2020 年
夏季オリンピック
脅威評価レポート

2021 年 4 月改訂版（version 2）

CYBER THREAT ALLIANCE

POWERED BY CTA

CTA（Cyber Threat Alliance）は、サイバーセキュリティプロバイダーが加盟する業界初の団体です。その目的は、脅威情報の共有と、高度なサイバー攻撃に対するグローバルな対抗措置の改善にあります。CTA は、サイバー脅威インテリジェンスの共有を通じて、防御の強化、重要インフラのセキュリティ強化、IT システムのセキュリティ、完全性、可用性の向上をサポートします。

CTA は次の 3 つのアプローチでミッションに取り組みます。

1. エンドユーザーを保護：自動化プラットフォームにより、実用的な脅威インテリジェンスの共有、検証、実装をリアルタイムで実現します。

2. 攻撃者の活動を阻止：脅威インテリジェンスの共有により、攻撃者のツールやインフラストラクチャを弱体化させます。

3. セキュリティ全体を強化：インテリジェンスの共有により、メンバー企業のサイバーインシデントへの対応とエンドユーザーの耐障害性を強化します。

CTA は、世界規模で成長を続けており、メンバー企業が共有する情報は、量と質いずれにおいても向上しています。CTA は、さらに安全な未来に向けた情報共有とコラボレーションの強化を目的に、サイバーセキュリティプロバイダーの加盟を歓迎しています。

CTA について詳しくは、https://www.cyberthreatalliance.org をご覧ください。

オリンピックサイバーセキュリティワーキンググループのメンバー

Cisco Talos：
Kendall McKay（主執筆者）、
Ryan Pentney

Fortinet：
Val Saengphaibul、
寺下 健一

NEC Corporation：
角丸 貴洋、
岩田 友臣、打田 貴樹

NETSCOUT：Richard Hummel

NTT：Jeremy Scott

Palo Alto Networks：
林 薫、Ryan Olson、
Brittany Ash

Radware：Daniel Smith

CTA：Neil Jenkins

本書では、CTA メンバー企業である ADT CAPS Infosec、Alien Labs、Anomali、Avast、Check Point、Dragos、Telefonica's ElevenPaths、Ericom、K7 Computing、Juniper Networks、McAfee、Morphisec、OneFirewall Alliance、Panda Security、Rapid7、ReversingLabs、Saint Security、Scitum、SecureBrain、SecurityScorecard、Sophos、SonicWall、Symantec、TEHTRIS、Verizon、VMware が提供する共有データおよび公開された分析結果が使用されています。本書には、CTA メンバーがレビューし、合意された内容が記載されています。

目次

概要

はじめに：2020 年 3 月、日本政府と IOC（国際オリンピック委員会）は、SARS-CoV-2 のパンデミックを考慮し、夏季オリンピックを 1 年延期することに合意しました。現在、夏季オリンピックは、2021 年 7 月 23 日～ 8 月 8 日の開催が予定されています。CTA（Cyber Threat Alliance）のオリンピックサイバーセキュリティワーキンググループ（Olympics Cybersecurity Working Group）は、過去 1 年の脅威トレンドに関する情報、サイバー攻撃の挙動とその戦術の変化、パンデミックを考慮した大会運営方法の調整を鑑みて本書（2020 年オリンピック脅威評価レポート）をレビューし、改訂を行いました。変更点を明確に示すために、改訂版はオリジナルとは別途提供されます。

CTA（Cyber Threat Alliance）は、2020 年日本の東京で開催される夏季オリンピックに影響を与える可能性のあるサイバーセキュリティイベントに対応すべく、情報共有と準備を目的にしたオリンピックサイバーセキュリティワーキンググループ（Olympics Cybersecurity Working Group）を立ち上げました。オリンピックに向けた準備作業として、CTA メンバーは、CTA 初となる脅威評価レポートを共同で作成しました。本書では、東京 2020 オリンピックを取り巻く脅威環境を概説し、東京オリンピック組織委員会への推奨事項を提示します。また、本書はオリンピックに関する CTA メンバーの情報共有を重視しており、サイバーセキュリティの脅威環境に基づくシナリオの計画立案の参考にもなります。

CTA は、オリンピックとその関連組織に最大の脅威となるのは、高度な攻撃能力と過去に経験を持つ国家的犯罪集団であると分析しています。過去の攻撃実績、並外れた技術力、地政的緊張関係から、ロシア、北朝鮮、中国が支援する組織が最大の脅威となる可能性が高いでしょう。一方で、イランについては、オリンピックのサイバー脅威となる可能性は低いと考えられます。イランはサイバー攻撃をグローバルに展開してきた経緯がありますが、東京オリンピックや関連組織を攻撃する戦略的利害はないと分析しています。

どの国際的なイベントでも、地政学要因の理解が重要です。また、時事問題、領土問題、歴史的な緊張関係も、日本に対するサイバー攻撃の動機になります。日本は複数の地域紛争の中心にあり、オリンピック開催国でもあることから、世界が注目する東京を混乱に陥れようとする攻撃者にとって格好の標的となります。

アップデート：大会開催地となる日本は、サイバー攻撃の主な標的になることは明らかですが、開催前の数ヵ月間、さまざまな国がライバル国に攻撃を仕掛けると予想されます。このような攻撃では、選手の身体的 / 精神的に関わる機密情報を収集および処理する各国のオリンピック組織が標的になる可能性が高くなります。攻撃の威力を最大限に高め、ナショナルチームの士気を下げることを目的に、窃取されたデータは試合の直前に公開されると考えられます。この予測は、2015 ～ 2016 年に発生した WADA ハッキングのような攻撃（後述）に基づくものです。攻撃を認識している他の国は、自国が有利になるように攻撃に乗じると考えられます。

国家的犯罪組織はさまざまな作戦を展開する恐れがありますが、最も可能性のある攻撃は、サービス中断や偽情報の拡散であると考えられます。特に想定されるのは、標的型のデータ流出、DDoS（分散型サービス拒否）攻撃、ランサムウェアによるシステム侵害、重要インフラの物理的な攻撃です。CTA の分析では、アンチドーピング機関と専門家、オリンピックの運営 / 物流をサポートするサービス（Wi-Fi ネットワークや発券システムなど）が、最も攻撃リスクが高いとされています。また、観光客や競技の観客、日本政府と参加国の政府、スポンサー企業、サプライチェーンとインフラストラクチャのプロバイダーも標的になる恐れがあります。

アップデート：本書のオリジナルバージョンの公開後、ランサムウェアの危険度は大幅に増しています。サイバー攻撃者は、ネットワーク全体を暗号化する新たな攻撃手法や戦術を採用しています。ランサムウェアを悪用する攻撃者には日和見的にチャンスをうかがう特性があるため、大会開催中、サプライチェーン内のベンダーをはじめとするオリンピック関連組織が標的になる可能性もあります。大会をサポートする組織の中には、提供するサービスのタイプによってはダウンタイムに極めて弱い（特に大会期間中のダウンタイム）組織もあり、手っ取り早く身代金を手に入れたい攻撃者の標的になる恐れがあります。

2020 東京オリンピックを狙うのは、国家的犯罪組織だけではありません。オンラインシステムの利用者が多い観光客はサイバーセキュリティに対する意識が低いことから、サイバー犯罪者の標的にもなります。既に、2020 オリンピック組織委員会は詐欺などのサイバー犯罪に直面しています。

日本ではオリンピックへの準備としてさまざまなサイバーセキュリティの課題に直面していますが、ここ数年、効果的な変更をいくつか行っています。このような取り組みは評価に値しますが、企業や政府を取り巻くサイバーセキュリティの問題はそう簡単に解決できるものではありません。これは、日本だけではなく、サービスの提供や経済を情報テクノロジーに依存する多くの国に共通した課題です。CTA は、オリンピック組織委員会と日本政府に対して、サイバーセキュリティインシデントに関するベストプラクティス、情報共有、連携による計画立案、重要度の高いシステムの定期的なチェックを推奨します。

アップデート：日本は、COVID-19 パンデミック、日本政府がオリンピック中止を検討しているという匿名報道、安部前首相の辞任、日本国民のオリンピック支持率の低さなど、さまざまな国内問題を抱えています。サイバー攻撃者は、このような問題を抱える日本はサイバーセキュリティ対策に注力できず、セキュリティ態勢は弱体化しているため、攻撃のチャンスだと捉えている可能性があります。CTA メンバーを含む、オリンピックのサイバーセキュリティプロバイダーは、脅威とリスクをきめ細かく監視し準備を整えていますが、過去の経験から、セキュリティと耐障害性を確保するには、関連組織すべてが、サイバーセキュリティへの準備と対策を優先的に取り組む必要があることは明らかです。

はじめに

CTA は、サイバーセキュリティ脅威の兆候、インテリジェンス、防御に関する情報共有と、コラボレーションによる問題解決に取り組む企業で構成されます。CTA メンバーは、エンドユーザー保護、攻撃者の阻止、全体的なサイバーセキュリティ強化に向けて協力しています。また、悪意のあるサイバー攻撃の検知を継続して行い、脅威に関する情報を共有するワーキンググループを編成しています。

CTA は、2019 年秋にオリンピックサイバーセキュリティワーキンググループを立ち上げました。このグループは、オリンピック関連アクティビティの情報共有、CTA メンバー間の協力、夏季オリンピックの準備に関わるさまざまな外部ステークホルダーとの協力を開始しました。CTA メンバーのコラボレーションと東京オリンピック組織委員会を支援するために、ワーキンググループは CTA 初となる脅威評価レポートを作成しています。本書では、過去のオリンピックと関連組織を狙った脅威の概要、競技、組織、ステークホルダーを狙う可能性のある攻撃者のレビュー、発生する恐れのある脅威、日本のセキュリティ態勢、そして以上から得た教訓と推奨事項をまとめています。2020 年夏季オリンピックの準備に向けたレビューで活用できるように、本書は東京オリンピック組織委員会に提供されています。

過去の脅威

オリンピックは、過去 10 年にわたってサイバー攻撃者の攻撃対象になってきました。年を追うごとにその攻撃は複雑になり、高度になっています。2008 年以来、オリンピック関連のサイバー脅威の頻度は高まり、巧妙化しています。中でも最も多いのがイベントを中断させる攻撃です。オリンピック開催前に攻撃が開始される事例もありますが、正式に競技が始まると攻撃頻度が高まり、数ヵ月にわたって攻撃が続く可能性もあります。攻撃にはさまざまな TTP（戦術、手法、手順）が使用されますが、フィッシング、スピアフィッシング、ドメインスプーフィング、レンタルボットネットが一般的です。過去の脅威から判断すると、アンチドーピング機関や職員をターゲットにした攻撃が増加しており、電力会社、放送システム、スタジアムの Wi-Fi ネットワークをはじめとする運営 / インフラストラクチャ関連もターゲットになっています。

以下に、過去のオリンピックで発生した脅威をまとめます。大規模な攻撃や大きく報道された攻撃であり、すべてを網羅しているわけではありません。

2008 北京オリンピック

2008 北京オリンピックの開催前および開催中に発生したサイバー脅威は、比較的限られていました。1 日あたり 1,100 ～ 1,200 万件のサイバーアラートが発生したと報告されていますが、いずれも成功していません[1]。また、チケット詐欺が数件検知されました。チケットの販売詐欺を目的にクレジットカード情報を窃取する Web サイトを、米国がシャットダウンしています[2]。

2012 ロンドンオリンピック

2012 ロンドンオリンピックでは、全体的にサイバーセキュリティインシデントはあまり発生しておらず、大きな影響を及ぼす攻撃には至りませんでした。中でも最大の攻撃は、オリンピックを支える電力インフラに対するサイバー脅威であり、これについては信憑性のある証拠が存在します。 報告によれば、開会式の中断を目論む攻撃者により、オリンピック会場の電力システムが 40 分間 DDoS 攻撃を受けました。攻撃は失敗したものの、スタジアムの停電に備えてバックアップシステムが設置されました。また、開幕から 5 日後、ハクティビストがソーシャルメディアで #letthegamesbegin というオペレーションを立ち上げ、オリンピック IT インフラをターゲットに DoS 攻撃を仕掛けようと呼びかけましたが、この攻撃による影響はほとんどありませんでした[3]。

2016 リオデジャネイロオリンピック

2016 リオデジャネイロオリンピックでは、開催前と開催中に、オリンピック関連組織が、IoT ボットネットである LizardStresser による大規模な DDoS 攻撃の標的になりました。ブラジルのオリンピック委員会と IOC は、脅威のリスク低減に取り組んだ結果、攻撃トラフィックは 540Gbps に達したものの、システムの連続稼働に成功しました[4]。CTA メンバーである NETSCOUT Arbor の調査部門である ASERT（Arbor Networks Security Engineering & Response Team）が発表した調査結果によれば、攻撃のほとんどは開催前に発生していますが、開催中も攻撃は続きました。ASERT は、大規模イベントでの DDoS 検知とリスク軽減に積極的に取り組む組織です[5]。また、ハクティビストの脅威も報告されています。

1 「Securing the 2012 Olympics」（英語）：https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics/

2 「Beijing Olympic ticket scam shut down」（英語）：https://www.scmagazine.com/home/security-news/beijing-olympic-ticket-scam-shut-down/

3 「Olympic-Caliber Cybersecurity」（英語）：https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2395/RAND_RR2395.pdf

4 「DDoS Attacks During Rio Olympics Peaked at 540 Gbps」（英語）：
https://news.softpedia.com/news/ddos-attacks-during-rio-olympics-peaked-at-540-gbps-507822.shtml

5 「How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics」（英語）：
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/

2014 年ワールドカップに対するブラジル政府による過剰支出に抗議し、#OpOlympicHacking オペレーションが展開されています [6]。

2016 ～ 2017 年に発生したアンチドーピング組織を狙った攻撃

2016 ～ 2017 年、ロシアによる国ぐるみの薬物検査隠蔽を告発するレポートが提出されました。これに対する報復措置として、ロシアが支援するサイバー犯罪集団は、複数のアンチドーピング組織を標的に大規模な攻撃を仕掛けました。マクラーレンレポートとして知られるこの報告書は、2016 年 7 月に WADA（世界反ドーピング機関）が公開したものであり、ロシア政府による組織的な隠蔽が報告されています。その行為は、2014 ソチ冬季オリンピックの開催前、開催中、開催後に行われました。WADA の報告を受けた IOC は、100 人を超えるロシア選手に 2016 リオオリンピックへの参加を禁止するなど、ロシアに厳しい制裁を加えています。

報復攻撃は 2016 年の半ばから末に始まっており、9 月には WADA から盗んだ機密情報がオンラインで公開されています。公開されたデータには、複数の国の有名選手の医療記録も含まれており、禁止薬物の検査結果が陽性であったにも関わらずリオオリンピックへの参加が認められた選手のデータもありました。WADA のデータ流出の後、ロシアの犯罪集団は、USADA（米国反ドーピング機関）、CCES（カナダ・スポーツにおける倫理センター）、IAAF（国際陸上競技連盟）、FIFA（国際サッカー連盟）の職員、そしておよそ 30 ヵ国の 35 のアンチドーピング機関やスポーツ組織を標的に攻撃を仕掛けています [7]。最終的に、およそ 30 ヵ国のアスリート 250 人の個人情報や医療情報が公開されました [8]。犯罪集団はこのような攻撃の準備として、WADA をはじめとするアンチドーピング機関を装ったドメインを用意し、ネットワークをプローブすることで、従業員にフィッシングメールを拡散しています [9]。

2018 平昌オリンピック

2018 年 2 月 9 日、平昌冬季オリンピックの開会式の前に、大会の混乱と攪乱を目的にネットワークが攻撃されました。攻撃には Olympic Destroyer と呼ばれるワームが使用され、公式 Web サイトのオフライン化、スタジアムの Wi-Fi アクセスの中断、開会式の放送中断が発生しました。その結果、多くの観客が会場にアクセスできなくなり、チケットが発券不能になりました。

Cisco Talos が複数のマルウェアサンプルを分析したところ、攻撃の目的はデータの持ち出しではなく、大会の妨害であったことが判明しています。Cisco Talos によれば、マルウェアはシャドーコピーとイベントログを削除することでマシンを使用不能にし、オペレーティングシステムの標準機能（PsExec[10]、Windows Management Instrumentation（WMI）[11] など）を使って感染を拡大していました [12]。

アップデート：2020 年 10 月 19 日、米国司法省（DOJ）は、2018 年の Olympic Destroyer 攻撃とその他の複数のサイバー攻撃（2015 年と 2016 年に発生したウクライナのパワーグリッドに対する攻撃と 2017 年の NotPetya を含む）の実行犯として、ロシア連邦軍参謀本部情報総局（GRU）職員 6 人を起訴しました [13]。この起訴に関連

6 「2016 Rio Summer Olympic Games Cyberthreat Environment」、Booz AllenおよびCyber4Sight、2016年5月26日（英語）：https://docplayer.net/50042593-2016-rio-20summer-olympic-games-cyberthreat-environment.html

7 「U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations」（英語）：https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

8 同上

9 同上

10 「PsExec」（英語）：https://attack.mitre.org/software/S0029/

11 「Windows Management Instrumentation」（英語）：https://attack.mitre.org/techniques/T1047/

12 「Olympic Destroyer Takes Aim At Winter Olympics」（英語）：https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

13 「Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace」（英語）：https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

して英国政府は、Olympic Destroyer に対する GRU の関与を確認しており、「北朝鮮と中国のハッカーになりすまし、2018 年冬季オリンピック開会式の攻撃を企てた」としています[14]。また、英国政府は、ロシアの GRU 職員は「大会延期の前、今年の夏に東京で開催される予定だった 2020 年オリンピック / パラリンピックの職員や組織に対してサイバー偵察を行っており、大会主催者、物流サービス、スポンサーが標的になっていた」と指摘しています。CTA メンバーは、2020 オリンピックに対する攻撃の標的については、独自には検証していません。

また、ほとんど報道されていないものの、2018 平昌オリンピックではこれ以外にも攻撃が発生しています。その 1 つが Clearsky Security が発見した攻撃であり、攻撃ベクトルとして CVE-2012-0158 を使った RTF ファイルが使用されています[15]。CVE-2012-0158 は、MSCOMCTL.OCX ライブラリに含まれる ListView / TreeView ActiveX コントロールに存在する Microsoft Office バッファオーバーフローの脆弱性です。この脆弱性を悪用することで、細工した DOC ファイルまたは RTF ファイルを使用し、MS Office バージョン 2003 / 2007 / 2010 で任意にリモートコードを実行できます。

