セキュリティリスクの拡大

巧妙化したランサムウェアやAIを駆使した標的型攻撃などにより、重要インフラを中心としたセキュリティリスクは今以上に拡大している。経営層によるビジネス主導のセキュリティ対策が行われている企業では、インターネット分離※1やCSIRT※2活動が行われている。セキュリティ専門人材の不足は解消されず、IT部門はITベンダーと協力して対策を進めている。その一方で簡易な防御に留まっている企業も残っており、二極化が進んでいる。

背景と現在の状況

世界規模でランサムウェアが猛威をふるっている。米国の医療機関などがランサムウェアの攻撃を受け、業務継続を最優先するため身代金を支払う事例が報道されている。国内でも2016年のランサムウェアによる被害件数は2015年の約7倍に急増、重要インフラを中心としたセキュリティリスクが増加している。外部からの攻撃だけでなく、社員や協力企業の要員による内部からの情報漏洩事故を受け、監視や防止の仕組み作りが急がれている。

企業でのクラウドやコンシューマITなどの活用は拡大し、これらを考慮したセキュリティポリシーの作成や対策の実施などが急がれている。IoTの普及により、各種センサーなどの数や種類が増え、潜在的なサイバーリスクも増加し、物理インフラとネットワークインフラの統合セキュリティが必要となっている。

世界中で頻発するセキュリティ事故を受け、企業の経営者はセキュリティリスクを経営リスクと捉え始めている。

※1　基幹系業務のネットワークとインターネット接続を行うネットワークを分離するセキュリティ対策
※2　CSIRT：Computer Security Incident Response Team

3～5年後の姿

セキュリティリスクが拡大する一方で、セキュリティ専門人材の不足は解消されていない。大規模なセキュリティ事故をきっかけとして、IT部門はITベンダーと共に対応に追われている。その一方で簡易な防御に留まっている企業もまだ残っており、二極化が進んでいる。

セキュリティリスク拡大への対応

巧妙化したランサムウェアやAIを駆使した標的型攻撃、アンダーグラウンドで取引される攻撃ツールの充実、RaaS※3の多様化などにより、重要インフラを中心としたセキュリティリスクは今以上に拡大している。大規模なセキュリティ事故をきっかけとして、セキュリティに敏感な企業が積極的に継続的な対策を実施している一方で、従来通りの簡易な防御のみ行っている企業もまだ残っており、セキュリティ対策レベルの二極化が進んでいる。

重要インフラを持つ企業は、インターネット分離やAIを搭載したセキュリティ製品による多層防御などのセキュリティ対策を実施し始めている。100%の防御は不可能であり、防御中心から検知/防御/復旧への重心の移動が必要との認識は、IT部門はもちろん、経営層や事業部門にも広がっている。セキュリティに敏感な経営層は、セキュリティ対策はコストではなく投資であると認識を切り替え、費用対効果を意識している。また、そのような経営層は、企業経営に影響を与えるセキュリティリスクをビジネス視点で可視化にすることをIT部門に求めている。可視化を行うためには、可視化プロセスのセキュリティポリシーへの組み込み、情報資産の棚卸し、事業継続のための優先順位付けなどをビジネス部門とIT部門が共同で取り組む必要があり、先進的な企業で進められている。

防御と事後対応の仕組み作り

重要なシステムを物理的にインターネットから分離すると安全性が高くなる。しかし、コストや利便性の観点から踏み切る企業は少ない。そのため、論理的なインターネットからの分離が進んでいる。当初は、自治体や重要インフラを扱う企業から始まったが、中堅企業でもセキュリティに敏感な企業は必要性を認識して分離が進んでいる。

多くの企業はCSIRTを立ち上げている。しかし、インシデントを防止/検知/解決するためのプロセスが定義され、承認/監査されている企業は現在よりも増加しているものの、3～5年後はまだ半数に満たない。CSIRTを立ち上げていない企業や、形だけの体制に留まっている企業がある。その一方で、セキュリティに関する多数の情報を集め、新たな知見を導き出す脅威インテリジェンスを活用して、実効性を伴ったCSIRTが活動している企業もある。

※3　RaaS：Ransomware as a Service

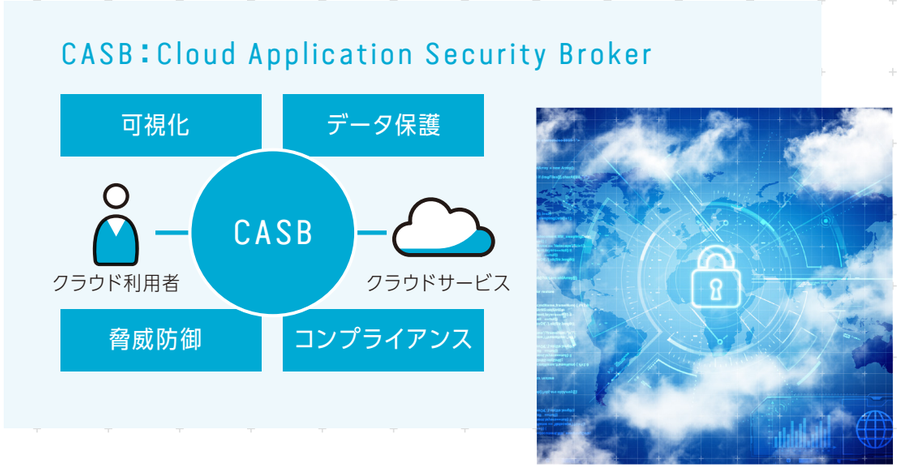
パブリッククラウドの安全な活用の広がり

オンプレミスより複数のセキュリティ標準の認証を受けているパブリッククラウドの方が、セキュアなシステムの構築/運用が可能であるとの考えが定着したことで、パブリッククラウドは業務を遂行するために不可欠になっている。

企業の多くは、オンプレミスの基幹系システムとパブリッククラウドの周辺システムのハイブリッドクラウド構成になっている。そのため、ID管理や認証システムをクラウドでサービス提供するIDaaS※4や、SECaaS※5と呼ばれるセキュリティ機能のクラウドサービス活用が増えている。システムのクラウド化の進行に伴い、セキュリティもクラウドサービス事業者に依存することが自然の流れとなり、多くのITベンダーがセキュリティ機能をクラウドサービスとして提供するという流れを加速させている。

IT部門に頼らず独自にSaaSなどパブリッククラウドの利用を始めている事業部門が増え、誰がなんのサービスを使っているのか把握できていない企業が出ている。そのため、CASB※6を経由してパブリッククラウドを利用させている。CASBとは、認証/アクセス制御/データ暗号化/ログ取得などを行い、セキュリティポリシーを適用することが可能なサービスである。CASBを利用して、パブリッククラウドの利用状況の可視化やデータ流出の防止などを実現している企業が増加している。

これらのパブリッククラウドの安全な活用の仕組み作りを行っている企業がある一方で、無秩序なシャドーITが蔓延している企業もある。



※4　IDaaS：Identity as a Service
※5　SECaaS：Security as a Service
※6　CASB：Cloud Application Security Broker

セキュリティ専門人材不足

セキュリティ対策は一過性ではなく、継続的に行わなければならないとの認識が広がり、経営層がセキュリティはコストではなく投資であると認識を切り替えつつも、予算獲得が困難な企業はまだ多い。セキュリティ人材に求められるスキルの特殊性や費用対効果を示せないため、企業内のセキュリティ専門人材育成の優先度は低いままである。この人材に投資できるかが中長期の企業セキュリティ戦略の推進に大きな影響をもたらしている。

IT駆動型ビジネスを実現するために、DevOpsを実施している企業が増えている。さらに、セキュリティチームが加わり、継続的な開発サイクルの中にセキュリティ対策を入れ込んでいくDevSecOpsを推進している企業が登場している。開発チームと運用チームとの連携を密にしてセキュリティ対策を行ったシステムを作り上げることができる、新たな人材が必要になっている。

セキュリティ対応の高度化と複雑化から、多層化されたセキュリティ対応を行うことが求められるが、情報システム部門が自営することは限界を迎えている。そのため、セキュリティオペレーションセンターやマネージドセキュリティサービスが活用されている。

IoTの普及に対応する新たなセキュリティ対策

IoTが普及して様々なモノがネットワークに接続され、保護対象の管理が困難になり、これらのシステムへのハッキングが行われ被害が発生している。逆にそれらのモノが侵入され踏み台となり、加害者となるケースも今まで以上に高まっている。IoTシステムは従来のセキュリティ対策では対応が困難であり、デバイスとエッジサーバ間の通信の認証/暗号化/盗聴と改ざん防止の仕組み作りや、基幹系システムのネットワークとIoT系のネットワークを分離したオーバレイネットワークの構築などが行われている。

また、監視カメラ画像の顔やSNSなどのパーソナルデータの利活用とプライバシー保護の両立のため、匿名加工技術と匿名加工情報の利活用の仕組み作りが行われている。

量子コンピューターによる公開鍵暗号方式破綻の懸念拡大

暗号アルゴリズムの多くは、大きな数の素因数分解を行うことが現在のコンピューターでは非常に長い時間を必要とすることで確立している。量子コンピューターの実用化が期待されるようになり、それに伴い現在使用されている公開鍵暗号方式が破綻する懸念が拡大している。公開鍵暗号方式は電子メールや銀行の取引、医療記録など社会のあらゆるところで使われているため、それが破られると社会生活が崩壊する可能性がある。そのため、量子コンピューターでも破ることができない暗号の研究が行われ、次世代暗号技術を模索している。