製品ガイド

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

1 はじめに 7

製品の機能 . . . 7
MSME が必要な理由 . . . 10
組織への脅威 . . . 10
MSME で Exchange サーバーが保護される仕組み . . . 11
電子メールのスキャン方法 . . . 13
受信メールのスキャン . . . 13
送信電子メールのスキャン . . . 15
内部電子メールのスキャン . . . 15

2 ダッシュボード 17

検出アイテムの統計情報 . . . 17
検出 . . . 18
ソフトウェア更新のスケジュールを設定する . . . 22
オンデマンド スキャンとそのビュー . . . 23
オンデマンド スキャン タスクの表示 . . . 23
オンデマンド スキャン タスクを作成する . . . 24
ステータス レポート . . . 27
ステータス レポート タスクの表示 . . . 27
新しいステータス レポートのスケジュール設定 . . . 28
ステータス レポートの電子メール通知 . . . 30
構成レポート . . . 30
構成レポート タスクの表示 . . . 31
新しい構成レポートのスケジュール設定 . . . 32
構成レポートの電子メール通知 . . . 33
グラフィカル レポート . . . 33
簡易検索フィルターを使用したグラフィカル レポートの表示 . . . 34
詳細検索フィルターを使用する . . . 35

3 検出アイテム 39

隔離データの管理 . . . 39
検出タイプ . . . 40
使用可能なプライマリ検索フィルター . . . 42
検索フィルター比較表 . . . 45
詳細検索オプション . . . 46
検出されたアイテムの検索 . . . 47
隔離されたアイテムに対して実行可能なアクション . . . 48

4 ポリシー マネージャ 51

脅威を処理するポリシー カテゴリ . . . 52
ポリシー マネージャー ビュー . . . 52
マスター ポリシーとサブポリシー . . . 53

サブポリシーの作成 . . . 54
コア スキャナとフィルタ . . . 55
スキャナーとフィルターの比較表 . . . 57
選択したポリシーのすべてのスキャナーとフィルターをリストで表示 . . . 58
スキャナーまたはフィルターを追加する . . . 59
指定ユーザー用ルールの新規作成 . . . 60
検出時に実行可能なアクション . . . 61
共有リソース . . . 62
スキャナー設定の構成 . . . 63
アラート設定の構成 . . . 63
アラートを作成する . . . 64
DLP とコンプライアンス ルールの設定 . . . 66
ファイル フィルタリング ルールの構成 . . . 69
タイム スロットの設定 . . . 70
ポリシー用コア スキャナー設定の管理 . . . 71
ウイルス対策スキャナー設定の構成 . . . 72
DLP とコンプライアンス スキャナー設定の構成 . . . 75
ファイル フィルタリング設定の構成 . . . 77
メール URL レピュテーションを設定する . . . 78
メールの添付ファイルに対する TIE レピュテーション チェック . . . 81
メールの添付ファイルをスキャンするように TIE を設定する . . . 83
スパム対策設定の構成 . . . 84
フィッシング対策設定の構成 . . . 88
ポリシー用フィルター設定の管理 . . . 89
破損したコンテンツ設定の構成 . . . 90
保護されたコンテンツ設定の構成 . . . 91
暗号化されたコンテンツ設定の構成 . . . 91
署名付きのコンテンツ設定の構成 . . . 92
パスワードで保護されたファイル設定の構成 . . . 92
メール サイズによるフィルタリング設定の構成 . . . 93
スキャナーの制御設定の構成 . . . 94
IP アドレスを手動でブロックする . . . 95
MIME メール設定の構成 . . . 96
HTML ファイル設定の構成 . . . 98
ポリシー用その他の設定の管理 . . . 99
アラート メッセージの設定 . . . 99
免責事項のテキストの設定 . . . 100

5 設定と診断 103

オンアクセスの設定 . . . 105
Microsoft ウイルス スキャン API（VSAPI）の設定 . . . 107
バックグラウンド スキャンの設定 . . . 108
トランスポート スキャン設定 . . . 109
オンデマンド設定 . . . 109
メールボックスの除外設定の構成 . . . 111
ワイルドカードによるメールボックスの除外設定の例 . . . 112
通知設定 . . . 112
通知設定の構成 . . . 113
通知テンプレートの編集 . . . 114
使用可能な通知フィールド . . . 115
製品の正常性に関するアラートの有効化 . . . 115
スパム対策の設定 . . . 117
検出されたアイテムの設定 . . . 118

McAfee Quarantine Manager による隔離 . . . 119
ローカル データベースを使用した隔離 . . . 120
ユーザーインターフェースの設定 . . . 121
ダッシュボード設定の構成 . . . 121
グラフと図の設定の構成 . . . 122
診断の設定 . . . 123
デバッグ ログ設定の構成 . . . 123
イベント ログ設定の構成 . . . 124
製品ログ設定の構成 . . . 125
エラー レポート サービス設定の構成 . . . 127
製品ログの表示 . . . 127
DAT 設定の構成 . . . 128
構成設定のインポートとエクスポート . . . 129
既存の MSME 設定のエクスポート . . . 129
別の MSME サーバーから設定をインポートする . . . 130
Sitelist のインポート . . . 130
スパム対策プロキシ設定の構成 . . . 131

6 プログラムの保守 133
インストールの変更 . . . 133
デフォルト設定の復元 . . . 134
削除と最適化 . . . 134

7 トラブルシューティング 135
デフォルトの構成設定と拡張構成設定 . . . 135
重要なレジストリ キー . . . 136

8 よくある質問 139
全般 . . . 139
ポリシー マネージャー . . . 140
設定と診断 . . . 141
McAfee Anti-Spam アドオン コンポーネント . . . 142
正規表現（regex） . . . 143

索引 145

目次

1 はじめに

McAfee® Security for Microsoft Exchange (MSME) を使用すると、コンピューター、ネットワーク、または従業員に悪影響を与える可能性があるさまざまな脅威から Microsoft Exchange サーバーを保護できます。

MSME では、ウイルス、好ましくないコンテンツ、不審なプログラム、禁止されたファイル タイプまたはメッセージに対して高度なヒューリスティックが使用されます。 また、次の項目をスキャンできます。

- 電子メール メッセージの件名と本文
- 添付ファイル (ファイルの種類、ファイル名、およびファイルのサイズに基づく)
- 添付ファイル内のテキスト
- メール本文の URL

なお、このソフトウェアには、Exchange サーバーをスパムやフィッシング電子メールから保護する McAfee Anti-Spam アドオン コンポーネントも含まれます。

目次

- *製品の機能*
- *MSME が必要な理由*
- *MSME で Exchange サーバーが保護される仕組み*
- *電子メールのスキャン方法*

製品の機能

このセクションでは、MSME の主な機能について説明します。

- **McAfee® Threat Intelligence Exchange (TIE) とファイル レピュテーション チェックの統合** — メールの添付ファイルに TIE ファイル レピュテーション チェックを実行できます。 環境の TIE サーバーに接続している複数の情報源から取得した情報に基づいてファイルのレピュテーションを検証することで、ファイルを迅速に分析し、的確な判断を行うことができます。 メールに圧縮ファイルが含まれている場合、ファイルが展開され、対応する種類のファイルが TIE に送信されます。 対応する圧縮ファイルについては、KB89577 を参照してください。
- **McAfee® Advanced Threat Defense ファイル レピュテーション チェック** — MSME が Advanced Threat Defense をサポートするようになりました。このオンプレミス アプライアンスが TIE を利用してマルウェアを検出し、侵入を阻止します。 Advanced Threat Defense により、ネットワーク ユーザーに対して QoS を犠牲にすることなく、既知のマルウェア、ニアゼロデイ マルウェア、ゼロデイ マルウェアからシステムを保護できます。
- **なりすましメールから保護** — なりすましメールからシステムを保護します。
- **サイズの大きいメールをスキャンから除外** — メールのサイズに基づいて、オンアクセス スキャンからメールを除外することができます。

- **特定の IP アドレスからのメールをブロック** — IP アドレスのレピュテーション スコアに関係なく、特定の IP アドレスまたは IP アドレスの範囲をブラックリストに登録し、組織へのメール送信をブロックできます。
- **Microsoft Exchange 2016 のサポート** — Microsoft Exchange 2016 累積更新プログラム (CU) 3 以降をサポートします。
- **Microsoft Windows Server 2016 のサポート** — Microsoft Windows 2016 64 ビット サーバー OS をサポートします。
- **ブラウザーの追加サポート** — Microsoft Internet Explorer 11.1066、Mozilla Firefox 54.0.1、Google Chrome 59.0.3071.115 に対応しています。

製品の Web インターフェースにアクセスできるように、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。

その他の機能

- **ウイルスからの保護** — すべての電子メール メッセージをウイルス スキャンし、検出したウイルスを阻止、駆除、削除することにより Exchange サーバーを保護します。 MSME では、先進のヒューリスティック方法によって、未知のウイルスやウイルスと思われる不審なアイテムが識別・ブロックされます。
- **スパムからの保護** — スキャン中にスパム スコアを各電子メール メッセージに割り当て、これらのメッセージに対して事前に設定されたアクションを実行することで、Exchange サーバに必要な帯域幅およびストレージ容量を節約できます。
- **フィッシングからの保護** — 個人情報を不正に取得しようとするフィッシング電子メールを検出します。
- **不正な URL からの保護** — 不正な URL からシステムを保護します。 有効にすると、MSME はメール本文の URL をスキャンしてリンクのレピュテーション スコアを取得します。このスコアと定義済みのしきい値を比較して、設定に従ってアクションを実行します。
- **パッカーと不審なプログラムの検出機能** — 実行可能ファイルのオリジナル コードを圧縮して暗号化するパッカーを検出します。また、不審なプログラム (PUP) も検出します。これはコンピュータのセキュリティ状態やプライバシーの状態を変更するための、合法的な会社によって記述されたソフトウェア プログラムです。
- **コンテンツ フィルタリング** — 各電子メール メッセージの件名行または本文、添付ファイルのコンテンツとテキストがスキャンされます。 MSME では、正規表現 (Regex) に基づくコンテンツ フィルタリングがサポートされます。
- **ファイルのフィルタリング** — 添付ファイルのファイル名、種類、サイズに応じて、電子メールの添付ファイルがスキャンされます。 また、MSME では、暗号化、破損、パスワード保護、デジタル署名が行われたコンテンツを含むファイルがフィルタリングされます。
- **DLP とコンプライアンス** — メール コンテンツが組織の機密性とコンプライアンス ポリシーに準拠することを保証する機能。 次のコンプライアンス ディクショナリが事前に定義されています。
  - DLP とコンプライアンス ディクショナリが新たに 60 種類追加されました。
  - 業界専用のコンプライアンス ディクショナリ — HIPAA、PCI、ソース コード (Java、C++ など) のサポート
  - 既存のフレーズ ベースの検出を機能強化しています。
  - しきい値のスコアと最高用語カウント数 (出現数) を組み合わせた数値に基づき、非対応コンテンツの検出機能を強化したことによる誤検知の削減。

  コンテンツ セキュリティと Data Loss Prevention (DLP) のカスタム ポリシー。

- **IP レピュテーション** — 送信サーバーの IP アドレスに基づき、電子メール メッセージから脅威を検出する方法。ネットワーク接続で脅威が発生する確率を反映する IP レピュテーション スコア。 IP レピュテーションでは、McAfee Global Threat Intelligence (GTI) を活用して、最後の電子メール サーバーのソース IP アドレスに基づいてゲートウェイで電子メール メッセージをブロックすることで、損失やデータ盗難が予防されます。 MSME では、IP レピュテーション スコアに基づいて接続を拒否またはドロップすることで、メッセージが組織に受信される前に処理されます。
- **詳細オンデマンド スキャン** — Exchange Server 2010 と 2013 で詳細レベルのオンデマンド スキャンを実行できるため、オンデマンド スキャンの速度が迅速化しました。 オンデマンド スキャンのスケジュールを設定するときに、件名、添付ファイル、送信者/受信者/CC、メール サイズ、メッセージ ID、未読アイテム、期間、などのフィルターを使用できます。
- **バックグラウンド スキャン** — 情報ストア内のすべてのファイルのスキャンが円滑化されます。 バックグラウンド スキャンのスケジュールを設定すると、最新のエンジンとスキャン設定を使用して、選択したメッセージを定期的にスキャンできます。 MSME では、スキャンしないメールボックスを除外できます。
- **製品の正常性に関するアラート** — 製品の正常性のステータスに関する通知です。 これらのアラートを設定することもスケジュール設定することもできます。
- **McAfee ePolicy Orchestrator 5.1.x、5.3.x、5.9.x との統合** — ePolicy Orchestrator 5.1.x、5.3.x、5.9.x との統合により、Exchange Server の MSME を一元管理し、更新できます。 これにより、さまざまなシステムを管理および更新するための複雑さと必要な時間が削減されます。
- **Web ベースのユーザ インターフェース** — DHTML に基づくユーザ フレンドリな Web ベースのインターフェースを提供します。
- **ポリシー管理**—製品ユーザー インターフェースの [ポリシー マネージャー] メニュー オプションには、MSME で設定および管理できるさまざまなポリシーがリストで表示されます。
- **中央スキャナ、フィルタ ルール、および拡張アラート設定** — スキャナを使用して、アイテムのスキャン時にポリシーが適用できる、設定を構成できます。[ファイル フィルタリング] ルールを使用すると、ファイル名、ファイルの種類、およびファイル サイズに適用されるルールを設定できます。
- **オンデマンド/タイムベースのスキャンおよびアクション** — 電子メール メッセージを都合の良い時間帯または定期的にスキャンできます。
- **MIME (Multipurpose Internet Mail Extensions) スキャン** — 7 ビットの ASCII 文字のみをサポートする プロトコル上 (SMTP など) で、非 ASCII 形式で転送できるようにする通信規格です。
- **隔離管理** — 感染した電子メール メッセージを隔離するリポジトリとして使用するローカル データベースを指定できます。 McAfee Quarantine Manager が実行されている独自のサーバーに隔離されたメッセージを保存することもできます。これは、**他のコンピューターの隔離**と呼ばれます。
- **ウイルス定義、Extra DAT、ウイルス対策エンジン、スパム対策エンジンの自動更新** — 最新の脅威を検出して駆除するため、更新された DAT ファイル、ウイルス対策スキャン エンジン、スパム対策エンジンを定期的に提供します。
- **古い DAT の保持とパージ** — 定義した期間、古い DAT ファイルを保持し、必要に応じてこれをパージします。
- **Sitelist エディターのサポート** — MSME 用に自動更新のダウンロード元の場所を指定します。
- **中小企業向けサーバーのサポート** — MSME は中小企業向けサーバーと互換性があります。
- **検出レポート** — 検出されたアイテムに関する情報を表示できる、状態レポートとグラフィカル レポートを生成します。
- **構成レポート**—サーバー、バージョン、ライセンスの状態と種類、製品、デバッグのログ、オンアクセス設定、オンアクセス ポリシー、およびゲートウェイ ポリシーなどに関する情報の製品構成の概要が表示されます。サーバーから構成レポートが管理者へ送信される時刻を指定できます。

- **サービス拒否攻撃の検出** — ネットワーク上の通常トラフィックをフラッディングおよび遮断する追加要求や攻撃を検出します。 サービス拒否攻撃では、正規の要求に応答できないように、攻撃対象に対して偽の接続要求を大量に送信します。 MSME は、次のシナリオをサービス拒否攻撃と見なします。
  - スキャン時間が定義した時間を超過している場合
  - ネスト レベルが定義済みのレベルを超えている場合
  - アーカイブ ファイルで展開可能なファイルのサイズが定義済みのサイズを超えている場合
- **詳細通知** — 検出カテゴリに基づき、コンプライアンス監査のために隔離された電子メールを複数のユーザーに転送します。
- VMware Workstation 7.0 以降と VMware ESX 5.5 のサポート

MSME が必要な理由

企業は、評判、従業員、コンピュータ、およびネットワークに影響を与える可能性のある多くの脅威から被害を受けやすくなっています。

- 企業の評判は、機密情報の消失や法的措置に発展するような中傷語句などに影響を受けます。
- 無制限に電子メールやインターネットを使用できる状態では、従業員の生産性に影響が出る場合があります。
- ウイルスやその他の不要なソフトウェアにより、コンピュータが使用できなくなる危険性があります。
- また、ネットワーク上で使用される各種ファイル タイプを制御しないと、組織全体のパフォーマンスが低下する危険性があります。

組織への脅威

組織に悪影響を及ぼす可能性がある各種の脅威について説明します。

脅威の種類	説明
企業の評判	免責事項で保護していない場合、従業員による軽率または無知な意見が原因で、法的な問題が発生する場合があります。
スパム (不要な電子メール)	不要な商用メールはスパム メールやジャンク メールと同じです。多くの場合、受信者が求めていない広告が含まれています。スパムは脅威というよりは迷惑ですが、ネットワークのパフォーマンスを低下させることがあります。
容量の大きい電子メール メッセージ	容量の大きい電子メール メッセージや大量のファイルが添付されたメール メッセージは、電子メール サーバのパフォーマンスを低下させることがあります。
大量メール送信型ウイルス	他のウイルスと同様、これらのウイルスは駆除可能ですが、急速に拡散してネットワークのパフォーマンスを低下させる可能性があります。
望ましくない送信元からの電子メール メッセージ	従業員のメール アドレスを知っている、不満を持つ元従業員や悪質な個人は望ましくないメールを送信して、厄介な問題を起こす可能性があります。
電子メールの私的な使用	従業員の多くが組織外の電子メール アドレスを使用している場合、このようなメールは私用や業務に無関係である可能性が高くなります。
機密情報の消失	発表前の製品、お客様、またはパートナーに関連する機密情報を従業員が漏出する可能性があります。
中傷語句	メール メッセージや添付ファイルに、中傷的な語句が使用されている場合があります。これらは侮辱的なだけでなく、法的措置に発展する場合もあります。
娯楽用ファイルの転送	娯楽目的の容量の大きい動画ファイルや音声ファイルは、ネットワークのパフォーマンスを低下させる場合があります。

脅威の種類	説明
非効率的なファイル タイプ	一部のファイルは多くのメモリを使用し、転送速度を遅くする場合があります。ただし多くの場合、別のファイルを代わりに使用できます。たとえば、GIF ファイルと JPEG ファイルは、BMP ファイルよりサイズが非常に小さくなります。
サイズの大きいファイルの転送	サイズの大きいファイルの転送はネットワークのパフォーマンスを低下させます。
サービス拒否攻撃	サイズの大きいファイルが意図的に大量に送信されると、ネットワークのパフォーマンスが大幅に低下し、正規のユーザーが使用できなくなる場合があります。 サイズの大きな圧縮ファイルをスキャンする場合、MSME は次の 3 つのパラメーターを使用して DoS 攻撃かどうかを判定します。 • 圧縮ファイルのスキャン時間がしきい値を超えた場合。 • 圧縮ファイルのネスト レベルが確認された場合。 たとえば、圧縮された .zip ファイル内に他の圧縮ファイルが含まれ、圧縮ファイルの展開を連続して行った場合。 • アーカイブ ファイルの展開可能サイズがしきい値を超えた場合。
ポルノ関連のテキスト	卑猥な語句を電子メールで使用してはいけません。
ウイルスやその他の不要なソフトウェア	ウイルスやその他の不要なソフトウェアは、コンピュータやデータの使用を不可能にする場合があります。
破損または暗号化されたコンテンツ	このようなコンテンツはスキャンできません。適切なポリシーを指定して処理する必要があります。

MSME で Exchange サーバーが保護される仕組み

Exchange Server によって受信されるすべての電子メール メッセージや、メールボックスから読み取られる電子メール、メールボックスに書き込まれる電子メールにアクセスすることで、MSME で Exchange Server が保護される仕組みについて説明します。

Microsoft Exchange サーバの保護

MSME では、Exchange サーバーのメールボックスから読み取られ、またそのメールボックスに書き込まれるすべての電子メール メッセージにアクセスするに当たり、ご使用の Exchange サーバーのウイルス スキャン用インターフェースが使用されます。

- ウイルス対策スキャン エンジンは、電子メール メッセージを DAT に格納されているすべての既知のウイルス シグネチャと比較します。
- コンテンツ管理エンジンでは、MSME でコンテンツ管理ポリシーに指定されている禁止されたコンテンツが電子メール メッセージに含まれていないかスキャンされます。

上記の検査で電子メール メッセージ内にウイルスまたは禁止されたコンテンツが検出された場合、MSME によって指定アクションが実行されます。 どんなアイテムも検出されなければ、MSME によって情報がウイルス スキャン用インターフェースに返され、Microsoft Exchange 内で元のメッセージ リクエストが完了します。

リアルタイム検出

MSME は Exchange サーバーに統合され、リアルタイムでウイルスまたは他の有害なコードや不審なコードの検出および削除が行われます。 また、Exchange サーバー上のデータベースをスキャンすることで、ウイルスのない環境の維持にも一役買っています。 電子メール メッセージがソースに送信またはソースから受信されるたびに、MSME に

よって電子メールメッセージがスキャンされ、既知のウイルスやウイルスと思われる不審な動作のリストと比較して、感染したファイルが広まる前にブロックおよび駆除されます。 また、ソフトウェアで定義されたルールとポリシーを使用することで、電子メール メッセージ (および添付ファイル) 内のコンテンツもスキャンされます。

電子メール メッセージのスキャン

- スパム対策、ウイルス対策、およびコンテンツ管理のエンジンによって、コンテンツがファイル システムに書き込まれたり、Microsoft Exchange ユーザーが読み取られたりする前に、電子メール メッセージがスキャンされ、その結果が MSME に出力されます。
- ウイルス対策およびスパム対策スキャン エンジンは、電子メール メッセージを、現在インストールされているウイルス定義 (DAT) ファイルに格納されているすべての既知のシグネチャや、スパム対策ルールと比較します。また、ウイルス対策エンジンは、選択したヒューリスティック検出方法を使用して、メッセージをスキャンします。
- コンテンツ管理エンジンによって、ソフトウェアで実行中のコンテンツ管理ポリシーに指定されている禁止コンテンツが電子メール メッセージに含まれていないかスキャンされます。 電子メール メッセージにウイルス、禁止されたコンテンツまたは好ましくないコンテンツがない場合、MSME によってこの情報が Microsoft Exchange に戻されます。 検出があった場合は、構成設定内で定義されたアクションが MSME によって実行されます。

スキャンの動作

- MSME の中心となる機能は、スキャン エンジンと DAT ファイルです。 スキャン エンジンは、複合データ アナライザーです。 DAT ファイル内には数千種類のドライバーなどの情報があり、それぞれにウイルスやウイルスの種類を識別するための詳細な命令が記述されています。
- スキャン エンジンは DAT ファイルと連動します。このエンジンが、スキャンの対象となるアイテムを定義し、そのオブジェクトの内容をデコードしてアイテムを解析します。次に、DAT ファイル内の情報を使用して既知のウイルスを検索し、特定します。各ウイルスは独特のシグネチャを持っています。ウイルスに固有の一連の文字情報があり、エンジンはそのシグネチャを検索します。エンジンは、未知のウイルスの検索には、ヒューリスティック解析という技術を使用します。この技術では、オブジェクトのプログラム コードを解析し、ウイルスが一般的に持つ独特な機能を検索します。
- ウイルスの特徴を確認すると、エンジンはそのオブジェクトから可能な限りウイルスを駆除します。たとえば、添付ファイルから検出された感染マクロを削除したり、実行可能ファイルからウイルスのコードを削除したりします。

スキャン対象とスキャン条件

- ウイルスの侵入経路としては、感染したマクロや、共有プログラム ファイル、ネットワーク上の共有ファイル、電子メール メッセージと添付ファイル、フロッピー ディスク、およびインターネットからダウンロードされたファイルなど様々な経路が考えられます。各 McAfee Security ウイルス対策製品では、特定の脆弱部分を保護対象にしています。 必要なウイルス検出、セキュリティ、および駆除機能をすべて提供するために、多重の対策を講じることをお勧めします。
- MSME では、システムの需要に応じて詳細な構成が可能な幅広いオプションを提供しています。 システムでの需要は、システムのコンポーネント部分の動作方法や動作時間、コンポーネント間や外部 (特に電子メールやインターネット) との通信方法によって異なります。
- さまざまなアクションを設定または有効にすると、検出されたアイテムや不審なアイテムに対して、MSME サーバーによるそれぞれのアイテムの処理方法や実行するアクションの種類を決定できます。

電子メールのスキャン方法

MSME では、受信、送信、または内部電子メールの種別に基づき、個別の方法で電子メールがスキャンされます。

電子メール メッセージがソースに送受信されるたびに、既知のウイルスやウイルスと疑われる動作のリストと比較して MSME によってスキャンされます。 また、MSME では、ソフトウェア内で定義されたルールとポリシーを使用して、電子メール メッセージ内のコンテンツもスキャンされます。

MSME が電子メールを受信すると、次の順序でスキャンされます。

1 IP アドレスのレピュテーション
2 スパム対策またはフィッシング詐欺対策
3 なりすまし対策
4 破損または暗号化されたコンテンツ
5 ファイル フィルター
6 コンテンツ スキャン（DLP およびコンプライアンス）
7 ウイルス対策
8 メール URL レピュテーション

この順序で電子メールがスキャンされたとしても、ファイル フィルタリング スキャナーによってアイテムが最初に検出されると、隔離される前にウイルス対策のためにスキャンされます。

IP レピュテーション機能を MSME で有効化すると、ソース IP アドレスに基づくメールの検出が可能になります。 この機能は、McAfee Anti-Spam コンポーネントをインストールすると使用できます。

受信メールのスキャン

電子メールがクリーンまたは感染済みかを判定するため、組織が受信する電子メールに対して起こるイベントや MSME によるそのスキャン方法について、段階別に説明します。

以下の説明は、すべての役割に MSME がインストールされていることを前提にしています。

Microsoft Exchange Server 2010:

- エッジ トランスポート
- ハブ トランスポート
- メールボックス

Microsoft Exchange Server 2013、2016:

- エッジ トランスポート
- MBX

エッジ トランスポートまたはハブ トランスポートのサーバー役割の Exchange Server が存在しない場合、MSME はこれらの役割に関するステップを無視します。

タスク

1 ハブ サーバーの役割で `EdgeTransport.exe` がホストする SMTP スタックによって、電子メールが受信されます。
2 MSME IP エージェント (McTxIPAgent) が送信元 IP アドレスのレピュテーションを確認します。 IP エージェントのチェックは、TxAgent の操作よりも前に実行されます。
3 MSME トランスポート エージェント (McAfeeTxAgent) がメールをスキャンし、スパム、フィッシング詐欺、メール サイズを確認します。
4 検出がある場合はドロップされ、それ以外は SMTP スタックに返されます。

5 電子メールがクリーンな場合は、McAfeeTxRoutingAgent によって処理されます。

6 MSME が同じストリームを受信し、ファイル フィルタリング、コンテンツ スキャン、ウイルス スキャン、URL フィルタリングを実行します。

7 検出がある場合は、製品の構成に従ってアクションが実行されます。

8 MSME によって、Microsoft の仕様に従って電子メールに AV スタンプが押されます。

9 電子メールが Exchange ハブ サーバーの役割に送信されます。

10 ハブ サーバーの役割で `EdgeTransport.exe` がホストする SMTP スタックによって、電子メールが受信されます。

11 MSME トランスポート エージェント（McAfeeTxAgent）によって、スパムやフィッシング詐欺でないか、またはメール サイズがスキャンされます。EdgeSync（エッジおよびハブ サーバー）の場合に限り、セッションが認証され、スパム対策スキャンは省略されます。この場合、セッションの認証には送信者検査が使用されます。

12 検出がある場合は電子メールがドロップされ、それ以外は SMTP スタックに返されます。

13 電子メールがクリーンな場合は、McAfeeTxRoutingAgent によって処理され、AV スタンプの検査が行われます（ある場合）。

14 AV スタンプがある場合、ハブ サーバーの役割でエンジン/DAT を用いて MSME によって押されたスタンプと検査・比較されます。

15 スタンプが異なる場合、MSME によって同じストリームが受信され、ファイル フィルタリング、コンテンツ スキャン、ウイルス対策スキャン用にスキャンされます。

16 トランスポートでは MSME によって AV スタンプが検索され、VSAPI では Exchange Store によって同じ処理が行われます。AV スタンプが一致する場合は、MSME ではスキャン コールは受信されません。

17 検出がある場合は、製品の構成に従ってアクションが実行されます。

18 MSME によって、Microsoft の仕様に従って電子メールに AV スタンプが押されます。

19 電子メールは Exchange メールボックス サーバーの役割にルーティングされます。

20 Exchange ストアによってメールが受信されると、そのデータベースに保存される前に AV スタンプの検査が行われます。

21 AV スタンプが一致する場合は、スキャンせずにアイテムは保存されます。

22 AV スタンプが一致しない場合、Exchange ストアが VSAPI (Virus Scanning API) を呼び出し、メールをスキャンします。

VSAPI チェックは、Microsoft Exchange 2010 サーバーでのみ実行されます。

23 脅威が検出された場合、製品の設定に従ってメールが置換または削除されます。

Microsoft Exchange server 2013 と 2016 の場合、ハブ トランスポートとメールボックスの役割は使用できません。

送信電子メールのスキャン

電子メールがクリーンまたは感染済みかを判定するため、組織から送信される電子メールに対して起こるイベントや MSME によるそのスキャン方法について、段階別に説明します。

タスク

1 エンドユーザーが電子メール クライアントを使用して外部ユーザーに電子メールを送信します。

2 Exchange ストアによって電子メールが受信され、アウトボックス フォルダーでスキャンされます。

3 検出がある場合は、製品設定に従って置換または削除されます。置換の場合は、置換後の内容が転送キューに送信されます。

4 Hub / MBX 役割の `EdgeTransport.exe` でホスティングされている SMTP スタックがメールを受信します。

5 MSME トランスポート エージェント (McAfeeTxRoutingAgent) がメールをスキャンし、ファイル フィルタリング、コンテンツ スキャン、ウイルス スキャン、URL レピュテーション チェック、免責事項の追加を行います。

6 検出がある場合は、ドロップまたは置換され、適切に SMTP スタックに返されます。

7 電子メールがクリーンな場合は、次のルーティングのために SMTP スタックに返されます。

8 メールがこのハブ サーバーからエッジ サーバー役割にルーティングされた場合には、次の処理が実行されます。

   a ハブ サーバーの役割で `EdgeTransport.exe` がホストする SMTP スタックによって、電子メールが受信されます。

   b MSME トランスポート エージェント（McAfeeTxRoutingAgent）によって AV スタンプ（ある場合）がないか検査されます。

   c AV スタンプがある場合、エッジ サーバーの役割でエンジン/DAT を用いて MSME によって押されたスタンプと検査・比較されます。

   d スタンプが異なる場合、MSME が同じストリームを受信し、ファイル フィルタリング、コンテンツ スキャン、ウイルス スキャン、URL レピュテーション チェックを実行します。

   e 検出がある場合は、製品の構成に従ってアクションが実行されます。

   f MSME によって、エッジ サーバーの役割で Microsoft 仕様に従って電子メールに AV スタンプが押されます。

9 エッジ サーバーの役割で `EdgeTransport.exe` によってホストされる SMTP スタックへ、さらにルーティングするために電子メールが返されます。

内部電子メールのスキャン

電子メールがクリーンまたは感染済みかを判定するため、組織内で送信される電子メールに対して起こるイベントや MSME によるそのスキャン方法について、段階別に説明します。

タスク

1 エンドユーザーが電子メール クライアントを使用して内部ユーザーに電子メールを送信します。

2 Exchange Server 2010 の場合、Exchange がメールを受信し、送信トレイ フォルダーでメールをスキャンします。 Exchange Server 2013 と 2016 の場合、メールが送信トレイ フォルダーからトランスポート キューにリダイレクトされます。

3 検出がある場合は、製品設定に従って置換または削除されます。置換の場合は、置換後の内容が転送キューに送信されます。

4 ハブ サーバーの役割で `EdgeTransport.exe` がホストする SMTP スタックによって、電子メールが受信されます。

5 MSME トランスポート エージェント（McAfeeTxRoutingAgent）によって、ファイル フィルタリング、コンテンツ スキャン、ウイルス対策スキャン用に電子メールがスキャンされます。

6 検出がある場合は、ドロップまたは置換され、適切に SMTP スタックに返されます。

7 MSME によって、ハブ サーバーの役割の Microsoft 仕様に従って電子メールに AV スタンプが押されます。

8 電子メールがクリーンな場合は、次のルーティングのために SMTP スタックに返されます。

9 Exchange メールボックス サーバーによって電子メールが受信されます。

10 Exchange ストアが AV スタンプを確認します。スタンプが一致した場合、メールは MSME に送信されません。一致しない場合には、VSAPI がメールにウイルス スキャン、URL レピュテーション チェック、ファイル フィルタリング、コンテンツ スキャンを実行します。

2 ダッシュボード

ダッシュボードには、読んでわかりやすいように情報が整理されて表示されます。

MSME ダッシュボードには、スパム、フィッシング詐欺、ウイルス、不審なプログラム、不正な URL、好ましくないコンテンツからサーバーがどの程度保護されているかに関する情報が表示されます。 また、検出統計、製品にインストールされた追加コンポーネント、エンジンや DAT ファイルなどのコンポーネントのバージョン情報、製品ライセンス情報、最近スキャンされたアイテムに関する情報も表示されます。

目次

- *検出アイテムの統計情報*
- *ソフトウェア更新のスケジュールを設定する*
- *オンデマンド スキャンとそのビュー*
- *ステータス レポート*
- *構成レポート*
- *グラフィカル レポート*

検出アイテムの統計情報

MSME によってスキャンされた合計電子メール数、検出をトリガーした電子メールの数、検出カテゴリに基づき隔離された電子メールの数に関する詳細情報が表示されます。また、ダッシュボードにはこうした統計情報がグラフ形式で表示されるため、簡単に内容を把握して検出率を監視できます。

[統計] タブは以下のセクションに分類されます。

- [検出]
- [スキャン]
- [グラフ]

[リセット] をクリックすると、[検出] セクション内のすべてのカウンターの統計情報が消去され、値がゼロにリセットされます。統計をリセットしても、隔離されたアイテムは [検出されたアイテム] から削除されません。これらのカウンターはデータベース パスに依存するため、[設定と診断] 、[検出されたアイテム] 、[ローカル データベース] でデータベース パスを変更すると、カウンターはゼロにリセットされます。

リフレッシュ レート、[最近スキャンされたアイテム] に表示するアイテムの最大数、グラフの目盛単位、グラフと図の設定（3D 円グラフ、分割円グラフ、半透明）などのダッシュボード設定を変更するには、[設定と診断] 、[ユーザー インターフェースの設定] にアクセスします。

検出

MSME によってスキャンされた電子メールのうちクリーンなメールの数や、検出をトリガーしたアイテムの数に関する統計情報がすべて表示されます。 検出カテゴリに基づき、それぞれのカウンターが増加します。

報告された数は、いずれかの検出方法によりトリガーされる電子メールおよび文書の数を示します。例えば、ある電子メールに 2 種類のウイルス ファイルが添付されている場合、[ウイルス] の統計は 2 ではなく 1 増加します。統計のレポートは、個々のファイルや検出に基づくものではなく、電子メール メッセージを基準とし、メール サーバー環境でより直感的になっています。

ご使用の MSME サーバーが ePolicy Orchestrator によって管理され、サービスを再起動するか、または [リセット] ボタンをクリックする場合、McAfee ePO に保存された履歴データに応じて McAfee ePO レポート内で統計情報は変動します。 McAfee ePO レポートの詳細については、『MSME と ePolicy Orchestrator の統合』を参照してください。

表 2-1 使用されるアイコン—検出セクション

アイコン	説明
	アイコンの上にカーソルを置いたときに、検出カテゴリに関する追加情報が表示されます。
	各検出カテゴリの統計がグラフ内に表示されていることを示します。
	各検出カテゴリの統計がグラフ内に表示されていないことを示します。

グラフィカル アイコン および が表示されるのは、[グラフ] ドロップダウン リストから [<選択された検出>] オプションを選択するときに限られます。

以下の表では、各検出カテゴリに関する詳細情報を確認できます。

表 2-2 検出定義

カテゴリ	追加情報	説明
[駆除]	メール フローに検出数を超える数のクリーンなメールがある場合、この アイコンをクリーンなメールに有効化すると、他のカテゴリのグラフが抑制されます。このような場合、[クリーン] カテゴリの横にある アイコンを無効にします。	ユーザーに対して脅威とならず、いかなる MSME スキャナーもトリガーしない正規のメール。
[スパム]	このカウンターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。	多くの場合、未承認広告電子メール メッセージは、請求や登録をしていないにもかかわらず大量の受信者に一括送信されます。
	[スパムのスキャン]	MSME によってスパムがないかスキャンされたすべての電子メール。
	[スパムを検出]	スパムとして識別されたものの、ポリシー設定によって隔離はされていない電子メール。
	[スパムとしてブロック]	スパムとして識別され、ポリシー設定によって隔離された電子メール。

表 2-2 検出定義 *(続き)*

カテゴリ	追加情報	説明
[フィッシング詐欺]	このカウンターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。	フィッシングまたはフィッシング詐欺とは、不正または詐欺的な手段によって第三者が個人情報を入手する方法を指します。 この個人情報には、クレジット カード情報、パスワード、銀行口座番号などの情報が含まれます。このようなフィッシング詐欺に使用される電子メールは、銀行や実在する企業が発行する電子メールに類似したり、模倣した内容になっています。通常、このような電子メールでは、特定の個人情報を確認または更新するためのリンクをクリックすることを要求します。 迷惑メールと同様に、フィッシング詐欺メールも一括で送信されます。
	[フィッシングの検出]	フィッシング詐欺として識別されたものの、ポリシー設定によって隔離はされていない電子メール。
	[ブロックされたフィッシング詐欺]	フィッシング詐欺として識別され、ポリシー設定によって隔離された電子メール。
[なりすましメール]	このカウンターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。	
	[検出された SPF ハード エラー]	ハード エラーのなりすましメールとして識別されたメール。
	[検出された SPF ソフト エラー]	ソフト エラーのなりすましメールとして識別されたメール。
[IP レピュテーション]	このカウンターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。	送信サーバーの IP アドレスに基づき、電子メール メッセージから脅威を検出する方法。ネットワーク接続で脅威が発生する確率を反映する IP レピュテーション スコア。 IP レピュテーションでは、McAfee Global Threat Intelligence (GTI) を活用して、最後の電子メール サーバーのソース IP アドレスに基づいてゲートウェイで電子メール メッセージをブロックすることで、損失やデータ盗難が予防されます。 MSME では、IP レピュテーション スコアに基づいて接続を拒否またはドロップすることで、メッセージが組織に受信される前に処理されます。
	[衝突した IP]	MSME サーバーによって受信されたすべての電子メール。
	[ドロップされた IP]	IP レピュテーション機能によって MSME で隔離された電子メール。 この場合、送信者には電子メール送信ステータスは通知されません。
	[拒否された IP]	IP レピュテーション機能によって MSME で隔離された電子メール。 この場合、送信者には電子メール送信ステータスが通知されます。
[ウイルス]		ディスクや他のファイルに付着し、繰り返し自己複製するコンピューター プログラム ファイル。通常は、ユーザーが気付いたり、許可を与えることはありません。 一部のウイルスはファイルに付着するため、感染したファイルを実行するとウイルスも実行されてしまいます。 また、コンピューターのメモリーの中に潜み、コンピューターによってファイルが開かれたり、変更・作成されたりするとファイルが感染する仕組みのウイルスもあります。 ウイルスには症状を示すものもあれば、ファイルやコンピューター システムに損傷を与えるものもあります。いずれにしても、ウイルスを定義する場合に極めて重要になるのは、「害のないウイルスでもウイルスはウイルスに違いない」という考え方です。
	[ウイルスの検出]	受信電子メール内で検出され、ポリシー設定によって適切なアクションが実行されたウイルス。
	[駆除されたウイルス]	受信電子メール内で駆除され、ポリシー設定によって適切なアクションが実行されたウイルス。

