資料３

令和３年１月 26 日
内閣サイバーセキュリティセンター

重要インフラを取り巻く情勢について

重要インフラは、豊かで便利な国民社会を支えている。機能性、コストなどの観点から重要インフラの IT 依存度は年々高まってきている。その一方で、重要インフラを取り巻く国際情勢、サイバー情勢、技術動向は時々刻々変化してきており、重要インフラの機能保証を確保していくためには、重要インフラを取り巻く情勢を把握し、関係者間で共有し、論点、価値観の共有が重要である。また、日々発生するサイバーインシデントを分析して得られた結果を共有することは、重要インフラの強靭性を高める観点から重要である。

このため、四半期ごとの重要インフラを取り巻く情勢分析と情報提供されたインシデント分析結果から得られた知見を共有する。

添付資料

サイバーセキュリティを取り巻く情勢(2020 年度第 2 四半期)

【目的】

サイバーセキュリティ技術の急速な進展により、重要インフラを取り巻く情勢は急速な変化を続けている反面、変化に追随することは容易とは言えなくなってきました。

本報告は、サイバーセキュリティに係る国外政策、国内外情勢、技術動向及びリスク関連動向に関して、2020 年度第 2 四半期(7 月～9 月)の主な公開情報をまとめたものであり、サイバーセキュリティを取り巻く情勢の把握の一助とすることを目的に編纂したものです。

【注意事項】

本報告は、公開情報をもとに作成したものである特性から、情報の真偽について保証するものではありません。ご活用の際はご留意ください。

1. 国外サイバーセキュリティ政策

1.1. 国際動向

1.1.1 5G サプライチェーンをめぐる情勢

- 2020 年 8 月 13 日、米国は政府調達のサプライチェーン対策として、ファーウエイを含む中国企業の製品・サービスを米国政府機関との取引から排除する条項を盛り込んだ 2019 年度米国防権限法を施行[1]。
- 本法施行に伴う日本企業への影響は不透明なものの、日本企業のファーウエイとの取引金額は 2018 年で 7,000 億円超の状況[2]。
- 2020 年 5 月及び 8 月、米国はファーウエイに対する半導体の規制強化策を相次いで発表し、猶予期間を経て、2020 年 9 月 15 日から発動[3]。
- 米国によるファーウエイ排除に向けた動きが欧州を中心とした諸外国に広がる中、日本でも新たに 5G サプライチェーン対策の取組が決定[4]。

1.1.2 TikTok をめぐる情勢

- 2020 年 8 月 6 日、米国は中国政府によるデータアクセスの懸念から TikTok の米国事業売却を命じる大統領令を発動、それに対して適正な手続きを欠

---

[1] *時事ドットコム「米、中国 5 社の取引先排除　政府調達で、ファーウエイなど―日本企業への影響必至(2020/8/13)」、https://www.jiji.com/jc/article?k=2020081300287（2020/9/16 閲覧）*

[2] *ダイヤモンド・オンライン「ファーウエイの息の根を止めかねない、米制裁「異次元の厳しさ」(2019/5/23)」、https://diamond.jp/articles/-/203400（2020/9/17 閲覧）*

[3] *朝日新聞「ファーウエイ輸出規制、米国が本格化へ　逃げ場失う中国(2020/9/11)」、https://www.asahi.com/articles/ASN9C6562N9BULFA017.html（2020/10/8 閲覧）*

[4] *経済産業省「「特定高度情報通信技術活用システムの開発供給及び導入の促進に定める政令」及び「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律施行令」が閣議決定(2020/8/25)」、https://www.meti.go.jp/press/2020/08/20200825004/20200825004.html（2020/9/17 閲覧）*

いたとして TikTok 側が米国政府を 2020 年 8 月 24 日に提訴[5]。

- ○ 米国は TikTok アプリのダウンロードを 2020 年 9 月 20 日に禁止し、TikTok の米国事業の閉鎖措置を 2020 年 11 月 12 日に行うとの大統領令を発表、TikTok 側は、連邦裁判所に異議申立てを行い、2020 年 9 月 27 日、同裁判所はダウンロード禁止令を暫定的に差し止める判決[6]。

1.1.3 新型コロナウイルス感染症関連サイバー攻撃

- ○ 世界的に流行している新型コロナウイルス感染症に便乗する偽メール[7]、偽ワクチンの提供をうたった不正サイトが観測。
- ○ その後、新型コロナウイルス感染症対策として急速に進んだテレワークの脆弱性を突いた Windows のリモートデスクトッププロトコルを狙った攻撃や新型コロナウイルス感染症に関連する研究機関[8]等へのサイバー攻撃が増加。
- ○ こうした事態を受け、英国、米国、カナダ等のサイバーセキュリティ機関は注意喚起を発出[9]。

1.2. 米国

1.2.1 米国大統領選挙

- ○ 米国大統領選挙は 2020 年 11 月 3 日に投開票を迎え、対立深まる中国への対応が主要争点に浮上するなど、トランプ、バイデン両候補者による対中政策は大きく注目[10]。
- ○ 開票作業が続く中、2020 年 11 月 7 日、米国主要メディアはバイデン候補が激しい競り合いを制し、当選を確実にしたと報道。これを受け、バイデン候補は勝利を宣言、他方、トランプ候補は、裁判を通じて争う構え[11]。
- ○ 大統領選挙の最中である 2020 年 9 月 10 日、Microsoft は大統領選挙関係者を標的としたサイバー攻撃があったことを発表。[12]

---

[5] *ByteDance「Why we are suing the Administration(2020/8/24)」、https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit（2020/8/25 閲覧）*

[6] *時事通信「TikTok 禁止差し止め 米連邦地裁が命令 配信継続へ(2020/9/28)」、https://www.jiji.com/jc/article?k=2020092800148&g=int（2020/9/30 閲覧）*

[7] *IPA「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(2020/9/2)」、https://www.ipa.go.jp/security/announce/20191202.html#L10（2020/9/21 閲覧）*

[8] *ITmedia「医療機関や学術機関を狙うサイバー攻撃が多発、米英が警戒呼びかけ(2020/5/8)」、https://www.itmedia.co.jp/enterprise/articles/2005/08/news055.html（2020/9/21 閲覧）*

[9] *CISA「Alert (AA20-099A)COVID-19 Exploited by Malicious Cyber Actors(2020/4/8)」、https://us-cert.cisa.gov/ncas/alerts/aa20-099a（2020/9/23 閲覧）*

[10] *時事通信「対中強硬姿勢、競い合い、米大統領選の争点に浮上―トランプ、バイデン両陣営(2020/8/3)」、https://www.jiji.com/jc/article?k=2020080100352&g=int（2020/10/20 閲覧）*

[11] *NHK「バイデン前副大統領が勝利宣言「分断ではなく結束を」(2020/11/8)」、https://www3.nhk.or.jp/news/html/20201108/k10012700691000.html（2020/11/8 閲覧）*

[12] *マイクロソフト「米国の選挙を標的とした新たなサイバー攻撃(2020/9/10)」、https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/（2020/10/4 閲覧）*

1.3. 中国

1.3.1 中国データセキュリティ法(草案)

- 2020 年 7 月 3 日、中国全国人民代表大会常務委員会はデータセキュリティ法の草案をパブリックコメント用に公開。本草案は、漏洩した場合、中国の国家安全保障、公共の利益に直接影響を与える可能性のある「重要なデータ」のガバナンスに重点を置いたものとなっている一方、多くの規定は曖昧との指摘[13]。
- 本草案は 2020 年 8 月 16 日までのパブリックコメントを踏まえ、今後正式に「中国データセキュリティ法」として公布される予定であるが、既存の「中国サイバーセキュリティ法」や今後起草が見込まれる「中国個人情報保護法」とともに情報分野での基本的な位置づけの法律になると考えられる[14]。

