KPMG

サイバーセキュリティ主要課題2022

序文

サイバーセキュリティは「できない」ではなく「できる」を追求すること

私たちを取り巻くサイバー攻撃の脅威は拡大する一方です。サイバー犯罪者はあの手この手で金もうけを画策し、使用するツールや技術は巧妙化する一方です。危険と隣り合わせの環境において、企業の最高情報セキュリティ責任者（CISO）とセキュリティチームには、「攻め」のマインドセットが不可欠です。「してはいけないこと」を社内に告げる「守り役」ではなく、「安全にできることは何か」を示すことが重要です。

強制者からインフルエンサーへ：変わるCISOのあり方

新型コロナウイルス感染症（COVID-19）の世界的な流行を受け、優れたサイバーセキュリティチームは、即座に従業員がリモートワークで安全に業務を継続できる環境を整えました。戦略的に重要な「気づき」もありました。コロナ禍の「オンライン・非対面」という制約のもと、顧客離れを防ぎ新たなニーズに応えるにはどうすべきか、各企業が改めて考えるきっかけになったことです。顧客中心主義へと考え方が変化し、企業がデジタルトランスフォーメーション（DX）に急速に取り組んだことで、顧客が安心して企業とコミュニケーションできるようにもなりました。

刻々と変化する環境において、サイバーセキュリティチームは従来の「組織の強制者」から、「組織を触発するインフルエンサー」へと変貌を遂げようとしています。経営幹部の関心も高まっており、「KPMGグローバルCEO調査2021」によると「強力なサイバーセキュリティ戦略は、主要ステークホルダーとの信頼構築に不可欠」と考えるCEO（最高経営責任者）が75%に達しています。

一方、DXの加速とともに、委託先のサードパーティのエコシステムに関連するリスクが増大することも事実です。79%のCEOが「提携先企業のエコシステムとサプライチェーンを守ることは、サイバー攻撃に対する自社の防御策と同等に重要」と回答しています。

「サイバー攻撃への備えは十分」と回答したCEOは過半数（58%）を占めたものの、ほぼすべての企業が「何らかのサイバー攻撃は不可避」と見ているようです。サイバーセキュリティチームは、従来以上に現実味を帯びているサイバーインシデントに対し、準備を怠ることなく、迅速に対応・復旧・信頼の再構築に取り組み、被害を軽減する体制を整えておかねばなりません。

この環境での最大のリスクは、敵が常に高度化と複雑化を続けている点です。取締役会から経営幹部、フロントオフィス、バックオフィスに至るまで、社内全体に統制をきかせ、自社や顧客にとって大切な「価値ある資産」を守り抜く必要があります。

実際にサイバー被害を受けなくても、準備が不足していたり、過剰反応したりすることも不利益をもたらしかねないことはかねてから指摘されており、とりわけコロナ禍では、この傾向が顕著です。したがって、シナリオごとに対応策をテストし、どのようなレベルや種類のサイバーセキュリティインシデントに対応できるかを把握しておくことが重要です。これは、業界を問わず、どの企業にとっても対応・復旧戦略を見直し、早い段階から前倒しでセキュリティを考慮する「シフトレフト」のセキュリティを実現する機会になります。

CISOが検討すべき8つの主要課題

CISOにはさまざまな役割がありますが、すべてを同時にこなすことはできません。だからこそ「セキュリティは全社員の役割」と認識することが重要ですが、それ以上に大切なのは「顧客やステークホルダーとの信頼関係を築き、維持する鍵となるのがセキュリティ」と理解することです。

本レポートでは、2022年以降を見据え、経営幹部や取締役会のレベルでCISOが優先的に問題提起すべき8つの課題を選定しました。これらの8項目は、共同責任の考えに則ったセキュリティ計画がいかに本業のプラスとなるか、経営幹部の理解を得る一助となるはずです。

今後もさらに巧妙化する脅威やランサムウェア、バックドア、新しいタイプの攻撃への対応を迫られることになります。どの企業にも経営目標を念頭に策定された行動原則があるはずです。CISOや配下のセキュリティチームは、この行動原則を守りながら、柔軟かつ最先端のセキュリティ計画を打ち出すことができれば、サイバー攻撃の影響を最小限に抑える組織づくりが可能になるでしょう。

Akhilesh Tuteja
KPMGインターナショナル
Global Cyber Security Leader

KPMGからの提言

サイバーセキュリティ主要課題 2022

1 戦略的なセキュリティ議論の拡大

コストやスピードだけでなく効果的なセキュリティのあり方に議論の軸足を移し、ビジネスバリューやユーザーエクスペリエンスの向上につなげる。

2 成功の決め手：不可欠な人材とスキルセット

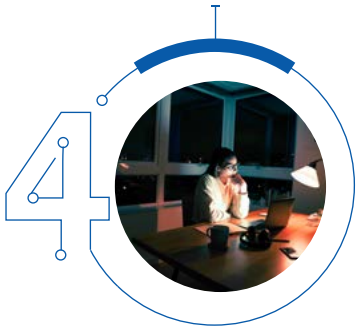
CISOやセキュリティチームの役割を、サイバーセキュリティの「強制者」から「インフルエンサー」へと転換する。

3 クラウド時代にふさわしいセキュリティ

導入・監視から復旧まで、自動化でクラウドのセキュリティを強化する。

4 ゼロトラストの中心軸となるID管理

あらゆるものがネットワークに接続された「ハイパーコネクテッド」にある今日の環境には、IAM（ID・アクセス管理）とゼロトラストで対応する。



5 セキュリティ自動化の活用

セキュリティ自動化をスマートに導入し、ビジネスバリューの実現を促進する。

6 プライバシーフロンティアの保護

プライバシー関連のリスク管理は、セキュリティとプライバシーに配慮した多層的な手法に切り替える。

7 境界を超えたセキュリティ対策

サプライチェーンのセキュリティ対策は、時間のかかる作業から自動化・協調型に転換する。

8 サイバーレジリエンスを巡る議論の見直し

サイバー攻撃を受けた際、業務を継続しながら、迅速に復旧し影響を緩和する体制を拡充する。

主要課題1

戦略的なセキュリティ議論の拡大

ビジネス目標とセキュリティニーズの整合性を目指す

この2年間で私たちの日常やガバナンス、ビジネスのあり方は一変しました。大切な資産やシステム、機密性が特に高いデータの安全を確保し守り抜くことは、もはやセキュリティ部門やIT部門だけの役割ではありません。むしろ、組織全体の戦略的な存続と業務の継続性を支えるためにも、組織全体でリスクに対応することが重要です。

経営幹部の認識を高める

産業革命の際に重要な役割を果たしたのが電力だとすれば、その現代版はデジタル技術で、これが企業の活力と能力を生み出します。同時に、セキュリティやレジリエンスが十分ではないデジタル技術は牙をむき、コミュニケーションの遮断やサプライチェーンの混乱を招きます。たった1度のデータ侵害やマルウェア攻撃でリアルタイムの取引やネットワークのやり取りが無力化され、結果的に数日間にわたって業務が停滞し、収益に悪影響が及びます。

「競争優位や長期的な成功を見据えたサイバーリスク管理には、取締役会や経営幹部のリーダーシップが必要」という理解が浸透してきています。特にデジタル化に伴うリスクに関して、戦略的な判断や管理を人任せにすることは、もはや通用しません。ビジネス目標に確かなセキュリティの枠組みが組み込まれていなければ、最新のセキュリティソリューションであってもリスク低減に大きな効果は望めません。

今日のグローバルなビジネス環境は、地政学、環境、社会、技術の面での不確実性がもたらす影響に常にさらされているにもかかわらず、相互接続が進んだネットワーク上での機密データのやり取りは拡大し、サイバーリスクも増大しています。CISOには、経営幹部や業務部門の目線を持つことが従来にも増して期待されており、他部門と協力しながら、自社の成長目標を踏まえた現実的なセキュリティ投資でレジリエンスを高める必要があります。そのため、サイバーセキュリティチームにも、自動化の推進やセキュリティ技術資産の強化、重要なスキルの獲得、パートナーエコシステムのリスクを排除するデリバリーモデルの構築など、さまざまな戦略を追求することが求められています。

求められる次の一手は？

自社の戦略的ビジネス目標とセキュリティとの整合性を高めるためにも、構想・設計段階からセキュリティとプライバシーの両方に配慮する重要性について経営幹部に理解を深めてもらえるよう、CISOやサイバーセキュリティチームは努める必要があります。ビジネスバリューやユーザーエクスペリエンスの改善に向け、社内の協議の力点を従来のコストやスピードから、実効性の高いセキュリティ体制のあり方に移します。顧客が利用するシステムの停止や、データの漏えいが発生した場合の代償は、一般的にサイバーセキュリティチームが想定している規模を上回り、加えて顧客や投資家からの信用失墜が拍車をかけます。さらに、その影響は長く続きます。

デジタルネイティブ企業やデジタル成熟度の高い企業は、開発側の都合でスピードを重視する傾向があり、リスクやセキュリティの原理原則に執着しません。

> CISOの大きなチャレンジは“通訳力”です。たとえば、CISOには絶えず変化するリスク環境について取締役会で説明する、協力してもらうために委員会を運営する、といった任務が求められます。業務を止めたいのではなく「顧客や投資家、提携先の信頼を高めたい」とわかりやすく説明することが大切です。セキュリティは社内の全員が当事者意識を持って取り組むべきものなのです。”

Rik Parker
KPMG米国
Principal, Cyber Security Services

ビジネスにはバランス感覚が求められます。言うまでもなく、競争力を高めるため、迅速に商品・サービスを投入することは重要ですが、業務のペースを維持できるようビジネスプロセスにセキュリティを組み込むことも同様に大切です。セキュリティに十分に注力しなかったがために顧客・投資家離れや信用失墜を招くことになれば、最初から時間をかけてセキュリティに適切に対応した場合より、はるかに大きな代償を払うことになりかねません。

