サイバーセキュリティレポート

2022.04

NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部 OSINT モニタリングチーム

目次

【当レポートについて】

当レポートでは 2022 年 4 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『2021 年ランサムウェア活動を分析したレポート』

- 2021 年のセキュリティインシデントを分析した 2 つのレポートが米国で公開された。これらにおいて、最も焦点が当てられていたインシデントは、過去最悪の状況とされるランサムウェア被害であった。
- 身代金の平均支払い額は約 6,000 万円で、昨年から約 3,500 万円減少した。多くの企業はデータのバックアップに力を入れるなどランサムウェア対策をしており、交渉期間を長引かせるなどして身代金支払い額を減少させている。
- ランサムウェアグループは盗んだデータを公開するとして被害組織を脅迫したり、身代金受け取り後のデータ復元に力を入れたりする等、進化しており、2022 年もさらなる被害拡大が予想される。

第 2 章『PCI DSS v4.0、発行される』

- クレジットカード会員データを安全に取り扱うことを目的とした、厳格なセキュリティ対策フレームワークである PCI DSS の v4.0（バージョン 4.0）が発行された。9 年ぶりのメジャーバージョンアップである。
- オンラインスキミングやフィッシングなどの攻撃手法や、クラウド・ゼロトラストといったセキュリティ環境等の変化に対応するため、セキュリティ上重要なアカウントに多要素認証（MFA）を求める等のアップデートがされた。
- PCI DSS に準拠している組織は新バージョンへの計画的な移行が必要となるほか、個人情報保護等の厳格なセキュリティ対策にも PCI DSS は援用できるため、準拠していない組織においてもセキュリティ基準・規程類の最新化や整理に役立つと考えられる。

第 3 章『世界最大級のハッカーフォーラム「RaidForums」、欧米各国の協力により閉鎖』

- 4 月 12 日、ユーロポールは違法なデータの取引に利用されていた「RaidForums」を閉鎖したと発表した。
- RaidForums は世界中のハッカーの間で名を馳せており、過去には日系企業から漏洩したデータが投稿されたこともあった。
- 専門家によると、RaidForums を利用していたハッカー達は窃取した情報の別の販売方法を新たに探したり、他のサイトに移動したりしており、RaidForums の閉鎖がハッカー達の活動の長期的阻止につながる可能性は低い。彼らの動きには引き続き警戒が必要である。

1. 2021 年ランサムウェア活動を分析したレポート

1.1. 概要

今年 4 月、2021 年のセキュリティインシデントを分析した 2 つのレポートがアメリカで公開された。それらの中で最も焦点が当てられたインシデントは、過去最悪の状況とされるランサムウェア被害であった。本章ではこれらのランサムウェアに関する分析の中から特に注意を要する結果について紹介する。

1.2. 2022 Data Security Incident Response Report

2022 年 4 月 7 日、アメリカの弁護士事務所である BakerHostetler が「2022 Data Security Incident Response Report」を発表した[1]。これは、BakerHostetler が支援した 1,270 以上のセキュリティインシデントを分析した結果をまとめたレポートであり、産業別の傾向が見て取れる。

【ランサムウェア被害は増加】

BakerHostetler が支援したセキュリティインシデントのうちランサムウェア被害の割合は、2020 年の 27%から 2021 年は 37%に増加した。特に医療分野では、ランサムウェアが 35%を占めており、2020 年の 20%から大幅に増加した。

【身代金支払い額は減少し、交渉は長期化】

ランサムウェア被害のうち、身代金支払い額の平均は 511,957 ドル（約 6,000 万円）で、2020 年の平均額 794,620 ドル（約 9,500 万円）の約 2/3 であった。交渉期間の中央値は、2020 年の 5 日に対して 8 日だった。

交渉期間の延長は支払い額の減少に繋がっている可能性が高い。多くの組織がデータバックアップ機能の向上に投資しており、攻撃後に部分的に業務が継続できるようになっている。これにより交渉期間を引き延ばし、当初の要求額からより大きな減額を得ることができるようになった。

【産業別被害額】

2021 年は、エネルギー・テクノロジー、及びヘルスケアの 2 つの業界で身代金要求額と支払額の高さが目立った。

エネルギー・テクノロジー業界の組織に対する平均要求額は 9,553,333 ドル（約 11 億円）、ヘルスケア業界の組織に対しては 8,329,520 ドル（約 9 億 9 千万円）であった（表 1）。 ランサムウェアグループは標的とする組織の年間収益に基づいて身代金要求額を決定することが多いため[2]、企業規模が大きい業界に対する要求額が大きくなったと考えられる。

