インストール ガイド

McAfee Security for Microsoft Exchange 8.6.0

使用許諾に関する情報

使用許諾契約

全ユーザーへの注意事項：購入された使用許諾に対応する適切な法的取り決めを熟読してください。これには使用許諾を受けたソフトウェアの使用に関する一般取引条件が明記されています。 獲得した使用許諾の種類が不明な場合は、セールスおよびその他関連するライセンス許諾に問い合わせるか、ソフトウェアに付属の発注書、または購入時に別途受領した文書（パンフレット、製品 CD ファイル、ソフトウェアパッケージをダウンロードしたウェブサイトから入手可能なファイル）を参照してください。 取り決めに明記された条件に同意できない場合は、ソフトウェアをインストールしないでください。 該当する場合、MCAFEE または購入店に製品を返却し、全額返金を請求できます。

目次

目次

1 インストールと構成

要件に最も適した MSME ソフトウェアをインストールして使用するためのオプションを選択します。

インストールの種類		説明
スタンドアローン	**ウィザードベース**	ウィザード ベースのセットアップ ファイルを使用する際には、ユーザーの要件に従い以下のオプションのいずれかを選択します。 • [標準]－McAfee Anti-Spam アドオンを除くすべての標準機能用に構成されています。McAfee Anti-Spam アドオンは後で個別にインストールできます。 • [完全]－スパムやフィッシング詐欺による攻撃に対して保護機能を提供する McAfee Anti-Spam アドオンを含むすべての標準機能用に構成されています。 • [カスタム]－詳細設定オプション使用してセットアップをカスタマイズするために構成されています。
	サイレント	ユーザーのインターラクションやプロンプトなしにソフトウェアをインストールします。インストール プロセスの選択内容を記録できる `Silent.bat` ファイルを変更して実行します。
ePolicy Orchestrator 管理型		MSME を ePolicy Orchestrator 環境で配備すると、ご使用の Microsoft Exchange Server でポリシーの管理と実施を一元化できます。

MSME は、Microsoft Exchange Server クラスターにも配備できます。 この配備を行うには、インストール後に設定作業が必要になります。

関連トピック:
16 ページの「*クラスター展開*」

目次

インストール前

この情報を使用して MSME のインストール準備をします。

目次

システム要件

ご使用のサーバーが以下の要件を満たしていることを確認してください。

コンポーネント	要件
オペレーティング システム	• Microsoft Windows 2008 Standard/Enterprise Server SP2 (64 ビット版) • Microsoft Windows 2008 Standard/Enterprise Server R2 (64 ビット版) • Microsoft Windows 2012 Standard/Enterprise Server（64 ビット版） • Microsoft Windows 2012 Standard/Enterprise Server R2 (64 ビット版) • Microsoft Windows Server 2016 (64 ビット)
Microsoft Exchange Server	• Microsoft Exchange Server 2010 SP3 • Microsoft Exchange Server 2013 CU 12 以降 • Microsoft Exchange Server 2016 CU 3 以降
ブラウザー	• Microsoft Internet Explorer 10.0、11.1016 • Mozilla Firefox 54.0.1 • Google Chrome 59.0.3071.115 ブラウザーの設定でポップアップ ブロックを無効にしてください。
プロセッサ	• Intel エクステンデッド メモリ 64 テクノロジ (Intel EM64T) をサポートする Intel x64 アーキテクチャベースのプロセッサ • AMD 64 ビット テクノロジ搭載の AMD x64 アーキテクチャベースのプロセッサ
メモリー	MSME のインストールに関するメモリー要件は、Microsoft Exchange サーバーの要件と同じです。 詳細については、『Microsoft Exchange』 の Web サイトを参照してください。 Microsoft Exchange Server 2010 • 最低－4 GB RAM • 推奨－4 GB RAM（1 つの役割）および 8 GB（複数の役割） Microsoft Exchange Server 2013 • 最低－8 GB RAM • 推奨－8 GB RAM Microsoft Exchange Server 2016 • 最低－8 GB RAM • 推奨－8 GB RAM
ディスク容量	最低－740 MB
ネットワーク	10/100/1000-Mbps イーサネット カード
画面解像度	1024 x 768
McAfee 管理ソフトウェア	McAfee ePolicy Orchestrator 5.1.x、5.3.x、5.9.x
McAfee Agent	McAfee Agent 5.0.5 (ビルド番号 658)

コンポーネント	要件
更新パス	McAfee Security for Microsoft Exchange 8.0 パッチ 2 McAfee Security for Microsoft Exchange 8.5 パッチ 1
IIS コンポーネント	IIS コンポーネントの要件については、KB77319 を参照してください。

更新済みのシステム要件を表示するには、KB76903 を参照してください。

サポート対象の Microsoft Exchange サーバーの役割

MSME インストールは、Microsoft Exchange サーバーのインストールに選択した役割に応じて異なります。

各バージョンの Microsoft Exchange Server には、以下の役割がサポートされています。

- Microsoft Exchange Server 2010:
  - エッジ トランスポート サーバ — ドメイン外の境界で実行され、メッセージ検疫およびセキュリティを提供します。Active Directory ドメインのメンバーではないスタンドアロン サーバにインストールされます。
  - ハブ サーバ — 組織内の電子メールのすべての流れを処理し、トランスポート ルールを適用して、Active Directory ドメインの受信者のメールボックスにメッセージを配信します。
  - メールボックス サーバ — ユーザ メールボックスを含んでいる Exchange データベースを保持します。
  - メールボックスとハブの 2 つの役割でのインストール。
- Microsoft Exchange Server 2013、2013 SP1、2016 CU 2
  - MBX Server ー メールボックスとハブの 2 つの役割が保持されます。
  - エッジ トランスポート サーバー (Microsoft Exchange Server 2013 SP1 のみ)

