サイバー
脅威分析

Recorded Future®

By Insikt Group®

2021 年 7 月 13 日

東京 2020 オリンピック・パラリンピックに関する脅威レポート

本レポートは、Recorded Future® Platform、ダークウェブコミュニティ、オープンソースインテリジェンス（OSINT）ソースから得られた知見を総合し、COVID-19 パンデミック関連の延期を経て 2021 年 7 月 23 日に開幕する 2020 年東京オリンピックを前にした脅威の状況を分析しています。本レポートは、オリンピック組織に所属する組織、オリンピックのスポンサー、または来るべきオリンピックへの参加や出席を予定している個人にとって最も興味深いものとなるでしょう。

エグゼクティブ・サマリー

オリンピックは、200 以上の国から選手が集まり、世界中のメディアが報道し、数万人もの観客が集まる、標的が多い環境です。注目度が高く、国際的なイベントであることから、オリンピックは、政治的な動機による危害を加えようとしたり、犯罪によって利益を得ようとしたり、国際舞台で開催国に恥をかかせようとする者の標的となります。過去のオリンピックでは、オリンピック組織やそのパートナーである世界アンチドーピング機構などが、さまざまな脅威アクターから標的にされてきました。

来るべきオリンピック大会には、国家が支援する脅威活動グループ、サイバー犯罪者、そして政治的不満や地域的緊張を動機とするグループが集まる可能性があります。しかし、本稿執筆時点では、レコーデッド・フューチャーは、東京オリンピックに対する直接的な脅威、計画的な攻撃、サイバー操作を現時点で確認していません。

キージャッジメント

- 国家が支援する脅威の行為者は、その高度な能力に加え、様々な国家と国際オリンピック委員会（IOC）や関連団体との間で進行中の紛争に基づいて、オリンピック大会やオリンピック関連団体に最も大きな脅威を与えていると考えられます。
- 過去のオリンピック大会やロシアの脅威活動グループに関連する関連組織を標的としたサイバーキャンペーンが行われていることや、国際的なスポーツイベントへの参加資格をめぐって IOC とロシアの間で現在論争が行われていることを考えると、ロシアの APT グループは、来るべき東京オリンピックを標的とし、混乱させることに最も意欲的であると考えられます。中国、北朝鮮、イランなど、他の国家にリンクしている APT グループは、このようなイベントを標的とした歴史的な前例がないか、東京オリンピックの場合には必要な動機がないと評価されています。
- ランサムウェアは、サイバー犯罪者の観点から、オリンピック関連組織にとって最大の脅威となる可能性が高い。2021 年 6 月 25 日、日本の新聞各紙は、日本オリンピック委員会（JOC）が昨年 4 月にランサムウェアの被害に遭ったことを報じました。ランサムウェアの運用者は、オリンピック期間中に基幹インフラやサービスのダウンタイムが許容される可能性が低いことから、オリンピックとその関連組織を魅力的な標的と見なしていると考えられます。その結果、被害組織は、通常の業務を復旧させるためにランサムを迅速に支払うことに大きなインセンティブを受ける可能性があります。
- 国が支援するプロパガンダや偽情報の発信者は、東京大会に対する最初の影響力活動を行い、論争を巻き起こし、人気がない、安全でない、不公平であると大会を貶めようとしています。このようなシナリオは大会期間中も継続される可能性があります。
- レコーデッド・フューチャーでは、東京オリンピックや選手を狙った直接的な物理的脅威は確認していません。COVID-19 の流行が続いていることや、それに伴う日本への外国人招待客の制限により、このような攻撃が行われる機会は少なくなっていると思われます。オリンピックは政治的な抗議活動の一般的な場であり、日本で進行中の COVID-19 パンデミックのために日本での大会に対する反対運動が広がれば、国内での抗議活動につながる可能性があります。しかし、これまでに観測された抗議活動では、暴力的なものはありませんでした。

2018 年以降のオリンピックを狙ったサイバー作戦

ロシア

APT の脅威グループと活動

ロシアの高度持続的脅威（APT）グループは、これまでにも、オリンピックや国際的なスポーツに関連する複数の組織を標的に、破壊的なサイバー攻撃やサイバースパイ活動を行ってきました。過去には、世界アンチ・ドーピング機構（WADA）、米国アンチ・ドーピング機構（USADA）、カナダスポーツ倫理センター（CCES）、国際陸上競技連盟（IAAF）、スポーツ仲裁裁判所（TAS/CAS）、国際サッカー連盟（FIFA）、フランスの多国籍情報技術サービス Atos などが標的となりました。

ロシアの国家支援を受けたサイバーグループは、2018 年の冬季オリンピックを標的にしていることが確認されており、2019 年の米国と英国の当局によると、ロシアの行為者は、2020 年の東京オリンピックに関わる関係者や組織に対して、すでに偵察活動を行っているとのことです。この活動は、ロシアがドーピング活動を理由に大会から追放されたことに関連していると考えられます。ロシアは 2015 年以降、国際陸上競技への国家としての出場を禁止されています。2020 年 12 月には、ロシアは次の 2 つのオリンピックへの代表チームの出場と、今後 2 年間の世界選手権のスポーツイベントへの出場を禁止されました。

APT28 と Sandworm は、それぞれロシアの GRU（Main Intelligence Directorate）ユニット 26165 と 74455 に関連しており、過去に行われたオリンピック関連組織への標的型侵入につながっています。これらの軍事情報ユニットとスポーツとの関連性は不明ですが、ロシア軍とオリンピック・スポーツとの間には長年の関係があり、ソ連時代には国防省がロシアのエリート・スポーツ・クラブを監督していました。ロシア最大のスポーツクラブは、中央陸軍スポーツクラブ（CSKA）モスクワで、少なくとも「CSKA の選手がオリンピックで獲得したメダルは 1,058 個、うち 463 個はオリンピックの金メダル」と主張しています。したがって、参加禁止処分を受けて国の誇りを失ったことが、国際的なスポーツイベントや組織に対するロシアのサイバー活動を少なくとも一部は後押ししていると考えられます。

