資料５

令和元年７月 19 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(平成 31 年 1 月～3 月)

【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、平成 31 年 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 米国

1.1.1 DNS ハイジャック攻撃キャンペーンについて[1-3]

- ○ 北米、中東を中心とした全世界的な DNS ハイジャック攻撃キャンペーンが発生。
- ○ 本攻撃は窃取した DNS サーバーの認証情報を用いて不正ログインし、各種 DNS レコードを書き換えることでユーザーの意図しないサイト等にアクセスを誘導。
- ○ 本事案の発生を受け、2019 年 1 月 22 日米国土安全保障省サイバーセキュリティ・インフラセキュリティ庁(DHS/CISA)は、全連邦政府に対する緊急指令 19-01 を発出し、緩和策を実施するよう指示。

---

[1] *Cisco Talos「DNSpionage Campaign Targets Middle East(2018/11/27)」、https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html (2019/2/14 閲覧)*

[2] *FireEye「Global DNS Hijacking Campaign: DNS Record Manipulation at Scale(2019/1/9)」、https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html (2019/2/14 閲覧)*

[3] *DHS CISA「Emergency Directive 19-01(2019/1/22)」、https://cyber.dhs.gov/ed/19-01/ (2019/2/14 閲覧)*

1.1.2 WannaCry で使用された NSA 攻撃ツール流出のまとめ[4-6]

- ○ 2017 年 5 月 12 日、ランサムウエア WannaCry による世界規模でのサイバー攻撃が発生。
- ○ WannaCry のワーム機能には、ハッキンググループ ShadowBrokers が米国家安全保障局(NSA)から窃取したとされる、Windows のファイル共有プロトコル SMBv1 を悪用する攻撃ツール Eternal Blue を使用。
- ○ カスペルスキー社の通報により、EternalBlue を含む米国連邦政府の機密情報を ShadowBrokers に漏えいした容疑で、米司法省(DoJ)は元 NSA 契約職員ハロルド・マーティンを逮捕。

1.1.3 米・欧州における 5G 関連動向[7-9]

- ○ 2019 年 3 月 26 日、欧州連合(EU)は 5G におけるサイバーセキュリティに関する勧告を発表し、EU として特定の企業を一律排除せず、各国が独自に調達基準を定めることを表明。
- ○ 同月 28 日、米国政府は、ファーウェイ社製品が 5G ネットワークの主流になった場合のリスク管理を検討し始めたとの報道。
- ○ 同日、英ファーウェイサイバーセキュリティ評価センター監視委員会と NATO CCDCoE は、それぞれファーウェイ社製品の採用によって生ずるリスクを取りまとめた報告書を公表。

1.2 中国

1.2.1 対米配慮を企図した中国全人代における変化・外商投資法の可決[10-11]

- ○ 中国政府は 2019 年 3 月 5 日から 15 日にかけ、全国人民代表大会を開催。
- ○ 同大会では同月 15 日、外資企業の権益保護の強化を目的とした「外商投資

---

[4] *POLITICO「Suspect's Twitter messages played role in NSA hacking-tools leak probe(2018/12/31)」、https://www.politico.com/story/2018/12/31/nsa-hacking-case-twitter-1077013 (2019/2/15 閲覧)*

[5] *POLITICO「Exclusive: How a Russian firm helped catch an alleged NSA data thief(2019/1/9)」、https://www.politico.com/story/2019/01/09/russia-kaspersky-lab-nsa-cybersecurity-1089131 (2019/2/15 閲覧)*

[6] *DoJ「Government Contractor Charged with Removal of Classified Materials and Theft of Government Property(2016/10/5)」、https://www.justice.gov/usao-md/pr/government-contractor-charged-removal-classified-materials-and-theft-government-property (2019/2/15 閲覧)*

[7] *日本経済新聞「EU、ファーウェイ製品の一律排除見送り 5G で勧告(2019/3/26)」、https://www.nikkei.com/article/DGXMZO42924760W9A320C1MM8000/ (2019/4/12 閲覧)*

[8] *Washington Post「U.S. officials planning for a future in which Huawei has a major share of 5G global networks(2019/4/1)」、https://www.washingtonpost.com/amphtml/world/national-security/us-officials-planning-for-a-future-in-which-huawei-has-a-major-share-of-5g-global-networks/2019/04/01/2bb60446-523c-11e9-a3f7-78b7525a8d5f_story.html&freshcontent=1 (2019/4/12 閲覧)*

[9] *NATO CCDCoE「Huawei, 5G and China as a Security Threat(2019/3/28)」、https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2018-03-28-FINAL.pdf (2019/4/15 閲覧)*

[10] *Wall Street Journal「Beijing Drops Contentious 'Made in China 2025' Slogan, but Policy Remains(2019/3/5)」、https://www.wsj.com/articles/china-drops-a-policy-the-u-s-dislikes-at-least-in-name-11551795370 (2019/4/9 閲覧)*

[11] *大紀元「中国、新しい外商投資法を可決 欧米の懸念払拭できるか(2019/3/19)」、https://www.epochtimes.jp/2019/03/41263.html (2019/4/9 閲覧)*

法」が可決され、また政府活動報告では、過去 3 年間報告の中心であった中国製造 2025 に言及しなかった。

○ これらの動きは米中通商協議を念頭に置いた中国政府による対米配慮であるとみられるが、米国の専門家らは中国製造 2025 で定められた政策は現在も実行されており、また外商投資法に実効性がないとして、これらの動きが見せかけであると批判。

1.3 豪州

1.3.1 豪州連邦議会へのサイバー攻撃について[12-14]

○ 2019 年 2 月 8 日、豪州連邦議会のコンピュータネットワークに対するサイバー攻撃が発生。

○ 同月 18 日、豪モリソン首相は同国の複数の政党に対してもサイバー攻撃があったと公表し、本攻撃に国家が関与していると指摘。

○ ロイター通信は本攻撃が中国によるものである可能性を指摘し、攻撃の動機として中国政府の内政干渉に対する豪州政府による非難を契機とした豪中関係の悪化について報道。

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 重要インフラに関連するサイバーセキュリティインシデント等

2.1.1 国際民間航空機関(ICAO)へのサイバー攻撃について[15-16]

○ 2019 年 2 月 27 日、カナダの報道機関 CBC は内部文書に基づき、国際民間航空機関(ICAO)が 2016 年 11 月にサイバー攻撃を受けたと報道。

○ 報道により、ICAO のセキュリティ担当者は攻撃を知りながら放置し、さらに対応を隠蔽していたことが判明。

○ 本攻撃には中国と関連する攻撃者グループ「Emissary Panda」が関与していると報道。

---

[12] *Reuters「Australia probes attempted hacking of national parliament(2019/2/8)」、https://af.reuters.com/article/worldNews/idAFKCN1PX05B (2019/3/13 閲覧)*

[13] *Reuters「Australia accuses foreign government of cyber attack on lawmakers(2019/2/18)」、https://www.reuters.com/article/us-australia-cyber/australia-accuses-foreign-government-of-cyber-attack-on-lawmakers-idUSKCN1Q704G (2019/3/14 閲覧)*

[14] *The Guardian「China rejects Australian parliament cyber attack claims as 'baseless' and 'irresponsible'(2019/2/19)」、https://www.theguardian.com/australia-news/2019/feb/19/china-rejects-australian-parliament-cyber-attack-claims-as-baseless-and-irresponsible (2019/3/14 閲覧)*

[15] *CBC「Montreal-based UN aviation agency tried to cover up 2016 cyberattack, documents show(2019/2/27)」、https://www.cbc.ca/news/canada/montreal/montreal-based-un-aviation-agency-tried-to-cover-up-2016-cyberattack-documents-show-1.5033733 (2019/3/14 閲覧)*

[16] *国際連合広報センター「国際民間航空機関 International Civil Aviation Organization(ICAO)」、https://www.unic.or.jp/info/un/unsystem/specialized_agencies/icao/ (2019/3/14 閲覧)*

2.2 その他の事案

2.2.1 米マリオット・インターナショナル 約 3.8 億人分の顧客情報の流出[17-19]

- ○ 米マリオット・インターナショナルは 2018 年 11 月 30 日、顧客のデータベースに不正アクセスがあり、最大約 5 億人(その後 3.8 億人に修正)の顧客の個人情報が流出した可能性があると発表。
- ○ 氏名、住所等の顧客情報のほか、暗号化されていないパスポート番号も流出。
- ○ 本事案に関し、米ポンペオ国務長官が中国の関与を指摘。

2.2.2 約 27 億件の巨大漏えいファイル「Collection#1」[20-22]

- ○ 2019 年 1 月 7 日頃、あるハッカーフォーラムに「Collection#1」という名称の巨大な漏えいデータの存在が投稿。
- ○ Microsoft Regional Director(豪州)の Hunt 氏は 2019 年 1 月 17 日に、自身のブログで「Collection#1」が合計約 27 億件の電子メールアドレスとパスワードのセットであること等の分析結果を公表。
- ○ 株式会社ソリトンシステムズは同年 2 月 21 日に、当該データに日本の約 2,000 万件のアカウント情報、42 ドメインが含まれていたこと等を公表。

2.2.3 Microsoft 社 Internet Explorer をめぐる話題[23-25]

- ○ 衆議院財務金融委員会において、政府機関等が提供するシステムが Microsoft 社の Web ブラウザ Internet Explorer(IE)に依存している点に関し、IE を指定のブラウザとすることで、利用者環境が制限され、IE の脆弱性によりセキュリティ上のリスクが高まるのではないかとの懸念が議論。
- ○ IE の脆弱性は、製品開発元の Microsoft 社が作成するセキュリティの修正モ

---

[17] *Kroll「Starwood Guest Reservation Database Security Incident(2019/1/4)」、https://answers.kroll.com/ (2019/2/12 閲覧)*

[18] *日本経済新聞「米国務長官、中国関与を指摘 マリオットの情報流出(2018/12/13)」、https://www.nikkei.com/article/DGXMZO38868280T11C18A2000000/ (2019/2/12 閲覧)*

[19] *日本経済新聞「米マリオット 旅券番号 500 万件、暗号化されず流出(2019/1/5)」、https://www.nikkei.com/article/DGXMZO39673000V00C19A1000000/ (2019/2/12 閲覧)*

[20] *Troy Hunt 氏ブログ「The 773 Million Record "Collection #1" Data Breach(2019/1/17)」、https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/ (2019/3/8 閲覧)*

[21] *パスワードは大文字と小文字を区別し、電子メールアドレスは大文字と小文字を区別しないものとして扱った場合の数字。*

[22] *Krebs on Security「773M Password 'Megabreach' is Years Old(2019/1/19)」、https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old/ (2019/3/9 閲覧)*

[23] *衆議院「第 198 回国会 財務金融委員会 第 3 号(平成 31 年 2 月 26 日(火曜日))」、http://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/009519820190226003.htm(2019/3/13 閲覧)*

[24] *Microsoft「The perils of using Internet Explorer as your default browser(2019/2/6)」、https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/The-perils-of-using-Internet-Explorer-as-your-default-browser/ba-p/331732 (2019/2/25 閲覧)*

[25] *Engadget Japan「マイクロソフト、企業に Internet Explorer の使用をやめるよう要請。「IE は技術的負債もたらす」(2019/2/9)」、https://japanese.engadget.com/2019/02/08/internet-explorer-ie/ (2019/3/14 閲覧)*

ジュールを適用することで対応され、他の代表的なブラウザである Google 社の Chrome や Apple 社の Safari 等と比べても、大きなリスクとなるものではないと考えられる。

○ Web アプリケーションの普及により、Web ブラウザの重要性が高まる中で、Microsoft 社も、最新の標準をサポートしていない IE の使用を継続することは技術的な負債となるとし、より新しい標準をサポートした最新のブラウザの使用を奨励。

2.2.4 Norsk Hydro のランサムウエア感染事案について [26-27]

○ ノルウェーの大手アルミ製造業者 Norsk Hydro 社がサイバー攻撃を受けランサムウエアに感染し、工場の操業を手動による操作に切り替えざるを得なくなった。

