

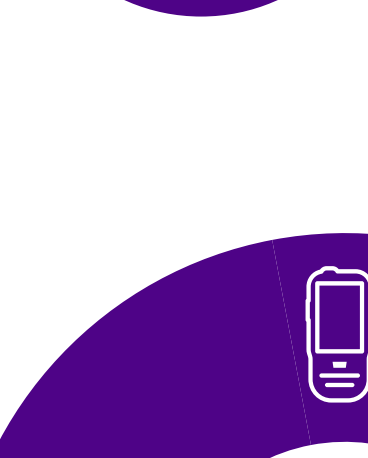
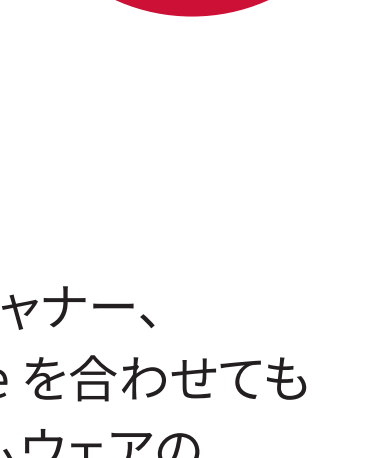
# 脆弱性管理について 修正すべき5つのこと

## 1 脆弱性の盲点

見えないものを保護したパッチを適用したりすることはできません。

### フォーチュン

1000 企業の従業員3人  
に1人は、承認されていな  
いクラウドベースのSaaS  
アプリケーションを使用



最も人気のある3つのスキャナー、  
Nessus, Qualys, Nexpose を合わせても、  
依然として既知のランサムウェアの

### 脆弱性の8%

近くを見逃している<sup>ii</sup>



## 2 チーム帯域幅の不足

存在するすべての脆弱性やリスクにパッチを適用しようとしたり、あるいは組織や環境に最も関連する脆弱性を手動で確認したりすると想像してください。



重大な脆弱性および  
エクスポージャー  
(CVEs)の総数

236,000以上



武器化されたCVE

29,000以上

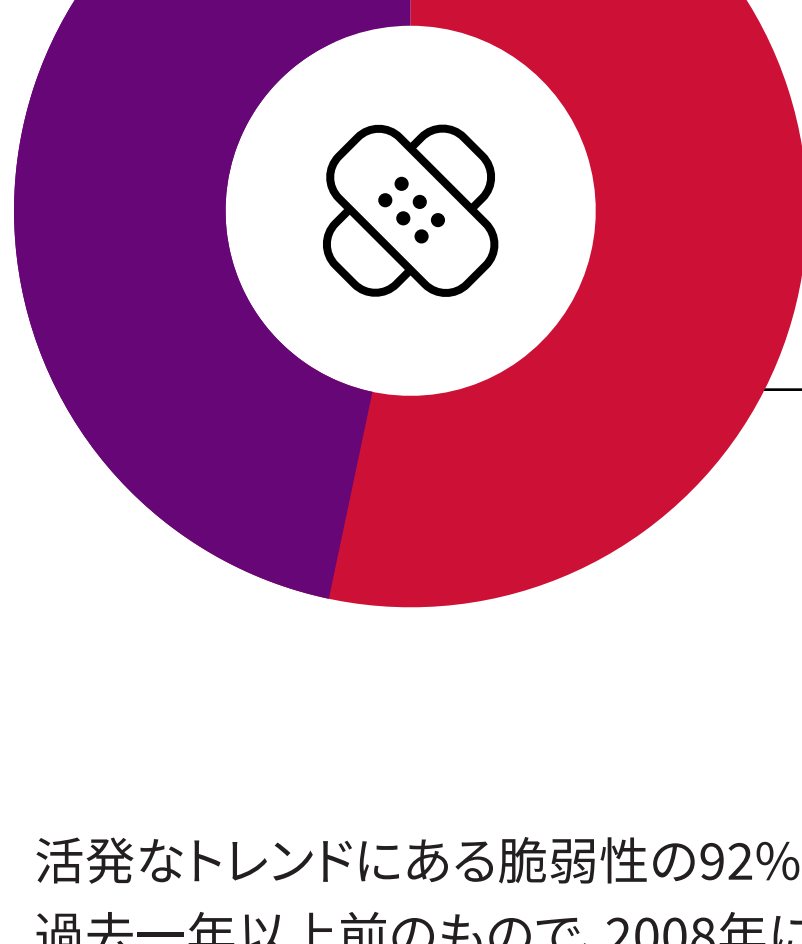


リモートコード実行  
(RCE)および/または  
権限昇格 (PE) 機能をもつCVE

9,600以上

## 3 より「重大さ」が低く古い CVEへのエクスポージャー

すべての脆弱性が同じリスクをもたらすわけではなく、さらに寿命や重大さだけでは、あなたの組織に何が関連するかはわかりません。

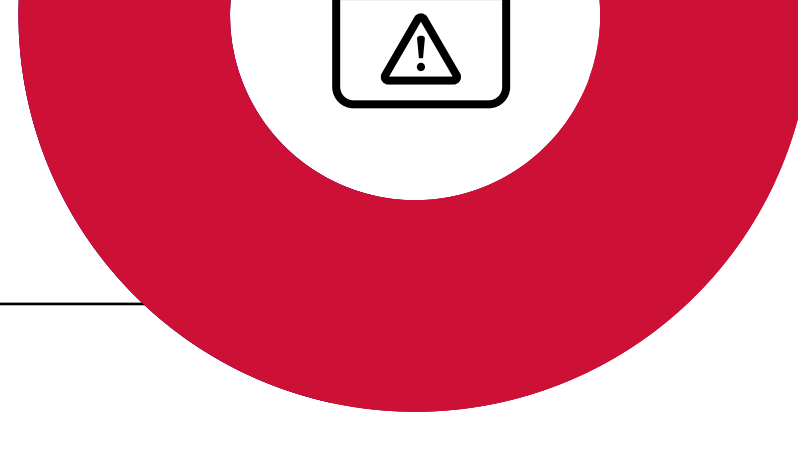


Critical格付けされたCVEにパッチを  
適用するだけでは、ランサムウェアに  
関連する悪用可能なすべての脆弱性の  
53%を見逃  
してしまうでしょう。<sup>iii</sup>

53%

活発なトレンドにある脆弱性の92%は、  
過去一年以上前のもので、2008年に初  
めて公開されたものもあります。<sup>iv</sup>

92%



## 4 少ないプログラムのリソース と社内賛同者

### 基本的 RBVM

CVSSスコアとスキャ  
ナスコアに基づく優  
先順位付け

弱点  
データの品質とスキャナの  
更新頻度に対する依存度が高い

組織固有のリスクに関連する  
低スコアの脆弱性を見逃  
している

強み  
脆弱性管理がある

### 中級 RBVM

過去1年間のCVE悪用  
可能性に基づく優先  
順位付け

弱点  
定期的な手動調整・検証が必要

依然関連性のある古い脆弱  
性を見逃す (1年以上)

強み  
CVSSスコア以外の改善策  
を優先して実施

新しい脆弱性パッチを重視

### 上級 RBVM

マルチソースの脅威  
インテリジェンス・文脈  
化された組織のリスクに  
基づく優先順位付け

弱点  
複数のデータソースをカバー  
する包括的なツールを必要とする

強み  
脆弱性データについて考え  
られるすべてのソースを含む

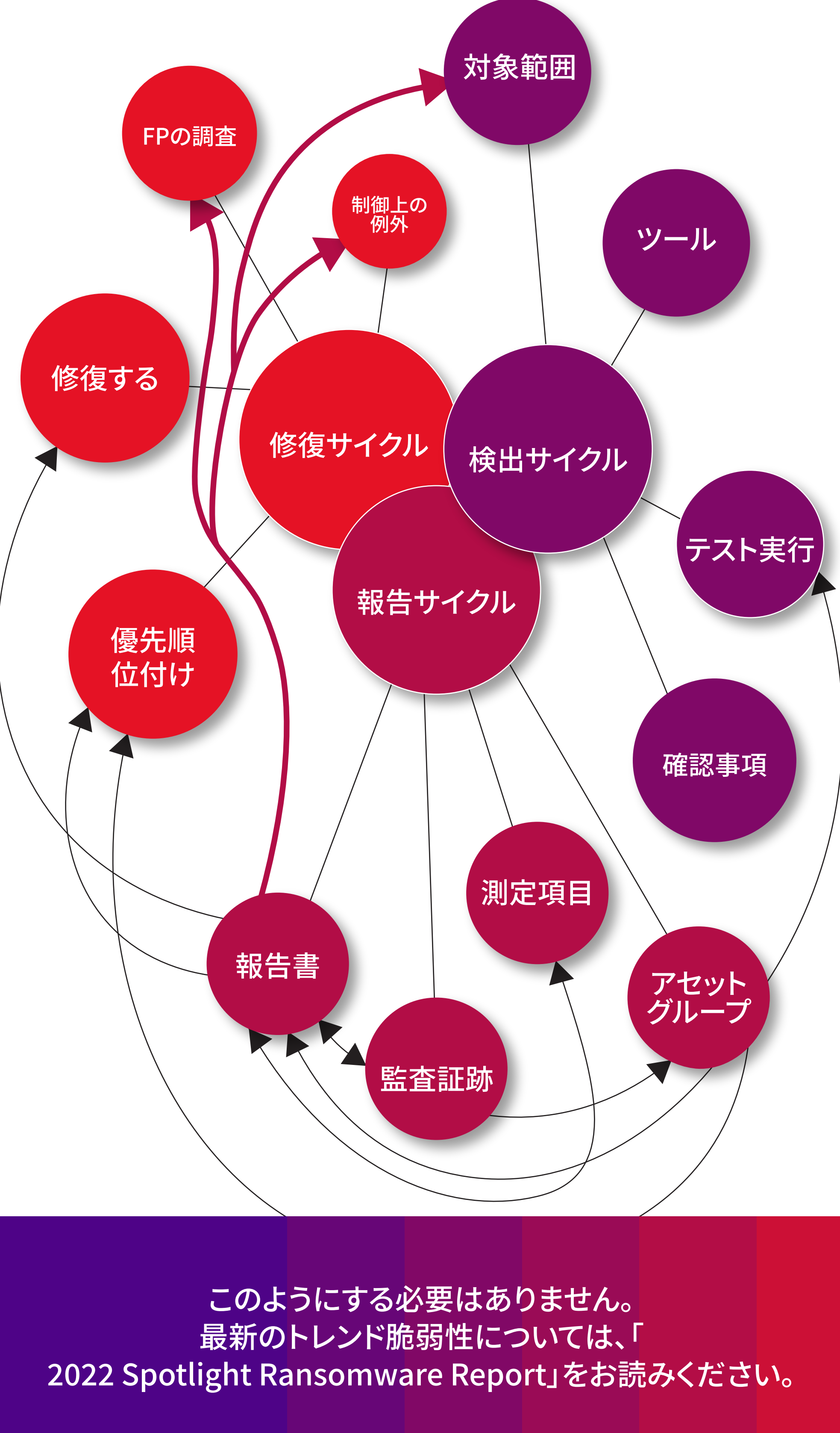
組織固有のリスクに基づく  
優先順位付け

新しいコンテキストを取り入  
れて優先順位付けを改良する  
ための迅速なレポート

## 5 報告

効果的な脆弱性管理プログラムは、適切な実行に必要な部門横断的な検出、改良、報告の張り巡らされたネットワークを作ることができます。

脆弱性情報と活動を集約、優先順位付けして表示するある種の自動化ツールがなければ、サイバーセキュリティプログラムは、開始する前に報告義務により停止させられる可能性があります。<sup>v</sup>



このようにする必要はありません。  
最新のトレンド脆弱性については、「  
2022 Spotlight Ransomware Report」をお読みください。

レポートをダウンロード

<sup>i</sup> "Why shadow IT is the next looming cybersecurity threat" (The Next Web)  
<sup>ii</sup> Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management  
<sup>iii</sup> Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management  
<sup>iv</sup> OWASP Vulnerability Management Guide (OVMG) - June 1, 2020  
Copyright 2022, Ivanti. All rights reserved. IVI-2706 06/22 FG