企画・制作＝日本経済新聞社クロスメディア営業局

広　告

NIKKEI BUSINESS INNOVATION FORUM

サイバーセキュリティ経営の実践

［主催］日本経済新聞社クロスメディア営業局
［協賛］KPMGコンサルティング、ラック
［後援］経済産業省

今や企業のサイバーセキュリティ対策は、喫緊の経営課題だ。先日、150カ国以上にわたり、ランサムウエア「WannaCry」によるサイバー攻撃が行われた。イギリスの病院では手術が延期になるなど、人命に関わる被害も出ている。また、鉄道などの重要インフラにおけるサイバー攻撃は、重大な混乱を引き起こす。経済産業省は2015年に「サイバーセキュリティ経営ガイドライン」を公表。経営者のリーダーシップの下でのサイバーセキュリティ対策を推進している。ビッグデータやAIなど、テクノロジーが進展するなか、企業はどのようなサイバーセキュリティ対策を講じるべきか。当該分野の有識者を招いた「サイバーセキュリティ経営の実践」が5月24日に開催された。

パネルディスカッション

サイバーセキュリティ経営をコントロールする際の重要ポイント

佐々木　サイバーセキュリティ経営では、多様なプレーヤーが登場する。あるべき情報共有の姿は。

阿部　ANAの場合、事業会社が多く、ガイドラインに疎い人もいる。エンジニアとセキュリティベンダー、事業会社など、対象によって伝え方を変えている。また、伝えるべき情報を精査している。

九野　今やサイバーセキュリティリスクは、企業を超えて共通する経営課題だ。自社で対応できることは限られる。業界や国全体で情報を共有すべきだ。

大井　東証では適時開示制度に伴い、企業がサイバー攻撃を受けた際、第三者調査委員会により、リポートが課されることがある。リポートはウェブで閲覧可能。リポートを読み込み、自社が攻撃を受けた場合どうなるのか、検証し、共有するといいだろう。

経済産業省
商務情報政策局
サイバーセキュリティ課長
師田 晃彦氏

ANAシステムズ
品質・セキュリティ監理室
エグゼクティブマネージャ
阿部 恭一氏

日立製作所
サービスプラットフォーム事業本部
セキュリティ事業統括本部
セキュリティ戦略本部 本部長
九野 伸氏

西本　経営戦略のなかで、情報共有すべき事項を明確化すべきだ。経営者のリーダーシップが問われている。

師田　普及が進んできたサイバーセキュリティ経営ガイドラインを、より充実したものにすべく、改定作業を進めていく。

佐々木　社会構造が変化するなか、サイバーセキュリティリスクと安全性をどう両立するか。

九野　リスクを定量化して考えることが必要だろう。IoTの進展には、サイバーセキュリティが必要不可欠。サイバーセキュリティは、コストではなく投資として捉えるべきだ。

阿部　リスクをどこまで許容するかが問われている。当社の場合、サイバーセキュリティは、安全品質に関わるコストと定義している。イノベーションとセキュリティの両立も重要だ。

西本　風評被害や賠償請求、顧客満足度の低下など、サイバーセキュリティにはさまざまなリスクがあり、対応策は一様ではない。

大井　経営戦略を踏まえて、守るべき資産を特定し、サイバーセキュリティリスクを洗い出す必要がある。どこに弱みがあり、どの程度の経済的損害があるのか、第三者の目で検証することも大切だ。

師田　経済産業省では、オリパラを見据えて、重要インフラのリスク評価事業を進めている。内閣官房をはじめ各省庁とも連携を取り、サイバーセキュリティの防衛力を高めるのみならず、産業化を後押ししたい。

佐々木　サイバーセキュリティリスクへの対応は、不断の努力が問われる。継続的な取り組みが必要不可欠だ。

●コーディネーター
東京電機大学　教授
佐々木 良一氏

ラック
代表取締役社長
西本 逸郎氏

TMI総合法律事務所
パートナー弁護士
大井 哲也氏

講演①

企業経営者が理解すべきリスクポイントとは ～これからのサイバーセキュリティリスク

ラック
代表取締役社長
西本 逸郎氏

IT運用もほかの経営課題と同様、リスクを予見し、あらかじめ手を打つことが求められる。すべての企業は、経済産業省が公表した「サイバーセキュリティ経営ガイドライン」の詳細を把握し、少なくとも基本姿勢を決める必要がある。

ガイドラインの内容は、一言でいえば、CISOを配置しCSIRTを構築せよ、という話だ。これを実効性のあるものにするためには、内部および外部のキーマンや組織との連携、協力が欠かせない。

CISOは、常にサイバーセキュリティリスクに目を光らせ、動くべき段階をすぐに判断しなければならない。場合によっては、個人情報を扱うなどの危険な業務の中止や分離のほか、関係者への注意喚起や公共機関への相談などを行い、速やかに問題を解決する必要がある。

サイバーセキュリティリスクに対応する一連の仕組みを自前で運用するには、一般的にある程度の規模がある程度の規模が求められる。サプライチェーントップやグループ企業、地域などを巻き込み、共助体制を構築することも検討すべきだ。しかし、ほとんどの中小企業では、予算や人材が不足しており、できることは限られるだろう。時宜に応じて、専門業者の活用も視野に入れ、柔軟に進めるべきだ。

講演②

企業経営者による“サイバーセキュリティ経営”実践のポイント

KPMGコンサルティング
サイバーセキュリティ
アドバイザリー パートナー
田口 篤氏

「サイバーセキュリティ経営」は、適切なマネジメントリポートがあってこそ機能する。経営者の多くは、サイバーセキュリティリスクが最も重要なリスクだと認識しながらも、「よくわからない」という理由から、効果的な対策を講じていない。

日々のマネジメントシステムの活動記録やシステムの運用監視ログを蓄積している企業は多い。しかし、多くの企業は、それらの情報を有効に活用できていない。収集した情報をタイムリーにトップマネジメントにリポートできれば、経営判断に生かすことができる。

では、その仕組みはどうやって構築すればよいか。まず、CEOやCISO、CSIRT責任者など、それぞれのマネジメントの役割や権限に合った報告内容を定義する必要がある。関係者間における適切なコミュニケーションが重要だ。

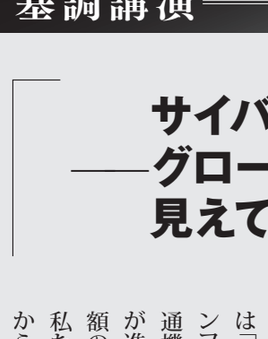
サイバーセキュリティ経営基盤の構築も必要不可欠だ。サイバーリスクをリポートしている企業は多いが、その内容が主観的だったり、過去データをマニュアル化しているだけのものも散見される。報告事項をKPI化し、セキュリティリスクを定量把握することやリアルタイムでのデータ自動集計など、経営モニタリングを自動化する仕組みを構築すべきだ。

基調講演

サイバーセキュリティ――グローバルな視点から見えてくること――

サイバー犯罪の産業化が進展している。サイバー犯罪も買う人、売る人がおり、オンライン上にブラックマーケットが確立されている。サイバー犯罪者は、ビッグデータやAIなど、最先端のテクノロジーを駆使して犯罪に及ぶ。IoTにより、彼らのビジネスチャンスは一層広がるだろう。

サイバー銀行強盗が目立つ。バングラデシュの中央銀行が被害に遭い、大規模な犯罪組織の関与が疑われている。データやシステムを〝人質〟としたサイバー犯罪も横行している。ハリウッドの病院の事例では、犯罪者が電子カルテを暗号化して金銭を要求。病院は「患者のためにならない」と金銭を支払った。重要インフラが狙われることもある。アメリカでは、公共交通機関の券売機が乗っ取られ、混乱を招いた。IoTが進展すれば、自動車がロックアウトされ、個人が多額の身代金を要求されるケースも出てくるだろう。私たちは、いつ何時サイバー犯罪に巻き込まれるかわからない時代に生きている。



インターポール
グローバルコンプレックス・フォー・イノベーション
総局長
中谷 昇氏

世界で多発した「WannaCry」など、主にビットコインを要求するランサムウエアの被害も無視できない。今回のケースでは、身代金の支払い額は大きくならなかったが、予断を許さない状況だ。

インターネット版の「オレオレ詐欺」と呼ばれる、ビジネスEメールによる詐欺の仕組みは巧妙でなかなか見抜けない。社長や副社長を名乗った犯人が経理担当者に対し、指定した銀行口座へ送金を指示するEメールを送信、金をだまし取るケースなどが見られる。犯人は、数カ月かけて対象者の文面を研究したうえで送信しているため、容易にだまされてしまう。全世界で被害件数は1万6000件、被害額は10億ドルに及び、100カ国以上で被害が確認されている。

警察にとって困難な時代だ。というのも、サイバー犯罪は、国境を容易に越えてしまうからだ。法執行の仕組みが国によって異なるため、思うように起訴できない実態もある。官民を挙げて、国際的な協力体制を構築する必要があるだろう。

CISO：Chief Information Security Officer（最高情報セキュリティ責任者）　**CSIRT**：Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）　**KPI**：Key Performance Indicator（重要業績評価指標）