資料５

令和元年 10 月 28 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 1 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 1 四半期(4 月～6 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 米国

1.1.1 2019 年 5 月の米中対立の動向[1-5]

- ○ 2019 年 5 月 10 日、米国政府は米中貿易交渉が決裂したとして中国製品への追加関税を 25%に引上げ、ファーウェイ製品の米国全体のネットワークからの全面排徐を決定し、米中覇権争いが本格化。
- ○ 覇権争いの背景としては、中国共産党一党独裁体制の下、中国による国有企業への補助金や外国企業からの知的財産の窃取等による産業構造が米国の権益を脅かしていることにある。
- ○ 相互の関税引上げの結果、中国では米国製品の値上げにより物価上昇したが、米国では、高い関税が課せられた中国製品の値下げによって物価は安定。

---

[1] *日本経済新聞「米、対中関税引上げ 日本企業にも影響広がる(2019/5/10)」、https://www.nikkei.com/article/DGXMZO44619180Q9A510C1000000/ (2019/5/23 閲覧)*

[2] *Whitehouse「Executive Order on Securing the Information and Communications Technology and Services Supply Chain(2019/5/15)」、https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (2019/5/17 閲覧)*

[3] *野村総研「中国政府の産業補助金の問題はどこにあるか(2019/5/16)」、https://www.nri.com/jp/knowledge/blog/lst/2019/fis/kiuchi/0516 (2019/5/22 閲覧)*

[4] *USTR「UPDATE CONCERNING CHINA'S ACTS, POLICIESAND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION(2018/11/20)」、https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf (2019/5/22 閲覧)*

[5] *日本経済新聞「貿易摩擦、痛みは中国に安定物価が米政権強気支える(2019/5/10)」、https://r.nikkei.com/article/DGXMZO44628380100520 19MM8000?unlock=1 (2019/5/22 閲覧)*

1.1.2 米国のインド太平洋戦略報告書[6]

- ○ 2019 年 6 月 1 日、米国防総省はインド太平洋戦略報告書を公表。
- ○ 本報告書は中国国民、中国政府及び中国共産党による支配体制を明確に区別した上で、中国共産党による支配体制がインド太平洋地域の脅威であると指摘。
- ○ 中国は軍事的及び経済的手段を行使して自国の影響力を拡大しており、国家安全保障と経済安全保障は一体であると明言。

1.1.3 米 Finite State 社のファーウェイに関する報告書[7]

- ○ 2019 年 6 月 27 日、米セキュリティ企業 Finite State は「Finite State サプライチェーン評価：ファーウェイテクノロジーズ」を発表し、ファーウェイ製機器がユーザーに高いリスクをもたらすことを指摘。
- ○ 調査したほぼ全てのカテゴリにおいて、ファーウェイの機器は他のベンダーの同等の機器よりも安全性が低く、同社の機器に存在する既知の脆弱性を多数放置していることが判明。
- ○ 本報告書は、ファーウェイ製機器には重大なセキュリティ上の脆弱性があるものの、これらが中国政府へのアクセス提供を企図して意図的に追加されたものかどうかは不明と指摘。

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 米インテリジェンス機関からのデータ流出[8-11]

- ○ 2019 年 4 月 12 日、FBI 関連組織の Web サイトがハッキングされ、米連邦機関に属する約 4,000 人分のデータが流出。
- ○ 流出データは、職員名、個人・業務用のメールアドレス、組織内での役職、電話番号、住所等。
- ○ 過去にも、米国の他のインテリジェンス機関において個人情報の流出事案が発生。

---

[6] *DoD「THE DEPARMENT OF DEFENSE Indo-Pacific Strategy Report Preparedness, Partnerships, and Promoting a Networked Region June 1, 2019(2019/6/1)」、https://media.defense.gov/2019/May/31/2002139210/-1/-1/1/DOD_INDO_PACIFIC_STRATEGY_REPORT_JUNE_2019.PDF (2019/6/16 閲覧)*

[7] *FINITE STATE「Finite State Supply Chain Assessment Huawei Technologies Co., Ltd(2019/6/27)」、https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf (2019/7/4 閲覧)*

