

マカフィー ポータルシールド

# McAfee PortalShield

For Microsoft SharePoint Server

ポータルは、社員、顧客、パートナーをつなぎ、データを共有する手段を組織に提供します。ポータルを利用する際は、コンテンツの安全性を確保しながら、連続的な情報アクセスを維持することが不可欠です。残念ながら、ポータルを使ってドキュメントを共有するユーザは有害なウイルス、ワーム、悪性コードや不適切なコンテンツを共有できるようになるため、企業サーバに甚大な被害を与え、企業システムとネットワークの障害を引き起こす可能性もあります。不十分なビジネス認証と組織内の混乱(役割や所有権、保証の不明確さ)が、ポータルの安全確保の問題をさらに深刻化させており、ポータルの利用によるビジネスの生産性向上とアクティビティの増加に伴い、ポータルのセキュリティと管理に関連した攻撃の可能性が高まります。

McAfee® PortalShield™ for Microsoft® SharePoint Server は、あらゆるドキュメント、ファイル、ウェブコンテンツ、ドキュメントストアのコンテンツセキュリティを提供し、以下の機能を備えています。

- ・包括的なウイルスプロテクション
- ・企業ポリシー管理とグラフィカルレポートの作成
- ・安全なコンテンツ管理
- ・TOC(総所有コスト)の削減

Microsoft SharePoint ユーザは、PortalShield を利用して、ポータル上の情報の物理的な位置に関係なく、ビジネスの生産性向上に必要な情報へのアクセス、検索、共有が安全に実行できるようになります。伝統的なウイルス対策およびコンテンツセキュリティソリューションを超越した PortalShield の機能が、ウイルスの検出、駆除と削除によって Microsoft SharePoint Server を保護します。さらに PortalShield は、SharePoint ワークスペースに保存されたドキュメントに含まれる、禁止されたコンテンツを検索する機能を備えています。これは、従来のウイルス対策やコンテンツ管理ソリューションにはない新機能です。

PortalShield は、SharePoint Portal Server が動作するサーバ上の全てのドキュメント、ファイル、ウェブコンテンツ、ドキュメントストアのための包括的なウイルススキャン機能を備えた単一のソフトウェアパッケージにより、柔軟で管理しやすい包括的なウイルス対策テクノロジーの配備に対する企業組織と中小規模ビジネスのニーズに対応します。その結果、企業は、コンテンツと機密データを狙う悪質な攻撃に対する脆弱性を低減させることができます。

McAfee ePolicy Orchestrator™ (ePO™) と統合された、Microsoft SharePoint 2003 を保護する最初のソリューションである Portal Shield は、包括的なポリシー管理・施行機能、企業全体の可視性の提供、ソフトウェアの高速配備と最新のウイルス定義アップデートの配布により、コラボレーティブコンピューティング環境を保護します。

## プロアクティブなウイルスプロテクション

McAfee は、現在の脅威に対応する包括的な「問題検出・解決」ソリューションを提供し、最先端のヒューリスティック技術と遺伝的アルゴリズム技術の活用によって新たな脅威による影響を未然に防ぎます。PortalShield は、定評あるウイルススキャンおよび駆除エンジンを利用して、Microsoft SharePoint のドキュメントライブラリとウェブパーツをウイルス感染、ワーム、トロイの木馬などの悪質な攻撃から保護します。

## グラフィカルレポートの作成と集中型ポリシー管理

PortalShield は、McAfee ePolicy Orchestrator との統合により、組織のセキュリティ管理投資の最大活用を可能にします。ePO は、プロテクション実行のための集中型の権限と、重要なプロテクションカバレッジの詳細情報を含む包括的なグラフィカルレポートを提供します。このレポートを利用して、全ての PortalShield サーバが最新のエンジンと DAT で保護されているかどうかを確認できます。さらに、ePolicy Orchestrator のリモート配備機能を使って、企業の大規模なソリューション配備を中央ロケーションで簡単に管理できます。

## 高度なコンテンツ管理機能

e-ビジネスの世界に現れた新たな脅威が、多くの組織のイメージを低下させ、不正な情報漏洩や社員の違法行為による法的責任を発生させています。その結果、組織の生産性も低下します。PortalShield は、語彙スキャン機能とコンテンツ管理機能を利用して、Adobe® Acrobat と Microsoft Office を含む 280 種以上のドキュメントにルールを適用します。PortalShield のコンテンツ管理ルールを使って、Microsoft SharePoint 2003 によるドキュメントのダウンロードとアップロードの実行を防止できます。ドキュメントに機密情報や攻撃的な情報が含まれる場合は、PortalShield が管理者にアラートを送信します。さらに管理者は、ビジネスに無関係なファイル(MP3 ファイルや AVI ファイルなど)の SharePoint Server へのアップロードを禁止し、帯域幅の減少を防ぐこともできます。

## 事前設定されたコンテンツルール

効果的なルールの条件が明確でなく、ルールセットを設定する時間がないことが原因で、侮辱的な言葉や人種差別的な内容などの不適切なコンテンツの禁止が難しくなります。事前設定された PortalShield のルールが、コンテンツ管理の成功を保証し、使いやすさを実現します。さらに管理者は、高度なカスタム ルールセットを利用して、ルールを微調整することもできます。

## ウェブ管理機能

PortalShield は管理者にとって、安全で使いやすいウェブベースの管理コンソールです。このコンソールを利用して、PortalShield のローカルおよびリモート管理と設定を実行できます。

## ウェブパーツのスキャン

PortalShield は、SharePoint 製品およびテクノロジーを利用するサーバのドキュメントストアに加えて、ウェブパーツをスキャンする機能を備えています。そのため、ドキュメントストアはもちろん、ポータルのデジタルダッシュボードも保護できます。

## Microsoft VSAPI

PortalShield は、SharePoint Portal Server 2001 用の Microsoft VSAPI 2.0 テクノロジーを使って、プロアクティブスキャンとバックグラウンドスキャンを実行します。また、Windows SharePoint Services v2.0 と併用する場合は、Microsoft WSS VSAPI 1.0 を使ってウイルス対策スキャンとコンテンツスキャンを実行します。

## 企業全体での配備が可能

PortalShield は、McAfee ePolicy Orchestrator を使ったりリモートインストールが可能です。そのため、複数ロケーションでのインストールを管理者がすばやく簡単に実行できます。さらに、ePolicy Orchestrator は、PortalShield アクティビティの集中的なレポート作成を可能にします。組織全体の PortalShield ソフトウェア配備を集中管理する機能が、システムの管理とアップデートの所要時間を短縮します。

## 自動アップデート

全ての McAfee ソリューションと同様に、PortalShield はウイルス定義とエンジンを自動的にアップデートし、Microsoft SharePoint を最新のウイルスプロテクションで確実に保護します。

PortalShield ソフトウェアは、Microsoft SharePoint との統合によってドキュメントとウェブパーツをスキャンし、ウイルスと禁止されたコンテンツを検出します。ドキュメントの読み取り・書き込みと、ウェブストアのウェブパーツの読み取り・書き込みを実行するたびに、PortalShield がコンテンツをスキャンし、既知のウイルスおよびウイルスに似た不審な動作のリストと照合します。さらに PortalShield は、PortalShield コンテンツ管理エンジン内部で定義したルールとポリシーを使って、ドキュメント内のコンテンツとウェブパーツをスキャンします。

PortalShield は、SharePoint に内蔵されたウイルス スキャン インターフェースを使って、SharePoint がウェブストアに書き込む、またはウェブストアから読み取る全てのドキュメントとディスカッションへのフルアクセスを取得します。この方法により、SharePoint ユーザがファイルシステムのファイル書き込みと読み取りを実行する前に、PortalShield に全てのファイルが引き渡され、ウイルススキャンおよびコンテンツ管理エンジンによるスキャンが実行されます。

PortalShield にドキュメントが提示されると、ウイルススキャンエンジンは、現行およびインストール済みウイルス定義 (DAT) ファイル内の全ての既知ウイルスシグネチャとドキュメントを照合し、指定されたヒューリスティック検出方法を使ってドキュメントを検査します。コンテンツ管理エンジンが、ドキュメントに含まれる禁止されたコンテンツ (コンテンツ管理ポリシーで指定されたもの) をリアル

タイムまたはオンデマンドスキャン実行時に検出します。この検査によってドキュメント内のウイルスまたは禁止コンテンツが検出されない場合は、PortalShield がウイルススキャン API に情報を引き渡し、SharePoint 内部で本来のドキュメント要求を完了します。

ドキュメント内のウイルスが検出された場合や、コンテンツ管理エンジンがコンテンツルール違反を検出した場合は、PortalShield が構成設定で定義された適切なアクションを実行します。一般的に、禁止コンテンツが検出された場合には、ドキュメントのウイルスを駆除および削除するかドキュメントをブロックするアクションを設定します。

### システム要件

以下は一般的なシステム要件です。実際のシステム要件は、お客様の環境によって異なる場合があります。

Intel 300 MHzプロセッサ以上  
256MB以上のRAM  
500MB以上のハードディスク空き容量 (Microsoft SharePoint がインストールされているドライブ上)  
200MB以上のハードディスク空き容量 (システムドライブ上)  
以下のオペレーションシステムのいずれか  
Microsoft Windows 2000 Server SP3以上  
Microsoft Windows Server 2003.

### その他ソフトウェア

- Microsoft Internet Information Server (IIS) v5以上
- 下記のいずれかをインストールしていること
  - ・ Microsoft SharePoint Portal Server 2001 SP1および Microsoft fix Q318627
  - ・ Microsoft SharePoint Portal Server 2001 SP2a以上
  - ・ Microsoft SharePoint Portal server v2.0
  - ・ Microsoft Windows SharePoint Services v2.0
- Microsoft Internet Explorer version 5.5 SP1以上
- Java™ 2 Standard Edition Runtime Environment



日本ネットワークアソシエイツ株式会社 [www.nai.com/japan/](http://www.nai.com/japan/)

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F  
TEL: 03-5428-1100(代) FAX: 03-5428-1480

名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内 2-20-25 丸の内 ST ビル 8F  
TEL: 052-203-8421(代) FAX: 052-203-8422

西日本営業所 〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F  
TEL: 06-6344-1511(代) FAX: 06-6344-1517

福岡営業所 〒812-0013 福岡県福岡市博多区博多駅東 1-10-27 アステシア博多ビル 8F  
TEL: 092-452-3511(代) FAX: 092-452-3515

製品、サービスに関するお問い合わせは下記へ