RedSeal 脆弱性分析機能とユースケース

はじめに：

RedSeal のソリューションは企業の脆弱性対策をより向上させる機能を搭載しています。他社製脆弱性スキャナによりスキャンしたデータを RedSeal に取り込み、ネットワークの経路情報などの情報と合わせて分析することが可能です。
その結果どのホストの脆弱性を優先的に対処する必要があるかの情報を提供することが可能です。従来の脆弱性対策は、脆弱性スキャナの情報のみに頼ったやり方で実施していたため、的確に優先順位を付けた対策を行うことは難しい状況でした。
RedSeal を利用することで効果的に脆弱性対策を行うことが可能となります。

RedSeal 脆弱性機能を活かすための条件：

RedSeal の脆弱性機能は他社製脆弱性スキャナのデータを取り込み分析することで機能します。対応している脆弱性スキャナ製品は以下の通りです：

- Alert Logic (Critical Watch) FusionVM
- Digital Defense Frontline
- BeyondTrust Retina CS
  BeyondTrust (eEye) Retina Network Security Scanner
- McAfee Vulnerability Manager
- Outpost24 OUTSCAN, HIAB
- nMap
- Qualys QualysGuard
- Rapid7 NeXpose
- Symantec Vulnerability Manager
- Tenable Nessus
- Tripwire (nCircle) IP360

RedSeal を活用した脆弱性対策のユースケース：

脆弱性スキャナを利用している企業は膨大な量の脆弱性情報に埋もれているのが現状です。一ホストにつき何十もの脆弱性をネットワークに存在するホストの数と掛け合わせると、何千、何万行もの脆弱性データが毎日出力されます。そのデータの使い方は、と言うと脆弱性の危険度を表す数値、もしくは脆弱性スキャナのセビリティ（High、Medium、Low）を頼りにパッチング作業を実施する、と言うやり方がほとんどです。

数値やセビリティをもとにパッチングをすると、危険度またはセビリティの高い順から作業をするので日々増して行く脆弱性に追いつけず、ハイスコア、もしくはハ

イセビリティの脆弱性しかパッチングされていないケースが多く見られます。その結果かなりの量の脆弱性が未パッチ済み、と言う事になります。その未パッチ済みの脆弱性の中に、踏み台攻撃の性質を持ち（即ち攻撃者がホストを乗っ取りそこから 2 次攻撃を展開できる状態になり得る）、その上そのホストが乗っ取られかつ機密性の高いネットワークにアクセスが可能と言う事実が明らかだとすると、本来であればその様なホストのパッチングは数値もセビリティも関係なくすぐパッチングする必要があります。しかし、現状はその様な情報がないため必要な対策が的確に行えていません。

そもそも数値もセビリティも高い脆弱性があってもその脆弱性を持つホストが外部から攻撃できない、そしてそのホストから機密性の高いネットワークにアクセスが可能ではない、と言う事実が分かればパッチングをしても徒労にすぎないと言っても過言ではありません。

RedSeal は以上の様な脆弱性対策においての悩みを解消する事ができます。結果、優先順位を付けて的確に脆弱性対策を実施することが可能になります。

RedSeal Risk Score（リスクスコア）：

RedSeal ではリスクスコアと言うメトリクス（数値）をもとに脆弱性の脅威を表します。このスコアは複数のメトリクスから成り立っています。（“図 1：RedSeal Risk Score（リスクスコア）”を参照）

