データ保護の強化に、いかに対処するか

著者：ジョー・ノセラ
監訳：米本 和希

欧州を中心に、個人データ保護に向けた動きが加速している。2018年5月にEU一般データ保護規則（GDPR）が施行され、企業が個人データの侵害を認識してから、原則72時間以内に監督機関へ通知する義務が発生するなど、個人データ保護にかかる企業への要求は年々高まっている。しかしながら、複雑化するデジタル社会において、新たなサイバーリスクの把握と管理に悪戦苦闘している企業も少なくない。本稿では、重要性が増すデータセキュリティについて企業がどのように対応すればよいか、サイバー攻撃に耐え得る危機対応力の構築に向けて考慮すべきポイントについて紹介する。（米本 和希）

消費者は自分の個人情報の扱いについて誰を信じればよいか分からないと感じている。PwCの最新の調査であるConsumer Intelligence Series: Protect.meによれば、自分の個人情報を企業が責任を持って扱ってくれると思うと回答したのはわずか25%で、政府による個人情報の保護について信頼できると答えたのはわずか17%だった。同時に69%の消費者は、企業はハッキングやサイバー攻撃に脆弱であると感じており、85%は情報セキュリティへの取り組み方に不安な点がある企業とは取引をしないと答えている。消費者がこれらを行動に移すかどうかは別としても、本調査結果は消費者が企業や政府のサイバーセキュリティ対策に抱く信頼感が低いという現状を浮き彫りにしている。

しかし、米国の消費者2,000人を調査したProtect.meでは、行動を起こせる企業にとってはチャンスとなる、前向きないくつかの情報も得られた。回答者の72%は、政府よりも企業の方がデータ保護の体制が整っていると感じており、81%は政府よりも企業に自身の個人情報の保護を行ってもらいたいと思っている。もちろん政府による規制は役立っている（回答者の82%が、企業によるデータ利用は政府が規制すべきだと答えている）。既に金融サービス業界とヘルスケア業界では政府による規制が行われており、それらの業界に関しては消費者の信頼が高いことがPwCの調査でも分かっている。しかし、データセキュリティについていえば、消費者は企業に高い期待を抱いていること、そしてその期待に添える企業は自社の利益を保護しながら信頼を築けることは明らかである。

多くの企業にとってこの目標への道のりは長い。122カ国9,500人のエグゼクティブの考えを調査したPwCのグローバル情報セキュリティ調査2018（GSISS）では、回答者の44%が包括的な情報セキュリティ戦略を策定していないと回答している。さらに多くの回答者（48%）が従業員に対するセキュリティ意識啓発のトレーニングプログラムを用意していないと回答しており、54%がインシデントレスポンスにかかわるプロセスが未策定と回答している。消費者から求められる今、企業は以下の手順を踏みサイバー攻撃に耐え得る危機対応力を構築する必要がある。

1. 取締役会を含む経営幹部メンバーを巻き込む。GSISSでは、自社の取締役会がセキュリティ戦略に積極的に参加しているという回答はわずか44%にすぎなかった。これは一部の企業がサイバーセキュリティを単にITの問題ととらえているからだと考えられる。しかし取締役会がサイバーセキュリティ戦略に関与すると、経営幹部はサイバーセキュリティ戦略を優先課

ジョー・ノセラ

PwCのプリンシパルで、シカゴを拠点とする。金融サービス業界向けのサイバーセキュリティおよびプライバシーサービス業務におけるリーダーを務める。

米本 和希（よねもと・かずき）
kazuki.yonemoto@pwc.com

PwCコンサルティング、Strategy&のシニアアソシエイト。電子機器メーカー、自動車メーカー、IT関連企業などに対し、事業戦略の立案および実行支援などのプロジェクトに数多く従事している。

題ととらえる傾向が高まることをこれまでの事例が示唆している。取締役会が関与すると、サイバーリスクはIT部門の単なる日常的な懸念事項からその企業の全社的な戦略計画の一部へと格上げされ、大規模なセキュリティ侵害にかかわるリスクと同程度の重要度が付与される。

情報セキュリティ戦略と予算のレビューに経営幹部を関与させると、サイバーセキュリティの優先度をさらに高められるだろう。これにより、特定のシステムやデータに障害が発生した場合に何が危険にさらされるのかが明確に把握でき、また最も緊急のリスクを軽減するための確実な計画を整えることもできる。企業が最高情報セキュリティ責任者（CISO）の権限をITの枠を超えて引き上げ始めていることがGSISSで明らかになったのは良い傾向だ。回答によればCISOがCIOの直属ではなく、CEO（40%）または取締役会（27%）の直属であることが一般的になってきている。

2. ネットワークの相互依存性を評価する。企業は自社のネットワークが依存するさまざまなネットワークを注意深く見ていく必要がある。これには会社の機密データが短期・長期で収容される可能性のある公共の送電網から第三者ネットワークやクラウドベースのネットワークまで含まれる。脆弱性は企業が所有するネットワークから何層か隔てたところに存在する。しかし停電になるまで自分がいかに電気に依存していたかに気が付かないように、ネットワークの相互依存性にも大惨事が起きてからでないと気が付かないことが多い。

例えば、サイバー攻撃が発生した際に、多くの企業は犯人を明確に特定できないという。GSISSでも攻撃元を特定する能力に強い自信を持っていると回答したのはわずか39%にすぎない。このギャップを埋めるために、企業幹部はサイバー攻撃を想定したシナリオで相互依存に対するストレステストを行う必要がある。また企業は、例えばIoTなどネットワーク上にあるシステムを悪用しようとする新しい技術について調査することも重要である。しかし、自社にビジネスエコシステム全体のIoTのリスクを評価する計画があると答えたGSISS回答者は比較的少数だった。IoTのセキュリティにおける責任の所在は企業によってさまざまで、29%がCISO、20%がエンジニアリングスタッフ、17%がCRO（最高リスク管理責任者）であるとしている。

3. データ操作とデータ破壊に注目する。サイバー攻撃が高度化するのに合わせて、企業のサイバーセキュリティの優先課題も常に適応させていかなければならない。企業はかつてデータの盗難を最も恐れていた。しかし、最近はハッカーが企業のITシステムやITアーキテクチャを、企業および社会全体に対してどのように悪用し得るかを企業幹部は知っておかなければならない。サイバー攻撃をする人たちの主な目的にはクレジットカード番号を盗むといった金銭目的だけではなく、データ操作によりその企業や個人に害を与えることも含まれるかもしれない。例えばもし犯人が病院のカルテにアクセスしデータ操作をしたり、航空管制システムを書き換えたりした場合、多大な被害が生じるだけでなく、人命が危ぶまれる事態にまで発展する可能性がある。

ハッカーは、いかにしてITシステムやITアーキテクチャを企業および社会全体に向けて悪用し得るか。企業幹部は知っておかなければならない。

組織はサイバーセキュリティ評価に際し、インサイドアウトのアプローチを取る必要がある。すなわち、自社において脆弱性がある領域を探し、攻撃を受ければ人の命や安全にかかわるシステムを優先して防護していく必要がある。そしてシナリオ・プランニングを行い「考えられないことを考える」と同時に、シミュレーションを行い自社がそれらの攻撃に耐え得る準備が

できているかを確認するべきである。また万一セキュリティ侵害が発生した際にはすぐに対応できるよう態勢を整えておかなければならない。金融分野のシェルタード・ハーバー（守られた港）イニシアチブ[1]では、他分野でのこうした新たなデータ破壊リスクへの対応に役立つモデルを提供できる可能性がある。この取り組みでは、銀行が大規模なサイバー攻撃を受けた際に口座データを復元・復旧するために役立つ標準が策定されている。

サイバー脅威は常に変化している。これら三つのステップに沿って対策を始めた企業は、進化するサイバー脅威をより深く理解できるようになると同時に、企業幹部が自らサイバー脅威に対する危機対応力の向上に最優先で取り組むような環境を醸成することができる。この危機対応力は大規模なサイバー攻撃により引き起こされる金銭的、風評的、法的大損害から企業を守ることができる。消費者はそこに注目している。

"How Companies Can Respond to Consumers' Demands for Better Data Protection" by Joe Nocera, strategy+business, December 19, 2017

1：米国の金融業界は、2017年にこの取り組みを開始。金融機関がハッキングやDDos攻撃を受けた際、他行が代理で顧客向け業務を継続できるようデータをそれぞれバックアップする