予測・予防・対応の視点で考えるサイバー攻撃

～自然災害対応との違いは何か?～

1月11日に開催された第13回パブリックカンファレンス

TIEMSとは

国際危機管理学会TIEMS（The International Emergency Management Society）は米国ワシントンで1993年に設立され、現在、ベルギーに事務局を置く国際的なNGO組織。約50カ国に会員を持ち、研究者や、管理者、医師、社会科学者のほか、危機管理や防災に関心が高い人々による世界的なネットワークを築いている。危機管理や防災に関するさまざまな対策や技術の情報共有を図り、自然災害やテクノロジー災害からの回避や、減災、危機対応力、復旧の能力を上げていくことを目的にしている。代表は、ノルウェー人のK.Harald Drager氏。日本支部は2012年5月に設立された。支部長は、防災科学技術研究所理事長の林春男氏。日本支部の入会費・会費は無料で、危機管理に関心があれば誰でも入会できる。主な活動として、年3回、パブリックカンファレンスを開催している。申込みは、本誌ウェブサイト（http://risktaisaku.com）のTIEMS会員募集ページより。

パネルディスカッションの様子

都市減災サブプロジェクト
Urban Resilience
都市災害における災害対応能力の向上方策に関する調査・研究

文部科学省委託研究 都市の脆弱性が引き起こす激甚災害の軽減化プロジェクト「3都市災害における災害対応能力の向上方策に関する研究・調査」の活動の一環です。

TIEMS（国際危機管理学会）日本支部は2017年1月11日、「予測・予防・対応の視点で考えるサイバー攻撃　自然災害対応との違いは何か？」と題したパブリックカンファレンスを都内で開催した。

講演を行ったのは、東京電機大学教授の佐々木良一氏、名古屋工業大学大学院教授の渡辺研司氏、そしてNTTセキュアプラットフォーム研究所理事・主席研究員の前田裕二氏。

佐々木氏は「IoT時代におけるサイバー攻撃のシナリオ」と題し、パソコン内のデータを暗号化し、身代金をユーザーに要求するコンピューターウイルス「ランサムウェア」を中心に解説。あらゆるモノがインターネットにつながるIoT時代においてはウェブカメラや家庭用ルーターなどが踏み台になるほか、家庭用ロボットがハッキングされる可能性もあるなど警戒を促した。

渡辺氏は近年の金融機関のシステム障害などを例に、こういった事例がサイバー攻撃を企てる者にとってヒントを与える可能性があると指摘。また実際に攻撃を受けた際には、能動的にシステムを止め、捨てる部分、守る部分の線引きをして被害を最小限に食い止める勇気がトップには必要だと説明した。

前田氏はウクライナの電力会社など、国内外のサイバー攻撃の事例について解説。その後、暗号化技術やログ情報分析、サイバー攻撃対策といったNTTのセキュアプラットフォーム研究所の取り組みを説明。2020年東京オリンピック・パラリンピックでは組織を超えた統合的な危機対応が必要であると述べた。

続いて、佐々木氏、渡辺氏、前田氏によるパネルディスカッションが開催された。コーディネーターは静岡大学情報学部講師の井ノ口宗成氏。

前田氏は安全性の確保について、「100％安全は無理。90％は可能として、残りの10％は保険や社会全体でカバーすることを考えたほうがいい。攻撃者をゼロにすることは不可能に近い」と説明。渡辺氏も「攻撃者が絶対有利。また人工知能（AI）が発達し、人間との機械の主導権がどうなるかも注目だ」とした。そして佐々木氏は「予測は難しい。攻撃の入口で頑張っても効果は薄いと言われるが、それでもリスクを30％下げる。入口対策の否定はよくない。入口対策は予防医学、中や出口での対処は高度医療だ。トータルでの対策を考えるべき」とした。

また安全性を高める方法については佐々木氏が「CSIRTを大学にも作っている。対策の組み合わせやコストと効果のバランスなどトータルでの対応検証と、組織内のコミュニケーションは大事だ」と述べた。

前田氏は「小さなデータを集めてリスクコミュニケーションをとることが大事。なにかあったらネットから遮断し、仲間と情報を共有すること。でもメモリを残すため電源は切らない。感染があったらしかるのではなく、情報をあげてくれたらほめるくらいの対処をすべきだ」と情報共有の大切さを強調した。

プライバシーや通信の秘密について渡辺氏は「社会システムを担っている事業者は、欧米では行政への報告義務が様々な形で生じるようになってきた。プライバシー問題では街角の防犯カメラがあるが、欧州ではプライバシーより安全をとるようになりつつある」と説明。佐々木氏は「通信の秘密は尊重されないといけないが、攻撃があるときはオープンにした方がいい」とした。前田氏も「日本は先進国で唯一、通信内容の解析ができない。スノーデン事件でも知られたように、米国ではCIAが解析を行っていた。そこのあたりの差は大きい」と説明した。

●IoT時代におけるサイバー攻撃のシナリオ

東京電機大学教授
佐々木 良一氏

サイバー攻撃の被害はランサムウェアをはじめとして様々な形で増えている。サイバー攻撃にはこれまでに2つのターニングポイントがあった。1つは2000年頃で、科学技術庁などのホームページが改ざんされたときだった。想定していた攻撃が実際に日本で起こってしまったことが衝撃だった。

2つ目のターニングポイントは2010年ころ。典型的な例はStuxnetの出現になる。Stuxnetは米国とイスラエルが協力して開発したとされるマルウェアで、イランの核燃料製造用の遠心分離機を破壊した有名なウイルス。イランの核開発を1年以上遅らせたと言われている。WindowsのPCから他のPCに感染し、普段は何もしないが、遠心分離機の回転を制御するソフトを見つけると動き出す。2011年には三菱重工業へも標的型攻撃が行われた。

2000年ごろと2010年以降では様相が変化している。まずは攻撃目的。当初は改ざんなどでメッセージを残すといったハッカーによる自己PRが中心だった。第2のターニングポイント以降は金や機密情報目的が増えている。犯罪者もハッカー以外にアクティビストという政治的主張者も目立つようになった。また犯罪者の組織化も進み、国家スパイや産業スパイもいる。標的はITから電力や交通といった重要インフラにまで広がりを見せている。攻撃パターンは不特定多数を対象にしたものから「標的型」という攻撃対象を絞ったものに変わってきている。先ほどのStuxnetによるイランへの攻撃だけでなく、日本年金機構への攻撃もそうだ。

日本年金機構に送られてきたメールは添付ファイルを開けたくなる文面になっており、4名がメールを開封してしまった。感染したPCから、ウイルスは環境を把握した上で、C＆Cというサーバーに強制的にアクセスさせて、その環境に最適な攻撃プログラムをダウンロードしてから暴れ出した。最終的には日本年金機構のPCやサーバー31台が感染してしまった。年金番号は基幹システムだけで扱うはずが業務の効率化のため、本来なら無いはずのPC内にあったために流出が拡大してしまった。なかなか足がつかない、高度で組織的な犯罪だったといえる。流出した情報は全部で125万件だったと報告されている。

この攻撃の特徴はウイルスの亜種をどんどん作り、ウイルスチェックやワクチンからの攻撃をすり抜けるように改良を重ねている点。そのファイル作成の時間を解析すると、9～12時、14～17時に偏っていた。一般的なの勤務時刻とほぼ一致している。普通、ハッカーの攻撃なら1日中、あるいは夜のみになる。おそらく企業のような組織によるもので、日本より1時間の時差があったことから、その組織の拠点となった国は断定できないが推測はできる。

米国では2015年に同様の攻撃が行われた。米連邦政府の人事管理局がサイバー攻撃を受け、政府機関の職員や契約業者ら2150万人分もの身元調査にかかわる情報が盗まれるという大変な被害を受けた。同年にはドイツでも連邦議会にハッカー攻撃が仕掛けられ、PCの総取り換えを余儀なくされた。サイバー空間では攻撃は簡単だが、守備はとても難しく対策は限られている。

今後はどのようなサイバー攻撃が増えるか。IoT時代となりその前兆のようなものはある。ひとつは被害形態が多様化している。従来は機密性の喪失、つまりは機密情報を盗むことに主眼が置かれていた。これからは完全性

や可用性の喪失ということで、情報の書き換えやシステムの停止などを狙うだろう。被害形態の多様化や攻撃対象の多様化、攻撃の多様化が起きる。結果として「機密性」の喪失だけではなく、サイバー攻撃でデータの欠損など「完全性」が崩れ、システムを継続して動かす「可用性」も失われる。

最近話題になっているのが身代金要求プログラムのランサムウェア。相手のPCの中に入り込みファイルを暗号技術で強制的にパッケージする。身代金を要求して支払われたら暗号を解除する仕組みで、足がつかないようビットコインで払うよう要求される。トレンドマイクロ社の調査によれば、25.1%の企業がこのウイルスの被害にあい、被害にあった企業のうち62.6%が支払っている。支払額は数百万円のケースもある。支払えば元に戻る場合が多いが、後で何度も攻撃を仕掛けられる可能性はあるし、裏社会に資金が流れるのでおすすめはできない。身代金なしでの対応では解除ツールを使うほか、ボリュームシャドウコピーによる復元もできる。しかし何よりも、バックアップをしっかりとり、保管することが一番の対策になる。このウイルスにかかるとデータが暗号化されるので、完全性の喪失と可用性の喪失が同時に起こる。今、最も注目すべき攻撃なので注意してほしい。

IoT化が加速すると様々なものがネットワークにつながるので、攻撃対象も当然多様化する。対策はとても難しい。制御システムへの攻撃の例としては、2015年にウクライナ西部の都市イヴァーノ＝フランキーウシク周辺で140万世帯が停電した。ウクライナ側はロシアからの攻撃と主張している。五輪を控える日本でもサイバー攻撃による停電には警戒が必要だ。

今後の一般的な攻撃対象として特に心配されているのが自動車。実際に起きた犯罪としては増幅器を使って電子キーの電波を増大させ、持ち主が車に対し近くにいると認識させ、ロックを解除させるケースがあった。そして車中のものを盗む。また、危惧されているのは外部から車をコントールしてしまう方法。良識的なハッカーが自動車会社に事前通告したうえで、自動車に対し遠隔操作を仕掛けた。すると数マイル離れたところからハンドル操作やブレーキの無効化などを実際に行うことができた。攻撃により車を制御するCAN（車載ネットワーク）が、つながらないはずのネットとつながってしまったためだ。ほかにもコンピューターが組み込まれている情報家電、防犯カメラ、コピーとFAXの複合機、医療機器などあらゆるものが攻撃対象になる。監視カメラのパスワードを設定しなかったばかりに、映像の流出も起こった。

今後の対応だがますます攻撃は激しくなる。IoT時代は制御システムが大事で、セキュリティ対策は難しい。技術革新が進むことから、既存のIoTと今後のIoTに対する対策は分けて考えたほうがいい。前者はセキュアケートウェイ、後者は暗号認証機能を持つ低価格のセキュアチップの利用が効果的になるだろう。

攻撃元の組織化が進んでいる。従来のサイバー攻撃はハッカー自身によるものが中心だった。最近は犯罪者がハッカーを雇って行ったり、組織化したりしている。またロシアなど国家の関与も疑われている。サイバー犯罪は割のいい犯罪という話がある。なぜなら元手がかからず、足がつきにくい。サイバー攻撃のほか殺人などの請負までウェブを通じて行われる始末だ。

企業にとっての脅威には、サプライチェーンから調達した機器にプログラムが仕込まれ勝手に通信されるケースも考えられる。米国では中国の大手通信メーカー「HUAWEI」から調達した機器が深夜に動き、本国にデータを送信していた疑惑がある。また、中国のスマートフォンメーカー「Coolpad」が製造したハイエンド向けAndroid端末にバックドアの設置が発覚。信頼している製造国から買えばいいというわけではない。部品の製造国も疑わねばならないからだ。

研究者は攻撃の進化に対応できるように今から検討する必要がある。一般の技術者はセキュリティの動向を注意深く監視しなければならない。

●事業継続とサイバー攻撃

名古屋工業大学大学院教授
渡辺研司氏

企業活動はIT依存が進み、情報システムが止まると業務がほぼ止まってしまう。情報システムはデータや取引の高速大量処理を、24時間365日止まらず続け、ネットワーク経由の分散処理もクラウド・コンピューティングなどにより進んできている。ユーザーには便利だが止まったら一大事。もはや手作業でリカバリーできないレベルに達している。さらに、ネットワーク経由でシステム同士がつながっているので、障害が発生した瞬間に、ドミノ倒しのように広い範囲に影響が波及、どのシステムやプログラムが原因かを特定しにくい。

一般的に、情報システムには、安定性、安全性、堅牢性、可用性、拡張性、柔軟性、信頼性が求められるが、経営効率化（コスト削減、アウトソーシングなど）に伴い全ての機能を維持するのは困難だ。そして1つでも欠けたところから問題が拡散してしまう。

2010年に、ニューヨーク証券取引所で、システムの意図しない連鎖障害によって、高速取引による大量の売り注文が発生し、過去最大の下落幅を記録したケース（フラッシュ・クラッシュ）がある。ダウ平均指数は一挙に前日比マイナス9.2%とブラックマンデー以来の大暴落を記録した。15分ほどで回復したが、原因究明は長期化し、その間、①証券会社の誤発注、②プログラム・ミスなどが原因として報道された。いずれにしても、何らかの理由で売買の需給バランスが瞬間的に崩れたことが引き金となり、HFT（高頻度プログラム取引）や、個別銘柄のボラティリティを制御する仕組みが機能しなくなり、さらに、同一銘柄が複数の市場で取引される市場構造が、問題を増幅させたといえる。このことは個別最適を求めるシステム群が接続されたシステム（system of systems）は、その集合体が全体最適を実現できるとは限らないということを示しており、また、この現象は意図的に再現可能、つまりサイバー攻撃によっても引き起こすことが可能であるということがわかる。

もう1つの例は、翌年、2011年3月の東日本大震災直後に、大手金融機関の義援金振込受付用の口座設定ミスにより、大規模な振込・ATMサービス障害が発生した事故である。都内2支店の複数の口座にあらかじめ設定されていた上限件数を超える大量の振り込みが集中したことが発端となった。銀行の口座というのは、いつどこで、いくらを下ろしたのか、誰から振り込みがあったかログを通帳に記帳印字したり、ウェブ表示できるように保存したりしておく仕組みになっているが、義援金では、短時間に多くの小口を含めて大量のデータが入ってくるので、そういった記帳ができるような形でのデータのログは残さない。その設定を間違えただけで、データがオーバーフローしてシステム障害を発生させ、振込・ATM障害が3日間にわたり発生した。この問題を起こしたシステムのモジュールにはPL/1という1980年代に金融機関の勘定系システムにつかわれていた開発言語で開発されたプログラムも含まれており、このセキュリティレベルの低いプログラムがまだ大手金融機関で使われていることがわかったことで、意図的にそこを攻撃して上記のような状況が再現可能、すなわちサイバー攻撃によって引き起こすことが可能であることがわかる。

ところで、リスク分析の手法にイベント・ツリー・アナリシス（ETA）という手法がある。これは、何か事象が起こると、連鎖的にどのようなことが起こっていくのかを、木の枝になぞらえて、時間経過とともに展開していく考

え方。例えば、地震発生によって物理的破壊、津波や液状化が発生するが、その先に情報システ障害も発生する、という起こりうる事象を想定する際にも用いられる。一方、フォルト・ツリー・アナリシス（FTA）という分析手法は、何か障害発生が懸念されるときに、その障害はどのような原因によって起こり得るのかを遡って分析する考え方。例えば上記の銀行のシステム障害で、他にどのような原因で同じようなシステム障害が起きるかを考えると、停電であったり、システムの統合によるミスであったり、人為的なヒューマンエラーであったり、あるいは、外部犯行やサイバー攻撃も原因になり得る。つまり、多様な要因による再現可能性を意識しなくてはいけないということだ。自然災害だからこうなってしまったというのではなく、その現象はたまたま自然災害によって引き起こされたが、他の要因でも発生する。ここに複数の脆弱性があるということを認識して、それらの脆弱性を潰すことも忘れなく対策していく必要がある。ETAとFTA、複眼的な視点を持たないと、いつまで経っても特定原因に伴う事案対応だけ限定的に取り組み、その他の要因による事案発生に対応できないということもありえる。

もう1つはシステムの自動化による功罪という点からも対策が求められる。高度に自動化されたシステムにおける人間の仕事は、自動装置が設計通りに動いていることを確認するだけでいい。しかし、それは同時に担当者のモチベーションや緊急時の対応能力の低下を招き、極めて稀にしか起こらない異常を見つけることが難しくなる、というジレンマを生み出している。そのような弱点をついてくるサイバー攻撃もある。つまり、人間と機械の関係を考えた時に、自動化が進んでいるシステム群に対して、何か通常時でないことが起きた時に、それをどうやって検知できる能力を身に付けるか、ここが大きなポイントになってくる。

一方で、サイバー攻撃の目的や手法は、高度化、複雑化している。サイバー攻撃は、検知のタイミングが遅れることが問題である。また例え検知ができても、原因究明をしている間にどんどん被害が広がるので、障害対応として、情報システムを継続させるだけでなく、能動的に止めるという経営レベルでの意思決定がしっかりできるかが、今問われている。

普通の経営者は情報システムを止めたくないだろうが、これが遅れたばかりに被害が広がるケースが多い。例えば、これ以上システムを動かしておくと、被害が拡大するので、システムの能動的な停止により被害を受けるお客様には迅速に通知をし、同時に記者会見や損害賠償金の支払い等の準備を始める、というような、情報システムを止めることによるインパクトを最小化させる判断をして、それに伴い必要はアクションを適時にとっていく必要がある。判断が遅れたら、ずるずると攻撃をされ続け、対応は後手に回ってしまう。また情報の機密性を死守しなくてはいけないという考え方だけではなく、場合によってはある程度までは機密性を捨て、ほかの残る情報を守るという判断も必要となる。現場がそれを判断できるような権限委譲やルールの制定と、それらのジレンマを感じながら意思決定するような訓練、演習もしていかなくてはいけない。

現場と経営の間を取り持つCSIRT（Computer Security Incident Response Team）の役割も不可欠だ。今起きているサイバー攻撃による情報システムの障害は経営上どういう影響をもたらすのか、売上がどれだけ下がるのか、お客様にどれだけ迷惑がかかるのか、それとも社会全体に迷惑がかかるのか、それはどの程度の規模なのか、どの時点までに経営者はシステム停止などの判断しなければいけないのか、CSIRTは、こうしたインパクトをわかりやすく翻訳し、経営陣に選択肢と共に説明し意思決定を求めなくてはいけない。演習を行う場合には、システム部門とビジネス部門が別々にやるのではなく、「事業継続」というくくりで、有機的に互いり、一緒にシナリオを作り、合同で訓練・演習をして、どのタイミングでどの情報をどう共有・協議していくかなどを検証していくことが大切である。

●サイバー攻撃の予防と対応策

名古屋工業大学大学院教授 主席研究員
前田裕二氏

近年のサイバー攻撃は、巧妙化・高度化し、システマティックに実行される。攻撃の目的も、金銭目的、機密情報の窃盗などから国家による他の組織活動の妨害などにまで拡大。米大統領選で他国が介入したというレポートも出ている。IoTの世界では自動車や航空機、人工衛星なども攻撃対象となってきておりリスクは増大している。昨年は米国のサイバーセキュリティのカンファレンスで、人工衛星のハッキングが簡単にできるという報告があった。

情報セキュリティに関する2016年の動向では、組織が対象だと標的型攻撃が、個人ではインターネットバンキングやクレジットカードの不正利用といった金銭を狙った犯行が多いと報告されている。標的型攻撃では日本年金機構やJTB、富山大が被害にあった事例が有名である。攻撃者は事前調査をしっかり行った上で攻撃する。「やりとり型」といって、関係者を装って担当者と複数回メールのやりとりを行う。質問書と題して添付ファイルを送り、そこにマルウェアをしのばせる。このようなやり方でコンピューターをのっとり、個人情報を盗むのだ。人は、駄目だと言っても添付ファイルを開けてしまう傾向にあり、100%感染を防ぐのは難しい。自然災害とも通じるが、感染した後の被害の極小化や再発防止を考えねばならない。インシデント対応やログ解析をしっかり実施する必要があるほか、対応する組織をしっかり作るべきである。しかし、日本の中小企業ではサイバーセキュリティへの投資が全く拡大していない。サイバーセキュリティ保険についても、日本では複数社で提供しているが、米国では100社以上あり市場規模が大きい。

