「現代のサイバーセキュリティの法的課題についての国際的な研究」に関する調査報告書

－ランサムウェアによる被害の実情及び支払いの可否に対する議論の動向、その他の対応における注目すべき事案－

株式会社 IT リサーチ・アート

はじめに

本報告書は、ランサムウェアによる被害の実情及び支払いの可否に対する議論の動向、その他の対応における注目すべき事案について、国際的な観点からまとめようとするものです。

もっとも、本調査は、調査委託期間の関係もあり、2021 年 3 月 10 日時点における情報をもとにしています。その後、米国においてコロニアルパイプライン事件等が発生しており、本調査報告書の公開にあたっては、同事件の情報を追加しています。

もっとも、同事件を契機に、米国において、重要インフラに対するランサムウェア攻撃への対応体制、復旧計画の見直し、捜査体制の問題、身代金支払いの問題についての議論が深まっていますが、それらの問題については、今後の研究課題となります。

なお、本報告は、経済産業省委託調査「令和２年度サイバー・フィジカル・セキュリティ対策促進事業（サプライチェーン・セキュリティ対策に関する調査）」（委託先　株式会社三菱総合研究所）において作成した「現代のサイバーセキュリティの法的課題についての国際的な研究に関する調査報告書」（株式会社 IT リサーチ・アート）を元に作成しました。

令和３年８月３日

株式会社ＩＴリサーチ・アート
代表取締役弁護士　高橋郁夫

（調査分担）
西貝吉晃　（千葉大学　准教授）
有本真由（弁護士）

内容

1　各国における代表的なランサムウェア被害事案

1.1　概念

ランサムウェアは、コンピュータシステム上のデータを暗号化してエンドユーザが使用できないようにする犯罪者によって配備された悪質なソフトウェア、又はマルウェアの一種であると定義することができる。サイバー犯罪者は、身代金が支払われるまでデータを人質にする。身代金が支払われない場合、被害者のデータは無期限に利用できないままになったり、一般の人々に公開されたりする可能性がある。

1.2　歴史

最初のランサムウェアは、1989 年の PC Cyborg であるとされる[1]。この攻撃は、エイズ研究者のジョセフ・ポップ博士が、90 カ国以上のエイズ研究者にフロッピーディスク 2 万枚を配布し、その中にはアンケートを使って個人のエイズ発症リスクを分析するプログラムが含まれていると主張して実行させたものである[2]。このランサムウェア攻撃は、「AIDS トロイの木馬」又は「PC サイボーグ」といわれている。

その後、2000 年代までは、ランサムウェアは、一般的ではなかった。その後、2000 年代中盤に RSA 方式（1024 ビット鍵）で暗号化される方式のランサムウェアが出現した。具体的には、TROJ／RANSOM.A（2006 年）[3]、Archiveus（2006 年）、Gpcode（2006 年）[4]などがある。また、2011 年には、マイクロソフトライセンス認証を模倣するランサムウェアが発生した。これは、利用者が、真正な通知との違いがわからないために、国際電話番号に電話をしてしまい高額な国際電話料金を発生させるというものであった。その後、種々のランサムウェアが流行した。その手法は、OS もしくはブラウザをブロックするタイプと暗号化するものとに分けられる。

例えば、カスペルスキー社の報告[5]によれば、2015 年度（2015 年 4 月から 2016 年 3 月、

---

[1] https://www.nomoreransom.org/ja/ransomware-qa.html　また、https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time　による。

[2] このマルウェアプログラムは、このプログラムは、最初はコンピュータの電源を 90 回入れただけで起動し、コンピュータの電源が入らない状態のままにするもので、マルウェアは 189 ドルの支払いを要求するメッセージを表示し、さらにソフトウェアのリース料として 378 ドルを要求するものであった。

[3] https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Ransom-A/detailed-analysis.aspx　また、「30 分ごとにファイルを一つずつ消していく「Troj/Ransom-A」（https://gigazine.net/news/20060501_troj_ransom_a/）

[4] 「ランサムウェア「Gpcode」で暗号化されたファイルの復元方法が公開」（https://www.itmedia.co.jp/enterprise/articles/0806/18/news102.html）

[5] https://securelist.com/pc-ransomware-in-2014-2016/75145/
2016 年度は、KSN Report: Ransomware in 2016-2017（https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/）、
2017 年度については、KSN Report:Ransomware and　malicious cryptominers　2016-2018（https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/）
その後、2019 年以降については同社によるランサムウェアに集中した調査は見当たらないが、一般的なものとして「2019 年のストーリー：ランサムウェア猛威の下の街」（Story of the year 2019: Cities under ransomware siege）（https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/）