表 2-2 検出定義 *(続き)*

カテゴリ	追加情報	説明
[TIE と ATD の検出]	[ファイル レピュテーション]	ファイルのレピュテーション チェックのために TIE サーバーに送信される添付ファイル。
	[証明書レピュテーション]	証明書のレピュテーション チェックのために TIE サーバーに送信される署名付きの添付ファイル。
	[ATD 送信]	許容されるカテゴリとファイル サイズに基づくレピュテーション チェックのために ATD サーバーに送信される添付ファイル。
	[TIE 検出の合計数]	TIE で検証された添付ファイルのレピュテーション。
[不審なプログラム]		不審なプログラム (PUP) は、合法的な企業によって作成されたソフトウェア プログラムですが、誤ってインストールすると、コンピューターのセキュリティまたはプライバシー ポリシーが変更される可能性があります。このようなプログラムは、正規のアプリケーションと一緒にダウンロードされる可能性があります。
	[PUP 検出]	受信電子メール内で検出され、ポリシー設定によって適切なアクションが実行された不審なプログラム (PUP)。
	[ブロックされた PUP]	受信電子メール内で駆除され、ポリシー設定によって適切なアクションが実行された不審なプログラム (PUP)。
[禁止されたファイル タイプとメッセージ]		特定の種類の添付ファイルは、ウイルスに感染しやすい傾向があります。ファイル拡張子によって添付をブロックする機能は、メール システムの別の層のセキュリティです。 内部メールと外部メールの両方で、禁止されたファイル タイプやメッセージが含まれていないかどうかが検査されます。
	[禁止されているファイルの種類]	特定の種類の添付ファイルは、ウイルスに感染しやすい傾向があります。ファイル拡張子によって添付をブロックする機能は、メール システムの別の層のセキュリティです。
	[禁止されたメッセージ]	自社のメール システムの通貨を禁止したい特定の電子メール メッセージ。内部メールと外部メールの両方に対して、禁止されたコンテンツが検査されます。
[DLP とコンプライアンス]	使用可能なディクショナリを表示するには、[ポリシー マネージャー]、[共有リソース]、[DLP とコンプライアンス ディクショナリ] の順に選択して、[カテゴリ] ドロップダウン リストをクリックします。	電子メールによる機密情報の漏えいを止めます。 MSME では、業界第 1 位の電子メール コンテンツ分析を提供し、あらゆる形式の機密コンテンツを極めて厳密に調整することで、州、国、および海外の規制への準拠をサポートしています。 業界で最高の拡張性を持つ電子メール Data Loss Prevention（DLP）や、ポリシー ベースのメッセージ処理機能を使用してデータ漏えいを予防します。前者はパターン一致を実行してデータを検出するツールで、後者は送信データの損失を防ぐツールです。
[好ましくないコンテンツ]		好ましくないコンテンツとは、ユーザーが電子メールを介して受信したくないコンテンツのことです。 所定の単語やフレーズによってルールが定義され、そのルールに違反する場合には対応するポリシーがトリガーされ、電子メールはブロックされます。
	[パッカー]	圧縮された実行ファイルは、実行中に自身をメモリー内に展開または復号 (あるいは両方とも実行) します。したがって、ディスク上のファイルはそのファイルのメモリー イメージと異なります。 パッカーは主に、セキュリティ ソフトウェアの回避やリバース エンジニアリングの防止を目的として設計されています。

表 2-2 検出定義 *(続き)*

カテゴリ	追加情報	説明
	[暗号化/破損したコンテンツ]	暗号化または破損したコンテンツが含まれるとは分類できない電子メール メッセージ。
	[暗号化されたコンテンツ]	メールが暗号化されている場合があります。この場合、メールのコンテンツはスキャンできません。 暗号化されたコンテンツのポリシーによって、暗号化された電子メール メッセージを検出したときの処理方法が指定されます。
	[署名付きのコンテンツ]	電子的に情報を送信すると、意図的かどうかにかかわらず、情報が変更される可能性があります。 この解決策として、一部のメール ソフトウェアでは電子署名 (手書きの署名を電子形態にしたもの) が使用されます。 電子署名は送信者のメッセージに追加される情報で、送信者とメッセージ内の情報の識別と認証を行う機能があります。電子署名は暗号化され、データ固有のサマリー情報のように機能します。通常は、受信した電子メール メッセージの末尾に、文字と数字が長く羅列されます。その後、電子メール ソフトウェアによって送信者のメッセージに含まれた情報が再検査され、電子署名が作成されます。作成した署名が元の署名と同じ場合、データは変更されていません。 電子メール メッセージにウイルスや不良コンテンツが含まれている場合や、電子メール メッセージが大き過ぎる場合、ソフトウェアによってメッセージの一部が駆除または削除される場合があります。電子メール メッセージは有効で、読むこともできますが、元の電子署名は「壊れて」います。電子メール メッセージの内容は他の方法で変更されている可能性もあるため、受信者はその内容を信じることはできません。
	[破損したコンテンツ]	メールのコンテンツが破損している場合があります。この場合、メールのコンテンツはスキャンできません。 破損したコンテンツのポリシーによって、破損したコンテンツを含む電子メール メッセージを検出したときの処理方法が指定されます。
	[サービス拒否]	コンピューター、サーバー、ネットワークに対する攻撃方法の一つです。攻撃には意図的なものと指示コードの副産物による偶然のものがあります。経路としては、個別のネットワーク経由、インターネットに接続したシステム経由、ホストからの直接攻撃、の 3 種類があります。 この攻撃は、攻撃対象を無効化またはシャットダウンし、正当な接続要求に対する応答を妨害します。 サービス拒否攻撃では、正規の要求に応答できないように、攻撃対象に対して偽の接続要求を大量に送信します。
	[保護されたコンテンツ]	メールのコンテンツが保護されている場合があります。この場合、メールのコンテンツはスキャンできません。 保護されたコンテンツのポリシーによって、保護されたコンテンツを含む電子メール メッセージを検出したときの処理方法が指定されます。
	[パスワードで保護されたファイル]	メールで送信するファイルはパスワードで保護できます。 パスワードで保護されたファイルはスキャンできません。 パスワードで保護されたファイルのポリシーによって、パスワードで保護されたファイルを含む電子メール メッセージの処理方法が指定されます。

表 2-2 検出定義 *(続き)*

カテゴリ	追加情報	説明
	[不完全な MIME メッセージ]	MIME (Multipurpose Internet Mail Extensions) は、7 ビットの ASCII 文字にのみ対応している SMTP などのプロトコルで ASCII 以外の文字の転送を可能にする通信規格です。 MIME では、非 ASCII 形式をエンコードするためのさまざまな方法が定義されています。したがって、非 ASCII 形式を、7 ビット ASCII 文字セットの文字を使用して表すことができます。 MIME メッセージの本文の内容が大きすぎてメール転送システム経由で渡すことができない場合、その本文を複数の小さな MIME メッセージとして渡すことができます。 この MIME メッセージは「分割または不完全な MIME メッセージ」として知られています。各 MIME メッセージには転送に必要なメッセージの断片のみが含まれるためです。
[メール URL レピュテーション]	[検出された URL]	URL レピュテーションで検出されたメールに含まれる不審な URL。

ソフトウェア更新のスケジュールを設定する

自動更新のスケジュールを設定し、最新のウイルス対策 DAT、ウイルス対策エンジン、エクストラ ドライバー、およびスパム対策エンジンを含めソフトウェアを最新の状態に保ちます。

デフォルトでは、[SiteList エディター] で指定したリポジトリ設定に基づいて製品の更新が実行されます。 リポジトリ設定を変更するには、[スタート] 、 [すべてのプログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] の順に移動し、[SiteList エディター] を選択します。 ただし、ご使用のコンピューターが ePolicy Orchestrator サーバーによって管理される場合、製品の更新は ePolicy Orchestrator の設定に基づいて実行されます。

タスク

1 [ダッシュボード] 、 [統計と情報] の順にクリックします。

2 [バージョンと更新] セクションで、[更新情報] タブをクリックします。

3 [更新の頻度] で、[スケジュールの編集] をクリックします。

[スケジュールの編集] ページが表示されます。

4 [時間を選択] で、必要なソフトウェア更新頻度に応じてオプションを選択します。

ベスト プラクティスとしては、[日] を選択して [日][ごと] テキスト ボックスで `1` を指定し、毎日の更新スケジュールを設定します。 営業時間以外やネットワーク トラフィックが少ないときにソフトウェア更新を実行します。

5 [保存] をクリックし、[適用] をクリックします。

これで、ソフトウェア更新のスケジュールを正常に設定できました。

オンデマンド スキャンとそのビュー

オンデマンド スキャナーは、好きな時や定期的に手動で開始するセキュリティ スキャナーです。各種構成を設定したり、特定のメールやメールボックスをスキャンしたりすることができます。

MSME では、定期オンデマンド スキャンを作成できます。複数のスケジュールを作成して、各スケジュールを設定された間隔または時間に自動的に実行することができます。

サーバーの負荷が低い時間帯や業務に影響を与えない時間帯に通常のスキャンが実行されるよう、スケジュールを設定することができます。

この機能を使用できるのは、メールボックスの役割を有する Exchange サーバー上に限られます。エッジ トランスポートまたはハブ トランスポートの役割しか有しない Exchange サーバーでは、オンデマンド スキャンのスケジュールを設定できません。

オンデマンド スキャンの実行に最適な時間帯

悪意のあるアクティビティによって組織内で停止が起こった場合には、オンデマンド スキャンの実行を強くお勧めできます。これによって、停止中に Microsoft Exchange データベースがクリーンで感染されていないことが確認されます。

McAfee では、営業時間以外にオンデマンド スキャン タスクを実行することをお勧めします。オンデマンド スキャン タスクの実行スケジュールを営業時間外に設定したものの、ピーク業務時間中にも実行が継続する場合は、スキャン中のデータベースを見直し、スキャン中のデータを変更して代替スケジュールを用いて作成する必要があります。

Exchange データベースがクリーンで、古い電子メールも最新のウイルス対策シグネチャによってスキャンされることを確実に行うため、オンデマンド スキャンは週末に実行するようにスケジュールを設定できます。管理者は、Exchange サーバー、データベース、およびメール フローの数を考慮してオンデマンド スキャンのスケジュールを設定する必要があります。営業時間前にこのタスクが必ず完了させることが目標となります。

オンデマンド スキャンを行う理由

オンデマンド スキャンを実行する理由にはさまざまなものがあります。以下に例を挙げます。

- アップロードまたはパブリッシュされた特定ファイルをチェックする。
- 新しいウイルスを検出できるように、DAT 更新の後で、Microsoft Exchange サーバ内のメッセージにウイルスがないかを確認する。
- ウイルスを検出して駆除した後、コンピュータが完全にクリーンであるかどうかを確認する場合。

オンデマンド スキャン タスクの表示

MSME 用に構成されたオンデマンド スキャン タスクのリストを表示します。

タスク

- [ダッシュボード] 、[オンデマンド スキャン] の順にクリックします。 [オンデマンド スキャン] ページが開き、設定済みのオンデマンド スキャン タスクが表示されます。

  デフォルトでは、MSME のインストール時に [Default Scan] という名前のスケジュール タスクが作成されます。

  [オンデマンド スキャン] ページでは、以下のオプションを使用できます。

表 2-3 オプションの定義

オプション	定義
[氏名]	オンデマンド スキャン タスクの名前を示します。
[ステータス]	オンデマンド スキャン タスクの現在のステータスが [アイドル状態]、[実行中]、[停止] または [完了] のどれであるかを示します。
[前回の実行日]	オンデマンド スキャンが最後に実行された日時を示します。
[次の実行日]	次のオンデマンド スキャンが実行されるようにスケジュールで設定されている日時を示します。
[アクション]	オンデマンド スキャン タスクで使用可能なすべてのオプションが表示されます。 • [変更] • [削除] • [今すぐ実行] • [状態の表示] [停止] オプションが表示されるのは、任意のオンデマンド スキャン タスクが実行中の場合に限られます。
[変更]	オンデマンド スキャン タスクの設定を編集します。
[削除]	選択したオンデマンド スキャン タスクを削除します。
[今すぐ実行]	選択したオンデマンド スキャン タスクをすぐに開始します。 [今すぐ実行] は、スケジュールを設定していないオンデマンド スキャン タスクを作成し、適用した場合にのみ実行できます。
[状態の表示]	オンデマンド スキャン タスクの現在のステータスが表示されます。[タスク ステータス] ページには以下のタブが表示されます。 • [全般]ータスクの合計実行回数、タスクの進行状況、スキャン用の DAT とエンジン バージョン、スキャン結果、スキャンされた合計アイテム数、破られたルール、およびスキャンされたフォルダーなどのオンデマンド スキャン タスクに関する詳細情報が表示されます。 • [設定]ースキャンされたデータベースと使用されたポリシーに関する詳細情報が表示されます。 [状態の表示] オプションを使用できるのは、オンデマンド スキャン タスクの開始後に限られます。
[停止]	実行中のオンデマンド スキャン タスクを停止します。
[更新]	ページを最新のオンデマンド スキャン情報に更新します。
[新規スキャン]	新しいオンデマンド スキャン タスクのスケジュールを設定します。

これで、MSME 用に構成されたすべての使用可能なオンデマンド スキャン タスクが正常に表示されました。

オンデマンド スキャン タスクを作成する

オンデマンド スキャン タスクのスケジュールを設定し、好みの間隔でメールボックス内のウイルスや禁止されたコンテンツを検出したり削除したりします。

開始する前に

製品のインストール時に作成された [MSMEODuser] は、Active Directory から絶対に削除しないでください。メールボックスでオンデマンド スキャンを実行するためには、このユーザーが必要になります。

タスク

1 [ダッシュボード] 、[オンデマンド スキャン] の順にクリックします。 [オンデマンド スキャン] ページが表示されます。

2 [新規スキャン] をクリックします。[スキャン実行時を選択] ページが表示されます。

3 [時間を選択] タブでスキャンの実行時間を指定します。 使用可能なオプションは次のとおりです。

- [スケジュールなし]−オンデマンド スキャンの実行時刻を決めていない場合や、既存のオンデマンド スキャンのスケジュールを無効にする場合にこのオプションを選択します。
- [1 回だけ]−オンデマンド スキャンを 1 回行うスケジュールの日時を指定します。
- [時間] − オンデマンド スキャン タスクを 1 日に複数回実行する必要がある場合、このオプションを選択して時間単位でタスクのスケジュールを設定します。 たとえば、現在の時刻が 14 時で、以下の条件を満たすオンデマンド スキャン タスクを作成する必要があるとします。
  - オンデマンド スキャンを 14 時 30 分ジャストに開始する必要がある
  - オンデマンド スキャンを 1 日に 2 回実行する必要がある

  上記のタスクを実現するには、時間に `12` を、分に `30` を指定します。
- [日] − 1 週間に実行するスキャンの回数に従ってタスクのスケジュールを設定する場合に選択します。 たとえば、オンデマンド スキャンを 3 日に 1 回実行する場合には、[日] で `3` を指定し、タスクの開始時刻を選択します。
- [週] − 1 か月に実行するスキャンの回数に従ってタスクのスケジュールを設定する場合に選択します。 たとえば、オンデマンド スキャンを 2 週間に 1 回実行する場合には、[週] で `2` を指定し、タスクを開始する曜日と時刻を選択します。
- [月] − 1 年間に実行するスキャンの回数に従ってタスクのスケジュールを設定する場合に選択します。 たとえば、オンデマンド スキャンを毎月第 2 土曜日に実行する場合、[指定週] ドロップダウン リストから [第 2] を選択し、[指定曜日] ドロップダウン リストから [土曜日] を選択して、タスクを開始するすべての月と時刻を選択します。

> 指定時間を過ぎたときにオンデマンド スキャン タスクを停止するには、[次の時間を超えたらタスクを停止する]: <n> [時間] <n> [分] を有効にします。

4 [次へ] をクリックします。 [スキャン対象の選択] ページが表示されます。 使用可能なオプションは次のとおりです。

- [すべてのフォルダーをスキャン]−Exchange サーバーのすべてのメールボックスをスキャンする場合はこのオプションを選択します。
- [選択したフォルダーをスキャン]−Exchange サーバーの指定したメールボックスのみをスキャンする場合はこのオプションを選択します。
- [選択したフォルダー以外のすべてのフォルダーをスキャン]−[スキャンするフォルダー] リストに追加される特定のメールボックスを除き、すべてのフォルダーをスキャンする場合はこのオプションを選択します。

> Microsoft Exchange 2013 と 2016 の場合、パブリック フォルダーはメールボックスの一部として表示されます。 オンデマンド スキャンは、パブリック フォルダーに再帰的に実行されます。 Microsoft Exchange 2010 の場合、オンデマンド スキャンを再帰的に実行するパブリック フォルダーをフォルダーまたはサブフォルダー レベルで選択できます。

5 [次へ] をクリックします。[スキャン設定の構成] ページが表示されます。

6 [使用するポリシー] ドロップダウン リストで、ユーザーのスキャン要件に基づいて任意のポリシー オプションを選択します。

ポリシー	説明
[デフォルト]	すべてのスキャナーおよびフィルターのデフォルト設定 (ただし、以下のスキャナーを除く)。 • [DLP とコンプライアンス スキャナー] • [ファイル フィルタリング]
[ウイルスの検出]	ウイルス対策設定およびフィルター。 このポリシーは、データベース内のウイルス性コンテンツを簡単にチェックする手段となります。
[ウイルスの駆除]	ウイルス対策設定およびフィルター。 このポリシーは、データベース内のウイルス性コンテンツを簡単に削除する手段となります。
[非対応コンテンツの検索]	コンテンツ スキャン設定。 これらのポリシーは、新たに作成または割り当てられたコンテンツ スキャン ルールの効果を確認する場合に便利です。
[非対応コンテンツの削除]	コンテンツ スキャン設定。 このポリシーは、新たに作成または割り当てられたコンテンツ スキャン ルールの効果を確認して、非対応コンテンツを削除する場合に便利です。
[フル スキャン]	すべてのスキャナーおよびフィルターの設定。 これらのポリシーは通常、定期的なスキャンに使用されます。

設定および実行するアクションは、[ポリシー マネージャー] に表示されるオンデマンド ポリシーで指定されます。

7 複数のセッションでメールボックス データベースにオンデマンド スキャン タスクを実行するには、[再開可能なスキャン] と [最後の項目から再開] オプションを選択します。

すべてのメールボックスにオンデマンド スキャン タスクを実行する場合もあります。 1 つのセッションですべてのメールボックスをスキャンすると、処理時間が長くなり、システムの生産性が低下する場合があります。 1 つのセッションですべてのメールボックスをスキャンするのではなく、複数のセッションでスキャンを実行するようにスケジュールを設定できます。

8 Exchange Server では、詳細なオンデマンド スキャン タスクを実行するオプションを使用できます。 以下のフィールドを使用してスキャンを絞り込むことができます。

- 件名
- 送信元
- 宛先
- メッセージ ID
- 受信者
- 日付の範囲
- メール サイズ
- 添付ファイル
- 未読アイテム

詳細なオンデマンド スキャンを実行すると、時間の節約になることはもちろん、特定のスキャン結果を取得できます。

9 [次へ] をクリックします。[スキャン名の入力] ページが表示されます。

10 前のページで選択したポリシーに基づき、分かりやすいオンデマンド スキャン タスク名を指定します。例えば、週末にフル スキャンを実行するオンデマンド スキャン タスクを作成する場合、週末フル スキャン のようにタスク名を指定します。

11 [完了]、[適用] の順にクリックします。

上記の手順を実行し、オンデマンド スキャン タスクを正常に作成できました。

ステータス レポート

ステータス レポートは、管理者に定期的に送信される、スケジュール設定されたレポートです。このレポートには、特定の期間内の検出統計情報が含まれています。

[ステータス レポート] を使用すると、定期的に統計情報にクエリーを実行するタスクを自動化できます。特定の日付の検出数などの簡単な統計情報を収集するための定期タスクのスケジュールを設定したり、Exchange 管理者や送信先リストに電子メールを送信したりすることができます。

こうしたレポートでは、脅威の状況を解消するにはどのメカニズムを用意できるかを考え、どの Exchange サーバーがより多くの脅威を受信しているかを見分ける際に役立ちます。

時間、受信者の電子メール アドレスまたはレポートの送信先の配布リスト、および電子メールの件名を選択することができます。ステータス レポートは、HTML または CSV 形式で送信されます。

構成に基づき、ステータス レポート電子メールには、ウイルス、スパム、フィッシング詐欺、IP レピュテーション、PUP、禁止されたファイル タイプ、好ましくないコンテンツ、DLP とコンプライアンス、駆除電子メールおよびスキャンされた合計電子メール数などの検出アイテムに関する統計情報が記載されます。ステータス レポートのスケジュール設定方法に関する詳細については、『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。

MSME のインストール後、通知電子メールに統計情報を設定するには、ステータス レポートの間隔を少なくとも 24 時間空ける必要があります。

ステータス レポート タスクの表示

MSME 用に構成されたステータス レポート タスクのリストを表示します。

タスク

- [ダッシュボード] 、[ステータス レポート] の順にクリックします。 [ステータス レポート] ページが表示され、設定済みの構成レポート タスクがリストで表示されます。

  [ステータス レポート] ページでは、以下のオプションを使用できます。

表 2-4 オプションの定義

オプション	定義
[名前]	レポート タスクの名前を示します。
[ステータス]	タスクが [アイドル状態]、[実行中]、[停止] または [完了] のいずれかのレポート タスクのステータスを示します。
[前回の実行日]	レポート タスクが最後に実行された日時を示します。
[次の実行日]	次のレポート タスクが実行されるようにスケジュールで設定されている日時を示します。

表 2-4 オプションの定義 *(続き)*

オプション	定義
[アクション]	使用可能なすべてのレポート タスクに関する以下のオプションがリストで表示されます。 • [変更] • [削除] • [今すぐ実行] • [状態の表示] [停止] オプションが表示されるのは、任意のレポート タスクが実行中の場合に限られます。
[変更]	オンデマンド スキャン タスクの設定を編集するには、[変更] をクリックします。
[削除]	選択したレポート タスクが削除されます。
[今すぐ実行]	選択したレポート タスクがすぐに開始されます。
[状態の表示]	レポート タスクの状態が表示されます。 [タスク ステータス] ページには以下のタブが表示されます。 • [全般]ー開始および終了時間、タスク実行、現在のアクション、およびタスクの進行状況などのレポート タスクに関する詳細情報が表示されます。 [状態の表示] オプションを使用できるのは、レポート タスクの開始後に限られます。
[最新の状態に更新]	ページを最新のレポート情報に更新します。
[新しいレポート]	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。

これで、MSME 用に構成されたすべての使用可能なステータス レポート タスクが正常に表示されました。

新しいステータス レポートのスケジュール設定

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、好みの間隔で検出統計情報を特定の電子メール アドレスや配布リストに送信します。

タスク

1 [ダッシュボード] 、 [ステータス レポート] の順にクリックします。[ステータス レポート] ページが表示されます。

2 [新規レポート] をクリックします。[レポート] ページが表示されます。

3 [レポート時刻] タブで、ステータス レポート タスクの実行時刻を指定します。使用可能なオプションは次のとおりです。

- [スケジュールなし]ーステータス レポート タスクの実行時刻を決めていない場合や、既存のステータス レポート タスクのスケジュールを無効にする場合にこのオプションを選択します。
- [1 回だけ]ーステータス レポート タスクを 1 回行うスケジュールの日時を指定します。

- [時間]－ステータス レポート タスクを 1 日に複数回実行する必要がある場合は、このオプションを選択して時間単位でタスクのスケジュールを設定します。例えば、現在の時刻が 14 時で、以下の条件を満たすレポート タスクを作成する必要があると仮定します。
  - ステータス レポート タスクを 14 時 30 分ジャストに開始する必要がある
  - ステータス レポート タスクを 1 日に 2 回実行する必要がある

  上記のタスクを実現するには、時間に `12` を、分に `30` を指定します。
- [日]－1 週間に実行する必要があるステータス レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、ステータス レポート タスクを 3 日に 1 回実行する場合は、[日] で `3` を指定し、タスクの開始時刻を選択します。
- [週]－1 か月に実行する必要があるステータス レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、ステータス レポート タスクを 2 週間に 1 回実行する場合は、[週] で `2` を指定し、タスクの開始曜日と時刻を選択します。
- [月]－1 年に実行する必要があるステータス レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、ステータス レポート タスクを毎月第 2 土曜日に実行する場合は、[On the（指定週）] ドロップダウン リストから [second（第 2）] を、[of（指定曜日）] ドロップダウン リストから [Saturday（土曜日）] を選択し、タスクを開始するすべての月と時刻を選択します。

> 指定時間を超える場合にステータス レポート タスクを停止するには、[分を超えたらタスクを停止する] <n> [時間] <n> [分] を有効にします。

4 [次へ] をクリックします。[レポートの設定] ページが表示されます。使用可能なオプションは次のとおりです。

表 2-5 オプションの定義

オプション	定義
[受信者の電子メール]	受信者の電子メール アドレスまたは配布リストの SMTP アドレスを指定します。大半の場合、これは Exchange 管理者の電子メール アドレスになるはずです。 デフォルトでは、[設定と診断] 、[通知] 、[設定] 、[全般] 、[管理者の電子メール] からの電子メール アドレスが受信者の電子メール アドレスとして使用されます。
[レポートの件名]	電子メールに分かりやすい件名を指定します。例えば、HTML 形式の日次ステータス レポートなら、`MSME 日次ステータス レポート（HTML）` のように指定します。
[行数]	ステータス レポート電子メールに表示する行数（n）を指定します。ステータス レポートの各行には、特定の日付の検出総数が表示されます。このレポートには、ステータス レポートがトリガーされた日を除く、最近（n）日間の検出数が記載されます。例えば、`1` を指定すると、ステータス レポートには昨日の検出数を表示する行が 1 つ記載されます。 指定できる最大値は 365 です。
[レポートの種類]	受信者へ送信されるステータス レポートの形式を指定します。使用可能なオプションは次のとおりです。 • [CSV]－カンマ区切りの値形式で `.csv` 添付ファイルとしてステータス レポートを受信者に送信する場合は、このオプションを選択します。 • [HTML]－ステータス レポートを HTML 形式の .html 添付ファイルで受信者に送信するか、または電子メール メッセージの本文に HTML 形式で表示する場合は、このオプションを選択します。

5 [次へ] をクリックします。[タスク名を入力してください] ページが表示されます。

6 前のページで選択したスケジュールと形式に基づき、分かりやすいステータス レポート タスク名を指定します。例えば、月曜日から金曜日までの検出統計情報を提供する HTML 形式の週次ステータス レポート タスクなら、週次ステータス レポート（HTML） というタスク名を指定します。

7 [完了]、[適用] の順にクリックします。

上記の手順を実行し、新しいステータス レポート タスクを正常に作成できました。

ステータス レポートの電子メール通知

スケジュール設定したステータス レポートに基づき、受信者は指定期間中に MSME によってスキャンされ検出されたすべての電子メールに関する統計情報が記載された電子メールを受信します。

ステータス レポート設定に基づき、ステータス レポート電子メールには、検出されたアイテム、合計駆除電子メール数、およびその日にスキャンされた電子メールの総数に関する統計情報が記載されます。

表 2-6 オプションの定義

オプション	定義
[送信元]	[設定と診断] 、[通知] 、[設定] 、[全般] 、[送信者の電子メール] の順に移動して指定した電子メール アドレスが表示されます。
[宛先]	[設定と診断] 、[通知] 、[設定] 、[全般] 、[管理者の電子メール] の順に移動して指定した目的の受信者の電子メール アドレスが表示されます。
[件名]	[ダッシュボード] 、[ステータス レポート] 、[レポート設定] 、[レポートの件名] の順に移動して指定したステータス レポートの電子メール通知の件名が表示されます。
[サーバーのスキャン統計]	MSME のインストール場所の [コンピューター名] が表示されます。
[日付]	日付が MM/DD/YYYY 形式で表示されます。
[検出]	メッセージ本文の [ウイルス]、[スパム]、[フィッシング詐欺]、[IP レピュテーション]、[不審なプログラム]、[禁止されたファイル タイプ]、[好ましくないコンテンツ]、および [DLP とコンプライアンス] の検出統計情報が表示されます。 [スパム]、[フィッシング詐欺]、[IP レピュテーション] の統計を使用できるのは、McAfee Anti-Spam アドオンをインストール済みの場合に限られます。
[駆除]	MSME によってクリーンとして検出され、脅威の原因にはならなかったクリーンな電子メールの合計数が表示されます。 たとえば、管理者に送信されたステータス レポート電子メールは、クリーン電子メールとして統計にカウントされます。
[スキャン済みの合計]	その日に MSME によってスキャンされた電子メールの合計数が表示されます。

[設定と診断] 、[スパム対策] 、[McAfee GTI IP レピュテーション] の順に移動して、[IP レピュテーションしきい値] に [信頼できる IP (0 未満)] または [中立 IP (0 以上)] を設定した場合、ステータス レポート メールがブロックされます。

構成レポート

構成レポートは、特定の時刻に管理者に送信されるようにスケジュールされたレポートです。 このレポートには、MSME 製品情報、ポリシー設定、システム情報が記載されます。

[構成レポート] を使用すると、製品構成のサマリーを定期的に表示するタスクを自動化できます。

この機能は、組織内の複数の管理者が MSME の構成を追跡する場合に役立ちます。 また、複数の MSME を ePolicy Orchestrator で管理し、製品構成を追跡する場合にも有効です。

時間、受信者の電子メール アドレスまたはレポートの送信先の配布リスト、電子メールの件名を選択できます。

構成に基づき、構成レポートには、サーバー情報、製品バージョン情報、製品ライセンスのステータスと種類、ホットフィックス情報、デバッグのログ情報、オンアクセス スキャナー設定、オンアクセス ポリシー設定、ゲートウェイ ポリシー設定などの製品およびシステム情報が記載されます。構成レポートのスケジュール設定方法に関する詳細については、「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。

構成レポート タスクの表示

MSME 用に構成された構成レポート タスクのリストを表示します。

タスク

- [ダッシュボード] 、 [構成レポート] の順にクリックします。 [構成レポート] ページが表示され、設定済みの構成レポート タスクがリストで表示されます。

  [構成レポート] ページでは、以下のオプションを使用できます。

表 2-7 オプションの定義

オプション	定義
[名前]	レポート タスクの名前を示します。
[ステータス]	タスクが [アイドル状態]、[実行中]、[停止] または [完了] のいずれかのレポート タスクのステータスを示します。
[前回の実行日]	レポート タスクが最後に実行された日時を示します。
[次の実行日]	次のレポート タスクが実行されるようにスケジュールで設定されている日時を示します。
[アクション]	使用可能なすべてのレポート タスクに関する以下のオプションがリストで表示されます。 • [変更] • [削除] • [今すぐ実行] • [状態の表示] [停止] オプションが表示されるのは、任意のレポート タスクが実行中の場合に限られます。
[変更]	オンデマンド スキャン タスクの設定を編集するには、[変更] をクリックします。
[削除]	選択したレポート タスクが削除されます。
[今すぐ実行]	選択したレポート タスクがすぐに開始されます。
[状態の表示]	レポート タスクの状態が表示されます。 [タスク ステータス] ページには以下のタブが表示されます。 • [全般]ー開始および終了時間、タスク実行、現在のアクション、およびタスクの進行状況などのレポート タスクに関する詳細情報が表示されます。 [状態の表示] オプションを使用できるのは、レポート タスクの開始後に限られます。
[最新の状態に更新]	ページを最新のレポート情報に更新します。
[新しいレポート]	新しい構成レポート タスクのスケジュールを設定します。

これで、MSME 用に構成されたすべての使用可能な構成レポート タスクが正常に表示されました。

新しい構成レポートのスケジュール設定

新しい構成レポート タスクのスケジュールを設定し、好みの間隔で製品構成やシステム情報を特定の電子メール アドレスや配布リストに送信します。

タスク

1 [ダッシュボード] 、 [構成レポート] の順にクリックします。[構成レポート] ページが表示されます。

2 [新規レポート] をクリックします。[レポート] ページが表示されます。

3 [レポート時刻] タブで、構成レポート タスクの実行時刻を指定します。使用可能なオプションは次のとおりです。

- [スケジュールなし]ー構成レポート タスクの実行時刻を決めていない場合や、既存の構成レポート タスクのスケジュールを無効にする場合にこのオプションを選択します。
- [1 回だけ]ー構成レポート タスクを 1 回行うスケジュールの日時を指定します。
- [時間]ー構成レポート タスクを 1 日に複数回実行する必要がある場合は、このオプションを選択して時間単位でタスクのスケジュールを設定します。例えば、現在の時刻が 14 時で、以下の条件を満たすレポート タスクを作成する必要があると仮定します。
  - 構成レポート タスクを 14 時 30 分ジャストに開始する必要がある
  - 構成レポート タスクを 1 日に 2 回実行する必要がある

  上記のタスクを実現するには、時間に `12` を、分に `30` を指定します。
- [日]ー1 週間に実行する必要がある構成レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、構成レポート タスクを 3 日に 1 回実行する場合は、[日] で `3` を指定し、タスクの開始時刻を選択します。
- [週]ー1 か月に実行する必要がある構成レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、構成レポート タスクを 2 週間に 1 回実行する場合は、[週] で `2` を指定し、タスクの開始曜日と時刻を選択します。
- [月]ー1 年に実行する必要がある構成レポート タスクの回数に基づき、タスクのスケジュールを設定する場合はこのオプションを選択します。例えば、構成レポート タスクを毎月第 2 土曜日に実行する場合は、[On the（指定週）] ドロップダウン リストから [second（第 2）] を、[of（指定曜日）] ドロップダウン リストから [Saturday（土曜日）] を選択し、タスクを開始するすべての月と時刻を選択します。

> 指定時間を超える場合に構成レポート タスクを停止するには、[分を超えたらタスクを停止する] <n> [時間] <n> [分] を有効にします。

4 [次へ] をクリックします。[レポートの設定] ページが表示されます。使用可能なオプションは次のとおりです。

表 2-8 オプションの定義

オプション	定義
[受信者の電子メール]	受信者の電子メール アドレスまたは配布リストの SMTP アドレスを指定します。大半の場合、これは Exchange 管理者の電子メール アドレスになるはずです。 デフォルトでは、[設定と診断] 、 [通知] 、 [設定] 、 [全般] 、 [管理者の電子メール] からの電子メール アドレスが受信者の電子メール アドレスとして使用されます。
[レポートの件名]	電子メールに分かりやすい件名を指定します。例えば、週次構成レポートなら `MSME` 週次構成レポート のように指定します。

5 [次へ] をクリックします。[タスク名を入力してください] ページが表示されます。

6 前のページで選択したスケジュールと形式に基づき、分かりやすい構成レポート タスク名を指定します。例えば、毎月第 1 月曜日に製品とシステムの情報を提供する月次構成レポート タスクを作成する場合は、タスク名を 月次構成レポート（第 1 月曜日） のように指定します。

7 [完了]、[適用] の順にクリックします。

上記の手順を実行し、新しい構成レポート タスクを正常に作成できました。

構成レポートの電子メール通知

スケジュール設定した構成レポートに基づき、受信者は指定期間の MSME 製品情報、ポリシー設定、およびシステム情報が記載された電子メールを受信します。

表 2-9 オプションの定義

オプション	定義
[サーバー情報]	コンピューター名、IP アドレス、および Exchange バージョンなどのサーバー情報が表示されます。
[バージョン情報]	製品バージョン、DAT バージョンと日付、エンジン バージョン、スパム対策ルール、およびエンジン情報（ある場合）などの MSME 情報が表示されます。
[ライセンス ステータス]	MSME およびスパム対策アドオン コンポーネントのライセンス タイプなどの製品ライセンス情報が表示されます。
[製品情報]	サービス パックまたはホットフィックスがインストールされているかどうかに関する追加製品情報が表示されます。
[デバッグのログ]	レベル、ログ ファイルの最大サイズ、およびファイルの場所などの [デバッグのログ] 情報が表示されます。
[オンアクセスの設定]	どの設定が有効または無効であるかを指定する現在の [オンアクセスの設定] が表示されます。
[オンアクセス ポリシー]	[オンアクセス] [マスター ポリシー] に有効化されたコア スキャナーおよびフィルターが表示されます。
[ゲートウェイ ポリシー]	[ゲートウェイ] 、[マスター ポリシー] のスパム対策およびフィッシング対策スキャナーの現在のステータスが表示されます。 このオプションを適用できるのは、McAfee Anti-Spam アドオン コンポーネントがインストール済みの場合に限られます。

グラフィカル レポート

グラフィカル レポートを生成し、特定の期間中の脅威レベルを把握します。検出されたアイテムを [棒グラフ] または [円グラフ] 形式で分かりやすく表示できます。

ステータス レポートと共にこのようなレポートを使用すると、サーバーがより深刻な脅威に直面する場合にユーザーとその組織がそれを認識し、ユーザーが軽減プランを策定する際に役立ちます。

現在の脅威レベルのみを表示し、検出されたアイテムに何のアクションも実行する必要がない場合には、グラフィカル レポートを使用します。 [グラフィカル レポート] を使用すると、特定のフィルターに基づいてクエリーを実行し、さまざまな検出の [トップ 10] レポートを表示できます。

[グラフィカル レポート] は以下のとおりに分類されます。

- [簡易]ー日次または週次のトップ 10 レポートを表示するための限定検索フィルター。
- [詳細]ーさまざまなフィルター、時間範囲、およびチャート オプションに関するクエリーを実行するための詳細検索オプション。

簡易検索フィルターを使用したグラフィカル レポートの表示

曜日または週の簡易検索フィルターを使用して、検出に関するグラフィカル レポートを生成します。

タスク

1 [ダッシュボード] 、[グラフィカル レポート] の順にクリックします。[グラフィカル レポート] ページが表示されます。

2 [簡易] タブをクリックします。

3 [時間範囲] ドロップダウンリストから、[今日] または [今週] を選択して曜日または週の隔離済み検出を表示します。

4 [フィルター] ドロップダウン リストから、表示するレポートを選択します。 使用可能なオプションは次のとおりです。
   - [上位 10 個のウイルス]ー各検出数別にランク付けされた上位 10 個のウイルス名がリストで表示されます。
   - [上位 10 個のスパム検出]ースパム メッセージ数別にランク付けされた上位 10 個のスパム検出電子メールがリストで表示されます。
   - [上位 10 のスパム受信者]ー合計受信スパム メッセージ数別にランク付けされた上位 10 名のスパム受信者がリストで表示されます。
   - [上位 10 個のフィッシング メールの検出]ーフィッシング詐欺メッセージ数別にランク付けされた上位 10 個のフィッシング詐欺検出電子メールがリストで表示されます。
   - [トップ 10 ブロックされた IP アドレス]ー宛先不明の電子メールのブロック数別にランク付けされた上位 10 個のブロックされた IP アドレスがリストで表示されます。
   - [不審なプログラムの上位 10]ー脅威の可能性がある検出された不審なプログラムの上位 10 個がリストで表示されます。
   - [TIE 検出の上位 10 件] ー TIE で検出された潜在的な脅威の上位 10 件が表示されます。
   - [なりすまし検出の上位 10 件] ー 検出されたなりすましメールの上位 10 件が表示されます。
   - [トップ 10 DLP とコンプライアンス検出]ールールをトリガーした検出数別にランク付けされた上位 10 個のデータ損失保護とコンプライアンス規制違反がリストで表示されます。
   - [上位 10 個の感染ファイル] ー 各検出数別にランク付けされた上位 10 個のファイル名がリストで表示されます。
   - [ブロックされた URL のトップ 10] ー 脅威の可能性がある上位 10 個の URL が表示されます。
   - [検出数の上位 10]ー各検出数別にランク付けされた上位 10 個の検出がリストで表示されます。 このグラフには、上記のリストに表示されたウイルス、スパム検出、スパム受信者、フィッシング メールの検出、ブロックされた IP アドレス、不審なプログラム、不正な URL、DLP とコンプライアンス、および感染ファイルなどのすべてのカテゴリが含まれます。

5 [検索] をクリックします。 検索結果が、[結果の表示] ペインに表示されます。

   [拡大グラフ] で、ズーム率を選択すると [結果の表示] ペインでグラフ表示を拡大または縮小できます。

詳細検索フィルターを使用する

詳細検索フィルターを使用して検出に関するグラフィカル レポートを作成します。

タスク

1 [ダッシュボード] 、[グラフィカル レポート] の順にクリックします。 [グラフィカル レポート] ページが表示されます。

2 [詳細] タブをクリックします。

3 リストから 1 つ以上 3 つ以下のフィルターを選択します。

表 2-10 プライマリ フィルター

フィルタ	説明
[件名]	電子メールの「件名」を使用して検索します。
[受信者]	受信者の電子メール アドレスを使用して検索します。
[理由]	検出トリガーまたはアイテムの隔離理由で検索します。 [理由] フィルターを選択すると、セカンダリ フィルターが有効になり、検索条件を絞り込むことができます。 たとえば、[メール サイズ] ルールで隔離されたすべてのアイテムを検索できます。
[チケット番号]	チケット番号で検索します。 チケット番号は、検出ごとに自動的に生成される 16 桁の英数字エントリです。
[検出名]	検出アイテムを名前で検索します。
[スパム スコア]	スパム スコアを基準に検索します。 たとえば、[スパム スコア] が 3 で隔離されたすべてのアイテムを検索できます。

