KPMG Newsletter

KPMG Insight

Topic ①

海外子会社におけるサイバーセキュリティガバナンスの要点

Vol. 61

July 2023

Topic　海外

海外子会社におけるサイバーセキュリティガバナンスの要点

KPMG FAS
フォレンジック
上原 豊史／パートナー

KPMGコンサルティング
テクノロジーリスクサービス
勝村 学／アソシエイトパートナー
保坂 範和／ディレクター
川合 恵巳／ディレクター

昨今のサイバー攻撃はますます高度化・巧妙化が進み、管理体制の脆弱な海外子会社が狙われるケースも増えています。そこで、本稿では近年増加している海外子会社でのサイバーインシデントに備える観点から、現地法人や日本本社が理解しておくべき「海外子会社におけるサイバーセキュリティガバナンスの要点」について解説します。ターゲットとなりやすい海外工場におけるセキュリティ対策、各国・地域で厳格化の進む個人データ保護規制への対応、実際に被害を受けてしまった場合のインシデント対応の各要点を整理するとともに、日本本社によるガバナンス上のポイントについて提言します。
なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

☑ POINT 1
海外工場のサイバーセキュリティ対策で重要となるのは、資産管理とネットワークの可視化、マイクロセグメンテーション、従業員教育、サプライチェーン上のリスク評価である。

☑ POINT 2
グローバル個人データ保護の対応は、規制情報の収集と対応方針検討をグループ全体で一元的に実施し、効果的な協力・連携を促進する役割・責任の割当てと、リスクに応じた管理の仕組み化を図ることがポイントとなる。

☑ POINT 3
インシデント対応時は、「事実」に基づいて意思決定を行うことが肝要。緊迫する状況下であっても、根拠のない予想や希望的観測に基づく見切り発車は危険。事実を確認するための「調査」がきわめて重要となる。

☑ POINT 4
グローバルガバナンスの要点には、本社主導でのリスク管理とセキュリティ施策の導入、定期的な海外拠点のセキュリティ点検と教育の実施、CISOの役割強化などが挙げられる。


上原 豊史
Toyofumi Uehara


勝村 学
Manabu Katsumura


保坂 範和
Norikazu Hosaka


川合 恵巳
Megumi Kawai

Ⅰ 海外工場に必要なセキュリティ対策

1.工場のサプライチェーンを狙うサイバー攻撃

(1) アフターコロナのサプライチェーンに迫るセキュリティ脅威

新型コロナウイルス感染症（以下、「COVID-19」という）のパンデミックは、物理世界とデジタル世界の境界線をあいまいにし、サイバーセキュリティインフラの断層を露呈させるなど、多くの新たな課題を明らかにしました。工場では従業員のリモートワークだけでなく、請負業者の遠隔サービスサポートなども増加しており、リモートアクセスに関連する脆弱性を狙ったサイバー攻撃のリスクが高まっています。

攻撃者は、海外拠点や中小企業をターゲットとしています。実際に、国内でも大手企業のサプライチェーンを狙ったサイバー攻撃は顕在化しており、その影響は工場の操業にまで波及しています。

(2) ランサムウェア（身代金要求型ウィルス）の猛威

サイバー攻撃のなかでもシステム停止や情報漏えいと引換えに身代金を要求するランサムウェアの脅威が勢いを増しています。ランサムウェアによる工場インフラの停止など、新聞の見出しをにぎわすようなインシデントが各国・地域で相次ぎ、工場のサイバーセキュリティにとって憂慮すべき状況が続いています。

このような状況を受け、多くの企業が重要な事業運営と俊敏性を維持しながら、必要な投資、人材、技術を最重要課題に充てるため、工場セキュリティの見直しを急いでいます。

2.サプライチェーンに対するセキュリティ要求

(1) 政府動向

日本国内では、サプライチェーンの安定供給を目的として経済安全保障推進法案が2022年5月に参議院で可決され、同11月には経済産業省から「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン　Ver.1」[1]が発行されました。工場のサプライチェーンに対するセキュリティ強化に向けた取組みが進められています。

