2024 年 5 月

シリーズ「日本のサイバーセキュリティ政策史」第 7 回（連載全2回）

すべての人が「自分ごと」として向き合える行動計画を【後編】

～TOKYO2020 のサイバーセキュリティ対策の舞台裏とレガシー～

前編に続き山内智生総務省サイバーセキュリティ統括官（元内閣サイバーセキュリテイセンター副センター長）にお話をうかがいます。2020 年東京オリンピック・パラリンピック競技大会（TOKYO2020）に向けた準備、開催期間中、そしてレガシーはいかなるものであったか。

【出席者】

山内 智生 氏
総務省 サイバーセキュリティ統括官（最高情報セキュリティ責任者）、
元内閣官房内閣審議官（内閣サイバーセキュリティセンター）

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

TOKYO2020 準備の下地の上に策定された第 4 次行動計画

三角 「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2017 年 4 月 18 日、サイバーセキュリティ戦略本部決定。以下、「第 4 次行動計画」という）では、第 3 次行動計画の 5 つの施策群の補強等を図ることとし、重点事項の一つに TOKYO2020 も見据えた情報共有体制の強化がありました。山内さんは 2014 年から総務省情報通信国際戦略局宇宙通信政策課長でいらっしゃいました。サイバーセキュリティ戦略本部で第 3 次行動計画の見直しに向けたロードマップで TOKYO2020 の運営を支障なく遂行させることなどが示された直後に内閣サイバーセキュリティセンター（NISC）の総括担当の内閣参事官に戻られて、同行動計画の策定に参画されたわけですね。

山内 私が NISC を離れていたのは 2014 年 7 月～2016 年 6 月です。再度 NISC に着任したときに、重要インフラ担当の参事官から、第 4 次行動計画策定に向けた検討資料を受け取りました。私が総務省に戻っていた間、日本の重要インフラ分野で大きな事故はありませんでしたが、2015 年 6 月に日本年金機構の不正アクセスによる情報流出事案がありました。一方、日本時間の 2013 年 9 月 8 日に、東京都が 2020 年オリンピック・パラリンピック夏季大会の開催地に決定していました。そのため、第 3 次行動計画期間中の早い時期から TOKYO2020 に向けた議論をし、そ

ういった下地の上に、第 4 次行動計画の検討がなされていました。正直、受け取った検討資料を見たときにあまり違和感はありませんでした。

第 4 次行動計画では、いろいろ対策強化をした部分があります。例えば、第 3 次行動計画をつくるころから組織を狙ったサイバー攻撃がだんだん目立ってきていました。2013 年には韓国の金融機関と放送局の編集システムが Windows に埋め込まれたマルウエアにより一斉にダウンする事案が発生しました。そういった重要インフラに対する顕著な事案を見ていると、いわゆる DDoS 攻撃や Web の改ざんというレベルではなくて、システムそのものに障害を与える攻撃も重大な課題であるということが多くの重要インフラ事業者の方々の認識の中にも入りつつあったと思います。そこで、高度化するサイバー攻撃を前提に、重要インフラのサービス提供機能を継続できるようにすることなどを行動計画に盛り込んでいきました。

TOKYO2020 対策──セキュリティ能力の底上げを図る

三角 NISC 副センター長ご在任中に TOKYO2020 の開催を迎えられました。その準備はどのように取り組まれたでしょうか。

山内 TOKYO2020 に向けた主たる対策としては、TOKYO2020 の開催・運営に影響を与えうる重要サービス（電力、通信、放送など）を提供する事業者などに対するリスクマネジメントの促進と対処体制の整備がありました。リスクマネジメントについては、事業者の方々にリスク評価、およびその評価結果を踏まえた対策を、当初の予定では 6 回実施していただくことにしていました。実際には、プラスアルファ的なものをもう一回追加的に行っています。プラスアルファ的というのは、新型コロナウイルス禍の影響で TOKYO2020 の開催が 1 年延期されたときに、当初の予定になかったチェック的な取組を追加して行ったことを指します。新型コロナウイルス禍の影響から、例えば、システムメンテナンスはリモートで行い、また、さまざまなデータをクラウド上に上げるようになるなど、経済社会の体制が変わっていました。前提にしていたシステムや体制がかなり変わっていると考えられたので、環境変化を踏まえたチェックを実施する必要があったわけです。このチェックは、2020 年の夏前後に実施しました。その時期は、まだ日本の経済社会が混乱している最中でしたが、本来だったら TOKYO2020 を開催している時期に、延期した 1 年後に向けて行ったということです。そして年末から年明けにかけて、最終回を行いました。

三角 公開されている年表では実施回数は 6 回と書いてあります。お話にあった追加的なチェックは、最終回である 6 回目に先立って、世の中がリモートに変わった影響、評価を見たという感じでしょうか。

山内 そのようになります。すなわち、6 回目のリスク評価の実施にあたって、チェックを事前に入念にやったという整理になります。

実は、リスク評価の実施については、もともと政府から言われなくても実施している事業者の方々もいらっしゃいました。一方で、「リスクアセスメントとは何？」という反応を示す方々もいらっしゃいました。結果的には、全体の底上げがなされたと考えます。事業者の方々の間で、サービス障害につながるシステムのマネジメントについて、さまざまな気づきが得られたというのが全体像

といえるでしょう。ただし、皆さんがそのよう思っていらっしゃるかというと、既に取り組んでいらっしゃった方々の間では、若干ご不満もあったようで、「既にできているのに政府は何回やらせるつもりだ」といった声も聞こえてきました。


山内氏

三角　一部にはそのようにとらえられていたと聞きます。

山内　陰に日なたに「いつまでやるのですか」、「われわれはできているから、やらなくてもいいですよね」などと言われることもあって、そうした方々には「すみませんけれど、お付き合いください」とお願いをしていました。

三角　事業者のサービスは連関し合っているので全体としての底が上がらないとなりませんね。

山内　そのとおりです。その点についてはある意味、統制を取らせていただいていました。実際のところ、同業他社の取組は自社もするという日本の文化が、結果として、いい方に働いたといったことが大きかったと思います。

サイバーセキュリティ対処調整センターの現場

三角　対処体制については、2019 年 4 月にサイバーセキュリティ対処調整センター（以下、「対処調整センター」という）が設置されました。同センターの運営はどのような感じでしたか。

山内　2012 年ロンドンオリンピックの経験を踏まえて英国政府など関係者からさまざまな助言をいただきました。例えば、サイバーの話だけで閉じるのではなく、物理的な脅威に対応する部署とも連携すべきということは相当言われていましたし、われわれの意識としてもそうでした。実は、大会期間中において関係機関の連携確保、緊密連携・調整を図るために内閣官房に「セキュリティ調整センター」が置かれました。対処調整センターは、この「セキュリティ調整センター」等危機管理担当部署との連携が必要でした。そこで、私は、構造的には対処調整センター側を取りまとめる立場にありましたが、肩書きはセンター長ではなく、副センター長となりました。センター長には、内閣官房危機管理審議官に就いてもらいました。もともと TOKYO2020 の物理・サイバー両面を検討するセキュリティ幹事会（座長：内閣危機管理監）があり、そこでのテロ対策ワーキンググループは危機管理審議官が、サイバーセキュリティワーキンググループは私のポストが座長を担っていました。そこで、危機管理審議官にサイバーセキュリティと実世界のセキュリティを一緒に調整してもらうことにしたのです。「実務は全て私が担当します。ただし、何かあったときの調整をセンター長がやってください」とお願いをしました。ですから、実際のところは、サイバーについて、対処調整センターの運営はほぼ全部任されていました。

三角　TOKYO2020 開催期間中、対処調整センターはどのような状況だったのでしょうか。

山内　開会式の式典は 2021 年 7 月 23 日の 20 時開始です。対処調整センターを収容する部屋は私の部屋とは別の場所にありました。私は 12 時頃から自分の部屋にいて、対処調整センターの運用にあたり導入された情報共有システムである「JISP（Japan cyber - security Information Sharing Platform）」とメール、それからもう一つの通信手段をずっとつなぎっぱなしにし、現地の音

声も聞こえる状態にして、さまざまな細かい報告も全部共有してもらっていました。

16 時頃までには、対処調整センター員は官邸の危機管理センターに行ってオペレーションに入りましたので、私は自分の部屋で一人、留守番をしました。関係者には「何かあったら私のところに連絡ください」と指示し、随時「何かありますか」と聞いて、「今のところ異常はないという報告です」というのを確認していました。何かあったときに困るので、開会式が終わるまで回線をつなぎっぱなしにするなど、リアルタイムで情報共有ができるかたちにしていました。現地の音声も聞いていましたけれど、叫び声などは聞こえなかったので、ある意味平和な開会式でした。

三角　対処調整センターの方々の現場でも、重要サービス事業者（電力、通信、放送など）の方々との間で回線はずっとつなぎっぱなしだったのでしょうか。

山内　それはほぼ JISP でやっていました。ただし、何か大きなことがあったら他の手段に切り替えることになっていました。JISP の良いところは、過去のやりとりも含めておもだった方々に同報できるところです。メールや電話にすると、特定の人にしか知らされません。

三角　JISP は気軽に使われていたのですね。

山内　機能、仕様には満足していましたし、われわれの想定を超えて、多くの方々に便利に使ってもらっていました。連絡手段はある意味、使い分けをしていました。サイバーセキュリティ協議会（サイバーセキュリティ基本法に基づく情報連携の制度）では、若干、プロフェッショナルな情報共有を指向している雰囲気があって、初歩的なものを含むさまざまなお問い合わせに対する気軽なカスタマーサービス的な対応を期待するには、少々敷居が高いようなところがありました。そのように感じる方々にも JISP は気軽に使っていただけていました。

三角　なるほど、JISP は TOKYO2020 対策には役立ったのですね。JISP を導入しようとした目的は、TOKYO2020 関係者の SNS 的な役割を負うことでした。ただし、TOKYO2020 対策用に導入されたものであるため、それ以降のリソースの投入はないのではないかと思います。

山内　SNS 的な機能としてはうまくいきました。「異常はない」という報告もそうですし、「あの件はどうなっているのか」といった気軽な質問もわりと出てきていました。重要インフラ事業者ではないけれど、TOKYO2020 で新たに重要サービス事業者（バス、旅行事業者など）に加わった方々などから、「こういう情報共有手段は残さないのですか」という声も聞かれたくらいで、TOKYO2020 の後もしばらく運用されています。

TOKYO2020 のレガシー

三角　あらためてお聞きいたしますが、TOKYO2020 のレガシーとは何でしょうか。

山内　われわれ NISC の中だけではなく、TOKYO2020 組織委員会なども含めて申しますと、TOKYO2020 というイベントに向けて、どのような対策や体制、対応を取る必要があるのかについての認識の共有ができたということ。そして、大会開催期間中も含めて、そこに対応する多くの人たちが集まって経験値を積んだということ自体が、とても大きな資産だと思っています。

三角　結局、何人ぐらいの方々が取組に参加されたのでしょうか。重要サービス事業関係者も含むと、相当な人数になるのではないでしょうか。

山内　厳密にはわかりませんが、そのオーダーでいえば、四捨五入して万の単位に近いですね。重要サービス事業者は 300 弱、そのうち NTT、NHK、JR 東日本、メトロなど主要な事業者は 100 近くいらっしゃいました。それほど大きくない組織のシステムはサイバーの上にあまり乗っていないだろうと思っていたのですが、「いやいや、そのようなことはありません」と自分たちでおっしゃっていた方々もいたので、そういった方々もそれなりの対応をしていらっしゃったと思います。

もう一つ、TOKYO2020 の重要なレガシーとして、サイバーセキュリティという観点で担保したい重要インフラ防護の目的が広く受け入れられたことを挙げられます。その目的とは何かというと、サービスが止まらないことです。サービスが止まるという観点で見たら、物理的な要因も当然あって、サイバーも同様にその要因の一つであるということを、リスクマネジメントに関するガバナンス全体として理解をいただけるようになってきたと認識しています。つまり、経営層のガバナンスの観点で見たときに、別に特殊なものを扱っているわけでもなく、リスクマネジメントに関するガバナンスをどうするかということを考える中に、サイバーの場合はどうか、それに対応する者は誰か、ということが決まってくる、というビッグピクチャーがあるということを、受け入れていただけるようになったのが大きいのではないかと思います。

三角　そこは社会のカルチャーになったと思われますか。

山内　TOKYO2020 ではありませんが、少なくとも今、ランサムウエアなどを見て再認識している方々は結構いらっしゃると思います。

2023 年 7 月 4 日、名古屋港がサイバー攻撃の被害に見舞われた際の例があります。名古屋港統一ターミナルシステム（NUTS）がランサムウエアに感染して、復旧までに約 3 日を要しました。それがシステム障害だけでとどまったのかというと、そうではありませんでした。実はこの事案が発生したとき、SNS を含めていろいろな情報を集めていたのですが、そこでの大きな気づきがありました。それは何かというと、あるトラックの運転手の方がランサムウエアのために港の機能が止まると自身の仕事も止まることに気づかれました。その方は自動車関係の仕事をされているらしいのですが、「名古屋港のシステムが止まり、コンテナの搬出入ができなくなって、港の前でものすごいトラックの車列になっている」と SNS に投稿されていました。また、NUTS は業務の指示を送る電子メール等にも関連していたようで、電子メールでの連絡ができなくなって、「俺の仕事は今日、動かないらしい。このファックスでそれを知った」などとその画像とともに投稿されていました。ほかにも「〇〇自動車は名古屋港から他の港湾に移すというオペレーションがあるかもしれない」、「国際的に期日が決まっている荷積みの日程が変更される」等の書き込みもあって、物流のリアル面に響くことを、改めて皆さんが認識したということに気づかされました。


三角氏

2022 年 3 月 1 日、部品仕入先企業がランサムウエアに感染したことで、自動車会社の国内全 14 工場 28 ラインを停止することになったトラブルがありました。当時の多くの人々の受け止め方は、「自動車業界も大変だね」というものでした。ところが、名古屋港の事例は、実は一旦事象が生じたことで、幅広くとても多くの方々の業務が止

まったわけです。港湾が止まると、実は自分の仕事が止まる、ということをサプライチェーンで港湾につながる幅広い産業の方々が再認識をしたのです。そういう意味では、経営リスクの一環にそういう話が入っているということが認識されたということだと思っています。こういった経営問題そのものであるということは、「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日、サイバーセキュリティ戦略本部。以下「第 5 次行動計画」という）の案を検討・執筆していた人たちも認識していました。

こぼれ話なのですが、名古屋港の事案があったときに、「日本でも、とうとう重要インフラで大事件が起きましたね」と私のところに電話かけてきた方が何人かいらっしゃいました。

三角　港湾は、重要なインフラではあるのですが、第 5 次行動計画において重要インフラとはなっていません（注：当時。2024 年 3 月 8 日の改定で港湾も対象となった）。

山内　はい、「港湾は重要インフラではありませんよ」と応えると、皆さん、驚かれていました。「物流は重要インフラとなっていますよね」と言う方もいらっしゃいましたが、「物流事業者は重要インフラ分野ですが、港湾そのものは重要インフラとはなっていません」と答えると、「それでは、いつ入るのですか」との反応でした。それぐらいのインパクトのあった事件でした。

環境はできつつある──「サイバーセキュリティ対策は投資か、コストか」問題

三角　物流と港湾の関係は、航空と空港の関係と同様のものですから、港湾が重要インフラとなっていないということは、一般には、わかりにくいところですね。

サイバーセキュリティが経営リスクの一環であるということは、ご紹介いただいたような経験をするとその瞬間は実感されるのですが、その後、組織の文化として定着するかどうか、そこが今後の課題です。

山内　はい。三角さんが NISC ご在任中におっしゃっていた、「サイバーセキュリティ対策は投資か、コストか」の問題です。ようやく、サイバー保険について、適用される分野は限定されているとしても、少なくとも主立った企業の方々は認知するに至りました。そうすると、ある種のリスクをカバーする手段としてどうするのかということを考えなければいけないし、そのためには自分たちがシステムだけでなく、クラウド等も含めたサイバー全体にどう依存をしているのかということをしっかりと認識をしなければいけない。少なくとも、そこを知らずに経営を担うということはこれからの世の中では難しいものがあるのではないかと思います。一旦、システムに何か生じれば、自社の業務が本当に止まってしまうわけですから。自分たちの依存関係のあるサービスなりシステムが止まると、どのような影響があるのかについて知らないと、仮に障害が発生したときに大変な困難に直面しかねません。今の日本社会の文化からすると、例えば、午前中に障害が起きてサービスが停止したとしたら、遅くとも夕方には記者会見を一回は開かなければならないと思います。そのときに、記者から「御社の事業への影響は」と問われて答えられないと信用を失いかねません。そういう観点では、どこまで定量的に迫れるかという点は別にしても、少なくとも事業への影響についての問いには答えられなくてはいけないという認識は、経営者の間で広がりつつあるのではないかと思います。

三角　そうですね。システムへの依存度にはよりますが、経営者が認識しているかどうかが課題となってきますね。また、重要インフラや（経済安全保障推進法におけるいわゆる）基幹インフラに指定されていない事業者がどこまで認識するかも今後の課題となってきますね。

山内　そのとおりです。サプライチェーン上の中小企業の方々が、ご自身は重要インフラ事業者ではないとしても、その方々の業務が止まって、その製品・サービス提供先にいる重要インフラ事業者の方々の業務も止まるということが起こるのであれば、さきほど三角さんがおっしゃったとおり、その方々は重要なインフラです。そうすると、サイバーセキュリティに関わらないことかもしれなくとも、そのサプライチェーン上の企業に係るリスク対策の一環として、サイバーセキュリティ対策をどこまでやっているかということについて、重要インフラ事業者などにおいて、真面目にご検討いただきたいと思います。もし対策を十分に行えないのであれば、自社の能力を知った上で、これ以上のことが起きると、重要インフラ事業者などの業務も止まってしまう可能性についてどこまで説明するかということになります。

三角　サプライチェーンの評価を行えていないとまずいですね。

山内　そのとおりです。リスクマネジメントのリスク対応として、リスクを軽減するのか、リスクを受容するのか、リスク転嫁するのかという点まで考えていないと、マネジメントにはなりません。

三角　まずリスクを特定しないといけないですね。ただし、サプライチェーン上の企業のリスクが特定され、その企業において対策を十分にしていないことを理由に、ただちに取引をやめるというと、今度は不正競争防止法や下請法などの観点で問題が生じる可能性があります。

山内　その取引が成立するかどうかの根幹に響く本質的問題です。おっしゃるように法律上の話が生じるかもしれませんが、ただ、競争防止の観点でいうと、日本の場合、その取引先の方が唯一無二だったりする可能性がゼロではありません。特に中小企業で、ある特定の人にしかつくることができないものも存在します。そういうときにどこまで対策をするか、ということになると思います。一方で、重要インフラなどの事業者側から見たら、取引先の事業が継続されていることを期待したいわけです。仮に取引先の事業が止まったときにどうするかということは考えておかざるをえないと思います。

三角　そうした意識が全体に広がっていくとよいと思います。

山内　そのあたりの認識を徹底していただく、啓発していくことも重要です。

三角　そうすると重要インフラ事業者の範囲にとどまらず、幅広い方々に意識をいかに広げていくかということがこれからの課題ですね。

山内　はい。そういうことだと思います。

三角　わかりました。今回は、TOKYO2020 の開催に向けた準備段階、特に TOKYO2020 が新型コロナウイルス禍のために延期された影響への対応や、開催期間中の物理面とサイバー面での連携の仕組みなど、サイバーセキュリティ対策の舞台裏について興味深いお話をうかがうことができました。また、TOKYO2020 のレガシーとして、関係者の多くの間で、サイバーセキュリティに係る体制などの認識を共有し、経験値を高めることができたということ、そのようなレガシーは、第 5 次行動計画の実施などにおいても大いに貢献していくことになると理解できました。今後、重要イ

ンフラ事業者のみならず、より広い企業などにおいて、事業、サービスを安定して提供していくという目的を達成するためにリスクマネジメントが進むことを期待したいと思います。本日は、どうもありがとうございました。

（2024 年 2 月 2 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】

山内 智生（やまうち ともお）氏

総務省 サイバーセキュリティ統括官（最高情報セキュリティ責任者）、元内閣官房内閣審議官（内閣サイバーセキュリテイセンター）

1989 年京都大学大学院工学研究科修了、郵政省（現総務省）入省。情報通信国際戦略局技術政策課研究推進室長などを経て、2011 年 8 月内閣官房情報セキュリティセンター参事官（重要インフラ担当）。2014 年 7 月総務省情報通信国際戦略局宇宙通信政策課長を経て、2016 年 6 月内閣官房内閣参事官（内閣サイバーセキュリティセンター、基本戦略担当）、2018 年 8 月同審議官（内閣サイバーセキュリティセンター） 内閣サイバーセキュリティセンター副センター長・内閣官房国家安全保障局・内閣官房副長官補付［事態］、2021 年 10 月総務省大臣官房審議官（国際技術、サイバーセキュリティ担当）・内閣官房内閣審議官（内閣サイバーセキュリティセンター）などを歴任し、2022 年 6 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