APT28 は、2016 年のリオ・オリンピックの時期に活動しており、疑似ハクティビストのフロントグループを採用して、世界アンチ・ドーピング機構への侵入時に盗まれたと思われるオリンピック選手の薬物検査ファイルを投棄するという影響力のある活動を行っていました。

Sandworm は、2018 年の平昌冬季オリンピックで活躍し、開会式の際に韓国で開催されたゲームの IT インフラを混乱させる破壊的なマルウェア攻撃を行いました。「Olympic Destroyer」と呼ばれるマルウェアの亜種は、2017 年 12 月以前に平昌オリンピックを標的にする一環として、大手通信事業者や IT 事業者を標的に使用されていました。Talos 社と Crowdstrike 社の研究者は、2018 年 2 月 9 日にオリンピックの開会式を混乱させるために Olympic Destroyer が使用されたことを発見しました。Sandworm が配信した Olympic Destroyer マルウェアは、カスペルスキーが「破壊的な自己改変型パスワード盗用自己増殖型悪意のあるプログラム」と表現しています。彼らの調査によると、Olympic Destroyer は、Powershell スクリプトが埋め込まれた文書が添付されたスピアフィッシングメールで配信され、実行されると、地元の会場、Pyeongchang2018[.]com サーバー、IT サービスプロバイダーの Atos など、オリンピックに関連する標的ホストにバックドアがインストールされました。その後、米国政府関係者の話として、この攻撃は、ロシアの GRU が、北朝鮮の IP アドレスと偽造したリッチヘッダーを使用して、北朝鮮が攻撃の背後にいるように見せかけた「偽旗」作戦であることが示唆されました。

北朝鮮

APT の脅威グループと活動

今年は北朝鮮が不参加であることに加え、COVID-19 の流行や食糧不足の深刻化など、さまざまな内政上の問題があるため、北朝鮮が東京オリンピックを妨害する可能性は低いと思われます。しかし、内部のプロパガンダのために、政権に密着している北朝鮮の国営メディアが、金メダルを獲得した選手の写真を加工したり、記事を捏造したりする可能性があります。

とはいえ、北朝鮮の脅威グループがオリンピック関連組織を標的にした歴史は限られています。2018 年 2 月、マカフィーは、オリンピック関連組織を標的にした「Gold Dragon」と名付けられたファイルレスマルウェアを検出しました。マカフィーが韓国の野生で観測した最初の Gold Dragon の亜種は、2017 年 7 月に登場しました。オリジナルの Gold Dragon マルウェアは、「한글추출 .exe」というファイル名を持ち、これは「Hangul Extraction」と訳され、韓国でのみ確認されました。当初は北朝鮮への帰属は明らかにされていませんでしたが、2018 年 8 月にマカフィーが北朝鮮のマルウェアの比較を公開し、Gold Dragon と NavRAT のコードの重複が詳細に示されました。2018 年のさまざまな報道では、NavRAT が北朝鮮の APT Group123（APT37 としても追跡されている）と関連している可能性が高いと言及されています。

Cybereason は、2020 年 11 月に、「Gold Dragon」と、同じく北朝鮮の国家支援型脅威グループである「Kimsuky」に関連するいくつかのマルウェアが使用する URL パターンやインフラストラクチャの類似性に関する詳細を発表しました。Kimsuky は歴史的に、韓国、日本、米国の様々な分野の個人や専門家、シンクタンク、政府機関、生物医学工学の専門家がいる大学などを標的にしてきました。

中国

APT の脅威グループと活動

中国の脅威活動グループが主要な国際スポーツイベントやスポーツ団体を標的にした歴史的な前例はありません。また、中国は、広範囲にわたる破壊的・混乱的な攻撃を行うことについて、他国に比べて著しく抑制的である。したがって、中国のグループは、重要な会議の前に特定の組織や政府を定期的に標的にしており、北京が国内外の少数民族や宗教団体をサイバーで監視していることはよく知られていますが、現時点では、中国がオリンピック大会に破壊的な脅威を与える可能性は低いと考えられます。

しかし、日本は、中国の主要な民間対外情報機関である国家安全部（MSS）と軍事情報機関である人民解放軍（PLA）戦略支援部隊（SSF）に所属する脅威活動グループを通じて、両国の地域的な近接性から、依然として中国のサイバースパイ活動の主要な焦点となっています。

レコーデッド・フューチャーは、日本に強い関心を持つ中国のグループ（以下に詳述）を追跡しており、彼らがオリンピック関係者やスポンサーを対象とした情報収集活動を行う可能性がある。さらに、オリンピックに関連した宣伝を利用して、新疆ウイグル自治区でのウイグル人の人権侵害など、中国国内で行われているとされる人権侵害に光を当てようとするアスリートや個人が、監視やモニタリングの目的で個別に標的にされる可能性が高いと考えられます。日本に焦点を当てた中国の主な APT グループは以下の通りです。

