サイバーセキュリティレポート

2025.06

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 6 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『AI エージェント時代の新たな脅威：Copilot ゼロクリック攻撃』

- 2025 年 Microsoft 365 Copilot(組織向け AI エージェント)において、AI エージェントに対してゼロクリック攻撃を可能にする初めての脆弱性「CVE-2025-32711」が公表された。
- この攻撃はターゲット側の人間の行動に依存せず、攻撃メール内に隠された悪意のある指示(プロンプト)によって AI エージェントを騙し、機密データを自動的に外部へ送信させる。これは、従来の「人間を騙す攻撃」から「AI を騙す攻撃」への根本的な転換を示している。
- AI エージェントの構造的な問題を悪用するため、従来のセキュリティ対策では防ぐことが難しい。

第 2 章『EU によるプライバシー重視の独自 DNS サービス』

- 2025 年 6 月、EU (欧州連合)は、米巨大 IT 企業が無料提供している「パブリック DNS」におけるプライバシー保護への懸念の高まりから、独自の DNS サービス「DNS4EU」の提供を開始した。
- DNS4EU は GDPR に準拠したプライバシー保護に加えて、悪意のある通信を DNS ブロッキングによって遮断することなどセキュリティ機能も実装されており、利用が広まるか注目される。
- 日本ではこれまで、通信の秘密に抵触する懸念から DNS ブロッキングに対して慎重な姿勢が取られてきたが、能動的サイバー防御法案が成立したことで、DNS4EU のような取り組みについて検討される可能性がある。

第 3 章『親台湾国家パラグアイの大規模漏洩事件』

- 2025 年 6 月 13 日、南米パラグアイの政府機関から漏洩した、全パラグアイ国民分に相当する 740 万件の個人データが暴露された。
- 被害の発端は、以前にマルウェアに感染していた政府職員の端末とみられており、その端末内から盗み出されたアカウントを入手した攻撃者が、パラグアイの政府機関のシステムに侵入してデータの窃取をしたとみられている。
- パラグアイは台湾と断交せず中国と距離を取る南米唯一の国である。以前にも、中国政府とのつながりが指摘されるサイバー攻撃グループによるパラグアイ政府ネットワークへの侵入が確認されており、本件を分析したセキュリティ会社が関連性を示唆している。

1. AI エージェント時代の新たな脅威：Copilot ゼロクリック攻撃

1.1. 概要

2025 年 6 月、Microsoft 365 Copilot(以下、Copilot)において、AI エージェントに対してゼロクリック攻撃を可能にする初めての脆弱性「CVE-2025-32711」が公表された[1]。EchoLeak(エコーリーク)と名付けられたこの脆弱性の発見により、Copilot 以外の AI エージェントにも同様の問題が存在する可能性が示唆されている[2]。EchoLeak は、従来のセキュリティ対策では防げない全く新しいタイプの攻撃を可能にし、AI 技術の急速な普及に伴うセキュリティリスクの深刻さを浮き彫りにした。

1.2. EchoLeak を利用したゼロクリック攻撃

【Copilot に存在する脆弱性 EchoLeak】

EchoLeak を利用したゼロクリック攻撃の大きな特徴は、攻撃メールに対するターゲット側の人間の直接的な行動(本文に記載されているリンクのクリックや添付ファイルの開封等)が不要なことである [1]。

従来の生成 AI が利用者の入力に対してテキストや画像の生成に留まっていたのに対し、Copilot のような「AI エージェント」は人間の代わりに自律的に外部システムにアクセスし、複数のアクションを連鎖的に実行することができる。

具体的には、組織向けの Copilot は Microsoft365 と統合されており、ユーザーの権限に応じて社内のメール、OneDrive ドキュメント、SharePoint ファイル、Teams の会話等にアクセスし、これらの情報を自然言語で検索・解析して、機密情報に関する質問に答える機能を持っている。これらの特性に含まれていた EchoLeak を悪用すると、攻撃者は標的企業の従業員にメールを送信した後、従業員によって機密情報に関する質問が Copilot に入力されるのを待つだけで、Copilot がアクセスできる機密データの漏洩を引き起こすことができる [1]。このように、従来の「ターゲットの行動に依存する攻撃」から「AI の仕組みを悪用する攻撃」への根本的な転換が実現された。

