

脆弱性リスク、パッチ適用レベル、ITアセットの管理を支援

## 脆弱性検査・監査ツール

# IBM Internet Scanner®

Internet Scannerは、ネットワークに接続されたサーバー、デスクトップおよびデバイスの脆弱性を自動的に発見し、脆弱性に対する改善アドバイスや包括的な傾向分析、明確かつ簡潔なリスク管理レポートを提供する脆弱性検査・監査ソリューションです。

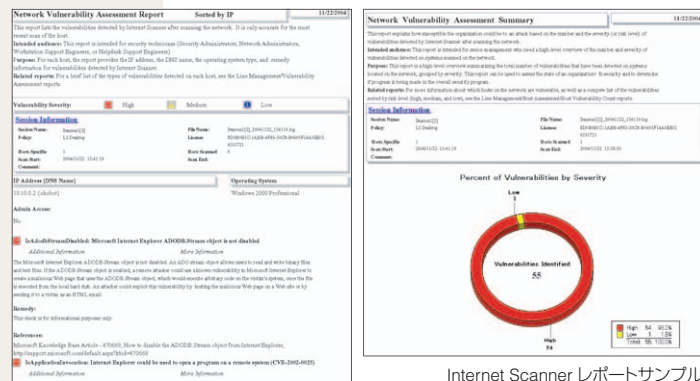
日々発見される脆弱性や企業ネットワークやシステムのセキュリティ状態を把握し、管理していくことは簡単ではありません。Internet Scannerは、ネットワーク上のシステムのセキュリティ状態の把握、管理を支援します。

さらに、大規模で複雑なネットワーク上のITアセットの管理や、ネットワーク上のシステムにおけるパッチ適用状態を自動的に管理することもできます。リスクを最低限に抑え、様々なセキュリティ侵害から保護するための改善作業や優先順位付け、そのスケジュール決定などを支援します。

