カテゴリ3 東京2020を『支えた』NTT R&Dの技術

ネットワークセキュリティ

オリンピックや国際博覧会といった世界的に注目が集まるイベントはサイバー攻撃のターゲットになりやすく，実際に被害が報告されることも決して稀なことではなくなってきました．さまざまな事情から1年延期され2021年に開催された東京2020オリンピック・パラリンピック競技大会において，NTTはゴールド通信サービスパートナーとして，大会を支えるネットワークインフラを運営する立場となり，サイバー攻撃の脅威に対応する重大な責任がありました．本稿では，NTT社会情報研究所の研究活動の1つとして実施しているNTT-CERTが，NTTグループの代表CSIRT（Computer Security Incident Response Team）としてどのようにしてサイバー攻撃と向き合ったのかを紹介します．

三科　貴（みしな　たかし）/松橋　亜希子（まつはし　あきこ）
仁佐瀬　剛美（にさせ　たけみ）/司東　秀浩（しとう　ひでひろ）

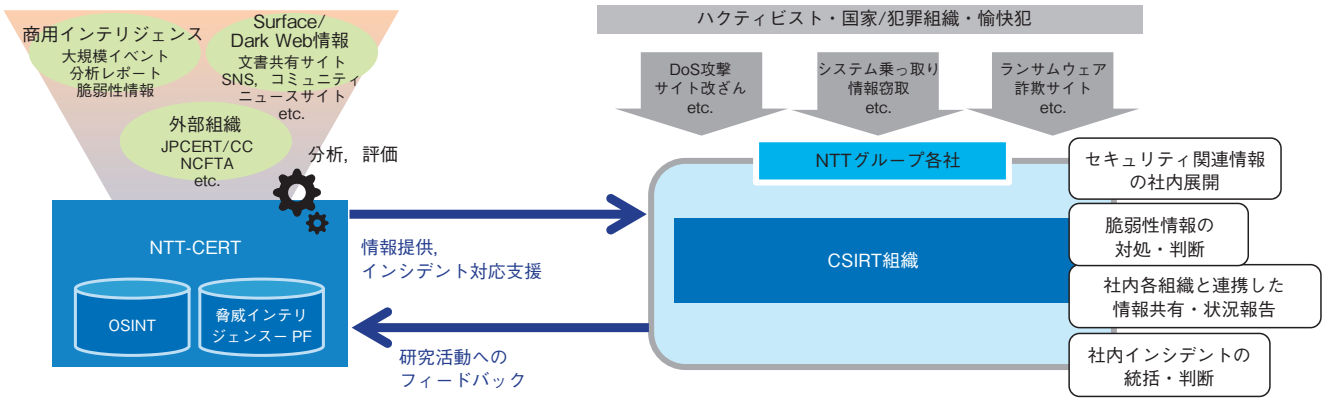
NTT社会情報研究所

オリンピック・パラリンピックとサイバー攻撃

オリンピック，パラリンピックは長い歴史を持つ国際的なイベントであり，世界中から注目が集まります．その注目度に便乗し，政治的な主張を広める場として悪用する，金銭をだまし取る，はたまた失敗を誘引し開催国家の信用失墜をねらうなど，さまざまな悪意を持つ人々のターゲットになり得ます．近年，そのような悪意を持つ攻撃者たちの手段が，物理的なものだけではなく，サイバー空間へと拡大し始めています．過去の大会では，大会関連サイトへのDoS（Denial of Service），DDoS（Distributed Denial of Service）攻撃による妨害行為，大会関連組織のシステムへの侵入，マルウェア感染が目的とみられる標的型攻撃など，大会運営に影響をおよぼしかねないさまざまな攻撃が確認されています．攻撃者たちは，この数年に一度の国際的なイベントで成果を上げるために，虎視眈々と技術を磨き，攻撃の準備をしています．大会関連組織は，大会をそのような高度な攻撃から守るために，万全の体制を敷く必要があります．NTTは，東京2020大会のゴールド通信サービスパートナーとして，大会を支えるネットワークインフラを運用する立場となり，サイバー攻撃の脅威に対応する重大な責任がありました．以下に，NTT社会情報研究所のNTT-CERTが東京2020大会において行った取り組みについて紹介します．

