

# Symantec™ Mail Security 8.0.5 for Domino® はじめま しょう



# Symantec™ Mail Security 8.0.5 for Domino® はじめましょう

本書で説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

Documentation version 8.0.5

## 法的通知と登録商標

Copyright © 2010 Symantec Corporation.

All rights reserved.

Symantec、Symantec ロゴは Symantec Corporation またはその関連会社の、その他の会社名、製品名は各社の登録商標または商標です。

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されています。本書のいかなる部分も、**Symantec Corporation** およびそのライセンサーからの事前に文書による許諾を得ることなく、いかなる方法によっても無断で複写、複製してはならないものとします。

本書は、現状有姿のまま提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。**SYMANTEC CORPORATION** およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書の内容は、事前の通知なく、変更される可能性があります。

ライセンス対象ソフトウェアおよび資料は、**FAR 12.212**の規定によって商用コンピュータソフトウェアとみなされ、場合に応じて、**FAR 52.227-19**「**Commercial Computer Licensed Software - Restricted Rights**」、**DFARS 227.7202**「**Rights in Commercial Computer Licensed Software or Commercial Computer Licensed Software Documentation**」、その後継規制の規定により制限された権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

弊社製品に関して、当資料で明示的に禁止、あるいは否定されていない利用形態およびシステム構成などについて、これを包括的かつ暗黙的に保証するものではありません。また、弊社製品が稼動するシステムの整合性や処理性能に関しても、これを暗黙的に保証するものではありません。

これらの保証がない状況で、弊社製品の導入、稼動、展開した結果として直接的、あるいは間接的に発生した損害等についてこれが補償されることはありません。製品の導入、稼動、展開にあたっては、お客様の利用目的に合致することを事前に十分に検証および確認いただく前提で、計画および準備をお願いします。

# Symantec™ Mail Security 8.0.5 for Domino® の紹介

この文書では以下の項目について説明しています。

- [Symantec Mail Security for Domino](#) について
- Mail Security の新機能
- Mail Security のコンポーネント
- Mail Security でできること
- Mail Security 8.0.5 for Domino をインストールする前に
- システムの必要条件
- Mail Security のインストール後のタスク
- 詳細情報の入手先

## Symantec Mail Security for Domino について

Symantec Information Foundation™ 製品ファミリーのメンバーである Symantec™ Mail Security for Domino® (Mail Security) は、Lotus Notes® データベース文書の書き込みと Lotus Domino® サーバーを通過する電子メールメッセージをスキャンする、カスタマイズと拡張が可能な総合的ソリューションです。IBM® Lotus Sametime® 7.x と QuickPlace® 6.5 と 7 にも対応しています。

Mail Security は次のものから Lotus Domino サーバーを保護します。

- 脅威 (ウイルス、ワームなど)
- セキュリティリスク (アドウェア、スパイウェアなど)
- 不要なコンテンツ

■ 迷惑な電子メールメッセージ

Mail Security では複数の Domino サーバーを管理することもできます。

Lotus Domino 環境は脅威がサイト内に侵入する通りの道の 1 つにすぎません。サイトを十分に保護するにはすべてのコンピュータとワークステーションをデスクトップ版ウイルス対策ソリューションで確実に保護してください。

p.9 の「[Mail Security でできること](#)」を参照してください。

## Mail Security の新機能

Windows プラットフォームにおける Mail Security for Domino の新しい製品機能を表 1-1 に示します。

表 1-1 Windows プラットフォームでの新機能

機能	説明
64 ビット Domino のサポート	Windows プラットフォーム上で 64 ビット Domino をサポートします。
プラットフォーム間での複製	SMSDOM の 32 ビットバージョンと 64 ビットバージョン間での SMSDOM データベースの複製がサポートされ、一元的な管理を実現します。  すべての SMSDOM データベースをプラットフォーム間で複製して、一元的な管理を強化することができます。同じサーバーグループで Windows と非 Windows のサーバーを使用することができます。
複数のプラットフォームでの定義の管理	定義データベースが拡張され、32 ビットの定義ファイルに加えて 64 ビットのウイルス定義ファイルも含まれるようになりました。  この強化された機能により、サーバーグループの任意のサーバーから、Windows と非 Windows のプラットフォームの定義ファイルを効果的で簡単に管理することができます。
コンテナファイルのコンテンツスキャン	添付コンテナファイル内のコンテンツファイルをスキャンの対象に含めるように、コンテンツフィルタールールを設定できます。添付ファイルの名前、拡張子、コンテンツについて、ファイルをスキャンできます。違反が検出されると、指定された設定に基づいてファイルが処理されます。  以前のバージョンの Mail Security から移行する場合は、添付コンテナファイルのコンテンツをスキャンの対象に含めるように既存のルールを修正できます。
ログ記録とエラー処理のサポートの強化	製品アーキテクチャの強化により、スキャントランザクションの追跡が向上しました。トランザクションエラーやスキャンの例外などの新しい適切なエラーコードが、さまざまなスキャンエラーを処理するために追加されました。また、エラーは効果的に処理され、修正処理のためにログ記録データベースに明確に記録されます。

