サイバーセキュリティレポート
2026.08

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 2026 年 8 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『米政府、民間企業による対サイバー犯罪攻撃制度を創設へ』

- 2026 年 8 月 12 日、米政府は大統領覚書を発表し、政府の監督下で民間企業がサイバー犯罪組織に対する攻撃的サイバー作戦へ参加できる新たな制度の創設を指示した。
- 本制度により、民間企業の技術力や知見を活用した対処能力の向上が期待される一方、参加要件の負担や国際法上の責任の所在など、実務上の課題も指摘されている。
- 中国やロシアでは、企業やサイバー犯罪組織等の民間主体が国家のサイバー活動へ関係している事例が指摘されている中、米国は民間企業の関与を制度化し、法的根拠や監督体制の下で運用しようとしており、その動向が注目される。

第 2 章『ロシア系 APT による公共 Wi-Fi 悪用攻撃「CaptiveCrunch」』

- マイクロソフトは、ロシア系のサイバー攻撃グループ「Storm-2945」が展開する攻撃キャンペーン「CaptiveCrunch」について報告した。
- CaptiveCrunch は、ホテルや会議施設などの公共 Wi-Fi 環境の認証基盤(キャプティブポータル基盤)を悪用したサイバー諜報活動であり、認証情報の窃取やマルウェアの展開を伴う。
- 公共 Wi-Fi などの外部ネットワークを信頼せず、「既に侵害されている可能性がある」というゼロトラストの前提に立った対策が求められる。

第 3 章『中国系ルーターのバックドア事案が示した通信機器リスク』

- 2026 年 8 月、米国のセキュリティ企業 VulnCheck は、中国メーカーの Zbtlink(深圳市志博通電子)が製造した複数のルーターに、バックドア「ENDLESSDOORS」が出荷時から組み込まれているとする調査結果を公表した。
- 当該ルーターはバックドアを通じて、自発的に外部サーバーと通信を行っており、接続先サーバーから送信されたコマンドを root 権限で実行できる機能を有していた。
- 本事案は、通信機器のリスクが脆弱性への対応や悪用対策だけでは十分に捉えきれない可能性があることを示した。今後は製品の機能や価格だけでなく、供給元の信頼性や開発・保守体制も含めた評価が重要になる。

1. 米政府、民間企業による対サイバー犯罪攻撃制度を創設へ

1.1. 概要

2026 年 8 月 12 日、ホワイトハウスは大統領覚書を発表し、民間企業が政府の監督下でサイバー犯罪組織に対する攻撃的サイバー作戦を実施できる、新たな制度の創設を指示した[1]。本制度は、米政府が承認した民間企業に対し、サイバー技術を利用する国際犯罪組織(Cyber-Enabled Transnational Criminal Organizations、以下 **CE-TCO**)を対象としたサイバー監視活動や妨害活動への参加を認める。民間企業を政府主導の攻撃的サイバー作戦へ制度的に組み込む取り組みは珍しく[2]、今後の官民連携やサイバー対処能力の在り方という観点からも注目されている。

1.2. 制度の枠組みと創設の背景

【発出情報】

文書名	国家安全保障大統領覚書「国際的なサイバー技術利用型犯罪への対抗能力の強化(Expanding Capabilities to Combat Transnational Cyber-Enabled Crime)」
署名日／署名者	2026 年 8 月 12 日／ドナルド・トランプ大統領
土台となる大統領令	2026 年 3 月 6 日付大統領令 14390 号
運営主体	国家調整センター(National Coordination Center)

表 1 大統領覚書の概要

【創設の背景】

ランサムウェアやオンライン詐欺、フィッシング詐欺などを行う CE-TCO によるサイバー犯罪が、米国市民や企業および国家安全保障への脅威として拡大する中、民間セクターが有する技術力や革新性が「十分活用されてこなかった」との認識が、当制度の背景にある [1]。実際に、2025 年にはサイバー犯罪に起因する損失額として 208 億ドル超が米国の消費者らによって報告されており[3]、米政府は対策強化を急いできた。また、ランサムウェア被害については、FBI への報告件数だけでも 2023 年以降は 20%以上増加しているが、これらの事案は実際の被害総数の一部に過ぎないと指摘されている[4]。このことは、サイバー犯罪被害の全容把握や対処が容易ではないことを示している。

---

[1] 出典: The White House『Expanding Capabilities to Combat Transnational Cyber-Enabled Crime』
https://www.whitehouse.gov/presidential-actions/2026/08/expanding-capabilities-to-combat-transnational-cyber-enabled-crime/

