情報セキュリティ白書

Information Security White Paper

2019

新しい基盤、巧妙化する攻撃：未知のリスクに対応する力を

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2019」の刊行にあたって

東京 2020 オリンピック・パラリンピック競技大会を 2 年後に控えた 2018 年度には、重要インフラのセキュリティ強化、IoT 機器の脆弱性の把握、企業経営層のセキュリティリスク管理への参画等、様々な分野でセキュリティ対策が進展しました。しかしその一方で、ランサムウェアや IoT 機器を狙ったサイバー攻撃、人間の弱点を狙ったネット上の詐欺等の手法は、更に巧妙化を続けています。2018 年度も、ビジネスメール詐欺、フィッシングや偽警告等の詐欺攻撃の被害は後を絶ちませんでした。海外に目を移せば、大規模な情報流出やランサムウェアによる被害等は引き続き起きています。対策が進んだので今後はセキュリティリスクが小さくなる、と考えるのは早計であると思います。

実際、守るべき対象はサイバー世界とフィジカル世界の融合により大規模化・複雑化しています。「情報セキュリティ 10 大脅威 2019」において、「サプライチェーンへの攻撃」が 4 位となり、つながる社会のセキュリティリスク管理の難しさが明らかになりました。IPA の調査によれば、サプライチェーン上のセキュリティ対策の把握は直接の取引先以外は難しい、取引先とのセキュリティ対策に関する取り決めが十分なされていない、等の課題が確認されています。リスクの可視化と情報共有、中小企業を含めたサプライチェーン上のセキュリティ対策等、やるべきことはたくさんあります。

2018 年度はまた、AI やキャッシュレス決済の急速な普及が実感された年でもあります。当然ながら、AI やキャッシュレス決済の普及を後押しするために、それぞれのサービスの脆弱性を把握し、起こりうる攻撃、あるいは悪用のリスクを正しく見定め、対応する必要があります。

これから東京 2020 オリンピック・パラリンピック競技大会、AI やキャッシュレス決済の普及、デジタル・トランスフォーメーションの本格化等で新しい IT 基盤によるサービスが次々と実用化されることでしょう。そうしたサービスを安全に利用するためにも、私達はそのサービスで生じうるリスクは何か、提供されるデータやシステムは信頼できるか、等を考えることが求められます。もちろんこれは容易ではありませんが、サービス提供者、利用者、セキュリティ専門家等がそれぞれの立場でリスクやその対処の方法について考え、少しずつでも情報を共有していくことが大変重要であると思います。

本白書が、多くの方々に広く利用され、このような未知のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2019年8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

序章　2018年度の情報セキュリティの概況 …… 6
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 …… 8
1.1 2018年度に観測されたインシデント状況 …… 8
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 …… 8
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 …… 11
1.2 情報セキュリティインシデント別の手口と対策 …… 14
1.2.1 標的型攻撃 …… 14
1.2.2 ビジネスメール詐欺（BEC） …… 20
1.2.3 DDoS攻撃 …… 25
1.2.4 ソフトウェアの脆弱性を悪用した攻撃 …… 27
1.2.5 ランサムウェア …… 29
1.2.6 パスワードリスト攻撃 …… 31
1.2.7 フィッシングによる詐欺 …… 33
1.2.8 偽の警告や偽サイトを用いた詐欺等 …… 36
1.2.9 情報漏えいによる被害 …… 41
1.3 情報システムの脆弱性の動向 …… 45
1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向 …… 45
1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向 …… 48
第2章 情報セキュリティを支える基盤の動向 …… 62
2.1 国内の情報セキュリティ政策の状況 …… 62
2.1.1 政府全体の政策動向 …… 62
2.1.2 経済産業省の政策 …… 65
2.1.3 総務省の政策 …… 71
2.1.4 警察によるサイバー犯罪対策 …… 74
2.1.5 CRYPTRECの動向 …… 77
2.2 国外の情報セキュリティ政策の状況 …… 80
2.2.1 国際社会と連携した取り組み …… 80
2.2.2 米国の政策 …… 82
2.2.3 欧州の政策 …… 87
2.2.4 中国の政策 …… 89
2.2.5 アジア太平洋地域でのCSIRTの動向 …… 91
2.3 情報セキュリティ人材の現状と育成 …… 95
2.3.1 情報セキュリティ人材の状況 …… 95
2.3.2 産業サイバーセキュリティセンター …… 101
2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度 …… 102
2.3.4 情報セキュリティ人材育成のための活動 …… 105
2.4 組織・個人における情報セキュリティの取り組み …… 107
2.4.1 企業における対策状況 …… 107
2.4.2 中小企業に向けた情報セキュリティ支援策 …… 111
2.4.3 教育機関・政府及び地方公共団体等法人における対策状況 …… 113

2.4.4 一般利用者における対策状況 115
2.4.5 政府・公共機関による普及啓発活動 118
2.4.6 団体・教育機関・学生・民間企業等による普及啓発活動 120
2.5 国際標準化活動 124
2.5.1 様々な標準化団体の活動 124
2.5.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27） 125
2.5.3 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） 131
2.6 安全な政府調達に向けて 132
2.6.1 ITセキュリティ評価及び認証制度 132
2.6.2 スマートカードの評価認証 135
2.6.3 暗号モジュール試験及び認証制度 136
2.7 その他の情報セキュリティ動向 138
2.7.1 情報セキュリティ市場の動向 138
2.7.2 データ利活用の実態と動向 139
2.7.3 暗号技術の動向 142
第3章 個別テーマ 156
3.1 制御システムの情報セキュリティ 156
3.1.1 インシデントの発生状況と動向 156
3.1.2 脆弱性と脅威の動向 158
3.1.3 海外の制御システムセキュリティの取り組み 159
3.1.4 国内の制御システムセキュリティの取り組み 160
3.2 IoTの情報セキュリティ 163
3.2.1 増大するIoTのセキュリティ脅威 163
3.2.2 脆弱なまま販売・運用されるIoT機器の散在 169
3.2.3 セキュリティ対策強化への取り組み 170
3.3 スマートフォンの情報セキュリティ 174
3.3.1 宅配便業者を装う不在通知SMSの手口 174
3.3.2 dアカウントを狙ったフィッシング 176
3.3.3 アプリ誘導 177
3.3.4 公式マーケット上に配布された不正アプリ 178
3.4 ITサプライチェーンのセキュリティ 179
3.4.1 インシデント、被害の事例 179
3.4.2 国内の政策動向 182
3.4.3 海外の政策動向 183
3.4.4 ITサプライチェーンにおける企業のセキュリティ対策状況 184
3.4.5 おわりに 187

3.5 AIのトラストとセキュリティ 188
3.5.1 本節で扱うAIのスコープ 188
3.5.2 AIの社会実装に関わるリスク 188
3.5.3 関連組織の活動 189
3.5.4 AIのトラストの検討状況 190
3.5.5 AIのセキュリティの検討状況 191
付録 資料・ツール 201
資料A 2018年のコンピュータウイルス届出状況 202
資料B 2018年のコンピュータ不正アクセス届出状況 203
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 205
ツール 208
第14回IPA「ひろげよう情報モラル・セキュリティコンクール」2018 受賞作品 222
索引 234

コラム

サイバーセキュリティ専門家に求められる倫理観 44
セキュリティ・バイ・デザインの勧め 56
サイバーセキュリティ目的のリバースエンジニアリングについて ～改正著作権法～ 79
CBPRシステム ～APECの越境個人情報保護～ 94
ネットで目立ちたい?? 123
サイバーセキュリティリスク対策に「サイバー保険」という選択肢も 145
Miraiの作成者の末路 173
情報セキュリティ10大脅威 2019 ～局面ごとにセキュリティ対策の最善手を～ 193

2019

情報セキュリティ白書

●序章　2018年度の情報セキュリティの概況

●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

1.1　2018年度に観測されたインシデント状況
1.2　情報セキュリティインシデント別の手口と対策
1.3　情報システムの脆弱性の動向

●第2章　情報セキュリティを支える基盤の動向

2.1　国内の情報セキュリティ政策の状況
2.2　国外の情報セキュリティ政策の状況
2.3　情報セキュリティ人材の現状と育成
2.4　組織・個人における情報セキュリティの取り組み
2.5　国際標準化活動
2.6　安全な政府調達に向けて
2.7　その他の情報セキュリティ動向

●第3章　個別テーマ

3.1　制御システムの情報セキュリティ
3.2　IoTの情報セキュリティ
3.3　スマートフォンの情報セキュリティ
3.4　ITサプライチェーンのセキュリティ
3.5　AIのトラストとセキュリティ

序章

2018年度の情報セキュリティの概況

2018 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。

国外では 2018 年 10 月に大手 SNS がユーザの個人情報 2,900 万件が流出した恐れがあると公表し、また 2019 年 1 月には大手ホテルチェーンが 3 億 8,300 万件の顧客情報が流出した恐れがあると公表した等、サイバー攻撃による大規模な被害が発生した。一方国内では、このような大規模な被害は確認されなかったものの、ビジネスメール詐欺や不正アクセス・内部不正による情報漏えい、ランサムウェア感染によるデータの暗号化被害、宅配便業者を装った SMS で不正アプリインストールに誘導する攻撃や EC サイトへのパスワードリスト攻撃等、企業や個人に対する攻撃・被害は継続して確認された。他にも、オンラインゲームのサーバが断続的な DDoS（Distributed Denial of Service）攻撃を受け、24 時間体制で対応にあたった事例や、複数の大学でフィッシングメールの被害が発生し、政府から全国の大学へ注意喚起を実施した事例等が報告された。また、委託先における運用上の過失に起因する情報漏えい被害や配布するアップデートファイルにウイルスを仕掛ける攻撃といった、サプライチェーン上のセキュリティリスクを浮き彫りにするインシデントもあった。

攻撃の基本的な手口には 2017 年度から目立った変化はなく、脆弱性の解消や適切なパスワード管理等、従来の対策で防げたはずの被害が多いが、人間の弱点を突く新しい手口も確認されている。例えば性的な画像等による脅迫を模した根拠のない脅迫で、仮想通貨を要求するというメールが 2018 年の夏ごろから多く確認された。事実無根の内容であるにも関わらず、指定された仮想通貨の口座には多数の入金が確認されたという。

政策面に関しては、2018 年度は国内外でセキュリティに関する戦略や法律の実践に向けた体制強化や施策が本格的に展開された、セキュリティ対策の過渡期とも言える年であった。

国内では、「サイバーセキュリティ戦略」が 3 年ぶりに見直され、以前よりもサイバー空間とフィジカル空間の一体化が進み、フィジカル空間への一層の影響が懸念される中、それらを包括したサプライチェーン上のリスク管理フレームワークの実装、中小企業対策の促進等が盛り込まれた。また、プロジェクト「NOTICE」や「情報処理支援機関（スマート SME サポーター）」認定制度等、企業の努力だけでは実現が困難な対策を、法律の見直しを含めて検討し、実現した。今後も官民が連携し、中小企業も含めたサプライチェーン全体のセキュリティ対策を進めることが求められる。

国際連携に関しては、日本は米国と、2018 年 7 月に重要インフラに対するサイバーセキュリティ、防衛面におけるサイバー連携や国際的なサイバーセキュリティに関する情報共有の強化に向け、協力することを確認した。欧州とは個人データの越境移転に関して 2018 年 7 月に包括合意を行い、2019 年 1 月に合意に基づいたデータ移転が可能となった。

米国では 2018 年 9 月､トランプ大統領が国家サイバー戦略を発表し、サイバー空間の敵対的行動を監視・対抗する、という安全保障重視の姿勢をより鮮明なものとした。特に、中国に対しては具体的に企業名を挙げ政府調達を禁止した。欧州では、2018 年 5 月に GDPR（General Data Protection Regulation：一般データ保護規則）が発効した。既に 2019 年 1 月には、グローバルサービスプロバイダの GDPR 違反が認定され、5,000 万ユーロ（約 62 億円）の制裁金が科せられた例が報告されている。また、重要インフラ向けのセキュリティ対策規範である NIS 指令に基づく EU 加盟国の各国内法整備については、ほぼ完了している状況である。中国に関しては、前述のとおり米国と対立が続いている一方、米国で政府調達禁止となった中国企業が EU 加盟国の一部で 5G ネットワークの調達ベンダとして認められたように、欧州と連携する等で独自の地位を模索している。

以上のように、セキュリティを国家戦略の一つとして掲げ、各国が独自に、あるいは連携した取り組みを進めている。日本は各国の戦略を理解し、必要な連携施策を講じつつ、国家を超えたサイバー脅威に対応する必要がある。

2018 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
2018 年　4 月	● 市の教育委員会が、不正アクセスによる情報漏えいがあったと公表（1.2.9、3.4.1） ● 監視カメラへの不正アクセスが相次ぐ（3.2.2）	■ NISC「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）」公表（2.1.1） ■ 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）」公表（2.1.2） ■ 米国国立標準技術研究所「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1」公表（3.4.3）
5 月		■ 「電気通信事業法及び国立開発研究法人情報通信研究機構法の一部を改正する法律」公布（2.1.3） ■ EU で GDPR が発効（2.2.3） ■ 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取組方針」決定（2.3.1） ■ 「不正競争防止法等の一部を改正する法律」公布（2.7.2）
6 月	● EC サイトで事前にスクリーニングされたリストによるパスワードリスト攻撃が発生（1.2.6） ● 大学で相次ぐフィッシングメール被害を受け、文部科学省が全国の大学に注意喚起（2.4.3）	■ 経済産業省・IPA「コラボレーション・プラットフォーム」開始（2.1.2） ■ 「G7 シャルルボワ・サミット」開催（2.2.1）
7 月	● IPA に国内のビジネスメール詐欺（BEC）の情報提供が相次ぐ（1.2.2） ● 宅配便業者を装う不在通知 SMS の相談急増（3.3.1）	■ 「サイバーセキュリティ戦略」閣議決定（2.1.1） ■ サイバーセキュリティ戦略本部「サイバーセキュリティ 2018」公表（2.1.1） ■ 「産業競争力強化法等の一部を改正する法律」施行（2.1.2） ■ 総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」公表（2.1.3）
8 月	● 携帯電話事業者が提供するサービスのアカウントへの不正ログイン被害 (1.2.6)	■ トランプ米国大統領が国防権限法に署名（2.2.2、3.4.3） ■ シンガポールでサイバーセキュリティ法が施行（2.2.5）
9 月	● 性的脅迫で仮想通貨を要求するメールの相談急増、日本語版も登場（1.2.8）	■ 経済産業省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」公表（2.1.2、3.1.4） ■ 経済産業省「技術等情報管理認証制度」開始（2.1.2） ■ 警察庁「サイバーセキュリティ重点施策」改定（2.1.4） ■ 米国「国家サイバー戦略」発表（2.2.2）
10 月	● 国内の病院で電子カルテシステムがランサムウェアに感染 (1.1.2) ● オンラインゲームのサーバに対する DDoS 攻撃が発生（1.2.3） ● 大手 SNS 事業者が、ユーザの個人情報 2,900 万件が漏えいした恐れがあると公表（2.2.3）	■ 総務省「プラットフォームサービスに関する研究会」設置（2.1.3）
11 月		
12 月		■ NISC「分野横断的演習」実施（2.1.1）
2019 年　1 月	● 海外の大手ホテルチェーンが、不正アクセスにより顧客情報 3 億 8,300 万件が漏えいした恐れがあると公表（1.1.1、1.2.9） ● 不正アクセスにより、ファイル転送サービス利用者の情報漏えいが発生（1.2.9） ● フランスのデータ保護機関が、グローバルインターネット事業者の GDPR 違反を認定（2.2.3）	■ 総務省「トラストサービス検討ワーキンググループ」設置（2.1.3） ■ 日本と EU との個人データ移転に関する包括的な枠組み発効（2.2.1）
2 月		■ 総務省・NICT「NOTICE」開始（2.1.3）
3 月	● 自動アップデートツールを悪用してウイルスを配布する攻撃の報告（3.4.1）	■ 欧州議会「EU サイバーセキュリティ法案」承認（2.2.3）

※ 2018 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。特に注目されたもののみを挙げた。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

2017 年に世界中で猛威を振るったランサムウェアやその後急激に被害が拡大した仮想通貨（暗号資産）の不正マイニングは、2018 年には減少傾向に転じた。このような傾向の要因としては、バックアップ等の対策が取られるようになったことや仮想通貨の価値が下がったこと等により、攻撃者が思うように金銭を獲得できなくなったことが考えられる。逆に CEO や取引先になりすましたビジネスメール詐欺や、E コマース等多くの人が利用しているサービスの偽サイトへの誘導、偽不在通知 SMS によるフィッシング、性的脅迫による金銭要求等、人の思い込みや後ろめたさを悪用した狡猾な手口のインシデントが増えた。便利なサービス、新しい技術は、攻撃者にとっても絶好の機会になることを忘れずに、利用者やサービス提供者は対策や情報共有を行い、立ち向かうことが求められている。

本章では、2018 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 2018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。2018 年においても、フィッシングやビジネスメール詐欺による金銭被害や大規模な個人情報漏えいが報告された。また、件数は減少傾向にあるもののランサムウェア感染や仮想通貨の不正マイニングも続いており、引き続き注意が必要である。また、セキュリティ製品の検知を回避するファイルレス攻撃が増加しており、新たな対策が求められている。

国内では大規模インシデントは発生しなかったものの、Web サイト改ざん、フィッシングによる金銭被害は増加傾向にある。また、宅配便業者に偽装した SMS や偽警告等、巧妙に人を騙して誘導する攻撃が継続しており、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

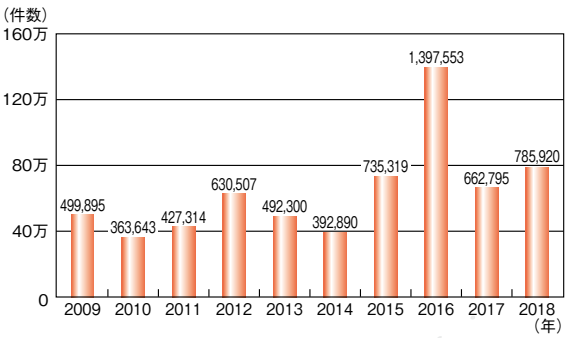
世界における情報セキュリティインシデントの発生状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

- International Business Machines Corporation（以下、IBM 社）：IBM X-Force Threat Intelligence Index 2019[※1]
- Symantec Corporation（以下、Symantec 社）：インターネットセキュリティ脅威レポート 第 23 号[※2]、第 24 号[※3]
- Verizon Communications Inc.（以下、Verizon 社）：2019 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）：2018 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) フィッシングとビジネスメール詐欺の傾向

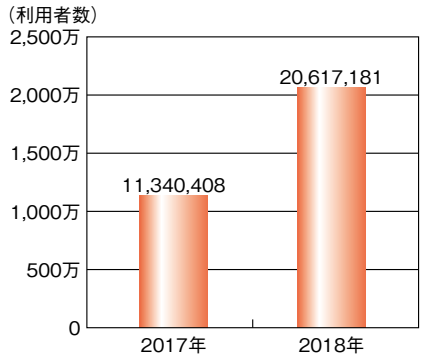
APWG によると、2018 年のフィッシングサイトの総数は約 78 万 6,000 件で、2017 年と比較して 18.6% の増加となり、依然高いレベルの脅威が継続している（図 1-1-1）。

ターゲットとなる業種は、2018 年 1 年間では「ペイメント（支払い）」が 37.0%、「SaaS/Webmail」が 21.6%、「金



■図 1-1-1　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」（2009～2018 年）を基に IPA が作成

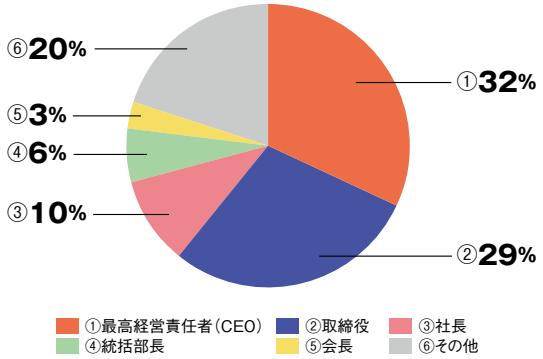
融機関」が 15.0% と続いている。特に 2017 年下期には 16.5% だった SaaS/Webmail を利用したフィッシングサイト数の割合は 2018 年下期には 24.7% に増加し、約 7 万 1,600 件となった。これは主に Office365 のログイン画面を偽装した Web サイトにターゲットを誘導することで、認証情報を窃取するというものである。更にトレンドマイクロ社の調査によれば、フィッシングメールの受信者がメール内のリンクをクリックしてフィッシングサイトに誘導された数は、2017 年と比較して約 8 割増加し、約 2,061 万 7,000 件となった（図 1-1-2）（フィッシングについては「1.2.7 フィッシングによる詐欺」参照）。



■図 1-1-2　フィッシングサイトに誘導された利用者数推移
（出典）トレンドマイクロ社「2018 年年間セキュリティラウンドアップ」を基に IPA が編集

ビジネスメール詐欺（Business Email Compromise：BEC）に関して、米国連邦捜査局（Federal Bureau of Investigation：FBI）の統計※7 によると、2013 年 10 月から 2018 年 5 月までに全世界で報告されたビジネスメール詐欺の発生件数は 7 万 8,617 件、被害総額は約 125 億米ドル（未遂を含む）に上っている。

また、トレンドマイクロ社の調査によれば、ビジネスメール詐欺は 2018 年も増え続け、前年比で約 3 割増となっており、2018 年にビジネスメールで最も多く詐称された役職は CEO（Chief Executive Officer：最高経営責任者）で全体の 32% にあたる（図 1-1-3）（ビジネスメール詐欺については「1.2.2 ビジネスメール詐欺（BEC）」参照）。



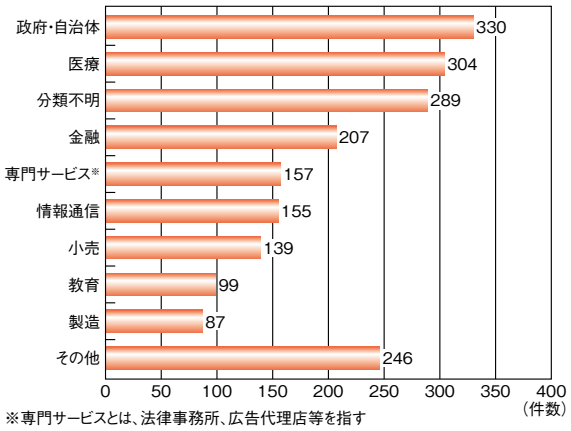
■図 1-1-3　ビジネスメール詐欺関連のなりすましに利用された職位の割合
（出典）トレンドマイクロ社「2018 年年間セキュリティラウンドアップ」を基に IPA が作成

(2) 情報漏えいインシデントの状況

2018 年も多くの情報漏えいインシデントが発生した。ここでは、その規模や影響度の大きさから、3 件のインシデントについて紹介する。

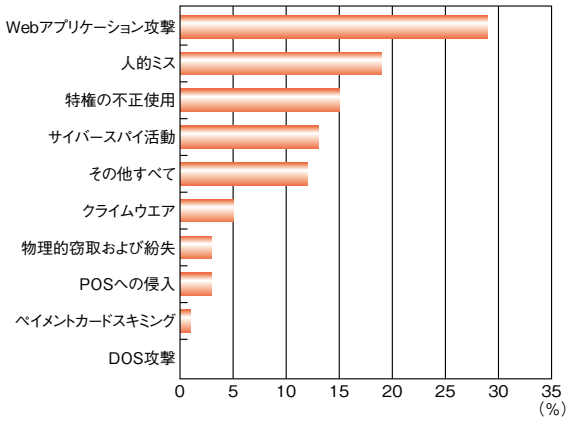
- 2018 年 7 月 20 日、シンガポール最大の医療グループ SingHealth は、2015 年からの約 3 年間に同社が運営する病院を訪れた、同国首相を含む 150 万人の患者の個人情報が不正にアクセスされコピーされたと発表した※8。流出したデータには、患者の氏名、国民登録番号、住所、性別、人種、生年月日等が含まれており、うち約 16 万人に関しては調剤情報も含まれていた。攻撃者はメールに添付したウイルス※9 をきっかけに侵入したと見られている。
- 2018 年 9 月 28 日、Facebook, Inc. は約 5,000 万件のアカウント情報が流出したと公表した※10（後に 3,000 万件の Facebook アカウントの情報に下方修正※11）。同社は、システムに実装されたプレビュー機能に関連するバグにより Facebook へのアクセストークンが盗まれ、不正アクセスによって利用者の氏名、電話番号、メールアドレス等の個人情報にアクセスされたと報告している。
- 2018 年 11 月 30 日、大手ホテルチェーンの Marriott International, Inc. は、傘下の Starwood Hotels & Resorts Worldwide, LLC のゲスト予約データベースに不正アクセスがあり、5 億人のゲストに関する個人情報が漏えいしたと公表した（後に約 3 億 8,300 万件に修正）※12。このうちカード番号約 860 万件（うち約 35 万 4,000 件の有効期限の切れていないカード番号）、暗号化されていないパスポート番号約 525 万件（暗号化されたパスポート番号は約 2,030 万件）が含まれていた。この不正アクセスは 2014 年から続いていたと報告されている。

Verizon 社によると、2018 年に発生した情報漏えいインシデント 2,013 件について、最も発生件数が多い業種は「政府・自治体」で 330 件、次いで「医療」が 304 件、「金融」が 207 件となっている（「分類不明」を除く）（次ページ図 1-1-4）。



■図 1-1-4　業種別の情報漏えいの件数
(出典)Verizon 社「2019 Data Breach Investigations Report」を基に IPA が作成

また、2018 年に発生した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、2018 年は 2017 年と同じく「Web アプリケーション攻撃」が全体の約 29% と最も多く、次いで「人的ミス」が 19% と 2 位になっている。2017 年に 3 位だった「POS への侵入」(15%) は 2018 年には 8 位 (3%) と大きく減少し、2018 年の 3 位 (15%) は「特権の不正使用」となっている (図 1-1-5)。



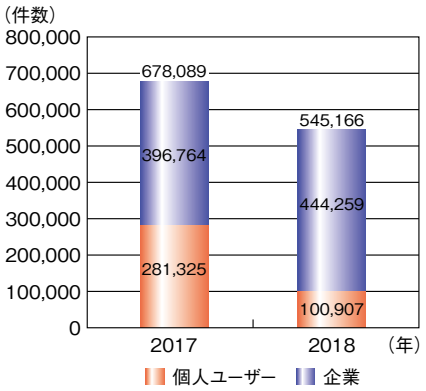
■図 1-1-5　情報漏えい事件の分類
(出典)Verizon 社「2019 Data Breach Investigations Report」を基に IPA が編集

IBM 社によると、2018 年の調査ではクラウドの設定ミスにより公に開示されたインシデントの総数は前年比で 20% 増加した。6 月には米国のマーケティング企業 Exactis LLC で、名前、住所、メールアドレスばかりでなく、子どもの数や喫煙の有無、趣味、宗教等、3 億 4,000 万件の情報が、公にアクセス可能なサーバ上に置かれていることが発覚した。

また、2018 年 5 月 25 日に EU 一般データ保護規則 (General Data Protection Regulation：GDPR) が施行され、実際に制裁金を科される事例が発生している[※13]。欧州連合 (European Union：EU) 居住者にサービスを提供している企業は、個人情報の取り扱いに一層の注意が必要となる (GDPR の制裁については「2.2.3 (1) GDPR の運用状況」参照。また情報漏えいについては「1.2.9 情報漏えいによる被害」参照)。

(3) ランサムウェアによる攻撃の傾向

Symantec 社によると、2018 年のランサムウェア検出件数は約 54 万 5,000 件と、2017 年より約 20%減少した。ただし、減少したのは個人ユーザを狙った件数であり、企業を標的とした件数は 2017 年より 12% 増加している (図 1-1-6) (ランサムウェアについては「1.2.5 ランサムウェア」参照)。



■図 1-1-6　ランサムウェアの市場別推移
(出典)Symantec 社「インターネットセキュリティ脅威レポート 第 23 号」「インターネットセキュリティ脅威レポート 第 24 号」を基に IPA が作成

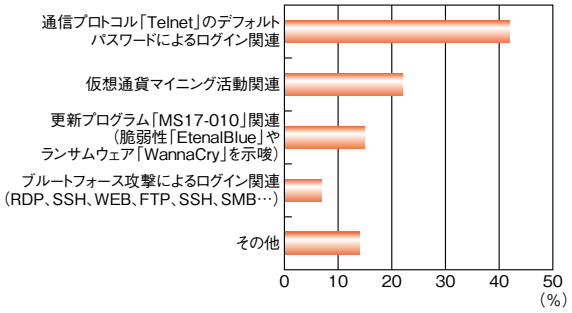
(4) 攻撃手法の傾向と変化

ランサムウェア以外も含めた攻撃者が使用するツールの傾向に関して 2018 年に注目されたのは、悪意あるプログラムの使用に代わって、PowerShell や WMI (Windows Management Instrumentation) コマンドラインユーティリティ等の正規アプリケーションのスクリプト実行により不正な活動を行う現地調達 (living off the land) 型の攻撃が増加した点である。このような正規アプリケーションを使うファイルレス攻撃の場合、特定のバイナリファイルや実行可能ファイルを使用せず、セキュリティ製品による検知を回避し証拠を残さないため、新たな対策が必要となる。IBM 社によると、攻撃における悪意のあるソフトウェアの使用は減少傾向にあり、攻撃の 57% で利用されていなかった。また Symantec 社も、2018 年にエンドポイントでブロックされた悪質な PowerShell スクリプトは 1,000% 増加したと報告している。

(5) スマートホームへの攻撃状況

トレンドマイクロ社によると、2017 年に続き、2018 年にスマートホーム向けのホームルータで観測した攻撃的なネットワークイベントの内訳では、「通信プロトコル『Telnet』のデフォルトパスワードによるログイン関連」「仮想通貨マイニング活動関連」「更新プログラム『MS17-010』関連（脆弱性『EternalBlue』やランサムウェア『WannaCry』を示唆）」の三つが、大きな割合を占めている（図 1-1-7）。

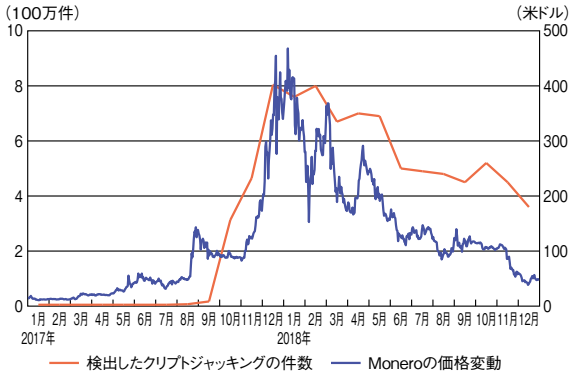
「通信プロトコル『Telnet』のデフォルトパスワードによるログイン関連」は、IoT 機器等のデフォルトパスワードを変更しない利用者を狙った攻撃であると考えられる（IoT 機器を狙った攻撃については「1.2.4 (4) IoT 機器を対象とした攻撃」「3.2 IoT の情報セキュリティ」参照）。



■図 1-1-7　観測されたネットワークイベントの内訳
（出典）トレンドマイクロ社「2018 年年間セキュリティラウンドアップ」を基に IPA が編集※14

(6) 仮想通貨の不正マイニングの傾向

Symantec 社によると、クリプトジャッキング※15 をブロックした件数は、2017 年の 1,600 万件から 2018 年には 6,900 万件に増加した。しかしながら、月ごとの遷移を見ると、2018 年始めをピークに、その後同年末には半減していることが分かる。この件数は仮想通貨の価格に大きく依存しており、価格が急騰した 2017 年末にクリプトジャッキングのブロック件数が急増し、その後仮想通貨の価格が低下するにつれて減少している（図 1-1-8）。



■図 1-1-8　検出したクリプトジャッキングの件数（単位 100 万件）と仮想通貨（Monero）の価格変動
（出典）Symantec 社「インターネットセキュリティ脅威レポート 第 23 号」「インターネットセキュリティ脅威レポート 第 24 号」を基に IPA が作成、Monero の価格変動については「CoinMarketCap※16」の情報を使用

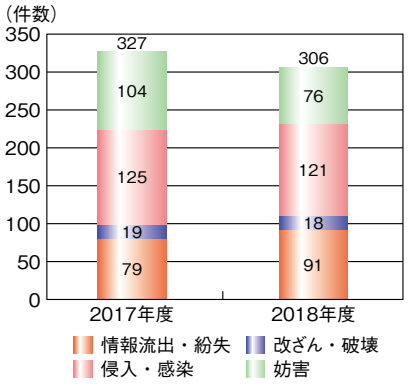
1.1.2 国内における情報セキュリティインシデント状況

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※17
- トレンドマイクロ社：2018 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※18
- フィッシング対策協議会：月次報告書※19

(1) 情報セキュリティインシデントの発生状況

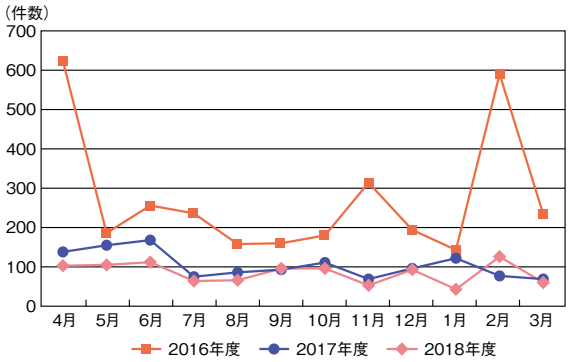
MBSD 社が集計した結果によると、2018 年度に報道された情報セキュリティインシデント発生件数は 2017 年度の 327 件から 306 件に減少した（図 1-1-9）。事象別に見ると「改ざん・破壊」「侵入・感染」は横ばいだったものの、「妨害」が 27% 減少し、「情報流出・紛失」が 15% 増加した。増加した「情報流出・紛失」の要因としては外部からの不正アクセスが多数を占めている（情報漏えいについては「1.2.9 情報漏えいによる被害」参照）。



■図 1-1-9　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

(2) Web サイト改ざんによる被害

2018 年度に JPCERT/CC へ報告された Web サイトの改ざん総件数は 1,017 件であった。ここ数年の傾向を見ると、2016 年度までは毎年 3,000 件を超えていたが、2017 年度は 1,259 件と大幅に減少し、2018 年度も減少傾向が続いている（図 1-1-10）。



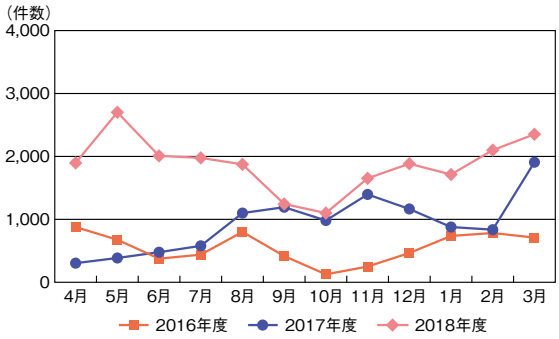
■図 1-1-10　Web サイト改ざん件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2016 年 4 月 1 日～ 2019 年 3 月 31 日）を基に IPA が作成

JPCERT/CC は、Web サイト改ざんの傾向について、2017 年度から引き続き、不正に埋め込まれたスクリプトによってウイルス感染したという偽の警告を表示するサイト等、不審なサイトに転送させ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（改ざん事例については「1.2.7 (5) メール・SMS 以外のフィッシングの手口」参照）。

(3) フィッシングによる被害

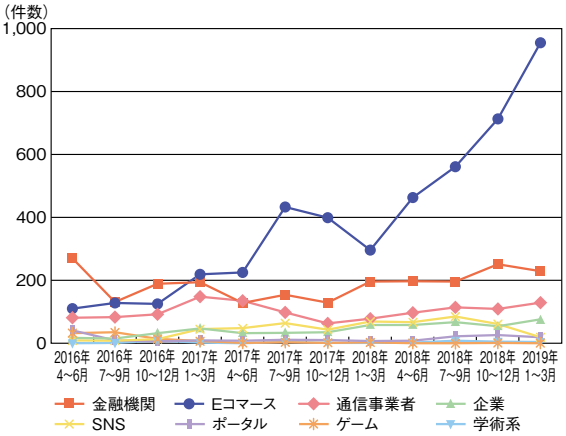
個人情報やクレジットカード番号、銀行口座番号等の各種サービスの認証情報の詐取を目的としたフィッシング詐欺が継続している。ここ数年のフィッシング対策協議会への報告件数は、2016 年度が 6,656 件、2017 年度が 1 万 1,205 件、2018 年度が 2 万 2,503 件、と 2 年連続して倍増している（図 1-1-11）。

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、2016 年度まで最多だった「金融機関」を 2017 年度に「E コマース」が上回り、2018 年度に入ってからも急増を続け、2019 年 1 ～ 3 月期には過去最多の 955 件に達している。その他のブランドの件数は横ばいなのに対して、「E コマース」は右肩上がり



■図 1-1-11　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」（2016 年 4 月～ 2019 年 3 月）を基に IPA が作成

となり、2018 年度の件数は全体の報告件数の 57% を占めるまでになっている（図 1-1-12）（フィッシングについては「1.2.7 フィッシングによる詐欺」参照）。



■図 1-1-12　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」（2016 年 4 月 1 日～ 2019 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 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が繰り返し報告されている。2017 年度に引き続き、Apple Inc. をかたるフィッシングの報告が特に多く、2018 年 5 月には全体の 65% を占めた。また 2017 年末から確認されていた宅配便業者からの不在通知を偽装した不正なテキストメッセージ（SMS）が年度を通じて拡散された。当初は Android 端末を対象として不審なアプリをインストールさせるという手口のみだったが、iOS 端末を対象に Apple ID とパスワード、また電話番号と認証コード等を狙ったフィッシングサイトに誘導する手口が登場している。更には、詐称する宅配便業者が複数になったり、iOS 端末に不審な構成プロファイルをインストールさせたりする手口も確認され、少しずつ手口

を変えて長期に継続して攻撃が行われた※20（「3.3.1 宅配便業者を装う不在通知 SMS の手口」参照）。

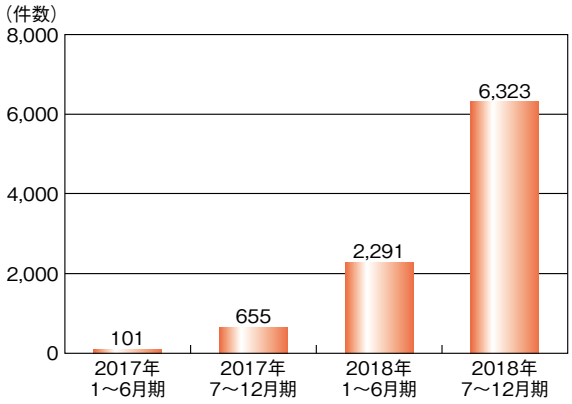
(4) 注目された新たな脅威

2018 年 7 月より海外で「アダルトサイトを閲覧している動画を公表されたくなければ仮想通貨を支払え」等の文面で指定のアドレスへのビットコイン送金を要求するメールが確認され始めた。同年 9 月からは国内でも同様のメールが確認されている。以前からある「性的脅迫（セクストーション）」の手口を想起させる文面であるが、不特定多数の対象者にばら撒かれている。そのため、実際には当該動画は存在しない架空の脅迫と考えられ、新たなスパムメールの手口と言える。しかし、当該動画が実際に存在すると信じさせるために、巧妙な騙しの手口が用いられており、実際、メール内で指定されていた送金先アドレスへの騙された受信者からと思われる送金も確認されている※20-1。

2018 年 12 月に大幅な減少が見られピークは過ぎたものの、フィッシング対策協議会の月次のフィッシング報告書では未だに警告がされており、今後も注意が必要である（「1.2.8 (1) 仮想通貨を要求する脅迫メール」参照）。

また、2018 年に急拡大した脅威として「偽警告」が挙げられる。トレンドマイクロ社への偽警告関連の問い合わせ件数の推移を見ると、2018 年 7 ～ 12 月期には 6,300 件に達し、前年同期の 10 倍近くに急増していることが分かる（図 1-1-13）。

「ウイルスに感染した」「システムが破損した」等の不安をあおる文言の警告メッセージを表示して、利用者を有償ソフトウェア購入に誘導する古典的な手口であるが、手口の複合化等により継続して被害が出ており、IPA でも注意喚起を行っている※20-2（「1.2.8 (2) 偽のセキュリティ警告」参照）。



■図 1-1-13　トレンドマイクロ社への偽警告関連問い合わせ数推移
（出典）トレンドマイクロ社「2018 年年間セキュリティラウンドアップ」を基に IPA が編集

悪意のある第三者が他者のリソースを使って仮想通貨を採掘させる不正マイニングが 2017 年から継続している。トレンドマイクロ社の調査によると、不正マイニングをさせるツール「コインマイナー」の国内での検出台数は、2018 年 4 ～ 6 月期にピークを迎えた後、2018 年 7 ～ 9 月期に半減して 2018 年 10 ～ 12 月期も横ばいとなっている。一方、兵庫県の学校内のネットワークでマイニングウイルスが蔓延した事例※20-3 等が散見されるため、引き続き不正マイニングへの警戒が必要である。

2017 年に世界で猛威を振るったランサムウェアは、日本国内では検出台数が減少しており、不特定多数を狙うばらまき型のランサムウェア攻撃は日本では収束傾向にある。しかし、奈良県の病院で電子カルテシステムがランサムウェアに感染し 1,133 人分の診療記録が暗号化される※20-4 等の被害も起きているため、引き続き警戒が必要である（「1.2.5 ランサムウェア」参照）。

1.2 情報セキュリティインシデント別の手口と対策

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。また、2018 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。

1.2.1 標的型攻撃

標的型攻撃とは、ある特定の企業･組織や業界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・組織や業界が保有している機密情報の窃取や、システム・設備の破壊・停止といった、明確な目的を持って行われる。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※21。

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 1-2-1）。

「事前調査段階」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なく、ソーシャルエンジニアリングや、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必要な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「事前調査段階」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。

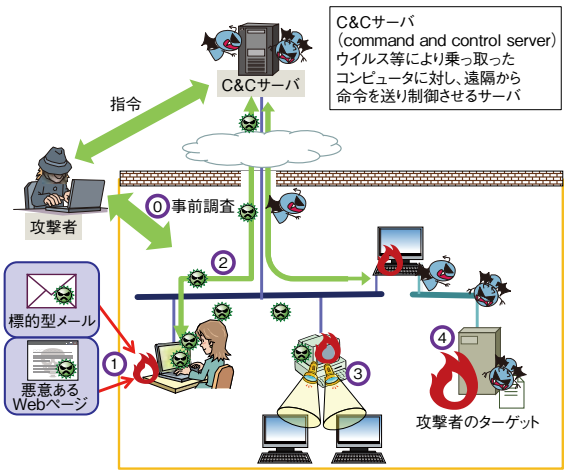
標的型攻撃メールに使用されるメールの文面は、標的とする組織に合わせて作成したものが用いられることが多い。また、過去事例では、メールの配送経路でウイルスが検出されることを回避するために、パスワードを設定した圧縮ファイルにウイルスを格納してメールに添付するといった細工が施されることもあった。

「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。攻撃者は内部にある端末を遠隔操作可能とするために、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。RAT 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。

続いて「システム調査段階」に移ると、攻撃者は先に感染させた RAT 等を用いて、必要に応じ、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。そして、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。このとき、OS の標準コマンドや正規のツールを使用することで、不正な活動を見つけにくくする手法も確認されている※23。

「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。

海外では、工場や生活インフラに関わる発電所のような施設の停止を目的とする等、情報の窃取以外を目的とした攻撃も過去に確認されている※24。



⓪［事前調査段階］
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］
標的型攻撃メールや、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 1-2-1　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※22」を基に編集

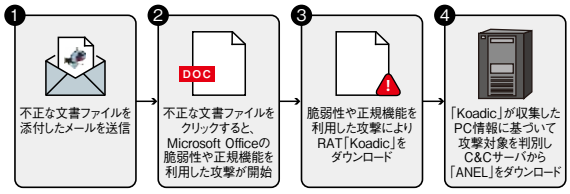
(1) 国内の標的型攻撃事例

2018 年に発生した標的型攻撃のうち、特徴的な三つ

の事例を紹介する。

(a) Microsoft Office の脆弱性と正規機能を悪用した標的型攻撃

2018 年 4 月に行われた、日本国内を標的にした標的型攻撃では、Microsoft Office の脆弱性や正規機能が悪用されていたことがセキュリティベンダによって報告されている（図 1-2-2）。



■図 1-2-2　攻撃による感染の流れ
（出典）トレンドマイクロ社「日本を狙う標的型サイバー攻撃キャンペーン『ChessMaster』、4 月に確認された最新攻撃手法を解説※25」を基に IPA が編集

この攻撃では、標的に対して、件名や添付された文書ファイル名にビジネスや日本経済に関する語句を用いたメールが送られてくるところから始まる。添付された文書ファイルには、脆弱性や DDE（Dynamic Data Exchange）※26 等の正規機能を悪用するプログラムが仕込まれており、ファイルが開かれると C&C（Command and Control）サーバから「Koadic」と呼ばれる RAT をダウンロードし、感染させる仕組みになっている。

RAT 感染後、感染端末のシステム情報が収集され、攻撃対象と判別された場合は、更に別の RAT「ANEL」が C&C サーバからダウンロードされ、RAT を切り替えて目的の情報を収集する。

本事例では、修正プログラムがリリース済みの脆弱性を悪用している。このように、攻撃者は修正プログラムがリリース済みの脆弱性であっても、修正プログラムが適用されていないことを期待して、当該脆弱性を悪用する攻撃を仕掛ける場合がある。

また、正規機能を悪用する攻撃では、その挙動が攻撃なのか正規の動作なのか判別が難しく、利用者が当該機能を有効にしてしまう場合がある。攻撃者はそれを期待して、正規機能の中で悪用できるものがあれば攻撃に取り入れる場合がある。

(b) ソーシャルエンジニアリングを組み合わせた標的型攻撃

2018 年 1 月、仮想通貨交換業者のコインチェック株式会社（以下、コインチェック社）が運営する取引所「Coincheck」が不正アクセスを受け、仮想通貨「NEM」が不正流出する事件が起きた。この事件では、「事前調査段階」で SNS 等を通じて同社の技術者らにソーシャルエンジニアリング※27 による事前工作が仕掛けられたという。

まず攻撃者は、事件の半年余り前から SNS 等を通じて同社のシステム管理権限を持つ技術者らを特定し、それぞれに対して偽名で交流を重ねていった。時間をかけて交流を重ねたことで技術者らから信用を得た攻撃者は、URL リンク付きの標的型攻撃メールを技術者らに送信し、技術者らはこれを疑うことなくクリックし、ウイルスに感染してしまったという。その後、攻撃者は、外部ネットワークからウイルス感染した端末を経由して社内の NEM サーバにアクセスし、RAT を使って NEM の秘密鍵を窃取した後、その秘密鍵を使って NEM を不正送金した※28。

本事例では、攻撃者は標的とした組織の関係者にソーシャルエンジニアリングによる事前工作を仕掛け、信用を得た上で標的型攻撃メールを送信している。これは、相手が標的型攻撃を警戒していたとしても、信用している人物から送られたメールであれば、警戒心が薄れ、標的型攻撃メールとは疑わずに開封してしまうことを狙ったものと推測できる。

(c) なりすましメールと正規のオンラインストレージサービスを組み合わせた標的型攻撃

2018 年 1 月、文部科学省をかたった不審なメールが送られてきたという情報が SNS に投稿された※29。このメールにはファイルが添付されておらず、ファイルのダウンロード先として、正規のオンラインストレージサービスの URL リンクが書かれていたという。

URL リンク先には圧縮ファイルが置かれており、その中には文書ファイルに偽装した実行ファイルが含まれていた。受信者が誤って実行してしまうと「PLEAD」と呼ばれる RAT がダウンロードされ、感染する仕組みになっていた。

本事例では、ウイルスが添付されたメールが送られるという典型的な標的型攻撃とは異なり、よく知られた正規のオンラインストレージから受信者自身にウイルスをダウンロードさせていた。これは、企業・組織内に設置されているメールゲートウェイでの検知を回避する意図があったものと推測される。

(2) 標的型攻撃の傾向

日本国内を対象とした標的型攻撃は 2018 年も継続して行われているが、その被害は公表されている事例の件数等から減少傾向にあったと推測される。しかし、コインチェック社の事例のようにソーシャルエンジニアリングを組み合わせた手口が確認されており、今後も従来の対策をすり抜ける巧妙な手口の出現が予想される。

引き続き、標的型攻撃に警戒するとともに、各種対策等を多層的に組み合わせたセキュリティ対策を講じていく必要がある。

(3) 標的型攻撃メールの手口

標的型攻撃メールは、標的とした企業・組織・業界でよく用いられる言葉を使用して非常に巧妙に偽装されているため、開封を完全に防ぐことは難しい。しかし、標的型攻撃メールに関する教育・訓練により攻撃手口を学ぶことで、開封リスクを低減することは可能である。ここでは標的型攻撃メールで用いられる手口について紹介する。

(a) 件名や本文の内容による騙しの手口

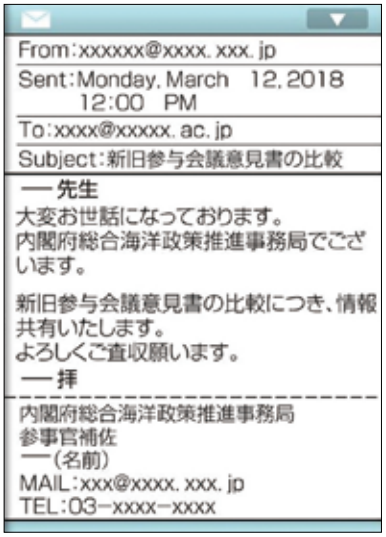
攻撃者は、標的型攻撃メールの受信者に不審に思われないようにするため、メールの件名や本文に特定の企業・組織・業界でよく用いられる言葉を使用することが多い。また、メールの信憑性をより高めるため、本文の最後に実在する関係者の署名が書かれる場合もある。

2018 年 3 月中旬に確認された、海洋政策関係者宛に送られた標的型攻撃メールでは、「新旧参与会議意見書の比較」という件名で、本文には実在する総合海洋政策本部参与会議の意見書に関する情報共有を示唆する内容と、実在する内閣府総合海洋政策推進事務局の職員の署名が書かれていたという(図 1-2-3)。

この事例で用いられた参与会議の意見書は内閣府の Web サイトで公開されており、誰でも閲覧可能になっている。攻撃者はこうした会議や文書の存在を「事前調査段階」で調べ、標的型攻撃メールで使用することが多い。また、高度な標的型攻撃になると、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

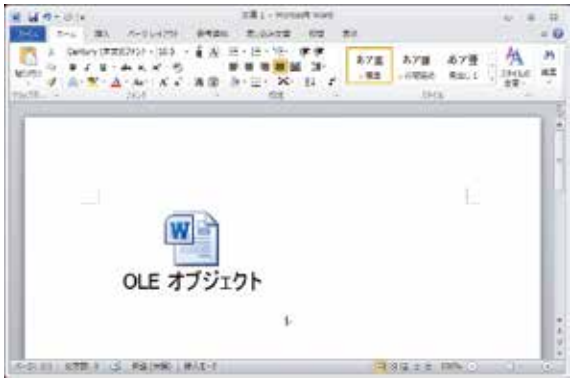
標的型攻撃メールの添付ファイルも同様に、受信者に攻撃であると気付かれにくくするために、巧妙な細工が施されることが多い。例えば、アイコンの偽装、RLO



■図 1-2-3　海洋政策関係者宛に送られた標的型攻撃メールの内容
(出典)産経ニュース「【サイバー攻撃】防衛省OBら標的、中国ハッカー集団関与か　情報流出の恐れ※30」(2018 年 4 月 12 日)

(Right-to-Left Override) 等による拡張子の偽装、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の手口がある。以下では、これまでに確認された手口について紹介する。

- LNK ファイルを悪用する手口
  Windows のショートカットファイル (LNK ファイル) の危険性はあまり認識されていないが、JavaScript や VBScript、PowerShell の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。
- Microsoft の OLE オブジェクトを悪用する手口
  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 1-2-4)。
- オンライン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メールにウイルスを添付して標的に送り付ける場合が多いが、「1.2.1 (1) (c) なりすましメールと正規のオンラインストレージサービスを組み合わせた標的型攻撃」のように、正規のオンラインストレー



■図 1-2-4　OLE オブジェクトを埋め込んだ Word ファイルの例

ジ上にウイルスを配置し、受信者にウイルスをダウンロードさせる手口が確認されている。受信者が普段からオンラインストレージを使用している場合、不審に思われる可能性が低いだけでなく、メールにウイルスを添付しないことでメールの配送経路での検知を回避できるため、注意を要する手口である。

- CSV ファイルを悪用した手口
  CSV（Comma Separated Values）とは、文字列や数字をカンマで区切ったテキスト形式のファイルで、表計算ソフト等のデータを交換するために利用されている。テキストエディタで開くとただのテキストデータ（文字列）だが、Microsoft Excel で開くと表データとして認識され、関数等が記載されていた場合、その関数が実行される。通常 CSV ファイルは Excel に関連付けられているため、この特性を悪用し、CSV ファイルに悪意のあるコードを埋め込み、Excel で開かせることで悪意のあるコードを実行させる手口が確認されている※31。
- マクロ機能を悪用した手口
  Microsoft Office のマクロ機能とは、Microsoft Office 製品に搭載されている VBA（Visual Basic for Applications）と呼ばれるプログラミング言語によって、特定の処理を自動化する機能である。この機能を悪用し、不正な処理を行うマクロを文書ファイル内に仕込むことができる。この文書ファイルが攻撃対象の端末で開かれ、マクロが有効化されると、攻撃者が意図した処理を実行できる。そのため、標的型攻撃の「初期潜入段階」において RAT を感染させる処理の一部で使用されている。

(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、複数の対策を多層的に組み合わせて防御すること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。

- ソーシャルエンジニアリングに対する注意力の向上
  標的とした組織への侵入や攻撃を容易にするため、攻撃者は電話や SNS 等、様々な方法で対象とする組織の関係者に接触し、心理的な隙やミスに付け込んで、重要情報を盗もうとする場合がある。
  ソーシャルエンジニアリングへの対策では、攻撃に気付けるかどうかが重要になるため、利用者は手口や対処方法を理解しておく必要がある※32。
  また、電話等で安易に重要情報を伝えてしまわないよう、少なくとも相手が特定できない状況においては、電話で重要情報は伝えないといった、情報授受の方法等を社内ルールで厳格に決めておくことも、ソーシャルエンジニアリング対策として有効である。
- 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乗っ取っ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で用いて不自然さをなくそうとしているもの等、受信者を騙すために巧妙な手口が多く用いられる。
  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。メールソフトが表示する送信者の名前の偽装もその一つである。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。確認の結果、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掲載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理解
  前述のとおり、Microsoft Office のマクロ機能を悪用すると、マクロを有効化された端末上で攻撃者が意図した処理を実行できる。Microsoft Office の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、マクロをデフォルトで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）を行わず、受け取った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。
- オンラインストレージサービスを悪用した手口の理解
  メール本文中に正規のオンラインストレージサービスのURL リンクを記載して、受信者にウイルスをダウンロードさせる手口も確認されている。普段から業務で外部のオンラインストレージサービスを利用している場合、このような手口を理解し、オンラインストレージサービスからファイルをダウンロードする際は、まずは本物のメールであるかどうかを確認することが有効である。
- Microsoft OLE オブジェクトの危険性の理解
  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ており、その手口について、IPA が注意喚起の資料※33 を公開している。この資料で紹介している手口では、文書ファイルにアイコンのような画像が埋め込まれ、これをダブルクリックすると領収書が確認できると記載されている。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手口も存在することを理解しておくことが重要である。
- 脆弱性放置の危険性の理解
  適切な対処をせずに脆弱性を放置していると、「1.2.1 (1) (a) Microsoft Office の脆弱性と正規機能を悪用した標的型攻撃」のように、脆弱性が RAT の感染に悪用され、攻撃者に容易に侵入されたり、その後の攻撃を許してしまう危険性がある。
  そのため、公開されたセキュリティ更新プログラムは適宜適用し、OS や使用しているソフトウェアを常に最新に保つことが重要である。

(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に連絡すべき窓口が組織内に周知されていることも、標的型攻撃対策として重要である。連絡窓口が周知されていない場合、利用者は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こともあるが、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 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が重要である。

(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、そのメールへの対応を調査する訓練（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。

CSIRT 向けの取り組みでは、他組織で起きたインシデントや自組織で起こりそうなインシデントを基にシナリオを作成し、インシデントが起きたことを想定して演習を行う※34。演習を通じて、CSIRT の対応能力の維持・向上や問題点の発見・改善を行い、実際のインシデントに備える。

また、ゲーム感覚で演習を行えるキットを使用し※35、利用者とCSIRTが合同で演習を行うことで相互理解を深め、インシデントが発生した際に協力し合える関係を確立しておくことも有効である。

(d)システムによる対策

ウイルス感染対策等の一般的なセキュリティ対策に加え、標的型攻撃に関して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
  セキュリティ製品で不審なメールやウイルスを検知した場合、システム管理者やCSIRTだけがアクセス可能な場所に隔離し、解析することによって組織内のセキュリティ対策に活かすことができる。例えば、ウイルスが不正な通信を行うドメインが分かれば、これをセキュリティ製品に設定することで、不正な通信の検出・遮断に利用できる。また、メールの送信元等のヘッダ情報から、メールの遮断や、他に同様のメールを受信していないかの調査もでき、隔離・解析の意義は大きい。
- 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。
  例えば、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※36」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
  PowerShellはWindowsに標準搭載されているスクリプト言語の実行環境で、主に運用・管理の自動化に用いられている。しかし、スクリプトの記述次第で様々な処理が実行できることから、文書ファイルにマクロとともに埋め込まれ、標的型攻撃の「初期潜入段階」でRATを感染させる処理の一部として悪用されている。日常の業務で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も対策として有効である。
- 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サーバへの通信の有無等を調査する必要がある。ログを取得するすべての機器の時刻を合わせておき、組織内の通信ログ等を目的に合わせて取得しておくことで上記の調査を行うことが容易になる。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しておく。また、SIEM(Security Information and Event Management)と呼ばれるログ管理ツールを活用して各種ログを一元管理し、相関分析を行うことで異常を早期に検知できるようにすることも重要である。自組織でこうした運用が困難な場合は、セキュリティ事業者が提供するSOC(Security Operation Center)サービス等を利用することを検討する。
- アクセス制御の実施
  利用者やシステム管理者に付与する権限は必要最低限に保ち、組織内のシステムであっても、業務上必要のないデータやサーバ、ネットワークセグメントへのアクセスを制限することが望ましい。適切にアクセス制御を実施することで、攻撃者に侵入された場合に内部侵害の拡大防止や被害の局所化につながる可能性がある。
- 適切な修正プログラムの適用
  「1.2.1 (1) (a) Microsoft Officeの脆弱性と正規機能を悪用した標的型攻撃」のように、標的型攻撃では、OSやアプリケーションの脆弱性が悪用されるケースもある。そのため、IT資産管理システム等を活用し、組織内の全サーバ・端末に適切に修正プログラムが適用できる仕組みを作ることが望ましい。
  運用上、サーバ・端末が停止できない場合や、使用しているアプリケーションの動作に問題が出る等の理由により、修正プログラムの適用が難しい場合は、修正プログラムの代わりに脆弱性を悪用する攻撃を検知・遮断する仮想パッチによる脆弱性対策を検討する。

以上のように、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を多層的に組み合わせ、複数の観点で対策を実施していくことが標的

型攻撃への対策として重要である。

1.2.2 ビジネスメール詐欺（BEC）

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※37。

本項では、ビジネスメール詐欺の状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の状況

米国連邦捜査局（Federal Bureau of Investigation: FBI）の統計※38によると、2013年10月から2018年5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）を含む複数の組織に報告されたビジネスメール詐欺の発生件数は7万8,617件、被害総額は約125億米ドル（未遂を含む）に上っている。この統計は全米50州と150ヵ国から報告されたものである。1件あたりの平均被害額は約16万米ドル（約1,800万円）であり、非常に大きな被害をもたらす脅威となっている。

国内でも、2014年以降、被害が増加傾向にあり※39、被害額が大きな事例としては、2017年11月に海外ファッションブランドの日本法人が約3億1,000万円の被害を受けた事例（表1-2-1項番3）や、2017年12月に大手航空会社が約3億8,000万円の被害を受けた事例※40が挙げられる。

また、トレンドマイクロ社の「ビジネスメール詐欺に関する実態調査2018」※41（調査対象：日本在住の法人組織の情報セキュリティ・社内IT・経理責任者ら1,030人）によると、調査対象全体の約4割（39.4%）がビジネスメール詐欺の攻撃を受けた経験があり、送金依頼メール受信者（253人）のうち8.7%（22人）が、実際に騙されて送金していたという。

このような状況を受け、警察庁※42や全国銀行協会※43、セキュリティ事業者等からビジネスメール詐欺に関する注意喚起がなされている。IPAも、J-CSIP※44の活動から得られた情報を基に、2017年4月に注意喚起※45（以下、2017年のBEC注意喚起）を行った。その後も国内組織への攻撃（日本語メールでの攻撃を含む）を確認したため、2018年8月に続報として注意喚起※46（以下、2018年のBEC注意喚起）を行った。

ビジネスメール詐欺は国内でも多くの攻撃が確認され、その勢いは衰えておらず、年々大きな脅威となっている。今後ますます注意が必要と考えられる。

(2) 2018年度に報道された事例の概要

2018年度に国内や海外で報道されたビジネスメール詐欺に関する事例について、概要を表1-2-1に示す。

多額の被害に遭った事例が多かったが、項番1のように、各国の捜査当局が連携して犯人を逮捕し、被害額の一部が回収された事例や、項番12のように保険で被害額の約9割を回復した事例もあった。

国内では、日本人やナイジェリア人が逮捕された事例（項番2、4、5、7、12、13）が大きく報道された。

日本語メールによる攻撃事例については、後述する。

(3) IPAが情報提供を受けた事例の概要

ここでは、IPAが情報提供を受けたビジネスメール詐欺事例（2015年から2018年7月にかけて発生した17件）のうち、2018年（1～7月）に情報提供を受けた8件の概要を表1-2-2（次々ページ）に示す。

なお、表1-2-2のうち1件（項番15）で金銭的被害が確認されている。

(4) 日本語メールによる攻撃事例

これまでのビジネスメール詐欺は、英語のメールのやり取りを伴う海外取り引きで多く発生していたが、2017年には国内の商社が日本語のメールによる攻撃を複数観測した※62。また、2018年7月に、実際に着信した日本語の攻撃メールについてIPAに情報提供があった（表1-2-2項番20）。更に、同時期（2018年7月）に複数の国内企業にも同様の日本語メールが着信していたことが確認された※63。今後、攻撃者が本格的に日本企業を狙ってくる可能性もあり、注意が必要である。

ここでは、表1-2-2の項番20の日本語メールによる攻撃とその手口について紹介する。

(a) 事例の概要

2018年7月、国内企業（A社）の担当者に対し、A社のCEOをかたる攻撃者から、ビットコインを購入するための準備と称して、国際送金をさせようとするビジネスメール詐欺が試みられた。メールの送信者として、本物のCEOの氏名とメールアドレスが使われていた。

この事例では、A社の担当者がやり取りの途中で不

項番	報道時期	概要	被害額
1	2018 年 6 月	FBI は「Wire Wire 作戦」を展開し、米国の関連政府機関や各国の捜査当局と連携して半年に及ぶ捜査を実施し、74 人を逮捕した※47。	約 1,400 万ドル（約 15 億円）※捜査当局が回収済
2	2018 年 7 月	警視庁組織犯罪対策総務課は 2018 年 7 月 4 日、組織犯罪処罰法違反（犯罪収益隠匿）と詐欺の疑いで、東京都江東区の会社役員ら男女 4 人を逮捕した。米国の農業関連会社から約 7,800 万円を不正に銀行口座へ送金させた上、正規の取り引きで得たように装い、2017 年 7 月 4 ～ 21 日に銀行等から計 6,020 万円を引き出した疑い※48。	約 7,800 万円
3	2018 年 8 月	イタリアのファッションブランドの日本法人である、ドルチェ&ガッバーナ ジャパン株式会社が BEC の被害に遭った。2017 年 11 月 2 日、ミラノ本社の経理部長を名乗る者から金融取り引きのために中国の銀行に送金を指示する内容のメールが日本法人の社長（当時）に送られ、社長は部下に送金を指示した。2017 年 11 月 6 日に詐欺だったことが判明し、社長と部下は同年 11 月 16 日に解雇され、280 万ドル（約 3 億 1,000 万円）の損害賠償請求訴訟を起こされた※49。	280 万ドル（約 3 億 1,000 万円）
4	2018 年 9 月	警視庁と宮城県警察は 2018 年 9 月 12 日、組織犯罪処罰法違反（犯罪収益隠匿）と詐欺の疑いで、ナイジェリア国籍の自称貿易業者を逮捕した。輸出会社役員の日本人と共謀し、2018 年 4 月 24 日、米国の民間団体が仙台市の銀行支店に送金した約 1 億 870 万円が不正な金銭と知りながら、同支店の男の会社預金口座に全額入金させ、9,300 万円を払い戻した疑い。また同年 6 月 5 日に米国の銀行からの返金要請を拒否し、正当な事業収益を装った疑い※50。	約 1 億 800 万円 ※うち 9,300 万円 不正引き出し
5	2018 年 10 月 ※項番 4 の続報	警視庁組織犯罪対策総務課は 2018 年 10 月 3 日、組織犯罪処罰法（犯罪収益隠匿）や詐欺等の疑いで、ナイジェリア国籍の自称貿易業者ら男 2 人を再逮捕した。2017 年 3 月、重機の輸出代金を装って、米国企業から仙台市の銀行の口座に振り込ませた現金約 500 万円を不正に引き出した疑い。現金詐取には取引先を装うメールの送信役等、複数の人物が関与※51。	約 500 万円
6	2018 年 11 月	2018 年 3 月にヨーロッパを拠点とする映画会社チェーンである Pathé が、BEC で同社の総収益の 10%にあたる 2,150 万ドル（約 1,900 万ユーロ）を失った。この攻撃は約 1 ヵ月間行われた※52。	2,150 万ドル（約 1,900 万ユーロ）
7	2018 年 11 月 ※項番 4、5 の続報	警視庁組織犯罪対策総務課は、組織犯罪処罰法違反（犯罪収益隠匿）等の疑いで、ナイジェリア国籍の容疑者を逮捕した。2017 年 1 月、重機の輸出代金を装ってタイの企業から騙し取った疑いがある約 300 万円を同国の銀行から仙台市の銀行に送金させ、このうち約 200 万円を不正に引き出した疑い※53。	約 300 万円 ※うち 200 万円 不正引き出し
8	2018 年 11 月	攻撃者が会社の CEO になりすまし、顧客がカリフォルニアの山火事の影響を受けているため、彼らに援助を送る必要があると、その会社の従業員を騙した。攻撃者は、従業員に Google Play ギフトカードを購入させ、裏面をスクラッチして引き換えコードを露出させ、その画像をメールで送信させた※54。	不明
9	2018 年 12 月	Agari Data, Inc.（米国のサイバー脅威の探知を専門とする会社）が London Blue と呼ばれる BEC の攻撃者グループによって作成された標的リスト（約 5 万人分）を発見した。主に標的とされたのは、企業の最高財務責任者（Chief Financial Officer：CFO）や会計担当者。同社はいくつかのケースで攻撃者が金銭の詐取に成功した証拠を見つけ、中には、「マネーミュール（資金の運び屋）」が銀行の損失防止部門を騙し、2 万ドル超の不正送金を正当なものと信じ込ませたケースもあった※55。	不明 ※一部 2 万ドル超のケースあり
10	2018 年 12 月 ※項番 4 と関連あり	2017 年 4 月に Save the Children Federation, Inc. が、約 100 万ドル（当時のレートで約 1 億 870 万円）の BEC の被害に遭った。2017 年 5 月に発覚し、FBI が日本の法執行機関と連携して事件を調査した。当時は回収できなかったが、その後、保険会社から 88 万 5,784 ドルが支払われ、財政損失を 11 万 1,616 ドルに抑えることができた※56。	約 100 万ドル ※保険で約 89 万ドルを回復
11	2019 年 1 月	Tecnimont Pvt Ltd（イタリアの EPC※57 企業 Maire Tecnimont SpA のインド子会社）が、中国のグループによって、1,860 万ドルの被害に遭った。中国グループは、Maire Tecnimont SpA グループ CEO のアカウントと非常によく似たアカウントを介して、Tecnimont Pvt Ltd のヘッドのインド人にメールを送った。更に彼らは、中国における機密性の高い買収について話し合うと称し、電話会議等にて詐欺を行った※58。	1,860 万ドル
12	2019 年 2 月 ※項番 4、5、7 の続報	警視庁組織犯罪対策総務課は組織犯罪処罰法違反（犯罪収益隠匿）等の疑いで、元防衛相公設秘書を逮捕した。2018 年 4 月、ナイジェリア人らと共謀し、台湾企業が容疑者の会社名義の口座に振り込んだ約 1,900 万円を引き出した疑い。「口座を貸してくれと日本人に頼まれた。やばい金とわかっていた」と容疑を認めているという※59。	約 1,900 万円
13	2019 年 3 月 ※項番 4、5、7、12 の続報	西インド諸島のセントクリストファー・ネビスにある会社の代表のメールアドレスを乗っ取って偽の振り込みを指示し、約 1 億 1,000 万円を詐取したとして、警視庁は東京都の会社役員と、大阪市の会社役員を詐欺と組織犯罪処罰法違反（犯罪収益隠匿）の疑いで逮捕した※60。	約 1 億 1,000 万円

■表 1-2-1　2018 年度に報道されたビジネスメール詐欺に関する事例の概要（報道または公表事例を基に IPA が作成）

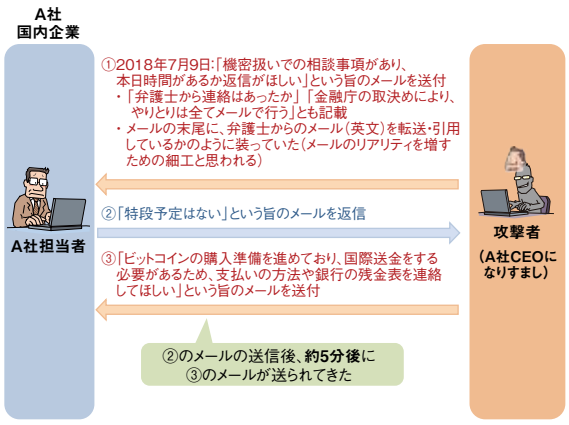
項番	情報提供日	事例概要	被害の有無	備考
14	2018 年 1 月 5 日	2017 年 12 月、国内企業（支払い側）と、東南アジアの企業（請求側）との取り引きにおいて、攻撃者が請求側企業の担当者になりすます BEC が試みられた。	なし	－
15	2 月 16 日	2018 年 2 月、国内企業が、海外のカンファレンスのブース出展に関するメールをやり取りしている中で、攻撃者がカンファレンス事務局の担当者になりすまし、偽の口座に送金させようとする BEC が発生した。	あり	サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 1 月～ 3 月］※61 に記載
16	3 月 12 日	2018 年 3 月、国内企業の海外関連会社において、同社の CEO になりすました攻撃者から、偽の振り込みを要求する BEC が試みられた。	なし	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］に記載
17	5 月 17 日	2018 年 5 月、国内企業（請求側）と、海外取引先（支払い側）との取り引きにおいて、攻撃者が請求側企業の担当者になりすます BEC が試みられた。	なし	サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 4 月～ 6 月］※31 に記載
18	6 月 4 日	2018 年 6 月、国内企業（請求側）と、海外関連企業（支払い側）との取り引きにおいて、攻撃者が請求側企業の担当者になりすまし、偽の振り込みを要求する BEC が試みられた。	不明	サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 4 月～ 6 月］に記載
19	7 月 6 日	2018 年 7 月、国内企業の CEO を詐称し、海外関連企業の CEO へ偽のメールが送られた。なお、同一文面のメールを用いた BEC が、本件と無関係なドイツの企業に対しても行われたことを示す情報が確認された。	不明	－
20	7 月 9 日	2018 年 7 月、国内企業の CEO を詐称し、同企業の担当者に対して、ビットコインを購入する準備と称して、国際送金させようとする BEC が試みられた。本事例では、日本語のメールが攻撃者から送られてきた。	なし	2018 年の BEC 注意喚起※46 に記載
21	7 月 19 日	2018 年 7 月、国内企業（請求側）と、海外取引先企業（支払い側）との取り引きにおいて、攻撃者が請求側の担当者になりすまし、偽の振り込みを要求する BEC が試みられた。	なし	2018 年の BEC 注意喚起に記載

■表 1-2-2　IPA が情報提供を受けたビジネスメール詐欺事例の概要
（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（続報）※46」

審であると気付くことができ、金銭被害は発生していない。攻撃者と担当者の具体的なやり取りは、図 1-2-5 のとおりである。

2018 年 7 月 9 日、攻撃者は、A 社の CEO になりすまし、機密扱いの相談事項があるという内容のメールを A 社担当者に送り付けてきた（図 1-2-5 の①）。このとき、A 社担当者は特段の予定はないと返信した（図 1-2-5 の②）。

A 社担当者がメールを返信した約 5 分後、攻撃者が、ビットコインの購入準備のために国際送金が必要であるという内容で、支払方法や銀行の情報を聞き出そうとするメールを送り付けてきた（図 1-2-5 の③）。



■図 1-2-5　攻撃者とのやり取り
（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（続報）」

(b) 詐称用ドメインの取得と悪用

攻撃者は、金融庁の正規のドメインに似た、偽の「詐称用ドメイン」を新規に取得し、DNS やメールサーバの設定も実施していた。この詐称用ドメインの DNS 情報には、SPF（Sender Policy Framework）レコードも存在しており、SPF 検証※64 を「Pass」する状態だった。このため、一般的に不審なメールを判断するシステム上の対策である、「フリーメールアドレスからのメールに警告を付与する」や「SPF 検証を行う」等は効果がないことになる。この場合、メール受信者がメールアドレスに注意して、ドメイン名が異常であることに気付くことが重要となる。

(c) 表示名 (display-name) の細工

攻撃者から送られてきたメールの送信者（From メールアドレス）として、本物の A 社 CEO の名前とメールアドレスが表示されるが、そのメールアドレスに返信メールが届かないようにする（攻撃に気付かれないようにする）細工が仕掛けられていた。

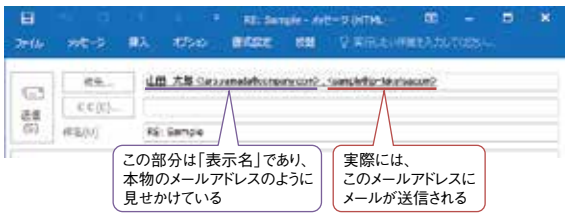
例えば、メールソフトのアカウント設定で、送信者の名前を「山田 太郎 <taro.yamada @ company.com> ;」と設定すると、メールを送信した場合、一部のメールソフトでは、図 1-2-6 の例のように、着信者側でメールの送信者として設定した文字列が表示される。

A社CEOの名前 <A社CEOの正規のメールアドレス> ; <金融庁に見せかけた偽のメールアドレス>

（例：山田 太郎 <taro.yamada @ company.com> ; <sample @ jp-fakefsa.com> ）

■図 1-2-6　From メールアドレスのイメージ
（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（続報）」

このメールに対して返信メールを作成すると、図 1-2-7 のように宛先メールアドレスが設定される。一見すると、A 社の CEO と（偽の）金融庁の二者宛てのメールとなっているが、A 社の CEO の名前とメールアドレスが表示されている部分は「見せかけ」（「;」までが表示名）であり、実際にはメールは送信されない。偽の金融庁のメールアドレス（攻撃者のメールアドレス）にのみメールが送信される。



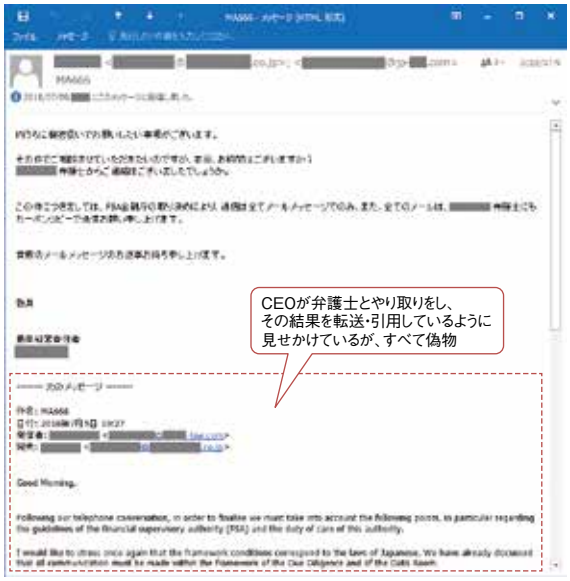
■図 1-2-7　返信先のメールアドレスを詐称する手口の例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）」

送信者欄で本物の CEO の氏名とメールアドレスを詐称しつつ、被害者がメールを返信する際にも、画面上に詐称した情報を表示させようとする巧妙な細工が施されていた。

(d) 攻撃者からのメール

攻撃者からの最初のメールは、A 社担当者に対して返信を要求する内容が日本語で書かれていた（図 1-2-8）。更に、メールのリアリティを増すため、国際法律事務所の日本人弁護士とのやり取り（英語）を装った内容を転送・引用しているように見せかけ、その弁護士にもメールの写し（CC）を送るよう指示していた。

この法律事務所のドメインも、実在する国内の法律事務所に似せた偽のドメインであり、攻撃者が偽の金融庁メールアドレスに使用した「詐称用ドメイン」と同じ経路（レジストラ）で、「詐称用ドメイン」の取得から約 10 分差で取得されていた。すなわち、指定された弁護士のメールアドレスへメールを送っても、結局は同じ攻撃者にメールが届く仕掛けになっており、攻撃者は必要に応じ CEO と弁護士の一人二役を演じるつもりであったと考えられる。



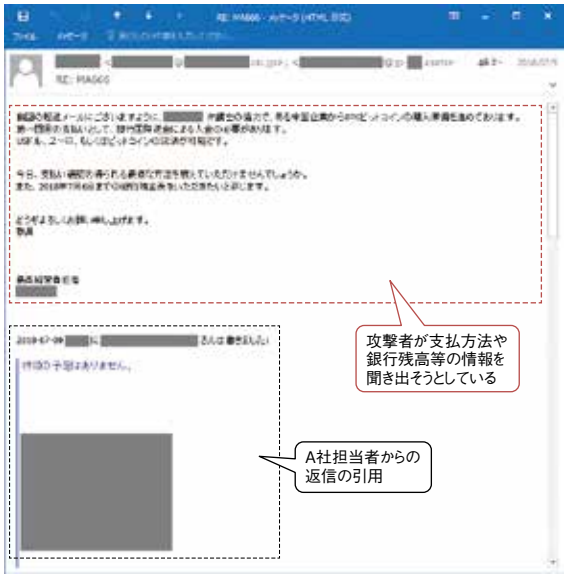
■図 1-2-8　攻撃者からの 1 通目のメール
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）」

更に、図 1-2-8 のメールに対して、A 社担当者が日本語で返信すると、次のメールが攻撃者から送られてきた（次ページ図 1-2-9）。そのメールでは、ビットコインの購入準備を進めているため国際送金を行う必要があるとし、支払方法や銀行残高等の情報を聞き出そうとしていた。

A 社担当者がこのメールに返信した場合、攻撃者から偽の口座への振り込みを指示する内容のメールが送られてきたものと考えられるが、担当者はこの時点で不審であると気付くことができ、被害を免れた。

(5) 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の対策を以下にまとめる。これらの対策を通じて、ビジネスメール詐欺の手口を理解するとともに、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が重要である。



■図 1-2-9　攻撃者からの 2 通目のメール
（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（続報）」

(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、被害を防止することは困難である。

このため、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、全グループ企業だけでなく、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。メールに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最も重要である。

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 等のメール以外の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。

また、外部のメールアドレスやフリーメールから着信したメールについて、件名や本文にその旨の注意喚起を表示するメールシステムを採用すれば、従業員は、紛らわしいドメインからのメールを見分けやすくなる。

(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、基本的なウイルス対策・不正アクセス対策が重要である。

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、多要素認証等の利用により、第三者による不正ログインを防ぐことが重要である。英国サイバーセキュリティセンター（National Cyber Security Centre）から、Office 365 の対策についての資料※65 が公開されているため、そちらも参照いただきたい。

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、不正な転送設定や、メールを削除するルールが設定※66されていないかを確認する等の対応を行う必要がある。

1.2.3 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃は、一般に、Webサーバ等の攻撃対象に対して多数の端末からデータを送信することで、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃を指す。

本項では、DDoS攻撃の仕組みと、2018年に確認されたDDoS攻撃に関わる事例を紹介した後に、その手口と対策について解説する。

(1) DDoS攻撃の事例、及び摘発事例

2018年度における、DDoS攻撃に関連する主だった事例を紹介する。

(a) オンラインゲームの運営サーバに対するDDoS攻撃

2018年10月に、株式会社スクウェア・エニックスが運営するオンラインゲーム「FINAL FANTASY XIV」が、DDoS攻撃を受けた※67。DDoS攻撃は手口を変えながら断続的に行われ、スクウェア・エニックス社はISP（Internet Service Provider）事業者と連携して24時間体制での対応を行った。

また2019年1月には、合同会社DMM.comが運営するゲーム「艦隊これくしょん」の運営サーバがDDoS攻撃を受けた※68。攻撃は10日程度の期間に、手口を変えながら断続的に行われ、海外を送信元としていた。こちらもISP業者と協力し、24時間体制で対応にあたった。

両者はいずれも、手口を変えながら断続的に攻撃されており、このような攻撃はマルチベクトル型攻撃（詳細は後述）と呼ばれる。

(b) DDoS攻撃代行サービスサイトの摘発

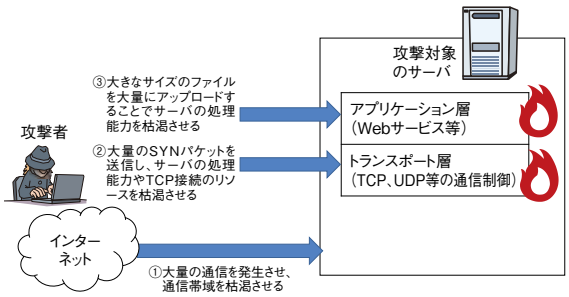
DDoS攻撃を代行するサービスが存在している。表向きは登録ユーザの所有、運用するサーバに対して負荷テストを行うサービスを装っているが、実際には第三者が運用するサーバへのDDoS攻撃に用いられている。

2018年4月には欧州刑事警察機構（Europol）が「Operation Power Off」と呼ばれる作戦を展開し、世界最大規模のDDoS攻撃サービス「Webstresser」を摘発し、管理者とされる人物を逮捕した※69。当該サービスには15万人以上のユーザが登録されており、3年間で400万件の攻撃が行われていた。

(2) DDoS攻撃の手口

DDoS攻撃では、攻撃対象のリソースに負荷をかけることができれば、そのサービス運用を妨害できる。リソースに負荷をかける手口は複数存在する。

主なものとして、ボットネット、IoTボットを用いる手口や、リフレクター攻撃と呼ばれるサーバの設定不備を悪用して、攻撃通信を増幅させる手口等が挙げられるが、これらは併用されることも多い。特に、様々な手口を併用して攻撃しつつ、攻撃効果や状況に応じて、有効な手口に絞った攻撃に切り替えるマルチベクトル型攻撃（図1-2-10）が主流となっている。



■図1-2-10　マルチベクトル型攻撃のイメージ

(a) ボットネット、IoTボットを用いる手口

脆弱性の悪用やウイルス感染によって、攻撃者に制御を奪われたインターネット上の端末は「ボット」と呼ばれる。そして、攻撃者がボットへ命令を送るためのC&Cサーバと、複数のボットで構成される、いわゆる「ボットネット」と呼ばれるネットワークがDDoS攻撃に悪用される。

また、近年のIoT機器の普及に伴い、IoT機器のボット化を狙った攻撃が確認されている。このようなボット化されたIoT機器は「IoTボット」と呼ばれる。

低コストで設計されるIoT機器は、十分なセキュリティ対策を実装しにくい場合や適切な管理がなされない場合があり、ボット化を狙う攻撃の標的になる傾向がある。2016年に確認された、工場出荷時の初期設定のままのネットワーク機器やIoT機器を狙うウイルス「Mirai」を皮切りに、ボット化されたネットワーク機器やIoT機器によるDDoS攻撃が増加している状況である（「3.2.1 増大するIoTのセキュリティ脅威」参照）。Miraiに関しては、多数の亜種が確認されており、2017年末から2018年前半まで日本でも感染が急増した※70。

こういった背景から、総務省はセキュリティ対策に不備のあるIoT機器を対象にした調査、及び当該機器の

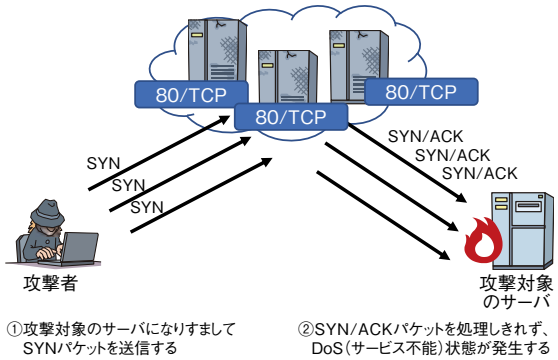
利用者への注意喚起等の施策に取り組んでいる※71（「2.1.3 (1) (a) 脆弱性対策に係る体制の整備に向けた主な取り組み」参照）。

(b) リフレクター攻撃

リフレクター攻撃は、送信元 IP アドレスを攻撃対象の IP アドレスに偽装したパケットを、不特定多数の正規のサーバに対して送信することで、それらのサーバからの応答パケットが攻撃対象の端末へ送信されることを悪用した攻撃である。

リフレクター攻撃の類型として、サーバ上で使用されるプロトコルやソフトウェアの挙動を悪用するものがある。

2018 年 9 月には、SYN/ACK リフレクション攻撃と呼ばれるリフレクター攻撃が確認された※72。これは、多くのサーバがインターネット上で Web サイトを公開するために TCP の 80 番ポートを開放していることを悪用した攻撃である。送信元を偽装した SYN パケットをこれらのサーバ群に送信し、応答の SYN/ACK パケットを攻撃対象の端末に送信させ、処理負荷を生じさせる（図 1-2-11）。



■図 1-2-11　SYN/ACK リフレクション攻撃のイメージ

攻撃に悪用されるサーバ群は、不要なポートを開放しているわけではなく、正規の目的で TCP の 80 番ポートを開放しているため、アクセス制御やポート閉塞等による対策が困難である。また、送信元を偽装した SYN パケットの送信状況等によっては、攻撃対象の端末から SYN フラッド攻撃を受けているようにも見えてしまう。

正規の通信処理を悪用した攻撃であることから、抜本的な対策が取れないため、ISP 事業者と連携したり、不審な SYN パケットあるいは SYN/ACK パケットの送信元 IP アドレス情報を基に、悪用されているサーバの運営者と攻撃対象サーバの運営者が連絡を取り合う等で、攻撃の全体像を把握した上での対処が必要となる。

(3) DDoS 攻撃への対策

DDoS 攻撃への対策では、DDoS 攻撃そのものの被害に遭わないための対策に加えて、管理、所有する端末のボット化やリフレクター攻撃への意図しない加担を防ぐための対策も求められる。これらの対策について解説する。

(a) DDoS 攻撃の被害に遭った場合の対策

DDoS 攻撃によって送られてくる通信データを遮断し、サービスを提供するサーバやネットワークのリソースを保護する対策が必要である。正常なアクセスと DDoS 攻撃によるアクセスを、いかにして切り分けるかが対策のポイントとなる。

以下に、具体的な対処方法を挙げる。

- アクセスログや通信ログ等を確認し、攻撃が特定の IP アドレスから行われていると判断できる場合は、当該 IP アドレスからのアクセスを遮断する。
- 国内からのアクセスを主に想定しているサイトでは、海外の IP アドレスからのアクセスを一時的に遮断することも検討する。
- 攻撃者が攻撃元の IP アドレスや攻撃方法を定期的に変更してくる場合があるため、継続して監視を行い、攻撃方法に合わせた対策を実施する。
- 組織内で対処できない程大規模な攻撃や執拗な攻撃を受けている場合は、ISP との連携や警察等への通報を実施する。

なお、攻撃の頻度や、攻撃対象サイトの重要性によっては、DDoS 対策製品や ISP 事業者が提供する DDoS 対策サービスの利用を検討する。

(b) 攻撃に加担しないための対策

以下に挙げるように、自組織や個人で使用する端末、ネットワーク機器、IoT 製品が DDoS 攻撃に悪用されないように、ウイルス対策や適切な設定変更等の対策が必要である。また企業においては、自組織の端末を悪用された場合、それを早期に検知できるように通信の監視を行うといった対策も推奨する。

- OS やファームウェアを最新の状態に保ち、脆弱性を突いて感染するウイルスを防ぐ。
- パスワードが初期設定のままの機器が存在しないか確認し、存在した場合は適切なパスワードを設定する。パスワードが初期設定のままの機器は、攻撃者により容易に侵入され、制御を奪われてしまう可能性がある。

前述したMiraiやその亜種のケースのように、パスワードが初期設定のままのネットワーク機器やIoT機器を狙って感染し、更に組織内の他の端末に対しても同様な挙動で感染拡大を試みるため、インターネットに直接つながっていない端末においても同様の対策が必要となる。

- 組織内のDNS（Domain Name System）、NTP（Network Time Protocol）、2017年度末に新たに悪用が確認されたmemcached等のDDoS攻撃に悪用されることの多いサービスが動作するサーバに関して、サーバのOSを始め、各サービスが脆弱性を含むバージョンで稼働していないことを確認する。また、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開していないことやDDoS攻撃に悪用され得る設定になっていないことを確認する。
- 組織内の端末の外向けの通信を監視し、異常な通信を確認した場合等は、組織内の端末が攻撃の踏み台となっている可能性があると判断し、ウイルス感染等が生じていないか調査、対処を行う。自組織での対処が困難な場合は関係当局やセキュリティベンダ等への相談を検討する。

1.2.4 ソフトウェアの脆弱性を悪用した攻撃

2018年度は、Windowsの脆弱性を対象とした攻撃が多く報告されている。Windowsの脆弱性以外にも、多くのWebアプリケーション開発で使用されるフレームワークであるApache Struts2や、Webサイト構築に使用されるコンテンツマネジメントシステム（Content Management System：CMS）に存在する既知の脆弱性を狙った攻撃が報告されている。また、IoT機器を対象とした新たなウイルスが報告されている。

本項では、これらの脆弱性の状況と対策について解説する。

(1) Windowsの脆弱性を対象とした攻撃

Microsoft社が毎月実施しているWindows Updateにおいて、2018年度に実施されたアップデートの半数以上（12件中8件）は、実際に悪用が確認されている脆弱性を修正する内容を含んでいた。また、脆弱性が公開され、Microsoft社による対策が提供される前に悪用が確認された脆弱性も存在していた※73。利用者は、修正プログラムが公開されたら速やかにアップデートを実施することが求められる。

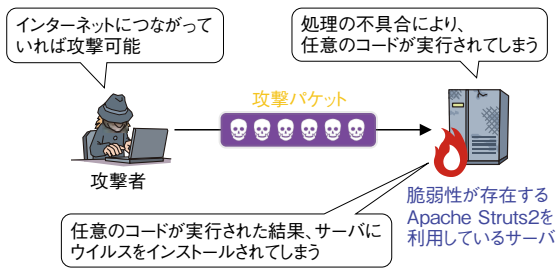
なお、2020年1月14日には、Windows 7、Windows Server 2008及びWindows Server 2008 R2のサポートが終了となる。一般的にサポート終了後に発見された脆弱性については、修正プログラムが提供されなくなるため、サポートが終了したOSを使い続けると脆弱性を悪用した攻撃により、被害を受ける可能性が大きくなる。そのため、利用者は、計画的に最新版へ移行することを推奨する※74（「1.3.2 (1) (c) 公式サポートが終了するソフトウェア製品」参照）。

(2) 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フレームワークである。2018年度は2017年度に引き続き、Apache Struts2の脆弱性を悪用する攻撃が確認された。

2018年8月にIPAが注意喚起を行ったApache Struts2の脆弱性CVE-2018-11776※75を悪用した攻撃を以下に示す。

攻撃者は、インターネットを通じて、同脆弱性が存在するApache Struts2を利用しているサーバに対して、細工したリクエストを送信する。これだけで、サーバ上で任意のコードが実行され、サーバに対してウイルスのインストール等が可能となる（図1-2-12）。



■図1-2-12　Apache Struts2の脆弱性を悪用した攻撃イメージ

2018年9月、攻撃対象のサーバにコインマイナーを不正にインストールしようとした事例が報告されている※76。

自身のWebサイトでApache Struts2を使用している場合、このような攻撃による被害を防ぐため、Apache Struts2を常に最新のバージョンにしておくことが望ましい。また、Apache Struts2以外にもソフトウェアを利用している場合は、それらについても使用しているバージョンの脆弱性情報の収集やアップデート等を実施することが重要となる。

(3) CMS の脆弱性を悪用した攻撃

CMS は、Web サイトのコンテンツの作成・管理に使用されるソフトウェアである。CMS の特徴として、「プラグイン」と呼ばれるソフトウェアを導入することで、機能の拡張が容易であることが挙げられる。プラグインを利用することで、Web サイトの運営者に専門知識がなくても、自身のニーズに合わせた Web サイトの作成・管理が可能となる。

2018 年度は 2017 年度に引き続き、WordPress や Drupal といった、利用者が多い CMS 本体やそのプラグインに存在する脆弱性が悪用されている。WordPress プラグイン「WP GDPR Compliance」には、権限昇格に関する脆弱性があり、これを悪用され、URL 設定を書き換えられたことで、不正なサイトに誘導する踏み台とされてしまった被害が多数報告されている※77。また、Drupal には、リモートから任意のコード実行が可能な脆弱性があり、これが悪用され、コインマイナーの不正なインストール等が行われたと報告されている※78。

脆弱性の中には、対策が公表されてから数時間の間に攻撃が行われるものがあり、2018 年度に公開された CMS の脆弱性でも公表直後の攻撃事例が報告されている※79。そのため、CMS の脆弱性に対する対策の実施手順を事前に整えていたとしても、攻撃が行われる前に対策の実施が終わらないことが被害発生の要因の一つと推測される。

対策が公開された直後に迅速にこれを実施するためには、事前の準備が重要である。システム等について、構成管理を適切に行い、システムを構成するソフトウェア等の脆弱性に関する情報収集を日々行う必要がある。同時に、事前に対策の実施手順を整えておくことで、脆弱性の対応を遅滞なく着実に実施できる。更に、公開している Web サイトのステージング環境※80 を事前に用意しておき、当該 Web サイトへ対策を実施する前に、実施による不具合が発生しないか迅速に検証することが望ましい。

対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

- 脆弱性情報の収集方法
- 脆弱性情報が確認された場合の対応方法
- 緊急度や深刻度に応じた対応の優先度
- 他部署への連絡の要否基準

また、このような実施手順の準備に加え、攻撃を受けてしまった場合に実施する対策を定めておくことを推奨する。

(4) IoT 機器を対象とした攻撃

2018 年度は、2017 年度に引き続き、IoT 機器を狙うウイルス「Mirai」の亜種が新しく登場している。亜種の一つとして、特定の IoT 機器をターゲットとする「Wicked」と呼ばれるウイルスが報告されている※81。Wicked は既知の脆弱性を悪用する手口を用い、感染させた IoT 機器に別のボットウイルスのダウンロードとインストールを実行する(「3.2.1(1)(e) Wicked」参照)。

製品開発者が IoT 機器に組み込まれているファームウェアの脆弱性に対応する修正プログラムを公開していたとしても、利用者の失念、認識不足等により修正プログラムの適用やアップデートがされず、放置される場合がある。Wicked は、そのような既知の脆弱性を有したままの IoT 機器を狙ったものと推察される。

今後も Wicked のように既知の脆弱性を有したままの IoT 機器を狙ったウイルスが登場する可能性がある。これを踏まえて、IoT 機器を安全に保つためには、以下の対策が必要となる。

- 製品開発者が行うべき対策
  - 開発ガイドラインにすべての工程で実施すべきセキュリティ対策を追加する。
  - 製品で使用する部品の調達に関し、契約等において脆弱性対処の項目を含める。
  - 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施する。
  - 製品に関する脆弱性が発見・報告された場合、速やかに修正プログラムを公開する。
  - 製品利用者が意識することなく、修正プログラムのアップデートが実施できるように製品に自動更新機能等を組み込む。
  - 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する。
- 製品利用者が行うべき対策
  - 製品開発者が提供する、製品の問題や安全に運用するための注意点、アップデートの方法等の情報を確認した上で使用する。
  - パソコン等の端末とは異なり、脆弱性情報が入手しづらい状況にあるため、積極的に情報を収集する。具体的には、IPA が公開している「JVN iPedia※82」や、IPA から送付されるセキュリティ対策情報の通知メール※83、製品開発者の Web サイトで公開される情報等について、利用している製品の脆弱性が公表されていないか定期的に確認する。
  - 製品開発者が修正プログラムを公開した場合、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。

1.2.5 ランサムウェア

ランサムウェアとは、パソコン及びネットワーク接続された共有フォルダ等に保管された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、「ransom」(身代金)と「software」(ソフトウェア)を組み合わせた造語で、ランサムウェアと呼ばれている。

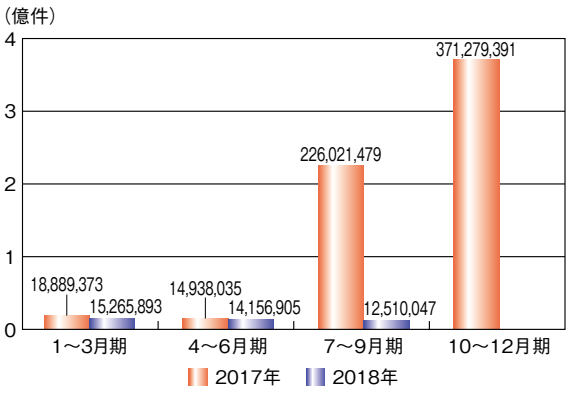
2017 年は 5 月の Wanna Cryptor(別名 WannaCry)の流行を皮切りに、ランサムウェアによる攻撃が大幅に増加していった。2018 年になって落ち着きを見せているものの、Wanna Cryptor やその亜種による攻撃は現在も続いており、新種のランサムウェアも確認されている。

本項では、ランサムウェアによる攻撃の傾向や、新たに確認されたランサムウェアについて解説する。

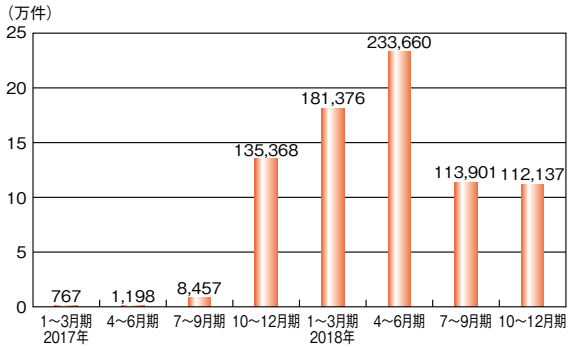
(1) 減少したランサムウェア攻撃

セキュリティベンダの調査によると、2017 年 7 ～ 9 月期のランサムウェアの全世界における攻撃総数は 2 億 2,602 万 1,479 件(前期比約 15 倍)、同年 10 ～ 12 月期は 3 億 7,127 万 9,391 件(前期比約 1.6 倍)と大きく増加している。しかし、2018 年 1 ～ 3 月期になると 1,526 万 5,893 件(前期比約 96% 減)と激減し、以降、横ばいで推移している(図 1-2-13)。

また、仮想通貨の不正な採掘(不正マイニング)に使用された可能性のあるプログラムの検出件数は、2017 年 10 ～ 12 月期から 2018 年 4 ～ 6 月期にかけて急激に増加し、2018 年 7 ～ 9 月期以降は減少したものの高止まりを続けている(図 1-2-14)。



■図 1-2-13 ランサムウェア攻撃総数
(出典)トレンドマイクロ社「日本と海外の脅威動向を分析した『2018 年第 3 四半期セキュリティラウンドアップ』を公開※84」を基に IPA が編集



■図 1-2-14 国内における仮想通貨採掘プログラムの検出件数
(出典)トレンドマイクロ社「2018 年 年間セキュリティラウンドアップ」を基に IPA が編集

これらの件数の推移から、2018 年においてランサムウェアの攻撃総数が減少した理由の一つとして、サイバー犯罪者による金銭獲得の手段がランサムウェアから仮想通貨の不正マイニングに移行している可能性が考えられる。ランサムウェア対策のためバックアップを取得する企業が増えたために金銭を得ることができないケースが多くなってきたことや、仮想通貨の価値が高騰し、少額ながらも確実に金銭を得られる仮想通貨の不正マイニングの方が高パフォーマンスと判断されたこと等が要因として推測される。

なお、2018 年第 3 四半期以降は仮想通貨の価格が暴落したこともあり、不正マイニングウイルスの感染に沈静化の傾向がみられる。

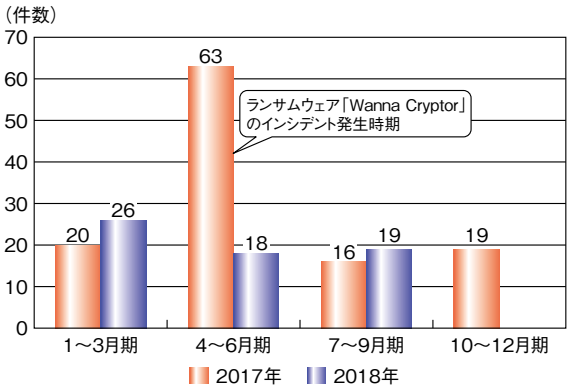
(2) 企業を狙ったランサムウェア攻撃

攻撃総数は減少しているものの、攻撃自体がなくなったわけではない。むしろ、手口が巧妙化し、企業等の重要な端末が狙われる傾向が見られ、依然として警戒が必要な状況である。ここでは、企業を狙ったランサムウェア攻撃について述べる。

(a) 増加する被害件数

セキュリティベンダの調査によると、2017 年と比較して、2018 年の国内外での法人の被害事例は、前年に Wanna Cryptor による攻撃が行われた 4 ～ 6 月期を除けば総じて前年同期比で増加している(次ページ図 1-2-15)。

ランサムウェアが要求する身代金は端末 1 台あたりお



■図 1-2-15　英語圏を中心とした主なランサムウェア被害事例件数
(出典)トレンドマイクロ社「日本と海外の脅威動向を分析した『2018 年第 3 四半期セキュリティラウンドアップ』を公開」を基に IPA が編集

おむね数百米ドル程度である（例：ランサムウェア「CryptoWall11」の身代金は 500 米ドル、日本円で約 5 万円）※85。

個人に支払わせることを想定すると、身代金を極端に高額にすることはできない。また、一般的に個人の端末では企業の端末に比べ重要な情報が保存されることが少ないため、高額な身代金が支払われる可能性も低い。

一方、企業には多くの端末や重要な情報が存在し多額の金銭を得られる可能性が高い。また企業では、バックアップを取得していてもバックアップからの復旧には日数がかかることもある。そのため、復旧までの経済的損失より少額となる身代金を払ってしまう企業も存在する※86。こうした背景から、ランサムウェアによる攻撃は企業に標的を絞り、被害が増加していると推察される。

(b) SamSam による被害

2018 年もランサムウェア SamSam※87 による被害が継続している。

SamSam に感染させる手口は、一般的なランサムウェア感染を狙う手口と異なる。ばらまき型メールにより添付ファイルを開かせたり、Wanna Cryptor のような自己感染機能によって感染させたりするのではなく、攻撃者は攻撃対象とする組織のネットワークに侵入することから始める。侵入後は組織内のシステムを調査し、バックアップデータ等の重要なデータを狙って SamSam に感染させる。ネットワークへの侵入やシステムの調査等、攻撃者の手間はかかるものの重要なデータが暗号化され、バックアップによる復旧もできない状態とすることから被害は大きく、身代金を支払う組織も少なくないという。

2018 年 3 月には米国アトランタ市が SamSam による攻撃を受け、多くのオンラインサービスが停止したという。同市は身代金を払わなかったが、重要なデータが失われ、被害額は最低でも 260 万ドル（約 2 億 8,800 万円）に上ると見られている。

以上のように、個人はもちろん、各企業もランサムウェアに対する継続した警戒が必要である。

(3) 特殊なランサムウェア

2018 年は、以下に示すような特殊なランサムウェアが確認された。

(a) ゲームのプレイが解除条件のランサムウェア

特定のゲームを 1 時間プレイすることが暗号化されたファイルの解除条件となるランサムウェアが確認された※88。実際にはゲームを 1 時間プレイする必要はなく、当該ゲームの TlsGame という名前のプロセスが 3 秒動作していれば解除されるというものであった。

「ジョークソフト」に近いものではあるが、ファイルを暗号化する動作はランサムウェアそのものであり、被害者からすればジョークでは済まないものである。

(b) ランサムウェアと不正マイニング機能を併せ持ったウイルス

ランサムウェアから仮想通貨の不正マイニングへ攻撃が移行していると前述したが、ランサムウェアと仮想通貨の不正マイニング機能を併せ持ったウイルスも確認されている※89。

セキュリティベンダによれば、当該ウイルスは、感染した端末の AppData フォルダ内にビットコインの取り引きで使用されるフォルダ「Bitcoin」が存在する場合は、ランサムウェアとして攻撃を行い、「Bitcoin」が存在せず、端末内に二つ以上の CPU が存在する場合は、不正なマイニングを行う仕組みであるという。

効率よく金銭を獲得したいと考える攻撃者によって作成され、攻撃に使われているものと推測される。

(4) ランサムウェア提供サービス

2013 年ごろからアンダーグラウンド市場でランサムウェアの需要が高まるとともに、ダークウェブ上で、ランサムウェアを提供するサービス RaaS（Ransomware as a Service の略称）が確認されており、2018 年にもその存在が確認されている。

このサービスは、ダークウェブにアクセスできれば利用可能であり、攻撃者は RaaS を使って新たなランサムウェアを容易に作成できる。RaaS によるランサムウェアで支

払われた身代金は、提供者と利用者によって山分けされる。RaaS 提供者は、ランサムウェア作成のハードルを下げ、攻撃をほう助することで金銭を獲得し、利用者はランサムウェアを作成する技術や手間を省いて金銭を獲得する仕組みである。

ランサムウェアは、RaaS によって手軽な攻撃手段となっているため、依然として警戒が必要である。

(5) ランサムウェアの感染を防ぐ対策

様々なランサムウェアが確認されているが、感染を防ぐ対策は他のウイルスと共通である。以下に基本的な対策を示す。

なお、IPA ではランサムウェアの概要や対策を解説したテクニカルウォッチを公開している※90。そちらも参考にしていただきたい。

(a) 基本的なウイルス対策

企業に対する標的型攻撃メール等と同様に、被害者にリンクをクリックさせることによって不正な Web サイトに誘導したり、不正なファイルを開かせることで、ランサムウェアに感染させる手口が想定される。以下のような基本的なウイルス対策を実施することが重要である。

- 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。
- セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ。

また、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て、ランサムウェアに感染させる手口も想定される。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も対策となる。

(b) 通信制御における対策

システムの環境によっては即時の修正プログラムの適用ができない等、脆弱性への至急の対策が難しい場合がある。このとき、脆弱性が存在する端末が不正な攻撃パケットを受け付けてしまうことで攻撃が成立し、ランサムウェアに感染してしまう可能性もある。このような場合、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。

(6) ランサムウェアの感染に備えた対策

ランサムウェアに感染した場合、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対象機器と接続する。
- バックアップ中に感染する可能性を考慮し、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。

また、バックアップを取得していても、復旧においてそれを活用できず、身代金の支払いを選択してしまっては対策の意味がない。バックアップからの復旧を素早くかつ確実に行えるよう、復旧のための対応フローの整備、訓練、復旧テスト等を実施しておくことも重要である。

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※91」では、複数の復号ツールを提供している。ツールはすべてのランサムウェアに対して有効とはいえないが、ランサムウェアの被害に遭ってしまった場合でも、暗号化されたファイルを復号できる可能性がある。

1.2.6 パスワードリスト攻撃

2018 年度は、パスワードリスト攻撃が原因とされる不正ログイン事案が多数発生、報道された。アカマイ・テクノロジーズ合同会社の調査結果によれば、2018 年 5 月から 6 月までの不正なログイン試行が 83 億件以上検出※92 されていた等、パスワードリスト攻撃による脅威の増加が世界規模で確認されている。

(1) パスワードリスト攻撃の被害事例

株式会社ドワンゴは、2018 年 5 月と 7 月に niconico アカウントに対してパスワードリスト攻撃によると考えられる不正ログインが複数検出されたとして、利用者に向けて注意喚起を行っている※93。

株式会社ケイ・オプティコム(現:株式会社オプテージ)は、2018 年 8 月、同社が提供するサービスを利用するための eoID に対して、パスワードリスト攻撃による不正なログイン試行が確認されたことを報告している※94。不

正ログインが確認された延べユーザ数は、7,131 件に上るという。

株式会社 NTT ドコモは、第三者が正規の利用者になりすまして iPhone X の購入手続きを行い、コンビニエンスストアでの受取指定とすることで不正に入手していた事案[※95]について、2018 年 8 月、パスワードリスト攻撃による d アカウントへの不正ログインが原因であったとして 2 段階認証の利用を呼びかけている[※96]。

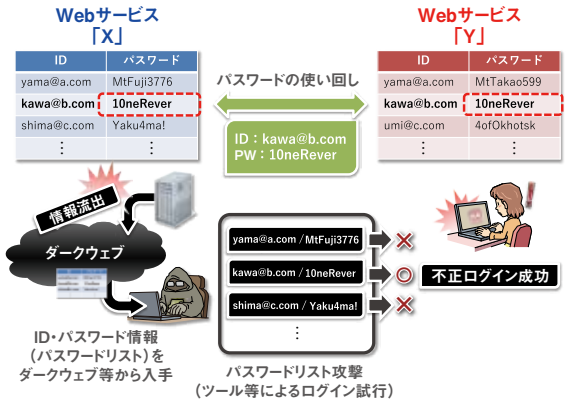
イオンマーケティング株式会社は、2018 年 9 月に同社の「smartWAON」サイトにおいて、パスワードリスト攻撃によって 52 名の利用者がワオンポイントの不正移行被害を受けたことを報告している[※97]。

株式会社ローソンは、2018 年 9 月にローソン ID サイトにパスワードリスト攻撃による不正なログイン試行が確認されたことを受け、会員のパスワードリセットを実施している[※98]。更に、翌 10 月には同社の「おさいふ Ponta」サイトにおいてパスワードリスト攻撃によってチャージ残高の不正移行被害が発生している[※99]。

上記以外にも、株式会社マーケティングアプリケーションズの「アンとケイト」[※100]、四国電力株式会社の「よんでんコンシェルジュ」[※101]、株式会社アプラスの「NETstation*APLUS」[※102]において、いずれも 2018 年 8 月にパスワードリスト攻撃が確認されたことが報告されている。

(2) パスワードリスト攻撃の手口

パスワードリスト攻撃とは、不正アクセスやダークウェブ[※103]から入手した ID とパスワードの組み合わせをリスト化した情報（パスワードリスト）を用いて、他の Web サービスに不正ログインを試みる手口である。そのため、複数の Web サービス利用において、パスワードの使い回し（同一パスワードの設定）をしていた場合、不正ログイン被害に遭う可能性が高まる（図 1-2-16）。



■図 1-2-16　パスワードリスト攻撃の例

パスワードリスト攻撃では、攻撃対象となる Web サービス以外の場所から入手した情報を用いるため、ログイン試行をする ID の一致率が高くなることはあまり考えにくい。しかし、2018 年 6 月に発生した株式会社ディノス・セシールの通販サイト「セシールオンラインショップ」へのパスワードリスト攻撃では、不正なログイン試行 1,938 件のすべてが登録済み ID と一致していた。そのため、一時は同社からの ID の流出も懸念されたが、後の調査において、同サイトが有する新規顧客登録申請時の二重登録防止機能を悪用され、事前にパスワードリストの ID がスクリーニングされていたことが判明した[※104]。

(3) パスワードリスト攻撃への対策

パスワードリスト攻撃による被害に遭わないための対策を、サービス利用者、提供者それぞれについて述べる。

(a) サービス利用者の対策

パスワードリスト攻撃は、複数の Web サービスで同一パスワードを設定していることを前提として、不正ログインを試みる手口である。そのため、サービス利用者が取るべき対策としては、パスワードの使い回しをしないことである。

また、ダークウェブ上には過去の不正アクセス等で蓄積された数十億以上のパスワード情報が、攻撃者が利用可能な状態で流通しているといわれる[※105]。過去、不正アクセス被害が報じられたサービスを利用していた場合は、その際に設定していたパスワードを使わないことも必要である。

多数の Web サービスを利用している場合は、それらのすべてに異なるパスワードを設定し、記憶することが難しいこともある。その際は、パスワード管理ツールを活用する、パスワードの一部をメモに書いて管理する等の手段を用いて、パスワードの使い回しをしないことを強く推奨する。

なお、パスワードリスト攻撃の手口に限らず、第三者による不正ログイン被害を防ぐことにも有効であるため、2 段階認証の機能が提供されている場合は積極的に利用することが望まれる。

(b) サービス提供者の対策

パスワードリスト攻撃では、基本的に一つの ID に対して 1 回のみのログイン試行となるため、正規の利用者がたまたま認証に失敗したログイン行為との区別が難しく、サービス提供者が攻撃の検知や対策がしにくい手口と言

