資料９

令和２年７月 13 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(2019 年度第 3 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、2019 年度第 3 四半期(10 月～12 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

- 米国は、インド太平洋戦略に基づき、共産党一党独裁下にある中国の産業構造の変化を求め、2019 年 10 月、ペンス副大統領は前年に続く対中制裁の演説を実施し、経済問題の他、人権問題や香港情勢に関しても言及[1]。
- 中国共産党は、2019 年 10 月、第 19 期中央委員会第 4 回全体会議(四中全会)を開催、香港問題への関与強化に重点を置く方針を発表[2]。
- 新疆ウイグル自治区において、中国政府による人権弾圧の実態が記された内部文書が流出する事態が発生[3]。
- 2019 年 12 月、世界アンチ・ドーピング機構(WADA)はロシアの五輪参加排除を決定、これによりロシアから日本へのサイバー攻撃の可能性が上昇[4]。
- 2020 年 1 月、イラン革命防衛隊スレイマニ司令官が米軍によって殺害されたことを受け、イランは米軍基地にミサイル攻撃を実施したが、両国とも戦争を望まないことから事態は収束傾向[5]。

---

[1] *日本経済新聞「ペンス米副大統領、中国は「検閲まで輸出」 演説概要 (2019/10/25)」、https://www.nikkei.com/article/DGXMZ O51377650V21C19A0FF8000/ (2019/11/21 閲覧)*

[2] *日本総研「異例の展開となった中国の四中全会(2019/11/12)」、https://www.jri.co.jp/MediaLibrary/file/report/researchfocus/pdf/11408.pdf (2020/2/6 閲覧)*

[3] *BBC「中国政府、ウイグル人を収容所で「洗脳」 公文書が流出(2019/11/25)」、https://www.bbc.com/japanese/50542004(2019/12/16 閲覧)*

[4] *ITmedia「日本が狙われる ロシアのドーピング処分で暴れる「クマさん」の危険(2019/12/12)」、https://www.itmedia.co.jp/busi ness/articles/1912/12/news024.html(2020/1/30 閲覧)*

[5] *FNN PRIME「米・イランの"エスカレーション・コントロール"が大規模戦争を回避した 日本の安全保障への教訓(2020/1/23)」、https://www.fnn.jp/posts/00049900HDK/202001231140_MasashiMurano_HDK(2020/1/23 閲覧)*

1.2 米国

1.2.1 新たな 5G 開発投資政策

- ○ 中国政府は一帯一路の下、5G 分野で巨額の輸出支援を行い、海外開発投資においてファーウェイ社等の中国企業を支援[6]。
- ○ 米国は一帯一路に対抗し、信頼できる西側企業を支援すべく投資認証の枠組を構築し、認証の枠組を国際的に展開する方針を公表[7]。
- ○ 欧州連合(EU)も中国製品が一部の強権主義国に悪用され、民主主義が脅かされる意識が高まり、一帯一路への警戒感を強め、日本とインド太平洋地域等におけるデジタル・インフラ投資での協力に関する合意書に署名し、協力して対抗する姿勢を表明[8]。

1.2.2 DHS Hunt and Incident Response Teams 法の可決[9]

- ○ 2016 年 1 月、国土安全保障省(DHS)国家サイバーセキュリティ通信統合センター(NCCIC)は、脅威の事前での特定・分析、及びインシデントレスポンスを担当する組織として Hunt and Incident Response Team(HIRT)を設置。
- ○ HIRT は設置に際して根拠法がなく、これまで正式な権限、任務がない状態が継続。
- ○ 2019 年 12 月 20 日、DHS Cyber Hunt and Incident Response Teams Act of 2019 が 2020 会計年度米国歳出法の一部として成立し、HIRT は正式に NCCIC 配下の組織として発足。

1.3 シンガポール

1.3.1 シンガポールの OT サイバーセキュリティマスタープラン[10]

- ○ CSA シンガポール(Cyber Security Agency of Singapore)は、OT(Operational Technology)サイバーセキュリティマスタープランを発行。
- ○ マスタープランは、サイバー脅威の軽減のための横断的な対応の改善、利害関係者とのパートナーシップの強化により重要インフラのセキュリティと回復力を強化することを目的。
- ○ OT と IT の違いに着目し、教育、情報共有、ポリシーとプロセスの強化、技術開発の 4 つの強化策を提示。

---

[6] *WSJ「ファーウェイ、台頭の裏に政府支援 8 兆円超(2019/12/27)」、https://jp.wsj.com/articles/SB11116437583125473536504586101500165500090 (2020/1/15 閲覧)*