[8] *TechCrunch「Hackers publish personal data on thousands of US police officers and federal agents(2019/4/12)」、https://techcrunch.com/2019/4/12/police-data-hack/ (2019/5/14 閲覧)*

[9] *ITmedia「米国土安全保障省や FBI の職員情報、大量に流出か(2016/2/9)」、https://www.itmedia.co.jp/enterprise/articles/1602/09/news059.html (2019/5/14 閲覧)*

[10] *ZDNet「約 24 万人分の個人情報漏えい、米国土安全保障省が明らかに(2018/1/5)」、https://japan.zdnet.com/article/35112766/ (2019/5/15 閲覧)*

[11] *ZDNet「米国防総省、セキュリティ侵害で職員約 3 万人の個人情報など流出との報道(2018/5/15)」、https://japan.zdnet.com/article/35126973/ (2019/5/14 閲覧)*

2.1.2　NASA の機密情報漏えいに関する報告書[12-14]

- ○ 2019 年 6 月 18 日、米航空宇宙局 NASA は、同局のジェット推進研究所(JPL)のネットワークに対するハッキングが 2018 年に行われていたことを公表。
- ○ JPL のネットワークに無許可で接続されていた市販の汎用小型コンピュータ Raspberry Pi を介して侵入されており、NASA のセキュリティ管理の問題点が露呈。
- ○ JPL のシステムのみならず、相互接続されたネットワークを介してジョンソン宇宙センターのシステム等にも侵入されたとみられるが、攻撃者は不明で継続調査中。

2.2 重要インフラ関連

2.2.1 ボーイング 737MAX 型機の墜落事故と安全設計[15-18]

- ○ 米ボーイング社の最新型の小型旅客機 737MAX8 において、ライオン航空 610 便、エチオピア航空 302 便と、相次いで墜落事故が発生。
- ○ 暫定報告書によると、機体のセンサーの不具合が操縦特性補助システムの動作に影響し墜落の要因となった可能性を示唆。
- ○ 安全を確保するためには、ISO/IEC Guide 51:2014 にあるように、設計段階における本質的安全設計、防護装置等の機能安全、使用上の注意喚起やオペレータの訓練により、リスクの軽減を実施する等により、リスクの軽減策を行うことが大前提。

---

[12] *NASA Office of Inspector General「CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JETPROPULSION LABORATORY(2019/6/18)」、https://oig.nasa.gov/docs/IG-19-022.pdf (2019/7/10 閲覧)*

[13] *NASA Jet Propulsion Laboratory「Deep Space Network」、https://deepspace.jpl.nasa.gov/ (2019/7/10 閲覧)*

[14] *NASA Johnson Space Center「Johnson Space Center Home」、https://www.nasa.gov/centers/johnson/home/index.html (2019/7/10 閲覧)*

[15] *Komite Nasional Keselamatan Transportasi「Preliminary Aircraft Accident Investigation Report (2018/11)」、http://knkt.dephub.go.id/knkt/ntsc_aviation/baru/pre/2018/2018%20-%20035%20-%20PK-LQP%20Preliminary%20Report.pdf (2019/5/21 閲覧)*

[16] *Ministry of Transport (Ethiopia)「Aircraft Accident Investigation Bureau Preliminary Report(2019/3/10)」、http://www.ecaa.gov.et/documents/20435/0/Preliminary+Report+B737-800MAX+%2C%28ET-AVJ%29.pdf (2019/5/10 閲覧)*

[17] *ISO/IEC ガイド 51 は、規格の作成者が安全側面を規格に導入する際の実質的な指針となり、安全に関する基本思想が定められている。JIS Z 8051。*

[18] *「機能安全」とは、「安全機能」と異なることに注意。機能安全とは、監視装置や防護装置等の付加機能によるリスク低減方策により安全性を実現するための方策の 1 つである。機能安全は、その装置等が正しく働いている時に実現できる安全性であり、機能が正しく働いている場合のみに実現される安全性である。*

2.3 その他

2.3.1 マルウエア感染に伴うHOYA社の生産ライン停止[19]

- ○ 日本の光学機器メーカーHOYA社が、2月末にサイバー攻撃を受けていたと公表。
- ○ 同社のタイ工場のPC約100台がマルウエアに感染し、生産ラインが3日間停止。
- ○ 感染したマルウエアの調査から、仮想通貨採掘目的と推測。

2.3.2 Amazon従業員によるAlexa入力音声の解析[20-21]

- ○ Amazon社のAIアシスタントAlexaに入力された音声を、同社の従業員が解析。
- ○ 同社の音声確認スタッフは顧客の位置情報にもアクセスが可能。
- ○ 同社は応答性能改善を目的とした対応であると説明したが、報道ではプライバシー上の問題が指摘。

2.3.3 米国の大手ウイルス対策ソフトベンダー3社へのサイバー攻撃[22-25]

- ○ 米セキュリティ企業Advanced Intelligence社は、米国の大手ウイルス対策ソフトベンダー3社がサイバー攻撃を受けたとの調査結果を発表。
- ○ サイバー攻撃を行ったロシアのハッカー集団「Fxmsp」は、入手した機密データや侵入方法を30万ドルで販売する準備ができているとの情報。
- ○ 攻撃を受けたとされている3社は、事実関係を公表し対応を実施。

---

[19] *中国新聞デジタル「HOYAにサイバー攻撃生産ライン3日ダウン(2019/4/7)」、https://www.chugoku-np.co.jp/local/news/article.php?comment_id=520019&comment_sub_id=0&category_id=256 (2019/5/21閲覧)*

[20] *Bloomberg「Amazon Workers Are Listening to What You Tell Alexa(2019/4/11)」、https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio (2019/5/14閲覧)*

[21] *Bloomberg「Amazon's Alexa Team Can Access Users' Home Addresses(2019/4/24)」、https://www.bloomberg.com/news/articles/2019-04-24/amazon-s-alexa-reviewers-can-access-customers-home-addresses (2019/5/14閲覧)*

[22] *Advanced Intelligence「Top-Tier Russian Hacking Collective Claims Breaches of Three Major Anti-Virus Companies(2019/5/9)」、https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies (2019/6/18閲覧)*

[23] *トレンドマイクロ「一部SNSや報道に関して(2019/5/20)」、https://www.trendmicro.com/ja_jp/about/announce/announces-20190520-01.html (2019/5/20閲覧)*

[24] *Symantec「Norton Community Fxmsp hack(2019/6/13)」、https://community.norton.com/en/forums/fxmsp-hack (2019/6/18閲覧)*

[25] *Computer Business Review「Trend Micro Admits it Was Hacked, Symantec Denies Claims of "Fxmsp" Breach(2019/5/11)」、https://www.cbronline.com/news/trend-micro-symantec-fxmsp (2019/6/17閲覧)*

2.3.4 古い Windows に影響する深刻な脆弱性「BlueKeep」[26-27]

- ○ 2019 年 5 月 15 日、マイクロソフト社がリモートデスクットプサービスの深刻な脆弱性「BlueKeep」に対するセキュリティアップデートをリリース。
- ○ マイクロソフト社は当該脆弱性を WannaCry のようなワームに使用される危険性がある「Wormable」と評価。
- ○ 影響の大きさから、サポートが終了した Windows OS にも異例のアップデートが提供されており、多くのセキュリティ関係機関が警告を発出。

2.3.5 マイクロソフト社の Office 365 を標的としたクラウドサービスへの攻撃[28-30]

- ○ フィッシング攻撃が高度化し、不正な Web サイトで信頼された証明書を利用した攻撃サイトが登場。
- ○ FBI や US-CERT は、クラウドサービスの利用に関して注意喚起を実施。
- ○ クラウドサービスの利用には、従来とは異なる新たなリスクの認識と対応が必要。

2.3.6 Gmail におけるショッピング履歴のリスト化[31-32]

- ○ Gmail で受信したショッピング履歴のデータが、ユーザーの知らないうちにリスト化されていたことが判明。
- ○ EC サイトで買い物を行った際に送付される注文確認メールの抜粋(日時、商品名、金額等)が自動的にリスト化。
- ○ Google は、これらの情報が広告利用される心配はないと説明。

---

[26] *Microsoft「Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)(2019/5/14)」、https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/ (2019/6/19 閲覧)*