以下同じ）におけるランサムウェアの被害件数は、2014 年度に比較して、17.7%増加しており、2016 年度は、11．4%増加している。また、特に暗号化のタイプのランサムウェアが急激に増大したことが報告されている。被害者の傾向は、従前は家庭ユーザが一般的であったが、その後、企業を狙ったランサムウェアが出現・増加している。もっとも、同社の調査によれば、2017 年度においてランサムウェアは、30%ほど減少したが、2018 年度においては、ランサムウェアの被害が再度、増大している。また、2021 年には、米国において、コロニアルパイプラインが発生し、重要インフラに被害が発生した事件として社会的な注目を浴びた。

各国で特徴的な被害を惹起したものとしては、以下のような事例がある。

1.3　報道等がなされた事件

世界的規模

ランサムウェアで世界的な被害を惹起したものとしては、WannaCry（2017）、NotPetya（2017）などがある。

米国[6]

SamSam ランサムウェア事件（2018）は、特にアメリカの地方自治体に対して被害を惹起した。具体的には、2018 年 3 月にアメリカ・アトランタ市のシステムに対して攻撃がなされ、市や警察などの公共機関が機能不全に陥っただけでなく、バックアップデータをも失われたという事件を引き起こしている[7]。

Ryuk（2020）は、アメリカの病院等を標的にしたランサムウェアである。また、米国の郡（カウンティ）も被害にあっており、多額の身代金を支払わなければならなかったとされている[8]。

Robinhood（2019）は、北米の 2 都市、ノースカロライナ州グリーンビルとメリーランド州ボルチモアの重要な IT システムをロックし、対応する公共サービスを停止させたと報道されている[9]。

コロニアルパイプライン事件（2021）は、アメリカの燃料送油管会社コロニアル・パイプラインが 2021 年 5 月 7 日にサイバー攻撃を受け、従業員の画面に身代金要求のメッセージ

---

[6] 2020 年のランサムウェアの状況の報告書として、　「米国におけるランサムウェアの状況：報告と統計」（The State of Ransomware in the US: Report and Statistics 2020）（https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/）などがある。

[7] SamSam についての詳細な分析としてソフォス「SamSam: 600 万ドル (約 6 億 7000 万円) 近くの身代金を手にしたランサムウェア」（https://www.sophos.com/ja-jp/press-office/press-releases/2018/08/samsam-the-almost-6-million-ransomware.aspx）がある。

[8]後述の 「ランサムウェア　その実態と対応（What it is & What to Do About It）」による。

[9] この記事としては「新種のランサムウェア RobbinHood がアメリカの自治体を攻撃」（https://www.acronis.com/ja-jp/blog/posts/xin-zhong-noransamuuearobbinhoodgaamerikanozi-zhi-ti-wogong-ji）。また、上記「ランサムウェア　その実態と対応（What it is & What to Do About It）」においても言及がなされている。

が表示され、流出したデータのサンプルへのリンクがあるとする Tor のウェブサイトのアドレスが提供され、約 75 ビットコイン（BTC）の身代金が要求された事件である。

この事件に関しては、同社が、予備的措置でパイプラインを停止したこと、同社が、身代金を 5 月 8 日にしたこと、同日、公聴会で、侵害の経緯を説明していること、5 月 13 日に、DarkSide（ロシアに所在するグループである）が活動を停止したこと、6 月 8 日にＦＢＩが身代金として支払われたビットコインの一部を差し押さえたこと、などの事実がある。

英国

英国において、被害が多く、また、特徴的なものとして報道されている[10]事件としては、以下があげられる。NHS 事件（2017）は、WannaCry によって、NHS（国民保健サービス）の多数のコンピュータが停止を余儀なくされたという事件である[11]。Reckitt Benckiser 事件（2017）は、NotPetya によって、英国の製薬会社である Reckitt Benckiser が、薬品の製造とその配送に支障を来して多大な損害を被ったという事案である。Eurofins Scientific 事件（2019）は、上述の Ryuk によって科学捜査サービスプロバイダが、ランサムウェアに感染し、血液や DNA サンプルの分析に支障が生じたという事件である[12]。The Police Federation of England and Wales (PFEW)事件（2019）は、警察官の労働組合である PFEW が、ランサムウェアによってデータベースやシステムが影響を受けて、データにアクセスができなくなったという事案である[13]。

ドイツ

IT セキュリティ庁（BSI（Bundesamt für Sicherheit in der Informationstechnik））が発行している「Ransomware Bedrohungslage, Prävention & Reaktion 2019」(以下「Ransomware 2019」[14]という)において、ランサムウェアの用いる動機や被害状況及び、それの対策についての議論がなされている。

ランサムウェアの被害として、会社の営業が害されること等によるコストという意味での固有の損害、レピュテーション侵害、さらに契約の相手方等の第三者への損害の 3 つがあると整理される（Ransomware 2019、8 頁、以下同じ）。ランサムウェアを用いる攻撃者の動機は金銭的な利益、（政治的、経済目的）破壊的活動、憂さ晴らし等がある(同 10 頁)。

