資料４

令和２年 10 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 1 四半期） ····· 2
・重要インフラにおける情報共有件数について（2020 年度第 2 四半期） ····· 10
・最近のインシデントから得られた教訓 ····· 11

サイバーセキュリティを取り巻く情勢(2020 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、2020 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. 新型コロナウイルス感染症拡大下における国際情勢

1.1.1 香港・台湾・国連をめぐる情勢及び中国に対する米国の対応

- 新型コロナウイルスの影響により延期されていた中国全国人民代表大会が 2020 年 5 月に開幕し、香港への国家安全法制の導入を決定、翌 6 月 30 日、香港国家安全維持法が施行、中国は海外在住者を含む香港の民主活動家への取締りを強化[1]。
- 中国は各国が新型コロナウイルスへの対応に追われる中、台湾に対する圧力を強化、また世界保健機関(WHO)をはじめとする国連の場でも中国の影響力浸透が顕在化[2]してきており、米中対立は各国を巻き込む展開が加速。
- 米国は一国二制度を反故にした中国に対し、金融制裁を可能にする香港自治法を成立させた上、政府高官 4 名による激しい中国批判演説を実施、これまでの関与政策とは決別した強硬な対中姿勢を明確化[3]。

1.1.2 新型コロナウイルスワクチンを狙ったサイバー攻撃

- 2020 年 7 月、英米は開発が進む新型コロナウイルスのワクチン情報をロシアと中国がサイバー攻撃により窃取しようとしたとし非難[4]、米国は医療機関

---

[1] *共同通信「香港国家安全法を施行　最高刑は無期懲役(2020/7/1)」、https://this.kiji.is/650623006869095521 (2020/8/6 閲覧)*

[2] *日本経済新聞「国連、中国台頭が再燃　専門機関のトップ増加 (2020/3/9)」、https://www.nikkei.com/article/DGXMZO56561300Z00C20A3PP8000/ (2020/5/13 閲覧)*

[3] *現代ビジネス「ポンペオ長官"怒りの演説"が中国共産党に突きつけた「究極の選択」(2020/7/28)」、https://gendai.ismedia.jp/articles/-/74415?page=2 (2020/8/7 閲覧)*

[4] *AFP「ロシア、新型コロナワクチン研究機関にサイバー攻撃か　英米加が非難(2020/7/17)」、https://www.afpbb.com/articles/-/3294232 (2020/8/6 閲覧)*

の集積地があるヒューストンの中国総領事館に関し、知的財産権を守るための措置として中国に閉鎖命令。

- 今後の国際政治を左右する戦略物資としての新型コロナウイルスワクチンを欧米日露中が開発競争、発展途上国の中にはワクチンを目的に中国との領有権争いを棚に置き、歩み寄りを図る姿勢がみられる[5]。

1.2. サプライチェーンに関する国際動向

1.2.1 5G:中国製機器をめぐる攻防

- ファーウエイの急速なシェア拡大は、「グローバルサプライチェーンによる高性能部品の安価な調達ビジネスモデル」によるもので、米国はこのモデルを弱体化する政策を展開。
- 5 月の米国による新たなファーウエイ規制は、ファーウエイの半導体へのアクセスを阻止するもので、中国製機器の市場からの締め出しをさらに強化[6]。
- 一方で、中国通信機器メーカーの世界シェアや存在感を踏まえれば、その製品の使用禁止だけを掲げる手法では排除に限界があり、米国は、「O-RAN」など産業政策的な対策を模索[7]。
- これに対して、中国は、政府及び企業が結託して「脱アメリカ」を目指し、半導体の内製化・国産化をはじめとする巻き返しを企図。
- 他方、米国の追加規制等によって、英国は 5G 政策を転換し、中国離れが顕在化。
- 中国製機器排除は、中国の「脱アメリカ」を促し、その技術能力の向上につながるようにもみえ、米中対立を起因とするグローバルサプライチェーンの構造変化が予想。

1.2.2 米国の電力インフラにおけるサプライチェーンに関する大統領令

- 2020 年 5 月、トランプ米大統領は、基幹電力系統を潜在的な外国の敵対勢力によるサイバー攻撃等の脅威から保護することを目的として、EO13920「米国の基幹電力系統の確保」に署名[8]。
- EO13920 は、米国の送電網の機器調達において、国家安全保障、経済、人の健康、セキュリティと安全に対して重大なリスクがある場合に、機器の取得、

---

[5] *NHK「フィリピン大統領 中国に歩み寄り ワクチンとひきかえの見方も(2020/7/28)」、https://www3.nhk.or.jp/news/html/20200728/k10012537511000.html（2020/8/9 閲覧）*

[6] *JBpress「半導体の歴史に重大事件、ファーウエイは"詰んだ"(2020/6/1)」、https://jbpress.ismedia.jp/articles/-/60730（2020/6/4 閲覧）*

[7] *日経 xTECH「米国が迫るもう 1 つのファーウエイ包囲網、「Open RAN」連合(2020/6/3)」、https://xtech.nikkei.com/atcl/nxt/column/18/01308/00004/（2020/7/13 閲覧）*

[8] *National Archives 「Securing the United States Bulk-Power System(2020/5/1)」、https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system（2020/6/24 閲覧）*

譲渡、又は設置を禁止するもの。

- ○ 米国エネルギー省(DOE)は、大統領で示された規制と規制を策定するためのプロセスを開始し、2020 年 7 月、基幹電力系統のサプライチェーンを脅威から保護するため、情報提供要請を実施し、利害関係者からの意見を求めており、今年後半に規則案(NOPR:Notice Of Proposed Rulemaking)を公開予定。
- ○ 今回の大統領令 EO13920 は、2019 年 5 月に、外国勢力により生産、提供、管理、支配されたICT技術又はサービスを伴う取引を禁止する EO13873「ICT に関するサプライチェーンに対する大統領令」と多くの点で類似しており、今後、公開される規則案では、同様に具体的な規制対象等が示されると推察。なお、対象として基幹電力に限定している。

1.3. 中国

1.3.1 香港国家安全維持法の施行

- ○ 香港の返還記念日であり毎年デモが恒例化している 7 月 1 日を前に、2020 年 6 月 30 日 23 時、中国政府は「中華人民共和国香港特別行政区国家安全維持法」(香港国家安全維持法)を公布と同時に施行[9]。
- ○ 同法は、国家分裂等 4 類型の犯罪を明示し、中国政府が関与し取締りを強化するための新組織の設立等を規定する他、域外適用により海外在住の香港人のみならず外国人も処罰の対象[10]。
- ○ 同法の施行に対し、米政府は非難、2020 年 7 月 14 日には金融機関への制裁を可能にする香港自治法を成立させ、英国・オーストラリア・ドイツなどの複数か国は香港との間での犯罪人引渡し条約を停止[11]。

1.3.2 中国サイバーセキュリティ審査弁法の施行

- ○ 2017 年 6 月 1 日、中国政府はサイバーセキュリィティ法を施行し、同日付で「インターネット製品及びサービス安全審査弁法(施行)」を施行。なお審査弁法とは、審査事務規則のことであり、日本の省令に相当。
- ○ 米中両国の覇権争いにおいて、2018 年以降、ネットワーク関連機器の調達等を制限する規則の応酬が続く中、2020 年 6 月 1 日、中国政府は、「インターネット製品及びサービス安全審査弁法(施行)」を廃止し、新たに「サイバ

---

[9] *共同通信「香港国家安全法を施行 最高刑は無期懲役(2020/7/1)」、https://this.kiji.is/650623006869095521 (2020/8/6 閲覧)*

[10] *東洋経済「香港・国家安全維持法、条文で読む深刻事態(2020/7/8)」、https://toyokeizai.net/articles/-/361267 (2020/8/9 閲覧)*

[11] *BBC「イギリス政府、香港との犯罪人引き渡しを停止～国安法受け(2020/7/21)」(2020/10/7 閲覧)、https://www.bbc.com/japanese/53481978*

ーセキュリティ審査弁法」を施行[12]し、中国の重要情報インフラ事業者によるネットワーク製品又はサービスの調達に対して、国家の安全に影響を及ぼす可能性がある場合の安全審査義務を規定[13]。

- 重要情報インフラ運営者は、調達の文書、合意書等を通じて、重要情報インフラ運営者へ製品・サービスを提供する者に対して、審査への協力を求め[14]、審査においては、ネットワーク製品・サービスの調達がもたらし得る国の安全へのリスクを重点的に評価。

1.4. オーストラリア

1.4.1 オーストラリアに対するサイバー攻撃

- 2020 年 4 月、オーストラリアが新型コロナウイルスの発生源調査を世界に呼びかけたところ、中国はオーストラリア産農産物に制裁措置を採るなど反発[15]。
- 2020 年 6 月 19 日、オーストラリアのモリソン首相は、自国の政府及び商業ネットワークに対して国家の関与が疑われるサイバー攻撃が発生していることを公表[16]。
- 同日、オーストラリアサイバーセキュリティセンター(ACSC)が、国家の関与が疑われるサイバー攻撃の攻撃手口や推奨する対策をまとめたアドバイザリーを公開[17]。

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 イラン・イスラエルをめぐる情勢

- 2020 年 4 月、イスラエルの水道施設がサイバー攻撃により一時停止、イスラエル国家サイバー総局は、初の実生活へ損害を及ぼすためのサイバー攻

---

[12] *中国国家インターネット情報弁公室「サイバーセキュリティ審査弁法(2020/4/27)」、http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm（2020/5/15 閲覧）*

[13] *JETRO「サイバーセキュリティー審査弁法、6 月 1 日より施行（2020/6/5）」(2020/10/7 閲覧)、https://www.jetro.go.jp/biznews/2020/06/0bbe3511d7dec13d.html*

[14] *Wall Street Journal「中国、IT 機器調達で新規定 米企業に悪影響か(2020/4/28)」、https://jp.wsj.com/articles/SB11818665177578993922304586349940449774096?mg=prod/com-wsj&mg=prod/com-wsj（2020/5/1 閲覧）*

[15] *時事通信「豪、中国との対立激化 日本やインドと連携（2020/6/14)」、https://www.jiji.com/jc/article?k=2020061300309（2020/7/14 閲覧）*

[16] *日本経済新聞「豪の政府機関にサイバー攻撃 中国関与と現地報道（2020/6/19)」、https://www.nikkei.com/article/DGXMZO60539550Z10C20A6EAF000/（2020/9/30 閲覧）*

[17] *ACSC「Advisory 2020-008: Copy-paste compromises – tactics, techniques and procedures used to target multiple Australian networks (2020/6/19)」、https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks（2020/7/1 閲覧）*

撃であったと分析[18]。

- 2020 年 5 月、イラン南部のシャヒド・ラジャイ港をイスラエルがサイバー攻撃、また 2020 年 7 月、イラン中部ナタンズの核濃縮施設で火災発生、イスラエル関与の疑惑[19]。
- 2020 年 10 月に予定されるイランへの武器禁輸措置の解除と 2020 年 11 月の米国大統領選挙を見据え、トランプ氏が大統領の間にイランの核開発能力をそぎたいイスラエルと、バイデン氏に米国の核合意復帰と制裁解除を期待するイランの思惑が交錯[20]。

2.2. 重要インフラ関連

2.2.1 ランサムウエア「Maze」の脅威

- ランサムウエア「Maze」は、暗号化による「身代金」の要求と、内部情報の公開の 2 段階で金銭を要求[21]。
- これまで日本企業の被害が報告されていなかったが、2020 年 7 月に日本企業の情報が公開された[22]。
- これまでのランサムウエア対策では、事前に取得したバックアップでデータ等の復旧が可能であった。「Maze」による攻撃においては、窃取された機微情報が公開されるリスクがあり、新たな対策が必要[23]。

2.2.2 ランサムウエア「EKANS」の分析について

- 2020 年 6 月に国内外の特定の企業を対象としたランサムウエア「EKANS」とみられるサイバー攻撃による被害が明らかになった。
- ウイルストータルにアップロードされた EKANS の検体に対し、セキュリティベンダーが分析を実施[24]した結果、EKANS はマルチプラットフォームで開発可能な「Go 言語」で作成され、標的のみに攻撃を仕掛け、暗号化中に正規の Windows ファイアウォールを利用してネットワーク通信を妨害することなどが

---

[18] *東洋経済「「イスラエル・イラン」サイバー攻撃応酬の実態 各国の「能力強化、人材選抜方法」の中身とは(2020/6/13)」、https://toyokeizai.net/articles/-/355528 (2020/7/8 閲覧)*

[19] *REUTER「イラン、核施設へのサイバー攻撃に報復表明 濃縮施設の火災受け(2020/7/4)」、https://jp.reuters.com/article/iran-nuclear-natanz-idJPKBN2442I0 (2020/7/8 閲覧)*

[20] *NHK「「再び『一触即発』 イラン情勢」(時論公論) (2020/7/31)」、https://www.nhk.or.jp/kaisetsu-blog/100/433619.html (2020/8/13 閲覧)*

[21] *ProofPoint 「TA2101 plays government imposter to distribute malware to German, Italian, and US organizations(2019/11/14)」、https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us (2020/7/7 閲覧)*

[22] *日経クロステック(xTECH)「愛知の車部品企業で情報漏洩、標的型のランサムウエアに感染か(2020/7/17)」、https://xtech.nikkei.com/atcl/nxt/news/18/08380/ (2020 年 7 月 20 日閲覧)*

[23] *NCFTA「Maze Ransomware(2019/12/2)」、https://1f3r982zgpjh2wuihs3suki9-wpengine.netdna-ssl.com/wp-content/uploads/2019/12/Maze_Whitepaper.pdf (2020/7/7 閲覧)*

[24] *三井物産セキュアディレクション「SNAKE(EKANS)ランサムウエアの内部構造を紐解く(2020/6/16)」、https://www.mbsd.jp/blog/20200616.html (2020/7/6 閲覧)*

判明。

2.3. その他

2.3.1 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

- ○ 新型コロナウイルス感染症拡大に伴い、各国で外出規制等を実施。
- ○ 対策支援の一環で、スマートフォンの位置情報ビックデータを活用して人流変化を分析[25]。
- ○ 一方、新型コロナウイルスに便乗するマルウエア等の脅威が出現[26]。

2.3.2 遠隔会議システムの普及に伴う様々な問題

- ○ 2020 年 4 月、米 Google 社、米 Facebook 社等が遠隔会議向けサービスを拡充するなど、各事業者等で遠隔会議システムの利用が活発化[27]。
- ○ 他方、遠隔会議システムの普及とともに、セキュリティ上の問題が顕在化[28]。

2.3.3 テレワークで利用される VPN について

- ○ 新型コロナウイルス感染症への対応のためテレワークが広がっており、VPN の利用が増加。
- ○ VPN は、リモートアクセスの際に利用される手法の一つ。脆弱性に対する適切な管理が必要[29]。

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 大量の政府機関等偽サイトの出現

- ○ 政府機関、自治体、民間企業等の Web サイトを模倣した偽サイトが大量に出現。
- ○ 偽サイト作成の目的は不明であるものの、詐欺などに利用される可能性があるとして各組織が注意喚起を発出。
- ○ 発見された偽サイトには、そっくりコピーされている点、ドメインが特定の国で

---

[25] *新型コロナウイルス感染症対策「統計情報」、https://corona.go.jp/dashboard/（2020/5/19 閲覧）*

[26] *三井物産セキュアディレクション「新型コロナに便乗する CoronaVirus ランサムウエアと Kpot 情報窃取マルウエア(2020/4/3)」、https://www.mbsd.jp/blog/20200403.html（2020/5/18 閲覧）*

[27] *マイナビニュース「Facebook の Web 会議「Messenger Rooms」の使い方 - Zoom とどう違う？(2020/5/19)」、https://news.mynavi.jp/article/20200519-1037315/（2020/9/30 閲覧）*

[28] *NHK「ネットのテレビ会議急増 専門家「セキュリティー対策を」(2020/4/9)」、https://www3.nhk.or.jp/news/html/20200409/k10012377491000.html（2020/10/12 閲覧）*

[29] *米国サイバーセキュリティ・インフラセキュリティ庁(CISA)「Alert（AA20-073A）Enterprise VPN Security（2020/3/13 発行、4/15 改訂)」、https://www.us-cert.gov/ncas/alerts/aa20-073at（2020/5/19 閲覧）*

ある点等の共通点が存在[30]。

3.1.2 特別定額給付金・雇用調整助成金オンライン申請関連トラブル

- 「特別定額給付金」について、早い自治体では 2020 年 5 月 1 日からオンライン申請を開始したが、オンライン申請に必要なマイナンバーカードの電子証明書関係手続の処理遅延[31]、申請者の重複申請[32]等のトラブルが発生。
- 厚生労働省は「雇用調整助成金」について、2020 年 5 月 20 日からオンライン申請を開始したが、運用開始直後にシステムの不具合が見つかり、運用を停止[33]。

3.1.3 新型コロナウイルス感染症接触通知システムの開発

- 新型コロナウイルス感染症の感染拡大防止のため、スマートフォンを利用した感染者と濃厚接触した可能性を通知する仕組みを構築[34]。
- 政府(厚生労働省)は、米 Apple 社 iOS と米 Google 社 Android の API を採用した Bluetooth を用いた新型コロナウイルス接触確認アプリ(COCOA)を開発、2020 年 6 月 19 日にリリース[35]。
- 複数の自治体は、QR コードを用いたコロナ追跡システムを開発[36]。

3.2. 重要インフラ関連

3.2.1 相次ぐクラウドサービスの障害

- 2020 年 5 月末から 6 月にかけて、クラウドサービスの障害が相次いで発生。
- クラウドサービスを利用していた自治体[37]や金融機関[38]等の重要インフラ事業者等でも、サービス障害が発生する等影響が波及。

---

[30] *朝日新聞「官邸も新聞社も…偽サイトが大量に出現　誰が何のために(2020/5/13)」、https://digital.asahi.com/articles/ASN5F64BQN5FULZU011.html（2020/6/15 閲覧）*

[31] *地方公共団体システム機構(J-LIS)「【お詫び】マイナンバーカードの電子証明書関係手続の混雑と処理遅延について(2020/5/12)」、https://www.j-lis.go.jp/about/announce/information20200512.html（2020/6/13 閲覧）*

[32] *読売新聞「10 万円オンライン申請でミス多発、6 割に不備…市が郵送に一本化(2020/5/19)」、https://www.yomiuri.co.jp/national/20200519-OYT1T50185/（2020/6/16 閲覧）*

[33] *朝日新聞「雇用助成金のオンライン申請を停止　開始初日にトラブル(2020/5/20)」、https://www.asahi.com/articles/ASN5N5VR4N5NULFA01F.html（2002/6/16 閲覧）*

[34] *厚生労働省「新型コロナウイルス接触確認アプリ　COVID-19 Contact-Confirming Application」、https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html（2020/6/19 閲覧）*

[35] *政府 CIO ポータル「接触確認アプリに関する仕様書等の公表」、https://cio.go.jp/node/2613（2020/6/19 閲覧）*

[36] *大阪府「5 月 29 日より「大阪コロナ追跡システム」の運用を開始します(2020/5/27)」、http://www.pref.osaka.lg.jp/hodo/index.php?site=fumin&pageId=38278（2020/6/19 閲覧）*

[37] *日経 xTECH「日本電子計算の自治体クラウドで障害、アップデート中に「想定外の事象が発生」(2020/6/1)」、https://xtech.nikkei.com/atcl/nxt/news/18/08006/（2020/7/2 閲覧）*

[38] *日経 xTECH「みずほ銀や住信 SBI でもシステムトラブル、IBM Cloud の障害の影響か（2020/6/10)」、https://xtech.nikkei.com/atcl/nxt/news/18/08081/（2020/7/2 閲覧）*

3.2.2 「お名前.com Navi」の不具合によるドメイン名ハイジャック

- 2020 年 6 月に、コインチェック及びビットバンクにおいて、第三者にドメイン登録情報が変更される事象(ドメイン名ハイジャック)が発生。
- 原因は、利用していたドメイン登録サービス「お名前.com Navi」における通信の改ざん[39]。

3.3. その他

3.3.1 「OpenSSL」の深刻な脆弱性(CVE-2020-1967)

- 2020 年 4 月に、OpenSSL Project は「OpenSSL」に関する深刻な脆弱性(CVE-2020-1967)を公開[40]。
- CVE-2020-1967 は、「OpenSSL」を実行するサーバーアプリケーションやクライアントアプリケーションをリモートからクラッシュさせることができる脆弱性として、US-CERT 等が最新版への更新を呼びかける注意喚起を実施。

3.3.2 DNS サーバーに関する深刻な脆弱性

- 2020 年 5 月、インターネット上でドメイン名を管理・運用する DNS(Domain Name System)の脆弱性を悪用する新たな攻撃手法「NXNS 攻撃」が公開[41]。
- さらに、DNS ソフトウエア「BIND」で、名前解決できなくなる脆弱性(CVE-2020-8617)が公開[42]。
- いずれの脆弱性も、可用性に影響は大きいが、機密性や完全性への影響はない。

3.3.3 多くのデバイスが影響を受ける脆弱性「Ripple20」

- 2020 年 6 月 16 日、ICS-CERT は、多くのデバイスが影響を受ける TCP/IP ライブラリに関する 19 個の脆弱性「Ripple20」のアドバイザリーを発行[43]。
- Ripple20 の脆弱性は、利用しているシステムや機器のサプライチェーンに関する問題となる可能性[44]。
- Ripple20 の概要を把握するとともに必要な対応を検討する必要。

以上

---

[39] コインチェック「当社利用のドメイン登録サービス「お名前.com」で発生した事象について(最終報告)(2020/6/4)」、https://corporate.coincheck.com/2020/06/04/98.html (2020/7/6 閲覧)

[40] OpenSSL Project「OpenSSL Security Advisory [21 April 2020] (2020/4/21)」、https://www.openssl.org/news/secadv/20200421.txt (2020/5/7 閲覧)

[41] Lior Shafir、Yehuda Afek、Anat Bremler-Barr、「NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities (2020/5/19)」、http://www.nxnsattack.com/shafir2020-nxnsattack-paper.pdf (2020/6/4 閲覧)

[42] ISC「CVE-2020-8617: A logic error in code which checks TSIG validity can be used to trigger an assertion failure in tsig.c (2020/5/19)」、https://kb.isc.org/docs/cve-2020-8617 (2020/6/4 閲覧)

[43] ICS-CERT「ICS Advisory (ICSA-20-168-01) -Treck TCP/IP Stack-(2020/8/4)」,https://www.us-cert.gov/ics/advisories/icsa-20-168-01(2020/8/11 閲覧)

[44] 内閣サイバーセキュリティセンター「多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報」、https://www.nisc.go.jp/active/infra/pdf/Ripple2020200624.pdf (2020/8/18 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 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	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	－	－	136
関係省庁・関係機関からのNISCへの情報共有	41	19	7	16	4	6	－	－	10
NISCからの情報提供	80	54	43	38	11	8	－	－	19

※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	－	－	7
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	－	－	9
	完全性を脅かす事象	情報の破壊	47	20	17	11	4	4	－	－	8
	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	－	－	80
	上記につながる事象	マルウェア等の感染	289	65	17	9	4	4	－	－	8
		不正コード等の実行	10	13	4	5	0	1	－	－	1
		システム等への侵入	26	17	14	14	1	3	－	－	4
		その他	44	35	34	47	6	13	－	－	19

※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	－	－	6
	ユーザＩＤ等の偽り	1	4	3	12	0	5	－	－	5
	DDoS攻撃等の大量アクセス	23	31	17	20	4	3	－	－	7
	情報の不正取得	14	16	10	8	3	2	－	－	5
	内部不正	0	4	1	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
偶発的な原因	ユーザの操作ミス	15	23	10	6	4	5	－	－	9
	ユーザの管理ミス	8	13	6	6	3	0	－	－	3
	不審なファイルの実行	243	42	16	7	0	4	－	－	4
	不審なサイトの閲覧	29	20	4	5	0	1	－	－	1
	外部委託先の管理ミス	20	41	29	39	9	12	－	－	21
	機器等の故障	22	32	27	62	10	11	－	－	21
	システムの脆弱性	56	36	19	16	3	3	－	－	6
	他分野の障害からの波及	0	10	6	4	2	2	－	－	4
環境的な原因	災害や疾病等	0	0	1	13	0	7	－	－	7
その他の原因	その他	34	29	29	33	9	9	－	－	18
	不明	92	57	46	53	18	14	－	－	32

（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

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、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。

○　サービスや利用者属性追加の際にはリスクの見直しが必要

追加したサービスや利用者属性における認証設計の弱さを突いた不正アクセスにより、サービスを不正利用された事例が多数あった。

○　マルウエア Emotet 対策は依然必要

受信メールの添付ファイルの開封により Emotet に感染した事例が複数あった。

また、メール送信先等の Emotet 感染によるメール関連情報の窃取により、自組織を騙る不審メールが出回った事例が多数あった。

パスワード付き ZIP ファイルにより、途中の検知をすり抜けてくることがあることに留意。

○　設定どおりの稼働の確保、切替手順の事前確認と訓練の実施が必要

システムに障害が発生した際、冗長化したバックアップシステムに切り替わらず、長時間にわたりサービスを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や自然災害に対する再点検が必要

利用する外部サービスの停止や自然災害による停電・断線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。

多重化や代替手段による多様化等の強靭性確保にも留意。

以上