機能	説明
処理効率の強化	製品アーキテクチャの強化により、スキャンの処理効率が向上しました。また、ファイルの入出力操作が大幅に減少し、妥当性検査が効率化されました。

**メモ:** Premium AntiSpam は、Windows プラットフォーム上の Symantec Mail Security for Domino (32 ビット) でのみサポートされます。

コンテンツフィルタールの Dynamic Document Review (DDR) 属性は、Symantec Mail Security for Domino (32 ビット) でのみサポートされます。

非 Windows のプラットフォームにおける Mail Security for Domino の新しい製品機能を表 1-2 に示します。

**表 1-2 非 Windows のプラットフォームでの新機能**

機能	説明
64 ビット Domino のサポート	非 Windows プラットフォーム上で 64 ビット Domino をサポートします。
コンテナファイルのコンテンツスキャン	添付コンテナファイル内のコンテンツファイルのスキャンの対象に含めるように、コンテンツフィルタールを設定できます。添付ファイルの名前、拡張子、コンテンツについて、ファイルのスキャンできます。違反が検出されると、指定された設定に基づいてファイルが処理されます。  以前のバージョンの Mail Security から移行する場合は、添付コンテナファイルのコンテンツをスキャンの対象に含めるように既存のルールを修正できます。
標準スパム対策	標準スパム対策機能は、スパム電子メールからの保護を提供します。この機能はヒューリスティック技術を使用してスパムを検出します。Mail Security は最初に脅威とセキュリティリスクをスキャンし、次にスパムをスキャンし、最後にコンテンツフィルタールをスキャンします。
手動スキャンと定時スキャンに対するコンテンツフィルタ違反のスキャンオプション	Mail Security では、手動スキャンと定時スキャンに対してコンテンツフィルタを独立して有効にできます。この機能により、マルチメディアファイルや実行可能ファイルを無視するように設定することもできます。
独立した処置オプション	Mail Security は、手動スキャン、定時スキャン、リアルタイムスキャンの間に検出されるセキュリティリスクを検出します。これらのスキャンのそれぞれに対して、セキュリティ上の脅威が検出されたときの処理を独立して設定できます。添付ファイルを監査または削除するように処理を設定できます。

機能	説明
複数のプラットフォームでの定義の管理	<p>定義データベースが拡張され、32ビットの定義ファイルに加えて64ビットのウイルス定義ファイルも含まれるようになりました。</p> <p>この強化された機能により、サーバーグループの任意のサーバーから、<b>Windows</b> と非 <b>Windows</b> のプラットフォームの定義ファイルを効果的で簡単に管理することができます。</p>
<b>Rapid Release</b> 定義の更新	<p><b>Rapid Release</b> を利用すると、シマンテックから 1 時間おきに最新のウイルス定義を入手できるので、新しい脅威やセキュリティリスクにすばやく対処できます。</p>
添付ファイルのコンテンツフィルタと関連するコンテンツフィルタルール	<p>添付ファイル内のコンテンツをスキャンの対象に含めるようにコンテンツフィルタルールを設定できます。違反が検出されると、指定された設定に基づいてファイルが処理されます。</p> <p>以前のバージョンの <b>Mail Security</b> から移行する場合は、添付ファイルのコンテンツをスキャンの対象に含めるように既存のルールを修正できます。</p> <p>添付コンテンツファイル内のコンテンツファイルをスキャンの対象に含めるように、コンテンツフィルタルールを設定できます。添付ファイルの名前、拡張子、コンテンツについて、ファイルをスキャンできます。</p>
一致リスト、コンテンツフィルタの語句カテゴリ (DDR)	<p>一致リストを作成して、会社または業界に独特または標準の語句や、コンテンツフィルタにしたい語句のカスタムリストを作成できます。一致リストを作成した後で一致リストの語句を使うコンテンツフィルタルールを作成できます。</p> <p><b>Symantec Mail Security</b> にはカテゴリと語句が用意されていますが、独自に作成することもできます。辞書ベースのコンテンツフィルタはメッセージの件名と本文のコンテンツを辞書カテゴリの語句と比較してフィルタ処理できます。</p> <p>コンテンツフィルタルールの <b>Dynamic Document Review (DDR)</b> 属性は、<b>Symantec Mail Security for Domino (32 ビット)</b> でのみサポートされます。</p>
マルチメディアと実行可能ファイルの分析 (実際のファイルタイプの判別)	<p>添付ファイルの実際のファイルタイプを検出するように <b>Mail Security</b> を設定できます。実際のファイルタイプと拡張子が一致しない場合でも、指定された処理が <b>Mail Security</b> によって実行されます。 <b>Mail Security</b> は、オーディオファイル、ビデオファイル、実行可能ファイルの実際のファイルタイプを検出できます。</p>
グラフ表示レポート	<p>特定の期間に起きた違反を視覚的に示すグラフ表示レポートを作成できます。グラフ表示レポートの形式、レポートに含める違反の種類、レポート期間は、自由にカスタマイズできます。</p>

機能	説明
サーバーグループに基づいた設定	サーバーグループごとに設定を行ったり、グループ内のすべてのサーバーに適用可能な設定を行うことができます。サーバーを別のサーバーグループに移動した場合、サーバーには移動先のサーバーグループの設定が適用されます。
<b>Windows と非 Windows</b> のプラットフォームでの UI の統一	ユーザーインターフェースは、 <b>Windows</b> と非 <b>Windows</b> のプラットフォームで統一されています。本書では日本語化された <b>Windows</b> 版を前提に説明されていますが、非 <b>Windows</b> 版は日本語化されていません。
ログ記録とエラー処理のサポートの強化	製品アーキテクチャの強化により、スキャントランザクションの追跡が向上しました。トランザクションエラーやスキャンの例外などの新しい適切なエラーコードが、さまざまなスキャンエラーを処理するために追加されました。エラーは効果的に処理され、修正処理のためにログ記録データベースに明確に記録されます。
免責	<p>部署によっては電子メールメッセージをスキャン済みであることを示す免責メッセージを付加する必要があります。免責として指定したテキストは電子メールメッセージのヘッダーまたはフッターに表示されます。このオプションが有効な場合、<b>Symantec Mail Security</b> は送信先に渡すすべての電子メールメッセージに免責メッセージを挿入します。</p> <p>部署用の免責マークを指定できます。また、スキャン後の電子メールメッセージに挿入されるヘッダーまたはフッターのテキストをカスタマイズできます。</p>
アウトブレイク検出	<p>アウトブレイク時に警告が発行されるように <b>Symantec Mail Security</b> を設定できます。アウトブレイク通知を誘発するのに必要な脅威検出の回数と感染の可能性を検出する時間間隔は変更できます。</p> <p><b>Symantec Mail Security</b> は、アウトブレイクを検出すると、検出したすべての脅威をログに記録します。したがって、アウトブレイクの気配を早急に察知することと、不要な通知を生成しないようにすることの、どちらが重要かを十分に検討する必要があります。</p>

機能	説明
Enterprise Vault のタグ	<p>Symantec Enterprise Vault は、情報のアーカイビングと検索を安全かつ一元的に行えるデータウェアハウスです。Mail Security では、次のいずれかの違反を含む電子メールメッセージに X-header を適用することができます。</p> <ul style="list-style-type: none"> <li>■ コンテンツフィルタールール</li> <li>■ リアルタイムの脅威とセキュリティリスク</li> <li>■ 実行可能ファイルまたはマルチメディアファイルのファイルタイプ検出</li> <li>■ スпам</li> </ul> <p>Enterprise Vault では、メッセージの分類、保存、検索などの目的にこれらの X-header が利用されます。</p>

メモ: これらの機能は、Linux と Solaris プラットフォームではサポートされません。

## Mail Security のコンポーネント

製品 DVD に含まれているコンポーネントを表 1-3 に示します。

表 1-3 製品コンポーネント

コンポーネント	説明
Mail Security	脅威(ウイルスなど)やセキュリティリスク(アドウェア、スパイウェアなど)から Lotus Domino サーバーを保護し、スパムメールや不要なコンテンツを検出するためにインストールするソフトウェアです。
LiveUpdate™ 管理ユーティリティ	<p>社内の LiveUpdate サーバーとして動作するように 1 つ以上のイントラネット FTP、HTTP、または LAN サーバーを設定するためのユーティリティです。LiveUpdate を使うとシマンテック製品はプログラムと定義ファイルの更新版をシマンテック社から直接または LiveUpdate サーバーからダウンロードできます。</p> <p>詳しくは製品 DVD 上にある『Symantec LiveUpdate Administrator ユーザーズガイド』を参照してください。</p>

コンポーネント	説明
Symantec Folder Agent for Domino インストーラ	フォルダエージェントをインストールするためのプログラムです。フォルダエージェントは <b>Symantec Premium AntiSpam</b> サービスと連携して働きます。フォルダエージェントを使うと各ユーザーのメールボックスのスパムフォルダにスパムとスパムの疑いがあるメッセージを自動的に配送できます。
Adobe® Reader® 8.0	PDF 形式の電子マニュアルを読むために必要なソフトウェアです。
『Symantec Mail Security 8.0.5 for Domino 実装ガイド』	PDF 版の『実装ガイド』で、この製品のインストールと設定についての情報が書かれています。

## Mail Security でできること

Mail Security を使うと、次の方法で Lotus Domino サーバーを保護できます。

- 「リスクと違反についての **Domino** サーバーのスキャン」
- 「リスクに対する保護」
- 「最新の保護状態の保持」
- 「スパムメールの識別」
- 「コンテンツフィルタールールの実施」
- 「感染文書の隔離」
- 「データの分析とレポートの生成」
- 「リスクまたは違反検出時の警告」
- 「複数の **Lotus Domino** サーバーの管理」
- 「アーカイブに保存するメッセージへの **X-header** の適用」

### リスクと違反についての Domino サーバーのスキャン

Mail Security では、Domino サーバーを定期的にスキャンしたり、手動でスキャンを開始することができます。Auto-Protect 機能は Lotus Domino サーバーを通して電子メールメッセージを配送するときまたは文書をサーバーに書き込むときに、リスク、スパム、コンテンツフィルタールール違反をリアルタイムに検出します。

Mail Security は、スキャン対象から除外されていない Lotus Domino サーバー上のデータベースに書き込まれる文書と電子メールメッセージをスキャンします。これには、

Zip などの形式で圧縮またはエンコードされたファイルも含まれます。また、添付ファイルを解析して脅威やセキュリティリスクをスキャンすることもできます。

---

**メモ:** スキャン操作を実行するには有効な製品ライセンスが必要です。

---

## リスクに対する保護

シマンテック社の技術者は新種のリスクを識別するために、リスク(ウイルス、トロイの木馬、ワーム、アドウェア、スパイウェアなど)のアウトブレイクを追跡しています。リスクが識別されると、そのリスクについての情報(シグネチャ)を含む定義ファイルが作成されます。このファイルにはリスクを検出して除去するための情報が入っています。**Mail Security** はリスクをスキャンするときに、これらのシグネチャを検索します。

**Mail Security** は既知の定義が存在しない脅威をスキャンするためにシマンテック社の **Bloodhound** ヒューリスティック技術も使います。**Bloodhound** ヒューリスティック技術は感染の可能性のある文書を対象にするために自己複製のような異常な動作をスキャンします。

大量メール送信型ワームまたはウイルスはセキュリティの脆弱性を攻略することによってコンピュータに侵入し、インターネットまたはネットワークを通して電子メールで自己の複製を送信することによって伝染できます。たとえば、単一の大量メール送信型ワームは社内での 1 台のコンピュータに感染してから電子メールを通して自己の複製を送信することでその会社のグローバルアドレス帳の全員に伝染可能です。

アウトブレイクに対してすばやく的確に対処するには、**Mail Security** でアウトブレイクルールを作成して、アウトブレイクが検出されたときに電子メールで警告を送信するように設定します。

**Domino** サーバーが大量メール送信型ワームまたは脅威から攻撃されると大量メール送信型ワームのクリーンアップ機能が大量メール送信型感染メッセージとその添付ファイルを自動的に削除します。

## 最新の保護状態の保持

**Mail Security** は最新の情報に基づいてリスクを検出して除去します。コンピュータが攻撃に対して無防備になる主な原因の 1 つは定義ファイルを更新していないことです。シマンテック社は定義ファイルを定期的に更新して提供しています。

**LiveUpdate** を使うと、**Mail Security** はシマンテック社のサーバーにインターネット経由で接続して定義ファイルを更新する必要があるかどうかを自動的に判断します。更新する必要がある場合には定義ファイルが適切な場所にダウンロードされてインストールされます。新しい脅威に対して迅速に対応する必要がある場合は、インテリジェント更新プログラムまたは **Rapid Release** を使って最新の定義ファイルを入手できます。定義ファイルを更新するには有効なコンテンツライセンスが必要です。

## スパムメールの識別

スパムは大量に送信される迷惑な電子メールメッセージの一種でそのほとんどは製品またはサービスの広告メッセージです。スパムは生産性、時間、ネットワーク帯域幅を浪費します。

**Mail Security** にはスパムメールを識別するためのヒューリスティックスパム対策検出エンジンがあります。スパム対策エンジンの感度レベルを選択し、メッセージがスパムと識別されたことをメッセージ受信者に警告するために電子メールメッセージの件名の先頭にカスタマイズしたテキストを付けたり、新しいヘッダーフィールドを追加したりできます。

**Symantec Premium AntiSpam** を利用するとスパムメッセージ検出機能がさらに強化されます。**Symantec Premium AntiSpam** は最新の技術と戦略を使ってサイトに入ってくる電子メールをフィルタ処理して分類します。

ホワイトリスト機能は標準スパム対策エンジンと **Symantec Premium AntiSpam** によって共有されます。ホワイトリストを使うとスパム対策スキャンのバイパスを許可するドメインを指定できるため、誤認のインシデントを減らし、システムリソースを節約できます。

## コンテンツフィルタルールの実施

**Mail Security** では、電子メールメッセージや文書の内容を基準としてフィルタ処理を適用することにより、セキュリティをさらに強化することができます。**Mail Security** は電子メールメッセージの件名または内容をスキャンして、不適切なコンテンツ（不快な表現、機密情報、法的な問題を含む可能性があるコンテンツなど）が含まれていないかどうかを確認します。

**Mail Security** では、送信者、受信者、グループ名、ドメインなどを基準として電子メールメッセージを遮断することもできます。また、添付ファイルのサイズ、ファイル名、拡張子を基準として電子メールメッセージを遮断することもできます。

不要なコンテンツをスキャンするためにコンテンツフィルタルールを作成します。文書の内容や添付ファイルの属性がいずれかのルールに違反している場合、**Mail Security** はそのルールで指定された設定に従って電子メールメッセージを処理します。

必要な数のコンテンツフィルタルールを設定できます。それぞれのルールはコンテンツフィルタルール違反のトリガになる条件を指定します。コンテンツフィルタルールの処理順序も指定できます。

## 感染文書の隔離

**Mail Security** の検疫には、スパムメール、リスクを含む文書、コンテンツフィルタルールに違反している文書などが格納されます。

検疫にある文書は、いくつかの方法で処理できます。たとえば、別の場所に保存したり、検疫から解放することができます。

## データの分析とレポートの生成

Mail Security は次の情報を監視します。

サーバーメッセージ	サーバーに関するイベントです。
製品情報	製品のバージョン、製品がインストールされているサーバー、定義ファイルのバージョンです。
インシデント	脅威、セキュリティリスク、スキャンエラー、スパム、コンテンツフィルタールール違反です。

統計とレポートは、Mail Security ログに記録されたインシデントから作成されます。

データの分析には次のレポートを使用できます。

統計	インシデントの事前定義済み統計レポートです。
スキャンレポート	定時スキャンと手動スキャンの概略です。
カスタムレポート	ユーザーが作成したカスタムレポートです。

## リスクまたは違反検出時の警告

Mail Security には、リスクや違反が検出されたときに、文書の作成者、文書の受信者、管理者などに警告を送信するオプションが用意されています。

警告のトリガになる条件を定義します。定義する警告条件ごとに警告メッセージのテキストをカスタマイズすることもできます。

## 複数の Lotus Domino サーバーの管理

Mail Security は、複数の Lotus Domino サーバーを保護することもできます。複数の Lotus Domino サーバー間で Domino データベースの作成と管理を単純化できます。この場合は、Mail Security を管理し、最新の定義ファイルを受信するために使うサーバー（ハブ）を 1 台選択します。ハブサーバーの Mail Security データベースを他のサーバー（スポーク）と同期するには、Lotus Domino の複製技術を使います。この複製処理を使って、すべてのサーバーのインシデントや統計に関するレポートをハブサーバーに送信することもできます。

データベースの複製について詳しくは Lotus Domino のマニュアルを参照してください。

複数の Lotus Domino サーバーの管理を単純化するためにサーバーグループを設定することもできます。サーバーグループを使うと共通の目的があつて同じ保護が必要なサーバーをグループ化できます。サーバーをグループ化すると、同じ保護設定を各サーバーに繰り返し適用する必要がなくなります。

## アーカイブに保存するメッセージへの X-header の適用

Mail Security では、違反を含む電子メールメッセージに X-header を適用できます。この X-header は、Symantec Enterprise Vault™ にアーカイブされているメッセージを検索して取得する目的に利用されます。Enterprise Vault は、情報のアーカイビングと検索を安全かつ一元的に行えるデータウェアハウスです。

---

**メモ:** SMTP で送信される電子メールメッセージに X-header を適用することはできません。

---

## Mail Security 8.0.5 for Domino をインストールする前に

Symantec Mail Security 8.0.5 for Domino をインストールする前に、サイトの環境がシステムの必要条件を満たしていることを確認してください。製品のインストールを行う管理者は、レジストリとファイルシステムに対する読み取りと書き込みが可能なフルアクセス権限を持っている必要があります。

p.18 の「[システムの必要条件](#)」を参照してください。

Mail Security インストールプログラムは Windows のレジストリを読み込んで Lotus Domino サーバーとデフォルトのデータフォルダを検索します。Mail Security のレジストリキーのほかに、Mail Security は次のディレクトリにファイルをインストールします(新規のディレクトリは必要に応じて作成されます)。

Windows および非 Windows のデータのインストールフォルダを [表 1-4](#) に示します。

表 1-4 インストールフォルダ

フォルダ	説明
[Domino バイナリフォルダ]	Mail Security のエンジン
[Domino データフォルダ]	Mail Security データベーステンプレート(sav.ntf、savlog.ntf、savquar.ntf、savdefs.ntf)

フォルダ	説明
<p>[Domino データフォルダ]¥SAV</p>	<p>Mail Security データベース(sav.nsf、savlog.nsf、savquar.nsf、savhelp.nsf)</p> <p>Mail Security が動作している他の Domino サーバーにウイルス定義を複製する場合、ここに定義データベース(savdefs.nsf)が作成されます。</p>
<p>Windows (32 ビット): ¥Program Files¥Common Files¥Symantec Shared¥VirusDefs</p> <p>Windows (64 ビット): ¥Program Files (x86)¥Common Files¥Symantec Shared¥VirusDefs</p> <p>非 Windows: /opt/Symantec/virusdefs</p>	<p>ウイルス定義ファイル(すべてのシマンテック製品で使います)</p>
<p>Windows: ¥Program Files¥Symantec¥SMSDOM または ¥Program Files (x86)¥Symantec¥SMSDOM</p> <p>非 Windows: /opt/Symantec/SMSDOM または /opt/Symantec/SMSDOM/docs</p>	<p>標準スパム対策の定義ファイル、Dynamic Document Review (DDR) フォルダ、圧縮解凍エンジンファイル、ファイルタイプ検出用のシグネチャファイル、Symantec Premium AntiSpam 関連のファイル、添付ファイルの内容をスキャンするためのファイル、Rapid Release スクリプト、README.TXT ファイル、バージョンサポート方針に関するファイル、PDF 版の『Symantec Mail Security 8.0.5 for Domino 実装ガイド』、『Symantec Mail Security 8.0.5 for Domino インストールガイド』(Windows)、『Symantec Mail Security 8.0.5 for Domino Multi-Platform Edition インストールガイド』(非 Windows)</p>

フォルダ	説明
Windows: ¥Program Files¥Common Files¥Symantec Shared¥Licenses または ¥Program Files (x86)¥Common Files¥Symantec Shared¥Licenses 非 Windows: /opt/Symantec/Licenses	Symantec ライセンスファイル  シマンテック製品のライセンスをインストールすると、この Licenses フォルダにライセンスファイルが保存されます。
Windows (32 ビット): ¥Program Files¥Common Files¥Symantec Shared¥Java LiveUpdate Windows (64 ビット): ¥Program Files (x86)¥Common Files¥Symantec Shared¥Java LiveUpdate 非 Windows: /opt/Symantec/LiveUpdate	ウイルス定義ファイルとプログラムの更新版をダウンロードする、プラットフォームに依存しない <b>LiveUpdate</b> 技術(すべてのシマンテック製品で使います)

同じサーバー上に複数の Lotus Domino パーティションがある場合、インストールプログラムは各パーティションを検出して Mail Security のインストール先パーティションを指定できるようにします。

**Windows** クラスタコンピュータ上でパーティション分割されているサーバーに **Mail Security** をインストールする場合、コンピュータに **Mail Security** をインストールしたことがなくても、インストールプログラムはどちらの **Mail Security** データベースを保持するかを尋ねるメッセージを表示します。どちらのオプションを選択しても、インストールは正常に続行します。

**Mail Security** は、同一コンピュータ上で稼働中の複数のバージョンの **Domino** サーバーを保護することはできません。最も新しくインストールされたバージョンの **Domino** のみが保護されます。

最大限の安全性を確保するには、**Mail Security** 拡張マネージャの DLL ファイル (**nnem.dll**) を他のサードパーティ **Domino** 拡張マネージャより先にロードする必要があります。 **notes.ini** ファイル内で **nnem.dll** が **EXTMGR\_ADDINS** パラメータの最初のエントリになっていることを確認してください。

一部のサードパーティソフトウェアは **Domino** アドインタスクとして提供され、**Windows** オペレーティングシステム上のサービスとして実行されます。 **Domino** サーバーが起動する前にこれらのサービスが開始されると **Mail Security** 拡張マネージャの DLL ファイルがロードされなくなる可能性があります。したがって、これらのプロセスは **Domino** サーバーが起動した後に開始するように設定してください。

## アップグレードする場合

SMSDOM 4.1、5.1、7.5、8.0 から SMSDOM 8.0.5 (32 ビット) へアップグレードできます。Mail Security の以前にインストールされたどのバージョンからも、Mail Security の 64 ビットバージョンへアップグレードすることはできません。

SMSDOM の 32 ビットバージョンから 64 ビットバージョンへの移行に関する直接サポートは提供されません。SMSDOM の 32 ビットバージョンから 64 ビットバージョンへ移行するには、次の手順を実行してください。

### SMSDOM の 32 ビットバージョンから 64 ビットバージョンへ移行するには

- 1 SMSDOM の 32 ビットバージョンをアンインストールします。ただし、この処理中 SMSDOM データベースを保持できます。
- 2 Symantec Endpoint Security (SEP) または Symantec Antivirus がコンピュータ上にインストールされていない場合、以前の SMSDOM の 32 ビットバージョンのウイルス定義が削除されたことを確認します。

これらのウイルス定義は、Symantec SharedVirusDefs フォルダにあります。

- 3 32 ビット Domino サーバーを 64 ビットにアップグレードしたことを確認します。
- 4 SMSDOM の 64 ビットバージョンを 64 ビット Domino サーバーへインストールします。

---

**メモ:** Premium AntiSpam は Windows プラットフォーム上の Symantec Mail Security for Domino (32 ビット) でのみサポートされます。Mail Security を 64 ビットにアップグレードする場合、既存の Premium AntiSpam ライセンスは無効になります。

---

Mail Security はバージョン 4.x 以降からのアップグレードのみをサポートします。バージョン 3.x 以前を実行している場合、その製品をアンインストールしてからバージョン 8.0.5 をインストールしてください。

バージョン 8.0.5 にアップグレードするための必要条件を [表 1-5](#) に示します。

表 1-5 アップグレードの必要条件

バージョン	アップグレードの必要条件
4.0	なし
4.1、5.x、7.5、または 8.0x	Symantec Premium AntiSpam が有効になっている場合は、バージョン 8.0.5 をインストールする前に無効にしてください。

バージョン 4.x 以降からのアップグレードの場合、旧来のデータベースをアップグレードできます。インストール処理中に保持するように選択したデータベースは、Lotus Domino

サーバーを次に開始したときにアップグレードされます。Domino サーバーのコンソールメッセージを表示して以前のデータベースが正しくアップグレードされたことを確認できます。新しいデータベースはテンプレートから作成されてデフォルトの Data フォルダの SAV サブフォルダに入ります。

バージョン 4.x からのアップグレード後に修正されるクエリ属性またはフィールドを [表 1-6](#) に示します。

**表 1-6**                      **バージョン 4.x のクエリアップグレード値**

属性またはフィールド	バージョン 4.x の値	バージョン 8.0.5 の値
[実行間隔]	[3 カ月単位]	値は[月単位]に設定されます。
[実行日は]	該当なし	[実行間隔]が[日単位]である場合、 [実行日は]は選択した週日に設定されます。  [実行間隔]が[週単位]であった場合、 [実行日は]はアップグレードを実行した曜日にデフォルト設定されます。
[出力の種類]	[概略の合計のみ]	値は[概略]に設定されます。
[出力の種類]	[詳細レポート]	値は[管理の概略]に設定されます。
[出力の種類]	[詳細レポートと概略の合計]	値は[詳細]に設定されます。
[出力形式]	[XML]	[出力の種類]が[概略の合計のみ]または[詳細レポート]である場合、[出力形式]は[HTML]に設定されます。
[ファイル名]	任意の値	ファイルの拡張子は削除されます。新規のレポートを生成すると、出力のファイル名が新しい形式になります。
[作成者]	任意の値	値はデフォルト値の[任意の作成者]に設定されます。
[サーバー]	任意の値	値はデフォルト値の[すべてのサーバー]に設定されます。
[適用した処理]	[無視した文書]	値は[監査/配信した文書]に設定されます。
[適用した処理]	[クリーニングした文書]	値は[修復した文書]に設定されます。
[適用した処理]	[削除した添付ファイル/文書]	値は[削除した添付ファイル/文書]に設定されます。

属性またはフィールド	バージョン 4.x の値	バージョン 8.0.5 の値
[ウイルス名選択]	任意の値	値は削除されました。バージョン 8.0.5 では、レポートクエリはすべての脅威に適用されます。

## システムの必要条件

Mail Security のインストールを行うユーザーには、Windows と Lotus Domino サーバーに対する管理者レベルの特権が必要です。Domino サーバーは IBM/Lotus が指定するガイドラインに沿って適切に調整されている必要があります。

Mail Security をインストールするには、次の最小必要条件を満たしている必要があります。

### オペレーティングシステム

SMSDOM の 32 ビットバージョン:

- Windows Server 2003 (32 ビットまたは 64 ビット)
- Windows Server 2008 (32 ビットまたは 64 ビット)

SMSDOM の 64 ビットバージョン:

- Windows Server 2003 (64 ビット)
- Windows Server 2008 (64 ビット)

### Lotus Domino

SMSDOM の 32 ビットバージョン:

- Domino 7.x または 8.x (32 ビット)

SMSDOM の 64 ビットバージョン:

- Domino 8.x (64 ビット)

### Lotus Notes

Lotus Notes Client 6.0.x、6.5.x、7.0.x、8.x

### プロセッサ

1 GHz Pentium またはそれ以上

### メモリ

512 MB

パフォーマンスはサーバーの負荷に依存します。

### インストール用のディスク容量

250 MB

処理用の空きディスク容量	最低 300 MB  インストール後に一時ファイルの場所を変更できます。 スキャン中にファイルを処理するディレクトリを指定する方法については、『Symantec Mail Security 8.0.5 for Domino 実装ガイド』を参照してください。
ハードウェア	DVD-ROM ドライブ
インターネットブラウザ	最新の Service Pack が適用された Microsoft Internet Explorer 6.0
JRE	SMSDOM の 32 ビットバージョン: <ul style="list-style-type: none"> <li>■ JRE 1.5x (32 ビット)</li> </ul> SMSDOM の 64 ビットバージョン: <ul style="list-style-type: none"> <li>■ JRE 1.5x (64 ビット)</li> </ul>

システムの必要条件に加えて、Java Runtime Environment (JRE) と JCE 無制限強度の管轄ポリシーファイルを有効にする必要があります。これらのポリシーファイルは JRE のバージョンによって異なり、Sun Microsystems 社の Web サイトからダウンロードできます。また、LiveUpdate がダウンロード時にファイルのキャッシュ機能をサポートするためには、さらに約 2 GB のハードディスク容量が必要です。

## AIX システムの必要条件

Symantec Mail Security for Domino MPE をインストールするには、AIX コンピュータと Domino サーバーに対する管理者レベルの権限が必要です。

AIX システムの最小必要条件是次のとおりです。

オペレーティングシステム	AIX バージョン 5.3 または 6.1
Lotus Domino	Domino 7.x または 8.x
Lotus Notes	7.x 以降
空きディスク容量	350 MB
JRE	SMSDOM の 32 ビットバージョン: <ul style="list-style-type: none"> <li>■ 1.5x (32 ビット)</li> </ul> SMSDOM の 64 ビットバージョン: <ul style="list-style-type: none"> <li>■ 1.5x (64 ビット)</li> </ul>
xlC ランタイムバイナリ	9.0.0.8

/tmp ディレクトリの空きディスク容量      最低 200 MB

/tmp ディレクトリのディスク容量は LiveUpdate および Rapid Release 定義をダウンロードするのに必要です。Rapid Release の定義管理を有効にする場合は、さらに 4 GB のハードディスク容量が必要です。Rapid Release の定義管理については、『Symantec Mail Security 8.0.5 for Domino 実装ガイド』の「Rapid Release 定義セットの保存」を参照してください。

## Mail Security のインストール後のタスク

Mail Security のインストールやアップグレード後に実行可能なインストール後のタスクを「[Mail Security のインストール後のタスク](#)」に示します。

表 1-7                      インストール後のタスク

タスク	説明
README.TXT ファイルを読む	このテキストファイルには Mail Security についての互換性情報と既知の問題が書かれています。README.TXT ファイルはインストール DVD にあります。Windows の場合、場所は ¥Program Files¥Symantec¥SMSDOM または ¥Program Files (x86)¥Symantec¥SMSDOM で、MPE の場合、場所は .../Symantec/SMSDOM です。
Mail Security データベースに署名する	初めてデータベースを開く前に信頼できる Notes ID ファイルで Mail Security データベースに署名してください。
無制限エージェントを実行する権利を認可する	無制限エージェントの有効化、無効化、または修正する権利をユーザーに与えることができます。
Mail Security データベースにアクセスする	Mail Security データベースを開いてからワークスペースに保存するとアクセスしやすくなります。
アクセス制御を設定する	アクセス制御設定では誰が Mail Security データベースにアクセスできるかを設定します。
ライセンスをアクティブにする	ウイルス定義ファイルの更新版を受信し、Mail Security のスキャン機能を操作するにはコンテンツライセンスと製品ライセンスを購入してアクティブにする必要があります。

インストール後のタスクについては、『Symantec Mail Security 8.0.5 for Domino 実装ガイド』を参照してください。

## 詳細情報の入手先

Mail Security には目次、トラブルシューティングのヒント、キーワードからアクセスできるヘルプトピックが用意されています。各タブで状況感知型ヘルプが利用できます。グループオプションに関する状況感知型ヘルプも各タブで利用できます。

Mail Security DVD には次のリソースが含まれています。

『Symantec LiveUpdate Administrator ユーザーズガイド』      DOCS¥LU¥LiveUpdate Administrator Users Guide.pdf

フォルダエージェントの Readme ファイル      Utilities¥Folder\_Agent¥README.txt

製品の詳しい情報についてはシマンテック社の Web サイトで次のオンラインリソースが利用可能です。

テクニカルサポートのナレッジベース、ニュース、問い合わせ先、ダウンロードなどの情報にアクセスできます。      [www.symantec.com/ja/jp/business/support](http://www.symantec.com/ja/jp/business/support)

登録、よくある質問、エラーメッセージへの応答方法、ライセンス登録の方法についての情報が  
あります。      [licensing.symantec.com/acctmgmt/index.jsp?localeStr=jp\\_JP](http://licensing.symantec.com/acctmgmt/index.jsp?localeStr=jp_JP)

製品ニュース、更新情報などにアクセスできます。      [www.symantec.com/ja/jp/business](http://www.symantec.com/ja/jp/business)

すべての既知の脅威についての情報が載っているウイルス辞典、デマについての情報、脅威  
についての白書にアクセスできます。      [www.symantec.com/ja/jp/business/security\\_response](http://www.symantec.com/ja/jp/business/security_response)