ただ、実際に組織が支払った金額は、エネルギー・テクノロジー業界が 3,000,000 ドル（約 3 億 5 千万円）、ヘルスケア業界は 875,784 ドル（約 1 億円）であり、要求額と支払額の差は大きかった。最初の要求額が高すぎて交渉決裂になったケースが多かった可能性がある。

---

[1] 出典：BakerHostetler『BakerHostetler Launches 2022 Data Security Incident Response Report - Resilience and Perseverance』
https://www.bakerlaw.com/BakerHostetler-Launches-2022-Data-Security-Incident-Response-Report-Resilience-and-Perseverance

[2] 出典 : Check Point Research『Behind the Curtains of the Ransomware Economy – The Victims and the Cyber criminals』
https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

産業	身代金要求額の平均	身代金支払い額の平均	許容できる復元までの日数
エネルギー・テクノロジー	$9,553,333 (中央値:$10,400,000)	$3,000,000 (中央値:$2,000,000)	4.6 日 (中央値:2 日)
ヘルスケア	$8,329,520 (中央値:$1,043,480)	$875,784 (中央値:$500,846)	6.1 日 (中央値:0 日)
金融サービス	$3,064,559 (中央値:$1,000,000)	$513,928 (中央値:$250,000)	12.8 日 (中央値:5 日)
小売、レストラン	$3,032,936 (中央値:$1,100,000)	$351,986 (中央値:$137,500)	7.8 日 (中央値:7 日)
製造業	$2,362,636 (中央値:$1,000,000)	$593,993 (中央値:$283,500)	10.2 日 (中央値:5 日)
教育	$1,588,468 (中央値:$558,000)	$196,071 (中央値:$154,000)	10.5 日 (中央値:8 日)
ビジネス・専門サービス	$1,383,704 (中央値:$409,800)	$342,370 (中央値:$120,892)	10.8 日 (中央値:7 日)
政府	$764,500 (中央値:$450,000)	$142,122 (中央値:$105,000)	11.5 日 (中央値:10 日)

表 1 産業別被害状況

【データ窃取による二重脅迫】

BakerHostetler が支援したランサムウェア被害企業のうち、24%の企業は自身でデータを完全に復元できたにも関わらず、身代金を支払った。これは、暗号化されたデータの復号と引き換えに身代金の支払いを要求するだけでなく、支払いを拒否すれば盗んだデータを公開するという二重脅迫を受けたために行った措置であった。

2021 年、ランサムウェア攻撃の 82%が二重脅迫であった。これは 2020 年の 70%から増加している。中でも医療機関へのランサムウェア攻撃のうち二重脅迫は全体の 89%を占めている（2020 年は 79%）。

二重脅迫のようなデータ窃取被害に備えるため、アメリカでは機密データは暗号化して保持し、ファイルサーバーへの個人情報または機密情報を含むドキュメントの保存を最小限にする等の対策が推奨されている。これは、行政への報告義務の発生や、訴訟につながる可能性がある個人情報または機密データの流出を回避するためである。

1.3. 2022 Cyberthreat Defense Report

アメリカのサイバーセキュリティリサーチコンサルティング会社である CyberEdge Group は「2022 Cyberthreat Defense

Report」を公開した[3]。これは、2021 年 11 月に、日本を含む 17 の国および 19 の業界について、従業員 500 人以上の企業の IT セキュリティ意思決定者および実務者 1,200 人からのメールでの回答をまとめたサイバーセキュリティレポートである。

【影響を受けた企業の割合】

ランサムウェアの影響を受けたと回答した企業の割合は 2018 年の 55.1%から 2022 年の 71%まで 4 年間で約 20%上昇した（図 1）。ランサムウェアに対し、企業の危機感が高まる背景が見て取れる。

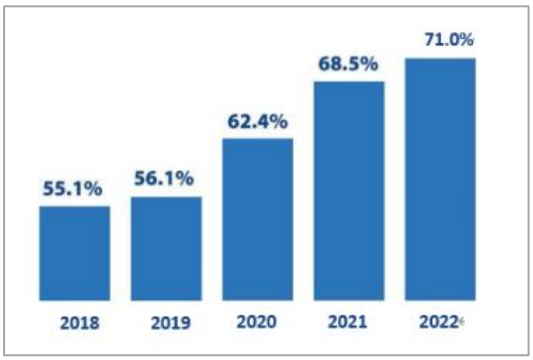

図 1 ランサムウェアの影響を受けた企業の割合

【身代金支払い後のデータ復元】

身代金支払い後にデータを復元できた企業は、2019 年の 61.2%から 2022 年の 72.2%まで年々増加している（図 2）。

現状、約 3 割は身代金を支払ってもデータを復元できない状況にあるが、ランサムウェアグループはこれを真剣に受け止めている。最も活発なロシア系ランサムウェアグループの一つである Conti は、身代金を支払ったにも関わらずデータを復元できなかった被害企業からの評判を気にしている[2]。悪い評判を聞いた他の被害企業が身代金を支払わない、もしくは身代金の交渉で大幅に減額を要求してくる可能性があるためである。したがって、身代金を支払った企業からデータを復元できなかったと連絡を受けた場合は、専門の技術スタッフが優先的に対応している[4]。

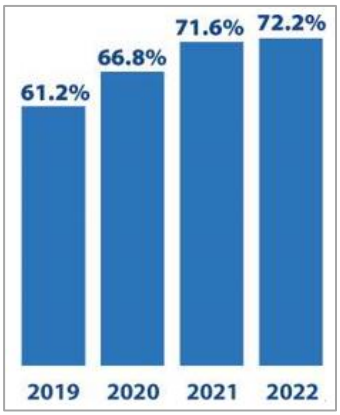

図 2 データを復元できた身代金支払い企業の割合

【身代金を支払った企業】

身代金を支払った企業の割合は 2019 年の 45.0%から 2022 年の 62.9%まで約 20%増加している(図 3)。

上述のように、ランサムウェアグループが被害企業のデータ復元の支援に力を入れることで、他の企業から身代金が支払われる可能性が高くなり、このことが攻撃を助長させることにつながっている。これを防ぐために、FBI はランサムウェアグループへ身代金を支払うことを非推奨としている[5]。

なお日本の警察庁は、ランサムウェア被害にあった場合、最寄りの警察署、各都道府県のサイバー犯罪窓口に通報することを呼び掛けてい

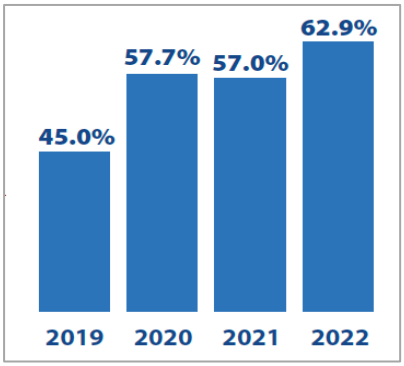

図 3 身代金を支払った企業の割合

[3] 出典 : CYBEREDGE『Cyberthreat Defense Report』 https://cyber-edge.com/cdr/

[4] 出典 : BreachQuest『The Conti Leaks | Insight into a Ransomware Unicorn』 https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/

[5] 出典 : FBI『Ransomware』 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

る[6]。

1.4. まとめ

これらのレポートによると、多くの企業はデータのバックアップに力を入れるなどランサムウェア対策をしており、攻撃が業務に影響を与えない場合は、交渉期間を長引かせるなどして身代金支払い額を減額させている。一方、ランサムウェアグループも身代金の要求において、被害組織の収益を調べ妥当と判断した金額を提示したり、身代金を受け取った後は被害組織のデータ復元支援に力を入れたりする等、まるでビジネスのように巧みな交渉やサポートを行っている。

活発に活動しているランサムウェアグループの拠点の多くがロシア語圏であるため、グループの摘発にはロシア政府の協力が必要となる。ただ 2022 年 2 月のウクライナ侵攻によるロシアと西側諸国との関係悪化によって、ロシア政府によるランサムウェアグループの摘発は期待できない。このことにより、2022 年はランサムウェア被害がさらに拡大することが予想される。

[6] 出典 ： 警察庁 サイバー犯罪対策プロジェクト 『ランサムウェア被害防止対策』
https://www.npa.go.jp/cyber/ransom/index.html

2. PCI DSS v4.0、発行される

2.1. 概要

2022 年 4 月 1 日、PCI セキュリティスタンダードカウンシル(以下「PCI SSC」)はセキュリティ対策フレームワークである PCI DSS v4.0（バージョン 4.0）を公開[7]した。

