第２節　技術上の課題

日本大学危機管理学部　教授　美濃輪　正行

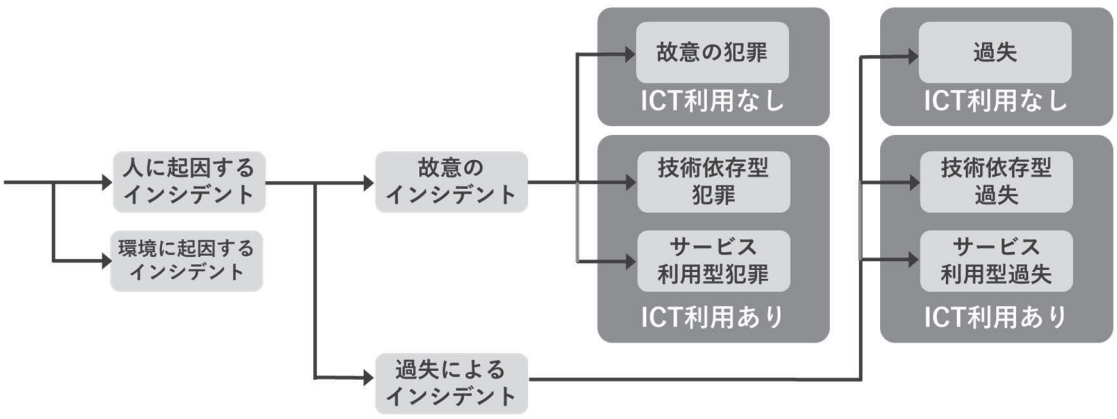
Ⅰ　情報セキュリティと ICT の関係

本節では ICT が主因となる情報セキュリティの課題を取り上げる。情報セキュリティのインシデントと ICT の関係を整理して、その対象を明示した上で考察する。

本節及び次節では、情報セキュリティに関するインシデントを図表 1 の通り分類して扱う。人に起因するものと環境に起因するものによってまず大別する。例として､ハードウェアの障害によるサービス停止は環境に起因するものの分類となる。人に起因するインシデントは、更に故意か否かによって分類する。故意であるものについてインシデントの主体者つまり攻撃者に ICT の利用があるか否かで細分化する。故意のインシデントで　かつ ICT の利用があるものは、英国内務省の分類[1]に倣って、技術依存型犯罪とサービス利用型犯罪としている。この 2 者が所謂サイバー犯罪である。サービスを構成する情報技術に改変等を行う犯罪か、手段としてサービスを利用する犯罪か、が 2 者の相違点である。尚、ICT の利用がない場合も、個人情報を含む文書の窃盗や機器の物理的破壊等は ICT 利用無しの分類となる。

下記の図では技術依存型のサイバー犯罪はサービス利用型犯罪を二者択一としているが、現実には技術依存型犯罪はサービス利用型の特性を合わせ持ち、その関係は不可分である。メールによる攻撃を例に考えると、メール内の添付ファイルを開封させたり、リンクをクリックさせたりする場合も、添付ファイルのマルウェアやリンクは技術に依存し、かつメールのサービスを介し、メールの文面は巧妙で不正行為に導くものとなっている。サービス依存型の犯罪には、マルウェアを含まないジャンクメールの発信、インターネッ

図表 1　情報セキュリティにかかるインシデントの分類



ト上の不当な個人情報の公開等が含まれる。

過失によるインシデントも故意のインシデントと同様に ICT 利用の有無と技術依存型か、サービス利用型かの分類の考え方が適用できる。ICT 利用がない場合の過失は機密情報を含む書類の紛失、技術依存型の過失はコンピュータ利用者の設定ミスによる個人情報の不慮の公開、サービス利用型にはメールの誤送信による機密情報の漏洩が例として挙げられる。