人材の採用・つなぎ止めも意識の差が表れる部分です。セキュリティ人材の補充・補完として、自動化や委託先を活用できるかを評価する必要があります。実際、希少な人材を巡り、多くの企業が獲得競争を繰り広げています。サイバーセキュリティの関係者が人材の採用・つなぎ止めに向け、大学と共同で人材パイプラインを強化し、魅力ある職場環境や仕事づくりに力を入れてもよいでしょう。ビジネスプロセスや業務計画にテクノロジーを活かし、単純作業や定型業務のためにリソースが圧迫されないようインテリジェントな自動化を導入することも重要です。自動化ができない部分では、デリバリーモデルや人材獲得の面で独創的なアイデアが求められます。

特にAI（人工知能）やML（機械学習）は、スマートなオーケストレーションツールと連動させて、セキュリティ上の弱点や脆弱性の隔離だけでなく、パッチや復旧の自動化にも活用を検討すべきです。理想的なシナリオは、開発時に開発チームが手作業で従事するのではなく、自動化により多くの作業を任せられるようになることです。

AIはソフトウェア開発におけるスピードの維持に役立つうえ、悪意のあるコードをうっかり顧客に納入してしまうという事態を未然に防ぐ助けになります。実際の運用では、統制の一部とリスクを外部のパートナーに移すことになります。これはCISOにとっても業務部門責任者にとっても、依然として認識しづらい概念ですが、今後ますます開発にかかわる作業量とリスクが増え続けるなか、近い将来、極めて重要なトレンドとなると考えられます。

> 今日のCISOは、テクノロジスト、伝道者（エバンジェリスト）、調査官、心理学者、投資家、交渉役と、多面的に物事を考える姿勢が大切です。セキュリティと経営戦略の整合性を確保し、インシデントをチャンスと捉え、サイバーセキュリティチームの仕事のあり方を見直す必要があります。

Akhilesh Tuteja
KPMGインターナショナル
Global Cyber Security Leader

2022年に検討すべき主な施策

1. 機密性と可用性を軸とした従来のセキュリティ思考から脱却し、完全性とレジリエンスをいかに確保するかを検討する。
2. 組織や顧客データの保護、リスク管理、短期・長期の経営戦略を守るセキュリティ戦略について、社内の主要なステークホルダーと連携する。
3. コストやスピードよりも現実味のある全社的なリスクに着目するよう、セキュリティに対する経営幹部の意識を変える。
4. 業務の重要業績評価指標（KPI）や重要リスク指標に一喜一憂せず、インシデントの種類、社内外のプログラムの差、データ関連の施策（進行中、計画中、承認待ち）といった基礎データから見えてくるテーマや動向に着目する。
5. 構想・設計段階からセキュリティを組み込んだ場合と、そうでない場合に起こり得る被害についての意識啓発を通じ、業務部門との関係を構築する。

さらに理解を深めるために

サイバーセキュリティを自社のDNAに刻み込む
CISOはサイバーセキュリティへの意識をすべての業務に取り込み、全社員が責任を持つ体制を築く必要がある。

「ニューノーマル」での新たなセキュリティの現実
世界のCEOは困難に直面しながらもサイバーセキュリティのリスクに向き合っている。

サイバーセキュリティの幻想を捨てる
かつてないほど信頼が重視されている理由とは？

主要課題2

成功の決め手：不可欠な人材とスキルセット

サイバーセキュリティチームの役割を
強制者からインフルエンサーへ

先見性あるセキュリティチームが主導する最新のセキュリティプログラムにより、企業が迅速に行動したり成長を追求したりし、顧客により良いサービスを提供できるようになることが、明らかになってきています。サイバーセキュリティの戦略やツールは、絶えずチェック機能が働いていることを示す象徴的な存在です。だからこそ、システム開発部門や業務部門のリーダーは、セキュリティ分野のパートナーの後ろ盾があると安心し、ペースを崩すことなく業務に専念できます。この後ろ盾は、担当者が直接駆けつけるサポートの場合もあれば、最近、増加傾向にある自動化方式の場合もあります。

脅威の変化に合わせ、セキュリティチームの役割も変化

セキュリティチームと業務部門との関係における最大の変化と言えば、リスクを承知のうえで、市場に（必要なものを）迅速に投入するニーズが高まったことでしょう。コロナ禍以降はもちろん、それ以前でさえ、この傾向が見られました。

コロナ禍の収束の兆しが見えないなか、どの企業もセキュリティ体制の強化を続けながら、デジタルフットプリント（デジタル利用の履歴や痕跡）の管理やサイクルの変更に取り組む時期を迎えています。その結果、構想・設計段階からセキュリティを確保する「セキュア・バイ・デザイン」の考え方への移行、開発・セキュリティ・運用の連携によるDevSecOpsの推進、SDLC（システム開発ライフサイクル）でのシフトレフト（セキュリティ関連工程の大幅な前倒し実施）に拍車がかかっています。

効果的なサイバーセキュリティプログラムの内容について考える場合、リーダーシップの要素とチームの要素があります。リーダーシップの面で言えば、有能なCISOは技術について長々とは語りません。むしろ、ビジネスの方向性について考えたり議論したりすることに注力し、セキュリティ計画について経営幹部の意識向上や協力を目指し、上層部の声に耳を傾けることに力を注ぎます。

ファイアウォールやパッチ管理、情報漏えい対策はいずれも極めて重要な課題ですが、そのような話題をいきなり持ち出しても、相手は困惑してしまうでしょう。最近は業務部門について理解を深め、彼らの目線で語ろうとするCISOやサイバーセキュリティチームが増えています。社内にサイバーセキュリティプログラムがあることで業績拡大にいかに貢献しているかを、積極的に発信する姿勢が大切です。

最近のサイバーセキュリティ分野では求職者数よりも求人数が上回り、人材不足が喫緊の課題と言えます。経験豊富な専門人材は数として不足しているだけでなく、そうした人材は業界内を転々とする傾向があります。異なる経験を重ねて自分のスキルを磨き、新たな技能を身につけたいと考えているからです。

さらに、インターネット経由で単発の仕事が受発注される「ギグエコノミー」の拡大により、（従業員ではなく）請負業者として自由に働く労働市場が影響しているとも言えます。将来的には、サイバーセキュリティチームが作業量に応じて信頼できる外部人材を活用する時代が来るかもしれません。そうなれば、戦略的に重要な中核メンバーは絞り込まれ、必要に応じて人員を増減しながらタスクをこなすことも可能になります。

外部人材を活用する場合に重要となるのは、信頼であり、サイバーセキュリティ専門人材の情報センター的な機能を持つ機関の存在です。機密性の高いサイバーセキュリティのプロジェクトに関与してもらう以上、本当に確かな人物かどうかという点で、社内外の信頼できるプロの選球眼にかなった人材でなければならないからです。

> ボクシング元世界ヘビー級統一王者マイク・タイソン氏の有名な言葉に「誰にだって最初は作戦がある。顔面に一発食らうまでは」[1]というものがありますが、サイバーセキュリティにも通じるところがあります。サイバーセキュリティチームにはたとえ攻撃されても立ち上がり、十分な情報を集め、巧みな戦略のもと、綿密に計算された方法で対応できる備えが必要です。

Fred Rica
KPMG米国
Principal, Cyber Security Services

1 Mike Berardino, "Mike Tyson explains one of his most famous quotes," *South Florida Sun-Sentinel*, November 09, 2012.

こうした考え方の変化を受け、CISOやサイバーセキュリティチームの役割も組織の「強制者」から「インフルエンサー」へと変貌を遂げることになります。

求められる次の一手は？

サイバーセキュリティチームの進化は、プログラムづくりと同様、情報発信のあり方にも表れます。サイバーセキュリティチームは「組織にとっての障壁ではなく、味方だ」とシステム開発部門や業務部門に納得してもらうため、CISOは情報発信のあり方を変えていく必要があります。これはシンプルながら重要なメッセージですが、往々にして見過ごされています。

サイバーセキュリティチームは、パスワードやPINコード（個人識別番号）の設定のほか、多要素認証、セキュリティ意識向上を目的とした研修の実施など、従業員が不満を感じることに対し、時間をかけて耳を傾け相手の立場になって考えることで、前向きになるよう啓発することが大切です。仕事のあらゆる面で安全性とセキュリティに配慮しながら業務にあたる重要性をはっきりと伝え、それを遵守することが組織の業績や未来に結びつくのだと訴えていくのです。遵守しなければどうなるのかも、あわせて説明します。

こうした要件を守ることは「罰則があるからではなく、責任があるからだ」という認識に変えていかなければなりません。サイバーセキュリティの啓発活動についても、もっと魅力的に、遊び心を加えつつ、場合によってはゲーム感覚を持たせることもできます。そのために、AR（拡張現実）やVR（仮想現実）を駆使する手もあります。サイバーセキュリティは路上の障害物ではなく、皆の安全を守るためにあることを明確にしておけば、サイバーセキュリティチームもその方針に合わせて活動できます。

CISOは、自分自身やサイバーセキュリティチームが何に時間を費やしているかをしっかりと分析し、戦略、計画、構築、運用のバランスを見直す必要があります。サイバーセキュリティの分野では、計画やポリシーを検討する際、技術に踊らされやすい傾向があり、導入する技術の選定に影響することがあります。

1つの可能性として挙げられるのが、自動化、データアナリティクス、AI（特に機械学習）を組み合わせた継続的統制モニタリングモデルです。このモデルでは意思決定支援システムのデータサイエンスの面が充実するため、リアルタイムのサイバーセキュリティ状況と、組織のリスクプロファイルや対応施策との整合性を確保することができます。継続的統制モニタリングモデルは、現実の脅威状況の変化を検知し対処する標準化された動的セキュリティ体制によって、リアルタイムにデータを取得・解析することが目標です。

CISOやサイバーセキュリティチームは、絶えず発生する混乱への備えを怠るわけにはいきません。技術的な観点で言えば、サイバーセキュリティは委託先ベンダーやサプライヤー、パートナーを相互に結ぶ広範なデジタルエコシステムの番人となるのです。このエコシステムを管理しセキュリティを確保することは、サイバーセキュリティチームの最優先課題の1つに挙げられます。

