NVC NETWORK VALUE COMPONENTS

REDSEAL

ネットワークの現状を可視化してセキュリティの穴を埋める

RedSealセキュリティ分析プラットフォーム

何故、想定と現実にギャップが生まれるのでしょうか？

86%
実際に発生していることを見る能力と、
理解する能力の間にギャップがあり、
それがハイレベルなセキュリティ対策が
実現しない理由になっている

84%
異なるグループでの運用や
製品、技術の繋ぎ合わせなどで
サイロ化したネットワークにより、
セキュリティ対策がなかなか進まない

79%
見えないもの
理解できないものは
安全とは思えない

32%
グローバルに展開している
ネットワークを完全に
可視化できている

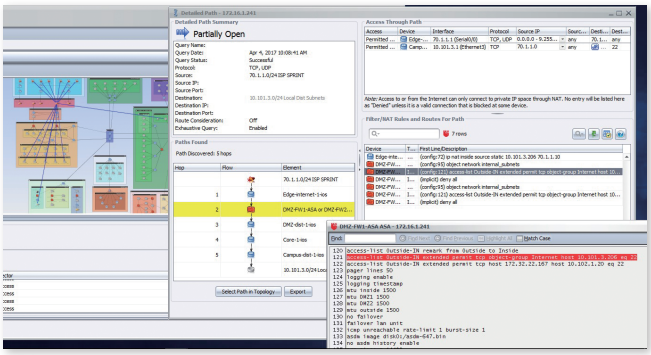
29%
自社ネットワークが、
現在ハッカーに攻撃されている、
という事実を把握している

Reference：RedSeal Strategic Security Study First Half 2015, Cisco ASR 2015, Cyberthreat Defense Report 2014, FireEye Study 2014

REDSEAL

ネットワークの実態把握

■ 全てのアクセスパスの道順を把握していますか？
■ 外部から重要DBへのアクセスパスはないですか？
■ デフォルトパスワードの使用など、
安全でない設定を使用していませんか？
■ コンプライアンスに反する設定はありませんか？

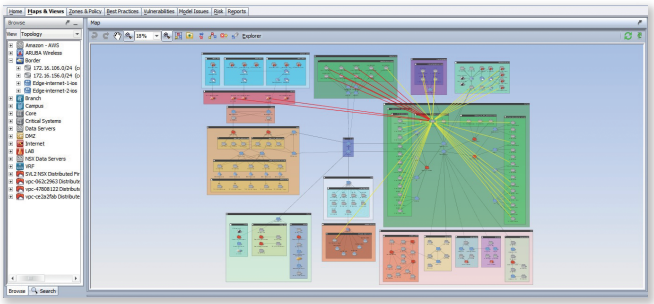


▲ Detailed Pathの機能で、アクセスパスがどのデバイスを通っているか、どの設定がそのアクセスを可能にしているのか情報を提示します。

ネットワークは、機器の新規導入や日々の運用での設定変更作業などにより、管理者が把握している状態と異なる状態になっている可能性があります。初期構築時には安全であったネットワークにも、攻撃者が利用できてしまう、予期せぬアクセスパスが存在しているかもしれません。しかし、人手でネットワークを完全に把握しようとするのは困難です。当たり前となったパブリッククラウドの利用に、導入が進むSoftware Defined Network（SDN）。物理環境もルーターが多段で組まれ、NATやファイアウォールルールなどのセキュリティの設定がアクセスパスの把握をより困難にします。このように複雑になってしまったネットワークを人手で正確に把握しようとすることは、現実的ではありません。
RedSeal社が提供するセキュリティ分析プラットフォームは、コンフィグレーションを読み取り、Network Address Translation（NAT）やAccess Control List（ACL）、ファイアウォールルールを反映させた、正確なネットワークのアクセス構成図を表示することができます。Amazon Web Service（AWS）やSDNの環境にも対応し、どのような環境であっても、同一画面で表示し、アクセスパスの一元管理を可能にします。
更に、RedSealは安全ではない設定、コンプライアンスに反する設定の洗い出しも行ないます。ネットワークベンダーそれぞれが出しているBest Practice Guideや、PCI-DSS、NERC-CIPなどコンプライアンスの情報を保持し、コンフィグレーションから読み取った情報に照らし合わせていきます。現在のネットワークの設定ミスやコンプライアンスから外れている設定をあぶりだすだけでなく、より安全なネットワークにするためのガイドとなります。

経路情報＋脆弱性情報でセキュリティ対策の優先順位付け

■ 自社ネットワークにとって深刻な影響を及ぼす脆弱性と、
そうではない脆弱性の判別はできていますか？
■ 一つの脆弱性が攻略されたとき、攻撃者が
次にどこまでアクセスできるのか、把握できていますか？



▲ 脆弱性を持つホストから直接アクセス可能なサブネット（赤線）、万が一攻略されたときに二次的にアクセスが可能になるサブネット（黄線）を数クリックで把握することが可能です。

日々、様々な脆弱性の情報が公開されています。ネットワーク運用担当者は、どうやってその優先順位を決めているのでしょうか。CVSSスコアでしょうか。CVSSスコアは、脆弱性自体の深刻さの度合いであり、自社のネットワークへの影響は考慮されません。セキュリティのリスクを低減するためには、自社ネットワークへの影響が大きい脆弱性から対処していくべきです。
RedSeal社が提供するセキュリティ分析プラットフォームは、数多くの脆弱性診断ツールと連携し、実際に攻撃される可能性とその場合のビジネスへのリスクを考慮した、RedSealリスクスコアを算出します。深刻な脆弱性だが外部からのアクセスパスは存在しない場合と、深刻な脆弱性ではないがインターネットからアクセス可能な場合。どちらの方が、脆弱性対処の優先順位が高いでしょうか。RedSealはCVSSスコアなどの一般的なスコアに加え、アクセスパスの有無、そのホストからアクセス可能な範囲、ホストのビジネスバリューを考慮し、自社ネットワークへの影響を基にした脆弱性対策の優先順位付けを行ないます。
一般的なCVSSスコアだけを見てもわからない、脆弱性が自社ネットワークへ与える影響をRedSealセキュリティ分析プラットフォームが正確に可視化します。

リスク要素	REDSEALプロセス
重要度	NIST NVDとCVSSスコアを毎週アップデート
可能性	攻撃の可能性を計算
インパクト	ホストのビジネスバリューを考慮

▼

REDSEAL
リスクスコア

NVC NETWORK VALUE COMPONENTS
株式会社ネットワークバリューコンポネンツ
〒144-0035 東京都大田区南蒲田2-16-2
電話：03-5714-2050　　http://www.nvc.co.jp/

(redseal_v2_B73)