2. 国外におけるサイバーセキュリティをめぐる情勢

2.1. 政府機関関連

2.1.1 米国政府 3 機関による中国マルウエア分析レポートの公開

- 2020 年 8 月 3 日、米国政府 3 機関(CISA、FBI 及び DoD)は共同で、中国政府の攻撃者が使用したとされるマルウエア「Taidoor」について分析レポートを公開、中国の悪意のあるサイバー活動に対し、セキュリティ体制強化を呼びかけ[15]。

2.1.2 米国の大規模サイバー演習 Cyber Storm 2020

- 2020 年 8 月、CISA は米国内で最も大規模なサイバー演習である「Cyber Storm 2020」を開催、3 日間の演習に連邦政府、州政府、地方自治体、民間企業等から約 2,000 人が参加[16]。
- 本演習の目的は、重要インフラを標的とした複数分野のサイバー攻撃を特定し、それに対応するための方針、プロセス、手順を実行することで、サイバーセキュリティへの備えと対応能力強化を図ること[17]。
- こうした目的の下、毎回複数の演習目標を設定し、演習終了後、レポートを

---

[13] *AXION「中国がデータセキュリティ法の草案を公表 (2020/8/7)」、https://www.axion.zone/china-issued-the-draft-data-security-law/ (2020/9/4 閲覧)*

[14] *BizRis「中国データセキュリティ法(草案)解説(2020/10/22)」、https://portal.bizrisk.iij.jp/feature/6 (2020/10/29 閲覧)*

[15] *CISA「Malware Analysis Report (AR20-216A)MAR-10292089-1.v1 – Chinese Remote Access Trojan: TAIDOOR(2020/8/3)」、https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a (2020/9/9 閲覧)*

[16] *CISA「CISA HOSTS SEVENTH CYBER STORM EXERCISE WITH GOVERNMENT, INDUSTRY AND INTERNATIONAL PARTNERS (2020/8/14)」、https://www.cisa.gov/news/2020/08/14/cisa-hosts-seventh-cyber-storm-exercise-government-industry-and-international (2020/9/7 閲覧)*

[17] *CISA「CYBER STORM 2020」、https://www.cisa.gov/cyber-storm-2020 (2020/9/9 閲覧)*

公開する予定[18]。

2.1.3　NIST SP800-207 ゼロトラストアーキテクチャ(ZTA)

- ○ 2020 年 8 月、米国国家標準技術研究所(NIST)は「SP800-207 Zero Trust Architecture（ゼロトラストアーキテクチャ）」の正式版をリリース[19]。
- ○ モバイルや IoT などの多様なデバイス、テレワーク、クラウドサービスの普及等により、従来のネットワーク境界での防御の技術で対応が難しい巧妙化する脅威に対し、効果的にリスクを低減させるもの。
- ○ ゼロトラストアーキテクチャは、全てのユーザーやデバイスなどを潜在的な脅威として扱い、適切に識別、認証し承認されるまでアクセスを阻止することで組織のデータとリソースを保護するもの。
- ○ NIST は、NCCoE(National Cyber Security Center of Excellence)を通じた官民連携により、「ゼロトラストアーキテクチャの実装」プロジェクトを実施[20]。

2.1.4　NIST SP800-53 の最新版 Rev.5 をリリース

- ○ 2020 年 9 月、米国国家標準技術研究所(NIST)は SP800-53 の最新版「SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations(情報システムと組織のためのセキュリティとプライバシーの管理策)」の正式版をリリース[21]。
- ○ SP800-53 は米国の連邦情報セキュリティ管理法(FISMA: Federal Information Security Management Act of 2002)に基づいており、米国政府機関におけるセキュリティ強化のための FISMA 実施プロジェクトに対する主要な成果物の一つ[22]。
- ○ Rev.5 は 7 年ぶりの改訂であり、個人情報保護やサプライチェーンリスク等の状況変化に対応。

