資料4

平成 30 年 10 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、今回の調査会から、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 4 月～6 月）
・情報共有の実施状況（平成 30 年度前期分）
・最近のインシデントから得られた教訓

平成 30 年 10 月 29 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 4 月～6 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ついて、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 米国のサイバーセキュリティ施策に関する最新動向[1]

- ○ 2018 年 6 月 1 日、ホワイトハウスは、連邦政府ネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令に基づく報告書が出揃った旨を発表。
- ○ DHS と DOC は、ボットネット等の脅威を大幅に軽減するための、5 つの目標と 24 の具体的なアクションを示した報告書を発行。

1.1.2 米国 DHS のサイバーセキュリティ戦略[2]

---

[1] *The White House「Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure(2018/6/1)」、https://www.whitehouse.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/ (2018/7/30 閲覧)*
DOC「Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats」、https://www.commerce.gov/file/report-president-enhancing-resilience-internet-and-communications-ecosystem-against-botnets-and (2018/6/20 閲覧)

[2] *DHS「Cybersecurity Strategy – Homeland Security(2018/5/17)」、https://www.dhs.gov/publication/dhs-cybersecurity-strat*

○ 2018 年 5 月 15 日、米国国土安全保障省(DHS)はサイバーセキュリティ戦略を発表。
○ 本戦略は米国に対するサイバー脅威として、サイバー攻撃とサイバー犯罪の 2 つを特定。
○ これらの脅威への対抗策として、本戦略は 5 つの柱及び 7 つの目標を設定し、DHS のとるべき施策の方針を規定。

1.1.3 米国 OMB 連邦政府機関のリスクマネジメント測定に関する報告書[3]

○ 2018 年 5 月 29 日、大統領令 EO13800 に基づき、行政管理予算局(OMB)は「Federal Cybersecurity Risk Determination Report and Action Plan」を公開。
○ 本報告書は連邦政府機関のリスクマネジメントプロセスにおける、国立標準技術研究所(NIST)のフレームワークへの準拠状況を明らかにすべく、76 の評価指標を用いて作成。
○ その結果 96 中 71 の連邦政府機関において、リスクが存在するセキュリティプログラムを運用していると特定。査定の結果から 4 つの問題を特定し、それぞれ対策を列挙。

1.1.4 米国クラウド法について[4]

○ 米国においてクラウド法が、「2018 統合歳出法 (Consolidated Appropriations ACT, 2018)」の一部(DIVISION V)として成立。
○ クラウド法の成立には、Microsoft 社が、アイルランドに所在するサーバーに保存されたデータの開示命令を拒んだことが発端。クラウド法に対する反応は賛否が分かれているが、Apple や Facebook、Google、Microsoft、Oath 等、主要な IT 企業は賛同。
○ クラウド法は、米政府がサーバー設置国の政府と協定を結ぶことによって、米国法に基づき当該サーバーにあるデータの提出をインターネット企業等に命じることができるようにするもの。同様に、同協定締結国は、米国内のサーバーのデータ提出を当該国の法律に従い命じることが可能。

1.1.5 米国国防総省サイバードクトリン[5]

○ 2018 年 6 月 20 日、米国国防総省(DOD)は、統合軍のサイバー空間作戦の原理原則を示した新たなドクトリン「Cyberspace Operations」を発表。

---

egy (2018/6/20 閲覧)

[3] *Whitehouse「Federal Cybersecurity Risk Determination Report and Action Plan(2018/5)」、https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf (2018/6/20 閲覧)*

