sysdig

セキュリティリーダーのための、将来を見据えた実践的脆弱性管理戦略ガイド

著者
プロダクトマーケティング部門マネージャー　Matt Kim

脆弱性管理は、日々巧妙化・加速するサイバー脅威との継続的な戦いの最前線を担っています。本稿は、セキュリティリーダーが今日の進化する脅威に打ち勝つための実践的なガイダンスを提供します。統合された脆弱性管理とよりスマートな優先順位付け（リスクベース評価）により、アクティブなリスクに即応し、攻撃者より常に一歩先を行くセキュリティ体制の構築方法をご紹介します。

目次

巧妙化するサイバー脅威に勝つ、統合された脆弱性管理とよりスマートな優先順位付け

今日の脅威ランドスケープにおいて、脆弱性管理（VM）は、もはや“チェックリストの項目”ではありません。それは、日々高度化する攻撃者と対峙する、最前線の防衛手段なのです。攻撃者は常に進化を続け、新たな戦術・ツール・手法を投入してきます。防御者である私たちは、ゼロデイ対応、深夜のインシデントコール、優先順位付けのせめぎ合いといった課題と日々向き合っています。一方で、攻撃者には「一度の成功」で十分。だからこそ、私たちは常に一歩先を行く必要があるのです。

セキュリティリーダーの使命は、単に終わりのない脆弱性リストを追いかけることではありません。真の課題は、脅威に打ち勝つために設計された、動的かつ統合的な最新の脆弱性管理プログラムを構築することにあります。

本稿では、セキュリティリーダーが直面する現実的な課題に立ち向かうための、実践的なガイダンスを提供します。目的は単なる情報提供ではありません。このガイドは、ノイズに埋もれがちな脆弱性情報の中から“本当に対応すべきリスク”を見極め、攻撃者よりも一歩先を行くための戦略的な脆弱性管理プログラムの構築を支援するものです。

脆弱性の渦：大量のアラート、データ、そして遅延

エンタープライズITランドスケープは今、イノベーションと相互接続性を原動力とした“ハイパーコネクテッド”なエコシステムへと変貌を遂げています。この変化は、ビジネスの成長と柔軟性を加速させる一方で、セキュリティリーダーにとっては“アタックサーフェスの拡大”という新たな悪夢を生み出しました。

このような複雑性の増大は、特にクラウドインフラへの移行において顕著に表れています。クラウドは、企業や組織のアプリケーションの構築方法とデプロイ手法に変革をもたらし、迅速なイノベーションを可能にしています。しかしその一方で、オープンソースコンポーネントやサードパーティ製ソフトウェアへの依存度が急速に高まり、それが新たなセキュリティリスク、特に高度化するサプライチェーン攻撃の土壌となっています。これらの外部コンポーネントは、ビジネスの成長を支える重要な要素である一方、攻撃者にとっての“新たな侵入口”を生み出し、信頼していたソフトウェア自体が脆弱性となるリスクを孕んでいるのです。

クラウド技術の導入、ハイブリッドインフラの運用、リモートワークの普及は、組織にもたらす業務効率の向上という恩恵において、これまでにないインパクトを与えています。しかしその一方で、こうした進化は組織をかつてないほど多くの脆弱性にさらしているのも事実です。さらに、それらの脆弱性の特定、優先順位付け、修正、軽減といった一連の対処プロセスも、環境の複雑化により著しく困難になりつつあります。

脆弱性管理を真にモダナイズするためには、まずその複雑性の本質を理解することが不可欠です。

あまりにも大量のアラートやノイズがセキュリティチームを疲弊させている

セキュリティチームは、すでに限界に達しつつあります。毎日何千件ものアラートが飛び交い、しかもその一つひとつが“緊急度高”とマークされている中、すべてに対応するのはもはや不可能です。脆弱性は山積みとなり、それらを適切に優先順位付けするために必要な「コンテキスト」も不足している状態です。。その結果、混乱と疲弊が重なり、チームの士気が低下していきます。

驚くべきことに、侵害の60%は、すでに修正プログラム（パッチ）が存在する脆弱性が放置されていたことが原因で発生しています[1]。なぜパッチが適用されないのでしょうか？理由は明白です。セキュリティチームが、あまりに多くの“ノイズ”に囲まれ、本当に重要な脆弱性にまで手が回らないからです。

60%

の侵害は、修正プログラムが提供されているにもかかわらず、脆弱性にパッチが適用されていないことが原因で発生しているのです。

1 Ponemon Institute. Cost and Consequences of Gaps in Vulnerability Response

アラートの数が多すぎることだけが問題なのではありません。ノイズがあまりにも多いために、セキュリティチームは“サバイバルモード”に陥り、どの脆弱性が最も高いリスクをもたらすのかを十分に把握できないまま、対応可能な範囲でトリアージを行っているのが現状です。深刻度スコアだけで判断できることには限界があり、複数のリスク要因を考慮した追加のコンテキストが必要です。それが欠落したままだと、重大な脆弱性を見逃したり、重要度の低い脆弱性にリソースを浪費したりするおそれがあります。さらに懸念されるのは、こうしたコンテキストが不足している状況では、チームが注力すべき範囲を正しく絞り込めなくなるという点です。たとえば、脆弱性の深刻度が高くても、それが悪用不可能なワークロードに存在する場合、直ちに対応すべき対象からは外れる可能性があります。このような状況では、チームはその脆弱性への対応を後回しにし、外部に公開されているリソースに影響を与える脆弱性の対応を優先する判断ができるようになります。

最も重大なリスクに優先順位を付けること—それは不可能なタスクである

本当に重要なのは、「どこに作業リソースを集中させるべきか」を自信を持って把握できることです。脆弱性は、さまざまなソース、プラットフォーム、セキュリティツールから報告されるため、その情報を統合するだけでも組織全体を巻き込んだプロセスが必要となります。しかも、これはまだ“出発点”にすぎません。そこからさらに、深刻度やリスクに基づいて個々の脆弱性を精査し、優先順位を付けていく作業は、膨大な時間と人的コストを伴い、スケーラブルではありません。

この課題は非常に複雑です。実際、セキュリティ専門家の72%が、脆弱性の優先順位付けの難しさが対応の遅れの主な原因であると回答しています[2]。

72%

のセキュリティ専門家が、脆弱性の優先順位の難しさが対応の遅れの主な原因であると回答しています。

2 Ponemon Institute. Cost and Consequences of Gaps in Vulnerability Response

修正の進捗状況を追跡する際の隠れた障害

例えセキュリティチームが脆弱性への対応計画を策定したとしても、課題が終わるわけでありません。実際、組織の32%が、修正の進捗状況を追跡することが、セキュリティリスクの管理における最も困難な課題の1つであると回答しています[3]。そして脆弱性が本当に修正されたかどうかことを直接検証できない限り、その脆弱性が確実に対処されたという確信を持つことはできません。

32%

の組織が、修正の進捗状況を追跡することを、セキュリティリスクの管理における最も困難な課題の1つであると回答しています。

さらに、責任の所在が不明確であることも、脆弱性対応を妨げる大きなハードルの1つです。誰の担当かが明確でないという理由だけで、修正作業が停滞してしまう可能性があります。

その結果、脆弱性が報告されてから数ヶ月経っても未対応のまま放置されるといった事態が、現実に発生しています。加えて、チームが日々の対応に追われている状況では、修正作業の進捗状況を追跡・検証する余力がなくなり、問題がさらに深刻化するリスクも高まります。

さまざまなツールが散在しているものの、統一された可視性は存在していない

セキュリティ業界は、自らが開発・導入したツールに強い信頼と愛着を持っています。しかし、脆弱性管理に使用されるツールの数があまりに多く、それらがインフラ全体や開発ライフサイクルの各所に分散している状況では、運用の一貫性が損なわれ、全体が混乱に陥りやすくなります。実際、開発チームとセキュリティチームは、それぞれ異なるツールセットと異なるデータソースを基に作業しており、共通の前提や認識を持たないまま並行して動いているのが現状です。

その結果、セキュリティチームは、複数のツール（それぞれ独自のインターフェイスとワークフローを持ち、癖のあるツール）を習得するために多くの時間を費やすか、あるいは別のプラットフォームからの情報更新を他チームに頼らざるを得ない状況に追い込まれます。いずれの場合も、作業は遅延し、コミュニケーションの齟齬が拡大していきます。さらに深刻なのは、チームが脆弱性に関する統一されたビューを持てなくなることです。このような包括的な可視性が欠如した状態では、どこに注意を集中させるべきかを正しく判断することは不可能です。例えば、最も重大な脆弱性はどれでしょうか? 後回しにできる軽微な問題はどれでしょうか? といった問いに答えようとしても、それはまるでピースの半分が欠けており、さらに残りのピースも複数の箱に分散しているパズルを解こうとしているようなものです。

セキュリティチームが信頼できる唯一の情報源を持たない場合、それはまるで片足を縛られ、目隠しをされた状態でレースを走っているようなものです。彼らは十分な速さで動けず、正しい方向へ進んでいるかどうかさえ分からなくなります。

3 Hyperproof: **2024 IT Risk and Compliance Benchmark Report**

脆弱性管理の詳細

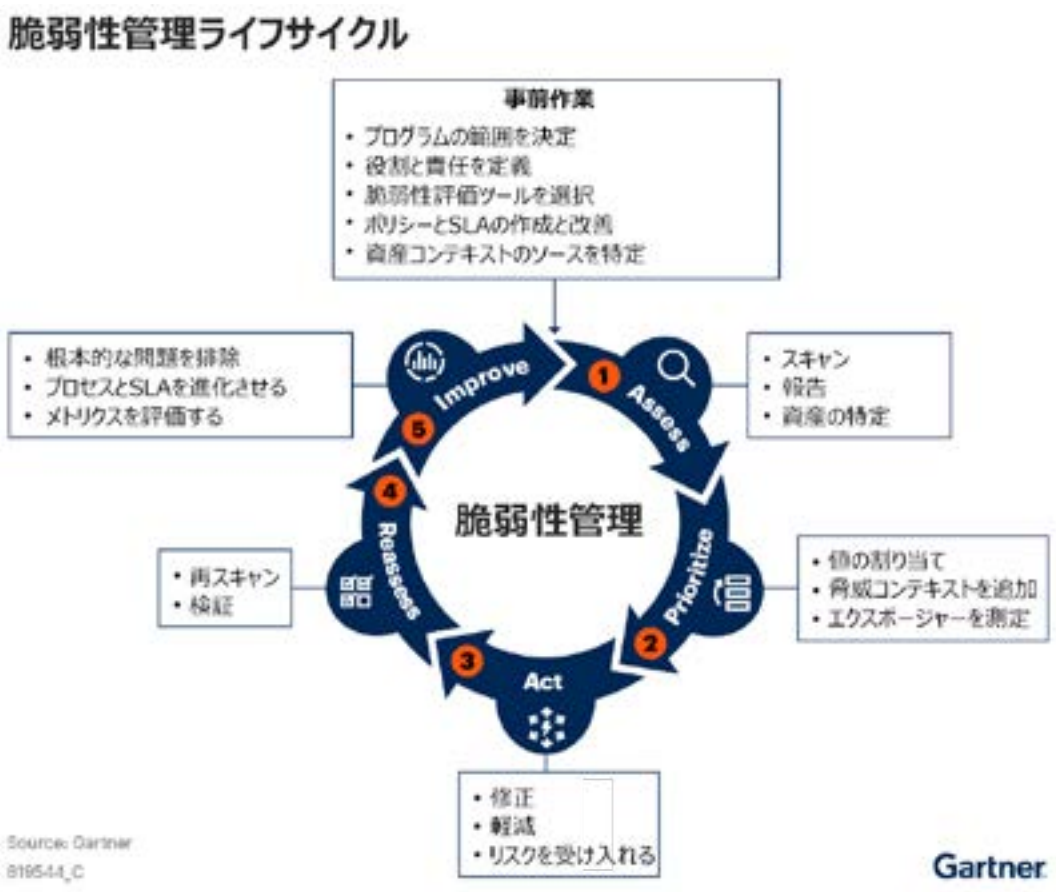
あらゆる組織のインフラは、サーバー、アプリケーション、クラウドワークロード、オープンソースコンポーネントなど、多層的な構造によって成り立っています。このような複雑な環境においては、脆弱性が入り込むことを完全に防ぐのは困難です。たとえば、サーバーの設定ミス、古いアプリケーション、パッチが適用されていないオープンソースのライブラリ、チーム間で見落とされた修正など、これら一つひとつの弱点が、潜在的な攻撃の足がかりとなる可能性があります。