パッケージ コンテンツ

ソフトウェア パッケージには、必要に応じてソフトウェアをインストールしてセットアップするのに必要なファイルが格納されています。

`MSMEv86_x64.ZIP` アーカイブを解凍し、以下のディレクトリを見つけます。

フォルダー	コンテンツ
スタンドアロン	製品のスタンドアロン インストールの実行に必要なファイルが格納されています。 • `Setup_x64.exe`ーウィザードを使用してソフトウェアをインストールするためのセットアップ ファイル。 • `Silent.bat`ープロンプトやウィザードを使用せずにソフトウェアをインストールするための レコード ファイル。
`ePO`	ePolicy Orchestrator を使用して製品の管理に必要なインストールファイルと設定ファイルが格納されています。 • `ePO_Extension_XX` ー 製品の拡張ファイルが含まれています。拡張ファイルは、ロケールごとに別のフォルダに保存されています。 例: `ePO_Extension_EN`。 • `MSME_Deployment_x64_xxxx.zip` ー 管理対象クライアントでソフトウェアを配備するための配備パッケージ。 • `MSME_AS_Deployment_xxxx.zip` ー 管理対象クライアントで McAfee Anti-Spam コンポーネントを配備するための配備パッケージ。 • `MSMEePOUpgrade.zip` ー アップグレード時にポリシーを MSME 8.0.2 または 8.5.1 から MSME 8.6 に移行するために必要な実行ファイルが格納されています。 • `MSME86REPORTS.zip`ーダッシュボードやクエリーなどの MSME レポート インターフェースを追加するための拡張ファイル。 • `help_msme_<version_number>.zip` ー 製品のヘルプ拡張ファイル
`AntiSpam`	McAfee Anti-Spam アドオン コンポーネントをインストールするための `ASAddon_x64.exe` が格納されています。

MSME インストーラーには、McAfee Agent 5.0.5 (ビルド番号 658) が含まれています。 エージェントによって ePolicy Orchestrator サーバーとリポジトリ間で情報が収集・送信され、ネットワーク全体のインストール環境が管理されます。

インストール

MSME は、ユーザーの環境に応じて各機能と共に互換性のある環境にインストールされます。

MSME は、スタンドアローン サーバーにインストールしたり、ePolicy Orchestrator と統合したりすることができます。

製品をインストールするための Windows 管理者の認証情報を持っていることを確認してください。このアカウントは、ドメイン管理者である必要があり、製品インストーラーの起動に認証情報が必要となります。

関連トピック:

目次

セットアップ ウィザードを使用したソフトウェアのインストール

Microsoft Exchange Server 2010、2013 または 2016 がインストールされたシステムにインストールします。

Microsoft Exchange Server 2010 では、MSME によってエッジ トランスポートとハブ トランスポートの役割用にトランスポート スキャンが実行され、メールボックスの役割用に VirusScan API が実行されます (設定された役割に基づきます)。

タスク

1 管理者として、Microsoft Exchange Server がインストールされているシステムにログオンします。

2 ローカル ドライブに一時ディレクトリを作成します。

3 アーカイブされたソフトウェア パッケージをダウンロードし、作成した一時ディレクトリに抽出します。

4 セットアップ フォルダーで [setup_x64.exe]（64 ビット オペレーティング システム用のセットアップ アプリケーション）をダブルクリックします。

5 ドロップダウン リストから言語を選択し、[OK] をクリックします。

6 [インストールの準備] 画面では、インストール ウィザードの準備が整い、必要なインストール ファイルがすべて展開されます。プロセスが完了すると、[ようこそ] 画面が表示されます。[次へ] をクリックします。

7 [Exchange Server の役割検出] 画面が開き、Microsoft Exchange Server のインストール中に選択した役割がリストで表示されます。[次へ] をクリックします。

8 インストール タイプを選択し、[次へ] をクリックします。

- [標準]ー一般的に使用される機能が Web ベースの製品設定とともにインストールされます。 McAfee Anti-Spam アドオンはインストールされません。
- [完全] ー (推奨) Web ベースの製品設定と McAfee Anti-Spam アドオンがインストールされます。 ノードがクラスター認識型の場合、必要なクラスター セットアップ コンポーネントとサービスもインストールされます。
- [カスタム] ー (上級ユーザーにのみ推奨) インストールするアプリケーション機能、およびそのインストール先を選択します。 この種類のインストールを選択すると、インストールできる機能がダイアログ ボックスに表示されます。 インストール ファイルのインストール先フォルダーを変更するには、[変更] をクリックします。

9 使用許諾契約に同意して、[次へ] をクリックします。

10 [追加の構成設定] 画面で以下のオプションを実行して、[次へ] をクリックします。

a [既存の設定のインポート] を選択し、同一または別のシステムの既存インストール環境から MSME の設定をインポートします。 この構成設定は、.cfg ファイルとして保存されます。 この設定をインポートするには、[インポート] をクリックし、.cfg ファイルを参照して[開く] をクリックします。

> 製品インターフェースから設定ファイルのエクスポートをすでに完了している必要があります。

b [隔離メカニズムの選択] ですべての隔離されたアイテムを保存する場所を選択し、選択した場所のオプションを完了します。

c [ローカル データベース] を選択した場合は、[参照] をクリックして、デフォルトの場所を変更します (オプション)。 [McAfee Quarantine Manager] を選択した場合は、McAfee Quarantine Manager サーバーの IP アド

レス、ポート番号、およびコールバック ポート番号を入力します。 McAfee Quarantine Manager サーバーが起動しており、隔離に使用可能な状態であることを確認します。

- [RPC] ー リモート プロシージャ コール (RPC) は、McAfee Quarantine Manager サーバーと中断のない通信を行う通信方法です。 ネットワーク接続が使用できない場合、隔離や解放などのプロセスが中断します。
- [HTTP] ー ステートレスな通信方法です。McAfee Quarantine Manager サーバーとの通信で使用します。McAfee Quarantine Manager サーバーとの通信で問題が発生した場合、接続が回復するまでアイテムはローカル データベースに保存されます。 MSME は、McAfee Quarantine Manager に隔離アイテムの送信を 3 回繰り返します。 3 回すべてが失敗すると、製品ログに書き込まれ、アイテムはローカル データベースに保存されます。
- [HTTPs] ー 安全な HTTP 通信方法。データは暗号化されて転送されます。

McAfee では、HTTP/HTTPS 通信チャネルの使用を推奨します。ステートレス通信では、McAfee Quarantine Manager とシームレスに接続できます。

d [管理者の電子メール アドレス] で、すべての通知、構成レポート、およびステータス レポートを送信する必要がある電子メール アドレスを入力します。

11 保護プロファイルを選択し、[次へ] をクリックします。

- [デフォルト] — このプロファイルは、保護を最適化してパフォーマンスを最大限向上させます。
- [拡張] — このプロファイルは、デフォルトのファイル フィルター ルールを有効にして、最大限の保護機能を提供します。 また、McAfee Global Threat Intelligence ファイルおよびメッセージ レピュテーションを使用すると、リアルタイム保護も可能になります。
- [既存を使用] — (アップグレードのみ) このオプションは、既存の保護プロファイルを使用します。

12 インストール ウィザードでデスクトップにアプリケーションのショートカットを作成する場合、[デスクトップにショートカットを作成] を選択し、[次へ] をクリックします。

13 [プログラムのインストール準備] 画面で選択した構成を確認し、[インストール] をクリックします。 [McAfee Security for Microsoft Exchange のインストール] 画面が開き、コピー、初期化、およびインストールされる機能が表示されます。

MSME によって、Active Directory に [MSMEODuser] という名前のユーザーが作成されます。 オンデマンド スキャンを実行するにはこのユーザーが必要です。

14 インストールが完了すると、[インストール ウィザードの完了] 画面が表示されます。 必要に応じてオプションを選択し、[完了] をクリックします。

プロンプトが表示されたら、ドメイン管理者の認証情報を入力します。

- [製品ユーザー インターフェースの起動]ーインストール ウィザードの終了後、MSME スタンドアロン ユーザー インターフェースを起動します。
- [readme ファイルを表示] ー 製品に関する最新情報、変更、既知の問題または解決された問題が記載されたリリース ノート ([Readme.pdf]) を表示します。
- [今すぐ更新] ー (推奨) 最新の DAT ファイル、エンジン、スパム対策更新機能を使用して MSME を更新します。

- [McAfee Business Community に登録して最新の状態を維持してください] ― 製品、新規リリース、更新、他の関連情報に関する情報を受信します。
- [Windows インストーラのログの表示] ― インストール プロセスのログ ファイルを表示します。

インストール プロセスの完了後、コンピューターを再起動することをお勧めします。

MSME ソフトウェアはシステムに正常にインストールされました。

McAfee Anti-Spam アドオンの手動インストール

MSME の完全またはカスタム インストールの一部として McAfee Anti-Spam をインストールしていない場合は、アドオンを手動でインストールします。

タスク

1 管理者として、Microsoft Exchange Server がインストールされているシステムにログオンします。

2 ソフトウェア パッケージ内の `\AntiSpam` フォルダーを参照し、[ASAddOn_x64_Eval.exe] をダブルクリックします。

3 ドロップダウン リストから言語を選択し、[OK] をクリックします。

4 [ようこそ] 画面で [次へ] をクリックし、[エンド ユーザー使用許諾条件] 画面を表示します。

5 使用許諾契約に同意して、[次へ] をクリックします。

6 [プログラムのインストール準備] 画面で選択した設定を確認し、[インストール] をクリックします。[Microsoft Exchange 用 McAfee Anti-Spam アドオンのインストール] 画面が開き、コピー、初期化、およびインストールされている機能が表示されます。

7 インストールが完了すると、インストール ウィザードの [完了] 画面が表示されます。必要に応じて、[Windows インストーラのログの表示] を選択してインストール プロセスのログ ファイルを表示し、[完了] をクリックします。

McAfee Anti-Spam アドオンがご使用のシステムに正常にインストールされました。

サイレント インストールの実行

インストール プロセスの選択内容を記録できる `Silent.bat` ファイルを使用して、インストールを自動化できます。

デフォルト設定で製品をインストールするには、ダウンロード パッケージで利用できる `Silent.bat` をダブルクリックします。

[Silent.bat] は内部で MSME セットアップ ファイルを呼び出します。 インストール内容を [Silent.bat] のみに引き継ぐことはできないため、同一ディレクトリ内で `setup_x64.exe` が使用できる状態であることを確認してください。

インストール内容をカスタマイズするには、バッチ ファイルを実行する前に以下のパラメーターを変更します。

パラメーター	値	説明
ADMIN_EMAIL_ID	`<admin>@<msme>.com`	管理者の通知用メール アドレスを指定します。たとえば、SET ADMIN_EMAIL_ID=administrator@msme.com のように指定します。 ポリシーで [通知送信] オプションを有効にすると、MSME はこのメール アドレスに通知を送信します。
AUTO_UPDATE	`1` または `0`	自動更新を有効化または無効化します。 • 1 = 有効化 • 0 = 無効化 有効にすると、ソフトウェアのインストールの完了直後に DAT とエンジンの更新が実行されます。 McAfee では、エンジンと DAT ファイルを常に最新の状態にするため、自動更新を有効にすることをお勧めします。
INSTALL_DIR	`%SystemDrive%\MSME`	インストール パスを指定します。 たとえば、`C:\MSME` と指定すると、MSME というフォルダーが C ドライブに作成されます。
NEED_DESKTOP_SHORTCUT	`1` または `0`	インストールが成功したらデスクトップ ショートカットを作成するかどうかを指定します。 • 1 = はい • 0 = いいえ デフォルト値は 1 です。
DB_PATH_CHANGED	`1` または `0`	Postgres データベース パスを変更するかどうかを指定します。 • 1 = はい • 0 = いいえ データベース パスはインストール後にいつでも変更できます。 パスを変更すると、新しいデータベースが作成され、検出アイテムが格納されます。 以前のデータベースに格納された検出アイテムは新しいデータベースで使用できません。
DATABASEDIR	<New Postgres DB Location>	新しい Postgres データベースの場所を指定します。例えば、`C:\TestDB` のように指定します。

