



業界最高クラスの精度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！

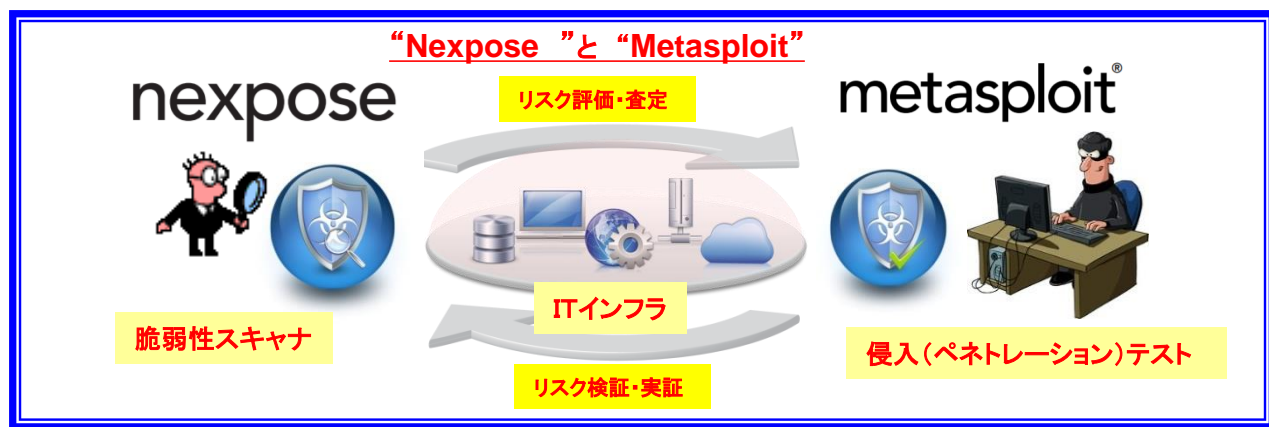


nexpose metasploit®

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™」(特許)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ィ・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。

Real Risk Scoreによる、脆弱性管理画面のイメージ

セキュリティリスクに付与された名称	既知のマルウェアへの感染リスクがあることを示します	Metasploitにexploitコードの登録があることを示します	Real Risk Score	CVSSのスコア (MAX 10.0)	Rapid7 Real Risk スコア (MAX 1,000)	製品ベンダー(マイクロソフト等)やセキュリティ機関(CERT等)によりセキュリティリスクが公開された日時
MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)	☞	☞	9.3	587	587	Wed Jun 13 2012
MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)	☞	☞	9.3	418	418	Mon Jun 11 2012
MS12-037: Cumulative Security Update for Internet Explorer (2699988)	☞	☞	9.3	555	555	Fri Jun 08 2012
AFPSB12-09: Security update available for Adobe Flash Player (CVE-2012-0779)	☞	☞	9.3	919	919	Fri May 25 2012
MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)	☞	☞	9.3	455	455	Mon Apr 09 2012
MS12-023: Cumulative Security Update for Internet Explorer (2675157)	☞	☞	9.3	435	435	Mon Apr 09 2012
MS12-024: Vulnerability in Windows Could Allow Remote Code Execution (2653956)	☞	☞	9.3	435	435	Mon Apr 09 2012
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	☞	☞	9.3	463	463	Tue Mar 27 2012
MS12-010: Cumulative Security Update for Internet Explorer (2647516)	☞	☞	9.3	449	449	Tue Feb 14 2012
MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)	☞	☞	9.3	616	616	Tue Jan 10 2012
MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)	☞	☞	9.3	535	535	Tue Jan 10 2012
MS12-002: Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)	☞	☞	9.3	457	457	Tue Jan 10 2012
VMSA-2012-0013: Update to ESX/ESXi userworld OpenSSL library (CVE-2011-4109)	☞	☞	9.3	458	458	Thu Jan 05 2012
MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)	☞	☞	9.3	483	483	Fri Dec 30 2011

● 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130,000件以上、脆弱性検出用のプラグイン数が400,000件以上と業界最多の脆弱性データベースを有しています(2018年11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は毎日更新され、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。



コーネットソリューションズ株式会社  
東京都台東区東上野1-12-2 〒110-0015  
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677  
www.cornet-solutions.co.jp

※本文中の会社名、製品名は、各社の商標又は登録商標です。

## 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。サイバー演習向けの機能を有した商用版である「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、コードと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り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ことを証明するには、脆弱性のあるIT資産に対する実際のデモを見せ、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

基本的な機能から、高度な機能までを有する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。

130,000種類以上の定義された脆弱性と  
400,000以上のスキャンパターンをサポート(※)

**Nexpose**

・同時スキャンIP数: 128、256、512、1,024...  
10,000..50,000...無制限モデルまでラインナップ

・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、仮想環境におけるIT資産の自動検出、マルチユーザアクセスを有する。

・無制限のスキャンエンジン、任意アプライアンス等を提供。

・スキャンサービスを提供するお客様用に「コンサルタント」ライセンスもラインナップ。  
※Nexposeのみ

(※)脆弱性、スキャンパターンは、日々更新、追加されています

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 Pro (Frameworkに下記がアドオン)

(セキュリティ業務御担当者からサイバー演習、セキュリティコンサルティングまで、幅広くご利用いただけます)

- ・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 ・プロキシポッピング機能 ・レポート出力機能
- ・Webアプリケーションのスキャン機能 ・VPNピポッピング機能
- ・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)
- ・100GB以上のディスクスペース

### オペレーティングシステム(64bit)

- ・Windows 7 SP1, 8.1, Server 2008 R2, 2012 R2, 2016 R2
- ・Ubuntu 14.04 LTS, 16.04LTS, 18.04LTS
- ・Red Hat Enterprise Linux Server 6.x, 7.x
- ・CentOS7, Oracle Linux7

### ブラウザ

- ・Google Chrome 最新バージョン
- ・Mozilla Firefox, FirefoxESR 最新バージョン
- ・Microsoft Edge, Internet Explorer 11

### 仮想プラットフォーム

- ・Vmware Player 6~, Workstation 9~, Fusion 8~, vCenter5.5.6.0, ESXi5.5.6.0

### Metasploitシステム要件

- ・2GHz以上のプロセッサ
- ・4GB RAM
- ・1GB以上のディスクスペース

### オペレーティングシステム(64bit)

- ・Windows 7 SP1~, 8.1, 10, Server 2008 R2, 2012 R2
- ・Ubuntu 14.04 LTS, 16.04 LTS
- ・Red Hat Enterprise Linux 5.1~, 6.5~, 7.1~

### ブラウザ

- ・Google Chrome 最新バージョン
- ・Mozilla Firefox 最新バージョン
- ・Microsoft Internet Explorer 11



vmware



amazon  
web services



## コーネットソリューションズ株式会社

東京都台東区東上野1-12-2 〒110-0015  
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677  
www.cornet-solutions.co.jp

※本文中の会社名、製品名は、各社の商標又は登録商標です。