一般的にサイバーセキュリティの専門家は、システム化を前提とした戦略的な経営指針について、スキルを磨き続けなければなりません。標準化、自動化、データアナリティクスを柱に、複数方式を組み合わせた考え方が必要です。業界全体で見ると、サイバーセキュリティチームは才能ある人材を惹きつけるだけでなく、インクルージョンの実現に立ちはだかる壁を壊し、幅広く多様な人材に門戸を開くことが大切です。

> 多くの企業がサイバー空間で「自動化競争」に突入しています。この状況に後れを取らないためにも、さまざまな産業や地域で生じる可能性のある脅威に対して現実的なシナリオ思考、テスト、対応を取り入れていかなければなりません。”

Matt O’ Keefe
KPMGオーストラリア
Partner, ASPAC Cyber Security Leader

2022年に検討すべき主な施策

1. 情報発信のあり方を変える。技術論ではなくビジネスを語る。
2. 従来からのサイバーセキュリティの定義にとらわれず、社内の他部門との関係構築、社内関係者とのネットワークづくりを続ける。
3. 社内のサイバーセキュリティチームの通常業務に、シナリオ思考、テスト、対応を組み込む。
4. コンプライアンスは、策定したセキュリティプログラムの重要な成果であって、チームの存在理由にすべきではない。
5. 伝道者（エバンジェリスト）を担う。セキュリティの重要性を説いて回り、社内のモチベーションを高める。
6. 「サイバーセキュリティは組織の重要な要素の1つで、組織のDNAに刻み込まれている」という考えのもと、セキュリティの役割についての意識改革を促す。

さらに理解を深めるために

将来のサイバーセキュリティを担う人材像
アウトソーシング、ギグワーカー、自動化を組み合わせ、能力活用のあり方に変革を起こす。

人的ファイアウォールの構築
サイバーセキュリティに潜む人的なリスクファクターを克服する。

機動性に優れたチーム文化の活用
責任感あるセキュリティ文化を醸成する4つの戦略。

主要課題3

クラウド時代にふさわしいセキュリティ

導入・監視から復旧まで、
自動化で強化するクラウドセキュリティ

サイバーセキュリティとクラウドセキュリティとの境界線は薄れてきています。両者の区別は、構築先の環境しかありません。データ保護、ID・アクセス管理、インフラ、脆弱性管理など、長年にわたってCISOが掲げてきた原則は、もれなくクラウドセキュリティにも当てはまります。違いがあるとすれば、それぞれに求められるテクノロジースタックです。こうしたセキュリティ対策が実装される環境には、監視から復旧までを網羅した自動化が求められます。「What」（対象）や「Why」（理由）は大きく変わっていませんが、「Where」（構築先）や「How」（手法）は明らかに変化しています。

DX（デジタルトランスフォーメーション）時代のクラウドセキュリティ

DXはクラウドの利用を加速させる一方、企業や組織を大きなサイバーリスクにさらすことにもなり、クラウドセキュリティのスキルが不足していると、組織を守る仕事は信頼性に欠けることになります。クラウドが場所を選ばないとすれば、ハッカーや犯罪者も同様に場所を選びません。

クラウドの広がりを受け、求められる技術が変化しています。クラウド環境は、導入から監視、復旧に至るまで自動化が求められるため、必然的に自動化への依存度が高まります。手動による操作があれば、内部の設定ミスによるインシデントの増加につながります。実際、Aqua Security社が実施した調査によれば、調査対象の90%の組織がクラウドの設定ミスに起因するセキュリティ攻撃に脆弱であることがわかりました[2]。

多くの企業から、クラウド開発チームがセキュリティエンジニアリングチームの機能も兼任できるのではないか、との意見が聞かれます。しかし、それは効果という意味で現実的ではなく、持続可能でもありません。理想を言えば、セキュリティエンジニアはこの重要分野に精通した専門家であり、クラウド環境の基本構造やニーズについて確かな視点を持った人材が担うべきです。同様に、クラウド開発者もセキュリティの役割に精通している必要がありますが、仕事の大部分を占めるのは、仮想環境のシステム設計、コーディング、分析・保守です。クラウド開発者には成果物に十分なセキュリティ対策を施すよう求める必要はあっても、開発チームがセキュリティの最後の砦になるべきではありません。

さらに、従来のセキュリティのロードマップに合致するスキルが、必ずしもクラウドやクラウドセキュリティの強化に適しているわけではありません。従来のトレーニングを受けたセキュリティ専門家がクラウド関連の細かい事情を把握するよりも、クラウド専門の開発者がセキュリティ慣行の最新情報を身につける方が負担は少ないと言えます。今日の世界では、オープンソース、IaC（Infrastructure as Code）、クラウドインフラのプロビジョニングに対応するツールは、あらゆるタイプのクラウド環境に欠かせません。

求められる次の一手は？

セキュリティの観点で言うと、クラウドトランスフォーメーションは幅広い規制や契約上の要素を優先しなければなりません。規制については、GDPR（EU一般データ保護規則）、HIPAA（医療保険の相互運用性と説明責任に関する法律）、NIS指令（ネットワークおよび情報システムのセキュリティに関する指令）、PCI DSS（クレジットカード業界の情報セキュリティ基準）など、略語の嵐のような多くの制度があるため、セキュ

> “クラウドやクラウドセキュリティに求められるのは、コードやスクリプトを書き、DevOpsの仕組みを理解している開発者のスキルセットです。これらの心得があるプロフェッショナルにセキュリティの原則を教える方が、セキュリティのプロフェッショナルにコードの書き方を教えるよりも、戦略としては実効性が高いのです。”
>
> **Steve Barlock**
> KPMG米国
> Principal, Cyber Security Services

2 Aqua Security, “2021 Cloud Security Report: Cloud Configuration Risks Exposed.”

リティ関連を中心にコンプライアンスが複雑になっていることが最大の課題と言えるでしょう。

このような環境では、セキュリティチームはCSPM（クラウドセキュリティ態勢管理）の導入も検討項目に加えておくことが重要です。CSPMには、規制や制度ごとにあらかじめ設定済みのポリシーチェック機能が用意されており、クラウド関連の設定ミスやコンプライアンス上のリスクの発見に役立ちます。クリック1つで、設定ミスがないかスキャンして問題点を特定することが可能です。

契約面では、クラウド事業者とユーザー企業は共同責任契約を取り交わしますが、クラウドそのもののセキュリティと、クラウド内部でのセキュリティの責任範囲が曖昧になりがちなため、ユーザー企業側で誤解が生じることが少なくありません。PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）、SaaS（Software as a Service）の解析となると、さらに困難です。ユーザー企業側のセキュリティチームは「クラウド上に格納されているすべてのデータがユーザー企業の責任範囲にある」という事実を社内に周知徹底しておく必要があります。そのうえで、データを（条件が合えば）暗号化し、適切なコントロールセキュリティ対策を講じて保護する必要があります。

CISOやサイバーセキュリティチームには、ビジネスパートナーと協力してクラウド特有のセキュリティ要件を周知徹底し、クラウド事業者側と共同で設定ミスを防ぐことを推奨します。この方法を採用し、絶えず情報収集を心がけていれば、クラウドの運用に成功するはずです。

責任範囲については「引き算」のモデルとして捉えることもできます。IaaSからSaaSへと移行するにつれ、セキュリティ対象領域全体のうち、セキュリティチームの責任は少なくなるからです。どのような契約形態であれ、クラウド化が加速するなか、自動化のツールやプロトコルを中心にクラウド上にある自社データのセキュリティ確保に備える必要があります。

クラウド環境に自社やそのリスクプロファイル、豊富な特徴・機能にふさわしい適正なレベルのセキュリティを確保するため、専任のクラウドセキュリティチームの設置が不可欠です。チームはガバナンスの観点から集権型とし、必要に応じて全社に分散配置します。チームの構成やスキルが確実に固まれば、あとは各事業部に分散させ、歩調を合わせることができます。導入、監視、復旧の領域を重点的に、できる限り自動化を推進していきます。

> “セキュリティ対策を自動化し、全体的なセキュリティ体制を強化するうえで鍵となるのが、セキュリティアーキテクチャとクラウド事業者側の技術やセキュリティのスキルを把握しておくことです。クラウドには自身を保護・復旧する機能はありませんが、ユーザー企業にどのような選択肢やセキュリティ関連の義務があるのかを把握することで、セキュリティ対策を効率的に実装することができます。”

Andreas Tomek
KPMGインターナショナル
Global Cloud Security Leader
KPMGオーストラリア
Partner

2022年に検討すべき主な施策

1. 導入・監視・復旧を中心に、人によるプロセスを排除し、クラウドのセキュリティを自動化する。
2. 集権型のクラウドセキュリティチームを編成し、メンバーには開発系の人材を揃えるとともに、従来のセキュリティのスキルを持った統括役を置く。
3. 責任共有モデルを利用する場合、クラウド事業者とユーザー企業の間で、クラウドのセキュリティにおける責任範囲を明確にする。
4. 数々の規制や制度に対応するポリシーチェック機能があらかじめ設定されたCSPMツールを活用する。
5. 自社の幅広いクラウド戦略に連動するインシデント対応プロセスを構築する。

さらに理解を深めるために

クラウドのセキュリティ確保
クラウド型ソリューションがもたらすビジネス上のメリットと脅威とは？

サイバープラグマティストの強さ
アフターコロナ時代にビジネスを守る新方式を採用。

クラウド上のデータ保護
拡張性に優れたデータ保護体制の実現。

主要課題4

ゼロトラストの中心軸となるID管理

「ハイパーコネクテッド」には、
IAM（ID・アクセス管理）とゼロトラストで対応

リモートワークが普及し、何十億人もの消費者がスマートフォンでいつでもどこでも買い物ができるようになり、サプライヤーやパートナー企業からなる複雑なエコシステムのなかで、機密データの保護はかつてないほど重要になっています。クリック1つでサイバー犯罪者の餌食になることも珍しくない環境では、ゼロトラストの姿勢とアーキテクチャを採用し、その中心軸にIAM（ID・アクセス管理）を据える必要があります。

求められているのはストレスフリー

官民を問わず爆発的なペースで広がるDX。コロナ禍でその動きに拍車がかかり、リモートワークも急速に普及するなか、悪事を企てる者にとって好都合な状況が生まれています。実際、過去に例のない件数のサイバー攻撃が発生しており、特にランサムウェア攻撃やサプライチェーン攻撃が目立ちます。現行のIAMモデルは、もともと1つの組織でIDとアクセス権を管理するために誕生しましたが、今では適正なレベルのレジリエンスを確保するとともに、プライベートクラウド型、パブリッククラウド型、マルチクラウド型を問わず、ゆるやかにつながったデジタル環境に適した重要な認証機能も担う仕組みへと変化しています。

その結果、ユーザー企業はもちろん、その顧客やサプライヤーも含め、度重なるパスワード変更や何段階ものIDの確認といった面倒な手続きをすることなく、ストレスフリーな使い勝手を期待する声が高まっています。現在は「企業の労働力」の定義が広がり、外部のパートナーや請負業者、ギグワーカーを含め、広範なエコシステムが形成されているため、異なる時間帯に異なるレベルの機密データが利用され、これに対応するアクセス権が必要となります。残念ながら、こうしたユーザー構成に対応する専用プロセスがなければ、連鎖状に構築されたセキュリティ体制に重大な侵害が頻繁に生じることになります。

B2C（消費者向け）とB2B（企業間）のセキュリティ境界はますます曖昧になっており、それぞれ別のセキュリティ規律に分ける方式が廃止されつつあります。多くの場合、両者の認証管理の方式は統合される傾向です。セキュリティ技術の成熟に伴い、消費者向けだけでなく、企業向けでも身元確認とパスワードレス認証への移行の動きが広がる可能性があります。企業のサイバーセキュリティ担当者の人数に対して、B2CやB2Bのクライアントの絶対数を考えれば、スケーラビリティの問題が浮上します。

サイバーセキュリティの自動化は、高コストで煩雑な手作業の排除、アタックサーフェス（攻撃対象領域）の縮小、目的に適ったセキュリティポリシー・原則の策定につながり、ゼロトラストセキュリティモデルは、アフターコロナ時代に有望なセキュリティ方式として注目されています。IDを中心軸に据えたゼロトラストであれば、(1) ユーザーが適切に認証されたかどうかの評価、(2) ユーザーに不要なリソースの隔離、(3) アクセス元が信頼できる端末か、盗難にあった端末か、第三者の端末かの判定、(4) アクセス権付与の可否判定、が実現します。

ゼロトラストは、サイバーセキュリティチームがシステムアクセスにかかわる侵害を想定し、ID、端末、データ、コンテクストに基づいてアクセス可否の判断を下すように考え方が変化したことの表れと言えます。ユーザーがアクセスの高速化を求め、クラウドを中心とすることによりアタックサーフェスが拡大しているため、既存のセキュリティソリューションやリソースでは、ネットワーク上を流れるデータを保護するうえで非常に心配な状況にあります。

> ゼロトラストモデルとアーキテクチャは、中心軸にIDを据えない限り、成功しません。導入促進やROI（投資収益率）強化を考慮しつつ、IDを中心軸に据えたゼロトラストのロードマップを策定することが重要です。

Deepak Mathur
KPMG米国
Managing Director,
Cyber Security Services

求められる次の一手は？

アクセスやID管理リスクの増大は、企業の財政的負担、および、事業運営の妨げとなるばかりではなく、強化される規制への対応にも影響します。こうした状況に対処するには、自社のシステムやデータ、インフラのセキュリティ強化につながる新たな戦略、標準、ツールを検討する必要があります。

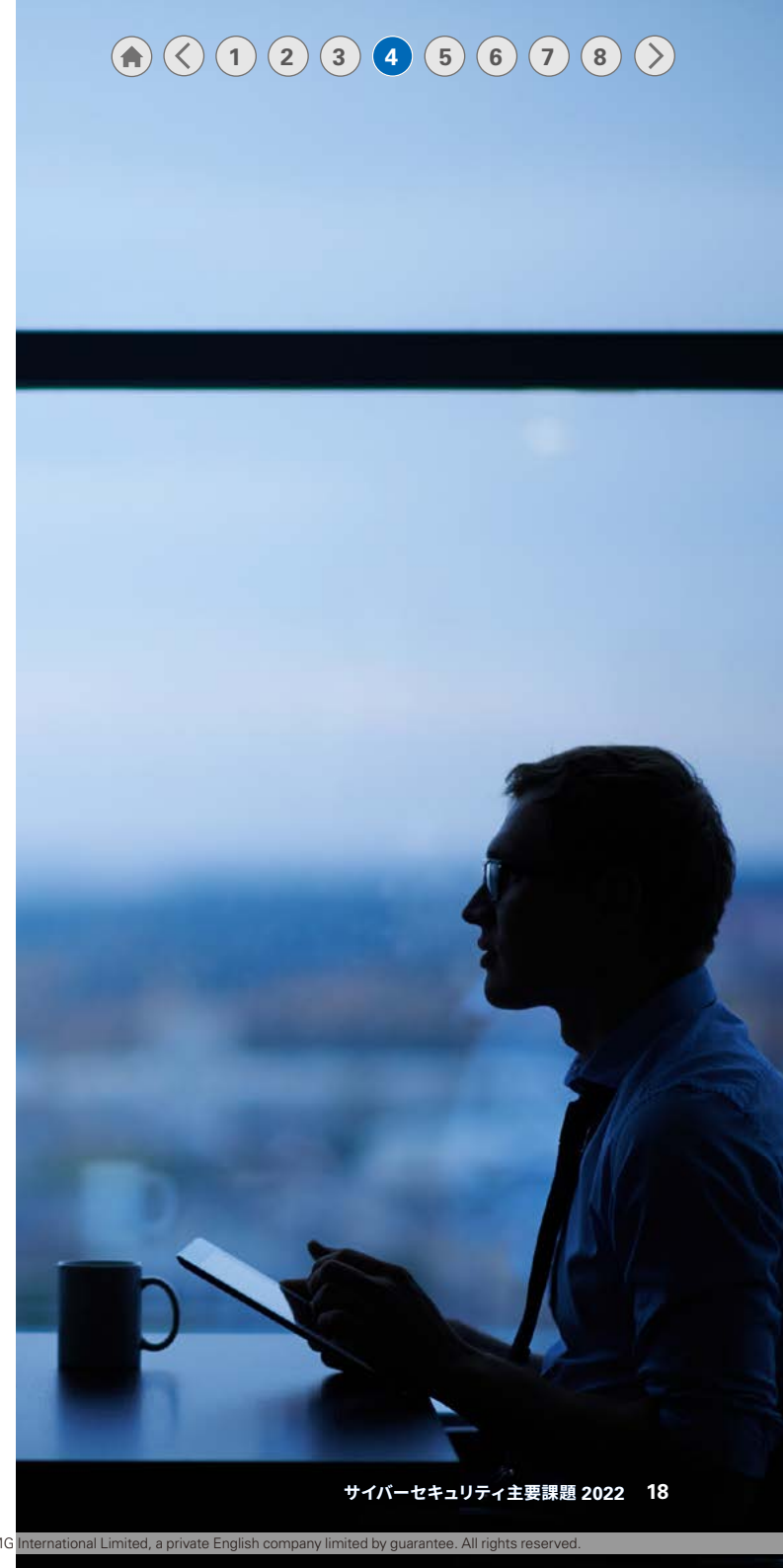
企業や政府機関が絶え間なくサイバー攻撃の脅威にさらされるなか、リモートワークが定着・拡大するアフターコロナのビジネス環境においては、暫定的な対応や応急処置では、こうした攻撃の頻度や悪質さに対応しきれなくなると予想されます。近い将来、リモートで業務するユーザーはVPN接続の必要がなくなります。アクセス権はユーザーが使用する端末、組織が実装する認証プロセスや判定プロセスによって決まる信頼性と確実性に基づき、条件付きになると考えられます。

「ゼロトラスト」という考え方が関心を集めるなか、CISOはもちろん、CIO（最高情報責任者）やインフラ担当責任者も、全社的なゼロトラストのアーキテクチャを最も効果的に実装する方法を検討し、経営や業務の優先課題と整合性のある原則づくりに取り組む必要があります。これらは、組織の全体的なサイバーセキュリティ、リスク管理、技術プログラムの流れのなかで考慮することが大切です。

データ保護の方法に関して、最もシンプルでありながら、同時に最も重要な考え方の1つに「最小権限の原則」があります。これはユーザー、プロセス、ワークロード、アプリケーションがシステムリソースを利用する場合に、それぞれの役割を遂行するために必要最低限のアクセス権のみを付与するものです。たとえば、ウェブデザイナーであれば、財務記録へのアクセス権は不要です。製品リスト更新の担当者であれば、管理者権限は必要ありません。最小権限の原則は今後もゼロトラストモデルの中核的な要素と捉えるべきです。

> ゼロトラストは機能ではなく、テクノロジーでもなければ、標準規格でもありません。IDを中心軸に据えるセキュリティの考え方であり、フレームワークです。”

Jim Wilhelm
KPMGインターナショナル
Global IAM Leader
KPMG米国
Principal



2022年に検討すべき主な施策

1. 一部のユースケースを対象に、パスワードレス認証の実証もしくは導入に着手する。
2. IDプログラムに健全なデータとアナリティクスの基盤が整っていることを確認する。
3. ゼロトラストをサイバーセキュリティの戦略全体に組み込む。
4. 何度も本人確認の必要がない、ストレスの少ない環境を作り、ユーザー・顧客体験の充実に注力する。
5. セキュリティ機能を自動化し、高度なスキルを持つプロフェッショナルがより戦略的な活動に専念できる体制を作る。
6. ゼロトラストモデルの導入は長期にわたる取組みで、実装には時間がかかると覚悟する。

さらに理解を深めるために

認証は未来への扉を開くか
なぜデジタルインフラの
シームレスな認証が必要か。

万人に受け入れられる「ゼロトラスト」
境界の概念を捨てた
サイバーセキュリティ
モデルは、深刻化する
一方の脅威への備えとして
有望なデザインである。

ID・アクセス管理の経済的合理性を追求
IAMに戦略的に取り組み、
自動化と規模適正化を
組み合わせることで、
運用コストを削減する。

主要課題5

セキュリティ自動化の活用

スマートな導入で競争優位を実現

多くの人が「自動化は万能薬」と考えていますが、経験則から言えば、実用主義的な観点でアプリケーションに取り組む方が大きな成果が生まれます。自動化による最大の効果を引き出すには、ビジネス上の課題解決を念頭に、実装することに重点を置くことが重要です。具体的には、日常的な仕事において人間の活動を補完する、スピードが重視される分野でさらなる迅速化を図る、量が多く構造化されていないデータセットを解析する、といった課題が挙げられます。あらゆるものがネットワークに接続されたハイパーコネクテッドワールドでは、数多くのツールが存在し、サイバー攻撃の脅威が拡大と複雑化を続けるため、企業は将来へ備える必要があります。

ビジネスバリューを実現

セキュリティ関連業務における定型的な反復作業を適切に自動化すれば、余ったリソースを他の業務に振り向けることができます。脆弱性スキャン、ログ分析、コンプライアンスなど、これまで専門知識を持つ人材が担っていた業務も標準化が進み、自動処理に移行しつつあります。この結果、セキュリティアナリストの生産性向上、インシデント検知や対応の時間短縮のほか、スケーラビリティも生まれます。司令塔となるSOC（セキュリティオペレーションセンター）の業務では、低レベルの脅威への対応は定型処理の自動化で補完できます。その結果、適正な優先順位に合わせて、人による対応が必要な脅威に素早く対応できるようになります。

データセットが膨大あるいは複雑な場合には、人による分析は困難です。このような状況では自動化の効果が極めて大きいことから、多くの業界で取り組まれており、見逃しかねない関係性やパターンの発見に役立っています。また、自動化は大量のログデータからのセキュリティインシデントの発見や、膨大なデータ検出作業など、スピードが重視される作業において効果を発揮しています。

DevOpsの観点から言えば、ユーザーストーリーやセキュアコードのレビューから、脅威モデリング、静的・動的の両アプリケーションセキュリティテスト（SASTとDAST）を利用したセキュア設計レビューなど、SDLCの工程の重要な節目ごとにセキュリティ自動化を組み込むべきです。クラウドデリバリーの速度に対応できる厳格なセキュリティのニーズの高まりを受け、DevSecOpsに弾みがついています。

クラウドへの移行が進むなか、ソフトウェアのバージョン管理やクラウド環境で利用できる一般的な機能に対して、ユーザー企業側はコントロール権限を有していません。リスクを確実に評価し、必要に応じて新たなベースライン機能を採用する際、自動化は重要な役割を担っています。マルチクラウド環境の場合、意図せぬデータ漏えい、アカウント権限の管理ミス、セキュリティ対策のないネットワーク回線、ランサムウェア攻撃など、さまざまなリスクが懸念されます。自動化されたセキュリティフレームワークであれば、可視化が進み統制も強化されます。

求められる次の一手は？

自動化の導入は「小さな一歩」から始め、自社がビジネスバリューを生み出すうえで必要な領域へと拡大していきます。統合型の全社的なセキュリティアーキテクチャの導入は賢明なやり方ですが、シンプルな状態を保ち、ソリューションが過剰

> “サイバーセキュリティの自動化は、性能の向上とともに、サイバーセキュリティ戦略の重要な要素となっています。自動化の活用により、繰り返しの多い手作業の置き換え、アナリスト向け情報の拡充、複雑なプロセスの遅延短縮、重要資産の保護に求められる規模感とスピード感を追求することが大切です。”

Matthew Miller
KPMG米国
Principal, Cyber Security Services

設計にならないようにする必要があります。多くの企業が最新トレンドに乗り遅れまいと、資金に糸目をつけずにさまざまなツールを買い込んだ挙句、知識のある従業員がおらず「宝の持ち腐れ」になることも少なくありません。

まずは、既存のテクノロジースタックを活かすことが重要です。実際に多くのケースで、すでに導入しているツールに高度な自動化機能があり、新たなツールを導入し直さなくて済む場合があります。また、過去に自動化のプロジェクトに携わったことのある経験者が社内にいないかを調査し、こうした人材をサイバーセキュリティチームに迎えられないかを検討すべきです。サイバーセキュリティの基礎的な知識しか持たない人材にRPA（ロボティック・プロセス・オートメーション）を教えるよりも、他の事業部や過去に在籍した組織でRPAの経験のある人材にサイバーセキュリティへの応用方法を教える方が効率的です。

増加する一方の作業量に、サイバーセキュリティチームは疲弊しています。まずはレベル1（低レベル）のインシデント管理の一部で、自動化のツールをしっかりと使いこなせるようにしていくことが賢い選択です。微妙な勘どころや工夫が必要な場面に遭遇しても、じっくり検討する余裕があるからです。

脆弱性や侵入を検知するために別のセキュリティチームを用意するよりも、セキュリティ自動化でシフトレフトを実現し、ユーザーストーリーやセキュアコードレビューから脅威モデリング、セキュア設計レビューに至るまで、SDLCの重要な節目に自動化を取り入れるべきです。CI／CD（継続的インテグレーション／継続的デリバリー）パイプラインにシームレスに統合できるSAST（静的解析セキュリティテスト）やDAST（動的解析セキュリティテスト）などの製品を使うと、SDLC全体にセキュリティを組み込む際のハードルを下げることができます。

> セキュリティ運用の自動化・効率化を実現するSOAR（Security Orchestration, Automation and Response）など一部のテクノロジーは、基本的に補完役であり、人間のセキュリティアナリストに取って代わるわけではありません。アナリストのスキルやワークフローを補強し、エンドユーザーである従業員の使用感を高めるためのものです。”

Shreyashi Sengupta
KPMGインド
Partner, Digital Trust

2022年に検討すべき主な施策

1. インシデントではなく脅威に重点を置き、セキュリティの自動化に先手を打って取り組む。
2. 日常的な作業を自動化し、人材とコグニティブスキルをより重要な活動に振り分ける。
3. 自社が保有する技術や自動化に精通した社内人材を活かす。
4. SDLCの重要な節目にセキュリティ自動化を組み込む。
5. 実行可能とわかっていることについては、限界に挑み、失敗を恐れず、そこから得た教訓をただちに次に活かす。
6. シンプルであることを重視する。ソリューションの過剰な設計を避け、自動化ツールであっても、問題解決につながらないものや自社のビジネスバリューに寄与しないものは導入しない。

さらに理解を深めるために

自動化は「期待の星」と受け止める
効率化や労働力の面で、数々の期待に沿ったメリットをもたらす。

クラウドDevOpsのアジャイルセキュリティ
セキュリティやソフトウェア開発の未来志向の手法。

ソフトウェア開発パイプラインのセキュリティ監視
開発環境の整合性について信頼を高める最初のステップ。

主要課題6

プライバシー フロンティアの保護

構想・設計段階から
セキュリティとプライバシーに
配慮した部門横断的な手法へ

多くの企業において、サイバーセキュリティとデータプライバシーは異なる分野とされ、しばしばまったく違った部署が対応しています。大量の機密データを保持・利用する環境では、サードパーティ、新たなシステム、新たなアプリケーションのレビューなど、部門横断的な手法でプライバシー侵害のリスクを管理することが求められます。具体的には、設計フェーズから組織変革管理に至るまで、プライバシーとセキュリティの両面でのリスク管理が必要です。

個人の権利を常に優先

個人の権利に対する意識や認識が世界的に高まっています。欧州のGDPRに始まり、アジア、北米・南米のさまざまな制度に至るまで、データの権利、プライバシー、セキュリティが重視されています。とりわけ、LGPD（ブラジルの個人情報保護法）、CCPA（カリフォルニア州消費者プライバシー法）をはじめとする新たな米国州法、カナダで制定が進む連邦法・州法が知られています。

データプライバシーに関する規制環境は、刻一刻と変化しています。政府や規制当局の見解に照らせば、データ漏えいに起因するプライバシーインシデントは、大きな概念であるサイバーインシデントの一部に過ぎません。政府や規制当局は企業に対し、データ漏えいが発生した場合にはプライバシーへの影響の有無にかかわらず、より早い段階で、透明性のある形で開示するよう要求しています。今や世界の大半の法制度で漏えい報告義務が定められ、産業界や管轄外の規制当局も大きな関心を示し同様の義務を定めています。GDPRの登場前は世界中で「間に合わせ」の規則や規制がつぎはぎのようにあるだけでしたが、わずか数年で様変わりしました。

現在は多くの国・地域が個人に裁量権を与え、自己情報コントロール権を個人の手に戻すことを目的に、権利に基づくプライバシーの規則・規制を導入しています。その意味では、ほぼ普遍的に足並みを揃えた動きと言えます。ただ、多種多様な規制が登場した結果、複数の法制度のもとで事業展開するグローバル企業を中心に、事業運営や法令への対応がますます難しい環境になりつつあります。

特に、プライバシーリスクの特定やレポーティングなどの分野を管理する能力やリソースを持たない企業にとって、自動化は重要な鍵となります。たとえば、効果的なメタデータ管理を土台にしたIAMプロセスが自動化されていない企業は、不利な立場に追い込まれることになります。仮想の世界でSAR（個人情報開示請求）処理の自動化など日常プロセスの管理が自動化されていなければ、新たにサーバーやデータストア、アプリケーションを効率的かつ有効に導入するための人員を揃えることは不可能だからです。

> “これからのプライバシープログラムは、構想・設計段階からプライバシー保護に配慮する「プライバシー・バイ・デザイン」の考え方を取り入れなければなりません。これは単なる設計思想ではなく、組織文化としての姿勢であり全社的な変革でもあります。また、プライバシー保護は法務だけで成り立つ話ではなく、プライバシーエンジニアリング、サイバーセキュリティ、テクノロジー、リスク管理などを含め、多面的にデータ保護に取り組む必要があります。”

Sylvia Klasovec Kingsmill
KPMGインターナショナル
Global Privacy Leader
KPMGカナダ
Partner

相手が個人でも法人でも、データを収集する時点か、それに先立って明確な同意を得ることが大切です。特に顧客からは、収集目的と個人情報の使途について理解したという意思表示をもらう必要があります。その都度、十分な透明性を確保することで信頼が醸成され、データマイニングにかかわる倫理上の問題を回避することができます。”

Matthew Quick
KPMGオーストラリア
Director, Technology
Risk and Cyber Security

求められる次の一手は？

個人情報のセキュリティを確保しデータプライバシーを重視するには、単に規制要件に適合するプロセスを導入すればよいというわけではなく、組織文化の変革が不可欠です。セキュリティと同様、「プライバシーファースト」あるいは「プライバシー・バイ・デザイン」の姿勢を取ることが大切です。まず取り組むべきことは、組織変革、組織文化、プロセス、テクノロジー、製品にプライバシーとセキュリティの考え方を反映させることです。これはコストのかかる改修や規制当局による調査に至る事態を回避し、組織内外で信頼を醸成する一助となります。

このような組織文化の変革は、組織のトップが率先するべきです。第一歩として「データは顧客、取引先、パートナーに帰属するものであり、収集・使用にあたっては法的にも倫理的にも自社が責任を負う」と経営幹部が認識を改めなければなりません。そのためには、業務部門、プライバシー担当部署、セキュリティチームの相互補完関係を築くことが求められます。同様に、プライバシーリスクの特定と報告について明確にするだけでなく、規制当局に的確に説明できるだけの結果責任を負い、これを実証するための透明性確保も必要です。

プライバシー影響評価（PIA）やデータ主体によるアクセス要求（DSAR）を始め、プライバシー保護プロセスの実効性ある管理や効率化に取り組むうえで、自動化は重要な役割を担います。その結果、企業が投資してきたガバナンス、リスク、コンプライアンスのテクノロジーを活用できるようになるのです。具体的には、コンテンツ管理やワークフロー管理、リスクアナリティクスといったテクノロジーです。こうしたテクノロジーを活かすことができれば、プライバシーモジュールの運用により、データとアクセス権のマッピングに目に見える効果が生まれます。

自動化は、サイバーセキュリティとプライバシーの各部門の縦割り構造を脱却する糸口にもなります。これら2つは非常に相互補完的な分野であり、足並みを揃えた運用体制を築くことができます。予算面でも多くの企業では、サイバーセキュリティチームが潤沢な予算を持つ一方、プライバシーチームは低予算という状態ですが、両者の予算を一本化すれば額も大きくなります。

たとえば、メタデータとデータをマッピングすれば、サイバーセキュリティチームとプライバシーチームが同じ資産を活用できます。全社的にどのデータにアクセスし、その利用や処理にどのような権限があるのか、両チームが揃って把握しておくことが重要です。そうすれば、ゼロトラストの方針を念頭に両者で協力してセキュリティとプライバシー保護の適切な対策を取ることができます。自動化は核となるデータ資産がある場所や効果的な利用方法について理解を深めることにもつながります。やがて、双方ともに自社の「一番大事なものを守る」という共通の目標を掲げ、共通の財源を活かそうとするようになります。

自動化やAIといった最新のテクノロジーに精通していることが大切なのは言うまでもないですが、セキュリティやプライバシーの観点から言えば、基本原則はほとんど変わっていません。それは、収集するデータの持ち主から同意を得ること、目的に沿ったデータだけを収集すること、必要な期間以上に保持しないこと、不要になった時点で廃棄すること、適切に保護することにほかなりません。

私たちは長年にわたり、例外こそあれ、ヒトの判断や善意に頼ってきました。今、AIの出現で膨大な情報を機械が処理するようになっています。機械は言われた通りに作業をすることにかけては非常に優秀で効率的ですが、倫理観を優先してくれません。消費者のプライバシー権を尊重し、消費者のデータの二次利用について十分に告知する「プライバシー・バイ・デザイン」の一環として、機械の脱線を防いでくれるガードレール（防護策）を導入する必要があります。”

Steven Stein
KPMG米国
Principal, Cyber Security Services

2022年に検討すべき主な施策

1. 個人データ収集になぜ同意が必要か、消費者の権利を尊重しなければ経営にどのような悪影響が生じるのか、経営幹部や業務部門の管理職を対象とした啓発活動が重要となる。
2. 経営幹部と業務部門トップが掲げる優先課題やビジョンと、データプライバシープログラムとの整合性を確保し、収集、同意、利用の各段階ですべての関係者の認識を合わせる。
3. プライバシーに関する規制や規制当局の要求を補足・補完するものとして、プライバシー・バイ・デザインの標準ルールを採用する。
4. 明文化されたポリシーを検証可能なビジネス慣行に落とし込むことで、消費者の権利やデータの保護への取組みについて消費者や規制当局の理解を求める。
5. データプライバシー管理技術ツールを導入し、プロセスの自動化、規制への適合、対応の迅速化、人為ミスの削減に取り組む。

さらに理解を深めるために

プライバシー保護技術：次に来るのは何か
自動化時代における
データプライバシー
保護技術の進化。

試されるバランス感覚：プライバシー、セキュリティ、倫理観
成長促進につながる最適な
データ保護のあり方とは。

データに対する企業の責任：消費者の不信感を払拭できるか
企業が収集する個人データが
増え続け、消費者の間に
懸念が広がっている。
信頼を取り戻すために
企業に何ができるか。

主要課題7

境界を超えたセキュリティ対策

広義のサプライチェーンの
サイバーセキュリティを守るには

事業規模の大小を問わず、企業の間では、デジタル化の推進が依然として優先課題になっています。「デジタルファースト」の企業に変わるには、パートナーやサプライヤーが複雑に絡み合うエコシステム全体で、ほぼ恒常的にデータが共有される「データ中心主義」を取ることになります。外部委託先を含むサードパーティはもちろん、フォースパーティ（再委託先）、フィフスパーティ（再々委託先）といった具合にデータの流れる範囲が広がれば、サイバー攻撃の可能性も高まり、システムやデータが狙われることになります。
では、自社のセキュリティ確保はもちろん、社外に広がるエコシステムのサイバーセキュリティ確保を推進するために、CISOはどのような道を進むべきでしょうか。

エコシステムのセキュリティ：ソリューションと障害の現状

外部の助けなしに何でも内製化できるような一社完結型の企業はほとんどないと言えるでしょう。強力なサプライチェーンのほか、取引業者など多くのパートナーに依存しており、こうした社外のパートナーが業務システムやデータに直接アクセスできる権限を持っていることも少なくありません。サードパーティにかかわるサイバーセキュリティ上の脅威に対し、規制当局が示す基準や関係者間で合意したセキュリティフレームワークがあれば、影響を最小限に抑える一助となります。ただし、クラウド事業者やSaaS事業者、IoT機器メーカーなど、複雑なエコシステムに関係する企業が、パートナーのデータ保護に十分な対策を取る明確な義務を負っていない状況もあり、ネットワーク全体がサイバー攻撃に対して脆弱になっています。

契約交渉の観点から言えば、取引の可能性が見込まれるあらゆる取引先ベンダーの社内セキュリティポリシーや、アクセス対象となる製品・サービスに組み込まれているセキュリティについて、適切に検証する必要があります。そのために、現時点ではエコシステムに参加するパートナーごとにデューデリジェンスが必要ですが、膨大な数に上り、現実的とは言えません。多くの場合、社内かアウトソーシング先が管理するサードパーティセキュリティプログラムを使い、定期的にその時点での状態を人が評価しています。

また、規制産業を中心に、セキュリティ格付け会社を上手に活用するケースも見られます。こうした格付け会社のサービスで、所定の条件に照らしてセキュリティリスクのスコアを算出することにより、人による評価で足りない部分を補強しています。この方法では詳細な定性・定量分析が実施されるため、エコシステムを構成するパートナーのセキュリティ状態が「合格点」か否かの判定に役立ちます。

残念ながら、この方法は絶えず進化を遂げる今日のデジタル環境には歯が立ちません。このような形の信頼検証の枠組みは、ほぼリアルタイムの可視化が可能ですが、多くの企業にとっては時間も費用もかかりすぎるという問題があります。そのため、多くの企業やサードパーティの事業者、場合によっては規制当局までもが、それぞれのエコシステムのセキュリティについて、継続的な保証を強く迫られています。その間にも、サプライヤーのエコシステムが複雑化するにつれ、骨の折れる状況に拍車がかかる一方です。さらに、再委託先であるフォースパーティ、シャドーIT、SaaS事業者の監督欠如の問題も注視されています。決まりを守っているかどうかのコンプライアンス型の戦略に甘んじることなく、より攻めの戦略に軸足を移し、継続的な監視、AIと機械学習を活かしたソリューション、脅威インテリジェンス、ゼロトラストをエコシステムのセキュリティモデルの中心に据えるべきですが、これはCISOにとって難題です。

> “クラウドやデジタルテクノロジーによって複数のパートナーが複雑につながり合うエコシステムが生まれており、これに伴うリスクに先手を打って対処したいという考え方も出てきています。サードパーティ、フォースパーティ、フィフスパーティにまでまたがる環境で適切な対応策を確実に打っていくうえで、今後、自動化が重要な役割を担います。”

Atul Gupta
KPMGインターナショナル
Global Cyber Security Lead for TMT
KPMGインド
Partner

求められる次の一手は？

サイバーセキュリティに関する規制は、サプライチェーンに関する米国大統領令や、改正を重ねるEU（欧州連合）のNIS指令からもわかるように、今後、厳格化と拡大が続く見込みです。NIS指令では、特にアフターコロナ時代を見据え、各加盟国や業界、企業に対し、内向き・外向きのサイバーセキュリティポリシーの強化について明確な条件を示しています。

内向きと外向きの両方をカバーする強力なリスク管理のフレームワークは、特に金融サービス、エネルギー、医療などのハイリスク業界にとって鍵となります。また、世界の主要産業では、広範なエコシステムを構成するあらゆるパートナーがシステムの保護に確実に取り組めるよう、将来性のある方式を適用することが大切です。

もう1つ重視したい分野として、エコシステム全体でのAI／機械学習の活用を含む自動化が挙げられます。セキュリティポリシーにAIと機械学習を活用し、シャドーIT問題への対処やサードパーティのSaaS製品に対する監視強化のほか、チャットボットの導入、サードパーティリスク管理プロセスなどの自動化に役立てることもできます。

この考え方をさらに一歩進めてくれるのがCCM（統制の継続的モニタリング）です。任意の時点で実施するセキュリティアセスメントではすぐに情報鮮度が落ちますが、CCMはこの欠点を克服できる方式をとっています。CCMの評価データは直接コンピュータで処理可能なため、委託先ベンダーのサイクルが促進され、最終的にリスクや統制の監視強化につながります。パートナーのエコシステムでもCCMの効果を発揮させるには、こうした評価方式に委託先ベンダーも巻き込み、受け入れてもらう必要があります。このモデルは、従来のようなコンプライアンスに基づく措置ではなく、運用面に重点を置いており、人の介入の有無にかかわらず、リアルタイムに是正措置を講じる体制に移行することを、エコシステムのパートナー各社に働きかける効果もあります。

継続的な検証体制への移行に伴い、規制当局や大企業にもエコシステムのセキュリティ強化を積極的に推進する「攻め」の姿勢が見られます。相互依存の進んだビジネスの世界では、サプライヤーで構成するエコシステム、とりわけ、同等規模のリソースを持っていないパートナーを守る、という責任感が強まっています。つまり、サプライヤーのエコシステム全体を対象に、監視・脅威インテリジェンスを実施し、脅威が発見された場合にはパートナーと共同で防御策を講じる可能性もあります。最初の段階では、まず規制当局や国家機関がこの方式を採用し始め、大手企業が後に続きます。

> 多くの企業が着目しているのは、評価結果をコンピュータで処理可能なフォーマットで入手できるかどうかです。処理できるのであれば、サイバーセキュリティチームがサードパーティのリスク評価を継続的な統制監視の一環と捉えられるようになります。こうなると、コンプライアンスベースではなく、運用ベースでの姿勢を構築することが可能です。ただ現在、多くの業界で採用されているサードパーティリスクプログラムでは、この移行に対応できていません。

Jonathan Dambrot
KPMGインターナショナル
Global Third Party Security Leader
KPMG米国
Principal

2022年に検討すべき主な施策

1. 規制は絶えず進化し、今後もサプライチェーンのセキュリティに重点が置かれるため、規制要件には常に目を光らせる。
2. コンプライアンス主義から運用に重きを置いたセキュリティにエコシステムを移行するための手段としてCCMを検討する。
3. セキュリティを強化するとともに、スキルの高いセキュリティ人材により戦略的な業務に専念してもらうため、AI／機械学習活用の機会を模索し、サプライチェーンのセキュリティ関連業務を自動化する。
4. 制御システムのサプライチェーンを見落としてはならない。ITとOT（オペレーショナルテクノロジー）のシステムが融合するにつれ、業務データを狙う攻撃者が制御システムの弱点を突く可能性が高まる。
5. リソースが豊富な大手企業は、自社の環境だけでなく、広範なエコシステムまで保護するセキュリティ対策を講じ、能力増強に取り組む必要がある。

さらに理解を深めるために

企業ネットワークが広がる時代、いかに未来を守り抜くか
サードパーティエコシステムのセキュリティ強化に向けた方向性を示す。

変わりゆくサードパーティエコシステム
進化するエコシステムのセキュリティを強化する。

AIを用いたサードパーティリスク管理の効率化
サードパーティセキュリティリスク管理に、AIという名のデジタルワーカーを導入する。

主要課題8

サイバーレジリエンスを巡る議論の見直し

サイバー攻撃への影響を緩和する能力の向上

刻々と変化する今日のデジタル環境では、大規模なサイバーインシデントが発生した場合、潜在的な影響の把握、想定、復旧の備えをいかに的確にこなせるかをあらかじめ検討しておくことがレジリエンスの基本となります。CISOとサイバーセキュリティチームは、経営幹部との対話の場を持ち、自社がサイバー攻撃に耐えられるか、最悪の場合でも数日で復旧可能か、直接、疑問を投げかけてみるとよいでしょう。仮に混乱状態が何週間も続いた場合、マスコミや規制当局、社会の目に対処しつつ、事業を継続するにはどうすべきかについても検証しておく必要があります。

「対応計画は策定済み」

サイバー攻撃が発生した場合の対応について問われると、ほとんどのCEOが「対応計画は策定済み」、「取締役会での優先議題となる」と答えています。経験から言えば、より核心を突いた質問をするべきです。たとえば、「サイバー攻撃で4〜6週間ほど麻痺状態に陥った場合、どういった備えがあるか」、「顧客サービスにはどのような影響が出るか」、「コールセンターや物流センターに影響はありそうか」、「給与の支給に問題はないのか」、「仕入れ先への支払いはどうなるのか」、「自社が機能停止に陥ったら、規制上・法律上の要件は満たせるのか」といった具合です。

レジリエンスのためには、自社の主な業務プロセスと、事業継続のための戦略を見直す必要があります。

現在、ほぼすべての企業において、サイバーセキュリティインシデントが発生する可能性がありますが、被害にあわないための対策だけでなく、インシデントが発生した場合に損害を軽減する対策にも取り組む必要があります。言うまでもなく、攻撃を検知するだけでは不十分で、被害を抑え込むための迅速な行動も大切です。サイバー攻撃のなかには、侵入した内部に数ヵ月にわたり潜伏し、ひそかに起動してシステムに再感染させる悪意のあるコードがあることもわかっています。

近年、ハッカーが重点的に仕掛けているサイバー攻撃として、次の2つのタイプが挙げられます。

- **ランサムウェア攻撃**：明らかに増加傾向にあるインシデントです。攻撃者が企業のシステムに不正侵入してデータを暗号化し、利用できない状態にしたうえで、暗号化を解除する見返りとして法外な身代金を要求するものです。攻撃者がオンラインのバックアップデータを狙うだけでなく、暗号化したデータを外部に公開すると脅して追加の身代金も要求する二重脅迫の手口も確認されています。

- **サプライチェーン攻撃**：重要ソフトウェアの開発ベンダーや極めて広範な大規模ネットワークで、ロジスティクス上の重要な接点を担う企業を標的にした攻撃が増えています。ハッカーの視点から言えば、小規模企業を標的にした方が少ない労力で済むうえに、甚大な被害をもたらすことになります。

こうした攻撃は、手口としては大して洗練されているわけではなく、依然としてフィッシングやパスワードスプレー攻撃、脆弱性スキャンが使われています。その効果は絶大で、今後もこの手の攻撃が増え続けると考えられます。特にランサムウェア攻撃に関しては、身代金の支払いに応じる企業がある限り、しぶとく続くでしょう。

> 企業は、デジタルレジリエンスで積極的な役割を果たす必要があります。たとえば、企業間の依存関係を把握するシナリオシミュレーションや、できることとできないことを見極める計画策定などに取り組む必要があります。そうすれば、総合的な対応が実現します。

Dani Michaux
KPMGアイルランド
Partner, EMA Cyber Security Leader

相互接続、相互依存が深まるデジタルの世界では、数年前の「WannaCry」や2021年に発生した米国のColonial Pipeline社への攻撃など、ランサムウェアを使った攻撃が1度発生すると、経済全体に広く影響が及ぶ恐れがあります。事態を重く見た各国の規制当局が幅広い業界に対し、新たな規則や指令の導入に動き出すことになりました。その典型例と言えるのが、ネットワークや情報のセキュリティに関して高い基準を設定したEUのNIS指令です。改正版として提案されているNIS2指令案では、幅広いデジタルインフラを対象としています。EUのDORA（デジタルオペレーショナルレジリエンス法）など、業界特化型の規制制度も、インシデント対応、脆弱性開示、ペネトレーションテスト（侵入テスト）、暗号化といった領域で義務となる項目を増やしているため、業界の負担が大きくなっています。

求められる次の一手は？

サイバーレジリエンスは、CISOやサイバーセキュリティチームが単独で実現できるものではありません。経営幹部、財務、マーケティング、その他のステークホルダーからの賛同と積極的な支援を得て、全社一丸となって取り組むべきです。欧州を中心に興味深い動きが活発化しています。CISOやCRO（最高リスク管理責任者）、CDO（最高データ責任者）などのさまざまな役職者が「最高デジタルレジリエンス責任者」ともいうべき立場へと進化し、共同セキュリティ、テクノロジーリスク、事業継続といった幅広い優先課題を担うようになっています。

CISOは、セキュリティ侵害のリスクや影響、サイバーレジリエンスの重要性を経営幹部に説明する役割を受け持つ必要があります。その際は、難解な専門用語は避け、脅威の状況、対応を怠った場合の代償、復旧にかかる期間、潜在的な影響について説明することが重要です。

社内のサイバーレジリエンス計画をチェックし、目的に合致しているかの検証を怠ってはいけません。ただし、物理的な世界のレジリエンス、たとえば、大規模災害への対応を前提とした計画は、サイバーセキュリティには当てはまらない可能性があります。レジリエンス計画と言っても、物理的な世界とサイバーの世界とでは大きな違いがいくつかあります。サイバーでは、実際にいつ、何が、どのように起こるか、大きな不確実性を伴います。影響を受ける範囲も特定の地域・拠点に限定されず、多くの場合、全社規模に及びます（しかも往々にして社外にまで波及します）。そして、インシデントが発生したら「IT部門が何とかしてくれるはず」と思われがちです。

サイバーセキュリティインシデントの発生を待たずに、策定した計画を実際に試してみてください。経営幹部を巻き込み、定期的にサイバーセキュリティインシデント対応の演習を実施することが大切です。こうすることで初めて、サイバー攻撃が自社に及ぼす影響や、対応・復旧のための条件や代償を経営幹部に把握してもらえるのです。現実に起こることを完全に再現することはできませんが、組織としての備えが充実すれば、その分だけ、インシデントをうまく乗り切る可能性も高まります。

サイバーセキュリティチームとしては全社的なレジリエンス強化に向け、セキュリティの基本に専念すべきであることに変わりありません。実際、セキュリティインシデントが数多く発生している背景には、標的となった企業が重要資産の特定、強力なパスワードによるアカウント保護、パッチ管理といった簡単な作業をおろそかにしていたことが挙げられます。ただ、目まぐるしく変化する今日のデジタルの世界では、それだけで十分とは言えません。基本的な対策を補完するものとしては、確かな検知能力、迅速な対応・復旧を実現する高度な能力、サイバー攻撃の影響への重点的な対応が挙げられます。

> 喫緊の課題が何かを見極める良い方法があります。5から10の業務プロセスを選定し、財務的な損失、データの破損、業務停止命令の可能性などの観点から、最大のリスクが発生し得る業務プロセスがサプライヤーにどれだけ依存しているかを分析します。これにより、優先すべき課題が明確になり、適切な対策と戦略を立案できるようになるでしょう。”

Wilhelm Dolle
KPMGドイツ
Partner, Head of Cyber Security

2022年に検討すべき主な施策

1. 重要機能が停止した場合にいつまで事業を継続できるか、顧客にどのような影響を及ぼすかを検討する。
2. 重大なサイバーセキュリティインシデントがサプライヤーへの依存にどのような影響を及ぼすのかを分析する。
3. サイバーセキュリティとサイバーレジリエンスのテーマを役員レベルで議論する。
4. 現行のレジリエンス計画がサイバー攻撃対策の目的に適合し、適切な対応措置を講じる内容になっているかを確認する。
5. 事前の想定が誤っていたかもしれないと認める謙虚な姿勢を忘れず、即座に運用可能な代替計画を用意しておく。
6. 定期的に実施する現実的な演習を通じ、経営幹部にはサイバー攻撃発生時の危機管理能力を高め、各自の役割を明確にしてもらう。
7. 基本を重視しつつ、検知能力や迅速な対応・復旧能力への投資も怠らない。
8. 社内に余力や能力がない場合は、しかるべき専門家と共同で取り組む。

さらに理解を深めるために

変貌するランサムウェア
ランサムウェア攻撃に対し、
いかに防御・対応するか。

重要インフラを標的とした
サイバー攻撃への備え
重要インフラを狙った
サイバー攻撃に対し、
いかに備え、対応するか。

ランサムウェアの
「パンデミック」から
OTを保護するには
手口が多様化する
ランサムウェアの実態に迫る。

終わりに

そう遠くない将来

あらゆるものがネットワークにつながったハイパーコネクテッドなスマート社会においては、今後、進化を続ける多種多様な脅威ベクター（攻撃経路）を通じ、サイバーリスクが増大する可能性があります。ビジネス、コミュニケーション、エンターテインメントを支えるテクノロジーの進歩に伴い、新たな危機がもたらされます。本レポートでは、サイバーセキュリティチームの進化やセキュリティ機能の自動化、データプライバシー、エコシステムのセキュリティ強化などのテーマについて考察してきました。
ここからは新たに浮かび上がったセキュリティ上の課題をいくつか取り上げます。いずれも新しいトピックではありませんが、近いうちに、ほぼすべての業界で、サイバーセキュリティの専門家にとって重点分野になると考えられます。

IIoT（Industrial Internet of Things）

IIoT、つまり産業分野向けのIoT（モノのインターネット）は今後も拡大を続け、クラウドにつながった何百万ものセンサーや機器、その他のネットワーク接続端末がサイバー攻撃を仕掛けやすい脆弱な入り口となる恐れがあります。サイバーセキュリティの観点から喫緊の課題と言えるのは、ハイパーコネクテッドシステムに使われるソフトウェアに適切なリスク管理対策が講じられていないことが多い点です。

IIoTが新たな攻撃対象になることは明らかです。メーカー側の優先課題は変化するとはいえ、現時点では、交通量、廃棄物管理、送電などにかかわるセンサーのアーキテクチャの設計には、十分なセキュリティ対策が講じられていない可能性があります。消費電力や重量の制限など端末には数多くの制約があり、セキュリティ対策を組み込む障壁となっているかもしれませんが、インフラのセキュリティは後付けで何とかなるものではありません。

そこで、IIoTを有効にしている機器にセキュリティ対策がどこまで深く組み込まれ、広範なエコシステムでこうした機器がどのように活用されているかに注目することが大切です。企業やスマートシティといった環境にこうした機器を戦略的に展開する場合、人員、ポリシー、手順、テクノロジーという幅広い項目のほか、異常監視、ID管理、ゼロトラストなどの課題も検討します。今後、IIoTは、より広範なソリューションのエコシステムを構成する要素と捉えるべきであり、最終的に極めて重要なセキュリティ体制を支えることになると考えられます。

> 新しいテクノロジーが登場するたびに脅威が拡大し、それが引き金となってサイバーセキュリティ対策に新たなイノベーションが促されます。こういった悪循環は今後も繰り返すしかないのでしょうか。悪循環から抜け出すには、IT、OT、関連のプロセスや手順のあらゆる面で、企業のDNAレベルにセキュリティ意識を刻み込むほかありません。”

Prasad Jayaraman
KPMG米国
Principal, Americas Cyber Security Leader

今日の社会は、暮らしもビジネスも、データ、端末、相互依存関係を特徴とするデジタルな世界で繰り広げられています。意識的か無意識的かは問わず、10年前には考えられなかったほどにテクノロジーに信頼が置かれるようになった結果、セキュリティ、安全、プライバシー、そして倫理観までも、疑問が提起されるようになりました。セキュリティの専門家は、この新しい現実にしっかり向き合って対処しなければなりません。業務部門の責任者には、信頼の置けるテクノロジーやそのレジリエンスがいかに大切か、テクノロジーがどのような形で他人に悪用されてしまうかを想定してもらえるよう、促していかねばなりません。この結果、これまでとは違う有益な視点が生まれますが、現実味のある実用的なアドバイスをすることも忘れてはなりません。

David Ferbrache
KPMGインターナショナル
Global Head of Cyber Futures

5Gネットワーク

5Gネットワークを前提とした新たなアプリケーションで実現する機能には大きな期待が持てます。ただ、このようなソフトウェアベースで接続を実現しているエコシステムは、テクノロジーイノベーションだけでなく、こうした接続を促進する端末のセキュリティも優先的に考慮する必要があります。

5Gネットワークは、高速、大容量、低遅延、全体的な先進性の面で4Gとは根本的に異なります。もちろん、5Gは通信技術として飛躍的な進歩をもたらしますが、これまでとは異なるセキュリティ上の課題も出てくるため、非常に高度なセキュリティアーキテクチャや監視、統制が必要になります。こうした課題のなかには、重要な技術要素やインフラの調達を巡りすでに顕在化しているサプライチェーンの地政学的な緊張を悪化させるものもあります。

信頼への疑念も生じます。5Gの登場を受け、サイバーセキュリティの専門家の間で、ある状況への懸念が高まっています。それは、非常に不安定な接続アーキテクチャを採用した環境で、固有のデジタルIDを持つ端末が何百万台も同時に接続するようなケースです。このような不確定要素が多い状況において、企業は絶えずゼロトラストの姿勢を崩さず、新たに生じた依存度やレジリエンスの問題にも柔軟に適応できる認証アーキテクチャを前提にすべきです。

AI

すでに急成長分野となっているAI、とりわけ機械学習とディープラーニングは、今後も注目が続くトピックと考えられます。

学習機能のあるAIアプリケーションのセキュリティ対策は、従来のシステムのセキュリティ対策とは大幅に異なります。ソフトウェアはトレーニング済みのパラメータの範囲内で動作するのか、無意識の偏見はどの程度発生するのか、機密情報を危険にさらす目的で悪事を企むAIや敵対的なAIによってアプリケーションが操作されることはあるかなど、サイバーセキュリティの専門家としては、AIアプリケーションのトレーニングと設計が実施された運用環境を勘案したうえで、AIアプリケーションの完全性、予測可能性、受容性を検討する必要もあります。この点に関して、CISOやサイバーセキュリティチームは、CTO（最高技術責任者）や配下のデータサイエンスチームと強力なパートナーシップを築くことが求められます。これは、セキュリティの問題としては、新たな領域に位置付けられます。

近い将来、サイバー攻撃を仕掛ける犯罪者は、RPAや機械学習、ディープラーニングを活用する可能性があります。脆弱性や業務環境防衛策に対する調査やテストといった行為は、近いうちにスパムメールの大量送信やメールのセキュリティ侵害と同じくらい簡単に自動化される可能性があります。攻撃者はAIを利用しますが、そこに境界線はありません。短期的には、こうした犯罪者がAIを駆使してサイバー攻撃を産業化し、ますます優位に立とうとするはずです。実はこうした動きはすでに始まっており、今後も続く見込みです。

AIを巡っては、数々の責任問題があります。法的な枠組みが驚くほど未成熟で、規制の動きが多数見られます。サイバーセキュリティの専門家がその影響を認識するには、もう少し時間がかかるかもしれませんが、その間にもサイバー犯罪者はますます大胆に一攫千金のチャンスを狙っているのです。

分析・執筆

サイバーセキュリティ主要課題事務局

Alissa Bernhardt
Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Paula Reis
Michael Thayer

執筆協力

KPMG米国
Steve Barlock

KPMG米国
Jonathan Dambrot

KPMGドイツ
Wilhelm Dolle

KPMGインターナショナル
David Ferbrache

KPMGインド
Atul Gupta

KPMG米国
Prasad Jayaraman

KPMGカナダ
Sylvia Klasovec Kingsmill

KPMG米国
Deepak Mathur

KPMGアイルランド
Dani Michaux

KPMG米国
Matthew Miller

KPMGオーストラリア
Matt O' Keefe

KPMG米国
Rik Parker

KPMGオーストラリア
Matthew Quick

KPMG米国
Fred Rica

KPMGインド
Shreyashi Sengupta

KPMG米国
Steven Stein

KPMGオーストリア
Andreas Tomek

KPMGインド
Akhilesh Tuteja

KPMG米国
Jim Wilhelm

お問合せ先

KPMGコンサルティング株式会社
T : 03-3548-5111
E : kc@jp.kpmg.com

home.kpmg/jp/kc

本レポートで紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、
提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。
詳しくはKPMGコンサルティング株式会社までお問い合わせください。

home.kpmg/jp/socialmedia

Publication name: Cyber security considerations 2022 | Publication number: 137803-G | Publication date: November 2021