[4] *U.S.Congress「H.R.1625- Consolidated Appropriations ACT, 2018(2018/3/23)」、https://www.congress.gov/bill/115th-congress/house-bill/1625/text (2018/6/12 閲覧)*
TechCrunch Japan「Microsoft のデータ保護問題に決着――米最高裁、CLOUD 法成立により過去のデータ提出命令を無効と決定(2018/4/18)」、https://jp.techcrunch.com/2018/04/18/2018-04-17-supreme-court-dismisses-warrant-case-against-microsoft-after-cloud-act-renders-it-moot/ (2018/6/12 閲覧)
TechCrunch「As the CLOUD Act sneaks into the omnibus, big tech butts heads with privacy advocates(2018/3/22)」、https://techcrunch.com/2018/03/22/cloud-act-omnibus-bill-house/ (2018/6/12 閲覧)

[5] *DoD Joint Chiefs of Staff「JP 3-12, Cyberspace Operations, 08 June 2018(2018/6/8)」、http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-09-103427-137 (2018/7/5 閲覧)*

○ 本ドクトリンは、DOD によるサイバー空間作戦の計画、実行、評価に関して規定。
○ 「サイバー空間における米国の優位性の低下」を認識し、「サイバー空間攻撃作戦」に関して記載。

1.2. EU

1.2.1 GDPR に関する各企業等の対応状況について[6]

○ 欧州において、2018 年 5 月 25 日、GDPR が施行。GDPR は、個人データの「移転」と「処理」に関して法的要件を定めたもの。違反した場合は高額の制裁金を課せられる可能性。欧州でビジネスを行う日本企業等にも適用。
○ 米国の大手 IT 企業等は、GDPR 施行を受け、各種対応を発表。欧米においては、GDPR 施行までに 52%の企業が対応を完了。
○ 日本においては、GDPRの認知度も低く未対応の組織も多数存在する模様。

1.2.2 EU における GDPR 特別法等のネット上の規制に関する取組について[7]

○ EU は、デジタル上のプライバシー保護強化のため、GDPR の特別法として「e プライバシー規則」(通称クッキー法)の策定作業を実施。
○ 「ネットニュース等のリンクを貼るだけで著作権料が発生」との批判があった「著作権指令」の改正案(通称「リンク税」)については、欧州議会で否決。9 月に再投票。

1.3. ロシア

1.3.1 ロシアにおけるネット規制の強化[8]

○ ロシアでは近年の法改正に基づき、既に「LinkedIn」及び「LINE」へのアクセスがブロック。
○ 今般「Telegram」へのアクセスがブロックされたことにロシア国民は反発。

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

---

[6] *JETRO「一般データ保護規則、発効前の対応が重要－「EU・英国最新経済動向セミナー」を東京で開催(2016/12/28)」、https://www.jetro.go.jp/biznews/2016/12/3bbbf5aa36a998f4.html (2018/7/30 閲覧)*
McDermott Will & Emery LLP and Ponemon Institute LLC「The Race to GDPR:A Study of Companies in the United States & Europe(2018/4)」、https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf (2018/7/30 閲覧)
トレンドマイクロ「EU 一般データ保護規則(GDPR)対応に関する実態調査を発表(2018/5/17)」、https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180517-01.html (2018/7/30 閲覧)

[7] *日本経済新聞「EU、GDPR の次はクッキー法 通信の秘密保護強化へ(2018/7/2)」、https://www.nikkei.com/article/DGKKZO32367250280620 18TCJ000/ (2018/7/9 閲覧)*
GIGAZINE「ハイパーリンクを貼るだけで著作権料がかかる通称「リンク税」が EU で導入されようとしている(2018/6/21)」、https://gigazine.net/news/20180621-eu-link-charge-copy-right/ (2018/7/9 閲覧)
欧州議会「Parliament to review copyright rules in September(2018/7/5)」、http://www.europarl.europa.eu/news/en/press-room/20180628IPR06809/parliament-to-review-copyright-rules-in-september (2018/7/9 閲覧)

[8] *RT「Russia bans several messaging apps for 'not complying with law'(2017/5/2)」、https://www.rt.com/news/386900-russia-bans-four-messengers/ (2018/7/30 閲覧)*
TASS「Rally against Telegram's blocking in central Moscow bring together some 7,500 participants(2018/4/30)」、http://tass.com/society/1002552 (2018/7/30 閲覧)

2.1.1 米国の中国通信機器メーカーZTE 等への制裁措置について[9]

- ○ 2018 年 4 月 16 日、米国政府は、ZTE がイラン等へ違法に米国製品を供給したとして、米企業による ZTE に対する製品販売を 7 年間禁止すると発表。
- ○ 米国政府はこれまで国家安全保障上の理由から、ファーウェイ及び ZTE に対する制裁措置を実施。
- ○ 一方で、トランプ大統領は、2018 年 5 月 13 日に Twitter で、事業停止状態にある ZTE が「ビジネスに復帰できるよう中国の習近平国家主席と協力している」ことを明らかにし、米商務省(DOC)は同年 7 月 13 日に、ZTE に対する制裁措置を解除。

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

2.2.1 メキシコの金融機関に対するサイバー攻撃による不正送金事案について[10]

- ○ メキシコの金融機関がサイバー攻撃を受け、少なくとも 4 億ペソが窃取。
- ○ メキシコ銀行は、銀行の情報セキュリティに関するガイドラインを策定し提供する部署を創設。

2.3. その他の事案

2.3.1 Drupal の脆弱性[11]

- ○ 主要なウェブコンテンツ管理ソフトウエア「Drupal」に、リモートから任意のコードが実行可能となる脆弱性があることが公表。
- ○ 脆弱性情報の公表の約 2 週間後には、この脆弱性に対する疑似攻撃の実証(PoC)コードが公開され、実際の攻撃が観測。
- ○ 脆弱性情報の公表から攻撃の発生までの時間が短く、各組織は、リスクに対応するため、修正済みバージョンの適用などの対応を実施することが必要。

---

[9] *ロイター「米国が中国 ZTE への製品販売 7 年間禁止、貿易摩擦の悪化も(2018/4/17)」、https://jp.reuters.com/article/usa-china-zte-commerce-idJPKBN1HN2H7 (2018/4/26 閲覧)*
CNBC「Six top US intelligence chiefs caution against buying Huawei phones(2018/2/13)」、https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html (2018/4/26 閲覧)
日本経済新聞「米軍基地でファーウェイ・ZTE 携帯の販売取りやめ(2018/5/4)」、https://www.nikkei.com/article/DGXMZO30129410U8A500C1000000/ (2018/5/7 閲覧)
Donald J. Trump ツイート、https://twitter.com/realDonaldTrump/status/995680316458262533 (2018/5/14 閲覧)
毎日新聞「米商務省:中国 ZTE、事業再開へ 制裁解除 議会、なお反発(2018/7/15)」、https://mainichi.jp/articles/20180715/ddm/008/020/071000c (2018/7/30 閲覧)

[10] *Welivesecurity「Mexico: Cybercriminals steal at least 400 million pesos through unauthorized transfers(2018/5/24)」、https://www.welivesecurity.com/2018/05/24/mexico-cybercriminals-steal-400-million/ (2018/7/19 閲覧)*

[11] *Drupal「Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002(2018/3/28)」、https://www.drupal.org/sa-core-2018-002 (2018/7/31 閲覧)*
GitHub,Inc「Proof-of-Concept for CVE-2018-7600 Drupal SA-CORE-2018-002」、https://github.com/a2u/CVE-2018-7600 (2018/7/27 閲覧)
Security Next「「Drupal」に「Drupalgeddon 2.0」とは別の脆弱性、更新が公開 - 早くも悪用を観測(2018/4/26)」、http://www.security-next.com/092731 (2018/7/27 閲覧)
NSFOCUS「DRUPAL REMOTE CODE EXECUTION VULNERABILITY ANALYSIS(2018/5/31)」、https://blog.nsfocusglobal.com/threats/vulnerability-analysis/drupal-remote-code-execution-vulnerability-analysis/ (2018/7/27 閲覧)
独立行政法人 情報処理推進機構「更新:Drupal の脆弱性対策について(CVE-2018-7600)(2018/4/13)」、https://www.ipa.go.jp/security/ciadr/vul/20180329-drupal.html (2018/7/27 閲覧)

2.3.2 Microsoft 社のクラウドサービス Office365 が障害により影響[12]

- ○ 日本時間 2018 年 4 月 6 日の夕方、Microsoft 社のクラウドサービスの 1 つである Office 365 が世界的な障害により、アジアや欧州の顧客を中心にサービスの利用ができない状態が継続。
- ○ 代表的なクラウドサービスは、高度な運用を実施しているとされているが、大小様々な障害が一定の割合で発生。
- ○ クラウドサービスは、障害が発生すると、影響範囲が大きくなることがあり、障害が起きた場合の事業継続に関してのリスク対策が必要。

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 海賊版サイト遮断措置について[13]

- ○ 政府は、インターネット接続事業者に対し、特定の海賊版サイトへのサイトブロッキングを促す緊急対策を決定。
- ○ 当該対策は法整備が行われるまでの緊急的な措置。
- ○ インターネット広告等が海賊版サイトの資金源となっている。ため、広告収入等を断つための方策も検討する必要。

3.1.2 内閣府 Web サイトからの意図しない外部サイトへのリンクについて[14]

- ○ 内閣府が主催したシンポジウムの告知用 Web サイトに使われたドメインが、シンポジウム終了後に第三者に取得され、異なる内容の Web サイトにリンク。
- ○ 原因は、有効期限が切れた当該ドメインを含む URL の削除漏れ。
- ○ 同様の問題を防ぐため、ドメイン管理の徹底とともに、新規 Web サイト立ち上げ時の政府ドメイン「go.jp」の使用が必要。

3.1.3 情報公開時における機微情報等の流出事案について[15]

---

[12] *OUTAGE.REPORT「Office 365 Down? Service Status,Map,Problems History」、https://outage.report/office-365#2018-04-06（2018/7/27 閲覧）*
OUTAGE.REPORT「Recent Outage」、https://outage.report/（2018/7/27 閲覧）
経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版」、http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf（2018/7/27 閲覧）

[13] *知的財産戦略本部「インターネット上の海賊版サイトに対する緊急対策(2018/4/13)」、https://www.kantei.go.jp/jp/singi/titeki2/kettei/honpen.pdf（2018/4/27 閲覧）*
読売新聞「海賊版サイトの「収入源根絶」、広告規制が対策の切り札(2018/5/7)」、https://www.yomiuri.co.jp/science/feature/CO017291/20180507-OYT8T50012.html（2018/5/7 閲覧）

[14] *ITmedia NEWS「内閣府のサイトから風俗体験記にリンク 削除忘れドメイン失効→第三者が再取得(2018/5/9)」、http://www.itmedia.co.jp/news/articles/1805/09/news089.html（2018/6/7 閲覧）*
政府 CIO ポータル「Web サイト等の整備及び廃止に係るドメイン管理ガイドライン(2018/3/30)」、https://cio.go.jp/guides（2018/6/7 閲覧）

[15] *産経ニュース「【原発最前線】原発構内図を誤って公開…職員が偽書類作成…「不祥事」相次ぐ規制庁(2018/4/24)」、https://www.sankei.com/premium/news/180424/prm1804240005-n1.html（2018/6/7 閲覧）*
日本経済新聞「ネットで出回る「黒塗り」外し文書 入管開示でミス(2018/4/26)」、https://www.nikkei.com/article/DGXMZO29880620W8A420C1AC8000/（2018/6/7 閲覧）
神戸新聞 NEXT「神戸中 3 自殺 黒塗り外せる文書を一時開示 市教委(2018/5/1)」、https://www.kobe-np.co.jp/news/sougou/201805/0011216274.shtml（2018/6/7 閲覧）
毎日新聞「大阪市教委ミス：黒塗り個人情報、HP で閲覧可能(2018/5/3)」、https://mainichi.jp/articles/20180503/ddn/041/040/047000c（2018/6/7 閲覧）