パラメーター	値	説明
QUARANTINE_MECHANISM	`1` または `2`	隔離アイテムの場所を指定します。 • 1 = [ローカル データベース] • 2 = [McAfee Quarantine Manager] **ローカル データベース** — ローカル システムで検出アイテムを隔離します。 **McAfee Quarantine Manager サーバー** — 検出アイテムを MQM サーバーのストレージで一元管理します。 McAfee Quarantine Manager を選択する場合には、MQMIPADDRESS、MQMPORTNUMBER、MQM_ COMMUNICATION_MECHANISM の設定も定義してください。 この設定は、インストール後にソフトウェアのインターフェースからいつでも変更できます。
MQMIPADDRESS	`IPv4` または `IPv6` アドレス	MQM サーバーの IP アドレスを指定します。MSME は、IPv4 と IPv6 の両方のネットワークをサポートしています。
MQM_COMMUNICATION_MECHANISM	`0` または `1` または `2`	MQM サーバーとの接続に使用する通信チャネルを指定します。 • 0 = RPC • 1 = HTTP • 2 = HTTP McAfee では、HTTP/HTTPS 通信チャネルの使用を推奨します。ステートレス通信では、MQM サーバーとシームレスに接続できます。
MQMPORTNUMBER	`80` または `443` または `49500`	通信チャネルのポート番号を指定します。 • 80 = HTTP プロトコル • 443 = HTTPs プロトコル • 49500 = RPC プロトコル
AGREE_TO_LICENSE	`Yes` または `No`	ライセンス使用許諾に同意してソフトウェアをインストールします。 たとえば、SET AGREE_TO_LICENSE = `Yes` のように指定します。

サイレント インストールは、McAfee Anti-Spam アドオンを除くすべての標準機能に対応しています。 McAfee Anti-Spam アドオンを別途インストールする必要があります。 詳細については、『McAfee Anti-Spam アドオンを手動でインストールする』を参照してください。

スタンドアローン配備のアップグレード

MSME 8.6 では、8.0 パッチ 2 または 8.5 パッチ 1 から設定をアップグレードできます。

開始する前に

Exchange データベースと Exchange トランスポート サービスがインストール プロセス中に再起動するため、Microsoft Exchange サーバーをメンテナンス モードで配置します。

McAfee Anti-spam モジュールの前のバージョンをインストールしている場合には、ソフトウェアのアップグレード前に McAfee Anti-spam モジュールを削除する必要があります。 アップグレード後に McAfee Anti-spam の最新バージョンをインストールできます。

MSME では、XSS の脆弱性が存在する HTML タグの使用を禁止し、セキュリティを強化しています。 McAfee では、アップグレードを行う前に、既存の通知テンプレートから XSS の脆弱性が存在する HTML タグを削除することをお勧めします。 アップグレード後に未対応のタグを含む通知テンプレートを変更しようとすると、プロンプトが表示され、テンプレートから未対応のタグを削除するか、変更を行わずにテンプレートを使用するのかを確認されます。 未対応の HTML タグについては、McAfee KnowledgeBase の記事 KB82214 を参照してください。

新しいバージョンにアップグレードする場合、既存のバージョンを削除する必要はありません。 インストール プログラムが新しいバージョンに更新します。

タスク

1 管理者として、Microsoft Exchange Server がインストールされているシステムにログオンします。

2 セットアップ フォルダーで [setup_x64.exe]（64 ビット オペレーティング システム用のセットアップ アプリケーション）をダブルクリックします。

3 [インストールの準備] 画面では、インストール ウィザードの準備が整い、必要なインストール ファイルがすべて展開されます。プロセスが完了すると、[ようこそ] 画面が表示されます。[次へ] をクリックします。

4 [Exchange Server の役割検出] 画面が開き、Microsoft Exchange Server のインストール中に選択した役割がリストで表示されます。[次へ] をクリックします。

5 [セットアップのタイプ] 画面では、[カスタム] オプションがデフォルトで選択されています。[次へ] をクリックします。

6 [カスタム セットアップ] 画面が開き、既存のインストール環境にインストール済みの機能がリストで表示されます。 McAfee Security for Microsoft Exchange で更新する機能を選択し、[次へ] をクリックします。

7 使用許諾契約に同意して、[次へ] をクリックします。

8 [追加の構成設定] 画面が開き、既存のインストール環境に適用された隔離メカニズムと隔離データベースの設定が表示されます。必要に応じて設定を変更し、[次へ] をクリックします。旧バージョンからポリシーを移行するには、[既存の設定のインポート] オプションを選択し、設定ファイルを参照して選択します。

9 [保護プロファイルの設定] 画面で、必要に応じて [デフォルト]、[拡張]、または [既存を使用] を選択し、[次へ] をクリックします。

> [既存の設定のインポート] を選択済みの場合、この画面ではすべてのオプションがグレー表示になっています。 デフォルトでは、[既存を使用] オプションが選択されています。

10 インストール ウィザードでデスクトップにアプリケーションのショートカットを作成する場合、[デスクトップにショートカットを作成] を選択し、[次へ] をクリックします。

11 [プログラムのインストール準備] 画面で選択した構成を確認し、[インストール] をクリックします。 [McAfee Security for Microsoft Exchange のインストール] 画面が開き、コピー、初期化、およびインストールされる機能が表示されます。

アップグレード時に、ソフトウェアがシステムに既存の DAT バージョンを確認します。ソフトウェア パッケージの DAT バージョンがシステムで使用可能な DAT バージョンよりも新しい場合にのみ、アップグレードが実行されます。

12 インストールが完了すると、[インストール ウィザードの完了] 画面が表示され、デフォルトで [隔離データの移行] オプションが選択されています。 [完了] をクリックします。

前のバージョンでプロキシを設定している場合には、アップグレード後にプロキシを再度設定する必要があります。 インストールの完了後、コンピューターを再起動することをお勧めします。

McAfee Security for Microsoft Exchange が正常にアップグレードされます。

インストール後

MSME をインストール後、特定の追加設定を実行し、ご使用の環境向けにセットアップします。

クイック セットアップ

MSME を簡単にセットアップし、組織の Exchange サーバー環境を保護する手順です。

組織の Exchange サーバーで MSME をインストールしたら、管理者として以下のタスクを実行します。

タスク

1 エンジン/DAT アップデートを実行し、ソフトウェアを更新します。詳細については、『 ソフトウェア アップデートのスケジュール設定』を参照してください。

2 エッジ トランスポートまたはハブ トランスポート サーバーで MSME をインストール済みの場合は、以下のコマンドを実行して Exchange Power Shell（Exchange Management Shell）に MSME エージェントが読み込まれていることを確認してください。

```
Get-TransportAgent
```

先頭が「McAfee」で始まるエージェントに対しては、「有効」のステータスは必ず true にしてください。

3 スパムやフィッシング詐欺電子メール メッセージを隔離するため、McAfee Anti-Spam アドオン コンポーネントを必ずインストールしてください。

4 [設定と診断] 、 [通知] 、 [設定] タブで、管理者の電子メール アドレスを更新します。

5 新しいステータス レポート タスクのスケジュールを設定します。詳細については、『新しいステータス レポートのスケジュール設定』を参照してください。

6 構成レポート タスクのスケジュールを設定します。詳細については、『新しい構成レポートのスケジュール設定』を参照してください。

7 ユーザーの要件に基づきオンデマンド スキャンのスケジュールを設定します。詳細については、『オンデマンド スキャンとそのビュー』を参照してください。

8 ユーザーの要件に従い、[設定と診断] 、 [オンアクセス設定] ページでオンアクセス スキャン設定を構成します。詳細については、『オンアクセス設定』を参照してください。

9 会社のポリシーに基づいて [DLP とコンプライアンス] スキャナー設定およびルールを構成します。詳細については、『ポリシー マネージャー』のポリシー、スキャナー、フィルターの構成手順を参照してください。

10 ポリシーの例外については、組織の要件に基づきサブポリシーを作成します。

11 設定を確認するためテスト電子メール メッセージを送信します。

クラスター展開

Microsoft Exchange Server 2010、2013、2016 CU 2 のクラスター環境に MSME をインストールするには、追加の設定が必要になります。

Microsoft Exchange 2010、2013、2016 CU2 用クラスター複製ユーティリティ

[クラスター複製セットアップ ユーティリティ] は、隔離データベース、ポリシーの設定、エンジンと DAT を複製する際に役立ちます。

このユーティリティを使用できるのは、MSME のインストール（**データ アベイラビリティ グループ**（DAG）によって認識される）のみです。その場合、MSME 複製サービスも使用できます。構成設定に応じて、このユーティリティによって、隔離されたアイテムが 1 つのサーバーから他のサーバーに複製され、高度なアクセスが可能になります。

データ アベイラビリティ グループのプライマリ コンポーネントは、アクティブ マネージャーと呼ばれます。Microsoft Exchange Server 2010 はアクティブ マネージャーに依存し、データ アベイラビリティ グループの一部であるメールボックス サーバー間の切り替えとフェールオーバーを管理します。アクティブ マネージャーは、特定のデータ アベイラビリティ グループのすべてのメールボックス サーバーで実行され、以下の 2 つの役割にインストールできます。

- プライマリ アクティブ マネージャ (PAM)
- スタンバイ アクティブ マネージャ (SAM)

これらの役割に関する詳細については、関連する Exchange 2010 のマニュアルを参照してください。

複製設定の構成

隔離データベース、ポリシーの設定、エンジン、および DAT の複製設定を構成します。

タスク

1 [スタート] メニューで、[すべてのプログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] 、 [クラスター複製セットアップ] の順にクリックします。 ダイアログ ボックスが開き、このサービスのオプションが表示されます。

> Microsoft Exchange Server 2010、2013、2016 にメールボックスの役割がインストールされている場合、標準、完全、カスタムのどのセットアップでも、[クラスター複製セットアップ] が自動的にインストールされます。

2 複製に使用できるサーバーを [サーバー名] から取得します。複製に使用できるのはデータ可用性グループの一部で、MSME とメールボックスの役割がインストールされているサーバーです。

- [使用可能なサーバー] には、隔離データベース、ポリシーの設定、エンジンおよび DAT を複製するために追加するサーバーのリストが表示されます。
- [複製サーバー] には、隔離データベース、ポリシーの設定、エンジンおよび DAT の複製サーバーとして設定されたサーバーのリストが表示されます。

3 [使用可能なサーバー] からサーバーを選択し、[>>] をクリックしてそのサーバーを複製サーバー リストに追加します。

4 [複製サービスの停止] を選択し、MSME クラスター複製サービスを停止します。

5 MSME クラスター複製サービスを管理するには、[複製サービス開始の対象] を選択します。 必要なオプションを選択します。

- [ポリシーの設定]
- [エンジン/DAT]
- [隔離データベース]

6 [適用] をクリックし、クラスタ複製設定を保存して適用します。

7 確認プロンプトが表示されたら、MSME サービスを再起動するオプションを選択します。複製の実行には再起動が必要です。

McAfee Security for Microsoft Exchange アクセス制御を設定する

特定のユーザーやグループの MSME ユーザー インターフェースへのアクセスを許可または拒否します。

タスク

1 [スタート] から、[プログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] 、 [Access Control] の順にクリックします。[アクセスのアクセス許可] ダイアログ ボックスが表示されます。