大企業の被害の実例としては 2019 年の Norsk Hydro 社の例がある。同社はランサムウェア LockerGoGa の被害者となった。同社は 35,000 人の従業員を抱えるアルミニウムの製造業を営む会社である。インシデントの際、同社の多くの IT システムがランサムウェアに感染した。同社は身代金を支払わず、既存のバックアップを使ったものの、ウェブサイトには

---

[10] 以下の事案は、“The top 5 ransomware attacks in the UK and their hidden costs on business”による（https://www.acronis.com/en-gb/articles/ransomware-attacks/）。

[11] 詳細な報道として BBC「英医療機関、ランサムウェアの被害拡大を懸念」（https://www.bbc.com/japanese/39918853）がある。

[12] “UK Law Enforcement Data Put at Risk in “Highly Sophisticated” Eurofins Scientific Attack”（ https://www.cbronline.com/news/eurofins-scientific-hacked）

[13] ” Brit Police Federation cops to ransomware attack on HQ systems” https://www.theregister.com/2019/03/21/police_federation_ransomware_attack/

[14] https://wod.wowow.co.jp/content/080281

一時的にアクセスができなくなり、4 週間にわたってマニュアルでの稼働を余儀なくされた。結局、最大 $ 43,000,000 の損害が出た（同 11－12 頁）。

日本

日本においては、2020 年 4-12 月において警察庁への相談が 23 件あったことが報道されている[15]。また、新聞報道された事件としては、カプコンの二重恐喝のランサムウェアの被害、ホンダの事案等がある。

2　各国におけるランサムウェアにおける脅迫金支払いの可否についての法的な助言・ガイドライン等の分析

2.1　米国

米国において公的な対応の努力、公的機関等から公表されているアドバイスとして、注目すべきものとしては、以下のものがある。

サイバーセキュリティ及びインフフラストラクチュアセキュリティ庁（CISA）

米国のサイバーセキュリティ及びインフフラストラクチュアセキュリティ庁（CISA）は、総合的なランサムウェア対応についての情報を整備している[16]。

そこでは、ランサムウェア対応の会議のビデオ（ウェビナー）、「CISA、MS-ISAC、NGA 及び NASCIO[17]によるランサムウェア攻撃からの保護のための即時行動の推奨事項」、CISA の分析などが紹介されている。そこで注目すべきものが、CISA と MS-ISAC による 2020 年 9 月の「共同ランサムウェアガイド」になる。このガイドは、パート 1　ベストプラクティスとパート 2　対応チョックリストからなる。パート 1 においては、準備すること、感染のベクターとして、脆弱性・誤った設定、フィッシング、感染の前兆、サードパーティやマネージドサービス提供者があげられている。パート 2 においては、探知の分析、封じ込みと消去、リカバリと事件後の活動、コンタクトリストがあげられている。

このガイドでは、ランサムウェアに対して支払う行為に対して「身代金を支払っても、データが復号化され、又はシステムやデータが危険にさらされることがなくなるわけではありません。CISA、MS-ISAC、及び連邦法執行機関は身代金の支払いを推奨していません。」というコメントがなされている。

FBI

米国連邦捜査局（FBI）は、ランサムウェアについての情報をまとめている[18]。そこでは、ランサムウェアとはどういうものか、また、ランサムウェアの被害にあわないための助言、

15　国家公安委員会委員長（代理）記者会見要旨（https://www.npsc.go.jp/pressconf_2021/03_04.htm）

16 https://www.cisa.gov/ransomware　なお、このサイトは、2021 年 1 月に整備されたものである（https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware）。

17 サイバーセキュリティ・インフラセキュリティ庁（CISA）、マルチステート情報共有・分析センター（MS-ISAC）、全米知事協会（NGA）、全米州最高情報責任者協会（NASCIO）になる。

18 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

また、IC3 の資料へのリンクが紹介されている。また、2016 年 4 月に既に、ランサムウェアの被害が増加傾向にあるとして、ニュースリリースで「FBI は、ランサムウェア攻撃に対して身代金を支払うことを支持していません。身代金を支払っても、組織がデータを取り戻せるという保証はありません。身代金を支払った後、組織が復号鍵を手に入れられなかったというケースを見たことがあります。身代金を支払うことは、現在のサイバー犯罪者がより多くの組織を標的にすることを助長するだけでなく、他の犯罪者がこの種の違法行為に関与する動機付けにもなります。そして最後に、身代金を支払うことで、組織は、犯罪者に関連した他の違法活動に不用意に資金を提供している可能性があります。」と伝えている[19]。

