資料５

平成 31 年 1 月 17 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 30 年 7 月～9 月）
・情報共有の実施状況（平成 30 年度第３四半期分）
・最近のインシデントから得られた教訓

平成 31 年 1 月 17 日
内閣サイバーセキュリティセンター

サイバーセキュリティを取り巻く情勢(平成 30 年 7 月～9 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 30 年 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 DHS が国家リスクマネジメントセンター(NRMC)を創設[1]

- ○ 2018 年 7 月 31 日、国土安全保障省(DHS)はサイバーセキュリティサミットを開催。
- ○ サイバーセキュリティサミット中、DHS ニールセン長官は、重要インフラの防護を目的とした新組織、国家リスクマネジメントセンター(NRMC)の創設を公表。
- ○ NRMC は、サイバー、物理両面における脅威から米国の重要インフラを防護するための官民共同での活動を調整。

[1] *DHS「Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech(2018/7/31)」、https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech (2018/8/23 閲覧)*

1.1.2 米国 NIST のエネルギー分野におけるサイバーセキュリティへの取組[2]

- ○ 2018 年 3 月、米国国立標準技術研究所(NIST) National Cybersecurity Center of Excellence(NCCoE)は、制御技術設備を効率的に特定、制御、監視することを目的として、エネルギーセクター資産マネジメント計画の立上げを公表。
- ○ 同年 7 月 9 日、NIST NCCoE は、エネルギーセクター資産マネジメント計画において、複数の米企業と共同で活動すると公表。

1.1.3 ZTE 制裁及び対米外国投資委員会(CFIUS)関連動向[3]

- ○ 2018 年 7 月 20 日、米国両院協議会は、ZTE への制裁再開を目的とした上院による 2019 会計年度(FY)国防授権法(NDAA)修正案の破棄を公表。
- ○ これによって、ZTE は米国企業との取引再開が可能。
- ○ 一方、トランプ政権が重視する対米外国投資委員会(CFIUS)に関して、権限強化のための新たな規定が NDAA に追加。

1.1.4 米大統領が FY2019 NDAA に署名[4]

- ○ 2018 年 8 月 13 日、トランプ大統領が 2019 会計年度(FY)国防授権法(NDAA)に署名。
- ○ FY2019 NDAA は、サイバーセキュリティに関する事項を含む、連邦政府全体の国防関連の予算権限を規定。

1.1.5 米国 国家サイバー戦略を公表[5]

- ○ 2018 年 9 月 20 日、ホワイトハウスは国家サイバー戦略を公表。
- ○ 本戦略はサイバー抑止を重要原則とする 4 つの柱で構成され、米国のとるべき施策の方針を規定。

1.1.6 米国 国家サイバーインシデント対処計画[6]

---

[2] *NCCoE「ENERGY SECTOR ASSET MANAGEMENT(2018/3)」、https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-am-project-description-final.pdf (2018/10/25 閲覧)*
NIST NCCoE「NCCoE Selects Technology Vendors to Collaborate on Asset Management Project for the Energy Sector(2018/7/9)」、https://www.nccoe.nist.gov/news/nccoe-selects-technology-vendors-collaborate-asset-management-project-energy-sector (2018/8/23 閲覧)

[3] *Engadget「Senate gives up on ZTE sanctions(2018/7/20)」、https://www.engadget.com/2018/07/20/senate-gives-up-zte-sanctions/ (2018/8/21 閲覧)*
ロイター通信「トランプ政権、中国の対米投資は CFIUS 活用し制限 他国も対象(2018/6/27)」、https://jp.reuters.com/article/usa-trade-china-idJPKBN1JN27E (2018/8/13 閲覧)

[4] *Congress「H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019(2018/8/13)」、https://www.congress.gov/bill/115th-congress/house-bill/5515/text (2018/9/10 閲覧)*

[5] *Whitehouse「National Cyber Strategy - The White House (2018/9/20)」、https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (2018/10/2 閲覧)*

[6] *DHS「National Cyber Incident Response Plan(2016/12)」、https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf (2018/10/8 閲覧)*
Whitehouse「Cyber Incident Severity Schema(2016/7/25)」、https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf (2018/10/1

○ 2016 年 12 月、国土安全保障省(DHS)は国家サイバーインシデント対処計画を公表。
○ 本計画では、PPD-41 で規定された重大サイバーインシデント対処活動における権限・役割をより具体的に規定。
○ 米国のサイバーインシデント深刻度スキーマは、米政府の初動体制におけるインシデント評価を目的としており、2018 年 7 月 28 日に NISC が公表した深刻度評価基準は本スキーマを参考として作成。

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. 政府機関に関連するサイバーセキュリティインシデント

2.1.1 米国大統領選挙におけるサイバー攻撃[7]