まさにこれこそが、強力な脆弱性管理の実践が不可欠となる理由です。脆弱性管理は、単なるセキュリティ対策のひとつに止まるものではありません。それは、堅牢なセキュリティ戦略を支える予防の要となる重要な基盤です。的確な脆弱性管理を実現することで、攻撃者がリスクを悪用する前に、脆弱性を特定し、リスクの度合いに応じて優先順位を付け、的確かつ迅速に修正することが可能になります。

脆弱性管理の変革

脆弱性管理は、何十年もの間、サイバーセキュリティの「縁の下の力持ち」として機能してきました。派手さはなく、その成果が現れても、ニュースの見出しになることはほとんどありません。しかし、実際には脆弱性管理こそが、システムを積極的に守ることと、侵害発生時に慌てて対応することの違いを生む、決定的な分岐点 なのです。

一方、企業のIT環境は日々変化し続けており、脆弱性管理もその変化に遅れず進化していく必要があります。とりわけ、クラウドネイティブのような、複雑化が進むインフラ環境や、巧妙さを増す攻撃者の手口に対応するためには、従来型のアプローチでは不十分です。5年前あるいは昨年まで有効だった対策が、今では 通用しなくなっているという現実を、私たちは直視しなければなりません。企業や組織が脅威に対して常に一歩先を行くためには、脆弱性管理の進化の軌跡を理解するとともに、現在市場が どこに向かっているのかを把握することが不可欠です。



コンプライアンスファーストの時代

かつての脆弱性管理は、主にコンプライアンス要件の遵守を目的としていました。一定の間隔でスキャンを実行し、目立った問題にパッチを適用した後は、それで対応を完了とみなすのが一般的でした。このプロセスは、実際にシステムを守るためのものというよりも、監査人を安心せることを目的として設計された運用だった、と言えるでしょう。こうしたアプローチは、当時の現場では一定の効果を持っていたかもしれません。しかし、今では、急速に拡大・複雑化するアタックサーフェスに対応するには明らかに限界があります。

スキャンの頻度が低かったことで、脆弱性は長期間にわたり放置され、攻撃者にとってはパッチ未適用の脆弱性を悪用する“十分な時間”が与えられていました。さらに、特定された脆弱性の数が膨大に上ったことで、セキュリティチームはすぐに圧倒され、最も重大なリスクに優先順位を付けて対処することがほぼ不可能な状況に陥りました。同時に、急拡大するアタックサーフェスに対する可視性が不十分だったため、多くの脆弱性がそもそも検知されることなく見過ごされていたのです。

静的なリスクベースの優先順位付け

セキュリティ環境の変化に伴い、脆弱性管理に対するアプローチも変化してきました。従来の手法に代わって登場したのが、リスクベースの脆弱性管理です。この新たなアプローチにより、チームはもはやすべての脆弱性を“平等に扱う”のではなく、悪用可能性、資産の重要度、ビジネス影響などの要素に基づいて優先順位を付けるようになりました。

これは、脆弱性管理における大きな前進と言えます。しかしながら、クラウドネイティブやハイブリッド環境が急速に拡大する中で、このアプローチだけでは十分ではありません。現実には、多くのチームがいまだに高優先度”分類される大量の脆弱性に圧倒されており、それらの中から本当に対処すべきものを見極めるために必要な“コンテキスト”が欠落しているのです。

クラウド環境では、多くの場合、静的なリスクベースの手法では、クラウドやソフトウェア開発パイプラインのスピードとスケールにネイティブかつシームレスに対応することが困難です。一方でチーム、オンプレミス環境とクラウド環境の間にまたがる、断片化された可視性とサイロ化されたツール群を操作せざるを得ません。その結果として、対応プロセス全体が複雑化・長期化し、応答時間に遅れが生じるという深刻な課題が発生しています。

クラウドネイティブVMへの市場シフト

クラウドネイティブインフラとハイブリッド環境の台頭は、脆弱性管理をその限界にまで押し上げています。このようなプレッシャーが、脆弱性管理市場の革新を促し、オンプレミス環境とクラウド環境の間にある隔たりを埋めるような、クラウドネイティブソリューションを生み出したのです。

クラウドネイティブ時代の脆弱性管理は、多様化するインフラ全体における可視性を統合することで、従来のレガシーシステムでは実現できなかったレベルの精度とスピードで脆弱性に対処する力をセキュリティチームにもたらします。このような変革は、企業や組織における 脆弱性管理 のアプローチそのものをへんかさせると同時に、リスクの特定、優先順位付け・対応といった一連のプロセスを、よりスマートで効率的なものへと導きます。

クラウドネイティブの脆弱性管理で、セキュリティオペレーションをモダナイズする

ハイパーコネクテッドなエコシステムを効果的に保護するには、クラウドネイティブ環境が持つ動的かつ変化しつづける特性に対応できる、柔軟でスピード感のある脆弱性管理ソリューションを優先的に採用する必要があります。

以下では、クラウドネイティブ脆弱性管理（VM）ソリューションにおける、5つの主要なフォーカスエリアをご紹介します。このソリューションは、プロアクティブな保護とスケーラブルなリスク管理の両方を可能にします。

フォーカスエリア01

エージェントレスおよびエージェントベース – 2つのアプローチが生む柔軟性と可視性

エージェントレス型のデプロイメントは、クラウド環境における脆弱性管理のモダナイズを加速するアプローチです。エージェントを導入することなく、大規模な環境に対して迅速かつ低メンテナンスで脆弱性スキャンを実現できるため、特に導入初期や広範囲のスキャンにおいて高い効果を発揮します。セキュリティチームは、単一の統合ソリューションを通じて、環境全体にわたる広範なカバレッジを即座に実現し、運用への影響を最小限に抑えつつ、すぐに価値を提供できるようになります。

さらに、クラウドプロバイダーのAPIを活用することで、既存ボリュームのスナップショットを迅速に生成・分析し、脆弱性を検出するプロセスを効率化できます。このようなスピードとシンプルさを兼ね備えた特性により、エージェントレス型のスキャンは、「将来を見据えた脆弱性管理の基盤」として業界から高く評価されています。

しかし、多くのケースにおいては、エージェントレス型スキャンだけでは必要とされる“可視性の深度”を十分にカバーできない可能性があります。この課題こそが、クラウドネイティブ脆弱性管理（VM）ソリューションにおいて、エージェントレス型とエージェントベース型、両方のデプロイメント方式を統合する必要がある理由です。

特により深いインサイトが求められる状況では、eBPFテクノロジーを活用した軽量エージェントの導入が有効です。このエージェントは、カーネルレベルで動作し、プロセスの実行、ファイルアクティビティ、ネットワーク接続といったランタイムの挙動に関するリアルタイムの可視性を提供します。脆弱性管理の観点からは実行中のアクティブなパッケージ内で存在する脆弱性を隔離・特定できることが特に重要であり、こうしたリアルタイムスキャンを可能にするのが、エージェントベースの強みです。

エージェントレスとエージェントベース、双方のアプローチを統合したソリューションは、両者のメリットを活かすことで、インフラ全体に対する継続的かつリアルタイムにスキャンを可能にします。このような柔軟かつ包括的な戦略により、クラウドプレゼンスやインフラの拡大に応じてセキュリティポスチャーを動的に適応させることができ、変化の激しい時代のIT環境に対応するシンプルさと堅牢性の両立を実現します。

フォーカスエリア02

包括的なカバレッジにより、あらゆる最新ワークロードに対して一貫性のあるアプローチを実現

今日の複雑なIT環境において、モダンな脆弱性管理には、広範かつ深層的なカバレッジを提供する能力が求められています。その実現の第一歩は、 ハイブリッドインフラと多様化するソフトウェア開発ライフサイクルのニーズの両方に対応できる、単一かつ統合されたソリューションの採用です。理想的な脆弱性管理ソリューションは、次の3つの主要分野に置いて卓越した機能を備えている必要があります。

→ **多様なワークロードのスキャン**

新たな脅威の一歩先を行くためには、クラウドネイティブな脆弱性管理ソリューションが 、あらゆるワークロードを包括的にサポートできる必要があります。この「ワークロード」には、オンプレミスサーバー、コンテナ、Kubernetes クラスター、サーバーレスアーキテクチャといったクラウドネイティブ環境全体、そしてその中間に位置するあらゆる構成が含まれます。包括的なワークロードスキャンを実現することで、ワークロードの種類や配置場所、運用形態にかかわらず、セキュリティカバレッジに“盲点”を残すことなく保護を提供することが可能になります。

→ **ライフサイクル駆動型のセキュリティ**

脆弱性の多くは、開発ライフサイクルのごく初期、すなわちソースコードそのものに起因して発生します。したがって、堅牢なセキュリティソリューションは、開発・ビルドフェーズから、ストレージ、さらにはランタイムに至るまで、ライフサイクル全体を対象とする必要があります。各フェーズにおいて可視性とスキャン機能を提供し、DevSecOpsのワークフローと完全に統合されたソリューションを活用することで、セキュリティチームは脆弱性への早期対応が可能になります。その結果、リスクを効果的に軽減し、後工程への影響や混乱を最小限に抑えることができます。

→ **スタック全体におけるシームレスな統合**

カバレッジの観点では、ワークロードやライフサイクルに加え、パートナーシップや統合の強化も欠かせません。優れたセキュリティソリューションは、CI/CDやDevOpsツール、アラート・チケット発行システム、さらにはクラウドプラットフォームに至るまで、テクノロジースタック全体にわたる主要なツールやプラットフォームとのシームレスな連携を実現する必要があります。

フォーカスエリア03

運用中のリソースに着目した、賢明な優先付け

あらゆるものが「重要」に見えてしまうと、セキュリティチームはすぐに圧倒され、終わりの見えない脆弱性のバックログに追われることになります。こうしたノイズを排除するには、コンテキストと現実世界のリスクに基づく、インテリジェントな優先順位付けが不可欠です。最新の脆弱性管理は、実行時に実際にロードされる脆弱なパッケージに焦点を当て、対応すべき対象を明確にします。

このように、よりスマートでコンテキストを重視したアプローチは、差し迫った脅威をもたらさない脆弱性への不要な対応に費やす時間と労力を大幅に削減します。注目すべきは、深刻度が高く修正プログラムが提供されている脆弱性のうち、実際に実行時に使用されているものはわずか5.4%に過ぎないという事実です[4]。このごく一部にフォーカスすることで、最も重要で、かつ現実に悪用されうる脆弱性への対応にリソースを集中できます。

4 Sysdigの**2025年版クラウドネイティブセキュリティおよび利用状況レポート**

このような脆弱性の優先順位付け方法に関する要件

理想的なクラウドネイティブの脆弱性管理ソリューションは、単にCVSSスコアに依存するのではなく、以下のような複数の優先順位付け基準を組み合わせたフレームワークを提供する必要があります。

- **修正プログラムの利用可能性**

  修正プログラムが利用可能な脆弱性を強調表示します。

- **実行時に使用中**

  実行時にアクティブにロードされ、実行されているパッケージに関連する脆弱性を優先します。脆弱性が使用されていない場合、その脆弱性は悪用可能ではありません。このような理由から、これは注意が必要な脆弱性を優先するための重要なフィルタリングメカニズムとなります。

- **実践的なリスクベースのコンテキスト**

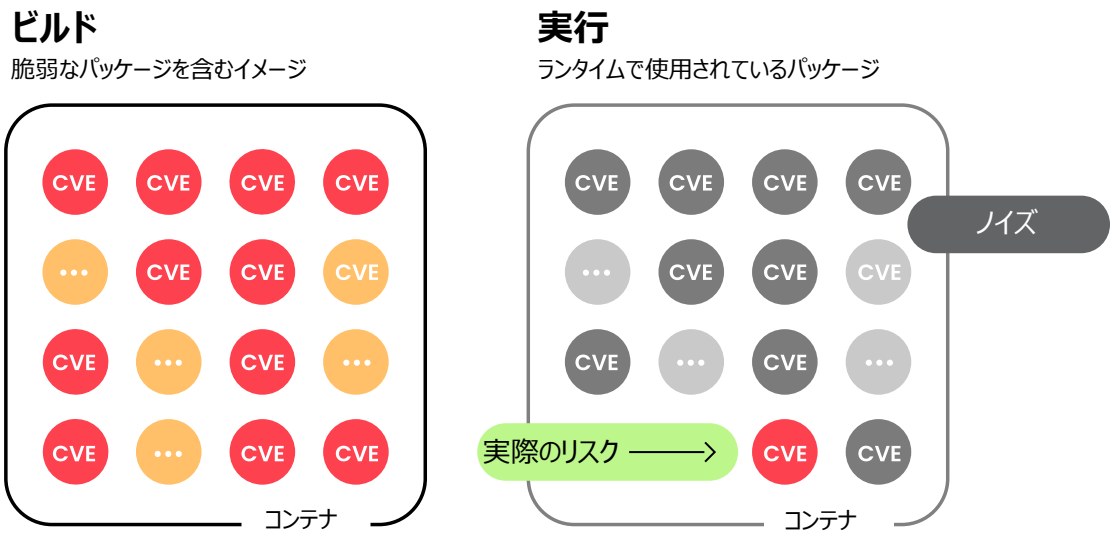
  ランタイムデータを詳細なコンテキストと結び付けることで、より実用的なインテリジェンスが得られます。このコンテキストには、対象のパッケージがインターネットに公開されているかどうか、または重要資産に関連しているかどうかといった情報が含まれます。こうした情報に基づく判断は、理論上の脅威ではなく、現実に影響を及ぼす可能性の高い脅威に優先的に対応するための基盤となります。

- **悪用可能性**

  既知のエクスプロイトが存在する脆弱性に優先的に対応します。これらの脆弱性は、システムに対して即時かつ現実的な脅威をもたらします。こうした「今そこにある危機」に焦点を当てることは、限られたリソースを最も重大なリスクの軽減に向けて効果的に活用するうえで不可欠です。

「使用中」に基づく優先順位付けとは、現在のインフラ環境に即した脆弱性管理戦略を構築することを意味します。実際に稼働しているコンポーネントやサービスに関する情報を活用することで、セキュリティチームは、より正確かつ効率的にリスクの高い脆弱性を特定し、対処の優先順位を明確に定めることができます。こうしたアプローチにより、対応すべき課題と後回しにできる課題とを切り分けることが可能となり、限られたリソースを最大限に活用することができます。

このアプローチは、現実の脅威に的を絞ることで、セキュリティチームが優先度の低い作業に振り回されるのを防ぎ、真に重要なリスクに対して迅速かつ的確な対応を可能にします。



フォーカスエリア04

自動修正により、攻撃者を凌駕するような対応を実現

セキュリティ対応において、時間は最大の武器です。Sysdigの調査によれば、攻撃者はわずか5分で脆弱性を悪用し、実害を引き起こす可能性があります。つまり、脆弱性が悪用される前に対応できるかどうかが、組織のリスクを大きく左右します。セキュリティチームには、かつてないスピードでの修正が求められています。

これこそが、新世代のVM（脆弱性管理）ソリューションが非常に強力である理由です。従来の手法を超えて、よりスマートな優先順位付けと自動化された修正ワークフローを備えることで、脆弱性の識別から修正に至るまでの一連のプロセスをシームレスに移行・最適化できます。

自動化されたワークフロー

クラウドネイティブの脆弱性管理ソリューションは、対応時間を最小化するために、統合された自動化ワークフローを提供する必要があります。その中核には、以下のような機能が含まれます。

→ アラートとチケット発行

重大な脆弱性が検出された場合、統合された自動化ワークフローは、まずリアルタイムのアラートを生成し、次いで既存のITサービス管理（ITSM）ツール内で対応チケットを自動作成します。このプロセスにより、脆弱性管理の一連の対応がシステム的に開始され、アラートおよびチケットは責任範囲に応じて適切なチーム（DevOps、セキュリティ、ITなど）へと自動的にルーティングされます。こうした自動化によって、適切な担当者に対して即座に通知が届き、手動によるトリアージの遅延を排除することで、迅速かつ的確な対応が可能になります。

→ 実用的な推奨事項

VMソリューションには、明確かつ実行可能な修正手順の提供が求められます。具体的には、修正可能な脆弱性を特定し、それぞれを適切なパッチやアップデートと関連付けることによって、対応チームが「次に何をすべきか」を考える時間を削減できます。これにより、判断の遅延を防ぎ、修正作業に即座に着手することが可能になります。さらに、修正アクションの優先順位は、影響範囲や重要性に基づいて決定されるべきです。特に、多数のワークロードやクリティカルな資産に関係する修正は、最優先で対応する必要があります。このような優先順位付けにより、限られたリソースを最大限に活用し、リスクを効果的に低減することができます。

→ 統合された修正ワークフロー

クラウドネイティブのVMソリューションは、ITSM、DevOps、修正ツールとのシームレスな統合を実現します。この統合により、セキュリティチームや開発チームは、既存のシステムやワークフローの中で直接アクションを実行できるようになります。たとえば、脆弱性が検出された際には、ITSMツールでのチケット作成、構成管理ツールによる設定変更、CI/CDパイプライン内での自動パッチ適用、あるいは問題のある変更のロールバックといった対応を即座に行えます。こうした運用の自動化と統合により、対応のスピードと正確性が大幅に向上し、セキュリティリスクを最小限に抑えることが可能になります。

→ リアルタイムの追跡とレポーティング

統合型VMソリューションは、修正の進捗を継続的に可視化できる必要があります。そのためには、直感的に理解できるダッシュボードと、詳細かつ信頼性の高いレポート機能を備えていることが求められます。これにより、修正作業が確実に実行され、コンプライアンス要件を満たしていることを、明確な証拠として示すことが可能になります。このような可視性を提供することで、セキュリティの取り組みに対するパフォーマンスを定量的に評価でき、関係者に対して進捗や成果を透明性の高い、データ駆動型の方法で伝えることができます。

フォーカスエリア05

ソフトウェアサプライチェーンの保護

ソフトウェアサプライチェーンのリスクは、最も制御が難しく、かつ最も深刻な脅威のひとつです。その根本的な理由は、現代のソフトウェア開発が社内作業だけにとどまらず、オープンソースライブラリやサードパーティ製の依存関係、コンテナイメージ、その他多数の外部コンポーネントによって構成される「アセンブリプロセス」へと進化しているためです。このような開発モデルはスピードと柔軟性を飛躍的に高める一方で、供給元の安全性や真正性を完全に把握・管理することが困難となり、結果として深刻なセキュリティリスクをもたらします。

多くの企業や組織は、サードパーティ製ソフトウェアの開発状況について十分な可視性を持っておらず、ソースコードへのアクセスも制限されているため、セキュリティ対策が適切に講じられているかどうかを確認する手段がありません。このような状況下では、1つのライブラリがハッキングされたり、検証されていない依存関係が含まれていたりするだけで、システム全体が重大なセキュリティリスクにさらされる可能性があります。実際、攻撃者がこうしたソフトウェアサプライチェーンの脆弱性を標的とする事例は急増しています。なぜなら、攻撃者は1つの脆弱なコンポーネントを悪用することで、数多くのアプリケーションやシステムに連鎖的な影響を与えられるという、きわめて効率的かつ破壊的な攻撃手段であることを理解しているからです。

クラウドネイティブの脆弱性管理ソリューションは、ソフトウェアサプライチェーンが抱える深刻なリスクに正面から対処するために、必要不可欠な可視性と制御機能を提供します。理想的なソリューションには、以下のような機能が含まれるべきです。

層化された分析

最新のアプリケーションは、多くの場合コンテナ化されたアーキテクチャを採用しており、セキュリティ管理にさらなる複雑さを加えています。各コンテナイメージは複数のレイヤー（層）で構成されており、それぞれが独自の依存関係、構成情報、あるいは脆弱性を含んでいる可能性があります。このため、1つの脆弱性の根本的な発生源を特定する作業は、まるで干し草の山から針を探すような困難を伴います。

クラウドネイティブソリューションは、コンテナイメージをレイヤー単位で分解・解析することで、脆弱性の特定と修正をより簡素化します。このようなきめ細かな可視性により、セキュリティチームは脆弱性の正確な発生源を迅速に特定できるため、修正作業を加速させるだけでなく、問題を根本から解消することが可能になります。その結果、下流工程でのリスク発生を最小限に抑えることができます。この精度レベルの対応は、無駄な推測や手戻りを避け、チームが効率的かつ確実に脆弱性へ対応できる体制を支えます。

イメージの系譜

脆弱性の起源を追跡することは、迅速かつ効果的な対応の鍵となります。脆弱性が発見された際には、それがどのように発生したのか、そしてシステム全体に与える影響を正確に把握することが不可欠です。このような起源の特定は、単なる修正にとどまらず、将来的な再発防止にもつながります。クラウドネイティブの脆弱性管理（VM）ソリューションは、イメージの「系譜」を可視化することで、こうした追跡を可能にします。具体的には、コンテナイメージの履歴や派生元をマッピングし、脆弱性が導入されたタイミングや経路を明らかにします。これにより、影響を受けているベースイメージやバージョンを特定しやすくなり、責任の所在も明確になります。さらに、このような可視化により、ソフトウェアサプライチェーン全体に対する理解が深まり、依存関係を体系的に把握することができます。結果として、類似の問題が他のシステムに波及するリスクを最小限に抑え、予防的な対応を実現します。

脆弱性管理プログラムの有効性を評価するには

クラウドネイティブの脆弱性管理ソリューションを活用することで、セキュリティプログラムのモダナイゼーションが実現し、よりプロアクティブなリスク軽減への取り組みが前進します。こうした取り組みの成果を評価し、継続的に改善していくには、進捗状況を定量的に測定することが不可欠です。そのためには、以下のような具体的かつ成果重視の指標に注目する必要があります。

脆弱性の検知にかかる時間

ゼロデイ攻撃をはじめとする新たに発見された脆弱性について、それが環境内で特定されるまでに要する時間は、脆弱性管理の有効性を測る上で極めて重要なメトリクスです。この検出スピードが早ければ早いほど、エクスポージャー（露出）の期間を短縮でき、攻撃者に悪用されるリスクを最小限に抑えることが可能になります。早期発見は、セキュリティ体制の即応性を高め、重大インシデントの発生防止にも直結します。

ノイズを排除し、リアルなリスクに集中する

管理対象となる脆弱性の数が膨大になる中で、効果的な優先順位付けは脆弱性管理における最重要課題のひとつです。クラウドネイティブのVM（脆弱性管理）ソリューションは、低リスクの問題を自動的にフィルタリングし、悪用される可能性が高い脆弱性を可視化することで、セキュリティチームが直面する情報のノイズを大幅に削減します。このように真に重要な脆弱性のみに集中できる環境を整えることで、アラート疲労の軽減、優先度の高い対応への迅速なリソース投入、時間と労力の効率化が実現され、組織全体のセキュリティ対応力が向上します。

脆弱性が本番環境に到達するのを防ぐ

効果的な脆弱性管理（VM）ソリューションは、開発サイクルの初期段階においてリスクを特定・対処することで、脆弱性が本番環境に到達する前に封じ込める役割を果たします。導入前に問題を検知し、修正することにより、セキュリティチームは以下の効果を得られます：

- リスクの早期軽減
- 本番環境への影響や混乱の最小化
- 継続的に強固なセキュリティポスチャーの維持

このような「シフトレフト」型のアプローチにより、セキュリティは開発プロセスの自然な一部として統合され、効率と安全性の両立が可能になります。

修正にかかる時間

セキュリティ対応の指標として、チームがパッチの適用・リスクの軽減・代替策の実装をどれだけ迅速に行えるかは、非常に重要です。この対応スピードを評価するには、以下の2つのメトリクスが有効です。

- 平均修正時間（MTTR：Mean Time to Remediate）
- 平均公開脆弱性年齢（MOVA：Mean Open Vulnerability Age）

これらの指標を継続的に追跡することで、チームの対応効率やプロセス上のボトルネックを可視化できます。さらに、悪用される可能性が高い、または広範な影響を及ぼす重大な脆弱性に優先的に対応することで、修正作業の効果を最大化できます。修正スピードを高めることで、攻撃のリスクを最小限に抑えつつ、運用や開発の要求とも適切なバランスを保てるようになります。

チームの効率性とリソース割り当ての最適化

クラウドおよびオンプレミスを含む組織全体のインフラストラクチャにおいて、脆弱性の検出、優先順位付け、修正の各ワークフローを自動化することで、セキュリティチームは貴重なリソースを解放し、大幅な時間の節約が可能になります。このような運用効率の向上と時間短縮の実現は、脆弱性管理プログラムの成功度を測定するうえで、極めて重要な指標の一つです。単なる対応の迅速化にとどまらず、戦略的なリソース配分や人的負荷の軽減にもつながります。

セキュリティリーダーは、MTTR（平均修正時間）や脆弱性の優先順位付け精度といった主要なメトリクスに加え、クラウドネイティブな脆弱性管理ツールの導入・統合にかかる時間や、チームがツールを効果的に活用できるまでの学習曲線といった運用効率にも目を向ける必要があります。さらに、アナリストのトレーニング時間やツール維持に必要な人的・技術的リソースといった運用コストを可視化・追跡することで、脆弱性管理プログラムの成熟度やROI（投資対効果）をより包括的に評価できます。

こうした測定可能な成果に焦点を当てることで、セキュリティチームは脆弱性管理プログラムをより成熟し、かつ俊敏なものへと進化させることが可能になります。データに裏打ちされた評価を通じて、継続的な改善を推進し、変化の激しい脅威環境においても効果的に対応できる態勢を整えることができます。

自己評価

現在採用している脆弱性管理（VM）プログラムが、最新のクラウドリスクに適切に対応できているかどうかを判断するには、まず自己評価から始めることが重要です。以下の質問群は、お使いのVMプログラムの成熟度を客観的に評価し、改善や迅速な対応が求められる領域を明らかにするためのガイドとして活用できます。

各質問について、組織の慣行に基づいて「**はい**」か「**いいえ**」で答えてください。

01 クラウド、オンプレミス、コンテナの各環境全体におけるすべての脆弱性を、自信を持って把握できていますか?

02 単一のツールで、脆弱性に関する統一されたビューを得られていますか？

03 ビジネスにとって重要なリスク要因に基づいて、脆弱性の優先順位を付ける明確なプロセスがありますか？

04 アクティブに実行されているパッケージに含まれる脆弱性を、未使用のソフトウェアの脆弱性よりも優先的に扱っていますか？

05 脆弱性の発生源を、ベースイメージやソフトウェアの依存関係といった根本原因までさかのぼって追跡できていますか？

06 脆弱性をその修正に関して責任を負う適切な所有者へと自動的に帰属させることができますか?

07 修正を迅速かつ効率的に行うための、自動チケット発行およびアラート通知システムを導入していますか？

08 修正のタイムラインを追跡し、SLA やその他の目標に対する進捗状況を測定していますか？

09 修正できない脆弱性のリスクを軽減するための対策を講じていますか?

10 脆弱性管理戦略は、自社の CI/CD パイプラインとシームレスに統合されていますか？

11 脆弱性管理プログラムの有効性を長期的に評価し、取締役会への報告に活用するために、主要リスク指標（KRI）を継続的に追跡していますか？

採点

「**いいえ**」は1つにつき**10ポイント**、「**はい**」の場合は**0ポイント**です。

付与されたポイントを合計することで、あなたの組織が採用している脆弱性管理プログラムの「現時点での成熟度」を判定できます。

0-10	**高度なプログラム** 採用中の脆弱性管理プログラムは、すでに高い成熟度を備え、最適化された状態にあります。かつ最適化された状態にあります。
11-20	**中程度の成熟度** 採用中の脆弱性管理プログラムは着実に前進していますが、さらなる効率性の向上とリスク軽減の強化に向けて、改善の余地がある可能性があります。
30+	**高リスク** 脆弱性管理の実践を強化し、セキュリティ上のギャップを最小限に抑えるためには、今すぐ行動を起こすことが求められます。

この自己評価を通じて、組織の現状と改善が求められる領域を明確に把握できます。診断結果により脆弱性管理の実践に強化が必要と示された場合は、本ガイドを活用し、セキュリティポスチャーの向上に向けた次の一歩を踏み出してください。

結論

攻撃者がクラウド環境の脆弱性を突いて行動を起こすまでの時間は、わずか10分とも言われています[5]。こうした迅速な攻撃に先んじるためには、 脆弱性を事前に特定・対処できる体制、すなわちレジリエンスを備えた最新の脆弱性管理プログラムの構築が不可欠です。

レガシーアプローチに依存している企業や組織は、攻撃対象領域（アタックサーフェス）が広大となり、極めて高いリスクにさらされることになります。こうした環境では、攻撃者に狙われる可能性も必然的に高まります。成熟した脆弱性管理プラクティスを構築するには、セキュリティリーダーがクラウドネイティブな脆弱性管理（VM）戦略への移行を推進する必要があります。このアプローチにより、使用状況に基づいたよりスマートな優先順位付け、クラウドおよびオンプレミス環境全体における統一的な可視性、そして迅速な対応を可能にする自動化機能が実現されます。

本ホワイトペーパーで概説したソリューション要件は、攻撃者よりも常に一歩先を行き、自社環境を防御するための明確なロードマップを提供します。 しかし、こうした取り組みを成功させるためには、まず誠実な自己評価から始めることが不可欠です。今こそ、現在採用している脆弱性管理プラクティスを振り返る時間を取りましょう。

- チームは過剰なノイズに圧倒されていませんか？
- リスクを効果的に優先順位付けすることに苦労していませんか？

もし自己評価の結果、現在の脆弱性対策プログラムに強化の余地があると判明した場合は、迅速に行動を起こすべきタイミングです。 脆弱性管理の成熟度を高めるための次のステップは、今、ここから始まります。

最新のクラウドネイティブ脆弱性管理アプローチを採用することで、ハイパーコネクテッドな現代の環境におけるリスクを効果的に軽減し、ビジネスの継続性を確保するための体制を整えることができます。

5 クラウドの検知と対応における555ベンチマーク

Sysdigによる脆弱性修復について学ぶ

さらに詳しく

著者について

Sysdig Inc.
プロダクトマーケティング部門マネージャー、
Matt Kim

コンテナセキュリティと脆弱性管理に注力するプロダクトマーケティングマネージャー。サイバーセキュリティ分野で10年以上の経験を持ち、複雑な技術トピックを分かりやすく、実践的なインサイトに変換することで、セキュリティチームが現代の高度な脅威に立ち向かうための支援を行っています。

sysdig

WHITE PAPER

WP-016 REV. A 04/25