IC3

IC3 は、インターネット犯罪申立センター（Internet Crime Complaint Center）である。その使命は、インターネットを介した犯罪行為の疑いに関する情報を連邦捜査局に提出し、法執行機関や業界のパートナーとの効果的な協力関係を構築するために、信頼性の高い便利な報告メカニズムを一般の人々に提供することである。IC3 のサイトでは、ランサムウェアについて、「ランサムウェアの被害者は、感染を連邦法執行機関に届けること」（2016 年 9 月）[20]、「米国企業及び組織を脅かすインパクトの高いランサムウェア攻撃」（2019 年 10 月）[21]、「ランサムウェア　その実態と対応（What it is & What to Do About It）」（2021 年 1 月）[22]が公表されている。もっとも、これらのほとんどは、ランサムウェアとは何か、そのための防御のためのベストプラクティスを叙述するものであり、法的な関係についての分析はなされていない。

財務省による制裁[23]

米国財務省外国資産管理室（OFAC：Office of Foreign Assets Control）は、「ランサムウェアに対する支払いを促進することに対する制裁の可能性についての助言」（Advisory on

---

[19] ” Incidents of Ransomware on the Rise Protect Yourself and Your Organization”のニュースリリースによる https://cdpsdocs.state.co.us/safeschools/Resources/FBI/IncidentsofRansomwareontheRise.pdf 。（https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise）また、このことを報道するものとして、FBI announcement: paying the ransom is a bad idea（ https://blog.malwarebytes.com/security-world/2016/05/fbi-announcement-paying-the-ransom-is-a-bad-idea/ ）、High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations（https://www.ic3.gov/Media/Y2019/PSA191002）

[20] ”Ransomware Victims Urged to Report Infections to Federal Law Enforcement”（ https://www.ic3.gov/Media/Y2016/PSA160915）

[21] “High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations”（https://www.ic3.gov/Media/Y2019/PSA191002）

[22] https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

[23] 米国におけるマネーロンダリングへの対応の基礎的な知識としては、岡崎正江「米国内国歳入庁におけるマネーロンダリングへの取組」（税大ジャーナル　5　2007 年 6 月）（https://www.nta.go.jp/about/organization/ntc/kenkyu/backnumber/journal/05/pdf/07.pdf）がある。

Potential Sanctions Risks for Facilitating Ransomware Payments）を公表している[24]。

この助言においては、悪意あるサイバー攻撃者に対して種々の制裁プログラムを有しており、そのなかにランサムウェアの攻撃者とそれを促進したものに対しての制裁も含まれていることが明らかにされている。具体例として、2016 年にクリプトロッカーの被害に対してその開発者であるエフゲニー・ミカイロビッチを指名手配した。2018 年に SamSam ランサムウェアに関連して、そのサイバー攻撃に対して重要な支援をなしたとして 2 名のイラン人を指名手配し、ランサムウェアの資金を送り込んだ仮想通貨のアドレスを特定した。また、ラザルスグループ（WannaCry2.0）、イービルコープ（Dridex）への指名手配も紹介されている。

制裁で指定されている犯罪者・敵（adversaries）に対して、ランサムウェアの支払いを促進（Facilitating）することは、彼らの違法な目的を利得させ、進めることになる。それは、国家安全保障を脅かし、対外ポリシーに反する行為とされる。

国際緊急経済権限法（IEEPA）又は敵国との取引法（TWEA）[25]のもと、 米国人は、OFAC の特別指定国民・凍結者リスト（SDN リスト）、その他の凍結者、及び包括的な国や地域の禁輸措置の対象となっている者（キューバ、ウクライナのクリミア地域、イラン、北朝鮮、シリアなど）の個人又は事業体（以下「者」）との間で、直接又は間接的に取引に関与することが一般的に禁止されている。また、IEEPA に基づく違反を引き起こすあらゆる取引も禁止されている。OFAC は、厳格責任に基づいて制裁違反に対して民事罰を課すことがありうる[26]。これらの規定は、サイバー保険、デジタルフォレンジックス、インシデントレスポンスや金融サービスにかかわる者に適用されるのであり、その制裁規定に違反しないようにしなければならないとされる。また、FinCEN 規則にも準拠しなければならない。これらの違反については、事案ごとのアプローチにより、免許付与において考慮されることがありうる。また、ランサムウェアの被害者については、制裁関連者（sanctions nexus）を含みうると考えた場合には、直ちに OFAC に連絡することが推奨されている。また、攻撃が金融機関をも含む者である場合には、財務省サイバーセキュリティ重要インフラ防護局に連絡することが推奨されている。

FinCEN アドバイザリ

財務省の金融犯罪取締ネットワーク（Financial Crimes Enforcement Network、FinCEN）も、「ランサムウェア及び支払いを促進するための金融機関の利用についての助言」（Advisory