○ ソーシャルメディア等を利用し、不正に大統領選挙に干渉し世論を操作したとして、ロシアの個人 13 人と企業 3 社を起訴。
○ 米民主党全国委員会(DNC)等に対してサイバー攻撃を行ったとして、ロシア連邦軍参謀本部情報総局(GRU)の情報当局者 12 人を起訴。

2.2. 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

2.2.1 シンガポール、サイバー攻撃で 150 万人分の患者記録流出[8]

○ 2018 年 7 月 20 日、シンガポール政府は、公的医療グループ SingHealth のデータベースがサイバー攻撃を受け、150 万人分の患者記録が流出したと発表。
○ 同国政府は、当該事案を受け、SingHealth やその他公的部門の IT システムの管理と保護を強化する対策を提案。

2.3. その他の事案

2.3.1 家庭用 IoT デバイスのセキュリティに関してと米国カリフォルニアの IoT 法の成立[9]

---

2 閲覧)
NISC「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)(2018/7/28)」、https://www.nisc.go.jp/active/infra/pdf/hyouka_kijun_shohan.pdf (2018/10/12 閲覧)
NISC「重要インフラサービス障害に係る深刻度判断基準の例について(2017/3/16)」、https://www.nisc.go.jp/conference/cs/ciip/index.html (2018/10/12 閲覧)

[7] *Department of Justice「Internet Research Agency Indictment(2018/2/16)」、https://www.justice.gov/file/1035477/download (2018/9/19/閲覧)*
REUTERS「米大陪審、ロシア情報当局者 12 人を起訴 大統領選介入疑惑で(2018/7/14)」、https://jp.reuters.com/article/usa-trump-russia-indictments-idJPKBN1K32ID (2018/9/19/閲覧)

[8] *CNET Japan「シンガポールの医療機関にサイバー攻撃、首相含む 150 万人の情報流出 政府が対策など示す(2018/7/21)」、https://japan.cnet.com/article/35122835/ (2018/8/2 閲覧)*
Smart Nation and Digital Government Office「The Government is lifting the pause on new ICT systems which it announced on 20 July, following the attacks on SingHealth's system. (2018/8/17)」、https://www.smartnation.sg/newsroom/press-releases/the-government-is-lifting-the-pause-on-new-ict-systems-which-it-announced-on-20-july--following-the-attacks-on-singhealths-system (2018/8/22 閲覧)

[9] *DOJ「Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybe*

○ 米司法省(DOJ：Department of Justice)は、2018 年 9 月 18 日、IoT デバイスを標的としたマルウエア「Mirai」の作成に関与したとして起訴されていた 3 名に対して、司法取引により保護観察処分を言い渡した。この 3 名は、サイバー犯罪の捜査に貢献を行ったとされ、引き続き捜査に協力することが義務付けられている。
○ 米国の非営利組織(NPO)の「American Consumer Institute(ACI)」は、米国で販売されている 14 社の Wi-Fi ルーター186 機種を調査し、83%の製品が、既知の脆弱性が修正されないまま放置されているとの調査結果を公表。
○ 米国カリフォルニア州で IoT デバイスのデフォルトパスワードを禁ずる法律(「カリフォルニア州 接続される機器(コネクテッド・デバイス)のセキュリティ法」(Senate Bill No.327 CHAPTER886))が成立。全ての IoT デバイス毎に異なるデフォルトパスワードを作成するか、初めてデバイスを使用する際にパスワード変更を求めることが必要で、デバイスの性質と機能に適した合理的なセキュリティ機能が必要となる。

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. 政府機関に関連するサイバーセキュリティインシデント

3.1.1 Google 社の Web ブラウザ Chrome の最新版で、中央官庁 HP に「警告」表示[10]

○ 2018 年 7 月にリリースされた Google 社の Web ブラウザ「Chrome 68」から HTTPS に対応していない Web サイトを閲覧する際に、警告が表示。
○ 全国の自治体サイトの 37%(うち都道府県サイトの 49%)、中央省庁等では 50%が常時 HTTPS 化に対応済で残りは未対応。
○ 「政府機関等の情報セキュリティ対策のための統一基準」では、常時 HTTPS 化対応は必須事項。

3.2. 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

3.2.1 NTT ドコモ、ケイ・オプティコム、四国電力でのリスト攻撃による被害[11]

---

rcrime Investigations(2018/9/18)」、https://www.justice.gov/usao-ak/pr/hackers-cooperation-fbi-leads-substantial-assistance-other-complex-cybercrime (2018/10/18 閲覧)
ACI「Securing IoT Devices: How Safe Is Your Wi-Fi Router?(2018/10/3)」、http://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf (2018/10/17 閲覧)
カリフォルニア州「SB-327 Information privacy: connected devices.(2018/9/28)」、http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (2018/10/17 閲覧)

