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
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機器の脆さの把握、企業経営層のセキュリティリスク管理への参画など、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ア攻撃、人間の弱点を狙ったネット上の詐欺等の手法は、更に巧緻化を続けています。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。海外に目を向ければ、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。対策が進んでいる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。「情報セキュリティ白書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
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
第2章 国際標準化活動
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
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 国内的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要なインシデントや実施された政策・制度について概説を述べる。

国外では2018年10月に大手SNSがユーザーの個人情報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3億3,800万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、企業や個人に対する攻撃・被害は継続して確認された。

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言える年であった。

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攻撃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セキュリティ戦略を発表し、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ーの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ーで認められたように、欧州と連携する等で独自の位置を模索している。

以上のよう、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セキュリティ対策を進めることを求められる。
<table>
<thead>
<tr>
<th>2018年度の情報セキュリティの概況</th>
<th>2018年度の情報セキュリティの概況</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018年4月</td>
<td>2018年4月</td>
</tr>
<tr>
<td>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)</td>
<td>NISC「重要インフラにおける情報セキュリティ確保に関する安全基準等策定指針(第5版)」公表(2.1.1)</td>
</tr>
<tr>
<td>監視カメラへの不正アクセスが相次ぐ(3.2.2)</td>
<td>経済産業省「サイバー・フィジカル・セキュリティ対策プレーヤーワーク(案)」公表(2.1.2)</td>
</tr>
<tr>
<td>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)</td>
<td>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)</td>
</tr>
<tr>
<td>5月</td>
<td>5月</td>
</tr>
<tr>
<td>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攻撃が発生(1.2.6)</td>
<td>サイバーセキュリティ戦略概要(1.2.9)</td>
</tr>
<tr>
<td>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)</td>
<td>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)</td>
</tr>
<tr>
<td>6月</td>
<td>6月</td>
</tr>
<tr>
<td>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)</td>
<td>「サイバーセキュリティ戦略」閣議決定(2.1.1)</td>
</tr>
<tr>
<td>宅配便業者を装う不正不在通知SMSの相談急増(3.3.1)</td>
<td>「サイバーセキュリティ戦略」閣議決定(2.1.1)</td>
</tr>
<tr>
<td>7月</td>
<td>7月</td>
</tr>
<tr>
<td>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)</td>
<td>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)</td>
</tr>
<tr>
<td>8月</td>
<td>8月</td>
</tr>
<tr>
<td>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)</td>
<td>綜合政策局でサイバーセキュリティ法が施行(2.2.5)</td>
</tr>
<tr>
<td>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)</td>
<td>トランプ米国大統領が国防権限法に署名(2.2.2、3.4.3)</td>
</tr>
<tr>
<td>9月</td>
<td>9月</td>
</tr>
<tr>
<td>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)</td>
<td>サイバーセキュリティ戦略(第2版)」公表(2.1.3)</td>
</tr>
<tr>
<td>10月</td>
<td>10月</td>
</tr>
<tr>
<td>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)</td>
<td>経済産業省「技術等情報管理認証制度」開始(2.1.2)</td>
</tr>
<tr>
<td>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)</td>
<td>警察庁「サイバーセキュリティ対策指導(1.2.8)</td>
</tr>
<tr>
<td>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)</td>
<td>米国「国家サイバー戦略」発表(2.2.2)</td>
</tr>
<tr>
<td>11月</td>
<td>11月</td>
</tr>
<tr>
<td>12月</td>
<td>12月</td>
</tr>
<tr>
<td>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3億8,000万件が漏えいした恐れがあると公表(1.1.1、1.2.9)</td>
<td>NISC「分野横断的演習」実施(2.1.1)</td>
</tr>
<tr>
<td>不正アクセスにより、ファイアーウォール利用者の情報漏えいが発生(1.2.9)</td>
<td>経済産業省「トラストサービス検討ワーキンググループ」設置(2.1.3)</td>
</tr>
<tr>
<td>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)</td>
<td>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)</td>
</tr>
<tr>
<td>2019年1月</td>
<td>2月</td>
</tr>
<tr>
<td>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3億8,000万件が漏えいした恐れがあると公表(1.1.1、1.2.9)</td>
<td>総務省・NICT「NOTICE」開始(2.1.3)</td>
</tr>
<tr>
<td>不正アクセスにより、ファイアーウォール利用者の情報漏えいが発生(1.2.9)</td>
<td>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)</td>
</tr>
<tr>
<td>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)</td>
<td>広域統合サービスの訓練(3.1.4)</td>
</tr>
<tr>
<td>3月</td>
<td>3月</td>
</tr>
<tr>
<td>自動アップデートツールを悪用してウイルスを散布する攻撃の報告(3.4.1)</td>
<td>欧州議会「EUサイバーセキュリティ法案」承認(2.2.3)</td>
</tr>
</tbody>
</table>

※2018年度の主要情報セキュリティインシデント・事件、及び主要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。表中の数字は本文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。
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、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ない、利用者やサービス提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や偽警報等、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年セキュリティランドアップ※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
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

情報セキュリティ白書 2019

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87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7万8617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詐欺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 ビジネスマイル詐欺（BEC）」参照）。

(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88。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ィルス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1-1-2】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

【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

【図1-1-4】情報セキュリティインシデント・脆弱性の現状と対策
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年には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）。

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年には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）。

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年には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）。

また、2018年5月25日にEU一覧データ保護規則（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、企業を対象とした件数は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）。

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一覧データ保護規則（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）。

(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、攻撃に関する悪意のあるソフトウェアの使用は減少傾向であり、攻撃の57%で利用されていたなかった。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。
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

(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中では、「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)。

(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年の6,900万件に増加した。しかしながら、月ごとの変動を見ると、2018年始めのピークを過ぎ、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とともに減少している(図1-1-8)。

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
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。
- 三井物産セキュアリテクノロジー株式会社（以下、MBSD社）: サイバーセキュリティ事件簿16
- 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

(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年度に報告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」は横ばいであったものの、「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大な占めている(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)。
(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き、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）。

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年連続して増加している（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増加を続け、2019年１〜３月期には過去最多の955件に達している。その後ブランドの件数は横ばいなので、「Eコマース」は右肩上がりとなり、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）。

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含め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.を含むフィッシングの詐欺が特に多く、2018年4月から全体の55%を占めた。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端末を対象にして不審なアプリをインストールさせるという手口ののみだったが、iOS端末を対象にApple IDとパスワード、または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数が複数になったり、iOS端末に不審な構成プロファイアルをインストールさせたりする手口も確認され、少しずつ手口が
(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い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、実際に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の送金は確認されている。

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、利用者に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。（「1.2.8 (2) 傷のセキュリティ警告」参照）。

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年から継続していっている。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その後、2018年7～9月期に半減して2018年10～12月期に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ムサウエアは、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ムサウエ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ムサウエアに感染し1,133人分の診療記録が暗号化される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）。

非公開情報
「3.3.1 宅配便業者を装う不在通知SMSの手口」参照
「1.2.8 (1) 仮想通貨を要求する脅迫メール」参照
「1.2.8 (2) 傷のセキュリティ警告」参照
「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ィ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。

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ィ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、ウィ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。

「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にするために、遠隔操作ウィルス（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、「ダウンロード」を呼ぶ、別のウィルスを外部からダウンロードする機能を持つウィルスが「初期潜入段階」で用いられることが多かった。

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ィルスを送り込む。そして、ツールやウィルスを用いて、攻撃者はネットワークの構成の把握、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、不正な活動を隠すような手法も確認されている。

「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。

(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、特徴的な三つを挙げる。
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、ファイルが開かれた後C&C（Command and Control）サーバから「Koadic」をダウンロードし、感染させた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、修正プログラムを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を特定し、それぞれに対して偽名で交流を重ねていた。時間をおいて交流を重ねたことで技術者らが信用を得る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通じて、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るとしても、信用してい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、文部科学省をかたつめ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った。

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、コンテ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法が確認されており、今後も従来の対策をすり抜ける巧妙な手法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・訓練により攻撃手法を学ぶことによって、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（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サイト上で公開されており、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（組織内部の人物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 (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法がある。以下では、これまでに確認された手法について紹介する。

• 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のスクリプトで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す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、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 の文書ファイルに恶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ィルスに感染してしまうよう、という手法が確認されている（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ィ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ジ
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

情報セキュリティ白書 2019

ジにウィルスを配置し、受信者にウィ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、メールにウィ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こと、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聞くとただのテキストデータ（文字列）だが、Microsoft Excelで聞くと表データとして認識され、関数等が記載されている場合、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。

• 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る場合、マクロが有効化され、マクロが有効化される案件、攻撃者が意図した処理を実行できる。そのため、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ある。

(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考えられている。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
標的を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近し、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。

• 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る場合や、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する場合等、受信者を騙すために精巧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、不審であることが気付いた場合、メールアドレスが表示される送信者の名前の偽装等、標的型攻撃メールでの対策として注意が必要である。

受信したメールが不審な場合は注意喚起情報が掲載されている企業のWebサイトで確認するのも有効である。
・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。マクロ機能は標型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おり、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には、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型型攻撃メール、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が注意喚起の資料も公開している。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 (a) Microsoft Office の脆弱性と正規機能を悪用した標型型攻撃」というように、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
利用者が標型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、標型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るかは良いか分からず、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っ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型型攻撃を受けていることに気付くこともあるが、その場合でも、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、セキュリティシナリオの調査、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。セキュリティシナリオの未然防止、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、疑似的な標型型攻撃メールを利用者に送信し、そのメールへの対応を調査する訓練（標型型攻撃メール訓練）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に、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・向上させることができる。また、先に紹介したMicrosoft Officeのマーク機能やOLEオブジェクトを用いた標型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シナリオ作成し、インシデントが起きたことを想定して演習を行う。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う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を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、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、悪用されることが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聞く「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オブジェクトを含むファイルを埋め込んだファイルの攻撃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を使用するかいない場合、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くと、組織内の通信ログ等を目的に合わせて取得しておく上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。

- 適切な修正プログラムの適用
「1.2.1（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替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の脆弱性対策を検討する。

以上のよう、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
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令を関与する等の金融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、情報を窃取するウイルスが使用されることがある。

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、被害額が大きな事例としては、2017年11月に海外企業に送金を依頼された事例（表1-2-3項目1）に約30億円の被害をもたらしたが、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、保険で被害額の約9割を回復した事例もある。

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。

(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、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、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。

(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引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。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）。

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預金を要請するというビジネスメール詐欺が試みられた。メールの送信元として、A社のCEOの氏名とメールアドレスが使用されていた。

この事例では、A社の担当者がやり取りの途中で不
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

情報セキュリティ白書  2019

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）

<table>
<thead>
<tr>
<th>項番</th>
<th>報道時期</th>
<th>ガリヤー</th>
<th>被害額</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2018年6月</td>
<td>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</td>
<td>約1,400万ドル（約15億円）</td>
</tr>
<tr>
<td>2</td>
<td>2018年7月</td>
<td>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、東京都中央区の会社役員で男性4人と逮捕した。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、正常の取引で得たように装い、2017年7月4日〜21日に銀行等から計6,020万円を引き出した疑い。</td>
<td>約7,800万円</td>
</tr>
<tr>
<td>3</td>
<td>2018年8月</td>
<td>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&amp;ガッバーナ株式会社がBECの被害に遭った。</td>
<td>280万ドル（約3億1,000万円）</td>
</tr>
<tr>
<td>4</td>
<td>2018年9月</td>
<td>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1億870万円が不正に金銭と知りながら、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。</td>
<td>約1億800万円（うち9,300万円）</td>
</tr>
<tr>
<td>5</td>
<td>2018年10月</td>
<td>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容疑者を逮捕した。2017年3月、重機の輸出代金を装って、米国企業から騙し取った約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。</td>
<td>約300万円（うち200万円）</td>
</tr>
<tr>
<td>6</td>
<td>2018年11月</td>
<td>攻撃が会社のCEOになりすまして、顧客がカリフォルニアの山火事の影響を受けており、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した。</td>
<td>不明</td>
</tr>
<tr>
<td>7</td>
<td>2018年11月</td>
<td>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。</td>
<td>不明</td>
</tr>
<tr>
<td>8</td>
<td>2018年12月</td>
<td>Tecnimont Pvt Ltd（イタリアのEPC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のヘッダーのインディにメールを送った。更に彼は、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。</td>
<td>1,860万ドル</td>
</tr>
<tr>
<td>9</td>
<td>2019年1月</td>
<td>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。</td>
<td>約1,900万円</td>
</tr>
<tr>
<td>10</td>
<td>2019年2月</td>
<td>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詐欺を実行して、約1億1,000万円の被害が出たとし、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。</td>
<td>約1億1,000万円</td>
</tr>
</tbody>
</table>

■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）
審であると気付かず、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
とのおりである。

2018年7月9日、攻撃者は、A社のCEOになり
ますとし、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したが返信した
（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す
ようメールを送ってきた（図1-2-5の③）。

(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検証が「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」等は効果がなかったことに
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。

■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(継報)」

<table>
<thead>
<tr>
<th>項番</th>
<th>情報 提供日</th>
<th>事例概要</th>
<th>被害の 有無</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>2018年1月5日</td>
<td>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。</td>
<td>なし</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>2月16日</td>
<td>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向けた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すようメールを送ってきた（図1-2-5の③）。</td>
<td>あり</td>
<td>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</td>
</tr>
<tr>
<td>16</td>
<td>3月12日</td>
<td>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が、偽の振り込みを要求するBECが試みられた。</td>
<td>なし</td>
<td>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</td>
</tr>
<tr>
<td>17</td>
<td>5月17日</td>
<td>2018年5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、攻撃者が請求側企業の担当者になりすますBECが試みられた。</td>
<td>なし</td>
<td>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</td>
</tr>
<tr>
<td>18</td>
<td>6月4日</td>
<td>2018年6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、攻撃者が請求側企業の担当者になりすますBECが試みられた。</td>
<td>不明</td>
<td>-</td>
</tr>
<tr>
<td>19</td>
<td>7月6日</td>
<td>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から、電話で確認した。</td>
<td>不明</td>
<td>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</td>
</tr>
<tr>
<td>20</td>
<td>7月9日</td>
<td>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、ビットコインの購入準備を行うことが必要であると偽の振り込みを要求するBECが試みられた。</td>
<td>なし</td>
<td>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</td>
</tr>
<tr>
<td>21</td>
<td>7月19日</td>
<td>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から、電話で確認した。</td>
<td>なし</td>
<td>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</td>
</tr>
</tbody>
</table>

■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(継報)」
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

(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（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<br>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のように、着信者側でメールの送信者として設定された文字列が表示される。

![図1-2-6 Fromメールアドレスのイメージ]

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」でであり、実際にはメールは送付されていない。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]

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やすため、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、実際の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、結局同じ攻撃者への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つつも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]

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と考えられが、担当者はこの時点で不安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と、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。
(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る。そのため、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も被害が及ぼすことがあり、取引先全員に対しては、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発信者に巻き込まれた場合、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ることで、更なる被害拡大を防ぐことが可能となる。

(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ることで、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名を取得し、攻撃を行うことがある。

そのため、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、不審なドメイン名が取得されていた場合、事前にあらかじめ注意喚起を行う。併せて、取引先等に対しても、不審なドメイン名が取得されてしま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るようになる。

(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 や、もーグークレイド雲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
第1章
情報セキュリティインシデント・脆弱性的現状と対策

情報セキュリティ白書 2019

情報セキュリティインシデント・脆弱性の現状と対策

1.2.3 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃は、一例に、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、その手法と対策について解説する。

(1) DDoS攻撃の事例、及び抜粋事例

2018年度における、DDoS攻撃に関連する主な事例を紹介する。

(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法等が挙げられるが、これらの手法は他の攻撃手口に比べて比較的単純であるため、攻撃者が不注意に操作をすることによって、攻撃されることが多くある。

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増加している状況である（「3.2.1增大するIoTのセキュリティ脅威」参照）。

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

情報セキュリティ白書 2019

情報セキュリティインシデント・脆弱性的現状と対策
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、それぞれ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存在する。

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、多数のサーバがインターネット上でWebサイトを公開していることを悪用した攻撃である。送信元に偽装した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いが、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、送信元が偽装した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フラグメント攻撃を受けているように見えててしまう。

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アドレス情報に基づき、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必要とする。

(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遇した対策に加えて、管理、所有する端末のポー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、該当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する場合もあるため、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。

• 組織内での対処が不可能な規模的な攻撃や、有機的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、ウィ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した場合、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検討する。

• OSやファームウェアを最新の状態に保ち、脆弱性を密に感染するウィルスを防ぐ。

• 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に公開していないことやDDoS攻撃に悪用され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されている可能性があると判断し、ウィ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。

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。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、Windows7、WindowsServer2008及びWindowsServer2008R2のサポートが終了となる。一般的にサポート終了後は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。「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) ApacheStruts2の脆弱性を悪用した攻撃

ApacheStruts2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、ApacheStruts2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ApacheStruts2の脆弱性CVE-2018-11776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ApacheStruts2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）。

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。

1.2.4ソフトウェアの脆弱性を悪用した攻撃
（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される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、コインマイナーやサイバーインフラ等が奪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から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って、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行うことが必要である。同時に、事前に対策の実施手順を事前に整えておくことで、脆弱性の対応を遅滞なく着実に実施できる。更に、公表されているWebサイトのステージング環境※80を事前に用意しておくと当該Webサイトへの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、以下の内容をアラカルトで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
- 他組織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、対策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も推奨する。

（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」に新たな登場をみせている。この一つとして、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法を用い、感染させたIoT機器に別のホス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、こ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機器を狙うウイルスが登場する可能性がある。これを見据えて、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利用する
- 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
永く修正プログラムを適用する。
- 攻撃者が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WannaCry（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た。2018年になって落ち着きを見せているものの、WannaCry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2億2602万1,479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、2017年1〜3月期を除くと2018年4〜6月期は前期比約3倍増加した（図1-2-14）。

