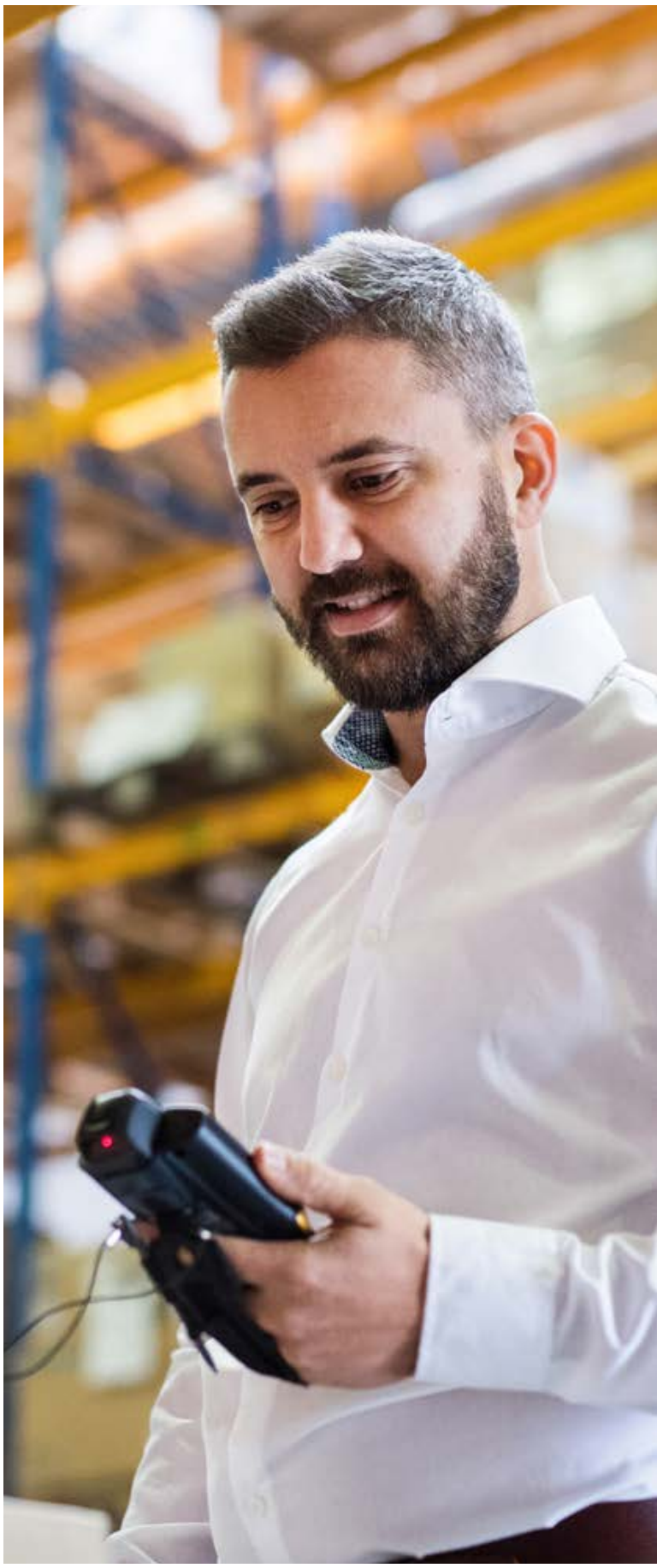
ガイド

サイバーレジリエンスを強化するための包括的アプローチ

verizon business

目次



サイバー脅威が増大する中、企業はどのようにレジリエンスを高めることができるでしょうか?

サイバー脅威のレベルと巧妙さが上昇し続けている中、企業はどのようにして保護された状態を維持できるのでしょうか? 重要なのは、より全体的な視点を持つことです。

テクノロジーが進歩し、あらゆる業種の企業がより密接につながるようになるにつれて、サイバー脅威のリスクも同時に増大しています。サイバー攻撃者は日々巧妙さを増しており、企業がデジタルツールやプロセスへの依存度を高め、クラウドに保存され、共有されるデータの量が増えるにつれて攻撃対象領域も拡大しています。

企業が自らを守るためには、企業の特定のニーズと事業環境における規制要件を満たす強力なサイバーセキュリティプログラムが必要です。

サイバー脅威は増加しています

ベライゾンビジネスの「2024年度データ漏洩/侵害調査報告書（DBIR）[1]」では、以下を分析しています。

30,458件
実際のインシデントの件数

10,626件
データ漏洩/侵害が確認された件数

94か国
被害が確認された国の数

増大する脅威の管理

DBIRでは、脆弱性を悪用した攻撃が大幅に増加していることが示されています。前年より180%増加し、これらの攻撃の主な侵入経路はWebアプリケーションでした。

攻撃の約3分の1はランサムウェアに関連しており、被害額がかなり高額になる可能性があるため、企業の92%が依然として大きな懸念を抱いています。FBIのインターネット犯罪苦情センター（IC3）のランサムウェア苦情データによると、「ランサムウェア」とその他の「脅迫」による漏洩/侵害の組み合わせに関連する損失の中央値は46,000ドル（95%のケースで3ドルから1,141,467ドルの範囲）です[2]。

1&2. 2024年度データ漏洩/侵害調査報告書(n.d.).Verizon Business. https://www.verizon.com/business/en-gb/resources/reports/dbir/

しかし、企業が懸念すべきは脅威の数だけではありません。サイバー攻撃者は能力を高めており、攻撃を阻止してデータ損失を防ぐ最新のテクノロジーや、企業の意識を向上させるための規制を突破するために、より洗練された攻撃を開発しています。フランスの国家情報システムセキュリティ庁（ANSSI）が発表した「Panorama of Cyberthreats 2022（サイバー脅威概観2022）」では、「悪意のある攻撃者は、金銭目的、スパイ活動、不安定化を図る能力を継続的に向上させています。この能力向上は、特に、被害者のネットワークへの慎重かつ永続的なアクセスを得ようとする攻撃者による攻撃対象選択に顕著に表れています[3]」と指摘しています。

脆弱性の増大

テクノロジー、ネットワーク機能、業務慣行の進歩により、企業はサイバー攻撃者が悪用できる脆弱性の増大を認識する必要があります。「考慮すべき重要な要素は、リモートワークの促進と組織のハイブリッド化であり、これによって情報システムセキュリティの境界が再定義されたのです」と、ベライゾンビジネス、Security Consulting ServicesアソシエイトディレクターのSteven Geversは指摘します。

3.ANSSI.(2022).PANORAMA DE LA CYBERMENACE 2022.In ANSSI. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

DBIRで説明されているように、脆弱性による漏洩/侵害は3倍に増加しており、その主な要因はゼロデイ攻撃の影響です。したがって、企業は基本的なセキュリティハイジーン（衛生管理）を常に維持することが不可欠です。また、ゼロトラストや多層防御などの概念がいかに重要であるかも示しています。

> 組織のどの部分が最大のリスクにさらされているかを包括的に把握し、セキュリティ予算を最もリスクの高い部分に投入することが重要です。
>
> **Steven Gevers**
> ベライゾンビジネス、Security Consulting Services
> アソシエイトディレクター

従業員が自ら問題を解決しようとする場合にも問題が発生する可能性があります。現在の従業員は、効率の良いデジタル利用の業務に慣れています。問題の解決策をすぐに見つけることができない場合、意図せずにセキュリティポリシーに違反し、許可あるいは保護されていないアプリケーション、ソフトウェア、またはハードウェアを使用する誘惑に駆られる可能性があります。Harvard Business Reviewの調査によると、回答者の67%が少なくとも1回はサイバーセキュリティポリシーを完全には遵守していない事実が明らかになっています[4]。このいわゆる"シャドーIT"によってさらなる脆弱性が生じ、攻撃者に新たな侵入可能な経路を与えることになってしまいます。

4.Verizon.(2023).2023 Mobile Security Index whitepaper. https://www.verizon.com/business/resources/T19d/reports/mobile-security-index-report.pdf

最適なセキュリティ対策を見つける

このようなサイバー脅威の増加に直面して、多くの企業がゼロトラストおよびSASEソリューションを導入しています。これはネットワークセキュリティを強化するのには非常に効果的ですが、客観的に全体がどのように連携して動作するかを確認することも重要です。

「ビジネスユニットごとに独自のビジネスアプリケーションがあり、独自のプロセスとニーズがあります」と、ベライゾンビジネス、Cyber Defense Consulting ServicesディレクターのStephen Youngは指摘します。「セキュリティには多様な局面があり、さまざまな種類の攻撃に対処する環境に影響を与えます。すべてを解決するソリューションは存在しません。したがって、セキュリティのレジリエンスの強化は、ゼロトラストとSASEだけにとどまらず、さらにその先を目指す必要があります」

> すべてを解決するソリューションは存在しません。したがって、セキュリティのレジリエンスの強化は、ゼロトラストとSASEだけにとどまらず、さらにその先を目指す必要があります。
>
> **Stephen Young**
> ベライゾンビジネス、Cyber Defense Consulting Services ディレクター

基本を大切にする

場合によっては、企業はセキュリティ上の大きな脅威に注目しすぎて、自社の環境におけるシンプルで基本的な要素を見過ごしてしまうことがあります。「状況が複雑になればなるほど、脅威の大きさが増し、企業は基本的なことをおろそかにする傾向があります」とYoungは言います。

> 基本原則は、効果的なセキュリティポリシーの関連性を構築することです。
>
> **Stephen Young**
> ベライゾンビジネス、Cyber Defense Consulting Services ディレクター

企業はインフラ全体のセキュリティを幅広く見直し、大きな問題に対する解決策を見つける必要がありますが、システムの更新やファイアウォールの正しい設定など、基本的なセキュリティ手順をおろそかにしないことが重要です。これらの基本を遵守することで、ITチームは小さなセキュリティ脅威の侵入を防ぐだけでなく、不必要なセキュリティツールに無駄なお金を使うことも回避できます。

より包括的なアプローチを採用

多くの企業は、複数のレイヤーを追加してセキュリティを強化したいという誘惑に駆られます。しかし、これは実際には逆効果となり、複雑さとコストがさらに増大する可能性があります。代わりに、全体を見て、何が、どこに、どのような理由で必要なのかを評価することをお勧めします。そのため、ベライゾンは、組織の運用エコシステムから個々のユーザのニーズに至るまで、ビジネスを深く理解した上で、より包括的なアプローチを採用します。

これを実現するために、ベライゾンは米国国立標準技術研究所（NIST）の5つの主要な軸に基づくセキュリティフレームワークに準拠しています[5]。

ベライゾンは、企業の特定のニーズを理解するために詳細なセキュリティ評価を実施した上で、それらのニーズを満たすカスタマイズされたセキュリティ対策の導入をサポートします。

- 特定
- 防御
- 検知
- 対応
- 復旧

5.National Institute of Standards and Technology.(2024).The NIST Cybersecurity Framework (CSF) 2.0.In NIST CSWP 29[Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

> 企業にはそれぞれ独自の文化とリスク許容度があり、その結果、セキュリティに対するアプローチも異なってきます。

Steven Gevers
ベライゾンビジネス、Security Consulting Services
アソシエイトディレクター

「生成AIのようなテクノロジーを、知的財産権のリスクとして利用不可にする必要があると考える企業もあれば、コーチングが必要なビジネスイネーブラーだと考える企業もあります。ベライゾンは、ビジネスニーズを念頭に置きながら、最大の脅威に焦点を当て、お客様のセキュリティ成熟度の向上をサポートします。企業の資産を保護するために複数のセキュリティ対策を活用する多層防御を採用することが、その鍵となります。企業は、あるレベルで柔軟性を確保しながら、別のレベルでの制御によってリスクを許容範囲内に抑えることができます。あるレイヤーが侵害された場合、別のレイヤーが攻撃を食い止めたり、その影響を軽減したりすることが可能になるのです」

このアプローチは、最も強固なIT防御を構築するのに役立つだけでなく、企業がより効果的にコストを管理し、ニーズに合ったソリューションに投資し、予算をより賢く管理することも可能にします。「ビジネスニーズをグローバルな視点でとらえ、オーダーメイドのソリューションを構築することで、冗長なセキュリティソリューションの増殖を回避できます。つまり合理化によるコスト管理の改善です」とYoungは指摘します。

セキュリティに対するこのような包括的なアプローチにより、企業は自社のニーズと予算に見合った適切なセキュリティを実現することができるのです。そして、サイバー攻撃者を寄せ付けないためのインフラを整えることができます。

ベライゾンが、お客様のビジネスに適した包括的なセキュリティソリューションで、どのようにサイバー脅威の軽減をサポートするのか、Verizon.com/business/ja-gbでご確認ください。ベライゾンのセキュリティおよびSASEソリューションの詳細情報の取得には、こちらからメールをご登録ください。