[27] *National Security Agency「NSA Cybersecurity Advisory: Patch Remote Desktop Services on Legacy Versions of Windows(2019/6/4)」、https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/ (2019/6/19 閲覧)*

[28] *Bleeping Computer「Phishing Emails Pretend to be Office 365 'File Deletion' Alerts(2019/5/28)」、https://www.bleepingcomputer.com/news/security/phishing-emails-pretend-to-be-office-365-file-deletion-alerts/ (2019/6/5 閲覧)*

[29] *日経 xTECH「クラウドメールは北朝鮮のサイバー攻撃なみに危険？米機関が注意喚起(2019/6/5)」、https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00675/00576/052200006/ (2019/6/11 閲覧)*

[30] *US-CERT,[Analysis Report (AR19-133A) Microsoft Office 365 Security Observations(2019/5/13)]、https://www.us-cert.gov/ncas/analysis-reports/AR19-133A (2019/6/12 閲覧)*

[31] *INTERNET Watch「Gmail で受信したショッピング履歴のデータ、リスト化されていたことが判明し騒動に(2019/5/20)」、https://internet.watch.impress.co.jp/docs/yajiuma/1185310.html (2019/6/12 閲覧)*

[32] *Google アカウント ヘルプ「購入、定期購入、予約をすべて表示する」、https://support.google.com/accounts/answer/7673989 (2019/6/12 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 改元及び 10 連休の対応[33-35]

- ○ 改元に伴い過去最長の 10 連休となり、事業者等ではシステムトラブルの発生が懸念されていたが、国民生活に支障を生じさせるような大きな混乱を招くシステムトラブルは発生しなかった。
- ○ 10 連休を迎えるにあたり、事前に政府機関や各事業者等から、期間中のサービス対応等に関する注意喚起を実施。
- ○ システムトラブルの発生した一部の事業者等においては、HP 上でお詫びやサービスの提供に支障はない旨を示して対応。

3.1.2 デジタル手続法[36-37]

- ○ 「未来投資戦略 2018」を受け、「デジタル手続法」が成立。
- ○ 未来投資戦略 2018 において、デジタル手続法は、デジタル・ガバメントの推進のための旗艦プロジェクトという位置付け。
- ○ デジタル手続法には、社会全体のデジタル化というビジョンと基本原則が記載。

3.2 重要インフラ関連

3.2.1 大阪市役所における統合基盤システムの障害[38-40]

- ○ 2019 年 6 月 7 日、大阪市役所の統合基盤システムに不具合が発生し、各種証明書の発行が停止。
- ○ 証明書の発行ができなかった等、約 8,000 件の影響が発生。
- ○ 統合基盤システムのデータベースソフトの不具合(バグ)が根本原因であり、これによりデータベース管理システムに障害が発生し、端末の認証機能や印刷機能等の利用不可に波及。

---

33 内閣府「天皇の即位の日及び即位礼正殿の儀の行われる日を休日とする法律の円滑な施行に関する関係省庁連絡会議」、https://www8.cao.go.jp/chosei/shukujitsu/about/gaiyou/syouchoukaigi.html

34 共同通信「改元前にコンビニ ATM で誤表記　道銀等、画面に「1989 年」(2019/4/29)」、https://this.kiji.is/495503386154763361 (2019/6/18 閲覧)

35 日本経済新聞 web「銀行、郵便、病院・・・10 連休中のサービスは？(2019/4/26)」、https://www.nikkei.com/article/DGXMZO44237910W9A420C1EA2000/ (2019/6/12 閲覧)

36 日本経済再生本部「未来投資戦略 2018―「Society 5.0」「データ駆動型社会」への変革―(2018/6/15)」、https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf (2019/6/18 閲覧)

37 内閣官房 IT 総合戦略室「デジタル手続法案の概要について(2019/3/5)」、https://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/bukai/20190305/190305bukai05.pdf (2019/6/18 閲覧)

38 大阪市「大阪市統合基盤システムサーバーの障害について【最終報】(2019/6/24)」、https://www.city.osaka.lg.jp/hodoshiryo/ictsenryakushitsu/0000474144.html (2019/7/22 閲覧)

39 大阪市「大阪市統合基盤システムサーバーの障害について【第 7 報】(2019/6/10)」、https://www.city.osaka.lg.jp/hodoshiryo/ictsenryakushitsu/0000472778.html (2019/7/22 閲覧)