---

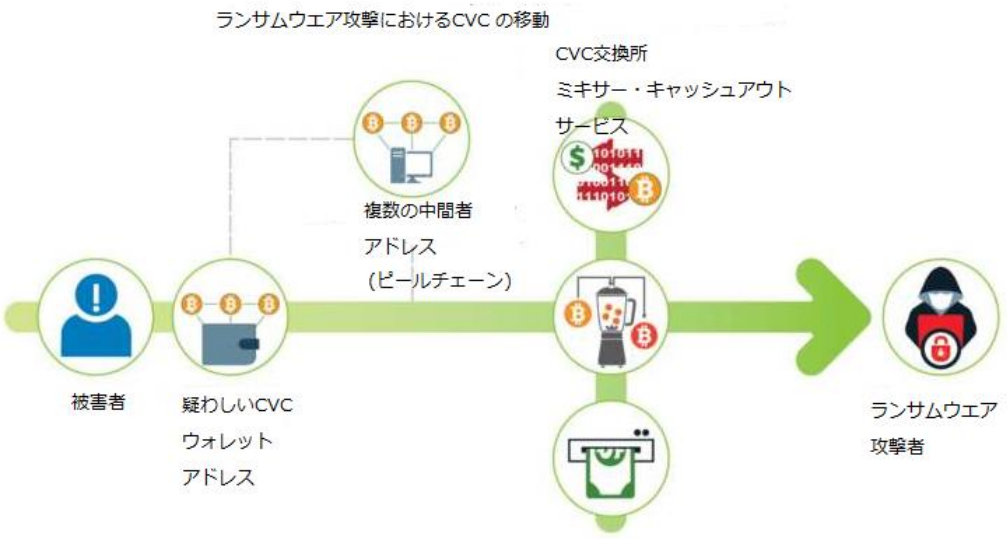
[24] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
なお、これを紹介する記事として、Alex Scroxton「ランサムウェアの身代金支払いを支援すると罰金＆制裁対象に」（コンピュータウイーク 2020 年 11 月 18 日号）がある。

[25] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06

[26] これらの制裁について考慮されるべき事項については、執行ガイドライン（31 CFR Appendix A to Part 501 - Economic Sanctions Enforcement Guidelines.－https://www.law.cornell.edu/cfr/text/31/appendix-A_to_part_501）がある。また、コンプライアンス・プログラムについては、OFAC がその枠組みについて公表している（「OFAC コンプライアンス・コミットメントの枠組み」参照（A Framework for OFAC Compliance Commitments）（https://www.piclub.or.jp/wp-content/uploads/2019/09/Framework-for-OFAC-Compliance-Commitments-1.pdf）。

on Ransomware and the Use of the Financial System to Facilitate Ransom Payments）を 2020 年 10 月に公表している[27]。この助言は、 (1)ランサムウェアの支払い処理における金融仲介機関の役割、(2)ランサムウェアと関連する支払いの傾向と類型、(3)ランサムウェア関連の金融レッドフラッグ指標、(4)ランサムウェア攻撃に関連する情報の報告と共有について論じている。

ランサムウェアの支払い処理における金融仲介機関の役割においては、いくつかのステップを踏んで、ランサムウェアの支払いがなされていることが説明されている。具体的には、その過程は、次の図で示される。



この図は、多くのランサムウェアのスキームは兌換可能な仮想通貨(convertible virtual currency－CVC)を含んでいることを示している。ランサムウェアの被害者は、通常、電信送金や自動化されたクリアリングハウス、クレジットカード決済で CVC 交換所への送金し、ランサムウェアの加害者が指定する CVC の種類と金額に従い購入する。次に、被害者は CVC を、一般には、交換所がホストしているウォレットから、加害者の指定口座又は CVC のアドレスに送金する。そして、ミキサーやタンブラーなど様々な手段を使って資金を洗浄し、他の CVC への交換や多くの口座や取引所をまたいだ取引がおこなわれ、海外拠点の取引所やアンチマネーロンダリングとテロ資金調達への対応（AML/CFT）の管理が弱い法域のピアツーピア（P2P）交換所へ資金が移動される。

このようなスキームに対して、デジタルフォレッジックス・インシデントレスポンス（DFIR）会社とサイバー保険会社（cyber insurance companies (CICs)）が、ランサムウェアの被害者に対して防護と緩和のサービスを提供している。それらの会社は、ときによっては、被害者からの資金を受領してランサムウェアの支払いを促進することもある。この場合、資

[27] https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

金移動となり、マネー・サービス・ビジネス（Money Service Businesses、MSB）と解される。MSB は、銀行秘密法（Bank Secrecy Act）における疑わしい取引報告の義務（suspicious activity reports、SARs）の義務が課されることになる。この点についての OFAC のガイダンスは、上述のとおりである。