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仮想通貨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で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だけではありません。もしそ、手法が巧妙化し、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WannaCryによる攻撃が行われた4〜6月期を除くと前年同期より増加している（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台あたりも
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）。

個人に支払わせることが想定すると、身代金を極端に高額にすることができない。また、一般的に個人の端末では企業の端末に比べて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、企業には多大な端末や重要な情報が存在し、高額の金銭を得られる可能性が高いため、効率よく金銭を獲得したいと考える攻撃者にあたる。

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2億8800万円）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。

一方、ゲームに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秒以内の動作でいきなり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、被害者はジョークでは済まないものである。

（b）ランサムウェアと正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。

セキュリティベンダによれば、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。
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を受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行う。
\* バックアップに使用する装置・媒体は、バックアップ時にのみ対象機器と接続する。
\* バックアップ中は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、復旧においてそれ等活用できず、身代金支払いを選択してしまう対策の意味がない。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。

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。

1.2.6 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※91 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。

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 eID 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アカウントへの不正ロー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で、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「おいしい 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「よんだんコンシェルジュ」※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。

(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り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法である。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。

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。

(3) サービス提供者の対策
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スニー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。

(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法である。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）をしていない場合、不正ログイン被害に遭う可能性が高まる（図 1-2-16）。

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スニー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法である。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
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

情報セキュリティ白書 2019

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、従来とは異なる環境（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、利用者が正常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）。

（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、注意を呼びかける※112。

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

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

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
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 を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つ（「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、以下のように対処が可能。
対応をいく必要がある。
- クレジットカード情報を利用した場合:
  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。
- アカウントの認定情報を利用した場合:
  常に、不正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。
- 銀行口座情報を利用した場合:
  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、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場合、それを確認し、最新情報を継続的にチェックしていく必要がある。

（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の詐取を目的にした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。
ディーエルマークテクト株式会社
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日間の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。

株式会社洋菓子舎ウエスト
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出した可能性がある。※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
ジッ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、クレジット決済を完了した場合に「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。

<table>
<thead>
<tr>
<th>組織</th>
<th>サイト</th>
<th>公表日</th>
<th>概要</th>
</tr>
</thead>
<tbody>
<tr>
<td>聖教新聞社</td>
<td>SOKAオンラインストア</td>
<td>2018年10月9日</td>
<td>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。</td>
</tr>
</tbody>
</table>

2018年度、Google Playに偽のファイナンスアプリが見つかりました。※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、盗み出すものでした。

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、ルートやパソコンに設定される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。この手法は「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利用者がMEWの公式サイトにアクセスしようとする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。

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、様々なものがある。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全世界で多数出回った。JPCERT/CCから事例が報告され、一般財団法人日本サイバー犯罪対策センター(JC3)からも、犯罪被害につながるメールととして注意喚起がされている。IPAでも、「安心相談窓口だよ」にてこの手口を取り上げた。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。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
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

情報セキュリティ白書 2019

（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 tochいた」等）や家族や友人の連絡先情報を盗みとったと、事実無根の内容で脅す。

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に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もの不自然なものが多かった（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し、不正に設立された Winscarという名前のジョンクライア ラウンドウェアを感染させることを考えられたため、メールには暗号化処理が施されていたが、暗号化されており、加えて暗号化されたIPアドレスが同一であると判断された。

情報漏えいで流出した個人情報リスト、何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る場合は、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、ウイルス感染を防ぐ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は冷静な対応をとらできるよう、日々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、日頃から使いまわりしないよう、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法であるが、2018年度に入って相談件数が増加し、また手法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な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。こうしたことの取り組みにより、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」「システムが破壊される」「○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（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、以下のようないかがが多い。
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る
第1章 情報セキュリティインシデントの現状と対策

情報セキュリティ白書 2019

情報セキュリティセキュリティの現状と対策

るとして、遠隔操作による対応を支えかける。
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」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、ウィ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。

2017年ごろより、「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。

(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、画面を閉じてください。問題がない。Webブラウザの「X」（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
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」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、当初の状態にシステムを戻すことが肝要である。

利用者やオペレーターが偽のセキュリティ警報を表示された場合は、インターネットやセキュリティソフトにより正規の警告画面や、セキュリティソフト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が肝要である。

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もが遭遇する可能性があるから、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て、メッセージを極端に必要とする必要がある。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イカーのサポート窓口等の相談窓口を、あらかじめ確認しておくことで、冷静な対処がしやすい。

(3) 偽サイト
正規のサイトに見え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が以前より注意喚起がされていているが、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。
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。

(a) 偽 EC サイトの手口
偽 EC サイトとは、インターネット上の商品・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する等により、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」が提供されている。

(c) 対策
EC サイトを利用の際は、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身に付けるのが望ましい。例えば消費生活センターが案内している偽サイトの特徴を以下に記載する。
・ サイト内容: 字体（フォント）に通常使用されない旧字体
第1章 情報セキュリティ・不正アクセスの現状と対策

情報セキュリティ白書 2019

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】」(以下、JNSA調査報告書)によると、漏れ人数最多的インシデントは118万8,355人で、その原因は不正アクセスであった。なお、漏れ人数の上位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、前橋市の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内にて給食喫食していた同市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。

株式会社ダブルアイ・システムの事例※142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※145では、外部からの不正アクセスにより会員の個人情報が最大で8928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。

JN極端に値引きされている。機械翻訳したような不自然な日本語表現がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

JR九州ドラッグライブ株式会社の事例※142では、外部からの不正アクセスにより、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。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。

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、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報が最大で5万3,000件、クレジットカード情報が458件流出した可能性がある。
兵庫県立図書館の事例では、同館の利用者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名のメールアドレスを閲覧できること態態となった。

株式会社ユー花園の事例では、同社が運営する通信販売サービス「スワンフロリスト」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ていた。なお、そのうち1,412件は未達であった。

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。

山形市役所の事例では、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週間で並べてWebサイト上に誤掲載していた。

米国のExactis LLCの事例では、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、誤って公開サーバー上に置いたことで誰でも閲覧できる状態にしていたという。

(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の逸脱による「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では、アルバイト従業員が勤務中に利用者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者のクレジットカード情報が、最大234件が盗え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チアイディーが管理するWebサーバー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。

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、安全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件がクレジットカード情報も流出した可能性がある。

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WEBSTORE」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。

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。

8月2日 アサヒ緩解金属工業 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。

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、メールアドレスとパスワード、氏名、電話番号等の会員情報、延べ最大9万885件が流出した可能性がある。

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に改ざんされ、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。

■ 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）
(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であるが、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やその他の意識向上活動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、過失を生じること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
過失への対策とは異なり、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」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」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、保全是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。
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ため、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）が必要であること自体です。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、技術を迫る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。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用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」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の行動規範や、基本指針をまとめるにあたり、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。

注釈
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」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」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）。

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）に分類すると、2018年は、「クロスサイト・スクリプティング」が最多の12.9％、「パッファーエラー」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き、「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パアラウンド」の割合が増加している一方、「パッファーエラー」「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）を用いて、脆弱性の深刻度を公開している。なお、JVN iPediaではCVSSv2及びCVSSv3の二つのバージョンの情報
公開しているが、本項では 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）。

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と要因として考えられる。

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。
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

(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、これらを悪用した攻撃が数多く観測されている。

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、前節の CVE-2018-7600 及び CVE-2018-7602 を含む 3 件が CVSS v2 を用い最も深刻度が高いレベルⅢ (危険) とされている（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ー又はセキュリティベンダーから収集し、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くなった状態で 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 ヶ月に 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
で、古いフィーチャ・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する※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。

このような、技術やサービスが世の中に急激に普及していく段階で、それに伴う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、これからの急激な普及に伴い脆弱性が発見されることがあると考えられる。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十分注意を払う必要がある。

2018年8月には、急激に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なされた事例が確認されている※183。このような、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おいて脆弱性が発見され、情報セキュリティ早期警戒パートナーシップの届出がなされていない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なされた事例が確認されている※183。このような、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おいて脆弱性が発見され、情報セキュリティ早期警戒パートナーシップの届出がなされていない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なされた事例が確認されている※183。このような、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可能性についても十分注意を払う必要がある。

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続いている。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、これらの件数を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）。

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）。

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うちに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」で検討される予定である。
ににより行われている。

(1) ソフトウェア製品の脆弱性

2018年の中央には、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年には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。

--グラフ--

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 フレーセティ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をある。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では、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。

- 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。

--グラフ--

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。

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] 登録ベンダー一覧」に「脆弱性情報受付窓口」欄を設けた。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っている。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。

(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年も継続してい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。

(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。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む。

<table>
<thead>
<tr>
<th>ソフトウェア製品</th>
<th>サポート期限</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>2020年01月14日</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>2020年01月14日</td>
</tr>
<tr>
<td>Windows Server 2008R2</td>
<td>2020年01月14日</td>
</tr>
<tr>
<td>Office 2010</td>
<td>2020年10月13日</td>
</tr>
</tbody>
</table>

※189：

※190：

※191：
第1章 情報セキュリティ・脆弱性の現状と対策

情報セキュリティ白書 2019

では、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。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い企業が43%と高い数値となっている。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。特に、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に1年を切る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、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必要である。

(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。

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

※「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

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）。

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）。

<table>
<thead>
<tr>
<th>番位</th>
<th>溼えいした人数</th>
<th>業種</th>
<th>原因</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>118万8,355人</td>
<td>製造業</td>
<td>不正アクセス</td>
</tr>
<tr>
<td>2</td>
<td>67万6,290人</td>
<td>公務</td>
<td>不正アクセス</td>
</tr>
<tr>
<td>3</td>
<td>59万7,452人</td>
<td>情報通信業</td>
<td>不正アクセス</td>
</tr>
<tr>
<td>4</td>
<td>37万1,200人</td>
<td>情報通信業</td>
<td>不正アクセス</td>
</tr>
<tr>
<td>5</td>
<td>19万9,169人</td>
<td>公務</td>
<td>不正アクセス</td>
</tr>
</tbody>
</table>

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 | 溼えい原因 | 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日に株式会社あぐりーん※194が、同社が運営する農業系求人サイト「農家のおしごとナビ」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が、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、同社が運営する「ショッパークラウド」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。

(2)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発生しており、対岸の火事と言えないうちである。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。様々な脆弱性に対する多様な対策があるので、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、自組織の体制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
人の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である。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ので、自社Webサイトに関する脆弱性の報告を受け付け。
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

情報セキュリティ白書 2019

このほかにも一般的な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。

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受けるサービス「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が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ことは一般に難しい。このため、Webサイトを構築する事業者にとっては、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ベテナジスタ試験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のもかかわらず、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あったか振り返り、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。

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

<table>
<thead>
<tr>
<th>年</th>
<th>ソフトウェア製品</th>
<th>組み込み機器</th>
<th>割合</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>209</td>
<td>27</td>
<td>12.9%</td>
</tr>
<tr>
<td>2015</td>
<td>442</td>
<td>67</td>
<td>15.2%</td>
</tr>
<tr>
<td>2016</td>
<td>1045</td>
<td>160</td>
<td>15.3%</td>
</tr>
<tr>
<td>2017</td>
<td>462</td>
<td>64</td>
<td>13.9%</td>
</tr>
<tr>
<td>2018</td>
<td>328</td>
<td>78</td>
<td>23.8%</td>
</tr>
</tbody>
</table>

製品開発者が自己を作成する、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るリスクがあることが、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。

(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製造出荷数は328件うち、組み込み機器の届出は78件で、23.8%を占めている。年ごとの届出の増減を見ると、2014年12.9%、2015年15.2%、2016年15.3%、2017年13.9%、2018年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少ない年となった（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、セキュリティが72.7%、(c) 組み込み機器の情報セキュリティ対策

近年、ネットワークのような製品にもソフトウェアが組み込まれ、インターネットプロトコルを用い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たない。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、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。そのため、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が活用される。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 株式会社やサイボウズ株式会社が実施している。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、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ウェブ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。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。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。

(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の改訂がなされた。ISO/IEC 29147は、ベンダーによる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。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。

このような、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「ソフトウェア製品等の脆弱性関連情報に関す
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

情報セキュリティ白書 2019

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

一部取扱規程※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、特別な取り組みを実施する。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、製品開発者と連絡が取れない等の公表を前提とし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て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。その場合、届出の途中で、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。

　このような調整不備案件について、公表されないため、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ため、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が公開すると、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する様々な要素を考慮しつつ、製品利用者が被害を受け可能を可能な限り低減するため、IPAでは、調整不備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、脆弱性情報が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。
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」（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み」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。

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いものです。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。

情報セキュリティインシデント・脆弱性の現状と対策

第1章
情報セキュリティ白書    2019

59

情
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全般で策定される。同戦略全般の事業局である内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity: NISC）は、関連府省庁等と連携し、「サイバーセキュリティ戦略」、「政府機関等の情報セキュリティ対策のための統一基準群」、「重要インフラの情報セキュリティ対策に係る行動計画」等の策定、並びにサイバーセキュリティに関わる施策、国際連携、国民への普及啓発等を推進している。

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を策定後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」(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う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
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である。個人や組織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、「経済社会の活動の向上及び持続的発展」「国民が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。

• 経済社会の活動の向上及び持続的発展
経済産業省とIPAは、経営者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の観点※6のもとに設置した情報開示分科会での検討を踏まえ、業界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、「サプライチェーン・プラットフォーム」を2018年6月に開設し、2019年度も継続して開催している（サプライチェーン・プラットフォームについては「2.12 (1) (c)」参照）
WG3（サイバーセキュリティビジネス化）参照】)。
経済産業省は、サイバー空間と物理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、全産業には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」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(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制に反映する等、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とのサイバーリンク」参照）。

(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4次行動計画」（以下、第4次行動計画）※17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。

・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。
第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

(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保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る場合に、その障害が社会に与えた影響の深刻さを表るものである。

評価基準は、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が検討される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分野におけ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で、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状況にも対応できることを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。

産業サイバーセキュリティ研究会

WG1 シチュエーション何か層技術・標準化

WG2 シチュエーション何か層技術・標準化

WG3 シチュエーション何か層技術・標準化

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、これを価値創造過程（バリューサプライチェーンプロセス）と定義した。また、バリューサプライチェーンプロセ

第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019
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）」（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クンググループ（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。※26

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、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。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。※27

CPSFでは、産業社会を三つの層で整理した「3層構造モデル」とともにセキュリティ確保のための信頼性の基盤を明確化するとともに、バリューチain線の導入に関連する、セキュリティ対策を講じる最小単位として「六つの構成要素」を提示している。これに基づいて、リスクを洗い出し、その対策要件※28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: バリューチain線に参加する企業・団体・組織
  ヒト: ソシキに属する人、及びバリューチain線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・解析・シミュレーションを通じて加工された情報
  プロセージ: 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、バリューチain線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関連する主体も、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タスクフォースやオープンソースソフトウェア等の活用・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 ※29」
情報セキュリティを支える基盤の動向

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）」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ダンス」を実践する上で参考とならないように、「サイバーセキュリティ経営ガイドラインVer 2.0」を公開した（プラクティスに於いては「2.4.1 (2) (c) サイバーセキュリティ対策の在り方」参照）。

まと、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。なお、IPAでは同年3月、主に中小企業の経営者とIT担当者を対象として、「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（「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備等を実施した（「2.3 情報セキュリティ人材の現状と育成」参照）。

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」を発足させた。本検討会では、「未来投資戦略（2018）」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（仮）」に反映することを想定している。

安全性評価の制度設計にあたって、情報・情報システムのクラウド区分、及びクラウドサービスの安全性評価の制度そのものに二つの観点における議論が行われていっている。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（仮）」では、特に他者との接続を含め、各政府機関基本的なクラウドサービス要件を設定し、一定の基準を満たしているということが示された場合に、各政府機関等と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に、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」を開発した。一方で、IoTやAI（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、「AI・データの利用に関する契約ガイドラインver2.0」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、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、②PoC（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。本法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」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することの、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等の一部改正に伴い、中小企業にITツールを提供する「情報処理支援機関（スマートSMEサポート）」として認定する制度が創設された。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、中小企業経営者に対する登録情報開示や中小企業の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サポートに対して、中小機構とIPAから、中小企業経営やサイ
第2章
情報セキュリティを支える基盤の動向

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。

（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ため、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。

IPAは2018年7月から、審査登録機関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」を公開している。

IPAは2018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。

（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、官民連携により対策を目的として、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）を運営している。

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、サイバーセキュリティの低減を目的としている。

2019年3月末時点で、IPAを情報の中継・集約点（情報ハブ）とさせて13の領域（SIG）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
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クウンシルのC'TAP*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。

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

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（ビジネスメール詐欺については「1.2.2 ビジネスマル詐欺(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年度でも多く発生し、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月ごろから観測されているブランク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。特定の対象に対して議論を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年まで観測されてきたよう、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。国内内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制・低減
・標的型攻撃による機密情報活動等の関連の遮断
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、被害緩和の対応の相談を「サイバーレスキュー活動」として実施している。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
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りず、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。
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」を設立した。
同タスクフォースは、2017 年4月、IoT セキュリティ対策の方向性となる「IoT セキュリティ対策に関する提言※62」をまとめて、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 プログレッブルポート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。

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」を設立した。
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、同月10日には、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 プログレッブルポート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 プログレッブルポート2018」
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、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。

  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」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。

  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。

  2018年7月、総務省は、本調査により検出した脆弱な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ある27件、パスワード設定は設定されているものの認証画面がインターネット上で公開されていたものがある9件であった。

  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」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。

  これにより、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。

  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」を開始した。

  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、効率的な広域的な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ット技術の研究開発に取り組んでいる。

