ivanti

リスクベースのパッチ管理におけるガイドブック

最新のパッチプログラム実装のためのIT運用とセキュリティのための実用書

エグゼクティブサマリー

現在、187,000件以上のセキュリティ脆弱性が脆弱性データベース（NVD）に登録されており[1]、毎日平均61件の新しい脆弱性が追加されています[2]。このため、組織がシステムに対するすべての潜在的脅威を修正することは現実的ではありません。

さらに、入手可能なすべてのデータを総合的に検討した結果、236,000件以上の脆弱性が存在し、その中でサイバー犯罪者によって武器化されている真の脅威の割合は約12.4%であることが判明しました[3]。

従来のパッチ管理の構造では、このような脆弱性の全体像を見通すことができず、サイバーセキュリティのカバー範囲に重大なギャップを残すことになります。

しかし、仮に存在する限りの脆弱性を知っていたとしても、その中からどのCVEに最初にパッチを当てるべきか、どうしたら判断できるのでしょうか？ 最優先のパッチ展開のために、通常のメンテナンスサイクルをいつ中断すべきでしょうか？

リスクベースのパッチ管理を導入しましょう。

リスク軽減のための最も効果的なアプローチの一つであるリスクベースのパッチマネジメントは、基本的な共通脆弱性評価システム（CVSS）スコアやスキャナを超えて、組織のデバイス、データ、エンドユーザーに最も大きなリスクをもたらす特定の脆弱性を特定するものです。

このリスクベースの脆弱性管理の拡張により、組織のセキュリティ態勢にとって最も重要である悪用された既知の脆弱性の更新を取り入れることで、現実のリスク状況をパッチマネジメントプロセスに反映させることができます。

> “企業は、システムに対するすべての 潜在的な脅威を現実的に修正することはできません”

このアプローチにより、脆弱性のコンテキストが提供されるため、パッチ管理者は重要な修正作業を優先することができ、運用チームはセキュリティチームと同じ現実に即したリスクへの視点から活動の緊急性を理解できるようになります。

リスクベースのパッチ管理には、従来の直線的なパッチの優先順位付けシステム以外に、以下のような追加的なリソースが必要です。

- **動的な更新と迅速な合成により、**既知の脆弱性やパッチと比較しながら組織固有のリスクを特定するのに必要な情報を作成できる複数のデータソース（外部と内部の両方を含む）
- **組織にとって重大な脆弱性を、**被害の可能性、ランサムウェアの既知の活動、修復のしやすさなどによって優先順位付けするスキーム
- **重大な脆弱性を特定して警告を発し、**発生した脆弱性の修正を実行するための十分な処理能力（人間のチームメンバーまたは進展する自動化機能のいずれか）

目次

重大な時間：脆弱性が多ぎて時間が足りない 5

従来のパッチ管理プロセス 8

従来のパッチ管理における課題 9

リスクベースのパッチ管理：概要 15

RBPMアプローチにおける4つのビジネスメリット 17

1. 現実的な中間地点 18

2.「現実に即した」優先順位決定プロセス 19

3. パッチ適用の時間短縮 21

4. IT運用チームとセキュリティチーム間での干渉を軽減 23

手動でRBPMプログラムを実行できますか？ 25

RBPMプログラムの5つのベストプラクティス 28

1. 今あるものを把握 29

RBPM向け資産管理 29

RBPM向けサービスマッピング 30

2. 情報への平等なアクセスを確保 31

3. 並行作業を実現 32

RBPM SLAの作成 33

4. パイロットグループを設定 34

ステークホルダーの賛同を得る 35

パッチのパイロットグループを形成 36

5. 自動化を活用 38

自動化パッチロールアウトのベストプラクティス 39

自動化されたメンテナンスのメリット 39

RBPMプロバイダーの選択 40

重大な時間：脆弱性が多すぎて時間が足りない

脆弱性データベースには187,000件以上の脆弱性が登録されていますが、それぞれの深刻度には、個々の組織に対する特定のリスクは考慮されていません[4]。

NVDやCISAのデータベース、業界のスキャナー、脆弱性報奨金制度、ペンテストや、脅威のトレンドに関するさまざまな業界リサーチなど、可能な限りすべてのデータソースを網羅できるまで監視能力を拡大できる組織においては、2022年6月時点で潜在的な脆弱性の本当の数は236,000件以上となります[5]。

このうち、ランサムウェアやサイバー犯罪者の悪用が分かっているのは12.4%です[6]。

脆弱性の膨大な数のみを考えても、企業がセキュリティを確実に維持するためには、パッチ管理に対する積極的かつ優先的なアプローチが必要です。

既知の脆弱性は236,000件以上存在します。

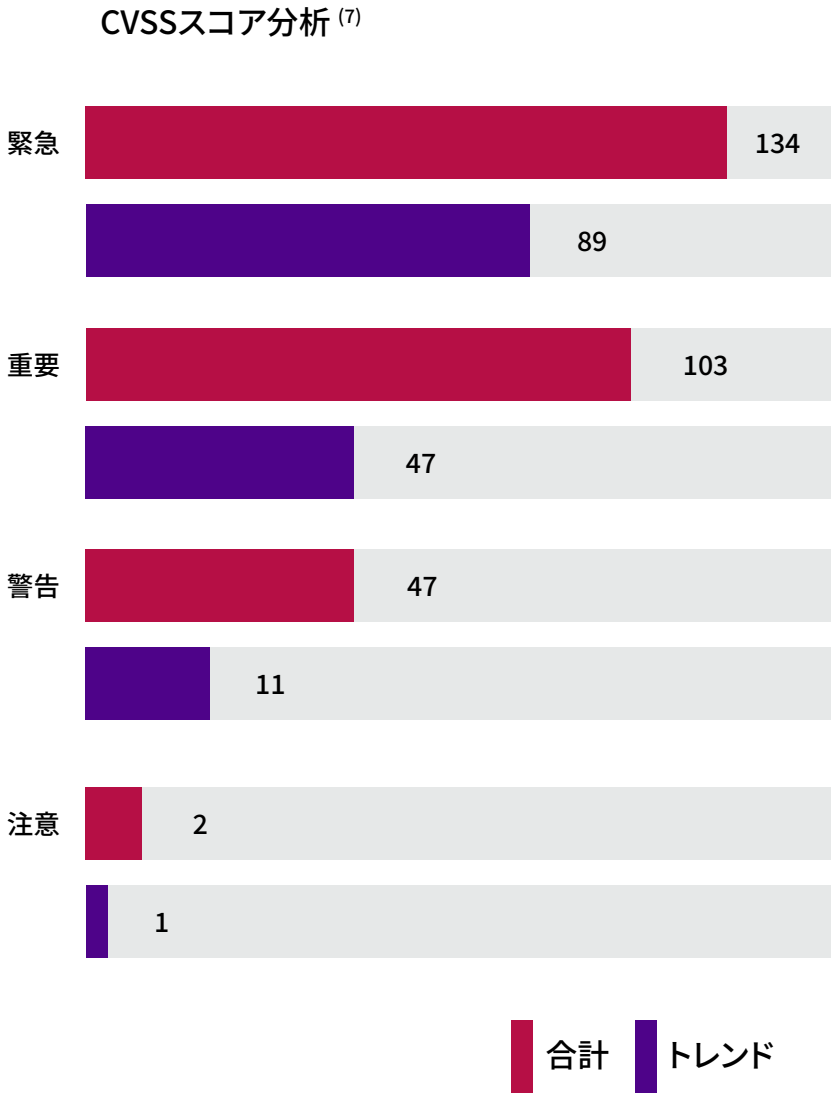
そのうち12.4%は、頻繁に悪用されているか、ランサムウェアに関連しています。

残念ながら、ベンダーの重要度評価やCVSSが提供する情報には、企業内のセキュリティチームが最初にフォーカスすべき脆弱性の優先順位付けに役立てられるコンテキストが含まれていません。