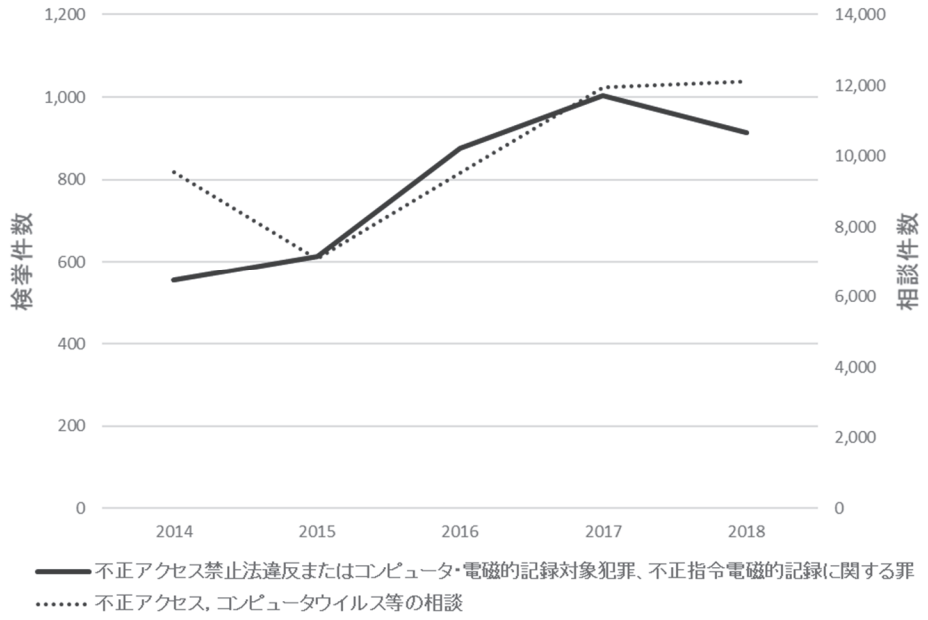
情報セキュリティのインシデントにとって ICT 利用は必要条件ではないことを強調したい。但し、被害の規模が大きいインシデントは技術依存型犯罪であり、国内の事例で考えると、2018 年に発生したコインチェック社の仮想通貨流出事件[2]、2014 年にベネッセ社で発生した個人情報流出事件[3]がその典型である。尚、その影響を勘案して、本節では技術依存型のサイバー犯罪を主に取り上げる。

Ⅱ　技術依存型犯罪の状況

技術依存型犯罪は適切な防御策をとっていれば被害に遭遇する可能性も低くなる。そのため、技術依存型犯罪の状況はその被害件数や規模の他、サイバー攻撃の試行がどの程度発生しているか理解することが第一歩である。

先ず技術依存型犯罪の国内のサイバー犯罪の件数について考察する。データは警察庁が 2019 年 3 月に発表したサイバー犯罪に関する統計値[4]を用いる。統計値には、全ての犯罪種別の検挙数や相談件数を含むが、著作権法違反、インターネットを介した詐欺行為、児童ポルノ法違反の件数は除外して不正アクセスとウイルスに限定して考察する。検挙件数

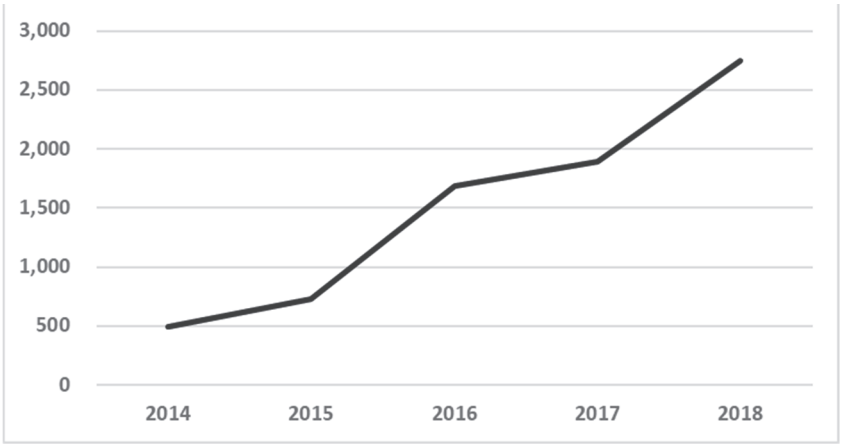
図表 2　技術依存型サイバー犯罪の検挙件数と相談件数



は、2014 年から 2018 年まで上昇基調であったが、2018 年には微減となっている。2018 年の統計値でみると、検挙件数 913 件に対して相談件数は 12,113 件である。他種の犯罪に比して全サイバー犯罪の検挙件数が少ないことから実態は判然としない[5]。

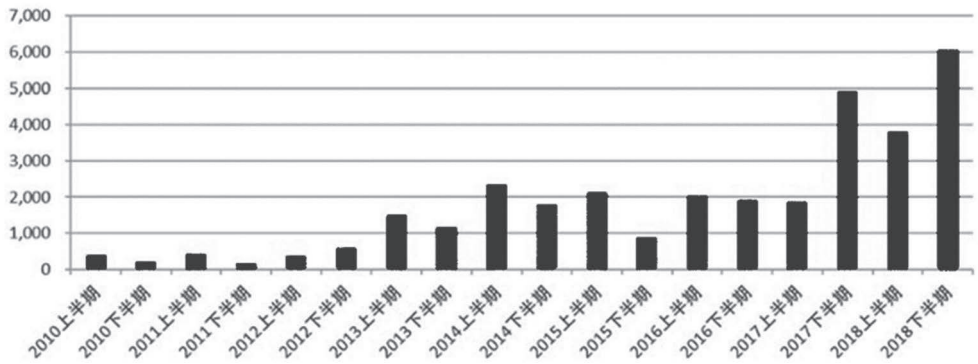
サイバー攻撃の初期段階においてはインターネット上のノードに対して通常の利用では想定されないアクセスが発生する。この状況を表すものとして、インターネット空間に試験的に設置されたセンサーに対する一日当たりのアクセス件数[6]が警察庁から公表されている。年別の推移をまとめたものが図表 3 である。サイバー攻撃の試行含むこのアクセス件数が年々上昇している。2019 年上半期の同値の集計では、前年の平均値が 2752.8 件に対して 3530.8 件、約 3 割の増加となっている[7]。2018 年 11 月に警察庁が公開した資料[8]の詳細な実績値でみると、その攻撃の内容は、サービスの妨害を意図した SYN/ACK リフレクター攻撃、インターネット上に公開されたサーバ構成の探索行為、特定のネットワークカメラ等の脆弱性を標的としたアクセスの試行を含み、攻撃内容ごとに一日・一 IP アドレスに対して最大アクセス件数は、順に 140,000 件、400 件弱、30 件超であり、攻撃手法によって大きく異なる。グラフの件数値は同一犯ごとに集約されたものではないこと、攻撃の内容によって影響は異なることの事情はあるが、全体的にインターネット空間での技術依存型犯罪に展開する初期段階のサイバー攻撃の発生頻度は上がっていることが分かる。

図表 3　センサーに対するアクセス件数（件／日・IP アドレス）



サイバー攻撃が活発化していることを示す統計値としては、フィッシング対策協議会が公開して

図表 4　フィッシングサイトの件数
（フィッシング対策協議会「フィッシングレポート 2019」より引用）



いるフィッシング詐欺やマルウェア感染を狙ったフィッシングサイトの件数[9]も参考になる。この件数の値は、フィッシングの届け出があったサイトの URL 文字列の重複を排除した件数であり、攻撃手口の多様性を表している。佐川急便を騙って SMS 経由でフィッシングサイトに誘導してマルウェア感染させる事案が大きく報道された[10]が、このような攻撃の手口が多数存在することを意味しており、依然としてサイバー攻撃が活発であることが分かる。

Ⅲ　サイバー攻撃の局面の考察

サイバー攻撃の対策を考える上で、攻撃の特性や手口の内容を理解することは有益であるが、被害に遭遇した場合に被害者が置かれている状況を適切に認識することは特に重要である。攻撃者の立場で局面を示すフレームワークとしては、サイバーキルチェーン[11]が知られている。これは Advanced Persistent Threat に対応したフレームワークであり、「偵察」「武器の準備」「配送」「攻撃」「導入」「遠隔操作」「目的活動」の局面で構成される。当該脅威のフレームワークに特化したものであり、サイバー攻撃全般を前提に考えると不要な項目も含まれる。よって、本論文では、①準備局面、②攻撃実行局面、③収穫局面の 3 局面に分けて考察する。この局面化の意図は、サイバー攻撃の多くの事案について、汎化された局面の考え方を以って手口や対策を考察するものである。

この局面化の①準備局面は、攻撃対象の情報の収集・選定、攻撃用ツールの開発、攻撃対象の環境の調査、攻撃計画の立案等を含む。この局面では被害者との直接的な接点は持たない。攻撃計画には、被害者にどの様に攻撃を仕掛けるか、犯行の隠蔽を図るための対策、最終的な目的をどのように達成するか等の内容も含む。②実行局面では、実際に攻撃を仕掛けるが、この局面は被害者及びその環境に働き掛ける行為全てを含む。被害者が認識しているか否かを問わず、この局面での対応によって被害を受けるか否かが決まる。③収穫局面では、②実行局面での成果を活用してサイバー攻撃の目的を達成する。この局面では被害者が被害を受けていることを明確に認識している場合もあればそうでない場合もある。

この局面化の考え方をいくつかのサイバー犯罪の事例に適用して考える。ランサムウェアに感染させて仮想通貨の支払いを求める WannaCry[12]のケースであれば、①準備局面では、ランサムウェアの感染手段の選定、被害者のメールアドレスの入手、ランサムウェア及び感染させるためのサイトの構築及びランサムウェアの開発、発信用メールアカウントの確保、メール文面の作成、仮想通貨口座の開設、暗号化キーの準備等の作業が挙げられる。②実行局面では、ランサムウェアに感染させるためのメールの送信、仮想通貨の入金があった場合の復号キーの送信、③収穫局面では、仮想通貨の現金化となる。年金基金の個人情報流出の事案[13]であれば、①準備局面は WannaCry とほぼ同じであるが、②実行局面と③収穫局面の区分は明確ではない。被害者の環境を探索する行為は実行局面となるが、個

人情報の大量入手自体を最終的な目的と解釈すれば、実行局面の最後に大量の情報をC2サーバに転送することが収穫局面となり、実行局面と収穫局面の明確な差異はなくなる。大量に入手した情報によって何某かの対価を得ることが目的ならば、その行為が収穫局面となる。WannaCryと年金基金の個人情報流出を比較して注意すべき点は、被害者がどの様な被害に遭遇しているか認識している場合もあればそうでない場合もあるという点である。また、企業・組織のイメージダウンや政治的メッセージをアピールすることを狙ったホームページの不正書き換えのケースでは、②実行局面と③収穫局面は攻撃者にとって差異はなく、被害者が被害状況を認識するまでの時間も短い。

Ⅳ　昨今の手口の傾向

昨今の被害の規模が大きかった技術依存型犯罪の特徴として、次の点が挙げられる。

①　攻撃者は局面毎に十分な時間をかけていること

②　目標達成のために広範な対象が標的となりうること

③　攻撃技術が高度に発達してきたこと

これらの特徴は、全ての攻撃に該当するものではないが、個々の事案についてはいくつかの特徴が該当する。次節よりその代表的な事例及び手口を取り上げて、これらの特徴について解説する。

Ⅴ　ビジネスメール詐欺

ビジネスメール詐欺の手口は、メールアカウント情報を窃取することから始まるが、その多くはクラウドサービスのメールを利用していることが前提となっている。クラウドサービスであればインターネットに接続された環境から容易にアクセスすることが可能であるが、ローカルデバイスにデータを保管するPOP3/Sendmail形式のメールではアクセス不可である。一旦メールアカウントを入手すると、メールの内容を参照することが可能となり、その後は巧妙ななりすましメールによって被害者を騙して不正行為を働く。

米国司法省が2017年3月に匿名のIT企業2社で100万ドル超の被害が発生したことを公表した[14]。更に翌4月にフォーチュン紙がこの2社がFacebookとGoogleであることを報道した[15]。司法省の発表によれば、犯人はリトアニアのエヴァルダス・リマサウスカス(Evaldas Rimasauskas)を中心とするグループであり、電子メールアドレス、請求書、社印を偽装、二社の経理部から2013年から2015年にかけて2年間にわたり、二社と取引があるアジアのQuanta社と偽って$ 100万超を騙し取った。この攻撃において犯行グループは、Quanta社と同名の会社を設立、エヴァルダス・リマサウスカスは被害を受けた二社の役員になりすまして請求書、契約書、レター等をやりとりしていた。また、詐取した金銭は様々な国の口座に分散して送金されている。国際的な協力を得てFBIは、被害の多

くを回収することができたとしている。しかしながら、Facebook、Google の 2 社からコメントは出されていない。この事案においては、攻撃の期間が長期に及んでいたことから、非常に計画性が高かったことが窺える。

Ⅵ　サプライチェーン攻撃

サイバー攻撃の手口を表す用語は、技術的な手段を指すもの、攻撃の操作を指すもの等があり、分かり難さの一因となっている。前者の代表的なものにはマルウェアやフィッシング・サイトが該当し、後者にはなりすましや DoS 攻撃等が該当する。また、ランサムウェアはマルウェアの一種であるが、この操作は攻撃の目的の意味も持ち合わせる。更にサプライチェーン攻撃は攻撃の対象を指す用語であり、本来の対象を直接攻撃するのではなく、その組織のサプライチェーンを狙った攻撃を意味する。

但しその解釈は多様性を持つ[16]。国内の事例では委託開発会社の社員が偶然 PC のデータをコピーできることを発見したベネッセの個人情報流出事件や平成 26 年 1 月に判決が下されたインテリア商材の会社のプログラムの委託開発に原因する個人情報漏洩の事案[17]等もこの分類に含まれる。後者はインテリア商材の卸小売、通信販売を行う会社が、自社のウェブサイトの受注システムの開発保守をソフトウェア開発会社に委託し、そのシステムの脆弱性によって SQL インジェクション攻撃が実行されカード情報が盗まれた事案である。これらの事案では、脆弱箇所の開発については、攻撃者が直接関与した訳ではない。

2017 年 7 月、ウクライナでは 80%の企業が利用している会計ソフトウェア M.E.Doc の更新版のソフトウェアにマルウェア紛れ込んで配信され、個人情報が盗まれた[18]。この事案の攻撃者は製品の開発システムに侵入し、配信ソフトウェアへの改竄を図ったものと考えられる。製品やサービスとして提供する対象にマルウェアが混入する事案としては、ファーウェイ製品にまつわる情報漏洩の疑惑がある[19]が実態は定かでない。コンピュータ上で稼働するソフトウェアであれば、サイバー攻撃の判別は容易であるが、ハードウェアに組み込まれているファームウェア上に攻撃因子が組み込まれている場合、その判定は困難である。仮にそのハードウェアに製品上の問題分析のため、一部の処理データをベンダに送信する仕様が備わっている場合は、その機能によって収集されるデータの利用はベンダの良心に委ねられ、一概に善悪の判断は難しい。

2018 年 に NIST が ”Framework for Improving Critical Infrastructure Cybersecurity Version1.1”の中で”Cyber Supply Chain Risk Management”の記述を追加した。ここでは、サイバーセキュリティ要件をまとめて、サプライヤーと検査条件について合意、検査・管理を行うことが提示されている。現実的に様々な経路で攻撃が企てられている状況では、自組織に関連するサプライチェーンも含めて広い範囲を考慮する必要がある。

Ⅶ　DNS 環境改竄

2019 年 1 月 22 日に米国土安全保障省から Emergency Directive 19-01[20] が発動された。その表題は "Mitigate DNS Infrastructure Tampering" であり、DNS 及び Web サイトの証明書を含む環境が偽のサイトに誘導されていることを指摘する内容であった。本緊急指令が発動される前に、ベンダより "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale"[21]、"DNSpionage Campaign Targets Middle East"[22] が公開されており、米国土安全保障省の発表はこれを受けての対応であった。前者の発表によれば攻撃の対象となったのは、中東、北アフリカ、ヨーロッパ、北アメリカの政府、通信会社、インターネット関連の会社であった。日本国内でも日本レジストリサービスが「(緊急) 米国国土安全保障省による DNS 設定の改ざんに関する緊急指令の公開について」の表題で緊急指令があったことを取り上げている [23]。統一的な命名は定まっていないが、ここでは他の攻撃と差異を明確にするために DNS 環境改竄と表記する。

従来から DNS に関係する攻撃には、DNS キャッシュサーバを対象にした DNS ポゾニング、DNS のプロトコルを悪用した DNS トネリング、DNS BIND の脆弱性を狙った DoS 攻撃が存在する。今回の攻撃の内容は、DNS 設定の改竄、正規サイトに成りすましたサーバ証明書の発行、正規サイトの経路上の介入であり、攻撃対象は DNS の機能の範囲に留まらない。DNS 環境改竄は、DNS サービスを提供しているサイトに何らかの方法で侵入することから始まる。ホスト名から IP アドレスを導出する A レコード、名前解決の権限サーバを示す NS レコード、メールサーバを示す MX レコードの設定を攻撃目的に応じて改竄する。更に攻撃対象のサイトに SSL が設定されている場合は、無償で利用できる“Let’s Encrypt”のサービスを利用して正規サイトになりすますためのサーバ証明書を発行して、自らのサーバに設定する。なりすまし用サイトは通信データが経由することが目的であるため、プロキシサーバ相当の機能となるが、情報窃取の機能を併せ持つ。本攻撃ではユーザの通信は正規のアクセスに比較して別サーバを経由するだけであり、若干の遅延はあるもののユーザが認識することは困難である。前述の緊急指令が管理者側の対応として求めたのは、DNS 設定変更アカウントの管理の徹底、DNS 設定の確認、ログの監査である。この DNS 環境改竄は既成概念を覆す高い技術レベルの攻撃の一例である。

