資料７

令和４年５月30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(2021 年度第 4 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、2021 年度第 4 四半期(1 月～3 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。御活用の際は御留意ください。

1. 国外サイバーセキュリティ政策

1.1. 米国

1.1.1 サプライチェーンやサイバーセキュリティの大統領令に対する政府機関等の取組

○ 2022 年 2 月 24 日までに、6 つの主要産業基盤分野を所管する省庁がそれぞれ、サプライチェーン・リスクや強靭性を評価する報告書を公表。これは、2021 年 2 月 24 日、バイデン大統領が署名した、米国サプライチェーンの強靭性を向上するための大統領令(EO14017)に基づき、6 つの主要産業基盤分野に対し、報告書を 2022 年 2 月までに提出するよう指示したことを受けたもの[1]。

○ 2022 年 1 月 13 日、バイデン政権は米国のオープンソースソフトウエアのセキュリティを向上させるための会議を開催。これは、2021 年 5 月 12 日に公表された「国家のサイバーセキュリティの向上に関する大統領令(EO14028)」に基づくもの[2]。

○ 2022 年 2 月 3 日、米国国土安全保障省(DHS)は、EO14028 の内容を受け、サイバー安全審査委員会(CSRB)を創設、Log4j に係る脆弱性に焦点を当て

---

[1] *U.S. DEPARTMENT OF COMMERCE AND U.S. DEPARTMENT OF HOMELAND SECURITY「ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S. INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY(2022/2/24)」、https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf (2022/4/5 閲覧)*

[2] *THE WHITE HOUSE「Readout of White House Meeting on Software Security(2022/1/13)」、https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/ (2022/2/15 閲覧)*

た一次報告書を 2022 年夏頃に公表予定[3]。

1.1.2 米国サイバーセキュリティ・インフラセキュリティ庁(CISA)による官民連携の取組

- ○ ウクライナ侵攻前の 2022 年 1 月頃からウクライナ周辺での大規模なサイバー攻撃を契機に、米国政府は米国国内の企業や重要インフラ等に影響が出る可能性を警告、サイバー攻撃の影響を軽減するプログラム「SHIELDS UP」を開設[4]。
- ○ 2022 年 2 月 28 日、米国政府は、官民連携による取組の一環として、中国に関連する攻撃者が使用していたとされるマルウエア「Daxin」に関する情報を開示[5]。
- ○ 2022 年 3 月 1 日、バイデン大統領は、米国連邦議会の上下両院合同本会議における一般教書演説で、多くの時間を割き、ロシアによるウクライナへの侵攻を批判[6]。

1.1.3 米国サイバースペースソラリウム委員会の最終報告書と同委員会の動向

- ○ サイバースペースソラリウム委員会は、サイバー攻撃から米国を守るための戦略的アプローチに関するコンセンサスを形成するために、2019 会計年度米国国防権限法(NDAA2019)により設立された委員会[7]。
- ○ 2020 年 3 月に公開されたサイバースペースソラリウム委員会による最終報告書では、新しい戦略的アプローチ「階層型サイバー抑止」を提唱[8]。
- ○ 最終報告書には、80 以上の提言が示され、このうち 2021 会計年度米国国防権限法(NDAA2021)に 26 の提言が盛り込まれるなど、米国のサイバーセキュリティ対する態勢に影響[9]。

---

[3] *DHS「DHS Launches First-Ever Cyber Safety Review Board(2022/2/3)」、https://www.dhs.gov/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board (2022/2/15 閲覧)*

[4] *CISA「SHIELDS UP」、https://www.cisa.gov/shields-up (2022/3/1 閲覧)*

[5] *CISA「Broadcom Software Discloses APT Actors Deploying Daxin Malware in Global Espionage Campaign (2022/2/28)」、https://www.cisa.gov/uscert/ncas/current-activity/2022/02/28/broadcom-software-discloses-apt-actors-deploying-daxin-malware (2022/3/15 閲覧)*

[6] *THE WHITE HOUSE「President Biden's State of the Union Address(2022/3/1)」、https://www.whitehouse.gov/state-of-the-union-2022/ (2022/3/14 閲覧)*

[7] *サイバースペースソラリウム委員会(Cyberspace Solarium Commission)は、2019 年度国防権限法に基づき、重大な影響を及ぼすサイバー攻撃からサイバースペースで米国を防衛するための戦略的アプローチについてコンセンサスを得るために設立された。最終報告書は 2020 年 3 月 11 日に公開されたが、2021 年度ウ国防権限法により、報告書の分析及び勧告に関するフィードバックを収集・評価し、勧告の実施を検討するために再認可された。*

[8] *Cyberspace Solarium Commission「Cyberspace Solarium Commission (2020/3)」、https://5kb.d9b.myftpupload.com/wp-content/uploads/2020/03/CSC-Final-Report.pdf (2021/2/22 閲覧)*

[9] *Cyberspace Solarium Commission「Solarium Co-Chairs Welcome 26 Recommendations in 2021 National Defense Authorization Act(2020/12/3)」、https://www.solarium.gov/press-and-news/ndaa-press-release (202*

1.2. 中国

1.2.1 中国輸出管理白書

- ○ 中国は、2021 年 12 月 29 日、初の輸出管理白書を公表[10]。
- ○ 白書は、中国の輸出管理に関する基本的な立場や政策思想を包括的に紹介し、中国の輸出管理に対する国際社会の理解を深めるために発行されたもの。
- ○ 白書の中では、いかなる国や地域も、輸出管理措置を濫用したり、不当な差別的制限を課したりしてはならないと批判。

1.2.2 第 13 期全国人民代表大会第 5 回会議

- ○ 2022 年 3 月 11 日、第 13 期全国人民代表大会第 5 回会議は、2022 年における経済成長率目標を前年比 5.5%前後とする政府活動報告の承認や国防費の増額を盛り込んだ 2022 年予算案等を採択・承認し、閉幕[11]。

1.2.3 中国におけるサイバーセキュリティ関連法

- ○ 2022 年 2 月 15 日、改訂サイバーセキュリティ審査弁法を施行し、100 万人を超える個人情報を保有するインターネットプラットフォーム運営者の情報を所有するインターネット企業が中国国外で上場する際、セキュリティ審査を義務[12]。

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 サイバー空間からみたウクライナ情勢

- ○ ウクライナ政府は、2022 年 1 月以降相次ぎ発生しているサイバー攻撃についてハイブリッド戦の兆候と言及[13]。
- ○ 米国のセキュリティ企業は、ランサムウエアによるハクティビズム活動は新し

1/2/22 閲覧）

[10] *中華人民共和国商務部「中国の輸出管理白書の公表に関する記者の質問に対する商務部担当者の回答(2021/12/30)」、http://exportcontrol.mofcom.gov.cn/article/gndt/202112/588.html（2022/2/22 閲覧）*

[11] *日経新聞「中国、国防費 7.1%増で伸び拡大 台湾統一へ軍備増強(2022/3/5)」、https://www.nikkei.com/article/DGXZQOGM043V70U2A300C2000000/（2022/3/15 閲覧）*

[12] *中华人民共和国国家互联网信息办公室「网络安全审查办法(2022/1/4)」、http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm（2022/3/17 閲覧）*

[13] *Міністерство та Комітет цифрової трансформації України「Росія має намір знизити довіру до влади фейками про вразливість критичної інформаційної інфраструктури та «злив» даних українців(2022/1/16)」、https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv（2022/2/20 閲覧）*

い戦略と評価[14]。

- ○ 2022 年 2 月、ウクライナ国防省等への DDoS 攻撃にロシア政府が関与していると米国、英国政府が声明を発表[15]。
- ○ CISA は、重要インフラ分野を標的とする国外からのインフルエンスオペレーションに対する準備と対策を公表し、事業者へ対応を推奨[16]。

2.1.2 破壊的なサイバー攻撃の概要と緩和策

- ○ 2022 年 2 月 26 日、米国 CISA と FBI は連名で警戒情報「ウクライナの組織を標的とした破壊型マルウエアについて」を公開[17]。
- ○ ウクライナの組織を標的としたサイバー攻撃は、意図せず他国の組織に波及する可能性があることから、警戒を強めるよう注意喚起。
- ○ サイバー攻撃の影響を低減するには、情報を収集し、IT 資産管理やパッチ管理等の緩和策を実施することが重要[18]。

2.1.3 CISA Insight「潜在的な脅威から今すぐ身を守るサイバーセキュリティ対策の実施」の概要

- ○ 2022 年 1 月 18 日、米国 CISA は「潜在的な脅威から今すぐ身を守るサイバーセキュリティ対策の実施」を発表[19]。
- ○ ランサムウエアやデータを破壊するマルウエアによる攻撃が米国の重要インフラやウクライナに対して発生していることから、米国の全ての組織に対応を呼びかけ。
- ○ リスクを減らし、組織の強靭性を高める取組が重要[20]。

---

[14] *SentinelLABS「Hacktivism and State-Sponsored Knock-Offs | Attributing Deceptive Hack-and-Leak Operations(2022/1/27)」、https://www.sentinelone.com/labs/hacktivism-and-state-sponsored-knock-offs-attributing-deceptive-hack-and-leak-operations/（2022/2/20 閲覧）*

[15] *National Cyber Security Centre「UK organisations encouraged to take action in response to current situation in and around Ukraine(2022/1/28)」、https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation（2022/2/20 閲覧）*

[16] *CISA INSIGHTS「Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure(2022/2/18)」、https://www.cisa.gov/news/2022/02/18/cisa-releases-new-insight-help-critical-infrastructure-owners-prepare-and-mitigate（2022/2/20 閲覧）*

[17] *CISA「Destructive Malware Targeting Organizations in Ukraine（2022/2/26)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-057a（2022/3/8 閲覧）*

[18] *Microsoft「Destructive malware targeting Ukrainian organizations(2022/1/15)」、https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/（2022/3/16 閲覧）*

[19] *CISA「Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats(2022/1/18)」、https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf（2022/2/15 閲覧）*

[20] *CISA「PREPARING FOR AND MITIGATING POTENTIAL CYBER THREATS(2021/12/15)」、https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf（2022/5/6 閲覧）*

2.2. その他

2.2.1 攻撃グループ LAPSUS$による多数のサイバー攻撃

- ○ 2021 年 12 月以降、ブラジル保健省、NVIDIA、サムスン電子、Microsoft や Okta など多数の組織が攻撃グループ LAPSUS$からの被害を報告[21]。
- ○ LAPSUS$は、VPN 機器の脆弱性の悪用や、ソーシャルエンジニアリング攻撃等の複数の手法を用いて組織の資産に不正にアクセスし、データを窃取[22]。
- ○ 標的組織の従業員やビジネスパートナーを通じてアクセス情報を入手する事例があり、パッチ管理等のシステムによる対策だけではなく、ソーシャルエンジニアリング攻撃に対する従業員への教育が重要[23]。

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. 政府機関関連

3.1.1 現下の情勢を踏まえた注意喚起

- ○ 昨今の情勢を踏まえたサイバー攻撃事案の潜在的なリスクが高まっていることから、政府は、2022 年 2 月 23 日、3 月 1 日及び 3 月 24 日と注意喚起を発出。
- ○ 2022 年 2 月 23 日、経済産業省は注意喚起を発出し、各企業・団体に対して、経営者のリーダーシップの下、脅威への認識を深め、リスク低減のための措置、インシデントの早期検知及びインシデント発生時の適切な対処・回復を要請[24]。
- ○ 2022 年 3 月 1 日、国内自動車メーカーのサプライチェーンにある部品メーカーがサイバー攻撃の被害にあったことを踏まえ、経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁及び NISC が連名で注意喚起を発出し、政府機関や重要インフラ事業者を始めとする各企業・団体等に対策の強化を要請[25]。
- ○ 2022 年 3 月 24 日、米国バイデン大統領がロシアによるサイバー攻撃へ