[2] 出典: Wiley『Navigating the New Presidential Memorandum on Transnational Cyber Enabled-Crime』
https://www.wiley.law/alert-Navigating-the-New-Presidential-Memorandum-on-Transnational-Cyber-Enabled-Crime

[3] 出典: The White House『Fact Sheet: President Donald J. Trump Expands Capabilities to Combat Transnational Cyber-Enabled Crime』
https://www.whitehouse.gov/fact-sheets/2026/08/fact-sheet-president-donald-j-trump-expands-capabilities-to-combat-transnational-cyber-enabled-crime/

[4] 出典: Homeland Security Committee『Testimony of Cynthia Kaiser (Halcyon Ransomware Research Center)』(on a joint hearing "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans")
https://homeland.house.gov/wp-content/uploads/2026/04/2026-04-21-BSECIP-Hearing.pdf

こうした状況を受け、政府機関だけでなく民間企業の能力も活用した対処体制の必要性が高まっていた。2026 年 3 月には民間企業の活用方針を示す大統領令 14390 号が発出されており[5]、今回の覚書はその方針を具体化し、制度的枠組みを整備したものである[1]。

【制度の枠組みと監督体制】

今回の新たな制度に参加する企業は、情報収集を目的とする「サイバー監視作戦(Cyber Surveillance Operation)」と、システムやインフラの妨害や機能停止を目的とする「サイバー効果作戦(Cyber Effects Operation)」を実施できる[1]。対象となるのは CE-TCO であり、覚書はこれを、米国政府・米国人・米国の利益を標的とする外国の組織と定義している[1]。ただし、国家機関やそれらの関与が疑われる脅威アクター(国家の指示・支援を受ける APT グループ等)は本制度の対象には含まれない[1]。

制度は国家調整センターが運営し、司法省および国土安全保障省の監督の下で運用される[1]。また、本制度は無制限な攻撃権限を民間企業へ付与するものではない[1]。特に、人の死亡または重傷を招くおそれのある作戦や、国際法上の武力行使に相当し得る作戦については、厳しい制限が設けられている[1]。

参加企業には技術・安全要件が課されるほか、最低 100 万ドルの保証金の預託が求められる[1]。また、覚書は大企業に加えて「より小規模で機動的な企業」も参加できるよう、参加資格基準を定めることを関係当局に指示している[1]。

【今後のスケジュール】

覚書では、署名から 60 日以内に制度の運用手続きや参加要件等を整備することとしている[1]。今後は参加企業の選定基準や運用体制の詳細が明らかになる見込みであり、制度の具体的な運用方法が注目される。

1.3. 期待される効果と課題

【期待される効果】

本制度の導入により、政府機関だけでは対応が難しい多数のランサムウェアグループや詐欺組織に対し、民間企業の技術力や人的リソースを活用した対処範囲の拡大が期待される。特に、脅威アクターの追跡やインフラ分析に強みを持つ民間企業の知見を活用すれば、サイバー犯罪組織の活動基盤の特定やそれらに対する妨害措置をより迅速に実施できる可能性がある。

また、官民の情報共有が促進されることで、サイバー犯罪に関する脅威情報の収集・分析能力の向上が期待される。さらに、小規模で機動的な企業を含む多様な民間企業の参加により、新たな技術や知見の取り込みが進む可能性がある。

【想定される課題・論点】

本制度は、民間企業が独断で自由に反撃する、いわゆる「ハックバック」を認めるものではなく、実態としては政府主導の攻撃的サイバー作戦へ民間企業を組み込む仕組みに近い[2]。そのため、参加企業の裁量は限定的となる可能性がある。また、中小企業やスタートアップ企業の参加拡大が期待される一方、資金力や運用体制が限られる企業にとって、最低 100 万ドルの保証金制度や各種審査要件は大きな負担となり得る。そのため、どのような企業が実際に参画可能となるかは、今後公表される詳細な参加要件や運用方法に左右されるとみられる。その結果によっては、参加企業が一部の大手企業や既存の政府請負企業に偏る可能性もある。

---

[5] 出典: The White House『Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens』 https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/

さらに、民間企業が政府の管理下で攻撃的サイバー作戦に参加することから、国際法上の責任の所在や外交上の摩擦が生じるおそれがある。また、参加企業の関係者がサイバー作戦の対象国政府によって、起訴や拘束などの法的措置を受けるリスクも指摘されている[6]。

【中国・ロシアとの比較】

中国とロシアにおいても、企業やサイバー犯罪組織等の民間主体が国家のサイバー活動に関係しているとされる事例が報告されている。中国では、従来から民間の企業・請負業者が国家のサイバー作戦を支援しているとされ、米司法省は中国政府系のハッカー活動に関与した民間企業関係者に対して摘発や起訴を実施している[7, 8]。