「PCI DSS」はクレジットカード会員データを安全に取り扱うことを目的とした、厳格なセキュリティ対策の基準である。これまで使われてきた PCI DSS v3.2.1 からは、2024 年 3 月 31 日までの切り替えが求められるため、PCI DSS に準拠している事業者は計画的な対応が必要となる。

図 4 PCI DSSv4.0 発行のお知らせ

2.2. PCI DSS とは

【世界基準の PCI DSS】[8]

PCI DSS(Payment Card Industry Data Security Standard) はクレジットカード業界のセキュリティ基準である。クレジットカード決済の加盟店やサービスプロバイダーにおける会員データの安全な取り扱いを目的として策定された。国際カードブランド 5 社(American Express、Discover、JCB、MasterCard、VISA)が共同で設立した PCI SSC (Payment Card Industry Security Standards Council)によって運用、管理されている。

日本では、日本クレジット協会の「クレジットカード・セキュリティガイドライン」[9]において、カード会社・決済代行業者等の PCI DSS への準拠を求めている。

【厳格なセキュリティ対策の基準】[10] [11]

PCI DSS は、サイバー攻撃等のシステムのリスクに対応するために講じるべき対策を、具体的な要求事項として提示している。また、事業者が保有する機密性の高いクレジットカード会員データの中でも、どの情報が特に重要であり、どのようなセキュリ

---

[7] 出典：共同通信 PR ワイヤー『ペイメントの未来を安全に： PCI SSC は PCI データセキュリティ規準 v4.0 を発行します | PCI セキュリティスタンダードカウンシルのプレスリリース』 ※時差により、書面上の発行日は米国時間 2022 年 3 月 31 日付となっている
https://kyodonewsprwire.jp/release/202204019492

[8] 出典：日本カード情報セキュリティ協議会『PCIDSS とは』
https://www.jcdsc.org/pci_dss.php

[9] 出典：一般社団法人日本クレジット協会『安全・安心なクレジットカード取引への取組』
https://www.j-credit.or.jp/security/document/index.html

[10] 出典：NTT データ先端技術株式会社『PCI DSS 徹底解説』
https://www.intellilink.co.jp/article/pcidss/pcidss.html

[11] 出典：NTT データ先端技術株式会社『PCI DSS の概要 －起源とその必要性－』
https://www.intellilink.co.jp/column/pcidss/2013/071700.aspx

ティ対策が実施されているべきかが、記載されている。

原則として PCI DSS は、要求される全ての事項をクリアしなければ取得できない厳格な基準である。単純に、対策済みであるかチェックリストをクリアすれば準拠できるわけではなく、脆弱性診断実施も組み込まれている。さらに、何か準拠に問題があった時には直ちに対策をとることが求められており、事業者にとって負担が大きいとされている。

2.3. PCI DSS v4.0 について

【時間がかかったバージョンアップ作業】

PCI DSS の前バージョンは V3.2.1 であった。2013 年公開の v3.0 以降 1～2 年ごとにマイナーバージョンアップを重ねることで最新化されていた PCI DSS であったが、2018 年に発行された v3.2.1 を最後にバージョンアップが 4 年間止まっていたため、陳腐化が懸念されていた。v4.0 は v3.0 系からのメジャーバージョンアップを意図しており、v3.0 公開から数えると約 9 年ぶりの刷新である。

v4.0 は当初は 2020 年発行予定だったが、メジャーバージョンアップにあたって、PCI SSC が最新のセキュリティを意識した基準に改訂するため意見募集を行ったところ、要望が殺到した。募集は 3 回行われ、最終的に 200 を超える組織から 6,000 を超えるフィードバックを受けた。反映に時間がかかり何度かの順延の末[12]、今回ようやく発行された。

【最新の状況に合わせたアップデート】[13] [14] [15]

12 の要件から成る等、基本的な構造は前バージョンから変更されていない。一方で採用するセキュリティ対策はオンラインスキミング・フィッシングなどの新しい攻撃手法や、クラウド・ゼロトラストへの対応を意識してアップデートされた。これにより、通信の暗号化の要求基準強化、Web サイトの全ての支払いページに対する悪性コード検知の実施、パスフレーズの長さを最小 7 文字から 12 文字に増やす等の新しい要件が盛り込まれた。

特に注目されているのが、以前から改善の要求が多かった認証分野について、NIST（米国標準技術研究所）のデジタル ID に関するガイダンス「800-63B」に準拠した点である。多要素認証を導入すべきという 800-63B のレベルに合わせ、セキュリティ上重要なアカウントである、クレジットカード会員データの管理権限アカウントすべてに対し多要素認証（MFA）を求める等、要求事項を最新の状況に合わせた。

他にも、審査員と被審査組織の間で見解に相違が出るといった問題に対応するため、用語の整理・現代化が行われた。例えば、侵入防御における「ファイアウォール」の語を、機器としてのファイアウォールに限定する等誤解があったため、「ネットワークセキュリティ制御」に置き換える等相違が出ない工夫が盛り込まれた。

また、PCI DSS はセキュリティ要件を厳密に満たすよう要求するため、対応に苦慮した組織が多かった。今回のアップデートで、組織側が自らのセキュリティ目標に基づいてセキュリティの実装手段を設計できる「カスタマイズバリデーション」や、ビジネスの

[12] 出典：ｆｊコンサルティング株式会社『PCI DSS v4.0 公開予定延期と追加 RFC の実施』
https://www.fjconsulting.jp/news/pci-dss-v4-update202103/

[13] 出典：ｆｊコンサルティング株式会社『PCI DSS v4.0 公開と移行のスケジュール』
https://www.fjconsulting.jp/news/pci-dss-v4-0-released/

[14] 出典：The State of Security『PCI DSS 4.0 and ISO 27001 – the dynamic duo』
https://www.tripwire.com/state-of-security/regulatory-compliance/pci-dss-4-0-iso-27001-dynamic-duo/

[15] 出典：TwoSense『BREAKING: What You Need to Know About PCI DSS 4.0』
https://www.twosense.ai/blog/pci-dss-4.0

必要性やリスクへの対応頻度を定義して、目標と対策実行の関係を整理した形で PCI DSS を実施できるようにする「ターゲットリスク分析」等、各組織に適した形で準拠するための手法を採用することにより、柔軟性が向上した。

【切り替え期間】

PCI DSS v4.0 の基準自体は発行されたが、審査等の体制がまだ整っていないのですぐに移行することはできない。PCI SSC は 6 月までを目標として、日本語を含む各国語への翻訳と、自己問診票（SAQ）等のサポート文書の公開を予定している。審査員へのトレーニングの提供開始がその後になることから、v4.0 での審査・準拠が可能となるのは最速でも 2022 年 6 月以降の予定となっている。

前バージョンの PCI DSS v3.2.1 からの移行の基準として、約 2 年間の切り替え期間が示されており、この期間での移行が推奨されている（図 5）。期限の 2024 年 3 月 31 日までは v3.2.1 と v4.0 のどちらでも準拠が有効と認められる。なお v4.0 の新要件の中には、2025 年 3 月まで準拠が猶予されているものもある。これは、技術的に移行が難しい・負担が重いといった場合を考慮して PCI SSC が「ベストプラクティス要件」と位置付けた緩和措置である。

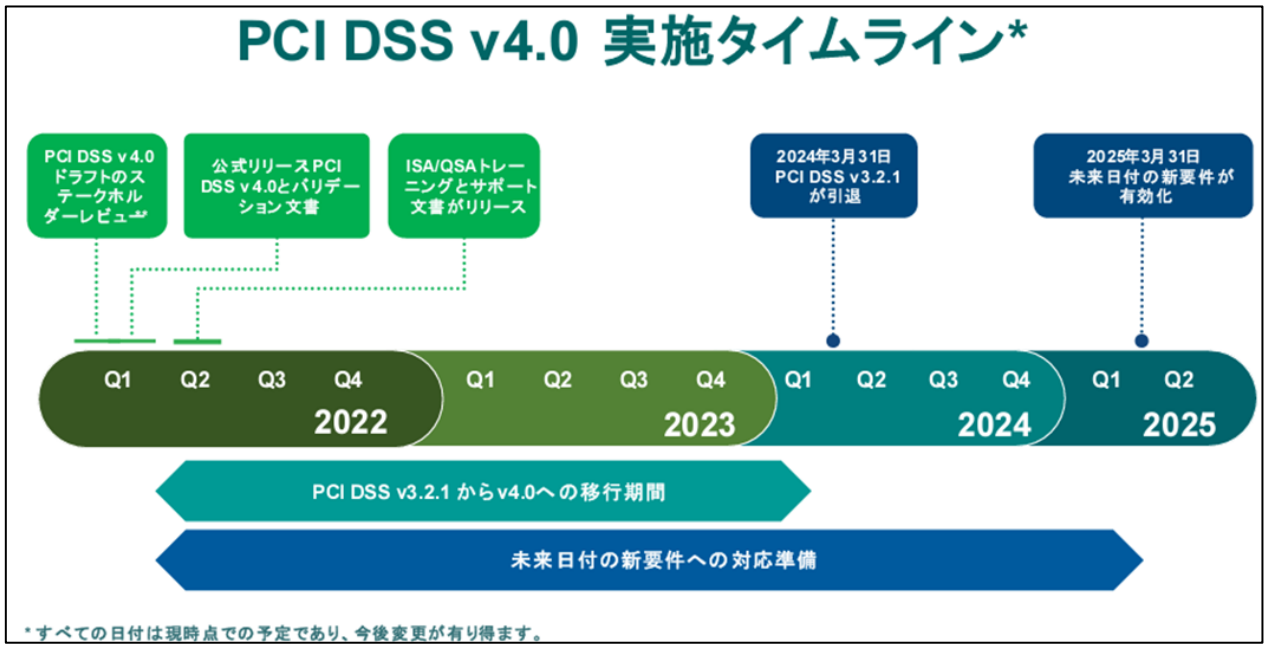

図 5 PCI DSS v4.0 への切り替えのタイムライン [16]

2.4. まとめ

PCI DSS v4.0 への切り替えが求められる 2024 年 3 月末まで、あと約 2 年である。PCI DSS に準拠している組織はその間、計画的に切り替えを進めていく必要がある。

また、これまで PCI DSS は他のセキュリティ基準・規程類の参考にされてきた。これは PCI DSS がクレジット決済を保護する強力なセキュリティの基準を具体的な条文にしており、個人情報保護等、他の強力な保護が必要な分野にも有用であるためである。さらに、1～2 年でアップデートされていた頃は最新のセキュリティに対応した基準と考えられていた。久々の PCI

[16] 出典：日本カード情報セキュリティ協議会『PCI DSS v4.0 へのカウントダウン』
https://www.jcdsc.org/news/pdf/2022/20220303_ssc-news.pdf

DSS の発行は準拠組織以外にとっても、多要素認証（MFA）を組織においてルール化する等の、セキュリティ基準・規程類の最新化や整理に役立つと考えられる。

3. 世界最大級のハッカーフォーラム「RaidForums」、欧米各国の協力により閉鎖

3.1. 概要

4 月 12 日、ユーロポール及び米司法省はそれぞれ、欧米の複数の法執行機関の協力により、ハッカー掲示板「RaidForums」のサイトを閉鎖したことを発表した[17]。

閉鎖にあたって RaidForums のドメイン等のインフラが押収されたほか、米司法省は、RaidForums の創設者であり管理者でもあるポルトガル国籍の「Diogo Santos Coelho（以下「コエーリョ容疑者」と表記）をイギリスで逮捕し、米国への身柄引き渡し手続き中であることを公表した[18]。

RaidForums は、サイバー攻撃で違法に窃取された漏洩情報のマーケットとしてハッカーの間で広く知られており、過去には日本を含む世界中の政府や企業、団体のデータや、そのシステムの脆弱性情報が販売されていた。

図 6 ユーロポールのツイート
『RaidForums を閉鎖した』[19]

図 7 現在の RaidForums サイト
「このサイトのドメインは押収された」と表示されている

3.2. RaidForums とは

RaidForums は、コエーリョ容疑者が 2015 年 1 月に開設したサイトである。 起訴状によるとコエーリョ容疑者は 2000 年 2 月生まれなので、開設当時は 14 歳だったことになる。コエーリョ容疑者は同フォーラム上で「Omnipotent(「オムニポテント」、全能者という意味)」と名乗っていた。

---

[17] 出典：EUROPOL『One of the world's biggest hacker forums taken down
https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

[18] 出典：United States Department of Justice『U.S. Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator』
https://www.justice.gov/usao-edva/pr/us-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator

[19] 出典：Twitter『@Europol』
https://twitter.com/Europol/status/1513865516154249217

図 8 コエーリョ容疑者の市民カード(起訴状の添付資料より)

米司法省によると、設立当初の RaidForums は、虚偽の通報でネットワークゲームの対戦相手の自宅等に警察特殊部隊(SWAT)を突入させる「スワッティング(Swatting)」など、電子ハラスメントについて情報交換を行う場として活用されていた。 その後、窃取された世界中の情報を販売するプラットフォームとしても利用されるようになり、窃取された情報へのアクセス権や様々な機能をユーザーが利用するのに必要なメンバーシップを販売していた。差し押さえられた時点で、同サイトでは、100 億レコード以上の窃取されたデータが販売されていた[20]。

過去には、米国の「T-mobile」や「Facebook」、日本の「株式会社コーエーテクモゲームス」の欧州関連会社をはじめとした様々な企業・団体から窃取されたデータや、その会社のシステムの持つ脆弱性が販売されていた[21]。

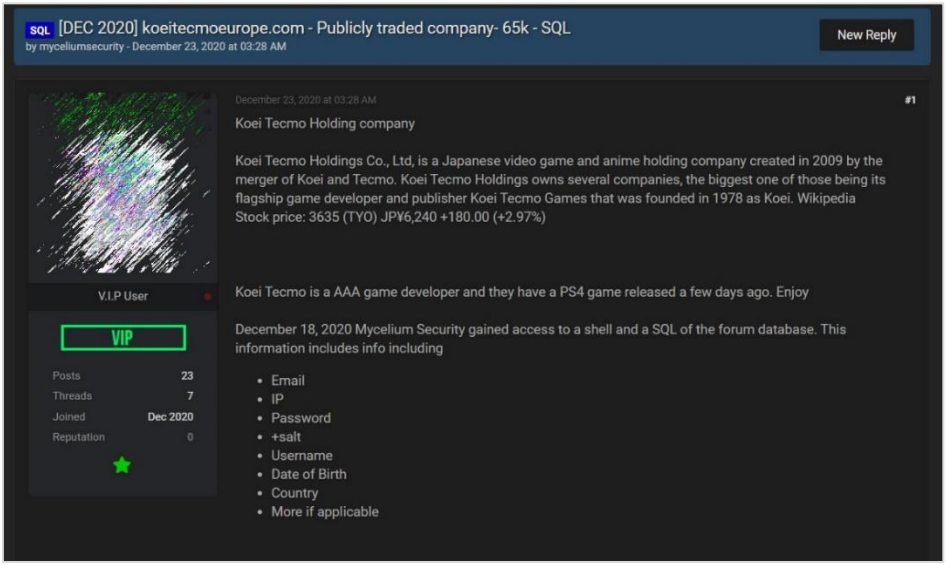

図 9 コーエーテクモゲームスに関する投稿

[20] 出典：ITmedia NEWS『世界最大級の闇取引市場、国際捜査で摘発 創設者とされる男は 21 歳 その正体は』 https://www.itmedia.co.jp/news/articles/2204/21/news062.html

[21] 出典：Bleeping Computer『Koei Tecmo discloses data breach after hacker leaks stolen data』 https://www.bleepingcomputer.com/news/security/koei-tecmo-discloses-data-breach-after-hacker-leaks-stolen-data/

3.3. コエーリョ容疑者逮捕の経緯

コエーリョ容疑者の逮捕のきっかけは、2018 年 6 月。アトランタにある国際空港から米国に入国しようとしたところ、米当局の捜査網にかかった[22]。

米当局は、彼が所持していたノートパソコンなどの電子機器を捜査する令状を取得し、捜査の結果、機器に保存されていたテキストメッセージ、ファイル、電子メール等から、この人物が RaidForums の管理者「Omnipotent」であることを確認した。

その後の詳細な経緯は不明だが、3 年半後の今年 1 月 31 日になって、彼は米国の要請を受けた英国の法執行機関により、現地で逮捕された。

コエーリョ容疑者は「陰謀」、「アクセスデバイス詐欺」、「個人情報の盗難」等、合計で 6 件において起訴されている。米司法省によるコエーリョ容疑者の宣誓供述書では、2021 年 8 月に RaidForums に投稿された T-mobile の漏洩情報販売について説明されており、この一件が逮捕に踏み切ったきっかけの一つだったと考えられる。

3.4. RaidForums 閉鎖と後継フォーラムの勃興

RaidForums は、コエーリョ容疑者の逮捕後間もない 2 月初めにはデータベースエラー画面が表示されたり、認証情報を入力後もログイン画面が繰り返し表示されたりするといった状態で、正常に利用できなくなっていた。

一部の専門家は、このころから捜査当局が同サイトを密かに乗っ取っており、ログイン画面が繰り返し表示されていたのも、アクセスしてきたハッカー達の認証情報を集めるために捜査当局がフィッシングをしかけたのではないかと推測している[23]。

図 10 繰り返し表示されたログイン画面(3 月 4 日時点)

また、そのころから RaidForums の後継を自称するサイトが複数乱立し始めた。どの新興フォーラムもあの手この手でユーザーを集めようとしており、例えば、何者かが開設した「RaidForums2」では、コエーリョ容疑者のアカウント名「Omnipotent」を

[22] 出典：Krebs on Security『RaidForums Gets Raided, Alleged Admin Arrested』
https://krebsonsecurity.com/2022/04/raidforums-get-raided-alleged-admin-arrested/

[23] 出典：Bleeping Computer『RaidForums hacking forum seized by police, owner arrested』
https://www.bleepingcomputer.com/news/security/raidforums-hacking-forum-seized-by-police-owner-arrested/

名乗るユーザーが、RaidForums2 を称賛する書き込みを行っている。(この書き込みがあった時点でコエーリョ容疑者は既に逮捕されているため、おそらく偽者によるものと考えられる)

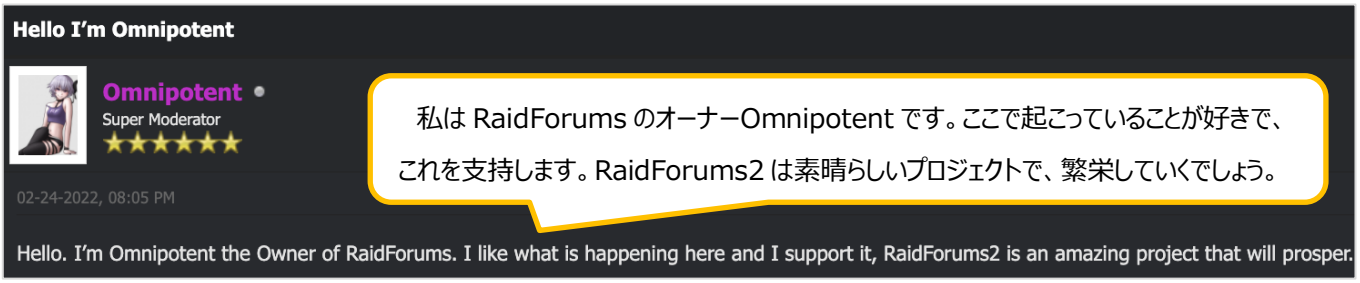

図 11 RaidForums2 に投稿された Omnipotent を名乗るユーザーの書き込み

一日当たりの投稿数や登録ユーザー数の観点から、新興フォーラムの中で最も多くのユーザーを獲得していると思われるのが、「Breached (別名 BreachForums)」である。このサイトは RaidForums で活動していたハッカー「pompompurin」が開設したもので、RaidForums の元ユーザーの移行を狙っているのか、サイトの見た目や機能を RaidForums によく似せて作っている。また、ユーロポールが RaidForums を閉鎖したことを知らせるツイートに返信する形で、pompompurin は「Breached では RaidForums の元ユーザーを優遇する」と宣伝のようなツイートも行っている（図 12）。実際、RaidForums で活動していたハッカーと同一人物と思われる者達が Breached に投稿を行っている。

図 12 ユーロポールへの返信ツイートで自分のサイトを宣伝

3.5. まとめ

世界中のハッカー達に利用され、多くの違法な取引の現場となった RaidForums は、オーナーが逮捕され、サイトが閉鎖されるという事態に至ったが、逮捕されたコエーリョ容疑者は開設当時わずか 14 歳の少年であった。こうした早熟な若者の才能を開花させるための環境が整っていないことも、犯罪に手を染める原因の一つと考えられる。

また、専門家によると、RaidForums を利用していたハッカー達は窃取した情報の別の販売方法を新たに探したり、他のサイトに移動したりしており、RaidForums の閉鎖がハッカー達の活動の長期的阻止につながる可能性は低いとしている[24]。窃

[24] 出典：Threatpost『Feds Shut Down RaidForums Hacking Marketplace』
https://threatpost.com/shut-down-raidforums-hacking-marketplace/179279/

取された情報の取引等、ハッカー達の活動には引き続き警戒が必要である。

以上

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム

メールアドレス： WA_Advisorysupport@ntt.com