---

[21] *Okta「LAPSUS$に関する Okta のステートメント(2022/3/22)」、https://www.okta.com/jp/blog/2022/03/updated-okta-statement-on-lapsus/（2022/5/6 閲覧）*

[22] *Palo Alto Networks「脅威に関する情報: Lapsus$グループ(2022/3/24)」、https://unit42.paloaltonetworks.jp/lapsus-group/（2022/4/20 閲覧）*

[23] *Microsoft「DEV-0537 criminal actor targeting organizations for data exfiltration and destruction(2022/3/22)」、https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/（2022/4/20 閲覧）*

[24] *経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について(注意喚起)(2022/2/23)」、https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf（2022/5/19 閲覧）*

[25] *NISC「サイバーセキュリティ対策の強化について(注意喚起)(2022/3/1)」、https://www.nisc.go.jp/pdf/press/20220301NISC_press.pdf（2022/5/19 閲覧）*

の警戒を呼びかける声明があったこと等を踏まえ、経済産業省、総務省、警察庁及び NISC が連名で注意喚起を発出し、政府機関や重要インフラ事業者を始めとする各企業・団体等に対策の強化を要請[26]。

3.2. 重要インフラ関連

3.2.1 個人情報漏えいに関するインシデントと改正個人情報保護法

- ○ 決済代行業者メタップスペイメントは、クレジットカード会社より不正利用の懸念の連絡を受けてから、「イベントペイ」など一部の機能で停止したが、不正アクセスにより個人情報流出の可能性が高いことが判明し、2022 年 1 月 25 日にクレジット決済サービス「トークン方式」について全停止を発表[27]。
- ○ 2021 年の情報漏えい・紛失の原因は、マルウエア感染・不正アクセスが最も多く、増加傾向[28]。
- ○ 改正個人情報保護法において、個人情報取扱事業者は、個人情報漏えい時に、個人情報保護委員会に報告し、本人通知することが義務化[29]。

3.2.2 海底ケーブルの故障と安全保障上のリスク

- ○ 海底ケーブルは、世界全体で延べ約 120 万 km(地球約 30 周分)の長さが地球を張り巡らされており、国際通信の 99%を収容[30]。
- ○ 海底ケーブルの主な故障原因は漁業活動や自然災害による損傷で、2022 年 1 月 15 日、トンガ諸島の海底火山の噴火の影響を受け、海底ケーブルが損傷、インターネットや国際電話等の国際通信が途絶[31]。
- ○ 海底ケーブル敷設プロジェクト PLNC は、ロサンゼルスと香港を直結する計画であったが、安全保障上の理由から計画変更[32]。
- ○ 中国は巨大経済圏構想「一帯一路」に基づき、各地で海底ケーブルの敷設

---

[26] *NISC「現下の情勢を踏まえたサイバーセキュリティ対策の強化について(注意喚起)(2022/3/24)」、https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf (2022/5/19 閲覧)*

[27] *メタップスペイメント「不正アクセスに関するご報告とお詫び(2022/1/25)」、https://www.metaps-payment.com/company/20220125.html (2022/2/8 閲覧)*

[28] *東京商工リサーチ「上場企業の個人情報漏えい・紛失事故は調査開始以来最多の 137 件 574 万人分(2021/1/17)」、https://www.tsr-net.co.jp/news/analysis/20210117_01.html (2022/2/8 閲覧)*

[29] *個人情報保護委員会「個人情報の保護に関する法律等の一部を改正する法律(概要)」、https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf (2022/2/3 閲覧)*

[30] *KDDI「通信・電力・観測資源探査に対応する「海底ケーブル敷設船」の名称を「KDDI CABLE INFINITY」に決定(2014/8/11)」、https://news.kddi.com/kddi/corporate/newsrelease/2018/02/23/2969.html (2022/2/14 閲覧)*

[31] *日経新聞「トンガ、噴火で海底ケーブル損傷 通信復旧に数週間(2021/1/19)」、https://www.nikkei.com/article/DGKKZO79335260Y2A110C2FF8000/ (2022/2/14 閲覧)*

[32] *U.S. Department of Justice「Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States (2020/6/17)」、https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea (2022/2/27 閲覧)*

を活発化させ、華海通信技術が世界 4 位とシェアを拡大[33]。

○ 日本では、「デジタル田園都市国家構想」の一環として、日本海側の国内海底ケーブルの新規敷設などを支援する方針[34]。

3.3. その他

3.3.1 マルウエア「Emotet」の攻撃活動の急拡大

○ 2021 年 11 月に再開したマルウエア「Emotet」の攻撃活動が、2022 年 2 月以降大幅に拡大[35]。

○ 2022 年 3 月 2 日、世界中で使用されているトップレベルドメインである「.com」を超えて、「.jp」が世界一の Emotet の攻撃メールの送信元[36]。

○ Emotet 対策の取組の一環として、PPAP の廃止が進んでいるが、未だに 5 割超の企業が継続利用[37]。

3.3.2 工場稼働等へ影響を与えるランサムウエア攻撃

○ 2022 年 3 月 1 日、小島プレス工業におけるシステム障害の影響を受け、トヨタ自動車は国内全工場を稼働停止[38]。

○ 2022 年 3 月、半導体関連の GlobalWafers Japan、自動車関連の GMB やデンソー、ブリヂストン、三桜工業の海外子会社等、産業界の企業が相次いで被害を公表[39]。

○ セキュリティ企業 Dragos のレポートによると、2021 年に産業インフラへの攻撃が急増し、ランサムウエアグループ LockBit と Conti による活動が顕著[40]。

以上

---

[33] *読売新聞「【独自】海底ケーブル敷設、日米豪が連携…急速に台頭する中国に対抗(2021/4/19)」、https://www.yomiuri.co.jp/economy/20210418-OYT1T50206/（2022/2/23 閲覧）*

[34] *経済産業省・総務省「デジタルインフラ(DC 等)整備に関する有識者会合 中間とりまとめ(概要)(2022/1/17)」、https://www.meti.go.jp/press/2021/01/20220117001/20220117001-2.pdf（2022/2/23 閲覧）*

[35] *JPCERT/CC「マルウェア Emotet の感染再拡大に関する注意喚起(2022/4/26)」、https://www.jpcert.or.jp/at/2022/at220006.html（2022/5/16 閲覧）*

[36] *TG Soft「TG Soft(@VirITeXplorer)の投稿(2022/3/4)」、https://twitter.com/VirITeXplorer/status/1499409017587785736（2022/3/23 閲覧）*

[37] *日本情報経済社会推進協会「コロナ禍の長期化に伴い、企業の 72.7%がテレワークを実施 電子契約の利用企業は 69.7%に拡大 ―JIPDEC と ITR が『企業 IT 利活用動向調査 2022』の速報結果を発表―(2022/3/17)」、https://www.jipdec.or.jp/topics/news/20220317.html（2022/3/22 閲覧）*

[38] *トヨタ自動車「3/2（水）以降の国内工場における稼働再開について(2022/3//1)」、https://global.toyota/jp/newsroom/corporate/36964714.html（2022/4/12 閲覧）*

[39] *日経 xTECH「部品メーカーが次々に被害、自動車業界とサプライチェーンを狙うランサムウエア(2022/5/6)」、https://active.nikkeibp.co.jp/atcl/act/19/00324/042000007/（2022/5/6 閲覧）*

[40] *Dragos「2021 ICS CYBERSECURITY YEAR IN REVIEW」、https://www.dragos.com/year-in-review/（2022/4/12 閲覧）*

重要インフラにおける情報共有件数について(2021 年度)

「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	FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
重要インフラ事業者等からNISCへの情報連絡(※)	388	223	269	309	109	79	95	124	407
関係省庁・関係機関からのNISCへの情報共有	19	7	16	16	4	1	1	0	6
NISCからの情報提供	54	43	38	64	17	24	28	22	91