[スパム スコア] は、1 件のメールにスパムが潜む可能性を表す数字です。 エンジンによって、スキャンされる各メールにスパム対策ルールが適用されます。 各ルールは 1 つのスコアに関連付けられています。 スパム メールの可能性を評価するために、このスコアは合計され、そのメール全体のスパム スコアが算出されます。 総スパム スコアが高いほど、スパム メールのリスクが高くなります。 スパム スコアの範囲は、0 ～ 100 です。 受信メッセージのスパム スコアは 0 から始まります。メッセージがフィルターに違反するたびに、スパム スコアが加算されます。

セカンダリ フィルターを使用できるのは、[理由] フィルターのみです。 セカンダリ フィルターを指定しない場合には、フィールドを空白にしてください。これにより、すべての検出アイテムがクエリーの対象になります。

表 2-11 セカンダリ フィルター

フィルタ	説明
[ウイルス対策]	メッセージでウイルス感染の可能性が検出されたために隔離されたアイテムを検索します。
[DLP とコンプライアンス]	メッセージで禁止されたコンテンツが検出されたために隔離されたアイテムを検索します。 たとえば、不適切な単語などがあります。
[ファイル フィルター]	メッセージで禁止されたファイルが検出されたために隔離されたアイテムを検索します。
[スパム対策]	スパムが検出されたために隔離されたアイテムを検索します。 たとえば、チェーン メールなどがあります。
[IP レピュテーション]	IP レピュテーションが定義済みのしきい値を超えたために隔離されたアイテムを検索します。
[暗号化または破損]	メールで暗号化または破損したコンテンツが検出されたために隔離されたアイテムを検索します。
[不審なプログラム]	メールで不審なプログラムが検出されたために隔離されたアイテムを検索します。
[フィッシング詐欺]	メールでフィッシング詐欺コンテンツが検出されたために隔離されたアイテムを検索します。
[パッカー]	メールでパッカー (小型プログラム、圧縮された実行可能ファイル、暗号化コード) が検出されたために隔離されたアイテムを検索します。
[メール サイズ]	メール サイズが最大設定制限を超えたために隔離されたアイテムを検索します。
[暗号化]	メールで暗号化コンテンツが検出されたために隔離されたアイテムを検索します。
[署名付き]	メールで署名付きのコンテンツが検出されたために隔離されたアイテムを検索します。

表 2-11 セカンダリ フィルター *(続き)*

フィルタ	説明
[破損]	メールで破損したコンテンツが検出されたために隔離されたアイテムを検索します。
[サービス拒否]	サービス拒否攻撃の発生時に隔離されたアイテムを検索します。 たとえば、イベント中に隔離されたすべてのメールを検索する場合などがあります。
[保護されたコンテンツ]	保護されたコンテンツが検出され、コンテンツにアクセスできなかったために隔離されたアイテムを検索します。
[パスワード保護]	パスワードで保護されたコンテンツが検出され、コンテンツにアクセスできなかったために隔離されたアイテムを検索します。
[ブロックされた MIME]	メールでブロックされた MIME (Multipurpose Internet Mail Extension) が検出されたために隔離されたアイテムを検索します。
[URL レピュテーション]	URL レピュテーションが定義済みのしきい値を超えたために隔離されたアイテムを検索します。
[TIE レピュテーション]	TIE レピュテーションが定義済みのしきい値を超えたために隔離されたアイテムを検索します。
[SPF ソフト エラー]	メールで偽装コンテンツが検出されたために隔離されたアイテムを検索します。
[SPF ハード エラー]	メールで偽装コンテンツが検出されたために隔離されたアイテムを検索します。

検索フィルターの詳細については、『検索フィルター』を参照してください。

4 ドロップダウン リストから [すべての日付] または [日付の範囲] を選択します。

[すべての日付] を選択する場合、検出アイテムの隔離が始まった日付以降の検索結果が隔離データベースからクエリーによって返されます。 [日付の範囲], を選択する場合、[開始] および [終了] フィールドから**日付**、**月**、**年**、**時間**、**分** を選択し、クエリーによる日付の範囲内の検索を有効化します。

5 必要に応じて [棒グラフ] または [円グラフ] を選択します。

6 [円グラフ] を選択した場合は、ドロップダウン リストからフィルターを選択し、検索内容をさらに絞り込みます。

表 2-12 クエリー条件

フィルタ	説明
受信者	受信者の電子メール アドレスを使用して検索します。
送信者	送信者の電子メール アドレスを使用して検索します。
ファイル名	隔離されたファイル名を使用して検索します。
検出名	検出されたアイテムの名前を使用して検索します。
件名	電子メールの「件名」を使用して検索します。
理由	検出トリガーまたはアイテムが隔離された理由を使用して検索します。
ルール名	検出をトリガーしたルール名を使用して検索します。
ポリシー名	検出を実行したポリシー名を使用して検索します。

a [最大結果] で、表示する検索結果数を指定します。最高 99 件の検索結果を表示できますが、このフィールドを使用できるのは円グラフを選択した場合に限られます。

7 [検索] をクリックします。 検索結果が、[結果の表示] ペインに表示されます。 [拡大グラフ] で、ズーム率を選択すると [結果の表示] ペインでグラフ表示を拡大または縮小できます。検索結果は、結果の表示 ペインに表示されます。

3 検出アイテム

MSME によって検出および隔離された潜在的な脅威について記載したすべての電子メール メッセージに関する情報を表示します。 様々な検索フィルターを使用して検索条件を絞り込むと、必要な隔離アイテムを表示し、必要なアクションを隔離アイテムに実行することができます。

製品のユーザー インターフェースから、[検出されたアイテム] をクリックして隔離されたアイテムを検出カテゴリに基づいて表示します。検出カテゴリは以下のとおりです。

- [スパム]
- [IP レピュテーション]
- [フィッシング詐欺]
- [ウイルス]
- [TIE と ATD の検出]
- [なりすましメール]
- [不審なプログラム]
- [好ましくないコンテンツ]
- [禁止されたファイル タイプとメッセージ]
- [DLP とコンプライアンス]
- [メール URL レピュテーション]
- [すべての項目]

[スパム]、[フィッシング詐欺]、[SPF フィルター]、[IP レピュテーション] オプションを使用できるのは、McAfee Anti-Spam アドオンをインストール済みの場合に限られます。

目次

- *隔離データの管理*
- *検出タイプ*
- *使用可能なプライマリ検索フィルター*
- *検索フィルター比較表*
- *詳細検索オプション*
- *検出されたアイテムの検索*
- *隔離されたアイテムに対して実行可能なアクション*

隔離データの管理

ユーザーの要件に基づき、検出されたアイテムを隔離する場合に、ローカル データベースまたは専用隔離管理サーバー (McAfee Quarantine Manager) のどちらを使用するかを決定します。

デフォルトでは、検出されたアイテムは、MSME によってインストールされる PostgreSQL データベースにローカルで隔離されます。

隔離場所の構成

[検出されたアイテム] の構成設定に基づき、検出されたアイテムをローカル データベースで隔離するか、または McAfee の隔離管理ソフトウェア (McAfee Quarantine Manager) を使用して個別のサーバーで隔離するかを選択できます。

管理対象システムの場合、検出したアイテムを隔離する MQM サーバーを選択するときに、必要なシステムにだけ設定を施行してください。 この操作を行わないと、[システム ツリー] のすべての MSME サーバーに設定が適用されます。

製品のユーザー インターフェースで、[設定と診断] 、[検出されたアイテム] の順にクリックし、次の項目を選択します。

- [McAfee Quarantine Manager]ー MQM サーバーで検出アイテムを隔離します。
- [ローカル データベース] ー ローカル MSME サーバーの指定パスで検出アイテムを隔離します。

ローカル データベースと McAfee Quarantine Manager ー使用する状況

以下の表を参照すると、隔離管理にローカル データベースまたは McAfee Quarantine Manager を使用する状況を把握できます。

ローカル データベースを使用する場合...	McAfee Quarantine Manager を使用する場合...
1 つの MSME インストールの隔離されたアイテムを管理する場合。	複数の MSME インストールから隔離されたアイテムや、ユーザーの組織で構成された任意の MSME 製品を管理する場合。 • McAfee Security for Microsoft Exchange • McAfee Email and WebSecurity Appliance • McAfee Security for Lotus Domino (Windows) 上記の製品のいずれかを購入済みの場合は、McAfee Quarantine Manager を無料でダウンロードしてインストールできます。
アイテムの隔離に PostgreSQL データベースを使用する場合。	アイテムの隔離に MySQL または Microsoft SQL Server データベースを使用する場合。

McAfee Quarantine Manager とその機能の詳細については、製品マニュアルを参照してください。

検出タイプ

検出されたアイテムは、MSME によって脅威の可能性が認められた電子メール メッセージです。その種類には、ウイルス、スパム、フィッシング詐欺、非対応コンテンツや禁止されたファイル タイプなどがあります。

MSME で検出される脅威の種類は以下のとおりです。

検出タイプ	説明
[スパム]	不審な電子メッセージ。最も顕著な例を挙げると、未承諾広告メールです。 通常、スパムは受信を求めていない複数の受信者に対して送信されます。 電子メール スパム、インスタント メッセージ スパム、USENET ニュースグループ スパム、Web 検索エンジン スパム、ブログ スパム、携帯電話メッセージ スパムなど、種類は多岐に渡ります。 スパムには、正当な情報提供、誤解を招く情報提供、フィッシング詐欺メッセージなどがあり、受信者をだまして個人情報やカード/銀行情報を提出させるように設計されています。 ユーザーが電子メール メッセージを受信するよう登録している場合、その電子メール メッセージはスパムとみなされません。
[IP レピュテーション]	送信サーバーの IP アドレスに基づき、メッセージを検出する方法。 McAfee では、何十億もの IP アドレスとネットワーク ポートからデータを収集し、何百兆通りもの独特の見解を提供するとともに、ネットワーク トラフィック (ポート、送信先、プロトコル、送信/受信接続リクエストなど) に基づいてレピュテーション スコアを計算しています。 このスコアは [IP レピュテーション スコア] として知られており、ネットワーク接続で脅威が発生する確率が反映されます。 MSME では、ローカル ポリシーに基づいてアクションを決定するため、このスコアが使用されます。
[フィッシング詐欺]	銀行や合法的な企業などの信頼できる送信元から送信されたように見せかけるなりすましの電子メール メッセージを送信して、パスワード、社会保障番号、クレジット カード番号などの個人情報を不正に取得する方法。 通常、フィッシング電子メールでは、受信者に電子メール内のリンクをクリックさせて、連絡先の詳細やクレジット カード情報を確認させたり更新させたりします。 フィッシング詐欺電子メールもスパムと同様に、誰かが電子メール内の情報に反応して個人情報を開示することを期待して、大量の電子メール アドレスに送信されます。
[ウイルス]	ディスクや他のファイルに付着し、繰り返し自己複製するコンピューター プログラム ファイル。通常は、ユーザーが気付いたり、許可を与えることはありません。 一部のウイルスはファイルに付着するため、感染したファイルを実行するとウイルスも実行されてしまいます。 また、コンピューターのメモリーの中に潜み、コンピューターによってファイルが開かれたり、変更・作成されたりするとファイルが感染する仕組みのウイルスもあります。 ウイルスには症状を示すものもあれば、ファイルやコンピューター システムに損傷を与えるものもあります。いずれにしても、ウイルスを定義する場合に極めて重要になるのは、「害のないウイルスでもウイルスはウイルスに違いない」という考え方です。 隔離されたアイテムは [ウイルス] 検出カテゴリから [ダウンロード]、[解放]、[転送] または [表示] することはできません。
[TIE と ATD の検出]	DAT と McAfee GTI 以外に、McAfee Global Threat Intelligence と McAfee Advanced Threat Defense の強化された検出機能を使用できます。
[なりすましメール]	なりすましメールは、ユーザーを騙すためによく利用される手口です。攻撃者は、別の送信者のメール アドレスを悪用してメールを送信します。 偽物とは気付かずにメールを開いてしまい、返信してしまうユーザーも少なくありません。
[不審なプログラム]	合法的な企業のソフトウェア (マルウェア以外) でも、インストール先システムのセキュリティ状態またはプライバシー ポスチャを変えてしまう場合があります。 この種のソフトウェアにはスパイウェア、アドウェア、キーロガー、パスワード クラッカー、ハッカー ツール、ダイアラー アプリケーションが含まれている場合があり、ユーザーが必要とするプログラムと一緒にダウンロードされる可能性があります。 セキュリティ意識の高いユーザーであれば、この種のプログラムについてよく知っているため、場合によっては自分で削除することもあります。
[好ましくないコンテンツ]	これは、コンテンツ スキャン ルールをトリガーするすべてのコンテンツです。 嫌がらせや誹謗中傷、会社の機密情報が含まれていることもあります。 [好ましくないコンテンツ] は以下のように分類できます。 • [パッカー] • [暗号化されたコンテンツ] • [署名付きのコンテンツ] • [破損したコンテンツ] • [サービス拒否] • [保護されたコンテンツ] • [パスワードで保護されたファイル] • [不完全な MIME メッセージ]
[禁止されたファイル タイプとメッセージ]	特定の種類の添付ファイルは、ウイルスに感染しやすい傾向があります。 ファイル拡張子によって添付をブロックする機能は、メール システムの別の層のセキュリティです。 内部メールと外部メールの両方で、禁止されたファイル タイプやメッセージが含まれていないかどうかが検査されます。

検出タイプ	説明
[DLP とコンプライアンス]	電子メールによる機密情報の漏えいを止めます。 MSME では、業界第 1 位の電子メール コンテンツ分析を提供し、あらゆる形式の機密コンテンツを極めて厳密に調整することで、州、国、および海外の規制への準拠をサポートしています。 業界で最高の拡張性を持つ電子メール Data Loss Prevention (DLP) や、ポリシー ベースのメッセージ処理機能を使用してデータ漏えいを予防します。前者はパターン一致を実行してデータを検出するツールで、後者は送信データの損失を防ぐツールです。
[メール URL レピュテーション]	不要なリンク、フィッシング詐欺リンクまたはマルウェアを含む電子メールの配信を防ぎます。

[スパム]、[フィッシング詐欺]、[SPF フィルター]、[IP レピュテーション] オプションを使用できるのは、McAfee Anti-Spam アドオンをインストール済みの場合に限られます。

関連トピック:

45 ページの「*検索フィルター比較表*」
46 ページの「*詳細検索オプション*」

使用可能なプライマリ検索フィルター

検索フィルターを使用すると、検索条件を定義して隔離データベースからより効率的かつ効果的な検索を実行できます。

使用可能なプライマリ検索フィルター オプションは、選択した検出アイテムのカテゴリに応じて異なります。こうした検索フィルターは、検出されたアイテム カテゴリの [結果の表示] セクションに表示されます。

表示する検索フィルターを選択するには、[結果の表示] セクションの [表示するカラム] を使用します。

表 3-1 検出されたアイテム—プライマリ検索フィルター

検索フィルタ	定義
[実行されたアクション]	実行されたアクションでアイテムを検索します。 MSME によって実行されたアクションは、以下のとおりです。 • [駆除] • [駆除済み] • [削除済み] • [メッセージの削除] • [アクセス拒否] • [ログ済み] • [置換済み] • [拒否]
[スパム対策エンジン]	スパムやフィッシング詐欺攻撃がないかスキャンするスパム対策エンジンを基準にアイテムを検索します。 現在使用中の [スパム対策エンジン] を表示するには、[ダッシュボード] 、 [バージョンと更新] 、 [更新情報] 、[スパム対策エンジン	ルール バージョン] の順に移動します。 たとえば、[スパム対策エンジン] バージョンは 9286 のような形式で表示されます。
[スパム対策ルール]	数分ごとに更新されて、スパム メール送信者が送信した最新のスパム キャンペーンを捕捉するスパム対策ルールを基準にアイテムを検索します。 現在使用中の [スパム対策ルール] を表示するには、[ダッシュボード] 、 [バージョンと更新] 、 [更新情報] 、[スパム対策エンジン	ルール バージョン] の順に移動します。 たとえば、ルール バージョンは core:4373:streams:840082:uri:1245250 のような形式で表示されます。

表 3-1 検出されたアイテム－プライマリ検索フィルター *(続き)*

検索フィルタ	定義
[ウイルス対策 DAT]	特殊なシグネチャ付きのウイルス対策 DAT バージョンを基準にアイテムを検索します。 現在使用中の [ウイルス対策 DAT] を表示するには、[ダッシュボード] 、[バージョンと更新] 、[更新情報] 、[ウイルス対策エンジン	DAT バージョン	エクストラ ドライバー] の順に移動します。 たとえば、DAT バージョンは 6860.0000 のような形式で表示されます。
[ウイルス対策エンジン]	ウイルス/好ましくないコンテンツに固有の文字シーケンスが含まれていたウイルス対策エンジンを基準にアイテムを検索します。 現在使用中の [ウイルス対策エンジン] を表示するには、[ダッシュボード] 、[バージョンと更新] 、[更新情報] 、[ウイルス対策エンジン	DAT バージョン	エクストラ ドライバー] の順に移動します。 たとえば、[ウイルス対策エンジン] バージョンは 5400.1158 のような形式で表示されます。
[禁止する語句]	[ポリシー マネージャー] 、[共有リソース] 、[DLP とコンプライアンス ディクショナリ] の順に移動し、[DLP とコンプライアンス ルール] で、定義済みの禁止語句のコンテンツを検索します。
[検出名]	名前を基準に検出アイテムを検索します。
[ファイル名]	検出されたファイルの名前で、隔離されたアイテムを検索します。 [ファイル名] を表示するには、[ポリシー マネージャー] 、[共有リソース] 、[DLP とコンプライアンス] 、[ファイル フィルタリング ルール] の順に移動します。
[フォルダー]	ユーザーのメールボックスなどの隔離されたアイテムの保存場所のフォルダーを基準に検索します。 電子メールの隔離がオンアクセス（トランスポート）レベルで行われている場合は、フォルダーを使用できません。
[IP レピュテーション スコア]	送信者の [IP レピュテーション スコア] を基準にアイテムを検索します。 アイテムは [IP レピュテーションしきい値] に基づいて隔離されます。この値を設定するには、[設定と診断] 、 [Anti-Spam] 、[McAfee GTI IP レピュテーション] の順に移動します。 このフィルターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。
[ポリシー名]	[マスター ポリシー] やアイテムを検出したサブポリシーなどのポリシー名を基準にアイテムを検索します。
[理由]	検出された理由を基準にアイテムを検索します。基準は、[ウイルス対策]、[スパム対策]、[フィッシング詐欺対策]、[DLP とコンプライアンス] などのスキャナーやフィルターになります。
[理由]	特定の電子メールによってトリガーされたルールを基準に検索します。 アイテムが複数のスキャナーやフィルターをトリガーした場合など。 たとえば、スパム電子メールにウイルスが感染していた場合、[理由] は [スパム対策]、[ウイルス対策] になります。
[受信者]	受信者の電子メール アドレスを基準にアイテムを検索します。
[レピュテーション スコア]	利用可能な最新データ情報に基づいた電子メールのソースの信頼性レベルを基準に検索します。 アイテムは [メッセージ レピュテーションしきい値] に基づいて隔離されます。この値を設定するには、[設定と診断] 、 [Anti-Spam] 、 [McAfee GTI IP レピュテーション] の順に移動します。 このフィルターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。
[ルール名]	1 つ以上のスキャナー/フィルターをトリガーしたルールを基準にアイテムを検索します。スキャナー/フィルターをトリガーしたルールの基準は、各ポリシーに定義した [アクション] になります。
[スキャンの種類]	アイテムを検出したスキャナー名を基準にアイテムを検索します。
[送信者]	送信者の電子メール アドレスを基準にアイテムを検索します。

表 3-1 検出されたアイテム－プライマリ検索フィルター *(続き)*

検索フィルタ	定義
[送信者 IP]	送信者のシステムの IP アドレスを基準にアイテムを検索します。 アイテムは [IP レピュテーションしきい値] に基づいて隔離されます。この値を設定するには、[設定と診断] 、 [Anti-Spam] 、 [McAfee GTI IP レピュテーション] の順に移動します。 このフィルターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。
[サーバー]	コンピューター名を基準にアイテムを検索します。
[スパム スコア]	スパム スコアを基準にアイテムを検索します。スパム スコアとは、メール メッセージにスパムが潜む可能性を示す数字です。 エンジンによって、スキャンされる各メールにスパム対策ルールが適用されます。 各ルールは 1 つのスコアに関連付けられています。 電子メール メッセージにスパムが含まれている可能性を評価するために、このスコアは合計され、その電子メール メッセージの全体のスパム スコアが算出されます。総スパム スコアが高いほど、電子メール メッセージにスパムが含まれているリスクは高くなります。 このフィルターを使用できるのは、McAfee Anti-Spam アドオンがインストール済みの場合に限られます。
[状態]	現在のステータスを基準にアイテムを検索します。 使用可能なアイテムのステータスは、以下のとおりです。 • [未学習]－削除、リリース、または転送などが作用されないアイテム。すべてのアイテムの初期状態はこの [未学習] になります。 • [リリース済み]－隔離データベースからリリースされたアイテム。 • [Quarantine Manager キュー内] － 現在、McAfee Quarantine Manager データベースのキューに入っているアイテム。 • [転送済み]－目標受信者に転送されたアイテム。
[件名]	電子メール メッセージの件名を基準にアイテムを検索します。
[タスク]	オンアクセス (VSAPI)、オンアクセス (トランスポート) スキャン タスクまたはオンデマンド スキャン タスクいずれかのスキャン タスク名を基準にアイテムを検索します。 [結果の表示] セクションに表示されるオンアクセス スキャン タスクは、[設定と診断] 、[オンアクセスの設定] の順に移動して有効にした設定に基づきます。 オンデマンド スキャン タスクによって検出されたアイテムかどうかを識別するには、[ダッシュボード] 、 [オンデマンド スキャン] の順に移動します。
[チケット番号]	チケット番号を基準にアイテムを検索します。チケット番号とは、特定の検出に割り当てられ、通知として電子メールで配信される固有の英数字 ID です。関連付けられた検出の識別に役立ちます。
[TIE のスコア]	TIE スコアのレピュテーションに基づいて、アイテムを検索します。

[スパム]、[フィッシング詐欺]、[IP レピュテーション] 検出カテゴリに適用されるプライマリ検索フィルターを使用できるのは、McAfee Anti-Spam アドオン コンポーネントをインストール済みの場合に限られます。

関連トピック:

46 ページの「*詳細検索オプション*」

検索フィルター比較表

選択した検出アイテムカテゴリに使用可能な検索フィルターについて説明します。

MSME で使用可能な検索フィルターの基準は、選択した検出アイテムのカテゴリになります。 特定の検出アイテムカテゴリにどの検索フィルターを使用できるか分からないときは、以下の表を参考資料として使用してください。

この比較表を見れば、特定の検出タイプに使用可能な検索フィルターがすぐに分かります。

表 3-2 比較表ー各検出タイプの検索フィルター

フィルター	スパム	IP レピュテーション	フィッシング詐欺	ウイルス	不審なプログラム	不要なコンテンツ	禁止されたファイルタイプとメッセージ	DLP とコンプライアンス	メール URL レピュテーション
[実行されたアクション]	✓	✓	✓	✓	✓	✓	✓	✓	✓
[スパム対策エンジン]	✓		✓						
[スパム対策ルール]	✓		✓						
[ウイルス対策 DAT]				✓	✓				
[ウイルス対策エンジン]				✓	✓				
[禁止する語句]						✓		✓	✓
[検出名]				✓	✓				
[ファイル名]				✓	✓	✓	✓	✓	✓
[フォルダー]				✓	✓	✓	✓	✓	✓
[IP レピュテーション スコア]		✓							
[ポリシー名]	✓		✓	✓	✓	✓	✓	✓	✓
[受信者]	✓		✓	✓	✓	✓	✓	✓	✓
[レピュテーション スコア]	✓		✓						
[ルール名]	✓		✓		✓	✓	✓	✓	✓
[スキャン実行者]	✓		✓	✓	✓	✓	✓	✓	✓
[送信者]	✓		✓	✓	✓	✓	✓	✓	✓
[送信者 IP]	✓	✓	✓						
[サーバー]	✓		✓	✓	✓	✓	✓	✓	✓
[スパム スコア]	✓		✓						
[件名]	✓		✓	✓	✓	✓	✓	✓	✓
[チケット番号]	✓		✓	✓	✓	✓	✓	✓	✓

[理由]、[理由]、[状態]、[タスク] 検索フィルターを使用できるのは、[検出されたアイテム] 、[すべてのアイテム] の順に移動して設定したカテゴリに限られるため、この比較表には記載されていません。

関連トピック:

40 ページの「*検出タイプ*」

詳細検索オプション

詳細検索オプションの情報を入力し、検索結果として検出されたアイテムを絞り込みます。

表 3-3 オプションの定義

オプション	定義
[AND]	前および次のフィルター オプションで設定された条件に基づきアイテムを検索します。両方の条件を満たす検索結果が得られます。
[OR]	前および次のフィルター オプションで設定された条件に基づきアイテムを検索します。いずれかの条件を満たす検索結果が得られます。
[含む]	最初の検索フィルターで指定したテキストを含むアイテムを検索します。例えば、**アウトボックス** フォルダーで検出された隔離アイテムを検索する場合、プライマリ検索フィルターとして [フォルダー] を選択し、ドロップダウン リストから [含む] を選択してテキスト ボックスに `out` と入力し、[検索] をクリックして [結果の表示] セクションで検索結果を表示します。
[含まない]	検索結果で指定したテキストを含まないアイテムを検索します。例えば、ログ記録したアイテムを検索結果に表示する場合、プライマリ検索フィルターとして [実行されたアクション] を選択し、ドロップダウン リストから [含まない] を選択して `log` と入力し、[検索] をクリックして [結果の表示] セクションで検索結果を表示します。
[完全一致]	指定したテキストと完全に一致するアイテムを検索します。例えば、特定の [ウイルス対策エンジン] バージョン番号 5400.1158 によって検出された隔離アイテムを検索する場合、プライマリ検索フィルターとして [ウイルス対策エンジン] を選択し、ドロップダウン リストから [完全一致] を選択してテキスト ボックスに `5400.1158` と入力し、[検索] をクリックして [結果の表示] セクションで検索結果を表示します。
[正規表現と一致]	正規表現を使用して、特定のパターンと一致するアイテムを検索します。例えば、検出内の任意の場所で有効な電子メール アドレスに基づいて検索する場合、プライマリ検索フィルターとして [検出名] を選択し、ドロップダウン リストから [正規表現と一致] を選択してテキスト ボックスに `\b[A-Z0-9._%+-]+@(?:[A-Z0-9-]+\.)+[A-Z]{2,4}\b` と入力し、[検索] をクリックして [結果の表示] セクションで検索結果を表示します。
[に等しい]	指定した値に等しい [スパム スコア]、[レピュテーション スコア] または [IP レピュテーション スコア] を含むアイテムを検索します。
[より小さい]	指定した値より小さい [スパム スコア]、[レピュテーション スコア] または [IP レピュテーション スコア] を含むアイテムを検索します。
[より大きい]	指定した値より大きい [スパム スコア]、[レピュテーション スコア] または [IP レピュテーション スコア] を含むアイテムを検索します。
[大文字と小文字を区別]	大文字または小文字を区別した検索条件を使用する場合に選択します。
[すべての日付]	すべての日付のアイテムを検索する場合に選択します。 隔離されたアイテムのデータベースに保存された日付に基づいて検索結果が表示されます。
[日付の範囲]	要件に合わせて定義した日付の範囲内でアイテムを検索します。ここでは、[開始] および [終了] パラメーターに対して年月日および時刻を指定できます。カレンダー アイコンを使用して、日付の範囲も指定できます。 日付の範囲は、システムのローカル時間に基づきます。
[検索]	クリックすると、検索条件に一致する隔離されたアイテムのリストが[結果の表示] セクションに表示されます。
[フィルターをクリア]	クリックすると、デフォルトの検索設定に戻ります。

関連トピック:

42 ページの「*使用可能なプライマリ検索フィルター*」

検出されたアイテムの検索

検索フィルターを使用して検索したい特定の隔離アイテムを検出し、対応するアクションを実行します。
ブール論理演算子、正規表現、大文字/小文字の区別や日付範囲などの検索フィルターを組み合わせて使用できます。

タスク

1 製品のユーザー インターフェースで、[検出されたアイテム] をクリックします。

2 左側のペインで、[スパム]、[フィッシング詐欺]、または[すべての項目] などの任意の検出カテゴリをクリックします。

3 [検索] ペインで、ドロップダウン リストから任意の検索フィルターを選択します（必要な場合）。使用可能な検索オプションは次のとおりです。

表 3-4 検索オプション

検索機能	説明
プライマリ検索フィルター	[ポリシー名]、[実行されたアクション]、[送信者] などの特定のフィルターに基づき、検索条件を絞り込む場合に選択します。 すべてのプライマリ検索フィルターの詳細については、『使用できるプライマリ検索フィルター』を参照してください。
ブール論理演算子	以下の論理演算子を使用して検索を絞り込む場合に選択します。 • [AND] • [OR] これらのフィルター オプションの詳細については、『追加検索オプション』を参照してください。
セカンダリ検索フィルター	以下のセカンダリ フィルターを使用して検索を絞り込む場合に選択します。 • [含む] • [含まない] • [完全一致] • [正規表現と一致] • [に等しい] • [より小さい] • [より大きい] これらのフィルター オプションの詳細については、『追加検索オプション』を参照してください。
[大文字と小文字を区別]	大文字または小文字を区別した検索条件を使用する場合に選択します。
[日付の範囲]	すべての日付や特定の期間に検索を絞り込む場合に選択します。 • [すべての日付] • [日付の範囲]

4 [検索] をクリックします。

このタスクを実行すると、検索条件に一致する検出アイテムを正常に検索し、[結果の表示] セクションに表示されました。

隔離されたアイテムに対して実行可能なアクション

定義したパラメーターに基づいた検索結果を表示し、隔離されたアイテムに対して必要なアクションを実行します。

以下の隔離されたアイテムに対して各種アクションを実行できます。

表 3-5 アクションの種類

アクション	定義
[解放]	隔離されているアイテムを解放します。 [結果の表示] ペインで適切なレコードを選択し、[解放] をクリックします。 目的の受信者に送信するために、元の電子メール メッセージがデータベースから解放されます。 • アイテムがダウンロード、解放または転送されると、ウイルス スキャンが実行されます。この結果を表示するには、[ダッシュボード] 、[最近スキャンされたアイテム] の順に移動します。 • 正常に解放されると、アイテムのステータスは [解放済み] になります。この状態を確認するには、[検出アイテム] 、 [すべての項目] の順に移動します。
[ダウンロード]	隔離されているアイテムをダウンロードまたは分析します。 [結果の表示] ペインで適切なレコードを 1 つ選択し、[ダウンロード] をクリックします。 [検出アイテム] 、 [すべての項目] の順に移動して、複数のレコードに対する [ダウンロード]、[転送]、[表示]、[解放] は一度に行うことはできません。 ただし、1 つの特定のカテゴリから複数のレコードを [解放] することはできます。
[CSV ファイルにエクスポート]	検索で戻されたすべての隔離アイテムに関する情報を .CSV 形式でエクスポートして保存します。 データベースに数千の隔離アイテムがある場合、膨大なページを移動する代わりに、このオプションを使用して、これらのレコードを CSV 形式でダウンロードし、後で Microsoft Excel 形式のカスタム レポートを生成できます。 [結果の表示] ペインで、[CSV ファイルにエクスポート] をクリックして検索結果を[開く]か、任意のフォルダーや場所に[保存]します。 [結果の表示] に表示する隔離アイテムの数を制限するには、[設定と診断] 、 [検出アイテム] 、 [ローカル データベース] の順に選択して、[クエリの最大サイズ (レコード)] の値を変更します。 • CSV ファイルの検索結果内に特定のフィールドが見つからない場合、[表示するカラム] オプションの必要なフィールドを必ず有効化します。 • Microsoft Excel の [インポート] オプションを使用して、別のロケールで CSV ファイルを開きます。
[転送]	隔離されたアイテムを任意の受信者に転送します。隔離されたアイテムを複数の受信者に転送する場合は、区切り文字としてセミコロン（;）を使用します。このアクションを実行すると、隔離されたアイテムが新しい電子メールで添付ファイル（.eml 形式）として送信されます。 組織内の送信先の配布リスト（DL）に隔離されたアイテムを転送する場合は、DL の SMTP アドレスを指定します。
[表示]	隔離されたアイテムを別ウィンドウで表示します。
[ブロック送信者に追加]	電子メールをブロックする必要があるアドレスの一覧に送信者の電子メール アドレスを追加します。これは、ブラックリスト登録ともいわれます。
[許可送信者に追加]	電子メールを許可する必要があるアドレスの一覧に送信者の電子メール アドレスを追加します。これは、ホワイトリスト登録ともいわれます。

表 3-5 アクションの種類 *(続き)*

アクション	定義
[表示するカラム]	[結果の表示] ペインに表示する追加のカラム ヘッダーを選択します。このオプションには、[検索] ペインで使用可能なすべてのフィルターと一部の追加オプションの一覧があります。
[すべて選択]	[結果の表示] セクションのページに表示される隔離されたアイテムをすべて選択します。 たとえば、隔離されたアイテムが 100 個あり、[1 ページあたり] の表示アイテム数を 10 個に設定する場合、[結果の表示] セクションに表示されるアイテム数は 10 個のみが選択されます。
[選択解除]	[結果の表示] セクションのページに表示されるすべての隔離されたアイテムの選択を解除します。
[削除]	選択したカテゴリの [結果の表示] セクション ページで選択した隔離されたアイテムを削除します。 複数のアイテムを選択するには、**Ctrl** キーを押しながら選択します。
[すべて削除]	選択したカテゴリのデータベースから隔離アイテムをすべて削除します。
[1 ページあたりの表示]	1 ページあたりに表示する隔離アイテムの最大数を指定します。 オプションは次のとおりです。 • [10] • [20] • [50] • [100]

[結果の表示] ペインの各アイテムには画像が付いています。それらには以下の意味があります。

アイコン	説明
	隔離されたアイテムで、ダウンロード、転送、解放、または表示できるアイテムです。
	ログにのみ記録されたアイテムで、ダウンロード、転送、解放、または表示できないアイテムです。

3 **検出アイテム**
隔離されたアイテムに対して実行可能なアクション

4 ポリシー マネージャ

製品内で各ポリシーと対応するアクションを設定したり管理したりすることができます。また、さまざまな種類の脅威が検出されたときの処理方法を決定します。

通常、ポリシーの定義は、判定のガイドや合理的な結果を実現するための原理やルールと説明されます。ポリシーを採用する目的は、組織で客観的な判断を下す際に役立てることです。

MSME では、使用される設定と、Exchange 環境で検出がトリガーされたときに実行されるアクションがポリシーによって指定されます。複数のポリシーを作成したり、特定のポリシーに対して特定の設定やアクションを定義したりすることができます。例えば、[オンアクセス] メニュー オプションに複数のサブポリシーを作成したり、各ポリシーに別々の設定やアクションを設定したりすることができます。

簡単に説明すると、MSME ポリシー = スキャナー設定 + 実行するアクションということになります。

1 つの共通の場所からスキャナー、フィルター、アラートの各設定ルールを変更または作成するには、[ポリシー マネージャー] の [共有リソース] を使用します。[共有リソース] を使用すると、MSME ポリシーの作成と適用における時間を節約できます。

ポリシーを作成する手順

管理者としてポリシーを作成する場合は、以下の手順を実行する必要があります。

1 スキャナーまたはフィルターを有効にします。

2 ポリシーまたは [共有リソース] からスキャナーまたはフィルターの設定を編集します。

3 検出がトリガーされたときに実行されるアクションを指定します。

4 このポリシーの適用先ユーザーを指定します。

5 必要なポリシー カテゴリの設定を適用します。

目次

- *脅威を処理するポリシー カテゴリ*
- *ポリシー マネージャー ビュー*
- *マスター ポリシーとサブポリシー*
- *コア スキャナとフィルタ*
- *スキャナーとフィルターの比較表*
- *選択したポリシーのすべてのスキャナーとフィルターをリストで表示*
- *スキャナーまたはフィルターを追加する*
- *指定ユーザー用ルールの新規作成*
- *検出時に実行可能なアクション*
- *共有リソース*
- *ポリシー用コア スキャナー設定の管理*
- *ポリシー用フィルター設定の管理*
- *ポリシー用その他の設定の管理*

脅威を処理するポリシー カテゴリ

使用可能なポリシー カテゴリを表示し、既存のデフォルト ポリシー（**マスタ ポリシー**として知られる）を組織全体に適用します。

MSME では、特別なルールと設定のセットを使用して電子的な脅威を軽減できます。このようなルールと設定のセットをポリシーといい、組織の Exchange 環境ニーズに合わせて作成することができます。

Exchange サーバーに MSME を最初にインストールする際には、以下のメニュー オプションにデフォルトの [マスター ポリシー] を使用できます。

- [オンアクセス]
- [オンデマンド (デフォルト)]
- [オンデマンド (ウイルスを検出)]
- [オンデマンド (ウイルスの駆除)]
- [オンデマンド (禁止されたコンテンツの検索)]
- [オンデマンド (禁止されたコンテンツの削除)]
- [オンデマンド (フル スキャン)]
- [ゲートウェイ]

各カテゴリのポリシーをカスタマイズすると、組織の Exchange 環境に影響を及ぼす可能性がある特別な脅威を精確に処理できます。

ポリシー マネージャー ビュー

継承または優先順位に基づきサブポリシーの表示・並べ替えを行います。

[ポリシー マネージャー] ビューには、以下の種類があります。

- [継承ビュー]
- [詳細ビュー]

継承ビュー

マスター ポリシーとサブポリシーの優先順位とステータスが表示されます。 最高の優先順位でサブポリシーに構成した設定に基づき、MSME によって電子メールが判定されます。 サブポリシーのルールが満たされない場合、MSME は次の優先順位のサブポリシーに移動します。 マスター ポリシーで構成された設定は、どのサブポリシーのルールも満たされないときに適用されます。[]

[継承ビュー] を選択すると、ポリシーの継承に基づいてサブポリシーが表示されます。

このビューでは、以下の操作を実行できます。

- ポリシーとその優先順位を表示する
- 継承したサブポリシーとその親ポリシーを表示する
- サブポリシーを有効/無効にする
- サブポリシーを削除する

詳細ビュー

優先順位に基づき昇順ですべてのポリシーが表示され、サブポリシーの優先順位を変更するためのオプションがあります。

このビューでは、以下の操作を実行できます。

- 優先順位に基づき並べ替えられたポリシーを表示する
- ポリシーの優先順位を変更する

以下のアイコンを使用すると、ポリシーの優先順位を変更できます。
- ^ーポリシーの優先順位を上げる
- v ーポリシーの優先順位を下げる

- サブポリシーを有効/無効にする
- サブポリシーを削除する
- [詳細] をクリックすると、ポリシー名、説明、親ポリシーを編集する

マスター ポリシーとサブポリシー

通常、階層構造内のポリシー設定は、親から子へ、子から孫へ、さらにその下へと受け渡されます。 この概念を「継承」といいます。 MSME では、デフォルトの親ポリシーを [マスター ポリシー]、子ポリシーを [サブポリシー] といいます。

マスター ポリシー

デフォルトの親ポリシーで、アイテムのウイルス スキャン方法、ファイルのフィルター方法、その他の各種設定を定義するすべてのポリシー カテゴリに使用できます。 マスタ ポリシーは、組織内のすべてのユーザに適用されます。

[マスター ポリシー] は、サブポリシーを作成するためのベースラインとして機能するので削除できません。

サブポリシー

別のポリシーから各設定とアクションを継承するポリシーは、サブポリシーと呼ばれます。 必要に応じて別々の設定とアクションを持つ追加サブポリシーを作成し、特定のユーザーに適用することができます。

サブポリシーが必要になるのは、地域、機能、メールボックス、ドメイン、または組織内の部門に適合するように、[マスター ポリシー] に例外を作成する必要があるときです。 MSME では、こうした追加ポリシーを一般的にポリシー グループと呼んでいます。