える。攻撃を早期に検知する方法としては、例えばWAF※106を導入して、複数のIDに対して同一の送信元からのログイン試行ではないか、従来と異なる環境（海外からのアクセス等）からのログイン試行ではないかといったことから判断、対処する等が挙げられる。

また、パスワードリスト攻撃の手口に限らず、利用者が不正ログイン被害に遭わないために、2段階認証の機能の提供を検討することも望まれる。

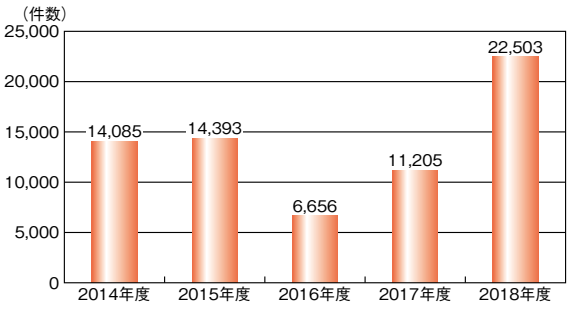
なお、前述の株式会社ディノス・セシールの事例のように、本来、二重登録を防止するための機能が、登録済みIDの有無を確認（スクリーニング）するために悪用されるケースもある。サービス提供者として、利用者の使いやすさに配慮する必要もあるが、便利な機能が意図せぬ目的に悪用される可能性もあることに留意されたい。使いやすさを向上させる機能の提供においては、一定の利用制限を設ける等、悪用されないための対策についても慎重に検討することが望まれる。

1.2.7 フィッシングによる詐欺

フィッシング（Phishing）は、クレジットカード情報、個人情報、銀行口座情報、アカウント情報（ユーザID・パスワード）等を、正規の企業等を装って、利用者から騙し取る攻撃である。近年仮想通貨の普及に伴い、仮想通貨関連サービスの認証情報が狙われる事例も確認されている※107。

フィッシング対策協議会に寄せられたフィッシングの報告件数は、2016年度に減少したが、その後増加傾向にあり（図1-2-17）、2018年度は毎月1,000件を超える状況が続いた（図1-2-18）。

同協議会の注意喚起事例では、前年度に引き続きAmazon.com, Inc.やApple Inc.といった利用者の多いサービス事業者や、カード会社をかたるものが多かった（次ページ図1-2-19）。



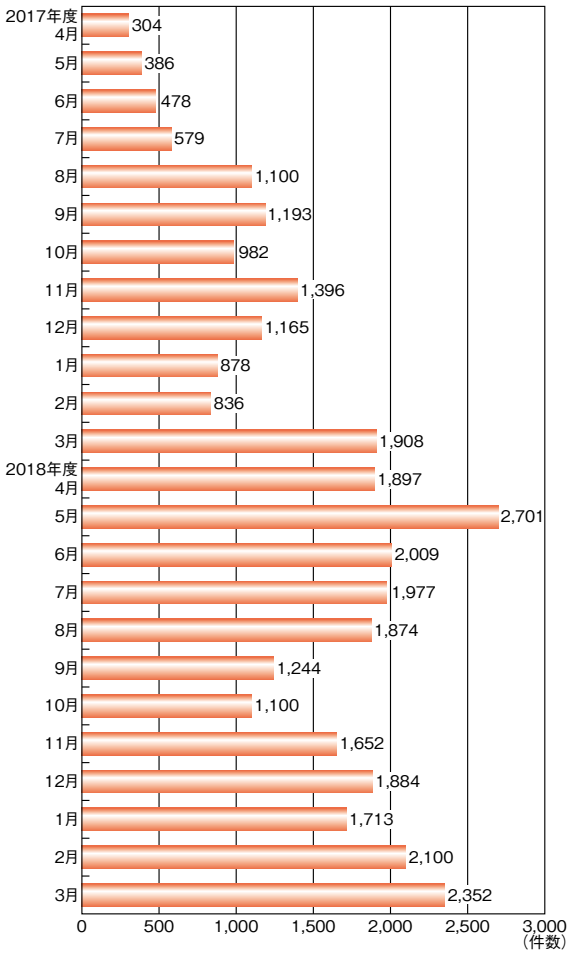
■図1-2-17　フィッシング対策協議会に寄せられた報告件数推移（年度別）
（出典）フィッシング対策協議会「月次報告書※108」（2014年4月～2019年3月）を基にIPAが作成

(1) メールによるフィッシングの手口

フィッシングの典型的な手口では、正規の企業等をかたって「第三者によるアクセスを確認した」「クレジットカードが有効期限切れである」等の内容の偽メールを送ってフィッシングサイトに誘導し、そこで情報を入力させ詐取する。メール本文中のURLからフィッシングサイトへ誘導するケースのほかに、メールの添付ファイルから誘導するケースもある※110。

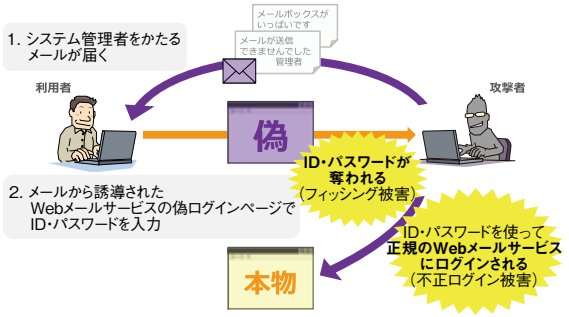
2018年4～6月を中心に、大学のWebメールサービスを狙ったフィッシング被害が相次ぎ、6月に文部科学省が全国の大学に対して注意喚起を行った※111。また、IPAでは、各大学による公開情報やIPAにて受け付けた不正アクセス届出を基に事例をまとめ、注意を呼びかけた※112。

IPAが注意喚起したフィッシングの手口は、主に次のような流れであった（次ページ図1-2-20）。



■図1-2-18　フィッシング対策協議会に寄せられた報告件数推移（月別）
（出典）フィッシング対策協議会「月次報告書」（2017年4月～2019年3月）を基にIPAが作成

■図 1-2-19　フィッシング対策協議会によるブランド別注意喚起件数
（出典）フィッシング対策協議会「緊急情報一覧※109」を基に IPA が作成



■図 1-2-20　大学における Web メールサービスを狙ったフィッシングの例

①大学で利用している Web メールサービスのシステム管理者を装い、送信エラーや「メールボックスがいっぱいである」等と記載されたメールが、大学の学生や教職員宛てに送られる。
②メールに記載されている URL をクリックすると、Web メールサービスの正規のログインページを模した偽ログインページに誘導され、そのページで利用者が ID とパスワードを入力してしまうと、それらが詐取される。

詐取された ID・パスワードで Web メールサービスのアカウントに不正ログインされたことで、設定を変更され受信メールが外部転送されたり、踏み台にされ他大学等へフィッシングメールが送信されたりする等の被害が発生した。

(2) SMS によるフィッシングの手口

携帯電話やスマートフォンの SMS（Short Message Service）を使用し、メッセージ本文中の URL からフィッシングサイトに誘導する手口も存在する。メールによるフィッシングと区別する意図で、SMS フィッシング（SMS phishing）やスミッシング（Smishing）と呼ぶこともある。

2018 年度は、佐川急便株式会社やヤマト運輸株式会社といった宅配便業者の不在通知を装う事例や、株式会社 NTT ドコモが提供する共通 ID サービス「d アカウント」を狙う事例での被害が目立った（「3.3.1 宅配便業者を装う不在通知 SMS の手口」「3.3.2（1）d アカウントを狙ったフィッシングの手口」参照）。

(3) 対処

フィッシングのメールや SMS が届いた場合は、記載された URL や添付ファイルには触れず、当該メールや SMS を削除するだけで問題ない。

もし、フィッシングサイトで情報を入力してしまった場合は、入力した情報に応じて、以下のように状況確認や

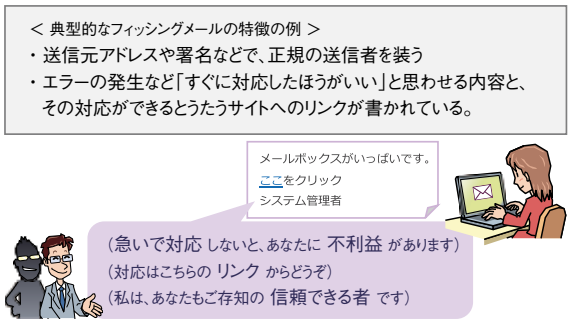
対応をしていく必要がある。

- クレジットカード情報を入力した場合：
  クレジットカード会社に相談し、利用履歴の確認やカード番号の変更を行う。
- アカウントの認証情報を入力した場合：
  至急、正規サイトでパスワードを変更し、不審なログインや利用の有無を確認する。不正利用があった場合等、必要に応じて、そのアカウントのサービス提供会社に相談する。
- 銀行口座情報を入力した場合：
  対象金融機関に相談する。

(4) 対策

フィッシングに対する対策を以下に示す。

- フィッシングの手口の基本を知る
  典型的なフィッシングの手口や、フィッシングのメールやSMSの特徴といった基本を知ることが重要である（図1-2-21）。そうすることで、多くの場合にフィッシングかどうか判断することが可能になる。フィッシング対策協議会からは、フィッシング対策ガイドラインが提供されており※113、こちらも参照されたい。なお、今後も新しい手口が出現することが予想されるため、最新情報を継続的にチェックしていく必要がある。



■図1-2-21　典型的なフィッシングメールの特徴の例

- メール・SMS内のリンクを安易にクリックしない
  メール・SMSのリンク機能は便利だが、不審なサイトへの誘導にも使われる。そのため、メール・SMS内のリンクを安易にクリックしない習慣を身に付けたい。
  - よく利用するサイトは、正しいと確認できているURLをあらかじめ「お気に入り」（ブックマーク）に登録しておき、それを使用してアクセスする。
  - もしメール・SMS内のリンクを使用する場合は、URLが正規のものであるかを必ず確認する。自身の行為によって送られてきたメール・SMS（例：パスワードの変更申請をして直後に届いた連絡メール等）ではなく、何もしていないのに突然送られてきたメール・SMSのリンクには、特に警戒する。
  - HTMLを使用しているメールの場合は、「表示上のURL」と「アクセス先のURL」を異なるものにできるため、リンクにマウスカーソルを当てる等の方法で実際のアクセス先となるURLを確認する。
  - SMSで使われることの多い短縮URL（元のURLを変換して短く表示するサービス）は、不審なサイトへの誘導に悪用されやすいため、元のURLを確認できるサービスを使用する等、信頼性を確認してから利用する。
- メール・SMSの真偽は確かな情報源で確認する
  送信元や文面が本物らしく、巧妙で判別が難しいフィッシングも確認されている。そのため、これまで届いたことのない内容のメール・SMSやリンクのクリックを誘う内容のメール・SMS等が届いた際に、それが本物かどうか判断に迷った場合は、確かな情報源を使って確認することを推奨する。メール・SMS本文に記載されている連絡先に連絡をしたり、届いたメール・SMSへ返信して問い合わせたりすることは避ける。
- システム的なセキュリティ対策を実施する
  手口や対策を知っていても、誰もが、いつでも、すべてのメールを正しく見分けることは容易ではない。そのため、フィッシング対策機能を持つセキュリティソフトを導入して判断しやすくする、万が一パスワードを詐取された場合の不正ログイン防止のために2段階認証を利用する等、システム的なセキュリティ対策の実施を検討していただきたい。

(5) メール・SMS以外のフィッシングの手口

フィッシングの手口は多様化してきている。そのため、インターネット利用者は、日頃から情報収集をして手口を知ることが重要である。

ここではメールやSMS以外のフィッシングの手口についていくつか概要を紹介する。

- 正規サイトの改ざんによるフィッシング
  ECサイト等の正規サイトが改ざんされ、商品購入手続きの過程で、本来のページではなく、攻撃者が用意した個人情報やクレジットカード情報を詐取するページに誘導される。2018年度には、複数のサイトで被害が報告されている（次ページ表1-2-3）。
- スマートフォンの不正アプリによるフィッシング
  スマートフォンの不正アプリの中には、フィッシングを目

組織	サイト	公表日	概要
聖教新聞社	SOKAオンラインストア	2018年10月9日	当該サイトが改ざんされ、商品購入時に「偽のクレジットカード決済画面」に誘導された。2018年7月30日～2018年8月24日の間に当該サイトでクレジットカードを使用した利用者のクレジットカード情報が不正に取得された可能性がある※114。
ディー・エル・マーケット株式会社	DLmarket	2018年10月22日	当該サイトのクレジットカード決済ページが改ざんされ、本来遷移するはずのクレジット決済代行会社のページではなく「偽の決済フォーム」に誘導された。2018年10月17日～2018年11月12日の間に偽の画面に入力した利用者のクレジットカード情報が不正に取得された可能性がある※115。
株式会社伊織	伊織ネットショップ	2018年10月24日	当該サイトが改ざんされ、支払い方法に関わらず「偽のクレジットカード番号入力画面」へ誘導された。2018年5月8日～2018年8月22日の間に偽の画面に入力した利用者のクレジットカード情報が流出し、一部のクレジットカード情報が不正利用された可能性がある※116。
株式会社洋菓子舗ウエスト	銀座ウエストオンライン通販サイト	2018年12月18日	当該サイトが改ざんされ、「偽のクレジットカード番号入力画面」へ誘導された。2018年9月12日～2018年11月2日の間に当該サイトでクレジットカードを使用した利用者のクレジットカード情報が漏えいした可能性がある※117。
株式会社ハセ・プロ	オンライン通販ショップ	2019年2月26日	当該サイトが改ざんされ、クレジットカード決済を選択した場合に、本来遷移するはずのクレジット決済代行会社のページではなく「偽の決済フォーム」に誘導された。2018年10月1日～2019年1月24日の間に偽の画面に入力した利用者のクレジットカード情報が不正に取得された可能性がある。取得されたクレジットカード情報が、他社のECサイト等で不正利用された事例が確認されている※118。
ジェイ・ワークス株式会社	ショコラ ベルアメール オンラインショップ	2019年4月15日	当該サイトが改ざんされ、クレジットカード決済を選択した場合に「偽のクレジットカード情報入力画面」に誘導された。2018年8月6日～2019年1月21日の間に偽の画面に入力した利用者のクレジットカード情報が流出した可能性がある※119。

■表 1-2-3　2018年度のサイト改ざんによるフィッシング事例

的としているものも存在する。

セキュリティベンダによると、2018年6月、Google LLCの公式アプリストアであるGoogle Playに偽のファイナンスアプリ（金融取引情報アプリ）が見つかった※120。これらのアプリはニュージーランド、オーストラリア、英国、スイス、ポーランドの銀行や、オーストリアの仮想通貨取引所のアプリを装い、クレジットカード情報やインターネットバンキングのログイン認証情報を入力させて、盗み出すものであった。

- DNS情報の書き換えによるフィッシング

DNSサーバのキャッシュや、ルータやパソコンに設定するDNSサーバ情報、パソコンのhostsファイル等、ドメインと接続先IPアドレスの対応付けを管理する情報を、攻撃者が脆弱性の悪用やウイルス等により不正に書き換えることで、利用者が正しいURLを指定しても、本物のサイトに模したフィッシングサイトへ誘導される。この手口は「ファーミング」（Pharming）とも呼ばれる。

2018年4月には、仮想通貨のウォレットサービスを行うMyEtherWallet.com（以下、MEW）で、利用者のウォレットから仮想通貨が盗まれる被害が発生した。DNSサーバが何者かによってハッキングされ、そのサーバを利用していた利用者がMEWの公式サイトにアクセスしようとするとフィッシングサイトにリダイレクトされることが原因とされている※121。

1.2.8 偽の警告や偽サイトを用いた詐欺等

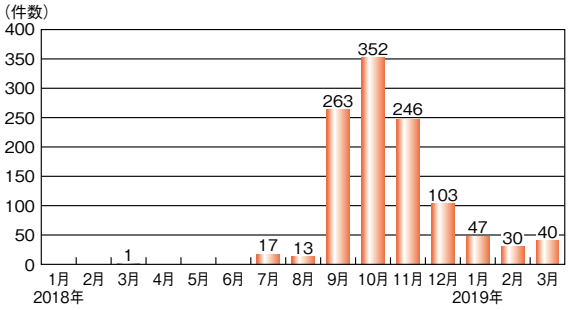
不安や恐怖心の喚起や、利得による誘惑等で、インターネットを利用する人を騙す手口には、様々なものが存在する。本項では、「仮想通貨を要求する脅迫メール」「偽セキュリティ警告」「偽サイト」の手口と対策を紹介する。

(1) 仮想通貨を要求する脅迫メール

2018年度、性的な映像をばらまく等と騙して、仮想通貨を要求する脅迫メールが世界中で多数出回った。JPCERT/CCから事例が報告され※122、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）からも、犯罪被害につながるメールとして注意喚起がなされている※123。

IPAでも、「安心相談窓口だより」にてこの手口を取り上げた※124。安心相談窓口において、初めてこの相談を受けたのは2018年3月であり、その後7月と8月は合わせて30件、9月は263件、10月には352件の相談が寄せられた（図1-2-22）。8月まではメールは英語で書かれていたが、9月中旬に日本語版が現れたほか、様々な言語の事例も確認されている。

2018年12月には、類似の文面でランサムウェア感染を狙ったメールが米国で観測された※125。メールには、パソコン内から盗み取った情報を保存してあるとしたURLが記載されており、それをクリックしてしまうと、GandCrab



■図 1-2-22　仮想通貨を要求する脅迫メールに関する月別相談件数推移

(ガンクラブ)という種類のランサムウェアに感染する。2019年3月末時点ではこの手口の日本語版メールは確認されていないが、JPCERT/CCは、今後日本語で日本国内に送られる可能性もあるとして注意を促している※126。

(a)手口

この手口のメールは複数のパターンが確認されているが、以下のような特徴がある。

①ウイルス感染やアカウントハッキングにより、他人に知られたくない情報(「アダルトサイトを閲覧している姿をWebカメラで撮影した」「不正を行っている証拠をつかんだ」等)や家族や友人の連絡先情報を盗みとったと、事実無根の内容で騙す。

②家族や友人へ映像等をばらまくと脅し、それを止める代わりとして、メールに記載されたビットコインアドレス(ウォレット)に仮想通貨(ビットコイン)の送金を要求する。

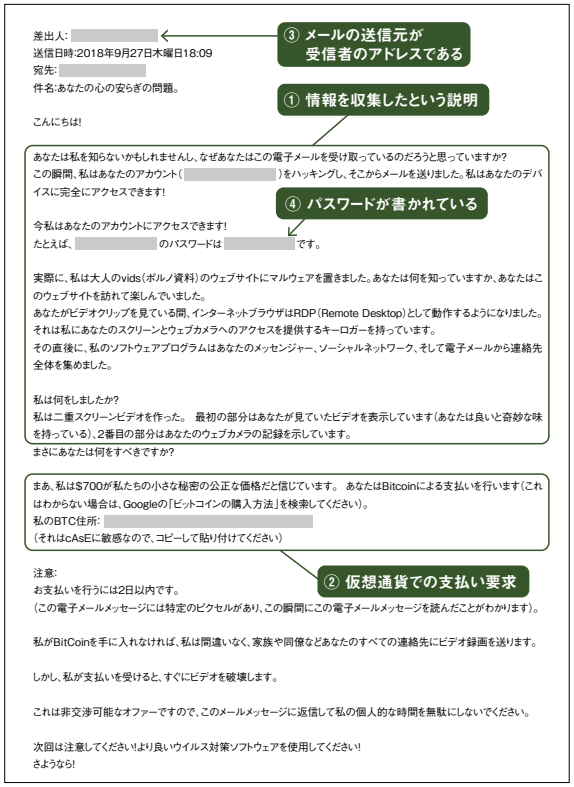
③メールの送信元がメール受信者自身のアドレスになっている場合がある。

④メールの件名や本文に、パスワードが一つ書かれている場合がある。

日本語版メールの日本語は、他言語から機械翻訳したような不自然なものであった(図1-2-23)。

メールに映像へのURLリンクや映像ファイルの添付があった、支払いに応じなかったためにばらまきを実行された等、実際に情報が窃取されていたという被害の報告はない。そのため、「セクストーション(性的脅迫)」※127の手口を模して、根拠のない内容で脅迫しているものと推測される。

なお、メールに書かれていたパスワードについては、相談事例では、まったく心当たりがないものである場合と、受信者が実際にWebサービス等で過去に設定した、または現在設定している場合があった。このため、攻撃者は、根拠なくパスワードを記載しているケースのほかに、



■図 1-2-23　仮想通貨を要求する脅迫メールの例(日本語版)

情報漏えいで流出した個人情報リスト等、何らかの方法でパスワードを入手しているケースもあると推測されるが、詳細は不明である。

(b)対処

仮想通貨を要求する脅迫メールが届いた場合、メールの内容は無視して、削除するだけで問題ない。なお、現在使用しているパスワードが書かれていた場合は、すぐにパスワードを変更し、併せて、そのパスワードを使っていたサービスへの不正アクセスがないか確認することを推奨する。

もし、URLの記載や添付ファイルがあった場合は、ウイルス感染等を狙う手口の可能性があるため、クリックしたりファイルを開いたりしてはならない。

(c)対策

こうした不審メールが届いた場合に冷静な確認と対処ができるよう、日頃から最新の動向を確認し、様々な不審メールが存在することを理解しておくことが望ましい。

パスワードについては、漏えいがあった場合の被害低減のためにも、日頃から使いまわしをしないよう、習慣づけたい。

(2) 偽のセキュリティ警告

2018 年度に IPA の安心相談窓口に寄せられた、偽のセキュリティ警告をきっかけに遠隔操作による有償サポート契約へ誘導される「偽警告」(別名 : サポート詐欺) の相談は、1,839 件だった (図 1-2-24)。また、同様の警告から有償ソフトウェアの購入に誘導される「偽セキュリティソフト」の相談は、2,030 件だった (図 1-2-25)。

以前より継続して多くの相談が寄せられている手口であるが、2018 年度に入って相談件数が増加し、また手口にも変化があったことから、IPA は 2018 年 7 月に「安心相談窓口だより」で改めて注意を呼びかけた※128。

2018 年 8 月に、Google LLC が、技術サポートをうたう詐欺的広告が増加しているとして対策を行うことを発表した※129。こうした取り組みにより、今後の被害低減が期待される。

(a) 手口

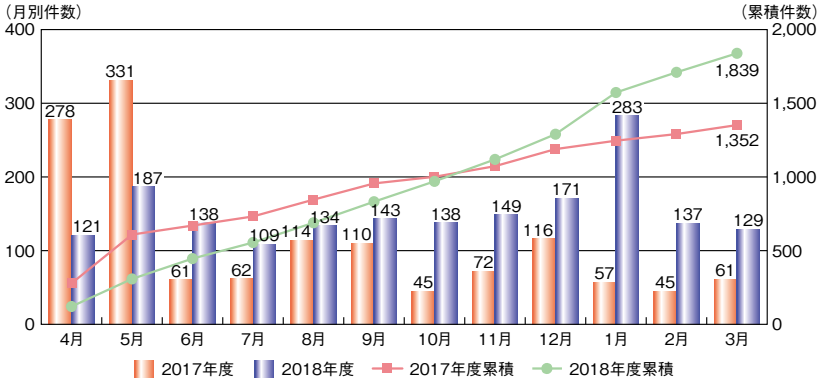
「偽警告」と「偽セキュリティソフト」の手口は、パソコンで Web サイトの閲覧中に、突然画面が切り替わり、「ウイルスに感染している」「システムが破損する」「○個のシステムの問題が見つかった」「○秒以内に対応しないとデータが全部削除される」「ドライバーが古い」等の偽のセキュリティ警告が表示されることから始まる (図 1-2-26)。これらの様々な警告画面では、次のような手口も確認されている。

- 画面表示とともに、警告音や警告メッセージを音声で流す。
- Web ブラウザの「×」(閉じる) ボタン等では閉じられない。また、ボタンを押す度に警告音が出る。
- カウントダウンを表示して、対応を急かす。
- メッセージ内容を信用させるため、実在の企業のロゴが使われている。

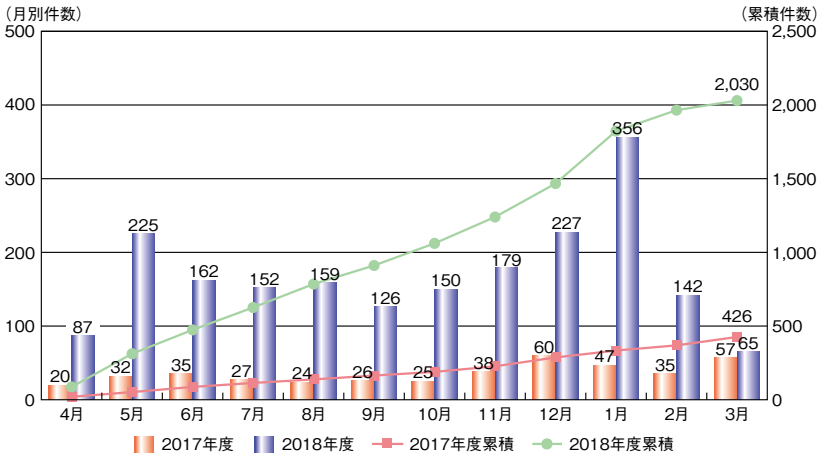
パソコンが壊れる等の不安が高まり、更に時間的な切迫もある状況では、偽のセキュリティ警告が信頼できる企業からの「助け舟」であるように見えるため、利用者は誘導に従ってしまう可能性がある。

「偽警告」の手口の流れは、以下のような場合が多い。

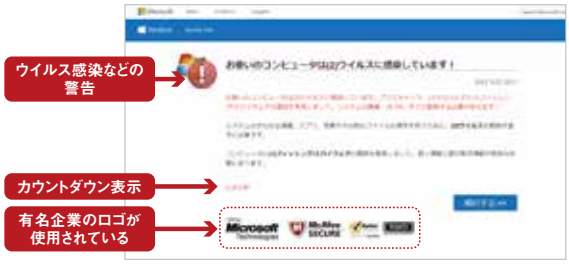
①警告画面に記載されている電話番号に電話をかけると、オペレーターがパソコンに至急の対処が必要であ



■図 1-2-24　偽警告に関する月別相談件数推移と年度累積



■図 1-2-25　偽セキュリティソフトに関する月別相談件数推移と年度累積



■図 1-2-26　偽のセキュリティ警告の画面例

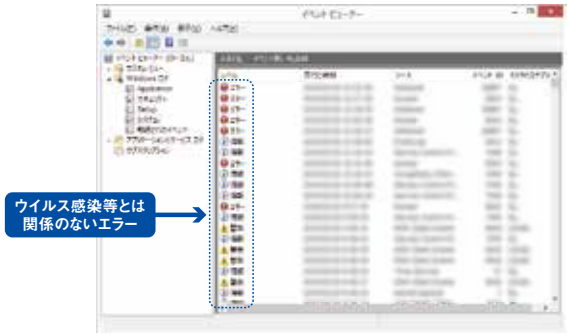
るとして、遠隔操作による対応を持ちかけてくる。

②オペレーターの指示に従い遠隔操作ソフトをインストールし、接続を許可すると、遠隔操作で「ウイルスに感染している証拠」等としていくつかの画面を表示させながらパソコンが危険な状況であると説明される。

③ウイルス除去等の作業料や今後の保守サポート契約料等として高額な代金を請求される。

④支払いに応じると、「パソコンの対処をする」として、オペレーターが数時間、遠隔操作で作業を行う。

なお、②において、ウイルス感染の証拠と称して示されるものの例としては、netstat（ネットワーク通信状況を確認するコマンド）の実行結果や、イベントビューアーの管理イベントのエラーログ（図 1-2-27）等がある。いずれもウイルス感染とは特に関係ない情報であるが、コマンドプロンプトの黒い画面に表示される英数字やエラーという言葉が、利用者の知識不足につけこんで、警告の信憑性を高めるために悪用されている。



■図 1-2-27　イベントビューアーの管理イベントのエラーログ例

また、④において、オペレーターが行う具体的な作業内容は不明であるが、この作業の中で、セキュリティソフトと称する詳細不明のソフトをインストールされる場合も多い。

「偽セキュリティソフト」の手口の流れは、以下のような場合が多い。

①警告画面に表示された問題を解決するためとして、「無料のセキュリティソフト」と称するものをインストールするよう誘導される。

②ソフトをインストールして実行すると、更にパソコンに問題が見つかったという診断結果が表示され（図 1-2-28）、有償版での対応が必要であるとして、ソフトの購入を迫る。

■図 1-2-28　無料セキュリティソフトによる検査（スキャン）結果表示の画面例

2017 年末ごろより、「偽警告」と「偽セキュリティソフト」を組み合わせた手口の相談が安心相談窓口に寄せられている。例えば、偽のセキュリティ警告から有償ソフトウェアの購入に誘導し、そのソフトウェアのアクティベーション（使用を可能にする操作）のために必要であるとして電話をかけさせ、遠隔操作による有償サポートで対処しないと危険な状況であると迫る、等の流れである。

これらの手口において請求される金額は様々であるが、サポート契約をした場合は 10 ～ 20 万円といった高額になる事例もある。支払い手段として指示されるのはクレジットカード決済が多いが、コンビニ決済、プリペイドカード、オンライン決済サービスの口座間送金等もある。また、一度支払ってしまうと、「まだ危険な状況がある」等様々な理由を付けて、追加の料金を得ようとする電話が何度もかかってくる場合もある。

契約してしまうと、契約先が海外事業者であることから英語が必要となり解約手続きがスムーズに進まないケースや、契約業者から届いたメールの案内に従って解約を申し出ても反応がないケースがある※130。

(b) 対処

偽のセキュリティ警告が表示された場合は、警告内容は根拠のないものであるため、画面を閉じるだけで問題はない。Web ブラウザの「×」（閉じる）ボタンで画面が閉じられない場合は、Windows であれば、タスクマネージャーから Web ブラウザを終了する、キーボードの「Alt」キーと「F4」キーを同時に押して Web ブラウザを終了す

るという方法がある。Mac であれば、「強制終了」ウィンドウから Web ブラウザを終了する、キーボードの「Command」キーと「Q」キーを同時に押して Web ブラウザを終了するという方法がある。またどちらの OS でも、パソコンを再起動する、といった方法でも対応できる。

パソコンに遠隔操作ソフトをインストールした場合は、アンインストールする。

利用者自身やオペレーターが偽のセキュリティソフト等をインストールした場合は、より安全な対応として、アンインストールではなく、当該ソフトをインストールする前の状態にシステムを戻すこと（Windows の「システムの復元」や、Mac の「Time Machine」で作成しておいたバックアップファイルによる復元）や、パソコンの初期化をすることを推奨する。

契約や購入をしてしまった場合は、消費生活センターや使用したクレジットカード会社へ相談していただきたい。

(c) 対策

偽のセキュリティ警告が表示される原因は、Web サイトに設置された広告枠に不正プログラムを含む広告が配信されることで偽の警告画面へリダイレクト（自動転送）される、あるいは Web サイトに故意または改ざんにより不正プログラムがあることで偽の警告が表示される等が推測される。安心相談窓口に寄せられる相談において、ニュースサイト、動画サイト、レシピサイト等、大手サイトを閲覧していたときに偽の警告画面が表示されたという事例も少なくないことから、不審なサイトを利用しないことだけでは、回避が困難である。インターネットを利用していれば誰でも遭遇する可能性があるものとして、偽のセキュリティ警告の手口と対処方法を知っておくことが肝要である。

セキュリティに関する警告画面が表示された際には、偽物である可能性を踏まえ、メッセージを見極める必要がある。使用している Web ブラウザやセキュリティソフトによる正規の警告画面や、セキュリティソフトメーカのサポート窓口等の相談先を、あらかじめ確認しておくことで、冷静な対処がしやすくなる。

(3) 偽サイト

正規のサイトに見せかけ不正行為を行う偽サイトは、様々なものが存在する。ここでは偽 EC サイトの手口を取り上げる。

偽 EC サイトは、警察、JC3、消費者庁、公益社団法人日本通信販売協会等で以前より注意喚起がされている[※131]が、2018 年度には、ふるさと納税サイトの偽サイトがあることが分かった[※132]。

2018 年 6 月には、JC3 が、国際的なフィッシング対策の非営利団体 Anti-Phishing Working Group（APWG）と共同で、偽 EC サイトの特徴を調査したレポートを作成し、公表した[※133]。

(a) 偽 EC サイトの手口

偽 EC サイトとは、インターネット上での商品・サービス販売を装った Web サイトで、金銭や個人情報を騙し取る手口である。正規の EC サイトをコピーしているタイプ（なりすまし EC サイト）と、一般的な EC サイトのように独自に作成されるタイプがある。偽 EC サイトでは、極端に値引きされた商品や、販売が終了して入手困難な商品が扱われている等の特徴がある。

偽 EC サイトの手口では、正規 EC サイトを運営する事業者も被害を受ける。自社の EC サイトに似せた偽サイトを作られる、偽 EC サイトの会社情報欄に自社の情報を使用される等により、偽 EC サイトの被害者から苦情や問い合わせが寄せられたり、信用が低下したりする。

2018 年 12 月、任意の自治体に寄付することで所得税と個人住民税から控除される「ふるさと納税」の寄付仲介サイトの偽サイトが複数あるとして、総務省、消費者庁、及び各自治体等から注意喚起がなされた。この偽サイトは、本来ありえない「寄付金額の割引」等をうたって返礼品を掲載し、利用者から寄付金を騙し取る。

(b) 対処

偽 EC サイトで購入してしまった場合は、消費生活センターや購入に使用したクレジットカード会社へ相談していただきたい。偽 EC サイトを見つけた場合は、通報先として、一般社団法人セーファーインターネット協会（Safer Internet Association：SIA）の「悪質 EC サイトホットライン[※134]」がある。

偽 EC サイトを作られてしまった事業者には、SIA より「なりすまし EC サイト対策マニュアル[※135]」として、対処方法が提供されている[※136]。

(c) 対策

EC サイトを利用する際は、各組織の注意喚起を参考に、対象サイトに偽サイトの特徴がないかを確認する習慣を付けるのが望ましい。一例として消費者庁が案内している偽サイトの特徴[※137]を以下に記載する。

- サイト内容：字体（フォント）に通常使用されない旧字体

が混じっている。機械翻訳したような不自然な日本語表現がある。
- 商品：極端に値引きされている。
- 支払方法：銀行振込のみ。
- 会社概要：住所が番地まで記載されていない。電話番号がなく連絡先がEメールしかない。

ただし、なりすましECサイトの場合等、偽ECサイトの見分けが困難である場合がある。正規のサイトをあらかじめWebブラウザのブックマーク（お気に入り）に登録しておきそこからアクセスする等、偽サイトに誘導されない工夫も必要である。

ECサイト運営者向けには、前述の「なりすましECサイト対策マニュアル」に予防方法も述べられている。

1.2.9 情報漏えいによる被害

2018年度も、多数の情報漏えい被害が発生している。本項では、外部からの攻撃、操作ミス等による過失、内部者の故意による不正のいずれかを主な要因とする情報漏えい被害について述べる。

(1) 外部からの攻撃による情報漏えい

2018年6月にJNSAが公開した「2017年 情報セキュリティインシデントに関する調査報告書【速報版】※138」（以下、JNSA調査報告書）によると、漏えい人数が最多のインシデントは118万8,355人で、その原因は不正アクセスであった。なお、漏えい人数の上位10件のインシデントの半数以上が、不正アクセスによるものだという（表1-2-4）。

前橋市教育委員会の事例※139では、前橋市教育情報ネットワークへの不正アクセスにより、2012年度から2017年度の前橋市在籍児童生徒及び教職員4万7,839人分の氏名や住所、電話番号等の情報ならびに同期間同市にて給食喫食していた園児児童生徒及び教職員2万8,209人の銀行名、支店名、口座番号等の情報が流出した可能性がある。

株式会社ダブリュ・アイ・システムの事例※140では、Webアプリケーションの脆弱性を悪用した外部からの不正アクセスにより、3,412件のクレジットカード情報が流出した可能性がある。

サンワ食研株式会社の事例※141では、外部からの不正なアクセスにより会員の個人情報が最大で8,928件、クレジットカード情報が最大で1,142件流出した可能性がある。

JR九州ドラッグイレブン株式会社の事例※142では、外部からの不正なアクセスにより、氏名や住所、電話番号、メールアドレス等の情報が最大で3万4,246件流出した可能性がある。更に、クレジットカード番号やセキュリティコード等、クレジットカード情報が458件流出した可能性があるという。

Marriott International, Inc.の事例※143では、傘下のStarwood Hotels & Resorts Worldwide, LLCの宿泊予約データベースへの不正アクセスにより、最大で3億8,300万件の情報が流出した可能性がある。流出した情報の中には、暗号化されていないパスポート番号約525万件が含まれるという。

株式会社オージス総研が運営する「宅ふぁいる便」サービスにおける事例※144では、外部からの不正なアクセスにより、氏名、メールアドレス、パスワード、生年月日、性別等の情報、481万5,399件が漏えいした。なお、漏えいしたパスワードは暗号化されていなかったとして、同サービスの利用者に対してパスワード変更を呼びかけている※145。また、2019年4月8日には、「宅ふぁいる便」に登録しているパスワードの確認や退会申し込みの受け付け等が行える特設サイトを公開している※146。

その他、外部からの攻撃によって情報漏えい被害が発生した主な事例を表1-2-5（次ページ）に示す。

順位	漏えい人数	業種	原因
1	118万8,355人	製造業	不正アクセス
2	67万6,290人	公務	不正アクセス
3	59万7,452人	情報通信業	不正アクセス
4	37万1,200人	情報通信業	不正アクセス
5	19万9,169人	公務	不正アクセス
6	19万人	サービス業	管理ミス
7	18万4,981人	公務	管理ミス
8	16万3,000人	公務	紛失・置忘れ
9	14万408人	情報通信業	不正アクセス
10	13万1,936人	卸売業、小売業	不正アクセス

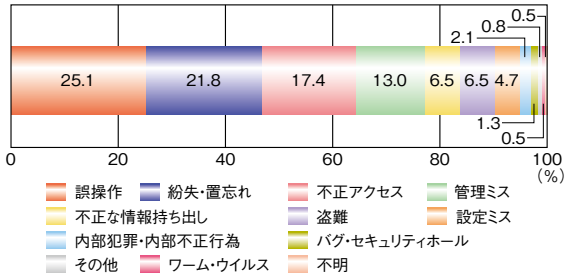
■表1-2-4　1件あたりの漏えい人数のトップ10
（出典）JNSA調査報告書を基にIPAが作成

(2) 過失による情報漏えい

前述のJNSA調査報告書によると、インシデント原因は「誤操作」が25.1%と最多であった。また、「紛失・置忘れ」が21.8%、「管理ミス」が13.0%、「盗難」が6.5%、「設定ミス」が4.7%等、原因の約7割が人為的な過失となっている（次ページ図1-2-29）。

情報公開日	組織名	内容
2018 年 4 月 27 日	宝塚山本ガーデン・ クリエイティブ株式会社	同社が園芸クチコミサイトの運営を委託している有限会社ビーアイティーが管理する Web サーバが不正アクセスを受け、メールアドレス、パスワード、氏名、性別等、最大 609 件の会員情報が流出した可能性がある※147。
6 月 4 日	森永乳業株式会社	同社が運営する健康食品通販サイトにおいて、脆弱性を悪用した不正アクセスによって、氏名、住所、電話番号等、最大 9 万 2,822 件の個人情報が流出した可能性がある。そのうち、最大 2 万 9,773 件はクレジットカード情報も流出した可能性がある※148。
6 月 16 日	ラッシュ株式会社	同社が運営する「キルフェボン WEB STORE」において、外部より不正アクセスを受け、会員のメールアドレスとパスワード情報 3 万 7,149 件が流出した※149。
6 月 26 日	FASTBOOKING	同社が管理するサーバにおいて、外部より不正アクセスを受け、利用者の氏名、国籍、住所、電話番号、メールアドレス等の個人情報やクレジットカード情報 32 万 5,717 件が流出した※150。
8 月 2 日	アサヒ軽金属工業 株式会社	同社が運営する Web ショッピングサイトにおいて、脆弱性を悪用した不正アクセスにより、利用者のクレジットカード情報最大 7 万 7,198 件が流出した可能性がある※151。
11 月 26 日	株式会社リガク	同社が運営する会員サイトに対して複数回の不正アクセスがあり、メールアドレスやパスワード、氏名、電話番号等の会員情報、延べ最大 9,885 件が流出した可能性がある※152。
12 月 25 日	ディー・エル・マーケット 株式会社	同社が運営する「DLmarket」において、不正アクセスにより、偽の決済フォームに誘導されるよう改ざんされ、利用者のクレジットカード情報最大 7,741 件が流出した可能性がある※115。

■表 1-2-5　外部からの攻撃による情報漏えいの主な事例（報道または公表事例を基に IPA が作成）



■図 1-2-29　漏えい原因の比率（n=386）
（出典）JNSA 調査報告書を基に IPA が作成

兵庫県立図書館の事例※153では、同館の利用者に向けたお知らせメールの誤送信により、メール受信者が延べ 3,294 名分のメールアドレスを閲覧できる状態となった。

株式会社ユー花園の事例※154では、同社が運営する通信販売サービス「スワンフローリスト」において、案内メールの誤送信により、メール受信者が 3,100 件のメールアドレスを閲覧できる状態となっていた。なお、そのうち 1,412 件は未達であったという。

いずれの事例も、本来 BCC に入力すべきメールアドレスを、誤って TO に入力して送信したものである。このような誤送信以外に、作業の不備等の過失による漏えい事案もある。

株式会社ポニーキャニオンの事例※155では、同社が運営する「ポニーキャニオンショッピングクラブ」において、顧客データの管理システムプログラムの障害により、購入手続き後の画面で他の会員の個人情報が誤表示されていた。これにより、氏名、住所、電話番号等、最大 27 名の個人情報が第三者に閲覧された可能性がある。

山形市役所の事例※156では、同市にふるさと納税を行い「寄附者からのメッセージ」を入力した寄附者の氏名、住所、電話番号等の個人情報を、1 週間にわたって Web サイト上に誤掲載していた。

米国の Exactis LLC の事例※157では、同社が保有する 2 億 3,000 万人分の個人情報と 1 億 1,000 万社の企業情報、合わせて 3 億 4,000 万件のデータを、誤って公開サーバ上に置いたことで誰でも閲覧できる状態になっていたという。

(3) 内部者の不正による情報漏えい

前述の JNSA 調査報告書によると、インシデント原因は「内部犯罪・内部不正行為」が 2.1% と、内部者の不正による情報漏えいは少ないと言える。しかしながら、業務上の必要性等によるルールを逸脱した「不正な情報持ち出し」は 6.5% となっている。これはルールの不徹底や運用における不備等で機密情報を容易に外部に持ち出せてしまう環境が主因と考えられ、このような環境は「内部犯罪・内部不正行為」につながる恐れもあるため注意が必要である。

株式会社セキ薬品の事例※158では、アルバイト従業員が勤務中に利用客のクレジットカード情報を盗み取り、その情報を用いてインターネット通販で不正購入をしていたことが分かった。内部調査において、当該アルバイト従業員が対応した利用客のクレジットカード情報、最大 234 件が盗み取られていた可能性がある。

東京女子医科大学東医療センターの事例※159では、退職した医師が在籍当時、担当していた患者の個人情

報を不正に持ち出していたことが分かった。

(4) 対策

それぞれの原因について、情報漏えい被害を発生させないための対策を以下に示す。

(a) 外部からの攻撃への対策

不正アクセス被害は、個人情報等の秘密情報を管理しているシステムの脆弱性や、当該情報にアクセスできるアカウントの不備が原因であるケースが多い。そのため、システムに脆弱性が存在したままの状態での運用とならないよう、利用しているソフトウェアの適切なアップデート等を心がけたい（「1.2.4 ソフトウェアの脆弱性を悪用した攻撃」参照）。また、アカウントについては、適切なアクセス権の設定やパスワードの管理を実施することはもちろん、アカウント所有者がフィッシング等により情報を詐取されないように適宜注意を促すことも重要である（「1.2.7 フィッシングによる詐欺」参照）。

(b) 人為的な過失への対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。過去の事例に基づく教育等で担当者の意識向上を図ることも有効であるが、それだけでなく、重要な情報の取り扱いルールを設け、その運用を徹底する、適宜見直す等で、過失の発生をできる限り抑止していく体制づくりが望まれる。

(c) 内部者の不正への対策

過失への対策と同様、内部不正による情報漏えい被害を完全に防ぐことは難しいが、情報を取り扱う者に対して正しい知識や規則を理解、遵守してもらう取り組みが不可欠である。その上で、監視カメラの設置や退職者のアカウント管理の徹底、通信や操作ログの監視及び保全、部署や役職に応じたアクセス権限の設定（最小権限化）等、不正を実行しにくい環境を整えることも望まれる。

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※160」や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※161」に記載されている対策も参考にされたい。

(d) 自組織以外での情報漏えい被害を想定した対策

情報漏えい被害は自組織だけでなく、委託先業者において発生することもある。個人情報等の秘密情報の管理や処理を委託する場合は、委託先が当該情報を適切に管理できる体制を整えているかの事前確認や、管理状況の報告や監査等で適宜チェックすることも重要となる（サプライチェーンについては「3.4 IT サプライチェーンのセキュリティ」参照）。

(e) その他の対策

これまでに挙げた対策以外に、情報漏えい発生時の被害や影響をできるだけ小さくする対策も重要である。例えば、取り扱う情報の機密レベルや必要性に応じて管理するデータベース（情報を保存するサーバ）を分離する、特段の必要性がなければクレジットカードやマイナンバー等の情報は取得、保有しないサービス仕様を検討する、利用者のパスワード情報はランダムな値を付加してハッシュ化した値（ソルト付きハッシュ値）として管理する、等の対策の検討、実施が望まれる。また、通信や操作ログの監視、保全は内部者の不正への対策となるだけでなく、情報漏えいが発生したときに、具体的にどの情報がどれだけ漏えいしたのかを把握することができ、適切な処置や迅速な情報公開による早期の事態収束に役立てることもできる。

COLUMN

サイバーセキュリティ専門家に求められる倫理観

2017年初冬、セキュリティサービスを提供している企業の社員がいわゆる「ウイルス保管罪」で逮捕された事件によりセキュリティ業界に衝撃が走りました。結果的には、2018年3月に不起訴処分の決定が下されましたが、逮捕された時点で社会的な制裁が下されてしまうことも多いことから、サイバーセキュリティ専門家の間では、今後のセキュリティサービスや製品の研究開発や提供、ひいてはサイバーセキュリティ専門家を志す人への影響が懸念されています。

サイバーセキュリティを生業とする限り、必然的に企業や組織の機密情報に触れる機会も多く、ウイルスや、各種脆弱性情報、攻撃情報等を収集・解析・保管することが必要になることから、サイバーセキュリティ専門家には高い倫理観と専門性を持つことが期待されています。しかしながら、サイバーセキュリティ専門家が戦っている相手は「悪意を持った」組織や人物であり、そのような相手と渡り合っていくためには、それなりの武器（情報や技術・ツール）が必要であることも事実です。一方的に守るだけでは到底防ぎきることはできず、常に新しい情報、技術を追い求める姿勢も必要で、そこにはそれなりにリスクがあることを認識した上で、新しいチャレンジを続けることが大切です。そこで、サイバーセキュリティ専門家が委縮することなく、そのようなチャレンジを続けていくために何が必要かについての議論が各所で始まっています。

学術分野では、サイバーセキュリティ研究における倫理的な研究プロセスの確立と普及を目的として、日本学術振興会（JSPS）のサイバーセキュリティ第192委員会に「サイバーセキュリティの研究倫理を考えるWG」が設置されています[i]。そこでは、サイバーセキュリティ研究を進める上で、研究手法自体が攻撃とみなされたり、結果として攻撃者を利することにならないよう、研究を進める際に事前の確認手順や倫理的な課題を整理し、研究者に普及しようとする取り組みがされています。

セキュリティ業界では、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（JNSA）の社会活動部会に「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会[ii]」が設置されています。そこでは、サイバーセキュリティ事業者が自らの責任において専門性と倫理観を兼ね備えた適切な事業運営を行うべきという考えのもと、サイバーセキュリティ事業者としての行動規範や、基本指針をまとめるとともに、各省庁、法執行機関等と円滑なコミュニケーションを図ることで、サイバーセキュリティ事業者の信頼性を向上させたり、法律運用上の課題について提言を行う取り組みを始めています。

サイバーセキュリティ専門家が高い倫理観と専門性を維持しつつ、安心して活動を行うことができるよう、これらの取り組みの今後に注目する必要がありそうです。

i　一般社団法人情報処理学会コンピュータセキュリティ研究会 MWS 組織委員会：サイバーセキュリティ研究における倫理的な研究プロセスについて　http://www.iwsec.org/mws/ethics.html〔参照 2019-06-18〕
ii　https://www.jnsa.org/active/2018/act.html#csrc〔参照 2019-06-18〕

1.3 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。

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

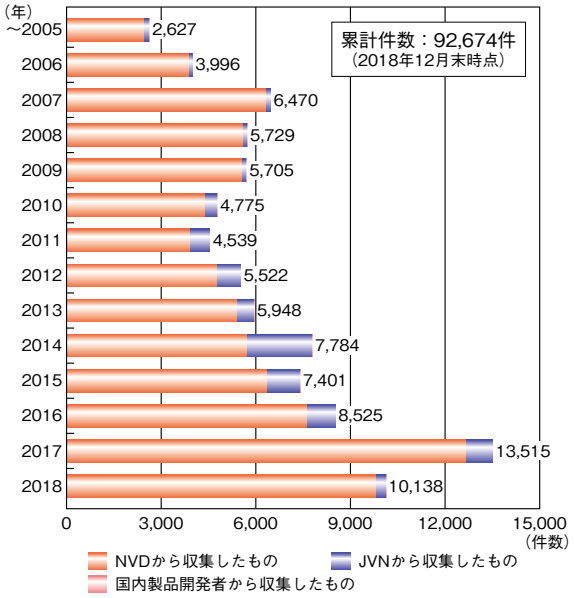
IPAは、脆弱性対策情報データベース「JVN iPedia※162」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2018年12月までに登録されたJVN iPediaの脆弱性対策情報の傾向を分析する。

(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※163」で公開された脆弱性対策情報

JVN iPediaに登録している情報を、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年別※164にまとめると、2011年を境にして増加傾向となっている。また2017年以降は、NVDから公開される脆弱性対策情報の件数が2016年以前より増加したため、JVN iPediaの登録件数が1万件以上となっている（図1-3-1）。NVDの公開件数が増加した理由としては、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）※165の採番機関（CVE Numbering Authority：CNA）※166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※167だったCNAは、2018年12月には93社※168と約2倍になっている。増加したCNA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。



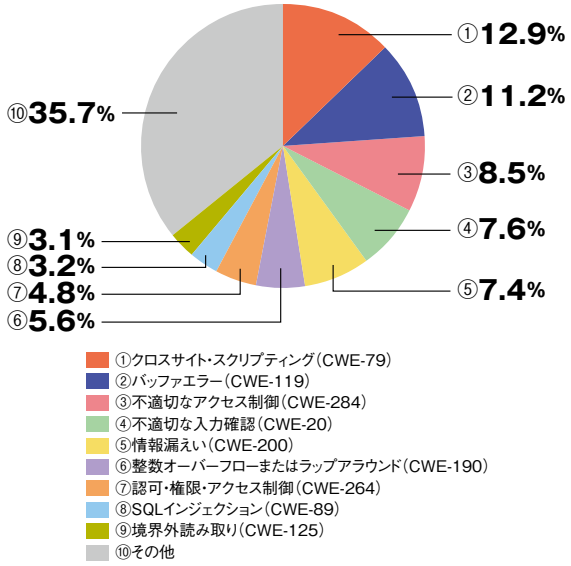
■図1-3-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

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）※169で分類すると、2018年は、「クロスサイト・スクリプティング」が最多の12.9%、「バッファエラー」が11.2%、「不適切なアクセス制御」が8.5%、「不適切な入力確認」が7.6%と続いている（次ページ図1-3-2）。

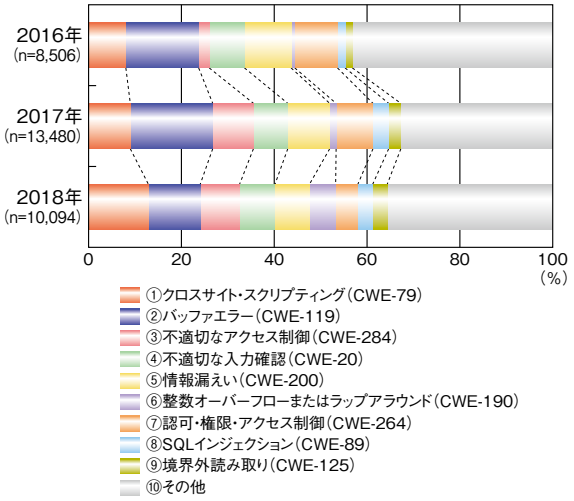
最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebページが表示されたり、情報が漏えいしたりする可能性がある。

2016年から2018年にかけての脆弱性タイプ別割合の変化を見ると、「クロスサイト・スクリプティング」「整数オーバーフローまたはラップアラウンド」の割合が増加している一方、「バッファエラー」「認可・権限・アクセス制御」の割合は、2018年には減少している（次ページ図1-3-3）。また、それ以外のCWE別の割合については、前年と同程度となっている。

JVN iPediaでは、オープンで汎用的な脆弱性評価手法である共通脆弱性評価システム（Common Vulnerability Scoring System：CVSS）※170を用いて、脆弱性の深刻度を公開している。なお、JVN iPediaではCVSS v2及びCVSS v3の二つのバージョンの情報



■図 1-3-2　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(2018 年、n=10,094)
(出典)JVN iPedia の登録情報を基に IPA が作成



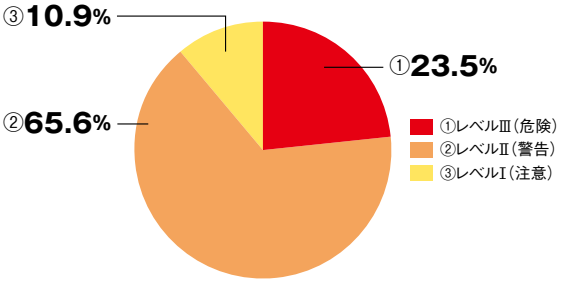
■図 1-3-3　JVN iPedia におけるソフトウェア製品の脆弱性対策情報の問題種別割合(2016 年～ 2018 年)
(出典)JVN iPedia の登録情報を基に IPA が作成

を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

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。

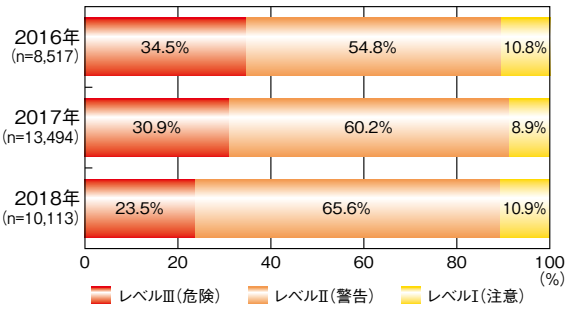
- 深刻度 レベルIII(危険)BM 7.0 ～ 10.0
  リモートからシステムを完全に制御されるような場合や大部分の情報が漏えいするような脅威等。
- 深刻度 レベルII(警告)BM 4.0 ～ 6.9
  一部の情報が漏えいするような場合やサービス停止につながるような脅威等。
- 深刻度 レベルI(注意)BM 0.0 ～ 3.9
  攻撃するために複雑な条件を必要とする脅威等。

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、2018 年はレベルIIIが 23.5%、レベルIIが 65.6%、レベルIが 10.9% となっている(図 1-3-4)。



■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル割合(2018 年、n=10,113)
(出典)JVN iPedia の登録情報を基に IPA が作成

更に、2016 年以降の CVSS v2 の深刻度のレベルの割合を年別に見ると、2018 年ではレベルIIとレベルIIIで全体の 89.1%であり、サービス停止につながるレベルII以上の脆弱性が多数を占めている(図 1-3-5)。最も危険なレベルIIIに該当する脆弱性は、2018 年では 23.5%と減少した。これは、レベルIIと評価されることが多い「クロスサイト・スクリプティング」や「整数オーバーフローまたはラップアラウンド」に分類される脆弱性が増加したことが要因として考えられる。



■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル割合(2016 ～ 2018 年)
(出典)JVN iPedia の登録情報を基に IPA が作成

件数で見ると、レベルIIIに該当する脆弱性は、2016 年は 2,937 件、2017 年は大きく伸びて 4,167 件、2018 年は 2,382 件と、3 年連続して 2,000 件以上の登録が確認されている。製品開発者には、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※171 を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が求められる。

(2) Drupal の脆弱性対策情報について

2018 年はオープンソースの CMS である Drupal の脆弱性が多数公表され、また、それらを狙った攻撃が度々観測されている。

2018 年 3 月 28 日に公表された Drupal の脆弱性（CVE-2018-7600）は、悪用されるとリモートで任意のコードを実行される可能性があり、影響の大きさから「Drupalgeddon 2.0」と名付けられた。4 月 12 日に攻撃コードが公開されると、直後の数日間で数万件単位の脆弱性を狙ったと見られるアクセスが国内で観測され、外部から不正プログラムのダウンロード及び実行を試みる攻撃が確認された※172。

また、これと関連する別の Drupal の脆弱性（CVE-2018-7602）が同年 4 月 25 日に公表された。この脆弱性を悪用し、サーバをボット化して仮想通貨の採掘を行わせる攻撃が 5 月中旬ごろから観測された※173。

その一方で、それぞれの脆弱性の公表と同時に、Drupal の開発チームはサポートが終了したバージョンも含めて、当該脆弱性を修正するセキュリティアップデートをリリースし※174、IPA でもそれぞれの脆弱性が公表された翌日に注意喚起情報※175 と緊急対策情報※176 を発信した。

JVN iPedia では、2018 年の 1 月から 12 月までに Drupal に関する脆弱性対策情報を 11 件登録した。そのうち、前述の CVE-2018-7600 及び CVE-2018-7602 を含む 3 件が CVSS v2 で最も深刻度が高いレベルⅢ（危険）となっており、また、7 件がレベルⅡ（警告）に分類されている（図 1-3-6）。深刻度が高いレベルⅢとレベルⅡの脆弱性が 9 割を占めており、脆弱性を悪用された場合、サーバの遠隔操作や情報の窃取等、深刻な影響を受ける可能性がある。

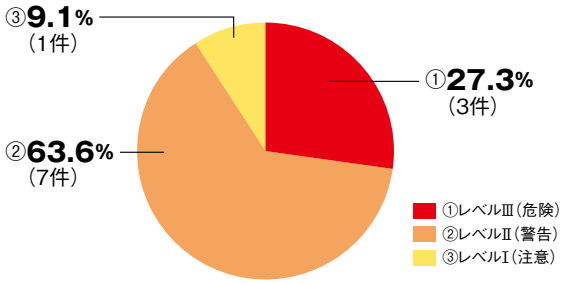
近年、Drupal のように広く利用されるソフトウェアの脆弱性が公表された場合、数日後には攻撃コードが公開され、攻撃が活発化する傾向にある。そのため、システム管理者は、日頃から自組織が利用する製品やシステムに影響する脆弱性情報を開発ベンダやセキュリティベンダから収集し、修正プログラムが公開された場合は、システム等の影響範囲を確認した上で、速やかに対策を行うことが望ましい。

(3) Java SE 8 の商用ユーザ向け無償サポート終了に伴う脆弱性対策について

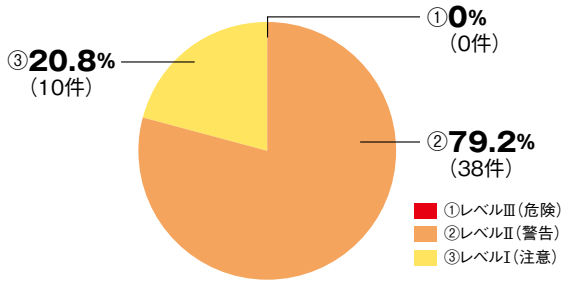
Oracle Corporation が提供する「Java Platform, Standard Edition 8（Java SE 8）」の商用ユーザ向けの無償アップデート・リリースが、2019 年 1 月をもって終了した※177。2 月以降、サポートを受けられない状態で Java SE 8 を利用し続けた場合、新たな脆弱性が発見されても修正プログラムが開発元から提供されないため、脆弱性を悪用した攻撃による情報漏えいや意図しないサービス停止等の被害を受けるリスクが高まる。Java SE は多くの組織で利用されており、被害が発生した場合の影響が大きいことから、IPA では 2018 年 11 月に注意喚起情報を発信した※178。

2018 年の 1 月から 12 月までに JVN iPedia へ登録された Java SE 8 の脆弱性対策情報を深刻度のレベルで分類すると、レベルⅢ（危険）の脆弱性は登録されていないが、レベルⅡ（警告）が 48 件中 38 件と全体の 8 割近くを占めている（図 1-3-7）。2017 年以前にはレベルⅢの脆弱性も複数公表されており、今後もレベルⅡ以上の脆弱性が公表される可能性があるため、Java SE 8 を継続利用する場合は有償サポート契約を結ぶ等の対応が必要となる。

また、同社からは、Java SE 11 以降の公式アップデートの提供方法の変更も公表されている。これまで 2 年に 1 度を目標に提供されてきた新機能追加によるメジャー・リリースが、フィーチャー・リリースと名称を変え 6 ヵ月に 1 度（毎年 3 月、9 月）提供されるようになった。また、新機能追加によるフィーチャー・リリースが提供された時点



■図 1-3-6　JVN iPedia に登録された Drupal の脆弱性対策情報のレベル割合（2018 年、n=11）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-3-7　JVN iPedia に登録された Java SE 8 の脆弱性対策情報のレベル割合（2018 年、n=48）
（出典）JVN iPedia の登録情報を基に IPA が作成

で、古いフィーチャー・リリースに対する脆弱性の対策等を含むアップデート・リリースはサポートが終了となる※179。そのため、無償サポートの対象となるバージョンへの移行を行う場合も、新しい提供方法に則した運用計画を検討する必要がある。

(4) 今後の展望

JVN iPedia へ登録した脆弱性対策情報の件数は、2018 年 12 月の時点で 9 万 2,000 件を超え、2019 年には 10 万件を超えると見込まれる。

また、2018 年は仮想通貨交換等に使われている分散アプリケーションプラットフォーム Ethereum※180 が提供するトークン規格のうち、ERC20※181 に準拠した複数のトークンにおいて脆弱性が発見され、JVN iPedia にも多数登録された※182。これらは、仮想通貨が 2017 年に広く世間に認知され、その後、更に市場が成長、活性化し、急激に普及した中で発見された脆弱性である。また、IoT 機器に関しても、その普及が進んでいく中で脆弱性が発見されている。

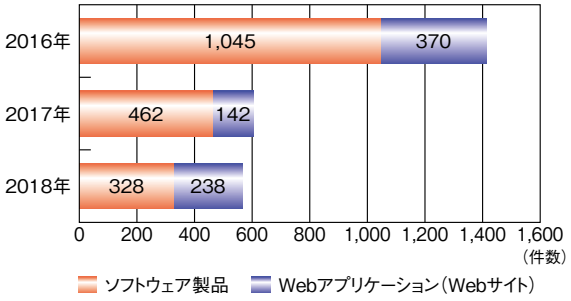
このように、技術やサービスが世の中に急激に普及していく段階で、それに関わる脆弱性が発見されることもある。例えば、最近では AI やキャッシュレス、e スポーツ、5G といった技術やサービスが注目されているが、今後これらの急激な普及に伴い脆弱性が発見されていくことが考えられる。普及が進む技術やサービスの開発者や利用者は、新たな脆弱性が発見される可能性についても十分注意を払う必要がある。

2018 年 8 月には、広く普及しているソフトウェアに発見された脆弱性について、対策がなされていない Web サイトのリストが短期間でダークウェブ等に流通し、大規模な攻撃キャンペーンの標的にされた事案も確認されている※183。このように、脆弱性を悪用した攻撃が組織的かつ迅速に行われている情勢を踏まえ、利用者は日頃からニュースやベンダの情報、JVN iPedia 等から情報収集を行い、速やかな脆弱性対策の実施に備えることが望まれる。

1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向

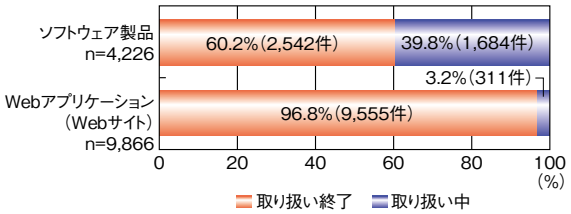
2018 年においてもソフトウェア製品や Web アプリケーションの脆弱性を悪用した攻撃による情報漏えい、及び Web サイトの改ざん等の被害が継続して発生している。情報漏えいに関する 2018 年の被害報告事例として、Web アプリケーションの脆弱性（SQL インジェクション）を悪用され続けた結果、最終的に個人情報が数十万件漏えいしたとする被害の報告があった※184。

2018 年に「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※185 の件数は、ソフトウェア製品が 328 件、Web サイトが 238 件、合計 566 件であった。2017 年の届出件数（604 件）と比較すると、約 6% 減少している。なお、それぞれの件数を 2017 年の届出件数（ソフトウェア製品：462 件、Web サイト：142 件）と比較すると、ソフトウェア製品に対する届出は約 29% 減少、Web サイトに対する届出は約 68% 増加した（図 1-3-8）。



■図 1-3-8　脆弱性関連情報の種類別届出状況（2016 ～ 2018 年）
（出典）パートナーシップの届出状況を基に IPA が作成

パートナーシップの開始（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 4,226 件、Web サイトは 9,866 件となり、2018 年 12 月末時点までの合計が 1 万 4,092 件に上る。これらの届出のうち IPA での取り扱いが終了※186 した届出件数は、ソフトウェア製品 2,542 件（60%）、Web サイト 9,555 件（97%）という状況である（図 1-3-9）。



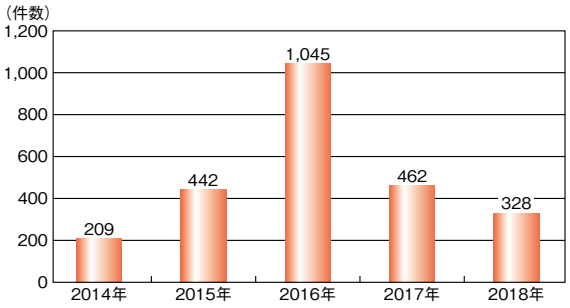
■図 1-3-9　脆弱性関連情報の種類別取扱終了状況（2018 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

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状況となっている。これを改善するため、ソフトウェア製品の脆弱性対策促進のための方法や、製品開発者と連絡が取れない届出への対応方法についてパートナーシップにおける制度及び運用の見直しが、「情報システム等の脆弱性情報の取扱いに関する研究会」

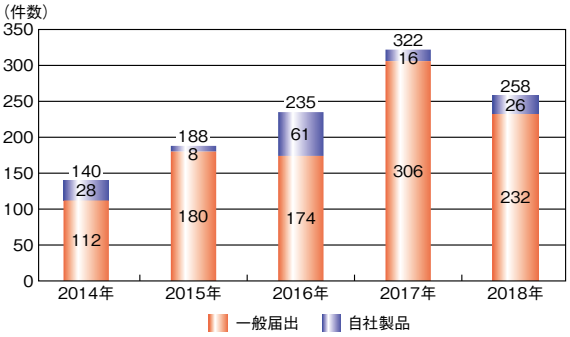
により行われている。

(1)ソフトウェア製品の脆弱性

2018 年の届出件数は、328 件（図 1-3-10）となり、2017 年と比較して約 3 割減少した。また、パートナーシップで取り扱った届出のうち、2018 年に JVN で公表された件数（図 1-3-11）は 258 件であった。なお、2018 年に製品開発者自身が、自社製品に関する脆弱性関連情報を届出し、JVN 公表に至った件数（図 1-3-11）は 26 件であり、2017 年の 16 件を上回った。



■図 1-3-10　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



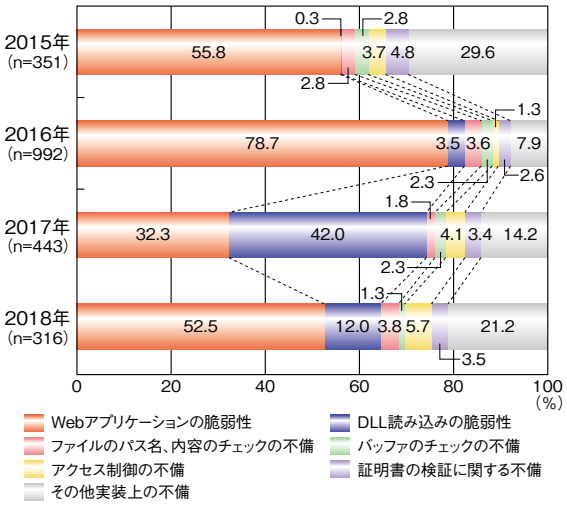
■図 1-3-11　ソフトウェア製品の脆弱性について JVN 公表された届出件数の推移
（出典）パートナーシップの届出状況を基に IPA が作成

(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 1-3-12 は、過去 4 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。2017 年には「DLL 読み込みの脆弱性」が急増したが、2018 年は全体の 12.0%となり、落ち着きを見せた。しかし、2016 年以前（2016 年 3.5%、2015 年 0.3%）と比較すると、まだ割合は高い。利用しているソフトウェア製品が「DLL 読み込みの脆弱性」について対策済みであるかを製品利用者が確認するのは、現実には困難である。製品利用者は自衛のため、以下のいずれかの対策を実施いただきたい[※187]。

- アプリケーションをダウンロードする場合には、ダウンロードフォルダに保存しない。新規にフォルダを作成し、そのフォルダに保存する。
- アプリケーションを実行する場合には、フォルダ内に不審ファイルがないかを確認する。

上記の対策は、あくまで暫定対策であるため、根本的な対策としては脆弱性が解消されたバージョンへアップデートすることが必要となる。



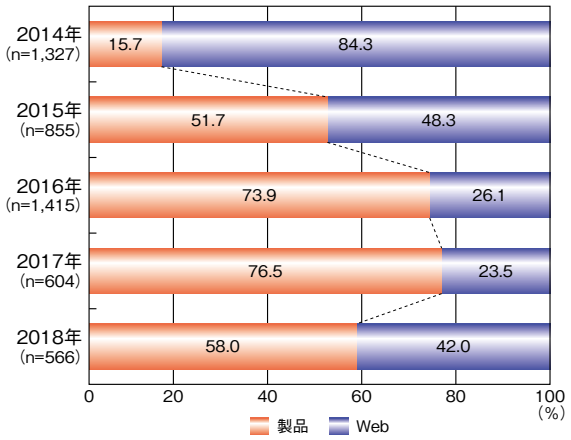
■図 1-3-12　脆弱性の種類別にみた届出の割合
（出典）パートナーシップの届出状況を基に IPA が作成

また、2015 年以降、Web サイトに関する届出と比べ、ソフトウェア製品の届出が占める割合が急激に増えており、2018 年も引き続き、届出全体の半数を超えている（次ページ図 1-3-13）。そのうち、自社製品に関する脆弱性関連情報の届出を積極的に行っている製品開発者は、過去 5 年間では平均 8 社となっている。2018 年に JVN 公表された届出のうち、自社届出では深刻度の高いレベルⅢ（危険）が 26.9%であり、一般届出に比べ高い割合を占めている（次ページ図 1-3-14）。

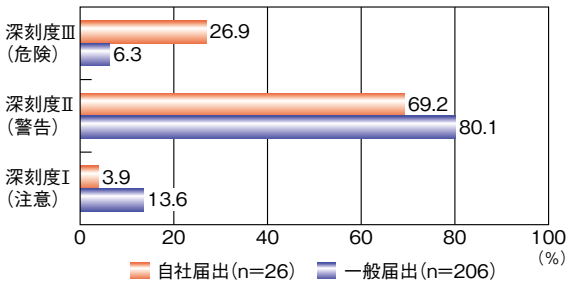
パートナーシップは善意の発見者による届出と、製品開発者の自主的な取り組みで成り立っている。更に多くの企業が自主的な取り組みにより、積極的に自社製品の脆弱性関連情報を公表することが望まれる。このため、例えば JPCERT/CC は、積極的に自社製品の脆弱性関連情報を開示し、利用者のサイバー攻撃被害の抑止や、IT 利用の安全性確保への協力に対し、2018 年に株式会社アイ・オー・データ機器へ感謝状を贈呈している。また過去には 2015 年にサイボウズ株式会社へ同様の感謝状を贈呈している[※188]。

更に、JPCERT/CC では、2018 年 12 月に、JVN を

リニューアルし、「『JPCERT/CC 製品開発者リスト』登録ベンダ一覧」に「脆弱性情報受付窓口」欄を設けた※189。これは、対外的な窓口を掲載することで、脆弱性の発見者と製品開発者とのコミュニケーションや連携を促進することを狙いとしている。脆弱性の発見者、及び、製品開発者は、積極的に活用していただきたい。



■図 1-3-13　脆弱性関連情報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



■図 1-3-14　2018 年に JVN 公表された届出のうち自社届出／一般届出ごとの深刻度の割合
(出典)パートナーシップの届出状況を基に IPA が作成

(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、当該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。2018 年に緊急対策情報として公表した情報は 16 件であった（表 1-3-1）。同 16 件のうち、PC クライアントソフトウェア製品の公表件数が 13 件(表 1-3-1 に●を示した情報) と約 8 割を占め、2018 年も継続した脅威となっている。自組織で使用しているクライアントソフトウェア製品を常に把握し、速やかにアップデートできる体制を整えておく必要がある。

公表日（2018 年）		タイトル
1 月 10 日	●	Microsoft 製品の脆弱性対策について（2018 年 01 月）
1 月 15 日		Oracle WebLogic Server の脆弱性（CVE-2017-10271）を悪用する攻撃事例について
2 月 2 日	●	Adobe Flash Player の脆弱性対策について（APSA18-01）（CVE-2018-4878）
2 月 7 日	●	更新：Adobe Flash Player の脆弱性対策について（APSA18-01）（APSB18-03）（CVE-2018-4878 等）
2 月 13 日		Cisco ASA の脆弱性対策について（CVE-2018-0101）
4 月 26 日		Drupal の脆弱性対策について（CVE-2018-7602）
5 月 9 日	●	Microsoft 製品の脆弱性対策について（2018 年 5 月）
5 月 16 日	●	更新：Adobe Acrobat および Reader の脆弱性対策について（APSB18-09）（CVE-2018-4990 等）
6 月 8 日	●	Adobe Flash Player の脆弱性対策について（APSB18-19）（CVE-2018-5002 等）
8 月 15 日	●	Microsoft 製品の脆弱性対策について（2018 年 8 月）
9 月 12 日	●	Microsoft 製品の脆弱性対策について（2018 年 9 月）
10 月 10 日	●	Microsoft 製品の脆弱性対策について（2018 年 10 月）
11 月 14 日	●	Microsoft 製品の脆弱性対策について（2018 年 11 月）
12 月 6 日	●	Adobe Flash Player の脆弱性対策について（APSB18-42）（CVE-2018-15982 等）
12 月 12 日	●	Microsoft 製品の脆弱性対策について（2018 年 12 月）
12 月 20 日	●	Microsoft Internet Explorer の脆弱性対策（CVE-2018-8653）について

■表 1-3-1　2018 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※190 を基に作成

(c)公式サポートが終了するソフトウェア製品

IPA は、2019 年 1 月に重要なセキュリティ情報として、Microsoft Corporation（以下、Microsoft 社）による公式サポートが 2020 年に終了する複数のソフトウェア製品（表 1-3-2）のバージョンアップを促す注意喚起を行った※191。

Microsoft 社によれば、大企業では Windows XP の教訓が生かされ、Windows 7 の計画的な移行が進

ソフトウェア製品	サポート期限
Windows 7	2020 年 01 月 14 日
Windows Server 2008	
Windows Server 2008R2	
Office 2010	2020 年 10 月 13 日

■表 1-3-2　公式サポートを終了予定の Microsoft 社製品とサポート期限

んでおり、移行に向けた活動を開始した大企業の割合は、2018 年 10 月時点で、95%に達しているという。一方、中小企業では、Windows 7 が 2020 年 1 月にサポートを終了することを認知していなかった企業が 43%と高い数値となっている※192。OS をバージョンアップする際の影響は多岐に渡り、以下のような確認・準備が必要となる。

- 現在使用しているパソコンや周辺機器が新 OS をサポートしているかどうかの確認
- 現行 OS 上で稼働しているソフトウェア製品が新 OS をサポートしているかの確認
- ブラウザやソフトウェア製品上で稼働するアプリケーション（自社開発した Web アプリケーション等）に影響があるかの確認
- 新 OS 利用に伴う企業内教育（ユーザインタフェースの変更点の周知等）の準備

また、上記以外にも、更新プログラム適用方式の決定や既存データ移行方法の決定等、様々な影響確認や対応が必要になる。更に、そのための予算確保も必要であることを考慮すると、Windows 7 の公式サポート終了まで既に 1 年を切り、時間的猶予はそれ程ない。中小企業における Windows 7 サポート終了の認知度を上げること、及び中小企業が早急に移行計画に着手することが望まれる。

Microsoft 社製以外のソフトウェア製品でも、PHP5.6、7.0 が 2018 年 12 月に既にサポートを終了し、Apache Struts 2.3 系が 2019 年 5 月に公式サポートの終了を予定している。これらはいずれも利用者が多いと推測される製品である。

OS だけでなく、企業内で使用しているソフトウェア製品を把握し、各ソフトウェア製品のサポート情報を収集し、いつサポート終了になるのかを認識した上で、計画的に移行準備を進めることが重要である。

(2) Web アプリケーション（Web サイト）の脆弱性

2018 年の Web サイトの脆弱性の状況をパートナーシップへの届出、セキュリティインシデントの実態から解説する。

(a) パートナーシップの届出から見た Web サイトの脆弱性の動向

2018 年は、パートナーシップの届出件数が 238 件となり、前年（141 件）と比較すると約 7 割増加している。

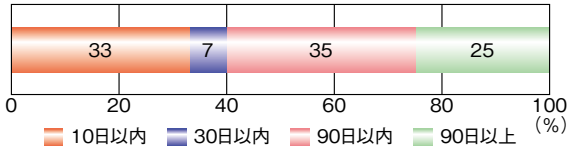
そのうち不受理（6 件）を除いた 232 件を脆弱性の種類別で見ると、「クロスサイト・スクリプティング」が例年どおり多くを占めるが、「SQL インジェクション」「ディレクトリ・トラバーサル」「ファイルの誤った公開」が前年と比べ大幅に増加している（表 1-3-3）。これらは、前年と同程度の届出件数であった「アクセスに関する不備」も合わせて、個人情報や、営業秘密等の機密情報が漏えいするといった、深刻な影響が考えられる脆弱性である。

脆弱性の種類	2017 年	2018 年
クロスサイト・スクリプティング	66	102
SQL インジェクション	18	46
ディレクトリ・トラバーサル	0	6
ファイルの誤った公開	5	20
アクセスに関する不備※	19	17
その他	24	41

※「認証に関する不備」「セッション管理の不備」「アクセス制限の回避」を含む

■表 1-3-3　パートナーシップの届出件数
（出典）パートナーシップの届出状況を基に IPA が作成

一方で、脆弱性情報を Web サイト運営者に通知してから修正されるまでに要した日数を見ると、10 日以内に修正されたケースは全体の 3 割強を、30 日以内では全体の 4 割を占める（図 1-3-15）。



■図 1-3-15　脆弱性情報を Web サイト運営者に通知してから修正されるまでに要した日数の割合（n=7,346）
（出典）パートナーシップの届出状況を基に IPA が作成

中には 1 日で修正されるケースもあり、数日で対策ができたものは、アクセス制限等のサーバやネットワーク設定に漏れがあった等、初歩的な対策が不十分であったものと推察される。

(b) Web サイトの脆弱性を突くセキュリティインシデントの実態

Web サイトの脆弱性を突いたと思われる攻撃により個人情報が漏えいする被害が公表されている。

JNSA が公開した 2017 年に個人情報が漏えいした人数が多いインシデントの上位 5 件の原因は不正アクセスとなっている（次ページ表 1-3-4）。ただし、インシデント原因別発生件数でみると、不正アクセスは 1 位ではなく 3 位である（次ページ表 1-3-5）。これらのことから不正アクセスは一度で大量の情報を取得できたり、また一度発

生すると被害が継続したりすることで、他の原因と比べて漏えいする情報の規模が大きくなっていると推察される。不正アクセスの要因となる脆弱性として、「SQL インジェクション」や「アクセスに関する不備」等が挙げられ、2018 年の被害事例も多数確認されている（「1.2.9 情報漏えいによる被害」参照）。

順位	漏えいした人数	業種	原因
1	118 万 8,355 人	製造業	不正アクセス
2	67 万 6,290 人	公務	不正アクセス
3	59 万 7,452 人	情報通信業	不正アクセス
4	37 万 1,200 人	情報通信業	不正アクセス
5	19 万 9,169 人	公務	不正アクセス

■表 1-3-4　2017 年に個人情報が漏えいしたインシデントの原因
（出典）JNSA「2017 年 情報セキュリティインシデントに関する調査報告書【速報版】」を基に IPA が編集

順位	漏えい原因	件数	割合
1	誤操作	97 件	25.1%
2	紛失・置き忘れ	84 件	21.8%
3	不正アクセス	67 件	17.4%
4	管理ミス	50 件	13.0%
5	不正な情報持ち出し	25 件	6.5%
6	盗難	25 件	6.5%
－	他	41 件	9.7%

■表 1-3-5　2017 年に個人情報が漏えいしたインシデントの原因別発生件数
（出典）JNSA「2017 年 情報セキュリティインシデントに関する調査報告書【速報版】」を基に IPA が編集

2018 年に公表された事例を紹介する。6 月 27 日に有限会社ひのでやエコライフ研究所※193 が、複数の地方自治体や公益財団法人から委託を受けて運営する省エネ関連サイトに対して不正アクセスが行われ、登録されている個人情報が漏えいした可能性があると発表した。このほかにも、12 月 4 日には株式会社あぐりーん※194 から同社が運営する農業系求人サイト「農家のおしごとナビ」への不正アクセスによる個人情報の漏えい、7 月 4 日には株式会社フレーバーライフ社※195 から同社が運営するサイトへの不正アクセスによる個人情報の漏えい、4 月 7 日には三菱地所・サイモン株式会社※196 が運営する「ショッパークラブ」への不正アクセスによる個人情報の漏えいの可能性について発表があった。

このように、業種や企業規模によらず Web サイトの脆弱性を突いたと思われるサイバー攻撃により個人情報が漏えいする被害が多数公表されている。

(c) Web サイトの脆弱性対策における課題

脆弱な Web サイトを狙った個人情報の窃取等のインシデントは企業の規模や業種によらず起きており、対岸の火事とは言えない状況である。一方で、個人情報の漏えいにつながる「SQL インジェクション」「セッション管理の不備」等の Web サイトの脆弱性が報告されており、サイバー攻撃に対して速やかに対策を取ることが求められる。Web サイト運営者及び Web サイト構築事業者は以下を参考にして、それぞれにできることから対策を検討いただきたい。

- Web サイト運営者に求められる対策

  自組織の Web サイトに関して、脆弱性がないか点検し、見つかった場合は適切な対策を取る必要があるが、様々な脆弱性に対する多様な対策がある中で、より完全で網羅的に対策を行うには相当の期間を要する。このため、自組織の体力とサイバー攻撃に対するリスクを考慮の上、優先順位を付けて、計画的に以下の対策を講じていただきたい。

  - 自組織のシステム環境の把握

    まず自組織のネットワークの構成やソフトウェア製品を把握し、バージョン及びサポート期間を管理する。新しいバージョンの公表を確認した場合や、サポート終了期間が迫っていることを確認した場合には最新のバージョンに切り替える等、計画的な対策が求められる。

  - 対処する脆弱性の優先順位の決定

    高いリスクが想定される脆弱性から対策を実施する必要がある。優先順位の決定には、「ウェブ健康診断仕様※197」の「2.1. 診断対象脆弱性（診断項目）及びその選定理由」に掲載された表が参考となる。危険度「高」かつ「能動的」攻撃かつ被害想定が「情報漏洩」である脆弱性（「SQL インジェクション」「OS コマンド・インジェクション」等）の高いリスクが想定される脆弱性を優先して対策を実施することが望ましい。

  - 脆弱性の対策方法の選定

    人的体制等で無理がなく、継続して実際に運用できる対策方法を選定する必要がある。

  - 脆弱性情報通知の受け入れ

    IPA※198 や、セキュリティに関心がある一般の方から自社 Web サイトに関する脆弱性について Web サイト運営者に通知されることがある。これらはセキュリティ上、重要な情報である可能性があるため、自社 Web サイトに関する脆弱性の報告を受け付け

る窓口を公開し、通知を受けた場合には誠実に対応するとともに、安全な Web サイト運営のために活用いただきたい。

このほかにも一般の Web サイトに関する脆弱性の報告を受け付けるサービス「OpenBugBounty[※199]」がある。当該サイトは海外の運営者により非営利で公開されている。これまでに 30 万件以上の報告を受け付けており、実際に日本の多くの Web サイトに関する脆弱性が公開されている。Web サイト運営者は自組織の Web サイトに関する脆弱性が当該サイトに公開されていないかを定期的に確認し、もし公開を確認した場合には速やかに対応いただきたい。

- Web サイト構築事業者に求められる対策

昨今、Web サイトを一般に公開する上で安全性を確保することは、Web サイト運営者に求められる責務であると考えられる。しかし Web サイト運営者に対し技術的なことを求めるのは一般に難しい。このため、Web サイトを構築する事業者に対しては、自ら安全な Web サイトを提案し Web サイト運営者の理解を得て構築することが求められる。例えば公開前には必ずセキュリティ診断としてペネトレーションテストの実施等を検討いただきたい。また、セキュリティ診断をしたにもかかわらず、後に脆弱性の存在が明らかになった場合には、診断の観点に不備がなかったか振り返り、組織的に改善を続けていただきたい。なお、セキュリティ診断を行う際には外部の情報セキュリティ専門企業[※200]等に依頼するほか、自ら行う場合には IPA が公開している「ウェブ健康診断仕様」等を参考にされたい。

(3) ソフトウェアが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) 組み込み機器の届出傾向

2018 年のソフトウェア製品の届出総数 328 件のうち、組み込み機器の届出は 78 件で、23.8%を占めている。年ごとの届出の推移を見ると、2014 年が 12.9%、2015 年が 15.2%、2016 年が 15.3%、2017 年が 13.9%、2018 年が 23.8% であり、2018 年は、直近 5 年で組み込み機器の届出の割合が最も多い年となった（表 1-3-6）。

2018 年に JVN 公表された組み込み機器の脆弱性は 21 件あり、届出者の割合は、セキュリティ企業が 72.7%、製品開発者自身が 4.5%、その他が 22.7% で、セキュリティ企業の割合が高い。これは、有償製品がほとんどと考えられる組み込み機器については、個人よりもセキュリティ企業の方が製品を用意しやすいためと推測される。

製品種別では、21 件中ルータは 14 件あり、定常的に届出され、公表もなされている組み込み機器の一つといえる。

年	ソフトウェア製品	組み込み機器	割合
2014	209	27	12.9%
2015	442	67	15.2%
2016	1045	160	15.3%
2017	462	64	13.9%
2018	328	78	23.8%

■表 1-3-6　ソフトウェア製品と組み込み機器の届出件数の推移
（出典）パートナーシップの届出状況を基に IPA が作成

(b) 深刻度が高い事例の紹介

2018 年に公表した深刻度が高い脆弱性として、製品開発者自身から届け出された、株式会社リコーの電子黒板「RICOH Interactive Whiteboard」における複数の脆弱性（JVN#55263945[※201]）がある。本件は遠隔の第三者によって、改ざんされたプログラムを実行されたり、データベース内の情報を取得あるいは改ざんされたりす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（CVSS については「1.3.1 (1) JVN iPedia への登録状況」参照）。対策として、ファームウェアのアップデートのほか、外部に直接接続しないネットワークでの運用や、管理者パスワードが初期状態であれば変更することが求められる。

(c) 組み込み機器の情報セキュリティ対策

近年、ホワイトボードのような製品にもソフトウェアが組み込まれ、インタラクティブホワイトボードとしてネットワークに接続する機能を持つ製品が登場している。これらの製品については、今までネットワークに接続されていなかったために、ネットワーク製品であるという意識を持ちにくい。利用者は、製品がネットワークに接続されていることを意識し、当該製品に脆弱性があれば、それを悪用され被害に遭うだけでなく、第三者へのサイバー攻撃の踏み台にされることで、被害者でありながら加害者にもなってしまう可能性もあることを理解する必要がある。

組み込み機器における具体的な対策としては、まずは製品開発者が充分なセキュリティ対策を施した上で製品を出荷することが求められるのは言うまでもない。また、

利用者は、製品利用時にネットワーク接続に関する適切なセキュリティ設定を行っていても、万全な対策とならない場合があることに注意されたい。例えば、通常、セキュリティ上の問題が発見されれば、製品開発者よりファームウェアのアップデートが提供されて問題を解消できる。しかし、利用している機器がサポート対象外である場合、アップデートが提供されない。このため、対策として同じ製品開発者からのサポートが受けられる機器や問題のない他の製品開発者の機器等への移行を検討する必要がある。利用している機器については、定期的な情報収集を心がけ、常に問題のない状態で利用することが重要である。

(4) 脆弱性情報の取り扱いに関する取り組み

脆弱性の発見や公表は、企業を含め様々な主体によって実施されるようになり、また、そのような取り組みを支援するような活動もなされるようになった。以下では、脆弱性情報の流通に関する動向、及び公的な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

2017年に引き続き、脆弱性情報の流通を促進する手法として、バグバウンティプログラムと呼ばれる、脆弱性の報告に対して報奨金を支払う取り組みが盛んになってきている。日本では、LINE株式会社※202やサイボウズ株式会社※203が実施していることで知られている。海外では、バグバウンティプログラムの運営をサービスとして提供している企業が存在しており、そのような企業の一つとしてBugcrowd Inc.がある。2017年度にBugcrowd Inc.において設置されたバグバウンティプログラムの数は、前年度比で40%増加しており※204、バグバウンティプログラムへの関心の高さを窺うことができる。

バグバウンティプログラムを実施しているのは、民間企業だけではない。米国国防総省（United States Department of Defense:DoD）は、2016年から「Hack the Pentagon」というバグバウンティプログラムを実施しているが、2018年には、一般公開されているWebサイト等を対象としていた当初の適用範囲を、国防目的の製品やシステムまで拡大することを発表している※205。また、英国の国家サイバーセキュリティ・センター（National Cyber Security Centre：NCSC）は、バグバウンティプログラムサービスを提供しているHackerOneのサービスを利用した、英国政府のWebサイト等の脆弱性の報告受付を2018年から実施している※206。シンガポール政府も、HackerOneをパートナーとしてバグバウンティプログラムを実施すると発表している※207。

(b) 脆弱性情報の流通に関する国際規格・ガイドラインの動向

2018年には、脆弱性開示に関する国際規格であるISO/IEC 29147※208の改訂がなされた。ISO/IEC 29147は、ベンダによる潜在的な脆弱性に関する報告の受領と脆弱性対策情報の公表についての指針を規定している。2014年版と比較して、いくつかの規定要素が追加されたほか、修辞上の修正等がなされている。

また、脆弱性の開示についてセキュリティ対策の一環として対応することとするフレームワーク・ガイドライン等も公表された。

2018年4月に公表された米国国立標準技術研究所（National Institute of Standards and Technology：NIST）の「Framework for Improving Critical Infrastructure Cybersecurity」の改訂版（Version 1.1）では、開示された脆弱性を取り扱うプロセスを策定することが、対策の一つとして掲げられている。

また、英国のデジタル・文化・メディア・スポーツ省（Department for Digital, Culture, Media and Sport：DCMS）は「消費者向けIoT製品のセキュリティに関する行動規範」を2018年10月に公表した※209。この行動規範は、IoTのセキュリティにおけるベストプラクティスをまとめ、13項目のガイドラインとしたもので、英語のほか、日本語訳※210も公表されている。その13項目の一つに「脆弱性に関する情報の公開方針を導入する」ことが設けられており、IoT製品の開発者等に、報告のための連絡窓口を設置し、開示された脆弱性を速やかに取り扱うよう推奨している。

このように、脆弱性情報の開示については、各国で対応を求められるようになってきている。日本においても、情報システム等のセキュリティを向上させる一手段として、各組織において脆弱性情報の開示に対応することが望まれる。

(c) 情報セキュリティ早期警戒パートナーシップの動向

「情報セキュリティ早期警戒パートナーシップ」とは、日本における、脆弱性情報の届出の受付及び流通を実施する公的な制度である。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※211」(以下、告示)と、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※212」(以下、ガイドライン)に則り運用されている。

パートナーシップでは、製品開発者やWebサイト運営者に脆弱性対策を依頼するだけでなく、取り扱う案件の特性に応じて、特殊な取り組みを実施している。例えば、重要インフラ事業者等に利用されているソフトウェア製品について、対策情報の公表の前に、重要インフラ事業者等に対して優先的に情報を提供する取り組み(優先情報提供)を実施している。他にも、製品開発者と連絡が取れない等の公表に向けた調整が難航する案件について、第三者委員会(公表判定委員会)の判定を経て公表する制度がある。

2018年には、これらの取り組みを利用した脆弱性情報の流通が実施された。

- 優先情報提供について

  重要インフラが国民の生活や経済を支える社会基盤であり、重要インフラのシステムに深刻な脆弱性が見つかった場合には、その問題を伝えリスク低減を促すことが求められる。そのため、パートナーシップでは、告示・ガイドラインが定める条件に従い、政府機関及び重要インフラ事業者等に対して、脆弱性対策情報をJVNでの公表の前に優先的に提供する取り組み(優先情報提供)を2018年4月から実施している。

  制度開始当初から、ガイドラインでは、政府機関や重要インフラ事業者等に対して、優先情報提供を可能とする条項の記載があったものの、サイバーセキュリティ基本法の制定等により重要インフラ保護の重要性が高まったことを受け、2014年以降優先情報提供の条件等の再整備について検討を行った。その結果、第一に電力分野について、次いで政府機関についての優先情報提供の手続きの準備が行われた。

  パートナーシップでは、これに基づき2018年第3四半期に電力分野1件、第4四半期に電力分野、政府機関ともに1件の優先情報提供を実施した※213。

- 公表判定委員会について

  パートナーシップでは、原則として、製品開発者の合意のもとで、脆弱性対策情報をJVNで公開している。そのため、届出の中には、製品開発者との連絡が取れない等の様々な理由により、公開に向けての製品開発者との調整が難航してしまうものが存在する。

  このような調整不能案件については、公表がされないため、利用者は脆弱性があることを認識できず、脆弱性のある製品の利用を継続することで、被害が生じる可能性が高まる。その一方で、対策がない状況で脆弱性情報を公開すると、製品開発者に不利益となる可能性や、攻撃者による悪用を誘発する可能性が発生する。このような脆弱性情報の公表に関わる様々な要素を考慮しつつ、製品利用者が被害を受ける可能性を可能な限り低減するため、IPAでは、調整不能案件の脆弱性情報について、公表が適当であるか否かを判定する第三者委員会である「公表判定委員会」を組織している。

  公表判定委員会は、法律やサイバーセキュリティの専門家等の専門的な知識経験を有する者が委員となり、告示・ガイドラインに定める手続きに則り、以下の4条件のすべてを満たす場合に公表することが適当であるとの判定を行う。

  - 調整機関と製品開発者との間の脆弱性情報の公表に係る調整が不可能であること
  - 脆弱性の存在が認められること
  - IPAが公表しない限り、脆弱性情報を知り得ない製品利用者がいる恐れがあること
  - 製品開発者や製品利用者の状況等を総合的に勘案して、公表が適当でないと判断する理由・事情がないこと

2018年には、公表判定委員会の判定を経て9件の脆弱性情報をJVNで公開した。

これらの様々な取り組みが活用されることで、効果的な脆弱性情報の流通が実現し、脆弱性の悪用による被害が軽減されることが期待される。

COLUMN

セキュリティ・バイ・デザインの勧め

内閣サイバーセキュリティセンター（NISC）によると「セキュリティ・バイ・デザイン」とは「情報セキュリティを企画・設計段階から確保するための方策」[i]（下図）であり、「安全な IoT システムのためのセキュリティに関する一般的枠組 [ii]」において、目的及び基本原則として掲げられている重要な概念です。IoT 時代を迎え、IoT システムへのセキュリティ上の脅威は社会生活に多大な被害を及ぼす可能性があります。安全な IoT システムの開発のためには、企画・要件定義工程や設計工程という、より早い段階から事前にセキュリティを作りこむことが求められています。またNIST SP800-160[iii]には、システムズエンジニアリングと対比したセキュリティ・エンジニアリングが提示されています。

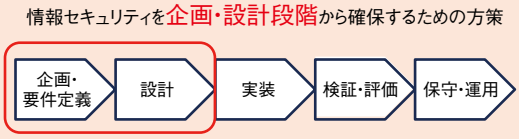


図　セキュリティ・バイ・デザインの定義

一方で、設計の段階で脆弱性の低減や脅威への対策を考慮にいれるセキュリティ設計の歴史が浅く、上流工程の開発プロセスが定まっていないことや、非機能要件のためコンセプトを決める企画段階で考慮がされづらい等の理由で、普及が難しいという課題も抱えています。

しかし、市場で運用されている段階で脆弱性が発見された場合のセキュリティ対策コストは、機器の交換やシステムの改修等が必要となるため、設計時に発見できた場合の 100 倍になるという試算もあり、セキュリティ・バイ・デザインによって開発者が得るメリットは大きなものがあります [iv]。他にも、企画・設計段階という開発の早い段階からセキュリティを考慮することで、手戻りを減らし納期を守れること、他の機能ができあがってから後付けでセキュリティ対応をするより、事前に対処したほうが保守性の良いソフトウェアができること等のメリットが挙げられます。安全な IoT システムの開発のために、ぜひセキュリティ・バイ・デザインについて考えてみてください。

i　NISC：「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」概要　https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf〔参照 2019-06-18〕
ii　https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf〔参照 2019-06-18〕
iii　NIST：Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems　https://csrc.nist.gov/publications/detail/sp/800-160/archive/2018-01-03〔参照 2019-06-18〕
iv　IPA：つながる世界のセーフティ&セキュリティ設計入門　https://www.ipa.go.jp/files/000055007.pdf〔参照 2019-06-18〕

※1 https://www.ibm.com/downloads/cas/ZGB3ERYD〔参照2019-06-18〕
※2 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〕
※3 Symantec 社：2019 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 2019-06-18〕
※4 https://enterprise.verizon.com/resources/reports/dbir/〔参照2019-06-25〕
※5 トレンドマイクロ社：2018 年年間セキュリティラウンドアップ 騙しの手口の多様化と急増するメールの脅威 https://resources.trendmicro.com/jp-docdownload-form-m113-web-2018-annualsecurityreport.html〔参照 2018-06-05〕
※6 APWG：Phishing Activity Trends Reports https://apwg.org/trendsreports/〔参照 2019-07-09〕
※7 BankInfoSecurity：FBI: Global Business Email Compromise Losses Hit $12.5 Billion https://www.bankinfosecurity.com/fbi-alert-reported-ceo-fraud-losses-hit-125-billion-a-11206〔参照 2019-06-18〕
Internet Crime Compliant Center（IC3）：BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM https://www.ic3.gov/media/2018/180712.aspx〔参照 2019-06-18〕
※8 CNET Japan：シンガポールの医療機関にサイバー攻撃、首相含む 150 万人の情報流出 -- 政府が対策など示す https://japan.cnet.com/article/35122835/〔参照 2019-06-18〕
Security NEXT：シンガポール医療機関の大規模情報漏洩、関与グループが判明 http://www.security-next.com/103337〔参照 2019-06-18〕
※9 「マルウェア」等の用語を混在して使用すると、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。
※10 朝日新聞デジタル：フェイスブック、5千万人情報流出の危険 昨年夏から https://www.asahi.com/articles/ASL9Y1DHTL9XUHBI044.html〔参照 2019-06-18〕
PC Watch：Facebook、5,000 万人分のアクセストークンが流出 https://pc.watch.impress.co.jp/docs/news/1145475.html〔参照2019-06-18〕
※11 Facebook, Inc.：Facebook の最新のセキュリティ問題に関する重要なアップデート https://www.facebook.com/help/securitynotice〔参照 2019-06-18〕
※12 Marriott International, Inc.：Marriott Announces Starwood Guest Reservation Database Security Incident https://marriott.gcs-web.com/news-releases/news-release-details/marriott-announces-starwood-guest-reservation-database-security〔参照2019-06-18〕
Marriott International, Inc.：Marriott Provides Update on Starwood Database Security Incident https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/〔参照 2019-06-18〕
※13 NRI セキュアテクノロジーズ株式会社：【事例】GDPR で制裁金が課せられたケースと求められるセキュリティ対策 https://www.secure-sketch.com/blog/case-of-gdpr-penalties〔参照 2019-06-18〕
※14 「SSDP ディフラクションの DoS 攻撃関連」「Netcore 製ルータの脆弱性を利用したバックドアアクセス関連」「通知プロトコル『ICMP』の DoS 攻撃『BlackNurse』関連」「Web サーバ『GoAhead』の脆弱性関連」「D-Link ルータの OS コマンドインジェクション関連」は、「その他」に合計した。
※15 クリプトジャッキングは、悪意あるコードが埋め込まれた Web ページにアクセスすることで利用者の知らないうちに仮想通貨のマイニングに資源が使われてしまうことと定義される場合もあるが、Symantec 社では、被害者のデバイスで仮想通貨マイニングプログラムを密かに実行し、CPU を使用して暗号通貨をマイニングする攻撃手法と定義している。
※16 CoinMarketCap OpCo, LLC：CoinMarketCap https://coinmarketcap.com/〔参照 2019-06-18〕
※17 http://www.mbsd.jp/casebook_index.html〔参照 2019-06-18〕
※18 https://www.jpcert.or.jp/ir/report.html〔参照 2019-06-18〕
※19 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 2019-06-18〕
※20 IPA：安心相談窓口だより 宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に https://www.ipa.go.jp/security/anshin/mgdayori20181129.html〔参照 2019-06-18〕
※20-1 トレンドマイクロ社：「アダルトサイト経由のハッキング」で脅す詐欺メール、12 日間で 250 万円を詐取か https://blog.trendmicro.co.jp/archives/19682〔参照 2019-06-18〕
※20-2IPA：安心相談窓口だより 偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中 https://www.ipa.go.jp/security/anshin/mgdayori20180718.html〔参照2019-06-18〕
※20-3学校法人甲南学園：【ご報告】2018 年 7 月の学内ネットワークにおけるマルウェア検出について http://www.konan-u.ac.jp/system/archives/1031〔参照 2019-06-18〕
※20-4日経メディカル：患者 1133 人分の電子カルテが閲覧不能に 奈良の宇陀市立病院がランサムウエアの被害に 身代金は支払わず https://medical.nikkeibp.co.jp/leaf/mem/pub/hotnews/int/201810/558453.html〔参照 2019-06-18〕
※21 朝日新聞：経団連を標的、中国人ハッカー集団 ウイルスは 2 年潜伏 https://www.asahi.com/articles/ASM196VTPM19ULZU01B.html〔参照 2019-05-22〕
※22 IPA：標的型サイバー攻撃の脅威と対策 https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔参照 2019-05-22〕
※23 ITmedia エンタープライズ：監視の裏をかく攻撃、ここまで――標的型攻撃、正規ツールを隠れみのにする傾向に http://www.itmedia.co.jp/enterprise/articles/1806/27/news093.html〔参照 2019-05-22〕
※24 McAfee, LLC：Updated BlackEnergy Trojan Grows More Powerful https://securingtomorrow.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/〔参照 2019-05-22〕
※25 https://blog.trendmicro.co.jp/archives/17280〔参照2019-05-22〕
※26 Dynamic Data Exchange：Windows 環境において、複数のソフトウェア間で通信を行う技術。
※27 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。
※28 NHK NEWS WEB：相手を信用させる前例なき手口 コインチェック攻撃で明らかに https://web.archive.org/web/20180517021140/https://www3.nhk.or.jp/news/html/20180512/k10011436321000.html〔参照 2019-05-22〕
コインチェック株式会社：仮想通貨 NEM の不正送金に関する質問 https://coincheck.com/ja/info/faq_nem〔参照 2019-06-18〕
※29 Piyolog：2018 年 1 月の文科省なりすましメールについてまとめてみた http://d.hatena.ne.jp/Kango/20180119/1516391079〔参照2019-05-22〕
JPCERT/CC：プラグインをダウンロードして実行するマルウエア TSCookie (2018-03-01) https://blogs.jpcert.or.jp/ja/2018/03/tscookie.html〔参照 2019-05-22〕
※30 https://www.sankei.com/world/news/180412/wor1804120001-n1.html〔参照 2019-05-22〕
※31 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 4 月～ 6 月］ https://www.ipa.go.jp/files/000068064.pdf〔参照2019-05-22〕
※32 マカフィー株式会社：ソーシャルエンジニアリングとは?手口・被害例・実践的な対策を知る https://blogs.mcafee.jp/what-is-social-engineering〔参照 2019-05-22〕
※33 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 2019-05-22〕
※34 ITmedia エンタープライズ：社長へのメールを秘書が開いてマルウェアに感染 !? 標的型攻撃の実践演習「サイバークエスト」を模擬体験 http://www.itmedia.co.jp/enterprise/articles/1901/07/news009.html〔参照 2019-05-22〕
※35 トレンドマイクロ社：インシデント対応ボードゲーム スタンダード版 https://resources.trendmicro.com/jp-docdownload-form-m057-web-incidentboardgamestandard.html〔参照 2019-05-22〕
※36 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 2019-05-22〕
※37 トレンドマイクロ株式会社：Tracking Trends in Business Email Compromise (BEC) Schemes https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf〔参照2019-05-22〕
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 2019-05-22〕
Secureworks：GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry〔参照 2019-05-22〕
※38 Internet Crime Complaint Center（IC3）：Business E-mail Compromise The 12 Billion Dollar Scam https://www.ic3.gov/

media/2018/180712.aspx〔参照 2019-05-22〕
※ 39 日本経済新聞：企業狙う振り込め詐欺 上司・取引先装い送金指示 被害約 60 社に 警視庁が捜査 https://www.nikkei.com/article/DGKKZO04776090S6A710C1CR8000/〔参照 2019-05-22〕
※ 40 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 2019-05-22〕
※ 41 トレンドマイクロ株式会社：「ビジネスメール詐欺に関する実態調査 2018」を発表 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html〔参照 2019-05-22〕
※ 42 警察庁：ビジネスメール詐欺に注意 https://www.npa.go.jp/cyber/bec/index.html〔参照 2019-05-22〕
※ 43 全国銀行協会：法人間の外国送金の資金をだまし取る詐欺にご注意! https://www.zenginkyo.or.jp/topic/detail/nid/3561/〔参照2019-05-22〕
※ 44 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。
IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ）） https://www.ipa.go.jp/security/J-CSIP/〔参照 2019-05-22〕
※ 45 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 2019-05-22〕
※ 46 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（続報） https://www.ipa.go.jp/security/announce/201808-bec.html〔参照 2019-05-22〕
※ 47 FBI：International Business E-Mail Compromise Takedown https://www.fbi.gov/news/stories/international-bec-takedown-061118〔参照 2019-05-22〕
※ 48 日本経済新聞：7 千万円送金させた疑い ビジネスメール詐欺で逮捕 https://www.nikkei.com/article/DGXMZO32602020U8A700C1CC1000/〔参照 2019-05-22〕
※ 49 デイリー新潮：「ドルチェ&ガッバーナ」が“3 億円ビジネスメール詐欺”被害 日本社長をクビ＆提訴 https://www.dailyshincho.jp/article/2018/08291658/〔参照 2019-05-22〕
※ 50 河北新報オンラインニュース：資金洗浄の疑いでナイジェリア人逮捕、仙台の銀行から9300万円払い戻し https://www.kahoku.co.jp/tohokunews/201809/20180914_13012.html〔参照 2019-05-22〕
※ 51 産経ニュース：「ビジネスメール詐欺」で犯罪収益引き出したナイジェリア人ら再逮捕 警視庁 https://www.sankei.com/affairs/news/181003/afr1810030018-n1.html〔参照 2019-05-22〕
※ 52 Linked Data Overheid：ECLI:NL:RBAMS:2018:7881 - Rechtbank Amsterdam, 31-10-2018 / 7018728 EA VERZ 18-544 https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:RBAMS:2018:7881〔参照 2019-05-22〕
E- Help Net Security：BEC scammers stole €19m from film company Pathé https://www.helpnetsecurity.com/2018/11/14/pathe-bec-scam/〔参照 2019-05-22〕
※ 53 産経ニュース：犯罪収益引き出したナイジェリア人ら逮捕、警視庁 https://www.sankei.com/affairs/news/181119/afr1811190012-n1.html〔参照 2019-05-22〕
※ 54 Agari Data, Inc.：Hostile Landscape of Email Threats Leverages California Wildfire Tragedy https://www.agari.com/email-security-blog/hostile-landscape-of-email-threats-leverages-california-wildfire-tragedy/〔参照 2019-05-22〕
※ 55 Agari Data, Inc.：London Blue https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf〔参照 2019-05-22〕
日本経済新聞：[FT] ハッカー集団 企業 CFO を詐欺メールの標的に https://www.nikkei.com/article/DGXMZO38558070V01C18A2000000/〔参照 2019-05-22〕
※ 56 Save the Children Federation, Inc.：2017 Form 990 https://www.savethechildren.org/content/dam/usa/reports/advocacy/stc-990-2017.pdf〔参照 2019-05-22〕
The Boston Globe：Hackers fooled Save the Children into sending $1 million to a phony account https://www.bostonglobe.com/business/2018/12/12/hackers-fooled-save-children-into-sending-million-phony-account/KPnRi8xIbPGuhGZaFmlhRP/story.html〔参照 2019-05-22〕
※ 57 EPC：Engineering, Procurement, Construction の略称。プラント建設等においてエンジニアリングの設計、資機材調達、製作、建設工事を含む一連の工程を請け負うことを指す。
※ 58 The Economic Times：How Chinese hackers pulled off the Italian con job, a Rs 130-crore heist https://economictimes.indiatimes.com/tech/internet/how-chinese-hackers-pulled-off-the-italian-con-job-a-rs-130-crore-heist/articleshow/67464588.cms〔参照 2019-05-22〕
※ 59 産経ニュース：元公設秘書の男逮捕 詐取金を不正引き出し容疑 https://www.sankei.com/smp/affairs/news/190214/afr1902140016-s1.html〔参照 2019-05-22〕
毎日新聞：元防衛相秘書を逮捕 詐欺容疑で警視庁 http://mainichi.jp/articles/20190214/k00/00m/040/108000c〔参照 2019-02-22〕
※ 60 日本経済新聞：ビジネスメール詐取金、不正引き出し疑い 日本人２人逮捕 https://www.nikkei.com/article/DGXMZO43069900Z20C19A3CC0000/〔参照 2019-05-22〕
朝日新聞デジタル：「ビジネスメール詐欺」容疑、2人逮捕 背後にナイジェリアの犯罪組織か https://www.asahi.com/articles/DA3S13954689.html〔参照 2019-05-22〕
※ 61 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] https://www.ipa.go.jp/files/000066063.pdf〔参照 2019-05-22〕
※ 62 日経 BP 社、メールの相手、本当は誰だ 手の内を知って対策を、日経コンピュータ 2018 年 12 月 20 日号、p.78
※ 63 トレンドマイクロ株式会社：日本語の使用が確認された「ビジネスメール詐欺」、その背景に迫る https://blog.trendmicro.co.jp/archives/19654〔参照 2019-05-22〕
※ 64 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 2019-05-22〕
※ 65 NCSC Site：The rise of Microsoft Office 365 compromise https://www.ncsc.gov.uk/alerts/rise-microsoft-office-365-compromise
※ 66 appriver：Office 365 Business Email Compromise Attacks Proliferate https://blog.appriver.com/2018/02/office-365-business-email-compromise-attacks-proliferate〔参照 2019-05-22〕
※ 67 株式会社スクウェア・エニックス：断続的に発生している DDoS 攻撃について https://jp.finalfantasyxiv.com/lodestone/news/detail/ac070d07a9b02577dec2feca92dddd57b82364e1〔参照2019-05-22〕
株式会社スクウェア・エニックス：[続報] 断続的に発生している DDoS 攻撃について https://jp.finalfantasyxiv.com/lodestone/news/detail/60713eb72c1afa8b2500135ed5c414cac33c2ca6〔参照 2019-05-22〕
※ 68 piyolog：艦隊これくしょんへの DoS 攻撃についてまとめみた https://piyolog.hatenadiary.jp/entry/20190112/1547244881〔参照 2019-05-22〕
※ 69 Krebs on Security：250 Webstresser Users to Face Legal Action https://krebsonsecurity.com/2019/02/250-webstresser-users-to-face-legal-action/〔参照 2019-05-22〕
※ 70 株式会社インターネットイニシアティブ：2018 年の IoT ボット観測状況と最近の動向 https://sect.iij.ad.jp/d/2019/01/288147.html〔参照 2019-05-22〕
INTERNET Watch：Mirai 亜種が国内の最大２万 4000 ホストに感染、ロジテック製 Wi-Fi ルーターの脆弱性を悪用 https://internet.watch.impress.co.jp/docs/news/1097777.html〔参照 2019-05-22〕
※ 71 NOTICE：https://notice.go.jp/〔参照 2019-05-22〕
※ 72 株式会社インターネットイニシアティブ：wizSafe Security Signal 2018 年９月 観測レポート https://wizsafe.iij.ad.jp/2018/10/470/〔参照 2019-05-22〕
※ 73 ZDNet Japan：「Windows」タスクスケジューラの脆弱性を悪用するマルウェア見つかる https://japan.zdnet.com/article/35125188/〔参照 2019-05-22〕
※ 74 Microsoft 社：2020 年 世代交代。Windows 7 Office 2010 サポート終了。 https://www.microsoft.com/ja-jp/business/windows/endofsupport.aspx〔参照 2019-05-22〕
IPA：複数の Microsoft 社製品のサポート終了に伴う注意喚起 https://www.ipa.go.jp/security/announce/win7_eos.html〔参照 2019-05-22〕
※ 75 IPA:Apache Struts2 の脆弱性対策について（CVE-2018-11776）（S2-057） https://www.ipa.go.jp/security/ciadr/vul/20180823-struts.html〔参照 2019-05-22〕
※ 76 ITmedia NEWS：「Apache Struts 2」の脆弱性、仮想通貨採掘攻撃に悪用される http://www.itmedia.co.jp/news/articles/1809/06/news066.html〔参照 2019-05-22〕
※ 77 Security NEXT：【セキュリティ ニュース】WordPress 向けの GDPR 対応プラグインに深刻な脆弱性 - 乗っ取りや改ざん被害が発生 http://www.security-next.com/100144〔参照 2019-05-22〕
※ 78 トレンドマイクロ社：「Drupal」の脆弱性「CVE-2018-7602」を利用した攻撃を確認、仮想通貨「Monero」発掘ツールを拡散 https://blog.trendmicro.co.jp/archives/19266〔参照 2019-05-22〕
※ 79 ITmedia エンタープライズ：Drupal の脆弱性を突く攻撃を確認、直