Ⅷ　技術上の課題

本節ではサイバー攻撃に絞って考察したが、その課題は次の通りである。

・サイバー攻撃の被害件数は増加基調であり、攻撃の頻度も高くなりつつあること

・サイバー攻撃の手口は広い範囲に及び、かつ高度化していること

次節ではこの状況への対応も考慮してセキュリティ管理上の課題について考察する。

◆さらに学ぶための参考文献

・神保哲生（2017 年）『PC 遠隔操作事件』（光文社）
・Michal Zalewski（2012 年）『めんどうくさい Web セキュリティ』（翔泳社）
・中村行宏・横田翔（2015 年）『事例から学ぶ情報セキュリティ』（技術評論社）

---

[1] Dr. Mike McGuire and Samantha Dowling(2013) "*Cyber crime: A review of the evidence Research Report 75*" http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf ; Dr. Mike McGuire and Samantha Dowling(2013) "*Cyber crime: A review of the evidence Research Report 75*" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf (2019 年 09 月 20 日アクセス)
[2]「コインチェックの仮想通貨不正流出、過去最大 580 億円」日本経済新聞社 2018/1/27
[3]「ベネッセ HD、最大 2070 万件の顧客情報漏洩か　住所・電話番号など」日本経済新聞社 2014/7/9
[4] 警察庁　(2019 年 3 月 7 日)「平成 30 年におけるサイバー空間をめぐる脅威の情勢等について」P.8「2 サイバー犯罪の情勢等」
[5] 金山泰介 (2017)「サイバー犯罪被害実態調査（第 1 回）の結果について」日本大学危機管理研究 創刊号　P.102「 I 調査の背景とその概要」
[6] 警察庁　(2019 年 3 月 7 日)「平成 30 年におけるサイバー空間をめぐる脅威の情勢等について」P.1「1 サイバー犯罪の情勢等」
[7] 警察庁　(2019 年 9 月 26 日)「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」P.2「1 サイバー攻撃の情勢等」
[8] 警察庁　(2018 年 11 月 30 日)「宛先ポート 80/TCP を利用した SYN/ACK リフレクター攻撃とみられる観測等について」P.1「1 宛先ポート 80/TCP を利用した SYN/ACK リフレクター攻撃とみられる観測」
[9] フィッシング対策協議会「フィッシングレポート 2019」 P.2「1.1. 国内外の状況」https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf　(2019 年 10 月 13 日アクセス)
[10]「『佐川急便』をかたる偽 SMS が横行　不正アプリを導入しないで！【サイバー護身術】」読売新聞　2018/07/30
[11] Lockheed Martin "*THE CYBER KILL CHAIN*" https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (2019 年 10 月 13 日アクセス)
[12] Zack Whittaker "*Two years after WannaCry, a million computers remain at risk*" TechCrunch https://techcrunch.com/2019/05/12/wannacry-two-years-on/ (2019 年 10 月 13 日アクセス)
[13]「予兆はあったが防げず　狙われた年金情報」日経新聞　2015/6/10
[14] U.S. Department of Justice(March 21, 2017) "*Lithuanian Man Arrested For Theft Of Over $100 Million*"　https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme　(2019 年 09 月 24 日アクセス)
[15] "*Exclusive: Facebook and Google Were Victims of $100M Payment Scam*" FORTUNE 2017/4/27
[16] 情報処理推進機構セキュリティセンターセキュリティ対策推進部セキュリティ分析グループグループリーダー小川 隆一研究員 小山 明美 (2019)「サプライチェーンのセキュリティ脅威に備える」P.8「事故事例」
[17] 同上　P.9「委託先へのサイバー攻撃②」

[18] “*Police seize servers of Ukrainian software firm after cyber attack*” REUTERS 2019/10/18
[19]「重要インフラの情報漏洩懸念　官民、安保リスクに対処」日経新聞　2019/4/2
[20] CISA “*Emergency Directive 19-01 Mitigate DNS Infrastructure Tampering*” 2019/01/22
[21] Muks Hirani, Sarah Jones, Ben Read (2019/01/10) “*Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*” FireEye Threat Research https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html (2019 年 10 月 25 日アクセス)
[22] Warren Mercer and Paul Rascagneres (2018/11/27) “*DNSpionage Campaign Targets Middle East* “ CISCO TALO (2019 年 10 月 25 日アクセス)
[23] 株式会社日本レジストリサービス (2019/01/28)「(緊急) 米国国土安全保障省による DNS 設定の改ざんに関する緊急指令の公開について」 (2019 年 10 月 25 日アクセス)