AI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クスフォースのもとに「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」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」「契約者間等の情報公開」「社会に対する情報公開」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門をつなぐ橋渡し人材育成が必要とされている。次に、「契約者間等の情報開示」では、プライバシー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されている。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されている。

総務省では、これらの検討を踏まえ、第三者間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。

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クスフォースのもとに「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」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」「契約者間等の情報公開」「社会に対する情報公開」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門をつなぐ橋渡し人材育成が必要とされている。次に、「契約者間等の情報開示」では、プライバシー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されている。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されている。

総務省では、これらの検討を踏まえ、第三者間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。

(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コンペティエンタルコース向けのコースを新設した。

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。

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、大会開催時に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策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。

(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、IT機器を悪用したDDoS（Distributed Denial of Service）攻撃の発生等の環境変化踏まえ、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図るためのTrarde 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、法制等に基づき、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*96。

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
セキュリティを支える基盤の動向

情報セキュリティ白書 2019

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。

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、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。

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。

(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・分析を通じて、インターネット上の違法情報の積極的な取り締まりを行っている。

警察庁では、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。

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オンラインセンター（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・有害情報を削除を進めている。

(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、「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。

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、ダークウェブの実態調査、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。

(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ま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、同期だけで被害額は約6億3,820万円相当になり、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。

(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（ID・パスワード等）を入力して不正に利用する識別符号増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、取引先等になら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、サイドバーで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未遂罪の疑いで逮捕した※114。

•2018年10月、奈良県警察は、奈良県内男性職員が、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」と書き込んだ上で、URLへのアクセスを誘導していた。

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、サイト閲覧者が無断で、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を無断で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。

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）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。

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）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。

(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、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暗号（RSA 暗号、格円曲線暗号）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かったため、「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、インタラ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。
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す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とっては、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。

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であり、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。

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。

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_kaiyakuuntaryu/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超えてつながり合い、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っています。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、国際連携が必要である。本稿では、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。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・共同ビジョン」が盛り込まれた。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ノウハウ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・実用化における日本の台頭、強制的な技術移転・データフローキャノン化政策の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。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レベル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めた課題に関し共同歩調をとることを確認した。これは、従来の両国政府の主張である「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スペース」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。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パーソナルセキュリティ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本国際の自由貿易協定（Trade Agreement on Goods:TAG）の交渉が中心となり、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と、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。今後サイバーフェイス面での協力が加速されると思われる。

(3) EU諸国とのサイバーリネン
EU地域とのサイバーリネンの状況について述べる。

(a) 日EUサイバーリネン
2018年3月5日、第3回日EUサイバーリネン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、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対策等が共同声明に盛り込まれた。

第4回日EUサイバーリネンは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リネン
2018年6月12日、第4回日仏サイバーリネン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議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・正直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持意した。

(c) 英国とのサイバーリネン
2018年3月16日、第4回日英サイバーリネン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外務省サイバーリネン政策部長が務め、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等の新興テクノロジーの機器の保護や悪意のあるサイバーアクティビティへの対策、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回日英サイバーリネン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・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軸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リネン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は、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に対処し、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リネン
2018年11月16日、第4回日・イスラエルサイバーリネンがイスラエル・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リネン
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回の討論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いる。同年12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。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。同会議ではASEAN加盟国からの情報通信関係政府機関の代表者と、日本からの関係省庁の審議官が参加した。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、サイバーセキュリティに関する懸案事項、重要な情報交換の形での情報交換、人材育成の3点における協力が明記されている。特に、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。

(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）と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会期会合が開催された。日本からは大輪審議官が出席し、共同議長を務めた。会合では、情報通信機器の安全対策を含む情報通信関連政策のための取り組みを提案し、各国の協力が確認された。

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」とも称される事態に至っている。一方、2018年前半の懸案であった北朝鮮の核問題は、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、停滞が見られる。こうした中、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）を署名し、この中で中国のHuawei Technologies Co., Ltd.（以下、Huawei）等の製品を連邦政府が調達することを禁止した。更に同年12月5日、HuaweiのMeng Wanzhou CFO（Chief Financial Officer：最高財務責任者）が米国の對イラン制裁に違反した疑いにより、カナダで逮捕された。
情報セキュリティを支える基盤の動向

第2章

情報セキュリティ白書 2019

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、とする見方もある。※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ウラ

2018年9月、トランプ大統領は国家サイバーウラ (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 Interests)※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、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。

② アイオンド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、業界横断的なソリューションをステークホルダーに検討させ、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。

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、契約等の仕方において、DoDの調達事業者が懸念となっているが、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。

革新型の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。

第2章
情報セキュリティを支える基盤の動向

83
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っていくことが求められる。

海外の犯罪者の身柄確保、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、今後の新たな取り組みが期待されることが注目されている。

(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の実用化を進める。評価する市場構築に向け、企業・公共団体等のスタークラウド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、標準やベストプラクティスを常に行う。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、プライマリー企業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最先端技術を検証し、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。保護主義や国家の制限等によるデータの不当なロ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自体の標準化・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、設計、更新等のライフサイクル管理におけ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米国の情報通信ネットワークへの敵対的国家の進入・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検討する。
- グローバルな知的財産保有の仕組みを育成し、敵対的国家が米国の研究開発成果不正利用を防ぐために、国際協力の促進を図る。
- 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通を防ぐ。

③高度なサイバーロジックの育成を行う。
- 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を政府への再雇用、再教育に推進する。
- 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項目が注目深い。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）に言及しているが、これらについては、民主党ももちろん、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。

(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
第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

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スペースに基づき、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。
- 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、法で行う。
  - 恶意のあるサイバー活動を阻止するため、必要な対応を実施する。
- 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、情報操作に事前に対応する。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重要であることを示している。

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。

② オープンで相互運用でき、高信頼かつ安全な通信インフラ構築を推進する。
- 監視に反対し、自由な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。

(e) 反響

本戦略は2003年以降で最も包括的なものと評価もあり、メディア・セキュリティ関係者が多数コメントしている。戦略の特徴に関しては、以下のよう指摘がある。
- 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。
- 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・実施が始まされている。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関するように、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。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在を懸念す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。

- 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イ、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。なお、国家サイバー戦略は踏襲されている。
- 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。同戦略はDoDのようないく具体的国家を想定せず、以下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。
- 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。
- 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ーと連携、情報を共有してリスクに対処する。
- 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ーと連携、情報を共有してリスクに対処する。
- 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ーと連携、情報を共有してリスクに対処する。

(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。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、サイバー軍の戦闘力の拡充、等の懸念が示されている。トランプ政権、DoDの今後の施策が注目される。
第2章 情報セキュリティを支える基盤の動向

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 奉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) 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。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たが、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。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もので、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いまいであると思うわれるが、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。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) は、2018 年度中の加盟国の国内法整備が完了し、基本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) 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、企業ごとの異なる国の監視当局に対して提訴した。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。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、制裁が厳しく行われるとなれば、Google など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。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。GDPR 発効以前の最高額となるが、事業者の被害規模 (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、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。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流出事案に科された 8 万ユーロ (約 990 万円) であった。また、GDPR 発効後、データ主体（個人情報処理者）に対する権利が強化され、企業は従来の対応から大きく変更が必要となった。
(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プロテクションに関する ePrivacy Regulation (ePR) 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 を大幅に改訂したもので、GDPR の特定領域における電気通信における不正な監視等防止の目的を有する。Cookie を始め、ユーザ情報の取得に対し、ユーザの同意が求められる。プライバシー侵害行為には GDPR と同様な罰則がある。

EU 離脱 (Brexit) に伴い、EU 内におけるプライバシー規定が適用されるが、Brexit が実施されて、EU が GDPR を優先的に適用する。EU 内でのプライバシー保護に対する意識は高まっている。この意識の高まりは各国共通で、例えば、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』

EU 離脱（Brexit）を控えた英国においても GDPR の適用は始まっているが、Brexit が実施されると、EU の GDPR は英国の連携目標とされ、EU 諸国との自由な個人情報の移転が可能となる。このため、英国は、GDPR と同等なデータ保護を提供し、GDPR 第 45 条に従って包括的合意を交渉する必要がある。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。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 と協議を続けているが、2019 年 1 月 23 日、包括合意が発効した （2.2.1 (3) EU 諸国とのサイバーサークル）参照）。これにより、日本・EU 間の個人情報を含むデータの移転がスムーズに行えることとなり、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、監視当局の監視が強化される。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を合意し、EU との合意なき離脱をかわすため、交渉が進まないことが懸念される。5 月 24 日にメイ首相が退任を表明等、英国の内情は混乱し、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 にも望まれているが、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と懸念される。今後の英国、EU の交渉が注目される。
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。まずENISAについては、これまで時間制限が設けられていたが、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目的としている。更にEU域内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目的としている。

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る、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じ認証で担保したいとの意図があると考えられる。前述のNIS指令に関する各国支援に加え、後述するEU域内の統合的なサイバーセキュリティ認証制度についても、ENISAが新た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る、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じ認証で担保したいとの意図があると考えられる。前述のNIS指令に関する各国支援に加え、後述するEU域内の統合的なサイバーセキュリティ認証制度についても、ENISAが新た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る、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じ認証で担保したいとの意図があると考えられる。前述のNIS指令に関する各国支援に加え、後述するEU域内の統合的なサイバーセキュリティ認証制度についても、ENISAが新たな型を提供すること、とされている。

(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。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し、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、本指針での判断は加盟国に任されたことになる。このうちイギリスの賢首相は同年4月23日、5Gネットワークの調達ベンダーとして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。この決断に先立ち、米国の監視機関（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。一方、イギリス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。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。

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っている。

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实上強制され、それにより政府の監視が強化されるとの懸念から、中国国内にデータセンターを構築する等の対応が迫られている。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※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%に引き上げるとし手続きに進んだ※199。第8回協議で国内法の改正を約束していた中国が大破返したとされ、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保障に関する大統領命令※201に署名し、Huaweiに対する自国製品の取引を事実上禁止した※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つつつ（「2.2.3 欧州の政策」参照）、米国と交渉ていくものと思われる。米国も、これまでこうし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、中国政府は「国务院关于印发社会信用体系建设规划纲要（2014-2020年）」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※205。2018年以降、この計画の全貌が明らかになっている※206。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し、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に許可を与えている※209。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社会信用を構築しようとしている。信用度の高い人を明確にし、アドバンテージを与えたりするやり方は、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。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。

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米欧においては、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、社会信用スキーム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。

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はいち早く情報を受け取ることや、他国とのネットワークを密に取ることで、情報共有やサイバー脅威に対する対応力の強化が求められている。このため、National CSIRTとしての役割の重要性から、各国で新たな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。特に、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）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、ASD（Australian Signals Directorate：オーストラリア通信電子局）の傘下に置かれるにいたった。このACSCは、組織改編の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、国内全般的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ウェア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」との中で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）の傘下でNCERT（National Computer Emergency Response Team）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わる技術面でのAPNIC（Asia Pacific Network Information Centre：アジア太平洋ネットワーク情報センター）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（22.5.2 アジア太平洋地域のCSIRT間連携）
(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」が National CSIRT である Sri Lanka CERT/CC 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ブラッドに加えて、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されている。

(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が施行された。同法により、National CSIRT である SingCERT を擁するサイバーセキュリティ庁（Cyber Security Agency: CSA）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明記された。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や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、運営委員会の一部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、センターを用いたサイバー脅威動向の
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 機器に関連するトラブルが引き起こすデータ漏えい」をテーマに実施された※220。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等により、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 の国※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。
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。これは、APECに参加している日本やカナダ、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。

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。更に、認証を受け取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、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）」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で、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。

---

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/u71kba0000000000ks3-att/20180531-jipdec-cbpr-3-ks3.pdf](https://www.jipdec.or.jp/sp/topics/event/u71kba0000000000ks3-att/20180531-jipdec-cbpr-3-ks3.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おき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、「セキュリティマイナー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る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層で整理をしている。

• 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理し、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指している。

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（リスク）の洗い出し
② 機能を担う役割（ロール）の整理

2.3.2 情報セキュリティ人材の現状
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」は、ユーザ企業におけるセキュリティ機能を、事業に関連した役割と、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ベンダー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
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、それはIT人材の65.4%がユーザ企業に所属しているためである（図2-3-3）。また、日本のIT人材の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下で認識し、以下の役割を担っている。

- 価値創出のための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たが、全体としてのリスクマネジメントとしてセキュリティ統括機能を設けることとしている。

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、企業ごとで様々に実現を目指している。

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廃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、主に次のものがある。

- IPA:コンピテンシディクション※241（セキュリティについて、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の必要な役割を、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、セキュリティ管理系、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おり、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」「フォレンジックス系」「SOC/CSIRT系」の四つのカテゴリに沿って整理が検討されている。
(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）。

よっておらず、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。

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
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、自身の伸ばすべき領域を把握できるよう、セキュリティ人材の配置や自組織に不足している人材を把握し、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られたものが望まれる。セキュリティ人材の様々な役割に応じた評価が得られる共通の評価指標と、それにしっかり紐付けられ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関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した際に、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：ものづくりの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、セキュリティ総括人材と呼称しており、図2-3-5 (97ページ)
に示した、戦略マネジメント層としてセキュリティを支える基盤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」を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、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構成し担当する部門が設置され、セキュリティに関連したキャリアパスが形成されることが期待される。

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、セキュリティ経括機能のさらなる明確化、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・社会を支える社会基盤や産業基盤のサイバーセキュリティ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、社会基盤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」の三つの事業に分けて構成している。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」を開設した。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。
セキュリティはOT分野の「防衛技術・ベテナリー分割」「インシデント対応・BCP」、IT分野の「ITセキュリティ」の3領域を基軸として、ビジネスマネジメントに関しての実務者による講義、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。
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セキュリティ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に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アメリカにて、英政府・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セキュリティ対策の取り組みに関する講義を実施した。
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の専門家から、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通演習」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ステム対応に従事したり、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内外でのセキュリティ活動に参加したりする等、1年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終え、その成果を受けて、各業界から参加した受講生たちは、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終え、その成果を受けて、各業界から参加した受講生たちは、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終え、その成果を受けて、各業界から参加した受講生たちは、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終え、その成果を受けて、各業界から参加した受講生たちは、様々な場面で活
講生同士の絆（人脈）ができたこととが財産とコメントもあり、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企業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。受講者には、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実施した。

(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、経営戦略企画、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、幅広い業種の人材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
第2章 情報セキュリティを支える基盤の動向

情報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的に、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 情報処理安全確保支援士のロゴマーク

登记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、登记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で、ITを活用した事業促進をセキュリティに進めることができる。また、登记セキスペが、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、信頼度を高めることができる※255。ITベンダー企業においては、登记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) 登記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では登記セキスペを対象として、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 登記セキスペ (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 登記セキスペの所属組織の組織長 (①の対象者から紹介による、回答数170、ヒアリング5)

主なアンケート項目は、担当業務や業務の難易度、登記セキスペ制度の活用状況等である。登記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。

ユーザ企業においては、登記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で、ITを活用した事業促進をセキュリティに進めることができる。また、登記セキスペが、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、信頼度を高めることができる※255。ITベンダー企業においては、登記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。

(a) 登記セキスペの IT との関わり方

登記セキスペは、ITベンダー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であり、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 登記セキスペの 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・監査等を請け負う」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記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の種類

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）。

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）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割強いためである。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。

(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・サービス提供に関わらない部署に所属」の回答者が3割強いためである。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。
情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

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、登録セキスペの入材タ
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
を全般に担当する人材

• ITライフサイクル全般に関わるセキュリティ確保
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入材数を合計すると、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。

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
リティ分野の新入材を育成する活動が行われている。

(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
る若年層のセキュリティ人材を育成・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 日に東京で開催された全国
大会が開催され、85 名が参加した。主に若
年層を対象としたセキュリティ・キャンプもセキュリティ
人材育成に重点的地域（兵庫／高知／山梨／三
重／北海道／愛媛／岡山／石川／秋田／福
岡）で開催された。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。

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。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。

(2) SecHack365

SecHack365 は、25 歳以下的学生や社会人約 40 名
を対象に、セキュリティに関わる活躍する人材の
育成を目的として NICT が主催する長期ハッカソンで、
2017 年度から日本全国各地において開催され
る。2019 年 3 月 8 日に東京で開催された成果発表
では、本プログラムの優秀者による発表のほか、トーナー
によるパネルディスカッションが行われた。

(3) enPiT

enPiT（教育ネットワーク for Practice 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
度度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。

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。
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というプロト仕の人材育成のための教育コースを幅広く展開している。

(4) SECCON 2018

JNSAは、日本における最大規模のCTF大会である「SECCON 2018」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、実力の競い合った。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。

SECCONではその他、CTF未経験者でも参加可能な「SECCON Beginners」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」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。
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2018（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）。

(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

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。

NRIセキュアテクノロジーズ社調査にみると、CISOに

第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

107
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。

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78.4%であり、日本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。

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。

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78.4%であり、日本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。

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。

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。

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。

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。

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。

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。

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。

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。

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。
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」／事業部門が自社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、経営の関与度が高い、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高位者とされ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が期待される。
・「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」企業群よりも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自体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、セキュリティが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。
・事業に求められ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られる。

（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」の「重要10項目」に対する具体的な対策の实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。
これを受けた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、ヒントをまとめられている。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部ともなることが期待される。
(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年以前の全世界の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8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-3.1%～13.1%であるのに対してISMSは18.7%と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。

(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 15001:2018 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

![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®を基にIPAが作成

![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

![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®を基にIPAが作成

![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
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」によると、IT の使用が業務上の「必須」、また「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」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」を設け、中小企業と関係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」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は「ほぼ実践している」と「十分ではないが実践している」を合計すると、84.6% と最も多く、次いで「不審な電子メールを受信したときはルールを決めたり、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 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 対策支援事業」（通称：IT 対策支援金）において 2018 年度に引き続き申請要件となり、また公益社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
セキュリティ対策促進助成事業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6万超えていた。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」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Ver2.0」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。