[10] *産経ニュース「経産・総務両省 HP に「警告」表示、グーグル閲覧ソフト最新版で(2018/7/25)」、https://www.sankei.com/economy/news/180725/ecn1807250045-n1.html (2018/7/31 閲覧)*
Google「A Secure web is here to stay(2018/2/8)」、https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html (2018/12/6 閲覧)
JIPDEC「常時 SSL/TLS 化調査レポート｜自治体サイト対応状況 -2018 年 6 月版-」、https://itc.jipdec.or.jp/aossl_local-government/201806.html (2018/8/22 閲覧)
NISC「政府機関等の情報セキュリティ対策のための統一基準群(平成 30 年度版)について」、https://www.nisc.go.jp/active/general/kijun30.html (2018/8/22 閲覧)

[11] *ITmedia「「iPhone X」不正購入被害 1,000 件、「ドコモオンラインショップ」に不正ログイン、リス*

○ NTT ドコモ、ケイ・オプティコム、四国電力等の Web サイトでリスト攻撃による不正アクセスが発生。
○ リスト攻撃とは、第三者が何らかの方法で入手した正規の ID とパスワードのリストを用いて認証を突破し、不正にアクセスを行うもの。
○ 2018 年 8 月以降、NTT ドコモが運営する通販 Web サイト「ドコモオンラインショップ」、携帯電話サービス「mineo」や光通信サービス「eo 光」等を提供するケイ・オプティコムの Web サイト、四国電力の Web サイト「よんでんコンシェルジュ」で、不正アクセスにより Web サイトやサービスで使用できるポイントの不正利用や、商品の不正購入等の被害が発生。

3.2.2 仮想通貨取引所「Zaif」からの仮想通貨流出事案について[12]

○ 2018 年 9 月 14 日、テックビューロ株式会社が運営する仮想通貨取引所「Zaif」が不正アクセスを受け、約 70 億円分の仮想通貨が流出。
○ 近畿財務局は、当該事案発生前に、同社に対し、2 度の業務改善命令を発出し、その改善状況を定期的に確認。
○ 同社は 2018 年 10 月 10 日に、株式会社フィスコ仮想通貨取引所と事業譲渡契約を締結。これにより顧客資産は、株式会社フィスコ仮想通貨取引所が補償。

4. 脅威動向

4.1.1 ランサムウエアによる被害の動向に関して[13]

ト型攻撃で(2018/8/13)」、http://www.itmedia.co.jp/news/articles/1808/13/news084.html (2018/9/18/閲覧)
ケイ・オプティコム「eoID に対する不正なログインについてのお知らせ(2018/8/21)」、http://www.k-opti.com/announce/180815/ (2018/9/13/閲覧)
四国電力「よんでんコンシェルジュへの不正アクセスによるポイント交換について(2018/8/24)」、http://www.yonden.co.jp/press/re1808/data/pr006.pdf (2018/9/13/閲覧)
NTT ドコモ「d ポイントを安心してご利用いただくためのお願い(2018/9/10)」、https://www.nttdocomo.co.jp/info/notice/page/180830_00.html (2018/12/6 閲覧)

[12] *テックビューロ株式会社「仮想通貨流出事件に関する状況報告、及び顧客対応状況について(2018/9/21)」、https://prtimes.jp/main/html/rd/p/000000094.000012906.html (2018/10/3 閲覧)*
近畿財務局「テックビューロ株式会社に対する行政処分について(2018/9/25)」、http://kinki.mof.go.jp/file/rizai/pagekinkihp025000049.html (2018/10/3 閲覧)
テックビューロ株式会社「お客様預かり資産に関する金融支援　正式契約締結のお知らせ(2018/10/10)」、https://prtimes.jp/main/html/rd/p/000000098.000012906.html (2018/10/19 閲覧)

[13] *JPCERT/CC「ランサムウエアの脅威動向および被害実態調査報告書(2018/7/30)」、https://www.jpcert.or.jp/research/Ransom-survey.html (2018/8/22 閲覧)*
IPA「情報セキュリティ 10 大脅威 2018(2018/3)」、https://www.ipa.go.jp/files/000065376.pdf (2018/8/22 閲覧)
US-CERT「Ransomware(2018/7/11)」、https://www.us-cert.gov/security-publications/Ransomware (2018/8/22 閲覧)
US-CERT「Data Backup Options(2013/2/6)」、https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf (2018/8/24 閲覧)
KasperskyLab「KeyPass ransomware(2018/8/13)」、https://securelist.com/keypass-ransomware/87412/ (2018/12/10 閲覧)
US-CERT「Alart(AA18-337A)SamSam Ransomeware(2018/12/3)」、https://www.us-cert.gov/ncas/a

○ 昨年度に拡散した WannaCry や NotPetya に引き続き、ランサムウエアによる被害が発生。
○ WannaCry のような自己伝染機能を持つものの他、SamSam や KeyPass のように手動で感染を広げることで高度な攻撃を行うもの等、感染手口が高度化。
○ これまでのランサムウエアに対する予防対策に加え、[1-2-3]バックアップなどの適切なバックアップの実施や復旧手順の確立が必要。

4.1.2 本物のパスワードで信用させる脅迫メール[14]

○ 受信者を信用させるため、受信者が使っている(使っていた)本物のパスワードが記載されている脅迫メールが出回り、JPCERT/CC が注意喚起を発出。
○ 当該脅迫メールにより仮想通貨(BTC)を要求。
○ パスワード漏えいの原因については不明。

以上

---

lerts/AA18-337A (2018/12/10 閲覧)

[14] *JPCERT/CC「仮想通貨を要求する不審な脅迫メールについて(2018/8/2)」、https://www.jpcert.or.jp/newsflash/2018080201.html (2018/8/14 閲覧)*
日経 XTECH「本物のパスワードで信用させる、脅迫メールのえげつない中身(2018/9/6)」、https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00139/082700025/?P=2 (2018/9/6 閲覧)

平成 31 年 1 月 17 日

内閣サイバーセキュリティセンター

情報共有の実施状況（平成 30 年度第３四半期分）

「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。

(FY:年度)

実施形態	FY26 計	FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
重要インフラ事業者等からNISCへの情報連絡(※)	124	401	856	388	69	50	60	－	179
関係省庁・関係機関からのNISCへの情報共有	27	52	41	19	0	1	3	－	4
NISCからの情報提供	38	44	80	54	7	17	8	－	32

※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			FY26 計	FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
未発生の事象		予兆・ヒヤリハット	9	75	330	80	7	8	8	－	23
発生した事象	機密性を脅かす事象	情報の漏えい	9	15	30	15	4	4	2	－	10
	完全性を脅かす事象	情報の破壊	14	52	47	20	5	7	3	－	15
	可用性を脅かす事象	システム等の利用困難	38	86	80	143	21	20	29	－	70
	上記につながる事象	マルウェア等の感染	27	111	289	65	9	2	4	－	15
		不正コード等の実行	3	11	10	13	2	1	0	－	3
		システム等への侵入	12	27	26	17	6	1	3	－	10
		その他	12	24	44	35	15	7	11	－	33

※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		FY26 計	FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
意図的な原因	不審メール等の受信	6	83	546	89	16	5	9	－	30
	ユーザＩＤ等の偽り	7	8	1	4	2	1	0	－	3
	DoS攻撃等の大量アクセス	25	47	23	31	6	4	5	－	15
	情報の不正取得	13	8	14	16	2	5	1	－	8
	内部不正	0	2	0	4	1	0	0	－	1
	適切なシステム等運用の未実施	4	10	19	15	4	1	7	－	12
偶発的な原因	ユーザの操作ミス	0	10	15	23	4	1	4	－	9
	ユーザの管理ミス	2	5	8	13	5	0	1	－	6
	不審なファイルの実行	1	51	243	42	10	5	1	－	16
	不審なサイトの閲覧	1	49	29	20	1	1	1	－	3
	外部委託先の管理ミス	10	12	20	41	11	9	5	－	25
	機器等の故障	7	17	22	32	8	8	7	－	23
	システムの脆弱性	9	29	56	36	7	6	5	－	18
	他分野の障害からの波及	1	5	0	10	2	0	1	－	3
環境的な原因	災害や疾病等	0	0	0	0	0	0	1	－	1
その他の原因	その他	9	22	34	29	6	7	8	－	21
	不明	43	105	92	57	10	9	14	－	33

平成 31 年 1 月 17 日
内閣サイバーセキュリティセンター

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

（１）障害発生の原因に関するもの

○　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

システム設定の不具合、システム更新の不具合、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多く発生している。

○　他のシステム障害の影響を受けにくいシステム構築が必要

接続する他の装置が機器交換により不具合が発生し、サービス停止が長時間継続する事例があった。

○　利用期間全体を見据えたシステム構築・維持が必要

ネットワーク機器のソフトウエアにおける電子証明書の有効期限切れにより、異常が発生し、通信が途絶する事例があった。

（２）障害発生後の対応に関するもの

○　切替手順の事前確認と訓練の実施（ＢＣＰの確保）が必要

回線が冗長化されているにもかかわらず、手順がわからなかったため、他の回線に切り替えることができず、システムが利用できなくなる事例があった。

以上