この攻撃で標的になったのは、未確認の組織に所属する個人であり、おそらくオリンピックに関心を持っていたと考えられます。攻撃では、「Russian figure skater won the Pyeongchang Winter Olympics in South Korea.doc」（ロシアのフィギュアスケーターが平昌冬季オリンピックで金メダル：ロシア語からの翻訳）という名前の Word ドキュメントが使用されました。このドキュメントを開くと、Icefog APT バックドアに関連するとみられるバックドアコンポーネントがドロップされます。このバックドアは、過去に APAC のさまざまな地域（特に日本と韓国）で発生した攻撃で使用されています。Icefog グループについては、CVE-2012-0158 を悪用した攻撃も確認されています。

2019 年 9 月に発生したアンチドーピング機関に対する攻撃

最近発生したオリンピック関連の脅威については、APT28 / Fancy Bear がアンチドーピング機関を攻撃した証拠が存在します。Microsoft によれば、2019 年 9 月半ばの WADA がロシア人選手のオリンピック参加禁止を発表する前、Strontium という組織が少なくとも 16 のエンティティを標的に攻撃を開始しています[16、17]。ただし、ほとんどは失敗に終わりました。

過去の攻撃者と潜在的な攻撃者

オリンピックと関連組織にとって最大の脅威となるのは、高度な技術力と非常に効果的な攻撃の実績を持つ国家的犯罪集団であると考えられます。このような集団の多くは国から暗黙の許可を得ており、多くの場合、国家の諜報機関の支援や指示で動いているため、通常のサイバー攻撃者には利用できない幅広いリソースが提供され、便宜が図られています。また、地政学要因も、オリンピック開催前の日本の環境に大きな影響力を持っています。というのは、日本は地域的紛争や歴史的対立の中心であり、それがサイバー脅威につながる恐れがあるからです。

過去の経験や風評から、ロシア、北朝鮮、中国が支援する犯罪集団がオリンピックに非常に大きな脅威となることはよく知られていますが、時事問題、領土問題、歴史的緊張も、日本に対するサイバー攻撃の動機になると考えられます。さらに領土問題は、韓国など、サイバー脅威には無関係の国が自国の利益を目的に攻撃を仕掛ける動機にもなり得ます。日本は複数の地域紛争の中心にあり、

14「UK exposes series of Russian cyber attacks against Olympic and Paralympic Games」（英語）：https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

15「Twitter」（英語）：https://twitter.com/ClearskySec/status/968104465818669057?s=20

16「New cyberattacks targeting sporting and anti-doping organizations」（英語）：https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

17「Russian doping scandal: Russia faces ban from all major sports events – Wada」（英語）：https://www.bbc.com/sport/athletics/49805296

オリンピック開催国でもあることから、世界が注目する中、東京を混乱に陥れようとする攻撃者に狙われている可能性があります。

ロシア

APT28 による過去のオリンピック関連の脅威や WADA によるロシア人選手に対する参加禁止処分を考えれば、東京オリンピックと関連組織にとって最大の脅威となるのはロシアだと言えます。現在ロシアは、2019 年 1 月に検査所に虚偽の検査データを提出したとして、国際的な競技会への参加を複数年禁止されています[18、19]。また、制裁措置として、2020 オリンピックでロシア国歌の斉唱は認められず、ロシア選手は五輪旗のもとで参加することになります。ロシアのオリンピック参加が禁止されたのは、今回で 2 回目です。この事による最初のインシデントは、本書でも説明したように、ロシアが支援するサイバー犯罪集団による WADA を標的にした攻撃でした。2 回目の参加禁止にも、同様の反応が見られるかもしれません。

オリンピックの関連組織と個人を狙ったロシアの国家的なサイバー攻撃には複数の前例があり、同様の標的に対して攻撃が仕掛けられる可能性は非常に高いと考えられます。本書でも説明したように、2016 ～ 2017 年、ロシアが支援するサイバー攻撃集団である APT28 は、WADA をはじめとするアンチドーピング機関に対して攻撃を仕掛けました。DOJ（米国司法省）は、この犯罪に関与したとして、複数の GRU（ロシア連邦軍参謀本部情報総局）職員を告発しています[20]。2018 平昌オリンピックの開催中に発生した攻撃にもロシアの関与が疑われており、米国諜報機関の複数の職員も同様の主張を行っています[21]。また、上記で説明したように、最近では Microsoft が、2019 年 9 月のアンチドーピング機関に対する度重なる攻撃は APT28 によるものだとしています[22]。

> **過去の経験や風評から、ロシア、北朝鮮、中国が支援する犯罪集団がオリンピックに非常に大きな脅威となることはよく知られていますが、時事問題、領土問題、歴史的緊張も、日本に対するサイバー攻撃の動機になると考えられます。**

アップデート：2020 年 10 月、米国と英国は、2018 平昌オリンピックに対するサイバー攻撃を画策したとしてロシアを告発し、DOJ は 6 人のロシア人を実行犯として特定しています[23、24]。また、英国の諜報サービスは、夏に東京で開催される予定だった 2020 オリンピック / パラリンピックが延期される前、ロシアの GRU 職員が

18「WADA Executive Committee unanimously endorses four-year period of non-compliance for the Russian Anti-Doping Agency」（英語）：
https://www.wada-ama.org/en/media/news/2019-12/wada-executive-committee-unanimously-endorses-four-year-period-of-non-compliance

19「Russia can't use its name and flag at the next 2 Olympics」（英語）：
https://apnews.com/article/russia-banned-name-flag-olympic-games-a8bd342806883f66152859701d5ae5d4

20「U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations」（英語）：
https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

21「Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say」（英語）：
https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html

22「New cyberattacks targeting sporting and anti-doping organizations」（英語）：
https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

23「UK exposes series of Russian cyber attacks against Olympic and Paralympic Games」（英語）：
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

24「Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace」（英語）：
https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

2020 オリンピックの職員や組織に対してサイバー偵察を行ったことを明らかにしています。この偵察では、大会主催者、物流サービス、スポンサーが標的になりました [25]。

> **ロシアには、オリンピックに関連する組織や個人を標的にした攻撃の前例があるだけでなく、最新の WADA に対する攻撃を考えると、ロシアが東京オリンピックの開催前や開催中に攻撃を仕掛けてくる可能性が高いといえます。また、最近のロシアの行動を考えれば、大会をサポートするベンダーのサプライチェーンを標的にする可能性もあります。**

このような前例を考えれば、ロシアには、屈辱や不公平感の報復として、標的を絞った攻撃を仕掛ける傾向があります。ロシアには、オリンピックに関連する組織や個人を標的にした攻撃の前例があるだけでなく、最新の WADA に対する攻撃を考えると、ロシアが東京オリンピックの開催前や開催中に攻撃を仕掛けてくる可能性が高いといえます。APT28 によるこれまでの攻撃は、APT28 による犯行であることが明らかな事例が多い一方で、他の国家による犯罪組織を装ったものや素性を明かさないものもあります。したがって、今後のオリンピックには両方の形態の脅威が発生すると想定されます [26]。

アップデート：ロシアに重要なサプライチェーンを攻撃する能力があることは、実証されています。2020 年末、FireEye と Microsoft は、「世界各国政府機関と多数の民間企業が、SolarWinds Orion 製品のバックドアを悪用したセキュリティ侵害の被害に遭う恐れがある」と公表しました [27、28]。ホワイトハウスは 2021 年 4 月 15 日、この攻撃の背後には、ロシアの対外情報庁（SVR：別名 APT29、Cozy Bear、The Dukes と呼ばれるサイバーセキュリティ研究組織）が存在することを発表しました [29]。多数のベンダーがオリンピックをさまざまな側面からサポートすることを考えると、同様の手口で攻撃が仕掛けられる可能性は高いと言えます。4 月 15 日の米国政府の発表では、「SolarWinds をはじめとする企業に対する SVR の攻撃は、サプライチェーンのエクスプロイトを介して世界中の企業が標的になるリスクを示している」と指摘されています [30]。米国の金融機関に対するロシア証券の新たな購入制限、ロシアのテクノロジー企業 6 社の指定、追加の制裁措置、ロシア外交官の国外退去、ロシアのサイバー攻撃に関連する技術情報の開示など、米国政府高官が 4 月にどのような対応を行うかは不明ですが、米国、オリンピック、その他の組織を狙ったロシアのサイバー攻撃を阻止する構えです。

25「UK exposes series of Russian cyber attacks against Olympic and Paralympic Games」（英語）：
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

26「Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say」（英語）：
https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html

27「Customer Guidance on Recent Nation-State Cyber Attacks」（英語）：
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

28「Unauthorized Access of FireEye Red Team Tools」（英語）：
https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

29「FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government」（英語）：
https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

30 同上

地政学的側面として、ロシアと日本には北方四島を巡る領土問題が存在します。緊張が高まれば、日本のロシアに対する脅威環境はさらに複雑になり、東京オリンピックでのサイバー攻撃の動機になる可能性もあるでしょう。

北朝鮮

2020 東京オリンピックに関連するサイバー攻撃に北朝鮮が関与したとする報告はないものの、北朝鮮は日本と敵対関係にあり、巧妙で標的型の攻撃を行う技術力を持っていることから、オリンピックの脅威だと考えることができます。北朝鮮が支援するサイバー犯罪集団は、銀行や暗号通貨交換所から数億ドルを強奪するなど、非常に悪質な攻撃で利益を上げています[31]。また、金銭目的のサイバー攻撃だけでなく、スパイ行為も行っています。これには、2013 年に発生したトロイ作戦と呼ばれる韓国に対する妨害および破壊的攻撃、2017 年に発生した WannaCry ランサムウェア攻撃、2014 年の Sony Pictures に対する攻撃があります。以上の攻撃は、複数の国の幅広い業種が標的となったことから、この犯罪集団は高い技術力とグローバル規模での攻撃能力を持っていることがわかります。

アップデート：米国政府は、北朝鮮によるサイバー攻撃を継続的に監視および諜報活動を行っていることから、北朝鮮を大きな脅威として認識しています。2021 年 2 月、DOJ は、Sony Pictures と WannaCry 攻撃から派生したグローバル規模のサイバー攻撃について、3 人の北朝鮮人を告訴しました[32]。北朝鮮は、国家安全保障の資金源としてサイバー攻撃を何度も利用しており、政府上層部が支持し、優先的に取り組む攻撃兵器の配備に関する重要事項となっています[33]。

第二次世界大戦の前後に発生した北朝鮮と日本の緊張関係は、2020 東京オリンピックを前にさらなる脅威をもたらしています。過去 20 年にわたって散発的に国交正常化が試みられてきましたが、ほとんどが失敗に終わっています。

北朝鮮が支援するサイバー犯罪集団は、おとりドキュメントを使ったメールスプーフィング、水飲み場型攻撃、サプライチェーンの侵害など、さまざまな感染手法を駆使します。最近では、MacOS とモバイルアプリ向けのカスタムツールを開発しており、その技術力は増していると言われています。また、このような犯罪集団、特に北朝鮮の支援を受けるラザラスグループは、身元特定を免れるために、ネットワーク防御やセキュリティソフトウェアを回避する難読化手法を使用しています。

中国

中国は、サイバー犯罪集団が日本企業を攻撃した前例があり、その高度な技術力や日中の緊張関係から考えると、東京オリンピックの脅威になると言えます。中国が関与する複数の集団は日本の組織に対して繰り返し攻撃を行っていることから、中国が支援するサイバー攻撃集団にとって日本は最優先の攻撃対象の 1 つです。特に APT10 は、このような不正行為について複数の国から非難されています。2018 年 12 月、FBI は、APT10 に関与する 2 人を、日本企業を標的にしたスパイ行為で告発しました[34、35]。

31 「North Korean Hackers Have Raked in $670 Million Via Cyberattacks」（英語）：https://www.forbes.com/sites/leemathews/2019/03/11/north-korean-hackers-have-raked-in-670-million-via-cyberattacks/#7a674c807018

32 「3 North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe」（英語）：https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

33 「UN experts: North Korea using cyber attacks to update nukes」（英語）：https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33

34 「Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information」（英語）：https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

35 「Japan condemns China-based cyberattacks, urges Beijing to take 'responsible' action」（英語）：https://www.scmp.com/news/asia/east-asia/article/2179072/japan-condemns-china-based-cyberattacks-urges-beijing-take

アップデート：2020 年に登場した中国の APT により、日本を標的に、中国が国家的に支援するサイバー攻撃が改めて注目されています。Palmerworm（別名 Black Tech）は、2019 ～ 2020 年に発生した攻撃の対象の中に、日本のエンジニアリング企業が含まれていたと報告されています [36]。CTA メンバーによると、このグループは 2020 年 10 月から頻繁にマルウェアを更新しています。このグループは日本企業 3 社のセキュリティを侵害しましたが、その 1 社はオリンピックに関連する企業でした。

中国と日本には歴史的な緊張関係と領土問題が存在し、サイバー脅威の動機になっています。また、2020 東京オリンピックが近づくにつれて、脅威環境の緊張は高まっています。

中国が支援する攻撃集団は、幅広いマルウェア（カスタムツールとオープンソースツール）を駆使してホストを侵害し、ネットワークに潜伏します。そして攻撃開始までネットワークを偵察し、標的を綿密に絞り込むのです。APT10 をはじめとする多くの犯罪集団は、スピアフィッシングメールを使い、マネージドサービスプロバイダーを介してネットワークにアクセスします。ほとんどの国家支援の犯罪集団と同様に、中国が支援する犯罪集団も高度な技術力を持っており、世界規模で大きな脅威となります。

アップデート：2021 年 3 月、Microsoft は、HAFNIUM というグループが、オンプレミスの Exchange Server ソフトウェアに関する未知のエクスプロイトを使った侵入に関与していることを発表しました [37]。Microsoft の調査によれば、HAFNIUM は、中国を拠点とする国家支援のグループです。主に、米国のさまざまな業界の企業を標的にしており、これには感染性疾患の研究所、法律事務所、高等教育機関、防衛関連企業、政策シンクタンク、NGO が含まれます [38]。HAFNIUM は、感染サーバーに Web シェルをインストールし、データ窃取などを行います。Microsoft がパッチのリリースと脆弱性報告を行う前に、サイバーセキュリティ研究者は、HAFNIUM と複数の APT グループ [39、40] による脆弱性をターゲットにした攻撃が増加していることを確認していました。攻撃者には、HAFNIUM 以外に、中国を拠点とする国家支援のグループが含まれると考えられています。この攻撃には、ほとんどが広範囲に広がり、ほぼ無差別に脆弱なサーバーのディスカバリ / エクスプロイトを自動実行するという特徴があります。オリンピック、日本政府、大会のスポンサーや関連組織が運営するシステムに影響を及ぼしたかどうかは不明ですが、中国を拠点とするグループの戦術、手法、手順が非常にアグレッシブであり、大規模な攻撃へと変化したことを示しています。オリンピックのサイバーセキュリティを担当する組織は、このようなアクティビティをしっかり追跡し、リスクを軽減する必要があります。また、CTA メンバーは、中国が支援するグループは関与していないと見られるものの、脆弱な Exchange Server を狙ったランサムウェアを追跡しています。

イラン

イランは、過去数年にわたってサイバー攻撃能力を高めており、Web サイトの改ざん、DDoS 攻撃、PII（個人情報）の窃取、ワイパー型マルウェア攻撃などを展開しています [41]。複数の悪名高い APT や攻撃集団はイランによるものであり、米国政府やサイバーセキュリティ研究組織

36「Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors」（英語）：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

37「New nation-state cyberattacks」（英語）：https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

38「HAFNIUM targeting Exchange Servers with 0-day exploits」（英語）：https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

39「Exchange servers under siege from at least 10 APT groups」（英語）：https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

40「Microsoft Exchange Server Attack Timeline」（英語）：https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/

41「Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad」（英語）：https://www.us-cert.gov/ncas/alerts/aa20-006a

は最新の動向を詳細に追跡しています。このように悪評高いイランですが、オリンピックや関連組織を狙ったサイバー攻撃については、戦略的な関心は持っていないと考えられます。本書で解説したように、日本には、イラン以外の国との地政学的関係がありますが、イランと日本には歴史的に緊張はなく、比較的友好な関係が維持されています[42]。さらにイランには、そのような攻撃を仕掛ける明確なメリットがありません。CTA は、イランによるオリンピック関連の脅威は低いと分析しています。ただし、イランと米国には、2019 年末から 2000 年のはじめに発生したインシデントに起因する緊張関係があるため、米国やその同盟国に対する攻撃戦略を見直す可能性は存在します。CTA はオリンピック組織委員会に対して、イランのサイバー攻撃に対して継続的に注意を払うことを要請します。

韓国

韓国と日本には、複雑な歴史と現在の外交問題に起因する緊張関係がありますが、韓国がオリンピックや関連組織に対してサイバー攻撃を仕掛ける可能性は低いと分析しています。韓国が支援するサイバー攻撃や犯罪集団の存在は知られていませんが、国際関係がサイバー攻撃に繋がる事例も多いため、両国関係を注視すべきです。その緊張関係は、第二次世界大戦前にまで遡ります。現在、両国間には、貿易摩擦と長期化する領土問題が存在します。

ハクティビストとサイバー犯罪者

ハクティビストとサイバー犯罪者も、本書で解説したさまざまな理由から、オリンピックの開会前、開催中、閉会後に攻撃を仕掛ける可能性があります。メディア報道や世界の注目を集めたい日和見的なハクティビストは、オリンピックを効果的な舞台として捉えるかもしれません。ソーシャルメディアによる悪質な活動や攻撃をオリンピックで行う方が、知名度の低いイベントで行うよりも世間の関心を引くことができるからです。同様に、サイバーセキュリティ対策をほとんど講じていない無防備な観光客が大勢集まるオリンピックは、サイバー犯罪者にとって絶好の攻撃機会となります。

アップデート：ここ数ヵ月、特にランサムウェア攻撃が増加しています。これは、COVID-19 パンデミックのさなか、医療関連組織の脆弱性を悪用しようとするものです。ランサムウェアを悪用する攻撃者には日和見的にチャンスをうかがう特性を持っているため、開催中の大会と、サプライチェーン内のベンダーをはじめとするオリンピック関連組織が標的になる恐れもあります。オリンピック支援組織は、提供するサービスのタイプによっては、病院と同様にダウンタイムへの耐性が低く、資金不足が原因でサイバーセキュリティチームが整備されていない可能性があります。

> **ランサムウェアを悪用する攻撃者には日和見的にチャンスをうかがう特性を持っているため、開催中の大会と、サプライチェーン内のベンダーをはじめとするオリンピック関連組織が標的になる恐れもあります。**

42「Explainer: Why is Japan's Abe going to Iran? What can he accomplish?」（英語）：
https://www.reuters.com/article/us-iran-japan-abe-explainer/explainer-why-is-japans-abe-going-to-iran-what-can-he-accomplish-idUSKCN1T80U9

標的になる可能性が高い攻撃対象

選手

ファンがいる有名選手がオリンピックに参加すると、オリンピックの人気が高まり収益も生まれます。したがって、オリンピック選手は格好の標的です。これには前例があり、2016 年に発生した WADA のセキュリティ侵害もその 1 つです。2016 年の夏、ロシアのサイバー犯罪集団が WADA からオリンピック選手の薬物検査結果を盗み、インターネットで公開しました。データには、機密性の高い情報や他者には知られたくない情報が含まれていました。たとえば、米国テニス界のスター選手であるセリーナ・ウィリアムズ、ビーナス・ウィリアムズ、米国の金メダリストであるシモーネ・バイルズは、禁止薬物の陽性反応が出たにもかかわらず、2016 リオオリンピックへの参加が認められていました。この攻撃が WADA の 2016 年 7 月のレポートへの報復であったことはほぼ明らかです。WADA のレポートでは、2014 年冬季オリンピックの開会前、開催中、閉会後にロシアが行った薬物検査管理方法が非難されていました。このレポートを受けて、100 人以上のロシア選手が 2016 夏季リオオリンピックの出場停止処分を受けています。したがって、このデータ流出には、ロシア以外の選手の信用を損ねるといった目的があったと考えられます。

アンチドーピング機関と専門家

アンチドーピング機関やその専門家もサイバー攻撃の標的になるリスクは高いといえます。ロシアは、WADA を大規模なデータ流出に陥れただけでなく、米国や英国のアンチドーピング機関や CCES（カナダ・スポーツにおける倫理センター）をはじめとする関連組織にも攻撃を試みています。また、IAAF や FIFA などの競技連盟の職員も標的になっています。不正行為の告発や国際舞台での失態は、報復としてサイバー攻撃を仕掛ける動機になる可能性が高くなります。

アップデート：2021 年 2 月、WADA は、欧州刑事警察機構（Europol）との覚書（MOU）に署名しました。これは、スポーツでのドーピング対策における相互協力に向けて、フレームワークを確立し取り組みを推進することを目的とします。このパートナーシップには、WADA を標的にしたサイバー攻撃に関する組織間の連携を高める効果があります [43]。

イベント運営、物流、重要インフラ事業者

オリンピックでは、競技の運営や物流に影響を与える目的で攻撃が仕掛けられることがあります。2018 年冬季オリンピックのように、発券システム、Wi-Fi ネットワーク、コミュニケーション、放送をシャットダウンすれば、会場の観客はもちろんグローバル規模で影響が発生します。特に、選手村、競技会場、日本の一般市民を支えるエネルギーや交通に関連する重要インフラも格好の標的です。攻撃が成功すれば大規模な混乱に陥り、すべてがシャットダウンしないとしても、オリンピックイベントは開催不能に陥るでしょう。最近になって報告された三菱電機で発生した大規模なセキュリティ侵害についても CTA では注目しています [44]。三菱電機は、日本で防衛 / 重要インフラ事業を請け負う最大手の 1 つです。オリンピック開催中の破壊的攻撃手段として、このようなサイバーセキュリティ侵害が発生する恐れがあります。

アップデート：イベントでは物理的な観戦と競技に制限が設けられる可能性が高いため、ブロードキャストやストリーミングの需要がある程度増えると予想されます。現在のところ、通常を大幅に上回る需要が発生するかどうかは不明です。パンデミックを受けて移動が制限され

43「WADA investigators strengthen cooperation with Europol」（英語）：
https://www.wada-ama.org/en/media/news/2021-02/wada-investigators-strengthen-cooperation-with-europol

44「Mitsubishi Electric discloses security breach, China is main suspect」（英語）：
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

るため、観戦者や観光客が利用する重要なインフラストラクチャ（輸送手段など）の需要は減ると考えられています。日本政府と民間企業は、重要度の高いインフラストラクチャ全体を警戒し、セキュリティと耐障害性を保持することを推奨します。

> **大きな影響を及ぼしてメディアの関心を最大限に集めたいなど、攻撃者の動機によっては、オリンピック開催中に攻撃が仕掛けられる可能性があります。オリンピックの開会式と閉会式は観客や視聴者が最も多いイベントです。**

また、POS システムも危険にさらされます。POS システムは、クレジットカードやデビットカードの情報窃取を目論むサイバー犯罪者の主な標的です。近年、このような攻撃が増加しており、オリンピックのような国際イベントでは商取引が増加することから、2020 東京オリンピックでも同様の攻撃が発生する可能性が高いとみられます。特に、オリンピックは世界中が注目するイベントであり、国は威信をかけて開催するため、オリンピックの混乱はホスト国にとって不名誉となります。

また、オリンピック開催中にインフラストラクチャをサポートする企業も、攻撃の標的になる可能性があります。たとえば、ATOS はクラウドサービスを提供する MSSP（マネージドセキュリティサービスプロバイダー）であり、長年にわたる IOC のワールドワイド IT パートナーです。オリンピックの IT とマネージドインフラストラクチャソリューションを提供する ATOS は、2018 平昌オリンピックで攻撃を受けました。その後、オリンピック開催前の数ヵ月にわたり、同じ集団が仕掛けた Olympic Destroyer マルウェアの攻撃にも遭っています[45]。この犯罪集団が、ATOS を介してオリンピックのインフラストラクチャにアクセスできたかどうかは、明らかになっていません。ただし、標的のサプライチェーンパートナーにアクセスするサイバー攻撃が最近増加していることから、インフラストラクチャプロバイダーとの緊密な連携が重要です。本書の作成に携わった複数の CTA メンバーがオリンピック組織委員会にインフラストラクチャを提供していますが、このようなシステムの脅威を認識しています。CTA は引き続き警戒を怠ることなく、メンバー企業と組織委員会で情報交換を行います。

アップデート：2020 年末、SolarWinds のアップデートプロセスを悪用したサプライチェーン攻撃が発覚しました。これは、類似した TTP を使用して、大会関連インフラストラクチャの破壊や中断を目論む犯罪者のブループリントになる可能性があります。ただし、SolarWinds サプライチェーン攻撃に関与する人物が、破壊的攻撃を実行した、または実行を計画したかどうかは不明です。

大きな影響を及ぼしてメディアの関心を最大限に集めたいなど、攻撃者の動機によっては、オリンピック開催中に攻撃が仕掛けられる可能性があります。オリンピックの開会式と閉会式は観客や視聴者が最も多いイベントであり、前回の夏季オリンピック（2016 リオデジャネイロ）の開会式の視聴者は 3,000 万人、閉会式は 1,500 万人にのぼりました[46、47]。また、2018 冬季オリンピックの開会式を中断しようとした前例もあります。

アップデート：今後、COVID 検査またはワクチン接種の追跡または報告を行うデジタルインフラストラクチャ（COCOA など）の登場が予測されます。このようなアプ

45「Atos, IT provider for Winter Olympics, hacked months before Opening Ceremony cyberattack」（英語）：
https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-malware-peyongchang/

46「TV Ratings: Olympics Opening Ceremony in Rio Falls From London 2012」（英語）：
https://variety.com/2016/tv/news/olympics-opening-ceremony-ratings-rio-fall-london-1201831995/

47「TV Ratings: Olympics Closing Ceremony Viewership Down Sharply From London 2012」（英語）：
https://variety.com/2016/tv/news/tv-ratings-olympics-closing-ceremony-ratings-down-1201842009/

リの目的は、接触追跡情報の共有にあります[48]。このようなインフラストラクチャが標的になれば、東京や周辺地域の公衆衛生を正確に評価する能力が低下しかねません。その結果、病院の負担は増大し、選手や観客の安全が損なわれます。ワクチン接種の証明書は、デジタル版に加えて書面でも取得し、携帯することが推奨されます。

観光客と観客

無防備な観光客と競技の観客は、十分なサイバーセキュリティ対策を講じておらず、脅威に関する十分な情報も持っていないことが多いため、簡単にサイバー攻撃の標的になってしまいます。海外旅行者には固有の課題があります。スマートフォン、タブレット、ラップトップといった幅広いデバイスで機密性の高いデータを持ち歩いています。また、ホテル、カフェ、スタジアムの公衆 Wi-Fi は暗号化されてないことが多く、個人のアカウント情報や機密情報を窃取するサイバー犯罪者の標的になります。特に、海外旅行者はデータ通信料を節約しようと公衆 Wi-Fi を使用する頻度が高まることを考えると、これは難しい問題です。

同様に、Bluetooth 接続にも、盗聴、データ窃取、デバイスの乗っ取りの危険があります。一般的に、政府は検問などでセキュリティ対策を強化するため、旅行者のデータが流出する危険も高まります。たとえば、セキュリティサービスが検査のためにデバイスを差し押さえ、情報収集を目的に悪意のあるソフトウェア（スパイウェアなど）をインストールする可能性があります。

アップデート：2021 年 3 月 20 日、組織委員会、東京都、日本政府は、COVID-19 パンデミックを考慮し、海外からのオリンピック観戦者の入国を許可しないことを IOC と IPC に通達しました[49]。東京の組織委員会によれば、大会の入札時、780 万人分の観戦チケットが用意され、そのうち 10 ～ 20% は海外からの観客が購入すると予想されていました[50]。4 月には、試合の観戦を許可する人数について討議される予定です[51]。上記で述べた、海外からの入国者を対象としたセキュリティ脅威については状況が変わっていますが、日本在住者の観戦については、引き続き自己所有のデバイスのセキュリティ保護を怠らないようにする必要があります。チケットの払い戻しを担当するオリンピック主催者は、返金を狙ったスキャムに注意し、リスクを軽減しなくてはなりません。チケットを購入した海外在住者は、スキャムとフィッシングメールに注意すべきです。