Ivantiが発表した最新のランサムウェアレポート[8]より、以下の点をご検討ください。

- Critical（緊急）に格付けされたCVEにのみパッチを適用している組織は、現在ランサムウェア集団やその他のサイバー犯罪者が活発に使用しているトレンドの脆弱性の40%近くを見逃すことになります。

- ランサムウェアに関連するアクティブな脆弱性の91%は、1年以上前のものです。



脆弱性と実際のランサムウェアの脅威、およびリモートコード実行（RCE）や権限昇格（PE）の影響を受けやすいエクスプロイトをマッピングしなければ、組織がセキュリティと生産性の両方を保証しながら効果的に修復作業を優先順位付けすることは困難です。

結局、セキュリティチームは、組織（デバイス、データ、エンドユーザー）の安全を確保するために、関連するすべての脆弱性にパッチを適用しなければならなくなります。

サイバー犯罪者は、一度だけ運が良ければいいのです。

現実世界への影響：

Microsoft[9]

2021年、Microsoftは23件のゼロデイ脆弱性を解決しました。

そのうち15件のパッチの優先順位は「重要」、つまり「緊急」ではないと評価されていました。

2021年のMicrosoftのゼロデイ全脆弱性の100%が、サイバー犯罪者やランサムウェアによって頻繁に悪用されていました。

従来のパッチ管理プロセス

これまで、パッチ管理は直線的なウォーターフォール型のアプローチで行われてきました。

1. セキュリティチームの脆弱性スキャナまたはデータベースが環境内の新しい脆弱性を検出し、CVSS重要度評価が高スコアの脆弱性を指示して、トリアージによる修復を行います。
2. 一方、パッチ管理者は、定期的なメンテナンスサイクルの一環としてアップデートが必要なソフトウェアを見つけるために環境を評価し、セキュリティチームの評価とは別に、修復の優先順位の一部として重要なベンダーの重大性を評価します。
3. セキュリティチームとパッチ管理者は、修正のための重要なパッチの優先順位付けを調整するために議論します。
   - 通常、セキュリティの推奨事項は、パッチ管理者およびIT運用チームのベンダーによる推奨事項よりも優先されます。
4. パッチ管理者は、脆弱性の優先リストを修正するための関連パッチが存在すれば、それを見つけます。可能であれば、修正をより広範な組織に展開する前に、サンドボックス環境内でテストします。
   - 管理者が直面する現実は、テスト環境はほとんどの場合、実際の組織ネットワークのあらゆるニュアンスを網羅しているわけではないということです。
5. たとえサンドボックステストでパッチに問題がなく、影響はないと判断された場合であっても、適用されたパッチが他のアプリケーションとの機能や相互接続を妨害するため、シャットダウンやクラッシュが発生する可能性があります。
6. パッチ管理者とセキュリティチームは同様に、導入の結果を確認し、アップデートに失敗したマシン、またはその過程で完全に見落とされたマシンを特定するため、クリーンアップのサイクルが繰り返されるようになります。

従来のパッチ管理における課題

パッチ管理に携わったことのある人なら、従来の直線的なアプローチの欠点を指摘することができるでしょう。
例えば、ランサムウェアの集団は、中央のデータベースから脆弱性を特定してから数日以内に悪用することができるため、パッチ管理者は攻撃までのより短い時間内に脆弱性を特定し、修正しなければなりません

QNAP、Sonic Wall、Kaseya、Apache Log4jなど、昨年のいくつかの主な脆弱性は、NVDに登録される前に悪用されました[11]。

のエクスプロイトがパッチ提供後14〜28日以内に発生しており(12)、サイバー犯罪者が機能するエクスプロイトを開発するのに必要な日数の中央値はわずか22日です[13]。

現実世界への影響：BlueKeep[10]

2019年5月14日
CVE-2019-0708についてパッチ公開

2019年5月15日
概念実証調査開始

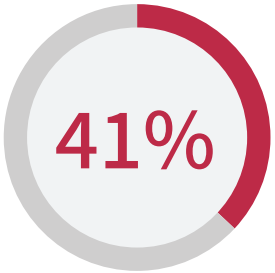
2019年5月20日
調査会社がBSODエクスプロイトを確認

2019年5月28日
独立系調査会社6社によりRCEが実行され、さらにサイバー犯罪者による悪用を確認

公開からサイバー犯罪者による実際の悪用までわずか14日

パッチ管理者やセキュリティチームは、処理能力やリソース、
人員が追加されることもなく、独自のリスク環境に関する詳細な情報を得られないまま、ベンダーの重要度評価やCVSSスコアリングのみに頼らざるを得なくなっています。

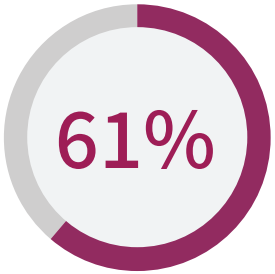
調査対象のIT運用およびセキュリティチームの53%が、積極的なパッチ適用ではなく、脆弱性の整理と優先順位付けにほとんどの時間を費やしていると回答しています[14]。



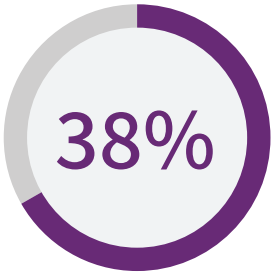
最近の国際調査によると、調査対象企業の41%が、極めて競争の激しい雇用市場の中で高い作業負荷のためにIT運用担当者を失ったという結果が出ています[15]。

セキュリティとIT運用チームの目標にズレは、

往々にしてパッチの失敗や生産性の低下を招きがちです。



調査対象のITおよびセキュリティ専門家の61%は、四半期に1回、毎月28%の頻度で生産性の「向上」のためメンテナンス期間の延期要請を受けており、それにより組織はサイバー攻撃の危険にさらされることになります[16]。

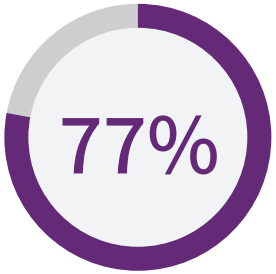


2021年には調査対象組織の63%がサイバー攻撃を受けましたが、そうした場合、被害企業の38%が組織全体の1週間分の生産性を失い、24%は1か月分の業務に値する損失を被りました[17]。

