標準化活動

ISO/IEC 27001 に関する手引きや指針を提供する規格である、ISO/IEC 27001:2013 発行に伴う改訂は、2018 年 3 月の時点でほぼ完了している。ISMS 活動のパフォーマンスや有効性の監視、測定、分析及び評価の規格である ISO/IEC 27004 は 2016 年に改訂され、ISMS 要求事項のガイダンスである ISO/IEC 27003 及び ISMS 監査の実施に関するガイドラインである ISO/IEC 27007 は 2017 年に改訂された。また、情報セキュリティ分野におけるリスクマネジメント規格である ISO/IEC 27005 も必要最低限の改訂を加えた版が発行待ちの状況にある。なお、ISO/IEC 27005 は、2013 年版へ本格的に対応するための改訂も並行して進められているが、こちらは発行まで時間がかかる見込みである。

ISO/IEC 27000 ファミリー規格の概要と用語を示した ISO/IEC 27000 は、発行された規格の状況及び ISMS 分野において共通に使用される用語の改訂を目的に、2016 年に改訂され、更に 2018 年改訂版が 2018 年 2 月に発行済みである。

(b) 分野別規格の国際標準化活動

分野別規格作成に関する要求事項を示す規格である ISO/IEC 27009 が 2016 年に発行されたが、2017 年には早期改訂の開始が決定されている。

分野別規格そのものについては、通信事業者のためのガイドラインとして ISO/IEC 27011 が 2008 年に発行、2016 年に改訂されている。セクター間及び組織間コミュニケーションのための規格として ISO/IEC 27010 が 2012 年に発行、2015 年に改訂されている。また、クラウドサービスに関するものとして、ISO/IEC 27017 が 2015 年に発行されている。これらは、いずれも ISO/IEC 27002 を拡張した分野別規格である。なお、エネルギー分野に関するものとして ISO/IEC 27019 が 2017 年に発行されており、これは、ISO/IEC 27009 へ適合している。

(c) その他の ISO/IEC 27000 ファミリー規格の国際標準化活動

その他の ISO/IEC 27000 ファミリー規格の国際標準化活動としては、ISMS 専門家に関する要求事項を示した規格である ISO/IEC 27021 が 2017 年に発行されている。また、情報セキュリティ管理策の評価のためのガイドラインである ISO/IEC TS 27008 が発行待ちの状況にある。情報セキュリティガバナンスに関する規格である ISO/IEC 27014:2013 からの改訂作業が開始されている。

新たなトピックとしては、サイバーセキュリティに関する規格化の検討が始まっている。まず、サイバーセキュリティの既存のフレームワークと ISO 及び IEC 規格類との対応関係を示した技術報告書 ISO/IEC TR 27103 が 2018 年に発行された。この他、サイバーセキュリティのフレームワーク構築に関するガイドライン規格の発行に向けたプロジェクトが開始され、サイバーセキュリティの概念やコンセプトの規格化についても検討が進められている。ただし、サイバーセキュリティに関する解釈は各国、各組織で多様化しているため、対象範囲の決定や用語定義等を行うことは難しく、今後の課題と認識されている。なお、関連するものとして、サイバー保険に関する規格も発行に向けたプロジェクトが開始されている。

また、IoT、プライバシー、サイバーレジリエンス等の新しい概念の ISMS ファミリー規格への取り込み方についても検討が行われている。前述の規格類の発行、改訂作業の中でこれらの検討は進められている。

(d) ISO/IEC 27001 及び ISO/IEC 27002 の改訂

2013 年の改訂から 5 年を経ている ISO/IEC 27002:2013 については、2018 年 3 月までの 1 年間の SP（Study Period：研究期間）において、次期改訂の設計仕様（Design Specification）が決定され、改訂作業が開始されている。ISO/IEC 27001:2013 についても、次期改訂において大きな課題となる附属書 A 及び適用宣言書の扱い方についての先行検討が行われている。

(2) WG2（暗号とセキュリティメカニズム）

WG2 では、暗号プリミティブ（暗号アルゴリズム）や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG2 の国際主査、副主査ともに日本人が選出され、WG2 での活動をリードしている。2017 年度は、「匿名エンティティ認証　第 4 部：弱い秘密に基づく機構（ISO/IEC 20009-4）」「秘密分散　第 2 部：基本機構（ISO/IEC 19592-2）」等が発行された。このほかの主な活動内容について以下に示す。

(a) 新規項目「墨塗り署名」

欧州からの提案で、「墨塗り署名」に関して規格化前検討※262 を行っていたが、標準化することが承認され、ドラフト作成が開始された。

(b) 軽量暗号「SIMON/SPECK」の規格化遅延

NSA（National Security Agency：米国国家安全保障局）が設計した軽量暗号 SIMON/SPECK※263 を、米国が「軽量暗号　第 2 部：ブロック暗号（ISO/IEC 29192-2）」へ提案し、追補として規格化作業が行われているが、2016 年から追補草案（Proposed Draft Amendment:PDAM）の段階にとどまっている。これは、仕様を記述した論文が学会またはジャーナルの査読を通っていない、アルゴリズムの設計指針を公表していない、等の不透明部分の存在、Edward Snowden による情報暴露事件以降、NSA の信頼性回復が依然としてできていないこと等による。

(c)「耐量子計算機暗号」の規格化前検討

量子計算機でも解読が困難な暗号技術の規格化前検討において、SC 27で標準化に着手する前に、他団体／組織で標準化している情報をまとめ、文書化することが決まっていたが、記載内容について2017年に議論があり、日本の専門家も数名加わり、以下の項目を記載していくこととなった。

- ハッシュベース署名
- 格子暗号※264
- 符号ベース暗号
- 多変数暗号
- その他の非対称鍵暗号（公開鍵暗号）
- 対称鍵暗号（共通鍵暗号）

(3) WG3（セキュリティの評価・試験・仕様）

2017年度、WG3は4月にハミルトン（ニュージーランド）、10～11月にベルリン（ドイツ）にて定期会合を開催した。そこでの議論内容を以下に概説する。

(a) ISO/IEC 15408、ISO/IEC 18045の改訂

ISO/IEC 15408（Evaluation Criteria for IT security）及びISO/IEC 18045（Methodology for IT security evaluation）※265はWG3の主要規格の一つであり、IT製品のセキュリティ機能を評価する手続きを定めた国際標準である。具体的には、製品開発元がどのような開発設計文書等を評価者に提供すべきか、評価者がそれらをどのように精査し、どのようなテストを実施し、製品のセキュリティ機能の信頼性を検査すべきかを定めている。本規格は、ハミルトン会合にてその内容を改訂することが合意され、ベルリン会合にて一次作業原案が議論された。

今回の改訂のポイントの一つは、詳細な評価手順を定める「評価アクティビティ」の標準化である。ISO/IEC 15408及びISO/IEC 18045はすべてのハードウェア・ソフトウェア製品に適用できる汎用的な規格であるが、例えばスマートカードやネットワーク機器等に実施するテストの内容は各々かなり異なる。各製品向けの詳細な評価手順（ISO/IEC 15408では「評価アクティビティ」と呼ぶ）を別途個別に定めているケースもあるが、そのフォーマットはこれまで共通化されていないため、今回の改訂において同フォーマットや作成方法の標準化を検討することになった。ベルリン会合では、作業原案に対し700近いコメントが寄せられ、活発な議論が行われた。この結果、次回会合で二次作業原案を作成し更なる議論を行うことで合意された。

(b) ISO/IEC 20897の分割提案承認

ISO/IEC 20897（Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters）とは、PUF（Physically Unclonable Function）と呼ばれる技術のセキュリティ要件、及びそのテスト手法に関する国際標準化である。LSIやICチップ等のデバイスを同じ工場で製造しても、各デバイスは完全に同一ではなく、各デバイスの電子回路には微小な差異が存在する。PUFとは、それら差異を個々のデバイスを識別する「デバイス指紋」として暗号等に活用する技術である。ただしそれら差異をデバイス指紋として利用するためには、指紋がデバイスごとに異なっていること、一つのデバイスの指紋から他のデバイスの指紋を類推できないこと等の性質を満たす必要がある。現在日本では、PUF技術の確立に向けた研究プロジェクトが進行している※266。ベルリン会合では同プロジェクト関係者も参加し、プロジェクトに関する説明のほか、今後のISO/IEC 20897の開発にプロジェクトの成果を取り込むため、20897をPart 1（Security requirements for physically unclonable functions for generating non-stored security parameters）及びPart 2（Test and evaluation methods for physically unclonable functions for generating non-stored security parameters）に分割することが提案され、同会合にて承認された。

(c) 新たな研究期間の開始

ISO規格の開発をする前に、一定の研究期間（SP）を設け標準化の内容に関しメンバー間で議論するケースが多い。2017年度、WG3においては、量子鍵配送やISO/IEC 15408評価機関に対する技能要件、IT製品のセキュリティパッチ開発の要件等、計五つの研究期間を開始することが、中国、フランス、米国、英国から提案されWG3総会で承認された。今後各研究期間での議論の結果に応じ、2018年度において関連するISO規格の新規開発が提案される可能性もある。

(d) ホワイトボックス暗号に関する技術レポート開発提案

2017年度は、ホワイトボックス暗号に関する技術レポート開発の提案が新たに承認された。暗号においては、攻撃者が暗号デバイスを入手し、物理的攻撃を加えることで秘密鍵を得てしまうという危険性がある。その対策

のために考案されたのが、ホワイトボックス暗号である。ホワイトボックス暗号は、攻撃者が暗号デバイスを完全に制御できるような状況でも、秘密鍵が漏えいしないことを目的としている。しかしながらホワイトボックス暗号技術自体が未成熟だとする意見が WG3 内部から挙がったため、ISO 規格にするのではなく、その最新動向を取りまとめたレポートを開発することがベルリン会合にて合意された。

(4) WG4(セキュリティコントロールとサービス)

WG4 では、WG1 が対象とする ISMS を実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG4 における 2017 年度の主な成果、活動を紹介する。

(a) アプリケーションセキュリティ(ISO/IEC 27034 シリーズ)

ISMS を支援する規格として、アプリケーションが必要とするセキュリティレベルを保証し、ICT のセキュリティリスクに適切に対応することを目的に、ISO/IEC 27034 シリーズの策定が進められている。ISO/IEC 27034 シリーズは、アプリケーションの設計、開発、実装、利用に関する情報セキュリティのガイダンスであり、以下の複数の Part から構成される。

- ISO/IEC 27034 Information technology – Security techniques – Application security:
  - Part 1: Overview and concepts (2011 年規格化完了)
  - Part 2: Organization normative framework (2015 年規格化完了)
  - Part 3: Application security management process(DIS)
  - Part 4: Application security validation(SP)
  - Part 5: Protocols and application security control data structure(2017 年 10 月規格化完了)
  - Part 5-1: Protocols and application security controls data structure – XML Schemes (4th PDTS)
  - Part 6: Case Studies(2016 年規格化完了)
  - Part 7: Application security control attribute predictability(2018 年 5 月規格化完了)

Part 4 については、規格の必要性に戻り、再審議を実施しているところである。2017 年度以降の主な成果としては、2017 年 10 月に ISO/IEC 27034-5 の規格化を完了、2018 年 5 月に ISO/IEC 27034-7 の規格化を完了した。これにより、本シリーズで重要な要素となるアプリケーションセキュリティコントロール (Application Security Control : ASC) (アプリケーションの共通部品となるコントロール)の設計、開発、実装、利用に関する一連の流れの規格化を完了したといえる。

(b) 情報セキュリティインシデント管理(ISO/IEC 27035 シリーズ)

情報セキュリティインシデントや脆弱性を管理するプロセスを規定した ISO/IEC 27035 の改訂が、複数 Part 構成として進められている。ISO/IEC 27035 シリーズは、ISO/IEC 27002 の箇条の一つである情報セキュリティインシデント管理を実施するためのガイドラインである。改訂では ISO/IEC で規定されるデジタルフォレンジック標準(ISO/IEC 27037 等)との関係の説明が追加されている。ISO/IEC 27035 シリーズの構成は以下のとおりである。

- ISO/IEC 27035 Information technology – Security techniques – Information security incident management:
  - Part 1: Principles of incident management (2016 年規格化完了)
  - Part 2: Guidelines to plan and prepare for incident response(2016 年規格化完了)
  - Part 3: Guidelines for incident response operations(SP にて再審議中)

Part 1 では、情報セキュリティインシデント管理について五つのフェーズ (計画と準備、検知と報告、評価と決定、対応、教訓) のプロセスが規定される。Part 2 は、インシデント対応の準備及び計画、並びに教訓の指針である。Part 3 は 2016 年 5 月に検討が打ち切られた。

(c) サプライヤ関係のセキュリティ(ISO/IEC 27036 シリーズ)

製品やサービスを外部調達する際のサプライヤに関するセキュリティマネジメント指針として ISO/IEC 27036 が策定されている。以下に示す四つの Part から構成されている。

- ISO/IEC 27036 Information technology – Security techniques – Information security for supplier relationships:
  - Part 1: Overview and concepts (2014 年規格化

完了）
- Part 2: Requirements（2014 年規格化完了）
- Part 3: Guidelines for information and communication technology supply chain security（2013 年規格化完了）
- Part 4: Guidelines for security of cloud services（2016 年規格化完了）

Part 1 は概要と概念、Part 2 は要求事項、Part 3 は ICT サプライチェーンセキュリティのためのガイドラインとしてそれぞれ規格化が完了している。Part 4 はクラウドサービスのセキュリティのためのガイドラインとして 2016 年 10 月に国際規格（IS）が発行された。Part 4 は、クラウドコンピューティングサービスの情報セキュリティ実践規範である ISO/IEC 27017 に規定されているサプライヤ関係の管理策を技術的に実装し、運用するガイドラインを提供する。具体的には、ISO/IEC 27017 の管理策について、ISO/IEC 27036 の他の Part と同様に、サプライヤ（クラウド事業者）と調達者（クラウド利用者）を対比し、システムライフサイクルに従ったプロセスごとに、相互に実践すべき事項を定義し、かつ、クラウドサービスの形態（SaaS、PaaS、IaaS 等）に応じてサプライヤが実施すべき事項を記述している。すなわち、Part 4 は、ISO/IEC 27036 シリーズを構成する規格として、ISO/IEC 27017 の実装を支援するものである。

（d）電子情報開示（Electronic Discovery）（ISO/IEC 27050 シリーズ）

電子情報開示は主に民事訴訟において、訴訟当事者間で訴訟に関連する資料を自ら収集し、開示する手続きである。日本においては当該手続きに関する法的裏付けはないが、米国、カナダ、アイルランド等では電子情報開示に関する法律が策定済みであり、近年の特許侵害や独占禁止に関する訴訟で実際に使われている。これらの訴訟は国際企業間で国をまたいで行われるケースも多いが、電子情報開示に関わる用語や手続きは、法体系、設立背景の違い等から国ごとに異なった用語、手続きとなっており、国際標準策定による共通化が求められている。上記の背景から、SC 27/WG 4 では、電子情報開示について、ISO/IEC 27050 シリーズとして規格化に取り組んでいる。

ISO/IEC 27050 シリーズは Part 1 ～ 4 の四つのパートにより構成されている。

- ISO/IEC 27050 Information technology – Security techniques – Electronic discovery:
  - Part 1: Overview and concepts（2016 年規格化完了）
  - Part 2: Guidance for governance and management of electronic discovery（FDIS）
  - Part 3: Code of practice for electronic discovery（2017 年 10 月規格化完了）
  - Part 4: ICT readiness for electronic discovery（NP）

Part 1 は、電子情報開示の全体像、プロセス及び電子保存情報（Electronically Stored Information：ESI）の基本概念を示したものである。

Part 2 は、電子情報開示に関する組織へのガバナンス及び要求事項について整理したもので、組織の管理者を対象とし、電子情報開示に関するガバナンスの責任と考慮点、準拠状況に関する定期的なレビューについて記載している。2018 年 5 月に FDIS 版を発行し、2018 年中には規格化完了の予定である。

Part 3 は、電子情報開示に関する具体的な手続きを明記したもので、米国 EDRM（Electrical Discovery Reference Model：電子情報開示参考モデル）をベースに検討が進められ、ESI の識別、保全、収集、処理、レビュー、発行の六つのプロセス要素について、目的、手続きの進め方、必要事項について記載している。本 Part には米国における電子情報開示作業の実経験が反映されており、失敗を避けるための考慮点が記載されている点がユニークである。

Part 4 では、電子情報開示の対象となる情報は企業または組織の持つすべての電子データが対象となるため、IT によるサポートに関する要件を取りまとめることを目的としている。本 Part の策定は難航しており、一度 SP に戻って再審議を行い、2018 年 3 月に NP となったことから再定義の上で審議が継続されている。

（5）WG5（アイデンティティ管理及びプライバシー技術）

WG5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2017 年度の主な活動を紹介する。

（a）アイデンティティ管理

アイデンティティ管理のフレームワークである ISO/IEC 24760 は以下の三つの Part で構成されている。

- Part 1：用語とコンセプト（2011 年規格化完了）
- Part 2：アーキテクチャと要求事項のリファレンス（2015 年規格化完了）
- Part 3：実施方法（2016 年規格化完了）

2011 年に発行された Part 1 について、用語及びコンセプトの変更／追加をするべく追補案の策定が進められている。

2013 年 4 月に発行されたエンティティ認証保証のフレームワークである ISO/IEC 29115 は、近年のサイバー攻撃の増加に伴う関心の高まりから、改訂の検討が進められている。また、アイデンティティの証明に関する技術仕様である ISO/IEC TS 29003 が 2018 年 3 月に発行された。

(b) プライバシー

プライバシー対策に関わる規格である ISO/IEC 27552 は 2018 年 3 月に委員会草案（CD）の投票が行われた。本規格は、ISMS の要求事項を規定した ISO/IEC 27001 及び ISMS を実施するためのプラクティスをまとめた ISO/IEC 27002 に、プライバシー対策に関する要求事項及びプラクティスを追加することにより、プライバシー対策に関するマネジメントシステム構築を支援することを目指している。

プライバシー影響評価（Privacy Impact Assessment: PIA）の規格である ISO/IEC 29134 は 2017 年 6 月に発行された。PIA は、個人情報を扱う情報システムの要件定義にあたり、事前に個人情報提供者のプライバシーへの影響を評価し、情報システムの設計・運用を適正に行うことを促すプロセスであり、本規格は PIA レポートに記載される内容及び実施方法等を規定している。

また、個人識別可能情報（Personally Identifiable Information：PII）の保護規範である ISO/IEC 29151 が 2017 年 8 月に発行された。

更に、プライバシーに関するデータの非識別化の方法等を規定する ISO/IEC 20889 は 2018 年 4 月に発行された。

経済産業省が 2014 年 10 月に公開した「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」に基づく国際規格である ISO/IEC 29184 は委員会草案（CD）になり、策定が進められている。

(c) バイオメトリクス

PKI（Public Key Infrastructure：公開鍵暗号基盤）認証のクライアントにおいて署名鍵がバイオメトリック認証によって使用可能になるハードウェアセキュリティモジュールを扱った認証フレームワーク ISO/IEC 17922 は、2017 年 9 月に発行された。バイオメトリック認証をリモート環境でも使用可能にするためのデータ構造を定義する ISO/IEC 24761 は、委員会原案段階にあり、策定が進められている。バイオメトリックデータの保護技術を扱う ISO/IEC 24745 は、2011 年に発行されたが、その後の新技術を反映するため、改訂開始が決定された。

(6) SC 27 と他の分科会・組織との連携

情報セキュリティが社会で注目されてきていることから、情報セキュリティ以外の分野の分科委員会（SC、TC）と SC 27 との連携が増えている。

例えば図 2-6-1（125 ページ）にあるように、カード及び個人識別については SC 17、バイオメトリクスについては SC 37、クラウドコンピューティングについては SC 38 がリエゾンしている。また、サプライチェーン管理の IT 化を進める要素として、電子タグ等の活用が期待されていることから、自動識別及びデータ取得技術の分科会である SC 31 との連携も進められている。

また、インシデント管理が重視されている中、情報セキュリティ分野の枠を超えた知見の共有が求められている。エネルギー分野や船舶分野等、他分野との知見を共有するためにリエゾンを立ち上げ、セキュリティ及びレジリエンス分野である TC 292、リスクマネジメント分野である TC 262、組織のガバナンス分野である TC 309 との連携も深めている。

更に、ブロックチェーンと分散台帳技術に関する専門委員会として活動を開始した TC 307[※268] は、情報セキュリティとも関係が深い分野であることから、2016 年 12 月にリエゾンを設立し、SC 27 と連携が行われている（ブロックチェーンのセキュリティについては「3.2 仮想通貨の情報セキュリティ」参照）。

また SC 27 は、ISO/IEC 27000 シリーズの情報セキュリティからサイバーセキュリティへの移行を検討するにあたり米国の NIST と情報交換し、NIST Cybersecurity Framework を参考にしつつサイバーセキュリティ関連規格 ISO/IEC 27100 シリーズが発行できるよう準備を進めている。

日本国内のガイドラインも標準化活動に活用されている。SC 27/WG 4 は、日本の「IoT セキュリティガイドライン」をベースに、米国の Cloud Security Alliance（CSA）等からの提案を加味した目次案を検討している。併せて、

SC 41 では、「IoT セキュリティガイドライン」レベルの議論と、既に発行されている IoT リファレンスアーキテクチャ（ISO/IEC 30141）の間を埋める文書「IoT を安全にするための一般的要求事項」を策定することを進めている。今後は、その一部として IoT システムの高信頼化のための設計要求事項を導出する予定である（IoT のセキュリティについては「3.1 IoT の情報セキュリティ」参照）。

国内の組織も SC 27 との連携を進めている。2016 年 12 月、一般社団法人情報処理学会の情報規格調査会は IoT ／スマートシティの国際標準化活動を本格化することを発表した。これは 2016 年 11 月に ISO/IEC JTC 1 により、IoT、及びセンサーネットワークやウェアラブル技術等の IoT 関連技術を対象とする分科委員会（JTC 1/SC 41）の創設が決まった※269 ことによる。これを受けて、情報規格調査会でも SC 41 専門委員会を設置した。SC 27 とも連携しながら IoT に関連する技術の標準化が統合的かつ相互に整合する形で進むことが期待される。

2.6.3 工業通信ネットワーク-ネットワーク及びシステムセキュリティ(IEC 62443)

近年の制御システムは、情報システム同様に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、サイバー攻撃の脅威に晒されるようになった。こうした動向に伴い、制御システムにおいてもリスク分析に基づくセキュリティ対策が喫緊の課題となっている。これについて、日米欧各国の政府機関・業界団体が取り組みを進めているが、本項では国際標準について述べる。

制御システムのセキュリティを包括的に網羅した国際標準は ISA（The International Society of Automation）99 Committee※270 と IEC Technical Committee 65 Working Group10（TC65WG10）※271 により作成されている。ISA99 Committee によって発行された標準は ISA-62443-X-Y と記され、IEC によって発行された標準は IEC 62443-X-Y と記される。この X、Y は各規格に付与された番号を示す。以下、ISA と IEC の双方を示す場合は、ISA/IEC 62443-X-Y と記載する。

ISA/IEC 62443 は大別して四つのグループに分類され、発行済みと策定中のものを合わせて 13 の規格が存在する※272（図 2-6-3）。

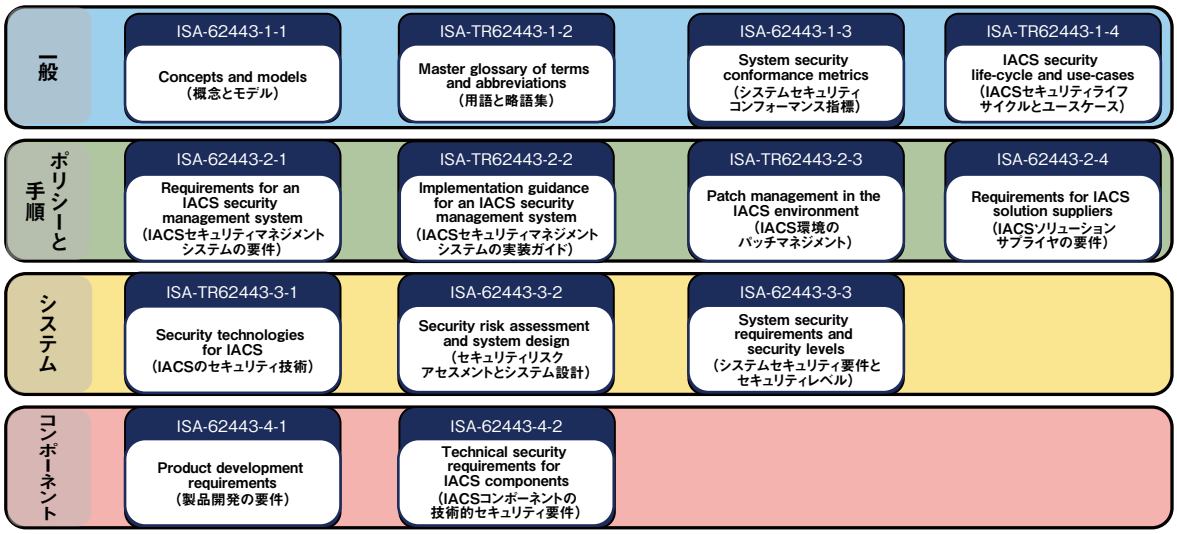
ここでは、各規格の概要と 2017 年度の状況について紹介する。以下は、各グループの概要である。

(1) ISA/IEC 62443-1 グループ（一般）

ISA/IEC 62443 の中で用いられる用語の解説や、制御システムのセキュリティ動向、地理的に分散したフィールド機器を遠隔から集中監視制御する SCADA※273 モデルの一般論等を規定している。このグループは、事業者やシステムインテグレータ、機器ベンダ等、すべての関係者が共通して参照する規格である。

(2) ISA/IEC 62443-2 グループ（ポリシーと手順）

事業者や運用者等の組織を対象とした、主にマネジメントに関連するセキュリティ要求事項等を規定した規格であり、組織としてのセキュリティマネジメントシステムの確立や、パッチ管理等の運用に関連する事項が記載さ



■図 2-6-3　ISA/IEC 62443 の概要
（出典）ISA99 Committee「ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS)※270」を基に IPA が編集・仮訳

れている。

(3) ISA/IEC 62443-3 グループ（システム）

複数の機器や製品を組み合わせて運用する制御システムを対象とした規格である。

ISA/IEC 62443-3-3 は、ISA/IEC TR 62443-1-1 で規定される基礎的要求事項（Foundational Requirement：FR）に対応する形で、システムの技術的なセキュリティ要求事項を規定している。要求事項は、システム要件（System Requirement：SR）と強化策（Requirement

ISA リファレンス	IEC リファレンス	規定内容	ISA99※272 ステータス（更新年月）	IEC※274 ステータス（更新年月）
ISA-62443-1-1	IEC/TS 62443-1-1	ISA/IEC 62443 に用いられる用語の解説や、制御システムの動向・状況、セキュリティ概念、及び SCADA モデルの一般論等を規定	Ed.1：発行済み Ed.2：ドラフト段階 （2017 年 3 月）	Ed.1：発行済み （2009 年 7 月）
ISA-TR62443-1-2	IEC/TR 62443-1-2	ISA/IEC 62443 に用いられる制御システムのセキュリティに関連する用語・略語集	【更新】 ドラフト段階 （2017 年）※275	不明
ISA-62443-1-3	IEC 62443-1-3	評価基準の策定や利用のためのフレームワーク等を規定	中断 （2016 年 9 月）	中断 （2016 年 3 月）
ISA-62443-1-4	IEC/TR 62443-1-4	制御システムのセキュリティに関するライフサイクルとそのユースケースに関連する事項を規定	検討中※276	不明
ISA-62443-2-1	IEC 62443-2-1	制御システムのセキュリティプログラムの確立方法について規定（既存規格である ISO/IEC 27000 シリーズ※277 を部分的に引用して策定されている）	Ed.1：発行済み Ed.2：ドラフト段階 （2015 年 11 月）	Ed.1：発行済み （2010 年 11 月）
ISA-TR62443-2-2	IEC/TR 62443-2-2	制御システムのセキュリティプログラムの運用ガイドラインについて規定	検討中 （2013 年 4 月）	Ed.1：削除 （2009 年 11 月）
ISA-TR62443-2-3	IEC/TR 62443-2-3	制御システムにおけるパッチ管理方法に関するガイドラインについて記した技術報告書	Ed.1：発行済み （2015 年 7 月）	Ed.1：発行済み （2015 年 6 月）
ISA-62443-2-4	IEC 62443-2-4	事業者が制御システムのコンポーネントやシステムを調達する際のセキュリティ要求事項等を規定	採択予定	【更新】 Ed.1：発行済み （2015 年 6 月） Ed.1：正誤表発行済み （2015 年 8 月） Ed.1：補遺版発行済み※278 （2017 年 8 月）
ISA-TR62443-3-1	IEC/TR 62443-3-1	一般的なセキュリティ技術のうち、制御システムで適用可能なものについて、解説等を記載した技術報告書	Ed.1：発行済み Ed.2：ドラフト段階 （2016 年 2 月）※279	Ed.1：発行済み （2009 年 7 月）
ISA-62443-3-2	IEC 62443-3-2	セキュリティゾーン（共通のセキュリティ要件を持つ論理的／物理的資産のグループ）や、それらを連結するコンジット（通信経路）に関するセキュリティについて規定	ドラフト段階 （2017 年 5 月）	【更新】 照会段階 （2018 年 1 月）
ISA-62443-3-3	IEC 62443-3-3	制御システムのセキュリティ機能要件を規定 ISA/IEC 62443-1-1 で規定されている七つの基礎的要求事項（FR1 ～ FR7）に対応する形でシステムの技術的なセキュリティ要求事項を規定	Ed.1：発行済み （2013 年 8 月）	Ed.1：発行済み （2013 年 8 月） Ed.1：正誤表発行済み （2014 年 4 月）
ISA-62443-4-1	IEC 62443-4-1	コンポーネント（機器・装置）の開発時のセキュリティ要求事項を定めた文書（セキュアなコンポーネントを開発するための方法を規定しており、ISCI※280 の EDSA※281 をベースにしている）	ドラフト段階承認済み （2016 年 3 月）	【更新】 Ed.1：発行済み （2018 年 1 月）
ISA-62443-4-2	IEC 62443-4-2	コンポーネントのセキュリティ要求事項を定めた文書。デバイスに搭載されたセキュリティ機能を規定	ドラフト段階 （2017 年 1 月）	【更新】 照会段階 （2018 年 2 月）

※ステータスが更新されているものには、表中に【更新】と記載

■表 2-6-1　ISA/IEC 62443 シリーズの規定内容とステータス
（出典）ISA99 Committee「Work Product List※272」を基に IPA が作成

Enhancement:RE）から構成され、各要求事項にセキュリティレベル（Security Level:SL）が割り当てられている。SL は、それぞれの要求事項を満たした場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階の SL が規定されており、最も高度な要求事項を満たすものをレベル 4 としている。

（4）ISA/IEC 62443-4 グループ（コンポーネント）

制御システムを構成する個別コンポーネント（機器や装置）を対象とした規格であり、主にコンポーネントのライフサイクルの各フェーズにおけるセキュリティ要求事項や、搭載されるセキュリティ機能等に関する事項が記載されている。表 2-6-1（前ページ）に規格の一覧を示す。2017 年度は、IEC 62443-2-4 の規格に補遺版が発行され、タイトルも「Security program requirements for IACS service providers」に変更となった。また、IEC 62443-4-1 は初版が発行され、IEC62443-3-2 及び IEC 62443-4-2 は照会段階に移行し、ISA-TR62443-1-2 はドラフト段階に移行した。

2.6.4 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準（TCG）

TCG（Trusted Computing Group）※282 は、信頼性の高いコンピューティング環境の実現のため、機器やネットワーク等のセキュリティ技術に関して統一的な標準仕様を開発、策定、普及させることを目的とし、世界各国 88 の企業、30 以上の政府機関、業界団体、大学、専門家で構成される国際的非営利団体（NPO）である（数字は 2018 年 1 月時点）。セキュリティチップ Trusted Platform Module（TPM）、自己暗号化ドライブ（Self Encrypting Drive：SED）、高信頼ネットワーク Trusted Network Communications（TNC）の三つを基本的な標準仕様と位置付けている。

TPM は 2009 年に ISO/IEC 11889:2009 として公開され、2013 年には改訂版の TPM2.0 が公開された。この TPM2.0 仕様（TPM Library Specification）も 2015 年に ISO/IEC 11889:2015 として公開された※283。

日本には 2008 年に設立された TCG の地域支部がある※284。この日本支部（Japan Regional Forum：JRF）では、国内向けの普及活動としてテクニカルセミナー※285、ワークショップ※286 を開いており、その経験を日本から世界へフィードバックしている。

以下では、現在 12 あるワークグループからいくつかの活動内容を紹介する。

（1）組み込み機器検討ワークグループ（Embedded Systems WG）

パソコンへの実装から始まった TPM 実装を、組み込み機器に幅広く展開する目的で活動しているワークグループである※287。

その配下の自動車サービスサブグループでは、自動車に実装することを想定した自動車向け TPM の仕様を策定し、2015 年に「TCG TPM 2.0 Library Profile for Automotive Thin Specification, Version 1.0」として公開した※288。同サブグループでは、この仕様書を具現化する種々の取り組みを進めている。この仕様書の改訂版及び同仕様書に合わせたセキュリティ要件（Protection Profile：PP）は、2018 年初めのパブリックレビューを経て 2018 年内に発行される予定である。自動車向け応用例として、前述の自動車向け TPM 仕様に基づく車載機器のリモートメンテナンス、近年話題の自動運転に必要な情報転送及びドライブレコーダにおけるデータ保障等があり、これらについても検討が続いている。

2017 年には、このワークグループから二つの新しいグループが派生した。

TPM とともにシステム起動の最初で読み出される RTM（Root of Trust for Measurement）と呼ばれるメモリを扱う RTM サブグループも、このワークグループの配下にあり、ここでの議論から DICE ワークグループが独立している。

もう一つは、産業用システムのセキュリティを検討するインダストリアル検討サブグループである。

（2）Device Identifier Composition Engine 検討ワークグループ（DICE WG）

DICE は、RTM サブグループが策定した RIoT（Robust IoT）※289 の Core 仕様上で動作するソフトウェア群の策定を目指しているワークグループである※290。RIoT と DICE の関係は、TPM と TSS（TPM を使用する Software Stack）※291 の関係に相当する。TPM 利用システムだけでなく、TPM を使わないシステムでもデバイス ID を最小のシリコンリソースで実現できるような新しい ID 管理アーキテクチャを開発している。具体的には、ID 生成の方法、ユースケース、要件、セキュリティ上の利点、及び DICE のためのソフトウェア API 等を定義しようとしている。

2017 年に活動を開始し、現在は DICE のためのハードウェア要件が公開されている※292。

(3) インダストリアル検討サブグループ (Industrial SG)

産業用システム、例えば工場内の設備同士がネットワークで接続されつつある中で、セキュリティ上の脅威に対抗する必要性が高まっている。これらのシステム、データ、ネットワーク等を守るために組み込み機器検討ワークグループ傘下で TCG 技術の利用を検討しているサブグループである※293。活動開始は 2017 年であり、将来は産業機器の要求仕様、ガイダンスの策定を予定している。

(4) ストレージ検討ワークグループ (Storage WG)

TCG 技術を、ストレージシステムのセキュリティ対策に応用し、これを標準化する目的で活動しているワークグループである※294。対象とするストレージシステムには、ハードディスクだけでなく USB メモリや SSD も含まれる。近年問題になっている USB メモリや PC の紛失、盗難によるデータの流出及びデータセンターからの個人情報の流出を防ぐための技術の一つとして、SED の重要性が増している。TCG では、SED 機能に対応する TCG 仕様として OPAL（オパール）と呼ばれる仕様を公開している※295。

2.7 安全な政府調達に向けて

IPA では、国民に向けた情報セキュリティに関する啓発活動のほか、政府機関が安全に IT 製品等を調達するために活用できる制度の運営を行っている。

本節では、IT 製品のセキュリティ機能を評価する「IT セキュリティ評価及び認証制度」の動向とスマートカード評価認証に関する取り組み、及び暗号アルゴリズムの適切な実装を確認する「暗号モジュール試験及び認証制度」の動向について報告する。

2.7.1 ITセキュリティ評価及び認証制度

情報セキュリティ政策会議の発行した「政府機関の情報セキュリティ対策のための統一基準（平成28年度版）※296」（以下、政府統一基準）では、マイナンバー等の国民の情報を扱う公共情報システムを構成する IT 製品等を調達する際に、調達者はセキュリティ要件を策定することが求められている。

このようなセキュリティ要件を満たした IT 製品を調達する仕組みとして、多くの国々では第三者セキュリティ評価制度が用いられている。日本でも「IT セキュリティ評価及び認証制度（Japan Information Technology Security Evaluation and Certification Scheme：JISEC）※297」を IPA が運営している。本項では、政府調達と JISEC についての動向を紹介する。

(1) 政府調達におけるセキュリティ要件確認

主要各国では、政府が市販の IT 製品を調達する際にセキュリティを確認する手段として、国際的な評価基準である ISO/IEC 15408（または CC（Common Criteria）と呼ばれる）を活用している。更に他の国で運営する認証制度で CC を用いて評価した結果を、自国の認証制度でも相互に受け入れる協定※298（Common Criteria Recognition Arrangement：CCRA）が締結され、PP（Protection Profile）と呼ばれる、政府調達において調達仕様として参照される製品分野ごとの国際的なセキュリティ要件も開発されている。

日本でも特定の製品分野においては、PP を活用した IT 製品の調達が行われている。対象となる製品分野は、経済産業省が発行し、政府統一基準から参照される「IT 製品の調達におけるセキュリティ要件リスト※299（以下、要件リスト）に指定されている。

この要件リストに掲載された製品分野の IT 製品を政府機関等が調達する場合、情報システムセキュリティ責任者は政府統一基準に基づき、それらが想定されるセキュリティ上の脅威に対応できていることを確認しなければならない。一般的にこの確認は、CCRA 加盟国で策定された製品分野ごとのセキュリティ要件の調達仕様である PP を指定し、CCRA 加盟国で運用される認証制度において PP の要件を満たしていることを認証された製品（以下、認証製品）を調達することで行われる。

要件リストで対象とされる製品分野は表 2-7-1 に示すとおりである。この要件リストは 2018 年 2 月に改正され、従来対象とされていた 6 分野に新たに 5 分野が追加された。

今回追加された製品分野は、暗号製品とネットワーク製品が中心となっている。これらには PP が存在し、更にそれらの要件に基づいて第三者が評価した認証製品も流通していることから追加された。外出時にデータを持ち出す場合に使用する USB メモリや通信基盤となるネットワークルータ／スイッチについては、政府機関等が調達する際、セキュリティ要件を求めることが予想されるが、これらの製品を供給する国内ベンダにおいて、対象製品の多くが国際標準に基づく第三者認証を取得していないことが課題となっている。

(2) IoT 分野に向けた活動

昨今は、これまでになく多種多様な機器がネットワークに接続され、データが有機的かつリアルタイムに処理される IoT 社会へと移行しつつある。このような状況において、政府機関でもネットワークカメラ等の IoT 機器を活用するようになっている。それらの機器は様々な情報を収集・分析するサービスに組み込まれているため、当然ながら IoT 機器の政府調達においてもセキュリティ対策が必須となる。一般に IoT 機器は製品の単価が安いものが多く、そのライフサイクルやコストを考慮した場合、従来のセキュリティ機能を具備する IT 製品に対して実施される広く深い保証を得るための評価方法を、そのまま IoT 機器の評価に適用することは困難である。

JISEC では、今後の IoT 機器の安全な政府調達に向けた二つの施策を 2017 年度に行った。一つは、既存評価における評価期間の短縮、もう一つはセキュリティ要件の自主的な確認に利用できるチェックリストの作成で

対象製品分野	製品分野定義
デジタル複合機（MFP）	プリント機能を有し、更に、スキャン、FAX、コピー機能のうちいずれか二つ以上の機能を装備している製品
ファイアウォール	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品
不正侵入検知 / 防止システム（IDS/IPS）	ネットワークやシステムの稼働状況を監視し、組織内のコンピュータネットワークへの外部からの侵入を報告、防御する製品
サーバ OS	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
データベース管理システム（DBMS）	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品
スマートカード（IC カード）	プラスチック製カード等に IC チップを埋め込み、情報を記録できるようにした製品
新たに追加された対象製品分野	**製品分野定義**
暗号化 USB メモリ	製品自体に USB コネクタを備えており、フラッシュメモリを内蔵した持ち運び可能な記憶装置に暗号化機能を有する製品
ルータ／レイヤ 3 スイッチ	OSI 基本参照モデル第 3 層を利用し、情報システム及びネットワークの基盤においてデータを中継する機能を持った通信回路装置
ドライブ全体暗号化システム	ノート PC 等のハードディスクドライブ、半導体ドライブ等のデータストレージ全体を暗号化するシステム
モバイル端末管理システム	スマートフォン、タブレット等のモバイル端末を安全に運用・管理するシステム
仮想プライベートネットワーク（VPN）ゲートウェイ	公共ネットワークを利用した、仮想的なプライベートネットワークシステムにおける終端装置

■表 2-7-1　IT 製品の調達におけるセキュリティ要件リスト
（出典）経済産業省「IT 製品の調達におけるセキュリティ要件リスト」を基に IPA が作成

ある。

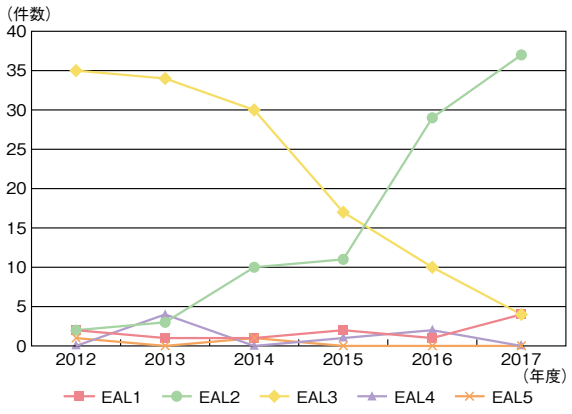
(a) 評価期間の短縮

先に述べたように IoT 機器は従来の IT セキュリティ製品に比べ比較的安価であり、扱うデータも個人情報等を含まない一般的なデータであることが多いため、必要最低限のセキュリティ機能の評価を短期間で完了させなければコスト的に見合うものではなくなる。

例えば、要件リストで求められるようなセキュリティ評価の国際標準に基づく調達要件では、2014 年度までは EAL（Evaluation Assurance Level）※300 3 と呼ばれる直接的なセキュリティ機能の評価に加え、開発環境の安全性を確認することを要求していた。IT 製品の政府機関における活用が多岐にわたり、タイムリーな製品調達が求められるようになったことで、2014 年度以後は開発環境や開発ツールのセキュリティ要件確認までは求めない、等で保証の範囲を絞った EAL2 が調達要件として指定され、その結果、日本における 2017 年度の認証製品は EAL2 が 85% 以上を占めるようになった（図 2-7-1）。

更に最新の要件リストでは、評価の範囲から開発環境等を省略し、セキュリティ機能そのものに焦点を当てた EAL1 相当の PP が、MFP（Multifunction Printers：デジタル複合機）調達の要件として採用された。

JISEC では 2017 年度、この MFP の PP に基づく評価をパイロットプロジェクトとし、過去に時間がかかった評価事例の分析を行い、評価期間の短縮を試みた。具体的には、認証機関への申請時点で、評価者が行うテストの項目や使用ツールの概要を示したテスト計画書、及び製品の暗号実装に関する基本設計資料の提出を義務付けた。これにより、申請前に評価者と開発者がテスト工程の評価内容を確認することとなり、申請後の評価において設計工程に後戻りするリスクを低減することができた。また、評価に対する指摘事項を、評価者や評価案件に依存しないように識別番号によりデータベース化し、同一評価案件における複数評価者間の情報共有や他評価案件への事前適用を促すことを可能とした。この結果、認証の申請から認証書の発行までの期間を 4 ヵ月とし、それまでの中央値である 7 ヵ月を大きく下回る



■図 2-7-1　日本の評価保証レベル別認証発行件数

ことができた。政府調達において、安価でセキュリティ機能が限定されたIoT製品が活用されているため、今後も評価の質を維持しながら、更なる評価コストの低減や期間の短縮について検討し、IoT製品の評価を行っていく。

(b) ネットワークカメラシステムチェックリスト

政府統一基準では、IT製品ではあるが簡易システムとして提供され、システム全体としてセキュリティ対策を必要とするような製品分野を「特定用途機器」と定義している。特定用途機器としては、IP電話やネットワーク会議システム、ネットワークカメラシステム等が挙げられ、調達及び運用時のセキュリティの確保は情報システムセキュリティ責任者に求められる。しかしながら、特定用途機器はセキュリティ機能を主要とする製品とは異なり、価格的な面から市場に認証製品が少なく、また調達・運用における具体的な確認指針もないため、情報システムセキュリティ責任者自身がセキュリティ対策を個別に考えなければならない。

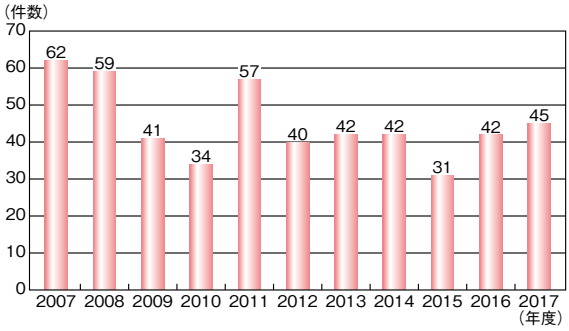
IPAでは、特定用途機器の中でも急速に普及し、インシデントが報告されているネットワークカメラシステムに焦点を当て、2017年度にネットワークカメラシステムの利用形態やセキュリティ課題の調査を実施した。また、これを基に、ネットワークカメラベンダ、調達者、有識者で構成された委員会の協力のもと、ネットワークカメラシステムにおいて想定される脅威に対し最低限講ずるべき情報セキュリティ対策の要件を示した「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト※301」を発表した(図2-7-2)。

■図2-7-2　ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト

本チェックリストは、政府機関を始め様々な組織でのネットワークカメラの調達・運用に活用できることから、新聞等の多くのメディアで紹介された。また、2018年度に改正を予定している政府統一基準において、特定用途機器のセキュリティ対策のための資料として参照されることとなった。今後JISECでは、IoT製品に対する調達者・運用者の自主的なセキュリティ要件の確認を可能とするチェックリストや、製品ベンダや第三者がそれらのセキュリティ要件を具体的に開発または評価するためのセキュリティ機能仕様レベルでの要件を公開していく。

(3) 認証の状況

日本の認証機関であるJISECでの2017年度までの認証発行件数の推移を図2-7-3に示す。2017年度の発行件数は前年度に比べてやや増加したが、ここ数年は40件程度を保っている。これには、近年の認証申請のほとんどをMFPが占めており、新規機種の市場投入が定常的に行われていることが反映されている。

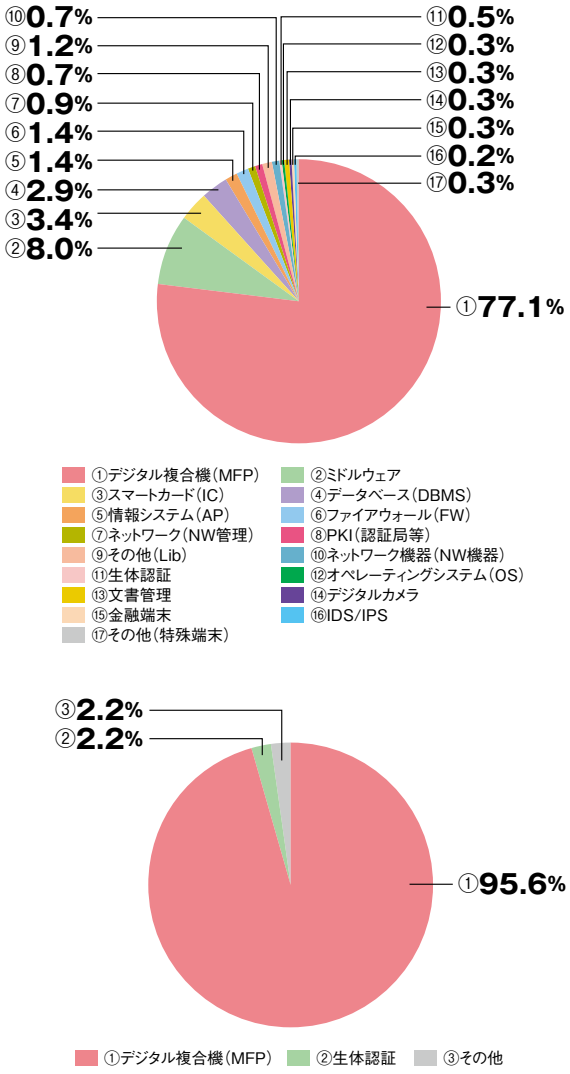


■図2-7-3　日本の認証発行件数の推移

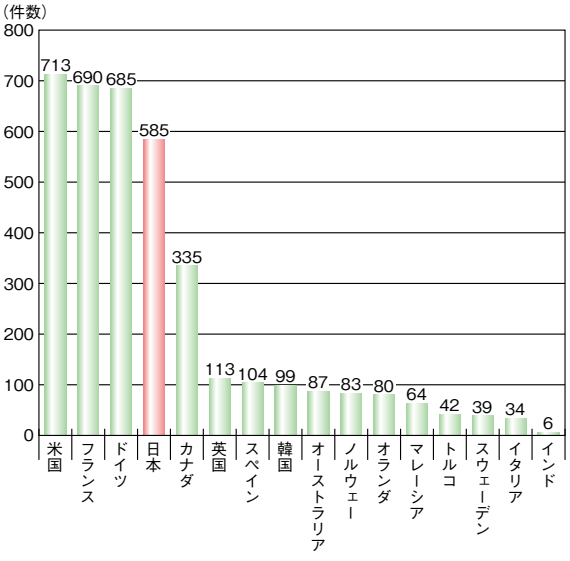
日本における認証製品分野の内訳は、図2-7-4に示すように圧倒的に「デジタル複合機（MFP)」が多く、2017年度は95.6%を占めている。要件リストの対象製品であるMFPは日本の製品ベンダが多く製造しているため一定件数の申請がなされているが、一方で、要件リストにはない製品分野については認証取得のメリットを感じなくなった製品ベンダが増え、申請が減少していると思われる。

2018年2月の要件リスト改正により、対象となる製品分野が大幅に拡大された。今後は、追加された新たな製品分野から政府調達を見据えた認証の申請が増えることが予想される。

CCRA加盟各国の認証制度のWebサイトで公開されている認証製品の2017年度までの累計数は、日本が米国、フランス、ドイツに次いで第4位である（図2-7-5)。



■図 2-7-4　日本の認証発行件数の内訳



■図 2-7-5　CCRA 加盟国の認証製品件数

米国ではネットワーク関連機器の認証製品が多く、ドイツやフランスではスマートカード関連の認証製品が中心となっている。日本は MFP の認証製品が中心であるが、製品のラインアップの豊富さと新製品のリリースの頻繁さから認証製品件数を伸ばしている。

2.7.2 スマートカードの評価認証

前項でも触れているスマートカードは、高い評価保証レベルを要求される等、他のセキュリティ製品と異なる特徴を持っている。これはスマートカードが課金情報や個人情報を扱うにもかかわらず、携帯可能な形状から攻撃に晒されやすいことに由来する。本項では、その評価内容と動向について紹介する。

(1) スマートカードの特徴

スマートカードには、ISO/IEC 7816 で定義された接触カードと ISO/IEC 14443 で定義された非接触カードがある。これらのカードは、クレジットカード、キャッシュカード、デビットカード、交通系カード、e-パスポート、マイナンバーカード等として身近なところで使われている。また、スマートカードのリーダ／ライタも駅の改札やバスの乗降口、コンビニエンスストア等の店舗に置いてある端末としてよく利用されている。

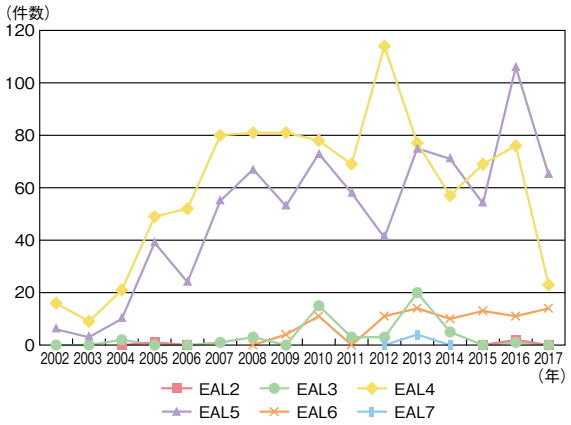
スマートカードは、名刺サイズのプラスチックカードに IC チップを搭載したものであり、ポケットに入れて持ち出す等、簡単に携帯できる。また、接触カードにおいては、通信端子がカード上に金属面として露出しており、比較的簡単に通信データを傍受できる構造になっている。

これらの特徴からスマートカードには、他のセキュリティ製品と異なり高いレベルの耐タンパ性※302 が要求されている。

(2) 認証の状況

JISEC では 2012 年にスマートカード製品（ハードウェア）として初めての認証製品を登録して以来、現在までに製品ベンダが公開を希望している認証製品として 8 製品をリストで公開している※303。EAL と呼ばれる評価保証レベルで分類すると 6 製品が EAL4（EAL4+）であり、2 製品が EAL5+ を取得している。前項では EAL2 ～ 3 が主流であったのに対し、スマートカードでは EAL4 ～ 5 が主流であることが分かる。これは CCRA 加盟国の認証機関が Web サイトで公開している認証製品の年別の推移を見ても同じ傾向が見える。図 2-7-6（次ページ）

はCCRAで公開されている認証製品リストからスマートカードに分類される認証件数をグラフ化したものである。欧州ではスマートカードのセキュリティ評価認証を10年以上も実施しており、初期の時点からEAL4/EAL5が主流である。しかも2014年以降は、EAL4よりEAL5の認証件数が増えてきており、更にここ数年はEAL6製品も数は少ないながらも伸びてきている。複数のアプリケーションを載せたマルチアプリケーションカード等、スマートカードの高機能化に対応したセキュリティ要求が背景にあると考えられる。



■図2-7-6　スマートカードの認証件数の推移

(3) スマートカードに対するセキュリティ要件と評価の特徴

スマートカードの評価認証で参照されるPPは、当初はBSI-PP-0035[※304]だったが、2014年にBSI-PP-0084[※305]がリリースされて以降は順次切り替わっている。このPPが要求している評価保証レベルはEAL4+であり、従ってスマートカードに要求される耐タンパ性を確保するためには物理攻撃[※306]、サイドチャネル攻撃[※307]、故障利用攻撃[※308]等に対抗する実装が求められる。一方ではシミュレータを使った対抗策の評価手法[※309]も報告されており、設計上流での検証が可能になってきている。同様に、評価者にもこれらの攻撃を模した脆弱性評価技術とそれに必要な評価機器が求められる。CCRAではこれら実装や評価に必要なガイドをサポート文書として公開しており、IPAではCCRAが公開しているCCサポート文書を原文と和訳の両方で公開している[※310]。