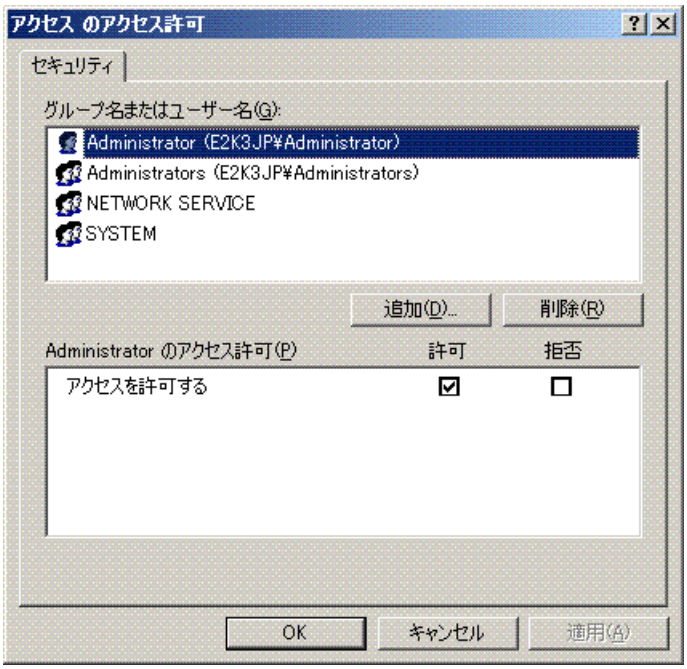

図 1-1 アクセスのアクセス許可

2 [グループ名またはユーザ名] で、MSME ユーザー インターフェースへのアクセスを許可または拒否するユーザーを選択します。

3 [OK] をクリックします。

Sitelist エディター

[Sitelist] は、自動更新 (DAT ファイルとスキャン エンジンを含む) をダウンロードする場所を指定します。

Sitelist エディターへのアクセス

- [スタート] メニューで [プログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] 、 [Sitelist エディター] の順にクリックします。

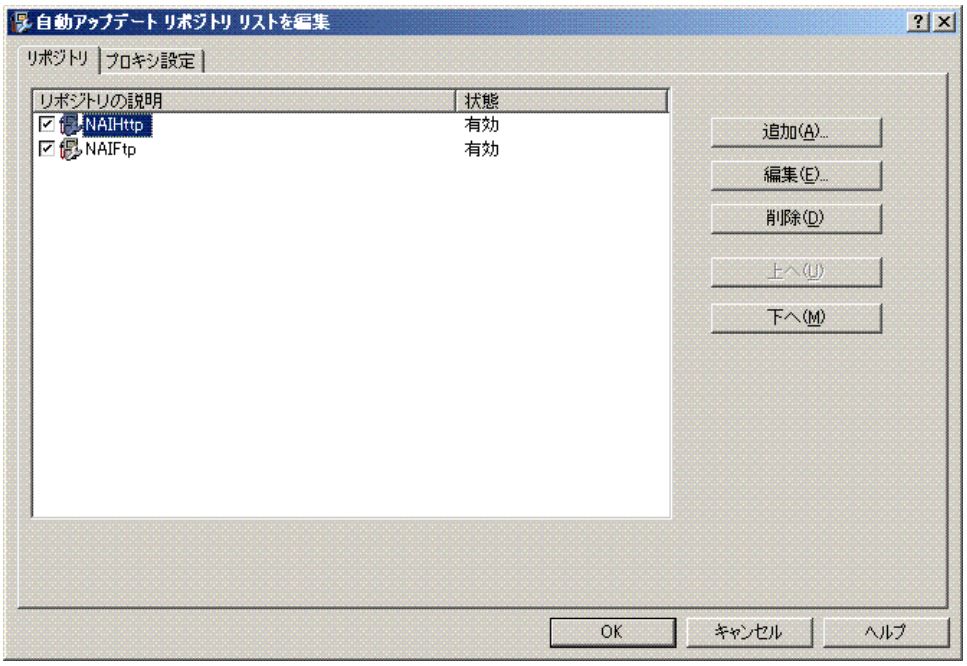

図 1-2 自動アップデート リポジトリ リストを編集

以下のタブを使用できます。

- [リポジトリ]ーMSME による自動更新のダウンロード元のリポジトリ設定を構成します。

  MSME では自動更新のために McAfee サイトをポイントする Sitelist がデフォルトで使用されますが、別の場所をポイントする代替 Sitelist を作成することもできます。例えば、自動更新をローカル リポジトリにコピーして、MSME システムからそのローカル リポジトリを示す Sitelist を作成できます。

- [プロキシ設定]ー自動更新をダウンロードするに当たり、プロキシ サーバーを使用して MSME からインターネットに接続できるように、プロキシ サーバーの設定を構成します。

Sitelist エディターに適用された設定は、`C:\ProgramData\McAfee\Common FrameWork\` ディレクトリの `SiteList.xml` ファイルに保存されます。

Sitelist リポジトリ設定の構成

[Sitelist] によって、自動更新のダウンロード元が指定されます。

McAfee Security for Microsoft Exchange のデフォルトでは、自動更新用に McAfee サイトをポイントする Sitelist が使用されますが、別の場所をポイントする Sitelist も使用できます。例えば、自動更新をローカル リポジトリにコピーし、そのローカル リポジトリを McAfee Security for Microsoft Exchange システムの場所としてポイントする Sitelist を作成する場合があります。

タスク

1 [スタート] 、 [プログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] 、 [Sitelist エディター] の順にクリックします。[自動更新リポジトリ リストを編集] ダイアログ ボックスが表示されます。

2 [リポジトリ] タブで [追加] をクリックします。[リポジトリの設定] ダイアログ ボックスが表示されます。

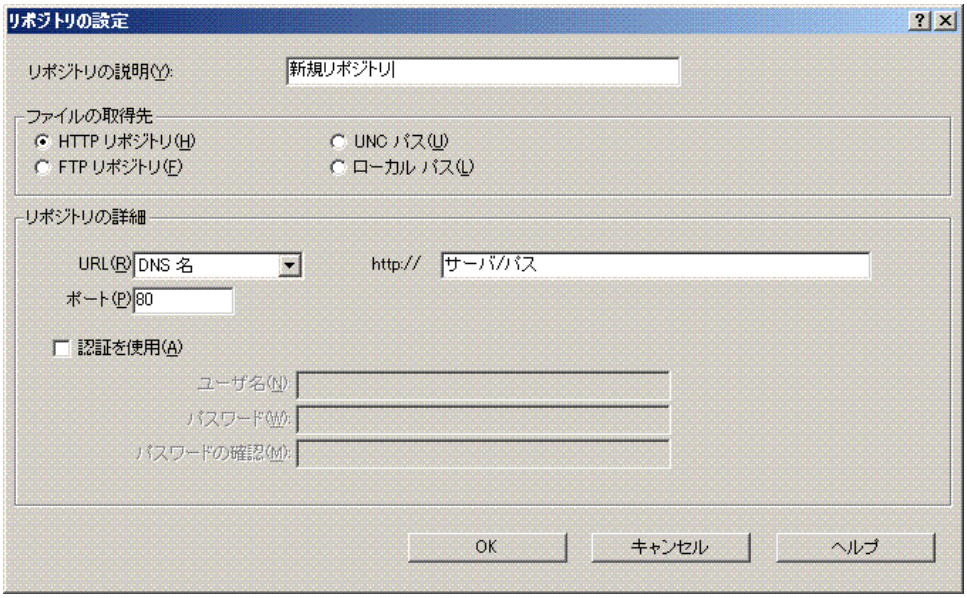

図 1-3 リポジトリの設定

3 以下のオプションを選択します。

- [リポジトリの説明] — リポジトリについての短い説明を入力します。
- [ファイルの取得先] — ファイルを取得するリポジトリの種類を指定します。使用可能なオプションは、[HTTP リポジトリ]、[FTP リポジトリ]、[UNC パス]、および [ローカル パス] です。
- [URL] — リポジトリの URL を指定します。
- [ポート] — リポジトリのポート番号を指定します。
- [認証を使用] — リポジトリにアクセスするためのユーザ認証を有効にします。

4 リポジトリの認証用にユーザ名とパスワードを指定し、パスワードを再入力して確認します。

5 [OK] をクリックして、新しいリポジトリを [リポジトリの説明] リストに追加します。

6 [OK] をクリックして [自動更新リポジトリ リストを編集] ダイアログ ボックスを閉じます。

Sitelist プロキシ設定の構成

ユーザーの組織でインターネットの接続にプロキシ設定を使用しており、MSME で製品アップデートをダウンロードする場合には、以下の設定を構成します。

組織がインターネットへの接続にプロキシ サーバを使用している場合は、[プロキシ設定] オプションを選択できます。

タスク

1 [スタート] 、 [プログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] 、 [Sitelist エディター] の順にクリックします。

[AutoUpdate リポジトリ リストを編集] ダイアログ ボックスが表示されます。

2 [プロキシ設定] タブをクリックします。

図 1-4 プロキシ設定

3 必要に応じて、[Internet Explorer のプロキシ設定を使用] または [プロキシを手動で設定] オプションを選択します。

4 HTTP または FTP サーバの IP アドレスとポート番号を入力します。

5 以下のオプションを使用できます。

- [認証を使用] — プロキシ サーバにアクセスするためのユーザ認証を有効にします。
- [ユーザー名]ープロキシ サーバーにアクセスするための認証用のユーザー名を指定します。
- [パスワード] — パスワードを指定します。
- [パスワードの確認] — 指定したパスワードを再確認します。
- [例外]ー特定のドメインのプロキシ サーバーを無視します。[例外] をクリックし、[例外の指定] を選択して無視する必要のあるドメインを入力します。

6 [OK] をクリックします。

インストールのテスト

MSME のインストールを完了したら、テストすることをお勧めします。

これにより、ソフトウェアが適切にインストールされており、電子メール メッセージ内のウイルスやスパムを検出できることを確認できます。

タスク

- 21 ページの「*ウイルス対策コンポーネントのテスト*」
  EICAR ウイルス対策テスト ファイルを電子メール メッセージに添付し、MSME をインストール済みの Microsoft Exchange サーバーを介してメッセージを送信します。
- 22 ページの「*スパム対策コンポーネントのテスト*」
  GTUBE（迷惑メールの一般テスト用メール）を実行し、McAfee Anti-Spam ソフトウェアをテストします。
- 22 ページの「*マカフィー バーチャル テクニシャンを使用したインストールのテスト*」
  マカフィー バーチャル テクニシャンを使用すると、製品をインストールしてから発生した可能性のある一般的な誤差を自動的に確認できます。

インストール済みのコンポーネントおよびサービス

MSME によって Microsoft Exchange サーバーに各種コンポーネントがインストールされます。

MSME コンポーネントにアクセスするには、[スタート] 、 [プログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] の順にクリックし、以下のコンポーネントをクリックします。

- [McAfee Security for Microsoft Exchange 用 McAfee Anti-Spam] — スパムおよびフィッシング詐欺のコンテンツを検出します。
- [アクセス制御]—MSME 特定のユーザーまたはグループのユーザーインターフェースへのアクセスを許可または拒否します。
- [製品設定]—Web インターフェースを介して MSME スタンドアローン バージョンを起動します。
- [Sitelist エディタ] — 自動更新 (DAT とスキャン エンジンを含む) のダウンロード元を指定します。
- [クラスタ複製セットアップ] — 隔離データベース、ポリシー設定、製品の更新を複製します (Microsoft Exchange Server 2010、2013、2016 CU 2 のみ)。 これは、MSME が認識する [データ可用性グループ] (DAG) の複製設定に依存します。

利用可能なサービス

- [McAfee Agent Service、McAfee Agent Common Service、McAfee Agent 下位互換性サービス] — McAfee ePO をインストールして使用する場合に必要です。 このサービスの詳細については、McAfee ePO 製品ドキュメントを参照してください。
- [McAfee Security for Microsoft Exchange] — Microsoft Exchange Server (バージョン 2010、2013、2016 CU 2) をウイルス、不要なコンテンツ、不要なプログラム、禁止されたファイル タイプ/メッセージから保護します。
- [McAfee スパム対策ルール アップデータ] — スパム対策ルールを更新する場合に必要になります。

