

Symantec Brightmail™ Gateway ファミリー

Symantec Brightmail™ 8300 Series (旧製品名: Symantec Mail Security 8300 Series) Symantec Brightmail™ Gateway Virtual Edition

アンチウイルス、アンチスパムなど、数々のセキュリティ機能を統合し、メッセージング環境の課題を解決

製品の概要

Symantec Brightmail 8300 SeriesとSymantec Brightmail Gateway Virtual Editionは同一の機能を有しており、信頼と実績のあるシマンテックのアンチウイルスと業界をリードするBrightmailのアンチスパムをはじめ、数々のセキュリティ機能を実装した統合型のメッセージングセキュリティソリューションです。メールファイアウォール、アンチスパム、インスタントメッセージングセキュリティ、アンチウイルス、コンテンツコンプライアンスなどのセキュリティ機能を多層的に配置し、メールおよびインスタントメッセージを媒介としたさまざまな攻撃からネットワークを保護するとともに、重要な情報の漏えい防止、ネットワークインフラに対する負担の低減を実現します。

Symantec Brightmail 8300 SeriesはOSとMTA、セキュリティソフトウェアの実装とセキュリティ強化が出荷時に行われているアプライアンス製品のため、容易に導入することができます。また、Symantec Brightmail Gateway Virtual EditionはVMware仮想化環境上においてSymantec Brightmail 8300 Seriesと同等のセキュリティ機能を提供します。両製品共にウイルス定義ファイルとスキャンエンジン、スパムフィルタなどの自動化されたアップデート、個々の受信者自身による操作も可能なスパム検疫機能により、少ない管理負担でセキュリティを確保することができます。

〈キーポイント〉

- メッセージングセキュリティの包括的な確保を可能にする、セキュリティ機能の統合
 - メールファイアウォール
 - アンチスパム
 - インスタントメッセージング (IM) セキュリティ
 - アンチウイルス
 - コンテンツコンプライアンス
- グローバル規模の情報収集にもとづく、信頼のコンテンツアップデート
- 常に最新の脅威やスパムに備え、管理者の負担を大きく軽減する、アップデートの自動化
- ウイルス感染が疑わしいメールを事前に検出し、一時的に隔離 (サスペクトウイルスシグネチャを使用)
- オプションのPCC (Premium Content Control) モジュールによるポリシー (HIPPA、GLBA等) テンプレートセットの提供
- 設定、インシデント情報ごとの柔軟なバックアップ機能を提供
- 分かりやすく一貫性のあるレポートを自動生成



製品の特長

複数のセキュリティ機能を統合

Symantec Brightmail 8300 Series / Symantec Brightmail Gateway Virtual Editionは、複数のセキュリティ機能を多層的に配置することにより、メッセージング環境に対するさまざまな脅威や課題に対し、高度なセキュリティを確保することができます。

メールファイアウォール

SMTP接続の解析やリストをもとに、内蔵されたMTAと連携して通信を制御。メールを媒介とした攻撃をフィルタリングプロセスの前段階でブロックするとともに、真に必要なメールトラフィックのスループットを向上することができます。

[メールファイアウォール機能の例]

- インバウンドのSMTP接続を分析し、悪意があると識別されたメールホストとの接続レートを制御。また、スパムメールやウイルスによる攻撃の可能性を検知
- オープンプロキシを使用した送信者、スパムメールの送信元と疑わしき送信者、安全な送信者に関するリストをもとに、SMTP接続の可否を制御
- SPF (Sender Policy Framework) レコードを使用してメールを認証
- DHA (Directory Harvest Attack) 攻撃をブロックしてメールサーバーを保護

アンチスパム

業界をリードするBrightmailを中心に20種類以上の技術を駆使し、マルチレイヤのフィルタリングによってスパムメールの評価と識別を高い精度で行います。グローバルに展開するオペレーションセンターが、3億以上のメールボックスからのスパム報告を含む200万以上のメールアドレスとドメインで構成されたハニーポットネットワークを使用してスパム情報を収集し、24時間体制で解析。それにもとづき、Symantec Brightmail 8300 Series / Symantec Brightmail Gateway Virtual Editionのスパムフィルタは約10分毎に更新されます。管理者は、最新情報にもとづいたスパムフィルタリングを、高精度/低負荷で行うことができます。

[アンチスパム機能の例]

- レピュテーションサービスが提供するデータにもとづき、SMTP接続の可否を制御
- ローカルでのレピュテーション学習によりSMTP接続制御の精度を向上
- 管理者によって指定されたIPアドレスベース (DNS、ローカルレベルで識別可) で受信を拒否
- 各種のシグネチャを使用して効率良く、確実にスパムメールを検出
 - スパム送信者が誘導を意図するWebサイトのURL
 - BrightSig2™シグネチャ (ランダム化やHTMLの使用によりフィルタリングの回避を意図するスパムを検出)
 - メール本文やメールヘッダのハッシュ値をベースにしたシグネチャ
 - 画像ファイルなどのMIME添付ファイルをベースとしたシグネチャ
- スパムメールのコンテンツやヘッダーに見られる傾向や共通性などの特徴にもとづき、ヒューリスティックに検出
- イメージスパムのコンテンツに対するルール設定、および、イメージスパムの検出
- スパムメールの言語を識別。結果にもとづき、言語に即したヒューリスティックな評価やフィルタリング処理の効率化を実行、または、言語別に受信を拒否
 - (対応言語)
 - 英語、日本語、イタリア語、オランダ語、韓国語、スペイン語、中国語、ドイツ語、フランス語、ポルトガル語、ロシア語
- スパムの疑いがあるメールに対して独自の定義を設定し、スパム検出のしきい値を調整

インスタントメッセージングセキュリティ

企業において電子メールと並び重要なメッセージングツールに位置付けられるIM環境におけるセキュリティを確保します。管理者はIM環境のセキュリティに関する設定を同一のインターフェースから行うことができます。

[インスタントメッセージングセキュリティ機能の例]

- IMによるファイル転送時のウイルス、スパイウェア、アドウェアスキャンを実行

- IM上のスパムメッセージ (SPIM) を遮断
- ウィルス、スパイウェアなどへのリンクを遮断
- グループ単位での以下のIMポリシーを設定
 - ネットワークアクセス
 - ファイル転送
 - SPIM

アンチウイルス

グローバル規模で多数のユーザーに使用されている信頼と実績のあるエンジンが、メールに潜むウイルスやワームなどの悪意のあるコードを検出し、除去します。

[アンチウイルス機能の特長]

- メール本文、メール添付ファイル (圧縮ファイル含む) 内部、IM環境で転送されるファイルをスキャンし、ウイルスを的確に検出してファイルを修復
- ヒューリスティックなスキャンにより、新種・亜種などの未知のウイルスも検出。ヒューリスティックのレベルは調整可能
- メールを大量に送信するタイプのワームと、それにより生成されたメールも検出して削除
- 添付ファイル、多重圧縮されたファイルのスキャンについては、ファイルサイズや解凍レベルの上限を設定。過大な負荷を利用した攻撃からプロセスを保護
- サスペクトウイルスシグネチャを用いたスキャンにより、ウイルス感染が疑わしいメールを事前に検出し、一時的に隔離

コンテンツコンプライアンス

コンテンツフィルタを使用し、取り扱いに注意を要するコンテンツを含むメールの送受信をコントロール。財務や人事に関する情報はじめとするさまざまな情報の発信を、メールのコンテンツポリシーの視点で保護します。情報漏えいの防止、メール利用上のポリシー遵守の徹底、法的なリスクの発生を抑止に役立てることができます。

[コンテンツフィルタリング機能の例]

- フィルタリングで利用可能な項目の例
 - FROM/TO/CC/BCC、ヘッダー、件名、本文中の言葉/フレーズ、添付ファイル (ファイル名、拡張子、サイズ、MIMEタイプなど)、サイズ
- 偽装された添付ファイルの検知
- フィルタリングで使用する言葉を辞書に登録、または外部からインポート
- メールを受信を許可/禁止するための送信者リストを、テキストファイルからインポート
- グラフィカルなユーザーインターフェースを使用して、フィルタを容易に作成

- オプションのPCCモジュールによるコンテンツ制御
 - HIPPA、GLBA、SOXなどの法令*に則したテンプレート以外にも数十種類の予め設定されたポリシーテンプレートによる高度なフィルタリングが可能
 - 特定のデータベースのフィンガープリントを生成し、データが外部へ送信されることを防止

* 北米および欧州の法令等に準拠しています(2007年12月現在)。

フィルタリングの結果に応じて多様なレスポンスを実行

Symantec Brightmail 8300 Series/Symantec Brightmail Gateway Virtual Editionは、ウイルススキャン、スパムとコンテンツのフィルタリングの結果に応じて、さまざまなレスポンスを自動的に実行します。

[レスポンスの例]

- ウイルスに感染したファイルの修復、または削除
- メールの配信と削除
 - コピーを指定したアドレスに送信
 - 指定したアドレスに転送、またはBCCで送信
 - 削除
 - 隔離して検疫
- 件名にタグを追加
- X-headerを追加
- 添付ファイルを削除
- 免責事項を本文に挿入

運用を容易にする管理機能を搭載

Symantec Brightmail 8300 Series/Symantec Brightmail Gateway Virtual Editionには、運用とセキュリティ管理を容易に行うための次のような機能が搭載されています。

- Webブラウザを使用して、各機能の集中管理、フィルタリングパフォーマンスのリアルタイム監視などが行えます。
- 検疫機能により、管理者はゲートウェイレベルでスパムメールを隔離し、集中管理することができます。検疫のために隔離されたメールについては、各受信者にダイジェストのリストを送って通知を行い、受信者自身にWebベースによるチェックを委ねることができます。
- ウイルス定義ファイルとスキャンエンジンの更新、スパムフィルタの更新は、自動化されています。
- 管理者のアカウントは複数の種類を設定することができ、異なるレベルの権限の設定やタスクの割り当てを行うことができます。

- メールアドレスやドメイン名、LDAPディレクトリ情報などによりユーザーグループを定義し、グループポリシーにもとづいた柔軟な管理を行うことができます。
- ウイルススキャン、スパムとコンテンツのフィルタリングの統計などに基づいた要約/詳細レポートを生成させることができます。



受信メールのステータスレポート表示例

Symantec Security Responseによる信頼のバックアップ

Symantec Security Responseは、グローバル規模で、ウイルスやワームをはじめ、悪意のあるプログラム、不正侵入の手法、OSやアプリケーションの脆弱性とそれを利用した攻撃方法、スパムメールなどに関する情報収集と解析、また、それにもとづくシマンテック製品のバックアップを行っています。そして、インターネット上における脅威の動向を365日24時間体制で監視し、情報発信、ソリューションとサポートを世界中のユーザーに提供しています。

Symantec Brightmail 8300 Series アプライアンス製品仕様

モデル	8340	8360	8380
プロセッサ	Intel® Core™2 Duo E4500 × 1	Intel® Xeon® E5405 × 2	Intel® Xeon® E5420 × 2
メモリ	4 GB	4 GB	8 GB
ハードディスク	160 GB × 2	146 GB × 2	300 GB × 6
ネットワーク I/F	10/100/1000 × 2	10/100/1000 × 2	10/100/1000 × 2
冗長構成	ハードディスク (RAID 1)	ハードディスク (RAID 1) 電源 / 電源ファン	ハードディスク (RAID 1+0) 電源 / 電源ファン
シャーシサイズ	1U (19インチラック)	1U (19インチラック)	2U (19インチラック)
外形寸法	44.7 W × 4.3 H × 54.6 D (cm)	48.3 W × 4.3 H × 78.6 D (cm)	48.3 W × 8.6 H × 74.4 D (cm)
電源定格出力	345 W	670 W	750 W
エネルギー消費効率	0.0032 f 区分	0.0053 d 区分	0.0042 d 区分
VCCI	Class A	Class A	Class A

システム要件

Symantec Brightmail Gateway Virtual Editionでサポートされる
仮想化環境

- VMware ESX Server 3.x
- VMware Server 1.x *

* 正式サポート対象外ですが、テストおよびデモ環境にて使用することが可能です

管理コンソールでサポートされるブラウザ

- Microsoft Internet Explorer 6.0 / 7.0
- Firefox 2.0 / 3.0

製品に関する最新の情報

シマンテックのWebサイトをご覧ください。

<http://www.symantec.com/jp/enterprise>