日本とパートナー国のサイバーセキュリティ組織と職員

サイバーセキュリティ対策を提供および管理する開催国の組織や政府高官も攻撃対象になります。ただし、CTA は、サイバー攻撃の標的になる可能性は低いと分析しています。というのは、上記で説明した攻撃対象の方が、サイバーセキュリティ対策が不十分であるという点で攻撃しやすいからです。日本とパートナー国のサイバーセキュリティ機関は標的になりにくいとはいえ、攻撃が成功すれば、その被害はより大きくなるでしょう。同様に、政府の職員、特にサイバーセキュリティの担当者は、

48「Japan's COVID-19 app failed to pass on some contact warnings」（英語）：
https://www.reuters.com/article/us-health-coronavirus-japan-app/japans-covid-19-app-failed-to-pass-on-some-contact-warnings-idUSKBN2A31BA

49「Statement on Overseas Spectators for the Olympic and Paralympic Games Tokyo 2020」（英語）：
https://tokyo2020.org/en/news/statement-on-overseas-spectators-for-the-olympic-and-paralympic-games-tokyo-2020

50「Spectators From Overseas Are Barred From Tokyo Olympics」（英語）：
https://www.nytimes.com/2021/03/20/world/asia/tokyo-olympics-spectators.html

51 同上

標的になる可能性は低いものの、特定の個人を狙う標的型攻撃を受ける可能性がないとは言えません。このタイプの攻撃には高度な技術が必要となるため、国家支援の犯罪集団が関与すると考えられます。

その一例が、2016 ～ 2017 年に発生したロシアによるアンチドーピング機関に対する攻撃です。IAAF と FIFA の幹部から、キーログ、複数のドキュメント、機密情報が盗み出されました。標的となったのは、アンチドーピング機関の幹部が使用したコンピュータやアカウントでした[52]。組織内で高い地位にあり、重要なデータにアクセスしているという点で、標的になるのはほぼ確実でした。

オリンピックのスポンサー企業 / 関連企業

公式スポンサー企業や関連企業も攻撃の標的になり得ます。大義を推し進め、特定の問題 / 不平不満に注目を集めようとするハクティビスト集団や個人にとって、このような企業は格好の標的です。特定の組織を狙った直接攻撃よりも、ソーシャルメディアや偽情報が使用される可能性が高いと考えられますが、直接攻撃の可能性も無視できません。具体的には、特定企業のボイコットがあります。これは、過去に米国で前例があります。2017 年、国歌斉唱で起立しなかった選手の権利を訴え、NFL スポンサー企業のボイコットがソーシャルメディアで呼びかけられました。オリンピックは世界的なイベントであり、関連企業への攻撃やソーシャルメディアでの批判は国際的な注目を集めます。この点で、オリンピックのスポンサー企業や関連企業が攻撃の標的になる可能性は高いと分析しています。

想定される脅威

データ流出と偽情報

データ流出は、混乱を引き起こす効果的な方法の 1 つです。また、被害者に壊滅的な影響を及ぼしかねません。近年、サイバー攻撃者によるハッキングとデータ流出が多発しています。その目的は、脅迫や強要によって犠牲者の情報を引き出すことや、単に大衆に不平不満を抱かせることにあります。注目すべきデータ流出としては、米国国務省の外交公電の流出（機密性の高い情報が流出）[53]、2015 年、映画『The Interview』の公開阻止を目論んだ攻撃者による Sony Pictures Entertainment のメール流出[54]、2016 年、ジョン・ポデスタのメールハッキング（大統領選に出馬するクリントン陣営と民主党全国委員会の間の私的なやりとりが流出）[55] などがあります。

> **オリンピックは世界的なイベントであり、関連企業への攻撃やソーシャルメディアでの批判は国際的な注目を集めます。この点で、オリンピックのスポンサー企業や関連企業が攻撃の標的になる可能性は高いと分析しています。**

52「U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations」（英語）：https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

53「United States diplomatic cables leak」（英語）：https://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak

54「Sony Pictures hack」（英語）：https://en.wikipedia.org/wiki/Sony_Pictures_hack

55「Podesta emails」（英語）：https://en.wikipedia.org/wiki/Podesta_emails

デマを信じ込ませようとする偽情報も、近年増加しています。また、偽情報とプロパガンダがデータ流出と並行して行われることも多々あります。2016 ～ 2017 年、ロシアがアンチドーピング機関に対して行った攻撃では、一部の WADA の文書が改ざんされた状態で流出しました。米国司法省によれば、窃取 / 流出した情報の一部には、アンチドーピング機関の所見に対してロシア政府が使用したテーマを立証する投稿が見つかっています [56]。攻撃者は、盗んだデータを依頼主に提供するためにソーシャルメディアで攻撃を仕掛け、公開された記事を拡散することで、攻撃効果を最大限に高めようとしました。この事件では、ロシアに有利になるように仕向けると同時に、選手やアンチドーピング機関の職員の信用を損ねる内容が投稿されました。

オリンピック関連やそれ以外で発生した攻撃のいずれにおいても偽情報とデータ流出が増加していることを考えると、2020 東京オリンピックの開会前、開催中、閉会後に同様の攻撃が発生する可能性は高いとみています。WADA による最新の処分でロシアはオリンピック参加が禁止されたため、ロシアがこのような攻撃を仕掛ける可能性は高いでしょう。こういった攻撃の有効性を認識している国はロシア以外にも存在することは間違いなく、偽情報やデータ流出は国家が支援する攻撃集団にとって有効な攻撃手段だと言えます。

アップデート：大会の開催状況に関する虚偽の情報が既に広まっており、2020 年 1 月にはソーシャルメディアに大会中止の記事が投稿されました [57]。パンデミックの現状を考えると、大会に関する流言は今後も増える見通しであり、ソーシャルメディアで簡単に拡散する可能性があります。CTA は組織委員会に対して、ソーシャルメディアパートナーと緊密に協力し、大会に関する流言をできるだけ早期に特定および排除するとともに、公式アカウントから明確なメッセージを発信することを提言します。

中断攻撃

最近、オリンピック開催中に発生した破壊的攻撃の一例が、2018 平昌オリンピックのサイバー攻撃です。中断攻撃は、発券システム、POS システム、Wi-Fi および放送ネットワーク、さらには公共の交通機関、電気、ガス、水道などの重要インフラで使用されるサービスの中断を目的とします。このような攻撃は、サービスの大規模な停滞や混乱を招きます。また、サービスの中断によって金銭を得ようとする攻撃者は、ランサムウェアも使用します。米国では、政府機関を標的にしたランサムウェア攻撃が多発していることから、日本の政府機関やオリンピック関連組織もターゲットになる可能性があります。このような攻撃が発生すると、重要箇所のオリンピック関連 IT システムが稼働不能に陥ります。

過去のオリンピックでは、オリンピック関連組織を標的にした DDoS 攻撃もいくつか発生しています。さらに、ハクティビストのメール送信による DDoS 攻撃が、FIFA ワールドカップ、コモンウェルスゲームズ、ラグビーワールドカップといった国際的なスポーツイベントでも発生しています。こういった過去の攻撃を踏まえて、CTA メンバーは DDoS 攻撃やオリンピックを直接狙った攻撃が発生する可能性を考えています。また、関連組織や、さらには一般的なクラウドサービス [58] を標的にし、アプリケーションを中断させる恐れもあります。

56「U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations」（英語）：https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

57「False rumors of Tokyo 2020 Olympic cancellation swamp social media despite denials」（英語）：https://mainichi.jp/english/articles/20200131/p2a/00m/0sp/010000c

58「DDoS Attacks Target Amazon, SoftLayer and Telecom Infrastructure」（英語）：https://threatpost.com/massive-ddos-amazon-telecom-infrastructure/150096/

アップデート：CTA メンバーは、企業スポンサーなどの関連組織（銀行、金融サービス、保険などの大企業）は、DDoS 攻撃の標的になり、大損害を被る危険があることを強調します。

サイバー犯罪

オリンピックでは、上記のサイバーセキュリティ攻撃に加えて、規模が小さい脅威も発生しています。特に、オンライン犯罪率の高いブラジルのような国では、ATM カードのスキミングや POS マルウェアが日常的に発生しています。2019 年末、悪名高いバンキングマルウェアである Emotet が再び登場し、特に日本で感染が拡大しました[59]。11 月には、2020 東京オリンピックの関連組織に政府が注意喚起を行っていますが、オリンピックを前に Emotet による打撃に関する政府の懸念が示されています[60]。

アップデート：2021 年 1 月、世界中の法執行機関と司法当局が Emotet ボットネットの無害化を行いました[61]。CTA メンバーは、引き続きボットネットの状態を監視しています。警察庁（NPA）は、法執行機関との協力を発表しており、ISP、ICT-ISAC、JPCERT/CC など複数の組織と連携して、日本国内の Emotet ボットネット被害者への通知を行っています[62]。Emotet の脅威は低下したものの、Trickbot をはじめとするバンキングを狙ったトロイの木馬を使ったネットワークアクセスやランサムウェアなどの攻撃が懸念されます。

オンライン詐欺

過去のオリンピックでは、チケット詐欺が多発しました。その多くは、詐欺 Web サイトを使った支払の認証情報および PII の窃取を目的としていました。また、人気の高いオリンピック関連 Web サイトのスプーフィングも多発しています。悪意のあるサイトに誘導し、個人データの窃取やマルウェアのダウンロードを行うものです。さらに、サービス、旅行、ホテル宿泊の無料提供を約束する偽の賞品やオファーもあります。このような攻撃には、フィッシングメールや、オリンピック関連のポップアップ広告が使用されます。攻撃者は、詐欺の取引に誘導し、情報を窃取しようとします。2020 東京オリンピックでは、既にフィッシング攻撃が発生しています。組織委員会や関連組織を装った偽メールが配信されています。たとえば、Special Olympics of New York のメールサーバーがセキュリティ侵害され、過去に寄付をした人にフィッシングメールが送信されました[63]。