図2-7-6で示されているとおり、ここ数年はEAL4/EAL5より高いレベルのEAL6での認証件数が少しずつ伸びてきている。EAL6/EAL7では準形式的／形式的な設計の検証が求められるが、今後は耐タンパ性能だけでなく、厳密な検証の根拠提示も求められる傾向にあると推測される。形式手法は、仕様記述の曖昧性に起因する設計の不備を避けるために設計工程の上流で使われるが、これをスマートカードのようなセキュリティ製品の設計に用いることで、セキュリティ対策仕様の不完全性等が分析できるようになる。

(4) 評価に関する人材育成

IPAでは、将来の攻撃に備えるために、レーザ光照射装置やレーザ顕微鏡等の最先端の評価ツールを導入して、国内の評価機関、事業者、大学等の関係者が利用できる評価環境の整備を進めている。2017年度は、14回にわたって延べ104名に評価ツールが利用された。

またIPAは、人材育成を目的としてハードウェアセキュリティに関心を持つ幅広い分野の技術者を対象に、試行評価用のテストビークル[※311]を用意し、貸し出しを行っている。2017年度は7社にテストビークルを貸し出した。

2.7.3 暗号モジュール試験及び認証制度

暗号モジュール試験及び認証制度（Japan Cryptographic Module Validation Program：JCMVP）とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者適合性評価制度である。本制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。国内ではIPAが認証機関として本制度を運用している。これは、北米で運用されているCMVP（Cryptographic Module Validation Program）と同等の制度である。ここでは、JCMVPの最新動向について述べる。

(1) ITセキュリティ評価及び認証制度との連携

IPAが運営する評価認証制度には、JISECとJCMVPの二つがあり、2017年に発行されたJISECのガイドライン[※312]によって、JCMVPの活用方針が示されている。

JISECのもとで、この方針に関連する「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015[※313]」に基づくデジタル複合機の認証が、2017年10月27日に完了した[※314]。このPPでは、信頼できるツールを用いた暗号アルゴリズムの実装のテストを求めている。この暗号アルゴリズムの実装のテストに、JCMVPの暗号アルゴリズム実装試験ツールが活用され、デジタル複合機の認証に貢献した。

(2) 鍵導出関数等の試験仕様の策定

JCMVPは、2013年に米国政府機関向けのセキュリティ規格であるNIST SP800-108[※315]、NIST SP800-132[※316]、NIST SP800-135[※317]に記載された鍵導出関数を承認したが、これらの鍵導出関数に対する試験仕様を2018年度中に策定する予定である。

また、JCMVPは、2013年にNIST SP800-56B[※318]に記載されたRSA暗号を用いた鍵確立手法を承認したが、この鍵確立手法に対する試験仕様を2018年度中に策定する予定である。

これらの試験仕様は、暗号アルゴリズムの実装の適合性を試験する際の、試験仕様に関する国際規格「ISO/IEC 18367:2016 Information technology — Security techniques — Cryptographic algorithms and security mechanism conformance testing[※319]」の内容を踏まえたものとなる予定である。

(3) IC旅券用の鍵確立手法に関する検討

IC旅券は公的な身分証明書として、そのセキュリティ確保が重要視されており、複数の国でセキュリティ評価及び認証の対象となっている。2015年に国際民間航空機関（International Civil Aviation Organization：ICAO）が発行した、IC旅券に関する規格ICAO Doc 9303 Part 11[※320]の中で、IC旅券と旅券検査端末装置との間の暗号通信に用いられる鍵確立手法が定められている。これを受けて、2016年に外務省領事局旅券課が、「旅券冊子用ICのためのプロテクションプロファイル− SAC対応（PACE）及び能動認証対応 −第1.00版[※321]」を発行している。このPPの記述から、日本のIC旅券には、楕円曲線暗号の一つであるECDH（Elliptic Curve Diffie-Hellman）を使った鍵確立手法が採用される。しかし、このECDHの仕様はCRYPTRECが定める電子政府推奨暗号リストに掲載されたECDHの仕様とは異なる。このため、JCMVPにおける技術審議委員会の暗号アルゴリズム実装試験要件検討WGの中で、2017年10月から安全性の検討に着手し、2018年度も引き続いて検討を行うこととなった（CRYPTRECについては「2.1.5 電子政府システムの安全性確保への取り組み」参照）。

また、暗号アルゴリズムが正確に実装されていることを、試験を通じて確認したいというニーズが見込めることから、IC旅券用のECDHに対する試験仕様を、2018年度からJCMVPの暗号アルゴリズム実装試験要件検討WGで検討することとなった。

2.8 情報セキュリティの普及啓発活動

ランサムウェアや仮想通貨取引所の不正アクセス等、インターネットを悪用した金銭を狙う事件が発生し、情報セキュリティの必要性が以前にも増して問われている。また、SNSを介した出会いによって命が奪われた凶悪な犯罪も明らかになり、インターネットによるつながり方を見直さざるを得ない状況となっている。

財産と情報、そして命を守るために、様々な機関が行っている情報セキュリティの啓発活動を紹介する。

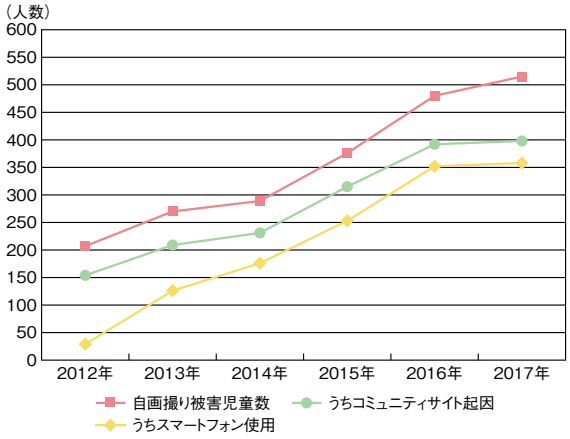
2.8.1 政府・公共機関による普及啓発活動

本項では、インターネット利用者の情報セキュリティ意識向上を目的として実施された、政府・公共機関による普及啓発活動について述べる。

(1) 青少年に対する取り組み

2017年5月、内閣府特命担当大臣決定として、7月を「青少年の非行・被害防止全国強調月間※322」に設定し、青少年によるインターネットの適切な利用の促進等の取り組みを集中的に実施するとの発表があった。月間の重点課題1には「子供の性被害の防止」、重点課題2では「インターネット利用に係る非行及び犯罪被害防止対策の推進」が掲げられ、フィルタリングの利用普及を一層促進すること、情報モラルを身に付けることの重要性を啓発すること、等が示された。このほか、重点課題7の「いじめ・暴力行為等の問題行動への対応」についてもインターネット上のいじめに関する取り組みが推進される等、青少年の生活環境の一部であるインターネットに関する対策を呼びかけた。

この活動の一環として、文部科学省と警察庁が連携して「夏休みを迎える君たちへ～ネットには危険もいっぱい～※323」と題したリーフレットを作成し、自画撮り画像の送信によるトラブルや、コミュニティサイトを介した出会いの危険性等について、子ども達に向けて発信した。また、警察庁による「自画撮り」被害の実態を紹介する漫画※324には、高校生の主人公がSNSだけでしか知らない相手とコミュニケーションする中で、言葉巧みに誘導されて下着姿の写真を送信してしまうストーリーが描かれた。この背景には、加害者による騙しや脅しにより、自分の裸体を自ら撮影し送信してしまう「自画撮り被害」に遭った子どもの数が年々増加していること、その被害者の8割近くがコミュニティサイト起因であったこと（図2-8-1）が挙げられる。



■図2-8-1 【児童ポルノ事件】自画撮り被害に遭った児童の推移
（出典）警察庁「平成29年における子供の性被害の状況※325」を基にIPAが編集

このような児童の自画撮り被害の防止を目的として、東京都は、青少年の健全な育成に関する条例の一部を改正し※326、全国に先駆けて2018年2月1日から、青少年に対し不当に裸体等を自画撮りさせ、メール等で送信させることを犯罪とする条例を施行した。

また、これに伴う啓発活動として、渋谷のスクランブル交差点等の大型街頭ビジョンによる広告（図2-8-2）や、啓発ドラマを公開し、条例改正の認知向上と被害の予防を目指している。

■図2-8-2 大型街頭ビジョン等による広告
（出典）東京都「18歳未満の子に裸の画像を不当に求めることは犯罪です!」

警察によるインターネット犯罪を抑止する様々な活動も実施されている。兵庫県警察では、「あひルのおやコ※327」

を頭文字にして、インターネットのお約束メッセージを掲載したポスターを県内すべての小学校に配布する等、児童の意識向上に向けた働きかけを行った。

(2) 保護者に向けた取り組み

内閣府が 2017 年 5 月に公表した「低年齢層の子供のインターネット利用環境実態調査※328」の結果によると、スマートフォン、タブレット、携帯ゲーム機等の通信機器を用いた子どものインターネットの利用は 1 歳で 9.1%、2 歳では 28.2% に達していることが判明した。これまでも、インターネット利用の低年齢化が指摘されていたものの、本調査は、改めて幼児及び児童に対する対策の必要性を示すものであった。本調査には、スマートフォンでインターネットを利用している子どもの保護者による対策の実施状況に関する設問もあり、99.0% の保護者が、何らかの取り組みを実施していると回答した。しかしながら、そのほとんどは、「大人の目の届く範囲で使わせている」であり、フィルタリングの利用は 8.0% にとどまった(表 2-8-1)。

総務省は、フィルタリングの利用推進策として、毎年 2 月から 5 月にかけて「春のあんしんネット・新学期一斉行動」を実施してきた。しかし、神奈川県座間市で発生した事件を背景に、例年より早く、2017 年 12 月の冬休みを含めて「あんしんネット　冬休み・新学期一斉緊急行動」の期間とし、フィルタリングの積極的な利用を促す取り組み等を集中的に行うこととした※330。

インターネットが、子どもの命を脅かすツールとならないよう、子ども達はもちろん、フィルタリングの効果について保護者の認知度を高める調査や活動が実施されている。

	管理している(計)	ネットの利用管理は行っていない	わからない・無回答	大人の目の届く範囲で使わせている	利用する時間や場所等のルールを決めている	子供向けの機器等を使わせている	子供の利用状況を把握している	フィルタリングを使っている	その他の方法で管理している
【総数】(n=301)	99.0%	–	1.0%	93.0%	45.2%	16.6%	27.6%	8.0%	3.3%
0 歳(n=3)	100.0%	–	–	100.0%	–	–	–	–	–
1 歳(n=6)	100.0%	–	–	83.3%	50.0%	66.7%	–	16.7%	–
2 歳(n=31)	100.0%	–	–	100.0%	32.3%	29.0%	32.3%	9.7%	–
3 歳(n=33)	97.0%	–	3.0%	93.9%	30.3%	24.2%	6.1%	3.0%	3.0%
4 歳(n=35)	100.0%	–	–	97.1%	51.4%	11.4%	25.7%	2.9%	2.9%
5 歳(n=41)	95.1%	–	4.9%	90.2%	53.7%	14.6%	26.8%	7.3%	2.4%
6 歳(n=33)	100.0%	–	–	93.9%	54.5%	30.3%	33.3%	12.1%	3.0%
7 歳(n=31)	100.0%	–	–	96.8%	64.5%	12.9%	38.7%	–	3.2%
8 歳(n=35)	100.0%	–	–	85.7%	42.9%	8.6%	25.7%	8.6%	5.7%
9 歳(n=53)	100.0%	–	–	90.6%	37.7%	3.8%	35.8%	15.1%	5.7%

■表 2-8-1　子供のインターネット利用に関する保護者の取り組み
(スマートフォン、子供の年齢別)
(出典)内閣府「低年齢層の子供のインターネット利用環境実態調査(概要)※329」

(3) サイバーセキュリティ月間

重点的かつ効果的にサイバーセキュリティに対する取り組みを推進するべく、政府は毎年 2 月 1 日から 3 月 18 日までを「サイバーセキュリティ月間」とし、各種啓発主体と連携して普及啓発活動に取り組んでいる。NISC は、2018 年のサイバーセキュリティ月間の初日にキックオフサミット※331 を開催した。講演やパネルディスカッションはインターネットで中継され、会場に足を運ばなくてもイベントへの参加が可能であった。イベントは「サイバーセキュリティは全員参加!」と参加者が宣言し、幕を閉じた。

NISC はまた、話題性のあるコンテンツとして TV アニメ「BEATLESS」とタイアップしたポスターを製作し、若者らの関心を高めている(図 2-8-3)。

このキックオフイベントを皮切りに同月間の期間中、全国各地でイベントが実施された。

■図 2-8-3　官民連携サイバーセキュリティ月間ポスター
(出典)NISC「BEATLESS タイアップについて※332」

宮城県警察は、ラジオをとおして「不審なメールを開かない」「偽ショッピングサイトへの注意」等を訴え、群馬県警察は音楽隊のコンサート会場において、セキュリティに関するクイズを実施した。

また、警視庁は、東京商工会議所中央支部らと、「バレンタイン・サイバーセキュリティキャンペーン」を開催してセキュリティの対策方法が記載されたリーフレット等とチョコレートを配布し、大阪府警察は、大阪工業大学において、大阪府クレジットカード犯罪対策連絡協議会とともに作成した、パスワード設定の啓発資料を配布した。

佐賀県では、県、教育委員会、警察が「情報セキュリティ・モラルシンポジウム※333」を共催し、主に保護者や教職員を対象とした、インターネットトラブルの現状や取り組みの事例紹介等を行った。

このように、サイバーセキュリティ月間には、公共機関による多彩な啓発活動が全国で開催されている。セキュリティについて初めて学ぶ人にも分かりやすい資料の提供や講演が実施されることから、多くの市民の積極的な参加が望まれる。

(4) 企業・組織に対する取り組み

個人情報保護委員会は、2017年6月に「はじめての個人情報保護法～シンプルレッスン～※334」を公表した。これは、2017年5月の改正個人情報保護法施行により、5,000人分以下の個人情報を取り扱う小規模な事業者にも同法が適用されたことが背景となっている。この資料では、個人情報保護法を初めて意識する中小企業の理解を促すため、個人情報の定義等の基本情報や個人情報取得時・保管時のルールについて解説している。

2017年7月、東京都産業労働局が実施した都内中小企業に対する標的型メール攻撃訓練は目を引く取り組みであった※335。攻撃者からのメールを模した訓練メールを受信した後の対象者による開封状況や、アンケート結果等のレポートを参加企業が受け取ることができるもので、募集数を上回る応募があった。

このように、中小企業におけるセキュリティ対策の推進活動が行われる中、中小企業が自社のセキュリティ対策の実施を宣言することで、信頼性・安全性を高めるSECURITY ACTION制度がIPAによって開始された(「3.5.2(1)SECURITY ACTIONの取り組み」参照)。

2.8.2 民間企業・団体等による活動

本項では、民間企業・団体等による普及啓発活動について述べる。

(1) 企業・組織に向けた啓発活動

2017年12月の大手航空会社におけるビジネスメール詐欺被害に代表されるように、企業におけるセキュリティインシデントは後を絶たない。ネットワークを介した攻撃に備えた対策の実施はもちろん、有事の際には、被害を最小限に抑えるための対応が重要となる。このため、組織におけるCISOや、CSIRTの設置拡大が望まれている。

このような中、日本セキュリティオペレーション事業者協議会(ISOG-J)は、「セキュリティ対応組織(SOC/CSIRT)の教科書※336」の第2.0版を2017年10月に公開した。第2.0版には、インシデントの対応フロー、現状の改善ポイント等を明らかにするための「成熟度測定」等が新たに加えられた。この教科書は、セキュリティ対応の役割分担や体制について図解する等、CSIRT設置時に活用できる情報が掲載されており、利用の拡大が期待される。

また、ビジネスメール詐欺の理解度チェッククイズをトレンドマイクロ株式会社が提供しており、詐欺の手口や対策の解説資料とともにWeb上で公開されている(図2-8-4)。また、マカフィー株式会社はランサムウェアの侵入経路から攻撃の手口、対策に至るまでを紹介する動画を制作する等、セキュリティベンダによる啓発活動も盛んに行われている。

■図2-8-4 「ビジネスメール詐欺」の理解度チェック
(出典)トレンドマイクロ株式会社「【理解度チェック】初めてでも分かる!多額の損失をもたらす『ビジネスメール詐欺』に要注意※337」

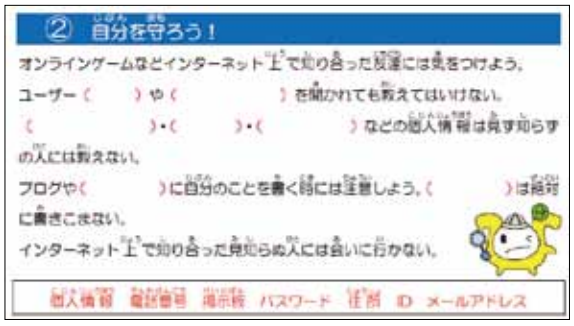
このような啓発資料のほか、セミナーによる情報発信も実施されている。特定非営利活動法人日本ネットワークセキュリティ協会(Japan Network Security Association:JNSA)は、2017年6月の福岡会場を皮切りに、全国5ヵ所において「全国横断セキュリティセミナー※338」を開催し

た。セミナーでは、中小企業でも発生し得る身近な脅威の動向や、情報セキュリティ対策ツールが紹介された。更に、情報セキュリティ機器等を導入する際に活用できる減税制度等についても解説がなされ、中小企業にとって有益な情報を得る機会となった。

(2) 一般国民に向けた啓発活動

安心ネットづくり促進協議会は、産業界、教育関係者等により組織され、青少年及びその保護者を対象とした普及啓発を行っている。2017 年 9 月には、10 歳ごろまでの子どものインターネット利用対策として、年齢に合わせたアプリの利用制限設定や、不適切な動画の除外設定を、保護者向けの資料として公開した※339。本資料は、大人のための「情報モラル & マナー」チェックシートも掲載しており、保護者が普段のインターネットの利用を見直す資料としても活用できる。

香川県の情報通信交流館「e-とぴあ・かがわ」では、子ども達がクイズを解きながら情報セキュリティを学べるイベントとして、セキュリティ啓発コーナーを設置した。子どもにとって多少困難な問題も出題し、保護者と一緒に考えてもらう工夫がなされている(図 2-8-5)。



■図 2-8-5　穴埋めセキュリティチェック
(出典)情報通信交流館 e-とぴあ・かがわ「サイバーセキュリティクイズ」

フィッシング対策協議会が開催した「STOP. THINK. CONNECT.」啓発イベント※340 では、主にインターネット安全利用の普及活動を行う人のスキル向上のために、カードゲーム等を利用したセキュリティ指導を体験する場を提供した。

このような指導者を育成する取り組みのほか、青少年の相談を受け付ける新たな体制の模索も始まっている。

SNS は子ども達のコミュニケーション手段として広く利用されているが、SNS 等を介したいじめは依然として大きな問題である。いじめに関して気軽に相談できる環境を提供するため、LINE 株式会社と長野県は、青少年の利用率が高い LINE によるいじめ等の相談窓口を試験的に開設した。中間報告資料※341 によると、相談期間の 2017 年 9 月 10 日から 9 月 23 日の間に約 188 人／日のアクセスがあり、子ども達の関心の高さがうかがえた。SNS による相談受付の課題として、共感や寄り添いを伝えやすい状況を作るために電話へ切り替えることも必要であること、コストが割高であること等が挙げられたものの、相談件数は 2 週間で、前年度の電話による年間件数の 2 倍以上となり、一定の効果も見られた。悩みを抱えた子ども達が相談できる環境の見直しと再構築が急務であり、この取り組みはその大きな一歩と言える。

SNS サービス事業者側の対策も進んでいる。Twitter, Inc. は、2017 年 12 月より新ルールの適用を開始した※342。新ルールでは、サービスを利用して差別や中傷、人権侵害となる表現を行うアカウントを永久凍結する等が追加され、また、自殺や自傷行為の助長や扇動も禁止された。Facebook, Inc.、Instagram, LLC においても、自殺をほのめかす投稿を報告できる措置が既に取られている。

これらのサービス事業者による対策の促進は、利用者の悪用、不適切・不道徳な利用が後を絶たないことが背景となっていることから、利用者一人ひとりの慎重な発言・表現が改めて重要になっている。

金銭を狙うサイバー攻撃等の手口から財産を守るための一般向け啓発資料としては、一般社団法人日本クレジット協会による動画「コロッ家の人々※343」が挙げられる。インターネットショッピングを行う際に注意すべきパスワードの設定について、ドラマをとおして理解することができる。

このようなツールや資料は、官民ボード※344 によって公開されている情報セキュリティ・ポータルサイト「ここからセキュリティ!※345」において、対象者別、脅威別に紹介されている。インターネットを取り巻く脅威や手口等を知ることが対策の一歩であることから、インターネットを利用するすべての人が当該サイトを活用することを推奨する。

2.8.3 児童・生徒・学生による活動

特定非営利活動法人東海インターネット協議会によるインターネット安全教室では、金城学院大学長谷川ゼミの学生が、大学生から見たネットの危険性について講演を実施した。セキュリティの専門家ではない女子学生が、同世代の利用率が高い SNS を解説し、写真等を投稿することのリスクについて説明を行った。

IPA が主催する「ひろげよう情報モラル・セキュリティコンクール※346」において文部科学大臣賞を受賞した兵

庫県立千種高等学校の活動は、自校内にとどまらない取り組みとしてモデルケースと言えるものである。生徒会執行部が中心となり、「情報モラル改善ルール」を定めたほか、地域の園児、小中学生を対象とした「情報モラル啓発劇」を毎年上演する等の活動を行ってきた。また、2015 年度は地域住民を対象とした「高校生によるスマートフォン教室」を、2016 年度は「教職員のためのスマートフォン教室」を主催する等、大人を巻き込む取り組みも行い、「教える立場」に立つことで、地域住民の知識と意識の向上を図った。更に、地域の小中高生を対象にした利用状況調査も実施し、高校生が結果を分析して「千種町インターネット宣言 2016」につなげている（図 2-8-6）。

■図 2-8-6　インターネットサミット in CHIKUSA における千種高等学校生徒の活動の様子

横浜市立大岡小学校では、6 年生の「総合的な学習」の中で株式会社ディー・エヌ・エーによるプログラミング授業を行い、児童が地域の魅力を伝えるアニメーションを制作した。アニメーションの中に商店街等のキャラクターを登場させる際、子ども達がその使用について承諾を求める文書を自ら作成し、商店街協同組合理事長に提出する等、関係者を驚かせる意識の高さを見せた（図 2-8-7）。

■図 2-8-7　横浜市立大岡小学校 6 年 2 組による商店街キャラクターの使用承諾を求める文書

2.8.4 インターネット利用者の責任

IPA が実施した「2017 年度情報セキュリティの倫理に対する意識調査※347」によると、会社員や生徒・学生におけるインターネットや情報に関する倫理教育の受講経験率は比較的高い。企業や学校に在籍していれば、このような教育を受ける機会を得ることができる。また、2022 年からの「高等学校学習指導要領（案）※348」では、「情報I」が新設され、情報セキュリティ及びモラルに関する指導が盛り込まれていることから、これからの子ども達は一定の知識を習得していくことが予定されている。一方で、専業主婦・主夫、定年による退職者や家事手伝い等、組織に属さない大人の受講経験率は 20% に満たない現状が見て取れ、大きな課題だと言える。

南カリフォルニア大学が日本の中高生 600 人とその保護者 600 人に行った調査※349では、中高生の 20% が「親は自分よりスマートフォン等の携帯機器のほうが大切だ」と感じたことがあると回答している。また、日本の保護者が「スマートフォン等の携帯機器の利用時間を減らすよう終始努めている」と回答した率はわずか 4% にとどまり、米国の 23% と大きな差があることも同調査により判明している。親のスマートフォン等の携帯機器利用が、子どもとのコミュニケーションを希薄にしている可能性があり、親の利用状況も課題と言える。

インターネットの危険から子ども達を守るためには、大人が常に見守るだけではなく子ども自身が自衛手段を身に付けることが重要であることは言うまでもない。しかし、そのために必要なインターネットの安全な使い方、手本となる使い方を示すべきなのは周囲の大人である。ここで紹介した啓発イベント、資料等を活用し、インターネット利用者全員が、情報セキュリティ意識を向上させ、情報の取り扱い、インターネット上の振る舞いに注意を傾けていくことが期待されている。

COLUMN

好きなものだけあれば良いの？

こんにちは！　ぼくは、IPA「ひろげよう情報モラル・セキュリティコンクール」応援隊長のまもるです。今回は「好きなものに囲まれる生活」について考えたことをお話しします。

ぼくはトマトとピーマンが苦手です。だから、いつもお皿のはしっこによけながら「嫌いなものはこの世の中からなくなって、好きなものだけに囲まれていられたらよいのに!」と思っていました。

でも、「今は、自分が好きなものや興味があるものだけを簡単に選べる時代だけど、それは本当に良いことなのかどうか、よく考えないといけないよ」とお父さんが話してくれました。

「例えば、おもちゃや本をインターネットで探していると、いつのまにかまもるが好きそうなおもちゃや本が表示されるようになるだろう。お父さんがインターネットでニュースを読んでいても、『おすすめのニュース』が表示されるんだ。好きなものや興味があるものが表示されるから、とても便利なんだけど、一方で限られた情報しか見ていない、という考え方もできるんだよ」

たしかに、学校では苦手な授業もあるし、いろいろな友達がいて意見が分かれることもある。でもインターネットだと、ぼくの好きなものだけを選んで見ることができるし、SNS では「意見が合う人」とだけつながることができる。

「ただ、そうやって選ばなかった情報やつながりの中には、自分の頭のなかにはなかった『新しい考え』や『ものの見かた』が隠れているかもしれない。好きなものばかり見ていると、そういうものに触れる機会が減ってしまうかもしれない。それに、『好きなものだけに囲まれている生活』に慣れてしまうと、『好きじゃないもの』に出会った時、どうしていいのかわからなくて、必要以上におびえたり、攻撃的になってしまったりするかもしれない。それはどうなのかな」とお父さんが話してくれました。

これからは、今までは興味がなかったものや苦手なものにも挑戦して「自分が知らなかった自分」を見つけてみようと思いました。

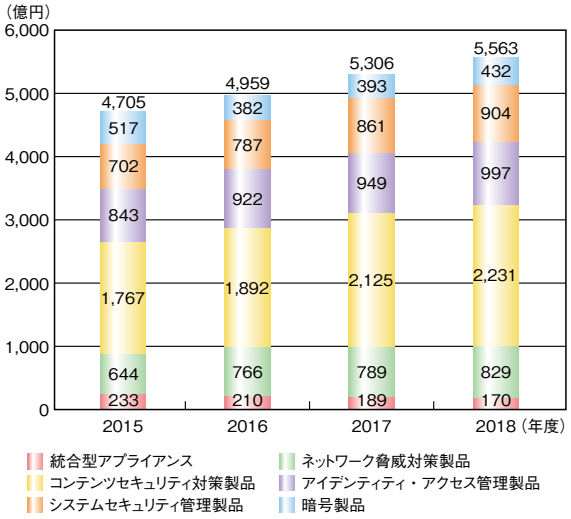
2.9 その他の情報セキュリティの状況

情報セキュリティ産業の規模と成長の動向、営業秘密保護の動向、及び暗号技術の動向について述べる。

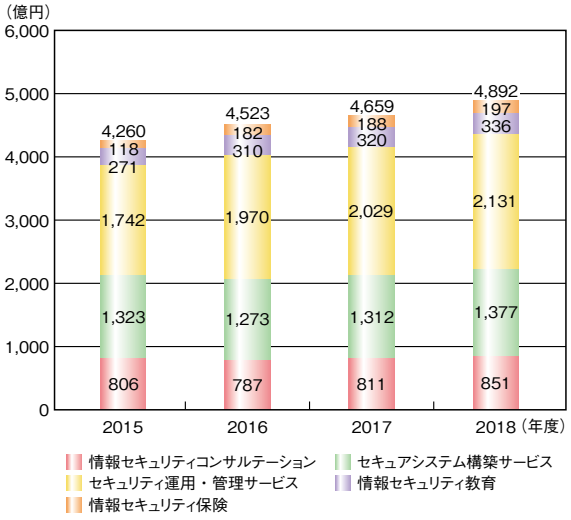
2.9.1 情報セキュリティ産業の規模と成長の動向

JNSA が発表した「国内情報セキュリティ市場 2017 年度調査報告（速報値）※350」によると、2017 年度の情報セキュリティ市場規模（ツールとサービスを合わせた数値）は、2016 年度より 5.1% の伸びとなる見込みである。

情報セキュリティのツールとサービスそれぞれの市場規模推移を図 2-9-1 と図 2-9-2 に示す（市場区分定義については表 2-9-1 参照）。なお、図中の 2015 年度、2016 年度について実績推定値、2017 年度については見込み推定値、2018 年度については予測値である。



■図 2-9-1　国内情報セキュリティツール市場規模の推移
（出典）JNSA「国内情報セキュリティ市場 2017 年度調査報告（速報値）」を基に IPA が編集



■図 2-9-2　国内情報セキュリティサービス市場規模の推移
（出典）JNSA「国内情報セキュリティ市場 2017 年度調査報告（速報値）」を基に IPA が編集

分類		説明
セキュリティツール		
	統合型アプライアンス	FW、IDS、ウイルス対策等複数機能を持ったアプライアンス
	ネットワーク脅威対策製品	FW、IDS/IPS、VPN、アプリケーションファイアウォール
	コンテンツセキュリティ対策製品	ウイルス対策、スパム対策、URL フィルタ、メールフィルタ、DLP 等
	アイデンティティ・アクセス管理製品	認証、ログオン管理・アクセス許可、PKI 製品
	システムセキュリティ管理製品	セキュリティ情報統合管理、ポリシー・アクティビティ管理ツール、脆弱性検査ツール　等
	暗号製品	暗号化製品、暗号モジュール
セキュリティサービス		
	情報セキュリティコンサルテーション	ポリシー構築、監査・診断等セキュリティ管理全般コンサルティング、規格認証取得支援サービス
	セキュアシステム構築サービス	IT セキュリティの設計、導入、製品選定支援　等
	セキュリティ運用・管理サービス	マネージドサービス（IT セキュリティの監視、運用支援）、プロフェッショナルサービス、電子認証サービス　等
	情報セキュリティ教育	教育実施、コンテンツ提供、教育 ASP、資格認定　等
	情報セキュリティ保険	情報セキュリティおよび IT セキュリティ保険

■表 2-9-1　情報セキュリティ産業の市場区分
（出典）JNSA「国内情報セキュリティ市場 2017 年度調査報告（速報値）」

情報セキュリティツールの市場規模全体では、2016年度から2017年度は7.0%伸びている。ツール別に見ると、「コンテンツセキュリティ対策製品」の前年度比12.3%増、「システムセキュリティ管理製品」の前年度比9.3%増を始め、各区分もおおむね増加傾向が続いているが、「統合型アプライアンス」は2015年度以降、前年比約10%減の状態が続いている。

情報セキュリティサービスの市場規模全体では、2016年度から2017年度は3.0%伸びており、2018年度には5.0%の伸びが見込まれている。これはツール全体の2018年度の見込み伸び率4.8%を上回っている。

2.9.2 営業秘密保護の動向

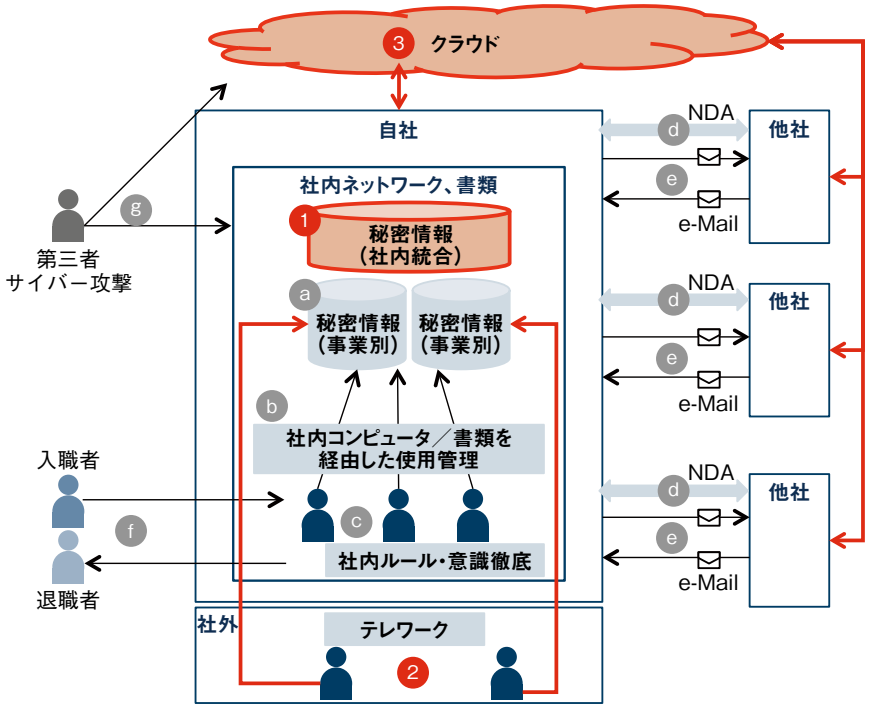
2017年度は大きな話題となる営業秘密※351の漏えい事案は報道されなかった。しかし、2016年度にIPAが実施した営業秘密管理の実態調査※352でも傾向が示されたとおり、報道されない水面下の情報漏えいインシデントは後を絶たない。

営業秘密保護に関しては、公的な指針・ガイドラインとして、2015年1月に全部改訂された「営業秘密管理指針※353」や2016年2月に公表された「秘密情報※354の保護ハンドブック※355」が整備され、その重要性や営業秘密情報管理の基本的な考え方、情報漏えい対策の例等が周知されてきた。一方で、近年の様々なIT技術の進展や社会環境の変化、例えば「モバイル機器の浸透と活用」「クラウド利用機会の浸透」「ビッグデータ分析機会の増加」等の変化により、データ利活用による新しい価値・サービスの創出が期待されている。今後の情報管理では、データ利活用のために関係組織と情報を共有しつつ、営業秘密は確実に保護することが求められる。

(1) 新しい営業秘密保護の課題

こうした新しい状況における営業秘密を含む秘密情報管理の在り方を探るため、IPAは2017年度に「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査※356」を実施した。本調査ではまず、新しい基盤・環境においてデータ利活用と秘密情報の保護を両立させるには何が必要か、という視点に基づいて、秘密情報管理上の課題やリスクを抽出した。また、それらの課題に対する現状認識や取り組み等について、新しい情報管理や基盤利用を積極的に行っている企業や有識者からヒアリングを行い、情報を収集した。

本調査では、企業の情報管理における新しい基盤・環境の影響を具体的に見るため、情報管理を中心とした企業の業務形態モデルを作成した（図2-9-3）。図中のａ～ｇは、従来行われている情報管理の流れを示し



■図2-9-3 「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」での課題の位置付け

ている。一方、新しい基盤・環境として、データ利活用、業務形態の変化等を考慮し、本モデルでは以下の三つの課題に注目して調査を実施した（図中の①～③）。

①事業単位で管理されてきた情報の利活用に向けた社内統合（秘密情報を含む）

②リモートで業務遂行ができる環境におけるテレワーク

③クラウド利用による情報の社外管理・分析

まず、本調査で得られた三つの課題に対する企業の課題認識についてまとめる。

①秘密情報の統合と利活用の課題認識

データ統合に際して、アクセス権と匿名性についての課題がある。

- 従来のデータ管理は基本的に事業単位であり、組織横断的な共有ルールが確立されていないことが多い。こうした場合、組織横断的にデータを統合しようとすると、利活用する部分のデータ切り出しとデータへのアクセス権が問題となる。例えば、複数の部門や事業を横断するデータの統合・共有により情報管理区分が重層化し、アクセス権管理が複雑化しがちである。
- 異なる顧客サービスの匿名化されたデータを統合すると、個人の属性が組み合わされ、個人情報の匿名性が損なわれる可能性があることや、個人データを他のデータと組み合わせて活用することを前提としてデータ収集が必ずしもされていない、といった懸念もある。

②テレワークの課題認識

多様な働き方が一定程度浸透し[※357]、テレワークを実践に移している企業でも、テレワークに伴う情報管理は必ずしも十分ではないことがある。企業によっては「リモートアクセス用端末の支給」「セキュリティ管理ツールの導入」「リモートアクセス時のアクセス権の厳格化」等の施策を、既に実施しているケースも多いが、社外で働く故に必然的に生じる「見えない部分」による情報漏えいリスクを考慮した対策までは難しい。例えば現状では、社外で会社が把握しない機器で業務が行われること等により、秘密情報が情報漏えいのリスクに晒されることを防ぐことは困難である。

③クラウド利用の課題認識

- クラウド上の情報も、オンプレミスの場合と同じく管理・保護されなければならない。しかし、パブリッククラウドに格納された情報は管理者から把握しづらく、自社のセキュリティポリシーをそのまま適用することが難しいことがある。そのため、情報管理区分を維持、徹底させることがオンプレミスでの管理に比べて困難である。
- クラウドのデータセンターが国外にある場合、問題発生時の責任範囲や原因分析等の運用が不明確、技術情報の国外流出等のセキュリティ上の懸念が生じ得る。
- 社内／社外から新規パブリッククラウドの利用希望があった場合等に、実績が少ないクラウドではセキュリティ上の懸念が生じ得る。

(2) 課題に対する対策

三つの課題について、本調査で得られた対策状況を述べる。状況を概括すると、①は全体として課題認識が進みつつあるが対策はまだこれからであり、②③は実践が進んでいるものの、管理しきれない課題が顕在化している。

①秘密情報の統合と利活用について

- アクセス権の対策

  組織横断的にデータを利活用するため、企業内の秘密情報の統合後のデータ保管場所や統合情報の情報管理区分の明確化、利活用の必要性に応じた適切なアクセス権の再検討が行われつつある。これらの対策を進める上で最も重要なことは「標準化」である。複数組織において秘密区分や情報の共有範囲、秘密保持期間等が異なっていては、統合すること自体が困難となる。また、同じ秘密区分の情報に対し、組織ごとにアクセス権限にばらつきがあると、統合後に支障が生じる。今後の秘密情報管理においては、それらを見越した標準化作業がポイントとなる。
- 匿名性の課題への対策

  GDPR への対応、個人情報保護関連法制への遵守等はこれまで以上に厳密に実施していかなければならない。複数の匿名化された顧客データを統合する場合、統合後に適切な再匿名化を行うことや、統合が必要かを慎重に点検しながらデータ利活用を進める等の対策が行われつつある。

②テレワークについて

テレワークは、企業によっては既に実践が進んでいる。シンクライアント PC[※358]、MDM[※359]、ログ管理ツール等の情報管理環境の整備等、適切なセキュリティ機能を導入しリスク低減を行っている企業が多い。

- 「見えない部分」の情報漏えいリスク対策

職務権限に応じたアクセス権限の厳格化や、テレワーク時のルールを徹底する等の運用上の対策が行われつつある。従業員との信頼関係を醸成し、許可されていないパソコンやデバイスの使用禁止といったルールや情報管理規則の徹底を行うことが、有効な対策として考えられる。

③クラウド利用について

クラウドの利活用も、企業によっては管理方針を決定しながら実践が進んでいる。管理方針検討の際は、関連するガイドライン※360 等が参照できる。クラウドを利用することで、情報管理の設備・管理コストを大幅に低減できる可能性があり、情報セキュリティに留意しながら有効に活用することが行われつつある。

- クラウド情報の管理・保護対策
  クラウドに格納するデータを選定する際のルールの厳格化や、データの可視化や保護を可能とする管理ツールの導入等が行われつつある。
- パブリッククラウド選定対策
  クラウドベンダ選定のルールや基準を厳格化する等のリスク軽減対策が行われつつある。なお、パブリッククラウド利用開始後は、サービス内容やセキュリティ内容の変更が行われていないか、定期的にクラウドの約款・規約等を確認することも、今後は重要な留意事項となる。
- サプライチェーン対策
  サプライチェーンの関係各社で情報を共有する場合、各社横並びで情報のセキュリティを確保するための対策が検討されつつある。共通のクラウド上で同一の運用ルールに従い共有情報を管理することが、そのための有効な対策として行われつつある。
- 事故発生時の対策
  クラウドでのセキュリティ事故発生時の原因究明の分担を決めておくことの重要性が認識されつつある。事故原因究明を行うためのログ分析等の分担をあらかじめ明らかにしておくこと等が、有効な対策として行われつつある。

本調査で得られた主な課題・対策を表 2-9-2 にまとめる。

2.9.3 暗号技術の動向

本項では暗号技術の動向として、共通鍵暗号技術に対する攻撃の動向と、公開鍵暗号技術に対する攻撃の動向について解説する。また、NIST で標準化が開始された耐量子計算機暗号の状況について解説する。

(1) 共通鍵暗号技術に対する攻撃の動向

共通鍵暗号技術に対する攻撃としては、2015 年度には「CRYPTREC 暗号リスト※94」掲載のブロック暗号 MISTY1 に対する攻撃に、また、2016 年度には同リスト掲載のハッシュ関数 SHA-1 に対する攻撃に大きな進展があった。

2017 年度はこれらに相当する大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃可能な段数の増加、攻撃に必要な計算量の削減等、

場面	課題	技術面の対策	運用面の対策
秘密情報の統合と利活用	アクセス権	・統合化データの区分に応じた隔離・アクセス権再設定	・統合前の管理区分・アクセス権限の明確化、標準化 ・統合後のデータ格納場所や管理方法の明確化
	匿名性確保	・統合前の対象データの適切な匿名化措置 ・統合後の再匿名化措置	・統合の必要性点検 ・匿名化状況のチェック ・法制遵守状況のチェック
テレワーク	情報漏えいリスク（「見えない部分」のリスク）	・シンクライアント PC、MDM、ログ管理ツール等の設備の整備	・職務権限に応じたアクセス権限の厳格化 ・テレワーク時の秘密情報管理規程等の運用ルール教育（例：テレワークで利用する機器とそのセキュリティ対策の申告等）
クラウド利活用	クラウド格納情報管理・保護	・データの可視化・保護を行う管理ツールの整備 ・クラウド事業者との責任分担に基づくセキュリティ対策（例：IaaS アプリケーションのアクセス権設定等）	・クラウド格納情報を選定する際のルールの強化 ・クラウドに預けるデータの適正な管理区分やアクセス権管理の強化 ・クラウド運用状況報告のタイムリーな把握 ・クラウドの情報管理関連ガイドラインの活用
	パブリッククラウド選定	・開示情報・認証等によるクラウド事業者の技術力評価	・クラウドベンダ選定ルールの策定、徹底 ・クラウド事業者の法制遵守状況評価

■表 2-9-2　秘密情報管理の主な課題・対策

着実な進展があった。ここでは主な発表を紹介する。

- 米国標準ブロック暗号 AES に対する攻撃
  国際会議 EUROCRYPT 2017[※361] において、米国標準ブロック暗号で CRYPTREC 暗号リスト（電子政府推奨暗号リスト）にも掲載されている 128 ビットブロック暗号 AES（Advanced Encryption Standard）の 5 段の識別子[※362] が示された。これまで AES の識別子としては 4 段のものは知られていたが、5 段のものが示されたのは初めてである。
  またその後開催された国際会議 Asiacrypt 2017[※363] において、SPN（Substitution Permutation Network）構造の新しい基本的性質を導入し、適応的選択暗号文／平文の設定において、AES の 3 ～ 5 段に対してこれまで知られていたものより、より効率的な識別子と攻撃に必要なデータ量（各段に対し各々 3, 4, $2^{25.8}$ の平文／暗号文のペア）が示された。更に、AES の 6 段の識別子が初めて示されたが、攻撃には $2^{122.83}$ の平文／暗号文ペアを必要とするためこの攻撃は現実的ではない。また、短縮化された 5 段の AES に対して、$2^{11.3}$ のデータ量及び 2^{31} の計算による鍵回復攻撃も示された。
  これらのように AES に対する攻撃は 2017 年度も着実な進展は見られたが、128 ビット鍵の AES のフルスペックの段数は 10 段であり、これらの結果は AES の安全性に直ちに影響を与えるものではない。
- 米国標準ハッシュ関数 SHA-3 に対する攻撃
  EUROCRYPT 2017 において、米国標準ハッシュ関数で CRYPTREC 暗号リスト（推奨候補暗号リスト）にも掲載されている SHA-3 の元となったハッシュ関数 Keccak に対する衝突攻撃が提案され、Keccak-224（224 は出力されるハッシュ値のビット数）の攻撃可能な段数を、従来示されていた 4 段から 5 段に伸ばした。また、Keccak-256（256 は出力されるハッシュ値のビット数）の従来の攻撃可能な段数（4 段）での解読計算量を削減した。更に、SHA-3 ファミリーの一つである SHAKE128（128 は内部処理の単位ビット数。出力されるハッシュ値のビット数は可変）の 5 段に対する攻撃を初めて示した。ただし、Keccak/SHA-3 のフルスペックの段数は 24 段であり、これらの結果は Keccak/SHA-3 の安全性に直ちに影響を与えるものではない。
- 米国標準ハッシュ関数 SHA-1 に対する攻撃
  国際会議 Crypto 2017[※364] において、米国標準ハッシュ関数で CRYPTREC 暗号リスト（運用監視暗号リスト）にも掲載されている SHA-1 に対して、フルスペックの SHA-1 に対する衝突攻撃が示された。「情報セキュリティ白書 2017」に詳細を記載しているので、そちらを参照していただきたい[※365]。なお、当該発表は Crypto 2017 において Best Paper Award を受賞した。権威ある Crypto 2017 での受賞であることから、学術的にも意義の高い成果であることが認められた形となった。
- ハッシュ関数 RIPEMD-160 に対する攻撃
  Asiacrypt 2017 において CRYPTREC 暗号リスト（運用監視暗号リスト）掲載のハッシュ関数 RIPEMD（RACE Integrity Primitives Evaluation Message Digest）-160（160 は出力されるハッシュ値のビット数）に対する衝突攻撃及び semi-free-start 衝突攻撃[※366] が発表された。RIPEMD-160 の段差分確率を理論的に計算する方法により、従来の差分パスを自動的に発見する方法を改良し、30 段に短縮化された RIPEMD-160 の衝突を 2^{67} の計算量で発見した。これは RIPEMD-160 の縮退版に対する初めての衝突攻撃である。更に 36 段に短縮化された RIPEMD-160 に対する既存の semi-free-start 衝突攻撃を改良することにより、計算量を $2^{70.4}$ から $2^{55.1}$ に削減した。ただし、RIPEMD-160 のフルスペックの段数は 80 段であり、これらの結果は RIPEMD-160 の安全性に直ちに影響を与えるものではない。なお、RIPEMD-160 は仮想通貨ビットコインで利用されているハッシュ関数の一つである。

なお、CRYPTREC としては、安全性を考慮してハッシュ関数のハッシュ長は 256 ビット以上を推奨している。ハッシュ長が 160 ビットである SHA-1 や RIPEMD-160 は従来システムとの互換性維持のために運用監視暗号リストに掲載し、より安全なハッシュ関数である SHA-256 等への移行を推奨している[※367] ことに注意されたい。

(2) 公開鍵暗号技術に対する攻撃の動向

電子署名及び鍵共有の安全性に影響する離散対数問題の解読に進展が見られた。電子政府推奨暗号 DSA（Digital Signature Algorithm）及び DH（Diffie-Hellman）を利用する際には、これらの解読の影響がないような鍵長やパラメータを選択するよう注意を要する。以下に主な発表を 2 件紹介する。

EUROCRYPT 2017 において、Thorsten Kleinjung 氏らは、NFS（Number Field Sieve、数体ふるい法）[※368] により 768 ビットの素体上の離散対数問題の計算に成功

したと報告した。これまでの素体上の離散対数問題の記録（596ビットの素体上）から大きく進展した結果であり、素因数分解問題と離散対数問題との解読記録のこれまでの差を大きく縮める結果でもある。計算時間はトータルで約5,300コア・年（Intel Xeon E5-2660 2.2GHz）であり、報告者らの大学のクラスタ環境で計算に2015年の5月から12月までをほぼ費やしたとのことである。CRYPTREC暗号リスト（電子政府推奨暗号リスト）掲載の公開鍵暗号で素体上の離散対数問題の困難さに安全性の根拠を置くものとして、署名のDSAと鍵共有のDHが該当するが、素数のサイズが2,048ビット以上であれば本報告の結果は直ちにその安全性に影響を与えるものではない。

同じくEUROCRYPT 2017において、Joshua Fried氏らは、SNFS（Special NFS、特殊数体ふるい法）※369により、1,024ビットの素体上での離散対数問題の計算に成功したと報告した。キロビットサイズの素体上の離散対数問題の計算としては世界初の結果である。計算時間はトータルで約400コア・年（Intel Xeon E5-2650 2.0GHz）であり、報告者らのクラスタ環境でオープンソースCADO-NFSで実装し、計算に2ヵ月程度費やしたとのことである。本計算で用いられた離散対数問題のパラメータ素数pはDSAのパラメータ推奨に沿って、p-1が160ビットの素因数を持つが、SNFSで離散対数問題が計算可能となるように、約25年前に提案されたGordonの方法により、pにトラップドア※370が仕掛けられている。提案当時はトラップドアが仕掛けられていることを隠すことは困難であったが、現在の技術では、見ただけでは分からないトラップドアを1,024ビットのパラメータpに仕掛けることが可能となった。署名のDSA、鍵共有のDHを用いる際には、上記のパラメータを利用する必要があるが、本トラップドアを防ぐには、ランダムに生成されたことが検証可能な素数pを用いる必要がある。ただし、現在の計算機能力では、素数のサイズが2,048ビット以上であれば本報告の結果は直ちに安全性に影響を与えるものではない。

(3) 耐量子計算機暗号標準化の動向

NISTによる量子計算機に耐性を持つ暗号（PQC：Post-Quantum Cryptography）公募が2017年11月30日に締め切られ、応募暗号の仕様がNISTホームページ上に公開され、評価が開始された。PQCコンペティションにおいて、応募暗号の安全性・処理性能評価は、これまでの標準ブロック暗号AESやハッシュ関数SHA-3のように、世界中の暗号研究者によりボランティアで行われることが見込まれる。Asiacrypt 2017におけるNISTの招待講演では、耐量子暗号コンペティションへの応募総数は82件と発表された。その内訳件数を表2-9-3に示す。

2018年4月12～13日に米国フロリダ州で第1回PQC標準化会議が開催され、これから5年程度かけて、PQC標準を制定していく予定である。

	電子署名	鍵カプセル化／暗号化	合計
格子ベース	4	24	28
符号ベース	5	19	24
多変数多項式	7	6	13
ハッシュベース	4	0	4
その他	3	10	13
合計	23	59	82

■表2-9-3　NIST PQCコンペティション応募暗号
（出典）Dustin Moody（NIST）「The ship has sailed: The NIST Post-Quantum Crypto "competition"※371」を基にIPAが編集

※ 1　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf〔参照 2018-05-18〕
※ 2　http://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf〔参照 2018-05-18〕
※ 3　http://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf〔参照 2018-05-18〕
※ 4　http://www.soumu.go.jp/main_content/000428393.pdf〔参照 2018-05-18〕
※ 5　http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf〔参照 2018-05-18〕
※ 6　サイバーセキュリティ戦略本部：サイバーセキュリティ人材育成プログラム　http://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf〔参照 2018-05-18〕
※ 7　http://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔参照 2018-05-18〕
※ 8　NICT：サイバーコロッセオ 平成 29 年度開催報告　http://colosseo.nict.go.jp/report_h29.html〔参照 2018-05-18〕
※ 9　サイバーセキュリティ対策推進専任審議官等会議・各府省情報化専任審議官等連絡会議 事務局：「各府省庁セキュリティ・IT 人材確保・育成計画」の実施状況等について　http://www.nisc.go.jp/conference/cs/taisaku/shingikan/dai10/pdf/10shiryou2.pdf〔参照 2018-05-18〕
※ 10 NISC：橋渡し人材のスキル認定の基準　http://www.nisc.go.jp/conference/cs/taisaku/shingikan/dai10/pdf/skill_nintei.pdf〔参照 2018-05-18〕
※ 11 NISC：「ネットワークビギナーのための情報セキュリティハンドブック」について　https://www.nisc.go.jp/security-site/handbook/index.html〔参照 2018-05-18〕
※ 12 http://www.nisc.go.jp/active/kihon/pdf/kenkyu2017.pdf〔参照 2018-05-18〕
※ 13 国立研究開発法人新エネルギー・産業技術総合開発機構：戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保　http://www.nedo.go.jp/activities/ZZJP_100109.html〔参照 2018-05-18〕
※ 14 NISC：「セキュリティマインドを持った企業経営ワーキンググループ報告書（案）」及び「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書（案）」に関する意見募集について（終了しました）　https://www.nisc.go.jp/active/kihon/jinzai-wg2018.html〔参照 2018-05-18〕
※ 15 https://sechack365.nict.go.jp/〔参照 2018-05-18〕
※ 16 https://cyder.nict.go.jp/〔参照 2018-05-18〕
※ 17 http://www.nisc.go.jp/active/infra/pdf/shishin5.pdf〔参照 2018-05-18〕
※ 18 NISC：重要インフラ専門調査会　http://www.nisc.go.jp/conference/cs/ciip/index.html〔参照 2018-05-18〕
※ 19 http://www.nisc.go.jp/active/infra/files/tebikisho.zip〔参照 2018-05-18〕
※ 20 http://www.nisc.go.jp/active/infra/files/riskhyoka.ZIP〔参照 2018-05-18〕
※ 21 NISC：リスクマネジメントの促進のための取組概要　https://www.nisc.go.jp/conference/cs/dai16/pdf/16shiryou05.pdf〔参照 2018-05-18〕
※ 22 NISC：2017年度「分野横断的演習」について　https://www.nisc.go.jp/conference/cs/ciip/dai14/pdf/14shiryou08.pdf〔参照 2018-05-18〕
※ 23 セプターカウンシル：セプターカウンシル総会第 10 回会合の開催について　http://www.nisc.go.jp/active/infra/pdf/cc_dai10.pdf〔参照 2018-05-18〕
※ 24 NISC：2017 年度セプター訓練について　http://www.nisc.go.jp/conference/cs/ciip/dai14/pdf/14shiryou09.pdf〔参照 2018-05-18〕
※ 25 NISC：「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）」に関する意見の募集について（終了しました）　https://www.nisc.go.jp/active/infra/pubcom_shinkokudo.html〔参照 2018-05-18〕
※ 26 http://www8.cao.go.jp/cstp/sogosenryaku/2017.html〔参照 2018-05-18〕
※ 27 https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf〔参照 2018-05-18〕
※ 28 http://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou02.pdf〔参照 2018-05-18〕
※ 29 経済産業省：サイバーセキュリティ経営ガイドラインを策定しました　http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html〔参照 2018-05-18〕
※ 30 経済産業省：サイバーセキュリティ経営ガイドライン 1.1 版　http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v1.1.pdf〔参照 2018-05-18〕
※ 31 IPA：サイバーセキュリティ経営ガイドライン改訂に関する研究会　https://www.ipa.go.jp/security/economics/CSM-Guideline-Workshop.html〔参照 2018-05-18〕
※ 32 http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔参照 2018-05-18〕
※ 33 NIST：Framework Documents　https://www.nist.gov/cyberframework/framework〔参照 2018-05-18〕
※ 34 経済産業省:我が国産業が目指す姿（コンセプト）として「Connected Industries」を発表しました　http://www.meti.go.jp/press/2016/03/20170320001/20170320001.html〔参照 2018-05-18〕
※ 35 経済産業省：「Connected Industries」大臣懇談会を開催しました　http://www.meti.go.jp/press/2017/05/20170529008/20170529008.html〔参照 2018-05-18〕
経済産業省：「Connected Industries」大臣懇談会（第 2 回）を開催しました　http://www.meti.go.jp/press/2017/07/20170706004/20170706004.html〔参照 2018-05-18〕
※ 36 経済産業省：”Connected Industries”シンポジウムを開催しました　http://www.meti.go.jp/press/2017/06/20170619005/20170619005.html〔参照 2018-05-18〕
経済産業省：IoT 推進ラボ合同イベント「Connected Industries」シンポジウムを開催します　http://www.meti.go.jp/press/2017/07/20170718002/20170718002.html〔参照 2018-05-18〕
経済産業省：CEATEC JAPAN 2017「Connected Industries」シンポジウムを開催します　http://www.meti.go.jp/press/2017/09/20170919001/20170919001.html〔参照 2018-05-18〕
※ 37 CEATEC JAPAN 運営事務局：CEATEC JAPAN 2017 開催実績　http://www.ceatec.com/ja/application/result/〔参照 2018-05-18〕
※ 38 http://www.meti.go.jp/press/2017/10/20171002012/20171002012-1.pdf
※ 39 経済産業省：Connected Industries　http://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html〔参照 2018-05-18〕
※ 40 経済産業省：「産業サイバーセキュリティ研究会」を開催します　http://www.meti.go.jp/press/2017/12/20171226004/20171226004.html〔参照 2018-05-18〕
※ 41 http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_05_00.pdf〔参照 2018-05-18〕
※ 42 経済産業省：「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」の意見公募手続（パブリックコメント）を開始しました。http://www.meti.go.jp/press/2018/05/20180502003/20180502003.html〔参照 2018-05-18〕
※ 43 経済産業省：セキュリティ産業のビジネス化研究会の取りまとめ　http://www.meti.go.jp/policy/netsecurity/downloadfiles/research_group_summary.pdf〔参照 2018-05-18〕
※ 44 経済産業省：情報セキュリティサービス基準及び情報セキュリティサービスに関する審査登録機関基準を策定しました http://www.meti.go.jp/press/2017/02/20180228002/20180228002.html〔参照 2018-05-18〕
※ 45 総務省：総務省と経済産業省の連携チームの発足　http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000219.html〔参照 2018-05-18〕
※ 46 経済産業省：総務省と経済産業省の連携チームの検討成果を取りまとめました　http://www.meti.go.jp/press/2018/05/20180502004/20180502004.html〔参照 2018-05-18〕
※ 47 経済産業省：経済産業関係　平成 30 年度税制改正のポイント　http://www.meti.go.jp/main/zeisei/zeisei_fy2018/zeisei_k/pdf/zeiseikaiseipoint.pdf〔参照 2018-05-18〕
※ 48 総務省：「情報銀行」の認定に係る指針　ver1.0（案）に対する意見募集　http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000247.html〔参照 2018-05-18〕
※ 49 経済産業省：「IoT 推進コンソーシアム IoT セキュリティワーキンググループ」を開催します　http://www.meti.go.jp/press/2017/12/20171206001/20171206001.html〔参照 2018-05-18〕
※ 50 経済産業省：「カメラ画像利活用ガイドブック ver2.0」を策定しました　http://www.meti.go.jp/press/2017/03/20180330005/20180330005.html〔参照 2018-05-18〕
※ 51 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 52 C^{4}TAP（Ceptoar Councils Capability for Cyber Targeted Attack Protection）：NISC が事務局を務めるセプターカウンシル（重要インフラのセキュリティ向上を目的とした分野横断的な情報共有のための協議会）における情報共有体制。

※ 53 https://www.ipa.go.jp/files/000066063.pdf〔参照 2018-05-18〕
※ 54 「マルウェア」等の用語が使われ、読者を混乱させる可能性があるため、本白書では特に断りのない限り、また文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 55 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート） https://www.ipa.go.jp/security/J-CRAT/index.html〔参照 2018-05-18〕
IPA：J-CRAT ／標的型サイバー攻撃特別相談窓口 https://www.ipa.go.jp/security/tokubetsu/index.html〔参照 2018-05-18〕
※ 56 https://www.ipa.go.jp/files/000065284.pdf〔参照 2018-05-18〕
※ 57 http://www.soumu.go.jp/main_content/000461785.pdf〔参照 2018-05-18〕
※ 58 総務省：「サイバーセキュリティタスクフォース」の開催 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html〔参照 2018-05-18〕
※ 59 http://www.soumu.go.jp/main_content/000478813.pdf〔参照 2018-05-18〕
※ 60 http://www.soumu.go.jp/main_content/000510701.pdf〔参照 2018-05-18〕
※ 61 総務省：「公衆無線 LAN セキュリティ分科会」の開催 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000133.html〔参照 2018-05-18〕
※ 62 http://www.soumu.go.jp/main_content/000539751.pdf〔参照 2018-05-18〕
※ 63 総務省：「情報開示分科会」の開催 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000135.html〔参照 2018-05-18〕
※ 64 http://www.soumu.go.jp/main_content/000547155.pdf〔参照 2018-05-18〕
※ 65 総務省：「サイバー攻撃（標的型攻撃）対策防御モデルの解説」の公表 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html〔参照 2018-05-18〕
※ 66 http://www.soumu.go.jp/main_content/000545372.pdf〔参照 2018-05-18〕
※ 67 総務省：電気通信事業法の一部改正案について http://www.soumu.go.jp/main_content/000536856.pdf〔参照 2018-05-18〕
※ 68 警察庁：サイバー攻撃特別捜査隊の設置について http://www.npa.go.jp/keibi/biki3/20130328kouhou.pdf〔参照 2018-05-18〕
※ 69 産経ニュース：「サイバー攻撃から日本守る」警視庁の新組織「サイバー攻撃対策センター」が発足 http://www.sankei.com/affairs/news/170403/afr1704030019-n1.html〔参照 2018-05-18〕
※ 70 時事ドットコムニュース：サイバー関連部署を集約＝連携強化へ横断チームも－警視庁 https://www.jiji.com/jc/article?k=2018040200318&g=soc〔参照 2018-05-18〕
※ 71 警察庁：平成 18 年版 警察白書 https://www.npa.go.jp/hakusyo/h18/honbun/hakusho/h18/html/i1230000.html〔参照 2018-05-18〕
※ 72 パスワードを初期設定のまま変更していない場合や、仕様としてパスワード変更ができない等、パスワード設定に問題がある IoT 機器は、ウィルス感染や不正な遠隔操作等の被害に遭うおそれがある。
※ 73 @police：ランサムウェア「WannaCry」に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について http://www.npa.go.jp/cyberpolice/detect/pdf/20170519.pdf〔参照 2018-05-18〕
@police：ランサムウェア「WannaCry」の亜種に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について http://www.npa.go.jp/cyberpolice/detect/pdf/20170622.pdf〔参照 2018-05-18〕
※ 74 https://www.npa.go.jp/cybersecurity/〔参照 2018-05-18〕
※ 75 JC3：インターネットバンキングマルウェア「DreamBot」による被害に注意 https://www.jc3.or.jp/topics/dreambot_cm.html〔参照 2018-05-18〕
※ 76 産経ニュース：ワンタイムパス盗む新型ウイルス「ドリームボット」初摘発 ネットバンク不正送金容疑 31 歳男を逮捕 http://www.sankei.com/affairs/news/171005/afr1710050022-n1.html〔参照 2018-05-18〕
※ 77 JPCERT/CC：インターネットバンキングに係わる不正送金の国際的な被害防止対策に協力 https://www.jpcert.or.jp/press/2017/20170323-avalanche.html〔参照 2018-05-18〕
※ 78 SIA：【プレスリリース】 SIA、悪質 EC サイト通報窓口「悪質 EC サイトホットライン」を開設 https://www.saferinternet.or.jp/info/1283/〔参照 2018-05-18〕
※ 79 日本経済新聞：振込先名義人ら 43 人摘発 全国警察、取り締まり強化 https://www.nikkei.com/article/DGXMZO24898590R21C17A2CR0000/〔参照 2018-05-18〕
※ 80 警察庁：平成 29 年上半期におけるコミュニティサイト等に起因する事犯の現状と対策について http://www.npa.go.jp/cyber/statics/h29/H29kami_comunity.pdf〔参照 2018-05-18〕
※ 81 朝日新聞 DIGITAL：座間 9 遺体、1 都 4 県の 15 ～ 26 歳と確認 警視庁発表 http://www.asahi.com/articles/ASKC97RCRKC9UTIL070.html〔参照 2018-05-18〕
※ 82 首相官邸：座間市における事件の再発防止に関する関係閣僚会議 https://www.kantei.go.jp/jp/singi/zamashi_jiken/〔参照 2018-05-18〕
※ 83 日本経済新聞：DeNA などネット事業者 6 社、「青少年ネット利用環境整備協議会」を発足 https://www.nikkei.com/article/DGXLRSP452306_W7A720C1000000/〔参照 2018-05-18〕
※ 84 毎日新聞：IT 協議会 SNS 規約での自殺勧誘禁止提言 https://mainichi.jp/articles/20171207/ddn/041/040/005000c〔参照 2018-05-18〕
※ 85 警察庁：座間市における事件の再発防止策について https://www.kantei.go.jp/jp/singi/zamashi_jiken/dai2/siryou4.pdf〔参照 2018-05-18〕
※ 86 朝日新聞 DIGITAL：青森）弘大生がサイバー防犯ボランティア、県警が委嘱 http://www.asahi.com/articles/ASKCF3Q41KCFUBNB008.html〔参照 2018-05-18〕
※ 87 警察庁：平成 29 年中におけるサイバー空間をめぐる脅威の情勢等についてhttp://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf〔参照 2018-05-18〕
※ 88 朝日新聞 DIGITAL: 身代金ウイルス作成容疑、中 3 を逮捕「力試しに作った」 https://www.asahi.com/articles/ASK653TVZK65ULOB00D.html〔参照 2018-05-18〕
※ 89 産経ニュース：「楽天」「ビックカメラ」の他人のポイント使い商品購入 中国籍の男 3 人を逮捕、グループで犯行か 警視庁 http://www.sankei.com/affairs/news/170919/afr1709190019-n1.html〔参照 2018-05-18〕
※ 90 岐阜県警察：サイバー犯罪の検挙状況 http://www.pref.gifu.lg.jp/police/kurashi-anzen/hanzai-yokushi/cyber-hanzai/kenkyo.html〔参照 2018-05-18〕
教育ネットワーク情報セキュリティ推進委員会：【岐阜県】市立中学校、パスワードを不正入手し、個人情報に不正アクセスされる http://school-security.jp/leak/2017/10/post-1197/〔参照 2018-05-18〕
※ 91 ダークウェブ：Tor ブラウザ等の専用のブラウザを介し、通信のリレー及び暗号化等により、通信元を匿名化する Web システム。Tor 以外に、Invisible Internet Project（I2P）、Freenet、Netsukuku 等、ダークウェブは複数存在している。（参考 Akamai Technologies, Inc.：ダークウェブの現状 2016 https://www.akamai.com/jp/ja/about/our-thinking/threat-advisories/akamai-2016-state-of-the-dark-web.jsp〔参照 2018-05-18〕）
※ 92 警察庁：サイバーセキュリティ重点施策の策定について（通達） https://www.npa.go.jp/pdc/notification/kanbou/soumu/soumu20150925.pdf〔参照 2018-05-18〕
※ 93 日本経済新聞：「ダークウェブ」初の実態調査へ 警察庁 https://www.nikkei.com/article/DGXMZO26246310Y8A120C1000000/〔参照 2018-05-18〕
※ 94 正式名称は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（http://www.cryptrec.go.jp/list/cryptrec-ls-0001-2016.pdf〔参照 2018-05-18〕）。現在は、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の三つのリストから構成される。
※ 95 Karthikeyan Bhargavan, Gaëtan Leurent：Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN https://sweet32.info/〔参照 2018-05-18〕
※ 96 CWI Amsterdam/Google Research：SHATTERED https://shattered.io/〔参照 2018-05-18〕
※ 97 IPA：SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～ https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html〔参照 2018-05-18〕
※ 98 経済産業省：「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の施行期日を定める政令」及び「情報処理の促進に関する法律施行令の一部を改正する政令」が閣議決定されました http://www.meti.go.jp/press/2016/10/20161014001/20161014001.html〔参照 2018-05-18〕
※ 99 NISC：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 ～ サイバーセキュリティ戦略中間レビュー ～ https://www.kantei.go.jp/jp/singi/it2/cio/dai72/siryou1.pdf〔参照 2018-05-18〕
※ 100 https://www.cas.go.jp/jp/houan/180308/siryou1.pdf〔参照 2018-05-18〕
※ 101 経済産業省：「Connected Industries」東京イニシアティブ 2017 を発表しました http://www.meti.go.jp/press/2017/10/20171002012/20171002012.html〔参照 2018-05-18〕
※ 102 知的財産戦略本部：知的財産推進計画 2017 https://www.

kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20170516.pdf〔参照 2018-05-18〕
※ 103 日本経済再生本部：未来投資戦略 2017　https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf〔参照 2018-05-18〕
※ 104 経済産業省：営業秘密の保護・活用に関する小委員会　http://www.meti.go.jp/committee/gizi_1/33.html#eigyohimitsu〔参照 2018-05-18〕
※ 105 経済産業省：第四次産業革命を視野に入れた不正競争防止法に関する検討 中間とりまとめ　http://www.meti.go.jp/report/whitepaper/data/pdf/20170509001_1.pdf〔参照 2018-05-18〕
※ 106 http://www.meti.go.jp/press/2017/02/20180227001/20180227001-3.pdf〔参照 2018-05-18〕
※ 107 外務省：第５回日米サイバー対話の開催　http://www.mofa.go.jp/mofaj/press/release/press3_000318.html〔参照 2018-05-18〕
※ 108 外務省：共同プレスリリース（仮訳）日米サイバー対話 2017年7月２１日　http://www.mofa.go.jp/mofaj/files/000275181.pdf〔参照 2018-05-18〕
※ 109 経済産業省：日本初の「サイバーセキュリティの日米共同演習」を実施しました　http://www.meti.go.jp/press/2017/09/20170927004/20170927004.html〔参照 2018-05-18〕
※ 110 外務省：日米首脳会談　http://www.mofa.go.jp/mofaj/na/na1/us/page4_003937.html
※ 111 外務省：第３回日 EU サイバー対話　http://www.mofa.go.jp/mofaj/erp/ep/page22_002975.html〔参照 2018-05-18〕
※ 112 外務省：2018 年３月５日　第３回日 EU サイバー対話　共同ステートメント http://www.mofa.go.jp/mofaj/files/000344033.pdf
※ 113 独立行政法人日本貿易振興機構：ネットワーク安全法　https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf〔参照 2018-05-18〕
※ 114 産経ニュース：サイバー攻撃対策で連携　日エストニア首脳会談　http://www.sankei.com/photo/story/news/180113/sty1801130002-n1.html〔参照 2018-05-18〕
※ 115 外務省：日英首脳会談　http://www.mofa.go.jp/mofaj/erp/we/gb/page4_003242.html〔参照 2018-05-18〕
※ 116 外務省：第４回日英サイバー協議の開催　http://www.mofa.go.jp/mofaj/press/release/press4_005821.html〔参照 2018-05-18〕
※ 117 個人情報保護委員会：【日本語仮訳】熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント　https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf〔参照 2018-05-18〕
※ 118 外務省：投資の自由化，促進及び保護に関する日本国とイスラエル国との間の協定（略称：日・イスラエル投資協定）　http://www.mofa.go.jp/mofaj/ila/et/page23_001948.html〔参照 2018-05-18〕
※ 119 外務省：第３回日・イスラエル・サイバー協議　http://www.mofa.go.jp/mofaj/me_a/me1/il/page23_002331.html〔参照 2018-05-18〕
※ 120 経済産業省：第 10 回 日・ASEAN 情報セキュリティ政策会議を開催しました　http://www.meti.go.jp/press/2017/10/20171016003/20171016003.html〔参照 2018-05-18〕
※ 121 外務省：サイバーセキュリティに関する ARF 会期間会合のための第１回専門家会合の開催　http://www.mofa.go.jp/mofaj/press/release/press4_005528.html〔参照 2018-05-18〕
※ 122 外務省：サイバーセキュリティに関する ARF 会期間会合のための第１回会期間会合等の開催　http://www.mofa.go.jp/mofaj/press/release/press4_005948.html〔参照 2018-05-18〕
※ 123 外務省：第２回日インド・サイバー協議の開催（共同プレスリリースの発出）　http://www.mofa.go.jp/mofaj/press/release/press4_004917.html〔参照 2018-05-18〕
※ 124 http://www.npr-event.jp/cyber3/〔参照 2018-05-18〕
※ 125 慶應義塾大学：慶應義塾大学の呼びかけによる世界初の国際連携組織「InterNational Cyber Security Center of Excellence (INCS-CoE)」を設立　https://www.keio.ac.jp/ja/press-releases/2016/11/1/28-18699/〔参照 2018-05-18〕
※ 126 INTERPOL：'Internet of Things' cyber risks tackled during INTERPOL Digital Security Challenge　https://www.interpol.int/News-and-media/News/2018/N2018-007〔参照 2018-05-18〕
※ 127 BBC：トランプ米大統領、鉄鋼・アルミ追加関税に署名　https://www.bbc.com/japanese/43340299〔参照 2018-05-18〕
※ 128 日本経済新聞：中国、対米報復関税を発動　128 品目に最大 25%　https://www.nikkei.com/article/DGXMZO28865690S8A400C1MM0000/〔参照 2018-05-18〕
※ 129 BBC：米政府、「過去最大の」北朝鮮制裁を発表　http://www.bbc.com/japanese/43179972〔参照 2018-05-18〕
※ 130 CNN：Trump accepts offer to meet Kim Jong Un　https://edition.cnn.com/2018/03/08/politics/donald-trump-kim-jong-un/index.html〔参照 2018-05-18〕
※ 131 The White House：Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure　https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/〔参照 2018-05-18〕
※ 132 The White House：The American Technology Council Summit to Modernize Government Services　https://www.whitehouse.gov/articles/american-technology-council-summit-modernize-government-services/〔参照 2018-05-18〕
※ 133 IPA：トランプ政権におけるサイバーセキュリティ政策の現状　https://www.ipa.go.jp/files/000061964.pdf〔参照 2018-05-18〕
※ 134 TechTargetジャパン:トランプ氏の「サイバーセキュリティ大統領令」を褒める人、けなす人、それぞれの見方 http://techtarget.itmedia.co.jp/tt/news/1705/26/news17.html〔参照 2018-05-18〕
※ 135 https://twitter.com/realDonaldTrump/status/898567378988015616〔参照 2018-05-18〕
※ 136 Newsweek：米国サイバー軍の格上げはトランプ大統領の心変わりを示すのか　https://www.newsweekjapan.jp/tsuchiya/2017/08/post-23.php〔参照 2018-05-18〕
※ 137 The White House：National Security Strategy of the United States of America　https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf〔参照 2018-05-18〕
※ 138 U.S. Congress：H.R.2810 - National Defense Authorization Act for Fiscal Year 2018　https://www.congress.gov/bill/115th-congress/house-bill/2810/text〔参照 2018-05-18〕
※ 139 The HILL：Trump sends cyber warfare strategy to Congress　http://thehill.com/policy/cybersecurity/384017-trump-sends-cyber-warfare-strategy-to-congress〔参照 2018-05-18〕
※ 140 New York Times：North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says　https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html〔参照 2018-05-18〕
※ 141 IPA：脅威情報構造化記述形式 STIX 概説　https://www.ipa.go.jp/security/vuln/STIX.html〔参照 2018-05-18〕
※ 142 IPA：検知指標情報自動交換手順 TAXII 概説　https://www.ipa.go.jp/security/vuln/TAXII.html〔参照 2018-05-18〕
※ 143 DHS：Information Sharing and Analysis Organizations (ISAOs)　https://www.dhs.gov/isao〔参照 2018-05-18〕
※ 144 Newsweek：ランサムウエア「WannaCry」被害拡大は NSA の責任なのか　https://www.newsweekjapan.jp/stories/technology/2017/05/wannacry-nsams_3.php〔参照 2018-05-18〕
※ 145 Bloomberg：Three Trump Associates Charged in Russia Collusion Probe　https://www.bloomberg.com/news/articles/2017-10-30/trump-s-ex-campaign-chairman-manafort-told-to-surrender-to-u-s〔参照 2018-05-18〕
※ 146 Bloomberg：Mueller Accuses Russians of Pro-Trump, Anti-Clinton Meddling　https://www.bloomberg.com/news/articles/2018-02-16/u-s-charges-13-russians-3-companies-for-hacking-election〔参照 2018-05-18〕
※ 147 The WhiteHouse：Executive Order on the President's Continuation of the National Emergency with Respect to Ukraine　https://www.whitehouse.gov/presidential-actions/executive-order-presidents-continuation-national-emergency-respect-ukraine/〔参照 2018-05-18〕
※ 148 CNN：Trump expelling 60 Russian diplomats in wake of UK nerve agent attack　https://edition.cnn.com/2018/03/26/politics/us-expel-russian-diplomats/index.html〔参照 2018-05-18〕
※ 149 The New York Times：U.N. Security Council Rejects Russian Resolution Condemning Syrian Strikes　https://www.nytimes.com/2018/04/14/world/middleeast/un-security-council-syria-airstrikes.html〔参照 2018-05-18〕
※ 150 The New York Times：Trump Fires Rex Tillerson and Will Replace Him With C.I.A. Chief Pompeo　https://www.nytimes.com/2018/03/13/us/politics/trump-tillerson-pompeo.html〔参照 2018-05-18〕
※ 151 POLITICO：Trump's homeland security adviser resigns, raising questions on Bolton's second day　https://www.politico.com/story/2018/04/10/tom-bossert-to-resign-512252〔参照 2018-05-18〕
※ 152 BBC: Mike Pompeo: CIA chief made secret trip to North Korea　http://www.bbc.com/news/world-asia-43792658〔参照 2018-05-18〕

※ 153 BBC：Koreas summit: Will historic talks lead to lasting peace? http://www.bbc.com/news/world-asia-43932032〔参照 2018-05-18〕
※ 154 NIST：NIST Releases Version 1.1 of its Popular Cybersecurity Framework https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework〔参照 2018-05-18〕
※ 155 NIST：Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final〔参照 2018-05-18〕
※ 156 マイクロターゲティング：個人の嗜好・行動パターン等を詳細に分析し、より効果的なコミュニケーション戦略を立案する手法であり、マーケティングや選挙対策などに応用される。
※ 157 POLITICO：Trump campaign's digital director agrees to meet with House Intel Committee https://www.politico.com/story/2017/07/14/brad-parscale-trump-digital-house-intel-committee-240557〔参照 2018-05-18〕
※ 158 The Guardian: 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump〔参照 2018-05-18〕
※ 159 日本経済新聞：フェイスブック、情報流用 8700 万人規模に拡大 https://www.nikkei.com/article/DGXMZO29021990V00C18A4000000/〔参照 2018-05-18〕
※ 160 Bloomberg：Facebook Problems 'My Mistake,' Zuckerberg to Tell Congress https://www.bloomberg.com/news/articles/2018-04-09/zuckerberg-to-say-in-testimony-facebook-problems-are-his-mistake〔参照 2018-05-18〕
※ 161 GEISTWERT：Pan-European Status of the NIS Directive https://www.linkedin.com/pulse/pan-european-status-nis-directive-rainer-schultes/〔参照 2018-05-18〕
※ 162 ANSSI：ANSSI WELCOMES AN IMPORTANT STEP TOWARD THE TRANSPOSITION OF THE NIS DIRECTIVE IN FRANCE https://www.ssi.gouv.fr/en/actualite/anssi-welcomes-an-important-step-toward-the-transposition-of-the-nis-directive-in-france/〔参照 2018-05-18〕
※ 163 LEXOLOGY：France's approach to implementing GDPR and NISD https://www.lexology.com/library/detail.aspx?g=5cada209-1f6e-4c38-8ade-8557365a4e0e〔参照 2018-05-18〕
※ 164 GOV.UK：Consultation on the Security of Network and Information Systems Directive https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive〔参照 2018-05-18〕
※ 165 legislation.gov.uk：The Network and Information Systems Regulations 2018 https://www.legislation.gov.uk/uksi/2018/506/made〔参照 2018-05-18〕
※ 166 European Commission：Cybersecurity Package https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en〔参照 2018-05-18〕
※ 167 European Commission：Digital Single Market Mid-term Review: Commission calls for swift adoption of key proposals and maps out challenges ahead https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review〔参照 2018-05-18〕
※ 168 tom's Hardware：European Commission Proposes Cybersecurity Certification Framework For Digital Products, Services https://www.tomshardware.com/news/european-commission-security-certification-framework,35457.html〔参照 2018-05-18〕
※ 169 IoT 推進コンソーシアム：海外の IoT 機器の動向 http://www.iotac.jp/wp-content/uploads/2016/01/%E8%B3%87%E6%96%99%EF%BC%94_%E6%B5%B7%E5%A4%96%E3%81%AEIoT%E6%A9%9F%E5%99%A8%E3%81%AE%E5%8B%95%E5%90%91%EF%BC%88%E4%BA%8B%E5%8B%99%E5%B1%80%E8%AA%AC%E6%98%8E%E8%B3%87%E6%96%99%EF%BC%89.pdf〔参照 2018-05-18〕
※ 170 DIGITALEUROPE：DIGITALEUROPE's position paper on the European Commission's proposal for a European framework for cybersecurity certification scheme for ICT products and services http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2587&language=en-US&PortalId=0&TabId=353〔参照 2018-05-18〕
※ 171 EUR-Lex：EUR-Lex - 32016R0679 - EN http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679〔参照 2018-05-18〕
※ 172 European Commission：Guidelines http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360〔参照 2018-05-18〕独立行政法人日本貿易振興機構より WP243 の和訳解説（独立行政法人日本貿易振興機構：「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編） https://www.jetro.go.jp/ext_images/_Reports/01/28dd771ad2a2c020/20170094.pdf〔参照 2018-05-18〕）が公表されている。
※ 173 個人情報保護委員会が日本語仮訳版を掲載している（個人情報保護委員会：EC's Infographic 仮訳 https://www.ppc.go.jp/files/pdf/EC-Infographic.pdf〔参照 2018-05-18〕）。
※ 174 European Banking Federation：Data breach notification under GDPR-WP250:EBF comments on the Article 29 Working Party guidelines https://www.ebf.eu/retail-payments/ebf-comments-on-the-art-29-wp-guidelines-on-data-breach-notification-under-gdpr-wp250〔参照 2018-05-18〕
※ 175 European Banking Federation：Automated individual decision-making and profiling-WP251:EBF comments on the Article 29 Working Party guidelines https://www.ebf.eu/retail-payments/automated-individual-decision-making-and-profiling-wp251-ebf-comments-on-the-article-29-working-party-guidelines/〔参照 2018-05-18〕
※ 176 eDisclosure Information Project：GDPR: WP 253 guidelines on the application and setting of fines https://chrisdale.wordpress.com/2018/02/27/gdpr-wp-253-guidelines-on-the-application-and-setting-of-fines/〔参照 2018-05-18〕
※ 177 Drinker Biddle & Reath LLP：Article 29 Working Party Releases Guideline WP259 on Consent under the GDPR http://dbrondata.com/2018/article-29-working-party-releases-guideline-wp259-consent-gdpr/〔参照 2018-05-18〕
※ 178 独立行政法人日本貿易振興機構：EU 加盟各国で整備が進む個人データ保護法 https://www.jetro.go.jp/ext_images/biz/areareports/2018/pdf/bef14bc82cad6929_1.pdf〔参照 2018-05-18〕
※ 179 杉本武重：加盟国法を踏まえたデータ保護コンプライアンスを（ジェトロセンサー 2017 年 10 月号） https://www.jetro.go.jp/ext_images/biz/special/2017/37d786f4de44651c/11.pdf〔参照 2018-05-18〕
※ 180 TaylorWessing：France's approach to implementing GDPR and NISD https://united-kingdom.taylorwessing.com/globaldatahub/article-france-gdpr-implementation.html〔参照 2018-05-18〕
※ 181 PASSWORD PROTECTED：France: Pragmatism and Flexibility for the GDPR Implementation https://www.passwordprotectedlaw.com/2018/02/france-pragmatism-and-flexibility-for-the-gdpr-implementation/〔参照 2018-05-18〕
※ 182 GOV.UK：Data Protection Bill: General Processing https://www.gov.uk/government/publications/data-protection-bill-general-processing〔参照 2018-05-18〕
※ 183 GOV.UK：Data Protection Act 2018 https://www.gov.uk/government/collections/data-protection-act-2018〔参照 2018-06-05〕
※ 184 The Guardian：Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election〔参照 2018-05-18〕
※ 185 China Briefing：Are You Ready for GDPR Day on May 25? http://www.china-briefing.com/news/2018/05/01/ready-gdpr-day-may-24.html〔参照 2018-05-18〕
※ 186 全国人民代表大会：中華人民共和国網絡安全法 http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm〔参照 2018-05-18〕
※ 187 THE WALL STREET JOURNAL: 中国のサイバーセキュリティー法、米企業は依然困惑 http://jp.wsj.com/articles/SB12781603698933324048504583559493204728244〔参照 2018-05-18〕
※ 188 REUTERS：焦点：米アップルの iCloud データ、中国移行に懸念の声 https://jp.reuters.com/article/china-apple-icloud-idJPKCN1GE0UZ〔参照 2018-05-18〕
※ 189 The New York Times：Apple Fights Order to Unlock San Bernardino Gunman's iPhone https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html〔参照 2018-05-18〕
※ 190 人民網：「インターネットニュース情報サービス管理規定」公布 http://j.people.com.cn/n3/2017/0503/c94475-9210599.html〔参照 2018-05-18〕
※ 191 朝日新聞：ネット規制強化は経済と社会の安定に必要＝中国の習国家主席 http://www.asahi.com/international/reuters/CRWKBN1HU01D.html〔参照 2018-05-18〕

※ 192 World Internet Conference：http://www.wuzhenwic.org/〔参照 2018-05-18〕
人民網：第 4 回世界インターネット大会が閉幕　http://j.people.com.cn/n3/2017/1206/c95952-9301170.html〔参照 2018-05-18〕
※ 193 朝日新聞：習主席「ネット、自由よりも統制を」　国際統治へ積極的　https://www.asahi.com/articles/ASL4Q5G7GL4QUHBI00Q.html〔参照 2018-05-18〕
※ 194 外務省：第四回日中ハイレベル経済対話　http://www.mofa.go.jp/mofaj/a_o/c_m2/ch/page3_002437.html〔参照 2018-05-18〕
※ 195 経済産業省：世耕経済産業大臣が鍾山中華人民共和国商務部部長及び張勇中華人民共和国国家発展改革委員会副主任（閣僚級）と会談を行いました　http://www.meti.go.jp/press/2018/04/20180416002/20180416002.html〔参照 2018-05-18〕
※ 196 外務省：第 7 回日中韓サミット　http://www.mofa.go.jp/mofaj/a_o/rp/page3_002460.html〔参照 2018-05-18〕
※ 197 https://www.cert.govt.nz/〔参照 2018-05-18〕
※ 198 Ministry of Business, Innovation and Employment：New national cyber security unit launched　http://www.mbie.govt.nz/about/whats-happening/news/2017/new-national-cyber-security-unit-launched〔参照 2018-05-18〕
※ 199 Department of the Prime Minister and Cabinet：New Zealand's Cyber Security Strategy　https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy〔参照 2018-05-18〕
※ 200 https://www.ncsc.govt.nz/〔参照 2018-05-18〕
※ 201 https://www.first.org/〔参照 2018-05-18〕
※ 202 Department of the Prime Minister and Cabinet：Australia's Cyber Security Strategy　https://cybersecuritystrategy.pmc.gov.au/〔参照 2018-05-18〕
※ 203 https://www.cert.gov.au/〔参照 2018-05-18〕
※ 204 https://www.apcert.org/〔参照 2018-05-18〕
※ 205 Ministry of Communication and Information Technology：Samoa National Cyber Security Strategy 2016-2021　http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf〔参照 2018-05-18〕
※ 206 https://www.etda.or.th/content/tb-cert-for-thailand-banking-sector.html〔参照 2018-05-18〕
※ 207 APCERT:Documents　https://www.apcert.org/documents/〔参照 2018-05-18〕
※ 208 APCERT：APCERT CYBER DRILL ON NEW DDOS THREAT　http://www.apcert.org/documents/pdf/APCERTDrill2017PressRelease.pdf〔参照 2018-05-18〕
※ 209 https://www.oic-cert.org/en/〔参照 2018-05-18〕
※ 210 http://cert-in.org.in/〔参照 2018-05-18〕
※ 211 APCERT：TSUBAME Working Group　https://www.apcert.org/about/structure/tsubame-wg/index.html〔参照 2018-05-18〕
※ 212 https://www.aspi.org.au/〔参照 2018-05-18〕
※ 213 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017〔参照 2018-05-18〕
※ 214 NISC：サイバーセキュリティ人材育成における施策間連携について　http://www.nisc.go.jp/conference/cs/jinzai/wg2/dai02/pdf/02shiryou0101.pdf〔参照 2018-05-18〕
※ 215 http://www.enpit.jp/〔参照 2018-05-18〕
※ 216 内閣府：戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保　研究開発計画　http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku/11_cyber.pdf〔参照 2018-05-18〕
※ 217 NISC：本 WG の主な検討事項　http://www.nisc.go.jp/conference/cs/jinzai/wg2/dai03/pdf/03shiryou02.pdf〔参照 2018-05-18〕
※ 218 NISC：サイバーセキュリティ人材育成の検討の方向性（案）　http://www.nisc.go.jp/conference/cs/jinzai/wg2/dai02/pdf/02shiryou0102.pdf〔参照 2018-05-18〕
※ 219 https://www.ipa.go.jp/files/000062153.pdf〔参照 2018-05-18〕
※ 220 IPA：情報処理技術者試験統計資料 平成 29 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_h29.pdf〔参照 2018-05-18〕
※ 221 IPA：プレス発表　平成 29 年度春期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表　https://www.ipa.go.jp/about/press/20170517.html〔参照 2018-05-18〕
IPA：プレス発表　平成 29 年度秋期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表　https://www.ipa.go.jp/about/press/20171115.html〔参照 2018-05-18〕
※ 222 https://www.ipa.go.jp/siensi/whatsriss/index.html〔参照 2018-05-18〕
※ 223 名称独占資格：業務独占資格と異なり、資格がなくても業務に携わることはできるが、資格がなければその名称を名乗ることはできない資格のこと。
※ 224 IPA：プレス発表　4 月 1 日付け「情報処理安全確保支援士（登録セキスペ）」は 2,206 名、登録人数は 9,181 名に https://www.ipa.go.jp/about/press/20180402_2.html〔参照 2018-05-18〕
※ 225 IPA：国家資格「情報処理安全確保支援士」情報処理安全確保支援士（登録セキスペ）の受講する講習について　https://www.ipa.go.jp/siensi/lecture/index.html〔参照 2018-05-18〕
IPA：国家資格「情報処理安全確保支援士」受講者の声　https://www.ipa.go.jp/siensi/lecture/voice.html〔参照 2018-05-18〕
※ 226 http://www.soumu.go.jp/main_content/000348295.pdf〔参照 2018-05-18〕
※ 227 IPA：プレス発表　「セキュリティ・キャンプ全国大会 2017」参加者を決定　https://www.ipa.go.jp/about/press/20170615.html〔参照 2018-05-18〕
※ 228 ハッカソン（hackathon）：ハック（hack）とマラソン（marathon）を組み合わせた造語。ソフトウェアエンジニア等が一定期間集中的にソフトウェア開発に取り組み、技能や成果を競うイベント。
※ 229 IPA：セキュリティ・キャンプ全国大会 2017　講義内容　https://www.ipa.go.jp/jinzai/camp/2017/zenkoku2017_kougi.html〔参照 2018-05-18〕
※ 230 一般社団法人セキュリティ・キャンプ協議会：地方大会　実施状況　http://www.security-camp.org/minicamp/index.html〔参照 2018-05-18〕
※ 231 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・ジュニアキャンプ in 高知 2017　http://www.security-camp.org/event/kochi2017.html〔参照 2018-05-18〕
※ 232 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・コアキャンプ 2017　http://www.security-camp.org/event/corecamp2017.html〔参照 2018-05-18〕
※ 233 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・キャンプアワード開催報告　http://www.security-camp.org/event/awardreport.html〔参照 2018-05-18〕
※ 234 enPiT：2017 年度 成果報告書　http://www.enpit.jp/img_new/publications/annual-report2017.pdf〔参照 2018-05-18〕
※ 235 文部科学省：平成 29 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」の公募（enPiT-Pro の公募）について　http://www.mext.go.jp/a_menu/koutou/kaikaku/enpit/1383644.htm〔参照 2018-05-18〕
※ 236 文部科学省：平成 29 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」enPiT-Pro の選定状況について　http://www.mext.go.jp/a_menu/koutou/kaikaku/enpit/1395904.htm〔参照 2018-05-18〕
enPiT-Pro Security：概要　http://www.seccap.pro/〔参照 2018-05-18〕
※ 237 CTF（Capture The Flag）：互いに相手陣地にある旗を奪い合う野外ゲームを情報セキュリティに適用したもので、例えば自分のホストを守りながら、相手チームのホストを攻撃する競技等がある。
※ 238 https://2017.seccon.jp/〔参照 2018-05-18〕
※ 239 Net IB News：SECCON2017 決勝大会～ 102 カ国、4,347 名の頂点　http://www.data-max.co.jp/300222_knk1/〔参照 2018-05-18〕
Security NEXT:SECCON 決勝戦が終幕 - 韓国チームが連覇、日本チームは 3 位と健闘　http://www.security-next.com/090357〔参照 2018-05-18〕
※ 240 NICT：「NIRVANA 改 SECCON カスタム Mk-IV」でサイバー模擬攻防戦を視覚化!　https://www.nict.go.jp/info/topics/2018/02/180215-1.html〔参照 2018-05-18〕
※ 241 SECCON2017：SECCON Beginners　https://2017.seccon.jp/about/beginners.html〔参照 2018-05-18〕
SECCON2017：CTF for GIRLS（女性限定）　https://2017.seccon.jp/about/girls.html〔参照 2018-05-18〕
SECCON2017：連携大会・その他関連大会　https://2017.seccon.jp/about/cooperation-event.html〔参照 2018-05-18〕
※ 242 JNSA 産学情報セキュリティ人材育成交流会:JNSA インターンシップ　http://www.jnsa.org/internship/2017/〔参照 2018-05-18〕
※ 243 connpass：JNSA 主催セミナー：これからの IT 人材のキャリアを考える～サイバーセキュリティの視点から～　https://connpass.com/event/69456/〔参照 2018-05-18〕
※ 244 http://cyber-risk.or.jp/index.html〔参照 2018-05-18〕
※ 245 産業横断サイバーセキュリティ人材育成検討会：A1. 産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～　http://cyber-risk.or.jp/sansanren/xs_20160914_A1_Report_JinzaiTeigiReference_1.0.pdf〔参照 2018-05-18〕

産業横断サイバーセキュリティ人材育成検討会：A2. 産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～（要求知識）http://cyber-risk.or.jp/sansanren/xs_20160914_A2_Report_JinzaiTeigiReference_1.0.pdf〔参照 2018-05-18〕
産業横断サイバーセキュリティ人材育成検討会：A3. 産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～（業務区分）http://cyber-risk.or.jp/sansanren/xs_20160914_A3_Report_JinzaiTeigiReference_1.0.pdf〔参照 2018-05-18〕
※ 246 産業横断サイバーセキュリティ人材育成検討会：第二期中間報告書 http://cyber-risk.or.jp/cric-csf/report/CRIC-CSF-2nd-Interim-Report.pdf〔参照 2018-05-18〕
※ 247 経済産業省／ IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔参照 2018-05-18〕
※ 248 IPA：CISO 等セキュリティ推進者の経営・事業に関する役割調査 https://www.ipa.go.jp/files/000065213.pdf〔参照 2018-05-18〕
※ 249 IPA:IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書 https://www.ipa.go.jp/files/000065162.pdf〔参照 2018-05-18〕
※ 250 https://www.iso.org/the-iso-survey.html〔参照 2018-05-18〕
※ 251 情報マネジメントシステム認定センター：ISMS クラウドセキュリティ認証取得組織一覧 https://isms.jp/isms-cls/lst/ind/index.html〔参照 2018-05-18〕
※ 252 https://www.jisa.or.jp/it_info/engineering/tabid/1157/Default.aspx〔参照 2018-05-18〕
※ 253 JIPDEC：プライバシーマーク制度 https://privacymark.jp/index.html〔参照 2018-05-18〕
※ 254 JIPDEC：平成 28 年度我が国におけるデータ駆動型社会に係る基盤整備（JIS 改訂等調査研究）調査研究報告書 http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/jis-houkokusho2017.pdf〔参照 2018-05-18〕
※ 255 フォーラム標準の定義については、「JIS Z 8002:2006」の「JA.1」の「100.5」を参照。
※ 256 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔参照 2018-05-28〕
※ 257 日本工業標準調査会：JISC について http://www.jisc.go.jp/jisc/index.html〔参照 2018-05-28〕
※ 258 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔参照 2018-05-28〕
※ 259 IETF：The IETF Security Area https://trac.ietf.org/trac/sec/wiki〔参照 2018-05-28〕
※ 260 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔参照 2018-05-28〕
※ 261 NIST の「Computer Security Division Annual Report 2015」（http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-182.pdf〔参照 2018-05-28〕）を参考に IPA が作成した。
※ 262 規格化前検討：Study Period（SP）。標準化作業を開始する前の事前検討のこと。
※ 263 SIMON/SPECK：2013 年 6 月、NSA が発表した軽量暗号。暗号に使用する回路の数が従来の 6 割程しか必要とされない軽量設計であるため、RFID のような小型デバイスの利用に適しているとされる。SIMON がハードウェア側、SPECK がソフトウェア側での利用を想定している。
※ 264 格子暗号：格子の最短ベクトル問題等を安全性の根拠とする公開鍵暗号方式。格子暗号を用いると、データを暗号化したままの状態で、検索や数値演算が可能となる。
※ 265 ISO/IEC15408 に基づく評価は CC（Common Criteria）評価とも呼ばれる。
※ 266 国立研究開発法人新エネルギー・産業技術総合開発機構による、複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発プロジェクトを指す。
※ 267 http://www.meti.go.jp/press/2014/10/20141017002/20141017002a.pdf〔参照 2018-05-28〕
※ 268 ISO：ISO/TC 307 https://www.iso.org/committee/6266604.html〔参照 2018-05-28〕
※ 269 一般社団法人情報処理学会：IoT の本格普及に向け国際標準化機関が規格開発を本格始動 http://www.ipsj.or.jp/release/itscj_release20161214.html〔参照 2018-05-28〕
※ 270 http://isa99.isa.org/ISA99%20Wiki/Home.aspx〔参照 2018-05-28〕
※ 271 IEC:TC 65 Scope http://www.iec.ch/dyn/www/f?p=103:7:16010101219185::::FSP_ORG_ID,FSP_LANG_ID:1250,25〔参照 2018-05-28〕
※ 272 ISA99 Committee：Work Product List http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx〔参照 2018-05-28〕
※ IEC 62443 は、ISA 62443（ISA99）を国際標準化したもの。
※ 273 SCADA（Supervisory Control and Data Acquisition）：主に、地理的に分散した制御対象を広域ネットワーク経由で遠隔集中監視するシステムを示す。制御機器を汎用パソコン上等で監視するためのソフトウェアを示す場合もある。
※ 274 以下を参照した。
IEC：TC 65 Stability date of publication http://www.iec.ch/dyn/www/f?p=103:21:3415922756895::::FSP_ORG_ID,FSP_LANG_ID:1250,25〔参照 2018-05-28〕
IEC：TC 65 Project files http://www.iec.ch/dyn/www/f?p=103:20:0::::FSP_ORG_ID,FSP_LANG_ID:1250,25〔参照 2018-05-28〕
※ 275 ISA99 Committee の「Work Product List」においては「Under Development」となっているが、「ISA-TR62443-1-2」（http://isa99.isa.org/ISA99%20Wiki/WP-1-2.aspx〔参照 2018-05-28〕）においては「Draft for Comment」となっており、「Public Documents」ページに掲載された http://isa99.isa.org/Public/Series/Documents/ISA-62443-1-2-Public.pdf〔参照 2018-02-27〕においても「Draft1、Edit6」となっていた。
※ 276 ISA99 Committee の「Work Product List」において更新されていない。
※ 277 ISO/IEC 27000 シリーズ：ISMS に関する国際標準。
※ 278 タイトル名が「Security program requirement for IACS service providers」に変更された。
※ 279 2016 年 12 月に公開された ISA99 Committee の「The 62443 series of standards」（http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf〔参照 2018-05-28〕）によると、ISA/IEC TR 62443-3-1 は Ed.2 が 2007 年に発行され、現在 Ed.3 を改版中と記されているが、ISA99 Committee の「Work Product List」に掲載されているドラフトは Ed.2（Revision 2）となっている。
※ 280 ISA Security Compliance Institute：ISA のメンバーのコンソーシアムにより創設された EDSA 認証の制度運営元。
※ 281 Embeded Device Security Assurance：制御機器（組み込み機器）のセキュリティ保証に関する認証制度。
※ 282 https://trustedcomputinggroup.org/〔参照 2018-05-28〕
※ 283 TCG：TPM Library Specification https://trustedcomputinggroup.org/tpm-library-specification/〔参照 2018-05-28〕
※ 284 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/〔参照 2018-05-28〕
※ 285 TCG：TCG 日本支部テクニカルセミナー https://trustedcomputinggroup.org/work-groups/regional-forums/japan/techseminar/〔参照 2018-05-28〕
※ 286 TCG：TCG 日本支部・公開ワークショップ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/jrfworkshop/〔参照 2018-05-28〕
※ 287 TCG：Embedded Systems https://trustedcomputinggroup.org/work-groups/embedded-systems/〔参照 2018-05-28〕
※ 288 TCG：TCG TPM 2.0 Library Profile for Automotive-Thin https://trustedcomputinggroup.org/tcg-tpm-2-0-library-profile-automotive-thin/〔参照 2018-05-28〕
※ 289 Micorsoft Research：RIoT – A Foundation for Trust in the Internet of Things https://www.microsoft.com/en-us/research/publication/riot-a-foundation-for-trust-in-the-internet-of-things/〔参照 2018-05-28〕
※ 290 TCG：Device Identifier Composition Engine (DICE) Architectures https://trustedcomputinggroup.org/work-groups/dice-architectures/〔参照 2018-05-28〕
※ 291 TCG：TCG Software Stack (TSS) Specification https://trustedcomputinggroup.org/tcg-software-stack-tss-specification/〔参照 2018-05-28〕
※ 292 TCG：Trusted Platform Architecture Hardware Requirements for a Device Identifier Composition Engine https://trustedcomputinggroup.org/resource/hardware-requirements-for-a-device-identifier-composition-engine/〔参照 2018-05-28〕
※ 293 TCG：Industrial https://trustedcomputinggroup.org/work-groups/industrial/〔参照 2018-05-28〕
※ 294 TCG：Storage https://trustedcomputinggroup.org/work-groups/storage/〔参照 2018-05-28〕
※ 295 TCG：Storage Work Group Storage Security Subsystem Class: Opal https://trustedcomputinggroup.org/storage-work-group-storage-security-subsystem-class-opal/〔参照 2018-05-28〕
※ 296 府省庁における情報セキュリティ対策の基準を示したもの。
http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf〔参照 2018-

05-28〕
※ 297 https://www.ipa.go.jp/security/jisec/index.html〔参照 2018-05-28〕
※ 298 2018 年 4 月現在、CCRA 加盟国は日本、米国、英国、イタリア、インド、オーストラリア、オランダ、カナダ、韓国、スウェーデン、スペイン、ドイツ、トルコ、ニュージーランド、ノルウェー、フランス、マレーシア（以上の国は認証制度を自国で運営）、イスラエル、エチオピア、オーストリア、カタール、ギリシャ、シンガポール、チェコ、デンマーク、パキスタン、ハンガリー、フィンランド（以上の国は自国に現時点で認証制度を持たないが参加国の発行した認証を認める）の 28 ヵ国。
※ 299 政府調達において特に情報セキュリティの確保を求める製品分野を示したもの。 http://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔参照 2018-05-28〕
※ 300 EAL（Evaluation Assurance Level）：評価の確からしさのレベルを示したもの。高い保証レベル程、評価する証拠資料が広範囲かつ深くなるが、コストも増大する。
※ 301 https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html〔参照 2018-05-28〕
※ 302 耐タンパ性：モジュールがあらかじめ準備したインタフェース以外のアクセス手段を用いて、許可なくモジュールの内部情報を読み取ろうとする攻撃に対する耐性。
※ 303 IPA：認証製品リスト（ハードウェア） https://www.ipa.go.jp/security/jisec/hardware/hw_cert_list.html〔参照 2018-05-28〕
※ 304 Bundesamt für Sicherheit in der Informationstechnik：BSI-CC-PP-0035-2007 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0035.html〔参照 2018-05-28〕
※ 305 Bundesamt für Sicherheit in der Informationstechnik：BSI-CC-PP-0084-2014 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0084.html〔参照 2018-05-28〕
※ 306 物理攻撃：リバースエンジニアリングでチップの構造を解析し、配線にプロービングして信号として流れる秘密情報を抽出したり、配線の切断や接続で回路の振る舞いを変更する攻撃。
※ 307 サイドチャネル攻撃：動作中の IC チップから生じる消費電力、電磁波等の変動を測定し、IC チップ内部の処理を推定する攻撃。最終的には暗号鍵の抽出に至る。
※ 308 故障利用攻撃：動作中の IC チップの電源やクロックに対して物理的な操作を行い、一過性の故障を意図的に発生させることで暗号鍵等の秘密情報の漏えいを誘発する攻撃。
※ 309 浅井稔也、吉川雅弥：イベントモデルシミュレーションによるサイドチャネル情報取得の効率化 http://www.jst.go.jp/crest/dvlsi/list/SCIS2013/pdf/SCIS2013_1E1-1.pdf〔参照 2018-05-28〕
※ 310 IPA：CC サポート文書 https://www.ipa.go.jp/security/jisec/hardware/cc_supporting_doc.html〔参照 2018-05-28〕
※ 311 テストビークル：評価者のハードウェアセキュリティ評価能力を確認するための評価対象となるスマートカード。
※ 312 IPA/JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.3 版 https://www.ipa.go.jp/security/jisec/application/documents/guidelineforHCD-PP_1.3.pdf〔参照 2018-06-06〕
※ 313 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔参照 2018-05-28〕
※ 314 IPA/JISEC：MX-6050N / 6050V / 5050N / 5050V / 4050N / 4050V / 3550N / 3550V / 3050N / 3050V / 2630N with MX-FR51U and MX-PK13 0700Kc00 https://www.ipa.go.jp/security/jisec/certified_products/c0579/c0579_it7639.html〔参照 2018-05-28〕
シャープ株式会社：業界初当社製デジタルフルカラー複合機が「ハードコピーデバイス プロテクションプロファイル v1.0」適合 Common Criteria 認証を取得 http://www.sharp.co.jp/corporate/news/171114-a.html〔参照 2018-05-28〕
※ 315 NIST：NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions (Revised) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf〔参照 2018-05-28〕
※ 316 NIST：NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Applications http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf〔参照 2018-05-28〕
※ 317 NIST：NIST Special Publication 800-135 Revision 1 Recommendation for Existing Application-Specific Key Derivation Functions http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf〔参照 2018-05-28〕
※ 318 NIST：NIST Special Publication 800-56B Revision 1 Recommendation for Pair-Wise KeyEstablishment Schemes Using Integer Factorization Cryptography http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf〔参照 2018-05-28〕
※ 319 ISO：ISO/IEC 18367:2016 https://www.iso.org/standard/62286.html〔参照 2018-05-28〕
※ 320 ICAO：Doc 9303, Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf〔参照 2018-05-28〕
※ 321 IPA/JISEC：旅券冊子用 IC のためのプロテクションプロファイル ー SAC 対応（PACE）及び能動認証対応 ー 第 1.00 版 https://www.ipa.go.jp/security/jisec/certified_pps/c0499/c0499_it5574.html〔参照 2018-05-28〕
※ 322 内閣府特命担当大臣決定：平成 29 年度「青少年の非行・被害防止全国強調月間」実施要綱 http://www8.cao.go.jp/youth/kankyou/hikouhigai/pdf/h29/gekkan_youkou.pdf〔参照 2018-05-28〕
※ 323 http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/27/1386963_1_1.pdf〔参照 2018-05-28〕
※ 324 警察庁：STOP! 自画撮り！ https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/2017_selfy_2.pdf〔参照 2018-05-28〕
※ 325 警察庁：平成 29 年における子供の性被害の状況 https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/2017_statistics_data.pdf〔参照 2018-05-28〕
※ 326 東京都：「自画撮り被害」防止に向けた改正条例について自治体の事務担当者へ情報提供しました! http://www.metro.tokyo.jp/tosei/hodohappyo/press/2017/12/22/002.html〔参照 2018-05-28〕
※ 327 兵庫県警察：インターネットのお約束 あひルのおやコ http://www.police.pref.hyogo.lg.jp/cyber/secur/data/ahiru_leaf.pdf〔参照 2018-05-28〕
※ 328 http://www8.cao.go.jp/youth/youth-harm/chousa/net-jittai_child.html〔参照 2018-05-28〕
※ 329 http://www8.cao.go.jp/youth/youth-harm/chousa/h28/net-jittai_child/pdf/gaiyo.pdf〔参照 2018-05-28〕
※ 330 総務省：「あんしんネット 冬休み・新学期一斉緊急行動」の取組 http://www.soumu.go.jp/menu_news/s-news/01kiban08_03000257.html〔参照 2018-05-28〕
※ 331 NISC：2018 年「サイバーセキュリティ月間」キックオフサミットの開催について https://www.nisc.go.jp/security-site/files/kickoff_180201.pdf〔参照 2018-05-28〕
※ 332 https://www.nisc.go.jp/security-site/month/beatless.html〔参照 2018-05-28〕
※ 333 佐賀県：平成 29 年度 佐賀県 情報セキュリティ・モラルシンポジウム https://www.pref.saga.lg.jp/kiji00359895/3_59895_82833_up_6pya3c0r.pdf〔参照 2018-05-28〕
※ 334 http://www.ppc.go.jp/files/pdf/1711_simple_lesson.pdf〔参照 2018-05-28〕
※ 335 東京都：都内中小企業向け標的型メール攻撃訓練について http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/mailtraining/〔参照 2018-05-28〕
※ 336 http://isog-j.org/output/2017/Textbook_soc-csirt_v2.0.pdf〔参照 2018-05-28〕
※ 337 トレンドマイクロ株式会社：資料ダウンロード https://www.is702.jp/download/partner/200_k/〔参照 2018-05-28〕
※ 338 JNSA：JNSA 全国横断セキュリティセミナー 2017（一般企業向け）福岡・名古屋・大阪・仙台・東京 http://www.jnsa.org/seminar/2017/cross02/〔参照 2018-05-28〕
※ 339 安心ネットづくり促進協議会：考えよう！ 子育てと子供の成長とデジタル機器 https://www.good-net.jp/files/original/20171101222036400710 3.pdf〔参照 2018-05-28〕
※ 340 フィッシング対策協議会：フィッシング対策協議会 STC 普及啓発 WG:STOP THINK CONNECT 啓発イベント https://peatix.com/event/332976/〔参照 2018-05-28〕
※ 341 LINE 株式会社：長野県と LINE 株式会社による LINE を活用したいじめ等相談の中間報告資料 https://scdn.line-apps.com/stf/linecorp/ja/pr/NaganoPrefectureReportMaterial.pdf〔参照 2018-05-28〕
※ 342 Twitter, Inc.:ヘイト行為や攻撃的な行為を減らすための新しいルールの施行 https://blog.twitter.com/official/ja_jp/topics/company/2017/1210policy.html〔参照 2018-05-28〕
※ 343 https://www.j-credit.or.jp/croket-movie/〔参照 2018-05-28〕
※ 344 官民ボード：警察庁、総務省及び経済産業省が設置した、不正アクセス防止に関する現状の課題や改善方策について意見を集約するための委員会。構成員として政府機関のほか、関連する民間企業、団体、研究機関等が参加。
※ 345 https://www.ipa.go.jp/security/kokokara/〔参照 2018-05-28〕
※ 346 https://www.ipa.go.jp/security/event/hyogo/index.html〔参