ランサムウェアと関連する支払いの傾向と類型においては、烈度と狡猾さが増していることが論じられている。特に狡猾さについては、「ビッグゲーム・ハンティングスキーム」「犯罪者集団のパートナーシップ・リソース共有」「二重恐喝スキーム」「匿名性強化暗号通貨（Anonymity-Enhanced Cryptocurrencies (AECs)）」「ファイルなしのランサムウェア」について説明がなされている。

ランサムウェア関連の金融レッドフラッグ指標において、FinCEN は、金融機関がランサムウェア攻撃に関連した不審な取引を検出、防止、報告する際に役立つよう、ランサムウェア関連の不正行為を示す金融レッドフラッグ指標を特定していることを論じている。具体的には、サイバー指標、口座開設の際などに、支払いがランサム事件に関することを明らかにすること、顧客の兌換可能な仮想通貨口座がランサムの支払いと結びつくという分析と一致すること、ランサムウェアの標的になるハイリスクの企業とランサムウェアの支払いを促進する企業（例えばフォレンジックス企業）との間の取引であること、フォレンジックス企業等が顧客企業から、資金を受領し、受領後、同額を兌換可能な仮想通貨で送金していること、などがあげられている。

ランサムウェア攻撃に関連する情報の報告と共有については、上記の場合において、疑わしい取引（SAR）として報告義務があること、また、法の定めによりその情報共有によって民事損害賠償を問われることがないことが述べられている。

保険金の支払い関する議論

ランサムウェアの被害によって支払った身代金はサイバー保険の補償対象になるかどうかについては、世界的に争いが存する。これは、これを認めてしまうと誘拐リスクを助長する可能性があのではないか、ということを理由とする。

米国においては、G&G Oil Co. of Indiana, Inc. v. Contl. W. Ins. Co., 20S-PL-617, 2021 WL 1034982（Ind. Mar. 18, 2021） というインディアナ州最高裁判所の判決がある。この判決は、保険会社が、ランサムウェアによる身代金の支払いが、支払いのための契約の条件である「直接起因する」という条件に該当するのかというのが争われた事件で、裁判所は、「直接起因する」と解釈することかできるとして、上記の条件は、身代金の支払いの補償に及ぶとした。

2.2 英国

英国におけるランサムウェア対応についての政府関係のコメントはあまり多くはない。代表的なものは、以下のとおりである。

NCSC

英国の国家サイバーセキュリティセンター（NCSC）は、「マルウェアとランサムウェア攻撃を緩和する－マルウェアとランサムウェア攻撃から組織をどのようにして防御するか」（Mitigating malware and ransomware attacks－How to defend organisations against malware or ransomware attacks）というページでガイダンス[28]をまとめている。そこでは、マルウェアの概念、アクション１（バックアップ）、アクション２（マルウェアの拡散防止）、アクション３（マルウェアの実行防止）、アクション４（インシデントに備える）、既に感染してししまったら、追加のアドバイスの項目にわけて論じられている。このガイダンスの中で、「支払うべきでしょうか（Should I pay the ransom?）」というガイダンスがある。

そこでは、法執行機関は、身代金要求の支払いを奨励したり、支持したり、容認したりしないこと、身代金を支払ったとしてもデータやパソコンにアクセスできる保証はないこと、コンピュータはまだ感染しること、犯罪者集団に金を払うことになること、将来的には狙われやすいことがあげられている。また、攻撃者は、支払いが行われない場合にはデータを公開すると脅迫してくることがあるが、それに対しては、組織はデータ流出の影響を最小限に抑えるための対策を講じる必要があり、NCSC の「バルク個人データの保護に関するガイダンス」[29]と「ロギングと保護監視のガイダンス」[30]が役立つことが述べられている。

なお、英国においても、ランサムウェアの攻撃者からの要求に応じて、支払いをなすことは、資金洗浄及びテロリスト金融犯罪の対象となりうる。この点についての金融規制機関からの助言等[31]については、現時点においてはみつからない。

資金洗浄及びテロリスト金融犯罪について

そこで、資金洗浄及びテロリスト金融犯罪の対象となりうることについて[32]分析する。

英国においては、2002 年犯罪収益法（POCA; Proceeds of Crime Act 2002）[33]、2000 年テロリズム法（Terrorism Act 2000）、2017 年資金洗浄、テロリスト資金供与及び資金移転規則（Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer)

---

[28] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[29] https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data

[30] https://www.ncsc.gov.uk/collection/mobile-device-guidance/logging-and-protective-monitoring

[31] なお、英国財務省及び内務省「資金洗浄及びテロリスト資金供与についての国家リスク評価（National risk assessment of money laundering and terrorist financing 2020（https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf））においては、サイバー犯罪が、資金洗浄やテロリスト資金と関連の深いものであり、ランサムウェアもそのひとつであるという記述がある（3.22）。