(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

112
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支援ネットワークプロジェクト」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）。ISEN調査報告書にのって、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）。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メモリー」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。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。

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、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。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。

(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、大学等が自立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図ることが重要である。
インシデント対応体制の高度化等が検討される。

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。

NII-SOCSでの情報共有・連携を図るため、2018年度からはますます情報セキュリティ対策の実施状況について述べる。

表2-4-1 大学における主なセキュリティインシデント

<table>
<thead>
<tr>
<th>公表日</th>
<th>大学名</th>
<th>概要</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018年</td>
<td>公立大学法人横浜市立大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>6月6日</td>
<td>学校法人北海道大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>6月22日</td>
<td>国立大学法人弘前大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>6月27日</td>
<td>学校法人明治大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>10月24日</td>
<td>国立大学法人兵庫教育大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>12月17日</td>
<td>国立大学法人奈良先端科学技術大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
<tr>
<td>2019年</td>
<td>国立大学法人東京理科大学</td>
<td>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URLに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ID及びパスワードを入れた29名宛と届いた3,512通のメールが正規のメールとは異なりとされていた。メール本文や添付ファイルに含まれていた氏名や住所、電話番号等の情報が漏洩した。</td>
</tr>
</tbody>
</table>

(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市町村を対象に実施している。ここでは2018年度の調査結果に基づき、地方公共団体の情報セキュリティ対策の実施状況の変化について述べる。

表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みると、2017年度と2016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54.9%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分類がされておらず、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ある。

「3. 情報セキュリティ対策の実施」については、「サーバルミント等の入退室管理を行っている」等の個別対策の実施率は、「緊急時対応訓練を実施している」の実施率は、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
第2章
情報セキュリティを支える基盤の動向

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いるものの、運用状況の監査や、定期的な報告義務等の実施状況は高くない。業務委託先からの情報漏えい等のイベ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。

### 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）

<table>
<thead>
<tr>
<th>No.</th>
<th>対象項目</th>
<th>対策実施率</th>
<th>対策実施率</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>都道府県</td>
<td>市区町村</td>
<td>都道府県</td>
</tr>
<tr>
<td>1</td>
<td>情報セキュリティの責任者や管理者等の任命の有無</td>
<td>100.0% (0.0ポイント)</td>
<td>98.7% (+0.6ポイント)</td>
</tr>
<tr>
<td>2</td>
<td>緊急時対応計画を整備</td>
<td>97.9% (+4.3ポイント)</td>
<td>55.1% (+5.4ポイント)</td>
</tr>
<tr>
<td>3</td>
<td>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</td>
<td>100.0% (0.0ポイント)</td>
<td>88.3% (+2.9ポイント)</td>
</tr>
<tr>
<td>4</td>
<td>情報資産について、機密性、完全性及び可用性による分類</td>
<td>70.2% (0.0ポイント)</td>
<td>49.7% (+5.1ポイント)</td>
</tr>
<tr>
<td>5</td>
<td>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</td>
<td>68.1% (+4.3ポイント)</td>
<td>38.3% (+2.1ポイント)</td>
</tr>
<tr>
<td>6</td>
<td>サーバ室等の入退室管理を行っている</td>
<td>100.0% (0.0ポイント)</td>
<td>99.1% (+0.2ポイント)</td>
</tr>
<tr>
<td>7</td>
<td>サーバ等への停電や免震対策を実施している</td>
<td>100.0% (0.0ポイント)</td>
<td>98.6% (+0.2ポイント)</td>
</tr>
<tr>
<td>8</td>
<td>重要な情報に含む紙媒体を適切に管理している</td>
<td>100.0% (0.0ポイント)</td>
<td>97.4% (+0.8ポイント)</td>
</tr>
<tr>
<td>9</td>
<td>CD-R、USBメモリー等によるデータの持ち出し、持ち込みを制限している</td>
<td>97.9% (0.0ポイント)</td>
<td>96.8% (+1.5ポイント)</td>
</tr>
<tr>
<td>10</td>
<td>クラウドサービスやデータセンターを利用している</td>
<td>93.6% (+4.2ポイント)</td>
<td>84.4% (+2.3ポイント)</td>
</tr>
<tr>
<td>11</td>
<td>情報セキュリティ研修を職員に対して実施している</td>
<td>100.0% (0.0ポイント)</td>
<td>89.6% (+2.8ポイント)</td>
</tr>
<tr>
<td>12</td>
<td>緊急時対応訓練を実施している</td>
<td>74.5% (+6.4ポイント)</td>
<td>26.2% (+3.4ポイント)</td>
</tr>
</tbody>
</table>

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」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。

### 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」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バッチの更新」をしている割合が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）である。
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、セキュリティソフトの更新やセキュリティソフトの導入でウィ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。これら対策を実施していても、不意にファイルをダウンロード、実行することでウィルス感染に至ることがある。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Google PlayやAppStoreでも不正なアプリが公開されていた事例もある。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化している割合は 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年度の携帯電話類の遺失届は 257,718件（*316）の数値を確認している。
第2章
情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

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、パスワードが悪意の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。サービスにおいては、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く、推測されにくいものとし、使い回しをしないこと」が最も高く、次に該当するものが続く。スマートデバイス利用者の実施率は低くない（図2-4-14, 図2-4-15）。

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。特にパスワード設定の実施状況は、利用者のセキュリティ意識を反映しているため、今後とも改善の余地があると考えられる。
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29%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%であるとされている。

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必要不可欠である。

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を守るための「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、家庭でのルール作成、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・安全な利用のために、「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）として実施している。

(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、全国の小学校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（主にウィ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の教育を促進するための普及啓発活動として実施している。
第2章 情報セキュリティを支える基盤の動向

情報セキュリティを支える基盤の動向
情報セキュリティ白書 2019

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」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月に賛同を公表した。

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」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標し、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」(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」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。

・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。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」
- IPA「はじめまして、ペアコです。〜親と子のスマホの約束〜」
- 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〜」
- 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!」

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。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。

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!

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 e-ネットキャラバンの実施」に紹介した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きた。2018年度は、「情報通信の安心安全な利用のための標語」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を作成し、2018年10月〜11月に秋の一斉キャンペーンを実施した。

（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、セキュリティ在例をテーマとして「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、周囲の人々を誘導しようとする意図のある方々を「SPREAD 報告セキュリティサポート」として認定し、必要な知識を伝えつつ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）。サポートの年齢制限はなく、年齢枠の能力検定試験により認定される。2019年1月1日時点でのサポート数は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、多くの関連企業と連携して、「STOP！パスワード使い回し！キャンペーン2018年」に誘導啓発活動を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 セキュリティ大ニュース」等）や調査資料（「2017年情報セキュリティインシデントに...」）を展開している。
第2章
情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

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。同イベントでは、イント・スマートフォンの安心・安全な利用方法を紹介し、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や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」

(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の提供を図っている。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) 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) サイバーセキュリティ小説コンテスト
「サイバーセキュリティ小説コンテスト」(出典) JNSA「サイバーセキュリティ小説コンテスト」

■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」

(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「ひろば Timber・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、年間で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セミナー・ポスターの募集（コンケール開催）や、地域の組織や団体向けのセキュリティ
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ー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。
第2章 情報セキュリティを支える基盤の動向

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！救急車を呼ばれなけりゃ！」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」と言っているんです。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？」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、衛生的よくないし、自分もいやな気分になるから拾って捨ててるよね。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かもしれないね？誰かの目を通して自分を見るのはなく、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』をもらおうと、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るような情報発信をしてきたか、振り返ってみませんか？
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いるされる国際的な共通規格であり、国際標準と呼ばれることを「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。

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」において国際標準化を知的財産政策の第1項目に掲げ取り組んできた。「知的財産推進計画2018」において、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を目指している。

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「デジタル標準（de jure standard）」、いくつかの団体が協力して自力的に作成する「フォーラム標準（forum standard）」、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、ビジネス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、時間をかけてデジタ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タ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、当該デジタ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。
第2章 情報セキュリティを支える基盤の動向

ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission):国際電気標準化委員会(Joint Technical Committee 1:第一合同技術委員会)は、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、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。

ITU-T(International Telecommunication Union Telecommunication Standardization Sector):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もSG(Study Group)17が設置され、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。

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。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。

2.5.2 情報処理関係の規格の標準化

IS規格化プロセス

<table>
<thead>
<tr>
<th>ステージ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP</td>
<td>研究期間(Study Period)</td>
</tr>
<tr>
<td>NP</td>
<td>新作業項目(New work item Proposal)</td>
</tr>
<tr>
<td>WD</td>
<td>作業原案(Working Draft)</td>
</tr>
<tr>
<td>CD</td>
<td>委員会原案(Committee Draft)</td>
</tr>
<tr>
<td>DIS</td>
<td>国際規格案(Draft International Standard)</td>
</tr>
<tr>
<td>FDIS</td>
<td>最終国際規格案(Final Draft International Standard)</td>
</tr>
<tr>
<td>IS</td>
<td>国際規格(International Standard)</td>
</tr>
</tbody>
</table>

TR/TS規格化プロセス

<table>
<thead>
<tr>
<th>ステージ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP</td>
<td>研究期間(Study Period)</td>
</tr>
<tr>
<td>NP</td>
<td>新作業項目(New work item Proposal)</td>
</tr>
<tr>
<td>WD</td>
<td>作業原案(Working Draft)</td>
</tr>
<tr>
<td>CD</td>
<td>委員会原案(Committee Draft)</td>
</tr>
<tr>
<td>DIS</td>
<td>国際規格案(Draft International Standard)</td>
</tr>
<tr>
<td>FDIS</td>
<td>最終国際規格案(Final Draft International Standard)</td>
</tr>
<tr>
<td>IS</td>
<td>国際規格(International Standard)</td>
</tr>
<tr>
<td>DTR/PDTR</td>
<td>予備技術報告(Preparatory Draft Technical Report)</td>
</tr>
<tr>
<td>DTS/PDTS</td>
<td>予備技術仕様書(Preparatory Draft Technical Specification)</td>
</tr>
<tr>
<td>TR/TRS</td>
<td>技術報告書(Technical Report)</td>
</tr>
<tr>
<td>TS/TS</td>
<td>技術仕様書(Technical Specification)</td>
</tr>
</tbody>
</table>

図2-5-2: ISO/IEC JTC 1/SC 27における文書のステータス

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)

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(Preparatory Draft Technical Report)

PDTS:予備技術仕様書(Preparatory Draft Technical Specification)

DTR:技術報告書(Technical Report)

DTS:技術仕様書(Technical Specification)
以下に、各WGの活動概要を述べる。

(1) WG1（情報セキュリティマネジメントシステム）


(a) ISO/IEC 27001:2013に関する手引きや指針の国際標準化活動


(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の審査中であり、2020年には改訂版が発行される見込みである。


(c) その他のISO/IEC 27000ファミリー規格の国際標準化活動


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は審査中であり、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、いずれも審査中である。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の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 関係用書の第 1 部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 に与える影響評価を行っており、この結果を受けて ISO/IEC 27002 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、暗号プロトタイプ（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な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 を、米国が「軽量暗号 第 2 部：ブロック暗号（ISO/IEC 29192-2）」に提案し、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長に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った。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で、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 でとその上位の 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 に対する解説論文が 2018 年 11 月に規格に 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：概念（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 月にイェービック（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）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 年度の会議にて評価の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 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 は 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ーと、個人使用となるモバイルデバイスでは、その使用環境や保護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、サーバーとモバイルデバイスでまったく同じ機能を実装す
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せず、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 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 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、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構を管理する機能のために、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 の概念の導入が検討されていく。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、メリット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、日本で行っている PUF の研究プロジェクト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ように、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」の国際標準化の提案をした。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 月のイービーキ会議で 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」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、訴訟当事者間での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定付けがないが、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されている。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く、電子情報開示に関する用語や手続きは、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 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て、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（アイデンティテイ管理とプライバシー技術）

WG 5 では、アイデンティテイ管理、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 年度の主要活動を紹介する。

(a) アイデンティテイ管理

アイデンティテイ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する規格であるISO/IEC 27552は2019年3月にDISの投票を行われた。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・アイデンティチ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。

日本案件の規格としては、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ブ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策定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度普及したことに伴って社会的に注目されていることから、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SC31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等との間でリゾンを締結し、セキュリティ及びプライバシーの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は、情報セキュリティと関係が深い分野であることから、2016年12月にリ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」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」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）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て世界各国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TrustedPlatformModule（TPM）、自動暗号化ディスクSelfEncryptingDrive（SED）、高信頼ネットワークTrustedNetworkCommunications（TNC）の三つを基本的な標準仕様と位置付けている。


日本には2008年に設立されたTCGの地域支部がある。この日本支部（JapanRegionalForum：JRF）では、内閣府の情報セキュリティ戦略会議（内閣府）で策定された標準仕様書と企業が独自に策定した標準仕様書を、世界に世界に提示するための活動を行っている。

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、組み込む環境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。

その配下の自動車サービスプラットフォームでは、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。同サブグループでは、この仕様書を基に、様々なタイプの取り組みを行っている。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（ProtectionProfile: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。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スタイル転送及びドライ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は、2018年4月に、joint IoT（Robust IoT）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。joint IoTとDICEの関係は、TPMとTSS（TCG Software Stack）の関係に相当する。DICEでは、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を最小のシステム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。

（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）」（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）」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「政府調達におけるセキュリティ要件リスト」（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。

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、調達ごとに各製品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

<table>
<thead>
<tr>
<th>対象製品分野</th>
<th>製品分野定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>デジタル複合機 (MFP)</td>
<td>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</td>
</tr>
<tr>
<td>ファイアウォール</td>
<td>インターネットと内部ネットワークの間を配置され、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の通過を制御する製品</td>
</tr>
<tr>
<td>不正侵入検知 / 防止システム (IDS/IPS)</td>
<td>ネットワークやシステムの健全状態を監視し、組織内のコンピュータネットワークへの外からの侵入を報告、防御する製品</td>
</tr>
<tr>
<td>サーバOS</td>
<td>コンピュータのハードウェア制御・操作のための基本ソフトウェア</td>
</tr>
<tr>
<td>データベース管理システム (DBMS)</td>
<td>共有データとしてのデータベースを管理する、データに対するアクセス制御をもつ製品</td>
</tr>
<tr>
<td>スマートカード (ICカード)</td>
<td>プラスチック製カード等にICチップを埋め込み、情報の記録をするようにした製品</td>
</tr>
<tr>
<td>USBメモリ</td>
<td>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持ち運び可能な記憶装置</td>
</tr>
<tr>
<td>ルータ / レイヤ3スイッチ</td>
<td>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バイス間の通信を可能にする装置</td>
</tr>
<tr>
<td>ドライバーセキュリティシステム</td>
<td>ネットワーク接続によるデバイス間の通信を可能にする装置</td>
</tr>
<tr>
<td>モバイル端末管理システム</td>
<td>スマートフォン、タブレット等のデバイスを管理し、安全に運用・管理するシステム</td>
</tr>
<tr>
<td>仮想プライベートネットワーク (VPN)</td>
<td>ネットワーク接続によるデバイス間の通信を可能にする装置</td>
</tr>
<tr>
<td>ゲートウェイ</td>
<td>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</td>
</tr>
</tbody>
</table>

※391 国の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用のための普及活動を行っている。

※392 「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チップが埋められたスマートカード等が製品である。
第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

情報セキュリティを支える基盤の動向

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、国内ベンダー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、アメリカ、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ヵ国以上に及び、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ル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ゲイミッシュ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は日本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になる。

(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れ戻し、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、基本的には毎年度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うつ定常的に行われていることを反映と考えられる。

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た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ウェブ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、その国の認証製品の利用を容易にしている。
(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) 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 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と新たに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 までとする方針が 2012 年に発表された。これを機に、我が国でも一般的な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。

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、一般的な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ヤウォールやネットワーク機器等の PP 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求める等、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る特性から来る。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す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している認証製品で8製品をリストで公開している*408。EAL4で分類するも製品が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れる。この傾向は、CCRAのWebサイトに公開され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で分類される認証製品に着目すると、欧州ではスマートカードのセキュリティ認証保証を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製品の数が増加している。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がリリースされて以降は順次切れてきている。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、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いる。EAL6/EAL7では形式的／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思われる。例えば、仕様記述のあいまい性に起因するデバイド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。

（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。

（2）貿易機関等における認証製品の活用
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。

（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、発行に付随す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
# 第2章 情報セキュリティを支える基盤の動向

情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019

<table>
<thead>
<tr>
<th>暗号アルゴリズム</th>
<th>2007年度～2016年度</th>
<th>2017年度</th>
<th>2018年度</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-key Triple DES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camellia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DRBG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KDF</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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、危険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、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。
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」に根拠として、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 ポイントの伸びを示している。

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。

<table>
<thead>
<tr>
<th>分類</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>情報セキュリティツール</td>
<td></td>
</tr>
<tr>
<td>統合型アプライアンス</td>
<td>FW、IDS、ウイルス対策等複数機能を持ったアプライアンス</td>
</tr>
<tr>
<td>ネットワーク脅威対策製品</td>
<td>FW、IDS/IPS、VPN、アプリケーションファイアウォール</td>
</tr>
<tr>
<td>コンテントセキュリティ対策製品</td>
<td>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</td>
</tr>
<tr>
<td>アイデンティティ・アクセス管理製品</td>
<td>認証、ログオン管理・アクセス許可、PKI製品</td>
</tr>
<tr>
<td>システムセキュリティ管理製品</td>
<td>セキュリティ情報統合管理、ポリシー・アクティビティブ管理ツール、脆弱性検査ツール 等</td>
</tr>
<tr>
<td>暗号製品</td>
<td>暗号化製品、暗号モジュール</td>
</tr>
<tr>
<td>情報セキュリティサービス</td>
<td></td>
</tr>
<tr>
<td>情報セキュリティコンサルテーション</td>
<td>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</td>
</tr>
<tr>
<td>セキュアシステム構築サービス</td>
<td>IT セキュリティの設計、導入、製品選定支援等</td>
</tr>
<tr>
<td>セキュリティ運用・管理サービス</td>
<td>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、電子証認証サービス等</td>
</tr>
<tr>
<td>情報セキュリティ教育</td>
<td>教育実施、コンテンツ提供、教育 ASP、資格認定等</td>
</tr>
<tr>
<td>情報セキュリティ保険</td>
<td>情報セキュリティおよび IT セキュリティ保険</td>
</tr>
</tbody>
</table>