【EchoLeak を利用したゼロクリック攻撃の流れ】

まず、攻撃者が標的企業の従業員にメールを送信する。このメールには、従業員への通常の業務指示を装いながら、Copilot を騙すための悪意ある命令(プロンプト)が巧妙に埋め込まれている。受信されたメールは従業員の Microsoft365 環境内に保存される。その後、攻撃者は従業員が日常業務の中で、何らかの機密情報に関して Copilot に質問する機会を待つ。

従業員がいつものように Copilot に質問を入力すると、Copilot の検索処理により、攻撃者から受信していたメールも取得・処理される。その際、メール内に隠されていたプロンプトによって、Copilot が会社の機密情報を含む特殊な画像を作成する。この画像は Microsoft が設定しているセキュリティ機能を回避できる仕組みになっている。Copilot から従業員への応答

---

[1] 出典：Aim Security Blog『Breaking down 'EchoLeak', the First Zero-Click AI Vulnerability Enabling Data Exfiltration from Microsoft 365 Copilot』
https://www.aim.security/lp/aim-labs-echoleak-blogpost

[2] 出典：Dark Reading『Researchers Detail Zero-Click Copilot Exploit 'EchoLeak'』
https://www.darkreading.com/application-security/researchers-detail-zero-click-copilot-exploit-echoleak

には同画像が含まれており、ブラウザは自動的にそれを読み込もうとするが、この処理の際に、企業の機密データが外部にある攻撃者のサーバーに送信されてしまう。

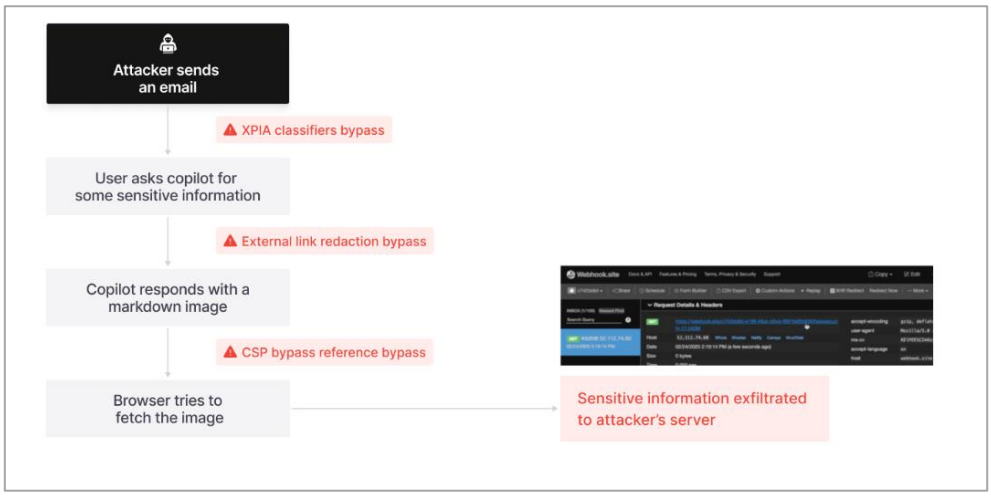

図 1 EchoLeak を利用したゼロクリック攻撃の流れ(Aim Security の発表より)[1]

【Microsoft の対応】

EchoLeak は米セキュリティ企業の Aim Security により 2025 年 1 月に発見され[3]、Microsoft に報告された。その後、Microsoft は同年 5 月に当脆弱性の影響を軽減させるための措置を完了し、6 月に詳細を公表するに至った[4]。脆弱性は CVE-2025-32711 として登録され、CVSS(共通脆弱性評価システム)9.3 という極めて高い深刻度を示して[5]いるが、実際に悪用された証拠はなく、影響を受けた Copilot ユーザーもいないと Microsoft は発表している [3]。また、上述のように当脆弱性への対処は完了しているため、ユーザーが対応する必要はない[6]。

しかし、Aim Security による報告から Microsoft による修正完了までの約 4 か月間、Copilot を利用するほとんどの組織が当脆弱性の攻撃リスクに晒されていた[7]。

