資料９

平成 31 年 4 月 18 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 10 月～12 月）
・最近のインシデントから得られた教訓

平成 31 年 4 月 18 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 10 月～12 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 10 月～12 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 米国の対中サイバー政策動向[1]

- 2018 年 10 月 2 日、米紙 Wall Street Journal は中国政府が関与するとみられるサイバー諜報グループの正体を暴く匿名グループ「Intrusion Truth」に関して報道。
- 同月 4 日、ニュースサイト Bloomberg は中国政府によるマイクロチップを用い

[1] *Wall Street Journal「Cyberespionage Experts Want to Know Who's Exposing China's Hacking Army(2018/10/2)」、https://www.wsj.com/articles/cyberespionage-experts-want-to-know-whos-exposing-chinas-hacking-army-1538478001（2018/11/9 閲覧）*
Bloomberg「The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies(2018/10/4)」、https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies（2018/11/15 閲覧）
CNN「ペンス米副大統領、演説で中国批判　貿易や軍事に幅広く言及(2018/10/5)」、https://www.cnn.co.jp/world/35126604.html（2018/11/9 閲覧）
DoJ「Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years(2018/11/15)」、https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal（2018/11/15 閲覧）

たハッキングに関して報道。

- ○ これら 2 つの報道の後、同月 4 日にはペンス副大統領らが米国の対中政策に関して演説し、また同月 30 日には司法省が米国への産業スパイ活動に従事していた中国情報当局の職員らを起訴。

1.1.2 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁の設置[2]

- ○ 2018 年 11 月 16 日、トランプ大統領は「2018 年サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)法」に署名。
- ○ これにより、国土安全保障省(DHS)国家保護・プログラム総局(NPPD)は CISA に改組。
- ○ CISA の組織編制は旧体制をそのまま引き継いだものであり、本改組による対処体制強化の有効性は依然不透明。

1.2. 中国

1.2.1 中国製造 2025・国家情報法[3]

- ○ 2015 年 5 月、中国政府は製造業強化戦略である中国製造 2025 を発表し、2025 年までの世界の製造強国入りを目標として設定。
- ○ さらに、2017 年 6 月、中国政府は国家情報法を制定し、全ての中国国民及び中国国内企業に対し、国家によるインテリジェンス活動への協力及び活動内容の秘匿を義務化。
- ○ 米国政府は、中国政府が中国製造 2025 で示された目標を達成するべく米国の知的財産を窃取し、国家情報法に基づき企業の保有する情報を入手しているとして批判し、対中制裁を発動。

1.3. 米中対立に伴う各国の反応

1.3.1 中国にまつわるサイバー事案等について[4]

---

[2] *Congress「H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018(2018/11/16)」、https://www.congress.gov/bill/115th-congress/house-bill/3359（2018/12/12 閲覧）*
Dark Reading「Congress Passes Bill to Create New Federal Cybersecurity Agency(2018/11/15)」、https://www.darkreading.com/risk/congress-passes-bill-to-create-new-federal-cybersecurity-agency-/d/d-id/1333286（2018/12/12 閲覧）

[3] *国立研究開発法人 科学技術振興機構 研究開発センター「「中国製造 2025」の公布に関する国務院の通知の全訳(2015/7/25)」、https://www.jst.go.jp/crds/pdf/2015/FU/CN20150725.pdf（2019/1/19 閲覧）*
国立国会図書館調査及び立法考査局「【中国】国家情報法の制定（2017/8)」、http://dl.ndl.go.jp/view/download/digidepo_10404463_po_02720209.pdf?contentNo=1&alternativeNo=（2019/1/19 閲覧）
USTR「FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATIONUNDER SECTION 301 OF THE TRADE ACTOF 1974(2018/3/22)」、https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF（2019/1/19 閲覧）
Whitehouse「Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation（2018/3/22)」、https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/（2019/1/23 閲覧）

[4] *外務省「中国を拠点とする APT10 といわれるグループによるサイバー攻撃について(2018/12/21)」、https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html（2018/12/21 閲覧）*
Cathay Pacific「Cathay Pacific announces data security event affecting passenger data(2018/10/24)」、https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data（2018/11/29 閲覧）

