TREND MICRO

InterScan™ for IBM Domino 5.6

管理者ガイド

Messaging Security

※注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
  http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

P/N: SNEM55971_130516_JP SLLNMM-AK0102_R1 (2016/11)

目次

はじめに

この管理者ガイドには、InterScan for IBM Domino (以下、InterScan) に関する説明、インストールとアンインストール手順、および特定のニーズに合わせた InterScan 機能の設定に役立つ情報が記載されています。

InterScan 管理者ガイドで説明する主な項目は次のとおりです。

- 第 1 章「 製品の概要」— 製品の概要とこのリリースのすべての新機能について説明します。
- 第 2 章「 インストール」— InterScan のインストール方法について手順を追って説明します。
- 第 3 章「 基本設定」— InterScan のインストール後に InterScan を設定するときの推奨手順を示します。
- 第 4 章「 検索タスクの設定」— InterScan で Domino 環境の保護に使用するポリシー、ルール、キーワードを作成する手順を説明します。
- 第 5 章「 管理の設定」— サーバのステータスを監視する手順、および個々の Domino サーバまたは Domino サーバグループにルールを作成する手順を説明します。
- 第 6 章「 アップデート」— ウイルス対策コンポーネントおよびコンテンツセキュリティコンポーネントをアップデートする手順を説明します。
- 第 7 章「 通知」— InterScan 通知を送信する手順を説明します。
- 第 8 章「 ログデータベースおよび隔離データベース」— InterScan のログデータベースおよび隔離データベースを最大限に利用するための手順を説明します。

- 第 9 章「 Trend Micro Control Manager からの管理」— Trend Micro Control Manager (以下、Control Manager) を使用して InterScan を管理する方法を詳しく説明します。
- 第 10 章「 アンインストール」— InterScan を削除する手順を説明します。
- 第 11 章「 トラブルシューティング」— トラブルシューティングのヒントを示します。
- 第 12 章「 サポート情報」— さらに多くの情報を得るためのガイドラインを示します。

また、InterScan 管理者ガイドには次の付録があります。

- 付録 A「 Domino 環境での脅威について」— Domino 環境で検出される脅威の種類についての情報を提供します。
- 付録 B「 ファイルおよびフォルダ一覧」— アプリケーションのインストールが正常に完了するとすぐに利用できる InterScan のファイルとフォルダの構造の一覧を示します。
- 付録 C「 バージョン 5.5 およびバージョン 5.6 の機能比較」— InterScan for Lotus Domino 5.5 と InterScan for IBM Domino 5.6 の機能の比較を示します。

バージョン 5.6 の新機能

InterScan は、IBM Domino 環境向けの強固な不正プログラム対策機能、APT 対策機能、コンテンツセキュリティ機能、および情報漏えい対策機能を備えています。InterScan は、ヒューリスティックなルールベースの検索、許可またはブロックする送信者のリスト、および署名データベースに基づいた最先端の検出機能を提供します。また、スパムメール対策機能、コンテンツフィルタ機能、および情報漏えい対策機能を組織のニーズに合わせて適用することができます。

注意： IBM Lotus Domino は、Domino 9.0 のリリースから、IBM Domino という名前に変更になりました。それに合わせて、トレンドマイクロの InterScan for Lotus Domino も、バージョン 5.6 以降は InterScan for IBM Domino という名前に変更しています。

高機能化により、これまで以上に柔軟かつスケーラブルな設定が可能となっています。

- 強化された Web レピュテーション
- 許可 / ブロックする送信者リストの強化
- ログの検索
- APT 対策の強化
- エンドユーザメール隔離 (EUQ) の強化
- マクロ検索の強化
- IBM Domino 9.0 のサポート
- IPv6 のサポート

強化された Web レピュテーション

Web レピュテーション検索は、トレンドマイクロの Smart Protection Networks (SPN) に基づいて、Web からの脅威や攻撃に対する最新の保護を提供します。本バージョンの InterScan では、Web レピュテーションの検出ログに、不正な URL のカテゴリ情報
(ソーシャル サイトやポルノ サイトなど) が示されるようになりました。さらに、パフォーマンスを高めるために、Web レピュテーションで検索するメッセージの種類を選択できるようになっています。たとえば、リソースを節約するために SMTP メールだけを検索したりすることが可能です。検索が完了すると、Web レピュテーションによる検出結果の通知が送信されます。

許可 / ブロックする送信者リストの強化

InterScan の以前のバージョンでは、スパムメールフィルタの許可 / ブロックする送信者リストと Web レピュテーションの承認する URL リストの両方について、サイズの制限がありました。本バージョンでは、これらのリストに対するサイズ制限が廃止されています。

ログの検索

InterScan の以前のバージョンでは、ログデータベース (smvlog.nsf) を検索することができませんでした。ログの検索は、セキュリティイベントを調査するうえで欠かせない機能です。本バージョンでは、ログを検索する機能が導入され、検索条件を設定できるようになりました。

ログ検索機能の詳細については、「ログの検索」(8-187 ページ) を参照してください。

APT 対策の強化

バージョン 5.5 以降の InterScan には、APT 対策として、高度な脅威検索エンジン (ATSE) と Deep Discovery Advisor (DDA) が統合されています。最新のサンドボックステクノロジを利用した DDA により、未知のリスクやゼロデイ攻撃について、セキュリティリスクレベルなどの検出結果が返されます。本バージョンでは、APT 対策のレベルを独自に設定できるようになりました。

特定の国からのメール攻撃はますます増加しています。本バージョンの InterScan では、文字セットを確認することで、このような国からのメール攻撃をブロックすることができます。

エンドユーザメール隔離 (EUQ) の強化

InterScan 5.5 以降では、エンドユーザメール隔離 (EUQ) を有効にした場合、すべてのユーザにこの機能が適用されます。InterScan 5.6 では、この機能が強化され、適用するユーザ / グループおよびメールテンプレートを指定できるようになりました。

マクロ検索の強化

マクロ検索では、ヒューリスティック検索を使用してマクロウイルスや不正プログラムを検出し、検出したすべてのマクロコードを除去します。本バージョンでは、マクロ検索のヒューリスティックレベルを設定できるようになりました。

IBM Domino 9.0 のサポート

このバージョンの InterScan は、最新の IBM Domino 9.0 に対応しています。

IPv6 のサポート

このバージョンの InterScan は、IPv6 に対応しています。

対象読者

InterScan のドキュメントでは、セキュリティシステムおよび IBM Domino のメール機能と情報共有システム機能の管理について基本的な知識があることが前提となっています。管理者ガイドおよび Domino ベースのオンラインヘルプは、Domino およびネットワーク管理者が対象となっています。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

第 1 章

製品の概要

InterScan for IBM Domino（以下、InterScan）5.6 は、Domino 環境に対するウイルス防御とコンテンツセキュリティを包括的に提供し、メールの添付ファイルやデータベースに潜むウイルスやアドウェア、スパイウェアをリアルタイムに検索できます。InterScan により、ウイルスや不正コードが Domino 環境に侵入しないように保護できます。

スイート版では、画期的なスパムメール対策技術や情報漏えい対策によって、より高いレベルの保護が実現されています。スイート版では、スパム検出を実行してから、リアルタイムでメール検索が行われます。

第 1 章で説明する項目は次のとおりです。

製品の概要

InterScan は、リアルタイムに動作して、ウイルス、不正コード (不正プログラム)、および迷惑な情報が、メール、データベース複製、または感染文書を通じて Domino 環境に侵入しないようにブロックします。不正プログラムの検索はメモリ内で実行されるので、極めて速い検索が可能です。

InterScan は、ネイティブの Domino サーバアプリケーションとして動作する よう設計されており、管理者にとって使 い慣れた、直感的に使用できるインタ フェースが用意されています。InterScan の設定インタフェースは Domino サーバと完全に統合されており、各種の IBM Notes ワークステーション、Web ブラウザ、または Domino R8/R9 Administrator クライアントからのリモート管理を実現できます。本バージョンの InterScan は、Microsoft Windows および Linux に対応しています。

InterScan では、すべてのモードでのセキュリティリスク検索とコンポーネントのアップデート、Web レピュテーション、コンテンツフィルタ、スパムフィルタ、エンドユーザメール隔離の機能を使用できます。情報漏えい対策付きスイート版では、さらに情報漏えい対策機能も使用できます。

InterScan では、Trend Micro Control Manager (以下、Control Manager) がサポートされています。Control Manager はトレンドマイクロが提供する集中管理コンソールであり、ウイルス対策やコンテンツセキュリティなどの保護を一元化するソリューションです。

管理者は、検索対象のデータベースを指定できるため、ユーザが感染していない文書を感染文書で上書きすることを防げます。手動データベース検索によって、既存の感染が駆除されます。

管理者は、InterScan を使用することで、企業のメールポリシーを施行したり、全体的なサーバの効率性を向上したりするだけでなく、ウイルスの大規模感染を最小限に抑えることができます。また、特定のファイルタイプをブロックするルールを作成したり、メッセージのブロック、遅延、優先順位付けを実行することもできます。企業ポリシーを実装すると、次のさまざまな方法で不正プログラムを処理できます。

- 後で駆除するかその他の処理を実行するために感染ファイルを隔離します。
- ファイルが感染しており駆除されていないことを示す通知とともに目的の受信者に感染アイテムを送信します。
- 感染ファイルを削除します。
- 感染ファイルをブロックして、配信されないようにします。
- 管理者に警告します。

マルチスレッド検索エンジンおよびメモリ検索を使用することにより、InterScan では効率性を最大限に高め、IBM Domino サーバへの影響を最小限に抑えることができます。管理者は、検索の不要なサーバを特定できるため、冗長な検索処理を排除できます。

お客さまの環境における InterScan を用いた包括的なセキュリティ対策については、次の Web サイトを参照してください。

http://jp.trendmicro.com/jp/home/

InterScan スタンダード版の機能

InterScan スタンダード版の機能は、次のとおりです。InterScan 日本語版ではスタンダード版の機能をすべて含むスイート版と、情報漏えい対策付きスイート版のみ提供されます。

- マルチスレッドのメモリ内検索処理により、高いパフォーマンスを実現。
- 不正プログラム検索と添付ファイルブロックの両方で、実際のファイル形式に基づく処理をサポート。
- 複数の Domino サーバで複数の InterScan インスタンスをサポート。
- リアルタイムメール検索、リアルタイムデータベース検索、手動データベース検索、および予約データベース検索。
- カスタマイズ可能な検索オプション (圧縮ファイル検索時の解凍後ファイルのサイズ制限、メッセージ本文検索の有効化など)。
- 検索の詳細なオプション
  - 新規文書や新たに変更された文書のみが検索されるため、データベースの手動検索および予約検索の際にサーバでの検索時間を大幅に短縮でき、システムリソースの消費を最小限に抑えられる増分検索オプション
  - 被害を受ける前にソースから不正なコードを除去する Notes スクリプト検索
  - リッチテキストおよび格納フォームホットスポットの検索
- 高度な脅威検索エンジン (ATSE) および Deep Discovery Advisor などの最新の技術による、APT (Advance Persistent Threat) 脅威からの保護。
- Domino 環境の保護、コンポーネントのアップデート、通知の送信、およびクラスタサーバに対する信頼を InterScan で実行する方法を定義する、ポリシーおよびルールの作成機能。
- 予約と手動によるコンポーネントのアップデート。
- InterScan による検索とアップデートの通知。
- Control Manager による先見的な大規模感染予防。
- 複数サーバ環境での信頼するサーバの設定。これにより、信頼するサーバで検索されたメッセージが再度検索されないようにして、サーバでの処理時間とリソースが節約されるように特定のサーバを設定できます。
- 隔離したメールと添付ファイルの情報を簡単に確認できる隔離データベース。

- 統計情報やグラフ作成が含まれる、ログとレポートの完全な機能。
- Trend Micro Threat Connect 情報ポータルとの統合。

InterScan スイート版の機能

InterScan スイート版には、スタンダード版のすべての機能と次の追加機能が含まれます。
InterScan 日本語版ではスタンダード版の機能をすべて含むスイート版と、情報漏えい対策付きスイート版のみ提供されます。

- エンドユーザメール隔離
- スパムメールフィルタ
- 件名または本文を基準としたメッセージの内容のフィルタ
- 添付ファイルの内容または名前を基準としたメッセージのフィルタ
- 添付の MS Office 文書、PDF、.txt、.html、および .rtf ファイルの検索
- Web レピュテーションフィルタ

情報漏えい対策付き InterScan スイート版の機能

情報漏えい対策付き InterScan スイート版には、スイート版のすべての機能と情報漏えい対策 (DLP) フィルタが含まれます。

InterScan のバージョンの比較

表 1-1 は、InterScan スイート版とスタンダード版の機能の簡単な比較を示しています。

表 1-1.　InterScan のスタンダード版とスイート版の機能の比較

機能	スタンダード版	スイート版	情報漏えい対策付きスイート版
ウイルス対策	あり	あり	あり
スパムメール対策	なし	あり	あり
Web レピュテーションサービス	なし	あり	あり
トレンドマイクロのアップデートサーバ	あり	あり	あり
Control Manager エージェント	あり	あり	あり

表 1-1. InterScan のスタンダード版とスイート版の機能の比較 (続き)

機能	スタンダード版	スイート版	情報漏えい対策付きスイート版
エンドユーザメール隔離	なし	あり	あり
APT (Advance Persistent Threat) 対策フィルタ	あり	あり	あり
Threat Connect との統合	あり	あり	あり
コンテンツフィルタ			
件名 / 添付ファイル / 本文 /MS Office、PDF、.txt、.html、および .rtf ファイル	なし	あり	あり
情報漏えい対策 (DLP) フィルタ			
件名 / 添付ファイル / 本文 /MS Office、PDF、.txt、.html、および .rtf ファイル	なし	なし	あり

注意： APT 対策フィルタは Windows 32 ビット版ではサポートされません。

InterScan が動作するしくみ

トレンドマイクロの検索エンジンでは、ルールベースの検出テクノロジとパターンファイルの検出テクノロジの両方が使用され、マクロウイルスを検出して削除する MacroTrap テクノロジも使用されています。ウイルスパターンファイルと検索エンジンの頻繁な自動アップデートには Web ベースのダウンロードメカニズムが使用されており、InterScan を終了する必要はありません。

InterScan では、図 1-1 に示すように、すべてのエントリポイントで添付ファイルや文書の内容が検索され、駆除が実行されます。

- IBM Domino メールサーバでは、メールの添付ファイルがリアルタイムに検索されます。
- データベースのイベントが監視され、ただちに添付ファイルが検索されます。
- 複製時に、データベースと変更されたデータが検索されます。

- メールボックスと Domino データベースに既存の添付ファイルが検索され、以前の感染が根絶されます。

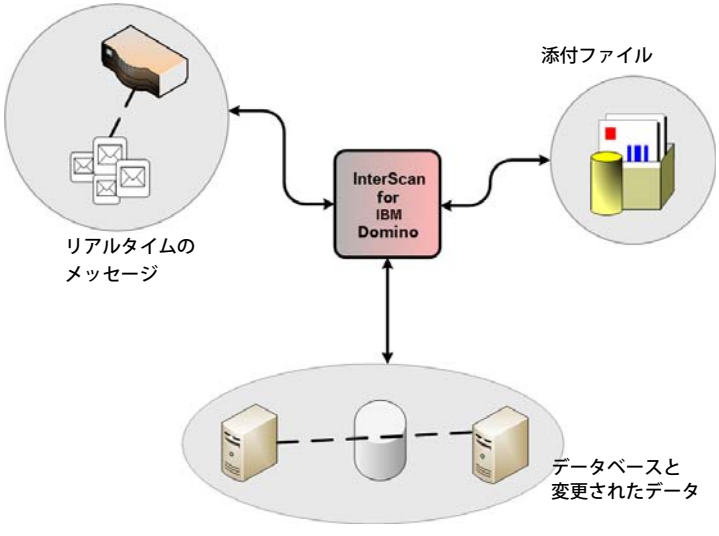


図 1-1.　脅威への感染は、デスクトップに広まる前に検出され、除去されます。

InterScan では、感染ファイルの詳細情報が示される包括的な活動ログが管理されます。

管理者は、Java ベースのグラフを使用することによって、企業の環境全体でウイルス感染を特定できます。さまざまなサーバから送られてきたレポートは、Notes のデータベース複製機能によって統合できます。

InterScan のコンポーネント

InterScan が正常にインストールされると、セットアッププログラムにより、Domino サーバに次のコンポーネントが追加されます。

- データベース
- データベーステンプレート
- タスク
- notes.ini エントリ

検索の種類

InterScan では、Domino メールルータタスクによって処理されたメッセージ、データベース、文書、およびディレクトリが検索されます。InterScan では、これらのアイテムが、指定のポリシーで定義されるフィルタとルールに基づいて処理されます。82 ページの「ポリシーベースのウイルス対策およびコンテンツセキュリティ保護の計画」を参照してください。

注意： InterScan には、インストール完了後ただちに Domino サーバを自動的に保護するための、初期設定のポリシーがあります。初期設定のポリシーは削除できません。

次の項目は検索されません。

- 暗号化メールとその添付ファイル
- パスワードで保護されたファイル
- 圧縮レベルが 21 以上のファイル
- 分割されたメッセージおよび不完全なメッセージ

InterScan で実行される検索の種類は、次のとおりです。

- リアルタイムメール検索
- リアルタイムデータベース検索
- 手動データベース検索と予約データベース検索

リアルタイムメール検索

リアルタイムメール検索では、メールトランザクションをすべて検索できます。これには、個別の Notes クライアントとの間で送受信されるメッセージのほかに、Domino ネットワークに属していない Notes クライアントとユーザの間で送受信されるメッセージも含まれます。たとえば、インターネットを経由するメッセージも検索できます。InterScan は、他の Notes ユーザや外部ソースから不正プログラムを受信しないようにユーザを保護します。

リアルタイムデータベース検索

リアルタイムデータベース検索では、どのデータベース文書が開かれたりアップデートされるときでも、リアルタイムでその変更を監視できます。リアルタイム監視では、すべてのデータベースまたは選択したデータベースを監視対象にでき、他のサーバとの間で相互に複製を実行するように指定されたデータベースの検索とフィルタが実行されます。

処理の効率化を図るために、変更された文書のみがチェックされ、不正プログラムがないか、ただちに検索されます。検索が終了するとその文書は閉じられ、次の文書の複製に移ります。この方法は、高速かつ正確で、経費がかかる回線または低速な電話回線を通じてリモートサーバとの間で複製を実行している場合に、特に役立ちます。

リアルタイムデータベース検索により複製プロセス全体が中断されることはありません。むしろ、感染ファイルが保存されることを防ぐだけで、その後の文書の複製が影響を受けることはありません。

Domino サーバにデータベースが多くあり、頻繁にアップデートされるファイルも多数ある場合は、リアルタイムデータベース検索に時間がかかり、プロセッサ集中型になることがあります。オーバーヘッドを最小限に抑えるため、ウイルス感染に対して最も脆弱なデータベースのみに対してリアルタイム検索を有効にすることができます。たとえば、ユーザデータベースは、Domino プログラムデータベースよりウイルスに感染しやすい傾向にあります。ユーザのメールファイルの文書と添付ファイルはリアルタイムメール検索で保護されるため、再検索する必要はありません。

頻繁には変更されないデータベースを保護するには、手動データベース検索または予約データベース検索を使用します。

手動データベース検索と予約データベース検索

手動検索と予約検索は、Notes データベースのみに適用されます。ハードディスクにあるその他のタイプのファイルは検索されませんが、

- Notes データベース内にあるファイルは、OLE 添付ファイルと不正スクリプトも含め、すべてのタイプをウイルスチェックできます。
- Notes データベース内にあるメールで送信された文書は、すべてコンテンツセキュリティと情報漏えい対策のチェックが行われます。

注意： 手動でメールボックスのデータベースを検索すると、リアルタイムメール検索タスクが開始され、その設定が適用されます。手動検索の開始時にリアルタイムメール検索タスクが実行されない場合は、Domino コンソールとログファイルにメッセージが表示されます。

予約検索および手動検索の操作に増分検索オプションを選択すると、新しい文書と前回の手動または予約検索以降に変更された文書のみが検索されます。これらの文書に検索を制限することによって、サーバのリソースと処理時間を節約できます。

警告： **検索時に使用するウイルスパターンファイルが期限切れになっていると、予約検索または手動検索で不正プログラムを検出できない場合があります。予約データベースルールまたは手動検索で増分検索を有効にすると、文書が感染していても再検索されず、不正プログラムを検出できません。最新のウイルス対策コンポーネントを使用して、全文書に対する手動検索を少なくとも週に 1 回は実行することをお勧めします (できるだけピークの時間帯を避けます)。**

詳細については、241 ページの「Domino 環境での脅威について」を参照してください。

ポリシー、ルール、およびフィルタの概要

InterScan では、Domino 環境の保護、コンポーネントのアップデート、通知の送信、およびクラスタサーバに対する信頼を実行する方法を定義するポリシーを作成できます。InterScan は、サーバごとに 1 つのポリシーを実装します。InterScan には、正常なインストール後に明示的なポリシーが実装されていないすべての Domino サーバを自動的に保護するための、リアルタイムメール検索ルールが含まれる初期設定のポリシーが用意されています。図 1-2 は、サーバのポリシーとそのポリシーを構成するルールとフィルタの関係を示しています。

- ポリシーは、Domino 環境の保護、コンポーネントのアップデート、通知の送信、およびクラスタサーバに対する信頼を InterScan で実行する方法を定義するルールで構成されています。1 つのポリシーが 1 つのサーバに適用されます。つまり、ポリシーは適用可能なすべてのプラットフォームで共有できます (たとえば、1 つの Windows サーバでホストされるすべての Domino サーバで同一のポリシーを実装できます)。
- ルールでは、次の項目が定義されます。
  - InterScan でリアルタイムメール検索を実行する方法
  - InterScan でリアルタイムデータベース検索を実行する方法
  - 予約データベース検索を開始する方法
  - ウイルス対策コンポーネントおよびコンテンツセキュリティコンポーネントのアップデートを実行するタイミング
  - 通知の配信方法

  ルールはポリシーごとに無限に定義できます。ただし、ルールの数が増えるほど、メッセージ 1 通の検査に要する時間も長くなります。

- ルールには、メッセージと添付ファイルに対する検索処理を実際に定義するフィルタが含まれます。

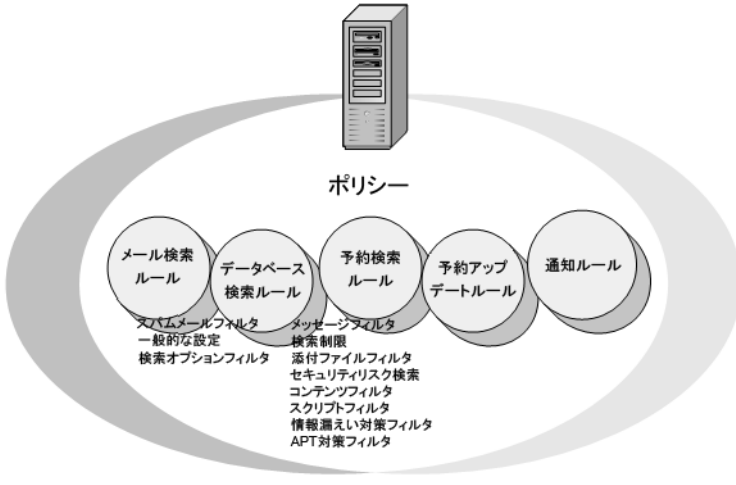


図 1-2.　ポリシー、フィルタ、ルールの関係

InterScan のルール

表 1-2 に示すように、InterScan では、InterScan がメッセージやデータベースを検索する方法を定義したルールを使用できます。

表 1-2.　InterScan のルールの種類

ルールの種類	InterScan による実行方法の定義対象
メール検索ルール	メッセージの内容と添付ファイルのリアルタイムでの検索およびフィルタ。リアルタイムメール検索ルールを作成するには、89 ページを参照してください。
データベース検索ルール	リアルタイムのデータベース検索。リアルタイムデータベース検索ルールを作成するには、94 ページを参照してください。
予約検索ルール	スケジュールに基づいたデータベース検索。予約データベース検索ルールを作成するには、96 ページを参照してください。

表 1-2. InterScan のルールの種類 (続き)

ルールの種類	InterScan による実行方法の定義対象
予約アップデートルール	ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントのアップデート。予約アップデートルールを作成するには、168 ページを参照してください。
通知ルール	通知の配信。通知ルールを作成するには、176 ページを参照してください。

