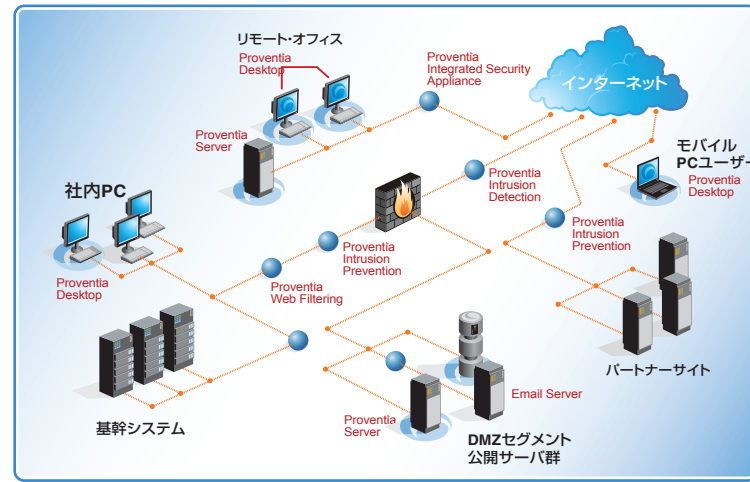


IBM Proventia® Management

SiteProtector™

Proventia Management SiteProtectorは、**IBM ISS セキュリティ・プラットフォームの全製品を集中管理することができる統合管理システムです。**

各プロテクション・エージェントの設定や、検出・防御イベントの集積、リアルタイムな表示が可能です。さらに、複数の異なる種類のエージェントからの情報を相関分析し、長中期的なイベント情報を、様々な観点から検索、解析することが可能です。さらに**X-Press Update (XPU)**により、管理するプロテクション・エージェントへ、迅速かつ容易にセキュリティ・アップデートを適用する事で、保護対象アセットは最新の脅威に対し並みそそえて対応することが可能です。**Proventia Management SiteProtector™**は企業全体のセキュリティ・レベルを維持・向上させる為の運用管理や、意思決定を強力に支援します。



Proventia Management SiteProtector の特長

集中管理

全てのIBM ISSのセキュリティ・プラットフォーム製品の設定・管理を一元的に集中管理できます。

グループ管理

IBM ISSのセキュリティ・プラットフォーム製品の管理やイベントの表示・解析は、論理的なグループを設定し、そのグループ毎に行うことができます。グループは、画面上でドラッグ&ドロップすることによって簡単に変更することができます。また、ネットワーク上のアセット管理は、IPアドレス、DNS名、NetBIOS名、OSの情報に基づいたグループへの自動振り分けが可能です。

ユーザ権限管理

Proventia Management SiteProtector を操作するユーザーに対し、Administrator ①すべての権限を持つ/Analyst ②イベントの解析/Operator ③閲覧もしくは限定的な操作のみ、の3つの権限が設定できます。また、このユーザー・アクセス権限は、論理的なグループに対しても設定することもできます。

ポリシー管理

ポリシーは、デフォルト・ポリシーおよびユーザーによるカスタマイズ・ポリシーを利用することができます。カスタマイズ・ポリシーは、作成したグループ、もしくは個別のプロテクション・エージェント毎に適用することができます。

X-Press Updateの管理

プロテクション・エージェントのX-Press Updateを自動でダウンロードし、各プロテクション・エージェントに自動的に配信、適用します。これにより各プロテクション・エージェントは常に最新のセキュリティ状態を維持することができます。自動アップデート機能はスケジューリングすることもできます。

スケジュール機能

X-Press Updateの適応、レポート作成、設定変更、ポリシー変更など日常、恒常的に発生するタスクのすべてをスケジュール化して自動実行することで作業効率をアップします。

イベント/インシデント解析

イベント・インシデント解析は、デフォルトで提供され

ている数種類の表示方法のほかに、必要に応じて柔軟にカスタマイズして表示することができます。例えばある時間までに検出されたイベント情報をベースラインとして登録し、時間が経過することにイベントがどのように変化していくかを観察することなども可能です。

グラフィカル・レポートと分析グラフの提供

レポートは、数十種類におよぶ解析情報をHTML、PDF、CSV形式で提供することができます。(別ライセンスが必要です。)

Proventia Management SiteProtector Webアクセス

Webブラウザ (Microsoft IE6以上) からセキュリティ・イベントを閲覧することが可能です。

Microsoft Active Directoryとの統合

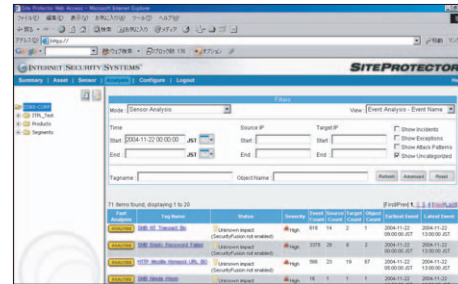
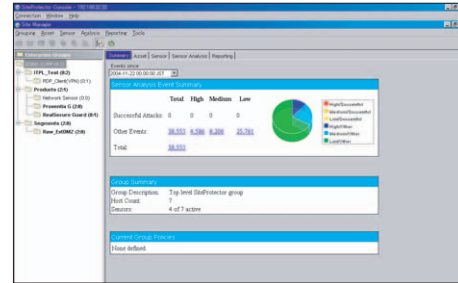
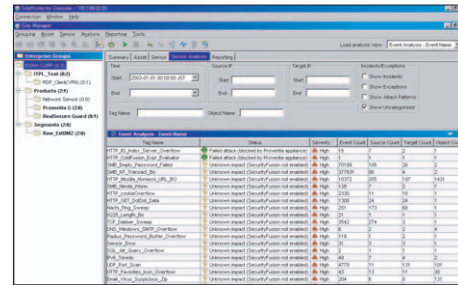
Microsoft Active Directoryのアセット情報とProventia Management SiteProtectorのアセット・グループを同期させることで、管理者はセキュリティ・イベントと組織内のユーザーを迅速に関連付けることができます。

セントラル・アラート機能

プロテクション・エージェントから直接通知レスポンスを行うのではなく、一度Proventia Management SiteProtectorに通知されたイベントに対してレスポンスを行いますので、閾値を含む様々な条件指定に合致したものだけSNMP/Emailレスポンスを送信することが可能です。例えばワームによる攻撃イベントを検知している場合、プロテクション・エージェントから1000個のemail/snmpレスポンスを送信するのではなく、Proventia Management SiteProtectorが該当イベントを1000個受信した場合に、一つのemail/snmpレスポンスを送信する等することが出来ます。

ユーザー監査機能

Proventia Management SiteProtectorのシステムにログインしたユーザーがどのような操作を行ったかを逐一トラッキングし証拠として保存しレポートする事が可能です。全てのユーザーの全てのアクションを出力することも可能ですし、特定のユーザーや特定のアクティビティのみを条件としたフィルターを実施しレポート出力することも可能です。



Webアクセスイベント/インシデント解析のカスタマイズ表示グラフィカルレポートと分析グラフの提供

セキュアシンク・フェイルオーバー機能

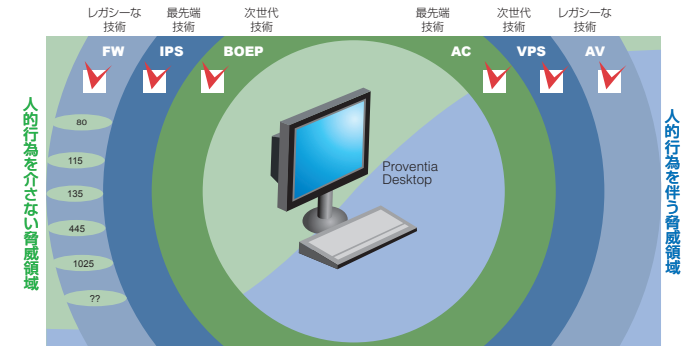
Proventia Management SiteProtectorをActive-Standby方式でクラスター化構成することが可能です。プライマリーのProventia Management SiteProtectorシステムに障害が発生した場合に、セカンダリーのProventia Management SiteProtectorシステムにプロテクション・エージェントの管理とイベント通知を切り替えることが可能な機能です。
※この機能をご利用いただく場合はご相談ください。

IBM Proventia® Desktop

Endpoint Security

Proventia Desktop Endpoint Security (略称: Proventia Desktop) は、ホスト型ファイアウォール機能 (FW)、不正侵入防御機能 (IPS)、バッファオーバーフロー・エクスプロイト・プリベンション機能 (BOEP)、アプリケーション・コントロール機能 (AC)、そして次世代型のウイルス・プリベンション機能 (VPS) を搭載しています。

望まれない通信、ウイルス・ワームの感染、不正侵入、スパイウェア、悪意のあるプログラムの実行など、様々なセキュリティ上の脅威からデスクトップPCを複数のレイヤーで保護することができます。また、管理者が設定したセキュリティ・ポリシーを、各デスクトップPCに適用することにより、ネットワーク内のセキュリティ・レベルを一定に保つこともできます。



<マルチレイヤーでのリアルタイムな防御>

Proventia Desktop Endpoint Security の特長

マルチレイヤーでのリアルタイムな防御

バッファオーバーフロー・エクスプロイト・プリベンション (BOEP)

バッファオーバーフローを試みるプログラムを自動的に判断し、その実行を遮断します。OSのみならずアプリケーションに対するバーチャルパッチ機能としても利用できます。

ホスト型ファイアウォール機能 (FW)

ホスト型ファイアウォールを搭載し、デスクトップ上で送受信されるネットワーク・トラフィックのアクセスを制御することができます。

不正侵入防御機能 (IPS)

プロトコル分析モジュール (PAM) により、160種類以上のプロトコルを解析し、脆弱性デコードなどの様々な技術を組み合わせ、未知の攻撃、ワームの伝播活動などはもちろん、誤使用や企業ポリシーに準拠しないトラフィックを検知・防御することができます。

アプリケーション・コントロール (AC)

Webブラウザやメール・クライアントでダウンロードされた悪意あるファイルの自動実行や、ウイルス・ワームの感染から防御することができます。

ウイルス・プリベンション・システム (VPS)

プログラムをOS内の安全な仮想環境内で実行し、そのプログラムの挙動に悪意がないか、ワームのような伝播活動を行わないかなど解析します。ウイルス・ワーム、悪意のあるプログラムであると判断した場合、対象のファイルを隔離、削除します。

VPSとアンチウイルスの比較

	VPS (Virus Prevention System)	アンチウイルス
防御戦略	事前防御: ウイルスのようにふるまう何かがあれば、ウイルスと判断します。	事後対応: 事前にウイルスとして識別されており、パターン・ファイルがデータベースにある場合のみウイルスと判断し防御します。
新種への対応	特定のパターンに依存しません。すなわち脅威にさらされる期間がありません。	パターン・マッチングの場合、パターン・ファイルが作成されるまでの間8~30時間のタイムラグがあり、その期間は脅威にさらされます。
亜種への対応	ワームやウイルスを含む悪意あるプログラム (マルウェア) が発生しても亜種まで防ぎます。	亜種が出るたびにパターン・ファイルを作成する必要があり、そのパターン・ファイルが作成されるまでの期間、脅威にさらされます。
実環境への影響	ウイルスを含む悪意あるプログラム (マルウェア) は実環境で動き出す前に仮想環境でとめることができます。	ウイルスを含む悪意あるプログラム (マルウェア) を実環境で実行されてしまうためパターン・ファイルができるまでの間にダメージを受ける可能性があります。

VPNインテグレーション

VPNを利用して社外のアクセスポイントから社内ネットワークにアクセスする際に、社外のクライアントホスト (PC) 上でProventia Desktopが稼動していない場合に、接続を拒否することができます。

アンチウイルス・コンプライアンス

Proventia Desktopと他社製のアンチウイルス・ソフトが同一のクライアントホスト (PC) にインストールされている場合、アンチウイルス・プログラム (Norton/ McAfee) のパターン・ファイルが最新かどうかを判断し、最新でない場合は、企業ネットワークへのアクセスを認めません。

アダプティブ・セキュリティ・ポリシー

外部ネットワーク、VPNネットワーク、企業内ネットワークのいずれのネットワークにPCが接続されているかを判断し、それぞれのネットワーク用に事前に定義されているセキュリティ・ポリシーに自動的に切り換えることが可能です。

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。

Proventia Management SiteProtector™による大規模実装

数十台規模から数十万台の規模までの Proventia Desktop に対し、セキュリティ・アップデートの一齐配信や、検出・遮断されたイベント情報の分析を行う事が可能です。さらにグループごとに設けられたセキュリティ・ポリシーを適用することでセキュリティ・レベルを一定に保つことが可能です。