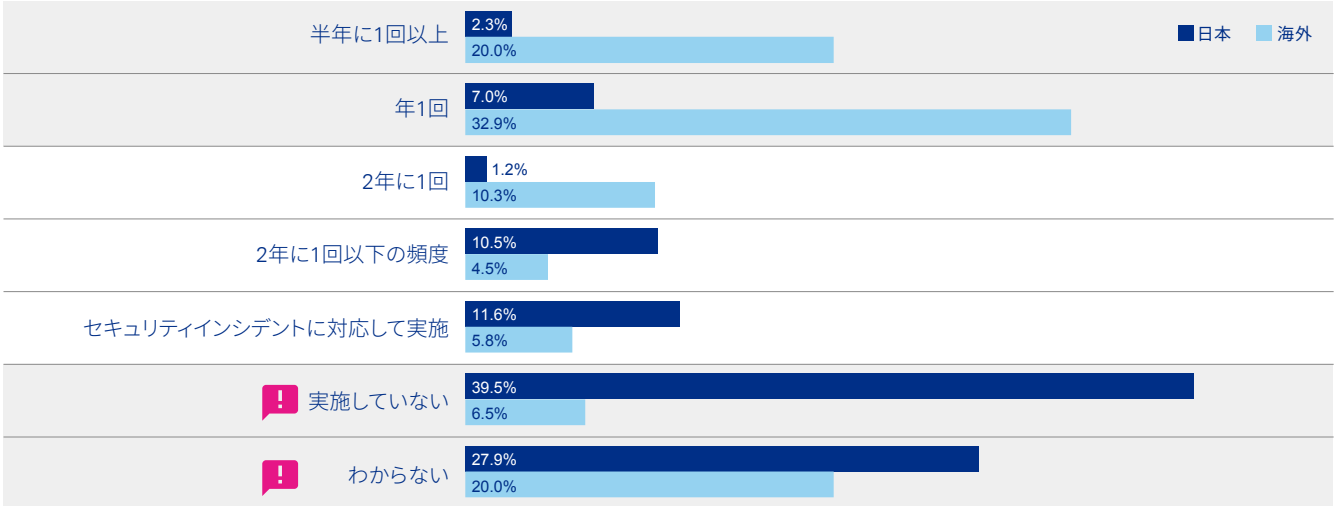
(2) 海外動向

海外では、エネルギー業界を中心にサプライチェーンに対するサイバーセキュリティ監査の取組みが進んでおり、業界標準のセキュリティフレームワークをベースとしたサイバーセキュリティ監査がサプライヤーに義務付けられています。なかでも欧州では、IoT機器の相互接続の増加によるリスクの増加を考慮して、サイバーレジリエンス規制（EU Cyber Resilience Act）が提案されています。同法案は、IoT機器を欧州に出荷する日本企業にも影響を与えるものであることから、製品の設計、開発、文書化手順の変更を余儀なくされる可能性があります。

図表1　進まない工場のセキュリティアセスメント

制御システムに対するセキュリティアセスメントの実施状況

海外と比べてセキュリティアセスメントの実施は大きく遅れている



出典：KPMGサイバーセキュリティサーベイ2022（https://kpmg.com/jp/ja/home/insights/2022/01/cyber-security-survey2022.html）

（日本：複数選択可／n=86）

3. 海外工場に求められるサイバーセキュリティ対策

「KPMGサイバーセキュリティサーベイ2022」[2]によると、年1回以上セキュリティアセスメントを実施している海外企業は半数以上ですが、日本企業は1割程度です（図表1参照）。

そのため、海外工場のセキュリティ責任者は、まずセキュリティアセスメントを実施し、工場のサイバーリスクを把握します。次に、リスクに応じたセキュリティ対策を実施して、許容水準までリスクを低減させます。これが、サプライチェーンにおける社会的責任として求められています。実践的なセキュリティ対策の候補としては、以下の4つが挙げられます。

①資産管理・ネットワーク可視化

資産管理とネットワークトラフィックの監視を改善することで、制御システム環境に対する洞察力を向上させます。これにより、障害の発生する可能性と期間を削減できます。

②マイクロセグメンテーション

工場の制御システムのネットワークをITネットワークから隔離します。可能な場合は、さらにネットワークをマイクロセグメンテーション化します。これにより、インシデントの広がりを抑え、被害の範囲を縮小できます。