InterScan のフィルタ

フィルタは、検索ルール (メール検索、データベース検索、または予約検索) のサブセットで、メッセージ、添付ファイル、および内容の検索処理を実際に定義します。フィルタオプションの種類は、次のとおりです。

表 1-3. InterScan のフィルタオプション

フィルタオプション	オプションによって設定される特定の検索処理の対象
セキュリティリスク検索	ウイルスおよびその他の不正プログラムの種類。
APT 対策フィルタ	文書の悪用を含む添付ファイル。
検索制限	圧縮、暗号化、およびその他の添付ファイルの種類。セキュリティリスク検索を有効にしておく必要があります。
メッセージフィルタ	さまざまなメッセージの種類。
添付ファイルフィルタ	迷惑な添付ファイル。
コンテンツフィルタ	管理者定義の明示的なルールに基づいて不適切とされる内容が含まれるメッセージ。
情報漏えい対策フィルタ	カスタムの情報漏えい対策ルールに違反するメッセージ。
スクリプトフィルタ	格納フォームまたはリッチテキストのホットスポットが含まれるメッセージ。

InterScan によるセキュリティ戦略

企業は、自社の環境を最大限に保護するためのセキュリティ戦略を構築する必要があります。InterScan による適切なセキュリティ戦略を選択するための重要な決定要素は次のとおりです。

- IT セキュリティにおける企業の総合的な方針
- Domino サーバで利用できるリソース (CPU、メモリなど)
- Domino 環境に不正コードが侵入する場合の考えられる侵入場所と侵入方法 (たとえば、メールメッセージ、Domino データベースの文書への添付ファイル、不正スクリプトコード)

ポリシーベースのウイルス対策およびコンテンツセキュリティ保護の計画

トレンドマイクロでは、ポリシーベースの機能を使用して、標準のウイルス対策設定およびコンテンツセキュリティ設定を確立および保守管理することをお勧めします。ポリシーを使用して、次の操作を実行できます。

- ウイルス対策設定とアップデート設定の繰り返し作成、およびその他のメンテナンス作業を自動化します。
- 1 台のサーバから環境内の全サーバを簡単に設定します。

ポリシーベースのウイルス対策を計画する際は、次の作業を考慮します。

- InterScan の初期設定ポリシーに基づいてグループポリシーを作成します。

  共通の役割を実行する複数のサーバが含まれる大規模なネットワークでは、個々のサーバに繰り返して作成するのではなく、共通の保護設定を一度だけ作成することによって、設定にかかる時間と管理作業が大幅に削減されます。
  初期設定のポリシーに基づくポリシーにすることにより、リアルタイムと予約によるメールとデータベースの検索保護設定の共通設定セットを、簡単に短時間で作成できます。これにより、個別のサーバに対して繰り返し作成する必要がなくなります。初期設定のポリシーについては、27 ページの「ポリシー、ルール、およびフィルタの概要」を参照してください。
- 特定の地域または管理範囲にあるすべての Domino サーバに適用可能な設定を割り当てるためのグループポリシーを作成します。マルチサーバ環境では、同じような機能または特性に基づいてサーバグループを定義することにより、適切なポリシーをグループ内のすべてのサーバに適用できます。
- 共通の目的を持つポリシーを作成します。たとえば、次のようなポリシーを作成します。
  - 同じ保護機能のリアルタイムメール検索が必要な、すべての Domino メールサーバ向けポリシー

- すべてのサーバ向けにリアルタイムと予約によるデータベース検索を要求するポリシー

  グループに含めるサーバ、およびそれらに適用する保護、アップデート、および通知方法を決定します。たとえば、1 つのメールサーバを保護するポリシーを作成して、同じくメールサーバとして機能する他のサーバにそのポリシーを適用できます。

- 特定の Domino サーバに設定を割り当てるための独自のポリシーを作成します。

  独自のポリシーにより、初期設定が個別のユーザ、ユーザグループ、またはサーバに割り当てられます。たとえば、特定の曜日にだけ実行される予約検索を設定するには、予約検索ルールを設定したポリシーを作成して、それを個別のデータベースサーバまたはそのグループに割り当てます。

ポリシーベースの環境でのルールとフィルタの実装の計画

トレンドマイクロでは、Domino 環境に対するウイルス対策およびスパムメール対策を最適化するためのルールおよびフィルタの実装について、次の戦略を実施することをお勧めします。

- すべてのメッセージと添付ファイルに対するリアルタイムメール検索ルールを作成します。
- 承認されない添付ファイルタイプと拡張子に対するフィルタルールを実装します (推奨設定のリストについては、128 ページの表 4-1 を参照)。
- すべてのデータベースに対するリアルタイムデータベース検索ルールを作成します。

ヒント： ユーザのメールファイル (メッセージ検索用にリアルタイムメール検索ルールを作成)、Domino システムデータベース、およびその他の頻繁には変更されないサイズの大きなデータベースの除外を検討してください。これによって、頻繁に変更されるデータベースにサーバリソースを割り当てることができます。

- ウイルス対策コンポーネントおよびコンテンツセキュリティコンポーネントの予約アップデートルールを作成します。
- すべての Domino データベースに対する予約データベース検索ルールを作成します。
- 不要なスパムや疑わしい URL メッセージに対する保護を実装するには、情報漏えい対策付き InterScan スイート版を購入します。InterScan 日本語版ではスタンダード版の機能をすべて含むスイート版と、情報漏えい対策付きスイート版のみ提供されます。
  - 包括的な情報漏えい対策を有効にします。
  - スパムメール対策を有効にして、実行する処理を指定します。
  - Web レピュテーション機能を有効にして、実行する処理を指定します。
  - IT セキュリティポリシーに従ってフィルタレベルを設定します。

- 許可する送信者とブロックする送信者を有効にして指定します。

また、システムに適切な数の検索タスクを指定します。InterScan の検索処理の詳細については、25 ページの「検索の種類」を参照してください。

第 2 章

インストール

第 2 章では、InterScan for IBM Domino (以下、InterScan) をインストールする方法について説明します。また、インストール後の設定方法、およびアクティベートする方法についても説明します。

第 2 章で説明する項目は次のとおりです。

InterScan の導入計画

ここでは、InterScan サーバを戦略的に分散配置して、Domino 環境に最適なウイルス対策とコンテンツ保護を実現する方法について説明します。同種のプラットフォームのみで構成した環境や異種プラットフォームが混在する環境に、InterScan のようなアプリケーションを導入する場合は、綿密な計画とその評価が必要です。

ネットワークに InterScan を導入する前に、次の項目を考慮することをお勧めします。

- 中央の InterScan サーバとして機能する Domino サーバを選択します。
- 選択した中央サーバに InterScan をインストールして、InterScan データベースの複製を有効にします。
- 他の Domino サーバ向けに、新しくインストールした ***smconf.nsf*** データベースと ***smvlog.nsf*** データベースの複製を作成します。
- 複製の競合を避けるため、各 Domino サーバの設定データベースは、InterScan ポリシーを管理する Domino Administrator のみで変更できるようにします。
- マスタの ***smvlog.nsf*** から InterScan ログデータベースの複製への Push 複製を開始して、ウイルスなどの不正なソフトウェアによるイベントをネットワーク全体にわたって集中管理します。
- 他の Domino サーバで、そのアップデートデータベースの複製にマスタアップデートデータベースから Pull 複製できるようにするかどうか決定し、中央の Domino サーバをトレンドマイクロのアップデートサーバに接続するだけで、最新コンポーネントのアップデートをダウンロードできるようにします。周辺サーバではアップデート元として複製データベースを選択すればよいことになります。詳細については、172 ページの「ダウンロード元の設定」を参照してください。

警告： バージョン 5.6 とそれよりも前のバージョンが同じネットワーク上にインストールされている場合は、ユーザインタフェースの競合を避けるため、前のバージョンのデザイン要素の複製設定を無効にする必要があります。

Domino サーバのアップグレード

InterScan をインストールしている Domino サーバをアップグレードする場合は、次の項目を考慮してください。

1. 次の InterScan ファイルのバックアップを作成して、元の設定内容を保存しておきます。
   - 次のフォルダ内のすべてのプログラムファイル

     Windows:C:¥Program Files¥Trend Micro¥ScanMail for Domino
     Linux:/opt/trend/SMID
   - 次のフォルダ内のすべてのデータファイル

     Windows: C:¥Program Files¥IBM¥Domino¥data¥smd
     Linux: /local/notesdata/smd
2. Domino サーバをアップグレードします。
3. Domino サーバのアップグレードが完了したら、InterScan が正常に機能することを確認します。機能しない場合は次を実行します。
   a. Domino サーバを停止します。
   b. 手順 1 で作成したバックアップファイルを対応するフォルダにコピーします。
   c. notes.ini ファイルを開き、次を追加します。
      - ServerTasks の最後に次を追加します。

        ```
        ,SMDemf,SMDreal,SMDsch,SMDmon,SMDcm
        ```
      - ファイルの最後に次を追加します。

        ```
        EXTMGR_ADDINS=SMDext
        SmStopMail=1
        ScanMailInstallPath=c:¥Program Files¥Trend
        Micro¥ScanMail for Domino
        SMLD_EUQ_ENABLED=0
        SMDSkipTaskList=COMPACT,FIXUP,UPDALL,UPDATE
        ```

      注意： c:¥Program Files¥Trend Micro¥ScanMail for Domino は、例として示したものです。InterScan バイナリをインストールした元のパスに置き換えてください。
4. Domino サーバを起動します。

試験的な導入

ネットワーク全体に InterScan を導入する前に、試験的なインストールを実施することをお勧めします。試験的な導入には次の利点があります。

- InterScan の習熟度の向上
- 企業ネットワークポリシーの構築や改善
- IT 部門やインストール担当部署では、導入プロセスの試行と改善ができ、導入計画が企業の事業要件と一致しているか検証できます。
- 各種機能の稼働状況や、本格的な導入後に必要になるサービスレベルについて確認するための機会となります。
- 改善が必要な設定を特定するのに役立ちます。

試験的な導入を実施するには

1. 導入の準備をします (36 ページの「導入の準備」を参照)。
2. 対象とするサイトを選択します (37 ページの「対象サイトの選択」を参照)。
3. ロールバック計画を作成します (37 ページの「ロールバック計画の作成」を参照)。
4. インストールを実施し、その結果を評価します (37 ページの「InterScan のインストールと評価」を参照)。

導入の準備

導入の準備段階では、次の作業を行います。

- テスト環境で使用する InterScan 複製モデルを決定します。

  InterScan 複製モデルとしては、ハブ - スポークモデルという中央集中モデルがよく使用されます。このモデルでは、ネットワーク管理者が、ハブの位置にある InterScan サーバで InterScan を設定します。他のサーバ、つまりスポークの先端に相当する周辺サーバでは、ハブサーバから InterScan 設定を Pull 取得します。
- 実行可能な導入パターンを評価して、自社の環境に最適な方法を決定します。
- 異種プラットフォームが混在する環境では、そこにあるすべてのシステム間で TCP/IP 接続を確立します。
- ハブサーバから各エージェントシステム、および各エージェントシステムからハブサーバに ping コマンドを送信して、双方向の TCP/IP 通信ができることを確認します。

対象サイトの選択

実稼働環境に類似のサイトを、テスト用のサイトとして選択します。InterScan 以外に実稼働環境での使用を計画しているウイルス対策と管理用のソフトウェア (Trend Micro ServerProtect (以下、ServerProtect) や Trend Micro Control Manager (以下、Control Manager))、およびサービスを使用しているサイトを選択します。実稼働環境を適切に再現できるようなサイトを選択してください。

ロールバック計画の作成

InterScan のインストール、稼働、またはアップグレードに伴う問題の発生に備え、対策措置を講じておくことをお勧めします。問題が発生したときに、ネットワークに発生する脆弱性の程度、および最小限のセキュリティを確保する方法を検討します。また、地域的な企業ポリシーや IT リソースも考慮します。

InterScan のインストールと評価

インストールを実施し、ウイルス対策とコンテンツのセキュリティ強化の観点、およびネットワークのパフォーマンスの観点の両面から求められるレベルに基づいて、その結果を評価します。このプロセスを通じて判明した利点、欠点を列挙します。発生する可能性のある問題点を特定し、それに応じて適切な導入計画を策定します。

この試験導入の結果は、実稼働環境への導入計画に反映させることができます。

システム要件

最新の情報については、次の Web サイトを参照してください。

http://www.go-tm.jp/isd/req

注意： システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

InterScan 5.6 のインストール

インストールプロセスを容易にするための事前タスクがいくつかあります。また、InterScan 5.6 をインストールする前に、次の点に注意してください。

- InterScan 5.6 をインストールした後では、InterScan 5.0/5.5 に自動的にはロールバックできなくなります。

  InterScan 5.0/5.5 にロールバックするには、InterScan 5.6 を削除して InterScan 5.0/5.5 を新規にインストールする必要があります。InterScan 5.0/5.5 のインストール方法については、該当するバージョンのマニュアルを参照してください。
- 物理的に同一のコンピュータに InterScan 5.0/5.5 と InterScan 5.6 の両方をインストールすることはできません (Windows のみ)。
- InterScan をインストールまたは削除する前に、Domino サーバをシャットダウンする必要があります。
- パーティションサーバでは、すべてのパーティションに対して同じバージョンの InterScan をインストールします。ただし、各パーティションには個別のバイナリをインストールできます。

注意： 各パーティションに個別のバイナリをインストールする場合、InterScan のインストール中はバイナリ共有を必ず無効にしてください。

インストール前のタスク

InterScan をインストールする前に、次のタスクを実行します。

1. Windows プラットフォームに管理者としてログオンするか、Linux プラットフォームに root ユーザとしてログオンします。
2. notes.ini の格納場所を指定します。パーティションサーバを使用する場合は、各パーティション上の notes.ini の格納場所を指定します。
3. Domino のデータパスとバイナリパスを指定します。
4. InterScan データベース管理に使用する管理者権限のあるユーザ / グループが存在することを確認します。初期設定のグループは **LocalDomainAdmins** です。
5. 空き容量が 1.5GB 以上あることを確認します。InterScan のハードウェアとソフトウェアの要件については、38 ページの「システム要件」を参照してください。
6. 開いている Notes クライアントをすべて閉じます。
7. 開いている Notes アカウントのセッションをすべて閉じます。
8. 次の作業を実行する前に、このコンピュータにインストールされたすべての Domino サーバを停止します。
   - InterScan 5.6 を初めてインストールする場合
   - InterScan 3.1 Linux 32 ビット版からアップグレードする場合
   - InterScan 5.0 Windows 版からアップグレードする場合
   - InterScan 5.5 Windows 版および Linux 32 ビット版からアップグレードする場合
   - InterScan 5.6 をアンインストールする場合
9. InterScan のアクティベーションコードを準備しておきます。
10. InterScan 3.1 Linux 版からアップグレードする場合は、CMAgent を削除します。手順については、InterScan 3.1 の管理者ガイドを参照してください。

目的のサーバがインストール可能な状態になっていることを確認した後、InterScan のプログラムファイルをインストールして、InterScan データベースを設定します。

セットアップモード

次の方法で、InterScan をインストールできます。

- ウィザードベースのインストール — 対話型のインストールであり、ユーザが各種情報を入力して、サーバに InterScan をインストールします。

ウィザードベースのインストールでは、InterScan のインストールを容易にするインタフェースが次々に表示されます。40 ページの「ウィザードベースのインストールの実行」を参照してください。

- サイレントインストール — InterScan のインストール時にユーザ操作を必要としません。

  サイレントインストールでは、セットアップで必要な情報をすべて収録した応答ファイルを使用します。スクリプトファイルを使用することで、複数の Domino サーバやパーティションサーバに短時間で InterScan をインストールできます。66 ページの「サイレントインストールの実行」を参照してください。

セットアップオプション

次に示す 4 種類のセットアップオプションが用意されています。

- 新規インストール — InterScan を初めてインストールする場合のオプションです。
- インストール — 追加した Domino サーバに、現在と同じバージョンの InterScan をインストールする場合のオプションです。
- アップグレード — 現在インストールされている InterScan を、最新のバージョンやビルドにアップグレードする場合のオプションです。
- インストールおよびアップグレード — 追加した Domino サーバに InterScan をインストールして、すでにインストールされている InterScan を最新のバージョンまたはビルドにアップグレードする場合のオプションです。

ウィザードベースのインストールの実行

セットアッププログラムを起動して、ウィザードベースのインストールを開始します。

InterScan 5.6 Windows 版のインストール

グラフィカルユーザインタフェースから InterScan 5.6 をインストールするには

1. 次のいずれかの方法で、セットアッププログラムに移動します。
   - InterScan の製品 CD からインストールする場合は、CD のプログラムフォルダに移動します。
   - トレンドマイクロの Web サイトからダウンロードしたソフトウェアをインストールする場合は、サーバ内でそのファイルを格納したフォルダに移動します。
2. setup.exe をダブルクリックします。

[InstallAnywhere] 画面　(図 2-1) に続いて、InterScan のインストール画面が表示されます。

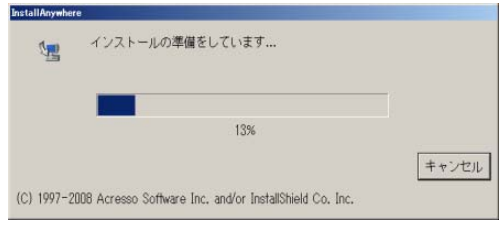


図 2-1.　[InstallAnywhere] 画面

InterScan の [InstallAnywhere] 画面の処理が終わると、InterScan の [ようこそ] 画面が表示されます。

図 2-2.　[ようこそ] 画面

3. [次へ] をクリックします。[使用許諾契約] 画面が表示されます。

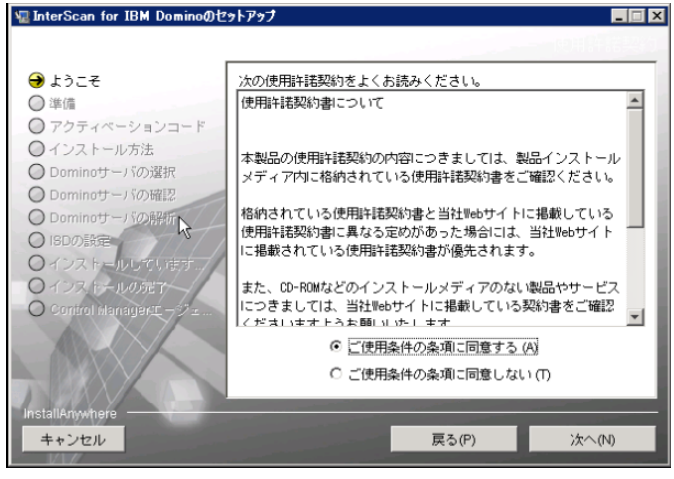


図 2-3.　[使用許諾契約] 画面

使用許諾の内容をご確認いただき同意できる場合は、[ご使用条件の条項に同意する] を選択して InterScan のインストールを続行します。使用許諾契約の条項に同意しない場合は、[ご使用条件の条項に同意しない] を選択します。インストールが中断されます。

4. [次へ] をクリックします。[アクティベーションコード] 画面が表示されます。

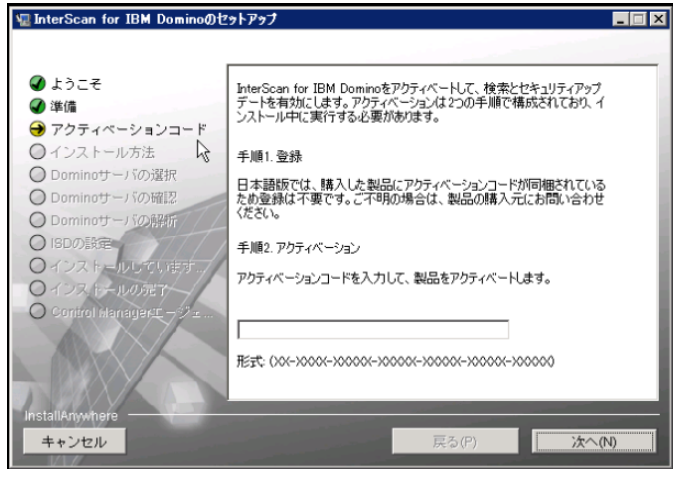


図 2-4.　[アクティベーションコード] 画面

5. 図 2-4 の　[アクティベーションコード] 画面では、InterScan をアクティベートするために、正確な InterScan のアクティベーションコードを入力する必要があります　(45 ページを参照)。

> **注意：** 新規インストールの場合は、InterScan の体験版、スタンダード版、スイート版、または情報漏えい対策付きスイート版をアクティベートするアクティベーションコードを取得してください。InterScan 5.0/5.5 に使用していたアクティベーションコードの期限が切れていなければ、同じアクティベーションコードを使用できます。

InterScan のアクティベーションコード　(45 ページを参照) を入力します。または、[次へ] をクリックして製品のアクティベーションを実行せずに、次へ進みます。次のいずれかを実行します。

- アクティベーションコードを入手済みの場合は、InterScan のアクティベーションコードを入力します。

  アクティベーションコードがない場合、または後日アクティベートする場合は何も入力せず、この画面から次の手順に進みます。InterScan はインストールされますが、InterScan の検索タスクおよびアップデートタスクはロードされません。Domino 環境を保護するために、インストール終了後、ただちに InterScan をアクティベートしてください 。

6. [次へ] をクリックします。[インストール方法] 画面が表示されます。

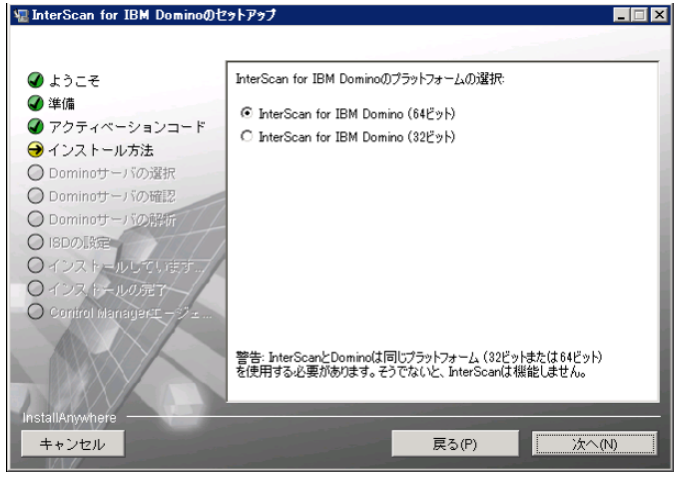


図 2-5.　[インストール方法] 画面

[インストール方法] 画面で、次のいずれかを選択します。

- InterScan for IBM Domino　(64 ビット)
- InterScan for IBM Domino　(32 ビット)

注意： Windows 32 ビット OS に InterScan をインストールする場合、または InterScan 5.0/5.5 からアップグレードする場合、[インストール方法] 画面 (図 2-5) は表示されません。

警告： Domino サーバプラットフォームは、InterScan のインストールタイプと一致する必要があり、一致していない場合は InterScan が機能しなくなります。たとえば、Domino サーバが 32 ビットの場合は、32 ビット用の InterScan をインストールする必要があります。Domino サーバが 64 ビットの場合は、64 ビット用の InterScan をインストールする必要があります。

---

7. [次へ] をクリックします。[Domino サーバの選択] 画面が表示されます。InterScan をインストールする ***notes.ini*** サーバを選択します。

注意： パーティションサーバがある場合は、保護するパーティションに InterScan をインストールします。

また、InterScan 5.0/5.5 からアップグレードする場合は、既存の ***notes.ini*** サーバファイルが表示されます。このファイルは削除できませんが、[追加] で他の場所を追加できます。

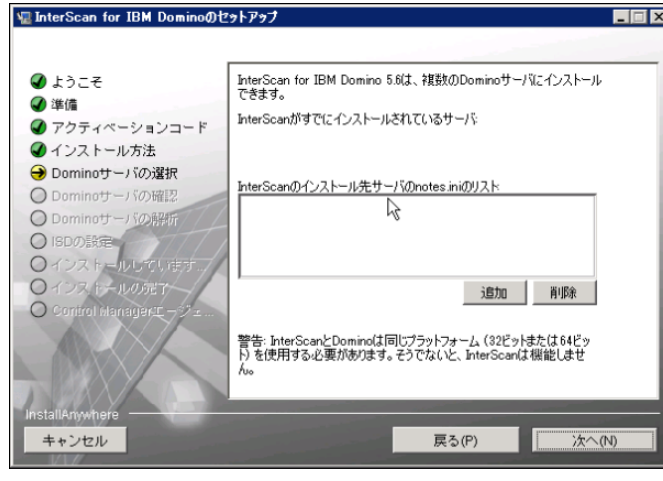


図 2-6. [Domino サーバの選択] 画面

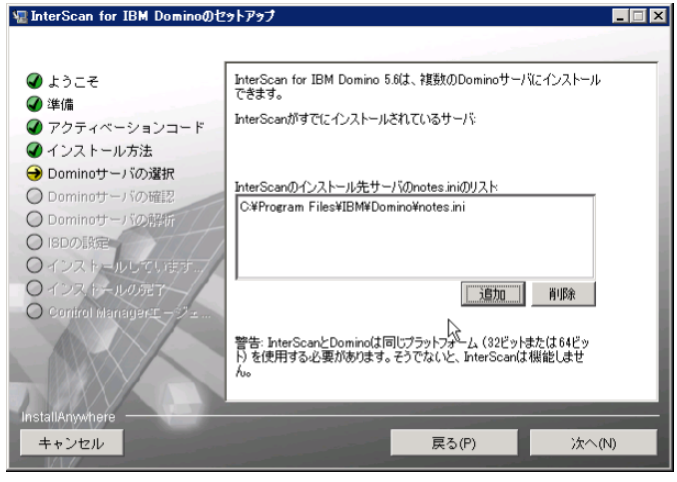


図 2-7. notes.ini のパスの選択

警告： InterScan が現在インストールされている場所を選択した場合には、警告メッセージが表示されます。これからインストールする場所を選択してください。

---

notes.ini のパスを選択したら、[追加] → [次へ] の順にクリックします。[Domino サーバの確認] 画面が表示されます。

8. [Domino サーバの確認] 画面で、Domino およびデータのディレクトリパスを確認します。

図 2-8. Domino プログラムとデータのディレクトリの確認画面

[次へ] をクリックします。[Domino サーバの解析] 画面が表示されます。

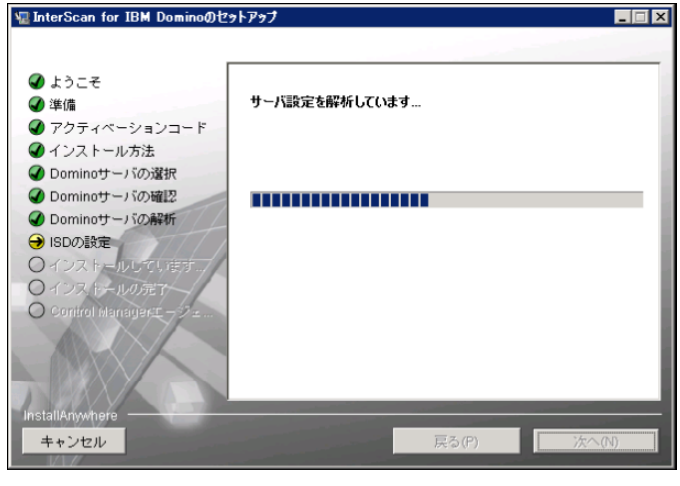


図 2-9. [Domino サーバの解析] 画面

9. 設定の解析画面での処理が終了したら、[次へ] をクリックします。[InterScan の設定] 画面が表示されます。

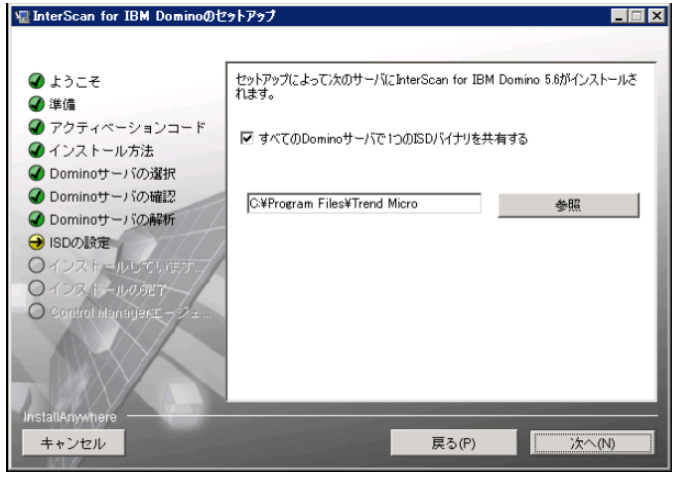


図 2-10.　[InterScan の設定] 画面

10. [InterScan の設定] 画面で、InterScan をインストールする場所を入力するか、参照します。[すべての Domino サーバで 1 つの InterScan バイナリを共有する] オプションをオフにした場合は、図 2-11 の画面が表示されます。

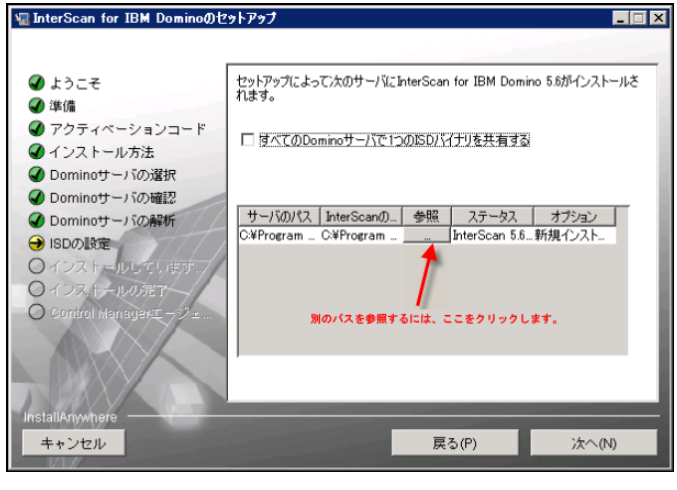


図 2-11.　サーバのインストールパスの選択

注意： Domino データフォルダには InterScan 製品バイナリをインストールしないことをお勧めします。InterScan で余分なログが生成される場合があります。

11. [すべての Domino サーバで 1 つの InterScan バイナリを共有する] オプションをオフにした場合は、図 2-11 に表示されている [...] をクリックして、新しいサーバパスを参照します。
12. [次へ] をクリックします。[データベース複製の選択] 画面が表示されます。

    初期設定では、隔離データベースを除くすべてのデータベースの複製が有効になります。初期設定を変更する場合は、セットアップで複製する InterScan データベースを選択するか、選択を解除します。

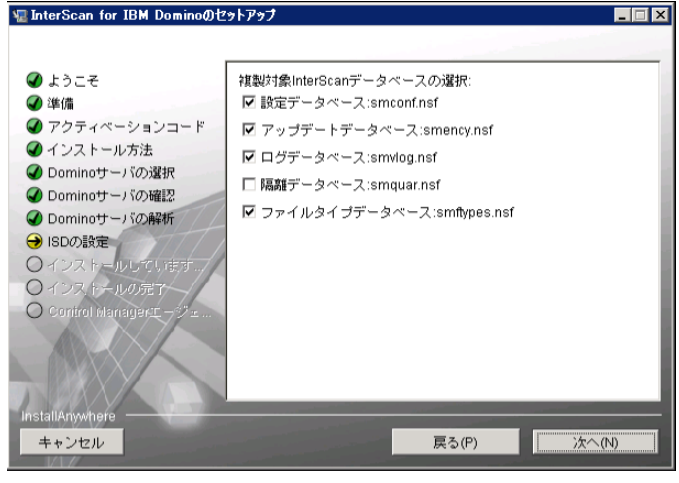


図 2-12.　データベースの複製設定

InterScan を複数のサーバにインストールしてデータベースの複製を実行する場合は、他のサーバの設定データベースへの複製を無効にしてください。1 つのサーバをプライマリサーバまたは管理サーバに選択して、他のすべてのサーバへ複製します。

注意： インストール終了後、すべてのサーバが初期設定ポリシーを取得できるように設定データベースの複製スケジュールを設定してください。

13. [次へ] をクリックします。初期設定ポリシーの選択画面が表示されます。初期設定ポリシーを取得するサーバを選択します。すでに InterScan がインストールされているサーバが存在し、設定データベースが複製対象に設定されている場合、その後のインストール作業ではこの画面での処理を省略できます。

単独の InterScan サーバ、中央サーバ (ハブ)、またはパーティションサーバのグループに属する最初のサーバは、常に初期設定ポリシーを取得する必要があります。サーバに初期設定ポリシーがインストールされていない場合は、新しいポリシーを作成した後に、そのサーバで `SMDReal` を再ロードします。

注意： `SMDReal` が適切に動作するためには、すべてのサーバにポリシーが存在する必要があります。インストールが完了したら、設定データベースの複製を予約して、すべてのサーバが初期設定ポリシーや指定したその他のポリシーを受信するようにします。

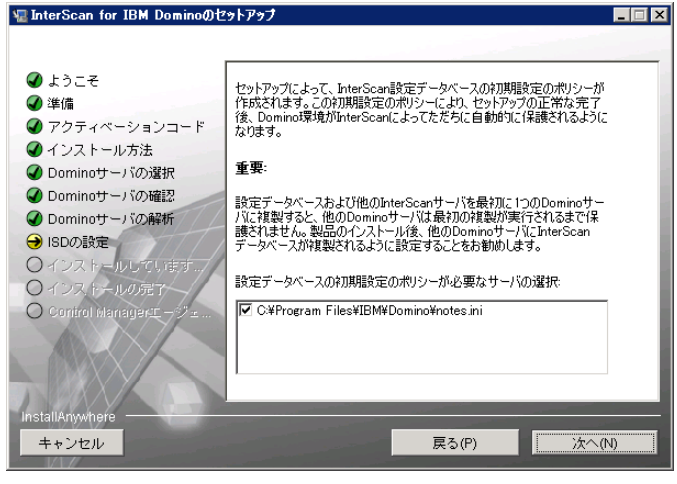


図 2-13. 初期設定ポリシー画面

14. [次へ] をクリックします。InterScan 管理者の選択画面が表示されます

    次のいずれかを実行します。

    - すべての InterScan データベースに管理者権限でアクセスできる単一の管理者アカウント名 / グループ名を入力します。

- インストール先のサーバがパーティションサーバで、パーティションごとに異なる管理者グループが設定されている場合は、パーティションサーバごとに異なるユーザまたはユーザグループを指定した後 (いずれも複数指定可)、[管理者アカウントの入力] フィールドに各サーバの管理者アカウントを入力します。

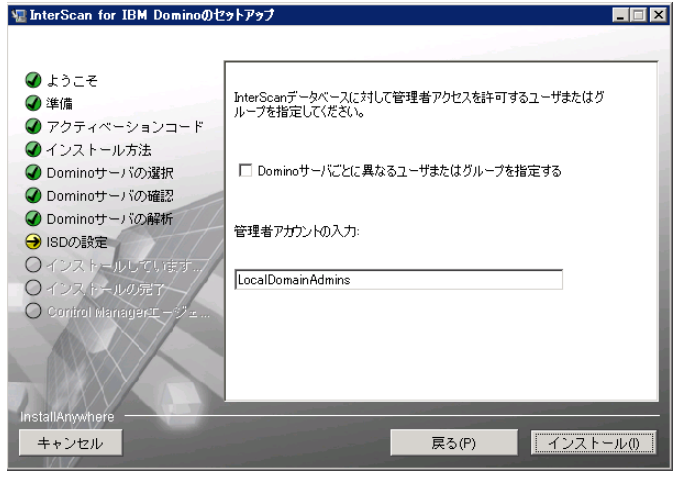


図 2-14. ユーザまたはグループアクセスの指定画面

注意： 指定したアカウントが存在しない場合は、インストールの完了時にそのアカウントを作成してください。そのアカウントには必ず管理者権限を与えてください。

15. [インストール] をクリックします。インストールが始まります。

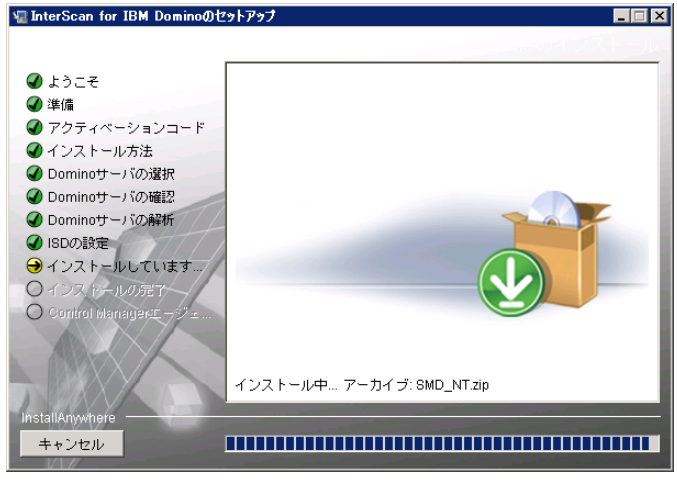


図 2-15. 選択したサーバに InterScan をインストール中

16. 図 2-15 のインストールが完了すると、[インストールの完了] 画面が表示されます。

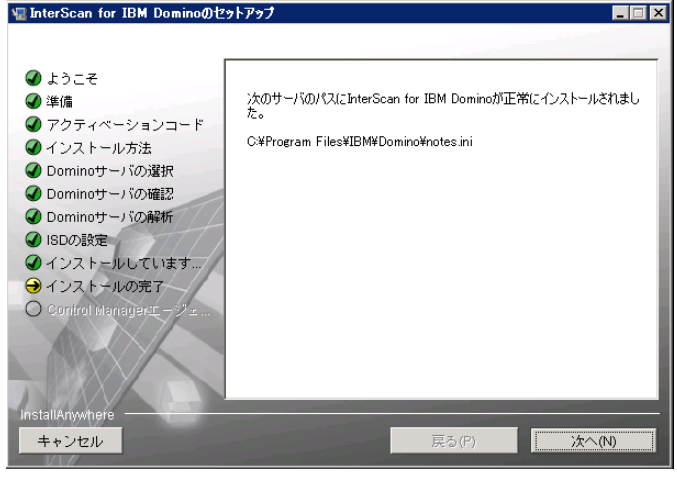


図 2-16. インストールの完了画面

17. [次へ] をクリックします。[Control Manager エージェントの起動] 画面が表示されます。

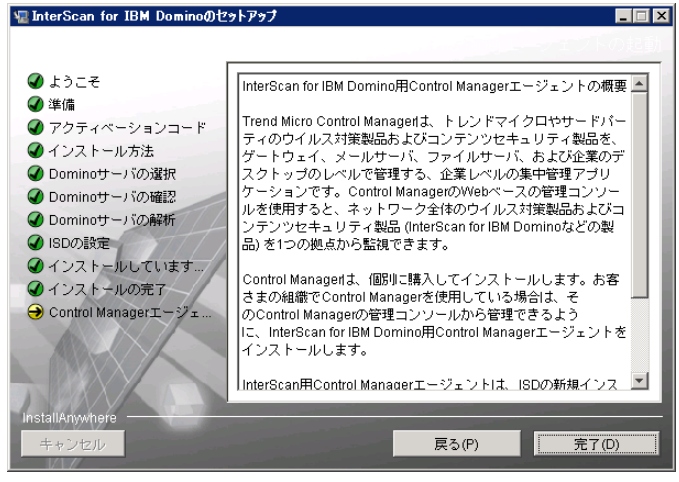


図 2-17.　[Control Manager エージェントの起動] 画面

18. [完了] をクリックしてセットアップ画面を閉じます。

InterScan が正常にインストールされたことを確認する方法については、71 ページの「EICAR によるインストールのテスト」参照してください。

InterScan をインストールする Domino サーバで ServerProtect などのウイルス対策製品を実行している場合は、71 ページの「InterScan の登録とアクティベーション」を参照してください。

InterScan 5.6 Linux 版のインストール

InterScan 5.6 をインストールするには、次の手順を実行します。

1. ターミナルを開きます。次のいずれかの方法で、インストールプログラムに移動します。
   - InterScan の製品 CD からインストールする場合は、CD のプログラムフォルダに移動します。
   - トレンドマイクロの Web サイトからダウンロードしたソフトウェアをインストールする場合は、サーバ内でそのファイルを格納したフォルダに移動します。

注意： 初期設定では、インストールファイルは `/tmp` ファイルシステムを一時フォルダとして使用します。ただし、IATEMPDIR 環境変数を十分な空き容量のあるパーティション上の別のディレクトリに設定することで、一時フォルダを変更できます。

この変数を設定するには、インストールを実行する前に UNIX のコマンドラインプロンプトで次のコマンドを入力します。

- Bourne シェル (sh)、Bourne-again シェル (bash)、Korn シェル (ksh)、および Z シェル (zsh) の場合

  ```
  $ IATEMPDIR=/your/directory/with/free/space
  $ export IATEMPDIR
  ```

- C シェル (csh) および TC シェル (tcsh) の場合

  ```
  $ setenv IATEMPDIR /your/directory/with/free/space
  ```

2. ***install.bin*** ファイルに実行権限があることを確実にするために、次のコマンドを入力します。

   chmod 755 install.bin

3. 次のコマンドを入力して、インストールファイル（***install.bin***）を実行します。

   ./install.bin -i console

   インストールプログラムによって、ファイルの展開が開始されます。

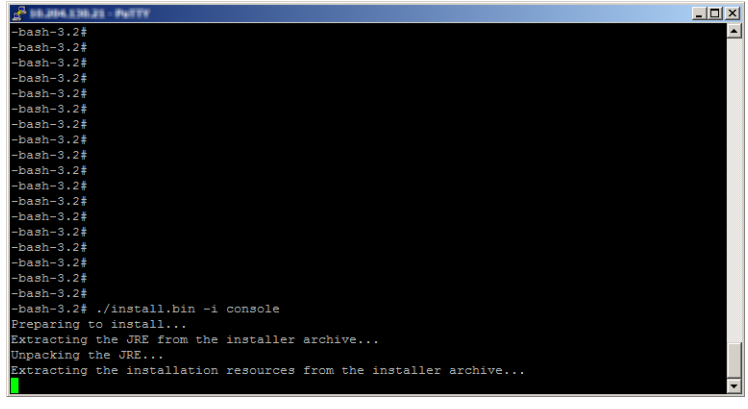


図 2-18.　インストールプログラムファイルの展開

インストールファイルの展開が完了すると、図 2-19 のように [ようこそ] 画面が表示されます。

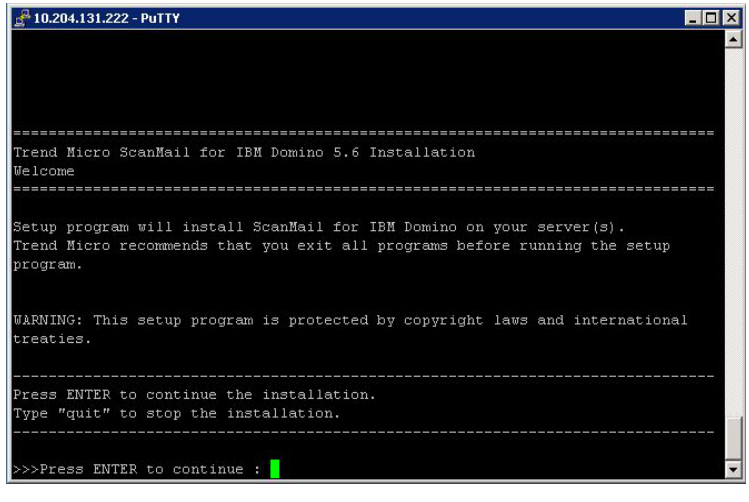


図 2-19.　[ようこそ] 画面

<Enter> キーを押して、インストールを続行します。使用許諾契約書の画面が表示されます。

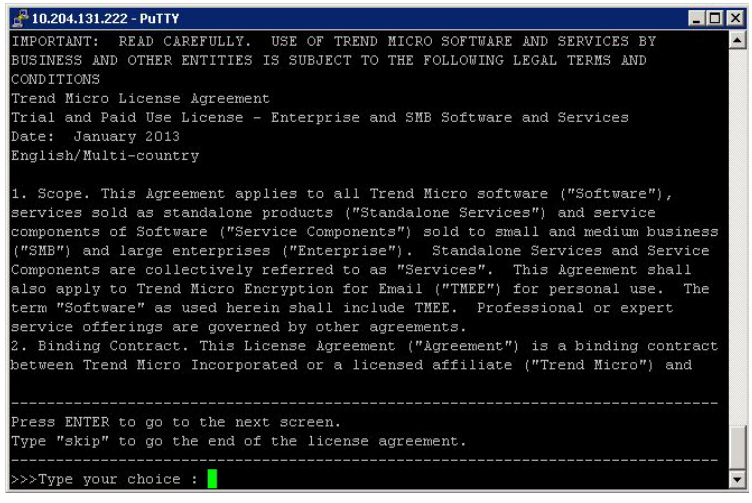


図 2-20. 使用許諾契約書の画面

4. 使用許諾契約書の画面で、<Enter> キーを押して、使用許諾契約の次の画面へスクロールを続行します。使用許諾契約の終わりまで移動する場合は、「*skip*」または「*s*」を入力し、<Enter> キーを押します。

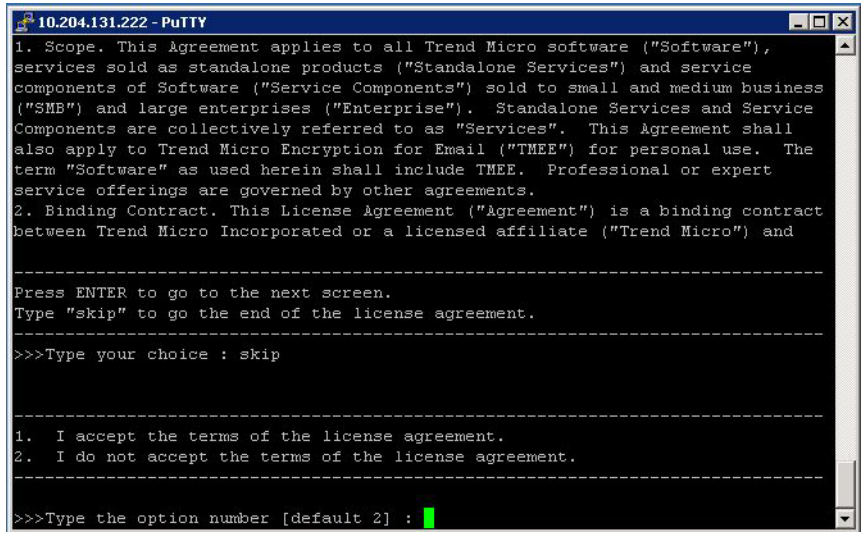


図 2-21. 使用許諾契約書の画面

5. 使用許諾契約の条項に同意する場合は、使用許諾契約書の画面の最後で、「*1*」を入力します。使用許諾契約の条項に同意しない場合は、「*2*」を入力します。「2」を入力すると、インストールが中断されます。

6. <Enter> キーを押します。製品のアクティベーション画面が表示されます。

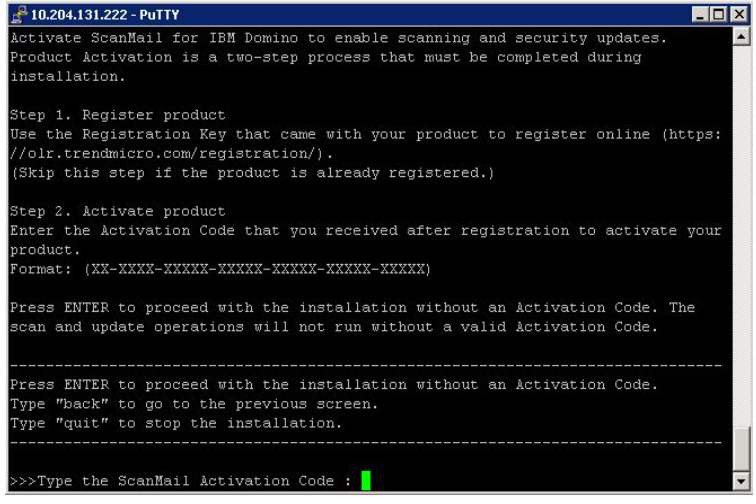


図 2-22. 製品のアクティベーション画面

7. 図 2-22 の製品のアクティベーション画面では、InterScan をアクティベートするために、正確な InterScan のアクティベーションコードを入力する必要があります (45 ページを参照)。

注意： 新規インストールの場合は、InterScan の体験版、スタンダード版、スイート版、または情報漏えい対策付きスイート版をアクティベートするアクティベーションコードを取得してください。

次のいずれかを実行します。

- アクティベーションコードを入手済みの場合は、InterScan のアクティベーションコードを入力します。

  アクティベーションコードがない場合、または後日アクティベートする場合は何も入力せず、この画面から次の手順に進みます。InterScan はインストールされますが、InterScan の検索タスクおよびアップデートタスクはロードされません。Domino 環境を保護するために、インストール終了後、ただちに InterScan をアクティベートしてください (71 ページを参照)。

