ZEBRA

Zebra セキュリティプラットフォーム

パフォーマンスエッジをセキュアに

ビジネスを加速するには広範な接続性が必須ですが、潜在的なセキュリティリスクに曝される可能性があります。ファイアウォールを設置することは出発点ですが、決して新たに発生する高度な脅威に対処できる十分な措置とは言えません。企業とデータをより適切に保護できるベストプラクティスとエンタープライズソリューションをご紹介します。

ビジネスに打撃を与えるセキュリティの脅威を阻止する方法

セキュリティは不可欠

クレジットカード情報、電子カルテ、マイナンバー、パスワード。顧客、患者、市民のいずれにサービスを提供するビジネスであっても、個人情報を非公開にすることが要求されており、大抵の場合必須義務となっています。

リスクの高まり

リスクは時間の経過とともに対処が困難になります。1例として、IoTとクラウドテクノロジーがこれまでにない方法で人と情報を結び付け、企業に前例のない事業経営の管理力と可視性を提供することです。想定される結果は素晴らしいですが、リスクがないわけではありません。

2022年までに予測される推定500億[1]の相互接続デバイスは、企業や機密データを無数の脆弱性に曝す可能性があります。高利益性と低い反動確率（ハッカーの5%しか起訴されていない[2]）が動機となり、サイバー犯罪に減速の兆しは見えません。

なにが最大の問題なのでしょうか？

たった1件の侵害でも多大な犠牲を払う恐れがあり、生産性と経済的損失に多大な損害を与え、企業評価を危険にさらす可能性があります。

これに対抗するために何ができるでしょうか？セキュリティを真剣に考える必要があります。企業にセキュリティプログラムがある場合でも、誤解が企業の整合性を損ない、思わぬ脆弱性を生み出している可能性があります。

390万ドル：
データ侵害の平均コスト[3]

25,575レコード：
データ侵害の平均サイズ[3]

12 時間:
サイバーハッカーの88%がサイバーセキュリティ防御を突破する平均時間[4]

197 日:
企業が侵害があったことに気付くまでの平均時間。[3]

ターゲット：

小売業：
オンライン小売業者のログイントラフィックの80%は、ハッカーによって盗まれたデータを使って攻撃されています。[5]

政府機関/公営企業：
スパイ活動と金銭的利益を伴うプライムターゲットが主要な動機付けとなる[6]

医療機関：
サイバー攻撃の15%を占める2番目に狙われる率の高い業界[6]

製造業：
この業界は過去数年間に他の業種よりも高いレベルのスパイ関連の被害を経験した[6]

誤解がセキュリティ脆弱性を高める

相次いでセキュリティ関連事案が広く公表されているにもかかわらず、多くの企業が自社のセキュリティに満足しています。誤ったセキュリティ感覚にだまされないでください。あなたが気づいた時には、既に被害にあっているかもしれません。

「自分の会社はセキュリティ侵害のターゲットにされるほどの規模ではないよ。」

サイバー攻撃の43%は中小企業を対象としています。[6] ハッカーは、中小企業のリソースと知識の不足を悪用します。より規模の大きい事業体との接続にアクセスするためにあなたの会社を利用することさえあります。

「自社のネットワークで充分保護されているよ。」

健全なセキュリティイニシアチブは多層構造であり、常に進化しています。玄関のドアをロックしても、窓を開けたままにしていては泥棒の侵入を防ぐことはできません。実際、ある研究では、ファイアウォールやウイルス対策などの従来の対策によってハッカーの侵入速度が低下することはほとんどありませんでしたが、エンドポイントセキュリティテクノロジーの方が攻撃を阻止するのに効果的であることが判明しました。[4]

「当社は一度もセキュリティ侵害を受けたことがないからうちのセキュリティは万全だよ。」

侵害がすでに発生していることに気付かない場合があります。調査によれば、1企業で侵害が検出されるまでに197日もかかる場合があります。[3]

「うちの社は既定のセキュリティプログラムを装備しているよ。」

しかし、絶えず変化する脅威に対応できるように貴社のセキュリティシステムは絶えず進化していますか？すべてのテクノロジーをカバーしていますか？「一回で終わり」のアプローチでは、今日の高度なサイバー犯罪にとても太刀打ちできません。

「セキュリティは複雑すぎるよ。」

適切に設計されたセキュリティは、直感的で簡単に実装できます。従業員にとってシームレスで、ITでの管理が簡素化されるセキュリティシステムにお任せください。

「セキュリティは生産性に悪影響を及ぼすのでは？」

セキュリティシステムが扱いにくい、統合が難しい、操作を停止するなどの不満は、すべて一般的な危惧に過ぎません。それでも、セキュリティ侵害は作業を中断させる可能性があります。このソリューションは、設計にセキュリティが組み込まれたテクノロジーを選択することです。これが、生産性を妨げるのではなく、セキュリティがサポートできる方法です。

複数のレイヤーで貴社のシステムを保護してください

すべてのセキュリティ対策がニーズに対応できるわけではありません。テクノロジーを検討するときは、Zebraテクノロジーに固有のこれらの重要なセキュリティ属性と安心を考慮にいれてください。

自動化されたセキュリティ機能：
IT部門が取得するまでに数週間かかっていたWi-Fi®認定が自動的に実行できるようになり、お客様とチームの安全な接続環境が加速されます。

ニーズに合わせてカスタマイズ可能：
独自のセキュリティトレランスを設定しますか？Zebraは、企業または部門のニーズに基づいてセキュリティレベルを調整する構成可能なソリューションを使用して簡単にこれを実現します。

シンプルなメンテナンスとサービス：
Zebraのセキュリティ機能、ソフトウェア、ハードウェアは、最小限のメンテナンスと最大限の稼働時間で動作するように開発およびテストされており高い信頼度をお約束します。さらに、24時間対応サービスチームが必要な場合にいつでも対応します。

統合が簡単：
Zebraを使用すると、スムーズで迅速な統合が可能になります。業界とアプリケーションに対する深い理解によって、統合ニーズを予測して満たすためのソリューションを既に設計済みです。

継続的な警戒とサポート：
トラブルシューティング、脆弱性評価、内部セキュリティコラボレーションによる、長年にわたるOSセキュリティアップデートとファームウェアの強化。

世界的で定評のあるベストプラクティスに従います：
Zebraは、ISO、米国国立標準技術研究所（NIST）、インターネットセキュリティベンチマークコントロールセンターなど、世界のセキュリティ専門家によって設定されたベストプラクティスとガイドラインに従っています。ご安心ください。Zebraの製品とソリューションは、事業体がHIPAA、PCI-DSS、およびGDPRへの準拠条件を満たすために役立つアプリケーションで使用されています。

セキュアエンタープライズテクノロジーのリーダー：
企業向けに セキュリティ強化 されたされたGoogle Android™と名付けられたオペレーティングシステムのパートナーであり、最大10年間のセキュリティOSサポートを提供します。強化されたエンタープライズモバイルコンピューターから、安全なプリンターや先見の明のあるテクノロジーまで、生産性とセキュリティがZebraの企業核心を形成していることがお分かりいただけると思います。

Zebra製品、ソリューション、およびサービス
NISTサイバーセキュリティフレームワークのあらゆる段階のサポート

見極める	リスクマネジメントモニタリング プリンターセキュリティ評価ウィザードプロフェッショナルサービス	サプライチェーンのリスクマネジメントセキュリティ委員会
保護する	Android LifeGuard™ プリンター保護モード デバイス制御	PrintSecureアップデート 自動Wi-Fi証明書管理 リスクマネジメントフレームワーク
検知する	プリンタープロファイルマネージャー エンタープライズ セキュリティ監視	リアルタイム検知
応答する	デバイスマネジメント 脅威検出対策	インシデント対応 顧客アラート
修復する	プロフェッショナルサービス システムの機能追加や性能向上	原状回復

パフォーマンスエッジの保護

セキュリティはビジネスとワークフローにとって重要です。そのため、Zebraはソリューションに複数の保護層を統合することにより、セキュリティの脆弱性を予防的に保護します。Zebraのデバイス、テクノロジー、およびサービスは、生産性を損なうことなく、セキュリティを考慮して設計されています。当社のセキュリティがデプロイメントが簡単で、最前線の従業員にとってシームレスであることがお分かりいただけます。Zebraのスマートで構成可能なテクノロジーを使用すると、実世界の運用目標とセキュリティをリアルタイムでバランスさせることができます。Zebraは、ビジネス戦略とテクノロジー戦略をエッジで実装するのに役立つ安心感をご提供します。Zebraにお任せください。

ZEBRA

Zebraのセキュリティを改善する秘策をごらんください
以下にアクセスしてください **www.zebra.com/product-security**

出典：
1. Juniper Research, 2018年版 **2.** Carbon Black Incident Response Threat Report, 2018年11月号
3.Ponemon Institute, 2018年および2019年版 Cost of Data Breach **4.**Black Report, Nuix 2017年版
5.Shape Credential Spill Report 2018版 **6.**2019年版 Data Breach Investigations Report