ちに対応を　http://www.itmedia.co.jp/enterprise/articles/1804/27/news075.html〔参照 2019-05-22〕
※ 80 ステージング環境：運用（本番）環境と同等のシステム構成（ハードウェア、ソフトウェアとも）のテスト環境のこと。修正プログラム等の適用前に、適用による問題発生の有無を検証する環境。仮想化されたサーバ、ストレージ上に構築されることもある。
※ 81 ITmedia エンタープライズ：IoT デバイスの脆弱性を突くマルウェア「Wicked」、Mirai の新手の亜種　http://www.itmedia.co.jp/enterprise/articles/1805/22/news064.html〔参照 2019-05-22〕
FORTINET：A Wicked Family of Bots　https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html〔参照 2019-05-22〕
※ 82 https://jvndb.jvn.jp/〔参照 2019-05-22〕
※ 83 IPA：メールニュース　https://www.ipa.go.jp/about/mail/index.html〔参照 2019-05-22〕
※ 84 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181129-01.html〔参照 2019-05-22〕
※ 85 JPCERT/CC：ランサムウエアの脅威動向および被害実態調査報告書 1.0 版　https://www.jpcert.or.jp/research/Ransom-survey.pdf〔参照 2019-05-22〕
※ 86 Daily Reporter：Hospital pays $55,000 ransom; no patient data stolen　http://www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/〔参照 2019-05-22〕
※ 87 SamSam: 600 万ドル近くの身代金を手にしたランサムウェア　https://www.sophos.com/ja-jp/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf〔参照 2019-05-22〕
※ 88 BleepingComputer：PUBG Ransomware Decrypts Your Files If You Play PlayerUnknown's Battlegrounds　https://www.bleepingcomputer.com/news/security/pubg-ransomware-decrypts-your-files-if-you-play-playerunknowns-battlegrounds/〔参照 2019-05-22〕
ScanNetSecurity：「PUBG」を 1 時間プレイすることが解除条件のランサムウェアを確認　https://scan.netsecurity.ne.jp/article/2018/04/12/40793.html〔参照 2019-05-22〕
※ 89 The Hacker News：New Virus Decides If Your Computer Good for Mining or Ransomware　https://thehackernews.com/2018/07/cryptocurrency-mining-ransomware.html〔参照 2019-05-22〕
GIGAZINE：ランサムウェアとマイニング両方の機能を持ち効率的な攻撃を選ぶウイルスが登場　https://gigazine.net/news/20180706-virus-desides-mining-or-ransomware/〔参照 2019-05-22〕
※ 90 IPA：IPA テクニカルウォッチ「ランサムウェアの脅威と対策」　https://www.ipa.go.jp/security/technicalwatch/20170123.html〔参照 2019-05-22〕
※ 91 https://www.nomoreransom.org/ja/index.html〔参照 2019-05-22〕
※ 92 アカマイ・テクノロジーズ合同会社：アカマイ、リスト型攻撃レポートを発表 金融サービス業界が絶え間なく自動アカウント乗っ取りツールの攻撃にさらされている現状を報告　https://www.akamai.com/jp/ja/about/news/press/2018-press/akamai-credential-stuffing-report-shows-financial-services-industry-under-constant-attack-from-automated-account-takeover-tools.jsp〔参照 2019-05-22〕
Security NEXT：不正ログインの試行件数が 5、6 月に上昇 - 1 カ月あたり40億件以上　http://www.security-next.com/099798〔参照 2019-05-22〕
※ 93 株式会社ドワンゴ：他社流出パスワードを用いた不正ログインについて (2018/05)　http://blog.nicovideo.jp/niconews/73053.html〔参照 2019-05-22〕
株式会社ドワンゴ：他社流出パスワードを用いた不正ログインについて (2018/07)　http://blog.nicovideo.jp/niconews/79797.html〔参照 2019-05-22〕
※ 94 株式会社ケイ・オプティコム：eoID に対する不正なログインについてのお知らせ（2018 年 8 月 21 日更新）　http://www.k-opti.com/announce/180815/〔参照 2019-05-22〕
※ 95 朝日新聞：不正購入のiPhoneX受け取った疑い　男4人を逮捕　https://www.asahi.com/articles/ASLCD2TNDLCDUTIL002.html〔参照 2019-05-22〕
※ 96 株式会社 NTT ドコモ：不正なアクセス対策としての「2 段階認証」ご利用のお願い　https://www.nttdocomo.co.jp/info/notice/page/180814_00_m.html〔参照 2019-05-22〕
※ 97 イオンマーケティング株式会社：「smartWAON ウェブサイト」における不正ログインについてお詫びと調査結果のお知らせ　http://www.aeonmarketing.co.jp/pdf/news_20180915.pdf〔参照 2019-05-22〕
※ 98 株式会社ローソン:ローソン ID 会員様へのアカウントメールアドレス・パスワード再設定のお願い　http://www.lawson.co.jp/info/20180910_mai.html〔参照 2019-05-22〕
※ 99 株式会社ローソン：「おさいふPonta」サイトへの不正アクセスについて　http://www.osaifuponta.lawson.co.jp/news/Detail?news_id=93〔参照 2019-05-22〕
※ 100 株式会社マーケティングアプリケーションズ：◆重要◆不正ログイン防止のための ID とパスワード定期更新のお願い　https://www.ann-kate.jp/〔参照 2019-02-08〕
※ 101 四国電力株式会社：よんでんコンシェルジュへの不正アクセスによるポイント交換について　https://www.yonden.co.jp/press/2018/__icsFiles/afieldfile/2018/12/27/pr006_5.pdf〔参照 2019-05-22〕
※ 102 株式会社アプラスフィナンシャル：アプラスカード会員様向けサイトに対する不正ログインとその対応について　https://news.aplusfinancial.co.jp/news/down2.php?attach_id=1262&seq=110007268&category=100&page=100&access_id=10007268〔参照 2019-05-22〕
※ 103 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 2019-05-22〕）
※ 104 株式会社ディノス・セシール：弊社「セシールオンラインショップ」への不正アクセスとお客様情報流出の可能性に関する調査結果のお知らせ　https://www.dinos-cecile.co.jp/whatsnew/20180706_topics.pdf〔参照 2019-05-22〕
※ 105 CNET Japan：22 億件超の流出アカウント情報、ダークウェブで一括公開　https://japan.cnet.com/article/35132120/〔参照 2019-05-22〕
※ 106 WAF（Web Application Firewall）：主に Web アプリケーションへの攻撃を防御するソフトウェアまたはハードウェア。
※ 107 トレンドマイクロ社：仮想通貨を狙うフィッシング詐欺、既に闇市場での「サービス化」も確認　https://blog.trendmicro.co.jp/archives/17128〔参照 2019-05-22〕
※ 108 フィッシング対策協議会：月次報告書　https://www.antiphishing.jp/report/monthly/〔参照 2019-05-22〕
※ 109 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 2019-05-22〕
※ 110 IPA：文書ファイルを悪用したフィッシング詐欺の手口に関する注意点　https://www.ipa.go.jp/files/000062173.pdf〔参照 2019-05-22〕
フィッシング対策協議会：Apple をかたるフィッシング (2018/04/25)　https://www.antiphishing.jp/news/alert/apple_20180425.html〔参照 2019-05-22〕
※ 111 日本経済新聞：文科省が Office365 の偽メールに注意喚起、6 大学で被害　https://www.nikkei.com/article/DGXMZO32489620S8A700C1000000/〔参照 2019-05-22〕
※ 112 IPA：安心相談窓口だより　大学におけるウェブメールサービスを狙ったフィッシングメールに注意　https://www.ipa.go.jp/security/anshin/mgdayori20181031.html〔参照 2019-05-22〕
※ 113 フィッシング対策協議会：ガイドライン　https://www.antiphishing.jp/report/guideline/〔参照 2019-05-22〕
※ 114 トランスコスモス株式会社：「SOKAオンラインストア」におけるクレジットカード情報ならびに個人情報の不正取得に関するお詫び、調査結果について　https://www.trans-cosmos.co.jp/company/news/pdf/2018/181009.pdf〔参照 2019-05-22〕
※ 115 ディー・エル・マーケット株式会社：不正アクセスによる個人情報流出に関するご報告とお詫び　https://www.dlmarket.jp/info20181225〔参照 2019-05-22〕
※ 116 株式会社伊織：【重要】クレジットカード情報流出についてのお知らせ（伊織ネットショップ）　http://www.i-ori.jp/wordpress/iori-press-release/20181024-0-37803.html〔参照 2019-05-22〕
※ 117 株式会社洋菓子舗ウエスト：不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.ginza-west.co.jp/info_2018/〔参照 2019-05-22〕
※ 118 株式会社ハセ・プロ：フィッシングサイトによるクレジットカード情報不正取得についてのお詫びと注意喚起のお知らせ　http://www.hasepro.com/corp/manager/wp-content/uploads/hasepro_release0226.pdf〔参照 2019-05-22〕
※ 119 ジェイ・ワークス株式会社:弊社が運営する「ショコラ ベルアメール」のオンラインショップ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お知らせ　https://www.j-works-net.co.jp/information/2959/〔参照 2019-05-22〕
※ 120 キヤノンマーケティングジャパン株式会社：世界中のユーザーを狙った不正ファイナンスアプリが Google Play 上に　https://eset-info.canon-its.jp/malware_info/special/detail/181106.html〔参照 2019-05-22〕
※ 121 ITmedia エンタープライズ：Amazon の DNS トラフィック乗っ取り、

仮想通貨盗まれる被害　https://www.itmedia.co.jp/enterprise/articles/1804/25/news063.html〔参照 2019-05-22〕
※ 122 JPCERT/CC：仮想通貨を要求する不審な脅迫メールについて https://www.jpcert.or.jp/newsflash/2018080201.html〔参照 2019-05-22〕
JPCERT/CC：仮想通貨を要求する日本語の脅迫メールについて https://www.jpcert.or.jp/newsflash/2018091901.html〔参照 2019-05-22〕
JPCERT/CC：仮想通貨を要求する不審な脅迫メールにご注意を https://www.jpcert.or.jp/tips/2018/wr183301.html〔参照2019-05-22〕
※ 123 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 2019-05-22〕
※ 124 IPA：安心相談窓口だより　性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意　https://www.ipa.go.jp/security/anshin/mgdayori20181010.html〔参照 2019-05-22〕
※ 125 Proofpoint：Sextortion with a side of ransomware　https://www.proofpoint.com/us/threat-insight/post/sextortion-side-ransomware〔参照 2019-05-22〕
※ 126 JPCERT/CC：マルウエアへの感染を誘導し、仮想通貨を要求する脅迫メールについて　https://www.jpcert.or.jp/newsflash/2018121101.html〔参照 2019-05-22〕
※ 127 セクストーション：スマートフォンの SNS アプリでのやり取り等で入手したプライベートな写真や動画をばらまくと脅して金銭を要求する脅迫。
※ 128 IPA：安心相談窓口だより　偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中　https://www.ipa.go.jp/security/anshin/mgdayori20180718.html〔参照2019-05-22〕
※ 129 Google LLC：Restricting ads in third-party tech support services　https://www.blog.google/products/ads/restricting-ads-third-party-tech-support-services/〔参照 2019-05-22〕
ZDNet Japan：グーグル、サポート詐欺などにつながる不正広告対策に着手--1秒で100件以上　https://japan.zdnet.com/article/35125015/〔参照 2019-06-11〕
※ 130 国民生活センター：インターネット使用中に突然表示される偽セキュリティ警告画面にご注意!　http://www.kokusen.go.jp/pdf/n-20181107_1.pdf〔参照 2019-05-22〕
※ 131 警視庁：通信販売サイトでのトラブルにご用心!　http://www.keishicho.metro.tokyo.jp/sodan/nettrouble/jirei/net_order_site.html〔参照 2019-05-22〕
JC3：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 2019-05-22〕
消費者庁：インターネット通販トラブル　https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/trouble/internet.html〔参照 2019-05-22〕
日本通信販売協会：通販のかしこい利用法 ネット通販詐欺的サイトに注意しましょう。　https://www.jadma.org/consumers/usage_fraud/〔参照 2019-05-22〕
※ 132 総務省：ふるさと納税の偽サイトにご注意ください　http://www.soumu.go.jp/main_sosiki/jichi_zeisei/czaisei/czaisei_seido/furusato/topics/20181207.html〔参照 2019-05-22〕
消費者庁：ふるさと納税の偽サイトに気を付けましょう!　https://www.caa.go.jp/policies/policy/consumer_policy/caution/caution_020/〔参照 2019-05-22〕
※ 133 JC3：顕在化した偽ショッピングサイトの脅威　https://www.jc3.or.jp/about/apwg_wp.html〔参照 2019-05-22〕
※ 134 SIA：悪質 EC サイトホットライン 通報フォーム　https://www.saferinternet.or.jp/akushitsu_ec_form/〔参照 2019-05-22〕
※ 135 https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf〔参照 2019-05-22〕
※ 136 SIA：なりすまし EC サイト対策協議会　https://www.saferinternet.or.jp/narisumashi/〔参照 2019-05-22〕
※ 137 消費者庁：インターネット通販トラブル　https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/trouble/internet.html〔参照 2019-05-22〕
※ 138 https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf〔参照 2019-05-22〕
※ 139 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　https://www.city.maebashi.gunma.jp/soshiki/kyoiku/gakkokyoiku/oshirase/3642.html〔参照 2019-05-22〕
※ 140 株式会社ダブリュ・アイ・システム：A ー Web 倶楽部「宅配サービス」におけるお客様情報流出に関するお詫びとご報告　https://goace.jp/files/user/pdf/180517.pdf〔参照 2019-05-22〕
※ 141 サンワ食研株式会社：【重要】個人情報、クレジット情報流出についてのお知らせ　https://shop.onkoh.com/user_data/press-release〔参照 2019-05-22〕
※ 142 JR九州ドラッグイレブン株式会社：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について（続報）　http://www.drugeleven.com/houkoku20190201〔参照 2019-05-22〕
Security NEXT：通販サイトで情報流出、不正プログラムでクレカ情報も窃取か - JR 九州傘下のドラッグストア　http://www.security-next.com/102200〔参照 2019-05-22〕
※ 143 Kroll：Starwood Guest Reservation Database Security Incident　https://answers.kroll.com/〔参照 2019-05-22〕
日本経済新聞：米マリオット　旅券番号 500 万件、暗号化されず流出 https://www.nikkei.com/article/DGXMZO39673000V00C19A1000000/〔参照 2019-05-22〕
※ 144 株式会社オージス総研：「宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～ https://www.ogis-ri.co.jp/news/1272165_6734.html〔参照 2019-05-22〕
※ 145 株式会社オージス総研：無料大容量ファイル転送サービス「宅ふぁいる便」ご質問一覧　https://www.ogis-ri.co.jp/news/takufile_faq.html〔参照 2019-03-11〕
※ 146 株式会社オージス総研：「宅ふぁいる便 Web 特設サイト」開設のご案内　https://info.ogis-support.jp/open.html〔参照 2019-05-22〕
※ 147 宝塚山本ガーデン・クリエイティブ株式会社：不正アクセスによるお客様情報流出の可能性に関するお知らせとお詫び　http://www.aiaipark.co.jp/kokuchi.pdf〔参照 2019-05-22〕
※ 148 森永乳業株式会社：健康食品通販サイトにおけるお客さま情報の流出に関するお詫びと調査結果のお知らせ　https://www.morinagamilk.co.jp/information2/newsentry-2900.html〔参照 2019-03-11〕
※ 149 ラッシュ株式会社：【メールアドレスおよびパスワード情報流出に関するお詫びとご報告】　http://www.quil-fait-bon.com/news/?twn=263&i=2〔参照 2019-05-22〕
※ 150 ZDNet Japan：ホテル予約サイトへの不正アクセス、情報漏えいは 401 施設で 32 万 5717 件に　https://japan.zdnet.com/article/35121520/〔参照 2019-05-22〕
※ 151 アサヒ軽金属工業株式会社：弊社が運営する「W eb ショッピングサイト」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お知らせ http://www.asahikei.co.jp/oshirase_o.html〔参照 2019-05-22〕
※ 152 株式会社リガク：不正アクセスによるお客様情報流出に関するお詫びと調査結果について　https://www.rigaku.co.jp/rigaku.com/news/181126.html〔参照 2019-05-22〕
※ 153 兵庫県立図書館：兵庫県立図書館におけるメールアドレスの誤送信について　https://www.library.pref.hyogo.lg.jp/news/owabi20181029.html〔参照 2019-05-22〕
※ 154 株式会社ユー花園：メール誤送信に関するお詫びとお知らせ【スワンフローリスト】　https://www.youkaen.com/archives/3584〔参照 2019-05-22〕
※ 155 株式会社ポニーキャニオン：ポニーキャニオンショッピングクラブ会員のお客様個人情報の誤表示に関するお知らせとお詫び　https://www.ponycanyon.co.jp/info/1496〔参照 2019-05-22〕
※ 156 山形市：平成29年度ふるさと納税に係る個人情報の誤掲載について（お詫び）　https://www.city.yamagata-yamagata.lg.jp/kakuka/shoko/brandsuishin/sogo/hurusatonouzei/hurusatonouzeiowabi.html〔参照 2019-05-22〕
※ 157 WIRED:個人情報など3億4,000万件、米企業から流出――データ収集をめぐるルール不足が浮き彫りに　https://wired.jp/2018/06/29/exactis-leak-340-million-records/〔参照 2019-05-22〕
※ 158 株式会社セキ薬品：弊社　愛宕店　元従業員によるお客様情報の不正利用について　https://www.sekiyakuhin.co.jp/uploads/topic_files/wdKANErMcpkpTKo15iCq7MIHUFTaSCYhgvGwar17.pdf〔参照 2019-05-22〕
※ 159 東京女子医科大学東医療センター：今般の患者情報に関する報道について　https://twmu-mce.jp/info/patient201808031457.html〔参照 2019-05-22〕
※ 160 https://www.ipa.go.jp/files/000057060.pdf〔参照2019-05-22〕
※ 161 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〔参照 2019-05-22〕
※ 162 https://jvndb.jvn.jp/〔参照 2019-05-22〕
※ 163 NIST：National Vulnerability Database（NVD）　https://nvd.nist.gov/〔参照 2019-05-22〕
※ 164 公表年は、ベンダがアドバイザリを公開した年、他組織やセキュリティポータルサイト等の登録 / 公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 165 IPA：共通脆弱性識別子 CVE 概説　https://www.ipa.go.jp/

security/vuln/CVE.html〔参照 2019-05-22〕
※ 166 The MITRE Corporation:CVE Numbering Authorities（CNA） https://cve.mitre.org/cve/cna.html〔参照 2019-05-22〕
※ 167 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs) https://cve.mitre.org/news/archives/2016/news.html〔参照 2019-05-22〕
※ 168 MongoDB Added as CVE Numbering Authority (CNA) https://cve.mitre.org/news/archives/2018/news.html〔参照 2019-05-22〕
※ 169 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 2019-05-22〕
※ 170 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 2019-05-22〕
※ 171 JPCERT/CC：セキュアコーディング https://www.jpcert.or.jp/securecoding/〔参照 2019-05-22〕
※ 172 Security Next:国内でも「Drupalgeddon 2.0」を観測 -「Drupal」利用者はアップデート状況の確認を http://www.security-next.com/092467〔参照 2019-05-22〕
※ 173 Security Next：脆弱な「Drupal」サイトをボット化、仮想通貨発掘させる攻撃が発生 http://www.security-next.com/095106〔参照 2019-05-22〕
※ 174 Drupal：Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002 https://www.drupal.org/sa-core-2018-002〔参照 2019-05-22〕
Drupal：Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-004 https://www.drupal.org/sa-core-2018-004〔参照 2019-05-22〕
※ 175 IPA：更新：Drupal の脆弱性対策について (CVE-2018-7600) https://www.ipa.go.jp/security/ciadr/vul/20180329-drupal.html〔参照 2019-05-22〕
※ 176 IPA：Drupal の脆弱性対策について (CVE-2018-7602) https://www.ipa.go.jp/security/ciadr/vul/20180426-drupal.html〔参照 2019-05-22〕
※ 177 日本オラクル株式会社：サポート・ロードマップ https://www.oracle.com/technetwork/jp/java/eol-135779-ja.html〔参照 2019-05-22〕
※ 178 IPA：公式アップデートの提供方法の変更に伴う Java SE の商用ユーザに向けた注意喚起 https://www.ipa.go.jp/security/announce/java8_eol.html〔参照 2019-05-22〕
※ 179 日本オラクル株式会社：JDK の新しいリリース・モデルおよび提供ライセンスについて https://www.oracle.com/technetwork/jp/articles/java/ja-topics/jdk-release-model-4487660-ja.html〔参照 2019-05-22〕
※ 180 Ethereum Foundation：Ethereum Project https://www.ethereum.org〔参照 2019-05-22〕
※ 181 GitHub：ERC-20 Token Standard https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md〔参照 2019-05-22〕
※ 182 IPA：脆弱性対策情報データベース JVN iPedia の登録状況［2018 年第 4 四半期（10 月～ 12 月）］ https://www.ipa.go.jp/security/vuln/report/JVNiPedia2018q4.html〔参照 2019-05-22〕
※ 183 Security NEXT：「Struts 2」脆弱性を狙う攻撃キャンペーン「Bleeding Thunder」- 国内企業のサイト含む標的リストも http://www.security-next.com/097318〔参照 2019-05-22〕
※ 184 株式会社 MS & Consulting：当社ホームページへの不正アクセスによるご登録情報の流出可能性について（続報） http://v4.eir-parts.net/v4Contents/View.aspx?cat=tdnet&sid=1596488〔参照 2019-05-22〕
三菱地所・サイモン株式会社：ショッパークラブ会員情報の流出に関する調査結果のご報告 https://www.premiumoutlets.co.jp/pressroom/pdf/180607.pdf〔参照 2019-05-22〕
※ 185 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 2019-05-22〕）
※ 186 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。
※ 187 IPA：安心相談窓口だより 脆弱性の悪用を防ぐため Windows アプリケーションの実行は新しいフォルダーで https://www.ipa.go.jp/security/anshin/mgdayori20171003.html〔参照 2019-05-22〕
※ 188 JPCERT/CC：感謝状 2018 https://www.jpcert.or.jp/press/priz/2018/PR20180710-priz.html〔参照 2019-05-22〕
JPCERT/CC：感謝状 2015 https://www.jpcert.or.jp/press/priz/2015/PR20150820-priz.html〔参照 2019-05-22〕
※ 189 JPCERT/CC：「JPCERT/CC 製品開発者リスト」登録ベンダー一覧 https://jvn.jp/nav/〔参照 2019-05-22〕
※ 190 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 2019-05-22〕
※ 191 IPA：複数の Microsoft 社製品のサポート終了に伴う注意喚起 https://www.ipa.go.jp/security/announce/win7_eos.html〔参照 2019-05-22〕
※ 192 Microsoft 社：Windows 7 と Office 2010 から、最新のクラウド環境（Microsoft 365）への移行状況と移行支援施策を発表 https://news.microsoft.com/ja-jp/2018/10/17/windows7_office2010_20181017/〔参照 2019-05-22〕
※ 193 有限会社ひのでやエコライフ研究所：不正アクセスによる個人情報流出のご報告とお詫び https://www.hinodeya-ecolife.com/article.php/20180627103210959〔参照 2019-05-22〕
※ 194 株式会社あぐりーん：会員情報の漏えいの可能性に関するご報告とお詫び https://www.agreen.jp/whatsnew/news.php?id=1955〔参照 2019-05-22〕
※ 195 株式会社フレーバーライフ社：弊社提携外部サーバーへの不正侵入について（第二報） https://www.flavorlife.co.jp/emergency.html〔参照 2019-05-22〕
※ 196 三菱地所・サイモン株式会社：会員情報流出の可能性について https://www.premiumoutlets.co.jp/pressroom/pdf/180407.pdf〔参照 2019-05-22〕
三菱地所・サイモン株式会社：ショッパークラブ会員情報の流出に関する調査結果のご報告 https://www.premiumoutlets.co.jp/pressroom/pdf/180607.pdf〔参照 2019-05-22〕
※ 197 https://www.ipa.go.jp/files/000017319.pdf〔参照 2019-05-22〕
※ 198 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 2019-05-22 f〕
※ 199 https://www.openbugbounty.org/〔参照 2019-05-22〕
※ 200 IPA：情報セキュリティサービス基準適合サービスリストの公開 https://www.ipa.go.jp/security/it-service/service_list.html〔参照 2019-05-22〕
※ 201 JVN：JVN#55263945: RICOH Interactive Whiteboard における複数の脆弱性 https://jvn.jp/jp/JVN55263945/〔参照 2019-05-22〕
※ 202 LINE 株式会社：LINE Security Bug Bounty Program https://bugbounty.linecorp.com/ja/〔参照 2019-05-22〕
※ 203 サイボウズ株式会社：サイボウズ脆弱性報奨金制度 https://cybozu.co.jp/products/bug-bounty/〔参照 2019-05-22〕
※ 204 Bugcrowd Inc.：2018 State of Bug Bounty Report https://www.bugcrowd.com/resource/2018-state-of-bug-bounty-report/〔参照 2019-05-22〕
※ 205 DoD：Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/〔参照 2019-05-22〕
※ 206 NCSC：NCSC vulnerability disclosure co-ordination https://www.ncsc.gov.uk/blog-post/ncsc-vulnerability-disclosure-co-ordination〔参照 2019-05-22〕
※ 207 Cyber Security Agency of Singapore：GovTech and CSA partner cybersecurity community on Government Bug Bounty Programme https://www.csa.gov.sg/news/press-releases/govtech-and-csa-partner-cybersecurity-community-on-government-bug-bounty-programme〔参照 2019-05-22〕
※ 208 ISO：ISO/IEC 29147:2018 Information technology -- Security techniques -- Vulnerability disclosure https://www.iso.org/standard/72311.html〔参照 2019-05-22〕
※ 209 DCMS：Guidance Code of Practice for consumer IoT security https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security〔参照 2019-05-22〕
※ 210 日本語訳は以下で公表されている。https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775860/054718_DCMS_IoT_Code_of_Practice_JAPANESE.pdf〔参照 2019-05-22〕
※ 211 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 https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔参照 2019-05-22〕
※ 212 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/security/ciadr/partnership_guide.html〔参照 2019-05-22〕
※ 213 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況［2018 年第 4 四半期（10 月～ 12 月）］ https://www.ipa.go.jp/files/000071102.pdf〔参照 2019-05-22〕

第2章
情報セキュリティを支える基盤の動向

2018 年度は、セキュリティ強化のための政策の見直しや制度の本格的な運用が始まった年であった。国内では、新たなサイバーセキュリティ戦略が策定され、産業サイバーセキュリティ研究会による産学官の取り組みの本格化、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発行、プロジェクト「NOTICE」の開始等、今後のセキュリティ対策に関わりが深いと思われる取り組みが行われた。国外では、米国の国家サイバー戦略の発表、欧州の GDPR の発効と他国にも大きく影響を及ぼす政策が動き出した。

本章では、情報セキュリティを支える基盤の動向として、2018 年度の主な国内外の政策、人材育成、国際標準化、各種認証、組織・個人における情報セキュリティの取り組みの実態等について解説する。

2.1 国内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※1」「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、新たなサイバーセキュリティ戦略と 2018 年度に実施された主な取り組みについて述べる。

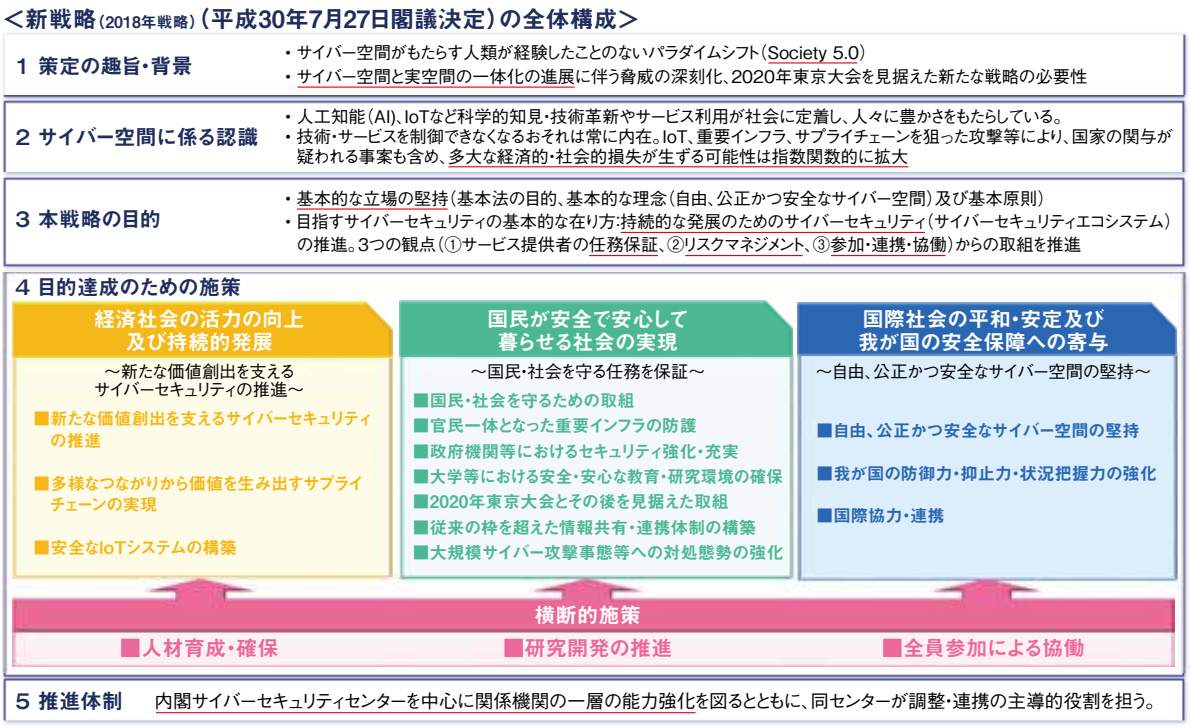
(1)「サイバーセキュリティ戦略」の見直し

「サイバーセキュリティ戦略」とは、我が国のサイバーセキュリティにおける基本的な立場等と策定後 3 年間の施策目標や実施方針を示した行動計画を指す。2015 年 9 月に初めてサイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」（以下、2015 年戦略）が閣議決定され、2018 年 7 月に 2 回目となる「サイバーセキュリティ戦略※2」（以下、2018 年戦略）が閣議決定された（図 2-1-1）。

2015 年戦略の策定以降、サイバー空間とフィジカル（実）空間の一体化がより進んでいることで、社会に豊かさをもたらす可能性がある一方、サイバー攻撃によってフィジカル空間における経済的・社会的損失のリスクが深刻化し得ることが懸念されている。

そこで 2018 年戦略では、サイバーセキュリティ基本法の目的や、2015 年戦略の基本的な理念及び基本原則を堅持しつつ、経済社会が自律的・持続的に進化・発展していくために、以下の三つの観点から官民での取り組みを推進することが示されている。

- サービス提供者の任務保証
  任務保証とは、企業や政府機関を含むあらゆる組織において、自ら遂行すべき業務やサービスを「任務」ととらえ、これを着実に遂行するために必要な能力及び資産を確保することを指す。その際、責任を有する者（経営層や幹部）が主体となり、「任務」とする業務やサービスを選定し、安全かつ持続的な提供に関する責任を全うすることが重要である。
- リスクマネジメント
  各組織の「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応を指す。これは組織を指揮統制することで、組織の資源を適切に分配し、リスクに対応していく一連の活動



■図 2-1-1　サイバーセキュリティ戦略の概要
（出典）NISC「サイバーセキュリティ戦略（閣議決定）の詳細概要※3」

全体を意味する。

- 参加・連携・協働
  個人または組織が、サイバー空間の脅威から発生し得る被害やその拡大を防止するために平素から講じる基本的な取り組みを指す。セキュリティ脅威が日常化し、サイバー空間で活動する主体は個人・組織にかかわらず誰もが脅威に晒される可能性がある中、個々の努力による取り組みでは対応が困難であることから、他者との協働が必要となる。個人や組織各々が常に情報共有を行い、連携・協働することを、サイバー空間における新たな公衆衛生活動ととらえる必要がある。

また、2018 年戦略の目的達成の施策として、「経済社会の活力の向上及び持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安定及び我が国の安全保障への寄与」「横断的施策」の四つの観点が示されている。2018 年度に実行された施策については次項で述べる。

(2)「サイバーセキュリティ 2018」の主な取り組み状況

「サイバーセキュリティ 2018※4」は、2018 年戦略に基づく 2018 年度の年次計画であり、関連府省庁はこれに基づき施策を実施する。以下、2018 年戦略の目的達成の施策として示されている四つの観点について、「サイバーセキュリティ 2018」で計画し実施された主な取り組みを述べる。

- 経済社会の活力の向上及び持続的発展
  経済産業省と IPA は、経営者が主体となってサイバーセキュリティ対策を推進するための指針である「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るため、具体的な対策事例等を示すプラクティス集※5を 2019 年 3 月に発行した。
  総務省は、サイバーセキュリティタスクフォース※6のもとに設置した情報開示分科会での検討を踏まえ、企業が積極的な情報開示を行い社会的な企業価値を向上させること等を目的とした「セキュリティ対策情報開示ガイドライン（仮称）」の策定に着手し、2019 年 4 月以降に公開予定としている※7（情報開示分科会での検討については「2.1.3 (1) (c) 民間企業等におけるセキュリティ対策の促進」参照）。
  経済産業省と IPA は、サイバーセキュリティの政策・課題に関する官民の情報共有や企業同士の連携を図るため、メンバーを限定しない情報交流の場である「コラボレーション・プラットフォーム※8」を 2018 年 6 月に開催し、2019 年度も継続して開催している（コラボレーション・プラットフォームについては「2.1.2 (1) (c)

WG3（サイバーセキュリティビジネス化）参照」）。
経済産業省は、サイバー空間とフィジカル空間を跨いだ新たな形のサプライチェーンのセキュリティに関して、全産業にほぼ共通したセキュリティリスク管理の枠組みとなる「サイバー・フィジカル・セキュリティ対策フレームワーク※9」を2019年4月に発行した（本フレームワークについては「2.1.2(1)(a)WG1（制度・技術・標準化）」参照）。

- 国民が安全で安心して暮らせる社会の実現
総務省と経済産業省は、2018年8月、官民双方が安心・安全にクラウドサービスを活用していくために、信頼性確保の観点から同サービスの安全性評価について検討を開始した（「2.1.2 (2) クラウドサービスの安全性評価」参照）。政府は、検討会での議論を踏まえ、政府のクラウドサービス規程に反映する等、必要な措置を講ずることとされている※10。
内閣官房は、2020年に開催される東京オリンピック・パラリンピック競技大会に向けて、リスクマネジメントの促進と対処態勢の整備を実施した※11。リスクマネジメントの促進については、同大会の開催・運営に影響を与え得る重要サービス事業者を選定してリスクアセスメントの実施を依頼し、その結果について分析・フィードバックを行った。また、同大会会場に提供されるサービスの重要度に応じて事業者を選定し、サイバーセキュリティ対策の実施状況を、NISCが横断的リスク評価により検証した。対処態勢の整備については、同大会に係るサイバーセキュリティの脅威・インシデント情報を収集し関係機関等に提供するほか、必要に応じて関係機関等のインシデント対応における対処支援調整を実施する「サイバーセキュリティ対処調整センター」を2019年4月に構築した※12。
- 国際社会の平和・安定及び我が国の安全保障への寄与
経済産業省及びIPAは、米国国土安全保障省（Department of Homeland Security：DHS）及びDHS傘下のICS-CERT（Industrial Control Systems Cyber Emergency Response Team）とともに、人材育成プログラムの一環として「ASEAN等向け日米サイバー共同演習※13」を実施した（同演習については「2.3.2 産業サイバーセキュリティセンター」参照）。また、関連府省庁は、ASEAN加盟国とサイバーセキュリティに関する協議を実施した（「2.2.1 (5) ASEANとのサイバー連携」参照）。
- 横断的施策
内閣官房は、経営層、戦略マネジメント層、実務者層・技術者層の3層の観点からなる「サイバーセキュリティ人材育成取組方針※14」（2018年5月決定）を踏まえ、関連府省庁と協力し、セキュリティ人材の育成や役割定義等について検討を行った（セキュリティ人材の育成については「2.3.1 情報セキュリティ人材の状況」参照）。また、内閣府に設置された総合科学技術・イノベーション会議のもと、戦略的イノベーション創造プログラム（Cross-ministerial Strategic Innovation Promotion Program：SIP）第2期が2018年度から開始された※15。同プログラムのうち、「IoT社会に対応したサイバー・フィジカル・セキュリティ※16」は、IoT（Internet of Things）システム・サービス及び中小企業を含むサプライチェーン全体のセキュリティ確保を実現する「サイバー・フィジカル・セキュリティ対策基盤」の開発と実証を行うものである。IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築することで、IoT社会の強靱化を図り、我が国のセキュアなSociety 5.0実現に寄与することが期待される。

(3) 重要インフラの情報セキュリティ対策強化

我が国の重要インフラの防護に係る基本的な枠組みとして、サイバーセキュリティ戦略本部は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※17」（以下、第4次行動計画）を決定した。そして、国民生活や社会経済活動に与える影響度を考慮した結果、新たな重要インフラ分野として「空港」分野を追加する形で、2018年7月に第4次行動計画を改定した※18。

また、各重要インフラ分野に共通して求められる情報セキュリティ対策の実施を訴求するため、2018年4月、サイバーセキュリティ戦略本部が「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）※19」を、重要インフラ専門調査会が「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）※20」を公開した（手引書については「3.1.4 (1) 重要インフラサービスを支えるシステムのリスクアセスメントの促進に関する取り組み」参照）。以下、2018年度における主な活動について述べる。

(a) 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(初版)

サイバーセキュリティ戦略本部は、第4次行動計画に基づく重要インフラ防護の取り組みの一環として、重要インフラ専門調査会の調査審議を経た2018年7月に「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(初版)※21」(以下、評価基準)を公開した。

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のサービス障害に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。初版は、第1段階として、発生したサービス障害が与えた影響全体の深刻度を事後に評価する基準を定めている。

深刻度は、レベル0(影響なし)～レベル4(著しく深刻な影響)の5段階で示され、「サービスの持続性への影響」「サービスに関する安全性への影響」「その他」の三つの観点ごとに独立に評価される。そして、この三つの観点における深刻度の中で最も高い値が、当該障害の深刻度となる。

次の段階として、サービス障害が発生した時点での社会への影響の予測に評価基準を活用し、政府の対応の判断基準や、官民の情報共有の体制や方法の基準とすること、また、評価基準の国際的整合性を図っていくことについて検討が行われている。

(b)「分野横断的演習」の実施

NISCは、重要インフラ分野における障害対応体制の強化を図るため、2018年12月に13回目となる分野横断的演習を実施した※22。新たに重要インフラ分野に指定された「空港」を含む計14分野にわたる重要インフラ事業者や重要インフラ所管省庁、情報セキュリティ関係機関等から、過去最大となる3,077名が参加した。本演習では設定された状況のもと、重要インフラ事業者が事業継続計画等に基づき、状況整理や所管省庁との連絡、対応方針の検討、関係機関や他事業者との情報共有等を実施した。

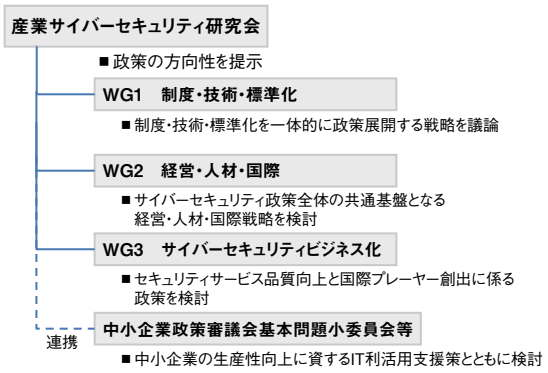
また、2019年度の演習についてNISCは、東京オリンピック・パラリンピック競技大会を見据え、同大会開催時に想定される一層困難な脅威にも対応できることを目指した内容にすることを検討している。

2.1.2 経済産業省の政策

経済産業省は、サイバー空間、フィジカル空間を統合したサプライチェーン全体にわたるセキュリティ対策の実現に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1) 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」を設置した※23。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取る。図2-1-2に同研究会の構成を示す。



■図2-1-2 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※24」

また、同研究会では「産業サイバーセキュリティ強化へ向けたアクションプラン※25」として以下の四つの政策パッケージを打ち出し、各WGがこれらに取り組む形となっている。

- サプライチェーンサイバーセキュリティ強化パッケージ
- サイバーセキュリティ経営強化パッケージ
- サイバーセキュリティ人材育成・活躍促進パッケージ
- セキュリティビジネスエコシステム創造パッケージ

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・標準化を一体として政策に展開する戦略を議論している。その前提として、サイバー空間とフィジカル空間の融合により、柔軟かつ動的なサプライチェーンが生まれるとし、これを価値創造過程(バリュークリエイションプロセス)と定義した。また、バリュークリエイションプロセ

ス全体の業界横断的な標準モデルを「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）※26」（以下、フレームワーク）として公開した。

またフレームワークをビル、電力、防衛産業、自動車産業、スマートホーム等の産業分野別のサブワーキンググループ（以下、SWG）に展開し、各分野での具体的な適用を検討した。このうちビルSWGは、2018年9月に「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」を公開した※27。

WG1はまた、分野横断SWGを設置し、各産業分野における検討から共通課題を抽出して、その対策の方向性等をフレームワークに反映するほか、国内外の意見を踏まえた修正について検討を行った※28。これらの結果、2019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（The Cyber/Physical Security Framework）Version 1.0」（以下、CPSF）を策定した※9。

CPSFでは、産業社会を三つの層で整理した「3層構造モデル」ととらえることでセキュリティ確保のための信頼性の基点を明確化するとともに、バリュークリエイションプロセスに関与する、セキュリティ対策を講じる最小単位として整理した「六つの構成要素」を提示している。これらに基づいて、リスク源を洗い出し、その対策要件※29を特定（リスクベースアプローチ）できるとしている（図2-1-3）。

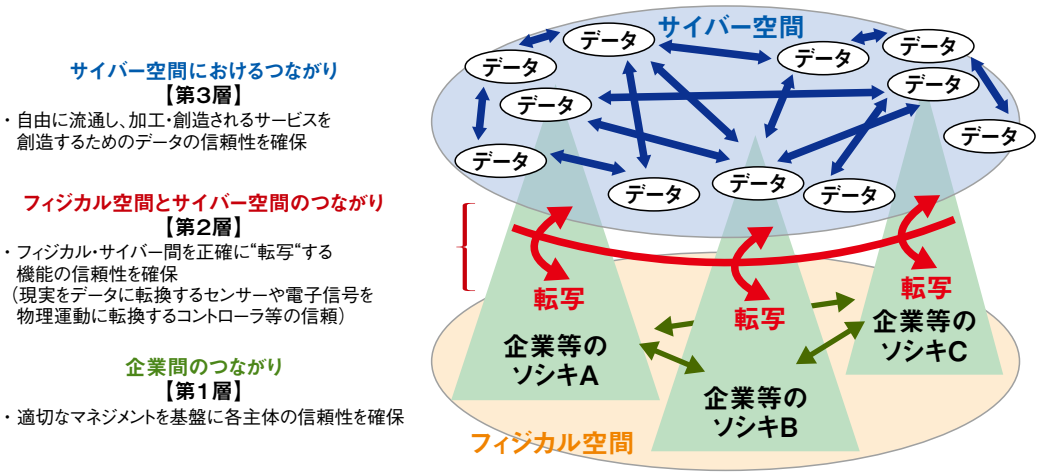
- 3層構造
  - 第1層－企業間のつながり
  - 第2層－フィジカル空間とサイバー空間のつながり
  - 第3層－サイバー空間におけるつながり
- 六つの構成要素
  - ソシキ:バリュークリエイションプロセスに参加する企業・団体・組織
  - ヒト：ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
  - モノ:ハードウェア、ソフトウェア、及びそれらの部品（操作する機器を含む）
  - データ:フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
  - プロシージャ：定義された目的を達成するための一連の活動の手続き
  - システム：目的を実現するためにモノで構成される仕組み・インフラ

また、3層構造モデルにおいて、第1層では企業ごとのマネジメントを中心にセキュリティ対策が実施される一方、第2層及び第3層においては、マルチステークホルダによるセキュリティ対策の取り組み（マルチステークホルダアプローチ）が求められる。第2層では、バリュークリエイションプロセスに直接関与する企業だけでなく、当該企業の転写※31機能を担うシステムに関わる企業の協力が不可欠となる。第3層では、データの流通や取り扱いに間接的に関与する主体も、セキュリティ確保のために一定の役割を果たすことが求められている。

今後WG1では、産業活動へのCPSF実装を促進するべく、第2層及び第3層に焦点を絞り検討する各タスクフォースや、オープンソースソフトウェア等のソフトウェアの活用・脆弱性管理手法を検討するタスクフォースを設置するとしている※32。

（b）WG2（経営・人材・国際）

WG2では、サイバーセキュリティ対策における経営者の参画と人材育成、国際連携に関する政策を議論して



■図2-1-3　3層構造モデルと各層における信頼性
（出典）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 Version 1.0※30」

いる。

経営に関して、CGS（コーポレート・ガバナンス・システム）研究会は2019年4月に、グループ経営を行う上場企業を主な対象として、グループ全体の価値向上を図るためのガバナンスの在り方を示す「グループ・ガバナンス・システムに関する実務指針（仮）[※33]」を公開した。本指針案では、サイバーセキュリティを内部統制システム上の重要なリスク項目としてとらえ、親会社の取締役会レベルでグループ全体やサプライチェーンを考慮に入れたサイバーセキュリティ対策の在り方を検討すべきと明記している。WG2は2019年3月、IPAを通じて、2017年11月に改訂された「サイバーセキュリティ経営ガイドライン Ver 2.0[※34]」の内容を実践する上で参考となるよう、「サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集」を公開した[※5]（プラクティス集については「2.4.1(2)(c)サイバーセキュリティ対策の在り方」参照）。

また、WG2は中小企業のセキュリティ強靭化に向けた「サイバーセキュリティお助け隊」の創設の議論を行った[※35]。なお、IPAでは同年3月に、主に中小企業の経営者とIT担当者を対象とした「中小企業の情報セキュリティ対策ガイドライン第3版」を公開した[※36]（「2.4.2(3)中小企業の情報セキュリティ対策ガイドライン」参照）。

人材に関して、WG2は企業に求められるセキュリティ機能を遂行する人材の活用の進め方を「セキュリティ人材活用モデル」として整理したほか、ユーザ企業内のセキュリティ体制の整理等を実施した（「2.3 情報セキュリティ人材の現状と育成」参照）。関連して、戦略マネジメント層[※37]の育成に関する取り組みとして、IPAは産業サイバーセキュリティセンターで2018年11～12月に「戦略マネジメント系セミナー」を実施した（「2.3.2(2)(c)戦略マネジメント系セミナー」参照）。また、一橋ビジネススクールICS（School of International Corporate Strategy：国際企業戦略専攻）の協力のもと、同年9～11月に「デジタル・トランスフォーメーション時代における人材育成プログラム」を実施した。他にも、国立高等専門学校におけるセキュリティ教育が産業界の求める人材像と整合していくために、独立行政法人国立高等専門学校機構と経済産業省、IPA及び業界団体における連携が検討された。

国際連携活動としては、2018年9月10～14日に「ASEAN等向け日米サイバー共同演習」を実施した（「2.3.2 産業サイバーセキュリティセンター」参照）。また、国際会議等で各国のステークホルダとCPSFを軸とした議論を行い、サイバー・フィジカル・セキュリティに関する共通認識を醸成した[※35]。

(c) WG3（サイバーセキュリティビジネス化）

WG3では、セキュリティ製品・サービスの品質向上と国際プレーヤー創出に係る政策として、サイバーセキュリティ検証基盤の整備による国内セキュリティビジネスの競争力創出等の議論を行った[※38]。

またWG3はIPAを通じて、2018年6月から、サイバー・フィジカル・セキュリティに関する情報交流の場として「コラボレーション・プラットフォーム」を設置した。ここではメンバーを限定せず、議論を通じてサイバーセキュリティ対策のニーズを明確化・具体化するとともに、シーズに関する情報提供・情報収集等を行うことで、政策等への反映や企業間のマッチングを図っている。2018年度は7回実施し、計886名が参加した。更に、情報セキュリティサービスに関して、一定の品質を維持・向上するための要件を定めた「情報セキュリティサービス基準」のもと、IPAは本基準に適合するサービスのリストを2018年7月から公開している（「2.1.2(5)情報セキュリティサービス基準適合サービスリスト」参照）。

(2) クラウドサービスの安全性評価

経済産業省と総務省は、2018年8月から「クラウドサービスの安全性評価に関する検討会[※10]」を発足させた。本検討会では、「未来投資戦略2018[※39]」を踏まえ、クラウドサービスに関する既存のガイドラインや国内外の認証制度、監査制度等を整理するとともに、適切なセキュリティを満たすクラウドサービスを導入するために必要な評価方法等を検討する。そして本検討会での議論を踏まえ、政府が具体的な内容を「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」や「政府情報システムにおけるクラウドサービスの利用に係る基本方針[※40]」に反映すること等を想定している。

安全性評価の制度設計にあたり、情報・情報システムのクラス分け、及びクラウドサービスの安全性評価の制度そのものの二つの観点における議論が行われている。2019年3月に公開された「クラウドサービスの安全性評価に関する検討会 中間取りまとめ（案）[※41]」では、特に後者の目指すべき姿として、各政府機関共通のクラウドサービス要件を設定し、一度当該要件を満たしていることが示された場合に各政府機関が結果の相互利用を可能とすることで、安全性評価の効率化を行うこととしている。なお、安全性評価の制度の枠組みは、情報セキュリティ監査の仕組みを活用したものとするとしている。

また、本枠組みを実施するために、本検討会から政府に示す基準等は、以下の四つに整理されている。

- 管理基準
- 監査主体の選定基準
- 監査基準
- 標準監査手続

本検討会は今後、2019 年内に最終取りまとめ及び安全性評価制度の立ち上げを実施し、2020 年秋に全政府機関等での制度活用を開始することを目指すとしている。

(3) AI・データの利用に関する契約ガイドライン

契約におけるデータの利用権限を公平に取り決めるための考え方を示すため、経済産業省は、2017 年 5 月に「データの利用権限に関する契約ガイドライン ver1.0[※42]」を公開した。一方で、IoT や AI(Artificial Intelligence:人工知能) 技術の急速な進展に伴い、新たなデータの取り扱いや活用方法が現れてきている。そこで、データ契約の類型別整理やユースケースの充実等を図るとともに、新たに AI の開発・利用に関する契約実務等の考え方を追加した「AI・データの利用に関する契約ガイドライン[※43]」を 2018 年 6 月に策定した。本ガイドラインは、以下の「データ編」と「AI 編」の二つで構成されている。

(a) データ編

データ編では、契約段階では価値が不明瞭なことが多いデータの流通や利用を対象とする契約について、各当事者の立場を検討し、一般的に定めておくべき事項を類型別に整理・列挙している。加えて、その契約条項例や条項作成時に考慮すべき要素等も提示している。

データ契約の類型は以下に示す「データ提供型」「データ創出型」「データ共用型」の三つに整理される。

- データ提供型
  取引対象のデータを提供者のみが保持している(適法にアクセス可能である) ことが明確な場合において、当該データを提供者から他方当事者へ提供する際、他方当事者のデータ利用権限やデータ提供条件等を取り決めるための契約。
- データ創出型
  複数当事者が関与することで新たにデータが創出される場合において、当該当事者間でデータの利用権限について取り決めるための契約。
- データ共用型
  複数事業者がデータをプラットフォームに提供し、プラットフォームが当該データを集約・保管、加工または分析し、複数事業者がプラットフォームを通じて当該データを共用するための契約。

(b) AI 編

AI 編では、AI 技術を活用したソフトウェア(特に学習済みモデル)の特性を踏まえ、開発・利用契約を作成するにあたり構成要素やトラブル予防方法等についての基本的な考え方を提示している。また、開発契約については、契約時に成果が不明瞭であり、開発後も再学習する需要がある等の特徴がある。そのため、開発プロセスを①アセスメント段階、② PoC (Proof of Concept:概念実証) 段階、③開発段階、④追加学習段階の四つに分け、段階的に検証し、当事者相互の確認を得ながら開発する「探索的段階型」の導入を提唱している(AI の開発・利用におけるトラスト(信頼)については「3.5 AI のトラストとセキュリティ」参照)。

(4) 産業競争力強化法等の一部改正

2018 年 5 月、「産業競争力強化法等の一部を改正する法律」が成立し、同年 7 月に施行された[※44]。本法律には複数の法律における改正内容が含まれている。

セキュリティに関する事項として、産業競争力強化法の一部改正に基づき、同年 9 月から「技術等情報管理認証制度[※45]」が開始された。これは、企業の技術情報等の管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関から認証を受けられる制度である。認証機関に対する支援措置として、独立行政法人中小企業基盤整備機構(以下、中小機構)や IPA からの情報提供支援がある。

また、「産業競争力強化法等の一部を改正する法律」に含まれていた中小企業等経営強化法の一部改正に伴い、中小企業に IT ツールを提供する IT ベンダ等を「情報処理支援機関(スマート SME サポーター)」として認定する制度が創設された[※46]。この背景として、サービス等生産性向上 IT 導入支援事業(IT 導入補助金)で対象となる IT ツールについて、どのツールに効果があり、安全に利用できるかが分かりにくい等の中小企業の声があった。本制度はこれを受けて、スマート SME サポーターと当該サポーターが提供する IT ツールに関する登録情報を開示することで中小企業の IT 導入を促進し、生産性向上を図るものである。また、スマート SME サポーターに対して、中小機構と IPA から、中小企業経営やサイ

バーセキュリティに関する講習会等への講師の派遣・情報提供といった支援を行う※47。

(5) 情報セキュリティサービス基準適合サービスリスト

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認定検討会」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※48。本サービス基準は、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否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。

IPA は 2018 年 7 月から、審査登録機関※49 による審査の結果サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつ IPA に誓約書を提出した事業者の情報セキュリティサービスを掲載した「情報セキュリティサービス基準適合サービスリスト※50」を公開している。本サービス基準では、情報セキュリティサービスを以下の四つに分類しており、これらのサービス登録数の合計が 2019 年 4 月に 100 件に到達した。

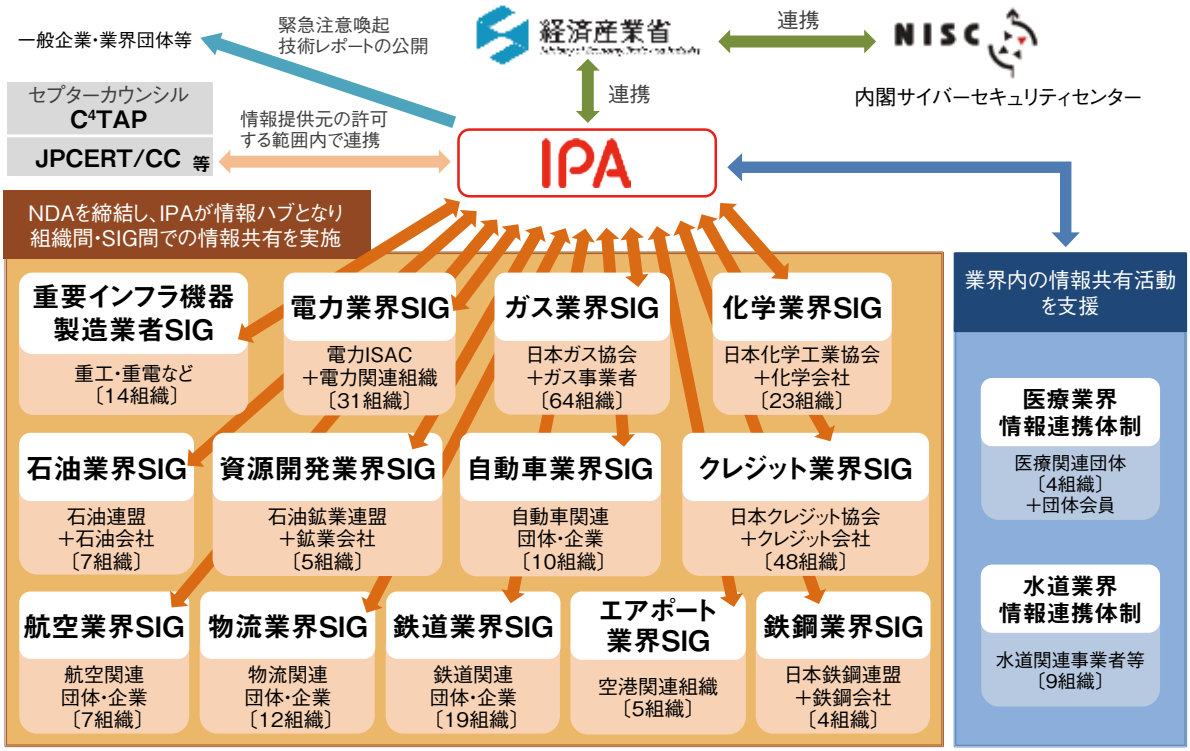
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

なお、本サービスリストに掲載されているサービス（デジタルフォレンジックサービスを除く）を利用した場合、コネクテッド・インダストリーズ税制の支援措置におけるセキュリティ要件の一部を満たすことになる※51。今後、本サービスリストの活用が進むことで、情報セキュリティサービス市場の活性化にもつながることが期待される。

(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 月から、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。2019 年 3 月末時点で、IPA を情報の中継・集約点（情報ハブ）として 13 の領域（SIG※52）から 249 の企業や業界団体（以下、組織）が J-CSIP に参加している。2018 年 11 月には「エアポート業界 SIG」、同年 12 月には「鉄鋼業界 SIG」が新たに発足した。既存 SIG も含め、2018 年



■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［2019 年 1 月～ 3 月］※53」

度は 2017 年度よりも全体で参加組織数が 21 拡大した。

また、2017 年度に調整を進めていた、個別に NDA（Non-Disclosure Agreement：秘密保持契約）を締結せず、規約を基に情報共有活動を支援するための新たな枠組みである「情報連携体制」が、2018 年 5 月から開始された。同年 5 月に「医療業界 情報連携体制」（4 組織）、11 月に「水道業界 情報連携体制」（9 組織）が発足している（前ページ図 2-1-4）。

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※54、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）等とも連携している。J-CSIP では、IPA と参加組織との間で NDA を締結し（「情報連携体制」を除く）、サイバー攻撃に関する手口や被害の情報、標的型攻撃メール等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。

	2015 年度	2016 年度	2017 年度	2018 年度
参加組織からの情報提供件数	1,092 件	2,505 件	3,456 件	2,020 件
攻撃メール件数	97 件	177 件	274 件	213 件
情報共有件数	133 件	96 件	242 件	195 件

■表 2-1-1　J-CSIP の運用実績

2018 年度は、いずれの件数においても 2017 年度より減少しているものの、継続して情報提供や共有が行われていることが分かる。

2018 年 7 月に、IPA としては初めて、「日本語のビジネスメール詐欺」について実際のメール内容の情報提供を受けた。この事例を含め改めて情報を整理し、IPA は同年 8 月にビジネスメール詐欺に関する攻撃の流れや技術的手口を解説した注意喚起レポートを公開した※55（ビジネスメール詐欺については「1.2.2 ビジネスメール詐欺（BEC）」参照）。

また、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 2018 年度も多く発生し、特に 2018 年 8 月には IQY ファイル※56 を悪用した同メールの情報提供が多くあった。IPA は、同年 7 月には海外の情報を基に既に IQY ファイルを悪用した攻撃手口に関する参考資料を公開していたが、8 月に日本語の事例を追加した第 2 版を公開した※57。

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に関して、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 参加組織から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等から、各種ウイルス※58 情報等を収集している。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※59。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)。

相談を受けた案件のうち、緊急を要する事案に対しては「レスキュー支援」を行い、更に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。

2018 年度の活動実績を 2017 年度と比較すると、相談件数はほぼ変わらず、レスキュー支援数は減少している一方、オンサイト支援数が増加している。

また、J-CRAT では、定期的に活動状況を公開するほか、情報収集活動や支援活動から得られた結果を技術レポートとして随時公開している。これらの取り組み等を通じ、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。

	2015 年度	2016 年度	2017 年度	2018 年度
相談件数	537 件	519 件	412 件	413 件
レスキュー支援数	160 件	123 件	144 件	127 件
オンサイト支援数※	39 件	17 件	27 件	31 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 の活動実績

2.1.3 総務省の政策

総務省は、IoT・AI 時代に対応したサイバーセキュリティ体制の早期確立を目指して 2017 年 1 月に公表した「IoT サイバーセキュリティ アクションプログラム 2017※60」を踏まえ、同月、必要な対策の推進を目的とした「サイバーセキュリティタスクフォース」を発足させた※61。

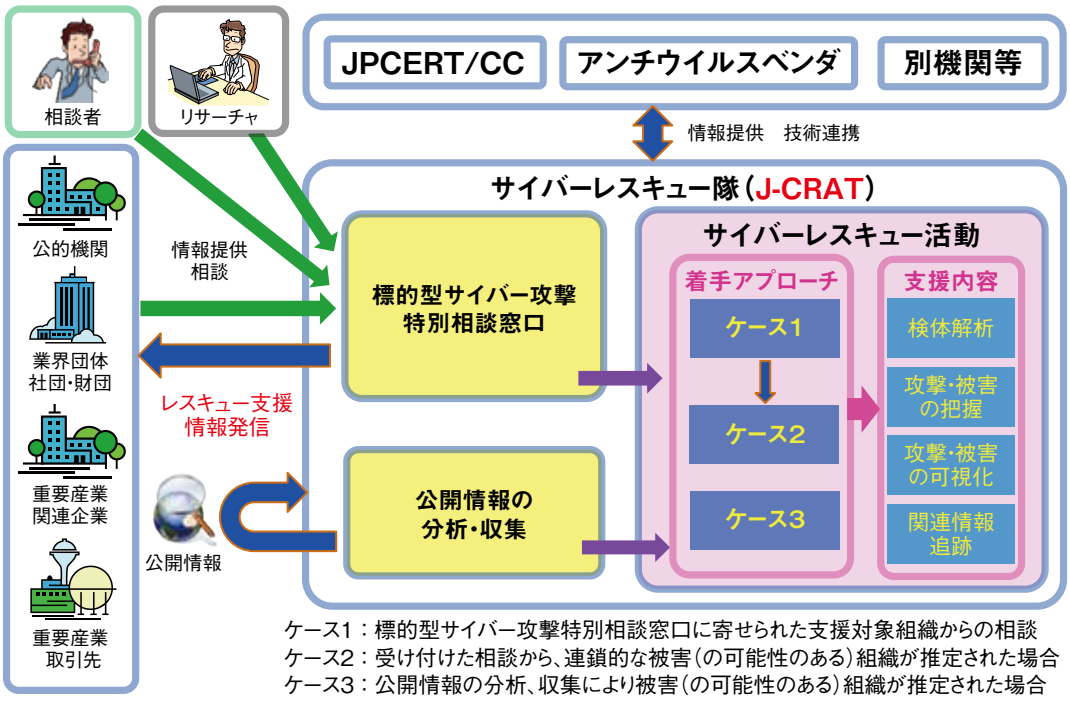
同タスクフォースは、2017 年 4 月、IoT セキュリティ対策の方針となる「IoT セキュリティ対策に関する提言※62」をまとめ、同年 10 月には、同提言に基づき、「IoT セキュリティ総合対策※63」を策定した。更に、翌 2018 年 7 月、同総合対策の進捗状況をまとめ、「IoT セキュリティ総合対策 プログレスレポート 2018※64」として公表した。

総務省は、同総合対策に基づき、脆弱性対策に係る体制の整備、研究開発の推進、民間企業等におけるセキュリティ対策の推進、人材育成の強化、国際連携の推進の各施策群について各種の取り組みを推進している。

以下に総務省の政策の概要を述べる。

(1)「IoT セキュリティ総合対策」に基づく主な取り組み

「IoT セキュリティ総合対策 プログレスレポート 2018」



■図 2-1-5　J-CRAT の活動の全体像とスキーム
(出典)IPA「サイバーレスキュー隊 J-CRAT(ジェイ・クラート)※65」

に基づき、主な取り組みの進捗状況を述べる。

(a)脆弱性対策に係る体制の整備に向けた主な取り組み

脆弱性対策に係る体制の整備に向けた主な取り組みについて述べる。

- セキュリティ・バイ・デザイン等の意識啓発・支援の実施

  IoT 機器等がサイバー攻撃の踏み台に悪用されることを防ぐためには、端末がウイルスに大量感染することを防ぐ最低限のセキュリティ対策が必要となる。

  総務省は、IoT 機器の利用者等が安全なセキュリティ設定を行えるように、IoT 機器の設計段階において、ID、パスワード等の設定仕様を盛り込むセキュリティ・バイ・デザインの意識啓発や支援を進めるとともに、セキュリティ・バイ・デザインの考え方を踏まえて設計された IoT 機器に認証マークを付与することで、IoT 機器の利用を推進する取り組みを検討している※66。

  これを踏まえ、IoT 推進コンソーシアムの IoT セキュリティ WG は、2018 年 7 月、「IoT 機器のセキュリティ対策に関する検討の方向性※67」を取りまとめた。

- IoT セキュアゲートウェイの実証実験の実施

  総務省は、IoT システム・サービス全体のセキュリティを確保する観点から、IoT 機器とインターネットの境界上にセキュアゲートウェイを設置する取り組みを推進しており、2017 年 12 月以降、カーモビリティ、スマートホーム、教育の 3 分野において、IoT セキュアゲートウェイの設置により、セキュリティ上の脅威に対して認証、検知、対処の一連のセキュリティ対策が実現できるかの実証実験を実施してきた※68。

  実証実験の結果、認証・検知・対処の機能を提供できていることが明らかになったが、一部の IoT サービスでは、電波が届かない場所で通信が途絶えた場合に誤検知が発生する等、運用上の課題も明らかになった。

- 重要 IoT 機器に係る脆弱性調査の実施

  総務省は、2017 年 9 月から、一般社団法人 ICT-ISAC（以下、ICT-ISAC）、国立大学法人横浜国立大学等と連携し、サイバー攻撃観測網やネットワークスキャンを活用することで、IPv4 のグローバル IP アドレスで接続された IoT 機器の脆弱性の調査を実施し、脆弱な IoT 機器の所有者等に対して注意喚起を行う取り組みを推進してきた※69。

  2018 年 7 月、総務省は、本調査により検出した脆弱な重要 IoT 機器は 150 件であり、そのうち実際の利用者等と連絡が取れた 36 件について注意喚起を行ったと発表した。この 36 件の脆弱性の内訳は、パスワード設定が適切になされていないものが 27 件、パスワードは設定されているが、認証画面がインターネット上で公開されていたものが 9 件であった※70。

- 国立研究開発法人情報通信研究機構による IoT 機器の調査の実施

  IoT 機器に対するサイバー攻撃の脅威等に対応するため、2018 年 5 月、「国立研究開発法人情報通信研究機構法」及び「電気通信事業法」が改正された※71。同改正により、国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology：NICT）の業務に、パスワード設定等に不備のある IoT 機器の調査等が追加された。この法律により、同調査等は不正アクセス禁止法の不正アクセス行為から除外される。同業務は 5 年間の時限措置である。

  また、電気通信事業法の改正により、電気通信事業者は、第三者機関を通じて、NICT が行った上記 IoT 機器の調査結果（サイバー攻撃の送信元情報等）を共有することが可能になり、通信事業者が異なっていても、IoT 機器の攻撃通信のブロックや、利用者等に注意喚起を行うことができるようになった。

  以上の法整備を経て、NICT は、パスワード設定等に不備のある IoT 機器の調査の事前調査として、2018 年 11 月から 2019 年 1 月までの間、日本国内の IPv4 アドレスを対象としてポートスキャンを実施し、ポートの開放状態のアドレス数の規模等の調査を実施した※72。

  そして、2019 年 2 月 20 日、NICT は、パスワード設定等に不備のある IoT 機器を調査し、電気通信事業者を通じて利用者等へ注意喚起を行うプロジェクト「NOTICE※73」を開始した※74。今後、NICT が行った調査結果は、改正電気通信事業法が定める第三者機関を通じてインターネットサービスプロバイダ（Internet Service Provider：ISP）に提供される。ISP は、提供されたデータを基に、該当する IoT 機器の利用者等に直接注意を呼びかけることになる。

(b)研究開発の推進の状況

「IoT セキュリティ総合対策」に基づく研究開発の推進状況を述べる。

- 広域ネットワークスキャンの軽量化への取り組み

  脆弱な IoT 機器のセキュリティ対策のために、効率的な広域的ネットワークスキャンを実現する必要がある。そのため、総務省は、2018 年度から、周波数

有効利用のための IoT ワイヤレス効率広域ネットワークスキャン技術の研究開発に取り組んでいる。

- AI を活用したサイバー攻撃の検知・解析技術の研究開発

  NICT では、高度化するサイバー攻撃に対応するため、機械学習を始めとする AI を活用したサイバーセキュリティの研究開発に取り組んでいる。具体的には、ウイルスに感染した端末の IP アドレスや C&C サーバとの通信に関する情報等を収集してデータベース化したデータセットを用いて、攻撃パターン分析等を機械学習により自動化する研究開発等を行っている。

(c) 民間企業等におけるセキュリティ対策の促進

民間企業等におけるセキュリティ対策を促進するための主な取り組みの進捗状況を述べる。

- 「情報開示分科会報告書」の公表

  巧妙化するサイバー攻撃に対する対策強化を進めるためには、企業が自社のセキュリティ対策情報を社内で把握するとともに、関係企業や社会全体との間で適切に共有できる環境の整備が必要である。

  そのため、2017 年 12 月、サイバーセキュリティタスクフォースのもとに「情報開示分科会」が設置され、民間企業のセキュリティ対策の情報開示に関する課題や普及の方策について検討が行われてきた。2018 年 6 月、その結果を取りまとめた「情報開示分科会報告書※75」が公表された。

  同報告書では、セキュリティ対策情報の開示について「社内の情報共有」「契約者間等の情報開示」「社会に対する情報開示」の三つの側面に分け、各側面において、企業に求められる取り組みを整理している。まず、「社内の情報共有」では、経営層のセキュリティ対策への理解促進の必要性があることから、経営層と自社のセキュリティ部署とをつなぐ橋渡し人材育成が必要だとしている。次に、「契約者間等の情報開示」では、サプライチェーンまたはグループ全体における情報共有体制の構築が必要だとしている。そして、「社会に対する情報開示」では、事業規模に応じて「情報セキュリティ報告書」の作成等、段階的に対策を講じていくことが必要だとしている。

  総務省では、これらの検討を踏まえ、第三者への開示の促進に向けた「セキュリティ対策情報開示の手引き（仮称）」の策定・公表を予定している※76。

- 「脅威情報の情報共有基盤　利用ガイドライン」の策定

  サイバー攻撃に迅速に対応して被害を最小化するためには、事業者間でサイバー攻撃に関する脅威情報を共有する仕組みを構築する必要がある。そのため、総務省では、ICT-ISAC を中心に、脅威情報の収集・分析・配布を行う情報共有基盤を運用する実証事業を行った※77。この実証事業は、サイバー攻撃に関する情報提供、情報利用者への脅威情報の配布等に、脅威情報構造化記述の標準形式 STIX※78 と検知指標情報自動交換手順 TAXII※79 を使用し、脅威情報の収集・分析・配布の自動化を目指すものである※80。また、上記実証事業の成果を基に、ICT-ISAC では、2018 年 6 月、脅威情報の情報共有基盤の利用方法等をまとめた「脅威情報の情報共有基盤　利用ガイドライン※81」を公表した。

(d) 人材育成の強化

総務省は、セキュリティ人材育成のため、NICT を通じて、体験型の「実践的サイバー防衛演習『CYDER』（Cyber Defense Exercise with Recurrence）」を実施している。2018 年度からは、これまで設置していた国の行政機関等向けコース、地方公共団体向けコースに加えて、重要社会基盤事業者等の情報システム担当者を対象とした重要インフラ事業者向けのコースを新設した※82。

また、サイバー演習の運営コスト削減と受講者のプロファイルに合わせた効果的な演習プログラムの提供を行うためにサイバー演習自動化システム（CYDERANGE）を開発し、2018 年 4 月から運用を開始した※83。

更に NICT では、東京 2020 オリンピック・パラリンピック競技大会の適切な運営に向け、大会組織委員会のセキュリティ関係者が、大会開催時を想定した模擬環境で、サイバー攻撃・防御双方の実践的な演習を行う「CYBER COLOSSEO」事業を実施している。2018 年からは、演習効果をより高めるために、実践的な演習だけでなく、大会のセキュリティ対応強化に必要な知識の習得を目的とした「コロッセオカレッジ」を新設した※84。

(2) その他の取り組み

総務省のその他の取り組みについて述べる。

(a)「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」の公表

総務省は、クラウドサービスの利用が拡大し、社会経済活動を支える重要な ICT 基盤となっていることから、2018 年 7 月、クラウド事業者がクラウドサービスを提供する際に実施すべき情報セキュリティ対策をまとめた「ク

ラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）[※85]」を策定・公表した。同ガイドラインは、これまで公表していた「クラウドサービス提供における情報セキュリティ対策ガイドライン」（2014 年 4 月策定）と「ASP・SaaS における情報セキュリティ対策ガイドライン」（2008 年 1 月策定）を統合したものである。自組織だけでなく、外部組織との連携を考慮したサプライチェーンにおけるセキュリティ対策をまとめているほか、クラウド事業者が IoT サービスに参入する際のリスク対応方針を整理している[※86]。

(b)「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」「地方公共団体における情報セキュリティ監査に関するガイドライン」の改定

総務省は、2018 年 9 月、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考になるように、情報セキュリティポリシーの考え方や内容について解説した「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[※87]」及び「地方公共団体における情報セキュリティ監査に関するガイドライン[※88]」を改定した。

改定版では、地方自治体の情報セキュリティ対策の強化を目的として、特にマイナンバー利用事務処理においては、原則、端末への多要素認証の導入により個人情報の流出防止策を講じるべきこと、CSIRT（Computer Security Incident Response Team）を設置し、その役割を明確化すべきこと等が規定されている。

(c)「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第三次とりまとめ」の公表

総務省は、電気通信事業者が、巧妙化するサイバー攻撃に対し、通信の秘密等に配慮しつつ適切に対処できるようにするため、2013 年 11 月から、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を開催し、対応すべき課題とその解決の方向性をまとめてきた。

総務省はまた、IoT 機器を悪用した DDoS（Distributed Denial of Service）攻撃の発生等の環境変化を踏まえ、2018 年 9 月、電気通信事業者が、より能動的にサイバー攻撃に対処できる取り組みの実施に向けて条件や留意点等を整理した「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第三次とりまとめ[※89]」を公表した。

同とりまとめでは、ISP 等の電気通信事業者が、ウイルスに感染している可能性の高い端末を検知し、同端末利用者に注意喚起等を行う目的で、IP アドレス等の情報から通信当事者を把握する行為等、通信の秘密の侵害に該当し得る行為について、どのような場合に違法性がないと認められるかを検討し、留意点を記載している。

(d)プラットフォームサービスにおけるデータ保護の検討

総務省は、ISP 等が大量の利用者情報を活用してサービスを提供している状況を踏まえ、利用者情報の適切な取り扱いについて検討を行うため、2018 年 10 月、「プラットフォームサービスに関する研究会」を開催した[※90]。また 2019 年 1 月、「トラストサービス検討ワーキンググループ」を開催し、プラットフォームサービスの信頼の基盤となる人・モノの ID、認証、電子署名、データの完全性等の正しさを担保するトラストサービスの制度化について、検討を開始した[※91]。

欧州連合（European Union：EU）では、2016 年 7 月に発効した eIDAS（electronic Identification and Trust Services）規則において、電子署名、タイムスタンプ、Web サイト認証、e シール（文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの）、e デリバリー（データの送受信の証明も含め、データの送信の取り扱いに関する証拠を提供するもの）等を「トラストサービス」と呼んで包括的に規定している[※92]。しかし、日本では、EU の eIDAS 規則に相当するトラストサービスを包括的に規定した法令は存在せず[※93]、例えば、タイムスタンプについては、国税関係帳簿書類であれば電子帳簿保存法に基づいてタイムスタンプが利用され[※94]、電子カルテや検査データ等の医療情報であれば、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に基づいてタイムスタンプが利用されている[※95]等、運用基準が統一されていない。今後、サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する Society 5.0 に向けて、国際的なデータ流通が加速することが予想される。国際的なデータ流通における相互運用性の確保等の観点から、法制度に基づく、電子署名やタイムスタンプ等のトラストサービスの構築が期待されている[※92]。

2.1.4 警察によるサイバー犯罪対策

警察は、これまで、2015 年 9 月に策定した「サイバー

セキュリティ重点施策」に基づき、サイバー空間の脅威に対する取り組みを推進してきた※96。

近年、インターネットに接続された家電等のいわゆるIoT機器の急速な普及等により、国民生活とサイバー空間は一層、密接な関連を持つこととなった。その一方で、2016年10月以降、IoT機器を狙った「Mirai」と呼ばれるウイルスやその亜種に感染した家庭用ルータやネットワークカメラ等で構築されたボットネットにより企業がDDoS攻撃を受ける等※97、サイバー空間における脅威は一層深刻化しており、サイバーセキュリティ対策は国民生活レベルで喫緊の課題となっている※98。

日本政府は、2018年7月、自由、公正かつ安全なサイバー空間を創出・発展させ、国民が安全に安心して暮らせる社会の実現等を目的として、サイバーセキュリティ基本法に基づき次期サイバーセキュリティ戦略を閣議決定した※99。警察庁においても、同戦略を踏まえ、2018年9月、「サイバーセキュリティ重点施策」を改定し、サイバー空間の脅威への対処に関する取り組みを一層推進することとした※100。

(1) 警察における主な取り組み

前述の「サイバーセキュリティ重点施策」は、「サイバー空間の脅威への対応の強化」「警察における組織基盤の更なる強化」及び「国際連携及び産学官連携の推進」を主な柱としている。この新たな戦略を踏まえ、2018年度の警察におけるサイバー犯罪対策に向けた主な取り組みについて述べる。

(a) サイバー空間の脅威への対応の強化

警察では、高度な情報技術が悪用された犯罪や組織的なサイバー犯罪の捜査を積極的に推進するとともに、脅威情報等の収集・分析を推進し、また、インターネット上の違法情報の積極的な取り締り等を行っている。

警察庁に設置されたサイバーフォースセンターでは、サイバー空間における脅威情報の収集・分析を推進するため、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時間体制で行い、サイバー攻撃の予兆、実態把握、不正プログラムの分析等を推進している※101。その観測において、2016年下半期以降減少傾向にあったサイバー空間における探索行為が、2018年上半期は増加傾向にあることが判明した。警察庁は、探索行為が再び増加した主な要因について、探索・攻撃の標的が多様化し、IoT機器等に拡大したことにあると推察している。また、増加した探索行為の特徴としては、Miraiボットからと見られるTCPの80番ポートに対するアクセス、Microsoft Windowsの脆弱性を標的としたTCPの445番ポートに対するアクセスがある※102。そのため、警察庁は、2018年6月、セキュリティ情報サイト「@Police」において、「宛先ポート80/TCPに対するMiraiボットの特徴を有するアクセスの増加について」と題する注意喚起を行った※103。

更に、警察は、サイバーパトロール等により違法情報・有害情報の収集に努めるとともに、一般社団法人セーファーインターネット協会（Safer Internet Association：SIA）が運営するインターネット・ホットラインセンター※104に対し、一般のインターネット利用者からの違法情報や有害情報に関する通報の受理業務、プロバイダに対する違法・有害サイトの削除依頼業務を委託し、インターネット上の違法・有害情報の削除を進めている※105。また、同センターが受理した違法情報等を基に、サイト管理者等の積極的な取り締りを推進している※100。

(b) 警察における組織基盤の更なる強化

警視庁サイバーセキュリティ対策本部は、2018年4月、これまで公安部や刑事部、生活安全部等6部署に分散していたサイバー犯罪の捜査員等を集め、サイバー犯罪等に対処する部署を新拠点に集約した。警視庁では、拠点の集約に伴い、部署横断型チームとして、ウイルス感染等の同時多発事案の初動捜査を行う「事案対処チーム（CAT）」、専門知識を有するサイバー犯罪捜査官が重要案件の捜査にあたる「サイバー犯罪捜査官チーム（C-SAT）」、通信記録等の証拠品を解析する「解析支援チーム（DFT）」を編成した※106。

また、新たな技術の活用及び研究開発推進のため、AI等の活用の検討、ダークウェブ※107の実態調査※108、ダークウェブにおける情報収集技術調査を実施し、収集手法の確立、効率的な不正プログラム解析手法の開発等を推進している。2018年6月、京都府警察は、ダークウェブ上に児童ポルノサイトを開設したとして、青森県内の男性を児童買春・ポルノ禁止法違反の疑いで逮捕している※109。

(c) 国際連携及び産学官連携の推進

警察は、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）等と連携し、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取り締り等に活用している。

例えば、愛知県警察は、JC3と共同開発したツール

を活用する等により詐欺サイトを発見し、詐欺サイトのURL情報を、米国に拠点を置くフィッシング詐欺対策業界団体Anti-Phishing Working Group（APWG）等に提供している※110。

(d) 仮想通貨（暗号資産）を狙った犯罪の対策等

2018年上半期には、仮想通貨交換業者への不正アクセス等による不正送金事案が多発し、同期だけでも被害額は約605億300万円に上った。警察庁は対策として、金融庁に対し、当該事案認知状況等に関する情報提供を行い、仮想通貨交換業者に対する指導等への金融庁の協力、支援を確認した※110。

また、2018年6月、警察庁は、Webサイト閲覧者等に明示することなく仮想通貨を採掘するプログラムをWebサイトに設置した場合、犯罪になる可能性がある旨の注意喚起を行った※111。

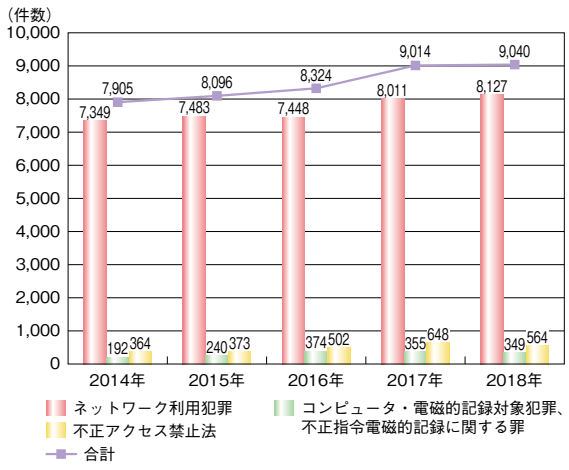
(2) サイバー犯罪の検挙件数等

2018年におけるサイバー犯罪の検挙件数、主な検挙事例について述べる。

(a) 2018年のサイバー犯罪の情勢、検挙件数

警察庁によれば、サイバー犯罪の検挙件数は増加傾向にあり、2018年の検挙件数は9,040件と過去最多であった※112（図2-1-6）。その中で、不正アクセス禁止法違反の検挙件数は564件、不正指令電磁的記録に関する罪の検挙件数は68件であり、いずれも過去5年間では2017年に次ぐ検挙件数であった。

不正アクセス禁止法違反事案では、アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号



■図2-1-6　サイバー犯罪検挙件数推移
（出典）警察庁「平成30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が作成

（ID・パスワード等）を入力して不正に利用する識別符号窃用型の犯罪の検挙が最多の502件を占めた。また、仮想通貨交換業者等への不正アクセス等による不正送信事案は、認知件数169件、被害額は約677億3,820万円相当に上り、2017年の認知件数149件、被害額約6億6,240万円相当を大きく上回った。

なお、2018年におけるインターネットバンキングに係る不正送金事案の発生件数は322件、被害額は約4億6,100万円であり、件数・被害額ともに減少傾向にある。この傾向は、金融機関によるモニタリング強化、ワンタイムパスワードの導入等の対策が効果を上げたものと考えられる。

不正指令電磁的記録に関する罪の手口としては、Webサイトに接続したパソコンに不当な料金請求画面を繰り返し表示させる不正プログラムを使用したもの等がみられた。同罪で補導または検挙された者は、10歳から58歳までと幅広い年齢層にわたっている。

(b) 主なサイバー犯罪の検挙事例

2018年度における、注目すべきサイバー犯罪の検挙事例として、以下の事例を挙げる。

- 2018年7月、警視庁は、取引先等になりすますビジネスメール詐欺で、米国の農業関連会社から約7,800万円を不正に銀行口座へ送金させ、そのうち6,020万円を引き出したとして、東京都内の会社役員の男性ら4人を組織犯罪処罰法違反及び詐欺の疑いで逮捕した（「1.2.2（2）2018年度に報道された事例の概要」参照）※113。
- 2018年7月、愛知県警察等6県警は、アダルト動画サイトに接続したパソコン等に虚偽の料金請求の文言を表示する不正プログラムを使用し、サイトを利用した愛知県内の男性等から現金を騙し取ったとして、東京都内の男性ら11人を、詐欺罪及び不正指令電磁的記録供用罪の疑いで逮捕した※114。
- 2018年10月、奈良県警察は、奈良県の男性職員が、部下である女性職員の机から公用パソコンにログインするためのワンタイムパスワードの表示に必要な機器を盗み、同機器を用いて、同女性職員の公用パソコンのパスワードを初期化した上、不正にログインしたことから、同男性職員を、窃盗罪及び不正アクセス禁止法違反の疑いで逮捕した※115。
- 2019年3月、兵庫県警察は、不正なプログラムに誘導するURLをインターネットの掲示板等に貼り付けたとして、不正指令電磁的記録供用未遂罪の疑いで、

愛知県内の女子中学生、鹿児島県内の男性ら3名の自宅に対する家宅捜索を実施した。不正とされたプログラムは、表示されたポップアップメッセージを消しても再び表示するという挙動を繰り返すものであった。鹿児島県内の男性は、2018年9月に発生した北海道地震を話題にしてインターネットの掲示板に「かなり深刻な事態になってそう」と書き込んだ上、URLへのアクセスを誘導する手口を使っていた※116。

- Webサイト運営者がWebサイトに仮想通貨の採掘（マイニング）プログラムを埋め込んだことを公表せず、サイト閲覧者に無断で、サイト閲覧者のコンピュータでマイニングプログラムを実行させ、採掘した仮想通貨をサイト運営者らが受け取るという事案が発生した。これに対し、全国の10の都道府県警察は、2018年3月から6月までの間に、Webサイトに、仮想通貨を採掘するプログラムである「コインハイブ」を埋め込んで、サイト閲覧者のパソコンのCPUを同意なしに使用して仮想通貨を採掘したとして、不正指令電磁的記録保管罪等の容疑で3人を逮捕、13人を書類送検した※117。

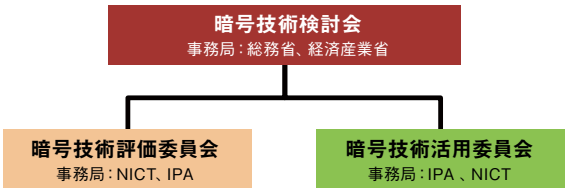
2.1.5 CRYPTRECの動向

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、NICT、及びIPA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※118）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) 2018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2-1-7）。



■図2-1-7　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) 2018年度の主な活動

2018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

2018年度は、各委員会の2018年度活動計画、及び活動報告の審議が行われ、承認された。

また、2022年度に予定されているCRYPTREC暗号リスト改定に向けての検討を開始した。

(b) 暗号技術評価委員会

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ほか、2018年度の主な活動内容・成果は以下のとおりである。

- XTSモードの安全性評価
  ストレージデバイス上のデータ暗号化に主に使用されている暗号利用モード（秘匿モード）であるXTS（Xor encrypt xor（XEX）Tweakable block cipher with ciphertext Stealing）モードについて安全性評

価を実施し、CRYPTREC 暗号リスト（推奨候補暗号リスト）への追加に必要な条件を満たしているかどうかの検討を行った。今後、実装性評価を行った上で、CRYPTREC 暗号リストに追加するかどうかの判断を行う予定である。

- 暗号技術調査ワーキンググループの活動
  2017 年度に引き続いて、「新技術等に関する調査及び評価」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。代表的な耐量子計算機暗号は、格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術の四つに分類される。各分類について、暗号化、署名、鍵交換の三つの機能の観点に基づいて整理を行い、2019 年 4 月に調査報告書[※119]として公開した。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検討を行っている。2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、2018 年度は暗号鍵管理に関するフレームワークの検討、並びにその検討結果に基づく運用ガイドラインとして「暗号鍵管理システム設計指針（基本編）」のドラフト版作成に向けた活動を行った。

フレームワークの検討では、暗号鍵管理を考える上でのあるべき構造を四つの構成要素（Guidance, Framework Requirements, Profile Requirements, System Requirements）として整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。この中の Framework Requirements の代表例として、米国の SP800-130[※120] は、あらゆる利用ケースにおける暗号鍵管理システムを構築する上で必要な検討項目を網羅的にカバーしている。しかしながら、日本では、SP800-130 と同じような包括的・統一的な暗号鍵管理に関する運用ガイドラインが作られていないため、「暗号鍵管理」の在り方や考え方が十分に解説されてこなかった。その点を踏まえ、イントロダクションとして暗号鍵管理の在り方や考え方を解説し、技術的には SP800-130 の理解を深める解説書・利用手引きとして活用するために、「暗号鍵管理システム設計指針（基本編）」の作成を開始した。具体的には、SP800-130 の日本語訳を作成するとともに、それに記載されている Framework Requirements を「暗号鍵管理における目的」に応じた対象範囲に分類・グループ化することによって、検討項目の目的や必要性を明確化し、分かりやすく表現することを目指している。2019 年度夏ごろに「暗号鍵管理システム設計指針（基本編）」のドラフト版、2019 年度末に完成版を公開する予定である。

COLUMN

サイバーセキュリティ目的のリバースエンジニアリングについて ～改正著作権法～

2019年1月1日、2018年改正の著作権法（以下、改正著作権法）が施行されました。この改正著作権法によって、基本的には、サイバーセキュリティ目的のリバースエンジニアリングは著作権法上、認められたと解釈することができるようになりました。

改正著作権法の施行以前は、権利者の許諾なく、サイバーセキュリティ目的でリバースエンジニアリングを行うことが著作権法に抵触するかという問題が議論されてきました。

しかし、改正著作権法では、第30条の4において、技術の開発等のための試験の用に供する場合や情報解析の用に供する場合、人の知覚による認識を伴うことなく電子計算機による情報処理の過程における利用等に供する場合その他の当該著作物に表現された思想または感情を自ら享受しまたは他人に享受させることを目的としない場合の著作物の利用については、必要と認められる限度において、権利制限の対象とすることが定められました（非享受目的の著作物の利用）。これは、著作物に表現された思想または感情の享受を目的としない行為については、著作権法が保護しようとした著作権者の対価回収の機会を損なうものではなく、著作権者の利益を通常害するものではないと評価できるためです 。

そして、サイバーセキュリティ目的のリバースエンジニアリングについては、プログラムの実行等によってその機能を享受することに向けられた利用行為ではないと評価でき、「著作物の表現された思想又は感情の享受を目的としない場合」に該当すると考えられることから、改正著作権法30条の4により、権利者の許諾なく行うことができるようになったものと考えられています[i、ii、iii]。

もっとも、改正著作権法は、第30条の4の本文但書において、「当該著作物の種類及び用途並びに当該利用の態様に照らし著作権者の利益を不当に害することとなる場合は、この限りではない。」と規定しています。著作権者の利益を不当に害するか否かについては、著作権者の著作物の利用市場と衝突するか、あるいは将来における著作物の潜在的販路を阻害するかという観点から判断されることとされており、注意が必要です。典型的な例としては、もともと情報解析を行う者に提供するために作成されたデータベースを、著作権者に無断で解析を行うために複製する行為が、著作権者の利益を不当に害する行為として挙げられています[iii]。

なお、リバースエンジニアリングを禁じるライセンス契約の有効性については、改正著作権法上、明らかにされていません。

i　文化庁：著作権法の一部を改正する法律（平成30年改正）について（解説）　http://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_11.pdf〔参照 2019-06-21〕
ii　文化庁：著作権法の一部を改正する法律案　概要説明資料　https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai4/siryou6.pdf〔参照 2019-06-21〕
iii　「第196回国会　文部科学委員会第5号（平成30年4月6日）」（http://www.shugiin.go.jp/Internet/itdb_kaigiroku.nsf/html/kaigiroku/009619620180406005.htm〔参照 2019-06-21〕）における中岡政府委員の回答。

2.2 国外の情報セキュリティ政策の状況

サイバー脅威・サイバー犯罪は国境を問わず、あらゆる国・地域の脆弱性を突き、ターゲットに攻撃を仕掛けてくる。また、IT 化した社会基盤やそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた他国へのサイバー脅威が現実になりつつある。こうした状況に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。

2.2.1 国際社会と連携した取り組み

2017 年度に引き続き、日本政府は 2018 年度も米国、欧州、イスラエル、その他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) シャルルボワ・サミット

2018 年 6 月 8 ～ 9 日、G7 シャルルボワ・サミットがカナダ・シャルルボワで開催された※ 121。保護主義の台頭に対する自由・公正な経済秩序の維持に向けた結束が主要議題となり、サイバーセキュリティは大きな話題とならなかった。一方で、サミットとしては初めて人工知能技術がトピックとなり、共同声明に「人工知能の未来のためのシャルルボワ・共通ビジョン」が盛り込まれた※ 122。

同ビジョンでは AI の経済・社会への潜在的なインパクトを認め、各国が AI の研究開発・商業的普及を推進するとともに、そのアプローチは技術的・倫理的・技術中立的になるよう努力し、人材育成に投資すること、またセキュリティ強化、プライバシー・個人データの保護、知的財産権の保護に取り組むことを明記した（AI のセキュリティについては「3.5 AI のトラストとセキュリティ」参照）。更には情報の自由な流通を含む、AI イノベーションのためのオープンで公正な市場環境への支持を明記したが、これは AI の研究・実用化における中国の台頭、強制的な技術移転・データローカライゼーション政策等への警戒感を鮮明にしたものと思われる（「2.2.4 中国の政策」参照）。

(2) 日米のサイバー連携

2018 年 7 月 26 日、第 6 回日米サイバー対話がワシントン D.C. にて開催された※ 123。日本からは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を始め、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、防衛省等の関係者が参加した。米国からは Robert Strayer 国務省次官補代理（サイバー及び国際通信情報政策担当）（Deputy Assistant Secretary for Cyber and International Communications and Information Policy, Department of State）を始め、国家安全保障会議（National Security Council:NSC）、DHS、商務省（Department of Commerce：DoC）、国防総省（Department of Defense：DoD）、連邦捜査局（Federal Bureau of Investigation：FBI）等の関係者が参加した。

両国は 2017 年の第 5 回日米サイバー対話のフォローアップを行い、重要インフラに対するサイバーセキュリティ、防衛面におけるサイバー連携や国際的なサイバーセキュリティに関する情報共有の強化に向け、協力することを確認した。また両国は、国際連合や ASEAN 地域フォーラム（ASEAN Regional Forum）等の多国間会議におけるサイバー上の課題に関し共同歩調をとることを確認した。これは、従来の両国の主張である「オープンで自由な情報流通・利用ができる安全なサイバー空間」を推進する、という立場を再確認したものである。

これに連動して 7 月 27 日、日米韓 3 ヵ国によるサイバーセキュリティに関する専門家会合がワシントン D.C. にて行われた※ 124。日本からは泰松昌樹外務省総合外交政策局サイバー政策室長を始め、日米対話に参加した政府機関のほか JPCERT/CC、IPA が参加した。協議では日米対話と同等な課題に対し共同歩調をとること、更に東京 2020 オリンピック・パラリンピック競技大会に向けたサイバー政策で協力することが確認された。

首脳レベルでは、安倍晋三首相とドナルド・トランプ（Donald John Trump）大統領がニューヨークにて 9 月 23 日に夕食会、26 日に首脳会談※ 125 を行ったが、同年 4 月の首脳会談に引き続き、北朝鮮に対する政策連携と日米間の自由貿易協定（Trade Agreement on Goods：TAG）の議論が中心となり、サイバーセキュリティについての言及はなかった。

一方、防衛面では、2019 年 1 月 16 日、岩屋防衛

大臣と Patrick Shanahan 米国国防長官代行（Acting secretary of Defense）がワシントン D.C. にて会談を行った※126。この会談は前任の James Mattis 氏から交代した直後の Shanahan 長官代行と対北朝鮮政策を始めとする連携を確認する意味が大きいと思われるが、その中で宇宙、サイバー、電磁波等の「新しい領域」の重要性が高まり、同領域の協力を推進することが合意された。今後サイバー防衛面での協力が加速すると思われる。

(3) EU 諸国とのサイバー連携

EU 地域とのサイバー連携の状況について述べる。

(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※127。日本からは大鷹外務省総合外交政策局審議官を始めとする関係機関の代表者が、EU からは 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。

第 4 回日 EU サイバー対話は 2019 年 5 月の時点で開催されていないが、第 3 回で合意された取り組みが継続すると思われる。

(b) フランスとのサイバー協議

2018 年 6 月 12 日、第 4 回日仏サイバー協議が東京にて開催された※128。日本側共同議長は大鷹審議官、フランス側共同議長は David Martinon フランス共和国欧州・外務省デジタル大使（Ambassador for Digital Affairs, Ministry of Europe and Foreign Affairs of the French Republic）が務め、両国の関係政府・産学官連携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政策、オリンピック等の大規模イベントにおけるセキュリティ、民間部門の役割、多国間連携、2019 年度 G7 議長国であるフランス、G20 議長国である日本のデジタル分野における協働等について討議が行われた。また両国は、オープンで自由かつ安全・公正なサイバー空間の維持に向けたコミットメントを再確認し、更に、東京 2020 オリンピック・パラリンピック競技大会、及び 2024 年パリ大会でのサイバーセキュリティ分野における協力を合意した。

(c) 英国とのサイバー協議

2018 年 3 月 16 日、第 4 回日英サイバー協議がロンドンにて開催された※129。日本側共同議長は大鷹審議官、英国側共同議長は 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出席した。協議においては、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あるサイバー活動への対策、能力構築への取り組み強化等が確認された。

2019 年 5 月時点で、第 5 回日英サイバー協議は開催されていないが、第 4 回で合意された取り組みが継続するものと思われる。

首脳レベルでは、2018 年 12 月 1 日、安倍首相と英国のテリーザ・メイ（Theresa May）首相がアルゼンチン・ブエノスアイレスにて会談を行った※130。同会談では、英国の EU 離脱に関する日英の経済関係に加え、自由でオープンなインド洋・太平洋の実現に向けた安全保障面の協力が主要議題になったことが注目される。ただし 2019 年 5 月時点では、日米のようなサイバー防衛に関する連携等は公表されていない。

(d) 欧州との個人データ移転に関する包括合意

2017 年 5 月 30 日に改正個人情報保護法が施行されて以来、個人情報保護委員会は個人データの越境移転に関する包括的な枠組み構築に向け、欧州委員会（European Commission：EC）と協議を続けてきたが、2018 年 7 月 17 日、最終合意がなされた※131。具体的には、相互の越境データについて、個人情報保護委員会が個人情報保護法第 24 条に基づく指定を EU に対して、EC が一般データ保護規則（General Data Protection Regulation：GDPR※132）第 45 条に基づく十分性認定を日本に対して行い、必要な手続きを 2018 年秋に完了することで合意したものである。

実際には認定手続きはやや遅れ、枠組みは 2019 年 1 月 23 日に正式に発効した※133。これにより、日本・EU で事業を行う企業は、個人情報保護法・GDPR の遵守を前提として、個人データの越境移転に関して個別契約を結ぶ必要がなくなった（GDPR の EU における運用については「2.2.3 (1) GDPR の運用状況」参照）。

(4) イスラエルとのサイバー協議

2018 年 11 月 16 日、第 4 回日・イスラエル・サイバー協議がイスラエル・テルアビブにて開催された※134。日本側は、大鷹審議官を始め、関係政府機関の代表者が、イスラエル側は、Yigal Unna 首相府国家サイバー総局

長を筆頭に、国家サイバー総局の各部門、イスラエル国防省から代表者が出席した。協議においては、第3回の討議内容をフォローアップし、サイバー政策や脅威の現状、人材育成・能力構築について議論が行われた。

また総務省は、2018年3月以降実務レベルでイスラエルとの協力検討を進めてきた。同年11月29日、石田真敏総務大臣とYaffa Ben-Ari 駐日イスラエル大使は、総務省とイスラエル・国家サイバー総局の間のサイバーセキュリティに関する覚書に調印した※135。同覚書はサイバーセキュリティ政策に関する情報交換、研究開発、人材育成の3点における協力を明記しており、特にIoT分野での協力が期待される。

(5) ASEANとのサイバー連携

ASEAN地域とのサイバー連携の状況について述べる。

(a) 日・ASEAN サイバーセキュリティ政策会議

NISC、総務省、経済産業省は、2018年10月16～17日、東京にて第11回日・ASEANサイバーセキュリティ政策会議を開催した※136。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。協議では、各国のセキュリティ政策に関する意見交換のほか、サイバーインシデントにおける連携対処演習、重要インフラ防護ワークショップによる事例共有、サイバーセキュリティ分野の人材育成事業・意識啓発の各活動が議論され、次年度の継続実施が確認された。

(b) ASEAN 地域フォーラム

外務省は、ASEAN地域の安全保障環境の向上を目的としたASEAN地域フォーラム（ASEAN Regional Forum：ARF）※137との連携を継続している。2018年4月25～26日、マレーシア・クアラルンプールにてサイバーセキュリティに関する第1回ARF会期間会合が開催された※138。日本からは大鷹審議官が出席し、共同議長を務めた。同会合では、事前に実施された2回の専門家会合を踏まえ、今後取り組むべき信頼醸成措置案や優先分野について議論し、その成果を会期間支援グループ会合で報告することとした。

また2019年1月29日、シンガポール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3回専門家会合が開催された※139。

本会合では、サイバーセキュリティ環境に対する各国・地域の取り組みについて意見交換し、必要な信頼醸成措置について議論が行われた。更に同年3月26日に第4回専門家会合が行われ、それらの討議結果は、同年3月28～29日にシンガポールで開催されたサイバーセキュリティに関する第2回ARF会期間会合※140に報告された。本会合では、具体的な信頼醸成措置案について議論が行われ、その成果を会期間支援グループ会合で報告することが確認された。また、合意された提案に基づく取り組みとして初めて、各国のサイバーセキュリティに関する政策等について情報共有が行われた。

(6) インドとのサイバー連携

2019年2月27日、第3回日インド・サイバー協議が東京にて開催された※141。日本側は大鷹審議官を始め、関係政府機関の代表者が出席した。インド側はUpender Singh Rawat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出席した。

協議では、サイバーセキュリティが国民生活や経済、安全保障を強化するという認識を共有し、2018年の第2回サイバー協議に引き続き、自由で開かれた安全なサイバー空間の実現に取り組むことを再確認した。第2回の共同プレスリリースと比べると、両国の安全保障への言及が加わっており、中国のインド洋進出への警戒が背景にあるものと思われる。

2.2.2 米国の政策

2018年、トランプ政権は中国とイランに対する強硬姿勢を鮮明にし、特に米中経済摩擦の激化は「新冷戦」とも呼ばれる深刻なものになりつつある※142。一方、2018年前半の懸案であった北朝鮮との非核化交渉は、2018年6月、2019年2月に米朝首脳会談が続けて行われたものの、具体的な合意はなされず、停滞が印象付けられた※143。

こうした中で、トランプ政権のサイバーセキュリティ政策はサイバー空間の敵対的行動を監視し、対抗する、という安全保障重視の姿勢がより鮮明になっている。2018年8月13日、トランプ大統領は国防権限法（National Defense Authorization Act）※144に署名し、この中で中国のHuawei Technologies Co., Ltd.（以下、Huawei）、ZTE Corporation等5社の製品を連邦政府が調達することを禁止した※145。更に同年12月5日、Huwaei の Meng Wanzhou CFO（Chief Financial Officer：最高財務責任者）が米国の対イラン貿易制裁に違反した疑いにより、カナダで逮捕された※146。これら

は、中国企業に重要インフラを委ねる安全保障上の懸念に加え、次世代 IT インフラにおける米中の覇権争いの現われ、とする見方もされている※147。

本項では、このような状況下で策定された米国政府のサイバーセキュリティ戦略と政策について述べる。

(1) 新しい国家サイバー戦略

2018 年 9 月、トランプ大統領は国家サイバー戦略（National Cyber Strategy）※148 を発表した。同戦略は 2017 年 12 月に策定された国家安全保障戦略（National Security Strategy to Advance America's Interest's）※149 が示す四つの柱（後述）に基づき、米国に対する敵対的活動への対抗策を示している。敵対的国家として、ロシア、中国、イラン、北朝鮮を名指しし、「これらの国は米国とその同盟者、パートナーに対してサイバー空間でしばしば向う見ずな挑戦をする」「中国はサイバー空間の経済スパイ行為で何兆ドルにも及ぶ知的財産を盗んだ」と非難する等、対決姿勢を前面に出している。また John Bolton 大統領補佐官は、同戦略公表時の記者会見において、「2015 年の米国人事管理局（Office of Personnel Management：OPM）へのサイバー攻撃（2,210 万人の雇用者情報が流出したといわれる）は中国によるもの」と断定した※150。

同戦略には以下の四つの柱が示されている。

- 「国民と国土、米国の生活様式を守る」
- 「米国の繁栄を促進する」
- 「力による平和を維持する」
- 「米国の影響力を増進する」

以下では、この四つの柱について紹介する。

(a)「国民と国土、米国の生活様式を守る」

具体的な優先項目について、以下に要約する。

①政府の情報ネットワークのセキュリティ強化

- 2017 年 5 月発効の大統領令 13800※151 により始まった連邦政府のリスクアセスメントを発展させ、政府機関の個別 IT 環境の共有サービスへの移行を推進し、サイバーセキュリティの統合管理を強化する。
- 2018 年 5 月に発効した大統領令 13833※152 に基づき、各政府機関の最高情報責任者（Chief Information Officer：CIO）が効率的な IT 投資と調達に責任を持ち、米国行政管理予算局（Office of Management and Budget：OMB）と DHS がリスクマネジメントを支援する。
- 政府のサプライチェーンリスク管理を向上させる。対策として、サプライチェーンの脅威に関する情報共有やサプライチェーンリスクアセスメントサービスの提供、リスクのあるベンダや製品の除外等が挙げられている。
- 連邦政府取引事業者のセキュリティを強化する。現在、契約等の仕方について、DoD の調達事業者が懸案となっているが、全連邦政府機関で統一したセキュアな調達戦略の策定を支援していく。
- 革新的な実践を政府が主導する。政府調達や補助金によるセキュリティ規格の民間への展開、標準化に加え、米国国立標準技術研究所（National Institute of Standards and Technology：NIST）を通じて、量子コンピュータによる公開鍵暗号解読等の脅威に対抗する技術開発・標準化を推進する。

②重要インフラのセキュリティ強化

- 重要インフラのリスク管理・インシデント対応に関する政府機関の役割と責任を明確化し、プロアクティブなリスク管理につなげるとともに、政府・非政府のインシデント対応活動や演習等の連携を促進する。
- 企業と連携して重要インフラに対する重大リスクを特定し、ナショナルセキュリティ、エネルギー、金融、医療と安全、通信、IT、交通の 7 領域において対応策を優先度付けする。
- 信頼できる ICT サービスプロバイダと機密情報・脆弱性情報等を共有し、ネットワーク上の敵対的行動に対抗する。また、業界横断のソリューションをステークホルダに検討させ、民間主導の認証制度等の策定を促す。
- 要求に応じ、各州・地方自治体の選挙関連の IT インフラの技術・リスクマネジメントに関して支援を行う。
- 国家重要インフラのセキュリティと頑健化に関する研究開発の優先度を高める。
- 貿易・物流に関するセキュリティを強化する。特に海運のサイバーセキュリティに関する役割と責任、国際協調、情報共有等の課題の明確化に至急取り組む。
- 人工衛星等の宇宙資産について、産業界やパートナー諸国と連携してセキュリティ強化に取り組む。

③サイバー犯罪対策・インシデント報告の強化

- 特に重要インフラに対する侵入やデータ詐取等のインシデント報告を引き続き推進する。
- サイバー犯罪に関する証拠を合法的に収集するための法制の改訂作業を議会とともに行う。

- 多国籍サイバー犯罪集団に対し、司法当局が効率的に捜査・起訴が行える仕組みを持てるように働きかける。
- 海外の犯罪者の身柄を確保し、司法の場に立たせるための仕組みの検討を続ける。また、犯罪者の引き渡しについて必要な外交等の努力を続ける。
- サイバー犯罪対策に関する能力構築について国際協力を推進する。

③の第4項目の海外犯罪者の引き渡しに関しては、今後新たな取り組みが提示されるのかが注目される。

(b)「米国の繁栄を促進する」

具体的な優先項目について、以下に要約する。

①活気ある、頑健なデジタルエコノミーを育成する。

- サイバー空間を頑健化するための革新的なセキュリティ技術・運用を受容し、評価する市場構築に向け、企業・公共団体等のステークホルダとベストプラクティスを作り、よりセキュアな製品・サービスへの需要を喚起する。
- 進化する脅威に対応するために、標準やベストプラクティスを常に新しくする。また、サイバーセキュリティ企業が革新的な機能を開発することを阻む規制を取り除く。
- 5G等の次世代情報通信インフラへの投資を加速するとともに、政府機関の調達を通じ、サプライチェーンセキュリティを強化する。また、民間との連携によりAIや量子コンピューティング等の先進技術を検証し、米国の技術優位を保つ。
- オープンで自由なデータの流通を推進する。保護主義や国家の規制等によるデータの不当なローカライズ化に対抗し、パートナー諸国とともにオープンで産業界主導の標準化・製品化を推進し、グローバルな革新と自由なデータ流通を確保する。
- 米国の最先端技術を詐取から守る。また、通商関連の契約等を通じて米国の革新的なサイバーセキュリティ技術を世界的に普及させる。
- セキュリティ製品のテスト、設定、更新等のライフサイクル全般にわたるセキュリティ施策を推進する。例えば攻撃に対して復旧しやすいシステムの設計、製品・システム開発時の定常的なセキュリティテストを推進していく。

②米国発の創意工夫・知的財産を保護する。

- 米国の情報通信ネットワークへの敵対的国家の侵入・悪用を防ぐために、連邦通信委員会(Federal Communications Commission：FCC)のライセンス事業を見直す。
- グローバルな知的財産保護の仕組みを育成し、敵対的国家が米国の研究開発成果を不正に利用して優位に立つことを防ぐ。
- 海外企業による官民の技術あるいは技術に関する知識の不当な流用を防ぐ。

③高度なサイバー労働力の育成を行う。

- トランプ大統領の移民法改正提案を更に強化し、有能な人材を供給するために投資を続ける。
- 議会と協力してサイバーセキュリティ人材育成の教育訓練プログラムを再整備する。様々なバックグラウンドを持つ人の政府への再雇用、再教育も推進する。
- 政府は優秀なサイバーセキュリティ教育者・専門家の確保を重点的に推進する。同時に、NISTの策定したサイバーセキュリティスキルマップの標準であるNICE(National Initiative for Cybersecurity Education)フレームワーク[※153]を活用し、サイバーセキュリティ業務と人材のギャップ確認、人材育成、維持を実践する。

①では、第5項目が興味深い。サイバーセキュリティは米国のビジネスツールである、と堂々と宣言している。

②では、明らかに中国企業を想定した施策が並ぶ。前述のHuawei等の調達禁止に発展しており、火急の課題とみなされている。

③の第1項目で、不法移民を厳しく制限し、「米国の負荷」にならない移民だけを受け入れる法改正提案(例えば9月21日付のDHS規制[※154])に言及しているが、これらについては、民主党はもちろん、共和党内でも反論があり、紛糾している。

一方、第3項目のNICEフレームワークは、サイバーセキュリティ人材に求められる役割と業務、知識、技術、能力がきめ細かく定義され、米国のセキュリティ求人・求職の参照モデルとなっている。2019年5月2日、トランプ大統領は、連邦政府のサイバーセキュリティ人材のジョブローテーションによる再教育、雇用契約におけるNICEフレームワーク活用等を盛り込んだ大統領令を発表した[※155]。

(c)「力による平和を維持する」

本戦略は、サイバー空間において米国の国益が損なわれる恐れがある場合、それを阻止するために実力を

行使するという宣言である。ただし、中国やロシア・アフリカ諸国等の国家主権の優越の主張とは一線を画し、マルチステークホルダを意識した配慮がみられる。「力による平和を維持する」の具体的な優先項目について、以下に要約する。

①国家の責任ある行動によりサイバー空間を安定させる。

- 国際法に準拠し、強制力を持たないサイバー規範に基づき責任ある行動をとることで、サイバー空間の安定とセキュリティを実現する。この原則をすべての国家が公式に確認し、相互に約束することを推奨する。

②サイバー空間における不正行為の究明と抑止を強化する。

- パートナーとともに、敵対的な国家や悪意のあるサイバー組織の同定・意図・能力・活動等に関する情報収集を客観的に、起訴できる形で行う。
- 悪意のあるサイバー活動を阻止するため、必要に応じて適切な制裁を加える※156。
- 結果の強制（制裁）の効果を高めるため、インテリジェンス情報の共有、行為者の特定、制裁の共同実施等を行う国際連携の提案（Cyber Deterrence Initiative）を行う。
- 非国家組織によるサイバー空間上のプロパガンダ、デマによる混乱、情報操作に対抗する。各国政府、企業・大学・市民と連携し、人権と自由を守りつつ対応する。

①では力の行使において、国際法やパートナーとの信頼構築、等の配慮を見せている。

②について、米国に対する悪意のあるサイバー活動に対しては、外交、軍事（サイバーを含む）、情報、金融、諜報、司法等あらゆる手段でこれを予防・対抗・阻止する、としている。攻撃的なオプションが除外されないことに注意する必要がある。

(d)「米国の影響力を増進する」

オープンで相互運用可能、高信頼で安全なインターネットは米国のサイバー空間に対する基本理念であり、本項でこの主張が繰り返される。ただし、「米国の国益に資する」という断り書きが付けられた。具体的な優先項目について、以下に要約する。

①オープンで相互運用でき、高信頼かつ安全なインターネットの普及推進を行う。

- インターネットの自由を守り、推進する。ここで言う推進は国境を越えた自由な情報流通の保障であり、通商に加え、サイバー犯罪対策・テロ対策等のために必須である。
- 監視に反対し、自由なサイバー空間を尊重する各国、産業界、学会、市民社会と連携する。市民社会が監視のないインターネットにアクセスできるよう努力を続ける。
- マルチステークホルダモデルを推進する。
- 相互運用でき、高信頼な通信インフラ構築を推進する。
- 米国の創意工夫を国際市場に展開する。セキュリティのコスト低減に関する米国の新技術について、海外の市場展開を継続する。

②国際的なサイバー能力開発を行う。

- 同盟者、及びパートナーのサイバー能力開発の支援を継続する。サイバー脅威情報の共有自動化、協調支援、分析や技術情報の共有等を強化し、パートナーと連携してサイバー犯罪・テロ対策のための能力開発を行う。

①の第3項目では、国家主導ではなく、マルチステークホルダが重要である、という従来の主張が繰り返されている。

①の第4項目について、通信インフラへの投資は、グローバルデジタルエコノミーにおける米国企業の優位の確保、及びセキュリティにも重要であることを示している。

①の第5項目は、前述したが、米国のサイバーセキュリティ技術・製品をビジネスツールとし、米国の優位を保つ、という宣言である。

(e)反響

本戦略は2003年以降で最も包括的なものとの評価もあり、メディア・セキュリティ関係者が多数コメントしている※157。戦略の特徴に関しては、以下のような指摘がある。

- 敵対的勢力に攻撃されるばかりだった状況を変え、必要に応じ攻撃オプションをとることを鮮明にした。例えばJohn Bolton大統領補佐官は前述の記者会見で、「我々は守備的にも、攻撃的にも対応する」と述べている※158。
- あらゆる連邦政府調達において、DHSにより調達ベンダのセキュリティが求められるだろう（2017年度はDoDのみがSP800-171遵守を要請していた）。
- 中長期的課題として人材育成に踏み込んだ。また宇宙のサイバーセキュリティを課題に挙げた。

- セキュリティベンダからは、望まれていたパートナーとの攻撃原因究明や市場拡大に対する期待が示された。

ただし、攻撃オプションについては、国家サイバー戦略中で明言されているわけではない。これについては後段の DoD の戦略において検討する。

(2) 連邦政府機関のセキュリティ政策

連邦政府の政策に関しては、2017 年 5 月の大統領令 13800[※151] に基づくセキュリティリスクアセスメントの結果が各省から報告され、具体的な施策検討・実施が開始された。以下ではこのうち、DoD、DHS の施策について述べる。

(a) 国防総省 (DoD) の戦略

2018 年 9 月、政府の国家サイバー戦略と同期するように、DoD は自身のサイバー戦略（Department of Defense Cyber Strategy 2018。以下、サイバー戦略）を公表した[※159]。サイバー戦略は米国統合軍（Joint Force）のサイバー戦力強化、重要インフラの防御、DoD の IT インフラ防御等を目的とし、国家サイバー戦略と自身の国防戦略に沿って体系化されている。軍事力増強の著しい中国とサイバー情報操作による国政介入が懸念されるロシアに対抗するため、以下の五つの施策が述べられている[※160]。

- 強力な統合軍の構築。サイバー能力構築、脅威の進化に対抗する革新のアジリティ、分析の自動化、既製品の活用、を重点項目としている。
- サイバー空間における戦闘力強化。悪意のあるサイバー活動の抑止、前進防御 (defend forward) の考え方に基づく日常のサイバー脅威対策（民間、他国との連携を含む）、重要インフラの頑健性向上、を重点項目としている。
- 同盟の強化とパートナーシップ拡大。企業との信頼構築、国際パートナーシップの強化、責任ある国家のサイバー活動に関する規範の強化、を重点項目としている。ほぼ国家サイバー戦略を踏襲している。
- DoD の意識改革。サイバーに対する省内の意識づけ、サイバーセキュリティに関する説明の充実、入手容易で柔軟・頑健な IT 調達、脆弱性情報収集の外部クラウドソース活用、を重点項目としている。
- 人材育成。サイバー労働力維持への投資、国家の人材育成への支援、DoD のコンピテンシーとしてのソフト・ハード専門性の維持、トップ人材育成プログラムの構築、を重点項目としている。

(b) 国土安全保障省 (DHS) の戦略

2018 年 5 月 15 日、DHS は今後 5 年間の自身のサイバーセキュリティ戦略を発表した[※161]。同戦略は DoD のような敵対的国家を想定せず、以下の五つの柱について戦略が示されている。

- 常に進化するサイバーリスクを評価し、リスク管理の優先度を決め、DHS の施策に反映する。
- 政府機関のシステムの脆弱性を削減、一定のセキュリティレベルに保つ。また重要インフラのステークホルダと連携、情報を共有してリスクに対処する。
- 司法等と連携し、グローバルな金融犯罪等の不正行為、重要人物・システム・イベントへの攻撃を阻止する。司法のサイバー捜査・フォレンジック能力向上を支援する。
- インシデント報告、通知、技術支援等により効果的なインシデント対応を実現、被害を軽減させる。インシデント対応者との協調を支援する。
- 技術、規格、運用、人材等を育成し、ネットワークエコシステム（サプライチェーン）の頑健性を高める。海外パートナーとの連携、高度な専門家の育成等で能力構築に努める。更に、DHS 自体のサイバーセキュリティ活動のマネジメントを向上させる。

(c) 戦略の分析

DoD、DHS の戦略は、国家サイバー戦略と比較して特に目新しい点はないが、進化する脅威への対応、パートナー（サプライチェーン）連携や情報共有、人材育成、2020 年の大統領選挙への攻撃警戒、等は両者に共通している。互いに相手との連携を明言している点は興味深い。今後数年の米国のセキュリティ政策の指針になると考えられる。

DoD の戦略に関しては、米国サイバー軍の Paul Nakasone 司令官がインタビューにおいて「物理的な戦闘と同様に、サイバーにおいても境界を越え、敵のサイバー空間に出て防御しなければならない（defend forward）」「敵との戦いは常に持続している。常に革新が必要である」と答えている[※162]。ここで Defend forward は攻撃ともとれるが、明言はされていない。むしろ全体の文脈から見て、インテリジェンス（諜報活動）や国際連携による抑止策が中心ではないかとも考えられる。一方、「常に革新が必要」との発言については、セキュリティ専門家から、サイバー軍拡競争、あるいはサイバー戦闘力の急拡散、等の懸念が示されている[※163]。トランプ政権、DoD の今後の施策が注目される。

DHSの戦略については、重要インフラ防御政策に関連して2018年11月、トランプ大統領がCybersecurity and Infrastructure Security Agency Actに署名した。これは、DHS傘下でサイバーセキュリティと重要インフラの防御を担当していたNational Protection and Programs Directorate（NPPD）をより戦略的な組織に格上げし、Cybersecurity and Infrastructure Security Agency（CISA）※164として改組したもので、DHS副補佐官のChristopher Krebs氏が長官を務める※165。2018年7月のDHSの呼びかけによる官民連携のICT Supply Chain Risk Management Task Forceは、CISAのもとでサプライチェーンリスク管理の検討を続けている※166が、CISAの調整力は未知数であり、今後が注目される。

なお2019年4月7日、DHSのKirstjen Nielsen長官が辞任した※167。トランプ政権の不法移民に対する「ゼロ寛容政策」への批判の矢面に立った格好で、現在米国税関・国境警備局長のKevin McAleenan氏が代行を務めている。サイバーセキュリティ政策への影響はあまりないと思われるが、移民政策に関してDHSは難しい舵取りを迫られる可能性がある。

2.2.3 欧州の政策

欧州では2018年5月25日、GDPRが発効した。実際の運用が注目される中、2019年1月、フランスの「情報処理と自由に関する国家委員会」（Commission Nationale de l'informatique et des Libertés：CNIL）がGoogle LLC（以下、Google）のGDPR違反を認定、5,000万ユーロ（約62億円）の制裁金を科した※168。

また、重要インフラ向けのセキュリティ対策規範であるNIS指令（Network Information Security Directive）※169は、2018年度中の加盟国の国内法整備が完了し、本格的な施行が開始された。更に、EUの統合的なサイバーセキュリティ対策強化に向けたEUサイバーセキュリティ法案（EU Cybersecurity Act）※170が2019年3月に承認される等、一連の施策が整備されつつある。本項ではこれらの進展状況について述べる。

(1) GDPRの運用状況

GDPRの運用については、施行以前からグローバルサービスプロバイダへの厳しい対応が予想されていたが、運用直後から提訴が相次いだ。例えば2018年5月25日のGDPR発効当日、非営利団体noybがGoogle、Facebook, Inc.（以下、Facebook）、Instagram、WhatsApp Inc.による「十分な説明がないままの同意の強制」等がGDPR違反であるとし、企業ごとに異なる国の監視当局に対して提訴した※171。更に同年9月12日、英国の複数の個人が、Googleと複数の広告会社によるターゲティング広告における個人情報の処理がGDPR違反であるとする訴えを英国、アイルランドの監視当局（Information Commissioner's Office：ICO）に起こした※172。これに対してGoogleは即座に反論したが、noybの提訴先となったCNILは前述のとおり違反を認定し、初のグローバルサービスプロバイダへの制裁となった。

個人情報保護団体はCNILの認定を歓迎したが、Googleは対応方針を明言していない。制裁金額自体が大きな痛手とはならなくても、このような訴えが今後も続き、制裁が厳密に行われるとなれば、Googleのようなサービスプロバイダは広告モデルの転換を迫られる可能性もあると言われる。一方で、GDPRの条文には「正当な利益のために収集データを利用する」等のあいまいな点が残り、法的な争点になる、とも言われている※173。今後もグローバルなサービスプロバイダに対するGDPR違反の提訴が起こり、その都度、前述の「グレーゾーン」に関する監視当局の解釈が具体化していくものと思われる。

なおGDPR発効以前の事案となるが、2007年から2014年までの間、アドインアプリケーションの不適切な運用により個人情報を流出させたとして、2018年10月25日、英国のICOはFacebookに50万ポンド（約7,400万円）の制裁金を科した※174。GDPR発効以前の最高額とはなるが、事案の被害規模（8,700万人に影響）や、米国大統領選挙に向けた世論誘導等の影響の深刻さから見ると、小さいものであった。しかしFacebookは2018年10月、サイバー攻撃により2,900万人の個人情報が漏えいした恐れがあると発表※175する等、漏えい事案が相次いで報じられ、新たな提訴を受ける恐れがある。また欧州だけでなく米国、カナダでもデータの不適切な扱いについて提訴・捜査が続いており※176、厳しい対応を迫られている。

一方、EU域内の事業者に対する運用では、監視当局は企業の準備不足等を考慮し、猶予期間を設けるものと想定されていた。例えばドイツでは、ほとんどの監視当局が当初の違反に寛大な対応をしたという※177。ドイツにおいて、2019年4月までの制裁金事案は41件で、最大の制裁金は、健康管理データのセキュリティ対策不備による露出事案に科された8万ユーロ（約990万円）であった。また、GDPR発効後、データ主体（個人情

報提供者）のデータ保護に対する意識は明らかに高まったとしている。この意識の高まりは各国共通で、実際、ベルギーでは自治体の違反行為に対して2,000ユーロ（約245万円）の制裁金が課されたが、これは目的外（選挙活動）の個人データ利用に関する苦情申し立てによるものであった※178。

EU離脱（Brexit）を控えた英国においてもGDPRの運用が始まっているが、Brexitが実施されると、英国はGDPRから見て第三国となり、EU諸国との自由な個人情報等の移転ができなくなる。このため英国は、GDPRと同等なデータ保護を提供し、GDPR第45条による十分性認定を受けるための包括合意を行う必要がある。Brexitの時期については、2019年5月、英国とEU首脳が同年10月31日に再延期することで合意し※179、「EUとの合意なき離脱」をかろうじて回避したが、包括合意に向けた交渉は5月末の時点で始まっておらず、10月31日には間に合わないと想定される※180。しかし、5月24日にメイ首相が退任を表明する※181等、英国の内政は混迷し、離脱の道筋は見えていない。Brexitの早急な決着は英国に加え、自身の改革を迫られるEUも望んでいるとされるが、準備が整わないままの離脱は双方のビジネス、ひいてはグローバルビジネスに混乱を招くことが懸念される。今後の英国、EUの交渉が注目される。

なお、データ移転に関する枠組みについては、日本もEUと協議を継続してきたが、2019年1月23日、包括合意が発効した※182（「2.2.1（3）EU諸国とのサイバー連携」参照）。これにより、日本・EU間の個人情報を含むデータの越境移転がスムーズに行われることになる。日本企業にとってもビジネス拡大のメリットがある反面、監視当局の猶予も今後なくなることから、前述の「グレーゾーン」や監視当局の認定事例に配慮しつつ、GDPRへの対応を強化する必要がある。

（2）ePrivacyに関する規則改正の状況

2017年10月1日、ECは電気通信におけるプライバシー保護規則であるePrivacy Regulation（ePR）※183を提案した。これは2002年に施行され、主に電話を対象としていたPrivacy and Electronic Communications Directiveを大幅に改訂した上で規則化するもので、GDPRの特定領域（電子通信）における実施規則（lex specialis：特別法※184）という位置付けとなる。具体的にはメール・Cookieを扱う事業者が規制対象となり、アプリケーションやインターネット通信における不正な盗聴・傍受・記録を防ぐことが目的とされる。Cookieを始め、ユーザ情報の取得に対し、ユーザの能動的な同意が必要である（「同意しないとサービスが受けられない」等は同意の強制とみなされる）。プライバシーに配慮した設計（Privacy by Design）も求められる。またEU域外にあっても、EU域内と通信等を行う事業者は規制の対象になり、プライバシー侵害行為にはGDPRと同様な罰則がある。

ePRに対しては、主要ITベンダが構成する非営利団体であるDevelopers Allianceを始め、欧州の広告業界も反対を表明したため、当初2018年5月とされていた同法案の発効は遅延し※185、2019年5月1日時点でも継続審議中である。ただし、成立した場合にはGDPRと同様に日本企業への影響があると考えられ、対応が必要である。

（3）NIS指令の運用状況

2016年に成立したNIS指令はEU加盟国が遵守すべき重要インフラ向けのセキュリティ対策であるが、施行には各国法制度への実装が必要であり、加盟国は2018年5月9日までにこの法整備を完了すること、更に同年11月までにNIS指令の適用対象となるプロバイダを選定することが求められた。各国の整備状況※186を見ると、2019年5月の時点で加盟国28ヵ国のうち、NIS指令に基づく国内法制の置き換え（transposition）、すなわち国内法の改訂等が完了した国が24ヵ国、国家のサイバーセキュリティ戦略が策定できた国が23ヵ国、National CSIRT相当の機関が設置できた国が26ヵ国、等でほぼ実装が終わっている。

各国の体制整備とともに、横断的な連携方策を検討するNIS連携グループ（NIS Cooperation Group）が構成され、EU加盟国、欧州ネットワーク・情報セキュリティー庁（European Network and Information Security Agency：ENISA）、ECが参加している※187。2018年度は、連携の基本的な枠組みが検討され、サイバーセキュリティインシデント用語の定義、重要サービス事業者（Operators of Essential Services：OES）のインシデント通知、デジタルサービス事業者（Digital Service Providers：DSP）のインシデント通知、加盟国間のネットワーク相互依存性に関する情報共有等についてガイドラインが公表されている。また関連して、上記のOESとDSPの相互依存性、あるいは業種間の相互依存性評価についてENISAが検討している※188。この検討は依存性のインパクトに関する評価指標の例示であるが、OT（Operational Technology）事業者、IT事業者、

政府機関の3者が共有できる指標を検討している点で興味深い。

(4) サイバーセキュリティ関連法案・指針の整備状況

冒頭で紹介したサイバーセキュリティ法案、及び5Gネットワークに関する指針について述べる。

(a) サイバーセキュリティ法案の承認

2017年9月にECが提案し、欧州議会(the European Parliament)、理事会(the Council)等で審議されてきたサイバーセキュリティ法案は、2019年3月12日、欧州議会にて正式に承認された(同年5月時点では未施行)。

同法案はENISAを強化し、更にEU域内での統合的なサイバーセキュリティ認証制度を導入することを主眼としている※189。まずENISAについては、これまでは時限付きだった同機関の執行権限(現行法制では2020年に失効)が恒久化される。また現在EU Cybersecurity Agencyと呼ばれているように、EU横断的なセキュリティ対策連携、各国のサイバーセキュリティ対策やインシデント対応の機能構築等の多岐にわたる業務に対してリソースが強化される。前述のNIS指令に関する各国支援に加え、後述するEU域内の統合的なセキュリティ認証制度についても、ENISAがひな型を提供すること、とされている。

EU域内の統合認証フレームワークは、従来Common Criteria(CC)等を活用して国ごとに実施されている製品のセキュリティ認証をEU内の統一規格に置き換え、EUデジタル単一市場(EU Digital Single Market)の実現を加速させる、というものである。特にIoT機器等で国境を越えてつながるバリューチェーンにおいて、機器のセキュリティレベルを同一の認証で担保したい、との意図があると思われる。しかし2018年の法案提出以来、「認証ルールは業界等で異なる」「民間に委ねるべき」等の反対意見が多く出されてきた。提案者であるECはこれに対し、EUレベルで統合認証の合意がなされている特定製品(スマートカード)のルールをベースとした包括的なスキームを作る※190、として法案成立にこぎつけた。上記スキームはENISAが中心となって策定することとなるが、難易度は高いと思われる。どのようなスキームができるか注目される。

(b) 5Gネットワークに関するリスクアセスメント指針

ECは2019年3月26日、EU全域における5Gネットワークのサイバーセキュリティリスク評価指針を発表した※191。同指針では、5GネットワークがEUのグローバルな競争力の鍵であるとし、加盟国は同年6月30日までに国内のリスクアセスメントを実施、7月15日までに欧州議会と理事会に結果を報告する、としている。同アセスメントには、海外のネットワーク調達事業者、運用事業者によるリスクの評価が含まれ、各国法制を遵守しない事業者の排除を求めている。

またEUレベルでは前述のNIS連携グループ(NIS Cooperation Group)が同年10月1日までに統合アセスメントを実施し、必要な対策について合意する、としている。対策はEUサイバーセキュリティ法による施策と整合させ、統一的な機器認証の要求項目、テスト、セキュリティ機能、セキュアでない製品・事業者の特定等が含まれる。

なお、米国は5Gネットワークからの Huawei の除外を欧州に要請しているが、本指針でその判断は加盟国に任されたことになる。このうち英国のメイ首相は同年4月23日、5Gネットワークの調達ベンダとして Huawei を認めるが、中核的な部分から外れる等の制約を課すとした※192。この決断に先立ち、英国の監視機関(Huawei Cyber Security Evaluation Centre:HCSEC)は Huawei のセキュリティ能力に厳しい評価を下していた※193。一方、英国国家サイバーセキュリティセンター(National Cybers Security Centre:NCSC)の Ciaran Martin CEOは、「Huawei がもたらすいかなるリスクも英当局は軽減できる」と自信を見せている※194。Huawei 自身は当然ながら米国の除外要請を不当とし、セキュリティ対策検証のための第3者機関としてHCSECを設ける等、セキュリティについて透明性があると主張している。

ドイツは更に積極的な Huawei 容認の姿勢を示している。ドイツ連邦ネットワーク庁の Jochen Homann 長官はインタビューに対し、「連邦ネットワーク庁は Huawei を含め、どの事業者も排除すべきでない」と述べたという※195。このように、5Gネットワークのサプライチェーンセキュリティについて、米国とEUは共同歩調をとれないことが明らかになりつつある。

2.2.4 中国の政策

2018年は米中経済摩擦が「新冷戦」と呼ばれる程に深刻化した年となった。本項では、貿易摩擦や米国との交渉経緯を交えて中国のセキュリティ関連施策の動向を述べる。

(1) 貿易摩擦と米中の覇権争い

2018 年 7 月、米国関税・国境警備局（US Customs and Border Protection：CBP）が中国製品 818 品目（340 億ドル相当）に対して 25%を課税し、中国は報復措置として米国製品 545 品目（340 億ドル相当）に同率の関税を課した。更に両国は同年 8 月、9 月に追加課税を実施し、その後 2 国間の通商協議が続けられた。

同協議におけるセキュリティに関する議題としては、2017 年 6 月に施行された中华人民共和国网络安全法※196、いわゆる「ネットワーク安全法」の扱いがある。同法により、中国で事業を行う海外企業は、越境データ流通の制限や、中国企業のネットワーク製品採用を事実上強制され、それにより政府の監視が強化される等の懸念から、中国国内にデータセンターを構築する等の個別の対応を迫られている。実際に海外企業の監視を政府が行っているかは不明であるが、先進技術等の不当な国内移転のために同法が転用されるという不安は根強く、米国は 2019 年 3 月 28 ～ 29 日の第 8 回米中通商協議において、同法の廃止を求めた。米国はまた、中国国内への技術移転制約の緩和、クラウド等の重要情報インフラ市場の開放等を迫り、ある程度の譲歩がなされたという※197。

しかし 2019 年 5 月 10 日にワシントンで行われた第 9 回閣僚級協議は、「建設的であった」とトランプ大統領が語ったものの合意に至らず※198、米国は中国製品 2,000 億ドル相当への関税を 10%から 25%に引き上げるとして手続きに入った※199。第 8 回協議で国内法の改正を約束していた中国が大詰めでこれをひっくり返したためとされ、中国の戦略ミスであったとも言われているが詳細は不明である※200。

更に安全保障に関わる問題として、米国政府は Huawei、ZTE Corporation 等の IT ベンダ製品の政府調達からの排除（2018 年 8 月）、5G ネットワーク事業からの排除を政策化した。更に 2019 年 5 月 15 日、トランプ大統領は情報通信技術とサービスサプライチェーンの安全に関する大統領令※201 に署名し、Huawei に対する自国製品の取引を事実上禁じた※202。またこれに連動する形で Google は Android OS の提供を、半導体設計ベンダ ARM Holdings plc は IC チップの提供を停止した※203。中国政府は Huawei を狙い撃ちにした制裁に対して報復措置を検討すると発表し、Huawei も自社の製品はセキュリティ脅威ではないと抗議した※204。

これらの措置は中国に対して確実に痛手であり、2019 年に入り底入れを見せている景気回復は鈍化せざるを得ない。中国は従来行ってきた貿易慣行や海外先端技術の国内移転施策等を見直し、国内市場をより開かれたものにする必要がある。一方で、Huawei への制裁は、5G 等の次世代 IT インフラ整備において米中どちらが覇権を握るかの争いでもあると言われる。次世代 IT インフラを制した国が安全保障上優位に立つことは明らかである。この点で中国政府、あるいは Huawei はしたたかであり、EU 諸国と良好な関係を保ちつつ（「2.2.3 欧州の政策」参照）、米国と交渉していくものと思われる。米国も、ここまでこじれた摩擦は簡単には解消しないと見ており、交渉は長期化が予想される。

(2) 行動履歴等による信用格付けの本格化

2014 年 6 月、中国国務院は「国务院关于印发社会信用体系建设规划纲要（2014-2020 年）：社会信用システム建設計画綱要（2014-2020 年）※205」を発表し、2020 年までに、国家規模での情報蓄積体制を整備し、活用する体制を整える、としていた※206。2018 年以降、この計画の全貌が明らかになりつつある※207。社会信用システムとは、国民のネット上の行動・購買活動等の履歴を分析し、それぞれがどの程度信用できるかを AI 技術等を用いてスコア化して与信評価等に用いる、いわゆる「格付けシステム」である。中国の全国民は今後、借金をしない、社会のルールを守る、等の信用スコア（誠実度）が付けられ、金融・不動産・医療等のサービスをどれだけ利用できるかに反映されることになる。

民間においては、2015 年以来パイロットサービス事業が 8 社により行われている。例えば Alibaba.com の信用スコアサービス「芝麻信用」は、2018 年 1 月の時点で 5 億 2,000 万ユーザを持つ電子決済サービス「Alipay」と連携し、顧客の購買行動や SNS の履歴等から信用スコアを算定、シェアサービス等の保証金免除、出国手続きの一部簡素化等の付加価値を提供している※208。中国政府は 2018 年に、政府が主導する信用調査機関として百行征信用※209 に許可を与えた※210。芝麻信用等で蓄積された技術・ノウハウを流用してシステムを構築していくものと思われる。

中国政府はこれまで、社会信用の根幹となる社会インフラや食品の安全、製品の模造や不正取引の撲滅等について悩まされてきたが、国民のネット上の行動履歴をプライバシーに踏み込んで分析し、格付けするという、ある意味強権的な手法によって信用を構築しようとしている。信用度の高い人を明確化し、アドバンテージを与えるやり方は、中国では民間の成功体験が既にあり、一

定程度受け入れられると思われる。

一方、不払い等で低く格付けられた人のサービス低下が懸念される等、運用の課題は既に顕在化している。また言うまでもなく、このシステムは監視強化というリスクを内包している※211。例えば、同システムの「違法な社会組織の取り締まり」への適用について、何を違法とするか、への政府の介入等が不安視されている。

インターネット空間において、マルチステークホルダによる統治や、GDPR に代表される個人の権利保護を最上位の価値とする日米欧にとっては、政府が国民を格付けするシステムの採用は総じて難しいと思われる。しかし、社会信用スコアという手法にはメリットもあると考えられ、中国の壮大な実験を注視していく必要がある。

2.2.5 アジア太平洋地域でのCSIRTの動向

サイバー攻撃による被害の未然防止や、迅速なインシデント対応のために、各国の窓口となる National CSIRT はいち早く情報を入手・分析し、また他国のカウンターパートとも連携を密に取りながら、自国内の関連組織やユーザに対して適切に情報を伝達・公開することが求められている。こうした CSIRT の役割の重要性から、各国では新たに CSIRT を立ち上げたり、あるいは既存の組織の役割や権限を、法制度やサイバーセキュリティ戦略の中で明文化したり、強化している。本項では、アジア太平洋地域における CSIRT の設立や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。

(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) オーストラリア

司法省傘下にあった National CSIRT である CERT Australia を含む、オーストラリア政府内のサイバーセキュリティに関連する複数の組織が、2015 年から ACSC（Australian Cyber Security Centre：オーストラリアサイバーセキュリティセンター）※212 という共同体を構成し、協力してインシデント対応等に当たっていた。この ACSC は 2018 年 7 月に改組され※213、ASD（Australian Signals Directorate：オーストラリア通信電子局）※214 傘下に置かれることになった。組織改編された ACSC が、同国の National CSIRT としてインシデント対応の窓口となるとともに、国内の産学官の連携を促進する、政府・中小企業を含めた民間セクター、重要インフラ事業者等、国内全般のコミュニティへのセキュリティ啓発活動や情報提供を進める等の方針が示されている。改組された ACSC の活動については以下の方針が示されている。

- National CSIRT としてインシデント対応の窓口となる。
- 国内の産学官の連携を促進し、情報共有やサイバー脅威に対する対応力を高める。
- 政府、中小企業を含めた民間セクター、重要インフラ事業者等、国内全般のコミュニティへのセキュリティ啓発活動を進める。
- オーストラリア国内のすべてのユーザに対し、情報・アドバイス・支援を提供する。

(b) フィリピン

2017 年 5 月発表の「国家サイバーセキュリティ計画 2022※215」の中で National CSIRT を設立することが示された。これを受け、DICT（Department of Information and Communications Technology：情報通信技術省）※216 の傘下で NCERT（National Computer Emergency Response Team）※217 が活動を開始した。基本的なインシデント対応のほか、セキュリティ意識向上のための活動等を行っている。また、前述のサイバーセキュリティ計画では、NCERT が国の政府機関や軍、民間企業の CERT 間の連携を統括する役割を担うと定めている。

(c) 南太平洋地域の国々

パプアニューギニアでは、2018 年 1 月に National CSIRT である PNG CERT※218 が NICTA（National Information and Communications Technology Authority：国家情報通信技術局）※219 の傘下に設立された。

また、バヌアツでも 2018 年 6 月に CERT VU※220 が活動を開始した。同国は、National CSIRT を設立することを 2013 年 12 月に発表したサイバーセキュリティ政策※221 の中で目標として掲げており、これがようやく実現した。

南太平洋地域での National CSIRT の設立や組織間の連携に関しては、技術面では APNIC（Asia Pacific Network Information Centre：アジア太平洋ネットワークインフォメーションセンター）※222 やニュージーランドの CERT NZ がトレーニング等を通じて、また資金面ではオーストラリア政府が支援を行っている（「2.2.5 (2) アジア太平洋地域の CSIRT 間連携」参照）。

(d) スリランカ

スリランカでは、2018 年 11 月に同国初の「情報・サイバーセキュリティ戦略」[※223] が National CSIRT である Sri Lanka CERT|CC[※224] から発表された。同戦略には、関係省庁が協力してサイバーセキュリティ脅威に立ち向かうため、国家情報・サイバーセキュリティ局（National Information and Cyber Security Agency）を設立することが明記されており、政府のサイバーセキュリティ体制の一元化と強化が期待されている。その他の目標として、サイバー空間保護のための法律や制度を整備すること、サイバー攻撃に対応するための高度な労働力を拡大すること、サイバーセキュリティに関する国民の意識向上の取り組みを推進すること、官民や国内外の組織間での連携を発展させることが掲げられている。

なお Sri Lanka CERT|CC は、新組織のもとで官民セクターのサイバー防護に加えて、一般ユーザに向けた情報提供の役割を担うほか、セクター CERT 間の情報共有や連携の調整役となることが定められている。

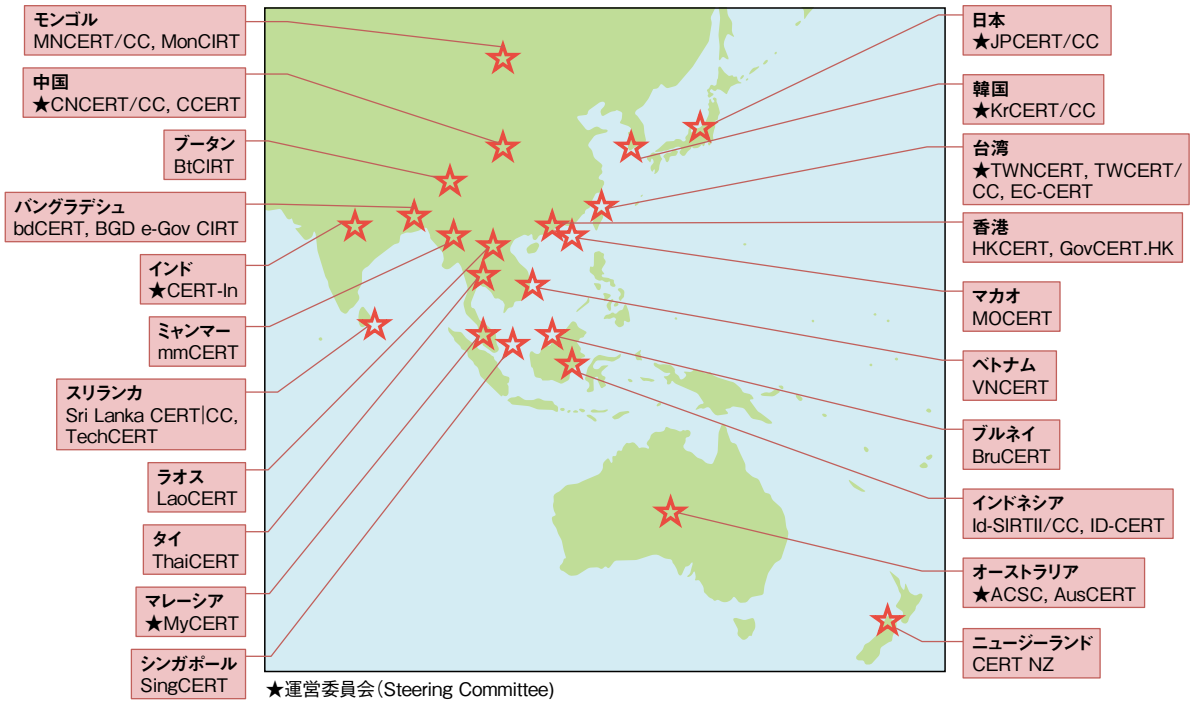
(e) シンガポール

シンガポールでは 2018 年 8 月にサイバーセキュリティ法[※225] が施行された。同法により、National CSIRT である SingCERT[※226] を擁するサイバーセキュリティ庁（Cyber Security Agency：CSA）[※227] が、サイバー脅威やインシデントの調査及び被害の予防措置を講じること、また脆弱性の特定やインシデントの予防に役立つ情報を CSA が集約し、関係機関と共有することが定められた[※228]。この法整備により、インシデントの予防や対応における SingCERT の役割の法的根拠が明確になった。

(2) アジア太平洋地域の CSIRT 間連携

アジア太平洋地域全体の CSIRT からなるコミュニティとして、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）があり、地域内で発生したインシデントにおける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、参加メンバーは 12 の国･経済地域の 15 チームだったが、地域内で National CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増え、2019 年 3 月末現在 21 の国・経済地域の 30 チームが、主要メンバーを意味するオペレーショナルメンバーとなっている（図 2-2-1）。

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組織運営を支えている。また、JPCERT/CC が主導するネットワーク定点観測共同プロジェクト「TSUBAME」に参加する APCERT メンバーも多く、APCERT 内にワーキンググループを設けて、センサーを用いたサイバー脅威動向の



■図 2-2-1　APCERT オペレーショナルメンバー（2019 年 3 月末現在）

観測や情報共有を推進している。

APCERT の主な活動は、年次報告書の発行、年次サイバー演習の実施、年次会合の開催である。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、対応したインシデント統計等をまとめた文書で、Web サイトで公開されている※229。

2018 年のサイバー演習は、「IoT 機器に関連するマルウエアが引き起こすデータ漏えい」をテーマに実施された※230。同演習には、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）に加盟するエジプト、モロッコ、ナイジェリア、オマーン、パキスタンの CSIRT も招待し、合計 25 の国・経済地域から 32 チームが参加した。

また、2018 年の年次会合は、中国の CNCERT/CC がホストとなり、10 月に上海で開催された。APCERT の運営方針について議論されたほか、CSIRT 担当者やセキュリティ専門家らにより、最新のインシデント動向等について活発な意見が交わされた。

このほか、APCERT では能力開発のための取り組みとして、電話会議システムを利用してインシデント対応に関するノウハウを教えるオンライン・トレーニングを 2014 年以来継続しているほか、年次会合の場を利用して技術的なトレーニングのワークショップも開催されている。

こうしたアジア太平洋地域全体での取り組みに加え、より狭い地域でも CSIRT 連携の活動が始まりつつある。例えば、シンガポールは ASEAN の国々のサイバーセキュリティ能力向上のため「ASEAN-Singapore Cybersecurity Center of Excellence（ASCCE）」を 2019 年中に開設すると発表した※231。同センターは、トレーニングや研究、CSIRT の能力向上、そして CSIRT 間の情報共有の推進に重点を置いて活動する予定である。

また、南太平洋地域では、オーストラリア政府が主導し CSIRT 間活動や他の政府組織間の連携を促進する 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）※232 が始動している。2018 年 5 月に最初の会合が開催され、オーストラリアを含めた南太平洋地域の 15ヵ国※233 が参加した。初代の議長チームとして、ニュージーランドの CERT NZ が選出されている。トレーニングや情報共有の場を設け、まだ National CSIRT の設立が進んでいない国々のサイバーセキュリティ能力の向上や、組織間の連携促進に資することが期待されている。

このように、アジア太平洋地域の各国における CSIRT の設立や役割強化に加えて、APCERT が主導する地域全体、あるいは ASEAN や PaCSON のようなより小さな地域でも CSIRT の能力向上を促し、連携を強化する取り組みが見られる。個々の CSIRT の能力向上、ひいてはアジア太平洋地域の CSIRT 全体の成熟度の向上や連携の促進につながることが期待される。

COLUMN

CBPRシステム ～APECの越境個人情報保護～

個人情報保護に関して、昨今 EU の GDPR（一般データ保護規則）が話題となっていますが、日本も参加している環太平洋地域の個人情報保護制度があることをご存知でしょうか。

2011 年に APEC（アジア太平洋経済協力）で、「CBPR（Cross-Border Privacy Rules：越境プライバシールール）システム」が構築されました[i]。これは、APEC に参加している国・地域（エコノミー）間で個人情報を取り扱う事業者が、APEC 域内で個人情報の越境移転を円滑に行うための制度です。2019 年 3 月末時点で、米国、メキシコ、日本、カナダ、韓国、シンガポール、オーストラリア、台湾の計八つの国・地域が CBPR システムに参加しています。また、日本では一般財団法人日本情報経済社会推進協会（JIPDEC）が CBPR システムの認証機関として、個人情報を取り扱う事業者の審査・認証業務を行っています[ii]。

では、日本の事業者が CBPR システム認証を取得することで、どのようなメリットがあるのでしょうか。例えば、CBPR システムへの取り組みを通じて、社内における個人情報保護の仕組みの改善につなげることができます[iii]。更に、認証を受けることで個人情報保護対策の度合いを客観的に示せることから、消費者や他社への信頼性アピールや事業者間のデータ取引の促進にもつながります。他にも、これまでに GDPR との相互運用性についても議論が行われており[iv]、相互運用ができるようになれば更なるデータ流通の円滑化が期待されます。

また、2017 年 5 月に施行された改正個人情報保護法[v]の第 24 条では、外国にある第三者への個人情報提供の制限として、原則本人の同意を得なければならないと規定されていますが、個人情報保護委員会による「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）[vi]」では、本人の同意の必要がない例の一つとして、個人情報の提供側または受領側の事業者が CBPR システム認証を受けていることを挙げています。そのため、CBPR システム認証を受けた日本の事業者は、日本から外国への個人情報提供を円滑に実施できることになります。

グローバル化やデータ利活用が進む中、セキュリティ対策強化のためにも、CBPR システム認証の取得について検討してみてはいかがでしょうか。

i　CBPRs：ABOUT CBPRS　http://cbprs.org/about-cbprs/〔参照 2019-07-01〕
ii　JIPDEC：CBPR 認証　https://www.jipdec.or.jp/protection_org/cbpr/index.html〔参照 2019-07-01〕
iii　CBPRs：BENEFITS OF THE APEC Cross-Border Privacy Rules　http://cbprs.org/wp-content/uploads/2019/05/Benefits-of-CBPR-System-Guide_Jan-2019_FINAL.pdf〔参照 2019-07-01〕
iv　経済産業省:APEC/CBPRシステムと個人情報の域外移転　https://www.jipdec.or.jp/sp/topics/event/u71kba000000k6i5-att/20180531-jipdec-cbpr-3-ks3.pdf〔参照 2019-07-01〕
v　個人情報保護委員会：個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）　https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf〔参照 2019-07-01〕
vi　https://www.ppc.go.jp/files/pdf/190123_guidelines02.pdf〔参照 2019-07-01〕

2.3 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。

2.3.1 情報セキュリティ人材の状況

サイバーセキュリティ戦略本部の普及啓発・人材育成専門調査会では2018年5月31日、「サイバーセキュリティ人材育成取組方針」として、「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※234」と「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※235」を取りまとめ、「サイバーセキュリティ戦略」（2018年7月27日閣議決定）にその内容が反映された（サイバーセキュリティ戦略については「2.1.1 政府全体の政策動向」参照）。本項では、「サイバーセキュリティ戦略」の人材育成政策と関連するセキュリティ人材育成の検討の状況について述べる。

「サイバーセキュリティ戦略」では、横断的施策の一つとして「人材育成・確保」が位置付けられており、「Society 5.0」の実現に向けてビジネスのデジタル化による新たな価値が創出されていく将来を見据え、企業等様々な組織の「任務」遂行や、デジタル空間における個人の安全な利用を支えるために、産学官が連携して、人材育成・確保を強化するとともに、イノベーションを推進する観点から、人材の多様性の確保を推進することが重要であるとしている。

推進する取り組みとしては戦略マネジメント層※236の育成・定着、実務者層・技術者層の育成、人材育成基盤の整備、各府省庁のセキュリティ人材の確保・育成強化、国際連携の推進が挙げられている。

具体的には、セキュリティ人材育成を進めていくために、以下の項目を実施し、人材の需要と供給が相互に満たされる好循環を形成することが必要と述べている。

- セキュリティ人材の役割の定着と明確化
  企業経営でサイバーセキュリティ対策を進めていく人材層として、経営層に加えて、戦略マネジメント層の育成・定着、実務者層・技術者層の育成が必要であるとしており、大学・高等専門学校等の教育で身に付けるべき知識や技術等、それぞれで保有すべき知識や技術等を明確化する。
- 能力可視化のための、資格・評価基準等の整備
  戦略マネジメント層、実務者層・技術者層向けの学び直しプログラムや実践的な演習環境、産学官連携による大学・高等専門学校等の情報技術人材の育成等、様々な人材層における育成基盤を整備するとともに、必要な能力を身に付けたことを証明する資格・評価基準等を整備することにより、セキュリティ人材の見える化を行う。
- キャリアパスの形成
  セキュリティ人材の能力に応じた適切な処遇を受け、実務経験を積んでいくことで更に評価が上がるキャリアパスを形成する。

以下ではこの三つの項目に沿ってセキュリティ人材育成政策の状況を説明する。

(1) セキュリティ人材の役割の定着と明確化

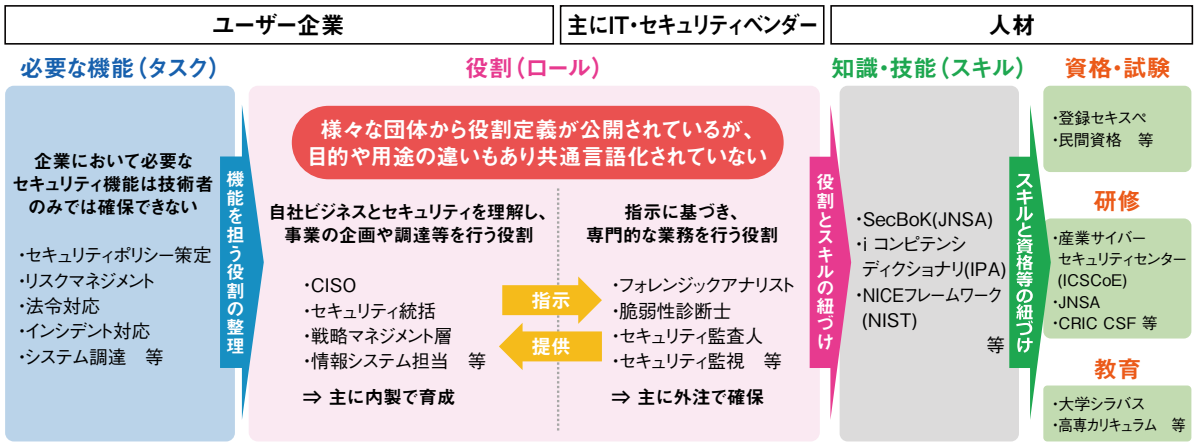
「サイバーセキュリティ戦略」では、企業のセキュリティ人材の類型の典型的なモデルとして、「人」ではなく「機能」に着目し、以下の3層で整理を行っている。

- 経営層
- 戦略マネジメント層
- 実務者層・技術者層（システム担当・システム構築担当を想定）

戦略マネジメント層の考え方を更に進めるために、経済産業省は産業サイバーセキュリティ研究会 ワーキンググループ2（以下、WG2）において人材育成関連の検討を行っている。様々な組織、団体から発表されている企業のセキュリティ人材に関する考え方を整合し、セキュリティ人材の役割定義に関して共通した整理（役割定義の共通言語化）を行うことにより、セキュリティ人材の需要と供給のマッチングが容易に行えるように見える化を実現することを目標としている。

WG2では、企業に求められるセキュリティ機能を遂行する人材を以下の手順で整理している（次ページ図2-3-1）。

①企業におけるセキュリティ機能（タスク）の洗い出し
②機能を担う役割（ロール）の整理



■図 2-3-1　セキュリティ人材の流動化に対応できる『セキュリティ人材活用モデル』の構築
（出典）経済産業省「事務局説明資料※237」（第 3 回産業サイバーセキュリティ研究会 WG2 資料）

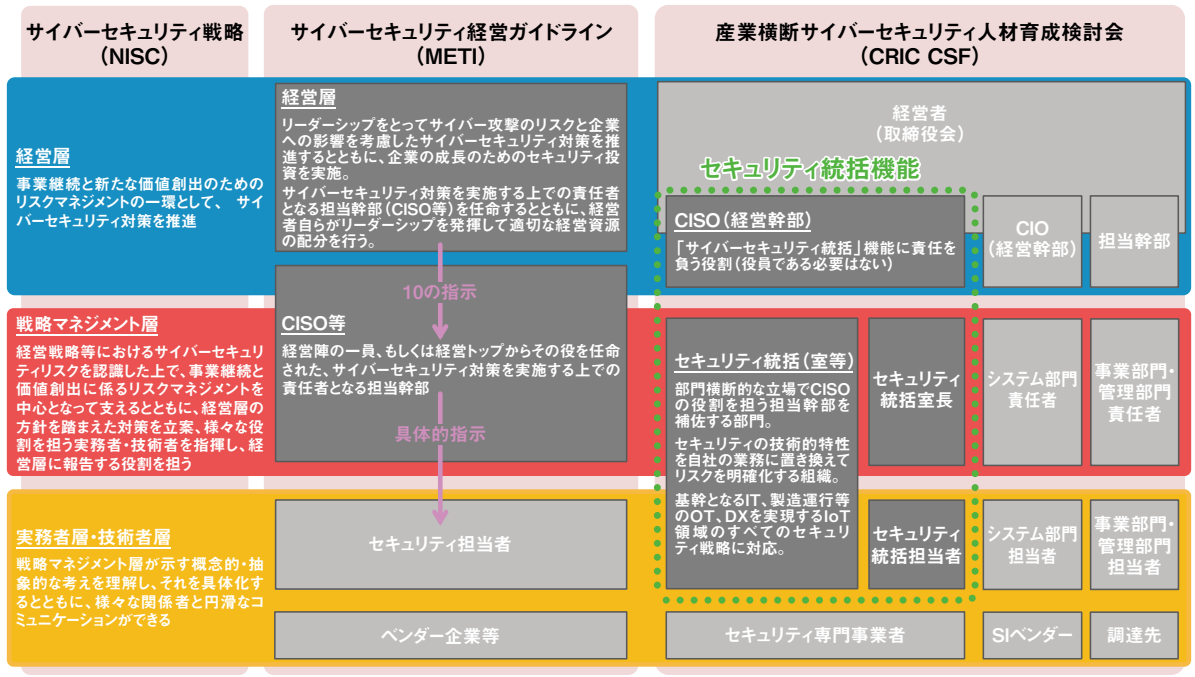
③役割の遂行に必要とされる知識・技能（スキル）の明確化
④スキルと資格等の紐付け

(a) ユーザ企業におけるセキュリティ体制・人材

WG2 では、ユーザ企業におけるセキュリティ体制・人材に関する概念整理として、NISC の「サイバーセキュリティ戦略」、経済産業省の「サイバーセキュリティ経営ガイドライン」、一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ人材育成検討会（Cyber Risk Intelligence Center - Cross Sectors Forum：CRIC CSF）の「セキュリティ統括機能」を比較し、検討を行っている（図 2-3-2）。

「サイバーセキュリティ戦略」では、経営層、戦略マネジメント層、実務者層・技術者層の 3 層で整理を行っているが、「サイバーセキュリティ経営ガイドライン」と CRIC CSF では、ユーザ企業におけるセキュリティ機能を、事業に深く関連した役割と、指示に基づき専門的な業務を行う役割で担うことを想定し、専門的な業務については、IT ベンダやセキュリティベンダ等の外部事業者に委託する 4 層構造で整理している。

このような 4 層構造を取った理由としては、日本の多く



■図 2-3-2　「サイバーセキュリティ戦略」、「サイバーセキュリティ経営ガイドライン」、CRIC CSF「セキュリティ統括機能」等の諸概念の関係整理
（出典）経済産業省「事務局説明資料※238」（第 4 回産業サイバーセキュリティ研究会 WG2 資料）

のユーザ企業では内製すべきセキュリティ人材が不足しているが充足の目途が立たない状況であること（図 2-3-3）、また、日本における IT 人材は、諸外国と比較してユーザ企業に所属している割合が低く、自社内で充足することが難しいためである。IPA の「IT 人材白書 2017[※239]」によれば、例えば、米国では IT 人材の 65.4% がユーザ企業に所属しているが、日本では、28.0% にとどまっている（図 2-3-4）。

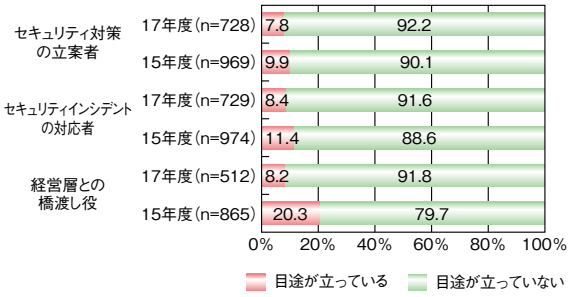
ユーザ企業のセキュリティ体制・人材の見える化について検討結果をまとめたものが図 2-3-5 である。

戦略マネジメント層は図中に赤い帯で示されている。戦略マネジメント層は、サイバーリスクを経営戦略や事業戦略のもとで認識し、以下の両方を担う役割とされており、必ずしも一人でこれらの役割を担うことは想定されていない。

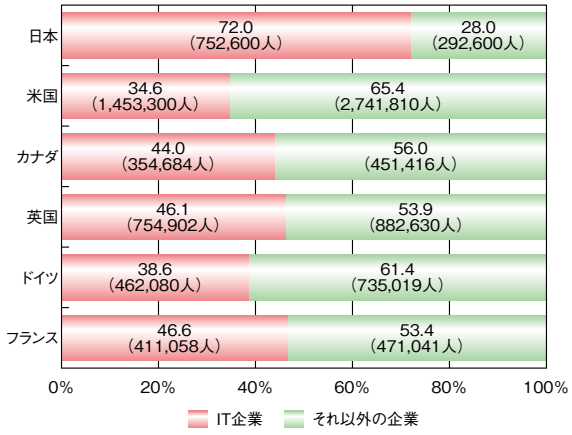
- 価値創出のための事業におけるリスクマネジメント
- インシデント発生時等への対応等の、企業全体の事業継続のためのリスクマネジメント

ユーザ企業のセキュリティ体制・人材の見える化では、事業そのものにおけるリスクマネジメントはそれぞれの事業部門の事業責任者が担うことを想定し、企業の全事業部門に共通であるべきリスクマネジメントを統轄する役割としてセキュリティ統括機能を設けるとしている。

また、セキュリティ統括機能の実現方法としては、情報システム部門の 1 機能から、組織上の 1 部門として設置、あるいは、委員会として設置等、企業ごとで様々

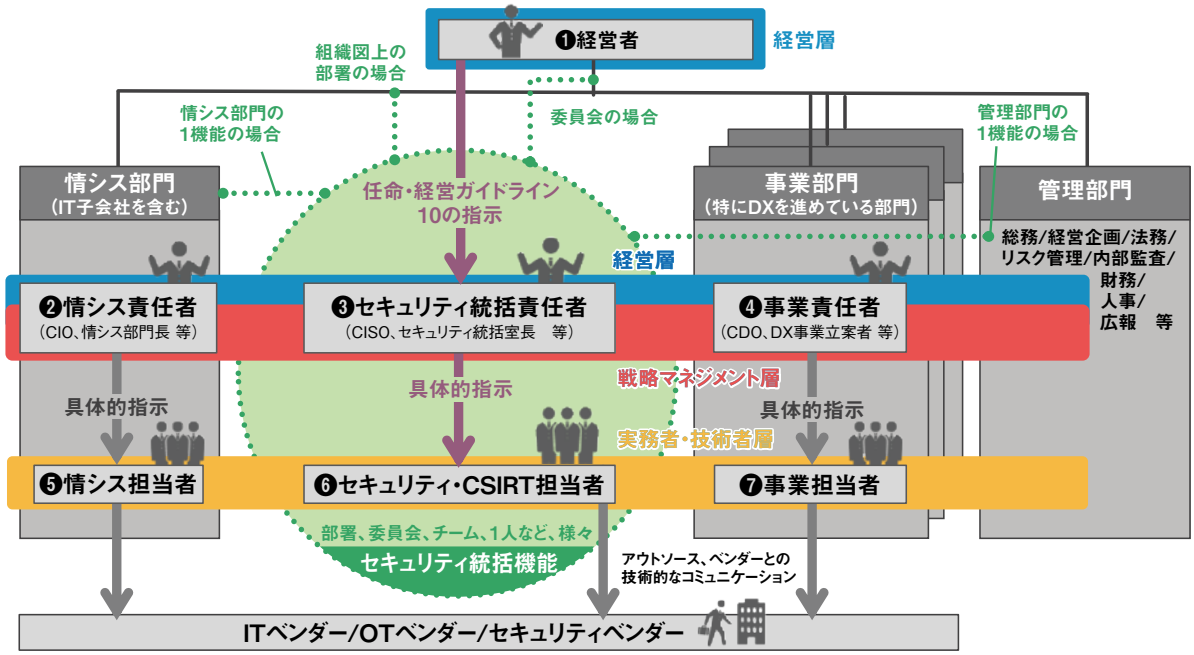


■図 2-3-3　不足しているセキュリティ人材の拡充目途
（出典）一般社団法人日本情報システム・ユーザー協会「第 24 回 企業 IT 動向調査 2018（17 年度調査）[※240]」を基に IPA が編集



※日本、米国、英国、ドイツ、フランス:2015年、カナダ:2014年

■図 2-3-4　情報処理・通信に携わる人材が所属する企業の国別比較（日、米、欧州等）
（出典）IPA「IT 人材白書 2017」を基に編集



■図 2-3-5　ユーザ企業におけるセキュリティ体制・人材に関する概念整理
（出典）経済産業省「事務局説明資料」（第 4 回産業サイバーセキュリティ研究会 WG2 資料）

な形式が可能としている。どのように実現するかは、企業によって異なるにしても、今後の経営においては何らかの形でサイバーリスクのマネジメントを全事業にまたがって統活する機能を持つことが求められている。

(b) IT ベンダ／セキュリティベンダにおける専門人材の役割・スキル定義

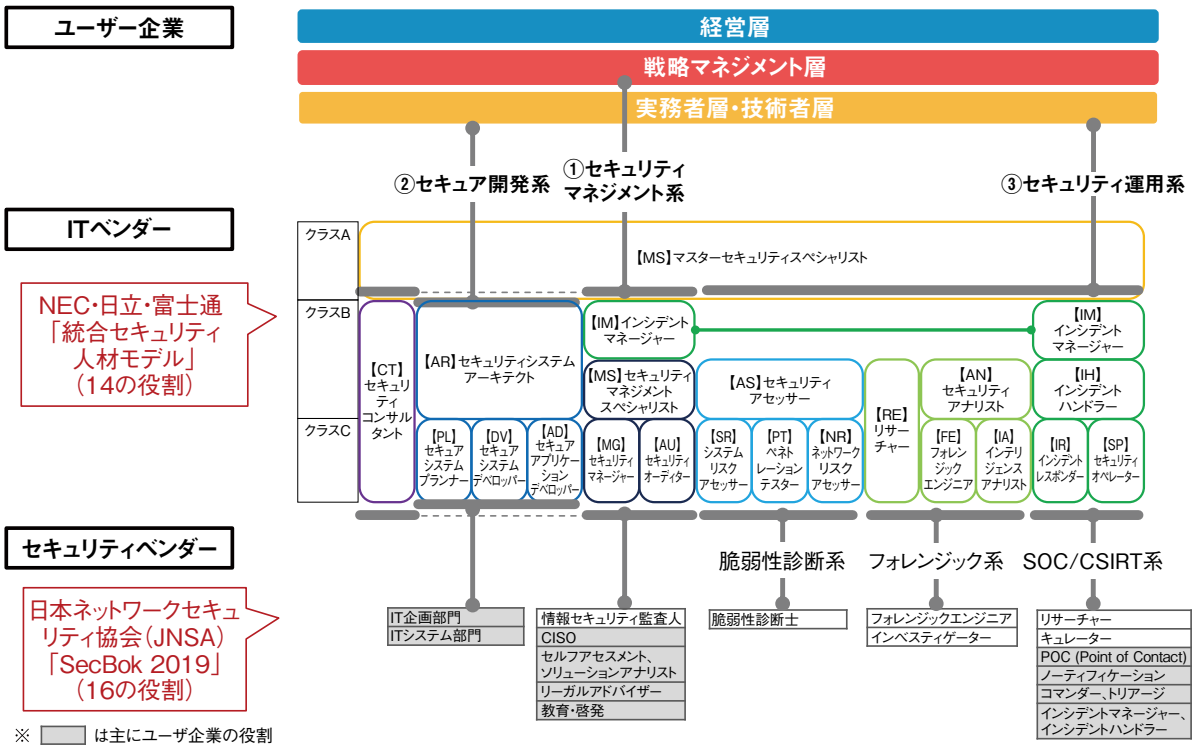
セキュリティの専門的な機能を担い、ユーザ企業を支援する IT ベンダ／セキュリティベンダのセキュリティ専門職の役割とスキルに関するモデル、スキルマップ等には、主に次のようなものがある。

- IPA：i コンピテンシディクショナリ※241（セキュリティについては、特定業務としてのセキュリティ領域のタスクセットを公開している。）
- NIST：NICE（SP800-181）※242
- 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）：セキュリティ知識分野（SecBok）人材スキルマップ 2019 年度版※243
- サイバーセキュリティ人材育成スキーム策定共同プロジェクト：統合セキュリティ人材モデル※244

WG2 では、それぞれの特徴を踏まえた上で、IT ベンダ／セキュリティベンダにおけるセキュリティ人材の役割・スキル定義に関する検討を行っている。2019 年 5 月時点では検討が終了していないが、図 2-3-6 に示すように、IT ベンダでのセキュリティ専門人材の役割に「統合セキュリティ人材モデル」、セキュリティベンダのセキュリティ専門人材の役割に「SecBok2019」を用いて整理しようとしている。

「統合セキュリティ人材モデル」は IT ベンダがユーザへのサービスや製品を提供する際に必要な役割を、日本電気株式会社、株式会社日立製作所、富士通株式会社の 3 社の既存の体系を整合し共通化したものであり、IT ベンダの役割として整理されている。また、ユーザ企業との連携に関しては、2018 年度に IPA で行った情報処理安全確保支援士（以下、登録セキスペ）の実態調査から、登録セキスペの主な三つの担当業務として、セキュリティマネジメント系、セキュア開発系、セキュリティ運用系※238 が抽出されており、その業務カテゴリに沿った整理が検討されている（実態調査については「2.3.3 (2) 情報処理安全確保支援士」参照）。

「SecBok 2019」の 16 の役割には、ユーザ企業の役割に整理できるものが含まれていて、その一部をセキュリティベンダの役割として、大きく「監査系」「脆弱性診断系」「フォレンジック系」「SOC/CSIRT 系」の四つのカテゴリと



■図 2-3-6　IT／セキュリティベンダにおける専門人材の役割・スキル定義の関係性概念整理
（出典）経済産業省「事務局説明資料」（第 4 回産業サイバーセキュリティ研究会 WG2 資料）

してとらえようとしている。経済産業省の情報セキュリティサービス審査登録制度との関連も含め議論していく必要がある。

(2) 能力の可視化を行うための資格・評価基準等の整備

セキュリティ人材の能力を可視化するための標準としては、IPA の「IT スキル標準（ITSS）」に対して、2017 年 4 月にセキュリティ領域を追加して策定した「ITSS+（プラス）」がある。これは、新しい領域の「学び直し」の指針として、従来の ITSS が対象としていた情報サービス提供やユーザ企業の情報システム部門の従事者のスキル強化に利用されることを想定しており、ITSS と同様に評価指標として 7 レベルが規定されている（図 2-3-7）。

領域	セキュリティ領域													
専門分野	情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTキュレーション	CSIRTリエゾン	CSIRTコマンド	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査
レベル 7		■	■	■		■	■				■		
レベル 6		■	■	■	■	■	■		■	■	■	■	■
レベル 5		■	■	■	■	■	■		■	■	■	■	■
レベル 4		■	■	■	■	■	■	■	■	■	■	■	■
レベル 3				■	■	■		■		■		■	■
レベル 2													
レベル 1													
登録セキスペ想定業務	経営課題	設計・開発		運用・保守			緊急対応						監査

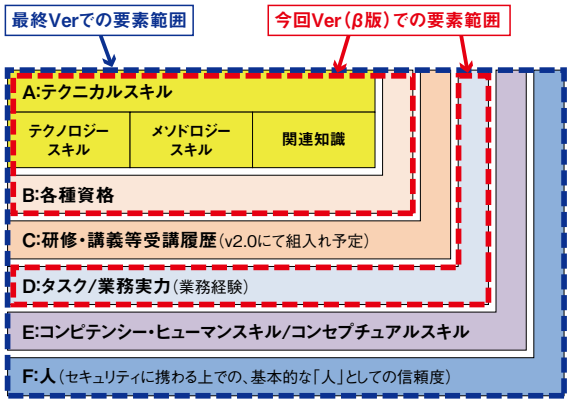
■図 2-3-7　ITSS+（セキュリティ領域）のスキル領域 I
（出典）IPA ITSS+（プラス）・IT スキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報※245

ITSS の 7 レベルは IT 人材の評価指標として広く使われており、セキュリティ人材の評価指標として共通のレベル定義を利用することは妥当と推察される。

「2.3.1 (1) セキュリティ人材の役割の定着と明確化」で述べたように、ユーザ企業、IT ベンダの様々な役割を定めたときに、現在の ITSS+（セキュリティ領域）の 13 の専門分野との整合をどのように取るか、また、セキュリティ人材は ITSS+ が想定している対象より広がりを持っており、今後、登録セキスペの位置付けも含めて、ITSS+ をどのように利用するかの議論が求められる。

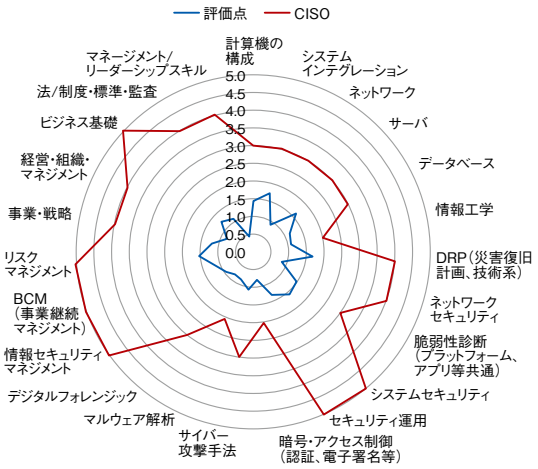
民間団体によるセキュリティ人材の評価認定の活動としては、JNSA が支援する ISEPA（Information Security Education Providers Association：情報セキュリティ教育事業者連絡会）※246 が JTAG※247 活動として、国内の情報セキュリティ事業者やユーザ企業、人材サービス事業者、教育提供事業者等と連携して、セキュリティ人材のスキル認定制度構築を目指している。2019 年 1 月に情報セキュリティ人材に対するスキルの可視化を行うためのガイドライン（β版）を発表した。

同ガイドラインは図 2-3-8 に示すように、評価基準としては、「A：テクニカルスキル」「B：各種資格」「D：タスク / 業務実力（教務経験）」を要素としているが、β版でのトライアル検証を実施し、精度を高めるとしている。



■図 2-3-8　評価基準の概念図
（出典）JTAG「セキュリティ業務を担う人材のスキル可視化ガイドライン～プラス・セキュリティ人材の可視化に向けて～〈β版〉※248」

最終的には、その他の評価要素を加えて、23 種類の指標を用いて、図 2-3-9 に示すようなレーダーチャートとして視覚的に表現することが予定されており、ITSS のレベル設定に基づき 7 レベルを上限として、161 ポイント



■図 2-3-9　セキュリティ業務遂行能力のレーダーチャートのサンプル
（出典）JTAG「セキュリティ業務を担う人材のスキル可視化ガイドライン～プラス・セキュリティ人材の可視化に向けて～〈β版〉」を基に IPA が編集

の数値化が行われる。

JTAGでは、評価指標により、対象者のセキュリティ業務遂行能力が数値化でき、また、各業務への適合度が計測できるとしている。また、利用イメージとしては、個人が能力を客観的に判断して、自身の伸ばすべき能力を把握する、キャリアパスの選択等で参考にする、あるいは企業等でのセキュリティ人材の適材適所への配置や自組織に不足している人材を把握する、等に活用できるとしている。

セキュリティ人材の可視化を行うためには、評価指標は共通で使えることが重要であり、資格制度と整合が取れたものであることが望まれる。セキュリティ人材の様々な役割に応じた評価ができる共通の評価指標と、それにしっかり紐付いた形での資格制度あるいは認定の仕組みを、既存の資格制度との整合を取りながら検討することが今後の課題である。

(3) キャリアパスの形成

セキュリティ人材不足が課題として取り上げられるようになって、セキュリティ人材のキャリアパスについての議論が続いているが、それぞれの企業は業態、業界、規模等様々な要因によって状況が異なっており、キャリアパスもそれに応じて検討する必要がある。

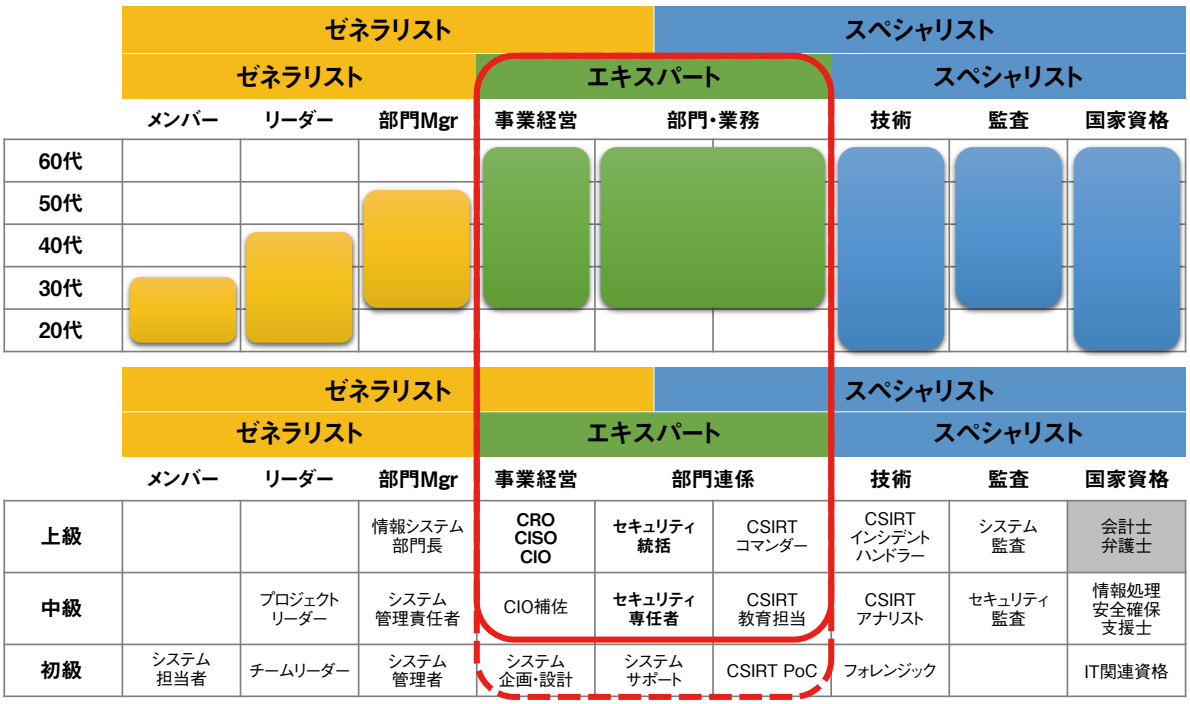
「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」では、CRIC CSFの第二期中間報告を参考として、キャリアパスを検討する際に、ユーザ企業の類型を以下の二つに分け、議論する必要があると述べている。

- ITビジネス企業：ビジネス自体がインターネット上にある企業、または、ITを駆使してビジネスを行う企業
- 伝統的な企業：ものづくり的な部分がビジネスの根幹である企業

「ITビジネス企業」においては、「伝統的な企業」よりは既に人事制度上でセキュリティ人材のキャリアパスが確立されている割合が多いと想定されており、セキュリティ人材のキャリアパスに関する議論は、主に「伝統的な企業」について行われている。

その一つとして、CRIC CSFでは、セキュリティ人材のキャリアパスをゼネラリスト、エキスパート、スペシャリストの三つに分類して検討を行っている（図2-3-10）。

このうち、ゼネラリストは企業における管理業務を行う人材であり、スペシャリストは専門技術を持った人材として、ITベンダ／セキュリティベンダ、情報子会社に所属していると推察しており、両者とも既に既存の人事制度上でキャリアパスが確立しているものと認識されている。CRIC CSFでは、エキスパートに分類される人材を、セキュリティ統括人材と呼称しており、図2-3-5（97ページ）



■図2-3-10　三つのキャリアパス
（出典）CRIC CSF「『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 第1.0版※249」

に示した、戦略マネジメント層としてセキュリティ統括機能を担っている人材を指している。

現時点では「伝統的な企業」と考えられるユーザ企業において、セキュリティに関連するキャリアパスの枠組みは構築されたものの、実際には定着していない。しかしながら、企業においてサイバーセキュリティが事業全体の課題となり、リスクマネジメントあるいは内部統制の一環として扱われるようになってきていることを受けて、企業内の多様な事業全体のセキュリティを横串で担当する部門が設置され※250、セキュリティに関連したキャリアパスが形成されると予想される。

今後、現在進行している各企業での取り組みを踏まえつつ、セキュリティ統括機能の更なる明確化、それを担う人材の育成、企業での処遇を可視化することが、セキュリティ人材のキャリアパス形成に重要である。

2.3.2 産業サイバーセキュリティセンター

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、2017 年 4 月、IPA は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。

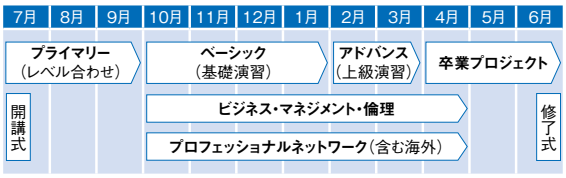
ICSCoE では、社会インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。同プログラムは、図 2-3-11 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 年をかけて実施する。

第 1 期の中核人材育成プログラムには 76 名の受講生が参加し、2018 年 7 月に開講した第 2 期では、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 83 名の受講生が参加した。

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による講義、米国や欧州、イスラエル等の海外先進事例を学ぶ海外派遣演習等を含む構成となっている。



■図 2-3-11　第 2 期中核人材育成プログラムの年間スケジュール

2018 年 9 月の海外派遣演習ではフランスにて、セキュリティの専門家によるサイバーレジリエンスの強化を目的とした研究の講義や、フランス政府関係者による重要インフラを守るためのセキュリティ関連の法制度の講義を実施した。2018 年 12 月の海外派遣演習では英国にて、英国政府・自動車業界・金融業界及びスタートアップ企業の代表者によるサイバーセキュリティの取り組みに関する講義を受講した。

また、2018 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 NCCIC ICS 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）で提供している制御システムのサイバーセキュリティに関するトレーニングを実施した。本トレーニングには、同プログラムの全受講者及びアジア太平洋地域の 15 の国・地域から、サイバーセキュリティ政策の担当者、National CSIRT の職員、重要インフラの実務者等計 36 名も参加し、「ASEAN 等向け日米サイバー共同演習」として初めて開催された。

2018 年 12 月には、2017 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、イスラエルのサイバーセキュリティ企業の担当者による重要インフラのサイバーセキュリティ対策に関する講義を実施した。

2018 年 7 月、中核人材育成プログラムの OB 会として、修了者コミュニティ「叶会」が発足し、第 1 期の修了者 76 名が中心となり活動している。同年 11 月に開催された年次総会では、各修了者が、CSIRT メンバーとして自社のセキュリティ対策の改善やインシデント対応に従事したり、グループ企業を含めた全社のセキュリティ対策の実施や社外でのセキュリティ活動に参加したりする等、1 年間に学んだことを生かし、様々な場面で活躍あるいは苦労している様子が共有された。1 年間の人材育成プログラムをともに受講したことで、各業界から参加した受

講生同士の絆（人脈）ができたことが財産とのコメントもあり、ICSCoEで得られた経験や知識、構築した人脈を活かした今後の活躍が期待される。

(2) 短期プログラム

ICSCoEでは、CIO・CISO（Chief Information Security Officer：最高情報セキュリティ責任者）や部門長等の責任者向けのプログラムとして、2日間で学ぶ短期トレーニング形式の「国際トレーニング」（旧：業界共通トレーニング）や「業界別トレーニング」を2017年から実施している。また、2018年には「戦略マネジメント系セミナー」を新設した。

(a) 国際トレーニング

2018年度は、国際トレーニングを2018年11月及び2019年2月に実施した。

本トレーニングは、OTを扱う事業領域を広く対象とし、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、講義や演習を行った。

この演習は、東京2020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るという内容で実施した。受講者は、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。

本トレーニングを通じて、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様々なステークホルダ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、実践につなげることが期待される。

(b) 業界別トレーニング

2018年度は、2018年8月に「金属、石油、化学、製薬、スマートファクトリー」、同年11月に「電力、ガス、水道、情報通信」、2019年2月に「鉄道、航空・ビル、船舶、スマートモビリティ」を対象業界として、業界別トレーニングを実施した。

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。受講者に加え、サイバーセキュリティの専門家や監督省庁の関係者も参加した形式でのグループ演習を行った。

(c) 戦略マネジメント系セミナー

2018年度に新設した「戦略マネジメント系セミナー」は、技術的側面に偏らず、総務や戦略企画、広報等、リスク管理全般に関する責任者を対象として、2018年11月より週1回、計7回シリーズとして実施した。

1回あたり2時間で、前半はサイバーセキュリティの専門家の講義を受講し、後半は仮想組織におけるセキュリティ対策の構築をテーマに「ケース討議」（グループディスカッション）を行うという構成で進められた。ケース討議では、組織におけるセキュリティ対策に必要な機能を模索する等、立場の異なる参加者の間で活発な議論が行われた。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

本項では情報セキュリティ人材の育成や確保を目的とした国家試験や国家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・組織においては、組織が定めた情報セキュリティポリシーを部門内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、「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年度春期より試験が実施された。試験は年2回実施され、2018年度の応募者数は3万8,992人であった[※251]。

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。2018年度の受験者のうち約9割を社会人が占めている。更に業種別に見ると、IT系企業が55.9%、非IT系企業が44.1%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可視化に有効な試験と考えられていることがうかがえる[※252]。

(2) 情報処理安全確保支援士

サイバー攻撃の増加・高度化に加え、社会的なIT依存度の高まりから、企業・組織におけるサイバーセキュ

リティ対策の重要性が高まっている。それに伴い、企業・組織での安全なセキュリティ対策を高度なスキルを活かして推進できる人材が求められている。

そこで、最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、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、新たな国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士は、試験合格者が登録簿に登録されることにより資格を取得する、サイバーセキュリティ分野初の名称独占資格である。試験は年 2 回実施され、2018 年度試験の応募者数は 4 万 5,627 人であった。また、情報処理安全確保支援士の登録人数は、2019 年 4 月 1 日時点で 1 万 8,330 人となった※253。図 2-3-12 は、情報処理安全確保支援士の資格保有者（以下、登録セキスペ）、またはその所属企業・組織のみが使えるロゴマークである。

■図 2-3-12　情報処理安全確保支援士のロゴマーク

登録セキスペには法定講習の受講が義務付けられており、最新知識や実践的な能力の維持が求められる。法定講習は毎年 1 回のオンライン講習と 3 年に 1 回の集合講習からなり、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※254。

ユーザ企業においては、登録セキスペに事業とのバランスを取りながら、セキュリティを担保する役割を担わせることで、IT を活用した事業促進をセキュアに進めることができる。また、登録セキスペが、セキュリティ対策が講じられていることを担保することで、税制優遇が受けられることもある※255。IT ベンダ企業においては、登録セキスペが在籍することで、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、入札要件の充足等によるビジネスチャンスの拡大といったメリットが期待できる。

(3) 登録セキスペの実態調査

制度の運用開始から 2 年が経過し、登録者が 1 万 8,000 人を超える規模となったことから、IPA では登録セキスペを主な対象として、サイバーセキュリティ対策に関わる人材の実態調査を 2018 年 12 月～ 2019 年 3 月に実施した。

実態調査では、以下を対象者としてアンケート、及び一部の方へのヒアリングを実施した。

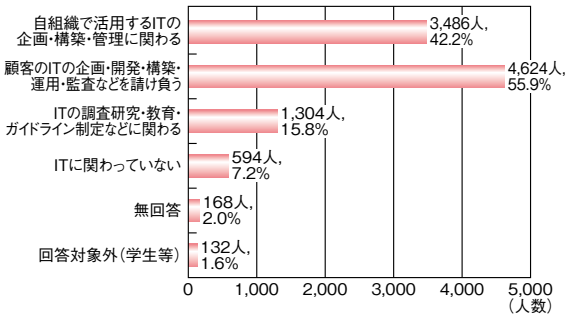
①登録セキスペ（回答数 8,266）
②高度 IT 人材（アンケートサービス企業のモニタ登録者から一定条件を満たす人を抽出、回答数 1,000）
③登録セキスペの所属組織の組織長（①の対象者からの紹介による、回答数 170、ヒアリング数 5）

主なアンケート項目は、担当業務や業務の難易度、登録セキスペ制度の活用状況等である。登録セキスペを対象としたアンケート調査結果の一部を紹介する。

なお、アンケートでは、活用スキルや他部署との連携状況等についても尋ねており、これらも併せて分析した結果を別途公開する予定である。

(a) 登録セキスペの IT との関わり方

登録セキスペは、IT ベンダ企業等において顧客の IT サービス・システムの構築・運用等を請け負う人と、ユーザ企業等において自組織で活用する IT の企画・構築・管理に関わる人に大別されると仮定し、その分布を確認した（図 2-3-13）。

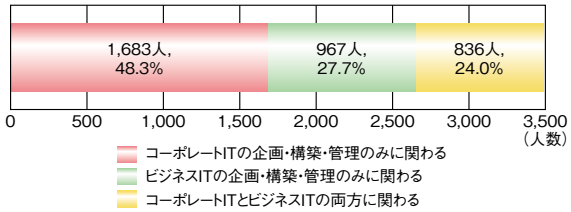


■図 2-3-13　登録セキスペの IT との関わり方（複数選択、n=8,266）

最も多いのは「顧客の IT の企画・開発・構築・運用・監査などを請け負う」人で 55.9% であったが、「自組織で活用する IT の企画・構築・管理に関わる」人も 42.2%おり、自組織の IT を守る立場にいる登録セキスペも多いことが分かった。

(b) 登録セキスペが関わる IT の種別

図 2-3-13（前ページ）の「自組織で活用する IT の企画・構築・管理に関わる」人が、組織内で活用する IT（コーポレート IT）に関わるのか、社外取引等の対外システム（ビジネス IT）に関わるのかを確認した（図 2-3-14）。



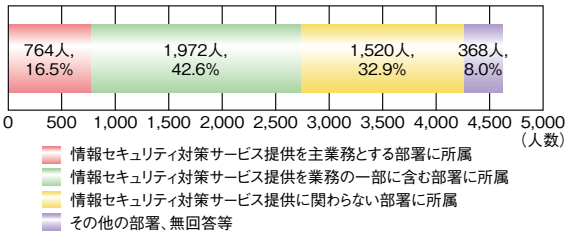
■図 2-3-14 「自組織で活用する IT の企画・構築・管理に関わる」を選択した登録セキスペが関わる IT の種別（複数選択、n=3,486）

結果としてはビジネス IT に関わる人よりもコーポレート IT に関わる人の方が多かった。今後、デジタル・トランスフォーメーション（通称：DX）※256 の進展により顧客のフロントライン業務の IT 化が進むと、ビジネス IT のセキュリティを担う登録セキスペが増えていくことが予測される。

(c) 登録セキスペの分類（セキュリティサービス提供形態）

図 2-3-13（前ページ）の「顧客の IT の企画・開発・構築・運用・監査などを請け負う」人が、どのような形態でセキュリティサービスを提供しているかを確認した（図 2-3-15）。

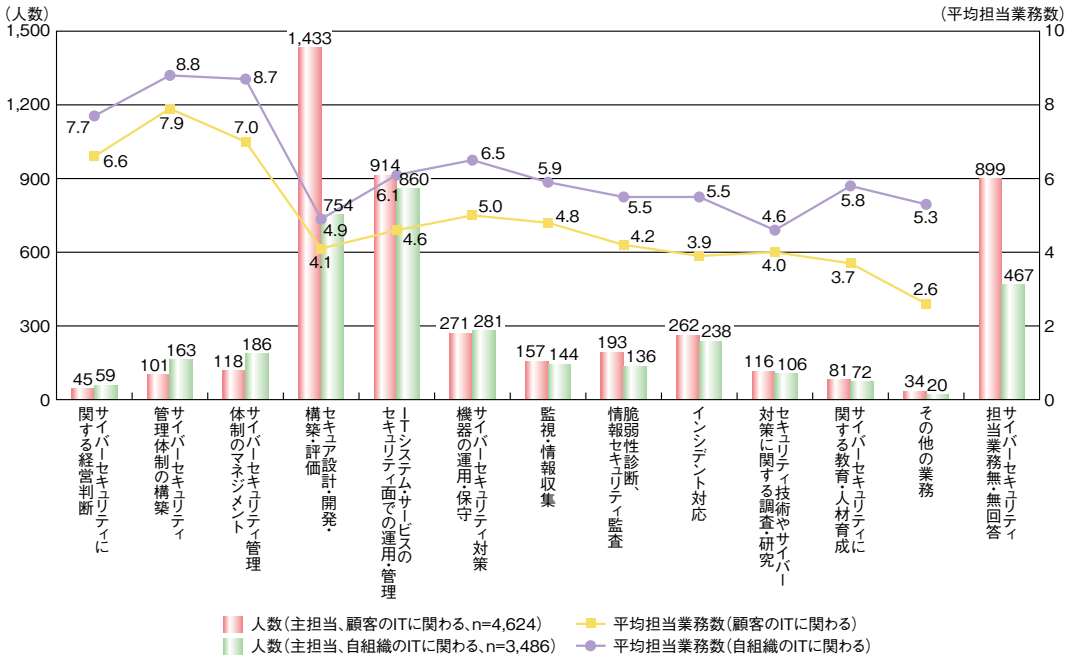
ここで興味深いのは、「情報セキュリティ対策サービス提供に関わらない部署に所属」の回答者が 3 割強いた点である。この回答者は、別の設問で「サイバーセキュリティ業務を担当している」と回答していることが多く、セキュリティサービスを明示的に行っていない部門にあって、セキュリティ対策関連業務を行っている人が一定数いることが分かった。



■図 2-3-15 「顧客の IT の企画・開発・構築・運用・監査などを請け負う」を選択した登録セキスペのセキュリティサービス提供形態（n=4,624）

(d) サイバーセキュリティ関連業務の担当者数と平均担当業務数

12 のサイバーセキュリティ関連業務を定義し、登録セキスペがどの業務を担当しているか、「自組織で活用する IT の企画・構築・管理に関わる人（自組織の IT に関わる人）」と「顧客の IT の企画・開発・構築・運用・監査などを請け負う人（顧客の IT に関わる人）」に分けて集計した。結果を図 2-3-16 に示す。なお、担当業務の複数回答を可としている。主担当業務としては、「セキュア設計・開発・構築・評価」及び「IT システム・サービ



■図 2-3-16 サイバーセキュリティ関連業務の担当者数（主担当）と平均担当業務数

スのセキュリティ面での運用・管理」の担当者が多いことが分かる。また平均担当業務数を見ると、特に上流の業務（経営判断や管理体制の構築等）において、業務を複数担当している人が多いことが分かる。

複数の業務を担当している人が多いことから、担当業務のまとまりを分析することで、登録セキスペの人材タイプが見えてきている。その人材タイプのうち主なものは、以下の三つである。

- セキュリティ管理系業務を中心にセキュリティ対策業務を全般的に担当する人材
- IT ライフサイクル全般に幅広く関わりセキュリティ確保をする人材
- 設計開発・運用系の業務をセキュアに実施する人材

これらに分類される人材数を合計すると、何らかのサイバーセキュリティ対策関連業務を担当する登録セキスペの中の約 8 割を占める。

上記の三つの人材タイプに分類される人材は、サイバーセキュリティ関連業務を専業とする人よりも、本来の業務を遂行する中でセキュリティスキルを活用する「プラス・セキュリティ人材※257」が多いと考えられる。これらの実態を基に、登録セキスペの活躍促進に向け、官民で連携したさらなる調査や制度拡充等の取り組みが望まれる。

2.3.4 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。

2018 年 8 月 14 ～ 18 日に東京で 15 回目となる全国大会が開催され、85 名が参加した※258。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（兵庫／高知／山梨／三重／北海道／愛媛／岡山／石川／沖縄／秋田／福岡）で開催された※259。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※260。

その他、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、第 2 回セキュリティ・コアキャンプが 2018 年 8 月 16 日に東京で開催された※261。また、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 2019 年 3 月 15 日に東京で開催された※262。

(2) SecHack365

SecHack365 は、25 歳以下の学生や社会人約 40 名を対象に、セキュリティに関わるモノづくりができる人材の育成を目的として NICT が主催する長期ハッカソン※263で、2017 年度から日本全国各地において開催されている※264。2019 年 3 月 8 日に東京で行われた成果発表会では、本プログラムの優秀者による発表のほか、トレーナー陣によるパネルディスカッションが行われた※265。

(3) 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、2018 年度は大学等 37 校、連携企業等 35 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、410 名が修了認定を取得した※266。

上記以外では、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 2017 年度に開始されている※267。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というプロ人材育成のための教育コースを幅広く展開している※268。

(4) SECCON 2018

JNSAは、日本における最大規模のCTF※269大会である「SECCON 2018※270」を開催した。

2018年12月22～23日の国際決勝大会では、80ヵ国1,407チーム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4、韓国5、台湾3、中国1、ウクライナ1、インドネシア1）が集まり、実力を競い合った。今回、死闘を征し第1位を獲得したのは日本チーム「TSG」で、経済産業大臣賞の栄誉に輝いた。これまで韓国のチームが4年連続で第1位であったが、2018年度はSECCON国際大会史上初めて第1位～第3位を日本勢が独占した※271。

SECCONではその他、CTF未経験者でも参加可能な「SECCON Beginners※272」や、情報セキュリティに興味がある女性を対象とした「CTF for GIRLS※273」等のイベントを定期的に開催しており、実践的情報セキュリティ人材の発掘・育成、技術の実践の場の提供に取り組んでいる。

(5) 産学情報セキュリティ人材育成交流会

JNSAの産学情報セキュリティ人材育成交流会は、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。2018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～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－～」を2018年4月28日に開催した。2018年度は企業15社がインターンシップを実施した※274。

2.4 組織・個人における情報セキュリティの取り組み

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基に述べる。

2.4.1 企業における対策状況

情報セキュリティマネジメントに対する企業等の経営層の関与、セキュリティ体制構築、セキュリティ対策への取り組み状況や情報セキュリティマネジメントシステム認証の動向について述べる。

(1) 経営層のセキュリティに対する関与と体制構築を含めた対策状況

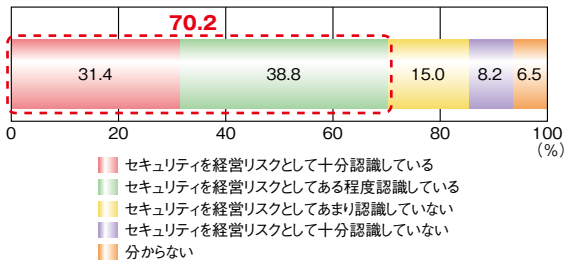
サイバー攻撃による企業の被害を最小化するには、セキュリティ担当部門だけでなく事業部門等も交えて対策を推進することが必要となる。事業活動の中でセキュリティ対策をどの程度優先するかについては、全社的な視点での俯瞰・判断が不可欠であることから、経営層が主体的にサイバーセキュリティ対策に取り組むことが重要である。企業の情報セキュリティ対策状況について、以下の資料を基に述べる。

- トレンドマイクロ株式会社（以下、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 2018 年版※275（国内企業 1,132 社及び官公庁自治体：323 団体を対象に調査。以下、トレンドマイクロ社調査）
- 一般社団法人日本情報システムユーザー協会（Japan Users Association of Information Systems；JUAS）：企業 IT 動向調査 2019（2018 年度調査）※276（国内企業 1,103 社を対象に調査。以下、JUAS 調査）
- NRI セキュアテクノロジーズ株式会社：企業における情報セキュリティ実態調査 2018※277（国内・海外企業 1,110 社を対象に調査。以下、NRI セキュアテクノロジーズ社調査）

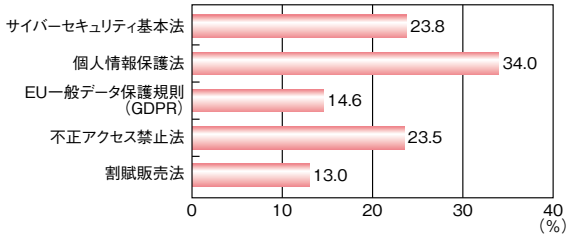
(a) 経営層のセキュリティ関与

情報セキュリティに関する企業経営層のリスク認識について、トレンドマイクロ社調査によると、図 2-4-1 に示すように、セキュリティを経営リスクとして認識している経営層※278 は 70.2%と高い割合となった。ただし、「セキュリティを経営リスクとして十分認識している」経営層の割合は 31.4%にとどまっている。

また、サイバーセキュリティ基本法等の法規制の内容を理解した上でセキュリティ対策に十分に反映させている割合は、最も高い「個人情報保護法」でも 34.0% にとどまっている（図 2-4-2）。



■図 2-4-1　経営層のリスク認識（n=1,455）
（出典）トレンドマイクロ社調査を基に IPA が作成



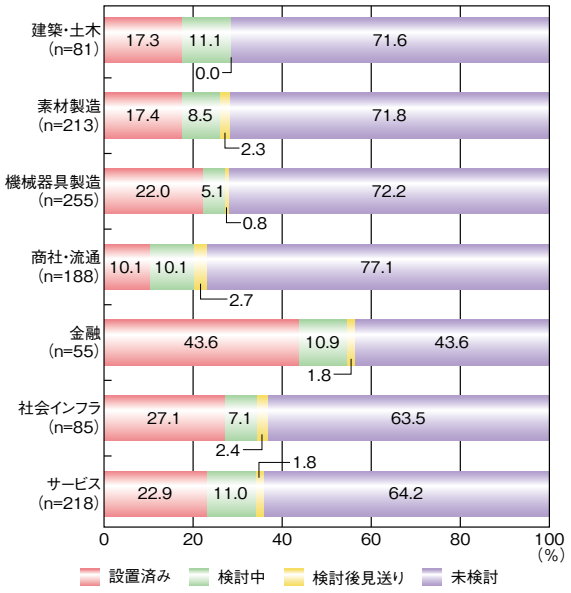
■図 2-4-2　法規制の理解・対策反映度（n=1,455）
（出典）トレンドマイクロ社調査を基に IPA が作成

経営層のセキュリティのリスク認識は高まっているものの、セキュリティを経営リスクとして十分に認識している経営層の割合や、法規制の内容をセキュリティ対策に反映させている割合から、具体的な行動に結びついていない企業がまだ多いと推測される。

(b) セキュリティ関連役職者とセキュリティ担当組織の設置状況

企業におけるセキュリティ関連役職者の設置状況について、JUAS 調査を基に述べる。図 2-4-3（次ページ）に示すように、CISO 設置済み企業の割合は、業種別に見ると「金融」が 43.6%と高く、次いで「社会インフラ」が 27.1%であった。しかし、その他の業種では「設置済み」「検討中」を合計しても 1 割台半ばから 3 割程度であった。なお、金融が突出しているのは、PCI DSS（Payment Card Industry Data Security Standard）や金融庁の安全対策基準等、セキュリティ基準への準拠やコンプライアンスを重視していることが理由として考えられる。

NRI セキュアテクノロジーズ社調査によると、CISO に



■図 2-4-3　企業における CISO 設置状況（n=1,095）
（出典）JUAS 調査を基に IPA が作成

経営層が就任している企業の割合は、国内企業が 35.5% であるのに対し、米国企業は 71.2%と、ほぼ倍であった。CSIRT の構築状況についても、現在構築中の企業まで含めると国内企業が 43.9% であるのに対し、米国企業は 78.8% と、倍近い差となった。

(c) セキュリティ対策状況

セキュリティ対策状況について、NRI セキュアテクノロジーズ社調査を基に述べる。セキュリティ対策評価を定期的に実施している割合は、国内企業が 41.1%であるのに対し、米国企業は 78.4%であり、日米で対策の実施割合に大きな差がある。

情報セキュリティ対策実施のきっかけとなるイベントの 1 位が、国内企業では「自社のセキュリティインシデント」であるのに対し、米国企業では「経営層のトップダウン指示」であった。また、セキュリティ担当者として最も対応に困っていることの 1 位は、国内企業では「セキュリティインシデント発生時の緊急対応」であるのに対し、米国では「セキュリティ対策のトレンド・他社動向の把握」であった。国内企業では、セキュリティ対策の計画スパンが「短期計画（1 年程度）」である割合が 42.1% と最も高く、そもそも 28.9% が計画自体を策定していなかった。それに対し、米国では「中長期計画（3 年程度）」である割合が 49.0% と最も高くなっていた。

(d) まとめ

以上のように、国内企業における経営層のセキュリティのリスク認識は高いものの、経営層の指示による計画的な対策実施はまだこれからであると思われる。例えば CSIRT 等の体制構築を含めた対策が十分でなく、結果としてセキュリティインシデント発生時の緊急対応に困難が生じている状況であることが推測される。今後は、経営層のセキュリティ対策に対する関与を深め、体制構築を進めると同時に、セキュリティ対策に関する情報収集を行って関係者で共有していくことが課題となると考えられる。

(2) セキュリティリスクマネジメントとセキュリティガバナンス

2018 年 7 月に閣議決定された「サイバーセキュリティ戦略」では、「サイバーセキュリティに係るリスクは企業が直面する様々なリスクの一つであり、その対策をリスクマネジメントの一環としてとらえ、業種・業態等の状況に応じて、自然な形で対策が組織に浸透していくことが重要である」と述べられている。本項では、そのために必須となる各種取り組みを紹介する。

(a) サイバーリスクの数値化

セキュリティリスクマネジメントを推進するためには、経営者が「サイバーリスクは経営リスクの一つである」と正しく認識する必要がある。

一般社団法人日本サイバーセキュリティ・イノベーション委員会（Japan Cybersecurity Innovation Committee：JCIC）は、2018 年 9 月に「取締役会で議論するためのサイバーリスクの数値化モデル※279」を発表した。これによると、日本企業の取締役会でサイバーリスクが議論されていない主な原因の一つとして「取締役が共通で理解できる指標が存在しない」ことを挙げている。そこで、サイバーリスクの金額換算を行い、IT に詳しくなくともリスクを把握できるようにする必要があるとしている。

本モデルでは各種調査結果を基に、セキュリティ事故発生時の想定損失額を、直接被害（①個人情報漏えいによる金銭被害、②ビジネス停止による機会損失、③法令違反による制裁金、④事故対応費用）と間接被害（⑤純利益への影響、⑥時価総額への影響）の観点から算出する。これと併せて、自社のセキュリティ対策ベンチマーク結果や業界標準を満たすためのセキュリティ投資額を報告することで、取締役会でのサイバーセキュリティリスクに関する議論が進み、取締役を含む経営者がサイバーリスクを経営リスクの一つとしてとらえるようになる、としている。

なお、JCICでは、保有する個人情報数等を入力することで「想定損失額の目安」を算出できる「サイバーリスク指標モデル『想定損失額の目安』簡易シミュレーション※280」も公開している（図2-4-4）。

■図2-4-4　サイバーリスク指標モデル「想定損失額の目安」（簡易版）
（出典）JCIC「サイバーリスク指標モデル『想定損失額の目安』簡易シミュレーション」

(b) サイバーセキュリティ体制の在り方

JUASは「企業におけるサイバーセキュリティ体制の構築及び戦略マネジメント層の育成に関する実態調査※281」を実施し、サイバーセキュリティ体制の実態と望ましい形態についてのまとめを2019年3月に公表した。

この調査ではセキュリティ体制を、セキュリティ組織形態（「専門組織型」／「委員会型」）と機能分担（全社がセキュリティ対策を一元管理する「集権型」／事業部門が固有システムのセキュリティ対策を担当する「連邦型」）の2軸で分類し、4パターンに類型化している。また、「サイバーセキュリティ経営ガイドラインVer 2.0」の付録A「サイバーセキュリティ経営チェックリスト」を活用し、組織の「セキュリティ成熟度」を指標化している。更に、各組織の特徴に応じた最適なセキュリティ体制が確立されていることを「セキュリティ成熟度が高い」と定義し、セキュリティ成熟度に影響を与える因子として、「経営者の認識・意識」と「事業形態（BtoB/BtoBtoC/BtoC、単一／多角化など）」を想定し、以下のように実態を分析している。

- セキュリティ成熟度が高い程、経営の関与度が高く、意思決定者も経営に近くなる傾向が見られる。経営者が経営リスクの一環としてセキュリティを認識するだけでなく、セキュリティ意思決定の最上位者となることでトップダウンの推進が容易になり、成熟度を高めることにつながっていると考えられる。
- 「単一事業が中心」である企業群は「事業が多角化している／しようとしている」企業群より成熟度が高い傾向がみられる。多角化すると事業が複雑化しやすいため、単一事業の方が比較的ガバナンスが効きやすいことが影響していると考えられる。
- 事業形態がBtoB、BtoBtoC、BtoCの順でセキュリティ成熟度が高くなる傾向が見られる。最終顧客である一般消費者に近づくにつれて、レピュテーションリスク等の影響が意識され、セキュリティガバナンスを高めようとする意識が強く働くのではないかと推察される。
- 事業に求めるスピード感やリスクのとらえ方は企業によって異なり、最適な体制の在り方は各社各様なため、個社事業に合わせて「集権型」「連邦型」を採用していると考えられる。ただしガバナンス展開のしやすさという点では「集権型」のほうが展開しやすい傾向が見て取れる。

(c) サイバーセキュリティ対策の在り方

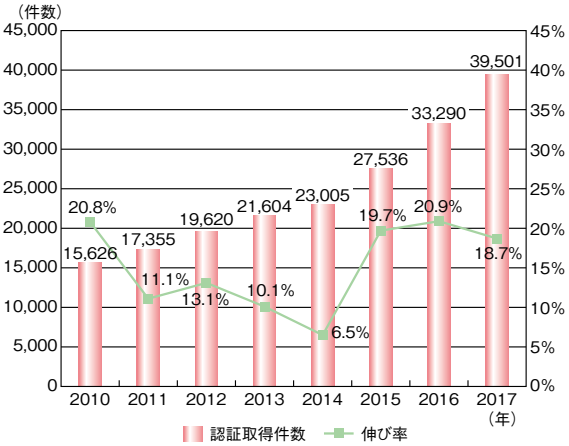
経済産業省のコーポレート・ガバナンス・システム研究会で取りまとめられている「グループ・ガバナンス・システムに関する実務指針（仮）※282」では、サイバーセキュリティ対策の在り方として「内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、親会社の取締役会レベルで、子会社も含めたグループ全体としてセキュリティ対策を行うことを検討すべき」としており、実際の対策検討に際しては、「サイバーセキュリティ経営ガイドライン」等を適宜参照することとしている。

また同省の産業サイバーセキュリティ研究会WG2において、現場向けの施策として「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るための事例集作成が挙げられた。これは「サイバーセキュリティ経営ガイドライン」の内容について認識をしている企業は増加しているものの、ガイドライン記載の「重要10項目」に対する具体的な対策の実施へ結びつける上での課題を感じている企業も多いとの声が以前よりあったためである。

これを受けてIPAでは「サイバーセキュリティ経営プラクティス検討会※283」を発足させ、同検討会での議論を踏まえながら、企業での実際の取り組み事例を収集、整理し、分かりやすく類型化した「サイバーセキュリティ経営ガイドラインVer 2.0実践のためのプラクティス集※5」を作成し、2019年3月に発行した（次ページ図2-4-5）。

本プラクティス集には、これからサイバーセキュリティ対策に取り組む企業が「重要10項目」を実践するにあたっての手順や考え方、ヒントがまとめられている。サイバーセキュリティ対策を何から始めるべきかという課題を感じている企業の経営者やセキュリティ担当者の一助となることが期待される。

■図 2-4-5　プラクティス集の記載例（セキュリティ対策実践者における“よくある”「悩み」とそれに対する「取組み」）
（出典）IPA「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集」



■図 2-4-6　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 Survey 2017※284」を基に IPA が作成

(3) 情報セキュリティマネジメント

ビジネス環境の変化等により、組織が保有する情報資産やシステムの種類・重要性も変化している。またサイバー攻撃が多様化、高度化し、対策のための製品やサービスも増加している。組織はこれらの変化を踏まえ、経営リスクを適宜見直し、適切なセキュリティ対策が取られているかを確認し、必要な処理を実施しなければならない。このような組織的な活動をマネジメントシステムと呼ぶ。マネジメントシステムが推奨する PDCA（Plan-Do-Check-Act）は、これら一連の活動を実現する方法の一つであり、多くの組織が取り組んでいる。また、マネジメントシステムの構築と運用を客観的に評価できる方法として、認証取得を目指す企業も多い。

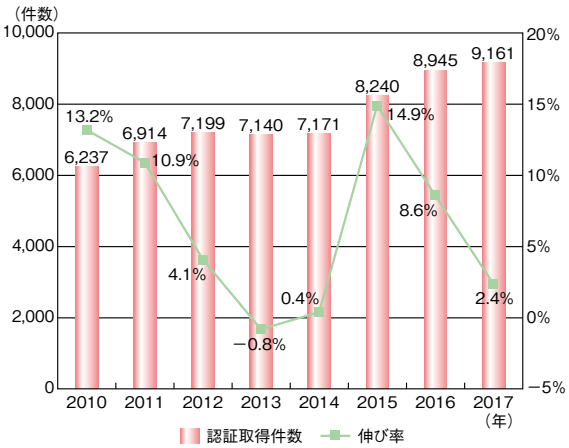
ここでは情報セキュリティマネジメントシステム（Information Security Management System：ISMS）認証やプライバシーマーク制度等のマネジメントシステム認証の現状を述べる。

(a) 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

ISO の最新の公開情報によると 2017 年の世界の ISO/IEC 27001 認証取得件数は、2016 年と比較して 18.7% 増加し、合計で 3 万 9,501 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 2-4-6 に示す。

「ISO Survey 2017」は、ISO/IEC 27001（ISMS）以外にも ISO 9001（QMS）や ISO 14001（EMS）等、全部で 10 の ISO 規格を対象としている。このうち 2015 年以前より調査が行われている八つの規格について取得件数の伸び率を比較すると、ISMS 以外の七つの規格は -4.3% ～ 13.1% であるのに対して ISMS は 18.7%と最も高い伸び率であった。このことからも、認証制度として ISMS の注目度の高さがうかがえる。

国別の取得件数の上位 5 ヵ国は、1 位日本（9,161 件）、2 位中国（5,069 件）、3 位英国（4,503 件）、4 位インド（3,272 件）、5 位米国（1,517 件）であり、日本は常に 1 位を保っている。しかし、図 2-4-7 に示すように日本の ISMS 認証取得件数の伸び率は 2.4% とわずかである。一方、中国の伸び率は 93.6%、英国の伸び率は 33.7% と勢いが衰えていない。2017 年 6 月に施行された中華人民共和国網絡安全法や 2018 年 5 月に発効された GDPR が中国、英国の取得件数増加の要因として考えられる。



■図 2-4-7　日本の ISO/IEC 27001 の年間認証取得件数と伸び率
（出典）「ISO Survey 2017」を基に IPA が作成

(b) プライバシーマーク制度の動向

プライバシーマーク制度は、日本工業規格※285「JIS Q 15001 個人情報保護マネジメントシステム−要求事項」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評価して、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、20 年間でプライバシーマークの付与事業者数は 1 万 6,275 事業者（2019 年 3 月末時点）となっている※286。

プライバシーマーク付与事業者の個人情報の取り扱いにおける事故については、認定個人情報保護団体や審査機関等に対して事業者からの報告が義務づけられている。事故には、個人情報の漏えい、紛失、滅失・き損、改ざん、正確性の未確保、不正・不適正取得、目的外利用・提供、不正利用、開示等の求め等の拒否、及びこれらの恐れが含まれている。

認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（JIPDEC）が 2018 年 8 月に公表した「（平成 29 年度）『個人情報の取り扱いにおける事故報告に見る傾向と注意点』※287」によると、2017 年度は 911 の付与事業者より、2,399 件の事故報告があった。事故の原因としては「メール誤送信」が 26.5% と最も多く、次いで「紛失」「その他漏えい等」が挙げられた。JIPDEC はメール誤送信が大幅に増加していることに対して、事業者向け啓発資料「メール誤送信事故を起こさないために※288」を公開し、事故防止の参考や従業者向け教材等としての活用を促している。

2.4.2 中小企業に向けた情報セキュリティ支援策

本項では、中小企業に向けた情報セキュリティ支援策の現状を紹介する。

(1) 中小企業のセキュリティ対策状況と JC 版サイバーセキュリティ問題解決プログラム

公益社団法人日本青年会議所（Junior Chamber International Japan：JCI-Japan）が 2018 年 7 月に公開した「中小企業に対するサイバーセキュリティ意識調査分析レポート※289」によると、IT の使用が業務上「必須」、または「一部必須」と回答した企業が合計で 95.9% に上っている。その一方で、「経営者がサイバーセキュリティを経営リスクの 1 つとして認識している」企業は 47.2% であった。また、サイバーセキュリティ経営ガイドラインへの取り組み状況について、「組織内にサイバーセキュリティリスク管理体制を考えていない」企業は 61.8%、「サイバーセキュリティ対策のための予算や人材の確保はできていない」企業は 61.1%、「系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握ができていない」企業は 74.7% であり、十分とはいえない状況であった。そこで JCI-Japan では、アクションプラン「JC 版サイバーセキュリティ問題解決プログラム※290」を発表し、動画や啓発資料を活用して、中小企業経営者及び個人事業主のセキュリティ意識の向上に取り組んでいる。

(2) SECURITY ACTION による対策推進

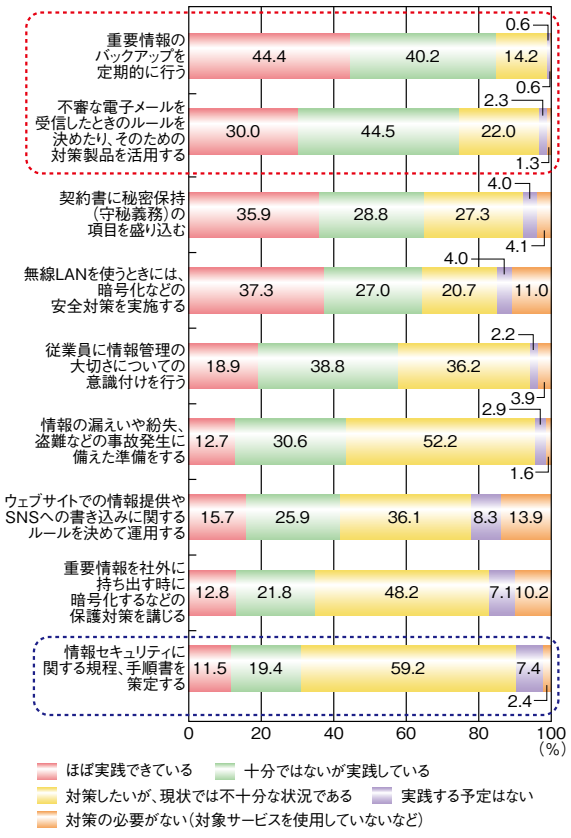
IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION※291」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及活動を行っている。

IPA が 2019 年 3 月に公開した「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査－調査報告書－※292」によると、宣言事業者における情報セキュリティ対策の取り組み状況について「ほぼ実践できている」と「十分ではないが実践している」を合計すると、「重要情報のバックアップを定期的に行う」が 84.6% と最も高く、次いで「不審な電子メールを受信したときのルールを決めたり、そのための対策製品を活用する」が 74.5% と続いている。一方で、「情報セキュリティに関する規程、手順書を策定する」は、30.9% にとどまっている（次ページ図 2-4-8）。

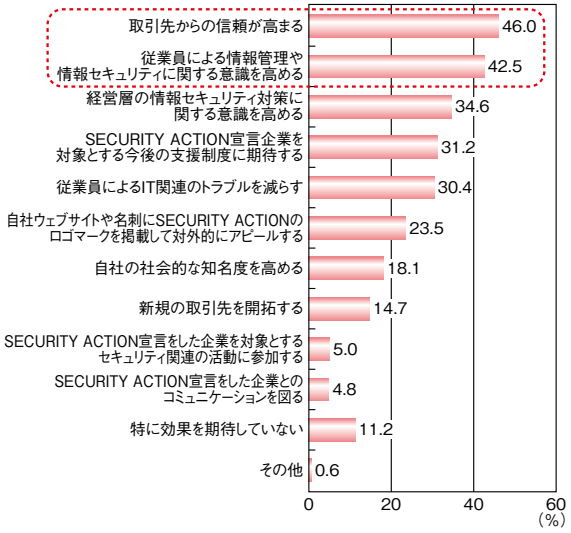
情報セキュリティの確保のためには、技術的な対策とマネジメント的な対策を両輪として進めていく必要がある。今後、規程や手順書の策定に取り組むことが望まれる。

SECURITY ACTION 宣言をしたことによる効果への期待は、「取引先からの信頼が高まる」が 46.0% と最も高く、次いで「従業員による情報管理や情報セキュリティに関する意識を高める」が 42.5% であった（次ページ図 2-4-9）。このことから、SECURITY ACTION に対して、自社従業員の意識を高め自発的に情報セキュリティ対策の取り組みを促すという本来の目的のみならず、社外への信頼性アピールという副次的効果に期待している企業も多いことが分かる。

SECURITY ACTION は、経済産業省が実施する「平成 30 年度補正サービス等生産性向上 IT 導入支援事業※293」（通称：IT 導入補助金）において 2018 年度に引き続き申請要件となり、また公益財団法人東京都中小企業振興公社が実施する「平成 30 年度 サイバー



■図 2-4-8　情報セキュリティ対策の取り組み状況（n=5,162）
（出典）IPA「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査ー調査報告書ー」を基に編集



■図 2-4-9　SECURITY ACTION 宣言で期待した効果（複数回答可、n=5,162）
（出典）IPA「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査ー調査報告書ー」を基に編集

セキュリティ対策促進助成事業※294」において申請要件になる等、公的にも広く活用されている。

2019 年 3 月末時点の宣言事業者は 6 万者を超えている。今後より多くの中小企業が SECURITY ACTION 宣言を行い、社内の意識付けや社外への信頼性のアピールに活用し、対策を推進することが望まれる。

(3) 中小企業の情報セキュリティ対策ガイドライン

2019 年 3 月、IPA は、中小企業における情報セキュリティ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 3 版※295」を公開した（図 2-4-10）。

中小企業の情報セキュリティ対策ガイドラインの第 1 部「経営者編」では、経営者が認識すべき「3 原則」、経営者が実施しなければならない「重要 7 項目の取組」を挙げて解説しており、2017 年 12 月に改訂された「サイバーセキュリティ経営ガイドライン Ver 2.0」の内容をコンパクトにまとめたものとなっている。第 2 部「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。また、実践編を進めるための各種ツール（「リスク分析シート」「情報セキュリティ関連規程（サンプル）」等）を付録として提供している。第 3 版では、中小企業においても活用が期待されるクラウドサービスについて、安全に利用するための「中小企業のためのクラウドサービス安全利用の手引き」を追加するとともに、旧版の利用者からの意見を参考に一層分かりやすく実践しやすい内容に改訂している。

■図 2-4-10　中小企業の情報セキュリティ対策ガイドライン第 3 版

(4) 神奈川県企業サイバーセキュリティ官民合同プロジェクト

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。2018 年 11 月、神奈川県警察が事務局となり、企業や大学、研究機関

のほか、行政、企業の支援機関等、26 団体が参加した「神奈川県企業サイバーセキュリティ官民合同プロジェクト※296」が発足した。サイバー犯罪の脅威に関する情報共有や効果的な対策の検討、中小企業への普及啓発を柱に活動を進めている。

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

教育機関、政府、地方公共団体等法人の情報セキュリティ対策の状況について、公表されている資料等を基に述べる。

(1) 教育機関における対策状況

教育機関の情報セキュリティ対策の状況について述べる。

(a) 教育機関におけるインシデント

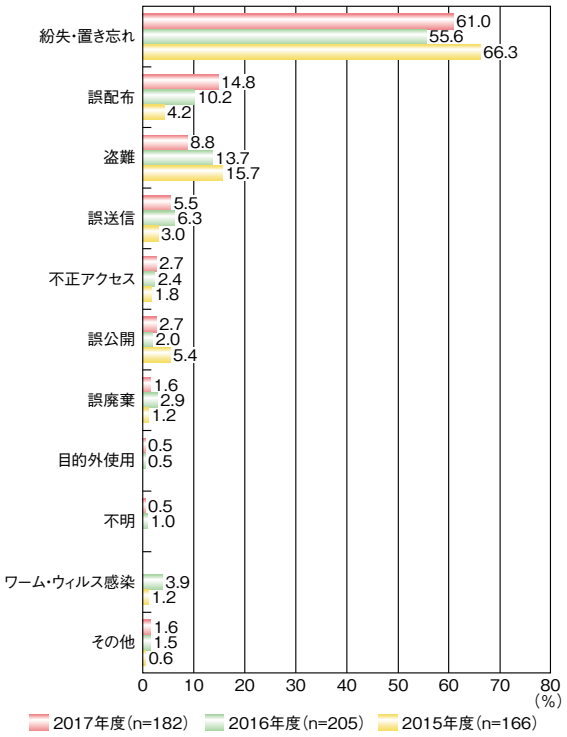
教育ネットワーク情報セキュリティ推進委員会（Information Security for Education Network：ISEN）では、学校、公的教育機関、関連組織で発生した、児童・生徒・保護者等の個人情報を含む情報の紛失・漏えい事故について公開情報を調査し、集計した結果を「学校教育機関における個人情報漏えい事故の発生状況−調査報告書−」（以下、ISEN 調査報告書）として毎年公表している。

ISEN 調査報告書※297 によると、2017 年度に教育機関において発生した個人情報漏えいに係るセキュリティインシデント数は 182 件に上った（2016 年度は 207 件、2015 年度は 169 件※298）。

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 2-4-11 に示す。最も割合が高いのは「紛失・置き忘れ」（2017 年度は 61.0%）であり、過去 3 年間にわたって第 1 位となっている。次いで「誤配布」（2017 年度は 14.8%）、「盗難」（2017 年度は 8.8%）となっている。なお、ISEN 調査報告書によると、情報漏えい経路・媒体の割合は「書類（紙の書類のみ）」が 60.0% と最も高く、次いで「USB メモリ」が 15.8% となっている。

次に、2018 年度の主なセキュリティインシデントを表 2-4-1（次ページ）に示す。ここでは、大学の事例を挙げている。

2018 年 4 月から 6 月にかけて連続してフィッシングによる被害が発生したことから、2018 年 6 月 27 日、文部科学省が全国の大学に対して対策を強化するように注意喚起を行った※306。この注意喚起にもかかわらず、フィッシングによる大学からの情報漏えいの被害は続いており、一層の対策強化が求められる。



■図 2-4-11　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
（出典）ISEN 調査報告書を基に IPA が作成

大学以外の教育機関でもセキュリティインシデントは発生している。2018 年 7 月 6 日、兵庫県の国立明石工業高等専門学校は、受験生の名前や過去の在校生の成績等、延べ 2,316 人分の個人情報が記載された資料が学生 4 名に持ち去られていたと公表した※307。

また 2019 年 2 月 4 日、取手市は、取手市立取手小学校の学校代表メールアカウントが不正アクセスを受け、同年 1 月 11 日から 21 日にかけて当該メールアカウントから外部に 1,523 件のスパムメールが送信されたと公表した※308。

(b) 教育機関の取り組み

2018 年 7 月 27 日に閣議決定された「サイバーセキュリティ戦略」では、新たに取り組むべき課題として「大学等における安全・安心な教育・研究環境の確保」が挙げられ、安全・安心な教育・研究環境を確保するためには、大学等が自律的にサイバーセキュリティ対策を行うとともに、サイバー攻撃に連携・協力して対応する体制の構築や情報共有等を国が積極的に支援することが重要であるとした。今後、文部科学省、国立情報学研究所（National Institute of Informatics：NII）においてガイドライン等の策定・普及、訓練・演習の体系化と実施、

公表日	大学名	概要
2018 年 6 月 6 日	公立大学法人 横浜市立大学	教職員や学生に対して、メールサービスのログイン画面を偽装したサイトの URL へ誘導するフィッシングメールが送付された。当該 URL にアクセスし ID 及びパスワードを入力した 29 名宛に届いた 3,512 通のメールが不正に外部へ転送され、差出人氏名とメールアドレス等の情報が漏えいした。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の個人情報（2,282 件）も合わせると、計 5,794 件の情報漏えいとなった※299。
6 月 22 日	学校法人 北海道科学大学	教員が学部生と北海道薬科大学の卒業生の氏名、学生番号、教職員の氏名、メールアドレス、当該教員の所属学会等の名簿、会議参加者の氏名や所属等の個人情報（約 3,000 件）を保存したノートパソコンを紛失した※300。
6 月 27 日	国立大学法人 弘前大学	教職員にフィッシングメールの送付があり、電子メールサービスのログイン画面に似せた偽サイトへ誘導され、12 名の教職員のパスワードが詐取された。これにより、これらのアカウントでメールが不正に外部へ転送され、メールアドレスを含む個人情報（4,974 件）が漏えいした※301。
10 月 24 日	学校法人 明治大学	外部からの不正アクセスによりメールアカウントが流失し、外部へスパムメールが送信された。更に、メール送受信データの一部がダウンロードされ、学生、教職員、卒業生及び学外者の個人情報（1,147 件）が漏えいした。同大学では 7 月にも同様の被害に遭っており、その対策を実施している過程で再度被害を受けた※302。
12 月 17 日	国立大学法人 兵庫教育大学	職員が大学のメールアドレス宛に届くメールを自身のフリーメールアドレスへ自動転送しており、このフリーメールが不正アクセスされ、第三者に閲覧されていた可能性があることが判明した。自動転送されたメールには、障害や病歴等が記述された要配慮個人情報を含む個人情報（1 万 1,322 人分）が含まれていた※303。
2019 年 1 月 30 日	国立大学法人 奈良先端科学 技術大学院大学	サーバの更新時にアクセス制御の設定を誤ったことで、学内に限定していた閲覧ページが、約 3 ヵ月学外からも閲覧可能な状態となっていた。当該ページには在校生と修了生の氏名と学生番号、求人情報を寄せていた企業の採用担当者の氏名等の個人情報（3,103 件）が掲載されていた※304。
2 月 19 日	学校法人 東京理科大学	教職員、学生及び卒業生に対しフィッシングメールが届き、教員 4 名及び学生 4 名のパスワードが詐取された。これらのメールアドレスに届いた 3,727 通のメールが不正に外部へ転送され、メールアドレスや氏名等を含む個人情報（3,538 件）が流出した※305。

■表 2-4-1　大学における主なセキュリティインシデント

インシデント対応体制の高度化等が検討される※4。

大学等の情報セキュリティに関する連携基盤としては、2017 年度から NII が情報セキュリティ運用連携サービス（NII Security Operation Collaboration Services：NII-SOCS）を運用しており、簡易なセキュリティ監視・解析、外部セキュリティ機関との情報共有等のサービスを提供している※309。

NII-SOCS での情報共有・連携にとどまらず、2018 年度には、国立大学法人の宮崎大学、大阪教育大、大阪大学、静岡大学の 4 大学が新たに日本コンピュータセキュリティインシデント対応チーム協議会に加盟した※310。

高度化するサイバー攻撃に対応するため、学術・研究領域にとどまらず、広く他業種の法人・団体との情報共有・連携を図って対応することが望まれる。

(2) 地方公共団体における対策状況

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、調査結果を「地方自治情報管理概要」の中で毎年公表している。本調査は、地方公共団体における行政情報化の推進状況について、47 都道府県、1,741 市区町村を対象に実施したもので、ここでは 2018 年度の調査結果※311 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 2-4-2 は、対策項目に関して、都道府県及び市区町村の実施率をまとめたものである。2018 年度と 2017 年度の実施率の差についても併せて記載している。全体的には 2017 年度と比較して、傾向に大きな変化は見られない。

「1. 組織体制・規程類の整備」については、情報セキュリティに関する体制は整備されているものの、市区町村の 44.9% が緊急時対応計画の整備ができておらず、インシデント発生時の対応の遅れ、被害の拡大等が懸念される。

「2. 情報資産の管理方法」については、50% 以上の市区町村において情報資産の機密性、完全性及び可用性による分類がなされておらず、また主要な情報資産の調査と調査結果に基づくリスク分析や、情報資産の把握と適正な管理も十分になされていない現状がうかがえる。

「3. 情報セキュリティ対策の実施」については、「サーバ室等の入退室管理を行っている」等の個別対策の実施率は、おおむね高いものの、「緊急時対応訓練を実施している」の実施率については都道府県で 74.5% にとどまり、市区町村では 26.2% と非常に低い。自治体が独力で訓練を計画・実施するのは難しい面もあるため、NICT

No.	対象項目	対策実施率	
		都道府県	市区町村
1. 組織体制・規程類の整備			
1	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)	98.7% (+0.6 ポイント)
2	緊急時対応計画を整備	97.9% (+4.3 ポイント)	55.1% (+5.4 ポイント)
2. 情報資産の管理方法			
3	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	100.0% (0.0 ポイント)	88.3% (+2.9 ポイント)
4	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% (0.0 ポイント)	49.7% (+5.1 ポイント)
5	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	68.1% (+4.3 ポイント)	38.3% (+2.1 ポイント)
3. 情報セキュリティ対策の実施 （1）物理的セキュリティ対策の実施			
6	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)	99.1% (+0.2 ポイント)
7	サーバ等への停電や免震対策を実施している	100.0% (0.0 ポイント)	98.6% (+0.2 ポイント)
8	重要な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)	97.4% (+0.8 ポイント)
9	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% (0.0 ポイント)	96.8% (+1.5 ポイント)
10	クラウドサービスやデータセンターを利用している	93.6% (+4.2 ポイント)	84.4% (+2.3 ポイント)
（2）人的セキュリティ対策の実施			
11	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)	89.6% (+2.8 ポイント)
12	緊急時対応訓練を実施している	74.5% (+6.4 ポイント)	26.2% (+3.4 ポイント)

No.	対象項目	対策実施率	
		都道府県	市区町村
（3）技術的セキュリティ対策の実施			
13	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% (0.0 ポイント)
14	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)	99.3% (+0.3 ポイント)
15	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)	99.0% (+0.4 ポイント)
16	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)	96.7% (+0.3 ポイント)
17	LGWAN 接続系において、OS及びアンチウイルスソフトウェアのプログラム更新を定期的に行っている	100.0% (－)	95.3% (－)
18	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)	91.7% (+1.6 ポイント)
19	重要なデータを暗号化し保存	80.9% (0.0 ポイント)	45.1% (+2.2 ポイント)
4. 情報セキュリティ対策の運用			
20	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	97.9% (+4.3 ポイント)	90.6% (+3.2 ポイント)
21	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	91.5% (+2.1 ポイント)	58.7% (+4.9 ポイント)
22	情報システムの運用等の業務委託事業者に対する指導・監査を実施している	59.6% (0.0 ポイント)	39.6% (+3.1 ポイント)
23	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	51.1% (+2.2 ポイント)	26.1% (+3.6 ポイント)

対策実施率の 1 行目の値は 2018 年度の値。2 行目の括弧付きの数値は 2017 年度の値との差。「－」記号の項目は、2017 年度と記載内容に変更があった項目。表中の色替えしている項目について注目して本文中に記載。

■表 2-4-2　地方公共団体における主な情報セキュリティ対策の実施状況（2018 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 30 年度）～」を基に IPA が作成

が主催する「実践的サイバー防御演習『CYDER』[※312]」等外部の演習プログラムを利用することも検討すべきと考えられる。

「4. 情報セキュリティ対策の運用」については、契約書等で情報漏えい防止策について業務委託事業者に義務づけてはいるものの、運用状況の指導・監査や、定期的な報告義務等の実施率は高くない。業務委託先からの情報漏えい等のインシデント発生リスクは潜在しており、各自治体の対策強化が求められる。

2.4.4 一般利用者における対策状況

IPA が実施した「2018 年度情報セキュリティの脅威に対する意識調査」[※313] の結果を基に、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) パソコン利用者のセキュリティ対策実施状況

パソコンのセキュリティ対策実施状況の調査結果によると、「WindowsUpdate などによるセキュリティパッチの更新」をしている割合は 55.7%（2017 年度から 4.2 ポイント増）、「セキュリティソフト・サービスの導入・活用」をしている割合は 60.9%（2017 年度から 2.4 ポイント増）で、どちらも半数以上が実施しており、更に 2017 年度よりも

増加している（図 2-4-12）。

一方、「不審な電子メールの添付ファイルは開かない」割合は 45.4%（2017 年度から 5.1 ポイント減）、「よく知らないウェブサイトではファイル（ソフトウェア）をダウンロードしない」割合は 38.4%（2017 年度から 6.0 ポイント減）である等、他の対策の実施率はいずれも減少している。

この理由として、セキュリティパッチの更新やセキュリティソフトの導入でウイルス感染への対策が十分である、という過信が一因となっている可能性が考えられる。これらの対策を実施していても、不用意にファイルをダウンロード、実行することでウイルス感染に至ることはある。リスク低減のためには、特定の対策のみに依存するのではなく、複合的な対策を講じておくことが望ましい。

(2) スマートデバイス利用者のセキュリティ対策実施状況

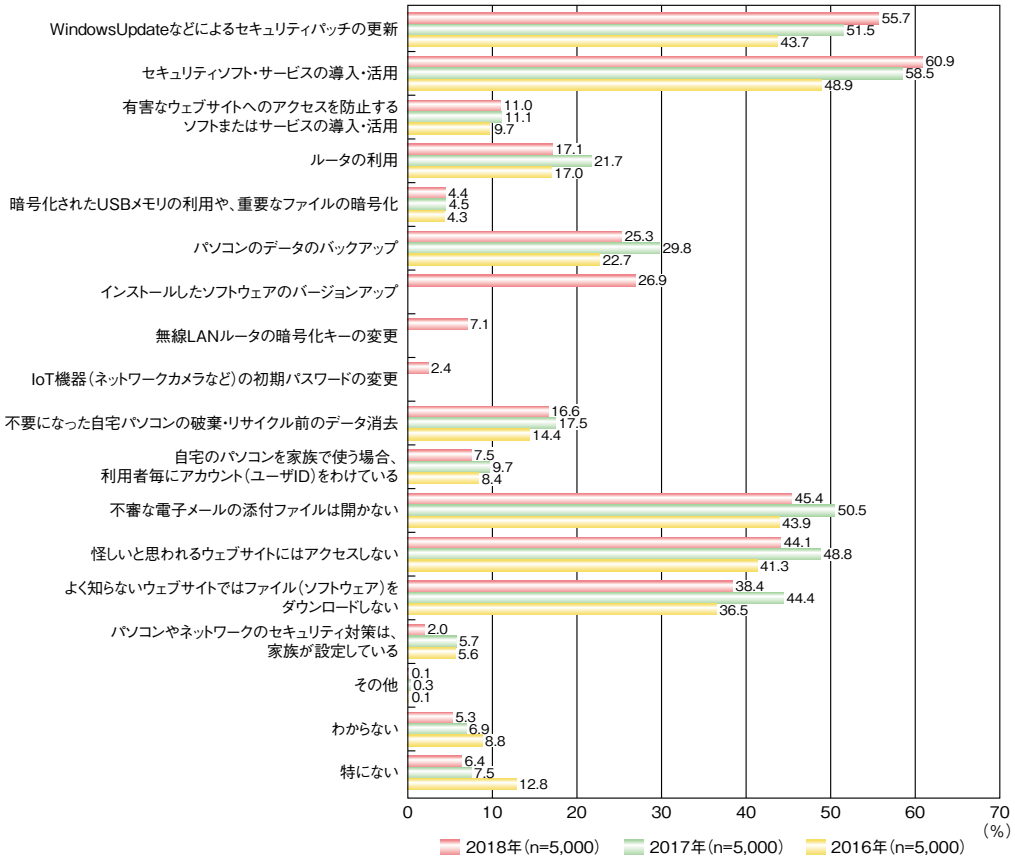
スマートフォンやタブレット端末等のスマートデバイスのセキュリティ対策実施状況の調査結果によると、「アプリをインストールする前または実行時に要求される権限を確認する」割合は 20.7%（2017 年度比から 1.6 ポイント増）と増加している一方で、「信頼できる場所（公式サイト）からアプリをインストールする」割合は 49.0%（2017 年度から 9.1 ポイント減）と減少している（図 2-4-13）。

不正アプリによる被害を防ぐためには、まずは信頼できる場所や開発元から提供されているアプリであるかを確認することが重要である。

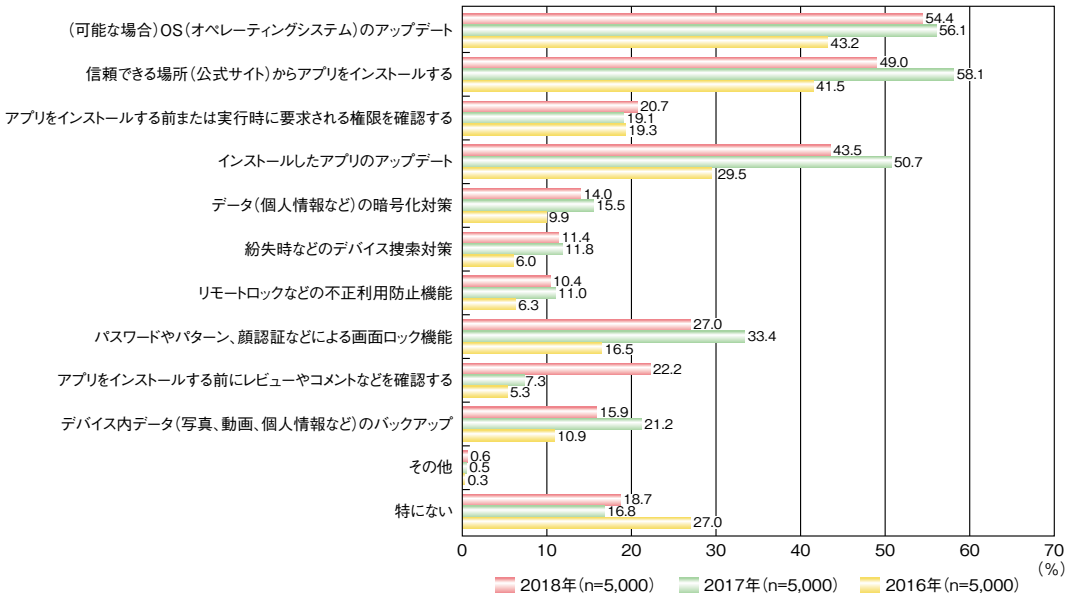
しかし、公式マーケットである GooglePlay や AppStore でも不正なアプリが公開されていた事例もある※314。そのため、アプリのレビューや要求される権限等の情報に不審な点がないかも確認した上で、インストールの可否を判断することが推奨される。なお、その判断が難しい場合には当該アプリの重要度や必要性に応じて、一時的にインストールを保留するといった慎重な対応を選択することが望ましい。

「パスワードやパターン、顔認証などによる画面ロック機能」を有効にしている割合は 27.0%（2017 年度から 6.4 ポイント減）と減少している。画面ロック機能は、主にスマートデバイス紛失時等に第三者の不正な利用を防ぐ対策となるが、日常的な利用では煩わしさを感じるものであることが減少の一因と考えられる。

しかし、警視庁の公開している遺失物取扱状況によれば、2018 年中の携帯電話類の遺失届は 257,718 件※315



■図 2-4-12　パソコン利用者のセキュリティ対策実施状況
（出典）IPA「2018 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



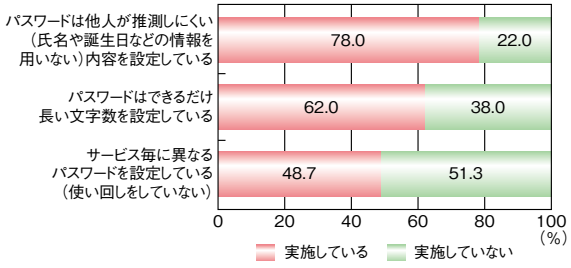
■図 2-4-13　スマートデバイス利用者のセキュリティ対策実施状況
（出典）IPA「2018 年度情報セキュリティの脅威に対する意識調査」を基に作成

であり、スマートデバイスの紛失は稀なことではない。また、知人のスマートフォンに無断で遠隔操作アプリをインストールしたとして、不正指令電磁的記録供用の疑いで書類送検された事案※316も発生している。スマートデバイスの紛失や放置による予期せぬ被害に発展することを防ぐため、画面ロック機能を始めとする第三者が容易に操作できない対策を講じておくことが推奨される（スマートフォンのセキュリティ対策については「3.3 スマートフォンの情報セキュリティ」参照）。

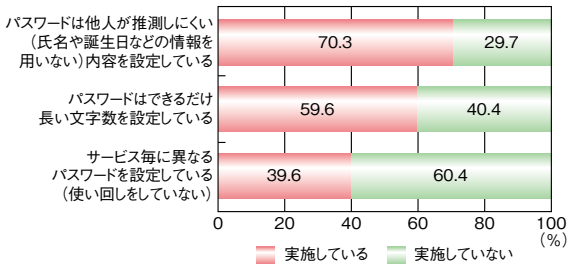
(3) パスワード設定の実施状況

インターネットサービスの利用における本人認証には、パスワードによる認証が広く用いられているため、パスワードが悪意ある第三者に知られてしまうとサービスを不正利用されてしまう恐れがある。サービスによっては、金銭被害に至る可能性もあることから、パスワードの適切な設定、管理による対策は必須と言える。

パスワード設定状況の調査結果によると、「パスワードはできるだけ長い文字数を設定している」割合はパソコンでは 62.0%、スマートデバイスでは 59.6%、「パスワードは他人が推測しにくい（氏名や誕生日などの情報を用いない）内容を設定している」割合はパソコンでは 78.0%、スマートデバイスでは 70.3%、「サービス毎に異なるパスワードを設定している（使い回しをしていない）」割合はパソコンでは 48.7%、スマートデバイスでは 39.6% である。いずれもスマートデバイス利用者の実施率が低くなっている（図 2-4-14、図 2-4-15）。



■図 2-4-14　パソコン利用者のパスワード設定の実施状況
（出典）IPA「2018 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 2-4-15　スマートデバイス利用者のパスワード設定の実施状況
（出典）IPA「2018 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、使い回しをしないことが肝要である。特に使い回しについては、2018 年度もパスワードリスト攻撃が原因とされる不正ログイン被害が多数確認されている（「1.2.6 パスワードリスト攻撃」参照）ことから、利用サービスごとに異なるパスワードを設定しておくことが強く推奨される。また、利用するサービスにおいて 2 段階認証が提供されている場合は、積極的に利用することが望ましい。

2.4.5 政府・公共機関による普及啓発活動

トレンドマイクロ社の「子どもと保護者のスマートフォン利用に関する実態調査 2018※317」によれば、子どもの7.3%、保護者の 18% がサイバー犯罪のトラブルを経験している。子どものサイバー犯罪に関するトラブルとしては「暴力、薬物、性的描写を含む有害サイトを閲覧した」が 2.9% と最も多く、モラルや意識不足に関するトラブルとしては「SNS に熱中して生活習慣に悪影響が出てしまった」が 14.7% と最も多い。ただし、子どもの 68.4%、保護者の 75.1%がトラブル経験は特になし、と回答している。

このような状況で、76.7%の家庭で子どもが安全にスマートフォンやインターネットを利用するためのセキュリティ教育を実施している、と回答しているが、SNS に投稿する写真のトラブルを知っている保護者はわずか 33.7%であるとしている。

こうした背景から、子どもとその保護者に対する情報セキュリティや情報モラルの教育は、現状では不十分と考えられ、官民を挙げて普及啓発活動を実施することが喫緊の課題である。

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及び情報リテラシーの向上を目的に実施された、政府・公共機関による普及啓発活動について述べる。

(1) 春のあんしんネット・新学期一斉行動

内閣府を始めとする関係府省庁では、「青少年有害環境対策※318」の一環として、ネットの危険から子ども守るための「春のあんしんネット・新学期一斉行動※319」を実施している(図 2-4-16)。

「春のあんしんネット・新学期一斉行動」では、多くの青少年が初めてスマートフォン等を手にする春の卒業・進学・新入学の時期に特に重点を置き、関係省庁、地方自治体、関係団体等と連携・協力して、スマートフォンや SNS 等の安全・安心な利用のための啓発活動等を集中的に展開し、家庭でのルール作り、積極的なフィルタリング、情報リテラシーの向上を目的とした各種取り組みを推進している。

(2) e-ネットキャラバンの実施

総務省と文部科学省では、インターネットの安心・安全な利用のため、「e-ネットキャラバン※321」において「小学生(中学年)～高校生向け」及び「その保護者・教職員等向け」に情報モラル教育(啓発・ガイダンス)として

■図 2-4-16 「春のあんしんネット・新学期一斉行動」普及啓発リーフレット
(出典)内閣府・内閣官房・警察庁・消費者庁・総務省・法務省・文部科学省・厚生労働省・経済産業省「普及啓発リーフレット集※320」

「全国規模で講師を派遣する出前講座」を行っている。

(3) 個人情報保護に関する標語コンテスト及び出前授業

内閣府の外局である個人情報保護委員会では、「個人情報の保護に関する法律についてのガイドライン」を公表※322しており、個人情報保護の啓発を推進するために、全国の小学生を対象とした標語コンテストを実施している※323。更に、個人情報保護制度や個人情報の扱いについて、子ども向けに作成したテキストや動画を使いながら、具体的な事例を交えた出前授業も実施している※324。

(4) 情報セキュリティ安心相談窓口

IPA では、一般的な情報セキュリティ(主にウイルスや不正アクセス)に関する技術的な相談に対してアドバイスを提供する窓口として、「情報セキュリティ安心相談窓口※325」(以下、相談窓口)を国民に向けて開設している。相談は電話・メール・FAX・郵送で受け付けている。

相談窓口に寄せられる相談内容等を基に、被害防止に向けた自己学習や普及啓発のための資料等として活用できるよう、「安心相談窓口だより※326」として情報セキュリティに関する様々なテーマをピックアップして紹介している。

(5) 情報モラル・セキュリティに関する標語・ポスター・4コマ漫画のコンクール

IPA では、児童・生徒・学生が標語、ポスター、4コマ漫画等の応募作品制作をとおして、情報モラルや情

報セキュリティについて考えるイベント「ひろげよう情報モラル・セキュリティコンクール※327」を開催している。開催にあたっては、NISCを始めとする政府機関、警察庁、各都道府県の教育機関や教育委員会、セキュリティベンダ、各種関連協会等の後援を得ており、2018年度は12月に各賞を公表した。

本コンクールには、小・中・高・高専生から標語作品55,524点、ポスター作品5,421点、4コマ漫画作品7,292点、書写（硬筆）2,395点、活動事例21点、総計70,653点の応募があり、このうち405作品が受賞した。（2018年度の受賞作品等については、本白書巻末の「第14回 IPA『ひろげよう情報モラル・セキュリティコンクール』2018受賞作品」を参照）。

(6)「インターネット安全教室」の実施

IPAでは、家庭や学校からインターネットにアクセスする一般利用者を対象にした「インターネット安全教室※328」を全国各地で実施している。同教室では、情報セキュリティの基礎知識だけでなく、情報リテラシーの向上を目指し、被害や事故にあったときにどのように対応すべきかを示す普及啓発ビデオを用いたセミナーを実施している。

また、前述の「ひろげよう情報モラル・セキュリティコンクール」の一環として以前より実施していた学校等への訪問授業は、2018年度から「インターネット安全教室」として実施している。

(7) サイバーセキュリティ月間

NISCが中核となり開催される「サイバーセキュリティ月間※329」（毎年2月1日から3月18日まで）では、政府・公共機関による全国展開のセミナーやイベント、ポスター掲示等の普及啓発活動が行われている。2018年度は、脅威に立ち向かう、といったイメージからアニメ作品「約束のネバーランド」とタイアップを実施した。「抗え。この世界（インターネット）の脅威に。」をキャッチコピーとして、2019年3月3日に同名のイベント※330が秋葉原で開催された。

(8) ツールの提供や情報発信

普及啓発活動の取り組みとして、情報セキュリティに関するツールの提供や情報発信も行われている。以下は無償で利用できるものであり、学校・家庭等において、情報セキュリティリテラシーや情報モラルの向上に役立てていただきたい。

- 「インターネットの安全・安心ハンドブック Ver.4.00※331」の作成、普及活用及びSNS等を用いた情報発信（NISC）

  学校の授業や家庭での利用を想定し、2019年1月に公開された（図2-4-17）。

■図2-4-17　インターネットの安全・安心ハンドブック
（出典）NISC「『インターネットの安全・安心ハンドブック』について※332」

- 大規模公開オンライン講座「これだけは知っておきたい公衆無線LANセキュリティ対策」の配信

  総務省公衆無線LANセキュリティ分科会の報告※333を基にした利用者への周知啓発事業として、2019年2～3月に開講した※334。公衆無線LAN利用時のセキュリティ対策に関する動画コンテンツを株式会社インプレスが作成し、株式会社ドコモ gaccoが公開オンライン講座プラットフォーム gaccoで配信を行った（図2-4-18）。

■図2-4-18　これだけは知っておきたい 公衆無線LAN セキュリティ対策
（出典）株式会社ドコモ gacco「これだけは知っておきたい公衆無線LAN セキュリティ対策」

- 情報セキュリティの脅威や対策を理解するための映像コンテンツ※335の公開（警視庁、IPA）

  2018年度以降では、例えばスマートフォン、パスワード、ネット家電の利用法に関する以下のコンテンツが公開

されている。

- 警視庁「サイバー犯罪被害防止対策用短編アニメーション映像※336」
- IPA「はじめまして、ペアコです。～親と子のスマホの約束～※337」（図 2-4-19）
- IPA「あなたのパスワードは大丈夫?～インターネットサービスの不正ログイン対策～※338」
- IPA「あなたの家も狙われている!? 家庭教師が教えるネット家電セキュリティ対策!※339」（図 2-4-20）

■図 2-4-19　はじめまして、ペアコです。～親と子のスマホの約束～

■図 2-4-20　あなたの家も狙われている !? 家庭教師が教えるネット家電セキュリティ対策!

2.4.6 団体・教育機関・学生・民間企業等による普及啓発活動

本項では、団体・教育機関・学生・民間企業等によるインターネット利用者向けの普及啓発活動について述べる。

(1) 一般財団法人草の根サイバーセキュリティ運動全国連絡会（Grafsec-J）

Grafsec-J は、地域において情報セキュリティ、情報モラル及び情報リテラシー向上のための普及啓発を実践する団体の交流・連携を支援している※340。その一環として、地域での講座研修、セミナー、セキュリティイベントの開催等に関する助成事業を実施し、人材、情報等の提供を通じて地域団体の活動を支援している。

2018 年度はインターネット上の性被害に関する講座研修やサイバーセキュリティの普及啓発等を実施する地域の 4 事業者を選定、助成を行った。

(2) 一般財団法人マルチメディア振興センター

一般財団法人マルチメディア振興センターは、情報通信ネットワークの安全・安心な利用、及びその促進に向けた普及啓発事業を行っている。その一環として、「2.4.5 (2) e- ネットキャラバンの実施」で紹介した e- ネットキャラバンを全国各地で運用・実施している。

また、「ネット社会の健全な発展に向けた連絡協議会」の事務局として、関係組織を取りまとめている。2018 年度は、「情報通信の安心安全な利用のための標語※341」募集において連絡協議会特別賞を受賞した標語のポスター※342 を作成し、2018 年 10 月～ 11 月に秋の一斉行動キャンペーンを実施した※343。

(3) 一般社団法人セキュリティ対策推進協議会（SPREAD）

SPREAD は情報セキュリティ対策を適切にアドバイスする人材の育成・支援を行う団体であり、セキュリティ事例をテーマとして「SPREAD 勉強会」を定期的に開催している。

また、地域や組織の中でセキュリティに関心があり、周囲の人にそれらを伝えようとする意欲のある方々を「SPREAD 情報セキュリティサポーター」として認定し、必要な知識を伝えるとともに活動用教材の提供を含めたバックアップを実施している（サポーター制度※344）。サポーターの年齢制限はなく、年数回の能力検定試験により認定される。2019 年 1 月 1 日時点でのサポーター数は 1,064 名である。

(4) JPCERT/CC

JPCERT/CC では、インターネット上のサービスを利用する際に入力するパスワードが漏えいし、パスワードリスト攻撃等に悪用される事例の増加を受け、多くの賛同企業と連携して、「STOP！パスワード使い回し! キャンペーン 2018※345」と題した啓発活動を 2018 年に実施した。

(5) JNSA

JNSA では、ネットワークセキュリティの普及啓発事業として各種セミナーを開催し、情報セキュリティに関するコンテンツ（「JNSA 2018 セキュリティ十大ニュース※346」等）や調査資料（「2017 年情報セキュリティインシデントに

関する調査報告※347」等）を公表している。

また新しい試みとして、2018年5月、サイバーセキュリティを題材とした魅力的な小説を募集する「サイバーセキュリティ小説コンテスト※348」（図2-4-21）を関係企業・省庁の後援のもとに開催した。この結果、noisy氏の「目つきの悪い女が眼鏡をかけたら美少女だった件」が大賞を受賞した。ライトノベルの枠組みに情報漏えいやハッカー等の要素が織り込まれ、現実に起こり得るサイバー脅威として分かりやすく描かれたことが評価された。同作は2019年5月1日、KADOKAWAスニーカー文庫より出版された※349。

■図2-4-21 「サイバーセキュリティ小説コンテスト」ポスター
（出典）JNSA「サイバーセキュリティ小説コンテスト」

(6) 一般社団法人安心ネットづくり促進協議会

安心なインターネット利用環境整備を推進する一般社団法人安心ネットづくり促進協議会（Japan Internet Safety Promotion Association：JISPA）では、普及啓発の一環として、「安心協ニュース」の発行※350や、若年層及び保護者向けリーフレット等の作成・提供を行い、青少年の健全なスマートフォン利用に資する情報を提供している。JISPAは2013年以降、総務省が開発したILAS（Internet Literacy Assessment indicator for Students：青少年がインターネットを安全に安心して活用するためのリテラシー指標）※351を基に、全国の小・中・高校生、保護者を対象としてインターネット・リテラシーの可視化調査を実施している。

(7) スマートフォン時代に対応した青少年のインターネット利用に関する連絡会

「スマートフォン時代に対応した青少年のインターネット利用に関する連絡会」（スマホ連絡会（近畿））では、「インターネットの安心・安全に関する動画フェスタin近畿2018」（図2-4-22）を実施した※352。同イベントでは、インターネット・スマートフォンの安心・安全な利用方法に関して、小・中・高生や大学・社会人が、グループ内での対話を通じて啓発動画を制作することにより、制作者のリテラシー向上を目指すとともに、制作された動画を用いた周知啓発活動も実施している。

同イベントの生徒部門最優秀賞は、「九条南☆23」（大阪市立九条南小学校）の「知ってる?フィルタリング!」、学生・社会人部門最優秀賞はTeam Nara Mamasの「スマホをポッケに」であった。

■図2-4-22 「インターネットの安心・安全に関する動画フェスタ」チラシ
（出典）総務省「スマートフォン時代に対応した青少年のインターネット利用に関する連絡会（スマホ連絡会（近畿））」

(8) 学校・学生等

学校・学生等による活動事例として、「第14回IPA『ひろげよう情報モラル・セキュリティコンクール』2018」において文部科学大臣賞を受賞した雲雀丘学園小学校（兵庫県）の事例を紹介する。同小学校では、使うことを前提に、安全で有効なICT機器、及び環境を利用できる児童を育成するために、インターネットや情報モラルの指導が大切という方針のもと、発達段階に合わせて、年間にわたり学校全体で取り組むカリキュラムを編成している。このカリキュラムに沿って、学年ごとに週1時間の指導を実施していることが評価された。

(9) セキュリティベンダ・ITベンダ

全国各地において、メーカ、セキュリティベンダ、プロバイダ等による各種のセミナーが実施されている。更に、情報セキュリティに関する標語やポスターの募集（コンクール開催）や、地域の組織や団体向けのセキュリティイ

ベントや勉強会等が開催されているほか、ブログ等を通じてサイバー攻撃や情報セキュリティ上の脅威に関する情報発信も行われている。以下に例を挙げる。

- キヤノン IT ソリューションズ株式会社は、サイバーセキュリティに関する情報を包括的に紹介する「マルウェア情報局」を公開している※353。
- 日本アイ・ビー・エム株式会社は、セキュリティに関する講演コンテンツの公開、CSIRT 研修の実施等を行っている※354。
- セキュリティベンダ各社はセキュリティ脅威、攻撃手法、セキュリティ対策等について最新の情報提供を行っている。例えば、株式会社カスペルスキー※355、株式会社シマンテック※356、トレンドマイクロ社※357、マカフィー株式会社※358 等は、それぞれ公式ブログにおいて情報を提供している。

COLUMN

ネットで目立ちたい??

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。今日は、インターネットで見つけた情報を読んで、びっくりしたことと悲しかったことをお話します。

ある日、「人が刃物で刺された。」というコメントと、人が刺されて倒れる様子を映した動画がSNSに投稿されていました。それを見たぼくが「大変だ!救急車を呼ばなくちゃ!」と大騒ぎしていたら、お父さんは「あわてないで。ちゃんと情報を確かめてみよう。」と言って、いろいろ調べ始めました。そうしたら、誰かがもう110番通報していたことや、警察の人が確認したけど本当は誰も刺されていなくて、この書き込みはウソの情報だったということがわかりました。こういうのを「フェイクニュース」って言うんだって。これを聞いて、「どうしてこんなウソをインターネットに書くんだろう?」とぼくはとても悲しく思いました。だって、こんなふうに、ウソを書く人が増えてしまったら、インターネットの情報を信じることができなくなってしまうもの。今回投稿した人たちは「目立ちたかった」って言ってたみたいだけど「目立つ」って良いことなのかな?　悪いことで有名になってもしかたないよね?　ぼくの質問に、お父さんが答えてくれました。

「目立って、誰かに『いいね』って言ってもらいたい人が多くなってきているのかもしれないね。誰でもほめられたり、認めてもらうのはうれしいと思うよね。でも『ほめられたいからこれをやる』っていう考え方になってしまうと、『目立つ』とか『ほめられる』ことが一番の目的になるから、やるべきこととやってはいけないことを見失ってしまうんだ。例えば足元にごみが落ちていたら、衛生的によくないし、自分もいやな気分になるから拾って捨てるよね。でも『目立つ』行動じゃないからやらない、とか、誰もまわりにいなくてほめてくれないからやらない、という判断になってしまうのはよくないことだと思わないかい?　誰かの目を通して自分を見るのではなく、自分がちゃんと自分を評価してあげる、ということが大切な気がするな」

そうだよね。インターネットにウソの情報を出す自分だったら、どんなに「いいね」をもらっても、自分のことは好きになれない気がする。反対に、誰も見ていなくても正しい行いができる自分は誇りに思えるもの。

みなさんも、自分のことを好きになれるような情報発信をしてきたか、振り返ってみませんか?

2.5 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。

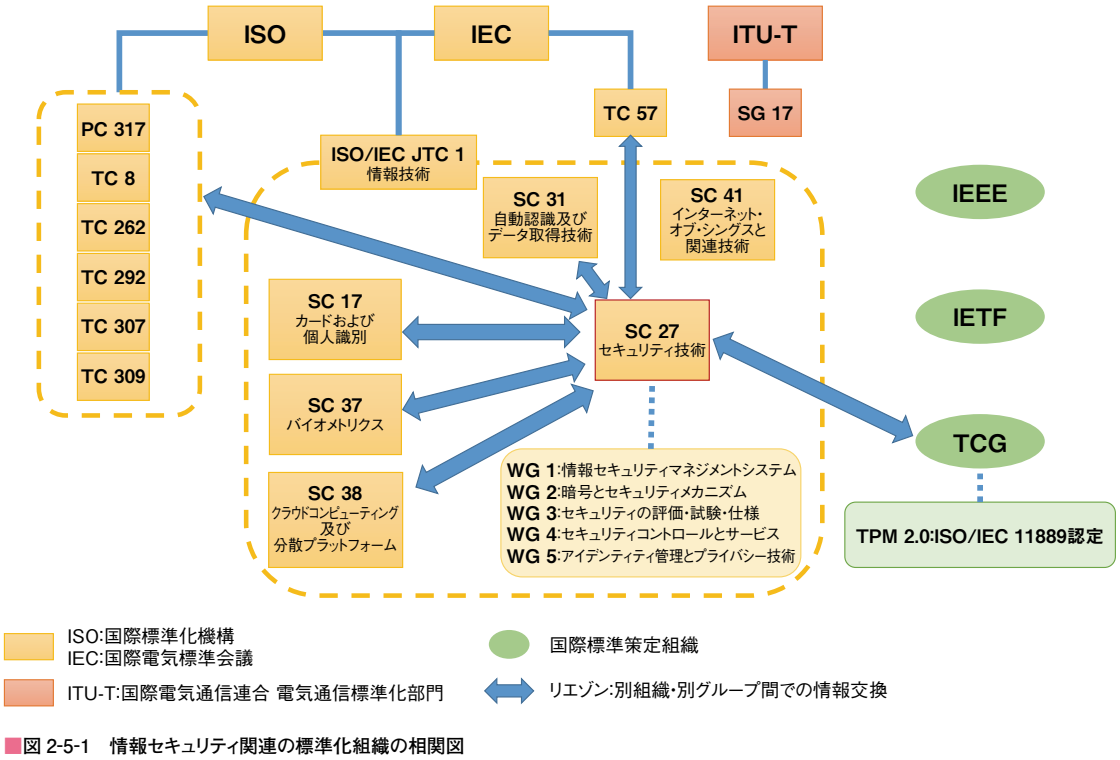
1995 年に WTO/TBT 協定が発効し、加盟国が製品や技術に適用する強制規格や適合性評価手続きの作成の際には原則として国際規格（ISO/IEC 等）を基礎とすることが義務付けられた※359。翌 1996 年に WTO・政府調達協定が発効し、政府調達における技術仕様等には国際規格を基礎とすることが各国に義務付けられた。欧米先進国では、国際競争力強化のために国際標準化活動を重要と考えて取り組んできたが、日本でも「知的財産推進計画 2010※360」において国際標準化を知的財産政策の第 1 項に掲げ取り組んできた。「知的財産推進計画 2018※361」においては、国際標準化が第 4 次産業革命時代の鍵を握るとして更に取り組みを強化しており、情報収集から普及までを見据えた官民標準化体制を構築し、新しい分野を中心に先手を打って国際的なルール形成に参画しようとしている※359。このような背景もあり、日本からの積極的な提案が行われている（「2.5.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27）」参照）。

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）※362」、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。

2.5.1 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 2-5-1 に示す。



■図 2-5-1　情報セキュリティ関連の標準化組織の相関図

- 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）※363：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、日本産業標準調査会（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※364。
- 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）：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※365、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。

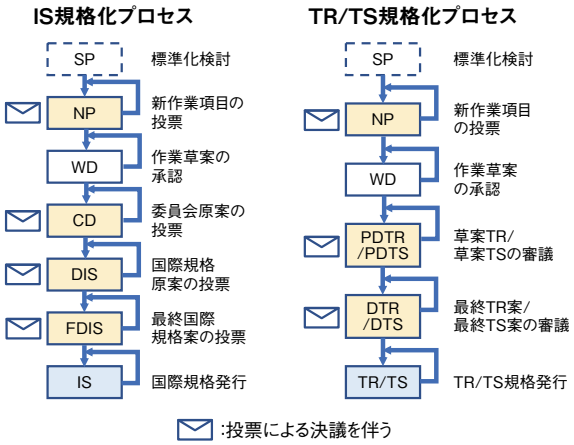
また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下のようなものがある。

- 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※366。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※367。

2.5.2 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（SC）である。SC 27は、テーマ別に五つのWGで構成される（図2-5-1）。

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2-5-2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、技術報告書または技術仕様書として出版する。



■図2-5-2 ISO/IEC JTC 1/SC 27における文書のステータス
（出典）JISC「ISO規格の制定手順※368」を基にIPAが作成

図2-5-2の各文書のステータスは、以下のとおりである。本文中では、略号を使用する。

SP：研究期間（Study Period）
※ SPはWGによって実施しない場合もある。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）
DTS：技術仕様書原案（Draft Technical Specification）

TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各 WG の活動概要を述べる。

（1）WG 1（情報セキュリティマネジメントシステム）

WG 1 では、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、及びその他の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 27001:2013 発行に伴う、ISO/IEC 27001 に関する手引きや指針を提供する規格の改訂は、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が 2018 年に行われた。なお、ISO/IEC 27005 は、ISO/IEC 27001:2013 へ本格的に対応するための取り組みも継続して進められ、更なる改訂が見込まれるが、それには時間を要することが想定される。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、都度改訂されてきたが、最新の改訂版が 2018 年に発行された。

(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 は 2016 年に発行されたが、2017 年には早期改訂が決定し、現在は DIS の審議中であり、2020 年には改訂版が発行される見込みである。

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 に適合した最初の規格である。その他の分野別規格も今後、ISO/IEC 27009 に適合することが想定される。

(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 2019 年 1 月に発行された。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 は、改訂作業が開始されており、現在は CD の審議中である。改訂版発行には、まだ時間がかかる見込みである。

新たなトピックである、サイバーセキュリティに関する規格化の活動については、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。サイバー保険に関する規格である ISO/IEC FDIS 27102 は審議中であり、2020 年には発行される見込みである。このほか、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（ISO/IEC WD TS 27101）、サイバーセキュリティの概念やコンセプトに関する規格（ISO/IEC WD TS 27100）についても検討が進められており、いずれも審議中である。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、規格化に向けた課題は多い。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、前述の規格類の発行、改訂作業の中で検討が進められている。

(d) ISO/IEC 27001 及び ISO/IEC 27002 の改訂

2013 年の改訂から 6 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 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。現在は WD の審議中であり、各国とも積極的に参加し、多くのコメントが寄せられている。ISO/IEC 27001:2013 についても、日本を含め多くの国が次期改訂の必要性を表明している。一方で、ISO/IEC 専門業務用指針、第 1 部[※369]において規定されたマネジメントシステム規格の共通フォーマットの改訂も 2022 年に改訂が予定されている。このため、現在 SC 27/WG 1 では、共通フォーマットの改訂作業が ISO/IEC 27001 改訂に与える影響評価を行っており、この結果を受けて ISO/IEC 27001 の改訂時期を決定する予定である。

(2) WG 2（暗号とセキュリティメカニズム）

WG 2 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。WG 2 の国際主査、副主査（2019 年 4 月より新任に交代）ともに日本人が選出され、WG 2 での活動をリードしている。2018 年度は、新しい規格の発行はなかったが、既存規格 2 件の改訂版が発行された。このほかの主な活動内容について以下に示す。

(a) 軽量暗号「SIMON/SPECK」の標準化中止

米国国家安全保障局（National Security Agency：NSA）が設計した軽量暗号 SIMON/SPECK[※370]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た。この間、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が指摘されていた。また、2013 年の Edward Snowden による情報暴露事件以降、NSA の信頼回復が依然としてできていなかった。このような状況の中、追補草案（Proposed Draft Amendment：PDAM）の段階ではあるが、2018 年 4 月の武漢会議にて標準化中止が提案され、WG 2 及びその上位の SC 27 で中止が議決された。その後、更に上位の JTC 1 にて中止の賛否を問う投票が行われ、賛成多数で標準化の中止が決定された。

(b) 認証暗号 OCB2 への対応

「認証暗号（ISO/IEC 19772）」には六つの認証暗号方式が規定されている。その中の認証暗号 OCB2 に対する解読論文が 2018 年 11 月に相次いで 3 件発表された。WG 2 で対応を協議した結果、OCB2 の使用取りやめ要請と規格から削除を予定している旨をアナウンスするプレスリリース[※371]を SC 27 から 2019 年 1 月に公表した。現在、規格から削除する作業を行っている。

(c) 新規標準化作業の開始

「鍵管理　第 7 部：クロスドメインパスワードに基づく認証鍵交換（ISO/IEC 11770-7）」と「認証データの墨塗り　第 1 部：概要（ISO/IEC 23264-1）、第 2 部：非対称機構に基づく墨塗り署名方式（ISO/IEC 23264-2）」の標準化作業が新たに開始された。

(3) WG 3（セキュリティの評価・試験・仕様）

2018 年度、WG 3 は 4 月に武漢（中国）、9 ～ 10 月にイェービク（ノルウェー）、そして 2019 年 4 月にテルアビブ（イスラエル）にて定期会議を開催した。それらの会議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）[※372]は WG 3 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。2017 年 4 月のハミルトン会議にて本規格を改訂することが合意され、それ以降、米国、英国、フランス、ドイツ、韓国、ポーランド、中国、南アフリカから指名された計 15 名のエディタが改訂作業に従事している。2018 年度の会議にて議論された主要な改訂点は下記のとおりである。なお、本規格は 2019 年 4 月のテルアビブ会議にて CD3 に進むことで合意された。

- Protection Profile（PP）のモジュール化

  PP とは、ISO/IEC 15408 のセキュリティ評価を実施する際に基点となる文書であり、評価すべきセキュリティ機能や、そのセキュリティ機能が何故必要なのかという背景がこの PP に記載されている。評価すべきセキュリティ機能は IT 製品ごとに異なるため、PP も OS やスマートカード等の製品分野ごとに開発される。しかしながら、複数の製品分野でまったく同じ機能が実装されることもある。

  例えば、複数人で共有されるサーバと、個人使用となるモバイルデバイスでは、その使用環境や保持すべきセキュリティ機能が異なるため、個別に PP が開発されている。

  しかしながら、例えば VPN 機能や生体認証機能等、サーバとモバイルデバイスでまったく同じ機能を実装す

ることもある。このような場合、サーバ用とモバイルデバイス用の各々の PP に、VPN 機能や生体認証機能に関した同一の記述をするのではなく、VPN 機能や生体認証機能を記述した部分を切り出し、サーバ用 PP やモバイルデバイス用 PP からその切り出した部分を適宜参照できるようにする方が、PP 開発を効率的に進めることができる。このような、個別機能ごとに切り出された部分は PP モジュールと呼ばれ、サーバやモバイルデバイス固有のセキュリティ機能を記載する PP はベース PP と呼ばれる。今回の改訂において、この PP のモジュール化の概念が ISO/IEC 15408 及び 18045 に取り込まれる予定である。

- Multi-assurance Evaluation

  IT 製品には、重要な情報を保持せず攻撃される恐れが少ない製品や、逆に高度なセキュリティを要求される製品もある。ISO/IEC 15408 に基づく評価では、評価保証レベルとして Evaluation Assurance Level（EAL）を定義し、セキュリティの重要度に基づく評価を可能にしている。例えば EAL1 では、製品マニュアルをベースにした簡易なブラックボックス評価が行われるが、評価保証レベルが高い EAL4 では製品のソースコードを参照しつつ実施するホワイトボックス評価となり、評価に要する期間やコストも大幅に増加する。

  現在の ISO/IEC 15408 に基づく評価では、一つの製品評価には一つの PP が適用され、その PP では一つの評価保証レベルしか定義できない。しかし、一つの製品の内部を詳しく見れば、重要なデータを暗号化するための暗号鍵を管理するような、セキュリティ的には極めて重要なモジュールも存在すれば、データへのアクセスログを管理する機能のように、暗号鍵管理と比較してセキュリティ上の重要度が下がるモジュールもある。

  そのため、前述したベース PP や PP モジュールで異なる EAL を指定することを可能にする、Multi-assurance Evaluation の概念の導入がイェービク会議にてフランスより提案され、承認された。Multi-assurance Evaluation により、製品単位だけでなく、機能モジュール単位で評価保証レベルを指定することで、メリハリの利いたセキュリティ評価が可能になる。

(b) ISO/IEC 20897 の開発

ISO/IEC 20897（Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters）では、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標準化が行われている。PUF は半導体チップ固有の物理特性から識別 ID や暗号鍵を生成し、IoT 機器等の認証やデータ秘匿等に用いる技術である。

現在、日本で進行している PUF の研究プロジェクト[※373]の成果を本規格に反映すべく、日本の技術者が積極的に標準化に貢献している。これまで、日本は PUF のセキュリティ要件の明確化に貢献するとともに、それらセキュリティ要件に対応するテスト手法を提案しており、開発者が自ら自社の PUF 実装製品のセキュリティ評価を実施し、PUF 実装製品のセキュアさを顧客に、または対外的に立証できることを可能にするような規格の開発を目指している。

(4) WG 4（セキュリティコントロールとサービス）

WG 4 では、WG 1 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、WG 4 における 2018 年度の主な成果、活動を紹介する。

(a) IoT セキュリティのための標準化活動

我が国は、IoT 関連の製品・システム開発の競争力を強化し、また IoT の国際的なセキュリティレベル向上に寄与するために、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン[※374]」の国際標準化を提案した。これらは ISO/IEC 27030（IoT のセキュリティとプライバシー）、ISO/IEC 30147（IoT システム／サービスの信頼性の方法論）の二つのプロジェクトで審議されている。

このうち、ISO/IEC 27030 については、2018 年 4 月の SC 27 武漢会議で NP が成立し、その後、2018 年 10 月のイェービク会議で WD1 が審議され、2018 年 11 月に承認された。また 2019 年 4 月のテルアビブ会議では、WD2 の審議が行われた。日本からは、IoT リスクに対するコメント、ライフサイクルに対するアップデート、IoT セキュリティ管理策の拡充（実施のガイダンスを付与）等を提案した。

英国から発行されているガイドライン「IoT セキュリティ行動規範（英国情報通信政策）」「消費者向け IoT 製品のセキュリティに関する行動規範」[※375]も今後の議論の中で検討材料となる可能性が高い。「消費者向け IoT 製品のセキュリティに関する行動規範」では、製造

メーカ等が実施すべき対策を 13 項目のガイドラインにまとめている。13 項目は以下のとおりである。

- デフォルトパスワードを使用しない
- 脆弱性の情報公開ポリシーを策定する
- ソフトウェアを定期的に更新する
- 認証情報とセキュリティ上重要な情報を安全に保存する
- 安全に通信する
- 攻撃対象になる場所を最小限に抑える
- ソフトウェアの整合性を確認する
- 個人データの保護を徹底する
- 機能停止時の復旧性を確保する
- システムの遠隔測定データを監視する
- 消費者が個人データを容易に削除できるよう配慮する
- デバイスの設置とメンテナンスを容易にできるように配慮する
- 入力データを検証する。

(b) 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 (2018 年 9 月規格化完了)
  - Part 3: Code of practice for electronic discovery (2017 年 10 月規格化完了)
  - Part 4: ICT readiness for electronic discovery (2018 年 12 月 WD)

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 9 月に規格策定が完了した。

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 となり、2018 年 12 月に WD が承認され、審議を継続している。

(5) WG 5 (アイデンティティ管理とプライバシー技術)

WG 5 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。2018 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 (改訂作業中)
- 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おり、現在、FDIS の段階である。

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 2019 年 3 月に DIS 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。なお、DIS 投票において反対票がなかったことから、FDIS の投票はスキップし、IS 投票に進む見込みである。

プライバシーアーキテクチャフレームワークを規定した ISO/IEC 29101 は、2018 年 11 月に第二版（2nd Edition）が発行された。本規格は、PII（Personally Identifiable Information：個人識別可能情報）を取り扱う ICT システムの指定、調達、設計、テスト、維持、管理、及び運用に携わる留意事項を整理し、フレームワーク（枠組み）として規定されたものである。

日本提案の規格としては、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 が DIS になり、策定が進められている。また、同じく日本提案である「ユーザのプライバシープリファレンスに基づくユーザ主導による PII 処理のためのフレームワーク」は、2019 年 1 月に NP 投票が行われ、新たに ISO/IEC 27556 として規格策定のプロジェクトが登録された。

なお、プライバシーに関連した他の技術委員会（TC）の動向として、2018 年に新たに設置されたプロジェクト委員会である ISO/PC 317 がある。ISO/PC 317 では、ISO 31700 として「消費者向け製品及びサービスのためのプライバシー・バイ・デザイン」の規格策定が行われており、同規格は ISO/IEC 29000 シリーズ等の既存規格も参照しつつ、製品やサービスの企画・設計段階からプライバシーに配慮した開発を行うためのプロセス仕様を検討している。

(c) バイオメトリクス

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、2009 年に発行され、現在改訂中で DIS 段階にある。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の改訂が開始され、WD 段階にある。また、モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定めるプロジェクトが、ISO/IEC 27553 として開始され、WD 段階にある。

(6) SC 27 と他の分科会・組織との連携

情報セキュリティは分野横断的な技術分野であり、また、特に近年、インターネットが社会生活に欠かせない程普及したことに伴って社会的に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 TC、SC と SC 27 との連携が増えている。

例えば図 2-5-1（124 ページ）にあるように、カード及び個人識別の SC 17、バイオメトリクスの SC 37、クラウドコンピューティング及び分散プラットフォームの SC 38 がリエゾンを締結している。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 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。SC 27 は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 IEC TC 57、ISO TC 8 等との間でリエゾンを締結し、セキュリティ及びレジリエンスの ISO TC 292、リスクマネジメントの ISO TC 262、組織のガバナンスの ISO 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 ISO TC 307※376 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 月にリエゾンを締結して連携が行われている。

日本は、国内で策定された IoT に関連するガイドライン等を検討の成果として標準化活動に提案している。

SC 27 には、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※377」をベースに提案し、ISO/IEC 27030（IoT のセキュリティとプライバシー）として、規格開発が開始された。また、SC 41 に対しては、NISC が策定した「安全な IoT システムのためのセキュリティに関する一般的枠組※378」を始めとして日本国内で公開された関連文書をベースに提案し、ISO/IEC 30147（IoT シ

ステム／サービスの信頼性の方法論）として規格開発が開始された（IoT のセキュリティについては「3.2 IoT の情報セキュリティ」参照）。

2.5.3 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）※379 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 81 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 2019 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※380。

日本には 2008 年に設立された TCG の地域支部がある※367。この日本支部（Japan Regional Forum：JRF）では、国内向けの普及活動として 2018 年は勉強会※381、ワークショップ※382 を開いており、その経験を世界へフィードバックしている。

以下では、2019 年 1 月現在 16 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）Embedded Systems ワークグループ

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※383。

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 Automotive Thin Profile for TPM Family 2.0; Level 0 Version 1.0」として公開し、2018 年には Version 1.01 Revision 15 に改訂している※384。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 12 月に「Protection Profile Automotive-Thin Specific TPM for TCG TPM 2.0 Automotive Thin Profile Family “2.0” Level 0 Version 1.0」としてリリースされた※385。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証等があり、これらについても検討が続いている。

（2）Device Identifier Composition Engine Architectures（DICE）ワークグループ

前述の Embedded Systems ワークグループには、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 サブグループがある。このサブグループでの議論により 2017 年に独立した DICE は、RIoT（Robust IoT）※386 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※387。RIoT と DICE の関係は、TPM と TSS（TCG Software Stack）※388 の関係に相当する。DICE は 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。2018 年 3 月には「Hardware Requirements for a Device Identifier Composition Engine」を公開している※389。

（3）Cyber Resilient Technologies（CyRes）ワークグループ

CyRes は、2018 年 6 月に設立されたワークグループであり、プラットフォームに依存しない技術として、次の 3 点を検討している。

- ウイルスの脅威からプログラムコードとデータを保護する技術
- 脆弱性にパッチが適用されていないコードの検出技術
- 脅威に晒されているプラットフォームを正常にリカバリーする技術

検討の成果物は、例えば NIST が公開している文書 SP800-193※390 を補完するものとなる。

2.6 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、政府機関や独立行政法人が安全にIT製品等を調達するために活用できる制度の運営及び利活用のための普及活動を行っている。

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」の動向やスマートカードの政府調達に向けた取り組み、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。

2.6.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部の発行した「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）※391」（以下、政府統一基準）では、府省庁や独立行政法人における情報セキュリティ対策の基準を示しており、公的なサービスにおいて国民の情報等を扱うシステムを構築する場合、そのシステムを構成する市販IT製品のセキュリティ要件を策定することを調達者に求めている。

このようなセキュリティ要件を確保する手段として、多くの国々では、第三者がIT製品の情報セキュリティを評価し、公的機関がその評価結果に基づき評価されたIT製品に認証を与える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）※392」をIPAが運営し、政府調達において活用されている。

(1) 政府調達のセキュリティ要件

政府統一基準では、特に政府調達においてセキュリティ要件を策定すべき機器として、経済産業省が発行している「IT製品の調達におけるセキュリティ要件リスト※393」（以下、要件リスト）が参照されている。この要件リストには、情報システムにおいて基盤となり、攻撃の対象となり得る製品分野のうち、セキュリティ要件を満たした製品の調達を求められている11の製品分野が指定されている（表2-6-1）。府省庁や独立行政法人の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、これらの製品分野のIT製品を調達する場合、想定されるセキュリティ上の脅威に対抗できていることを確認することが義務付けられている。

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
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で、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2-6-1　政府調達における要件確認対象製品
（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

具体的には、情報システムセキュリティ責任者は、要件リスト対象のIT製品を調達する際、要件リストに示された脅威を識別し、その脅威に調達するIT製品が対抗できることを確認する必要がある。確認の方法として、調達ごとに各組織で受け入れテスト等を実施する方法と、確認すべきセキュリティ要件が国際標準に基づいて確認されている場合に、当該標準に基づく第三者認証を取得していることの確認をもって受け入れテスト等を代替する方法がある。

「ITセキュリティ評価及び認証制度」は、情報セキュリティ評価の国際標準であるISO/IEC 15408に基づいて第三者評価を実施し認証を与える制度であり、2001年より運営が開始された。現在まで、ICチップが埋め

込まれたマイナンバーカードや旅券、デジタル複合機等の製品分野で調達要件として本制度が活用されている。データベースやサーバ OS、ファイアウォール等の海外製品がデファクトとなっている製品分野については、既に多くの認証が海外で取得されているが、2018 年度に要件リストに追加されたルータ／スイッチ等の製品分野については、国内ベンダが多くの製品を製造しているにも関わらず、まだ認証された製品が極端に少ない。このため、これらの調達においては、認証を調達要件とすることができず、個別の受入れテストを実施することとなり、政府調達の効率化という側面からも課題となっている。

(2) 第三者認証制度の国際連携

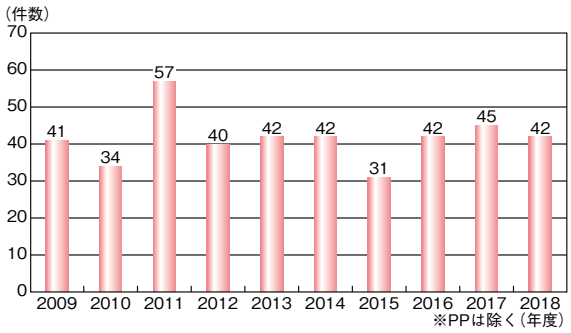
政府調達の安全と効率化のため、欧米 6 ヵ国により情報セキュリティ評価のための共通基準（Common Criteria：CC）が 90 年代半ばに開発され、CC に基づく評価・認証制度が各国で立ち上がった。1999 年に CC は ISO/IEC 15408 として国際標準となった。国際的な調達における国ごとの再評価のコスト低減を目的に、CC による評価・認証制度を持つ国々で、認証結果を相互に受け入れるアレンジメント（Common Criteria Recognition Arrangement：CCRA）が締結された。日本も CC に基づく評価・認証制度である JISEC の運用を 2001 年に始め、2003 年に CCRA へ加盟している。

近年は、アフリカ、東南アジア、東ヨーロッパ諸国の CCRA 参加が増加しており、2018 年以降もポーランド、インドネシアが加盟した。2019 年 4 月現在、CCRA 加盟国は 30 ヵ国※394 に及び、更に数ヵ国が加盟申請を表明している。

CCRA は、認証結果の相互承認のほかに、IT 製品の共通のセキュリティ要件の策定も行っている。同一製品分野でありながら、国や組織ごとに異なる調達要件が提示されると、似たような評価が繰り返し実施されることになる。特定の製品分野のミニマルなセキュリティ要件を策定し、国際的な調達要件として用いることで、重複する評価コストを軽減できる。現在 CCRA では、ファイアウォール、ドライブ全体暗号化システム、及びルータや VPN の基盤となるネットワークデバイスの共通セキュリティ要件をリリースしており※395、CCRA 加盟各国は、これらの製品分野の政府調達において共通のセキュリティ要件を必要最小限のセキュリティ要件として指定することになっている。日本に多くの製品ベンダを有するデジタル複合機の分野では、2015 年に日本と米国が共同で「Protection Profile for Hardcopy Devices」（HCD-PP）を策定した。現在 HCD-PP は日米両国の政府調達要件として用いられている。この HCD-PP をベースに、日本は韓国とともに発起人となり、CCRA の場でデジタル複合機の共通セキュリティ要件の策定を行うことを 2019 年 4 月の CCRA 会合で発表した。これが完成すれば、CCRA 加盟国の政府調達要件として活用され、製品ベンダにとって第三者認証制度の利便性が高まることとなる。

(3) 認証の状況

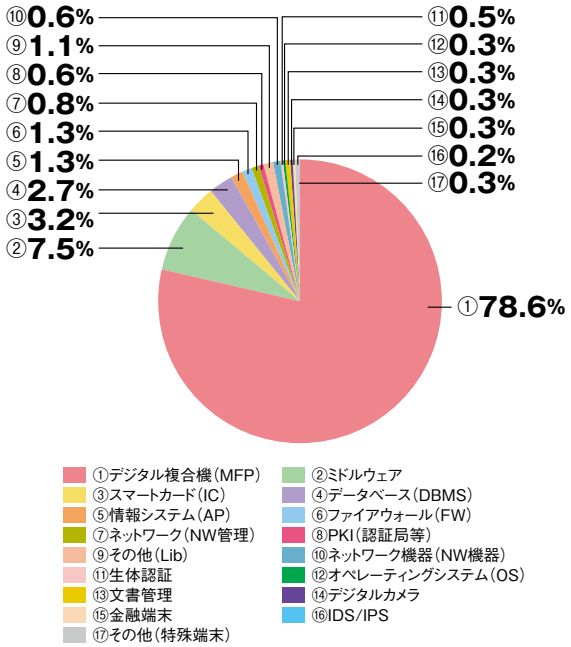
2018 年度までの JISEC での認証発行件数の推移を図 2-6-1 に示す。2009 年度から 2011 年度はリーマンショックによる申請の減少とその揺り戻し、2015 年度は規程の改正により長期滞留案件（申請より 24 ヵ月を超えたもの）が申請取り下げとなった影響があるが、基本的には毎年 40 件程度の認証を発行している。これは、本制度における申請をデジタル複合機が占めており、新規機種の市場投入が認証申請を伴い定常的に行われていることの反映と考えられる。



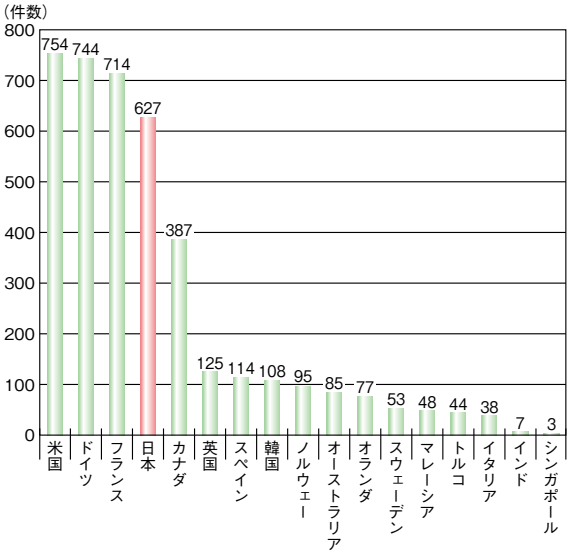
■図 2-6-1　日本の認証発行件数の推移

日本における認証発行製品分野の内訳は、図 2-6-2（次ページ）に示すように圧倒的にデジタル複合機が多く、2018 年度の認証発行においてはすべてがデジタル複合機である。2018 年 2 月に対象製品分野が 6 分野からルータや VPN ゲートウェイ等、11 分野に拡大されたが、ネットワーク機器の場合、基盤システムとして構築され個別のシステムとして納品時に検査されるため、新たな製品認証の申請に結びついていないと考えられる。

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 2018 年度までの累計は、米国、フランス、ドイツに次いで日本が第 4 位である（次ページ図 2-6-3）。ドイツやフランスの主な認証製品はスマートカードであり、米国はルータ、ファイアウォールといったネットワーク関連機器となっている。日本のデジタル複合機のように、各国における主要なベンダの存在が、その国の認証製



■図 2-6-2　日本の認証発行件数の内訳(n=627)



■図 2-6-3　CCRA 加盟国の認証状況

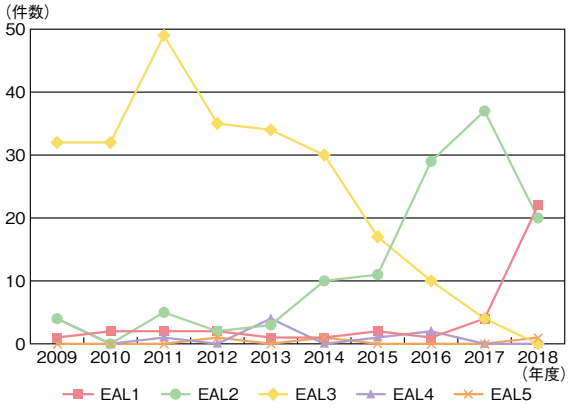
品分野を特徴づけている。

(4) 評価保証レベルの変化

国際的なセキュリティ評価基準である CC では、セキュリティ評価のベースとなるセキュリティ要件の形式を規定している。このセキュリティ要件は Protection Profile (PP) と呼ばれ、製品分野ごとに評価すべきセキュリティ機能と、評価する範囲や深さを示す評価保証レベル (Evaluation Assurance Level:EAL[※396])を規定する。各国の政府調達では、調達仕様においてそれらの PP を指定することで、安全な製品調達を実現している。

デジタル複合機では、IEEE[※397] が 2009 年に策定した PP である IEEE 2600 が政府調達要件として広く用いられてきた。国内の複合機ベンダ各社は、非常に高いセキュリティを要求される環境での運用を想定した「IEEE Std 2600.1™-2009」(EAL3 相当) に適合した製品を開発し認証を取得してきた。その後、新製品の迅速な調達を期待する調達関係者と実効的な評価によるコスト低減を期待するベンダ等の要望を受け、CCRA の場で基本的な評価保証レベルを EAL2 までとする方針[※398] が 2012 年に発表された。これを機に、我が国でも一般のオフィス環境での運用を想定した「IEEE Std 2600.2™-2009」(EAL2 相当) に適合した認証にシフトし、2015 年度を境に EAL3 と EAL2 の認証発行件数は逆転した (図 2-6-4)。

IPA は、米国の認証機関である NIAP (National Information Assurance Partnership) と共同で、日米のデジタル複合機ベンダや評価機関の協力のもと、開発環境セキュリティ等を評価の範囲から外し、製品セキュリティの具体的な評価手順を規定した EAL1 相当の HCD-PP を 2015 年に発表した。この PP は日米両国の政府調達要件としても採用され、デジタル複合機各ベンダが対応したことにより、図 2-6-4 に示すように EAL1 の件数が急速に増えた。



■図 2-6-4　日本の評価保証レベル別認証発行件数の推移

評価保証レベルについては、スマートカードのように一度広く行き渡ると回収が困難であり、その保護資産への攻撃機会が無制限であるような製品については、EAL5 以上と高い保証を要件とする一方、一般のオフィス環境で運用される製品については、EAL1 が主流となっている。例えば、CCRA 加盟国が政府調達に用いることを前提に CCRA で策定されたファイアウォールやネットワーク機器等の PP[※399] も、すべて EAL1 相当となっている。

かつては、調達者の無理解により厳格な保証を一律に求める傾向にあったが、昨今はそれぞれの製品分野のPPにおいて使用環境や保護資産に見合った適切な保証を求める本来のCCの使われ方が定着しつつある。このような背景から、今後は政府調達におけるIoT分野あるいはスマート家電のような民需製品についても適切な保証レベルのPPが策定され、安全な調達の裾野が広がることが期待できる。

2.6.2 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※400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※401。EAL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/EAL3が主流であったのに対し、スマートカードではEAL4/EAL5が主流であることが分かる。この傾向は、CCRAのWebサイトに公開している認証製品の年別の推移でも確認できる。例えばスマートカードに分類される認証件数に着目すると、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が主流であることが分かる。しかも2013年以降は、EAL4よりEAL5の認証件数が増えている。更に、ここ数年の特徴としてEAL4/EAL5製品が減少している一方、EAL6製品の数が微増している。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。

(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※402だったが、2014年にBSI-PP-0084※403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※404、サイドチャネル攻撃※405、故障利用攻撃※406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※407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CC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※408。2018年は、このCCサポート文書のうちComposite product evaluation for Smart Cards and similar devicesが更新されている。また、IPAとCCRAではスマートカード以外のセキュリティボックスに関するCCサポート文書も公開しており、同じく2018年に更新されている。

前述のとおり、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※409が、今後は耐タンパ性だけでなく、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。例えば、仕様記述のあいまい性に起因する不備を避けるための数理・論理手法である形式手法※410をスマートカード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 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。2018 年度末までに延べ 309 名が評価ツールを利用している。

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※411 を用意し、2015 年より貸し出しを行っている。2018 年度末までに 13 団体がテストビークルを利用し、試行評価、論文発表等を行っている。

2.6.3 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営している。これは、北米で運営されている CMVP（Cryptographic Module Validation Program）と同等の制度である。本節では、JCMVP の最新動向について述べる。

(1) 暗号モジュールのセキュリティ要求事項の新規格への移行開始

JCMVP では、暗号モジュールが満たすべきセキュリティ要求事項（アクセス制御、物理的セキュリティ等）を定めた規格として、ISO/IEC 19790:2006 を 2007 年から採用してきた。

この規格の改訂の審議が SC 27 において行われ、NIST で策定中であった FIPS 140-3※412 を基にした、ISO/IEC 19790:2012（Corrected version 2015-12-15）※413 が 2015 年に発行され、更に 2017 年に対応する試験項目を定めた規格である ISO/IEC 24759:2017※414 が発行された。

JCMVP はこれを受け、下部組織である技術審議委員会の審議を経て、ISO/IEC 19790:2012（Corrected version 2015-12-15）及び ISO/IEC 24759:2017 を採用することを決定した。JCMVP では、それらに基づく認証申請の受付を 2018 年 6 月から開始した※415。なお、これまで採用してきた ISO/IEC 19790:2006 に基づく試験報告書の受付は 2020 年 6 月末をもって終了となる。

関連する北米 CMVP の動向として、FIPS 140-3 は、2019 年 3 月 22 日に承認され、2019 年 5 月 1 日に米国連邦政府の官報公示が行われた※416。北米 CMVP における FIPS 140-3 に基づく試験報告書の受付は、2020 年 9 月 22 日から開始される。

(2) 政府機関等における認証製品の活用

経済産業省が公開している「IT 製品の調達におけるセキュリティ要件リスト」が 2018 年 2 月に見直され、次の二つの製品分野に対する適切なセキュリティ要件として、ISO/IEC 19790 及びその国際一致規格 JIS X 19790 が記載された。

- 暗号化 USB メモリ
- ドライブ全体暗号化システム

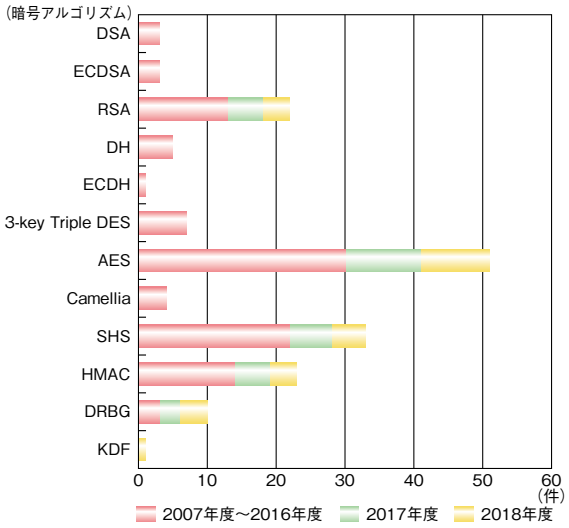
同リストは、NISC が発行する、「政府機関等の対策基準策定のためのガイドライン※417」の遵守事項から参照されているものである。

製品ベンダは、前述の製品分野の製品について、ISO/IEC 19790 に適合することを、JCMVP の暗号モジュール認証を取得することにより主張できる。また、政府機関等の調達者は、受け入れ検査を通じて、暗号アルゴリズムが正確に実装され、暗号鍵等の重要情報が適切に保護されていることを、JCMVP の暗号モジュール認証を確認することにより、容易に確認できる。

(3) 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 の二つがある。JISEC が 2017 年に発行、2019 年に改定したガイドライン※418 によって、JCMVP の活用方針が示されている（JISEC の活動については「2.6.1 IT セキュリティ評価及び認証制度」参照）。

2018 年度は、JISEC のもとで、この活用方針に関連する「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※419」に基づくデジタル複合機の認証が、19 件完了している※420。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実装のテストを求めている。このテストに、JCMVP の暗号アルゴリズム実装試験ツール（Japan Cryptographic Algorithm implementation Testing Tool：JCATT）が活用され、認証に貢献している。具体的には、図 2-6-5 に示すように、JCATT を使って確認された暗号アルゴリズム実装の実績が、2017 年度及び 2018 年度において堅調に増加し



■図 2-6-5　JCATT により確認された暗号アルゴリズム実装の実績

ている。

また、前述の 19 件のデジタル複合機の認証のうち 5 件※421 については、PP が要求するセキュリティを実現するために、JCMVP の暗号モジュール認証を取得した自己暗号化ハードディスクドライブ※422 が搭載され活用された。

(4) GCM-AES-XPN の試験仕様の策定

JCMVP は、米国政府機関向けのセキュリティ規格である NIST SP800-38D※423 に記載されたブロック暗号利用モード GCM（Galois Counter Mode）を、2012 年に承認されたセキュリティ機能に追加している。この GCM を使用したネットワークのレイヤ 2 レベルの暗号化の仕様として、IEEE 802.1AE-2006※424 及び IEEE 802.1AEbw-2013※425 で規定された Media Access Control Security という規格が存在する。このうち、IEEE 802.1AEbw-2013 で規定された暗号化仕様は、GCM-AES-XPN と呼ばれる。

JCMVP の下部組織であ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 では、GCM-AES-XPN の安全性について議論し、GCM の安全性と同様であることを確認した。これにより 2019 年度中に、GCM-AES-XPN を承認されたセキュリティ機能に追加するとともに、GCM-AES-XPN に対する試験仕様を策定する予定である。

(5) 承認されたセキュリティ機能からの 3-key Triple DES の削除

CRYPTREC は 2018 年 3 月に、危殆化の懸念が高まったブロック暗号 3-key Triple DES を、電子政府推奨暗号リストから運用監視暗号リストに移した※426。これを受けて、JCMVP の下部組織であ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 では、承認されたセキュリティ機能から 3-key Triple DES を削除するスケジュールについて、米国※427、ドイツ※428、フランス※429 の動向を踏まえつつ議論を行った。この結果、同 WG から技術審議委員会に、2019 年末をもって、承認されたセキュリティ機能から削除する方針を答申することが決まった。

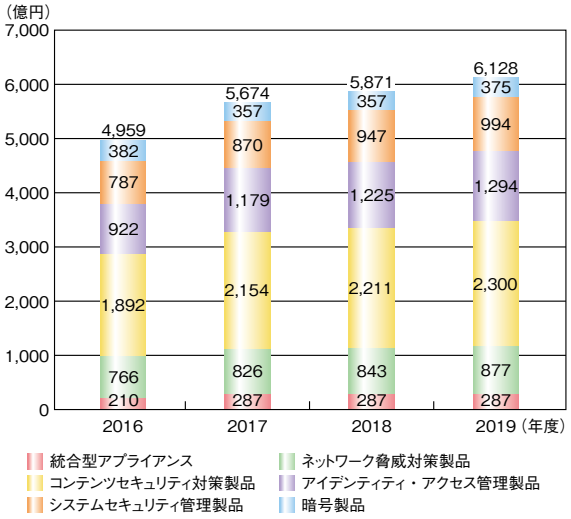
2.7 その他の情報セキュリティ動向

情報セキュリティ市場の規模と成長の動向、データ利活用の動向、及び暗号技術の動向について述べる。

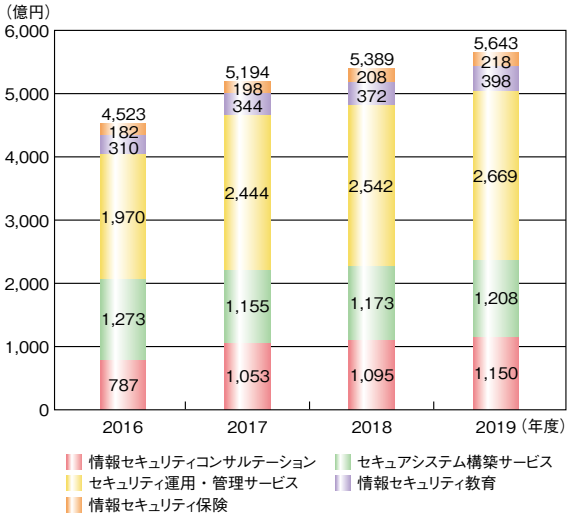
2.7.1 情報セキュリティ市場の動向

JNSA が発表した「国内情報セキュリティ市場 2018 年度調査報告※430」によると、2018 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、2017 年度より 3.6 ポイント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 2-7-1 と図 2-7-2 に示す（市場区分定義については表 2-7-1 参照）。なお、図中の 2016 年度、2017 年度については推定実績値で、2018 年度については推定見込値、2019 年度については予測値である。



■図 2-7-1　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 2018 年度調査報告」を基に IPA が編集



■図 2-7-2　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 2018 年度調査報告」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 2-7-1　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 2018 年度調査報告」を基に IPA が編集

情報セキュリティツールの市場規模全体では、2017年度から2018年度は3.5ポイント伸びている。ツール別に見ると、「コンテンツセキュリティ対策製品」の2017年度比2.6ポイント増、「アイデンティティ・アクセス管理製品」の2017年度比3.9ポイント増、「システムセキュリティ管理製品」の2017年度比8.9ポイント増等、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」は横ばい傾向にある。

情報セキュリティサービスの市場規模全体では、2017年度から2018年度は3.8ポイント伸びている。サービス別に見ると、「セキュリティ運用・管理サービス」の2017年度比4.0ポイント増、「セキュアシステム構築サービス」の前年度比1.6ポイント増を始め、各分類でおおむね増加傾向が続いている。

2.7.2 データ利活用の実態と動向

データを有効活用し、技術革新や生産性向上といった新たな付加価値の創出や課題解決を目指すべく提唱された「Connected Industries※431」の観点から、データを安心・安全に利活用できる環境整備をするため、2018年に不正競争防止法の改正がなされた。同改正では、これまで保護の対象となってきた「営業秘密」に加え、他者に提供することを想定した上で管理するデータ(「限定提供データ※432」)に対する不正取得等を不正競争行為として位置付け、当該行為に対する救済が可能となった。しかし、価値あるデータを保有する企業・研究機関等において、他者にデータを提供することを前提としたビジネスモデルの構築や、その実現にあたって必要となる知的財産戦略やデータの漏えい防止策の検討等、様々な課題に取り組む必要がある。

経済産業省では、2018年に「産業データ共有促進事業※433」として、Connected Industries重点5分野の協調領域における事業者等が保有するデータのさらなる活用(共有・共用)のため、その基盤となるシステムを補助する事業を実施し、衛星データ、宿泊ビッグデータ、船舶運航データ、カメラ画像データ、素材・化学研究開発データ、プラントデータ・解析モデル等を活用する25件が採択されている。

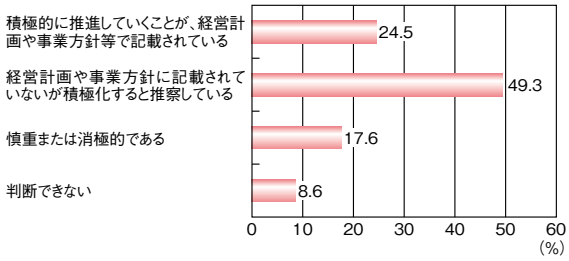
こうした状況を踏まえ、企業のデータ利活用における全般的な実態を明らかにするため、IPAは2018年度に「安全なデータ利活用に向けた準備状況及び課題認識に関する調査※434」を実施した。本調査では東京証券取引所の上場企業(一部、二部、マザーズ)やコンソーシアム、及び有識者を対象に、データ利活用の実態と安全なデータ利活用に関する課題・対応策等を調査している。本項では、本調査で得られた結果を紹介する。

(1)データ利活用の実態

企業におけるデータ利活用の事業としての位置付けや懸念等の実態について述べる。なお、以下でデータの取得について述べる場合、当該データは他社・他組織から取得することを意味する。

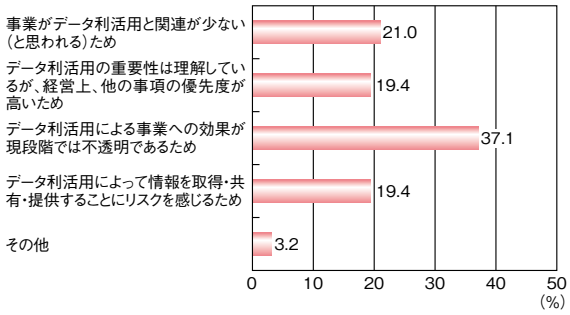
(a)企業の事業方針におけるデータ利活用の位置付け

企業の事業方針におけるデータ利活用の位置付けの現状は、「経営計画や事業方針に記載されていないが積極化すると推察している」割合が49.3%と最も高く、次いで「積極的に推進していくことが、経営計画や事業方針等で記載されている」が24.5%と高くなっている(図2-7-3)。



■図2-7-3　データ利活用の位置付け(現状)(n=278)
(出典)IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

また、図2-7-3でデータ利活用に「慎重または消極的である」あるいは「判断できない」と回答した社に対して更にその理由を質問した結果、「データ利活用による事業への効果が現段階では不透明であるため」の割合が37.1%と最も高く、次いで「事業がデータ利活用と関連が少ない(と思われる)ため」が21.0%と高くなっている(図2-7-4)。

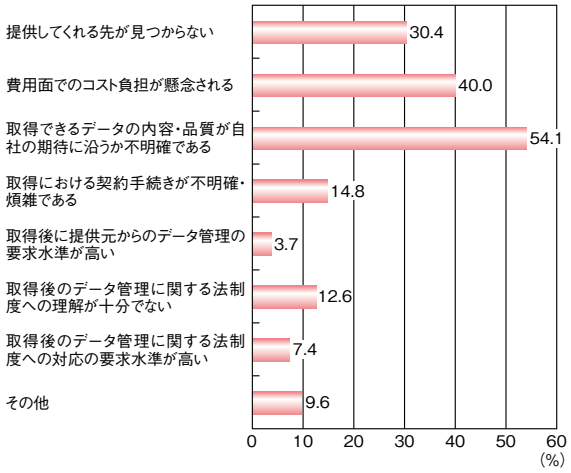


■図2-7-4　データ利活用を推進しない理由(n=62)
(出典)IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

(b) データ利活用に関する懸念

データ利活用を推進したいにもかかわらず「データを取得していない（できていない）理由」について、「取得できるデータの内容・品質が自社の期待に沿うか不明確である」を挙げている企業の割合が 54.1% と最も高く、次いで「費用面でのコスト負担が懸念される」が 40.0% と高くなっている（図 2-7-5）。

このことから、データを取得していない主な理由としては、費用対効果が不透明である点が懸念されていると推測される。



■図 2-7-5　データを取得しない理由（複数選択、n=135）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

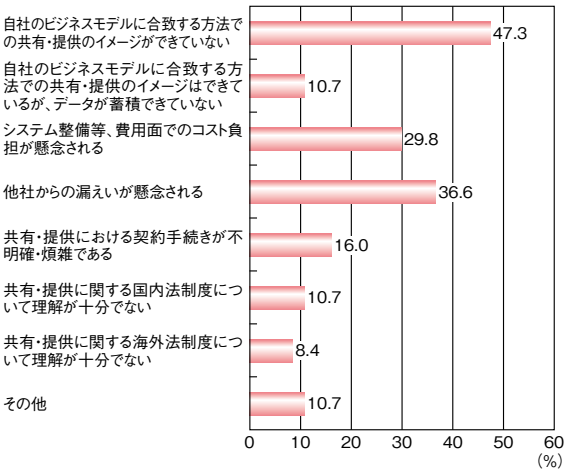
またデータ利活用においては、自社のデータを他社へ提供することも期待されるが、現状「データを共有・提供していない（できていない）理由」については、「自社のビジネスモデルに合致する方法での共有・提供のイメージができていない」を挙げている企業の割合が 47.3% と最も高く、「他社からの漏えいが懸念される」が 36.6%、「システム整備等、費用面でのコスト負担が懸念される」が 29.8% で続いている（図 2-7-6）。

このことから、データの共有・提供に対して慎重となる要因としてデータ利活用を前提としたビジネスモデルを構築していない点、漏えいリスクの懸念が挙げられる。

(c) IoT 機器・システムのデータ利活用

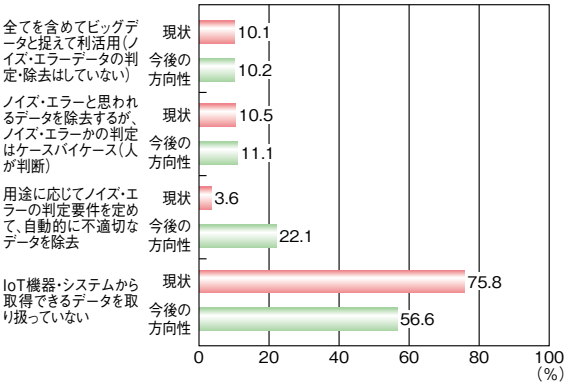
IoT 機器・システムからの取得データの品質管理については、「IoT 機器・システムから取得できるデータを取り扱っていない」企業の割合が 75.8% と最も高く、IoT 機器・システムの利用が現状では進んでいないと推測される。

しかしながら、「今後の方向性」として IoT データを扱わないとする企業は 56.6% であり、19.2 ポイント低くなっていることから、IoT データの利用が拡大すると推測される。



■図 2-7-6　データを共有・提供しない理由（複数選択、n=131）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

また、「用途に応じてノイズ・エラーの判定要件を定めて、自動的に不適切なデータを除去」では「今後の方向性」が 18.5 ポイント高くなっており、IoT 機器・システムのデータ品質管理について AI 等を利用してノイズ・エラーを自動的に判定・除去する必要性を認識していることが推測される（図 2-7-7）。



■図 2-7-7　IoT 機器・システムのデータ品質管理
（現状：n=248、今後の方向性：n=235）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

(d) データ取引・流通プラットフォームの運営形態

データ取引・流通プラットフォームにおけるデータ利活用のビジネスモデルは、データ自体を保有して新たなサービスを創出するもの（データ保有型）と、データ自体は保有しないでデータ提供者とデータ利用者がマッチングする場を提供するだけのもの（第三者市場運営型）に大別

できることが確認された。

データ保有型は、データ取引・流通プラットフォーム運営企業（以下、運営企業）がデータを大量に保有しており、運営企業がそのデータを分析し、既存の取引先企業（データ提供者とデータ利用者）に対して付加価値のある新しいサービスの提供が可能である（図 2-7-8）。

第三者市場運営型は、データ取引･流通プラットフォームの運営自体が運営企業の収益になる。そのため、取り引きされるデータの種類・量が自社の収益と直接的につながることから、データ提供者の参加を促すインセンティブの付与が重要である（図 2-7-9）。

(2) 安全なデータ利活用の課題と推進に向けて

以下、データ利活用の実態から見えた課題を踏まえつつ、安全なデータ利活用を行うための課題と推進に向けた環境整備について述べる。

(a) 安全なデータ利活用の課題

安全なデータ利活用における課題（他社・コンソーシアムとのデータ取得、共有・提供）についてのアンケート調査結果では、課題の第 1 位に「秘密保持契約の締結」を挙げている企業の割合が 46.7% と最も高く、次いで「流出防止対策」が 21.3% となっている（次ページ図 2-7-10）。

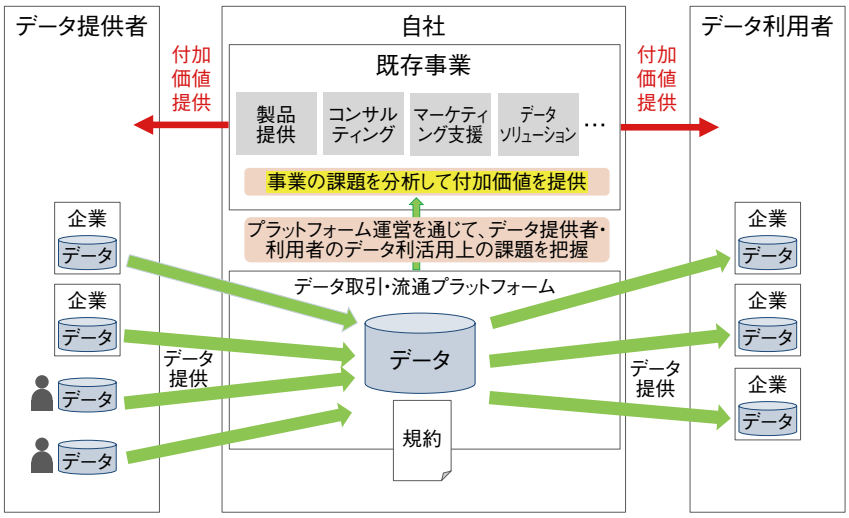
インタビュー調査を含めて、安全なデータ利活用の課題をまとめると、次の四つの観点が挙げられる。

- ビジネスモデル、成果イメージの具体化

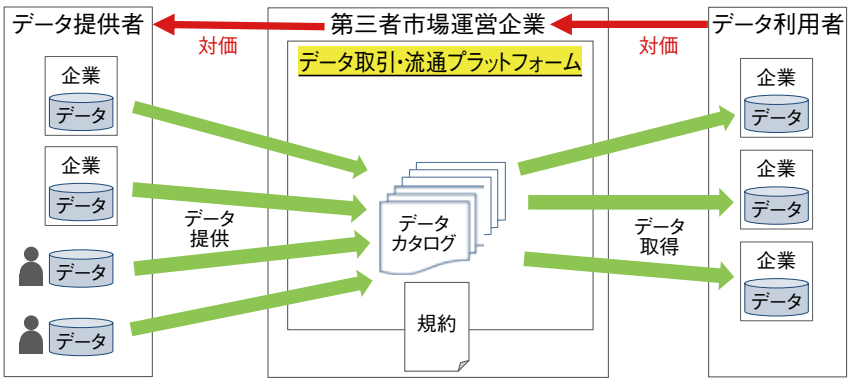
  データ利活用の費用対効果が不透明であるという課題に対しては、データ利活用を事業に組み入れる場合のビジネスモデルの類型化、特定の業種・データの流通・取引プラットフォーム構築による付加価値の明確化、成功事例の蓄積・共有によるデータ利活用の効果イメージの具体化等が重要である。

- 契約・規約

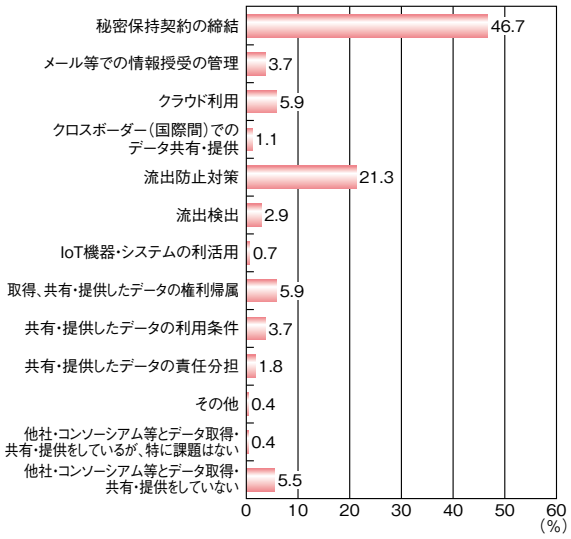
  不正競争防止法が改正され、2019 年 7 月 1 日から



■図 2-7-8　データ保有型のデータ取引・流通プラットフォーム
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成



■図 2-7-9　第三者市場運営型のデータ取引・流通プラットフォーム
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成



■図 2-7-10　安全なデータ利活用の課題（第 1 位）（n=272）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を基に作成

施行されたことから、法規制や契約を全社的に見直す体制を整備する必要がある。また、今後のデータ利活用に関する契約においては、「AI・データの利用に関する契約ガイドライン※435」等を参考に、データの帰属を明確化することやデータ品質を担保することも重要となる。

- 情報漏えい対策
  情報漏えい対策としては、従業員一人ひとりのセキュリティ意識のような人的側面のガバナンスに加えて、技術的側面からは、データのトレーサビリティ（アクセス履歴、メール送信履歴等の記録）、電子証明（電子署名、タイムスタンプ等）※436といった対策も必要となる。
- データの品質
  データ利活用の利用者が、データ取引・流通プラットフォームを選択して利用する際、データの品質は利用者にとって重要である。現在は、データ取引・流通プラットフォームの運営事業者認定基準※437、データの要件、品質基準等について細部が検討され、一部試行されている段階である。

(b) 安全なデータ利活用の推進に向けて

今後、データ利活用に取り組む企業は、データ利活用に関する事業でのビジネスモデルや成果イメージを具体化し、その上で対処すべきリスクを見定め、対応策を講じることが重要である。そのためには、事例の蓄積・参照が有効であり、政策として安全なデータ利活用を推進し、事業成果につながっている事例の調査・共有（公開）に取り組むことは重要である。

また、データ利活用に関する事業の一層の推進にあたっては、秘密保持契約締結にあたり、「限定提供データ」の扱いを明文化する必要があり、「情報漏えい対策」については、これまでの人為的な情報漏えい対策に加え、最新の技術的な情報漏えい対策（トレーサビリティ等）を実施する必要がある。

更に、企業の事業戦略におけるグローバル化はデータ利活用に関する事業にも当てはまる。データ利活用の海外展開にあたっては、各国・地域における関連法制度の差異に留意することが必要である。

2.7.3 暗号技術の動向

一般に暗号技術は、共通鍵暗号系の技術（以下、「共通鍵暗号」）と公開鍵暗号系の技術（以下、「公開鍵暗号」）とに大別される。本項では 2018 年度における、共通鍵暗号、公開鍵暗号に係る研究及び標準化の動向についてそれぞれ解説する。

(1) 共通鍵暗号に係る研究及び標準化の動向

共通鍵暗号に対する攻撃に係る研究として、2015 年度は「CRYPTREC 暗号リスト」掲載のブロック暗号 MISTY1 に対する攻撃に、また、2016 年度は同リスト掲載のハッシュ関数 SHA（Secure Hash Algorithm）-1 に対する攻撃に大きな進展があった。

2017 年度は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、着実な進展がいくつかあったものの、2015 年度の MISTY1、2016 年度の SHA-1 への攻撃に相当するような大きな進展はなかった。続く 2018 年度も既存暗号アルゴリズムへの攻撃において着実な進展はいくつかあるものの、大きな進展はないまま終わるかに思われた。

しかし 2018 年 11 月、一本の論文※438 が国際暗号学会 IACR※439 の ePrint※440 において公開された。その論文は、認証暗号のカテゴリーで国際標準（ISO/IEC 19772）として採用されている六つの認証暗号の一つである「OCB2」を攻撃対象とするものであった。具体的には「OCB2」の認証暗号としての「改ざん検知機能」に対する攻撃で、現実的な攻撃コストによって「改ざん検知」を誤認させる（すなわち「改ざん」が可能となる）手法を示していた。

以下に認証暗号「OCB2」の概要、ePrint で公開された OCB2 の攻撃論文の概要、その後の関連研究の動向、ISO 国際標準等における影響について示す。

(a) 認証暗号「OCB2」とは

認証暗号とは、共通鍵暗号（主にブロック暗号）によって実現される暗号技術（プロトコル）の一つである。共通鍵暗号のベース機能であるデータの秘匿（暗号化）に加えて、データに改ざん検知用のタグデータを生成・付加することによって、改ざん検知を同時に行うことができる。

認証暗号「OCB2」は、世界的に著名な暗号研究者である Phillip Rogaway 氏らによって提案された OCB（Offset Code Book）と名付けられた認証暗号の三つあるバージョン（OCB1、OCB2、OCB3）の一つである。OCB1 は 2001 年に仕様が論文※441 によって公開され、後に無線 LAN のセキュリティ規格（IEEE802-11）に提案された。OCB2 は 2004 年に仕様が論文※442 によって公開され、その後、ISO 国際標準の認証暗号のカテゴリーに提案され採択された。OCB3 は 2011 年に仕様が論文※443 によって公開され、その後、国際的な認証暗号コンペティションである CAESAR※444 に提案され、現在、ファイナリストの一つに残っている。また OCB3 はインターネット技術の国際標準を策定する IETF の議論を経て RFC7253※445 として採用されている。

OCB シリーズの仕様の特長としては、すべてのバージョン（OCB1、OCB2、OCB3）において安全性が数学的に証明されていること、及び構造がシンプルで実用性に優れていることが挙げられる。これらの特長により OCB シリーズは上述のような様々な標準化の場に提案され、採択または採択されつつある状況にある。

(b) OCB2 の攻撃論文の概要について

OCB2 の攻撃論文の核心となる部分は、「OCB2 の安全性の証明に誤りがあった」ことと、「OCB2 は認証暗号としての改ざん検知機能に問題があり、改ざん攻撃（偽造攻撃）が可能である」ことである。攻撃論文はその誤りの部分に着目し、実際の攻撃にまで結び付けている。

(c) 関連研究動向について

前述の OCB2 の攻撃論文が ePrint に公開された後、ePrint で 2 件の攻撃論文※446 が公開された。それらの論文の核心となる部分は、「OCB2 は認証暗号としての秘匿機能に問題があり、例えば平文回復攻撃が可能である」ことである。この攻撃論文と前述の最初の攻撃論文から、「OCB2 は認証暗号としての二つの機能（秘匿、改ざん検知）の両方に欠陥があり、認証暗号として（完全に）不適切である」と言えたことになる。更にその後も OCB2 の攻撃論文が公開されている※447 が、いずれも上記の三つの論文の詳細版や改良版に相当するものである。

(d) ISO 国際標準等における影響について

OCB2 が提案・採択されている ISO（ISO/IEC 19772）では、これらの攻撃論文が公開されたことから OCB2 への対応を検討し、OCB2 の使用取りやめ要請と規格からの削除をアナウンスした（「2.5.2 (2) WG 2（暗号とセキュリティメカニズム）」参照）。

なお、これまで公開されている OCB2 に対する攻撃は OCB2 にのみ適用可能であり、他の OCB シリーズ（OCB1、OCB3）に対しては適用が不可であることが示されていることから、現在判明している範囲では ISO 以外の国際標準等について影響はない。

日本では、電子政府推奨暗号を議論する CRYPTREC において CRYPTREC 暗号リスト（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）を策定・公開している。CRYPTREC 暗号リストは 2018 年 3 月の小改定において新たな技術分類として「認証暗号」が新設された。しかし、OCB2 を含む OCB シリーズに関しては現在のところ、どのリストの「認証暗号」にも採択されていないという状況であり、影響は出ていない。

(2) 公開鍵暗号に係る研究及び標準化の動向

NIST による「量子計算機に耐性を持つ暗号（耐量子暗号、PQC：Post-Quantum Cryptography）」の標準化が本格的に開始され、公開鍵暗号研究の多くは耐量子暗号を対象とする傾向にある。2017 年 11 月 30 日に暗号公募が締め切られた時点では、6 大陸 25 ヵ国から応募があり、応募総数は 82 件と発表されたが、仕様の精査を経て第 1 ラウンドの対象は計 69 件となった※448。

2018 年 4 月 9 ～ 13 日に米国フロリダ州フォートローダーデールにて国際会議 PQCrypto 2018 及び第 1 回 NIST PQC 標準化会議が開催された。更に 5 件の取り下げを経て、その時点での対象暗号は 64 件であった。その内訳件数を表 2-7-2（次ページ）に示す。

2018 年 12 月 22 日以降、米国政府機関閉鎖の影響で約 1 ヵ月にわたり NIST 耐量子暗号チームの活動は停止したが、再開後の 1 月 30 日には、第 2 ラウンドへ進む 26 件が発表された※450。その内訳件数を表 2-7-3（次ページ）に示す。

第 2 ラウンドへ進んだ 26 件のアルゴリズム名を以下に示す。

	署名	鍵確立／暗号化	合計
格子ベース	5	21	26
符号ベース	2	17	19
多変数	7	2	9
対称/ハッシュベース	3	0	3
その他	2	5	7
合計	19	45	64

■表 2-7-2　NIST PQC コンペティション応募暗号（第 1 ラウンド）
（出典）Dustin Moody（NIST）「Let's Get Ready to Rumble - The NIST PQC "competition"」[※449]を基に IPA が編集

	署名	鍵確立／暗号化	合計
格子ベース	3	9	12
符号ベース	0	7	7
多変数	4	0	4
対称/ハッシュベース	2	0	2
その他	0	1	1
合計	9	17	26

■表 2-7-3　NIST PQC コンペティション応募暗号（第 2 ラウンド）
（出典）NIST「Round 2 Submissions」[※450]を基に IPA が作成

- 鍵確立／暗号化アルゴリズム
  - 格子ベース：
    CRYSTALS-KYBER、FrodoKEM、LAC、NewHope、NTRU、NTRU Prime、Round5、SABER、Three Bears
  - 符号ベース：
    BIKE、Classic McEliece、HQC、LEDAcrypt、NTS-KEM、ROLLO、RQC
  - その他：
    SIKE（同種写像ベース）
- 署名アルゴリズム
  - 格子ベース：
    CRYSTALS-DILITHIUM、FALCON、qTESLA
  - 多変数：
    GeMSS、LUOV、MQDSS、Rainbow
  - 対称／ハッシュベース：
    Picnic、SPHINCS+

今後は 2019 年 8 月に第 2 回 NIST PQC 標準化会議が開催され、2020 ～ 2021 年に最終アルゴリズムを選択するか、または第 3 ラウンドへ進み、2022 ～ 2024 年に標準ドラフトを公開する予定となっている。

COLUMN

サイバーセキュリティリスク対策に「サイバー保険」という選択肢も

みなさんは、「サイバー保険」を知っていますか。

サイバー保険とは、サイバーリスクに起因する損害や調査費用等に対して金銭的な補償を受けられる保険です。「個人情報漏えい保険」は情報漏えいによる被害者への損害賠償金や費用損害に対する補償に限られていましたが、サイバー保険はそれらの補償に加えて、サイバー攻撃による業務停止に伴う損失利益の補償、原因調査、再発防止策の策定・実施費用等も対象となり、包括的な補償であるという違いがあります。

サイバー攻撃は日々進化しており、日常の業務に潜むサイバーリスクも日増しに大きくなる中、サイバーセキュリティ対策に充てられる予算にも限りがあり、残存リスクがなかなか低減しないことが、多くの企業で課題となっていると思われます。このような中、サイバー保険の加入により情報漏えい以外のインシデントによる金銭的損失が補償されることは、残存リスクにより想定外の損失を被ることへの対策となります。

経済産業省とIPAが策定している「サイバーセキュリティ経営ガイドライン[i]」でもリスク移転の対策例の一つとして、サイバー保険への加入が挙げられています。企業によって業務形態や扱う情報の機密の度合いや保有量等が異なるため、サイバー保険の加入だけではリスクを完全に移転することはできませんが、自社のセキュリティリスク分析（評価）の結果及びサイバー保険の補償内容や加入費用との兼ね合いによっては、経営戦略において検討すべき選択肢と言えそうです。

サイバー保険の加入は、セキュリティインシデントが発生した場合の賠償に対する資力の確保だけでなく、社内のセキュリティ態勢や意識の向上、取引先からの信頼力向上等にもつながります[ii]。サイバー保険に加入した場合でも、サイバーリスクに起因する事故を発生させないための対策は必要となりますが、今後、自社のセキュリティリスクを見直す際には、サイバー保険についても情報を収集した上で、サイバーセキュリティリスク対策の選択肢の一つとして検討してみてはいかがでしょうか。

i　https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔参照 2019-06-25〕
ii　一般社団法人日本損害保険協会：「サイバー保険に関する調査 2018」 http://www.sonpo.or.jp/cyber-hoken/data/pdf/cyber_report2018.pdf〔参照 2019-06-25〕

※ 1　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：国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みを指す。国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
※ 2　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf〔参照 2019-06-15〕
※ 3　NISC：サイバーセキュリティ戦略（閣議決定）の詳細概要　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-shousaigaiyou.pdf〔参照 2019-06-15〕
※ 4　NISC：サイバーセキュリティ 2018　https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf〔参照 2019-06-15〕
※ 5　IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集　https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔参照 2019-06-15〕
※ 6　サイバーセキュリティタスクフォース：総務省が 2017 年 1 月に設置した、IoT/AI 時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取り組みの改善等幅広い観点から検討を行い、必要な方策を推進することを目的とした組織。
※ 7　総務省：セキュリティ対策情報開示ガイドライン（仮称）に係る論点（案）　http://www.soumu.go.jp/main_content/000597448.pdf〔参照 2019-06-15〕
総務省：今後のスケジュール（案）　http://www.soumu.go.jp/main_content/000597450.pdf〔参照 2019-06-15〕
※ 8　IPA：コラボレーション・プラットフォームについて　https://www.ipa.go.jp/security/announce/collapla_index.html〔参照 2019-06-15〕
※ 9　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（CPSF）を策定しました　https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html〔参照 2019-06-15〕
※ 10 経済産業省：クラウドサービスの安全性評価に関する検討会について https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf
※ 11 NISC：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の取組状況　https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou09.pdf〔参照 2019-06-15〕
※ 12 NISC：サイバーセキュリティ対処調整センターについて　https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryou11.pdf〔参照 2019-06-15〕
東京都：東京 2020 大会の安全・安心の確保のための対処要領（第二版）　http://www.metro.tokyo.jp/tosei/hodohappyo/press/2019/04/16/documents/13_02.pdf〔参照 2019-06-15〕
※ 13 経済産業省：「ASEAN 等向け日米サイバー共同演習」を実施しました　https://www.meti.go.jp/press/2018/09/20180914008/20180914008.html〔参照 2019-06-15〕
※ 14 NISC：サイバーセキュリティ人材育成取組方針の決定について https://www.nisc.go.jp/conference/cs/pdf/jinzai-hoshin2018.pdf〔参照 2019-06-15〕
※ 15 内閣府：戦略的イノベーション創造プログラム（SIP）概要　https://www8.cao.go.jp/cstp/gaiyo/sip/sipgaiyou.pdf〔参照 2019-06-15〕
※ 16 内閣府：戦略的イノベーション創造プログラム（SIP）IoT 社会に対応したサイバー・フィジカル・セキュリティ研究開発計画　https://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/3_iot.pdf〔参照 2019-06-15〕
※ 17 NISC：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　https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔参照 2019-06-15〕
※ 18 NISC：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（改定）　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf〔参照 2019-06-15〕
※ 19 NISC：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）　https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf〔参照 2019-06-15〕
※ 20 NISC：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）　https://www.nisc.go.jp/active/infra/shisaku1.html〔参照 2019-06-15〕
※ 21 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（初版）　https://www.nisc.go.jp/active/infra/pdf/hyouka_kijun_shohan.pdf〔参照 2019-06-15〕
※ 22 NISC：2020 年オリパラ東京大会に向けた分野横断的演習のあり方について　https://www.nisc.go.jp/conference/cs/ciip/dai17/pdf/17shiryo08.pdf〔参照 2019-06-15〕
※ 23 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 https://www.meti.go.jp/press/2017/12/20171226004/20171226004.html〔参照 2019-06-15〕
※ 24 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　https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_05_00.pdf〔参照 2019-06-15〕
※ 25 経済産業省：産業サイバーセキュリティ強化へ向けたアクションプラン　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔参照 2019-06-15〕
※ 26 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。　https://www.meti.go.jp/press/2018/05/20180502003/20180502003.html〔参照 2019-06-15〕
※ 27 経済産業省：ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20180903_report.html〔参照 2019-06-15〕
※ 28 経済産業省：産業サイバーセキュリティ研究会 WG1 分野横断 SWG の設置について　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/pdf/001_04_00.pdf〔参照 2019-06-15〕
※ 29 対策要件のカテゴリは NIST の「Cybersecurity Framework Version 1.1」に対応する形で整理している。
※ 30 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 Version 1.0　https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf〔参照 2019-06-15〕
※ 31 転写：CPSF においては、温度や距離等の物理事象をデータに変換するといった、サイバー空間とフィジカル空間の境界において行われる情報の変換を意味する。
※ 32 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」策定後の WG1 の進め方（案）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/005_08_00.pdf〔参照 2019-06-15〕
※ 33 https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/pdf/2_016_04_00.pdf〔参照 2019-06-15〕
※ 34 経済産業省・IPA：サイバーセキュリティ経営ガイドライン Ver2.0 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔参照 2019-06-15〕
※ 35 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf〔参照 2019-06-15〕
経済産業省：産業サイバーセキュリティの加速化指針 ～アクションプランの深化・拡大～　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/003_04_00.pdf〔参照 2019-06-15〕
※ 36 IPA：中小企業の情報セキュリティ対策ガイドライン　https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html〔参照 2019-06-15〕
※ 37 戦略マネジメント層：「サイバーセキュリティ戦略」では、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」と定義している。
※ 38 経済産業省：事務局説明資料（産業サイバーセキュリティ研究会 WG3（サイバーセキュリティビジネス化）第 3 回）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/003_03_00.pdf〔参照 2019-06-15〕
※ 39 日本経済再生本部：未来投資戦略 2018　https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf〔参照 2019-06-15〕
※ 40 各府省情報化統括責任者（CIO）連絡会議：政府情報システムにおけるクラウドサービスの利用に係る基本方針　https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔参照 2019-06-15〕
※ 41 経済産業省：「クラウドサービスの安全性評価に関する検討会　中間とりまとめ（案）」の意見公募手続（パブリックコメント）を開始します https://www.meti.go.jp/press/2018/03/20190315002/20190315002.html〔参照 2019-06-15〕
総務省：クラウドサービスの安全性評価に関する検討会　中間とりまとめ（案）に対する意見募集　http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000277.html〔参照 2019-06-15〕
※ 42 経済産業省：データの利用権限に関する契約ガイドライン ver1.0　https://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf〔参照 2019-06-15〕
※ 43 経済産業省：「AI・データの利用に関する契約ガイドライン」を策定しました　https://www.meti.go.jp/press/2018/06/20180615001/20180615001.html〔参照 2019-06-15〕
※ 44 衆議院：議案名「産業競争力強化法等の一部を改正する法律案」の審議経過情報　http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DC7D8E.htm〔参照 2019-06-15〕
経済産業省：「産業競争力強化法」の一部改正が施行されました https://www.meti.go.jp/press/2018/07/20180709006/201807