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

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。ツール別にみると、「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ポイント増と、おおむね増加傾向が続いているが、「統合型アプリアンス」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。サービス別にみると、「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、各分野でおおむね増加傾向が続いている。

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価加価値の創出や課題解決を図られた「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されていた「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、当該行為に対する救済が可能とされた。しかし価値あるデータを有する企業・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「産業デーク共有促進事業※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完する事業を実施し、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）やコンサム、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」が49.3%と最も高く、次いで「積極的に推進していこうと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）。

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2-7-3 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

![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、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。

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ない」を挙げている企業の割合が47.3%と最も高く、次いで「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かったと推測される。

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。

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)。

(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

140
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）については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」を挙げている業界の割合が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型化化、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必要である。

・契約・規約
不正競争防止法が改正され、2019年7月1日から
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」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向上、技術的対策
として、データのトーセルサービス（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）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
への対応も模索されているが、一部の技術的な課題はまだ残されている。

(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」についても、これまでは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、公開鍵暗号に関す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関する研究として、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、攻撃可能な数段の増加、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 に対する攻撃に相当す
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、大きな進展はまだ終わるかに思われた。

しかし 2018 年 11 月、一本の論文が国際暗号
学会 IACR の ePrint 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
検知を誤認させることの可能性（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。
情報セキュリティを支える基盤の動向

第2章

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に提案され採択された。OCB3は2011年に仕様が論文によって公開され、その後、国際的な認証暗号コンペティションであるCAESARに提案され、現在、フライデ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の議論を通じてRFC7253として採用されている。

OCBシリーズの仕様の特長として、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シリーズは全て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。

(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件となり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PQCrypto2018及び第1回NISTPQC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。それらの内訳件数を表2-7-2（次ページ）に示す。

第2ラウンドに進んだ26件のアルゴリズム名を以下に示す。
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表する予定となっている。
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支払いに対する補償に限られていたが、サイバー保険はこ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ときは、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」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、取引先からの信頼度向上等にもつながります。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。

第2章 情報セキュリティを支える基盤の動向

情報セキュリティ白書 2019
情報セキュリティ白書 2019

第2章
情報セキュリティを支える基盤の動向

60-25）
※350 JISPA:「安心価値を発信した 一平成 31 年春号－」
※ 31 総務省:「青少年インターネットを安全に安心して活用するための
リテラシーコミュニティ」
http://www.ccc.or.jp/cecre/soumu/PDF/ILAS.pdf
(参照2019-06-25)
※ 32 総務省:スマートフォン時代に対応した青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））
※ 33 キャンパスソリューション株式会社:マルチケア情報局
※ 34 日本アイ・ピー・エム株式会社:セキュリティ・インテリジェンス
https://www.ibm.com/blogs/security/ip/ia/category/security-
intelligence/（参照2019-06-25）
※ 35 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)
symantec.com/connect/ja/symantec-blogs.jp (参照2019-06-25)
※ 37 トレンドマイクロ:トレンドマイクログリム公式ブログ
※ 38 マクファーレ株式会社:マクフェア公式株式会社公式ブログ
※ 39 経済産業省:「今後の基準認証の在り方−ルール形成を通じたグ
ローバル市場の獲得に向けて」答申
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 JTC1/SC27 STATEMENT ON OCB2.0
--- Major weakness found in a standardized cipher scheme (ISO
IEC 19772:2009-02, 1st ed) https://www.din.de/blob/321470-
dad39bce7116deb51016aded2ed0b4d/20190107-press-
※ 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
要件の厳格化・高速化を可能とする 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 社会を実現する新規の技術開発・複製不
可能なデバイスを活用したIoT ハーハウサー 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
※ 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
2019-06-25)
※ 377 https://www.iotac.jp/wp-content/uploads/2016/01/03IoT
%3E%2BBB%E3%82%A1%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%83%89%E3%82%B0%E3%83%AB%E3%83%B3ver1.0%E5%88%99%E5%B4%99%E5%85%B7
https://www.nisc.go.jp/active/kiken/pdf/iot_framework
2016.pdf （参照2019-06-25）
※ 379 TCG: TPM Library Specification https://trustedcomputing
group.org/tpm-library-specification/（参照2019-06-25）
※ 380 TCG: TCG Library specification https://trustedcomputing
group.org/tcg-library specifications/（参照2019-06-25）
※ 381 TCG: TCG Japanese Translation https://trustedcomputing
group.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://trustedcomputing
group.org/work-groups/regional-forums/japan/jfworkshop/（参照
2019-06-25）
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-automotive-profile-automotive-thin/
TCG: Protection Profile Automotive-Thin Specific TPC
https://trustedcomputinggroup.org/resource/protection-profile-automotive-
thin-specific-profile-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/
（参照2019-06-25）
※ 385 Microsoft Corporation: RIoT – A Foundation for Trust in the
2019-06-25）
※ 386 TCG: Protection Profile Automotive-Thin Specific TPC
https://trustedcomputinggroup.org/resource/protection-profile-automotive-
thin-specific-profile-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/
（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: Protection Profile Automotive-Thin Specific TPC
https://trustedcomputinggroup.org/resource/protection-profile-automotive-
thin-specific-profile-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/
（参照2019-06-25）
※ 389 TCG: Trusted Platform Architecture Hardware Requirements
for a Device Identifier Composition Engine https://trustedcomputing
organization/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）
2019-06-25）
※ 392 https://www.ipa.go.jp/security/jisec/index.html（参照2019-
06-25）
※ 393 政府調査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
を示したものです。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
ジ、スペイン、ドイツ、トルコ、ニュージーランド、ロールー、マレーシア、
フランス（上記の国は認証制度を自国で運営）、イス 兰教、インドネシア、
エチオピア、オーストラリア、カタール、ギリシャ、チェコ、デマリカ、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）
154
第2章
情報セキュリティを支える基盤の動向

306-327, 2011.
※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．
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、従来からのネットワーク、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がり、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され広がる。

しかし、近代においてコンピュータとインターネットの普及により、制御システムのセキュリティはますます重要なものとなっている。

3.1.1 インシデントの発生状況と動向

2018年は、ここ数年続いている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。

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、2018年に発生した制御システムの運用障害について、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。また、世界各地の製造、エネルギー、輸送、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。

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）ウィルスへの感染

制御システムのウィルスへの感染は毎年報告されている。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、ネットワーク機器に感染したものでないウィルス「VPNFilter」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シアンウェアに感染し、24日間運用が停止した。感染流れ後すぐに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、米国の大型の新聞社の印刷プラットフォームがウィルス（関係者によればラシアンウェアとも）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。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、米国の国内の工場で、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、4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と判明した。ウィルスはインターネットバンギ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、ラシアンウェアに変化型ウィルスであれば、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、サプライヤーの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ィ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メモリがウィ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ているが、当該ウィルスは主要なウィルス対策プログラムで検知可能なウィルス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。

(2) サプライチェーン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ィ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ということ、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、ハッカーはまずサプライヤーのネットワークを標的型攻撃によって侵入し、サプライヤーがサプライド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、同様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）のウィルス感染が発覚した。同工場に設置したデータセンタのシステムがラシアンウェアに感染した事例が報告されている※14。これからの事例では運用やサービスに影響はなかったとの報告もあるが、3月にも欧州の水道事業者の制御システムが仮想通貨（暗号資産）のマイニングウィルスに感染した事例が報じられた※13。さらに、10月には米国のノースカロライナ州の水道当局のシステムがラシアン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しているが、サイバー脅威やデータを消去する破壊型ウィルス、感染機器の処理能力を低下させるマイニングウィルス等は、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、製造業へのラシアンウェア攻撃と同様に、制御システムの可用性を人質にし、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ィルス対策、外部から持ち込む情報端末や媒体のウィルス対策を徹底することが重要である。

3章個別テーマ
情報セキュリティ白書 2019

(3) サプライチェーン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ィ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、ハッカーはまずサプライヤーのネットワークを標的型攻撃によって侵入し、サプライヤーがサプライド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、同様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）のウィルス感染が発覚した。同工場に設置したデータセンタのシステムがラシアン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しているが、サイバー脅威やデータを消去する破壊型ウィルス、感染機器の処理能力を低下させるマイニングウィルス等は、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、製造業へのラシアンウェア攻撃と同様に、制御システムの可用性を人質にし、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ィルス対策、外部から持ち込む情報端末や媒体のウィルス対策を徹底することが重要である。

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、ハッカーはまずサプライヤーのネットワークを標的型攻撃によって侵入し、サプライヤーがサプライド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、同様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）のウィルス感染が発覚した。同工場に設置したデータセンタのシステムがラシアン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しているが、サイバー脅威やデータを消去する破壊型ウィルス、感染機器の処理能力を低下させるマイニングウィルス等は、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、製造業へのラシアンウェア攻撃と同様に、制御システムの可用性を人質にし、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ィルス対策、外部から持ち込む情報端末や媒体のウィルス対策を徹底することが重要である。

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、ハッカーはまずサプライヤーのネットワークを標的型攻撃によって侵入し、サプライヤーがサプライド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、同様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。
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で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、同様カウント方法で比較できるよう図を分けている）。

■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※22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※22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も※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ーは、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、脆弱性を作り込む、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
第3章 個別テーマ
情報セキュリティ白書 2019

されたウイルス「CrashOverride」（別名 Industroyer）の解析の続報や※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ある「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ずの外部への公開（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400万台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プラットフォーム製品がシステムに接続され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調査の子分を有する国家（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。しかし最近では、国家以外の攻撃者による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年のイラク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、アンダークラウドのハッカー・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ーも、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いつけ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も、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。

海外の制御システムセキュリティの取り組み

(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、電力網の基幹システムで使用される製品（制御システム製品を含む）のセキュリティを認証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、基幹システムで使用する製品・機器の洗い出し、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求めていた。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「ブレイクスター」を想定し、実際にブレイクスター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たもので、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、議論も喚んでいる。

(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3.2.2 欧州の政策）に使用された。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たもので、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、議論も喚んでいる。

(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／アウトソーシングに関わらず、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、施設日から6ヶ月以内に当局に提出することを義務付けています（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かけており、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対策として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。

同手引書は、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された「機能保証のためのリスクアセスメントガイドライン」を活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」を基準値及びリスク値を算定し、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、影響度及び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向けには、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。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している。

### 表3-1-1

<table>
<thead>
<tr>
<th>要素</th>
<th>予想発生頻度</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>非常に多い</td>
</tr>
<tr>
<td>4</td>
<td>多い</td>
</tr>
<tr>
<td>3</td>
<td>中程度の頻度</td>
</tr>
<tr>
<td>2</td>
<td>少ない</td>
</tr>
<tr>
<td>1</td>
<td>非常に少ない</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>発生頻度</th>
<th>事象の予想発生頻度</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>非常に多い</td>
</tr>
<tr>
<td>4</td>
<td>多い</td>
</tr>
<tr>
<td>3</td>
<td>中程度の頻度</td>
</tr>
<tr>
<td>2</td>
<td>少ない</td>
</tr>
<tr>
<td>1</td>
<td>非常に少ない</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>影響度</th>
<th>影響度合い</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>重大な影響</td>
</tr>
<tr>
<td>4</td>
<td>大きな影響</td>
</tr>
<tr>
<td>3</td>
<td>中程度の影響</td>
</tr>
<tr>
<td>2</td>
<td>小さな影響</td>
</tr>
<tr>
<td>1</td>
<td>軽微な影響</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>影響度</th>
<th>影響度合い</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>重大な影響</td>
</tr>
<tr>
<td>4</td>
<td>大きな影響</td>
</tr>
<tr>
<td>3</td>
<td>中程度の影響</td>
</tr>
<tr>
<td>2</td>
<td>小さな影響</td>
</tr>
<tr>
<td>1</td>
<td>軽微な影響</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>影響度</th>
<th>影響度合い</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>重大な影響</td>
</tr>
<tr>
<td>4</td>
<td>大きな影響</td>
</tr>
<tr>
<td>3</td>
<td>中程度の影響</td>
</tr>
<tr>
<td>2</td>
<td>小さな影響</td>
</tr>
<tr>
<td>1</td>
<td>軽微な影響</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>影響度</th>
<th>影響度合い</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>重大な影響</td>
</tr>
<tr>
<td>4</td>
<td>大きな影響</td>
</tr>
<tr>
<td>3</td>
<td>中程度の影響</td>
</tr>
<tr>
<td>2</td>
<td>小さな影響</td>
</tr>
<tr>
<td>1</td>
<td>軽微な影響</td>
</tr>
</tbody>
</table>

### 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)」
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性）、「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版を用いて多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基準と評価値、とりわけ判断要素が多岐にわたる検討が難しい「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。これにより、投入可能な人件と予算で、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のビルサプライキンググループにより、「ビルシステムにおけるサイバー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※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高まる状況で、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以外のウィルスの亜種等が出現し、各々のウィ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、新たに出現したウィルスや進化した既存のウィ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月から観測されておりが、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、次の解析結果が報告された。

- 暗号鍵は0xedeefba（Miraiは0xdeadbeef）。
- Miraiの亜種「Satori」が用いたC&Cサーバの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C&Cの初期設定値を保有。
- ソースコード内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)製ルーターDIR-645のコマンドインジェクション脆弱性を悪用して感染するよう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）を狙うように拡張されたMasutaが観測されている。

(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トムネットが発見され、「JenX」と命名された。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、以下の脆弱性を用いて感染を拡大する。

- CVE-2014-8361 (Realtek SDKにおける任意のコード実行の脆弱性)
- CVE-2017-17215 (Huawei HG532ルーター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機器を破壊するウィルス「BrickerBot」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）。

関して、次の解析結果が報告された。

- 暗号鍵は0xedeefba（Miraiは0xdeadbeef）。
- Miraiの亜種「Satori」が用いたC&Cサーバの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C&Cの初期設定値を保有。
- ソースコード内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)製ルーターDIR-645のコマンドインジェクション脆弱性を悪用して感染するよう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）を狙うように拡張されたMasutaが観測されている。

(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トムネットが発見され、「JenX」と命名された。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、以下の脆弱性を用いて感染を拡大する。

- CVE-2014-8361 (Realtek SDKにおける任意のコード実行の脆弱性)
- CVE-2017-17215 (Huawei HG532ルーター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機器を破壊するウィルス「BrickerBot」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）。
(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。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）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探索サービス SHODAN 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。

<table>
<thead>
<tr>
<th>国名</th>
<th>感染ホスト台数</th>
</tr>
</thead>
<tbody>
<tr>
<td>ベトナム</td>
<td>2,125</td>
</tr>
<tr>
<td>中国</td>
<td>407</td>
</tr>
<tr>
<td>米国</td>
<td>312</td>
</tr>
<tr>
<td>タイ</td>
<td>160</td>
</tr>
<tr>
<td>韓国</td>
<td>126</td>
</tr>
</tbody>
</table>

(3) 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」を基にIPAが編集

(d) Omni

2018年5月、DASAN Networks, Inc.製GPONホームルータが発見され、「Omni」と命名された。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）を狙うように拡張されており、「Omni」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探索サービス SHODAN 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。

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。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）を狙うように拡張されており、「Wicked」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探索サービス SHODAN 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。

解析結果によると、Wicked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。また、IoT機器の脆弱性を直接悪用する代わりに、既に侵害を受けて恶意のある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。

(g) 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。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製の組込み用Webサーバuc-httpd 1.0.0のバッファーフローの脆弱性（CVE-2018-10088）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）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（CVE-2016-6277）を狙うように更に拡張された。感染が観測され、数千台のIoT機器の国別分布を図3-2-2に示す。

解析結果によると、Wicked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。

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。

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。
第3章 個別テーマ
情報セキュリティ白書 2019

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。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
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。

■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」を基にIPAが編集

■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」を基にIPAが作成

<table>
<thead>
<tr>
<th>No.</th>
<th>ベンダ名</th>
<th>機器名</th>
<th>脆弱性</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DASAN Networks, Inc.</td>
<td>GPONルータ</td>
<td>CVE-2018-10561 , CVE-2018-10562</td>
</tr>
<tr>
<td>2</td>
<td>各社</td>
<td>Realtek SDKを用いた各機器</td>
<td>CVE-2014-8361</td>
</tr>
<tr>
<td>3</td>
<td>Netgear</td>
<td>ルータ DGN1000/DGN 2200v1</td>
<td>Netgear setup.cgi非認証リモートコード実行の脆弱性</td>
</tr>
<tr>
<td>4</td>
<td>Huawei Technologies Co., Ltd.</td>
<td>HG532</td>
<td>CVE-2017-17215</td>
</tr>
<tr>
<td>5</td>
<td>ZyXEL Communications Corp.</td>
<td>ADSLルータ eir D1000 modem</td>
<td>CVE-2016-10372</td>
</tr>
<tr>
<td>6</td>
<td>D-Link</td>
<td>ルータ DIR-645他</td>
<td>CVE-2015-2051</td>
</tr>
<tr>
<td>7</td>
<td>各社（70社以上）</td>
<td>CCTVやDVR</td>
<td>CCTV/DVRのリモートコード実行の脆弱性</td>
</tr>
<tr>
<td>8</td>
<td>MVPower</td>
<td>DVR TV-7104HE, TV-7108HE等</td>
<td>JAWS Webサーバの非認証シェルコマンド実行の脆弱性</td>
</tr>
<tr>
<td>9</td>
<td>D-Link</td>
<td>ルータ DIR-300/600/645/845/865等</td>
<td>UPnP SOAP Telnetdコマンド実行の脆弱性</td>
</tr>
<tr>
<td>10</td>
<td>Netgear</td>
<td>ルータ R7000/R6400</td>
<td>CVE-2016-6277</td>
</tr>
<tr>
<td>11</td>
<td>FUHO Technology Co., Ltd.</td>
<td>VACRON NVR</td>
<td>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</td>
</tr>
</tbody>
</table>

■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）Palo Alto Networks, Inc.「Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns」を基にIPAが作成

<table>
<thead>
<tr>
<th>ユーザ名</th>
<th>パスワード</th>
<th>該当するIoT機器の例</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>t0talc0ntr0l4!</td>
<td>Control4 Corporation製 Home Theater Controller AVM-HTC1-Bの初期ユーザ名とパスワード</td>
</tr>
<tr>
<td>admin</td>
<td>ad123</td>
<td>CommScope, Inc.製 ADC FlexWave Prismの初期ユーザ名とパスワード</td>
</tr>
</tbody>
</table>
| mg3500   | merlin   | Camtron Industrial Inc.製 CMNC-200の初期ユーザ名とパスワード（CVE-2010-4233）
### 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。感染に際して悪用する典型的な認証情報とされる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

<table>
<thead>
<tr>
<th>Yowai</th>
</tr>
</thead>
<tbody>
<tr>
<td>OxhlwSG8, defautl~Jwpbo~6S2~GqNF~admin, daemon, 12345, guest, support, 4321, root, vixxv, 10tal~corn~041, bin, adm, synnet</td>
</tr>
</tbody>
</table>

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
- CVE-2014-8361
- Linksys製ルータのリモートコード実行の脆弱性
- CVE-2018-10561
- CCTV/DVRリモートコード実行の脆弱性

(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。また、Mirai系ウイルスとは異なり、Gaftgyt（ Bashli teやQBot等の別名あり）のソースコードを基にビルズされており、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サーバーの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。

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。

- ThinkPHPのリモートコード実行の脆弱性
- D-Link製DSL-2750Bルータの脆弱性
- CVE-2015-2051
- CVE-2014-8361
- CVE-2017-17215

#### ビルドインされたパスワードの例

<table>
<thead>
<tr>
<th>Yowai</th>
</tr>
</thead>
<tbody>
<tr>
<td>OxhlwSG8, defautl~Jwpbo~6S2~GqNF~admin, daemon, 12345, guest, support, 4321, root, vixxv, 10tal~corn~041, bin, adm, synnet</td>
</tr>
</tbody>
</table>

#### ビルドインされたユーザ名やパスワードの例

<table>
<thead>
<tr>
<th>Mirai</th>
<th>IZ1H9</th>
<th>APEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001chin, adm, admin123, admintelecom, e8ehome, e8telnet, GM8182, gpon, oh, root, support, taZ2@23495859, teleadmin, telnetadmin, tsogoingon, tinet, vixxv, zte</td>
<td>00000000, 12345, 54321, 123456, 111111, 20080826, 20150602, 88888888, 1234567890, ADMIN, admin1, admin123, admin1234, antslq, changeme, D13hhj, default, ezdrv, GM8182, guest, hi3518, ipc71a, IPCam~~sw, ipcam_rt5350, juanotech, jybdz, k1212, k12243, ninda, password, qwertyp, Qwest~M~dom, root123, service, smadmin, support, svgodie, system, telnet, tl789, vixxv, vstarcam2015, xc3511, xmhdpic, zixxv, zsun1188, Zte521</td>
<td>123456, 888888, 20150602, 1q2w3e4r5, 2011vita, 3epSwu2, admintelecom, bcpb+;serial=, default, e8ehome, e8telnet, fliruser, guest, hiujiu309, juniper123, kvl1234, linux, maintainer, Maxitaxi~01, super, support, taZ2@01, taZ2@23495859, teleadmin, telewin, telnetadmin, tsogoingon, vstarcam2015, Zte521, ZXDSL</td>
</tr>
</tbody>
</table>

#### (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。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る等、発生し、NICTは注意喚起を行った。
感染ルータ経由でインターネットにアクセスすると、恶意のある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）。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ーのルータ製品で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す機能と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

<table>
<thead>
<tr>
<th>事業者・製造者</th>
<th>対象機種</th>
<th>注意喚起日</th>
</tr>
</thead>
<tbody>
<tr>
<td>東日本電信電話株式会社※94</td>
<td>Netcommunity OG410Xa、OG410Xt、OG810Xa、OG810Xt</td>
<td>2018年3月28日</td>
</tr>
<tr>
<td>西日本電信電話株式会社※95</td>
<td>Netcommunity OG400Xa、OG400Xt、OG800Xa、OG800Xtの一部機器</td>
<td></td>
</tr>
<tr>
<td>ロジテック株式会社※96</td>
<td>LAN-W300N/R、LAN-W301NR等</td>
<td>2018年4月2日</td>
</tr>
<tr>
<td>株式会社バッファロー※97</td>
<td>WHR-300HP2、WHR-G301N、WHR-1166DHP4等</td>
<td>2018年4月5日</td>
</tr>
<tr>
<td>NECプラットフォームズ株式会社※98</td>
<td>機種情報なし</td>
<td>2018年4月6日</td>
</tr>
<tr>
<td>株式会社アイ・オー・データ機器※99</td>
<td>機種情報なし</td>
<td>2018年4月12日</td>
</tr>
<tr>
<td>ニフティ株式会社※100</td>
<td>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 DR300Cシリーズ、Aterm WD600Cシリーズ、Aterm WD700Cシリーズ</td>
<td>2018年4月26日</td>
</tr>
</tbody>
</table>

■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※92」を基にIPAが作成
攻撃者のウェ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サトリ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、サトリの亜種が発見され、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WindowsPC）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、設定情報を取得する機能、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年から確認されており、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、さら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の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、ミライの亜種「Reaper」*113に悪用され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（ネットワークベンダ名 機器名

<table>
<thead>
<tr>
<th>ベンダ名</th>
<th>機器名</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASUSTeK Computer Inc. (以下、ASUS)</td>
<td>RT-AC66U、RT-N10、RT-N10E、RT-N10U、RT-N56U、RT-N66U</td>
</tr>
<tr>
<td>D-Link</td>
<td>DES-1210-08P、DIR-300、DIR-300A、DSR-250N、DSR-500N、DSR-1000、DSR-1000N</td>
</tr>
<tr>
<td>Huawei Technologies Co., Ltd.</td>
<td>HG8245</td>
</tr>
<tr>
<td>Linksys</td>
<td>E1200、E2500、E3000、E3200、E4200、RV082、WRVS4400N</td>
</tr>
<tr>
<td>MicroTik</td>
<td>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</td>
</tr>
<tr>
<td>Netgear</td>
<td>DGB834、DGN1000、DGN2200、DGN3500、FVS318N、MBRN3000、R6400、R7000、R8000、WNR1000、WNR2000、WNR2200、WNR4000、WNDR3700、WNDR4000、WNDR4300、WNDR4300-TN、UTM50</td>
</tr>
<tr>
<td>QNAP</td>
<td>TS5251、TS439 Pro、QSソフトウェアが動作する他のQNAP NAS</td>
</tr>
<tr>
<td>TP-LINK</td>
<td>R600VPN、TL-WR741ND、TL-WR841N</td>
</tr>
<tr>
<td>Ubiquiti Networks, Inc.</td>
<td>NSM2、PBE M5</td>
</tr>
<tr>
<td>Upvel LLC</td>
<td>機種不明</td>
</tr>
<tr>
<td>ZTE Corporation</td>
<td>ZXHN H108N</td>
</tr>
</tbody>
</table>

（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」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に感染していると説明される。\(^{127}\)

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法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され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、無人時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発見されたと報告した。\(^{129}\)。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。\(^{131}\)

<table>
<thead>
<tr>
<th>No.</th>
<th>ベンダ名</th>
<th>機器名/サービス名</th>
<th>脆弱性</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>QNAP</td>
<td>NAS 各機種の FTP サービス</td>
<td>CVE-2015-7261</td>
</tr>
<tr>
<td>2</td>
<td>D-Link</td>
<td>ルータ DIR-300</td>
<td>CVE-2011-4723</td>
</tr>
<tr>
<td>3</td>
<td>ASUS</td>
<td>ルータ RT-AC66U、RT-N66U</td>
<td>CVE-2014-9583</td>
</tr>
<tr>
<td>4</td>
<td>Linksys</td>
<td>ルータ E1500、E2500</td>
<td>CVE-2013-2678</td>
</tr>
<tr>
<td>5</td>
<td>Netgear、TP-LINK、D-Link等</td>
<td>各機種の脆弱性を有するUPnP サービス</td>
<td>CVE-2013-0229</td>
</tr>
<tr>
<td>6</td>
<td>QNAP</td>
<td>NAS 各機種の QTS ソフトウェア (4.2.4 Build 20170313 以前)</td>
<td>CVE-2017-6361</td>
</tr>
<tr>
<td>7</td>
<td>ASUS</td>
<td>ルータ RT-AC、RT-N</td>
<td>CVE-2017-8877</td>
</tr>
<tr>
<td>8</td>
<td>Netgear</td>
<td>ルータ R6400、R7000、R8000</td>
<td>CVE-2017-5521</td>
</tr>
<tr>
<td>9</td>
<td>Netgear、TP-LINK、D-Link等</td>
<td>各機種の脆弱性を有するUPnP サービス</td>
<td>CVE-2012-5958</td>
</tr>
<tr>
<td>10</td>
<td>D-Link</td>
<td>ルータ DIR-300</td>
<td>リモートコード実行の脆弱性</td>
</tr>
<tr>
<td>11</td>
<td>Netgear</td>
<td>ルータ RT-AC66U、RT-N66U</td>
<td>CVE-2013-0229</td>
</tr>
<tr>
<td>12</td>
<td>ASUS</td>
<td>ルータ R6400、R7000</td>
<td>CVE-2016-6277</td>
</tr>
<tr>
<td>13</td>
<td>ASUS</td>
<td>ルータ RT-AC66U、RT-N66U</td>
<td>CVE-2017-5521</td>
</tr>
<tr>
<td>14</td>
<td>Linksys</td>
<td>ルータ E4200</td>
<td>CVE-2013-2679</td>
</tr>
<tr>
<td>15</td>
<td>Netgear</td>
<td>ルータ WNR2000</td>
<td>パスワードの漏えいの脆弱性</td>
</tr>
<tr>
<td>16</td>
<td>TP-LINK</td>
<td>ルータ TL-WR841N</td>
<td>CVE-2017-5521</td>
</tr>
<tr>
<td>17</td>
<td>Linksys</td>
<td>ルータ E4200</td>
<td>CVE-2013-2679</td>
</tr>
<tr>
<td>18</td>
<td>Netgear</td>
<td>ルータ WNR1000</td>
<td>バッファオーバーフローの脆弱性</td>
</tr>
<tr>
<td>19</td>
<td>Netgear</td>
<td>ルータ WNR1000</td>
<td>警戒指針の脆弱性</td>
</tr>
<tr>
<td>20</td>
<td>Linksys</td>
<td>ルータ E4200</td>
<td>ストックオーバーフローの脆弱性</td>
</tr>
</tbody>
</table>

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」を基にIPAが作成
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。2018年12月、神戸地方検察庁は男を不起訴処分とした。

(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）。

(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機器を中心に取ったIoT機器の実態調査結果を公開した。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い。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る。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。

• 関係者（所有者、利用者、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、多くの機器がウィルス感染の危機に晒されており、抜本的な対策を進めている時期が来ている。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）」を開始した。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(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。
第3章 個別テーマ

情報セキュリティ白書 2019

<table>
<thead>
<tr>
<th>No.</th>
<th>ベンダ</th>
<th>モデル</th>
<th>デバイス種別</th>
<th>脆弱性の種類</th>
<th>RCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Belkin International, Inc.</td>
<td>NetCam HD+ WiFi Camera</td>
<td>ネットワークカメラ</td>
<td>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)</td>
<td>有</td>
</tr>
<tr>
<td>2</td>
<td>WeMo® LED Lighting Starter Set</td>
<td>すべての WeMo® 製品</td>
<td>各種IoT機器</td>
<td>DoS (Denial of Service: サービス拒否)</td>
<td>無</td>
</tr>
<tr>
<td>3</td>
<td>東京通信株式会社パッファロー</td>
<td>WSR-300HP</td>
<td>ルータ</td>
<td>コマンドインジェクション</td>
<td>有</td>
</tr>
<tr>
<td>4</td>
<td>D-Link DCS825L EyeOn Baby Monitor</td>
<td>ベビーモニタ</td>
<td>コマンドインジェクション</td>
<td>有</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Dahua Technology Co., Ltd.</td>
<td>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)</td>
<td>ネットワークカメラ</td>
<td>預測可能な復旧用パスワード</td>
<td>無</td>
</tr>
</tbody>
</table>

■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

<table>
<thead>
<tr>
<th>公開機関・団体</th>
<th>公開資料名</th>
<th>対象読者と主な内容</th>
<th>公開年月</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPA</td>
<td>IoT製品・サービス脆弱性対応ガイド※137</td>
<td>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</td>
<td>2018年3月</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>調達者（利用者、運用者）・機能要件、対策要件、対策方法</td>
<td>2018年3月</td>
</tr>
<tr>
<td></td>
<td>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）</td>
<td>開発者・具体的な設計手法</td>
<td>2019年4月</td>
</tr>
<tr>
<td>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)</td>
<td>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</td>
<td>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</td>
<td>2018年5月</td>
</tr>
<tr>
<td>JPCERT/CC</td>
<td>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</td>
<td>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</td>
<td>2018年8月</td>
</tr>
<tr>
<td>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)</td>
<td>IoT分野共通セキュリティ要件ガイドライン2018年度版（案）</td>
<td>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</td>
<td>2018年11月</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>IoT機器の製造者、調達者・フレームワークの概要</td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>JSSEC IoTセキュリティチェックシート第二版※143</td>
<td>IoTを利用・導入する一般企業・検討・考慮すべき項目</td>
<td>2019年2月</td>
</tr>
</tbody>
</table>

■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
<table>
<thead>
<tr>
<th>公開機関・団体</th>
<th>公開資料名</th>
<th>対象読者と主な内容</th>
<th>公開年月</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST (National Institute of Standards and Technology)</td>
<td>NISTIR 8228 (DRAFT): Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks</td>
<td>・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&lt;br&gt;・リスクを低減するための対策例</td>
<td>2018年9月</td>
</tr>
<tr>
<td></td>
<td>NISTIR 8200: Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)</td>
<td>・IoT セキュリティ標準の開発者&lt;br&gt;・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</td>
<td>2018年11月</td>
</tr>
<tr>
<td></td>
<td>DRAFT Considerations for a Core IoT Cybersecurity Capabilities Baseline</td>
<td>・IoT 機器の製造者、ベースラインを&lt;br&gt;開発するコミュニティ&lt;br&gt;・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</td>
<td>2019年2月</td>
</tr>
<tr>
<td>OWASP (Open Web Application Security Project)</td>
<td>Internet of Things (IoT) Top 10 2018</td>
<td>・製造者、開発者、利用者&lt;br&gt;・10 大脆弱性的概要</td>
<td>2018年12月</td>
</tr>
<tr>
<td>ENISA (European Network and Information Security Agency)</td>
<td>Towards secure convergence of Cloud and IoT</td>
<td>・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&lt;br&gt;・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</td>
<td>2018年9月</td>
</tr>
<tr>
<td></td>
<td>Good Practices for Security of Internet of Things in the context of Smart Manufacturing</td>
<td>・産業 IoT の運用者、ユーザ、製造者、ベンダ&lt;br&gt;・産業 IoT のセキュリティ対策指針</td>
<td>2018年11月</td>
</tr>
<tr>
<td></td>
<td>IoT Security Standards Gap Analysis</td>
<td>・IoT セキュリティ標準の開発者&lt;br&gt;・セキュリティ要件と標準の対応</td>
<td>2019年1月</td>
</tr>
<tr>
<td>Department for DCMS (Digital, Culture, Media &amp; Sport), UK</td>
<td>Code of Practice for Consumer IoT Security</td>
<td>・開発者、製造者、販売者&lt;br&gt;・実践すべきセキュリティ対策</td>
<td>2018年10月</td>
</tr>
<tr>
<td>German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik : BSI)</td>
<td>BSI TR-03148: Secure Broadband Routers Version 1.0</td>
<td>・製造者、販売者、利用者&lt;br&gt;・ルータのセキュリティ要件</td>
<td>2018年11月</td>
</tr>
</tbody>
</table>

※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
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。彼らは2017年12月に罪状を認めて有罪判決を言い渡され、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。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ます。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。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。

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。

---

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]
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 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）を受けた」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（図3-3-1）、その手口にも変化が見られた※156。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。

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サイトにつながらが、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、宅配便業者を装う偽サイトにアクセスすると、「sagawaapk」、「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、7月以降はこの不正アプリをインストールしたAndroid端末からの、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が発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が拡散されることになる（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。

(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、認証コードの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。

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 への不正ログインにその可能性がある。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、現在では設定が必要となっている。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」という 2 段階認証サービスが提供されている。この設定をオフにすると、インストールしようとする偽サイトの警告が表示される。なお、本手口では、不正アプリのインストールへの誘導するため、偽サイト上に当該設定をオフにする画像付きの説明が掲載されている。本手口では、偽サイトに設定をオフにする画像付きの説明が掲載されている。以上、本手口では、不正アプリのインストールへの誘導するため、偽サイト上に当該設定をオフにする画像付きの説明が掲載されている。
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い。メールアドレス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を推奨する。もしそれぞれの情報を入手した場合は、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。

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、無関にインストールしない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手した場合（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手した場合は、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願いします」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法は多く確認されているが、この手法では2段階認証のセキュリティコードを盗まれた場合、キャリア決済を悪用される可能性がある。この手法では、ログイン情報の取得だけでなく、2段階認証のセキュリティコードも取得される可能性がある。

![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](image)

### (1) dアカウントを狙ったフィッシングの手口

本手法では、認証情報の取得手段を自動的に収集し、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動いている可能性がある。この手法では、dアカウントのログイン画面に誘導された場合、ホーム画面は白黒、画面は表示されないが、実際には、2段階認証のセキュリティコードを盗まれている。この手法では、2段階認証のセキュリティコードを盗まれられた場合、dアカウントを画像に表示するものではない。2段階認証のセキュリティコードを盗まれれば、正規のdアカウント画面では2段階認証のセキュリティコードが表示されない。
第3章 個別テーマ
情報セキュリティ白書 2019

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、「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と考えられる。

(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った場合、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様々なサービスを悪用され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
手口を知っており、騙されないことが重要である。正規のログイン画面を把握しており、その画面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を目的であり、被害者から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双方向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ヶ月、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是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に費用があることを認識できておりず、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こと、決済も完了することになる。

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するために、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 公式マーケットに配布された不正アプリ

2018年もiOS及び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く発見されている。

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。

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わず、広告をポップアップで表示させただけのアプリがGoogle Play上に少なくとも68個確認された。

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。これ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った。

2019年1月には、不正アプリが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。

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わず、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上に全面広告を定期的に表示させる。

また、同じ月にモバイルバンキングを狙うウィルス「Anubis」をインストールさせる不正アプリが確認された。この不正アプリは、モーションセンサーを感知する仕組みになっている。通常、サンドボックス環境にはモーションセンサーはいないため、モーションセンサーが感知できなくなった場合、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で偽のインストール画面を表示する。Anubisはキーロガーをスクリーンショットを取得する機能を持っている。

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。このアプリは心拍数を計るアプリとしてiPhoneのホームボタン上に指を置くように指示する。ユーザがこの指示に従って、Touch IDに登録した指を置くと、99.99ドルのアプリ内課金を支払うことになる。現在、この心拍数計測アプリはApp Storeでは削除されている。

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、騙して課金するもの等、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」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重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、再再委託先と、ある目的を達成するために必要な関係者が連鎖して形成される企業の棟梁セキュリティ対策の重要性が強調されている。

同じ企業・グループであれば、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、セキュリティポリシーが不完全な場合、セキュリティ対策が弱い場合がある。その結果、情報漏えいやシステム停止等の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。

#### (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、竊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、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引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った可能性が高まる。

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とされた攻撃者から航空機リース料（約3億6000万円）の被害に遭った。僞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ィルス感染させたり、バック

| 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 |
|-----------------|-----------------|
| 取引先を踏み台とする攻撃や取引先になりすまず攻撃 | 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 |
| 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 | 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 |

不正アクセス

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

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
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。これにより、遠隔支援ツール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。

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。同ユーザの場合も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。

(2) 過失に基づくインシデント

人が介在することにより発生してしまう事故や事件は、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、機会がついていない（必要性は分かっているが、仕事の手間が増える）など、関連ないってしまい、監視や実施により被害を最小限にする努力が必要である。

(c) 対策

不正アクセスは、高度な攻撃が次々と発見されているが、完全に防止することは難しい。自社が踏み台やなら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。

(b) 過失による対策

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去事故が発生した。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去され、多くの企業に影響があった。原因は、社内の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。

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洩したことも報告した。このインシデントでは、管理・運用が不十分であったために発生したことが明らかになった。

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確認された。「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のみで、運用には含まれていないという委託先の認識があった。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、バック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、多くの脆弱性が抱えられ、運用が行われた結果、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。

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。

(c) 対策

人が介在する事故や事件の原因には、実作業での注意喚起、及び対応方法を公表していたが、ユーザからの要件には対策が含まれておりず、ベンダからも対策の提案はされなかった。この事例では詐欺においてペンダの過失が認められた。

不正アクセスに起因する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。
うっかりミスに加え、ユーザとベンダの間の認識の違いが惹起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れほどは大きくないことがあるが、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共有し、協力することにより、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ろ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、ユーザ要件に対応したセキュリティ提案を行い、設計・製造・検査の各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。未発見の脆弱性は、公開後速やかに対処することがある。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クレジット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。

再委託に関する条項が契約書に含まれる珍しくはなかった。しかし、契約の事務手続きを取らなければ直接の交渉を営業部門が行うこともないため、契約の内容確認をするよう推奨している\(^{184}\)。

(3) 内部不正に惹起するインシデント
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扱う部門があったり、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結ばれる恐れがあり、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洩等の事案が顕在化した 10 年前かより重要性が指摘されている。近年では、省庁等におけ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 IT サプライチェーンリスク対策が重要視されている。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のセキュリティ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、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」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」
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、管理運用の低廉化的手段として、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ことが求められる。

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を定義している。このガイドラインは、規制化したリスクに対するセキュリティ要求事項及び基準的な動向を踏まえた追補を行い、2013年に改版されている。

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」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。このガイドラインは、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2016年に策定した「情報セキュリティ対策ガイドライン」を統合してクラウド事業者が参考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。

リソースの制限が大きな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」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について述べる。

(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 : CNCl）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。これを通して、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クイドライン、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、国際基準化にも影響を与えているが、NIST SP800-161の作成が中心となり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）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に対する対応を求められた。今後、あ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・導入者の同意を求めることが求められる。NDAA2019の適用対象は、サプライチェーン全体に及び、米国政府関係機関と直接取引していない、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される。そのため日本企業においても、委託先のセキュリティ対策が確認され、利用していれば取り引きでない可能性があり、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）。

(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が不足している実態を調査し、「再委託先に委託先のセキュリティ対策の徹底状況の把握や委託先が受け入れ確認のためのレビューの実施状況の把握等が不足している」「委託先に対する情報セキュリテイ管理の明示がない」等の結果が得られた。

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対策や情報セキュリティの実態、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。委託元が実施すべき具体的な情報セキュリティ対策を、委託先が仕様書等で明示しているかどう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先の業種では十分な明示がなされていないことがあるが、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確にしていないと答えており、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分かった。

(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一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）で合意が得られれば、ルータ等の具体的な製品・カテゴリー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。

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）

※199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対策及びマネジメントに関する調査－調査報告書－」注9に基づき編集

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
テリ上の責任範囲（責任分界点）が分からなかったことを課題に挙げていた（図3-4-2、図3-4-3）。

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ベ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、セキュリティイベ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、連携がうまくいかない等の恐れがある。

新たに脅威（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るか、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。

(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年度調査では委託元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関す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。
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的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て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、
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の違いがあるものの、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、契約関連文書の確認を有効と考えており、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、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の変更を含め、契約内容に適合しない場合には修補・追完を求めることが求められている。

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契約元の立場は弱くならないため、仕様書を作成する契約元が、より要件を明示しなければならない。

民法改正への対応として、契約書や自社の契約書の確認及び見直しが求められている。このような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。

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。更に複雑になることが予想され、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りおり、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、 (_,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の関与が進んでいる。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・安全に関わるトランスト（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、すべての人同士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」、「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、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。

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。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、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。実用化が進め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推定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動き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、細工され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(「3.4.5 (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にとっては、学習データや学習モデルの安定性・正確性確保や秘密、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) 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 (アカウンタビリテイ)
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 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) 等の規格が策定中である。
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。

(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。
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一事に関連事項の適切に考慮し、AI発表利用規則に体系化されている(後者の内容は今後策定)。
このような、「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AI社会（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「包括的な成長、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」「アメリカンパターン」が含まれる。①11

(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。①12

- 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）①13、International Business Machines Corporation（以下、IBM社）①14、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、トクスト（信頼）が必要であると言われる。トク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
前述の三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良い課題と、品質・安全の保証等で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は、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は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接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展している。

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。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順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されている。

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クストは担保される。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。
第3章 個別テーマ

情報セキュリティ白書 2019

以上から、製品・サービスの信頼性を構築するため、以下の二つが重要であると考えられる。

① AI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。

② AI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）を理解してもらう、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サービス利用者間の連携する。

以上から、製品・サービスのトランスポートについて、以下の二つが重要であると考えられる。

① AI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。

② AI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）を理解してもらう、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サービス利用者間の連携する。

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・安全性の確保に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。

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・安全性の確保に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。

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。

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

AIを利用したセキュリティは、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・ウィ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用されており、今後も自動化・効率化に貢献することが期待されている。

例えばウィルス検知では、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。近年には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ていることが、継続的な学習のためのウィルスの網羅的な収集が課題となる。またウィルス自身は、巧妙化が進んでおり、ウィ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、ウィルスでないと検知したウィルスを検知してしまう（誤検知：false positive）ことが起こり得る。

更に、攻撃者にAI技術の専門家がいる場合、ウィルス検知のAIを自ら作り、その学習モデルをすり抜けるようなウィルスを生成することも考えられる。こうした状況において、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くことを考えられ、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必要とする。

(2) AI自身のセキュリティ

AI自身のセキュリティに関しては、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活動と課題について詳細に報告している。

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、意図的で誤判定を起こさせることで、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、人間には理解できないノイズを含めることで判定結果を誤らせ、敵対的なサンプル（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なう可能性がある。ただし、このような攻撃は、AIアルゴリズムの特性や学
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。

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システム固有的脅威としては、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。これは顔画像の学習事例であるが、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Tayへ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。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。

一般的利用者向けの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存在する。しかし学習モデルのそれぞれが営業秘密であり、正規のビジネスを侵害する類似AIは出回ることはないと考えられる。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。

(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。実際、IBM社はAIを利用して検出しづら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。

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伝言をする追真の動画を作成してしまう。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、安易に作られ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、といわれている。

2016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。

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。

(4) まとめ

上述でみたように、AIシステム自身のセキュリティについての検証は始まったばかりであるが、当面のリスクとしては、AIシステムへの攻撃が最も攻撃者による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。
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月に公表した「情報セキュリティ10大脅威 2019」は、下表のとおりです。

<table>
<thead>
<tr>
<th>「個人」向け脅威</th>
<th>「組織」向け脅威</th>
</tr>
</thead>
<tbody>
<tr>
<td>クレジットカード情報の不正利用</td>
<td>標的型攻撃による被害</td>
</tr>
<tr>
<td>伪装メールによる個人情報等の詐取</td>
<td>ビジネスメール詐欺による被害</td>
</tr>
<tr>
<td>不正アプリによる</td>
<td>ランサムウェアによる被害</td>
</tr>
<tr>
<td>スマートフォン利用者の被害</td>
<td></td>
</tr>
<tr>
<td>メール等を使った脅迫・詐欺の手口による金銭要求</td>
<td>サプライチェーンの脆弱点を悪用した攻撃の高まり</td>
</tr>
<tr>
<td>ネット上の誹謗・中傷・デマ</td>
<td>内部不正による情報漏えい</td>
</tr>
<tr>
<td>偽警告によるインターネット詐欺</td>
<td>サービス妨害攻撃によるサービスの停止</td>
</tr>
<tr>
<td>インターネットバンキングの不正利用</td>
<td>インターネットサービスからの個人情報の窃取</td>
</tr>
<tr>
<td>インターネットサービスへの不正ログイン</td>
<td>IoT 機器の脆弱性の顕在化</td>
</tr>
<tr>
<td>ランサムウェアによる被害</td>
<td>脆弱性対策情報の公開による悪用増加</td>
</tr>
<tr>
<td>IoT 機器の不適切な管理</td>
<td>不注意による情報漏えい</td>
</tr>
</tbody>
</table>

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

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ていくことで、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、ぜひご覧ください。
194
バッファエラーの脆弱性

JVNDB-2018-004885

Accessの増加について
http://www.npa.go.jp/cyberpolice/detect/

JVNDB-2018-004886

遠隔地に存在するシステムの脆弱性

Fortinet, Inc.: A Wicked Family of Bots
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

JVNDB-2018-004886

複数のネットワーク機器を標的とするマルウェア

Cisco Systems, Inc.: VPNFilter-affected Devices Still Endpoints, Targets New Devices
https://blog.talosintelligence.com/2019/05/VPNFilter.html

Trend Micro Incorporated: ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai

VULDB:Cisco Linksys Router up to E4200 tmUnblock.cgi
http://www.exploit-db.com/exploits/45978

Palo Alto Networks, Inc.: A Wicked Family of Bots

Cisco Systems, Inc.: New VPNFilter malware targets at least 500K networking devices worldwide

Trend Micro Incorporated: Open ADB Ports Being Exploited to Spread Possible Satori Variant in Android Devices

Qihoo 360 Technology Co. Ltd.: Not Only Botnets: Hacking Group in Brazil Targets IoT Devices With Malware

Trend Micro Incorporated: Not Only Botnets: Hacking Group in Brazil Targets IoT Devices With Malware

Trend Micro Incorporated: VPNFilter-affected Devices Still Endpoints, Targets New Devices
https://blog.talosintelligence.com/2019/05/VPNFilter.html

Trend Micro Incorporated: Open ADB Ports Being Exploited to Spread Possible Satori Variant in Android Devices

Qihoo 360 Technology Co. Ltd.: Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading

Cisco Systems, Inc.: New ADB ports being exploited to spread possible Satori variant in Android devices
https://www.exploit-db.com/exploits/39596

Qihoo 360 Technology Co. Ltd.: Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading

Cisco Systems, Inc.: VPNFilter Update - VPNFilter exploits endpoints, targets new devices

Trend Micro Incorporated: VPNFilter-affected Devices Still Riddled With 19 Vulnerabilities
https://blog.trendmicro.com/
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なることが懸念となり，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させる可能性もあると考えられる。これについては別途議論が必要である。

※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ソフツウェア。
※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。
※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。
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。

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
资料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。

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）。

<table>
<thead>
<tr>
<th>届出種別</th>
<th>2018年</th>
<th>2017年</th>
<th>2016年</th>
</tr>
</thead>
<tbody>
<tr>
<td>像替</td>
<td>8</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>メール不正中綴</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>チーム感染</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DoS（サービス妨害）</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>アドレス詐称</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>なりすまし</td>
<td>24</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>不正プログラム埋込</td>
<td>3</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>その他（被害あり）</td>
<td>1</td>
<td>18</td>
<td>14</td>
</tr>
<tr>
<td>アクセス形跡（未遂）</td>
<td>9</td>
<td>22</td>
<td>19</td>
</tr>
<tr>
<td>チーム形跡</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>その他（被害なし）</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

合計（件）       54（43） 79（54） 83（61）
※合計のカッコ内の数値は、被害ありの届出種別の合計を示している。

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）。

<table>
<thead>
<tr>
<th>被害内容</th>
<th>2018年</th>
<th>2017年</th>
<th>2016年</th>
</tr>
</thead>
<tbody>
<tr>
<td>メール不正中綴</td>
<td>0</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>サーバダウン</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>不正アカウントの作成</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Web サイト改ざん</td>
<td>5</td>
<td>12</td>
<td>9</td>
</tr>
<tr>
<td>パスワードファイルの盗用</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>サービス低下</td>
<td>5</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>オープンプロキシ</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ファイルの書き換え</td>
<td>3</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>調査台として悪用</td>
<td>13</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>オンラインサービスの不正利用</td>
<td>10</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>データの窃取、盗み見</td>
<td>9</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>その他</td>
<td>4</td>
<td>23</td>
<td>16</td>
</tr>
</tbody>
</table>

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総合と一致していない。

■表B-2 2018年不正アクセス被害内容
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）。

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）。

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。

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」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
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。

C.2 ソフトウェア製品の脆弱性の処理状況届出種別
2018年末時点で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、告知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合計は 2,542 件に達した（表 C-2）。

C.3 ソフトウェア製品の脆弱性関連情報に関する届出状況

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四半期別推移を図 C-2（次ページ）に示す。
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。
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）]
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」の確立が求められています。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、ひとつ上の企業がセキュリティ対策を怠ったとしても、社会的に大きな損害を与える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問で構成されています。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。

### 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、業種別の診断基礎データと比較診断が行われます。結果、それぞれの比較対照別の、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、重要な役割を持つ情報を保有する数、ITの依存度などを計算する企業が抱えるリスクを表す指標のことです。

### データの表示

診断結果の表示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）、診断基礎データの平均値や業界別の診断結果が示されやすいレーダーチャート（図2参照）で示されます。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高く、円状に大きく広がっているほどバランスの良い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。

### 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業界別の診断結果が示されやすいレーダーチャート（図2参照）で示されます。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高く、円状に大きく広がっているほどバランスの良い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。

![散布図](https://www.ipa.go.jp/security/benchmark/)

![レーダーチャート](https://www.ipa.go.jp/security/benchmark/)
脆弱性体験学習ツール「AppGoat」
一突いてみますか？脆弱性！—

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、個人で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・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。

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「図2の構成」となります。また、「図3の画面イメージ」学習時の画面です。
今日は、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、有効な対策をとることができず、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調査や対策の情報発表し、「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、データは日々増える傾向です。

JVN iPediaでは、これだけの量のデータから特定の脆弱性を探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を調査したい」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

### 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。

<table>
<thead>
<tr>
<th>項目</th>
<th>情報内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>脆弱性対策情報ごとに付与されるJVN iPediaのIDです。</td>
</tr>
<tr>
<td>タイトル</td>
<td>脆弱性対策情報のタイトルです。</td>
</tr>
<tr>
<td>概要</td>
<td>脆弱性対策情報の概要です。</td>
</tr>
<tr>
<td>CVSSによる深刻度</td>
<td>CVSSによる脆弱性の深刻度を評価しています。</td>
</tr>
<tr>
<td>影響を受けるシステム</td>
<td>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。</td>
</tr>
<tr>
<td>想定される影響</td>
<td>脆弱性による想定される影響を記載しています。</td>
</tr>
<tr>
<td>対策</td>
<td>脆弱性の対策が記載されています。</td>
</tr>
<tr>
<td>ベンダ情報</td>
<td>ベンダの情報を発表しています。</td>
</tr>
<tr>
<td>参考情報</td>
<td>脆弱性対策情報に関連する情報へのリンクです。</td>
</tr>
<tr>
<td>更新履歴</td>
<td>更新履歴です。</td>
</tr>
<tr>
<td>公表日/登録日/最終更新日</td>
<td>公表日、登録日、最終更新日を記載しています。</td>
</tr>
</tbody>
</table>

※CVSS：共通脆弱性評価システム
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）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に登録されている情報の中から、利用者自身に関係する情報を効率的に検索できるように、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し、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。

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。

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]

付録

(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_YYMMDD.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。

※ 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/
※ 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/
※ 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
※ 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
※ 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
近年、特定の企業や組織の社員向け、関係者を装ってウィ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。

表1. チェック対象製品

<table>
<thead>
<tr>
<th>種別</th>
<th>ソフトウェア製品名</th>
<th>概要</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS向けアプリケーション</td>
<td>Adobe Flash Player (ActiveX, Plug-in)</td>
<td>動画再生ソフト</td>
</tr>
<tr>
<td></td>
<td>Adobe Reader</td>
<td>PDFファイル閲覧ソフト</td>
</tr>
<tr>
<td></td>
<td>Adobe Shockwave Player</td>
<td>動画再生ソフト</td>
</tr>
<tr>
<td></td>
<td>JRE</td>
<td>Java実行環境</td>
</tr>
<tr>
<td></td>
<td>Lhaplus</td>
<td>ファイル圧縮・解凍ソフト</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox</td>
<td>ウェブブラウザ</td>
</tr>
<tr>
<td></td>
<td>Mozilla Thunderbird</td>
<td>メールソフト</td>
</tr>
<tr>
<td></td>
<td>QuickTime</td>
<td>動画再生ソフト</td>
</tr>
<tr>
<td></td>
<td>iTunes</td>
<td>音楽・動画管理ソフト</td>
</tr>
<tr>
<td></td>
<td>Lunascape</td>
<td>ウェブブラウザ</td>
</tr>
<tr>
<td></td>
<td>Becky! Internet Mail</td>
<td>メールソフト</td>
</tr>
<tr>
<td></td>
<td>OpenOffice.org</td>
<td>文書編集ソフト</td>
</tr>
<tr>
<td></td>
<td>VMware Player</td>
<td>仮想化ソフト</td>
</tr>
<tr>
<td></td>
<td>Google Chrome</td>
<td>ウェブブラウザ</td>
</tr>
<tr>
<td></td>
<td>LibreOffice</td>
<td>文書編集ソフト</td>
</tr>
</tbody>
</table>

2019年3月時点

表2. 動作環境

<table>
<thead>
<tr>
<th>OS</th>
<th>製品バージョン</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (32bit版/64bit版)</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1 (32bit版/64bit版)</td>
<td></td>
</tr>
<tr>
<td>Windows 10 (32bit版/64bit版)</td>
<td></td>
</tr>
</tbody>
</table>

実行環境 .NET Framework 4.6

2019年3月時点
緊急に必要な脆弱性をリアルタイムに配信
https://www.ipa.go.jp/security/vuln/icat.html

ついに他に Economist がついに america とし始めた。

「icat for JSON」の利用イメージは図1通りです。

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

```html
<script type="text/javascript" src="https://www.ipa.go.jp/security/announce/irss/icath.js"> </script>
```
緊急性の高いセキュリティ情報発信
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。


表1.「注意警戒情報サービス」の対象となる情報

<table>
<thead>
<tr>
<th>重要なセキュリティ情報</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>サーバ製品リリース情報</td>
<td>Apache Struts, Bind, OpenSSL, WordPress</td>
</tr>
</tbody>
</table>

（2019年3月時点）

「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。

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を利用して、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。
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、自組織の危険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。誤検出の場合もあります。iLogScannerで攻撃が検出された場合、ウェブサイトの開発者やセキュリティベンダーに相談されることをお勧めします。

(*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に、攻撃者が悪意のあるSQL文を埋め込む（Injection）すると、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、重要情報の漏洩や悪意あるプロセスの実行が可能となります。

(*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、アプリケーションを実行する問題です。これにより、重要な情報が漏洩したり、不正なアプリケーションを実行されたりする危険があります。

(*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信してしまう問題です。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などの情報の漏洩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。パスワードを総当た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。同一のパスワードを総当た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、サーバーに不正アクセスが試みられている可能性があります。
クロスサイト・スクリプティング (XSS) の解説例（抜粋）

画像①：ストーリー仕立てで脆弱性を解説
画像②：難しい用語や略語は、注釈で解説
画像③：○×テストで理解度チェック
画像④：脆弱性の仕組みもアニメで分かりやすく解説
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。そのため、中小企業においても、ITの安全な活用に向けて、情報セキュリティ対策の重要性を認識し、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営しています。

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」と「企業の経営者を主な対象としての「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針に向けた「セキュリティプレゼンター支援」等で構成されています。

せキュリティプレサエントとは、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

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する企業を、セキュリティ向けの「セキュリティ対策支援サイト」、中小企業向けセキュリティ資料へのアクセスを提供します。
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、相互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
■ 5分できる！ポイント学習
「5分できる！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いて、インターネット利用ができない環境でも、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

情報セキュリティ対策の「知りたい」「学びたい」「始めたい」「続けたい」をサポートするサイト
https://security-shien.ipa.go.jp/
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
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がちで、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、目的に合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で到達できるサイトが異なることもあります。これらの問題解決のため、官民ボードを通じ、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。

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ー化しています。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。
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

■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

■おいしい話
東京都・筑波大学附属中学校・1年阿部遥香さん

■SNSは誰に見られるのか
鹿児島県・鹿児島県立川内商工高等学校・3年杉菌はるなさん
優秀賞

〈標語部門〉
メッセージ 怒った時に 送らない
疑って！ タダの裏には 何かある
災害時 うそとホントを見分けよう

〈ポスター部門〉

德島県 吉野川市立鴨島小学校 5年 上藤 幸歩さん
富山県 富山市立塚川中学校 2年 大田 詞也さん
大阪府 大阪市立東高等学校 2年 木原 涼さん

〈4コマ漫画部門〉

大人ばっかり!!
住所なんてのせちゃったら……
スマホに頼る男 田中

東京都 筑波大学附属中学校 2年 謙刈 雄大さん
京都府 同志社高等学校 1年 北村 祐樹さん
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 将真さん

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 広島商船高等学校専門学校 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 濱さん

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 隆人さん

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
アプリした 写真の未来に 笑顔ある?
岩手県 岩手県立西磐井高等学校 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 潤さん

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 茨城県立栃木中等教育学校 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 遥さん

茨城県教育庁学校教育部学校教育課
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 筑西市立上野小学校 3年
成田 真輝さん

茨城県メディア教育指導員連絡会
今日は スマホをやって 家ぞくでだれらん
茨城県 筑西市立上野小学校 3年
川原井 亜人さん

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 埼玉県立江南中学校 2年
倉野 美羽さん
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

千葉県 鎌ケ谷市立鎌ケ谷中学校 3年 野田 拓利さん

拡散しない 猟奇にしない デマや嘘

東京都 世田谷区立玉川小学校 6年 山崎 素直さん

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

ウイルスは あなたの興味の そばにする

石川県 石川県立小松明峰高等学校 1年 東出 美桜さん

たん生日 名前は危険 パスワード

長野県 松本市立九ノ内中学校 1年 出井 あさ美さん

ネットでは 自分もなく得る 悪い人

長野県 松本市立九ノ内中学校 1年 柴田 菜津美さん

たん生日 名前は危険 パスワード

長野県 松本市立九ノ内中学校 1年 髙橋 沙綾さん

ネットにあげたその写真 全て消すこと不可能です

愛知県 豊川市立一宮中学校 3年 平川 太進さん

「みつけたぞ」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

フォロワー数 それは君の 價値じゃない

特定非営利活動法人東海インターネット協議会

京都府 京都大学附属京都市中学校 6年 嶋村 和子さん

好奇心 軽くクリック 招くパニック

愛知県 日本大学三島高等学校 1年 山崎 晚紀さん

ネットをあがったその写真 全て消すこと不可能です

愛知県 田原市立福江中学校 3年 早川 太進さん

「みつけたぞ」写真でばれる あなたの居場所

愛知県 場内 達太郎さん

軽いノリ その代償は 永遠に

京都市立堀川高等学校 3年 嶋村 尚子さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都府 舞鶴市立青葉中学校 3年 嶋村 和子さん

「ごめんなさい」スマホを使わず あやまろう

京都市立堀川高等学校 3年 嶋村 尚子さん

軽いノリ その代償は 永遠に

京都市立堀川高等学校 3年 嶋村 尚子さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都市立堀川高等学校 3年 嶋村 尚子さん

「ごめんなさい」スマホを使わず あやまろう

京都市立堀川高等学校 3年 嶋村 尚子さん

軽いノリ その代償は 永遠に

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都市立堀川高等学校 3年 嶋村 尚子さん

「ごめんなさい」スマホを使わず あやまろう

京都市立堀川高等学校 3年 嶋村 尚子さん

軽いノリ その代償は 永遠に

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都市立堀川高等学校 3年 嶋村 尚子さん

「ごめんなさい」スマホを使わず あやまろう

京都市立堀川高等学校 3年 嶋村 尚子さん

軽いノリ その代償は 永遠に

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都市立堀川高等学校 3年 嶋村 尚子さん

「ごめんなさい」スマホを使わず あやまろう

京都市立堀川高等学校 3年 嶋村 尚子さん

軽いノリ その代償は 永遠に

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

ネット上 嘘の情報 見抜く目を

京都府 京都産業大学附属高等学校 1年 北 彩奈さん

人気より 高めるべきは セキュリティー

京都市立堀川高等学校 3年 嶋村 尚子さん
秋田県・大潟村立大潟中学校・1年
後藤 茉莉花さん

福井県・福井市湊小学校・5年
勝見 いろはさん

三重県・三重県立名張高等学校・3年
柴田 すずなさん

長野県・長野県駒ケ根工業高等学校・3年
松下 脚緒奈さん
奈良県・奈良県立奈良北高等学校 2年
後藤・碧さん

島根県・島根県立浜田商業高等学校 1年
中・小織さん

山口県・山口県立宇部商業高等学校 3年
久保・裕亮さん

広島県・熊野町立熊野中学校 2年
緒方・真珠さん

岡山県・岡山県立高梁城南高等学校 2年
新谷・怜桜さん

(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

（公益社団法人京都府防犯協会連合会）

鳥取県・鳥取県立鳥取湖陵高等学校 3年
大西・桃夏さん

（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 2年
河原・未玖さん

（特定非営利活動法人
奈良地域の学び推進機構）

滋賀県・大津市立北大路中学校 3年
吉岡・翼菜さん

（滋賀県警察本部）

鳥取県・島根県立浜田商業高等学校 1年
中小織さん

（鳥取県警察本部）

岡山県・岡山県立高梁城南高等学校 2年
新谷・怜桜さん

（岡山県警察本部）

広島県・熊野町立熊野中学校 2年
緒方・真珠さん

（広島県警察本部）

山口県・山口県立宇部商業高等学校 3年
久保・裕亮さん

（山口県警察本部）
德島県 徳島市立津田中学校 3年
滑川 由菜さん

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 久万高原町立久万中学校 1年
梶川 春菜さん

佐賀県 小城市立崎田小学校 5年
中島 椿さん

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 御船町立御船中学校 2年
麻井 春陽さん

宮崎県 宮崎市立赤江中学校 3年
横田 百音さん

鹿児島県 鹿児島県立鹿児島工業高等学校 2年
濱田 優季さん

沖縄県 沖縄県立八重山商工高等学校 3年
新垣 宝さん
<table>
<thead>
<tr>
<th>索引</th>
</tr>
</thead>
<tbody>
<tr>
<td>数字</td>
</tr>
<tr>
<td>5G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADB.Miner</td>
</tr>
<tr>
<td>AI・データの利用に関する契約ガイドライン</td>
</tr>
<tr>
<td>AI プロダクト品質保証ガイドライン</td>
</tr>
<tr>
<td>Anti-Phishing Working Group, Inc. (APWG)</td>
</tr>
<tr>
<td>Apache Struts2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>BrickerBot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC (Common Criteria:共通基準)</td>
</tr>
<tr>
<td>CCRA (Common Criteria Recognition Arrangement)</td>
</tr>
<tr>
<td>CISO (Chief Information Security Officer:最高情報セキュリティ責任者)</td>
</tr>
<tr>
<td>Connected Industries</td>
</tr>
<tr>
<td>CRYPTREC</td>
</tr>
<tr>
<td>CSIRT (Computer Security Incident Response Team)</td>
</tr>
<tr>
<td>CSV ファイル</td>
</tr>
<tr>
<td>CYBER COLOSSEO</td>
</tr>
<tr>
<td>Cyber Sense Act</td>
</tr>
<tr>
<td>Cybersecurity and Infrastructure Security Agency (CISA)</td>
</tr>
<tr>
<td>CYDER (Cyber Defense Exercise with Recurrence：実践的サイバー防衛演習)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS 攻撃</td>
</tr>
<tr>
<td>DDoS 攻撃代行サービス</td>
</tr>
<tr>
<td>Drupal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENISA (European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ庁)</td>
</tr>
</tbody>
</table>

| 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-ネットキャラバン | 118 |

<table>
<thead>
<tr>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framework for Improving Critical Infrastructure Cybersecurity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>G20 AI 原則</td>
</tr>
<tr>
<td>G7 シャルルポワ・サミット</td>
</tr>
<tr>
<td>GCM-AES-XPN</td>
</tr>
<tr>
<td>GDPR (General Data Protection Regulation：一般データ保護規則)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIoT (Industrial Internet of Things)</td>
</tr>
<tr>
<td>IoT</td>
</tr>
<tr>
<td>IoT 機器のセキュリティ対策に関する検討の方向性</td>
</tr>
<tr>
<td>IoT サイバーセキュリティアクションプログラム 2017</td>
</tr>
<tr>
<td>IoT 社会に対応したサイバー・フィジカル・セキュリティ</td>
</tr>
<tr>
<td>IoT セキュリティガイドライン</td>
</tr>
<tr>
<td>IoT セキュリティ総合対策</td>
</tr>
<tr>
<td>IoT セキュリティ総合対策 プログレスレポート 2018</td>
</tr>
<tr>
<td>IoT セキュリティ対策に関する提言</td>
</tr>
<tr>
<td>IoT ボット</td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 27</td>
</tr>
<tr>
<td>ITSS+</td>
</tr>
<tr>
<td>IT サプライチェーン</td>
</tr>
<tr>
<td>IT 製品の調達におけるセキュリティ要件リスト</td>
</tr>
<tr>
<td>IT セキュリティ評価及び認証制度(Japan Information Technology Security Evaluation and Certification Scheme: JISEC)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java SE 8</td>
</tr>
<tr>
<td>JC 版サイバーセキュリティ問題解決プログラム</td>
</tr>
<tr>
<td>J-CRAT (Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊)</td>
</tr>
<tr>
<td>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)</td>
</tr>
</tbody>
</table>
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
サイバーセキュリティの構想 ................................................... 65
サイバーセキュリティ18 ........................................... 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, 112, 182
サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのブラウティス集 ................................................... 67, 109
サイバーセキュリティ経営ブラウティス検討会 ......................... 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ラボレーション ......................... 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 ........................... 95, 100
ワーキンググループ報告書 ............................................. 62, 95, 108, 113
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策調整センター ......................... 64, 68
サイバーセキュリティタスクフォース .................................... 63, 71
サイバーセキュリティ研究会 ............................................. 65
サイバーセキュリティ研究会 ............................................. 65
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概要 ...................................... 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関する基本策定指針 ......................... 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
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
中央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
データ活用..........................................................139
デジタルトランسمファッション時代における人材育成プログラム
67
デジタル標準（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対策と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
統合セキュリティー人材モデル...........................................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

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

バイオメトリックス.....................................................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
プラックス・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

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

ランサムウェア..........................................................10, 29, 31, 36, 157
リフレクター攻撃.......................................................25, 26
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、より気軽に読んでもいただけるよう、著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

おわりに
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 慶一 武洋 洋 山里 拓己 坂田 剛雄 神田 雅透
西尾 秀一 小川 隆一 江島 将和 大谷 祐子 内山 友弘
廣田 美幸 浅井 優子 山崎 知嗣 天野 農 丸 宏
福原 聡 猪城 明 板橋 博之 井上 真弓 大友 更紗
岡下 博子 龜山 友彦 唐亀 信久 小林 桂 佐藤 輝夫
田村 智和 渡邉 祥樹 麗野 一人 須藤 直樹 神戸 世二
伊東 隆司 架原 史康 竹内 智子 西村 奏一 甲斐 佳樹
篠倉 玄弥 橋本 徹 小暮 淳 近澤 武 塚元 卓
細野 元 河合 和哉 金子 子一 嶋藤 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
桜名 利幸 高橋 将 橋山 尚人 小宮 弥生 加賀谷 伸一郎
渡辺 貴仁 松坂 志 松井 靖二 輝谷 萩莉衣 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 逃山 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 嶴明
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