[7] *Bloomberg「U.S. to Tap $60 Billion War Chest in Boon for Huawei Rivals(2019/12/3)」、https://www.bloomberg.com/news/articles/2019-12-03/u-s-to-tap-60-billion-war-chest-in-boon-for-huawei-rivals (2020/1/5 閲覧)*

[8] *産経新聞「米、インド太平洋地域でインフラ支援強化 日豪と基準策定へ(2019/11/11)」、https://www.sankei.com/world/news/191111/wor1911110006-n1.html (2020/1/15 閲覧)*

[9] *米国議会「Consolidated Appropriations Act, 2020(2019/12/20)」、https://www.congress.gov/bill/116th-congress/house-bill/1158 (2020/1/20 閲覧)*

[10] *CSA シンガポール「Singapore's Operational Technology Cybersecurity Masterplan 2019(2019/10/1)」、https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan (2019/11/21 閲覧)*

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 重要インフラ関連

2.1.1 英国の金融分野におけるサイバーシミュレーション演習[11]

- ○ イングランド銀行が金融当局と連携し、2018 年 11 月 18 日に金融分野におけるサイバーシミュレーション演習を実施。
- ○ 同行は演習に対する調査結果を 2019 年 9 月 27 日に公表。
- ○ 調査結果では、運用レベルでの調整、サービス中断に対するリスク許容度の不一致、データ保存方法の違い、コミュニケーションの重要性を指摘。

2.1.2 米国電力網へのサイバー攻撃[12]

- ○ 2019 年 9 月、北米電力信頼度協会(NERC)は、米国電力網に対するサイバー攻撃について公表。
- ○ 攻撃は、ファイアウォールの管理機能の脆弱性を利用しサービス不能状態にするもの。
- ○ 攻撃によりコントロールセンターと発電所間で 5 分以内の通信断が発生したが送電網は影響なし。
- ○ NERC は電力システムの信頼性維持を目的に、この攻撃に関する教訓事項を公表。

2.2 その他

2.2.1 サービス開始時を狙ったアカウントハッキング

- ○ 2019 年、サービス開始時を狙ったアカウントハッキングが複数発生。
- ○ 動画配信サービス Disney+では、サービス開始直後からハッキングされたアカウントがダークウェブ上で売買[13]。
- ○ QR コード決済セブンペイでは、サービス開始直後からハッキングされたアカウントでの不正利用が発生[14]。

---

[11] *イングランド銀行「Bank of England sector resilience exercise(2019/9/27)」、https://www.bankofengland.co.uk/news/2019/september/boe-sector-resilience-exercise (2019/11/20 閲覧)*

[12] *NERC「Lesson Learned Risks Posed by Firewall Firmware Vulnerabilities(2019/9/4)」、https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf (2019/12/17 閲覧)*

[13] *BBC「「ディズニー+」の利用者情報が盗まれ売買に 数千人分(2019/11/19)」、https://www.bbc.com/japanese/50469833 (2019/11/27 閲覧)*

[14] *セブン＆アイ・ホールディングス「「7pay(セブンペイ)」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について(2019/8/1)」、https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf (2019/8/5 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 政府機関関連

3.1.1 日米デジタル貿易協定[15]

- ○ 2019 年 10 月 7 日、日本と米国との間で、円滑で信頼性の高い自由なデジタル貿易を促進するための法的基盤を確立することを目的として、日米デジタル貿易協定を締結。
- ○ デジタル貿易とは、インターネットを利用した国境を越える情報やサービスの取引のことであり、例として音楽や映像などのコンテンツ配信、電子商取引が存在。
- ○ 日米デジタル貿易協定は、データ保管を当該国内に求めるデータローカライゼーションの禁止や、SNS 等のプラットフォーム上でやりとりされた情報により発生した損害への責任を事業者に問わない免責事項を規定。

3.2 重要インフラ関連

3.2.1 台風 19 号に関連する自然災害時における情報発信

- ○ 台風 19 号の際に複数の自治体のウェブサイトでアクセス集中による障害が発生[16]。
- ○ アクセス集中に対応する CDN(Content Delivery Network)を導入している地方自治体は、J-Stream 社の調査によると、約 7%[17]。
- ○ ウェブサイトの補完としての SNS の活用などを含めた情報発信のための対策が必要[18]。

3.2.2 国内のデータセンター障害と波及して発生したサービス障害[19,20]

- ○ 2019 年 11 月、データセンターにおける障害が相次いで 2 社で発生。
- ○ 原因は、両社ともセンター内の電気機器に係る工事の不手際によるサーバー電源停止。
- ○ この障害により、データセンター利用者のサービス提供にも大きな影響。