---

[18] *HSToday「CISA's Cyber Storm 2020 Tests Interconnected Preparedness for a Widespread Attack (2020/8/15)」、https://www.hstoday.us/subject-matter-areas/infrastructure-security/cisas-cyber-storm-2020-tests-interconnected-preparedness-for-a-widespread-attack/ (2020/9/7 閲覧)*

[19] *NIST「NIST Special Publication (SP) 800-207, Zero Trust Architecture(2020/8/11)」、https://csrc.nist.gov/publications/detail/sp/800-207/final (2020/9/23 閲覧)*

[20] *NCCoE「Zero Trust Architecture」、https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture (2020/12/21 閲覧)*

[21] *NIST「SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations(2020/9/23)」、https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (2020/10/19 閲覧)*

[22] *NIST「FISMA Implementation Project(2020/10/13 更新)」、https://csrc.nist.gov/projects/risk-management/ (2020/10/19 閲覧)*

2.2. 重要インフラ関連

2.2.1 医療機関等に対するランサムウエア攻撃

- 医療機関や医療関連企業に対するランサムウエア攻撃が頻発。
- 2020 年 9 月、ドイツのデュッセルドルフ大学病院に対するランサムウエア攻撃が患者 1 名の死亡につながったと報道[23]。
- 2020 年 9 月、米国ニュージャージー州の大学病院がランサムウエア攻撃を受け、身代金 67 万ドルを支払い[24]。
- 2020 年 9 月、米国医療サービス大手 Universal Health Services がランサムウエア攻撃を受け、米国各地の医療施設のシステムが停止[25]。

2.2.2 ニュージーランド証券取引所に対する DDoS 攻撃

- 2020 年 8 月中旬以降、世界中の様々な組織で、攻撃者グループ「Fancy Bear」や「Armada Collective」を名乗る攻撃者による DDoS 脅迫キャンペーンを確認[26]。
- DDoS 攻撃の影響により、ニュージーランド証券取引所の取引が 2020 年 8 月 25 日から 4 日間連続、一時停止する等の被害が発生[27]。

2.3. その他

2.3.1 マルウエア「Emotet」に関する攻撃活動の再開

- 2020 年 7 月以降、再びマルウエア「Emotet」に関する攻撃活動が活発化[28]。
- 2020 年 7 月には感染端末から窃取したメールの添付ファイルを使用し、端末の利用者になりすます新たな手口[29]を、また 2020 年 9 月にはパスワード付き ZIP ファイルを利用した新たな手口[30]を確認。

---

[23] *ZDNet「First death reported following a ransomware attack on a German hospital(2020/9/17)」、https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/ (2020/10/5 閲覧)*

[24] *Bleeping Computer「New Jersey hospital paid ransomware gang $670K to prevent data leak(2020/10/3)」、https://www.bleepingcomputer.com/news/security/new-jersey-hospital-paid-ransomware-gang-670k-to-prevent-data-leak/ (2020/10/5 閲覧)*

[25] *Bleeping Computer「UHS hospitals hit by reported country-wide Ryuk ransomware attack(2020/9/28)」、https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/ (2020/10/5 閲覧)*

[26] *Akamai Technologies「RANSOM DEMANDS RETURN: NEW DDOS EXTORTION THREATS FROM OLD ACTORS TARGETING FINANCE AND RETAIL(2020/8/24)」、https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html (2020/9/7 閲覧)*

[27] *REUTERS「NZ 証取が取引再開、サイバー攻撃で 4 日連続停止、政府が支援へ(2020/8/28)」、https://jp.reuters.com/article/nzx-cyber-idJPKBN25O03C (2020/9/7 閲覧)*

[28] *Proofpoint「Emotet が 5 か月ぶりに攻撃再開(2020/7/17)」、https://www.proofpoint.com/jp/blog/security-briefs/emotet-returns-after-five-month-hiatus (2020/8/4 閲覧)*

[29] *Cofenselabs(Twitter)「Cofense Labs(@CofenseLabs)の投稿(2020/7/29)」、https://twitter.com/CofenseLabs/status/1288201468030464001 (2020/8/3 閲覧)*

[30] *JPCERT/CC「マルウェア Emotet の感染拡大および新たな攻撃手法について(2020/9/4)」、https://www.jp*

2.3.2 ソフトウエアのサプライチェーンにおけるサイバーセキュリティの脅威

- ○ 米国のシンクタンク、アトランティックカウンシルはソフトウエア・サプライチェーンへの攻撃と脆弱性についての報告書を公開し、過去 10 年間、合計 115 件の事例について調査・分析[31]。
- ○ その結果、「国家が関与する攻撃」、「更新プログラムのハイジャック」、「コード署名の無効化」、「オープンソースソフトウェアの危殆化」及び「アプリストアへの攻撃」と 5 つの傾向を特定し、それらに対処、緩和及び対抗するため、ツールやベストプラクティスの標準化による「ベースラインの改善」、「オープンソースの保護」、国際的な連携による「システミックな脅威への対抗」の 3 つの奨励事項を提示。

2.3.3 影響が大きい脆弱性の相次ぐ公表

- ○ 新型コロナウイルス感染症拡大に伴う緊急事態宣言期間中(2020 年 4 月 7 日～5 月 25 日)は、サイバー攻撃が宣言発出前と比べ約 20%増加[32]。
- ○ 2020 年 7 月、ネットワーク機器や DNS サーバー等に関する脆弱性[33]が多数公開。
- ○ これらの脆弱性のいくつかについては、概念実証(PoC)が公開されており、CISA が注意喚起を発出[34]するなど影響の大きいものも見受けられた。

2.3.4 Netlogon の特権昇格が可能な脆弱性「Zerologon」

- ○ 2020 年 8 月 12 日、Microsoft が Netlogon の特権昇格が可能な脆弱性(CVE-2020-1472)[通称:Zerologon]を公開[35]。
- ○ 2020 年 9 月 15 日以降、本脆弱性に関する概念実証(PoC)が複数公開されたことを契機に CISA 等の機関が迅速なパッチ適用を呼びかけ[36]。

---

cert.or.jp/newsflash/2020090401.html (2021/1/4 閲覧)

[31] *Atlantic Council「Breaking trust: Shades of crisis across an insecure software supply chain(2020/7/16)」、https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/ (2020/8/25 閲覧)*

[32] *サイバーセキュリティクラウド「サイバーセキュリティクラウド、2020 年度上半期攻撃検知レポートを発表 ～緊急.事態宣言発出前と比較して宣言中はサイバー攻撃が約 20%増加～(2020/7/22)」、https://www.cscloud.co.jp/news/press/202007222753/ (2020/8/4 閲覧)*

[33] *F5 Networks「K52145254: TMUI RCE vulnerability CVE-2020-5902(2020/7/1)」、https://support.f5.com/csp/article/K52145254 (2020/8/18 閲覧)*

[34] *CISA「Alert (AA20-206A) Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902(2020/7/24)」、https://us-cert.cisa.gov/ncas/alerts/aa20-206a (2020/8/18 閲覧)*

[35] *Microsoft「CVE-2020-1472 | Netlogon の特権の昇格の脆弱性(2020/10/29)」、https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-1472 (2020/12/16 閲覧)*

[36] *CISA「Unpatched Domain Controllers Remain Vulnerable to Netlogon Vulnerability, CVE-2020-1472(2020/9/24)」、https://us-cert.cisa.gov/ncas/current-activity/2020/09/24/unpatched-domain-controllers-remain-vulnerable-netlogon (2020/10/2 閲覧)*

3. 国内におけるサイバーセキュリティをめぐる情勢

3.1. 重要インフラ関連

3.1.1 ドコモ口座等について

- NTT ドコモの「ドコモ口座」をはじめとした電子決済サービスを利用した口座振替による不正出金が複数の金融機関で発生[37]。
- ゆうちょ銀行のデビット・プリペイドカード「mijica」の会員サイトへの不正アクセスにより、個人情報が流出した可能性があるほか、不正引出が発生[38]。
- SBI 証券においては、不正アクセスにより、顧客資産が流出[39]。
- いずれも、利用者認証(本人確認)の甘さが原因。

3.2. その他

3.2.1 SNS を悪用したソーシャルエンジニアリングにより組織内に侵入する攻撃

- 2020 年 8 月 7 日、三菱重工は、SNS を悪用したソーシャルエンジニアリングにより、同社グループのネットワークが第三者による不正アクセスを受けたことを発表[40]。
- 2019 年以降、SNS を悪用したソーシャルエンジニアリングの手法を利用し、防衛、航空宇宙産業のネットワークへの侵入を試みる攻撃が複数発生[41]。

3.2.2 NTT コミュニケーションズへの BYOD 端末等を通じた不正アクセス

- 2020 年 5 月、NTT コミュニケーションズに対する不正アクセスにより、社内に保存されていたファイルが閲覧された可能性のある事案が発生[42]。
- 調査の結果、当初は海外拠点への攻撃及び侵入を起点とした不正アクセスが明らかになったが、その後社内の BYOD 端末による不正アクセスも発覚し、今後の対応・対策の実施を発表[43]。

以上

---

[37] *NTT ドコモ「ドコモ口座への銀行口座の新規登録における対策強化について(2020/9/9)」、https://www.nttdocomo.co.jp/info/news_release/detail/20200909_00_m.html (2020/10/20 閲覧)*

[38] *ゆうちょ銀行「mijica 専用 WEB サイトへの不正ログインの範囲・規模について(2020/10/4)」、https://www.jp-bank.japanpost.jp/aboutus/press/2020/pdf/pr201004.pdf (2020/10/20 閲覧)*

[39] *SBI 証券「悪意のある第三者による不正アクセスに関するお知らせ(2020/9/16)」、https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html (2020/10/20 閲覧)*

[40] *三菱重工「当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件(2020/8/7)」、https://www.mhi.com/jp/notice/notice_200807.html (2020/9/10 閲覧)*

[41] *ClearSky「Operation 'Dream Job' Widespread North Korean Espionage Campaign(2020/8/13)」、https://www.clearskysec.com/operation-dream-job/ (2020/9/11 閲覧)*

[42] *NTT コミュニケーションズ「当社への不正アクセスによる情報流出の可能性について(2020/5/28)」、https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html (2020/8/3 閲覧)*

[43] *NTT コミュニケーションズ「当社への不正アクセスによる情報流出の可能性について(第 2 報)(2020/7/2)」、https://www.ntt.com/about-us/press-releases/news/article/2020/0702.html (2020/8/3 閲覧)*

重要インフラにおける情報共有件数について（2020 年度第 3 四半期）

「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」に基づき、内閣官房(NISC)、関係省庁、関係機関及び重要インフラ事業者等との間で行われた情報共有の実施状況は以下のとおり。

（単位:件）

実施形態	FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
重要インフラ事業者等からNISCへの情報連絡(※)	856	388	223	269	61	75	86	－	222
関係省庁・関係機関からのNISCへの情報共有	41	19	7	16	4	6	1	－	11
NISCからの情報提供	80	54	43	38	11	8	21	－	40

※1)重要インフラ事業者等からNISCへの情報連絡の事象別内訳は以下のとおり。

事象の類型			FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
未発生の事象		予兆・ヒヤリハット	330	80	27	12	3	4	13	－	20
発生した事象	機密性を脅かす事象	情報の漏えい	30	15	13	13	4	5	4	－	13
	完全性を脅かす事象	情報の破壊	47	20	17	11	4	4	3	－	11
	可用性を脅かす事象	システム等の利用困難	80	143	97	158	39	41	37	－	117
	上記につながる事象	マルウェア等の感染	289	65	17	9	4	4	3	－	11
		不正コード等の実行	10	13	4	5	0	1	1	－	2
		システム等への侵入	26	17	14	14	1	3	11	－	15
		その他	44	35	34	47	6	13	14	－	33

※2)上記事象における原因別類型は以下のとおり。（複数選択）

事象の類型		FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
意図的な原因	不審メール等の受信	546	89	36	13	2	4	0	－	6
	ユーザＩＤ等の偽り	1	4	3	12	0	5	2	－	7
	DDoS攻撃等の大量アクセス	23	31	17	20	4	3	1	－	8
	情報の不正取得	14	16	10	8	3	2	4	－	9
	内部不正	0	4	1	0	0	0	0	－	0
	適切なシステム等運用の未実施	19	15	14	11	4	3	7	－	14
偶発的な原因	ユーザの操作ミス	15	23	10	6	4	5	3	－	12
	ユーザの管理ミス	8	13	6	6	3	0	2	－	5
	不審なファイルの実行	243	42	16	7	0	4	1	－	5
	不審なサイトの閲覧	29	20	4	5	0	1	2	－	3
	外部委託先の管理ミス	20	41	29	39	9	12	15	－	36
	機器等の故障	22	32	27	62	10	11	13	－	34
	システムの脆弱性	56	36	19	16	3	3	22	－	28
	他分野の障害からの波及	0	10	6	4	2	2	2	－	6
環境的な原因	災害や疾病等	0	0	1	13	0	7	2	－	9
その他の原因	その他	34	29	29	33	9	9	6	－	24
	不明	92	57	46	53	18	14	18	－	50

（注）FY:年度、Q:四半期

最近のインシデントから得られた教訓

1　趣旨

重要インフラサービスに関連したインシデント情報は、重要インフラ所管省庁からの情報連絡を通じて内閣サイバーセキュリティセンターに集約されているが、これらの情報から教訓を案出し共有を図る等、これらの情報の有効活用を促進していくことを考えている。

なお、説明を簡潔にするため、複雑な状況を簡易に整理しており、一部具体性に欠ける記載がある旨を御承知置きいただきたい。

2　インシデントから得られた教訓

○　サイバー攻撃対応は引き続き必要であるが、他のリスク源にも注意が必要

システムの更新・設定の不具合、外部委託先の不具合、内部の人的統制の不具合、自然災害に起因するサービス障害等、外部からのサイバー攻撃以外の要因によるサービス障害の事例のほうが依然として多く発生している。

○　サプライチェーン管理の徹底が必要

クラウドに構築したシステム更改に伴う仕様変更の連絡不徹底による意図しない公開設定により、クラウドに保存した機密情報が外部に公開された事例があった。

サプライチェーンに携わる事業者間のコミュニケーション強化や設定どおりの稼働の確保に留意。

○　接続機器の資産（構成）管理が必要

セキュリティアップデート未適用の VPN の脆弱性を突いた認証情報の窃取により機密情報漏えいのリスクが高まったほか、外部に接続していないはずのネットワーク内のシステムが外部委託した運用監視機器経由でマルウエアに感染した事例があった。

○　リスクに応じた外部サービスの利用が必要

外部委託先である DNS ドメイン名登録事業者が残した脆弱性を突いた、第三者による DNS ドメイン名登録情報の書換えによる別サーバへのメール誘導により、メールが窃取された事例があった。

○　システム更改時等の作業誤り等に対する備えが必要

年末年始を利用したシステム更改の際のプログラムミス・設定誤りや、年末での電子証明書の有効期限切れにより不具合が発生し、サービスが提供できなかった事例があった。

以上