新年特別対談

2022 New Year Talk〈第2弾〉

巧妙化するサイバー攻撃から企業をいかに守るか ～セキュリティ対策とデータガバナンスの強化

新年特別対談の第2弾は当法人のアシュアランスイノベーション本部 イノベーション戦略部部長である加藤信彦とEYストラテジー・アンド・コンサルティング(株)でエンタープライズリスクを担当する川勝健司、当法人Forensics事業部でプリンシパルを務める杉山一郎が、増加するサイバー攻撃の現状と企業が取るべき対策についてお伝えします。

モデレーター：
EY新日本有限責任監査法人
アシュアランスイノベーション本部
公認会計士
加藤信彦

▸ Nobuhiko Kato

製造業や小売業の会計監査に従事した後、現在は金融機関に対する監査業務に従事しながら、デジタル&イノベーションリーダーとして監査業務変革をリード。主な著書（共著）に『Q&A コーポレートガバナンス・コードとスチュワードシップ・コード』（第一法規）がある。公認会計士、米ニューハンプシャー州公認会計士。当法人アシュアランスイノベーション本部イノベーション戦略部およびAIラボ部長。

EYストラテジー・アンド・
コンサルティング株式会社
エンタープライズリスク
川勝健司

▸ Kenji Kawakatsu

ITガバナンス領域において約20年のコンサルティング経験を有する。デジタルガバナンスユニットのリーダーとして、IT・デジタルガバナンス構築、データガバナンス態勢構築／評価、DX人材育成、アジャイル開発プロセスへの移行の支援のほか、サイバーセキュリティ等のコンサルティング案件に、プロジェクト責任者として関与。データベーススペシャリスト、公認情報システム監査人（CISA）。

EY新日本有限責任監査法人
Forensic & Integrity Services
杉山一郎

▸ Ichiro Sugiyama

EY Japan Forensicsにてサイバーインシデント対応やeDiscovery対応などを主な取り扱い分野とするフォレンジック・テクノロジーの責任者を務める。デジタルフォレンジックの分野において15年以上の業務経験を持ち、特にサイバーインシデント対応の領域において法執行機関を中心に数多くの組織に対して講義を行うなど多岐にわたる活動を行っている。GIAC Certified Forensic Analyst（GCFA）。

Nobuhiko Kato × Kenji Kawakatsu × Ichiro Sugiyama

I　増加するサイバー攻撃 その手口は巧妙化している

加藤　現代は「予測不能の時代」といわれています。また、ビジネスの世界ではデジタル技術の飛躍的な進展によって大きな変革期を迎えています。こうした変化の激しい時代にあって、新しいリスクに備えるために何をすべきか。DX時代のガバナンスには数々の課題がありますが、特にリモートワークが進展した2021年は、同時にサイバー攻撃の被害も増加した印象があります。今回は2名の専門家を交えて、主にサイバー攻撃への対策とデータガバナンスを両輪で進める重要性についてお話を伺いたいと思います。

杉山さん、最近のサイバー攻撃の傾向はどのようなものでしょうか。

杉山　私たちEY Globalが毎年実施している「グローバル・インフォメーション・セキュリティ・サーベイ」（GISS）の2021年度版によると、確かに多くの企業が「サイバー攻撃の増加」を感じており、特にランサムウェアによる破壊的な攻撃に対して全回答者の3／4が大きな脅威と受け止めています。一方で、多くの企業では危機対応やリスク軽減に対して「自信がない」と回答している実情があります。サイバー攻撃には私たちが関わる会計監査にも多大な影響が出る事案も発生しています。またリモートワーク下でインターネットから直接アクセスできる社内システムを狙う攻撃や在宅勤務者を狙ったフィッシング詐欺なども増えてきました。

加藤　それらのサイバーインシデントは企業経営に大きな被害や影響を与えますね。

杉山　その通りです。会計監査の視点で見ると、無形資産の破壊や不正送金による直接的な毀損だけでなく、データ侵害による多額の罰金や訴訟リスク増大も大きな問題です。プライバシー関連の規制違反や契約違反など多様なリスクをはらんでおり、組織として保険の補償範囲と賠償費用を考慮した予測と対策を立てる必要があります。

川勝　データガバナンスの観点から考えますと、まずDX化の進展によりデータ量が増大していることに注目したいと思います。現状、少なからぬ企業で自社の膨大なデータを管理できていないケースが見受けられます。そのため組織横断的にデータを活用する場合も、データの統合や更新のタイミングの齟齬から効果的に利活用できないケースがしばしば見られます。社内システムのどこに、どのようなデータが存在しているかを把握しきれていないことが大きな要因となっているため、データの利活用どころか、セキュリティ面でも危険な状態にさらされ続けることになります。

杉山　インターネットから直接アクセス可能なVPNやクラウドサービス、特にVPNが起点となっているサイバー攻撃が目立っています。日本ではシステムを運用に合わせて構築していく企業が少なくはなく、その結果として社内システムの脆弱性が後手に回っていることがあります。そうした脆弱性管理の隙を突かれて盗まれたID、パスワードなどの認証情報は、いわゆるダークマーケット等で売買され、攻撃に悪用されています。

加藤　お二人のお話を伺い、サイバー攻撃は事業展開

や事業継続にとどまらず、財務報告の観点でのリスクでもあるということをあらためて感じています。企業内の膨大なデータが管理されない状態で散らばって、それを外部から狙う侵入者がいる。そうした状況において、攻撃は具体的にどのように起きるものでしょうか。

杉山　特に被害件数が多いのはランサムウェアです。かつては暗号化による業務妨害が主でしたが、現在はそれに加えて企業の重要データを不特定多数の人々に晒すという脅迫が行われています。“身代金”として金銭（多くの場合は暗号資産）を要求されるわけですが、支払いを拒否した場合にはその情報を使って別の組織を脅すなど、二重三重の攻撃の手を繰り出してきます。

加藤　ダークマーケットでは、データがお金になるという認識が定着しているわけですね。

杉山　はい。データの盗取にとどまらず「企業活動の継続」を人質に取ることによって、莫大な“身代金”が手に入ることが周知されています。こうしたサイバー犯罪の手口の巧妙化が、企業へのサイバー攻撃の大きな背景になっているといえるでしょう。

Ⅱ　データガバナンスの第一歩は データの「重要性」を見極めること

加藤　リモートワークなど、オフィスに固定されない働き方は、ウィズコロナ／アフターコロナにおいても定着していくものと思われますが、DX化の伸展により企業が保有するデータは今後ますます増大していくことが考えられます。この不可逆的な時代の流れの中で、どうやってサイバー攻撃から身を守ればいいのでしょうか。

杉山　まずデータセキュリティの「基本」に立ち返ることだと思います。今一度、自社はどのようなデータを保有していて、どのようなリスクがあり、何を守らなければいけないのか。そもそも自社にとって重要なデータとは何なのかなど、サイバーセキュリティの視点で全て見直してください。また、データそのものだけでなく、サイバー攻撃時の事業停止や信用失墜を防ぐためにどのような対策をすべきなのかなど、今一度、データの把握や管理状況について調査や評価をやり直すことが何よりも重要でしょう。

加藤　データガバナンスがより一層重要になるということですね。川勝さんはどのようにお考えですか。

川勝　データの重要性に基づいて、管理体制や方策を検討していくというのは杉山さんのおっしゃるとおりです。私はそれを推進するにあたって重要なポイントが3点あると思っています。まず1点目は「管理体制」。経営者がデータ保護・セキュリティを経営課題として考え、しかるべき管理戦略が明確になる体制をトップダウンで整備していかなければなりません。2点目は「プロセス」。データには取得・作成、利用、配備などのライフサイクルがあり、各データのライフサイクルに合わせた保護策を検討することが重要です。それらの管理を人間の力だけでまかなうのは現実的に難しいため、3点目としてITの力を借りる、すなわち「テクノロジー」の活用を挙げたいと思います。例えば、データの来歴を管理するためのデータリネージュソリューション。または、一元管理のためのデータウェアハウス（DWH）やデータレイクソリューションのメタデータの自動付与機能など。これらを活用すれば膨大な企業データの「見える化」を図ることができます。

Ⅲ　安全な場所は存在しないという 「ゼロトラスト」の発想で対処する

加藤　川勝さんのお話を伺いながら、データの管理についても、お金の管理と同様に内部統制を構築していかなければならないということを痛感しました。一方で、事前対策を行っていてもサイバー攻撃を受けてしまうことはあります。そうした場合はどのように対応すべきでしょうか。

杉山　リモートワークが一般化した今、社内システムにアクセスするユーザーが必ずしも社内にいるとは限らず、加えて情報資産はクラウドを含むさまざまな場所に点在しています。つまり社内外の「境界」がなくなっている状況といえます。このような現状を踏まえて、近年、社内ネットワーク上に安全な場所など存在しないという前提で、全てのアクセスを確認するという発想「ゼロトラスト」の考え方が普及しています。この観点に立ち、例えば従業員のアクセスを1件ごとに精査するなどの対策が必要になってくるでしょう。

川勝　サイバー攻撃対策には当然コストがかかりますから、対策を実施するにあたっては、まずどのデータを重点的に防御するかを検討しなくてはなりません。そのためにデータ固有の性質、ステークホルダーの関心、法規制による要請など、多様な要素を基に判断する必要があります。さらに、仮に情報が漏えいしてしまった場合の社会的影響や被害額なども想定して判断しなければならないため、それは「経営判断」となるわけです。

加藤　先ほど挙げられた三つのポイントにもつながるお話ですね。ただ、そこまで対策を講じても弱い部分を突かれて攻撃されてしまう可能性もあるのではないかと思います。万が一、攻撃を受けた後の事業継続についてお話を伺いたいと思います。

杉山　多くの企業では基幹システムなどの重要システムについては、データのバックアップを取っています。しかしバックアップデータがあったとしても、例えばランサムウェアによる暗号化からの復旧に手間取ってしまうとビジネスへのダメージが大きくなりま

す。そのため、事前に復旧訓練を行うなどの備えが欠かせません。また、事業継続にあたっては取引先など「ステークホルダーへの通知・承認」「事実確認」などを速やかに行うことが求められます。さらに、データ漏えい等に伴う訴訟などにおいて正確な情報開示をしていくことも留意すべき点であると思います。

川勝　データバックアップの目的は、自然災害からの復旧、システム障害からの復旧、マルウェア被害からの復旧などさまざまです。いずれにしても投資対効果という観点で、無差別にバックアップを取るのではなく、ビジネスに与える影響を分析して対象となるデータや頻度、世代などを決めていくことが大切です。昨今ではオンプレミスのシステムだけでなく、クラウド環境についても考える必要があります。その場合、クラウドベンダーのService Level Agreement（SLA）に依拠しなければならないこともしばしば見受けられます。また、バックアップに留まらず、データの越境・移転問題も含めて検討することが重要です。

杉山　データの越境・移転問題に関して付け加えると、サーバが海外にあるケースでは、データ移転ができないためにインシデント対応ができないという場合もあります。また、バックアップについても付け加えると、基幹システムさえバックアップしていれば安心かといえばそうではありません。サブシステム側が復旧できないために、一部の業務で通常と異なる例外的な対応が発生すれば、業務全体としては継続が困難になります。こういう実際の対応を通じて発覚する問題もセキュリティの面で重要なポイントの一つだと思っています。

Ⅳ　平時のコストだけではなく有事のコストも試算することが重要

加藤　重要なデータがどこに保存されているかを認識し、バックアップの範囲や復旧手段をあらかじめ考慮し、準備をしておくことが大切ですね。では最後に、DX化を進める企業に向けて、それぞれサイバーセキュリティとデータガバナンスの専門家として伝えておきたいメッセージをお願いします。

杉山　サイバー攻撃者の存在とリスクを常に意識することが大切です。保有データの評価やセキュリティ対策の見直しを行うことは、データ侵害に伴う訴訟や調査などの有事対応のコストを大幅に削減することにつながりますので、ぜひ対策を講じていただきたいと思います。

川勝　データガバナンスの立場からも、データリスクへの対応は、まず「影響分析」に尽きると考えます。仮に重要データの流出や改ざんなどが発生した場合、データの性質によって致命的なダメージを受けることがあります。データの重要性を把握するためには、被害に遭った場合を想定した被害総額を算出するのは適切な試みです。その際、直接的な被害だけでなく、レピュテーションリスクを含めることをお勧めします。以上を踏まえると、データ管理はシステム部門だけの問題ではなく、経営課題として捉える問題であることがお分かりかと思います。今回は主に「守り」に関する話をしましたが、データ利活用といった「攻め」の

側面を武器にすることが重要な経営判断につながる時代です。「攻め」の姿勢を強化するためにも「データガバナンス」の構築が企業によって必要不可欠になってくるということです。

加藤　なるほど。被害額をあらかじめ試算するというのはとても重要なことですね。

川勝　EY Japanは企業がデータガバナンスをどの程度推進しているかをリサーチした「データガバナンスサーベイ」を発表しています。その2021年度版を見ると、多くの企業がデータガバナンスに関する取り組みとしては道半ばであるという結果でしたが、その重要性については認識されている印象を受けました。私たちEY Japanでもデータガバナンスを診断・評価するサービスを実施しているので、ぜひご利用いただければと思います。

加藤　予測不能であり、変革が激しい時代において、EY新日本も監査法人として、企業の立場に立ってサイバーセキュリティとデータガバナンスの課題を考えていきたいと思います。お二方には貴重なご意見を伺うことができ、本日はありがとうございました。