○ 攻撃にはランサムウエア LockerGoga が使用されたとしており、Norsk Hydro 社の他、フランス Altran Technology 社、米 Hexion 社及び米 Momentive 社等複数の組織から LockerGoga の被害が報告された。フランス ANSSI、米国 MS-ISAC は注意喚起を実施。

○ LockerGoga の感染に至る初期の侵入経路や攻撃の意図は不明。

2.2.5 ASUS 社製 PC に対するサプライチェーン攻撃[28-29]

○ 2019 年 3 月 25 日、セキュリティ企業 Kaspersky 社が、PC メーカーASUS 社製の PC に対する過去最大級のサプライチェーン攻撃「Shadow Hammer」を公表。

○ 攻撃者は、ASUS 社の正規のソフトウエアを改ざんし、バックドアを組み込んだソフトウエアを正規のアップデートサーバーから配信。

○ 改ざんされたソフトウエアは特定の条件を満たす機器でのみ、更なる攻撃を実行するよう設計されており、Kaspersky 社は今回の攻撃を標的型攻撃と分析。

---

[26] *Norsk Hydro「Hydro subject to cyber attack(2019/3/19)」,https://www.hydro.com/ja-JP/medeia/news/2019/hydro-subject-to-cyber-attack/ (2019/4/5 閲覧)*

[27] *MS-ISAC「Security Primer LockerGoga(2019/3/28)」、https://www.cisecurity.org/wp-content/uploads/2019/03/LockerGoga-Security-Primer.pdf (2019/4/5 閲覧)*

[28] *Kaspersky「Shadow Hammer: Malicious updates for ASUS laptops(2019/3/25)」、https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/ (2019/4/10 閲覧)*

[29] *ASUS「ASUS response to the recent media reports regarding ASUS Live Update tool attack by Advanced Persistent Threat (APT) groups(2019/3/26)」、https://www.asus.com/News/hqfgVUyZ6uyAyJe1 (2019/4/10 閲覧)*

2.2.6 Google、Apple、Facebook における障害[30-32]

- ○ 2019 年 3 月、主要な IT 企業である Google 社、Apple 社、Facebook 社のサービスに相次いで障害が発生した。
- ○ Google 社及び Facebook 社の障害は、サイバー攻撃によるものではなく、設定変更に起因するもの。
- ○ Google 社及び Facebook 社は、障害時における情報公開について、積極的に公表する一方、Apple 社の対応はサービス状況を示すのみ等、対応に差があった。

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 重要インフラに関連するサイバーセキュリティインシデント等

3.1.1 JCB カード等の決済システム障害[33-35]

- ○ 2019 年 2 月 2 日、JCB カード等の一部のクレジットカードが約 40 分間加盟店で利用できない事象が発生。
- ○ 原因は、日本カードネットワーク社が運営する CARDNET センターにおけるネットワーク障害。
- ○ 同社に対し経済産業省は、原因究明と再発防止を要請。

3.1.2 新幹線自動券売機のシステム障害[36]

- ○ 2019 年 2 月 15 日、JR 各社の新幹線自動券売機が停止し、特急券等の購入ができなくなるトラブルが発生。
- ○ JR のチケット予約・販売システムを管理する鉄道情報システム株式会社は、このトラブルの原因について、同年 3 月のダイヤ改正に対応するために行った、自動券売機のプログラムの改修にミスがあったと発表。

---

[30] *TechCrunch[Apple's iCloud recovers after a four-hour outage(2019/3/15)」、https://techcrunch.com/2019/03/14/apples-icloud-is-having-an-outage-too/ (2019/4/4 閲覧)*

[31] *Twitter「@facebook(2019/3/15)」、https://twitter.com/facebook/status/1106229690069442560 (2019/4/4 閲覧)*

[32] *Google「Google Cloud Status Dashboard」、https://status.cloud.google.com/incident/storage/19002 (2019/4/4 閲覧)*

[33] *日本カードネットワーク「2 月 2 日 CARDNET センターの障害について(2019/2/2)」、http://www.cardnet.co.jp/release/20190202.html (2019/3/12 閲覧)*

[34] *共同通信「クレカ障害の原因究明要請(2019/2/4)」、https://this.kiji.is/465066203523040353 (2019/3/12 閲覧)*

[35] *日経 xTECH「CARDNET のクレジット決済に 6 時間強障害、原因は L3 スイッチ故障(2017/4/17)」、https://tech.nikkeibp.co.jp/it/atcl/news/17/041701170/ (2019/3/12 閲覧)*

[36] *日経 xTECH「新幹線の券売機トラブルが復旧、ダイヤ改正に伴うプログラム改修にミス(2019/2/19)」、https://tech.nikkeibp.co.jp/atcl/nxt/news/18/04193/ (2019/3/19 閲覧)*

3.2 その他の事案

3.2.1 NICT による脆弱な IoT 機器の調査「NOTICE」の開始[37-38]

- ○ 総務省は、サイバー攻撃に悪用されるおそれのある IoT 機器を洗い出し、利用者に注意喚起を行う取組「NOTICE」を情報通信研究機構(NICT)が行うと公表。
- ○ 「NOTICE」に関して、「国によるサイバー攻撃ではないか」と不安視する一部報道があり、総務省は理解を得られるように国民に周知。

3.2.2 「宅ふぁいる便」約 480 万件の個人情報漏えい[39-41]

- ○ 2019 年 1 月 24 日、株式会社オージス総研はファイル共有サービス「宅ふぁいる便」が不正アクセスを受けたことを発表。
- ○ 流出した情報は、氏名(ふりがな)、ログイン用メールアドレス、ログインパスワード等を含む約 480 万件の顧客情報。
- ○ 同社はその後、「パスワードを暗号化せずに保管していたこと」、「退会済の会員情報も漏えいしたこと」等を発表。

3.2.3 ホスティングサービスへの不正アクセスによる Web サイトの改ざん [42-44]

- ○ 大塚商会が提供するホスティングサービスへの不正アクセスにより、Web サイトの改ざんが発生。
- ○ 犯人はインターネット上の情報共有サイトに、本インシデントの犯行声明を掲載。
- ○ Web サイトのコンテンツを管理するソフトウエアの ID を踏み台にした Web サーバーの OS の脆弱性を利用した不正アクセスと判明。

---

[37] *総務省「国立研究開発法人情報通信研究機構法附則第 8 条第 2 項に規定する業務の実施に関する計画の認可(2019/1/25)」、http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00012.html (2019/2/20 閲覧)*

[38] *総務省「IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施(2019/2/1)」、http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html (2019/2/20 閲覧)*

[39] *オージス総研「宅ふぁいる便サービスの一時停止に関するお知らせとお詫び(2019/1/24)」、https://www.ogis-ri.co.jp/news/1268666_6734.html (2019/2/9 閲覧)*

[40] *オージス総研「(第 1 報)「宅ふぁいる便」サービスにおける不正アクセスによる、お客さま情報の漏えいについて(お詫びとお願い)(2019/1/25)」、https://www.ogis-ri.co.jp/news/1268714_6734.html (2019/2/9 閲覧)*

[41] *オージス総研「無料大容量ファイル転送サービス「宅ふぁいる便」 ご質問一覧(2019/1/31)」、https://www.ogis-ri.co.jp/news/takufile_faq.html (2019/2/10 閲覧)*

[42] *大塚商会「お客様ご利用の Web 環境に対する不正アクセス発生のご報告(2019/1/25)」、https://www.alpha-mail.jp/new/service/2019/0123_8402.html (2019/2/12 閲覧)*

[43] *Pastebin「Japanese Hosting Hijacked By Legion BOmb3r - Pastebin.com(2019/1/18)」、https://pastebin.com/y1NYPf0X (2019/2/12 閲覧)*

[44] *piyolog「国内ホスティングのっとりを主張する投稿について調べてみた(2019/1/23)」、http://d.hatena.ne.jp/Kango/20190123/1548169903 (2019/2/12 閲覧)*

3.2.4　T カードの会員情報の提供について[45-47]

○ 2019 年 1 月 20 日、「T カード」を展開するカルチュア・コンビニエンス・クラブ社が、会員情報等を令状なしに捜査当局へ提供していると報道。
○ 報道を受け、同社は同月 21 日、個人情報保護方針を改定。
○ 捜査関係事項照会書に応ずる個人情報の任意提供は、同様のサービスを提供する各社でも実施。

3.2.5 仮想通貨大規模流出事案その後[48-50]

○ 2018 年 1 月 26 日に 580 億円相当の仮想通貨を流出したコインチェック社(当時みなし業者)は、マネックスグループ社に買収された後、登録要件を満たしたことから 2019 年 1 月 11 日に仮想通貨交換業者に登録された。
○ 2018 年 9 月 14 日に 70 億円相当の仮想通貨を流出したテックビューロ社(仮想通貨取引所「Zaif」)は、同年 11 月 22 日にフィスコ仮想通貨取引所社(登録業者)に事業譲渡し、顧客資産は同社が返還等した。
○ 「crypto-asset」との表現が用いられつつある国際的な動向等を踏まえ、法令上「仮想通貨」の呼称を「暗号資産」に変更することが盛り込まれた法律が、2019 年 6 月に公布され、1 年以内に施行予定。

以上

---

[45] *共同通信「T カード情報令状なく捜査に提供(2019/1/20)」、https://this.kiji.is/459642838872769633?c=395467418394624 01/ (2019/2/19 閲覧)*
[46] *カルチュア・コンビニエンス・クラブ株式会社「個人情報保護方針を改訂いたしました(2019/1/21)」、https://www.ccc.co.jp/news/2018/20180121_005470.html (2019/2/19 閲覧)*
[47] *朝日新聞デジタル「T カードだけじゃなかった 個人情報提供どこまで(2019/2/4)」、https://www.asahi.com/articles/ASM236GYTM23UTIL01C.html (2019/2/20 閲覧)*
[48] *コインチェック社「仮想通貨交換業者登録に関するお知らせ(2019/1/11)」、https://corporate.coincheck.com/2019/01/11/63.html (2019/3/15 閲覧)*
[49] *フィスコ仮想通貨取引所社「Zaif 事業譲受の現状と今後のスケジュール(2019/12/26)」、http://www.fisco.co.jp/uploads/20181226_fisco_pr.pdf (2019/3/15 閲覧*
[50] *金融庁「国会提出法案等(2019/3/15)」、https://www.fsa.go.jp/common/diet/index.html (2019/3/15 閲覧))、情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律（令和元年法律第 28 号）*

重要インフラにおける情報共有件数について（2019 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	FY2015 計	FY2016 計	FY2017 計	FY2018 計	FY2019 1Q	2Q	3Q	4Q	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	－	－	－	48
関係省庁・関係機関からのNISCへの情報共有	52	41	19	7	6	－	－	－	6
NISCからの情報提供	44	80	54	43	10	－	－	－	10

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

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

（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、ネットワーク機器の不具合、内部の人的統制の不具合など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。

○　障害発生時にはリスクに応じた対応が必要

システムにおいて、取引自体には問題がないが、期間限定で表示上の問題が発生した際に、他への影響が発生するおそれがあることから、あえて改修せず、その旨顧客等に周知することにより対応した事例があった。

不具合に対応したシステム改修が、必ずしも最適解になるとは限らないことに留意。

○　閉鎖されたネットワーク内でもセキュリティ対策が必要

閉鎖されたネットワーク内で、USB メモリやメンテナンス用 PC 等の外部接続機器経由でマルウェアに感染、拡散した可能性がある事例があった。

組込機器・IoT 機器もマルウェアに感染するなどして悪用される可能性があることに留意。

○　侵入を前提として検知・対応できるシステム設計が必要

受信した不審メールの添付ファイルを実行したことによりマルウェアに感染し、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ほか、個人情報が流出した事例があった。

不審メールに対する個人の警戒意識だけでは限界があることに留意。

以上