2016年2月、Operation Dust Stormというレポートが公表された。その中には重要インフラを狙うサイバー攻撃が2010年から行われ、日本もターゲットになっているという記述がある。対象は電力や石油、ガス、金融、交通、建設といった分野の関連民間企業だ。被害はよくわからないが、攻撃されているのは間違いない。2015年12月23日、少なくともウクライナの電力会社3社がサイバー攻撃を受けた。そのうちの1社では27変電所が停止し、103都市で全域停電、186都市が一部停電したと発表された。ほかの会社も30変電所が停止し、8万世帯が停電したと発表している。民間の調査報告だが、マルウェアのブラックエナジーの亜種が使われたことや、スピアフィッシングメール攻撃でネットワークに侵入したこと、さらにロシアのハッキンググループの関与などが記載された。さらに昨年1月はウクライナの空港の管制制御システムにもマルウェアによる攻撃があったが、すぐに検知されて大事には至らなかった。また、改めて電力会社に対するgcatバックドアを用いたスピアフィッシング攻撃が行われていることなどが報告されている。スイスでは国営軍需産業RUAG社でマルウェアが検知された。昨年1月に検知されたが、少なくとも2014年9月から侵害されていたようだ。また、防衛市民保護スポーツ省に対しても類似した攻撃が観測され、これにはロシアの関与が疑われている。スウェーデンでは2014年に航空管制システムに攻撃があり、システムダウンにより終日フライトがキャンセルされた。軍も2016年にウェブサーバがジャックされた。英国では鉄道ネットワークが過去1年間に少なくとも4回のサイバー攻撃を受けていたことも明らかになっている。

私はNTT持株会社のセキュアプラットフォーム研究所

に在籍している。ここには220名ほどが所属しセキュリティに関する研究を行っており、NTT東西、NTTコミュニケーションズ、NTTデータ、NTTドコモのサービス向上に役立っている。研究所は世界最先端の暗号技術を20～30年研究している。これとサイバー攻撃対策技術をコアにして、情報を危機対応に使えるようインテリジェンス化する研究も行っている。また、CSIRT(サイバー攻撃対応組織)を運営している。暗号技術には注力しており、例えば、絶対に盗聴できない電話をスノーデン事件をきっかけに作った。

サイバーセキュリティの世界は人材が少なく、育てようとしても教える人がおらず教育が追いつかない。このため、当社でも有望な人材のスカウトを積極的に進めている。秘密計算はデータを暗号化したまま複数のデータベースに分散して保存し、復号せずに暗号化したまま統計解析できる技術であり、特に注力している。1つのデータベースが盗まれても解読は不可能で安全だ。しかも世界最速の統計解析速度を誇る。今はゲノム解析に主に使われている。匿名化は2017年5月から個人情報保護法が改正され、扱いやすくなるため需要は増えるだろう。各種匿名化についてはコンテストも行われ、当社も優秀な成績を収めている。

サイバー攻撃については、アクセスしては駄目なサイトのアドレスを独自の技術でブラックリスト化している。市販のソフトからの情報だけでは足りず、情報を米国等の大学等とも提携して集めている。サイバー攻撃はメールやUSBなどあらゆるルートからやってくる。ログ分析、不正ログイン検知、DDoS、Slow DoS対策等も行っている。また、セキュリティオーケストレーションという技術も検討している。ログ情報を分析することで攻撃を検知し、オペレーションセンターからコントローラーに制御指示を自動的に出して最適なポイントで攻撃を遮断し、クリーニングセンターで制御する。

NTT CERTでは様々なサイバーセキュリティに関する対応をNTTグループ向けに行っている。このNTT-CERTは発足から12年目で、日本でも最も古い部類のCSIRTである。高度のセキュリティ診断や分析も行っている。

これまで説明してきたように、東京2020大会に向けて、重要インフラがサイバー攻撃のリスクにさらされている。現状では、当社でも自然災害は災害対策本部、情報システムはSOC・CSIRTと対応は縦割りになりがちだ。縦割りのまま、なんとか自然災害などの危機対応を行い、今に至っているのが多くの日本企業の姿だ。まだ日本はサイバー攻撃で人命が失われるほどの大きな被害を受けたことがないということもあろう。しかしこれからは現状のような、バラバラの対応ではだめで、組織・分野を統合した危機対応のマネジメントが必要だ。東京2020大会では政府を始めとして、多くの様々な組織がかかわる。サイバーからリアルな事象に至る複合的な危機が発生した場合、単一組織での解決は困難だ。リオオリンピックでは大きな問題は発生しなかったが、東京2020大会では万全の体制を構築しておく必要がある。

リスクマネジメントをする組織は基本的に一つで良いはずである。「総合リスクマネジメント」として、サイバーだけでなくリアル・フィジカルも含めた異なる組織・分野間における共通プロセスSOP(共通の運用手順)を作る。そこをどうICTでカバーするか。当社では「KADAN」という経営層、管理層に対して危機対応マネジメントを支援するツールの開発を進めている。これからは現場支援というより、経営層と管理層の危機対応に対する考えに変革を促すことに重きを置いてやっていきたい。