電子メールで実行されるアクションは、最高の優先順位でサブポリシーに構成した設定に基づきます。 最高の優先順位を持つサブポリシーのルールが満たされない場合、MSME は次の優先順位のサブポリシーに移動します。 マスター ポリシーで構成された設定は、どのサブポリシーのルールも満たされないときにのみ適用されます。

スキャナーまたはフィルター設定ページで [親ポリシーから設定を継承] を選択する場合、継承したポリシー（サブポリシー）では同じ設定が親ポリシーとして使用されます。 ただし、検出がある場合は別のアクションを実行できます。 親または [マスター ポリシー] で設定に加えた変更は、それぞれのサブポリシーに反映されます。

例えば、MSME によって脅威として識別されたすべての電子メール メッセージを次のとおりに判定するサブポリシーを作成します。

- 隔離ー全ユーザー対象
- ログ記録して隔離し、管理者に通知ー全管理者対象

以下の簡単な例では、サブポリシーが必要になる場合についてさらに詳しく説明します。

表 4-1 例ーサブポリシーが必要になるとき

ポリシーの種類	スキャナー	保護レベル	ユーザー	実行するアクション
マスター ポリシー	ウイルス対策	保護レベル（中）	全ユーザー	[隔離]
サブポリシー	ウイルス対策	保護レベル（高）	管理者	[ログ]、[隔離]、および [管理者に通知]

MSME をデフォルト設定に戻すと、既存のサブポリシーは削除されます。 MSME を工場設定に戻す前に、[設定と診断]、[設定のインポート/エクスポート] 、[設定] タブで [エクスポート] を使用してポリシーと設定を必ずバックアップしてください。

サブポリシーの作成

組織の任意の部門における特定のニーズに適合するように、[マスター ポリシー] または親ポリシーに基づいて他のポリシーを作成します。また、[マスター ポリシー] によってカバーされない例外状況用のサブポリシーを作成します。

このサブポリシーが役立つのは、組織内の特定のユーザーやグループ用の [マスター ポリシー] からルールを適用したくないときです。例外を作成し、MSME で特定のスキャンを実行できるようにします。

どんな時にサブポリシーを作成するかに関する例を以下に示します。

- スキャン後に組織内の重役レベルのユーザーに対して受信電子メールの通過を許可するが、他のユーザー用に隔離する。
- 特定のユーザー グループに特定のファイル形式を許可する。例えば、組織内の特定の部門を除き、すべてのユーザーに .wav ファイルをブロックする場合などです。

タスク

1 [ポリシー マネージャー] で、サブポリシーを作成する対象のメニュー アイテムを選択します。

2 [サブポリシーの作成] をクリックします。

[サブポリシーの作成] ページが表示されます。

3 [初期設定] 、[Identification（識別）] 、[サブポリシー名] で、ポリシーとその機能を識別する名前を指定します。

4 ポリシーの [説明] を入力します (オプション)。

5 設定の継承元のサブポリシーの [親ポリシー] を選択します。

6 [次へ] をクリックします。

7 [トリガー ルール] 、 [ルール] で [新規ルール] をクリックします。

8 [ポリシー ルールの指定] では、以下を選択できます。

- [<ルール テンプレートの選択>]ー送信者または受信者に基づいてポリシー ルールを指定します。以下のオプションに基づいてルールを新規作成できます。
  - [送信者の SMTP アドレスは電子メール アドレスです]
  - [送信者の SMTP アドレスは電子メール アドレスではありません]
  - [送信者は Active Directory グループにあります]
  - [送信者は Active Directory グループにありません]

- [受信者の SMTP アドレスは電子メール アドレスです]
- [受信者の SMTP アドレスは電子メール アドレスではありません]
- [いずれかの受信者が Active Directory グループにあります]
- [いずれかの受信者が Active Directory グループにありません]

電子メール アドレスやユーザー名が競合するルールを作成しないように注意してください。ユーザーを指定する際には正規表現（regex）はサポートされていません。サポートされるのはワイルドカードのみです。

- [別のポリシーからのルールのコピー]ー別のポリシーからルールをコピーします。

9 [追加] をクリックします。

10 ユーザーに対してポリシーが必ずトリガーされる条件を指定します。次を選択できます。

- [いずれかのルールが適用される]
- [すべてのルールが適用される]
- [いずれのルールも適用されない]

11 [次へ] をクリックします。

12 [スキャナーとフィルター] では、次のオプションを選択できます。

- [親ポリシーからすべての設定を継承]ー親ポリシーのすべてのプロパティを継承します。
- [他のポリシーからコピーした値で選択した設定を初期化します]ー使用可能なポリシーから特定のスキャナーとフィルターを選択します。

13 [完了] をクリックします。

コア スキャナとフィルタ

ポリシーの作成時に適用できるスキャナーとフィルターの種類を決定します。

コア スキャナー

[ポリシー マネージャー] 、 [共有リソース] の順に移動し、以下のスキャナーの設定を表示して設定します。

スキャナー	定義
[ウイルス対策スキャナー]	ウイルス、トロイの木馬、ワーム、パッカー、スパイウェア、アドウェアなどの脅威を検出するように設定を行います。
[DLP とコンプライアンス スキャナー]	60 種類の新しい [DLP とコンプライアンス ディクショナリ] の追加と共に、組織の Exchange 環境の機密ポリシーやコンプライアンス ポリシーを満たすため、[DLP とコンプライアンス ルール] を作成または構成します。
[ファイル フィルタリング]	組織の Exchange 環境ニーズを満たすため、新しいファイル フィルタリング ルールを作成します。 ファイル名、ファイル カテゴリ、またはファイル サイズに基づき以下の設定を構成します。
[メール URL レピュテーション]	不要なリンク、フィッシング詐欺リンク、マルウェアを含む URL を検出するように設定します。

スキャナー	定義
[スパム対策]	スパム スコア、サイズ、ルール、メーリング リストに基づき、スパムとして分類される電子メール メッセージを検出するための設定を構成します。
[フィッシング詐欺対策]	フィッシング詐欺として分類される電子メール メッセージのレポート設定を構成します。

[スパム対策]と[フィッシング詐欺対策] オプションは、McAfee Anti-Spam アドオン コンポーネントをインストールしている場合にのみ使用できます。

フィルタ

組織の Exchange 環境ニーズに基づき、各種フィルターを有効/無効にし、検出がある場合に実行されるアクションを指定します。

一部のフィルターは有効/無効にできますが、カスタマイズした設定を構成できません。 [共有リソース] 、[スキャナーとアラート] 、[スキャナー] 、[カテゴリ] の順に移動した場合、このようなフィルターはドロップダウン リストに表示されません。

フィルター	定義
[破損したコンテンツ]	破損したコンテンツとして検出される電子メール メッセージを判定するための設定を構成します。
[保護されたコンテンツ]	保護されたコンテンツとして検出される電子メール メッセージを判定するための設定を構成します。
[暗号化されたコンテンツ]	暗号化されたコンテンツとして検出される電子メール メッセージを判定するための設定を構成します。
[署名付きのコンテンツ]	署名付きのコンテンツとして検出される電子メール メッセージを判定するための設定を構成します。
[パスワードで保護されたファイル]	パスワードで保護されたコンテンツを含む電子メール メッセージを判定するための設定を構成します。 必要に応じて、ファイル フィルタリング ポリシーを上書きし、パスワード保護ファイルが添付された電子メールの通過を許可できます。 詳細については、「パスワードで保護されたファイルを設定する」を参照してください。
[メール サイズ フィルタリング]	メール サイズによるフィルタリング オプションを超過する電子メール メッセージを判定するための設定を作成または構成します。 全体のメール サイズ、添付ファイル サイズ、添付ファイル数に基づいて電子メール メッセージを隔離するための設定を構成します。
[スキャナー制御]	階層の深さ、展開したファイル サイズ、スキャン時間に基づいて電子メール メッセージを判定するためのコア スキャナー設定を作成または構成します。
[MIME メールの設定]	MIME メッセージとして分類される脅威を検出するための設定を作成または構成します。
[HTML ファイル]	コメント、URL、メタデータ、スクリプトなどの HTML 要素を含む電子メール メッセージを判定するための設定を作成または構成します。

その他

検出があった場合にエンドユーザーに送信されるアラートや免責事項といったその他の設定を構成します。

その他	定義
[アラート設定]	検出があった場合の電子メール アラートの設定を作成または構成します。 アラート電子メール形式 (HTML またはテキスト)、エンコーディング、ファイル名、ヘッダー、フッターなどの設定を構成します。
[免責事項のテキスト]	検出があった場合にエンドユーザーに送信される電子メールに表示する必要がある免責事項のテキストを作成または構成します。

スキャナーとフィルターの比較表

デフォルトで各ポリシー カテゴリにはどの検索スキャナーまたはフィルターを使用できるかについて参照できます。

MSME で使用可能なスキャナーは、選択したポリシー カテゴリに応じて異なります。

特定のポリシー カテゴリにどのスキャナーまたはフィルターを使用できるか分からないときは、以下の表を参考資料として使用してください。この比較表を参照すると、各ポリシー カテゴリに使用可能なスキャナーとフィルターが分かります。ここで使用される頭字語は次のような定義になっています。

- OA—[オンアクセス]
- OD (D)—[オンデマンド（デフォルト）]
- OD (FV)—[オンデマンド（ウイルス検出）]
- OD (RV)—[オンデマンド（ウイルス駆除）]
- OD (FC)—[オンデマンド（非対応コンテンツの検出）]
- OD (RC)—[オンデマンド（非対応コンテンツの駆除）]
- OD (FS)—[オンデマンド（フル スキャン）]
- GW—[ゲートウェイ]

コア スキャナー

コア スキャナー	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
[ウイルス対策スキャナー]	✓	✓	✓	✓			✓	
[DLP とコンプライアンス スキャナー]	✓	✓			✓	✓	✓	
[ファイル フィルタリング]	✓	✓					✓	
[メール URL レピュテーション]	✓	✓					✓	
[スパム対策]								✓
[フィッシング詐欺対策]								✓

[DLP とコンプライアンス スキャナー] が [オンアクセス] と [オンデマンド (デフォルト)] ポリシー カテゴリに使用できる場合でも、デフォルトではアクティブまたは有効ではありません。 必要なルールを作成し、ルールのトリガー時に実行されるアクションを指定してスキャナーを有効にする必要があります。

フィルター

フィルター	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
[破損したコンテンツ]	✓	✓					✓	
[保護されたコンテンツ]	✓	✓			✓	✓	✓	
[暗号化されたコンテンツ]	✓	✓			✓	✓	✓	
[署名付きのコンテンツ]	✓	✓			✓	✓	✓	
[パスワードで保護されたファイル]	✓	✓			✓	✓	✓	
[メール サイズ フィルタリング]	✓							✓
[スキャナー制御]	✓	✓	✓	✓	✓	✓	✓	✓
[MIME メールの設定]	✓	✓			✓		✓	✓
[HTML ファイル]	✓	✓			✓		✓	✓

アラートと免責事項の設定

その他の設定	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
[アラート設定]	✓	✓		✓	✓	✓	✓	✓
[免責事項のテキスト]	✓							

選択したポリシーのすべてのスキャナーとフィルターをリストで表示

選択したポリシー カテゴリに使用可能なスキャナーとフィルターのステータスを表示します。

使用可能な設定の種類は、選択したポリシーによって異なります。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] とポリシー カテゴリのメニュー アイテムをクリックします。

選択したメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または必要なサブポリシーをクリックします。

対応するポリシーのページが表示されます。 それぞれのポリシー ページで使用可能なフィルターが表示されます。

3 ポリシー ページでは、以下のタブを使用できます。

- [全スキャナー一覧]－ポリシーに対して有効化するスキャナーまたはスキャナーを表示します。
- [設定の表示]－スキャナーまたはフィルターの設定と指定アクションを表示します。
- [ユーザーの指定]－特定のユーザーに適用するポリシー ルールを指定します。

ユーザーを指定できる対象はサブポリシーに限られます。

4 [全スキャナー一覧] タブでは、以下の項目を使用できます。

表 4-2 ポリシーの設定

オプション	定義
[ポリシー]	設定するポリシーを選択します。
[スキャナー/フィルターの追加]	特定の時間のみに適用されるようにポリシーを設定します。例えば、週末のみに適用される、別々のルールを含む新しいウイルス対策設定を作成できます。
[コア スキャナー]	各スキャナーごとにポリシーを設定します。 • [ウイルス対策スキャナー] • [DLP とコンプライアンス スキャナー] • [ファイル フィルタリング] • [メール URL レピュテーション] • [スパム対策] • [フィッシング詐欺対策]
[フィルター]	各フィルターごとにポリシーを設定します。 • [破損したコンテンツ] • [保護されたコンテンツ] • [暗号化されたコンテンツ] • [署名付きのコンテンツ] • [パスワードで保護されたファイル] • [メール サイズ フィルタリング] • [スキャナー制御] • [MIME メールの設定] • [HTML ファイル]
[その他の設定]	ポリシーのアラート設定と免責事項のメッセージを設定します。 [その他] には、次のものが含まれます。 • [アラート設定] • [免責事項のテキスト]

スキャナーまたはフィルターを追加する

スキャナーやフィルターを追加して、組織の Exchange 環境における例外的な使用状況を設定します。

スキャナーまたはフィルターを追加すると有益なのは、追加のスキャナーまたはフィルターを以下の条件で使用するときです。

- 異なるオプションとルールを設定する
- 指定タイム スロット中にのみ有効にする

タスク

1 [ポリシー マネージャー] でポリシー カテゴリを選択します。

2 [マスター ポリシー] または任意のサブポリシーをクリックします。

3 [全スキャナー一覧] タブで [スキャナー/フィルターの追加] をクリックします。

[スキャナー/フィルターの追加] オプションを使用できるのは、[オンアクセス] および [ゲートウェイ] ポリシー カテゴリのみです。

4 [カテゴリの指定] ドロップダウン リストから、必要なスキャナまたはフィルタを指定します。

5 [このインスタンスを使用するとき] セクションから、既存のタイム スロットを選択するか、新しく作成します。

6 [保存] をクリックします。

7 [適用] をクリックします。

組織環境のニーズに適合するようにオプションとルールを編集します。

指定ユーザー用ルールの新規作成

新しいルールを作成し、特定のユーザーに適用する条件を指定します。

ポリシー内で例外を設けるように指定ユーザーまたはグループのルールを作成できます。

タスク

1 [ポリシー マネージャー] でポリシー カテゴリを選択します。

2 特定のユーザーに設定するサブポリシーをクリックします。

3 [ユーザの指定] タブをクリックします。

4 [新規ルール] をクリックします。

5 [ポリシー ルールの指定] で、次の項目を選択します。

- [<ルール テンプレートの選択>]ー送信者または受信者に基づいてポリシー ルールを指定します。以下のオプションに基づいてルールを新規作成できます。
  - [送信者の SMTP アドレスは電子メール アドレスです]
  - [送信者の SMTP アドレスは電子メール アドレスではありません]
  - [受信者の SMTP アドレスは電子メール アドレスです]
  - [受信者の SMTP アドレスは電子メール アドレスではありません]
  - [送信者は Active Directory グループにあります]
  - [送信者は Active Directory グループにありません]
  - [いずれかの受信者が Active Directory グループにあります]
  - [いずれかの受信者が Active Directory グループにありません]

  電子メール アドレスやユーザー名が競合するルールを作成しないように注意してください。ユーザーを指定する際には正規表現（regex）はサポートされていません。サポートされるのはワイルドカードのみです。

- [別のポリシーからのルールのコピー]ー別のポリシーからルールをコピーします。

6 [追加] をクリックします。

7 ユーザーにポリシーをトリガーする条件を指定します。 次のオプションを選択できます。

- [いずれかのルールが適用される]
- [すべてのルールが適用される]
- [いずれのルールも適用されない]

8 [適用] をクリックして特定のユーザにルールを保存します。

検出時に実行可能なアクション

ポリシー内の各スキャナーとフィルター設定について、検出時に実行する基本アクションと 2 番目のアクションを指定できます。検出をトリガーすると電子メール メッセージまたは添付ファイルに実行されるアクションを指定できます。

スキャナーまたはフィルターの設定に基づいてポリシー ルールがトリガーされると、設定した基本アクションおよび 2 番目のアクションに基づき MSME によって検出が判定されます。

アクションを設定するときには、少なくとも 1 つの基本アクションを選択する必要があります。なお、2 番目のアクションは複数個選択できます。例えば、基本アクションが検出をトリガーする電子メールの削除である場合、2 番目のアクションは検出の記録と管理者への通知にできます。

使用可能な基本アクションは、ポリシー カテゴリの種類と、構成するスキャナーまたはフィルターの設定に応じて異なります。

ポリシー カテゴリとスキャナーのデフォルト設定にアクションを戻すには、[リセット] をクリックします。

表 4-3 基本アクション

アクション	定義
[検出したウイルスまたはトロイの木馬の駆除を試みる]	[ウイルス対策スキャナー] によって検出されたウイルスまたはトロイの木馬が含まれる電子メールを駆除します。
[アラートが発せられた項目を置き換え]	検出をトリガーした電子メールをアラートに置き換えます。
[組み込み項目の削除]	電子メール内の検出をトリガーした添付ファイルを削除します。
[メッセージを削除]	検出をトリガーした電子メールを削除します。
[通過を許可]	電子メールが次のスキャン フェーズに進んだり、エンドユーザーに送信されたりすることを許可します。
[スコア ベースのアクション]	スパム スコアを基準にアクションを実行します。このオプションを使用できるのはスパム対策スキャナーに限られ、[スパム スコア] が高/中/低の場合から選択する必要があります。
[システム迷惑メール フォルダーにルーティングする]	[スパム対策] スキャナーによって検出された電子メールを、[設定と診断] 、 [スパム対策] 、 [ゲートウェイ スパム フィルター] 、 [システム迷惑メール フォルダー アドレス] で指定した電子メール アドレスにルーティングします。
[ユーザー迷惑メール フォルダーにルーティングする]	[スパム対策] スキャナーによって検出された電子メールを受信者の [迷惑メール] フォルダーにルーティングします。
[メッセージを拒否する]	電子メールを拒否してユーザーに通知を送信します。
[アラートが発せられた添付ファイルを置き換える]	添付ファイル サイズが超過すると [メール サイズによるフィルタリング] スキャナーがトリガーされる場合、電子メール メッセージ内の添付ファイルをアラートに置き換えます。

表 4-3 基本アクション *(続き)*

アクション	定義
[すべての添付ファイルを 1 つのアラートに置き換える]	添付ファイル数が超過すると [メール サイズによるフィルタリング] スキャナーがトリガーされる場合、複数の添付ファイルを含む電子メール メッセージを 1 つのアラートに置き換えます。
[署名を分離する変更を許可しない]	[署名付きのコンテンツ] を含む電子メール メッセージが検出されたときに、MSME で署名が分離されないようにします。
[署名を分離する変更を許可する]	[署名付きのコンテンツ] を含む電子メール メッセージが検出されたときに、MSME で署名の分離を許可します。

表 4-4 2 番目のアクション

アクション	定義
[ログ]	検出をログに記録します。
[隔離]	検出をトリガーした電子メールのコピーを隔離データベースに保存します。隔離されたアイテムをすべて表示するには、[検出アイテム] 、[すべての項目] または特定の検出カテゴリにアクセスします。 検出カテゴリに基づいて特定のレビュー担当者または配布リストに電子メールを送信するには、[隔離された電子メールの転送] を選択します。検出カテゴリに基づいて通知を設定するには、[設定と診断] 、 [通知] 、 [設定] 、 [詳細] にアクセスします。 [隔離された電子メールの転送] オプションは、[ウイルス対策スキャナー] や [ゲートウェイ] ポリシーには利用できません。
[管理者に通知]	[設定と診断] 、 [通知] 、 [設定] 、 [全般] の [管理者電子メール] で指定した管理者へ、電子メールのコピーを送信します。
[内部送信者に通知]	元の電子メールの発信元が Exchange サーバーの認証ドメイン内の場合、アラート メッセージを内部送信者に送信します。
[外部送信者に通知する]	元の電子メールの発信元が Exchange サーバーの認証ドメイン内ではない場合、アラート メッセージを送信者に送信します。
[内部受信者に通知]	受信者が Exchange サーバーの認証ドメイン内の場合、アラート メッセージを受信者に送信します。
[外部受信者に通知する]	受信者が Exchange サーバーの認証ドメイン内ではない場合、アラート メッセージを受信者に送信します。

共有リソース

スキャナー、フィルター、アラート、DLP とコンプライアンス ディクショナリ、およびタイム スロットの各設定を編集する共通の場所です。ポリシーを設定する際には、同じリソース（スキャナーとフィルターの設定）を複数のポリシーに適用する場合があります。その場合には、[共有リソース] を使用してください。

例えば、内部および外部の受信者用に別々の免責事項を使用する場合、受信者用の免責事項を作成して必要なサブポリシーに適用します。

製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] をクリックします。以下のタブを使用できます。

- [スキャナーとアラート]ー新しいスキャナーとフィルターの設定を編集または作成します。
- [DLP とコンプライアンス ディクショナリ]ー新しい [DLP とコンプライアンス ルール] および [ファイル フィルタリング ルール] を編集または作成します。
- [タイム スロット]ー平日または週末などの新しいタイム スロットを編集または作成します。

上記の設定に加えた変更は、以下の構成を使用してすべてのポリシーに自動的に適用されます。

スキャナー設定の構成

組織の Exchange 環境の要件に適合するようにスキャナー設定を作成または変更します。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] をクリックします。

[共有リソース] ページが表示されます。

2 [スキャナーとアラート] タブをクリックします。

3 [スキャナー] セクションの [カテゴリ] ドロップダウン リストで、設定するスキャナーを選択します。設定名、ポリシー使用主体、設定するアクションと共にスキャナーの種類が表示されます。以下のいずれかを使用できます。

表 4-5 オプションの定義

オプション	定義
[カテゴリ]	設定する必要なスキャナーを選択します。
[新規作成]	ユーザーの要件に基づきスキャナーの設定を新規作成します。特定のスキャナーに例外を設け、それをポリシーに適用する場合に必要になります。
[編集]	選択したスキャナーの設定を編集します。
[削除]	スキャナー設定を削除します。 次の場合にはスキャナーを削除できません。 • デフォルト スキャナーの場合。 • 任意のポリシーによって使用されている場合。当該スキャナー設定を使用するポリシーがいくつあるかを把握するには、[Used By（使用主体）] 列を参照してください。

4 スキャナー設定を構成したら、[保存]、[適用] の順にクリックします。

これで組織の Exchange 環境要件に基づき、スキャナーの設定を正常に構成できました。

アラート設定の構成

組織の Exchange 環境の要件に適合するように選択したスキャナーのアラート設定を作成または変更します。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] をクリックします。

[共有リソース] ページが表示されます。

2 [スキャナーとアラート] タブをクリックします。

3 [アラート] セクションの [カテゴリ] ドロップダウン リストで、スキャナーに設定するアラートを選択します。設定名、ポリシー使用主体、設定するアクションと共にスキャナーの種類が表示されます。以下のいずれかを使用できます。

表 4-6 オプションの定義

オプション	定義
[カテゴリ]	設定する必要なスキャナーを選択します。
[新規作成]	ユーザーの要件に基づきスキャナーの設定を新規作成します。特定のスキャナーに例外を設け、それをポリシーに適用する場合に必要になります。
[表示]	スキャナーのデフォルト アラート設定を表示します。
[編集]	選択したスキャナーの設定を編集します。アラートで使用可能な変数の詳細については、『使用可能な通知フィールド』を参照してください。
[削除]	スキャナー設定を削除します。 次の場合にはアラートを削除できません。 • デフォルト スキャナー アラートの場合。 • 任意のポリシーによって使用されている場合。当該アラート設定を使用するポリシーがいくつあるかを把握するには、[Used By（使用主体）] 列を参照してください。

4 スキャナー設定を構成したら、[保存]、[適用] の順にクリックします。

これで組織の Exchange 環境要件に基づき、アラートの設定を正常に構成できました。

アラートを作成する

スキャナーまたはフィルターによって実行されたアクションのアラート メッセージを作成します。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] の順にクリックします。

[共有リソース] ページが表示されます。

2 [スキャナーとアラート] タブをクリックします。

3 [アラート] セクションの [カテゴリ] ドロップダウン リストで、スキャナーに設定するアラートを選択します。

4 [新規作成] をクリックします。

[アラート エディター] ページが表示されます。

5 [アラート名] にわかりやすい名前を入力します。

6 それぞれのドロップダウン リストから必要な [スタイル]、[フォント]、[サイズ]、および[トークン] を選択します。

これらのオプションは、[表示] ドロップダウン メニューから [HTML コンテンツ（WYSIWYG）] を選択した場合にのみ使用できます。

7 以下のいずれかのツールを使用して、アラートをカスタマイズします。

表 4-7 ツールバー オプション

オプション	説明
太字	選択したテキストを太字にします。
斜体	選択したテキストを斜体にします。
下線	選択したテキストに下線を引きます。
左揃え	選択した段落を左揃えにします。
中央	選択した段落を中央揃えにします。
右揃え	選択した段落を右揃えにします。
揃える	直線で結んだ左右の端を使用して、選択した段落の行が特定の幅を埋めるように、その段落を調整します。
順序リスト	選択したテキストを番号が付いたリストにします。
非順序リスト	選択したテキストを箇条書きにします。
アウトデント	選択したテキストを設定されている距離だけ右に移動します。
インデント	選択したテキストを設定されている距離だけ左に移動します。
テキストの色	選択したテキストの色を変更します。
背景色	選択したテキストの背景色を変更します。
水平方向のけい線	水平線を挿入します。
リンクを挿入	カーソルの現在位置にハイパーリンクを挿入します。[URL] に [URL] を入力します。[テキスト] に、アラート メッセージに表示するハイパーリンクの名前を入力します。リンク先を新しいウィンドウで開く場合は、[リンクを新しいウィンドウで開く] を選択して、[リンクを挿入する] をクリックします。
イメージを挿入	カーソルの現在位置にイメージを挿入します。[イメージ URL] にイメージの位置を入力します。[代替テキスト] に、イメージが抑制されている場合、またはテキスト専用ブラウザでアラート メッセージが表示される場合に、イメージの代わりに使用するテキストを入力します。イメージにタイトルを付ける場合は、[このテキストをイメージのタイトルとして使用する] にタイトルを入力します。[イメージを挿入する] をクリックします。
表の挿入	カーソルの現在位置に表を挿入します。[行]、[列]、[表の幅]、[罫線の幅]、[セル内の余白]、および [セル間のスペース] に値を入力して表を設定し、[表の挿入] をクリックします。

8 [表示] ドロップダウン メニューから、ユーザー インターフェースでのアラート メッセージの表示方法を指定します。 次の項目を選択できます。

- [HTML コンテンツ (WYSIWYG)] — 基になっている HTML コードを表示せず、アラート メッセージのコンテンツのみを表示します。
- [HTML コンテンツ (ソース)] — コンパイルされる前の状態でアラート メッセージの HTML コードを表示します。
- [プレーンテキスト コンテンツ] — コンテンツを平文として表示します。

以下の通知フィールドを使用して、それらをアラート メッセージに含めることができます。 たとえば、アラート メッセージで、検出されたアイテムの名前と、検出されたときに実行されたアクションを知りたい場合は、**アラート エディター** ページの **%vrs%** と [%act%] を使用します。 通知フィールド オプションの詳細については、「使用可能な通知フィールド」を参照してください。

McAfee では、アラートをテキスト形式でログ ファイルに保存することをお勧めします。他の形式にすると、メール クライアントによっては正しく表示されない場合があります。

9 [保存] をクリックしてポリシー ページに戻ります。

アラート メッセージを最後に保存してから行ったすべての変更を取り消すには、[リセット] をクリックします。

DLP とコンプライアンス ルールの設定

組織の Exchange 環境要件に適合するように、DLP とコンプライアンス ルール/ディクショナリを作成または変更します。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] の順にクリックします。

[共有リソース] ページが表示されます。

2 [DLP とコンプライアンス ディクショナリ] タブをクリックします。

3 [DLP とコンプライアンス ルール] セクションの [言語を選択] ドロップダウン リストから言語を選択します。

対応しているすべてのロケールのディクショナリを表示し、編集できます。 (対応ロケール: 中国語簡体字、フランス語、ドイツ語、日本語、スペイン語)

4 [DLP とコンプライアンス ルール] セクションの [カテゴリ] ドロップダウン リストで、表示または設定するカテゴリを選択します。 名前、ポリシー使用主体、設定するアクションと一緒にルール グループが表示されます。 以下のオプションを使用できます。

表 4-8 オプションの定義

オプション	定義
[カテゴリ]	設定するスキャナーを選択します。 今回のリリースには 60 種類以上の DLP とコンプライアンス ディクショナリがあるので、電子メール コンテンツが組織の機密およびコンプライアンスに関するポリシーに準拠することが保証されます。 事前に定義されたコンプライアンス ディクショナリには、以下の項目が含まれます。 • 新しい DLP とコンプライアンス ディクショナリが 60 種類追加 • 業界専用のコンプライアンス ディクショナリ（HIPAA、PCI、ソース コード（Java、C++ など））のサポート こうしたディクショナリは以下のように分類されます。 • スコア ベース－しきい値スコアと最大用語数を電子メールが超過するとルールがトリガーされ、誤検知が減少します。 • スコア以外のベース－電子メール メッセージにワードやフレーズが検出されるとルールがトリガーされます。
[新規カテゴリ]	新しい [DLP とコンプライアンス ルール] ディクショナリを作成します。 新しく作成するカテゴリまたは条件はスコア ベース以外のものとなります。
[新規作成]	ユーザーの要件に従って、選択したカテゴリに新しいルール グループを作成します。 この操作は、検出をトリガーする特定のルールを作成してポリシーに適用する場合に行います。
[編集]	選択した [DLP とコンプライアンス] ルールの設定を編集します。
[削除]	[DLP とコンプライアンス] ルールを削除します。 次の場合には、[DLP とコンプライアンス] ルールを削除できません。 • 有効な場合。ルールの選択を解除し、設定を [適用] して [削除] をクリックします。 • 任意のポリシーによって使用されている場合。当該スキャナー設定を使用するポリシーがいくつあるかを把握するには、[Used By（使用主体）] 列を参照してください。

たとえば、[カテゴリ] ドロップダウン リストから [クレジットカード番号] を選択するか、あるいは要件を満たすディクショナリを選択して、使用可能な拡張[ルール グループ] オプションを表示します。

5 ルール グループを新規作成するには、選択したカテゴリの [DLP とコンプライアンス ルール] の [新規作成] をクリックします。

選択したカテゴリの [新しい DLP とコンプライアンス スキャナー ルール] ページが表示されます。

6 ルールの [ルール名] と [説明] を入力します。

7 [このルールを、このカテゴリのルール グループに追加します] を選択し、選択したカテゴリのルール グループに新しいルールを追加します。

8 [次の単語またはフレーズが発見されたらルールをトリガーする] の [単語または語句] に、検索する単語またはフレーズを指定します。 以下のいずれかのオプションを選択します。

- [正規表現] ー 有効にすると、指定した正規表現 (regex) に一致したときにルールがトリガーされます。 正規表現は、単語、文字、文字パターンなどのテキスト文字列を照合する正確かつ簡潔な方法です。

例えば、内容はどのようなものでも、trees、street、backstreet など、「tree」が連続して使用されている文字のシーケンスです。

- 一部のフレーズでは正規表現は無効になっています。
- 詳細については、http://www.regular-expressions.info/reference.html または http://www.zytrax.com/tech/web/regex.htm を参照してください。

- [ワイルドカードを使用する]ー有効にすると、ワイルドカード文字を含む指定したワードまたはフレーズに対して、ルールがトリガーされます（ワイルドカード文字は、ほとんどの場合、本当の文字がわからないとき、または名前全体を入力したくないときに 1 つ以上の文字の代わりに使用します）。
- [次の値で始まる] — 有効にすると、ワードまたはフレーズの先頭を形成する指定されたテキストに対して、ルールがトリガされます。
- [で終わる] — 有効にすると、ワードまたはフレーズの最後の部分を形成する指定されたテキストに対して、ルールがトリガされます。
- [大文字と小文字を区別] — 有効にすると、指定したテキストの大文字と小文字がワードまたはフレーズと一致した場合にルールがトリガされます。

単語またはフレーズと完全に一致するものを検出するには、[次の値で始まる] と [次の値で終わる] の両方のオプションを選択します。

9 [コンテキストに応じた追加のワードまたはフレーズを指定する] を選択します。これは、1 番目のワードまたはフレーズが検出されたときの 2 番目のアクションになります。検出をトリガーする 1 番目のワードまたはフレーズを伴う追加のワードまたはフレーズを指定します。

10 ドロップダウン メニューから、[すべての語句が存在する場合にトリガする]、[いずれかの語句が存在する場合にトリガする]、[どの語句も存在しない場合にトリガする] のいずれかを選択します。

11 [ブロック] を選択し、スキャンするブロックの [文字列に含まれる] の数を指定します。

12 追加のワードまたはフレーズを入力するには、[コンテキストに応じたワードを追加する] をクリックします。

13 [ワードまたはフレーズの指定] でワードまたはフレーズを指定し、いずれかの条件を選択し（手順 7 と同じオプション）、[追加] をクリックします。

14 すべてのファイル カテゴリとそのサブカテゴリを有効にするには、[ファイル形式] で [すべて] を選択します。複数のカテゴリと選択したカテゴリ内でファイルの種類を選択して、照合対象にすることができます。サブカテゴリ セレクターで [すべて] を選択すると、すでに選択されている可能性がある他のすべての選択項目が無視されます。

15 [すべて] を選択しなかった場合は、[選択のクリア] をクリックして、選択したファイルの種類のオプションの選択をすべて解除します。

16 [保存] をクリックして [共有リソース] ページに戻ります。

17 [適用] をクリックして設定を保存します。

組織の Exchange 環境要件に適合するように、DLP とコンプライアンス ルール/ディクショナリが正常に設定されました。

ファイル フィルタリング ルールの構成

新しいルールを作成し、それぞれの名前、種類、またはサイズに基づいてファイルを検出します。

開始する前に

ファイル フィルタリング ルールがトリガーされるのは、ある条件を選択したときに限られます。以下のいずれかのカテゴリに個別のルールを必ず作成してください。

- ファイル名
- ファイル カテゴリ
- ファイル サイズ

このタスクを実行すると、3 種類全部のカテゴリの設定に関する情報が得られます。 組織の Exchange 環境要件に基づき、ファイル フィルタリング ルールのカテゴリを 1 つのみ選択し、各カテゴリに個別のルールを作成します。 1 つのルールに [ファイル名フィルタリング]、[ファイル カテゴリ フィルタリング]、[ファイル サイズ フィルタリング] などの複数の条件が含まれている場合、すべての条件を満たさないとルールはトリガーされません。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] の順にクリックします。

2 [DLP とコンプライアンス ディクショナリ] タブをクリックします。

3 [ファイル フィルタリング ルール] で [新規作成] をクリックします。

4 [ルール名] に一意のルール名を入力します。ルールを簡単に識別でき、その機能がわかるように、ルールにはわかりやすい名前を付けてください。例えば、FilesOver5MB や MPP ファイルのブロックなどです。

5 [アーカイブ ファイル内のアイテムを評価する] を有効にします。

アーカイブ ファイルのスキャンにファイル フィルター ルールを適用できる場合には、このオプションを選択します。 このルールを選択すると、後続のファイル フィルター ルールがアーカイブ ファイルに適用されます。

6 [ファイル フィルタリング ルール] ページでは、以下の項目を使用できます。

表 4-9 オプション定義 ー ファイル名フィルタリング

オプション	定義
[ファイル名フィルタリングを有効にする]	ファイル名でファイルをフィルタリングします。
[ファイル名が一致したらアクションを実行する]	このルールをトリガーするファイルの名前を指定します。 複数のファイル名に一致するワイルドカード文字 (* または ?) を使用できます。 たとえば、任意の Microsoft PowerPoint ファイルをフィルタリングする場合、`*.ppt` と入力します。
[追加]	[ファイル名が一致したらアクションを実行する] で指定したファイル名をファイル名フィルタリング リストに追加します。
[編集]	既存のファイル フィルタリング ルールを編集または変更します。
[削除]	ファイル名をフィルター リストから削除します。 ポリシーで使用されているファイル フィルタリング ルールは削除できません。 [使用主体] 列の値が [0] でないルールは削除できません。 ポリシーからファイル フィルタリング ルールを削除してから [削除] をクリックしてください。

表 4-10 オプション定義ーファイル カテゴリのフィルタリング

オプション	定義
[ファイル カテゴリ フィルタリングを有効にする]	ファイルの種類でファイルをフィルタリングします。
[次のファイル カテゴリのときにアクションを実行する]	このルールに影響を及ぼすファイルの種類を指定します。 ファイルの種類は、カテゴリとサブカテゴリに分かれています。
[ファイル カテゴリ]	ファイルの種類カテゴリを選択します。 ファイルの種類の横にアスタリスク (*) が表示され、選択したファイルの種類がフィルタリングされることを示します。
[サブカテゴリ]	フィルタリングするサブカテゴリを選択します。 複数のサブカテゴリを選択するには、[Ctrl] キーを押しながら[クリック]するか、[Shift] キーを押しながら[クリック]します。 すべてのサブカテゴリを選択するには、[すべて] をクリックします。 直前の選択を取り消すには、[選択のクリア] をクリックします。
[このルールを認識不能なファイル カテゴリに拡張]	カテゴリ リストとサブカテゴリ リストで指定していないファイル カテゴリとサブカテゴリにもこのルールを適用します。

制限付きファイルを含むパスワード保護 .zip ファイルの通過を許可するには、ルール リストの先頭に [パスワードで保護されたバイパス ルール] を追加する必要があります。

表 4-11 オプション定義ーファイル サイズのフィルタリング

オプション	定義
[ファイル サイズ フィルタリングを有効にする]	ファイル サイズでファイルをフィルタリングします。
[次のファイル サイズのときにアクションを実行する]	隣接するテキスト ボックスとドロップダウン リストで値を指定し、以下を選択します。 • [より大きい]ー指定したサイズよりファイルが大きい場合にのみアクションを適用するように指定します。 • [より小さい]ー指定したサイズよりファイルが小さい場合にのみアクションを適用するように指定します。

7 [保存] をクリックして [共有リソース] ページに戻ります。

8 [適用] をクリックしてファイル フィルタリング ルールを作成します。

これで、組織の Exchange 環境の要件に適するようにファイル フィルタリング ルールを正常に作成できました。

タイム スロットの設定

組織の Exchange 環境の要件に基づき、別々のタイム スロットを設定したり、ポリシーに適用可能な既存のタイム スロットを設定します。

[タイム スロット] では、特定のルールが必ずトリガーされる時間を指定できます。例えば、営業時間中の大きなファイルのアップロードやダウンロードを制限することができます。

個別のユーザー、それぞれの所在地、または営業時間に基づき、より多くのタイム スロットを必要とする場合があります。営業時間、営業時間外、週間メンテナンスなどに基づいてより多くのタイム スロットを作成できます。

デフォルトでは、MSME には以下のタイム スロットがあります。

- [常時]
- [平日]
- [週末]

[マスター ポリシー] で使用されるため、デフォルトのタイム スロット [常時] を削除したり編集したりすることはできません。

タスク

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] をクリックします。

[共有リソース] ページが表示されます。

2 [タイム スロット] タブをクリックします。

3 [新規作成] をクリックします。

[タイム スロット] ページが表示されます。

4 [営業時間] や システム メンテナンス（週間） などの一意の タイム スロット名 を入力します。

5 [日付と時刻を選択] で、必要な日数を選択します。

6 [すべての曜日] または [選択した時間] を選択します。

7 [選択した時間] を選択する場合は、ドロップダウン リストから [開始] と [終了] の時間を指定します。

8 [保存] をクリックして [共有リソース] ページに戻ります。

9 [適用] をクリックして設定を保存します。

これで、組織の Exchange 環境の要件に適するようにタイム スロットを正常に設定または作成できました。

ポリシー用コア スキャナー設定の管理

スキャナー オプションを作成または編集し、ポリシーのトリガー時に検出アイテムに実行する適切なアクションを指定します。
使用できるコア スキャナーは以下のとおりです。

- [ウイルス対策スキャナー]
- [DLP とコンプライアンス スキャナー]
- [ファイル フィルタリング]
- [スパム対策]
- [フィッシング対策]

