# サイバーセキュリティレポート

# 2022.08

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 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『親ロシアハッカーグループの動向』

- ウクライナ侵攻以降、複数の親ロシアハッカーグループが、西側諸国への攻撃を行っている。
- 特に、Killnet はロッキードマーティン社等の欧米の組織のみならず、日本の組織に対しても攻撃を実行し、日本政府に対しては「宣戦布告」を行っている。
- ロシアとウクライナをめぐる国際情勢に関連し、ロシア系ハクティヴィストの攻撃手法や活動原理について今後も目が離せない。

第 2 章『SSVC による脆弱性管理』

- 脆弱性管理に広く利用されている CVSS には様々な問題があり、脆弱性管理業務は各組織がそれぞれに工夫を加えて対処を行っている。
- CVSS の問題解消のために提唱されているのが SSVC で、決定木による脆弱性の分類と明確な優先度決定が特徴として挙げられる。
- シンプルに意思決定を行うことができる SSVC は、CISA の重要インフラのアセスメントでも採用されており、今後さまざまな組織で利用が広がることが想定される。

第 3 章『Cisco へのソーシャルエンジニアリング攻撃』

- サイバー攻撃グループが、Cisco 社のシステムに侵入して窃取したデータを暴露サイト上で公開した。
- 被害分析から、Cisco への侵入には、MFA 疲労攻撃（MFA fatigue）や、ビッシング（vishing：音声フィッシング攻撃）といったソーシャルエンジニアリングが使われたことが判明した。
- 最新のソーシャルエンジニアリングに対しての脅威や対策をアップデートし、従業員の訓練に取り入れることが重要である。

# 1. 親ロシアのハッカーグループの動向

## 1.1. Killnet、ロッキードマーティン社への攻撃を開始

8 月 1 日、親ロシアのハッカーグループ「Killnet」は自身の Telegram チャンネルでロッキードマーティン社への攻撃開始を宣言した。ロッキードマーティン社が製造する高機動ロケット砲システム「HIMARS(ハイマース)」や、対戦車ミサイル「Javelin(ジャベリン)」は[1]、アメリカからウクライナに供与されており、高い戦果を上げていることから、同社が標的とされたと考えられる。

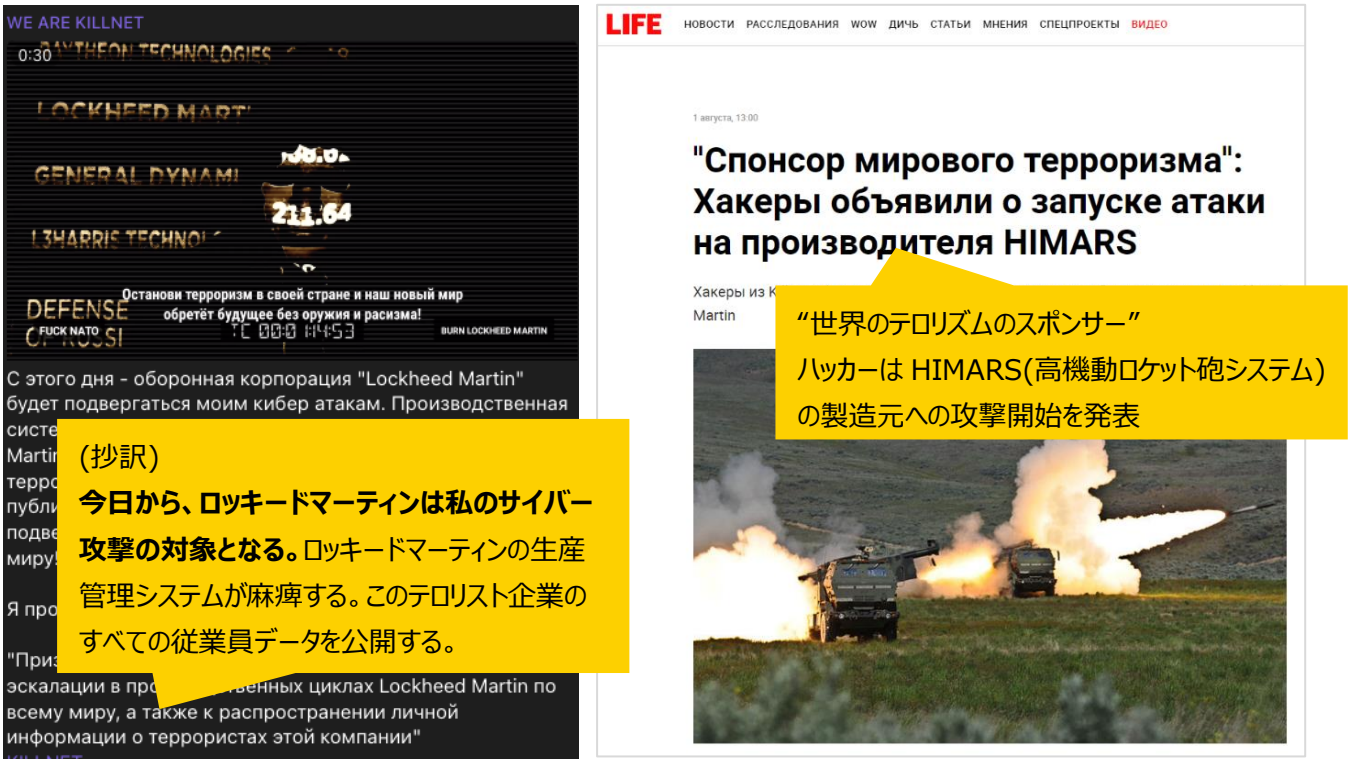


**図 1 (左)Killnet がロッキードマーティンを標的とすると宣言した投稿**
**(右)それを伝えるロシア語メディア「LIFE」の記事**

その後 8 月 11 日、Killnet は「もし何もやることが無ければ、ロッキードマーティンのテロリスト達にメールを送れ。写真とビデオを送り、彼らが作り出した兵器とそれが何をもたらしたか分からせるのだ」と自身の Telegram チャンネル上で発信。あわせて、ロッキードマーティンの従業員の氏名、メールアドレス、電話番号のリストと思われるファイルを提示した[2]。

[1] 出典：Newsweek 日本版『ロシアの進軍を止める？最強兵器「ハイマース」』
https://www.newsweekjapan.jp/stories/world/2022/07/post-99204.php

