資料５

令和２年１月 29 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 2 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 2 四半期(7 月～9 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 米国の戦略と中国の動向[1-6]

- ○ 中国は、共産党一党独裁体制の下、不公正な手段による経済・軍事面で急激に拡大。中でも「一帯一路」は、中国主導の経済・外交圏構想であり、アジア、中東、東欧諸国に対するインフラ投資により当該地域の貿易、投資を活性化し、ユーラシア地域の経済を一体化することが目的。
- ○ 米国は、「一帯一路」が中国主導で新たな経済圏を創出することで自国の地政学的影響力を高め、最終的に自国を世界秩序の中心に据えることを目的としていると批判し、中国の一党独裁体制に影響を与えるべく、対中国関税の段階的引上げ、「インド太平洋戦略」の公表、香港及び台湾を支援する法案準備等の対抗策を実施。

---

[1] *AFP「中国「一帯一路」、構想の現状と今後の見通し(2019/5/2)」、https://www.afpbb.com/articles/-/3223182(2019/8/5 閲覧)*

[2] *AFP「【図解】中国が進める「一帯一路」構想(2017/5/15)」、https://www.afpbb.com/articles/-/3128278 (2019/8/20 閲覧)*

[3] *みずほ銀行「「ADB」と「AIIB」の違いって？ 変化しつつあるアジアの金融事情(2016/12/13)」、https://money-campus.net/archives/1697(2019/11/13 閲覧)*

[4] *現代ビジネス「米副大統領の演説は、実は対中国への「本気の宣戦布告」だった(2019/8/16)」、https://gendai.ismedia.jp/articles/-/57929 (2019/8/16 閲覧)*

[5] *Bloomberg「米上院、香港人権法案を早期採決目指す-中国の警告よそに(2019/10/23)」、https://www.bloomberg.co.jp/news/articles/2019-10-23/PZSRM0T0G1L601(2019/10/23 閲覧)*

[6] *THE WALL STREET JOUNAL「【社説】中国の台湾いじめ、対抗する米上院(2019/10/7) 」、https://jp.wsj.com/articles/SB12480707376259223915504585595712236321580(2019/10/22 閲覧)*

1.1.2 中東地域の動向に対する米国の戦略[7-11]

- ○ 米国は、現行の 15 年間としているイラン核合意では不十分として、新たな核合意締結を目指し、現行の核合意を離脱し経済制裁を行いつつ、対話を試行していたところ、2019 年 9 月のサウジアラビア石油施設への攻撃により、対話が困難化。
- ○ 2020 年 11 月の米国大統領選挙戦を控え、中東地域への積極的な関与から撤退しようとしている米国の姿勢を念頭に、イランに続きトルコも行動を一段と具体化、米国は同盟諸国からの信頼を低下させる状況となっており、中東情勢は一層不透明化。

1.2 国連

1.2.1 北朝鮮のサイバー活動(国連安保理北朝鮮制裁委員会専門家パネル報告書) [12-13]

- ○ 国連安保理北朝鮮制裁委員会専門家パネルが北朝鮮制裁に係る安保理決議に基づき作成した報告書が公表。
- ○ 本報告書は北朝鮮による制裁逃れの実態のほか、マイニング等のサイバー活動についても記載。
- ○ 北朝鮮は報告書の記載内容を否定。

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 NIST による政府機関のサプライチェーンに関する文書のドラフトの公表[14-16]

---

[7] *BBC「トランプ大統領、イラン核合意からの離脱を発表　欧州説得実らず(2018/5/9)」、https://www.bbc.com/japanese/44049644(2019/9/29 閲覧)*

[8] *CNN「サウジの石油施設にドローン攻撃、生産半減　フーシが犯行声明(2019/9/15)」、https://www.cnn.co.jp/world/35142690.html(2019/10/22 閲覧)*

[9] *日本経済新聞「トルコ、親米クルド人勢力を攻撃 シリア北東部(2019/10/9)」、https://www.nikkei.com/article/DGXMZO50817670Z01C19A0FF8000/ (2019/10/22 閲覧)*

[10] *朝日新聞「米軍、シリア北部の撤退開始 クルド人を切り捨てる形に(2019/10/8)」、https://www.asahi.com/articles/photo/AS20191007003700.html (2019/10/22 閲覧)*

[11] *NHK NEWS WEB「トランプ大統領 トルコへの制裁解除発表 シリアでの攻撃停止で(2019/10/24)」、https://www3.nhk.or.jp/news/html/20191024/k10012145991000.html (2019/10/24 閲覧)*

[12] *国連「Report of the Panel of Experts established pursuant to resolution 1874 (2009) (2019/8/30)」、https://undocs.org/S/2019/691(2019/10/21 閲覧)*

[13] *日本経済新聞「R 北朝鮮のサイバー攻撃、韓国など 17 カ国に　国連報告書(2019/9/6)」、https://www.nikkei.com/article/DGXMZO49487370W9A900C1000000/(2019/10/21 閲覧)*

[14] *NIST「SP800-171:Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations(2018/6/7)」、https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final(2019/8/14 閲覧)*

[15] *SP800-171B の他に、SP800-171A「Assessing Security Requirements for Controlled Unclassified Information」が発行されている。*

[16] *NIST は、同時に SP800-171 の最新版である SP800-171 Rev.2 のドラフトも公開し、同様にパブリックコメントを開始した。こちらは、編集上の表記等マイナー変更のみで内容に関する変更点はない。*

- SP800-171 は、米国連邦政府機関が調達する製品や技術等を開発・製造する企業に対して、一定のセキュリティ基準に準拠するように求めるガイドラインであり、米国連邦政府機関のサプライチェーンに関する要件についての文書で 2017 年に制定。
- SP800-171 は、米国連邦政府機関全体として CUI(管理すべき非格付の情報: Controlled Unclassified Information)のセキュリティ強化を行うものであり、非政府機関の情報システム等における CUI の保護を目的としたサイバーセキュリティ対策の要件を規定。
- SP800-171B は、既存の SP800-171 に上乗せする形で、CUI が重要なプログラムまたは高価値資産(High Value Assets(VA))の一部である場合、先進的で執拗な脅威(Advanced Persistent Threat: APT)から保護するための追加のセキュリティ要件を提供。
- NIST は 2019 年 6 月から 8 月までパブリックコメントを実施。

2.2 重要インフラ関連

2.2.1 ランサムウエアの標的とされる米国自治体[17-20]

- 米国の自治体を標的としたランサムウエア攻撃が活発化。
- 一部の自治体は身代金を支払い。
- 全米市長会議はランサムウエア攻撃に対する身代金支払い拒否を決議。

2.3 その他

2.3.1 NIST によるオンライン取引の多要素認証に関するガイドの公表[21-22]

- 2019 年 7 月、NIST はオンライン小売事業者向けに、オンライン取引における多要素認証導入のための実践的なガイド SP1800-17 を公表。
- 本人認証に利用される本人固有の情報は、知識情報、所持情報、生体情報の 3 つに分類され、セキュリティを強化するには少なくとも 2 つの異なるカテゴリの情報の提示が必要としている。
- 本ガイドは、多要素認証導入のためのアーキテクチャに加え、その中で紹介された標準的なサービスについて、多要素認証を導入するための考え方か

---

17 *「Early Findings: Review of State and Local Government Ransomware Attacks(2019/5/10)」、https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf (2019/8/19 閲覧)*

18 *「フロリダの小都市、ランサムウエアに屈する--身代金約 6440 万円を支払いへ(2019/6/21)」、https://japan.zdnet.com/article/35138825/(2019/8/19 閲覧)*

19 *「ランサムウエアに屈した地方自治体が IT 担当職員を解雇--フロリダ州レイク・シティ(2019/7/2)」、https://japan.zdnet.com/article/35139315/(2019/8/19 閲覧)*

20 *「全米市長会議、ランサムウエア攻撃で身代金支払い拒否へ--年次総会で決議採択 (2019/7/16)」、https://japan.zdnet.com/article/35139937/(2019/8/19 閲覧)*

21 *NIST「SP1800-17 Multifactor Authentication for E-Commerce(2019/7/30)」、https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf (2019/9/11 閲覧)*

22 *本ガイドの中で一連の市販製品を紹介しているが、これらの特定の製品を推奨するものではないとの注意書きもあり、あくまでオンライン小売事業者が多要素認証を導入するための出発点として本ガイドを使用できるとしている。*

ら導入手順までを説明する小売事業者向けの実践的なガイド。

2.3.2 NIST SP800-207 ゼロトラストアーキテクチャ[23]

- NIST は、ゼロトラストアーキテクチャに関する文書「NIST SP800-207 Zero Trust Architecture」のドラフト版を公開しコメントを募集。
- ゼロトラストアーキテクチャとは、高度化する脅威に対するネットワークアーキテクチャで、従来の境界ネットワークで保護するものに対し、モバイル等のアクセスの多様化やクラウドサービスの導入など変化する IT 環境に対応しながら、組織のデータとリソースを保護し、組織の生産性を高めるためのもの。
- ドラフト版では、ゼロトラストアーキテクチャに関して、その論理的なコンポーネント、可能な展開シナリオ、脅威を定義し、移行へのロードマップを提示。

2.3.3 VxWorks のゼロデイ脆弱性「URGENT/11」[24-26]

- 2019 年 7 月 29 日 Armis 社は、リアルタイム OS「VxWorks」の 11 個のゼロデイ脆弱性「URGENT/11」を発見したと発表。
- VxWorks は、制御システム、産業機器、医療機器、通信機器等、20 億以上の機器に搭載。
- URGENT/11 によって影響を受ける機器は 2 億台以上。

2.3.4 Facebook の暗号資産 Libra[27-28]

- 2019 年 6 月 18 日、Facebook 社が主導する「Libra 協会」は、独自の暗号資産「Libra」のホワイトペーパー(概要書)を、2020 年前半の運用開始を目指し、公表。
- Libra は、他の暗号資産と同様ブロックチェーンを用いるものの、Libra リザーブによる資産の裏付けから価格変動率が小さいステーブルコイン。
- G20 では Libra を含むグローバル・ステーブルコインに対し、政策や規制上の深刻なリスクを生むことを指摘。

---

[23] *NIST「SP800-207(Draft) Zero Trust Architecture(2019/9)」、https://csrc.nist.gov/publications/detail/sp/800-207/draft (2019/10/18 閲覧)*

[24] *MONOist「「VxWorks」にゼロデイ脆弱性、「URGENT/11」は 2 億個のデバイスに影響(2019/7/30)」、https://monoist.atmarkit.co.jp/mn/articles/1907/30/news047.html(2019/9/9 閲覧)*

[25] *Wind River Systems「Wind River Ranked Global Leading Provider of Embedded Operating Systems(2019/3/12)」、https://www.windriver.com/japan/news/press/2019/190329_WR.html(2019/9/24 閲覧)*

[26] *Armis「Security Disclosure: URGENT/11」, https://www.armis.com/urgent11/(2019/9/17 閲覧)*

[27] *Libra 協会「Libra White Paper(2019/6/18)」、https://libra.org/en-US/white-paper/、https://libra.org/ja-JP/white-paper/(2019/9/24 閲覧)*

[28] *金融庁「グローバル・ステーブルコインに関する G20 プレスリリース(2019/10/17,18)」、https://www.fsa.go.jp/inter/etc/20191021_2/1.pdf、https://www.fsa.go.jp/inter/etc/20191021_2/2.pdf (2019/11/14 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 インシデント発生時の情報発信[29-30]

- ○ 台風 15 号による千葉県を中心とする大規模な長期停電発生に対して、東京電力は早期の復旧見込みとアナウンスしたが、結果的にそれが実現できず、利用者からの不満が続出。
- ○ ドコモメールのサービス障害が発生した際、障害情報発信の遅さに対して、利用者からの不満が続出。
- ○ これらの事案は、重要インフラにおけるサービス障害発生時において、利用者に対して、適時的確な情報発信を行うことが重要であることを示唆。

3.2 その他

3.2.1 QR コード決済サービス 7pay の不正利用[31-33]

- ○ 2019 年 7 月 1 日、QR コード決済サービス 7pay がサービス開始。
- ○ 不正利用された旨の問合せがあったことから、同月 3 日以降、クレジット/デビットカードによるチャージ、現金によるチャージ、新規会員登録を順次停止。
- ○ 同年 8 月 1 日セブン・ペイ社は、同年 9 月末で同サービスを終了すると発表。

3.2.2 d 払いの不正利用から見えるスマホ決済サービスの問題点[34-37]

- ○ 2019 年 6 月から 8 月にかけて、NTT ドコモは、同社のスマホ決済サービスである d 払い等で使用される d アカウントにおいて、不正アクセスに係る事象を確認し、複数回にわたり注意等を発信。
- ○ NTT ドコモユーザーに対するスミッシングにより、第三者が ID やパスワードを不正入手し、Amazon で d 払いを不正利用。
- ○ クレジットカードの場合と異なり、スマホ決済サービスで不正利用の被害に遭った場合は、消費者を救済する制度が不十分。

---

29 FNN PRIME「台風 15 号直撃から一ヶ月…なぜ東京電力の復旧見通しは二転三転したのか？(2019/10/10)」、https://www.fnn.jp/posts/00048486HDK/201911301200_hikariide_HDK(2019/10/17 閲覧)

30 iPhone Mania「ドコモメールで 22 日朝から大規模な通信障害発生 メール受信ができず(2019/9/22)」、https://iphone-mania.jp/news-261382/ (2020/1/20 閲覧)

31 セブン・ペイ「セブン&アイのバーコード決済「7pay（セブンペイ）」本日サービススタート！(2019/7/1)」、https://www.7pay.co.jp/news/news_20190701_01.pdf(2019/8/15 閲覧)

32 セブン・ペイ「一部アカウントへの不正アクセス発生によるチャージ機能の一時停止について(2019/7/4)」、https://www.7pay.co.jp/news/news_20190704_01.html(2019/8/15 閲覧)

33 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)

34 株式会社 NTT ドコモ「インターネットサービス「ドコモを装ったフィッシング SMS にご注意ください！(2019/6/17)」、https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/(2019/8/7 閲覧)

35 piyolog「d 払い不正利用の被害報告総額を調べてみた(2019/8/4)」、httpspiyolog.hatenadiary.jp/entry/2019/08/04/011910 (2019/8/5 閲覧)

36 株式会社 NTT ドコモ「Amazon における d 払い設定時の認証方法変更について(2019/8/9)」、https://service.smt.docomo.ne.jp/keitai_payment/info/info_20190809.html (2019/8/14 閲覧)

37 日本経済新聞「スマホ決済の不正被害、「補償」8 割明記なし(2019/7/24)」、https://www.nikkei.com/article/DGXMZO47686670T20C19A7EE9000/ (2019/8/15 閲覧)

3.3.3　Amazon Web Service の大規模障害[38-39]

○　2019 年 8 月 23 日、米 Amazon 社のクラウドサービス AWS の東京リージョンで、データセンターの空調設備の障害を原因とした大規模な障害が約 6 時間にわたり発生。

○　AWS を利用して提供される国内の多種多様なサービスに影響。

以上

[38] *Amazon Web Services「東京リージョン（AP-NORTHEAST-1）で発生した Amazon EC2 と Amazon EBS の事象概要（2019/8/25）」、https://aws.amazon.com/jp/message/56489/（2019/9/19 閲覧）*

[39] *日本経済新聞「クラウド集中にもろさ　アマゾン「AWS」大規模障害（2019/8/23）」、https://www.nikkei.com/article/DGXMZO48956120T20C19A8EA1000/（2019/9/19 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 3 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	111	－	216
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	－	15
NISCからの情報提供	44	80	54	43	10	8	8	－	26

※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	－	9
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	－	10
	完全性を脅かす事象	情報の破壊	52	47	20	17	4	3	1	－	8
	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	－	130
	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	－	8
		不正コード等の実行	11	10	13	4	1	1	1	－	3
		システム等への侵入	27	26	17	14	4	5	3	－	12
		その他	24	44	35	34	10	13	13	－	36

※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	－	11
	ユーザＩＤ等の偽り	8	1	4	3	1	5	6	－	12
	DoS攻撃等の大量アクセス	47	23	31	17	3	4	7	－	14
	情報の不正取得	8	14	16	10	0	3	2	－	5
	内部不正	2	0	4	1	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	－	10
偶発的な原因	ユーザの操作ミス	10	15	23	10	2	3	1	－	6
	ユーザの管理ミス	5	8	13	6	4	0	0	－	4
	不審なファイルの実行	51	243	42	16	3	1	2	－	6
	不審なサイトの閲覧	49	29	20	4	1	2	2	－	5
	外部委託先の管理ミス	12	20	41	29	8	4	18	－	30
	機器等の故障	17	22	32	27	3	4	47	－	54
	システムの脆弱性	29	56	36	19	5	3	3	－	11
	他分野の障害からの波及	5	0	10	6	0	0	4	－	4
環境的な原因	災害や疾病等	0	0	0	1	0	13	0	－	13
その他の原因	その他	22	34	29	29	5	7	11	－	23
	不明	105	92	57	46	10	12	20	－	42

（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。

○　サイバー攻撃手法への正しい理解と対策の実施が必要

実在の組織や人物になりすましたメールの添付ファイル等を開いたことによりマルウエア Emotet に感染し、メール関連情報が窃取され、自らを騙る不審メールの送信に利用された事例が多数あった。

○　機器交換の際の手順の十分な事前検討と障害発生時の回復手段の事前準備が必要

機器の電源設備交換時の不具合発生による停電により機器が停止し、長時間にわたりサービスが提供できなかった事例が複数あった。

○　設定どおりの稼働の確保が必要

記憶装置に不具合が発生した際に、設定していたはずのバックアップが取得できておらず、一部データが回復できなかった事例があった。

機密性・完全性・可用性の適切なバランスを踏まえた措置の実施にも留意。

○　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。

○　データのライフサイクル全般を通じたサプライチェーンリスクの再検討が必要

リース返却物件から記憶装置が流出し、重要情報が流出したおそれが発生した事例があった。

以上