ロシアでは APT グループ等の国家支援型サイバー活動が継続的に確認されているほか[9]、国家との関係が指摘されるサイバー犯罪組織の事例も報告されている。例えば、ランサムウェアグループ Evil Corp の指導者は、ロシア連邦保安庁(FSB)に機密情報を提供する見返りに活動上の便宜を得ていたとされる[10]。また、ランサムウェアグループ Conti についても、内部チャットの流出により FSB との関係が指摘されている[11]。さらに、Conti は明確な役割分担や階層構造を備えた企業に類似する組織として運営されていたと分析されている[12]。加えて、サイバー犯罪グループ FIN7 は、複数のフロント企業を運営し、サイバーセキュリティ企業を装ってセキュリティ人材の採用活動を行っていたことが確認されており[13, 14]、サイバー犯罪組織が企業を隠れ蓑にして活動する事例として知られている。

米国ではこれまで、攻撃的サイバー能力を提供する民間企業との契約や当該能力の調達において、高い信頼性や秘匿性が重視される傾向があることから、大手防衛請負企業が有利になりやすく、中小企業やスタートアップ企業が政府案件へ参入しにくい状況が続いていた[15, 16]。一方、中国では大手企業から中小企業までを含む民間企業がサイバー活動を支援する体

---

[6] 出典: TechCrunch『In a first, US will allow some private firms to carry out cyberattacks』 https://techcrunch.com/2026/08/13/in-a-first-us-will-allow-some-private-firms-to-carry-out-cyberattacks/

[7] 出典: U.S. Department of Justice『Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure』 https://www.justice.gov/opa/pr/justice-department-and-fbi-seize-platforms-operated-and-used-china-state-sponsored-hackers

[8] 出典: CISA『China Threat Overview and Advisories』 https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

[9] 出典: CISA『Russia Threat Overview and Advisories』 https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

[10] 出典: The Record『Eduard Benderskiy: Western authorities link Russian intelligence officer to Evil Corp cybercrime empire』 https://therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence

[11] 出典: ProPublica『Why It's Hard to Sanction Ransomware Groups』 https://www.propublica.org/article/ransomware-russia-ukraine-sanctions-ofac-conti

[12] 出典: CrimRxiv『Inside the Leak: Exploring the Structure of the Conti Ransomware Group』 https://www.crimrxiv.com/pub/i6n43dnf/release/1

[13] 出典: U.S. Department of Justice『Three Members of Notorious International Cybercrime Group "Fin7" in Custody for Role in Attacking Over 100 U.S. Companies』 https://www.justice.gov/usao-wdwa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over

[14] 出典: The Record『FIN7 hacker trialed in Russia gets no prison time』 https://therecord.media/fin7-hacker-trialed-in-russia-gets-no-prison-time

[15] 出典: CSIS『The Presidential Memo on Combating Transnational Cybercrime: Implications for Industry and Government』 https://www.csis.org/analysis/presidential-memo-combating-transnational-cybercrime-implications-industry-and-government

[16] 出典: Atlantic Council『Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace』 https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

制が構築されており、攻撃的サイバー能力や技術の提供だけでなく、実際のサイバー作戦の実施にも民間企業が関与しているとされる [16]。こうした差が、中国と比較した際の米国の機動性や戦略的優位性の低下につながっている見方も示されている[16]。前述の「大企業に加えて小規模で機動的な企業も参加可能とする基準」は、こうした従来の構造的な課題を是正し、民間企業活用の裾野を広げ、多様な企業の能力を取り込む狙いがあるとみられる。

1.4. まとめ

本制度は、民間企業が持つ高度な技術力や、サイバー脅威に関する知見を活用し、CE-TCO への対処能力向上を目指す新たな官民連携モデルである。一方で、制度は現時点で「創設の指示」段階にあり、具体的な運用手続きや参加企業等の公表はこれからである。中国やロシアにおいて民間主体が国家のサイバー活動に関係していると指摘される中、米国は民間企業の関与を制度的に位置付け、法的根拠や監督体制の明確化を図っている。日本においても、能動的サイバー防御関連法では能動的サイバー防御措置の実施主体を政府に限定していることから[17]、米国での制度運用の結果は、官民の役割分担を巡る議論において参考事例となる可能性がある。

[17] 出典：内閣官房国家サイバー統括室『サイバー対処能力強化法及び同整備法について』(内閣府)
https://www.cao.go.jp/cybersecurity/pdf/setsumei.pdf