40 日経コンピュータ 2019 7.11 号「大阪市 住民票発行が 21 時間停止、8000 件影響 Oracle DB の非公開バグが原因」

3.2.2 シーサイドラインにおける逆走事故[41-43]

- ○ 横浜市の新交通システム金沢シーサイドライン新杉田駅において、車両が折り返す際に逆走事故が発生。
- ○ 事故は、進行方向を指示する回路の断線により、進行方向の切替えが制御装置に伝わらず、直前の進行方向を維持する動作となり、結果として逆走。
- ○ 鉄道のような安全に直結するシステムは、たとえ断線のような障害が発生した際にも、本質的安全設計によるフェールセーフの原則に則り、常に安全側に制御されることが必要。

3.3 その他

3.3.1 頻発するドメイン移管の悪用[44-48]

- ○ 大学・企業等が登録していたドメイン名が第三者に移管され、元のドメイン名登録者の運営目的とは異なる目的に利用される事案が多発。
- ○ ドメイン名が第三者に取得された原因は、JPRS が提供するドメイン名登録制度の運用上の不備。
- ○ 総務省は JPRS に対して、ドメイン名の適切な管理・運用を要請。

---

41 Wikipedia「横浜シーサイドライン金沢シーサイドライン(2019/7/5)」、https://ja.wikipedia.org/wiki/%E6%A8%AA%E6%B5%9C%E3%82%B7%E3%83%BC%E3%82%B5%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3%E9%87%91%E6%B2%A2%E3%82%B7%E3%83%BC%E3%82%B5%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3 (2019/7/22 閲覧)

42 国土交通省「無人で自動運転を行う鉄軌道の事故防止に関する検討会 第３回 資料 3(2019/7/19)」、https://www.mlit.go.jp/common/001300033.pdf (2019/7/19 閲覧)

43 国土交通省「無人で自動運転を行う鉄軌道の事故防止に関する検討会 中間とりまとめ(2019/7/19)」、https://www.mlit.go.jp/common/001300038.pdf (2019/7/19 閲覧)

44 朝日新聞デジタル「旧山梨医大 HP が風俗サイトに「なぜか分からない」(2019/4/5)」、https://www.asahi.com/articles/ASM456F6NM45UPQJ008.html (2019/5/21 閲覧)

45 ITmedia NEWS「「ラブライブは我々が頂いた！」人気アニメの公式サイト乗っ取りか 公式「原因究明中」 ドメイン移管された?(2019/4/5)」、https://www.itmedia.co.jp/news/articles/1904/05/news051.html (2019/5/21 閲覧)

46 J-CAST ニュース「ラブライブ！乗っ取り事件、「第三者によるドメイン移管申請」説の真偽は?サンライズは「ドメインロック含め安全対策」(2019/4/5)」、https://www.j-cast.com/2019/04/05354572.html (2019/5/21 閲覧)

47 総務省「株式会社日本レジストリサービスに対する「.jp」ドメイン名の管理・運用に係る措置（要請）(2019/4/26)」、http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000152.html (2019/5/21 閲覧)

48 ITmedia NEWS「「ラブライブ！」乗っ取りを"教訓"にドメイン名の価値に見合った管理方法(2019/4/11)」、https://www.itmedia.co.jp/news/articles/1904/11/news024.html (2019/5/21 閲覧)

3.3.2 ヤマダウェブコム等におけるクレジットカード情報漏えい[49-50]

○ ヤマダ電機が運営する「ヤマダウェブコム・ヤマダモール」からクレジットカード情報が最大 37,832 件流出。
○ 2019 年、多数のクレジットカード情報漏えい事案が公表。
○ 「リダイレクト(リンク)型」又は「Java Script 型(トークン型)」を狙った攻撃で、セキュリティコードまで漏えいした事案が大半。

3.3.3 クレジットカードの不正利用[51]

○ 外部で不正に取得したと思われる ID・パスワードを使ったなりすましにより、イオンカードが不正に利用され、708 名の会員において 2,200 万円余りの被害が発生。

3.3.4 東京 2020 オリンピック競技大会の観戦チケット販売関連事案[52-56]

○ 2019 年 6 月 20 日、東京 2020 オリンピック競技大会の観戦チケット抽選結果が発表。
○ 抽選申込受付開始時、抽選申込受付終了時、抽選結果発表時には、公式販売サイトの順番待ちで、それぞれ長時間の待ちが発生。
○ 抽選結果の発表に伴い、偽の当選メールを使った詐欺が発生。

以上

---

[49] 株式会社ヤマダ電機「弊社が運営する「ヤマダウェブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ(2019/5/29)」、https://www.yamada-denki.jp/information/190529/ (2019/6/10 閲覧)

[50] 徳丸浩の日記「2019 年 1 月から 5 月に公表されたウェブサイトからのクレジットカード情報漏えい事件まとめ(2019/5/30)」、https://blog.tokumaru.org/2019/05/credit-card-information-leak-incidents-2019-1-5.html (2019/6/10 閲覧)[49]

[51] 株式会社イオン銀行及びイオンクレジットサービス株式会社「インターネットサービス「暮らしのマネーサイト」での不正ログイン発生のお知らせおよびパスワード変更のお願いについて(2019/6/13)」、https://www.aeon.co.jp/information/201906_info/index.html (2019/7/17 閲覧)

[52] NHK「東京五輪チケット 公式サイトに延べ 130 万人のアクセス(2019/5/9)」、https://www3.nhk.or.jp/news/html/20190509/k10011910381000.html (2019/5/13 閲覧)

[53] 日本経済新聞「五輪チケット、見通し甘く 期限を半日延長し終了(2019/7/4)」、https://www.nikkei.com/article/DGXMZO45399920Z20C19A5CC0000/ (2019/5/13 閲覧)

[54] 毎日新聞「東京五輪・パラ、チケット抽選結果発表 公式 HP100 万人以上待機(2019/6/20)」、https://mainichi.jp/sportsspecial/articles/20190620/k00/00m/050/062000c (2019/6/20 閲覧)

[55] 毎日新聞「五輪チケット抽選結果装い詐欺メール 個人情報抜き取り狙う 広島(2019/6/21)」、https://mainichi.jp/sportsspecial/articles/20190621/k00/00m/050/118000c (2019/6/25 閲覧)

[56] 東京新聞「「五輪抽選」SMS で偽サイト誘導 個人情報盗む詐欺注意を(2019/7/14)」、https://www.tokyo-np.co.jp/article/national/list/201907/CK2019071502000104.html (2019/7/16 閲覧)

重要インフラにおける情報共有件数について（2019 年度第 2 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	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	―	―	105
関係省庁・関係機関からのNISCへの情報共有	52	41	19	7	6	3	―	―	9
NISCからの情報提供	44	80	54	43	10	8	―	―	18

※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	―	―	4
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	―	―	9
	完全性を脅かす事象	情報の破壊	52	47	20	17	4	3	―	―	7
	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	―	―	46
	上記につながる事象	マルウェア等の感染	111	289	65	17	3	2	―	―	5
		不正コード等の実行	11	10	13	4	1	1	―	―	2
		システム等への侵入	27	26	17	14	4	5	―	―	9
		その他	24	44	35	34	10	13	―	―	23

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

（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

自然災害、システムの更新・設定の不具合、ネットワーク機器の不具合、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。

○　海外の動向にも注視が必要

複数アドレスからの分散した検知されにくい時間をかけたリスト型攻撃によるアカウント乗っ取りから、サービスが不正利用された事例があった。

海外においては過去からあった攻撃手法が、遅れて日本にも持ち込まれることがあることに留意。

○　システムの企画・設計段階からのセキュリティ確保が必要

認証設計の不備に起因するアカウント乗っ取りから、サービスが不正利用された事例があった。

○　重要システムを支える設備の信頼性確保が必要

空調設備が制御システムの不具合により停止したことに伴うオーバーヒートでシステムが停止し、長時間にわたりサービスの提供が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、長時間にわたりサービスの提供ができなかった事例が多数あった。

○　適時・適切な対外説明も考慮に入れたインシデント対応が必要

インシデント発生後のサービス利用者に対する不適切な対応から、混乱・不安を与えた事例があった。

以上