タスク

- 72 ページの「*ウイルス対策スキャナー設定の構成*」
  コンピューター ウイルスやその他のマルウェアを識別、防御、駆除するため、ポリシーの [ウイルス対策スキャナー] 設定を構成します。
- 75 ページの「*DLP とコンプライアンス スキャナー設定の構成*」
  ポリシー内の [DLP とコンプライアンス スキャナー] 設定を構成し、電子メールまたは添付ファイル内の非対応テキスト データを識別して必要なアクションを実行します。
- 77 ページの「*ファイル フィルタリング設定の構成*」
  ファイルの名前、種類、またはサイズに基づいてファイルを検出し、必要なアクションを実行するためにポリシーの設定を構成します。
- 78 ページの「*メール URL レピュテーションを設定する*」
  メール本文で不正な URL を検出するには、[メール URL レピュテーション] で設定を行います。
- 81 ページの「*メールの添付ファイルに対する TIE レピュテーション チェック*」
  MSME に脅威検出機能が追加されました。ゲートウェイ、ハブ、メールボックス レベルで、メールの添付ファイルに TIE レピュテーション チェックを実行できます。
- 83 ページの「*メールの添付ファイルをスキャンするように TIE を設定する*」
  ファイル レピュテーションのカテゴリに基づいて、添付ファイルに TIE レピュテーション チェックを実行します。
- 84 ページの「*スパム対策設定の構成*」
  スパム電子メール メッセージを検出して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 88 ページの「*フィッシング対策設定の構成*」
  スパム対策ルールおよびエンジンを使用してフィッシング詐欺メッセージをブロックし、必要なアクションを実行するためのポリシーの設定を構成します。

ウイルス対策スキャナー設定の構成

コンピューター ウイルスやその他のマルウェアを識別、防御、駆除するため、ポリシーの [ウイルス対策スキャナー] 設定を構成します。

タスク

1 [ポリシー マネージャー] から、ウイルス対策スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [ウイルス対策スキャナ] をクリックします。

4 [アクティブ化] で [有効] を選択し、選択したサブメニュー項目でウイルス対策スキャナーの設定をアクティブにします。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しいスキャナーをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでスキャナーを有効化する時間のタイム スロットを指定できます。

5 [オプション] セクションでは、以下の項目を使用できます。

オプション	定義
[保護レベル (高)]	すべてのファイル、アーカイブ ファイル、未知のウイルス、未知のマクロ ウイルス、大量メーラー、不審なプログラムをスキャンし、すべてのファイルにマクロが含まれないかスキャンします。
[保護レベル (中)]	すべてのファイル、アーカイブ ファイル、未知のウイルス、未知のマクロ ウイルス、大量メーラー、不審なプログラムをスキャンします。
[保護レベル (低)]	デフォルトのファイル タイプ、アーカイブ ファイル、大量メーラー、不審なプログラムのみをスキャンします。
[<新しいオプション セットを作成>]	ウイルス対策スキャナーのカスタム設定を作成します。
[編集]	既存の保護レベルを編集します。

6 スキャナー設定の編集または変更を選択する場合、[インスタンス名] にウイルス対策スキャナー設定インスタンスの一意の名前を入力してください。このフィールドは必須です。

7 [基本オプション] タブの [スキャン対象のファイルを指定する] で、次のいずれかのオプションを選択します。

- [すべてのファイルをスキャンする]ーファイルの種類に関係なく、すべてのファイルをスキャンするように指定します。
- [デフォルトのファイルの種類]ーデフォルトのファイルの種類だけをスキャンするように指定します。
- [定義済みのファイルの種類]ースキャンするファイルの種類を指定します。

8 [スキャナー オプション] で、使用可能な追加スキャナー オプションを選択します。 次のオプションを選択できます。

- [アーカイブ ファイル (ZIP、ARJ、RAR ...) をスキャンする]
- [不明のウイルス ファイルを検索する]
- [未知のマクロ ウイルスを検出]
- [McAfee Global Threat Intelligence ファイル レピュテーションを有効にする] — McAfee Labs が収集した脅威情報を利用して、シグネチャ更新が利用可能になる前に損害や情報漏洩を防止します。オプションから [重大度レベル] を選択します。
- [すべてのファイルでマクロをスキャンする]
- [すべてのマクロを検索し、感染として扱う]
- [文書ファイルからすべてのマクロを削除する]

> [すべてのマクロを検索し、感染として扱う] と [文書ファイルからすべてのマクロを削除する] は連動しています。[すべてのマクロを検索し、感染として扱う] を選択すると、[文書ファイルからすべてのマクロを削除する] オプションが自動的に選択されます。 このオプションを有効にすると、添付ファイルに含まれるすべてのマクロが感染として扱われます。

9 [詳細] タブの [カスタム マルウェア カテゴリ] で、マルウェアとして処理するアイテムを指定します。 マルウェアの種類を選択するには、次の 2 つの方法があります。

- チェックボックスのリストからマルウェアの種類を選択します。
- [特定の検出名] を選択し、マルウェアのカテゴリを入力して、[追加] をクリックします。

> マルウェアのカテゴリ名を入力するときに、パターン マッチングにワイルドカードを使用できます。

10 駆除したアイテムをカスタム マルウェア チェックの対象にしない場合は、[オブジェクトがすでに駆除されている場合はカスタム マルウェア チェックを実行しない] オプションを選択します。

11 [駆除オプション] で、駆除後にゼロ バイトになったファイルの処理を指定します。 以下のいずれかのオプションを選択します。

- [ゼロ バイトのファイルを保持する] — 駆除後にゼロ バイトになったファイルを残しておきます。
- [ゼロ バイトのファイルは削除する] — 駆除後にゼロ バイトになったファイルを削除します。
- [駆除失敗として扱う]ーゼロバイトのファイルは駆除不可能として扱い、駆除失敗時のアクションを適用します。

12 [パッカー] タブで、以下のオプションを選択します。

- [検出を有効にする] — パッカーの検出を有効または無効にします。
- [指定した名前を除外する] — スキャンから除外できるパッカーを指定します。
- [指定した名前だけを含める] — ソフトウェアで検出するパッカーを指定します。
- [追加] — パッカー名をリストに追加します。ワイルドカードを使用して、名前を照合できます。
- [削除] — 追加したパッカー名を削除します。[追加] をクリックすると、このリンクがアクティブになります。

13 [PUP] タブで、以下のオプションを選択します。

- [検出を有効にする]ー不審なプログラムの検出を有効/無効にします。不審なプログラムの検出を設定する前に、免責事項リンクをクリックして内容を読んでください。
- [検出するプログラムの種類を選択する]ーリストにある不審なプログラムの各種類について、検出するか無視するかを指定します。
- [指定した名前を除外する]ースキャンから除外できる不審なプログラムを指定します。例えば、スパイウェア検出を有効にした場合、自動的に無視されるスパイウェア プログラムのリストを作成できます。
- [指定した名前だけを含める]ー自動的に検出される不審なプログラムの種類を指定します。例えば、スパイウェアの検出を有効にし、指定したスパイウェア プログラムだけを検出するようにした場合、それ以外のスパイウェア プログラムはすべて無視されます。
- [追加]ー不審なプログラム名をリストに追加します。ワイルドカードを使用すると、名前を照合できます。
- [削除]ー追加した不審なプログラム名を削除します。[追加] をクリックすると、このリンクがアクティブになります。

McAfee Threat Intelligence の Web サイトには、最新のマルウェア名リストがあります。[Search the Threat Library（脅威ライブラリの検索）] を使用すると、特定のマルウェアに関する情報を表示できます。

14 [保存] をクリックしてポリシー ページに戻ります。

15 [実行するアクション] で、[編集] をクリックします。 以下のタブでは、ウイルス対策スキャナーでウイルス (またはウイルスのような動作) が検出された場合に実行するアクションを指定します。

- [駆除] ー [検出されたウイルスやトロイの木馬を駆除します] を選択して、適切なアクションをアクティブにします。 実行するアクションを、次のオプションから選択します。
  - [ログ]
  - [隔離]
  - [外部送信者に通知する]
  - [内部受信者に通知]

- [管理者に通知]
- [外部受信者に通知する]
- [内部送信者に通知]

- [デフォルトのアクション] ー [次のアクションを実行する] ドロップダウン リストから、アクションを選択します。
  - [アイテムをアラームに置き換える].
  - [組み込み項目の削除]
  - [メッセージを削除する]
  - [通過を許可]

1 番目および 2 番目のアクションの詳細については、『検出に対して実行可能なアクション』を参照してください。

16 対応するアラート ドキュメントを選択するか、[作成] をクリックして新しいアラート ドキュメントを作成します。 [次も] から、実行する追加のアクション タブを選択します。
- [カスタム マルウェア]
- [パッカー]
- [不審なプログラム]

17 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

18 [適用] をクリックし、対象設定をポリシーに構成します。

DLP とコンプライアンス スキャナー設定の構成

ポリシー内の [DLP とコンプライアンス スキャナー] 設定を構成し、電子メールまたは添付ファイル内の非対応テキスト データを識別して必要なアクションを実行します。

タスク

1 [ポリシー マネージャー] で、[DLP とコンプライアンス] スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナーー覧] タブをクリックします。

3 [DLP とコンプライアンス スキャナー] をクリックします。

4 [アクティブ化] で [有効] を選択します。選択したサブメニュー項目の DLP とコンプライアンス スキャナーの設定がアクティブになります。

- デフォルトでは、[DLP とコンプライアンス スキャナー] のすべてのスキャナー設定オプションは無効になっています。
- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しいスキャナーをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでスキャナーを有効化する時間のタイム スロットを指定できます。

5 [オプション] では、次のオプションを選択できます。

- [ドキュメントおよびデータベース形式を含める]ー ドキュメントおよびデータベース形式に非対応コンテンツがないかスキャンします。
- [すべての添付ファイルのテキストをスキャンする] — すべての添付ファイルのテキストをスキャンします。
- [作成] ー ルールがトリガーされたことによって電子メール メッセージのコンテンツが置き換えられた場合に、アラート メッセージを作成します。 詳細については、「アラートを作成する」を参照してください。
- [表示/非表示] — アラート メッセージのプレビューを表示または非表示にします。プレビューが非表示の場合は、このリンクをクリックすると表示されます。プレビューが表示されている場合は、このリンクをクリックすると非表示になります。

6 [DLP とコンプライアンス ルールと関連するアクション] で、[ルールの追加] をクリックします。

[DLP とコンプライアンス ルール] ページが表示されます。

7 [ルールにアクションを指定] で、[言語を選択] ドロップダウン メニューから言語を選択します。

対応しているすべてのロケールのディクショナリを表示し、編集できます。 (対応ロケール: 中国語簡体字、フランス語、ドイツ語、日本語、スペイン語)

たとえば、MSME をドイツ語のロケールにインストールした場合、他の対応ロケールのディクショナリを表示して編集できます。 作成した新しいカテゴリはすべての対応ロケールで使用できます。

8 [ルールにアクションを指定] の [ルール グループの選択] ドロップダウン リストで、1 つ以上のルールに違反した場合にアクションを実行するルール グループを選択します。 [DLP とコンプライアンス スキャナー フレーズ] では、各フレーズのカテゴリごとに[スコア]が設定されています。

一部のルール グループの場合、以下のオプションを指定する必要があります。

- [しきい値スコア]ースキャナーがトリガーされる条件となるしきい値スコアを指定します。
- [最大期間数]ー当該ルール グループがトリガーされる最大回数を指定します。この数を超えるとスキャナーがトリガーされ、指定アクションが実行されます。

計算式は、現在の[しきい値スコア] = [スコア] x 回数 (インスタンス) となります。 値が[しきい値スコア]以上になると、ルールがトリガーされます。

ルールのトリガーにおいて [しきい値スコア] と [最大期間数] がどのように役立つかについて理解するため、Pascal Language ディクショナリの例を考えてみましょう。[DLP と コンプライアンス スキャナー フレーズ] 「PAnsiChar」の [スコア] を 5 に設定したとします。

[ルール グループの選択] で [Pascal Language] ディクショナリを選択した場合、以下の値を設定します。

- [しきい値スコア] = 15
- [最大期間数] = 4

「PAnsiChar」がコード内で 2 回検出される場合、現在のしきい値スコアは 10 になるため、ルールはトリガーされません。

「PAnsiChar」がコード内で 5 回検出される場合、現在のしきい値スコアの計算値は [スコア] x [最大期間数] (5 * 4 = 20) となります。 この値は、定義済みのしきい値スコアよりも大きくなります。 このため、ルールがトリガーされます。

「PAnsiChar」の [スコア] を 8 に変更したとします。「PAnsiChar」というフレーズがコード内で 2 回検出される場合、現在のしきい値スコアは 24 になります。この場合、指定した [しきい値スコア] を超えているためルールがトリガーされます。

複数のルールがある場合、[しきい値スコア] は 1 つのディクショナリの全ルールを組み合わせた値になります。

ルールがトリガーされるのは、値が [しきい値スコア] 以上になるときに限られ、電子メール内でフレーズのインスタンスが [最大期間数] の値を超える場合でもルールはトリガーされません。

9 [検出された場合、次のアクションを実行する:] で、電子メール メッセージの内容が非対応と検出された場合に実行する必要がある DLP とコンプライアンス スキャナーのアクションを選択します。

10 [次も] から、1 つ以上のアクションを選択します。

11 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

12 [適用] をクリックし、対象設定をポリシーに構成します。

ファイル フィルタリング設定の構成

ファイルの名前、種類、またはサイズに基づいてファイルを検出し、必要なアクションを実行するためにポリシーの設定を構成します。

タスク

1 [ポリシー マネージャー] で、[ファイル フィルタリング] スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [ファイル フィルタリング] をクリックします。

4 [アクティブ化] で [有効にする] を選択し、選択したサブメニュー項目でファイル フィルタリング スキャナーの設定をアクティブにします。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- スキャナーをポリシーに追加する場合、[これをいつ適用しますか] ドロップダウン リストでスキャナーを有効化する時間のタイム スロットを指定できます。

5 埋め込まれたメールをスキャンするには、[埋め込みファイルのスキャン] を選択します。

6 [アラートの選択] で、以下をクリックします。

- [作成] ― ルールがトリガーされたことによってメールの添付ファイルが置き換えられた場合に、アラート メッセージを作成します。 詳細については、『アラートを作成する』を参照してください。
- [表示/非表示] — アラート メッセージのプレビューを表示または非表示にします。プレビューが非表示の場合は、このリンクをクリックすると表示されます。プレビューが表示されている場合は、このリンクをクリックすると非表示になります。

7 [ファイル フィルタリング ルールと関連するアクション] で、[使用可能なルール] ドロップダウン メニューの使用可能なルールを選択します。 新しいファイル フィルタリング ルールを作成する場合は、[<新しいルールの作成...>] を選択します。 新しいファイル フィルタリング ルールの作成方法に関する詳細な手順については、『ファイル フィルタリング ルールを設定する』を参照してください。

ファイル フィルタリング ルールは、電子メールに添付されている .exe ファイルなど、制限付きのファイルをブロックします。 パスワードで保護された .zip ファイルに .exe ファイルが含まれている場合、[パスワードで保護されたファイル] の設定で許可していても、ファイル フィルタリング ルールがこのファイルをブロックします。

正規の制限付きファイルが、パスワードで保護された .zip ファイルで送信される場合があります。 .exe ファイルなどの制限付きファイルを含むパスワード保護 .zip ファイルを許可するには、[使用可能なルール] ドロップダウン リストから [パスワードで保護されたバイパス ルール] を追加する必要があります。

このルールはリストの先頭に置いてください。 このルールが別のレベルにある場合には、ルールを削除して [使用可能なルール] ドロップダウン リストからルールを選択します。

ファイル名、種類、サイズなどの各カテゴリに個別のファイル フィルタリング ルールを必ず作成してください。

8 [変更] をクリックし、電子メール メッセージ内のファイル/添付ファイルによってスキャナーがトリガーされると必ず実行されるアクションを指定します。

9 [削除] をクリックし、既存のルールをポリシーから削除します。

10 [適用] をクリックし、対象設定をポリシーに構成します。

メール URL レピュテーションを設定する

メール本文で不正な URL を検出するには、[メール URL レピュテーション] で設定を行います。

有効にすると、MSME はメール本文の URL をスキャンしてレピュテーション スコアを取得します。このスコアと定義済みのしきい値を比較して、該当するアクションを実行します。

組織内に入る前にメール本文から不正な URL が削除されます。 電子メールに複数の URL が存在している場合、その中の 1 つのスコアが定義済みのしきい値を超えていると、設定に従って電子メールにアクションが実行されます。

この機能を有効にすると、サービス拒否 (DoS) 攻撃、フィッシング詐欺リンク、マルウェアが存在する URL、不要な URL からシステムを保護できます。

メール URL レピュテーション機能は次のポリシーで使用できます。

- [オンアクセス]
- [オンデマンド (デフォルト)]、
- [オンデマンド (フル スキャン)]

ソフトウェアのインストール時に選択したオプションに応じて、ポリシーのデフォルトでメール URL レピュテーションが有効または無効になっています。

- [デフォルトの設定] ― すべてのポリシーで無効になっています。
- [拡張設定] ― オンアクセス スキャン ポリシーでのみ有効になっています。

[メール URL レピュテーション] を最初に有効にするときに、URL のローカル キャッシュが McAfee GTI サーバーからダウンロードされます。

URL ごとにローカル データベースに記録されているレピュテーション スコアが確認され、設定に従って適切なアクションが実行されます。 ローカル データベースでレピュテーション スコアが使用できない場合、McAfee GTI サーバーからスコアが取得されます。 McAfee GTI サーバーに定期的に接続され、ローカル データベースが更新されます。

ローカル データベースが 30 日間更新されていない場合、次回の更新処理でデータベース全体がダウンロードされます。 それ以外の場合は差分更新になります。 デフォルトでは、ローカル データベースは 1 日に 1 回更新されます。 データベースの保存場所は変更できません。

サーバーがインターネットに直接接続する必要があるため、ePolicy Orchestrator 経由でローカル データベースを更新することはできません。 ただし、スパム対策ルールのダウンロードにプロキシ サーバーを使用している場合、URL データベースのダウンロードにも同じ設定を使用できます。

タスク

1 [ポリシー マネージャー] で、[メール URL レピュテーション] のスキャナーが存在するサブメニュー項目を選択します。

[メール URL レピュテーション] は、[オンアクセス]、[オンデマンド (デフォルト)]、[オンデマンド (フル スキャン)] ポリシーでのみ使用できます。

2 [マスター ポリシー] または設定する [サブポリシー] をクリックします。[全スキャナー覧] タブをクリックして、[メール URL レピュテーション] をクリックします。

3 [アクティブ化] で、[有効] を選択します。

- サブポリシーの設定を構成する場合、[親ポリシーからの設定を使用] を選択すると親ポリシーから設定を継承できます。
- スキャナーをポリシーに追加する場合、[これをいつ適用しますか] ドロップダウン リストでスキャナーを有効にする時間を指定できます。

4 [オプション] ドロップダウン メニューから次を選択できます。

- [デフォルトのメール URL 設定] ― デフォルトのしきい値を適用します。
- [新しいオプション セットを作成] ― 必要に応じて、しきい値を定義します。

既存の設定を編集する場合には、[インスタンス名] にスキャナーの設定に固有の名前を入力してください。

5 スキャナーの設定を削除するには、[新しいオプション セットを作成] を選択します。

6 [メール URL レピュテーション] ページで次の値を定義し、[保存] をクリックします。

- [インスタンス名]
- [高い方の URL レピュテーションしきい値]
- [低い方の URL レピュテーションしきい値]
- [電子メール 1 通あたりの URL の最大数]

[高い方の URL レピュテーションしきい値] の値は、[低い方の URL レピュテーションしきい値] の値よりも常に大きくする必要があります。

URL が複数回出現する場合、出現回数に関係なく、この URL は 1 つとして計算されます。 たとえば、電子メールに 50 個の URL があり、その中の 1 つが 20 個あるとすると、URL の合計は 50 ではなく 31 となります。

7 [実行するアクション] セクションで [編集] をクリックして、アクションを定義します。

デフォルトの設定を使用することもできます。

8 [メール URL レピュテーションのアクション] ページで、[メール URL レピュテーション スコアが高い方のしきい値を超えている場合]、[メール URL レピュテーション スコアが低い方のしきい値を超えている場合]、[メール URL の参照回数が制限を超えている場合] の設定を定義します。

a [次のアクションを実行] ドロップダウン リストから、以下のいずれかを選択します。

- [アイテムをアラームに置き換える].
- [メッセージを削除する].
- [通過させる].

[アイテムをアラームに置き換える] を選択した場合には、アラームの形式を選択します。

- [デフォルトのメール URL レピュテーション アラート] — デフォルトのアラート メッセージを使用します。
- [作成] — 必要に応じて、アラート メッセージを定義します。 [アラート名] に固有の名前を入力して、アラート メッセージを定義します。[表示] ドロップダウン リストからテキストの形式を定義し、[保存] をクリックします。

アラートはテキスト形式で保存するようにしてください。他の形式にすると、メール クライアントによっては正しく表示されない場合があります。

b [次も] セクションで、次のオプションを定義します。

- [ログ]
- [隔離]
- [隔離された電子メールの転送]
- [管理者に通知]
- [内部送信者に通知]
- [外部送信者に通知する]
- [内部受信者に通知]
- [外部受信者に通知する]

各オプションの定義については、「検出時に実行可能なアクション」を参照してください。

9 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

10 [適用] をクリックし、これらの設定をポリシーに実装します。

検出された URL は、[メール URL レピュテーション] ページの [検出アイテム] で確認できます。 [結果の表示] セクションで、検出された URL のリストを確認できます。 [禁止する語句] 列の [ブロックされた URL] をクリックして、詳細ビューを開きます。

高い方または低い方の URL レピュテーションしきい値の例

[高い方の URL レピュテーションしきい値] に 80 を設定し、[低い方の URL レピュテーションしきい値] に 50 を設定します。 URL のレピュテーション スコア:

GTI レピュテーション スコア	アクション
80 より大きい	メール URL レピュテーションの設定に従ってアクションを実行します。
50 より小さい	MSME はこの URL を含む電子メールを許可します。
50 から 80	MSME は、不審な URL と見なし、設定に従ってアクションを実行します。

しきい値に [非常に疑わしい] を設定すると、最も危険な大半の URL が検出されます。 しきい値を低くすると、誤検知が増える可能性があります。 誤検知 ― データベースで不正な可能性があると評価された URL が実際には正規の URL である場合。

メールの添付ファイルに対する TIE レピュテーション チェック

MSME に脅威検出機能が追加されました。ゲートウェイ、ハブ、メールボックス レベルで、メールの添付ファイルに TIE レピュテーション チェックを実行できます。

TIE とは

Threat Intelligence Exchange は、ファイルに対して総合的なレピュテーション チェックを行い、脅威の拡散を防ぎます。これにより、保護能力と検出能力を強化することができます。 TIE サーバーは、ゲートウェイ、ハブ、メールボックス レベルで添付ファイルを迅速に分析します。 Threat Intelligence Exchange の詳細については、『Threat Intelligence Exchange 2.0 製品ガイド』を参照してください。

TIE レピュテーションには次の 2 つの種類があります。

- 証明書レピュテーション
- ファイル レピュテーション

TIE は、まず証明書のレピュテーション スコアを確認します。 証明書のレピュテーションが「不正なことが確認されている」の場合にのみ、ファイル レピュテーション スコアが使用されます。

MSME が TIE を使用する方法

ポリシー設定で TIE を有効にし、ファイル フィルタリング ルールを適用すると、MSME が TIE サーバーに接続し、添付ファイルのレピュテーションを確認します。 TIE のファイル レピュテーションに基づき、スコアがいずかのカテゴリにマッピングされます。MSME は、カテゴリに定義された設定に従ってアクションを実行します。

- 信頼できることが確認されている ― 99
- 信頼できる可能性が非常に高い ― 85
- 信頼できる可能性がある ― 70
- 不明 ― 50
- 不正な可能性がある ― 30
- 不正な可能性が非常に高い ― 15
- 不正なことが確認されている ― 1

特定のカテゴリのアクションを設定すると、TIE レピュテーション スコアがこのカテゴリよりも下回っているすべてのカテゴリに同じアクションが適用されます。 デフォルトでは、[次のレベル以下の場合にアクションを実行する] は [不正な可能性がある] に設定されています。

たとえば、[次のレベル以下の場合にアクションを実行する] を [不明] に設定し、スコアが 50 のファイルに対するアクションを [アラートに置き換える] を設定すると、TIE レピュテーション スコアが 50 以下のすべての添付ファイルがアラート メッセージに置換されます。 アラートに 2 番目のアクションを選択することもできます。

レピュテーション スコアはローカルに保存され、MSME は最新のローカル キャッシュを使用してレピュテーションを確認します。

TIE を無効にすると、ポリシーの設定に従ってスキャン アクションが実行されます。 TIE を有効にしても TIE サーバーに接続できず、ローカル キャッシュにファイルの情報がない場合には、TIE のレピュテーション チェックはスキップされ、ポリシーの設定に従ってメールがスキャンされます。

レピュテーション スコアのマッピングについては、『TIE 製品ガイド』を参照してください。

MSME が TIE レピュテーション チェックに送信するのは、次の種類のファイルです。

- exe
- pdf
- Microsoft Office 文書

対応するファイルの種類については、KB89578 を参照してください。

圧縮されたファイルがメールに添付されている場合、圧縮ファイルが展開され、対応する種類のファイルだけが TIE に送信され、レピュテーション チェックが実行されます。 対応する圧縮ファイルの種類については、KB89577 を参照してください。

他の種類のファイルと TIE レピュテーション チェックの実行後は、MSME がポリシーの設定に従って添付ファイルをスキャンします。 TIE 検出で隔離されたアイテムを解放すると、ファイルにはウイルス スキャンだけが実行されます。 TIE で検出されたファイル数と ATD に送信されたファイル数は [ダッシュボード] ページで確認できます。

Advanced Threat Defense レピュテーションの使用

ファイルの特定のレピュテーション カテゴリと添付ファイルのサイズに Advanced Threat Defense の検出を有効にすることもできます。

TIE のファイル レピュテーションの実行後、TIE はレピュテーション スコアを戻しますが、ファイルの詳細な分析を推奨する場合があります。 その場合、設定されたカテゴリとファイル サイズに基づき、MSME がファイルを Advanced Threat Defense に送信します。 ファイルのレピュテーション スコアが変更されると、ローカル キャッシュが新しいレピュテーション スコアで更新されます。 新しいスコアは次の検索で使用されます。 [次のレベル以下の場合にアクションを実行する] のデフォルトは [不正な可能性がある] で [ファイル サイズ] は 8 MB です。

MSME で利用する場合の TIE サーバーの推奨設定

McAfee では、次のことをお勧めします。

- セカンダリ構成に TIE サーバーを配備し、MSME からのすべての TIE レピュテーション要求を Exchange Server と同じデータセンター内で処理します。 これにより、TIE サーバーが専用のインフラで処理する 1 秒あたりの添付ファイル数を最大にすることができます。

  TIE レピュテーション チェックに送信される添付ファイルを処理するため、最大で 2 つの TIE 要求が呼び出されます。

- MSME サーバーがレピュテーションをローカル キャッシュに格納すると、レピュテーション トラフィックの量が減少します。 ただし、サーバーが再起動すると MSME がローカル キャッシュをクリアするため、トラフィックが急増する可能性があります。
- MSME のダッシュボード カウンターで MSME からの要求数を予測します。 TIE サーバーに対する 1 秒あたりの要求数を確認するには、McAfee ePO の [サーバー設定] で [TIE サーバー トポロジ管理] ページを開きます。このページで、[パフォーマンス ステータス] の [スループット] に要求数が表示されます。 また、[TIE サーバー データのクリーンアップ] ページの [TIE サーバーで確認された新しいファイル] でも確認できます。

メールの添付ファイルをスキャンするように TIE を設定する

ファイル レピュテーションのカテゴリに基づいて、添付ファイルに TIE レピュテーション チェックを実行します。

タスク

1 製品のインターフェースで、[設定と診断] 、 [TIE の設定] の順にクリックします。

2 [次のレベル以下の場合にアクションを実行する] ドロップダウン リストから項目を選択します。

- [信頼できることが確認されている] ー ファイルのレピュテーションは 99 です。
- [信頼できる可能性が非常に高い] ー ファイルのレピュテーションは 85 です。
- [信頼できる可能性がある] ー ファイルのレピュテーションは 70 です。
- [不明] ー ファイルのレピュテーションは 50 です。
- [不正な可能性がある] ー ファイルのレピュテーションは 30 です。

  デフォルトでは、[不正な可能性がある] が選択されています。

- [不正な可能性が非常に高い] ー ファイルのレピュテーションは 15 です。
- [不正なことが確認されている] ー ファイルのレピュテーションは 1 です。

3 [次のアクションを実行] で、必要に応じて設定を定義します。

- [アイテムをアラートに置き換える] ー 項目をアラート メッセージで置き換え、[次も] の定義に従ってロギング、隔離または通知を行います。
- [組み込み項目の削除] ー メールの添付ファイルを削除し、[以下も実行] の定義に従ってロギング、隔離または通知を行います。
- [組み込み項目の削除] ー メールの添付ファイルを削除し、[以下も実行] の定義に従ってロギング、隔離または通知を行います。

4 [以下も実行] で、必要に応じて設定を行います。

- [ログ]
- [隔離]
- [隔離メールの転送]
- [管理者に通知]
- [内部送信者に通知]
- [外部送信者に通知する]
- [内部受信者に通知]
- [外部受信者に通知する]

5 [次のレベル以下の場合にファイルを ATD に送信する] で、Advanced Threat Defense レピュテーションのカテゴリとファイル サイズを選択します。

スパム対策設定の構成

スパム電子メール メッセージを検出して必要なアクションを実行するため、ポリシー内の設定を構成します。

タスク

1 [ポリシー マネージャー] で、[スパム対策] スキャナーが含まれるサブメニュー アイテム [ゲートウェイ] を選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [スパム対策] をクリックします。

4 [アクティブ化] で、[有効にする] を選択し、選択したサブメニュー項目のスパム対策スキャナ設定をアクティブにします。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しいスキャナーをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでスキャナーを有効化する時間のタイム スロットを指定できます。

5 [オプション] ドロップダウン リストで、既存のスキャナー設定または [<新しいオプション セットの作成>] を選択します。

[スパム対策設定] ページが表示されます。

6 [インスタンス名] で、スパム対策スキャナ設定インスタンスの一意の名前を指定します。このフィールドは必須です。

7 [オプション] タブで [スコア] の以下のフィールドに値を入力します。

- [高スコアしきい値] — 総合スパム スコアが 15 以上の場合。
- [中程度のスコアのしきい値]ー総合スパム スコアが 10 ～ 15 の場合。
- [低いスコアのしきい値]ー総合スパム スコアが 5 ～ 10 の場合。

スパム スコアのデフォルト値を使用するには、[デフォルトを使用する] オプションを選択します。これらのデフォルト設定は、高いスパム検出率と低い誤検知率との間でバランスを保つように入念に最適化されています。万一これらの設定を変更する必要がある場合は、テクニカル サポートからの技術通知を参照できます。

8 [レポート] で、[スパム レポートしきい値] ドロップダウン リストから、[高]、[中]、[低]、または [カスタム] を選択して電子メール メッセージをスパムとしてマークする時点を指定します。

9 [カスタム スコア] では、電子メール メッセージをスパムとしてマークする特定のスパム スコアを入力します。このフィールドが有効になるのは、[スパム レポートしきい値] ドロップダウン リストから [カスタム] オプションを選択した場合に限られます。

10 [スパム メッセージの件名にプレフィックスを追加する] オプションを必要に応じて選択または選択解除します。

11 [スパム スコア指標の追加] ドロップダウン リストから、以下のいずれかを選択します。

- [なし] — 電子メール メッセージのインターネット ヘッダーにスパム スコア指標を追加しません。
- [スパム メッセージのみ] — スパムである電子メール メッセージのインターネット ヘッダーにのみスパム スコア指標を追加します。
- [非スパム メッセージのみ] — スパムでない電子メール メッセージのインターネット ヘッダーにのみスパム スコア指標を追加します。
- [すべてのメッセージ] — すべての電子メール メッセージのインターネット ヘッダーにスパム スコア指標を追加します。

スパム スコア指標は、スパム レポートで使用される記号で、電子メール メッセージのインターネット ヘッダーに付加され、電子メール メッセージに含まれているスパムの度合いを示します。

12 [スパム レポートの添付] ドロップダウン リストから、以下のいずれかを選択します。

- [なし] — 電子メール メッセージにスパム スコア指標を表示しません。
- [スパム メッセージのみ] — スパムである電子メール メッセージにのみスパム レポートを追加します。
- [非スパム メッセージのみ] — スパムでない電子メール メッセージにのみスパム レポートを追加します。
- [すべてのメッセージ] — すべての電子メール メッセージにスパム レポートを追加します。

13 [詳細レポート] を選択または選択解除して、詳細レポートが必要かどうかを指定します。詳細レポートには、トリガーされたスパム対策ルールの名前および説明が含まれます。

[スパム レポートの添付] に [なし] を選択すると、[詳細レポート] が無効になります。

14 [詳細] タブでは、以下のオプションを使用します。

- [スキャンする最大メッセージ サイズ（KB）]—電子メールのスキャン可能な最大メッセージ サイズをキロバイトで指定します。通常のスパム メールのサイズは小さいのですが、サイズは 999,999,999 キロバイトまで入力できます。デフォルト値は 250 KB です。
- [スパム ヘッダーの最大幅 (バイト)] — スパム メールのメッセージ ヘッダーの最大サイズをバイトで指定します。指定可能な最小ヘッダー幅は 40 文字で、最大は 999 文字です。デフォルト値は 76 です。

  スパム送信者は、自身で利用するための余分な情報をヘッダーに追加することがよくあります。

- [レポートするルールの最大数] — スパム レポートに含めることのできるスパム対策ルールの最大数を指定します。指定可能なルールの最小値は 1 で、最大値は 999 文字です。デフォルト値は 180 です。
- [ヘッダー名] — 電子メール ヘッダーに別の名前を指定します。電子メール メッセージを追跡して、それらのメッセージにルールを適用する際に、この電子メール ヘッダーとそのヘッダー値 (以下を参照) を使用できます。これらのフィールドはオプションで、40 文字まで入力できます。
- [ヘッダー値] — 電子メール ヘッダーに別の値を指定します。
- [ヘッダーの追加]—ヘッダーをどの電子メール メッセージにも追加しない、すべての電子メール メッセージに追加する、スパムである電子メール メッセージにのみ追加する、スパムでない電子メール メッセージにのみ追加する、のいずれかを指定します。
- 必要に応じて、[メールがスパムでない場合は代替ヘッダー名を使用する] オプションを選択または選択解除します。

15 [メール リスト] タブの [ブラックリストに含まれる送信者]、[ホワイトリストに含まれる送信者]、[ブラックリストに含まれる受信者]、および [ホワイトリストに含まれる受信者] で、ブラックリストとホワイトリストに含まれている送信者と受信者の電子メール アドレスを入力します。

電子メール アドレスがブラックリストに入っている送信先や送信元の電子メール メッセージは、スパムらしき特性が含まれていない場合でもスパムとして処理されます。ホワイトリストに登録されている電子メール アドレスへ送信される、またはホワイトリストに登録されている電子メール アドレスから送信される電子メール メッセージは、スパムに似た特性を含んでいても、スパムとして処理されません。

電子メール アドレスをリストに追加するには、[追加] をクリックします。また、アドレスが有効であるかどうかを指定するには、各アドレスの横にあるチェック ボックスをクリックします。電子メール アドレスをリストから削除するには、[すべて削除] をクリックします。同じ電子メール アドレスを複数回追加することはできません。ワイルドカード文字を使用すると、複数のアドレスを照合できます。

16 [ルール] タブで、ルール名を入力し [ルールの有効化] を選択してアクティブにします。使用可能なルールのリストを表示するには、[追加] をクリックします。

デフォルトのスパム対策設定に戻すには、[リセット] をクリックします。

17 このリストで、各ルールに対して [編集] をクリックしてルールを変更します。

18 ルールを削除するには、[削除] をクリックします。

19 [保存] をクリックしてポリシー ページに戻ります。

20 [スパムが検出された場合に実行するアクション] で、[編集] をクリックします。以下のタブでは、スパム対策スキャナーでスパムが検出された場合に実行するアクションを指定します。

- [高いスコア]
- [中程度のスコア]
- [低いスコア]

21 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

22 [適用] をクリックし、対象設定をポリシーに構成します。

タスク

- 87 ページの「*ブラックリストとホワイトリストのインポートまたはエクスポート*」
  バックアップまたは他の Exchange サーバーでの使用のためにブラックリストとホワイトリストをインポート/エクスポートします。
- 87 ページの「*スプーフィング対策を使用する*」
  なりすましメールは、ユーザーを騙すためによく利用される手口です。攻撃者は、送信者のメール アドレスを偽装し、ユーザーにメールを開かせようとします。偽物とは気付かずにメールを開いてしまい、返信してしまうユーザーも少なくありません。
- 88 ページの「*スプーフィング対策を設定する*」
  スプーフィング対策を有効にして、なりすましメールからシステムを保護します。

ブラックリストとホワイトリストのインポートまたはエクスポート

バックアップまたは他の Exchange サーバーでの使用のためにブラックリストとホワイトリストをインポート/エクスポートします。

タスク

1 [ポリシー マネージャー] で、スパム対策スキャナーが含まれているサブメニュー アイテムの [ゲートウェイ] を選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [スパム対策] をクリックします。

4 [オプション] で [ブロック リストと許可リスト] のリンクをクリックします。

[スパム対策設定] ページが表示されます。

5 [メール リスト] タブをクリックします。

6 以下から必要なリストを選択します。

- [ブラックリストに含まれる送信者]
- [ホワイトリストに含まれる送信者]
- [ブラックリストに含まれる受信者]
- [ホワイトリストに含まれる受信者]

7 リストをインポートするには、[インポート] をクリックします。ポップアップ ウィンドウで [参照] をクリックし、必要な `.cfg` ファイルに移動して、[OK] をクリックします。

8 リストをエクスポートするには、[エクスポート] リンクをクリックします。

データベースからリストを削除するには、[削除] をクリックします。

9 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

スプーフィング対策を使用する

なりすましメールは、ユーザーを騙すためによく利用される手口です。攻撃者は、送信者のメール アドレスを偽装し、ユーザーにメールを開かせようとします。偽物とは気付かずにメールを開いてしまい、返信してしまうユーザーも少なくありません。

MSME は、Internet Engineering Task Force の Sender Policy Framework (SPF) を利用してスプーフィング対策をサポートしています。 SPF フレームワークは、メールでのドメイン名の使用を規定する RFC 7208 をベースにしています。

送信者のドメインを SPF で評価し、結果を次のように分類します。

- なし
- ニュートラル
- パス
- エラーまたはハード エラー
- ソフト エラー
- 一時エラー
- 永続エラー

SPF フィルターを使用すると、ソフト エラーまたはハード エラーのアクションを設定できます。 誤検知を減らすため、MSME では、残りのカテゴリをパスとみなします。 SPF を有効にすると、[Received-SPF] で SPF の結果を確認できます。

スプーフィング対策を設定する

スプーフィング対策を有効にして、なりすましメールからシステムを保護します。

開始する前に

Exchange Server に McAfee Anti-spam コンポーネントがインストールされている必要があります。

タスク

1 [設定と診断] 、 [スパム対策] の順に移動します。

2 [SPF フィルター] セクションで [有効] を選択します。

3 必要に応じて、[ハード エラー] と [ソフト エラー] にアクションを設定します。

- [通過を許可する] ― 受信者にメールを送信します。
- [通過を許可して隔離する] ― 受信者にメールを送信しますが、隔離されたアイテムにコピーを残します。
- [メールを拒否して隔離する] ― メールをブロックして隔離します。

このオプションを有効にすると、スプーフィング対策が DNS サーバーにクエリーを実行したときに、製品のパフォーマンスが低下する可能性があります。この機能はネットワークの待機時間に依存しています。

フィッシング対策設定の構成

スパム対策ルールおよびエンジンを使用してフィッシング詐欺メッセージをブロックし、必要なアクションを実行するためのポリシーの設定を構成します。

タスク

1 [ポリシー マネージャー] で、[フィッシング対策] スキャナーが含まれるサブメニュー アイテム [ゲートウェイ] を選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [フィッシング対策] をクリックします。

4 [アクティブ化] で、[有効にする] を選択し、選択したサブメニュー アイテムのフィッシング対策スキャナー設定をアクティブにします。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しいスキャナーをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでスキャナーを有効化する時間のタイム スロットを指定できます。