アップデート:サイバー攻撃者は、「オリンピック」ブランドをさまざまな方法で悪用し、日本だけでなく世界から大会を観戦する観客とファンを標的にする可能性があります。大会の人気を悪用した手口としては、不正なスコア配信、偽のチケット、選手との会合、選手に関する扇情的なニュースの限定配信、無料チケットなどがあります。このような攻撃は大会に直接的な影響を及ぼさないものの、オリンピックブランドのイメージダウンにつながります。CTA メンバーは、スポンサー、政府職員、セキュリティプロバイダーに対して、キーワードが登録されたドメインの監視、必要に応じて停止またはブロックを行うアクションプランの立案を推奨します。日本政府とオリンピック組織委員会は、レジストリおよび主要なセキュリティプロバイダーと連携し、詐欺行為の影響を最小限に抑制するプロセスを整備する必要があります。

59「TrickBot Expands in Japan Ahead of the Holidays」（英語）：
https://www.darkreading.com/threat-intelligence/trickbot-expands-in-japan-ahead-of-the-holidays/d/d-id/1336510

60「Emotet computer virus spreading in Japan, Suga warns」（英語）：
https://www.japantimes.co.jp/news/2019/11/28/national/emotet-computer-virus-spreading-japan-warns-official/

61「WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION」（英語）：
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

62「マルウェアに感染している機器の利用者に対する注意喚起の実施について」：https://www.npa.go.jp/cyber/policy/mw-attention.html

63「Special Olympics New York Hacked to Send Phishing Emails」（英語）：
https://www.bleepingcomputer.com/news/security/special-olympics-new-york-hacked-to-send-phishing-emails/

ハクティビズム

ほとんどのハクティビストの活動では高度な手法は使用されないものの、攻撃が成功すれば大きな被害が発生します。ハクティビストの攻撃には、特定の企業の組織的なボイコット、Web サイトの改ざん、DDoS 攻撃、注目を集める大規模なデータ流出などがあります。

無線ネットワーク

観光客や競技の観客が流れ込むと、東京内外でモバイルデータアクセスのニーズが高まるため、犠牲者が増える可能性があります。日本の通信プロバイダーは、サービスが不十分だった地域でのモバイルアクセスポイントの増設など、モバイルデバイスの使用増加に備えていますが、PII の窃取や Man-in-the-Middle（中間者）攻撃を目的に偽の Wi-Fi ネットワークを設置しようとする攻撃者も存在します。このようなネットワークの名前には、地名、観光地、オリンピック関連の名称が使用されている可能性があります。観光客は、通信料金やローミング料金を払わなくてもよい無料の Wi-Fi ネットワークに接続しますが、セキュリティ保護されていないネットワークは、標的をより脆弱にしてしまいます。

他の国際イベントに向けた下準備でも、このような攻撃が既に発生しています。WADA 攻撃に関するロシアに対する米国司法省の起訴状によると、2 人の GRU 職員がリオデジャネイロに行き、アンチドーピング機関の職人が使用する Wi-Fi ネットワークを攻撃したとしています。そして、IOC 職員の認証情報を入手し、医療情報やアンチドーピング関連情報が格納された WADA のデータベースに不正アクセスしました[64]。

これに関連する事件が、2016 年に発生しています。アンチドーピング機関である USADA の幹部がオリンピックのためにリオに行った際、ホテルの Wi-Fi に接続し、USADA のコンピュータシステムにリモートアクセスしました。リオの滞在中に USADA メールアカウントの認証情報が侵害され、選手の薬物検査結果と処方薬の概要が流出しました。同年発生したロシアによる攻撃では、アンチドーピング会議の開催場所となったスイスのホテルで、Wi-Fi ネットワークが侵害されました。そこで不正アクセスされた CCES 幹部のラップトップと認証情報は、カナダの CCES ネットワークの不正アクセスに悪用されています[65]。

モバイルマルウェア

オリンピックのような大規模なスポーツイベントでは、イベントスケジュール、ライブストリーミング、競技結果の表示、発券、商品購入、会場アクセス、詳細情報などを提供するためのモバイルアプリが開発されます。公式アプリの偽装や侵害を目的に、悪意のあるアプリが拡散される危険があります。

これまで悪意のあるアプリは、個人を特定できる情報、クレジットカード情報、ログイン認証の窃取、感染デバイスでの広告表示による収益化、モバイルデバイスにインストールされている他のアプリや連絡先への感染拡大に悪用されてきました。また、モバイルマルウェアは、ユーザーの現在位置や機密性の高いコミュニケーションの追跡にも利用される恐れがあります。モバイルマルウェアへの最善の対策は、悪意のあるアプリに対する注意喚起、公式アプリストアのみからのダウンロード、アプリストアとの連携を通じた悪意のあるアプリの特定と撲滅です。

アップデート: COVID-19 接触追跡アプリ（COCOA など）や個人 / 医療情報管理アプリを偽装したアプリが、アプリストアに登場する可能性があります。このようなアプ

64「U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations」（英語）：https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

65 同上

リは、個人情報の窃取を目的に、ダウンロードさせようと選手や観客を誘導します。アプリストア、政府職員、民間企業は、モバイルマルウェアに対する警戒を強化し、排除に取り組む必要があります。

日本のセキュリティ態勢

日本は、高度で複雑なサイバー攻撃から 2020 東京オリンピックをセキュリティ保護するという課題に直面しています。こういった課題の多くは、準備不足や、必要なサイバーセキュリティプラクティスの欠落に起因しています。これは、日本だけが直面している問題ではないものの、政府の統計によれば、サイバーセキュリティ対策において、日本の民間企業は米国や欧州の企業に後れをとっています[66]。多くの日本企業には、ガバナンス、ビジネスプロセス、適切な IT アーキテクチャサポート[67]が欠落しており、国のサイバーセキュリティのスキルギャップによって状況はさらに深刻化しています。

このような課題がある中、安倍晋三首相は、オリンピック開催国になったことを、東京のサイバーセキュリティ機能の開発に緊迫感を持って取り組む機会として捉えています。2018 年、政府はサイバーセキュリティ戦略の概要を発表しました。この戦略は、民間企業のサイバーセキュリティ強化に重点を置いたものでした。また、業務、リスク管理、イノベーションを目的にしたサイバーセキュリティ投資の強化を業界に要請するものでもありました[68]。

具体的な戦術としては、2019 年 1 月、日本政府は国内インターネットに接続されている 2 億台のデバイス（ルーター、ウェブカメラ、スマートホームアプライアンスなど）を対象に脆弱性チェックを行うことを発表しました。その目的は、物理ケーブルを使ってインターネットアクセスするハードウェアをチェックし、脆弱なユーザーが存在する場合には ISP（インターネットサービスプロバイダー）に通知することにあります。これは、2020 夏季オリンピックに加えて、ラグビーワールドカップ（2019 年秋）や G20 サミット（2019 年夏）といった国際イベントの開催準備として、セキュリティ強化を目的とした計画の一部です。

アップデート：情報通信研究機構（NICT）の NOTICE（National Operation Towards IoT Clean Environment）プロジェクトでは、脆弱なパスワードが設定されている IP アドレスに多数の通知を行っています[69]。発行されたユーザーアラートは、2021 年 2 月だけでも 1,948 件にのぼります[70]。この通知は、顧客の代理でプロジェクトに参加している 66 の ISP に送信されています。

また、日本政府は、2014 年サイバーセキュリティ基本法案を改定し、オリンピック関連のサイバーセキュリティ対策を担当する専門委員会を立ち上げることにしました。この委員会は、国や地方自治体の機関、重要インフラのプロバイダー、学術機関、民間企業で構成されます[71]。日本のメディアも、オリンピックを見据えた EU との連携強化を報じていますが、パートナーシップの詳細については広く報告されていません[72]。

66「How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World」（英語）：https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world

67「Cyber Security Talent Shortage in Japan」（英語）：https://www.accenture.com/_acnmedia/pdf-87/acenture-comptia-eng.pdf

68「CYBERSECURITY STRATEGY」（英語）：https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

69「NOTICE National Operation Towards IoT Clean Environment」（英語）：https://notice.go.jp/en/

70「Progress on the Projects」（英語）：https://notice.go.jp/docs/status_202102_en.pdf

71「Japan sets up cybersecurity council to secure the 2020 Olympics」（英語）：https://govinsider.asia/connected-gov/japan-sets-up-cybersecurity-council-to-secure-the-2020-olympics/

72「Japan strengthens cybersecurity cooperation with EU ahead of Olympics」（英語）：https://www.japantimes.co.jp/news/2018/07/16/national/japan-strengthens-cybersecurity-cooperation-eu-ahead-olympics/

アップデート:日本の内閣サイバーセキュリティセンター（NISC）は、CSIRCC（Cyber Security Incident Response Coordination Center）[73]を設置しました。この組織の目的は、関連組織、重要なインフラストラクチャ会社、オリンピック委員会、いくつかのサイバーセキュリティ会社（CTAメンバーを含む）による脅威インテリジェンスの共有にあります。2020年7月のレポートには、オリンピックイベントに関連する多数の組織を対象に実施したセキュリティ評価の結果が掲載されています[74]。また、日本政府は、いくつかの業界の情報共有 / 分析センター（ISAC）を介して、コミュニケーションの円滑化とサイバーセキュリティ情報の共有を推進しています。ISACには、Japan Automotive ISAC（J-Auto-ISAC）[75]、Information and Communications ISAC（ICT-ISAC）[76]、Financials ISAC Japan（F-ISAC）[77]が含まれます。

日本の積極的な取り組みは評価すべきですが、サイバーセキュリティに対する企業や政府のアプローチには根深い問題があり、わずか数年で変えることは難しいでしょう。この問題は日本だけではなく、サービスの提供や経済を情報テクノロジーに依存する多くの国に共通したものです。それでも、日本のサイバーセキュリティ能力は不十分であり、オリンピック開催中に発生するサイバー脅威の検知、防御、対応に影響を与える可能性があります。この点で、2020 東京オリンピックは攻撃者にとって非常に魅力的な標的だと言えます。

アップデート：数々の国内問題を抱え、オリンピックのホスト役に集中できない状況にある今、攻撃者は、日本のサイバーセキュリティ態勢は弱体化しており、サイバー攻撃を仕掛けるチャンスと見ています。日本は、大会の延期やスケジュール変更に伴って物流を大きく変更したことに加え、数多くの国内問題に直面しています。2021 年の初め、COVID-19 の感染拡大を受けて緊急事態宣言が発令されると[78]、「政府官僚がオリンピック中止を検討している」という匿名報道もありました[79]。オリンピックの開催を危ぶむ声が国際的に高まる中、オーストラリアは、コロナウイルスの感染が拡大する日本にオリンピックのホスト国を務める能力があるのか、公の場で疑問を呈しています[80]。

数々の国内問題を抱え、オリンピックのホスト役に集中できない状況にある今、攻撃者は、日本のサイバーセキュリティ態勢は弱体化しており、サイバー攻撃を仕掛けるチャンスと見ています。

最近の世論調査によると、日本国内のオリンピック支持率は依然として低く、国民の 80% は中止または延期するべきだと考えています[81]。さらに 2 月には、差別的発言をめぐり、東京オリンピック組織委員会の会長が辞任しました[82]。このような一連の動きには、2020 年半ばに起こった安倍晋三前首相の辞任表明が影響しています。連続在任最長となった安倍元首相は強力なオリン

73「Cybersecurity Measures for Tokyo 2020 Olympic/Paralympic Games」（英語）：https://project.inria.fr/FranceJapanICST/files/2019/04/Kumota.pdf
74「2020年東京オリンピック・パラリンピック競技大会に向けての取組状況」：https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou09.pdf
75「一般社団法人 Japan Automotive ISACが発足」：https://prtimes.jp/main/html/rd/p/000000002.000073805.html
76「一般社団法人ICT-ISAC」：https://www.ict-isac.jp/public/news.html
77「Financials ISAC Japan」（英語）：http://www.f-isac.jp/index_e.html
78「Japan Tries To Remain Optimistic As COVID-19 Threatens To Cancel Tokyo Olympics」（英語）：https://www.npr.org/sections/coronavirus-live-updates/2021/01/22/959534841/japan-tries-to-remain-optimistic-as-covid-19-threatens-to-cancel-tokyoolympics
79「Japan looks for a way out of Tokyo Olympics because of Covid」（英語）：https://www.thetimes.co.uk/article/japan-looks-for-a-way-out-of-tokyo-olympics-because-of-virus-lf868xfnd
80「Virus surge puts 'real pressure' on Japan to cancel Olympics, Australia leader says」（英語）：https://www.washingtonpost.com/world/asia_pacific/japan-olympics-cancel-tokyo-coronavirus/2021/01/22/866fef06-5c61-11eb-a849-6f9423a75ffd_story.html
81「About 80% Of Japanese Think Olympic Games Should Be Canceled Or Postponed, Poll Shows」（英語）：https://www.npr.org/2021/01/18/958120783/about-80-of-japanese-think-olympic-games-should-be-canceled-or-postponed-poll-sh
82「Mori is gone but gender issues remain for Tokyo Olympics」（英語）：https://apnews.com/article/yoshiro-mori-resign-tokyo-olympics-e2e7f3864a331aaf8372b811357d48a0

ピック支持者であり、2020 年東京オリンピック招致をサポートした中心的人物でした。日本が大きな国内問題に直面する中、安倍元首相の辞任によって状況はさらに複雑になったと言えます。

以上の状況を考えると、日本の関心はオリンピックのサイバーセキュリティよりも、COVID-19 対策といったより緊急性の高い取り組みに向いていると考えられます。国民の支持率の低さと、上記で示したオリンピック関連の諸問題は、政府や国民のサイバーセキュリティに対する意識の低下や準備不足の原因になっている可能性があります。CTA メンバーを含む、オリンピックのサイバーセキュリティプロバイダーは、脅威とリスクをきめ細かく監視しています。ただし、過去の経験から考えると、どの組織の責任者も、セキュリティと耐障害性の確保に向けて、サイバーセキュリティへの準備と対策に優先課題として取り組む必要があります。厳しい状況にあった昨年、政府と日本国民はサイバーセキュリティ問題に注力してきましたが、攻撃者の視点から考えると、このような弱点を認識することの重要性に変わりはありません。

教訓と推奨事項

夏季オリンピックが間近に迫る今、サイバーセキュリティの備えが進行中であり、多くのステークホルダーがアクションプランに取り組んでいます。CTA は、オリンピック関連のサイバーセキュリティ担当者にこのセクションをよく読み、セキュリティ態勢の強化に役立てることを推奨します。ここで記載する推奨事項は、オリンピックに向けたプランニングのみならず、政府機関、民間企業、スポンサー企業が参加する大規模イベントにも適用できる内容であり、政府機関、企業、ネットワークでセキュリティ対策に携わる幹部が計画および支持すべき内容となっています。

基本原則

サイバーセキュリティで最も重要なのは、基本的なプラクティスを順守し、効率的に実行することにあります。ステークホルダーは、ネットワークに接続されているシステムの把握、定期的なパッチ適用、ネットワークセグメンテーション、MFA（多要素認証）の有効化を行うべきです。これにより、あまり高度な手法を使わない攻撃者に対する防御を強化できるだけでなく、高度な技術を持つ国家支援の犯罪グループも、攻撃に大量のリソースを投入せざるを得なくなります。

情報共有

関係者間のコミュニケーションチャネルの確立と情報フローを定期的に確認するには、主要なステークホルダーとの定期的なエンゲージメントが不可欠です。政府機関、業界、スポンサー企業の関係者、公共の交通機関、放送ネットワーク、一般大衆と情報を共有すべきです。また、エネルギー会社、通信業者、ISP（インターネットサービスプロバイダー）といった商業サービスプロバイダーは、サイバー攻撃の標的になる可能性が高いため、このような組織との関係構築は特に重要です。このような情報共有チャネルを確立することで、迅速なインシデント対応が容易になるだけでなく、連携強化や脅威の事前警告にも役立ちます。平時に関係を確立しておかなければ、緊急時に効果的な対処はできません。

攻撃発生時に実際に指揮を執るリーダーとして、主なサイバーセキュリティファシリテーター（政府機関や内部の「専門チーム」など）を任命することを検討すべきです。これにより、コミュニケーション、情報共有、意思決定を合理化できます。またこのリーダーは、情報開示や現状説明を定期的に行うことで、信頼関係の構築や情報共有を推進できます。ただし、サイバーセキュリティプログラムの責任を「1 人」が担うことなく、定期的な

情報共有とコラボレーションが鍵となることに、意識と実践の両面で留意する必要があります。

可能であれば、公共と民間のサイバーセキュリティプロバイダーに依頼し、他のパートナー企業や組織内にアナリストを何人か常駐させます。複数のチームや組織の代表が集まることで、情報共有とチームワークが推進されます。

連携に基づくサイバーセキュリティ計画

計画立案には早期に着手し、できるだけ速やかに、人材や機器など必要なリソースをすべて調達します。イベント開始前の十分な時間があるタイミングで、脅威と脆弱性の詳細なリスク分析を行います。これにより、関連組織とサイバーセキュリティプログラムは、時間をかけて推奨事項をまとめることができ、それに基づいてアクションプランの立案が可能になります。このリスク評価では、脅威と対応策をまとめたサイバーセキュリティ機能マトリックスを作成します。

ステークホルダーはインシデント対応能力をレビューし、パートナー組織全体を網羅したプランニングを行う必要があります。このレビューでは、標準となる作業手順を定義します。手順では、インシデント発生時に関係者が果たすべき責務と対応時間を明確に示します。対応計画では、それぞれの役割で混乱が発生しないように、責務の定義と割り当てを明確に行います。脅威対応の構造やプラクティスのテストとして、脅威シミュレーション（机上演習や実地演習など）を行うと効果的です。

重要度の高いシステムの定期チェック

戦術的な面としては、イベントの開会前、開催中、閉会後に重要度の高いシステムを定期チェックします。具体的には、実装中のセキュリティツールの監視、不必要にWebに接続されているサービスのシャットダウン、一元的なログ記録を行います。また、ネットワークセグメンテーションにより、機密性の高い情報が格納されているサーバーを隔離します。正常稼働状態を確認することで、異常の検知や調査にかかる時間を最小限に短縮できます。また、定期的なテストやレッドチームテストも、セキュリティギャップの特定に役立ちます。さらに、スタッフのセキュリティトレーニングを行い、イベントを狙った脅威を検知および対処する方法を学習する必要もあります。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Report-2020-Summer-Olympics-Threat-Assesment-202106-R2