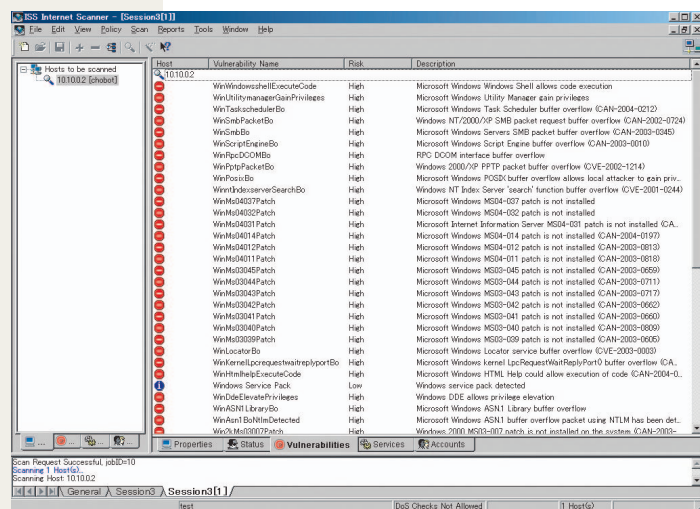
### Internet Scanner の特長

#### ● 簡単で多様なグラフィカル・レポート

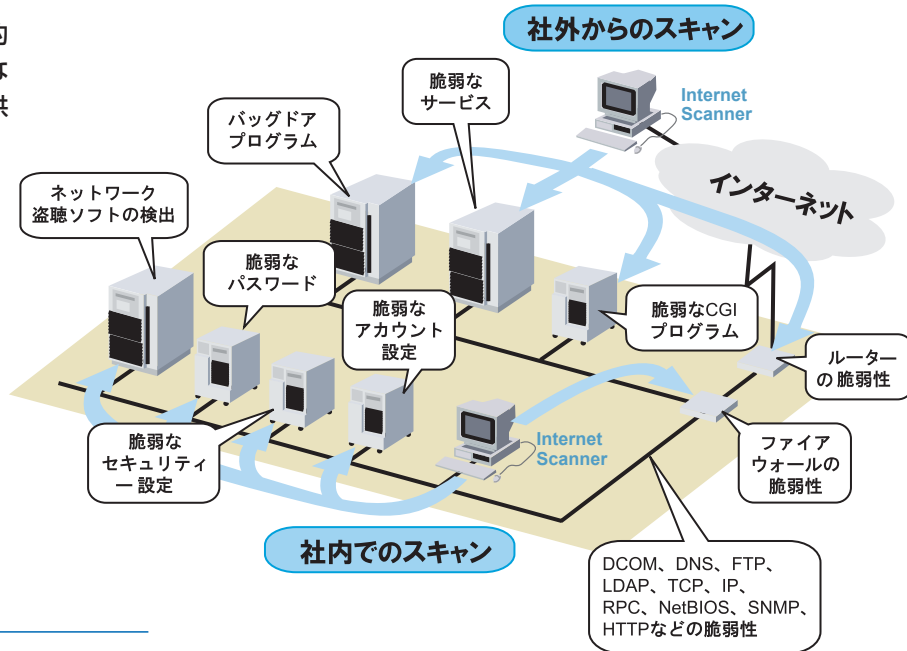
発見された脆弱性とその修正方法を記載した詳細な技術レポートから、経営者などへ提出するグラフィカル・サマリー・レポートまで、様々なレポートをPDFやHTMLなどで出力することができます。



Internet Scanner レポートサンプル



Internet Scanner画面管理は全て一元化



#### ● 高精度スキャン

Nmap Finger Print Databaseとダイナミック・チェック機能 (Dynamic Check Assignment : DCA) により、広範囲にわたる脆弱性チェックの実行を自動化することができます。スキャン対象ホストのOSを識別し、最も適切なポリシーを選択して自動的にスキャンを実行します。

#### ● ディスカバリー・スキャン機能とホスト・リスト作成と管理

ディスカバリー・スキャン機能によりネットワークに接続しているホストを自動的に探索し、OSやデバイスの種類を正確に検出します。ディスカバリー・スキャンの結果を元に、脆弱性検査・監査の対象となるホスト・リストを作成し、管理することができます。この機能を定期的にご利用することにより、ITアセットの管理を行うこともできます。

#### ● 統合管理システムProventia Management SiteProtector™による強力な情報収集と分析

リモートに設置したInternet ScannerをSiteProtectorで管理することで、企業全体の脆弱性検査・監査を、自動かつ定期的に実施することができます。SiteProtectorに、スキャン・データを集積・解析し、分析用の画面で各ホストにおける脆弱性の状態、パッチ適用レベルや脆弱性の改善状態などを多角的に簡単に把握することができます。

#### ● X-Press Updateによるチェック項目の自動更新

X-Force の脆弱性に関する最新の調査・研究結果を、X-Press Updateにより自動かつ迅速に反映することができます。

重要サーバーを守るサーバー・プロテクション

# IBM Proventia Server® Intrusion Prevention System

## IBM RealSecure® Server Sensor / IBM Proventia Server for Linux

RealSecure Server Sensor/Proventia Server for Linuxは、ホスト型ファイアウォール機能、機密データの漏洩や重要ファイルの改ざんなどを防止する内部アクティビティ監視機能、さらに、アプリケーション監視・防御機能を搭載したホスト型不正侵入防御システムです。

ネットワーク・トラフィックやOS、アプリケーション内での様々なアクティビティをリアルタイムに監視し、被害が発生する前に、不正侵入、誤使用、情報漏洩などから、重要なサーバーを保護します。サーバー上のビジネス・アプリケーションの動作や重要なデータ処理に要求される、信頼性、可用性、機密性を高めることができます。

### RealSecure Server Sensor の特長

#### ● プロトコル分析モジュール (PAM) による高精度な不正侵入防御機能

ホスト型ファイアウォール機能によるネットワーク・アクセス・コントロールと、PAMによるサーバーのネットワーク・トラフィックの送信・受信の両方を監視し、機密性、完全性、アクセスビリティを保ったまま、不正侵入や望まれない通信を検知・防御することができます。

#### ● OS監査ログやシステムログの監視

OSの監査ログやユーザーが指定するログを監視し、どのユーザーが、どのファイルに、どのような操作を行ったかなど、監査・追跡することができます。サーバー上の機密性の高いデータへのアクセスを細かく監査することで、情報が漏洩するのを未然に防ぐための対応をとることができます。

#### ● Webアプリケーション・プロテクション機能

ApacheおよびIIS Webサーバーで利用されるSSL通信 (HTTPS) を監視・分析し、通信に含まれる攻撃を検知・防御することができます。

#### ● バッファオーバーフロー・エクスプロイト・プロテクション (RealSecure Server Sensor for Windows / Proventia Server for Linux)

シグネチャーを必要としない技術により、メモリー・バッファオーバーフローを引き起こそうとする悪意のあるコードを効果的にブロックします。サーバー・システムでバッファオーバーフローを引き起こし任意のコードを実行するワームの伝搬や攻撃を防ぎます。

#### ● 柔軟で多様なレスポンス

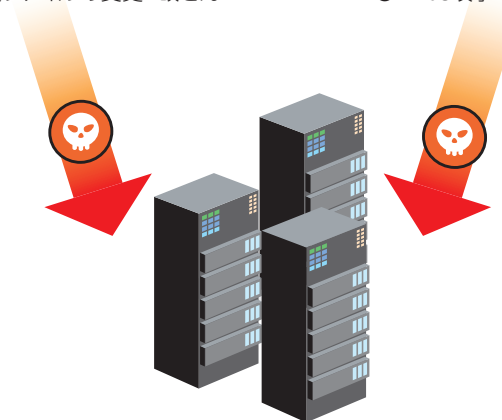
様々なイベントを検知した際、統合管理コンソールProventia Management SiteProtectorへのリアルタイム通知、管理者へのメール送信、SNMPの送信、任意のプログラムの実行など、多様なレスポンスが可能です。さらに、カスタマイズしたTelスクリプトを利用し、サーバー内で不正な操作を行ったユーザーのアカウントをロックアウトしたり、重要なファイルが改ざんされた場合に、バックアップ・ファイルを元の場所にコピーし直したりなど、柔軟で効果的なアクションを実行することもできます。

#### 企業内部からの脅威

- 悪意のある活動・振る舞い
- 許可されていないアプリケーション
- 許可されていないユーザーのアクセス
- 重要ファイルの変更・改ざん

#### ネットワーク・ベースの攻撃

- 不正侵入
- バックドア、トロイの木馬
- 悪意のあるコード
- DDoS攻撃



Proventia Server

## RealSecure Server Sensor Proventia Server for Linux

- 不正、悪意のある振る舞いからの防御
- 管理者への通知、任意プログラムの実行など

#### ● 広範囲なOSのサポート

- RealSecure Server Sensor  
Microsoft® Windows Server™ 2003
- Microsoft® Windows® 2000 Server SP1 ~ 4
- Microsoft® Windows NT® 4.0 Server SP4 ~ 6a
- HP-UX / Solaris / Linux® / Red Hat Linux 7.1

#### ● Proventia Server for Linux

- Red Hat Enterprise Linux (RHEL) 4.0 AS Updates 2 & 3
- Red Hat Enterprise Linux (RHEL) 4.0 ES Updates 2 & 3
- Red Hat Enterprise Linux (RHEL) 3.0 AS Updates 6 & 7
- Red Hat Enterprise Linux (RHEL) 3.0 ES Updates 6 & 7
- SuSE Linux Enterprise Server (SLES) 9 SP3

#### ● X-Force®の調査・研究結果に基づく高い防御技術 ~ X-Press Updateによる自動更新 ~

X-Forceによる調査・研究結果を迅速に製品に反映し、サーバーに対する最新の脅威から、実際に影響を受ける前に保護する事が可能です。最新のセキュリティ・アップデートは、X-Press Updateで自動的に更新することができます。