5 [オプション] ドロップダウン リストで、既存のスキャナー設定または [<新しいオプション セットの作成>] を選択します。

[フィッシング対策設定] ページが表示されます。

6 [インスタンス名] で、フィッシング対策スキャナー設定インスタンスの一意の名前を指定します。このフィールドは必須です。

7 [レポート オプション] で、以下のオプションを必要に応じて選択または選択解除します。

- [フィッシング メッセージの件名にプレフィックスを追加する]－フィッシング詐欺が疑われるすべての電子メール メッセージの件名の先頭にテキストを追加するように指定します。
- [フィッシング インジケーター ヘッダーをメッセージに追加する]－フィッシング詐欺が疑われるすべての電子メール メッセージのインターネット ヘッダーにフィッシング指標を追加するかどうかを指定します。
- [フィッシング レポートを添付する]－フィッシング レポートを生成し、フィッシング メールとして検出された電子メール メッセージに添付するかどうかを指定します。
- [詳細レポート]－トリガーされたフィッシング対策ルールの名前と詳しい説明を電子メール メッセージに含めるかどうかを指定します。このオプションは、[フィッシング レポートを添付する] オプションを選択した場合にのみ使用できます。

8 [保存] をクリックしてポリシー ページに戻ります。

9 [実行するアクション] で、[編集] をクリックし、フィッシングが検出された場合に実行するフィッシング対策スキャナ アクションを指定します。

10 [保存] をクリックして設定を適用し、ポリシー設定ページに戻ります。

11 [適用] をクリックし、対象設定をポリシーに構成します。

ポリシー用フィルター設定の管理

フィルター オプションを有効化または無効化し、ポリシーのトリガー時に検出アイテムに実行する適切なアクションを指定します。
使用できるフィルターは以下のとおりです。

- [破損したコンテンツ]
- [保護されたコンテンツ]
- [暗号化されたコンテンツ]
- [署名付きのコンテンツ]
- [パスワードで保護されたファイル]
- [メール サイズによるフィルタリング]
- [スキャナーの制御]
- [MIME メールの設定]
- [HTML ファイル]

タスク

- 90 ページの「*破損したコンテンツ設定の構成*」
  破損したコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 91 ページの「*保護されたコンテンツ設定の構成*」
  保護されたコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 91 ページの「*暗号化されたコンテンツ設定の構成*」
  暗号化されたコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 92 ページの「*署名付きのコンテンツ設定の構成*」
  署名付きのコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 92 ページの「*パスワードで保護されたファイル設定の構成*」
  パスワードで保護されたアーカイブを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 93 ページの「*メール サイズによるフィルタリング設定の構成*」
  ポリシーのメール サイズによるフィルタリング設定により、電子メールのサイズ、添付ファイル数、添付ファイル サイズに基づいて電子メールが検出されます。
- 94 ページの「*スキャナーの制御設定の構成*」
  階層の深さ、展開したファイル サイズ、許容可能な最長スキャン時間、電子メールのスキャン日時を定義するポリシーの設定を構成します。
- 95 ページの「*IP アドレスを手動でブロックする*」
  IP アドレスのレピュテーションに関係なく、特定の IP アドレスまたは IP アドレスの範囲から組織へのメール送信をブロックできます。 このオプションを有効にするには、次のレジストリを更新する必要があります。
- 96 ページの「*MIME メール設定の構成*」
  暗号化された MIME メッセージを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
- 98 ページの「*HTML ファイル設定の構成*」
  要素のスキャンや、電子メール内の HTML コンポーネントにある ActiveX、Java アプレット、VBScript などの実行ファイルの削除を行うポリシーの設定を構成します。

破損したコンテンツ設定の構成

破損したコンテンツを含む電子メールを識別して必要なアクションを実行するため､ポリシー内の設定を構成します。

一部の電子メール メッセージのコンテンツは破損する可能性があり､スキャンできません。破損したコンテンツのポリシーによって、破損したコンテンツを含む電子メール メッセージを検出したときの処理方法が指定されます。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [破損したコンテンツ] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [アクション] で、[編集] をクリックして、破損したコンテンツが検出された場合に実行するフィルタ アクションを指定します。

5 [保存] をクリックしてポリシー ページに戻ります。

6 [適用] をクリックし、対象設定をポリシーに構成します。

保護されたコンテンツ設定の構成

保護されたコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
保護されたコンテンツのポリシーには、保護されたコンテンツを含む電子メール メッセージを検出したときの処理方法を指定します。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [保護されたコンテンツ] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [アクション] で、[編集] をクリックして、保護されたコンテンツが検出された場合に実行するフィルタ アクションを指定します。

5 [保存] をクリックしてポリシー ページに戻ります。

6 [適用] をクリックし、対象設定をポリシーに構成します。

暗号化されたコンテンツ設定の構成

暗号化されたコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。
不正なユーザーによるアクセスを防ぐため、電子メール メッセージを暗号化できます。暗号化されたコンテンツは、**鍵**と数学的な暗号化アルゴリズムを使用して復号化します。暗号化されたコンテンツのポリシーによって、暗号化された電子メール メッセージを検出したときの処理方法が指定されます。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [暗号化されたコンテンツ] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [アクション] で、[編集] をクリックして、暗号化されたコンテンツが検出された場合に実行するフィルタ アクションを指定します。

5 [保存] をクリックしてポリシー ページに戻ります。

暗号化されたコンテンツの設定は、内部電子メールと暗号化されたインターネット電子メール メッセージに適用されます。

6 [適用] をクリックし、対象設定をポリシーに構成します。

署名付きのコンテンツ設定の構成

署名付きのコンテンツを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。

電子的に情報を送信すると、意図的かどうかにかかわらず、情報が変えられてしまうことがあります。この解決策として、一部の電子メール ソフトウェアでは電子署名（手書きの署名を電子形態にしたもの）が使用されます。

電子署名は送信者のメッセージに追加される情報で、送信者とメッセージ内の情報の識別と認証を行います。電子署名は暗号化され、データ固有のサマリ情報のように機能します。通常は、受信した電子メール メッセージの末尾に、文字と数字が長く羅列されます。その後、電子メール ソフトウェアが送信者のメッセージに含まれた情報を再検査して電子署名を作成します。作成した書名が元の署名と同じ場合、データは変更されていません。

電子メール メッセージにウイルスや不良コンテンツが含まれている場合や、電子メール メッセージが大き過ぎる場合、ソフトウェアによってメッセージの一部が駆除または削除される場合があります。電子メール メッセージは有効で読むこともできますが、元の電子署名は「壊れて」います。電子メール メッセージの内容は他の方法で変更されている可能性もあるため、受信者はその内容を信じることはできません。署名付きのコンテンツのポリシーによって、電子署名付きの電子メール メッセージの処理方法が指定されます。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [署名付きのコンテンツ] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [アクション] で、[編集] をクリックして、署名付きのコンテンツが検出された場合に実行するフィルタ アクションを指定します。

5 [保存] をクリックしてポリシー ページに戻ります。

署名付きのコンテンツの設定は、署名付きのインターネット電子メールと添付ファイルに適用できます。

6 [適用] をクリックし、対象設定をポリシーに構成します。

パスワードで保護されたファイル設定の構成

パスワードで保護されたアーカイブを含む電子メールを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。

パスワードで保護されたファイルは、パスワードなしではアクセスできないため、スキャンできません。 パスワードで保護されたファイルのポリシーによって、パスワードで保護されたファイルを含む電子メール メッセージの処理方法が指定されます。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [パスワードで保護されたファイル] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [アクション] で、[編集] をクリックして、パスワードで保護されたファイルが含まれている電子メール メッセージが検出された場合に実行するフィルタ アクションを指定します。

アクションに [通過させる] を設定した場合、[ファイル フィルタリング] スキャン設定の [ファイル フィルタリング ルールと関連するアクション] で [パスワードで保護されたバイパス ルール] がリストの先頭にある必要があります。 このルールが別のレベルにある場合には、ルールを削除して [使用可能なルール] ドロップダウン リストからルールを選択します。

5 [保存] をクリックしてポリシー ページに戻ります。

6 [適用] をクリックし、対象設定をポリシーに構成します。

メール サイズによるフィルタリング設定の構成

ポリシーのメール サイズによるフィルタリング設定により、電子メールのサイズ、添付ファイル数、添付ファイル サイズに基づいて電子メールが検出されます。

開始する前に

[オンアクセス設定] ページで、[受信メールをスキャン] オプションと [送信メールをスキャン] オプションを選択します。

[ゲートウェイ] ポリシーと [オンアクセス] ポリシーでメール サイズのフィルタリング設定を別々に行うこともできます。 受信メールの設定を [ゲートウェイ] で、送信メールの設定を [オンアクセス] で行います。 例:

- 6 個以上のファイルが添付されている受信メールをブロックするには、[ゲートウェイ] ポリシーで [メール サイズ フィルタリング] に値を設定します。
- 4 個以上のファイルが添付されている送信メールをブロックするには、[オンアクセス] ポリシーで [メール サイズ フィルタリング] に値を設定します。

オンアクセス スキャンのメール サイズ フィルタリングは、メールボックス サーバー役割に使用できませんん。

タスク

1 [ポリシー マネージャー] で、ウイルス対策スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 必要に応じて、[オンアクセス] または [ゲートウェイ] でポリシーを選択します。

3 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

4 [メール サイズ フィルタリング] をクリックします。

5 [アクティブ化] で [有効] を選択し、選択したサブメニュー アイテムの電子メール サイズ フィルター設定をアクティブにします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

6 [オプション] では、次のオプションを選択できます。

- [デフォルト設定] — デフォルトで使用されるメール サイズ オプション セットの概要を表示します。
- [デフォルトのゲートウェイ設定] — ゲートウェイ ポリシーで使用されるデフォルトのメール サイズ オプションの概要を表示します。
- [<新しいオプションのセットの作成>] — メール サイズ フィルタリングのオプションを設定します。 オプションは次のとおりです。
  - [インスタンス名] — メール サイズ フィルタ設定インスタンスの一意の名前を入力します。このフィールドは必須です。
  - [メール全体の最大サイズ（KB）]ー電子メール メッセージの最大サイズをキロバイトで指定します。値は 2 KB ～ 2 GB の範囲で指定でき、デフォルト値は 20,000 KB です。
  - [添付ファイルの最大サイズ（KB）]ー電子メール メッセージの添付ファイルの最大サイズをキロバイトで指定します。値は 1 KB ～ 2 GB の範囲で指定でき、デフォルト値は 4,096 KB です。
  - [添付ファイルの最大数]ー電子メール メッセージに添付できる添付ファイルの最大数を指定します。最高 999 まで指定でき、デフォルト値は 25 です。
- [編集] — 選択したオプション セットを編集します。

7 [アクション] で、[編集] をクリックします。 以下のオプションの指定設定を値が超えると実行されるメール サイズ フィルター アクションを指定します。

- [メッセージ サイズ]
- [添付ファイルのサイズ]
- [添付ファイル数]

8 [保存] をクリックして、ポリシー ページに戻ります。

内部メールは、メール サイズ フィルタリング ルールで検出されません。

スキャナーの制御設定の構成

階層の深さ、展開したファイル サイズ、許容可能な最長スキャン時間、電子メールのスキャン日時を定義するポリシーの設定を構成します。

タスク

1 [ポリシー マネージャー] で、スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [スキャナー コントロール] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [オプション] ドロップダウン リストで、[<新しいオプションのセットの作成>] をクリックします。

5 [インスタンス名] で、スキャナ コントロール フィルタ設定インスタンスの一意の名前を入力します。このフィールドは必須です。

6 [入れ子の最大レベル] で、添付ファイルに含まれている圧縮ファイル内にさらに他の圧縮ファイルが含まれている場合、どの深さのレベルまでスキャンの対象とするかを指定します。値は 2 ～ 100 の範囲で指定でき、デフォルト値は 10 です。

7 [拡張ファイルの最大サイズ（MB）] で、スキャン用に展開したときのファイルの最大許容サイズを指定します。値は 1 ～ 2047 の範囲で指定でき、デフォルト値は 10 です。

8 [スキャンの最大時間（分）] で、ファイルをスキャンする際の最長許容時間を指定します。値は 1 ～ 999 の範囲で指定でき、デフォルト値は 1 です。

9 [保存] をクリックしてポリシー ページに戻ります。

10 [アラートの選択] では、スキャナーの制御オプションがトリガーされた場合に使用するアラートを選択できます。以下のいずれかを使用できます。

- [作成] — このポリシーに対して新しいアラート メッセージを作成します。
- [表示/非表示] — アラート テキストを表示または非表示にします。テキストが非表示の場合、このリンクをクリックすると表示されます。テキストが表示されている場合、このリンクをクリックすると非表示になります。

11 [アクション] で [編集] をクリックして、以下のオプションの指定設定を値が超えた場合に実行されるアクションを指定します。

- [入れ子の最大レベル]
- [拡張ファイルの最大サイズ（MB）]
- [スキャンの最大時間（分）]

12 [保存] をクリックしてポリシー ページに戻ります。

13 [適用] をクリックし、対象設定をポリシーに構成します。

IP アドレスを手動でブロックする

IP アドレスのレピュテーションに関係なく、特定の IP アドレスまたは IP アドレスの範囲から組織へのメール送信をブロックできます。 このオプションを有効にするには、次のレジストリを更新する必要があります。

開始する前に

IP アドレスを手動でブロックできるのは、Exchange 役割、Hub、Edge、MailBox、HubMB だけです。IP アドレスを手動でブラックリストに登録するには、MSME で McAfee Anti-spam の検出機能を有効にする必要があります。

タスク

1 MSME がインストールされているシステムで、次のレジストリ キーに移動します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState
```

2 `IPBlackList` という文字列値を追加します。

3 メール送信をブロックする IPv4 アドレスを割り当てます。

複数の IP アドレスをブロックするには、セミコロンを使用します。 IP アドレスの範囲をブロックするには、ワイルドカード * を使用します。 例:

- 10.21.22.* ー 10.21.22.0 から 10.21.22.255 までのすべての IP アドレスをブロックします。
- 10.21.*.* ー 10.21.0.1 から 10.21.255.255 までのすべての IP アドレスをブロックします。

MIME メール設定の構成

暗号化された MIME メッセージを識別して必要なアクションを実行するため、ポリシー内の設定を構成します。

MIME（Multipurpose Internet Mail Extensions）は、7 ビット ASCII 文字のみをサポートする SMTP などのプロトコルで ASCII 以外の形式の転送を可能にする通信規格です。

MIME では、非 ASCII 形式をエンコードするためのさまざまな方法が定義されています。したがって、非 ASCII 形式を、7 ビット ASCII 文字セットの文字を使用して表すことができます。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [MIME メールの設定] をクリックします。

新しいフィルターをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストでフィルターを有効化する時間のタイム スロットを指定できます。

4 [オプション] ドロップダウン リストで、[<新しいオプション セットの作成>] を選択します。

[メール設定] ページが表示されます。

5 [インスタンス名] で、MIME 電子メール フィルタ設定インスタンスの一意の名前を入力します。このフィールドは必須です。

6 [オプション] タブで [メッセージ件名のプレフィックス] を入力します。

a [MIME メッセージでの添付ファイルの優先再エンコード] で、MIME メッセージの添付ファイルを再エンコードするときに使用する再エンコード方法を使用可能なオプションから選択します。

b [変更された件名ヘッダーの優先再エンコード] で、MIME メッセージの件名ヘッダーを再エンコードするときに使用する再エンコード方法を使用可能なオプションから選択します。

c [件名ヘッダーの再エンコードが失敗した場合] で、次のいずれかのオプションを選択します。

- [エラーとして処理]ーMIME メッセージはバウンスされます。
- [UTF-8 に戻す]ーMIME メッセージは UTF-8 にエンコードされます。

7 [詳細] タブで、電子メール メッセージのテキスト部分のエンコードに使用するエンコード方式を以下から選択します。

- [引用部 - 印刷可能]。ASCII 文字を主体とした内容で、ASCII 範囲外のバイト値もいくらか含まれるようなメッセージに最適です。
- [Base64]。オーバーヘッドが固定されており、非テキスト データや、ASCII テキストがそれほど多くないメッセージに最適です。
- [8 ビット版]。8BIT MIME 転送 SMTP 拡張機能をサポートする SMTP サーバでの使用に最適です。

「手順 6b」を実行できるのは、[変更された件名ヘッダーの優先再エンコード] から [元のエンコード方式を使用する再エンコード] または [次の文字セットを使用する再エンコード] を選択した場合に限られます。

a 必要に応じて、[テキストが 7 ビットの場合にはエンコードしない] を選択するか、選択を解除します。

b [デフォルトのデコード文字セット] で、MIME ヘッダーで文字セットが指定されていない場合に、デコードに使用する文字セットを選択します。

c [MIME 部分の最大数] — MIME メッセージに含めることができる MIME 部分の最大数を指定します。デフォルト値では、MIME 部分の数は 10,000 です。

d [MIME メッセージでのヘッダー破損] で、必要なオプションを選択します。

e [MIME メッセージのヘッダー内の NULL 文字] で、必要なオプションを選択します。

f [MIME メッセージの Quoted-Printable 文字エンコード] で、必要なオプションを選択します。

8 [MIME タイプ] タブで、テキスト添付ファイルとして処理する MIME タイプと、バイナリ添付ファイルとして処理する MIME タイプを指定します。

[追加] をクリックしてリストに MIME タイプを追加するか、[削除] をクリックしてリストから MIME タイプを削除します。重複する入力は許されません。

9 [文字セット] タブで、[文字セット] と [代替] を選択し、[固定] チェック ボックスを選択解除します。次に、[追加] をクリックして、MIME メッセージで指定した文字セットに代替文字コードのマッピングを指定します。

文字マッピングを編集するには [編集] をクリックし、文字マッピングを削除するには [削除] をクリックし、文字マッピングに対して行った任意の変更を適用するには [保存] をクリックします。

[保存] オプションは、[編集] をクリックした場合にのみ使用できます。

10 [保存] をクリックします。

11 [アラートの選択] では、MIME タイプがブロックされた場合に使用するアラートを選択できます。 以下のオプションを使用できます。

- [作成] — このポリシーに対して新しいアラート メッセージを作成します。
- [表示/非表示] — アラート テキストを表示または非表示にします。テキストが非表示の場合、このリンクをクリックすると表示されます。テキストが表示されている場合、このリンクをクリックすると非表示になります。

12 [不完全なメッセージ アクション] で、[編集] をクリックして、MIME の一部分または外部 MIME タイプが検出されたときに実行するフィルタ アクションを指定します。

13 [保存] をクリックしてポリシー ページに戻ります。

14 [適用] をクリックし、対象設定をポリシーに構成します。

HTML ファイル設定の構成

要素のスキャンや、電子メール内の HTML コンポーネントにある ActiveX、Java アプレット、VBScript などの実行ファイルの削除を行うポリシーの設定を構成します。
HTML 内にいずれかのコンテンツが見つかると、それが削除されます。このフィルタは、コンテンツ スキャナが有効の場合にのみ機能します。

タスク

1 [ポリシー マネージャー] で、フィルターが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [HTML ファイル] をクリックします。

4 [オプション] ドロップダウン リストで、[<新しいオプション セットの作成>] をクリックします。

[HTML ファイル] ページが表示されます。

5 [インスタンス名] で、フィルター設定インスタンスの一意の名前を入力します。このフィールドは必須です。

6 [次の要素をスキャンする] で、以下のいずれかのオプションを選択します。

- [コメント] — HTML メッセージのコメント要素をスキャンします。例:

```
<!-- コメント テキスト --!>
```

- [メタデータ]—HTML メッセージのメタデータ要素をスキャンします。例:

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- [リンク URL ("<ahref=...")] — HTML メッセージの URL 要素をスキャンします。例:

```
<a HREF="McAfee.htm">
```

- [ソース URL ("<img src=...")] — HTML メッセージのソース URL 要素をスキャンします。例:

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- [JavaScript / VBScript] — HTML メッセージの JavaScript または Visual Basic スクリプトをスキャンします。例:

```
<script language="javascript" scr="mfe/mfe.js">
```

7 [次の実行可能要素を削除する] で、以下のいずれかのオプションを選択します。

- [JavaScript / VBScript] — JavaScript または Visual Basic スクリプト要素を HTML メッセージから削除します。例:

```
<script language="javascript" scr="mfe/mfe.js">
```

- [Java アプレット] — Java アプレット要素を HTML メッセージから削除します。例:

```
<APPLET code="XYZApp.class" codebase="HTML ....."></APPLET>
```

- [ActiveX コントロール] — ActiveX コントロール要素を HTML メッセージから削除します。例:

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan Image </OBJECT>
```

- [Macromedia Flash] — Macromedia Flash 要素を HTML メッセージから削除します。このオプションは、[ActiveX コントロール] を選択した場合にのみ使用できます。例:

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 [保存] をクリックしてポリシー ページに戻ります。

9 [適用] をクリックし、対象設定をポリシーに構成します。

ポリシー用その他の設定の管理

ポリシーのトリガー時に適用されるアラートや免責事項などのその他の設定を作成または編集します。

使用できるオプションは以下のとおりです。

- [アラート設定]
- [免責事項のテキスト]

タスク

- 99 ページの「*アラート メッセージの設定*」
  検出が行われた際にエンド ユーザーにアラート メッセージで通知するポリシーの設定を構成します。
- 100 ページの「*免責事項のテキストの設定*」
  本文の一部としてポリシーの免責事項のテキスト設定を構成します。通常、免責事項のテキストは、すべての送信電子メール メッセージに追加される法律文書のことをいいます。

アラート メッセージの設定

検出が行われた際にエンド ユーザーにアラート メッセージで通知するポリシーの設定を構成します。

タスク

1 [ポリシー マネージャー] で、スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [アラート設定] をクリックします。

4 選択したサブメニュー アイテムのアラート メッセージをアクティブにするには、[有効] を選択します。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しいアラート メッセージをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストで有効化する時間のタイム スロットを指定できます。

5 [オプション] で、使用可能なデフォルトのアラート設定を選択するか、[<新しいオプション セットの作成>] を選択してアラート設定を定義します。

アラートの新規作成方法に関するステップごとの説明については、『アラートの新規作成』を参照してください。

6 [編集] をクリックし、既存のアラートを変更します。

[アラート設定] ページが表示されます。

7 [アラートの形式] として [HTML] または [平文] を選択します。

8 [文字エンコード] ドロップダウン メニューから、必要な文字セットを選択します。

9 [アラート ファイル名] で、このアラートのファイル名を指定します。HTML (.htm) または平文 (.txt) の適切なファイル拡張子を含みます。

10 [アラート ヘッダーを有効にする] を選択または選択解除して、アラート ヘッダーの使用を有効にします。

11 [アラート ヘッダー] テキスト入力ボックスに、アラートのヘッダーを入力します。

12 [アラート ヘッダー] に HTML テキストをコンパイル済みコードとして表示するか、ソース コードとして表示するかによって、[表示] から、[HTML コンテンツ (WYSIWYG)] または [HTML コンテンツ (ソース)] を選択します。

[表示] オプションは、アラート メッセージの形式として [HTML] を選択している場合にのみ使用できます。

13 [アラート フッターを有効にする] を選択して、必要に応じてアラート フッターの使用を有効にします。

14 [アラート フッター] テキスト入力ボックスに、アラートのフッターを入力します。

15 [アラート フッター] に HTML テキストをコンパイル済みコードとして表示するか、ソース コードとして表示するかによって、[表示] から、[HTML コンテンツ (WYSIWYG)] または [HTML コンテンツ (ソース)] を選択します。

[表示] オプションは、アラート メッセージの形式として [HTML] を選択している場合にのみ使用できます。

16 [保存] をクリックしてポリシー ページに戻ります。

17 [適用] をクリックし、対象設定をポリシーに構成します。

免責事項のテキストの設定

本文の一部としてポリシーの免責事項のテキスト設定を構成します。通常、免責事項のテキストは、すべての送信電子メール メッセージに追加される法律文書のことをいいます。

ポリシーを割り当てる際、組織の Exchange 環境から MSME サーバーを介して送信されるすべての電子メールには、構成された設定に基づいて免責事項のテキストが適用されます。

免責事項のテキストが適用されるのは、Microsoft Exchange トランスポート サーバーのみです。

タスク

1 [ポリシー マネージャー] で、スキャナーが含まれているサブメニュー アイテムを選択します。

サブメニュー アイテムのポリシー ページが表示されます。

2 [マスター ポリシー] または構成する任意のサブポリシーをクリックし、[全スキャナー一覧] タブをクリックします。

3 [免責事項のテキスト] をクリックします。

4 選択したサブメニュー アイテムの免責事項のテキスト設定をアクティブにするには、[有効] を選択します。

- サブポリシーの設定を構成する場合、[Use configuration from parent policy（親ポリシーからの設定を使用）] を選択すると親ポリシーから設定を継承できます。
- 新しい免責事項テキストをポリシーに追加する場合、[What time would you like this to apply（いつこの設定を適用しますか）] ドロップダウン リストで有効化する時間のタイム スロットを指定できます。

5 [オプション] ドロップダウン リストで、[<新しいオプションのセットの作成>] を選択します。[免責事項のテキスト] ページが表示されます。

6 [インスタンス名] で、免責事項のテキスト設定インスタンスの一意の名前を指定します。このフィールドは必須です。

7 免責事項の書式では、以下を選択できます。

- [HTML]ー通知電子メールで免責事項を HTML 形式で表示するかどうかを指定します。
- [プレーンテキスト]ー通知電子メールで免責事項をプレーンテキスト形式で表示するかどうかを指定します。

8 [免責事項の内容を編集する] に、免責事項のテキスト メッセージを入力します。

9 [アラート フッター] に HTML テキストをコンパイル済みコードとして表示するか、ソース コードとして表示するかに応じて、[表示] で [HTML コンテンツ（WYSIWYG）] または [HTML コンテンツ（ソース）] を選択します。

[表示] オプションは、免責事項テキスト形式として [HTML] を選択している場合にのみ使用できます。

10 免責事項のテキストを電子メール メッセージのどこにどのように挿入するかに応じて、[免責事項の挿入] ドロップダウン リストから、[メッセージ テキストの前]、[メッセージ テキストの後]、[添付ファイルとして] のいずれかを選択します。

11 [保存] をクリックしてポリシー ページに戻ります。

免責事項は、送信する電子メール メッセージに対してのみ適用できます。

12 [適用] をクリックし、対象設定をポリシーに構成します。

5 設定と診断

[設定と診断] には、MSME の機能の有効化/無効化、機能設定、機能管理、ログに関するメニューがあります。 これらの設定をユーザーの組織のセキュリティ ポリシーに基づいて構成します。

MSME 製品設定を変更または表示するには、製品のユーザー インターフェースで [設定と診断] をクリックします。 次の表では、これらの設定の機能について簡単に説明します。

表 5-1 設定と診断

使用する設定	機能
[オンアクセスの設定] [オンアクセスの設定] を使用できるのは、Microsoft Exchange 2010 サーバーだけです。 Microsoft VSAPI サポートは Microsoft Exchange 2013 および 2016 で削除されているため、オンアクセス VSAPI およびバックグラウンド スキャン設定機能は Exchange 2013 および 2016 サーバー上で無効になります。	スキャン エラーが発生した場合のメールの処理方法を定義します。 オプションは次のとおりです。 • [通過を許可] • [削除] また、以下の設定の有効化/無効化に関するサブメニューもあります。 • [Microsoft ウイルス スキャン API (VSAPI)] • [バックグラウンド スキャンの設定] • [トランスポート スキャン設定]
[オンデマンド設定]	[MSMEODUser] のパスワードを変更し、Active Directory や他の Exchange サーバーとパスワードの更新を同期します。
[メールボックスの除外設定]	オンアクセス VSAPI スキャンから除外するメールボックス、フォルダーまたはサブフォルダーを定義します。
[通知]	• 電子メールの検出時に、通知の受信や、特定のレビューアーや DL に通知電子メールを送信するための管理者用電子メール アカウントを定義します。 • 電子メールの隔離時にユーザーに送信されるカスタマイズした通知電子メールを作成します。 • Postgres データベースやサービスのロード エラーに関する問題といった特定のイベントが発生した直後や、毎日定期的に、管理者に電子メールで通知される製品の正常性アラートを定義します。

表 5-1 設定と診断 *(続き)*

使用する設定	機能
[スパム対策]	• エッジ トランスポート (ゲートウェイ) サーバーで検出されたスパムの転送先のジャンク電子メール フォルダーの設定を定義します。 • [McAfee GTI メッセージ レピュテーション] 機能を有効/無効にします。 • [SPF フィルター] を有効または無効にします。 • [McAfee GTI IP レピュテーション] 機能を有効/無効にします。

[TIE の設定]	TIE の検出を設定し、管理します。
	• [次のレベル以下の場合にアクションを実行する] ー レピュテーション スコアが定義済みのしきい値以下の場合にアクションを有効にします。
	• [次のアクションを実行]
	  • [アイテムをアラートに置き換える].
	  • [組み込み項目の削除]
	  • [メッセージを削除する]
	  • [以下も実行] ー ロギング、隔離、通知など、様々なオプションを設定できます。
	• [次のレベル以下の場合にファイルを ATD に送信する] と [ファイル サイズの制限] ー TIE レピュテーションしきい値とファイル サイズの制限に一致したファイルを Advanced Threat Defense レピュテーション チェックに送信します。

[検出されたアイテム]	以下のいずれかを使用して隔離リポジトリを構成および管理します。 • [McAfee Quarantine Manager] ー MSME と MQM サーバー間の通信を設定します (ある場合)。 • [ローカル データベース]ー削除や最適化などのローカル隔離データベース アクティビティを管理します。
[ユーザー インターフェースの設定]	[ダッシュボード] で、リフレッシュ レート、レポート設定、グラフィックの単位目盛、レポート間隔、グラフと図などの設定を定義します。
[診断]	ログ ファイルの大きさや保存場所などのデバッグ イベントおよび製品ログの設定を定義します。 診断設定では、以下の項目が表示されます。 • [デバッグ ロギング] • [イベント ロギング] • [製品ログ] • [エラー レポート サービス]
[製品ログ]	[製品ログ] を表示し、日付、種類、説明別に出力をフィルタリングします。
[DAT 設定]	各更新ファイルを上書きせずに古い DAT ファイルを保持し、保管する検出定義ファイルの数を定義します。

表 5-1 設定と診断 *(続き)*

使用する設定	機能
[設定のインポート/エクスポート]	現在の MSME サーバーを既存の構築済みサーバーと同じ構成でセットアップしたり、デフォルトまたは拡張設定を回復したり、DAT ダウンロード サイトをポイントする Sitelist を作成したりします。
[プロキシ設定]	[McAfee スパム対策ルール アップデーター サービス] のプロキシ設定を構成または変更します。

設定を変更した場合、[適用] をクリックして、変更内容を保存してください。 [適用] の背景色が以下のように変わります。

- 黄色－既存の設定を変更したか、または変更内容がまだ適用されていない。
- 緑色－既存の設定を変更していないか、または変更内容が適用されている。

目次

- *オンアクセスの設定*
- *オンデマンド設定*
- *メールボックスの除外設定の構成*
- *通知設定*
- *スパム対策の設定*
- *検出されたアイテムの設定*
- *ユーザーインターフェースの設定*
- *診断の設定*
- *製品ログの表示*
- *DAT 設定の構成*
- *構成設定のインポートとエクスポート*
- *スパム対策プロキシ設定の構成*

オンアクセスの設定

オンアクセス スキャンのトリガーは、オンアクセス ポリシーによってアイテムが検出されるかどうかを決めるため、ゲートウェイか、または電子メール メッセージがアクセスを受けるたびに行われます。オンアクセス スキャンは、リアルタイム スキャンとも呼ばれます。

各スキャンには、MSME のインストール先の Exchange サーバーの役割に基づいた独自の利点があります。 以下の表を参照すると、スキャンの種類、その機能、および各スキャンの適用可能タイミングが分かります。

Exchange Server の役割	適用可能なポリシー	スキャンの種類	説明
エッジ トランスポートまたはハブ トランスポート	• オンアクセス • ゲートウェイ	オンアクセス トランスポート スキャン	メールボックス サーバーによって受信される前に脅威がないかスキャンされます。 これを有効にすると、MSME ではユーザーの組織周辺にある脅威が検出されるため、メールボックス サーバーの負荷が軽減されます。
メールボックス	• オンアクセス	オンアクセス VSAPI スキャン	Outlook などの電子メール クライアントを使用してユーザーがアクセスする場合に脅威がないかスキャンされます。
		プロアクティブ スキャン	電子メールが Microsoft Exchange Information Store に書き込まれる前に脅威がないかスキャンされます。

Exchange Server の役割	適用可能なポリシー	スキャンの種類	説明
		送信トレイのスキャン	現在送信トレイ フォルダーにある電子メールに脅威がないかスキャンされます。
		バックグラウンド スキャン	優先順位が低いスキャンで、すべての Exchange データベースで脅威がないかバックグラウンドでスキャンされます。

[全般] セクションで、スキャンにエラーが発生したときに実行するアクションを定義します。

スキャン エラーが起こる理由はさまざまです。

- [一般的なエラー] ― スキャナーが特定のファイルをスキャンできません。
- [製品エラー] ― DAT またはエンジンが無効またはスパム ルールが正しくないいため、スキャンに失敗しています。

理由の一部には、以下の技術的な問題が原因の場合があります。

- スキャン タイムアウト
- スキャン エンジンがロードに失敗した
- DAT 問題
- 不適切な形式の電子メール

例えば、レジストリと実際の場所（`\bin\DATs`）で DAT の不一致が見られる場合は、スキャン エラーが発生します。

スキャン エラーが発生した場合、[設定と診断] 、 [オンアクセス設定] 、 [全般] の順に移動して指定した設定に基づいて、アクションがトリガーされます。

表 5-2 オプションの定義

オプション	定義
[一般的なスキャンが失敗した場合]	• [通過を許可] ― スキャン エラー発生時に、目的の受信者への電子メール メッセージの通過が許可されます。 • [削除]―スキャン エラー発生時に、電子メール メッセージが削除されます。
[製品スキャンが失敗した場合]	• [通過を許可] ― スキャン エラー発生時に、目的の受信者への電子メール メッセージの通過が許可されます。 • [削除]―スキャン エラー発生時に、電子メール メッセージが削除されます。
McAfee では、万一スキャン エラーが発生した場合に正規の電子メールが隔離されないように、このオプションは常に [通過を許可] に設定することをお勧めします。 デフォルトでは、このオプションは [通過を許可] に設定されているため、スキャン エラー時にも電子メールは消失しません。	

[オンアクセスの設定] ページには、以下に示す他のカテゴリがあります。

- [Microsoft ウイルス スキャン API (VSAPI)]
- [バックグラウンド スキャンの設定]
- [トランスポート スキャン設定]

[トランスポート スキャン設定] で、定義したサイズのメールをスキャンから除外できます。 有効にした場合、除外されるファイルのデフォルト サイズは 4 MB です。

スキャンの種類の詳細については、McAfee KnowledgeBase の記事 KB51129 を参照してください。

Microsoft ウイルス スキャン API（VSAPI）の設定

Microsoft VSAPI を使用すると、電子メール クライアントを使用してエンドユーザーが電子メールにアクセスする際に、MSME によってその電子メールがスキャンされます。

Microsoft Exchange では、電子メールの保存先は Exchange Information Store というデータベースになります。新しいメールを受信すると、Exchange サーバーから Outlook クライアントに変更内容が通知されます。これによって、オンアクセス スキャンがトリガーされます。

この機能を使用できるのは、メールボックスの役割を有する Microsoft Exchange 2007/2010 Server 上に限られます。

表 5-3 オプションの定義

オプション	定義
[有効]	選択すると、Outlook などの電子メール クライアントを使用してエンドユーザーがアクセスする場合にのみ電子メール メッセージがスキャンされます。この機能によってスキャンされるのは、Microsoft Exchange Information Store ですでに使用可能な電子メールか、または AV スタンプに不一致がある電子メールです。
[プロアクティブ スキャン]	選択すると、Microsoft Exchange Information Store に書き込まれる前に電子メール メッセージがスキャンされます。 この機能は、以下の状況で有効にします。 • ハブ トランスポート サーバーで MSME が構成されていない状態で、感染した電子メールがメールボックス サーバーによって受信された場合、Exchange Information Store に書き込まれる前にその電子メールは検出されます。 • 通常、パブリック フォルダー データベースに送信されたコンテンツは、ハブ トランスポート サーバー経由でルーティングされません。コンテンツがストアに受信される前に必ずスキャンされるようにするためには、パブリック フォルダー データベースのプロアクティブ スキャンを有効化することをお勧めします。
[送信トレイのスキャン]	選択すると、送信トレイ フォルダーの電子メール メッセージがスキャンされます。 電子メールがハブ トランスポート サーバーによって受信される前でも、MSME によって送信トレイ内の電子メールがスキャンされ、ハブ サーバーの負荷が軽減されます。
[最小の保存期間（秒）]	指定期間内に受信された電子メールのみがスキャンされるように値を指定します。指定時間前に受信された電子メールはスキャンされません。 デフォルトでは値が 86400 秒に設定され、これは 1 日に相当します。
[スキャンのタイムアウト（秒）]	電子メールのスキャンに許可される最大時間。電子メールのスキャン時間が指定値を超えると、[設定と診断] 、[オンアクセス設定] 、[全般] 、[スキャンが失敗した場合] で指定したアクションが実行されます。デフォルトでは、値は 180 秒に設定されています。
[スキャン スレッドの数]	オンアクセスおよびプロアクティブ スキャン キュー内のアイテムの処理に使用されるプール スレッドの数を指定します。デフォルト値は 2 * <プロセッサ数> + 1 です。McAfee では、パフォーマンスを向上させるため、[デフォルト] チェックボックスを選択することをお勧めします。

バックグラウンド スキャンの設定

データベースに保存されている任意のメッセージを系統的にスキャンします。 各データベースについて、通常の優先順位より下で実行中のスレッドによってデータベース内ですべてのフォルダーが列挙され、必要に応じてコンテンツをスキャンするように MSME に要求します。

表 5-4 オプションの定義

オプション	定義
[有効]	ウイルスのアウトブレーク後、バックグラウンドでデータベース全体をスキャンすることを選択します。デフォルトでは、このオプションは無効になっています。
[スケジュール]	バックグラウンド スキャンを有効化または無効化する時刻のスケジュールを設定します。 • バックグラウンド スキャンの開始時刻を指定するには、[有効にする時刻] をクリックします。 • バックグラウンド スキャンの停止時刻を指定するには、[無効にする時刻] をクリックします。 • この時刻は、曜日のオフピーク時間中または週末時にスケジュール設定してください。 • スケジュールを作成していない場合は、DAT 更新が実行されるとバックグラウンド スキャンが開始されます。
[添付ファイルのあるメッセージのみ]	選択すると、添付ファイルのある電子メール メッセージのみをスキャンできます。 この機能は、添付ファイルの広範囲に広がる特定のウイルスを心配する場合に役立ちます。 添付ファイルがある電子メールメッセージの方が脆弱性や悪意のあるコンテンツが含まれる可能性が高まるため、このタスクでウイルスや実行ファイルは置換されます。 MSME によって添付ファイルのある電子メールのみがスキャンされるため、この機能を有効にすると時間が節約されます。
[スキャンされていないアイテムのみ]	選択すると、スキャンされていない電子メール メッセージをスキャンできます。 メールボックス サーバーで Microsoft VSAPI を無効にして、スキャンされていないアイテムをスキャンする場合には、このオプションを有効にしてください。
[すべてを強制的にスキャンする]	アイテムに AV スキャン スタンプがあるかどうかに関係なく、すべてのアイテムをスキャンすることを選択します。
[スキャン スタンプを更新する]	最新の AV スタンプを持つ電子メール メッセージを更新することを選択します。
[送信日]	指定日から受信した電子メールにのみバックグラウンド スキャンを実行します。
[受信日]	指定日までに受信した電子メールにのみバックグラウンド スキャンを実行します。 現在のシステム日付まで電子メールをスキャンするには、[次の日付まで] を選択します。

トランスポート スキャン設定

トランスポート スキャンでは、SMTP トラフィックが Exchange 情報ストアに入る前に、その SMTP トラフィックをスキャンできます。SMTP トランスポート スキャンを使用すれば、ローカル サーバー宛てではないルーティングされた電子メール メッセージをスキャンして、メッセージの配信を停止できます。

