業界最高クラスの正確さを誇る脆弱性スキャナと
世界最高クラスの「侵入試験ツール」の組み合わせによる
リアルなリスクに対応した唯一の脆弱性対策ソリューション！

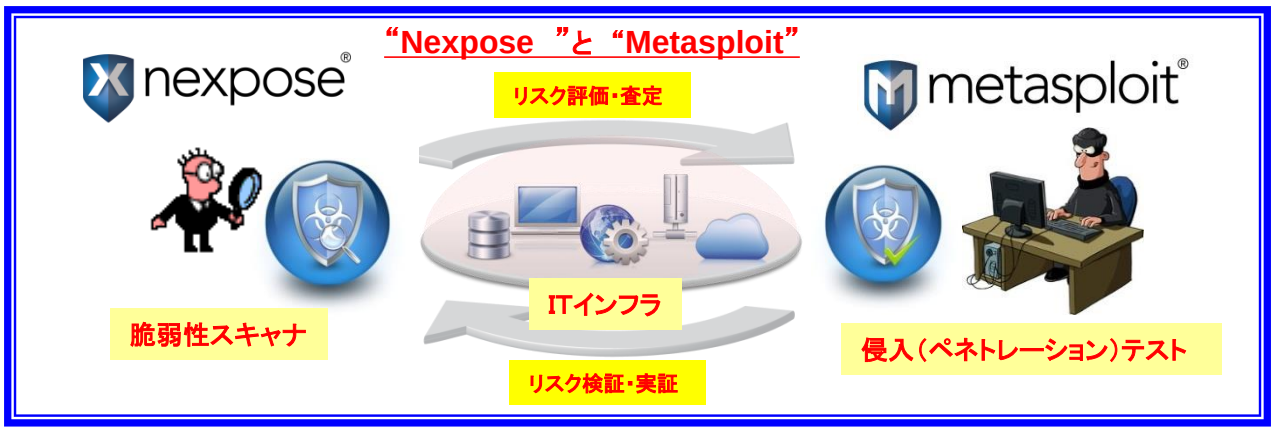
RAPID7

nexpose® metasploit®

日本語レポート対応！

Metasploit projectの創設者であるH.D.ムーア氏を擁するRapid7社(米国) は、オープンソースの侵入(ペネトレーションテスト)ツールでは、業界標準となっている「Metasploit Framework」を基に徹底的に改良を行い、最新のサイバー攻撃の演習機能が付与された「Metasploit Pro」と、企業インフラの脆弱性を具体的な脅威度に応じてスコアリングを行う「Real Risk Score」(特許出願中)を搭載する脆弱性スキャナ「Nexpose」を有した「統合型セキュリティリスク・インテリジェンス・ソリューション」を提供できる業界で唯一のセキュリテイ・ソリューションプロバイダです。

Nexpose と Metasploit により、全ての顧客は脅威やリスクへの対応策について正確で実用的な解決方法を得ることができます。
Rapid7社のソリューションは、66以上の国の2,000以上の企業や政府機関で使用されており、同社の無償の製品は年間100万回以上ダウンロードされ、200,000人を超えるセキュリティコミュニティのユーザや投稿者によって日々進化しています。

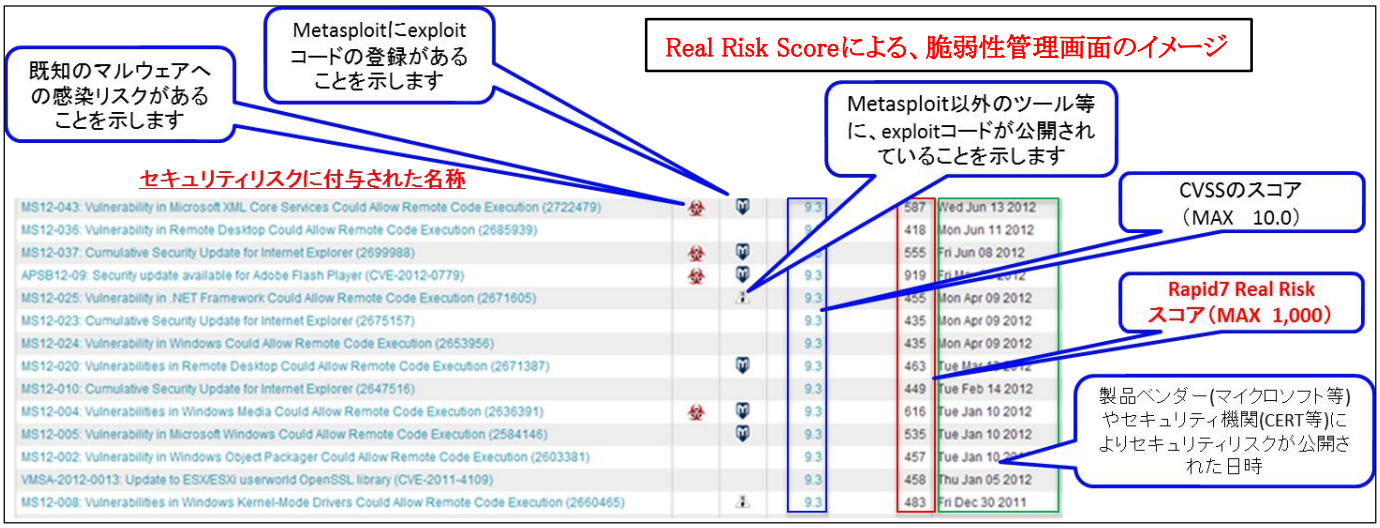


脆弱性スキャナ nexpose® の特長(一部抜粋)

“Nexpose”はNIST (アメリカ国立標準技術研究所)によるUSGCB(米国政府共通設定基準)認定を得た、最初のITセキュリティ管理用の脆弱性スキャナです。Nexposeを使用することで、真のリスクに基づいた脆弱性管理環境を御社に構築できます。

● Real Risk Scoreによる、脆弱性管理

Nexposeは、発見した脆弱性を「既知のマルウェアへの感染リスクがあるか」、「Metasploitに攻撃コードが登録されているか？」、「CVSS(世界標準の脆弱性評価基準)におけるスコアはいくつか」、「その脆弱性がいつ発見されたのか」の4つ要素でスコアリングを行う「Real Risk Score」機能を有しています。優先的に対処すべき脆弱性が一目で分かるため、他社製品を使用する場合に比べ、管理工数が大幅に削減されます。



● 業界最高クラスの脆弱性検知精度

Nexposeは脆弱性の登録数が42,000件、脆弱性検出用のプラグイン数が115,000件と業界最多の脆弱性データベースを有しています(2014年5月現在)。その為、脆弱性スキャナで最も重要視される、誤検知・検知漏れが少ないのもNexposeの特長です。
Nexposeの脆弱性データベースの少なくとも週1回以上、緊急性の高い脆弱性については24時間以内にアップデートとして反映します。

CORNET TECHNOLOGY 日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2 〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp

先ずは評価版で、Rapid7の脆弱性改善ソリューションを体験してください！

RAPID7

侵入（ペネトレーション）テストツール metasploit® の特長（一部抜粋）

● GUIによる直感的な操作

オープンソースの「Metasploit Framework」は操作をコマンドラインで行う必要があり、更にPerl言語の習得等の必要性があることから、侵入（ペネトレーション）テストが出来るのは一部の方に限られていました。商用版である「Metasploit Express」及び、サイバー演習向けの機能を有した「Metasploit Pro」は、洗練されたGUIにより、多くの方に侵入（ペネトレーション）テストを行う環境を提供します。また、既に「Metasploit Framework」をお使いの方に対しても、テスト工数の削減と、結果レポート出力機能等、テスト業務の効率向上に寄与する機能を備えています。

● 侵入（ペネトレーション）テストに有効なコードを自動選択

「Metasploit Framework」を含め、多くの侵入（ペネトレーション）テストツールは、ユーザ自身が試験に使用するコード（エクスプロイトコード）とその対象を選択する必要がありましたが、これは間違った試験を行ってしまう可能性がありました。商用版のMetasploitは、品質が保証された世界最大のデータベースから、コードその実行を補助するモジュールを選定し、ユーザに提示します。各コード及びモジュールにはその信頼性に応じて5段階でランキングされています。これは侵入の成功率及び試験対象（サーバ、クライアントPC等）に及ぼす影響度を示しています。

● 脆弱性スキャナと統合する

Nexposeおよびサードパーティ製脆弱性スキャナからスキャンデータをインポートします。Nexposeによるスキャンは、MetasploitのGUI上から直接行うこともできます。