10.101.3.0/24 Local Dist Subnets

Details | Devices | **Hosts** | Vulnerabilities

75 rows

Name	IP Address	Vulnerability Co...	Primary Service	Value	Attack Depth	Exposure	Risk	Downstream Risk
10.101.3.206	10.101.3.206	3	ssh	20	1	0.99	20	10,529
10.101.3.239	10.101.3.239	3	POP3	10	2	0.77	8	0
WinServ6	10.101.3.133	0	NetBIOS Session Service	10	Unreachable	0	0	0
10.101.3.124	10.101.3.124	4	HTTP	50	2	0.74	37	0
WinServ9	10.101.3.171	60	ssh	20	2	0.98	20	0
10.101.3.135	10.101.3.135	2	ssh	20	2	0.98	20	0
WinServ7	10.101.3.167	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ1	10.101.3.147	15	NetBIOS Session Service	10	2	0.93	9	0
WinServ2	10.101.3.131	11	SMTP	60	2	0.93	56	0
10.101.3.168	10.101.3.168	2	ssh	20	2	0.98	20	0
10.101.3.165	10.101.3.165	0	ssh	20	Unreachable	0	0	0
WinServ7	10.101.3.134	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ8	10.101.3.136	0	ssh	20	Unreachable	0	0	0

図 1: RedSeal Risk Score（リスクスコア）

- Value
  - 各ホスト上で動作しているアプリケーションの価値を数値化（例：SSH 20, HTTP 50, DB 75 等）
- Attack Depth
  - “攻撃深度”、即ち信頼性の低い（例えばインターネット、DMZ、や第 3 者に繋がっているネットワークの事を言う）ネットワークからどれだけ直接的に攻撃が可能なのかの度合い

- 数値は 1：直接攻撃可能、2：間接的に攻撃可能、Unreachable：攻撃不可能

- Exposure
  - 脆弱性には CVSS スコアと言う数値があり、その数値は脅威の概要的な危険度を表します
  - RedSeal では CVSS スコアと Attack Depth、そして RedSeal 独特のアナリティクスを含めた計算をし、Exposure と言う独特の“露出度”の数値を弾き出します

RedSeal Risk Score は Value と Exposure を掛け合わせた結果のセキュリティメトリクスです。

- Value x Exposure = RedSeal Risk Score

RedSeal Downstream Risk Score（ダウンストリームリスクスコア）

RedSeal では Risk Score、踏み台攻撃を考慮し、対象となるホストが乗っ取られたことを想定し、そのホストからアクセス可能なホストすべての Risk Score を合算した数値を計算する事ができます。この数値は Downstream Risk Score と言うメトリクスです。RedSeal はネットワークの繋がり、そして ACL・NAT 等を考慮したアクセス全てを把握できます。そのナレッジを脆弱性情報と組み合わせると他のセキュリティアナリティクス製品には真似ができないデータを出せます。

踏み台攻撃（Leapfrog Attack）とは脆弱性の性質であり、その性質を持つ脆弱性が攻撃者に攻略された際にホストを乗っ取られる事が可能になる為、危険な性質とみなされます。踏み台攻撃があるとなると、そのホストからアクセスが可能（即ち 2 次攻撃の対象となるホスト）なネットワークを把握する事が最重要事項となります。踏み台攻撃を持つホストは優先的にパッチングを施す必要性が高いと思われます。

RedSeal Downstream Risk Score はまず始めに踏み台攻撃が可能か否かを確認します。次に、その踏み台攻撃が攻略されると仮定して当該ホストからどれだけの攻撃範囲があるのかの“ダメージポイント”的な数値を計算します。（“図 2：RedSeal Downstream Risk（ダウンストリームリスク）の仕組み”を参照）

この様な計算をする為にはネットワークの繋がりとファイアウォールやルータの ACL、NAT 等を把握していないと計算できません。

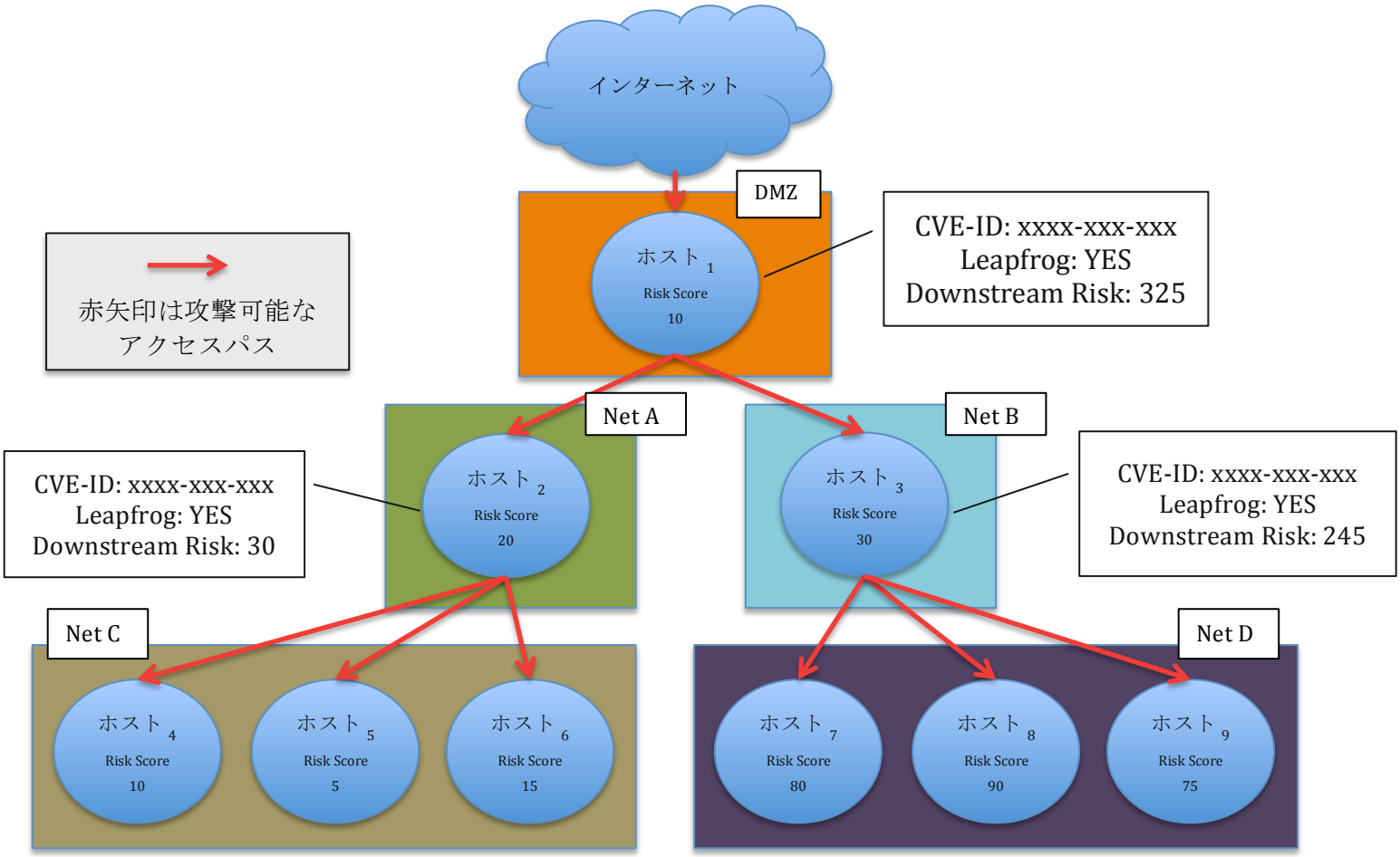

図 2: RedSeal Downstream Risk（ダウンストリームリスク）の仕組み

最後に：

RedSeal の脆弱性機能から計算される Risk Score と Downstream Risk Score は脆弱性対策に大きく貢献します。ネットワークのアクセスを考慮しない脆弱性のパッチング作業は徒労と言っても過言ではありません。Risk Score と Downstream Risk Score を基に実施するパッチング作業は最も脅威に晒されているホストから優先的に対応できるので、脆弱性対策の向上に大きく貢献します。