- APT10 は、「Stone Panda」、「CVNX」、「MenuPass」、「POTASSIUM」、「Red Apollo」などの名称で知られ、2009 年頃から活動している中国の国家支援型脅威グループです。このグループは、一連のフロント企業を通じて活動する民間業者で構成されており、中国の MSS の地方局である天津国家安全局に代わって活動しています。APT10 はこれまで日本を中心に活動してきましたが、世界中の組織を標的とした活動も行ってきました。しかし、米国政府が起訴した後、APT10 はさらに地域を絞って活動しており、最近発表された活動はすべて、日本に関連する民間組織を特に標的としています。
- Tick は、Bronze Butler という名前でも知られており、歴史的にカスタムメイドのマルウェアの亜種を使用して、防衛、航空宇宙、化学、衛星産業を標的にしており、主に日本に本社があり、中国に子会社がある組織を対象にしています。2021 年 4 月、日本のニュースソースは、このグループが青島に所在する PLA-SSF 61419 部隊に関連していると報じました。ティックは、日本を標的とし、PLA（特に瀋陽軍区技術偵察局）との関係が指摘されている中国のグループ「トント・チーム」との密接な関係が疑われている。この 2 つのグループは、異なる戦術・技術・手順（TTPs）と標的プロファイルを持つ一方で、能力を共有していることが確認されています。2020 年初頭、Tick Group は、日本の多国籍企業である三菱電機が公開した歴史的な侵入事件に関連していました。
- 2020 年の JPCERT レポートでは、2020 年 8 月頃に報告された標的型攻撃において、WINNTI マルウェアの使用が観測されています。また、過去には、様々な日本のセキュリティ研究者（1、2）が、2013 年から 2020 年までずっと WINNTI マルウェアの亜種の使用を観測しています。WINNTI（別名：HIGHNOON）は、APT17 や APT41 など、複数の APT グループが歴史的に使用してきたバックドアおよびルートキットです。
- 日本のコンピュータ緊急対応チーム（JPCERT）からの多数の報告によると、Palmerworm や Temp.Overboard としても知られる Blacktech は、2017 年と 2018 年に日本企業を標的にして非常に活発に活動しており、最近の報告では同グループが継続的に活動していることが示されています。ブラックテックは、日本の大手多国籍企業である三菱電機に対する 2019 年の侵入事件にも名を連ねており、この組織はその後、ティックの標的となった組織と同じです。同じく日本の情報筋は、BlackTech を武漢に拠点を置く軍の部隊と関連づけていますが、現在のところ、このグループが特定の PLA の部隊に起因するとは断定されていません。

イラン

APT の脅威グループと活動

イランの APT はこれまで、オリンピックやスポーツ連盟に関連する組織に対して破壊的なサイバー攻撃やサイバースパイ侵入を行ったことは確認されていません。しかし、このことは、イランの APT が、オリンピックを支援する組織や、オリンピックに参加する人々に対して、スパイ活動による侵入を試みることを妨げるものではありません。イランの主要な脅威活動グループのうち、APT39 は、日本で開催されるオリンピックをイランの選手やそのチーム、政府の代表者と接触する機会として利用しようとする反政府ネットワークへの侵入を担当する可能性が最も高いと考えられます。そのため、イラン人選手を受け入れている施設は、標的にされるリスクが高まります。

イランの国内政治では、政治的な動機に基づくスポーツ論争が頻発している。その中には、オリンピックのボイコットや、イスラエルの選手が参加するスポーツ大会、女性の選手やサポーターが参加するスポーツ大会などが含まれています。オリンピックに関連したテーマ性のあるルアーの使用も、歴史的に見て、イランの APT の戦術には含まれていません。しかし、イランの APT グループがスポーツの領域に進出する可能性は、特にイランの国内政治活動や、他の中東のスポーツ・オリンピック連盟との関係で高まっています。

APT35（Charming Kitten、Phosphorus） と APT39（Rana Intelligence Computing Company、Chafer）の少なくとも 2 つのイラン関連の脅威アクターが、2020 年のオリンピックに参加する組織や個人に対して攻撃を仕掛けるための情報や防諜活動を行っていることが報告されています。APT35 は、イスラム革命防衛隊（IRGC）の要請を受けて、戦略的・戦術的な情報を求め、防諜活動も行っていることが報告されています。また、APT39 は、防諜活動や長期的なスパイ活動に重点を置いていることが報告されています。

2020 年 10 月 28 日にマイクロソフトが発表したレポートによると、APT35 は、サウジアラビアで開催されたミュンヘンセキュリティ会議および Think20（T20）サミットの会議主催者を装ったスパイ活動を行いました。マイクロソフトの Threat Intelligence Center（MSTIC）は、このキャンペーンの主な目的は、大使や上級政策専門家など、セキュリティ会議に出席する高名な人物を標的にしたものであると評価しています。この作戦において、APT35 は、元政府高官、政策専門家、学者、非政府組織（NGO）のリーダーなどを対象に、なりすました招待メールを送信しました。電子メールにはほぼ完璧な英語が使用されており、COVID-19 パンデミックの際の旅行への不安を解消するための遠隔セッションへの招待が含まれていました。

レコーデッド・フューチャーは、日本政府や開催都市、オリンピックの計画に関連する組織を標的とする意図を示すような APT35 関連の活動を検出していませんが、APT35 は、オリンピックをテーマにしたルアーを使って、オリンピックの前、中、後に開催される会議やイベントを標的にするという点で、過去のキャンペーンと同じ TTP を示す可能性が高いです。これには、会議に出席する研究者、政治家、政策担当者、外交官なども含まれます。

APT39 はこれまでにも、防諜・監視活動や、政府のネットワーク、旅行、通信分野への標的型侵入など、情報安全保障省（MOIS）の要請に基づいた活動に関連しています。この脅威主体グループと同様の活動を行っているグループは、イランのスポーツ選手やディアスポラのコミュニティメンバー、活動家、イランの反体制派を追跡する任務を負っていると考えられます。

また、オープンソースの報告によると、政府内の標的も発生しており、IRGC のメンバーがハッサン・ルーハニ大統領の閣僚に対して標的侵入を行ったとのことです。APT39 とオリンピックとの間に直接的な関係はありませんが、このような過去の標的事例は、オリンピックに参加する可能性のあるイラン政府関係者に対する監視の可能性が高まっていることを示しています。