東京2020大会におけるNTT-CERTの活動

NTT社会情報研究所の研究活動の1つであるNTT-CERTは，NTTグループを代表するCSIRT（Computer Security Incident Response Team）として活動しています（**図1**）．機器の運用などをしておらず，サイバー攻撃を未然に防ぐための情報収集および収集した情報の



NTT-CERTの主な活動
① 情報収集分析
② インシデント対応支援
③ 技術調査，製品評価・教育

図1　NTT-CERTの位置付け

NTTグループ各社への円滑な共有，および，発生したインシデントの被害極小化や再発防止の支援といった，主に2つの目標を持って活動しています．また，これらの活動の中で得られた知見を研究活動にフィードバックし，さらなるセキュリティ技術の高度化，強化に向けた研究を推進しています．前述のとおり，NTTグループは東京2020大会を支えるネットワークインフラの安心・安全な運用の責任を担っており，私たちは世界中のさまざまな攻撃者からNTTグループそしてネットワークインフラを守るため，NTT-CERTの機能を強化する必要があると考えました．今回は，東京2020大会のネットワークインフラを支える大会関連組織としてサイバー攻撃の可能性を未然に防止し，万が一インシデントが発生した場合にも被害を極小化して大会への影響を最小にするという方針を策定し，特に情報収集分析機能の強化に力を入れました．

NTT-CERTは直接運用するネットワーク設備等を持たないため，情報収集の対象は主に外部のOSINT（Open Source Intelligence）情報になります．ただ漫然と，莫大な量のOSINT情報を集めていては，いくら人の手があっても足りません．そこで私たちは，東京2020大会における脅威分析と，収集すべき情報の優先順位付けを行うことにしました．私たちの行った脅威分析とは，どのような「攻撃者」組織が，どのような「攻撃手法」を用いて，どのような「目的」をもって，どの「攻撃対象」へ攻撃を仕掛けるのか，という4つの観点をもって，東京2020大会で発生し得るサイバー攻撃を分析することです．この4つの観点があることで，NTT-CERTが優先して守るべき「攻撃対象」は何なのか，優先して検知すべき「攻撃手法」の情報は何なのかという点で情報を整理でき，優先して収集すべき情報を効率良く分類することができます．そのためにはまず，東京2020大会で発生し得るすべてのサイバー攻撃を可能な限り挙げ，分析することが必要でした．そこで，まず過去に実際に発生したサイバー攻撃に関する情報を収集しました．サイバー攻撃の発生が本格化した2012年のロンドン大会から，標的型攻撃も確認された2018年の平昌大会まで，過去の大会における国内外のニュース記事や各セキュリティベンダが発表したレポートなどを分析しました．ここでは想定すべき攻撃を網羅的に把握するため，大会関係者，一般のお客さまを標的にした攻撃まで調査範囲を広げ，実際に起きた被害や想定された被害などのリストを作成しました．それらのデータを，上記の脅威分析を行うべく，「攻撃者」「目的」「手段」「攻撃対象」に分類しました．そのリストから，外部から攻撃を検知可能な「攻撃者」「目的」「手段」を定め，NTT-CERTが情報について収集するべき「攻撃対象」の観点から優先順位付けを行いました．具体的には，“NTTグループ”を直接の「攻撃対象」とする攻撃を第一優先とし，続いて“NTTグループ”への影響の波及が懸念される“大会関係者”への攻撃，そして“一般のお客さま”への攻撃という順で優先順位付けを行いました．また「攻撃手法」や「目的」に関してはNTT-CERTの立場でOSINT情報から検知できることを基準に優先順位付けを行いました．例えば，NTTグループを対象にした標的型メール攻撃などは脅威度が高いものの，そのようなメールの受信をNTT-CERTで直接検知することは難しいため，ここにリソースを割くことは非効率です．外部で検知可能な情報で，このような脅威からNTTグループを守るためにはどのようにしたらよいかを検討し，誘引されるであろうNTTの類似ドメインを持つフィッシングサイトの検知，窃取された情報がダークウェブで販売されていないかどうか，また政治的主張を目的に攻撃予告を行っているハクティビスト（社会的・政治的な主張を目的としたハッキング活動を行う者）の有無など，さまざまな攻撃をNTT-CERTの立場から検知できるように検討しました（**図2**）．

収集すべき情報の優先順位を定めた後，続いて行ったことは，情報収集範囲，量の強化です．これまでNTT-CERTの主な情報収集対象は，サーフェスウェブとインテリジェンスベンダからのダークウェブ情報，調査言語は日本語，英語でした．前述のようにダークウェブ上での販売情報やハクティビストによる主張を可能な限り検知するためには不十分であると考え，機械翻訳を活用した，過去の

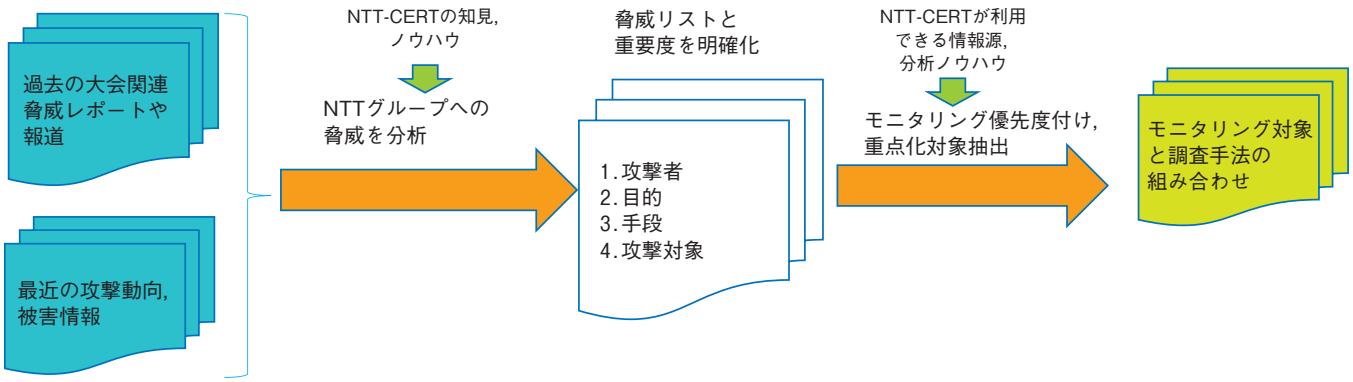


図２　モニタリング強化に向けた分析

事例の多い２カ国語の調査言語の追加，およびNTT-CERT独自のダークウェブ調査を開始しました．また，これまでもNTTグループの類似ドメイン調査は行っていましたが，大会期間（準備期間含む）に増加すると予測される東京2020大会の類似ドメイン調査も同時に行い，検知したドメインのフィッシングサイトの情報収集も実施しました．これらは，新規ツールの導入やこれまでのノウハウを活かした調査，およびCSIRT機能自動化の研究成果を活かした機能強化といえます．

このような取り組みによって１社の機能をいくら強化しても収集できる情報には限界があります．NTT-CERTはこれまで培ってきたさまざまなコミュニティと連携した情報共有も積極的に行いました．内閣サイバーセキュリティセンターの情報共有ツールである「Japan cyber security Information Sharing Platform（JISP）」や一般社団法人ICT-ISACによる東京2020オリンピック・パラリンピック競技大会向け情報共有プラットフォームへ参加し，未公開情報や独自情報を入手可能な状態にしました．またNTTセキュリティのGlobal Threat Intelligence Centerと連携し，東京2020大会へのサイバー攻撃に関する海外現地からの情報を逐一共有可能な状態を構築しました．このような外部連携によって得られた情報を，さらにNTT-CERTで追加調査，分析結果を加え，NTTグループ各社へ展開しました．これはNTT-CERTにおける，外部とNTTグループとのハブ役としての機能の強化といえます．

また，ネットワークインフラや運用体制に影響する脆弱性情報が発見された場合に備え，脆弱性情報収集体制および攻撃コードが公開された場合の検証体制の強化も実施しました．

上記のような活動に向けた準備を大会本番まで積み重ね，最後に東京2020大会での攻撃を見据えたNTTグループ内サイバー演習を開催しました．演習においてNTT-CERTは，シナリオ作成を担当しました．実際に攻撃が発生したと想定し，検知されると想定される情報をNTTグループ内に共有し，各社の連絡体制や対応手順に問題がないか，適切な対処が取れるかを演習にて確認し，大会前の最後の仕上げとして，NTTグループ一丸となり東京2020大会に向けた準備を整えることができました．

東京2020大会の活動結果

今回の機能強化の取り組みの結果として，NTT-CERTではさまざまな情報源から情報を収集・解析し，要確認情報をNTTグループ各社へ展開しました（**表**）．ただし，要確認情報には放置すると攻撃の足掛かりになり得る可能性がある検知内容や東南アジア情勢にまつわる政治的主張が絡む攻撃予告および小規模なDDoS攻撃，被害はなかったものの大会関係と思われるクレデンシャル情報売買などを共有しており，そのような情報提供の積み重ねによって重大な被害の芽を摘むことができ，またNTTグループ

表　モニタリング結果 情報源と検知結果例

情報源	情報源の詳細	検知結果例
公的組織	JPCERT/CC，IPA等	脆弱性情報，一般的な攻撃情報など
SNS	Twitter，ブログ，掲示板	大会関係者への攻撃をあおる書き込み，発見されたフィッシングサイト情報など
ニュースサイト	新聞社，放送局，IT関連ニュースサイト	大会動画配信を装う偽サイトの報道，過去の大会関係組織へのサイバー攻撃の報道，大会関係を装うマルウェアの記事など
ダークウェブ	ハッカーフォーラム，闇取引サイト等	大会関係と思われるクレデンシャルの売買情報など
偽サイト情報	DomainAbuse※，Google検索結果等	大会関係と誤認させるような新たなドメイン情報（一部はフィッシングサイトであることを確認）
その他	手動，ベンダ等のレポート	想定される攻撃者についての分析情報，マルウェアの分析情報など

※DomainAbuse：インテリジェンスサービスによるドメイン悪用情報

各社に安心感を与えることができたと考えています．実際に，大会終了後には警察庁が「五輪・パラ大会中のテロやサイバー攻撃なし」と発表したことが報道されており（https://www.sankei.com/article/20210909-KOK2GCDO3JK2LPIBAJOBHBRW6Y/），私たちの検知内容と一致していることが分かりました．

過去大会との比較考察

東京2020大会が過去一連の大会と大きく異なっていることは，コロナ禍によってほとんどの会場が無観客大会となったことです．その影響からか，過去大会でみられた偽チケット販売サイトや入場システムへのサイバー攻撃は確認されませんでした．また，偽のグッズ販売サイトなども今大会ではほぼみられませんでした．過去の大会でみられたハクティビストによるDDoS攻撃なども危険視していたのですが，近年はこのような政治的主張を伴うDDoS攻撃自体の頻度が低下しており，日本での東京2020大会に大きく反対する組織もありませんでした．そのため，このようなDDoS攻撃も発生しなかったと考えています．

総括としては，NTT-CERTの機能や連携の強化により，これまでになかった情報の検知が可能となり，小規模ですがいくつか攻撃の足掛かりとなり得る情報を共有することができました．また，大会を支えるネットワークインフラ自体もサイバー攻撃による事故等がなく無事閉会を迎えることができ，私たちの活動は意義のあるものであったと考えます．

今後の展望

今回初めて行った2020大会に対するサイバー攻撃への脅威分析は有効なものであったと考えます．NTTグループへの影響を考慮した外部関係者を含めた脅威の分析やこれまでにない情報や脅威を検知できたことは，今後，NTTグループがネットワークインフラ提供などの立場で関与する大規模イベントに対し，柔軟な調査を行えることを示していると感じています．また，今回の強化の取り組みとして，言語やダークウェブ上の調査の深化および攻撃アクター分析など，調査範囲を拡大しましたが，大会終了後も平時の調査範囲へと適用していくことで，これまでより高品質な情報収集が行えると感じています．このようなノウハウが明文化できた際には，NTTグループ各社へ展開しNTTグループ全体のセキュリティ向上に貢献していきたいと思っています．

（左から）三科　貴/ 松橋　亜希子/
仁佐瀬　剛美/ 司東　秀浩

◆問い合わせ先
NTTサービスイノベーション総合研究所
E-mail　svkoho-ml@hco.ntt.co.jp