[2] 出典：HACKREAD『Killnet Claim They’ve Stolen Employee Data from Lockheed Martin』
https://www.hackread.com/killnet-hackers-hit-lockheed-martin-employee-data/

| | | | | | | |
|---|---|---|---|---|---|---|
| 120 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Bob Ba[redacted] | Bethesda, MD | +1 479 |
| 121 | [redacted] | z@lockheedmartin.com | Lockheed Martin Corporation | Kristen[redacted] | Bethesda, MD | +1 303 |
| 122 | [redacted] | ger@lockheedmartin.com | | | | |
| 123 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Nathar[redacted] | Bethesda, MD | +1 301 |
| 124 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Mark C[redacted] | Bethesda, MD | +1 301 |
| 125 | [redacted] | l@lockheedmartin.com | Lockheed Martin Corporation | Roxann[redacted] | Bethesda, MD | +1 301 |
| 126 | [redacted] | kheedmartin.com | Lockheed Martin Corporation | Benjam[redacted] | Bethesda, MD | +1 301 |
| 127 | [redacted] | @lockheedmartin.com | Lockheed Martin Corporation | Michae[redacted] | Bethesda, MD | +1 727 |
| 128 | [redacted] | heedmartin.com | Lockheed Martin Corporation | Kristin [redacted] | Bethesda, MD | +1 301 |
| 129 | [redacted] | n@lockheedmartin.com | Lockheed Martin Corporation | Marie V[redacted] | Bethesda, MD | +1 301 |
| 130 | [redacted] | r@lockheedmartin.com | Lockheed Martin Corporation | Cindy E[redacted] | Bethesda, MD | +1 301 |
| 131 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Bob Ba[redacted] | Bethesda, MD | +1 303 |
| 132 | [redacted] | n@lockheedmartin.com | Lockheed Martin Corporation | Chris B[redacted] | Bethesda, MD | +1 301 |
| 133 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Michae[redacted] | Bethesda, MD | +1 301 |
| 134 | [redacted] | ockheedmartin.com | Lockheed Martin Corporation | Eric La[redacted] | Bethesda, MD | +1 727 |
| 135 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Charle[redacted] | Bethesda, MD | +1 540 |
| 136 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Charle[redacted] | Bethesda, MD | +1 407 |
| 137 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Mat Hc[redacted] | Bethesda, MD | +1 301 |
| 138 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | David S[redacted] | Bethesda, MD | +1 301 |
| 139 | [redacted] | n@lockheedmartin.com | Lockheed Martin Corporation | Ehud M[redacted] | Bethesda, MD | +1 727 |
| 140 | [redacted] | heedmartin.com | Lockheed Martin Corporation | Brian J[redacted] | Bethesda, MD | |
| 141 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Steve M[redacted] | Bethesda, MD | +1 301 |
| 142 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Nichol[redacted] | Bethesda, MD | |
| 143 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Donald[redacted] | Bethesda, MD | +1 303 |
| 144 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Emmit[redacted] | Bethesda, MD | +1 301 |
| 145 | [redacted] | tt@lockheedmartin.com | Lockheed Martin Corporation | Edward[redacted] | Bethesda, MD | +1 301 |
| 146 | [redacted] | lockheedmartin.com | Lockheed Martin Corporation | Laurie [redacted] | Bethesda, MD | +1 301 |
| 147 | [redacted] | ckheedmartin.com | Lockheed Martin Corporation | Tyler H[redacted] | Bethesda, MD | +1 301 |
| 148 | [redacted] | ford@lockheedmartin.com | Lockheed Martin Corporation | Colin R[redacted] | Bethesda, MD | +1 301 |
| 149 | [redacted] | heedmartin.com | Lockheed Martin Corporation | George[redacted] | Bethesda, MD | +1 607 |
| 150 | [redacted] | s@lockheedmartin.com | Lockheed Martin Corporation | Sheila [redacted] | Bethesda, MD | +1 301 |
| 151 | [redacted] | ockheedmartin.com | Lockheed Martin Corporation | Larry S[redacted] | Bethesda, MD | +1 301 |

**図 2 投稿されたロッキードマーティンの従業員リスト(HackRead の記事より [2])**

ロッキードマーティンは Newsweek の取材に対し、この暴露については認識しており、ビジネスに対する脅威を低減させるポリシーや手順を定めている、また、堅牢で多層的な情報システムとデータセキュリティの完全性には、変わらず自信を持っていると答えた[3]が、Killnet が公開した従業員情報が攻撃によって窃取されたものかは明らかとなっていない。セキュリティ研究者は、「リストに掲載されている人々はロッキードマーティンの本物の従業員であるように見えるが、必ずしも同社が侵害されたとは限らず、古いデータやオープンソースデータを再構築したものである可能性もある」と指摘している[4]。

ロッキードマーティンの件は一例にすぎず、親ロシアのハッカーグループにより様々な攻撃が行われている。次項からは、ロシアのウクライナ侵攻以降、Killnet を始めとする親ロシアのハッカーグループが西側諸国に対して行っている攻撃を紹介する。

## 1.2. 親ロシアのハッカーグループ

親ロシアのグループの多数派は DDoS 攻撃を行っているが、この他にもデータの破壊・消去を目的としたワイパー型マルウェアの展開やランサムウェア攻撃、ウクライナ国内や NATO 勢力の分断工作等の心理戦といった多面的な攻撃を行っている。また、多くのグループで、ロシア製のメッセージツールである Telegram が攻撃の呼びかけや成果発表に利用されている[5]。

[3] 出典：Newsweek『Russian Hacker Warns Cyberwarfare Will Turn Deadly』
https://www.newsweek.com/deadly-cyberwarfare-warning-russian-hacker-killnet-1731949

[4] 出典：Spiceworks『Killnet Threatens “Lockheed Martin Terrorists” With More Cyberattacks』
https://www.spiceworks.com/it-security/security-general/news/killnet-threatens-lockheed-martin/

[5] 出典：Twitter『@Cyberknow20』
https://twitter.com/Cyberknow20/status/1556617972839751680

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Russia | Hydra | Dox/DDoS | Twitter | Russia | StriderHack | DDoS | Telegram |
| Russia | RaHDit | Hack | Telegram | Russia | Carbon | DDoS | Telegram |
| Russia | Xaknet | Hack | Telegram | Russia | KillMilk | DDoS/Hack | Telegram |
| Russia | Killnet | DDoS | Telegram | Russia | Graph | DDoS | Telegram |
| Russia | punisher_346 | PsyOps | Twitter | State-Sponsored | | | |
| Russia | DDoS Hacktivist Team | DDoS | Telegram | Russia | GhostWriter | Hack | UNK |
| Russia | Zsecnet | Dox/DDoS | Telegram | Russia | SandWorm | Hack/Wiper | UNK |
| Russia | DivisionZ | DDoS | Telegram | Russia | Gamaredon | Hack/Wiper | UNK |
| Russia | ZOV cyber army | Hack/Psyops | Telegram | Russia | DEV-0586 | Hack/Wiper | UNK |
| Russia | Cyber Front Z | Psyops/Dox | Telegram | Russia | DEV-0665 | Hack/Wiper | UNK |
| Russia | Info Front VoZzdie | Psyops/DDoS | Telegram | Russia | FancyBear/APT28 | Hack/Wiper | UNK |
| Russia | Cyber Army of Russia | DDoS/psyops | Telegram | Ukraine | IT Army of Ukraine | DDoS | Telegram |
| Russia | Legion | DDoS | Telegram | Ukraine | Internet Forces of Ukraine | Pysops | UNK |
| Russia | Beregini | Pysops/Dox | Telegram | Ukraine | US CyberCom | Hack | UNK |
| Russia | NoName057(16) | DDoS/Hack | Telegram | UNK | MustangPanda | Hack | UNK |
| Russia | ZSNOSINT | Pysops/Dox | Telegram | UNK | Curious George | Hack | UNK |
| Russia | FRwLteam | Hack/DDoS | Telegram | Russia | Turla APT | Hack | UNK |
| Russia | Zarya - Legion SF unit | Hack | Telegram | Russia | SaintBear/TA471 | Hack | UNK |
| Russia | Deadnet | DDoS | Telegram | UNK | TontoTeam | Hack | UNK |
| Russia | RedHackersAlliance | DDoS | Telegram | UNK | Space Pirates | Hack | UNK |
| Russia | Phantom Dev (AIDLocker) | Botnet | Telegram | UNK | Scarab | Hack | UNK |
| Russia | Blood Pirates | DDoS | Telegram | Russia | Calisto | Hack | UNK |
| Russia | Wizard Spider (Trickbot Crew) | Ransomware | UNK | | | | |
| Russia | AttackNet | DDoS | Telegram | KEY: | | | |
| Russia | 404Cyber (Readd) | DDoS/Hack | Telegram | Total Groups | 93 | Highest ever | |
| Russia | Anonymous Russia | DDoS | Telegram | Added | 14 | | |
| Russia | NBP Hackers | DDoS/Hack | Telegram | Removed | 10 | | |
| Russia | Phoinex | DDoS/Hack | Telegram | | Is for New Groups | | |
| Russia | Zeus | DDoS | Telegram | Pro-Russian | 43 | Highest ever | |
| Russia | Fr13ndsNetw0rk | DDoS | Telegram | Pro-Ukraine | 45 | | |
| | | | | UNK | 5 | | |

**図 3 親ロシア等のハッカーグループの分類 [5]**

**左から、国、当該国を支持・支援するグループ、主な攻撃手段、情報発信手段**

## 【Killnet】

前述の Killnet は「Killmilk」というハッカーが設立したグループである [3]。DDoS 攻撃を得意とすることで知られ、特に、Slow HTTP と呼ばれる手法を多用している[6]。これは他の DDos 攻撃と比べ、帯域幅をほとんど使用せず、リクエストの送信速度を遅くしたり、不完全なリクエストを送信したりすることで、サーバーを待機状態のままにさせることが可能である。ロシアによるウクライナ侵攻後には、同様の手法を用いて、コネチカット空港や米議会の公式 Web サイト[7]、欧州各国を跨いで開催されるユーロビジョンソングコンテストの投票システムに対して攻撃を行った。

前述のロッキードマーティンについても、データ窃取の他に DDoS 攻撃を行ったことを主張している。同社のドメインの Web サイトがアクセス不能になっている様子のスクリーンショットを示し、Akamai の DDoS 防衛システムを突破して攻撃を成功させたことを誇るかのようなメッセージを投稿している。

なお、設立者 Killmilk はロッキードマーティンへの攻撃前に Killnet からの脱退を表明しているが、その後も Killmilk はグループを保護するために動いていると語っており、Killnet の方も Killmilk が新しいグループを始めると語ったチャンネルを紹介しているので、完全に関係が切れているわけではないようである [7]。

[6] 出典：Bleeping Computer『Italian CERT: Hacktivists hit govt sites in 'Slow HTTP' DDoS attacks』
https://www.bleepingcomputer.com/news/security/italian-cert-hacktivists-hit-govt-sites-in-slow-http-ddos-attacks/

[7] 出典：CyberRisk Alliance『Founder of pro-Russian hacktivist Killnet quitting group』
https://www.scmagazine.com/analysis/cybercrime/founder-of-pro-russian-hacktivist-killnet-quitting-group

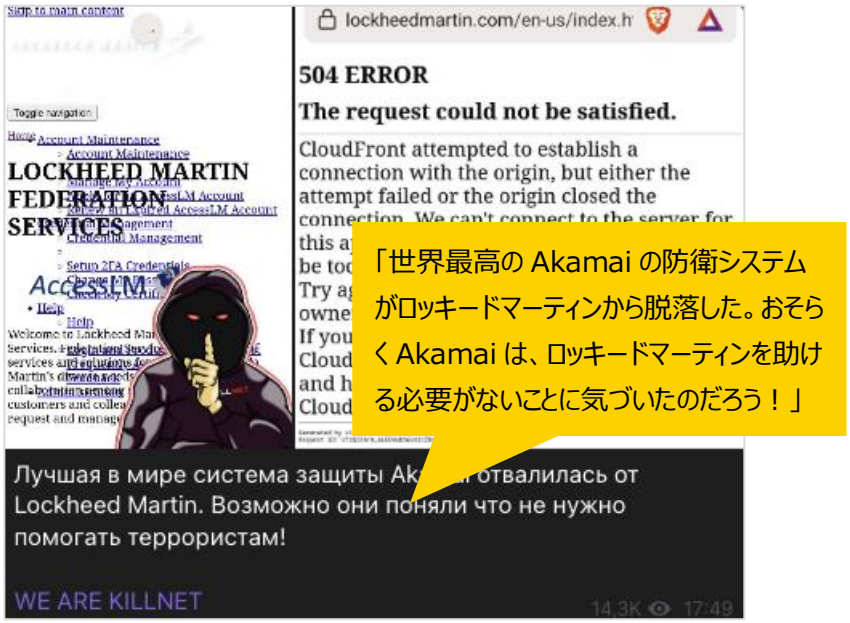


**図 4 ロッキードマーティンへの攻撃成功を伝える Killnet の投稿**

6 月 27 日に公開された NHK のインタビューで、Killnet は日本について、「反ロシア的な政策をとり、ウクライナを支援している国を攻撃している」、「日本も例外ではない。現時点では優先順位は低いが、日本がロシアに敵対的であるという事実を忘れてはいない」と語った[8]。

9 月 6 日、Killnet は日本の電子政府窓口「e-Gov」を含む複数のサイトを攻撃しオフラインにさせたと主張する投稿を行った。実際にそれらのサイトは一時的にアクセスできない状態となっていた。


**図 5 e-Gov を始めとする日本の公共サービスへの攻撃成功を伝える Killnet の投稿**

[8] 出典：NHK『世界に飛び火 “サイバー市民戦争” パンドラの箱は開かれた』
https://www3.nhk.or.jp/news/html/20220627/k10013690121000.html

さらに同日、Killnet は、「もしあなたが日本人なら、最も重要な日本のインターネットサービス名をコメント欄に書き込んでくれ」と支持者らに向けて投稿を行い、攻撃対象を募った。これに対し、支持者らから 200 件以上のコメントが寄せられ、日本の政府、銀行、交通サービス、公共サービス等、様々な組織の名が挙げられていた。そのうちの 1 件であった「mixi」は後に攻撃を受けている。

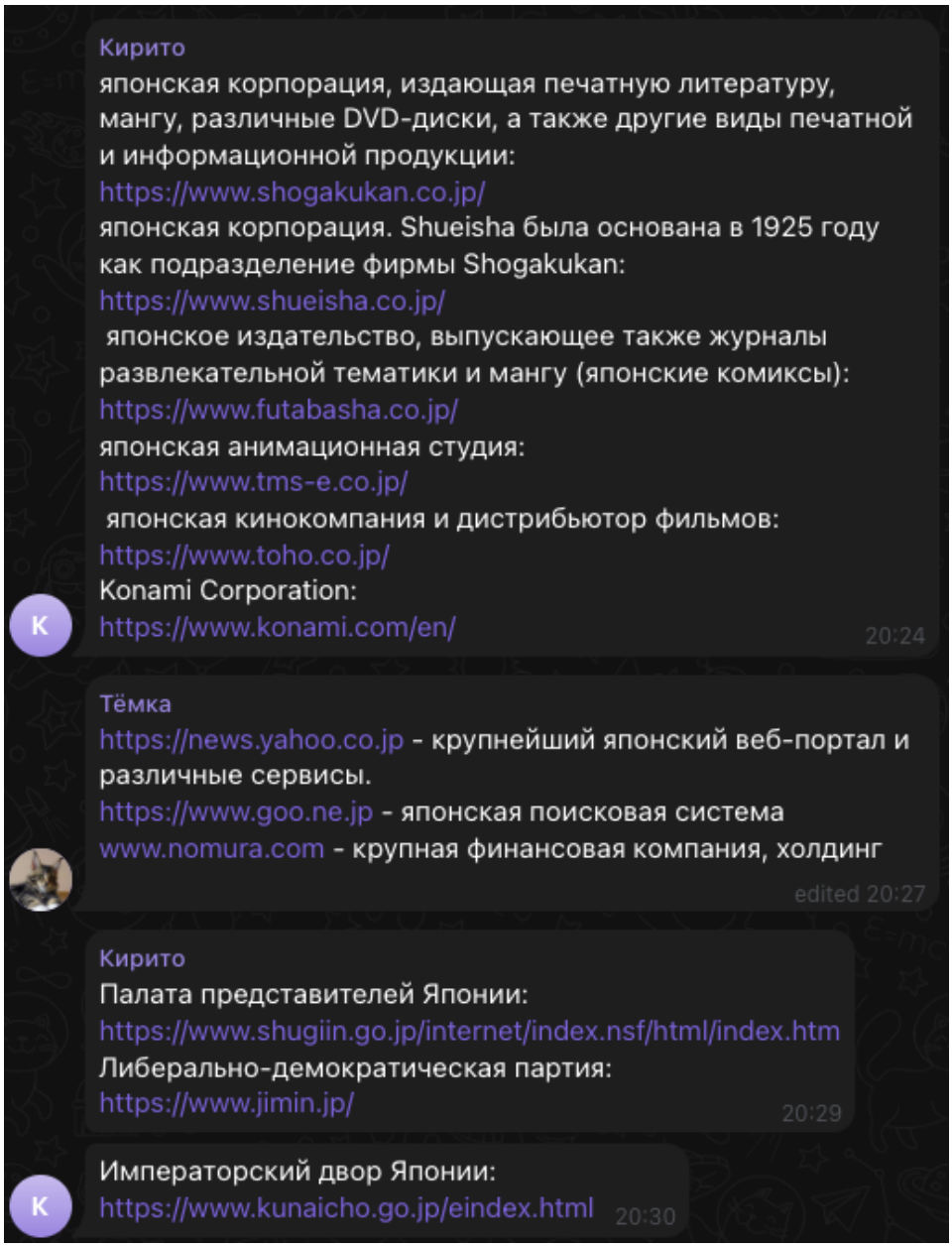


**図 6 Killnet の支持者らによって重要な攻撃対象としてあげられた日本のサイトの URL(一部)**

9 月 7 日、Killnet は日本語字幕付きで「ロシアはウクライナで犯罪を犯していません」「日本人は(このことを)知っているが、未だに反ロシアキャンペーンを行っている！」などと主張し、「**日本国政府全体に宣戦布告**」するという動画を投稿した。

これら一連の攻撃は、9 月 1 日から 7 日まで行われた、ロシア軍の極東での大規模軍事演習「ボストーク 2022」にタイミン

グをあわせて実行された可能性がある[9]。

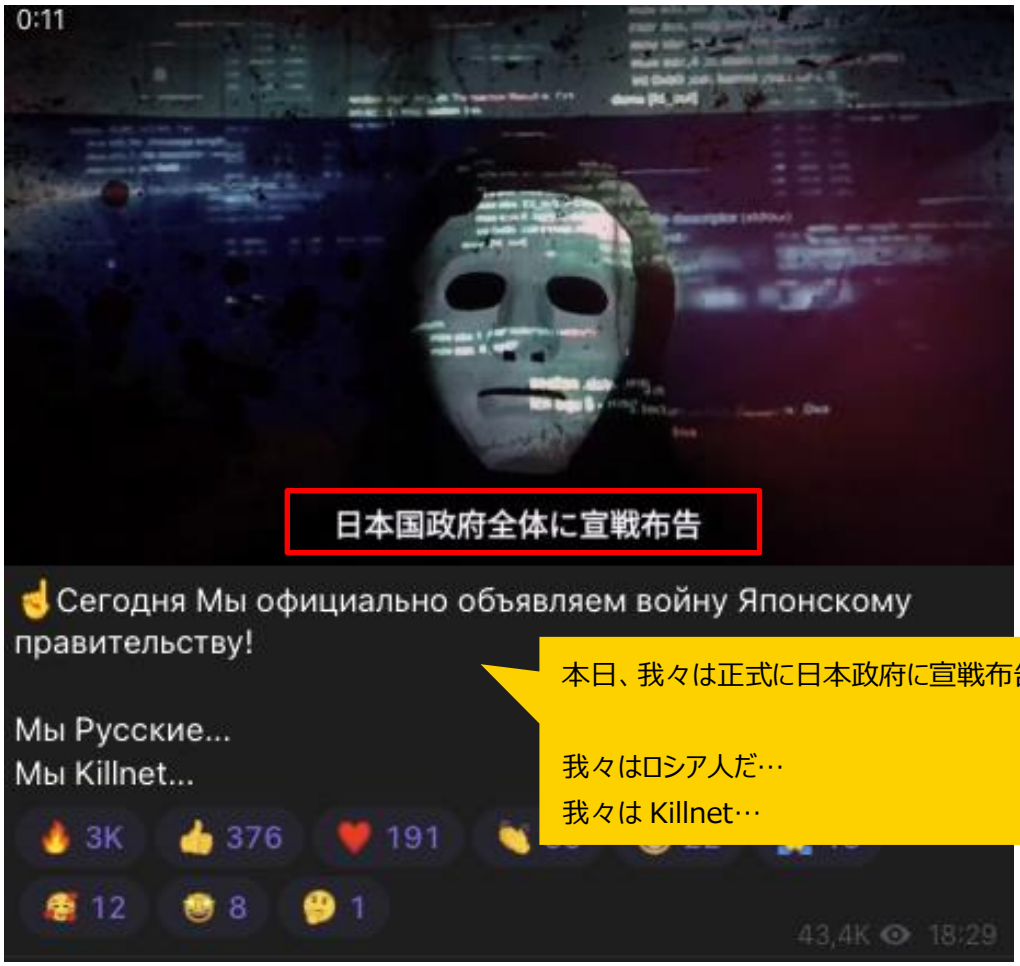


**図 7 Killnet による日本への宣戦布告**

**【HeawsNet】**

Killnet 以外にも日本を狙った攻撃を行うグループが確認されている。

「HeawsNet」は「DDoS 攻撃軍団(LEGION by DDoS)」を標榜している。Telegram チャンネルは 8 月 6 日に開設したばかりであり、新しいハッカーグループであると考えられる。開設時の投稿で「これらの国々に攻撃を行っていく」と述べ、攻撃対象となる 21 か国のリストを発表した。この中には日本も含まれている。