---

[15] *外務省「デジタル貿易に関する日本国とアメリカ合衆国との間の協定(2019/12/18)」、https://www.mofa.go.jp/mofaj/ila/et/page3_002912.html（2020/1/21 閲覧）*

[16] *NHK「自治体のホームページが…(2019/11/6)」、https://www.nhk.or.jp/ohayou/digest/2019/11/1106.html（2019/11/18 閲覧）*

[17] *J-Stream CDN 情報サイト「国内 CDN シェア(2019 年 4 月)(2019/4/25)」、https://tech.jstream.jp/blog/cdn/cdn-share-apl2019/（2019/11/15 閲覧）*

[18] *内閣官房 情報通信技術(IT)総合戦略室「災害対応における SNS 活用ガイドブック(2016 年 3 月)」、https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/pdf/h2903guidebook.pdf（2019/11/19 閲覧）*

[19] *QTnet「データセンターの電源障害による停止について(障害お知らせ 第 12 報 11/26 10 時現在)(2019/11/26)」、https://www.qtnet.co.jp/info/2019/20191126.html（2019/12/16 閲覧）*

[20] *エヌ・ティ・ティ・コミュニケーションズ「岐阜県内の弊社データセンターにて発生した電源故障について(2019/11/28)」、https://www.ntt.com/about-us/nw-condition/2019/1128.html（2019/12/16 閲覧）*

3.2.3 神奈川県庁の廃棄 HDD からのデータ流出事案[21]

- ○ 神奈川県庁がリース契約をしていた HDD の情報が流出。
- ○ 神奈川県で使用していた HDD は、リース元の企業が契約していたデータ破壊を行う企業の従業員が盗み、ネットオークションに出品。
- ○ HDD 購入者がデータ復旧ソフトを使用したところ、神奈川県のデータ流出があったことから判明。

3.2.4 自治体向けクラウドサービスで発生した障害[22]

- ○ 2019 年 12 月 4 日、自治体向けクラウドサービスに障害が発生。
- ○ 根本原因はストレージ中のファームウエアの不具合。
- ○ ファームウエアのアップデートによりストレージの物理的回復はできたが、ストレージへのアクセス不可やバックアップミス等により、サービス支障は長期化。

3.3 その他

3.3.1 2019 年 10 月 1 日の消費税率変更に伴うシステムトラブル

- ○ 消費税率変更により、国民生活に影響するシステムトラブルが発生[23]。
- ○ システムトラブルが発生した事業者等は対応に努め、政府機関関係には大きなトラブルはなし[24]。

3.3.2 マルウエア「Emotet」の流行

- ○ 2018 年 10 月に確認された感染端末に保存されたメールの件名と本文を窃取する機能の追加を契機にマルウエア「Emotet」の感染が全世界的に拡大[25]。
- ○ 日本国内でも「Emotet」の感染が発生[26]。
- ○ 感染端末から窃取したメールを悪用し、感染端末の利用者になりすます手口で「Emotet」が感染を拡大していたことから、US-CERT やオーストラリアサイバーセキュリティセンター(ACSC)が注意喚起を発出。

---

[21] *朝日新聞「【独自】行政文書が大量流出　納税記録などのHDD転売」、https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html（2020/1/20 閲覧）*

[22] *日本電子計算「「Jip-Base」の障害における復旧状況のご報告(2019/12/16)」、https://www.jip.co.jp/news/20191216/、https://www.jip.co.jp/news/pdf/20191216.pdf(2020/1/20 閲覧)*

[23] *piyolog「増税に伴うシステムトラブルをまとめてみた(2019/10/2)」、https://piyolog.hatenadiary.jp/entry/2019/10/02/063748（2019/11/1 閲覧）*

[24] *朝日新聞「消費増税、還元制度が開始 政府「大きなトラブル無し」(2019/10/1)」、https://www.asahi.com/articles/ASMB152SJMB1ULFA022.html（2019/11/14 閲覧）*

[25] *US-CERT「ACSC Releases Advisory on Emotet Malware Campaign(2019/10/29)」、https://www.us-cert.gov/ncas/current-activity/2019/10/25/acsc-releases-advisory-emotet-malware-campaign（2019/11/22 閲覧）*

[26] *公益財団法人東京都保健医療公社「公益財団法人東京都保健医療公社が運用する端末等に対する不正アクセス被害の発生による、メールアドレス等の個人情報の流出と対応について（第二報）」、https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2019/06/07/06.html（2020/6/9 閲覧）*