③トレーニング・教育

トレーニング、教育、組織内のセキュリティ文化の醸成と改善を通じて、従業員を育成します。これにより、インシデントの発生リスク、被害、復旧時間を抑えることができます。

④サプライチェーン

サプライチェーンのセキュリティを調査し、システムへの侵入経路をコントロールします。これにより、サプライヤーへの攻撃が自組織に影響を及ぼす可能性を低減できます。

Ⅱ グローバル個人データ保護対応

1. 日本企業における個人データ保護の課題

（1）データ利活用に関する動向

競合他社との差別化を図るため、日本企業は製品・サービスの海外市場に対する展開やDX（デジタルトランスフォーメーション）推進の文脈において、全世界の消費者・取引先から多くのデータを収集し、高度に分析を行って積極的に活用する局面に差し掛かっています。これに対して、各国政府・監督機関による個人データ保護規制の執行や、消費者・投資家などのプライバシー意識の高まりを背景に、個人データ保護の重要性はますます高まっています。日本企業も、早急に課題の論点整理と解決に向けた優先順位付けが必要な状況にあります。

（2）個人データ保護規制の厳格化

2017年頃を起点に、世界の各国・地域で、個人データ保護を目的とした規制の新設・改訂が進みました。日本の個人情報保護法も2020年に改正されましたが、世界的な傾向として、多くの規制がEU GDPR（欧州一般データ保護規則、以下「GDPR」という）に追随した、厳格な要求事項を定めており、実際に違反事例に多額の制裁金が課されています。

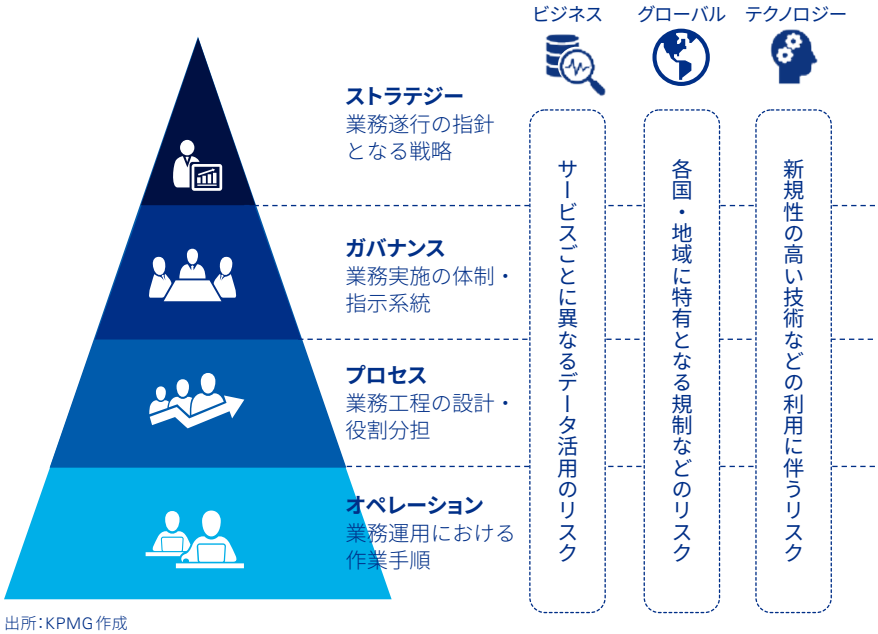
これまでの日本企業における個人データ保護は、こうした規制を遵守さえしておけば問題ないという理解でした。しかし、近年の個人データ漏えい事故や社会の反応を鑑みるに、そのような企業の見解や態度と、消費者・投資家などが期待する個人データ保護の水準には若干の乖離があるものと推察されます。

2. 個人データ保護に関する対応方針

（1）複雑化するリスクへの対応

データ利活用の推進にはさまざまなリスクが伴います。特に、事業活動において世界各地の消費者や従業員などから個人データを取得している、またボーダーレスに個人データが流通している状況は、そのリスクを一層複雑にし、課題解決へのハー

