2025 年 7 月

シリーズ 「日本のサイバーセキュリティ政策史」第 9 回

東京オリパラ
サイバー攻撃を防いだ舞台裏

サイバーセキュリティ政策分野に詳しい三角育生氏が日本の同政策史をひもとくシリーズ。第 9 回は、前回に引き続き、2025 年万国博覧会（大阪・関西万博）が開催されるタイミングをとらえ、大規模イベントにおけるサイバーセキュリティ政策史として東京オリパラを振り返ります。運営に影響を与えるようなサイバー攻撃は確認されなかった同大会。開催前・期間中にどのような取り組みが行われていたのか。当時 NTT セキュリティ最高技術責任者（CTO）として大会運営側の現場で尽力された与沢和紀氏に話をうかがいます。

【出席者】

与沢 和紀 氏
フォーティネットジャパン合同会社社長執行役員
元 NTT セキュリティ・ホールディングス株式会社代表取締役社長

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

防御対象を二分して

三角 本日は、大規模な国際イベントである東京 2020 オリンピック・パラリンピック競技大会（以下、「東京オリパラ」）におけるご経験をおうかがいしたいと思います。NTT グループは、「通信サービス」のカテゴリーで東京 2020 オリンピック・パラリンピック競技大会組織委員会（以下、「組織委員会」）とパートナー契約を結び、製品やサービスを提供しました。与沢さんは当時、NTT セキュリティ株式会社最高技術責任者（CTO）でいらっしゃいました。組織委員会・開催側の立場で SOC（Security Operation Center）ならびに国から委託されたさまざまなインテリジェンス関係の活動に携わられたと承知しています。

そこで、東京オリパラの開催前、準備段階における取り組みについてうかがいます。当時、私は

内閣サイバーセキュリティセンター（NISC）にいました。国としては東京オリパラに向けて大きく分類して2つの施策を行っていました。一つは、東京オリパラの準備・運営への影響の未然防止・軽減などのためのリスクマネジメントの促進。すなわち、大会を支える各種サービスを提供する事業者等によるリスクマネジメントの強化を通じたサイバーセキュリティ上のリスクへの対策の促進です。もう一つは、東京オリパラのサイバーセキュリティに係る脅威やインシデント情報の収集、また、これら情報の関係機関等への提供、さらに、必要に応じて関係機関等のインシデント対処についての対処調整を行う組織として、サイバーセキュリティ対処調整センター（政府オリパラ CSIRT）の構築です。

与沢さんは、このような国の取り組みと、結果的には一緒にやっていただいたことになるわけですが、NTT セキュリティとしてはどのようなことに注力されたのでしょうか。

与沢　東京オリパラの開催が決定したのは 2013 年 9 月でした。そして、NTT グループが組織委員会とゴールドパートナー契約を結んだのは 2015 年1月です。その後、早い段階で通信インフラの整備に着手しました。国際オリンピック委員会（IOC）による要件を満たすため、必要に応じて新たにファイバーを引く、ルートの二重化を図るといったことに時間をかけて地道に取り組みました。

2018 年頃、本来の大会開催予定の2年ほど前にはシステム構成をしっかりと考えました。韓国の平昌オリパラ（2018 年 2～3 月）では、大会運営に重大な影響を与えるようなサイバー攻撃はなかったものの、かなり多く発生していました。同大会のシステム全体を見ていたのはフランスの IT 企業 Atos（アトス）ですが、同社の大会運営システムのサーバーも標的になり、欧州側まで侵入されました。そうしたことを参考とし、かつ重視して、東京オリパラではネットワークの構成およびそれを司るシステム構成について、大きく 2 つに分けて考えて対応を準備しました。

三角　どのように切り分けたのですか。

与沢　一つは、絶対に守らねばならない領域、すなわち組織委員会など大会を直接運営・管理する組織や人に関するものです。もう一つは、利用者の自由度をある程度認めるメディアや観客等に関するものです。それらについて、WiFi からケーブルテレビ（CATV）、通信、放送までの接続を完全に二分しました。これは、組織委員会の意向を踏まえ、われわれ自身として考えたものです。

結果から言うと、コロナ禍の影響で 1 年遅れて開催した中で、本来守るべきネットワークの方は、全くサイバー攻撃に入り込まれませんでした。一方、メディアや観客等が使うネットワークの方には、サイバー攻撃によるインシデントはありました。開幕式に向けて徐々に増えて、しばらく続きました。

三角　それはどういう攻撃でしょうか。DDoS 攻撃ですか。または、不正アクセスをしようとしてのポートスキャンといったものでしょうか。

与沢　ポートスキャンはありましたし、また、ID・パスワード、クレデンシャルが盗まれていたことによるものもありました。

三角　サイバー攻撃の常套手段ですね。

与沢　そうです。それから、脆弱性を突かれるようなものもありました。無観客であっても、特にメディアその他の皆さんがパソコンなどをネットにつなぎます。それらに脆弱性があれば、そこを突


与沢氏

かれて入り込まれるというものです。ただし、それらも NTT セキュリティの SOC が最終段階でしっかり監視していたので、確実に検知でき、当該 PC に告知するなど対処しました。

三角　サイバー攻撃を受けているデバイスを特定して、そこに感染していることを教えていたわけですか。

与沢　そうです。「即座に対応を取るように」と組織委員会から通知しました。それを大会期間中を通して実施しました。

「ダークネット」まで調べる

三角　大会開催前、ほかにはどのような取り組みをされたのでしょうか。

与沢　脅威情報を把握しました。何が起きつつあるのかを完全に捕捉するべく外部機関の情報を活用して「ダークネット」をチェックしたり、NTT 研究所の独自技術をもちいて調べました。NTT セキュリティとして、自ら全リンクをクローリングしました。

三角　直接見ていらっしゃったのですか。

与沢　はい。最後は人間がチェックしていかなければならないので、結構手間暇がかかります。そこは専門の会社に任せました。考えうる最高のダークネットに係る脅威インテリジェンス会社を使いこなしました。

三角　脅威インテリジェンスを入手してきても情報は玉石混交だと思います。そこはどのようにされたのですか。

与沢　指示・依頼の内容を明確にしました。例えば、気にすべきドメイン名や企業名を約 2,000 件リストアップして、これに関わる、あるいは近似のドメインの発生に対する何らかの情報のやり取りを抽出せよ、といったような指示です。

三角　そのリストは誰が決めたのですか。

与沢　国がある程度スコープを定めていたので、それを踏まえてわれわれで特定しました。国の定めるスコープに明示されなかったものとしては、スコープ内にある企業が利用したり調達したりしている IT 企業に関するものです。過去にクレデンシャルが盗まれていれば、それらを対象にしておかないと、そこを起点としてスコープ内にある企業などが侵害されてしまいます。それらはクラウドサービスや IT バックボーンなどです。システム系の企業はさまざまなところで攻撃を受けるので、情報漏洩している可能性が高いわけです。そういったところをスペシフィックに脅威インテリジェンスサービス事業者に指示をすれば、短時間でいい情報を出してくれます。真剣にダークネットを見たのはいい経験になりました。それらは NTT コミュニケーションズと NTT セキュリティの新たな力にもなりました。

三角　その中でどのような動きが見えたのでしょうか。

与沢　われわれを含め組織委員会全体で気になったのが、大量の偽サイトです。すでに開催 2 年前から作成され始めていました。例えば、偽のチケットサイトが立ち上がり、そこに誘導して金銭を


三角氏

搾取しようとする動きがありました。ただ、最終的には、チケットはほぼ販売しなかった、あるいは返金したので意味をなさなかったと思います。また、地方公共団体もターゲットになりました。東京オリパラ会場エリアの地方自治体はほぼ全て偽のドメインが作られていました。金銭搾取を目的とすること、また攻撃手法が過去に発生したサイバー攻撃者のグループと同様だったことから、それらの近傍からの攻撃の可能性が高いと見ていました。

三角　それは金銭目的と評価されているわけですか。

与沢　金銭目的と、日本の信用失墜もあります。

三角　だから、守りが強固な大会そのものというよりは、その周辺の信用に関わるようなところなどがターゲットになったわけですね。

与沢　そうだと思います。その一部として、DDoS 攻撃はありうる話でしたが、東京オリパラの時にはほぼ発生しませんでした。公共サービスを含めたサービスがダウンするといったことにはあまり行かない感じではありました。

1年延期、無観客開催の影響

三角　NTT セキュリティはビジネスとして、自治体に対してもセキュリティ体制をサービスとして提供されたのですか。

与沢　いいえ。私どもは、NTT グループとして通常のビジネスとは切り離して東京オリパラのために、国の監視の業務の一環としてやっていたということです。NTT グループから組織委員会のテクノロジー担当の責任者などとして職員を出向させていたので、こうした関係者と連携しながら、重要な侵害やダウンがあれば NTT グループが攻撃される方向になるので、それも含めて見ていたというところです。

三角　そこは NTT セキュリティとしてですか、それとも NTT グループとしてということですか。

与沢　NTT グループとしてです。実質的に動き回るのは NTT セキュリティや NTT 研究所の技術者です。NTT セキュリティのセキュリティオペレーションセンターは、通常約 90 名で構成されているのですが、開催期間中および前後は全員体制でオリパラに注力しました。コロナ禍の時期はリモート環境にせざるをえなかったのですが、大会期間中は出社し、即座の対応が取れる、あるいは横で連携や相談ができるかたちを取りました。

三角　当初、大会は 2020 年開催予定でした。そこに向けて構築していた体制を 2021 年開催用に組み替えが必要になったと思います。そういったリモート対応の変更が主でしたか。

与沢　実は、東京オリパラに向けて 2018 年頃から本格的に準備していたところ、2020 年 5 月にシンガポールにある NTT コミュニケーションズのグループ会社がサイバー攻撃を受けて情報漏洩する事案が発生しました。その対策の一環で、設計の見直しを行いました。これについては、1 年延期され時間的余裕ができたことで若干助かりました。

もともと開催期間中はオンサイトでしっかり見守ろうとしていました。具体的には、現場にネットワ

ークエンジニアやインシデント対応エンジニアを配置し、セキュリティ関係の最終監視は NTT セキュリティ側が実行しました。

三角　国は、基本的には、さまざまなチェックやリスク評価、体制構築についてはスケジュール通り 2020 年までに行い、大会開催が延期されたことによって体制の変わったところを評価し直したと承知しています。

与沢　体制変更による評価し直しは行いましたし、チェックする重要インフラ事業者の範囲も広げました。

三角　無観客開催になったことの影響はありましたか。

与沢　どちらかというとサイバーに係る負荷がバランスされる影響があったといえるかもしれません。オンサイトがなくなり、本来のゲームに注力できるようになったというのはあります。オンサイトでは大量の WiFi 設備を設置・接続し、さながらサイバーセキュリティ対策製品の品評会のように、名だたるサイバーセキュリティベンダーの最高品質のものを使いこなす計画でした。

三角　そこには資金が投入されたということですね。

与沢　はい。

三角　各社協力するという感じもありましたでしょうか。

与沢　協力とマーケティングの意味合いもあったと思います。

ベンダー側の積極的な協力によって多段防御など最高に近いものとすることができました。「ふるまい検知」も、その時点で最も有名だったものを導入しました。こうしてエンドポイントの端末も含めて脅威を遮断するということに注力しました。

三角　それらは大きな経験になったわけですね。

与沢　そのとおりです。

ゲームと放送の継続を目指して

三角　NTT セキュリティにおいては、大会期間中は監視を中心に行っていらっしゃったのですか。

与沢　はい。大会開催 1 年半前から、関係するシステムは常時監視していました。先ほど申したように、期間中、結果的に基幹のネットワークには入り込まれなかったので、モニタリングしているのみでした。一方、メディア等が入るネットワークについては、インシデントレスポンスを実施しました。

三角　当時、事業継続、すなわちゲームの継続と放送の中断がないことが目指されていたと思います。

与沢　まさにそうです。

三角　そのための特別な体制は何か組まれていたのですか。

与沢　情報連携のための体制を整備しました。

NTT グループはネットワークと運営に一定の範囲で参画していました。例えば、ヨットレースなどでは 5G や衛星を使いますが、状況を把握するため、セキュリテイ担当者もヨットレースに係る業務に関与していました。

三角　確かに、ヨットや自転車のレースなどはそういった通信体制が必要になりますね。

与沢　それらのゲームはテレビカメラが終始追い続けることはできないので特殊な手法をとりました。

東京オリパラのために NTT グループが提供した通信サービスとしては、まず、放送用のネットワークのため 1,900 キロメートルの光ファイバーを引きました。これはその後の再利用が可能です。オリパラ開催国では大体、その国のメインの通信キャリアは、そのような貢献をしています。ロンドンやロサンゼルスの大会際にもオリパラ開催のためだけに光ファイバーを引いていますし、長野の大会の際にも、ほとんど人の居住していないところにも光ファイバーを引きました。

大会用のデータネットワークには 1,200 キロメートルの LAN ケーブルを用いました。また、特にメディアと近隣住民のために CATV セットトップボックス 6,800 台、さらに、結果的にあまり用いられなかったわけですが、会場の WiFi のために 1 万 1,000 アクセスポイントを設置しました。加えて、携帯電話 1 万 9,600 台と固定電話 2,800 台を用意しました。

今申した設備については、組織委員会としてどの程度予算を用意できるかについて、頻繁に打ち合わせを行いました。われわれとしても、できる限りその予算内で賄えるように努めました。

人的には、NTT グループからは協力会社を含め延べ約 1 万人が大会に関与しました。

平昌オリパラ時に人材を送り込み、信頼構築していた

三角　平昌オリパラでは、Atos 社が整備したシステムがサイバー攻撃を受けました。NTT セキュリティと同社との関係はどうだったのでしょう。

与沢　平昌オリパラ開催時には、Atos 社が東京オリパラに関与することはわかっていましたし、われわれとしても東京オリパラを見据えて、Atos 社とはかなり深い連携を平昌オリパラ時から行っていました。東京オリパラに活かそうとかなり詳しく見ていました。Atos 社のインシデント対応も現場で見ていました。

先方は IT 企業なのでソフトウェアと IT エンジニアが非常に多くいました。しかし、サイバーセキュリティの専門家はそれほど多くいませんでした。少なくとも 24 時間見守り続けるオペレーションを十分に行える人数はいない感じでした。そこで、われわれも貢献する機会があったということです。

三角　Atos 社は長年、IOC と契約を結び、大会向けのシステム構築を手掛けています。IOC もサイバーセキュリティについて重視していたはずですので、当然 Atos 社としてもしっかりと体制を組んでいると思っていました。

与沢　エンジニアの人数は大勢いますが、そのほとんどがシステム側のソフトソエンジニアです。そうした技術者は「運転を止めない」ところに注力します。しかし、サイバーセキュリティの視点で攻撃を受けた場合の挙動を捕まえて対処するエンジニアはおらず、対処体制があるとは言えませんでした。

そこで、われわれのエンジニアのリーダーはかなり Atos 社側に助言しました。当初は、「何を言いに来たのか」という感じだったのですが、次第に「助言を受け入れた方がいい」となり、最後は「仲良くやりましょう、成功させるのが重要だ」という関係になりました。

三角　共通目的が認識されたのですね。セキュリティ人材による深い連携協力を行った効果もあ

ったし、信頼関係も作れていたというのは戦略的です。東京オリパラの時には、Atos 社は改善してくれたのですか。

与沢　改善しています。Atos 社は過去からの積み重ねがあります。ミリ秒単位でのゲームを進行させるのは大変なことだと思います。

三角　Atos 社が平昌オリパラでサイバー攻撃を受けたときには、どこに問題があったのでしょうか。

与沢　ウィンドウズサーバーの中に入っているシステムにあった脆弱性が悪用された模様です。

三角　脆弱性への対応が十分になされないということはありがちです。脆弱性はしばしば公表されますが、それに対して、全てのサーバー、デバイスが迅速にアップデートされるかというと、そうでもありませんね。

与沢　迅速に対応されていないことはしばしばあります。東京オリパラ開催前のことですが、私がいま在籍する会社のネットワークファイアウォール「フォーティゲート」の脆弱性が問題になりました。報道前に当社自ら気が付いて発表しましたが、お客様側ですぐに OS のアップデートとかパッチを当てるといった対処をしていただけないことはありました。

三角　顧客側のパッチの適用ポリシーによるわけですし、多数のデバイスが起動されてアップデートがなされるまでには時間がかかりますね。

与沢　そこが難しいところです。

具体的な指示と双方向のやり取りで

三角　一緒に守っていた側として、国の政策について、何かお感じになられたことはありますか。

与沢　国の関係機関の指示・指導は完璧に近いと思います。ここでチェックするように、といった指示は的を射ていました。それに対してどういう技術で、どのように確認をするか、必要な情報を取得するかというのは、われわれの側の仕事です。

三角　どのような指示がありましたか。

与沢　偽ドメインを調べてくれというときに、この組織、この類の組織について確認するように、というように指示が具体的でした。例えば、特定の会場がある自治体や重要インフラ企業について、過去に漏洩したクレデンシャル、ID やパスワードなどが再利用されていないかをチェックせよ、といった具合です。

三角　その場合に、どの程度具体的だったのですか。

与沢　例えば、この企業は 600 万件と大量の ID が漏洩しているから注意してくれ、といった感じでした。一方的に指示を受けるというよりは、定期的にインタラクティブにやりとりしましたし、そうした過程で指示の具体性は高まっていきました。リアルタイムに発見された重要性の高いものについては、その関係の企業、自治体、その他へ即座に NISC 等から指導がなされていたようです。さすがだなと思いました。

三角　今後の大規模国際的イベントの機会に向けての改善点としてお気付きになったことはありますか。

与沢　東京オリパラはほぼ無観客開催でした。今後の大規模国際的イベントに向けての視点で充足が必要と思われるものとしては、オンサイトの聴衆が大勢いる環境でも同じように振る舞えるようになるための経験です。会場に物理的に何か仕込まれることもありえます。例えば、WiFi ルーターは悪用されるリスクを抱えています。何かを仕掛けられたり、あるいは調達ルートを間違えたりすると、中に何か仕込まれたまま到達してしまい、それが全ての脆弱性の入り口になりえます。それらが現実に悪用されたときに、オンサイトにおける対応についてはこれから経験していくのだろうと思います。特に万博のように長期間にわたって開催されるものは緊張が長く続くことになるでしょうね。

三角　観客がいる中では点検、対処していくのも大変ですね。

与沢　もう一つは、東京オリパラのそれぞれの場面で優秀な人を集め、経験を積みました。それを継続することの難しさがあると思います。

三角　国は通常2、3年で人事異動があります。東京オリパラから 4 年経つ今、各組織の人員はほとんど入れ替わってしまっている可能性があります。東京オリパラのときのような集中的に取り組む経験を得る機会はなかなかないので、インシデントレスポンスについては経験不足になりがちです。そういう記憶や記録を少しでも残しておく取り組みは大切だと思います。歴史は繰り返します。

そういう観点で世の中に伝えておきたいと思われることはありますか。

脆弱性アラートを放置しない

与沢　先ほど少し話題にしましたが、サイバー攻撃対策用の装置やソフトそれ自体に脆弱性が露呈することがあります。購入し導入したから、それでおしまい、ではなくて、しっかりと運用するチームや要員を配置してほしいと思います。それは国だけでなく、自治体、企業、その他組織においても同様です。ただし、難しいのは、大規模の企業、組織にはリソースを充てる余裕があるかもしれませんが、中小の規模になると対応しきれないところもあるでしょう。また、サイバーセキュリティのシステムを導入し全体を運用することが重要です。脆弱性の警告が公表され、「パッチをあててください」「OS をバージョンアップしてください」といったアドバイザリがあれば放置しないことです。現実には、システムを構築するのは業務を請け負った外部の会社であることが多いため、運用者との間でどちらが責任を果たすのかといった議論がよく起きます。その結果、困るのはエンドユーザーです。

三角　最初に契約で明確化させておくことが大切ということですね。

与沢　システム自体は継続して運用をしているはずなので、単に導入しておしまいにしないことが重要です。

三角　システムの運用の契約の中に、しっかりと脆弱性対応などのサイバーセキュリティの取り組みを入れておくということですね。

与沢　「システムが止まらないように」という中には、「サイバー攻撃を受けないように」が入っているという認識を持っていただけたらと思います。現在の会社に入っていっそう感じました。「フォーティゲート」は日本でのシェア 50 パーセント以上で、50 万台以上出荷しています。のべ 50 万台のお客様の情報を全て知っているかというと、途中でリセラーが何段か入りますので、その先のデータは 100 パーセント揃えられません。私どもが注意喚起を出しても、お客様まで確実に届くか確認し難いところもあり、かゆいところに手が届かないところがあったりします。一つの脆弱性が発生すると 50 万台全てに影響が出てしまうので、数が多いことは良し悪しです。

三角　何かあれば企業や製品の名前の方が先に走ります。「フォーティゲートの脆弱性が悪用された」というニュースが出れば、そんなに脆弱性があるのかと思われてしまいます。パッチを当ててくれないと、いつまでも脆弱性が残り、攻撃の対象となってしまいますね。加えて、昨今のようにリモートが増えてくると、どうしてもそこが攻撃対象領域になりがちです。

与沢　そうですね。しかし、われわれが勝手にアップデートするわけにもいきません。

もう一つ注意が必要な点は、いろいろなシステムやデータがクラウドへシフトしている中で、クラウドに脆弱性があることです。クラウドサービス提供者は自分の責任はここまで、と線引きするので、利用者側がもう一段突っ込んだ防御の仕組みを作らざるをえません。今後クラウドへの攻撃がいっそう増えるでしょう。

三角　脆弱性対応は、オンプレ、クラウドいずれもサイバーセキュリティ対策として不可欠であり、企業等はシステムの運用においてその点を忘れないようにすることが不可欠ですね。

本日は、東京オリパラにおける経験をお話しいただきました。国、組織委員会、システム構築事業者、サイバーセキュリティ会社、重要インフラ事業者など関係者が、いかに連携して、リスクマネジメントやインシデント対応をなさったかについてよくわかりました。そこで組織や人々が得た経験をいかに継承していくかが、今後の大規模国際イベントにおけるサイバーセキュリティの取り組みとして鍵であることを改めて認識いたしました。

本日はどうもありがとうございます。

（2025 年 3 月 11 日収録。取材・構成：一般社団法人日本サイバーセキュリティ・イノベーション委員会[JCIC]）

【出席者略歴】

与沢 和紀（よざわ かずのり） 氏

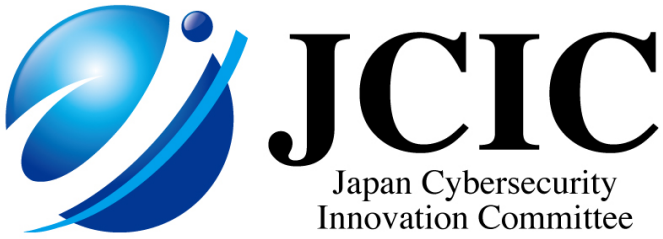
フォーティネットジャパン合同会社社長執行役員

千葉大学にて電子工学学士号、米スタンフォード大学大学院にて経営修士号を取得。日本電信電話公社（現 NTT）、NTT America, Inc. 副社長などを経て、2006～2010 年エヌ・ティ・ティ・コミュニケーションズ株式会社にて、海外サイバーセキュリティ会社等の買収を牽引。2016 年 NTT セキュリティ・ジャパン株式会社代表取締役社長に就任。2018～2021 年 NTT セキュリティ株式会社最高技術責任者（CTO）としてグローバル R&D を率いて脅威インテリジェンスの高度化、AI 検知技術開発、コネクテッドワールド向け次世代サイバーセキュリティのイノベーションに注力。NTT セキュリティホールディングス株式会社代表取締役社長を経て、2023 年 7 月より現職。

三角 育生（みすみ いくお） 氏

東海大学情報通信学部長・教授

1987 年通商産業省(現経済産業省)入省。内閣サイバーセキュリティセンター(副センター長等)や経済産業省(サイバーセキュリティ・情報化審議官等)等において、サイバーセキュリティ、安全保障貿易管理といった行政に長く携わり、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法制定・改正、日本年金機構のインシデント対応等に従事。2020 年 7 月退官。2022 年 4 月より現職。博士(工学)、MA in Management。



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com