サイバーレスキュー隊（J-CRAT） 活動状況
[2021 年度上半期]

2021 年 11 月 26 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、相談対応やレスキュー活動及び情報収集を行っている。

本報告の期間におけるレスキュー活動や情報共有活動、公開情報の収集、サイバースレットインテリジェンスの活用等を通したサイバー状況把握の結果、従来の標的型攻撃メールやネットワーク貫通型攻撃に加え、クラウドサービスやVPNの認証情報窃取を目的としたクレデンシャルフィッシング（データエントリー型フィッシング）、組織ネットワーク境界装置に対するスキャンを標的型サイバー攻撃の初期活動として観測している。

なお、この期間には東京 2020 オリンピック競技大会（第 32 回オリンピック競技大会）、東京 2020 パラリンピック競技大会の開催もあったが、各方面での報道にみられるように、わが国に対する明らかに国家支援型とみられるサイバー攻撃は当隊でも認識していない。

本活動報告で紹介するサイバー状況の報告が、各組織及び個人に対するサイバー諜報活動に対する理解の一助となり、対抗策としての政府による利活用を前提とした情報共有の促進、ひいてはわ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　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

	2018 年度	2019 年度	2020 年度	2021 年度 上半期
相談・情報提供	413	392	406	128
リモートレスキュー	127	139	102	38
オンサイトレスキュー	31	20	17	3

※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

今年度上半期に「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 **128 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 **38 件**、うち**オンサイト支援**を行った事案数は **3 件**であった。

2　2021 年度上半期の活動を通じてみられた特徴的な事項

2020 年度上半期の当隊活動状況報告でも述べているように、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、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、本報告期間の活動を通して観測したサイバーエス

[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。

ピオナージの特徴をいくつか述べ、最後に認知領域作戦（インフルエンスオペレーション）[2]として考えるべき事案について述べる。

2.1 継続する中国に関係するサイバー攻撃グループの活動

2.1.1 APT10 とみられる活動

LODEINFO と呼ばれる諜報用マルウェアを用いた攻撃が 2019 年 12 月以来継続しており、本報告期間中も断続的に観測された。同一種のマルウェアを用いた攻撃キャンペーンの観測期間としては、当隊の発足以来、最長を記録するもののひとつとなっている。標的とされる分野（安全保障、国際政治、外交、メディア）、感染の手口（主に時事をテーマとする標的型攻撃メール。侵害された標的の関係者が連鎖的な攻撃を受ける。）に変化はみられておらず、マルウェアの小規模な改変も続いている。

本事案に関与していると考えられる攻撃グループは、以前から変わらずわが国の政策や安全保障分野への執着心が特に強い。通信インフラ、使用ツールといった各種インディケータは APT10 と一致している。

2.1.2 BlackTech とみられる活動

2021 年 6 月、国内企業の海外拠点を狙った標的型攻撃メールの存在を公開情報において確認した。攻撃メールは関連会社を装い、業務に関係する資料を送付する旨の簡素な文面と、マルウェアを含むドキュメントファイルが添付されたものである。添付ファイルを分析した結果、用いられたマルウェアは 2020 年 10 月に国内組織を狙った攻撃でも観測していた種別であることが判明した。

これらの攻撃で使用された通信先、攻撃手口、囮ファイル等には従来の BlackTech の攻撃インフラとの共通点がみられることから、当隊では同攻撃グループが何らかの関与をしているとみている。本件についてはセキュリティベンダからも分析報告が挙がっている[3]。

また、攻撃に用いられた通信インフラの調査からは、国内の政党、行政機関、学術組織等を偽装した完全修飾ドメインが多数発見されている。当隊では本報告書の公表時点までにこれらのインフラを用いた攻撃を観測していないものの、広範囲を標的とする攻撃に発展する可能性を警戒し、動向を注視している。

その他、国内の報道機関によると[4]、2021 年 5 月に発覚した国内のシステムエンジニア向けクラウドシステムに対する侵害における不正アクセスの手段から BlackTech の関与が示唆されると報じられている。当隊では本件の状況把握に努めているものの、具体的な情報が得られていない。関連する情報を持つ組織におかれては、どのような断片情報であっても、是非当隊との情報共有をお願いする。

2.1.3 A41APT と呼ばれる攻撃グループの活動

先期の当隊活動状況報告で報告した、国内の複数企業を標的としたネットワーク貫通型の攻撃を行う攻撃グループは、一部のセキュリティベンダに A41APT と呼ばれている。当隊では、2021 年 9 月に同攻撃グループとの関与が疑われるツールが発見された、という断片的な情報を得ていることを除き、本報告期間の活動について具体的な情報を得られていない。

ネットワーク境界に設置された装置からの侵入事例に関する経験、痕跡情報を有する組織においては、サイバー状況把握のため、粒度、精度、時期を問わず、当隊との情報共有をお願いしたい。

2.2 北朝鮮に関係した攻撃

2021 年 5 月から 7 月にかけて、朝鮮半島に関係の深く、安全保障やメディアに従事する複数の人物を標

---

[2] インフルエンスオペレーションは認知領域における作戦の一つの手段とされる。
Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations
https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/

[3] 標的型攻撃グループ BlackTech が使用するマルウェア Flagpro について
https://insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro

[4] Hackers sought government data on nuclear plants, Olympics
https://www.asahi.com/ajw/articles/14430219

的として同時に配信される標的型攻撃メールを複数回観測した。攻撃メールは何れも国内の北朝鮮有識者を詐称し、朝鮮半島情勢に関するテーマが用いられていた。本文中に記載された正規のニュースサイトを連想させる URL リンクから偽のログイン画面へ誘導し、認証情報を窃取することを目的としたフィッシングメールである。

2021 年 8 月には、5 月の標的型攻撃メールと類似の手口で、URL リンクではなくマルウェアを内包するドキュメントファイルが添付された標的型攻撃メールを観測した。分析の結果、このマルウェアは北朝鮮に関連する攻撃グループが使用すると報告されている遠隔操作ツール[5]に一致する点が多くみられた。

従来、国内で観測される北朝鮮に関係した標的型攻撃メールは極めて少数の専門家を標的としていたことから、本事案が攻撃側の戦略転換を示している可能性も考慮し、警戒している。

さらに、先期から引き続き、わが国の安全保障や北朝鮮関係の有識者に対する執拗なフィッシングメール攻撃が継続している。攻撃メールのテーマにはプロバイダからの通知が用いられる点に変化がみられない一方、送信元やリンク先に侵害されたサーバが用いられるケースが新たに観測されている。この微細な変化の目的は、不審通信先のフィルタリング回避、帰属特定の困難化、新しい戦術のテスト、等の可能性が考えられるものの、推測の域を出ない。

上述の一連の攻撃で使われたツールやインフラをサイバースレットインテリジェンスの観点で分析すると、全ての攻撃に関連があり、特定国からのステートスポンサード攻撃と推察可能なものもあるが、サイバー以外の領域も含めた情報活動全体の把握が不十分であるため、先期に引き続き当隊では、現時点での判断は難しいと考えている。

2.3 日本語話者を標的とするインフルエンスオペレーション

2021 年 9 月、台湾のセキュリティ業界、及び台湾政府の信用を損なうことを目的としたとみられる記事が、複数のサイトに投稿されたことを観測した[6]。記事の内容は、『台湾のマルウェア調査会社が日本国内の企業に対しフィッシング攻撃を行っており、台湾政府の関与が疑われる』という主旨が日本語で記載されたものである。

この記事は、簡体字を扱うコンテンツファームの管理組織が所有するとみられる複数のブログやニュースサイトを通じて投稿された他、数日中にインターネット百科事典や国内向けの匿名掲示板にも投稿された。その後、日本及び台湾の一部のコミュニティサイトでは、記事の内容や信ぴょう性に関する議論が散発的に行われたものの、一般利用者の管理するウェブサイトや SNS への拡散は観測されていない。

本件は、日本人の台湾へ向けた不信感を煽り、結果として両国の関係悪化を狙ったものとも考えられることから、当隊ではステートスポンサードによる認知領域作戦である可能性を排除せずに動向を追跡している。今回投稿された記事の文面には文法誤りや簡体字の混在等の不自然な点が複数含まれており、その不備を指摘して偽情報を疑う議論も散見された。

なお、2021 年 4 月には、台湾政府が『福島第一原発の汚染水を台湾政府が引き受ける』という内容の、虚偽の公式文書に関する注意喚起を発表しており[7]、同じく両国の関係悪化を狙ったものとも考えられる。わが国に対する認知領域作戦は発展途上にあり、経過とともにより巧妙に進化し続けていく恐れがある。情報の受け手には、未知のソースからのメッセージを受けた際に、そのメッセージの背後の意図を疑い、虚実を判断するリテラシーが求められている。

一般に、ステートスポンサードによる認知領域作戦では、目に見える形での情報の拡散だけでなく、無意識の領域への刷り込みが行われるといった分析もあるため、以後、国家間の関係に何らかの印象を与える

---

[5] Kimsuky が利用している KGH スパイウェアスイートの内部解析
https://www.cybereason.co.jp/blog/cyberattack/5373/

[6] 中國認知作戰新手法！鎖定臺灣資安公司製造假新聞，挑撥臺日政府關係
https://www.ithome.com.tw/news/146834

[7] facebook 蔡英文 Tsai Ing-wen 4 月 15 日
https://www.facebook.com/tsaiingwen/posts/10157418821221065

ような情報の発言や拡散をインディケータの枠組みで扱うべきか、どのような扱いが可能かといった論点でも着目していく。

3 わが国を取り巻くサイバー攻撃グループ

当隊では、わが国に対するサイバーエスピオナージにつながる恐れのある攻撃グループの動向を把握することを重要と考え、ステートスポンサードとされるさまざまな攻撃グループの情報を集めてサイバー状況把握へ活用することを検討している。本項では、本報告期間の情報収集を通じてみられた特徴的な動向の一部を紹介する。

3.1 中国に関係するサイバー攻撃グループ

2021 年 7 月 19 日、米国政府は 2021 年 1 月以降に行われた Microsoft Exchange サーバの脆弱性を悪用した活動を正式に中国に帰属させるとともに [8]、中国政府が不正な活動を行うハッカーと契約していること、及び中国国家安全部に関与するハッカーが金銭的利益を目的とした不正な活動を世界中で行っていることについて声明を発表した。同日、カナダ、EU、NATO、英国、豪州、ニュージーランド、及びわが国は「悪意あるサイバー活動は看過できない」旨の声明を発表している[9]。対して、翌日、中国外務省や各国の中国大使館は事実無根の中傷に反対する主旨を表明している。

2021 年 10 月、国内外のセキュリティベンダより BlackTech と呼ばれる攻撃グループによる標的型サイバー攻撃キャンペーンが報告されている[3]。攻撃は遅くとも 2020 年 10 月頃より開始され、国内の防衛、メディア、通信に関わる企業が標的となったとされている。項番 2.1 で述べたように当隊もその一部に対処しており、全容把握に努めている。

国外を標的とした活動に関しては、2021 年 8 月から 9 月にかけて、複数のセキュリティベンダより APT41 と呼ばれる攻撃グループに関係する攻撃が報告されている[10][11][12]。標的とされた地域として、台湾、東南アジア、インド、ネパールが挙げられている。

その他、2021 年 6 月にセキュリティベンダより公開されたレポートによると、新疆ウイグル地区のウルムチを拠点としている人民解放軍旧蘭州軍区第 2 技術偵察局 69010 部隊が関与するとされる、中央アジア諸国やインドに対するミリタリーインテリジェンス活動が報告されている。その活動の痕跡として東莞信大融合創新研究院（東莞市人民政府と中国人民解放軍戦略支援部隊信息工程大学が設立）のコードサイニング証明書が挙げられるなど、政府・軍の関与が指摘されている。一帯一路や中パ経済回廊に関わる中央アジアから南アジア地域におけるサイバー状況として、その実態の全容把握が期待される。

3.2 ロシアに関係するサイバー攻撃グループ

当隊では本報告期間中、ロシアに関係するサイバー攻撃グループによる、国内での明らかなサイバー諜報活動は把握していない。

セキュリティベンダの公開レポートによると、Strontium (APT28; ロシア連邦軍参謀本部情報総局（通称

---

[8] The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China
https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[9] 中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html

[10] APT41 Resurfaces as Earth Baku With New Cyberespionage Campaign
https://www.trendmicro.com/en_us/research/21/h/apt41-resurfaces-as-earth-baku-with-new-cyberespionage-campaign.html

[11] Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/

[12] Operation 'Harvest': A Deep Dive into a Long-term Campaign
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/

GRU）が関与といわれている）と呼ばれる攻撃グループが 2020 年の夏までに行った、COVID-19 ワクチン開発に関する情報収集活動の標的として、米国や豪州等と並んで日本も追記されている[13]。

その他、本報告期間中にも、ステートスポンサードの攻撃とは認識されていないものの、社会・公共インフラに多大な影響を及ぼすランサムウェア攻撃が世界各国で多発した。Darkside と呼ばれる攻撃グループによる 2021 年 5 月の米国 Colonial Pipeline 社への攻撃、並びに Sodinokibi（別名 Revil）と呼ばれる攻撃グループによるブラジル JBS 社への攻撃は、対象企業の活動を停止させ、ライフラインとなる燃料や食料の供給、市場価格にまで影響を及ぼした。また、Sodinokibi による 2021 年 7 月の米国 Kaseya 社への攻撃では、同社が提供するアウトソーシング用ソフトウェアツールの一部が破壊されたことにより、その顧客である 800～1500 社の会計システム等が停止するなどの影響を及ぼした[14]。これらの攻撃基盤は、ロシア国内に活動拠点を置く犯罪グループが提供するサービス化されたランサムウェア（RaaS）とみられている。

これらの RaaS の中にはロシア語圏を攻撃対象から除外しているものがある。ロシア政府は自国に被害を及ぼさないサイバー犯罪を取り締まらない傾向があり、ランサムウェアによる西側諸国の混乱は間接的にロシア政府の利益に合致することから、黙認されているとの主張がある[15]。2021 年 6 月の G7 サミットでは、ランサムウェアは世界的な課題であり、ロシア政府を名指ししてサイバー犯罪の対策を求める内容が声明に組み込まれた[16]。続いて行われた米露首脳会談においても、米国側がロシア政府に対してロシアに居住するサイバー犯罪者への対処を要求したところ、ロシア側は、サイバー犯罪者を庇護していることは否定した一方、対策に関する特定の分野で協力を強化することに合意したと報じられている。

これらの報道の後、RaaS を提供する一部のサイバー犯罪グループは活動停止を表明しているが、水面下では活動が継続しているとの見方もある。当隊では、本件のような政府放任型のサイバー犯罪に対する国家間の非難にどの程度の効果があるのかという視点を含めて、ランサムウェアについての大局的な状況把握を継続する。また、このような「国家が放任しているサイバー犯罪グループ」が、国家支援型のサイバー活動に関与する可能性も踏まえ、昨今の「国家放任型サイバークライム」に対するわが国としての対応ができるよう、拡大化したサイバー犯罪などについては、APT 同様にサイバー状況把握が重要である一例ともいえるであろう。

3.3 北朝鮮に関係するサイバー攻撃グループ

当隊では、2.2 項で述べたように、Kimsuky に関係すると考えられる攻撃グループの国内活動を複数観測している。一方、本報告期間中の公開情報において、北朝鮮に関係するサイバー攻撃グループによるわが国に対するサイバー諜報活動の情報は得られていない。

わが国以外での北朝鮮に関係するとされるサイバー活動に関しては、2021 年 6 月に韓国の国会議員が、Kimsuky による韓国原子力研究所へのネットワーク侵害を公表した他[17]、2021 年 6 月から 9 月にかけてのセキュリティベンダの公開情報によると、韓国の政府、外交、安全保障、通信事業部門へのスピアフィッ

---

[13] Microsoft Digital Defense Report OCTOBER 2021
https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

[14] Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says
https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

[15] Assessing Russia's role and responsibility in the Colonial Pipeline attack
https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

[16] CARBIS BAY G7 SUMMIT COMMUNIQUÉ
https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/

[17] 北朝鮮のハッカー集団、5 月に韓国原子力研究所に侵入＝韓国議員
https://jp.reuters.com/article/southkorea-northkorea-hack-idJPKCN2DU0VM

シングメールが報告されている[18][19][20]。

その他、先期に引き続き、脆弱性に興味を持つセキュリティ研究者を標的にし、同業者を装い様々なSNS を介して接近、最終的にマルウェアに感染させようとする攻撃が継続しており、関連する SNS アカウントが 2021 年 8 月から 10 月にかけて凍結されたとの報告がある[21]。この攻撃には北朝鮮に拠点を置くステートスポンサードのグループが背後にあると主張されている。

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

上記に示したリージョン以外にも、ステートスポンサードのサイバー活動の存在が報告されている（※）。わが国の組織や個人に対する被害に関する情報は確認されていないが、その可能性を否定する十分な情報も得られてないのが実情である。これらの国々に関係するグローバル企業や国際的な活動を行う組織、個人との情報共有の輪を広げ、サイバー状況把握を進める必要があると考えている。

（※） イランを含む MENA 地域、インド、パキスタンを含む南アジア、ベトナムを含む東南アジア、中南米。

4 活動を通しての所感

本報告期間を振り返ると、以前からみられた政策や安全保障に関わる動向の諜報活動、科学技術や製造技術など技術情報の窃取といったアクティビティの把握が少ない一方、連日のように重要インフラ、大手企業や医療機関に対するランサムウェア攻撃、それに乗じた脅迫行為、情報暴露の事例がわが国を含む世界中で報じられた。

被害組織の視点で見ると、サイバーエスピオナージとサイバークライムとは攻撃の目的こそ異なるものの、その攻撃手口には多くの共通点がある。特に、企業を標的とする暴露型ランサムウェア攻撃では、偵察段階の脆弱性スキャン、初期侵入の手口として用いられるクレデンシャルフィッシングメールやネットワーク境界装置の脆弱性の悪用、システムの広範囲にランサムウェアを仕掛けるための横展開、暴露する機密情報の窃取など、サイバーキルチェーンの様々な段階が標的型サイバー攻撃と重複する。両者の違いを挙げるならば、エスピオナージでは標的分野が予め定められており、未知のマルウェアが使用される可能性が高く、破壊的な攻撃が行われることは稀であるため攻撃の検知が難しいと言えるが、対策の観点では大きな違いはないとみている。

サイバークライムの対策としても、まずは自組織の情報インフラ構成とその弱点、特にグローバル IP を持つインターネット境界を把握し、侵入を前提とした多層防御の導入、入口対策、内部対策、出口対策といった予防措置、事案発生時の状況把握能力強化や復旧のための体制を整備することは、サイバーエスピオナージの対策としても極めて有効だろう。

2 項では攻撃グループの同定に関する判断について述べたが、当隊ではその考察過程において、攻撃に用いられた通信インフラ、攻撃ツール、活動痕跡といったインディケータを過去のアクティビティと比較するだけでなく、攻撃背景を理解するべきと考えている。そのためには、攻撃側のモチベーションとして想定される情報要求や潜在ニーズの動向、攻撃の運用フェーズで用いられる言語や専門知識といった非サイ

---

[18] Kimsuky APT continues to target South Korean government using AppleSeed backdoor
https://blog.malwarebytes.com/threat-intelligence/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/

[19] 北 연계 사이버 위협 조직 탈륨, PDF 문서 취약점 이용한 공격 수행
https://blog.alyac.co.kr/3970

[20] 탈륨(Thallium) 조직, 한국통신사업자연합회 사칭 스피어 피싱 공격 중
https://blog.alyac.co.kr/4130

[21] Twitter Suspends Accounts Used to Snare Security Researchers
https://threatpost.com/twitter-suspends-security-researchers/175524/

バー領域の様々な知見も求められる。これらの知見を積み重ねたうえで、過去の APT 活動を再考することも有用とみている。

本報告期間中に報告されたセキュリティベンダのコラム [22]に、国家主導型（当隊では国家支援型、ステートスポンサードと表記）の脅威と一般的なサイバー犯罪の境界が曖昧になりつつあるとする、興味深い主張が述べられている。その背景として、国家機関に対するエクスプロイトやマルウェアの販売、汎用マルウェアの使用、APT と金銭目的の活動との双方を行う攻撃グループの存在、下請けハッカーの雇用等が挙げられている。この傾向は当隊のサイバー状況把握でも以前よりみられており、同意できる部分も多くある。

ステートスポンサードのサイバー活動に対する名指しの非難声明が発表される場合においても、軍や情報機関の主導する活動だけでなく、政府がサイバー犯罪者を放任していることを指摘するケース（サイバー犯罪者の取り締まりという国家の責務が追及される。当隊では、国家放任型サイバークライムと呼称。）も生まれている。

こうした複雑化する状況下で、ステートスポンサードといわれるサイバー領域の敵対的活動に対抗していくためには、各組織や個人から提供された貴重な情報、事案対応を通じて把握した確かな活動痕跡、各種情報元から収集したマルウェア、操作履歴、通信先等の情報等を総合的に蓄積・分析し、点と点を丹念に繋ぎ合わせ、複雑に絡み合った関係の中から攻撃グループの輪郭やその背景を見出していくことが必要である。

従来の繰り返しとなるが、各組織がインシデント対応と脅威情報の共有ネットワークをより成熟させるとともに、政府関係機関との連携力を強化し、わが国としての対応力を高めていくことが必要不可欠である。そしてその先に、ナショナルサイバーセキュリティの観点で、そのような活動の痕跡を収集して共有し、同盟国・有志国と連携して様々な手段と能力を活用できるよう、国家レベルでのサイバー空間における状況把握（サイバードメインアウェアネス）を高めることが重要であると考えている。

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、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、サイバークライムとされる活動の概況を含めた幅広い脅威情報の収集、情報提供などの活動を引き続き進めていく。

本報告では、特にサイバーセキュリティに関わる組織や人物に影響を与えることを目的としたとみられる認知領域作戦の事例を紹介したが、当隊ではサイバーエスピオナージと同様、国家支援型、国家放任型、等々の可能性を踏まえた調査、記録を含め対応を続けていく。

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。

[22] 国家主導型のサイバー攻撃組織と金銭的な利益を目的とするサイバー犯罪組織の相違点とは？
https://www.eset.com/jp/blog/welivesecurity/state-sponsored-financially-motivated-is-there-any-difference-anymore/