金銭的な動機によるサイバー脅威

クリミナル・ターゲティング

レコーデッド・フューチャーは、ダークウェブやアンダーグラウンドのフォーラムにおいて、東京オリンピックに対する直接的な脅威、計画された攻撃、サイバーオペレーションを確認していませんが、主に以下のアンダーグラウンドのフォーラムでオリンピックに言及した書き込みが見られました。オリンピックに関連する投稿は、主に以下のアンダーグラウンド・フォーラムで見つかりました：Club2CRD、Omerta、Korovka、Verified、the Honker Union of China。これらの情報源で見つかった関連する投稿の大半は、以下のようなトピックに関連しています。

- ニュースメディアへの引用と再掲載
- 医薬品 / 薬の広告・販売
- オリンピックおよび関連するオリンピック組織に関連する危険なログインアカウント認証情報の販売
- ランサムウェアの配布サイトに流出したファイル名にオリンピックの文字が含まれていた件について

さらに 2 つのダークウェブマーケットプレイスでは、2020 年のオリンピックに関連する情報が販売されているのが確認されました。「Genesis Store」と「Russian Market」です。

Genesis Store：Recorded Future 社は、被害者の情報を「ボット」と呼ばれる形式で販売するダークウェブマーケット「Genesis Store」で、2020 年のオリンピックへの言及を確認しました。ボットには、被害者のアカウント認証情報、ブラウザのフィンガープリント、IP アドレス、セッションクッキーの組み合わせが含まれます。Genesis Store で発見された 20 個のブラウザログインはすべて、組織委員会のウェブサイトである tokyo2020[.]org に関連していました。サブドメインの 1 つは、2020 年東京オリンピックの日本人ボランティア専用と思われます。

Russian Market：レコーデッド・フューチャー社は、脅威アクター「Russian Market」が運営するショップ「Russian Market」において、2020 年東京オリンピックに関連して記載されている文献を発見しました。Russian Market は、ダンプ、RDP や SSH のアクセス、ログ、各種アカウント情報を販売しています。Genesis Store と同様に、Russian Market には「tokyo2020[.]org」への様々なウェブサイトのログイン情報が含まれています。これらの認証情報にアクセスできるようになると、認証情報を購入した脅威アクターは、アカウントにログインし、ビジネスメールの漏洩（BEC）、権限の昇格、正当な認証情報保持者の全体的なオンラインアイデンティティの乗っ取りなどの悪意のある活動を行うことができます。これは、クレデンシャルのセットには通常、クレデンシャルのソースに関する広範な情報や、被害者からスクレイプされたクッキーが含まれていることに起因します。

ランサムウェアの脅威

ランサムウェアは、オリンピック関連組織にとって最大のサイバー犯罪の脅威となる可能性が高い。2021 年 6 月 25 日、日本国内の新聞各紙は、日本オリンピック委員会（JOC）が 4 月にランサムウェアの被害に遭ったことを報じました。

レコーデッド・フューチャーは、現時点ではランサムウェアの運営者が特にオリンピック関連組織を標的にしていることを示唆する情報や指標を確認していません。しかし、ランサムウェアの操作は一般的に日和見的な性質を持っており、また、注目度の高い国際的な大会であることから、このような組織はランサムウェア操作の魅力的なターゲットとなる可能性が高いと考えています。大会期間中は、中核となるインフラやサービスのダウンタイムが許容される可能性は低く、その結果、被害者は身代金を支払って迅速に通常業務を復旧させるよう誘導されると考えられます。

レコーデッド・フューチャーは、2020 年 1 月以降のランサムウェアの恐喝サイトを調査し、ランサムウェア「Nefilim」の運営者が管理する恐喝サイト「Corporate Leaks」に掲載されている 2020 年オリンピック関連団体への言及を 35 件確認しました。このウェブサイトは、Nefilim ランサムウェアに感染した被害者の名前やドメインを、被害者のネットワークから盗んだデータのサンプルセットとともに掲載するために使用されています。「Corporate Leaks」に投稿された内容を分析した結果、オリンピック関連文書は、2020 年 9 月にランサムウェア攻撃を受けたイタリアの眼鏡コングロマリットで世界最大の眼鏡会社である Luxottica Group に対する攻撃の一部である可能性が高いことが分かりました。ランサムウェア「Nefilim」の運営者が公開した以下の東京オリンピック関連文書を確認しました。

- 24532 2020-01-13 11:08 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics\MOTOGP Simulation (WHSL).xlsx
- 758183 2020-01-13 11:09 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics\Tokyo Olympic + Mugello 2020 - TH.pptx
- 0 2020-01-14 03:39 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics

オリンピックインフラへの脅威

2020 年のオリンピックのインフラは、サイバー攻撃や物理的な脅威など、複数のソースからの脅威に直面しています。オリンピックの開催日が近づくにつれ、オリンピックの従業員、パートナー、ベンダー、顧客を狙ったフィッシング詐欺が増加する可能性があると考えています。さらに、オリンピックの企画者や政策立案者は、分散型サービス拒否（DDoS）攻撃、ウェブサイトの改ざん、ドメインのタイポスクワッティング、スピアフィッシング攻撃など、よく使われる手法に注意する必要があります。

フィッシング攻撃

フィッシング攻撃は、APT やその他の脅威グループが過去の大会でオリンピックのインフラを標的にする際の共通の手段となっているため、特に注意が必要です。このようなフィッシング攻撃は、マルウェアへの感染につながり、データの損失やオリンピック施設への物理的な損害を引き起こす可能性があります。

過去 3 カ月間に確認されたオリンピック関連のフィッシング・イベントは約 721 件です。フィッシング・イベントにおける脅威の主体の特定は困難ですが、電子メールでの緊急の言葉の使用、役員やベンダーへのなりすまし、ベンダーやチケット販売システムを装った悪意のあるウェブサイトの使用など、フィッシング・メッセージの構造には共通のテーマがあることが確認されました。これらのフィッシング・メールの全体的な目的は、標的となるネットワークにマルウェアをインストールすることと、より標的を絞った攻撃に使用できるユーザー認証情報を収集することであると考えられます。

2020 年の東京オリンピックは、2021 年 5 月に発生した ProjectWEB プラットフォームの不正アクセスの影響を受けました。ProjectWEB は、1998 年に立ち上げられた日本のクラウドベースの企業コラボレーションおよびファイル共有プラットフォームで、現在は日本の政府機関で広く利用されています。今回の侵入では、未知の脅威主体が ProjectWEB にアクセスし、少なくとも 76,000 件の電子メールアドレス、専有情報、メールシステムの設定を取得することができました。さらに、この攻撃者は、ProjectWEB を通じて日本の外務省と東京の成田国際空港にアクセスし、航空管制データ、フライトスケジュール、業務に関する情報を盗み出しました。

2021 年 6 月 2 日、日本政府のサイバーセキュリティ国家危機管理センター（NISC）は、声明の中で、オリンピックに先立って行われたサイバーセキュリティ訓練に参加した約 170 名のデータが漏洩したことを確認しました。ジャパンタイムズの記事によると、流出したデータには、オリンピックの開催に関わる 90 の組織の人々の名前と所属が含まれていました。しかし、ProjectWEB への侵入は、オリンピックを狙ったものではなく、日本の様々な組織から情報を盗むためのサプライチェーン攻撃であった可能性が高く、ProjectWEB プラットフォームの主なユーザーは日本の政府機関であるとのことです。

DDoS およびウェブサイトの改ざん

平昌やリオデジャネイロなどの過去のオリンピックでは、ハクティビスト集団による DDoS 攻撃が主な脅威でした。しかし、レコーデッド・フューチャー社では、現時点で、2020 年のオリンピックのインフラを標的にすることを表明している組織的なハクティビスト集団を確認していません。

過去のキャンペーンには、2016 年のアノニマスのキャンペーン「#OpOlympicHacking」があり、オリンピック大会を標的にしたことに関して最も広く注目されています。前述のキャンペーンでは、ハクティビストたちがソーシャルメディアのチャンネルを利用して、協調的な DDoS 攻撃を組織したり、標的となるネットワーク内の脆弱性について議論したり、キャンペーンの結果を発表したりしました。これらの攻撃は、オリンピック関連のウェブサイトに限らず、スポンサーや開催都市、政府機関のウェブサイトなど、オリンピックに関連する企業にも影響を与えました。

しかし、当社のデータと分析によると、過去 1 年間に他社が行った調査と同様に、ハクティビストの攻撃にまつわる会話は、2015 年から 2016 年にかけてのピーク以降、急減していることがわかりました。SQL インジェクション攻撃や DDoS フラッドの影響を受けやすい大企業の数が減少しているのは、ウェブサイトの構造がより成熟していることや、Akamai や Cloudflare などの DDoS 対策サービスが利用されているためと考えられます。ハクティビストの中には高度な技術を持つ者もいますが、多くの場合、ハクティビスト組織のメンバーは初心者であり、有能なネットワーク防御者が容易に打ち負かすことができるシンプルで時代遅れのツールや技術に頼っています。

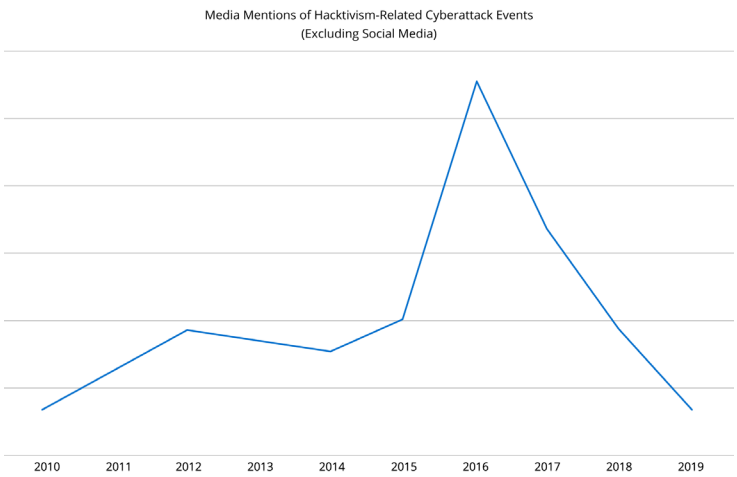

図 1: ハクティビズム関連のサイバー攻撃に関するメディアの言及（2010 年～ 2019 年）（出典：Recorded Future 社）

ハクティビストグループは、自分たちのメッセージを広めるためにメディアの注目を頼りにしており、2018 年の平昌オリンピックの際に観察されたように、イベント中の破壊的なサイバー活動はすぐに報道陣の注目を集めることになります。例えば、イランの様々なハクティビストグループは、歴史的に、国際大会に出場するイランのローカルチームを支援するため、またはイランのナショナルサッカーチームを支援するために、国際的なサッカーチームに対して標的となるウェブサイトの改ざん攻撃を行ってきました。このような攻撃は、ALFA TEaM の AlfaShell に責任を持つメンバーによって行われており、多くの国際的、地域的なサッカースポーツ組織を標的にしてきました。

図 2：ALFA TEaM のメンバーがシリアサッカー連盟に対して投稿した改ざん画像（出典：tarafdari[.]com）

2018 年 FIFA ワールドカップ予選の試合後にシリアサッカー連盟に対して行われた攻撃や、2022 年ワールドカップ予選の試合後にバーレーンサッカー協会（BFA）に対して行われた攻撃の大部分は、ハクティビストが不公平感を感じたり、イランのサッカーチームや国家に対する侮辱に反応したりして実現したものです。現在の日本と韓国の緊張関係や、中国との尖閣諸島・釣魚島に関する政治的紛争を考えると、特に中国から日本のインフラを標的とした民族主義的なハクティビストのキャンペーンが行われる可能性はありますが、近年、愛国的なハクティビズムが減少していることを考えると、その可能性は低いと考えられます。

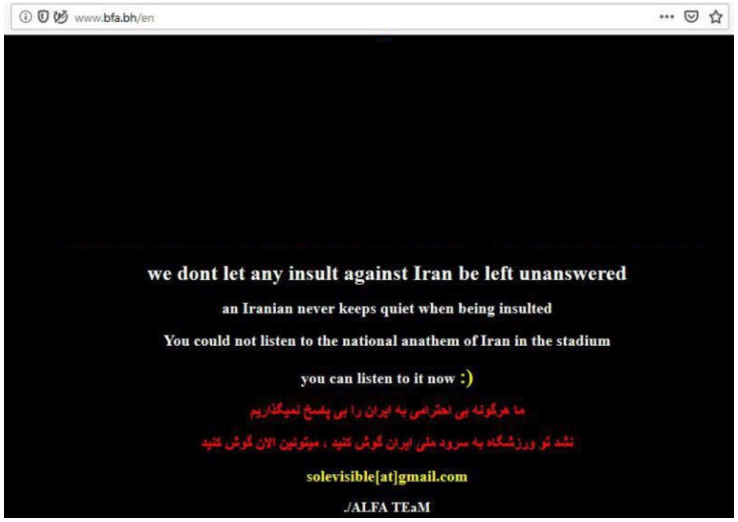

図 3：バーレーンのスタジアムでのイラン国歌斉唱時に聞こえた侮辱的な言葉を受けて、BFA のウェブサイトが ALFA TEaM によって改ざんされた（出典：ILNA ニュース [1]）

[1] https[:]//www.ilna[.]news/%D8%A8%D8%AE%D8%B4-%D9%88%D8%B1%D8%B2%D8%B4%DB%8C-7/825013-%D8%B3%D8%A7%DB%8C%D8%AA-%D9%81%D8%AF%D8%B1%D8%A7%D8%B3%DB%8C%D9%88%D9%86-%D9%8

東京オリンピックをテーマにしたドメイン

2021 年 4 月 1 日以降、Recorded Future 社は、2020 年のオリンピックとそのブランディングを模倣した 44 個のドメインの登録を確認しています。また、これらのドメインの大半は、現在パークされている一般的なドメインに解決されていますが、ゲームの開始が近づくにつれて、これらのページはよりアクティブになる可能性が高いと考えています。

本稿執筆時点では、悪意のある活動は確認されていませんが、これらのドメインの一部は、オリンピックの開催間近になると、将来的に悪意のある目的で使用される可能性があります。これらのドメインの完全なリストは、付録 A に含まれています。

2020 年オリンピックへの非サイバー的脅威

インフォメーション&インフルエンス・オペレーション

国家のプロパガンダや偽情報の発信者は、東京大会に対して最初の影響力活動を行い、論争を巻き起こし、イベントが不人気、安全でない、不正であると貶めようとしています。

COVID-19 によって 2020 年の東京大会が中止に追い込まれる前に、Cyber Threat Alliance（CTA）は、破壊的なサイバー攻撃と並んで、オリンピックにまつわる偽情報キャンペーンが「最も可能性が高い」と予測していました。さらに CTA は、悪意のあるサイバー活動は「特定の組織を危険にさらす直接的な試みではなく、ソーシャルメディアや偽情報キャンペーンの形で行われる可能性が高い」と判断しています。この可能性は、ロシアのオリンピック禁止令によってさらに高まっています。ロシアはほぼ確実にクレムリンを怒らせており、少なくとも、オリンピックや他国から参加するアスリートを弱体化させるために、国が支援するあからさまな影響力活動を行わざるを得ないでしょう。

現在、大会の開催が決まっており、ロシアの参加資格にはほとんど変化がない（ロシア選手はロシア連邦ではなく、ロシアオリンピック委員会（ROC）に所属して参加している）ことから、ロシアの偽情報活動が実現する可能性は引き続き高いと考えています。

COVID-19

COVID-19 が発生して以来、外国政府、国家の宣伝・偽情報機関、ソーシャルメディアは、ウイルスの症状や致死性、治療法、症例数、そして最近ではワクチンの有効性、さらにはその使用をめぐる法的・道徳的な議論などについて、誤った誤解を招くような物語を提示してきた。東京オリンピックを目前に控え、COVID-19 はメディア報道の中で根強い議論の対象であり続け、ほぼ間違いなく偽情報やプロパガンダのサブテーマとして機能すると考えられる。大まかに言えば、日本のローカルメディアと海外のメディアの両方で、地域の症例数、野生での亜種、世界中のアスリートが日本に到着する際の地元住民の安全性に関する誤解を招く可能性のある情報に関して、少なくとも単独の誤った主張が確認されると予想しています。

さらに、COVID-19 関連の誤報や偽情報が特定の会場について広まる可能性があります。スポーツイベント会場とオリンピック村などの人通りの多い場所の両方で、COVID-19 の緩和処置（検査、マスク、ワクチンなどの他の義務化など）が行われます。

最後に、特定のアスリートや国の代表団がウイルスの亜種を「持ち込んだ」とか、一般市民を危険にさらすような内部発生の原因になったとする主張など、各国のアスリート代表を対象とした偽物語や偽情報が発生する可能性が高いと考えられます。2020 年、米軍は、COVID-19 の最初の症例が記録される前に、中国湖北省武漢で開催された 2019 年の軍事ワールドゲームの後に、軍当局が中国国民に COVID-19 を導入したと示唆する、中国の国家公務員および国家の公式報道機関が作成し、増幅した虚偽の主張の対象となっていることに気付きました。中国当局は、何の裏付けもなく、この陰謀論を繰り返し再登場させています。

私たちは、以下のテーマに集中しているロシアの国営メディアを特定しました。

- **2020 年の東京大会は安全ではない。**ロシアの国営メディアは、オリンピック組織委員会が、日本で COVID-19 の緊急事態が発生している中で、計算不足のリスクを取っていると表現したり、患者数が増加していることからオリンピックが全面的に中止される可能性があると評価したり、北朝鮮が安全上の理由から出場しないことを選択したことから大会に疑問を投げかけたりしています。
- **2020 年の東京大会は、一般の人々には不人気。**ロシア・トゥデイは、COVID-19 の影響で日本国民が大会を支持していないことを大きく取り上げています。この感情は大部分が本物であるにもかかわらず、「『オリンピックは貧乏人を殺す』：2020 年に開催される東京オリンピックに抗議し、中止を求める声が高まっている。」のようなセンセーショナルな記事で描かれています。同様に、日本政府やオリンピック企画委員会に対する性差別の疑惑により、オリンピックが不人気であるとも主張しています。また、中国とロシアの情報源は、日本人の大多数が今年のゲーム開催を望んでいないという世論調査にも注目しています。[2]
- **ロシアは国際オリンピック委員会から公正な扱いを受けていない。**ロシアの国営メディアは、WADA による国際競技でのスポーツ禁止措置を「不当」と強く批判し、不快感を示しています。また、西欧の政治的圧力を理由に、東京 2020 でのロシアの国旗、国歌、名前の使用を禁止しています。2018 年のある RT 社説は、WADA を「反ロシア的なアジェンダ」の導管と呼んでいます。

[2] http://en.people[.]cn/n3/2021/0111/c90000-9807866.html

抗議活動とネガティブなセンチメント

オリンピックは歴史的に、時事問題や社会問題に対する声を増幅させるプラットフォームとして利用されてきました。国際オリンピック委員会のトーマス・バッハ会長は、アスリートはオリンピックを利用してブラック・ライブズ・マター（BLM）運動に関連するアパレルを着用するなどの政治的抗議活動を行うべきではないと発言し、反発を受けました。アスリートや他のオリンピック参加者が推進する可能性のある時事問題や社会的活動は、以下の通りです。

Black Lives Matter と人種的正義の抗議活動

BLM とオリンピックは、2021 年 4 月に IOC がプレスリリースに記載されているルール 50 が BLM の服やシンボル、ジェスチャーに適用されることを確認し、一緒にニュースになりました。これには、2020 年 1 月に IOC が作成した文書によると、膝をついたり、拳を上げたりすることも含まれており、この文書が発表された時点でもメディアの注目を集めていました。ここ数週間のニュースサイトでは、この決定を誤って要約しており、ルール 50 が IOC にとって新しいものであるかのような表現や、日本政府が BLM の表現を特に禁止したかのような表現が含まれています。BLM やそれに類するデモは、東京大会に参加するアスリートから行われる可能性が高いでしょう。選手組合である世界選手協会は、COVID による選手の安全性を理由に東京オリンピックの開催を控えるだけでなく、政治的なジェスチャーでペナルティを受けた選手に法的支援を行うことをここ数週間で表明しています。2020 年 6 月に日本で BLM の抗議活動が行われましたが、日本の市民や居住者で構成される参加者による抗議活動やデモは、代わりにオリンピックに対する一般的な反対活動に焦点を当てる可能性が高いと考えています。

ウイグル、香港、そして反中国の抗議活動

また、香港での政治的な問題や、中国の少数民族であるウイグル人の扱いに関する反中国的な感情も、デモの動機となる可能性があります。すでに、これらの問題をめぐって、2022 年の北京冬季オリンピックをボイコットしようとするデモや呼びかけが行われており、中国関連の抗議活動ではこれらの問題が話題の中心となるでしょう。

日本国内の反対運動

世界的な動きやイベントに加えて、日本国内でもオリンピック開催に反対する声が強くなっています。日本の雑誌「朝日新聞」が最近行った世論調査によると、回答者の 83%がオリンピック開催に反対しており、オリンピックの中止または延期を希望しており、中止を希望する人が僅差で過半数を占めています。この世論調査は、ここ数ヶ月間に日本で行われた同様の調査と類似しています。主に IOC 東京本部付近では、大小さまざまな抗議活動が行われています。本稿執筆時点では、これらの抗議活動はいずれも暴力的にはなっていません。

オリンピックに反対する主な動機は、「COVID-19」の状況が悪化することへの懸念です。レコーデッド・フューチャーの調査によると、オリンピックをテーマにした日本語のソーシャルメディアでの議論では、「世論に従わない日本政府への怒り」と「オリンピック開催による環境破壊」が最も多く挙げられています。後者については、オリンピック村を中心に議論されている。オリンピックへの抗議や妨害を目的とする環境保護団体は、注目度の高いアスリートの数や、オリンピックの「中心」とみなされているオリンピック村をターゲットにすることを、他の可能性のあるターゲットと比較して、より高い優先順位で考えるでしょう。オリンピック村への出入りは COVID-19 対策の観点から運営により厳しく監視・制限されているにもかかわらず、オリンピックへの抗議や妨害を目的とします。

大会期間中の抗議活動は、日本オリンピック委員会（JOC）のオフィスがある日本スポーツオリンピック・スクエア（JSOS）を中心に行われるでしょう。JSOS ではここ数週間、小規模な抗議活動が行われてきましたが、大会が近づくにつれ、抗議活動の頻度と規模が大きくなっていくと Recorded Future は見ています。JSOS には、JOC の他に、日本オリンピック博物館があり、東京オリンピックのメイン会場である国立競技場をはじめとする複数のオリンピック会場に隣接しています。

図 4：5 月 18 日に JSOS ビル前で行われた抗議活動の様子をソーシャルメディアでシェアした画像（出典：Labornetjp）

物理的な脅威

本稿執筆時点で、Recorded Future は、東京オリンピックや選手を狙った直接的な物理的脅威を確認していません。オリンピック大会で物理的な攻撃が行われるのは珍しいことですが、前代未聞のことではありません。日本では COVID-19 の規制が残っているため、脅威主体が観客や選手への物理的攻撃を実行する機会は減少していると考えられます。さらに、観客の数が減ることで、そのような攻撃の潜在的な効果は大幅に減少します。

現在、在留資格を持つ外国人を除き、すべての外国人が日本への入国を禁止されています。2021 年 6 月 20 日、東京都をはじめとする 6 つの都道府県は、7 月 11 日までの期間、準非常事態宣言を発令しました。その後、政府関係者は、大会に向けて、より厳しい緊急事態措置の発動も選択肢として残っていることを示唆しています。また、政府は国内での観戦を可能にすることを目指していると発表しましたが、本稿執筆時点では、代表者やスポンサーを含まない 1 万人としています。

2021 年 5 月 14 日、東京オリンピック・パラリンピック競技大会組織委員会は、来日する関係者を 9 万人に減らし、「役割を持った人、運営上の役割を持った人だけが東京に来る」と発表しました。この削減は、IOC と国際パラリンピック委員会（IPC）からの訪問者に向けたものです。さらに、この削減は、国際スポーツ連盟関係者、メディア、スポンサー、およびそのゲストにも影響を与える可能性が高い。

展　望

オリンピックのような国際的な大イベントは、世界中のスレットアクターにとって、関心のある個人や組織をスパイしたり、イベントを妨害して開催国に恥をかかせたり、政治的な立場を表明したり、犯罪行為で利益を得たりするための絶好の機会です。2020 年に開催される東京オリンピックも例外ではありませんが、今回は COVID-19 の流行が続いているため、例年のオリンピックとは脅威の状況が大きく異なります。

COVID の規制により、物理的な脅威や広範囲に及ぶ破壊的な抗議活動の可能性は低くなりますが、国家、犯罪者、ハクティビストは、それぞれの目的を達成するために活動を行う動機を持ち続けると思われます。例えば、ロシアの APT グループは、東京大会を標的にしている可能性が最も高いと考えられますが、大会を混乱させることは、国が参加を禁止されたことに対する単なる報復と考えられます。一方、ランサムウェア・ギャングは、主要インフラのダウンタイムが長引くとイベントに大きな混乱が生じるため、大会を恐喝攻撃の格好のターゲットと見なすでしょう。最後に、ハクティビストたちは、愛国心を持っていたり、特定のモラルに不満を持っていたりして、オリンピックを自分たちの特定のメッセージを表現するための注目度の高い機会と考えているようですが、このような活動は数年前から全般的に減少しています。

国が支援する活動やランサムウェアの活動を予測することは困難ですが、オリンピックが近づくにつれて、イベントに関連する脅威アクターの話題が増え、タイポスクワートやオリンピックをテーマにしたドメインが追加登録され、クレデンシャルハーベストやマルウェアキャンペーンで活発になり、計画されている抗議活動についての議論が増えることが予想されます。

付録 A

観察された東京オリンピックをテーマにしたドメインのリストは以下の通りです。

2021olympic[.]cn
2021olympics[.]jp
2021olympicupdates[.]com
2021olympicupdates[.]live
2021olympicupdateslive[.]com
cancel-olympic[.]tokyo
cxaolympicgames2021[.]org
lost-olympic[.]tokyo
no-olympic[.]tokyo
olympic2020[.]in
olympic2020in[.]tokyo
olympic2021[.]in
olympicgames2021[.]cn
olympicgames2021.co.za
olympicnewstokyo[.]com
olympics2020[.]icu
olympics2020[.]in
olympics2020[.]vip
olympics2021[.]in
olympicsjapan2021[.]in
olympicvirtual2021[.]com
perrigoselfcareolympics2021[.]com
stop-olympic[.]tokyo
summerolympics-2020[.]org
teamnl2020-olympic-paralympic[.]games
the2021olympicgames[.]com
the2021olympicgames[.]org
the2021olympicstokyo[.]com
theolympicstokyo2021[.]com
tokyo----olympics[.]org
tokyo---olympics[.]org
tokyo--olympics[.]org
tokyo-olympicslive[.]com
tokyoolympicplay.blogspot[.]com
tokyoolympicplay[.]com
tokyoolympics[.]org
tokyoolympicsfootballlive[.]com
tokyoolympicsolympics[.]com
tokyoolympicsplay.blogspot[.]com
tokyoolympicsport[.]com
tokyoolympicswaterpololive[.]com
tokyotokyoolympics[.]com
usolympics2020[.]com
usolympics2021[.]com

レコーデッド・フューチャーについて

レコーデッド・フューチャーは、エンタープライズ・セキュリティのためのインテリジェンスを提供するリーディングカンパニーです。レコーデッド・フューチャーは、持続的かつ広範な自動データ収集・分析と人間による分析を組み合わせることで、タイムリーで正確、かつ実用的なインテリジェンスを提供します。混沌と不確実性が高まる世界において、レコーデッド・フューチャーは、脅威をより早く特定・検知し、敵対者を阻止するために事前に行動を起こし、従業員、システム、資産を保護するために必要な可視性を企業に提供し、安心してビジネスを遂行できるようにします。レコーデッド・フューチャーは、世界中の 1,000 を超える企業や政府機関から信頼を得ています。

詳細は www.recordedfuture.com、ツイッターでは @RecordedFuture をご覧ください。