2. ロシア系 APT による公共 Wi-Fi 悪用攻撃「CaptiveCrunch」

2.1. 概要

マイクロソフトは、ロシア系のサイバー攻撃グループ「Storm-2945」が展開する攻撃キャンペーン「CaptiveCrunch」(キャプティブクランチ)について報告した。CaptiveCrunch は、ホテルや会議施設などの公共 Wi-Fi 環境の認証基盤(キャプティブポータル基盤)を悪用したサイバー諜報活動であり、認証情報の窃取やマルウェアの展開を伴う[18]。

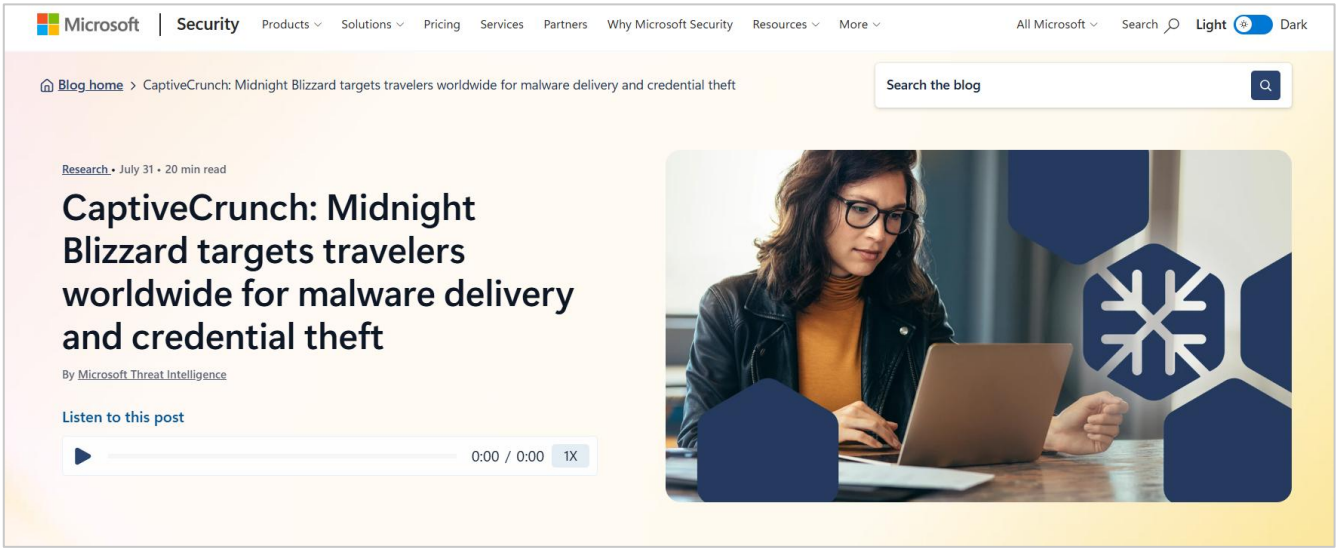

図 1 Microsoft の CaptiveCrunch のレポート [18]

2.2. CaptiveCrunch について

CaptiveCrunch は、2026 年 5 月頃から確認されている。攻撃者は、キャプティブポータル基盤にアクセスする利用者から Microsoft 365 の認証情報や認証トークンを窃取したり、クラウド環境への不正アクセス、マルウェアを展開したりするなどして、機密情報の収集や継続的な監視に利用できるアクセス基盤を確保する。政府・外交・防衛分野の関係者や、機密情報にアクセス可能な企業幹部、ならびに出張や国際会議などで公共 Wi-Fi に接続する機会が多い利用者が標的と考えられている[18]。

[18] 出典：Microsoft『CaptiveCrunch: Midnight Blizzard targets travelers worldwide for malware delivery and credential theft』
https://www.microsoft.com/en-us/security/blog/2026/07/31/captivecrunch-midnight-blizzard-targets-travelers-worldwide-for-malware-delivery-and-credential-theft/

【攻撃手法】[18]

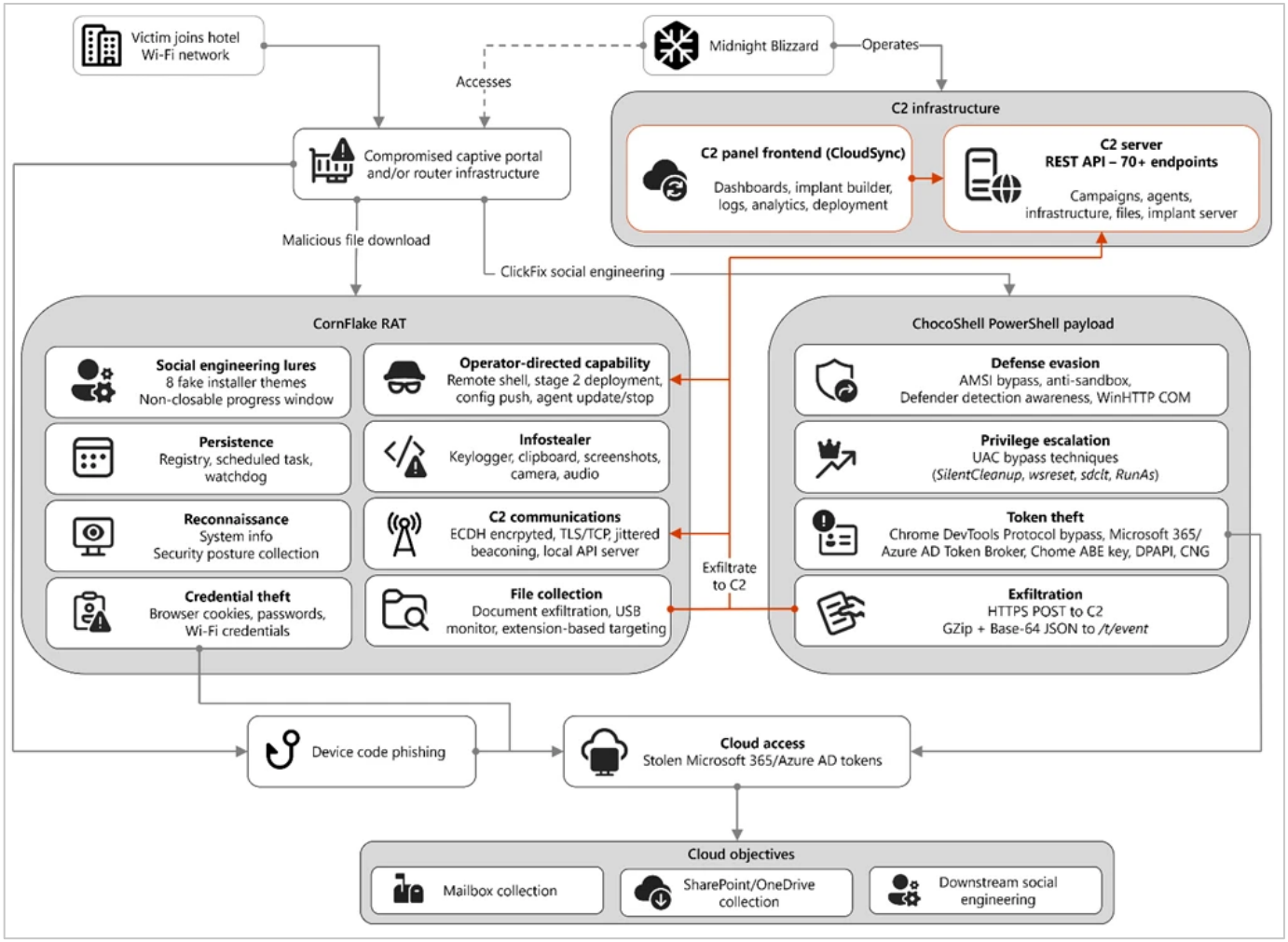

図 2 CaptiveCrunch の攻撃フロー(Microsoft のレポートより)[18]

攻撃は主に以下のような手順で実行される：

① ホテル等の施設が提供する公共 Wi-Fi のキャプティブポータル基盤を侵害する。これにより、当該 Wi-Fi に接続した利用者の通信を操作できる状態となる。

② 侵害したキャプティブポータル基盤を用いて DNS 応答や HTTP 通信を改ざんし、利用者を攻撃者が管理する Web サイトへ誘導する。

③ 誘導先のサイトでは以下のような攻撃が実行される：

◎認証情報窃取

Microsoft 365 などの正規サービスを装った偽ログインサイトが表示される。利用者が認証情報を入力すると、それらの情報や有効な認証トークンが窃取され、不正アクセスに利用される。

◎マルウェア感染

Windows や Web ブラウザのアップデート、セキュリティチェック、ネットワーク接続の修復等を装った偽サイトが表示される。利用者がファイルをダウンロードしたりコマンドを実行したりすると端末がマルウェアに感染し、攻撃者によるファイル窃取やリモート制御等が可能となる。

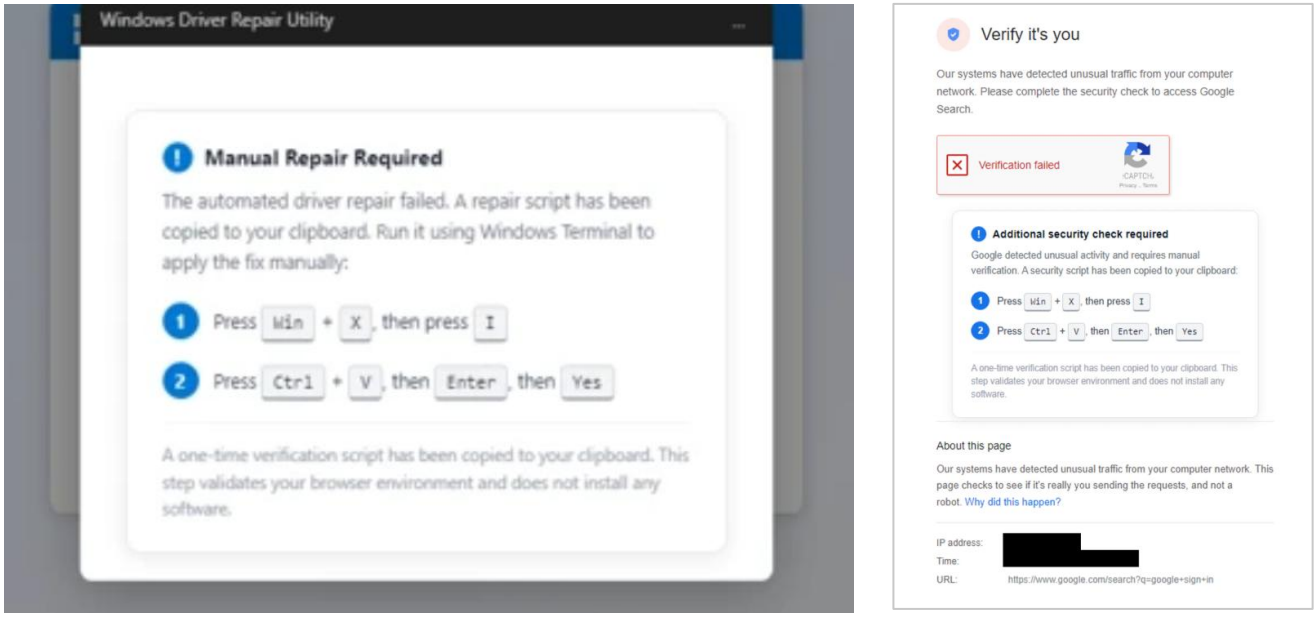

図 3 マルウェアを実行するため当該 Wi-Fi の利用者に操作を促す画面 [18]

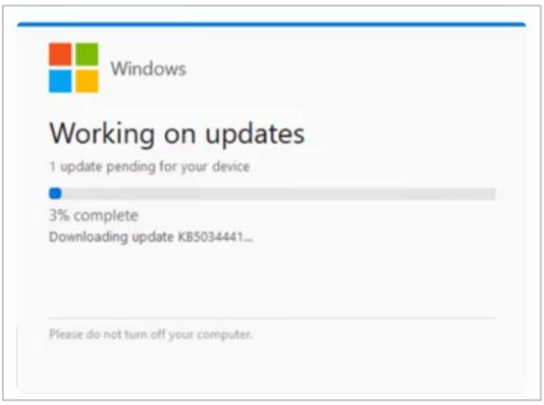

図 4 偽の Windows アップデート画面 [18]

2.3. 攻撃者について

CaptiveCrunch を展開している「Storm-2945」は、ロシア対外情報庁(SVR)との関係が指摘されるサイバー諜報組織「Midnight Blizzard (APT29、Cozy Bear)」の下位グループとされる。Midnight Blizzard の主な活動目的は、ロシア政府の安全保障上の利益に資する外交・軍事・政治・技術分野の情報収集であり、CaptiveCrunch もそのような活動の一環とみられている [18]。

Midnight Blizzard による攻撃事例としては、ネットワーク管理ソフトウェア「SolarWinds Orion」の正規アップデートにバックドアを混入したサプライチェーン攻撃[19]や Microsoft 幹部らを標的としたアカウント侵害[20]等が挙げられる。

[19] 出典：Zscaler『SolarWinds サイバー攻撃とは』
https://www.zscaler.com/jp/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack

[20] 出典：Reuters『Microsoft says Russian state-sponsored hackers spied on its executives』
https://www.reuters.com/technology/cybersecurity/microsoft-says-it-was-hacked-by-russian-state-sponsored-group-2024-01-19/

2.4. 類似事例「ダークホテル」

CaptiveCrunch は新たな脅威として注目されているが、ホテル利用者を狙ったサイバー諜報活動は目新しいものではない。2014 年には、「ダークホテル」(Darkhotel)と呼ばれる攻撃が報告されている。攻撃者は高級ホテルのネットワークを侵害し、政府高官や企業幹部など、自身が選別した標的に対して偽のソフトウェア更新画面を表示させ、マルウェアに感染させることで情報窃取を行っていた。なお、一部の調査機関は攻撃者と韓国との関連性を指摘しているものの、国家レベルでの帰属については明確になっていない。

ダークホテルが特定の少数の人物を標的としていたのに対し、CaptiveCrunch は侵害した Wi-Fi 環境の利用者を広範囲に狙う点に特徴がある。このように両者には標的や攻撃手法において違いが見られるものの、いずれもホテルの Wi-Fi 環境を攻撃の足掛かりとし、その利用者の信頼に付け込む点で共通している[21]。

2.5. 推奨対策

CaptiveCrunch への対策として最も確実なのは、公共 Wi-Fi の利用を避けることである。しかし、出張や外出先での業務により利用が避けられない場合は、通信をすべて VPN 経由で送信するフルトンネル(Full Tunnel)モードに対応した VPN や、クラウド型セキュリティ基盤である SASE を利用し、DNS 通信を含むトラフィック全体を保護することが重要である。

通信の一部のみを VPN 経由とするスプリットトンネル構成では、DNS 通信が公共 Wi-Fi 側の DNS サーバーへ送信される設定となっている場合があり、CaptiveCrunch のような DNS 操作による偽サイトへの誘導を防げない可能性がある。また、多要素認証(MFA)を導入している場合でも、認証後のセッションやトークンが悪用された場合には、不正アクセスを許す可能性がある。

そのため、MFA に加えて、フィッシング耐性を備えた、パスワードに依存しない認証方式である FIDO2 を導入するとともに、条件付きアクセスによってアクセス元や端末の信頼性を継続的に検証することが重要である。

2.6. まとめ

CaptiveCrunch は、企業が直接管理できないホテルや会議施設等の第三者インフラを悪用し、企業アカウントの侵害やマルウェア感染を通じた情報収集を狙う攻撃キャンペーンである。また、本事例は、企業内部のネットワークや端末のみを防御対象とする従来型のセキュリティ対策には限界があることを浮き彫りにしている。ホテルなどの公共 Wi-Fi がサイバー諜報活動に悪用される危険性は、ダークホテルなどの攻撃事例により以前から指摘されていたが、CaptiveCrunch はその脅威が現在も現実的なリスクであることを改めて示した。

今後は、公共 Wi-Fi などの外部ネットワークを信頼せず、「既に侵害されている可能性がある」というゼロトラストの前提に立った対策が求められる。また、攻撃の主眼が Microsoft 365 アカウントや認証トークンなどのアイデンティティ侵害へと移っている点も注目される。ネットワーク境界ではなくアイデンティティを防御の中心に据え、認証情報や認証トークンが窃取され得ることを前提としたセキュリティ戦略を推進することが重要である。

[21] 出典：MITRE『Darkhotel』
https://attack.mitre.org/groups/G0012/

3. 中国系ルーターのバックドア事案が示した通信機器リスク

3.1. 概要

2026 年 8 月 5 日、米国のセキュリティ企業 VulnCheck は、中国メーカーの Zbtlink(深圳市志博通電子)が製造した複数のルーターに、出荷時からバックドア（外部から不正にアクセスするための仕組み）が組み込まれているとする調査結果を公表した。VulnCheck によると、世界中で利用されている 10 万台以上の機種が、本件の影響を受ける可能性がある[22]。

3.2. バックドアの概要

VulnCheck はこのバックドアを「ENDLESSDOORS」と命名した。現時点では製造元から修正パッチ等は提供されておらず、根本的な解消手段は示されていない。なお、本件には、共通脆弱性識別子として CVE-2026-66747 が割り当てられている。

【動作の仕組み】

調査対象のルーターでは、バックドアが実際に稼働しており、約 35 秒ごとに外部サーバーと通信し、中国関連のドメインや IP アドレスへ接続していた。さらに、このバックドアは接続先サーバーの正当性を検証することなく、そのサーバーから送信されてきたコマンドを root 権限で実行できるほか、対話型シェル(外部からコマンドを実行できる環境)を起動する機能も有していた。

これらの通信はルーターの利用者に知られることなく行われており、バックドアは出荷後も継続的に稼働していた。

Role	Endpoint	Resolves to	Hosting
Primary	zbtctl.epplink[.]net	47.100.190[.]96	Alibaba Cloud, Shanghai
Primary	hardcoded IP	47.107.224[.]89	Alibaba Cloud, Shenzhen
Secondary	online-string.com	45.32.81[.]152	Vultr
Secondary	rbdg4nzqadui[.]wikaba[.]com	43.248.136[.]125	Jiangsu Dongyun Cloud