表 5-5 オプションの定義

オプション	定義
[有効]	Exchange トランスポート レベルでスキャンの有効化を選択します。デフォルトでは、このオプションは有効になっています。 このオプションは、Microsoft Exchange サーバーでエッジ トランスポート、ハブ トランスポートまたはメールボックス + ハブの役割がある場合にのみ機能します。
[トランスポート スキャン スタンプ]	メール ヘッダーに DAT シグネチャを適用します。このメールは、メールボックス役割で再度スキャンされません。 **推奨設定**ートランスポート スキャンを有効にする場合は、このオプションも必ず有効化してください。
[次のサイズを超えるメールをスキャンしない]	メールのサイズに基づいて、オンアクセス スキャンからメールを除外します。 ファイル サイズは KB または MB で定義します。 McAfee では、潜在的な脅威からシステムを保護するため、どのファイルもアクセス前にスキャンすることをお勧めします。
[方向スキャン]	電子メール フローに基づいてオンアクセス スキャン設定を構成します。
[受信メールをスキャン]	Exchange サーバーまたは Exchange 組織に送信される電子メール メッセージをスキャンすることを選択します。
[送信メールをスキャン]	Exchange サーバーまたは Exchange 組織から送信される電子メール メッセージをスキャンすることを選択します。1 人以上の受信者のアドレスが外部アドレスの場合、電子メール メッセージは送信とみなされます。
[内部メールをスキャン]	ユーザーのドメイン内で、ある場所から別の場所にルーティングされている電子メール メッセージをスキャンすることを選択します。Exchange サーバーの権限のあるドメイン内にあるものは、内部ドメインとみなされます。電子メール メッセージがユーザーのドメイン内から送信され、すべての受信者がドメイン内に存在する場合、その電子メール メッセージは内部メールとみなされます。

オンデマンド設定

[オンデマンド設定] ページにアクセスして、[MSMEODUser] のパスワードを変更します。

メールボックス サーバーにインストールしているときに、McAfee Security for Microsoft Exchange は [MSMEODUser] というユーザーを Active Directory に作成します。 メールボックスでオンデマンド スキャンを実行するには、このユーザーが必要になります。

組織のセキュリティ ポリシーによっては、[MSMEODUser] のパスワードを定期的に更新する必要があります。

インターフェースで、[設定と診断]、[オンデマンド設定] の順に移動します。

オプション	定義
[ユーザー名]	[MSMEODUser] ー オンデマンド スキャンを実行するユーザー。 これは読み取り専用フィールドです。
[パスワードの入力]	パスワードを入力します。
[パスワードの確認]	パスワードを再度入力します。
[LDAP の次のパスワードもリセットする]	Active Directory と他の Exchange サーバーの間でパスワードの更新を同期する場合に選択します。 このオプションは、パスワードのリセットを [オンデマンド設定] ページで行う場合にのみ選択してください。

MSMEODUser のパスワードは、次の 2 つの方法で更新できます。

- Active Directory でパスワードをリセットし、[オンデマンド設定] ページでパスワードを更新する。
- [オンデマンド設定] ページでパスワードをリセットする。

Active Directory を使用してパスワードをリセットする	[オンデマンド設定] ページでパスワードをリセットする
1 Active Directory でパスワードを更新します。 2 同じ Active Directory 内でメールボックス役割のあるシステムに移動します。 3 McAfee Security for Microsoft Exchange インターフェースを起動します。 4 [設定と診断] で [オンデマンド設定] ページに移動し、パスワードを更新します。 5 [LDAP の次のパスワードもリセットする] オプションの選択を解除します。 6 [適用] をクリックします。	1 McAfee Security for Microsoft Exchange インターフェースを起動します。 2 [設定と診断] で [オンデマンド設定] ページに移動し、パスワードを更新します。 3 Active Directory 内でパスワードを更新するため、[LDAP の次のパスワードもリセットする] オプションを選択します。 4 [適用] をクリックします。

管理対象システムの場合には、ePolicy Orchestrator から [MSMEODUser] パスのパスワードを更新できます。

この設定がドメイン内のすべての Exchange サーバーに適用されるまで 1 分ほどかかる場合があります。 確認用のパスワードを更新してからオンデマンド スキャンを実行してください。

[MSMEODUser] の詳細については、McAfee KnowledgeBase の記事 KB82332 を参照してください。

メールボックスの除外設定の構成

VSAPI スキャンから除外するメールボックスまたはフォルダーを設定します。

以下の特定のシナリオでメールボックスの除外設定を構成します。

- 会社役員が電子メールをスキャンしたくない。
- カンパニー ポリシーによってスキャン対象外フォルダーが識別される。
- スキャンの対象外にするフォルダー

McAfee では、メールボックスの除外はお勧めしません。また、除外設定によってメールボックスが感染しても責任を負うことはできません。

タスク

1 [設定と診断] 、 [メールボックスの除外設定] の順にクリックします。[メールボックスの除外設定] ページが表示されます。

2 メールボックスまたはサブフォルダーを除外するには、次の手順に従います。

メールボックスを除外する	メールボックスのフォルダーを除外する
1 [使用可能なメールボックス] ペインから、メールボックスを選択し、[>>] をクリックします。 選択したメールボックスが [除外するメールボックス] ペインに移動します。 VSAPI スキャンから除外するすべてのメールボックスに対してこの手順を繰り返します。 除外リストからメールボックスを削除するには、[除外するメールボックス] ペインでメールボックスを選択し、[<<] をクリックして [使用可能なメールボックス] のリストにメールボックスを移動します。 メールボックスが [除外するメールボックス] ペインに追加されると、メールボックスのすべてのフォルダーがスキャンの対象外になります。	1 [使用可能なメールボックス] ペインから、メールボックスを選択します。 2 [メールボックス内で除外するフォルダー] ボックスで、除外するフォルダー名を入力し、[>>] をクリックします。 選択したメールボックス フォルダーが [除外するメールボックス] ペインに移動します。 ワイルドカードを使用すると、複数のフォルダーを VSAPI スキャンから除外できます。 詳細については、「ワイルドカードによる複数のメールボックスの除外」を参照してください。

ePolicy Orchestrator でメールボックスの除外を設定する場合には、完全なパスを手動で設定する必要があります。

3 [適用] をクリックして、設定を保存します。

この除外設定は、[オンアクセス設定] ページで [Microsoft ウイルス スキャン API (VSAPI)] の [送信トレイのスキャン] で行った設定を上書きします。 たとえば、ユーザーの送信トレイのスキャンを除外している場合、メールボックスの除外設定により、グローバルな送信トレイ スキャンが無効になります。

メールボックスの除外設定の例については、「ワイルドカードによるメールボックスの除外設定の例」を参照してください。

ワイルドカードによるメールボックスの除外設定の例

カンマ区切り文字またはワイルドカード * を使用すると、VSAPI スキャンから除外するフォルダーをメールボックス レベルまたはデータベース レベルで指定できます。

表 5-6 例

レベル...	除外対象...	設定...
データベース レベル	データベースのすべてのメールボックスの [Draft] フォルダー。	1 製品インターフェースで、[設定と診断]、[メールボックスの除外設定] の順にクリックします。 2 [使用可能なメールボックス] ペインから、データベースを選択します。 3 [メールボックス内で除外するフォルダー] ボックスで、[Draft] と入力して、[>>]、[適用] の順にクリックします。 選択したメールボックス フォルダーが [除外するメールボックス] ペインに表示されます。 除外するフォルダーを指定しないと、除外対象のデータベースを選択できません。
	データベースで名前が [person] で始まるメールボックスのすべてのフォルダー。	1 製品インターフェースで、[設定と診断]、[メールボックスの除外設定] の順にクリックします。 2 [使用可能なメールボックス] ペインから、データベースを選択します。 3 [メールボックス内で除外するフォルダー] ボックスで、[person*] と入力して、[>>]、[適用] の順にクリックします。 選択したメールボックス フォルダーが [除外するメールボックス] ペインに表示されます。
メールボックス レベル	カンマ区切り文字を使用してメールボックス内の複数のフォルダーを指定します。 たとえば、[Inbox] 内の Data1、Project1、Report1 フォルダーを除外できます。	1 製品インターフェースで、[設定と診断]、[メールボックスの除外設定] の順にクリックします。 2 [使用可能なメールボックス] ペインから、メールボックスを選択します。 3 [メールボックス内で除外するフォルダー] ボックスで、`Inbox\Data1,Inbox\Project1,Inbox\Report1` と入力して、[>>]、[適用] の順にクリックします。
	フォルダーとそのサブフォルダー。 • サブフォルダーの電子メールを除外し、親フォルダーの電子メールをスキャンできます。 • フォルダーの電子メールとサブフォルダーを除外できます。	1 製品インターフェースで、[設定と診断]、[メールボックスの除外設定] の順にクリックします。 2 [使用可能なメールボックス] ペインから、メールボックスを選択します。 • `Inbox\Personal*` ー [Personal] フォルダーの電子メールとサブフォルダーが VSAPI スキャンの対象外になります。 • `Inbox\Personal\*` ー [Personal] フォルダーのすべてのサブフォルダーが VSAPI スキャンの対象外になります。 [Personal] フォルダー内の電子メールは、VSAPI スキャンから除外されません。

通知設定

電子メールが隔離された場合に管理者が電子メール通知を送信するためのコンテンツや SMTP アドレスを設定できます。

製品のユーザー インターフェースで、[設定と診断] 、 [通知] の順にクリックして、通知を設定します。

[通知] ページでは、以下の項目を使用できます。

- [設定]－電子メールが隔離された場合に通知を受信するための電子メール アカウントを定義します。 また、特定のスキャナーやフィルターによって電子メールが隔離された場合に、特定のレビュー担当者または DL に通知電子メールを送信することもできます。

  管理対象システムとスタンドアロン システムの通知を受信できるように、[通知] ページで、システムまたはグループ システムの電子メール アドレスを必要に応じて更新してください。

  電子メール通知を配布リスト (DL) に送信し、DL の SMTP アドレスを指定します。

- [テンプレート]－電子メールが隔離された場合に特定のユーザーに送信されるカスタマイズ通知電子メールを作成します。
- [製品の正常性アラート]－Postgres データベースやサービスのロード エラーに関する問題といった特定のイベントが発生した直後や、毎日定期的に、管理者に電子メールで通知される製品の正常性アラートを定義します。

  通知またはポリシー名などの設定を行うときに、クロス サイト スクリプティング (XSS) で狙われる文字を使用しないでください。 使用を避ける必要がある文字については、McAfee KnowledgeBase の記事 KB82214 を参照してください。

通知設定の構成

電子メールが隔離された場合に通知を受信するための電子メール アカウントを構成します。 また、電子メールが検出された場合には、通知電子メールを特定の受信者または DL に送信します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [通知] の順にクリックします。

2 [通知] 、 [設定] の順に移動すると、以下の項目を使用できます。

表 5-7 オプションの定義

オプション	定義
[全般]	簡単な電子メール設定を定義します。
[管理者の電子メール]	隔離アクションやアラートなどのイベントが発生した場合に、Microsoft Exchange 管理者に通知します。 • 複数のユーザーに電子メール通知を送信します。区切り記号にはセミコロン（;）を使用してください。 • 電子メール通知を配布リスト（DL）に送信し、DL の SMTP アドレスを指定します。
[送信者の電子メール]	通知電子メールの [送信元] フィールドで送信者の電子メール アドレスを指定します。 McAfee では、このアドレスは様々な目的で使用されるため、[送信者の電子メール] のアドレスを変更しないことをお勧めします。 この電子メール アドレスを変更した場合、Microsoft Exchange の受信コネクターで [匿名] を有効にしないと、製品通知が受信できなくなります。
[結果の通知タスクを有効にする]	オンデマンド スキャンを行った電子メールを送信し、タスク結果を更新します。 電子メールは HTML 形式で、ユーザー インターフェースの [タスクの結果] ウィンドウと同じデータと書式が使用されます。 この機能は、このオプションを使用して有効または無効にできます。 デフォルトでは、この機能は無効になっています。

表 5-7 オプションの定義 *(続き)*

オプション	定義
[詳細設定]	各スキャナーやフィルター用に個別の電子メール アドレスと件名を指定するなど、通知の詳細設定を定義します。
[メールの本文]	すべての通知に使用する汎用電子メール メッセージの本文を定義します。

3 [適用] をクリックして設定を保存します。

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。

通知テンプレートの編集

エンドユーザーに送信した通知電子メールのメッセージ本文を表示または編集します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [通知] の順にクリックします。

2 [通知] 、 [テンプレート] タブでは、以下の項目を使用できます。

表 5-8 オプションの定義

オプション	定義
[テンプレート]	特定のエンドユーザー用の通知テンプレートを表示します。使用可能なオプションは次のとおりです。 • [内部送信者] • [内部受信者] • [外部送信者] • [外部受信者] これらの各ユーザー タイプには特定の通知テキストを定義できます。
[件名]	通知電子メールの件名を指定します。デフォルトの通知件名は [McAfee Security for Microsoft Exchange アラート] です。
[通知テキスト]	選択した [テンプレート] に基づき、通知電子メールのメッセージ本文をプレビューを表示します。通知テキストには、日時、件名、実行されたアクションなどの隔離されたアイテムに関する情報が記載されます。
[編集]	平文形式の HTML で通知テキストを変更します。会社の要件に基づいて通知を編集した後、[保存] をクリックして変更内容を適用します。

3 [適用] をクリックして設定を保存します。

通知テンプレートを正常に表示または変更できました。使用可能な通知フィールドの詳細については、『使用可能な通知フィールド』を参照してください。

使用可能な通知フィールド

通知に含めるには以下のフィールドを使用します。例えば、検出されたアイテムと検出時に実行されたアクションの名前が必要になる場合は、[設定と診断] 、 [通知] 、 [テンプレート] ページで **%vrs%** および **%act%** を使用します。

表 5-9 使用可能な通知フィールド

通知フィールドのオプション	説明
%dts%	日付/時刻
%sdr%	送信者
%ftr%	フィルター
%fln%	ファイル名
%rul%	ルール名
%act%	実行されたアクション
%fdr%	フォルダー
%vrs%	検出名
%trs%	状態（学習状態）
%tik%	チケット番号
%idy%	スキャンの種類
%psn%	ポリシー名
%svr%	サーバー
%avd%	ウイルス対策 DAT
%ave%	ウイルス対策エンジン
%rpt%	受信者
%rsn%	理由
%sbj%	件名
%ssc%	スパム スコア
%ase%	スパム対策エンジン
%asr%	スパム対策ルール

製品の正常性に関するアラートの有効化

製品固有のタスクが失敗した際に、Microsoft Exchange 管理者へ早急に、または毎日通知を送信します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [通知] の順にクリックします。

2 [通知] 、 [製品の正常性に関するアラート] タブでは、以下の項目を使用できます。

表 5-10 オプションの定義

オプション	定義
[有効]	製品固有のタスクが失敗した際に、製品の正常性に関するアラート通知の管理者への送信を有効にします。
[アラート ePolicy Orchestrator]	製品固有のタスクが失敗した際に、この MSME サーバーを管理する McAfee ePolicy Orchestrator サーバーにアラートを送信します。
[アラート管理者]	[設定と診断] 、 [通知] 、 [設定] 、 [管理者の電子メール] で指定した電子メール アドレスへ製品の正常性に関するアラートを送信します。

表 5-10 オプションの定義 *(続き)*

オプション	定義
[次の場合に通知する]	選択した製品固有のタスクのいずれかが失敗した際に管理者に通知します。製品の正常性に関するアラートを管理者に送信する場合、以下のオプションを選択できます。 これらのオプションは、ご使用の Exchange サーバーの役割に応じて異なる場合があります。 • [DAT/ウイルス対策エンジンのダウンロードに失敗しました] • [スパム対策ルールのダウンロードに失敗しました] • [ウイルス対策エンジンの読み込みに失敗しました] • [トランスポート スキャン モジュールの読み込みに失敗しました] • [VSAPI モジュールの読み込みに失敗しました] • [RPCServ プロセスが予期せず終了しました] • [DLLHost プロセスが予期せず終了しました] • [Postgres 処理に失敗しました] • [Postgres は検出した項目を隔離または記録できませんでした] • [Postgres データベースの初期化に失敗しました] • [Postgres はレコードの格納に失敗しました] • [オンデマンド スキャンに失敗しました] • [データベースのディスク容量がしきい値より小さくなります] • [製品サービスを開始できません] • [McAfee Global Threat Intelligence ファイル レピュテーション スキャンが失敗しました]
[即時]	タスクが失敗した直後に管理者へ通知を送信します。
[毎日]	タスクが失敗した際に毎日の指定時刻に管理者へ通知を送信します。

3 [適用] をクリックして設定を保存します。

[製品の正常性に関するアラート] 機能を正常に有効化できました。

スパム対策の設定

エッジ トランスポートまたはハブ トランスポート サーバーで検出されたスパムの転送先のジャンク電子メール フォルダーの設定を定義します。 また、McAfee GTI メッセージ レピュテーションと McAfee GTI IP レピュテーション機能を有効または無効にします。

表 5-11 オプションの定義

オプション	定義
[システム ジャンク メール フォルダーのアドレス]	スパムとして分類される電子メールの送信先となる電子メール アドレスを指定します。
[McAfee GTI メッセージ レピュテーション]	McAfee Global Threat Intelligence メッセージ レピュテーションは、クラウド ベースでメッセージと送信者の評価情報をリアルタイムで提供する McAfee の包括的なサービスです。これにより、MSME は、スパムなどのメッセージの脅威から Exchange サーバーを保護します。 MSME は、毎日何百万もの電子メール クエリーを受信し、メッセージ コンテンツのフィンガープリントを (セキュリティ上の理由からコンテンツ自体と) 照合し、あらゆる方向から分析します。 メッセージ レピュテーションは、スパムが送信するパターンや IP の挙動などの要素と結び付き、問題になっているメッセージが悪意のあるメッセージである可能性を判断します。 センサーが McAfee クラウド、McAfee Labs の研究者が行った分析結果、自動化ツールから収集した情報と、ファイル、Web、ネットワークの脅威データを相関分析し、スコアを設定します。 MSME は、このスコアを使用してアクションを実行します。実行するアクションは、[ポリシー マネージャー] 、 [ゲートウェイ] の順に移動して設定します。
[有効]	電子メール メッセージのレピュテーション スコアに基づいて、ゲートウェイで電子メールを阻止します。
[スパム対策の後にメッセージ レピュテーションを実行]	ローカルの McAfee GTI ポリシーに基づいてスキャンを実行した後で MSME メッセージ レピュテーションを実行します。
[メッセージ レピュテーションのしきい値]	しきい値を指定して、メッセージ レピュテーション スコアに基づいて、電子メール メッセージを阻止します。 デフォルトでは、値は 80 秒に設定されています。
[実行するアクション]	以下を選択します。 • [ドロップして隔離する] ― 電子メールをドロップし、データベースに隔離します。この設定によって電子メールがドロップされた場合、電子メール送信ステータスについて送信者には通知されません。 • [スパム対策エンジンにスコアを渡す] ― McAfee GTI により検出されたメッセージのレピュテーション スコアをスパム対策エンジンに送信します。 このオプションは、[スパム対策の後にメッセージ レピュテーションを実行] おプ sy ンを有効にした場合にのみ使用できます。
[McAfee GTI IP レピュテーション]	安全でない電子メール ソースからご使用の Exchange サーバーを保護することにより、IP レピュテーションは、ご使用の Exchange 環境に対する第 1 レベルの保護として機能します。 McAfee Global Threat Intelligence が収集した脅威情報を利用してゲートウェイで電子メール メッセージを阻止します。これにより、損害と情報漏洩を防ぎます。
[有効]	ソース IP アドレスに基づいて、ゲートウェイで電子メール メッセージを阻止します。

表 5-11 オプションの定義 *(続き)*

オプション	定義
[IP 評価しきい値]	しきい値を指定して、IP レピュテーション スコアに基づいてメールを阻止します。 アクションは、選択したしきい値より上のレピュテーション スコアの IP アドレスすべてに適用されます。 その他すべてのメールの通信は許可されます。 [スパム対策設定] ページの [IP レピュテーションしきい値] に設定された値で正規の IP アドレスがブロックされた場合には、レジストリ値を変更して、この IP アドレスをホワイトリストに追加できます。 IP アドレスをホワイトリストに登録すると、このアドレスから送信された電子メールは、レピュテーション スコアに関係なく通過が許可されます。 **重要**: IP アドレスをホワイトリストに登録した場合、[IP レピュテーションしきい値] の設定だけが上書きされます。 MSME は、電子メールをスキャンして壊れたコンテンツや暗号化されたコンテンツを検出し、ファイル フィルタリング、コンテンツ スキャン、URL レピュテーション、マルウェア対策などを行います。 脅威が検出された場合は、製品の構成に従ってアクションが実行されます。 McAfee では、IP アドレスをホワイトリストに登録する前に、www.trustedsource.org で IP アドレスのレピュテーション スコアを確認し、アドレスの正当性を検証することを推奨します。 McAfee は、ホワイトリストに登録された IP アドレスが原因でメールボックスが感染しても、一切責任を負いません。 レジストリを使用して IP エージェントの IP をホワイトリストに登録する方法については、McAfee KnowledgeBase の記事 KB82216 を参照してください。
[実行するアクション]	ソース IP アドレスのレピュテーション スコアに基づいて、いずれかのオプションを選択し、電子メール メッセージに対しアクションを取ります。 • [接続をドロップして記録] ― 検出されたソース IP アドレスから電子メールをドロップし、アイテムに対して取るべきアクションを記録します。 • [接続を拒否して記録] ― 送信者に通知し、アイテムに対して取るべきアクションを記録して、検出されたソース IP アドレスから電子メールを拒否します。
[SPF フィルター]	なりすましメールからシステムを保護します。ハード エラーやソフト エラーのメッセージに対するアクションを設定できます。

検出されたアイテムの設定

MSME によって検出された隔離されたアイテムを保存するためのリポジトリ設定を指定します。

以下を使用して隔離リポジトリを構成および管理します。

- [McAfee Quarantine Manager]－MQM サーバーで検出アイテムを隔離します。
- [ローカル データベース]－ローカル MSME サーバーで検出アイテムを隔離します。

McAfee Quarantine Manager による隔離

MSME によって McAfee Quarantine Manager サーバーで検出されたアイテムを隔離するため、リポジトリ設定を指定します。

McAfee Security for Microsoft Exchange や McAfee Email Gateway などの McAfee 製品では、検出情報を McAfee Quarantine Manager に送信する際に事前に割り当てられたポート番号が使用されます。 McAfee Quarantine Manager では同様に、検出された電子メール メッセージの設定情報を McAfee 製品にリリースまたは送信する際には、デフォルトで同じポート番号が使用されます。

McAfee Security for Microsoft Exchange と McAfee Quarantine Manager のユーザー インターフェースで使用される通信ポートは同じにする必要があります。

McAfee Quarantine Manager を使用すると、隔離とスパム対策の管理機能を統合できます。 それにより、隔離された電子メールやファイルに対して 1 か所から分析とアクションを実行できます。

このガイドでは、McAfee Quarantine Manager のインストール方法や使用方法の詳細については説明しません。 詳細については、McAfee Quarantine Manager の製品マニュアルを参照してください。

タスク

1 McAfee Security for Microsoft Exchange を <サーバー 1> にインストールします。

2 サポート対象の McAfee Quarantine Manager を <サーバー 2> にインストールします。

3 MSME ユーザー インターフェースを <サーバー 1> で起動します。

4 製品のユーザー インターフェースで、[設定と診断] 、 [検出されたアイテム] の順にクリックします。

[検出アイテム] ページが表示されます。

5 [McAfee Quarantine Manager] セクションで、[有効にする] を選択します。

6 [通信モード] でモードを選択します。

- [RPC] ― 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。 McAfee Quarantine Manager サーバーとの通信でエラーが発生すると、隔離や開放などのプロセスが中断します。
- [HTTP] ― 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障害が発生した場合、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、MQM 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] ― 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。

7 [IP アドレス] で、MQM サーバーの IP アドレスを指定します。

8 [ポート] と [コールバック ポート]で、デフォルトの値を指定します。

通信モード	ポート値	コールバック ポート	BW リストの更新間隔 (時間)
RPC	49500	49500	–
HTTP	80	–	4
HTTPs	443	–	4

McAfee Quarantine Manager サーバーで異なるポート値を設定済みの場合にのみ、この値を変更します。

9 [適用] をクリックして設定を保存します。

MSME サーバーで検出アイテムの隔離を開始するための MQM サーバーの設定が正常に完了しました。

ローカル データベースを使用した隔離

MSME によって検出されたアイテムをローカル MSME サーバーの PostgreSQL データベースに隔離するため、リポジトリ設定を指定します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [検出されたアイテム] の順にクリックします。

[検出アイテム] ページが表示されます。

2 [ローカル データベース] セクションでは、以下の項目を使用できます。

表 5-12 オプションの定義

オプション	定義
[データベースの場所を指定]	MSME によって検出された隔離アイテムを保存するための [データベースの場所] を有効にします。
[データベースの場所]	MSME によって検出されたアイテムを保存可能なデータベースの場所のパスを指定します。次を選択できます。 • [<インストール フォルダー>]—MSME インストール ディレクトリ直下にデータベース サブフォルダーを作成します。 • [<システム ドライブ>]—`C:\Windows\system32` ディレクトリ直下にデータベース サブフォルダーを作成します。 • [<プログラム ファイル>]—Windows の `C:\Program Files (x86)` ディレクトリ直下にデータベース サブフォルダーを作成します。 • [<Windows フォルダー>]—`C:\Windows` ディレクトリ直下にデータベース サブフォルダーを作成します。 • [<データ フォルダー>]—`C:\ProgramData\` ディレクトリ直下にデータベース サブフォルダーを作成します。 • [<フル パス>]—指定した完全パスに MSME データベースを保存します。 ドロップダウン リストの横にあるフィールドでサブフォルダーのパスを指定します。デフォルトで指定されるサブフォルダーのパスは、`McAfee\MSME\Data\` です。
[アイテムの最大サイズ（MB）]	データベース内に保存可能な隔離されたアイテムの最大サイズを指定します。値は 1 ～ 999 の範囲で指定でき、デフォルト値は 100 です。
[クエリーの最大サイズ（レコード）]	[検出アイテム] ページからクエリーを実行できるレコードや隔離されたアイテムの最大数を指定します。値は 1 ～ 20000 の範囲で指定でき、デフォルト値は 1000 です。

表 5-12 オプションの定義 *(続き)*

オプション	定義
[アイテムの最大経過期間（日）]	削除対象として指定される前に、ローカル隔離データベースでアイテムが保管される最大日数を指定します。値は 1 ～ 365 の範囲で指定でき、デフォルト値は 30 です。
[ディスク サイズの確認間隔（分）]	MSME で使用可能なディスク容量を確認する回数を指定します。値は 6 ～ 2880 の範囲で指定でき、デフォルト値は 6 です。
[ディスク容量のしきい値（MB）]	管理者に警告通知が送信される際の基準となるディスク容量不足のしきい値を指定します。値は 1 ～ 512000 の範囲で指定でき、デフォルト値は 2048 です。 [設定と診断] 、 [通知] 、 [製品の正常性アラート] 、 [次の場合に通知する] の [データベースのディスク容量がしきい値より小さくなります] を必ず有効にしてください。
[古いアイテムを削除する頻度]	削除対象の古いアイテムを MSME データベースから削除する頻度を指定します。デフォルト値は [毎月] に設定されています。
[最適化の頻度]	削除したデータベース レコードにより占有されていたディスク容量を回復します。[アイテムの最大経過期間（日）] で設定した値に基づいて削除タスクをスケジュール設定済みの場合、古いレコードは削除されます。古いレコードを削除した後は、隔離データベースがサイズ制限に到達していない場合でも、MSME では [ディスク容量のしきい値（MB）] フィールドで指定したディスク容量が引き続き使用されます。データベースを最適化して縮小するには、最適化タスクのスケジュールを設定します。デフォルト値は [毎月] に設定されています。 最適化タスクのスケジュールは、常に削除タスクを実行してから数時間後に設定します。
[スケジュールの編集]	削除または最適化タスクのスケジュールを変更します。スケジュールの変更後に [保存] をクリックします。

3 [適用] をクリックして設定を保存します。

ローカル データベースで検出アイテムの隔離を開始するための MSME サーバーの設定が正常に完了しました。

ユーザーインターフェースの設定

[ダッシュボード]で、更新間隔、レポート設定、グラフィックの単位目盛、間隔のレポート、グラフと図の設定などの設定を定義します。

ダッシュボード設定の構成

統計情報、グラフの目盛単位、[最近スキャンされたアイテム] に表示するアイテム、ステータス レポート間隔などの設定を [ダッシュボード] で構成します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [ユーザー インターフェースの設定] の順にクリックします。

[ユーザ インターフェースの設定] ページが表示されます。

2 [ダッシュボード設定] タブをクリックします。以下のいずれかを使用できます。

表 5-13 オプションの定義

オプション	定義
[自動更新]	[ダッシュボード] 、[統計] カウンターに表示される情報を自動的に更新するかどうかを指定します。
[リフレッシュ レート（秒）]	ダッシュボードの情報が更新されるまでの時間（秒）を指定します。値は 30 ～ 3600 の範囲で指定でき、デフォルト値は 60 です。
[最近スキャンした項目の最大数]	[ダッシュボード] 、[レポート] 、[最近スキャンされたアイテム] セクションに表示される項目の最大数を指定します。値は 10 ～ 100 の範囲で指定でき、デフォルト値は 10 です。
[グラフの目盛（単位）]	[ダッシュボード] 、[グラフ] セクションで生成される棒グラフの目盛の測定単位を指定します。値は 100 ～ 500 の範囲で指定でき、デフォルト値は 100 です。
[レポート時間]	ステータス レポートや構成レポートなどのレポートを生成するためのレポート生成間隔（時間単位）を指定します。値は 1 ～ 24 の範囲で指定でき、デフォルト値は 7 です。

3 [適用] をクリックして設定を保存します。

グラフと図の設定の構成

[ダッシュボード] 、[グラフ] セクションで設定を構成し、グラフと図の設定を強化します。

タスク

1 [設定と診断] 、[ユーザー インターフェースの設定] の順にクリックします。

2 [グラフと図の設定] タブをクリックします。以下のいずれかを使用できます。

表 5-14 オプションの定義

オプション	定義
[3D]	ダッシュボードのグラフを 3 次元（3D）グラフとして表示するかどうかを指定します。
[半透明描画]	3 次元（3D）棒グラフの棒を半透明表示にするかどうかを指定します。棒を半透明表示にしない場合、その後ろの棒の一部が隠れます。棒を半透明表示にした場合、棒が透けて見えるため、その後ろの半透明の棒も見ることができます。
[アンチエイリアス]	円グラフを表示する際にアンチエイリアス手法を使用するかどうかを指定します。アンチエイリアスを使用すると、円グラフの曲線が滑らかに表示されます。アンチエイリアスを使用しないと、円グラフの曲線がギザギザに表示されます。
[円グラフを分離して表示]	セグメントを円グラフの円内に残すか、または分離したセグメントで表示するかどうかを指定します。
[円グラフの角度（度）]	円グラフを表示する際に使用する角度を指定します。値は 1 ～ 360 の範囲で指定でき、デフォルト値は 45 です。

3 [適用] をクリックして設定を保存します。

診断の設定

症状の原因、問題の移行、および MSME の使用中に直面した問題へのソリューションを決定します。

[設定と診断] 、 [診断] ページでは、以下を使用できます。

- [デバッグのログ]ーデバッグ ログ レベル、ログ ファイルの最大ファイル サイズ制限、およびファイルの場所の指定などのデバッグ ログ設定を構成します。
- [イベント ログ]ー情報、警告、エラーに基づいて製品またはイベント関連ログをキャプチャするための設定を構成します。
- [製品ログ]ーMSME 製品ログ ファイル（`productlog.bin`）の設定を構成します。この設定に加えた変更は、[設定と診断] 、 [製品ログ] ページに反映されます。
- [エラー レポート サービス]ーシステム クラッシュなどの例外を検出したらユーザーに報告するかどうかを決定するための設定を構成します。

デバッグ ログ設定の構成

デバッグ ログ レベル、ログ ファイルの最大ファイル サイズ制限、ログ ファイルの場所を指定します。 これらの設定は、製品のトラブルシューティングや McAfee テクニカル サポートにログを提供する場合に使用されます。

[デバッグ ログ] 設定の構成は、制限期間内に限り、トラブルシューティングの目的で行います。トラブルシューティング用に十分なログをキャプチャしたら、[レベル] の値を [なし] に設定します。デバッグのログ記録を無差別に使用しないでください。ハード ディスクの空き容量が不足し、サーバー全体のパフォーマンスに影響が及ぶ可能性があります。承認された担当者（McAfee テクニカル サポート エンジニア）が推奨する限られた期間だけ有効にしてください。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [診断] の順にクリックします。

[診断] ページが表示されます。

2 [デバッグ ログ] タブでは、以下のオプションを使用できます。

表 5-15 オプションの定義

オプション	定義
[レベル]	デバッグ ロギングを有効/無効にして、デバッグ ログ ファイルに記録する情報のレベルを指定します。 次の項目を選択できます。 • [なし]ーデバッグのログを無効にします。 • [低]ーエラー、例外、関数の戻り値などの重要イベントをデバッグ ログ ファイルに記録します。デバッグ ログ ファイルのサイズを小さくとどめたい場合はこのレベルを選択します。 • [中]ー[低] レベルで説明したイベントと、テクニカル サポート チームに有益となる可能性がある追加情報をログに記録します。 • [高]ーデバッグ ログ ファイルに重要なエラー、警告、デバッグ メッセージをすべて記録します。製品によって実行されたすべての活動に関する情報が記載されます。これは、製品でサポートされるログレベルの中で最も詳細なものです。
[サイズ制限の有効化]	デバッグ ログ ファイルに最大ファイル サイズを指定します。

表 5-15 オプションの定義 *(続き)*

オプション	定義
[最大ファイル サイズの指定]	デバッグ ログ ファイルの最大サイズを指定します。 1 KB から 2000 MB までの値を指定できます。 デバッグ ログ ファイルが指定ファイル サイズを超えると、循環ロギングによって古いイベントが上書きされます。最も古いログ エントリを削除すると、新しいログ エントリがファイルに追加されます。
[デバッグ ロギングの有効化]	デバッグ ログ ファイルのデフォルトの場所を変更します。 このオプションを無効にすると、デバッグ ログ ファイルは <インストール フォルダー>\bin \debuglogs デフォルト ディレクトリに保存されます。
[ファイルの場所の指定]	MSME によってトリガーされたイベントを保存可能なデバッグ ログ ファイルの場所のパスを指定します。 次の項目を選択できます。 • [<インストール フォルダー>]ーMSME インストール ディレクトリ直下にデバッグ ログ ファイルを作成します。 • [<システム ドライブ>]ーC:\Windows\system32 ディレクトリ直下にデバッグ ログ ファイルを作成します。 • [<プログラム ファイル>]ーWindows の C:\Program Files (x86) ディレクトリ直下にデバッグ ログ ファイルを作成します。 • [<Windows フォルダー>]ーC:\Windows ディレクトリ直下にデバッグ ログ ファイルを作成します。 • [<データ フォルダー>]ーC:\ProgramData\ ディレクトリ直下にデバッグ ログ ファイルを作成します。 • [<フル パス>]ー指定した完全パスにデバッグ ログ ファイルを保存します。 デバッグ ログ ファイルを任意の場所またはサブフォルダーに保存するには、ドロップダウン リストの横にあるフィールドでサブフォルダー名またはパスを指定します。

デバッグ ログ収集用フォルダーには、ネットワーク サービス アカウントの書き込み権限を必ず割り当ててください。

3 [適用] をクリックして、設定を保存します。

オンデマンド スキャン タスクの Exchange Web Services (EWS) ラッパー ログの生成方法については、McAfee KnowledgeBase の記事 KB82215 を参照してください。

これで、デバッグ ログ設定の構成を正常に完了したので、トラブルシューティングに使用できます。

イベント ログ設定の構成

[製品ログ] および Windows イベント ビューアーで MSME イベントの種類を記録する設定を構成します。

イベントとは実行可能なアクションで、MSME によって監視されます。 [イベント ログ] には、診断と監査に有益な情報が表示されます。各イベントのクラスは以下のとおりです。

- エラー
- 情報
- 警告

これによって、システム管理者は発生する問題に関する情報をより簡単に入手することができます。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [診断] の順にクリックします。

[診断] ページが表示されます。

2 [イベント ログ] タブをクリックします。以下のいずれかを使用できます。

表 5-16 オプションの定義

オプション	定義
[製品ログ]	[製品ログ] に MSME イベントを記録します。当該イベントは、[設定と診断] 、 [製品ログ] 、 [結果の表示] セクションに表示されます。
[イベント ログ]	Windows イベント ビューアーで MSME イベントを記録します。 Windows イベント ビューアーで MSME 関連イベントを記録します。 1 [イベント ビューアー（ローカル）] 、 [Windows ログ] 、 [アプリケーション] にアクセスします。 2 [アプリケーション] ペインには、製品関連イベントが [ソース] 列の [MSME] に表示されます。
[情報イベントを書き込む]	[情報] として分類されるイベントを記録します。
[警告イベントを書き込む]	[警告] として分類されるイベントを記録します。
[エラー イベントを書き込む]	[エラー] として分類されるイベントを記録します。

3 [適用] をクリックして設定を保存します。

製品ログ設定の構成

製品ログの生成に必要なパラメーターを指定し、[設定と診断] 、 [製品ログ] ページの設定を構成します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [診断] の順にクリックします。

[診断] ページが表示されます。

2 [製品ログ] タブをクリックします。以下のいずれかを使用できます。

表 5-17 オプションの定義

オプション	定義
[場所]	製品ログの保存場所を構成する場合。カスタムの場所を指定するには、[有効] を選択します。
[データベース場所の指定]	製品ログ イベントを保存可能な製品ログ ファイルの場所のパスを指定します。次を選択できます。 • [<インストール フォルダー>]ーMSME インストール ディレクトリ直下に製品ログ ファイルを作成します。 • [<システム ドライブ>]ーC:\Windows\system32 ディレクトリ直下に製品ログ ファイルを作成します。 • [<プログラム ファイル>]ーWindows の C:\Program Files (x86) ディレクトリ直下に製品ログ ファイルを作成します。 • [<Windows フォルダー>]ーC:\Windows ディレクトリ直下に製品ログ ファイルを作成します。 • [<データ フォルダー>]ーC:\ProgramData\ ディレクトリ直下に製品ログ ファイルを作成します。 • [<フル パス>]ー指定した完全パスに製品ログ ファイルを保存します。 製品ログ ファイルをカスタムの場所やサブフォルダーに保存するには、ドロップダウン リストの横にあるフィールドでサブフォルダー名またはパスを指定します。
[ファイル名]	製品ログの保存に別のファイル名を指定する場合。カスタム ファイル名を指定するには、[有効] を選択します。
[データベース ファイル名の指定]	製品ログにカスタム ファイル名を指定します。デフォルトのファイル名は、<インストール フォルダー>\Data\ ディレクトリの productlog.bin となります。 デフォルトの製品ログ ファイル名またはパスを変更する場合、[設定と診断] 、[製品ログ] ページ内のログ エントリはリセットされ、古いログ エントリは表示されません。
[サイズ制限]	製品ログ ファイルに別のサイズ制限を指定する場合。カスタム ファイル サイズを指定するには、[データベース サイズ制限の有効化] を選択します。
[最大データベース サイズの指定]	製品ログ ファイルの許容可能サイズを指定します。値は 1 KB ～ 2000 MB の範囲で指定できます。 製品ログ ファイルが指定ファイル サイズを超える場合、循環ログによって古いログ イベントは再書き込みされ、最も古いログ エントリを削除すると新しいログ エントリがファイルに追加されます。
[エントリの保存期間を制限する]	設定した期間が経過したら、製品ログ エントリが削除されるようにする場合。
[エントリの最大保存期間の指定]	製品ログ ファイルに保存されたエントリを削除するまでの日数を指定します。値は 1 ～ 365 の範囲で指定できます。
[クエリーのタイムアウト]	製品ログ クエリーに対する許容応答時間を制限する場合。期間を指定するには、[有効] を選択します。
[クエリーのタイムアウトを指定（秒）]	製品ログ クエリーの最大許容応答時間（秒）を指定します。値は 1 ～ 3600 の範囲で指定できます。

3 [適用] をクリックして設定を保存します。

これで、[製品ログ] ページの設定を正常に構成できました。

エラー レポート サービス設定の構成

製品関連のエラーまたは例外を McAfee.

タスク

1 製品のユーザー インターフェースから、 [設定と診断] 、 [診断].