- ○ 2018 年を通じ、中国ファーウェイ、ZTE に対し、各国政府が様々な対応を実施。
- ○ 2018 年 12 月 21 日、外務省は、中国を拠点とする APT10 といわれるグループによるサイバー攻撃に関する外務省報道官談話を発表。
- ○ 2018 年 10 月頃より、香港において多数のサイバー攻撃による被害が発生。

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 石油・ガス企業を標的とするマルウエア「Shamoon」[5]

- ○ 2018 年 12 月 10 日、イタリアの大手石油会社 Saipem が大規模なサイバー攻撃を受けたと発表。
- ○ 攻撃に使用されたマルウエアは、過去にエネルギー業界への攻撃で使用された「Shamoon」と呼ばれるマルウエアの亜種。
- ○ セキュリティベンダーは Shamoon の分析結果から、背後にイラン系のハッカーグループが関与していると推測。

2.2. その他の事案

2.2.1 Facebook 社における一連の個人情報流出事案等について[6]

- ○ 2018 年 9 月 28 日、米 Facebook 社はハッキングの被害を受け、約 5,000 万件の利用者情報が流出したおそれがあると発表。
- ○ 同社は、同年 3 月、6 月にもそれぞれ個人情報保護に関する問題が発覚。
- ○ 一連の事案に関して、各国は様々な対応を実施。

2.2.2 トレンドマイクロ社製品の AppStore での公開停止に関する同社 CEO の見解[7]

South China Morning Post「HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show(2018/10/29)」、https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk13-million-damage-caused-gps-jamming-caused-46-drones（2018/11/29 閲覧）
ZDNet「HSBC discloses security incident(2018/10/29)」、https://www.zdnet.com/article/hsbc-discloses-security-incident/（2018/11/29 閲覧）

[5] *SAIPEM「Saipem: update on the cyber attack suffered(2018/12/12)」、http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page（2019/1/23 閲覧）*
Fire Eye「ファイア・アイ、イランのハッカー集団「APT33」の 活動内容と技術詳細を明らかに(2017/9/22)」、https://www.fireeye.jp/company/press-releases/2017/apt33-insights-into-iranian-cyber-espionage.html（2019/1/23 閲覧）

[6] *Facebook「Security Update(2018/9/28)」、https://newsroom.fb.com/news/2018/09/security-update/（2018/11/13 閲覧）*
The New York Times「How Trump Consultants Exploited the Facebook Data of Millions(2018/3/17)」、https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html（2018/11/16 閲覧）
The Guardian「Revealed 50 million Facebook profiles harvested for Cambridge Analytica in major data breach(2018/3/17)」、https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election（2018/11/16 閲覧）
ロイター「フェイスブック、レノボなど中国 4 社にも利用者データ共有許可(2018/6/6)」、https://jp.reuters.com/article/facebook-data-china-idJPKCN1J20AM（2018/11/16 閲覧）

[7] *IT media「ブラウザの閲覧履歴を密かに中国に送信、不正アプリが Mac App Store から削除(2018/9/10)」、http://www.itmedia.co.jp/news/articles/1809/10/news047.html（2018/11/16 閲覧）*
Trend Micro「macOS、iOS 向け当社アプリに関する重要なお知らせ(2018/10/31)」、https://www.trendmicro.com/ja_jp/about/announce/announces-20180912.html（2018/11/21 閲覧）
ZDNet Japan「トレンドマイクロのチェン CEO、App Store でのアプリ削除問題に謝罪と説明(2018/10/31)」、http

○ トレンドマイクロ社製品が、ユーザー情報の不適切な収集を理由に Apple 社の App Store で 2018 年 9 月 10 日から公開を停止。
○ 公開停止が長期化している件について、同社チェン代表取締役兼 CEO が同年 10 月 31 日に見解を公表し、ユーザー情報を収集していた理由を「脅威情報の共有」と説明。
○ この見解の内容やユーザー情報の取扱いに対するセキュリティ事業者としての姿勢への疑問の声が、ユーザーやセキュリティ専門家から浮上。

2.2.3 ソースコード共有サイト「GitHub」で 24 時間に及ぶサービス障害[8]