3.3.3 Windows の深刻な脆弱性「BlueKeep」を悪用した攻撃の発生

- Windows のリモートデスクトップサービスに存在する深刻な脆弱性として、2019 年 5 月に脆弱性 CVE-2019-0708[通称:「BlueKeep」][27]が、2019 年 8 月に脆弱性 CVE-2019-1181 及び CVE-2019-1182[通称:「DejaBlue」][28]が公開。
- 2019 年 9 月にペネトレーションツール「Metasploit Framework」で、「BlueKeep」を再現したコードが使用可能となったことを契機に、「BlueKeep」を悪用した攻撃が発生[29]。
- 攻撃の発生を受け、2019 年 11 月に Microsoft 社がパッチ適用状況の確認と迅速なパッチ適用を呼びかける注意喚起を実施。

3.3.4 「Office365」環境を狙った新たなフィッシング攻撃[30]

- 米国 PhishLabs 社は、Microsoft 社のクラウドサービス「Office365」に対する新たなフィッシング攻撃手法を報告。
- 攻撃者は、ユーザーから窃取したアクセストークンを使うことで、「Office365」に対する不正アクセスを実施。
- 従来のフィッシング攻撃に対する対処策・対策が通用しないため、攻撃の手口を正確に把握した上で、本攻撃に対する対処策・対策を確実に実施することが必要。

以上

---

[27] *Microsoft「CVE-2019-0708 | リモートデスクトップサービスのリモートでコードが実行される脆弱性(2019/5/14)」、https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708 (2019/12/10 閲覧)*

[28] *Microsoft「Patch new wormable vulnerabilities in Remote Desktop Services(CVE-2019-1181/1182) (2019/8/13)」、https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/ (2020/6/12 閲覧)*

[29] *Microsoft「Microsoft works with researchers to detect and protect against new RDP exploits(2019/11/7)」、https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/ (2019/12/10 閲覧)*

[30] *PhishLabs「Phishing Campaign Uses Malicious Office 365 App(2019/12/9)」、https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset (2020/1/17 閲覧)*

サイバーセキュリティを取り巻く情勢(2019 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、2019 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。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 5G に関する国際動向

- ○ 米国は、国家安全保障上の懸念からファーウェイ社製品の使用を米国内で禁じるとともに、欧州をはじめとする同盟国に対しても使用しないよう働きかけを進めている[1]。
- ○ 一方、このような米国の働きかけに対し、2020 年 1 月、EU は、原則として各加盟国に対応を任せるとの姿勢を表明したほか、米国の重要な同盟国である英国は、ファーウェイ社を 5G 調達から完全には排除しないことを表明[2]。
- ○ EU の主要 2 大国においては、ドイツは政府内で意見がまとまらず、明確な方針を出していない一方、フランスは特定企業の排除はしないと公表し、一貫して中立的な立場を維持。

1.2 米国

1.2.1 5G サプライチェーンの取組[3]

- ○ 米国は、これまで、ファーウェイをはじめとする中国系通信機器ベンダー5 社の排除のための法律の施行準備や、国内の地方中小通信事業者に対する経済的支援策としての補助金制度の創設など取組を推進。また、国防総省

---

[1] *米国商務省産業安全保障局「Supplement No. 4 to Part 744 - ENTITY LIST(2019/5/15)」、https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file (2020/2/13 閲覧)*

[2] *英国政府「New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity(2020/1/28)」、https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity (2020/2/18 閲覧)*

[3] *現代ビジネス「「5G ファーウェイ排除」をめぐり欧州と米国の分断が始まった(2020/2/21)」https://gendai.ismedia.jp/articles/-/70545 (2020/3/12 閲覧)*

のサプライチェーン強化を目的とした認証制度 CMMC(Cybersecurity Maturity Model Certification: CMMC)を構築。

1.2.2 サイバーセキュリティ成熟度モデル認証(CMMC)[4]

- 2019 年から、米国国防総省(DoD)は、調達先の情報の保護に重きを置いたサプライチェーンマネジメントのセキュリティ強化を目的とした認証制度である「サイバーセキュリティ成熟度モデル認証」の構築について検討を開始。
- これは DoD が制度化したものであり、DoD の調達先を具体的に評価する第三者審査機関(C3PAO: Certified Third-Party Assessment Organizations)の認定を CMMC AB (Accreditation Body)が行うもの。
- CMMC 認証は、DoD の調達先組織のサイバーセキュリティの成熟度を仕組みの構築状況(Process)及び活動状況(Practice)の 2 つの側面から 5 段階のレベルで評価。

1.2.3 国土安全保障省(DHS)指令案(脆弱性公表ポリシーの作成義務付け)公表[5]

- 2019 年 11 月、米国国土安全保障省(DHS)のサイバーセキュリティ・インフラセキュリティ庁(CISA)は、連邦政府機関全てに対して、セキュリティ脆弱性情報の取り扱いに関するポリシーの作成を義務付ける指令案を公表。
- さらに、同年 12 月には、CISA は、政府共通の脆弱性公開プラットフォームに関する市場調査を開始。

1.2.4 エネルギー省の政策[6]

- 2020 年 2 月 10 日、米国行政管理予算局(OMB)が予算教書を公表し、2021 会計年度の米国連邦政府の予算要求が判明。
- エネルギー省全体では減額となる中、サイバーセキュリティ関連機関の予算は軒並み増額となり、ホワイトハウスはエネルギー分野のセキュリティを重視する方針。
- さらに 2020 年 2 月 27 日に上院に提出されたエネルギー改革法案は、電力事業者のサイバーセキュリティにインセンティブを与える新たなプログラムを規定するほか、これまで石油・ガスに依存していた米国のエネルギー源を多様化するべく原子力発電を近代化。

---

[4] *米国国防総省「Cybersecurity Maturity Model Certification(CMMC) Version 1.02(2020/3/18)」、https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf (2020/3/26 閲覧)*

[5] *米国国土安全保障省「Develop and Publish a Vulnerability Disclosure(2019/11/27)」、https://cyber.dhs.gov/bod/20-01/ (2020/2/12 閲覧)*

[6] *米国上院エネルギー・天然資源委員会「S. 2657 AMERICAN ENERGY INNOVATION ACT (AEIA)(2020/2/29)」、https://www.energy.senate.gov/public/index.cfm?a=files.serve&File_id=09AF16B7-1920-4C22-96E2-26039A24B55D (2020/3/17 閲覧)*

1.3 中国

1.3.1 中国による「New IP」の提案

- ○ 中国情報通信省とファーウェイ社が、「New IP」と呼ばれる先端技術活用を可能とするインターネットのプロトコルを国際電気通信連合(ITU-T)に提案[7]。
- ○ 「New IP」は、従来の IP プロトコルが持つ欠点を改善し、低遅延、広帯域で、信頼されるネットワークを提供するとしているが、政府による規制・統制・検閲が強化されるものとして、IETF(Internet Engineering Task Force)など各方面から批判[8]。
- ○ 経済と技術の能力向上により、中国が世界的な基準や標準の策定に影響。

1.3.2 新型コロナウイルス感染症をめぐる米中対立

- ○ 新型コロナウイルス感染症が世界中で猛威をふるう中、中国は感染の拡大を隠蔽し、サプライヤーとしての優位性を利用して、マスク等の医療物資の支援を通じた各国への外交を展開[9]。
- ○ 他方で自国に批判的な米国に対しては情報戦を仕掛け、さらに海洋覇権の拡大のための行動を継続[10]。
- ○ 米国、欧州は中国への批判を強め、中国の責任を問う動きが拡大[11]。

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 重要インフラ関連

2.1.1 電力網へのサイバー攻撃に対する抑止～2 つのアプローチ～[12]

- ○ 米国 RAND 研究所は、米国国防総省における電力網に対するサイバー攻撃への対応を検討する場合の抑止オプションに関する調査レポートを公表。
- ○ 電力網の強靭性と信頼性の向上による「拒否的抑止」(Deterrence by Denial)とサイバー攻撃に対する報復の脅威による「懲罰的抑止」(Deterrence by Cost Imposition)の 2 つのアプローチについて提示。

---

[7] *Future Networks Team, Huawei Technologies, USA「Internet 2030-Towards a New Internet for the Year 2030 and Beyond(2018/07/18)」、https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Documents/Internet_2030%20.pdf（2020/4/8 閲覧）*

[8] *Financial Times「China and Huawei propose reinvention of the internet(2020/3/28)」、https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2（2020/4/8 閲覧）*

[9] *JBpress「世界の苦悶をよそに海洋覇権の拡張を図る中国の蛮行(2020/3/26)」、https://jbpress.ismedia.jp/articles/-/59874（2020/4/7 閲覧）*

[10] *Global Times「COVID-19 blunders signal end of 'American Century'(2020/3/30)」、https://www.globaltimes.cn/content/1184201.shtml（2020/4/7 閲覧）*