○ 情報公開時における機微情報等の流出事案が多数発生。原因は、PDF 操作の不備等の人為的なミス。

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[16]

3.2.1 複数の EC サイトにおけるクレジットカード情報の漏えい

○ 2018 年 5 月以降、複数の EC サイトにおいてクレジットカード情報等の個人情報が漏えいしたと公表。
○ カード情報や利用者情報は、適切な管理や不正利用の防止等のセキュリティ対策が義務付け。

3.2.2 金融分野におけるシステム障害事案[17]

○ みずほ証券のインターネット経由で株式を売買するシステムである「みずほ証券ネット倶楽部」がシステムの設定ミスにより、2 日間利用できない障害が発生。
○ りそな銀行、セブン銀行等複数の銀行で、使用する外部の認証サービスの問題により、インターネットによる振込サービスが使用できない障害が発生。

3.2.3 仮想通貨関連の最近の事案等について[18]

○ 多くの仮想通貨相場は、2018 年 1 月以降、下落傾向。
○ 仮想通貨交換業者「コインチェック」への不正アクセス事案発生以降、多くの交換業者に対する行政処分が実施。
○ 仮想通貨マイニング関連で 16 人が摘発。

3.3. その他の事案

NHK ニュース「「森友」交渉記録 黒塗り見える状態で掲載 財務省(2018/5/24)」、https://www3.nhk.or.jp/news/html/20180524/k10011450641000.html (2018/5/30 閲覧)

[16] *株式会社ナカミツ「不正アクセスによるカード情報流出に関するお知らせとお詫び(2018/5/21)」、http://www.worldimporttools.com/ (2018/5/30 閲覧)*
森永乳業株式会社「(第一報)健康食品通販サイトにおけるお客さま情報の流出懸念に関するお知らせ(2018/5/9)」、http://www.morinagamilk.co.jp/information2/newsentry-2876.html (2018/5/30 閲覧)
株式会社ダブリュ・アイ・システム「エースコンタクト会員専用サイト「A-Web 倶楽部」におけるお客様情報流出に関するお詫びとお知らせ(2018/5)」、http://www.menicon.co.jp/company/news/vol679.html (2018/5/30 閲覧)
株式会社一康商事「「こうのとり検査薬.NET」への不正アクセス発生についてのご報告とお詫び(2018/5/23)」、https://kensayaku.net/user_data/info20180523.html (2018/5/30 閲覧)
経済産業省「割賦販売法」、http://www.meti.go.jp/policy/economy/consumer/credit/11kappuhanbaihou.html (2018/6/20 閲覧)

[17] *みずほ証券「ネット倶楽部サービスの再開について(2018 年 6 月 28 日 12:00 再開)(2018/6/28)」、https://www.mizuho-sc.com/information/pdf/20180628_2.pdf (2018/7/10 閲覧)*
日経 xTECH「りそなやセブン銀行のネットバンキングで障害、ワンタイムパスワードでエラー(2018/6/27)」、https://tech.nikkeibp.co.jp/atcl/nxt/news/18/01744/ (2018/7/10 閲覧)

[18] *DMM Bitcoin「チャート・レート一覧」、https://bitcoin.dmm.com/info/trade_chart_rate_list (2018/7/5 閲覧)*
仮想通貨に関する総合ニュースサイトビットプレス「【金融庁】仮想通貨交換業者に対する行政処分&詳細まとめ(2018/6/22)」、https://bitpress.jp/news/information/entry-8147.html (2018/7/5 閲覧)
産経ニュース「違法マイニングで 16 人摘発 10 県警、仮想通貨獲得で不正アクセス(2018/6/14)」、https://www.sankei.com/affairs/news/180614/afr1806140035-n1.html (2018/6/28 閲覧)

3.3.1 フィッシングメールによる被害[19]

○ 複数の大学で、Office 365 の管理者を騙るフィッシングメールにより、認証情報が搾取され、約 12,000 人分の個人情報が漏えい。

○ 実在の企業を騙り、偽の当選通知メールや実在の企業を装ったフィッシングメールが相次ぎ発生。

4. 脅威動向

4.1.1 サイバー空間を巡る米ロの攻防[20]

○ 2018 年 3 月には米国が、同年 4 月には米英両国が、ロシアが関与するサイバー攻撃について警告。

○ 他方、ロシア及びイランにおいてもサイバー攻撃が発生したとの報道。

5. 技術動向

5.1.1 NIST Cyber Security Framework の最新版(Version1.1)をリリース[21]

○ NIST Cyber Security Framework のバージョン 1.1 がリリース。

○ バージョン 1.0 に対して、「サプライチェーンリスク管理」がフレームワークコアに追加され、セルフアセスメントの章がガイドに追加。

○ 米国連邦政府機関では、本フレームワークの使用が義務付けられ、重要インフラをはじめとする民間組織でも引き続き利用。

以上

---

[19] *日経 xTECH「6 大学で 1 万件超の情報流出、文科省がフィッシングメールの注意喚起(2018/6/29)」、https://tech.nikkeibp.co.jp/atcl/nxt/news/18/01788/ (2018/7/10 閲覧)*
日本フィッシング対策協議会「緊急情報(2018/7/4)」、https://www.antiphishing.jp/news/alert (2018/7/12 閲覧)

[20] *US-CERT「Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors(2018/3/16)」、https://www.us-cert.gov/ncas/alerts/TA18-074A (2018/7/30 閲覧)*
US-CERT「Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices(2018/4/20)」、https://www.us-cert.gov/ncas/alerts/TA18-106A (2018/7/30 閲覧)
ZDNet Japan「ロシアやイランでシスコのスイッチ製品に対する攻撃が発生(2018/4/10)」、https://japan.zdnet.com/article/35117462/ (2018/7/30 閲覧)

[21] *NIST「New to Framework」、https://www.nist.gov/cyberframework/new-framework (2018/7/30 閲覧)*
Whitehouse「Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure(2017/5/11)」、https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (2018/7/30 閲覧)

平成 30 年 10 月 29 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 年度前期分）

「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	49	―	―	118
関係省庁・関係機関からのNISCへの情報共有	27	52	41	19	0	1	―	―	1
NISCからの情報提供	38	44	80	54	7	17	―	―	24

※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	7	―	―	14
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	―	―	8
	完全性を脅かす事象	情報の破壊	14	52	47	20	5	7	―	―	12
	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	―	―	41
	上記につながる事象	マルウェア等の感染	27	111	289	65	9	2	―	―	11
		不正コード等の実行	3	11	10	13	2	1	―	―	3
		システム等への侵入	12	27	26	17	6	1	―	―	7
		その他	12	24	44	35	15	7	―	―	22

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

平成 30 年 10 月 29 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、今後は、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ご承知おきいただきたい。

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

自然災害、システム設定の不具合、ネットワーク機器の不具合、システム更新の不具合、及び、内部の人的統制の不具合等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。

○　業務手順における監査の必要性

正規の手順に反して業務利用していたフリーメールアカウントがリスト型攻撃による不正アクセスを受ける事例が発生し、結果として情報が漏えいした。

（２）障害発生後の対応に関するもの

○　被害軽減のための復旧要領の確立・訓練及び代替情報公開手段への配慮

同一の原因により、複数事業者にわたるシステム障害事案が発生した際、事業者によって復旧の迅速性に差異がみられた。

また、重要インフラサービスに障害が起きた際、復旧見込みに関する情報を公開する Web サイトにも障害が及ぶ事案があったが、SNS で代替し、適時の情報公開が維持された事例もあった。

以上