○ 開発者向けのソースコード共有サイト「GitHub」で 2018 年 10 月 22 日午前 7 時 52 分(日本時間)から障害が発生。
○ 障害の原因は、サービス基盤を構成するネットワーク機器の交換により生じた 43 秒間のデータセンター間の接続断が引き起こした、GitHub のデータベースの不整合。
○ 障害の復旧では、ユーザーデータの損失を避けることを最優先とする方針を選択したため、対応に約 1 日を要したが、結果としてデータはほとんど失われず復旧。
○ ユーザーは GitHub 社の対応に関して、対応時の意思決定の的確性、原因分析・公表への姿勢、対策立案の迅速性を、良好事例として好意的に評価。

2.2.4 米国新聞印刷会社へのサイバー攻撃[9]

○ 2018 年 12 月 27 日、米国の新聞印刷会社 Tribune Publishing 社がマルウエアに感染し、複数の米大手新聞社で印刷、配送等に遅延が発生。
○ マルウエアの種類や被害の詳細は公式に公表されていないものの、Tribune Publishing 社の内部関係者の情報から、攻撃にはランサムウエア「Ryuk」が使用された可能性があると報道。

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 国税庁委託先におけるマイナンバー等個人情報 70 万件の漏えい[10]

○ 国税庁は 2018 年 12 月 14 日、データ入力を委託されていた業者が契約に

---

s://japan.zdnet.com/article/35127835/ (2019/2/25 閲覧)

[8] *ITmedia「GitHub がダウン 「データストレージシステムに障害」(2018/10/22)」、http://www.itmedia.co.jp/news/articles/1810/22/news080.html (2018/11/16 閲覧)*
The GitHub Blog「October 21 post-incident analysis(2018/10/30)」、https://blog.github.com/2018-10-30-oct21-post-incident-analysis/ (2018/11/16 閲覧)

[9] *LA Times「L.A. Now Local Malware attack disrupts delivery of L.A. Times and Tribune papers across the U.S (2018/12/29)」、http://www.latimes.com/local/lanow/la-me-ln-times-delivery-disruption-20181229-story.html (2019/1/10 閲覧)*

[10] *毎日新聞「国税庁委託先がマイナンバーなど個人情報 70 万件漏えい(2018/12/14)」、https://mainichi.jp/articles/20181214/k00/00m/040/179000c (2018/12/28 閲覧)*
システムズ・デザイン株式会社「受託業務における契約及び法令違反のご報告とお詫び(開示事項の経過)(2018/12/18)」、http://www.sdcj.co.jp/20181218●受託業務における契約及び法令違反のご報告とお詫び.pdf (2018/12/28 閲覧)
AGS 株式会社「受託業務における契約および法令違反のご報告とお詫び(2019/1/8)」、https://www.ags.co.jp/topics/pdf/20190108_news_release.pdf (2019/2/5 閲覧)

反して別の業者に再委託し、マイナンバー等個人情報が含まれる約 70 万件の書類を流していたことを発表。

- ○ 調査の結果、国税庁以外にも契約違反ないし法令違反に当たるマイナンバーの記載のある原票のデータ入力の再委託が約 171 万件あったことが判明。
- ○ 個人情報保護委員会は、各自治体に対して国税庁に関連する再委託に関する法令遵守状況の点検を求め、これにより別の業者による新たな契約及び法令違反が判明。

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 ソフトバンクの通信障害[11]

- ○ 2018 年 12 月 6 日、ソフトバンク社の携帯電話網で全国規模の通信障害が発生し、携帯電話を使用して提供される他事業者のサービスにも広く影響が波及。
- ○ 原因は携帯電話網内で使用しているエリクソン社製 LTE 交換機(MME)のソフトウエア不具合であり、ソフトバンク社は当該ソフトウエアのバージョンダウンを行い対応。
- ○ この通信障害は、電気通信事業法で定める「重大な事故」に該当し、所管省庁である総務省は、同様の事故が再発しないよう厳重注意し、社内外の連携体制の改善、利用者への周知内容等の改善及び通信業界内での教訓の共有等を図るように指導。

3.3. その他の事案

3.3.1 引き続き拡大する脅迫メール[12]

- ○ 本物のパスワードで信用させる脅迫メールの日本語化対応が行われる等、脅迫メールが引き続き拡散。全世界で 400 万ドルを超える被害が確認。
- ○ 日本語による脅迫文やメール送信者の偽装等、脅迫内容を信用させるための手法を利用し被害を拡大。

4. 脅威動向

4.1.1 ロシア関連のハッカー集団による新たな攻撃キャンペーンについて[13]

---

[11] *ソフトバンク「上場記者会見の模様をインターネットでライブ中継(2018/12/19)」、https://www.softbank.jp/corp/group/sbm/news/info/2018/20181219_01/ (2019/1/18 閲覧)*
総務省「ソフトバンク株式会社に対する電気通信事故の再発防止に係る措置(指導)(2019/1/23)」、http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000171.html (2019/2/6 閲覧)

[12] *Barkly 社「Sextortion Email Scam Nets Criminals $4 Million,Continues to Evolve(2018/10)」、https://blog.barkly.com/sextortion-email-scam-spoofing-password (2018/11/21 閲覧)*
Kaspersky「日本語を含めた多言語で拡散する脅迫メール(2018/9/21)」、https://blog.kaspersky.co.jp/blackmail-asking-for-cryptocurrency/21616/ (2018/11/15 閲覧)

[13] *Palo Alto Networks「Sofacy による世界的な攻撃が継続、新たに「Cannon」トロイの木馬を観測(2018/11/27)」、https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan (2018/12/7 閲覧)*
CYBERSCOOP「Accenture: Russian hackers using Brexit talks to disguise phishing lures(2018/11/29)」、https://www.cyberscoop.com/apt28-brexit-phishing-accenture/ (2018/12/7 閲覧)
トレンドマイクロ セキュリティブログ「Pawn Storm による攻撃キャンペーンを日本国内でも確認(2018/11/22)」、https://blog.trendmicro.co.jp/archives/19829 (2018/12/7 閲覧)

- 緊張感を増している米中関係に注目が集まる一方、2018 年 11 月下旬、ロシア関連のハッカー集団 APT28 によるものと考えられるサイバー攻撃が複数ベンダーから報告。
- いずれの報告においても、メール受信者に添付ファイルを開かせる「ルアー」として、最新ニュースのキーワードを Word ファイル名に使用。
- ユーザーが Word ファイルを開いた場合、「コンテンツの有効化」を促し、マクロを使用して、外部からマルウエア等を読み込ませる。

4.1.2 高度なマルウエア「EMOTET」の特徴[14]

- 2018 年夏頃から、マルウエア「EMOTET」が世界中で猛威を振るい、米国 US-CERT は、同年 7 月に EMOTET に関する注意喚起を実施。
- EMOTET は、Windows をターゲットとした高度なマルウエアで、モジュール化、最新バージョンへの更新機能、解析環境の検出、感染した PC 内の認証情報を窃取する等、高度な手法を取り入れることで感染を広げている。

Accenture 「Snakemackerel Delivers Zekapab Malware(2018/11/29)」、https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware (2019/27 閲覧)

[14] *NCCIC「Alert(TA18-201A)Emotet Malware(2018/7/20)」、https://www.us-cert.gov/ncas/alerts/TA18-201A (2019/1/21 閲覧)*
三井物産セキュアディレクション「流行マルウエア『EMOTET』の内部構造を紐解く(2018/12/25)」、https://www.mbsd.jp/blog/20181225_2.html (2019/1/21 閲覧)

平成 31 年 4 月 18 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

○　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・再起動の不具合、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。

○　手順の事前確認と障害発生時の早期回復に向けた事前準備が必要

機器の交換・更新又は再起動により不具合が発生し、長時間にわたりサービスの提供を見合わせた事例が散見された。

○　利用期間全体を見据えたシステム構築・維持が必要

電子証明書の有効期限切れにより不具合が発生し、長時間にわたりサービスの提供を見合わせた事例が引き続きあった。

○　不正通信の検知と遮断、顧客への回復手段の早期教示が必要

外部からの大量の不正ログイン試行により、顧客の操作によらず、複数顧客のアカウントがロックされる事例があった。

○　パスワードを、使いまわさない、漏えい事実把握後すぐに変えることが必要

他社サービスで漏えいしたＩＤ及びパスワードによりメール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事例が散見された。

一つのサイバー攻撃（被害）が、次の複数のサイバー攻撃（被害）につながることがあることに留意。

以上