ウイルス対策コンポーネントのテスト

EICAR ウイルス対策テスト ファイルを電子メール メッセージに添付し、MSME をインストール済みの Microsoft Exchange サーバーを介してメッセージを送信します。

世界中のウイルス対策ベンダー数社が共同で EICAR 標準ウイルス対策テスト ファイルを作成しました。このファイルがウイルス対策インストールの検証規格となっています。

このファイルはウイルスではありません。他のユーザーに通知されないよう、インストールのテストが終了したら必ずこのファイルを削除してください。

タスク

1 テキスト エディターを開き、以下のコードをメモ帳にコピーして名前を付けてファイルを保存します。 EICAR.COM:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

ファイル サイズは 68 バイトまたは 70 バイトです。

2 Microsoft Exchange サーバーから、EICAR テスト ファイルを添付した電子メール メッセージを送信します。

MSME によって電子メール メッセージが確認されると、EICAR テスト ファイルの検出が報告されます。ただし、EICAR ファイルはテスト ファイルに過ぎないため、駆除や修復はできません。

3 MSME によって EICAR テスト ファイルがアラート メッセージに置き換えられます。

スパム対策コンポーネントのテスト

GTUBE（迷惑メールの一般テスト用メール）を実行し、McAfee Anti-Spam ソフトウェアをテストします。

テスト用の電子メール メッセージは、外部の電子メール アカウント（別のドメイン）から送信する必要があります。

タスク

1 電子メール メッセージを作成します。

2 次のコードを本文テキストにコピーします。

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

このテキストは、必ずスペースや改行を入れずにコピーしてください。

3 外部電子メール アドレスから、McAfee Anti-Spam アドオン コンポーネントと共に MSME をインストールしたサーバー上にあるメールボックス アドレスにこの電子メール メッセージを送信します。 McAfee Anti-Spam によってメッセージがスキャンされ、ジャンク電子メール メッセージと認識して必要なアクションが実行されます。

GTUBE テストは、ブラックリストおよびホワイトリストより優先されます。GTUBE テスト ファイルの詳細については、 http://spamassassin.apache.org/.

マカフィー バーチャル テクニシャンを使用したインストールのテスト

マカフィー バーチャル テクニシャンを使用すると、製品をインストールしてから発生した可能性のある一般的な誤差を自動的に確認できます。

マカフィー バーチャル テクニシャンを実行し、MSME が正しくインストールされているかどうかテストします。

マカフィー バーチャル テクニシャンをダウンロードするには、 http://mvt.mcafee.com/mvt/index.asp.

2 インストール内容の修復

ファイルの破損や紛失、ショートカットおよびレジストリ エントリを修正し、プログラム内のインストール エラーを解決します。

また、MSME インストール内容は、[アンインストール/変更]をクリックして [コントロール パネル] 、[プログラムと機能] 、[プログラムのアンインストール] コンソールからも修復できます。インストール内容を修復すると、デフォルト設定に戻ります。

タスク

1 インストール ファイルが格納されたフォルダーで、`setup_x64.exe` をダブルクリックします。

2 [次へ] をクリックします。[プログラムのメンテナンス] 画面が表示されます。

3 [プログラムのメンテナンス] 画面で、[修復] を選択し、[次へ] をクリックします。[プログラムの修復準備] 画面が表示されます。

4 [インストール] をクリックして修復を完了します。[InstallShield ウィザードの完了] ダイアログ ボックスが表示されます。

5 [完了] をクリックして終了します。

3 ソフトウェアのアンインストール

Exchange サーバーから MSME を削除またはアンインストールします。

また、MSME の削除は、[コントロール パネル] 、[プログラムと機能] 、[プログラムのアンインストール] コンソールから実行することもできます。この方法では、デフォルトで隔離データベースが保持されます。

タスク

1 インストール ファイルが格納されたフォルダーで、`setup_x64.exe` をダブルクリックします。

[ようこそ] 画面が表示されます。

2 [次へ] をクリックします。

[プログラムのメンテナンス] 画面が表示されます。

3 [削除] を選択し、[次へ] をクリックします。

[設定の保持] 画面が表示されます。

4 [隔離データベースの保持] を選択して隔離データベースを保持し、[次へ] をクリックします。

[プログラムの削除] 画面が表示されます。

5 [削除] をクリックし、Exchange サーバーから MSME をアンインストールします。

[InstallShield ウィザードの完了] 画面が表示されます。

6 [完了] をクリックして終了します。

3 ソフトウェアのアンインストール

A よくある質問

この項では、MSME のインストールに関してよくある質問に対する回答を記載しています。

サイレント インストールはどのように実行できますか？

ダウンロード パッケージで `Silent.bat` ファイルを実行します。 カスタマイズに関する詳細については、『サイレント インストールの実行』を参照してください。

ドメイン管理者以外のアカウントで McAfee Security for Microsoft Exchange をインストールできますか？

インストールできます。 詳細については、McAfee KnowledgeBase の記事 KB82190 を参照してください。

サポート対象の ePolicy Orchestrator バージョンを教えてください。

McAfee ePolicy Orchestrator 5.1.x、5.3.x、5.9.x です。

サポート対象の McAfee Agent バージョンを教えてください。

McAfee Agent 5.0.5 ビルド番号 658 です。

MSME 構成の複製が機能するポートを教えてください。

このサービスはポートでは機能しません。ただし、管理者が複製ユーザー インターフェースを使用して設定するフォルダーを監視し続けます。

DAG 環境で MSME 8.0 パッチ 2 または 8.5 パッチ 1 から MSME 8.6 にアップグレードするときに、特に注意すべきことはありますか？

特に考慮する事項はありません。 スタンドアロン インストールの手順に従ってください。

索引

や

よ

り