● 脆弱性を改善する時間を減らす

Metasploitを使用することで、どの脆弱性が実際に悪用可能である改善されなければならないのか、またどの脆弱性がそうではないのかを確認することが可能です。その為、脆弱性管理に費やす時間が減り、貴社のセキュリティ関連コストが削減されます。

● 脆弱性を持った機器の管理部門から賛同を得る

脆弱性を悪用できるということを証明することは、脆弱性もったIT資産に実際のデモを見せ、納得させることが問題を改善する最善の方法です。

● 改善策の効果を確認する

実施した改善策がエクスプロイトを防ぐことに成功したか確認し、脆弱性が実際に修正されたことを確認できます。

● ユーザの要望にあわせたラインナップ

基本的な機能を有するMetasploit Expressと、更に高度な機能を追加したMetasploit Proをラインナップ。貴社の要望に合わせた最適な組み合わせを弊社がご提案させていただきます。

NexposeとMetasploitのラインナップは以下の通りです。弊社ではRapid7製品の導入支援からアフターサポートまで一貫して行っております。

41,000種類以上の定義された脆弱性と 110,000以上のスキャンパターンをサポート

Nexpose

Community（トライアル用、商用利用禁止）

最大32のIPまで。スキャン、レポート

Express（様々な用途に使用できる汎用版）

128、256、512、1024IPの4モデル。スキャンやレポートのカスタマイズ、ネットワークやOS, DBのスキャン、PCIDSS準拠のスキャンとレポート機能を有する

Consultant（セキュリティプロフェッショナル用）

セキュリティ・コンサルタントおよびセキュリティ監査法人向け。仮想環境におけるIT資産の自動検出に対応

Enterprise（大規模環境向け）

IPアドレスに上限なし、Consultantの機能に加えマルチユーザアクセス、無制限のスキャンエンジン、任意アプライアンス等、Nexposeの全機能を使用可能

世界標準のペネトレーションテストツールと、その商用版

Metasploit

Metasploit Framework（オープンソース版、コマンドライン操作のみ）

・最新のエクスプロイトコードとペイロードをサポート

Metasploit Express (Frameworkに下記がアドオン)（セキュリティ業務御担当者に最適です）

・GUI操作対応　・Nexposeやサードパーティ製のスキャナのスキャン結果を読み込み
・セキュリティ機器（IPS/IDS/UTM等）の性能評価　・スマートブルートフォース攻撃（総当たり攻撃）機能
・侵入証拠の収集機能　・パスワード監査機能　・プロキシピボッティング機能　・レポート出力機能

Metasploit Pro (Express に下記がアドオン) (サイバー演習、セキュリティコンサルテーションに最適です)

・Webアプリケーションのスキャン機能　・VPNピボッティング機能
・ソーシャルエンジニアリングキャンペーン機能 （フィッシングメール,USB攻撃演習機能）
・サイバー演習向けチーム協力機能　・カスタマイズ可能なレポート機能　・IDS/IPS/Antivirus回避機能
・PCI-DSS ver.3.0に対応したFWのルールやネットワーク構成の確認機能と、レポート機能
・Nexposeとの統合　・VMwareとAmazon EC2仮想化対応　・永続的なセッション保持機能、等

Nexposeシステム要件

・2GHz以上のプロセッサ（デュアルコア以上）
・8GB RAM（64bit）
・80GB以上のディスクスペース（Nexposeコンソール）
・10GB以上のディスクスペース（Nexposeスキャンエンジン）

オペレーティングシステム
・Windows Server 2008 R2,2012、Windows 7, 8
・VMware ESX 4.x
・VMware ESXi 4.x、5.x
・Red Hat Enterprise Linux Server 5.x、6.x
・Ubuntu 12.04 LTS(64bit)

ブラウザ
・Mozilla Firefox 最新バージョン
・Microsoft IE 最新バージョン
・Google Chrome 最新バージョン

Metasploitシステム要件

・2GHz以上のプロセッサ
・2GB RAM
・500MB以上のディスクスペース

オペレーティングシステム
・Windows XP,2003,Vista,2008 Server,Windows 7,8
・Red Hat Enterprise Linux 5.x、.6.x x86_64
・Ubuntu Linux 8.04、10.04-x86、64、 12.04 LTS x86_64

ブラウザ
・Mozilla Firefox 最新バージョン
・Microsoft IE 最新バージョン
・Google Chrome 最新バージョン

CORNET TECHNOLOGY
日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2　〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp