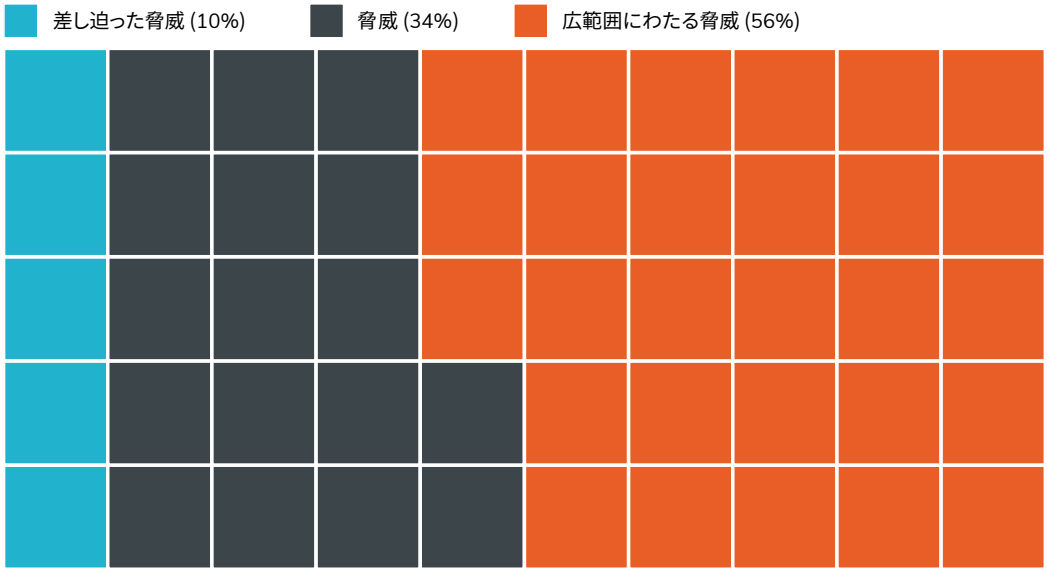
2022年脆弱性インテリジェンスレポート：状況は改善しつつも高まる複雑性

2022年は、2021年に発生した大量のエクスプロイトとゼロデイ脅威の猛攻撃と比較すると、ある意味緩やかな結果となりました。2022年に広く悪用された脆弱性は比較的少なかったものの、Rapid7の研究者が昨年調査したCVEの大部分は広く悪用された脆弱性でした。「4Shell」攻撃の大半はそれほど脅威ではなかったものの、セキュリティチームの時間と労力を大量に費やす結果となりました。エクスプロイトが判明するまでの平均時間は年々変動しますが、公開から7日以内に悪用される脆弱性の割合が高くなっており、危惧すべき状況だと言えます。

2022年の脆弱性 (脅威ステータス別)

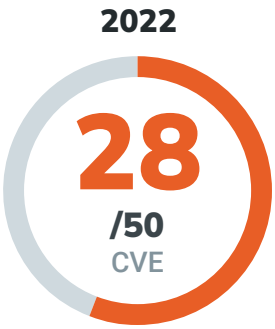


エクスプロイトステータスの比較：

積極的に悪用

エクスプロイトレベルの比較：

広範囲



エクスプロイトまでの時間の比較：

7日以内

2022

56%

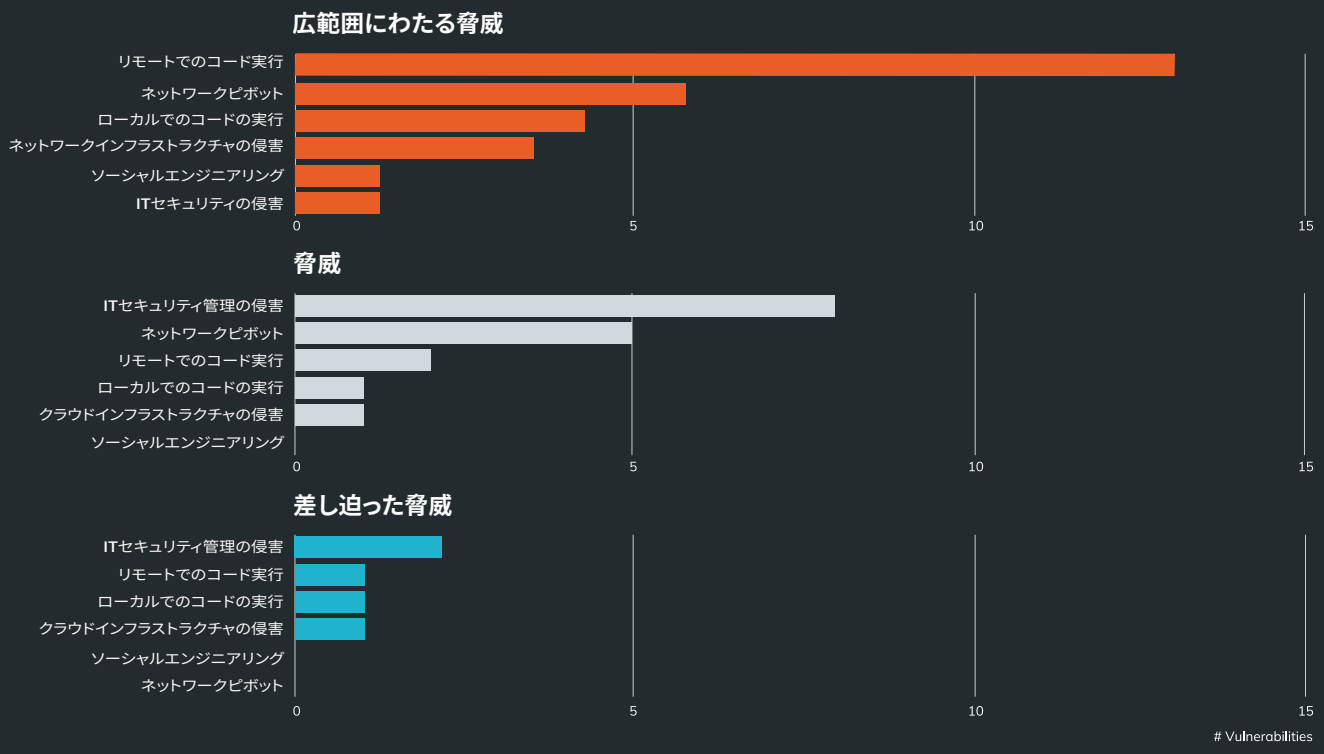
一般公開後7日以内

2021

50%

一般公開後7日以内

2022年の脆弱性 (攻撃者ユーティリティおよび脅威ステータス別)



2022年における脆弱性の優先順位付けは微妙なものといえ、Rapid7の分析では、さらなるエクスプロイトの長期化と、わずかではあるものの、攻撃の減少という両局面が明らかになっています。2023年以降も、新規・既知の脅威から被害を受けるリスクを軽減するためには、これまでと同様、しっかりとした脆弱性管理の実践が必要不可欠となります。

Rapid7の2022年脆弱性インテリジェンスレポートの全文を入手(英語)

レポートをダウンロード(英語)