KPMG

KPMG Insight

KPMG Newsletter

Vol.29

March 2018

【特集①】

ハイパーコネクティビティの時代に求められる、企業のサイバーリスク対応とは

kpmg.com/jp

対談

ハイパーコネクティビティの時代に求められる、企業のサイバーリスク対応とは

貴島　直也氏

きしま　なおや

EMC ジャパン株式会社
執行役員
RSAゼネラルマネージャー

2001年、EMCジャパンに入社。一貫して金融機関、グローバル企業を担当し、安定したストレージ基盤の提案と手厚いフォローをモットーに営業活動を展開。2014年に現職であるRSA事業本部　本部長に就任。標的型サイバー攻撃の被害が深刻化するなか、セキュリティ対策を経営課題として実践していくための啓蒙、提案活動を行っているほか、RSAが推進するBusiness-Driven Securityによるセキュリティアプローチを広める活動に尽力している。

情報システム部のみがかかわっていた、「情報セキュリティ」の時代、サイバー攻撃はサーバールームで起こっていた。しかし、企業活動の全フィールドがデジタル化した今、サイバーリスクは、企業の実際の現場作業など、フィジカルな部分にも拡大している。

これは、決して対岸の火事ではない。経営陣が積極的に関与していかなくては、円滑な企業活動を守ることができなくなってきているのである。

今回は、サイバーセキュリティの最前線で活躍する、EMCジャパンRSAゼネラルマネージャーの貴島直也氏に、ハイパーコネクティビティの時代に求められるサイバーリスクへの対応について、KPMGコンサルティング パートナーの田口篤が話を伺った。

コネクティビティの向上で加速するサイバーリスク

田口：最近、工場のセキュリティに関するご相談がすごく増えていると聞いています。おそらく、工場のシステムがすべてデジタル化され、ネットワークに接続されたことでサイバー攻撃を受けるような環境になったからですよね。生産停止やラインの誤作動など、単なる情報漏洩よりも大きな経営ダメージを受ける可能性が高くなってきています。

サイバー攻撃は、デジタルな事象だけに留まらず、フィジカルなダメージまで発生するようなリスクに変質してきたように思えるのですが、貴島さん、いかがでしょうか？

貴島：確かにそうです。ターゲットもですが、攻撃手法も変わってきています。2017年5月に、世界中の20万台以上のコンピュータがWannaCryというワーム型ランサムウェアに感染するという大規模なサイバー攻撃がありました。

これは、コンピュータ内の情報を暗号化し、金銭を要求するというものです。このような攻撃ができるということは、つまりは工場を人質にとってお金を要求することもできるということです。工場は製造系の企業にとって一番大事なエンジンですから、そこを止められたら被害は甚大ですよね。

工場や発電所、プラントなどもそうですが、今はいろいろなものがデジタル化されて、ネットワークでつながっています。IoT化され、コネクティビティが上がっている現代社会です。つながっているのですから、攻撃可能性が増えるのは当たり前のことです。

田口：製造業に限らず、サービス業やインフラに係る企業まで多くの企業がWannaCryに感染し、世界中でこれまでにない規模の被害がでました。

貴島：2年ほど前にも、ウクライナで年末に大停電が起こったことがあるのですが、それもサイバー攻撃だと言われています。まさにフィジカルなダメージまでもたらすように、サイバーリスクは変質してきました。

田口：工場の一番のミッションは、生産ラインを止めないことです。一方、セキュリティ対策は、最初に機能がデザインされているもの、あるいはすでに組み込まれているものに対して後から付加していきます。工場の方から見ると、それが原因で止まったり、故障したりしないかという懸念があります。

工場を止めないでずっと稼働させることと、止める可能性があるセキュリティ対策を入れていくということにはコンフリクトが起こることもあるのではないかと思いますが、この点はどうでしょうか？

貴島：おっしゃる通りです。私もIT業界に20年くらいおりますが、やはり、安定した仕組みがあると、「せっかく安定しているのだからこれ以上触りたくない」と思われる方が多いですね。

一般的に、工場への投資は10年単位など非常に長いスパンで行われます。機械も、それを管理するシステムも工場建設に付随して導入されるわけですが、一度投資すると、システムのバージョンアップはなかなかなされません。

一方、情報システムへの投資はだいたい3年から5年でされることが多いです。常に脆弱性が発見され、アップデートされる。そのようなセキュリティの世界から見ると、たとえ安定している工場システムであっても、アップデートしていかなくてはならないことは明白です。

大事なことは、脆弱性の管理をしっかりすること。そのうえで、その脆弱性がどういう影響を与え得るかということを把握し、随時正しいアップデートをしていくことです。

田口：でも、通常、工場にはサイバーの専門家はいませんよね。そうなると、随時アップデートしていくのも難しいのではないでしょうか。IoTにした後が心配になるというか……

田口　篤
たぐち　あつし
KPMG コンサルティング株式会社
パートナー
KPMG ジャパン
サイバーセキュリティアドバイザリー
リーダー
セキュリティ管理態勢の構築、個人情報保護、インシデント対応計画の策定等、ITのリスクアドバイザリー業務を中心に従事。

貴島：まさに、そこが大事なところです。日本特有なのか、私も判断がつきませんが、工場の投資というのは工場ごとにされているケースが多い。また、管理者も工場関係者であることが多いのです。

これは、必ずしも情報システム部門の人間やセキュリティの技術者が管理しているわけではないということです。ですので、今後は工場のシステムもできるだけ情報システム部門やセキュリティの技術者と一緒に管理していくべきだと思っています。

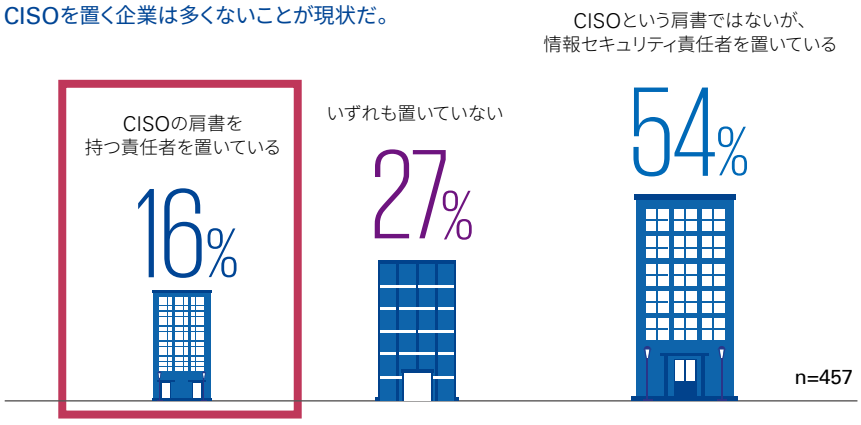
「サイバーリスクを理解していない」ことが、経営層の課題

田口：これまでサイバーリスクとは無縁と思われていた工場ですら、いつ攻撃を受けるかわからないのは怖いことですね。

今でも日本の企業の経営層の方々の多くが、サイバーリスクは自分とは縁遠いものと捉えています。どういう攻撃があり、どのような被害が出ているのか。また、脅威

CISO設置状況

CISOを置く企業は多くないことが現状だ。



出典：KPMGセキュリティサーベイ2017

に備えるにはどうしたらいいのかなど、サイバーリスクの前提知識が圧倒的に不足しているように見えるのですが、これは何が原因だと思われますか？

貴島：「サイバー」という言葉だけで難しそうと思われているからでしょう。経営層の方々から見ると、ITやサイバーはデジタルで、よくわからない世界なのです。

ところが、今の世の中、ビジネスの現場はどんどんデジタル化しています。我々は「デジタルトランスフォーメーション」と呼んでいるのですが、ビジネスがデジタル化していく以上、残念ながら、経営層の方々も知らない、わからないでは済まなくなっています。

田口：確かに、「サイバー」という言葉はわかりにくいのかもしれません。企業の資産としての重要な情報は、わずか20〜30年前までは紙の書類が原本として保管され、施錠管理や入退管理で物理的に守っていました。

同じように、サイバーの世界でも、暗号化やアクセス制御で大事な情報を守っています。こう考えれば、サイバーの世界のセキュリティも、物理の世界のセキュリティも似たようなところがありますよね。

貴島：物理の世界では、セキュリティはある程度できあがっていますから、イメージしやすいかと思います。ですから私たちは、高度なサイバー攻撃なども、できるだけシンプルに物理の世界に例えた形で説明するようにしています。

セキュリティ業界の人間としては、経営層の方々にできる限りサイバーリスクを理解してほしいと思っています。サイバーリスクを理解していないこと、このことは、経営層の課題の1つではないでしょうか。

田口：経営層の方々がどうしても理解できない、あるいは企業がそこまで管理できないときにはどうしたらいいのでしょうか？

貴島：望ましいのは、社内にセキュリティを専門とする部門なり、役職を置くことです。今、海外では、チーフ・インフォメーション・オフィサー（最高情報責任者：以下「CIO」という）と同じような権限を持つチーフ・インフォメーション・セキュリティ・オフィサー（最高情報セキュリティ責任者：以下「CISO」という）やチーフ・リスク・オフィサー（最高リスク管理責任者：以下「CRO」という）を置く会社が増えています。リスクを総合的に管理し、経営層にアドバイスをするという役職です。

経営層の方々は、CISOまたはCROを配置して、自社にどのような情報資産があるのかを評価・防御することを考えていくべきです。ただし、残念ながら、セキュリティの技術者というのは、どこの企業でも不足しています。これは政府もそうです。日本全体で十数万人欠けていると言われています。

サイバーリスク対応に、企業はどの程度投資すべきか？

田口：経営層の方々から見るとサイバーリスク対応は投資ではなくて、コスト的な色合いが強くなります。そうなると、どこまで費用をかけるべきか、悩まれると思うのです。そのあたりの適切性について、どう考えたらいいのでしょうか？

貴島：すごくお答えしにくい質問ですね。一般的なことで言えば、従来のセキュリティコストとは、防御壁を作るための費用でした。例えば、入口でゲートを作り、IDカードを配付してリスクが発生する可能性のある人や物を入れないようにするためのものです。

これからは、それにモニタリングのコストが加わります。そして、このモニタリングコストはどんどん上がっていきます。その中には、さきほどお話したCROやCISOの人件費や外部のコンサル費用なども入りますし、サイバー攻撃を受ければ、第三者調査のための費用も入ります。

どこまで投資するかですが、どこの視点で見ていくかで考えるとわかりやすくなるでしょう。例えば、100億円の商品を生産する工場が1日止まったらどれだけの売上機会を失うか、というのは予想できますよね。それをベースに、ではどのくらいの投資だったら可能かというのを経営判断していただくとよいのではないでしょうか。

田口：精緻な数値ではないかもしれないけれども、ダメージ算定をすることでセキュリティのおおまかな費用を計算できるということですね。

ビジネスとセキュリティを可視化する“ビジネス・ドリブン・セキュリティ”

田口：先ほどCROまたはCISOを置いて権限を渡すというお話をお伺いしましたが、権限を渡したら、経営層は何をすべきなのでしょうか？

貴島：権限を渡さないといけないのは当然ですが、現実にはそうできないケースもあります。今は、このことが経営層にとってジレンマとなっているように見えます。

田口：具体的にはどういうことでしょうか？

貴島：権限を渡せるのは、エンジニアと経営とがつながっている企業です。そうでない企業では、まず、社内にしっかりとしたアドバイザーをすぐに選定すべきです。これがステップ1ですね。

その次に経営層がすべきことは、サイバーセキュリティリスクにさらされる資産を把握し、その対策に関わる関係者とのコミュニケーションを密に持っておくことです。これがステップ2です。

今の日本はアウトソーシングが流行っており、餅は餅屋で、サイバーリスクも外部のスペシャリストにお願いすれば安全だと思っている経営層の方々もいます。

もちろん、外部のスペシャリストはセキュリティに特化した技術力を持っています。しかし、企業の持っている情報資産にどれほどの価値があるのかは、外部の人間にはわかりません。情報資産の価値は、それを持つ企業が判断しなければならないのです。

田口：権限のある適切なアドバイザーを置く、情報資産の算定をするというのはいずれも判断が難しいところだと思いますが、不可欠なステップですよね。

貴島：はい。外注ですべての問題を完結できると考えている企業には、ステップ1に戻ってもらう必要があります。その後で、自社でどこまでできるのか、判断する人間は社内に置くかなどを決めます。さらに、外注するのであれば、どこまでを社内でやり、どこから先を社外でやるかということをしっかりと定義していかなくてはいけません。

要するに、セキュリティの運用主体もフレームワークとして構築する必要があるということです。そうしたことも、経営層の方々はきちんと考えないといけないのです。

田口：私は、経営者の役割は2つあると思っています。1つはリソースの確保。さきほどのお話に出てきたCROやCISOといった適切な人材、そして適切な費用の確保です。

もう1つは、1ヵ月でサイバーアタックを何回受けているか、怪しいメールが何件届いているかなどといった、サイバーリスクの状況がどうなっているかについてのモニタリングです。

でも、そういった状況を把握できている経営層の方は少ない。これは問題だと思っています。その原因の1つには、仕組みが圧倒的に不足していることがあります。ですから、次はサイバーリスクの状況の見える化をやるべきだと思っているのですが、いかがでしょうか？

貴島：そうですね。機会としては、例えば経営会議で毎回サイバーリスクのことを議題にしていくといいのかもしれません。

情報システム部門が運用している実績データをグラフや表で見える化して、それの経年変化を報告してもらえば、サイバーリスクへの理解も深まることでしょう。リソースが確保できた後は、それがきちんと機能しているか、うちの会社が本当は今どれほどの危機的状況にあるのかということを、見える化する手立てを作っていくことです。

我々は、今、「ビジネス・ドリブン・セキュリティ」という考え方を提唱しています。これは、ビジネスの大事なものとセキュリティとをつないで可視化するという仕組みです。

物理の世界で言えば、人が入ってきました、受付しました、名前を書きました、そしてゲートを通っていきます。その際、持って入る物はX線撮影します。出るときも、何も持ち出されていないことを確認するためにX線を通します。というように、すべての行動を見えるようにするのが可視化です。

セキュリティの世界でも同じです。どのような通信をしてデータが入ってきて、どのようなデータが流れたのか、流れたデータは持ち出してもよかったのか否か、それを判断するための可視化ツールです。大事なのは、しっかりとルールを守っているか、運用されているのかを確実に管理できるようにすることです。

田口：ビジネス・ドリブン・セキュリティっ

て、すごくいい言葉ですね。私は、セキュリティの技術者は経営のことがわからないために、経営層が何を心配しているかが見えていないのではないかと思っています。

でも、ビジネス・ドリブン・セキュリティという共通言語があれば、セキュリティの技術者と経営層がお互いに理解し合えそうな気がします。

貴島：まさにその通りです。どうしてもセキュリティの技術者は、細部にこだわる傾向があります。例えば先ほどのWannaCryならば、WannaCryがどういうふうに機能するか、どういうふうに攻撃してくるかなどは細かく報告してきますが、それがビジネスにどのような影響を与えるかは触れません。それはわからないからです。

ビジネス・ドリブン・セキュリティは、そこを可視化します。どういう情報を止められたら、あるいはシステム障害が起きたらビジネスに支障をきたすのか、どれだけの売上損害を与えるのか。そういったことを最初に定義しておけば、経営層の方々もセキュリティ部門の担当者もサイバー攻撃を受けたときの自社ビジネスへの影響が理解できるようになるのではないかと思います。

今、GDPRに取り組んでいる企業は多いですよね。GDPRはEU（欧州連合）の個人情報保護法ですが、グローバル企業ならば、GDPRに限らず、ビジネスを展開する国・地域のルールは守らないといけません。

ただ、法律やルールは国・地域ごとにまったく違います。ですから、その国・地域のルールを可視化して管理する必要があります。しかも、残念ながら一回守ればいいというわけでもありません。それは、国・地域によって、また時代によって、法律が変わるからです。

そのため、随時リアルタイムで、アクティブに管理する必要があります。そのためにも、今後はビジネス・ドリブン・セキュリティのような仕組みで、可視化を推し進めるツールが必要になってくると思っています。

サイバーリスク対応は、全拠点を一律均質かつ一斉に防御する

田口：物理の世界にいると、日本の本社が大事だからと、そこにばかり重点的に防御したくなります。でも、インターネットの世界はフラットで、攻撃者はボーダーレスですから、日本本社のセキュリティだけを高めても意味がありません。

彼らは、本社のセキュリティが強固なら、最も弱い場所を見つけて、そこから侵入してきます。それは、もしかしたらアフリカの小さな支所かもしれません。

ですから、サイバーリスクは日本の本社だけではなく、グローバルな拠点を一律均質に、しかも一斉に防御しなくてはならない。このことを、日本の企業の経営層の方々はあまり気にしていないように見えるのですが、これはどうしてだと思いますか？

貴島：世界で起こっているサイバー攻撃というのは非常にたくさんあります。日本にもサイバー攻撃はありますが、世界規模からみると圧倒的に少ない。だから、危機感がないのでしょうね。

しかし、だからといって、サイバー攻撃の手法や、世界でどのようなサイバー攻撃が行われているかを知らなくていいわけではありません。世界がつながっているということは、つまりどこにいようと攻撃者が攻撃してくるということ。ですから、この世界で起こっていることを知ることは、大きな強みになると思います。

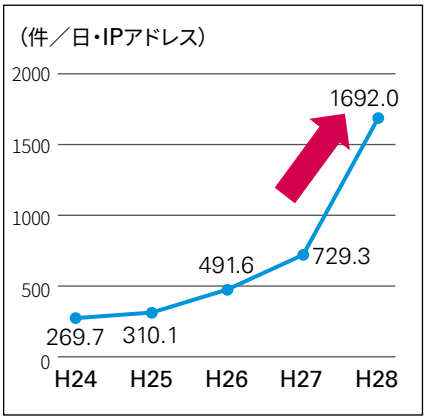
田口：おっしゃる通りです。日本企業であっても、海外売上のほうが圧倒的に多い会社はたくさんあります。グローバル化している以上、経営管理課題の1つであるサイバーリスクにも、グローバルでどうやって対応をしていくかが重要となりますよね。

そうなると、海外拠点に対して、日本の本社がいかにしてサイバー分野でガバナンスをきかせていくか、マネジメントをしていくか。これは、グローバル企業の経営層がこれから考えなければいけないテーマといえそうです。

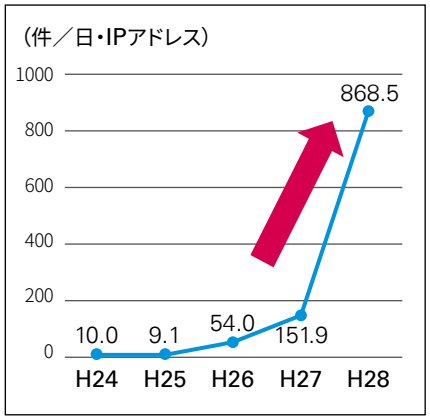
日本のサイバー脅威動向（外部攻撃）

日本のサイバー攻撃数は年々増加しているものの、今後は、世界で起こっているサイバー攻撃にも目を向け、対応策をマネジメントすることが重要だ。

サイバー攻撃センサーでの検知数



遠隔制御（Telnet）の試行数



出典：「平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）より KPMG 作成

本稿に関するご質問等は、以下に記載のメールアドレスにご連絡くださいますようお願いいたします。

KPMG ジャパン
marketing@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp