つながる世界のITとデータを守り、イノベーションを加速

FUJITSU JOURNAL / 2018年1月5日

IoT機器の普及やITとOT（Operational Technology）の融合など、企業におけるデジタル革新の進展によって、サイバー攻撃への対応を含むセキュリティ対策の重要性がますます増しています。十分なセキュリティ対策を講じ、つながる世界におけるモノと流通するデータを守ることで初めてイノベーションを加速することができます。この難しい課題にどのように取り組むのか、富士通のセキュリティ戦略をお伝えします。
【Fujitsu Insight 2017 「セキュリティ」基調講演レポート】

依然として増加・巧妙化するサイバー攻撃

富士通株式会社
サイバーセキュリティ事業戦略本部 本部長
飯島 淳一

あらためて強調するまでもなく、セキュリティを取り巻く環境は課題が山積みであり、サイバー攻撃はますます増加、巧妙化しています。企業の4割がサイバー攻撃によって重大な被害を受け、機会損失なども含む平均被害額は1件当たり2億3000万円にも上ると言われています。また攻撃手法の巧妙化は、ランサムウェアやゼロデイ攻撃、脆弱なIoT機器を悪用した大規模DDoS攻撃など、予断を許さない状況です。今後、デジタル化が進展し、あらゆるものがつながればつながるほど、サイバー攻撃によるリスクはさらに高まります。

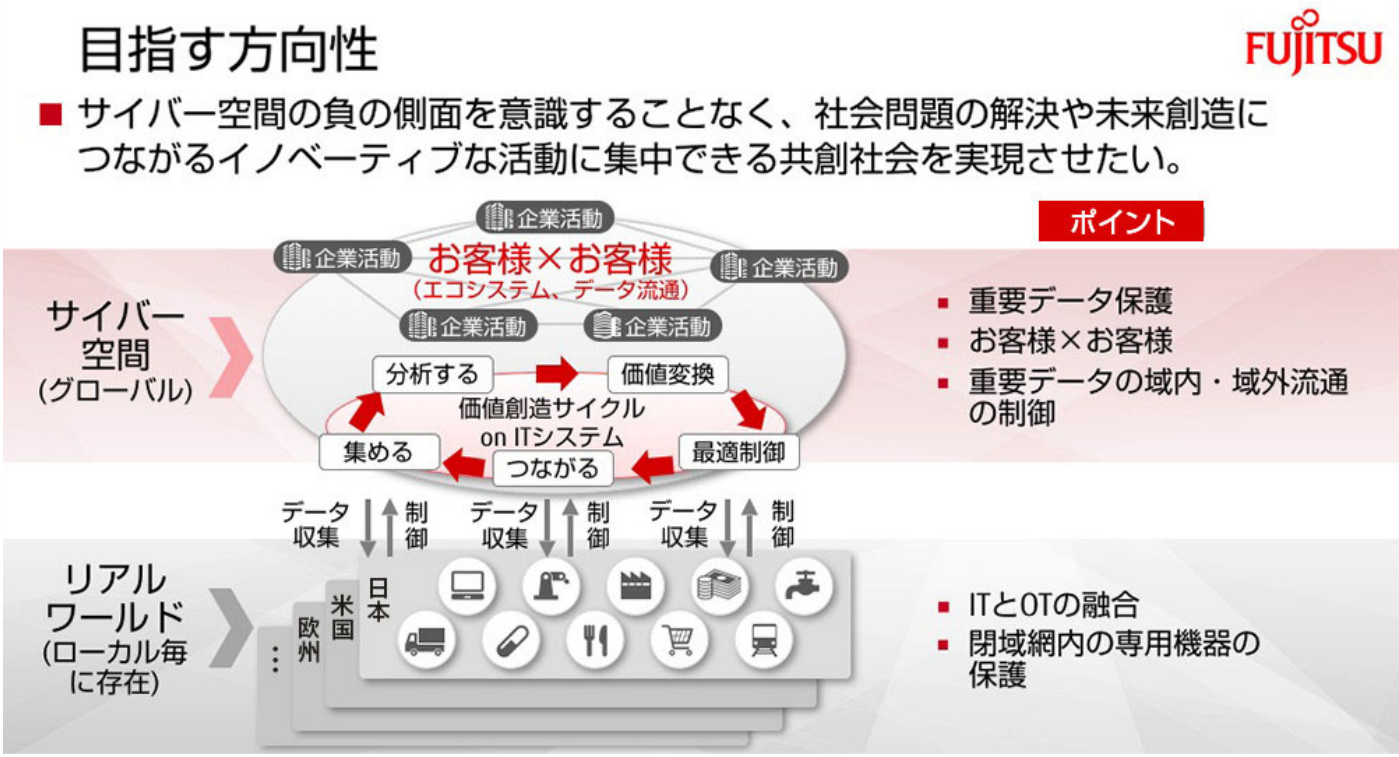
サイバーセキュリティの必要性が高まる中、セキュリティ人材の確保も喫緊の課題です。経済産業省は、2020年までに不足するセキュリティ人材は約20万人と試算していますが、その一方で、企業が導入しているセキュリティ機器は平均6～7製品に上り、十分に運用が回せる状況ではありません。そのためセンサーがアラートを出しても、10～15%は見逃されている恐れがあります。組織内に脅威が侵入してから検出できるまでにかかる時間はグローバル平均で99日間に対して、攻撃者は3日もあれば管理者権限が奪取可能と言われており、このギャップをいかに埋めるかが喫緊の課題です。

セキュリティベンダーに求められること

こうした背景から、セキュリティベンダーには、脅威侵入から検知・復旧までの時間短縮や過剰なアラートへの対応、セキュリティ人材の育成・活用など、様々なチャレンジへの取り組みが求められています。またIoT/OT分野やデータ保護の領域にもセキュリティ対策の範囲を広げることで、お客様の事業を継続するためのトータルなセキュリティリスクマネジメントに貢献していくことも重要な役割と考えています。

ただ、富士通は、脅威から守ることだけがセキュリティではないと考えています。セキュリティ技術はお客様の事業継続を支え、ひいては、ICTを活用した価値創造サイクルを回していく上で不可欠な要素です。

そこで、お客様の事業にセキュリティを組み込むことにより、お客様が「これまでできなかったことを実現する」「いままでにないユーザー体験を実現する」ということを支えていきたいと考えています。つまり、お客様がサイバー攻撃というサイバー空間の負の側面を意識することなく、社会問題の解決や未来創造につながるイノベーティブな活動に集中できる環境の提供を通じて、「共創社会」を実現することが富士通が目指すビジョンです。



お客様を守るための2つの方向性

富士通は、ポリシーの立案から対策の導入、運用に至るまで幅広くカバーするセキュリティソリューションを「SafetyValue」というブランドで提供しています。これを発展させ、セキュリティ対策の切り口ごとの推奨パターンを、他社製品も取り入れた「SafetyValueソリューションセット」という形で提案し、「何を選択したら良いか分からない」というお客様の悩みに応えたいと考えています。

またトータルにお客様を守るために、「仲間を増やす」「範囲を広げる」という2つの方向性で取り組みを進めていきます。

「仲間を増やす」という観点では、富士通グループのシステムエンジニアに、システムの要件定義や設計といった上流からセキュリティを組み込む「セキュリティバイデザイン」の考え方を浸透させ、さらにシステム構築時のテンプレートを用意することで、従来よりも短期間で高品質、高セキュアなインテグレーションを実現していきます。同時に、クラウドサービスやネットワークサービスへのセキュリティ機能の組み込みや、パートナー企業とともにより幅広いお客様へセキュリティサービスを提供するといったことも始めています。

これまでは、ITインフラを守ることを中心にソリューションを提供してきました。それに加えて、「範囲を広げる」という観点から、IoT/OT分野や重要データの保護まで領域を拡大していきたいと考えています。

IoT/OT分野に関しては、Industrial Internet Consortiumが提唱する「Trustworthiness」（信頼性）という概念の実現を目指しています。アセスメントや方針策定といった上流工程から、デバイス認証やホワイトリストなどの機能も含めた設計・実装。さらに運用・保守段階における定期的なペネトレーションテストといったソリューションをライフサイクル全体に渡り提供します。そして日々の運用を支えるマネージドセキュリティサービスのIoT/OT分野への対応を図ります。万が一の際にも早急な復旧を可能にするレジリエンシーや重要データのプライバシーの確保も実現していきます。

さらにデータを守るために、欧州のGDPRをはじめとする法規制や業界標準に対応するためにITの側面で対応すべき事柄が多くあります。Data Protection Officer（DPO）の任命をはじめとする体制・ガバナンス面の整備に始まり、個人データの洗い出しやプライバシー影響度調査の実施、事故発生時のタイムリーな報告といった要求事項に対応するための支援を行います。

富士通が提供するセキュリティのポイントは、アセスメントから設計・構築、運用までをワンストップで対応できることです。アセスメント結果をプロダクト選定やシステムインテグレーションに結び付け、必要に応じてインフラ構成の見直しを行い、システムのセキュリティ強化につなげていきます。こうして改善したシステムをマネージドセキュリティサービスで監視させて頂き、インシデントへの対処を行い、定期的にセキュリティ対策レベルを評価する、といったライフサイクル全体を通したセキュリティ対策をご提供します。

IoT/OT分野への対応も視野にグローバルでマネジメント

サイバー空間に国境はありません。したがって富士通では、様々なセキュリティ課題に対応するソリューションおよびこれらの運用をサポートするマネージドセキュリティサービス「グローバ

ルマネージドセキュリティサービス（GMSS）」をグローバルに展開し、お客様のセキュリティ対策をトータルに支援しています。すでに世界各地にSecurity Operation Center（SOC）やサポート拠点を構築しており、約1,400社のお客様にサービスを提供しています。監視しているネットワークセンサーは約6,400台、エンドポイント数は19万3000台という規模です。

また、世界各地のお客様拠点に導入済みのセンサーを一箇所で集中監視する方法だけでなく、日米欧のSOCから最寄りのお客様拠点を監視・サポートする方法、お客様自身が構築・運用しているSOCに富士通のテクノロジーを導入していただき技術的なサポートのみ提供する方法など、お客様の状況やニーズに合わせた多様な形でサービスを提供することができます。

今後はさらに拡張し、EDR （Endpoint Detection and Response）やUEBA（User Entity Behavior Analytics）も含めて、お客様の環境に置かれたセンサーからイベントやログを収集し、AI技術等を活用して解析・可視化し、外部インテリジェンス情報も活用しながらGMSS を進化させていきます。この中で、先に述べたIoT/OT分野やデータ保護といった領域にも管理対象を広げて行く計画です。また脅威情報やインシデント対応状況をお客様と共有できるマネジメントダッシュボードを通じて、お客様CSIRTとの連携やサポートも深めていきます。

「人材不足」を補う新技術開発と実践的な人材育成で貢献

富士通はメーカーとして様々な分野の研究開発に取り組み、セキュリティ分野でも先端技術の研究開発とその活用に注力しています。それらは当社の社内環境で実際に試し、効果や運用性を検証した上で製品やサービスに組み込む形で、お客様にお届けしています。

独自技術を社内実践し実用化

その1つが、ネットワークトラフィックを攻撃者の行動特徴と照らし合わせることで未知の攻撃を発見する「Malicious Intrusion Process Scan」です。実際に一定水準のセキュリティ対策を施した数万台規模の環境に導入したところ、1カ月で300件を超える未知の攻撃を発見する実績を上げています。また、Active Directoryとプロキシサーバのログを解析して、通常のセキュリティセンサーでは発見が難しい特権IDへの昇格等の振る舞いを検出する「Advanced Analysis技術」。イントラネットを流れるエンドポイント同士の通信を解析し、侵害調査にかかる時間を大幅に短縮する「高速フォレンジック技術」といった独自技術を実用化することで、より付加価値の高いサービスの提供につなげています。

今後は、AI技術の適用を進め、検知したイベントが管理者による正規の作業なのか、あるいは攻撃者による不正な動きなのかという判断精度の向上を図っていきます。このような取り組みにより、高度な分析技術を持たないエンジニアでも適切な判断ができるようになりますので、セキュリティ人材の不足という社会問題に対しても貢献できると考えています。

2,700名を超した富士通のセキュリティ人材

技術開発と同時に力を入れているのが人材育成です。富士通は、3年前に「セキュリティマイスター認定制度」を立ち上げ、すでに富士通グループ全体で2,700名以上の「マイスター」を育成・認定しています。これを2019年度末までに1万人規模に増やし、各SIプロジェクトには必ずマイスターが加わることで、これまで以上にセキュアなシステムをお客様に提供できるようにしていく方針です。また、マイスターを育成するために自社開発した「サイバーレンジ」をお客様にも提供することで、お客様組織におけるセキュリティ人材育成にも貢献していきたいと考えています。

セキュリティ対策はコストではなく投資と考え、経営者が自らリーダーシップをとって進めるべき経営課題です。また、法令対応や業界標準への対応ができなければ、市場参入すらできなくなる重要な課題でもあります。富士通はお客様の様々なニーズや課題にお応えするサービスを揃えることで、お客様の事業継続性を高めるだけでなく、イノベーションの創出にも貢献して参ります。

登壇者

富士通株式会社
サイバーセキュリティ事業戦略本部
本部長
飯島 淳一

FUJITSU JOURNAL / 2018年1月5日