09006.html〔参照 2019-06-15〕
※ 45 経済産業省：重要技術マネジメント　https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔参照 2019-06-15〕
※ 46 経済産業省：「中小企業等経営強化法」及び「中小企業における経営の承継の円滑化に関する法律」の一部改正が施行されました　https://www.meti.go.jp/press/2018/07/20180709007/20180709007.html〔参照 2019-06-15〕
中小企業庁：認定情報処理支援機関（スマート SME サポーター）　https://www.chusho.meti.go.jp/keiei/gijut/2018/180709supporter.htm〔参照 2019-06-15〕
※ 47 中小企業庁：認定情報処理支援機関制度に関する説明会を開催します　https://www.chusho.meti.go.jp/keiei/gijut/2018/180726setsumeikai.htm〔参照 2019-06-15〕
※ 48 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　https://www.meti.go.jp/press/2017/02/20180228002/20180228002.html〔参照 2019-06-15〕
※ 49 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合するとIPAが確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※ 50 IPA：情報セキュリティサービス基準適合サービスリストの公開　https://www.ipa.go.jp/security/it-service/service_list.html〔参照 2019-06-15〕
※ 51 経済産業省：「革新的データ産業活用計画」認定申請のご利用の手引き　https://www.meti.go.jp/policy/it_policy/data-katsuyo/iot-zeisei/190327tebiki.pdf〔参照 2019-06-15〕
※ 52 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。
※ 53 https://www.ipa.go.jp/files/000073456.pdf〔参照 2019-06-15〕
※ 54 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。
※ 55 IPA：ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）　https://www.ipa.go.jp/files/000068781.pdf〔参照 2019-06-15〕
※ 56 IQY ファイル：Microsoft Excel に関連付けされている、拡張子が「.iqy」のファイル。当該ファイルを開くと Microsoft Excel が起動する。
※ 57 IPA：IQY ファイルを悪用する攻撃手口に関する注意点（第二版）　https://www.ipa.go.jp/files/000068065.pdf〔参照 2019-06-15〕
※ 58 「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。
※ 59 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 2019-06-15〕
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 2019-06-15〕
※ 60 http://www.soumu.go.jp/main_content/000461785.pdf〔参照 2019-06-15〕
※ 61 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 2019-06-15〕
※ 62 http://www.soumu.go.jp/main_content/000478813.pdf〔参照 2019-06-15〕
※ 63 http://www.soumu.go.jp/main_content/000510701.pdf〔参照 2019-06-15〕
※ 64 http://www.soumu.go.jp/main_content/000566458.pdf〔参照 2019-06-15〕
※ 65 https://www.ipa.go.jp/security/J-CRAT/index.html〔参照 2019-06-15〕
※ 66 WirelessWireNews：セキュアなIoTプラットフォームの確立を支援へ、総務省の「IoTセキュリティ総合対策」レポート　https://wirelesswire.jp/2018/08/66521/〔参照 2019-06-15〕
総務省：IoT セキュリティ総合対策　http://www.soumu.go.jp/main_content/000510701.pdf〔参照 2019-06-15〕
※ 67 http://www.iotac.jp/wp-content/uploads/2016/01/IoT 機器のセキュリティ対策に関する検討の方向性 .pdf〔参照 2019-06-15〕
※ 68 総務省：「IoT セキュリティ基盤を活用した安心安全な社会の実現に向けた実証実験」の結果の公表　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000155.html〔参照 2019-06-15〕
※ 69 総務省：IoT 機器に関する脆弱性調査等の実施　http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html〔参照 2019-06-15〕
※ 70 総務省：IoT 機器に関する脆弱性調査等の実施結果の公表　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000154.html〔参照 2019-06-15〕
※ 71 総務省：新規制定・改正法令・告示　法律「電気通信事業法及び国立開発研究法人情報通信研究機構法の一部を改正する法律（平成 30 年法律第 24 号）」　http://www.soumu.go.jp/menu_hourei/s_houritsu.html〔参照 2019-06-15〕
※ 72 NICT：日本国内でインターネットに接続された IoT 機器等に関する事前調査の実施について　https://www.NICT.go.jp/info/topics/2018/11/07-2.html〔参照 2019-06-15〕
※ 73 https://notice.go.jp/〔参照 2019-06-15〕
※ 74 NISC：サイバーセキュリティ戦略本部第 21 回会合　総務省提出資料　https://www.nisc.go.jp/conference/cs/dai21/pdf/21sankou.pdf〔参照 2019-06-15〕
Security NEXT：政府の脆弱 IoT 機器調査「NOTICE」、2 月 20 日から - イメージキャラクターにカンニング竹山さん　http://www.security-next.com/102208〔参照 2019-06-15〕
※ 75 http://www.soumu.go.jp/main_content/000555901.pdf〔参照 2019-06-15〕
※ 76 総務省：情報開示分科会（第 8 回）開催案内　http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00027.html〔参照 2019-06-15〕
※ 77 総務省：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業の成果の公表　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000153.html〔参照 2019-06-15〕
※ 78 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 2019-06-15〕
※ 79 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 2019-06-15〕
※ 80 ICT-ISAC：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業について　https://www.ict-isac.jp/news/news20180629.html〔参照 2019-06-15〕
※ 81 ICT-ISAC：脅威情報の情報共有基盤利用ガイドライン（事業者向け）の概要　https://www.ict-isac.jp/news/ict-isac_tip_ov.pdf〔参照 2019-06-15〕
※ 82 NICT：実践的サイバー防御演習 CYDER　https://cyder.nict.go.jp/〔参照 2019-06-15〕
※ 83 NICT：サイバー演習自動化システム“CYDERANGE”の開発と実運用の開始　https://www.nict.go.jp/press/2018/03/08-1.html〔参照 2019-06-15〕
※ 84 NICT:cyber colosseo　https://colosseo.nict.go.jp/〔参照 2019-06-15〕
※ 85 http://www.soumu.go.jp/main_content/000566969.pdf〔参照 2019-06-15〕
※ 86 ITmedia：「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」（案）について　http://blogs.itmedia.co.jp/business20/2018/06/2.html〔参照 2019-06-15〕
※ 87 http://www.soumu.go.jp/main_content/000575052.pdf〔参照 2019-06-15〕
※ 88 http://www.soumu.go.jp/main_content/000575053.pdf〔参照 2019-06-15〕
※ 89 http://www.soumu.go.jp/main_content/000575399.pdf〔参照 2019-06-15〕
※ 90 総務省：「プラットフォームサービスに関する研究会」の開催　http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000050.html〔参照 2019-06-15〕
※ 91 総務省：トラストサービス検討ワーキンググループ（第 1 回）　http://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02cyber01_04000001_00016.html〔参照 2019-06-15〕
※ 92 総務省:プラットフォームサービスに関する研究会　中間報告書（案）　http://www.soumu.go.jp/main_content/000600599.pdf〔参照 2019-06-15〕
※ 93 総務省：トラストサービスに関する現状　http://www.soumu.go.jp/main_content/000583371.pdf〔参照 2019-06-15〕
※ 94 経理プラス：電子帳簿保存法のスキャナ保存要件となるタイムスタンプとは?　https://keiriplus.jp/tips/dencyohou_timestamp/〔参照 2019-06-15〕
※ 95 アマノセキュアジャパン株式会社：医療情報システムの安全管理に関するガイドライン　https://www.e-timing.ne.jp/info/law/medical-care-information/〔参照 2019-06-15〕
厚生労働省：医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）　https://www.mhlw.go.jp/stf/shingi2/0000166275.html〔参照 2019-06-15〕
※ 96 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 2019-06-15〕
※ 97 IPA：安心相談窓口だより　ネットワークカメラや家庭用ルータ等のIoT機器は利用前に必ずパスワードの変更を　https://www.ipa.go.jp/security/anshin/mgdayori20161125.html〔参照 2019-06-15〕
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 2019-06-15〕
※ 98 IPA：情報セキュリティ10大脅威 2018　https://www.ipa.go.jp/files/000065376.pdf〔参照 2019-06-15〕
※ 99 NISC：サイバーセキュリティ戦略の変更について　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔参照 2019-06-15〕
※ 100 警察庁：サイバーセキュリティ重点施策の改訂について（通達）https://www.npa.go.jp/cybersecurity/pdf/300906_juutensesaku.pdf〔参照 2019-06-15〕
※ 101 警察庁：平成30年警察白書　https://www.npa.go.jp/hakusyo/h30/pdf/07_dai3sho.pdf〔参照 2019-06-15〕
※ 102 トレンドマイクロ社：サイバー空間の探索行為が再び増加、2018年上半期の脅威動向｜警察庁　https://www.trendmicro.com/jp/iot-security/news/50223〔参照 2019-06-15〕
※ 103 警察庁：宛先ポート80/TCPに対するMiraiボットの特徴を有するアクセス増加について　http://www.npa.go.jp/cyberpolice/important/2018/201806131.html〔参照 2019-06-15〕
※ 104 http://www.internethotline.jp/〔参照 2019-06-15〕
※ 105 一般社団法人日本データ通信協会：サイバー空間における警察活動　https://www.dekyo.or.jp/info/2018/07/security/2639/〔参照 2019-06-15〕
警察庁：インターネット・ホットラインセンターの運用変更について　http://www.npa.go.jp/cyber/statics/h28/ihc_change.pdf〔参照 2019-06-15〕
※ 106 産経ニュース：サイバービル始動　警視庁、部署集約「総力挙げ結果」　https://www.sankei.com/region/news/180403/rgn1804030049-n1.html〔参照 2019-06-15〕
日本経済新聞：サイバー捜査の新拠点開設　部署横断で対処しやすく警視庁　https://www.nikkei.com/article/DGXMZO28867630020420 18CR0000/〔参照 2019-06-15〕
※ 107 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2019-06-15〕）。
※ 108 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 2019-06-15〕
※ 109 産経ニュース：匿名化ソフト「Tor」使い児童ポルノ公開疑い　京都府警が初摘発　https://www.sankei.com/west/news/180605/wst1806050108-n1.html〔参照 2019-06-15〕
※ 110 警察庁：平成30年上半期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/H30_kami_cyber_jousei.pdf〔参照 2019-06-15〕
※ 111 警察庁：仮想通貨を採掘するツール（マイニングツール）に関する注意喚起　https://www.npa.go.jp/cyber/policy/180614_2.html〔参照 2019-06-15〕
※ 112 警察庁：平成30年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/H30_cyber_jousei.pdf〔参照 2019-06-15〕
※ 113 日本経済新聞:ビジネスメールで6020万円詐取容疑　取引先装った4人逮捕　https://www.nikkei.com/article/DGKKZO32602020U8A700C1CC1000/〔参照 2019-06-15〕
※ 114 産経ニュース：パソコンなど押収し公開　アダルト動画詐欺、1万人9億2000万円被害か　愛知県警　https://www.sankei.com/west/news/180705/wst1807050041-n1.html〔参照 2019-06-15〕
※ 115 サイバーセキュリティ.com：セキュリティニュース：奈良県職員が不正アクセス禁止法違反の疑いで逮捕、女性職員の個人情報が目的か　https://cybersecurity-jp.com/news/27522〔参照 2019-06-15〕
※ 116 サンケイスポーツ：消せない画面…不正URL貼り付けた疑いで中1女子ら家宅捜索　https://www.sanspo.com/geino/news/20190304/tro19030418410013-n1.html〔参照 2019-06-15〕
※ 117 朝日新聞：仮想通貨「採掘」に他人のPC無断使用容疑　16人摘発　https://www.asahi.com/articles/ASL6F5QWJL6FUTIL04J.html〔参照 2019-06-15〕
※ 118 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）」（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf〔参照 2019-06-15〕）。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。
※ 119 CRYPTREC：耐量子計算機暗号の研究動向調査報告書の公開　https://www.cryptrec.go.jp/topics/cryptrec_20190405_tr_2001_2018.html〔参照 2019-06-15〕
※ 120 NIST：A Framework for Designing Cryptographic Key Management Systems　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf〔参照 2019-06-15〕
※ 121 外務省：G7シャルルボワ・サミット　https://www.mofa.go.jp/mofaj/ecm/ec/page4_004124.html#section7〔参照 2019-06-15〕
※ 122 外務省：人工知能の未来のためのシャルルボワ・共通ビジョン　https://www.mofa.go.jp/mofaj/files/000373835.pdf〔参照 2019-06-15〕
※ 123 U.S. Department of State：The Sixth U.S.-Japan Cyber Dialogue　https://www.state.gov/r/pa/prs/ps/2018/07/284573.htm〔参照 2019-06-15〕
※ 124 外務省：サイバーセキュリティに関する日米韓専門家会合の開催　https://www.mofa.go.jp/mofaj/press/release/press4_006290.html〔参照 2019-06-15〕
※ 125 外務省：日米首脳会談　https://www.mofa.go.jp/mofaj/na/na1/us/page4_004367.html〔参照 2019-06-15〕
※ 126 防衛省：岩屋防衛大臣とシャナハン米国防長官代行との会談の概要　http://www.mod.go.jp/j/approach/anpo/kyougi/2019/01/16_gaiyo.html〔参照 2019-06-15〕
※ 127 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 2019-06-15〕
※ 128 外務省：第4回日仏サイバー協議　https://www.mofa.go.jp/mofaj/press/release/press4_006129.html〔参照 2019-06-15〕
※ 129 外務省：第4回日英サイバー協議　https://www.mofa.go.jp/mofaj/press/release/press4_005821.html〔参照 2019-06-15〕
※ 130 外務省：日英首脳会談　https://www.mofa.go.jp/mofaj/erp/we/gb/page1_000713.html〔参照 2019-06-15〕
※ 131 個人情報保護委員会：日EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意　https://www.ppc.go.jp/enforcement/cooperation/cooperation/300717/〔参照 2019-06-15〕
※ 132 EC：REGULATIONS　http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf〔参照 2019-06-15〕
※ 133 個人情報保護委員会：日EU間の相互の円滑な個人データ移転を図る枠組み発効　https://www.ppc.go.jp/enforcement/cooperation/cooperation/310123/〔参照 2019-06-15〕
※ 134 外務省：第4回日・イスラエル・サイバー協議　https://www.mofa.go.jp/mofaj/me_a/me1/il/page23_002728.html〔参照 2019-06-15〕
※ 135 総務省：イスラエルとのサイバーセキュリティ分野における協力に関する覚書の署名　http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000079.html〔参照 2019-06-15〕
※ 136 経済産業省：第11回日・ASEANサイバーセキュリティ政策会議を開催しました　https://www.meti.go.jp/press/2018/10/20181026005/20181026005.html〔参照 2019-06-15〕
※ 137 http://aseanregionalforum.asean.org/〔参照 2019-06-15〕
※ 138 外務省：サイバーセキュリティに関する第1回ARF会期間会合等の開催　https://www.mofa.go.jp/mofaj/press/release/press4_005948.html〔参照 2019-06-15〕
※ 139 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3回専門家会合の開催　https://www.mofa.go.jp/mofaj/press/release/press4_007030.html〔参照 2019-06-15〕
※ 140 外務省：サイバーセキュリティに関する第2回ARF会期間会合等の開催　https://www.mofa.go.jp/mofaj/press/release/press4_007262.html〔参照 2019-06-15〕
※ 141 外務省：第3回日インド・サイバー協議の開催　https://www.mofa.go.jp/mofaj/press/release/press1_000330.html〔参照 2019-06-15〕
※ 142 The Washington Post：China hawks call on America to fight a new Cold War　https://www.washingtonpost.com/opinions/2019/04/10/china-hawks-call-america-fight-new-cold-war/?utm_term=.254f6654b930〔参照 2019-06-15〕
※ 143 The New York Times：North Korea Threatens to Scuttle Talks With the U.S. and Resume Tests　https://www.nytimes.com/2019/03/15/world/asia/north-korea-kim-jong-un-nuclear.html〔参照 2019-06-15〕
※ 144 CONGRESS.GOV：H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019　https://www.congress.gov/bill/115th-congress/house-bill/5515/text〔参照2019-06-15〕

※ 145 TechCrunch：New defense bill bans the U.S. government from using Huawei and ZTE tech https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/〔参照 2019-06-15〕
※ 146 TechCrunch：Huawei CFO arrested in Canada, awaits US extradition https://techcrunch.com/2018/12/05/huawei-cfo-arrested-in-canada-awaits-us-extradition/〔参照 2019-06-15〕
※ 147 BLOGOS：米国がファーウェイを禁止する本当の理由 https://blogos.com/article/369897/?p=2〔参照 2019-06-15〕
※ 148 The White House：NATIONAL CYBER STRATEGY of the United States of America https://assets.documentcloud.org/documents/4911834/Read-the-Trump-administration-s-National-Cyber.pdf〔参照 2019-06-15〕
※ 149 The White House：President Donald J. Trump Announces a National Security Strategy to Advance America's Interests https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-announces-national-security-strategy-advance-americas-interests/〔参照 2019-06-15〕
※ 150 JBPRESS：米国に桁外れサイバー攻撃、やはり中国の犯行だった http://jbpress.ismedia.jp/articles/-/54196〔参照 2019-06-15〕
※ 151 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 2019-06-15〕
※ 152 The White House：Executive Order Enhancing the Effectiveness of Agency Chief Information Officers https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-effectiveness-agency-chief-information-officers/〔参照 2019-06-15〕
※ 153 NIST：NICE Cybersecurity Workforce Framework https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework〔参照 2019-06-15〕
※ 154 EdSource：Trump's proposed regulations limiting benefits for immigrants could hurt many US-born children https://edsource.org/2018/trumps-proposed-regulations-limiting-benefits-for-immigrants-could-hurt-many-u-s-born-children/604645〔参照 2019-06-15〕
※ 155 MeriTalk：White House Orders Cyber Workforce Rotation, Reskilling Efforts https://www.meritalk.com/articles/white-house-orders-cyber-workforce-rotation-reskilling-efforts/?fbclid=IwAR0PqdkNkxast2g47IqfHGN0cR-tL39ozCiBUyR2KnXraTQY8rKdns0K9v4〔参照 2019-06-15〕
※ 156 本項目の原文は「結果を強制する（impose consequences）」であり、「制裁」の文言はないが、意訳した。
※ 157 Government Technology：New National Cyber Strategy Message: Deterrence Through U.S. Strength https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-national-cyber-strategy-message-deterrence-through-us-strength.html〔参照 2019-06-15〕
※ 158 USA TODAY: Cybersecurity：Donald Trump's new strategy allows more offensive operations https://www.usatoday.com/story/news/politics/2018/09/20/donald-trumps-new-cybersecurity-plan-allows-more-offensive-operations/1370946002/〔参照 2019-06-15〕
※ 159 DoD：SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF〔参照 2019-06-15〕
※ 160 FIFTH DOMAIN：DoD releases first new cyber strategy in three years https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/〔参照 2019-06-15〕
※ 161 DHS：U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf〔参照 2019-06-15〕
※ 162 Joint Force Quarterly Issue 92.1：An Interview with Paul M. Nakasone https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf〔参照 2019-06-15〕
※ 163 Shneier on Security：Gen. Nakasone on US Cyber Command https://www.schneier.com/blog/archives/2019/02/gen_nakasone_on.html〔参照 2019-06-15〕
※ 164 DHS：CISA CYBER + INFRASTRUCTURE https://www.dhs.gov/CISA〔参照 2019-06-15〕
※ 165 DHS：Christopher C. Krebs https://www.dhs.gov/person/christopher-c-krebs〔参照 2019-06-15〕
※ 166 DHS：CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams https://www.dhs.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams〔参照 2019-06-15〕
※ 167 REUTERS：米国土安全保障長官が辞任、解任との指摘も 不法移民対策巡り https://jp.reuters.com/article/nielsen-idJPKCN1RJ0QI〔参照 2019-06-15〕
※ 168 ZDNET Japan：グーグル、GDPR 違反で制裁金 62 億円 -- 仏当局 https://japan.zdnet.com/article/35131577/〔参照 2019-06-15〕
※ 169 EUR-REX：DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 https://eur-lex.europa.eu/eli/dir/2016/1148/oj〔参照 2019-06-15〕
※ 170 European Parliament：EU Cybersecurity Act ***I http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf?redirect〔参照 2019-06-15〕
※ 171 Noyb：GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf〔参照 2019-06-15〕
※ 172 Brave Software：Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR https://brave.com/adtech-data-breach-complaint〔参照 2019-06-15〕
※ 173 WIRED：EU PRIVACY LAW SNARES ITS FIRST TECH GIANT: GOOGLE https://www.wired.com/story/eu-privacy-law-snares-first-tech-giant-google/〔参照 2019-06-15〕
※ 174 BBC NEWS：Facebook fined £500,000 for Cambridge Analytica scandal https://www.bbc.com/news/technology-45976300〔参照 2019-06-15〕
※ 175 REUTERS：Facebook now says data breach affected 29 million users, details impact https://www.reuters.com/article/us-facebook-cyber/facebook-now-says-data-breach-affected-29-million-users-details-impact-idUSKCN1MM297〔参照 2019-06-15〕
※ 176 BLOGOS：針のむしろのフェイスブック https://blogos.com/article/373553/〔参照 2019-06-15〕
※ 177 Mayer Brown：Germany: Post GDPR Enforcement In Germany - A Sneak Peek http://www.mondaq.com/germany/x/802180/data+protection/Post+GDPR+enforcement+in+Germany+a+sneak+peek〔参照 2019-06-15〕
※ 178 独立行政法人日本貿易振興機構：GDPR 適用開始から 1 年、EU 市民の権利意識高まる https://www.jetro.go.jp/biznews/2019/05/96a07780c60ca6c5.html〔参照 2019-06-15〕
※ 179 BBC：Brexit: UK and EU agree delay to 31 October https://www.bbc.com/news/uk-politics-47889404〔参照 2019-06-15〕
※ 180 Legalfutures：GDPR and Brexit – a view from the European Commission https://www.legalfutures.co.uk/blog/gdpr-and-brexit-a-view-from-the-european-commission〔参照 2019-06-15〕
※ 181 BBC：Theresa May resigns over Brexit: What happened? https://www.bbc.com/news/uk-politics-48379730〔参照 2019-06-15〕
※ 182 個人情報保護委員会：日 EU 間の相互の円滑な個人データの移転 ～ボーダレスな越境移転が実現～ https://www.ppc.go.jp/files/pdf/310122_houdou.pdf〔参照 2019-06-15〕
※ 183 EUR-REX：REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010〔参照 2019-06-15〕
※ 184 Lex specialis（特別法）：ある特定の事項について、一般法よりも優先して適用される法律。
※ 185 IT Media NEWS：GDPR の次は「ePrivacy Regulation」―― Facebook や Google が警戒する規則とは https://www.itmedia.co.jp/news/articles/1805/29/news075.html〔参照 2019-06-15〕
※ 186 EC：State-of-play of the transposition of the NIS Directive https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive〔参照 2019-06-15〕
※ 187 EC：NIS Cooperation Group https://ec.europa.eu/digital-single-market/en/nis-cooperation-group〔参照 2019-06-15〕
※ 188 ENISA：Good practices on interdependencies between OES and DSPs https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps〔参照 2019-06-15〕
※ 189 Inside Privacy：European Parliament Approves EU

Cybersecurity Act https://www.insideprivacy.com/international/european-union/european-parliament-approves-eu-cybersecurity-act/〔参照 2019-06-15〕
※ 190 EC：The EU cybersecurity certification framework https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework〔参照 2019-06-15〕
※ 191 EC：European Commission recommends common EU approach to the security of 5G networks http://europa.eu/rapid/press-release_IP-19-1832_en.htm〔参照 2019-06-15〕
※ 192 The Telegraph：Theresa May defies security warnings of ministers and US to allow Huawei to help build Britain's 5G network https://www.telegraph.co.uk/politics/2019/04/23/theresa-may-defies-security-warnings-ministers-us-allow-huawei/〔参照 2019-06-15〕
※ 193 HCSEC Oversight Board：HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf〔参照 2019-06-15〕
※ 194 Tech Crunch：UK gives Huawei an amber light to supply 5G https://techcrunch.com/2019/04/24/uk-gives-huawei-an-amber-light-to-supply-5g/〔参照 2019-06-15〕
※ 195 Financial Times：German regulator says Huawei can stay in 5G race https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a〔参照 2019-06-15〕
※ 196 全国人民代表大会：中华人民共和国网络安全法 http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm〔参照 2019-06-15〕
※ 197 THE WALL STREET JOURNAL：U.S. Trade Negotiators Take Aim at China's Cybersecurity Law https://www.wsj.com/articles/u-s-trade-negotiators-take-aim-at-chinas-cybersecurity-law-11553867916〔参照 2019-06-15〕
大紀元 ¦EPOCH TIMES：米、中国に「ネット安全法」の撤廃を求める https://www.epochtimes.jp/2019/04/41633.html〔参照 2019-06-15〕
※ 198 BLOOMBERG：米中の通商協議が終了ー合意に至らずも決裂は回避、交渉継続へ https://www.bloomberg.co.jp/news/articles/2019-05-10/-10-jvhklmb1〔参照 2019-06-15〕
※ 199 CHINA BRIEFING：The US-China Trade War: A Timeline https://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/〔参照 2019-06-15〕
※ 200 東洋経済：トランプ政権が対中追加関税を決めた真の理由 https://toyokeizai.net/articles/-/281451〔参照 2019-06-15〕
※ 201 The White House：Executive Order on Securing the Information and Communications Technology and Services Supply Chain https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/〔参照 2019-06-15〕
※ 202 日本経済新聞：米、ファーウェイへの輸出を事実上禁止 https://www.nikkei.com/article/DGXMZO44862730W9A510C1MM0000/〔参照 2019-06-15〕
※ 203 TECH CRUNCH：ARM halts Huawei relationship following US ban https://techcrunch.com/2019/05/22/arm-halts-huawei-relationship-following-us-ban/〔参照 2019-06-15〕
※ 204 BBC：Huawei: China threatens to retaliate over US sanctions https://www.bbc.com/news/world-us-canada-48299522〔参照 2019-06-15〕
※ 205 国务院：国务院关于印发社会信用体系建设规划纲要（2014-2020 年）的通知 http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm〔参照 2019-06-15〕
※ 206 China copyright and Media：Planning Outline for the Construction of a Social Credit System (2014-2020) https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/〔参照 2019-06-15〕
※ 207 NEWSWEEK：14 億人を格付けする中国の「社会信用システム」本格始動へ準備 https://www.newsweekjapan.jp/stories/world/2018/05/14-8_2.php〔参照 2019-06-15〕
※ 208 MUFG：INNOVATION HUB 中国社会で活用が進む信用スコアは日本でも普及するのか? https://innovation.mufg.jp/detail/id=244〔参照 2019-06-15〕
※ 209 信用中国：https://www.creditchina.gov.cn/home/index.html〔参照 2019-06-15〕
※ 210 PRESIDENT Online：中国を変えた“信用格付けシステム”の怖さ https://president.jp/articles/-/26480〔参照 2019-06-15〕
※ 211 WIRED：The complicated truth about China's social credit system https://www.wired.co.uk/article/china-social-credit-system-explained〔参照 2019-06-15〕
※ 212 https://www.acsc.gov.au/〔参照 2019-06-15〕
※ 213 The Parliament of the Commonwealth of Australia, House of Representatives:Intelligence Service Amendment (Establishment of the Australian Signals Directorate Bill 2018 Explanatory Memorandum https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6047_ems_971b2a45-d794-4b0b-bd29-3a57a8c1d5ac/upload_pdf/662713.pdf;fileType=application%2Fpdf〔参照 2019-06-15〕
※ 214 https://asd.gov.au/〔参照 2019-06-15〕
※ 215 Department of the Information and Communication Technologies, Republic of the Philippines：National Cybersecurity Plan 2022 http://dict.gov.ph/national-cybersecurity-plan-2022/〔参照 2019-06-15〕
※ 216 http://dict.gov.ph/〔参照 2019-06-15〕
※ 217 https://www.ncert.gov.ph/〔参照 2019-06-15〕
※ 218 https://www.pngcert.org.pg/〔参照 2019-06-15〕
※ 219 https://www.nicta.gov.pg/〔参照 2019-06-15〕
※ 220 https://cert.gov.vu/〔参照 2019-06-15〕
※ 221 Office of the Government Chief Information Officer, Government of the Republic of Vanuatu：National Cybersecurity Policy https://ogcio.gov.vu/images/Cybersecurity-Policy-EN-FR-BI.pdf〔参照 2019-06-15〕
※ 222 https://www.apnic.net/〔参照 2019-06-15〕
※ 223 Sri Lanka CERT|CC：National Information and Cyber Security Strategy of Sri Lanka 2019-2013 http://www.slcert.gov.lk/Downloads/NCSStrategy.pdf〔参照 2019-06-15〕
※ 224 http://www.slcert.gov.lk/〔参照 2019-06-15〕
※ 225 Singapore Statutes Online：Cybersecurity Act 2018 https://sso.agc.gov.sg/Acts-Supp/9-2018/〔参照 2019-06-15〕
※ 226 https://www.csa.gov.sg/singcert〔参照 2019-06-15〕
※ 227 https://www.csa.gov.sg/〔参照 2019-06-15〕
※ 228 CSA Singapore：Cybersecurity Act https://www.csa.gov.sg/legislation/cybersecurity-act〔参照 2019-06-15〕
※ 229 APCERT：Documents https://www.apcert.org/documents/index.html〔参照 2019-06-15〕
※ 230 APCERT：APCERT CYBER DRILL ON NEW DDOS THREAT https://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf〔参照 2019-06-15〕
※ 231 The Diplomat: What's Next for the New ASEAN-Singapore Cyber Center? https://thediplomat.com/2018/09/whats-next-for-the-new-asean-singapore-cyber-center/〔参照 2019-06-15〕
※ 232 CERT Australia：Pacific Cyber Security Operational Network https://www.cert.gov.au/news/pacific-cyber-security-operational-network〔参照 2019-06-15〕
※ 233 2019 年 2 月現在、PaCSON に参加しているのは、オーストラリア、クック諸島、フィジー、キリバス、マーシャル諸島、ニュージーランド、ニウエ、パラオ、パプアニューギニア、サモア、ソロモン諸島、トケラウ、トンガ、バヌアツの 15 ヵ国。
※ 234 https://www.nisc.go.jp/conference/cs/pdf/jinzai-keiei2018set.pdf〔参照 2019-06-15〕
※ 235 https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf〔参照 2019-06-15〕
※ 236 戦略マネジメント層：サイバーセキュリティ戦略では、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」と定義している。
※ 237 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/003_03_00.pdf〔参照 2019-06-15〕
※ 238 経済産業省：事務局説明資料 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf〔参照 2019-06-15〕
※ 239 https://www.ipa.go.jp/files/000059086.pdf〔参照 2019-06-15〕
※ 240 https://www.juas.or.jp/cms/media/2017/02/it18_ppt.pdf〔参照 2019-06-15〕
※ 241 https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/index.html〔参照 2019-06-15〕
※ 242 NIST:National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf〔参照 2019-06-15〕
※ 243 JNSA：セキュリティ知識分野（SecBoK2019）～スキル中心から

タスク・ロールとの連携強化へ～　https://www.jnsa.org/result/2018/skillmap/〔参照 2019-06-15〕
※ 244 日本電気株式会社、株式会社日立製作所、富士通株式会社：NEC・日立・富士通、サイバーセキュリティ技術者の共通人材モデル「統合セキュリティ人材モデル」を策定　https://pr.fujitsu.com/jp/news/2018/10/24-1.html〔参照 2019-06-15〕
※ 245 ITSS+（プラス）・IT スキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報（https://www.ipa.go.jp/jinzai/itss/itssplus.html〔参照 2019-06-15〕）にあるセキュリティ領域のファイル（https://www.ipa.go.jp/files/000058688.xlsx〔参照 2019-06-15〕）より抜粋。
※ 246 https://www.jnsa.org/isepa/〔参照 2019-06-15〕
※ 247 https://www.jnsa.org/isepa/activities/jtag.html〔参照 2019-06-15〕
※ 248 https://www.jnsa.org/isepa/images/outputs/JTAG_guideline-β_190118.pdf〔参照 2019-06-15〕
※ 249 https://cyber-risk.or.jp/cric-csf/report/CRIC-CSF-2nd-Interim-Report.pdf〔参照 2019-06-15〕
※ 250 例えば株式会社日立製作所では、2017 年 5 月に発生した Wanna Cryptor 事案をきっかけとして、2017 年 10 月からグループ横断での情報セキュリティ専門部門として CISO 配下にセキュリティ統括専門組織を設置している（株式会社日立製作所：情報セキュリティ報告書 2018　https://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf〔参照 2019-06-15〕）。
※ 251 IPA：情報処理技術者試験統計資料 平成 30 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_h30a.pdf〔参照 2019-06-15〕
※ 252 IPA：プレス発表　平成 30 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/20180516.html〔参照 2019-06-15〕
IPA：プレス発表　平成 30 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/20181121.html〔参照 2019-06-15〕
※ 253 IPA：国家資格「情報処理安全確保支援士（登録セキスペ）」2019 年 4 月 1 日付登録人数は 1,052 人　https://www.ipa.go.jp/siensi/data/20190401newriss.html〔参照 2019-06-15〕
※ 254 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 2019-06-15〕
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 2019-06-15〕
※ 255 経済産業省：コネクテッド・インダストリーズ税制（IoT 税制）https://www.meti.go.jp/policy/it_policy/data-katsuyo/iot-zeisei/iot-zeisei.html〔参照 2019-06-15〕
コネクテッド・インダストリーズ税制では、税制優遇の条件の一つ「一定のサイバーセキュリティ対策が講じられている」ことを担保する役割を登録セキスペが担う。
※ 256 デジタル・トランスフォーメーション：企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること（経済産業省：デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）Ver. 1.0　https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf〔参照 2019-06-15〕）。
※ 257 一般社団法人日本サイバーセキュリティ・イノベーション委員会：セキュリティ人材不足の真実と今なすべき対策とは～今必要なのは「プラス（＋）・セキュリティ人材」だ～　https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf〔参照 2019-06-15〕
※ 258 IPA：プレス発表　「セキュリティ・キャンプ全国大会 2018」参加者を決定　https://www.ipa.go.jp/about/press/20180614.html〔参照 2019-06-15〕
※ 259 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　https://www.security-camp.or.jp/minicamp/index.html〔参照 2019-06-15〕
※ 260 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 2018　https://www.security-camp.or.jp/minicamp/kochi2018.html〔参照 2019-06-15〕
※ 261 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 2018　https://www.security-camp.or.jp/event/corecamp2018.html〔参照 2019-06-15〕
※ 262 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　https://www.security-camp.or.jp/event/award2019.html〔参照 2019-06-15〕
※ 263 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。
※ 264 NICT：SecHack365 開催概要 2019　https://sechack365.nict.go.jp/document/〔参照 2019-06-15〕
※ 265 NICT：SecHack365 成果発表会　https://sechack365.nict.go.jp/report/2018/report07.html〔参照 2019-06-15〕
※ 266 enPiT：2018 年度 成果報告　http://www.enpit.jp/files/enPiT_annualreport_uni_2018.pdf〔参照 2019-06-15〕
※ 267 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 2019-06-15〕
※ 268 enPiT-Pro Serurity：http://www.seccap.pro/〔参照 2019-06-15〕
※ 269 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。
※ 270 https://2018.seccon.jp/〔参照 2019-06-15〕
※ 271 NETIB-NEWS：新生 SECCON ～国際大会で第 1 位ー第 3 位を日本勢が独占!　https://www.data-max.co.jp/article/27496/1/〔参照 2019-06-15〕
※ 272 SECCON2018 運営事務局：SECCON Beginners とは　https://2018.seccon.jp/beginners/about-seccon-beginners.html〔参照 2019-06-15〕
※ 273 http://girls.seccon.jp/〔参照 2019-06-15〕
※ 274 JNSA：インターンシップ募集　https://www.jnsa.org/internship/2018/index.html〔参照 2019-06-15〕
※ 275 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 2018 年版を発表　https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181219-01.html〔参照 2019-06-25〕
※ 276 https://juas.or.jp/cms/media/2017/02/it19_ppt.pdf〔参照 2019-06-25〕
※ 277 https://www.secure-sketch.com/hubfs/e-book/NRISecure_Insight2018_Report.pdf〔参照 2019-06-25〕
※ 278 図 2-4-1 の「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」の合計。
※ 279 https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf〔参照 2019-06-25〕
※ 280 https://www.j-cic.com/pdf/report/CyberRiskEstimationModel-20180919.xls〔参照 2019-06-25〕
※ 281 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_05_00.pdf〔参照 2019-06-25〕
※ 282 https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/pdf/2_016_04_00.pdf〔参照 2019-06-25〕
※ 283 https://www.ipa.go.jp/security/economics/CSM-Guideline-Practice.html〔参照 2019-06-25〕
※ 284 https://www.iso.org/the-iso-survey.html〔参照 2019-06-25〕
※ 285 平成 30 年第 196 回通常国会において、「不正競争防止法等の一部を改正する法律」（法律第 33 号）が可決成立し、2019 年 7 月 1 日を施行日として工業標準化法が一部改正され、“産業標準化法”に変わり、日本工業規格（JIS）が日本産業規格（JIS）に変わることとなった。
※ 286 JIPDEC：プライバシーマーク付与事業者情報　https://privacymark.jp/certification_info/jdi6lq00000017af-att/pmark_data_20190331.pdf〔参照 2019-06-25〕
※ 287 https://privacymark.jp/system/reference/pdf/H29JikoHoukoku_180831.pdf〔参照 2019-06-25〕
※ 288 https://privacymark.jp/system/reference/pdf/H29JikoHoukoku_shiryo_180928.pdf〔参照 2019-06-25〕
※ 289 http://www.jaycee.or.jp/2018/org/summerconference/wp-content/uploads/2018/07/anzenhoshou_act_saiba1.pdf〔参照 2019-06-25〕
なお、「中小企業に対するサイバーセキュテリィ意識調査分析レポート」は 11 ページ以降に掲載されている。
※ 290 JCI-Japan：これであなたの会社も大丈夫! JC 版サイバーセキュリティ問題解決プログラム　http://www.jaycee.or.jp/2018/org/summerconference/?page_id=867#a1〔参照 2019-06-25〕
※ 291 https://www.ipa.go.jp/security/security-action/〔参照 2019-06-25〕
※ 292 https://www.ipa.go.jp/files/000072383.pdf〔参照 2019-06-25〕
※ 293 一般社団法人サービスデザイン推進協議会：IT 導入補助金 https://www.it-hojo.jp/〔参照 2019-06-25〕
※ 294 公益財団法人東京都中小企業振興公社：サイバーセキュリティ対策促進助成金の申請案内　http://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html〔参照 2019-06-25〕

※ 295 https://www.ipa.go.jp/files/000055520.pdf〔参照 2019-06-25〕
※ 296 神奈川県商工会議所連合会：神奈川県警察「SEAGULL（シーガル）」が運用開始しました　http://www.kanagawa-cci.or.jp/kenren/2435〔参照 2019-06-25〕
※ 297 ISEN：平成 29 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　https://school-security.jp/pdf/2017.pdf〔参照 2019-06-25〕
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　https://school-security.jp/pdf/2016.pdf〔参照 2019-06-25〕
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　https://school-security.jp/pdf/2015.pdf〔参照 2019-06-25〕
※ 298 2017 年度と 2016 年度のセキュリティインシデント数は「平成 29 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 2-4-11 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－」及び「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－」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。
※ 299 公立大学法人横浜市立大学：電子メールの不正転送被害による個人情報の漏えいについて　https://www.yokohama-cu.ac.jp/news/2018/pr/dr3e64000000d0fh-att/180606_emailpressrelease.pdf〔参照 2019-06-25〕
※ 300 学校法人北海道科学大学：個人情報の紛失について　https://jc.hus.ac.jp/news/2018/06/20180622463.html〔参照 2019-06-25〕
※ 301 国立大学法人弘前大学：フィッシングメールによる個人情報の漏えいについて　https://www.hirosaki-u.ac.jp/wordpress2014/wp-content/uploads/2018/06/300627_siryou.pdf〔参照 2019-03-08〕
※ 302 学校法人明治大学：不正アクセスによる SPAM メールの送信及び個人情報漏えいについて　https://www.meiji.ac.jp/koho/news/2018/6t5h7p00000t4bw0-att/20181024.pdf〔参照 2019-06-25〕
※ 303 国立大学法人兵庫教育大学：電子メールの転送先での不正ログインによる個人情報漏えいについて　https://www.hyogo-u.ac.jp/info/015726.php〔参照 2019-06-25〕
※ 304 国立大学法人奈良先端科学技術大学院大学：情報システムの不適切運用による個人情報の漏えいについて（お詫び）　http://www.naist.jp/news/2019/01/005543.html〔参照 2019-06-25〕
※ 305 学校法人東京理科大：サイバー攻撃による個人情報等の流出について　https://www.tus.ac.jp/today/archive/201902190900.html〔参照 2019-06-25〕
※ 306 SankeiBiz：文科省が偽メール注意喚起、6 大学で情報流出 1 万件超　https://www.sankeibiz.jp/compliance/news/180629/cpb1806290746001-n1.htm〔参照 2019-06-25〕
※ 307 神戸新聞 NEXT：受験生の合否など 2 千人の個人情報、男子学生 4 人が持ち去る　明石高専　https://www.kobe-np.co.jp/news/sougou/201807/0011421577.shtml〔参照 2019-06-25〕
※ 308 取手市：取手市立取手小学校メールアカウントへの不正アクセスおよびスパムメールの送信について　https://www.city.toride.ibaraki.jp/gakumukyushoku/kurashi/kosodate/gakko/torisho_mail.html〔参照 2019-06-25〕
※ 309 NII：大学間連携に基づく情報セキュリティ体制の基盤構築　https://www.nii.ac.jp/service/upload/7_setsumeikai2017_security_20171114.pdf〔参照 2019-06-25〕
※ 310 日本シーサート協議会ホームページ（https://www.nca.gr.jp/〔参照 2019-06-25〕）の「What's New」から IPA が抽出。
※ 311 総務省：平成 30 年度（平成 31 年 3 月 29 日発表）　http://www.soumu.go.jp/denshijiti/060213_02.html〔参照 2019-06-25〕
※ 312 https://cyder.nict.go.jp〔参照 2019-06-25〕
※ 313 IPA：「2018 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/fy30/reports/ishiki/index.html〔参照 2019-06-25〕
※ 314 ITmedia エンタープライズ：広告詐欺の不正コード混入か、Google Play の人気アプリ削除　http://www.itmedia.co.jp/enterprise/articles/1812/05/news071.html〔参照 2019-06-25〕
ITmedia エンタープライズ：フィットネス装い金銭詐取　Apple App Store に不正アプリ　http://www.itmedia.co.jp/enterprise/articles/1812/04/news069.html〔参照 2019-06-25〕
※ 315 警視庁：遺失物取扱状況（平成 30 年中）　http://www.keishicho.metro.tokyo.jp/about_mpd/jokyo_tokei/kakushu/kaikei.html〔参照 2019-06-25〕
※ 316 長崎新聞：女性スマホに遠隔操作アプリ 容疑で男性書類送検 長崎県警　https://this.kiji.is/428376316409136225〔参照 2019-06-25〕
※ 317 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181226-01.html〔参照 2019-06-25〕
※ 318 内閣府：青少年有害環境対策（インターネット利用環境整備・非行対策・健全育成）について　https://www8.cao.go.jp/youth/kankyou/index.html〔参照 2019-06-25〕
※ 319 内閣府：平成 31 年「春のあんしんネット・新学期一斉行動」https://www8.cao.go.jp/youth/kankyou/internet_use/2019/index.html〔参照 2019-06-25〕
※ 320 https://www8.cao.go.jp/youth/kankyou/internet_use/h29/leaflet.html〔参照 2019-06-25〕
※ 321 https://www.fmmc.or.jp/e-netcaravan/〔参照 2019-06-25〕
※ 322 個人情報保護委員会：法令・ガイドライン等　https://www.ppc.go.jp/personalinfo/legal/〔参照 2019-06-25〕
※ 323 個人情報保護委員会：小学生を対象とした「個人情報の大切さ」に係る標語の募集について　https://www.ppc.go.jp/news/press/2018/20181109/〔参照 2019-06-25〕
※ 324 個人情報保護委員会：小学生を対象とした「個人情報の大切さ」に係る出前授業の実施について　https://www.ppc.go.jp/files/pdf/181226_houdou.pdf〔参照 2019-06-25〕
※ 325 https://www.ipa.go.jp/security/anshin/〔参照 2019-06-25〕
※ 326 https://www.ipa.go.jp/security/anshin/mgdayoriindex.html〔参照 2019-06-25〕
※ 327 https://www.ipa.go.jp/security/event/hyogo/〔参照 2019-06-25〕
※ 328 https://www.ipa.go.jp/security/keihatsu/net-anzen.html〔参照 2019-06-25〕
※ 329 https://www.nisc.go.jp/security-site/month/index.html〔参照 2019-06-25〕
※ 330 https://www.nisc.go.jp/security-site/month/event/index.html〔参照 2019-06-25〕
※ 331 https://www.nisc.go.jp/security-site/files/handbook-all.pdf〔参照 2019-06-25〕
※ 332 https://www.nisc.go.jp/security-site/handbook/index.html〔参照 2019-06-25〕
※ 333 公衆無線 LAN セキュリティ分科会：公衆無線 LAN セキュリティ分科会報告書　http://www.soumu.go.jp/main_content/000539751.pdf〔参照 2019-06-25〕
※ 334 総務省：公衆無線 LAN のセキュリティ対策に係るオンライン講座の開講　http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00013.html〔参照 2019-06-25〕
※ 335 https://www.ipa.go.jp/security/keihatsu/videos/index.html〔参照 2019-06-25〕
※ 336 https://www.keishicho.metro.tokyo.jp/about_mpd/joho/movie/cyber/cs_anime/index.html〔参照 2019-06-25〕
※ 337 IPA：情報セキュリティ啓発映像　ペアレンタルコントロール　https://www.ipa.go.jp/security/keihatsu/videos/20190304.html〔参照 2019-06-25〕
※ 338 IPA：情報セキュリティ啓発映像　不正ログイン対策　https://www.ipa.go.jp/security/keihatsu/videos/20180403-1.html〔参照 2019-06-25〕
※ 339 IPA：情報セキュリティ啓発映像　インターネット接続機器のセキュリティ対策　https://www.ipa.go.jp/security/keihatsu/videos/20180403-2.html〔参照 2019-06-25〕
※ 340 一般財団法人草の根サイバーセキュリティ運動全国連絡会：一般財団法人草の根サイバーセキュリティ運動全国連絡会（Grafsec-J）のご紹介　https://www.nisc.go.jp/security-site/spc/soukai/dai03/pdf/03shiryou04.pdf〔参照 2019-06-25〕
※ 341 https://www.fmmc.or.jp/hyogo/〔参照 2019-06-25〕
※ 342 ネット社会の健全な発展に向けた連絡協議会：秋の一斉行動キャンペーンポスター　https://www.fmmc.or.jp/Portals/0/20181017_netsyakai2.png〔参照 2019-06-25〕
※ 343 ネット社会の健全な発展に向けた連絡協議会：平成 30 年「秋の集中キャンペーン期間」等について　https://www.fmmc.or.jp/Portals/0/images/net-shakai/news/2018/autumn%20torikumi.pdf〔参照 2019-06-25〕
※ 344 SPREAD：SPREAD 情報セキュリティサポーターになるには　https://www.spread.or.jp/kentei/〔参照 2019-06-25〕
※ 345 https://www.jpcert.or.jp/pr/2018/stop-password2018.html〔参照 2019-06-25〕
※ 346 https://www.jnsa.org/active/news10/〔参照 2019-06-25〕
※ 347 https://www.jnsa.org/seminar/2018/0612/data/A1-2incident.pdf〔参照 2019-06-25〕
※ 348 https://www.jnsa.org/novel_contest/〔参照 2019-06-25〕
※ 349 JNSA：サイバーセキュリティ小説コンテスト 最終選考結果を発表しました!　https://www.jnsa.org/press/2018/181220.pdf〔参照 2019-

06-25〕
※ 350 JISPA：安心協ニュースを発行しました　ー平成 31 年春号ー https://www.good-net.jp/information/news/228〔参照 2019-06-25〕
※ 351 総務省：青少年がインターネットを安全に安心して活用するためのリテラシー指標　http://www.cec.or.jp/cecre/soumu/PDF/ILAS.pdf〔参照 2019-06-25〕
※ 352 総務省：スマートフォン時代に対応した青少年のインターネット利用に関する連絡会（スマホ連絡会（近畿））　http://www.soumu.go.jp/soutsu/kinki/sumaho-kinki/index.html〔参照 2019-06-25〕
※ 353 キヤノン IT ソリューションズ株式会社：マルウェア情報局 https://eset-info.canon-its.jp/malware_info/〔参照 2019-06-25〕
※ 354 日本アイ・ビー・エム株式会社：セキュリティー・インテリジェンス　https://www.ibm.com/blogs/security/jp-ja/category/security-intelligence/〔参照 2019-06-25〕
※ 355 株式会社カスペルスキー：カスペルスキー公式ブログ　https://blog.kaspersky.co.jp/〔参照 2019-06-25〕
※ 356 株式会社シマンテック：Symantec Connect　https://www.symantec.com/connect/ja/symantec-blogs/sr〔参照 2019-06-25〕
※ 357 トレンドマイクロ社：トレンドマイクロセキュリティブログ　https://blog.trendmicro.co.jp/〔参照 2019-06-25〕
※ 358 マカフィー株式会社：マカフィー株式会社公式ブログ　https://blogs.mcafee.jp/〔参照 2019-06-25〕
※ 359 経済産業省：今後の基準認証の在り方ールール形成を通じたグローバル市場の獲得に向けてー答申　https://www.meti.go.jp/shingikai/sankoshin/sangyo_gijutsu/kijun_ninsho/pdf/20171011001_1.pdf〔参照 2019-06-25〕
※ 360 https://www.kantei.go.jp/jp/singi/titeki2/2010keikaku.pdf〔参照 2019-06-25〕
※ 361 https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku2018.pdf〔参照 2019-06-25〕
※ 362 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。
※ 363 ISO：ISO/IEC JTC 1　https://www.iso.org/committee/45020.html〔参照 2019-06-25〕
※ 364 JISC：JISC について　http://www.jisc.go.jp/jisc/index.html〔参照 2019-06-25〕
※ 365 ITU：SG17: Security　https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔参照 2019-06-25〕
※ 366 IETF：The IETF Security Area　https://trac.ietf.org/trac/sec/wiki〔参照 2019-06-25〕
※ 367 TCG：Trusted Computing Group へようこそ　https://trustedcomputinggroup.org/work-groups/regional-forums/japan/〔参照 2019-06-25〕
※ 368 JISC：ISO 規格の制定手順　https://www.jisc.go.jp/international/iso-prcs.html〔参照 2019-06-25〕
※ 369 一般財団法人日本規格協会：ISO/IEC 専門業務用指針，第 1 部　統合版 ISO 補足指針 -ISO 専用手順　https://www.jsa.or.jp/datas/media/10000/md_3819.pdf〔参照 2019-06-25〕
※ 370 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サイズが従来の 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、SPECK がソフトウェアでの利用を想定している。なお、RFID 等の標準化を担当している ISO/IEC JTC1/SC31 においては、SIMON や SPECK を利用する RFID の規格が発行されている。
※ 371 ISO/IEC：ISO/IEC JTC 1/SC 27 STATEMENT ON OCB2.0 -- -- Major weakness found in a standardised cipher scheme (ISO/IEC 19772:2009-02, 1st ed)　https://www.din.de/blob/321470/da3d9bce7116deb510f6aded2ed0b4df/20190107-press-release-19772-2009-1sted-ocb2-0-data.pdf〔参照 2019-06-25〕
※ 372 ISO/IEC15408 及び ISO/IEC18045 に基づく評価は CC（Common Criteria）評価とも呼ばれる。
※ 373 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委託事業「高効率・高速処理を可能とする AI チップ・次世代コンピューティングの技術開発／高度な IoT 社会を実現する横断的技術開発／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」を指す。
※ 374 IoT 推進コンソーシアム：IoT セキュリティガイドライン Ver1.0 http://www.soumu.go.jp/main_content/000428393.pdf〔参照 2019-06-25〕
※ 375 経済産業省：サプライチェーン・サイバーセキュリティ等に関する海外の動き　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/004_03_04.pdf〔参照 2019-06-25〕
※ 376 ISO：ISO/TC 307　https://www.iso.org/committee/6266604.html〔参照 2019-06-25〕
※ 377 http://www.iotac.jp/wp-content/uploads/2016/01/03-IoT%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3ver1.0%E5%88%A5%E7%B4%99%EF%BC%91.pdf〔参照 2019-06-25〕
※ 378 https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf〔参照 2019-06-25〕
※ 379 https://trustedcomputinggroup.org/〔参照 2019-06-25〕
※ 380 TCG：TPM Library Specification　https://trustedcomputinggroup.org/tpm-library-specification/〔参照 2019-06-25〕
※ 381 TCG：TCG 日本支部勉強会　https://trustedcomputinggroup.org/work-groups/regional-forums/japan/studymeeting/〔参照 2019-06-25〕
※ 382 TCG：TCG 日本支部ワークショップ　https://trustedcomputinggroup.org/work-groups/regional-forums/japan/jrfworkshop/〔参照 2019-06-25〕
※ 383 TCG：Embedded Systems　https://trustedcomputinggroup.org/work-groups/embedded-systems/〔参照 2019-06-25〕
※ 384 TCG：TCG TPM 2.0 Automotive Thin Profile　https://trustedcomputinggroup.org/tcg-tpm-2-0-library-profile-automotive-thin/〔参照 2019-06-25〕
※ 385 TCG：Protection Profile Automotive-Thin Specific TPM https://trustedcomputinggroup.org/resource/protection-profile-automotive-thin-specific-tpm-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/〔参照 2019-06-25〕
※ 386 Microsoft Corporation：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 2019-06-25〕
※ 387 TCG：Device Identifier Composition Engine (DICE) Architectures　https://trustedcomputinggroup.org/work-groups/dice-architectures/〔参照 2019-06-25〕
※ 388 TCG：TCG Software Stack (TSS) Specification　https://trustedcomputinggroup.org/tcg-software-stack-tss-specification/〔参照 2019-06-25〕
※ 389 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 2019-06-25〕
※ 390 TCG：NIST SP800-193 Platform Firmware Resiliency Guidelines　https://csrc.nist.gov/publications/detail/sp/800-193/final〔参照 2019-06-25〕
※ 391 https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf〔参照 2019-06-25〕
※ 392 https://www.ipa.go.jp/security/jisec/index.html〔参照 2019-06-25〕
※ 393 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。　https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔参照 2019-06-25〕
※ 394 2019 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、シンガポール、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、マレーシア、フランス（以上の国は認証制度を自国で運営）、イスラエル、インドネシア、エチオピア、オーストリア、カタール、ギリシャ、チェコ、デンマーク、パキスタン、ハンガリー、フィンランド、ポーランド（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 30 ヵ国。
※ 395 CCRA：Collaborative Protection Profiles (cPP) and Supporting Documents (SD)　https://www.commoncriteriaportal.org/pps/?cpp=1〔参照 2019-06-25〕
※ 396 IPA：セキュリティ機能と保証レベル　https://www.ipa.go.jp/security/jisec/forusers/abouteal.html〔参照 2019-06-25〕
※ 397 IEEE（Institute of Electrical and Electronics Engineers）：電気・電子技術に関する国際的な学会。
※ 398 CCRA：Vision statement for the future direction of the application of the CC and the CCRA　https://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf〔参照 2019-06-25〕
CCRA：CC 及び CCRA の適用についての今後の方向性に関するビジョンステートメント　https://www.ipa.go.jp/security/jisec/ccra/documents/vision_statement_J.pdf〔参照 2019-06-25〕
※ 399 Collaborative Protection Profile と呼ばれ、CCRA 加盟国が政府調達において用いることを想定して策定された PP 群。
CCRA：Collaborative Protection Profiles (cPP) and Supporting Documents (SD)　https://www.commoncriteriaportal.org/pps/?cpp=1〔参照 2019-06-25〕

※ 400 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。
※ 401 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 2019-06-25〕
※ 402 Bundesamt für Sicherheit in der Informationstechnik：BSI-CC-PP-0035-2007 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/Archiv/PP_0035.html〔参照 2019-06-25〕
※ 403 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 2019-06-25〕
※ 404 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。
※ 405 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。
※ 406 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。
※ 407 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 2019-06-25〕
※ 408 IPA：CC サポート文書 https://www.ipa.go.jp/security/jisec/hardware/cc_supporting_doc.html〔参照 2019-06-25〕
※ 409 IPA：形式手法は何に使えるか? https://www.ipa.go.jp/security/event/2013/ist-expo/documents/preso18.pdf〔参照2019-06-25〕
※ 410 IPA：形式手法を用いたセキュリティ検証 https://www.ipa.go.jp/files/000039110.pdf〔参照 2019-06-25〕
※ 411 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。
※ 412 NIST：FIPS 140-3 Security Requirements for Cryptographic Modules https://csrc.nist.gov/publications/detail/fips/140/3/final〔参照 2019-06-25〕
※ 413 https://www.iso.org/standard/52906.html〔参照 2019-06-25〕
※ 414 https://www.iso.org/standard/72515.html〔参照 2019-06-25〕
※ 415 https://www.ipa.go.jp/security/jcmvp/topics.html〔参照2019-06-25〕
※ 416 NIST：FIPS 140-3 Development https://csrc.nist.gov/projects/fips-140-3-development〔参照 2019-06-25〕
※ 417 https://www.nisc.go.jp/active/general/pdf/guide30.pdf〔参照 2019-06-25〕
※ 418 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 1.5 版 https://www.ipa.go.jp/security/jisec/application/documents/guidelineforHCD-PP_1.5.pdf〔参照 2019-06-25〕
※ 419 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔参照 2019-06-25〕
※ 420 IPA/JISEC：認証製品リスト https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔参照 2019-06-25〕
※ 421 IPA/JISEC：TOSHIBA e-STUDIO2010AC/2510AC ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPS ハードディスクキット（GE-1230）付モデル SYS V1.0 https://www.ipa.go.jp/security/jisec/certified_products/c0629/c0629_it8689.html〔参照 2019-06-25〕
IPA/JISEC：TOSHIBA e-STUDIO5518A/6518A/7518A/8518A ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPS ハードディスクキット（GE-1230）付モデル SYS V1.0 https://www.ipa.go.jp/security/jisec/certified_products/c0630/c0630_it8691.html〔参照 2019-06-25〕
IPA/JISEC：TOSHIBA e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPS ハードディスクキット（GE-1230）付モデル SYS V1.0 https://www.ipa.go.jp/security/jisec/certified_products/c0631/c0631_it8692.html〔参照 2019-06-25〕
IPA/JISEC：TOSHIBA e-STUDIO5516AC/6516AC/7516AC ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPS ハードディスクキット（GE-1230）付モデル SYS V1.0 https://www.ipa.go.jp/security/jisec/certified_products/c0632/c0632_it8693.html〔参照 2019-06-25〕
IPA/JISEC：TOSHIBA e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPS ハードディスクキット（GE-1230）付モデル SYS V1.0 https://www.ipa.go.jp/security/jisec/certified_products/c0633/c0633_it8690.html〔参照 2019-06-25〕
※ 422 IPA/JCMVP：暗号モジュール認証製品リスト F0022 https://www.ipa.go.jp/security/jcmvp/val.html#F0022〔参照 2019-06-25〕
※ 423 NIST：NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf〔参照 2019-06-25〕
※ 424 https://standards.ieee.org/standard/802_1AE-2006.html〔参照 2019-06-25〕
※ 425 https://standards.ieee.org/standard/802_1AEbw-2013.html〔参照 2019-06-25〕
※ 426 CRYPTREC：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） https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf〔参照 2019-06-25〕
※ 427 NIST：Draft NIST Special Publication 800-131A Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths https://csrc.nist.gov/CSRC/media/Publications/sp/800-131a/rev-2/draft/documents/sp800-131Ar2-draft.pdf〔参照 2019-06-25〕
※ 428 Federal Office for Information Security：BSI TR-02102-1: "Cryptographic Mechanisms: Recommendations and Key Lengths" Version: 2018-02 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf〔参照 2019-06-25〕
※ 429 Agence nationale de la sécurité des systèmes d'information: Référentiel Général de Sécurité version 2.0 Annexe B1 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf〔参照2019-06-25〕
※ 430 https://www.jnsa.org/result/2019/surv_mrk/data/2018_mktreport.pdf〔参照 2019-06-25〕
※ 431 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 https://www.meti.go.jp/press/2016/03/20170320001/20170320001.html〔2019-06-25〕
※ 432 経済産業省：限定提供データに関する指針の概要 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pdoutline.pdf〔2019-06-25〕
経済産業省：限定提供データに関する指針 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf〔2019-06-25〕
※ 433 経済産業省：産業データ共有事業について https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/dai5/dcwg_siryou3-1.pdf〔2019-06-25〕
※ 434 IPA：「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」報告書について https://www.ipa.go.jp/security/fy30/reports/ts_research/index.html〔2019-06-25〕
※ 435 経済産業省：AI・データの利用に関する契約ガイドライン https://www.meti.go.jp/press/2018/06/20180615001/20180615001-1.pdf〔2019-06-25〕
※ 436 一般財団法人日本データ通信協会：トラストサービス推進フォーラム https://www.dekyo.or.jp/tsf/〔2019-06-25〕
※ 437 一般財団法人データ流通推進協議会：データ取引市場運営事業者認定基準の説明 https://data-trading.org/wp-content/uploads/2019/01/dta_20180928_02.pdf〔2019-06-25〕
※ 438 Akiko Inoue and Kazuhiko Minematsu：Cryptanalysis of OCB2 https://eprint.iacr.org/2018/1040.pdf〔参照 2019-06-25〕
※ 439 International Association for Cryptologic Research（IACR）：https://www.iacr.org/〔参照 2019-06-25〕
※ 440 Cryptology ePrint Archive（ePrint）：https://eprint.iacr.org/〔参照 2019-06-25〕
※ 441 Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz：“OCB: a block-cipher mode of operation for efficient authenticated encryption.”, In CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001., pp. 196-205, 2001.
※ 442 Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Advances in Cryptology - ASIACRYPT2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings, pp. 16-31, 2004.
※ 443 Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers, pp.

306-327, 2011.
※ 444 CAESAR：CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness https://competitions.cr.yp.to/caesar.html〔参照 2019-06-25〕
※ 445 Internet Research Task Force(IRTF):The OCB Authenticated-Encryption Algorithm https://tools.ietf.org/html/rfc7253〔参照2019-06-25〕
※ 446 Bertram Poettering：Breaking the confidentiality of OCB2 https://eprint.iacr.org/2018/1087.pdf〔参照 2019-06-25〕
Tetsu Iwata：Plaintext Recovery Attack of OCB2 https://eprint.iacr.org/2018/1090.pdf〔参照 2019-06-25〕
※ 447 井上明子，峯松一彦，“OCB2 の安全性解析”，2019 年暗号と情報セキュリティシンポジウム(SCIS2019)，1B1-2, 2019.
岩田 哲，“OCB2 に対する平文回復攻撃”，2019 年暗号と情報セキュリティシンポジウム(SCIS2019)，1B1-3, 2019.
※ 448 NIST：Round 1 Submissions https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions〔参照 2019-06-25〕
※ 449 https://csrc.nist.gov/Presentations/2018/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti〔参照 2019-06-25〕
※ 450 NIST：Round 2 Submissions https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions〔参照 2019-06-25〕

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、スマートフォン、IT サプライチェーン、AI のセキュリティについて解説する。

「情報セキュリティ白書 2018」に続いて、制御システム、IoT、スマートフォンについては、より巧妙化、多様化する攻撃の実態を報告する。

また、脅威の高まりとともに注目されている IT サプライチェーンのセキュリティと、技術の進展により実生活でも利用されるようになった AI のトラスト（信頼）とセキュリティについて新たに取り上げる。

3.1 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、制御システム固有のプロトコル、事業者ごとに異なる仕様で構築・運用されることが多く、外部から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、また、10 ～ 20 年に及ぶシステムライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今なお多数稼働していることから、制御システムに対するサイバー脅威が高まっている。実際にここ数年は、サイバー攻撃による製鉄所の溶鉱炉の損壊（2014 年：ドイツ）※1、大規模停電（2015 年、2016 年：ウクライナ）※2、安全計装システムのハッキングによる緊急停止（2017 年：中東）※3 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主な取り組みについて述べる。

3.1.1 インシデントの発生状況と動向

2018 年は、ここ数年続いていた、制御システムにおける重大なサイバーインシデントは特に報告されなかった。国内においても、JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）に報告された制御システムのインシデント件数は 7 件で、2017 年の 77 件から大幅に減少している※4。

しかし、海外における制御システムユーザ等へのアンケート調査によれば、制御システムへの侵入や運用障害が発生したという回答は一定数以上あった。

例えば、中東の石油・ガス事業者のセキュリティ責任者約 200 人を対象とした調査では、75% が過去 1 年間に機密情報の窃取または制御システムの運用障害につながるインシデントが少なくとも 1 回発生したと回答している※5。また、世界各地の製造、エネルギー、運輸、物流分野等の制御システムのセキュリティ責任者 320 人を対象とした調査では、31% が過去 1 年間に制御システムのインシデント（環境被害、機器損壊を含む）が 1 回以上発生したと回答している※6。

従って、公にはなっていないが、制御システムの運用や機器に実害をもたらしたインシデントは、2018 年も一定程度発生したと推察される。一方で、公になったインシデントには二つの傾向が見られた。一つは、特に制御システムを狙ったものではないウイルス※7 への感染による運用障害、もう一つはサプライチェーン上のサイバー脅威に起因する運用障害である。

(1) ウイルスへの感染

制御システムのウイルスへの感染は毎年報告されている※8。2018 年は感染に加え、運用やサービスに影響を及ぼしたインシデントや、その恐れがあった「ニアミス」も複数報告されている。

例えば 7 月には、ウクライナの塩素プラントのプロセス制御システム及び緊急事態を検知するシステムが、ネットワーク機器を標的とするウイルス「VPNFilter※9」に感染した。当該プラントはウクライナ全土の浄水場及び下水処理場に塩素を供給しており、同国の情報機関は、被害を阻止したものの、プロセスの停止や事故につながっ

た可能性もあったと話した※10（VPNFilterについては「3.2.1(3)VPNFilter」参照）。

11月には、モスクワのロープウェーのシステムサーバがランサムウェアに感染し、2日間運行が停止した。感染発覚後すぐに35台すべてのゴンドラを停止させており、怪我人等は出なかった※11。

12月には、米国西部の新聞社の印刷プラットフォームがウイルス（関係者によればランサムウェアとも）に感染し、プラットフォームを共用する複数紙の印刷に影響を及ぼし、配達が大幅に遅延した。東部の大手紙も西海岸の購読者用に当該プラットフォームを利用していたため、影響は東部の新聞社にも及んだ※12。

なお、2018年2月には欧州の水道事業者の制御システムが仮想通貨（暗号資産）のマイニングウイルスに感染した事例が※13、10月には米国ノースカロライナ州の水道当局のシステムがランサムウェアに感染した事例が報告されている※14。

これらの事例では運用やサービスに影響はなかったとされている。しかし、ランサムウェアやデータを消去する破壊型ウイルス、感染機器の処理能力を低下させるマイニングウイルス等は、ひと度感染すれば、制御システムの可用性を阻害する可能性がある。特に、病院へのランサムウェア攻撃と同様に、制御システムの可用性を人質に身代金を取ろうとするランサムウェア攻撃も、ひと度成功事例が報道されれば一気に増加する危険性がある。

一般的に、制御システム内部では、ウイルスの感染拡大防止といったセキュリティ観点での機器間の通信制限はなされていない場合が多く、セキュリティソフトを始めとする対策を導入可能な機器も限られている。そのため、ウイルスが内部に入り込んだ場合、感染が拡大しやすい制御システムも多いと推測される。制御システムの保有者は、予期せずに入り込むウイルスに備え、情報ネットワークを含む外部ネットワークとの境界機器、及び制御システム内部にあってインターネットを含む外部ネットワークに接続している、あるいは接続する可能性のある機器のウイルス対策、外部から持ち込む情報端末や媒体のウイルス対策を徹底することが重要である。

(2) サプライチェーンに起因するサイバー脅威

機器調達・運用等のサプライヤーを介した標的型攻撃等、サプライチェーン上の脆弱性に起因したインシデントは、情報漏えい事件等において注目を集めてきたが、2018年は制御システムでもサプライチェーンに関連した運用障害やウイルス感染が複数報告されている。

例えば、7月には、Wall Street Journal紙（以下、WSJ）が、外国のハッカーが米国の複数の電力事業者の制御システムに侵入し、停電を引き起こすことも可能な状態にあったことを、国土安全保障省（Department of Homeland Security：DHS）が重要インフラ事業者に警告したと報じた。DHSによれば、ハッカーらはまずサプライヤーのネットワークに標的型攻撃によって侵入し、サプライヤーがソフトウェアのアップデートや機器の診断に使用する特別なアクセス方法を悪用して事業者のネットワークに侵入したという※15。WSJは2019年1月にも、同紙の調査や関係者へのインタビューから、サプライヤーを踏み台としたソーシャルエンジニアリング攻撃の経緯を再現した記事を公開している※16。

8月には、日本国内の工場で、産業機器（鉄板に加工を施す機器）のウイルス感染が発覚した。同工場に設置した侵入検知システム（Intrusion Detection System：IDS）が不審な通信を検知したため調査したところ、2年前に導入した当該産業機器が開発段階で感染し、サプライヤーからそのまま納品された可能性が高いことが判明した。ウイルスはインターネットバンキングの情報窃取を目的としたもので、被害はなかった。しかし、ランサムウェアや破壊型ウイルスであれば、工場システムに障害が発生していた可能性もあった※17。

そして、その可能性はすぐに現実となった。同じく8月に、台湾の半導体大手の工場システムが、ランサムウェア「Wanna Cryptor」（別名WannaCry）の亜種に感染し、工場の操業が停止した。サプライヤーが新しいツールのインストール作業用に持ち込んだソフトウェアがウイルスに感染していたことが原因となり、修正プログラムを適用していなかったWindows 7システムを中心に感染が広がった結果であった。当該企業はApple Inc.（以下、Apple社）のチップサプライヤーであり、当時はiPhoneの出荷への影響も懸念された※18。

8月には、フランスの大手制御システムベンダが製品に同梱して出荷したUSBメモリがウイルスに感染していることが判明した。調査の結果、サプライヤーの工場での製造過程で感染していた。ベンダは、問題のUSBメモリはインストールに必須ではないため、使用せず破棄するよう求めるとともに、当該ウイルスは主要なウイルス対策プログラムで検知可能との声明を出した※19。しかしながら、ウイルス対策プログラムの種類やパターンファイルの更新状況によっては、検知できない可能性がある。

これらの事例で特徴的なのはサプライヤーがウイルスに感染した機器や媒体を制御システム環境に持ち込む

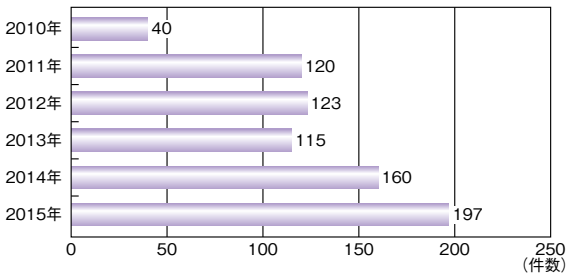
ケースだが、サプライヤーを踏み台にしたソーシャルエンジニアリング攻撃／標的型攻撃も顕在化しており、サプライヤーとの信頼関係が盲点となったり、悪用されたりしている。制御システムの保有者は、サプライヤーに対して持ち込む情報端末や媒体のウイルス対策を今一度徹底させるとともに、従業員に対するソーシャルエンジニアリング攻撃／標的型攻撃対策教育を繰り返し実施することが重要である。

3.1.2 脆弱性と脅威の動向

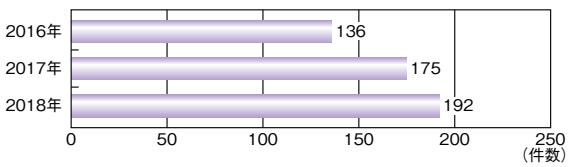
本項では、2018 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2018 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である DHS の NCCIC（National Cybersecurity and Communications Integration Center）が 2018 年に公開したアドバイザリは 192 件で、図 3-1-1 及び図 3-1-2 に示す公開件数から分かるように、増加傾向が続いている（2016 年から NCCIC における脆弱性情報の公開件数のカウント方法が見直されたため、同じカウント方法で比較できるように図を分けている）。



■図 3-1-1　NCCIC が公開した制御システムの脆弱性の件数（2010 ～ 2015 年）
（出典）NCCIC 公開情報[※20] を基に IPA が作成



■図 3-1-2　NCCIC が公開した制御システムの脆弱性の件数（2016 ～ 2018 年）
（出典）NCCIC 公開情報[※21] を基に IPA が作成

2018 年に公表された脆弱性の内容には、特に顕著な傾向は見られなかった。しかし、制御システムの脆弱性対策という観点では、対策の要否や優先度の判断の指標となる深刻度の評価に関する課題と、対策に関する課題が改めて浮き彫りになった。

(a) 制御システムの脆弱性の深刻度の評価に関する課題

公表される脆弱性の件数は多いが、実際にはすべての脆弱性に対応する必要はなく、リスクが高い脆弱性に迅速に対応することが重要である。対策の要否や優先度の判断には、発見された脆弱性がどの程度危険かを示す「深刻度」が重要な指標となる。深刻度の評価については、情報システムの脆弱性に対するオープンで汎用的な評価手法 CVSS（Common Vulnerability Scoring System）[※22] が、制御システムの脆弱性の評価にも利用されている（CVSS については「1.3.1 JVN iPedia の登録情報から見る脆弱性の傾向」参照）。しかし、機密性・完全性を重視する情報システムと、可用性を重視する制御システムの違いを考えた場合、制御システムの脆弱性に対しては適切な評価が行われておらず、対策の要否や優先度の判断に使えないといった指摘や[※23]、そもそも CVSS 自体が制御システムの脆弱性の評価には適していないとして、新たな評価手法を提案する動きも出ている[※24]。

(b) 制御システムにおける脆弱性対策に関する課題

通常、脆弱性への対策は、修正プログラムの適用や対策版へのアップデートが提示される。しかし、可用性が重視される制御システムでは、修正プログラムやアップデートの適用のためだけにシステムを停止することが困難である、修正プログラム等を適用した機器が正常に動作することの検証に費用と工数がかかる、問題なく稼働しているシステムに変更を加えることを避ける傾向がある、等の理由で定期修理時等にまとめて対応するケースも多く、リスクの高い脆弱性であっても、対応に一定の時間を要している。制御システムベンダには、すぐに対応できない場合のリスク緩和に関する情報提供の充実と、何より、脆弱性を作り込まず、セキュリティを考慮した製品の設計・開発（セキュリティ・バイ・デザイン）が求められる。一方で、脆弱性を完全になくすことは困難なため、製品やシステムの稼働後の脆弱性発見に備え、制御システム環境における修正プログラムの適用判断やアップデートをより容易にする仕組みの検討が期待される。

(2) 脅威の動向

2018 年は、2016 年の大規模停電インシデントで使用

されたウイルス「CrashOverride」（別名 Industroyer）の分析の続報や※25、2017 年の安全計装システムへの攻撃の詳細情報が新たに報告されたが※26、制御システムを標的とした目新しいウイルスや攻撃手法等は見られなかった。しかし、留意すべき脅威の動向が大きく二つ見られた。一つは、セキュリティ対策が不十分な IIoT（Industrial Internet of Things）の普及であり、もう一つは、攻撃ツールの高度化と汎用化による攻撃者の裾野の拡大である。

(a) IIoT の普及による脅威の高まり

エネルギー、電力、ガス、水道、製造等の分野の 200 人以上を対象に行われた調査では、IIoT 機器の接続先として 43.1% が制御システムの階層モデルでいう「レベル 3：Operations Support」（生産に関するスケジューリングや各種管理を行う階層）及び「レベル 2：Supervisory Control」（生産の物理的なプロセスを監視制御する階層）のネットワークと回答しており、制御システム環境における IIoT の導入が進んでいる。懸念事項としては、47.6% が製品自体のセキュリティの低さ／欠如、56.0% がアップデートの困難さ／欠如、41.7% がヒューマンエラーやシステムの複雑さに起因する意図せぬ外部への公開（外部からアクセス可能な状態になる）を挙げており※27、多くの組織が IIoT のセキュリティ上の問題点を認識しつつ、その上でなお導入を進めていることが窺える。実際に、製造業界 250 社以上の 400 万以上の機器から収集したデータを解析した調査では、攻撃者による情報収集活動が非常に多く確認され、セグメント化が行われていないフラットな製造系ネットワークに接続された IIoT 機器が、攻撃活動の増加の原因となっている可能性が指摘されている※28。

(b) 攻撃者の裾野の拡大

一般的にインターネットにつながっていない制御システムへの攻撃には高い攻撃スキルが必要で、エリートハッカーと潤沢な予算を有する国家（軍や情報機関）によるサイバー攻撃が主要な脅威と考えられてきた。しかし最近は、国家以外の攻撃者の攻撃スキルが上がり、制御システムに対する攻撃者の裾野が拡大している傾向が見られる。

攻撃スキルの向上の要因としては、2010 年のイランの核燃料施設への攻撃に使用され、特に制御システムを狙った初のウイルスとして話題となった Stuxnet 以降、大規模サイバー攻撃で使用されて公になった高度な攻撃ツールや、国家の情報機関から窃取されて流出した攻撃ツール等が、ハッカーグループやサイバー犯罪組織によって活用されていることが挙げられる。また、アンダーグラウンドのハッカーコミュニティにおいて、サイバー犯罪産業としての「Cybercrime-as-a-Service」が拡大しており、攻撃に必要な情報やツールの購入を可能にしていると見られる※29。英国の情報機関やセキュリティベンダも、国家のハッカーと、民間のハッカーグループやサイバー犯罪組織との境界があいまいになりつつある傾向を指摘している※30。

攻撃者の裾野の拡大の一例として、大手電力事業者の送電変電所の制御システムを模したハニーポットを使って攻撃の観測実験を行った研究者も、実験の結果から、攻撃スキルも OT（Operational Technology）の知識も高くない攻撃者ですら、様々なツールを駆使して制御システムを狙っていると述べ、攻撃者が意図せず制御システムを不正操作し、不測の事態を引き起こす危険性を警告している※31。制御システムを標的とする攻撃者の裾野は、今後も拡大していくことが推測される。

3.1.3 海外の制御システムセキュリティの取り組み

本項では、海外における制御システムのセキュリティに関する取り組みについて述べる。

(1) 米国の取り組み

米国では情報機関の報告書や DHS の注意喚起において、電力網へのサイバー攻撃の脅威が毎年のように警告されている。2018 年も例外ではなく※32、制御システムのセキュリティに特化した取り組みとして、電力網のセキュリティ強化に関するものが目立った。ここでは、そのうちの三つの事例について、概要を紹介する。

(a) 電力網で使用する製品のセキュリティ認証制度の検討

連邦議会下院では、2018 年 3 月に、電力網の基幹系統で使用される製品（制御システム製品を含む）のセキュリティを認定する任意の制度の立ち上げを求める法案「Cyber Sense Act」が提出された。同法案はエネルギー省に対し、基幹系統で使用する製品・機器を洗い出し、セキュアであることをテスト・認定する「Cyber Sense」プログラムを確立するよう定めている。また、認定された製品については、脆弱性を報告する仕組みとデータベースの整備を要求している※33。

(b) サイバー攻撃により落ちた電力網の復旧演習

DARPA（Defense Advanced Research Projects Agency：国防高等研究事業局）では、11月に、ニューヨーク州ロングアイランド沖のプラムアイランドにある試験用の電力網を使い、サイバー攻撃によって落とされた電力網の制御を取り戻し、電力供給を復旧させる演習「Liberty Eclipse」を実施した。演習は、電力系統からの電力供給なしに、発電機を起動させて系統復旧に必要な発電を行う「ブラックスタート」を想定し、実際にブラックスタートが必要な状態を再現して実施された。防衛チームは、攻撃チームによる妨害に対応しつつ復旧に取り組んだ※34。

(c) セキュリティ対策としての電力網の一部アナログ化の検討

連邦議会上院では、12月に、サイバー攻撃対策として電力網の基幹系統にあえてアナログ技術を取り入れることを検討する法案「Securing Energy Infrastructure Act」が通過し、下院に送られた。同法案は、2015年のウクライナの大規模停電が、手動運用により比較的迅速に復旧できたことを受けて起案された。同法案はエネルギー省に対し、サイバー攻撃による影響の低減につながる、現行の電力網に統合可能なアナログ／非デジタル／物理的技術を検討する2年間のパイロットプログラムの実施を定めている※35。なお、アナログ化によるセキュリティ効果に関しては、議論も呼んでいる。

(2) 欧州の取り組み

欧州では5月10日に、重要インフラのセキュリティ強化の取り組みとしてNIS指令（Network and Information Security Directive）が実質的に発効した（NIS指令については「2.2.3 欧州の政策」参照）。

制御システムのセキュリティに特化した取り組みで目立ったものはなかったが、例年どおり、NATO（North Atlantic Treaty Organization：北大西洋条約機構）による世界最大規模のサイバー演習「Locked Shields」が実施された。2018年の演習では、架空の国家Crimsoniaのハッカーが、同じく架空の国家Beryliaの浄水場の薬液注入を制御する装置に侵入して水道水を汚染し、中毒者や犠牲者が発生した等の攻撃シナリオのもと、約30ヵ国、1,000人以上のセキュリティ専門家が22チームに別れ、状況の把握とシステムの制御奪還を競った※36。

(3) オーストラリアの取り組み

オーストラリアでは、重要インフラの制御システムに関する詳細情報の国への提出を義務付ける法案「Security of Critical Infrastructure Bill 2018」が成立し、7月11日に施行された。同法では、主要な電力・ガス・水道事業者及び港湾施設の運用事業者に対し、国内／オフショア、自社運用／アウトソーシングを問わず、重要インフラシステムやデータについて、何をどこに所有し、誰が制御・管理しているのか等の詳細情報を、施行日から6ヵ月以内に当局に提出することを義務付けている（変更があった場合の30日以内の更新も義務付け）※37。オフショアやアウトソーシングの資産を含むことで、重要インフラのサプライチェーン上の脅威を把握する狙いがあると思われる。

(4) その他の取り組み

その他の傾向として、法規制に関してはコンプライアンスの強化策として、高額な罰金を制定したり、課したりするケースが見受けられた。NIS指令の加盟国の国内法化にあたっては、EU（European Union：欧州連合）が罰金を高額に制定するよう呼び掛けており、英国では最高1,700万ポンド（約23億円）と決められている※38。また、米国ではNERC（North American Electric Reliability Corporation：北米電力信頼度協議会）が、CIP（Critical Infrastructure Protection）サイバーセキュリティ基準に違反した電力会社に、過去最高額となる1,000万ドル（約11億円）の罰金を課している※39。コンプライアンスの向上につながるのか、今後の動きが注目される。

3.1.4 国内の制御システムセキュリティの取り組み

国内では、制御システムを含む重要インフラのセキュリティ政策は、重要インフラ防護に係る基本的な枠組みである「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」（2017年4月策定、2018年7月改定）（以下、第4次行動計画）※40、日本のサイバーセキュリティ政策として3年ごとに見直される「サイバーセキュリティ戦略」（2018年7月変更）※41、同戦略に基づく各年度の取り組み方針として毎年策定される「サイバーセキュリティ2018」（2018年7月策定）※42において規定され、実施されている。

2018年時点の上記政策では、重要インフラサービスの安全かつ継続的な提供のため、事業者によるリスクマ

ネジメントを大きな柱の一つとし、定期的なリスクアセスメントの実施を促進している。本項では、制御システムを含む、重要インフラサービスを支えるシステムのリスクアセスメントに関する取り組み、及び、制御システムのセキュリティ強化に関するその他の主な取り組みの概要を紹介する。

(1) 重要インフラサービスを支えるシステムのリスクアセスメントの促進に関する取り組み

重要インフラシステムのリスクマネジメントの推進は、政府機関では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）と経済産業省が中心となって取り組んでいる。

NISC では、4 月に、「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」を公開した※43。同手引書は、NISC が 2017 年 7 月に東京 2020 オリンピック・パラリンピック競技大会の関連事業者向けに提供した「機能保証のためのリスクアセスメント・ガイドライン※44」を汎用のリスクアセスメント向けに改定したものである。同手引書では、リスクを特定し、そのリスクが発生した場合の「影響度」及び「発生頻度」（発生可能性）を縦軸と横軸にそれぞれ 5 段階で評価してリスク値を算定し、あらかじめ定めた基準値以上の値を持つリスクについてリスク対応を行う手法を紹介している。図 3-1-3 に、影響度と発生頻度によるリスク値算定のイメージを示す。NISC では、同手引書を用いて、事業者によるリスクアセスメントの普及に取り組んでいる。

より詳細なリスクアセスメントが必要な事業者に向けては、IPA が 10 月に「制御システムのセキュリティリスク分析ガイド第 2 版」を公開している※46。同ガイドは、制御システムの詳細なリスクアセスメントを実施するために、「資産ベースの分析」と「事業被害ベースのリスク分析」の二つの分析手法を紹介し、具体的な実施手順を解説

※リスク基準を「5 以上」とした場合、黄色い個所に該当するリスクがリスク対応の対象となります。

発生頻度		事象の予想発生頻度
5	非常に多い	頻発
4	多い	1 年に 1 回程度発生
3	中程度の頻度	数年に 1 回程度発生
2	少ない	10 年に 1 回程度発生
1	非常に少ない	ごくまれに、例外的な状況で発生

事象の予想発生頻度						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		事象の結果の影響度				

影響度		影響度合い（下記のような要素を総合的に勘案して影響度を決定します。）			
		業務に対する影響の範囲・程度	予想復旧時間	対応に要するコスト	人命や環境への影響範囲・程度
5	重大な影響	当該業務が停止する。	業務の復旧自体が困難である。	業務の復旧や事象の結果の対処（情報漏えいに係る損害賠償金の支払いや代替手段の手配等を含む。）のために要するコスト（業務停止中の損失等を含む。）の負担が、事業者にとって甚大である。	複数の死亡者が発生する。
4	大きな影響	当該業務が阻害され、業務の最低水準の維持が困難である。	業務の最大許容停止時間内での業務の復旧が困難である。	業務の復旧や事象の結果のために要するコストの負担が、事業者にとって大きい。	1 人の死亡者あるいは複数の重傷者が発生する。
3	中程度の影響	当該業務が阻害され、業務の最低水準を維持できないおそれがある。	業務の最大許容停止時間内での業務の復旧が可能である。	業務の復旧や事象の結果のために要するコストの負担が、事業者にとって中程度である。	1 人の重傷者あるいは複数の軽症者が発生する。
2	小さな影響	当該業務が阻害されるが、業務の最低水準は維持される。	業務の阻害が軽度で収まる時間内での復旧が可能である。	業務の復旧や事象の結果のために要するコストの負担が、事業者にとって小さい。	1 人の軽症者が発生する。
1	軽微な影響	–	業務の阻害が生じない時間内での復旧が可能である。	業務の復旧や事象の結果のために要するコストの負担が、事業者にとって軽微である。	–

■図 3-1-3　影響度と発生頻度によるリスク値算定のイメージ
（出典）NISC「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）※45」

している。

資産ベースのリスク分析は、システムを構成する機器等の資産に対する分析で、「脅威」（脅威の発生可能性）、「脆弱性」（脅威に対する資産の脆弱度）、「資産の重要度」からリスク値を算定する。また、事業被害ベースのリスク分析は、システムが実現する事業・サービス等に対する分析で、「脅威」、「脆弱性」、「事業被害」（脅威が発生した場合の事業への影響）からリスク値を算定する。

第2版では、重要インフラの制御システムのリスク評価事業※47の実施主体として、IPAが実際に同ガイドの第1版を用いて複数事業者の制御システムのリスクアセスメント支援を行った中で得たフィードバックを踏まえ、主に以下の2点を改定している。

(a) 説明の補足・拡充

リスクアセスメントにおける評価指標と評価値、とりわけ判断要素が多岐にわたり検討が難しい「脅威」の考え方について、説明を拡充した。また、リスクアセスメントの結果として得られるリスク値の意味を、より厳密に定義した。

(b) リスク分析手法の見直しによる工数の削減

リスクアセスメントの工数をより削減できるように、二つのリスク分析手法について、それぞれ以下の見直しを行った。

- 資産ベースのリスク分析
  第1版では事前準備（システム構成図の作成）と実際のリスク分析の2段階で実施していた「資産のグループ化」を、事前準備段階で一括実施するようにした。また、複数の手順を要していた「資産に対する脅威と対策候補の抽出」について、資産種別（情報系資産か、制御系資産か、ネットワーク資産か）を用いて一手順で抽出できるようにした。
- 事業被害ベースのリスク分析
  攻撃者がどのように攻撃を行うかを示す「攻撃ツリー」は、攻撃のシナリオ、侵入口、攻撃者、攻撃ルートの4要素の組み合わせとなる。第1版では、すべての攻撃ツリー（すべての組み合わせ）を洗い出してから、優先度が低いと考えられる攻撃ツリーを除外し、実際に分析対象とする攻撃ツリーを絞り込んでいた。第2版では、攻撃ツリーの各要素について、優先度の観点と判断基準を提示し、最初から基準に合致する侵入口や攻撃ルートのみに絞り込むことで、自然と優先度の高い攻撃ツリーのみが導出されるように、分析作業をより手順化・簡略化した。これは、現実的に投入可能な人員と予算で、まずは重要かつ攻撃者に狙われやすいところからリスク分析を実施し、分析対象外とした攻撃ツリーは、リスクアセスメントのPDCAサイクル（Plan（計画）-Do（実施）-Check（確認・監査）-Act（見直し・改善））の中で、適宜対象を拡大し、分析していくことを想定している。

(2) その他の取り組み

国内におけるその他の主な取り組みとしては、制御システムのサイバーセキュリティに関するガイドラインの策定や、既存の規程への組み込み等があった。

経済産業省の「産業サイバーセキュリティ研究会WG1」では、「Connected Industries」におけるサプライチェーンのサイバーセキュリティ対策指針として「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定している※48。2018年はこの一環として、同WGのビルサブワーキンググループにより、「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」が公開された※49。同ガイドラインは、建物の空調、エレベーター、防災設備等を監視・制御するビルディング・オートメーション・システムにおいて考慮すべきセキュリティリスク及び対策をまとめている。

また、経済産業省では、「サイバーセキュリティ2018」に基づき、ガス事業法第97条によってガス事業者に策定と遵守が義務付けられている保安規程に※50、「製造・供給に係る制御システムのサイバーセキュリティ対策」に関する規定を今後、具体的な検討を進めていく※42。「安全性（セーフティ）」を守るための内規として事業者に重んじられてきた保安規程に「セキュリティ」が組み込まれることで、事業者のセキュリティ意識が否応なく変わっていくことも見込まれる。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術を適用した製品市場の拡大は、インターネットにつながる機器（IoT 機器）の台数を増加させている。一方で、設定不備のまま、あるいは脆弱性を有したままインターネットに接続される IoT 機器の増加は、悪意を持った攻撃者にとって絶好の機会となり、その脅威は増大している。

IoT 技術の恩恵を受ける世界中の人々がこの課題や問題点を認識・共有し、抜本的な対策を進めるべき時期が来ている。世界各国において、脆弱な IoT 機器を減少させるため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。

3.2.1 増大するIoTのセキュリティ脅威

IoT 機器に感染するウイルス「Mirai」は、作成者が公開したソースコードを元に、新旧様々な脆弱性を悪用した亜種が発生し、IoT 機器への感染手段を巧妙化させている。また、感染後の IoT 機器の悪用方法が多様化するとともに、その被害範囲も拡大している。IoT 機器に感染する Mirai 以外のウイルス（Gafgyt や VPNFilter）もこれらの機能を取り込み、悪質に進化を遂げており、IoT に対する脅威は更に増大している。

(1) 感染手段の巧妙化

感染手段として、典型的な認証情報※51 の辞書攻撃を用いていた Mirai に対して、2017 年に出現した Mirai の亜種は、特定の IoT 機器が持つ脆弱性を狙って感染を試みるようになった。その後、Mirai の様々な亜種や「亜種の亜種」、IoT 機器を狙う Mirai 以外のウイルスの亜種等が出現し、各々のウイルスが古くから存在する脆弱性や新たに発見された脆弱性を悪用する等、感染手段が更に巧妙化している。ここでは、新たに出現したウイルスや進化した既存のウイルスとその感染手段について解説する。

(a) Masuta

Mirai の亜種の一つ「Masuta」の活動については、2017 年 11 月から観測されていた※52 が、2018 年 1 月、ダークフォーラムで発見された Masuta のソースコードに関して、次のような解析結果が報告された※53。

- 暗号鍵は 0xdedeffba（Mirai は 0xdeadbeef）。
- Mirai の亜種「Satori」※54 が用いた C&C サーバ※55 の URL が埋め込まれている。
- root/ パスワード未設定、admin/admin、admin/1234 といった典型的な認証情報※51 の初期設定値を保有。
- ソースコード中でセキュリティ専門家 Brian Krebs 氏について言及。

なお、ソースコードは発見されなかったものの、検体の異なる Masuta の亜種（発見者は「PureMasuta」と命名）が存在し、D-Link Systems, Inc.（以下、D-Link）製ルータ DIR-645 のコマンドインジェクション脆弱性※56 を悪用して感染するように拡張されていることも報告された。

また、2018 年 5 月、メキシコを発信源とするネットワークスキャン活動において、後述する家庭用 GPON ルータの脆弱性（「3.2.1 (1) (d) Omni」参照）を狙うように拡張された Masuta が観測されている※57。

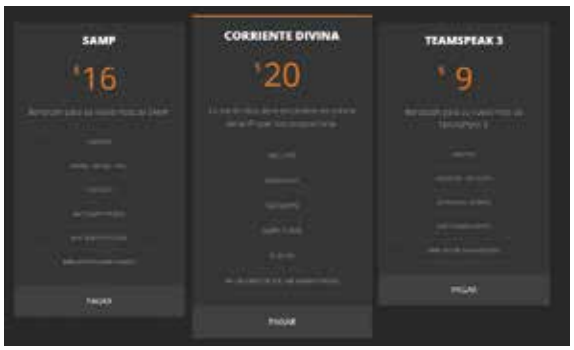
(b) JenX／Jennifer

2018 年 2 月、Jennifer と呼ばれるウイルスに感染した IoT 機器で構成される新たなボットネットが発見され、「JenX」と命名された※58。JenX は、2017 年 12 月にインターネット上の Web サービス Pastebin でソースコードが公開された※59、以下の脆弱性を用いて感染を拡大する。

- CVE-2014-8361※60（Realtek SDK における任意のコード実行の脆弱性）
- CVE-2017-17215※61（Huawei HG532 ルータにおける任意のコード実行の脆弱性）

これらは、2017 年に Satori や IoT 機器を破壊するウイルス「BrickerBot」※62 によって、感染手段として悪用され始めた脆弱性である。

攻撃者は、セーシェル共和国でオンラインゲーム用のホストサーバを提供しているドメインに C&C サーバを設置し、第三者に対して DDoS 攻撃をレンタル提供するサービスを提供していた（次ページ図 3-2-1）。



■図 3-2-1　DDoS-as-Service の提供例
（出典）Radware Ltd.「JenX – Los Calvos de San Calvicie※58」

(c) Satori.Dasan

2018 年 2 月、Satori の新たな亜種によるネットワークスキャン活動が観測された※63。DASAN Networks, Inc. 製 GPON Wi-Fi ルータ H640X の非認証リモートコード実行の脆弱性（CVE-2017-18046※64）を狙うように拡張されており、「Satori.Dasan」と命名された。観測された感染機器（表 3-2-1）の大半はベトナムに集中しており、インターネット接続機器検索サービス SHODAN※65 を用いた同社製ルータの探索においても、40,605 台中 26,519 台がベトナムに存在することが指摘されている。

国名	感染ホスト台数
ベトナム	2,125
中国	407
米国	312
タイ	160
韓国	126

■表 3-2-1　Satori.Dasan の国別感染観測台数
（出典）Radware Ltd.「New Satori Botnet Variant Enslaves Thousands of Dasan WiFi Routers※63」を基に IPA が編集

(d) Omni

2018 年 5 月、DASAN Networks, Inc. 製 GPON ホームルータの以下に示す脆弱性を狙って構築中のボットネットが発見され、「Omni」と命名された※66。

- CVE-2018-10561※67（認証回避の脆弱性）
- CVE-2018-10562※68（コマンドインジェクションの脆弱性）

解析結果によると、Omni は Mirai の亜種の一つである Owari に酷似しており、同じ作成者によるウイルスであると報告されている。

(e) Wicked

2018 年 5 月、以下に示す 3 種類の脆弱性を狙うボットネットが発見され、「Wicked」と命名された※69。

- Netgear 製ルータ DGN1000, DGN2200 v1 非認証リモートコード実行の脆弱性※70
- CCTV/DVR リモートコード実行の脆弱性※71
- CVE-2016-6277※72（Netgear 製ルータ R7000/R6400 コマンドインジェクションの脆弱性）

また、IoT 機器の脆弱性を直接悪用する代わりに、既に侵害を受けて悪意のある Web シェルがインストールされた Web サーバを利用して感染を試みることも確認されている。

その後の調査の結果、Wicked、Owari、Omni の作成者は同一人物であり、「Wicked」のハンドルネームを使用してインタビューに答えている、と報告されている。

(f) Satori の亜種

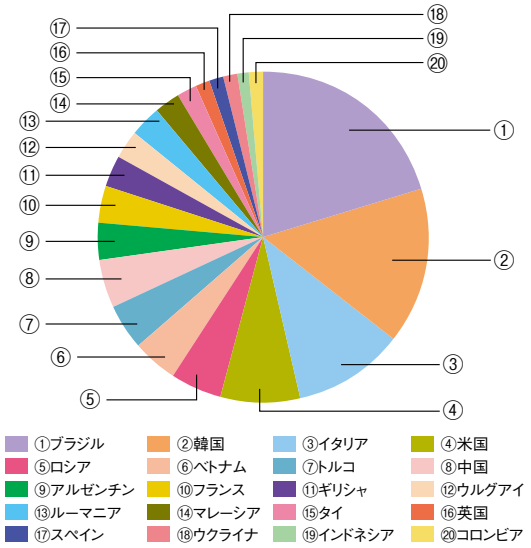
2018 年 6 月、Satori の新たな検体（亜種）とそれを用いた DDoS 攻撃の観測が報告された※73。この亜種は、ネットワークカメラやデジタルビデオレコーダー等の IoT 機器に搭載されている、Hangzhou Xiongmai Technology Co., Ltd 製の組み込み用 Web サーバ uc-httpd 1.0.0 のバッファオーバーフローの脆弱性（CVE-2018-10088※74）を感染経路とするように拡張されている。日本国内においても感染したと考えられる機器が急増したことから、警察庁※75 や国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology：NICT）※76 は注意喚起を行った。

同月、この亜種は、D-Link 製ルータ DSL-2750B のコマンドインジェクションの脆弱性※77 を狙うように更に拡張された。感染が観測された、数千台の IoT 機器の国別分布を図 3-2-2 に示す※78。

(g) Omni の亜種

2018 年 5 月、表 3-2-2 に示す 11 種類の脆弱性を狙うように拡張された Omni の亜種が発見された※79。これらは、これまで Mirai の様々な亜種が悪用した脆弱性であるが、11 種類すべてを悪用する亜種が初めて確認された。また、この亜種は、以下に示す特徴を有する。

- 二つめの暗号鍵を利用する。
- 感染手段としては脆弱性を悪用するのみで、典型的な認証情報※51 を用いた辞書攻撃による不正ログインを試みない。
- 感染した IoT 機器が他のウイルスに感染することを防



■図 3-2-2　Satori 亜種の感染機器の国別分布
（出典）Radware Ltd.「Satori IoT Botnet Variant※78」を基に IPA が編集

止するために、特定のポートで受信したパケットをドロップするように iptables を用いて設定変更する。

(h) Okane

2018 年 5 月、Mirai の亜種「Okane」の攻撃が観測された※79。前項で示した Omni の亜種と同様に、11 種類の脆弱性を悪用して感染を試みる点に加えて、従来の Mirai やその亜種と同様に、典型的な認証情報※51を用いた辞書攻撃による不正ログインを試みる。この際、従来の亜種には見られない認証情報（表 3-2-3）が含まれている。また、従来の亜種には存在しない新しい DDoS 攻撃手法が組み込まれている。

(i) Miori ／ IZ1H9 ／ APEP

2018 年 12 月、主に中国で利用されている Web アプリケーションフレームワーク ThinkPHP の脆弱性※86（遠隔からのコード実行）を悪用して拡散する Mirai の亜種が発見され、「Miori」と命名された※87。

No.	ベンダ名	機器名	脆弱性
1	DASAN Networks, Inc.	GPON ルータ	CVE-2018-10561※67, CVE-2018-10562※68
2	各社	Realtek SDK を用いた各機器	CVE-2014-8361※60
3	Netgear	ルータ DGN1000/DGN 2200v1	Netgear setup.cgi 非認証リモートコード実行の脆弱性※70
4	Huawei Technologies Co., Ltd.	HG532	CVE-2017-17215※61
5	ZyXEL Communications Corp.	ADSL ルータ eir D1000 modem	CVE-2016-10372※80 （WAN 側からのリモートコードインジェクションの脆弱性）
6	D-Link	ルータ DIR-645 他	CVE-2015-2051※81 （HNAP SoapAction ヘッダコマンド実行の脆弱性）
7	各社（70 社以上）	CCTV や DVR	CCTV/DVR のリモートコード実行の脆弱性※71
8	MVPower	DVR TV-7104HE, TV-7108HE 等	JAWS Web サーバの非認証シェルコマンド実行の脆弱性※82
9	D-Link	ルータ DIR-300/600/645/845/865 等	UPnP SOAP Telnetd コマンド実行の脆弱性※83
10	Netgear	ルータ R7000/R6400	CVE-2016-6277※72（cgi-bin コマンドインジェクションの脆弱性）
11	FUHO Technology Co., Ltd.	VACRON NVR	リモートコマンド実行（board.cgi コマンドインジェクション）の脆弱性※84

■表 3-2-2　Omni 亜種が感染に悪用する脆弱性
（出典）Palo Alto Networks, Inc.「Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns※79」を基に IPA が作成

ユーザ名	パスワード	該当する IoT 機器の例
root	t0talc0ntr0l4!	Control4 Corporation 製 Home Theater Controller AVM-HTC1-B の初期ユーザ名とパスワード
admin	adc123	CommScope, Inc. 製 ADC FlexWave Prism の初期ユーザ名とパスワード
mg3500	merlin	Camtron Industrial Inc. 製 CMNC-200 IP カメラ 説明書未記載の初期ユーザ名とパスワード（CVE-2010-4233※85）

■表 3-2-3　Okane に組み込まれた不正ログイン用認証情報の例
（出典）Paro Alto Networks, Inc.「Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns」を基に IPA が作成

ビルドインされたユーザ名やパスワードの例		
Miori	IZ1H9	APEP
1001chin、adm、admin123、admintelecom、aquario、default、e8ehome、e8telnet、GM8182、gpon、oh、root、support、taZz@23495859、telecomadmin、telnetadmin、tsgoingon、ttnet、vizxv、zte	00000000、12345、54321、123456、1111111、20080826、20150602、88888888、1234567890、/ADMIN/、admin1、admin123、admin1234、antslq、changeme、D13hh[、default、ezdvr、GM8182、guest、hi3518、ipc71a、IPCam@sw、ipcam_rt5350、juantech、jvbzd、klv123、klv1234、nimda、password、qwerty、QwestM0dem、root123、service、smcadmin、support、svgodie、system、telnet、tl789、vizxv、vstarcam2015、xc3511、xmhdpic、zlxx.、zsun1188、Zte521	123456、888888、20150602、1q2w3e4r5、2011vsta、3ep5w2u、admintelecom、bcpb+serial#、default、e8ehome、e8telnet、fliruser、guest、huigu309、juniper123、klv1234、linux、maintainer、Maxitaxi01、super、support、taZz@01、taZz@23495859、telecomadmin、telnetadmin、tsgoingon、vstarcam2015、Zte521、ZXDSL

■表 3-2-4　Miori ／ IZ1H9 ／ APEP に組み込まれた不正ログイン用認証情報の例
（出典）Trend Micro Incorporated「With Mirai Comes Miori: IoT Botnet Delivered via ThinkPHP Remote Code Execution Exploit※87」を基に IPA が作成

同月、Mirai の既知の亜種「IZ1H9」や「APEP」も同じ脆弱性を悪用して拡散していることが確認されている。これらの Mirai の亜種は、典型的な認証情報※51 を用いた辞書攻撃による不正ログインも試みるが、あらかじめ埋め込まれたユーザ名やパスワードが異なっている（表 3-2-4）。

(j) Yowai

2019 年 1 月、Mirai の亜種が発見され、「Yowai」と命名された※88。感染に際して悪用する典型的な認証情報※51 として、表 3-2-5 に示すパスワード辞書を保有している。

ビルドインされたパスワードの例
Yowai
OxhlwSG8、defaulttlJwpbo6S2fGqNFsadmin、daemon、12345、guest、support、4321、root、vizxv、t0talc0ntr0l4!、bin、adm、synnet

■表 3-2-5　Yowai に組み込まれた不正ログイン用認証情報の例
（出典）Trend Micro Incorporated「ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai※88」を基に IPA が作成

また、以下に示す脆弱性を悪用した感染を試みることも確認されている。

- ThinkPHP のリモートコード実行の脆弱性※86
- CVE-2014-8361※60
- Linksys 製ルータのリモートコード実行の脆弱性※89
- CVE-2018-10561※67
- CCTV/DVR リモートコード実行の脆弱性※71

(k) Hakai

2018 年 5 月、10 種類の脆弱性（前ページの表 3-2-2 の 11 種類のうち No.9 を除く）を感染経路とするウイルス「Hakai」が発見された※79。他の Mirai 系ウイルスとは異なり、Gafgyt（Bashlite や QBot 等の別名あり）のソースコードを基にビルドされており、その後、D-Link 製ルータ DSL-2750B のコマンドインジェクションの脆弱性※77 を狙うように拡張されたことが確認されている。

2018 年 8 月、C&C サーバや一部の攻撃コードが異なる Hakai の亜種が確認され、「Kenjiro」と「Izuku」と名付けられた※90。

また、2019 年 1 月に発見された Hakai の亜種は、以下に示す脆弱性を悪用した感染を試みることが確認されている※88。

- ThinkPHP のリモートコード実行の脆弱性※86
- D-Link DSL-2750B ルータの脆弱性※77
- CVE-2015-2051※81
- CVE-2014-8361※60
- CVE-2017-17215※61

(2) 悪用方法の多様化と被害対象の範囲拡大

ウイルスに感染した IoT 機器の悪用方法は、初期の Mirai では、第三者のサーバに対する DDoS 攻撃の踏み台であった。その後、IoT 機器を破壊して機器の利用者に直接被害を与える BrickerBot が出現したが、IoT 機器以外への攻撃に用いられる等、更に悪用方法が多様化するとともに、被害対象の範囲が拡大している。

(a) ホームルータの DNS 設定書き換えによる不正サイトへの誘導

2018 年 3 月、日本国内にて、ルータの設定情報が改ざんされ、インターネット接続が不能となったり、Android 用不正アプリのインストールを促すサイトに誘導されたりする事件が発生し、NICT は注意喚起を行った※91。

感染ルータ経由でインターネットにアクセスすると、悪意のあるDNSサーバによって名前解決が行われ、facebook.com、twitter.com、www.google.com以外のWebサイトへのアクセスは、「Facebook拡張ツールバッグ」や「Chrome最新バージョン」に偽装したAndroid用不正アプリをインストールさせようとするサイトに誘導される（図3-2-3）※92。このサイトは、韓国語、中国語（繁体字、簡体字）、日本語、英語に対応しており、特にアジア圏を狙った攻撃と推測される。サイトの指示に従うと、正規アプリに偽装した、情報を窃取する不正アプリをインストールすることになる。

■図3-2-3　Android用不正アプリ配布サイトへの誘導例
（出典）トレンドマイクロ株式会社「不正アプリをダウンロードさせるルータのDNS設定書き換え攻撃が発生※92」

国内の複数の通信事業者やメーカのルータ製品でDNS設定書き換えが発生し、各社は最新ファームウェアへの更新やセキュリティ設定変更、管理用パスワード変更等の案内・注意喚起を行った（表3-2-6）※93。

2018年4月、ブラジルを中心に、MikroTik製ルータの脆弱性を悪用して感染し、DNS設定情報を改ざんする攻撃が観測された※101。過去の事例から、インターネットバンキングのサイトへのアクセスを、不正なサイトへ誘導するために改ざんしたと見られている。更に、感染したルータはプロキシサーバとして動作するよう、初期設定で閉じたポートを開放する挙動が報告されている。

（b）プロキシサーバとしての悪用（OMG）

2018年2月、感染したIoT機器をプロキシサーバとして悪用する機能が追加されたMiraiの亜種が発見され、「OMG」と命名された※102。OMGは、Miraiと同様に他の感染対象機器を探索する機能とDDoS攻撃を仕掛ける機能に加えて、感染機器のファイアウォール設定を変更した上で、オープンソースのプロキシサーバ3proxyを動作させる機能を有する。

プロキシサーバは、サイバー攻撃において匿名性を高めるために悪用されるため、攻撃者は自ら利用するだけでなく、感染機器上で動作させたプロキシサーバへのアクセス権を他のサイバー攻撃者に販売することによって、利益を得ようとしたのではないか、と発見者は推察している。

（c）仮想通貨マイニングへの悪用（ADB.Miner）

2018年2月、Miraiのソースコードを流用し、Android OSを採用したIoT機器（スマートフォンやスマートテレビ）を狙うウイルスが発見され、ADB.Minerと名付けられた※103。ADB.Minerは、ポート番号5555を探索して、対象機器のデバッグ用インタフェースADB（Android Debug Bridge）に接続し、仮想通貨Monero／XMRのマイニングを行うウイルスを不正インストールする。C&Cサーバは存在せず、マイニングで得られた仮想通貨は

事業者・製造者	対象機種	注意喚起日
東日本電信電話株式会社※94 西日本電信電話株式会社※95	Netcommunity OG410Xa、OG410Xi、OG810Xa、OG810Xi Netcommunity OG400Xa、OG400Xi、OG800X、OG800Xa、OG800Xiの一部機器	2018年3月28日
ロジテック株式会社※96	LAN-W300N/R、LAN-W301NR等	2018年4月2日
株式会社バッファロー※97	WHR-300HP2、WHR-G301N、WHR-1166DHP4等	2018年4月5日
NECプラットフォームズ株式会社※98	機種情報なし	2018年4月6日
株式会社アイ・オー・データ機器※99	機種情報なし	2018年4月12日
ニフティ株式会社※100	住友電気工業製TE/4C、TE4111C、TE4121C、TE4551、TE4571EW NECプラットフォームズ製Aterm DR200Cシリーズ、Aterm DR300CVシリーズ、Aterm WD600CVシリーズ、Aterm WD700CVシリーズ	2018年4月26日

■表3-2-6　DNS設定書き換えに対する各社の注意喚起
（出典）piyolog「ルーターの設定情報改ざんについてまとめてみた※93」を基にIPAが作成

攻撃者のウォレットに入るように設定されている※104。感染機器の大半は、中国（香港・台湾を含む、全体の39%）と韓国（全体の39%）であった。

2018年7月、ADBポートを用いた拡散や仮想通貨マイニングがSatoriの亜種にも悪用されており、中国と米国、韓国を中心に活動していることが報告された※105。

(d) PC上の仮想通貨マイニングソフトウェアへの攻撃（Satori.Coin.Robber）

2018年1月、脆弱なIoT機器を狙う攻撃コードに加えて、IoT機器以外で動作する仮想通貨マイニングソフトウェアへの攻撃機能を有する、Satoriの亜種が発見され、Satori.Coin.Robberと名付けられた※106。この亜種は、ポート番号3333をスキャンして、仮想通貨マイニングソフトウェアClaymore Minerが動作する機器（主にWindows PC）を探索する。Claymore Minerの遠隔管理インタフェースの脆弱性（非認証でアクセス可能な初期設定）を攻撃することで、設定情報（マイニングプールとウォレットアドレス）を書き換えて、得られた仮想通貨を横取りし、攻撃者のウォレットに入るようにする。攻撃者は乗っ取ったClaymore Minerを悪用して、10日間で1.01000710ETH（約980米ドル）を得たと報告されている※107。

2018年3月、警察庁はSatori.Coin.RobberとADB.Miner（「3.2.1(2)(c)仮想通貨マイニングへの悪用（ADB.Miner）」参照）に関して、注意喚起を行った※108。

(3) VPNFilter

2018年5月、世界54ヵ国以上において50万台以上のネットワーク機器が「VPNFilter」と呼ばれるウイルスに感染していることが報告された※109。感染機器には、Linksys、MikroTik、Netgear、TP-LINK Technologies Co., Ltd.（以下、TP-LINK）製小規模事業者向けルータやQNAP Systems, Inc.（以下、QNAP）製NAS（Network-Attached Storage：ネットワーク接続ストレージ）が含まれる。VPNFilterのソースコードは、2015年12月に発生したウクライナの大規模停電で用いられたウイルスBlackEnergyに酷似しており、Webサイトの認証情報を窃取する機能、制御システムで用いられているSCADA（Supervisory Control And Data Acquisition）のModbusプロトコルを監視する機能、感染機器を使用不能とする「Kill」コマンド実行機能を持つ。

VPNFilterの感染活動は2016年から確認されていたが、世界中で活動が拡大したことから、JPCERT/CCは注意喚起を行った※110。

2018年6月、更に多くの機器が感染対象となっていることが報告された（表3-2-7）※111。

2018年7月の時点でVPNFilterに感染していることが確認されたネットワーク機器において、19件の脆弱性が検出されている（表3-2-8）※112。表において、No.2、No.4、No.12は、Miraiの亜種「Reaper」※113が悪用する脆弱性と同一である。調査結果によると、家庭用ネットワークの34%で、脆弱性を有するIoT機器（ネットワー

ベンダ名	機器名
ASUSTeK Computer Inc.（以下、ASUS）	RT-AC66U、RT-N10、RT-N10E、RT-N10U、RT-N56U、RT-N66U
D-Link	DES-1210-08P、DIR-300、DIR-300A、DSR-250N、DSR-500N、DSR-1000、DSR-1000N
Huawei Technologies Co., Ltd.	HG8245
Linksys	E1200、E2500、E3000、E3200、E4200、RV082、WRVS4400N
MicroTik	CCR1009、CCR1016、CCR1036、CCR1072、CRS109、CRS112、CRS125、RB411、RB450、RB750、RB911、RB921、RB941、RB951、RB952、RB960、RB962、RB1100、RB1200、RB2011、RB3011、RB Groove、RB Omnitik、STX5
Netgear	DG834、DGN1000、DGN2200、DGN3500、FVS318N、MBRN3000、R6400、R7000、R8000、WNR1000、WNR2000、WNR2200、WNR4000、WNDR3700、WNDR4000、WNDR4300、WNDR4300-TN、UTM50
QNAP	TS251、TS439 Pro、QTSソフトウェアが動作する他のQNAP NAS
TP-LINK	R600VPN、TL-WR741ND、TL-WR841N
Ubiquiti Networks, Inc.	NSM2、PBE M5
Upvel LLC	機種不明
ZTE Corporation	ZXHN H108N

■表3-2-7　VPNFilterの感染対象機器
（出典）Cisco Systems, Inc.「VPNFilter Update - VPNFilter exploits endpoints, targets new devices※111」を基にIPAが作成

No.	ベンダ名	機器名／サービス名	脆弱性
1	QNAP	NAS 各機種の FTP サービス	CVE-2015-7261[※114]（認証回避の脆弱性）
2	D-Link	ルータ DIR-300	CVE-2011-4723[※115]（パスワード漏えいの脆弱性）
3	ASUS	ルータ RT-AC66U、RT-N66U	CVE-2014-9583[※116]（リモートコード実行の脆弱性）
4	Linksys	ルータ E1500、E2500	CVE-2013-2678[※117]（コマンドインジェクションの脆弱性）
5	Netgear、TP-LINK、D-Link 等	各機種の脆弱性を有する UPnP サービス	CVE-2013-0229[※118]（バッファオーバーフローの脆弱性）
6			CVE-2013-0230[※119]（スタックオーバーフローの脆弱性）
7	QNAP	NAS 各機種の QTS ソフトウェア（4.2.4 Build 20170313 以前）	CVE-2017-6361[※120]（リモートコード実行の脆弱性）
8	ASUS	ルータ RT-AC、RT-N	CVE-2017-8877[※121]（ルータ JSONP 情報漏えいの脆弱性）
9	Netgear	ルータ R6400、R7000、R8000	CVE-2017-5521[※122]（ルータパスワード漏えいの脆弱性）
10	Netgear、TP-LINK、D-Link 等	各機種の脆弱性を有する UPnP サービス	CVE-2012-5958[※123]（スタックオーバーフローの脆弱性）
11			CVE-2012-5959[※124]（スタックオーバーフローの脆弱性）
12	D-Link	ルータ DIR-300	リモートコード実行の脆弱性[※125]
13	Netgear	ルータ WNR2000	パスワードの漏えいの脆弱性
14	Netgear	ルータ R6400、R7000	CVE-2016-6277[※72]（リモートコード実行の脆弱性）
15	ASUS	ルータ RT-N66U	CVE-2017-6549[※126]（ルータセッションハイジャックの脆弱性）
16	Linksys	ルータ E4200	CVE-2013-2679[※127]（OS コマンドインジェクションの脆弱性）
17	Netgear	ルータ WNR1000	認証回避の脆弱性
18			パスワードの漏えいの脆弱性
19	TP-LINK	ルータ TL-WR841N	非認証ルータアクセスの脆弱性

■表 3-2-8　VPNFilter に狙われる IoT 機器の脆弱性
（出典）Trend Micro Incorporated「VPNFilter-affected Devices Still Riddled with 19 Vulnerabilities[※112]」を基に IPA が作成

ク機器を含む）が少なくとも 1 台以上確認されている。更に、これらの脆弱な IoT 機器の約 9% が VPNFilter に感染している可能性があるという。

3.2.2 脆弱なまま販売・運用される IoT機器の散在

IoT 機器を狙った攻撃の手口が進化を続ける一方で、攻撃を受ける側の対策が進んでいないことが明らかになっている。本項では、国内におけるインシデント発生状況と、高リスク状態であることを示す調査結果について述べる。

(1) 初期設定パスワードのままでの運用

2018 年 4 月、千葉県八千代市は、同市上下水道局が八千代 1 号幹線沿線に設置した水位監視カメラへの不正アクセスが判明したと報告した[※128]。設置した 3 台のうち 2 台がインターネット経由で不正アクセスを受けてシステムが改ざんされ、ホームページ上で公開しているカメラ画像に、日時と「I'm hacked. bye2」の文字が表示される状態となった（図 3-2-4）。監視カメラにはパスワードが設定されていたが、侵入時に変更されて制御不能となり、同市は画像の公開を停止した。

同月、埼玉県上尾市は、同市河川課が芝川都市下水路鎌倉橋に設置した河川監視カメラへの不正アクセスが判明したと報告した[※129]。八千代市の事件と同様に、インターネット経由で侵入され、カメラ画像の改ざんとパスワード変更による制御不能攻撃を受けたため、カメラ画像の公開は停止された。

2018 年 5 月、全国各地で 60 台以上のキヤノン株式会社製の監視カメラが不正アクセス被害を受けていると報道された[※130]。

八千代市と上尾市の事件において、監視カメラのパスワードは初期設定値のままであったと報じられている。なお、キヤノン株式会社は 4 月 26 日の時点でパスワードの変更等の不正アクセス防止対策を呼び掛けている[※131]。

■図 3-2-4　改ざんされた水位監視カメラの画像例
（出典）八千代市より提供

2018 年 11 月、神戸市東灘区の就労支援施設の監視カメラ映像記録装置や、千葉県八千代市の水位監視カメラ 2 台に不正アクセスしたとして、神戸市在住の男性が電子計算機損壊等業務妨害の疑いで逮捕された※132。2018 年 12 月、神戸地方検察庁は男を不起訴処分とした※133。

(2) 脆弱性を有する IoT 機器の流通

2018 年 4 月、世界中の様々な地域の Amazon で販売され、日本でも広く利用されている IoT 機器を調査した結果、調査時点で脆弱性を有する製品（表 3-2-9）が販売されていることが報告された（各脆弱性は現時点で修正済み）※134。

(3) 重要インフラ等で利用される IoT 機器の不適切な設定

2018 年 7 月、総務省は、一般社団法人 ICT-ISAC、国立大学法人横浜国立大学等と連携して、重要インフラ等で利用される IoT 機器を中心として行った IoT 機器の実態調査結果を公開した※135。報告によると、脆弱な重要 IoT 機器（消費電力監視装置、水位監視装置、防災設備制御装置、ガス観測警報通知装置等）を 150 件検出し、内 27 件で適切なパスワード設定がされていなかった。また、9 件で適切なパスワード設定はされているが、認証画面がインターネット上に公開されていた。当該機器の所有者等にヒアリング調査結果を実施した結果として、以下を挙げている※136。

- 関係者（所有者、利用者、運用者、導入者、製造者）の脅威に対する認識が不十分、または認識の共有が不十分
- 多様な関係者間の責任の所在が不明確

3.2.3 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 を取り巻くセキュリティ脅威は更に増大している。国内で脆弱な IoT 機器が流通し、多くの機器がウイルス感染の危機に晒されており、抜本的な対策を進める時期が来ている。本項では、対策を検討・推進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

2018 年以降も、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、あるいは新たに発行されたガイドライン等が公開された。2018 年以降に国内及び海外で公開された資料を、表 3-2-10 と表 3-2-11（次々ページ）に示す。

(2) IoT 機器調査及び利用者への注意喚起の取り組み

2019 年 2 月、総務省及び NICT は、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE（National Operation Towards IoT Clean Environment）※153」を開始した※154。インターネット上の IoT 機器に、容易に推測されるパスワードを入力すること等により、悪用の対象となる機器を調査し、当該機器の情報をインターネット接続事業者に通知する。接続事業者は、機器の利用者を特定し、注意喚起を行う（NOTICE の詳細については「2.1.3 (1) (a) 脆弱性対策に係る体制の整備に向けた主な取り組み」参照）。

No.	ベンダ	モデル	デバイス種別	脆弱性の種類	RCE脆弱性有無
1	Belkin International, Inc.	NetCam HD+ WiFi Camera	ネットワークカメラ	SSRF（Server Side Request Forgery：サーバサイドのリクエストフォージェリ）、LCE（Local Code Execution：ローカルコード実行）	有
2		WeMo® LED Lighting Starter Set	スマート電球	不正な SYSEVENT サービス	有
3		すべての WeMo® 製品	各種 IoT 機器	DoS（Denial of Service：サービス拒否）	無
4	株式会社バッファロー	WSR-300HP	ルータ	コマンドインジェクション	有
5	D-Link	DCS825L EyeOn Baby Monitor	ベビーモニタ	コマンドインジェクション	有
6				スタックオーバーフロー	有
7	Dahua Technology Co., Ltd.	ネットワークカメラ及び PTZ カメラ（他社への OEM 製品を含む）	ネットワークカメラ	予測可能な復旧用パスワード	無

■表 3-2-9　脆弱性を有したまま販売されていた IoT 機器の例
（出典）Trend Micro Incorporated「Device Vulnerabilities in the Connected Home: Uncovering Remote Code Execution and More※134」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
IPA	IoT 製品・サービス脆弱性対応ガイド※137	・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
	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※138 第 2 版	・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 開発におけるセキュリティ設計の手引き※139（2019 年 4 月版）	・開発者 ・具体的な設計手法	2019 年 4 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（Japan Network Security Association：JNSA）	IoT セキュリティガイド 標準／ガイドライン ハンドブック 2017 年度版※140	・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
JPCERT/CC	工場における産業用 IoT 導入のためのセキュリティ ファーストステップ ～産業用 IoT を導入する企業のためのセキュリティガイド～※141	・導入者（経営者、現場担当者）、構築請負者 ・基本的考え方、具体的手法	2018 年 8 月
一般社団法人重要生活機器連携セキュリティ協議会※142（Connected Consumer Device Security Council：CCDS）	IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）	・セキュリティ基準や検証スキームの検討者 ・最低限守るべき要件	2018 年 11 月
	製品分野別セキュリティガイドライン _ スマートホーム編 _Draft 版	・スマートホームの設計者、生産・施工者、現場監督者、運用保守担当者 ・設計から施工までに考慮すべき設計・開発プロセス	
	IoT システム調達のためのセキュリティ要件フレームワーク　概要	・IoT 機器の製造者、調達者 ・フレームワークの概要	
一般社団法人日本スマートフォンセキュリティ協会（Japan Smartphone Security Association：JSSEC）	JSSEC IoTセキュリティチェックシート 第二版※143	・IoT を利用・導入する一般企業 ・検討・考慮すべき項目	2019 年 2 月

■表 3-2-10　2018 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
NIST （National Institute of Standards and Technology）	NISTIR 8228 (DRAFT): Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ※144	・IoT 機器の導入に伴うサイバーセキュリティとプライバシーのリスク管理担当者 ・リスクを低減するための対策例	2018 年 9 月
	NISTIR 8200: Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) ※145	・IoT セキュリティ標準の開発者 ・5 種類の適用例に対するセキュリティの目的・リスク・脅威の分析、IoT セキュリティの標準化状況	2018 年 11 月
	DRAFT Considerations for a Core IoT Cybersecurity Capabilities Baseline ※146	・IoT 機器の製造者、ベースラインを開発するコミュニティ ・IoT 機器のセキュリティ機能のコアとなるベースライン候補	2019 年 2 月
OWASP （Open Web Application Security Project）	Internet of Things (IoT) Top 10 2018 ※147	・製造者、開発者、利用者 ・10 大脆弱性の概要	2018 年 12 月
ENISA （European Network and Information Security Agency）	Towards secure convergence of Cloud and IoT ※148	・クラウドを利用する IoT 開発者とインテグレータ、クラウドサービス提供者 ・IoT とクラウドの融合によるセキュリティ上の課題と対策	2018 年 9 月
	Good Practices for Security of Internet of Things in the context of Smart Manufacturing ※149	・産業 IoT の運用者･ユーザ、製造者･ベンダ ・産業 IoT のセキュリティ対策指針	2018 年 11 月
	IoT Security Standards Gap Analysis ※150	・IoT セキュリティ標準の開発者 ・セキュリティ要件と標準の対応	2019 年 1 月
Department for DCMS（Digital, Culture, Media & Sport）, UK	Code of Practice for Consumer IoT Security ※151	・開発者、製造者、販売者 ・実践すべきセキュリティ対策	2018 年 10 月
German Federal Office for Information Security（Bundesamt für Sicherheit in der Informationstechnik：BSI）	BSI TR-03148: Secure Broadband Routers Version 1.0 ※152	・製造者、販売者、利用者 ・ルータのセキュリティ要件	2018 年 11 月

■表 3-2-11　2018 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

COLUMN

Miraiの作成者の末路

2018年9月、IoT機器を攻撃対象とした2種類のボットネット（MiraiとClickdraud）を作成・運用したとして、20代の男性3名に判決が下されました[i]。彼らは2017年12月に罪状を認めて有罪判決を言い渡されていました[ii]が、その後、複数のサイバーセキュリティに関する捜査において連邦捜査局（FBI）に協力していたそうです。具体的な内容を示す文書等はありませんが、「memcached（分散型メモリキャッシュシステム）を悪用したDDoS攻撃」「クリスマスに発生するDDoS攻撃」「VPNFilterのボットネット」への捜査協力だったと考えられています[iii]。これらの捜査への貢献が評価され、この度の判決では禁固刑はなく、5年間の保護観察処分、2,500時間の社会奉仕活動、12万7,000ドル（約1,400万円）の賠償金支払い、今後の捜査協力等の義務が命じられました。

3名のうち2名はDDoS攻撃対策サービスを提供する会社の共同創始者であり、その1名は自身の通う大学のネットワークに対して執拗にDDoS攻撃を仕掛け、自分達の会社のサービスを利用させようとしていたと見られています[iv]。この件については、別途、2018年10月に判決が下され、860万ドル（約10億円）という巨額の賠償金の支払いと6ヵ月間の自宅での拘禁及び奉仕活動が命じられました[v]。かつて、英国で報酬を得るために放火をしていた消防士が逮捕されています[vi]が、このような自分勝手な行為は許されるものではなく、上記の異なる判決の賠償金額の違いからもいかに悪質な行為であったかが推測されます。

なお、彼らが公開したMiraiのソースコードを元に亜種を作成し、日本国内にも多くの感染被害を与えたSatoriの作成者も起訴・逮捕・収監されています[vii]。

情報セキュリティの専門家を志す者は、ウイルスや脆弱性情報等について深く学ぶ必要がありますが、その過程で得た知識や技術は安全なIT社会の実現のために使うべきです。Miraiの作成者と同じ末路とならないよう、情報セキュリティの専門家には自分を律する強い意志や倫理観が求められます。

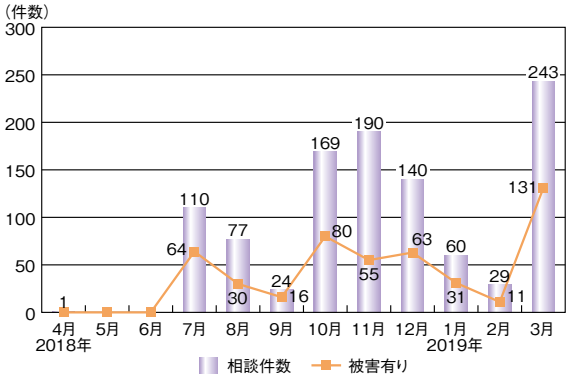
i U.S. Department of Justice：Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybercrime Investigations https://www.justice.gov/usao-ak/pr/hackers-cooperation-fbi-leads-substantial-assistance-other-complex-cybercrime〔参照 2019-06-11〕
ii U.S. Department of Justice：Justice Department 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 2019-06-11〕
iii ZDNet：Mirai botnet authors avoid prison after "substantial assistance" to the FBI https://www.zdnet.com/article/mirai-botnet-authors-avoid-prison-after-substantial-assistance-to-the-fbi/〔参照 2019-06-11〕
iv Krebs On Security：Mirai IoT Botnet Co-Authors Plead Guilty https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/〔参照 2019-06-11〕
v U.S. Department of Justice：Computer Hacker Who Launched Attacks On Rutgers University Ordered To Pay $8.6m Restitution; Sentenced To Six Months Home Incarceration https://www.justice.gov/usao-nj/pr/computer-hacker-who-launched-attacks-rutgers-university-ordered-pay-86m-restitution〔参照 2019-06-11〕
vi excite ニュース：パート消防士が放火「出動すれば金になる」（英）https://www.excite.co.jp/news/article/Techinsight_20160106_220174/〔参照 2019-06-11〕
vii Daily Beast：Newbie Hacker Fingered for Monster Botnet https://www.thedailybeast.com/newbie-hacker-fingered-for-monster-botnet〔参照 2019-06-11〕
ZDNet：Satori botnet author in jail again after breaking pretrial release conditions https://www.zdnet.com/article/satori-botnet-author-in-jail-again-after-breaking-pretrial-release-conditions/〔参照 2019-06-11〕

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）の利用者を狙う手口は巧妙化を続けている。本節では、巧妙化する手口とその対策を紹介する。

3.3.1 宅配便業者を装う不在通知SMSの手口

2018 年 7 月、「宅配便業者から不在通知を連絡する SMS（ショートメッセージ）を受信した」ことに関する相談が IPA に寄せられた。同様の相談は 2018 年 1 月から寄せられていたが、7 月以降相談件数が急増し（図 3-3-1）、その手口にも変化が見られた※155。また、12 月からは佐川急便株式会社だけでなく、ヤマト運輸株式会社を装った SMS についての相談も寄せられた※156。更に、3 月からは「構成プロファイルに関する許可を求めるようなメッセージが表示された」という相談も寄せられた※157。



■図 3-3-1　宅配便業者を装う不在通知 SMS の手口に関する相談件数

受信した SMS 内の URL にアクセスすると、実際の宅配便業者のホームページを装う偽サイトにつながるが、端末が Android 端末であるか iPhone であるかで手口が分かれる。以下ではそれぞれの手口について解説する。

(1) Android 端末でアクセスした場合の手口

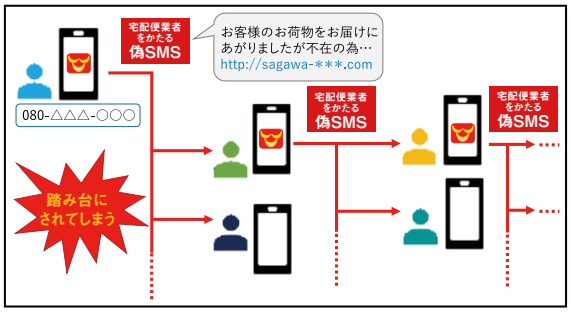
Android 端末で、宅配便企業を装う偽サイトにアクセスすると、「sagawa.apk」「koyamato.apk」等の Android 端末にアプリをインストールするためのファイルが自動的にダウンロードされる仕組みとなっている（図 3-3-2）。偽サイトの下部には当該ファイルでアプリをインストールする手順が画像付きで説明されている。記載された手順に沿って操作をすると、不正アプリがインストールされる。

この手口は 2018 年 1 月から確認されていた※158 が、

■図 3-3-2　Android 端末で偽サイトにアクセスした場合の画面例
（出典）IPA「安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に※156」

7 月以降はこの不正アプリをインストールした Android 端末から、不特定多数の宛先（登録されているアドレス帳にはない電話番号）に SMS が勝手に送信されるという挙動が見られるようになった。

SMS は自身が受信したものと同様の不在通知をかたった内容であり、Android 端末の電話番号を発信者として送信される。不正アプリをインストールした Android 端末が踏み台とされ、宅配便業者を装う不在通知 SMS が拡散されることとなる（図 3-3-3）。そのため、「アプリを入れてから、見知らぬ番号から『宅配便業者さんですか?』という問い合わせの電話がくるようになった」という相談も寄せられている。

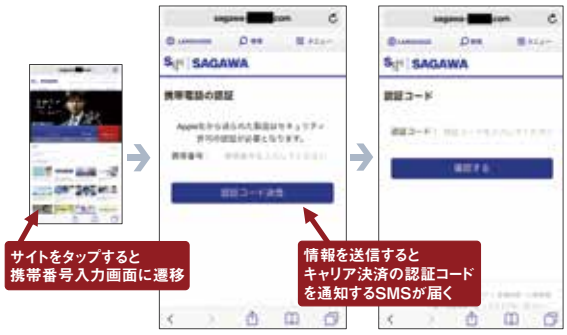


■図 3-3-3　Android 端末が SMS 拡散の踏み台にされる被害のイメージ

(2) iPhone でアクセスした場合の手口

iPhone で、宅配便業者を装う偽サイトにアクセスすると、携帯通信会社（以下、キャリア）決済の認証情報を

狙った偽サイトが表示される。下記の図 3-3-4 に示す流れに従って画面が遷移する。携帯番号入力画面で電話番号を送信すると、キャリア決済の認証コードを通知するSMSが届き、認証コード入力画面で届いた認証コードを送信してしまうと不正にキャリア決済をされてしまう。



■図 3-3-4　iPhone で偽サイトにアクセスした場合の画面例①
（出典）IPA「安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に」

また、Apple ID の ID・パスワードを狙った偽サイトに誘導されるケースもある（図 3-3-5）。寄せられた相談の中で実際の被害事例は確認されていないが、もし、ID・パスワードを入力してしまった場合は、Apple ID への不正ログイン被害に遭う可能性がある。Apple ID の情報を入力した場合、パスワードの変更が適切な対処となる。

ただし、Apple ID は「2 ファクタ認証」という 2 段階認証サービスが提供されており、現在では設定が必須となっている。2 ファクタ認証を設定している場合、パスワードが詐取されたとしても、所有する iPhone 上で表示される 6 桁の認証コードが正しく入力されない限り、Apple ID が不正ログインされることはない。

なお、2019 年 3 月からは「構成プロファイル※159」をインストールさせようとする手口（図 3-3-6）も確認されている。構成プロファイルをインストールしたことによる具体的な被害の影響範囲は確認できていないが、構成プロファイルをインストールした場合、自動的に Apple ID を狙ったフィッシングサイトに誘導（ブラウザアプリが起動し、当該サイトに接続）される挙動を確認している。

■図 3-3-6　iPhone で「構成プロファイル」をインストールさせる手口
（出典）IPA「安心相談窓口だより　宅配便業者をかたる偽ショートメッセージで、また新たな手口が出現」

■図 3-3-5　iPhone で偽サイトにアクセスした場合の画面例②
（出典）IPA「安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に」

(3) Android 端末における対策と対処

「3.3.1（1）Android 端末でアクセスした場合の手口」で確認された不正アプリは公式マーケットである Google Play 上には配信されておらず、Google の管理外の場所からダウンロードされる。そのため、公式マーケット以外からアプリをインストールしないように心がけることが重要である。また、Android 端末のセキュリティ設定で、「提供元不明のアプリ」をオフにすることを推奨する。設定をオフにしていると、インストールしようとすると警告が表示されるため、インストールへ進まずその場でキャンセルすることができる。

なお、本手口では、不正アプリのインストールへ誘導するため、偽サイト上に当該設定をオフにする画像付きの手順が掲載されているが、その手順に従わないように注意する必要がある。実際にこれを宅配便業者が公式に掲載した手順であると勘違いして、手順を実施して被害に遭った相談も確認されている。

もし、不正アプリをインストールしてしまった場合は、以下の対処を順番にすることを推奨する。

①スマートフォンを機内モードにする

機内モードによって通信を停止させることで、それ以降は不正アプリによる SMS の拡散や当該スマートフォン内の情報の外部送信を防ぐことが可能である。

②不正アプリをアンインストールする

不正アプリはホーム画面上には表示されないが、「設定」画面の「アプリケーション」の一覧で確認できる。

例えば「佐川急便」といった名前で表示されるため、見分けるのが難しい場合があるが、インストールした日付から不正アプリを特定することができる。不正アプリを削除すれば、以降は機内モードをオフにしても、SMS を拡散されたりすることはなくなる。アドレス帳等のバックアップを取得したい場合は、アンインストール後であれば安全に行うことができる。

③スマートフォンを初期化する

不正アプリをインストールしてしまったことによる、スマートフォン本体への影響は不明である。より安全な対処として初期化を推奨する。

④アカウントのパスワードを変更する

初期化後、安全のため、Google アカウントや利用している SNS 等のサービスに登録しているアカウントのパスワードを変更することを推奨する。

なお、不正アプリにより、キャリア決済を悪用されたと考えられる被害が確認されている。IPA に寄せられた相談でも「3 万円の iTunes カードを購入されていた」といった被害報告が複数あった。そのため、上記に加え、不審なキャリア決済の利用がないか確認することも推奨する。もし、不審な利用が確認された場合は、キャリアに相談していただきたい。また、キャリア決済をあまり利用しないのであれば、本手口に限らず不正なキャリア決済をされた際の被害を低減できるため、予防策として限度額を最小限に設定しておくことも推奨する。

(4) iPhone における対策と対処

ID やパスワードの入力を促す偽サイトが表示された場合、情報を入力しなければ被害に発展することはない。そのため、「3.3.1(2)iPhone でアクセスした場合の手口」で誘導されたのであれば、本物に酷似した画面であっても安易に情報を入力しないことが重要である。偽サイトかどうかを見極めるポイントとしては、Web サイトの URL に着目するとよい。偽の Web サイトであるため、公式サイトとは URL が違っていることが確認できる。また、公式サイトを利用する場合は、事前にブックマークに登録しておき、SMS 等で送られてきた URL ではなく、ブックマークから公式サイトを開くようにすれば、偽サイトにアクセスすることはなくなる。もし、公式アプリがあれば、そちらを利用することを推奨する。

構成プロファイルは勝手にインストールされることはなく、利用者の許可が必要となる。プロファイルの利用目的等が明確でない場合は、無闇にインストールしないよう心がけることも重要である。もし、誤って構成プロファイルをインストールした場合、安全のため iPhone を初期化することを推奨する。具体的な影響範囲は不明ながらも、iPhone を初期化してから、Apple ID のパスワードを変更すれば、以降は安全に利用できるようになる。

携帯電話番号と認証コードを入力した場合（前ページ図 3-3-4）、キャリア決済を悪用され、金銭被害に至る場合がある。もしそれぞれの情報を入力した場合は、不審なキャリア決済の利用がないか確認することを推奨する。

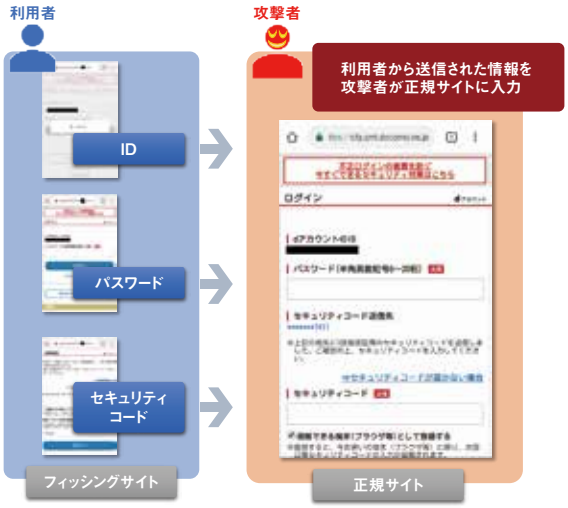
3.3.2 dアカウントを狙ったフィッシング

2018 年 12 月、IPA に「『お客様のキャリア決済に不正利用の可能性があります。ウェブページで検証おねがいします』という内容の NTT ドコモをかたる SMS が届き、偽の d アカウントのログイン画面に誘導された」という相談が寄せられた。アカウント詐取を狙った手口自体は多く確認されているが、この手口では2段階認証のセキュリティコードまで盗み取ろうとしていることが確認された（図 3-3-7）。

■図 3-3-7　d アカウントを狙ったフィッシングサイトの画面例

(1) d アカウントを狙ったフィッシングの手口

本手口では入力情報を自動的に収集したり、ログイン試行をしたりするのではなく、図 3-3-8 に示すとおり、リアルタイムで攻撃者が手動で不正ログインを試みている可能性がある。この偽サイトでは、ID やパスワードを入力して「次へ」のボタンをタップすると、「loading…」と表示されるが、この「loading…」は正規の d アカウントページで表示されることはない。d アカウントに 2 段階認証を設定していた場合、この表示の後に SMS で NTT ドコモから d アカウントの正規のセキュリティコードが届く。正規の d アカウントページでも ID を入力すると、SMS でセキュリティコードが届くため、同じ挙動をしているかのように見



■図 3-3-8　d アカウントを狙ったフィッシングのイメージ

える。

「loading..」の表示が消えると、パスワードの入力画面に移る。そこで d アカウントのパスワードを入力して、画面内のログインボタンを押すと、再び「loading…」と表示され、すぐにセキュリティコードを入力する画面となる。この流れにおいて、偽サイトと正規サイトに違いがあることが確認された。正規サイトでは、一つの画面内にパスワードの入力項目とセキュリティコードの入力項目がある。一方、偽サイトでは、パスワード入力とセキュリティコード入力で画面が別々になっている。なお、IPA では、登録のない d アカウント ID を入力すると、「ID またはパスワードが間違っている」と表示されることが確認された。このことから入力される情報を一方的に収集するのではなく、実在する d アカウントを選別して、より効率的に金銭等を窃取しようとしていることが考えられる。

(2) 被害と対処

偽サイトに、セキュリティコードまで入力してしまうと、結果として ID、パスワード、セキュリティコードを詐取される。そのため、2 段階認証を設定していた場合でも、d アカウントが乗っ取られてしまう。また、この手口ではセキュリティコードだけでなく、キャリア契約時に設定した 4 桁の暗証番号の入力も求められることが確認されている。この暗証番号を入力してしまい、詐取されると、d アカウントで利用できる各種サービスを悪用した被害に発展することが推測される。

IPA に寄せられた相談では、利用者の身に覚えのないキャリア決済による被害が確認された。また、d アカウントで利用できるドコモ口座からお金が不正送金されたという報告も寄せられた。d アカウントでは様々なサービスと連携できるため、被害の影響範囲は多大なものになることが推測される。もし偽サイトに情報を入力してしまったら、パスワードを変更することが必須である。また、不正なキャリア決済が発生していないか NTT ドコモのサポートに問い合わせることも推奨する。

(3) 対策

手口を知っておき、騙されないことが重要である。正規のログイン手順を把握しておき、その手順でだけログインするように心がけることを推奨する。事前にブックマークに登録しておいた URL を利用することで、SMS 等で送られてきた URL にはアクセスしないようにすることで被害を回避できる。また、正規のアプリがあれば、それを利用することも対策となる。

3.3.3 アプリ誘導

2018 年は「アプリ誘導」に関する相談件数が大きく減少した。

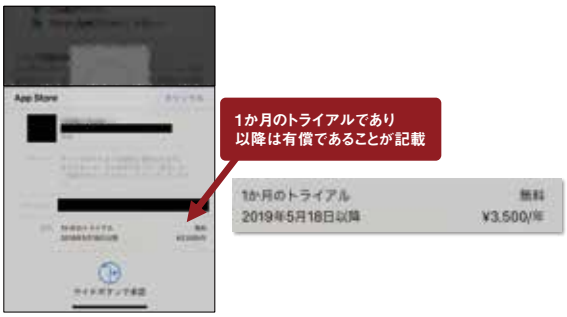
「アプリ誘導」とは、スマートフォンでインターネットを閲覧していると、突然ウイルス検出を知らせる警告と「今すぐ解決が必要」等のメッセージを表示させ、特定のアプリのインストールを促す手口である。偽の警告画面を表示させて利用者を誘導するという点で、「偽警告」や「偽セキュリティソフト」の手口と類似しているが、最終的にアプリをインストールさせることが目的であり、被害者から直接金銭を得ることが目的ではない点に違いがある（偽警告の詳細については「1.2.8(2) 偽のセキュリティ警告」参照）。

2018 年のアプリ誘導に関する相談件数は 92 件で、2017 年の 243 件と比較して半分以下となった。また、継続して iOS と Android 双方の利用者から相談が寄せられているが、全体の 70% は Android 利用者だった。

IPA の相談窓口で確認できている範囲では、誘導されるアプリのすべてが公式マーケット上にあるもので、中にはセキュリティベンダが配布している正式なセキュリティアプリもあった。また、偽のセキュリティ警告で誘導されるケースが多いためか、App Store 上のあるアプリでは「自社のアプリをインストールさせるための詐欺である」というレビューが多数投稿されているものもあった。

このような、公式マーケットで公開されている正式なセキュリティアプリに誘導されるケースから、不正アプリをインストールさせることではなく、多くの利用者にアプリをインストールさせることで 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。

上記の理由で、誘導されるアプリをインストールしたことで被害に至ることは考えにくいが、注意が必要となるアプリもある。初めの 1 ヵ月、あるいは 1 週間はお試し期間による無料であっても、その後継続して利用する場合は有料となるアプリに誘導され、インストールした場合は、気付かないうちに金銭被害が発生することがある。実際に一定期間経過後は費用がかかることを認識できておらず、請求が発生してから課金に気が付いたという相談も寄せられた。この種のアプリでは、インストール自体は無料であるため、インストール時に決済の認証画面は表示されない。インストールしたアプリを起動すると、無料お試し期間である旨のメッセージが表示されて、お試し期間が過ぎた後も利用する場合の価格情報と決済の認証画面が表示される（図 3-3-9）。例えば iPhone ならこの画面で Apple ID の認証を有効にすると、決済も完了することになる。



■図 3-3-9　決済の認証画面

これまでの手口と同じように警告を鵜呑みにしないことはもちろん、誘導されたアプリがどのようなものか公式マーケットに掲載されている説明文や開発元等の情報を確認することも重要である。アプリの利用規約でも、今後も無料のまま利用継続できるのか等を確認できるため、これらの情報からインストール可否を判断することを習慣とするのが望ましい。

3.3.4 公式マーケット上に配布された不正アプリ

2018 年も iOS や Android の公式マーケットである App Store 及び Google Play 上で、悪意のある機能を仕込まれた不正アプリが多数発見されている。

5 月にはゲームや教育アプリに偽装した 38 種の不正アプリが Google Play 上で発見され、1 万以上のデバイスにダウンロードされたと見られる※160。

8 月にはインストール画面に掲載されている説明どおりの機能は一切使えず、広告をポップアップで表示させるだけのアプリが Google Play 上に少なくとも 68 個確認された※161。

12 月には、Google Play 上に音声アプリに偽装した不正アプリが確認された。このアプリをインストールすると、Android の既定ブラウザである Chrome 上に偽のアンケートフォームが表示され、名前や電話番号といった個人情報を入力させるようになっていた※162。

2019 年 1 月には、執拗に広告を全画面に表示させる不正なアプリが Google Play 上で 85 個確認された。これらは合計約 900 万回ダウンロードされていた※163。このアプリを起動しても、アプリの説明どおりの機能は使えず、広告だけが表示され、最終的にホーム画面上から見えなくなり、バックグラウンドで動き続けるようになる。バックグラウンドで動き続けた後も、Android 上に全画面広告を定期的に表示させる。

また、同月にモバイルバンキングを狙うウイルス「Anubis」をインストールさせる不正アプリが確認された※164。この不正アプリは、スマートフォンのモーションセンサーを感知することで動作する仕組みになっている。通常、サンドボックス環境※165 にはモーションセンサー※166 はないため、モーションセンサーが感知できなかった場合、自身の動作を止めることで、サンドボックス環境を回避することが、この仕組みの目的と考えられる。モーションセンサーを感知すると Android のシステム更新プログラムと偽って Anubis のインストール画面を表示する。Anubis はキーロガーやスクリーンショットを取得する機能を持っていて、オンラインバンキングの認証情報を窃取する。

また、2018 年 12 月に iPhone の指紋認証（Touch ID）を利用して、アプリ内課金を騙し取るアプリが確認された※167。このアプリは心拍数を計ると称して、iPhone のホームボタン上に指を置くように指示してくる。ユーザがこの指示に従って、Touch ID に登録した指を置くと、89.99 ドルのアプリ内課金を承認してしまうことになる。現在、この心拍数計測アプリは App Store 上から削除されている。

2018 年度は情報を窃取する不正アプリだけでなく、広告を執拗に表示するもの、騙して課金させるもの等、多様な手口で金銭を狙うアプリも多く見られた。このような被害を回避するために、アプリをインストールして利用する際は、開発元の信頼性やアプリの機能、利用規約等を慎重に確認する必要がある。

3.4 ITサプライチェーンのセキュリティ

多くの企業では、IT システム・サービスに関する業務を系列企業やビジネスパートナー等に外部委託しており、「サイバーセキュリティ経営ガイドライン※168」においても、自社だけでなくビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策の必要性が強調されている。

本節では、IT システム・サービスの企画・設計・製造・運用・保守・利用・提供等のプロセスを複数の組織で分担し、一連の流れとして活動する形態である IT サプライチェーンについて、そのセキュリティ脅威、インシデント、政府の施策、企業の対策の実態を述べる。

なお、本白書では IT サプライチェーンのセキュリティを初めて個別テーマとするため、2018 年以前に発生、発表されたインシデントや施策、実態調査結果等の情報についても取り上げている。

3.4.1 インシデント、被害の事例

サプライチェーンは、委託元と委託先だけでなく、再委託先、再々委託先と、ある目的を達成するために必要となる取引関係が連鎖することから、その一連のつながりのどこかに問題が発生すると、何らかの影響が複数の組織に波及する恐れがある。その影響を最小化するために、リスクを制御し、目的達成のために取り組まれる活動がサプライチェーンリスクマネジメントである。

同じ企業・グループであれば、セキュリティガバナンスにより、セキュリティポリシーに従った対策の実施、管理を徹底できる。しかし、同じ企業・グループではない取引先は、セキュリティガバナンスがきかない等で、セキュリティ対策が弱い場合があり、そこが狙われる可能性がある。その結果、情報漏えいやシステム停止といったインシデントが実際に発生している。表 3-4-1 に、インシデントの発生等で問題となる IT サプライチェーンの主なリスク分類を示す。

不正アクセス	取引先を踏み台とする攻撃や取引先になりすます攻撃
	調達する製品・システムへの不正プログラム等埋め込みによる攻撃
過失	開発時の対策不備
	運用時の対策不備
内部不正	開発・保守・運用担当者による不正
	ルール・規範を逸脱した取り引き

■表 3-4-1　IT サプライチェーンでのインシデントの起因別分類

(1) 不正アクセスに起因するインシデント

不正アクセスにより、システムの乗っ取り、情報の改ざん、窃取した情報を悪用して行われるインシデントは、取引先を踏み台とする攻撃や取引先になりすます攻撃と、調達する製品・システムへの不正プログラム埋め込みによる攻撃等が挙げられる。

(a) 取引先を踏み台とする攻撃や取引先になりすます攻撃

取引先を踏み台とする攻撃や取引先になりすます攻撃は、ターゲットとなる企業を直接狙うのではなく、ターゲット企業と取り引きや関連があるサプライチェーン上の企業を狙い、不正アクセス等によって、システム・ネットワークの情報やアカウント情報、メールのやり取り等の情報を窃取し、ターゲットへの攻撃材料や、侵入の踏み台とする。外部からの攻撃には十分な対策を取っている企業でも、取引先からのアクセスやメールは問題ないものと判断してしまう可能性が高まる。

実際、取引先を装い、指定口座への振込等を促すビジネスメール詐欺による被害も多数発生している（「1.2.2 ビジネスメール詐欺（BEC）」参照）。2017 年 9 月には、日本航空株式会社（以下、JAL）が米国の金融会社になりすました攻撃者から航空機リース料（約 3 億 6,000 万円）の被害に遭った※169。偽メールのメールアドレスは正規のものと 1 文字違いで、画面上は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、送信先が偽の口座に変更された PDF ファイルが添付されていた。JAL では、再発防止策として、JAL グループ内の情報共有と口座情報確認や登録手続きの厳格化を行った。

(b) 調達する製品・システムへの不正プログラム埋め込みによる攻撃

調達する製品・システムへの埋め込みによる攻撃は、IT 機器やプログラムに不正部品や不正なプログラムを埋め込み、正規の配信サービスやアップデート機能を悪用し、配布対象となる端末をウイルス感染させたり、バック

ドアを設置したりするものである。

2018 年 7 月には、韓国の法人組織を標的とした「Red Signature 作戦」が確認された。これは遠隔支援ツールプロバイダの電子証明書を窃取し、更新サーバをハッキングし、標的とした IP アドレスが範囲内のユーザの更新要求に対して不正なファイルを送信するというものであった※170。

2019 年 3 月には ASUS Live Update Utility のユーザを標的とした「ShadowHammer」という攻撃が報告された。同ユーティリティは BIOS、UEFI、ドライバー、アプリケーションの自動アップデートのために、ASUSTeK Computer Inc. 製の最新のパソコンの大部分にプリインストールされている。攻撃者は、攻撃対象を数百人のユーザに絞り込み、標的となったデバイス上で実行された場合のみ、次のステージのウイルスをダウンロードする仕組みとなっていた。このようにして標的を絞り込むことにより、検知されにくくなり、より高い精度で攻撃することが可能であったと考えられている※171。

(c) 対策

不正アクセスは、高度な攻撃が次々と発見されており、完全に防止することは難しい。自社が踏み台やなりすましに利用されないように基本的な対策を実施することは必要であるが、サプライチェーンにおける対策として、サプライチェーン上の企業間での最新攻撃情報の共有や、重要な情報に関する管理施策の明確化・共有等の協力や連携により被害を最小限にする努力が必要である。

(2) 過失に起因するインシデント

人が介在することにより発生してしまう事件や事故は、あらゆる分野で起きているが、セキュリティの場合は、一般に専門知識がない、動機づけが弱い（必要性は分かるが仕事の手間が増える）、人手が足りない等で、間違いや不徹底により被害を大きくしてしまうことがある。

(a) 開発時の対策不備

製品やシステムを開発する際に、セキュリティの脆弱性対策が実装されず、検査においてもセキュリティが確保されているか確認されずに出荷されてしまうことがある。稼働後も脆弱性が放置された状態だった場合、攻撃を受けインシデントが発生することがある。

2011 年にはインテリア通販サイトが SQL インジェクション攻撃を受け、クレジットカード情報が漏えいした。契約時点で既に IPA が SQL インジェクション攻撃に対する注意喚起、及び対応方法を公開していた※172 が、ユーザからの要件には対策が含まれておらず、ベンダからも対策の提案はされなかった。この事例では訴訟においてベンダの過失が認められた※173。

(b) 運用時の対策不備

2012 年 6 月、クラウドサービス事業者であるファーストサーバ株式会社で大規模なデータ消失事故が発生した。本番環境、検証環境、バックアップ環境も含めてすべてのデータが消失し、多くの企業に影響があった。原因は、社内マニュアルに従わずに実施されたシステムメンテナンス作業によるものであった※174。

2017 年には、B.LEAGUE のチケットサイト、ファンクラブ受付サイトの委託を受けていたぴあ株式会社が Apache Struts2 の脆弱性を悪用した攻撃が行われ、個人情報、クレジットカード情報等が再委託先から漏えいしたことを報告した※175。このインシデントでは、保管してはならないと発注仕様や運用ガイドラインに定めていた情報が再委託先のデータベース、通信ログに残っており、このことを委託先は把握しておらず、確認の徹底が不十分であったことが本質的な原因だったと報告している。

2018 年 3 月、前橋市学校教育ネットワークシステムの公開用サーバへの不正アクセスが確認され、児童、生徒及び保護者の個人情報が流出した可能性が高いことが報告された（「1.2.9 情報漏えいによる被害」参照）。この公開用サーバは、委託先事業者のデータセンターに移設されていたが、データセンター移管業務は物理的移設のみで、運用は含まれていないという委託先の認識であった。しかし、この認識は委託元の管理者には十分に周知されておらず、バーションアップが必要という認識がなかった。移設後は、サーバへの追加、変更、確認が行われず、多くの脆弱性を抱えたまま運用された結果、脆弱性が利用されてバックドアが作られた。このインシデントの背景には、教育委員会、市、委託事業者等関係者全体のシステム及びセキュリティに対する理解不足があったと検証報告書では述べられている※176。

不正アクセスによって発生した情報漏えい等の事案として、EC サイトや会員用 Web サイトにおける事案が多く報告されており、2018 年 6 月、個人情報保護委員会では、Web サイトの運営事業者向けの注意喚起を行っている※177。

(c) 対策

人が介在する事故や事件の原因には、実作業での

うっかりミスに加え、ユーザとベンダの間の認識のずれが起因していることがある。契約時点では、業務知識やセキュリティ技術の専門知識の有無からこのずれは大きいことがあるが、双方が対象とするシステムやサービス、取り扱う情報の重要度、想定されるリスク等について情報を共有し、協力しあうことにより、ずれを小さくすることが期待できる。更に、委託先に「お任せ」ではなく、委託元も遂行状況を確認することや委託先が専門家としてセキュリティの脅威や脆弱性について委託元に報告し、協力して対策を検討することにより、リスクを低減することが推奨される。

製品・システムのセキュリティ対策は、運用後の対策も含めた包括的なものになるよう設計段階から配慮する、セキュリティ・バイ・デザインの設計思想が重要視されている。ユーザ企業の場合、セキュリティの専門知識を有する人材は限られており、セキュリティ対策についてもベンダの協力が必要となることが多い。ベンダは、ユーザ要件に応じたセキュリティ提案を行い、設計・製造・検査の各々の段階で考慮できているか、実装できているか確認することが望ましい。

ソフトウェアの脆弱性については、開発時点で既知のものは対策をとり、検査等により確認を行う。未知の脆弱性は、公開後速やかに対処することが望まれるが、ゼロデイ攻撃等のように対処をする前に攻撃されたり、稼働中のシステムを停止することができなかったりといった課題がある。脆弱性が発見された場合の情報共有や対処については、企業間であらかじめ取り決めておくことが速やかな対応のためには重要である。また、被害を最小にするために、情報の機密レベルに応じた保管場所を決定し、保管場所以外にデータが残されていないことを委託元が監査、あるいは委託先が確認し、委託元に報告することが望ましい。

JPCERT/CC では、委託元と委託先で Web サイトを管理する場合に、互いに相手が管理していると誤認してセキュリティパッチが未適用、アップデート未実施といった状態にならないよう、注意喚起を行っており、年 1 回程度（契約更新時等）、及び機能追加等の変更が行われたときは、委託契約の内容確認をするよう推奨している※178。

(3) 内部不正に起因するインシデント

内部不正に起因するインシデントとして、委託先等の開発・保守・運用担当者が委託元の環境内で不正を行う場合と、法律や契約により禁止、あるいは事前の許諾が必要とされている再委託を行った事案について述べる。

(a) 開発・保守・運用担当者による不正

開発・保守・運用の業務を委託された企業の担当者が、不正に情報を窃取したり、悪用したりしてインシデントが発生することがある。

2014 年 2 月、株式会社横浜銀行の保守管理業務を請け負っていた再委託先の元社員が顧客のカード情報を不正に取得しキャッシュカードを偽装したとして逮捕された。この元社員は長年同一業務に携わり、システムに係る権限が集中していた※179。また、2014 年 7 月には、株式会社ベネッセコーポレーションで国内史上最大の個人情報漏えい事故が発生した※180。原因は、グループ会社が運用の業務委託をした元社員による金銭目的の内部不正だった。

(b) ルール・規範を逸脱した取り引き

法律や契約で禁止された取り引きが行われ、問題となることがある。

2018 年 3 月、日本年金機構からデータ入力を委託された情報処理会社が、日本年金機構の契約に反して中国の関連会社に再委託を行っていたことが公表された※181。2019 年 1 月には、埼玉県のある事業者が自治体の許諾を得ないまま特定個人情報のデータ入力業務を再委託していたことが判明した。その原因は受託手続きの失念または許諾書面の一部不備と報告されている※182。

マイナンバー等の特定個人情報の取り扱いは「行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）」により定められ、無断再委託は禁止事項に抵触する行為である。個人情報保護委員会は、2019 年 2 月に特定個人情報の取り扱いの委託における注意喚起を行った※183。

(c) 対策

内部不正は組織内部者の不正行為を指すことが多いが、開発、保守や運用等の業務委託では、委託元の組織内に委託先、再々委託先等の作業者が常駐して作業することも多く、組織内部者と同様の対策が有効であることも多い。IPA では、業務委託を行う場合の対策を含む「組織における内部不正防止ガイドライン」を発行し、対策の実施を促している※184。

再委託に関する条項が契約書に含まれることは珍しくはなくなった。しかし、契約の事務手続きを取りまとめる部門があったり、直接の交渉を営業部門が行ったりして

いる場合は、具体的にどのように記述されているか現場担当者が理解しないまま契約が締結される恐れがあり、注意が必要である。委託先では社内監査や点検時に契約遵守状況を確認することが望ましい。委託元では、契約にあたり、体制やインシデント発生時のエスカレーション等の取り決めを現場担当者同士で確認する際に、再委託先についても確認することが望ましい。

3.4.2 国内の政策動向

IT サプライチェーンリスクマネジメントに関しては、前述のように取引先からの個人情報漏えい事案が顕在化した 10 年以上前からその重要性が指摘されている。近年では省庁等に対するサイバー攻撃が増加していることも踏まえ、国家安全保障上の観点からも IT サプライチェーンリスクへの対応が重視されている。以下に国内の政策動向として、検討の状況やガイドラインの策定等について述べる。

(1) サプライチェーン対策の必要性

「サイバーセキュリティ戦略」では、「Society 5.0」の実現に向けて、サプライチェーンはより多様化することが見込まれており、サプライチェーン上で発生したセキュリティの問題が経済社会全体に広く波及し、甚大な悪影響を及ぼす恐れがあることから、サプライチェーンを俯瞰した取り組みを推進することが不可欠である※185、と述べられている（サイバーセキュリティ戦略については「2.1.1 政府全体の政策動向」参照）。

経済産業省では、2007 年度から情報セキュリティガバナンスの確立・普及のための施策に取り組んでおり、2015 年には、企業が IT の利活用を推進していく中で、経営者が認識すべきサイバーセキュリティに関する 3 原則や、経営者のリーダーシップによって取り組むべき 10 項目を「サイバーセキュリティ経営ガイドライン」の中で策定している。同ガイドラインではサプライチェーン全体を視野に入れた取り組み、体制の整備を求めており、「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」等がチェック項目に含まれている。なお、本ガイドラインは 2017 年に Ver 2.0 に改訂されている。

経済産業省は更に、Society 5.0 におけるサプライチェーン全般のセキュリティ強化に向け、産業サイバーセキュリティ研究会を立ち上げ、制度、経営、人材、ビジネス等に関する検討を開始した。このうち WG1 においては、IT、OT を統合したサプライチェーン全体のセキュリティリスクを洗い出す枠組みとして、「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進めている（「2.1.2 経済産業省の政策」参照）。

また、NISC では 2016 年に国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みとして定めた「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※186」において、外部委託の実施に際して、情報セキュリティ対策を実施することを委託先選定条件とし、仕様内容にも含めるよう規定している。

このように、我が国の政策としてサプライチェーン対策の必要性が明確に規定され、組織においてはトップダウンで対策の検討と実施が求められている。

(2) サプライチェーンのガイドライン

IT サプライチェーンのリスク対策の必要性に伴い、各省庁が策定している具体的な対策のガイドラインや基準を以下に示す。

経済産業省では、企業が業務委託を行う際に、計画、実行・評価、改善の各プロセスに沿ってリスク管理体制を構築・実施するためのガイダンスとして、2009 年に「アウトソーシングに関する情報セキュリティ対策ガイダンス※187」を取りまとめている。更に、2012 年には、経済産業省の委託事業として、特定非営利活動法人日本セキュリティ監査協会（Japan Information Security Audit Association：JASA）が IPA の情報セキュリティ対策ベンチマーク（JIS Q 27002 をベース）を基に、サプライチェーンに参加する企業が順守すべき最低限の情報セキュリティ管理を示した「サプライチェーン情報セキュリティ管理基準※188」を策定している（情報セキュリティ対策ベンチマークについては巻末の「ツール 1 企業や組織の情報セキュリティ対策自己診断テスト」参照）。

これらのガイドラインは、委託元の委託先管理体制の構築、委託先へのセキュリティ対策要求事項の検討、委託先の対策実施状況の確認等の場面で参考になる。また、委託先は委託元からの要求に備えて対策を検討する際に参考になる。

NISC では、「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」に示された情報システムの構築等の外部委託や機器等の調達における情報セキュリティ対策要件の定め方や仕様書への記載事項の例を示した「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書※189」

を 2016 年に策定している。この手引書は政府調達担当者を対象に作成されているが、民間の企業においてもリスク対応の考え方や、仕様書の記載例等を参考にすることができる。

(3) クラウドサービスのガイドライン

情報システム構築の迅速化、管理運用の低廉化の手段として、IT サプライチェーンでもクラウドサービスの利用が増えている。クラウドサービスには、クラウドサービスの利用者と、クラウドサービスを提供する事業者（以下、クラウド事業者）でセキュリティ対策の責任分担があり、各々が必要とされる対策を実施してセキュリティを維持・向上させることが求められる。

パブリッククラウドでは、簡単な手続きですぐに利用を始めることができ、必要なときに必要なだけのリソースが使用できる柔軟性もあり便利であるが、セキュリティ対策のカスタマイズは難しく、クラウド事業者が提供する対策から選択せざるを得ないことが多い。また、セキュリティ対策状況は通常は限定的にしか利用者には開示されない。クラウドサービスの利用者は、こうしたクラウドサービスの特性を認識し、必要なセキュリティ対策をとる必要がある。

その参考となる、セキュリティに関する確認のポイント等が記載されたクラウドを安全に利用するためのガイドラインが策定されている。

経済産業省は、2011 年に「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」を策定しており、クラウド事業者が提供するクラウドサービスがサプライチェーンを形成する場合のリスク管理について定義している。本ガイドラインは、顕在化したリスクに対するセキュリティ要求事項及び国際的な動向を踏まえた追補を行い、2013 年に改版されている※190。また、総務省は 2014 年に「クラウドサービス提供における情報セキュリティ対策ガイドライン※191」を策定しており、クラウド事業者が実施すべき情報セキュリティ対策やサプライチェーンにおける実務ポイントをまとめている。本ガイドラインは、IoT サービスを提供する際のリスクに対する対応方針の追加及び 2008 年に策定した「ASP・SaaS における情報セキュリティ対策ガイドライン※192」を統合してクラウド事業者が参照するガイドラインの一元化を図り、2018 年に 2 版に改版されている※193。

リソースの制約が大きい中小企業では今後クラウドサービスの活用が進むことが想定される。IPA では「中小企業のためのクラウドサービス安全利用の手引き※194」を発行し、中小企業においても適切な安全性対策を実施することを求めている。

3.4.3 海外の政策動向

海外ではサプライチェーンのセキュリティ確保が国家の安全保障戦略や経済戦略の一つとして扱われており、各国の政策の中で具体化されている。これらの政策の中には各国と取り引きを行う日本の企業にも影響があると考えられるものもある。以下に主な海外の政策動向として、米国及び欧州の政策動向を述べる。

(1) 米国の政策動向

2008 年、George W. Bush 大統領（当時）の指示で策定されたサイバーセキュリティ戦略（Comprehensive National Cybersecurity Initiative：CNCI）では、「グローバルサプライチェーンのリスク管理に関する多方面アプローチの開発」が規定され、その必要性が示された。これを受けて、米国国立標準技術研究所（National Institute of Standards and Technology:NIST）では、NIST IR 7622 から移行する形で整備されたサプライチェーンリスクマネジメントに関するプラクティス集、NIST SP800-161 が 2015 年に制定された。2015 年より一部の米国連邦政府機関において、NIST SP 800-161 の遵守が義務化され、2016 年には、米国行政管理予算局（Office of Management and Budget：OMB）が発行する通達 A-130 号の改訂に、サプライチェーンリスクマネジメントの要件として追加された。NIST SP800-161 の制定は、国際標準化にも影響を与えており、NIST SP800-161 の作成者が中心となり ISO/IEC 27002 の「供給者関係」に関する管理策を詳細化する形で、IT の製品・サービスの調達における管理策をまとめた ISO/IEC 27036 が制定されている。また、米国連邦政府外のシステムと組織（民間組織）に提供される管理された非格付け情報（Controlled Unclassified Information）※195 の保護については、政府機関向けのセキュリティ規格 NIST SP 800-53 を基に、民間組織向けの要件として抽出された NIST SP800-171※196 が 2016 年に制定されている。米国国防総省に防衛装備品を納める全世界の調達事業者は 2017 年 12 月末までにこの基準への対応を求められた。今後、あらゆる連邦政府調達において調達ベンダのセキュリティが求められる可能性がある（「2.2.2 米国の政策」参照）。

更に、NIST が発行する重要インフラ向けサイバーセ

キュリティフレームワーク Framework for Improving Critical Infrastructure Cybersecurity[※197] は、2018 年 4 月に改訂された 1.1 版で、「Identify」（識別）の対策に「Supply Chain Risk Management」（ID.SC）を追加しており、サイバーサプライチェーンリスクマネジメントとして組織の優先順位付け、契約、リスク許容度、リスク推定等が定められリスク評価に利用されていること、サプライチェーンリスクを識別、分析、評価、管理するプロセスを定めて実行することを規定している。

2018 年 8 月には米国国防権限法 2019（NDAA2019）が成立した。NDAA2019 では米国政府機関に対し、「特定 5 社を含む中国企業製の通信・監視関連の機器・サービスを利用している機器・システム・サービス」の購入・取得・利用、及び「特定 5 社を含む中国企業製の通信・監視関連の機器・サービスを利用している、機器、システム又はサービス」を利用している企業・拠点との契約・取り引きを広汎に禁止している[※198]。NDAA2019 の適用対象は、サプライチェーン全体に及んでおり、米国政府機関と直接取り引きしていない、2 次、3 次サプライヤーの場合も、政府機関に納入される製品用のシステムや部分品を納めていれば対象となる。そのため日本企業においても、対象となる企業の部品、システム等を利用していないかの確認を求められ、利用していれば取り引きできなくなる可能性があり、十分注意し、対応を検討することが望まれる（米国による中国製品調達排除の動きについては「2.2.4 中国の政策」参照）。

(2) 欧州の政策動向

欧州では、EU 全体のサプライチェーンセキュリティを同じレベルで確保するための統一的な認証基盤を策定し、EU デジタル単一市場（EU Digital Single Market）の形成を加速しようとしている。具体的には、IoT 機器の統合セキュリティ認証でサプライチェーンセキュリティを確保するという、新たなサイバーセキュリティ認証フレームワーク（Cybersecurity Certification Framework）の導入に向けた議論が継続中である。欧州各国及び欧州議会（the European Parliament）で合意がとれれば、ルータ等の具体的な製品・カテゴリごとに基準が順次策定されていく予定である（「2.2.3 欧州の政策」参照）。

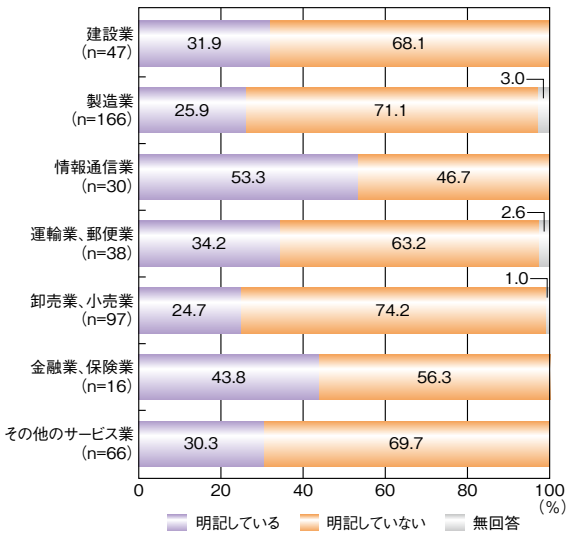
3.4.4 ITサプライチェーンにおける企業のセキュリティ対策状況

IPA では、2016 年度より IT サプライチェーンリスクマネジメントで扱うべきリスクや課題を整理するため、企業の IT サプライチェーンリスクマネジメントに対する認識や姿勢、取り組みの実態調査を開始した。以降にその結果を述べる。

(1) IT サプライチェーンリスクマネジメントの状況

2016 年度の調査では、委託元の委託先に対するセキュリティ対策ガバナンスの実態を調査し、「再委託先以降へのセキュリティ対策の徹底・状況の把握は委託先に依存せざるを得ない」「委託先に対して情報セキュリティ管理ルールの徹底を図る委託元の負担が大きい」「納品物のセキュリティを委託元による受け入れ確認や委託先による納品前の確認だけで検証するには限界がある」という結果が得られた[※199]。

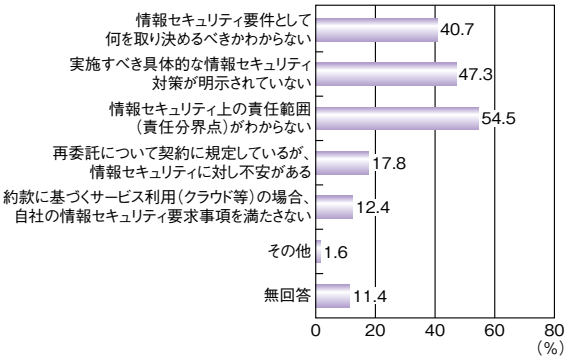
この結果を基に、2017 年度は業務委託におけるセキュリティインシデントや情報セキュリティリスクの実態、及び企業における当該リスクの防止・低減のためのマネジメントについて調査した。委託先が実施すべき具体的な情報セキュリティ対策を、委託元が仕様書等で明示しているかを調査した結果を図 3-4-1 に示す。情報通信業以外の委託元の業種では半数以上が明記していない。特に製造業、卸売・小売業、その他サービス業では約 7 割が委託契約時に具体的なセキュリティ対策の内容を明記していないと回答しており、セキュリティ対策について要求があいまいなまま作業が実施されていることが多いことが分かった。



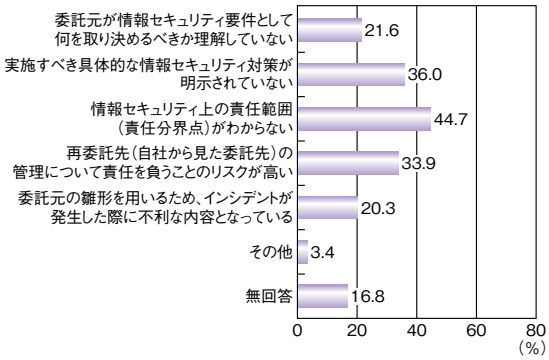
■図 3-4-1　委託先が実施すべき具体的な情報セキュリティ対策の仕様書等での明示の有無（n=499）
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査―調査報告書―[※199]」を基に編集

このような契約の実態に対して委託元、委託先ともに約半数の企業が、委託元と委託先の間の情報セキュリ

ティ上の責任範囲（責任分界点）が分からないことを課題に挙げていた（図 3-4-2、図 3-4-3）。



■図 3-4-2　委託先との契約における情報セキュリティの観点での課題（委託元）（複数選択、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ー調査報告書ー」を基に編集



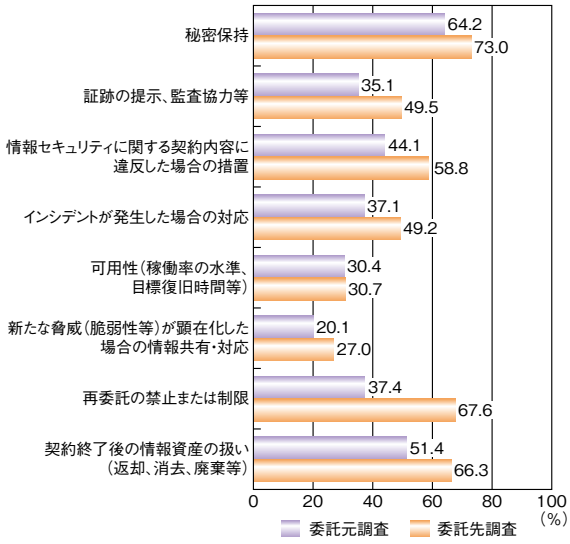
■図 3-4-3　委託元との契約における情報セキュリティの観点での課題（委託先）（複数選択、n=620）
（出典）IPA「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査ー調査報告書ー」を基に編集

例えば、情報漏えいや不正アクセスといったセキュリティインシデントが発生した場合、被害の影響を最小化するためには、委託元、委託先の双方の協力、連携が不可欠である。しかし、セキュリティインシデントに関する責任範囲が明確になっていない場合、初動が遅れる、連携がうまくできない等の恐れがある。

(2) IT サプライチェーンにおける責任範囲の明確化

このような背景から、2018 年度の調査では、情報セキュリティの責任範囲の明確化を阻害する要因を明らかにするため、2017 年度調査では委託先が実施すべき具体的な情報セキュリティ対策が明記されている割合が少なかった委託元の業種（製造業、卸売業・小売業、サービス業）及び委託先を対象に調査を実施した。

業務委託契約時にセキュリティに係る責任範囲についてどのような内容を文書に明記していたかについて調査した結果を図 3-4-4 に示す。委託元、委託先ともに、傾向は同じであり、「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」について明確にしているケースが最も少ない結果となった。

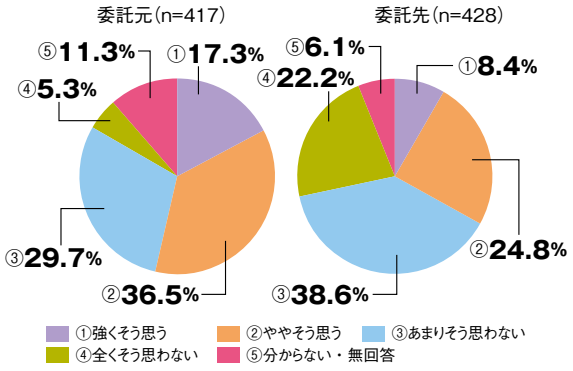


■図 3-4-4　IT 業務委託時に明確にしている責任範囲の内容
委託元調査（n=313）、委託先調査（n=374）
（出典）IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書※200」を基に編集

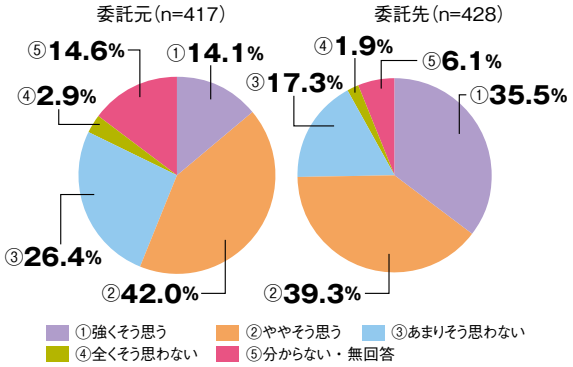
新たな脅威（脆弱性等）が顕在化したとき、誰の責任で対応するのかが決まっていないと、脆弱性が放置され、インシデントの発生、被害の拡大につながる恐れがある。また、情報共有についても、例えばユーザからシステムの詳細情報や関連する事業への影響度合い等について、ベンダに伝えられなければ、正しい判断、適切な対応ができず、初動の遅れや対応時間の長期化等の恐れがある。

システム納品後に見つかった未知の脆弱性への対応に関する意識について調査した結果を図 3-4-5（次ページ）、図 3-4-6（次ページ）、図 3-4-7（次ページ）に示す。

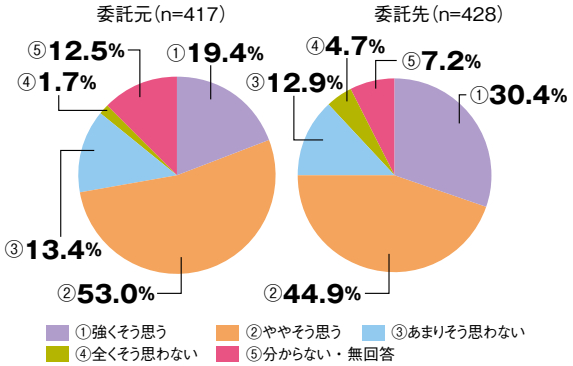
納品後に発見された未知の脆弱性について、委託先が責任を持つべきと考えている委託元企業は、「強くそう思う」「ややそう思う」という回答を合わせて 53.8% であるのに対し、委託先企業は 33.2% であり、委託先と委託元の認識に違いがある傾向がみられた。更に、未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだと考えている委託元企業は、「強くそう思う」「ややそう思う」という回答を合わせて 56.1% であるのに対し、委託元企業は 74.8% であり、委託先と委託元の認識に違いがある傾向がみられた。しかし、未知の脆弱性への対応について契約書等で定めるべき



■図 3-4-5　脆弱性への対応(納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ)
(出典)IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に編集



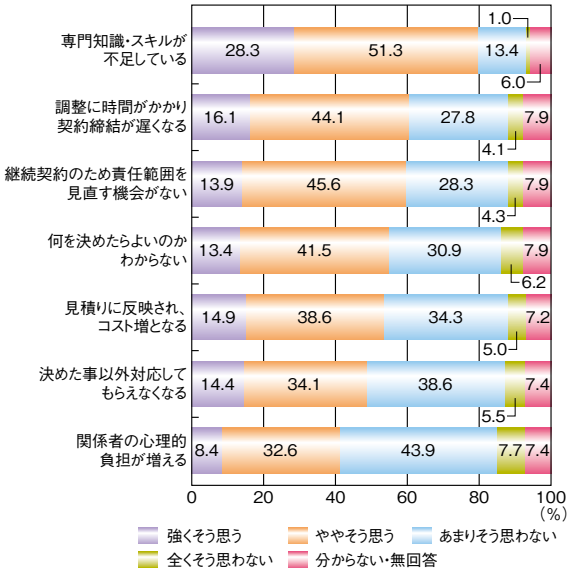
■図 3-4-6　脆弱性への対応(納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ)
(出典)IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に編集



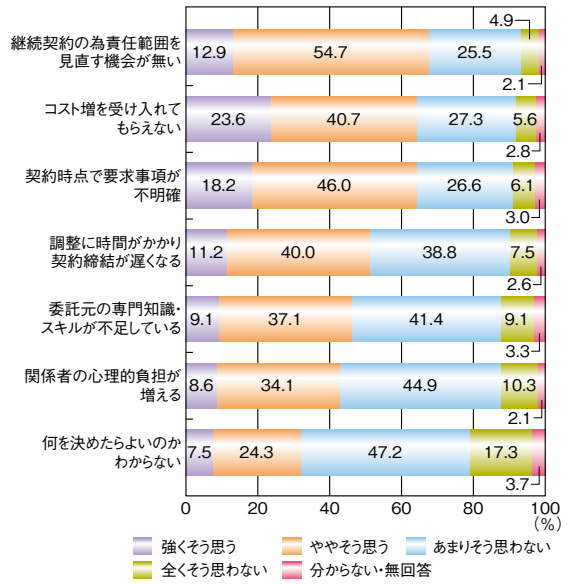
■図 3-4-7　脆弱性への対応(納品後の IT システムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ)
(出典)IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に編集

かについては、委託先、委託元ともに、70% 以上が定めるべきと考えており、責任分担や対応についての考え方に違いはあるが、契約により責任範囲を明確化したいと考えていることが分かった。

このように、責任範囲を明確にしたいと考えているにも関わらず、実際の契約では明示されていない原因を明らかにするために、業務委託契約時に責任範囲が明確にならない理由について調査した結果を図 3-4-8、図 3-4-9 に示す。委託元が考える最大の理由がスキル不足であるのに対し、委託先は見直しの機会がないことが「強くそう思う」「ややそう思う」という回答を合わせると 67.6%で最大の理由であった。また、委託元では何を決めたらいいのか分からないという理由が、「強くそう思う」「ややそう思う」という回答を合わせて 54.9% であるのに対し、委託先は 31.8% であり、委託元と委託先では、



■図 3-4-8　責任範囲が明確にならない理由(委託元調査)(n=417)
(出典)IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に編集※201



■図 3-4-9　責任範囲が明確にならない理由(委託先調査)(n=428)
(出典)IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に編集

責任範囲を明確にできない理由の傾向に違いがあることが分かった。

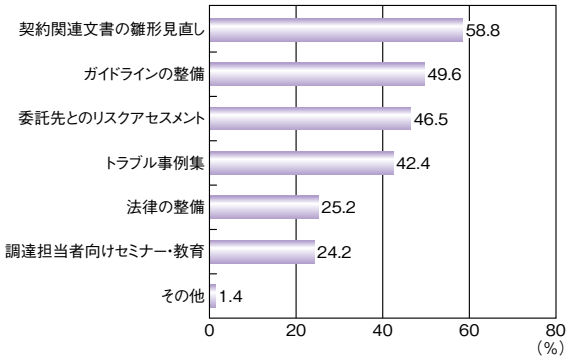
(3)IT サプライチェーンにおける責任範囲の明確化に必要な取り組み

これまでに述べたように、業務委託契約における責任範囲の明確化において、委託先と委託元の間では明確にできない理由や責任分担の考え方に違いはあるものの、責任範囲を契約書等で定めるべきと考えており、このような背景から、責任範囲を明確化するための有効な施策について調査した結果を図 3-4-10、図 3-4-11 に示す。

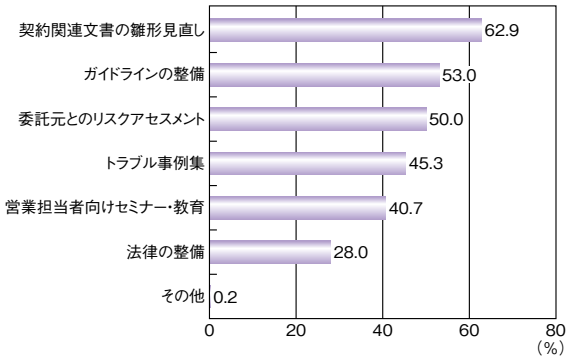
委託元、委託先ともに、契約関連文書の雛形を見直すことが有効と考えており、次いでガイドラインの整備、委託元、委託先によるリスクアセスメントが有効であるという結果となった。

2017 年 5 月に、約 10 年ぶりに改正された「個人情報保護法」の全面施行、2018 年 5 月に施行された EU の一般データ保護規則（General Data Protection Regulation：GDPR）※202 等、個人情報を取り扱う事業者には影響の大きい出来事が続いている。また、2017 年 5 月に 120 年ぶりに国会で可決された改正民法が 2020 年 4 月に施行される。IT システム・サービス等の業務委託契約に関連するところでは、瑕疵担保責任の考え方や、請負や準委任に関する考え方が変更になっており、「瑕疵担保責任」が、契約内容に適合しない場合に修補・追完を請求できる「契約不適合責任」に変更された。これにより、契約時における契約内容の明確化がより一層求められるようになり IT サプライチェーンにも大きく影響するものと考えられる。例えば、納品後のソフトウェアプログラムに脆弱性が発見され、委託先に修補を求めようとする場合、あらかじめ、そのような脆弱性のないプログラムの納品を契約内容としておく必要がある。情報漏えい等の紛争時に、委託先の契約不適合責任を追及する委託元の立場は弱くなるため、仕様書を作成する委託元が、より要件を明示しなければならなくなる。

民法改正への対応として、契約書や自社の契約書の雛形の見直しがある可能性が高い。そうした機会にセキュリティに関する見直しも行うことが望まれる。



■図 3-4-10　責任範囲を明確化するために有効であると考えられている対策（委託元）（複数選択、n=417）
（出典）IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に作成



■図 3-4-11　責任範囲を明確化するために有効であると考えられている対策（委託先）（複数選択、n=428）
（出典）IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」を基に作成

3.4.5 おわりに

IoT、AI、ビッグデータ等の新技術により新たなビジネスパートナーが増え、ネットワークを介してつながることにより国内外を問わず、多種・大量の情報をやり取りするようになったことは、IT サプライチェーンの構造をより複雑にしている。以前より再委託先以降の状況がよく分からず、IT サプライチェーン全体の状況の可視化が問題視されているが、更に複雑になることが想定され、IT サプライチェーンのセキュリティ対策は企業が抱える難しい課題の一つとされている。

本節では IT サプライチェーンに関連したインシデントの事例を取り上げ、リスクの把握と対策の確実な実施の重要性を述べた。IT サプライチェーンに関連したインシデントは多岐に渡っており、対策も様々であるが、企業間での情報共有、ガイドラインの活用、契約の見直し等、本節で紹介した対策等を参考に実施できるところから始めていただきたい。

3.5 AIのトラストとセキュリティ

AI（Artificial Intelligence：人工知能）は第三次ブームを迎えているといわれ、実用化への期待が高まっている。

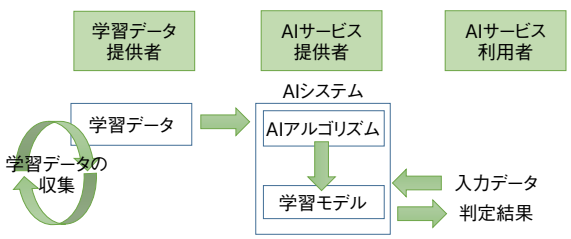
AIは、1980～1990年代のブーム（第二次ブーム）終焉後はしばらく利用が進んでいなかったが、2000年代のビッグデータ分析基盤の実用化を経て、2010年代のディープラーニング（深層学習）を代表とする機械学習技術の革新以降大きく注目され、医療・自動走行等の応用に向けた研究開発・実用化が進んでいる（第三次ブーム）[※203]。これと並行して、AIの実用化に向けた社会実装や人材育成に向けた議論が進んでいる。またその中で、実用化に関するリスクとして、AI利用の倫理、社会生活・労働形態の変化、法制面の不備等の様々な課題についての議論も始まっている[※204]。

本節では、まずAIという言葉のスコープを定義し、その社会実装に関わるリスクを概観する。その後、特にAIアルゴリズム・学習データ・AIサービス等の真正性・品質・安全に関わるトラスト（信頼）、及びセキュリティについて、検討状況を概説する。

3.5.1 本節で扱うAIのスコープ

2019年の時点において、AIという言葉は使われ方が多面的であり、すべての人が同じ意味で使っているわけではないと考えられる。本節では、AIを「学習によってモデルを作り出す機能」と、「学習モデルを使って予測、分析、計画等の処理を行う機能」を持ついわゆる機械学習技術としてとらえることとし、機械学習技術を応用したシステムを、AIシステムとして説明する。

以下の説明を具体的にするため、AIシステムの提供・利用に関わる人とデータの流れを図3-5-1に示す。図中のAIサービス提供者は、AIシステムを用いてAIサービス利用者に分析等のサービスを提供する。学習データ提供者は学習に必要なデータを収集し、学習に向けた処理を行う。AIシステムは、学習データ提供者からの学習データに基づき、AIアルゴリズムで、学習モデルを生成する。また、AIサービス利用者からの入力データを学習モデルに入力して判定結果を返す。



■図3-5-1　AIシステムの関係者とデータ

通常のソフトウェアと比較した場合、「学習」のプロセスや「学習モデル」がAIシステムの性能・品質に大きく影響する点、また、AIサービス利用者が実環境から「入力データ」を提供し、上記の性能・品質に影響を与える点が特徴的である（「3.5.5（2）（b）学習データへの脅威」参照）。

3.5.2 AIの社会実装に関わるリスク

これまで技術者・研究者・法律家等の専門家によって技術・倫理・制度等の様々な観点から、AIの社会実装に関わるリスクが議論されてきた[※205]。これは以下の5項目に整理される。

（1）不適切な利用・悪用

不適切な利用に関しては、AIが公平・公正な利用に反した目的に使われるリスクが指摘されている。具体的には、犯罪利用、軍事利用、プライバシー侵害、差別的な利用等を含む倫理面の課題が懸念される。このため、運用面では正規の学習が不公正な結果を生むリスクを検証することが求められる。制度面では、GDPR等で、差別・偏見につながる個人情報利用への対応が始まっている。

（2）責任分担

AIが人間の業務を自動化できるとしても、人間と同等の責任を分担させることは難しい。実際、AIシステムの判断・操作によって事故が発生した場合の責任の所在や責任分界点は、法的にも制度的にも明確になっていない。実用化が急がれる自動走行等の分野では、AI利用の責任範囲、法制度、運転者とAIとの連携等について官民で議論が進められている。

（3）説明責任

AIで分析を行った際に、なぜその分析結果に至ったか、分析のための学習は妥当だったのか、等の説明は一般に困難である。この「説明」の問題はAIの社会へ

の受容を阻む要因として技術者・研究者・事業者に共有されており、「説明責任」「透明性」等をキーワードとして、何をどこまで説明し、透明に(検証可能に)すればよいのか、の議論が進められている。

(4) 性能・品質

AIシステムは従来のソフトウェアとは異なり、学習の質や量によって分析の精度・品質が左右されるが、学習の評価手法や品質維持の方法論はまだ模索段階である。このためソフトウェア工学者を中心に、AI品質工学とも呼ぶべき技術構築の機運が急激に高まっている。

(5) セキュリティ

AIのセキュリティ分野での利用が期待される一方で、AIシステムが脆弱でないことも重要である。近年、学習アルゴリズムの脆弱性を突いて、細工したデータにより誤判断を起こさせる手法が研究されている(「3.5.5 (2) (a) アルゴリズムへの脅威」参照)が、AIシステム全体のセキュリティとしては、学習データや学習モデルの真正性確保や秘匿、学習・運用の妥当性(悪用・誤用されない)等を含めた包括的なリスクを検証することが重要になる。

3.5.3 関連組織の活動

上記の項目を含めて、AIが社会で信頼され、受容されるための議論が以下のような組織で行われ、規格や原則が公開されている。

(1) 国際標準化団体の取り組み

IEEE (Institute of Electrical and Electronics Engineers)はAIの社会実装、特に開発者の倫理に関する議論をいち早く開始しており、有識者によりまとめられたEthically Aligned Design, Version2 (EADv2)[※206]を公開している。EADv2ではAIの設計・開発・実装に関する倫理的な原則として以下の5項目を挙げている。

原則1 Human Rights(人権)
原則2 Prioritizing Well-being(幸福)
原則3 Accountability(アカウンタビリティ)
原則4 Transparency(透明性)
原則5 A/IS Technology Misuse and Awareness of It(悪用への警戒)

これらの原則に関しては、IEEE P7000 Engineering Methodologies for Ethical Life-Cycle Concerns Working Group[※207]において、設計段階における倫理課題対応のモデルプロセス(P7000)、自律型システムの透明性(P7001)、データプライバシー(P7002)、アルゴリズムのバイアス検討(P7003)等の規格を策定中である。

また2017年10月、ISO(International Organization for Standardization)とIEC (International Electrotechnical Commission)の情報技術に関する合同委員会であるISO/IEC JTC 1のもとにSC 42 Artificial Intelligenceの設置が決定された。トラストに関しては、WG 3 Trustworthinessの中でBiasやRobustnessに関する標準報告書(TR)の策定が進められているほか、Risk managementに関する国際標準化も開始されている[※208]。

(2) 国の取り組み

欧州委員会(European Commission:EC)のAI高等専門家グループはEthics Guidelines for Trustworthy AIを策定し、2018年12月にドラフトを公表、2019年4月にパブリックコメントを反映した正式版を公表した[※209]。本ガイドラインでは、「Trustworthy」は①合法性:すべての適用法令の尊重、②倫理:倫理の原則と価値観の尊重、③堅牢性:社会的環境への考慮と技術的観点の両面、であるべきとしている。

日本では、内閣府「人間中心のAI社会原則検討会議」が、「AI-Readyな社会」を実現しAIの適切で積極的な社会実装を推進するための「人間中心のAI社会原則(平成31年3月29日統合イノベーション戦略推進会議決定)」を策定した。その中で同原則は、AIが社会に受け入れられ適正に利用されるため、社会が留意すべき「AI社会原則」とAIの研究開発と社会実装に従事する開発・事業者側が留意すべき「AI開発利用原則」に体系化されている(後者の内容は今後策定)[※210]。このうち、「AI社会原則」は以下のとおりである。

- 人間中心の原則
- 教育・リテラシーの原則
- プライバシー確保の原則
- セキュリティ確保の原則
- 公正競争確保の原則
- 公平性、説明責任及び透明性の原則
- イノベーションの原則

なお、2019年6月に開催されたG20貿易・デジタル経済相合同会合において「人間中心の人工知能(AI)」に関する検討が行われ、「G20 AI原則」として合意され

た。本原則には「包摂的な成長、持続可能な開発及び幸福」「人間中心の価値観及び公平性」「透明性及び説明可能性」「頑健性、セキュリティ及び安全性」「アカウンタビリティ」が含まれる※211。

(3) 産業界の取り組み

Google LLC は AI の研究開発や製品開発の方針として、意思決定における 7 原則を公開している※212。

- 社会的に有益なこと
- 不公正な偏見の創出や強化を避けること
- 安全性のための構築と検査がされること
- 人に対して責任を負うこと
- プライバシーデザインの原則を組み込むこと
- 科学的に卓越した基準を守ること
- これらの原則に一致する用途に利用できること

他にも Microsoft Corporation（以下、Microsoft 社）※213、International Business Machines Corporation（以下、IBM 社）※214、SAP SE、ソニー株式会社等が AI に関する倫理原則を公開している。

3.5.4 AIのトラストの検討状況

社会が AI を受容するためにはトラスト（信頼）が必要である、と言われるが、トラストの要件は様々である。以下ではその検討状況を整理する。

(1) トラストのタイプ分類

前述の五つのリスクの低減には、社会全体、組織間、組織と個人間等で合意を形成していきながら、AI を社会が安心して受容できる環境を整えていく必要がある。これを AI に対するトラスト構築という視点で見た場合、倫理・説明責任等、AI サービス利用者との合意形成に時間をかけた方がよい課題と、品質・安全の評価等で AI サービス提供者が早期に方法を提示すべき課題の二つに分けて整理することが有効と思われる。これを以下のように定義する。

①社会受容のトラスト

AI サービス利用者を含む社会全体が AI を受容し、使ってもよいと実感するために、中長期にわたり分野横断的に構築されるべきトラストである。このようなトラストの構築には、制度・技術を整備することに加え、AI サービス利用者の心理的な納得が必要である。

②製品・サービスとしてのトラスト

AI システムの品質・セキュリティ等が妥当であり、実用に足ることを示すためのトラストである。製品ベンダや AI サービス提供者が製品利用者や AI サービス利用者に示す品質保証に近いもので、従来のソフトウェアでいえば不具合なく仕様どおり動作すること、セキュリティ的に脆弱でないことがこれにあたる。しかし、AI システムでは品質の維持向上に「学習」というプロセスが入るため、保証の仕方は従来の手法の援用では不十分と考えられる。

(2) 製品・サービスとしてのトラスト

前項のリスクやトラストに関する議論は、主として①の社会受容のトラスト、特に開発・利用の倫理や説明責任が重点的に議論されてきた。一方、②の製品・サービスとしてのトラストに関しては、実用化の進展とともに議論が進み始めている。

国内では、例えば国立研究開発法人科学技術振興機構（Japan Science and Technology Agency：JST）が AI システムの安全性・信頼性を確保する新世代ソフトウェア工学の確立が必要であるとの戦略プロポーザルを行った※215。またソフトウェアエンジニアリングの分野では、AI プロダクトの品質保証技術の研究開発の促進や品質保証レベルの策定等を目的とするコンソーシアム（QA4AI）が設立され、2019 年 5 月 17 日、AI プロダクト品質保証ガイドライン※216を公開した。同ガイドラインは、機械学習に代表される AI 技術を適用した製品の品質保証に対する共通の指針を示している。このような製品の開発では、ハードウェアや従来のソフトウェアの品質保証手段や開発プロセス管理による品質保証を適用しても寄与する割合が小さいとし、新たな品質保証技術の調査・体系化、適用支援、研究開発が急務であると述べている。また品質保証では、顧客が AI 技術の特性を理解することも重要としている。

例えば従来のソフトウェア開発では、仕様どおり、あるいは求められるセキュリティレベルで機能を実装するための手法が確立されており、ベンダがそれらの手法を用いたと保証することでトラストは担保される。しかし機械学習においては、目標とする分析性能等が達成できるかどうかは学習手法や学習データにも依存する。仮に間違った学習をした場合、アルゴリズムの修正で間違いが解消する保証はなく、更なる学習で学習モデルを修復する必要もあると考えられる。更に、分析性能等を維持向上させるため、実環境で継続的に学習しなければならない状況が想定される。

以上から、製品・サービスのトラスト構築について、以下の二つが重要であると考えられる。

①AI システムの学習データの妥当性（量や質、密度等）や学習プロセスの妥当性の評価手法を確立する。提供する AI システムに求められる品質を学習プロセスにも作り込むことが求められる。

②AI サービス利用者に、学習に関する特性（通常のソフトウェアとの違い等）を理解してもらい、求める品質・セキュリティレベルについて合意する。また、利用者環境で学習を行う場合は利用者も参画する等で AI サービス提供者・AI サービス利用者が連携する。

①については、前掲のガイドライン等で検討が本格化している。一方、②については、特に AI の品質・安全の確保に AI サービス利用者が能動的に関わるという意識付けが重要になる※217 ため、今後 AI システムの実用に向け、ステークホルダ間の幅広い議論が必要と考えられる。

3.5.5 AIのセキュリティの検討状況

AI のセキュリティに関しては、「AI を利用したセキュリティ（AI for security）」と「AI 自身のセキュリティ（Security for AI）」の二つの視点がある。前者については、ビッグデータ分析が普及した 2000 年代後半、いち早くスパムメール検知や異常検知等への機械学習の適用が始まっており、検知精度の向上やリスク分析への適用等、セキュリティ強化への期待が大きい。一方で、AI 自身のセキュリティについては、2015 年ごろより AI の倫理に関連した悪用・誤用やプライバシー保護の議論、あるいは AI アルゴリズムの脆弱性に関する研究が進展し、AI システム全体のセキュリティ議論は 2018 年ごろより本格化している。本項ではこの二つの視点についてそれぞれの検討動向を概説する。

(1) AI を利用したセキュリティ

上記のとおり、2000 年代後半にはビッグデータ分析への機械学習技術の応用が普及し、メール学習によるスパムメール検出、トラフィック解析やシステムのログ分析によるネットワーク異常検知・ウイルス検知等の分野で実用化が始まった。分析官に高度なスキルが必要とされる SOC（Security Operation Center）や CSIRT（Computer Security Incident Response Team）等の運用業務に既に適応されており、今後も自動化・効率化に貢献することが期待されている。

例えばウイルス検知では、悪意の振る舞いや悪性コード等を学習し、その学習モデルに基づいて検出することが試みられてきた。近年は何億、何十億もの大量のデータを学習することで、学習モデルの精度や検知率が向上しているが、新種や大量の亜種が日常的に出現し続けていることから、継続的な学習のためのウイルスの網羅的な収集が課題となる。またウイルス自身は、巧妙化が進んでおり、ウイルスであるとの判断が難しく、検知をすり抜ける（検知漏れ：false negative）恐れがある。そこで学習モデルをチューニングして false negative を小さくしていくと、ウイルスでないものを多く検知してしまうこと（誤検知：false positive）が起こり得る。

更に、攻撃者に AI 技術の専門家がいる場合、ウイルス検知の AI を自ら作り、その学習モデルをすり抜けるようなウイルスを生成することも考えられる※218。こうしたいたちごっこの状況において、誤検知・検知漏れの排除は容易ではない。将来さらなる AI 技術の革新があるとしても、攻撃者も同様な AI 技術を悪用してすり抜けを試みると考えられ、攻撃検知を志向した AI システムは現状のように継続的なチューニングを迫られると考えられる。

(2) AI 自身のセキュリティ

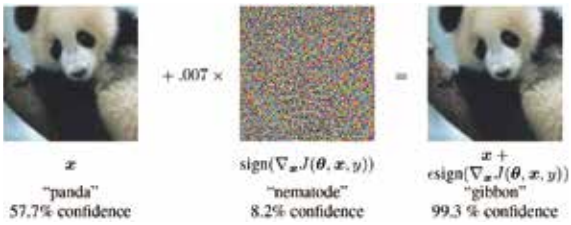
AI 自身のセキュリティについては、2018 年ごろから体系的な議論が行われるようになってきた。国内では 2018 年 8 月、日本銀行金融研究所が機械学習システムのセキュリティに関する研究動向と課題について詳細に報告している※219。

以下では、AI アルゴリズム、学習データ、学習モデルの 3 要素に対する脅威について述べる。

(a) アルゴリズムへの脅威

AI アルゴリズム自身の特性（あるいは不備）を悪用し、意図的に誤判定を起こさせることは、AI システムの性能劣化、あるいは誤判定による事故等を目的とするサイバー攻撃の手段となり得る。近年、AI アルゴリズムが誤判断を起こすデータを意図的に与える研究が注目されている。例えば画像認識において、人間には知覚できないノイズを含めることで判定結果を誤らせる敵対的サンプル（Adversarial Example）の事例（次ページ図 3-5-2）等が報告されている。

誤判断を起こす目的で改ざんされたデータを分析させれば、AI システムの性能を大きく損ねる可能性がある。ただし、このような攻撃は、AI アルゴリズムの特性や学



■図 3-5-2　人間が知覚できないノイズを画像に加え、パンダをテナガザルと誤認識させる例
（出典）Goodfellow et al.「EXPLAINING AND HARNESSING ADVERSARIAL EXAMPLES※220」

習モデルの専門知識を持ち、入力データに容易にアクセスできることが前提となるため難度が高く、当面攻撃のリスクは小さいと考えられる※221。Adversarial Example のような研究は攻撃対策の探索に加え、アルゴリズムの弱点を発見し、改良の方策を探る手法として重要な意味を持つものと思われる。

(b) 学習データへの脅威

通常システムと共通するセキュリティ要件として、図 3-5-1（188 ページ）のデータ流通経路からのデータの漏えいがないこと、また学習データへの改ざんがないことを担保する必要がある。

AI システム固有の脅威としては、偏ったデータや改ざんされたデータを学習させることで、学習モデルの精度を低下させる、誤判定を起こさせる等の攻撃に備えることが必要である。例えば学習データを実環境で大量に収集する場合等で、データ改ざん等のリスクに対処することが求められる。

学習データへの攻撃ではなく、正規のデータ入力と判定結果から、学習データを推定する研究事例が報告されている※222。これは顔画像の学習事例であったため、プライバシー侵害の可能性が示唆された。しかし、この推定も攻撃としての難度は高く、当面のリスクは小さいと考えられる。

悪意の攻撃によるものではないが、偏ったデータ入力で AI サービスの品質が劣化した事例として、Microsoft 社の AI チャットボット※223 Tay のサービス停止がある。2016 年 3 月 23 日、同社の Tay はサービスイン直後に人種差別的な応答をすることが発覚、サービスが停止された※224。これは Tay が人種差別的なコメントをジョークととらえ、対話を続けるという特性に一般利用者が気付き、意図的に差別的な入力を行った結果だといわれる。一般利用者向けの AI システムにおいて、学習データを意図的に偏らせることへの対策が必要であることを示す事例となった。

(c) 学習モデルへの脅威

学習モデルを不正コピーにより詐取され、同等の性能を持つ類似 AI を安価に作られる、等の脅威がどの程度のインパクトになるかはまだ自明でない。しかし学習モデルはそれ自体が営業秘密であり、正規のビジネスを侵害する類似 AI が出回るというケースも将来はあると考えられる。保護の対象としてセキュリティを確保することが重要と思われる※225。

(3) AI の悪用

セキュリティベンダは、ウイルス検知等のセキュリティ対策に AI を活用している。一方で、サイバー犯罪者も、セキュリティ対策を回避するために AI を活用することが可能である。セキュリティベンダのレポートでは、AI を悪用したサイバー攻撃の巧妙化が懸念されている※226。実際に、IBM 社は AI を利用して検出されにくいウイルスを生成できる DeepLocker というツールを発表している※227。

AI の悪用について、2019 年時点で懸念されている脅威は、インターネット上の巧妙なデマ、あるいは詐欺、更には世論操作である。その例として、ディープフェイク※228 と呼ばれる画像合成技術がある。機械学習技術の応用により、例えば本物の政治家が虚偽の発言をする迫真の動画が作れてしまう※229。ディープフェイクの怖さは、それを見た人が簡単に信じてしまう、すなわち、安易に作った偽動画が思わぬ人権侵害、世論操作等の悪影響を及ぼしかねない点にある、ともいわれる※230。2019 年 6 月、米国下院特別情報委員会はディープフェイク、あるいは類似技術の大統領選挙への影響を懸念し、公聴会を開くと発表した※231。

総務省「プラットフォームサービスに関する研究会」が 2019 年 3 月に取りまとめた中間報告書（案）では、ディープフェイクを含めた「オンライン上のフェイクニュースや偽情報への対応」が検討課題として挙げられている※232。

(4) まとめ

以上でみたように、AI システム自身のセキュリティについての検討は始まったばかりであるが、当面のリスクとしては、AI システムへの攻撃よりは、攻撃者による AI システムの悪用、あるいは AI サービス利用者の安易な利用による悪影響が懸念される状況にある。本節で概観した AI システム開発・利用における倫理規定の策定とその周知徹底は、一見遠回りではあるが、これらに対する対処として重要なものと考えられる。

COLUMN

情報セキュリティ10大脅威 2019
～局面ごとにセキュリティ対策の最善手を～

IPA では 2006 年から毎年、情報セキュリティ専門家を中心に構成する「10 大脅威選考会」の協力により、前年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けした「情報セキュリティ 10 大脅威」を発表しています。2016 年からは「個人」と「組織」という異なる立場で、それぞれの脅威を順位付けし、10 大脅威を決定しています。2019 年 2 月に公開した「情報セキュリティ 10 大脅威 2019」は、下表のとおりです。

表　情報セキュリティ 10 大脅威 2019「個人」・「組織」向け脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
クレジットカード情報の不正利用	1	標的型攻撃による被害
フィッシングによる個人情報等の詐取	2	ビジネスメール詐欺による被害
不正アプリによる スマートフォン利用者への被害	3	ランサムウェアによる被害
メール等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した 攻撃の高まり
ネット上の誹謗・中傷・デマ	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	サービス妨害攻撃によるサービスの停止
インターネットバンキングの不正利用	7	インターネットサービスからの 個人情報の窃取
インターネットサービスへの不正ログイン	8	IoT 機器の脆弱性の顕在化
ランサムウェアによる被害	9	脆弱性対策情報の公開に伴う悪用増加
IoT 機器の不適切な管理	10	不注意による情報漏えい

10 大脅威のそれぞれや、その他の注目すべき脅威について解説している「情報セキュリティ 10 大脅威 2019」は、以下の URL からダウンロードできます。

IPA：情報セキュリティ 10 大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

各脅威が自分自身や自組織にどう影響するか確認しながらこの資料を読み進めることで、様々な脅威と対策を網羅的に把握できます。また、この資料は、自組織での研修やセキュリティ教育等に活用することができますので、ぜひご一読ください。

※ 1　BBC：Hack attack causes 'massive damage' at steel works　https://www.bbc.com/news/technology-30575104〔参照 2019-05-28〕
※ 2　Cisco Systems, Inc.：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 2019-05-28〕
キヤノンマーケティングジャパン株式会社：産業制御システムに最大級の脅威をもたらすマルウェア「インダストロイヤー」　https://eset-info.canon-its.jp/malware_info/trend/detail/170620.html〔参照 2019-05-28〕
※ 3　FireEye, Inc.:産業制御システム（ICS）への新たな攻撃フレームワーク「TRITON」が重要インフラの運用停止を誘発　https://www.fireeye.jp/company/press-releases/2017/attackers-deploy-new-ics-attack-framework-triton.html〔参照 2019-05-28〕
※ 4　インシデント件数については「JPCERT/CC インシデント報告対応レポート [2017 年 1 月 1 日～ 2017 年 3 月 31 日]」～「JPCERT/CC インシデント報告対応レポート [2018 年 10 月 1 日～ 2018 年 12 月 31 日]」（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 2019-05-28〕）を参照した。
※ 5　Help Net Security：Middle East oil and gas companies are unprepared to address OT cyber risk　https://www.helpnetsecurity.com/2018/03/21/middle-east-ot-cyber-risk/〔参照 2019-05-28〕
※ 6　Kaspersky Lab ICS CERT：The State of Industrial Cybersecurity 2018: findings of joint survey by Kaspersky Lab and PAC　https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf〔参照 2019-05-28〕
※ 7　「マルウェア」等の用語を混在して使用すると、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。
※ 8　Kaspersky Lab ICS CERT：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/#210〔参照 2019-05-28〕
Kaspersky Lab ICS CERT：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/#_Toc509229764〔参照 2019-05-28〕
Kaspersky Lab ICS CERT：Threat Landscape for Industrial Automation Systems in H1 2018　https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523849957〔参照 2019-05-28〕
Kaspersky Lab ICS CERT：Threat Landscape for Industrial Automation Systems in H2 2018　https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/#_Toc4416135〔参照 2019-05-28〕
※ 9　VPNFilter は、ネットワーク機器を標的とした IoT ボットであるが、制御システムで利用される Modbus プロトコルをモニタリングする機能を有しており、制御システムも意識したウイルスである可能性も指摘されている。
※ 10　The Register：Ukraine claims it blocked VPNFilter attack at chemical plant　http://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/〔参照 2019-05-28〕
※ 11　ZDNet：Moscow's new cable car system infected with ransomware two days after launch　https://www.zdnet.com/article/moscows-new-cable-car-system-infected-with-ransomware-two-days-after-launch/〔参照 2019-05-28〕
※ 12　Los Angeles Times：Malware attack disrupts delivery of L.A. Times and Tribune papers across the U.S.　http://www.latimes.com/local/lanow/la-me-ln-times-delivery-disruption-20181229-story.html〔参照 2019-05-28〕
※ 13　eWEEK：Water Utility in Europe Hit by Cryptocurrency Malware Mining Attack　http://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack〔参照 2019-05-28〕
※ 14　SC Media：North Carolina water utility ONWASA taken down by ransomware　https://www.scmagazine.com/home/security-news/north-carolina-water-utility-onwasa-taken-down-by-ransomware/〔参照 2019-05-28〕
※ 15　New Energy Update：Russian hackers penetrate US power control rooms; Quinbrook plans 690 MW PV plant near Las Vegas　http://newenergyupdate.com/pv-insider/russian-hackers-penetrate-us-power-control-rooms-quinbrook-plans-690-mw-pv-plant-near-las〔参照 2019-05-28〕
※ 16　Wall Street Journal：America's Electric Grid Has a Vulnerable Back Door-and Russia Walked Through It　https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112〔参照 2019-05-28〕
※ 17　IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 7 月～ 9 月］　https://www.ipa.go.jp/files/000069662.pdf〔参照 2019-05-28〕
※ 18　ESET, spol. s r.o.：Apple chip supplier blames WannaCryptor variant for plant shutdowns　https://www.welivesecurity.com/2018/08/07/apple-chip-wannacryptor-shutdowns/〔参照 2019-05-28〕
※ 19　SecurityWeek：Malware Found on USB Drives Shipped With Schneider Solar Products　https://www.securityweek.com/malware-found-usb-drives-shipped-schneider-solar-products〔参照 2019-05-28〕
Schneider Electric：Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor　https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SESN-2018-236-01+Conext+USB+Malware.pdf&p_Doc_Ref=SESN-2018-236-01〔参照 2019-05-28〕
※ 20　ICS-CERT Annual Vulnerability Coordination Report の Figure 1.（p.3）の「Advisories - FY」の数字を採用した。ただし、Figure 1. の 2016 年には暦年（CY）の件数があるが、件数が 185 件と、実際に Web サイト上で公開されている件数（140 件）と大きく乖離しており、カウント方法の詳細が不明なため、2017 年、2018 年と同様に ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントして図 3-1-2 に掲載した。
NCCIC：ICS-CERT Annual Vulnerability Coordination Report　https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf〔参照 2019-05-28〕
※ 21　ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2018 年なら、採番年度が 2017（ICSA-2017-xxx-x）でも 2018 年でカウント）。
NCCIC：ICS-CERT Advisories　https://ics-cert.us-cert.gov/advisories〔参照 2019-05-28〕
※ 22　IPA：共通脆弱性評価システム CVSS v3 概説　https://www.ipa.go.jp/security/vuln/CVSSv3.html〔参照 2019-05-28〕
※ 23　Dragos, Inc.：Industrial Controls System Vulnerabilities　https://dragos.com/resource/industrial-controls-system-vulnerabilities/〔参照 2019-05-28〕
※ 24　Radiflow. Ltd.：Radiflow Offers New Approach for Classifying and Assessing OT Attack Vulnerabilities　https://radiflow.com/news/radiflow-offers-new-approach-for-classifying-and-assessing-ot-attack-vulnerabilities/〔参照 2019-05-28〕
S4 Events：A New CVSS For ICS Vulnerabilities　https://www.youtube.com/watch?v=-6cThOCm9co〔参照 2019-05-28〕
※ 25　Dragos, Inc.：Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE　https://dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/〔参照 2019-05-28〕
※ 26　Dark Reading：Triton/Trisis Attack Was More Widespread Than Publicly Known　https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661〔参照 2019-05-28〕
※ 27　SANS Institute：The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns　https://www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505〔参照 2019-05-28〕
※ 28　Infosecurity Magazine：Industrial IoT Enables Attacks in Manufacturing Industry　https://www.infosecurity-magazine.com/news/iiot-enables-attacks-in/〔参照 2019-05-28〕
※ 29　Dark Reading：Cybercrime-as-a-Service: No End in Sight　https://www.darkreading.com/endpoint/cybercrime-as-a-service-no-end-in-sight/a/d-id/1333033〔参照 2019-05-28〕
※ 30　Data Breach Today：Cybercrime Groups and Nation-State Attackers Blur Together　https://www.databreachtoday.com/cybercrime-groups-nation-state-attackers-blur-together-a-11141〔参照 2019-05-28〕
Nine Digital Pty Ltd：Military-grade hacking techniques are now in the hands of amateurs　https://finance.nine.com.au/2018/02/27/11/27/military-hacking-techniques-now-in-the-hands-of-the-masses〔参照 2019-05-28〕
※ 31　ZDNet：Hackers found and cracked this fake electricity substation network in just two days　https://www.zdnet.com/article/hackers-found-and-cracked-this-fake-electricity-substation-network-in-just-two-days/〔参照 2019-05-28〕
※ 32　Director of National Intelligence：Worldwide Threat

Assessment of the US Intelligence Community https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf〔参照2019-05-28〕
National Cybersecurity and Communications Integration Center：Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors https://www.us-cert.gov/ncas/alerts/TA17-293A〔参照 2019-05-28〕
National Cybersecurity and Communications Integration Center：Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors https://www.us-cert.gov/ncas/alerts/TA18-074A〔参照 2019-05-28〕
※ 33 Congress.gov：H.R. 5239 - Cyber Sense Act of 2018 https://www.congress.gov/bill/115th-congress/house-bill/5239〔参照 2019-05-28〕
なお、2019 年 7 月上旬の時点では「H.R. 360 - Cyber Sense Act of 2019」（https://www.congress.gov/bill/116th-congress/house-bill/360〔参照 2019-07-04〕）として審議されている。
Chemical Facility Security News：HR 5239 Introduced – DOE Cyber Sense https://chemical-facility-security-news.blogspot.com/2018/03/hr-5239-introduced-doe-cyber-sense.html〔参照 2019-05-28〕
※ 34 E&E News：DOE to vet grid's ability to reboot after a cyberattack https://www.eenews.net/stories/1060092675〔参照 2019-05-28〕
WIRED：The Hail Mary Plan to Restart a Hacked US Electric Grid https://www.wired.com/story/black-start-power-grid-darpa-plum-island/〔参照 2019-05-28〕
※ 35 Congress.gov：S.79 - Securing Energy Infrastructure Act https://www.congress.gov/bill/115th-congress/senate-bill/79〔参照 2019-05-28〕
なお、2019 年 7 月上旬の時点では「S.174 - Securing Energy Infrastructure Act」（https://www.congress.gov/bill/116th-congress/senate-bill/174〔参照 2019-07-04〕）として審議されており、2019 年 6 月 27 日に他法案（S.1790）の一部として上院を通過している。
Nextgov：Plan to Dumb-Down the Power Grid In Name of Cybersecurity Passes Senate https://www.nextgov.com/cybersecurity/2018/12/plan-dumb-down-power-grid-name-cybersecurity-passes-senate/153719/〔参照 2019-05-28〕
※ 36 Security Affairs：The NATO team is the winner of the cyber defence exercise Locked Shields 2018 https://securityaffairs.co/wordpress/71975/breaking-news/locked-shields-2018.html〔参照 2019-05-28〕
Sydney Morning Herald：Trial run for cyberwar: 'Crimsonia' on the attack in Estonia https://www.smh.com.au/world/europe/trial-run-for-cyberwar-crimsonia-on-the-attack-in-estonia-20180426-p4zbp9.html〔参照 2019-05-28〕
※ 37 Legislation.gov.au：Security of Critical Infrastructure Act 2018 https://www.legislation.gov.au/Details/C2018A00029〔参照 2019-05-28〕
Clayton Utz：Critical information: Are you ready for the Security of Critical Infrastructure Act's January reporting deadline – Part 1 https://www.claytonutz.com/knowledge/2018/september/critical-information-are-you-ready-for-the-security-of-critical-infrastructure-acts-january-reporting-deadline-part-1〔参照 2019-05-28〕
ZDNet：Government passes critical infrastructure national security Bill https://www.zdnet.com/article/government-passes-critical-infrastructure-national-security-bill/〔参照 2019-05-28〕
※ 38 EURACTIV：Commission expects EU countries to set 'high fines' under new cybersecurity law https://www.euractiv.com/section/cybersecurity/news/commission-expects-eu-countries-to-set-high-fines-under-new-cybersecurity-law/〔参照 2019-05-28〕
※ 39 E&E News：Duke agreed to pay record fine for lax security — sources https://www.eenews.net/stories/1060119265〔参照 2019-05-28〕
※ 40 サイバーセキュリティ戦略本部：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 https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf〔参照 2019-05-28〕
※ 41 サイバーセキュリティ戦略本部：サイバーセキュリティ戦略 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf〔参照 2019-05-28〕
※ 42 サイバーセキュリティ戦略本部：サイバーセキュリティ 2018 https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf〔参照 2019-05-28〕
※ 43 NISC：重要インフラの情報セキュリティ対策に関する主な資料 https://www.nisc.go.jp/active/infra/siryou.html〔参照 2019-05-28〕
※ 44 NISC：東京 2020 グループの概要 https://www.nisc.go.jp/active/2020/index.html〔参照 2019-05-28〕
※ 45 NISC：施策① 安全基準等の整備及び浸透 https://www.nisc.go.jp/active/infra/shisaku1.html〔参照 2019-05-28〕
※ 46 IPA：「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を公開 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔参照 2019-05-28〕
※ 47 経済産業省：サイバーセキュリティの現状と経済産業省としての取組 https://www.jssec.org/dl/20180309_Hiroshi_itou.pdf〔参照 2019-05-28〕
※ 48 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 https://www.meti.go.jp/press/2018/01/20190109001/20190109001.html〔参照 2019-05-28〕
※ 49 経済産業省：「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」を取りまとめました https://www.meti.go.jp/press/2018/09/20180903003/20180903003.html〔参照 2019-05-28〕
※ 50 e-Gov：ガス事業法 https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=329AC0000000051#579〔参照 2019-05-28〕
※ 51 Mirai とその亜種が内部に保持する、特定の IoT 機器の初期設定値やその後の変更値として用いられやすい典型的で類推可能なログイン名とパスワードの組み合わせ。
※ 52 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 2019-05-31〕
※ 53 Newsky Security Solutions Inc.：Masuta：Satori Creators' Second Botnet Weaponizes A New Router Exploit. https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7〔参照 2019-05-31〕
※ 54 Satori の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1（3）（d）satori/okiru」（p.164）を参照。
※ 55 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。
※ 56 Exploit Database：D-Link DIR-645 - Multiple UPNP Vulnerabilities https://www.exploit-db.com/exploits/38722〔参照 2019-05-31〕
※ 57 Trend Micro Incorporated：GPON Vulnerabilities Exploited for Mexico-based Mirai-like Scanning Activities https://blog.trendmicro.com/trendlabs-security-intelligence/gpon-vulnerabilities-exploited-for-mexico-based-mirai-like-scanning-activities/〔参照 2019-05-31〕
※ 58 Radware Ltd.：JenX – Los Calvos de San Calvicie https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/〔参照 2019-05-31〕
※ 59 Newsky Security Solutions Inc.：Huawei router exploit involved in Satori and Brickerbot given away for free on Christmas by Blackhat Santa https://blog.newskysecurity.com/huawei-router-exploit-involved-in-satori-and-brickerbot-given-away-for-free-on-christmas-by-ac52fe5e4516〔参照 2019-05-31〕
※ 60 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 2019-05-31〕
※ 61 JVN iPedia：JVNDB-2017-013014 Huawei HG532 における入力確認に関する脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-013014.html〔参照 2019-05-31〕
※ 62 BrickerBot の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1（2）IoT 機器を破壊するウイルス『BrickerBot』」（p.163）を参照。
※ 63 Radware Ltd.：New Satori Botnet Variant Enslaves Thousands of Dasan WiFi Routers https://blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/〔参照 2019-05-31〕
※ 64 JVN iPedia：JVNDB-2017-012245 Dasan GPON ONT WiFi ルータ H640X デバイスにおけるバッファエラーの脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-012245.html〔参照 2019-05-31〕
※ 65 SHODAN：https://www.shodan.io/〔参照 2019-05-31〕
※ 66 Newsky Security Solutions Inc.：CVE-2018–10561 Dasan GPON exploit weaponized in Omni and Muhstik botnets https://blog.newskysecurity.com/cve-2018-10561-dasan-gpon-exploit-weaponized-in-omni-and-muhstik-botnets-ad7b1f89cff3〔参照 2019-05-31〕