照 2018-05-28〕
※ 347 https://www.ipa.go.jp/files/000062903.pdf〔参照 2018-05-28〕
※ 348 http://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000170358〔参照 2018-05-28〕
※ 349 USC Annenberg School for Communication and Journalism、COMMON SENSE MEDIA：THE NEW NORMAL：PARENTS, TEENS, AND DIGITAL DEVICES IN JAPAN http://assets.uscannenberg.org/docs/CS_DigitalDevicesJapan_v8_press.pdf〔参照 2018-05-28〕
※ 350 http://www.jnsa.org/result/2018/surv_mrk/data/2017_mrk-report_sokuhou.pdf〔参照 2018-05-28〕
※ 351 「営業秘密」とは、不正競争防止法上で定義される「秘密として管理されている生産方法、販売方法その他事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」で、秘密管理性、有用性、非公知性の 3 要件をすべて満たすものである。
※ 352 IPA：「企業における営業秘密管理に関する実態調査」報告書について https://www.ipa.go.jp/security/fy28/reports/ts_kanri/〔参照 2018-05-28〕
※ 353 経済産業省：営業秘密管理指針 http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf〔参照 2018-05-28〕
※ 354 ここでは、営業秘密として法的保護を受けられる定義を越え、外部に漏えいすると損害が生じるような様々な営業情報・技術情報等の重要情報を包含して秘密情報と呼ぶ。
※ 355 経済産業省：秘密情報の保護ハンドブック http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〔参照 2018-05-28〕
※ 356 IPA：「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」報告書について https://www.ipa.go.jp/security/fy29/reports/ts_research/20180322.html〔参照 2018-05-28〕
※ 357 経済産業省：平成 29 年度 新・ダイバーシティ経営企業 100 選 / 100 選プライム http://www.meti.go.jp/policy/economy/jinzai/diversity/kigyo100sen/〔参照 2018-05-28〕
※ 358 シンクライアント PC：使用するクライアント端末には必要最小限の処理をさせ、ほとんどの処理をサーバ側に集中させる仕組みのパソコン。
※ 359 MDM（Mobile Device Management）：スマートフォンやタブレット端末等のスマートデバイスに関して、情報セキュリティの観点からパソコンと同様の管理を実現するためのソフトウェア製品の総称。
※ 360 例えば、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf〔参照 2018-05-28〕）がある。
※ 361 EUROCRYPT 2017：https://eurocrypt2017.di.ens.fr/index.html〔参照 2018-05-28〕
※ 362 段数：暗号の基本となる処理の繰り返し数。 識別子：実際の攻撃の際に用いられる、攻撃対象暗号アルゴリズムの統計的特徴。
※ 363 Asiacrypt 2017：https://asiacrypt.iacr.org/2017/index.html〔参照 2018-05-28〕
※ 364 Crypto 2017：https://www.iacr.org/conferences/crypto2017/index.html〔参照 2018-05-28〕
※ 365 「情報セキュリティ白書 2017」の「2.10.2（1）共通鍵暗号技術に対する攻撃の動向」（P.158）参照。
※ 366 semi-free-start 衝突攻撃：攻撃者により初期値をある程度変更することが可能とする攻撃者有利な状況下での衝突攻撃の一種。
※ 367 CRYPTREC：SHA-1 の安全性低下について http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html〔参照 2018-05-28〕
※ 368 NFS（Number Field Sieve、数体ふるい法）：離散対数問題を解く最も高速な方法。
※ 369 SNFS（Special NFS、特殊数体ふるい法）：特殊な形をした p に対して高速に動作する数体ふるい法。
※ 370 トラップドア：落とし戸。その情報を知っているものだけが暗号を高速に解読できる。
※ 371 https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf〔参照 2018-05-28〕

第3章
個別テーマ

本章では個別テーマとして、IoT、仮想通貨、スマートフォン、制御システム、中小企業の情報セキュリティについて解説する。

このうちIoT、スマートフォン、制御システムについては「情報セキュリティ白書2017」に続いて、より巧妙化、多様化する攻撃の実態を報告する。また制御システムについては、国内の重要インフラシステムのリスクアセスメントを支援するための「制御システムのセキュリティリスク分析ガイド」を紹介する。

仮想通貨については、2017年度は市場の急拡大が進む一方、過去最大の仮想通貨流出事件や、脆弱な端末を狙った不正マイニングの急増等が起こった。本章ではこうしたインシデントのほか、拡大する市場に対応しきれない仮想通貨基盤の課題や事業体制の整備の遅れ、必要な対策等を解説する。

中小企業の情報セキュリティは、重視されながらこれまで有効な対策が十分に実施できていない領域であり、一層の取り組みが求められている。本章では中小企業のセキュリティの実態、及び施策の一つとして2017年に創設されたSECURITY ACTIONを中心に、現状を紹介する。

3.1 IoTの情報セキュリティ

IoT（Internet of Things）技術を適用した家庭向け製品の低価格化や多様化により、ネットにつながる家電製品の普及が進んでいる。その反面、2016年に問題となった、脆弱なIoT機器を狙うウイルス※1も進化を遂げる等、IoTに対するセキュリティ脅威も多様化している。日本国内における脅威が急速に増大する中で、セキュリティ対策が不十分な製品が多く存在しており、政府や民間による対策強化の取り組みが始まっている。本節では、IoTの情報セキュリティの動向と取り組みについて述べる。

3.1.1 多様化するIoTのセキュリティ脅威

2016年、ウイルス「Mirai」に感染したIoT機器によって構成されたボットネットがサーバに対するDDoS攻撃に悪用され、世界中のインフラに大打撃を与えられることを示した※2。2016年末から2017年にかけては、IoT機器に感染する「Miraiと異なるウイルス」や様々な「Miraiの亜種」が出現し、IoT機器の利用者自身への攻撃や、特定のIoT機器を狙った攻撃が行われる等、IoTに対するセキュリティ脅威が多様化しつつある。ここでは、新たに検出されたこれらのウイルスや脅威について解説する。

(1) IoT機器のMirai等の感染に対抗する「Hajime」

2016年10月、Miraiを解析するために設置されたハニーポットによって、Miraiの感染経路、すなわちポート番号23で動作するTELNETと既定のパスワードを用いて感染する新たなウイルスが検出され、このウイルスは「Hajime」と名付けられた※3。感染したIoT機器によるボットネットを遠隔操作するC&Cサーバ※4のアドレスがハードコーディングされているMiraiに対して、Hajimeに感染したIoT機器はP2P通信を用いて遠隔操作されるため、特定のC&Cサーバが存在せず、ボットネットの無力化が困難となっている。また、感染したIoT機器のファイルシステムから自身を削除するとともに、実行中のプロセスリスト上のプロセス名を書き換えて自身の存在を隠蔽する機能を備える等、その隠密性も高度化している。

2017年4月、Hajimeの感染が急速に拡散し、全世界で数万台と想定されること、Hajimeに感染したIoT機器はDDoS攻撃の踏み台に悪用されないこと、代わりに善意の警告メッセージ（図3-1-1）がターミナル上に表示されること、ポート番号23、5358、5555、7547のポートへのアクセスが遮断され、Miraiやその亜種等のウイルスの感染を防御すること等により、結果的にセキュリティが向上することが報告された※5。同月、Hajimeの感染

手段として、Mirai の亜種と同様にポート番号 7547 または 5555 で動作するホームルータの管理プロトコル TR-064：LAN-Side DSL CPE Configuration の脆弱性を悪用する手口が拡張され、約 30 万台の感染機器（表 3-1-1）がボットネットを形成していることが判明した※6。また、ハニーポットを用いた解析により、感染を試みる機器が返すログイン時のバナーに応じて、その機器に対応するログイン名とパスワードを利用して不正侵入を試みる、等の挙動が明らかとなった※7。2017 年 9 月、ポート番号 5358 の TELNET も感染手段とされていること、ピーク時には 40 万台を超えた感染機器が 10 万台以下に減少したことが報告された※8。結果として感染機器を防御する状態が続いているが、ボットネットであることに変わりはなく、注意が必要である。

> *Just a white hat, securing some systems.*
> *Important messages will be signed like this!*
> *Hajime Author.*
> *Contact CLOSED*
> *Stay sharp!*

■図 3-1-1　Hajime が表示する善意の警告メッセージ例
（出典）Symantec Corporation「Hajime worm battles Mirai for control of the Internet of Things※5」

国・地域名	感染ホスト台数	比率
イラン	58,465	19.65%
ブラジル	26,188	8.80%
ベトナム	23,418	7.87%
ロシア	22,268	7.49%
トルコ	18,312	6.16%
インド	16,445	5.53%
パキスタン	14,069	4.73%
イタリア	10,530	3.54%
台湾	10,486	3.52%
オーストラリア	9,436	3.17%
その他	87,882	29.54%
合計	297,499	100%

■表 3-1-1　Hajime に感染した IoT 機器の国・地域別台数と比率
（出典）Kaspersky Lab「Hajime, the mysterious evolving botnet※6」を基に IPA が編集

(2) IoT 機器を破壊するウイルス「BrickerBot」

Mirai は、IoT 機器の機能は正常に動作させつつ、第三者への DDoS 攻撃に悪用するため、利用者は感染に気付かず、攻撃に加担させられていた。これに対して、IoT 機器の利用者に直接被害を与えるウイルスが出現した。2017 年 3 月、セキュリティベンダのハニーポットが検出したウイルス「BrickerBot」は、Mirai と同様にポート番号 23 の TELNET と既定のパスワードで IoT 機器に感染した後、IoT 機器のストレージ機能とカーネルパラメータの設定変更、インターネット接続の妨害、動作速度の低下、機器内の全ファイルの削除等の不正コマンドを実行して機器に致命的な改変を与え、最終的に使用不能にする。IoT 機器を永続的に使用不能とすることから、発見者はこれを「PDoS（Permanent Denial of Service）攻撃」と名付けた※9。同月、IoT 機器の破壊を試みるコマンドシーケンスが異なる複数のバージョンが検出されている※10。

2017 年 4 月、ハッキングフォーラムで「Janit0r」を名乗る BrickerBot の作者は、「脆弱性を有したままネットワークに接続される IoT 機器やそれによって発生する DDoS 攻撃を憂慮し、それらを駆逐するために、2016 年 11 月以降 200 万台を超す機器を使用不能状態にした」と主張した※11。同月、米国カリフォルニアの通信事業者 Sierra Tel が顧客に配布した Zyxel Communications Corp. 製のモデム HN-51 が Mirai と BrickerBot の感染攻撃を受けてネットワークに接続できなくなり、顧客のインターネット接続機能及び電話接続機能が失われ、同社はモデムの修理・交換に追われることとなった※12。

2017 年 7 月、インドの州立通信事業者 Bharat Sanchar Nigam Limited（以下、BSNL 社）及び Mahanagar Telephone Nigam Limited（MTNL）が顧客に配布したモデムやルータが BrickerBot の攻撃を受け、インターネット接続機能を失った。BSNL 社は、6 万台のモデム、全顧客の 45%のブロードバンド接続が影響を受けたこと、パスワードが初期設定のままのモデムのみが攻撃を受けたこと、新たに導入したモデムの 90%が影響を受けたこと等を報告した。BrickerBot の作者は、BSNL 社の数十万台のモデムにおいて、機器の設定を変更し、中間者攻撃や DNS ハイジャックを可能とする TR-069（ISP がモデムを遠隔管理するためのプロトコル）が動作しており、TR-069 に接続するためのポート番号 7547 が通信事業者以外からのアクセスにも開放されている問題点を指摘した※13。

2017 年 12 月、BrickerBot の作者は、2016 年 11 月から開始した「インターネット化学療法」プロジェクトで 1,000 万台以上の IoT 機器を攻撃してきたが、引退することを表明した※14。

(3) 続々と出現する Mirai の亜種

2016 年 9 月に公開された Mirai のソースコードを元に

派生したMiraiの亜種は、2017年に入ってからも次々と出現した。Miraiと比較して、IoT機器に対する侵入方法が高度化している。

(a) PERSIRAI

2017年4月に発見された「PERSIRAI」は、ポート番号81経由で管理画面にアクセス可能な、OEM生産された様々なネットワークカメラを感染対象とするウイルスである[※15]。4月26日の時点で、全世界で約12万台のPERSIRAIに感染する恐れのあるネットワークカメラがネットワークに接続されていることが報告されている（表3-1-2）。また、PERSIRAIは、ネットワークカメラに侵入後、3種類の既知の脆弱性（空の資格情報でHTTPアクセスすることによってユーザ名やパスワードが記載された設定ファイルの内容を返す脆弱性、CVE-2017-5674[※16]他）を突いて他のネットワークカメラを攻撃するようになっており、Miraiと比較して、特定のIoT機器への攻撃に特化した進化を遂げている点が特徴的である[※17]。

国・地域名	比率
中国	20.30%
タイ	11.60%
米国	8.84%
香港	4.66%
メキシコ	3.44%
ブラジル	3.43%
英国	3.40%
イタリア	3.37%
日本	3.33%
韓国	3.00%
その他	34.65%
合計台数：122,069台	

■表3-1-2　PERSIRAIに感染する恐れのあるネットワークカメラの国・地域別比率と合計台数（2017年4月26日時点）
（出典）Trend Micro Incorporated「Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras[※15]」を基にIPAが作成

(b) Reaper

2017年10月、Miraiのソースコードの一部を流用して作られたウイルス「Reaper」（発見者によっては「IoTroop」または「IoT reaper」と命名）が発見された[※18]。Reaperは、各種のネットワークカメラやルータ等のIoT機器が持つ、複数の脆弱性を突いて感染を試みる（表3-1-3）[※19-1]。これらの脆弱性には、PERSIRAIが悪用するネットワークカメラに対する脆弱性と同等の脆弱性（CVE-2017-8225[※19-2]、表中のNo.2）が含まれており、攻撃方法が更に多様化している。Reaperに感染する恐れのあるIoT機器は約200万台存在し、直近の7日間で2万台以上が感染していると報告された[※20]。

No.	ベンダ名	脆弱性
1	D-Link	D-Link DIR-600/DIR-300(rev B) ルータにおける複数の脆弱性[※21]
2	GoAhead及び各OEM	Wireless IP Camera (P2P) WIFICAMにおける複数の脆弱性[※22]（CVE-2017-8225他）
3	NETGEAR	NETGEAR ReadyNASにおける非認証のリモートコマンド実行の脆弱性[※23]
4	VACRON	VACRON NVRにおけるリモートコマンド実行の脆弱性[※24]
5	D-Link	D-Link 850Lルータにおける複数の脆弱性[※25]
6	Linksys	Linksys E1500/E2500ルータにおける複数の脆弱性[※26]
7	NETGEAR	NETGEAR DGN1000/2200 v1 ルータにおける非認証のコマンド実行の脆弱性[※27]
8	AVTECH	AVTECHネットワークカメラ・DVR・NVRにおける非認証の情報漏えい、認証バイパス等の脆弱性
9	各社	JAWS/1.0のHTTPサーバヘッダを返すカスタムWebサーバにおける非認証リモートコマンド実行の脆弱性[※28]

■表3-1-3　Reaperが感染に悪用する脆弱性
（出典）Radware Ltd.「Why the World is Under the Spell of IoT_Reaper[※19-1]」を基にIPAが作成

(c) 南米や北アフリカにおける亜種の拡散

2017年11月、Miraiの新たな亜種と見られる攻撃がアルゼンチンを中心に観測された[※29]。この攻撃は、Zyxel Communications Corp.製のモデムPK5001Zに存在する脆弱性（ハードコーディングされた管理者権限のパスワードによるログイン可能なバックドアの存在、CVE-2016-10401[※30]）を突いて感染を試みるもので、ポート番号2323及び23に対するスキャンが急増した。その後、南米での攻撃は、コロンビア、エクアドル、パナマ、エジプト、チュニジアに拡散するとともに、対象機器をネットワークカメラ、デジタルビデオレコーダ（DVR）、ネットワークビデオレコーダ（NVR）に拡大した[※31]。これらの攻撃は、後述するMiraiの亜種「Satori」に関連するものであったと報告されている[※32]。

(d) Satori ／ Okiru

2017年12月、Satoriと名付けられたMiraiの亜種による攻撃の観測と約28万台のボットネットの構築が報告された[※33]。Satoriの攻撃方法は2種類あり、一方はポート番号52869を狙い、ルータ等において無線

LAN 機能の実装に用いられるネットワークコントローラチップ用の Realtek SDK の脆弱性（任意のコードの実行、CVE-2014-8361[※34]）を突いて感染を試みるもので、1 万 9,403 台の感染が報告された。他方は、ポート番号 37215 を狙い、未知の脆弱性を突いて感染を試みるもので、26 万 3,250 台の感染が報告された。後日、Huawei Technologies Co., Ltd. 製ホームルータ HG532 に存在する未知の脆弱性（遠隔からの任意のコード実行、CVE-2017-17215）を悪用するものと判明し、「Okiru」の別名が与えられるとともに、世界各地で攻撃が観測された[※35]。

(4) 仮想通貨マイニングへの悪用

IoT 機器に対する脅威として、ボットネット形成、第三者に対する攻撃への悪用、機器そのものの破壊に加えて、仮想通貨マイニングへの悪用が確認された。2017 年 4 月、Mirai の亜種が仮想通貨の一つであるビットコインの採掘機能を有していることが報告された[※36]。また、2017 年 1 ～ 9 月の間に仮想通貨のマイニングの通信を検出した家庭用デバイス 1 万 2,669 台中、6.35% が IoT 機器であったとの報告がある[※37]。

3.1.2 国内に広がる感染被害や DDoS攻撃の脅威

2016 年、Mirai の存在が明らかとなった時点では、感染機器の大半は海外に設置されたものであった。また、感染機器によるボットネットの DDoS 攻撃被害も、海外に設置されたサーバ等に集中していた。しかし、2017 年 11 月以降、Mirai やその亜種についての感染事例が国内でも多数観測され、「対岸の火事」と無視できない状況となっている。

(1) 国内における IoT 機器のウイルス感染の急増

2017 年 11 月、国内における IoT 機器のウイルス感染が急増していることを示す調査結果が複数の情報源から報告された。他の IoT 機器への攻撃の観測結果に基づく、ウイルスに感染したと見られる IoT 機器の国別台数の調査結果によれば、これまで圏外であった日本が前月の約 94 倍、2 万 7,693 台の攻撃ホスト数を観測し、4 位にランクインした（表 3-1-4）[※38]。別の調査報告では、

順位	2017 年 8 月		2017 年 9 月		2017 年 10 月		2017 年 11 月	
	国・地域名	攻撃ホスト数	国・地域名	攻撃ホスト数	国・地域名	攻撃ホスト数	国・地域名	攻撃ホスト数
1	メキシコ	78,765	ブラジル	61,812	ブラジル	93,202	ブラジル	122,952
2	中国	57,525	中国	36,868	中国	44,244	中国	70,461
3	ブラジル	46,760	メキシコ	36,830	インド	22,772	アルゼンチン	66,989
4	インド	44,424	インド	25,086	ロシア	19,190	日本	27,693
5	ロシア	21,571	ロシア	19,271	トルコ	18,874	インド	23,380
6	トルコ	20,260	トルコ	18,071	米国	17,242	トルコ	23,172
7	イラン	12,199	米国	15,757	イラン	7,598	ロシア	15,037
8	米国	10,279	イラン	11,706	イタリア	7,415	米国	14,058
9	アルゼンチン	9,196	アルゼンチン	7,844	アルゼンチン	6,764	コロンビア	11,934
10	ベトナム	7,254	イタリア	7,423	メキシコ	5,472	エジプト	11,178
11	フィリピン	7,193	ベトナム	4,857	英国	4,860	イタリア	6,896
12	イタリア	6,533	英国	4,729	タイ	4,635	イラン	4,906
13	タイ	5,914	タイ	4,276	ベトナム	4,095	チュニジア	4,622
14	ポーランド	5,845	韓国	4,141	韓国	3,918	メキシコ	4,613
15	台湾	3,850	オーストラリア	3,518	オーストラリア	3,408	タイ	4,083
16	韓国	3,501	台湾	3,246	台湾	2,877	英国	4,023
17	オーストラリア	3,031	スペイン	1,977	ギリシャ	2,755	ベトナム	3,649
18	スペイン	2,558	ギリシャ	1,887	ポーランド	2,119	韓国	3,614
19	スウェーデン	2,379	ポーランド	1,796	スペイン	1,905	ウクライナ	3,287
20	英国	2,251	スウェーデン	1,774	エクアドル	1,897	エクアドル	3,220
―	ユニークな攻撃ホスト数	382,876	ユニークな攻撃ホスト数	299,597	ユニークな攻撃ホスト数	304,256	ユニークな攻撃ホスト数	470,212

■表 3-1-4　攻撃ホスト数国別順位の推移
（出典）横浜国立大学・BB ソフトサービス株式会社 IoT サイバーセキュリティ共同研究プロジェクト「平成 29 年度 横浜国立大学・BB ソフトサービス共同研究プロジェクト 研究開発成果報告書[※48]」の調査結果を基に IPA が作成

マルウェア活動観測プロジェクトMITFのハニーポットにおいて観測されたMiraiの亜種によるスキャン通信が11月から急増し、国内の感染機器数は4万台程度と推定されている※32。12月には、警察庁※39、国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology：NICT）※40、一般社団法人JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）※41から、Miraiの亜種に感染した国内のIoT機器からのスキャン急増に関する注意喚起が相次いで出された。観測結果からは、「3.1.1(3)(d)Satori／Okiru」で述べたMiraiの亜種であるSatori／Okiruの感染拡大であり、多くの感染機器に、脆弱性（CVE-2014-8361）を有する国内メーカ製無線LANブロードバンドルータが含まれていることが確認された。当該メーカは既に問題を認識しており、2013年6月より順次更新ファームウェアを公開していたが、その適用が徹底されていないことが明らかになり、改めて利用者に対して適用を呼びかけた※42。

(2) 脆弱性やバックドアを有するIoT機器の国内での流通

2017年1月、個人宅に設置したネットワークカメラが勝手に動き出すとともに、カメラのスピーカーから外国語が聞こえてくる事件が発生した※43。利用者はパスワードを設定していたが、何者かによって不正に遠隔操作されたと考えられた。8月、テレビ局の取材により、聞こえてきた音声がベトナム語であることが判明した※44。また、このネットワークカメラは、価格比較サイトで売れ筋ランキング及び注目ランキング1位（1月の時点）であった中国製カメラの並行輸入品であることが明らかになった※45。

同月、セキュリティ研究者が公開したハッキング実験結果によると、当該製品には、前項で述べた、空の資格情報でHTTPアクセスすることによってユーザ名やパスワードが記載された設定ファイルの内容を返す脆弱性（CVE-2017-8225、図3-1-2）があり、パスワードを変更していても第三者による不正操作が可能であった※46。

各社のネットワークカメラに共通部品として利用されている、電子回路基板上のネットワークカメラ用プログラムに脆弱性が存在するため、同様の脆弱性を有する製品が国内に大量に流通している可能性が高いことが指摘されている。セキュリティ研究者によると、中国製を含む一部ネットワークカメラのAPIが公開されており、出荷時に停止されていたTELNETを外部から起動するという、バックドアに相当する機能を攻撃者が悪用し、リモートからアクセス可能であるという※47。このようなIoT機器の流通拡大が、国内におけるウイルス感染の急増につながっていると推測される。

3.1.3 攻撃者の逮捕後も残る脅威

感染したIoT機器を乗っ取り、構築したボットネットでDDoS攻撃を行うウイルスは過去にも存在したが、Miraiの感染や攻撃では、従来のDDoS対策では防御不能な高い攻撃力、社会に大きな影響を与えるインフラを対象とした攻撃、ソースコード公開による様々な亜種の派生が世界中に大きな衝撃をもたらした。「Anna-senpai」を名乗りソースコードを公開した攻撃者の正体や目的にも関心が高まる中、2017年に入ると事態は大きく変化した。

(1) Deutsche Telekomのルータを攻撃した容疑者の逮捕

2017年2月、英国の国家犯罪対策庁（National Crime Agency：NCA）は、2016年11月に発生したド

```
user@kali$ wget -qO- 'http://192.168.1.107/system.ini?loginuse&loginpas'|xxd|less
00000000: 5749 4649 4341 4d00 0000 0000 0000 0000  WIFICAM.........
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0100 0000 0000 0000 0000 0000 0000  ................
[...]
00000690: 6164 6d69 6e00 0000 0000 0000 0000 0000  admin...........
000006a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000006b0: 6164 6d69 6e00 0000 0000 0000 0000 0000  admin...........
[...]
```

■図3-1-2　空の設定情報のHTTPアクセスで設定ファイルを不正取得する例
（出典）IT Security Research by Pierre「Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server※22」

イツの通信事業者 Deutsche Telekom が顧客に配布したルータへのウイルス感染攻撃に関与したとして、29 歳の英国人男性を逮捕した※49。被疑者は乗っ取ったルータでボットネットを構築し、ダークウェブ市場で販売することを目的としていたが、攻撃に失敗して結果的に約 90 万台のルータの通信障害を引き起こしたとされる。後日、Deutsche Telekom は、被害総額が約 200 万ユーロであったと報告している※50。2017 年 7 月、被疑者の犯罪行為の調査結果をセキュリティ専門家が報告した※51。同月に行われた裁判において、被疑者は自らの罪を認め、執行猶予付き 1 年 8 ヵ月の禁固刑を言い渡された※52。

(2) Mirai の作者とされる 3 名が罪状を自認

2017 年 1 月、Mirai に感染した IoT 機器からの DDoS 攻撃を受けた被害者であるセキュリティ専門家が、Mirai の開発者である Anna-senpai と考えられる人物の情報を公開した※53。同月、FBI が当該の人物である 20 歳の大学生に聞き取り調査を行った、と報じられた※54。

2017 年 12 月、米国司法省（U.S. Department of Justice）は、20 代の 3 人の若者が Mirai を開発して IoT ボットネットを構築し、大規模 DDoS 攻撃を仕掛けた罪状を認めた、と公表した※55。うち 2 名は、1 月に専門家が公開した情報で触れられていた人物で、DDoS 攻撃対策サービスを提供する会社（Protraf Solutions LLC）の共同創始者であった。主犯の大学生は、自身が入学した Rutgers 大学に対する DDoS 攻撃を実施し、大学のサーバを継続的にダウンさせていたことも判明した※56。自分達が起業した DDoS 攻撃対策サービスを利用させようとしたと見られており、ニュージャージー州裁判所は有罪判決を言い渡した。司法省は、Mirai を開発・利用した罪に関して、3 名に対して 5 年以下の懲役、25 万ドルの罰金、執行猶予 3 年の有罪を言い渡した※57。その他複数の罪状があり、公判が続けられている。

(3) Mirai の亜種の進化と脅威の残存

Mirai やその亜種を開発し、大規模 DDoS 攻撃を仕掛けた実行犯の一部は逮捕されたが、世界中の IoT 機器に対する脅威は残存している。「3.1.1 多様化する IoT のセキュリティ脅威」で述べたとおり、特定の IoT 機器の脆弱性を突いて感染し、初期の Mirai から得られた基本的な対策（初期パスワードの変更や不要な TELNET の停止等）を実施しただけでは防御不能な、Mirai の亜種の進化が続いている。

3.1.4 IoTセキュリティ対策強化への取り組み

これまで述べたように、IoT に対するセキュリティ脅威は多様化し、また国内での被害が拡大しており、以前にも増して対策強化が急務となっている。本項では、対策を検討する上で参考となるセキュリティガイド等の発行状況や政府及び民間の取り組みについて紹介する。

(1) IoT 関連セキュリティガイド等の改訂・新規発行

これまでに公開された IoT のセキュリティに関するガイドラインや手引き等の改訂版、新たに発行されたガイドライン等が公開された。2017 年以降に国内及び海外で公開された資料を、表 3-1-5（次ページ）と表 3-1-6（次ページ）に示す。

(2) IoT 機器に対する認証マーク付与制度の導入検討

2017 年 10 月、総務省は「IoT セキュリティ総合対策」を公表した※72。同年 1 月から開催してきたサイバーセキュリティタスクフォース※73 において取りまとめられた、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ものである。五項目に分けて整理された具体的施策のうち、「(1) 脆弱性対策に係る体制の整備」の一つとして「②認証マークの付与及び比較サイト等を通じた推奨」を挙げている。販売段階において脆弱性を有する機器の流通を防止することが重要との観点から、一定のセキュリティ要件を満たす IoT 機器に認証マークを付与することや、比較サイト等を通して認証マークが付与された機器が推奨される仕組みの構築について、具体的な検討を進める必要がある、としている（IoT セキュリティ総合対策については「2.1.3 (1) (a) IoT セキュリティ総合対策」参照）。

(3) 官民連携による「サイバー攻撃に係る通信の遮断」の検討

2017 年 10 月以降、総務省は「円滑なインターネット利用環境の確保に関する検討会」を開催している※74。この中では、IoT 機器を含む脆弱な端末設備への対策が検討事項の一つとして挙げられている。世界中に散在する IoT 機器自身を防御することや、それらの機器からの DDoS 攻撃を攻撃対象者側（エンドポイント）で防御す

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
IPA	つながる世界の開発指針 第２版※58	・経営者、開発者、保守者 ・考慮すべき事項、指針	2017 年 6 月
	IoT 開発におけるセキュリティ設計の手引き※59（2018 年 4 月版）	・開発者 ・具体的な設計手法	2018 年 4 月
	ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト 第２版※60	・調達者（利用者、運用者） ・機能要件、対策要件、対策方法	2018 年 3 月
	IoT 製品・サービス脆弱性対応ガイド※61	・IoT 製品・サービスの開発・提供企業の経営者・管理者 ・脆弱性対策の必要性の解説	2018 年 3 月
一般社団法人日本クラウドセキュリティアライアンス※62（Cloud Security Alliance Japan Chapter: CSA-JC）	「つながる世界」を破綻させないためのセキュアな IoT 製品開発　13 のステップ（2016 年 11 月公開英語版の翻訳）	・IoT 機器の開発者 ・具体的な設計・開発手法	2017 年 5 月
一般社団法人重要生活機器連携セキュリティ協議会※63（Connected Consumer Device Security Council: CCDS）	製品分野別セキュリティガイドライン 車載器編 Ver. 2.0	・特定の IoT 機器の設計に関わる会社の経営者、設計者、開発者 ・システムインテグレータ、利用者（金融端末（ATM）編のみ） ・特定の製品分野において考慮すべき設計・開発手法	2017 年 5 月
	製品分野別セキュリティガイドライン IoT-GW 編 Ver. 2.0		
	製品分野別セキュリティガイドライン オープン POS 編 Ver 2.0		
	IoT セキュリティ評価検証ガイドライン Rev1.0	・設計者、開発者、評価検証エンジニア、管理責任者 ・セキュリティ評価検証プロセス、リスク評価手法	2017 年 6 月
特定非営利活動法人日本ネットワークセキュリティ協会※64（Japan Network Security Association: JNSA）	IoT セキュリティ 標準 / ガイドライン ハンドブック 2017 年度版	・IoT ビジネス関係者全般 ・発行済みガイドの目的、主たる読者、特徴のまとめ	2018 年 5 月
公益社団法人日本防犯設備協会※65	防犯カメラシステムネットワーク構築ガイド Ⅱ ーインターネットとの接続に係る脅威と対策ー	・システム設計／構築／運営者 ・設計時・運営時の留意点	2017 年 5 月

■表 3-1-5　2017 年以降に国内で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
OWASP（Open Web Application Security Project）	IoT Vulnerabilities※66	・製造者、開発者、利用者 ・脆弱性と攻撃対象の概要	2017 年 8 月
GSMA（GSM Association）	GSMA IoT Security Guidelines Version 2.0※67	・設計者、開発者、サービス提供者、通信事業者 ・設計・実装方法、運用方法	2017 年 10 月
	GSMA IoT Security Assessment※68	・開発者、サービス提供者 ・セキュリティ評価チェックリスト	2017 年 10 月
OTA（Online Trust Alliance）	IoT Security & Privacy Trust Framework v2.5※69	・開発者、利用者 ・戦略的な原則	2017 年 6 月
	IoT Trust Framework - Resource Guide Updated January 5, 2017※70		2017 年 1 月
ENISA（European Union Agency for Network and Information Security）	Baseline Security Recommendations for IoT※71	・製造者、開発者、運用者、利用者 ・基本的な推奨要件	2017 年 11 月

■表 3-1-6　2017 年以降に海外で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

ることは容易ではない。検討会では、ボットネットを用いた大規模 DDoS 攻撃対策として、攻撃者の管理する C&C サーバからボット（乗っ取った IoT 機器等）への攻撃命令を通信事業者が遮断して、不正な遠隔操作を不能とする対策の検討が始められた※75。

総務省は、そのような対策を可能とする「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案」を国会へ提出した。法案は可決成立し、2018 年 5 月に公布された※76（改正の内容については「2.1.3（4）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改正に関する政策」参照）。通信事業者は、電気通信事業法の第 4 条「通信の秘密を守ること」に抵触する恐れがあり、実現に向けた課題と対処方法を整理する必要があるが、脆弱な IoT 機器に対する有効な対策の一つとして期待される。

（4）IoT セキュリティ基盤の民間団体の発足

2017 年 4 月、国内 IT ベンダ、セキュリティベンダ、クラウドサービス事業者等、IoT 事業を推進する 25 社・団体が集結し、IoT セキュリティ基盤のデファクトスタンダード構築を目的とした、一般社団法人セキュア IoT プラットフォーム協議会が発足した※77。同月、IoT 機器の製造時のセキュリティ標準（IC チップの耐タンパ領域内への公開鍵証明書組み込みによる認証や暗号化等）の策定を開始した※78。また、同年 10 月には、技術／標準化委員会内に三つの部会を立ち上げ、IoT セキュリティにおけるリスクと対策の整理や IoT 向け IC チップ／デバイスに要求されるセキュリティ仕様の検討を開始している※79。

3.2 仮想通貨の情報セキュリティ

2017 年 4 月、改正資金決済法が施行された。同法によれば、不特定の者に対して代金の支払い等に使用でき、法定通貨と相互に交換できる等の一定の要件を満たすものが、法律上、「仮想通貨」と認められる。

そして、金融庁・財務局の登録を受けた事業者（以下、登録業者）のみが、国内において仮想通貨の交換等を行うことができる。併せて、登録業者には、仮想通貨利用者の財産保護・マネーロンダリング対策の観点から、利用者財産の分別管理義務や本人確認義務等が課せられる。

登録業者等を会員とする、一般社団法人日本仮想通貨事業者協会（Japan Cryptocurrency Business Association：JCBA）は、2017 年 1 月 1 日を「仮想通貨元年の幕開け」と表現し、仮想通貨に関わる業者が連携してガイドラインや自主規制の策定に取り組むとした※80。

金融業界でも、独自仮想通貨の発行や、ブロックチェーン技術応用のための各種実証研究等が進められている。

このような中、主要な仮想通貨の価格は 2017 年末までバブルのような急騰を見せた後、一転暴落した。仮想通貨や新規仮想通貨公開（Initial Coin Offering：ICO）に対する各国の規制強化、仮想通貨「Tether」の対ドル可換性に対する疑惑※81 等が下落の要因として挙げられているが、2018 年 1 月の交換事業者コインチェック株式会社（以下、コインチェック社）における「仮想通貨 NEM（ネム）流出事件」は、国内の仮想通貨事業に対して更に冷水を浴びせた。

本節では、仮想通貨をめぐる動向とセキュリティ課題について述べる。

3.2.1 仮想通貨交換業の動向

現在、我が国の仮想通貨交換業のほぼすべてが、ビットコインを取り扱っている。2017 年、ビットコインのブロックチェーン仕様は数度にわたって分岐し、新通貨の生成※82 と取引停止等の混乱が生じた（ブロックチェーン分岐問題）。

また、2018 年 1 月、仮想通貨「NEM」の不正流出（不正移転）が発生し、仮想通貨交換業のセキュリティ上の問題点等が浮き彫りとなった（仮想通貨不正移転問題）。

(1) ブロックチェーン分岐問題

2017 年 7 月、ビットコインにおけるブロックチェーンの分岐問題が発生した。ブロックチェーンの分岐の方式には、過去のブロックチェーンと互換性が保たれる「ソフトフォーク」と、互換性がなくなる「ハードフォーク」があるが、それらがほぼ同時期に発生する恐れが生じた。その間、取引所における取り引きが一時停止する等の混乱が生じた。

結局、ソフトフォークは回避されたが、同年 8 月、ハードフォークにより、新通貨として BCH（ビットコインキャッシュ）が誕生した。

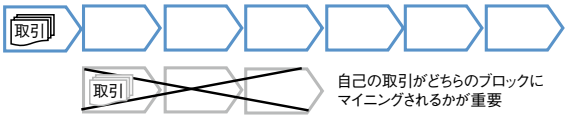
(a) 分岐問題の背景

ブロックチェーン分岐の原因は、ビットコインの「ファイナリティ問題」と、その解決手法をめぐるネットワーク参加者らの合意形成に困難が生じたことにある※83。

ビットコインの移転取り引きは、マイニング※84 によりブロックチェーンに記録される必要がある。ブロックチェーンの一時的な分岐問題※85 を考慮すると、単にブロックに記録されるだけではなく、最終的に長い方のブロックチェーンに記録されないと、取り引きは事後的に無効となる危険性がある（図 3-2-1）。

一般に、ある取り引きがブロックに記録された後、更に 6 ブロック程度が後続して、初めて、当該取り引きはその後覆されない状態になる（ファイナライズ）と言われる※86。現状のブロックチェーン仕様では 1 ブロックの形成に約 10 分かかるため、ビットコイン取り引きが確定するには約 1 時間程度かかる※87。

ビットコイン取り引きの増大とともに、ブロックチェーンに直ちに記録されない未承認取り引きの増加が深刻化する恐れがある。このような問題は「ファイナリティ問題」と呼ばれる。



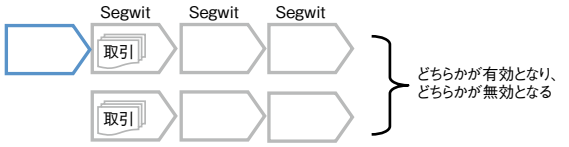
■図 3-2-1　ブロックチェーンの一時的分岐の概念図

ファイナリティ問題解決のため、ビットコイン開発者グループらは、取り引きトランザクションデータを小さくする案（Segwit：Segregated Witness※88）を提示した。マイ

ニングの際、より多くの取り引きをブロックに取り込む方法である。この仕様変更は、過去連なってきたブロックチェーンと互換性が認められ、多数の参加者が合意すれば、ブロックチェーンは一つに安定する。

しかし、Segwit 実装の合意が得られないまま、一部参加者が実装を強行しようとしたため、Segwit を支持するブロックと支持しないブロックが、どちらかが無効となるまで分岐を競争させる事態が生じた（UASF：User Activated Soft Fork）（図 3-2-2）※89。

この状況で取り引きを継続させた場合、将来消滅するブロックに記録された取り引きはすべて無効となり、それを基礎とした商品売買等の実体取り引きにも混乱が生じることになる。

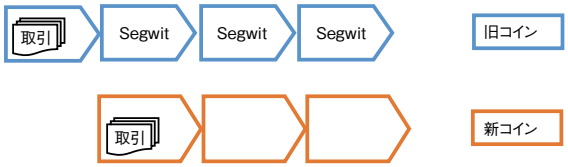


■図 3-2-2　UASF の概念図

他方、中国を拠点とするマイナー（採掘者）らは、ブロックチェーンのサイズを大きくする仕様変更案を提示し、有効化した（UAHF：User Activated Hard Fork）（図 3-2-3）。

この仕様変更は、過去連なってきたブロックチェーンと互換性がないため、このブロックチェーンに基づく新たな仮想通貨 BCH が誕生した（ハードフォーク）。

しかし、ハードフォークが発生した場合、直後の取り引きを、マイナーが新旧どちらのブロックに記録するか予測がつかず、また、新通貨の移転と旧通貨の移転が混在し、意図せず通貨を奪われる危険性もある※90。意図した送金がされる保証がない限り、ハードフォークの際に取り引きを継続するのは危険である。



■図 3-2-3　UAHF の概念図

(b) 分岐の影響

JCBA は、2017 年 7 月 18 日、ブロックチェーン分岐問題が収束するまで、会員の対応として、ビットコインの受け入れ及び引き出し受付を停止すると公表した※91。

また、同年 11 月、今後予想されるハードフォークや派生する新コインに関し、仮想通貨流通上の混乱を防ぎ、顧客資産の保護を図るための自主規制を策定した。会員は当該自主規制の趣旨に従った自社の対応方針を策定し、顧客に周知するとともに、その概要を一般公表するものとした※92。

(c) 今後の動向等

今後も、ビットコインの仕様変更等が行われる可能性があるが、参加者らの合意形成が困難な場合、円滑にシステムを維持する仕組みが存在せず、再び混乱が生じる恐れがある。ビットコイン等の多くの仮想通貨は、オープンソースソフトウェアとして開発され、参加者を限定しない「パブリック型」であることに由来する問題である。

また、今後、マイナー勢力が、新通貨による利得を目論んだ投機的ハードフォークを自由に行う可能性があり※93、いつ分岐が起きるか予測がつかない。2017 年 10 月、香港を拠点とするマイナーがブロックチェーンを分岐させ、BTG（ビットコインゴールド）が誕生した。その理由は、競争相手である中国勢マイナーが利用していたマイニング技術を使えないようにするためであったとされる※94。

ビットコインが採用するコンセンサスアルゴリズム PoW（Proof of Work）※95 のもとでは、マイニングパワーは特定勢力に独占されている※96。マイナーの支持のない通貨は、迅速かつ安定的な取り引きを実現できず、実質、無価値となる。マイナー勢力は、通貨の価格形成に加え、新通貨の発行と存続にまで影響を与えている。

このように、ブロックチェーンの分岐は、取引停止等の重大な弊害を生じさせるリスクをはらむが、現状ではマイナー等が恣意的に決めることができる。仮想通貨利用者を適切に保護するためには、仮想通貨交換業者らが相互に連携し、マイナーの動向等を常に注視し、利用者に対して適切な情報提供を行う必要がある（資金決済法 63 条の 10）。

更に、パブリック型システムでは、悪意ある参加者を排除する仕組みはなく、分岐等を契機に不正プログラムやバグ等の不備のあるプログラムが組み入れられ、コイン奪取等の被害が生じる恐れがある。

JCBA は、「会員取扱い仮想通貨一覧並びに仮想通貨概要説明書※97」を公開し、各仮想通貨プログラムの適正性やリスク評価をしている。しかし、リスク評価の基準は不明で、信頼性の保証もない。仮想通貨プログラムの瑕疵に起因する損害が発生した場合、仮想通貨交換業者と利用者間において、責任の所在や責任の

分配の問題が生じ得る。問題を解決する前提として、プログラムの安全性確認のための、「信頼性の保証された基準」が、事業者・利用者双方に必要になると思われる。

(2) 仮想通貨不正移転問題

2018 年 1 月 26 日、コインチェック社が運営する取引所「Coincheck」から、5 億 2,300 万の仮想通貨「NEM」が何者かによって不正移転された。被害者数は 26 万人、被害総額は当時の換算で約 580 億円相当に上る[※98]。国内取引所における事件規模としては、2014 年に発生したマウントゴックス事件を上回る、過去最悪の事案である。

(a) 不正移転問題の背景

NEM もビットコインと同じく、通貨移転行為は、その通貨を保有する権利者が実施しなければならない。それを保障する仕組みが、公開鍵暗号方式に基づく秘密鍵情報による電子署名技術である。

しかし、システムとして行うのは、署名の機械的検証だけで、実体的権利の有無は確認しない。秘密鍵情報による署名さえあれば、実体的権利者でなくとも、通貨の移転は可能である。

秘密鍵情報は、利用者自身のパソコン等で管理することも可能だが、多くの場合は取引所に預けている。2018 年 3 月時点で未だ捜査中であるが、コインチェック社の従業員のパソコンがウイルスに感染し、秘密鍵が盗み出された疑いがあるとされる[※99]。

(b) NEM 流出事件に対する評価

本事件後、秘密鍵情報の管理方法につき、コールドウォレット[※100]による管理の必要性やマルチシグネチャ[※101]実装の必要性等が指摘され、コインチェック社はこれらを怠ったとして非難された。

他方、当時、NEM 専用のコールドウォレット技術は開発されたばかりで、実装が間に合わなかった可能性があるとの指摘がある。また、マルチシグネチャであっても、完全なオフラインのもと、アクセス権限を限定する等の措置を併用しなければ意味はなく、そうした措置を徹底する場合、コストが高額になり、取り引きの利便性を欠く等の指摘もある[※102]。

なお、NEM の開発・普及を推進する NEM.io 財団は、ハードフォークにより不正移転取り引きを無効とすることはしない旨を発表した[※103]。NEM については、NEM.io 財団がブロックチェーンをコントロール可能であることを意味していると思われる。

(c) 金融庁の措置

金融庁は、2018 年 3 月、コインチェック社に対し業務改善命令を発出した。その中で、コインチェック社が、顧客保護とリスク管理を経営上の最重要課題と位置付けておらず、経営陣の顧客保護の認識が不十分なまま、業容拡大を優先させる等、内部管理態勢等に重大な問題が認められると指摘した[※104]。

またコインチェック社以外の取引所（登録業者を含む）に対しても立入調査等が実施された[※105]。その結果、不正出金事案等に対する原因分析の不足、顧客に対する情報開示の不備、実効性あるシステムリスク管理態勢の不備等を理由とした行政処分が複数社に対して発せられた。

(d) 今後の動向

秘密鍵情報を取引所が管理すること自体は禁止されておらず[※106]、その管理方法は、今後更に問題となる。

ここでいう秘密鍵情報には、HD ウォレット[※107]における seed 情報や API キー[※108]等、仮想通貨移転に関連するあらゆる情報が含まれる。これらは銀行口座における暗証番号と異なり再発行できない性質があるため、漏えいが発覚しても不用意に破棄できない。マルチシグネチャ等の技術も必ずしも万全ではない。マルチシグネチャでも、システムのバグにより不正移転が生じた事例があり[※109]、コールドウォレットでも、インターネット接続した際に中間者攻撃を受ける可能性が指摘されている[※110]。

仮想通貨交換業者は、こうした秘密鍵情報の性質、適用できるセキュリティ技術等を踏まえたリスク分析・リスク評価を行い、対策を講じることが必要である。また、業界全体に効力を及ぼす実効性のある自主規制ルールが必要である[※111]。

他方、取引所を介さず、利用者自身が秘密鍵情報を管理し、利用者間で直接取り引きできる仕組みとして、分散型取引所（DEX：decentralized exchange）の構想がある[※112]。DEX は取引所に対するサイバー攻撃の影響を受けないが、取引所における本人確認を通じて、マネーロンダリング対策等を実施する我が国の法制度との整合性が問題となる。

仮想通貨システムでは、不正移転があっても事後追跡が可能との指摘もある。しかし、本人確認不徹底の取引所[※113]や分散型取引所を介した上、取引経過を公開しない等の匿名通貨[※114]と交換する、等で事後追跡を免れる恐れがある。実際、コインチェック社から不正移転された NEM は、当初 NEM のモザイク機能等

を利用することで、ホワイトハッカーらに監視されたものの、その後匿名通貨との交換やダークウェブ取引所を介する等により、ほぼすべてが他の仮想通貨へ交換され、事後追跡が困難となった※115。事後追跡可能性の担保には、グローバルな対応が必要である※116。

金融庁は、2018年3月、仮想通貨交換業等をめぐる諸問題について制度的な対応を検討するため、「仮想通貨交換業等に関する研究会」を設置した※117。今後、みなし登録業者に対する規制強化、交換業者の情報開示や利用者保護の仕組み等を含めて、総合的な検討が行われると思われる。

3.2.2 金融業界の動向

金融業界では、ネットワークで分散して取り引きデータの検証や記録等を行うブロックチェーン技術が、取引記録の自動化、事務処理手続きの簡略化等の観点から注目され、実証研究が進められている。

ビットコインのような管理者なし・自由参加型の仮想通貨システムには、前述のとおり、ファイナリティ問題や、マイニングパワーを一部マイナーに独占された場合にブロックチェーンが任意にコントロールされ得る問題、悪意ある参加者を排除できない問題等がある。そのため金融業界においては、ネットワーク参加者を制限し、特定の管理者を置く等、集中管理的なアプローチである「コンソーシアム型」を採用する方向にある。

(1) 日銀による共同調査

日本銀行と欧州中央銀行は、2016年12月より、金融市場インフラへのブロックチェーン技術の応用可能性を調査してきた。調査の第一段階として、当該技術を即時グロス決済システムに応用した場合の処理スピードや障害耐性に焦点を当てて各種実験を行った。2017年9月、調査結果が発表され、ブロックチェーン技術を応用した場合でも、現行の決済システムとほぼ同等のパフォーマンスを示し得ること等が確認された※118。

ただし、当該実験ではブロックチェーンにブロックを追加できる権利を得る方式（コンセンサスアルゴリズム）として、管理者の存在を前提とするPBFT（Practical Byzantine Fault Tolerance）を採用している。PBFTは取り引きトランザクションの認証を限定された参加者（ノード）の合議で行うため、ビットコインの管理者なしのコンセンサスアルゴリズムPoWよりも比較的高速にファイナリティを実現できるとしている。

(2) 金融機関による独自仮想通貨の開発

株式会社三菱UFJフィナンシャル・グループは、2017年10月、ブロックチェーン技術を応用した独自仮想通貨「MUFGコイン」を初めて一般向けに公開した。ビットコインとは異なり、1コイン1円の価値に固定するステーブルコインと呼ばれるものである。公開ではスマートフォンを利用し、自動販売機による少額かつ即時決済の様子が実演された。2018年には、利用者拡大に向けた更なる開発を行うと発表している※119。

ビットコインシステムでは、マイニングのインセンティブとして手数料が不可欠であり、手数料の額も安定せず、少額決済にも適さないとされる。また、価値の変動も激しく、安定しない。

上記のような少額かつ即時決済の機能や、価値の安定性を実現するためには、報酬をインセンティブとして不特定多数の者にマイニングさせる仕組みではなく、運営側がブロックチェーンを管理する等の集中管理型アプローチが取られる可能性があり、今後が注目される。

(3) 今後の動向等

仮想通貨をめぐる金融業界の動向は様々である。

前記のとおり、「ブロックチェーン技術により、金融システムのコスト削減等を目指す試み」や、「当事者同士が国際間で自由に価値のやり取りを行うという、決済手段としての仮想通貨シェア確立を目指し、独自の仮想通貨を発行する試み」があるほか、「仮想通貨システムを銀行間決済に積極的に利用する試み」もある※120。

いずれの場合も、金融業界は集中管理型アプローチを採用する方向にあるが、パブリック型と比べて不利な点もある。例えば、取り引きトランザクションの正しさを検証する検証ノードを限定すると、当該ノードに対する攻撃があった場合、すべての取り引きが停止する危険性がある※121。集中管理型アプローチ固有の課題は、今後の実証実験等の蓄積の中で更に明らかにされると思われる。

金融庁は、通貨のデジタル化やブロックチェーン技術による分散処理等が進むことで、顧客同士が直接取り引きを行う仕組み（「分散型」）へ移行する等、金融サービスや金融機関の在り方に抜本的な変革がもたらされるとしている。その上で、2017年11月から、金融に関する法規制の横断化、「金銭」等の基本的概念の横断化（仮想通貨も金銭に該当するかという問題）、分散型取り引きに対する実効的な監督の在り方等について議論を開始している※122。仮想通貨をめぐる金融業界の動向は、こ

うした金融法令関係の動向と併せて注視していく必要がある。

3.2.3 その他の動向

その他の動向として、ICO が挙げられる。ICO とは、企業等が電子的にトークン（証票）を発行し、公衆から資金を調達する行為の総称である。電子的なトークンを仮想通貨とすることで、国際的かつ自由な資金調達が可能となる。

他方、簡単に資金調達ができることから詐欺の横行が問題となっており※123、詐欺被害や投資損失のリスクを避けるため、仮想通貨や ICO の広告を禁止した SNS もある※124。また、仮想通貨である以上、ブロックチェーン分岐やファイナリティ等の「ネットワークによるリスク」（以下、ネットワークリスク）及び不正移転対策も必要になる※125。ICO の資金源に、不正移転された仮想通貨が含まれた場合の法的効力等も検討する必要がある※126。

金融庁は 2018 年 3 月 8 日、仮想通貨交換業者登録をしていない海外法人の ICO について、日本居住者への販売はできない方針を示したが※127、海外の ICO への参加はリスクを見極め、慎重に行う必要がある。

3.2.4 おわりに

2017 年度は、仮想通貨をめぐって様々な問題やインシデントが発生した。この原因としては、ブロックチェーン技術等の仮想通貨固有の課題（ファイナリティ問題等）もあるが、事業者や政府の対応が急拡大するビジネスに追いつかなかったことも大きいと考えられる。問題分野や課題等を正確に把握し、対策を検討していく必要がある（表 3-2-1）。

例えば ICO 等における詐欺対策については、一般投資取り引きと同じく、消費者対策や、事業者の財政基盤等に対する監視※128 等が必要である。ただし、国際取り引きに対して、我が国の監視・監督が及びにくいという課題がある。

ネットワークリスク対策については、各仮想通貨のマイニングアルゴリズムやブロックチェーン仕様を正確に把握した上で、特にパブリック型においては、予測困難なマイナーの動向に対する対応方法等が課題となる。

取引所のセキュリティ対策については、秘密鍵情報の管理方法がとりわけ重要であり、取り引きの利便性やコスト等を踏まえつつ、実効性ある対策の検討が必要である。

標的型攻撃、DDoS 攻撃※129、リスト型攻撃※130、フィッシング※131 等、一般的なサイバー攻撃リスクへの対応も当然必要である。仮想通貨交換事業が本格運用された直後に重大なインシデントが発生した状況に鑑みれば、仮想通貨交換業者は、業界としてのセキュリティ対策の明示と実践（監査・情報開示等を含む）、そのための体制整備が急務といえる。その際、取引所によってセキュリティ基準が異なるのは、利用者保護の観点から問題があり、業界内での統一的な安全基準が必要と思われる。