ほとんどの部署では、パッチを適用する前にアップデートをテストしたり、他の部署と調整したりする時間がありません。

パッチのテストに最も時間を費やしていると回答したIT運用・セキュリティチームはわずか15%で、他部門との調整に最も時間を費やしていると回答したチームはわずか10%でした[18]。

スキャナやデータベースは、悪用可能なすべての脆弱性を発見し公表しているわけではありません。

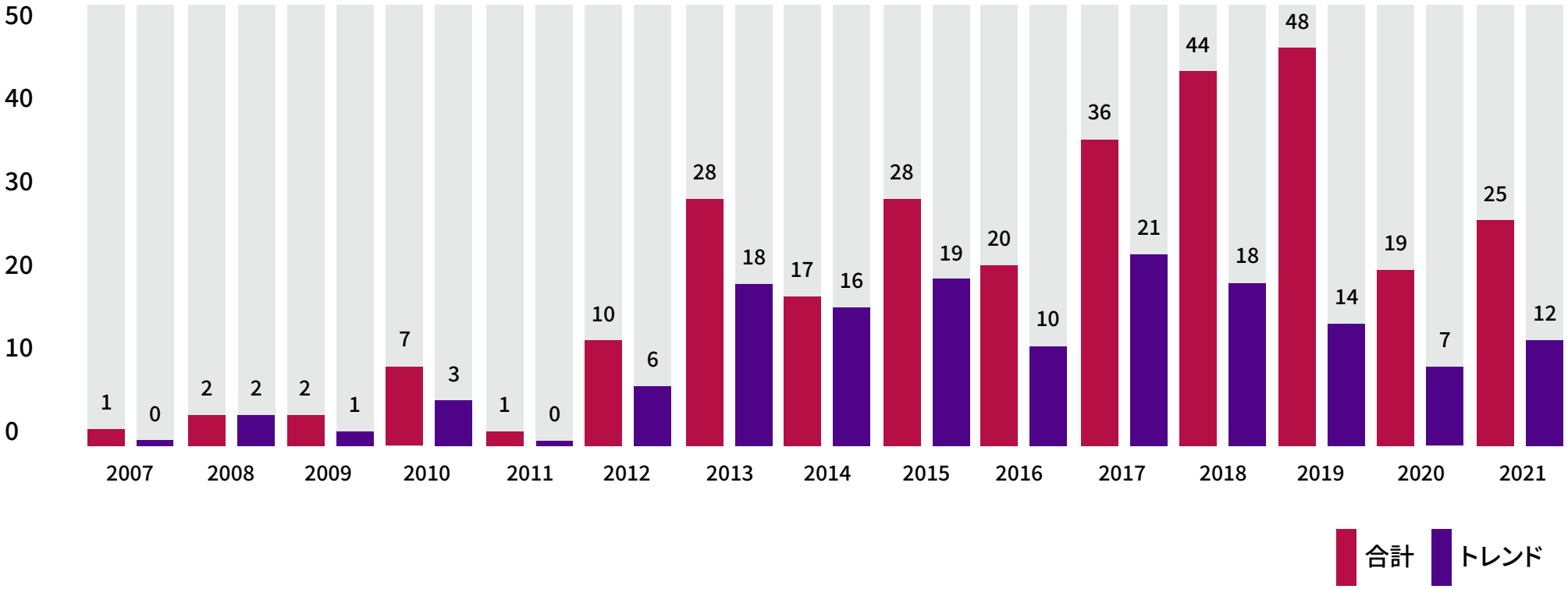


人気のある脆弱性スキャナートップ3のNessus、Qualys、Nexposeが昨年検出したのは、悪用可能な脆弱性全体の77%に過ぎませんでした[19]。

サイバー犯罪者やランサムウェアの集団はまた、重要でない脆弱性や古い脆弱性を攻撃に利用することができます。

- CVSSで「緊急」と評価されたCVEにしかパッチを適用しない組織では、ランサムウェアに結び付く悪用可能な全脆弱性の53%を見逃すことになります[20]
- 非常に流行している全脆弱性の92%は2021年以前に公開されており、最近活発に悪用されている2つの脆弱性が初めて公開されたのは2008年です。[21]
- Rand Consulting Groupの調査によると、脆弱性は最初に公表されてから最大7年後まで、サイバー犯罪者によって活発に悪用され続けています[22]。

ランサムウェアに結び付く脆弱性とNVD公開年別の傾向[23]



サイバー犯罪の被害に遭った組織の

38%

が1週間分の生産力を失っています。

24%

は1か月分を失っているのです。

ランサムウェアグループにとって、パッチ未適用の脆弱性は引き続きメインの攻撃経路となっています。迅速な対応ができない場合、組織のセキュリティ環境はすぐに侵害され、生産性や収益性に重大な影響を与えることになります。

また、ランサムウェアによる侵害の平均総コストは462万ドル(24)と推定されており、セキュリティチームやIT運用チームが抜け穴や脆弱性を修正するためには、効果的な脆弱性修正戦略が極めて重要です。

しかし、すべての脆弱性にパッチを適用することは、人員不足や多忙な部門は言うまでもなく、どんなIT運用チームやセキュリティチームにとっても実現可能な解決策ではありません。

パッチ管理者は、サイバー犯罪者やその他の脅威アクターの先を行きながら、時間、スタッフ、社内の処理能力といった限られたリソースを最大限に活用する戦略的な取り組みの計画を立てる必要があります。

リスクベースのパッチ管理（RBPM）を導入しましょう。

ランサムウェアの平均的な侵害コストは

462

万ドルと推定されています。

リスクベースのパッチ管理：概要

リスクベースのパッチ管理戦略では、従来から使われている画一的で直線的なパッチ適用アプローチに組織独自のリスクプロファイルを詰め込もうとするのではなく、エリアを絞り込んでいくアプローチでパッチを適用していきます。

まず、管理者は、ネットワークスキャナ、NVDやCISAなどのデータベース、手動調査やペンテストにより発見された脆弱性など、外部の情報源から情報を収集します。

また、社内のデータポイントを収集し、組織全体のITフットプリントの正確なリスクプロファイルをマッピングします。

このデータセットには以下のものが含まれます：

- 組織のITおよび運用チームがサポートする使用中のデバイスとOSのリスト。
- 組織のエンドユーザーが現在使用しているすべてのアプリケーションとソフトウェア（正式にインストールされたソフトウェアと、ユーザーが入手したダウンロードまたはクラウドベースのアプリケーションの両方を含む）
- 独自データおよび顧客データの取得方法、保存場所、使用方法の把握

パッチ管理者は、外部の脆弱性・脅威情報を組織内の独自のセキュリティ環境と照らし合わせることで脅威情報のコンテキストを把握し、外部ソースが認識している脅威ではなく、組織にとって最も重要なパッチの優先順位を決定することができます。

RBPMを利用することで、小人数のチームでも増え続ける脆弱性に対応でき、すでに多忙なIT運用チームやセキュリティチームに負担をかけることなく、組織やエンドユーザー、顧客の安全を確保することができます。

リスクベースのパッチ管理アプローチにおける4つのビジネスメリット

- RBPMは、”あらゆるものにパッチで対応”と”わざわざする必要はない”の中間に位置する現実的な手法です。
- RBPMは、組織に合わせてカスタマイズされた「リアリティベース」の脆弱性の優先順位付けを提供し、実際の攻撃情報を状況に当てはめることで、本当に重要なものを判断できるようにします。
- RBPMは、従来のパッチ管理のアプローチよりも迅速に処理することができます。
- RBPMは、セキュリティとIT運用の部門を超えた橋渡しをします。

ivanti

1. RBPMが推奨するのは、パッチ適用への理想的なアプローチではなく、実用的なアプローチです。

リスクベースの手法によるパッチ管理は、すべての管理者が直面する現実、すなわち、脆弱性があまりにも多く、すべてに対応するにはリソースが少なすぎることを認め、それに対応するものです。

2021年には、ランサムウェアに関連する脆弱性の数が、前年比で29%増加

一方、何もしないという選択肢はありません。パッチを適用していない脆弱性は、ランサムウェアグループや脅威アクターが最も悪用する攻撃ベクトルとなっているからです。昨年、ランサムウェアに結び付く脆弱性は、前年比29%増という驚異的な増加を示しました[25]。

“あらゆるものにパッチで対応”と”わざわざする必要はない”の中間に位置する最適化された手法がRBPMです。

CVSS評価やベンダーのCVE評価の「緊急」であっても、無差別にすべてパッチすることはもはや現実的な目標ではないことを組織が早く理解すれば、ユーザー、システム、資産をより確かに保護するためのプロアクティブで最新のパッチ管理戦略にそれだけ早く移行することができるのです。

リスクベースの積極的な脆弱性対策プログラムにより、組織のデータ漏洩事案を80%削減することができます。

また、Gartner Researchによると、組織がすべてのパッチを適用しない場合でも、RBPMを含む包括的なリスクベースの脆弱性管理プログラムにより、組織のデータ漏洩事案を80%削減することができます[26]。

これは、比較的小さな考え方の変化であるにもかかわらず、ビジネスにおける驚くべき改善です。

2. RBPMは、組織の状況に応じてリスクをランク付けする「リアリティベース」の優先順位付けプロセスです。

RCEやPEの可能性などを含むその他の優先事項の中で、ランサムウェア集団の行動や悪用されがちな脆弱性に基づいて問題をランク付けすることで、組織のパッチ管理者は、脆弱性がもたらしうる影響についてより現実的な評価を行うことができるようになります。

これらの評価では、脆弱性を単独の脅威としてだけでなく、「脆弱性の連鎖」によって複数のエクスプロイトの組み合わせも考慮しています。

脆弱性の連鎖とは、ランサムウェアが複数の脆弱性（多くの場合、重大度や時期が異なる脆弱性）を一度に悪用し、組織に対して包括的な攻撃を仕掛けることを指します。

例えば、2021年のLockFileランサムウェア攻撃[27]では、Microsoft ExchangeとWindows OSから合計4つの脆弱性を連鎖させていました。

「ProxyShell」の脆弱性は、

サイバー犯罪者が組織のネットワークに侵入し、さらに追加で悪用するリモートコードを起動させたり、後でアクセスするためのバックドアを設置したりすることを可能にしてしまいます[28]。

「PetitPotam」の脆弱性では、

攻撃者が組織のシステムにさらに潜り込み、より重要な基幹システムにまでアクセスできるようになります。

従来の直線的なパッチ管理プロセスにのみ従っていた組織では、この攻撃や類似の攻撃に関連するすべての脆弱性にパッチを適用していなかったでしょう。

ランサムウェア「LockFile」に連鎖する4つの脆弱性のうち、パッチを適用すべき「緊急」の脆弱性は1つだけで、
2つはパッチの重要性について「警告」と評価されていました[30]。

LockFile脆弱性

脆弱性	CVSSスコア	CVSS重大度	製品
CVE-2021-31207	7.2	重要	Microsoft Exchange Server
CVE-2021-34473	9.8	緊急	Microsoft Exchange Server
CVE-2021-34523	9.8	警告	Microsoft Exchange Server
CVE-2021-36942	5.3	警告	Microsoft Windows Windows Server 2008、2012、2016および2019

また、2021年に初めてLockFileランサムウェア攻撃が発生したにもかかわらず、調査によると、
34,000以上のProxyShellはまだネット上に存在しており[29]、さらなる脆弱性のエクスプロイトを招きかねない状態です。

3. RBPMは脆弱性へのパッチ適用を迅速化します。

重大な脆弱性にパッチが適用されない期間が長ければ長いほど、企業はデータ漏洩やランサムウェア攻撃のリスクにさらされることになります。

2021年、国土安全保障省はCISA（サイバーセキュリティ・インフラストラクチャセキュリティ庁）を通じて「拘束力のある運用指令22-01」を発表しました。

公共部門の組織に対するこの新しい要件は、重要な脆弱性のパッチ適用期間を2週間に短縮し、組織のインフラに対する「非常に重大なリスク」の場合には、さらにスケジュールの調整を勧奨しています[32]。

ちなみに、現在ランサムウェアファミリーに頻繁に悪用されていることが確認されている全CVEの中で、このCISAの脆弱性必須パッチリストに含まれているのは20%に留まります[33]。

したがって、脆弱性の優先順位付けシステムを活用して最も重要なパッチを決定しているセキュリティチームであっても、パッチを適用すべき脆弱性の数は膨大であり、パッチを適用するための時間も十分ではありません。

従来のパッチ管理手法では、管理者は脆弱性の報告を受けるたびに、どのような対処をすべきかを調査し決定するのに何時間も費やしてしまいがちです。

一方、最新のパッチ管理システムの中には、脆弱性情報とパッチデータを組織の状況に対して自動照合できるものもあります。これらの調整により、組織固有のリスクを可視化し、全体的な修正プロセスをスピードアップして、各メンテナンスサイクル後に残るクリーンアップを削減することができます。

CISAのパッチが必要な脆弱性リストは、活発に悪用されている全脆弱性の20%しかカバーしていません。

加えて、リスクベースの包括的なパッチ管理のアプローチは、次の点によりゼロデイ脆弱性に対抗し、その影響を抑えるために最も有効な手段であると考えられます。

- 脆弱性が存在することが分かっていれば、パッチが利用可能になった時に優先的にリリースし、組織のシステム上で展開することができます。
- 日常業務に支障をきたすことなく、潜在的な脆弱性を持つシステムへの影響を軽減するために当面の戦略を策定できます。
- サイバー犯罪者が脆弱性を利用する可能性があることを即座に知ることができるよう、社内に警告システムを設定できます。

組織内の最も脆弱なシステムを保護するためのアップデートを発見し、優先することで、パッチ管理者はリソースを最大限に活用し、外部のサイバー犯罪者やランサムウェア集団からシステムを保護することができます。

ゼロデイ脆弱性とは？

ゼロデイ脆弱性とは、以下のような脆弱性のことです。

- 多くの場合、エクスプロイト攻撃が発生した後にベンダーによって特定されます。
- サイバー犯罪者によって頻繁にエクスプロイトされます。
- パッチを適用できない、または適用できるパッチがありません。

4. RBPMは、IT運用チームとセキュリティチーム間のよく起こりがちな摩擦を軽減します。

リスクベースのパッチ管理は、共感の余地を生み出します。

IT運用チームは、

セキュリティチームの優先順位と、緊急性のある脆弱性に対する真に重要なパッチの根拠をより良く理解することができます。

セキュリティチームは、

不適切なパッチがビジネスにどのような影響を与え、重要なアプリケーションを破壊し、ユーザーチケットを急増させるかを正しく認識できるようになります。

IT運用チームが、セキュリティチームによるパッチの優先順位設定は適切である（だから自分たちやエンドユーザーが起こりうる脆弱性に時間を無駄にすることはない）と信頼していれば、IT運用チームはより協力的になり、セキュリティの最重要リスクに対応する時間をプロアクティブに確保できるようになります。もっと大まかにいえば、リスクベースの脆弱性管理プロセスでは、特定の脆弱性にパッチを適用しなかった場合の損失リスクについて、これらのチームが学習することができるのです。

要求されたパッチは突然、もはや数ある脆弱性のうちの1つだけを解決するものではなくなります。リスクは部門やビジネスの成果という観点からコンテキスト化され、対処しない場合、エンドユーザーの体験や収益に影響を与える可能性があります。

2021年、ランサムウェアの平均的な侵害コストは462万ドルに上りました[34]。

アップデートのために数時間を確保するのは一時的に不便ではありますが、ランサムウェアの攻撃によって1週間以上の時間を失うという長期的なリスクに比べればずっとメリットがあります。

同様に、セキュリティがあらゆる未解決の問題を一度に解決しようとせず、最も重要な問題だけを解決しようとすれば、IT運用部門のパートナーとより柔軟に連携し、重要な時間帯にパッチ適用を行わないようにして、メンテナンスサイクルを短縮し、予定外のアップデートによるシステムのクラッシュを避けることができます。

さらに、最新のRBPMプラットフォームでは、データの分析と優先順位付けが、アクセスしやすい単一の場所またはダッシュボードに一元化されており、これにはいくつかのメリットがあります。

IT運用チームは、

セキュリティ部門から脆弱性レポートが提出されるのを待つ必要がありません。ダッシュボードで組織にとって最も重要なものを確認し、関連するCVEを社内環境にマッピングするなど、クリーンな環境ですぐにアップデートのテストを開始してレスポンスタイムを改善することができます。

セキュリティチームは、

パッチの展開状況、ボトルネックの可能性、将来のスプリントやメンテナンスサイクルで対処すべきバックログに残っているパッチを一目で確認することができます。

RBPMのプロセスは、常に起こる中断ではなく、相互の協調をもたらします。

手動でリスクベースのパッチ管理プログラムを実行できますか？

リスクベースのパッチ管理は、すべてにパッチを適用するのに代わる自然な方法ですが、簡単なプロセスではありません。

（つまるところ、簡単に実装できるのであれば、この資料は必要ないのです。）

系統立てられたツールや自動化プロセスを使わず手動でRBPMに取り組もうとする準備不足のチームでは、適切なテストやパッチの展開はもちろん、リスクベースの優先順位設定や、脆弱性の変化のリアルタイム追跡にはすぐに対応不可能になってしまいます。

たとえば、組織がRBPM戦略を実行しようとしているとしましょう。あまりに多くのデータソースに対応できなくなるのを避けるため、この組織では昨年、毎日平均61件の新しい脆弱性が追加されたNVDだけに注力することにしました[35]。

新しい脆弱性は、単に外部の重要度評価に頼らず、社内で起こりうる攻撃対象との関連性を考慮する必要があるというRBPMの考え方の一環として、チームは毎日61件の新しいNVD脆弱性すべてを手作業でレビューし、61回に分けて優先順位付けを行わなければなりません。

（そのチームにおける月曜日のバックログは恐ろしいものになるでしょう）

そして、この仮想の会社は、包括的とはいえ一つのデータソースを参照しているに過ぎないのです。

そこに他のデータベースや調査、レポートが加われば、生の脆弱性情報の洪水に溺れることになるでしょう。

現実への影響：

脆弱性とパッチの整合性

Ivantiの専門家との対話の中で、世界中の企業のIT運用・セキュリティチームは、従来の脆弱性とパッチの照合レポートを手作業で完成させるのに少なくとも8時間かかるという話を紹介しています。これらの手作業でのレポートに携わるプロフェッショナルは、最終的な文書が非常に重要であるにもかかわらず、100%正確でない可能性があることを認めています。

ただしここでは仮定上の話として、組織にはMicrosoft、Apple、Linux、その他のアプリ・プロバイダーなどの大手ベンダーを定期的に直接監視し、脆弱性や悪用が公表されたらすぐに見つけられるだけのセキュリティとIT運用のスタッフがいるとしましょう。

PatchMangement.org, Reddit, Ivanti Patch Tuesday Webinar など、特に関連性の高い脆弱性を集めたオンラインサイトも存在します。これらやその他の業界ウェブサイトは、RBPMプロセスのこの部分についてチームを無料でガイドする素晴らしいリソースであることは間違いありません。

しかし、モニタリングは、パッチサイクルの終了までに完了させなければならない複数のタスクの一つに過ぎません。

RBPMプロセスの一部として、この仮想組織のセキュリティとIT運用チームは、この他に以下を行う必要があります。

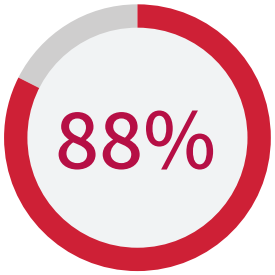
- ITが認可したもの、ユーザーがインストールしたものなど、すべての社内デバイスとアプリケーションを特定する。
- どのエンドユーザーとユースケースに最初にパッチを適用するかを決定する。
- すべてのバリエーションと変数、または特定の脆弱性に対して実用的な数だけパッチをテストする。

パッチのロールアウトをスケジュール設定し、実行する。特にハイブリッドまたは完全リモートワークの場合、これらの手続きは、現実のスピードに追いつけずに終わりのないプロセスへとエスカレートしていく可能性があります。

多くの手動システムでは、スプレッドシートタイプの文書とデータベース照合が使用されていることも忘れてはいけません。

しかし、スプレッドシートに頼っていては、ミスが発生する可能性があります。同じレポートを頻繁に調整する人が多ければ多いほど、エラーが雪だるま式に増えて、遅延や修正にコストがかかる可能性が高くなります。

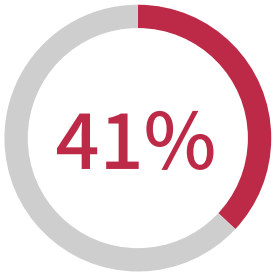
実際に、ある調査によると、すべてのスプレッドシートの88%に「重大な」誤りがあり、その大部分は、まさにそのスプレッドシートを使って作業をしている人々によって引き起こされているのです[36]。



すべてのスプレッドシートの88%に「重大な」人為的エラーがあります。

したがって、特に初期段階では、アプローチの感触をつかむため、また専用ツールを購入する前に、リスクベースのパッチ管理戦略を手動で実行することは確かに可能です。しかし、この方法はRBPMの考え方を本格的に取り入れたいと考えるチームにとって最適な構成とは言えません。

調査対象組織の41%が、高い作業負荷のためにITスタッフを失ったと回答している今、さらにマニュアル作業を増やすのも賢明ではないでしょう[37]。



調査対象組織の41%が、高い作業負荷のために重要なITスタッフを失ったと回答しています。

最終的にマニュアル優先のアプローチは、終わりのない管理とタイムラインの延長によって、実用的なRBPM計画を本質的に破壊してしまうことになります。

リスクベースのパッチ管理プログラムの5つのベストプラクティス

1. 知らないものには、パッチを適用できません。
2. IT部門とセキュリティ部門が意思伝達できるように。
3. 社内SLAで並行作業を実現します
4. 社内SLAで並行作業を実現します
5. 自動化を活用しましょう!

1. 現在あるものと、その使い方を把握します。

存在を把握していないものを保護したり、パッチを適用することはできません。したがって、あらゆる脆弱性管理の取り組みにおいて、資産の発見（どのようなエンドユーザープロファイルで何があるのかを見つけること）は非常に重要な役割を果たします。

RBPM向け資産マネジメント

最新の資産管理ツールは、組織が現在の技術スタックを把握し、追跡するのに役立ちます。これは、ノートパソコン、デスクトップ、携帯電話、タブレット端末、サーバー、ネットワークデバイスなど、組織内で稼働するすべてのデバイスとソフトウェアを特定することから始まります。

広範なパッチマネジメントプログラムと同様に、資産に関する情報は、以下のような複数のソースから取得できます[38]。

- ☐ Microsoft Endpoint Configuration Manager (SCCM)とMicrosoft Intune
- ☐ CSVファイルまたはスプレッドシート
- ☐ Microsoft Active Directory
- ☐ Workspace One (AirWatch)
- ☐ Ivanti Neurons for Discovery

すべての資産をリストアップした後、重複を排除し、すべてのデータがデータベース内で一貫していることを確認する必要があります。

最後に重要なことは、IT運用部門のアセットマネージャーは記録を整理し、パッチ管理者が最も重要な端末と潜在的な弱点など、パッチの優先順位付けに役立つ情報を見つけられるようにすることです。

RBPM向けサービスマッピング

検知のプロセスの延長として、サービスマッピングにより、管理と保護が必要なシステムを見つけ出し、そのシステムとそれらが使用するデータがどのように相互接続され、アクセスされているかを明らかにすることができます。

サービスマップには以下のものが含まれます。

- ☐ インフラストラクチャとハードウェアのインベントリ
- ☐ アプリケーション、設定文書と、使用されたソフトウェアの最新バージョンを掲載したソフトウェアライブラリ
- ☐ 情報の流れや組織全体のデバイスの接続方法を明示した設定・ネットワーク図
- ☐ エンドユーザー、ユーザープロファイル、高リスクの端末、およびそれらが侵害された場合に組織の重要なシステムに与える影響のレベル

そして、セキュリティチームは、接続されているユーザーシステムやアプリケーションによって、攻撃者が脆弱性を経由して重要なシステムに到達するまでの経路をマッピングすることができます。

同時に、IT運用チームは、ミッションクリティカルなアプリケーションに接続する可能性のあるシステムの数を把握し、パッチテストの最適な構成と実施方法について重要な情報を得ることができます。

ivanti

2. 誰もが同じ情報にアクセスできるようにします。

リスクベースのパッチマネジメントの効率性は、IT運用チームとセキュリティチームがいかにうまく連携し、介入を同期させるかに左右されます。そのためには、すべての共通の目的を達成するために、部門を超えた連携が必要となるでしょう。

理論的には、すべてのチームが同じゴール、つまりサイバー攻撃による中断を経験することなく業務を遂行できる安全な組織を目指しているはずです。

実際のところは、セキュリティ部門はリスクの軽減を目指し、IT運用チームはエンドユーザーのパフォーマンスとエクスペリエンスの最適化を目指すというように、両者の目的は正反対のようにも思われます。

以前は、

セキュリティチームには組織に関連する脅威を特定する現実的な方法がなく、パッチ適用が日常業務にどのような影響を与えるかについてほとんど意識しないまま、すべてをリスクとして扱っていました。

IT運用チームは、

エンドユーザーのサービス品質保証（SLA）を遵守して通常業務を予定通り進めることと、衰えを知らない潜在的なランサムウェアの理論上の脅威の間でバランスを取る必要があります。

優れたRBPMシステムは、情報の共有と相互理解を得たリスク分析によって、当然発生しうるこの摩擦を緩和しようとするものです。

セキュリティ部門は、

組織のサイバーセキュリティ態勢にとって本当に重要な脆弱性のみに優先順位を付けます。

IT運用部門は、

脆弱性がエンドユーザーに与える影響をリアルタイムで確認できるため、ロールアウトのための時間を積極的に確保することができます。

3. RBPMのSLAを通じて、パッチまでの時間を短縮するために並行して作業できます。

最良のシナリオは、リスクベースのパッチマネジメントソリューションにより、関係者全員がリアルタイムで脆弱性とその対策方法を認識することです。

IT運用チームとセキュリティチームは、リスクの優先順位付けに同じ手法を使用し、理解します。そのため、修復プロセスの複数のポイントで並行して作業および同期し、解決すべき内容について確実に意思統一することができます。

このアプローチにより、脆弱性の重要度や、部門を越えたパートナーとの同期状況に応じて、メンテナンスサイクルを数週間から数日、数時間に短縮することができます。

IT運用チームとセキュリティチームは、社内のベストプラクティスを確立し、各チームや組織全体の目標を考慮したメンテナンス期間に合意する必要があります。

そのため、IT運用チームとセキュリティ・チームの間で、パッチマネジメントに関するサービスレベル合意書の作成を検討します。

SLAの作成

このSLAでは、各ステップにおけるコラボレーションの期待値とタイムフレームを定義し、いつ、誰が、何をするのかを全員が把握できるようにします。

SLAには以下の点を含めます。

- すべての定義 -「脆弱性」とは何か、など基本的なことまで定義します。
- 各ステージに必要な仕様と展開される技術スタック
- 脆弱性の優先順位付けの基準
- パッチ適用サイクル中の連絡頻度
- **Explicit exceptions** for when vulnerabilities must be remediated out-of-band and/or out of the regular maintenance cycle.