※ 67 JVN iPedia：JVNDB-2018-004885 Dasan GPON home router における認証に関する脆弱性 https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-004885.html〔参照 2019-05-31〕
※ 68 JVN iPedia：JVNDB-2018-004886 Dasan GPON home routers におけるコマンドインジェクションの脆弱性 https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-004886.html〔参照 2019-05-31〕
※ 69 Fortinet, Inc.：A Wicked Family of Bots https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html〔参照 2019-05-31〕
※ 70 Exploit Database：Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/43055〔参照 2019-05-31〕
※ 71 Exploit Database：Multiple CCTV-DVR Vendors - Remote Code Execution https://www.exploit-db.com/exploits/39596〔参照 2019-05-31〕
※ 72 JVN iPedia：JVNDB-2016-006166 複数の NETGEAR 製ルータに脆弱性 https://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-006166.html〔参照 2019-05-31〕
※ 73 Qihoo 360 Technology Co. Ltd.：Botnets never Die, Satori REFUSES to Fade Away https://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/〔参照 2019-05-31〕
※ 74 JVN iPedia：JVNDB-2018-006301 XiongMai uc-httpd におけるバッファエラーの脆弱性 https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-006301.html〔参照 2019-05-31〕
※ 75 警察庁：宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスの増加について https://www.npa.go.jp/cyberpolice/detect/pdf/20180613.pdf〔参照 2019-05-31〕
※ 76 NICT：NICTER Blog 80/TCP 宛通信の増加 https://blog.nicter.jp/reports/2018-04/mirai-80/〔参照 2019-05-31〕
※ 77 Exploit Database：D-Link DSL-2750B - OS Command Injection (Metasploit) https://www.exploit-db.com/exploits/44760〔参照 2019-05-31〕
※ 78 Radware Ltd.：Satori IoT Botnet Variant https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/〔参照 2019-05-31〕
※ 79 Palo Alto Networks, Inc.：Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/〔参照 2019-05-31〕
※ 80 JVN iPedia：JVNDB-2016-008586 Eir D1000 モデムにおける認可・権限・アクセス制御に関する脆弱性 https://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-008586.html〔参照 2019-05-31〕
※ 81 JVN iPedia：JVNDB-2015-001591 D-Link DIR-645 Wired/Wireless ルータのファームウェアにおける任意のコマンドを実行される脆弱性 https://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001591.html〔参照 2019-05-31〕
※ 82 Exploit Database：MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution (Metasploit) https://www.exploit-db.com/exploits/41471〔参照 2019-05-31〕
※ 83 Exploit Database：D-Link Devices - UPnP SOAP TelnetD Command Execution (Metasploit) https://www.exploit-db.com/exploits/28333〔参照 2019-05-31〕
※ 84 SSD Secure Disclosure：SSD Advisory – Vacron NVR Remote Command Execution https://ssd-disclosure.com/index.php/archives/3445〔参照 2019-05-31〕
※ 85 JVN iPedia：JVNDB-2010-003392 Camtron CMNC-200 Full HD IP Camera の Linux インストールにおけるアクセスを取得される脆弱性 https://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-003392.html〔参照 2019-05-31〕
※ 86 Exploit Database：ThinkPHP 5.0.23/5.1.31 - Remote Code Execution https://www.exploit-db.com/exploits/45978〔参照2019-05-31〕
※ 87 Trend Micro Incorporated：With Mirai Comes Miori: IoT Botnet Delivered via ThinkPHP Remote Code Execution Exploit https://blog.trendmicro.com/trendlabs-security-intelligence/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit/〔参照 2019-05-31〕
※ 88 Trend Micro Incorporated：ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai https://blog.trendmicro.com/trendlabs-security-intelligence/thinkphp-vulnerability-abused-by-botnets-hakai-and-yowai/〔参照 2019-05-31〕
※ 89 VULDB：Cisco Linksys Router up to E4200 tmUnblock.cgi ttcp_ip privilege escalation https://vuldb.com/?id.12362〔参照 2019-05-31〕
※ 90 Intezar：Intezer Analyze™ ELF Support Release: Hakai Variant Case Study https://www.intezer.com/elf-support-released-hakai-malware/〔参照 2019-05-31〕
※ 91 NICT：Wi-Fi ルータの DNS 情報の書換え後に発生する事象について https://blog.nicter.jp/2018/03/router-dns-hack/〔参照 2019-05-31〕
※ 92 トレンドマイクロ株式会社：不正アプリをダウンロードさせるルータの DNS 設定書き換え攻撃が発生 https://blog.trendmicro.co.jp/archives/17170〔参照 2019-05-31〕
※ 93 piyolog：ルーターの設定情報改ざんについてまとめてみた https://piyolog.hatenadiary.jp/entry/20180328/1522253693〔参照 2019-05-31〕
※ 94 東日本電信電話株式会社：「Netcommunity OG シリーズ」におけるインターネット接続不可事象について https://www.ntt-east.co.jp/info/detail/180328_01.html〔参照 2019-05-31〕
※ 95 西日本電信電話株式会社：「Netcommunity OG シリーズ」におけるインターネット接続不可事象について https://www.ntt-west.co.jp/newscms/notice/7279/20180328.pdf〔参照 2019-05-31〕
※ 96 ロジテック株式会社：インターネット上での接続障害について https://www.logitec.co.jp/info/2018/0402.html〔参照 2019-05-31〕
※ 97 株式会社バッファロー：フェイスブックの機能追加を求めるメッセージが表示される障害について https://www.buffalo.jp/news/detail/20180405-01.html〔参照 2019-05-31〕
※ 98 NEC プラットフォームズ株式会社：不正なアプリのダウンロード案内がされる事象について http://www.aterm.jp/support/tech/2018/0406.html〔参照 2019-05-31〕
※ 99 株式会社アイ・オー・データ機器：不正なアプリのダウンロード案内が表示される事象について https://www.iodata.jp/support/information/2018/facebook_app/〔参照 2019-05-31〕
※ 100 ニフティ株式会社：@ niftyADSL 接続サービス インターネットに接続できない事象について https://support.nifty.com/cs/suptopics/detail/180426479514/1.htm〔参照 2019-05-31〕
※ 101 Trend Micro Incorporated：Not Only Botnets: Hacking Group in Brazil Targets IoT Devices With Malware https://blog.trendmicro.com/trendlabs-security-intelligence/not-only-botnets-hacking-group-in-brazil-targets-iot-devices-with-malware/〔参照 2019-05-31〕
※ 102 Fortinet, Inc.：OMG: Mirai-based Bot Turns IoT Devices into Proxy Servers https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html〔参照 2019-05-31〕
※ 103 Qihoo 360 Technology Co. Ltd.：Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading https://blog.netlab.360.com/early-warning-adb-miner-a-mining-botnet-utilizing-android-adb-is-now-rapidly-spreading-en/〔参照 2019-05-31〕
※ 104 Qihoo 360 Technology Co. Ltd.：ADB.Miner: More Information https://blog.netlab.360.com/adb-miner-more-information-en/〔参照 2019-05-31〕
※ 105 Trend Micro Incorporated：Open ADB Ports Being Exploited to Spread Possible Satori Variant in Android Devices https://blog.trendmicro.com/trendlabs-security-intelligence/open-adb-ports-being-exploited-to-spread-possible-satori-variant-in-android-devices/〔参照 2019-05-31〕
※ 106 Qihoo 360 Technology Co. Ltd.：Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing Wallet Address https://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/〔参照 2019-05-31〕
※ 107 Bleeping Computer：Satori Botnet Is Now Attacking Ethereum Mining Rigs https://www.bleepingcomputer.com/news/security/satori-botnet-is-now-attacking-ethereum-mining-rigs/〔参照 2019-05-31〕
※ 108 警察庁：仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20180312.pdf〔参照 2019-05-31〕
※ 109 Cisco Systems, Inc.：New VPNFilter malware targets at least 500K networking devices worldwide https://blog.talosintelligence.com/2018/05/VPNFilter.html〔参照 2019-05-31〕
※ 110 JPCERT/CC：ネットワーク機器を標的とするマルウェア「VPNFilter」について https://www.jpcert.or.jp/newsflash/2018052401.html〔参照 2019-05-31〕
※ 111 Cisco Systems, Inc.：VPNFilter Update - VPNFilter exploits endpoints, targets new devices https://blog.talosintelligence.com/2018/06/vpnfilter-update.html〔参照 2019-05-31〕
※ 112 Trend Micro Incorporated：VPNFilter-affected Devices Still Riddled with 19 Vulnerabilities https://blog.trendmicro.com/

trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities/〔参照 2019-05-31〕
※ 113 Reaperの詳細に関しては、「情報セキュリティ白書2018」の「3.1.1 (3) (b)Reaper」(p.164)を参照。
※ 114 JVN iPedia：JVNDB-2015-006966 QNAP Signage Station に同梱されている iArtist Lite の FTP サービスにおけるアクセス権を取得される脆弱性 https://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-006966.html〔参照 2019-05-31〕
※ 115 JVN iPedia：JVNDB-2011-003481 D-Link DIR-300 ルータにおける重要な情報を取得される脆弱性 https://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-003481.html〔参照 2019-05-31〕
※ 116 JVN iPedia：JVNDB-2014-007550 複数の ASUS ルータで使用される WRT ファームウェアにおける認証を回避される脆弱性 https://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-007550.html〔参照 2019-05-31〕
※ 117 Exploit Database：Linksys E1500/E2500 - Multiple Vulnerabilities https://www.exploit-db.com/exploits/24475〔参照 2019-05-31〕
※ 118 JVN iPedia：JVNDB-2013-001349 MiniUPnP MiniUPnPd の SSDP ハンドラにおけるサービス運用妨害 (サービスクラッシュ) の脆弱性 https://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001349.html〔参照 2019-05-31〕
※ 119 JVN iPedia：JVNDB-2013-001350 MiniUPnP MiniUPnPd の HTTP サービスにおけるスタックベースのバッファオーバーフローの脆弱性 https://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001350.html〔参照 2019-05-31〕
※ 120 JVN iPedia：JVNDB-2017-002695 QNAP QTS における任意のコマンドを実行される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002695.html〔参照 2019-05-31〕
※ 121 JVN iPedia：JVNDB-2017-003778 ASUS RT-AC* および RT-N* デバイスのファームウェアにおける JSONP 情報を公開される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-003778.html〔参照 2019-05-31〕
※ 122 JVN iPedia JVNDB-2017-001263 複数の NETGEAR デバイス製品におけるパスワードを公開される脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-001263.html〔参照 2019-05-31〕
※ 123 JVN iPedia：JVNDB-2012-005922 Portable SDK for UPnP Devices におけるスタックベースのバッファオーバーフローの脆弱性 https://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-005922.html〔参照 2019-05-31〕
※ 124 JVN iPedia：JVNDB-2012-005923 Portable SDK for UPnP Devices におけるスタックベースのバッファオーバーフローの脆弱性 https://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-005923.html〔参照 2019-05-31〕
※ 125 Exploit Database：D-Link DIR-600 / DIR-300 (Rev B) - Multiple Vulnerabilities https://www.exploit-db.com/exploits/24453〔参照 2019-05-31〕
※ 126 JVN iPedia：JVNDB-2017-002139 ASUS RT-AC53 デバイス上で稼動する ASUSWRT の httpd におけるセッションをハイジャックされる脆弱性 https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002139.html〔参照 2019-05-31〕
※ 127 Exploit Database：Cisco Linksys E4200 - Multiple Vulnerabilities https://www.exploit-db.com/exploits/25292〔参照 2019-05-31〕
※ 128 Security NEXT：水位監視カメラ２台に不正アクセス、制御不能に - 八千代市 http://www.security-next.com/092716〔参照 2019-05-31〕
※ 129 ScanNetSecurity：河川監視カメラへ不正アクセス、「I'm hacked.bye2」のメッセージ残す（上尾市） https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html〔参照 2019-05-31〕
※ 130 産経新聞：監視カメラに不正アクセス キヤノン製、60台以上被害 セキュリティーに弱点 https://www.sankei.com/affairs/news/180507/afr1805070007-n1.html〔参照 2019-05-31〕
※ 131 キヤノン株式会社：ネットワークカメラの不正アクセス防止対策について https://cweb.canon.jp/caution/180426.html〔参照 2019-05-31〕
※ 132 朝日新聞：監視カメラ乗っ取りからかう 容疑の元自衛官を書類送検 https://digital.asahi.com/articles/ASLCN4K50LCNPIHB01F.html〔参照 2019-05-31〕
※ 133 piyolog：監視カメラへの不正アクセスについて調べてみた https://piyolog.hatenadiary.jp/entry/20180428/1524936297〔参照 2019-05-31〕
※ 134 Trend Micro Incorporated：Device Vulnerabilities in the Connected Home: Uncovering Remote Code Execution and More https://blog.trendmicro.com/trendlabs-security-intelligence/device-vulnerabilities-connected-home-remote-code-execution-and-more/〔参照 2019-05-31〕
※ 135 総務省：IoT 機器に関する脆弱性調査等の実施結果の公表 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000154.html〔参照 2019-05-31〕
※ 136 総務省：重要インフラ等で利用される IoT 機器の調査 http://www.soumu.go.jp/main_content/000561906.pdf〔参照 2019-05-31〕
※ 137 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2019-05-31〕
※ 138 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 2019-05-31〕
※ 139 IPA：「IoT 開発におけるセキュリティ設計の手引き」を公開 https://www.ipa.go.jp/security/iot/iotguide.html〔参照 2019-05-31〕
※ 140 JNSA：IoT セキュリティガイド 標準／ガイドライン ハンドブック 2017 年度版 https://www.jnsa.org/result/iot/2018.html〔参照 2019-05-31〕
※ 141 JPCERT/CC：工場における産業用 IoT 導入のためのセキュリティファーストステップ https://www.jpcert.or.jp/ics/information06.html〔参照 2019-05-31〕
※ 142 CCDS：協議会・研究会公開資料 https://www.ccds.or.jp/public_document/index.html〔参照 2019-05-31〕
※ 143 JSSEC：『IoT セキュリティチェックシート』 https://www.jssec.org/iot〔参照 2019-05-31〕
※ 144 NIST：NISTIR 8228 (DRAFT) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks https://csrc.nist.gov/publications/detail/nistir/8228/draft〔参照 2019-05-31〕
※ 145 NIST：NISTIR 8200 Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf〔参照 2019-05-31〕
※ 146 NIST：Considerations for a Core IoT Cybersecurity Capabilities Baseline https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf〔参照 2019-05-31〕
※ 147 OWASP：Internet of Things (IoT) Top 10 2018 https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf〔参照 2019-05-31〕
※ 148 ENISA：Towards secure convergence of Cloud and IoT https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot〔参照 2019-05-31〕
※ 149 ENISA：Good Practices for Security of Internet of Things in the context of Smart Manufacturing https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot〔参照 2019-05-31〕
※ 150 ENISA：IoT Security Standards Gap Analysis https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis〔参照 2019-05-31〕
※ 151 Department for DCMS, UK：Secure by Design https://www.gov.uk/government/collections/secure-by-design〔参照 2019-05-31〕
※ 152 German Federal Office for Information Security：BSI TR-03148:Secure Broadband Routers Version 1.0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf〔参照 2019-05-31〕
※ 153 https://notice.go.jp/〔参照 2019-05-31〕
※ 154 総務省・NICT：IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施 https://www.nict.go.jp/press/2019/02/01-1.html〔参照 2019-05-31〕
※ 155 IPA：安心相談窓口だより 宅配便業者をかたる偽ショートメッセージに関する相談が急増中 https://www.ipa.go.jp/security/anshin/mgdayori20180808.html〔参照 2019-05-31〕
※ 156 IPA：安心相談窓口だより 宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に https://www.ipa.go.jp/security/anshin/mgdayori20181129.html〔参照 2019-05-31〕
※ 157 IPA：安心相談窓口だより 宅配便業者をかたる偽ショートメッセージで、また新たな手口が出現 https://www.ipa.go.jp/security/anshin/mgdayori20190320.html〔参照 2019-05-31〕
※ 158 「情報セキュリティ白書 2018」の「3.3.2 SMS から不正アプリをインストールさせる手口」(p.176)参照。
※ 159 構成プロファイル：iOS において各種設定を自動で行えるファイルのこと。
※ 160 Symantec Corporation：アプリに偽装したマルウェア、Google Play ストアで発見 https://www.symantec.com/connect/ja/blogs/google-play-11?om_ext_cid=biz_social_APJ_twitter_Asset%20Type%20%20-%20Blog,Region%20-%20APJ〔参照 2019-05-31〕

※ 161 Symantec Corporation：悪質なアドウェアを含む詐欺アプリを Google Play で確認　https://www.symantec.com/connect/ja/blogs/google-play-12?om_ext_cid=biz_social_APJ_twitter_Asset%20Type%20%20-%20Blog,Region%20-%20APJ〔参照 2019-05-31〕
※ 162 トレンドマイクロ株式会社：Google Play で複数の偽音声アプリを確認、ボットネット構築機能の追加が予想される　https://blog.trendmicro.co.jp/archives/19996〔参照 2019-05-31〕
※ 163 トレンドマイクロ株式会社：Google Play にアドウェアを含む偽アプリ、既に 900 万回ダウンロード　https://blog.trendmicro.co.jp/archives/20079〔参照 2019-05-31〕
※ 164 トレンドマイクロ株式会社：モバイルバンキングを狙う不正アプリ「Anubis」を Google Play で確認、モーションセンサーを利用して検出を回避　https://blog.trendmicro.co.jp/archives/20168〔参照 2019-05-31〕
※ 165 サンドボックス環境：外部から受信したプログラムを動作させても影響がない、保護された環境のこと。仮想環境等で構築される。
※ 166 モーションセンサー：機器内部に搭載され、加速度・傾き等を検出する装置の総称。例えば、スマートフォンを横向きにするとディスプレイに表示されている画面も自動的に横向きになるのは、モーションセンサーの働きによる。
※ 167 livedoor NEWS：心拍数計測と見せかけ、Touch ID で約 1 万円を課金する詐欺アプリが出現　http://news.livedoor.com/article/detail/15679835/〔参照 2019-05-31〕
※ 168 経済産業省：サイバーセキュリティ経営ガイドライン Ver2.0(2017 年)　https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔参照 2019-06-21〕
※ 169 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
※ 170 トレンドマイクロ株式会社：韓国を狙うサプライチェーン攻撃「Red Signature 作戦」について解説　https://blog.trendmicro.co.jp/archives/19475〔参照 2019-06-21〕
※ 171 Kaspersky Lab：Kaspersky Lab、サプライチェーン攻撃手法を利用した APT「ShadowHammer」を発見　https://www.kaspersky.co.jp/about/press-releases/2019_vir29032019〔参照 2019-06-21〕
※ 172 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 2019-06-21〕
※ 173 東京地裁平成 26 年 1 月 23 日判決（平成 23（ワ）32060）
※ 174 ファーストサーバ株式会社：調査報告書（最終報告書）＜要約版＞　https://www.firstserver.co.jp/pdf/effort/fs-report.pdf〔参照 2019-06-21〕
※ 175 びあ株式会社：び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　https://corporate.pia.jp/news/files/security_incident20170425.pdf〔参照 2019-06-21〕
※ 176 前橋市教育委員会：前橋市学校教育ネットワークセキュリティ調査対策検討委員（第三者委員会）の検証報告書を掲載します https://www.city.maebashi.gunma.jp/kosodate_kyoiku/3/6/15782.html〔参照 2019-06-21〕
※ 177 個人情報保護委員会：～ウェブサイトを運営している事業者の皆様への注意喚起～　https://www.ppc.go.jp/files/pdf/20180628_warning.pdf〔参照 2019-06-21〕
※ 178 JPCERT/CC：Web サイトへのサイバー攻撃に備えて 2018 年 7 月　https://www.jpcert.or.jp/newsflash/2018071801.html〔参照 2019-06-21〕
※ 179 株式会社横浜銀行：業務委託先従業員の逮捕について　https://www.boy.co.jp/news/oshirase/__icsFiles/afieldfile/2014/02/05/Oshirase_260205-2.pdf〔参照 2019-06-21〕
※ 180 株式会社ベネッセホールディングス：事故の概要　https://www.benesse.co.jp/customer/bcinfo/01.html〔参照 2019-06-21〕
※ 181 日本年金機構における業務委託のあり方等に関する調査委員会：日本年金機構における業務委託のあり方等に関する調査委員会報告書 https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000210080.pdf〔参照 2019-06-21〕
※ 182 AGS 株式会社：受託業務における契約および法令違反のご報告とお詫び　https://www.ags.co.jp/topics/pdf/20190108_news_release.pdf〔参照 2019-06-21〕
※ 183 個人情報保護委員会：特定個人情報の取扱いの委託における注意喚起　https://www.ppc.go.jp/news/careful_information/itaku/〔参照 2019-06-21〕
※ 184 IPA：組織における内部不正防止ガイドライン　https://www.ipa.go.jp/security/fy24/reports/insider/〔参照 2019-06-21〕
※ 185 NISC：サイバーセキュリティ戦略　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔参照 2019-06-21〕
※ 186 NISC：「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（平成 28 年度版）」について　https://www.nisc.go.jp/active/general/kijun28.html〔参照 2019-06-21〕
※ 187 経済産業省：アウトソーシングに関する情報セキュリティ対策ガイダンス　https://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf〔参照 2019-06-21〕
※ 188 JASA：サプライチェーン情報セキュリティ管理基準　http://www.jasa.jp/information/result.html?key=2011&result=%E7%B5%8C%E6%B8%88%E7%94%A3%E6%A5%AD%E7%9C%81%E5%8F%97%E8%A8%97%E4%BA%8B%E6%A5%AD〔参照 2019-06-21〕
※ 189 NISC:外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書　https://www.nisc.go.jp/active/general/pdf/risktaiou28.pdf〔参照 2019-06-21〕
※ 190 経済産業省：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 2013 年度版　https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf〔参照 2019-06-21〕
※ 191 総務省：クラウドサービス提供における情報セキュリティ対策ガイドライン　http://www.soumu.go.jp/main_content/000283647.pdf〔参照 2019-06-21〕
※ 192 https://www.mhlw.go.jp/shingi/2008/07/dl/s0730-18l.pdf〔参照 2019-06-21〕
※ 193 総務省：「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」の公表　http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html〔参照 2019-06-21〕
※ 194 https://www.ipa.go.jp/files/000072150.pdf〔参照 2019-06-21〕
※ 195 管理された非格付け情報（Controlled Unclassified Information）：米国連邦政府機関ごとに定められた重要情報。
※ 196 NIST：NIST Special Publication 800-171 Revision 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations　http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf〔参照 2019-06-21〕
※ 197 NIST：Framework for Improving Critical Infrastructure Cybersecurity Version 1.1　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf〔参照 2019-06-21〕
※ 198 一般財団法人安全保障貿易情報センター：米国国防権限法 2019 の概要　http://www.cistec.or.jp/service/uschina/5-ndaa2019_gaiyou.pdf〔参照 2019-06-21〕
※ 199 IPA：情報セキュリティに関するサプライチェーンリスクマネジメント調査－調査報告書－　https://www.ipa.go.jp/files/000058299.pdf〔参照 2019-06-21〕
※ 200 IPA：「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について　https://www.ipa.go.jp/security/fy30/reports/scrm/index.html〔参照 2019-06-21〕
※ 201 見やすくするため、以降のグラフでは、項目名を一部省略している。省略していない項目名については「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査 調査報告書」参照。
※ 202 EU：Document 32016R0679　https://eur-lex.europa.eu/eli/reg/2016/679/oj〔参照 2019-06-21〕
※ 203 総務省：情報通信白書 28 年版 人工知能（AI）研究の歴史 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc142120.html〔参照 2019-06-21〕
※ 204 IPA：AI 白書 2019 第 5 章 AI の社会実装課題と対策
※ 205 いわゆる汎用人工知能が人間の知性を凌駕するシンギュラリティがリスクとして議論されることがあるが、本稿ではこの課題は扱わない。
※ 206 IEEE：ETHICALLY ALIGNED DESIGN, v2　https://ethicsinaction.ieee.org/〔参照 2019-06-21〕
※ 207 IEEE：IEEE P7000 Working Group　http://sites.ieee.org/sagroups-7000/〔参照 2019-06-21〕
※ 208 ISO：Standards catalogue ISO/IEC JTC 1/SC 42 Artificial intelligence　https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0〔参照 2019-06-21〕
※ 209 EC：Ethics guidelines for trustworthy AI　https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai〔参照 2019-06-21〕
※ 210 内閣官房：人間中心のAI社会原則会議　https://www.cas.go.jp/jp/seisaku/jinkouchinou/〔参照 2019-06-21〕
※ 211 外務省：G20（金融・世界経済に関する首脳会合）　https://www.mofa.go.jp/mofaj/ecm/it/page4_005041.html〔参照 2019-06-21〕
※ 212 Google LLC：AI at Google: our principles　https://www.

blog.google/technology/ai/ai-principles/〔参照 2019-06-21〕
※ 213 Microsoft 社：Microsoft AI principles https://www.microsoft.com/en-us/ai/our-approach-to-ai〔参照 2019-06-21〕
※ 214 IBM 社：Everyday Ethics for Artificial Intelligence https://medium.com/design-ibm/everyday-ethics-for-artificial-intelligence-75e173a9d8e8〔参照 2019-06-21〕
※ 215 国立研究開発法人科学技術振興機構 研究開発戦略センター：（戦略プロポーザル）AI 応用システムの安全性・信頼性を確保する新世代ソフトウェア工学の確立／ CRDS-FY2018-SP-03 https://www.jst.go.jp/crds/report/report01/CRDS-FY2018-SP-03.html〔参照 2019-06-21〕
※ 216 AI プロダクト品質保証コンソーシアム：AI プロダクト品質保証ガイドライン http://www.qa4ai.jp/QA4AI.Guideline.201905.pdf〔参照 2019-06-21〕
※ 217 情報処理学会：小川，島，機械学習システムのトラスト構築に関する課題分析，研究報告セキュリティ心理学とトラスト，2019-SPT32, Vol.21, 1-6, Feb. 2019 https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=194947&item_no=1〔参照 2019-06-21〕
※ 218 WatchGuard：機械学習によるマルウェア検知をめぐるセキュリティ業界とハッカーの戦い https://www.watchguard.co.jp/security-news/%E6%A9%9F%E6%A2%B0%E5%AD%A6%E7%BF%92%E3%81%AB%E3%82%88%E3%82%8B%E3%83%9E%E3%83%AB%E3%82%A6%E3%82%A7%E3%82%A2%E6%A4%9C%E7%9F%A5%E3%82%92%E3%82%81%E3%81%90%E3%82%8B%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA.html〔参照 2019-06-21〕
※ 219 日本銀行金融研究所：宇根 Discussion Paper No.2018-J-16 機械学習システムのセキュリティに関する研究動向と課題 http://www.imes.boj.or.jp/research/papers/japanese/18-J-16.pdf〔参照 2019-06-21〕
※ 220 ICLR：Proceedings of ICLR2015, Goodfellow et al., EXPLAINING AND HARNESSING ADVERSARIAL EXAMPLES https://arxiv.org/pdf/1412.6572.pdf〔参照 2019-06-21〕
※ 221 AI の透明性、すなわち学習や分析の経緯について説明可能にすることが懸案となり、議論が始まっている。一方で、それが攻撃者の解析を容易にしてしまう可能性もあると考えられる。これについても別途議論が必要である。
※ 222 ACM：Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communication Security, 2015, Fredrikson et al., Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf〔参照 2019-06-21〕
※ 223 チャットボット：ユーザのメッセージに対話形式で自動応答する AI ソフトウェア。
※ 224 TechCrunch：Microsoft silences its new A.I. bot Tay, after Twitter users teach it racism [Updated] https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/〔参照 2019-06-21〕
※ 225 学習モデルの知的財産としての扱い等も別途検討すべき重要課題である。例えば「AI 白書 2019」の p.354 ～ p.361 参照。
※ 226 トレンドマイクロ株式会社：2019 年セキュリティ脅威予測 https://resources.trendmicro.com/jp-docdownload-form-m099-web-2019prediction.html〔参照 2019-06-21〕
Symantec Corporation：2019 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 2019-06-21〕
※ 227 IBM 社：DeepLocker: How AI Can Power a Stealthy New Breed of Malware https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/〔参照 2019-06-21〕
※ 228 ディープフェイク:機械学習を利用した人物画像の合成技術を指す。ディープラーニングとフェイクを組み合わせた造語。
※ 229 DGLAB HAUS：ディープフェイク動画の衝撃、AI で作られる「高品質なデマ」 https://media.dglab.com/2019/02/11-afp-01-6/〔参照 2019-06-21〕
※ 230 CNET Japan：広まる「ディープフェイク」の脅威 -- 虚実の分からない世界が到来する https://japan.cnet.com/article/35135448/〔参照 2019-06-21〕
※ 231 日本経済新聞：米議会、AI 使った偽動画を調査へ 大統領選への影響懸念 https://www.nikkei.com/article/DGXMZO45750070W9A600C1000000/〔参照 2019-06-21〕
※ 232 総務省：プラットフォームサービスに関する研究会中間報告書（案） http://www.soumu.go.jp/main_content/000615674.pdf〔参照 2019-06-21〕

付録

資料･ツール

資料A　2018年のコンピュータウイルス届出状況

IPA が 2018 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

2018 年の年間届出件数は、前年の 1,918 件より 803 件（41.9%）少ない 1,115 件となった（図 A-1）。

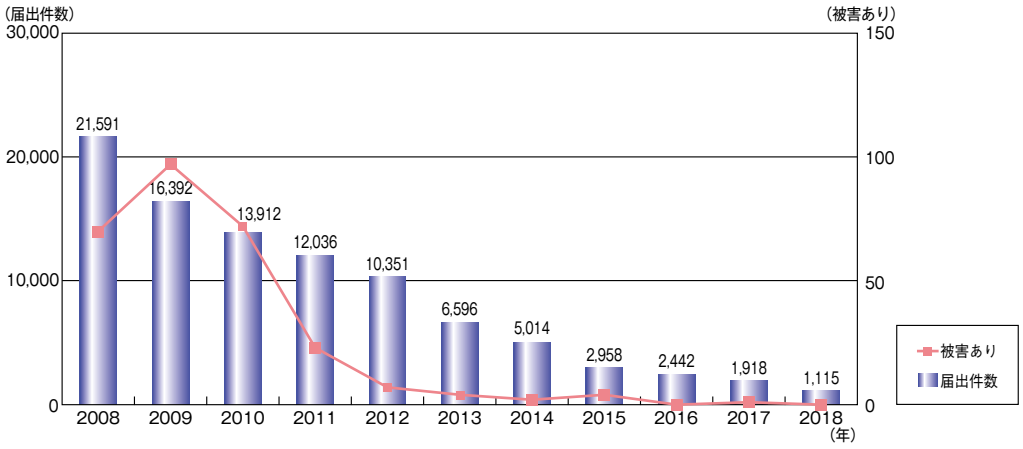
A.2　届出ウイルス

2018 年に届出を受け付けたウイルスのうち、届出数の多いウイルスは上位から、W32/Mydoom（2,026 個）、W32/Bagle（1,811 個）、W32/Netsky（684 個）であった（図 A-2）。

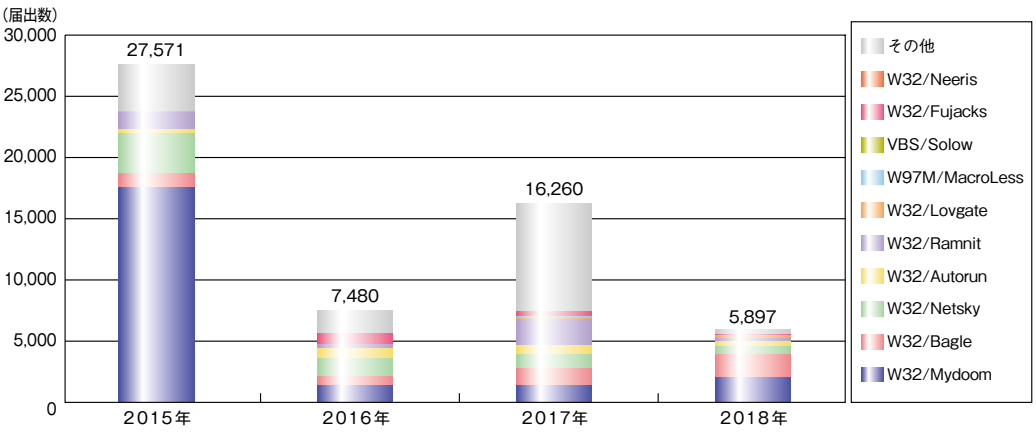
W32/Mydoom は、前年の 1,325 個より 701 多い 2,026 個、W32/Bagle は、前年の 1,460 個より 351 多い 1,811 個となり、どちらも増加した。

また、W32/Netsky については前年の 1,108 個より、424 少ない 684 個となり、減少した。

その他に W32/Neeris が前年の 0 個から、28 個の届出があった。



■図 A-1　ウイルス届出件数の年別推移（2008 ～ 2018 年）



■図 A-2　ウイルス別届出数の年別推移（2015 ～ 2018 年）

参照

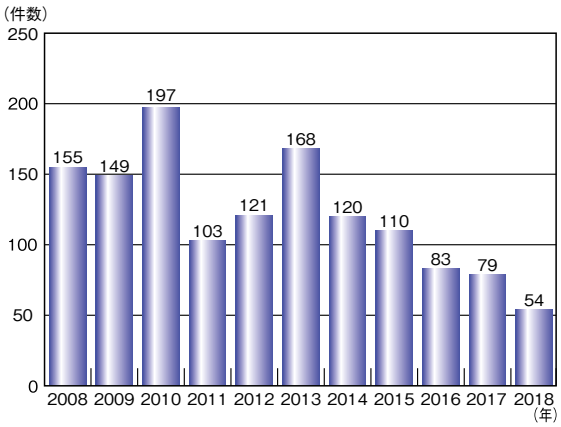
■コンピュータウイルス・不正アクセスの届出状況［2018年10月～12月］
https://www.ipa.go.jp/security/outline/todokede-j.html

資料B　2018年のコンピュータ不正アクセス届出状況

IPA が 2018 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

2018 年の年間届出件数は 54 件となり、2017 年の届出件数 79 件から 25 件（31.6%）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（2008 ～ 2018 年）

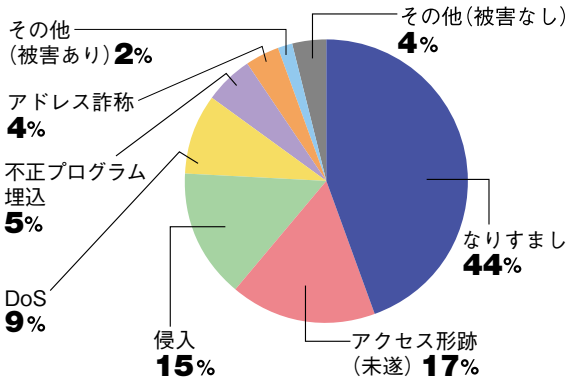
B.2　届出種別

前年と比較すると、「その他（被害あり）」が 18 件から 1 件に減少（94.4% 減）した一方で、「なりすまし」が 15 件から 24 件に増加（60% 増）している（表 B-1）。

届出種別		2018年	2017年	2016年
被害あり	侵入	8	7	4
	メール不正中継	0	2	1
	ワーム感染	0	0	0
	DoS（サービス妨害）	5	6	7
	アドレス詐称	2	0	0
	なりすまし	24	15	30
	不正プログラム埋込	3	6	5
	その他（被害あり）	1	18	14
被害なし	アクセス形跡（未遂）	9	22	19
	ワーム形跡	0	0	0
	その他（被害なし）	2	3	3
合計（件）		54（43）	79（54）	83（61）

※合計のカッコ内の数字は、被害ありの届出種別の合計を示している。

■表 B-1　2018 年不正アクセス届出種別



■図 B-2　2018 年不正アクセス届出種別

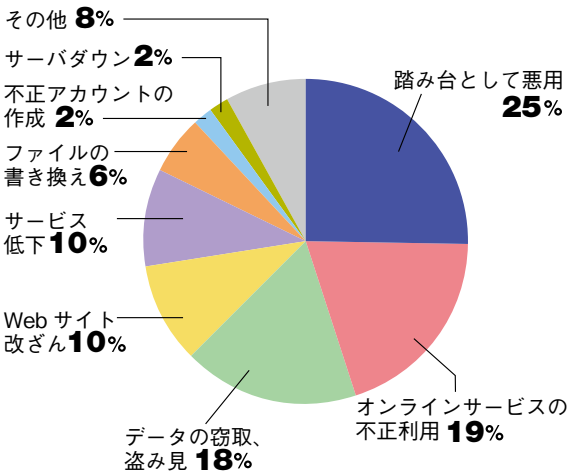
B.3　被害内容

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 24 件（32%）減少した（表 B-2）。

被害内容	2018年	2017年	2016年
メール不正中継	0	5	1
サーバダウン	1	0	0
不正アカウントの作成	1	2	0
Web サイト改ざん	5	12	9
パスワードファイルの盗用	0	0	0
サービス低下	5	9	7
オープンプロキシ	0	0	0
ファイルの書き換え	3	6	2
踏み台として悪用	13	7	13
オンラインサービスの不正利用	10	0	17
データの窃取、盗み見	9	11	5
その他	4	23	16
合計（件）	51（※）	75（※）	70（※）

※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。

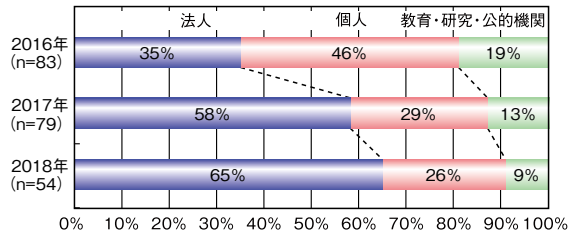
■表 B-2　2018 年不正アクセス被害内容



■図 B-3　2018 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」「個人」「教育・研究・公的機関」からの届出件数について、いずれも減少した。割合で見ると、「法人」からの届出の割合が更に高くなった（図 B-4）。



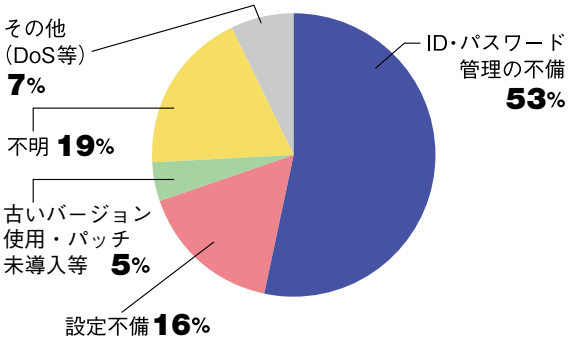
■図 B-4　不正アクセス届出者推移（2016 ～ 2018 年）

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 23 件（53%）と最も多く、次いで「設定不備」が 7 件（16%）等であった（表 B-3、図 B-5）。

被害原因	2018年	2017年	2016年
ID・パスワード管理の不備	23	20	26
設定不備	7	7	7
古いバージョン使用・パッチ未導入等	2	10	4
不明	8	11	15
その他（DoS 等）	3	6	9
合計（件）	43	54	61

■表 B-3　2018 年不正アクセス届出被害原因



■図 B-5　2018 年不正アクセス届出被害原因

B.6 対策情報

2018 年の届出において、被害原因では、「ID・パスワード管理の不備」が 23 件（前年 20 件）と依然大きな割合を占めている。複雑なパスワードを設定する、二段階認証等のセキュリティオプションを採用するといった適切なアカウント管理とリスクへの対策が望まれる。

参照

■コンピュータウイルス・不正アクセスの届出状況［2018年10月～12月］
https://www.ipa.go.jp/security/outline/todokede-j.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

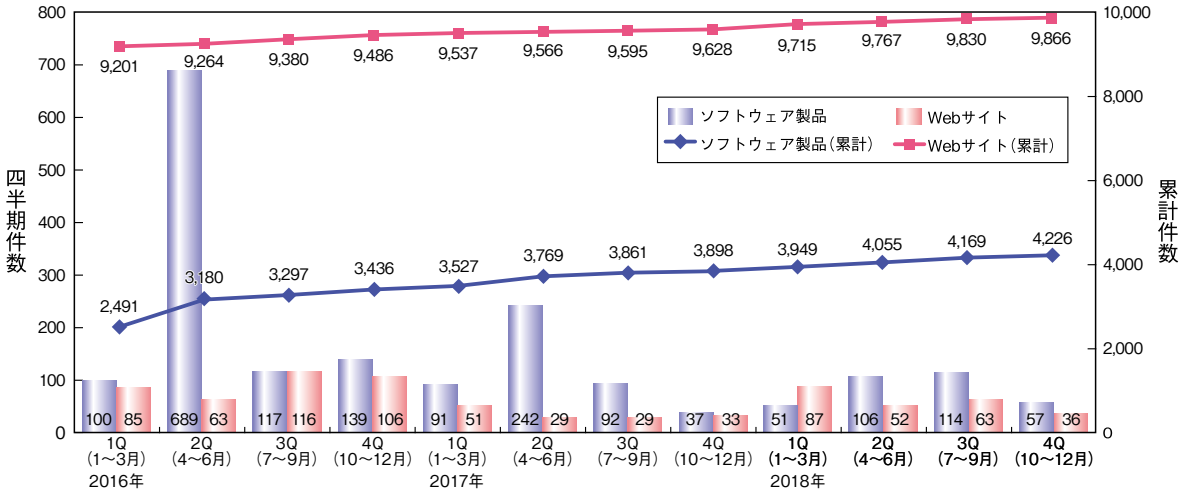
IPA が受け付けた脆弱性関連情報に関する届け出は、2018年末までに1万4,092件に達した。

C.1　脆弱性の届出概況

2018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4,226件、Webサイトに関するもの9,866件、合計1万4,092件で、Webサイトに関する届出が全体の70%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、2018年第4四半期末時点で3.99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

2017年1Q (1~3月)	2017年2Q (4~6月)	2017年3Q (7~9月)	2017年4Q (10~12月)	2018年1Q (1~3月)	2018年2Q (4~6月)	2018年3Q (7~9月)	2018年4Q (10~12月)
4.21	4.21	4.17	4.11	4.08	4.06	4.03	3.99

■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）

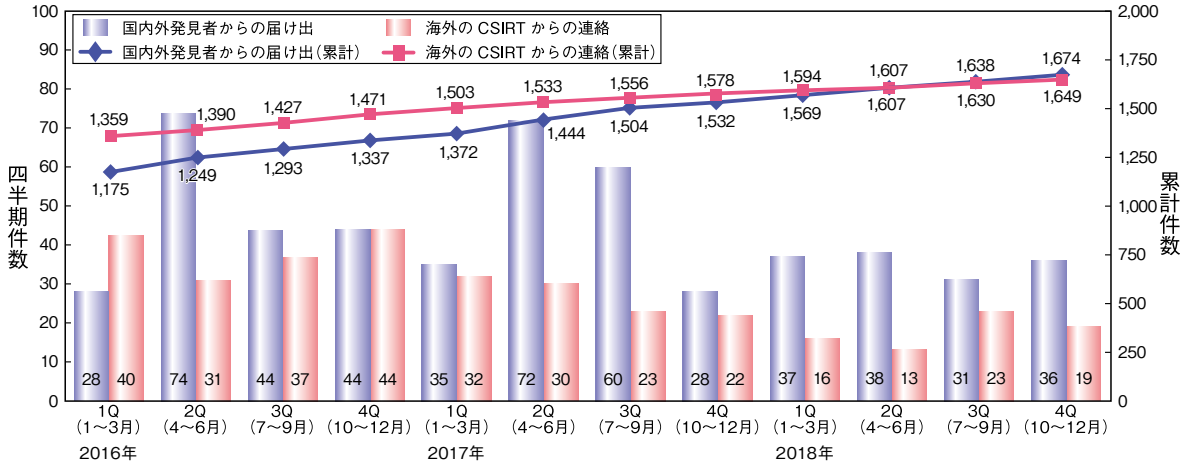
C.2　ソフトウェア製品の脆弱性の処理状況届出種別

2018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1,936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39件、製品開発者が脆弱性ではないと判断したものは95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472件で、これらの取り扱いを終了したものの合計は2,542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1,649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(次ページ)に示す。

分類		累計件数
修正完了	公表済み	1,936件
	個別対応	39件
脆弱性ではない		95件
不受理		472件
合計		2,542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

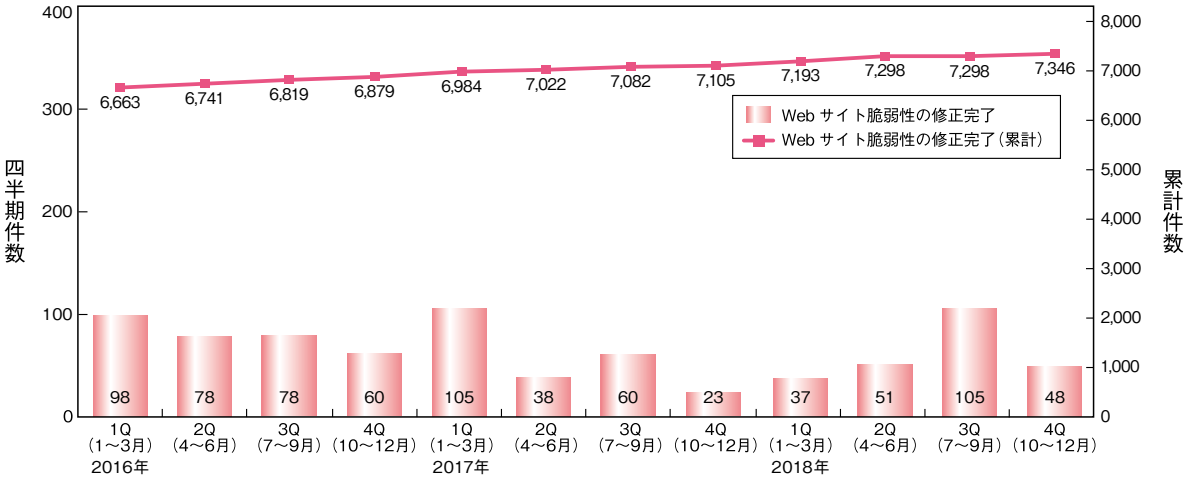
C.3 Webサイトの脆弱性の処理状況

2018 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 7,346 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 621 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 207 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 251 件で、これらの取り扱いを終了したものの合計は 9,555 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	7,346件
注意喚起	1,130件
脆弱性ではない	621件
取扱不能	207件
不受理	251件
合計	9,555件

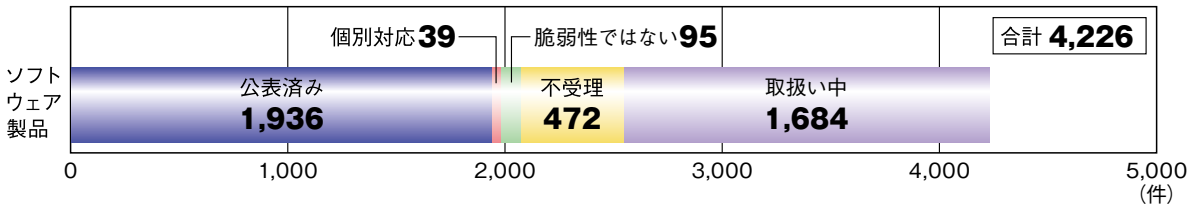
■表 C-3　Web サイトの脆弱性の終了件数



■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

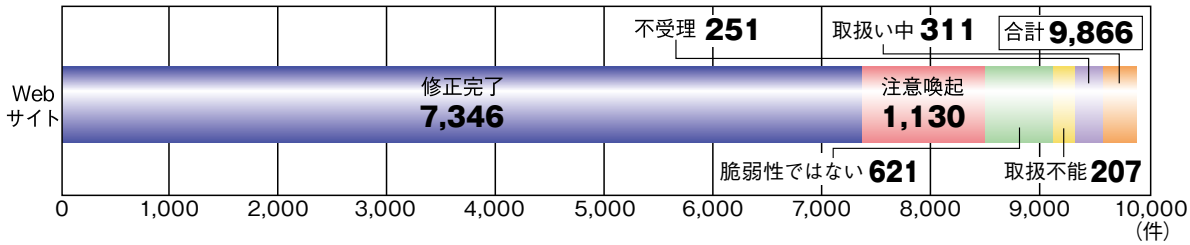
ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。



■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［2018年第4四半期（10月～12月）］
https://www.ipa.go.jp/files/000071102.pdf

ツール1

簡単な設問で自社のセキュリティレベルが分かる診断テスト
https://www.ipa.go.jp/security/benchmark/

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。

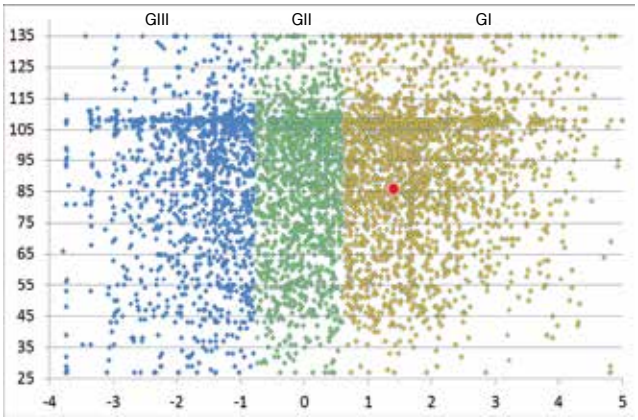
本ツールは、インターネットを通じてウェブページ上の設問に答えるだけで、他社と比較した自社のセキュリティレベルを診断できます。簡単な操作で自社の現状を把握し、取り組みの道筋を見つけることからスタートできます。

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

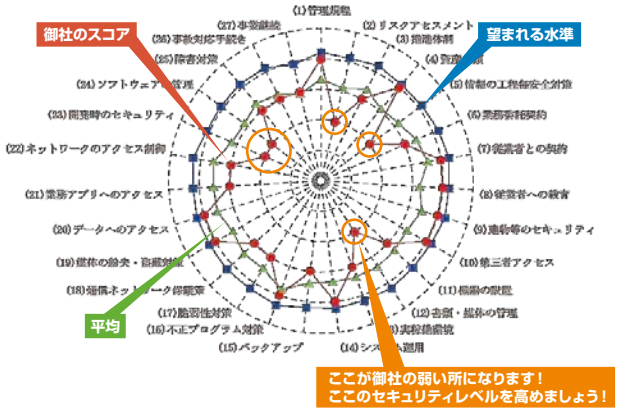
情報セキュリティリスク指標とは、従業員数、売上高、重要情報の保有数、IT依存度などから計算される企業が抱えるリスクを表す指標のことです。情報セキュリティ対策ベンチマークでは、情報セキュリティリスク指標の値の高い順に、以下の3つのグループのいずれかに分類しています。

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2

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。

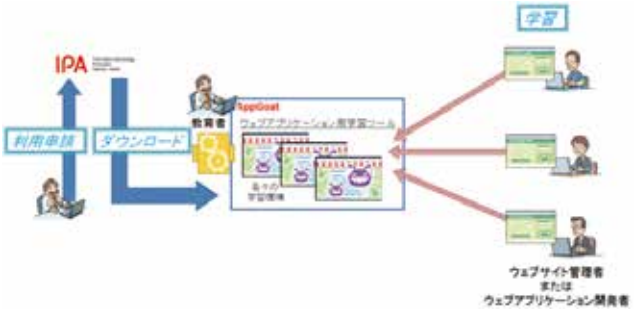
・ウェブアプリケーション用学習ツール（集合学習モード）（図１参照）

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

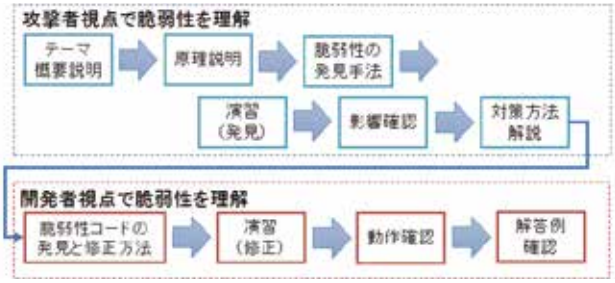
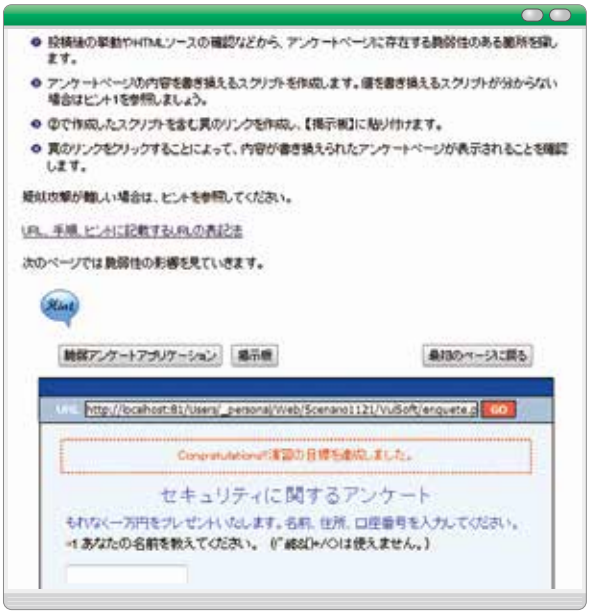


図3. 演習（発見）の画面イメージ



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3

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。2019年3月時点で約97,000件の情報があり、データは日々増え続けています。

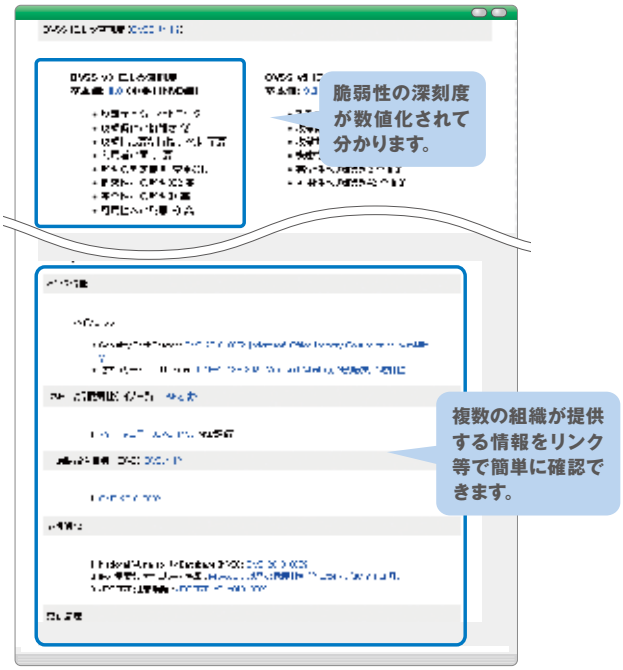
JVN iPediaでは、これだけの量のデータから目的の脆弱性を探索するために検索機能やRSS※配信機能を備えています。「特定の製品に存在する脆弱性を確認したい」、「JVN・他組織で公開される情報をもとに脆弱性対策を調べたい」など、入手したい情報が特定されている場合に、検索機能によって効果的に探すことが可能です。RSS配信機能を利用することで、定期的に脆弱性情報を取得することもできます。

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。
ベンダ情報	ベンダ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4

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］

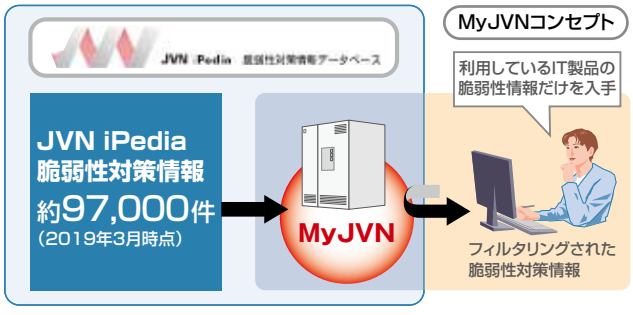
MyJVN 脆弱性対策情報収集ツール

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

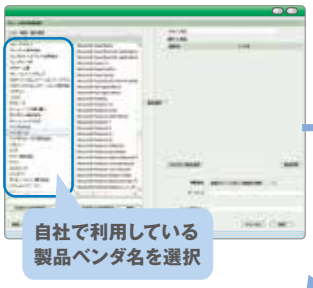


図 2. 製品名選択画面

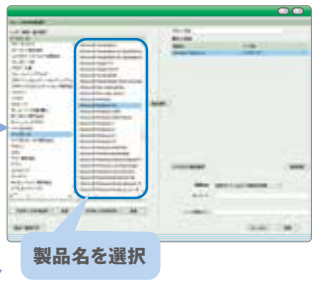


図 3. フィルタリングした脆弱性対策情報一覧画面

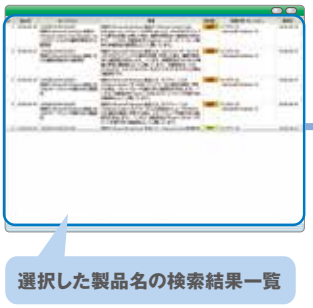
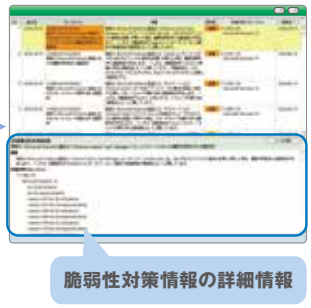


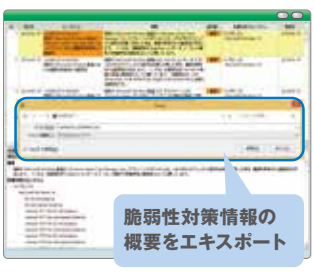
図 4. 脆弱性対策情報 詳細情報



（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5

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］

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）。図2は「MyJVN バージョンチェッカ（.NET Framework 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 にようこそ」画面
（https://jvndb.jvn.jp/apis/myjvn/index.html）

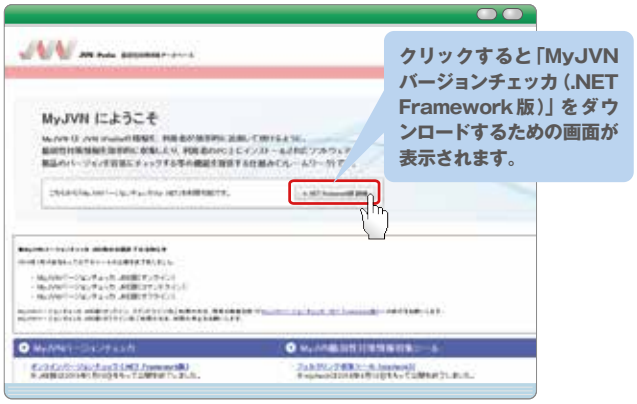


図 2.「MyJVN バージョンチェッカ」実行画面

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

2019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）
実行環境	.NET Framework 4.6

2019年3月時点

ツール6 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>

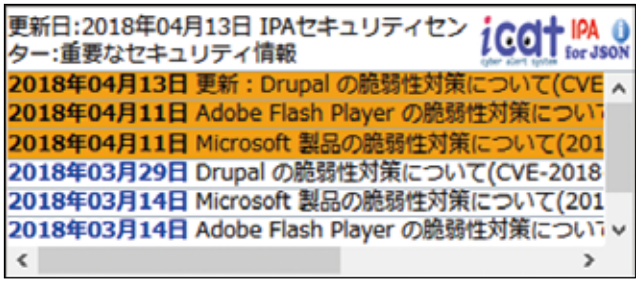
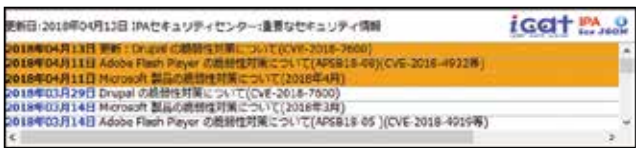


図2. 縦表示 <350 ×150pixel>

図4. 横表示2 <700 ×150pixel>



ツール7

注意警戒情報サービス

緊急性の高いセキュリティ情報を発信
https://jvndb.jvn.jp/alert/

近年、公表される脆弱性対策情報の数は膨大なものになっています。システム管理者は、利用しているソフトウェア製品の脆弱性対策情報を日々収集する中で、各脆弱性の優先度を見極め対応にあたる必要があります。

そこでIPAでは、緊急性の高いセキュリティ情報の一覧をウェブサイトで確認することができる「注意警戒情報サービス」を公開しています。対象となるのは、“重要なセキュリティ情報”（https://www.ipa.go.jp/security/announce/alert.html）、及び脆弱性を悪用されることが多いサーバ4製品（Apache Struts、Bind、OpenSSL、WordPress）のリリース情報です（表1）。

「注意警戒情報サービス」では、“重要なセキュリティ情報”で発信した情報を緊急度に応じて「緊急」、「注意」、それ以外の情報を「INFO」として分類しています（図1）。効率的な脆弱性対策の実施にご活用ください。

表1.「注意警戒情報サービス」の対象となる情報

重要なセキュリティ情報	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
サーバ製品リリース情報	Apache Struts
	Bind
	OpenSSL
	WordPress

（2019年3月時点）

図1.「注意警戒情報サービス」画面（https://jvndb.jvn.jp/alert/）

MyJVN注意警戒API

「注意警戒情報サービス」は、注意警戒情報一覧を取得することができる「MyJVN注意警戒API」を利用しています。このAPIを利用することで、製品や公開時期を指定して注意警戒情報を取得できます。更に、APIによる情報収集を自動化することで、効率化を図ることができます。

利用方法や仕様等の詳細については、「getAlertList（ver. HND）」ページ（https://jvndb.jvn.jp/apis/getAlertList_api_hnd.html）を参照ください。

ツール 8

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

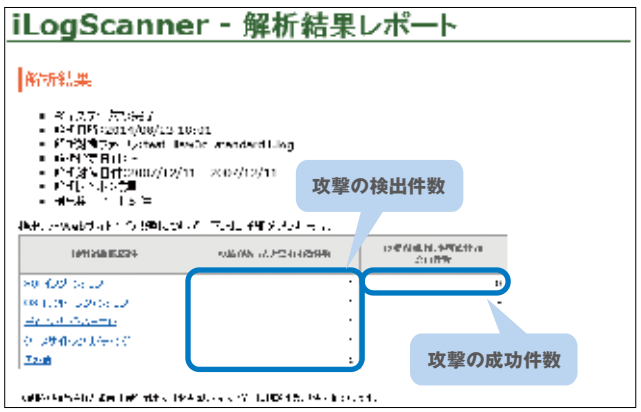
■ SSH/FTPなどメンテナンス用のアプリケーションを狙った不正アクセスの兆候
- 大量のログイン失敗(*4)
- 短時間の集中ログイン(*5)
- 組織外(指定IP外)からのアクセス(*6)など

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、一度ダウンロードすればネットワークに接続していない環境でご利用いただけます。コマンドラインから実行することもできるため、バッチファイルと組み合わせて自動で実行可能です(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。

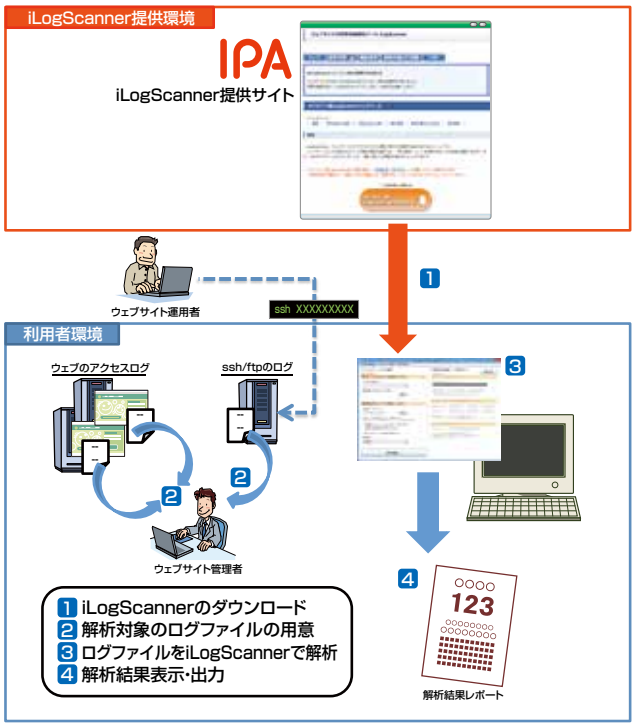
(*5) 短時間の集中ログイン

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



付録

ツール9

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。

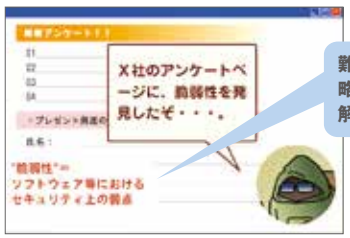
しかし、現実には脆弱性の脅威や仕組み、対策についての知識が必ずしも社会に広まっておらず、ウェブサイトの脆弱性が原因となって起こる被害を未然に防ぐことができていません。

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10

情報セキュリティ対策支援サイト①
【経営者／管理者向け】５分でできる！自社診断、セキュリティプレゼンター検索

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運用しています。

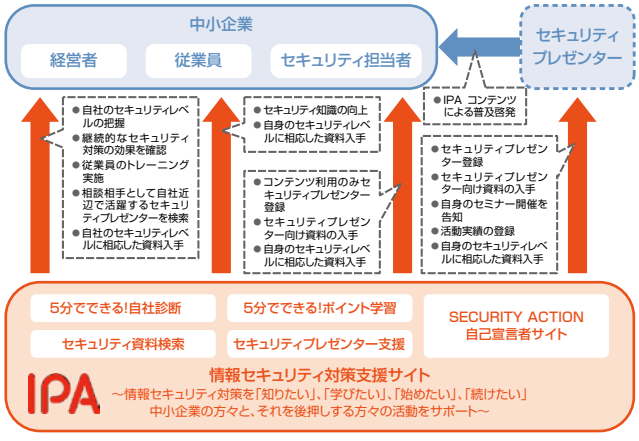
本サイトは、情報セキュリティ対策を「知りたい」「学びたい」「始めたい」「続けたい」中小企業の方々と、それを後押しする方々の活動をサポートします。

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」と「SECURITY ACTION自己宣言者サイト」、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」等で構成されています。

※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）

情報セキュリティ対策支援サイト②
【経営者／管理者向け】SECURITY ACTION自己宣言者サイト、【啓発者向け】セキュリティプレゼンター支援

■ SECURITY ACTION自己宣言者サイト

「SECURITY ACTION自己宣言者サイト」は、情報セキュリティ対策に取り組むことを自己宣言する中小企業等を支援するサイトです。

本サイトでは、自己宣言、SECURITY ACTIONロゴマークダウンロード、SECURITY ACTION自己宣言企業の検索等が行えます。

(1) 自己宣言事業者検索

自己宣言事業者検索はすべての方が利用できるサービスです。「SECURITY ACTION自己宣言」を行っている事業者を検索することができます。例えば、取引先の自己宣言状況の確認や、自社の宣言状況を他者に確認してもらうことができます（図1）。

図1. 自己宣言事業者検索結果

(2) SECURITY ACTION自己宣言

本サイトで「SECURITY ACTION自己宣言」を行うことができます（図2）。

図2. 自己宣言

(3) ロゴマークダウンロード

「SECURITY ACTION自己宣言」の必要な手続きが完了すると、ロゴマークダウンロードが行えます。ロゴマークを、ポスター、パンフレット、名刺、封筒、会社案内、ウェブサイト等に表示して、自社の取り組みをアピールすることができます。

■ 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自身のプロフィールや普及活動実績等を情報登録（無料）すれば、セキュリティプレゼンター検索結果に表示され、相談相手を探している利用者にPRすることができます。

(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（図3）。

図3. 普及啓発コンテンツ

(3) 活動実績・活動告知の登録

セキュリティプレゼンターとしての普及・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、セキュリティプレゼンター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」のトップページ上でPRすることができます（図4）。

図4. 活動告知

情報セキュリティ対策支援サイト③
【従業員向け】５分でできる！ポイント学習

■ 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等で分類された「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１に示します。

図１.「学習の流れ」

1 学習テーマを選択

2 学習テーマを開始

3 学習の目的を理解

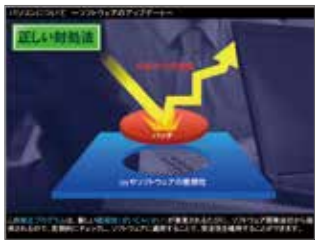
4 事例を疑似体験

5 事例を疑似体験

6 用語の確認

7 学習の意図を確認

8 正しい対処法を理解



9 確認テスト

10 答えと解説

11 修了証

付録

ツール11

さまざまな情報システムにおける適切なセキュリティ要件定義を容易に確認できるツール
https://www.ipa.go.jp/security/isec-sras/

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。

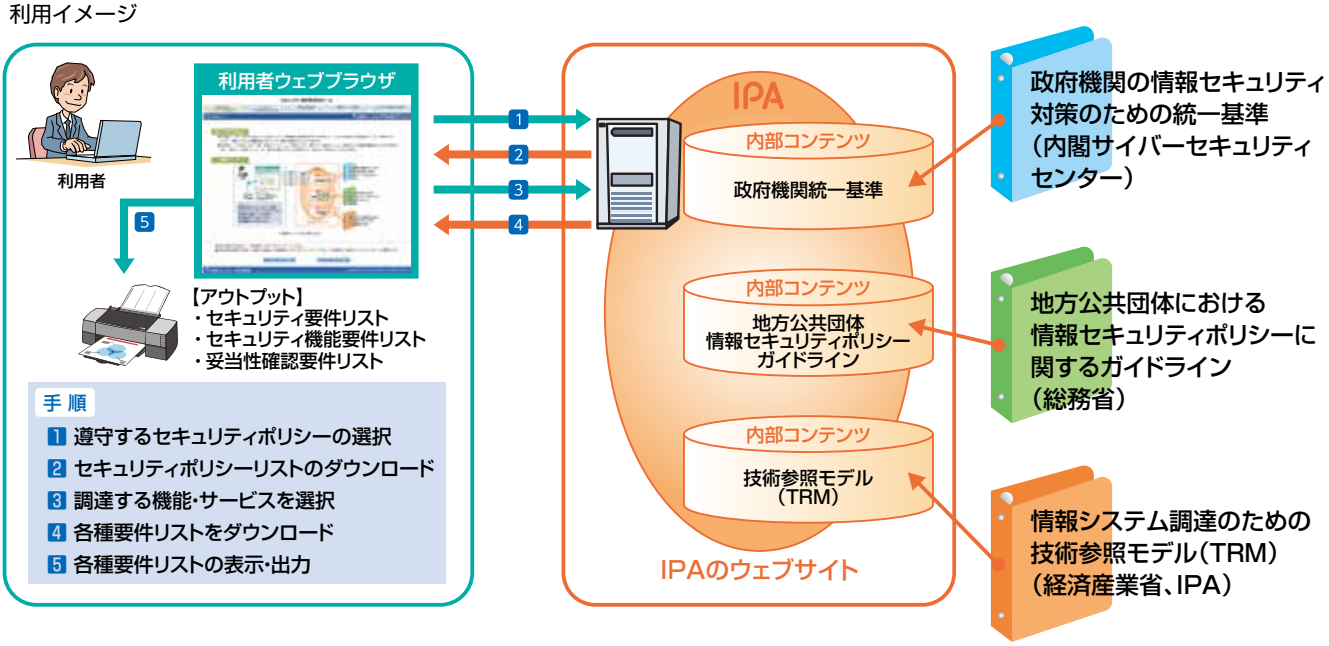
本ツールは、情報システムの調達担当者などが、IPAのウェブサイトから技術参照モデル（TRM※1）で定義された「機能・サービス」を入力することで、必要な「セキュリティ要件」（「政府機関の情報セキュリティ対策のための統一基準」※2または「地方公共団体における情報セキュリティポリシーに関するガイドライン」※3）に関する情報や、情報システムを構成する機器の「セキュリティ機能要件」に関する情報などを提供します。出力された情報を参考にシステムのセキュリティ要件を検討することで、自組織のセキュリティポリシーと適合し、かつ必要なセキュリティ機能を満足するシステム構築が実現できます。

※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



ツール12

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

IPAコンクール応援隊長
「まもるくん」

第14回 IPA「ひろげよう情報モラル・セキュリティコンクール」2018 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。

ここでは、その中から優秀な作品の一部をご紹介いたします。なお、すべての受賞作品はIPA「ひろげよう情報モラル・セキュリティコンクール」Webサイト〈https://www.ipa.go.jp/security/event/hyogo/〉で公開しています。

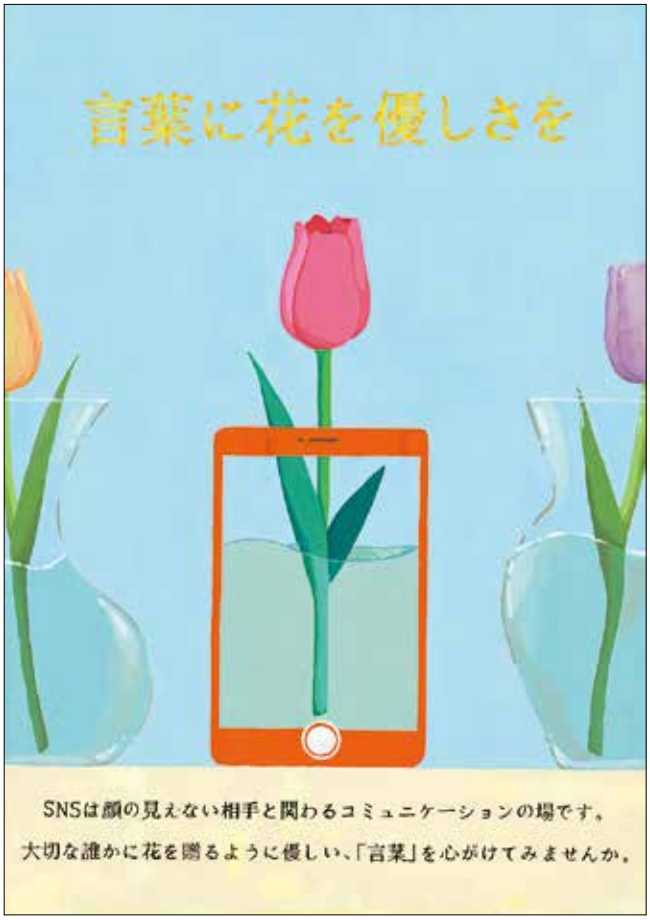
最優秀賞

〈標語部門〉

つぶやきが　自分をおいて　一人旅

大阪府 桃山学院高等学校 2年　**郷司 篤希**さん

〈ポスター部門〉



鹿児島県 鹿児島県立川内商工高等学校 3年
杉薗 はるなさん

〈4コマ漫画部門〉

東京都 筑波大学附属中学校 1年
阿部 遥香さん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

メッセージ　怒った時に　送らない

千葉県　日出学園小学校　5年
和田 瑠子さん

疑って！　タダの裏には　何かある

鹿児島県　鹿児島市立喜入中学校　2年
中村 美月さん

災害時　うそとホントを　見分けよう

大阪府　大阪市立東高等学校　2年
山崎 茉奈美さん

〈ポスター部門〉

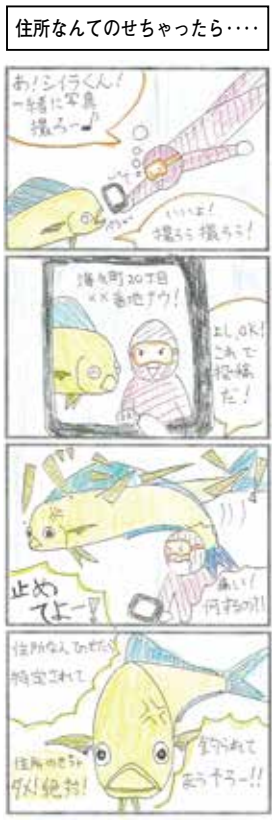
徳島県 吉野川市立鴨島小学校 5年
上藤 幸歩さん

富山県 富山市立堀川中学校 2年
大田 詞也さん

大阪府 大阪市立工芸高等学校 2年
木原 涼さん

〈4コマ漫画部門〉

秋田県 秋田市立中通小学校 3年
安達 岳美さん



東京都 筑波大学附属中学校 2年
鎌刈 雄大さん

京都府 同志社高等学校 1年
北村 祐樹さん

標語部門　優秀賞

〈一般社団法人コンピュータソフトウェア協会〉
戻らない　売ったパソコン　あのデータ
愛知県　名古屋市立工芸高等学校　2年
玉山 雄大さん

〈一般社団法人コンピュータソフトウェア著作権協会〉
その写真　そのイラストに　著作権
岡山県　岡山大学教育学部附属中学校　2年
小林 慶之さん

〈一般社団法人全国地域情報産業団体連合会〉
情報とは　清濁あわせた　川のよう
千葉県　日出学園小学校　5年
藤原 将眞さん

〈特定非営利活動法人ITコーディネータ協会〉
インターネット　みているはずが　みられてる
鹿児島県　鹿児島市立広木小学校　1年
市前 大樹さん

〈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〉
パスワード　やさしくないのが　ちょうどいい
広島県　広島商船高等専門学校　5年
大坪 尚希さん

〈株式会社カスペルスキー〉
セキュリティ　あなたの未来　守るかも
岐阜県　関市立武芸川中学校　3年
早川 実奈さん

〈実教出版株式会社〉
問題は　スマホじゃなくて　使い方
沖縄県　沖縄県立北部農林高等学校　1年
前原 凜さん

〈ソースネクスト株式会社〉
パスワード　おしえちゃだめよ　ひみつだよ
兵庫県　雲雀丘学園小学校　3年
向井 陸人さん

〈株式会社ディー・エヌ・エー〉
「あとちょっと」依存するまで「もうちょっと」
滋賀県　大津市立北大路中学校　3年
川口 祐果さん

〈LINE株式会社〉
情報モラル　自分の心で　フィルタリング
山形県　山形県立酒田光陵高等学校　1年
佐藤 心乃助さん

〈北海道警察本部〉
その気持ち　文字より直接　伝えよう
北海道　札幌市立西野中学校　3年
奥野 優名さん

〈札幌市教育委員会〉
始めよう。個人情報　防衛戦
北海道　札幌市立新川西中学校　2年
東 宏樹さん

〈一般社団法人北海道情報システム産業協会〉
1秒で　送る悪口　深い傷　何秒あれば　癒える傷かな
北海道　北海道帯広柏葉高等学校　2年
畠山 紗采さん

〈岩手県警察本部〉
アップした　写真の未来に　笑顔ある?
岩手県　奥州市立江刺東中学校　3年
千田 彩乃さん

〈公益財団法人仙台応用情報学研究振興財団〉
目立ちたい　その書き込みが　落とし穴
宮城県　宮城県涌谷高等学校　1年
大谷 遼さん

〈一般社団法人宮城県情報サービス産業協会〉
情報の　モラルを守れば　まモラれル
宮城県　宮城県松島高等学校　1年
尾野 幸輝さん

〈一般社団法人秋田県情報産業協会〉
強めよう　友との絆と　セキュリティ
秋田県　横手市立横手南中学校　2年
畑田 優夏さん

〈山形県警察本部〉
その言葉　直接言われて　耐えられる?
山形県　鶴岡東高等学校　1年
五十嵐 優海さん

〈茨城県〉
ネットでは　答えちゃいけない　君の名は?
茨城県　茨城県立並木中等教育学校　1年
小林 拓心さん

〈茨城県教育庁学校教育部高校教育課〉
考えよう　その一言の　影響を　受けとる人を　第一に
茨城県　茨城県立下妻第二高等学校　2年
安藤 源輝さん

〈茨城県教育庁学校教育部義務教育課〉
学ぼうモラル　守ろうルール　築こう僕らの　明るい未来
茨城県　清真学園中学校　1年
和田 健太郎さん

〈茨城県メディア教育指導員連絡会〉
今日は　スマホをやめて　家ぞくでだんらん
茨城県　筑西市立上野小学校　3年
成田 真輝さん

〈茨城県情報通信ネットワークセキュリティ協議会〉
Noモラルから　knowモラルへ
茨城県　清真学園中学校　2年
川原井 詩織さん

〈栃木県警察本部〉
消せないよ　自分を失う　その言葉
栃木県　栃木県立宇都宮東高等学校附属中学校　2年
玉野 心菜さん

〈埼玉県警察本部〉
そのメール　読み手の気持ちも　考えた?
埼玉県　熊谷市立江南中学校　2年
倉野 美羽さん

〈公益社団法人埼玉県情報サービス産業協会〉
スマホ見て　下向き歩く　帰り道　石は見えても　車は見えない
埼玉県　立教新座高等学校　2年
芝田 晏慈さん

〈東京情報大学〉
住所のせ　悪い意味での　有名人
千葉県　鎌ケ谷市立鎌ケ谷中学校　3年
野田 拓利さん

〈警視庁〉
たった今　シェアした所は　全世界
東京都　東京都立町田総合高等学校　1年
髙橋 沙綾さん

〈一般社団法人東京都情報産業協会〉
拡散しない　鵜呑みにしない　デマや嘘
東京都　世田谷区立東玉川小学校　6年
山崎 素直さん

〈新潟県警察本部少年課〉
やめようよ　人の悪口　消せないよ
新潟県　南魚沼市立城内小学校　4年
水澤 快成さん

〈石川県警察本部〉
ウイルスは　あなたの興味の　そばにいる
石川県　石川県立小松明峰高等学校　1年
東出 美桜さん

〈山梨県警察本部〉
たん生日　名前は危険　パスワード
山梨県　山梨学院小学校　5年
三浦 朝陽さん

〈長野県青少年インターネット適正利用推進協議会〉
その相手　ほんとにあなたの　お友達?
長野県　松本市立丸ノ内中学校　1年
出井 あさ美さん

〈長野県インターネットプロバイダ防犯連絡協議会〉
ネットでは　自分もなり得る　悪い人
長野県　松本市立丸ノ内中学校　1年
柴田 菜津美さん

〈岐阜県警察本部〉
忘れたい　あの日にさらした　自撮り写真
岐阜県　岐阜県立岐南工業高等学校　1年
辻 恵吾さん

〈静岡県警察本部〉
ネットにあげたその写真　全て消すこと不可能です
静岡県　日本大学三島高等学校　1年
高山 千早紀さん

〈愛知県警察〉
「みーつけた。」写真でばれる　あなたの居場所
愛知県　田原市立福江中学校　3年
秋元 美空さん

〈特定非営利活動法人東海インターネット協議会〉
フォロワー数　それは君の　価値じゃない
愛知県　豊川市立一宮中学校　3年
早川 太進さん

〈京都府警察本部〉
好奇心　軽くクリック　招くパニック
京都府　京都教育大学附属京都小中学校　6年
嶋村 和子さん

〈京都府教育委員会〉
「ごめんなさい」スマホを使わず　あやまろう
京都府　舞鶴市立青葉中学校　3年
堀内 遼太郎さん

〈京都市教育委員会〉
軽いノリ　その代償は　永遠に
京都府　京都市立堀川高等学校　3年
嶋村 尚子さん

〈一般社団法人京都府情報産業協会〉
ネット上　嘘の情報　見抜く目を
京都府　洛陽総合高等学校　2年
山下 輝人さん

〈京都府私立中学高等学校情報科研究会〉
人気より　高めるべきは　セキュリティー
京都府　京都産業大学附属高等学校　1年
北 彩奈さん

〈京都コンピュータ学院〉
一押しが　招く被害は　想定外
京都府　京都学園中学校　2年
嶋村 康さん

〈京都情報大学院大学〉
勉強しよう　ネットの嘘を　見抜く力
京都府　東山高等学校　2年
石見 裕太さん

〈大阪府警察本部〉
パスワード　いつも同じは　身の危険
大阪府　東大谷高等学校　1年
髙井 保希さん

〈兵庫県警察本部〉
小さなあなたの悪口が　ネットの中では大音量
兵庫県　兵庫県立高砂高等学校　1年
岸本 眞由子さん

〈鳥取県警察本部生活安全部サイバー犯罪対策課〉
あなたの指で発信しても　あなたの指では消せない情報
鳥取県　鳥取県立鳥取西高等学校　1年
田中 苑希さん

〈鳥取県警察本部生活安全部少年課〉
同じだよ　文字も言葉も　責任を
鳥取県　鳥取県立鳥取西高等学校　1年
黒田 澪さん

〈島根県教育委員会〉
バーチャルも　リアルもマナー　大切に
島根県　島根県立松江北高等学校　2年
内田 茉奈美さん

〈一般社団法人島根県情報産業協会〉
決めようね　スマホの時間　家族会議
島根県　島根県立松江商業高等学校　1年
祝部 真琴さん

〈一般社団法人システムエンジニアリング岡山〉
人との関わり広げるが、人の秘密は広げない
岡山県　岡山大学教育学部附属中学校　1年
高下 大和さん

〈岡山県情報セキュリティ協議会〉
親たちは　スマホ片手に　子と遊ぶ
岡山県　岡山市立石井中学校　2年
常藤 滉生さん

〈一般社団法人広島県情報産業協会〉
タダだから　不正upで　著者は泣く
広島県　広島県立福山葦陽高等学校　2年
三山 大貴さん

〈広島県インターネット・セキュリティ対策推進協議会〉
「情報の　真偽をちゃんと　確かめて」
広島県　広島市立広島商業高等学校　1年
羽賀 帆花さん

〈徳島県警察本部〉
1通の　メールにスマホを　奪われる
徳島県　徳島県立城ノ内高等学校　1年
近藤 朱嶺さん

〈徳島県教育委員会〉
要確認　写真の中の　位置情報
徳島県　徳島市城東中学校　3年
村澤 晴貴さん

〈一般社団法人徳島県情報産業協会〉
ネットじゃなく　リアルでつもう　良いけいけん
徳島県　美馬市立脇町中学校　2年
篠原 陽太さん

〈香川県教育委員会〉
もらさない　自分の秘密　他人の秘密
香川県　高松市立香東中学校　1年
宮西 康太さん

〈香川県プロバイダ等防犯連絡協議会〉
虫の良い　広告バナーに　近付くな
香川県　高松市立香東中学校　1年
入江 凜太朗さん

〈愛媛県警察本部〉
位置情報　あなたの家への　ナビゲート
愛媛県　愛媛県立松山南高等学校　1年
東野 亨省さん

〈高知県教育委員会〉
ばれないよう　プライバシーに　鍵かけよう
高知県　高知市立高知商業高等学校　3年
森光 真由さん

〈一般社団法人高知県情報産業協会〉
情報モラル　きちんと守って　つながろう
高知県　南国市立久礼田小学校　6年
高橋 ここあさん

〈福岡県警察本部〉
ひと手間が　君を守るよ　パスワード
福岡県　福岡県立戸畑高等学校　1年
藤白 理那さん

〈一般社団法人長崎県情報産業協会〉
ちゃんと見て　スマホじゃなくて　目の前を
長崎県　諫早市立諫早中学校　3年
戸野口 瑠依さん

〈長崎県ネットワーク・セキュリティ連絡協議会〉
ネットより　家ぞくとむき合う　安心かん
長崎県　諫早市立西諫早中学校　1年
丸尾 鈴華さん

〈大分県警察本部〉
一瞬で　みんなの情報　分かる時代
大分県　日本文理大学附属高等学校　1年
西條 由季乃さん

〈宮崎県警察本部〉
パスワード　強固でなければ　意味もなし
宮崎県　宮崎県立宮崎南高等学校　1年
鬼束 大輝さん

〈鹿児島県教育委員会〉
「これでよし」　そう載せる前に　再確認
鹿児島県　鹿児島市立伊敷中学校　1年
上園 彩夏さん

〈鹿児島市教育委員会〉
セキュリティ　目には見えない　守り神
鹿児島県　鹿児島市立和田小学校　4年
山元 理子さん

〈特定非営利活動法人ITかごしま支援隊〉
自由でも　良いこと悪いこと　考えよう
鹿児島県　鹿児島市立東谷山小学校　6年
田中 あきほさん

〈特定非営利活動法人鹿児島インファーメーション〉
おもいやり　ネットのなかでも　だいじだね
鹿児島県　鹿児島市立伊敷小学校　1年
小野 心裕さん

〈沖縄県〉
いいねより　大事にしよう　思いやり
沖縄県　沖縄県立那覇商業高等学校　3年
田中 尚幸さん

〈沖縄県警察本部〉
S 知らない人に　N 名前と行動　S 知られてる
沖縄県　沖縄県立那覇西高等学校　2年
江洲 宇翔さん

〈沖縄県情報通信関連産業団体連合会〉
パソコンに　入るウイルス　出る情報
沖縄県　昭和薬科大学附属中学校　2年
崎原 和創希さん

ポスター部門　優秀賞

〈警察庁〉

東京都 東京都立工芸高等学校 3年

亀井 美緒さん

〈一般社団法人
JPCERT コーディネーションセンター〉

埼玉県 所沢市立南陵中学校 2年

中島 颯希さん

〈一般社団法人日本教育情報化振興会〉

大阪府 大阪教育大学附属池田中学校 2年

濱田 萌友さん

〈モバイルコンピューティング
推進コンソーシアム〉

東京都 東京都立工芸高等学校 3年

長南 芽依さん

〈フィッシング対策協議会
「STOP. THINK. CONNECT.」〉

大阪府 大阪市立工芸高等学校 3年

土居 なつのさん

〈株式会社シマンテック〉

香川県 大手前丸亀中学校 2年

櫛田 花音さん

〈トレンドマイクロ株式会社〉

千葉県 日出学園中学校 1年

伊藤 鈴さん

〈マカフィー株式会社〉

福島県 本宮市立本宮第一中学校 2年

古宮 まことさん

〈株式会社ラック〉

神奈川県 神奈川県立神奈川工業高等学校 3年

小田島 輝さん

〈青森県警察本部〉

青森県 十和田市立甲東中学校 2年

野中 海天さん

〈秋田県教育委員会〉

秋田県 秋田県立矢島高等学校 1年

佐藤 綾香さん

〈秋田県警察本部〉

秋田県 大潟村立大潟中学校 1年

後藤 茉莉花さん

〈茨城県警察本部〉

茨城県 つくば市立吾妻中学校 3年

松本 勇人さん

〈富山県警察本部〉

富山県 富山市立堀川中学校 2年

野口 風花さん

〈福井県警察本部〉

福井県 福井市湊小学校 5年

勝見 いろはさん

〈一般社団法人山梨県情報通信業協会〉

山梨県 山梨英和高等学校 3年

大井 遥さん

〈一般社団法人
長野県情報サービス振興協会〉

長野県 長野県駒ケ根工業高等学校 3年

柴田 すずなさん

〈三重県警察本部〉

三重県 三重県立名張高等学校 3年

松下 麗緒奈さん

〈滋賀県警察本部〉

滋賀県 大津市立北大路中学校 3年

吉岡 眞菜さん

〈公益社団法人京都府防犯協会連合会〉

京都府 京都翔英高等学校 1年

木村 天音さん

〈奈良県警察本部〉

奈良県 奈良県立奈良北高等学校 2年

後藤 碧さん

〈特定非営利活動法人
奈良地域の学び推進機構〉

奈良県 奈良県立奈良北高等学校 2年

河原 未玖さん

〈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

大西 桃夏さん

〈島根県警察本部〉

島根県 島根県立浜田商業高等学校 1年

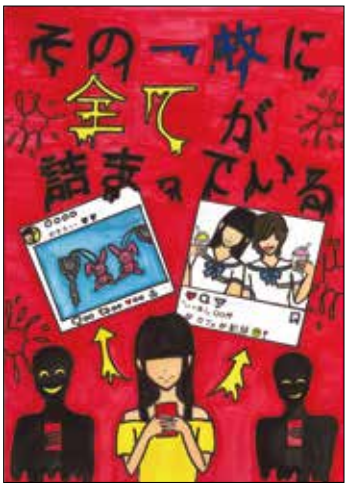
中 小織さん

〈岡山県警察本部〉

岡山県 岡山県立高梁城南高等学校 2年

新谷 怜桜さん

〈広島県警察本部〉



広島県 熊野町立熊野中学校 2年

緒方 真珠さん

〈山口県警察本部〉

山口県 山口県立宇部商業高等学校 3年

久保 裕亮さん

〈公益財団法人e-とくしま推進財団〉

徳島県 徳島市立津田中学校 3年

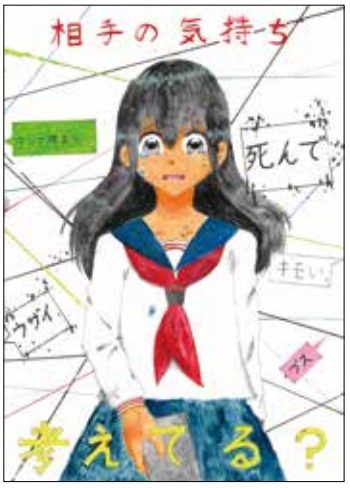
滑川 由菜さん

〈かがわ情報化推進協議会〉

香川県 香川県立高松工芸高等学校 2年

上原 さんごさん

〈愛媛県情報サービス産業協議会〉



愛媛県 久万高原町立久万中学校 1年

梶川 春菜さん

〈佐賀県警察本部〉

佐賀県 小城市立晴田小学校 5年

中島 椿さん

〈長崎県警察本部〉

長崎県 長崎県立佐世保北高等学校 1年

宮崎 万由子さん

〈熊本県警察本部〉

熊本県 御船町立御船中学校 2年

麻井 春陽さん

〈一般社団法人宮崎県情報産業協会〉

宮崎県 宮崎市立赤江中学校 3年

横田 百音さん

〈鹿児島県警察本部〉

鹿児島県 鹿児島県立鹿児島工業高等学校 2年

濵田 優季さん

〈特定非営利活動法人
フロム沖縄推進機構〉

沖縄県 沖縄県立八重山商工高等学校 3年

新垣 宝さん

4コマ漫画部門　優秀賞

〈一般社団法人組込みシステム技術協会〉

そもそも女の子？

山形県 山形県立酒田光陵高等学校 1年

日向 咲良さん

〈一般社団法人情報サービス産業協会〉

その書き込み…消せないよ

兵庫県 西宮市立浜脇中学校 3年

梅崎 はるくさん

〈公益社団法人著作権情報センター〉

著作権

広島県 広島県立可部高等学校 1年

吉井 雛子さん

〈一般社団法人日本情報システム・ユーザー協会〉

歩きスマホは危険がいっぱい!!

愛知県 愛知県立豊田東高等学校 1年

加納 優里さん

〈デジタルアーツ株式会社〉

善意と SNS の拡散

北海道 北海道北見柏陽高等学校 1年

髙橋 風花さん

〈株式会社ネットワールド〉

確認しよう！

埼玉県 埼玉県立新座総合技術高等学校 2年

麻生 いづみさん

〈宮城県警察本部〉

画面越し

宮城県 聖和学園高等学校 2年

伊藤 凪沙さん

〈福島県警察本部〉

SNS 投稿

福島県 福島市立信陵中学校 2年

大島 葵さん

〈群馬県警察本部〉

正しい？その情報

群馬県 桐生市立中央中学校 2年

本山 実咲さん

〈千葉県警察本部〉

忍者のおしえ

千葉県 市川学園市川高等学校 1年

荒巻 静花さん

〈神奈川県警察本部〉

ネズミかと思ったら…

神奈川県 横浜市立六角橋中学校 2年

谷内 紬さん

〈新潟県警察本部サイバー犯罪対策課〉

アイコンに釣られるな！

新潟県 新潟県立新潟向陽高等学校 3年

吉田 彩乃さん

〈一般社団法人石川県情報システム工業会〉

失ってしまうもの

石川県 石川県立小松明峰高等学校 1年

長清 珠希さん

〈長野県警察本部〉

反面教師

長野県 上田市立菅平小学校 6年

髙下 真莉佳さん

〈ネット安全・安心ぎふコンソーシアム〉

だまされないで!!

岐阜県 土岐市立泉中学校 1年

伊佐次 桃香さん

〈特定非営利活動法人ふじのくに情報ネットワーク機構〉

慎重に!!

静岡県 静岡県立三島南高等学校 1年

大杉 美奈さん

〈大阪私学教育情報化研究会〉

SNS なりすまし

大阪府 大阪府立三島高等学校 2年

小澤 諒子さん

〈和歌山県警察本部〉

位置情報

和歌山県 和歌山県立粉河高等学校 1年

鈴木 望愛さん

〈情報通信交流館（e-とびあ・かがわ）〉

信じていいもの

香川県 三豊市立三野津中学校 3年

田中 友菜さん

〈高知県警察本部〉

パスワード

高知県 高知工業高等専門学校 1年

岡﨑 序実さん

〈福岡県教育委員会〉

本当に危ないよ

福岡県 飯塚市立筑穂中学校 1年

末永 千尋さん

〈特定非営利活動法人ITサポートさが〉

特定

佐賀県 有田町立西有田中学校 2年

川内 稜夏さん

〈大分県情報サービス産業協会〉

おじさん

大分県 臼杵市立北中学校 2年

中村 さきさん

〈一般社団法人鹿児島県情報サービス産業協会〉

僕じゃないのに！

鹿児島県 湧水町立吉松中学校 1年

永野 未侑さん

索引

数字

5G ……84, 89, 90

A

ADB.Miner ……167
AI・データの利用に関する契約ガイドライン……68, 142
AI プロダクト品質保証ガイドライン ……190
Anti-Phishing Working Group, Inc.（APWG）
……8, 40, 76
Apache Struts2 ……27, 180
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）……92
ASEAN 地域フォーラム……80, 82
ASEAN 等向け日米サイバー共同演習 ……64, 67, 101
ASP・SaaS における情報セキュリティ対策ガイドライン
……74, 183

B

BrickerBot ……163, 166

C

CC（Common Criteria：共通基準）……89, 133
CCRA（Common Criteria Recognition Arrangement）……133
CISO（Chief Information Security Officer：最高情報セキュリティ責任者）……18, 102, 107
Connected Industries ……139, 162
CRYPTREC ……77, 137, 143
CSIRT（Computer Security Incident Response Team）……18, 74, 91, 191
CSV ファイル……17
CYBER COLOSSEO……73
Cyber Sense Act……159
Cybersecurity and Infrastructure Security Agency（CISA）……87
CYDER（Cyber Defense Exercise with Recurrence：実践的サイバー防衛演習）……73

D

DDoS 攻撃 ……25, 74, 163
DDoS 攻撃代行サービス ……25
Drupal……28, 47

E

ENISA（European Network and Information Security Agency：欧州ネットワーク・情報セキュリティー庁）……88, 172
enPiT（Education Network for Practical Information Technologies）……105
ePrivacy Regulation（ePR）……88
Ethically Aligned Design, Version2（EADv2）……189
Ethics Guidelines for Trustworthy AI……189
EUサイバーセキュリティ法案（EU Cybersecurity Act）…87
eーネットキャラバン……118

F

Framework for Improving Critical Infrastructure Cybersecurity……54, 184

G

G20 AI 原則 ……189
G7 シャルルボワ・サミット……80
GCM-AES-XPN……137
GDPR（General Data Protection Regulation：一般データ保護規則）……10, 81, 187

I

IIoT（Industrial Internet of Things）……159
IoT……28, 64, 71, 128, 140, 163
IoT 機器のセキュリティ対策に関する検討の方向性…72
IoT サイバーセキュリティ アクションプログラム 2017…71
IoT 社会に対応したサイバー・フィジカル・セキュリティ
……64
IoT セキュリティガイドライン……128, 130
IoT セキュリティ総合対策 ……71
IoT セキュリティ総合対策 プログレスレポート 2018 …71
IoT セキュリティ対策に関する提言 ……71
IoT ボット……25
ISO/IEC 27001 ……110, 126
ISO/IEC JTC 1/SC 27……125
ITSS+ ……99
IT サプライチェーン ……179, 182
IT 製品の調達におけるセキュリティ要件リスト…… 132, 136
IT セキュリティ評価及び認証制度（Japan Information Technology Security Evaluation and Certification Scheme：JISEC）……132, 136

J

Java SE 8 ……47
JC 版サイバーセキュリティ問題解決プログラム ……111
J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）
……70
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）……20, 69

JVN iPedia 28, 45

L

Liberty Eclipse 160
LNK ファイル 16
Locked Shields 160

M

Mirai 25, 27, 28, 75, 163
Mirai の亜種 163

N

NICE 84, 98
NIS 指令（Network Information Security Directive） 87, 160
NOTICE 72, 170
NVD（National Vulnerability Database） 45

O

OCB2 ..... 127, 142
OLE オブジェクト 16, 18
OMG 167
OpenBugBounty 53
Operation Power Off 25

P

PowerShell 10, 16, 19
Protection Profile（PP） 127, 131, 134

R

RaaS（Ransomware as a Service） 30

S

SamSam 30
Satori 163, 168
SecBok2019 98
SECCON 2018 106
SecHack365 105
Securing Energy Infrastructure Act 160
SECURITY ACTION 111
ShadowHammer 180
SIMON/SPECK 127
SMS（Short Message Service） 12, 34, 174
Society 5.0 ..... 64, 74, 95, 182
SYN/ACK リフレクション攻撃 26

T

TCG（Trusted Computing Group） 125, 131

V

VPNFilter 156, 168

W

Wanna Cryptor（WannaCry） 11, 29, 157
Wicked 28, 164
Windows 27, 50

あ

アイデンティティ管理 129
悪質 EC サイトホットライン 40
アプリ誘導 177
暗号モジュール試験及び認証制度（Japan Cryptographic Module Validation Program：JCMVP） 136
インターネット安全教室 119
インターネットの安全・安心ハンドブック Ver.4.00 119
遠隔操作ウイルス（Remote Access Trojan：RAT） 14
オンラインゲーム 25
オンラインストレージサービス 15

か

仮想通貨（暗号資産） 11, 29, 36, 47, 76, 167
仮想通貨を要求する脅迫メール 36
神奈川県企業サイバーセキュリティ官民合同プロジェクト 112
技術等情報管理認証制度 68
機能保証のためのリスクアセスメント・ガイドライン 161
脅威情報の情報共有基盤　利用ガイドライン 73
共通脆弱性タイプ一覧（Common Weakness Enumeration：CWE） 45
共通脆弱性評価システム（Common Vulnerability Scoring System：CVSS） 45
組み込み機器 53, 131
クラウドサービス提供における情報セキュリティ対策ガイドライン 74
クラウドサービスの安全性評価に関する検討会 67
クラウドサービスの安全性評価に関する検討会 中間取りまとめ（案） 67
クラウドサービスのガイドライン 183
クリプトジャッキング 11
グループ・ガバナンス・システムに関する実務指針（仮） 67, 109
クロスサイト・スクリプティング 45, 51
現地調達（living off the land）型の攻撃 10
公表判定委員会 55
国際標準化活動 124
国防権限法（National Defense Authorization Act） 82, 184
個人情報の保護に関する法律についてのガイドライン 118

個人情報保護法……81, 107, 187
個人データ移転に関する包括合意……81
国家サイバー戦略……83, 86
コラボレーション・プラットフォーム……63, 67
コンテンツマネジメントシステム（Content Management System：CMS）……27, 28, 47

さ

サイトの改ざん……12, 35, 48
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……65
サイバーセキュリティ 2018……63, 160, 162
サイバーセキュリティ経営ガイドライン……63, 96, 109, 111, 182
サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集……67, 109
サイバーセキュリティ経営プラクティス検討会……109
サイバーセキュリティ月間……119
サイバーセキュリティ重点施策……75
サイバーセキュリティ小説コンテスト……121
サイバーセキュリティ人材育成取組方針……64, 95
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……95, 100
サイバーセキュリティ戦略……62, 95, 108, 113
サイバーセキュリティ対処調整センター……64
サイバーセキュリティタスクフォース……63, 71
サイバー犯罪検挙件数……76
サイバー・フィジカル・セキュリティ対策フレームワーク……64, 66, 162
サイバーフォースセンター……75
サプライチェーン……64, 74, 83, 157, 179
サプライチェーン情報セキュリティ管理基準……182
サポート詐欺……38
産学情報セキュリティ人材育成交流会……106
産業横断サイバーセキュリティ人材育成検討会（Cyber Risk Intelligence Center - Cross Sectors Forum：CRIC CSF）……96
産業競争力強化法等の一部を改正する法律……68
産業サイバーセキュリティ強化へ向けたアクションプラン……65
産業サイバーセキュリティ研究会……65
産業サイバーセキュリティセンター……101
社会信用システム建設計画綱要……90
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……64, 161
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……64
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……64, 160
消費者向け IoT 製品のセキュリティに関する行動規範……54, 128
情報開示分科会報告書……73
情報処理安全確保支援士（登録セキスペ）……98, 102, 103
情報処理支援機関（スマート SME サポーター）……68
情報セキュリティ安心相談窓口……118
情報セキュリティ運用連携サービス（NII Security Operation Collaboration Services：NII-SOCS）……114
情報セキュリティサービス基準……67
情報セキュリティサービス基準適合サービスリスト……69
情報セキュリティサービスに関する審査登録機関基準……69
情報セキュリティ市場規模……138
情報セキュリティ早期警戒パートナーシップ……48, 54
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……54
情報セキュリティマネジメント試験……102
情報セキュリティマネジメントシステム（Information Security Management System：ISMS）……110, 126
情報漏えい……9, 11, 41, 52, 113
人工知能の未来のためのシャルルボワ・共通ビジョン……80
スマートカードの評価認証……135
スマートフォン時代に対応した青少年のインターネット利用に関する連絡会……121
制御システムのセキュリティリスク分析ガイド第 2 版……161
脆弱性……27, 49, 51, 72, 158
脆弱性情報の流通……54
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……62, 67, 182
政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）……132
政府機関等の対策基準策定のためのガイドライン……136
政府情報システムにおけるクラウドサービスの利用に係る基本方針……67
セキュリティ・キャンプ……105
セキュリティサービス認定検討会……69
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……95
セクストーション（性的脅迫）……13, 37
戦略マネジメント系セミナー……67, 102
ソーシャルエンジニアリング……14, 157
組織における内部不正防止ガイドライン……43, 181
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……54

た

ダークウェブ……30, 32, 48, 75
耐量子暗号（Post-Quantum Cryptography：PQC）……143
知的財産推進計画 2018……124

地方公共団体における情報セキュリティ監査に関するガイドライン……74
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……74
中核人材育成プログラム……101
中小企業の情報セキュリティ対策ガイドライン……67, 112
データ取引・流通プラットフォーム……140
データの利用権限に関する契約ガイドライン……68
データ利活用……139
デジタル・トランスフォーメーション時代における人材育成プログラム……67
デジュール標準（de jure standard）……124
デファクト標準（de facto standard）……124
電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会……74
電気通信事業法及び国立開発研究法人情報通信研究機構法の一部を改正する法律……72
電子情報開示（Electronic Discovery）……129
東京 2020 オリンピック・パラリンピック競技大会……64, 73, 80, 81, 102, 161
統合セキュリティ人材モデル……98
トラストサービス……74
トラストサービス検討ワーキンググループ……74

な

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）……62, 80, 96, 119, 136, 182
内部不正……42, 181
なりすまし……15, 22, 40
なりすまし EC サイト対策マニュアル……40
偽 EC サイト……40
偽サイト……40, 174
偽（の）警告……12, 13, 38, 177
偽のセキュリティ警告……38, 177
偽（の）セキュリティソフト……38, 177
日・ASEAN サイバーセキュリティ政策会議……82
日 EU サイバー対話……81
日・イスラエル・サイバー協議……81
日インド・サイバー協議……82
日英サイバー協議……81
日仏サイバー協議……81
日米サイバー対話……80
人間中心の AI 社会原則……189
ネットワーク安全法……90

は

バイオメトリクス……130
バグバウンティプログラム……54
パスワード設定……72, 117, 170
パスワードリスト攻撃……31, 117, 120
春のあんしんネット・新学期一斉行動……118
ビジネスメール詐欺（Business Email Compromise：BEC）……8, 20, 23, 70, 179
秘密情報の保護ハンドブック……43
標的型攻撃……14, 70, 157
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）……66, 162
ファーミング……36
ファイルレス攻撃……10
フィッシング……8, 12, 33, 113, 176
フォーラム標準（forum standard）……124
不在通知 SMS……12, 34, 174
不正アプリ……35, 116, 166, 174, 178
不正競争防止法……139
不正マイニング……11, 29, 30
プライバシーマーク制度……110
プラス・セキュリティ人材……105
プラットフォームサービスに関する研究会……74, 192
分野横断的演習……65
ボットネット……25, 75, 163

ま

マクロ機能……17
マルチベクトル型攻撃……25
未来投資戦略 2018……67

ら

ランサムウェア……10, 29, 31, 36, 157
リフレクター攻撃……25, 26

おわりに

情報セキュリティ白書2019では、読みやすさの向上のため、例年から少し手を加えてみました。 例えば第1章において、これまでインシデントの状況・事例と、攻撃や手口の動向・対策を別の節に分けて記載していましたが、今回は一気通貫で読めるように一つの節にまとめています。他にも、より気軽に読んでいただけるよう、箸休めとなるコラムの数を増やしています。

情報セキュリティ白書2017では「広がる利用、見えてきた脅威:つながる社会へ着実な備えを」、情報セキュリティ白書2018では「深刻化する事業への影響:つながる社会で立ち向かえ」というように、共通して「つながる社会」というキーワードをサブタイトルで使用していました。前者はネットワークで機器同士がつながる社会を、後者は人や組織が協働・団結して脅威に立ち向かう社会を示しています。今回のサブタイトルは、サイバー空間とフィジカル空間が「つながる」ことで新たなインフラやサービスが形成され、新たな脅威が潜んでいるかもしれない、そのため、2018年度に大きな事案があまりなかったからといって安心せず、新しいリスクに備えてほしい、と期待して「新しい基盤、巧妙化する攻撃:未知のリスクに対応する力を」としました。

本白書は、IPAの職員を始めとする多くの関係者が、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。 皆様のサイバーセキュリティ対策の検討・実践の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　瓜生 和久　小川 隆一　竹腰 智

執筆者　IPA

花村 憲一	武智 洋	山里 拓己	時田 俊雄	神田 雅透
西尾 秀一	小川 隆一	江島 将和	大谷 祐子	内山 友弘
奥田 美幸	浅井 優子	山﨑 知嗣	天野 農	辻 宏郷
福原 聡	猪城 明	板橋 博之	井上 真弓	大友 更紗
岡下 博子	亀山 友彦	唐亀 侑久	小林 桂	佐藤 輝夫
田村 智和	渡邉 祥樹	鹿野 一人	須藤 直樹	神市 章二
伊東 隆司	栗原 史泰	竹内 智子	西村 奏一	甲斐 成樹
櫻井 玄弥	橋本 徹	小暮 淳	近澤 武	塚元 卓
畑野 元	河合 和哉	金子 朋子	延藤 里奈	井上 勝浩
増田 亮太	佐川 陽一	木内 直人	小山 明美	ジリエ 陽子
半貫 貴久	森 淳子	野澤 裕一	竹腰 智	

一般社団法人 JPCERT コーディネーションセンター　内田 有香子
株式会社日立製作所　相羽 律子
情報規格調査会 JTC 1/SC 27/WG 5 小委員会
日本電気株式会社　島 成佳

協力者　IPA

桑名 利幸	高橋 将	横山 尚人	小宮 弥生	加賀谷 伸一郎
渡辺 貴仁	松坂 志	松井 洋二	幡谷 茉莉衣	近藤 裕貴
土屋 正	木下 弦	黒谷 欣史	伊東 宏明	田村 百合子
小沢 理康	西原 栄太郎	岩政 幹人	遠山 真	秋元 裕和
本多 康弘	田口 聡			

国立研究開発法人産業技術総合研究所　堀 洋平
富士通株式会社　小谷 誠剛
一般社団法人 JPCERT コーディネーションセンター
経済産業省商務情報政策局サイバーセキュリティ課

情報セキュリティ白書 2019

新しい基盤、巧妙化する攻撃：未知のリスクに対応する力を

2019 年 8 月 8 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　03-5978-7503
Fax　03-5978-7510
E-Mail spd-book@ipa.go.jp

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**