図 5 Zbtlink AX3000 Dual SIM 5G CPE WiFi 6 (型番: Z8102AX-2DSIM)と「ENDLESSDOORS」の通信先(C2 サーバー)[22]

3.3. 中国製通信機器を巡る懸念

これまで中国製通信機器を巡っては、安全保障やサプライチェーンリスクの観点から様々な懸念が指摘されてきた。その多くは、未知の脆弱性やバックドアが存在する可能性の他、発見された脆弱性への対応が適切に行われるのかといった将来的なリスクに関するものであった。

こうした懸念の背景の一つとして、中国における脆弱性管理制度が挙げられる。中国では脆弱性情報を政府機関へ報告することが義務付けられており、未修正の脆弱性情報の公開にも一定の制限が設けられている[23]。その結果、製品を利用す

[22] 出典: VulnCheck『ENDLESSDOORS Is Phoning Home. Pick Up.』
https://www.vulncheck.com/blog/zbt-endlessdoors

[23] 出典: 中央网络安全和信息化委员会办公室『工业和信息化部国家互联网信息办公室公安部关于印发网络产品安全漏洞管理规定的通知』
https://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

る個人や企業に情報が共有される前に政府が把握できる仕組みとなっていることから、脆弱性情報の管理・公開プロセスの透明性について欧米諸国から懸念が示されてきた。

なお、2024 年には TP-Link ルーターの脆弱性が中国系脅威アクターによって悪用され、大規模なボットネットの構築に利用されていたことが明らかになった。この事案では、TP-Link による情報隠蔽や中国政府への優先報告を示す直接的な証拠は確認されていない。しかし、中国メーカーの製品が中国系脅威アクターによる活動に利用されたことは、中国製通信機器に対して従来から存在していた安全保障上の懸念を改めて想起させる出来事として受け止められた[24]。

【各国における規制・対策の動向】

米国では従来から Huawei や ZTE など国家安全保障上の懸念があるとされた企業を米連邦通信委員会(FCC)の Covered List(国家安全保障上のリスクがあると判断された通信機器・サービスの一覧)に掲載している。これらの企業が製造する通信機器については、FCC 認証（無線通信機器などを米国内で販売する際に必要となる認証）の新規取得を制限すること[25]で、米国市場での販売や導入を抑制してきた[26]。

こうしたサプライチェーンリスクへの対応は米国以外の国々でも進められている。英国では Huawei を高リスクベンダーと位置付け、5G ネットワークからの排除を進めている[27]。一方、日本では特定企業を指定する方式ではなく、政府調達において製品やサービスのリスク評価を行うことで対応している[28]。

3.4. 本事案の特異性

Zbtlink 製ルーターに組み込まれていたバックドアについて VulnCheck は、単なる設計上の欠陥ではなく、意図的に実装された可能性が高いと評価している。製品自体に外部からの遠隔操作を可能とする機能が組み込まれていたとされる点で、本件は従来の脆弱性悪用事例とは性質を異にしている。

3.5. まとめ

本事案は、通信機器のリスクが、脆弱性への対応や悪用対策だけでは捉えきれない可能性があることを示した事例であり、これまで指摘されてきた設計・製造段階に起因するリスクが、単なる懸念にとどまらず現実の事象として顕在化し得ることを示した。さらに、通信機器の信頼性は運用段階のセキュリティ対策だけでなく、設計・製造・供給を含むサプライチェーン全体に

---

[24] 出典: Select Committee on the CCP『Letter to Commerce on Call for Investigation into Chinese Wi-Fi Routers in U.S. Vulnerable to CCP Hacking & Data Harvesting』
https://chinaselectcommittee.house.gov/media/letters/letter-commerce-call-investigation-chinese-wi-fi-routers-us-vulnerable-ccp-hacking

[25] 出典: Federal Communications Commission『Prohibition on Authorization of “Covered” Equipment』
https://www.fcc.gov/laboratory-division/equipment-authorization-approval-guide/equipment-authorization-system

[26] 出典: Federal Communications Commission『List of Equipment and Services Covered By Section 2 of The Secure Networks Act』
https://www.fcc.gov/supplychain/coveredlist

[27] 出典: GOV.UK『Huawei legal notices issued』
https://www.gov.uk/government/news/huawei-legal-notices-issued

[28] 出典: 国家サイバー統括室『IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ等について』
https://www.cyber.go.jp/pdf/council/cs/dai21/21shiryou05.pdf

依存することを改めて認識させた。今後は、製品の機能や価格だけでなく、供給元の信頼性や開発・保守体制も含めて評価する視点が、これまで以上に重要になると考えられる。

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
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-ps-osintmonitoring@security.ntt