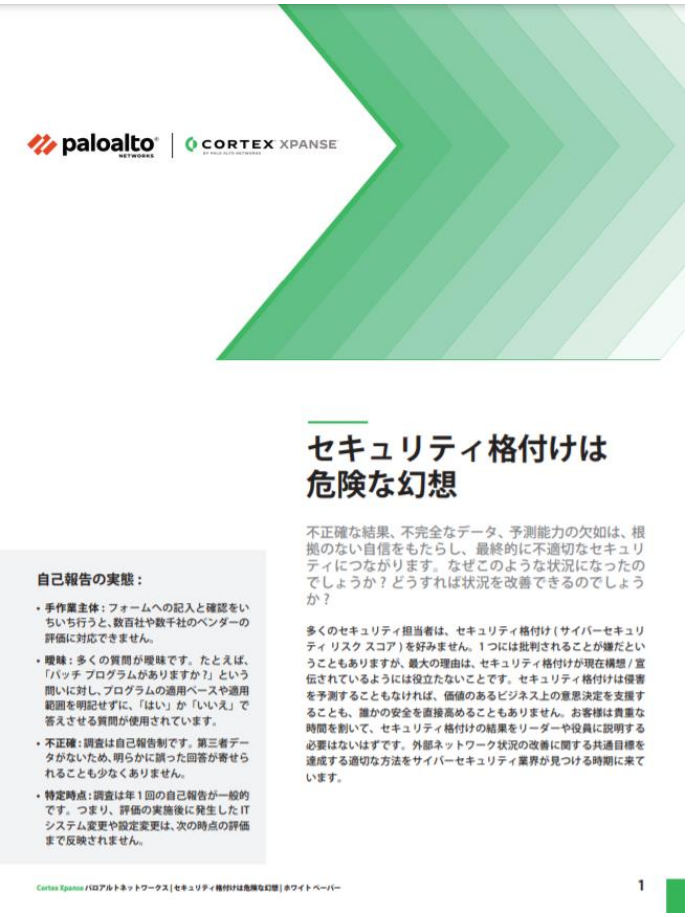
Cortex Xpanse_WP_SecurityRatings-JP

セキュリティ評価: 危険で誤った方法
ホワイト ペーパー


paloalto NETWORKS | CORTEX XPANSE

セキュリティ格付けは
危険な幻想

不正確な結果、不完全なデータ、予測能力の欠如は、根拠のない自信をもたらし、最終的に不適切なセキュリティにつながります。なぜこのような状況になったのでしょうか？どうすれば状況を改善できるのでしょうか？

多くのセキュリティ担当者は、セキュリティ格付け（サイバーセキュリティ リスク スコア）を好みません。1つには批判されることが嫌だということもありますが、最大の理由は、セキュリティ格付けが現在構想／宣伝されているようには役立たないことです。セキュリティ格付けは侵害を予測することもなければ、価値のあるビジネス上の意思決定を支援することも、誰かの安全を直接高めることもありません。お客様は貴重な時間を割いて、セキュリティ格付けの結果をリーダーや役員に説明する必要はないはずです。外部ネットワーク状況の改善に関する共通目標を達成する適切な方法をサイバーセキュリティ業界が見つける時期に来ています。

自己報告の実態：

- 手作業主体：フォームへの記入と確認をいちいち行うと、数百社や数千社のベンダーの評価に対応できません。
- 曖昧：多くの質問が曖昧です。たとえば、「パッチ プログラムがありますか？」という問いに対し、プログラムの適用ベースや適用範囲を明記せずに、「はい」か「いいえ」で答えさせる質問が使用されています。
- 不正確：調査は自己報告制です。第三者データがないため、明らかに誤った回答が寄せられることも少なくありません。
- 特定時点：調査は年1回の自己報告が一般的です。つまり、評価の実施後に発生したITシステム変更や設定変更は、次の時点の評価まで反映されません。

Cortex Xpanse パロアルトネットワークス | セキュリティ格付けは危険な幻想 | ホワイト ペーパー

1

セキュリティ パフォーマンスの指標を見直す

セキュリティ管理に妥協は禁物です。セキュリティ評価のような古いやり方から得られるものは、セキュリティに対する誤った自信だけです。本当に必要なものは、サプライチェーンを含む攻撃対象領域を絶えず管理する手段です。

このホワイト　ペーパーではリスク評価の限界を明らかにした上で、サイバーセキュリティ体制と組織のパフォーマンスの改善に向けたより良いアプローチを検討します。