

脆弱性管理から ビジネス重視の リスク軽減へ 移行する方法

よりスマートな脆弱性管理のための5ステップ実践ガイド

2025年11月10日

目次

寄稿者

Russ Sandarlin

Director, Subject Matter Expert,
Vulnerability Management
Detection and Response

Anthony Williams

Subject Matter Expert,
Vulnerability Management
Detection and Response

3	エグゼクティブサマリー
4	はじめに
5	ビジネスに沿った行動のための 共通リスク言語
9	ステップ 1—優先順位主導型戦略 への移行: サイロ化された縦割り型 の意思決定から統合されたリスクイ ンテリジェンスへ
12	ステップ 2—現状把握: 脅威認識に 基づく測定
15	ステップ 3—視点を変える: ビジネスにとって重要な資産 を特定し、優先順位を付ける
20	ステップ 4—サイバーリスクの 伝達と追跡
23	ステップ 5—リスクを排除する: 自信を持ってリードする
27	より少ないリソースでより多くの 成果を: Qualys TruRisk™で変 革をリードする
30	結論
31	洞察から行動へ移行しよう
31	Qualysについて

エグゼクティブサマリー

今日のサイバーセキュリティリーダーは、あるパラドックスに直面しています。

かつてないほどの可視性は高まっているものの、真に重要なことが何なのかが明確になっていません。約30万件もの既知の脆弱性が注目を集めようと競い合っており、パッチ適用数やCVSSスコアで成功を測る従来の手法では、もはや十分な保護を提供できません。

ノイズから明瞭さへ

- 現在、約30万件の脆弱性が存在します。組織がそれらすべてに対応することは不可能です。
- 従来の指標（パッチ適用件数、CVSSスコア）は、進歩ではなく、単なる動きを生み出すだけです。
- 転換点はシンプルです。最も重要なことに集中しましょう。

リスクとは、量ではなく結果に関わるものです。この視点に基づいたセキュリティ対策は、信頼と成長の原動力となります。

本稿では、**量重視型のセキュリティからリスクベースのセキュリティへの転換**を提唱する。組織はあらゆる問題に追及するのではなく、収益、顧客からの信頼、コンプライアンスに最も悪影響を及ぼす可能性のある問題を優先的に対処すべきである。

ここで提示する枠組みは、シンプルながらも強力な考え方に集約されます。

効果的なリスク管理とは、より多くの対策を講じることではありません。成功の尺度は、活動量ではなく、回復力です。

経営幹部にとって、この変化は3つの決定的な結果をもたらします。

- **レジリエンス** — 事業継続の中核となるシステムとデータを保護する。
- **効率性** — 最も効果的な場所にリソースを投入する。
- **明確性** — サイバーリスクを、自信に満ちた意思決定を導くビジネスシグナルへと転換する。

以降のページでは、セキュリティチームがこの変革を5つのステップでどのように実現できるかを概説します。しかし、目指すべき目標は最初から明確です。それは、測定可能で説明可能であり、ビジネスの優先事項と整合したセキュリティ体制を構築することです。

はじめに

2025年6月現在、米国国家脆弱性データベース（NVD）には、驚くべきことに299,496件もの脆弱性が登録されています。

この膨大な数は、サイバー脅威環境の急速かつ持続的な拡大を示しており、あらゆる脆弱性を網羅的に調査することは非現実的であるという厳しい現実を突きつけています。

すべての脆弱性を同等に扱うことの隠れたコスト

発見された脆弱性の数、あるいは修正された脆弱性の数だけで組織のリスクを評価することは、もはや全体像を捉えることはできません。発見される問題の数が急増するにつれ、それぞれを同等の緊急度で扱うことは、リソースを浪費し、最も重要な対策を遅らせることとなります。課題はもはや脅威を特定することではなく、どの脅威に注意を払うべきか、そしてその理由を判断することです。このような状況では、問題の数はむしろ注意をそらす要因となります。真に意味のある指標とは、リスクへのエクスポージャーの低減、レジリエンスの向上、そしてビジネスリスクとの整合性を反映するものです。

すべての脆弱性が同じ重大度を持つわけではありません。悪用された兆候のない重大な脆弱性は、インターネットに接続された高価値システム上の軽微な脆弱性よりも、差し迫った危険性が低い場合があります。状況、悪用可能性、資産の重要性、およびビジネスへの影響を理解しなければ、対策は場当たりのものになるリスクがあります。

リスクベースの優先順位付けは、より戦略的な前進の道筋を示します。どの脆弱性が悪用される可能性が最も高く、その影響が最も深刻になる可能性があるかをチームが評価するのに役立ちます。例えば、サンドボックス化されたシステム上の重大な脆弱性を修正するよりも、機密データをホストするシステム上の軽微な欠陥を軽減する方が、緊急性は低いかもしれません。

転換点はまさにそこにある。量から結果へ。広範囲な修正から、的確な対応へ。問われるべきは「どれだけパッチを適用したか」ではなく、「何を防いだか」だ。

この考え方を取り入れることで、組織は明確なビジョンを持って行動し、必要なところにリソースを集中させ、セキュリティ運用を事業継続性やレジリエンスと整合させることができる。事後対応型のパッチ適用から、情報に基づいた優先順位付けへと進化していくことで、現代のサイバーセキュリティ体制は成熟していく。

「これらの数字は警鐘であり、全体像の一部しか捉えていない。組織はセキュリティ戦略を見直し、真に重要な点に焦点を当てる必要がある。」

ビジネスに沿った 行動のための 共通リスク言語

想像してみてください。デジタル変革の波に乗って急成長を遂げていた企業が、突然停止状態に陥ります。セキュリティチームの努力不足ではなく、誤った脅威にばかり目を向けていたために、重要なシステムが脆弱性の悪用によってオフラインになってしまうのです。このようなシナリオは決して珍しいものではありません。多くの組織は依然としてサイバーセキュリティに受動的なアプローチを取り、脅威の発生可能性やビジネス上の優先順位を明確に把握することなく、際限のない脆弱性リストを追いかけているのが現状です。

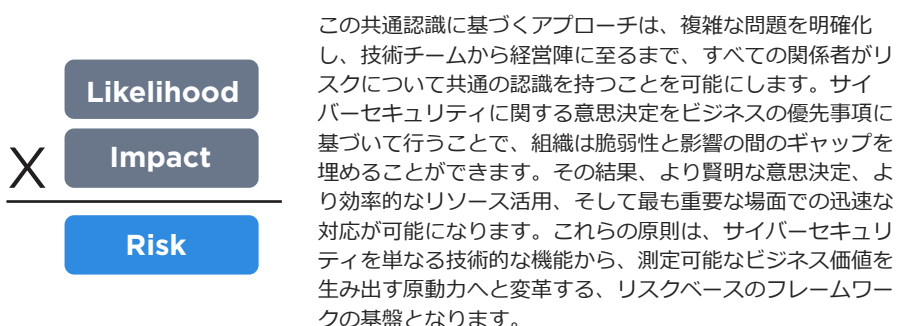
効果的な優先順位付けは、共通理解から始まります。セキュリティ、IT、そしてビジネスリーダーが、ビジネスへの影響、業務の中断、規制リスクといった共通の認識に基づいて共通の言語でコミュニケーションを取ることで、チームは明確な優先順位付けを行い、意思決定を迅速化し、より強力なサポートを得ることができます。ビジネスに沿った言葉遣いは、緊急性を明確にし、行動の正当性を証明し、重要な分野にリソースを集中させるのに役立ちます。

このように、個々の行動から共通の認識へと移行することで、戦略は実行へと転換します。全員がリスクを同じように認識することで、セキュリティリーダーは組織のサイロ化された縦割り構造を解消し、サイバーセキュリティを単なるコストセンターではなく、レジリエンスと成長の原動力へと変えることができるのです。

ビジネスに即したサイバーリスク管理で基盤を築く

このビジョンを実現するには、組織は脆弱性管理とビジネス上の優先事項とのギャップを埋める、最新のデータ駆動型ツールを必要としています。事業継続性を確保するには、この変化を追跡し、促進する、包括的でビジネスファーストな脆弱性管理アプローチが不可欠です。

明確かつ効果的な戦略を策定する、よく知られたビジネス優先のリスク管理手法について考えてみましょう。



重要なことを測定する

リスクを理解するには、脆弱性の数だけにとらわれず、ビジネスにとって何が最も重要なかを問いかける必要があります。リスクを測定する際には、脆弱性の発生場所、脆弱性の露出度、そして影響を受けるシステムが業務にとってどれほど重要かを考慮する必要があります。まさにこの理由から、効果的なリスク管理とは、脆弱性を悪用される可能性、ビジネスへの影響、そして業務上の関連性という観点から捉えることなのです。セキュリティチームが目的意識を持って測定を行うことで、ノイズを排除し、現実世界に深刻な影響を及ぼす可能性のある少数の問題を特定し、技術的に健全かつ戦略的に整合性の取れたリスクプロファイルを作成できます。そうして初めて、チームは明確かつ自信を持って、迅速に行動できるのです。



明確なコミュニケーション

セキュリティリーダーがリスクの本質を的確に伝える方法を知らない限り、リスクは専門用語に埋もれたり、スプレッドシートの中に閉じ込められたりして、その緊急性を失ってしまいます。たとえ最高のリスクデータであっても、何が危機に瀕しているのか誰も理解していなければ、その価値は失われてしまいます。リスクを重視するCISOは、技術的な調査結果をビジネスの文脈に落とし込み、リスク要因と影響をマッピングし、SOCから役員会まで、あらゆる立場の人々に理解される言葉で説明します。重要なのは、脆弱性と、稼働時間、評判、収益といった重要な成果との関連性を明確にすることです。適切なツールは、インシデントのレビューであれ、経営幹部レベルでの優先順位の説明であれ、あらゆる場面で通用する信頼性の高い指標とレポートによって、その明確さをさらに強化します。



的確な排除

ここで、優先順位付けが具体的な進歩へと繋がります。リスク状況を把握し、重大な脆弱性を特定したら、次のステップは的を絞った対策です。すべてをパッチで修正するのではなく、業務に最も大きな影響を与える脅威を慎重に無力化していくことが重要です。外科手術のようなアプローチを取ることで、チームはプレッシャーに押しつぶされることなく、明確な目的意識を持って行動できます。

修正プログラムの適用、システムの隔離、設定ミスの修正など、あらゆるステップは、業務に不可欠な運用を保護するという目標に立ち返るべきです。これにより、リスクインテリジェンスは測定可能なリスク軽減へと転換し、チームは脅威への対応から、脅威が拡大する前に静かに無力化する体制へと移行できます。

このアプローチを採用する組織は、以下の重要なメリットを享受できます。

- 影響度の高い脆弱性の軽減を優先することで、収益源を保護できます。
- 破壊的な情報漏洩のリスクを低減することで、ブランドの信頼性を維持できます。
- データに基づいたリソース配分により、セキュリティ投資対効果（ROI）を最大化できます。
- ビジネス中心の共通リスク言語を用いることで、セキュリティ担当者、技術担当者、経営陣間のギャップを埋めることができます。

組織が近代化を急ぐ中、俊敏なデジタル変革の必要性は、サイバーセキュリティがもはやバックオフィスIT機能としての役割をはるかに超えていることを示しています。今日、サイバーセキュリティは事業の中核を支える要素であり、業務全体に組み込まれ、回復力、俊敏性、そして成長にとって不可欠なものとなっています。

組織のあらゆる階層にセキュリティが組み込まれることで、その効果は飛躍的に高まります。大胆なイノベーションを促進し、自信に満ちた市場参入を後押しし、企業がためらうことなく変化に適応できるよう支援します。

しかし、レジリエンスは集中力から生まれます。真に重要なリスクを測定し、明確で状況に応じたコミュニケーションを通じて意思決定を整合させ、進歩を阻害するリスク要因を排除することが重要です。従来、量に重点を置いてきた脆弱性管理の手法に頼るのではなく、リスクへのアプローチ方法を根本的に見直す必要があります。リスクを、削減すべきバックログとしてではなく、最適化すべきビジネス機能として捉えるべきなのです。

このガイドでは、セキュリティリーダーが事後対応型の管理から、優先順位付け、状況把握、明確化を基盤としたビジネスに沿ったリスク軽減へと移行するための、5つの実践的なステップを概説します。

ステップ 1

優先順位主導型戦略への移行: サイロ化された縦割りの意思決定から 統合されたリスクインテリジェンスへ

共通のリスク言語で 強固な基盤を構築する

明確なビジネスコンテキストなしに脆弱性を修正するだけでは、誤った安心感を生み出す可能性があります。脆弱性の数が減少すれば進歩の兆しに見えるかもしれませんが、多くの場合、より深刻な問題、つまり脆弱性がビジネスリスクに及ぼす真の影響を正確に把握できていないという問題を覆い隠しています。

リスクコンテキストは、そのギャップを埋める役割を果たします。それは、旧式の中層ウェアスタックに存在するCVEと、顧客向けアプリケーションの潜在的な障害を結びつける結合組織のようなものです。パッチ適用に関する意思決定を、戦術的なものから戦略的なものへと高めるものなのです。

よくあるシナリオを考えてみましょう。基幹アプリケーションが脆弱性を悪用されてダウンしたとします。セキュリティチームは迅速に対応して侵害を封じ込めますが、事業部門は不意を突かれます。なぜでしょうか？それは、事業部門が理解できる基準でシステムが高リスクとして認識されていなかったからです。セキュリティチームはCVSSスコアや悪用可能性データに基づいて業務を行うことが多い一方、事業部門のリーダーは収益、事業継続性、そして評判への影響といった観点からリスクを評価します。こうした視点が一致しない場合、リスク管理は断片化し、組織は重要な部分でリスクにさらされたままになります。

このギャップを埋めるには、より優れた指標だけでは不十分です。リスクの解釈と共有方法について、意図的な再調整が求められます。ここでリーダーは、戦略を形成する共通認識を確立し、何が重大なリスクであり、何がそうでないかを明確に定義する必要があります。そして、その際、修復チームだけでなく、事業継続、コンプライアンス、顧客体験を担当する人々にも明確な指針を示す必要があります。

現代のリスク状況は、セキュリティ境界の内側だけに限定されるものではありません。サードパーティプラットフォーム、SaaSへの依存、アウトソーシングサービスなどはすべて潜在的な脆弱性を生み出し、その多くは直接的なセキュリティ管理の対象外となっています。こうした複雑な関係性を可視化できなければ、優先順位の高いパッチ適用作業でさえ不十分になる可能性があります。サードパーティの状況を内部リスク評価に組み込むことは、正確で実行可能なリスク戦略を構築する上で不可欠です。

リスクに関する共通認識を構築するには、初日から完璧な連携を図るよりも、これまで必ずしも緊密に連携してこなかったチーム間の協働を促進することから始まります。これは、孤立した対応から共に先を見越した対応へと、姿勢の転換を意味します。セキュリティチームが、ビジネスが真に重視する価値観に基づいてリスクを捉えることができれば、議論の方向性が変わります。トレードオフがより明確になり、優先順位が明確化されます。そして、難しい決断でさえも、必要な明確さを得られるようになります。

まずは、厳しい問いを投げかけてみましょう。



技術的な観点だけでなく、財務、評判、そして業務への影響という観点から、真のリスク許容度はどの程度でしょうか？



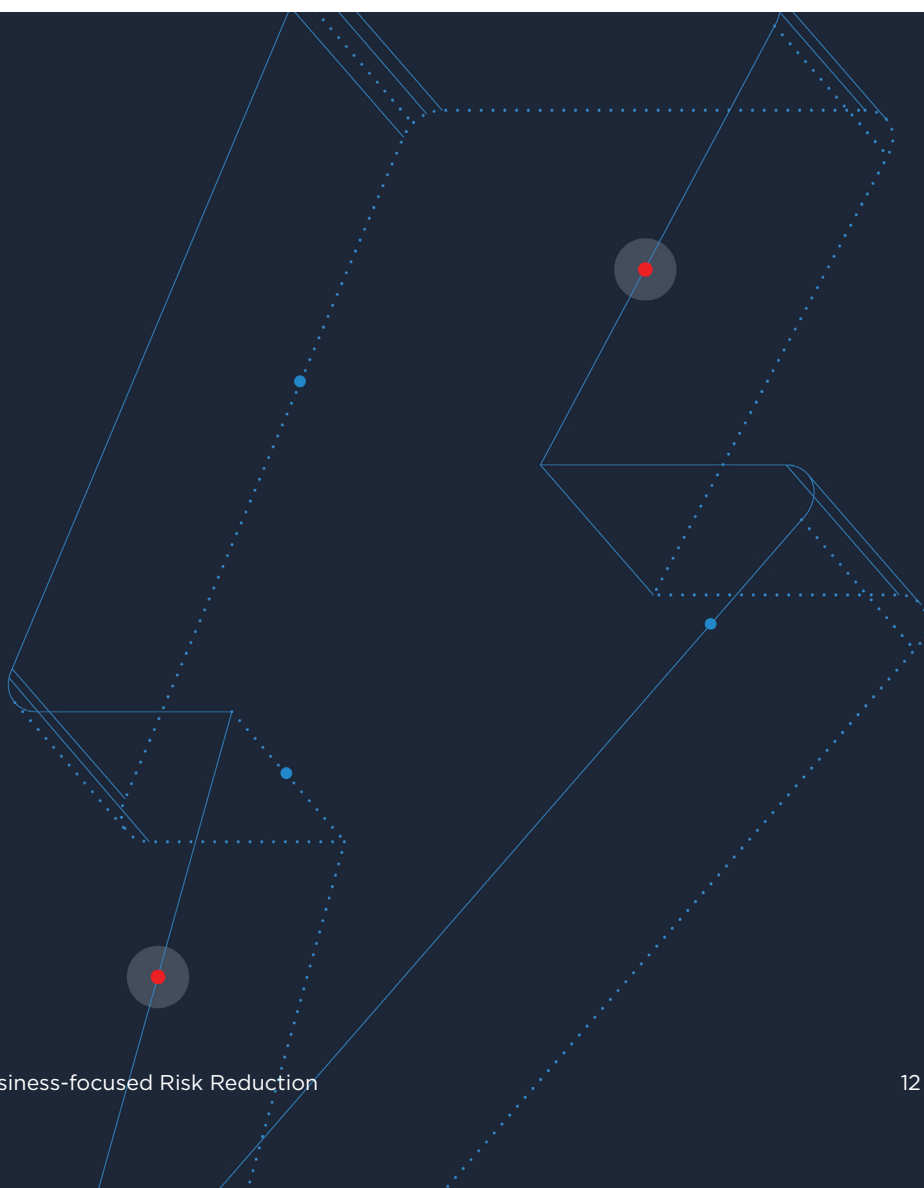
収益、規制遵守、そして事業継続にとって、どの資産やシステムがミッションクリティカルでしょうか？



それらの資産やシステムが侵害された場合、どのような影響が生じるでしょうか？

ステップ 2

現状把握: 脅威認識に基づく測定



深深度評価を超えて、可能性スコアリングを活用する

長年にわたり、脆弱性管理は共通脆弱性評価システム（CVSS）のような静的な指標に基づいて行われてきました。CVSSは技術的な深深度を評価するものの、現実世界の状況を見落としがちです。こうしたスコアは有用な基礎的見解を提供しますが、実際の悪用の可能性を反映することはほとんどありません。技術的に深刻な脆弱性は示してくれますが、実際に危険な脆弱性は示してくれないのです。

「中程度」の脆弱性は、実際に悪用され、**CISAの既知の悪用脆弱性（KEV）**カタログに掲載されていると知るまでは、リスクが低いように思えるかもしれません。このように、理論上の深深度と現実世界の脅威との間に乖離が生じることで、セキュリティチームは非効率的な対応を強いられ、優先度の低い問題に過剰に対処してしまう一方で、リスクの高い脆弱性が放置されてしまうのです。

情報からインテリジェンスへ: 進化するリスク優先順位付け

サイバーリスク管理には、単なるデータやダッシュボードにとどまらず、技術的な知見を脅威の挙動、悪用可能性、対策の有効性、そして業界全体との関連性といった要素と照らし合わせて評価する能力が求められます。この変化により、チームはビジネスへの攻撃に最も利用される可能性の高い脅威に焦点を当てることができ、時間、労力、そして注意力を本当に重要な部分に集中させることができます。

この進化したアプローチは、以下の3つの基本要素に基づいています。



状況に応じた 深深度

CVSSは技術的な深深度を測る一貫した基準値を提供するものの、現実世界の脅威を正確に反映しきれない場合が少なくありません。すべての重大な脆弱性が緊急を要するわけではなく、中程度の脆弱性でも、信頼できるエクスプロイトが出現した瞬間に重大な脆弱性へと変化する可能性があります。しかし、多くのチームは、対策を講じる前にスコアの調整を待ってしまうという状況に陥っています。

真の脅威認識は、脆弱性が何に影響を与えるのか、どの程度露出しているのか、そして悪用される可能性はどの程度なのかといった、コンテキストに依存します。コンテキストがなければ、チームは間違った優先順位に時間を費やし、高い信頼性を持つ脅威を見落とししてしまうことになります。



リアルタイムの 脅威インテリジェンス

潜在的な脆弱性も、エクスプロイトコードが公開されたり、攻撃者が標的に始めたたりすると、一夜にして優先度の高い問題に発展する可能性があります。常に先手を打つためには、静的な深深度スコアだけでなく、より多くの情報を追跡する必要があります。エクスプロイト活動、攻撃者の行動などを含むリアルタイムの脅威インテリジェンスは、EPSS、CISA KEV、MITRE ATT&CKなどの情報源から補強することができ、セキュリティチームは被害が発生する前に対応するための追加的な洞察を得ることができます。



現実世界における 緩和策

すべてのリスクにパッチ適用が必要なわけではありません。最新のリスクモデルでは、即時の修復の必要性を軽減できる補償・緩和策が考慮されています。これには、ファイアウォール、エンドポイント検出、ネットワークセグメンテーション、サービス強化、さらにはレジストリキーの変更などが含まれます。保護されたネットワークセグメント内の露出度の低い資産に脆弱性が存在する場合、実際のリスクは低い可能性があります。これらの安全対策を認識することで、チームは安全に優先順位を下げ、安全策が組み込まれておらず、時間的制約が真に重要な箇所にリソースを集中させることができます。

これらの要素が組み合わさることで、より鋭敏で、より強靱なリスク優先順位付けのレンズが形成される。

コンテキストの一元化: 脅威データを実用的なものにする

多くの組織では、脆弱性データは複数のツールやフィードから流入し、それぞれ独自のフォーマット、頻度、前提に基づいています。アナリストは、断片化されたコンテキストをつなぎ合わせ、ノイズを管理しながら時間との戦いを強いられています。

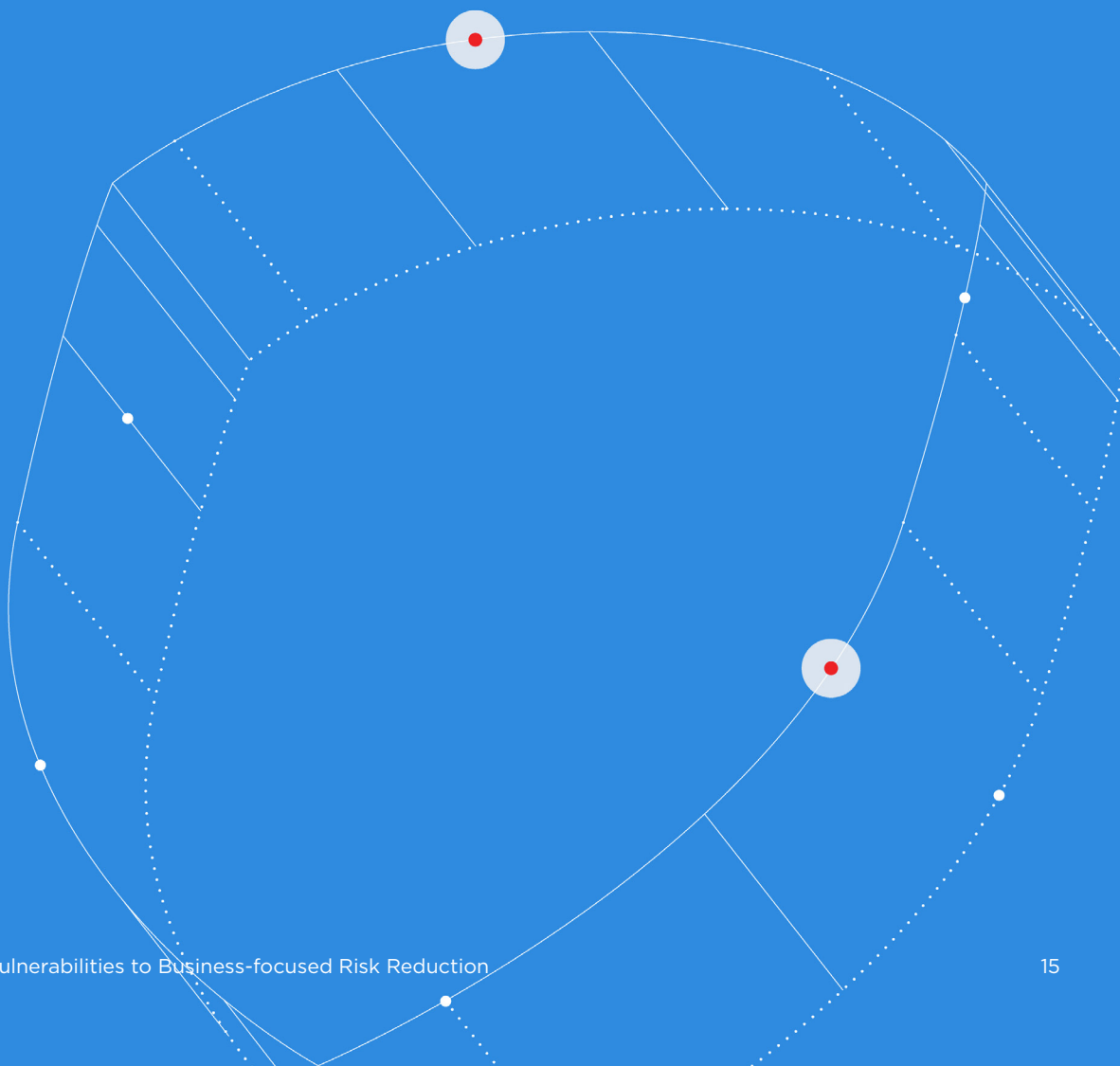
より効果的なアプローチは、そうした情報を統合して統一されたリスク像を構築することです。EPSS、KEV、MITRE ATT&CK®などの脅威インテリジェンスソースからのシグナルを相関させることで、組織は最終的に、現在どの脆弱性が深刻な脅威となっているかを把握できるようになります。悪用された脆弱性、マッピングされた脆弱性、そして破壊的な脆弱性が上位に表示されるのは、単に数値的な理由からではなく、状況がそれを必要とするからです。

静的なスコアリングから動的な脅威インテリジェンスの優先順位付けへと移行することで、デジタル紛争のスピードに対応するための基盤を築くことができます。

明確でコンテキストに沿ったリスク情報を提供することで、企業は不要な情報を排除し、最も差し迫った脅威を優先順位付けし、リソースを効果的に配分できるようになります。実用的なサイバーセキュリティに関する洞察は、事後対応型の防御と、先を見越した戦略的な優位性の分かれ目となる可能性があります。

ステップ 3

視点を変える： ビジネスにとって重要な資産 を特定し、優先順位を付ける



サイバーリスクを ビジネスに即した アクションへと 変換する

どのサイバーセキュリティチームも、最終的には同じ疑問に直面します。それは、問いかけは簡単でありながら、明確かつ合意に基づいた答えを出すのが驚くほど難しい問いです。「ビジネスにとって最も重要な資産は何か、そしてその理由は何か？」。

多くのリスク管理プログラムがここでつまづきます。

周知の落とし穴があるにもかかわらず、リスクの優先順位付けはしばしば深刻度スコアに基づいて行われる。アイドル状態の内部サーバー上の「重大な」CVEはエスカレーションされる一方で、決済プラットフォームの設定ミスは静かに放置される。これはツールの不具合ではなく、コンテキストのギャップを反映している。

このギャップを埋めるには、資産の重要性について明確かつ共通の認識を持つことが不可欠です。そのためには、システムレベルの脅威ではなく、ビジネスレベルへの影響に焦点を当てることから始める必要があります。

ビジネスインパクト分析 (BIA): リスク要因の把握

真のリスクベースの意思決定には、考え方の転換が必要です。技術的な深刻度から、状況に応じた重要性へと焦点を移す必要があります。その第一歩がビジネスインパクト分析 (BIA) です。BIAは単なる概念的なチェックリストではなく、真にリスク要因を把握するための、構造化された標準準拠のプロセスです。成熟したプログラムでは、NIST 8286Dなどの認知されたフレームワークに基づいてBIAを実施し、リスク管理機能全体にわたる一貫性とトレーサビリティを確保するとともに、特定のシステムへの障害が業務、収益、コンプライアンス、顧客信頼にどのような影響を与えるかを深く理解します。

強固な事業影響度分析 (BIA) フレームワークは、以下の最も重要な疑問に答えるのに役立ちます。

- この資産に依存している主要な事業機能は何ですか？
- 侵害された場合、どのプロセスや部門が混乱しますか？
- ダウンタイムは、収益損失、規制リスク、評判の低下といった点でどのような影響をもたらしますか？

しかし、BIAの価値は文書化にあるだけでなく、業務上の意思決定を促進する能力にある。

ビジネスインパクトの具体化: 資産重要度スコア (ACS)

資産重要度スコア (ACS) は、ビジネスインパクト分析 (BIA) から得られた定性的な知見を、測定可能な数値に変換します。機密性、完全性、可用性といった技術的な基本要素と、収益への影響、顧客への可視性、コンプライアンスへの関連性といったビジネス上の考慮事項を組み合わせます。

効果的なACSモデルは、この3つの要素を基盤としつつ、その関連性をビジネス領域にまで拡張する。



機密性

- 処理または保管されている情報の機密性はどの程度か？
- 情報漏洩は法令違反を引き起こしたり、顧客の信頼を損なったりする可能性があるか？



完全性

- このシステムのデータが改ざんされた場合、どのような影響がありますか？
- 財務報告、業務の正確性、意思決定に影響はありますか？



可用性

- システム停止によるビジネスコストはどれくらいか？
例えば、ECサイトが繁忙期にダウンした場合、どのような影響が出るのか？

これらの要素をビジネスへの影響という観点と統合することで、ACSはセキュリティ責任者が、ミッションクリティカルな資産と、運用を支援する資産または任意的な資産を区別することを可能にします。

ACSはBIAから入力情報を直接継承するため、両者の関係は1対1です。BIAで定義されたビジネス影響のコンテキストはACSにシームレスに反映され、優先順位付けが技術的側面とビジネス上の現実の両方を反映したものとなります。このマッピングを業界標準に合わせることで、組織は最初に何を保護すべきかを決定するための、再現性があり、かつ正当性のある方法を確立できます。

「ほとんどの組織において、ACSデータは決して完璧でも完全でもありませんが、それで問題ありません。進歩は、最も価値の高い資産、つまり「至宝」を日常的なセキュリティワークフローに組み込むことから始まります。影響が最も大きい箇所を優先することで、最も重要なものを守るだけでなく、データ品質と組織の成熟度を高め、ACSを長期的に強化することにもつながります。」

BIAとACS — 鍵となる要素とは？

	BUSINESS IMPACT ANALYSIS (BIA)	ASSET CRITICALITY SCORING (ACS)
目的	資産の障害が業務、収益、コンプライアンス、信頼にどのような影響を与えるかを理解する	技術的リスクとビジネスリスクに基づいて、各資産に定量的なスコアを割り当てる
焦点	混乱による機能的影響	意思決定のための優先順位付け情報
アウトプット	重要なビジネスプロセスを支える資産に関する定性的な洞察	パッチ適用、対応、レポート作成において使用される各資産の数値または段階別評価値
利用対象者	ビジネスリーダー、リスクマネージャー、セキュリティアーキテクト	セキュリティ運用、脆弱性管理、GRCチーム
関係性	BIAからのインプットはACSスコアリングに反映される	ACSはBIAの知見を日々のワークフローに組み込む

実践的な優先順位付け: 資産価値の階層的アプローチ

階層的なACSモデルは、リーダーに資産の重要度に関する明確かつ一貫した階層構造を提供します。最上位には、損なわれた場合に収益、コンプライアンス、またはブランド信頼を直接脅かす「至宝」が位置づけられます。

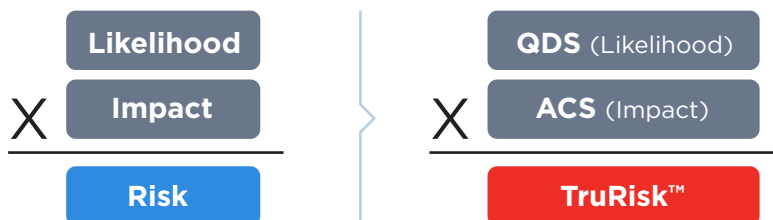
これらには、多くの場合、以下が含まれます。

- 顧客の個人情報（PII）を保持するデータベース
- 決済システムまたは金融取引システム
- ERPおよびサプライチェーンプラットフォーム
- 独自のコードリポジトリまたは知的財産ストア
- 顧客向けアプリケーションを備えた本番環境のクラウド環境

これらのシステムには、すべてのリスク管理プロセスにおいて最上位レベルのステータスを割り当ててください。

資産の重要度 – 事業への影響レベル

5	Severe (重大)	基幹インフラおよび収益を生み出すシステム。これらのシステムで障害が発生すると、業務が停止するか、壊滅的な損害が発生する。
4	Significant (重要)	基幹業務を支える高価値システムだが、重要なプロセスに直接結びついていないもの。
3	Moderate (中程度)	重要度は低いものの、不可欠な業務を支えるシステム。これらのシステムは業務継続性を支えるが、収益創出とは直接的な関係がないもの。
2	Minor (軽微)	障害発生の可能性が限定的なシステム。これらは日常業務に役立つが、事業継続性とは直接関係がないもの。
1	Negligible (低)	非必須資産。事業への影響はほとんど、あるいは全くない。事業運営や収益に大きな影響はない。



そこからさらに上の階層では、段階的に低いビジネスへの影響を捉えることで、資産全体の状況を見失うことなく意思決定を効率化します。

事後対応型からレジリエンス型へ

ビジネスインサイトと技術データの融合により、リスクの優先順位付けは事後対応型の慌ただしいものから、事前対応型の戦略へと変革されます。どの資産が最も重要かをより明確に把握することで、セキュリティチームは以下のことが可能になります。

- リスクを最も効果的に低減できる箇所に修復対策を集中させる
- ビジネス関係者と効果的にコミュニケーションを取る
- セキュリティ対策が企業目標と整合していることを示す
- 優先度の低い脆弱性に関するノイズや疲労を軽減する

資産の重要性を定量化し、それを運用リスクに関する意思決定に組み込むことは、組織の成熟度における転換点となる。つまり、単なるチェックリストへの記入から、組織が真に価値を置くものに基づいたレジリエンスの構築へと移行することを意味する。

ステップ 4

サイバーリスクの 伝達と追跡

実用的なビジネス インテリジェンス と長期的な回復力 のためのリスク指 標の再考

次々と新しいフロアが追加され、壁の形状が変わり、インフラがリアルタイムで再配置される超高層ビルを警備しようとする状況を想像してみてください。これが現代のセキュリティチームが直面する現実です。クラウド環境はオンデマンドで拡張され、アプリケーションは日々更新され、ビジネス戦略は四半期ごとに進化します。こうした変化の激しい状況下で、攻撃者は時代遅れの評価、静的な防御、そして断片化された可視性を悪用します。

優位性を維持するためには、セキュリティリーダーはリスクを技術的な指標からビジネス上重要な変数へと位置づけることが不可欠です。そのためには、リスクの測定方法と伝達方法を変えることから始めなければなりません。

リスク定量化の実践

リスク定量化は、現代のサイバーセキュリティプログラムの基盤です。パッチの量や深刻度スコアに埋もれるのではなく、先進的な組織は、技術的なシグナルをビジネスのコンテキストに沿った洞察に変換するプラットフォームとツールに投資しています。

この変化の核心にあるのは、次の2つの重要な問いです。

1. 脅威が悪用される可能性はどの程度か？

2. もし悪用された場合、ビジネスにどのような影響が出るのか？

脅威インテリジェンス、悪用可能性のコンテキスト、資産の重要度を組み合わせることで、セキュリティチームはリスクへのエクスポージャーだけでなく、その影響度に基づいて優先順位付けを行うことができます。

これにより、サイバーセキュリティを企業リスク管理や取締役会レベルの報告に統合することが可能になり、技術的なノイズを意味のある意思決定へと変換できます。

静的なレポートからリアルタイムな状況把握へ

従来の静的なリスクレポートは、現実世界の脅威とすぐに乖離してしまいます。組織には、状況の変化に合わせて進化するリアルタイムな状況把握が必要です。

そのためには、以下のものを導入する必要があります。

- **リアルタイムリスクスコアリング:** 新たな脆弱性や変化するビジネス環境に基づいて、リスクレベルが動的に更新されます。
- **自動追跡:** 重要な領域におけるリスク軽減策の効果を測定する組み込みメカニズム。
- **ステークホルダー別レポート:** 経営幹部、セキュリティチーム、運用部門向けにカスタマイズされたインサイトを提供します。

重要な指標を測るためのベンチマーク設定

効果的なコミュニケーションは、実際のビジネスリスクを反映した指標を設定することから始まります。

以下のような指標に注目しましょう。

- **リスク軽減の速度:** 最も影響の大きい脆弱性は、どの程度の速さで対処されているか？
- **リスクエクスポージャー期間:** 重要な資産は、既知の悪用可能な脅威に対して、どの程度の期間脆弱な状態に放置されているか？
- **リスク集中:** 特定の事業部門やシステムが、組織のサイバーリスクを不均衡に負担していないか？
- **運用上の回復力:** 組織は、重要なシステムへの攻撃に対して、どの程度耐え、復旧できるか？

これらを継続的に追跡することで、チームは集中力を維持し、方向性を一致させ、責任を果たすことができます。

リスクに関する対話を深化させる

最も効果的なプログラムとは、技術的なリスクをビジネスへの影響として具体化するものです。

つまり、リスクを次のような観点から捉えるということです。

- **業務中断:** どのようなリスクが重要なワークフローを停止させたり、規制上の義務に違反したりする可能性があるか？
- **財務リスク:** 侵害が発生した場合、どのようなコストが発生するか？また、セキュリティ対策によってそのリスクをどのように軽減できるか？
- **投資対効果:** セキュリティ投資がレジリエンス向上に貢献していることを示すことができるか？

リスクがビジネス用語で伝えられるようになると、セキュリティはコストセンターとしてではなく、長期的な回復力と競争優位性を得るための手段として認識されるようになる。

ステップ 5

リスクを排除する： 自信を持ってリードする

修復活動は、 起こりうる事態、 影響、および 予防可能性に基づいて行う。

サイバーセキュリティプログラムへの投資が増加しているにもかかわらず、セキュリティリーダーは、可視性と緊急性が高まる一方で、あらゆる事態に対応できる能力には限りがあるという、おなじみのジレンマに直面している。効果を実証するプレッシャーが高まるにつれ、最も効果的なプログラムは焦点を絞り込んでいる。単に問題に対応するだけでなく、ビジネスにとって最も重要な事柄に重点を置いた対応を行っているのだ。

その進化は、ダッシュボードの数を増やしたり、予算を増やしたりすることから始まるわけではありません。それは、目標を再定義することから始まります。パッチ適用作業から脱却し、業務継続性、コンプライアンス、そしてビジネスにとって重要な優先事項を支援する成果を提供することへと移行するのです。

事業運営の実態に合わせたリスク軽減策の策定

グローバル企業から急成長中のスタートアップ企業まで、セキュリティ責任者はそれぞれ異なるリソース環境に直面していますが、共通の課題は、サイバーセキュリティを、事後対応の繰り返しの消火活動ではなく、戦略的な事業推進力へと転換する方法です。

大企業、中堅企業、中小企業が直面する主要な課題



大企業

- 広大なインフラストラクチャ
- 分散型チーム
- 増大するコンプライアンス要件



中堅企業

- 少人数チーム
- 限られた予算
- セキュリティ投資対効果 (ROI)



中小企業/ スタートアップ

- セキュリティ専任リソースの不足
- 差し迫ったリスク以外には注意を払えない状況

大企業にとって、分散環境全体にわたって、ほぼリアルタイムでサイバーリスクを測定、伝達、そして対応できる能力は不可欠です。中規模組織の成功の鍵は、ノイズを排除し、インテリジェントな自動化を実現し、非技術系のステークホルダーにセキュリティの投資対効果（ROI）を示すことにあります。中小企業やスタートアップ企業は、優先順位やリソースの制約が全く異なるため、これらの懸念事項を抱えていないかもしれません。彼らの最優先事項は明確です。業務や評判を脅かす可能性のある最も緊急性の高いリスクを明らかにしつつ、複雑さを軽減するソリューションを導入することです。

これらのアプローチに共通するのは、最も効果的なところに努力を集中させるという意図です。

リスク低減のための4つの戦略

業界を問わず、先進的な組織が脆弱性管理を実践する方法に一貫した変化が見られます。これらの4つの戦略は、リスク低減を的確かつ目的意識を持って推進するための、新たなベストプラクティスを反映しています。

1. 明確な優先順位付けロジックを確立する

成熟したプログラムでは、脆弱性の悪用可能性、資産の重要度、脅威インテリジェンスを組み合わせる修復対策を導きます。これらの要素を統合したリスクビューを作成するスコアリングモデルを採用しているプログラムもあります。また、検出からの経過時間、ビジネスへの影響、規制上のリスクといった追加的なコンテキストを考慮に入れて、意思決定をよりの確に行うプログラムもあります。

目標は、誤検知とアラート疲労を最小限に抑えつつ、重大な脆弱性を確実に削減することです。

2. パッチ適用と修復ワークフローの効率化

高リスクの脆弱性が特定されたら、スピードが極めて重要になります。

高度に最適化された組織:

- 不足しているパッチを迅速に特定する
- 可能な限り展開を自動化する
- 修復中のダウンタイムを最小限に抑える

これらの組織では、セキュリティ、IT、コンプライアンスは円滑に機能する組織として機能し、ビジネスの円滑な運営と、ツールにおける優先事項の明確な連携を保証している。

3. MITRE ATT&CK を活用した脅威情報に基づく防御の優先順位付け

脆弱性と攻撃者の行動をマッピングすることは、脆弱性管理の成熟度を左右する重要な要素です。MITRE ATT&CK フレームワークは、チームが以下のことを実現するのに役立ちます。

- 攻撃者が特定の脆弱性をどのように悪用する可能性があるかを理解する
- 想定される脅威シナリオに沿った戦術に基づいて、修復の優先順位を決定する
- 理論上の深刻度から現実世界における関連性へと移行する

このアプローチは、サイバーセキュリティを技術的な衛生管理から戦略的な先見性へと高めるものである。

4. 単なる認識ではなく、行動を促すダッシュボードを構築する

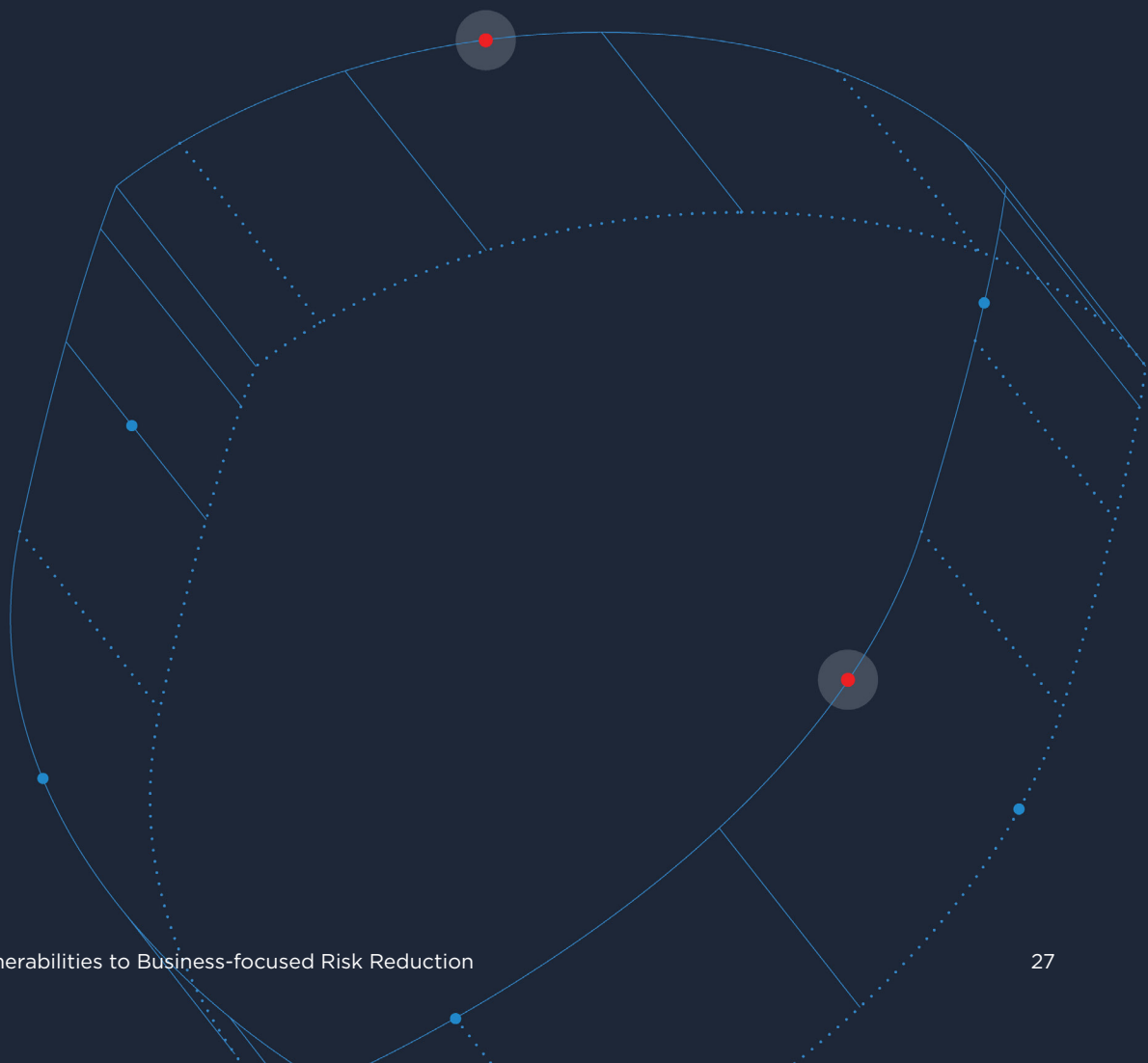
可視性は基本ですが、優先順位を決めるのはコンテキストです。先進的な組織は、ダッシュボードを単にデータ量を追跡するためだけでなく、リスクに関するストーリーを伝えるために活用しています。

- 上昇傾向にあるもの、下降傾向にあるものは何か？
- 残存リスクはどこに存在するのか？
- これらのリスクは、既知の脆弱性、業務システム、およびコンプライアンス要件とどのように整合しているのか？

単なるデータポイントではなく、行動を促すために構築されたダッシュボードは、セキュリティリーダーが役員会でリスクに関する言葉で自信を持って発言できるようになり、現場で意義のある変化を推進するためのツールを提供します。

サイバーセキュリティが企業の取り組みと融合し続ける中で、最も効果的な組織は、事後対応的な姿勢から、リスクを考慮した計画的な行動へと移行し、あらゆる対策が測定可能な成果につながる組織となるだろう。

より少ないリソースで より多くの成果を



Qualys TruRisk™で 変革をリード

単一プラットフォームでサイバーリスクを測定、共有、排除

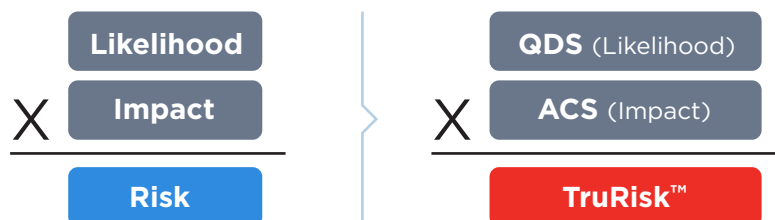
脅威が蔓延する現代において、明確な情報把握は貴重な資産です。毎年数万件もの新たな脆弱性が発見される中、セキュリティチームは優先順位付けが困難なまま、次々と発生する脅威のトリアージに追われています。その結果、意思決定の麻痺、リソースの誤配分、そしてビジネスにとって最も重要な部分を強化する機会の逸失といった事態が生じています。

ここでQualys TruRisk™が重要な役割を果たします。単なるツール群の一つとしてではなく、セキュリティ戦略と企業価値を整合させるためのレンズとして機能し、リアルタイムのエクспロイトインテリジェンス、資産の重要度、動的な状況認識を組み合わせることで、技術的な脆弱性を定量化されたビジネスリスクへと変換します。その結果、組織の現状と取るべき行動を、常に最新の情報に基づいた統一的な視点から把握できるようになります。

Qualys Detection Score (QDS) を活用したこのアプローチは、チームが単なるCVEの深刻度評価にとどまらず、より高度な分析を行うのに役立ちます。脆弱性とはもはや単独で評価されるのではなく、実際の攻撃動向を踏まえて評価されるため、推測ではなく、発生可能性とビジネスへの影響に基づいて優先順位付けが可能になります。

脅威発生可能性 - Qualys検出スコア (QDS)

技術情報	CVSS、QIDに登録されているCVEの中で最も高いQVS。
時系列情報	脅威インテリジェンス（エクспロイトコードの成熟度、マルウェア、トレンド、脅威アクターの活動など）。
CID	修復対策およびコンプライアンス／リスク軽減策。



リスクポスチャーは継続的に測定され、あらゆる修復対策決定が状況にどのような影響を与えるかが明らかになります。リアルタイムの視覚的な分析により、技術データはビジネスに即した指標（現在のリスク、アクティブな脅威、修復対策のスピードなど）に変換されます。これらは、セキュリティオペレーションセンター（SOC）だけでなく、経営陣にとっても重要な指標です。

TruRisk™は、IT、セキュリティ、ビジネスチーム間で共通のリスク用語を構築することで、従来の縦割りのサイロ構造を解消します。その結果、より一貫性があり、責任感のある意思決定が可能になり、セキュリティ対策は緊急対応から、より集中的な実行へと移行します。

絶え間ない複雑さに満ちた状況において、このモデルはノイズをより扱いやすくするだけでなく、シグナルをより意味のあるものにします。サイバーセキュリティをビジネスパフォーマンスの推進力として捉え直し、組織がより迅速に、そしてより賢く優先順位付けできるよう支援します。そして、そうすることで、セキュリティを事後対応的な必要性から、回復力と成長を促進する積極的な手段へと変革します。

結論

ビジネスに即した戦略的なセキュリティ: セキュリティ対策からビジネスへの影響へ

今日のセキュリティリーダーは、防御にとどまらない、より幅広い役割を担うようになっています。リスクとビジネス成果を結びつけ、投資判断に影響を与え、組織の成長と適応のあり方を形作っています。リスクはもはや静的な指標ではなく、行動を促す動的なシグナルなのです。

この変革は理論上の話ではなく、既に始まっている。先見性のあるチームは、戦略策定の議論にリスクを組み込み、部門横断的な優先事項と連携させ、セキュリティを単なる保護手段ではなく、事業運営の不可欠な要素として位置づけている。

TruRisk™は、チームが重要な事柄を定量化し、進捗状況を追跡し、迅速に行動できるよう支援することで、この進化を支えます。エクスプロイト情報、資産の重要度、リアルタイムのエクスポージャーデータを統合することで、業務の中断、信頼の失墜、収益への影響といった潜在的なリスクを明らかにします。

このモデルでは、デジタル信号はリスクを単に記述するだけでなく、決定的な動きを明らかにし、ビジネスリスクを管理可能で実行可能なものへと変えます。未来は、役員会議室に入って「これが重要なリスクです。理由はこうです。そして、私たちはこれに対してこう対処しています」と言えるリーダーたちのものです。

セキュリティの役割は、ゲートキーパーからイネーブラーへと進化しています。そして、セキュリティが明確な方向性を示すことで、企業は自信を持って前進できるようになります。

リスクベースセキュリティへの移行は既に始まっています。次のステップは、明確な洞察に基づき、目標に沿って、目的意識を持ってそれを適用することです。

洞察から行動へ 移行しよう

リスクという概念は普遍的に理解されているものの、その管理方法こそが差別化要因となる。複雑さを解消し、真に重要なことに焦点を当て、可視性をビジネス成果に結びつける能力こそが、リスクを単なる指標から戦略的価値を高める原動力へと高めるのである。

**Qualys TruRisk™プラットフォームの活用方法をご覧ください。
詳しくはこちら:**

- 脆弱性だけでなく、真のリスクを定量化する方法
- 自動化によって無駄な労力を削減し、意思決定を迅速化する方法
- 経営陣の共感を呼ぶリスクストーリーの伝え方

より強力でスマートなセキュリティ対策はここから始まります。
可能性は無限大。ぜひご自身で探求してみてください。



**Qualys TruRisk™を活用することで、リスクに基づいた意思決定が
理論から測定可能な行動へとどのように移行するかをご覧ください。**

評価版を申し込む

www.qualys.com/free-trial-new/

Qualysについて

1999年にSaaSセキュリティ企業の草分け的存在として設立されたQualysは、主要なクラウドプロバイダー、マネージドサービスプロバイダー、コンサルティング組織と戦略的パートナーシップを構築してきました。また、同社はクラウドセキュリティアライアンス（CSA）の創設メンバーでもあります。