（※）重要インフラ事業者等からNISCへの情報連絡は以下のとおり。

1.事象別内訳

事象の類型			FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
未発生の事象		予兆・ヒヤリハット	80	27	12	28	5	2	4	14	25
発生した事象	機密性を脅かす事象	情報の漏えい	15	13	13	23	11	5	2	11	29
	完全性を脅かす事象	情報の破壊	20	17	11	12	4	7	5	4	20
	可用性を脅かす事象	システム等の利用困難	143	97	158	157	62	41	41	37	181
	上記につながる事象	マルウェア等の感染	65	17	9	18	6	7	4	29	46
		不正コード等の実行	13	4	5	3	0	0	2	0	2
		システム等への侵入	17	14	14	26	5	8	7	4	24
		その他	35	34	47	42	16	9	30	25	80

2.原因別類型（複数選択）

原因の類型		FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
意図的な原因	不審メール等の受信	89	36	13	9	3	0	4	40	47
	ユーザＩＤ等の偽り	4	3	12	9	3	0	2	2	7
	DDoS攻撃等の大量アクセス	31	17	20	10	3	4	1	11	19
	情報の不正取得	16	10	8	13	5	0	3	5	13
	内部不正	4	1	0	0	0	1	0	0	1
	適切なシステム等運用の未実施	15	14	11	23	4	3	3	5	15
偶発的な原因	ユーザの操作ミス	23	10	6	18	5	1	1	3	10
	ユーザの管理ミス	13	6	6	13	5	2	2	5	14
	不審なファイルの実行	42	16	7	7	1	0	3	18	22
	不審なサイトの閲覧	20	4	5	3	2	0	0	4	6
	外部委託先の管理ミス	41	29	39	56	25	29	31	22	107
	機器等の故障	32	27	62	39	11	6	15	6	38
	システムの脆弱性	36	19	16	38	5	7	16	4	32
	他分野の障害からの波及	10	6	4	7	4	2	3	1	10
環境的な原因	災害や疾病等	0	1	13	9	0	3	0	0	3
その他の原因	その他	29	29	33	35	21	4	13	10	48
	不明	57	46	53	68	23	25	10	21	79

（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(2021 年度第 4 四半期)

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

○　管理不良による障害発生低減のため経営層を含めた組織全体の対応が必要

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が依然として発生している。なお、サイバー攻撃は、適切な管理により防げたものが多くあった。

管理不良による障害発生を低減させるためには大局を俯瞰した上でのリスクの明確化や対応策の検討等、経営層及び戦略マネジメント層を含めた組織全体での多層的な対応が求められる。

○　ネット接続に係る資産管理及びバックアップの重要性の再認識が必要

ランサムウエア感染により、データが暗号化され、長時間にわたりサービスを提供できなかった事例が多数あった。

VPN の重要性の再認識と海外拠点等セキュリティ対策が弱い拠点から侵入されることがあることに留意する必要がある。また、業務委託先のランサムウエア感染により、自組織の業務停止や同先に格納される自組織のデータが被害に遭うことがあることに留意する必要がある。なお、暗号化に加え機密情報を公開すると身代金を要求されることがある(二重脅迫型)。

○　攻撃傾向の把握と対策の技術的有効性にかかる継続的な評価が必要

マルウエア Emotet 感染により、個人情報が流出し、自組織を騙る不審メールに利用される事例が多数あった。また感染事実が確認されないものの自組織を騙る不審メールが確認された事例が多数あった。

○　情報漏えいを念頭に置いた対策の検討が必要

外部サービスを提供する組織が不正アクセスを受け、個人情報が流出し、サービスを利用する複数の組織に影響が及ぶ事例があった。

○　リスクに応じた外部サービスの利用が必要

外部サービスを提供する組織が第三者によりスパムメール送信の踏み台に利用された事例が多数あった。そのうち、一部ではブラックリストに登録され、正規のメール送信に支障が生じた事例があった。

○　サプライチェーン管理の徹底が必要

利用する外部サービスの停止によりシステムに不具合が発生し、長時間にわたりサービスが提供できなかった事例があった。

以上