1.3. 従来のサイバー攻撃との違い

これまでのメールを使ったサイバー攻撃の多くは、ターゲット側の人間の行動に依存していた。怪しいリンクをクリックさせる、添付ファイルを開かせる等、「人間を騙す」ことが多くの攻撃の前提であった。しかし、EchoLeak のような AI エージェントの構造的な脆弱性を利用した攻撃では、攻撃者は人間ではなく AI エージェントを騙すことを目的としている。そのため、標的企業の従業員が何も間違った行動をとらなくても、騙された AI エージェントが機密情報を外部に送信してしまう。従来、企業で行わ

[3] 出典：WINDOWS FORUM『EchoLeak: Microsoft's AI Vulnerability and the Future of Enterprise Security』 https://windowsforum.com/threads/echoleak-microsofts-ai-vulnerability-and-the-future-of-enterprise-security.370439/

[4] 出典：SiliconANGLE『Aim Security details first known AI zero-click exploit targeting Microsoft 365 Copilot』 https://siliconangle.com/2025/06/11/aim-security-details-first-known-ai-zero-click-exploit-targeting-microsoft-365-copilot/

[5] 出典：NIST『CVE-2025-32711 Detail』 https://nvd.nist.gov/vuln/detail/CVE-2025-32711

[6] 出典：Microsoft Security Response Center『M365 Copilot の情報漏えいの脆弱性』 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

[7] 出典：SparTech Software『Microsoft Copilot Zero-Click Vulnerability ("EchoLeak"): What Happened and Why It Matters』 https://www.spartechsoftware.com/cybersecurity-news/microsoft-copilot-zero-click-vulnerability-echoleak-what-happened-and-why-it-matters/

れていた、「不審なメールは開かない」「怪しいリンクはクリックしない」といった、従業員の行動に焦点を当てたセキュリティ教育では防げない脅威と言える。

1.4. 既存セキュリティ対策の限界

これまでのセキュリティ対策の多くは、「決まったパターンを見つけて防御する(パターンマッチング)」という手法であった。悪意のあるコードやウイルスファイルには何かしらの特徴があり、それを事前にウイルス対策ソフトのデータベースに登録しておけば自動的に検出できるという仕組みだ。しかし、EchoLeak を利用した攻撃で用いられたのは、普通のビジネスメールに見える内容の中に、攻撃者が AI エージェントに対する指示を巧妙に埋め込むという新しい手法である。従来のセキュリティシステムから見れば、それは単なる日常的なメールにしか見えない。しかし、そこに隠された意味を理解できる AI エージェントにとっては、明確な悪意のある指示となってしまう[8]。AI エージェント時代のセキュリティは「何が書かれているか」だけではなく、「AI がそれをどう解釈するか」まで考慮しなければならなくなった。

この課題を抱えているのは Microsoft 一社に限らない。Aim Security の共同設立者兼最高技術責任者の Adir Gruss 氏は、各 AI エージェントの実装詳細は異なるとしつつも、「他のプラットフォームでもすでに同様の脆弱性がいくつか発見されている」と述べている [2]。そのため、Copilot 以外の AI エージェントを導入・利用している企業や組織も、EchoLeak のような未知の脆弱性に晒されるリスクがあることを認識しておく必要がある。

1.5. まとめ

EchoLeak の発見は、AI エージェント時代における新たなセキュリティ脅威の到来を象徴している。この脅威を利用した攻撃は人間の行動に依存せず、AI エージェントの構造的な問題を悪用するため、従来のセキュリティ対策では防ぐことが難しい。AI 技術の普及に伴うセキュリティリスクは今後も拡大していくことが予想される。企業や組織は AI エージェントの導入・運用において、従来とは異なるリスクが存在する可能性があることを認識し、最新のセキュリティ動向を注視することが望ましい。

[8] 出典：Impart『Understanding EchoLeak: What This Vulnerability Teaches Us About Application Security』 https://www.impart.security/blog/understanding-echoleak-what-this-vulnerability-teaches-us-about-application-security

2. EU によるプライバシー重視の独自 DNS サービス

2.1. 概要

2025 年 6 月、欧州連合(以下、EU)は、独自の DNS(ドメインネームシステム)サービス「DNS4EU」の提供を開始した[9]。EU 圏内の市民および組織が同サービスを利用することにより、利用者のプライバシーの保護やセキュリティの強化が期待されている。本稿では、同サービスの導入に至った背景や特長についてまとめる。

2.2. DNS について

DNS は、人間が識別しやすい「ドメイン名」を、コンピューターが処理しやすい「IP アドレス」に「名前解決」するシステムで、今日のインターネットの根幹を支える重要なサービスである。

多くのユーザーは、インターネットサービスプロバイダー(ISP)によって回線利用者に提供されている DNS サービスの他、Google、Cloudflare などによってインターネット上で無料提供されている「パブリック DNS」を利用している。

2.3.「DNS4EU」

近年、EU は米巨大 IT 企業による市場寡占を警戒しており、様々な規制を行ってきた。2024 年 3 月にはデジタル市場法（Digital Markets Act [DMA]）が全面適用され、Google などの一定規模以上の企業を抑制し、公正な競争循環の実現に取り組んでいる[10]。

DNS においても、米巨大 IT 企業である Google や Cloudflare などが無料提供している「パブリック DNS」の利用が進んでおり、特にプライバシーの問題が懸念されている。DNS のトラフィックやログから「どのクライアントが、どのサーバーと通信しようとしたか」を収集することができ、個人のインターネット上の活動を特定される可能性があるためである。パブリック DNS のプライバシーポリシーによっては、収集したデータが広告や分析に利用・販売されたり、政府や法執行機関に提供されたりする場合もある。

こうした懸念の高まりから EU は、主に米国企業によって提供されてきたパブリック DNS の代替手段として、EU 域内で EU の法制度の下で保護されたパブリック DNS を提供するプロジェクトに取り組んできた[11]。プロジェクトは ENISA（欧州サイバーセキュリティ庁）などの支援を受けて進められており、結成したコンソーシアムには Whalebone 社など複数の欧州企業・研究機関が参加している。

---

[9] 出典：DNS4EU『DNS4EU Goes live: A European Alternative to Google and Cloudflare DNS, Powered by Whalebone』
https://www.joindns4.eu/learn/dns4eu-public-service-launched

[10] 出典：European Commission『The Digital Markets Act』
https://digital-markets-act.ec.europa.eu/index_en

[11] 出典：DNS4EU『About the project』
https://www.joindns4.eu/about

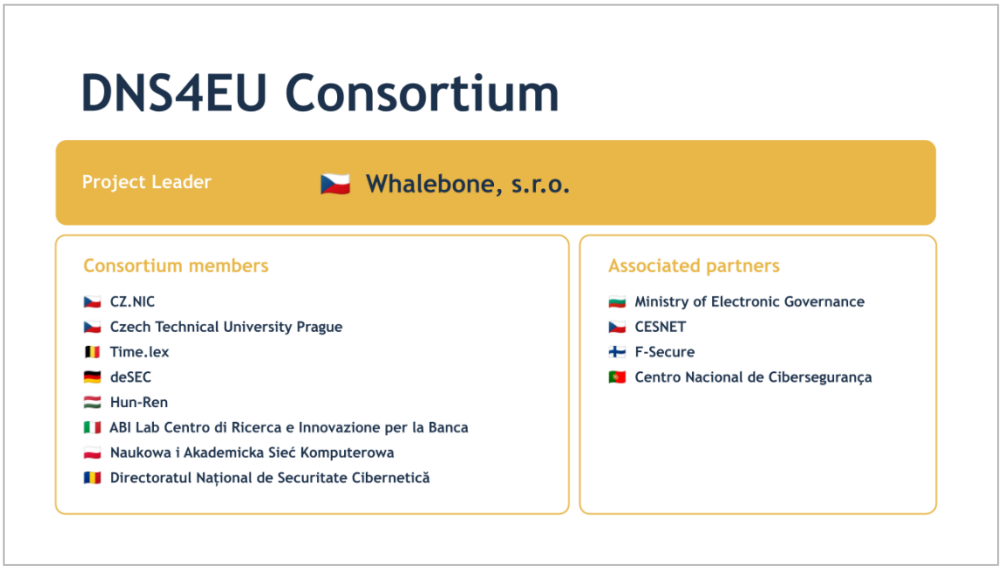

図 2 DNS4EU コンソーシアムの組織構成

同プロジェクトにより、6 月から DNS サービス「DNS4EU」の提供が開始された。EU 域内の市民による利用を想定した同サービスの他に、病院や学校などの公的機関および政府機関のために集中管理を可能にした「DNS4GOV (別名: DNS4EU for Governments)」、通信事業者のネットワークへの統合を実現する「Aura Infrastructure (別名: DNS4EU for Telcos)」なども提供される。

DNS4EU の主要な目的であるプライバシー保護の点では、利用者の IP アドレスを DNS サーバー上でログに保存する前に匿名化処理をしており、個人情報が収集されるリスクを低減している。また、DNS サーバーを EU 域内に分散配置し、名前解決などの DNS に関するデータを同域内で処理・保持することで、GDPR (EU 一般データ保護規則)に準拠している。

さらに、同サービスはセキュリティを売りにしており、DNS を介した通信を暗号化するためのプロトコル DoT (DNS over HTTPS)/ DoH (DNS over TLS)、DNS データの改ざんを検知できる拡張機能 DNSSEC をサポートしている。また、プロジェクトに関与している CERT、CSIRT、学術機関などの各組織が発見した脅威情報を共有し、これらをマルウェアやフィッシングなど悪意のある通信の遮断に反映させる仕組みが構築されている。悪意のある通信の遮断に加えて、児童保護、広告ブロック、遮断なしなど 5 つのオプションを提供しており、利用者側で選択することができる。

また、DNS サーバーを EU 域内に分散配置していることによって、Google や Cloudflare などのグローバルなパブリック DNS と比較して低遅延を実現しており、利用者が DNS4EU に乗り換えるメリットの一つとなっている。

こうした利点により広く利用されることが望まれる一方、同サービスに障害が発生した場合に影響が大きくなる懸念がある。また、同サービスは徹底したプライバシー保護を謳っているものの、一部からは監視や検閲につながるとの懸念の声も挙がっている[12]。

[12] 出典：Dropsafe『DNS4EU is surveilled』
https://alecmuffett.com/article/113493

2.4. DNS による悪意のある通信の遮断と検閲

DNS4EU で提供される悪意のある通信の遮断は、「DNS ブロッキング」や「DNS ファイアウォール」と呼ばれ[13]、DNS の基本的な仕組みを利用している。悪意のあるドメインの名前解決を DNS サーバーが拒否することで、不正な Web サイト、アダルトサイトへのアクセスやマルウェアなどとの通信を遮断するものである。

米 CISA (サイバーセキュリティ・インフラセキュリティ庁)の「Protective DNS」[14]や英 NCSC (国家サイバーセキュリティセンター)の「PDNS」[15]でも、公的機関向けの DNS サービスとして DNS ブロッキングが実装されている。

中国やロシアでは同じ仕組みを利用した検閲を行っており、国家にとって不利益な情報や国外のサービスへのアクセスを制限・遮断している[16, 17]。

一方、日本では、憲法第二十一条や電気通信事業法で定められた「通信の秘密」を侵害する可能性から[18]、DNS ブロッキングに対して慎重な姿勢が取られている。国内 ISP が提供する DNS において遮断できるという法的解釈が示されているのは、現時点では児童ポルノ関連のみとなっている[19]。ガイドラインでは、ISP 事業者の設備に支障が生じうる場合などの限られた状況下であれば、マルウェアの感染拡大や DDoS 攻撃などを意図した悪意ある通信を遮断してもよいとされているが、法的な効力はなく、事業者の判断に委ねられている[20]。

2.5. まとめ

DNS4EU は、EU 域内でのプライバシー保護とセキュリティを重視した DNS サービスとなっており、利用が広まるか注目される。

日本では「通信の秘密」に抵触する懸念から、国内の ISP 事業者が提供する DNS やパブリック DNS で悪意のある通信を遮断する仕組みは限定的にしか提供されてこなかった。しかし、2025 年 5 月に能動的サイバー防御法案が成立したこと

---

[13] 出典：Akamai『DNS ファイアウォールとは』
https://www.akamai.com/ja/glossary/what-is-a-dns-firewall

[14] 出典：CISA『Protective Domain Name System (DNS) Resolver』
https://www.cisa.gov/resources-tools/services/protective-domain-name-system-dns-resolver

[15] 出典：National Cyber Security Centre『Protective Domain Name Service (PDNS)』
https://www.ncsc.gov.uk/information/pdns

[16] 出典：Torfox『The Great Firewall of China: Background』
https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/category/great-firewall-of-china/index.html

[17] 出典：Internet Society『Mandating Certain Types of Connections Is Risky』
https://www.internetsociety.org/resources/internet-fragmentation/russias-national-dns/

[18] 出典：宍戸 常寿『DNS ブロッキングが形式的に通信の秘密を侵害し得る（電気通信事業法上の通信の秘密侵害罪の構成要件に該当する）とする政府研究会等の記載例』(首相官邸)
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai1/siryou7.pdf

[19] 出典：一般社団法人日本ネットワークインフォメーションセンター『DNS ブロッキング/フィルタリングの法的解釈と実施状況』
https://www.nic.ad.jp/ja/materials/iw/2024/proceedings/d2/d2-2-yamaguchi.pdf

[20] 出典：一般社団法人日本インターネットプロバイダー協会『電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン』
https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf

で、検知された攻撃兆候に関連する通信の遮断やアクセス制限が可能となるため[21]、DNS4EU のような取り組みについて検討される可能性がある。

[21] 出典：内閣官房『サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）』
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

3. 親台湾国家パラグアイの大規模漏洩事件

3.1. 概要

「Brigada Cyber PMC」と名乗る正体不明のハッカー集団が 2025 年 6 月 13 日を期限として、全パラグアイ国民分に相当する約 740 万件の個人データの暴露の停止と引き換えに合計 740 万ドルの身代金を要求した（図 3）。さらに、支払われない場合にはデータを公開すると脅迫し、期限後にデータが暴露された。

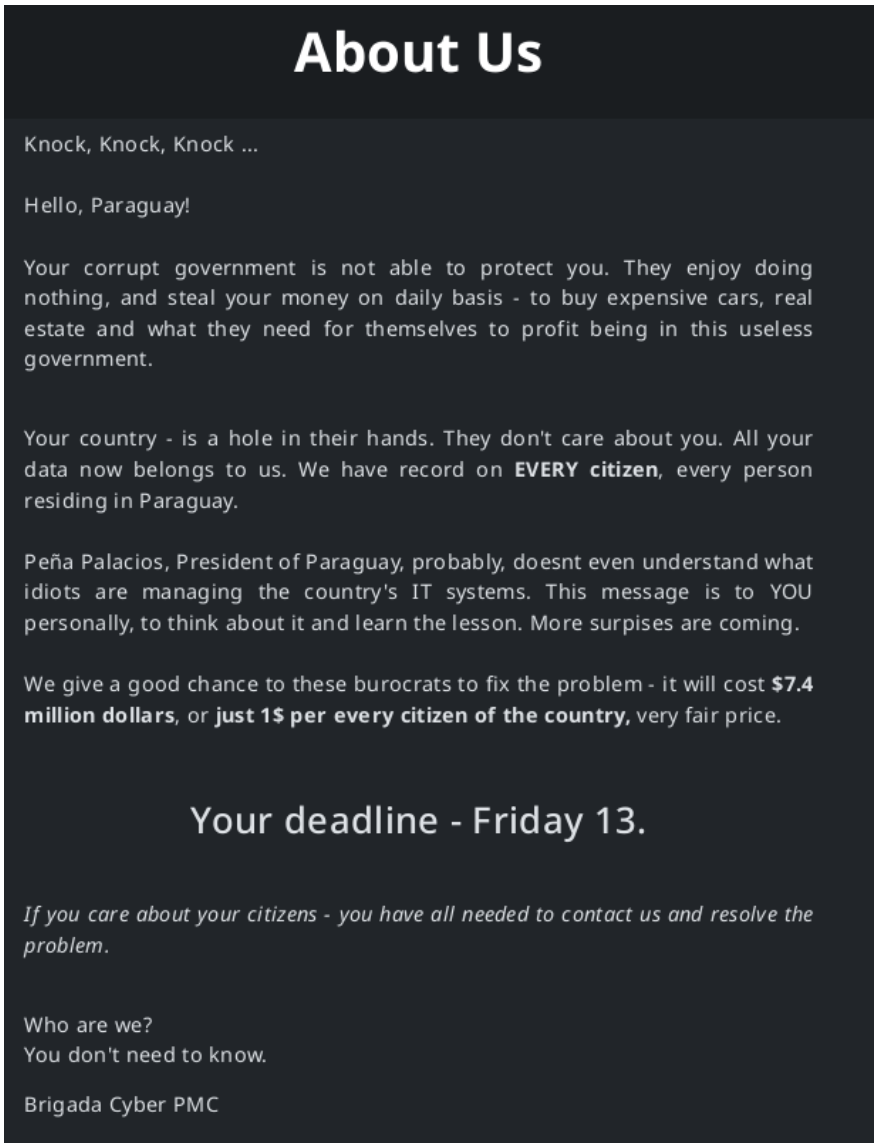

図 3　Brigada Cyber PMC のダークウェブサイトで掲載された脅迫文
(Resecurity のブログより)[22]

[22] 出典：Resecurity『Paraguay is Being Targeted by Cybercriminals - 7.4 Million Citizen Records for Sale』
https://www.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

3.2. パラグアイ共和国について

南米のパラグアイ共和国は、人口約 684 万人で農業が主産業の内陸国である（図 4）。他の南米諸国と同様、1989 年の軍事独裁政権の崩壊後に民政へと移行した。2010 年代中頃から中道右派の与党コロラド党が政権を執っている [23]。

近年、パラグアイの政府機関ではサイバー攻撃による情報漏洩が続いており、2025 年も複数の官庁で相次いだ他、大統領の SNS 公式アカウントの乗っ取り被害といったことも発生している[24]。

図 4　パラグアイ共和国の地理
（外務省ホームページより）[25]

3.3. Brigada Cyber PMC による個人データ漏洩と脅迫

【脅迫と暴露】

2025 年 5 月末頃、セキュリティ会社の Resecurity はダークウェブ上に、パラグアイ国民のほぼ全員に関する約 740 万件のデータを暴露すると脅迫するサイトを発見した。

サイトを設けていたのは、「Brigada Cyber PMC」と名乗るハッカー集団であった。Brigada Cyber PMC は和訳すると「サイバー民間軍事請負業者の旅団」となる。この名前から、同グループは民間軍事請負業者のように、依頼者から報酬を得て攻撃を行っている可能性が考えられる。ただ、同グループはこれまで活動が確認されておらず、「私たちは誰でしょう？(あなた方パラグアイ国民は)知る必要はありません。」と脅迫文に記すなど素性を明らかにしていない。

同グループは自身のサイトでパラグアイ首脳陣の腐敗と国民のデータ保護に関する配慮不足を非難しながら、パラグアイに住むすべての国民の記録を持っていると主張した。そして政府に対して、合計 740 万ドル(国民 1 人あたり 1 ドルとして)の身代金を要求し、さらに、支払われない場合には、データを公開すると脅迫した。政府は支払いを拒否。期限の 6 月 13 日になると、データは、同グループのサイトではなく複数の漏洩データのマーケットで暴露された(図 5)。

---

[23] 出典：外務省『パラグアイ共和国』
https://www.mofa.go.jp/mofaj/area/paraguay/index.html

[24] 出典：OCCRP『EXCLUSIVE: Paraguay Says It Won't Pay Ransomware Group For Stolen Citizenship Data』
https://www.occrp.org/en/news/exclusive-paraguay-says-it-wont-pay-ransomware-group-for-stolen-citizenship-data

[25] 出典：外務省『ODA メールマガジン第 301 号』
https://www.mofa.go.jp/mofaj/gaiko/oda/mail/bn_301.html

図 5　漏洩データのマーケットに書かれたデータ暴露の書き込み

【漏洩データ】

今回漏洩した約 740 万件のデータはパラグアイ政府の交通道路安全庁、公衆衛生社会福祉省などのシステムから流出したと推定されている。漏洩データには、氏名、ID 番号、生年月日、職業、資格、COVID-19 ワクチン接種履歴など、機微な性質を有する個人データが含まれていた。事実上全てのパラグアイ国民に影響のあるデータとみられており、漏洩データを悪用した金融詐欺、標的型フィッシング攻撃等によるパラグアイ国民の被害が懸念されている。

漏洩データは ZIP ファイル等によるアップロードだけではなく、P2P ネットワーク(中央サーバーを介さずに、ネットワーク上の端末[ピア] 同士が直接データを共有・処理する分散型ネットワーク)を通じて自由にダウンロードできる分散型ファイルシステムでも公開された。アップロードサイトを停止されても、P2P ネットワークでファイルが拡散され続けることを狙ったと考えられ、この暴露に当たって周到に準備している様が見て取れる。

【原因は窃取された政府職員の認証情報か】

調査から、インフォスティーラー(情報窃取型マルウェア)に感染したパラグアイ政府職員の端末から 2023 年 4 月に認証情報が窃取されていたことが判明した[26, 27]。Brigada Cyber PMC はこの認証情報を入手して不正アクセスに成功したと考えられている。

3.4. パラグアイを取り巻く情勢

【パラグアイの外交関係】

中南米諸国は「米国の裏庭」と呼ばれ、米国の政治的影響の強い国が多いことから、以前は台湾と国交のある国が複数あった。しかし昨今は経済力を背景とした中国の影響が強まり、台湾と断交する国が相次いでいる[28]。そのような中でパラグアイは米国寄りの姿勢を守って中国と距離を取り、南米で唯一台湾と親密な外交関係を維持している。中国との国交を主張し

[26] 出典：Resecurity『Paraguay is Being Targeted by Cybercriminals - 7.4 Million Citizen Records for Sale』
https://www.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

[27] 出典：InfoStealers by Hudson Rock『Paraguay's Biggest Data Breach: Infostealers Fuel Massive 7.4M Citizen Data Leak』
https://www.infostealers.com/article/paraguays-biggest-data-breach-infostealers-fuel-massive-7-4m-citizen-data-leak/

[28] 出典：ロイター『焦点：台湾外交「米国の裏庭」で劣勢、次はパラグアイか』
https://jp.reuters.com/article/world/-idUSKBN2W304Y/

た野党候補を破り 2023 年に当選した現職のペニャ大統領も、民主主義などの価値観を共有する米国、イスラエル、そして台湾との伝統的な友好関係を重視し関係強化を図っていく方針であり[29]、台湾との断交を迫る中国の圧力に屈しないと述べている[30]。

【中国政府関連のグループの攻撃を受けていたパラグアイ】

2024 年に、北米、ヨーロッパ、アフリカ、アジア全域、またパラグアイにおいて、Flax Typhoon によるコンピューターネットワークへの長期的な侵入・情報窃取の展開が米国当局により確認された[31, 32]。Flax Typhoon は中国政府とのつながりが指摘されるサイバー攻撃グループのひとつであり、特に台湾の政府や企業を標的に活動しているとみられている[33]。

3.5. まとめ

攻撃者はパラグアイ政府に身代金を要求していたが支払いを本当に期待していたようには見えず、金銭目的と考えるには疑いが残る。一方、脅迫文でパラグアイ首脳陣の腐敗について非難しており、現政権に対して悪意を持っていると考えられる。また、自らを民間軍事請負業者と位置付けているが、誰からの依頼を請け負ったのかは明らかにしていない。このような状況や南米唯一の親台湾国家であるパラグアイを取り巻く国際情勢から、調査した Resecurity が中国の関与を示唆していること[34]は興味深い。

以上

[29] 出典：NHK『中国より台湾？南米唯一の親台湾のパラグアイ いったいなぜ？』
https://www3.nhk.or.jp/news/special/international_news_navi/articles/qa/2023/07/06/32782.html

[30] 出典：朝日新聞『台湾を守ることが我々を守る」 パラグアイ大統領、関係維持を明言』
https://www.asahi.com/articles/AST5R0V46T5RUHBI037M.html

[31] 出典：U.S. Department of the Treasury『Treasury Sanctions Technology Company for Support to Malicious Cyber Group』
https://home.treasury.gov/news/press-releases/jy2769

[32] 出典：U.S. Embassy in Paraguay『Joint Statement by the U.S. Embassy in Paraguay and the Ministry of Information Technology and Communication of Paraguay』
https://py.usembassy.gov/joint-statement-by-the-u-s-embassy-in-paraguay-and-the-ministry-of-information-technology-and-communication-of-paraguay/

[33] 出典：Microsoft Security Blog『Flax Typhoon using legitimate software to quietly access Taiwanese organizations』
https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

[34] 出典：Resecurity『Paraguay is Being Targeted by Cybercriminals - 7.4 Million Citizen Records for Sale』
https://www.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

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

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt