≪講演概要≫

図解で理解するサイバー脅威と『思い切って』変革すべき対策の考え方

はい。今紹介いただきました、名和と申します。

本日はタイトルのとおり、「図解で理解するサイバー脅威と『思い切って』変革すべき対策の考え方」についてお伝えします。

まず、紹介いただいた中で私の所属名がありましたが、本講演については、個人的な立場でお話をさせていただきます。

今日お伝えする内容は、図解で理解するサイバー脅威等でございます。この講演資料については、数年前から行政機関や民間企業等へのセキュリティレクチャーで使用している内容を今回アップデートしたものです。やや分量的には多いのですが、専門用語をなるべく少なくした形でお伝えします。しかし、ある程度の専門的な概念を含めないと最近のサイバー脅威を感覚として理解いただくことが困難になってきているところがありますので、今回の皆さんに対する情報提供、又は認識共有においては、専門的な概念をできるだけ「絵」にして、重要なポイントを絞ってお伝えしたいと思います。

最初のトピック１は、「図解で理解するサイバー脅威」です。

まず、スライド５をご覧ください。「マルウェア感染」は、以前は「コンピューターウイルス感染」という言い回しで説明されていたものです。これは数十年前から、悪意のあるウェブサイトの閲覧、それから、情報セキュリティー専門機関やメディアにより言及されることは少ないですが、研究機関等で未だに発生している「悪意のあるUSBデバイスの投入」というものがあります。いずれも、人間の心理的な隙を突いた攻撃です。したがって、これらのサイバー攻撃は、セキュリティー教育を適切に実施することによって、この発生確率を下げることが期待できるものとなります。

最近は、サイバー攻撃者による創意工夫や努力によって、私たちの人間の心理の隙を突いた攻撃「以外」のやり方が常態化します。これがアップデートサーバーを介したマルウェアの意図的混入です。これは現在、ウクライナにおいて発生しているサイバー事案で最も多い攻撃手法の一つとなっています。近い将来、日本周辺で有事が発生する場合、その数年前からの緊張の高まりの中において、日本国内で発生することが十分に想定されるものです。

このたった１枚のスライドから言えることは、もし、皆さんが近い将来の日本

周辺の有事を想定されていらっしゃるのであれば、今皆さんが手がけているセキュリティー対策では「自組織を守ることはできない」ということです。これを冷静に受け入れていただく必要があります。

これに対して「どうすればいいのか」という質問に対しては、この攻撃の仕組みを十分に理解した方が、その組織の実情に合わせた取組をしていただく必要があるとの答えになります。大前提として、アップデートを実施するときには、十分な検証を行うことが求められますが、組織において予算と理解が乏しい場合は、このリスクを受け入れて、早期検知と迅速対処に力を入れる方策が考えられます。

また、外部に委託している場合、どのように要請すればよいのか、そして要請だけでなく、どのように確認すべきなのかを取り決めておく必要があります。最近、他の自治体において、あまり良くない事象が発生しています。丸投げはもう全く駄目な状況だということを知らしめてくれているのかもしれません。

次のスライド６は、「正規サービスを時間差で踏み台にするC2通信」です。C2という言葉はテクニカル用語ですが、悪意のある通信と捉えてください。標的システムに感染したマルウェアを「子分」とすると、C2サーバに命令を与えるのが、その「親分」に相当します。

しかし、この親分と子分のやり取り、すなわちＣ２通信は、総務省やISPの努力により見つけることができるようになってきました。これに対して、攻撃者は改善を行いました。皆さんがよく見ているインスタグラムやYouTubeなどのSNSメッセージ、あるいは有名な方々のブログのコメント欄を介したやり取りです。悪意のある者たちが、SNSメッセージやコメント欄に人間では理解不能な特殊な文字列を書き込むことによって、それを読みにきた感染PCを操作（コントロール）します。このようなC2通信は、ISPによる努力で検知することは困難であり、高度なセキュリティソリューションを導入しない限り、自組織による検知や遮断も困難です。検知されない攻撃は、情報窃取の被害を甚大化させます。

スライド７です。従来のマルウェアという悪意のあるソフトウェアからシステムを守るために、私たちは現在、ウイルス対策ソフトを多く利用しています。

これは、交番に掲示されている指名手配書のようなものです。指名手配書がどんどん組み込まれることで、皆さんのシステムの中にある不都合な存在であるマルウェアを見つけることが期待されます。

しかし、最近の一部の攻撃は、このマルウェアを一切使いません。皆さんが恐らくお使いになっているだろうWindows10やWindows11には、ソフトウェアの部品に相当するものが多数内在しており、それらがスクリプトと言われる命令文により組み合わさって動作することで、以前のマルウェアよりかなり高度で堅牢（けんろう）な動きを実現させています。そのため、指名手配書をベースにした従来のウイルス対策ソフトでは、新しいタイプの攻撃を見つけることは極めて困難あるいは不可能になりつつあります。

そのため、比較的大きな規模の企業や団体において、このマルウェアが存在しない攻撃の発生が目立ってきています。この命令文は、感染したシステムに合わせて個別具体的に変容します。そのため、指名手配書が何万、何千あっても足りません。このような攻撃の仕組みを理解した組織は、積極的にセキュリティー投資を行っています。

一方、このような認識がされていない企業や団体は、「我々は予算がないからできない」と言います。この発言は「私たちは、このような脅威を想定していない」と言っているようなものです。そして、この攻撃を受けると、表向きに謝罪をしつつも、内実は無自覚なまま責任の所在を見つけることに翻弄します。このような態度や姿勢は住民サービスを提供する者としてはよくないと考えます。十分な予算がないなりに、できることはあるはずです。ただし、幾ばくかの予算を使って、人事制度を変えたり、あるいは外部の専門家と積極的に対話を重ねたりするという努力が必要かと思います。

スライド8です。正規サービスの同期を使うものですが、こちらは先ほどの正規サービスの踏み台利用とは大きく異なります。この攻撃は、よく利用されている無償のメールサービスやファイル共有サービスを悪用します。

皆さんの方で御経験あるかと思いますが、スマートフォンとPCで同じメールアカウントを設定し、スマートフォンでメールを送受信すると、次の瞬間、PCにおいて、その送受信した結果が反映されます。これをサーバーと端末間の「同

期」といいます。これにより、悪意のある者は、皆さんのPCにマルウェアではなく命令文を動作させ、Windows10やWindows11にあるソフトウェアの部品に相当するものを組み立てて動作させることができます。しかも、以前のマルウェアより柔軟に動作し、検知されにくいものとなります。現在、諸外国において、このような見つからない攻撃が深刻な影響を与えています。

スライド9は、さまざまな対象から調達や窃取した認証情報です。日本ではフィッシング詐欺による被害が跡を絶たない状況となっていますが、これに加えて、みなさんがよく利用されているブラウザーにおける拡張機能を通じて窃取されるケースが目立ってきています。この拡張機能とは、業務の効率性を高めるために利用されることが多いものです。例えば、外国人とやりとりや外国の情報を収集する、翻訳サービスを提供する拡張機能をブラウザーにインストールすることがあります。特に、役所において多い印象があります。

この拡張機能は、ブラウザーの開発及び提供している有名企業ではなく、全く異なる第三者が開発及び提供することが多いものです。しかし、それらの安全性や信頼性の仕組みは十分とは言えないものです。ブラウザーに表示されている情報やデータの全てが外部流出するという被害が諸外国で報告されています。

ただし、このような情報窃取のやり方は、非常に巧妙で念入りに準備されたものです。したがって、ネット上に広く公開された攻撃手法ではありません。攻撃者は、数カ月から数年かけて、多くの失敗を重ねながら、幅広の標的からブラウザーで表示された情報やデータを窃取します。その一つの現れとして、数年前、政府主導のキャッシュレス事業が始まった直後、国内の有名な事業者がアプリを配信しました。ところが、すぐに外国人によって、そのユーザーのアカウントが乗っ取られ、一部では、そのユーザーの銀行口座から不正に出金される事態が発生しました。

ここで皆さんに疑問に思っていただきたいことは、「なぜ攻撃者が事前にアプリユーザーの電話番号、メールアドレス、銀行口座等を知っていたのか」ということです。攻撃者は、私達の想定を超える長い期間に渡って、さまざまな手口で、日本の個人情報等を窃取し、悪用可能な状態にしていたということになります。その一つの手口に、ブラウザーの拡張機能があります。このような情報窃取

は、すぐに被害が顕在化するものではありません。そして、半年以上経過すると、多くの方がこのような懸念やリスクを忘却します。そして、しばらく経ってから実害が発生します。残念ながら、一つ一つの被害について因果関係を検証することは不可能です。しかし、状況証拠から攻撃者が、以前に窃取された個人情報等を悪用したことは明白です。住民の利益を守るためには、このような脅威の理解と状況認識を持続的に持つことが非常に重要となります。

ブラックマーケットでは、日本の人口の数倍以上の個人情報等が販売されています。詐欺や重複もありますので、正確な実数はわかりません。しかし、明らかに、悪用可能な個人情報等がかなり高値で売られています。

最近では、中国のある警察組織から10億人というデータが抜かれ、高値で販売されるという事態が発生しています。サンプルとして公開されている一部の情報は本物です。このような個人情報等の販売は、日常的なものとなっています。

そのため、標的のシステムに関する技術や知識を十分に持たない攻撃者は、ブラックマーケットから個人情報を購入すれば、すぐにアカウント乗っ取りという手段で侵入することができます。もう５～６年以上前から、このような深刻な状況になっています。

スライド10は、敵対国のソフトウェアです。これはもう一般報道でされているとおり、経済安全保障の領域として問題視されているものです。以前までの日本における大半の企業や団体は、インターネットに積極的に利用したサービスの提供を増やすことにより、組織の中に閉じた形でIT化による業務の効率化を多く手掛けてきました。しかし、最近中央省庁が強くリードする形で、生産性を向上させるためのIT化やDX化の推進が加速しています。悪意のある者らは、皆さんの執務室に盗聴器を仕掛ける、遠方から双眼鏡で窓を眺める、あるいは嘱託社員を装って皆さんの執務室で勤務するなどして、内部情報を取る努力をすることがありました。ところが、IT化やDX化がされていくことで、インターネット越しから内部に侵入可能な入り口が増えていきます。これにより、悪意のある者らが飛行機代や宿泊代を使うことなく、それぞれの国から私たちの組織の中にあるシステムに侵入して情報を窃取することができると期待します。そして、一部の組織で本当に成功させています。一般に、これをサイバースパイと言います

が、他の主要国では、これを見抜く能力を持つ情報機関が対応してします。しかし、日本には存在しません。したがって、不正に取られていることが明確であるのにも関わらず、日本は自らの力で見つけることができない。そして何かあった場合、すぐに甚大な被害が発生する状況になってしまっています。このような状況を、私たちは理解する必要があると思います。

スライド11は、機械設備です。近年、SNSの台頭により、顧客のニーズの変化は常に流動的です。テレビも業界全体で視聴率低下やCMスポンサー離れが深刻になっていると言われており、その影響で番組自体が視聴者の購買意欲を高めることに偏重したものが増加しています。そのため、テレビを小一時間見ただけで、「欲しくなる」、「食べたくなる」、「行くたくなる」という衝動が次々に発生します。このようなSNSやテレビの影響によって、常に変動する顧客の消費行動に応えることができる生産や流通を整備する必要が出てきました。それも、迅速かつ低コストで実現させなければなりません。ところが、旧来の電話ファクスや文書等による対応では消費行動の変化に追いつくことができず、専用システムの開発では高コストになるため、ビジネス機会の損失になります。そのため、多くの場合、工場におけるインターネットの利用とデジタル化により、本社が工場の生産状況をリアルタイムで把握し、即時指示を出せる仕組みを整備するようになってきました。

これにより、最近の計測制御ネットワーク、すなわち工場の内部設備は、私たちが想像している以上にインターネットと直接つながっているところがあり、時間の経過とともに、その数が増えています。しかし、この仕組みの全てが、ITの詳しい方により整備されているわけではありません。利益をあげている事業部門たる工場の電気技術者等が自身の知識と経験で整備することがあります。これにより、工場の電気技術者等にとって想定外のセキュテリィ上の不備が発生してしまい、外部からの侵入がされやすくなります。

スライド12は、偽Wi-Fiのアクセスポイントです。皆さんは今、私の講演をPCの前で座って聞かれているかと思います。日本の伝統的なものかもしれませんが、役職者の方は窓の近くに座っている方が多いのではないかと思います。もし窓の近くで、PCやスマートフォン等のデバイスが組織内のWi-Fiアクセス

ポイントに接続されているようであれば、十分に警戒していただきたいと思います。それは、窓の外で悪意のある者が皆さんの執務室の中にあるWi-Fiルーターと同じものを作って、それで皆さんのPCやスマートフォン等のデバイスを、窓の外のWi-Fiルーターに接続させようとします。皆さんのデバイスとWi-Fiルーターが、このような脅威を想定した設定になっているのであればよいのですが、そうでなければ、一部のデバイスが窓の外の不正なWi-Fiルーターにつながってしまうことがあります。実際、日本国内で、このような被害が発生しています。日本にとって重要な知的財産や個人情報を有する企業や団体が明確な標的になっています。

スライド13は、悪意のあるDNSサーバです。これは若干小難しいテクノロジーの話です。私たちのウェブアクセスは例えばYahoo!のサイトを見るためには、ユーザーがyahoo.co.jpという文字列を打ち込むか、検索エンジンが出力した、その文字列のサイトを選択します。しかし、インターネットの世界では人間が識別可能な文字列を理解することはできません。DNSというサーバに問い合わせてIPアドレスを取得します。このIPアドレスは、インターネット上の住所に相当するものです。ところが、このDNSサーバは、皆さんが独自に運営されているようなものではありません。ISPから提供されたり、あるいは全く違うところを指定されたりしているはずです。そのため、誤って悪意のあるDNSサーバを指定してしまった場合、Yahoo!のサイトを見ていると思いきや、実は悪意のあるサイトにアクセスしてしまうことがあります。これは、非常に広い範囲で一斉に仕掛けることができる攻撃手法であるため、以前から、他国で幾多も発生しています。

最後のスライド14は、ソフトウェアによる不正挙動です。いわゆるサプライチェーンの問題です。最近、少ない予算で高い能力を持ったソフトウェアの開発を求める組織や団体が多くなっています。この背景には、厳しい財政状況の中で、中央省庁からの指針等によるIT化・デジタル化・DX化を推進しなければならない状況が見え隠れしています。請負側のベンダーにとっては、彼らのビジネスモデルからすると、利益を生みにくい要求事項であるため、ゼロから開発することはせず、安価で安定性のある出来合いのものを組み合わせて作り上げる手

法をとります。特に、サードパーティーと言われる第三者により開発され広く利用されているものを積極的に利用することで、バグが少なく高機能なシステムに仕立てることができます。このようなサードパーティーのソフトウェアの中には、信頼性が確認されていない個人が改廃したものが含まれています。一般に個人の開発環境への侵害は、組織より容易です。そのため、入念な準備を行う攻撃者は、侵害可能なサードパーティーの個人の開発環境を狙い、乗っ取りを成功させた上で、アップデート等のタイミングで、そのサードパーティーを利用する組織や団体への侵害を試みます。海外において、このような攻撃の発生が増加傾向にありますが、日本については、日本が誇るベンダーの力がまだ残っている影響か、海外のような増加傾向の様子は伺えません。しかし、日本のITベンダーのビジネスモデルは崩壊しつつあると言われてから10年以上経っています。最近は、開発や運用維持する能力が低下の一途を辿り、諸外国と同様なビジネスモデルに変容しています。そのため、攻撃者にとっては、日本以外の国々で成熟度を上げてソフトウェア・サプライチェーン攻撃を日本の組織に対して仕掛けやすくなってきていると見るべきです。

次のトピック2は「受け入れなければならない現実」です。

サイバー脅威に関する状況認識の獲得が、主要国の中で最も難しいのは日本です。

スライド16における、氷山の一角に位置する「公表あり・報告あり」は、全ての組織が認知できます。新聞報道でされているものです。正確な統計データはありませんが、私の活動で得られている感覚的な割合は１％以下です。その次は、コミュニティ限りで流通する「公表なし・報告あり」で、数%程度です。一方、一番下に示している「公表なし・報告なし・決定なし・認知なし」は、サイバー事案が進行中なものですが、海外のセキュリティソリューションによって検知までされなくとも統計的な分析から得られた結果から侵害されている可能性が見積もられたものや、海外で発見されたC2サーバの分析により、C2通信が発生させている日本の組織がマルウェア感染していることを全く認知していないものなどです。これが非常に多い状況です。

特に、日本の組織はITシステムの運用保守を外部に委託する傾向が強いため、固定化された予算と人的リソースの中で発生するサイバー攻撃は非常に厄介なものです。この対処に係る予算や人的リソースは、あらかじめ確保されていないことが多く、組織内の手続きにおいて困難となるシーンが数多く発生します。

スライド17は、日本はいまだにベンダーに丸投げによる弊害を示したものです。この丸投げは、サイバーセキュリティーも含まれることがあります。組織内でサイバーセキュリティーの責任を持つ幹部や担当者を指定したとしても、それ以外の方々は、「リソースがない」、「難しい」、「実感ない」などのような発言で、サイバーセキュリティーを他人事のように捉えがちです。サイバーセキュリティーの責任を持つ幹部や担当者は、従来の正攻法を踏襲しようとします。その結果、「どこまで対応すべきか分からない」、「マニュアル・手順書が欲しい」などと、受け身の姿勢をとります。この主な要因は、サイバー脅威に関する状況認識が悲劇的に不足していることで、想像力を得られず、本来持つべき危機感が希薄になっていることがあげられます。そのため、事前の備えができずに、サイバー攻撃が発生した場合、他の主要国では数日から数週間程度で完結するところを、日本は数ヶ月以上もかかることがあります。サイバー攻撃による実害が、「レビューテーション（評判）の低下」や「数十万円程度の損失」程度であったとしても、原因究明のための調査・復旧・改善するために多額の費用がかかります。日本のように、調査・復旧・改善に非常に長い時間をかけてしまうと、機会損失や他の施策や事業にも遅延やリソース不足の等の2次的被害が追加的に発生することになります。

このようなことを理解せずに、未だに「備え」としての事前に対応準備をしようとしません。これにより、サイバー攻撃を受けた日本の組織が、被害をいたずらに拡大している現実があります。

スライド18は、「方向性の異なる準備姿勢」を示したものです。

日本は「体制」、つまり政治的支配の様式を取ることを好むようです。誰が何をするかの責任と役割をきめておく必要があるため、「文書」を作成することとなります。私が支援している複数の公的機関の一部では、セキュリティー対策に係る文書は、各部門に分散かつ階層的になっているものを含め、数千ページに及

んでいます。ところが、大規模なサイバー攻撃が発生すると、関与あるいは連携しなければならない部門や組織が多岐にわたるため、そのような文書が要求する杓子定規的な行動を取ることは難しいばかりか、そのような行動は被害軽減や原因究明の妨げになることさえあります。その大きな要因は、サイバー脅威の変化とそれに対応するための最適な行動が文書に適切に反映されていないためです。国内の組織によくみられるサイバーセキュリティーに関する規定の多くは10年以上前の脅威をベースにしています。

どんなに、文書の内容が素晴らしくても、常に進展するサイバー脅威に適合したものにしなければ、役に立ちません。他の主要国でも20年以上前までは、学術的な観点で記述されたような文書が多く作成されていましたが、進展するサイバー攻撃への対処は、「文書」ではなく「能力」が必要であることが理解されていくと、前もっての身構えの態勢の強化にシフトしていきました。

スライド19で示したように、日本は、諸外国に比べて非常にユニークな傾向として、いまだに「情報保証」に偏重したセキュリティー対策が取られています。これは、「情報漏えい」への対策としては最適ですが、攻撃プロセスの後半で発揮されるものとなります。攻撃プロセスの前半に対する取り組みとして弱いものとなります。先程説明したように、日本の組織はIT運用を外部委託する傾向が強いため、攻撃プロセスの前半は、委託先が主体的に対応することになります。これを、委託先に依存して良いものなのかを見直す必要があります。発生したサイバー攻撃の被害抑制と原因究明を委託先の努力に依存するという姿勢は、責任ある行動とは言い難いです。

次のスライド20は、今までお伝えした重要事項にもなりますが、「状況認識の不足による想像力の欠如」です。朝から晩までサイバー脅威に対するモニタリング・分析、そして、現場に赴いている数としては一般のユーザーよりは多いのが専門家と言われるものですが、そうかと言って専門家が全部分かっているとは限りませんし、その発言がいつも正しいわけではありません。

ただし、さまざまな現場対応の経験から申し上げると、目の前に落とし穴があるのに、多くの日本の組織、企業、公共団体はそこを見ようとしません。目先のことばかりに注目しすぎているのか、もしかしたら単に視力が悪いのかもしれま

せん。そのため、落とし穴に落っこちてしまいます。

できれば、右のほうで示しているように、「的確な状況認識」が必要です。現場の方が十分に理解していても、上層部や委託元からの理解が得られなければ、組織としての認識は得られません。つまり、組織として落とし穴を見つけることができなくなります。

スライド21は、「ほぼ全てにおいて意思決定プロセスが遅い」ことを示したものです。表面的には階層化された権限、上意下達、ガバナンスがありますが、実際には非公式なやりとりが多すぎます。横並び意識、同調圧力、そして、忖度（そんたく）、根回しです。上場企業の経営層の中には、他の同業他社は、何かを行っているか教えてほしい、調べてほしいなどと要望される役員がいらっしゃいます。これは、典型的な横並び意識であり、かなり間違った状況認識の獲得姿勢です。自組織の状況を認識するには、自組織の現場を見る必要があります。旧態依然の硬直化した組織でキャリアを積んだことによる弊害かもしれません。このような幹部は、一刻も早く経営幹部から追い出さないと、近い将来に組織に甚大なる被害を発生させる可能性があります。

最後のトピック3として、「思い切って変革すべき対策の考え方」を皆さんと共有させていただきます。

まず、スライド23の「サイバーレジリエンス」です。昨年（2021年）9月28日に閣議決定された「サイバーセキュリティー戦略」に、「サイバー攻撃を食い止めることは困難である」、「被害を軽減させるべき」と読み取れるメッセージがいくつも並んでいます。

そして、さまざまな施策が並んでいますが、最初に位置づけられているのは、「経営層の意識改革」です。他の主要国における戦略の内容のほとんどが運用的措置になっていることと比べると、日本は、この時代になって、ようやく組織のトップ層の意識が課題であったことを認め、進展するサイバー脅威に対して、遅々として進まないセキュリティー対策に対する危機感が強く現れています。

しかし、他の国々が導入しているものとそう変わらないテクノロジーを私たちが利用することによって、低予算かつ短期間で、高機能なサービスやプロダクト

を獲得できるようになりました。このようなものに依存すればするほど、サイバー攻撃が発生しやすくなり、その被害の規模も大きくなります。これが、経営層、あるいは皆さんのような意思決定層が適切に認識してこなかったことで、組織構造な問題から、必要なセキュリティー対策が困難になる状況が増えてきました。これにより、重要インフラサービスに影響が及ぶ懸念が高まってきたため、国家として看過できない状況になったのです。

この中で、もっとも強調されているのが、「サイバーレジリエンス」です。自然災害に備えたレジリエンスは、「倒れてくる壁」で例えると、倒れた1枚の壁を元に戻す努力に似ています。壊れたインフラを復旧することで、住民生活の日常を元に戻すことにつなげることができます。

しかし、サイバー攻撃は人間の強い悪意のある意思によってもたらされます。そして、彼らは持続的に攻撃をしようとします。そのため、「倒れている壁」は何重にもなりますので、目の前にある壁だけを元に戻しただけでは、またすぐに倒れようとします。したがって、私たちがやるべきことは、この壁が倒れるメカニズムをよく理解することです。倒れてくる壁の後ろに何枚の他の壁が倒れてくるのかを知ることです。これを知ることによって、実施すべき対処を立案し、適切な関係者に解決に直結する要請をすることができます。

スライド24の「高いレジリエンスの態勢」は、日本が世界に誇る素晴らしい防災対策です。しかし、これに至るまでには多くの犠牲を払ってきました。「積極的監視」や「予兆情報」に基づく対処については、気象庁が涙ぐましい努力を行っています。これは、防災に係る法律の整備にも現れています。

スライド25の「低いレジリエンスの態勢」は、自然災害に対する取組の希薄が国に見られるものです。震災が起こると、「事態進行」及び「事態対処・管理」に長い時間がかかり、多くの命が失われます。

スライド26の「実現すべきサイバーレジリエンス態勢」のイメージをご覧ください。

サイバーインシデントは必ず発生します。理由は、IT化・デジタル化・DX化によって、サイバー攻撃を受ける可能性のある領域が一気に増大するためです。私達は、それらを確実に認識して対処するに足りる知識や能力を持っていないば

かりか、それを行うための意識すら持ち得ていません。

しかも、今後、私たちが経験するサイバー攻撃は、すでに他国において成熟してしまったものとなりますので、一部でなす術がないという状況に陥る可能性もあります。

サイバー脅威に適合したセキュリティー投資は、この「事態進行」の時間を短くし、「原因特定・早期復旧」を迅速にします。一部の日本の組織に見られるように原因究明に数カ月以上かけて関係各所におわびを繰り返すのか、一週間程度で全ての混乱を収束させることができるのかのどちらかを選択すべきかは、火を見るより明らかです。

このための努力とコストを「事態発生」の前のほうに持ってくるだけです。「予兆管理・警戒」と「早期検知・調査・抑制」に対する、セキュリティー投資をすることを強くお勧めします。これを行うことができるのは、現場のシステムエンジニア、システム管理部門、あるいはベンダーではありません。組織全体で、強いリーダーシップを取る必要があるため、意思決定層が行うことが求められます。

最後のスライド27に、「組織を守るための努力方法」を紹介します。

今の日本の組織にとって馴染みのないアクションアイテムが示されていますが、1つ目として、今の従来の情報セキュリティーの概念、体制では自分たちの「組織は守れない」ことを受け入れていただく必要があります。

2つ目に、「サイバーレジリエンスの成熟度の向上」です。日本の防災対策は、これまで相当な犠牲を払いながら、レジリエンスを高めていきました。私たちがサイバーレジリエンスを高めていくためには、相応の犠牲を払っていく必要があると言えます。皆さんの組織が犠牲となるのか、あるいは他者の犠牲から学ぶのかのどちらかとなります。さまざまなサイバー攻撃の事例を積極的に収集して、自らの意識を高めていくことによって、組織や住民に提供すべきサービスを守るための予算を作り出すことが重要となります。加えて、人の育成もしながら、段階的にサイバーレジリエンスの成熟度を向上させていく必要があります。

3つ目は、全ての組織構成員、職員等に対する「意識向上トレーニング」です。例外はありません。職員も他組織からの常駐や嘱託の方も全員同じです。そ

して、お忙しい首長、あるいは幹部の方も含まれます。誰一人としてセキュリティー上の穴を作らない。この強い意志を持ってこそ、初めて意識向上トレーニングの存在意義があります。ちなみに、職員等に不審なメールを開かせないようにする標的型メール攻撃訓練は、意識向上には不向きなものとなります。

４つ目は、「セキュリティー監査」です。どんなに頑張ってもセキュリティー上の穴が発生します。そのための取組には過剰あるいは過少なものが少なくありません。特に、問題なのは過剰な取組です。直近のサイバー脅威に適合しないセキュリティポリシーを放置してしまうと、すでに十分な効果が期待できない取組を積極的に行い、劇的な効果が期待できる取組を後回しにするという不合理な状況が散見されています。一方、やるべきことをほとんどやっていない「過小」な取組も目立っています。セキュリティー監査は、このような不合理な状況を改善して、セキュリティー投資を適正化するための取り組みてす。責任者や担当者を評価するものではありません。

最後は、最大のパフォーマンスを発揮するための「自動化の推進」です。IT化・デジタル化・DX化のために、さまざまな自動化ツールを利用することになります。同時に、セキュリティーにおいても自動化のツールの利用をする必要があります。採用や育成が困難なセキュリティー人材の能力の一部をマシーンに転化するようなイメージです。

私の話は以上です。ありがとうございました。