サイバーレスキュー隊（J-CRAT）活動状況
[2022 年度上半期]

2022 年 12 月 28 日

サイバーレスキュー隊（J-CRAT）では、主に国家支援型（ステートスポンサード、ネイションバックド）[1]とされる攻撃者によるサイバー活動（標的型サイバー攻撃）、特にサイバーエスピオナージに対して、相談対応、レスキュー活動、脅威情報の収集及びサイバースレットインテリジェンスの活用等を通じた情報収集（スレットハンティング）等を行っている。

2022 年度上半期及び本活動状況報告の発出にいたる期間を通じたサイバー状況把握の結果、我が国に対するサイバーエスピオナージは依然として継続していることを確認している。特に、国際情勢などを背景としたエネルギー需給のひっ迫や地球環境問題への関心が高まっている状況で、エネルギー・環境関連分野が国家を背景とする攻撃グループによるサイバーエスピオナージの重点的な攻撃対象となっている可能性が改めて認識された。

またロシアによるウクライナ侵攻に際して、システムの物理的な破壊を伴うサイバー攻撃やサイバーエスピオナージが実施されると同時に、ウクライナ国民の士気を下げ、ウクライナと同盟国を分断させようとするサイバー空間上の情報工作が行われていると報じられた。そして、有事においてはハクティビストによる Web サイト改ざんや分散型サービス妨害（DDoS）攻撃、ランサムウェアなどサイバー犯罪についても、有事当事国の関与が疑われるなど、非常に広範囲なサイバー状況把握の必要性を再確認することとなった。

我が国近隣に着目すると、米国ペロシ下院議長の訪台に伴い緊張の高まった 8 月、実空間で行われた中国による大規模軍事演習に合わせて、サイバー空間では台湾に対するフェイクニュースの大量流布など認知領域での活動から、政府機関への DDoS 攻撃、デジタルサイネージのハッキングが複合的に実行されたと報じられており、ハイブリッド戦や網電一体戦と呼ばれるマルチドメインでの攻撃形態の可能性が浮き彫りとなったともいえよう。

このような状況を鑑み、我が国においてもナショナルサイバーセキュリティやナショナルサイバーディフェンスなど、国家によるサイバー空間をめぐる安心・安全の在り方が広く議論されているが、当隊でも引き続き国家的意志を背景としたと目されるサイバー領域（ドメイン）及びそこに直接的・間接的・副次的に関わる物理領域や認知領域にまたがる活動に対して、広範囲な視点によるサイバー状況把握を継続していく所存である。

本活動報告で紹介するサイバー状況の報告が、我が国そして各組織及び個人に対する国家支援型サイバー活動に対する理解の一助となり、即応を目的とした情報の利活用に加え、中長期的な政府による抑止や防御対応に資する情報共有の推進、ひいては我が国一丸となったサイバーセキュリティ活動の形成につながることを望む。

[1] 公開情報などによれば、実際の活動は外国の軍及び情報機関、宣伝機関が直接、または下請のハッカー（Hack-For-Hire）や犯罪者（政府放任型サイバー犯罪グループ）を介して行われるとされる。

1　活動結果

年度毎の「標的型サイバー攻撃特別相談窓口」に対して寄せられた相談や情報提供の件数、緊急を要する事案に対してレスキュー支援を行った件数及びオンサイトでの支援件数を表 1 に示す。

表 1 J-CRAT 支援件数の推移

	2019 年度	2020 年度	2021 年度	2022 年度 上半期
相談・情報提供	392	406	375	205
リモートレスキュー	139	102	94	91
オンサイトレスキュー	20	17	9	15

※中長期に渡る 1 つの事案に対して複数回のオンサイト対応を要した場合も、1 件として集計

2022 年度上半期に「標的型サイバー攻撃特別相談窓口」に対して寄せられた**相談・情報提供**は **205 件**であった。このうち、**リモートレスキュー支援**へ移行したものは **91 件**、うち**オンサイト支援**を行った事案数は **15 件**であった。

なお、近年では実際の事案発生に対するレスキュー対応だけでなく、事案発生前のキャパシティビルディングや、事案発生後の対処内容に対する助言活動からスレットハンティングといったアクティブなサイバーレスキュー活動（アクティブサイバーレスキュー）も増えている。

2　2022 年度上半期の活動を通じてみられた特徴的な事項

当隊では、脅威情報を認知領域や物理領域といったマルチドメインで複合的に把握することや、攻撃の背景を窺うに値する地政学的傾向や安全保障、国際経済など、近隣諸国や同盟国、有志国の動向を重要視している。本項では、2022 年度上半期を中心に、当隊活動を通して把握した国家支援型サイバー活動のうち、特にサイバーエスピオナージを中心にいくつか特徴を述べる。

2.1　エネルギー政策関係者等を標的としたと目される攻撃活動（Op.EneLink）

2021 年下半期の活動報告に記載した国内の資源・エネルギー部門に関係する組織や研究者、メディア関係者等を標的とする攻撃は、2022 年上半期には、学術機関のエネルギー政策関係者を中心に、公共政策、金融、経済、安全保障といった分野に対する攻撃も新たに確認され、より活発に確認された。2022 年 5 月にセキュリティベンダが公開したレポートでは、本攻撃に関連する活動を「RestyLink」と呼んでいるが[2]、当隊ではその後の観測状況等も踏まえ、本攻撃活動を「オペレーション・エネリン（Op.EneLink）」と呼称し、活動を注視している。

メールに記載されたリンク先から攻撃ファイルをダウンロードさせる手法や、メール文面の丁寧かつ流暢な日本語といった特徴は変わっていないが、6 月以降に観測された攻撃では、実在する組織、関係者を詐称し、ごく少数の特定の受信者に対してイベントや交流会への参加依頼、取材や講演の依頼などを行い、二回目以降のやり取りで悪性コードを含んだファイルのリンクを提示しダウンロード・実行をさせ、その後も日程調整などのやり取りを継続した後、最終的には新型コロナなどを理由に依頼を中止することで被害者に不信感を抱かせないようにするのが典型的手法であった。以前は攻撃メールの送信元はフリーメールであったが、2022 年上半期には詐称した組織に似せたドメインを取得し、国内のメールサービスを利用して、詐称した送信者を模したメールアドレスから攻撃メールが送付される事例が新たに確認されている。

また、初期侵入後の特徴として、数日から十数日後に、クラウドのオンラインストレージサービスを悪用し

[2] Operation RestyLink: 日本企業を狙った標的型攻撃キャンペーン
https://insight-jp.nttsecurity.com/post/102ho8o/operation-restylink

たマルウェアを用いて端末内のドキュメントファイル等を窃取する動きが見られた。

さらに、攻撃基盤について調査したところ、一部 IP アドレスについて、中国が関与していると指摘されている攻撃グループが使用していた IP アドレスと一致していたものがあったことを確認している[3]。

当隊では引き続き攻撃活動の更なる拡大を警戒すると同時に全容の把握に努めており、皆様からの情報提供にも期待している。些細と思われる情報であっても、是非当隊へ御連絡いただきたい。

加えて、このような脅威は組織だけでなく、個人のプライベートメールを攻撃対象ともするため、地政学や国際関係に関わる方や組織は相互に注意しあうと同時に、学術関係者、シンクタンク研究員が標的になっているという情況を踏まえ[4]、警察など政府機関や当方ら政府関係機関とよく連携をとり、不審な脅威情報（不審メール）があった場合は情報連携（情報提供）にご協力いただきたい。

2.2 安全保障、国際政治、外交、メディアを標的としたと目される攻撃活動

LODEINFO と呼ばれる諜報用マルウェアを用いた攻撃は、2019 年末以降 2022 年上半期も継続して活発な活動が確認された。攻撃の標的とされた分野も従来同様、安全保障、国際政治、外交、メディアであった。

一連の活動では、攻撃メールは主にフリーメールから送信されているが、送信者名（表示名）はメール受信者に関係のある、実在する組織、個人を詐称している。メールの添付ファイルで送付する資料（マルウェアのダウンローダを内包した攻撃ファイル）のテーマも攻撃ターゲットが興味を持ちそうな分野とするなど、攻撃の成功率を上げるため事前にターゲットの調査を入念に行っていることが伺える。同一のターゲットに対しテーマを変えながら何度も攻撃メールを送付するなどしつこく粘り強い攻撃が行われており、事前準備の周到さと合わせ、いかにも高度な持続的脅威（Advanced Persistent Threat; 通称 APT）の攻撃であると言える。

ただ、事前準備の周到さに対して攻撃メール自体はやや不自然、お粗末なところが見受けられるところもあり、特に 2.1 に記載した攻撃に比べると不自然さが目立つ。この攻撃者は詳細なやり取りに耐えられるほどの語学、知識、慣習に習熟していない可能性はある。また、事前調査と実際の攻撃で異なるチームが担当している可能性もあるだろう。

2022 年上半期にある攻撃で攻撃メールの送信元に詐称されていた組織、個人が、別の攻撃ではターゲットとされ攻撃メールを受信していた事例も確認されている。通常、攻撃メールを受信した場合は継続した他の攻撃を受けていないか、マルウェア感染などに至っていないかなど、攻撃を受けた前提での調査、対応を行うが、詐称された送信元側でもサプライチェーン攻撃のように攻撃が連鎖していないか注意すべきであろう。

また、2.1 に記載した攻撃でターゲットとなった組織、個人が、こちらの攻撃では詐称された送信元となっていた事例も確認されている。ターゲットとなる攻撃分野が重複しているためたまたまそうなったのか、あるいは攻撃者に共通部分がある、攻撃者間で情報を共有しているといったことがあるのかはこの事例からは判断できないが、両方の攻撃でターゲットとなりうることには注意が必要であろう。

昨今の攻撃では、いきなり攻撃メールを送付せず、着信と関心度を確認しながら、メールのやりとりを通じた添付ファイルや悪性リンククリックへの心理的負荷を減らすようなソーシャルエンジニアリング技術を取り込むこともあり、不審メールに気づいた段階で防御にまわると、攻撃者の推定に関わる攻撃ツールの回収にいたらないケースもある。一方でこのようなケースでは、政府や政府関係機関と協力し、攻撃ツールを回収し、被害の抑止や防御に向けた対応の検討に資することも可能なため、再掲となるが脅威情報（不審メール）があった場合は政府での利活用を目的とした情報連携（情報提供）にご協力いただきたい。

2.3 インターネット境界装置の脆弱性を悪用した攻撃

2022 年 5 月 4 日に公開された通信制御装置（ネットワーク装置、ゲートウェイ製品）の脆弱性（CVE-

[3] RISING TIDE: 中国 APT による南シナ海における諜報活動の潮流を追う
https://www.proofpoint.com/jp/blog/threat-insight/chasing-currents-espionage-south-china-sea
[4] 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）
https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf
https://www.nisc.go.jp/pdf/press/20221130NISC_gaiyou.pdf

2022-1388）を悪用し、国内組織への侵入が試みられたネットワーク貫通型の攻撃事例が報告されている[5]。攻撃コードの中に国内に位置する通信制御装置の IP アドレスが記載されていたこと、攻撃者の使用したサーバの調査から、TSCookie 及び Bifrose といった攻撃グループ BlackTech と関係の深いマルウェアが発見されている。

当隊の収集した情報からは、攻撃インフラは遅くとも 2021 年 12 月頃より段階的に更新されており、5 月に当該脆弱性が公開された以降に活動が活発化したことが示唆されている。攻撃グループは常時より攻撃準備を整えており、脆弱性情報に即応する体制を敷いていると推察する。対する防御側の姿勢として適時の脆弱性管理が求められることは当然として、自組織のインターネット境界装置が侵害された場合を想定し、セグメンテーションの構成や侵害検出の仕組みを点検しておくことで、侵害を検知可能か、窃取リスクに晒されている情報は何か、横展開される範囲はどこまでか、などを予め把握し対策することも有効である。

また、このような国家を背景とすると目される組織的かつ巧妙なサイバー攻撃に対しては、各主体間によるサイバー防御活動としての脅威情報の共有活動だけでなく、政府による抑止及び防御に向けた対応が必須であり、ナショナルサイバーセキュリティの時代、新たな情報共有の必要性を考えるうえでも重要なケースであると考えている。

3 我が国を取り巻くサイバー攻撃グループ

本項では、我が国周辺国を中心に、本報告期間の情報収集を通じてみられた国家支援型サイバー活動として報じられている情報の中から特徴的な動向の一部を紹介する。公開情報として報告されている攻撃グループの属性を地域毎に分類したこれらの脅威情報は、日本国内への影響度を判断してリスク管理、危機管理につなげていくべきと考えている。直接の影響が少ないと思える脅威情報であっても、現地法人や海外支店などの海外拠点が被害に巻き込まれるだけでなく、それらを介して国内まで侵害を受ける可能性も考慮すべきと考える。また、グローバル展開されている企業などで、日本国外における国家を背景としたサイバー活動に関わる事象を把握された場合は、国際連携も含めた政府による抑止や防御のための対応に資するためにも、ぜひ政府や政府関係機関への情報連携をしていただくことを期待する。

3.1 中国に関係するサイバー攻撃グループ

中国の関与が疑われるサイバー諜報活動では、前述の活動や、日本国外での活動とされる TA423、APT10、Mustang Panda、Tonto、Winnti といった攻撃グループについて報告されている。

日本国内を標的とした新たな攻撃者グループによる活動では、2022 年 6 月に日本の組織を対象とした攻撃 Operation MINAZUKI がセキュリティベンダにより報告されている[6]。2019 年ごろから日本組織の子会社または関連会社の取引先ネットワークなどのサプライチェーンを経由して侵入し、標的となる日本組織に継続的な攻撃を行っていたとされている。同セキュリティベンダの追加の調査結果によると、標的となったのは電機に関連する組織とされており、Tick と呼ばれる攻撃グループに起因する可能性が示唆されているものの、明確な証拠はないとされている[7]。当隊においても、本攻撃の情報収集に努めており、心当たりのある組織においては、不完全な情報や、古い情報でも構わないので当隊との情報共有にぜひ御協力をいただきたい。

また、日本国外の活動では、2022 年 8 月のペロシ米国下院議長の訪台以降、台湾を狙う数多くのサイバー攻撃が観測されている[8]。セキュリティベンダによると、APT27 を名乗る中国偽旗ハッカー集団「APT27_Attack」は、DDoS 攻撃による台湾政府のウェブサイトのダウンや台湾の大手コンビニや駅構内のデジタルサイネージにペロシ氏を揶揄するメッセージを表示するなどのサイバー攻撃を行っている。また、

[5] 攻撃グループ BlackTech による F5 BIG-IP の脆弱性（CVE-2022-1388）を悪用した攻撃
https://blogs.jpcert.or.jp/ja/2022/09/bigip-exploit.html
[6] 日本組織を狙った新たな標的型攻撃（Operation MINAZUKI）
https://www.lac.co.jp/lacwatch/report/20220630_003037.html
[7] Operation MINAZUKI: underwater invasive espionage
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/slides/VB2022-Operation-MINAZUKI-underwater-invasive-espionage.pdf
[8] サイバーツールと外交政策：中国「APT」偽旗作戦とペロシ米下院議長の台湾訪問
https://blogs.trellix.jp/cyber-tools-and-foreign-policy

台湾関係だけでなく、選挙やサイバー領域での攻撃者像に関わる印象操作活動が英語や繁体字で実施されていたと報じられる[9]など、我が国としても、マルチドメインなサイバー状況把握の重要性をより一層考える契機でもあったといえよう。

オーストラリア、マレーシアを標的とするサイバー攻撃として、偽のニュースサイトを用いた水飲み場攻撃並びにフィッシングメールを用いた、TA423（別名 APT40）と見られる攻撃活動がセキュリティベンダにより報告された[10]。南シナ海のオフショアエネルギープロジェクトに関連する複数の組織や天然ガス、油田探査や風力発電に関わる複数の組織などが攻撃活動の対象であり、資源・エネルギー部門に対する強い関心が伺える。また、台湾の風力発電所に関わるヨーロッパの企業への攻撃も報告されており、我が国の東シナ海沿岸並びに南西諸島などにも攻撃が及んでいないか注視している。

ロシアを標的としたサイバー攻撃については、ロシアによるウクライナ侵攻（2022 年 2 月）を前後して、APT10、Mustang Panda や Tonto による攻撃が報告されている。APT10 と Mustang Panda に関連していると見られる攻撃キャンペーンとして、ロシアの国営防衛企業に対し少なくとも 2021 年 7 月から攻撃が実行され、最新の活動は 2022 年 4 月にセキュリティベンダにより観測されている[11]。この攻撃は、不審なリンクと悪意のあるドキュメントを含むスピアフィッシングメールを起点とし、多層インメモリローダやコンパイラレベルの難読化など高度な分析防止技術が適用された新たなツールが使用されている。また、Tonto に関連していると見られる攻撃キャンペーンとして、ロシアの政府機関に対しフィッシングメールを介して悪意のある RTF 形式の Word 文書ファイル及び Bisonal バックドアを展開する攻撃活動がセキュリティベンダにより確認されている[12]。Tonto は、主に東アジア（日本、韓国、台湾）とロシアを標的にした攻撃グループとして知られているが、直近ではロシアに対する活動が増加しており、どの地域を対象に活動するのか優先度を調整した可能性も指摘されている[13]。

東南アジアのミャンマーを標的とするサイバー攻撃として、報道機関になりすました C2 サーバのドメインや PlugX を使用した Mustang Panda と見られる攻撃活動がセキュリティベンダにより確認されている[14] 。この攻撃キャンペーンは Mustang Panda の攻撃手法と一致しており、無害な実行可能ファイルを使用して、悪意のある DLL ローダーをサイドロードする、PlugX を使用した典型的な攻撃チェーンが確認されている。Mustang Panda は 2022 年 3 月にロシア語のドキュメントを使った攻撃を行っていた可能性も指摘[15]されており、ファイル名には黒竜江省黒河市愛輝区対岸の極東アジア地域ロシア都市ブラゴヴェシチェンスクがキリル文字で使われていた。国境の近接性も踏まえた地政学的見地も含めて、一国だけではなく関連する複数の国を含めた解釈のための情報収集の必要性を感じさせる報告であった。

南アジアのスリランカでは、2022 年 8 月中旬に中国のロケットの打ち上げを追跡する調査船「遠望 5 号」がスリランカ南部のハンバントタ港に停泊と同時期に、Winnti によるスリランカ政府機関を標的としたサイバー攻撃が行われたことがセキュリティベンダにより確認されている[16]。大規模な抗議デモが発生し経済危機に見舞われ、国連によりスリランカの経済危機への人道的な支援が必要だという呼びかけが行われている状況下で、スリランカへの経済支援に関する情報を含む文書に見せかけた ISO イメージがスリランカ政

---

[9] Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance
https://www.mandiant.com/resources/dragonbridge-targets-rare-earths-mining-companies
[10] Rising Tide: Chasing the Currents of Espionage in the South China Sea
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
[11] Twisted Panda: Check Point Research unveils a Chinese APT espionage campaign against Russian state-owned defense institutes
https://blog.checkpoint.com/2022/05/19/twisted-panda-check-point-research-unveils-a-chinese-apt-espionage-campaign-against-russian-state-owned-defense-institutes/
[12] Targets of Interest | Russian Organizations Increasingly Under Attack By Chinese APTs
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
[13] China's Tonto Team increases espionage activities against Russia
https://www.malwarebytes.com/blog/news/2022/07/chinas-tonto-team-increases-espionage-activities-against-russia
[14] Mustang Panda Abuses Legitimate Apps to Target Myanmar Based Victims
https://blogs.blackberry.com/en/2022/10/mustang-panda-abuses-legitimate-apps-to-target-myanmar-based-victims
[15] BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
[16] Winnti APT group docks in Sri Lanka for new campaign
https://www.malwarebytes.com/blog/threat-intelligence/2022/10/winnti-apt-group-docks-in-sri-lanka-for-new-campaign

府機関へ送信されている。この攻撃では C2 サーバに Dropbox が使用された。同セキュリティベンダによると、今回の Dropbox の C2 サーバはこれまでの Winnti では見られなかったものであるが、クラウドサービスを悪意のある目的に使用することが攻撃者グループ間でより一般的になってきていることが伺える。なお、このキャンペーンが特定された後、C2 サーバとして使用されていた Dropbox のアカウントは、直ちに無効化されている。

3.2 ロシアに関係するサイバー攻撃グループ

ロシアによるウクライナ侵攻に関し、サイバー攻撃とともにウクライナ国民の士気低下やウクライナと同盟諸国との分断を意図した偽情報工作がロシアに関係するサイバー攻撃グループにより実施されたとセキュリティベンダによって分析されている[17]。また、SNS を使用してウクライナとウクライナ難民を批判し、西側諸国の対ロシア制裁は効果がないと主張する組織的なインフルエンスオペレーションが継続されている [18]。これらの情報工作には AI によるディープフェイクも用いられており、ウクライナのゼレンスキー大統領がロシアに降伏を表明するフェイク動画の流布も行われている。

2022 年 5 月頃から主にドイツを標的にヨーロッパで活動しているとされる Doppelganger と呼称されるフェイクニュース記事のキャンペーンでは、既存のニュースメディアに似せたドメインを使用し、デザインやクレジットを複製した偽のニュースサイトが作成され、さらに SNS を使用してフェイクニュースの拡散まで行われていた[19] [20]。本キャンペーンを分析したテクニカルレポート[21]では、2022 年 6 月から 3 か月の間に、フェイクニュースを広めるために少なくとも 50 のウェブサイトが作成されており、インフラストラクチャ署名、コンテンツのメタデータ、SSL 証明書の履歴データの分析を含むフォレンジック情報から、すべてのウェブサイトが同一の攻撃者によって調整された方法で運営されていることが強く示唆されている。

ロシア軍によるウクライナ侵攻にともなうウクライナへのサイバー攻撃に関連し、日本を含む 42 カ国 128 組織に対するネットワーク侵入とスパイ活動が報告されている[22]。政府機関、非政府組織（NGO）、シンクタンク、民間人への援助や難民支援に関与する人道支援団体、防衛、エネルギーに関連する企業を対象とした攻撃において、3 割弱の割合で侵入に成功し、さらにその 4 分の 1 で情報流出につながったとされている。

以下、ロシアに関係する攻撃グループごとにウクライナ侵攻にともなうサイバー攻撃を数点取り上げる。

Sandworm（別名 Voodoo Bear、Iridium）は、CVE-2022-30190 脆弱性を悪用してウクライナ政府のメールサーバを侵害し、ラジオ局、新聞や通信社などのウクライナ報道機関へマルウェア添付したメールを大量配布する攻撃を行った[23]。悪用された脆弱性は「Follina」とも呼称され 2022 年 5 月にマイクロソフトが Microsoft Support Diagnostic Tool（MSDT）に存在するリモートコード実行の脆弱性として公開したものである。

APT28（別名 Fancy Bear、Strontium）は、メディアを含むウクライナ組織、外交政策に関与する米国及び EU の政府機関、シンクタンクを対象としたフィッシングキャンペーンを 2016 年以降継続して実施している

---

[17] IO の攻勢：ロシアのウクライナ侵攻をめぐる情報操作活動
https://www.mandiant.jp/resources/information-operations-surrounding-ukraine
[18] Removing Coordinated Inauthentic Behavior From China and Russia
https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/
[19] Doppelganger – Media clones serving Russian propaganda
https://www.disinfo.eu/doppelganger
[20] Massenweise falsche News-Seiten enttarnt
https://www.zdf.de/nachrichten/politik/desinformation-kampagne-facebook-ukraine-krieg-russland-100.html
[21] UNDER THE HOOD OF A DOPPELGÄNGER
https://www.qurium.org/alerts/under-the-hood-of-a-doppelganger/
[22] Defending Ukraine: Early Lessons from the Cyber War
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
[23] а с о в а н а к і б е р а т а к а н а м е д і й н і о р г а н і з а ц і ї У к р а ї н и з в и к о р и с т а н н я м ш к і д л и в о ї п р о г р а м и CrescentImp (CERT-UA#4797)
https://cert.gov.ua/article/160530

[24]。また、ブラウザから保存されたパスワードを窃取する新たなマルウェアを使用した攻撃[25]や、脆弱性「Follina」を悪用した攻撃[26]も行っている。

APT29（別名 Cozy Bear、Nobelium）は、複数の国の外交、大使館関係者を対象とする攻撃キャンペーンを継続して実施している[27]。この攻撃では行政組織からの通知を詐称したスピアフィッシングメールが用いられ、Dropbox や Google Drive といったクラウドストレージサービスにペイロードを配置することで悪意のある通信の検出を難しくしていることが特徴である。最終的に被害者の PC には CobaltStrike が設置され、遠隔操作可能な状態となる。さらに別のキャンペーンとして、米国国務省の広報担当者を詐称したスピアフィッシングメールを使用し、シンクタンク、法執行機関、メディア、米軍、画像、運輸、製薬、政府、防衛請負分野を対象とした攻撃も報告されている[28]。こちらも最終的に被害者の PC には CobaltStrike が設置される。

また、APT29 は Active Directory Federated Service（AD FS）サーバの正規 DLL を悪意のある DLL（MagicWeb バックドアを含む）に置き換える攻撃方法を使用している[29]。この攻撃は、米国、ヨーロッパ、中央アジアの政府機関、NGO、政府間組織（IGO）、及びシンクタンクを対象に行われた。なお、この攻撃方法は被害者のネットワークに一度侵入した後にアクセスを維持するための方法であり、最初の侵入は別途何らかの方法で行う必要がある。

Seaborgium（別名 Callisto Group、Coldriver）は、主に NATO 諸国を中心に、その他バルト諸国、北欧、東欧を含む防衛、諜報コンサルティング会社、NGO、IGO に対して情報窃取を目的とした攻撃を行っている[30]。この攻撃では長期にわたるソーシャルエンジニアリングにより攻撃対象との関係を築き、最終的にメールで送信したリンクからダウンロードさせたマルウェアにより資格情報を窃取している。さらに窃取した資格情報を使用して攻撃対象のメールアカウントにサインインし、メールの窃取や転送設定を行うなどにより長期間にわたり情報を窃取している。

2022 年 9 月初頭に Killnet が日本の省庁や民間企業のウェブサイトへ DDoS 攻撃を行い、SNS に犯行声明を投稿した[31]。この攻撃グループでは当初は DDoS 攻撃の活動が目立っていたが、Chaos Ransomware を改変した Killnet Ransomware を使用した攻撃も報告されている[32]。Killnet は親ロシアの活動家集団、いわゆるハクティビストに分類される攻撃グループであり、国家の支援を受けた高い技術を持つ APT 攻撃グループではないと考えられている[33]。しかし、戦時におけるサイバー犯罪やハクティビストの活動は、国家放任型サイバー攻撃とも考えられるため、平時においても攻撃懸念国における国家支援型のサイバー活動とあわせ把握する必要性を、あらためて考えさせる事象となった。特に、従来のプロパガンダや軍事欺瞞（マスキロフカ）がどのようにサイバー観点で実現されているか、西側諸国がハイブリッド戦と呼ぶ行動原理とあわせ、歴史的考察をする必要があるが、そのためにもサイバー攻撃だけでなく、物理領域や認知領域の活動における事実の収集を、情報の揮発前に行う必要があることが容易に推測できるであろう。

---

[24] Disrupting cyberattacks targeting Ukraine
https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/
[25] Update on cyber activity in Eastern Europe
https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
[26] Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine
https://blog.malwarebytes.com/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine/
[27] Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
[28] Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign
https://www.mandiant.com/resources/blog/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign
[29] MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone
https://www.microsoft.com/en-us/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/
[30] Disrupting SEABORGIUM's ongoing phishing operations
https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/
[31] 政府運営「e-Gov」などにサイバー攻撃か ロシア支持のハッカー集団「KILLNET」が声明 mixi や JCB への攻撃にも言及
https://www.itmedia.co.jp/news/articles/2209/06/news174.html
[32] Pro-Russian Hacktivists Targeting Adversaries With Killnet Ransomware
https://blog.cyble.com/2022/11/08/pro-russian-hacktivists-targeting-adversaries-with-killnet-ransomware/
[33] KillNet: Who, What, Where, Why, How
https://warnerchad.medium.com/killnet-who-what-where-why-how-971eee52a7c5

3.3 北朝鮮に関係するサイバー攻撃グループ

2022 年 10 月 14 日、金融庁、警察庁、内閣サイバーセキュリティセンターの連名で、北朝鮮のサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について注意喚起が行われた[34]。日本の暗号資産関連事業者に対し、幹部を詐称したフィッシングメールや虚偽 SNS アカウントを用いたソーシャルエンジニアリングにより従業員に接近し、マルウェアをダウンロード、感染させる手口で、最終的には暗号資産を窃取することを目的とした攻撃が続いているとしている。この注意喚起で参照している国連安全保障理事会北朝鮮制裁委員会専門家パネルの中間報告書では、北朝鮮の朝鮮人民軍偵察総局に所属する攻撃者グループとして Kimsuky、Lazarus Group、BlueNoroff、Stonefly の 4 グループに言及しており、これらの攻撃グループは制裁の影響から逃れ、北朝鮮にとって価値ある情報を不正に窃取し、金銭を獲得するためにサイバー攻撃を行っていると指摘している[35]。

Kimsuky（別名 Velvet Chollima）の関与が疑われる活動として、2022 年 8 月、瀋陽ロシア総領事館アカウントを使用して、在日本のロシア大使館を標的とした攻撃が観測されている[36]。同キャンペーンでは、メールで大使館会計課を偽装して、資金振替のための大使館情報を送信するという内容とともに、悪意あるファイルを添付して行われた。なお、この攻撃は Konni（別名 APT37、Ricochet Chollima、Group123）が実行したとするレポート[37]や、Kimsuky と Konni には関連がある可能性が高いとの主張[38]がある点は気に留めておく必要があろう。

Lazarus（別名 Labyrinth Chollima、Hidden Cobra）の関与が疑われる活動として、2022 年 2 月～7 月頃、日本の組織をはじめ、カナダ、米国を含む世界中のエネルギープロバイダーを標的とした攻撃が観測されている[39]。このキャンペーンでは、VMWare Horizon の脆弱性を悪用し、標的先への侵入の足がかりを確立した後、同攻撃グループのカスタムマルウェアインプラントを展開したと報告されている。本攻撃の目的は、世界中の組織に侵入して長期的なアクセスを確立し、北朝鮮国家が関心のある情報を盗み出すこととされており、今後も注視する必要性が高いとしている。

さらに Lazarus の活動として、日本の金融機関の採用情報をおとり文書とした攻撃について報告されている[40]。Lazarus は以前から偽の求人を攻撃の手口にしており、ソーシャルエンジニアリングで攻撃対象の信用を得てからマルウェア配布を行うこともある。今回報告された攻撃では、アンチウイルスソフトによる検知を回避するため仮想ハードディスク（VHD ファイル）形式でマルウェアを配布し、マルウェア感染時に複数のアンチウイルスソフトを無効化することが特徴である。また、同様に求人を手口とする Operation DreamJob に続く攻撃キャンペーンとして、オランダの航空宇宙会社とベルギーの報道機関の従業員を標的とした攻撃が報告されている[41]。この攻撃では、最初に LinkedIn でメッセージやり取りを行った後に、メールで悪意のあるドキュメントが送付された。ドキュメントは Amazon のロゴが入った白紙であったが、サーバからのコンテンツダウンロードに成功していた場合は、白紙部分には Amazon の宇宙計画 Project Kuiper の求人情報が表示された可能性がある。

Lazarus のサブグループとされる BlueNoroff（別名 APT38、Stardust Chollima）の関与が疑われる別の

---

[34]「北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）」の公表について
https://www.fsa.go.jp/news/r4/sonota/20221014/20221014.html
[35] Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)
https://undocs.org/S/2022/668
[36] 김수키(Kimsuky) 그룹, 러시아 외무부를 타겟으로 공격 진행중!
https://blog.alyac.co.kr/4892
[37] Meeting the "Ministrer
https://www.fortinet.com/blog/threat-research/konni-rat-phishing-email-deploying-malware
[38] [스페셜 리포트] APT 캠페인 'Konni' & 'Thallium(Kimsuky)' 조직의 공통점 발견
https://blog.alyac.co.kr/2347
[39] Lazarus and the tale of three RATs
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
[40] 求职陷阱：Lazarus 组织以日本瑞穗銀行等招聘信息为诱饵的攻击活动分析
https://www.secrss.com/articles/49506
[41] Amazon-themed campaigns of Lazarus in the Netherlands and Belgium
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

攻撃では、日本を含む世界各国の金融機関を詐称し、詐称した組織の公式サイトに類似したドメインを取得してソーシャルエンジニアリングを行う攻撃が報告されている[42][43]。この攻撃はマルウェアに感染させた後にユーザのプロファイルを取得し、暗号通貨を扱うユーザであった場合はブラウザ拡張機能のソフトウェアウォレットを侵害、最終的には暗号通貨の送金トランザクションを改ざんすることで暗号通貨を窃取することを目的としている。

別の Lazarus サブグループとされる Andariel（別名 Silent Chollima、Stonefly）の関与が疑われる攻撃として、Dtrack マルウェアと Maui ランサムウェアを用いた攻撃について報告されている[44]。この攻撃ではロシア、インド、ベトナムの企業とともに日本の住宅会社が 2021 年 4 月にランサムウェア被害に遭ったとされており、インターネットに接続された脆弱なサーバが攻撃の起点になったと想定されている。

2022 年 3 月に開始された、株式及び暗号通貨の投資家を対象とした、非常に活発なキャンペーンが発見されたと報告されている[45]。このキャンペーンでは Konni グループの関与が疑われており、暗号通貨関連のコンテンツと法執行機関からの苦情をテーマとした悪意のある文書を使用して、被害者の環境にマルウェアを展開したとされている。ステートスポンサードな APT 攻撃グループが金銭的利益を追求することは珍しいが、その傾向は益々強まっているとされている。

3.4 その他リージョンに関係するサイバー攻撃グループ

本項で紹介する事例は、当隊の注目したトピックの一部である。これらのリージョンで活動する日本企業は直接、または間接的に影響を受ける可能性がありうる。各地における脅威認識のあり方や、参考情報などをお持ちであれば、是非当隊との意見交換などを通じてサイバー状況把握に協力頂きたい。

3.4.1 イラン

イランが関与するとみられる APT 攻撃グループとして、APT35、APT42、MuddyWater、APT34 の活動が報告されている。当隊が特に着目したイベントとして、2022 年 9 月、米国財務省の外国資産管理局（OFAC）が、ランサムウェア攻撃に関与したとして、イランのイスラム革命防衛隊（IRGC）に所属する個人や組織に制裁を発表している[46]。同報告によると、APT35 は世界中の組織や関係者に対して大規模なキャンペーンを展開しており、特に米国や中東の防衛、外交、政府関係者、メディア、エネルギー、ビジネスサービス、テレコミュニケーションなどの民間企業が標的とされている。

また、APT42 も IRGC と関係があることがセキュリティベンダにより報告されている[47]。この報告では、APT35 と APT42 には共通するサブグループ UNC2448 が存在し、IRGC の情報機関に代わってサイバー活動を行っていると指摘している。APT42 は 2022 年 9 月にソーシャルエンジニアリングとフィッシングにより中東地域を対象とするジャーナリスト、研究者、外交官、政治家の資格情報を窃取し、機密情報や連絡先にアクセスしたことが被害組織により報告されている[48]。

イランの情報省（MOIS）の下部組織とされる MuddyWater（別名 Static Kitten）による、中央アジア、中東などのイラン周辺国を対象とした攻撃キャンペーンが 2022 年 9 月から実施されていたことがセキュリティベンダにより報告されている[49]。この攻撃グループは一般に流通する正規のリモート管理ツールを攻撃に

[42] The BlueNoroff cryptocurrency hunt is still on
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
[43] Talent Need Not Apply
https://i.blackhat.com/USA-22/Thursday/US-22-Wikoff-Talent-Need-Not-Apply.pdf
[44] Andariel deploys DTrack and Maui ransomware
https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/
[45] APT trends report Q2 2022
https://securelist.com/apt-trends-report-q2-2022/106995/
[46] Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity
https://home.treasury.gov/news/press-releases/jy0948
[47] APT42: Crooked Charms, Cons and Compromises
https://www.mandiant.com/resources/reports/apt42-spear-phishing-and-surveillance
[48] Iran: State-Backed Hacking of Activists, Journalists, Politicians Ongoing Phishing Campaign Imperils Independent Groups
https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians
[49] New MuddyWater Threat: Old Kitten; New Tricks
https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks

使用しており、以前の攻撃では RemoteUtilities や ScreenConnect を使用していたが、今回新たにマネージドサービスプロバイダ向けの管理ツールである Syncro を使用したことが確認されている。

APT34（別名 OilRig、Helix Kitten）は、2022 年 4 月にヨルダン政府関係者に対して悪意のあるファイルを添付したスピアフィッシングメールを送付する攻撃を行っていたことがセキュリティベンダにより報告されている[50]。この攻撃では、送付された Excel のマクロを実行すると Saitama バックドアに感染する。Saitama バックドアは C2 サーバと DNS 通信を使用して交信し、また通信待ち時間を細かく制御し不要な通信をできるだけ行わないようにするなど感染の発覚を遅らせるための工夫が施されている。なお、バックドアの PDB パスに残されたプロジェクト名から Saitama と名付けられているが、バックドア作者がどのような理由で埼玉と名付けたのかは不明である。

2022 年 9 月、アルバニア政府はイランから政府機関に対するサイバー攻撃を受けたことを理由に、イランとの国交を断絶し、イランの外交官と大使館職員に国外退去を命じたと発表した[51]。本件はサイバー攻撃を理由とした国交断絶の初の事例である[52]。

3.4.2 インド

インドが関与するとみられる APT 攻撃グループとして、Patchwork（別名 Viceroy Tiger, Hangover, White Elephant）の活動が報告されている。2022 年 9 月のセキュリティベンダの報告によると、最近の Patchwork の活動として、「パキスタン国防省」からのものであると主張する文書を使用したテンプレートインジェクション攻撃を行ったと指摘されている[53]。また、Patchwork の関連組織と考えられる Confucius が、2022 年 5 月から 6 月にかけてパキスタン首相官邸、パキスタン外務省に対し立て続けにスピアフィッシングメールで攻撃したことが報告されている[54]。地政学的見地を踏まえたインドとパキスタン、中国の対立関係がサイバー攻撃の背景にあることを意識しておく必要があるだろう。

3.4.3 パキスタン

パキスタンが関与するとみられる APT 攻撃グループ APT36（別名 Mythic Leopard, Transparent Tribe）は、2021 年 6 月以降、インドの安全保障及び軍関係者を標的とする継続的な活動を実施していると報じられており、攻撃手口として、正規組織やファイル共有サービスの偽装ウェブサイトを使用し、ソーシャルエンジニアリングに注力している点が挙げられている。2022 年 7 月に米国のセキュリティベンダが公表したレポートでは、インドの教育機関を標的としたフィッシングキャンペーンは APT36 によるものと指摘されている[55]。

また、2022 年 8 月には、米国のベンダーが SNS を利用したマルウェアの配布によるスパイ活動に対して対策を講じたと発表しており、最近の攻撃では、アフガニスタン、インド、パキスタン、UAE、サウジアラビアの軍関係者、政府関係者、人権団体、非営利団体の職員、学生などあらゆる分野がターゲットとして混在していると指摘されている[56]。

3.4.4 ベトナム

ベトナムが関与するとされる攻撃グループ Ocean Lotus（別名 APT32、海莲花、APT-C-00、APT-Q-31）

---

[50] APT34 targets Jordan Government using new Saitama backdoor
https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/
[51] Videomessage of Prime Minister Edi Rama
https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/
[52] Albania cuts diplomatic ties with Iran over July cyberattack
https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a
[53] Isolation: A vaccine for template injection attacks
https://www.menlosecurity.com/blog/isolation-a-vaccine-for-template-injection-attacks/
[54] Confucius：隐藏在 CloudFlare 下的垂钓者
https://www.antiy.cn/research/notice&report/research_report/20220713.html
[55] Transparent Tribe begins targeting education sector in latest campaign
https://blog.talosintelligence.com/transparent-tribe-targets-education/
[56] Meta's Adversarial Threat Report, Second Quarter 2022
https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/

は、2012 年頃より近隣諸国や米国等を標的として活動していると指摘されている。セキュリティベンダの報告によると、2022 年 5 月から 7 月にかけて中国の製造会社を対象に研究資料や技術的成果といった機密情報や重要文書の窃取を狙った攻撃が行われたと指摘されている[57]。この攻撃では、Ocean Lotus 独自のツールとして RemyRAT と呼ばれるリモート操作ツールが使用されたことが特徴である。

APT32 以外の活動としては、2022 年 7 月にセキュリティベンダが公表したレポートによると、ベトナムのサイバー攻撃者 DUCKTAIL によるビジネスアカウントを利用する個人、企業を対象とした金銭目的の活動が報告されている[58]。

3.4.5 中南米

主に中南米で活動しているスペイン語話者の APT 攻撃グループ El Machete（別名 APT-C-43）は、2010 年頃より、ニカラグア及びベネズエラの政府・金融部門を主な標的として活動していると指摘されている。本報告期間中、セキュリティベンダ等からの同グループの活動に関する公開情報は確認していない。

3.4.6 トルコ

トルコが関与するとされる攻撃グループとして TA482 の活動が報告されている。2022 年初頭から米国のジャーナリストやメディア組織のソーシャルメディアアカウントを標的とした継続的な活動を実施していると報じられており[59]、2023 年に行われるトルコの選挙が近づくにつれ、攻撃が活発化する可能性が指摘されている。

4 活動を通しての所感

2022 年上半期には、ロシアによるウクライナ侵略、北朝鮮による極めて高い頻度による弾道ミサイルの発射、ペロシ米国下院議長の台湾訪問といった、我が国並びに国際情勢に影響の大きい事象が突発してきた状況下で、我が国に対する国家支援型と推定されるサイバー活動は継続的に発生している。数年単位で継続している攻撃もあり、このような長期にわたる持続的な脅威の継続（APT）の背後には、国家による関与又は国家による何らかの支援があるものと疑われる。当隊はそのような攻撃の状況把握とともに、適正な対策につなげるためにも、攻撃主体の目的や意図に対する見解の理解を得るべくサイバーセキュリティの観点にとどまらないあらゆる情報の収集に努めている。

中国では、中国共産党第 20 期中央委員会において習近平国家主席が引き続き3期目の総書記に選任された。共産党新人事では、公安・司法部門を統括する中央政法委員会書記に前国家安全部部長が、新国家安全部部長には前中央政法委員会秘書長がそれぞれ就任しており、従来の「強国」路線は継続するとの見方がある[60]。さらに、中央軍事委員会副主席に台湾や日本に対応する東部戦区の司令官が抜擢され、台湾への軍事面、心理面での圧力はより強硬になるとの見通しもある[61]。また、2024 年に相次いで行われる予定の台湾総統選挙、米国大統領選挙では、これまで以上に情報操作、ディスインフォメーションなどの心理戦も激しくなると指摘されている[62]。こうした状況下で、中国では産官学軍が連携してサイバーセキュリティの技術研究、要員育成の取り組みが進められ、サイバー攻撃、防御ともに能力を大きく向上させていると指摘されている [63]。

---

[57] APT32 组织针对我国关基单位攻击活动分析
http://www.ctfiot.com/52152.html
[58] ウィズセキュア、Facebook ビジネスアカウントから情報を盗むインフォスティーラー型マルウェア『DUCKTAIL』を発見
https://www.withsecure.com/jp-ja/whats-new/pressroom/20220726-ducktail
[59] ジャーナリストの仕事用メール アカウントを標的にする
https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists
[60] 「強国」路線を継続する中国 ― 3 期目を始動させた習近平指導部が直面する課題 ―
https://www.mizuho-rt.co.jp/publication/report/2022/pdf/insight-as221102.pdf
[61] Taiwan Braces for 'Grim' Times After China's Xi Extends Power
https://jp.wsj.com/articles/taiwan-braces-for-grim-times-after-chinas-xi-extends-power-11666924930
[62] 習近平 3 期目の「台湾政策」：強化される軍事圧力と「心理戦」必要な 2024 年問題の「危機管理」
https://www.nippon.com/ja/in-depth/a08501/
[63] Downrange: A Survey of China's Cyber Ranges
https://cset.georgetown.edu/publication/downrange-a-survey-of-chinas-cyber-ranges/

以上のように、国家の関与が疑われるサイバー攻撃によるリスクがグローバルレベルで顕在化している状況を踏まえれば、日本においても、サイバーセキュリティ能力の向上と人材育成を、価値観を共有する同盟国・有志国とともに進めていく必要があろう。日本の NATO CCDCOE への正式参加[64]、並びに CCDCOE 主催のサイバー防衛演習 Locked Shields への官民での継続参加[65]はその一環と言えるものであり、引き続きこのような取り組みが推進されることを期待したい。

当隊としては、サイバー空間における安心・安全実現の観点において、国家支援型と推測されるサイバーエスピオナージへの対応に加え、その関連領域としての認知領域作戦、国家放任型と推測されるサイバークライム活動や有事を中心としたハクティビストの概況を含めた幅広い脅威情報の収集及び情報提供などの活動を引き続き進めていき、国家レベルでのサイバー領域における状況把握（サイバードメインアウェアネス）を高めることに努めていく所存である。

技術的観点として、ネットワーク貫通型攻撃に対する備えの重要性へも継続的な対応が必要である。ネットワーク貫通型攻撃は、APT だけではなくランサムウェアの侵入口や、興味本位のいたずらレベルでも悪用されるものであり、インターネット接続状況（アタックサーフェイス）の把握を確実に実行し、そのリスク判断と脆弱性情報などを活用した適切な対処が求められる。特に 2024 年 1 月に ISDN 回線が終了すると、いくつかの接続ではインターネットを専用線として使う Internet-VPN を採用するケースもでてくると考えられる。このようなケースではウェブ閲覧やメール、ソーシャルネットサービスなどは使っていないためインターネットを利用している自覚に至らず、アタックサーフェイスの把握が難しいかもしれないが、たとえ VPN を通すとしてもインターネットに接続する以上、リスク判断と適切な対処は不可欠である。ネットワーク貫通型のリスクについては、今回記載した事例も踏まえ、システム管理や権限把握の及ばないアタックサーフェイスがないか、今一度見直していただきたいと考えている。特に、クローズドシステム、スタンドアローンとされるシステムについては、念を押すようにインターネット接続の有無と、接続状況の確認を再度実施することを強く提案したい。

関係者の皆様には本稿をご活用いただくとともに、当隊の活動改善のためのご指摘やご教示をいただければ幸甚である。

[64] Japan Ministry of Defense/Self-Defense Forces
https://twitter.com/ModJapan_en/status/1588467077043875842
[65] Locked Shields 2022 参加記
https://blogs.jpcert.or.jp/ja/2022/05/locked-shields-2022.html

サイバーレスキュー隊（J-CRAT）活動状況［2022 年度上半期］
https://www.ipa.go.jp/security/J-CRAT/index.html

2022 年 12 月 28 日
独立行政法人情報処理推進機構

https://www.ipa.go.jp/