[11] *Business Insider「Boris Johnson's government is furious with China and believes it could have 40 times the number of coronavirus cases it says(2020/3/29)」、https://www.businessinsider.com/coronavirus-boris-johnsons-government-reportedly-furious-with-china-2020-3（2020/4/7 閲覧）*

[12] *米国ランド研究所「Deterring Attacks Against the Power Grid Two Approaches for the U.S. Department of Defense(2020/1)」,https://www.rand.org/pubs/research_reports/RR3187.html(2020/3/27 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 九州電力の送配電部門分社化に伴うシステム障害[13]

- ○ 改正電気事業法に基づき、大手電力各社が 2020 年 4 月に送配電部門の分社化を迫られる中、九州電力において 2020 年 1 月に電気料金計算に関連するシステム障害が発生。
- ○ 九州電力は影響範囲の拡大及び収束時期のずれ込みを数回にわたり公表し、システム障害の原因については、プログラム誤りとデータ不備であったと表明。
- ○ 背景に開発マネジメントとリスク見積の不足があった旨を自ら公表しているが、経営層の関与不足との指摘もあり。

3.2 その他

3.2.1 コインハイブ事件の逆転有罪[14]

- ○ 2020 年 2 月 7 日、東京高等裁判所(控訴審)は、「コインハイブ事件」について原審を破棄し、逆転有罪と判断。
- ○ 本件は、被告が自身のウェブサイト上に他人のパソコンを使って仮想通貨をマイニングするプログラム「コインハイブ(Coinhive)」を保管したとして不正指令電磁記録保管の罪に問われていたもの。
- ○ 本判決に対しては、実害の程度やイノベーション阻害への懸念から批判的な意見も相次いでいる。

3.2.2 新型コロナウイルス感染症に関連したサイバー空間の動向

- ○ 2020 年 3 月、新型コロナウイルス感染症(COVID-19)が世界中で流行。
- ○ 新型コロナウイルスの流行に伴い、サイバー空間においても偽サイトを利用した個人情報の窃取、DDoS 攻撃、インターネットトラフィック増加等の影響が発生[15]。
- ○ 外出自粛要請の影響で在宅勤務を採用する企業が増加したことを受け、テレワークに関する様々な課題が顕在化[16]。

---

[13] *九州電力「託送料金計算システムの障害に伴う自社需要家に対する電気料金 請求書送付遅延及び小売電気事業者への誤請求等について(報告)(2020/2/6)」、http://www.kyuden.co.jp/var/rev0/0231/1557/kew334s0.pdf (2020/4/10 閲覧)*

[14] *Abema TIMES「コインハイブ事件、高裁の"逆転"判決に危機感・・・自民・山田太郎議員「日本だけが遅れていく。刑法の条文の再検討が必要」(2020/2/12)」、https://times.abema.tv/posts/7041157 (2020/3/9 閲覧)*

[15] *トレンドマイクロ「日本と海外の「新型コロナウイルス」便乗脅威事例(2020/3/13)」、https://blog.trendmicro.co.jp/archives/24147 (2020/4/17 閲覧)*

[16] *内閣サイバーセキュリティセンター「テレワークを実施する際にセキュリティ上留意すべき点について (2020/4/14)」、https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf (2020/6/12 閲覧)*

3.2.3 新型コロナウイルス感染症の流行に伴うテレワークの普及

- ○ 2020 年 2 月 25 日、新型コロナウイルス感染症の対応として、新型コロナウイルス感染症対策本部は「新型コロナウイルス感染症対策の基本方針」を発表[17]。
- ○ 同方針の発表を契機に、重要インフラ分野をはじめとする多くの組織でテレワークの積極的な導入が加速[18]。
- ○ 事業継続の観点から、テレワークの実施に向けた社内ルール整備やテレワークを円滑に実施するための ICT 環境準備が必要。

3.2.4 相次ぐ深刻な脆弱性情報の公開

- ○ 2020 年 3 月に、Microsoft 社は SMBv3 に関する深刻な脆弱性 CVE-2020-0796[通称: SMBGhost][19]を、トレンドマイクロ社は同社製品に関する深刻な脆弱性[20]を公開。
- ○ 「SMBGhost」は、リモートから任意のコードの実行が可能な脆弱性として、US-CERT 等がセキュリティ更新プログラムの適用を呼びかける注意喚起を実施[21]。
- ○ トレンドマイクロ社製品の複数の脆弱性については、同社が既に一部の脆弱性を悪用する攻撃を確認していることを公表。

3.2.5 Windows CryptoAPI の深刻な脆弱性「Curveball」

- ○ 2020 年 1 月に、Microsoft 社は Windows CryptoAPI(Crypt32.dll)の深刻な脆弱性 CVE-2020-0601[通称:Curveball]を公開[22]。
- ○ 「Curveball」は米国国家安全保障局(NSA)が発見した脆弱性であり、NSA や Microsoft 社が迅速なパッチ適用を呼びかける注意喚起を実施[23]。

---

[17] *新型コロナウイルス感染症対策本部「新型コロナウイルス感染症対策の基本方針（2020/2/25)」https://www.kantei.go.jp/jp/singi/novel_coronavirus/th_siryou/kihonhousin.pdf（2020/6/11 閲覧）*

[18] *NHK「NTT 従業員約 20 万人にテレワーク・時差出勤を呼びかけへ（2020/2/17)」、https://www1.nhk.or.jp/news/html/20200217/k10012288351000.html（2020/6/11 閲覧）*

[19] *Microsoft「CVE-2020-0796|Windows SMBv3 クライアント/サーバーのリモートでコードが実行される脆弱性(2020/3/13)」、https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-0796（2020/4/8 閲覧）*

[20] *トレンドマイクロ「アラート/アドバイザリ: Apex One とウイルスバスターコーポレートエディションで確認された深刻度の高い複数の脆弱性について(2020/3/16)」、https://success.trendmicro.com/jp/solution/000244253（2020/4/9 閲覧）*

[21] *US-CERT「Microsoft Releases Out-of-Band Security Updates for SMB RCE Vulnerability(2020/3/13)」、https://www.us-cert.gov/ncas/current-activity/2020/03/12/microsoft-releases-out-band-security-updates-smb-rce-vulnerability（2020/4/8 閲覧）*

[22] *Microsoft「CVE-2020-0601 | Windows CryptoAPI のなりすましの脆弱性(2020/1/14)」、https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-0601（2020/2/12 閲覧）*

[23] *National Security Agency「Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers(2020/1/14)」、https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.pdf（2020/2/12 閲覧）*

3.2.6 機密情報を暴露するランサムウエア

- ○ 2019 年 10 月～12 月において、ランサムウエアの被害を受けた組織の平均復旧日数、平均身代金要求額はともに増加しており、米国を中心に深刻な被害が発生[24]。
- ○ 2019 年 12 月頃から、攻撃者が身代金を得るための新たな手段として、複数のランサムウエアが感染端末上の機密情報を暴露する手口を採用[25]。

3.2.7 防衛関連企業で相次ぐ不正アクセス[26]

- ○ 三菱電機社は、不正アクセスを受け、個人情報や企業機密が外部に流出した可能性があると発表。
- ○ 流出した可能性のある情報に、防衛省の「注意情報」が含まれていたと判明。
- ○ NEC 社、神戸製鋼所、パスコ社も相次いで不正アクセスを受けていたと公表。

以上

---

[24] *Coveware「Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate(2020/1/23)」、https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate（2020/2/4 閲覧）*

[25] *CYWARE「Maze ransomware operators once again take to the internet to publish a list of victim organizations(2020/1/13)」、https://cyware.com/news/maze-ransomware-operators-once-again-take-to-the-internet-to-publish-a-list-of-victim-organizations-916f3a49（2020/2/3 閲覧）*

[26] *三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について(第 2 報)(2020/2/10)」、http://www.mitsubishielectric.co.jp/news/2020/0210-b.pdf（2020/2/12 閲覧）*

重要インフラにおける情報共有件数について（2019 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	FY2015 計	FY2016 計	FY2017 計	FY2018 計	FY2019 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
重要インフラ事業者等からNISCへの情報連絡(※)	401	856	388	223	48	57	111	53	269
関係省庁・関係機関からのNISCへの情報共有	52	41	19	7	6	3	6	1	16
NISCからの情報提供	44	80	54	43	10	8	8	12	38

※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			FY2015 計	FY2016 計	FY2017 計	FY2018 計	FY2019 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
未発生の事象		予兆・ヒヤリハット	75	330	80	27	3	1	5	3	12
発生した事象	機密性を脅かす事象	情報の漏えい	15	30	15	13	4	5	1	3	13
	完全性を脅かす事象	情報の破壊	52	47	20	17	4	3	1	3	11
	可用性を脅かす事象	システム等の利用困難	86	80	143	97	19	27	84	28	158
	上記につながる事象	マルウェア等の感染	111	289	65	17	3	2	3	1	9
		不正コード等の実行	11	10	13	4	1	1	1	2	5
		システム等への侵入	27	26	17	14	4	5	3	2	14
		その他	24	44	35	34	10	13	13	11	47