他方、仮想通貨利用者も、2 段階認証の利用の徹底、セキュリティ意識の高い取引所を選択する等、情報リテラシーの更なる向上が必要である。

仮想通貨をめぐっては、少額かつ即時決済を実現す

	脅威	問題分野	主な対策	課題
仮想通貨固有の問題	仮想通貨不正移転	秘密鍵等管理方法	コールドウォレット、マルチシグネチャ、権限管理	開発不備、取引利便性への障害、コスト過大等を考慮したリスク分析
			分散型取引所	資金決済法との整合性
			事後追跡機能	本人確認不十分な取引所、匿名通貨との交換
	ネットワークリスク（ブロックチェーンの分岐、取引遅延等）	コンセンサスアルゴリズム	マイナー等の動向注視、オフチェーン技術等の実装	マイナー勢力等の意向の影響が大きく、予想が困難。新技術の実装研究は未だ発展途上
			PBTF 等集中管理型コンセンサスアルゴリズムの採用	限定ノードに対する攻撃の危険、パブリックシステムへの適用困難
	不正プログラム	各仮想通貨の OSS	十分な検証、安全性確認	信頼性の保証のある基準の確立
一般的問題	その他サイバー攻撃	各取引所、個人のセキュリティー般	パッチ適用、通信暗号化、サーバ冗長化、2 段階認証等	統一的な安全性基準の確立、情報リテラシーの向上
	詐欺（ICO 詐欺含む）	取引関係者の説明義務、財政基盤の有無	消費者対策、取引業者に対する監視・監督	国際的取り引きが容易に行われ、我が国の監視が及ばない場合

■表 3-2-1　仮想通貨の問題分野別検討表

るため、マイクロペイメントチャネル※132 やライトニングネットワーク※133 といったブロックチェーンの外側（オフチェーン）を利用する技術や、ブロックチェーンとは異なるアプローチを取る「Tangle※134」と呼ばれる技術も実装され始めている。これらの技術は IoT 分野での応用が期待されている。

今後も、新たな技術が研究・応用され、仮想通貨を基盤とするサービスの発展に資することが期待される。それとともに、セキュリティ対策の向上に向けた積極的な検討も並行して進める必要がある。

3.3 スマートフォンの情報セキュリティ

スマートフォンやタブレット端末（以下、スマートフォン）の利用者を狙った攻撃は依然として存在する。ここでは、更に巧妙化するそれらの手口と対策を紹介する。

3.3.1 アプリ誘導

2017 年も、前年に引き続き「アプリ誘導」に関する相談が IPA に多く寄せられた。

アプリ誘導とは、スマートフォンでインターネットを閲覧していると、突然、ウイルス検出を知らせる警告画面を表示させ、「今すぐ解決が必要」等のメッセージでアプリのインストールを促す手口のことである（図 3-3-1）※135。偽の警告画面を表示させて利用者の行動を誘導するという点で「偽警告」や「偽セキュリティソフト」の手口と類似しているが、最終的にアプリをインストールさせることが目的であり、直接的な金銭目的ではない点で違いがある（パソコン利用者を狙った偽警告の手口については「1.3.7 (1) 偽警告の手口と対策」参照）。

■図 3-3-1　アプリ誘導の警告画面例

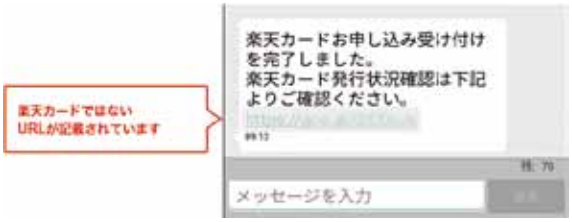
2017 年のアプリ誘導に関する相談件数は 243 件で、2016 年から継続して発生している。また、iOS、Android 双方の利用者から相談が寄せられているが、全体の 90.1%は Android 利用者からの相談である。

相談において誘導されるアプリとして挙げられたものは、どれも App Store または Google Play 等の公式マーケット上にあるもので、セキュリティ対策やスマートフォンの動作軽量化をうたうものが多い。公式マーケットにあるアプリのため、情報を窃取するような不正アプリである可能性は低い。IPA で実際に確認するため、主要ベンダのセキュリティアプリをあらかじめインストールした上で、実際にアプリ誘導の手口で誘導されるアプリのインストールを行ったが、問題等は検出されなかった。これらのことから、本手口は PPI（Pay Per Install）によるアフィリエイト収入を目的としていると考えられる※136。ただし、不適切な警告で誘導されるアプリであるため、まずは警告を鵜呑みにせずにインストールしないことが重要である。仮にインストールした場合でも、意図しない形でインストールした本来は不要なアプリと言えるため、アンインストールすることを推奨する。

3.3.2 SMSから不正アプリをインストールさせる手口

2018 年 1 月、IPA に「佐川急便から不在通知を連絡する SMS（ショートメッセージサービス）のメッセージを受信して、記載されたリンク先を開いてしまった」「楽天カードから申し込み受付の連絡が来て、URL を開いてしまった」という相談が寄せられた（図 3-3-2、図 3-3-3）。相談によると、リンク先にアクセスしたところ、その企業の Web サイトと見た目が酷似した Web サイトが表示されたという。

■図 3-3-2　佐川急便をかたる不審な SMS メッセージ
（出典）佐川急便株式会社「佐川急便を装った迷惑メールにご注意ください※137」



■図 3-3-3　楽天カードをかたる不審な SMS メッセージ
（出典）楽天カード株式会社「フィッシングの被害からお客様を守るために※138」

これらは、リンク先にアクセスさせて不正アプリをインストールさせる手口であることが確認された※139。

リンク先の Web サイトは、実際の企業の Web サイトをコピーして見た目をそっくりにしている（図 3-3-4）。この Web サイトから「sagawa.apk」または「rakuten-card.apk」という Android のアプリケーションファイルをダウンロードさせる仕組みとなっている。また、Web サイトの下部には、ダウンロードした不正アプリのインストールのブロックを解除させる手順が GIF アニメーションで説明されている。アニメーションの画像では手順中に押すボタンを赤丸で囲む等の工夫がなされ、利用者を騙すために巧妙な作りとなっている（図 3-3-5）。

■図 3-3-4　楽天カードをかたった不正な Web サイト

■図 3-3-5　楽天カードをかたった不正な Web サイト上の GIF アニメーション例

表示される手順に沿って操作をすると、不正アプリがインストールされるがホーム画面上にアイコンは表示されない。見た目は変化がないため、気付かれにくい仕組みとなっている。この不正アプリはアドレス帳等の個人情報を含めた端末内データの収集や、端末の管理者権限の取得、遠隔操作による画面ロックの可能性があることが確認されている（図 3-3-6）。

インストールされた不正アプリは、スマートフォンの設定項目にあるアプリ一覧でその存在を確認できるため（図 3-3-7）、そこからアンインストールすることはできる。ただし、不正アプリをインストールした場合は、念のため端末を初期化してから利用することを推奨する。

■図 3-3-6　楽天カードをかたった不正アプリが端末に求める権限一覧

■図 3-3-7　アプリ一覧にある楽天カードをかたった不正アプリ

不正な Web サイトから公式マーケット外にあるアプリをダウンロードさせるという仕組み上、この手口は Android を対象としていると考えられる。iOS では公式マーケット以外から入手したアプリをインストールできないように制限されているため、ここに挙げた手口で被害に遭う可能性は低いと言える。

ただし、寄せられた相談では iOS でも同様の SMS メッセージを受信したことが確認されている。リンクを開いただけで被害に遭う事例は確認されていないが、念のため、もし受信した場合はリンク先を開かず、メッセージを削除することを推奨する。

なお、本手口については、既に佐川急便株式会社、楽天カード株式会社のそれぞれが自社の Web サイト上で注意喚起※140 を行っている。

海外でも広告等から誘導し、アプリを公式マーケット以外からダウンロードさせる手口を用いる不正アプリが確認されている※141。この不正アプリは公式マーケット上に実在するアプリに偽装されているが、公式マーケットのアプリではないため、このような偽装が可能となる。

3.3.3 中高生を対象としたセクストーション被害

これまでにも、IPA ではセクストーション（性的脅迫）被害に関する注意喚起を行ってきた※142。典型的な手口は以下のとおりである。

① SNS を通じて知り合った異性から、プライベートな動画を見せ合おうと、ビデオチャット機能を持つアプリ（実際はアドレス帳等の情報を窃取する不正アプリ）のインストールを持ちかけられる。

②相談者（被害者）は当該アプリをインストールして、ビデオチャットの最中に服を脱ぐ等の行為でプライベートな動画のやりとりをする。

③その後、「ビデオチャットの動画をアドレス帳の相手にばら撒かれたくなかったら、指定の金額を払え」と脅迫される。

不正アプリのインストールを用いないセクストーションの相談も寄せられている。SNS の正規のメッセージ機能等を通じて、写真や動画のやり取りをした結果、「インターネット上に公開する」と脅迫されたという（図 3-3-8）。

警察庁・文部科学省は 2017 年 6 月の注意喚起で、SNS 上の相手にそそのかされて、プライベートな写真や動画を送ってしまう「自画撮り被害」の危険性を指摘している※143（「2.8.1（1）青少年に対する取り組み」参照）。また、セクストーションの被害は中高生で増加傾向にあり、そのことについて IPA は注意喚起を行った※144。

一方、IPA が行った「2017 年度情報セキュリティに対する意識調査※145」では、10 代において「SNS で自身の性的な写真や動画を撮影して投稿した」を問題であると回答した割合は 51.5%にとどまった。

■図 3-3-8　SNS アプリを通じたセクストーション被害のイメージ

セクストーションの被害を防止するには、以下の点に注意することが重要である。

- SNS を通じて知り合い、実際には会ったことのない相手はもちろんのこと、例え友人や恋人であっても第三者に見られたら困るプライベートな写真や動画を撮影したり、送ったりしない。
- 第三者に渡してしまった写真や動画は、自分の手の届かないところで、インターネット上に拡散されてしまう等、管理が及ばない状態となる。そうなった場合、完全に削除することは極めて困難であることを理解する。

3.3.4 遠隔監視アプリの悪用による被害

2017 年は、遠隔監視アプリを悪用した犯罪が多数確認されている。6 月には、女子大生のスマートフォンに遠隔監視アプリを無断でインストールし、私生活を隠し撮りしたとして、「不正指令電磁的記録供用」と「ストーカー規制法」違反の疑いで会社員が逮捕される事件があった※146。愛知県警察によると、遠隔監視アプリでの撮影に対してストーカー規制法を適用したのは、全国でも初めてとのことである。

また 11 月にも、交際していた女性のスマートフォンに遠隔監視アプリを無断でインストールしたことで、不正指令電磁的記録供用の疑いで逮捕者が出た※147。容疑者は、スマートフォンのマイクで録音した音声や SNS 等の交流サイトでのやり取りを監視していたと見られる。

悪用された遠隔監視アプリとして確認されているものの一つに「TrackView」があり、Google Play と App Store の両公式マーケットに公開されている。マーケット上の説明では、赤ん坊やペットの遠隔監視等、防犯目的のアプリであり、正規のアプリを悪用した事例と言える。

無断でこうした遠隔監視アプリをインストールされてし

まった原因としては、逮捕された容疑者が、当該スマートフォンを自由に操作できる状況であったことが挙げられる。そのため、無断でアプリをインストールさせない対策としては以下の点に注意する必要がある。

- 例え信頼できる相手だとしても、所有するスマートフォンに無断で触らせないようにする。
- 指紋・顔認証等を含めたパスコードロックをかけ、本人以外はスマートフォンを操作できないようにする。

3.3.5 iOSで動作する不正プロファイル「iXintpwn」

2017年6月、日本の男子中学生がランサムウェアを作成し、不正指令電磁的記録作成・保管の容疑で逮捕された※148。未成年がランサムウェアを作成し、逮捕まで至ったという事例のため、複数のマスメディアに大きく取り上げられた。

本項では、同じ男子中学生が作成したiOS上で動作する不正な「構成プロファイル」（以下、不正プロファイル）を取り上げる※149。iOSの各種設定を自動的に行うためのプロファイルを構成プロファイルという。

今回作成された不正プロファイル「iXintpwn」（アイシントポウン）は、この自動設定の仕組みを悪用して、iOS端末のホーム画面に大量の無意味な顔写真のアイコンを作成する。更にiXintpwnは、作成されたアイコンが削除不可となるように設定されていた。

iOSは、Apple Inc.によって厳しく審査され、公式マーケット上に配布されたアプリしかインストールできないよう制限されている。こうした仕組みから、設定変更をするだけで公式マーケット以外から入手したアプリもインストールできるAndroidと比較してiOSの方が安全といわれている。

しかしながら、構成プロファイルはアプリではないため、このような制限は適用されない。iXintpwnでは、未署名の不正プロファイルをダウンロードするページへのリンクがSNS等を通じて拡散された。リンク先のページにおいて、「iOSを脱獄※150できるアプリ」と称したダウンロードボタンを押すと、iXintpwnがダウンロードされる仕組みとなっていた。

また、国内における被害は確認されていないが、iXintpwnの亜種が既に確認されている※151。亜種はiXintpwnと違って署名済みの不正プロファイルとして配布されたため、署名済みの構成ファイルであっても安易に信用すべきではない。iOSは比較的安全だからと、ネット上に拡散されるリンク等から不用意に構成プロファイルをダウンロードしてしまうと、意図しない被害に遭うことも考えられ、注意が必要である。

iXintpwnは設定上、削除不可となっているが、以下のいずれかの方法でiOSを元に戻すことが可能である。

- Macを所有している場合、Apple Inc.の公式iOS構成管理アプリケーション「Apple Configurator 2」を使って削除する。
- iTunesまたはiCloudでバックアップしたデータを復元する。

3.3.6 公式マーケット上に配布された不正アプリ

2017年もiOSやAndroidの公式マーケットで悪意ある機能を仕込まれた不正アプリが相次いで発見された。

4月には人気ゲームアプリの攻略法を解説する、40本以上のガイドアプリの中に、不正な広告表示等を行うウイルス「FalseGuide」が発見され、200万人以上の利用者に影響していると見られている※152。

8月にはDDoS攻撃を発生させるウイルスが仕組まれた悪質なアプリが配信され、100ヵ国以上の端末が関わる大規模な攻撃へと発展した※153。「WireX」と呼ばれるこのウイルスは、300本以上のアプリに組み込まれて配信された（「1.2.2(1)DDoS攻撃の傾向」参照）。

また、同月にはオンラインバンキングを狙う「BankBot」の亜種が報告された※154。BankBotは2017年1月ごろよりその存在が確認されていたが、日本の銀行が対象に含まれていることが8月に初めて確認された。正規のオンラインバンキングに見せかけた偽の認証画面を表示させるだけでなく、SMS機能を乗っ取ることで、2段階認証の突破も可能としている。

10月には、仮想通貨のマイニングを勝手に行う不正アプリが確認された※155。複数種の不正アプリが確認されたが、そのうちのいくつかは仮想通貨マイニングサービスである「Coinhive※156」を利用している。これらのアプリを起動させると、端末のリソースを使って勝手に仮想通貨のマイニングを行う。CPU使用率は高い数値を示し、パフォーマンスに影響を及ぼす。

2018年2月に、App Store上でサードパーティーのアプリストアへ誘導する不正アプリが確認された※157。このアプリは実在する日本のアプリ名と酷似しており、家計簿アプリを装っている。このアプリを起動すると許可を求めるメッセージが表示され、最終的にはサードパーティーのアプリストアへ接続する細工がされている。アプリ名は日本語のため、日本を標的としているように思われるが、

誘導されるアプリストアは中国語表記となっている上、日本以外の複数の国でも確認されている。なお、このサードパーティーのアプリストアには iOS を脱獄するアプリ等があり、ダウンロードが可能となっていた。

現在、この家計簿アプリを装った不正アプリは App Store 上から削除されている。

これらの事例の、日本における被害は確認されていない。しかし、既に国内の銀行が攻撃対象とされていたという事実がある。例え公式マーケット上のアプリであっても、開発元の信頼性や、求められる権限等に注意を払う必要がある。

3.4 制御システムの情報セキュリティ

制御システムは、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラやサービスを動かしているシステムである。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、外部からいわゆるサイバー攻撃を行うことは困難と考えられていた。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、制御システムもサイバー攻撃を受ける恐れが高まってきている。実際に、サイバー攻撃による路面電車の脱線※158、浄水施設における薬液注入量の改ざん※159、大規模停電※160等も発生している。本節では制御システムのセキュリティの動向と取り組みについて述べる。

3.4.1 制御システムのインシデント事例

2017年は、大規模かつ甚大な被害につながったインシデントは公表されなかった。しかし、制御システム関係者へのアンケート調査では、377社中68%が過去1年間に「機密情報の窃取や操業停止が発生した」と回答していることから※161、インシデントはそれなりに発生しているが、多くが公表されていないと推察される。

そのような中、制御システムが一般的なランサムウェアに感染し、操業が停止した事例が国内外で報道された。2017年1月には、「つい最近の事例」として、ブラジルの大手電力会社の制御システムがUSB経由で「CryptoLocker」に感染した事例が報告された。この電力会社では冗長化が適切に行われていたため、運用への影響はなかったという※162。また同年5～6月には、フランス、英国、日本で大手自動車メーカの工場のコンピュータが「Wanna Cryptor」（別名 WannaCry）に感染し、1日～数日間操業が停止した※163。

同じく6月には、大手海運グループの荷役（コンテナの積み込み・積み下ろし）を管理するシステムが「NotPetya」に感染し、同グループの世界各地のターミナルで操業が停止した。更に、アジアの港では感染が港に停泊していたコンテナ船の船舶システムにも広がり、配電盤がシャットダウンして動力系統等への電力供給ができなくなったという※164。最終的な損害は2億5,000万～3億ドル（約270億～330億円）に上るとされている※165。

これらの事例は、制御システムネットワークにランサムウェアが侵入する経路や手段が存在すること、また、国家等による高度な攻撃ではなく、不特定多数を標的とするウイルスや汎用的な攻撃によっても操業に影響を及ぼす被害が発生し得ることを示した。

12月には、米国のセキュリティベンダが、8月に発生した中東の重要インフラ事業者の安全計装システム※166を狙ったサイバー攻撃に使われたウイルス「Triton」（別名 Trisis、HatMan）の解析結果を発表した。Tritonは Schneider Electric 製の安全計装システム「Triconex Tricon Safety Instrumented System（SIS）」を標的とし、安全計装コントローラのファームウェアのゼロデイ脆弱性を悪用して、遠隔操作ウイルス（Remote Access Trojan：RAT）をインストールすることが判明した。実際の攻撃では同コントローラが安全のために制御システム（プロセス）を緊急シャットダウンしたことでそれ以上の被害は発生しなかった。ウイルスの解析では最終的な目的は分かっていないが、安全計装コントローラによって緊急シャットダウンが引き起こされたのは攻撃者らの計算違いであり、より深刻な被害を引き起こすことを狙っていたと推測されている※167。制御システム運用の安全を守る安全計装システムを標的とするウイルスが出現し、実際に緊急シャットダウンが引き起こされた事実は重大であり、今後同様の攻撃が発生することも予想される。

表3-4-1（次ページ）に、2017年に公にされた、その他の主な制御システムのインシデント事例を示す。内部関係者（「元」を含む）の故意または過失や、第三者による既存のリモートアクセス経路の悪用、ソーシャルエンジニアリングによる不正アクセス等、これまでに想定されてきた脅威によって、実際にインシデントが発生している。制御システム運用者はこれらの事例を教訓に、自組織のリスクを見直していただきたい。

事例名	分野	発生国	発生年月（報道年月）	影響・被害	内容（原因等）
小規模電力会社の電力システムのランサムウェア感染による給電停止※168	電力	不明	2016年1月（2017年1月）	制御システムへのランサムウェアの感染拡大により、顧客への給電が一時的に停止した。身代金を支払ったにもかかわらず復旧できなかったが、バックアップを取得していたことからシステムダウンは2日間にとどまった。	脆弱なWebサーバが「SamSam」の亜種に感染した。DMZがなかったため、情報系から制御系に感染が拡大した。
警察の監視カメラシステムのランサムウェア感染による録画停止※169	行政	米国	2017年1月	ワシントンD.C.の公共の場所に設置されている監視カメラの映像を記録する警察の監視カメラシステム（ネットワークビデオレコーダ）の約70%（187台中123台）がランサムウェアに感染し、4日間映像が録画できなかった。	不明
刑務所システムへの侵入による記録の改ざん※170	行政	米国	2017年1月	攻撃者が刑務所のコンピュータシステムに侵入し、友人である服役囚を不正に早期出所させるため、記録を改ざんした。改ざんはすぐに検知されたが、被害の調査・対応に23万5,488ドル（約2,700万円）の費用を要した。	攻撃者は当初刑務所の職員に標的型メールを送りつけたが失敗した。その後、電話によるソーシャルエンジニアリングによって、「刑務所システムのアップグレード」と偽ってウイルスをダウンロードさせることに成功した。
市の非常警報サイレンシステムのハッキングによる不正操作※171	行政	米国	2017年4月	市の全156台の非常警報サイレンが真夜中に鳴り響く事態が発生した。4月8日の深夜0時30分から1時20分にシステムを停止させるまで断続的に12回以上発報した。	攻撃者は、システムがサイレンを制御する無線信号を不正送信した。
交通関連のカメラのランサムウェア感染によるスピード違反処理妨害※172	交通	オーストラリア	2017年6月	ヴィクトリア州で、159台のスピード違反取り締まりカメラと交差点監視カメラが、Wanna Cryptorに感染し、断続的に再起動を繰り返す状態が発生した。7,500件の違反切符につき、調査の間、いったん取り消しすることが発表された。	保守作業用に持ち込まれたUSBメモリ経由で感染した。
運輸当局へのDDoS攻撃による列車の運行遅延※173	鉄道	スウェーデン	2017年10月	スウェーデンの運輸当局がDDoS攻撃を受け、列車運行を管理するシステムがダウンして運行に影響が生じた。	不明

■表3-4-1　2017年に公にされた、その他の主な制御システムのインシデント事例

3.4.2 制御システムに対するサイバー脅威の動向

本項では、制御システムの脆弱性の報告状況、及び制御システムへのサイバー攻撃からうかがえる脅威の動向を示す。

(1) 脆弱性の動向

米国国土安全保障省（Department of Homeland Security：DHS）の組織で、制御システムの脆弱性情報の収集やインシデント対応支援を行っているICS-CERT（Industrial Control Systems Cyber Emergency Response Team）が2017年に公開した制御システム関連の脆弱性は、322件であった※174。ICS-CERTにおける脆弱性の集計方法の変更※175及びDHSの組織再編※176のため、過去の公開件数と一概には比較できないが、少なくない数の制御システム関連の脆弱性が公開されている。

SCADA（Supervisory Control and Data Acquisition）※177システムの脆弱性に絞ると、セキュリティベンダが2015～2016年にICS-CERTに報告されたSCADA/HMIソフトウェアの脆弱性を調査した結果によれば、23%が認証の欠如及び権限認可に関する問題、20%がメモリ破損の脆弱性※178であり、不正アクセスや任意のコード実行を許しかねない脆弱性が多く見つかっている。併せて同調査では、ベンダの製品開発に多層防御の観点がなく、セキュリティが確保された環境での運用を想定したセキュリティ設計となっている傾向を指摘している※179。また、IOActive, Inc.とEmbediが行ったGoogle Playで公開されている34のモバイルSCADAアプリケーションの調査では、重要インフラサービスの妨害に悪用される可能性のある脆弱性が147件発見された。調査したアプリケーションの94%でプログラムの改ざんが可能な問題、59%で権限認可に関する問題が見つかっており、従来の制御システム開発者や運

用者が認識していないところに攻撃の糸口が存在する可能性がある※180。

また、制御システムに影響を及ぼす可能性のある脆弱性も複数公開された。2017年10月に公開された、Wi-Fi通信の暗号化プロトコル「WPA2」における、暗号鍵が解読され、通信が盗聴される可能性のある脆弱性「KRACK」※181、及び、2018年1月に公開された、マイクロプロセッサ（CPU）におけるメモリから機微な情報が窃取される可能性のある脆弱性「Meltdown」及び「Spectre」※182は、ともに制御システムで広く利用されている汎用プロトコルやプラットフォームの脆弱性であった。

制御システムの運用者は、ベンダの推奨する環境や設定を考慮して運用するとともに、ベンダから情報を入手して脆弱性の影響及び対応の要否を確認し、修正プログラムの適用が必要な脆弱性については早急に対応することが望まれる。一方、制御システムの開発者は、製品がセキュアでない環境で利用される可能性も考慮してセキュリティ設計を行うほか、セキュアなプログラミングを実施することが望まれる。

(2) 脅威の動向

2017年は、大規模なインシデントこそ発生しなかったものの、今後制御システムのサイバー脅威が高まる予兆となる事件や傾向が見られた。

(a) 制御システムのランサムウェア感染

制御システム分野でもランサムウェアが話題となった。Kaspersky Lab, Inc.では、2017年1～6月に制御システムのランサムウェア感染を435件確認しており、うち、WannaCryptorが登場した5月は80件、6月は131件であった※183。「3.4.1 制御システムのインシデント事例」で挙げたように、ある程度詳細が公表された事例だけでも複数件報告されている※184。また、制御システムへの影響は不明だが、ロシアの大手鉄鋼メーカ及び石油会社、ウクライナの国際空港、ドイツの鉄道事業者等もランサムウェアの感染を公表している（ただし、製造や列車の運行等への影響はなかったとされる）※185。

ある調査では制御システムのインシデントの53%がウイルス感染によって引き起こされており、ランサムウェアも同じ経路で感染する可能性がある※186。また、ランサムウェアをトップレベルの脅威と考える事業者の存在も2016年の18%から倍増して2017年は35%となっている※187。

ランサムウェアの悪用が2018年も続くと推測されること、制御システムはその重要性から狙う価値が高い（身代金の支払いが見込める）と見なされること、産業用IoT（Industrial Internet of Things：IIoT）の普及に伴い制御システムにつながるIoT機器の増加が見込まれること等から、制御システムに対するランサムウェアの脅威はますます高まると推測される。事業者は可能な限りウイルス対策を行うとともに、重要なデータのバックアップが適切にされているかを確認し、備えを固めることが望まれる。

(b) 情報機関からの高度なハッキングツールの流出

2017年3月、機密告発サイトWikiLeaksが、米中央情報局（CIA：Central Intelligence Agency）が保有していたゼロデイを含む脆弱性や高度なハッキングツール等の機密情報（約9,000ドキュメント）を公開した※188。4月には、ハッカーグループShadow Brokersが、米国家安全保障局（NSA：National Security Agency）が保有していた同様の情報（約300MB）を公開した。流出した脆弱性の多くは公開前にベンダによって修正されていたが、直後に世界的な大感染を引き起こしたランサムウェアWanna Cryptorの拡散には、NSAからの流出情報が利用されたとも言われる※189。他のハッカーやサイバー犯罪者が同様に流出情報を悪用することが予想され、今後出現するウイルスや攻撃の高度化が懸念される。

(c) 内部関係者の過失によるウイルス感染

複数のセキュリティベンダが、事業者が認識している脅威、及び実際のインシデントの原因となった脅威について調査した結果によれば、数字の差及び順位の差はあるものの、「マルウェア／ランサムウェア」「内部脅威（過失）」「外部脅威（APT（Advanced Persistent Threat：標的型攻撃）及び破壊工作を含む）」が共通して上位に挙げられた※190。中でも、マルウェア（ウイルス）と内部関係者による過失は、実際の脅威に関してもそれぞれ1位（53%）と3位（29%）であった※186。マルウェア（ウイルス）の感染経路の1位はインターネットであった（最新の2017年上半期のデータで20.4%）。これは、社内のITネットワークからの感染拡大や、制御システム内に運用上インターネットにアクセスする機器が存在すること、メンテナンス時に内部関係者が持ち込んだパソコンを制御システムにつなぐこと等が原因と考えられる。感染経路の2位は外部記憶媒体であった（同データで9.6%）※183。ウイルス感染の大きな要因の一つは、内部関係者の過失（接続機器や媒体のウイルス対策不足）である可能性が高い。

調査で言及されているマルウェア（ウイルス）は、特に

制御システムを狙ったものではなく汎用的なウイルスだが、ランサムウェアを始め、重要なファイルやハードディスクを消去する破壊型ウイルスや、コンピュータのリソースを盗用しパフォーマンスを低下させる仮想通貨マイニングウイルス等、制御システムの運用に影響を及ぼす可能性のある汎用ウイルスは多くある。事業者は、制御システムに外部から持ち込んだ機器を接続する運用がある場合、改めてこうしたリスクを想定して対策を見直すことが望ましい。

3.4.3 海外の制御システムセキュリティの取り組み

2017年は主に米欧において、政府による電力システムのセキュリティテストの実施を検討する法案の提出や、より臨場感のあるサイバー演習の実施のほか、民間によるサイバー攻撃やハッキングに関する調査研究も多数発表された。

(1) セキュリティ強化の取り組み

米国では2017年1月、上院議会に「Securing Energy Infrastructure Act」が提出された。同法案では、エネルギー分野の制御システムのサイバー攻撃への脆弱性をテストする、連邦レベルのパイロットプログラムの設置が提案された※191。また10月には、下院議会に「Grid Cybersecurity Research and Development Act」が提出された。同法案は、電力システムのサイバーセキュリティ対策強化を目的に、既存の産業制御プロトコルの脆弱性の調査やセキュアな産業制御プロトコルの開発、セキュリティ対策を導入するコストの低減方法の立案等を提起し、セキュリティ向上の促進を図っている※192。

電力システムや軍事システムへの大規模サイバー攻撃を想定したサイバー演習も各国で実施されたが、2017年10月にスウェーデンで実施された、石炭火力発電所の制御システムを模したサイバー演習は、臨場感に富んでいた。技術的・シナリオ的に高度であっただけでなく、模擬攻撃者によって実際に水浸しにされた設備の復旧にゴム長靴を履いてあたる等、スウェーデン国内の3ヵ所の原子力発電所から参加した担当者に、サイバー攻撃による物理的被害をリアルに実感させた※193。

(2) セキュリティ調査研究(ペネトレーションテスト)

制御システムのセキュリティに関する調査研究では、ペネトレーションテストが報告された。

7月にラスベガスで開催されたBlack Hatでは、米国タルサ大学の研究者らが、米国中部及び西海岸の五つの集合型風力発電所のペネトレーションテストの結果を紹介した。研究者らはフィールドに設置された風力タービンのタワーの物理錠をピッキングして建物内部に侵入し、持ち込んだ通信機能を持つコンピュータをシステムに接続した。その後、タワーの外部からネットワーク経由で風力タービンを停止させたり、攻撃を検知されないよう監視システムに偽のデータを送信したりした。研究者らは、「制御監視システムは認証やネットワークセグメントの分割等の対策が施されておらず、侵入したタービンだけでなくネットワークに接続されたすべてのタービンの停止を始め、様々な攻撃が実行可能であった」と報告している※194。

11月に米国バージニア州で開催されたCyberSat Summitでは、DHSが2016年に実施したボーイング757型機のペネトレーションテストについて公表した。マサチューセッツ工科大学、パシフィック・ノースウェスト国立研究所、カリフォルニア大学サンディエゴ校、SRI International等が参加したセキュリティ専門家チームが、無線通信を介して2日で航空機システムへの侵入に成功したと報告している。現在運用中の航空機のほとんどは、製造年代的にサイバーセキュリティを考慮して設計されていない。航空機の通信の脆弱性は数年前から報告されているが、航空機のアップデートはテストに時間と費用がかかるため、航空機システムの多くのコンポーネントはアップデートされておらず※195、脆弱性への対応が課題となっている。

(3) セキュリティ調査研究(ウイルス)

制御システムを狙ったウイルスの調査研究は、実際にインシデントで使われたウイルスの解析から新たなウイルスのデモまで、幅広く発表された。

2017年2月のRSA Conference 2017では、ジョージア工科大学の研究者らが、浄水施設へのランサムウェア攻撃のデモを発表した。デモでは、バルブの不正操作、塩素レベルの改ざん、測定データの改ざん等が可能であることを示し、攻撃者が制御システムを「人質」として脅迫を行う日が来ると警告した※196。

同じく2月に開催されたNetwork and Distributed System Security Symposium 2017では、ニュージャージー州立大学、フロリダ国際大学、及びダルムシュタット工科大学の研究者らが、プログラマブルコントローラ(Programmable Logic Controller:PLC)※197のルートキット「Harvey」を発表した。HarveyはPLCのファームウェアに潜み、フィールド機器に送られる制御コマンド

や、フィールド機器から送られたセンサー値等を改ざんする。発表者らは実際的なテストベッドで検証を行い、実環境でも同様な攻撃の可能性があるとしている※198。

また、2月には、インドの International Institute of Information Technology の研究者らが、PLC に仕掛ける「ラダーロジック※199 爆弾（Ladder Logic Bomb：LLB）」を発表した。発表者は、PLC 製品をテストした結果、ファームウェアは更新時に署名により真正性が保証される一方で、ラダーロジックは保護されないことを発見し、オペレータに気付かれずにシステムをシャットダウンしたり、センサー値やコマンドを改ざんしたりする LLB を作成してみせた※200。

更に2月には、ジョージア工科大学の研究者らが、PLC ランサムウェア「LogicLocker」を発表した。LogicLocker は認証に関する既知の脆弱性が存在する2機種の PLC を探し、感染すると正規のユーザをロックアウトし、プログラムを人や機器を危険に晒すような不正なラダーロジックに差し替える。研究者らがインターネット接続機器検索サービス「Shodan※201」で該当する2機種を検索したところ1,400台が見つかったと報告しており、現実的な脅威が示唆されている※202。

4月には、イスラエルの制御システムセキュリティベンダが、PLC ランサムウェア「ClearEnergy」を発表した。ClearEnergy は幅広いモデルの PLC に感染させることが可能で、同社が発見した脆弱性 CVE-2017-6032（認証回避）及び CVE-2017-6034（セキュア設計の原則に反した設計）を悪用する。標的ネットワークへの侵入後は、脆弱な PLC を探し、可能ならラダーロジックを窃取して外部サーバに送信を試み、最後に発見したすべての PLC のラダーロジックを1時間後に消去するプログラムをセットする※203。

6月には、スロバキアのセキュリティベンダと米国の制御システムセキュリティベンダが、2016年のウクライナの電力システムへの攻撃に使われたと見られるウイルス「Industroyer/CrashOverride」の解析結果を発表した。このウイルスは、複数の制御システムの標準プロトコルに対応し、変電所の遮断器を直接操作できる機能等を持っている等、Stuxnet を始めとするこれまでの制御システムを狙ったウイルスを進化させたものとなっている。今後出現する制御システムウイルスも同様に高度化されると推測される※204。

3.4.4 国内の制御システムセキュリティへの取り組み

国内においても制御システムのセキュリティ確保は、ますます重要な課題となっている。政府は、2017年4月に発表した「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※205（以下、第4次行動計画）において、重要インフラサービスを提供する制御システムのセキュリティ向上のための施策を示している（第4次行動計画の内容については「2.1.1（2）重要インフラの情報セキュリティ対策強化」参照）。

本項では、第4次行動計画で掲げられている「リスクアセスメントの浸透」を支援するため、IPA が2017年10月に公開した「制御システムのセキュリティリスク分析ガイド※206」（以下、ガイド）に示されたリスク分析のアプローチを紹介する。また、後半で、国内における制御システム関連のセキュリティ評価認証制度の活用状況について述べる。

（1）制御システムのセキュリティリスク分析

セキュリティ対策において、リスク分析の重要性は様々な基準やガイドラインで取り上げられている。リスク分析により、以下を実現することが可能となる。

①実効的なセキュリティ強化策とリスク低減効果の定量的な把握
②効率的なセキュリティ投資戦略の策定
③リスク分析結果に基づく継続的なセキュリティの維持向上（PDCA サイクルの実現）

しかし、以下の課題から、リスク分析は充分に浸透していない。

- リスク分析の具体的な方法論や手順が分からない。
- 従来のリスク分析は膨大な工数を要することが多い。

本ガイドは、この二つの課題に応えるため、IPA が培ってきた知見を活かし※207、工数に配慮したリスク分析の具体的手順を示したものであり、以下の構成となっている。

1章　セキュリティ対策におけるリスク分析の位置付け
2章　リスク分析の全体像と作業手順
3章　リスク分析のための事前準備
4章　リスク分析の実施
　4.1節　資産ベースのリスク分析
　4.2節　事業被害ベースのリスク分析
5章　リスク分析結果の解釈と活用法
6章　セキュリティテスト

7 章　特定セキュリティ対策に対する追加基準

以下に、実際のリスク分析の実施方法を解説した 3 章、4 章、5 章の概要とポイントを示す。

(a)リスク分析のための事前準備(ガイド 3 章)

3 章では、実際にリスク分析を始める前に把握するべきこと、決めておくべきことを挙げ、その手順を解説している。

3.1 節で行うシステム構成とデータフローの明確化は、リスク分析中で最も重要な作業の一つとなる。ガイドでは、既存のネットワーク図やシステム構成図を基にリスク分析の対象範囲を検討し、機器の設置場所や機能によるグループ化等を通じ、リスク分析用にモデル化したシステム構成図を作成するための手順や留意事項を解説している。

3.2 節から 3.5 節では、リスク分析で用いる評価指標「資産の重要度」「事業被害」「脅威」「脆弱性」の定義と各評価指標の判断基準の考え方について記している。表 3-4-2 に、評価指標の概要を示す。各評価指標について具体的な検討例を提供しており、検討例をカスタマイズすることで、事業者はより自組織に沿った判断基準を作成可能である。

「資産の重要度」及び「事業被害」の判断基準は各事業者が決める必要があるため、判断基準の検討のポイントとして、「CIA」(C:機密性、I:完全性、A:可用性)及び「HSE」(H:健康、S:安全性、E:環境への影響)を踏まえた考え方を紹介している。一方、リスク分析において想定する基本的な脅威、及びセキュリティ対策候補は事業者によらず共通であるため、一覧として提供している。共通の用語と定義により、社内の各部門及び社外の関係者が、同じ認識で議論を行うことが可能となる。

(b)資産ベースのリスク分析(ガイド 4.1 節)

4.1 節では、資産ベースのリスク分析の手順を解説している。資産ベースのリスク分析は、保護すべき制御システムを構成する各資産に対して、その資産の重要度、想定される脅威、その脅威に対する脆弱性、の三つを評価指標として、各資産のリスクを分析する。これにより、資産に対して網羅的に脅威と対策状況を評価することができる。

資産ベースのリスク分析では、各資産の攻撃者視点による攻撃用途を明確化する。攻撃用途とは、実際の

評価指標		指標の意味	ガイドで提供している検討例 (各事業者で定義または例をカスタマイズ)
脅威 (資産ベース・ 事業被害ベース共通)	脅威	想定される脅威(攻撃手法)	「資産に対する脅威(攻撃手法)」 「資産(通信経路)に対する脅威(攻撃手法)」
	脅威レベル	脅威が発生する可能性の評価点	―
	判断基準	脅威レベルの判断基準	「脅威レベルの判断基準の定義例」
脆弱性 (資産ベース・ 事業被害ベース共通)	脆弱性	脅威に対する脆さ。セキュリティ対策の実施状況で判断	「セキュリティ対策項目一覧」
	脆弱性レベル (対策レベル)	脆弱性レベル:脅威を受け入れてしまう可能性の評価点(対策レベル:脅威を防止できる可能性の評価点で、脆弱性レベルの裏返しの値となる e.g. 脆弱性レベル=3 → 対策レベル=1)	―
	判断基準	脆弱性レベル(対策レベル)の判断基準	「脆弱性レベルと対策レベルの定義(評価点と判断基準)」
資産の重要度 (資産ベース)	資産の重要度	何をもってその資産を重要とするか	「CIA 要件及び HSE 要件を考慮した資産の重要度の評価例」
	資産の重要度 (レベル)	資産の価値、事業被害及び事情継続への影響から見た評価点	―
	判断基準	資産の重要度の判断基準	「資産の重要度の判断基準の定義例」
事業被害 (事業被害ベース)	事業被害	自組織にとっての事業被害は何か	「事業被害の定義例」
	事業被害レベル	事業上の被害や経営上の打撃の大きさの評価点	―
	判断基準	事業被害レベルの判断基準	「事業被害レベルの判断基準の定義例」

※レベルはそれぞれ「1:低」～「3:高」で評価

■表 3-4-2　ガイドにおけるリスク分析で用いている評価指標

攻撃の際に当該資産を用いる用途を表し、「侵入口」「経由」「攻撃拠点」「攻撃対象」に分類される。表 3-4-3 に、攻撃用途の概要を示す。

攻撃用途	説明
侵入口	攻撃者がサイバー攻撃を行う際に侵入する入口。
経由	侵入した攻撃者が攻撃拠点、もしくは攻撃対象に到達するまでに経由する装置等。
攻撃拠点	攻撃対象に対して攻撃を実行する（コマンド等を送信する）ことが可能な装置等。攻撃拠点と攻撃対象となる装置が同一になる場合もある。
攻撃対象	攻撃が行われ、破壊、情報窃取、改ざん等が行われる装置等。

■表 3-4-3　攻撃者視点による資産の攻撃用途

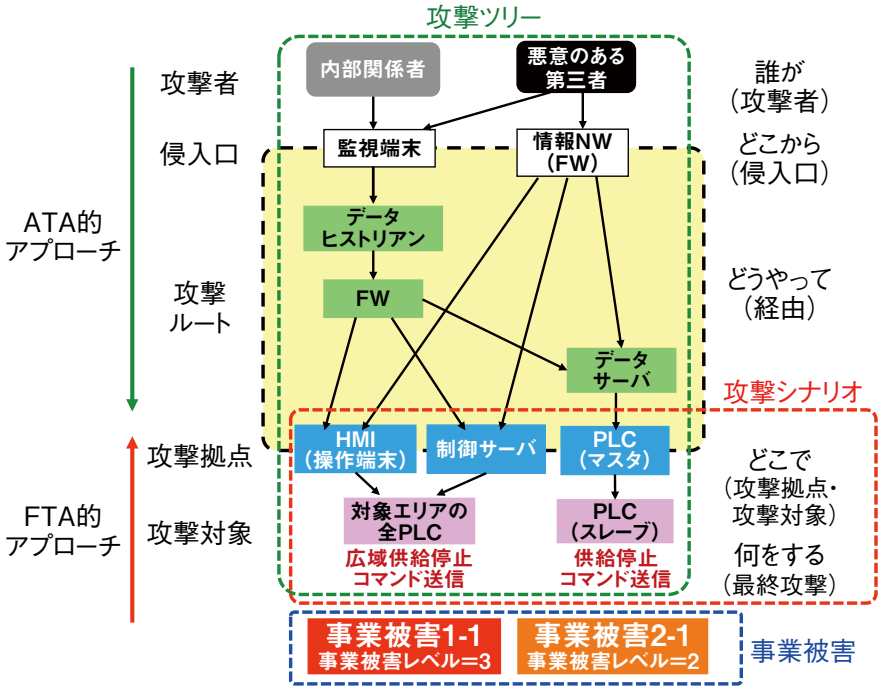
ガイドでは、攻撃用途と脅威（攻撃手法）の対応表、及び脅威（攻撃手法）と対策候補の対応表を提供しており、各資産の攻撃用途を明確化することで、より重要な脅威（攻撃手法）が分析でき、より実効的なリスク分析を可能にしている。

(c) 事業被害ベースのリスク分析（ガイド 4.2 節）

4.2 節は、事業被害ベースのリスク分析の手順を解説している。事業被害ベースのリスク分析は、保護すべきシステムが実現する事業やサービスに対して、回避したい事業被害を定義し、その事業被害を引き起こす可能性のある攻撃のシナリオ（ガイドでは「攻撃シナリオ※208」と呼称）、そのシナリオを実現するための侵入から目的遂行までの一連の攻撃手順（ガイドでは「攻撃ツリー※209」と呼称）を洗い出す。そして、各攻撃ツリーによる事業被害、脅威（攻撃ツリーが発生する可能性）、脆弱性の三つを評価指標として、各攻撃ツリーのリスクを分析する。机上でのペネトレーションテストに相当し、資産ベースのリスク分析だけでは検証できない、事業被害に直結する攻撃のリスクを評価することができる。

事業被害ベースのリスク分析では、事故分析の手法であるフォルトツリー解析（Fault Tree Analysis：FTA※210）の「被害を起点に、事の起こり（上流）に向かって考え得る可能性を網羅的に検討できる」という利点と、セキュリティ分析の手法である攻撃ツリー解析（Attack Tree Analysis：ATA※211）の「攻撃者視点で、侵入口を起点に、被害の発生（下流）に向かって考え得る可能性を網羅的に検討できる」という利点を融合させ、ともすれば際限なく分岐するツリーの中で、両者がつながるツリーを検討することで効率化を図っている。図 3-4-1 に、事業被害ベースのリスク分析における、事業被害、攻撃シナリオ、攻撃ツリーの関係を表した模式図を示す。

それでも攻撃ツリーの数は、システム構成の複雑さ（侵入口の多さ、侵入口から攻撃拠点までの攻撃経路（ガイドでは「攻撃ルート※212」と呼称）の複雑さ）等によって、膨大になる可能性がある。ガイドでは、「深刻な被害に絞る」「可能性の高い攻撃シナリオに絞る」「危険性の高



■図 3-4-1　事業被害、攻撃シナリオ、攻撃ツリーの関係

い攻撃ルートに絞る」等、実際にリスク分析を行う攻撃ツリーを絞り込む観点を紹介し、リスク分析の負荷低減を図っている。

(d)リスク分析結果の解釈と活用法(ガイド 5 章)

リスク分析の目的はリスクの把握ではなく、把握したリスクを検証し、許容できないリスクに対して低減策(改善策)を実施してセキュリティを向上させることである。5 章では、資産ベース、及び事業被害ベースのリスク分析により算定されたリスク値を、どのようにとらえ、セキュリティ強化につなげていくか、その考え方と手順について解説している。

基本的には、リスク値が高い資産及び攻撃ツリーを中心に改善箇所を選定し、リスクの低減を図る。しかし、制御システムにおいては、例えリスクが高くても、それらのリスクをすべて低減するのは可用性(システムを停止できない等)、信頼性(対策を実装した場合の信頼性をベンダが保証していない等)、コスト(費用がかかる等)、技術(OS のアップグレードやセキュリティ機能の搭載ができない、適切なセキュリティソリューションが存在しない等)の問題から、現実には非常に困難である場合が多い。この場合、資産ベースと事業被害ベースのリスク分析の両方の結果を活用し、「リスク値の高い攻撃ツリー上のどの資産のどの脅威への対策を強化することがリスク低減に有効か」を検討することで最適解が得られやすい。リスク値が高いが対策が困難であったり、対策に高いコストが発生する資産があっても、攻撃ルートの上流にある資産で対策を行ったり、ルート上にセキュリティ機器を新たに設置したりすること等で、リスクを低減できる可能性がある。ガイドでは、改善箇所の選択のアプローチ、対策の優先度の考え方を、具体例を用いて示している。

また、机上のリスク分析では把握できない事実(関係者の知らない機器やネットワーク接続が存在した、対策していたつもりが実際にはできていなかった等)から発生するリスクを確認するため、リスク分析の結果をセキュリティテストの検討材料として活用する方法についても述べている。リスクの高低にかかわらず、最重要な資産/攻撃ツリー/攻撃ルートにおいて、机上のリスク分析だけでは把握できないリスクの見逃しが万が一にも許されない場合、実施箇所を絞ったピンポイントなセキュリティテストの実施を検討するという選択肢もある。

本ガイドは、事業者が自身でリスク分析を実施する際の参考とするほか、外注する場合の発注要件や要件の検討に活用することも可能である。

(2)セキュリティ評価認証制度の運用状況

日本では、制御システムセキュリティの国際標準である IEC 62443 を基に、制御システムで使用される制御機器のセキュリティ、及び制御システムを運用する組織のセキュリティマネジメントシステムの評価認証制度が、2014 年に開始されている。

制御機器のセキュリティ評価は、米国の ISA Security Compliance Institute(ISCI)が運営する「EDSA(Embedded Device Security Assurance)認証」を活用し、技術研究組合制御システムセキュリティセンター(Control System Security Center:CSSC)が国内における EDSA 認証制度を立ち上げ、評価を実施している※213。

制御システム運用組織のセキュリティマネジメントシステムの評価は、一般財団法人日本情報経済社会推進協会(JIPDEC)が「サイバーセキュリティマネジメントシステム(Cyber Security Management System:CSMS)認証制度」を運用している※214(表 3-4-4)。

経済産業省の「平成 28 年度 IoT 推進のための社会

	EDSA 認証	CSMS 認証
評価対象	制御機器	セキュリティマネジメントシステム
規格	ISCI EDSA 認証規格(IEC 62443-4-1、IEC 62443-4-2 に準拠)	IEC 62443-2-1
想定される認証取得者	制御機器ベンダ	制御システム運用組織(制御システムの保有事業者、構築事業者、運用・保守事業者)
認証制度の運用開始	2014 年	2014 年
認証の有効期限	無期限	通常 1 年ごとにサーベイランス審査 3 年ごとに再認証
認証機関	第三者認証機関 (CSSC 認証ラボラトリー(CSSC-CL))	第三者認証機関(BSI グループジャパン株式会社等)
認定機関	公益財団法人日本適合性認定協会(JAB)	一般財団法人日本情報経済社会推進協会(JIPDEC)

■表 3-4-4　制御システムのセキュリティ評価認証制度

システム推進事業（スマート工場実証事業）」では、セキュリティ確保のための対策例として、「通信及びデータの暗号化」「相互認証」等と併せて、「EDSA 認証を取得した IoT 製品の選択」が挙げられている※215。IIoT の普及が進み、制御システム環境に接続される IIoT 機器がもたらすリスクが指摘される中、制御機器だけでなく IIoT についてもセキュリティの確保が重要となっている。国や都道府県が所管するスマート化事業の調達要件に、セキュリティ認定製品の使用等を加えることによって、IIoT 機器のセキュリティ対策を促進し、セキュリティ認証制度の普及、及び制御システム全体のセキュリティ確保につながることが期待される。

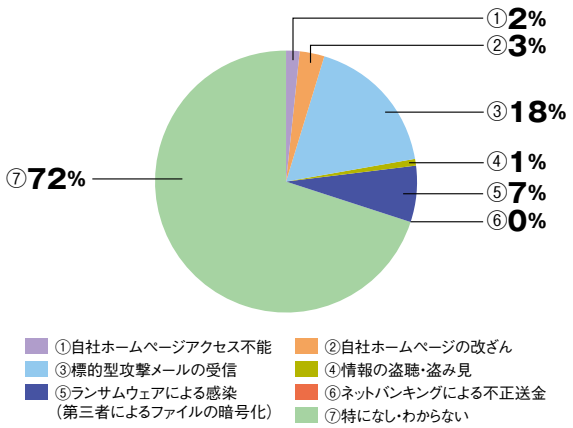
3.5 中小企業における情報セキュリティ

中小企業は、国内の企業数の 99.7%、雇用者数の約 7 割を占め、日本経済の根幹を支えている※216。本節では、中小企業における情報セキュリティの現状を述べる。

3.5.1 中小企業における情報セキュリティ対策の実態

大阪商工会議所が 2017 年 6 月に公開した「中小企業におけるサイバー攻撃対策に関するアンケート調査結果※217」によると、「電子メール」(95%)や「ホームページ」(87%)、「ネットバンキング」(66%) 等、多くの中小企業が IT を利活用している。一方サイバー攻撃対策としては、「アンチウイルスソフトの導入」(78%)、「ファイアーウオールや UTM の導入」(56%)、「データ等へのパスワード設定」(37%)、「民間企業が実施するセキュリティーサービス」(37%) 等が実施されているが、現在実施しているセキュリティ対策で「十分でないと思っている」企業が 68%であった。その理由としては、「情報セキュリティーに経費がかけられない」が 60%、次いで「専門人材がいないのでわからない」が 48%であった。中小企業のセキュリティ対策の実施状況は、セキュリティ対策の費用や専門人材の確保に問題があり、IT 利活用の進展と比べて遅れていると言える。

また、中小企業が受けたサイバー攻撃としては、「標的型攻撃メールの受信」が 18%、「ランサムウェアによる感染」が 7%、「自社ホームページの改ざん」が 3%等となっており (図 3-5-1)、合計すると約 3 割の中小企業が何らかのサイバー攻撃を受けている。ただし、ファイアウォールや UTM(Unified Threat Management：統合型脅威管理) の導入が 56%にとどまっているという調査結果から、サイバー攻撃を受けていること自体を認識できていない中小企業も相当数存在すると推測される。



■図 3-5-1　中小企業が受けたサイバー攻撃(n=315、複数回答可)
(出典)大阪商工会議所「『中小企業向けサイバー攻撃対策支援事業の開始』ならびに『中小企業におけるサイバー攻撃対策に関するアンケート調査結果』について※217」を基に IPA が作成

IPA が 2017 年 7 月に公開した「中小企業における情報セキュリティ対策の実態調査－事例集－※218」では、中小企業における情報セキュリティの取り組み事例が 68 例掲載されており、うち 32 例は事故事例である。以下に、掲載された事故事例の一部を示す。

- 従業員が不審なメールの添付ファイルを不用意に開き、ウイルス感染した。基幹システムの設定が書き換わる障害が発生し、復旧するまでの 1 週間程、基幹システムの一部が使用できなくなった(静岡県・製造業)。
- オフライン運用していた Windows XP パソコンを不注意でネットワーク接続したところ、Web サイトの閲覧を通じてランサムウェアに感染し、ファイルが暗号化された。幸いバックアップファイルからデータを復元できたため被害は最小限で済んだ(新潟県・製造業)。

事故事例からは、企業規模や業種、地域的な偏りなくサイバー攻撃等による事故が発生していることが分かる。また、ソフトウェアは最新の状態で利用する、セキュリティソフトを導入して定義ファイルを更新する、といった基本的な対策を怠ったためサイバー攻撃の被害にあった事例も多く、中小企業においてもサイバー攻撃を自分のこととととらえて基本的な対策から確実に実施することが望まれる。

事例集には、以下のように、情報セキュリティ対策への取り組みが経営にプラスの効果を発揮した事例も掲載されている。

- 大手企業やコンプライアンス意識の高い組織と取り引きを行う場合、社内の管理体制についての情報提供を求められることがある。当社の情報セキュリティ対策を含めた管理体制は、取引先から評価され、安定した取り引きにつながっている(徳島県・農林水産業)。
- セキュリティ認証取得が業務の見直しのきっかけとなり、業務が全体的に効率化され、残業時間が減る等の効果が出ている。クリアデスクポリシーの徹底、書類等の置き場所のルール化等も業務の効率化に影響している。また、セキュリティ認証取得後は作業の意義、

予想されるリスク、必要な記録は何かを従業員が考える習慣がつき、訪問記録や報告書の品質向上に結びついている（香川県・情報通信業）。

このような事例から、情報セキュリティ対策に積極的に取り組む中小企業が存在すること、取り組みが取引先からの評価や業務の改善等にプラスの効果を発揮したことが確認できる。事故事例とともに中小企業が情報セキュリティ対策に取り組む際の参考としていただきたい。

3.5.2 中小企業の情報セキュリティ対策支援の取り組み

中小企業の情報セキュリティ対策支援の取り組みとして2017年に活動が始まったSECURITY ACTIONと都道府県警察と自治体の連携による対策推進の取り組みについて概要を述べる。

(1) SECURITY ACTIONの取り組み

2017年2月、IPAと中小企業支援機関、士業団体、IT関連団体等の10団体は、中小企業におけるITの利活用拡大に向け、中小企業における情報セキュリティへの意識啓発及び自発的な対策の策定、実践を促進するため、連携して活動することを共同宣言した※219。本宣言における「自発的な情報セキュリティ対策を促す」ための核となる取り組みとして、IPAは2017年4月、中小企業が自ら取り組みを宣言する制度「SECURITY ACTION※220」を創設し、共同宣言参加団体とともに中小企業に参加を呼びかける活動を展開している。

SECURITY ACTIONとは、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度である。IPAが公開している「中小企業の情報セキュリティ対策ガイドライン※221」の実践をベースに、2段階の取組目標を設定している。

第1段階では、上記ガイドラインの付録「情報セキュリティ5か条」に取り組むことを宣言することで、宣言企業であることを示す一つ星のロゴマークを使用できる。第2段階では、同ガイドラインの付録「5分でできる!情報セキュリティ自社診断」で自社の状況を把握した上で、「情報セキュリティポリシー（基本方針）」を定め、外部に公開したことを宣言することで、ステップアップした二つ星のロゴマークを使用できる※222（図3-5-2）。

ロゴマークは、自社のWebサイトや名刺等に表示することができ、情報セキュリティに自ら取り組んでいることを取引先等へアピールすることが可能である。また、従業員のセキュリティ意識の向上にも有用と考えられる。

SECURITY ACTIONは、政府が2017年度補正予算として措置した経済産業省の「サービス等生産性向上IT導入支援事業」（通称：IT導入補助金）の申請要件となった※223。2018年4月末時点の宣言企業数は636社であるが、同補助金は13万5,000社への交付が見込まれており※224、中小企業へのIT利活用の拡大とあわせて同制度が広く普及していくことが見込まれる。

■図3-5-2　一つ星（左）と二つ星（右）のロゴマーク

(2) 都道府県警察と自治体の連携による対策推進

地域における中小企業の情報セキュリティ対策支援の取り組みとして、都道府県警察と自治体を中心とした情報セキュリティ対策支援が進んでいる。IPA調べによると2018年3月末時点で、北海道、秋田県、山形県、宮城県、福島県、茨城県、群馬県、埼玉県、東京都、千葉県、静岡県、新潟県、石川県、岐阜県、愛知県、滋賀県、京都府、大阪府、兵庫県、鳥取県、島根県、山口県、香川県、高知県、福岡県、長崎県、大分県、沖縄県の28の都道府県において、産学官連携の協議会等の枠組みを構築する等により、中小企業のサイバーセキュリティ対策の推進に向けた取り組みを実施している。

具体例としては、2017年7月、群馬県警察と群馬県、中小企業支援機関、学術機関等の10団体で構成される「群馬県中小企業等サイバーセキュリティ支援連絡会」が設立された※225。また同年7月、北海道警察と国、自治体、中小企業支援機関等の12団体で構成される「北海道中小企業サイバーセキュリティ支援ネットワーク（略称:Cyber-道net）」が設立された。Cyber-道netでは、情報共有、情報発信、共同対処支援、相談及び技術的支援要請への対応等の活動を通じて、道内の中小企業のサイバーセキュリティ対策を支援している※226。

3.5.3 中小企業のための情報セキュリティ対策支援ツール

公的機関等が提供する中小企業における情報セキュリティ対策の水準向上の支援ツールについて述べる。

これらの支援ツールは無償で入手・利用できる。中小企業は、適宜支援ツールを参照し、それぞれの業務においてセキュリティの強化を図っていただきたい。

(1) 中小企業の情報セキュリティ対策ガイドライン

IPA では、情報セキュリティ対策の考え方や実践方法について解説した「中小企業の情報セキュリティ対策ガイドライン第 2.1 版※221」を提供している(図 3-5-3)。

同ガイドラインの第 1 部「経営者編」では、経営者が認識すべき「3 原則」、経営者がやらなければならない「重要 7 項目の取組」を挙げて解説している。これは、経済産業省が企業の経営層向けに公開している「サイバーセキュリティ経営ガイドライン」の内容を中小企業向けにコンパクトにしたものと言える。第 2 部「管理実践編」では、情報セキュリティ対策の具体的な進め方や実施、改善について手順を分かりやすく解説している。「中小企業の情報セキュリティ対策ガイドライン」に掲載され、多くの中小企業で活用されている「5 分でできる!情報セキュリティ自社診断」も昨今の脅威や攻撃の変化、IT 環境の変化に合わせて改訂が行われている。また、自社のセキュリティポリシーを策定する際にすぐに役立つひな形や情報資産管理台帳のサンプルを付録としてデータ提供している。

■図 3-5-3　中小企業の情報セキュリティ対策ガイドライン第 2.1 版

(2) 情報セキュリティ対策支援サイト

IPA では、中小企業における情報セキュリティ対策を支援するためのポータルサイト「情報セキュリティ対策支援サイト※227」を提供している(図 3-5-4)。

本サイトでは、25 の診断項目に答えるだけで情報セキュリティの対策状況を把握することができる診断ツール「5 分でできる!情報セキュリティ自社診断」、従業員が情報セキュリティ対策を e-Learning 形式で学習できるツール「5 分でできる!情報セキュリティポイント学習」、IPA が作成・公開している様々な情報セキュリティに関する資料やツールを利用者自身の属性(企業経営者、従業員、一般、企業向け啓発者等)と、利用目的(知りたい、学びたい、始めたい、続けたい)を条件に検索できるツール「中小企業向けセキュリティ資料提供」等の機能を提供している(「付録」の「ツール 1 情報セキュリティ対策支援サイト」参照)。

■図 3-5-4　情報セキュリティ対策支援サイトのトップページ

(3) 中小企業向けサイバーセキュリティ対策の極意

東京都産業労働局では、都内の中小企業を対象にサイバーセキュリティに関する初心者向けの内容を網羅したガイドブック「中小企業向けサイバーセキュリティ対策の極意※228」を制作し、中小企業支援機関を通じて都内の中小企業への配布も実施している。冊子では、実際に発生したサイバー攻撃のケーススタディを始め、経営者の備えやサイバー攻撃対策のシミュレーションを掲載する等、企業における対策マニュアルの役割を果たしている。本資料は東京都産業労働局の Web サイト上でも公開されている(図 3-5-5)。

(4) 企業と組織のネットトラブル対応マニュアル

鳥取県サイバーセキュリティ対策ネットワークでは、中小企業のパソコンでネットトラブルが発生したとき、まず何をすればよいのかを解説した「企業と組織のネットトラブル対応マニュアル※229」を提供している(図 3-5-6)。

情報セキュリティ対策に関する社内の意識調査を行う

■図 3-5-5　中小企業向けサイバーセキュリティ対策の極意
（出典）東京都産業労働局「中小企業向けサイバーセキュリティ対策の極意」

ための「情報セキュリティ対策チェックシート」、内部不正・営業秘密漏えい対策の基本的な対策状況を確認するための「内部不正・営業秘密漏えい対策チェックシート」、鳥取県内企業を対象とした「情報セキュリティに関するアンケート調査結果」等を多彩なイラストを用いて分かりやすく解説している。

■図 3-5-6　企業と組織のネットトラブル対応マニュアル
（出典）鳥取県サイバーセキュリティ対策ネットワーク「企業と組織のネットトラブル対応マニュアル」

(5) 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き

JNSA では、中小企業を対象とした情報セキュリティ対策の手引き書「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き[※230]」を提供している。

第 1 部では、中小企業に行ってほしいセキュリティ境界と入退室管理、クラウドサービスの利用、障害・事故管理等、21 の管理項目について管理策を解説している。第 2 部では、中小企業で行う業務を大きく、「出社」「社内業務」「社外業務」「退社」「帰宅」「システム管理業務」に分け、各業務に潜むセキュリティ上の脆弱性により発生し得るリスクに対応した情報セキュリティ対策を、技術的な対策と人的な対策に分けて解説している。

COLUMN

情報セキュリティ監査に向いている人

ここ数年、中央官庁、独立行政法人、地方自治体等の公的機関や、電力等の重要インフラ事業者、クラウド事業者が、各セグメントにおけるセキュリティ対策の基準を明確化したことから、それらの基準を満たしているかどうかをチェックするための情報セキュリティ監査が注目されています。そんな中、「情報セキュリティ監査を頼みたいんだけど、どのような会社に頼んだら良いの?」という質問を受けることがあります。経済産業省では、監査を受けたい企業や団体が、どこに監査を依頼したらよいかという選定の目安として、一定の情報を開示することを定めた任意登録制の「情報セキュリティ監査企業台帳」を運用しています。2017年度の情報セキュリティ監査企業台帳には、約180社の情報セキュリティ監査企業が登録されていて、監査主体が得意な監査対象の分野、監査従事者が保有する資格、前年度の監査実績等が一覧できます。2018年度からは、情報セキュリティ監査を含む情報セキュリティサービスについて一定の品質の維持向上が図られていることを第三者が客観的に判断し、その結果を台帳等で取りまとめて公開する情報セキュリティサービス審査登録制度が開始されました。

情報セキュリティ監査の需要が高まるのに伴い、「情報セキュリティ監査を実施する人」、すなわち「情報セキュリティ監査人」の需要も高まっています。特定非営利活動法人日本セキュリティ監査協会(JASA)は、「公認情報セキュリティ監査人(CAIS)資格制度」を運用しており、2018年4月の時点で、主任監査人54名、監査人157名、監査人補575名、監査アソシエイト384名が登録されています。2017年度からは情報処理安全確保支援士等の高度情報セキュリティ資格保有者に対する優遇制度も開始され、注目されています。しかし、全国に3万人弱いると言われている公認会計士と比較するとかなり少ない人数です。情報セキュリティ監査を受けるのが当たり前という時代がいつ来るかは別として、情報セキュリティ監査人がもっと増えないとそのような状況には到達できません。

それでは、どんな人が情報セキュリティ監査人に向いているのでしょうか。監査人に求められる力量は、「資質」「能力」「知識」という切り口で語られることが多いと思いますが、ここでは「資質」についてのみ考察します。まず、「①学ぶことが好きな人」。情報セキュリティ監査はセキュリティのみならず監査をする相手の業務、法制度等について常に最新の知識が求められるため、監査業務をやりつつ勉強することが大切で、勉強が好きでない人には向きません。次に、「②(ちょっと)天邪鬼な人」。監査と言うと真面目な人というイメージがあるかもしれませんが、ものごとの裏に潜む本質を見極めるためには健全なる猜疑心を持つことが必要で、何事も疑ってかかるぐらいの(ちょっと)ひねくれた人の方が監査人に向きます。また、監査の場合、相手に対して過度に忖度してもいけません。「No!」とはっきり言えることが大切です。そして、「③ストレスを上手く処理できる人」。監査の発見事項の合意プロセスでは、相手とタフな交渉を要求される場面もあり、かなりのストレスが溜まります。プライベートも含めて、それらのストレスを上手く処理して、監査の活力に変えられる人が監査に向くと思います。

当てはまる方!　あなたも情報セキュリティ監査人を目指しませんか?

※1 「マルウェア」等の用語が使われ、読者を混乱させる可能性があるため、本白書では特に断りのない限り、また文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※2 IPA：情報セキュリティ 10 大脅威 2017 https://www.ipa.go.jp/files/000058504.pdf〔参照 2018-05-01〕
※3 Rapidity Networks：Hajime：Analysis of a decentralized internet worm for IoT devices https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf〔参照 2018-05-01〕
※4 C&C サーバ :Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等（ここでは IoT 機器）に対し、遠隔から命令を送り制御するサーバ。
※5 Symantec Corporation：Hajime worm battles Mirai for control of the Internet of Things https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things〔参照 2018-05-01〕
※6 Kaspersky Lab：Hajime, the mysterious evolving botnet https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/〔参照 2018-05-01〕
※7 Radware Ltd.：Hajime Botnet - Friend or Foe? https://security.radware.com/ddos-threats-attacks/hajime-iot-botnet/〔参照 2018-05-01〕
※8 株式会社インターネットイニシアティブ：Hajime ボットの観測状況 https://sect.iij.ad.jp/d/2017/09/293589.html〔参照 2018-05-01〕
※9 Radware Ltd.：”BrickerBot” Results In PDoS Attack https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/〔参照 2018-05-01〕
※10 Radware Ltd.：BrickerBot PDoS Attack: Back With A Vengeance https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/〔参照 2018-05-01〕
※11 Bleeping Computer：BrickerBot Author Claims He Bricked Two Million Devices https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/〔参照 2018-05-01〕
※12 Bleeping Computer：US ISP Goes Down as Two Malware Families Go to War Over Its Modems https://www.bleepingcomputer.com/news/security/us-isp-goes-down-as-two-malware-families-go-to-war-over-its-modems/〔参照 2018-05-01〕
※13 Bleeping Computer：BrickerBot Dev Claims Cyber-Attack That Affected Over 60,000 Indian Modems https://www.bleepingcomputer.com/news/security/brickerbot-dev-claims-cyber-attack-that-affected-over-60-000-indian-modems/〔参照 2018-05-01〕
※14 Bleeping Computer：BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/〔参照 2018-05-01〕
※15 Trend Micro Incorporated：Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/〔参照 2018-05-01〕
※16 JVN iPedia：JVNDB-2017-002241 Foscam などのホワイトラベルの IP カメラモデルで使用されるカスタムビルドされた GoAhead Web サーバにおける設定ファイルを公開される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002241.html〔参照 2018-06-01〕
※17 Trend Micro Incorporated：The Reigning King of IP Camera Botnets and its Challengers https://blog.trendmicro.com/trendlabs-security-intelligence/reigning-king-ip-camera-botnets-challengers/〔参照 2018-05-01〕
※18 Check Point Software Technologies LTD.：A New IoT Botnet Storm is Coming https://research.checkpoint.com/new-iot-botnet-storm-coming/〔参照 2018-05-01〕
※19-1 Radware Ltd.：Why the World is Under the Spell of IoT_Reaper https://blog.radware.com/security/2017/10/iot_reaper-botnet/〔参照 2018-05-01〕
※19-2 JVN iPedia：JVNDB-2017-003612 Wireless IP Camera WIFICAM デバイスにおける認可・権限・アクセス制御に関する脆弱性 http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-003612.html〔参照 2018-05-01〕
※20 Qihoo 360 Technology Co.,Ltd：IoT_reaper: A Rappid Spreading New IoT Botnet http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/〔参照 2018-05-01〕
※21 s3cur1ty：Multiple Vulnerabilities in D'Link DIR-600 and DIR-300 (rev B) http://www.s3cur1ty.de/m1adv2013-003〔参照 2018-05-01〕
※22 IT Security Research by Pierre：Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html〔参照 2018-05-01〕
※23 SecuriTeam Secure Disclosure：SSD Advisory – Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution https://blogs.securiteam.com/index.php/archives/3409〔参照 2018-05-01〕
※24 SecuriTeam Secure Disclosure：SSD Advisory - Vacron NVR Remote Command Execution https://blogs.securiteam.com/index.php/archives/3445〔参照 2018-05-01〕
※25 SecuriTeam Secure Disclosure：SSD Advisory - D-Link 850L Multiple Vulnerabilities (Hack2Win Contest) https://blogs.securiteam.com/index.php/archives/3364〔参照 2018-05-01〕
※26 s3cur1ty：Multiple Vulnerabilities in Linksys E1500/E2500 http://www.s3cur1ty.de/m1adv2013-004〔参照 2018-05-01〕
※27 Insecure.Org：Unauthenticated command execution on Netgear DGN devices http://seclists.org/bugtraq/2013/Jun/8〔参照 2018-05-01〕
※28 Pen Test Partners：Pwning CCTV cameras https://www.pentestpartners.com/security-blog/pwning-cctv-cameras/〔参照 2018-05-01〕
※29 Qihoo 360 Technology Co.,Ltd：Early Warning: A New Mirai Variant is Spreading Quickly on Port 23 and 2323 http://blog.netlab.360.com/early-warning-a-new-mirai-variant-is-spreading-quickly-on-port-23-and-2323-en/〔参照 2018-05-01〕
※30 JVN iPedia：JVNDB-2017-006833 ZyXEL PK5001Z デバイスにおける証明書・パスワードの管理に関する脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-006833.html〔参照 2018-05-01〕
※31 Trend Micro Incorporated：New Mirai Attack Attempts Detected in South America and North African Countries https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-attack-attempts-detected-south-america-north-african-countries/〔参照 2018-05-01〕
※32 株式会社インターネットイニシアティブ：国内における Mirai 亜種の感染急増 (2017 年 11 月の観測状況) https://sect.iij.ad.jp/d/2017/12/074702.html〔参照 2018-05-01〕
※33 Qihoo 360 Technology Co.,Ltd：Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869 http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/〔参照 2018-05-01〕
※34 JVN iPedia：JVNDB-2014-008039 Realtek SDK の miniigd SOAP サービスにおける任意のコードを実行される脆弱性 http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-008039.html〔参照 2018-05-01〕
※35 Check Point Software Technologies LTD.：Huawei Home Routers in Botnet Recruitment https://research.checkpoint.com/good-zero-day-skiddie〔参照 2018-05-01〕
※36 International Business Machines Corporation：Mirai IoT Botnet: Mining for Bitcoins? https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/〔参照 2018-05-01〕
※37 トレンドマイクロ株式会社：サイバー犯罪者の狙いは「仮想通貨」に拡大、2017 年第 3 四半期の脅威動向を分析 https://blog.trendmicro.co.jp/archives/16533〔参照 2018-05-01〕
※38 BB ソフトサービス株式会社：11 月度 IoT サイバー脅威分析リポート https://www.onlinesecurity.jp/iotsec_reports/2017/201712.html〔参照 2018-05-01〕
※39 警察庁：脆弱性が存在するルータを標的とした宛先ポート 52869/TCP に対するアクセス及び日本国内からの Telnet による探索を実施するアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/201712191.pdf〔参照 2018-05-01〕
※40 NICT：NICTER 観測レポート ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19) http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf〔参照 2018-05-01〕
※41 JPCERT/CC：Mirai 亜種の感染活動に関する注意喚起 https://www.jpcert.or.jp/at/2017/at170049.html〔参照 2018-05-01〕
※42 ロジテック株式会社：ロジテック製 300Mbps 無線 LAN ブロードバンドルータおよびセットモデル（全 11 モデル）に関する重要なお知らせとお願い http://www.logitec.co.jp/info/2017/1219.html〔参照 2018-05-01〕
※43 僕とネットショッピング：中国製ネットワークカメラが勝手に動き出して中国語が聞こえてきた怖い話（動画あり） http://hardshopper.hatenablog.com/entry/networkcamera〔参照 2018-05-01〕
※44 僕とネットショッピング：中国製ネットワークカメラの取材でテレビから口止めされてた話 http://hardshopper.hatenablog.com/entry/nsta

〔参照 2018-05-01〕
※ 45 僕とネットショッピング：【お詫び】中国製ネットワークカメラの記事に大きな誤りがあった話　http://hardshopper.hatenablog.com/entry/2017/08/16/022801〔参照 2018-05-01〕
※ 46 黒林檎のお部屋：「中華ウェブカメラ」のセキュリティについて　http://r00tapple.hatenablog.com/entry/2017/08/12/050252〔参照 2018-05-01〕
※ 47 黒林檎のお部屋：IoT 診断入門（続）　http://r00tapple.hatenablog.com/entry/2017/08/10/180852〔参照 2018-05-01〕
※ 48 https://bbss.co.jp/business/service/pdf/YNU-BBSS_IoTSecPJReport.pdf〔参照 2018-05-01〕
※ 49 Security Affairs：UK police arrested the alleged mastermind of the MIRAI attack on Deutsche Telekom　https://securityaffairs.co/wordpress/56604/cyber-crime/mirai-attack-deutsche-telekom.html〔参照 2018-05-01〕
※ 50 The Guardian：Briton admits to cyber-attack on Deutsche Telekom　https://www.theguardian.com/world/2017/jul/21/briton-admits-to-cyber-attack-on-deutsche-telekom-court〔参照 2018-05-01〕
※ 51 Krebs on Security：Who is the GovRAT Author and Mirai Botmaster 'Bestbuy'？　https://krebsonsecurity.com/2017/07/who-is-the-govrat-author-and-mirai-botmaster-bestbuy/〔参照 2018-05-01〕
※ 52 Krebs on Security：Suspended Sentence for Mirai Botmaster Daniel Kaye　https://krebsonsecurity.com/2017/07/suspended-sentence-for-mirai-botmaster-daniel-kaye/〔参照 2018-05-01〕
※ 53 Krebs on Security：Who is Anna-Senpai, the Mirai Worm Author?　https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/〔参照 2018-05-01〕
※ 54 New Jersey On-Line LLC.：FBI questions Rutgers student about massive cyber attack　https://www.nj.com/news/index.ssf/2017/01/rutgers_student_questioned_cyber_attack.html〔参照 2018-05-01〕
※ 55 U.S. Department of Justice：Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks　https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving〔参照 2018-05-01〕
※ 56 New Jersey On-Line LLC.：Former Rutgers student admits to creating code that crashed internet　https://www.nj.com/education/2017/12/rutgers_student_charged_in_series_of_cyber_attacks.html〔参照 2018-05-01〕
※ 57 Krebs On Security：Mirai IoT Botnet Co-Authors Plead Guilty　https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/〔参照 2018-05-01〕
※ 58 IPA：利用時の品質の観点を盛り込んだ「つながる世界の開発指針（第 2 版）」を発行　https://www.ipa.go.jp/sec/reports/20170630.html〔参照 2018-05-01〕
※ 59 IPA：「IoT 開発におけるセキュリティ設定の手引き」を公開　https://www.ipa.go.jp/security/iot/iotguide.html〔参照 2018-05-01〕
※ 60 IPA：ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト　https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html〔参照 2018-05-01〕
※ 61 IPA：IoT 製品・サービス脆弱性対応ガイド　https://www.ipa.go.jp/security/fy29/reports/vuln_handling/index.html#L3〔参照 2018-05-01〕
※ 62 https://www.cloudsecurityalliance.jp〔参照 2018-05-01〕
※ 63 https://www.ccds.or.jp〔参照 2018-05-01〕
※ 64 http://www.jnsa.org〔参照 2018-05-01〕
※ 65 http://www.ssaj.or.jp〔参照 2018-05-01〕
※ 66 OWASP：IoT Vulnerabilities Project　https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Vulnerabilities〔参照 2018-05-01〕
※ 67 GSMA：GSMA IoT Security Guidelines & Assessment　https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/〔参照 2018-05-01〕
※ 68 GSMA：IoT Security Assessment　https://www.gsma.com/iot/iot-security-assessment/〔参照 2018-05-01〕
※ 69 OTA:Internet of Things　https://otalliance.org/IoT〔参照 2018-05-01〕
※ 70 OTA：IoT - Industry Resources　https://otalliance.org/resources/iot-industry-resources〔参照 2018-05-01〕
※ 71 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot〔参照 2018-05-01〕
※ 72 総務省：「IoT セキュリティ総合対策」の公表　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html〔参照 2018-05-01〕
※ 73 総務省：サイバーセキュリティタスクフォース　http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html〔参照 2018-05-01〕
※ 74 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　http://www.soumu.go.jp/main_sosiki/kenkyu/smooth_internet/index.html〔参照 2018-05-01〕
※ 75 日経 xTECH：サイバー攻撃をプロバイダーは止められるか、総務省の意欲　http://itpro.nikkeibp.co.jp/atcl/column/14/346926/110101186/〔参照 2018-05-01〕
※ 76 総務省：新規制定・改正法令・告示　法律　http://www.soumu.go.jp/menu_hourei/s_houritsu.html〔参照 2018-07-02〕
※ 77 一般社団法人セキュア IoT プラットフォーム協議会：協議会が発足、IoT システムの次世代セキュリティ標準の策定を開始　http://www.secureiotplatform.org/press/release/2017-04-03/〔参照 2018-05-01〕
※ 78 一般社団法人セキュア IoT プラットフォーム協議会：IoT デバイス製造時でのセキュリティ標準の整備を開始　http://www.secureiotplatform.org/press/release/2017-04-13/〔参照 2018-05-01〕
※ 79 一般社団法人セキュア IoT プラットフォーム協議会：IoT セキュリティにおけるリスクの整理や仕様に関する検討を開始　https://www.secureiotplatform.org/press/release/2017-10-18/〔参照 2018-05-01〕
※ 80 JCBA：一般社団法人日本仮想通貨事業者協会　年頭所感　https://cryptocurrency-association.org/news/main-info/%e4%b8%80%e8%88%ac%e7%a4%be%e5%9b%a3%e6%b3%95%e4%ba%ba%e6%97%a5%e6%9c%ac%e4%bb%ae%e6%83%b3%e9%80%9a%e8%b2%a8%e4%ba%8b%e6%a5%ad%e8%80%85%e5%8d%94%e4%bc%9a%e3%80%80%e5%b9%b4%e9%a0%ad%e6%89%80%e6%84%9f/〔参照 2018-05-01〕
※ 81 WIRED：仮想通貨「テザー」の疑惑が本当なら、市場が崩壊するかもしれない - 信頼性を損なう"事件"が続発　https://wired.jp/2018/01/31/tethers-collapse/〔参照 2018-05-01〕
※ 82 日本経済新聞：ビットコイン、相次ぐ分裂　新通貨が乱立　https://www.nikkei.com/article/DGXMZO24384680X01C17A2EA2000/?n_cid=SPTMG002〔参照 2018-05-01〕
※ 83 CNET Japan：ビットコインに訪れた"成長痛"--8 月 1 日に予期される「フォーク」とは　https://japan.cnet.com/article/35104451/〔参照 2018-05-01〕
※ 84 マイニング:仮想通貨移転のトランザクションの正しさを検証し、ブロックに追記することをマイニングと呼ぶ。マイニングを行う人（マイナー:採掘者）には報酬として仮想通貨が支払われる。
※ 85 ビットコインシステムでは、偶然複数の者が同時にマイニングに成功する等の事情により、複数のブロックが並列に追加され、一時的にブロックチェーンが分岐することが起きる。この場合、一定時間後に一番長く連なるブロックチェーンのみが採用し、それ以外のブロックチェーンは破棄される。ブロックチェーンに取り込まれなかった取り引きトランザクションを参照した取引群は、二重取り引きとして無効となる恐れがある。
※ 86 経済産業省：平成 27 年度　我が国経済社会の情報化・サービス化に係る基礎整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書　http://www.meti.go.jp/press/2016/04/20160428003/20160428003-2.pdf〔参照 2018-05-01〕
※ 87 厳密には、51 パーセント攻撃の可能性がある以上、どれだけブロックの連なりが後続したとしても、ある取り引きトランザクションが無効となる可能性はゼロにはならない。
※ 88 Segwit（Segregated Witness）：取り引きトランザクションに含まれている署名データを別管理することで、取り引きトランザクションデータを小さくする案。
※ 89 JBA：ビットコインの動向に関する当協会の見解　http://jba-web.jp/archives/20170722bitcoin_statement〔参照 2018-05-01〕
※ 90 「リプレイアタック」と呼ばれる。
※ 91 JCBA：8 月 1 日に予期されるビットコイン分岐危機に向けた対応について　https://cryptocurrency-association.org/news/main-info/8%e6%9c%881%e6%97%a5%e3%81%ab%e4%ba%88%e6%9c%9f%e3%81%95%e3%82%8c%e3%82%8b%e3%83%93%e3%83%83%e3%83%88%e3%82%b3%e3%82%a4%e3%83%b3%e5%88%86%e5%b2%90%e5%8d%b1%e6%a9%9f%e3%81%ab%e5%90%91%e3%81%91%e3%81%9f/〔参照 2018-05-01〕
※ 92 JCBA：計画されたハードフォークおよび新コインへの対応指針の公表について（お知らせ）　https://cryptocurrency-association.org/cms2017/wp-content/uploads/2017/11/ec9b32ad9b04357f6c4a65fa502e28fe.pdf〔参照 2018-05-01〕
※ 93 Yahoo Japan ニュース：仮想通貨の 2018 年、熱狂に次ぐ幻滅の先に光明はあるか　https://news.yahoo.co.jp/byline/kusunokimas

anori/20180104-00080086/〔参照 2018-05-01〕
※ 94 日本経済新聞：ビットコインゴールド、付与は 11 月 1 日以降 https://www.nikkei.com/article/DGXMZO22644920U7A021C1EE9000/〔参照 2018-05-01〕
※ 95 Proof of Work（PoW）：一般には計算機サービスの要求者に、ある計算負荷を課してサービス乱用を抑止する手段を指す。ビットコイン等の仮想通貨では、ブロックを生成したいマイナーに対し、PoW としてブロックの特殊なハッシュ値を作る計算負荷を課す。最初に計算に成功したマイナーがブロック生成を承認される（コンセンサスアルゴリズム）。
※ 96 PoW の実施は、マイニング専用コンピュータ等を用意するための投資額の差や、マイニングの際のコスト（電気料金等）の差等の事情により、マイナーは特定勢力に独占されている。有力マイナー同士の共謀も問題となっている。
※ 97 https://cryptocurrency-association.org/list/〔参照 2018-05-01〕
※ 98 日本経済新聞：コインチェック、NEM 保有 26 万人に返金へ 460 億円 https://www.nikkei.com/article/DGXMZO26241420Y8A120C1MM8000/〔参照 2018-05-01〕
※ 99 日本経済新聞：不審通信、数週間前から NEM 流出 ウイルスが発端か https://www.nikkei.com/article/DGKKZO27977750R10C18A3CC1000/〔参照 2018-05-01〕
※ 100 コールドウォレット：取り引きトランザクションの形成からブロックチェーンへの記録までをオフラインで行うシステム。
※ 101 マルチシグネチャ：秘密鍵情報を複数の者でなければ利用できないようにするシステム。ある秘密鍵情報が窃取されても、他のそれが適切に権利者の元で保有されている限り、権利者の意に反する取り引きを阻止できる。
※ 102 日経 xTECH：コインチェックに業務改善命令、MTGOX の教訓が生かされなかった理由 http://tech.nikkeibp.co.jp/it/atcl/column/14/346926/012901289/?P=2〔参照 2018-05-01〕
※ 103 BUSINESS INSIDER JAPAN：[コインチェック流出] その技術的ミスを NEM 財団 VP が語る 公式インタビュー全文翻訳 https://www.businessinsider.jp/post-161098〔参照 2018-05-01〕
※ 104 金融庁・関東財務局：コインチェック株式会社に対する行政処分について http://kantou.mof.go.jp/rizai/pagekthp0130000001_00013.html〔参照 2018-05-01〕
※ 105 金融庁：コインチェック株式会社に対する立入検査の着手及び仮想通貨交換業者に対する報告徴求命令の発出について https://www.fsa.go.jp/policy/virtual_currency/09.pdf〔参照 2018-05-01〕
※ 106 金融庁：平成 29 年 4 月から、「仮想通貨」に関する新しい制度が始まります http://www.fsa.go.jp/common/about/20170403.pdf〔参照 2018-05-01〕
※ 107 HD ウォレット：HMAC（Keyed-Hash-Message Authenticaition Code）を利用した、決定論的ウォレット。一つの seed から複数の公開鍵と秘密鍵の生成が可能。一つの seed を管理することで、多数ある顧客の秘密鍵情報を一元管理できる。一方、seed 情報が窃取されれば、それに紐づく多数の秘密鍵情報も窃取されたに等しい。
※ 108 テックビューロ株式会社：1 月 6 日から 7 日未明にかけて発生した API キーの不正利用、および 1 月 9 日に報告された不正アクセスおよび不正出金に関するご報告 https://corp.zaif.jp/info/8265/〔参照 2018-05-01〕
※ 109 日本経済新聞：仮想通貨イーサリアム、トラブルで 200 億円以上が凍結中 https://www.nikkei.com/article/DGXMZO23337890Q7A111C1000000/〔参照 2018-05-01〕
※ 110 Neowin LLC.：Ledger wallets could let hackers steal your money https://www.neowin.net/news/ledger-wallets-could-let-hackers-steal-your-money〔参照 2018-05-01〕
※ 111 日本経済新聞：仮想通貨業界、4 月に新団体発足 ICO 基準など整備 https://www.nikkei.com/article/DGXMZO27626090S8A300C1EA1000/〔参照 2018-05-01〕
※ 112 finte：破綻するリスクがない取引所?分散型取引所（DEX）とは? https://www.enigma.co.jp/media/dex/〔参照 2018-05-01〕
※ 113 2017 年 7 月、取引所「BTC-E」の管理人が、麻薬売買等の不法収益を含む 40 億ドルをマネーロンダリングしたとして逮捕された。同取引所では本人確認が徹底されていなかったとされる。（The New York Times：Bitcoin Exchange Was a Nexus of Crime, Indictment Says https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html〔参照 2018-05-01〕）
また、2018 年 4 月、日本国内の取引所「ビットフライヤー」が、本人確認を終えていない顧客の通貨売買を可能にしていることが判明した。（日本経済新聞：仮想通貨、本人確認前に売買も 悪用のリスク https://www.nikkei.com/article/DGXMZO29289910S8A410C1MM0000/〔参照 2018-05-01〕）
※ 114 ゼロ知識証明を利用し、取引経過を一切明らかにしない「Zcash」、リング署名技術により、誰が電子署名したかを匿名化する「Monero」、coinjoin 技術によって送金元アドレスをブロックチェーンに記録しない取り引きを実現する「DASH」がある。いずれも、我が国の登録業者では扱われていない仮想通貨である。
※ 115 日本経済新聞：流出 NEM ほぼ全額交換 https://www.nikkei.com/article/DGKKZO28443600S8A320C1CR8000/〔参照 2018-05-01〕
※ 116 金融庁は、2018 年 3 月、香港に所在する無登録事業者「Binance」に対し、警告を発した。（金融庁：無登録で仮想通貨交換業を行う者について（Binance） https://www.fsa.go.jp/policy/virtual_currency02/Binance_keikokushilyo.pdf〔参照 2018-05-01〕）
※ 117 金融庁：「仮想通貨交換業等に関する研究会」の設置について https://www.fsa.go.jp/news/30/singi/20180308.html〔参照 2018-05-01〕
※ 118 日本銀行：Project Stella 日本銀行・欧州中央銀行による分散型台帳技術に関する共同調査 https://www.boj.or.jp/announcements/release_2017/data/rel170906a3.pdf〔参照 2018-05-01〕
※ 119 株式会社三菱 UFJ フィナンシャル・グループ：MUFG が CEATEC JAPAN 2017 にて“MUFG コイン”を初展示 https://innovation.mufg.jp/detail/id=213〔参照 2018-05-01〕
※ 120 CnetJapan：Ripple の技術を使った銀行間送金アプリ「Money Tap」--コンソーシアムは 61 行が参加 https://japan.cnet.com/article/35115750/〔参照 2018-05-01〕
※ 121 前記日銀の調査では、取り引きトランザクションの真正性を検証する CA（Certification Authority：認証局）が設置されており、CA が停止している間、新たな取り引きが行えなくなる等、単一障害点の問題が報告されている。
※ 122 金融庁：金融審議会「金融制度スタディグループ」（第 1 回）議事次第 https://www.fsa.go.jp/singi/singi_kinyu/seido-sg/siryou/seido_sg1.html〔参照 2018-05-01〕
※ 123 金融庁：ICO（Initial Coin Offering）について～利用者及び事業者に対する注意喚起～ http://www.fsa.go.jp/policy/virtual_currency/06.pdf〔参照 2018-05-01〕
※ 124 日本経済新聞：ツイッターも仮想通貨の広告禁止 https://www.nikkei.com/article/DGXMZO28616340X20C18A3000000/〔参照 2018-05-01〕
※ 125 JCBA：イニシャル・コンオファリグへの対応について（お知らせ） https://cryptocurrency-association.org/cms2017/wp-content/uploads/2017/12/20171208_01.pdf〔参照 2018-05-01〕
※ 126 日本経済新聞：流出した仮想通貨「NEM」、他コインに交換か https://www.nikkei.com/article/DGXMZO26503380T00C18A2EA4000/〔参照 2018-05-01〕
※ 127 Tavitt (Thailand) Co.,Ltd.：ニュース一覧 金融庁、日本居住者は ICO 購入不可と伝える http://tavitt.co.jp/2018/03/07_347/〔参照 2018-05-01〕
※ 128 2017 年 10 月、仮想通貨リップル取り引きをめぐり、実質的に破たん状態であったにもかかわらず、顧客から現金を預かったとして、リップルトレードジャパン（RTJ）の代表者が詐欺罪で逮捕された。（産経ニュース：仮想通貨「リップル」めぐる詐欺事件 取引所代表の 31 歳男逮捕 大筋で容疑認める http://www.sankei.com/affairs/news/171018/afr1710180020-n1.html〔参照 2018-05-01〕）
※ 129 インターネットコム：ビットコイン、大手取引所「bitFlyer」にサイバー攻撃―5 時間にわたり影響 https://internetcom.jp/203437/bitflyer-ddos〔参照 2018-05-01〕
※ 130 Chosun Online：中国朝鮮族、ハッキングで得た個人情報でビットコイン盗む http://www.chosunonline.com/m/svc/article.html?contid=2018011100963〔参照 2018-05-01〕
※ 131 Google AdWords を悪用したフィッシングリンクを利用し、被害者から秘密鍵情報を窃取した事例が報告されている。（Cisco Systems, Inc.：COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style http://blog.talosintelligence.com/2018/02/coinhoarder.html〔参照 2018-05-01〕）
※ 132 マイクロペイメントチャネル：主に、二者間での継続的取り引きを念頭に、中途の取引過程をブロックチェーンの外で管理し、必要な取り引きトランザクションだけをブロックチェーンに記録することで、少額かつ迅速な決済の実現を目指す技術。
※ 133 ライトニングネットワーク：ペイメントチャネルを多数の者で構築し、迅速かつ少額な決済の実現を目指す技術。
※ 134 Tangle：取引当事者自身が他の取り引きの承認を行う仕組み。ブロックは一つのチェーンではなく、有向非巡回グラフ「DAG（Directed Acyclic Graph）」を形成する点に特徴がある。取引当事者以外のマイナーが不要となり、手数料が不要となる。（IOTA Japanese Fan Site：IOTA White paper ver.1.4.1 の日本語訳 https://iotafan.jp/wp/iota-wp-jp/〔参照 2018-05-01〕）
※ 135 IPA：安心相談窓口だより ウイルス感染したという警告でアプリのインストールを誘導する手口が急増 https://www.ipa.go.jp/security/

anshin/mgdayori20160711.html〔参照 2018-05-01〕
※ 136 INTERNET Watch：スマホのブラウザーに突然ウイルス感染メッセージが! ネット広告経由で拡散する偽警告に注意 https://internet.watch.impress.co.jp/docs/news/1091916.html〔参照 2018-05-01〕
※ 137 http://www2.sagawa-exp.co.jp/whatsnew/detail/721/〔参照 2018-05-01〕
※ 138 https://www.rakuten-card.co.jp/guide/securityinfo/〔参照 2018-05-01〕
※ 139 トレンドマイクロ株式会社：実例で学ぶネットの危険：「通知 お客様宛にお荷物のお届きました」 http://blog.trendmicro.co.jp/archives/16787〔参照 2018-05-01〕
※ 140 佐川急便株式会社：佐川急便を装った迷惑メールにご注意ください http://www2.sagawa-exp.co.jp/whatsnew/detail/721/〔参照 2018-05-01〕
楽天カード株式会社：フィッシングの被害からお客様を守るために https://www.rakuten-card.co.jp/guide/securityinfo/〔参照 2018-05-01〕
※ 141 Kaspersky Lab：まさに「ホット」なトロイの木馬：Loapi https://blog.kaspersky.co.jp/loapi-trojan/19061/〔参照 2018-05-01〕
※ 142 IPA：安心相談窓口だより iPhone ユーザを狙った不正アプリによるセクストーション被害が発生 https://www.ipa.go.jp/security/anshin/mgdayori20161110.html〔参照 2018-05-01〕
※ 143 警察庁・文部科学省：夏休みを迎える君たちへ〜ネットには危険もいっぱい〜 http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/27/1386963_1_1.pdf〔参照 2018-05-01〕
※ 144 IPA：安心相談窓口だより 主に中高生を対象としたセクストーション被害に関する注意喚起 https://www.ipa.go.jp/security/anshin/mgdayori20170810.html〔参照 2018-05-01〕
※ 145 IPA：「2017 年度情報セキュリティに対する意識調査」報告書について https://www.ipa.go.jp/security/fy29/reports/ishiki/index.html〔参照 2018-05-01〕
※ 146 産経 WEST：スマホの監視アプリで女子大生を隠し撮り 疑いで会社員再逮捕 http://www.sankei.com/west/news/170608/wst1706080088-n1.html〔参照 2018-05-01〕
※ 147 産経ニュース：「俺の元カノと一緒にいるだろ」…交際女性のスマホを遠隔アプリで監視疑い 33歳男を逮捕 http://www.sankei.com/affairs/news/171129/afr1711290050-n1.html〔参照 2018-05-01〕
※ 148 トレンドマイクロ株式会社：未成年者がランサムウェアを作る時代、日本初の逮捕事例を読み解く http://blog.trendmicro.co.jp/archives/15133〔参照 2018-05-01〕
※ 149 トレンドマイクロ株式会社：iOS 上で大量のアイコンを作成する不正プロファイル 「YJSNPI ウイルス」こと「iXintpwn」を解説 http://blog.trendmicro.co.jp/archives/16007〔参照 2018-05-01〕
※ 150 脱獄（Jail Break）：端末保護の目的で施されている制限を取り除き、開発者が意図しない方法でソフトウェアを動作できるようにすること。
※ 151 トレンドマイクロ株式会社：Android 向け不正アプリ「ZNIU」を配布していたアプリストアで iOS の不正プロファイル「iXintpwn」の新しい亜種を確認 http://blog.trendmicro.co.jp/archives/16343〔参照 2018-05-01〕
※ 152 Check Point Software Technologies Ltd.：FalseGuide misleads users on GooglePlay https://blog.checkpoint.com/2017/04/24/falaseguide-misleads-users-googleplay/〔参照 2018-05-01〕
※ 153 ITmedia NEWS：Android 端末を踏み台にした DDoS 攻撃発生 Google Play に 300 本の不正アプリ http://www.itmedia.co.jp/news/articles/1708/29/news052.html〔参照 2018-05-01〕
※ 154 トレンドマイクロ株式会社：オンラインバンキングアプリを狙う「BankBot」を「Google Play」上で確認、国内銀行 7 行も対象 http://blog.trendmicro.co.jp/archives/15950〔参照 2018-05-01〕
※ 155 トレンドマイクロ株式会社：モバイル端末向け仮想通貨発掘マルウェア、Google Play で確認 http://blog.trendmicro.co.jp/archives/16293〔参照 2018-05-01〕
※ 156 ITmedia NEWS：話題の「Coinhive」とは? 仮想通貨の新たな可能性か、迷惑なマルウェアか http://www.itmedia.co.jp/news/articles/1710/11/news084.html〔参照 2018-05-01〕
※ 157 トレンドマイクロ株式会社：iOS 端末の不正／迷惑アプリ、「App Store」で確認。1 つはサードパーティアプリストアへ誘導 http://blog.trendmicro.co.jp/archives/14631〔参照 2018-05-01〕
※ 158 WIRED：Polish Teen Hacks His City's Trams, Chaos Ensues https://www.wired.com/2008/01/polish-teen-hac/〔参照2018-05-01〕
※ 159 The Register：Water treatment plant hacked, chemical mix changed for tap supplies http://www.theregister.co.uk/2016/03/24/water_utility_hacked/〔参照 2018-05-01〕
※ 160 シスコシステムズ合同会社：ウクライナにおける制御系システムへのサイバー攻撃 https://gblogs.cisco.com/jp/2016/03/syber-attack-in-ukraine/〔参照 2018-05-01〕
ITmedia エンタープライズ：停電の原因は産業制御システム狙うマルウェアか 「Stuxnet 以来、最大の脅威」 http://www.itmedia.co.jp/enterprise/articles/1706/13/news052.html〔参照 2018-05-01〕
※ 161 Ponemon Institute LLC：The State of Cybersecurity in the Oil & Gas Industry: United States https://siemensusa.newshq.businesswire.com/sites/siemensusa.newshq.businesswire.com/files/doc_library/file/Cyber_readiness_in_Oil__Gas_Final_4.pdf〔参照 2018-05-01〕
※ 162 Dark Reading：Ransomware Rising On The Plant Floor https://www.darkreading.com/endpoint/ransomware-rising-on-the-plant-floor/d/d-id/1327870?〔参照 2018-05-01〕
※ 163 Business Insider：Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants http://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5〔参照 2018-05-01〕
日経 xTECH：ホンダが工場など複数拠点で WannaCry 感染、一部の生産に影響 http://itpro.nikkeibp.co.jp/atcl/news/17/062101713/?rt=nocnt〔参照 2018-05-01〕
RS-NEWS：Honda Shuts Production As WannaCry Ransomware Cyber Attack Prevails https://www.researchsnipers.com/honda-shuts-production-wannacry-ransomware-cyber-attack-prevails/〔参照 2018-05-01〕
※ 164 BBC：How hackers are targeting the shipping industry https://www.bbc.com/news/technology-40685821〔参照 2018-05-01〕
Marine Electronics & Communications：Maritime industry moves from awareness to action on cyber security http://www.marinemec.com/news/view,maritime-industry-moves-from-awareness-to-action-on-cyber-security_48744.htm〔参照 2018-05-01〕
Bloomberg：Ransomware Cyberattack Goes Global https://www.bloomberg.com/news/articles/2017-06-28/cyberattack-reaches-asia-as-new-targets-hit-by-ransomware-demand〔参照 2018-05-01〕
※ 165 itnews：Maersk had to reinstall all IT systems after NotPetya infection https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815〔参照 2018-05-01〕
※ 166 安全計装システム（Safety Instrument System：SIS）：異常な状態を検知し、プラントを安全な状態に保つため、あるいは安全な状態に戻すため、自動的に作動し、様々な危険からプラントを保護する機能を提供するシステム。
※ 167 FireEye, Inc.：Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html〔参照 2018-05-01〕
Dark Reading: Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845〔参照 2018-05-01〕
The New York Times: A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.
https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html〔参照 2018-05-01〕
※ 168 Dark Reading：Ransomware Rising On The Plant Floor https://www.darkreading.com/endpoint/ransomware-rising-on-the-plant-floor/d/d-id/1327870〔参照 2018-05-01〕
※ 169 IT News：Ransomware disrupts Washington DC's CCTV system https://www.itnews.com/article/3162721/security/ransomware-disrupts-washington-dcs-cctv-system.html〔参照 2018-05-01〕
※ 170 Bleeping Computer：Man Hacks Jail Computer Network to Get Friend Released Early https://www.bleepingcomputer.com/news/security/man-hacks-jail-computer-network-to-get-friend-released-early/〔参照 2018-05-01〕
※ 171 TechNewsWorld：Hackers Blast Emergency Sirens in Dallas https://www.technewsworld.com/story/84447.html〔参照 2018-05-01〕
Ars Technica：Pirate radio: Signal spoof set off Dallas emergency sirens, not network hack https://arstechnica.com/information-technology/2017/04/dallas-siren-hack-used-radio-signals-to-spoof-alarm-says-city-manager/〔参照 2018-05-01〕
※ 172 ZDNet：WannaCry now claiming 159 traffic cameras in Victoria http://www.zdnet.com/article/wannacry-now-claiming-159-traffic-cameras-in-victoria/〔参照 2018-05-01〕
※ 173 BleepingComputer：DDoS Attacks Cause Train Delays Across

Sweden https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/〔参照 2018-05-01〕
※ 174 Kaspersky Lab：Threat Landscape for Industrial Automation Systems in H2 2017 https://ics-cert.kaspersky.com/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/#_Toc509229751〔参照 2018-05-01〕
※ 175 NCCIC：ICS-CERT Annual Vulnerability Coordination Report 2016 https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf〔参照 2018-05-01〕
※ 176 NCCIC/ICS-CERT：About Us https://ics-cert.us-cert.gov/about-us〔参照 2018-05-01〕
※ 177 SCADA（Supervisory Control and Data Acquisition）：主に、地理的に分散した制御対象を広域ネットワーク経由で遠隔集中監視するシステムを示す。制御機器を汎用パソコン上等で監視するためのソフトウェアを示す場合もある。
※ 178 バッファオーバーフローの脆弱性や、境界外の読み書き等、プログラムのクラッシュや任意のコード実行につながる可能性がある。
※ 179 Trend Micro Incorporated：Hacker Machine Interface: The State of SCADA HMI Vulnerabilities https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf〔参照 2018-05-01〕
※ 180 ZDNet：SCADA security: Bad app design could give hackers access to industrial control systems http://www.zdnet.com/article/scada-security-bad-app-design-could-give-hackers-access-to-industrial-control-systems/〔参照 2018-05-01〕
※ 181 トレンドマイクロ株式会社：WPA2 の脆弱性「KRACKs」、ほぼすべての Wi-Fi 通信可能な端末機器に影響 http://blog.trendmicro.co.jp/archives/16162〔参照 2018-05-01〕
Kaspersky Lab：The Relevance of WPA2 Vulnerabilities and KRACK Attacks to Industrial Systems https://ics-cert.kaspersky.com/reports/2017/11/15/the-relevance-of-wpa2-vulnerabilities-and-krack-attacks-to-industrial-systems/〔参照 2018-05-01〕
※ 182 シスコシステムズ合同会社：Meltdown と Spectre https://gblogs.cisco.com/jp/2018/01/meltdown-and-spectre/〔参照 2018-05-01〕
マカフィー株式会社：「Meltdown」と「Spectre」にまつわる噂を読み解く https://blogs.mcafee.jp/meltdown-spectre〔参照 2018-05-01〕
ICS-CERT：Alert (ICS-ALERT-18-011-01G) Meltdown and Spectre Vulnerabilities (Update G) https://ics-cert.us-cert.gov/alerts/ICS-ALERT-18-011-01〔参照 2018-05-01〕
※ 183 Kaspersky Lab：Threat Landscape for Industrial Automation Systems in H1 2017 https://ics-cert.kaspersky.com/reports/2017/09/28/threat-landscape-for-industrial-automation-systems-in-h1-2017/〔参照 2018-05-01〕
※ 184 BBC：How hackers are targeting the shipping industry http://www.bbc.com/news/technology-40685821〔参照 2018-05-01〕
※ 185 Fortune：Cyber Attack Strikes Airports, Banks, and Oil Giants in Russia and Ukraine http://fortune.com/2017/06/27/maersk-cyber-hack-russia/〔参照 2018-05-01〕
Reuters：German rail operator affected by global cyber attack https://www.reuters.com/article/us-cyber-attack-germany-rail/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM〔参照 2018-05-01〕
※ 186 The Business Advantage Group Limited.：The State of Industrial Cybersecurity 2017 https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf〔参照 2018-05-01〕
※ 187 SANS Institute：Securing Industrial Control Systems-2017 https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860/〔参照 2018-05-01〕
※ 188 The Register：That CIA exploit list in full: The good, the bad, and the very ugly https://www.theregister.co.uk/2017/03/08/cia_exploit_list_in_full/〔参照 2018-05-01〕
※ 189 Ars Technica：NSA-leaking Shadow Brokers just dumped its most damaging release yet https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/〔参照 2018-05-01〕
Bussiness Insider UK：The hackers that leaked NSA cyber-weapons say they will dump more data on on a monthly basis http://uk.businessinsider.com/wannacry-nsa-cyber-weapon-leakers-shadow-brokers-promise-monthly-data-dumps-2017-5〔参照 2018-05-01〕
※ 190 The Business Advantage Group Limited.：The State of Industrial Cybersecurity 2017 https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf〔参照 2018-05-01〕
SANS Institute：Securing Industrial Control Systems-2017 https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860/〔参照 2018-05-01〕
※ 191 The Hill：Lawmakers call for pilot program to test for energy sector vulnerabilities http://thehill.com/policy/cybersecurity/326191-lawmakers-push-for-pilot-program-to-test-for-energy-sector〔参照 2018-05-01〕
※ 192 U.S. Congress：H.R. 4120 https://www.congress.gov/115/bills/hr4120/BILLS-115hr4120ih.pdf〔参照 2018-05-01〕
※ 193 The Verge：Hacking nuclear systems is the ultimate cyber threat. Are we prepared? https://www.theverge.com/2018/1/23/16920062/hacking-nuclear-systems-cyberattack〔参照 2018-05-01〕
※ 194 PC Magazine：Wind Farms Are Not Ready for Ransomware http://uk.pcmag.com/news/90488/wind-farms-are-not-ready-for-ransomware〔参照 2018-05-01〕
WIRED：風力発電所のハッキングはあまりに簡単だった――米大学の侵入テストで判明 https://wired.jp/2017/08/30/wind-turbine-hack/〔参照 2018-05-01〕
※ 195 The Register：How can airlines stop hackers pwning planes over the air? And don't say 'regular patches' http://www.theregister.co.uk/2017/11/15/airplanes_vulnerable_rf_hacking/〔参照 2018-05-01〕
※ 196 Nextgov：Water Treatment Plant Hack Kicks Off RSA Conference http://www.nextgov.com/cybersecurity/2017/02/water-treatment-plant-hack-kicks-rsa-conference/135380/〔参照 2018-05-01〕
※ 197 プログラマブルロジックコントローラ（PLC）：センサー等の入力機器の信号（ON/OFF 等）に応じて、バルブアクチュエータ等の出力機器の ON/OFF を制御する制御装置。あらかじめ決められた条件（プログラム）に従い、機器を制御することができる。
※ 198 Network and Distributed System Security Symposium：Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/hey-my-malware-knows-physics-attacking-plcs-physical-model-aware-rootkit/〔参照 2018-05-01〕
Luis A. Garcia ほか：Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/ndss2017_08-1_Garcia_paper.pdf〔参照 2018-05-01〕
※ 199 ラダーロジック：論理回路を記述するための手法で、多くの PLC で採用されているプログラム言語。PLC を動かすためのプログラム。
※ 200 The Register：Researchers offer simple scheme to stop the next Stuxnet http://www.theregister.co.uk/2017/02/22/how_to_stop_the_next_stuxnet/〔参照 2018-05-01〕
※ 201 https://www.shodan.io/〔参照 2018-05-01〕
IPA：IPA テクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」 https://www.ipa.go.jp/security/technicalwatch/20160531.html〔参照 2018-05-01〕
※ 202 Tripwire, Inc.：New Proof-of-Concept Ransomware Can Target PLCs at Industrial Sites https://www.tripwire.com/state-of-security/latest-security-news/new-proof-concept-ransomware-can-target-plcs-industrial-sites/〔参照 2018-05-01〕
※ 203 Security Affairs：ClearEnergy ransomware aim to destroy process automation logics in critical infrastructure, SCADA and industrial control systems. http://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html〔参照 2018-05-01〕
※ 204 ESET North America：ESET discovers dangerous malware designed to disrupt industrial control systems https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-dangerous-malware-designed-to-disrupt-industrial-control-systems/〔参照 2018-05-01〕
Dragos, Inc.：CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations https://dragos.com/blog/crashoverride/CrashOverride-01.pdf〔参照 2018-05-01〕
※ 205 https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔参照 2018-05-01〕
※ 206 IPA：「制御システムのセキュリティリスク分析ガイド ～セキュリティ対策におけるリスク分析実施のススメ～」を公開 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔参照 2018-05-01〕
※ 207 経済産業省：平成 27 年度補正予算の概要（PR 資料） http://www.meti.go.jp/main/yosan/yosan_fy2015/hosei/pdf/pr_01.pdf〔参照 2018-05-01〕
※ 208 攻撃シナリオ：何がどうなったら／何をどうしたら、その事業被害が

起こるか、というシナリオ。
※ 209 攻撃ツリー：攻撃者視点で、誰が、どこから侵入し、どうやってシナリオを実行できる機器に到達し、どこで（シナリオを実行できる機器で）、何をするか、という一連の攻撃手順。
※ 210 フォルトツリー解析（Fault Tree Analysis：FTA）：シナリオベースのリスク分析手法における解析手法の一つ。被害（インシデント等）事象を起点として、その被害に至る 1 ステップ前の攻撃事象を順次追跡するツリー（フォルトツリー）を攻撃の原点までボトムアップに構成し、各ツリーの成立の可能性を算定する手法。
※ 211 攻撃ツリー解析（Attack Tree Analysis：ATA）：シナリオベースのリスク分析手法における解析手法の一つ。攻撃者視点で、トップダウンに、誰が、どこから、どのルートを経由して被害発生を引き起こし得るかのシナリオを、攻撃ツリー（攻撃のステップからなる一連の攻撃フロー）として構成し、各ツリーの成立の可能性を算定する手法。
※ 212 攻撃ルート：侵入口にあたる機器から、攻撃拠点にあたる機器までの経路。
※ 213 CSSC 認証ラボラトリー：ISASecure EDSA 認証とは　http://www.cssc-cl.org/jp/about_edsa/index.html〔参照 2018-05-01〕
※ 214 JIPDEC：CSMS 適合性評価制度　https://isms.jp/csms.html〔参照 2018-05-01〕
※ 215 株式会社日立製作所（経済産業省委託事業）：平成 28 年度 IoT 推進のための社会システム推進事業（スマート工場実証事業）報告書 http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report.pdf〔参照 2018-05-01〕
※ 216 中小企業庁調査室：2016 年版 中小企業白書概要　http://www.chusho.meti.go.jp/pamflet/hakusyo/H28/PDF/h28_pdf_mokujityuuGaiyou.pdf〔参照 2018-05-07〕
※ 217 大阪商工会議所：「中小企業向けサイバー攻撃対策支援事業の開始」ならびに「中小企業におけるサイバー攻撃対策に関するアンケート調査結果」について　http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf〔参照 2018-05-07〕
※ 218 https://www.ipa.go.jp/files/000060549.pdf〔参照 2018-05-07〕
※ 219 IPA：プレス発表　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　https://www.ipa.go.jp/about/press/20170207.html〔参照 2018-05-07〕
※ 220 https://www.ipa.go.jp/security/security-action/index.html〔参照 2018-05-07〕
※ 221 https://www.ipa.go.jp/security/keihatsu/sme/guideline/〔参照 2018-05-07〕
※ 222 IPA：SECURITY ACTION ロゴマークについて　https://www.ipa.go.jp/security/security-action/about-sa/index.html〔参照 2018-05-07〕
※ 223 一般社団法人 サービスデザイン推進協議会：平成29年度補正 サービス等生産性向上IT導入支援事業公募要領（第一次公募） https://www.it-hojo.jp/h29/doc/pdf/h29_application_guidelines.pdf〔参照 2018-05-07〕
※ 224 日本経済新聞：中小 13 万社のIT導入に補助金 500 億円　経産省　https://www.nikkei.com/article/DGXMZO24587760T11C17A2EE8000/〔参照 2018-05-07〕
※ 225 公益財団法人群馬県産業支援機構：群馬県中小企業等サイバーセキュリティ支援連絡会　http://www.g-inf.or.jp/security/〔参照2018-05-07〕
※ 226 北海道警察：Cyber- 道 net　https://www.police.pref.hokkaido.lg.jp/info/seian/cyber-bouhan-hiroba/cyber-donet/cybere-donet.html〔参照 2018-05-07〕
※ 227 https://security-shien.ipa.go.jp/〔参照 2018-05-07〕
※ 228 http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/〔参照 2018-05-07〕
※ 229 http://www.pref.tottori.lg.jp/secure/1096988/cybermanual.pdf〔参照 2018-05-07〕
※ 230 http://www.jnsa.org/result/2013/chusho_sec/data/chusho_security_tebiki_20140331.pdf〔参照 2018-05-07〕

付録

情報セキュリティ10大脅威2018・資料・ツール

情報セキュリティ10大脅威 2018
～引き続き行われるサイバー攻撃、あなたは守りきれますか?～

「情報セキュリティ 10 大脅威 2018」は、2017 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等からなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定した。資料は、下記の 3 章構成となっている。

■第 1 章　情報セキュリティ対策の基本 IoT機器（情報家電）編

IoT 機器を利用する上で、実施しておくべき情報セキュリティ対策の基本について解説

■第 2 章　情報セキュリティ 10 大脅威 2018

2017 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威選考会」の投票結果に基づき、「個人」「組織」における脅威を 1 位から 10 位に順位付けして解説

■第 3 章　注目すべき脅威や懸念

社会に影響を与える可能性が高く、現時点で注目しておきたい脅威や懸念等について解説

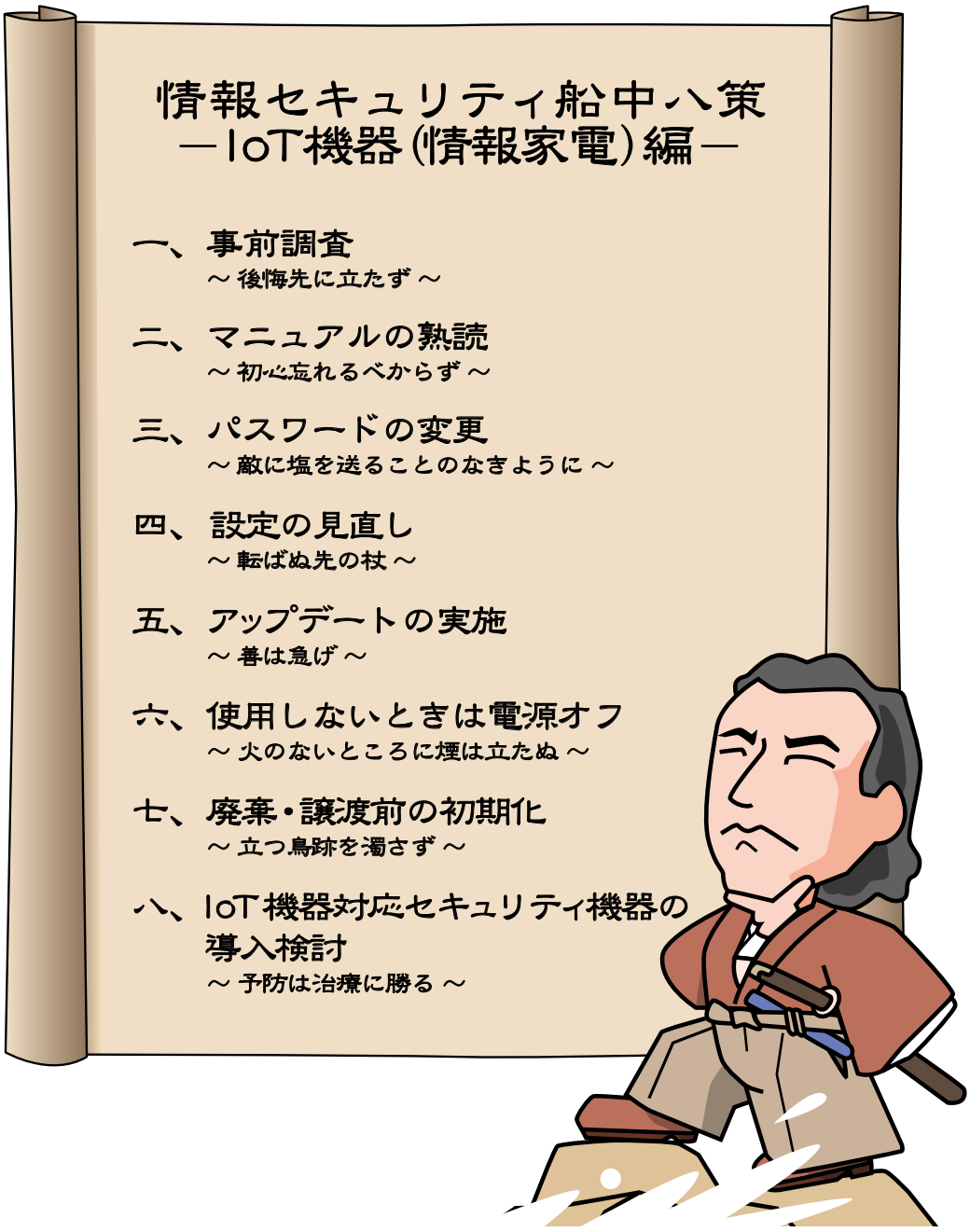
「情報セキュリティ 10 大脅威 2018」でも 2017 年と同様に「個人」と「組織」という異なる視点で、以下の表に示す 10 大脅威を選出した。

「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングやクレジットカード情報等の不正利用	1	標的型攻撃による被害
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを狙った攻撃	4	脆弱性対策情報の公開に伴う悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するためのセキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT 機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT 機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告によるインターネット詐欺	10	犯罪のビジネス化（アンダーグラウンドサービス）

■表　情報セキュリティ 10 大脅威 2018「個人」及び「組織」向けの脅威の順位

情報セキュリティ船中八策 IoT機器（情報家電）編

江戸時代に坂本龍馬がまとめたと言われる「船中八策」にあやかり、IoT 機器の情報セキュリティの基本的な対策から八つを厳選し、解説的にことわざと併記した「情報セキュリティ船中八策 IoT 機器（情報家電）編」を以下に示す。



■「情報セキュリティ 10 大脅威 2018」は、以下の URL からダウンロードできます。
https://www.ipa.go.jp/security/vuln/10threats2018.html

資料A　2017年のコンピュータウイルス届出状況

IPA が 2017 年 1 月から 12 月の期間に受け付けた、コンピュータウイルス届出の集計結果について述べる。

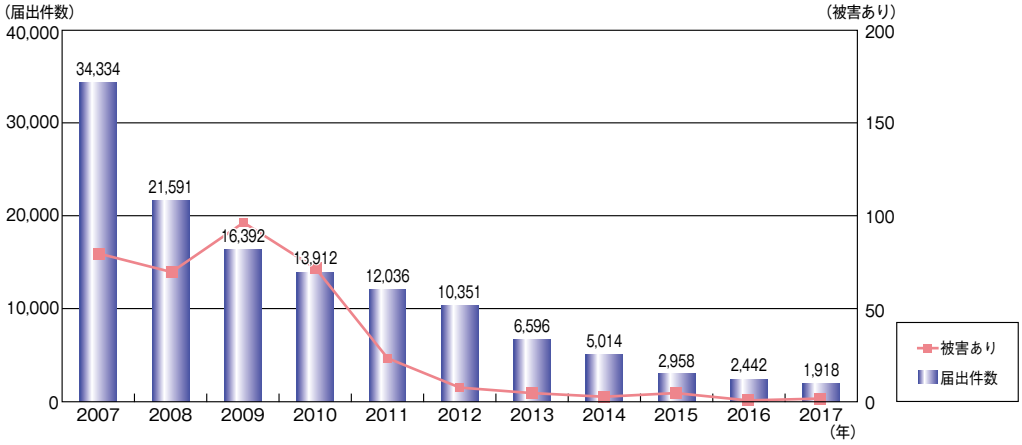
A.1　届出件数

2017 年の年間届出件数は、前年の 2,442 件より 524 件（約 21.5%）少ない 1,918 件となった（図 A-1）。

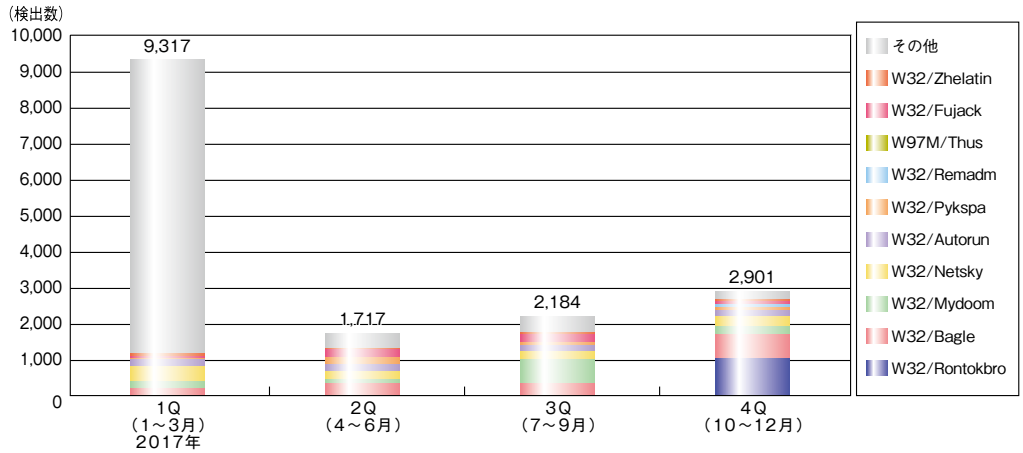
A.2　届出ウイルス

2017 年に届け出されたウイルスのうち、検出数の多いウイルスは上から、W32/Downad（5,757 個）、W32/Ramnit（2,083 個）、W32/Bagle（1,460 個）となっている。なお、W32/Downad と W32/Ramnit は図 A-2 では「その他」に含まれる。

W32/Downad は、前年の 304 個より 5,453 個多い 5,757 個、W32/Ramnit は前年の 302 個より 1,781 個多い 2,083 個となり、どちらも増加傾向となった。



■図 A-1　ウイルス届出件数推移（2007 ～ 2017 年）



■図 A-2　2017 年ウイルス別検出数の推移

参照

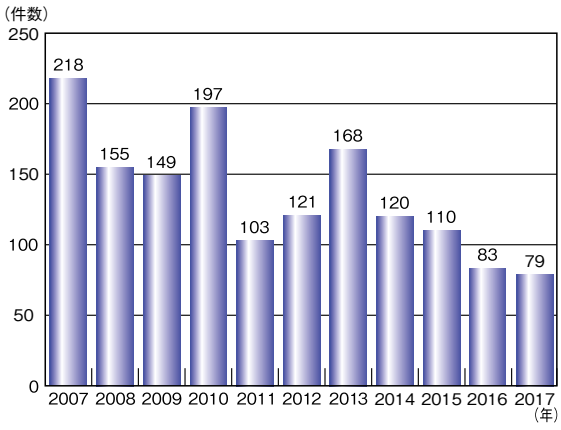
■コンピュータウイルス・不正アクセスの届出状況および相談状況［2017年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/txt/2017/q4outline.html

資料B　2017年のコンピュータ不正アクセス届出状況

IPA が 2017 年 1 月から 12 月の期間に受け付けた、コンピュータ不正アクセス届出の集計結果について述べる。

B.1　届出件数

2017 年の年間届出件数は 79 件となり、2016 年の届出件数 83 件から 4 件（約 4.8%）減少した。過去 10 年間に IPA セキュリティセンターが受け付けた届出件数の推移を図 B-1 に示す。



■図 B-1　不正アクセス届出件数推移（2007 ～ 2017 年）

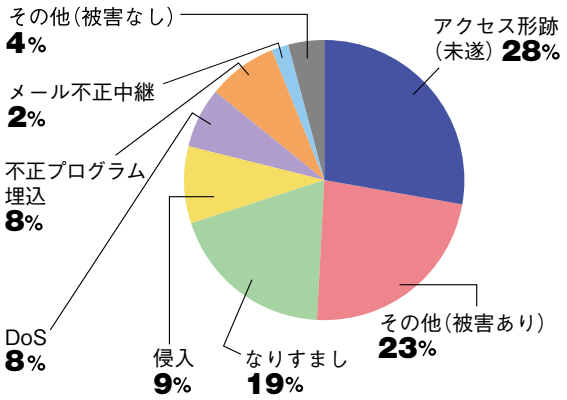
B.2　届出種別

前年と比較すると、「なりすまし」が 30 件から 15 件に減少（50% 減）した一方で、「侵入」が 4 件から 7 件に増加（75% 増）している（表 B-1）。

届出種別		2017年	2016年	2015年
被害あり	侵入	7	4	12
	メール不正中継	2	1	0
	ワーム感染	0	0	0
	DoS（サービス妨害）	6	7	11
	アドレス詐称	0	0	0
	なりすまし	15	30	44
	不正プログラム埋込	6	5	8
	その他（被害あり）	18	14	13
被害なし	アクセス形跡（未遂）	22	19	10
	ワーム形跡	0	0	0
	その他（被害なし）	3	3	12
合計（件）		79(54)	83(61)	110(88)

※合計のカッコ内の数字は、被害があった届出種別の合計を示している。

■表 B-1　2017 年不正アクセス届出種別



■図 B-2　2017 年不正アクセス被害内容

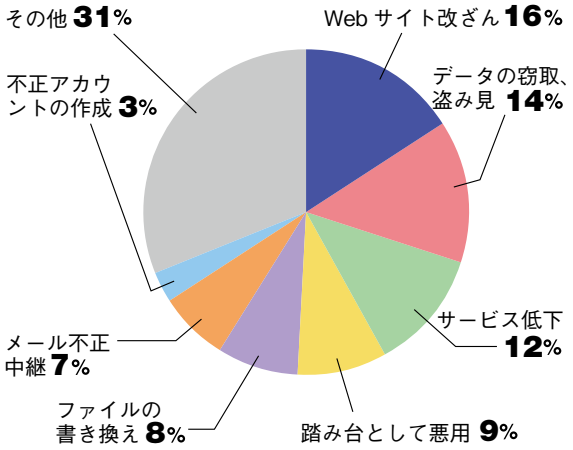
B.3　被害内容

届出のうち実際に被害があった内容の分類について述べる。延べ被害件数は前年から 5 件（約 7.1%）増加した（表 B-2）。

被害内容	2017年	2016年	2015年
メール不正中継	5	1	1
サーバダウン	0	0	0
不正アカウントの作成	2	0	1
Web サイト改ざん	12	9	14
パスワードファイルの盗用	0	0	0
サービス低下	9	7	13
オープンプロキシ	0	0	0
ファイルの書き換え	6	2	4
踏み台として悪用	7	13	33
オンラインサービスの不正利用	0	17	16
データの窃取、盗み見	11	5	12
その他	23	16	22
合計（件）	75（※）	70（※）	116(※)

※実被害届出1件に複数の被害内容が存在するケースもあるため実被害届出件数合計と一致していない。

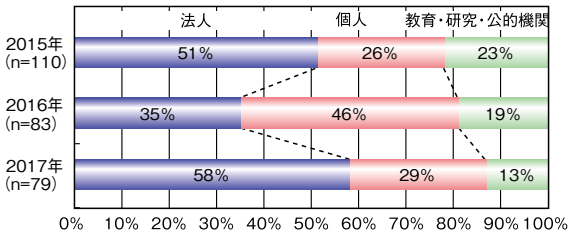
■表 B-2　2017 年不正アクセス被害内容



■図 B-3　2017 年不正アクセス被害内容

B.4 届出者の分類

前年と比較すると届出者別の内訳は「法人」からの届出件数が増加し、「教育・研究・公的機関」からの届出件数が減少した（図 B-4）。



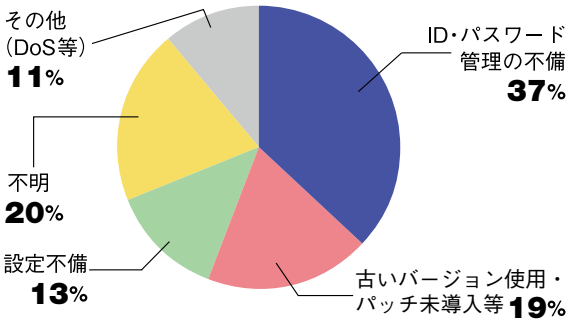
■図 B-4　不正アクセス届出者推移（2015 ～ 2017 年）

B.5 被害原因

実際に被害があった届出の被害原因の内訳は、「ID・パスワード管理の不備」が 20 件（37%）と最も多く、次いで「古いバージョン使用・パッチ未導入等」が 10 件（19%）等であった。

被害原因	2017年	2016年	2015年
ID・パスワード管理の不備	20	26	35
古いバージョン使用・パッチ未導入等	10	4	15
設定不備	7	7	6
不明	11	15	16
その他（DoS 等）	6	9	16
合計（件）	54	61	88

■表 B-3　2017 年不正アクセス届出被害原因



■図 B-5　2017 年不正アクセス届出被害原因

B.6 対策情報

2017 年の届出において、被害原因の「古いバージョン使用・パッチ未導入等」が前年の 4 件から 10 件（150% 増）と大きく増加している。被害防止のためにも利用しているソフトウェアの把握及びバージョン管理の徹底が望まれる。

参照

■コンピュータウイルス・不正アクセスの届出状況および相談状況［2017年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/txt/2017/q4outline.html

資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

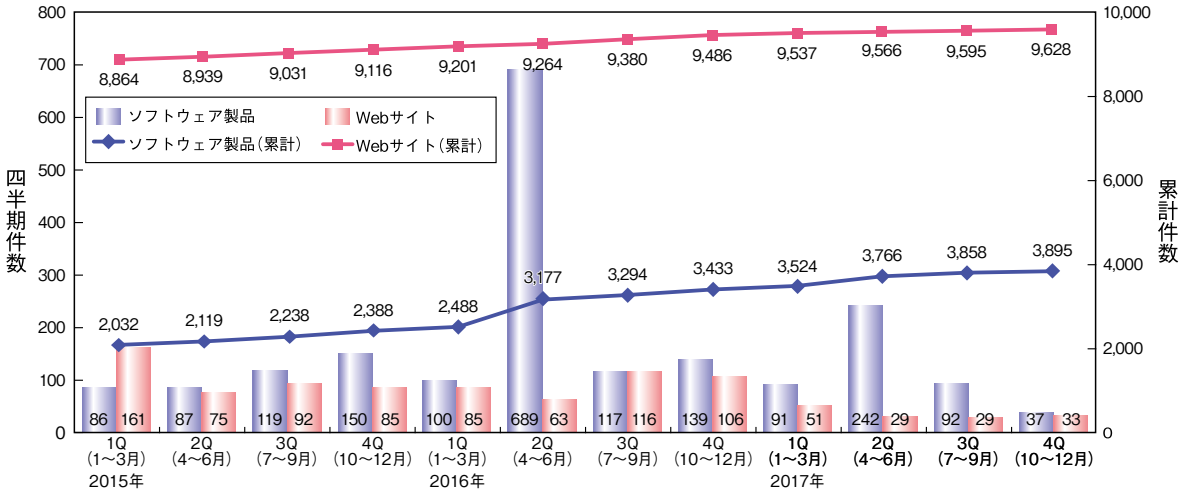
IPA が受け付けた脆弱性関連情報に関する届出は、2017 年末までに 1 万 3,523 件に達した。

C.1　脆弱性の届出概況

2017 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 3,895 件、Web サイトに関するもの 9,628 件、合計 1 万 3,523 件で、Web サイトに関する届出が全体の 71% を占めている。

表 C-1 に示すように、届出受付開始から各四半期末時点までの就業日 1 日あたりの届出件数は、2017 年第 4 四半期末時点で 4.11 件となっている。

届けられた脆弱性の種類はソフトウェア製品、Web サイトともにクロスサイト・スクリプティングの脆弱性が一番多くなっている。



■図 C-1　脆弱性関連情報の届出件数の四半期別推移

2016年1Q（1～3月）	2016年2Q（4～6月）	2016年3Q（7～9月）	2016年4Q（10～12月）	2017年1Q（1～3月）	2017年2Q（4～6月）	2017年3Q（7～9月）	2017年4Q（10～12月）
4.09	4.26	4.25	4.25	4.21	4.21	4.17	4.11

■表 C-1　就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

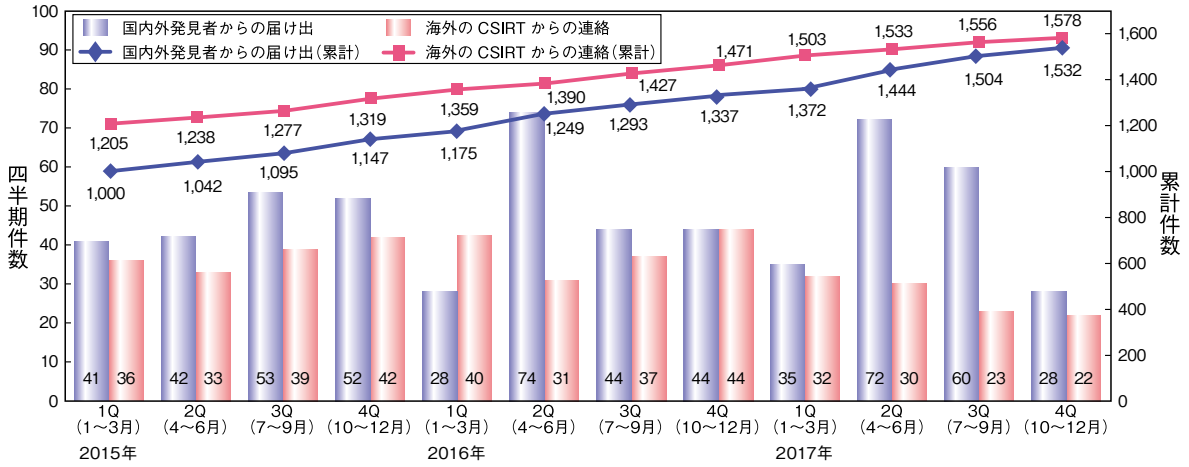
C.2　ソフトウェア製品の脆弱性の処理状況届出種別

2017 年末時点のソフトウェア製品に関する脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものは 1,704 件、製品開発者からの届出のうち JVN で公表せず製品開発者が個別対応を行ったものは 37 件、製品開発者が脆弱性ではないと判断したものは 89 件、告示で定める届出の対象に該当せず不受理としたものは 445 件で、これらの取り扱いを終了したものの合計は 2,275 件に達した（表 C-2）。

この他、海外の CSIRT から JPCERT/CC が連絡を受けた 1,578 件を JVN で公表した。これらの公表済み件数の期別推移を図 C-2 に示す。

分類		累計件数
修正完了	公表済み	1,704件
	個別対応	37件
脆弱性ではない		89件
不受理		445件
合計		2,275件

■表 C-2　ソフトウェア製品の脆弱性の終了件数



■図 C-2　ソフトウェア製品の脆弱性対策情報の公表件数

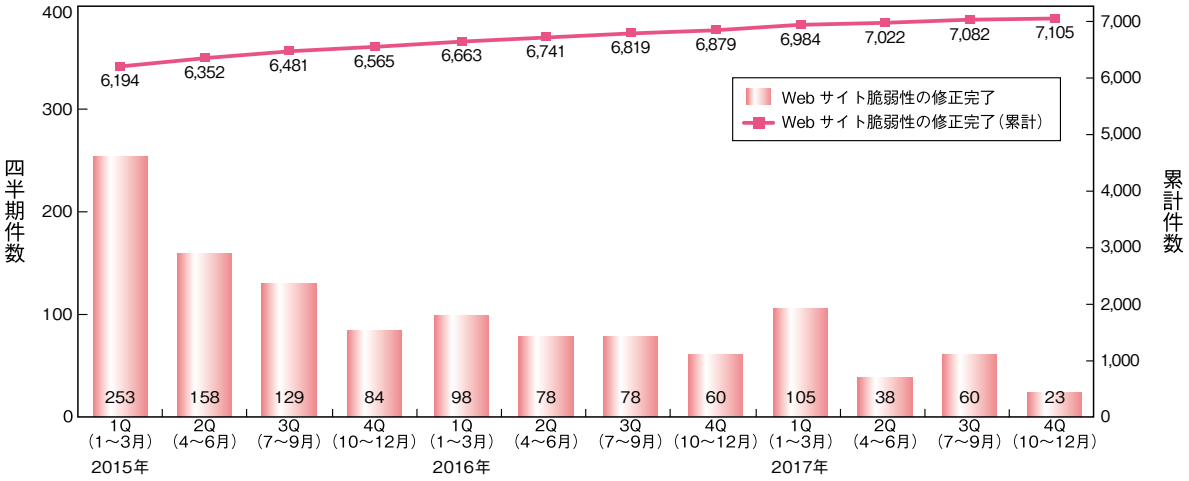
C.3 Webサイトの脆弱性の処理状況

2017 年末時点の Web サイトに関する脆弱性の処理状況は、IPA が通知を行い Web サイト運営者が修正を完了したものは 7,105 件、IPA が注意喚起等を行った後に処理を終了させたものは 1,130 件、IPA 及び Web サイト運営者が脆弱性ではないと判断したものは 578 件、Web サイト運営者と連絡が不可能なもの、または Web サイト運営者の対応により取り扱いが不能なものが 175 件、告示で定める届出の対象に該当せず不受理としたものは 241 件で、これらの取り扱いを終了したものの合計は 9,229 件に達した(表 C-3)。

これらのうち、修正完了件数の期別推移を図 C-3 に示す。

分類	累計件数
修正完了	7,105件
注意喚起	1,130件
脆弱性ではない	578件
取り扱い不能	175件
不受理	241件
合計	9,229件

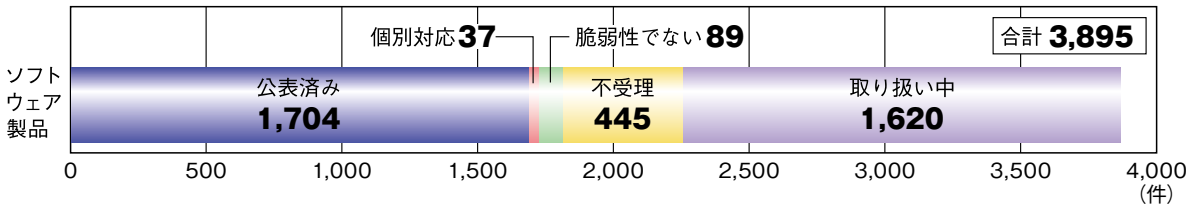
■表 C-3　Web サイトの脆弱性の終了件数



■図 C-3　Web サイトの脆弱性の修正完了件数

C.4 ソフトウェア製品の脆弱性の届出の処理状況

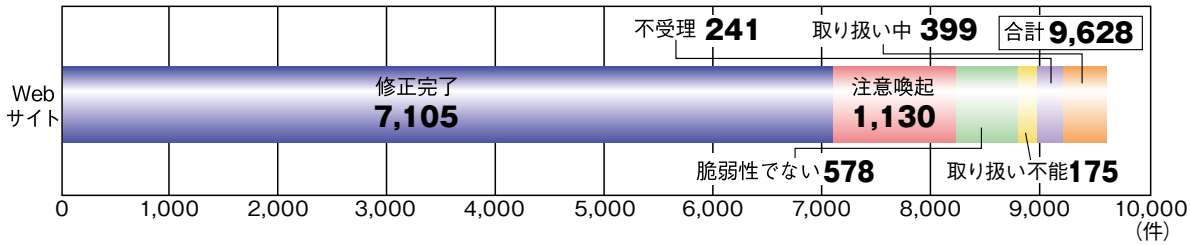
ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。



■図 C-4　ソフトウェア製品の脆弱性関連情報届出の処理状況

C.5 Webサイトの脆弱性の届出の処理状況

Web サイトの脆弱性関連情報の届出について処理状況を図 C-5 に示す。



■図 C-5　Web サイトの脆弱性関連情報届出の処理状況

参照

■ソフトウェア等の脆弱性関連情報に関する届出状況［2017年第4四半期（10月～12月）］
https://www.ipa.go.jp/files/000063751.pdf

ツール1

情報セキュリティ対策支援サイト
情報セキュリティ対策の「知りたい」、「学びたい」、「始めたい」、「続けたい」をサポート

IT化の進展に伴い、企業の情報資産の窃取や業務妨害を狙ったサイバー攻撃・犯罪は巧妙化・悪質化しており、これらのターゲットは、政府機関や大手企業だけでなく、中小企業にまで拡大しています。このため、中小企業においても、ITの安全な利活用に向け、情報セキュリティ対策の必要性を認識し、適切な対策を実施することが必要です。

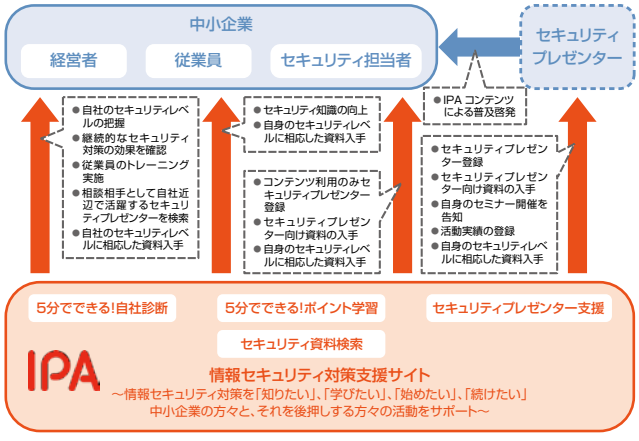
このような状況をふまえ、IPAでは、中小企業を中心に、企業・組織内の情報セキュリティ対策水準の向上を支援するための情報セキュリティ対策支援サイトを公開しました。
本サイトは、情報セキュリティ対策を「知りたい」「学びたい」「始めたい」「続けたい」中小企業の方々と、それを後押しする方々の活動をサポートします。

情報セキュリティ対策支援サイトの構成

「情報セキュリティ対策支援サイト」は、「中小企業向けセキュリティ資料提供」、中小企業の経営者を主な対象とした「5分でできる！自社診断」、中小企業向けの「5分でできる！ポイント学習」、そして中小企業のセキュリティ対策水準向上を支援する方に向けた「セキュリティプレゼンター※支援」等で構成しています。

※セキュリティプレゼンターとは、IPAが開発・作成した情報セキュリティコンテンツ等を使用し、企業に対して情報セキュリティの普及啓発を行う人

図1. 情報セキュリティ対策支援サイトを利用した活動イメージ



■中小企業向けセキュリティ資料提供

IPAが作成・公開している様々な情報セキュリティに関する資料やツールを、利用者自身の属性（企業経営者、従業員、一般、企業向け啓発者等）と利用目的（知りたい、学びたい、始めたい、続けたい）を条件に検索することができる環境を提供します。

■５分でできる！自社診断

「５分でできる！自社診断」は、中小企業において実施が望まれている基本的な情報セキュリティ対策の状況を診断できる無料のツールです。

2016年11月15日に刷新された「中小企業の情報セキュリティ対策ガイドライン」とともに改訂された「５分でできる！情報セキュリティ自社診断」の25の診断項目をオンラインで提供します。

「５分でできる！情報セキュリティ自社診断」シートのダウンロードや自分で診断結果の計算を行うことなく、情報セキュリティ対策の現状把握ができます。

アカウントを作成することで、診断結果を保存することができ、過去５回分の診断結果や他社、同業他社との比較を行うことができます。継続して行っているセキュリティ対策の状況や効果を確認する際にご利用ください。

診断後は、診断結果に即した推奨資料が表示されます。同時に活用方法の説明が表示され、該当資料にもすぐにアクセスできるようになっているため、今後の対策に必要な資料を探す必要はありません。

図2. 診断項目

図3. 診断結果

■セキュリティプレゼンター検索

セキュリティプレゼンターに相談したい、講演を依頼したいといったときには、資格や活動地域で検索し、過去の活動履歴等を確認して、セキュリティプレゼンターを探すことができます。

図4. 検索結果（詳細）

■ ５分でできる！ポイント学習

「５分でできる！ポイント学習」は、情報セキュリティについてe-Learning形式の勉強ができる１テーマ５分の学習ツールです。職場の日常の１コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。PDF版も提供していますので、あらかじめダウンロードしておくことで、インターネットが利用できない環境でも、いつでもどこでも学習できます。

また、アカウントを作成することで、都合の良いタイミングで学習の中断・再開ができ、これまでの学習進捗状況を表形式で確認することができます。

(1) 学習内容の概要

学習テーマは､「保管について」「廃棄について」「パソコンについて」「個人所有端末について」等があり、事例を疑似体験しながら学習できます。学習後にはその内容に関する確認テストを用意しています。テスト結果を確認することで、学習結果の理解度をチェックできます。

学習テーマごとに、自社診断に対応したものや職種などで分類された「コース」を提供しています。コースを選択して学習を開始してください。

コースに含まれている確認テストにすべて正解すると、「修了証」が発行されます。修了証には修了日（年月日）が記載されますので、従業員の学習完了の確認等に利用できます。

(2) 学習の流れ

「５分でできる！ポイント学習」の学習の流れを図５に示します。

■ セキュリティプレゼンター支援

「セキュリティプレゼンター支援」は、中小企業における情報セキュリティ対策水準向上のため、IPAが開発・作成した情報セキュリティコンテンツ等を活用し、地域においてその活動に携わる“セキュリティプレゼンター”のサイトです。セキュリティプレゼンターに対しては情報登録のほか、普及活動用資料の提供サービスを行っています。

(1) 登録情報の公開

セキュリティプレゼンターとして情報登録（無料）すれば、相談相手を探している利用者の検索結果に表示されます。

(2) セキュリティプレゼンター向け資料ダウンロード

IPAが登録者向けに提供する情報セキュリティに関する資料をダウンロードできます。セキュリティプレゼンター自身が開催するセミナー資料等にご活用ください。

(3) 活動実績・活動告知の登録

情報セキュリティに関する普及・啓発活動（セミナー開催、セミナー受講、チラシ配布、事例提供等）を登録することで、検索結果に表示させることができます。また、開催予定のセミナー情報を活動告知として登録することで、「セキュリティプレゼンター支援」のトップページに表示させることができます。

図5.「学習の流れ」

1 学習テーマを開始

2 学習の目的を理解

3 事例を疑似体験

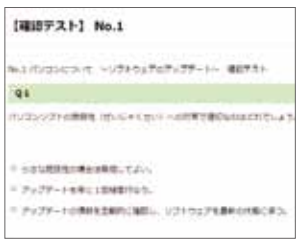
4 事例を疑似体験

5 用語の確認

6 学習の意図を確認

7 正しい対処法を理解

8 確認テスト



付録

ツール2

企業や組織の情報セキュリティ対策自己診断テスト
情報セキュリティ対策ベンチマーク

近年「コンプライアンス（法令順守）」の重要性が叫ばれ、それに伴う企業の責務として「コーポレートガバナンス（企業統治）」や「内部統制」の確立が急務となっています。同時に、こうした仕組みをITの観点から考える「情報セキュリティガバナンス」の取り組みも、企業の重要な課題となりつつあります。あらゆるコンピュータがネットワークで結ばれている現在、たったひとつの企業がセキュリティ対策を怠っただけでも、社会的に大きな損害を与えてしまうことがあるからです。

しかし、IT事故のリスクは「目に見えない」ため、投資に向けた経営判断が難しいのが実情です。また、情報セキュリティ対策は利益に直接結びつかないことが多く、企業の認識不足も手伝って、対策が不十分なケースが多数見受けられます。

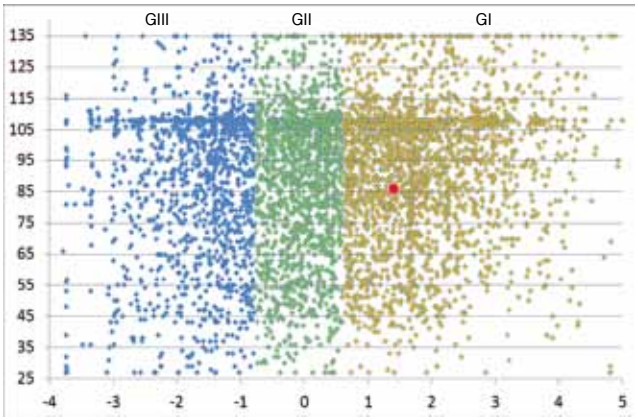
本ツールは、インターネットを通じてウェブページ上の設問に答えるだけで、他社と比較した自社のセキュリティレベルを診断できます。簡単な操作で自社の現状を把握し、取り組みの道筋を見つけることからスタートできます。

情報セキュリティ対策ベンチマークの設問

本ツールの設問は、「セキュリティ対策の取り組み状況に関する評価項目」27問と、自社の状況を回答する「企業プロフィールに関する評価項目」19問の計46問で構成しています。これらの設問に回答することで、セキュリティに関する自社の取り組みがどの程度のレベルにあるかが分かります。

「セキュリティ対策の取り組み状況に関する評価項目」27問は、5つのレベルから選択しますが、具体的な設問に関する解説と対策のポイントがウェブページ上で展開でき、それらを参考に回答することができます。回答すると、それぞれスコアが1点から5点で記録され、トータルスコアの最大は135点となります。また、「企業プロフィールに関する評価項目」19問も選択肢の中から自社に適した内容で回答できるようになっています。

図1. トータルスコアとリスク指標による診断基礎データの散布図及び自社の位置付け（●は自社の診断結果）



情報セキュリティ対策ベンチマークによる診断

前述の設問に回答すると、回答された企業プロフィールに基づいて算出される情報セキュリティリスク指標※によるグループ別、企業の規模別、及び業種別の診断基礎データと比較診断が行われます。結果、それぞれの比較対象別の、他社と比較した自社のセキュリティレベルが示され、他社と比べて自社に不足しているセキュリティ対策が明確になります。

※ 情報セキュリティリスク指標

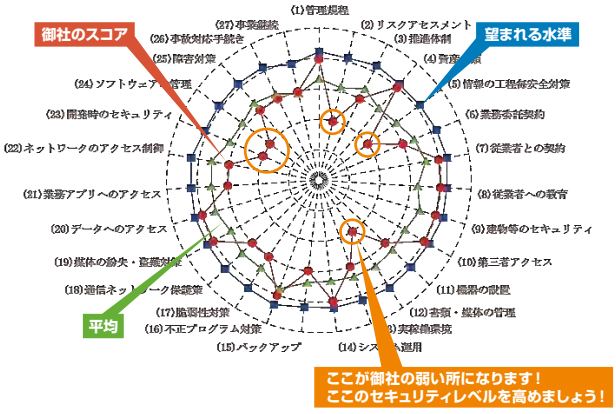
情報セキュリティリスク指標とは、従業員数、売上高、重要情報の保有数、IT依存度などから計算される企業が抱えるリスクを表す指標のことです。情報セキュリティ対策ベンチマークでは、情報セキュリティリスク指標の値の高い順に、以下の3つのグループのいずれかに分類しています。

グループⅠ（GI）：高い水準のセキュリティレベルが要求される層
グループⅡ（GII）：相応の水準のセキュリティレベルが望まれる層
グループⅢ（GIII）：情報セキュリティ対策が喫緊の課題でない層

診断結果の表示

診断結果は、診断基礎データの散布図上に自社の診断結果がプロットされる散布図（図1参照）や、診断基礎データの平均値や望まれる水準値と併せて自社の診断結果が表示される見やすいレーダーチャート（図2参照）で表示されます。レーダーチャートでは、中心に近いほどセキュリティレベルが低く、円状に大きく広がっているほどバランスの取れた良好なセキュリティレベルであることを示します。取り組みを継続しながら繰り返し診断を行うことで、実施した対策の効果を確認することもできます。

図2. レーダーチャートによる診断結果の表示



ツール3

官民の情報セキュリティコンテンツを集約したポータルサイト
https://www.ipa.go.jp/security/kokokara/

情報セキュリティ・ポータルサイト「ここからセキュリティ!」

現在、複数の政府機関や多くの企業・団体によって、さまざまな情報セキュリティに関する情報が公開されています。しかし、それらは各組織で独自に作成・公開しているため、分野ごとの偏りが見られることが多く、情報を求める利用者は、場合によっては複数のウェブサイトから情報を探し集める必要がありました。また、ウェブ検索の際は、目の前に起こった現象をキーワードとして検索する場合と、被害（脅威）の名称をキーワードとして検索する場合とで到達できるサイトが異なることもあるため※1、入手できる情報は、利用者の知識量や経験値によって差異が生じることもありました。

これらの問題解決のため、官民ボード※2では、IPAを取組主体として官・民合わせた国内の情報セキュリティ普及啓発関連情報を集約したポータルサイト「ここからセキュリティ！」を公開しています。

※1 例えば、クリックしただけで料金を請求される「ワンクリック請求」への対処方法を検索する場合、「ワンクリック請求」という名称で検索するか「料金画面が消えない」「料金請求された」などで検索するかで、表示されるサイトが異なることがあります。

※2 警察庁、総務省および経済産業省が設置した、不正アクセス防止に関する現状の課題や改善方策について意見を集約するための委員会。構成員として政府機関のほか、関連する民間企業、団体、研究機関等が参加。

検索しやすい項目分類

「ここからセキュリティ！」は、脅威の名称とその現象をひとつにまとめ、利用者がセキュリティ初心者であっても有効なセキュリティ情報にたどり着けるよう、各項目を大分類と小分類でカテゴリ化しています。

また、「被害に遭ったら」「対策する」「教育・学習」など、利用者が情報を検索する場面ごとに分類することによって、必要な情報を見つけやすくする工夫も行っています。

付録

ツール4

脆弱性の正しい知識を分かりやすいアニメで解説
https://www.ipa.go.jp/security/vuln/vuln_contents/

知っていますか？脆弱性
ーアニメで見るウェブサイトの脅威と仕組みー

「脆弱性」とは、ソフトウェアなどに潜むセキュリティ上の弱点のことで、情報システム全般に対する大きな脅威となります。近年、この脆弱性を悪用したウェブサイトへの不正アクセス事件や、個人情報の漏えい事件が増加しています。

ウェブサイトの担当者は、自らの情報資産だけでなく、ウェブサイトのアクセス利用者の被害を防ぐため、脆弱性対策を適切に行う必要があります。

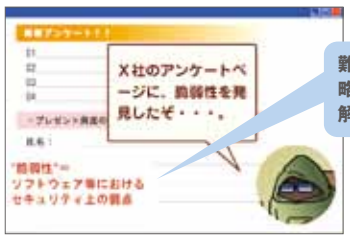
しかし、現実には脆弱性の脅威や仕組み、対策についての知識が必ずしも社会に広まっておらず、ウェブサイトの脆弱性が原因となって起こる被害を未然に防ぐことができていません。

IPAでは、「知っていますか？脆弱性（ぜいじゃくせい）」というコンテンツを公開しています。このコンテンツは、ウェブサイトの運営者や一般利用者に向けて、ウェブサイトにおける代表的な10種類の脆弱性について、分かりやすくアニメーションで解説したものです。脆弱性についての理解を深める第一歩としてご活用ください。

クロスサイト・スクリプティング（XSS）の解説例（抜粋）

①

②



③

④

○×テストで理解度チェック

ツール5

脆弱性体験学習ツール「AppGoat」
ー突いてみますか？脆弱性！ー

脆弱性体験学習ツール「AppGoat」は、脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べるツールです。利用者は、学習テーマ毎に用意された演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法の学習を対話的に実施できます。

ウェブアプリケーションやサーバ・デスクトップアプリケーションの脆弱性対策に必要なスキルを習得したい開発者やウェブサイトの管理者におすすめです。

AppGoatの種類

AppGoatは下記の３種類を提供しています。

・ウェブアプリケーション用学習ツール（個人学習モード）

ウェブアプリケーションに関連する脆弱性について学習できるツールです。個人学習モードは、自宅や職場、学校で自習を行いたい場合におすすめです。

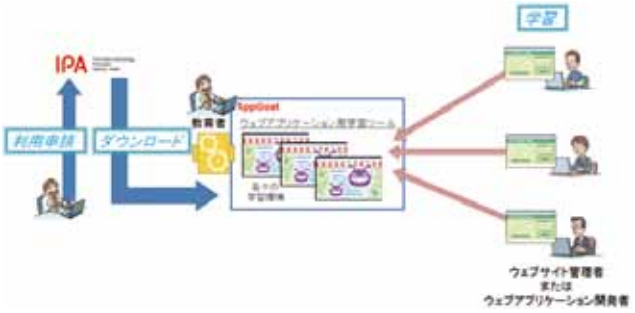
・ウェブアプリケーション用学習ツール（集合学習モード）（図１参照）

ウェブアプリケーションに関連する脆弱性について学習できるツールです。セミナールームや教室でセミナーや授業を行いたい場合におすすめです。

・サーバ・デスクトップアプリケーション用学習ツール

サーバ・デスクトップアプリケーションに関連する脆弱性について学習できるツールです。自宅や職場、学校で自習を行いたい場合におすすめです。

図1. 集合学習モードの利用イメージ



学習の流れ

各脆弱性毎に複数の学習テーマがあり、各学習テーマを順に学習することで脆弱性に対する理解を深めることができます。ウェブアプリケーション用学習ツール（個人学習用）を例にすると、各テーマは主に図２の構成となります。また、図３はテーマ構成の中の「演習（発見）」学習時の画面です。

図2. テーマの構成

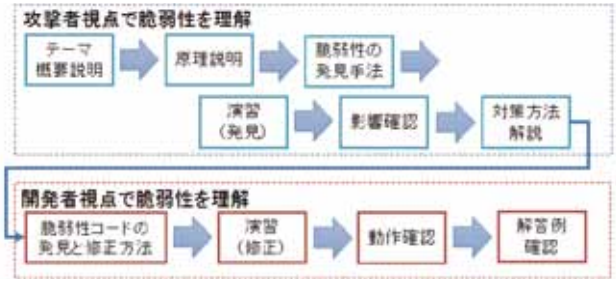
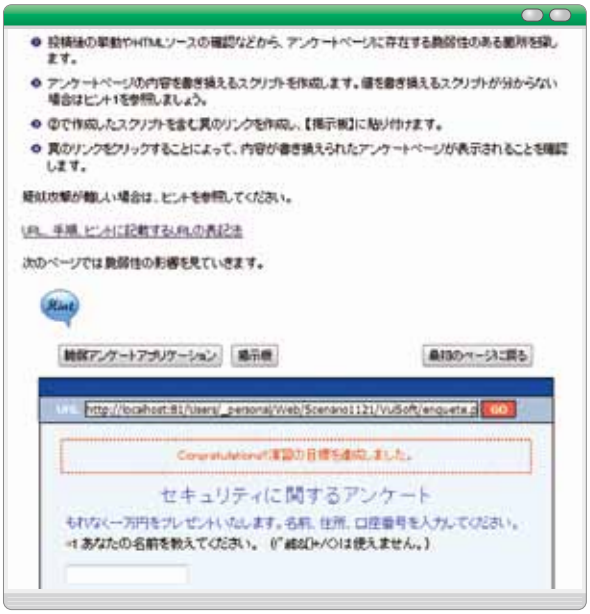


図3. 演習（発見）の画面イメージ



学習できる脆弱性一覧

表1. ウェブアプリケーション用学習ツール

クロスサイト・スクリプティング
SQLインジェクション
CSRF（クロスサイト・リクエスト・フォージェリ）
ディレクトリ・トラバーサル
OSコマンド・インジェクション
セッション管理の不備
認証制御や認可制御の欠落
HTTPヘッダ・インジェクション
バッファオーバーフロー
クリックジャッキング
メールヘッダ・インジェクション
その他の脆弱性（システム情報漏えい等）

表2. サーバ・デスクトップアプリケーション用学習ツール

バッファオーバーフロー
ディレクトリ・トラバーサル
リソースリーク
整数オーバーフロー
フォーマット文字列
認証・認可
その他の脆弱性（ジャンクションへの考慮不足の問題等）

ツール6

ソフトウェアの脆弱性対策情報に関する総合データベース
https://jvndb.jvn.jp/

脆弱性対策情報データベース「JVN iPedia」

今日、社会や経済の基盤はITに依存しています。この基盤を安全に維持するには、自然災害やシステム障害に備えるだけでなく、コンピュータウイルスや不正アクセスなど、インターネットを介したサイバー攻撃への対策が必要です。最近でも、OSやウェブブラウザを中心に深刻な脆弱性が多数報告されており、ソフトウェアのアップデートなどの対策が不可欠です。

一方で従来、有効な対策をとりたくても、脆弱性に関する日本語の情報は不十分でした。そこでIPAでは、JVN（Japan Vulnerability Notes：脆弱性対策情報ポータルサイト）に掲載される情報などをもとに、国内向けソフトウェアの脆弱性に関する概要や対策の情報を蓄積し、「JVN iPedia」（脆弱性対策情報データベース）として公開しました。2018年3月時点で約81,000件の情報があり、データは日々増え続けています。

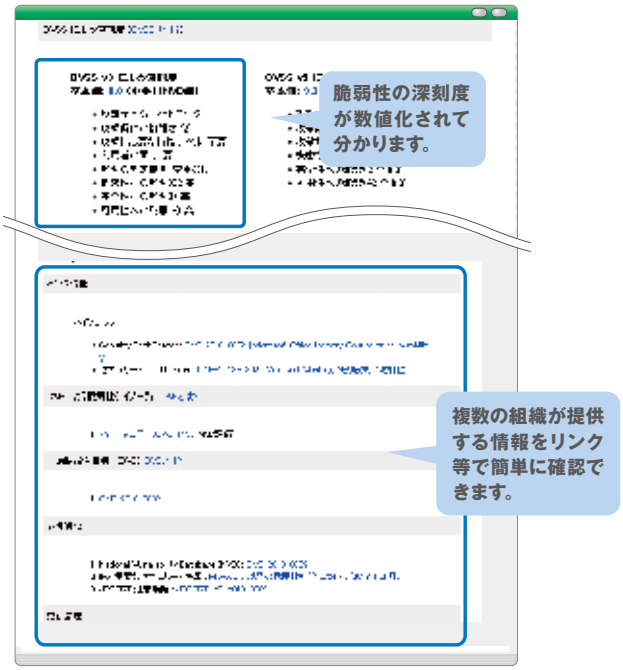
JVN iPediaでは、これだけの量のデータから目的の脆弱性を探索するために検索機能やRSS※配信機能を備えています。「特定の製品に存在する脆弱性を確認したい」、「JVN・他組織で公開される情報をもとに脆弱性対策を調べたい」など、入手したい情報が特定されている場合に、検索機能によって効果的に探すことが可能です。RSS配信機能を利用することで、定期的に脆弱性情報を取得することもできます。

さらに、「MyJVN 脆弱性対策情報収集ツール」（ツール4参照）を利用することで、脆弱性の対策情報の収集が効率的になります。

また、昨今、製品のグローバル化により、国内製品に関する脆弱性対策情報は国内のみならず海外でも重要性が高まっていることから、JVN iPedia 英語版（https://jvndb.jvn.jp/en/）も公開しています。

※RSS：ウェブサイトから最新情報を効率よく収集／配信するための統一的な形式

脆弱性対策情報の表示例



JVN iPediaの項目

JVN iPediaでは次のような項目を設定し、脆弱性の概要やその対策、影響を受けるソフトウェアなど、幅広い情報を提供しています。

項　目	情報内容
ID	脆弱性対策情報ごとに付与されるJVN iPedia独自のIDです。
タイトル	脆弱性対策情報のタイトルです。
概要	脆弱性対策情報の概要です。
CVSS※による深刻度	CVSSによる脆弱性の深刻度を評価しています。
影響を受けるシステム	どのベンダーのどのシステムに対して影響があるかを表記しています。
想定される影響	脆弱性による想定される影響を記載しています。
対策	脆弱性の対策が記載されています。
ベンダー情報	ベンダーの情報を発表しています。
参考情報	脆弱性対策情報に関連する情報へのリンクです。
更新履歴	更新履歴です。
公表日/登録日/最終更新日	公表日、登録日、最終更新日を記載しています。

※CVSS：共通脆弱性評価システム

ツール 7

自社システムに関連する脆弱性情報を効率よく収集
https://jvndb.jvn.jp/apis/myjvn/mjcheck3.html［Adobe AIR 版］

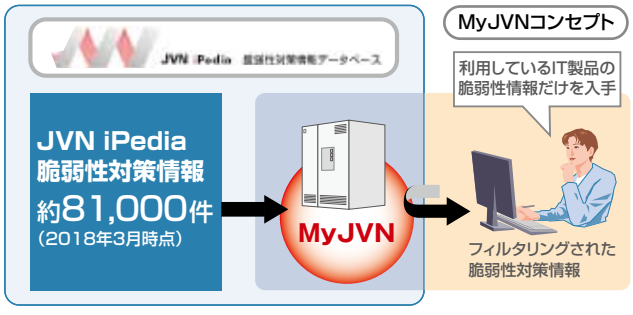
MyJVN 脆弱性対策情報収集ツール

最近では、各種サイトで多数の脆弱性対策情報が提供され、IPAでもJVN iPedia（脆弱性対策情報データベース）※1を整備しています。しかし、情報セキュリティの専門家を持たない企業や組織にとって、必要な情報の収集は容易ではありません。そこで、JVN iPediaに登録された情報の中から、利用者自身に関係する情報のみを効率的に収集できるよう、IPAが開発したツールがMyJVN 脆弱性対策情報収集ツールです。

MyJVN 脆弱性対策情報収集ツールは、フィルタリング条件設定機能、自動再検索機能などを持ち、自社（組織）で利用しているソフトウェア製品を選択することにより、JVN iPediaによる脆弱性対策情報のうち、必要な情報だけを効率よく入手できます。素早く適切な脆弱性対策を行うことを通じ、情報システムを常に安全な状態に維持することが可能になります。2018年4月には、Flash版の後継にあたるAdobe AIR版を公開しており、複数のフィルタリング条件設定、メール転送、概要情報のエキスポート、といった機能が利用可能です。

また、MyJVNでは、国際協力の強化に向け、米国政府の支援を受けた非営利団体のMITRE※2が中心となって仕様策定を進めているソフトウェアの製品名を記述するための共通の基準であるCPE（共通プラットフォーム一覧：Common Platform Enumeration）の試行を開始しました。詳しくは次のURLの「共通プラットフォーム一覧CPE 概説」を参照ください。（https://www.ipa.go.jp/security/vuln/CPE.html）

すでに、JVN iPedia、MyJVN では、CVE※3、CVSS※4、CWE※5 を適用しています。今回のCPE 適用に引き続き、今後も共通基準の導入を進めることにより、利用者側の客観的・効率的な脆弱性対策を目指した利活用基盤を整備していきます。



※1 IPA が公開している脆弱性対策情報データベース https://jvndb.jvn.jp/
※2 MITRE Corporation 米国政府向けの技術支援や研究開発を行う非営利組織 https://www.mitre.org/
※3 CVE（Common Vulnerabilities and Exposures）「共通脆弱性識別子 CVE 概説」を参照ください。https://www.ipa.go.jp/security/vuln/CVE.html
※4 CVSS（Common Vulnerability Scoring System）「共通脆弱性評価システム CVSS 概説」を参照ください。https://www.ipa.go.jp/security/vuln/CVSS.html
※5 CWE（Common Weakness Enumeration）「共通脆弱性タイプ一覧 CWE 概説」を参照ください。https://www.ipa.go.jp/security/vuln/CWE.html

利用イメージ

（1）フィルタリング条件設定機能

MyJVNは、JVN iPediaに登録されている脆弱性対策情報のうち、利用者に関係する情報のみを表示できます。使用しているソフトウェアのベンダー名（図1）と製品名（図2）を選択すると、関連する脆弱性対策情報のみを表示します（図3）。

さらに、脆弱性対策情報一覧の中からひとつをクリックすると詳細な脆弱性対策情報を見ることができます（図4）。「脆弱性対策情報 詳細情報」画面では、影響を受けるシステムや影響を受けた時の深刻度、対策情報などが表示されます。

（2）自動再検索機能

一度フィルタリング条件を設定しておけば、2回目以降はアクセスするだけで同じ条件で検索を行いますので、（1）のベンダー名選択（図1）や製品名選択（図2）を再度設定する必要がありません。利用者はMyJVNの画面を開くだけで、常に自分に関係する最新の脆弱性対策情報を確認することができます。

図 1. ベンダー名選択画面

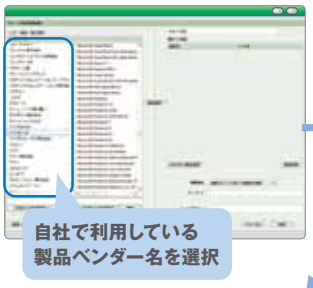


図 2. 製品名選択画面

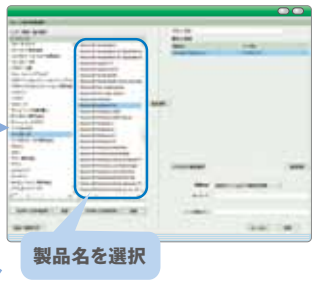


図 3. フィルタリングした脆弱性対策情報一覧画面

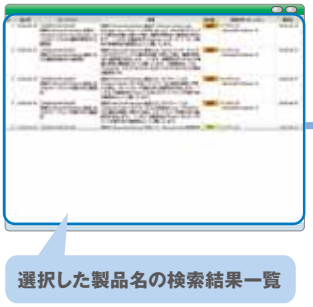
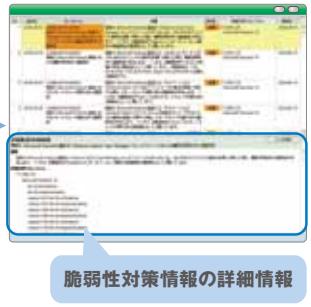


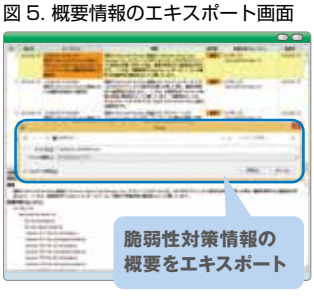
図 4. 脆弱性対策情報 詳細情報



（3）概要情報のエキスポート

エキスポートしたい脆弱性対策情報を選択し、概要情報をCSV形式でファイル保存（ファイル名：mjcheck３_YYYYMMDD.csv）できます（図5）。保存したファイルをメールに添付して送信したり、共有フォルダに保存することで関係者への情報の共有等に活用できます。

図 5. 概要情報のエキスポート画面



付録

ツール8

PCにインストールされているソフトウェア製品が最新のバージョンであるかを簡単な操作で確認
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html［.NET Framework 版］
https://jvndb.jvn.jp/apis/myjvn/vccheck.html［JRE 版］

MyJVN バージョンチェッカ

近年、特定の企業や組織の社員に向け、関係者を装ってウイルス添付メールを送信する攻撃（標的型攻撃）や、有名な企業や組織のウェブサイトを改ざんし、ウェブブラウザや動画再生ソフトなどのセキュリティ上の弱点（脆弱性）を狙う攻撃など、攻撃手法の多様化が進んでいます。これらの攻撃の多くは、古いバージョンのソフトウェアの脆弱性を悪用しています。

そこでIPAでは、簡単な操作でPCにインストールされているソフトウェア製品が最新のバージョンであるかを確認することができるツール「MyJVN バージョンチェッカ」を開発、公開しました。図1は「MyJVN バージョンチェッカ（JRE版）」の実行画面です。マウスクリックだけの簡単な操作で、複数のソフトウェア製品が最新のバージョンかどうかをチェックできます。

「MyJVN バージョンチェッカ」がチェック対象とするソフトウェア製品は表1の通りです。IPAは今後も脆弱性対策の処理の柔軟性と効率性を高めるとともに、チェック対象となる製品を拡充させていきます。「MyJVN バージョンチェッカ」の動作環境は表2の通りです。

図 1.「MyJVN バージョンチェッカ」実行画面

表 1. チェック対象製品

種別	ソフトウェア製品名	概要
クライアントOS向けアプリケーション	Adobe Flash Player (ActiveX, Plug-in)	動画再生ソフト
	Adobe Reader	PDFファイル閲覧ソフト
	Adobe Shockwave Player	動画再生ソフト
	JRE	Java実行環境
	Lhaplus	ファイル圧縮・解凍ソフト
	Mozilla Firefox	ウェブブラウザ
	Mozilla Thunderbird	メールソフト
	QuickTime	動画再生ソフト
	iTunes	音楽・動画管理ソフト
	Lunascape	ウェブブラウザ
	Becky! Internet Mail	メールソフト
	OpenOffice.org	文書編集ソフト
	VMware Player	仮想化ソフト
	Google Chrome	ウェブブラウザ
	LibreOffice	文書編集ソフト

2018年3月時点

表 2. 動作環境

OS	・Windows 7（32bit 版/64bit 版） ・Windows 8.1（32bit 版/64bit 版） ・Windows 10（32bit 版/64bit 版）
ブラウザ	Internet Explorer 7 以降 または Firefox 24 以降
実行環境	Java Runtime Environment 1.6.0 update12以降 または .NET Framework 4.6

2018年3月時点

ツール9 サイバーセキュリティ注意喚起サービス「icat for JSON（アイキャット･フォー･ジェイソン）」

近年、情報窃取が目的と考えられるサーバー攻撃が顕在化しています。組織のシステム管理者や個人利用者においては、迅速にセキュリティ対策情報を自ら入手し、システム（PCやサーバー）に対策を適用することが求められています。

IPAでは、広く普及しているソフトウェアや攻撃が確認された脆弱性の対策情報について、“重要なセキュリティ情報”としてウェブサイトに掲出するほか、メール配信により周知しています。その取り組みを促進するためにこれらの情報をリアルタイムにウェブサイト上に表示し確認ができる、サイバーセキュリティ注意喚起サービス「icat for JSON（アイキャット･フォー･ジェイソン）」を公開しました。「icat for JSON」の利用イメージは図1の通りです。

図1. icat for JSONの利用イメージ

機能概要

本ツールの特徴は以下の通りです。

- 表示方法は「縦表示」または「横表示」の指定が可能です
- 直近1週間以内の情報は、オレンジの背景色で強調しています
- HTMLタグのsrc属性にhttpsを付与します
（ただし、HTTPSで動作するウェブサイトの場合は不要です）

下記のHTMLタグをウェブページに記載することで図2～図4のように表示されます。

■例

```
<script type="text/javascript" src="https://www.ipa.go.jp/security/announce/irss/icath.js"> </script>
```

図3. 横表示1 <190×350pixel>

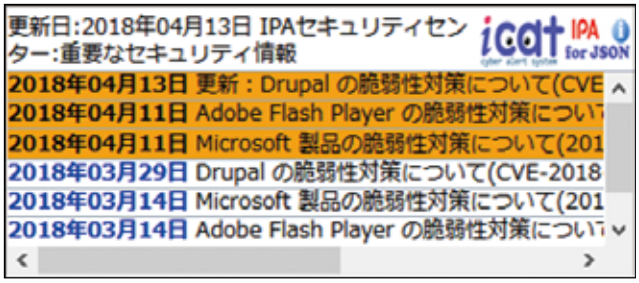
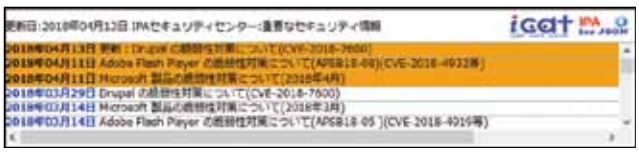


図2. 縦表示 <350×150pixel>

図4. 横表示2 <700×150pixel>



ツール10

ウェブサイトを狙った攻撃を簡単に検出できるツール
https://www.ipa.go.jp/security/vuln/iLogScanner/

ウェブサイトの攻撃兆候検出ツール「iLogScanner」

近年、ウェブサイトを狙った攻撃が増えています。サイト運営者は、ウェブサイトがどれほど攻撃を受けているか、また攻撃による被害が発生していないか、常に状況を把握し対策を検討する必要があります。

しかし、ウェブサイトへの攻撃状況を確認するには専門的なスキルが必要であり、一般のサイト運営者にとって簡単とは言えません。

「iLogScanner」はウェブサイトを狙った以下の兆候についてチェックすることが可能です。

■ ウェブサイトの脆弱性を狙った攻撃の兆候
- SQLインジェクション(*1)
- ディレクトリ・トラバーサル(*2)
- クロスサイト・スクリプティング(*3)など

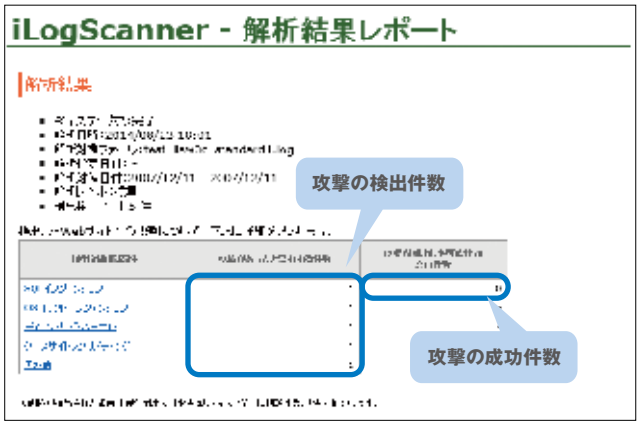
■ SSH/FTPなどメンテナンス用のアプリケーションを狙った不正アクセスの兆候
- 大量のログイン失敗(*4)
- 短時間の集中ログイン(*5)
- 組織外(指定IP外)からのアクセス(*6)など

チェック結果は任意のレポート形式(HTML、TEXT、XML形式)で確認することが可能です(図1)。サイト運営者や経営者は定期的にレポートを確認することで、自組織の狙われている状況を確認することができ、早期の対策をとる指標として活用できます。

iLogScannerは、手軽にブラウザ上で実行できるオンライン版およびバッチファイルと組み合わせて自動で実行可能なオフライン版の2種類の形態でご利用いただけます(図2)。

※iLogScannerは簡易ツールであり、攻撃と思われる痕跡をすべて網羅し、確実に検出するものではありません。また誤検出の場合もあります。iLogScannerで攻撃が検出された場合、ウェブサイトの開発者やセキュリティベンダーに相談されることをお勧めします。

図1. ウェブサイトを狙った脆弱性攻撃の解析結果レポート(HTML形式)



(*1) SQLインジェクション

SQLインジェクションとは、データベースと連携したウェブアプリケーションへ宛てた要求に悪意のあるSQL文を埋め込まれて(Injection)しまうと、データベースを不正に操作されてしまう問題です。これにより、重要情報が盗まれたり、情報が書き換えられたりする被害を受ける場合があります。

(*2) ディレクトリ・トラバーサル

ディレクトリ・トラバーサルとは、相対パス記法を利用して、管理者が意図しないウェブサーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、重要情報が盗まれたり、不正にアプリケーションを実行されるなどの危険があります。

(*3) クロスサイト・スクリプティング

クロスサイト・スクリプティングとは、ウェブサイトの掲示板などが、悪意あるスクリプト(命令)を訪問者のブラウザに送ってしまう問題です。これにより、悪意を持ったスクリプト(命令)を埋め込まれ、訪問者のブラウザ環境で実行されてしまう恐れがあります。その結果、cookieなどの情報の漏えいや意図しないページの参照が行われてしまいます。

(*4) 大量のログイン失敗

一定時間内に、同一のユーザIDで大量のログイン失敗があったことを検出します。パスワードを総当りで入力するなどの手段で不正アクセスを試みられている可能性があります。

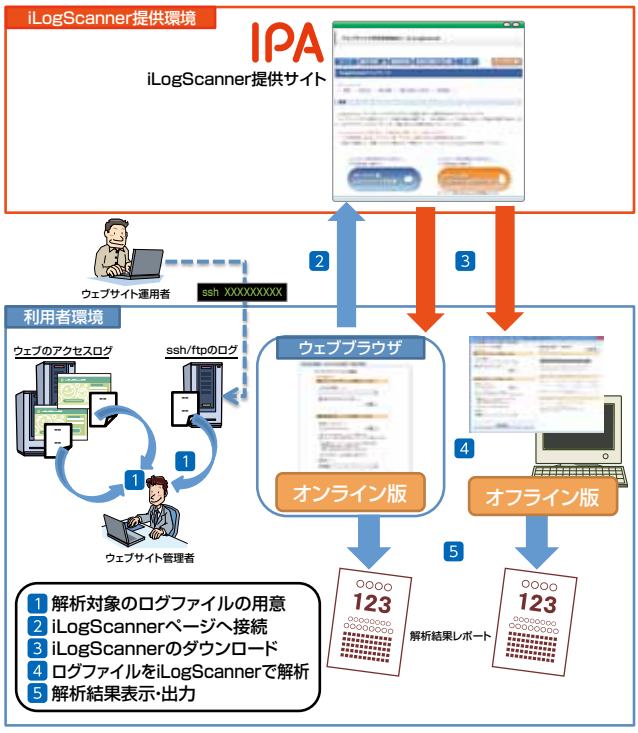
(*5) 短時間の集中ログイン

一定時間内に大量のログイン要求があったことを検出します。同一のパスワードでユーザIDを総当りで入力するなどの手段で不正アクセスを試みられている可能性や、サーバリソースに負荷をかける目的で大量アクセスが行われている可能性があります。

(*6) 組織外(指定IP外)からのアクセス

指定した範囲外のIPアドレス(自組織以外のIPアドレス等)からのアクセスを検出します。通常利用されないIPアドレスからのアクセスがあった場合、サーバに不正アクセスが試みられている可能性があります。

図2. iLogScanner利用イメージ



ツール11

JPEGテスト支援ツール「iFuzzMaker」

昨今、ソフトウェアは様々な製品に組み込まれ、多様な機能を実現させています。IPAでは、2011年8月から組込み製品に潜む脆弱性を低減させる取り組みを行っていますが、その一環で行った検証テストでは、JPEG画像を閲覧する機能に不都合をきたす可能性のある脆弱性を検出しました。

この機能の脆弱性によっては、JPEG画像を閲覧しただけで、ウイルスに感染したり外部から遠隔操作されたりする可能性があります。現在はパソコン用の画像表示や編集ソフトのみならず、スマートテレビなどの情報家電、スマートフォンやタブレットなどでもJPEG画像を閲覧できる機能が組み込まれており、組込み製品の中にも同様の脆弱性が意図せず作り込まれてしまう可能性があります。これらの製品は今後さらなる普及が見込まれることから、実害発生時の影響が懸念されます。

脆弱性の解消には、セキュリティテストの一つである「ファジング」が有効であり、このためのツールには商用製品やオープンソースソフトウェアなど複数あります。既存のツールのみではJPEG画像の閲覧機能に対しては十分なテストが難しいことが、先述のIPAでの検証テストの際に判明しました。「iFuzzMaker」は既存のテストツールの機能不足を補うことを目的としています。幅広く製品開発の関係者に活用されるよう、利用マニュアルとともにオープンソースソフトウェアとしてIPAのWebサイトで公開しました。

図1.「iFuzzMaker」利用の流れ

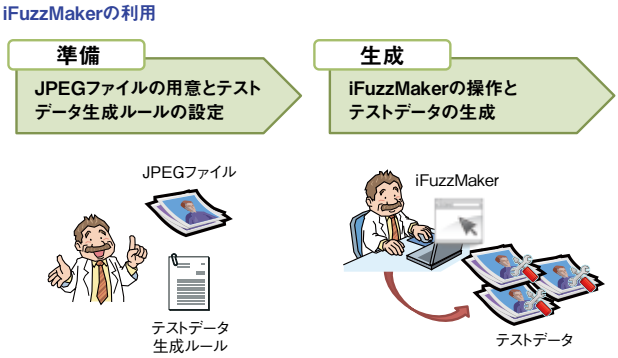
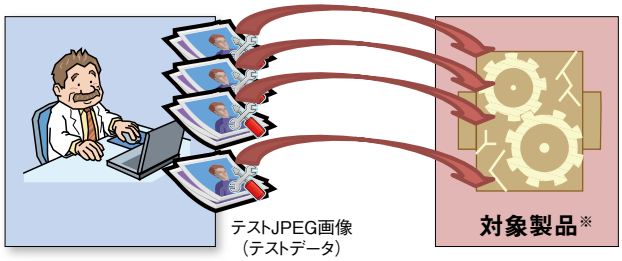


図2.「JPEG 画像を読み込む機能」に対するセキュリティテスト「ファジング」のイメージ

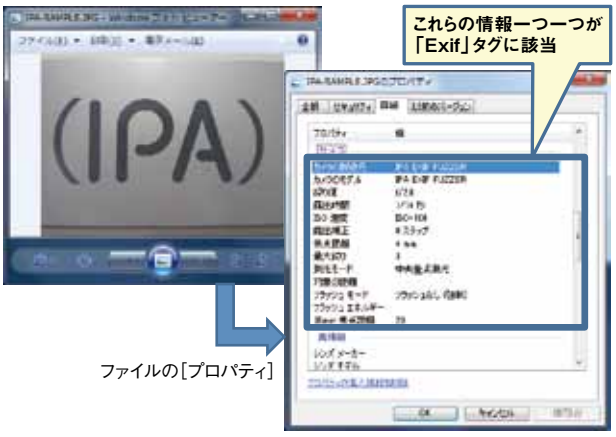


※:「JPEG画像を読み込む機能」を持つ製品

JPEGテスト支援ツール「iFuzzMaker」の概要

対象利用者	JPEG画像を扱う情報家電やソフトウェア製品の関係者 （開発者や品質保証担当者などを想定）
動作環境	OS　：Windows 7 SP1 Windows 8.1 Windows 10 ※上記OSは32bit版/64bit版共に動作を確認しております。 CPU　：1GHz以上のx86互換プロセッサ メモリ：1GB以上の空きメモリ HDD　：1GB以上の空き領域
機能	・JPEG画像を読み込む機能に対するファジングで使う、テストJPEG画像を作ること ・利用者が指定した値をExifタグに持つJPEG画像を作ること

図3. Exif タグの例



付録

ツール12

情報漏えい対策ツール

情報漏えい対策ツールは、ファイル共有ソフト（Winny、Winnyp、Share）による『情報漏えい』を防ぐためのソフトウェアです。例えば、家族で共有している自宅のパソコンや企業・組織のパソコンに情報漏えい対策ツールをインストールすることで、そのパソコン上におけるファイル共有ソフトの実行を禁止することができます。 また、企業や組織等の情報漏えい対策で、自宅のパソコンにファイル共有ソフトがインストールされていないことを証明する用途にも利用できます。

機能

次の４つの機能があります。

- ファイル共有ソフト（Winny、Winnyp、Share）の有無のチェックおよび起動防止
- ファイル共有ソフト経由での、ウイルスの疑いのあるファイルダウンロードを防止
- ファイル共有ソフトでの、ウイルス等の中継を防止
- ファイル共有ソフトを介した、パソコンからの情報漏えいを防止

図１.「情報漏えい対策ツール」起動画面

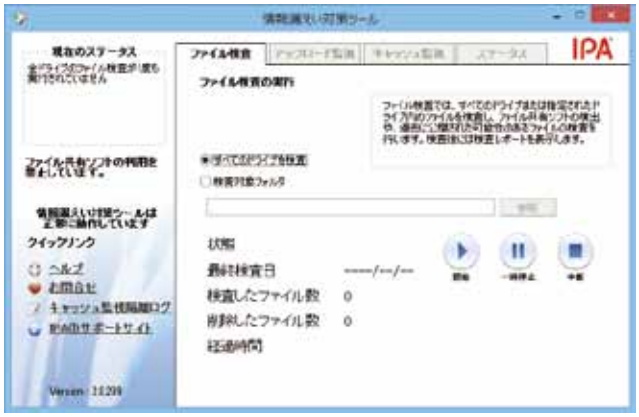


図２. ファイル共有ソフト起動検出時の警告画面

入手方法

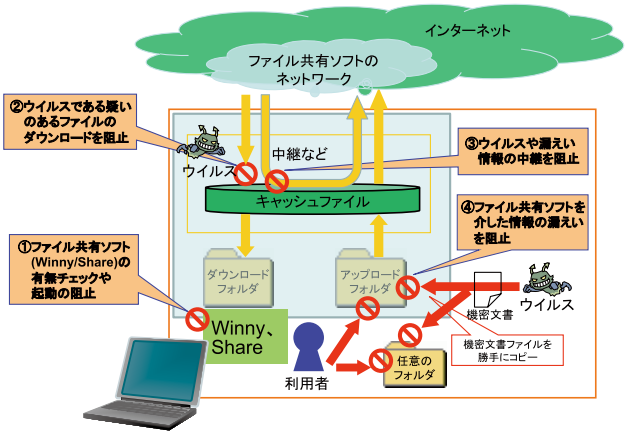
Vectorのソフトウェアライブラリから無料でダウンロードできます。

http://www.vector.co.jp/soft/winnt/util/se501912.html

詳細はIPAのWebサイトをご覧ください。

https://www.ipa.go.jp/security/winny119/

図３.「情報漏えい対策ツール」動作概要図



「情報漏えい対策ツール」の概要

動作環境	OS　：Windows 10（32bit、64bit） Windows 8.1（32bit、64bit） Windows 7 SP1（32bit、64bit） CPU　：Pentium Ⅱ以上の性能を持つもの、もしくはその互換CPU メモリ：256MB以上の空きメモリ インストールに必要なHDD容量：150MB
対応するファイル共有ソフト	・Winny 2.0b7.1 ・Winnyp 2.0b7.28 ・Share 1.0 EX2

ツール13

セキュリティ要件確認支援ツール

情報システムの企画、調達、設計、構築、運用等を実施するには、機能要件やサービス要件等の適切な定義・実現とともに、リスク等を考慮したセキュリティ要件の定義も重要です。しかし、そのためには、専門知識や経験等が要求されるため、セキュリティに詳しくない担当者にとっては、相当な困難を伴います。また、検討不足により、情報システムのセキュリティレベルが低下してしまう恐れもあります。

セキュリティ要件確認支援ツールは、このような問題を解決するため、情報システムの企画、調達、設計、構築、運用等の各場面で、調達対象となる機能・サービスに応じた情報システムのセキュリティ要件定義を容易に確認することを目的としたツールです。

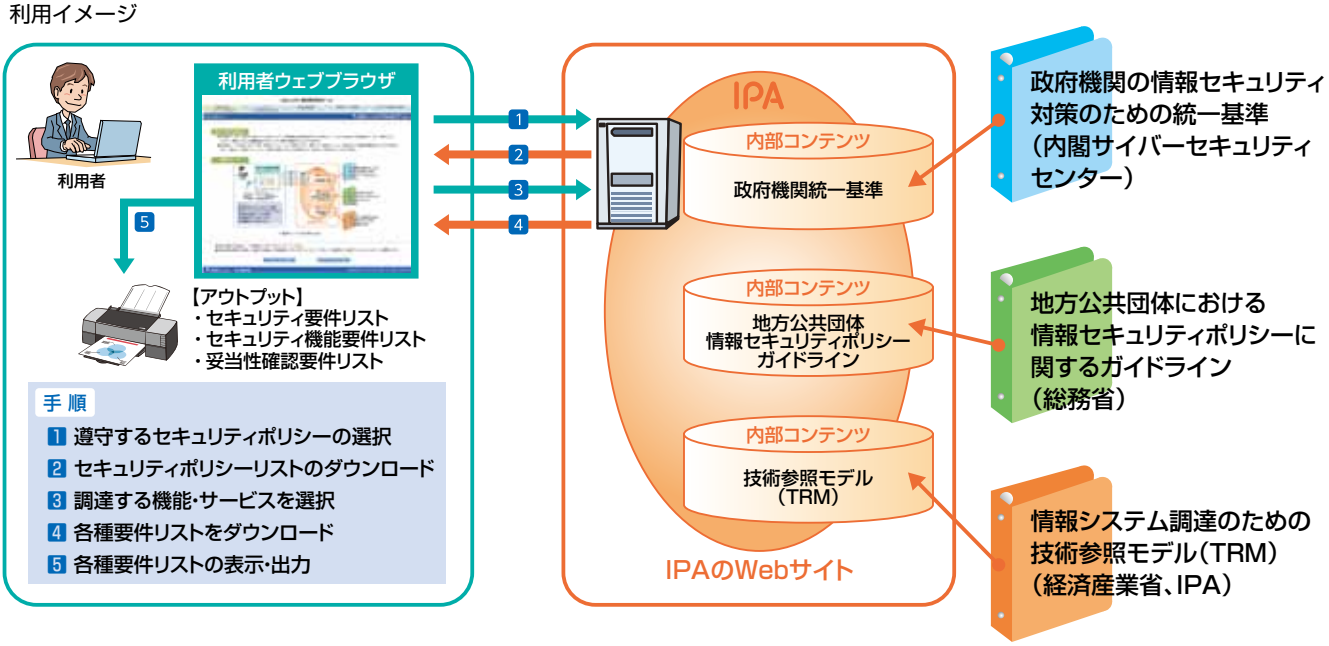
本ツールは、情報システムの調達担当者などが、IPAのウェブサイトから技術参照モデル（TRM※1）で定義された「機能・サービス」を入力することで、必要な「セキュリティ要件」（「政府機関の情報セキュリティ対策のための統一基準」※2または「地方公共団体における情報セキュリティポリシーに関するガイドライン」※3）に関する情報や、情報システムを構成する機器の「セキュリティ機能要件」に関する情報などを提供します。出力された情報を参考にシステムのセキュリティ要件を検討することで、自組織のセキュリティポリシーと適合し、かつ必要なセキュリティ機能を満足するシステム構築が実現できます。

※1 TRM（Technical Reference Model）
情報システムを技術ドメインおよび機能・サービスごとにモデル化して必要な機能要件をまとめた技術体系の定義集
https://www.ipa.go.jp/osc/trm/index.html

※2 政府機関の情報セキュリティ対策のための統一基準
http://www.nisc.go.jp/active/general/index.html

※3 地方公共団体における情報セキュリティポリシーに関するガイドライン
http://www.soumu.go.jp/denshijiti/jyouhou_policy/index.html

利用イメージ



付録

IPAコンクール応援隊長
「まもるくん」

第13回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017 受賞作品

インターネットを利用して、子どもたちが新たな「つながり」を形成し始めています。しかしそれが思わぬトラブルを生じさせていることも事実です。「誰と」つながるのか、ネットから得た情報を「正しく活用」できているか、また、発信した情報の「影響力を想定」できているかなど、子どもたちもインターネット利用者としての注意が必要です。

これらの問題に、子どもたちが自ら向き合い、解決策を見出すきっかけとして、情報セキュリティ意識の向上となるような作品を全国の小学生・中学生・高校生・高専生を対象に募集しました。

最優秀賞

〈独立行政法人情報処理推進機構〉

＝ 標語部門 ＝

わたしのひみつだいじにしよう　あなたのひみつものぞかない

鹿児島県　鹿児島市立伊敷小学校　1年　**早﨑 夕璃**さん

＝ ポスター部門 ＝

徳島県　徳島市加茂名南小学校　2年
岡本 彩佐さん

＝ 4コマ漫画部門 ＝

岐阜県　岐阜県立岐南工業高等学校　1年
坪内 祐太朗さん

標語部門　優秀賞

〈北海道警察サイバーセキュリティ対策本部〉
パスワード　またそれ使う？　危ないよ
北海道　北海道札幌北高等学校　定時制　1年
谷口 優里菜さん

〈青森県警察本部生活安全部保安課〉
合い言葉（パスワード）　スマホと2人の　秘密だよ
青森県　むつ市立むつ中学校　1年
坪 優希さん

〈岩手県警察本部生活環境課〉
パスワード　自分で作る　防衛軍
岩手県　花巻市立花巻北中学校　3年
千葉 陽太さん

〈宮城県警察本部サイバー犯罪対策課〉
戻れない　あの日の書き込み　永遠に
宮城県　大崎市立田尻中学校　2年
佐野 美恵さん

〈一般社団法人宮城県情報サービス産業協会〉
ネット依存　気づいてないのは　自分だけ
宮城県　宮城県涌谷高等学校　1年
加藤 大晴さん

〈秋田県警察本部生活安全部〉
一文字で　関係消滅!!　戻れない
秋田県　仙北市立角館中学校　2年
大信田 ななかさん

〈一般社団法人秋田県情報産業協会〉
コメントは　ネットの中を　旅してる
秋田県　秋田市立下浜中学校　3年
納家 聖弥さん

〈山形県警察本部生活安全部生活環境課〉
「ごめんなさい」　ことばで伝えて　文字でなく
山形県　山形県立酒田光陵高等学校　1年
田岡 蘭さん

〈茨城県警察本部生活安全部サイバー犯罪対策課〉
気づいてる　もうけせないよ　書きこみは
茨城県　つくば市立竹園東小学校　4年
西野 健太さん

〈茨城県教育庁学校教育部高校教育課〉
朝眠い　昼も眠くて　夜スマホ
茨城県　茨城県立並木中等教育学校　1年
杉山 諒丞さん

〈茨城県教育庁学校教育部義務教育課〉
情報社会　自分の心に　セキュリティ
茨城県　神栖市立矢田部小学校　5年
安藤 成真さん

〈茨城県メディア教育指導員連絡会〉
情報選択　最後はやっぱり自己責任
茨城県　清真学園高等学校　1年
中島 一翔さん

〈茨城県情報通信ネットワークセキュリティ協議会〉
大丈夫？　他のと同じ　パスワード
茨城県　茨城県立下妻第二高等学校　2年
内田 輝弥さん

〈栃木県警察本部生活安全部生活環境課〉
文字だけの　甘い言葉に　要注意
栃木県　宇都宮市立晃陽中学校　3年
荒井 奈都美さん

〈群馬県警察本部生活安全部サイバー犯罪対策課〉
SNS　見えない相手は　落とし穴
群馬県　渋川市立金島小学校　5年
松村 侑真さん

〈埼玉県警察本部生活安全部サイバー犯罪対策課〉
今もある　消したはずの　その情報
埼玉県　熊谷市立大里中学校　2年
齊藤 幸葵さん

〈公益社団法人埼玉県情報サービス産業協会〉
送ったら　戻らぬ　帰らぬ　あなたの言葉
埼玉県　立教新座高等学校　2年
安藤 颯人さん

〈千葉県警察本部生活安全部サイバー犯罪対策課〉
ネットでの　信頼関係　ほんとかな？
千葉県　鎌ケ谷市立鎌ケ谷中学校　3年
吉田 陽向子さん

〈千葉県高等学校教育研究会情報教育部会〉
その画像　使っていいの？　人のかも
千葉県　鎌ケ谷市立鎌ケ谷中学校　3年
石井 華椰さん

〈東京情報大学〉
幸せより　炎上運ぶ　青い鳥
千葉県　千葉県立八千代東高等学校　2年
関口 瑠美奈さん

〈神奈川県警察本部生活安全部サイバー犯罪対策課〉
君の名は　見知らぬ人が　なりすまし　入れかわってる　ネットの私
神奈川県　神奈川県立相模原総合高等学校　1年
安藤 真路さん

〈新潟県警察本部サイバー犯罪対策課〉
一度書く　悪口メールは　もう消えない
新潟県　加茂市立葵中学校　1年
髙橋 ひかるさん

〈石川県警察本部生活環境課〉
ホントにいいの？　ずっと残るよ　その言葉
石川県　石川県立小松明峰高等学校　1年
谷 大地さん

〈一般社団法人石川県情報システム工業会〉
パスワード　スマホも口も　鍵かける
石川県　石川県立小松明峰高等学校　1年
嶋 亜弥梨さん

〈山梨県警察本部生活安全部生活安全捜査課〉
大丈夫？　その表現と　その画像
山梨県　山梨県立身延高等学校　3年
清水 涼雅さん

〈長野県警察本部生活環境課〉
時と場所　モラルを守れ　スマートフォン
長野県　松本市立丸ノ内中学校　1年
秋葉 楓さん

〈一般社団法人長野県情報サービス振興協会〉
やっていい事　悪い事　ネットの中でも同じだよ
長野県　長野市立加茂小学校　4年
田邉 心蒔さん

〈長野県インターネットプロバイダ防犯連絡協議会〉
SNS　日記とちがう　危険です
長野県　長野市立加茂小学校　6年
今井 咲枝さん

〈ネット安全・安心ぎふコンソーシアム〉
クリック前　いったん落ちつき　よくみよう。
岐阜県　関市立武芸川中学校　2年
飯沼 歩夢さん

〈静岡県警察本部生活安全部サイバー犯罪対策課〉
気をつけて　相手がみえない　恐ろしさ
静岡県　函南町立函南中学校　2年
相馬 桜渚さん

〈三重県警察本部生活安全部サイバー犯罪対策課〉
家族一人一人の　安全を守るため　話し合おう　セキュリティ対さく
三重県　いなべ市立石榑小学校　4年
楠 亜花さん

〈滋賀県警察本部サイバー犯罪対策課〉
フォロワーが　増えてもあなたは　偉くない
滋賀県　大津市立北大路中学校　3年
東 香織さん

〈京都府警察本部サイバー犯罪対策課〉
よくみてね　それは本当の　事実かな
京都府　京都市立大宮小学校　6年
岸田 妃代さん

〈京都市教育委員会〉
スマホではうそか本当か分からない
京都府　京都市立大宮小学校　6年
仲田 早穂さん

〈一般社団法人京都府情報産業協会〉
なりすまし　焦るな落ち着け　まず確認
京都府　京都府立北嵯峨高等学校　1年
芳井 千珠さん

〈公益社団法人京都府防犯協会連合会〉
その一瞬　一生ネットで　さらされる
京都府　京田辺市立培良中学校　3年
梅澤 天我さん

〈京都府私立中学高等学校情報科研究会〉
ネット社会　気づかぬ場所から　闇社会
京都府　ノートルダム女学院高等学校　1年
沖潮 百代さん

〈京都コンピュータ学院〉
画面上　文字は読めても　心は読めない
京都府　舞鶴市立城北中学校　1年
小﨑 聖也さん

〈京都情報大学院大学〉
大丈夫?　正しい情報　再確認
京都府　舞鶴市立青葉中学校　3年
竹野 羽菜さん

〈大阪府警察本部サイバー犯罪対策課〉
ツイートは　一生消えない　独り言
大阪府　大阪府立泉北高等学校　1年
松尾 華音さん

〈兵庫県警察本部サイバー犯罪対策課〉
クリックを　1回押すと　別世界
兵庫県　雲雀丘学園小学校　6年
田村 紗愛さん

〈奈良県警察本部サイバー犯罪対策課〉
消せないよ　感情まかせに　打った文字
奈良県　斑鳩町立斑鳩中学校　3年
増谷 百香さん

〈特定非営利活動法人奈良地域の学び推進機構〉
その発言　匿名だからと　軽はずみ
奈良県　斑鳩町立斑鳩中学校　3年
広瀬 美律さん

〈和歌山県警察本部生活安全部生活環境課〉
知ってるの?　スマホの先の　人のこと
和歌山県　和歌山市立東和中学校　3年
青木 真結さん

〈島根県警察本部生活安全部生活環境課〉
分かったぞ　誕生日だな　パスワード
島根県　益田市立鎌手中学校　3年
川﨑 元気さん

〈一般社団法人島根県情報産業協会〉
インターネット　遊び半分で書いた一言は、もう消えない
島根県　美郷町立邑智中学校　1年
竹内 紫奈乃さん

〈岡山県警察本部サイバー犯罪対策課〉
SNS　油断がいつしか　SOS
岡山県　岡山大学教育学部附属中学校　2年
笹野 裕矢さん

〈一般社団法人システムエンジニアリング岡山〉
パスワード　覚えやすさは　命とり
岡山県　岡山市立石井中学校　3年
山本 海璃さん

〈広島県警察本部生活安全部サイバー犯罪対策課〉
「ネタだから」　ネタじゃすまない　こともある
広島県　広島市立広島商業高等学校　3年
中本 紗綾さん

〈一般社団法人広島県情報産業協会〉
こまったら　大人に相談　なやまずに
広島県　呉市立昭和中央小学校　6年
渡邊 ほのかさん

〈広島県インターネット・セキュリティ対策推進協議会 〉
ネットでは　好奇心より　警戒心
広島県　熊野町立熊野中学校　1年
片岡 あいさん

〈山口県警察本部生活安全部生活環境課〉
ついてくる　あなたの過去が永遠に
山口県　山口県立長府高等学校　1年
上田 凜花さん

〈徳島県警察本部サイバー犯罪対策室〉
インターネット　情報正しさ　見きわめて
徳島県　阿波市立阿波中学校　3年
福井 蒼哉さん

〈一般社団法人徳島県情報産業協会〉
このサイト　どうしてあるの？　ぼくの写真
徳島県　徳島市津田小学校　5年
林 創太さん

〈公益財団法人e－とくしま推進財団〉
パスワード　気軽につけずに　大切に
徳島県　小松島市小松島南中学校　1年
新田 拓実さん

〈情報通信交流館〉
「教えない」　自分の心を　守るかぎ
香川県　東かがわ市立白鳥中学校　2年
岡本 香乃さん

〈かがわ情報化推進協議会〉
ネットでは　リセットボタンは　ありえない
香川県　東かがわ市立白鳥中学校　2年
岡部 大さん

〈愛媛県警察本部生活環境課〉
あやしくて　危険なサイトは　ノータッチ
愛媛県　久万高原町立久万中学校　1年
濵口 康介さん

〈愛媛県情報サービス産業協議会〉
ネットも　リアルも　マナーが大事
愛媛県　聖カタリナ学園高等学校　1年
武田 洋則さん

〈高知県警察本部生活安全部〉
その書きこみ　もう消せないよ　大丈夫?
高知県　南国市立久礼田小学校　6年
安岡 桃香さん

〈一般社団法人高知県情報産業協会〉
気をつけて　心も体も　ネットにスマホに奪れる
高知県　香南市立赤岡中学校　3年
大庭 葵さん

〈福岡県警察本部生活安全部サイバー犯罪対策課〉
知らぬうち　知らぬ誰かに　知られてる
福岡県　福岡県立小倉南高等学校　2年
北井 桜咲さん

〈佐賀県警察本部生活安全部生活環境課〉
ネットはさ　便利だけれど　穴だらけ　詐欺の罠に気を付けて
佐賀県　佐賀県立盲学校　3年
古賀 建成さん

〈特定非営利活動法人ITサポートさが〉
スマートフォン、笑わせるの？　きずつけるの?
佐賀県　小城市立牛津小学校　5年
山田 睦美さん

〈一般社団法人長崎県情報産業協会〉
気づいてね　SNSの危険性
長崎県　松浦市立志佐中学校　2年
大村 武弘さん

〈長崎県ネットワーク・セキュリティ連絡協議会〉
書き込みは　その後の未来も　左右する
長崎県　諫早市立諫早中学校　3年
江島 彩さん

〈熊本県警察本部生活安全部サイバー犯罪対策課〉
考えて　自撮りアップの　危険性
熊本県　水俣市立袋中学校　3年
田上 佐和さん

〈大分県警察本部生活環境課〉
向かい合い　文字より言葉で　話そうよ
大分県　日本文理大学附属高等学校　1年
衛藤 昇王さん

〈大分県情報サービス産業協会〉
顔文字は　ほんとの気持ちじゃ　ないかもね
大分県　日本文理大学附属高等学校　2年
川野 なずなさん

〈宮崎県警察本部生活安全部サイバー犯罪対策課〉
パスワード　分かりづらい程　心強い
宮崎県　宮崎市立赤江中学校　3年
新田 陽光さん

〈鹿児島県警察本部生活安全部生活環境課〉
もれてます　あなたのじょうほう　写真から
鹿児島県　鹿児島市立伊敷小学校　4年
田代 梨乃さん

〈鹿児島市教育委員会 学習情報センター〉
自分の価値は　いいねの数では　決まらない
鹿児島県　鹿児島市立東谷山中学校　3年
宝満 耀太さん

〈一般社団法人鹿児島県情報サービス産業協会〉
歩きスマホ　大人がたいど　みせようよ
鹿児島県　鹿児島市立宇宿小学校　3年
箱丸 晴士さん

〈特定非営利活動法人ITかごしま支援隊〉
きずつけないで　大切な人と　大切なじょうほう
鹿児島県　鹿児島市立石谷小学校　4年
新藏 花幸さん

〈特定非営利活動法人鹿児島インファーメーション〉
君の打つ　ささいな言葉が　針となる
鹿児島県　鹿児島玉龍高等学校　1年
廣田 有紀さん

〈沖縄県警察本部サイバー犯罪対策課〉
違法じゃない？　あなたが見てる　その映画
沖縄県　昭和薬科大学附属中学校　2年
柳原 琉音さん

〈沖縄県情報通信関連産業団体連合会〉
一行で　生まれるイジメ　消える未来
沖縄県　昭和薬科大学附属中学校　2年
楠 拓也さん

〈特定非営利活動法人フロム沖縄推進機構〉
ははがいう　あんたのともだち　スマホなの?
沖縄県　沖縄県立那覇商業高等学校　3年
知念 早希さん

ポスター部門　優秀賞

〈一般社団法人
コンピュータソフトウェア著作権協会〉

和歌山県 和歌山市立和歌山高等学校 3年

小阪 碧さん

〈一般社団法人 JPCERT コーディネーションセンター〉

宮崎県 宮崎県立佐土原高等学校 3年

長友 日向子さん

〈一般社団法人情報サービス産業協会〉

愛知県 刈谷市立依佐美中学校 3年

北川 桃子さん

〈一般社団法人
全国地域情報産業団体連合会〉

長崎県 長崎県立佐世保北高等学校 1年

山領 駿斗さん

〈特定非営利活動法人
IT コーディネータ協会〉

香川県 香川県立高松工芸高等学校 2年

實川 愛理さん

〈特定非営利活動法人
日本ネットワークセキュリティ協会〉

長野県 南箕輪村立南箕輪中学校 1年

中村 新さん

〈デジタルアーツ株式会社〉

岐阜県 下呂市立萩原北中学校 3年

岩嶋 百伽さん

〈トレンドマイクロ株式会社〉

東京都 聖学院小学校 6年

治田 慶さん

〈マカフィー株式会社〉

千葉県 千葉市立幕張本郷中学校 3年

牧野 佳南さん

〈札幌市教育委員会〉

北海道 札幌市立新川西中学校 2年

酒井 梨緒さん

〈公益財団法人
仙台応用情報学研究振興財団〉

宮城県 宮城県涌谷高等学校 2年

今野 志保さん

〈秋田県教育委員会〉

秋田県 秋田県立矢島高等学校 1年

高橋 優奈さん

〈茨城県知事公室女性青少年課〉

茨城県 つくば市立吾妻中学校 2年

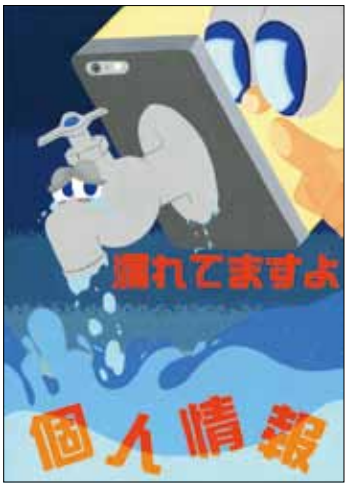
長谷川　志歩さん

〈警視庁生活安全部サイバー犯罪対策課〉

東京都 東京都立工芸高等学校 3年

髙橋 倭生さん

〈一般社団法人
山梨県情報通信業協会〉



山梨県 駿台甲府高等学校 2年

長田 ひかりさん

〈長野県青少年インターネット適正利用推進協議会〉

長野県 長野県須坂高等学校 2年

廣瀬 ジュリアさん

〈特定非営利活動法人
ふじのくに情報ネットワーク機構〉

静岡県 静岡県立浜松工業高等学校 3年

髙林 あいりさん

〈滋賀県警察本部警務部〉

滋賀県 大津市立北大路中学校 2年

森野 湖春さん

〈京都府教育委員会〉

京都府 京都府立大江高等学校 2年

田中 天花さん

〈大阪私学教育情報化研究会〉

大阪府 大阪府立三国丘高等学校 1年

梅田 大夢さん

〈鳥取県警察本部生活安全部〉

鳥取県 鳥取県立鳥取湖陵高等学校 3年

田渕 梨花さん

〈香川県教育委員会〉

香川県 大手前丸亀中学校 2年

白川 さくらさん

〈高知県教育委員会〉

高知県 高知商業高等学校 3年

小田 理央さん

〈福岡県教育委員会〉

福岡県 真颯館高等学校 3年

森 奈々さん

〈長崎県警察本部〉

長崎県 長崎県立佐世保北高等学校 1年

酒元 菜々さん

〈一般社団法人宮崎県情報産業協会〉

宮崎県 宮崎市立檍中学校 3年

御筆 満里奈さん

〈沖縄県〉

沖縄県 沖縄県立豊見城高等学校 3年

上原 千忠さん

4コマ漫画部門　優秀賞

〈警察庁〉

メアド泥棒にご用心 !!

福島県 会津美里町立高田中学校 3年

佐藤 小雪さん

〈一般社団法人組込みシステム技術協会〉

誰と出かけてるの？

大阪府 大阪府立泉北高等学校 1年

土師 未珠穂さん

〈一般社団法人コンピュータソフトウェア協会〉

アップする前に確認 !!

埼玉県 埼玉県立草加東高等学校 2年

増田 未夢さん

〈一般社団法人日本教育情報化振興会〉

信頼無くすよね…。

兵庫県 加古川市立中部中学校 3年

福原 咲来さん

〈一般社団法人日本情報システム・ユーザー協会〉

友達になりたかったのに…

岡山県 岡山市立岡北中学校 3年

薬師寺 宏行さん

〈公益社団法人日本PTA全国協議会〉

スマホ依存。

兵庫県 西宮市立浜脇中学校 3年

薩美 友希さん

〈フィッシング対策協議会〉

本当の情報 !?

愛知県 愛知県立豊田東高等学校 1年

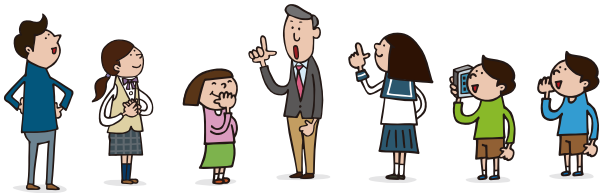
川合 杏奈さん

〈モバイルコンピューティング推進コンソーシアム〉

どこにいても…

愛知県 愛知県立豊田東高等学校 1年

金松 瑞季さん



〈株式会社ウェブテクノロジ・コム〉

携帯電話を拾った

京都府 京都女子高等学校 3年

橋本 菜々子さん

〈ウォッチガード・テクノロジー・ジャパン株式会社〉

内緒のつもりが…

兵庫県 西宮市立浜脇中学校 3年

犬塚 紗弥さん

〈株式会社カスペルスキー〉

ウイルス感染

福島県 福島大学附属中学校 1年

八巻 沙和さん

〈実教出版株式会社〉

SNS の相手は…？

静岡県 静岡県立三島南高等学校 1年

本間 友紀乃さん

〈株式会社シマンテック〉

いいね！

大阪府 大阪府立三島高等学校 2年

小川 桃佳さん

〈ソースネクスト株式会社〉

アップデートはこまめに！

埼玉県 埼玉県立草加東高等学校 3年

齊藤 菜美さん

〈株式会社ディー・エヌ・エー〉

顔の見えない相手

兵庫県 西宮市立浜脇中学校 3年

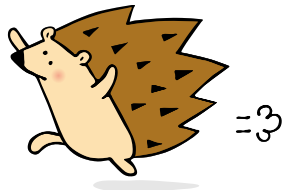
辻本 めいさん

〈株式会社ネットワールド〉

ながらスマホ

宮崎県 宮崎市立赤江中学校 3年

佐藤 留華さん



〈BBソフトサービス株式会社〉

リンクの裏側

岡山県 岡山大学教育学部附属中学校 1年

秋山 創太さん

〈LINE株式会社〉

ログアウト

岐阜県 岐阜県立岐南工業高等学校 1年

柴田 舞華さん

〈株式会社ラック〉

SNS の信頼性

千葉県 千葉県立安房拓心高等学校 3年

渡辺 実華さん

〈一般社団法人北海道情報システム産業協会〉

「笑」ってる？

北海道 北海道帯広柏葉高等学校 2年

鳥倉 捺央さん

〈一般社団法人東京都情報産業協会〉

その情報、信じて良いの？

東京都 筑波大学附属中学校 3年

横山 七海さん

〈特定非営利活動法人東海インターネット協議会〉

画像の無断使用は…？

愛知県 名古屋市立緑高等学校 1年

阪野 琳香さん

〈岡山県情報セキュリティ協議会〉

一枚の写真

岡山県 岡山大学教育学部附属中学校 2年

葛西 珠子さん

〈鹿児島県教育委員会〉

注意不足は漏洩の元

鹿児島県 鹿児島市立明和中学校 3年

宮薗 華和さん

索引

さ

おわりに

2017年度は、世界規模でのWanna Cryptorによるサービスや業務の停止、国内外でのビジネスメール詐欺や仮想通貨取引所への不正アクセスによる多額の金銭被害の発生等、サイバー攻撃が事業に大きく影響を与えており、見えていた脅威が更に深刻化したと言える年でした。本白書のサブタイトルである「深刻化する事業への影響:つながる社会で立ち向かえ」は、こうした脅威に対して、個人・組織が注意して自らを守るだけでなく、皆が結びついて社会全体を守っていくという意識を持つ必要がある、という思いでつけています。

「情報セキュリティ白書2018」は、IPAの職員を中心に、多岐にわたる情報セキュリティに関する国内外の事象や動向を調査・分析し、読者の方々に伝わるよう分かりやすい解説を心掛けて作成しました。本白書が、皆様のサイバーセキュリティへの関心を一層芽生えさせ、つながる社会を形成する一助となれば幸いです。

編集子

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　江口 純一　小川 隆一　竹腰 智

執筆者

IPA

江口 純一	金野 千里	桑名 利幸	松坂 志	加賀谷 伸一郎
山里 拓己	時田 俊雄	西尾 秀一	小川 隆一	渡辺 貴仁
土屋 正	辻 宏郷	工藤 誠也	徳竹 敬一	中島 尚樹
黒谷 欣史	山﨑 知嗣	板橋 博之	熊谷 悠平	竹村 純輝
田中 里実	猪城 明	堀江 亘	岡下 博子	大塚 龍彦
鹿野 一人	竹内 智子	立花 里奈	浜本 翔太郎	亀山 友彦
吉本 賢樹	渡邉 祥樹	唐亀 侑久	吉田 和之	塚元 卓
甲斐 成樹	櫻井 玄弥	近澤 武	小暮 淳	神田 雅透
九嶋 真衣子	江島 将和	奥田 美幸	大谷 祐子	畑野 元
深谷 貴宣	市ノ渡 佳明	島田 毅	佐川 陽一	小山 明美
木内 直人	島 成佳	圓道 なおみ	伊藤 千絵	田村 滋基
野澤 裕一	竹腰 智			

JPCERT コーディネーションセンター　内田 有香子

協力者　（以下、氏名 50 音順）

相羽 律子	株式会社日立製作所
小谷 誠剛	富士通株式会社
堀 洋平	国立研究開発法人産業技術総合研究所
吉岡 克成	横浜国立大学

経済産業省商務情報政策局サイバーセキュリティ課

JPCERT コーディネーションセンター

情報セキュリティ白書 2018

深刻化する事業への影響：つながる社会で立ち向かえ

2018 年 7 月 17 日　第 1 版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**
〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7550（セキュリティセンター）
Fax　03-5978-7546（セキュリティセンター）
E-Mail isec-wp-book@ipa.go.jp

印刷・製本　**岩橋印刷株式会社**

表紙デザイン／本文 DTP・編集サポート　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平、岩田 直也**