[診断] ページが表示されます。

2 [エラー レポート サービス] タブをクリックします。以下のいずれかを使用できます。

表 5-18 オプションの定義

オプション	定義
[有効]	エラー レポート サービスを有効または無効にします。
[例外の取得]	システム クラッシュなどの例外的なイベントに関する情報を記録します。
[ユーザーに例外を報告]	例外を管理者に報告するかどうかを指定します。

3 [適用] をクリックして設定を保存します。

製品ログの表示

イベント、情報、警告、およびエラーに関するログ エントリを使用して製品の正常性を表示します。例えば、タスクの開始および終了時刻、製品サービス エラーなどに関する情報を表示できます。

使用可能な検索フィルターを使用すると、検索したいログ エントリを検出できます。

製品ログ クエリー ページに関連する設定を変更するには、[設定と診断] 、 [診断] 、 [製品ログ] にアクセスします。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [製品ログ] の順にクリックします。[製品ログ] ページが表示されます。

2 [製品ログ] セクションでは、以下の項目を使用できます。

表 5-19 オプションの定義

オプション	定義
[ID]	特定の製品ログ エントリを識別する数字を指定します。例えば、2000 を超える ID で製品ログのみを表示する場合は、`200*` を指定します。
[レベル]	表示するログの種類に応じて、ドロップダウン リストから [情報]、[警告] または [エラー] を選択します。
[説明]	関連する説明を指定します。例えば、サービスの開始または停止に基づいてログを表示する場合は、`*service*` と入力します。
[すべての日付]	製品ログ ファイルのエントリに基づくすべての日付からイベントを含めます。
[日付の範囲]	要件に従って定義した日付の範囲内でイベントを検索します。ここでは、[開始] および [終了] パラメーターに対して年月日および時刻を指定できます。カレンダー アイコンを使用して、日付の範囲も指定できます。

表 5-19 オプションの定義 *(続き)*

オプション	定義
[フィルターをクリア]	デフォルトの検索設定に戻ります。
[CSV ファイルにエクスポート]	検索によって返されたすべてのアイテムに関する情報を .CSV 形式でエクスポートして保存します。ログに数千のイベントがある場合、複数のページを移動する代わりにこのオプションを使用して、これらのイベントを CSV 形式でファイルをダウンロードし、後で Microsoft Excel 形式のカスタム レポートを生成できます。 • CSV ファイルの検索結果内に特定のフィールドが見つからない場合、[表示するカラム] オプションの必要なフィールドを必ず有効化します。 • Microsoft Excel で [データのインポート] オプションを使用して、別のロケールで CSV ファイルを開きます。

3 [検索] をクリックします。

製品ログに保存可能なレコードの最大数は、ログ ファイルのサイズに基づきます。

検索条件と一致するイベントのリストが [結果の表示] セクションに表示されます。

DAT 設定の構成

システムに保管できる古い DAT の数を指定します。

DAT ファイルは検出定義ファイルのことで、シグネチャ ファイルとも呼ばれ、ウイルス、トロイの木馬、および怪しいプログラム（PUP）を修復するために、ウイルス対策ソフトウェアまたはスパイウェア対策ソフトウェアが検出するコードを識別します。DAT ファイルの用語については、http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat を参照してください。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [DAT 設定] の順にクリックします。

[DAT 設定] ページが表示されます。

2 [古い DAT の最大数] を使用して、通常のアップデート時にシステムに保管する必要がある DAT 生成の最大数を指定します。 MSME では、`<Install Folder>\bin\DATs` ディレクトリ直下に古い DAT と共に最新の DAT が保持されます。新しい DAT アップデートがあると、MSME によって利用可能な DAT の数が検証されます。利用可能な DAT 数が DAT 保持値を超える場合、最も古い DAT が削除されます。値は 3 ～ 10 の範囲で指定でき、デフォルト値は 10 です。

3 [適用] をクリックして設定を保存します。

構成設定のインポートとエクスポート

インポートして別の MSME サーバーで使用するために、設定を既存の MSME 設定 (設定とポリシー) をエクスポートします。 また、Sitelist をインポートして、自動更新のダウンロード元を指定できます。

製品のユーザー インターフェースで、[設定と診断] 、 [設定のインポート/エクスポート] の順にクリックします。[設定のインポート/エクスポート] ページでは、以下のタブを使用できます。

- [設定] ― 製品の設定をエクスポート、インポートまたは復元します。

表 5-20 設定タブーオプションの定義

オプション	定義
[エクスポート]	このサーバーの MSME 設定 (設定とポリシー) をコピーし、他の MSME サーバーがインポートに使用できる場所に保存します。 デフォルトの MSME 設定ファイルは `McAfeeConfigXML.cfg` です。
[デフォルトに戻す]	最大のパフォーマンスを得るため、MSME の設定をリセットします。
[拡張機能の復元]	MSME の設定を最大保護にリセットします。
[参照]	インポートする設定ファイル (`McAfeeConfigXML.cfg`) を検索します。
[インポート]	別の MSME サーバーの設定をこのサーバーに適用します。 たとえば、5 つのシステムに MSME 8.5 をインストールするには、次の手順に従います。 **1** システム 1 に MSME をインストールします。 **2** 必要な設定を行います。 **3** 設定を cfg ファイルにエクスポートします。 設定のインポート方法については、「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」の手順 10 を参照してください。 設定のインポートは、同じ製品バージョン間で行う必要があります。 たとえば、設定を MSME 7.6 または 8.0 サーバーから MSME 8.5 サーバーにインポートしないでください。

- [SiteList] ― 自動更新のダウンロード元の指定する Sitelist をインポートします。

表 5-21 Sitelist タブーオプションの定義

オプション	定義
[参照]	使用する Sitelist ファイル (`SiteList.xml`) を検索します。
[インポート]	DAT 更新をダウンロードするため、ファイルに指定された Sitelist の設定を適用します。

既存の MSME 設定のエクスポート

MSME サーバーの設定をエクスポートし、他の MSME サーバーからインポート可能な場所に保存します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [設定のインポート/エクスポート] の順にクリックします。

[設定のインポート/エクスポート] ページが表示されます。

2 [設定] タブをクリックします。

3 [エクスポート] をクリックします。

4 設定ファイルの保存先を指定します。デフォルトの設定ファイル名は `McAfeeConfigXML.cfg` です。

5 [保存] をクリックします。

これで既存の MSME 設定とポリシーが設定ファイルに正常にエクスポートされたので、他の MSME サーバーからインポートできます。

別の MSME サーバーから設定をインポートする

別のサーバーから MSME の設定を MSME サーバーに適用します。

設定は、次の 2 つの方法でインポートできます。

- ソフトウェアのインストール中に設定をインポートする。
- ソフトウェアのインストール後に、[設定と診断] ページで [設定のインポートとエクスポート] オプションを使用して設定ファイルをインポートする。

- 設定のインポートは、同じ製品バージョン間で行う必要があります。 たとえば、MSME サーバーの設定を MSME 7.6 サーバーから MSME 8.0 サーバーにインポートしないでください。
- 同じ Exchange の役割を有する MSME サーバーから設定をインポートすることをお勧めします。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [設定のインポート/エクスポート] の順にクリックします。

[設定のインポート/エクスポート] ページが表示されます。

2 [設定] タブをクリックします。

3 [設定のインポート] セクションから [参照] をクリックして、設定ファイルを見つけます。デフォルトの設定ファイル名は `McAfeeConfigXML.cfg` です。

4 [インポート] をクリックします。

[The operation completed successfully（処理が正常に完了しました）] というメッセージのダイアログ ボックスが表示されます。

5 [OK] をクリックします。

これで別の MSME サーバーからこのサーバーに設定が正常にインポートされました。

Sitelist のインポート

自動更新のダウンロード元の場所を指定する Sitelist をインポートします。

Sitelist には、自動更新のダウンロード元が指定されています。 デフォルトでは、自動更新のために McAfee URL をポイントする [SiteList エディター] が MSME で使用されます。

ご使用の MSME サーバーが McAfee ePO によって管理されている場合、自動更新の実行には ePolicy Orchestrator の Sitelist が使用されます。 MSME サーバーの管理に ePolicy Orchestrator を使用する場合は、MSME サーバーをローカル リポジトリにポイントする Sitelist を作成します。

代替 Sitelist は、McAfee AutoUpdate Architect ソフトウェアまたは McAfee ePO を使用して作成できます。

タスク

1 [設定と診断] 、[設定のインポート/エクスポート] の順にクリックします。[設定のインポート/エクスポート] ページが表示されます。

2 [Sitelist] タブをクリックします。

3 [Sitelist のインポート] セクションから [参照] をクリックして、`SiteList.xml` ファイルを見つけます。 このファイルには、リポジトリ名、サーバー URL などのリポジトリに関する情報が含まれます。

> `SiteList.xml` ファイルは `C:\ProgramData\McAfee\Common FrameWork\` ディレクトリにあります。 [スタート] 、[すべてのプログラム] 、 [McAfee] 、 [Security for Microsoft Exchange] の順に移動して、[SiteList エディター] を選択します。このファイルが使用され、レジストリの設定が表示されます。

4 [インポート] をクリックします。

[The operation completed successfully（処理が正常に完了しました）] というメッセージのダイアログ ボックスが表示されます。

5 [OK] をクリックします。

製品の更新をダウンロードするため、新しいリポジトリの場所をポイントする Sitelist が正常にインポートされました。

スパム対策プロキシ設定の構成

MSME がスパム対策ルールをダウンロードできるように、組織でインターネットへの接続にプロキシー サーバーを使用している場合に以下の設定を構成します。

このプロキシを使用して IP レピュテーションやメッセージ レピュテーションを取得したり、GTI サーバーからローカル URL データベースをダウンロードします。

> この機能を使用できるのは、McAfee Anti-Spam アドオン コンポーネントがインストール済みの場合に限られます。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [プロキシ設定] の順にクリックします。

[プロキシ設定] ページが表示されます。

2 [プロキシを使用する] を選択します。 [プロキシ サーバーの詳細] セクションでは、以下の項目を使用できます。

表 5-22 オプションの定義

オプション	定義
[IP アドレス]	プロキシ サーバーの IP アドレスを指定します。
[ポート]	インターネットにアクセスする通信に使用されるポートを指定します。
[認証情報の詳細]	認証の種類を指定します。 以下のオプションを使用できます。 • [匿名]－認証情報の詳細を指定せずにプロキシ コンピューターにアクセスします。 • [NTLM]－NT LAN Manager 認証情報を使用してプロキシ コンピューターにアクセスします。 • [基本認証]－プロキシ コンピューターにアクセスするためのシステムの [ユーザー名] および [パスワード] を入力します。[パスワードの確認] にパスワードを再入力します。

3 [適用] をクリックして設定を保存します。

6 プログラムの保守

インストール、修理、アンインストール、デフォルト設定の復元、データベースの削除および最適化などの製品メンテナンス タスクを実行します。

目次

- *インストールの変更*
- *デフォルト設定の復元*
- *削除と最適化*

インストールの変更

必要に応じて MSME プログラムを変更し、Exchange サーバーの役割を変更した場合にプログラム機能をコンピューターにインストールする方法を変更します。

また、MSME のインストール変更は、[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] コンソールからも実行できます。

タスク

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

2 ようこそ画面で [次へ] をクリックします。

[プログラムの管理] 画面が表示されます。

3 [変更] を選択し、[次へ] をクリックします。

4 変更するプログラム機能を選択し、[次へ] をクリックします。

5 [ライセンスに同意します] を選択して [次へ] をクリックします。

6 [インストール] をクリックして、変更したプログラム機能でインストールを完了します。

7 インストールが完了したら、[完了] をクリックします。

デフォルト設定の復元

製品をデフォルト設定に戻し、最高のパフォーマンスを実現します。

タスク

1 製品のユーザー インターフェースで [設定と診断] 、 [設定のインポート/エクスポート] をクリックします。[設定のインポート/エクスポート] ページが表示されます。

2 [設定] タブで [デフォルトの復元] をクリックします。

デフォルト設定を復元すると、構成済みのすべての設定とサブポリシーが削除されます。既存の設定のバックアップを取り、後で設定を復元することをお勧めします。

設定の確認を求めるダイアログ ボックスが表示されます。

3 [OK] をクリックします。

デフォルトの構成設定が適用されることを確認するダイアログ ボックスが表示されます。

4 [OK] をクリックします。

これで最高のパフォーマンスを発揮するために MSME サーバーがデフォルト構成設定に正常に復元されました。

削除と最適化

削除対象の古いアイテムをデータベースから削除し、最適化タスクを実行して、削除したデータベース レコードによって占有されていたディスク容量を回復します。

タスク

1 製品のユーザー インターフェースで、[設定と診断] 、 [検出されたアイテム] の順にクリックします。

[検出アイテム] ページが表示されます。

2 [ローカル データベース] セクションで、以下の項目を使用できます。

- [古いアイテムを削除する頻度]－削除対象の古いアイテムを MSME データベースから削除する頻度を指定します。デフォルト値は [毎月] に設定されています。
- [最適化の頻度]－削除したデータベース レコードによって占有されていたディスク容量を回復します。[アイテムの最大経過期間（日）] で設定した値に基づいて削除タスクをスケジュール設定済みの場合、古いレコードは削除されます。古いレコードを削除した後は、隔離データベースがサイズ制限に到達していない場合でも、MSME では [ディスク容量のしきい値（MB）] フィールドで指定したディスク容量が引き続き使用されます。データベースを最適化して縮小するには、最適化タスクのスケジュールを設定します。デフォルト値は [毎月] に設定されています。

最適化タスクのスケジュールは、常に削除タスクを実行してから数時間後に設定します。

3 スケジュール設定を変更するには、[スケジュールの編集] をクリックします。

これらのタスクを定期的に実行して、データベースに十分な空き容量を維持する必要があります。

7 トラブルシューティング

MSME 使用時の問題を判定し、対策を立てます。使用可能なパフォーマンス カウンターと、この製品に関連する重要なレジストリ キーについて説明します。

目次

- *デフォルトの構成設定と拡張構成設定*
- *重要なレジストリ キー*

デフォルトの構成設定と拡張構成設定

ユーザーの要件に基づき、最高のパフォーマンスまたは最高の保護機能を実現するように MSME を構成できます。

MSME の構成を変更するには、[設定と診断] 、 [設定のインポート/エクスポート] の順に移動します。 以下のオプションを使用できます。

- [デフォルトに戻す]ー最高のパフォーマンスを発揮できるように MSME を構成します。
- [拡張機能の復元]ー最高の保護機能を実現できるように MSME を構成します。

表 7-1 デフォルト構成と拡張構成の違い

機能	デフォルト	拡張
メッセージ レピュテーション	無効	有効
IP レピュテーション	無効	有効
入れ子の最大レベル	10	50
パスワードで保護されたファイル	通過を許可	置換と隔離
保護されたファイル	通過を許可	置換と隔離
ファイル フィルター	無効	デフォルト ルールで有効化（*.exe, *.com, *.bat, *.scr）
暗号化されたファイル	通過を許可	置換と隔離
破損したファイル	通過を許可	置換と隔離
メール URL レピュテーション	無効	オンアクセス スキャン ポリシーの場合にのみ有効にします。

重要なレジストリ キー

ユーザーの要件に重要性が一致する場合は、以下のレジストリ キーを作成します。

表 7-2 MSME－重要なレジストリ キー

レジストリ キー	パス	重要性
名前: DigestMail 種類:DWORD 値: 1	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\ADUserCache	SMTP アドレスに対するユーザー エイリアスのキャッシュを管理します。このレジストリ キーが使用されるのは、MSME が MQM に統合され、ダイジェスト メール機能に同じアドレスが使用されるときです。
名前: ODUserID 種類:REG_SZ 値:[例:<admin@domain.com>]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\E2007	すべての Exchange メールボックス サーバーにのみ有効です。 このレジストリ キーは、製品によって作成されるオンデマンド ユーザーのメール アドレスにする必要があり、Exchange データベースからメール データを取得するための Exchange Web サービスとの相互通信に使用する必要があります。
名前: EWSUrl 種類:REG_SZ 値:https://<IP address>/EWS/Exchange.asmx	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\OnDemand	Exchange 2010 メールボックス サーバーにのみ有効です。 このレジストリ キーは、CAS サーバーによってホスティングされる Exchange Web サービスへの接続に使用される URL です。 この値は、インストール時と MSME サービスの再起動時に PowerShell スクリプト GetHubTxDetails.ps1 によって自動的に設定されます。
名前: SCLJunkThreshold 種類:DWORD デフォルト値: 4	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	Exchange 2010 メールボックス サーバーにのみ有効です。 このレジストリ キーは SCL ジャンクのしきい値で、AD から取得され組織レベルに配置されます。 この値より上のスコアは迷惑メールとして処理されるため、Exchange 2007/2010 ハブ サーバーの迷惑メール ルーティングに役立ちます。 この値は、インストール後にしばしば PowerShell スクリプト GetSCLJunkThreshold.ps1 によって自動的に設定されます。
名前: IPBlackList 種類:REG_SZ 値: [例: 10.0.0.1]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState	IP レピュテーションに関係なく、特定の IP アドレスまたは IP アドレスの範囲からのメール送信を手動でブロックします。
名前: SPFMaxTimeSec 種類:DWORD デフォルト値: 5	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	SPF の実行が許可される最大時間。 定義した時間を経過すると、**一時エラー**が発生しますが、メールは配信されます。
名前: SPFCacheTimeoutSec 種類:DWORD デフォルト値: 43200	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	キャッシュ エントリが古くなるまでの時間。 デフォルトの期間は 12 時間です。
名前: SPFCacheMaxEntries 種類:DWORD デフォルト値: 5000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	キャッシュ内の最大エントリ数。

表 7-2 MSMEー重要なレジストリ キー *(続き)*

レジストリ キー	パス	重要性
名前: SPFDNSTimeoutMS 種類:DWORD デフォルト値: 1000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	DNS 要求のタイムアウト (ミリ秒)。
名前: CacheTimeOutForNullRecords 種類:DWORD デフォルト値: 60	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	NULL レコードのタイムアウト (ミリ秒) (一時エラーの場合)。

レジストリ キー SPFMaxTimeSec、SPFCacheTimeoutSec、SPFCacheMaxEntries、SPFDNSTimeoutMS、CacheTimeOutForNullRecords は、McAfee Anti-Spam コンポーネントをインストールするか、完全インストール オプションでソフトウェアをインストールした場合にのみ作成されます。

8 よくある質問

製品のインストール時や使用時によく発生しやすい状況に対する解決策を示し、よくある質問形式でトラブルシューティング情報を提供します。

今回のリリースに関連する質問の更新リストを表示するには、McAfee KnowledgeBase の記事 KB76886 を参照してください。

目次

- *全般*
- *ポリシー マネージャー*
- *設定と診断*
- *McAfee Anti-Spam アドオン コンポーネント*
- *正規表現（regex）*

全般

この項では、一般的によくある質問に対する回答を記載しています。

メールの配信に優先順位を付けることはできますか？

いいえ。Exchange サーバー タスクであるため優先順位を付けることはできません。

Exchange サーバー受信コネクターとの匿名アクセスを有効にする必要はありますか？

MSME では、Exchange 受信コネクターと匿名でアクセスする必要はありません。 オンデマンド ユーザーは、これらの機能の影響を受けます。 匿名アクセスの設定方法については、McAfee KnowledgeBase の記事 KB81752 を参照してください。

メールがハブ トランスポート サーバーでスキャンされる場合、メールボックス サーバーでもスキャンされますか？

状況に応じて異なります。 メールがハブ サーバーでスキャンされ、ウイルス対策 (AV) スタンプが押される場合、メールボックス サーバーではスキャンされません。 AV スタンプの AV ベンダーやエンジン/DAT バージョンのいずれかが異なる場合、メールボックス サーバーでもスキャンされます。

MSME ユーザー インターフェースを開く場合、Windows 2008 で「管理者として実行」オプションを使用する必要があるのはなぜですか？

セキュリティ上の理由のため、MSME は RPC サーバーと通信できません。 これは、SID には RPC プロセスとプロセス間通信 (IPC) を実行する権限があるためです。

どの実行可能ファイルを利用すると、MSME モジュールのスキャンがすべての Exchange バージョン全体で読み込まれますか？

`RPCServ.exe` プロセスによってすべてのスキャン バイナリが読み込まれます。 スキャナー プロセスのプロセス ID を検索するには、[タスク マネージャー] でコマンド ラインを確認し、`RPCServ.exe` プロセスにコマンド ライン パラメーター (/EVENTNAME:Global\MSME_scanner_RPCEvent) が含まれているか確認します。

どんな MSME 構成が最適ですか？

構成は、[拡張保護機能] および [最高パフォーマンス] を実現するためのものです。 デフォルト構成では、最高のパフォーマンスを発揮できます。

MSME とファイル レベルのウイルス対策が同じサーバーにインストールされている場合、何を除外する必要がありますか？

MSME バイナリ フォルダーとサブフォルダー、Postgres データベース、複製フォルダー、Exchange フォルダー、McAfee ePO イベント フォルダー、製品ログをすべて除外してください。

メール セキュリティに関する詳細情報はどこで参照できますか？

メール セキュリティに関する製品ソリューションについては、http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx を参照してください。

リモート システムの製品インストールにアクセスする方法を教えてください。

リモートの MSME スタンドアロン インターフェースにアクセスするには、次の手順を行います。

1 [McAfee Security for Microsoft Exchange - 製品構成] を開きます。

2 [サーバーの変更] メニューで、[新しい接続] をクリックします。

3 [コンピューターの参照] ダイアログ ボックスで、リモート システムの IP アドレスを入力し、[OK] をクリックします。

リモートの MSME Web インターフェースにアクセスするには、次の手順を行います。

1 [McAfee Security for Microsoft Exchange - 製品構成 (Web インターフェース)] を開きます。

2 アドレス バーに、`https://<リモート システムの IP アドレス>/MSME/0409/html/index.htm` を入力します。

3 プロンプトが表示されたら、ログイン認証情報を入力します。

MSME は TIE サーバーにどのように接続しますか？

MSME は、McAfee ePO から Data Exchange Layer (DXL) 経由で TIE サーバーに接続します。 MSME を管理する McAfee ePO で、TIE サーバーが管理されている必要があります。

MSME で TIE サーバーを設定する方法を教えてください。

MSME から TIE サーバーを直接設定することはできません。 MSME を管理している McAfee ePO サーバーで TIE サーバーを管理する必要があります。TIE サーバーと McAfee ePO を統合する方法については、『McAfee Threat Intelligence Exchange 製品ガイド』を参照してください。

ポリシー マネージャー

ここでは、[ポリシー マネージャー] 機能に関してよくある質問の回答を記載します。

電子メール ポリシーの作成と使用はどのように行えば良いですか？

ポリシーの作成は常に、ゲートウェイ サーバーでは SMTP アドレスを使用し、メールボックス サーバーでは Active Directory (AD) グループを使用して行います。 メールボックス サーバーでは、本製品によって SMTP アドレスが取得されないため SMTP アドレスに基づくポリシーの設計には非常にコストがかかります。同じアドレスを解決するためには、AD クエリーが実行されます。 これを実行すると、メールボックス サーバーでパフォーマンスが低下してしまいます。

ポリシー内のドメイン名はパフォーマンスに影響を及ぼしますか？

はい。 詳細については、前の質問 (「電子メール ポリシーの作成と使用はどのように行えば良いですか？」) を参照してください。

ポリシーの優先順位はどのように機能しますか？

解決の優先順位に基づき子ポリシーが最初に見たされると、次のポリシーは決して評価されません。

複数のポリシーを設定することに利点はありますか？また、そうするとサーバーのパフォーマンスに影響はありますか？

はい、複数ポリシーの設定によってパフォーマンスには影響があります。 ポリシーの評価時に最初の子ポリシーが満たされず次のポリシーが評価されると、AD クエリーが実行される可能性があり、これによってパフォーマンスが低下します。

詳細レベルで実行可能ファイルをブロックするためには、MSME をどのように設定すれば良いですか？

[ファイル フィルタリング ルール] オプションを使用すると実行できます。 たとえば、Windows の実行可能ファイルなど特定の実行可能ファイルをフィルタリングする方法について確認してみましょう。

1 製品のユーザー インターフェースで、[ポリシー マネージャー] 、[オンアクセス (マスター ポリシー)] の順にクリックします。

2 [コア スキャナー] で [ファイル フィルタリング] をクリックし、このオプションを有効にします。

3 [オプション（コアのスパム対策の設定）] で [編集] をクリックします。

4 [使用可能なルール] ドロップダウン リストで、[<新しいルールの作成...>] を選択します。

5 ルール名を指定し、[ファイル カテゴリ フィルタリング] で [ファイル カテゴリ フィルタリングを有効にする] を選択します。

6 [ファイル カテゴリ] リストから [Other specific formats（他の特定の形式）] を選択します。

7 [サブカテゴリ] リストで [Windows 実行可能ファイル] を選択します。

8 [保存] をクリックします。

どのような種類のファイルがパッカーまたは PUP として検出されますか？また、この設定はどこから制御できますか？

パッカーと PUP は悪意のあるコンテンツ カテゴリに属し、カテゴリに基づいて検出されます。 通常、パッカーとは所定のアルゴリズムを使用して圧縮またはパッキングされ、実行時に解凍されるファイルのことを指します。

この設定は、MSME ユーザー インターフェースの [ウイルス対策設定] から行います。

設定と診断

ここでは、[設定と診断] 機能に関してよくある質問の回答を記載します。

McAfee GTI で ca を有効にすると、電子メールが遅延しますか？

はい、McAfee GTI による電子メールの検証によって遅延が生じます。

トランスポート スキャナーがスパム電子メールをスキャンしているかどうかをどのように確認できますか？

これについては、以下のいずれかの方法で製品のユーザー インターフェースから確認できます。

- [最近スキャンされたアイテム] ページで、スキャンされたメールを参照して電子メールのスキャンに使用されたポリシーを確認します。[スキャンの種類] フィールドに [ゲートウェイ] が表示されるはずです。
- [検出アイテム] データベースで、スパム電子メールが検出されているかどうかを確認します。 最後に電子メールが認証されたセッションを介しているかどうかを確認します。これは、MSME の [デバッグ ロギング] で記録されます。

ブラックリストとホワイトリストを MSME サーバーから別のサーバーにエクスポートできますか？

はい。ブラックリストとホワイトリストを MSME サーバーから別のサーバーにエクスポートできます。 これを実行するには、次の手順を実行します。

1 製品のユーザー インターフェースで、[ポリシー マネージャー] 、[ゲートウェイ (マスター ポリシー)] の順にクリックします。

2 [コア スキャナー] で [スパム対策] をクリックします。

3 [オプション（コアのスパム対策の設定）] で [編集] をクリックします。.

4 [メール リスト] タブをクリックし、[エクスポート] をクリックしてすべてのブラックリストおよびホワイトリストに登録された送信者/受信者を CSV ファイルに保存します。

McAfee Anti-Spam アドオン コンポーネント

Anti-Spam アドオン コンポーネントに関してよくある質問への回答を以下に記します。

スパム対策エンジンを手動で更新するにはどうしたら良いですか？

レジストリ キーをアップグレードし、新しいエンジンを指定ディレクトリに配置します。このディレクトリは、`MSME\SystemState` レジストリの `SpamEngineVersion` レジストリ キーのレジストリで入力されます。これら 2 つの値は同期させる必要があります。例えば、エンジン バージョンが 9039 の場合、`MSME\Bin\AntiSpam\Engine` に `9039` という名前のディレクトリを作成し、エンジン ファイル `masecore.dll` をこのディレクトリにコピーします。

スパム対策ルールは手動で編集できますか？

いいえ。

電子メール アドレスをブラックリストに追加する前に、どのようなことを考慮する必要がありますか？

- McAfee Anti-Spam アドオン コンポーネントがインストールされていることを確認します。
- Microsoft Exchange サーバーはトランスポート サーバーにしてください。例えば、Exchange サーバーにはエッジ トランスポートまたはハブ トランスポートの役割を割り当てます。
- ユーザーが識別されない接続（電子メールをインターネットからサーバーが直接受信）を使用します。

電子メール アドレスをブラックリストまたはホワイトリストに登録するにはどうすれば良いですか？

1 製品のユーザー インターフェースで、[ポリシー マネージャー] 、[ゲートウェイ（マスター ポリシー）] の順にクリックします。

2 [コア スキャナー] で [スパム対策] をクリックします。

3 [オプション（コアのスパム対策の設定）] で [編集] をクリックします。

4 [メール リスト] タブをクリックし、ブラックリスト対象またはホワイトリスト対象の送信者/受信者などの必要なオプションの [追加] をクリックします。

電子メールのほとんどがスパムとして検出されていないのですが、どうすれば良いですか？

[設定と診断] 、[スパム対策] で、[メッセージ レピュテーションを有効にする] を選択して設定を適用します。また、スパム スコアを 51 ～ 79 の検出率を上げる値に調整します。

低めのスパム スコア（51 ～ 59）の電子メールは、それでも問題なしと判定される可能性があるため、スコアの微調整が必要になります。

Anti-Spam アドオン ライセンスはどこで入手できますか？

有効な McAfee Anti-Spam 承認番号をお持ちの場合は、McAfee ダウンロード サイトから MSMEASA.ZIP ファイルをダウンロードしていただけます。有効な McAfee Anti-Spam 承認番号をお持ちでない場合は、McAfee カスタマー サービス チームにお電話ください。

正規表現（regex）

ここでは、正規表現（regex）に関してよくある質問の回答を記載します。

正規表現を有効にすると、電子メールが遅延しますか？

はい。コンテンツ スキャンはプロセス集中型の設定であるため、正規表現を有効にすると電子メールが遅延します。

正規表現に関する詳細情報はどこで参照できますか？

正規表現の詳細については、インターネットのいくつかの Web サイトを参照してください。

以下にいくつか例を挙げます。

- http://www.regular-expressions.info/reference.html
- http://www.regexbuddy.com/regex.html

正規表現を使用して特定のクレジット カードや社会保障番号をブロックするにはどうすれば良いですか？

1 製品のユーザー インターフェースで [ポリシー マネージャー] 、 [共有リソース] の順にクリックします。[共有リソース] ページが表示されます。

2 [DLP とコンプライアンス ディクショナリ] タブで、[新規カテゴリ] をクリックしてカテゴリ名を指定します。

3 [OK] をクリックします。

4 [DLP とコンプライアンス ルール] で [新規作成] をクリックします。

5 [ルール名] と [説明] を指定し、[ワードまたはフレーズ] で正規表現を指定します。

表 8-1 例:クレジット カード番号の検証方法

カードの種類	正規表現	説明
Visa	`^4[0-9]{12}(?:[0-9]{3})?$`	先頭が 4 で始まるすべての Visa カード番号（新規カードは 16 桁、旧カードは 13 桁）。
MasterCard	`^5[1-5][0-9]{14}$`	先頭が 51 ～ 55 で始まる 16 桁の MasterCard 番号すべて。
American Express	`^3[47][0-9]{13}$`	先頭が 34 または 37 で始まる 15 桁の American Express カード番号。
Diners Club	`^3(?:0[0-5]|[68][0-9])[0-9]{11}$`	先頭が 305 ～ 305、36 または 38 で始まる 14 桁の Diners Club カード番号すべて。先頭が 5 で始まる 16 桁の Diners Club カードがあります。これは Diners Club と MasterCard のジョイント ベンチャーで、MasterCard として処理されるはずです。
Discover	`^6(?:011|5[0-9]{2})[0-9]{12}$`	先頭が 6011 または 65 で始まる 16 桁の Discover カード番号すべて。
JCB	`^(?:2131|1800|35\d{3})\d{11}$`	先頭が 2131 または 1800 で始まる 15 桁の JCB カード。先頭が 35 で始まる 16 桁の JCB カード。

上述の例に基づき、社会保障番号にも同様の正規表現を作成することもできます。 正規表現の詳細については、http://www.regular-expressions.info/examples.html を参照してください。

6 [正規表現] オプションを選択し、[保存] をクリックします。

7 [ポリシー マネージャー] 、[オンアクセス (マスター ポリシー)] 、[DLP とコンプライアンス] の順にクリックし、[ポリシー マネージャー] の [DLP とコンプライアンス] にこの正規表現を追加します。

8 [アクティブ化] で、[有効] を選択します。

9 [DLP とコンプライアンス ルールと関連するアクション] で、[ルールの追加] をクリックします。

10 [ルール グループの選択] で、以前に作成した正規表現ルールをドロップダウン リストから選択します。

11 ルールがトリガーされたときに実行されるアクションを指定します。

12 [保存] をクリックします。

索引

数字

2 番目
    アクション 61

A

Anti-Spam アドオン
    FAQ 142

D

DAT 設定
    構成 128
DLP とコンプライアンス 40
DLP とコンプライアンス スキャナー
    設定の構成 75
DLP とコンプライアンス ルール
    構成 66

E

Exchange Server
    保護 11

F

FAQ
    Anti-Spam アドオン 142
    regex 143
    正規表現 143
    設定と診断 141
    全般 139
    ポリシー マネージャー 140

H

HTML ファイル
    設定の構成 98

M

McAfee Quarantine Manager
    使用による隔離 119
MIME 35
MIME メール
    設定の構成 96
MQM とローカル データベース 39

P

PostgreSQL データベース 120

R

regex
    FAQ 143

S

Sitelist
    インポート 129, 130

V

VSAPI の設定
    構成 107

あ

アクション
    2 番目 61
    基本 61
    実行する 61
アラート
    新規作成 64
    構成 63
    製品の正常性の有効化 115
アラート メッセージ
    設定の構成 99

い

イベント ログ
    構成設定 124
インストール
    変更 133
インポート
    Sitelist 129, 130
    構成設定 129
    ブラックリスト 87

インポート *(続き)*
別のサーバーからの設定 130
ホワイトリスト 87

う

ウイルス 40
ウイルス対策スキャナー
設定 72

え

エクスポート
構成設定 129
ブラックリスト 87
ホワイトリスト 87
既存の構成 129
エラー レポート サービス
設定の構成 127

お

オンアクセス スキャンの種類
トランスポート 109
バックグラウンド 108
オンアクセス設定の構成
トランスポート スキャン 109
バックグラウンド スキャン 108
オンアクセスの設定 105
VSAPI の構成 107
オンデマンド
スキャン 23
オンデマンド スキャン 23
作成 24
スケジュールの設定 24
表示 23
オンデマンド ユーザー
パスワードのリセット 109

か

隔離されたアイテム
実行するアクション 48
隔離されたデータ
管理 39
隔離場所
設定 39
簡易検索フィルタ 34
管理
隔離されたデータ 39
スキャナー設定 71
その他の設定 99
フィルター設定 89

き

キー
レジストリ 136
機能
製品 7
脅威
組織に対する 10
禁止されたファイル メッセージ 40
禁止されているファイルの種類 40

く

グラフ
構成設定 122
グラフィカル レポート 33

け

継承
ポリシー表示 52
検索フィルター
比較表 45
プライマリ 42
検出
リアルタイム 11
検出アイテム
検索結果 48
実行するアクション 48
表示 39
詳細検索オプション 46
検出されたアイテム
比較表 45
プライマリ検索フィルター 42
検索 47
構成設定 118
検出タイプ 40
検出名 35
件名 35

こ

コア
スキャナ 55
フィルタ 55
コア スキャナー
設定の管理 71
更新
ソフトウェア 22
構成設定
DAT 128
McAfee Quarantine Manager 119
インポート 129
エクスポート 129
別のサーバーから 130

構成設定 *(続き)*
ローカル データベース 120
構成レポート 30
スケジュール設定 32
表示 31
電子メール通知 33

さ

サービス拒否 35
最適化
データベース 134
削除
データベース 134
作成
新しいアラート 64
オンデマンド スキャン タスク 24
サブポリシー 54
新規ユーザー用の新しいルール 60
サブポリシー 53
作成 54

し

実行するアクション
検出されたアイテム 48
自動更新
スケジュール設定 22
手動ブロック
IP アドレス 95
種類、オンアクセス スキャン
VSAPI 105
送信ボックス 105
トランスポート 105
バックグラウンド 105
プロアクティブ 105
使用可能
スキャナーとフィルター 57
詳細
ポリシー表示 52
詳細検索フィルター 35

す

スキャナ 55
スキャナー
使用可能 57
追加 59
設定 63
スキャナーとフィルター
比較表 57
リスト 58
スキャナ制御
設定の構成 94
スキャンの種類
オンデマンド 23
オンデマンド スキャン 23
スケジュール
オンデマンド スキャン タスク 24
スケジュール設定
自動更新 22
ステータス レポート 28
構成レポート 32
ステータス レポート 27
スケジュール設定 28
電子メール通知 30
表示 27
スパム 40
スパム スコア 35
スパム対策
設定 117
スパム対策スキャナー
設定の構成 84

せ

正規表現
FAQ 143
製品の機能 7
設定
McAfee Quarantine Manager の構成 119
イベント ログの構成 124
ウイルス対策スキャナー 72
エラー レポート サービスの構成 127
隔離場所 39
グラフの構成 122
スキャナー 63
設定、オンアクセス 105
設定、スパム対策 117
ダッシュボードの構成 121
通知 112
通知設定 113
デバッグ ログの構成 123
デフォルトと拡張 135
ファイル フィルタリング 77
ファイル フィルタリング ルール 69
ユーザーインターフェースの設定 121
ローカル データベースの構成 120
検出アイテムの構成 118
診断の構成 123
図の構成 122
製品ログの構成 125
設定と診断
FAQ 141
概要 103

設定の構成
DLP とコンプライアンス スキャナー 75
HTML ファイル 98
MIME メール 96
アラート メッセージ 99
スキャナ制御 94
スパム対策スキャナ 84
パスワード保護ファイル 92
フィッシング対策スキャナー 88
メール サイズ フィルタ 93
免責事項のテキスト 100
暗号化されたコンテンツ 91
署名付きのコンテンツ 92
破損したコンテンツ 90
保護されたコンテンツ 91
全般
FAQ 139

そ

組織への脅威 10
その他
設定の管理 99
ソフトウェア更新
スケジュール設定 22

た

タイプ、検出 40
タイム スロット 70
ダッシュボード 17
構成設定 121

ち

チケット番号 35

つ

追加
スキャナー 59
フィルター 59
通知
ステータス レポート 30
設定 112, 113
構成レポート 33

て

データベース
PostgreSQL 120
最適化 134
削除 134
デバッグ ログ
構成設定 123
デフォルトと拡張
設定 135
デフォルト設定
復元 134

と

統計 17
トランスポート スキャン
オンアクセス設定の構成 109

な

並べ替え
ポリシー 52
なりすまし
設定 87

は

はじめに 7
パスワード保護ファイル
設定の構成 92
パッカー 35
バックグラウンド スキャン
オンアクセス設定の構成 108

ひ

比較表
スキャナーとフィルター 57

ふ

ファイル フィルター
設定 77
ファイル フィルタリング ルール
設定 69
フィッシング詐欺 35, 40
フィッシング対策スキャナー
設定の構成 88
フィルタ 55
フィルター
使用可能 57
追加 59
設定の管理 89
フォルダーの除外
構成設定 111
不審なプログラム 35, 40
不要なコンテンツ 40
ブラックリスト
インポート 87
エクスポート 87
ブラックリストへの登録
IP アドレス 95

プロキシ設定
スパム対策の設定 131
プログラム
メンテナンス 133

ほ

保護
Exchange Server 11
ポリシー
並べ替え 52
優先順位 52
ポリシー表示
アドバンス 52
継承 52
ポリシー マネージャー
FAQ 140
ポリシー設定
コア スキャナーの管理 71
その他の管理 99
フィルターの管理 89
ホワイトリスト
インポート 87
エクスポート 87

ま

マスター ポリシー 53

め

メール
スキャン方法 13
メール URL レピュテーション 40
設定 78
メール サイズによるフィルタリング
設定の構成 93
メール、なりすまし
設定、ソフト エラー 88
設定、ハード エラー 88
メールボックスの除外 111
構成設定 111
免責事項のテキスト
設定の構成 100

ゆ

ユーザー
指定 60
ユーザーインターフェースの設定
設定の構成 121
優先順位付け
ポリシー 52

よ

よくある質問 139

り

リアルタイム
検出 11
リスト
スキャナー 58
フィルター 58

る

ルール
DLP とコンプライアンス 66
ファイルのフィルタリング 69
指定ユーザー用の新規作成 60

れ

レジストリ キー
MSME 136
レピュテーション チェック
使用、TIE 81
レポート
グラフィカル 33

ろ

ローカル データベース
使用による隔離 120
ローカル データベースと MQM 39

わ

ワイルドカード
例 112