※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		FY2015 計	FY2016 計	FY2017 計	FY2018 計	FY2019 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
意図的な原因	不審メール等の受信	83	546	89	36	3	1	7	2	13
	ユーザＩＤ等の偽り	8	1	4	3	1	5	6	0	12
	DDoS攻撃等の大量アクセス	47	23	31	17	3	4	7	6	20
	情報の不正取得	8	14	16	10	0	3	2	3	8
	内部不正	2	0	4	1	0	0	0	0	0
	適切なシステム等運用の未実施	10	19	15	14	4	3	3	1	11
偶発的な原因	ユーザの操作ミス	10	15	23	10	2	3	1	0	6
	ユーザの管理ミス	5	8	13	6	4	0	0	2	6
	不審なファイルの実行	51	243	42	16	3	1	2	1	7
	不審なサイトの閲覧	49	29	20	4	1	2	2	0	5
	外部委託先の管理ミス	12	20	41	29	8	4	18	9	39
	機器等の故障	17	22	32	27	3	4	47	8	62
	システムの脆弱性	29	56	36	19	5	3	3	5	16
	他分野の障害からの波及	5	0	10	6	0	0	4	0	4
環境的な原因	災害や疾病等	0	0	0	1	0	13	0	0	13
その他の原因	その他	22	34	29	29	5	7	11	10	33
	不明	105	92	57	46	10	12	20	11	53

（注）FY:年度、Q:四半期

重要インフラにおける情報共有件数について（2020 年度第 1 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	―	―	―	61
関係省庁・関係機関からのNISCへの情報共有	41	19	7	16	4	―	―	―	4
NISCからの情報提供	80	54	43	38	11	―	―	―	11

※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	―	―	―	3
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	―	―	―	4
	完全性を脅かす事象	情報の破壊	47	20	17	11	4	―	―	―	4
	可用性を脅かす事象	システム等の利用困難	80	143	97	158	39	―	―	―	39
	上記につながる事象	マルウェア等の感染	289	65	17	9	4	―	―	―	4
		不正コード等の実行	10	13	4	5	0	―	―	―	0
		システム等への侵入	26	17	14	14	1	―	―	―	1
		その他	44	35	34	47	6	―	―	―	6

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

（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（2019 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

○　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

外部委託先の不具合、システムの更新・設定の不具合、内部の人的統制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のほうが依然として多く発生している。

○　アカウントの厳格管理が必要

人事異動により使われなくなったアカウントへの不正ログインにより、不正操作された事例があった。

○　特殊ケースに対する備えが必要

うるう年対応の設定漏れで、システムが正常始動しなかった事例があった。

○　重要システムを支える設備の信頼性確保が必要

電源設備の不具合発生による停電で機器が停止し、サービスが提供できなかった事例があった。

○　リスクに応じた外部サービスの利用が必要

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、サービスが提供できなかった事例が多数あった。

契約形態に応じたバックアップの取得と早期回復手段の確保、外部システムの不具合を前提とした多重化・多様化等による代替手段の確保にも留意。

○　利用期間全体を見据えたシステム構築・維持が必要

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

最近のインシデントから得られた教訓（2020 年度第 1 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

○　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

外部委託先の不具合、システムの更新・設定の不具合、内部の人的統制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のほうが依然として多く発生している。なお、新型コロナウイルス感染症(COVID-19)の対応としてテレワークの採用が増加しているが、その運用に当たっては、セキュリティ上のリスクの適切な把握、管理が必要なことに留意。

○　世代管理によるバックアップの取得等、ランサムウエア対策は依然必要

ランサムウエアに感染し、ファイルが暗号化された事例が複数あった。

○　ドメイン登録状況にも注視が必要

ドメイン登録サービスの脆弱性を突いてドメイン登録情報が書き換えられたり、第三者により別ドメインが登録されたりした事例があった。

○　乗っ取りの事実を確認したら、即時のアカウント停止が必要

フィッシングサイトへの ID とパスワードの入力により、メールアカウントが乗っ取られ、スパムメールの送信に利用された事例があった。

自身が被害者から加害者になってしまうことがあることに留意。

○　重要システムを支える設備の信頼性確保が必要

電源設備の不具合発生による停電で機器が停止し、サービスが提供できなかった事例が引き続きあった。

○　リスクに応じた外部サービスの利用が必要

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、サービスが提供できなかった事例が引き続き多数あった。

契約形態に応じたバックアップの取得と早期回復手段の確保、外部システムの不具合を前提とした多重化・多様化等による代替手段の確保にも留意。

以上