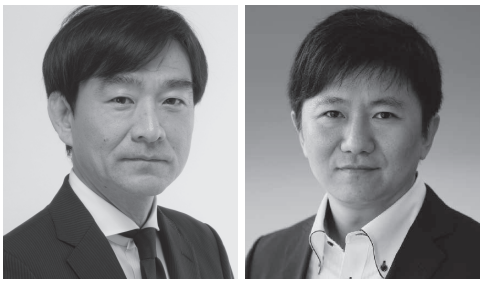
コロナ後の新常態において、サイバー攻撃から自社をいかに守るか



クロール・インターナショナル・インク
日本支社代表・マネージング・ディレクター　片山　浩樹
シニアヴァイスプレジデント・サイバーリスク
ジャパンヘッド　アレックス・シム

1．はじめに

新型コロナウィルスの収束がみえないなか、サイバー攻撃による脅威は、世界的に増加の一途を辿っている。

本稿では、サイバー攻撃による最近の被害事例を振り返ったうえで、貴社が今とるべきサイバーセキュリティ対策のあり方について、紹介したいと思う。

2．サイバー攻撃とは何か？

サイバー攻撃とは、標的のコンピュータやネットワークに侵入してデータの搾取や破壊を実施したり、標的のシステムを機能不全にしたりすることにより、事業などさまざまな活動を困難ならしめることである。

このサイバーとは、「人間と情報機器が交じり合ってネットワーク化した状態やシステム」と定義することができる。

現代の企業は、さまざまな情報機器によって構成され、人がそれらを使用し、ときにはひとつの情報機器がそれ以外の情報機器を操作・コントロールしながら、企業活動は成り立っている。さらには、企業は、そのサプライチェーン（仕入れ先や得意先との関係）においても、情報機器と人間とが交じり合いながら、ネットワークを形成している。

その意味において、サイバーは、システムや技術といった事業要素の一部ではなく企業自体を指しており、サイバー攻撃からサイバーをいかに防御するかというサイバーセキュリティは、企業経営そのものということができる。サイバーセキュリティは、事業の継続に直結する経営課題そのものなのである。

3．最近のサイバー攻撃の傾向

従来からの標的型攻撃による機密情報窃取、ランサムウェア攻撃、こなれた日本語や日本の商慣習を利用したばらまき型メール（ビジネスメール詐欺による金銭被害など）に加え、最近では、サプライチェーンの弱点や第三者を悪用した攻撃が増加傾向にある。防御が甘い取引先の中小企業などを経由してフィッシングメールを送り付け、ウイルスに感染させる事案が増えている。また、在宅勤務によるVPNの脆弱性を突いたサイバー攻撃によって、情報漏洩を引き起こす事案も増加傾向にある（図表１）。

4．サイバー攻撃から自社をいかに守るか

（1）何を守るか

・守るべき対象の優先順位付け

攻撃側と防御側は日々イタチごっこを続けているが、攻撃側のほうが防御側に比べ、圧倒的な情報量をもっていることを考えれば、サイバーセキュリティを検討する際、企業は、サイバー攻撃に対して100％の防御を図ることは不可能であるということを前提に取り組むべきであろう。そして、そのうえで大切なのが「守るべき対象を優先順位付ける」という考え方である。

前述したように、サイバーセキュリティは企業経営そのものである。そう考えた場合、まずは事業の継続性を担保するために必要かつ重要な資産・プロセスに

図表１　最近のサイバーセキュリティに関する脅威ランキング

1	標的型攻撃による機密情報の窃取
2	内部不正による情報漏えい
3	ビジネスメール詐欺による金銭被害
4	サプライチェーンの弱点を悪用した攻撃
5	ランサムウェアによる被害

出典：情報処理推進機構（IPA）「情報セキュリティ10大脅威2020」

絞り込んで、防御策を検討すべきである。

そのとき、「自社の競争優位性や今後のマーケットを考えた場合、自社の経営リスクとしては何があげられるのか」というビジネスの視点から検討するアプローチが有効である。

たとえば、「新しい技術に関する特許情報が盗まれた場合、投資回収への影響は幾らか」、「サプライチェーンの断絶による生産遅れによる影響はどの程度か」といった視点から、経営に大きな影響を与えるリスクシナリオをまずは洗い出すことをお勧めしたい。そのうえで、最優先に守るべきは何かを考え（情報資産を守るべきか、知的財産を守るべきか、生産管理システムはどうかなど）優先順位をつける手順が好ましいと考える。いきなり個別資産ごと（端末、サーバーなど）の優先順位付けの検討から入ってしまうと、特定の資産は守れても「人間と情報機器が交じり合ってネットワーク化した状態やシステム（＝企業）」を守ることにつながらないケースがあるからである。

（2）どう守るか

・早期の検知・対応・復旧

不正リスクなど他のリスクにも当てはまることだが、サイバー攻撃に対しても、企業による早期の検知・対応・復旧という組織行動が欠かせない。そして、この組織行動のなかでも、特に重要なのが、組織による日ごろの訓練と評価・フィードバックである。よくある訓練としてあげられるのが、社員向けのセキュリティ研修や演習である。弊社のような外部専門家が講師を務めるケースもあれば、企業のセキュリティ部署が務める場合もある。また演習の場合、疑似的な攻撃や脅威を発生させて、一般社員が身をもって攻撃への対応を体験するものもある。疑似的な偽メールを社員に送って偽メールの見極め方を身につけるものである。また組織横断的な訓練もある。インシデントが発生した場合、セキュリティ部署が中心となって、組織（各部門）がどう動き、連携するかについて確認するものである。この場合、各部門の動き方や連携の仕方をルール化したマニュアル（サイバー危機管理マニュアル）を事前に制定しておく必要があることはいうまでもない。

また、評価としては、ペネトレーション（侵入）テストといわれる、抜き打ち的なセキュリティレベルの評価が有効である。テストの実行者が攻撃者になったつもりで自社のシステムや社員に攻撃を仕かけることにより、防御側の視点では見落としていた脆弱性や対応の不備を明らかにしようとするテストである。このペネトレーションテストは、セキュリティ部署やCSIRT[注1]が中心となって実施する場合と、われわれのような外部専門家に委託して実施する場合がある。後者の場合、前者と異なり、企業は、これぐらいのテストをやったら大丈夫だろうという先入観を排除でき、どの程度までテストをやればよいのかという疑問から解放されるため、より現実的なテストを受けることができる。また自社のセキュリティレベルが他社に比べてどの程度のレベルにあるのか、客観的に測ることができるのも、外部専門家を起用するメリットといえる。

・多重的防御

企業の防護すべき対象をサイバー攻撃からどう守るかを考えるうえで重要なのが「多重的防御」という考え方である。これは、守りたいものに対して、攻撃が仕かけられてから盗み出されるまでの過程に、複数の関門を設けることである。たとえば、サイバーセキュリティと物理的セキュリティを一体化させることにより防御力を高めることなどがそうである。サーバールームへの入退室の際のセキュリティーカードと生体認証による二重認証、ログ取得による入退室管理、監視カメラの設置、サーバーラックの施錠管理、LANケーブルの色分け（基幹系は赤、情報系は青など）、オフィスをセキュリティゾーンとオープンエリアにエリア化して入退室者を区分する、などの取り組みが有効である。

・マネジメントによる定期的なレビュー

特に日本企業のマネジメントは、実際に起こっている問題の広がりと自社がさらされている脅威とを関連付けられず、自社の喫緊の経営課題としてとらえていないケースが多く見受けられる。

実際、取締役会の監督プロセスの有効性についてアンケートしたところ、サイバー攻撃に高い懸念を抱いているが、サイバーセキュリティへの取り組み率は低いことがわかる（図表２）。

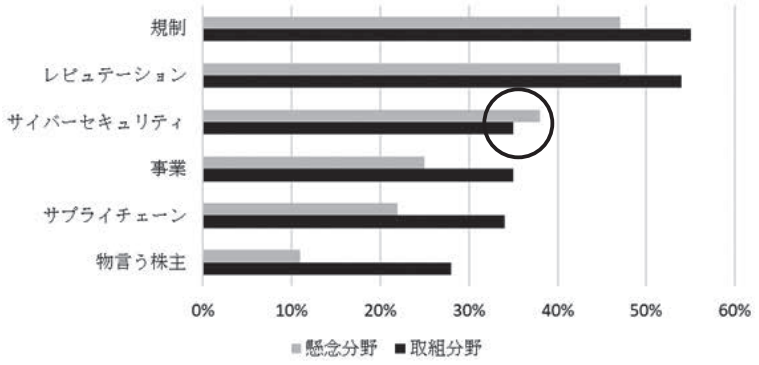
これを是正するためには、常時、取締役会でサイバーセキュリティを議題に載せ、定期的にレビューを実施し、ときには外部専門家を招聘し、経営陣に説明会を実施するなど、常にマネジメント全体として認識を共有する必要がある。

前述した優先順位付け、早期の検知、対応、復旧の各プロセスを現場や担当役員に任せきりにするのではなく、経営を大きく左右する最優先アジェンダとして取り組む必要がある。しかし、実際、こうしたプロアクティブな取り組みをしている企業は、まだ少ない。

では、どのような議題を取締役会に載せればよいの

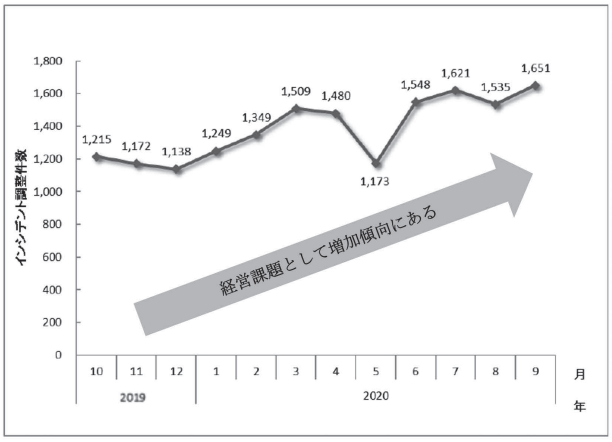
か。そのヒントとして、企業の取締役をメンバーとした非営利団体が公表している「サイバー・リスク・オーバーサイト[注2]」が参考になる（図表３）。

図表２　マネジメントはサイバー攻撃の脅威を重視していない



出典：Diamond Harvard Business Review June 2018

図表３　インシデント調整件数[注3]の推移



出典：JPCERT/CCインシデント報告対応レポート（2020-10-15号）

・情報共有体制の見直し

日本の組織では、情報の流れが下から上への報告というかたちで運用されるケースが非常に多い。しかしこのようなやり方では、もはやインシデントとして取り扱う必要がない雑多なものまで報告されたり、一方、標的型攻撃によって機密情報が知らないうちに何カ月も社外に流出していたといった高度な事案が報告されなかったり、というような事態が起こりうる。

そのような事態を避けるためにも、社内ネットワークのような情報共有の場を社内に設けることが重要である。CSIRTなどセキュリティの専門チームが主体となって、社内での問い合わせ内容を整理・分析・共有化できるプラットフォームを準備すること、社員の啓発活動に取り組むことが有効である。

また、情報を共有するうえで重要なことは、情報を共有することが目的になってはいけない、という点である。自社にとって必要な情報は何か、他社や業界団体との情報共有から自社は何を求めたいのか、また自社は、最新の脅威情報など環境を認識するための情報を求めているのか、それともサイバーセキュリティの意思決定やアクションにつながる情報を求めているのか、をあらかじめ明確にしておくことが重要である。

・情報ネットワークへの積極的な参加

サイバーセキュリティにはさまざまな要素が複雑に絡み合う。ネットワーク、通信機器、端末機器、基本ソフト、各種アプリケーションといった技術要素から、海外犯罪への対策、個人情報の保護からグループ企業も含めた内部統制まで、経営者が気を配らなければならない要素は実に広範に及ぶ。そのため、サイバー攻撃を防御するための情報収集を一企業だけで行うにはどうしても限界がある。サイバー攻撃に対抗するには、企業の垣根を超えたネットワークによって情報を共有することも重要である[注4]。

5．結語

サイバーセキュリティは、とりわけ技術的な問題と考えられがちだが、そうではなく、企業活動そのもの、企業経営そのものである、という理解にまずは立つ必要がある。そして、企業活動、企業経営である以上、新しい価値の創造という視点から考えなければならない。そのためにも、経営者による強いリーダーシップのもと、サイバーリスクに正面から立ち向かう姿勢が求められる。また、サプラインチェーンの弱点を悪用した攻撃も増えていることから、自社だけではなく、取引先のサイバー防衛策も確認し、取引関係のある複数社で連携して対応を進めることも重要である。

注１　CSIRT：Computer Security Incident Response Teamの略。インシデント対応を担当する企業内の専門部署。

注２　企業のボードメンバーによって設立された非営利団体であるNACD（National Association of Corporate Directors, 全米取締役協会）が公表。
https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

注３　「インシデント調整件数」とは、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応をJPCERT/CCが依頼した件数を示す。

注４　JPCRET/CC（Japan Computer Emergency Response Team Coordination Centerの略）が公表する情報は対策を講じるうえで参考にされたい。