DX推進を支えるセキュリティ対策
～拡大するセキュリティ格差を勝ち抜くには

七宮　弘将

2010年　入社
ビジネスコンサルティング本部
テクノロジーストラテジー&
アドバイザリーグループ
プリンシパル・ディレクター

和知　恭平

2017年　入社
ビジネスコンサルティング本部
テクノロジーストラテジー&
アドバイザリーグループ
プリンシパル・ディレクター

2023年、国内金融業界においてサイバー攻撃による被害が急増。各企業は可及的速やかな対応が求められている。一方で、IT部門はDXの推進も同時並行的に進める必要がある。

このようなジレンマを抱える中、グローバルでは双方を推進する勝ち組企業とそうでない企業とのセキュリティ格差が広がりつつあり、国内金融でも今後同様の格差が生じ得ることが予想される。

本稿では、ゼロトラストセキュリティの具体的な内容だけでなく、被害にあった場合を想定した事前の備えについてもご紹介したい。

1. 拡大する攻撃への対応とDXのジレンマ

金融業界へのサイバー攻撃は急増している。警察庁・金融庁によると、2023年度のサイバー攻撃によるインターネットバンキングの不正送金が5,147件、被害額80億円を超え、約5倍に増加している(図表1)。Akamai社の調査では、グローバルの金融サービスにおけるWebやAPIへの攻撃は約90億件(65%増)に達し、DDoS攻撃が最多となった(図表2)。

そのような状況下、新たな技術活用に伴うリスクが増大する懸念もある。昨年から爆発的に利用が進んでいる生成AIもその一例だ。グローバル企業のCEOに生成AIがセキュリティの分野でどのような変化をもたらすのかのアンケートを行った結果、55.9%が味方ではなく敵(脅威)に成り得ると答えている。

一方、金融業界のDX推進は待ったなしの状況である。生成AI含むクラウドサービスの利用拡大、非金融との協業による新サービス創造の過熱化や外部連携強化等のアジェンダに向き合っていく必要がある。“サイバー攻撃の拡大“と”DX推進“、まさにジレンマに直面している。

2. セキュリティ対策の強化こそがDX推進のイネーブラー

グローバルでは、セキュリティ強化を進めている企業こそが、最新テクノロジーを活用して収益性を伸ばしている。

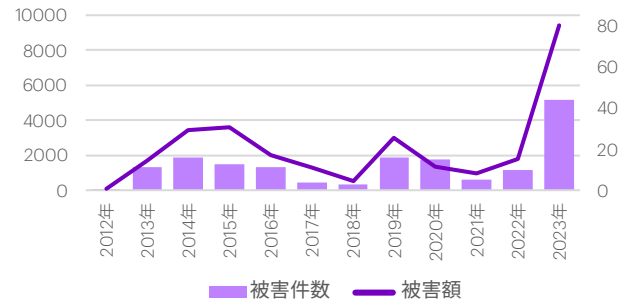
図表3は、グローバル企業に対してセキュリティ強化の取り組みが十分か否かを調査した結果である。高収益企業では「自社のセキュリティ対策は要求レベル以上」という回答が近年格段に増えていることがわかる。弊社調査においても、強力なセキュリティ対応を実現している企業は、そうでない企業に比べ、より効果的なDXを実現する可能性が約6倍高いという結果も出ている。セキュリティ対策の強化こそが、安心してDXを推進するためのイネーブラーとなっていることが伺える。

では、取るべきセキュリティ施策とは何か。それは、「脅威を完全排除する」という考え方の限界を踏まえ、リスクとの共存を前提とし、リスクに応じ動的な対策を実現するゼロトラストセキュリティの体現である。

3. ゼロトラストに求められる対応

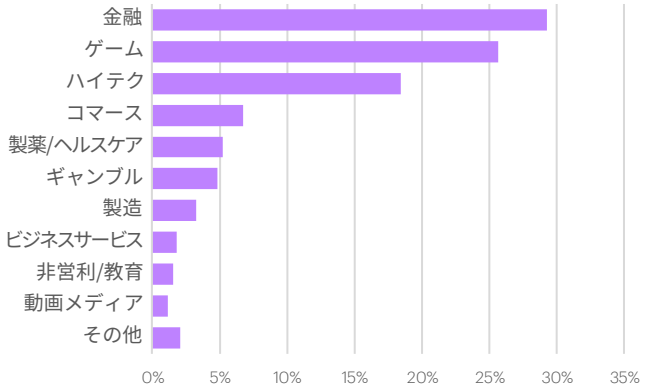
ゼロトラストの概念は、企業内外の間に壁を設け脅威を排除するという従来の「境界型セキュリティ」の考え方に留まらず、侵入されることを前提に、通信・アクセスを動的に検証、制御、管理、監視する考え方である(図表4)。

図表1． 不正送金発生状況



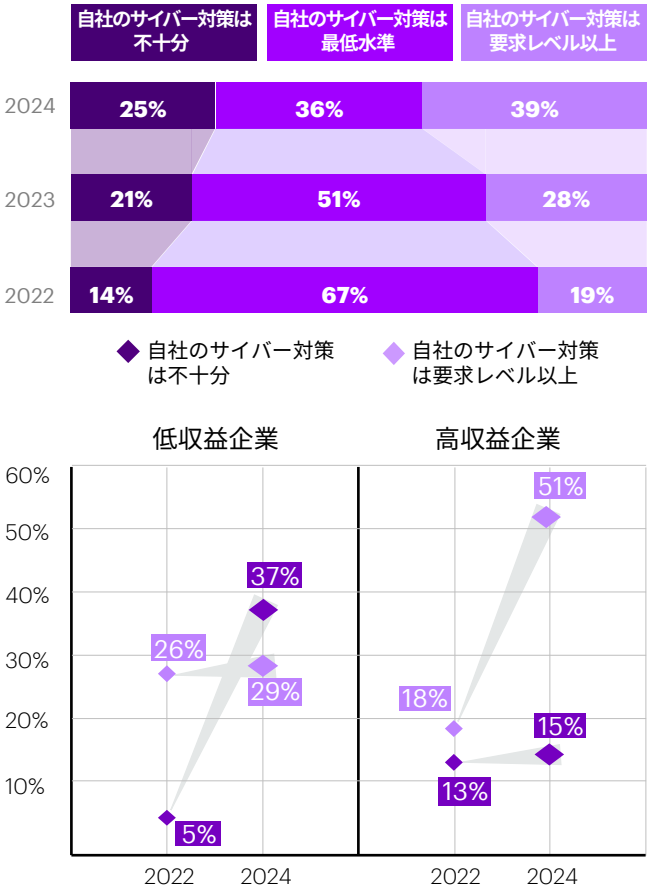
(出典) フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）警察庁、金融庁

図表2． 業界別DDoS攻撃割合



(出典)イノベーションに潜む高いリスク 金融サービス業界の攻撃トレンドAkamai

図表3． グローバル企業のサイバー対策と収益性の関係



本稿では、検討に苦慮するケースが多いEntityとResourceに関し、対応事項を具体例として説明する。

Entity - User

各リソースへのアクセスは“必要最低限”のみ許可する考え方が大前提となる。その上で、各アクセスのリスクを評価し、リスクに応じた制御を行うことが必要である。不正アクセスの可能性が高い場合は、多要素認証の要求やアクセス自体のブロックなど、アクセス試行の振舞いや接続元などをもとに算出したリスクに応じた制御を行う認証基盤を整備すべきである。

Entity - Device

セキュリティポリシーやパッチの強制適用、振る舞い検知型セキュリティソフトによる異常検知、異常時の隔離対応等が可能な端末管理基盤を整備する必要がある。また、ポリシー非準拠端末からのアクセスは接続を拒否するなど、動的なアクセス制御にも活用すべきである。

Entity - Network

「境界型」セキュリティにおいては、境界内は自由に通信が可能なケースが散見されるが、ゼロトラストにおいては、あらゆる通信において必要最低限のみ許可するよう制限すべく、マイクロセグメンテーション化が不可欠である。マイクロセグメンテーションツールの活用を検討されたい。

Resource - Application

インフラからアプリに至る全レイヤにおいて、脆弱性スキャンやペネトレーションテスト等を通じた脆弱性の可視化、可及的速やかな対応を行う管理基盤・プロセス整備が必須である。加えて、アプリケーションを構成するあらゆる通信を暗号化することも徹底すべきである。

Resource - Data

機密度に応じた分類を行い、分類ごとに暗号化を必須とするか否か等の保護レベル定義が必要である。例えば、マイクロソフトオフィス(Word, Excel等)では、保護レベルのラベリングやファイル単位でのアクセス制御が可能なので、当該機能の導入も積極的に検討すべきである。

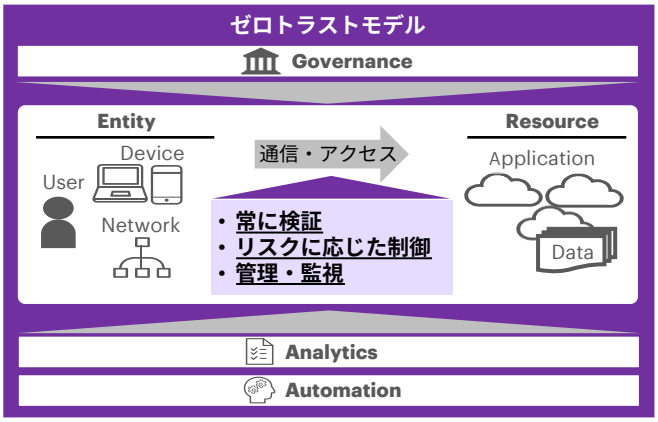
4. 事業インパクトに応じた対応推進と被害時の備え

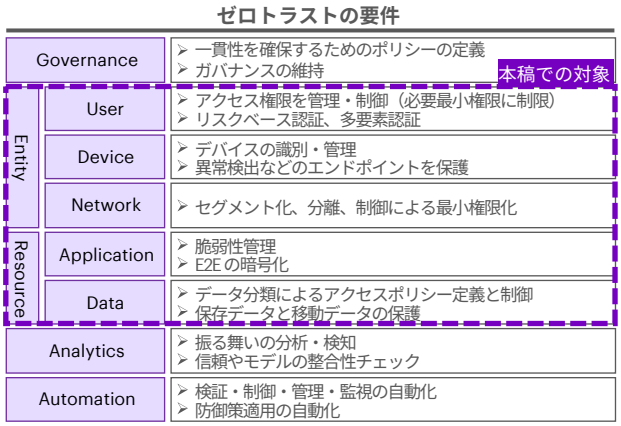
ここまでゼロトラストの対応例を述べたが、どこまでいっても絶対防御というものはない。そのため、“被害時の備え”も重要である。

影響・リスク分析

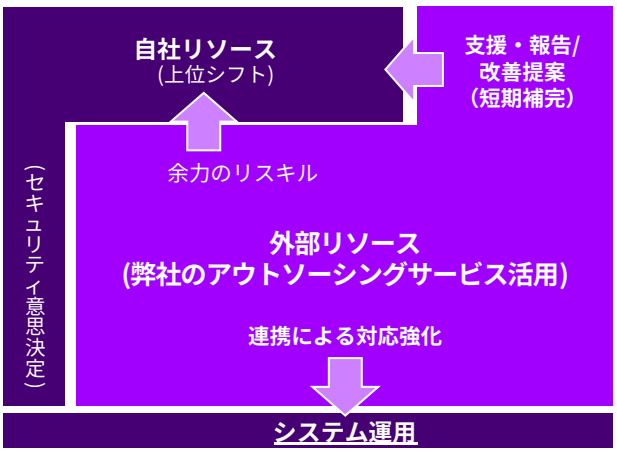
セキュリティインシデントが発生してから事業へのインパクトを確認するのでは遅きに失する。インパクトを見極めセキュリティ対策の軽重を勘案す

図表4．ゼロトラストセキュリティモデルの概念と要件





図表5．外部リソース活用イメージ



ると共に、いざ事態が発生した場合の対策・公表の迅速化を図るために、事前の影響・リスク分析が重要である。

バックアップ強化

バックアップデータまで攻撃されないよう、物理・論理隔離したバックアップデータ保管を実現する基盤の整備、およびデータ更新の頻度や重要性に応じたバックアップ頻度の設計が求められる。

プレイブック整備

ランサムウェア感染時は、感染拡大防止に向けた隔離対応、フォレンジック調査、またそのための証拠保全等、システム障害時とは異なる対応が求められる。対応事項を“プレイブック”として事前に整備しておくことで、対応の迅速化を図りたい。また、身代金対応方針等も経営陣含め事前に整備しておくことを推奨する。

訓練

定期的な訓練による関係者の意識醸成だけでなく、整備したプレイブックの実効性を検証した上で、事業継続マニュアルにも落とし込んでおくことが肝要である。

5. ソーシング戦略の重要性

前述の事項を推進するにあたり、人材確保が課題となる。この分野は育成、採用ともにハードルが高いが故、外部リソースの活用含むソーシング戦略が重要な検討テーマとなる。弊社では、セキュリティ分野で必要となる人材タイプと必要なケイパビリティを整理している。自社で内製化すべき領域の見極めと必要リソースの試算に活用頂きたい。また、セキュリティ運用を中心にアウトソーシングサービスも提供している(図表5)。自社の貴重なセキュリティ人材を有効活用するための選択肢として検討頂ければ幸いである。

6. おわりに

サイバー攻撃も例外なく技術進化が進んでいる現在、事業者側も絶えず対応し続けなければならない。この終わらないセキュリティ競争から離脱したものはDXの世界での敗者となる。弊社では、セキュリティ対応とDX化を両輪で推進し勝ち組企業になるための知見を多数有しているため、ご興味があればぜひお声がけ頂きたい。