これまでに米国の学校紹介サイトやウクライナの銀行の Web サイト等へ DDoS 攻撃を行い、成果を報告しているが、日本の組織に攻撃を行ったという報告はない。

[9] 出典：読売新聞『ロシア軍の極東軍事演習「ボストーク」、プーチン氏が観閲…発言は公表されず』
https://www.yomiuri.co.jp/world/20220906-OYT1T50177/


**図 8 HeawsNet の Telegram チャンネル開設時の投稿(攻撃対象リスト)**

**【不明な攻撃者】**

DDoS 攻撃等のサイバー攻撃以外にも、親ロシアのグループによると考えられる日本関連の活動が見られる。攻撃者は判明していないが、8 月 13 日、ウクライナの偽情報対策センターは、ロシアが日本の寿司チェーン「寿司の美登利」を利用して、ウクライナ戦争に関する話は聞き飽きたというメッセージを拡散していたと発表した[10]。

寿司職人がウクライナ人女性の口を押さえた絵の横に「話題を変えよう！美味しい寿司について話そう！」と書かれた、同チェーン店の看板のように見える画像が Twitter 等で拡散された。同センターとウクライナ大使館が寿司の美登利に問い合わせたところ、拡散された画像は「当社と一切の関係が無い」と回答があった。

[10] 出典：UKRINFORM『ウクライナ偽情報対策センター、ロシアが日本の寿司店ブランドを利用した偽情報を拡散したと報告』
https://www.ukrinform.jp/rubric-society/3550018-ukuraina-wei-qing-bao-dui-cesentaroshiaga-ri-benno-shou-si-dianburandowo-li-yongshita-wei-qing-baowo-kuo-sanshitato-bao-gao.html


**図 9 ウクライナ偽情報対策センターによる注意喚起**

**【NoName057(16)】**

現在、フィンランドとスウェーデンは NATO への加盟を申請しているが、これについてジョー・バイデン米大統領が 8 月 9 日に支持を表明した。すると同日、フィンランド議会の Web サーバーが何者かによる DDoS 攻撃を受け、14 時半から 23 時頃までダウンする事態が発生した[11]。

「NoName057(16)」と名乗るグループが自身の Telegram チャンネルで、「我々は NATO への加盟を熱望する隣国フィンランドを"友好的に"訪問することを決め、同国の議会ウェブサイトの内部認証サービスを停止させた」とのメッセージを投稿。フィンランドが NATO への加盟手続きを進めていることに反発し、この攻撃を行ったことが窺える。

[11] 出典：Helsinki Times『Finnish Parliament's website brought down by Russian hacker group』 https://www.helsinkitimes.fi/finland/finland-news/domestic/22011-finnish-parliament-s-website-brought-down-by-russian-hacker-group.html

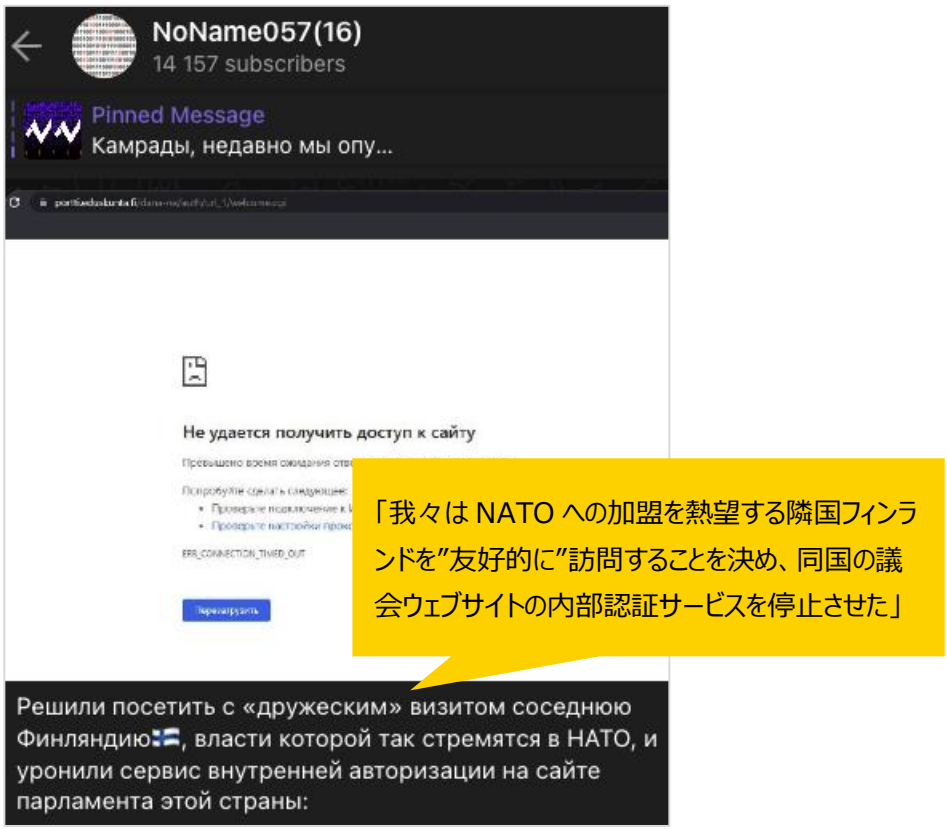


**図 10 NoName057(16)のフィンランド議会への攻撃を示唆する投稿**

NoName057(16)は、「ロシアに対して情報戦争が繰り広げられており、西側諸国がわが国の情報インフラストラクチャを攻撃しているが、ただ傍観するつもりはない」と述べている。同グループはその Telegram チャンネルに、フィンランド議会の他に、ラトビアやポーランドの裁判所・軍等の政府組織の Web サイトに対する攻撃成果を連日投稿している。

## 【Beregini】

8 月 9 日、「Beregini」という攻撃グループが、ウクライナ国防省のコンピューターから見つけたというデータについて Telegram チャンネルに投稿した。このデータは中東ヨルダンの企業が、カザフスタンの Technoexport 社から、旧ソ連時代の弾薬や装甲車等を購入する際の契約書であり、Beregini は、この取引にカザフスタンの駐英武官や英国国防省が関与していることを明らかにした。この契約書の存在は旧ソ連構成国家からなる CSTO(旧ソ連の安全保障条約機構)諸国の一角であるカザフスタンが裏切りととられる活動を行っていたことを示しており、ロシア系のメディアで大きく取り上げられた。本件について、カザフスタンの産業インフラ開発省は「Technoexport 社はそのような武器を海外に輸出するライセンスを持っていない」、「フェイクニュースである」と非難する声明を発表した[12]。しかし、親ロシア系メディア「Rybar」は、Technoexport 社が実際にはライセンスを取得していることを裏付ける資料を、カザフスタン政府内部から発見したと発表した。Beregini や Rybar が出した文書の真贋は不明だが、彼らの目論見通り、8 月 27 日、カザフスタン政府は 1 年間武器輸出を停止すると発表し[13]、

[12] 出典：Caliber.az『Russia's information attack on Kazakhstan: Who benefits from it?』 https://caliber.az/en/post/101391/

[13] 出典：EURACTIV『Kazakhstan halts arms exports amid Ukraine war』 https://www.euractiv.com/section/central-asia/news/kazakhstan-halts-arms-exports-amid-ukraine-war/

BereginiとRybarはそれぞれ「勝利宣言」を行った。

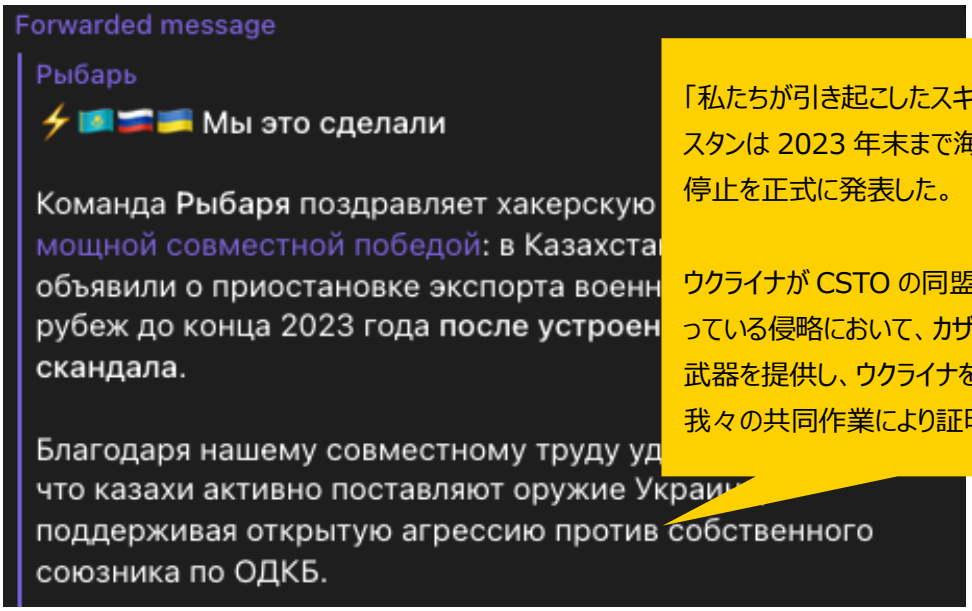


**図 11 Beregini が紹介した Rybar の「勝利宣言」**

## 1.3. まとめ

今回はロシア国家を支援する攻撃グループの中から特に注目を集める４つを紹介したが、ウクライナやその支援国／企業に対して攻撃を行うグループは他にも多く存在する。日本への攻撃も行われており、このようなロシア系ハクティヴィストの攻撃手法や活動原理について今後も注視したい。

# 2. SSVC による脆弱性管理

## 2.1. 概要

脆弱性管理の業界標準として利用されている CVSS（Common Vulnerability Scoring System）には様々な問題があり、脆弱性管理業務は各組織がそれぞれに工夫を加えて対処を行う必要があった。近年提唱されている **SSVC** は CVSS の問題に対応しており、今後利用が広がることが想定される。

## 2.2. CVSS を使った脆弱性評価の問題点 [14]

脆弱性の対応の優先度を決めるために、脆弱性の深刻度を総合的に評価して数値で示す CVSS がセキュリティ業界標準の指標として、広く利用されている。

しかし、CVSS でよく用いられる CVSS 基本値には、適切に深刻度を表現できていないという批判がある。これは、CVSS 基本値が反映する深刻度が、「攻撃の容易さ」「影響度」といった脆弱性発表時の技術的な観点のみで、「脆弱性の悪用状況」「ユーザー環境の重要性」といった評価時の観点までは反映していないことによる。また、CVSS は脆弱性を数値化して表現するだけに留まり、脆弱性対応をどのように行うのか方針を示すガイドラインが提示されていないといった問題もある。

このため、CVSS を利用した脆弱性対応は、各組織がそれぞれ工夫をして独自の対応基準や方針を別途定めての運用が行なわれている。

## 2.3. SSVC による新たな手法

### 【SSVC とは】

カーネギーメロン大学ソフトウェア工学研究所が CVSS の問題点を解決するために開発した、脆弱性分類の手法が **SSVC** である。「**S**takeholder-**S**pecific **V**ulnerability **C**ategorization」（利害関係者固有の脆弱性の分類）の略で、CVSS を逆から読んだ文字列になっている。2019 年に初公開され、2021 年 4 月のバージョン 2.0 が最新版である[15]。

SSVC は脆弱性の対応優先度を決定するために決定木を採用している。決定木は使用者の立場に合わせ、脆弱性のあるソフトウェアのパッチを提供するサプライヤー用、提供されたパッチをシステムに当てるパッチ展開者用、CERT/CC のようにパッチ実施の調整をする組織のコーディネーター用の 3 パターンが提示されている。

一部で利用が始まっており、米 CISA は、重要インフラ事業者のシステムに脆弱性修正の命令を出す際の根拠となるアセスメントに、SSVC を使用している[16]。

以降、SSVC の重要な特徴である、決定木と優先度の決定について説明する。

---

[14] 出典：PwC Japan グループ『SSVC（Stakeholder-Specific Vulnerability Categorization）を活用した脆弱性管理』
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/stakeholder-specific-vulnerability-categorization.html

[15] 出典：Carnegie Mellon University『Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)』
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653459

[16] 出典：CISA『Subpoena Process』
https://www.cisa.gov/subpoena-process

**【特徴 1：決定木による脆弱性の分類】**

「脆弱性の悪用状況」「攻撃者にとっての攻撃の有用性」「ユーザー環境の重要性」等の問いに対し、決定木（図 12）で対話的に行う。使用者が利用する決定木により異なるが、わずか 3～4 段階の分岐で決定するシンプルな構成となっている。

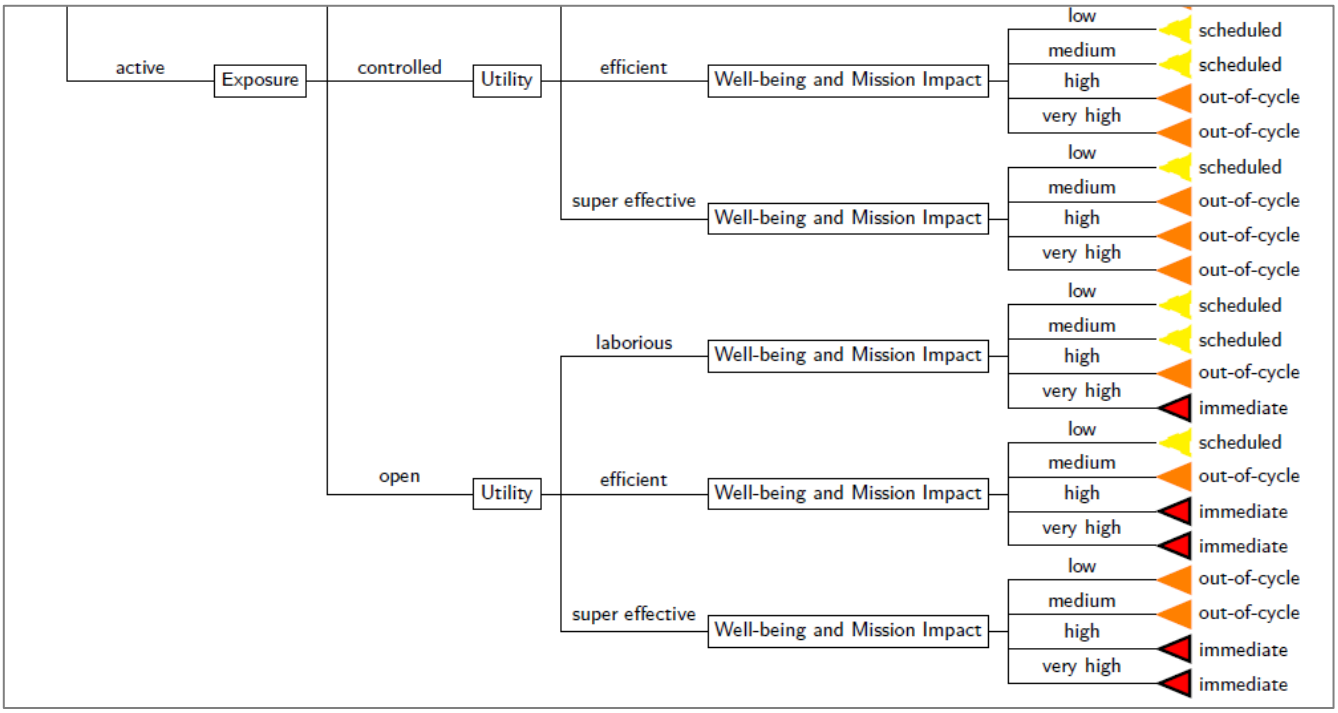


**図 12 SSVC の決定木の例（一部拡大）**[17]

**【特徴 2：優先度の決定】**

決定木により、どれくらい優先して対応すべきかのアクションを表す 4 段階の**「対応の優先順位」**（表 1）を導き出すことができる。この結果に従い、使用者は対応方針を決定する。

| 優先度 | 内容 |
|---|---|
| Immediate | 全てのリソースを集中し、必要に応じて組織の通常業務を停止して、可能な限り迅速に対応する |
| Out-of-Cycle | 通常よりも迅速に行動し、計画外の機会に緩和策または修復策を実施する |
| Scheduled | 定期メンテナンス時に対応する |
| Defer | 現時点では対応しない |

**表 1 対応の優先順位**

[17] 出典：Carnegie Mellon University『Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)』
https://resources.sei.cmu.edu/asset_files/WhitePaper/2021_019_001_653461.pdf

## 2.4. まとめ

SSVC は決定木に基づき脆弱性を分類し、ストレートに対応の優先度を導き出す。CVSS に比べてシンプルに意思決定を行うことができ、今後、脆弱性管理のスタンダードになる可能性がある。

# 3. Cisco へのソーシャルエンジニアリング攻撃

## 3.1. 概要

2022 年 8 月 10 日、ランサムウェアグループとみられるサイバー攻撃グループが Cisco 社から盗んだデータを暴露サイトで公開し、同日、Cisco 社は内部データの流出があったことを同社のサイトで明らかにした[18] [19]。被害分析から、多要素認証がソーシャルエンジニアリング攻撃で突破され、侵入口となっていたことが判明した。

## 3.2. Cisco への侵入方法

侵入は 2022 年 5 月下旬に行われたとみられている。

Cisco の従業員 1 名が、内部へのログイン認証情報を Google Chrome に保存しており、更にこれを自身の Google アカウントに同期させるよう、設定していた。そして攻撃者は、何らかの方法でその従業員の Google アカウントに侵入し、同期されていた Cisco のログイン認証情報を盗み出した[20]。その後、Cisco への不正アクセスを試み、導入している多要素認証（MFA）を突破するために、この従業員に対し、**MFA 疲労攻撃**（MFA fatigue）や**ビッシング**（vishing：音声フィッシング攻撃）を実行。最終的に Cisco 社内のドメインコントローラーへの特権アクセスを取得し、データを盗み出すことに成功した。なお Cisco 社によると、ランサムウェアによる暗号化は行われていない。

### 【MFA 疲労攻撃（MFA fatigue）】[21] [22]

多要素認証の一例として、パスワードを入力したユーザーのスマートフォンに「MFA プッシュ通知」を送信し、その画面に表示された承認ボタンをユーザーがタップすることにより、ログインさせる方法がある。攻撃者は何らかの方法でユーザーのログイン情報を入手後、MFA プッシュ通知を自動的に作成するツール等を利用し、ユーザーに対して大量の通知を送信する。ユーザーはこの現象を単なるバグと考えるか、或いは大量の通知を受信する煩わしさに根負けし、通知を承認してしまう。これが、MFA 疲労攻撃である。

---

[18] 出典：Bleeping Computer『Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen』
https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

[19] 出典：Cisco『Cisco Event Response: Corporate Network Security Incident
https://tools.cisco.com/security/center/resources/corp_network_security_incident

[20] 出典：Cisco Talos『Cisco Talos shares insights related to recent cyber attack on Cisco』
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html

[21] 出典：HIGHTOUCHTECHNOLOGIES『What Is MFA Fatigue?』
https://hightouchtechnologies.com/what-is-mfa-fatigue/

[22] 出典：GoSecure『Current MFA Fatigue Attack Campaign Targeting Microsoft Office 365 Users』
https://www.gosecure.net/blog/2022/02/14/current-mfa-fatigue-attack-campaign-targeting-microsoft-office-365-users/

**【ビッシング（vishing：音声フィッシング攻撃）】**[23] [24]

ビッシングとは、voice phishing の略で、電話で人を騙し、機密情報を提供させる攻撃である。例えば、攻撃者は IT ヘルプデスクになりすまして従業員に電話をかけ、従業員からログイン認証情報を聞き出す。また、ソフトウェアベンダーやサービスプロバイダーを騙り、ログイン認証情報を顧客から攻撃者に提供させることもある。

被害に遭った Cisco の従業員も、様々な信頼できる組織を名乗る者から数日間、複数回にわたり電話を受け、訛りのある英語で説得された結果、MFA プッシュ通知を承認してしまった [18] [20]。

## 3.3. 攻撃グループの特徴

**【侵入した攻撃グループ】**[20]

Cisco のセキュリティチームは侵入した攻撃グループの特定を試みており、攻撃の特徴から**イニシャルアクセスブローカー（IAB）**と呼ばれるタイプの組織であると推定している。IAB は脆弱性をついた攻撃やブルートフォース攻撃等を実行することにより、外部から企業ネットワークへのログインを可能とする「初期アクセス権」を不正に取得し、更にそれらを脅威アクターに販売している。

また、Yanluowang と呼ばれるランサムウェアグループの暴露サイトを利用していることから、Yanluowang 運営者と関係のあるイニシャルアクセスブローカーであると分析している。

他にも、侵入後のハッキングの技術等に UNC2447 や Lapsus$といった攻撃グループの特徴が見られることから、これらの組織とも接点があると推察している。

**【Yanluowang の暴露サイト】**

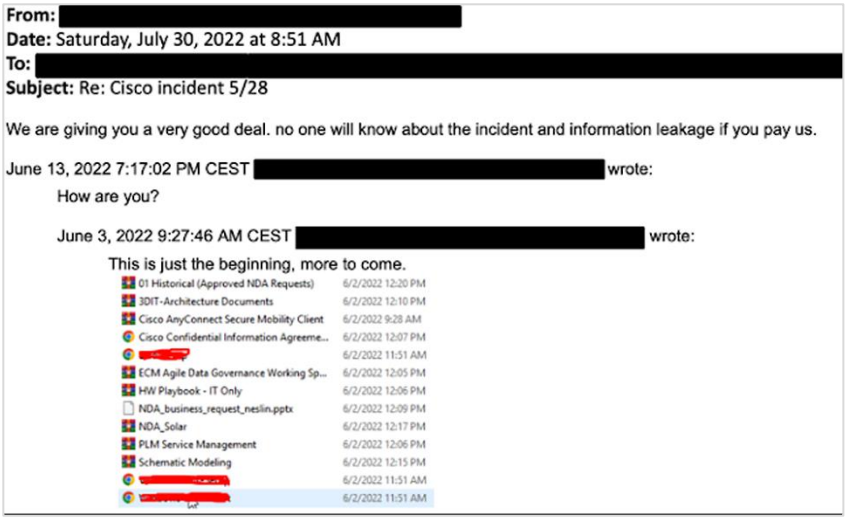


**図 13 攻撃グループから Cisco へのメール**

[23] 出典：IRONSCALES『Vishing Attacks Explained』
https://ironscales.com/blog/vishing-attacks-explained

[24] 出典：TechRepublic『Voice phishing attacks reach all-time high』
https://www.techrepublic.com/article/voice-phishing-attacks-reach-all-time-high/

Cisco は 5 月末に本インシデントを検知後、全社的にパスワードリセットを行う等、攻撃者の封じ込めを図った[20]。Cisco が対応した後、攻撃グループは Cisco との間でメールのやり取りを行い、攻撃成功の証拠として、流出したディレクトリの一覧を添付したメールを送った。さらに 2022 年 8 月 10 日に、Yanluowang の暴露サイト上で Cisco から奪ったファイルのリストを公開した。

同社によると、侵入に使われた従業員のアカウントからアクセスできるデータのみ流出しており、これに機密情報等は含まれていない。

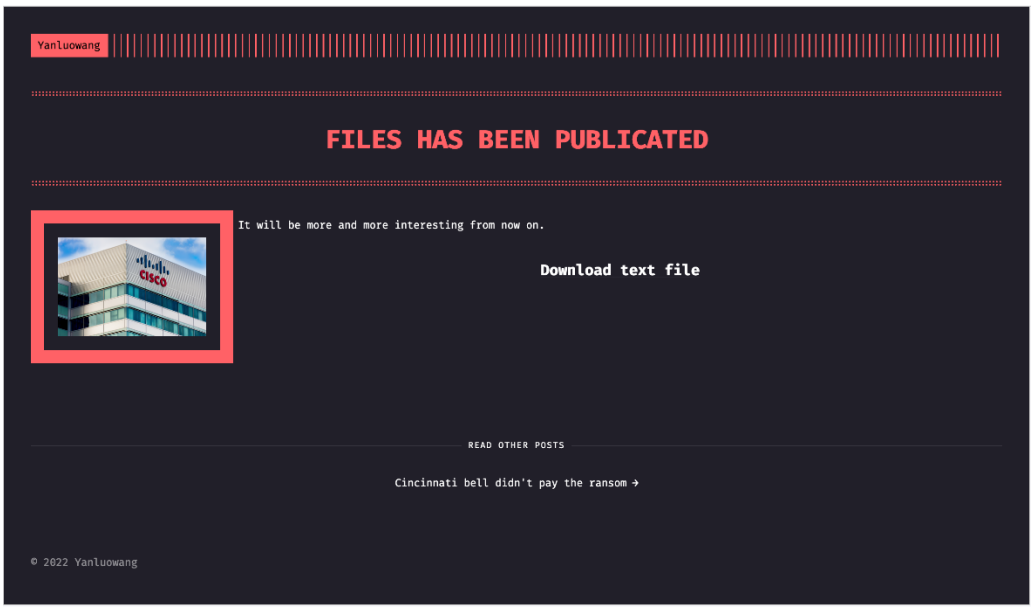


**図 14 Yanluowang の暴露サイト上の Cisco の暴露**

Yanluowang は、ファイル暗号化、ダークウェブに設けた暴露サイトでの暴露、DDoS の 3 種で被害者を脅迫する、三重脅迫型ランサムウェアグループである[25]。Yanluowang の名前は、地獄の王として死者の生前の罪を裁く閻羅王（閻魔王）の中国語読みに由来しているが、本グループと中国との関連性は不明である。

主に米国、トルコ、ブラジルの大企業に攻撃を仕掛けており、2022 年 6 月にはアメリカの小売業者ウォルマート社にランサムウェア攻撃を仕掛けたと主張したが、同社は否定している[26]。

**【接点がみられた他グループ】**

ロシア系の UNC2447 は、過去には FIVEHANDS、HELLOKITY など様々なランサムウェアを使用し、窃取後に暗号化したデータの復号、及びそれらのデータの非公開と引き換えに金銭を支払うことを被害組織に要求する「二重脅迫」を行っていた。

Lapsus$は 2021 年 12 月から本格的に活動していたとみられるハッキンググループである。Microsoft 等の有名企業にソーシャルエンジニアリングを用いて侵入し、2022 年 3 月には Lapsus$のメンバーである 16 歳から 21 歳までの 7 人がロンド

[25] 出典：Kaspersky 『Kaspersky、ランサムウェア「Yanluowang」の感染に対応する復号ツールをリリース』 https://www.kaspersky.co.jp/about/press-releases/2022_vir27042022

[26] 出典：Bleeping Computer 『Walmart denies being hit by Yanluowang ransomware attack』 https://www.bleepingcomputer.com/news/security/walmart-denies-being-hit-by-yanluowang-ransomware-attack

ン市警察に逮捕された[27]。

どちらのグループも最近は活動がみられないため、かつてこれらのグループに参加していたメンバーが Cisco を攻撃したグループと接点を持っている可能性が考えられる。

## 3.4. Cisco の教訓

Cisco は事件発生の報告と同日に、自社のセキュリティチームが調査した攻撃手法についての詳細な分析記事を公開した[20]。同社はこの一件を受け、ビッシングなどのソーシャルエンジニアリングの脅威に対応するためには、脅威の周知が大切であると呼び掛けている。また、MFA の導入後、スマートフォンに不正なプッシュ通知を受けた場合、従業員はどのように対応する必要があるのか、誰に連絡すればよいのか等、ユーザー教育が必要であると述べている。

## 3.5. まとめ

ハッキング技術だけでなく、ソーシャルエンジニアリング手法も年々巧妙化している。Cisco は、ビッシングなどのソーシャルエンジニアリングの脅威に備えるために様々な対策を提示しているが、中でも、**ユーザー教育が最も重要**と述べている。

被害企業が語る経験からも、最新の手法を取り入れた訓練や教育を実施して、従業員のソーシャルエンジニアリング耐性を上げることの重要性が高まっていることが伺える。

以上

[27] 出典：Palo Alto Networks 『脅威に関する情報：Lapsus$グループ』
https://unit42.paloaltonetworks.jp/lapsus-group/

**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