図表2　個人データ保護対応のフレームワーク



出所：KPMG作成

ドルを高めます。

たとえば、多くの個人データ保護規制では、国外に個人データを移転する場合に、自国規制と同等水準でデータを保護するよう義務付けています。加えて、各国・地域では消費者・投資家などのプライバシー意識にも大きく違いがあります。したがって、ある国・地域では許容され得る個人データの取扱いも、他の地域では規制により禁止されている、または社会的な炎上の火種になってしまうことがあります。

(2) 個人データ保護対応の発想転換

日本企業の個人データ保護対応は、今まさに発想の転換を迫られています。従来は本社・関係会社（海外含む）が各々の責任で所在する各国・地域の個人データ保護規制を遵守することが主流でした。しかし、こうした方針は本社が業務を統括し、主要な事業や製品・サービスの開発設計を担う典型的な日本企業のグローバル機能役割モデルには、必ずしも効果的とは言い難いでしょう。

それは、どのような規制環境の市場に進出するか、どういった個人データを製品やサービスを通じて取得・分析するかなどは開発設計の段階で決定するものであり、海外拠点の主要な機能である生産や販売の段階で可能な保護対策は限られてしまうからです。個人データの保護対策として最も強力な「個人データを取得しない」という対策も、製品・サービスの仕様がすでに決まっているのであれば、その実施に限界があることは容易に想像がつきます。

3.グローバル個人データ保護対応の進め方

以上より、複雑化するリスクを前提に、日本企業では今後、個人データ保護対応のフレームワーク（図表2参照）を参考として、一気通貫で体系的に施策を進めていくことが、課題解決への第一歩となります。

(1) ストラテジー

ストラテジーの観点では、本社で主要な各国・地域の個人データ保護規制を把握するとともに、リスクを評価することが重要となります。通常、グループ全体で見ても個人データ保護対応のリソースは限られています。そこで、事業の重要性や規制執行の重大性を軸に、どの領域や拠点などにリソースを投下するかを議論します。評価の結果、本社が高リスクの領域や拠点を重点的にサポートし、加えてモニタリングを強化することで、規制違反やそれに伴う被害拡大の可能性を効率的に低減することができます。

(2) ガバナンス

ガバナンスの観点では、本社・関係会社間の機能役割の違いや関係性などを踏まえて、グループ横断的に個人データ保護の責任分担を整理します。ポイントは、適切なリスク管理に必要な専門性を補うように体制を構築することです。そのためには、ビジネスとグローバルの側面から、個人データ保護を統括する管理部門だけでなく、事業部門や地域統括部門などからも協力を得られるよう働きかけます。定期的な情報共有の機会を設けるなど、関係各位の巻込みを図ることにより、当事者としての意識を醸成しながら進めるとよいでしょう

(3) プロセス

プロセスの観点では、必要な対応項目をライフサイクルを軸に整理して、網羅的に実施内容を定め、業務手順と実務担当者を整理します。特に、スマートフォンアプリやIoT（センサー）を介したデータの収集、ビッグデータやAIによる分析などテクノロジーを駆使した個人データの取扱いは、処理がブラックボックスになりやすく、必然的にプライバシー侵害と認識されるリスクが高くなります。消費者などにそのような懸念を抱かせることがないような保護対策を講じなければ製品・サービスを販売開始できないといった仕組みを備えるべきと考えます。

(4) オペレーション

オペレーションの観点では、従業員などが迷わず適切に作業するための手順や運用書類などを整備します。一般的には、事業企画時に講じる対策を示すチェックリストを作成し、製品・サービス導入時からリスクの低減を図ることが肝要です。加えて、個人データを利活用する際のルールも明確に周知することで、運用上の不適切な取扱いを防止できます。

個人データ保護の最後の砦は、実務を担当する従業員です。定めた手順などが形骸化しないように定期的な見直しや、システムによる作業の自動化などに中長期的に取り組むことが望ましいでしょう。こうした取組みは、リスクの低減に大きく貢献します。

