2025 年 4 月

シリーズ 「日本のサイバーセキュリティ政策史」第 8 回

重要インフラのサイバーセキュリティ

東京オリパラに向けた鉄道運輸セキュリティの現場

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 8 回 は、2018 年 6 月～2021 年 6 月に東日本旅客鉄道株式会社（JR 東日本）で最高情報セキュリティ責任者（CISO）を務められた太田朝道氏をお迎えし、話をうかがいます。東京オリパラに向けて、国をあげてサイバーセキュリティ確保を図る中で、同社はどのようなリスクを想定し、どのような取り組みを行ったのか、またどのようなチャレンジを乗り越えたのか。世界有数の大規模鉄道事業者であり、幅広い事業を行う 70 社以上のグループ会社を束ねる本社の取り組みを明かしていただきます。

【出席者】
太田 朝道 氏
JR東日本メカトロニクス株式会社代表取締役社長・
元東日本旅客鉄道株式会社常務取締役

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

セキュリティとセーフティの両方を見る

三角 太田さんは 2018 年 6 月～2021 年 6 月に JR 東日本で最高情報セキュリティ責任者（CISO）を務められました。ちょうど東京オリンピック・パラリンピック（以下、東京オリパラ。2021 年 7～ 9 月開催）の準備と重なる時期ですから、相当重要な仕事を担われたと拝察します。

太田 そうですね。当時、私は技術イノベーション推進本部長を務めていて、システム関係も見ていたので CISO であり最高技術責任者（CTO）でもありました。あわせて、鉄道事業本部の安全担当も務めていたので、セキュリティとセーフティの両方の責任者でした。

三角 東京オリパラに向けて、貴社のリスクマネジメントにかかる関心事項は何であったのでしょうか。

太田　大きく 3 つありました。安全上一番に考慮したのは、人が密集して大混乱になることです。東京オリパラが開催されれば、当然、東京を中心とする各駅構内は混雑します。当時はコロナ禍前だったので、今よりも通勤・通学時間帯などは混雑していました。そこに例えば朝、メインスタジアムの国立競技場で競技が行われるとなると、観客も加わります。もし、人身事故や車両トラブルなどで運行障害が発生すれば、人が密集して大混乱になります。2022 年 10 月に発生した韓国・ソウルの梨泰院の雑踏事故では 150 名以上が亡くなりました。日本でも 2001 年 7 月に兵庫県明石市の花火大会で歩道橋事故が起きています。そこで、特に競技場に近い千駄ヶ谷駅と信濃町駅について、人流マネジメントの専門家のお知恵もお借りして、混雑緩和のための人流予測や制御の方策について検討を重ねました。

三角　それは駅の構内だけはなくて、出入りの部分も含めてですか。

太田　駅構内までの出入りの部分は JR 東日本の直接の管轄ではないので、自治体や警察の方々と協力しながら、ということになります。

2 つ目は、競技終了後に帰宅困難者が発生することです。各競技の会場は東京の中心部だけではなくて、東京外縁部の各所にも設置されました。そこで競技が終電近い時間帯に終了した際にも、お客様が自宅や宿泊先にまで行き着く必要があります。ただ、検討しようにも、オリンピック委員会（JOC）から各会場の競技スケジュールをいただけるまでには時間を要します。仕方がないので、JR 東日本と東京メトロ、東京都交通局の 3 者で、とにかくわれわれで前提をつくってシミュレーションしようといって、夜の延長運転計画案を作成しました。そして、その後民鉄各社とも情報共有して連携しました。

ただ、たいへん残念なことに、結果的に東京オリパラは無観客開催になってしまったので、これらの取り組みは空振りに終わりましたが、われわれにとっては非常によい知見を残すことができたと思います。

三角　雑踏において安全を確保するためには、乗客などその場にいる人たちにいろいろな情報を流さないといけないし、人流の制御をしないといけないと思います。そこはどのように行うつもりでしたか。

太田　JOC からは鉄道輸送に関する物事は、基本的には事業者でお願いします、といわれていました。ですから、国土交通省等のお力をお借りしつつ、まずは、われわれ事業者間で連携してやるしかない、という思いでした。

三角　ダイヤの調整などは事業者間でやるということでしょうか。駅構内で大混雑したときには、乗降客の制御はどのようにするつもりだったのですか。

太田　あらかじめ、できる限り人流が滞りづらくなるルートを設定して、ご案内することがまず大切です。ただ、どうしてもオーバーフローとなる事態が予測されたときは、あらかじめ決めておいた箇所で、人流をストップさせる必要があります。イベント対応などの場合には、警察のお力をお借りすることもあります。人流の詰まりが大規模になると制御不能の状況になり、事故につながりますので、絶対に避けなければなりません。

三角　東京オリパラに限らず、自然災害や事故などで運行障害が発生した際と同じですね。


太田氏

太田　同じです。もう一つ、東京オリパラ開催期間中は訪日外国人も相当増えるので、そのことも考慮しました。

三角　言葉や情報の流し方をどうするのかといった点でしょうか。

太田　そうです。社員の英語教育に力を入れるとともに、IT を活用した外国語での案内を充実させました。例えば、乗務員が持っているタブレットで翻訳した内容を車内で放送できるようにしたり、運行障害時に駅で掲出する運行情報について、二次元バーコードをスマートフォンなどで読み取れば、日・英・中・韓の 4 カ国語で案内することも実施しました。先ほど申し上げたように、東京オリパラは無観客開催になりましたが、それらのサービスは現在も活用しています。

三角　いまインバウンドが増えていますし、意味はありましたね。

太田　そのとおりです。

システムのセキュリティ対策

三角　リスクマネジメントにかかる関心事の 3 つ目とは何でしたか。

太田　システムのセキュリティです。鉄道のオペレーションについては、われわれは長い経験と知見を持っていますが、システムのセキュリティ関係は、社内の担当部署と情報システム専門のグループ会社「JR 東日本情報システム」と連携して取り組みました。同社は JR 東日本が保有する鉄道系のシステムのほぼ全てを所管しています。

三角　運行のためのシステムですね。

太田　ええ、運行の制御システムの設計、製作、運用管理を担っています。例えば、JR 東日本のシステムに何か異常が起きたことに備えて、JR 東日本情報システムが 24 時間体制で対応しています。鉄道の運行を制御・管理するシステムは結構たくさんあって、そこに対してきちんとした体制を取っていこうということが一つ。

もう一つは、社内向けの情報システムです。そこをセキュリティ上強固にするということです。

三角　社内システムは情報系で、運行のほうは制御系ということですね。

太田　ええ、そのとおりです。制御系については、運行管理システムなどのシステムがたくさんあるのですが、それらに対して、自分たちでもセキュリティ上問題がないかどうかを、外部機関を使って診断試験を実施しました。

三角　太田さんが着任した頃のことでしょうか。政府がそういうことを点検するようにと具体的かつ明示的に求め始めたのは、2016 年度後半頃だったと思います。

太田　制御系システムのセキュリティ診断は 2016 年度から毎年実施していました。私が CISO に着任したときにもちょうど診断を行っていて、その過程の後段に入った頃に NISC からも診断するよう要請がきました。われわれが多くのシステムを幅広く診断していたのに対して、NISC の要請は、中でも最重要システムを選んでリスクチェックせよということで、われわれがやっていたものよりも追加の点検項目がありました。


三角氏

三角　どんな項目がプラスアルファ的なものとなりましたか。

太田　NISC がいろいろなリスクシナリオを持たれていて、技術的・運用的・組織的な多面的な観点から検証しなさいということでした。われわれはどちらかというと技術的な観点を中心に見ていたので、運用的・組織的な面でプラスアルファ的な知見をいただいたと記憶しています。われわれとしても最重要システムについては、改めて徹底してやろうということで NISC からの要請に対応しました。

三角　組織的観点とは、情報セキュリティマネジメント的な話ですね。制御系そのものに関する点検でしたら、情報セキュリティマネジメント的な話よりは、運行管理的な面をしっかり見るということでしょうか。NISC と制御系の事業者さんの関心事項に乖離はありませんでしたか。NISC は情報セキュリティの分野では長年経験があります。ただ、情報セキュリティの分野がだんだん広がり、制御系システムのセキュリティについても政策対象となってきました。政府はある意味で第三者的なところがあるので、包括的、総合的見地から見てしまいがちです。

太田　「横断的リスク評価」にあたっては、事前に NISC の担当者との調整を通じ、シナリオや対象システムを摺り合わせ決定しましたが、このやりとりがありがたかったです。政府側の包括的、総合的見地とわれわれの個別技術的見地を融合させることができたと思います。また、幸いにして制御系システムについては指摘事項はなく、東京オリパラが延期されたことで、2020 年に「対応を推奨する事項」についてのフォローアップも NISC から受けることができました。

三角　NISC の提示した評価項目は基本的に情報系であったと思います。なので、制御系の方には直接適用できないところもあったかもしれません。

太田　おっしゃるとおりですが、従前は技術的見地による「点」での確認になりがちでしたが、一気通貫のシナリオによる「面」での確認やリスク評価ができたのは、たいへん参考になりました。また、今回制御系システムを診断した「横断的リスク評価」をもとに、情報系システムについても多面的に点検・評価することができました。こちらの方は、さまざまな課題が浮き彫りになりました。

全グループ会社を一つのセキュリティネットワークに束ねるまで

三角　情報システムに対してはどのような取り組みをされましたか。

太田　当時、本社が十分に情報セキュリティ対策を講じていても、グループ会社のセキュリティレベルが低ければ、そこがサイバー攻撃の脅威にさらされて、網羅的に被害に巻き込まれるという事象が世の中ではかなり発生していました。そこで、JR 東日本でも全グループ会社を点検・評価したところ、会社ごとに大きなレベル差があって、対策が急務であるということがわかりました。多くのグループ会社にとって、情報セキュリティの優先度は高くなかったわけです。そこで、CISO として、70 社以上あるグループ会社の社長を前にセキュリティ対策を強化するよう強く要請するとともに、具体的な対策を提示しました。

三角　事業の種類によっては、情報セキュリティが優先事項となりにくいところもあったでしょうね。情報システム会社だったらセキュリティ意識は高いけれど、情報システムの利活用がメインではな

い事業会社、例えば機械系や生活サービス系の会社は必ずしもそうではないかもしれないですね。

太田　ええ。JR 東日本情報システムは、われわれとタッグを組んでセキュリティ対策にしっかり取り組もうという立場でした。一方で、グループ会社の中には、情報セキュリティに対する必要な人員まで配置できないところも多くありました。

そこで、全グループ会社に JR 東日本のトータルセキュリティネットワークの中に入ってもらうことにしました。そうすれば、JR 東日本情報システムが 24 時間監視するかたちになります。そうすることにより、グループ内のシステムを常時モニタリングできるので、油断はできませんが、不審な挙動があれば察知できることとなります。各社には、その点を納得してもらうべく、丁寧に時間をかけて説明しました。私の後任の CISO のときに、計画していたグループ会社全社がトータルセキュリティネットワークに組み込まれました。

三角　サイバー攻撃に関してグループ会社が踏み台になる可能性があるということを政府は指摘しましたが、そうしたことによって、全グループ会社を束ねることができた感じでしょうか。

太田　それもありましたし、JR 東日本グループの話ではないですが、実際、親会社ではなくグループ会社がサイバー攻撃を受ける事象が多く発生し、報道されていました。私は当初からその話をしていましたが、各社が自身の課題であることを理解してもらう点に労力を要しました。

制御系は絶対に守らないといけない

三角　太田さんの在任中、ほかにどのような取り組みをされましたか。

太田　一つは、コンピューター・セキュリティ・インシデント・レスポンス・チーム（CSIRT［シーサート］）訓練を初めて実施しました。

三角　シナリオづくりなどはどうされたのですか。

太田　第 1 回目は、関係企業からノウハウをいただきました。第 2 回目は、われわれとは別の分野の重要インフラ企業から「一緒にやろう」とありがたい提案があって、一緒に実施して、かなり勉強になりました。

三角　それはいつ頃の話ですか。

太田　担当クラスでは 2016 年度から始めていましたが、社をあげて大々的にやり始めたのは 2019 年度からです。

三角　先ほどお話ししたように、2019 年頃には NISC が情報連携のシステムを構築し、情報連携の訓練などの音頭を取り始めていますが、それとはまた別にやっていたわけですね。

太田　自主的に実施しました。

三角　それはインシデントがあったときの情報連絡の確認だけではなくて、実際に対処するシナリオも含めて実施していたのですか。

太田　そうです。先ほどいった、運行の制御システムに影響が出たことを一つの想定材料としてシナリオを作成し、シミュレーションしました。サイバー攻撃を受けたときに何が起こるのかを想定し、どういうふうに初動をして、どういう情報を連携し合うかを明確にしました。事故対応能力や不測の事態への応用力の能力向上につながったと思います。やってよかったです。

三角　運行が安全に回るかどうかも含めて点検しているわけですね。システムが使えなくなった場合、マニュアルで、例えば運行間隔を、過密な平日ダイヤから比較的余裕のある休日ダイヤに転換して運行するといったことも考えられているのでしょうか。

太田　それは難しいです。手作業で運行させることは、この首都圏の過密ダイヤでは現実的ではありません。サイバー攻撃とは関係なく、制御系システムに不具合が発生すれば、運行を停止して回復を優先します。それと同じです。安全が確証できなければ基本的に止めざるをえません。ですから、制御系システムは絶対に守らないといけないわけです。

狙われているという話もあったが、影響はなかった

三角　情報システムにサイバー攻撃を受けたとき、制御系については切り離されているから問題ない、というふうにすぐに判断するのですか。それとも、つながっている部分もあるかもしれないから、要注意と警戒してシステムを止めたりするのですか。

太田　そこは、システム的には完全に独立しているので運行への直接の影響はありません。

三角　それがはっきりしていればだいぶやりやすいですね。例えば、米国では、鉄道会社ではありませんが、情報系にサイバー攻撃を受けたとき、制御系に影響はないとは判断できないから、安全のためにサービスを止めた事案もあります。

太田　ただ、情報系には 2 つ意味合いがあります。今、私がいった情報系とは、いわゆる社内システムです。同じ情報といっても、チケッティングやお客様案内に関するシステムは、われわれは制御系に近い位置づけであると考えています。

三角　私が NISC にいたとき、重要インフラ事業者間で横断的な点検を何回か実施してもらいました。自社でできることだけではなく、他社からいろいろなサービスを受けて自社のサービスを成立させているところもあるので、他社がサイバー攻撃を受けたら影響を受けます。

太田　鉄道の運行制御系以外の多くのシステムは、パブリック・クラウドも使い始めているので、クラウドやネットワークのセキュリティによってしまうところが大きいです。最近では、それらのセキュリティレベルもかなり上がってきていると思います。

東京オリパラ前は、いろいろな情報がありました。鉄道が狙われている、という話もありました。東京オリパラは私の退任後となりましたが、結果的にいうと、おかげさまで影響はなかった。これはたいへんありがたかったです。

政府主導のサイバーセキュリティの取り組みをいっそう積極的にやってほしい

三角　2019 年ラグビーワールドカップ（W 杯）のときには何かありましたか。NISC では東京オリパラに先立つ取り組みとしてラグビーW 杯に対していろいろと準備していましたが、貴社ではどうだったのでしょう。

太田　東京オリパラ対策の流れにありましたので、W 杯のために、特別な準備はしませんでしたし、サイバー攻撃を受けるようなこともありませんでした。

サイバー攻撃を受けた事例としては、東京オリパラ後ではありますが、2023 年 1～2 月に JR 東日本のホームページが DDoS 攻撃を受けました。そのときは、早い段階で NISC から情報提供いただきました。攻撃は複数回続いたので、その後の攻撃に備えた監視・対応体制を取る上で情報提供をいただいたことは、たいへんありがたかったです。一民間企業でやれる範囲には限界があるので、予算を増やしていただき、政府が主動して情報提供などサイバーセキュリティ確保の取り組みをいっそう積極的にしていただけるとありがたいという思いです。

三角　どういうところを政府に主導してやってほしいですか。

太田　一つは、サイバー攻撃などが発生したときに、関係企業に直ちに情報提供していただきたい。2023 年 1～2 月に DDoS 攻撃を受けた際、もちろん当社としても検知はしましたが、どこからどういう手法で攻撃されているのか、なおかつ、どう対応すればいいのかを NISC から発信していただき、たいへん有益でした。ありがたい情報だったがゆえに、さらに早く情報をいただいていたら、より被害を小さくできたのではないかと思うのです。NISC はもっと早い段階で検知されていたのではないでしょうか。

三角　どこから情報を得ているかによると思います。NISC が直接モニタリングしているネットワークは、国・政府と独立行政法人、日本年金機構等までです。幅広いネットワークを見る中で検知しているというよりは、協力関係を持っている関連機関などさまざまなところから情報を入手します。具体的に当該事案についてどこから情報を得ているかは、私は知る立場にはありませんが、国の機関であれば、例えば国立研究開発法人情報通信研究機構（NICT）などがネットワークを観測している中で、日本に対する外からの DDoS などの攻撃の状況はある程度知ることができると思います。

太田　個人的には、NISC やデジタル庁の権限をもっと増やしたほうがいいと思います。

三角　どのような権限でしょうか。

太田　予算や施策などを決める権限を含め、情報系に関わるあらゆる権限です。一昨年、台湾に行き、デジタル発展省の方々と面談させていただく機会がありました。同省は、日本のデジタル庁に比べると、強大な権限と予算を持っています。各省庁の情報系の権限を全部とりまとめたようなかたちです。

三角　日本では、関係省庁なども多く、すぐに実現できるかというと難しいところがあると思います。

太田　情報系は横串で。それも太い横串が必要です。日本ではどうしても各省庁での縦割りになりがちですね。

三角　企業の立場からすると、報告先は一箇所にしてほしいでしょうね。それも、フランスやシンガポールなどのように、規制当局ではなくて、技術的なことについて気軽に会話できる NISC のような専門の官庁に集めるようにすれば、結果的に有益な情報が集まりやすくなると思います。

太田　NISC やデジタル庁にはもっと力を持っていただいて、引っ張っていっていただきたいと思います。

三角　NISC は権限を強化する方向にありますが、安全保障分野が中心となりそうです。安全保障という言葉は、万人に受け入れられた明確な概念規定はなく、意味は抽象的な範囲で多様であるといわれています。法令が整備・改正され、政策の対象範囲が改めて明確になっていく段階で、発展的改組される NISC の責任や権限、そのサービスの内容もはっきりすると思います。今の流れは、政府主導の取り組みはいっそう積極的に強化されていくのではないかと思います。

本日はありがとうございました。

（2025 年 1 月 21 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】

太田　朝道（おおた　ともみち）氏

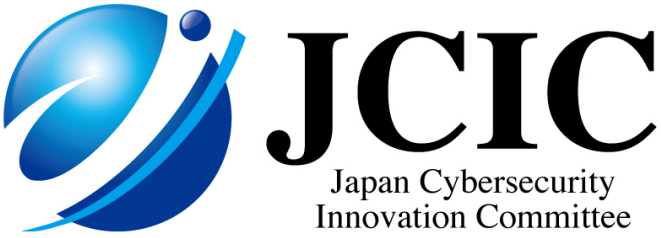
JR東日本メカトロニクス株式会社代表取締役社長・元東日本旅客鉄道株式会社（JR 東日本）常務取締役

1985 年 4 月日本国有鉄道入社、1987 年 4 月 JR 東日本入社。2016 年 6 月常務執行役員鉄道事業本部運輸車両部長、2017 年 6 月常務取締役鉄道事業本部副本部長、2018 年 6 月常務取締役技術イノベーション推進本部長、鉄道事業本部安全企画部担当、2021 年 6 月JR東日本テクノロジー株式会社代表取締役社長などを歴任。2018 年 6 月～2021 年 6 月最高情報セキュリティ責任者（CISO）・最高技術責任者（CTO）。2024 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