[32] この点については、OUT-LAW NEWS “Cyber attacks: due diligence essential prior to paying ransoms”（https://www.pinsentmasons.com/out-law/news/cyber-attacks-due-diligence-essential-prior-to-paying-ransoms）、”Money Laundering and Terrorist Financing”（https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/Money-Laundering-and-Terrorist-Financing-2.pdf）など参照

[33] なお、分析については、坂東俊矢「英国における「行政による不法収益の剥奪、財産の隠匿・散逸防止制度、及び集団的消費者被害救済制度」の実際」（https://www.caa.go.jp/policies/policy/consumer_system/other/method_for_property_damege/report/pdf/1_UK.pdf）

Regulations 2017）が、上記の資金洗浄及びテロリスト金融犯罪についての対応策の枠組を定めている。2002 年犯罪収益法は、327 条以下で、犯罪収益の隠匿、転換、移転等を犯罪としている。また、テロリズム法は、資金獲得（同 15 条）、資産の使用もしくは保有（16 条）などを犯罪としている。したがって、ランサムウェアの支払いそれ自体は、違法とはいえないものの、相手先が、誰に、どのような状況で支払われたかによっては、マネーロンダリングやテロリストの資金調達犯罪が行われる可能性があり、具体的な事実については常に専門家のアドバイスを求めるべきであるとされる[34]。

2.3 ドイツ

ランサムウェア対策

ランサムウェア対策は、Ransomware 2019 において、予防、対応に分けて論じられる。予防においては、感染を予防する方策（迅速なソフトウェア・アップデート、攻撃範囲の最小化、スパムメールの取扱い、管理者アカウントの安全な取扱い、ウィルスの保護等）、バックアップ、従業員の意識改革、といった観点から論じられる。技術的な推奨事項だけでなく、従業員への啓蒙も重要だとされている。例えば、意識向上キャンペーンや従業員のトレーニングにおいては、悪意のあるプログラムの感染方法について、email の添付ファイルを誤って開くことによる侵入や、信頼されていない Web サイトへのアクセス（ドライブバイエクスプロイト）という 2 つの重大な感染方法が常に問題とされる。特に、被害者側の誤った行動は、ソーシャルエンジニアリングによる場合もある。私的な関係を装ったり、利益を約束したりするソーシャルエンジニアリングに対しては、レポートやニュースを盲目的に信頼しないということが何よりも重要である。どんなに魅力的であっても、当該ニュース等を信頼して、求めに応じてクリックなどしてはならない。例えば Ransamware 2019 では、怪しい事象に遭遇した場合には、クリックではなく、そこに書いてある連絡先に電話をしてみることを推奨している。

対応については、身代金の必要性、苦情（Anzeige）の申立て、インシデント対応、外部のエキスパートの支援があげられている（Ransamware 2019, 22 頁）。

BSI は、身代金の必要性に関し、予め準備をし、損害が発生したときにその準備を実行しつつ、支払をしてはならない、と強く述べる。恐喝の成功経験によって、攻撃者はさらなる恐喝について動機付けを得る。身代金はさらなるマルウェアの開発に利用され、その拡大を促進し、さらにその態様もより洗練されたものにしてしまう。そもそも、攻撃者が身代金を受け取ることで約束を守って暗号化を解除する保障はないし、現にそうした事例がある。

次に警察に被害届を出すことは重要である。警察は、例えば、身代金の流れを追う、C&C サーバを監視して情報を取得する等の、ランサム企業や CERT が遂行できない捜査をすることができる。結局のところ、ランサムウェアのビジネスモデルは、追跡のプレッシャーに

[34] 前記 OUT-LAW NEWS

よってのみ打ち破ることができ、こうして行為者は特定され、終局的に有罪の判決がなされることで、同人に他の犯罪の遂行をできなくさせることができる。連邦及び州警察は、苦情を受け付ける電話相談窓口をつくって、サイバー犯罪の被害者となった企業にアドバイスをし、苦情に基づいてサポートを行っている。

インシデント対応早期に感染したコンピュータのネットワーク接続（無線を含む）を切る必要がある。その上で、ログデータの助けを借りて、例えば、ネットワークドライブへのアクセスに基づいて影響を受けたコンピュータを特定していく。さらに暗号化されたファイルのメタデータ、例えば、どのユーザアカウントがそのファイルを作成したか、といったことも、感染したシステムについての一定の情報源となる。

フォレンジックを行うか否かは早期に決定しなければならない。一次キャッシュやハードディスクのバックアップを従業員により、影響を受けたシステムのさらなる修理や再起動が行われる前にしておくべきである。そうでないとフォレンジックが著しく困難になるか不可能になってしまうかもしれない。フォレンジックの経験がない場合には、エキスパートに相談すべきである。

