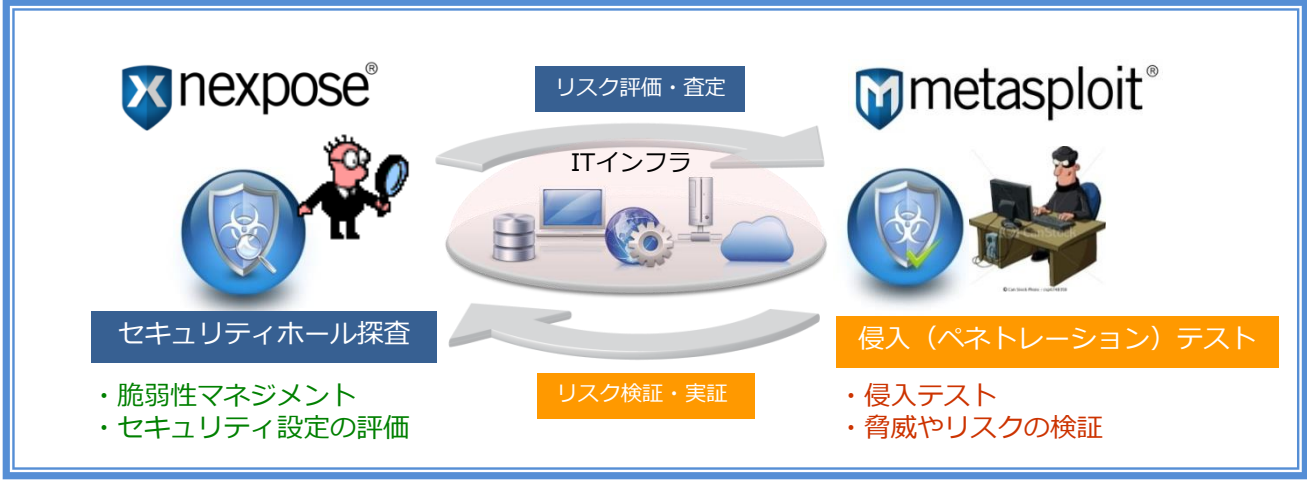


最強の脆弱性対策ソリューション！

米国政府 共通設定基準認定
脆弱性検査スキャナ

業界標準！
侵入テストソリューション



セキュリティホール探査

- 脆弱性マネジメント
- セキュリティ設定の評価

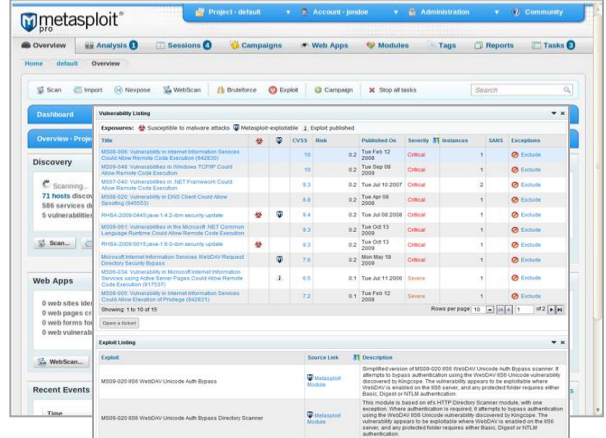
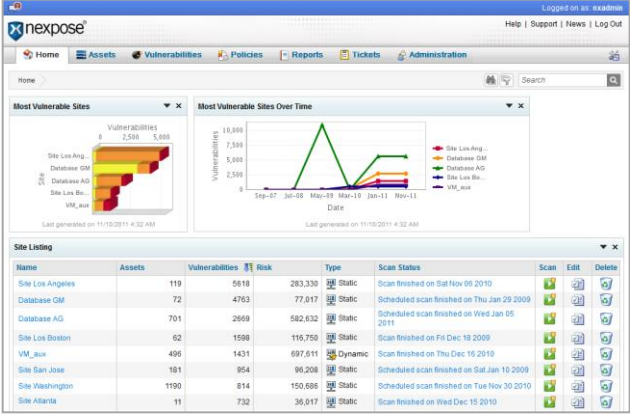
リスク検証・実証

侵入（ペネトレーション）テスト

- 侵入テスト
- 脅威やリスクの検証

■ **Nexpose (ネクスポーズ) とは？**
37,000種類以上の定義された脆弱性と100,500以上のスキャンパターンにより、仮想環境、OS、Webアプリケーション、データベースなど広範囲にわたるセキュリティ上の脆弱性や設定ミスを自動的にスキャンして、リアルタイム監視・管理を行います。

■ **Metasploit (メタスプロイト) とは？**
ネットワーク外部や内部から侵入を試み、スキャンツールで検知された脆弱性の存在を実証します。これにより脆弱性対策を行った後にその対策が十分適用されているかチェックする事が可能です。



脆弱性を探査

侵入テスト

対策

- 修正パッチの適用
- 設定ミスの修正
- IDS/IPS/WAFなど機器の導入など

■ Nexpose の特徴

1. 豊富なスキャンパターン

37,000種類以上の脆弱性定義と100,500以上のスキャンパターンにより、OS、仮想環境、Webアプリケーション、DBなどの様々な脆弱性について高い精度で検査できます。Nexposeインテリジェントスキャンエンジンは、発見した脆弱性から自動的に関連する脆弱性も検出します。

2. 確実なセキュリティ基準遵守のチェック

様々なセキュリティ基準（PCI DSS, FDCC, USGCB, HIPAA, NERC/FISMAなど）を順守しているか確実にチェックできます。

3. 仮想化環境の脆弱性検査も可能

Vmware EPSEC（End Point Security）APIに対応していますので、ハイパーバイザーレイヤーの脆弱性検査が可能です。そして、仮想資産の移動が多い環境でも「vAsset Discovery」機能と、「移動資産グループ分け」機能によりグループごとの脆弱性検査が可能です。

■ Metasploit の特徴

1. 様々なネットワーク資産に侵入テストが可能

サーバ、スイッチ、ルータ、データベース、Webアプリケーション、仮想マシンなどに対して、様々な方法で侵入を試みる事が可能です。

2. サードパーティツールとの連携

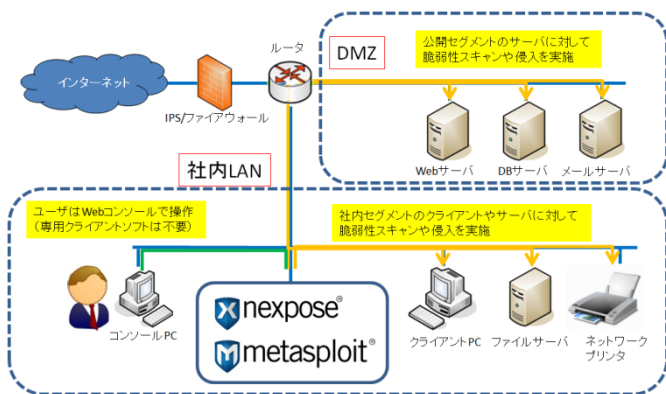
Nexposeとの連携だけでなく、他社スキャンツールとXMLファイルにより連携可能です。

3. 信頼の証

世界の11万人以上のユーザに支えられたMetasploitコミュニティの協力により、ユーザ間で共有された有益な情報を基に日々改良しています。

エディション	nexpose® Community	nexpose® Express	nexpose® Consultant	nexpose® Consultant Pro
Webアプリケーション	—	標準サポート	標準サポート	標準サポート
PCI DSSオプション	—	標準サポート	標準サポート	標準サポート
SCADAスキャンオプション	—	—	標準サポート	標準サポート
FDCC/USGCBベーススキャンオプション	—	—	標準サポート	標準サポート
スキャン機能				
スキャン可能なIPアドレス数	32	128~1024	256~1024	65534
既知の脆弱性スキャンテンプレート	✓	✓	✓	✓
スキャンテンプレートのカスタマイズ	—	✓	✓	✓
(VMware)仮想化資産の自動探索機能*	—	—	✓	✓
ネットワーク脆弱性	✓	✓	✓	✓
OS脆弱性	✓	✓	✓	✓
デスクトップアプリケーション脆弱性	✓	✓	✓	✓
Webアプリケーション脆弱性	—	✓	✓	✓
データベース脆弱性	✓	✓	✓	✓
FDCC, USGCBポリシーに則したスキャン評価	—	—	✓	✓
SCADAスキャン	—	—	✓	✓
PCI DSSに準拠したスキャン	—	✓	✓	✓
Metasploitとの統合	✓	✓	✓	✓

社内資産を対象としたシステム構成例



導入実績 65カ国/2000社以上!