Ⅲ サイバーインシデント発生時の対応

1.インシデント対応は「事実」に基づいて意思決定する

(1) 感染（異変）への気づき

サイバーインシデント対応の第一歩は、サイバー攻撃を見つけることです。そのためには、日頃からシステムやサーバなどを監視し、わずかな異変も見逃さないことが重要です。たとえば、ランサムウェアに感染した場合、通常、以下のような異変が発生します。

- 業務システムやファイルサーバのデータが暗号化され、通常利用ができなくなります。場合によっては、サーバのログ（アクセス記録）情報が消去されていることもあります。
- ネットワークなどのトラフィックを監視している場合、内部から外部に向けて

データを送信している不自然な通信を見つけることができます。

- 身代金を要求した「犯行声明文」（電子ファイル）がサーバ内に保存されています。
- ダークウェブサイトなどに社内の情報が一部公開されていることがあり、警察や外部の方から連絡を受けることがあります。
- SNSなどを利用して情報拡散（身代金の要求の手段として）されることがあります。
- 攻撃者への反応を無視していると、会社のウェブサイト管理者や従業員宛てに電子メールが届くことがあります。

ランサムウェアは身代金が目的であるため、多くの場合、攻撃者はどうにかして身代金を払わせるような圧力（時として継続的なアクション）をかけるからです（図表3参照）。

（2）最大リスクは業務の完全停止

攻撃を受けた側の企業にとって最大のリスクは、業務停止です。攻撃によってシステムデータやファイルサーバのファイルが暗号化されてしまうので、システムの稼働が止まってしまうからです。そうなると、特定の業務のシステムが利用できなくなるなど、社内ネットワークに影響を与えます。最悪の場合は、社内に留まらず、ネットワークを共有するグループ企業やサプライチェーンでつながっている企業の業務オペレーションも停止となることがあります。

よく耳にする話としては、生産・販売管理システムがダウンしてしまったが、生産装置は切り離されているので、工場での生産活動は継続できたり、在庫の販売を継続しつつ、事務連絡は電話やFAXをフル活用して復旧するまで代替したりといったことがあります。

（3）刻々と変わる状況に応じた意思決定

状況によっては、これまで自社が経験したことのない緊迫した事態に陥ることもあり得ます。そのような場合は、初動対応で同時にさまざまな対応を求められることになります。

たとえば、B to Cビジネスで大量の個人情報を保有している企業の場合、当局報告が必要になります。また、被害が発生するケースでは、被害者保護に向けたアクションも必要です。システム回復に時間を要することが想定されれば、マニュアルでの代替オペレーションの手順の整備が急務となります。サプライチェーンの一翼を担う企業であれば、仕入先、納入先との連絡調整が必要になります。

こうした対応には事前の備えが効いてきます。誰がどのような役割を担当するか、想定外の状況が発生した場合はどのような指揮命令系統に基づき意思決定を下すか、刻々と変化する状況を集約し、統制を掛けてコミュニケーションを取っていくことが重要です。

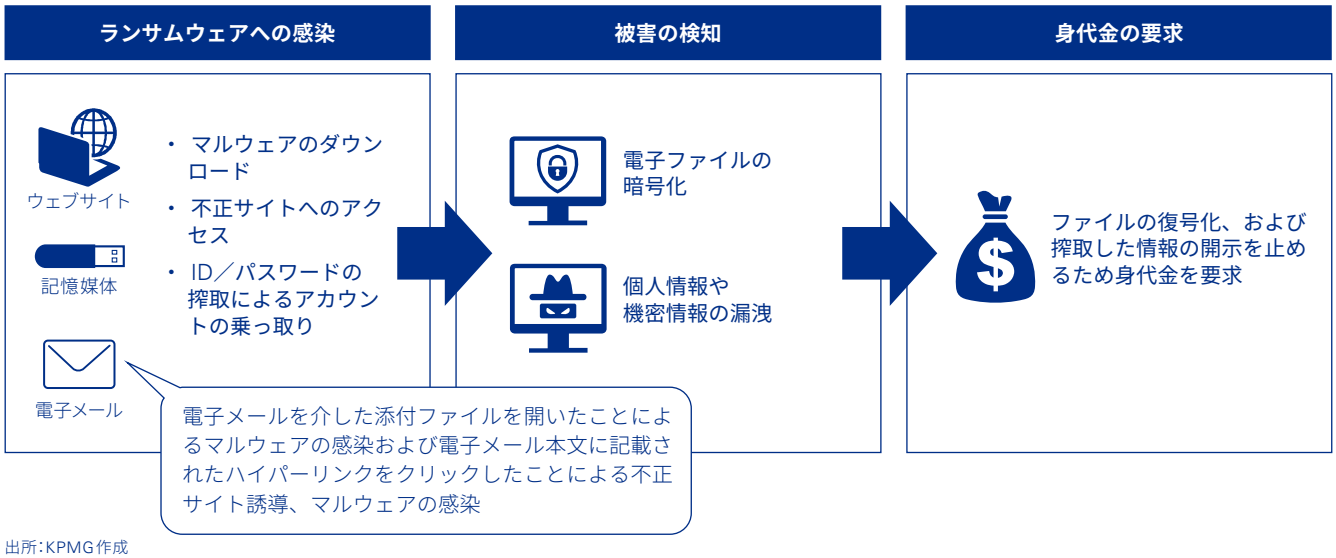
2.時系列別サイバーインシデントへの具体的対応

（1）「事実」の見極め（＝調査）

あらゆるコミュニケーションを取るうえで「事実確認」なしには、何もできません。初動対応で一刻も早い事実確認こそが、最も重要なアクションになります。

✓ 被害範囲（マシン、システム、ネットワーク、システムユーザなど）の特定

図表3　被害企業側からみたランサムウェア攻撃



出所：KPMG作成

✓ 被害状況（流出データの特定）の把握
✓ 手口（侵入ルート、攻撃手法）の特定
✓ いつ攻撃を受けたか
✓ 原因（ソフトウエアの脆弱性、アカウントの乗っ取りなど）の把握

正しい事実の理解がなければ、作業のやり直し、無駄な作業／投資、事実と異なる情報公開など、誤ったアクションを取ることになります。

（2）リスクエリアの切離し・隔離

サイバー攻撃を受けたとしても、可能な限り事業活動を継続しなければなりません。そのためには、止血作業をしつつも、安全が確認できたところから通常モードに戻していきます。

たとえば、ネットワークの管理者権限を乗っ取られた場合ならば、ネットワーク（ドメイン）の再構築、ユーザID・パスワードの再設定、振舞い検知（EDR）の導入による監視体制など、整備ができたところから復帰していきます。あるいは、古いマシンやOSで脆弱性を有したまま利用していた場合ならば、マシンそのものを新しいものにリプレイスし、OSも最新版をインストールします。

（3）システムやデータの原状回復のシナリオ策定

ネットワークやハードウェアの対処とともに、データの復旧も業務再開に向けてきわめて重要です。災害対策用のバックアップシステムやデータのフルバックアップがあれば、システムを回復させることができます。ただし、どの断面のデータを復旧させるかは慎重な判断を要します。たとえば、バックアップデータから復旧（リストア）させる場合、マルウェアが数回に分けて仕込まれていることに気づかず、攻撃をされる前の最新の状態に戻せばいいと思いこんで拙速に対応してしまうと、マルウェアを含んだ状態で復旧させてしまうことになります。

（4）当該インシデント対応に係る情報の一元管理

被害が明らかになり、事態が徐々に関係者に知れ渡っていくことになりますが、そうなると社内広報、および対外的な広報対応でどのような情報をどのように発信していくかという課題に突き当たります。

このとき最も注意すべきことは、各現場からの勝手な（憶測も含む）情報発信を防ぐことです。たとえば、従業員が勝手にマスコミの取材を受けてしまったり、取引先との何気ない会話で事実と異なる内容を話してしまったりなどの事態を避ける必要があります。

これは、情報を隠蔽することが目的ではなく、会社として正しい情報を発信するためです。把握している最新の情報を一元的に集約して情報発信をコントロールし、企業価値の棄損を最小限に留める活動の一環なのです。

（5）取引先への説明対応

社内における被害の実態把握や切離しを実施することと並行して、重要クライアント企業や原材料・部品などの仕入先に今後の対応などを説明したり、要請をしたりすることになります。

ここで対応を誤ると、信用問題に発展しますので、クイックでありつつも慎重な対応が求められます。留意したいことは、仮に自社がサイバー攻撃を受けた被害者だったとしても、取引先企業からすると、迷惑をかけてきた加害者（きちんとセキュリティ対応をしていなかった者）だということです。とりわけ、強弱がはっきりした企業間の関係性がある場合、定期的な状況報告を個別に求められたり、特定のアクションについて期日を切って対応を迫られたりするということもあります。また、取引継続のためには、セキュリティに関する追加的な監査を要求されたり、機密情報が漏えいした可能性がある場合などには守秘義務契約の違反を指摘されたりする事態が想定されます。

（6）個人情報の流出への対応

ファイルサーバなどが攻撃を受け、情報流出が疑われる場合、個人情報の流出の可能性を考える必要があります。攻撃者は、個人情報をターゲットに情報搾取を試みます。また、電子メールにも個人情報が多く含まれていますので、電子メールが流出した場合も注意が必要です。

個人情報の漏えいによって金銭的、精神的な被害が発生することが予想される場合、コールセンターや問い合わせ窓口を設置することが求められます。

また、国・地域によって個人情報関連の法規制の要件は異なりますので、自社のビジネスを展開している国・地域の個人情報の定義、当局への報告要件などを事前に確認しておきます。なお、アジア地域の国・地域によっては、個人情報関連の法整備が未整備／検討中ということもあります。その場合は、GDPRの要件に基づいて管理態勢を整備するとよいでしょう。

（7）機密情報の流出への対応

個人情報と併せて、機密情報の流出の可能性についても確認する必要があります。機密情報とは、たとえば重要事実に関するインサイダー情報であれば、次のようなものが挙げられます。

✓ 業績変動に関する情報
✓ M&Aなどに関する情報
✓ 訴訟など紛争に関する情報

上記以外にも、重要な契約書や製造方法、原料の配合方法に関する情報、販売価格や仕入値など営業機密に関する情報なども機密情報となります。また、広範囲な情報が「秘密」と定義されている守秘義務契約が存在する場合には、情報の重要度にかかわらず、守秘義務違反が生じる可能性があります。

（8）インターネットサイトやダークウェブなどの継続的なモニタリング

一般的にどのマシンが攻撃を受けたかを把握することができても、どの情報（ファイル）が流出したかを特定することは困難です。それは、システムが出力するログデータにはファイル名の記述がないからです。多くの場合、不正アクセスがあったマシンの特定とそこから外部へ送信した通信量（データ量）を頼りにあたりを付けることになります。犯行グループが公開した情報を通じて、漏えいの事実を確定することもあります。攻撃グループは身代金の支払いを誘発させる手法として、搾取した情報をダークウェブサイトに小出しにして開示をしてくることがあるからです。

したがって、インシデント発生から3ヵ月程度は継続してインターネットサイトやダークウェブサイトにどのような情報が公開されているかをモニタリングする必要があります。

（9）真摯な対応を継続する

これだけ世の中にランサムウェア攻撃が増えてくると、サイバー攻撃を受けているのは自社だけとは限りません。仮に取引先から厳しい対応を迫られることがあったとしても、実はその取引先自身も過去に同様のサイバー攻撃を受けた経験がある場合もあります。

人間の心理としては、「少しでも被害が小さくあってほしい」、「きわめて初歩的なセキュリティ対策の不備で攻撃されたと思われたくない」など、希望的な観測や保身的な発想を取りがちですが、最悪の事態も想定しつつ、事実に基づいて、冷静（ある意味、冷徹）に対応していくことが求められます。希望的な憶測に基づく解釈や都合よく作り上げたシナリオは、後になって訂正やさらなるお詫びを招くことになるからです。

（10）再発防止に向けて取り組む

ひとたび事態が鎮静化してくると、次のアクションは再発防止に向けた取組みの検討です。各事案によって個別性が高いので、ここでは何をどのレベルまで対処すべきかについては触れませんが、何らかの原因（脆弱性の放置、人材不足、IT機器などの老朽化への対応不足、従業員への教育不足など）がそこにはあったはずです。事実に即した対応を実施しなければ、対処したつもりでも穴が開いたままとなってしまい、数ヵ月後に2次攻撃に晒されることになります。正しい対処を行うには、正しい事実の把握に基づきます。事実から目を背けない姿勢が大切です。

Ⅳ グローバルセキュリティガバナンス構築、5つのポイント

海外事業に伴うセキュリティリスクはますます複雑化してきています。しかしながら、多くの日本企業では十分な現地人材や駐在員を確保することが難しく、現地拠点のガバナンスは日を追うごとに困難さを増しています。駐在員まかせのセキュリティ管理・推進は限界を迎えており、日本本社の関与とグループを挙げての仕組み作りの取組みが欠かせません。

海外子会社のサイバーセキュリティを確保するためには、以下の5つのポイントが重要となります。

①CISOの役割強化とグローバルでのガバナンス体制の構築

CISO（Chief Information Security Officer、最高情報セキュリティ責任者）が取締役会で十分な役割を果たし、セキュリティ課題をグループ全体の取組みとしてコントロールしていくことが重要です。また、本社、各地域統括などの役割を定義し、課題を個社だけのものとせず、グループとして対応を推進していくことのできるガバナンス体制の構築が求められます。

②本社主導でのリスク管理とセキュリティ施策の導入

各拠点が場当たり的に対策を講じるのではなく、本社主導で海外拠点のセキュリティリスクを正確に把握し、グループ全体で整然と最適なセキュリティ施策を計画し、導入することが求められます。

③定期的な海外拠点のセキュリティ点検の実施

全般的なセルフチェックの実施だけでなく、新たなサイバーセキュリティリスクにも対応した外部の点検ツールなども活用し、定期的に最新のリスク点検を行うサイクルをグループ全体で確立する必要があります。

④グローバルでのセキュリティポリシー策定とセキュリティ教育の徹底

最低限遵守すべきセキュリティレベルをグループ共通のセキュリティポリシーとして定義し、本社から継続的に情報発信を行うとともに、現地従業員の教育をサポートしていくことが求められます。

⑤インシデント報告ルートの明確化と事後対応の計画

海外拠点でサイバー攻撃被害が発生した場合の報告ルートの確立と、技術的な対応だけでなく、ステークホルダーへの説明や広報面も含めたレスポンス対応全般について、事前に計画を立てておきます。事前の準備が、被害や問題を拡大させない重要なポイントとなります。

以上、大きく4つの視点から、海外子会社におけるサイバーセキュリティガバナンスの要点を解説してきました。いずれの視点においても、日本本社によるリードと、現地法人との緊密な連携が重要なポイントとなります。

グローバルグループでのセキュリティガバナンスの重要性はこれまでにないレベルにまで高まっています。現地法人はもちろ

ん、日本本社の経営層の理解度が、海外事業の今後の命運を分ける大きな鍵となるかもしれません。

1 経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン　Ver.1.0」
factorysystems_guideline_ver1.0.pdf (meti.go.jp)

2 KPMGジャパン「サイバーセキュリティサーベイ2022」
https://kpmg.com/jp/ja/home/insights/2022/01/cyber-security-survey2022.html

関連情報

工場サイバーセキュリティ対応支援などを紹介しています。

https://kpmg.com/jp/ja/home/services/advisory/sectors-markets/factory-advisory.html

本稿に関するご質問等は、
以下の担当者までお願いいたします。

株式会社 KPMG FAS
上原 豊史／パートナー
Toyofumi.uehara@jp.kpmg.com

KPMGコンサルティング株式会社
勝村 学／アソシエイトパートナー
manabu.katsumura@jp.kpmg.com

保坂 範和／ディレクター
norikazu.hosaka@jp.kpmg.com

川合 恵巳／ディレクター
megumi.kawai@jp.kpmg.com

KPMGジャパン
home.kpmg/jp

home.kpmg/jp/socialmedia