データの再作成が行われる前に感染したシステムの再インストールが必要である。OS は、信頼できるデータ媒体から持ってくる必要がある。

いくつかの条件の下（ランサムウェアが Windows 内に暗号化しないで、又は消去しない形でコピーを保持している場合やランサムウェアの暗号化が不完全である場合、そしてフォレンジックによる復元が可能である等）で、バックアップによるデータの保護を用いずとも、部分的又は完全なデータの復元が可能である。しかし、大概は復元できると期待しない方が良い。結局、インシデント対応は、原状回復というよりは、損害を限定し、感染源を特定して、そこを塞いで再感染を防止し、システムを設定し直してデータを再作成するという方法を採ることになる。

なお、インシデントに対応できる独自の IT セキュリティチームや CERT 等をもたない企業が被害を受けた場合には、外部の有償サポートを受けることが推奨され得る。BSI は、そうしたサービスをリスト化して公表している。ランサムウェアの被害者は、アンチボットネットアドバイザリーセンターのエキスパートに質問して回答を得ることができる（同 22-23 頁）。

また、ドイツにおいては、身代金の支払いに対して、保険金の補償が許されるのかという論点に対して、許されるようになったという報道があります[35]。

---

[35] 損保総研レポート「ドイツ連邦金融監督庁（BaFin）がサイバー保険への身代金補償の組込みの認可を決定」（同レポートの 24 ページ）
https://www.sonposoken.or.jp/media/reports/sonposokenreport121_2.pdf

ランサムウェアに対抗する法的構成

上記のようなランサムウェアの頒布は、通例、恐喝未遂の構成要件（刑法 253 条 1 項、3 項）だけでなく、データ変更罪（刑法 303 条 a、「隠匿」（処分権者のアクセスを排除して利用できなくさせること（BT-Drs.10/5058, 34）の類型にあたるとされる(Tobias Singelnstein/Louisa Zech in Hornung/Schallbruch, IT-Sicherheitsrecht, Rn 66) ）、さらには、コンピュータ・サボタージュ罪（刑法 303 条 b）に該当し得、かつ特に刑法 303 条 b の罪については、2 項、そして組織的に行為が行われる場合には 4 項 2 号にも該当し得る(より重い犯罪となる、詳しく末尾の条文資料参照)とされる(Salomon、 Cybercrime und Lösegeld - Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575, 576)。

3　我が国への示唆について

支払いの可否について

我が国においては、経済産業省が、「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」を公表している(2020 年 12 月 18 日)[36]。この「注意喚起」は、1 趣旨、2 サイバー攻撃の事例、3 対応、4 セキュリティ対策やインシデント対応等に関する相談窓口からなりたっており、この注意喚起においては

金銭の支払いに関する問題である。データ公開の圧力から、攻撃者からの支払い要求に屈しているケースは少なくないとの報告は存在するが、こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。

とされている(7 ページ)。

なお、指示 7 においては、

犯行グループへの対峙。

*レ 一般論としては、ランサムウェア攻*撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。

とされている。

保険金の支払いについて

我が国では、ランサムウェアの被害によって支払った身代金はサイバー保険の補償対象

[36] https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf

にならないとされる[37]。同様の論点として「誘拐保険」というのがあって、我が国では、誘拐保険の取扱はありませんとされる[38]。これは、これを認めてしまうと誘拐リスクを助長する可能性があり公序良俗に反することが理由となる。

企業に対する示唆

ランサムウェアに対する支払いの法的な問題については、以上の調査の結果、資金洗浄やテロリストへの支払い対応という観点が重要なことが明らかになった[39]。また、コンプライアンス等の体制構築の問題も存在する。

これらの問題については、第２部である「脅威インテリジェンスサービスの利用における注意すべき法令上の問題についての調査」において検討するので詳細は、そこに譲る。

---

[37] 「サイバー保険に関する Q&A」https://www.sonpo.or.jp/cyber-hoken/about/

[38]「保険の玉手箱」 https://www.homemate-research-insurer.com/useful/18520_facil_041/

[39] また、ドイツ刑法 303 条 a, b は、我が国の私用電磁的記録毀棄罪等と異なり、その内容や価値を問わず、保存されたデータ全体を無権限の変更から保護する点で、無差別的なランサムウェアによる攻撃に対して使いやすい規定となっている。我が国は文書毀棄に対応する電磁的記録毀棄しか持たず、器物損壊罪に対するデータ損壊を持たないが、ドイツはそれを持っている点が重要な相違であり、我が国においても、ランサムウェアの使用それ自体を処罰する規定の整備も重要になってくるかもしれないという指摘もなされる。