特に、すべての関係部署で達成可能で現実的な重要業績評価指標（KPI）を設定し、可能な限りKPIを共有することに注意を払う必要があります。

現実世界への影響：

パッチおよび脆弱性に関するSLA

10万台以上のデバイスを保有するある世界的大手メーカーは、IT運用チームとセキュリティチームの間で脆弱性に関するSLAを導入しました。

この企業ではその後、SLAで定められた2週間という期間内に、95%の脆弱性修正遵守率を達成しました。

4. パッチの優先順位付けとテストのために、主要なステークホルダーとパイロットグループを設定します。

パイロットグループとは、あらかじめ決められた（そして事前に訓練された）代表的なユーザーロールやデバイス構成からなるグループのことで、組織全体にパッチを展開する前に、実環境で脆弱性をテストすることができます。

つまり、パッチがミッションクリティカルなソフトウェアをクラッシュさせるのであれば、組織全体をシャットダウンさせるよりも、マシン数台でそれがわかる方がいいということです。

パイロットグループは、パッチが事業活動に与える影響をより正確に予測するために、コントロールされたテストラボ環境を補完します。

テストシステムでダウンストリームへの影響が明らかになることはほとんどないため、パッチのロールアウトに際して1つ以上のパイロットグループを設定することは、運用に悪影響を与える可能性を減らすために重要です。

つまり、パッチがミッションクリティカルなソフトウェアをクラッシュさせるのであれば、組織全体をシャットダウンさせるよりも、マシン数台でそれがわかる方がいいということです。

パイロットグループへの賛同を得る

このベストプラクティスでは、パッチ管理者は、IT運用部門だけでなく、組織全体から賛同を得る必要があります。関連するパイロットグループには、重要なアプリケーショングループや、ミッションクリティカルなシステムが配置されているような部門を含める必要があるためです。

そのためには、IT部門のサービスマップにとどまらず、対象となるユーザーグループに、デバイスとデータの相互作用、および各アップデートによる通常のプロセスへの影響について、直接尋ねる必要があります。

また、パッチによって就業時間中に誤ってアプリケーションをシャットダウンしてしまうようなことが起こる前に話をしておくことで、関係を良好に保つことができます。さらに、このために築いた人脈が、他の方法では得られない支援や洞察を積極的に提供してくれる利害関係者などを含む、将来のパイロットグループの基礎になるのです。

パッチパイロットグループを設定

パイロットグループは：

- 少なくとも1つの初期「メイン」パイロットグループを編成して重大な不具合がないことを確認し、拡張パイロットグループを編成して発生頻度の低い問題やアプリケーション固有の問題を特定します。
- 組織の目的と、すべての関係部署（つまり、IT運用とセキュリティ）が目指す具体的な目標を考慮します。
- 常にフィードバックをやり取りします。
- 組織内で使用されているすべてのデバイスの代表として、パッチの互換性の問題を特定します。
- 組織の環境におけるすべてのユーザープロファイル（「ユーザーペルソナ」とも呼ばれる）を考慮します。

従業員や利害関係者は、パイロットグループへの参加にかかわらず、ランサムウェアやその他のサイバー攻撃のリスクを低減するために、なぜ脆弱性のパッチ適用が重要なのかを理解する必要があります。

「組織とあなたの仕事の安全を守るために、テストは不可欠である」というメッセージを明確に発信します。パイロットグループテストとして割り当てられたデバイスで多少の不便を我慢することが、部門全体を重大な障害から救うことになるのです。

現実世界への影響：

PrintNightmare[39]

2021年6月、ある研究者がWindowsのプリントスプーラーの中にRCEの脆弱性を発見しました。

- 同月にWindowsがプリントスプーラーの脆弱性パッチをリリースしたとき、その研究者は自分たちが特定したエクスプロイトが解決されたと思い、その研究結果を発表したのですが、Windowsは別の脆弱性パッチを適用していたことが判明しました。
- サイバー犯罪者はこの研究をすぐに、脅威アクターが管理者レベルの権限で被害システムをリモートで乗っ取ることができるアクティブなエクスプロイトに利用しました。
- 最初のPrintNightmareのエクスプロイトは、2021年7月1日にパッチが適用され、2021年7月16日に再リリースされました。
- その後、プリントスプーラーのパッチがいくつかリリースされ、2022年5月にはさらに4つのパッチがリリースされました。

事業運営に大きな影響を与えるため、これらのパッチは現在、多くの組織の修正作業やパイロットグループのテストで優先されています。

2021年6月
研究者がWindowsプリントスプーラーの脆弱性を発見

2021年7月
Windows、PrintNightmareの最初のパッチをリリース

2021年6月
Windowsが異なる脆弱性にパッチ、研究者が調査結果を公表

2022年5月
さらに4つプリントスプーラーのパッチをリリース

5. 特にロールアウトに、自動化の活用を

自動化はリスクベースのパッチマネジメントプログラムに対し、特に外部からの脆弱性レポートの収集、コンテキスト化、優先順位付けにおいて、大きなメリットをもたらします。

先に触れたように、RBPMプログラムを手動で実行するのは控えめに言っても維持が難しく、スタッフの定着率に悪影響が出るのは言うまでもありません。

しかし、自動化はパッチのロールアウトをセグメント化して、大規模にパッチを適用しながらプロジェクトを円滑に進めるのにも役立ちます。

ivanti

自動化パッチロールアウトのベストプラクティス

自動化ルールとゲートにより、テストシステム、パイロットグループ、本番環境グループの拡大に関するベストプラクティスを実施し、ビジネスへの影響を最小限に抑えながら迅速に実行できるパッチマネジメント体験を創出します。

自動化パッチロールアウトは、小規模なメインテストグループから開始することを検討してください。それから次のように拡大します。

1. アクティブな環境の初期パイロットグループ
2. 自社環境の10%程度のアーリーアダプター
3. 組織の残りの大多数のエンドユーザー

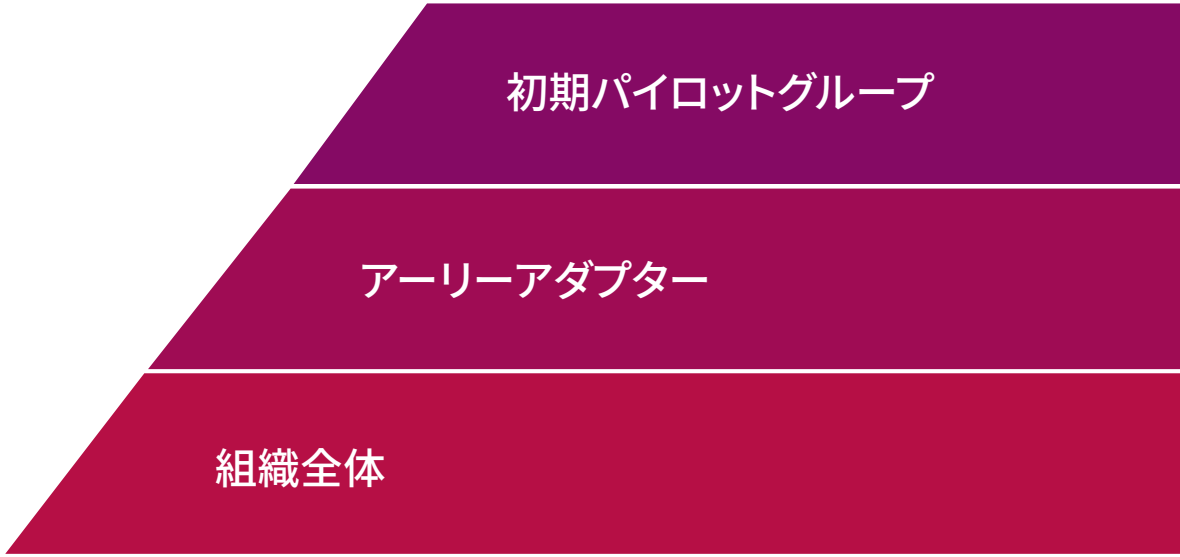
このユースケースの場合、パッチ管理者は、完全なパッチロールアウトの一部として、基準を設定し、各エンドユーザーに別々のグループ内の特定のロールを割り当てることができます。そして、誰がいつパッチ適用を受けるかは、オートメーションによって管理されます。

パッチ管理者は、新しいロールアウト段階の開始について、特定の応答率や直接的なユーザーフィードバックの要求など、複雑なルールや受け入れ基準で動作するように自動化プロセスをプログラムすることができます。

自動化されたメンテナンスのメリット

定期メンテナンスが自動化されると、各部門のスタッフは、コラボレーションの改善、一貫した照合プロセスのサポート、例外的な脅威が発生した場合の対処などに時間を割けるようになります。

IT運用部門とセキュリティ部門は、自動化されたセキュリティ制御を共同で開発・構成することもできます。これにより、セキュリティチームは、すべてのタスクについてIT運用チームに頼ることなく、あらかじめ決められたトリガーで起動する小規模な封じ込め操作を実行し監視することができます。

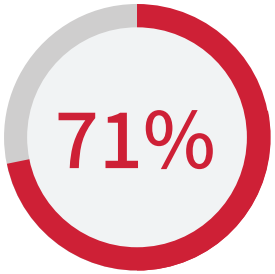


リスクベースのパッチ管理プロバイダーの選択

ITおよびセキュリティ専門家の71%は、パッチ適用は過度に複雑で時間がかかると感じています(40)。これは主に、パッチ管理戦略をサポートする適切なツールがないことが原因です。

リスクベースのアプローチを導入する前に、現在の脆弱性管理およびパッチ管理のプロセスを評価してください。セキュリティチームとIT運用チームは、プロジェクトの目標について同じ認識を持ち、使用する指標に合意する必要があります。

具体的には、両チームはアップデートの優先順位付けに、同じリスクベースのアプローチとベンダーの重要度やCVSSスコア以上のものを採用したランキングシステムを使用することに同意することが必要です。



調査対象のITおよびセキュリティ専門家の71%は、パッチ適用が過度に複雑で時間を要すると感じています(41)

新しいリスクベースのパッチ管理プラットフォームには、次のようなものが必要です。

- ☐ 深いレベルのインサイトを提供する、ネットワークスキャナ、エンドポイント、データベース、手動での調査結果、IoTデバイス、その他の独立したソースからのデータ
- ☐ 社内でサポートされているすべてのオペレーティングシステムをカバーする異機種対応
- ☐ 人が作ったソースと他の脅威インテリジェンスの両方から得られる、ランサムウェアにつながる脆弱性や悪用可能なRCEやPEの脆弱性などに関する脅威についてのインサイト
- ☐ 正確さと妥当性のために、脆弱性の本質的な属性と現実での脅威のコンテキストを考慮する、明確なリスク評価システム（自動またはセットアップ時にカスタマイズ可能）
- ☐ 組織の資産、複数の脅威情報ソース、外部からのアクセシビリティに基づく独自のリスク要因への配慮
- ☐ 自動化機能（または自動化ネットワークとの連携）による修復とリスク監視
- ☐ ユーザーのニーズや緊急性に応じて、特定のユーザープロファイルに送信可能なアラートと通知
- ☐ メール転送やチェーンリマインダーを待つことなく、適切なステークホルダーと関連情報を迅速に共有できる、既製の、またはカスタマイズ可能なダッシュボード
- ☐ エクスプロイトされた脆弱性が組織の特定の環境でどのように現れるかを示す脅威ベースのカスタマイズ可能なフィルター

参照元

1. The National Vulnerability Database（脆弱性情報データベース、2022年5月アクセス）
2. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
3. 48,285を超えるNVD未登録の脆弱性：Ivanti Researchの最新情報
4. The National Vulnerability Database,（脆弱性情報データベース、2022年5月アクセス）
5. 48,285を超えるNVD未登録の脆弱性：Ivanti Researchの最新情報
6. 48,285を超えるNVD未登録の脆弱性：Ivanti Researchの最新情報
7. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
8. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
9. 重要な脆弱性のみへのパッチ適用の問題点：Microsoftのゼロデイ脆弱性のケーススタディ
10. Bluekeepについて知っておくべきすべてのこと
11. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
12. 2016年データ漏洩調査レポート
13. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits
14. パッチ管理の課題：Everywhere Workplaceへの移行に伴う調査結果と考察 (2021)
15. Everywhere Workplaceのための主要ITトレンド (2021)
16. パッチ管理の課題：Everywhere Workplaceへの移行に伴う調査結果と考察 (2021)
17. 知っておくべきランサムウェアのトレンド 7 (2021)
18. パッチマネジメントの課題：Everywhere Workplaceへの移行に伴う調査結果と考察 (2021)
19. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
20. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
21. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
22. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits
23. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
24. IBM Security：2021年「データ侵害のコストに関する調査」レポート
25. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
26. リスクベースのアプローチによる脆弱性管理の実施
27. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
28. Microsoft Exchange ProxyShellとWindows PetitPotamの脆弱性を連鎖させた新たな攻撃
29. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
30. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
31. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
32. 拘束力のある運用指令22-01 - 悪用された既知の脆弱性についての重大なリスクの低減
33. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
34. IBM Security：2021年「データ侵害のコストに関する調査」レポート
35. ランサムウェア2022年スポットライトレポート：脅威と脆弱性管理の視点から
36. Pank, Raymond R. “What We Know About Spreadsheet Errors.” Journal of Organizational and End User Computing (JOEUC) 10, no.2: 15-21. http://doi.org/10.4018/joeuc.1998040102
37. Everywhere Workplaceのための主要ITトレンド (2021)
38. IT資産管理がジグソーパズルに似ている理由
39. 2022年5月
40. パッチ管理の課題：Everywhere Workplaceへの移行に伴う調査結果と考察
41. パッチ管理の課題：Everywhere Workplaceへの移行に伴う調査結果と考察

Ivantiについて

Ivantiは「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons自動化プラットフォームは、業界をリードする統合エ ンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの 自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合ITプラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまでIT資産の管理、検出、保護、サービスのためにIvanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

Ivanti Neurons for Patch Management について

Ivanti Neurons for Patch Management は、アクティブなリスクの露出、パッチの信頼性、デバイスのコンプライアンス、健全性、リスクに関する実用的なインテリジェンスを備えたクラウドネイティブなパッチ管理ソリューションであり、ランサムウェアなどの脅威から企業をより適切に保護するのに役立ちます。

ivanti

Ivanti.co.jp
03-6432-4180
contact@ivanti.co.jp