<Enter> キーを押します。

8. アクティベーションコードを使用せずに続行するように選択した場合は、確認を求められます。次のいずれかを実行します。

a. アクティベーションコードを使用せずに InterScan のインストールを続行するには、「*y*」を入力して、<Enter> キーを押します。

b. インストールのこの時点でアクティベーションコードを入力する場合は、次の操作をします。

   i. 「*n*」を入力して、<Enter> キーを押します。セットアッププログラムからアクティベーションコードの入力を求められます。

   ii. InterScan のアクティベーションコードを入力して、<Enter> キーを押します。

Domino サーバの追加または削除画面が表示されます。

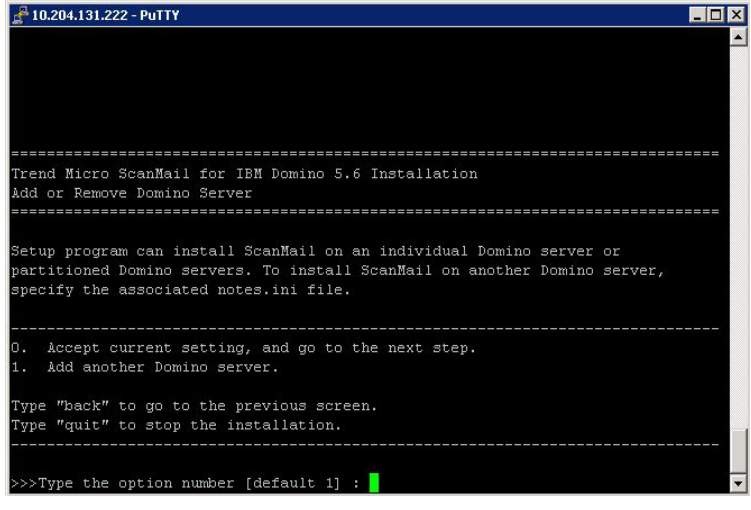


図 2-23. Domino サーバの追加または削除画面

9. 図 2-23 の Domino サーバの追加または削除画面で「*1*」を入力して <Enter> キーを押し、InterScan をインストールする ***notes.ini*** サーバを追加します。

注意： パーティションサーバがある場合は、保護するパーティションに InterScan をインストールします。

[Accept current setting, and go to the next step] オプションは、選択した Domino サーバ (***notes.ini***) のインストールを開始します。いずれの ***notes.ini*** も選択していない場合、[Accept current setting, and go to the next step] オプションはアクティブになりません。インストールプロセスを開始する前に、少なくとも 1 つの Domino サーバ (***notes.ini***) を選択する必要があります。

a. <Enter> キーを押します。図 2-24 の Domino サーバの追加画面 (notes.ini のパス [手順 1/4]) が表示されます。***notes.ini*** ファイルが存在する場所のパスを入力します。

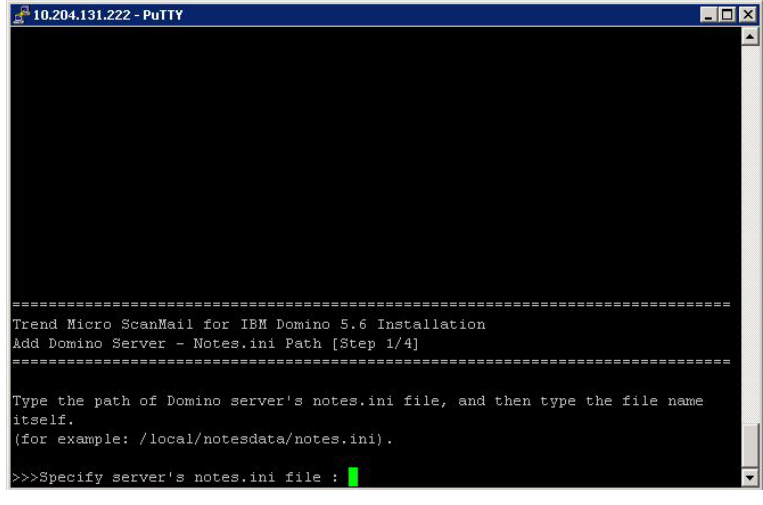


図 2-24. Domino サーバの選択画面

b. <Enter> キーを押します。Domino サーバの追加画面 (複製の設定 [手順 2/4]) が表示されます。

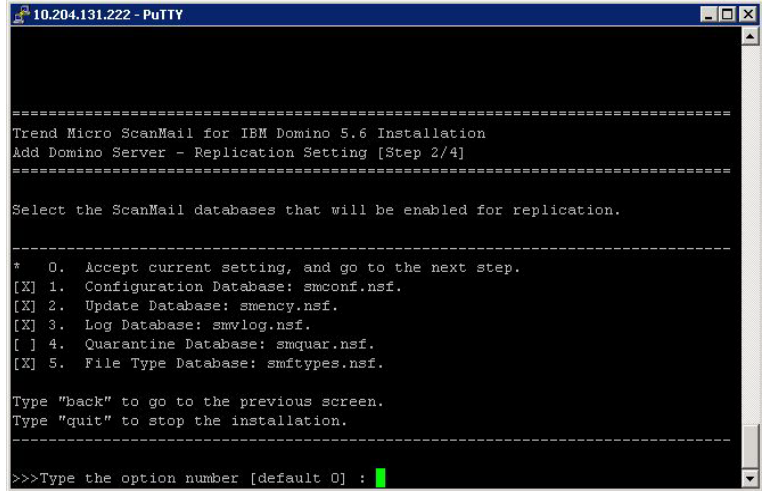


図 2-25. 複製の設定画面

初期設定では、隔離データベースを除くすべてのデータベースの複製が有効になります。初期設定を変更する場合は、セットアップで複製または無視する InterScan データベースを選択するか、選択を解除します。InterScan データベースを選択または選択解除するには、次の手順を実行します。

i. *1 ～ 5* の該当するオプション番号を入力します (たとえば、隔離データベースを選択する場合は「*4*」を入力します)。

ii. <Enter> キーを押します。

ヒント： InterScan を複数のサーバにインストールしてデータベースの複製を実行する場合は、他のサーバの設定データベースへの複製を無効にしてください。1 つのサーバをプライマリサーバまたは管理サーバに選択して、他のすべてのサーバへ複製します。

注意： インストール終了後、すべてのサーバが初期設定ポリシーを取得できるように設定データベースの複製スケジュールを設定してください。

選択後、「*0*」 (ゼロ) を入力し、設定を受け入れて次の手順に進みます。

c. <Enter> キーを押します。Domino サーバの追加画面 (InterScan の管理 [手順 3/4]) が表示されます。

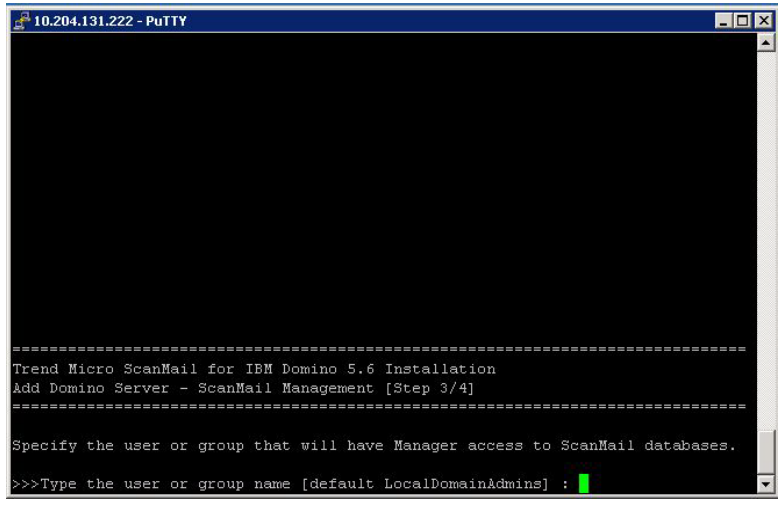


図 2-26. InterScan の管理画面

初期設定の管理グループは LocalDomainAdmins です。管理タスク用に別のユーザまたはグループを指定する場合は、すべての InterScan データベースに管理者権限でアクセスできる単一の管理者アカウント名またはグループ名を入力します。

注意： 指定したアカウントが存在しない場合は、インストールの完了時にそのアカウントを作成してください。そのアカウントには必ず管理者権限を与えてください。

d. <Enter> キーを押します。Domino サーバの追加画面 (インストールパス [手順 4/4]) が表示されます。

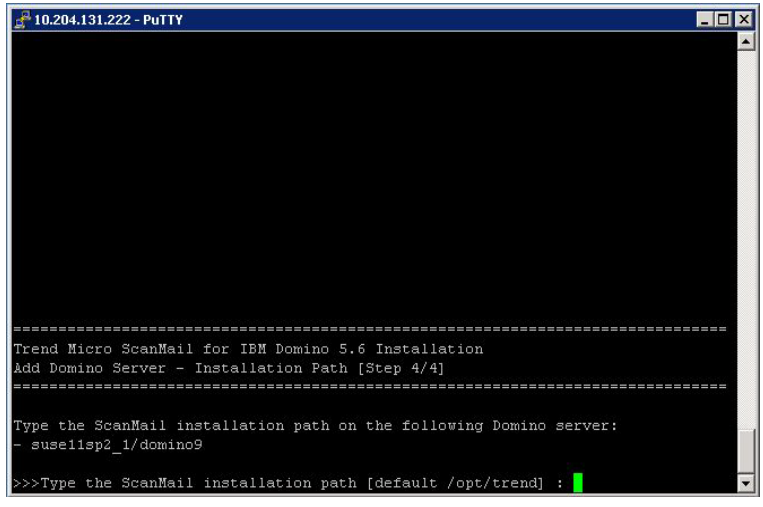


図 2-27. インストールパスの選択画面

InterScan をインストールする場所のインストールパスを入力します。初期設定では、`/opt/trend` にインストールされます。

注意： 1 つのパーティションサーバに InterScan 5.6 がすでにインストールされている場合は、それ以降のインストールの初期設定のインストールパスが同じになり、変更できなくなります。

e. インストールパスを入力したら、<Enter> キーを押します。1 つの Domino サーバの選択が完了し、Domino サーバの追加または削除画面が再度表示され、選択された Domino サーバが一覧表示されます。

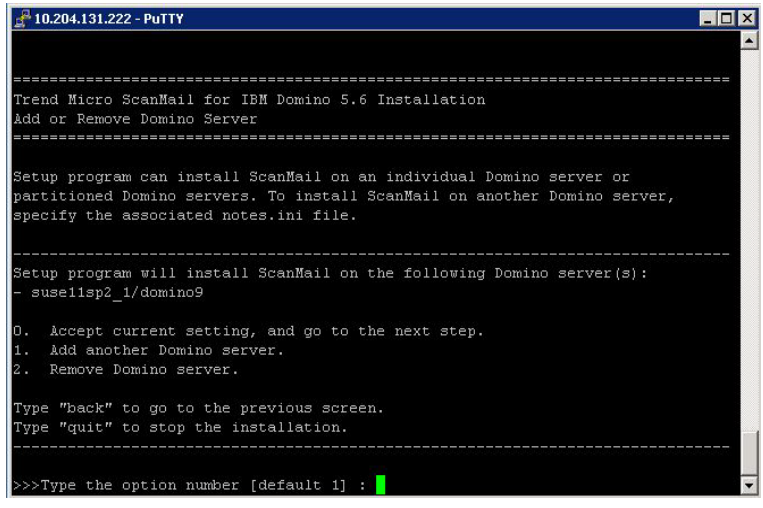


図 2-28. Domino サーバの追加または削除画面

図 2-28 の Domino サーバの追加または削除画面で、次のいずれかを選択します。

- 現在の設定を選択して、選択済みの Domino サーバのインストールを開始する場合は、「*0*」 (ゼロ) を入力します。
- 別の Domino サーバ (***notes.ini***) を追加する場合は、「*1*」を入力し、59 ページの手順 9 のサブ手順 a ～サブ手順 d の手順に従ってください。
- 前に選択した Domino サーバを削除する場合は、「*2*」を入力します。

10. <Enter> キーを押します。概要画面が表示されます。選択された Domino サーバのインストールを開始するには、「Y」または「y」を入力します。

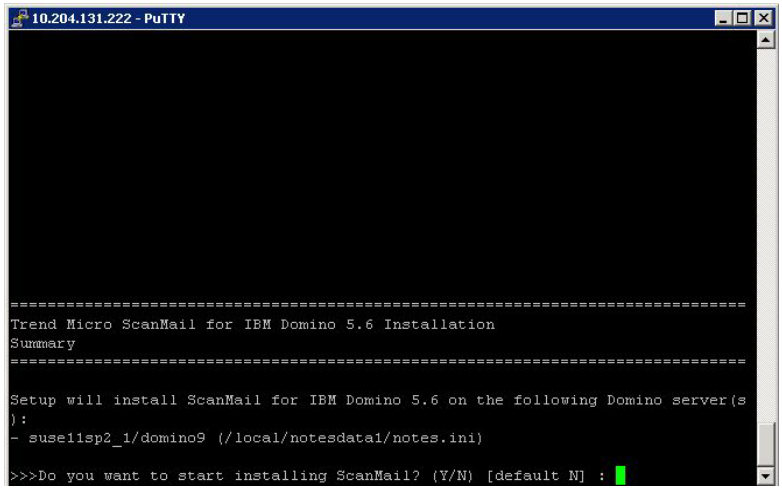


図 2-29. インストールの概要画面

11. <Enter> キーを押します。インストールが始まります。

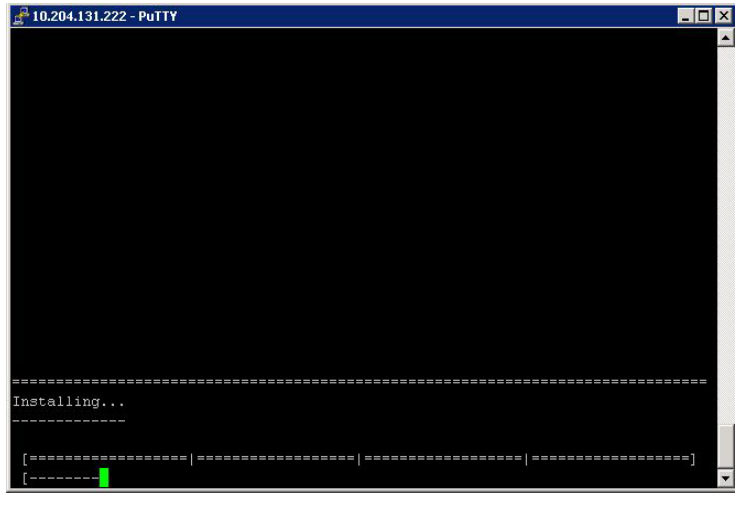


図 2-30. 選択したサーバに InterScan をインストール中

図 2-30 のインストールが完了すると、画面にインストール完了のメッセージが表示されます。

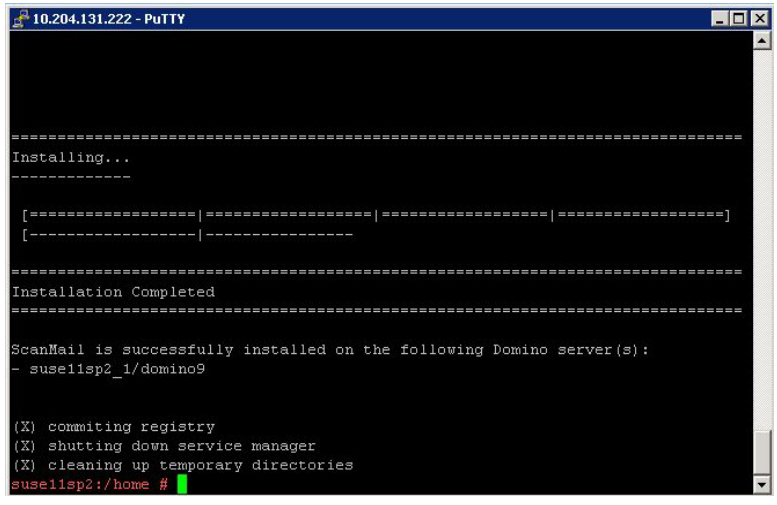


図 2-31. インストールの完了画面

注意： InterScan を初めてインストールする場合は、現在のターミナルセッションを終了して新しいセッションを開始します。

サイレントインストールの実行

InterScan のサイレントインストールでは、インストールで実行する手順の数を最小限にしてインストールを簡素化しています。`*.txt` 形式のスクリプトファイルに、InterScan のインストールに必要な情報が収められています。

このインストールプロセスを開始する前に、次を実行します。

- 必要なハードウェアコンポーネントとソフトウェアコンポーネントが正しく配置され、動作していることを確認します。
- ハードウェアとソフトウェアの要件について、弊社の「最新版ダウンロード」サイトにある最新の Readme をご参照ください。
- Domino サーバを停止し、他の Notes アプリケーションをすべて閉じます。この処理を忘れると、共有ファイルが破損し、セットアップを正常に実行できないことがあります。
- インストールスクリプトを準備します。

インストールスクリプトを使用して、以前に実行した InterScan のインストールを記録し、InterScan をインストールするすべてのサーバに対する InterScan のインストールを自動化します。このインストールスクリプトとは、インストールの過程で入力した応答を含むスクリプトファイルです。または、イントールスクリプトを使用して、InterScan のセットアップの種類をカスタマイズしたり、Domino サーバへのインストールオプションを指定したりします。

注意： サイレントインストールでは、InterScan の新規インストールおよびバージョン 5.6 へのアップグレードがサポートされます。ただし、インストールまたはアップグレードされるのは、記録スクリプトで指定されたサーバ上の InterScan のみです。以前のバージョンの InterScan がインストールされた環境でサイレントインストールを実行する場合は、すべてのサーバの情報をスクリプトファイルに必ず追加してください。

InterScan Windows 版のインストール

サイレントモードで InterScan をインストールするには

1. InterScan を単一の Domino サーバ、または複数の Domino サーバにインストールするときに、コマンドコンソールから次の情報を入力して、インストールの内容をサイレントインストールスクリプトに記録します。

   setup.exe -r “{スクリプトの絶対パスとファイル名}”

   例 :

   setup.exe -r “c:¥smd_silent.txt”

注意： InterScan のサイレントインストール用スクリプトを記録するときは、グラフィカルデスクトップ環境で開いたコマンドラインプロンプトからこのコマンドを実行します。

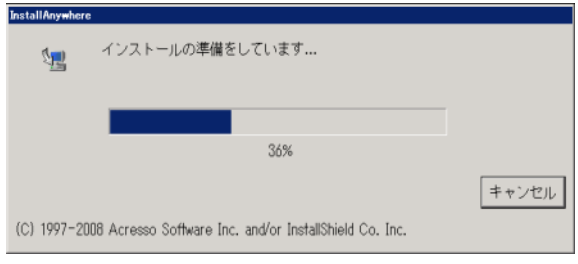


図 2-32. Windows サーバに対する InterScan のインストールを記録中の画面

2. コマンドコンソールで、次のコマンドを入力してサイレントインストールを開始します。

   silentinstall.bat

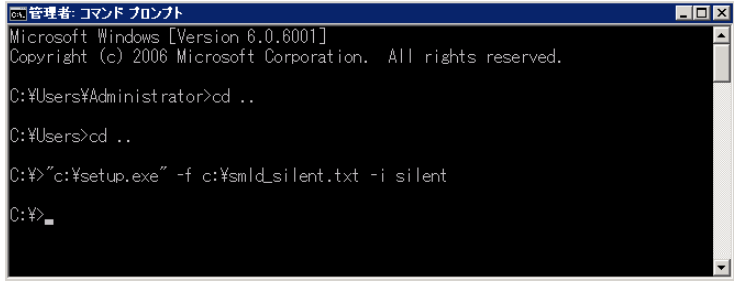


図 2-33. Windows サーバに対する InterScan のサイレントインストールを実行中の画面

3. サイレントインストールのログファイル ***smdins.log*** を開いて、インストール結果を確認します。このファイルは、ユーザの初期設定の一時フォルダに作成されます。エクスプローラアドレスとして「%windir%¥temp」と入力するとこのフォルダにアクセスできます。71 ページの「EICAR によるインストールのテスト」の手順に従って、InterScan が正常にインストールされているかどうか確認します。

InterScan Linux 版のインストール

サイレントモードで InterScan をインストールするには

Linux 版のインストールプログラムは以下の 2 種類があります。
該当するソフトウェアをインストールしてください。

32 ビット版 SMID.5.6.xLinux.x86_32.GM.b3349.tar.gz
64 ビット版 SMID.5.6.xLinux.x86_64.GM.b3349.tar.gz

1. InterScan を単一の Domino サーバ、またはパーティション化された Domino サーバにインストールするときに、ターミナルコンソールから次の情報を入力して、インストールの内容をサイレントインストールスクリプトファイルに記録します。

   ./install.bin -i console -r { パスとスクリプトファイル名 }

   たとえば、次のようなポリシーを作成します。

   ```
   ./install.bin -i console -r /tmp/silent.txt
   ```

2. ターミナルコンソールで、次のコマンドを入力してサイレントインストールを開始します。

   ./install.bin -i silent -f { パスとスクリプトファイル名 }

   たとえば、次のようなポリシーを作成します。

   ```
   ./install.bin -i silent -f /tmp/silent.txt
   ```

3. サイレントインストールのログファイル ***smdins.log*** を開いて、インストール結果を確認します。このファイルは、`/var/log` フォルダに作成されます。71 ページの「EICAR によるインストールのテスト」の手順に従って、InterScan が正常にインストールされているかどうか確認します。

Domino サーバの起動

InterScan 5.6 のインストールが終了したら、Domino サーバを起動して InterScan のタスクを開始します。EICAR を使用してインストール状況をテストし、InterScan が正常にインストールされているか確認します。詳細については、71 ページを参照してください。インストール後の設定については、73 ページの「基本設定」も参照してください。

Windows プラットフォームで Domino サーバを起動するには

1. 管理者としてログオンしていることを確認します。
2. [スタート] → [プログラム] → [IBM アプリケーション] → [IBM Domino サーバ] の順にクリックします。

Linux で Domino サーバを起動するには

1. InterScan をサーバコンピュータに初めてインストールした場合は、新規ターミナル (シェル) セッションを開きます。
2. root としてではなく、Domino ユーザアカウントでログインしていることを確認します。これは、コマンド **whoami** または **id** を実行することで確認できます。
3. Domino データディレクトリに移動し (たとえば、`local/notesdata`)、次のコマンドを実行して Domino サーバを起動します。

   $ <Domino binary directory>/server –jc &

ヒント： シェル環境をカスタマイズしていない場合は、次のコマンド実行し、Domino 起動スクリプトの場所を探して実行します。

<Domino binary directory>/server

注意： **<Domino binary directory>** は実際の Domino バイナリディレクトリに置き換えます。

Domino サーバの起動方法の詳細については、Domino のドキュメントを参照してください。

InterScan と他のウイルス対策製品

InterScan をインストールする Domino サーバ上で、ServerProtect などのウイルス対策製品を実行している場合は、各パーティションにある InterScan の `smd` ディレクトリと作業ディレクトリを、これらウイルス対策製品の検索対象から除外して、検索の競合を防ぎます (「検索ディレクトリの設定」にある作業ディレクトリの設定を参照)。

ServerProtect を使用している場合、その検索対象から Domino のフォルダとディレクトリを除外する方法については、ServerProtect のマニュアルを参照してください。

InterScan の登録とアクティベーション

InterScan の機能を利用するには、アクティベーションコードを入力して製品をアクティベートする必要があります。

アクティベーションコードはご購入の製品に添付されています。詳細については購入先にお問い合わせください。

EICAR によるインストールのテスト

EICAR (European Institute for Computer Antivirus Research) テストファイルを使用して InterScan をテストし、正常に動作することを確認しておくことをお勧めします。このテストスクリプトは、ウイルス対策製品が正しくインストールされ、設定されていることを確認するための安全な手段として、EICAR によって開発されました。

警告： ウイルス対策製品のインストールをテストする目的で、本物のウイルスを使用することは絶対にしないでください。

EICAR を使用してウイルスイベントをトリガし、メール通知機能が正しく設定されていること、およびログ機能に問題がないことを確認します。

注意： EICAR ファイルは、.com 拡張子を持つテキストファイルです。したがって、このファイル自体は活動しません。このファイルはウイルスではなく、自己複製機能もありません。また、ペイロードも持っていません。

EICAR を使用して InterScan のインストールをテストするには

1. ASCII テキストファイルを作成し、そこに次の 68 文字の文字列をコピーします。

   X5O!P%@AP [4¥PZX54 (P^) 7CC) 7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
2. このファイルに `eicar_test.com` というファイル名を付け、作業ディレクトリに保存して閉じます。
3. `eicar_test.com` を添付ファイルとしたメールを、自分のメールボックスまたはテスト用のメールボックスに送信します。

InterScan ログデータベースのウイルスログを確認します。通知機能が設定されている場合は、管理者に送信された通知を確認します。

InterScan のファイルとフォルダの確認

InterScan のファイルとフォルダの詳細については、次の付録を参照してください。

- 248 ページの「InterScan Windows 版」
- 249 ページの「InterScan Linux 版」

第 3 章

基本設定

第 3 章では、InterScan for IBM Domino (以下、InterScan) 5.6 のインストール後およびアクティベーション後に実行する必要がある設定作業について説明します。

第 3 章で説明する項目は次のとおりです。

InterScan のユーザインタフェースの概要

InterScan のユーザインタフェースのレイアウトは、次のとおりです。

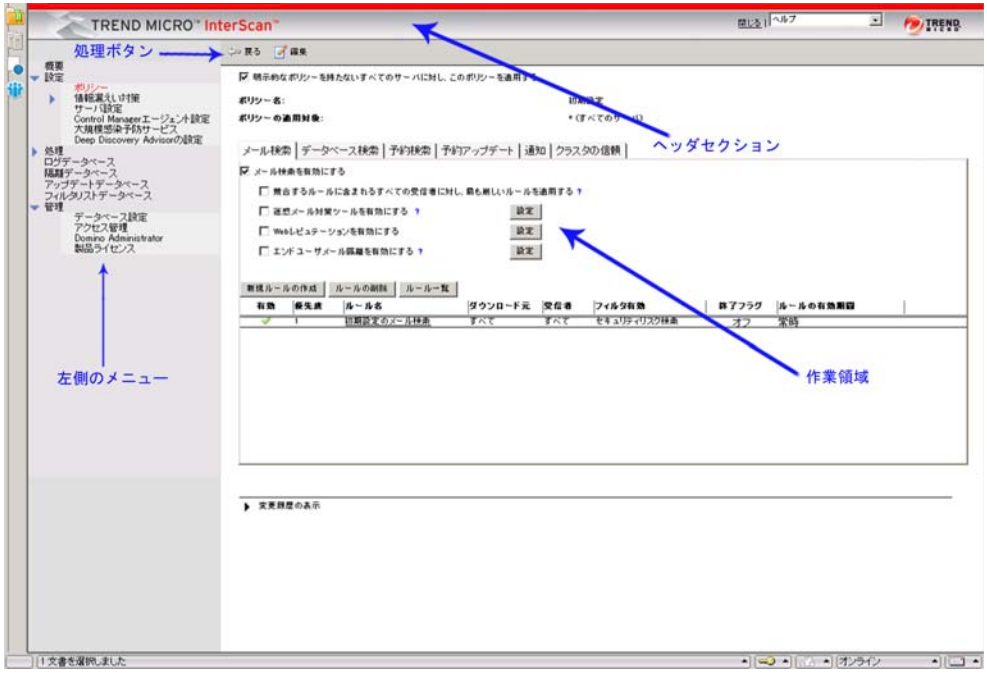


図 3-1. InterScan のインタフェース

ユーザインタフェースには、次の領域があります。

表 3-1. InterScan のインタフェースのレイアウトに関する説明

領域	目的
処理ボタン	設定の [編集] や前の表示文書に [戻る] など、特定の処理を実行できます。
ヘッダセクション	InterScan ヘルプデータベース、トレンドマイクロの Web サイト、およびその他のサポートツールへのリンクが表示されます。
左側のメニュー	InterScan の各機能およびその他の InterScan データベースへのショートカットが表示されます。
作業領域	InterScan ユーザインタフェースの中心となる領域。InterScan のオプションを設定できます。

ヒント： InterScan データベースを表示するには、1024 x 768 ピクセルの解像度を持つ画面が最適です。

困ったときは

InterScan ヘルプデータベースには、InterScan のすべての機能に関する情報が収録されており、関連トピックへの相互参照リンクがあります。操作手順の各セクションでは、一般的な設定の方法がわかりやすく体系的に説明されています。InterScan で操作を実行する方法について情報が必要な場合は、ヘルプのリストを参照してください。

InterScan の使用時に疑問が発生した場合は、次のいずれかを実行します。

- InterScan データベースのヘッダセクションのリストから [目次とキーワード] を選択します。
- 下線の付いているラベル、またはオプションの前にあるヘルプアイコン (?) をクリックすると、オプションのヒントが表示されます。

注意： Web ブラウザから InterScan データベースにアクセスしている場合は、ヒントは表示されません。

インストール後の手動検索の実行

すべての Notes データベースの手動検索を実行し、既存のウイルスを検出して駆除することをお勧めします。手動検索については、144 ページの「手動検索の実行」を参照してください。

すべての Notes データベースで最初のウイルス検索を実行した後、ローカルまたはリモートのハードディスク上にある Notes データベースを定期的に検索するように予約設定します。予約検索については、96 ページの「予約データベース検索ルールの作成」を参照してください。

Notes ワークスペースへの InterScan データベースアイコンの追加

Notes のワークスペースにアイコンを追加することで、簡単に InterScan データベースにアクセスできるようになります。

Notes のワークスペースに InterScan データベースアイコンを追加するには

1. Notes のワークスペースで、[ファイル] → [開く] → [IBM Notes アプリケーション] の順にクリックします。
2. [ファイル名] にパスとファイル名を入力します。
3. [開く] をクリックします。

Notes ワークスペースの詳細については、IBM Notes ヘルプで Notes ワークスペースのトピックを参照してください。

異なる ID を使用した InterScan データベースの署名

次の場合は、異なる ID を使用して InterScan データベースに署名します。

- インストール時にデータベースの署名に使用した `server.id` に代え、別の ID を割り当てる場合

異なる ID を使用して InterScan データベースに署名するには

1. InterScan データベースの署名に使用する ID を切り替えるには、IBM Notes クライアントで [ファイル] → [セキュリティ] → [ID の切り替え] の順にクリックします。
2. IBM Notes Administrator を起動し、InterScan をインストールした Domino サーバを選択して、[ファイル] タブをクリックします。
3. [表示内容] リストから [全種類のデータベース] を選択します。
4. リストから InterScan データベースを選択します。通常、InterScan データベースは `SMD` フォルダ内にあります。
5. 右側のツールのリストから [データベース] → [署名] を選択します。
6. [データベースの署名] 画面で、[すべての設計文書] を選択します。
7. [既存の署名のみ更新する (高速)] がオンになっている場合はオフにします。
8. [OK] をクリックして操作を完了します。

InterScan データベースへのアクセスと役割の定義

Notes クライアントを使用して、InterScan データベースにアクセスできるアカウントを定義します。これらのアカウントからは、InterScan の機能に無制限にアクセスできます。

注意： InterScan データベースへのアクセスと役割に含まれないアカウントは、管理者権限を持つ場合でも、InterScan の機能にアクセスすることはできません。

InterScan データベースへのアクセスを定義するには

1. Notes のワークスペースから、InterScan アイコンを選択します。
2. [ファイル] → [アプリケーション] → [アクセス制御] の順にクリックします。
3. [アクセス制御リスト] 画面の [基本] タブで、データベースの初期設定のアクセスを [なし] に変更します。

   次のオプションを設定します。
   種類 : 指定なし
   アクセス権 : なし
   [-Default-] と同じリスト内の [ユーザ] または [グループ] として、InterScan サーバ、LocalDomainServers、OtherDomainServers とともに、InterScan 管理者が表示されます。
4. InterScan 管理者、InterScan サーバ、LocalDomainServer、または OtherDomainServer が [ユーザ]、[サーバ]、[グループ] のどれにも表示されていない場合は、[追加] →  の順にクリックします。
   a. [名前] 画面で、左上隅のボックスからアドレス帳を選択します。
   b. 左側の画面に表示されているリストからユーザを選択します。
   c. [追加 >] をクリックして、ユーザの名前をリストに追加します。すべての名前がそろうまで前述の操作を繰り返します。
   d. 完了後、[OK] をクリックします。
5. [基本] タブに戻り、InterScan 管理者の名前をハイライトします。InterScan 管理者に次の権限を割り当てます。

   種類 : ユーザまたはユーザグループ
   アクセス権 : 編集者以上

6. InterScan 管理者に「文書の削除」権限を割り当て、続いて表 3-2 に指定するようにアクセス権限を割り当てます。

表 3-2. InterScan データベースのアクセス制御リスト

ユーザ、サーバ、またはグループ	推奨アクセス権	文書の削除オプション
-Default-	なし	オフ
InterScan データベースへの署名に使用する ID	管理者	オン
InterScan 管理者	編集者以上	オン
Domino サーバ	管理者	オン
LocalDomainServers (複製を使用する場合)	編集者以上	オン
OtherDomainServers	なし	オフ

Notes データベースの手動検索および予約検索を実行するには、InterScan では編集者以上の権限が必要です。また、指定した日数よりも古いログを削除するには、文書の削除権限が必要です (190 ページを参照)。初期設定のユーザについては、どのチェックボックスもオンにしないでください。

7. [ロール] セクションで [PolicyCreator]、[PolicyModifier] および [PolicyReader] チェックボックスをオンにし、制限されたアクセスが設定されている InterScan データベースコンポーネントへのアクセスを有効にします。
8. [OK] をクリックします。

役割の割り当てと Notes データベースへのアクセスの調整に関する詳細については、Notes ヘルプの「ローカルデータベースへのアクセスの制限」を参照してください。

InterScan データベースへのアクセス

InterScan データベースには、次の方法でアクセスできます。

- Notes クライアントを使用する方法

Notes クライアントを使用した InterScan データベースへのアクセス

Notes クライアントを使用すると、InterScan の機能に迅速かつ簡単にアクセスできます。

Notes クライアントを使用して InterScan データベースにアクセスするには

1. Notes クライアントを開きます。
2. [ファイル] → [開く] → [IBM Notes アプリケーション] の順にクリックします。
3. [サーバ] テキストボックスで、InterScan がインストールされている Domino サーバを指定します。
4. [データベース] リストで、InterScan 設定データベース (***smconf.nsf***) を探します。
5. [開く] をクリックします。

図 3-2. 設定データベースでは初期設定で最初のページとしてサーバの概要が表示されます。

IBM Notes のワークスペースに InterScan データベースアイコンが作成されます。

設定データベースからのその他の InterScan データベースへのアクセス

その他の InterScan データベースにアクセスするには、設定データベースを使用します。

設定データベースからその他の InterScan データベースにアクセスするには

1. InterScan 設定データベースを開きます。
2. メインメニューから該当するリンクをクリックして次のデータベースにアクセスします。
   - ログデータベース
   - 隔離データベース
   - アップデートデータベース

第 4 章

検索タスクの設定

第 4 章では、社内のさまざまな個人とグループ向けにポリシーを設定して、不正プログラムと迷惑メールからリアルタイムで保護する方法、および予約して保護する方法について説明します。また、手動検索の手順についても説明します。

第 4 章で説明する項目は次のとおりです。

ポリシーベースのウイルス対策およびコンテンツセキュリティ保護の計画

トレンドマイクロでは、InterScan for IBM Domino (以下、InterScan) のポリシーベースの機能を使用して、標準のウイルス対策設定、情報漏えい対策、およびコンテンツセキュリティ設定を確立および保守管理することをお勧めします。ポリシーを使用して、次の操作を実行できます。

- ウイルス対策設定とアップデート設定の繰り返し作成、およびその他のメンテナンス作業を自動化します。
- 1 台のサーバから環境内の全サーバを簡単に設定します。

ポリシーベースのウイルス対策を計画する際は、次の作業を考慮します。

- InterScan の初期設定ポリシーに基づいてグループポリシーを作成します。

  共通の役割を実行する複数のサーバが含まれる大規模なネットワークでは、初期設定のポリシーに基づいたポリシーを使用することで、設定にかかる時間と管理作業を大幅に削減できます (27 ページの「ポリシー、ルール、およびフィルタの概要」を参照)。個々のサーバに繰り返して作成するのではなく、リアルタイムメール検索と予約メール検索の共通の保護設定を一度だけ簡単かつ迅速に作成できます。
- 特定の地域または管理範囲にあるすべての Domino サーバに適用可能な設定を割り当てるためのグループポリシーを作成します。

  マルチサーバ環境では、同じような機能または特性に基づいてサーバグループを定義することにより、適切なポリシーをグループ内のすべてのサーバに適用できます。
  共通の目的を持つポリシーを作成します。たとえば、次のようなポリシーを作成します。
  - 同じ保護機能のリアルタイムメール検索が必要な、すべての Domino メールサーバ向けポリシー
  - リアルタイムと予約によるデータベース検索が必要な、すべてのサーバ向けポリシー

  グループに含めるサーバ、およびそれらに適用する保護、アップデート、および通知方法を決定します。たとえば、1 つのメールサーバを保護するポリシーを作成して、同じくメールサーバとして機能する他のサーバにそのポリシーを適用できます。
- 特定の Domino サーバに設定を割り当てるための独自のポリシーを作成します。

  独自のポリシーにより、初期設定が個別のユーザ、ユーザグループ、またはサーバに割り当てられます。たとえば、特定の曜日にだけ実行される予約検索を設定するには、予約検索ルールを設定したポリシーを作成して、それを個別のデータベースサーバまたはそのグループに割り当てます。

ポリシーベースのウイルス対策

ポリシーベースのウイルス対策は、次の操作を実行した場合に機能します。

1. InterScan の検索タスク、通知、アップデート、および一般的な設定のオプション向けのポリシーを作成します。27 ページの「ポリシー、ルール、およびフィルタの概要」を参照してください。
2. 環境内の各サーバに対してサーバ設定を作成します。149 ページの「[サーバ設定] メニューオプションの指定」を参照してください。
3. 同期スケジュールを設定して、環境内のサーバに複製するためのポリシーを有効にした場合。

   ポリシー関連文書とサーバプロファイルの作成後、環境内にあるサーバ用の複製スケジュールに InterScan 設定データベース (***smconf.nsf***) を追加する必要があります。[概要] 表示に示されているすべてのサーバのステータスを表示します。すべてのサーバの概要の表示を参照してください。

注意： サーバ間で正しく複製を実行するには、対象サーバをデータベースのアクセス制御リストに追加して、管理者アクセス権を付与します。163 ページの「アクセス制御リスト (ACL) のエントリの新規作成と適用」を参照してください。

ポリシーの管理

ここでは、InterScan 設定データベースを使用してポリシーを管理する方法について説明します。

ポリシーの作成

ポリシーを作成するには、InterScan 設定データベースを使用します。

ポリシーを作成するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」参照)。
2. 左側のメニューで、[設定] → [ポリシー] の順にクリックします。

図 4-1.　ポリシーリスト

3. 作業領域で、[新規ポリシーの作成] をクリックします。
4. [ポリシー名] を入力します。

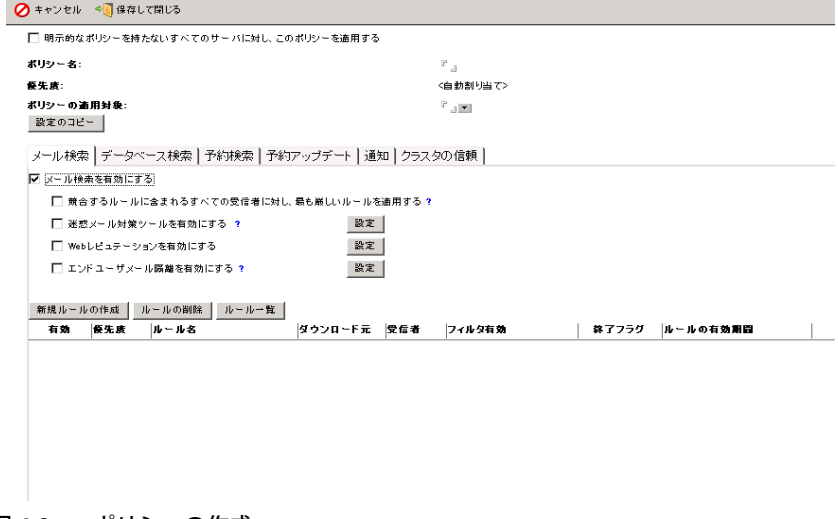


図 4-2.　ポリシーの作成

5. [ポリシーの適用対象] で、ポリシーを適用するサーバまたはサーバグループを選択します。

   注意： Domino R8 を使用している場合は、サーバグループの種類を多目的に設定する必要があります。

6. [設定のコピー] をクリックして、使用できるポリシーのリストから検索、アップデート、または通知のルールをコピーします。

   注意： [設定のコピー] を使用することにより、ポリシー名、ポリシーの適用対象などを除き、コピー元のポリシーと同じポリシーを作成できます。

7. リアルタイムメール検索ルールを作成します (89 ページの「リアルタイムメール検索ルールの作成」参照)。
8. リアルタイムデータベース検索ルールを作成します (94 ページの「リアルタイムデータベース検索ルールの作成」参照)。
9. 予約データベース検索ルールを作成します (96 ページの「予約データベース検索ルールの作成」参照)。
10. InterScan による通知の配信方法を設定します (180 ページの「通知の配信方法の設定」参照)。
11. クラスタの信頼を定義します (87 ページの「ポリシーの承認クラスタサーバの管理」参照)。
12. [保存して閉じる] をクリックします。

InterScan によって、[ポリシー] 表示に新しいポリシーが追加されます。

ポリシーの変更

ポリシーを変更するには、InterScan 設定データベースを使用します。

ポリシーを変更するには

1. InterScan 設定データベースを開きます (78 ページを参照)。
2. 左側のメニューで、[設定] → [ポリシー] の順にクリックします。
3. 作業領域で、目的のポリシーの名前をダブルクリックします。
4. [メール検索] (89 ページ)、[データベース検索] (94 ページ)、[予約検索] (96 ページ)、[予約アップデート] (169 ページ)、[通知] (180 ページ)、または [クラスタの信頼] (87 ページ) タブの設定を変更します。
5. [保存して閉じる] をクリックします。

ポリシーの削除

ポリシーを削除するには、[ポリシー] 表示を使用します。

ポリシーを削除するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」参照)。
2. 左側のメニューで、[設定] → [ポリシー] の順にクリックします。[ポリシー] 表示が表示されます。
3. 削除するポリシーを選択します。
4. 作業領域で、[ポリシーの削除] をクリックします。

注意： InterScan の初期設定のポリシーは削除できません。

ポリシーの優先度

[ポリシーの優先度] 表示を使用すると、すべてのポリシーの優先順位を選択できます (図 4-1 を参照)。

ポリシーの優先度を設定するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」参照)。
2. 左側のメニューで、[設定] → [ポリシー] の順にクリックします。[ポリシー] 表示が表示されます。
3. 作業領域で、[ポリシーの優先度] をクリックします。[ポリシー一覧] が表示されます。
4. 優先度を変更するポリシーを選択し、必要に応じて [上へ] または [下へ] をクリックします。
5. すべての優先度が設定されるまで必要に応じて操作を繰り返します。
6. [閉じる] をクリックします。

ポリシーの承認クラスタサーバの管理

[クラスタの信頼] タブを使用すると、選択したポリシーの適用先のクラスタサーバを確認したり、クラスタグループ内で承認サーバを選択したりできます。

注意： 初期設定のポリシーは特定のクラスタグループには適用できません。このため、初期設定のポリシーを [クラスタの信頼] タブで使用することはできません。

ポリシーの承認クラスタサーバを管理するには

1. ポリシーを作成 (88 ページの「ルールの作成」参照) または変更 (85 ページの「ポリシーの変更」参照) します。
2. [クラスタの信頼] タブをクリックします。

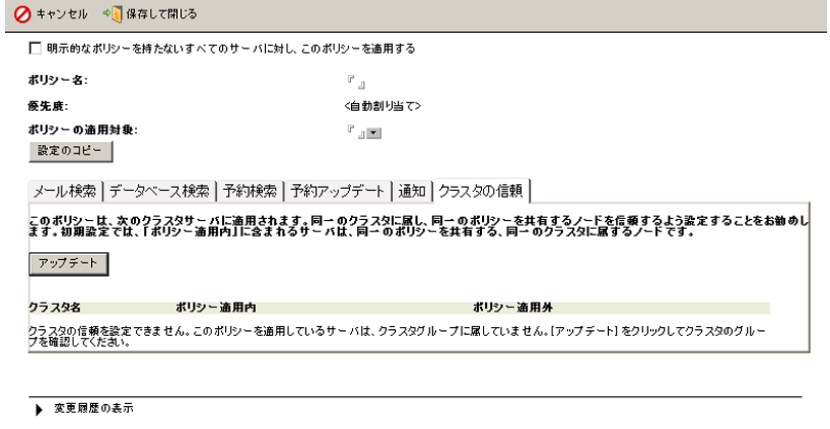


図 4-3. クラスタグループ内のサーバを一覧表示する [クラスタの信頼] 表

3. 次のいずれかを実行します。
   - [クラスタの信頼] 表に何も表示されていない場合、[アップデート] をクリックしてクラスタサーバのグループを確認、展開してから、表示を更新します。
   - [クラスタの信頼] 表に適用可能なサーバが一覧表示されている場合は、承認クラスタグループに追加するサーバを選択します。

注意： [クラスタの信頼] 表には、[ポリシー適用内] と [ポリシー適用外] という 2 つの列があります。[ポリシー適用内] 列に表示されているサーバは、選択したポリシーを適用するサーバです。図 4-4 を参照してください。

図 4-4.　承認クラスタグループに追加するサーバの選択

図 4-4 では、ASD_DOM1 という名前のクラスタには、CN=ASD_S1、CN=ASD_S2、および CN=ASD_S3 という 3 つのサーバが含まれています。test という名前のポリシーは、CN=ASD_S1 のみに適用されます。[クラスタの信頼] 表では、サーバ CN=ASD_S1 および CN=ASD_S3 がオンになっています。このため、CN=ASD_S1 では CN=ASD_S3 が信頼され、CN=ASD_S2 は信頼されません。

4. [保存して閉じる] をクリックします。

ルールの作成

メールとデータベースのルールを作成し、メッセージとデータベースをリアルタイムでフィルタ処理して検索する方法を定義します。または、予データベース検索ルールを作成して、Notes データベースを定期的に予約検索します。

注意： ルールを作成する前に、smdreal が開始されており、そのステータスがアイドルになっていることを確認してください。

ヒント： 1 つのルールに設定する条件が多すぎると、ルールが予想以上に複雑になる場合があります。ポリシーごとに 1 つまたは 2 つの複雑なルールを作成するよりも、単純なルールを複数作成することをお勧めします。

リアルタイムメール検索ルールの作成

リアルタイムメール検索ルールでは、送受信メールを検索してフィルタ処理する方法を定義します。

メール検索ルールを作成するには

1. ポリシーを作成 (88 ページの「ルールの作成」参照) または変更 (85 ページの「ポリシーの変更」参照) します。
2. 作業領域で、[メール検索] タブをクリックします。

図 4-5. [メール検索] タブでリアルタイムメール検索を設定

3. メール検索で複数のルールが適用される状況になったときに、最も厳しいメール検索ルールが実行されるようにするには、[競合するルールに含まれるすべての受信者に対し、最も厳しい

ルールを適用する] をオンにします。詳細は、92 ページの「最も厳しいルールの適用」参照してください。

4. スイート版または情報漏えい対策付きスイート版の場合は、[スパムメールフィルタを有効にする] をオンにし、[設定] をクリックしてスパムメール検索設定を指定します (106 ページの「スパムメールフィルタの設定」参照)。
5. スイート版または情報漏えい対策付きスイート版の場合は、[Web レピュテーションを有効にする] をオンにし、[設定] をクリックして Web レピュテーション設定を指定します。
6. [新規ルールの作成] をクリックします。
7. メッセージに一致するルールが見つかったとき、その他のルールを実行せずに処理を終了する場合は、[新規メール検索ルール] 画面で [メールがこのルールに一致した場合、後続のルールを処理しない (終了フラグを有効)] をオンにします。

ヒント： メール検索のパフォーマンスを向上させるには、[メールがこのルールに一致した場合、後続のルールを処理しない] を有効にします。

8. [一般] タブでルール名を指定します。
9. 一般的な設定を行います (93 ページの「メール検索ルールの一般的な設定」参照)。
10. [検索オプション] タブをクリックして、InterScan でメッセージを検索およびフィルタ処理する方法を設定します。
    - セキュリティリスク検索 (120 ページの「セキュリティリスク検索の設定」参照)
    - APT 対策フィルタ (124 ページの「APT 対策フィルタの設定」参照)
    - 検索制限 (126 ページの「検索制限の設定」参照)
    - メッセージフィルタ (127 ページの「メッセージフィルタの設定」参照)
    - 添付ファイルフィルタ (128 ページの「添付ファイルフィルタの設定」参照)
    - コンテンツフィルタ (132 ページの「コンテンツフィルタの新規作成」参照)
    - 情報漏えい対策フィルタ (139 ページの「情報漏えい対策フィルタの設定」参照)
    - スクリプトフィルタ (141 ページの「スクリプトフィルタの設定」参照)

ヒント： ルールを作成するときは、ブロックされたメールは削除せずに、そのコピーを隔離データベースに保存することをお勧めします。作成した新規ルールが想定外の結果を招かないことを確認した後、検索処理を変更します。

11. 検索通知を設定します (181 ページの「InterScan 通知の設定」参照)。
12. [転送オプション] を設定します (142 ページの「転送オプションの設定」参照)。
13. 検査証明 (ディスクレーマー) を挿入します (143 ページの「検査証明 (ディスクレーマー) の挿入」参照)。
14. ルール予約を設定します (143 ページの「ルール予約の設定」参照)。
15. [保存して閉じる] をクリックします。

最も厳しいルールの適用

オプションの [競合するルールに含まれるすべての受信者に対し、最も厳しいルールを適用する] をオンにすると、適用するルールが競合するすべての受信者に対して、最も厳しいメール検索ルールを適用できます。

次の例を考えてみます。

- メール検索ルール A の設定

[一般] :	[対象指定する受信者] = `All of Accounting`
[検索オプション] → [添付ファイルフィルタ] :	[サイズによる添付ファイルフィルタを有効にする] = 10MB [処理] = メールをブロック

- メール検索ルール B の設定

[一般] :	[対象指定する受信者] = `user@domain.com` 「`user@example.com`」は、All of Accounting グループのメンバーです。
[検索オプション] → [添付ファイルフィルタ] :	[サイズによる添付ファイルフィルタを有効にする] = 5MB [処理] = メールをブロック

添付ファイルが 7MB である、`All of Accounting` および `user@example.com` 宛てのメールが着信した場合、次の処理が実行されます。

- [競合するルールに含まれるすべての受信者に対し、最も厳しいルールを適用する] がオンになっている場合、`All of Accounting` グループ内のすべてのユーザがこのメールを受信しません。
- [競合するルールに含まれるすべての受信者に対し、最も厳しいルールを適用する] がオフになっている場合、`user@example.com` を除くすべてのユーザがこのメールと添付ファイルの両方を受信します。

このオプションを無効にすると、グループ内の特定のユーザに最も厳しいメール検索ルールを適用できます。

ヒント： 正確で完全なアドレスグループを定義することで、そのグループ内の個々のユーザに適切なポリシーが適用されます。

メール検索ルールの一般的な設定

メール検索の [一般] タブを使用すると、メール検索ルールで許可および除外する送信者と受信者を設定できます。

メール検索ルールの一般的な設定を設定するには

1. [一般] タブをクリックします。
2. [ルール識別子] に、ルールの名前を入力します。

   ヒント： ルールを適切に表現する名前を使用することをお勧めします (たとえば、finance_confidential)。

3. このルールの適用対象となる送信者または受信者を指定します。この送信者と受信者は、次のように選択します。
   - [送信者] セクションで、対象となる送信者を選択します。
     i. ルールで許可する送信者を選択します。
        - 指定サーバに属するすべての送信者にルールを適用するには、[すべての送信者] をクリックします。
        - 特定の送信者にルールを適用するには、[指定する送信者] をクリックします。

        次のいずれかを実行します。
        - Notes のユーザまたはグループを入力するか、をクリックしてリストから選択します。たとえば、`user@example.com` を選択します。
        - ワイルドカード文字 * または？を使用して、ユーザまたはグループの名前の一部を入力します。たとえば、「`*@example`」と入力します。

     ii. ルールで除外する送信者を指定します。
   - [受信者] セクションで、対象となる受信者を選択します。
     i. ルールで許可する受信者を選択します。
        - 指定サーバに属するすべての受信者にルールを適用するには、[すべての受信者] をクリックします。
        - 特定の受信者にルールを適用するには、[指定する受信者] をクリックします。

次のいずれかを実行します。

- Notes のユーザまたはグループを入力するか、  をクリックしてリストから選択します。たとえば、user@example.com を選択します。
- ワイルドカード文字 * または ? を使用して、ユーザまたはグループの名前の一部を入力します。たとえば、「*@example」と入力します。

ii. ルールで除外する受信者を指定します。

注意： 送信者と受信者の両方を指定した場合は、このルールで処理する際に使用する演算子 (100 ページを参照) を選択します。

---

4. [送信者と受信者が上記の条件に一致した場合の処理] セクションで、送信者または受信者が一致した場合の処理を [ブロック] または [配信] から選択します。

   [配信] オプションを選択した場合は、優先度を低く設定するかどうか、または指定する時間帯に配信するかどうかを選択します。

注意： 初期設定では、Domino R8 サーバは優先度が低いメッセージを午前 0 ～ 6 時に配信します。

---

5. メール送信者に通知を送信するには、[通知] セクションから [送信者への通知] を選択します。
   a. [件名] に名前を入力します。
   b. メッセージを新たに入力するか、必要な箇所で [追加 >>] をクリックして、メッセージフィールドにタグを追加します。
6. [保存して閉じる] をクリックします。

ルール名、優先度、送信者と受信者の許可または除外、予約などの設定、終了フラグの設定、および [検索オプション] の有効化は、[メール検索] タブ表示で指定できます。

リアルタイムデータベース検索ルールの作成

データベースのリアルタイム検索ルールにより、Notes データベースを検索する方法を定義します。

データベース検索ルールを作成するには

1. ポリシーを作成 (88 ページの「ルールの作成」参照) または変更 (85 ページの「ポリシーの変更」参照) します。
2. 作業領域で、[データベース検索] タブをクリックします。

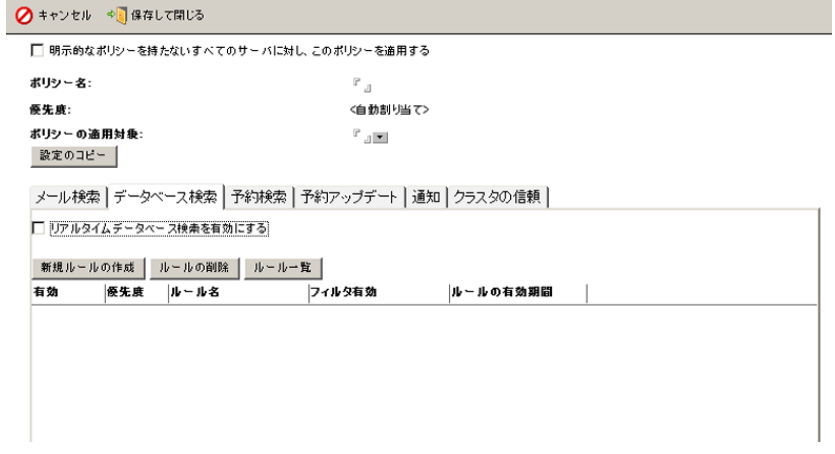


図 4-6. [データベース検索] タブ

3. [リアルタイムデータベース検索を有効にする] をオンにして、データベース検索機能を有効にします。
4. [新規ルールの作成] をクリックします。[新規データベース検索ルール] 画面が表示されます。
5. [ルール識別子] セクションで、[名前] に新規ルールの名前を入力します。

注意： 作成したルールの優先度は自動的に割り当てられます。優先度の設定を変更する方法については、100 ページの「ルールの優先度の変更」を参照してください。

---

6. [検索するデータベース] タブをクリックして、検索するデータベースを次の項目で設定します。
   - すべてのデータベース — Domino サーバに格納されているすべてのデータベースを検索します。
   - 選択されたデータベースのみ検索 — ディレクトリとデータベースのリストに基づいて、特定のデータベースを検索します。
   - 検索から除外するデータベース — 指定したデータベースは検索しません。

[追加]、[削除]、および [すべて削除] の各ボタンを使用して、リストにあるデータベースを操作します。

7. [検索オプション] タブをクリックして、次の項目ごとにデータベースの検索方法を設定します。
   - セキュリティリスク検索 (120 ページの「セキュリティリスク検索の設定」参照)
   - 検索制限 (126 ページの「検索制限の設定」参照)
   - スクリプトフィルタ (141 ページの「スクリプトフィルタの設定」参照)
   - 添付ファイルフィルタ (128 ページの「添付ファイルフィルタの設定」参照)
8. 検索通知を設定します (181 ページの「InterScan 通知の設定」参照)。
9. ルール予約を設定します (143 ページの「ルール予約の設定」参照)。
10. [保存して閉じる] をクリックします。

ヒント： データベースが変更された場合だけでなく、データベースファイルが開かれたときは常にリアルタイム検索を実行するよう InterScan を設定するには ***notes.ini*** に `SMDEnableOpenEvent=1` を追記します。

予約データベース検索ルールの作成

予約検索ルールにより、特定の時刻に Notes データベースを検索する方法を定義します。

予約検索ルールを作成するには

1. ポリシーを作成 (88 ページの「ルールの作成」参照) または変更 (85 ページの「ポリシーの変更」参照) します。
2. 作業領域で、[予約検索] タブをクリックします。

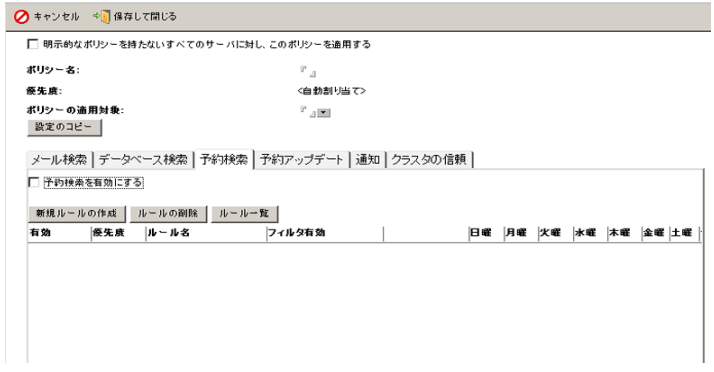


図 4-7. [予約検索] タブ

3. [新規ルールの作成] をクリックします。
4. 「新規予約検索ルール」文書の [一般] タブで、次の項目を指定します。
   a. ルール名を指定します。
   b. 次から検索条件を選択します。
      - 増分検索を有効にする — 前回実施した検索以降に更新または新規作成された文書のみ検索します。

        増分検索では、サーバの使用時間とリソースをかなり節約できます。前回の検索以降に変更されたファイルのみ検索します。
      - パターンファイルのアップデート時に全文書を検索する — パターンファイルがアップデートされた場合にすべての文書を検索します。
      - 検索エンジンのアップデート時に全文書を検索する — 検索エンジンがアップデートされた場合にすべての文書を検索します。

        InterScan が検索を始めるまでの最短日数を表す整数を入力します。たとえば、最短日数が 4 の場合、予約検索は前回の検索から 4 日目に実行されます。
        最短日数の設定は、パターンファイルと検索エンジンの両方のアップデート条件に適用されます。

注意： 増分検索設定の方が、[パターンファイルのアップデート時に全文書を検索する] および [検索エンジンのアップデート時に全文書を検索する] の 2 つの条件より優先されます。

5. [検索するデータベース] タブをクリックして、検索するデータベースを次の項目で設定します。
   - すべてのデータベース — Domino サーバ上のすべてのデータベースを検索します。
   - 指定するデータベース — 特定のメールファイルまたはデータベースを検索します。または、検索から除外します。

     [追加]、[削除]、および [すべて削除] の各ボタンを使用して、リストにあるデータベースを操作します。
6. [検索オプション] タブをクリックして、次の検索オプションを設定します。
   - セキュリティリスク検索 (120 ページの「セキュリティリスク検索の設定」参照)
   - APT 対策フィルタ (124 ページの「APT 対策フィルタの設定」参照)
   - 検索制限 (126 ページの「検索制限の設定」参照)
   - 添付ファイルフィルタ (128 ページの「添付ファイルフィルタの設定」参照)
   - コンテンツフィルタ (132 ページの「コンテンツフィルタの新規作成」参照)
   - 情報漏えい対策フィルタ (139 ページの「情報漏えい対策フィルタの設定」参照)
   - スクリプトフィルタ (141 ページの「スクリプトフィルタの設定」参照)
7. 検索通知を設定します (181 ページの「InterScan 通知の設定」参照)。
8. 予約を設定します。
   a. [実行時刻] に、予約検索ルールを実行する時刻を入力します。たとえば、「06:00 AM」と入力します。

      注意： [実行時刻] を空白のままにすると、予約検索ルールは無効になります。

   b. [検索時間の上限] に、検索の最長実行時間を入力します。「0」を入力すると、すべて完了するまで検索を続けます。
   c. ルールが実行される曜日を入力するか、  をクリックして選択します。
9. [保存して閉じる] をクリックします。

注意： ルールを新規に作成するときは、ブロックされたメールは削除せずに、そのコピーを隔離データベースに保存することをお勧めします。作成した新規ルールが想定外の結果を招かないことを確認した後、検索処理を変更します。

ルール一覧

メール検索、データベース検索、または予約検索のルールを整理するには、ルール一覧を使用します。

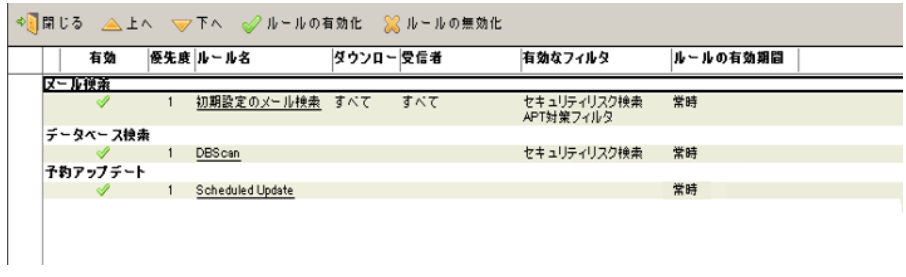


図 4-8. ルールの優先度を変更するには、上へ または 下へ をクリックします。ルールの有効と無効を切り替えるには、[ルールの有効化] または [ルールの無効化] のボタンを使用します。

ルールを整理する際は、次のガイドラインに従うことをお勧めします。

- 最も広義で、一致する可能性が最も高いものに、最高の優先度を与えます。

  InterScan は優先順位 1 位のルールから順に、有効なルールすべてをメッセージや添付ファイルと比較します。[メールがこのルールに一致した場合、後続のルールを処理しない] が有効の場合、一致するルールが見つかると、ルール比較はそれ以上実施されず、指定された処理 (通常は隔離) が実行されます。

  たとえば、有効なルールが 12 個あり、ルールリストの最後にあるルールと一致する確率が 50% である場合、上位 11 個のルールがすべてチェックされた後、12 番目のルールで初めて一致する可能性があります。このようなルールの優先度を 1 にすると、すぐに一致が見つかる可能性が高くなり、残りの 11 個のルールを処理する時間を節約できます。
- 適用範囲が極めて広いルールを少数作成して適用するのではなく、範囲を絞ったルールを多数作成して適用します。

すべてのオプションを有効にしたルールを 2、3 個作成するよりも、チェックする条件または実行するブロック処理それぞれに対して、1 つずつルールを作成するようにします。

ルールの優先度の変更

メール検索、データベース検索、予約検索、および予約アップデートのルールを適用する順序を変更するには、[ルール一覧] 文書を使用します。[ルール一覧] には、ルールを有効または無効にするショートカットもあります。

ルールの優先度を変更するには

1. [メール検索]、[データベース検索]、[予約検索]、または [予約アップデート] のタブで、[ルール一覧] ボタンをクリックします。
2. ルールの優先度を変更します。
   - ルールの優先度を上げるには、 

をクリックします。
   - ルールの優先度を下げるには、 

をクリックします。
3. [閉じる] をクリックします。

ルールの演算子

OR 演算子は、ルール内の送信者のリストと受信者のリストを結合します。

AND 演算子は、所定のリスト内だけを対象にします。つまり、同じ行にある、カンマで区切られた項目がすべて結合されます。たとえば、次のエントリがあるとします。

```
1@example.com, 2@example.com, 3@example.com
```

これは、`1@example.com AND 2@example.com AND 3@example.com` という意味です。

InterScan のフィルタの概要

フィルタは、検索ルールのサブセットであり、[検索オプション] タブを通して InterScan の検索およびフィルタ処理の動作を実際に定義します。

フィルタの実行順序

[検索オプション] タブでは、データベースおよびメールの検索ルールを構成するフィルタを作成できます。

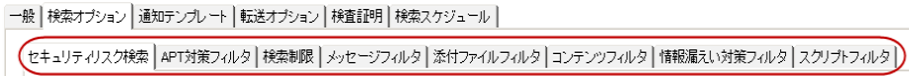


図 4-9.　[検索オプション] タブ

メッセージの添付ファイルと内容を検索またはフィルタ処理する方法を定義するには、次の表を使用します　(この表の順序でフィルタが適用されます)。

順序	フィルタ	オプションによって設定される特定の検索処理の対象
1a	検索制限	圧縮、暗号化、およびその他の添付ファイルの種類 **注意：** 検索制限設定を適用するには、セキュリティリスク検索でウイルス検索機能を有効にしておく必要があります。
1b	セキュリティリスク検索	文書の悪用を含む添付ファイル
2	APT 対策フィルタ	疑わしい添付ファイル
3	メッセージフィルタ	さまざまなメッセージの種類
4	添付ファイルフィルタ	迷惑な添付ファイル
5	コンテンツフィルタ	管理者定義の明示的なルールに基づいて不適切とされる内容が含まれるメッセージ
6	情報漏えい対策フィルタ	カスタムの情報漏えい対策ルールに違反するメッセージ (29 ページの表 1-3 を参照)
7	スクリプトフィルタ	格納フォームまたはリッチテキストのホットスポットが含まれるメッセージ

注意： スパムフィルタを設定すると、メール検索ルールが次のフィルタ処理順序で実行されます。

1. 受信メッセージのスパムフィルタ (106 ページの「スパムメールフィルタの設定」)。これは、[許可する送信者] と [ブロックする送信者] (有効になっている場合)、またはスパムメール検索エンジンに基づいて適用されます。
2. Web レピュテーション (115 ページの「Web レピュテーションの設定」)。
3. 一般的な設定 (93 ページの「メール検索ルールの一般的な設定」)。
4. [検索オプション] タブで有効になっているフィルタ。

スパムフィルタ (スイート版または情報漏えい対策付きスイート版のみ)

スパムメール検索エンジンには、受信メッセージのスパムフィルタ処理機能があります。受信メッセージとは、SMTP プロトコルを使用して送信されたメッセージのことです。スパムフィルタ処理機能を使用すると、次のコンポーネントに基づいて迷惑メールをブロックできます。

順序	コンポーネント	提供方法	説明
1	承認される送信者	ユーザ定義	受け入れ可能なメッセージの送信元である人物または組織、あるいはその両方のリスト。 その他のメッセージでは、迷惑メールに対する処理を施します。
2	ブロックされる送信者	ユーザ定義	ブロックするメッセージの送信元であるユーザまたは組織のリスト。 その他のメッセージは、受け入れられます。

順序	コンポーネント	提供方法	説明
3	ルールファイル	トレンドマイクロ	学習的ファイルと URL 署名ファイルとで構成。承認される送信者もブロックされる送信者も定義されていない場合、スパムメール検索エンジンでは、このファイルを使用してスパムメールをフィルタ処理します。

注意： 承認される送信者もブロックされる送信者も設定されていない場合、スパムメール検索エンジンではトレンドマイクロが用意したルールファイルを使用します。

スパムメール検索エンジンには、フィルタレベルが 3 つあります。次の表は、スパムメール検索エンジンがメッセージにスパムとしてタグ付けする場合とその方法の例を示しています。

フィルタレベル	しきい値レベル
高 (厳しいフィルタ)	4.0
中 (初期設定)	5.0
低 (寛容なフィルタ)	8.0

- フィルタレベルは、スパムメール検索エンジンがスパムをフィルタ処理する際のフィルタレベルを定義します。
- しきい値レベルは、スパムスコアの許容最大値を定義します。

  スパムスコアの合計がしきい値レベル以上の場合、スパムメール検索エンジンはメッセージをスパムとしてタグ付けします。スパムスコアの合計値がしきい値レベル未満の場合、次の順番のフィルタ処理に進みます (101 ページを参照)。

注意： InterScan 5.0 以上では、さまざまなスパム判定ルールに従って変更される動的なしきい値レベルを使用できます。

例 :

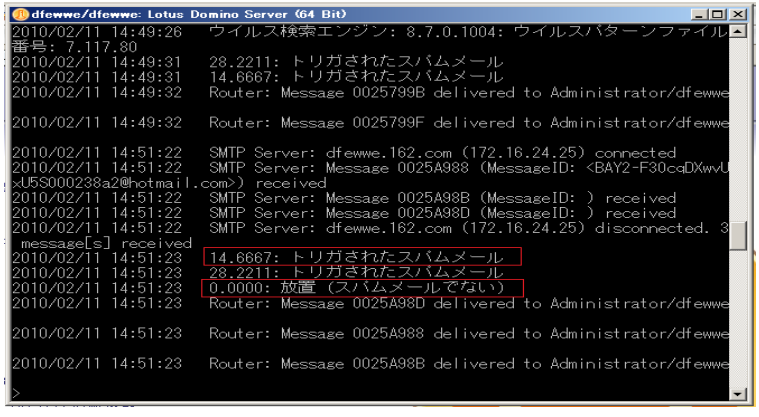


図 4-10. スパムスコアの例

この例では、フィルタレベルは中に設定されています。赤い線で囲まれた項目が、スパムスコアです。最初のスパムスコアは、15.20 で、これはしきい値レベル「5」を超えています。そのため、スパムメール検索エンジンは、このメッセージをスパムとしてタグ付けしません。一方、2 つ目のスパムスコアは、3.726 で、これはしきい値レベルに達していません。そのため、スパムメール検索エンジンによりこのメッセージがスパムと見なされることはありません。

フィルタレベル、または [許可する送信者] と [ブロックする送信者] のリストを設定するには、106 ページを参照してください。

コンテンツフィルタ (スイート版または情報漏えい対策付きスイート版のみ)

コンテンツフィルタによって、管理者が定義する明示的なルールに基づいて InterScan がメッセージの内容をフィルタ処理する方法が定義されます。

企業秘密のリーク、侮辱的または不適切な言葉遣い、競合他社または敵国との不審な接触がないかをチェックすることなど、コンテンツセキュリティにはさまざまな形があります。

[コンテンツフィルタ] タブでは、一般的なルールと詳細なルールを定義できます。

一般的なコンテンツフィルタのルールを作成するのは、次のような場合です。

- 最初にキーワードを作成せずに、すばやくルールを作成する場合
- 「件名」に表示されるテキストに基づいてメッセージをフィルタ処理する場合

- 本文に表示されるテキストに基づいてメッセージをフィルタ処理する場合（キーワードの一部またはすべて）
- 添付ファイル名に基づいてメッセージをフィルタ処理する場合

詳細なコンテンツフィルタのルールを作成するのは、次のような場合です。

- キーワードを 1 つ以上使用して複雑なフィルタを作成する場合
- OR 演算子でつながれた複数のキーワードを使用したフィルタを作成する場合
- メッセージ本文のみを検索する場合
- 添付ファイルの内容のみを検索する場合
- 「件名」、「宛先」、「CC」、「送信者」など、メッセージヘッダの特定のフィールドのみに注目して検索する場合
- 特定の添付ファイルの検出回数のしきい値を設定する場合。たとえば、指定した添付ファイルが X 回検出されない限り、メッセージをブロックしないようにできます。この設定は、たとえば、マスメーリング型の攻撃を受けたときに役立ちます。この種のメールは、広範囲に広まり、しかも同じ名前の添付ファイルを持つことがあるからです。
- .OCCUR に対する値を追加する場合
- .NEAR に対する値を追加する場合

キーワード

キーワードとは、InterScan がメールのヘッダと内容に基づいてメッセージをフィルタ処理するときに使用する単語またはフレーズのことです。

コンテンツフィルタのキーワードを作成または変更する際は、[新規キーワード] ワークスペースの最下部にあるヘルプセクションを参照して、論理演算子の使用方法に目を通してください。

キーワードの各オペランドの前後に、スペースを挿入します。1 つのキーワードの中に、強制改行または復帰改行を挿入しないでください。その場合は、キーワードを 2 つ作成します。

たとえば、果物の「apple」とコンピュータの「apple」を区別するためのキーワードを作成するには、次のようなルールを作成します。

```
.(. .OCCUR. apple .)..AND..(.apple .NEAR. computer .)..OR..(.apple .NEAR.
macintosh .)..AND..(..NOT..(..OCCUR. eat .)..).
```

次の条件が満たされると、このルールに一致していると判定されます。

- 単語「Apple」が、文書に 2 回以上、単語「computer」の前後 25 語以内に現れる
- 単語「Macintosh」が文書に現れる

ただし、同じ文書内に単語「eat」も現れる場合は、一致とは見なされません。

キーワードは、単純で意味が狭いものにすることをお勧めします。上に示したような複雑なルールを 1 つ作成するのではなく、単純なキーワードを 2 つ作成して、それぞれをメール検索ルールに適用します。

キーワード 1: `.(. .OCCUR. apple .)..AND..(.apple .NEAR. computer .).`
キーワード 2: `.(. apple .NEAR. macintosh .)..AND..(..NOT..(..OCCUR. eat .)..).`

メール検索ルールに複数のキーワードを設定するときは、キーワード間に OR 演算子を挿入します。キーワードを作成するには、134 ページを参照してください。

検索の設定とフィルタの設定

[検索オプション] タブを使用すると、検索制限とフィルタの設定を指定できます。

注意： スパムメールフィルタ、Web レピュテーションフィルタ、情報漏えい対策フィルタ、コンテンツフィルタ、およびエンドユーザメール隔離 (EUQ) の機能は、InterScan スイート版でのみ使用できます。InterScan のスパムフィルタは、メール検索ルールにのみ適用されます。

* 情報漏えい対策は、情報漏えい対策付きスイート版でのみ使用できます。

スパムメールフィルタの設定

一方的に送られてきたメッセージまたは迷惑メールをスパムメール検索エンジンでどのようにフィルタ処理するか設定するには、[スパムメールフィルタの設定] 画面を使用します (102 ページを参照)。この画面には、学習的な検出のレベル、または [許可する送信者] と [拒否する送信者] のリストを定義するオプションがあります。スパムメールは、これらのオプションによりフィルタ処理されます。

スパムメールフィルタを設定するには

1. [メール検索] タブで、[スパムメールフィルタを有効にする] を選択してから [設定] をクリックします。[スパムメールフィルタの設定] 画面が表示されます。

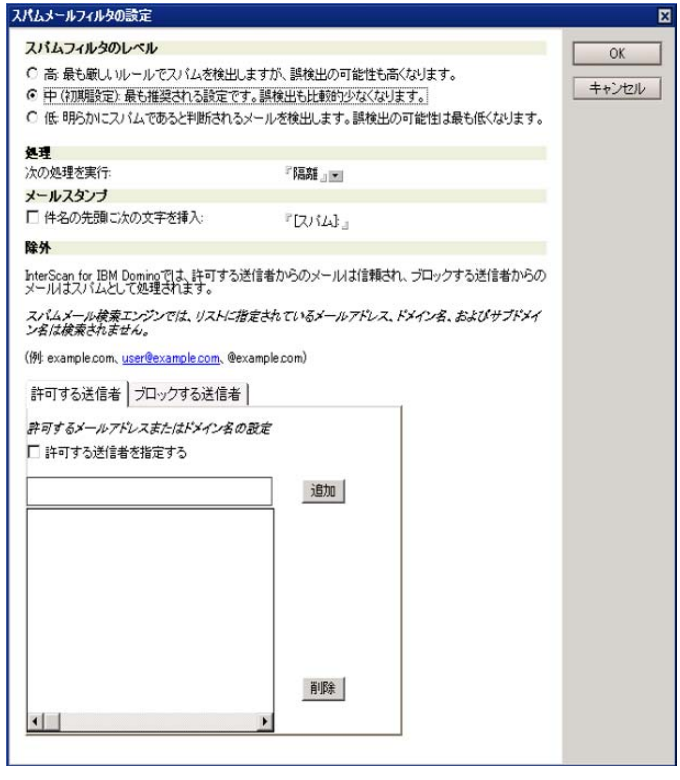


図 4-11. [スパムメールフィルタの設定] 画面

2. [スパムメールフィルタの設定] 画面で、スパムメールフィルタのレベルを選択します。
   - 高 — 最も厳しいスパム検出レベル

     InterScan では、すべてのメッセージについて疑念のあるファイルまたはテキストが含まれていないか監視しますが、一方で誤検出の可能性も高くなります。誤検出とは、実際には正当なメッセージなのに、InterScan によってスパムとしてフィルタ処理されてしまうことです。
   - 中 — 初期設定

ある程度高いレベルのスパム検出でメッセージが監視されますが、誤検出の可能性は「高」より低くなります。

- 低 — 最も寛容なスパム検出レベル

  一般的で明らかにスパムと判断されるメッセージのみをフィルタ処理します。誤検出の可能性は極めて低くなります。

3. [処理] で、迷惑メールに対する処理として [放置]、[隔離]、または [ブロック] から選択します。
4. 件名ヘッダに人目を引く注意やキーワードを追加する場合は、[件名の先頭に次の文字を挿入] を選択してスタンプを入力します。
5. [許可する送信者] と [ブロックする送信者] を有効にして、これらのリストに送信者を指定し、誤検出を最小限に抑えます。
   - [許可する送信者を指定する] チェックボックスをオンにします。

     ブロック対象から除外するメールアドレスまたはドメインを入力した後、[追加] をクリックします。リストからメールアドレスまたはドメインを削除するには、それを選択して [削除] をクリックします。
   - [ブロックする送信者を指定する] チェックボックスをオンにします。

     ブロックするメールアドレスまたはドメインを入力した後、[追加] をクリックします。リストからメールアドレスまたはドメインを削除するには、それを選択して [削除] をクリックします。

注意： [許可する送信者] と [ブロックする送信者] のリストを有効にし、各リストにある送信者をカスタマイズすることにより、誤検出を減らせます。トレンドマイクロが用意したルールとユーザ定義のリストがどのように適用されるかについては、102 ページの「スパムフィルタ (スイート版または情報漏えい対策付きスイート版のみ)」を参照してください。

注意： 承認する送信者、ブロックする送信者、および承認する URL のリストは、いずれも同じデータベース (smlists.nsf) に格納されます。各リストをデータベースで管理できます。リストの管理方法の詳細については、160 ページの「フィルタリストの管理」を参照してください。

---

6. 次のボタンをクリックしてスパムフィルタ設定を保存します。
   - Notes コンソールインタフェースでは、[スパムメールフィルタの設定] 画面の右上隅にある [OK] をクリックしてから、[保存して閉じる] をクリックします。

     または

- Web インタフェースでは、[保存] をクリックします。

EUQ 付きスパムメールフィルタの有効化

1. [メール検索] タブで、[スパムメールフィルタを有効にする] を選択してから [設定] をクリックします。[スパムメールフィルタの設定] 画面が表示されます。

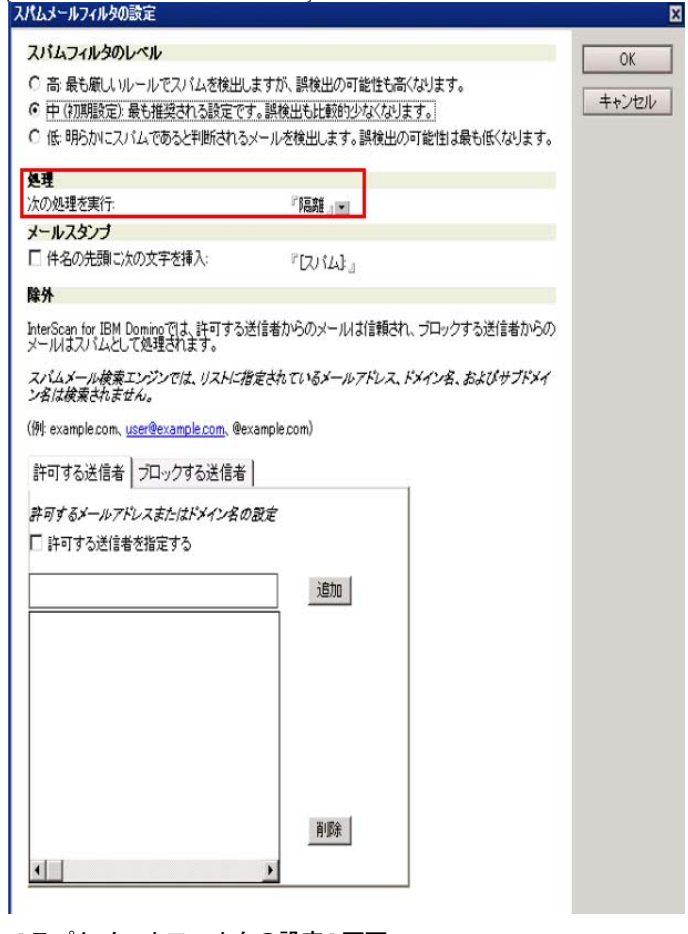


図 4-12. [スパムメールフィルタの設定] 画面

2. [処理] セクションで、迷惑メールに対する処理として [隔離] を選択します。
3. [OK] をクリックします。
4. [スパムメールを許可するが、受信者の迷惑メールフォルダに移動する] を選択します。

エンドユーザメール隔離

エンドユーザメール隔離 (EUQ) 機能によって、メールアカウントでのスパムの表示を許可するかどうかを選択できます。この機能を使用すると、スパムメールを表示して、それを保持、削除、または隔離するかどうかを決定できます。InterScan 5.5 では、EUQ 機能を有効にした場合、すべてのユーザにこの機能が適用されます。InterScan 5.6 では、適用するユーザやグループを選択できるようになりました。

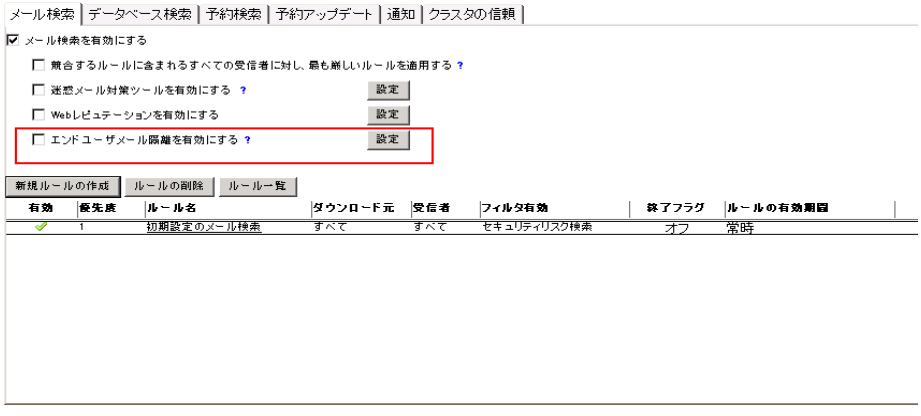


図 4-13.　エンドユーザメール隔離の有効化

警告： Domino サーバで EUQ が有効であり、メールテンプレートの複製も有効な場合は、すべてのサーバ間でメールテンプレートが自動的に複製されます。つまり、メールテンプレートは InterScan がインストールされていないサーバや旧バージョンの InterScan を使用しているサーバにも複製されます。

エンドユーザメール隔離を有効にするには

1. [メール検索] タブで [スパムメールを許可するが、受信者の迷惑メールフォルダに移動する] を選択します。
2. [設定] をクリックします。[すべての受信者] または [選択したユーザ / グループ] のどちらかを選択します。

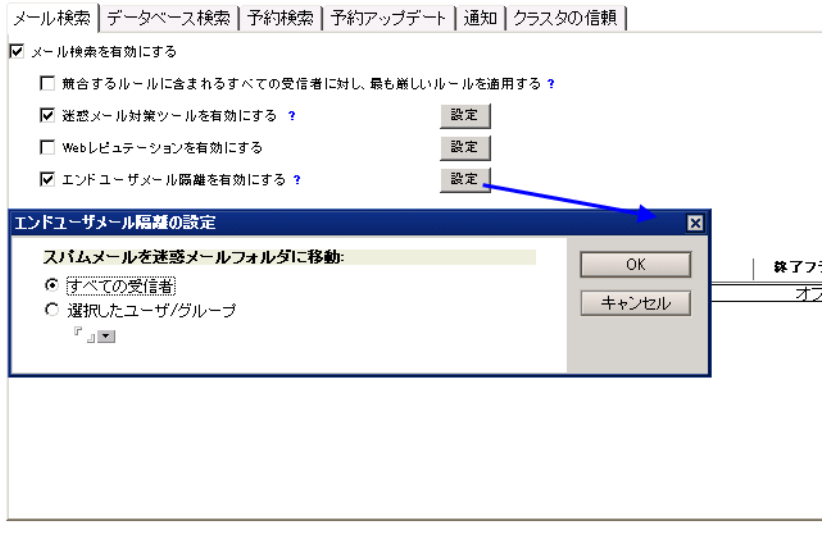


図 4-14. エンドユーザメール隔離の設定

3. [保存して閉じる] をクリックします。

EUQ をユーザのメールボックスに導入するには

1. Domino サーバコンソールで、対象のメールテンプレートに EUQ を導入します。
   - 初期設定のメールテンプレートに EUQ を導入するには、`load smdeuq -install` を実行します。

```
load smdeuq -install
[0A74:0002-069C] 2013/12/04 22:51:17   SMDeuq: 開始しています
[0A74:0002-069C] 2013/12/04 22:51:17   SMDeuq: シャットダウン
[0868:0002-086C] 2013/12/04 22:52:17   Admin Process: Searching Administration Requests database
```

図 4-15. 初期設定のメールテンプレートへの EUQ の導入

- 指定したメールテンプレートに EUQ を導入するには、`load smdeuq -install ${` メールテンプレートのファイルパス `}` を実行します。

```
load smdeuq -install mail85.ntf
[0C88:0002-0DD4] 2013/12/04 22:53:39   SMDeuq: 開始しています
[0C88:0002-0DD4] 2013/12/04 22:53:39   SMDeuq: シャットダウン
```

図 4-16. 指定したメールテンプレートへの EUQ の導入

注意： Domino データフォルダで設定されているメールテンプレートを指定する必要があります。

---

2. Domino サーバコンソールでデザインのロードを実行するか、初期設定を受け入れて午前 1 時に変更を反映させることもできます。

```
load design

[0F30:0002-0ED8] 2013/12/04 22:46:22   Database Designer started
[0D64:0002-0F04] 2013/12/04 22:46:41   Chronos: Performing hourly full text indexing
[0D64:0002-0F04] 2013/12/04 22:46:45   Chronos: Full text indexer terminating
[0F30:0002-0ED8] 2013/12/04 22:47:08   警告: 設計テンプレート cpp freebusy web service が見つかりません。:
[0F30:0002-0ED8] 2013/12/04 22:47:10   警告: 言語 英語 がテンプレート DOLS 管理テンプレート に見つかりません
[0F30:0002-0ED8] 2013/12/04 22:47:10   データベース 'doladmin.nsf' の設計エラー: いくつかの指定した言語が設
[0F30:0002-0ED8] 2013/12/04 22:47:11   警告: 設計テンプレート IBM Notes/Domino S が見つかりません。: IBM N
[0F30:0002-0ED8] 2013/12/04 22:47:11   actnl12.gif をデータベース InterScan承認 へテンプレート InterScan承認
[0F30:0002-0ED8] 2013/12/04 22:47:11   Approval をデータベース InterScan承認 へテンプレート InterScan承認 か
[0F30:0002-0ED8] 2013/12/04 22:47:11   CopyrightTime をデータベース InterScan承認 へテンプレート InterScan承
[0F30:0002-0ED8] 2013/12/04 22:47:11   FormBackground.gif をデータベース InterScan承認 へテンプレート Inter
[0F30:0002-0ED8] 2013/12/04 22:47:11   HiddenCreditsBack.gif をデータベース InterScan承認 へテンプレート In
[0F30:0002-0ED8] 2013/12/04 22:47:11   Logo をデータベース InterScan承認 へテンプレート InterScan承認 から更
[0F30:0002-0ED8] 2013/12/04 22:47:11   MasterFrame をデータベース InterScan承認 へテンプレート InterScan承認
[0F30:0002-0ED8] 2013/12/04 22:47:11   MasterNavigation をデータベース InterScan承認 へテンプレート InterSc
[0F30:0002-0ED8] 2013/12/04 22:47:11   MasterOutline をデータベース InterScan承認 へテンプレート InterScan承
[0F30:0002-0ED8] 2013/12/04 22:47:11   Memo をデータベース InterScan承認 へテンプレート InterScan承認 から更
[0F30:0002-0ED8] 2013/12/04 22:47:11   NoDocuments をデータベース InterScan承認 へテンプレート InterScan承認
[0F30:0002-0ED8] 2013/12/04 22:47:11   Product.jpg をデータベース InterScan承認 へテンプレート InterScan承認
[0F30:0002-0ED8] 2013/12/04 22:47:11   question_mark.gif をデータベース InterScan承認 へテンプレート InterS
[0F30:0002-0ED8] 2013/12/04 22:47:11   RedLine をデータベース InterScan承認 へテンプレート InterScan承認 か
[0F30:0002-0ED8] 2013/12/04 22:47:11   WebNavBackground.gif をデータベース InterScan承認 へテンプレート Int
```

図 4-17. デザインのロード画面

注意： EUQ を導入したら、ユーザのメールボックスを確認します。迷惑メールフォルダに、[ジャンクメール送信者リストの管理] および [承認済みメール送信者リストの管理] の 2 つのメニューアイテムがあるはずです。これらのメニューアイテムは、[すべての受信者] または [選択したユーザ / グループ] のどちらを選択したかに関係なく、すべてのユーザのメールボックスに表示されます。

注意： メールテンプレートに迷惑メールフォルダがない場合、スパムメールはユーザの受信ボックスフォルダに移動されます。

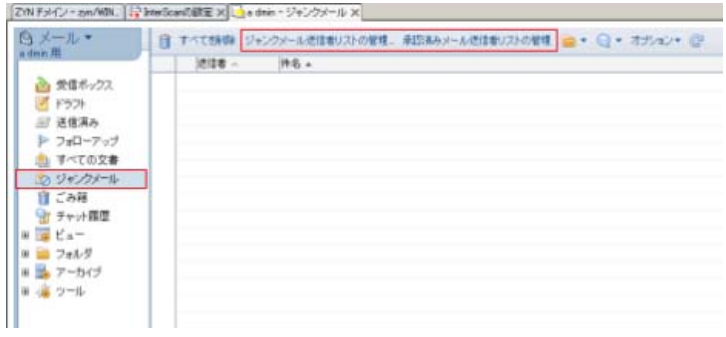


図 4-18. メールの管理画面

承認済みメール送信者リストに送信者を追加するには

1. 迷惑メールフォルダでメールを右クリックして、[送信者を承認済みメール送信者リストに追加する] を選択します。

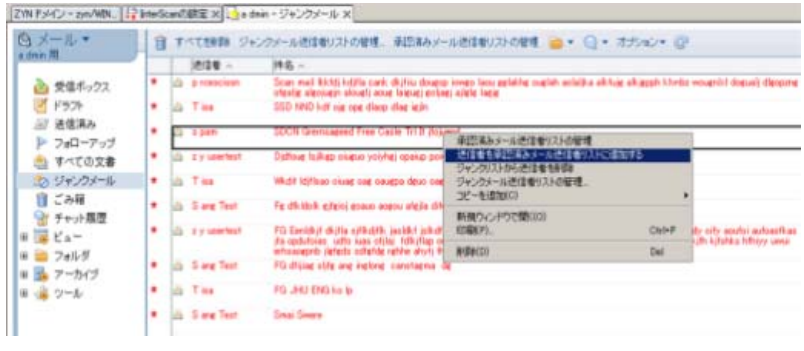


図 4-19. 承認済みリストへの送信者の追加

2. 次のいずれかを選択します。
   - メールアドレスのみ追加

- メールアドレスドメインの追加

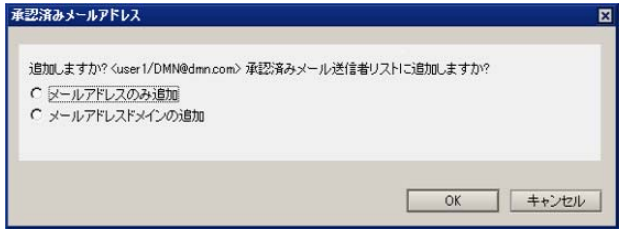


図 4-20. メールアドレスまたはメールアドレスドメインの追加

注意： メールアドレスを承認済みメールアドレスリストから削除するには、メニューバーの [承認済みメール送信者リストの管理] をクリックします。

エンドユーザメール隔離を無効にするには

1. Domino サーバコンソールで、対象のメールテンプレートの EUQ を無効にします。
   - 初期設定のメールテンプレートの EUQ を無効にするには、`load smdeuq -uninstall` を実行します。

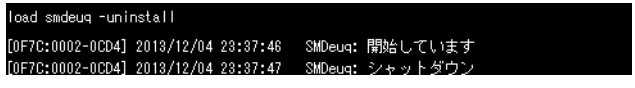


図 4-21. 初期設定のメールテンプレートの EUQ の無効化

   - 指定したメールテンプレートの EUQ を無効にするには、`load smdeuq -uninstall ${` メールテンプレートのファイルパス `}` を実行します。

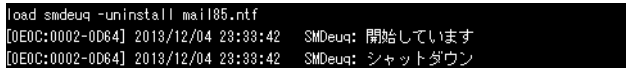


図 4-22. 指定したメールテンプレートの EUQ の無効化

2. Domino サーバコンソールでデザインのロードを実行するか、初期設定を受け入れて午前 1 時に変更を反映させることもできます。
3. [メール検索] タブで、[スパムメールを許可するが、受信者の迷惑メールフォルダに移動する] チェックボックスをオフにします。

Web レピュテーションの設定

[トレンドマイクロの Web レピュテーション] 画面では、Web レピュテーションレーティングに従って、トレンドマイクロの URL フィルタエンジンを使用し、メールに含まれる危険な URL から保護する方法を設定できます。

ローカルおよびグローバルスマートプロテクション

本バージョンの InterScan には、グローバル Smart Protection Network とローカル Smart Protection Server という、URL のレピュテーションと安全性を決定するための 2 つのオプションがあります。グローバル Smart Protection Network は、URL のレピュテーションを調べるために Trend Micro Smart Protection Network に要求を送信します。ローカル Smart Protection Server は、これらの要求をローカルのスマートプロテクションサーバに送信します。ローカル Smart Protection Server は、プライバシーを強化して、要求の処理速度を向上させます。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ保護機能が自動的に更新および強化されることになり、ユーザ自身のリアルタイムな自警システムが構築されていきます。スマートスキャンソリューションでは、クラウド内保護のために Smart Protection Network が利用されます。

Web レピュテーションを設定するには

1. [メール検索] タブで、[Web レピュテーションを有効にする] を選択してから [設定] をクリックします。[トレンドマイクロの Web レピュテーション] 画面が表示されます。

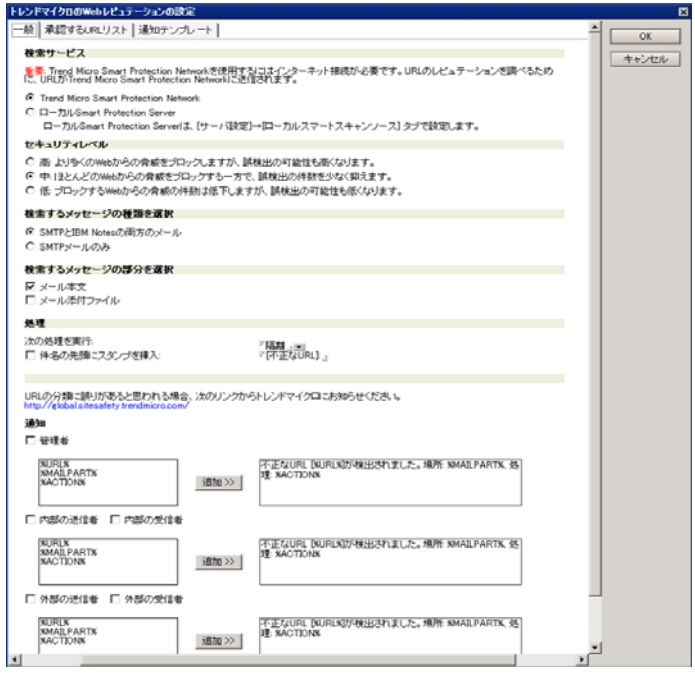


図 4-23. [トレンドマイクロの Web レピュテーション] 画面

2. [トレンドマイクロの Web レピュテーションの設定] 画面の [一般] タブで、使用する検索サービスの方式を選択します。
   - Trend Micro Smart Protection Network
   - ローカル Smart Protection Server

注意： ローカル Smart Protection Server を選択した場合は、[Smart Protection Server による Smart Protection Network への外部クエリの実行を許可しない] も選択できます。

この機能は、Smart Protection Server 2.1 以上を使用している場合のみ動作します。

注意： Smart Protection Server による Smart Protection Network への外部クエリの送信を停止するよう設定する必要もあります。手順については、Smart Protection Server のドキュメントを参照してください。

3. [トレンドマイクロの Web レピュテーションの設定] 画面の [一般] タブで、セキュリティレベルを選択します。
   - 高 — より多くの Web からの脅威をブロックしますが、誤検出の可能性も高くなります。

     InterScan では、すべてのメッセージについて疑念のある URL が含まれていないか監視しますが、一方で誤検出の可能性も高くなります。誤検出とは、実際には正当なメッセージなのに、InterScan によって危険な URL が含まれるメッセージとしてフィルタ処理されてしまうことです。
   - 中 — ほとんどの Web からの脅威をブロックする一方で、誤検出の件数を少なく抑えます。

     ある程度高いレベルの検出でメッセージが監視されますが、誤検出の可能性は「高」より低くなります。
   - 低 — ブロックする Web からの脅威の件数は低下しますが、誤検出の可能性も低くなります。

     一般的で明らかに Web からの脅威と判断される URL が含まれるメッセージのみをフィルタ処理します。誤検出の可能性は極めて低くなります。
4. 検索するメッセージの種類を選択します。
   - SMTP と IBM Notes の両方のメール
   - SMTP メールのみ
5. メッセージの検索対象部分を選択します。
   - メール本文
   - メール添付ファイル
6. [処理] セクションの [次の処理を実行] で、[放置]、[隔離]、または [ブロック] から選択します。

注意： [検索するメッセージ部分の選択] セクションで [メール添付ファイル] を選択し、[処理] セクションで [ブロック] を選択した場合は、[添付ファイルに不要な URL のみ含まれる場合は添付ファイルを削除する] を選択して不要な URL を含む添付ファイルのみを削除し、メールを受信者に渡すこともできます。ただし、[検索するメッセージ部分の選択] セクションで [メール本文] を選択し、[処理] セクションで [ブロック] を選択した場合は、メール本文に不要な URL が含まれるとメッセージ全体がブロックされます。

7. 件名ヘッダに人目を引く注意やキーワードを追加する場合は、[件名の先頭にスタンプを挿入] を選択してスタンプを入力します。

   注意： URL の分類に誤りがあると思われる場合、次のリンクからトレンドマイクロにお知らせください。
   http://global.sitesafety.trendmicro.com

8. [通知] セクションで、Web レピュテーションフィルタによって URL が識別されたときに適用する通知オプションを選択します。
9. [承認する URL リスト] タブで、[承認する URL リストを有効にする] をオンにし、次の手順で URL リストに対して URL の [追加]、[インポート]、[エクスポート]、または [削除] を実行すると、誤検出を最小限に抑えることができます。
   - [追加] フィールドに URL を入力して、[追加] をクリックします。
   - テキストファイル (*.txt) から URL のリストをインポートするには、[インポート] をクリックして、[追加] をクリックします。
   - URL のリストをテキストファイル (*.txt) にエクスポートするには、[エクスポート] をクリックします。
   - 1 つの URL を削除するには、削除する URL を選択して、[削除] をクリックします。
   - すべての URL を削除するには、[すべて削除] をクリックします。
10. [通知テンプレート] タブで、通知テンプレートを設定します。
11. すべての設定を完了したら、[OK] をクリックして設定内容を保存し、終了します。

    注意： 承認する URL のリストは、smlists.nsf データベースで管理できます。データベースでのリストの管理方法の詳細については、160 ページの「フィルタリストの管理」を参照してください。

Web レピュテーションの最適化

適宜設定を行うことで、Web レピュテーション検索のパフォーマンスを最適化できます。次を実装して、使用しているバージョンの Web レピュテーションを最適化することを検討してください。

- 会社の内部 URL を [承認済み URL リスト] に追加します。内部 URL を含むメッセージの検索が省略され、ネットワーク帯域幅の使用量を削減することでパフォーマンスが向上します。

- Smart Protection Server を使用してネットワーク帯域幅の使用量を削減します。Web レピュテーションサービスは、URL クエリを外部 Smart Protection Network またはローカル Smart Protection Server に送信します。Smart Protection Network にクエリを送信する場合、インターネット接続が低速であるとネットワークのパフォーマンスに悪影響を及ぼすことがあります。管理コンソールを使用して Smart Protection Server を設定し、[サーバ設定] → [ローカルスマートスキャンソース] をクリックして Web レピュテーションソースを変更します。
- Smart Protection Server のパフォーマンスを最適化するには、InterScan 専用の Smart Protection Server の導入を検討します。Smart Protection Server が InterScan とウイルスバスター Corp. の両方にサービスを提供している場合は、サーバパフォーマンスが低下することがあります。

Web レピュテーションのパフォーマンスの問題に関するトラブルシューティング

Web レピュテーションの実行速度が遅い場合は、次のように Web レピュテーションの設定をテストします。

- ネットワーク接続が安定していることを確認します。
- InterScan は、Web レピュテーションサービスを提供している Smart Protection Network と Smart Protection Server への接続ステータスを監視します。InterScan が Web レピュテーションソースに接続できないときは必ず通知を受け取るように、[Web レピュテーションサービスが次の場合に通知を送信する :] (使用不可 / 使用可能) を有効にします。頻繁にこのアラートを受信する場合は、ネットワーク接続の安定性に問題がある可能性を示しています。

セキュリティリスク検索の設定

文書にウイルスなどの不正プログラムが含まれていないか検索する方法を定義するには、[セキュリティリスク検索] タブを使用します。

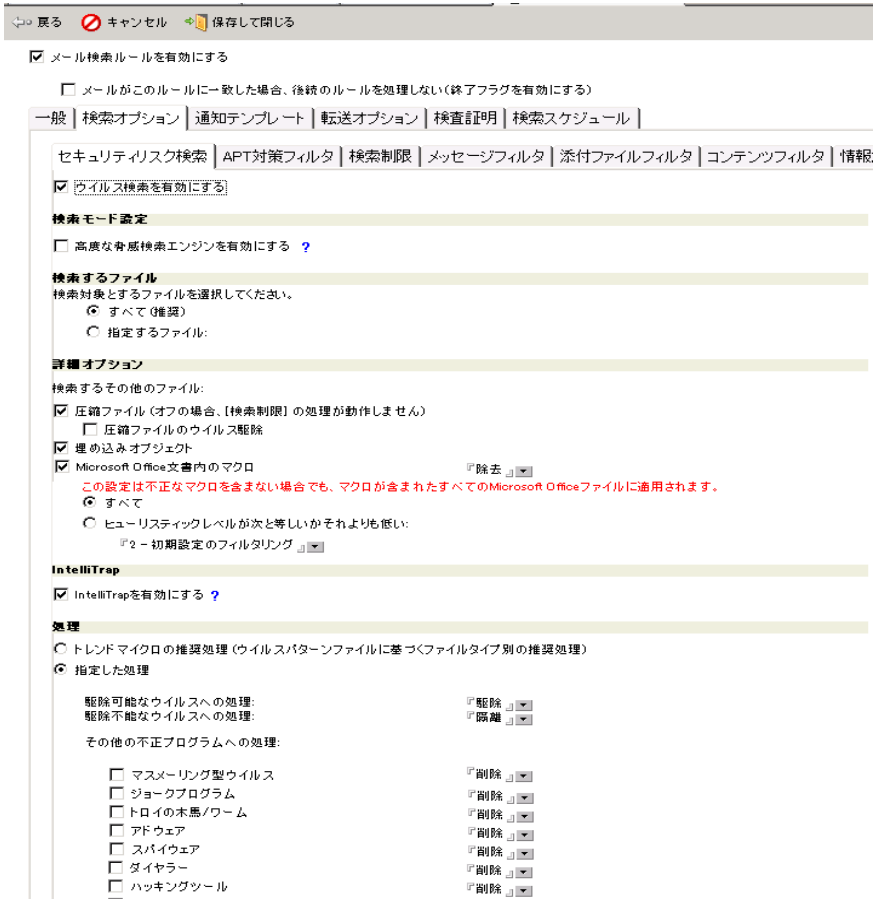


図 4-24.　[検索オプション] → [セキュリティリスク検索] 画面 >

セキュリティリスク検索オプションを設定するには

1. [検索オプション] で、[セキュリティリスク検索] タブをクリックします。
2. [セキュリティリスク検索] タブの [検索モード設定] セクションで [高度な脅威検索エンジンを有効にする] をクリックします。

注意： 高度な脅威検索エンジンは、文書の悪用を含め、従来とは異なる脅威がないかどうかファイルを確認します。ただし、実際には安全なファイルを検出してしまう場合もあります。そのため、Deep Discovery Advisor によって提供される仮想環境でさらに監視して分析する必要があります。Deep Discovery Advisor の詳細については 16 ページの「APT 対策の強化」を、設定手順については 159 ページの「Deep Discovery Advisor の設定」を参照してください。

3. [検索するファイル] セクションで、セキュリティリスク検索オプションを次のように設定します。

   a. 次のオプションから、検索するファイルを選択します。

      - [すべて (推奨)] を選択すると、ファイルタイプ、ファイル名、または拡張子で指定したファイルを除くすべての文書が検索されます。

        除外するファイルを実際のファイルタイプ別に定義するには、[検索から除外する実際のファイルタイプ] にファイル名か拡張子を入力します。または、 をクリックしてリストから選択します。[検索から除外するファイル名 / 拡張子] にファイル名または拡張子を入力するか、 をクリックしてリストから選択し、ファイル名または拡張子に基づいて除外対象を指定することもできます。

      - [指定するファイル] を選択すると、ファイル名または拡張子に基づいて文書が検索されます。

        拡張子については、初期設定リストが事前に用意されています。検索するファイル名または拡張子を新規に定義するには、[ファイル名または拡張子によるファイル検索] にファイル名か拡張子を入力します。または、 をクリックしてリストから選択します。

4. [詳細オプション] セクションで、次のように設定を指定します。

   - [圧縮ファイル] をオンにすると、圧縮ファイルが検索されます。

     InterScan には、検索する圧縮ファイルのタイプの初期設定リストがあります。検索する圧縮レベル数は、[検索制限] タブで指定できます。[圧縮ファイルのウイルス駆除] を選択すると、検索のためにファイルが解凍されます。この処理では、ディスクスペースが大量に消費されることがあります。

     注意： InterScan でサポートされている圧縮ファイルタイプのリストについては、トレンドマイクロの製品 Q&A を参照してください。

   - [埋め込みオブジェクト] をオンにすると、OLE が検索されます。

InterScan では、IBM Notes メール内の埋め込みオブジェクトを検索できます。

- [Microsoft Office 文書内のマクロ] をオンにすると、ヒューリスティック検索を使用して Microsoft Office ファイル (*.doc、*.xls など) に含まれるマクロウイルスや不正プログラムが検出されます。

  ヒューリスティック検索は、パターンファイルの検出テクノロジとルールベースの検出テクノロジを使用して不正なマクロを検出する評価方法です。

  [Microsoft Office 文書内のマクロ] をオンにした場合は、さらに次のいずれかのオプションを選択します。

  - [すべて] を選択すると、検出されたすべてのマクロに対して処理が実行されます。

  注意： この設定は、不正であるかどうかに関係なく、マクロを含むすべての Microsoft Office ファイルに適用されます。

  - [ヒューリスティックレベルが次と等しいかそれよりも低い] を選択すると、検出されたマクロのうち、ヒューリスティックレベルが指定したレベルと同じかそれよりも低いマクロに対して処理が実行されます。

    [ヒューリスティックレベルが次と等しいかそれよりも低い] を選択した場合は、ヒューリスティックレベルも選択する必要があります。

    注意： ヒューリスティックレベルを選択する場合には、以下を参考にしてください。

    - レベル 1 は、基準が最も高く、検出されるマクロの数が最も少なくなります。
    - レベル 4 は、基準が最も低く、検出されるマクロの数が最も多くなりますが、安全なマクロも不正なマクロとして誤検出される可能性があります。
    - トレンドマイクロが推奨するレベルはレベル 2 です。このレベルを選択すると、高いレベルの検出を短時間で実行できます。このレベルは、マクロウイルスや不正プログラムの文字列を検出するために必要なルールだけを使用し、誤検出の可能性も低くなります。

5. [IntelliTrap] セクションで、IntelliTrap による検索を有効にするかどうかを指定します。

注意： ウイルス作成者は、リアルタイム圧縮のアルゴリズムを使用してウイルスフィルタを回避しようとすることがあります。IntelliTrap は、メールの添付ファイルとして着信するリアルタイム圧縮された実行可能ファイルをブロックし、他の不正プログラムの特性とこれらのファイルを照合することによって、ユーザのネットワークにウイルスが侵入するリスクを軽減します。

6. [処理] セクションで、次のように感染ファイルに対する検索処理を設定します。

   - [トレンドマイクロの推奨処理を使用する (ウイルスパターンファイルに基づくファイルタイプ別の推奨処理)] を選択すると、不正プログラムの種類が特定され、トレンドマイクロのパターンファイルを使用して、それぞれの種類によるコンピュータシステムまたは環境への感染の影響に基づいて検索処理またはフィルタ処理が自動的に推奨されます。駆除できない項目に対する初期設定処理は、[隔離] です。

     [トレンドマイクロの推奨処理] を選択した場合は、駆除できない Microsoft Office ファイルに対して実行する処理を選択する必要があります。Microsoft Office ファイルには、除去できないマクロが含まれている場合があり、このようなファイルは駆除できないファイルとして検索されます。[駆除不能なウイルスへの処理] で選択する処理は、Microsoft Office ファイルにのみ適用されます。パターンファイルで定義されている処理は、その他すべてのファイルタイプに適用されます。

   - [指定する処理] を選択すると、不正プログラムの種類に応じて InterScan で実行する処理を選択できます。

注意： [圧縮ファイルのウイルス駆除] が無効な場合は、不正プログラムが含まれる圧縮ファイル全体に、検出された不正プログラムに対する処理が適用されます。[圧縮ファイルのウイルス駆除] が有効な場合は、不正プログラムが含まれる特定のファイルのみに処理が適用されます。

対象とする脅威とそれに対する指定処理が [その他の不正プログラムへの処理] で有効になっていない場合、検出された脅威すべてに対して、[駆除可能なウイルスへの処理] または [駆除不能なウイルスへの処理] が適用されます。[その他の不正プログラムへの処理] をカスタマイズするには、対象の脅威を有効にしてから、対応する処理を選択します。

たとえば、[マスメーリング型ウイルス] が有効で、それに対する処理として [削除] を選択している場合、マスメーリング型ウイルスは検出されると自動的に削除されます。

7. [通知] セクションで、不正プログラムが検出されたとき、または駆除不能なとき、あるいは検索処理が感染ファイルに適用されたときの通知オプションを選択します。
8. [メールのスタンプ] セクションで、適切なオプションを選択して入力します。
9. [保存して閉じる] をクリックします。

APT 対策フィルタの設定

[APT 対策フィルタ] タブを使用すると、APT 脅威や最新または不明なセキュリティ脅威について、疑わしいファイルに対する InterScan の処理を設定できます。

注意： APT 対策フィルタを設定する前に、Deep Discovery Advisor を設定して起動する必要があります。手順については、159 ページの「Deep Discovery Advisor の設定」参照および 126 ページの「Deep Discovery Advisor エージェントの起動」参照してください。

APT 対策フィルタオプションを設定するには

1. [検索オプション] で、[APT 対策フィルタ] タブをクリックします。
2. [分析するメッセージを Deep Discovery Advisor に送信する] を選択します。

   注意： Deep Discovery Advisor はシミュレータを使用して、疑わしいファイルが示す有害な可能性のある挙動を識別します。これにより、APT 脅威や最新または不明なセキュリティ脅威で使用されているファイルを特定できます。

3. [APT 対策フィルタ] タブの [検索設定] セクションで、APT 対策フィルタオプションを次のように設定します。
   - 次のオプションから、検索するメッセージを選択します。
     - 受信メッセージのみ (推奨)
     - 受信メッセージと送信メッセージ
   - 次のオプションから、検索する添付ファイルを選択します。
     - 高度な脅威検索エンジンにより検出 (推奨)

注意： [高度な脅威検索エンジンにより検出] オプションを使用するには、[セキュリティリスク検索] タブで高度な脅威検索エンジンを有効にする必要があります。手順については、120 ページの「セキュリティリスク検索の設定」参照を参照してください。

- 指定したタイプのファイル — InterScan では、200 種類を超えるファイル形式のコンテンツ (Notes のデータベース形式を含む) と添付ファイルとして使用される可能性のあるさまざまなファイルタイプを開き、整理して、検索できます。[指定したタイプのファイル] を選択すると次を実行できます。
  - [編集] をクリックして、InterScan ファイルタイプデータベースのファイルタイプグループを変更できます。
  - 検索するファイルタイプを、[アーカイブ]、[実行可能ファイルとアプリケーション]、[画像]、[オーディオ / ビデオ]、[Flash ファイル]、[文書]、[その他] から選択します。
  - 新しいファイルタイプを入力するか、  をクリックして [実際のファイルタイプ] でタイプを選択します。

注意： [APT 対策フィルタ] でファイルタイプグループを変更すると、[添付ファイルフィルタ] のファイルタイプグループ情報も更新されることに注意してください。

4. [セキュリティレベル] セクションで、処理を適用する InterScan のセキュリティレベルを次のオプションから選択します。
   - 高 : 挙動が不審なすべてのメッセージに処理を適用
   - 中 : 不正なメッセージである可能性が比較的高いメッセージに処理を適用
   - 低 : 不正なメッセージである可能性が高いメッセージだけに処理を適用
5. [処理] セクションで、[放置]、[隔離]、[ブロック]、または [添付ファイルの削除] からフィルタ処理を選択します。
6. [通知] セクションで、APT 対策フィルタによって疑わしいファイルが識別されたときの通知オプションを選択します。
7. [メールのスタンプ] セクションで、通知メールのメールスタンプ設定を定義します。
8. [保存して閉じる] をクリックします。

Deep Discovery Advisor エージェントの起動

Deep Discovery Advisor エージェントを手動で起動するには

- Domino コンソールで次のコマンドを入力し実行します。

  load smddtas

Deep Discovery Advisor エージェントを Domino サーバによって自動的に起動するには

1. テキストエディタを使用して、InterScan がインストールされている Domino サーバの ***notes.ini*** を開き、`ServerTasks` に次のアイテムを追加します。

   SMDdtas

2. ***notes.ini*** を保存して閉じます。

検索制限の設定

圧縮ファイル、および特殊な動作や未知の動作をするファイルに対する処理を設定するには、[検索制限] タブを使用します。

検索制限を設定するには

1. [検索オプション] で、[検索制限] タブをクリックします。
2. 圧縮ファイル、および特殊な動作や未知の動作をするファイルに対する検索処理を指定します。
   - 解凍ファイルサイズが次の上限を超えた場合 — [解凍ファイルサイズの上限] の設定値を超える圧縮ファイルの検索を制限します。

     ファイルサイズをキロバイト (KB) 単位で指定します。
   - 圧縮レベルが次の上限を超えた場合 — [圧縮レベルの上限] の設定値を超える圧縮ファイルの検索を制限します。

     [圧縮レベルの上限] を設定して、検索する圧縮レベル数の限度を指定します。たとえば、圧縮後に再圧縮されたファイル (圧縮レベル数は 2) のみを検索するには、[圧縮レベルの上限] を「3」に設定します。

     注意： InterScan では、20 レベルまで検索できます。
   - 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ファイルの検索を制限します。

- 不明な原因により添付ファイルを検索できない場合 — 検索できないファイルの処理方法を選択できます。

3. [通知] セクションで、ファイルが添付ファイルフィルタに一致したときの通知オプションを選択します。
4. [メールのスタンプ] セクションで、適切なメールスタンプの設定を定義します。
5. [保存して閉じる] をクリックします。

メッセージフィルタの設定

メッセージを扱う方法を定義するには、[メッセージフィルタ] タブを使用します。

メッセージフィルタオプションを設定するには

1. [検索オプション] で、[メッセージフィルタ] タブをクリックします。
2. [メッセージフィルタを有効にする] チェックボックスをオンにします。
3. [処理] セクションで、次の条件のいずれかに該当する暗号化されたメッセージに対する検索処理を定義します。
   - メッセージサイズが次の条件に一致する場合 — 指定制限値の条件に一致するメッセージについては、検索を省略して指定処理を自動的に実行できるようにします。

     サイズの上限をバイト (B)、キロバイト (KB)、またはメガバイト (MB) 単位で設定します。
   - ドメイン内の暗号化メール — 同じドメインにいるユーザどうしで送受信した暗号化メッセージについては、検索を省略して指定処理を自動的に実行できるようにします。
   - インバウンドの暗号化メール — 暗号化された受信メッセージについては、検索を省略して指定処理を自動的に実行できるようにします。
   - アウトバウンドの暗号化メール — 暗号化された送信メッセージについては、検索を省略して指定処理を自動的に実行できるようにします。
   - 分割メッセージ — 不完全なメッセージについては、検索を省略して指定処理を自動的に実行できるようにします。
   - 次の文字セットのメッセージ — 特定の文字セットのメッセージについては、検索を省略して指定処理を自動的に実行できるようにします。
4. [通知] セクションで、ファイルが通知フィルタに一致したときの通知オプションを選択します。
5. [メールのスタンプ] セクションで、適切なメールスタンプの設定を定義します。
6. [保存して閉じる] をクリックします。

添付ファイルフィルタの設定

メッセージの添付ファイルをフィルタ処理する方法を定義するには、[添付ファイルフィルタ] タブを使用します。

次の添付ファイルは、InterScan サーバでブロックすることをお勧めします。

表 4-1.　ブロックが推奨されるファイルの拡張子

拡張子	説明
.386	Windows の拡張モードドライバまたはスワップファイル
.ACM	Windows のオーディオ圧縮マネージャドライバとシステムファイル
.ASP	Active Server Page
.AVB	Inoculan Anti-Virus が検出したウイルス感染ファイル
.BAT	バッチ処理
.BIN	バイナリファイル
.CLA	Java クラスファイル (通常は `*.CLASS` だが短縮形の場合もある)
.CLASS	Java クラスファイル
.CMD	OS/2 と Windows NT のコマンドファイル、DOS と CP/M のコマンドファイル、dBase II のプログラムファイル
.CNV	MS Word のデータ変換ファイル
.COM	実行可能ファイル
.CS*	Corel Script
.DLL	ダイナミックリンクライブラリ
.DRV	デバイスドライバ
.EXE	実行可能ファイル
.GMS	Corel Global Macro Storage
.HLP	Windows のヘルプファイル
.HTA	ハイパーテキストアプリケーション　(HTML ファイルから実行するアプリケーション)
.HTM .HTML	ハイパーテキストマークアップ言語

表 4-1.　ブロックが推奨されるファイルの拡張子

拡張子	説明
.HTT	ハイパーテキストテンプレート
.INF	情報ファイルまたはセットアップファイル
.INI	初期化ファイルまたは設定ファイル
.JS* .JS .JSE	JavaScript ソースコード
.LNK	リンカファイル、Windows のショートカットファイル
.MHT*	Microsoft の MHTML 文書　(Web ページのアーカイブ)
.MPD	ミニポートドライバ
.OCX	OLE　(Object Linking and Embedding) の制御拡張
.OV*	プログラムオーバーレイファイル　(.OVL)
.PIF	Windows のプログラム情報ファイル
.SCR	スクリーンセーバスクリプト
.SHS	シェルスクラップオブジェクトファイル
.SYS	システムデバイスドライバ
.TLB	リモートオートメーション用タイプライブラリファイル
.TSP	Windows のテレフォニサービスプロバイダ
.VBS	Visual Basic スクリプト
.VBE	暗号化された Visual Basic スクリプト
.VXD	仮想デバイスドライバ
.WBT	WinBatch スクリプト
.WIZ	ウィザードファイル
.WSH	Windows のスクリプトホスト設定ファイル

添付ファイルフィルタオプションを設定するには

1. [検索オプション] → [添付ファイルフィルタ] タブをクリックします。
2. [添付ファイルフィルタを有効にする] をオンにします。

3. ファイルサイズに基づいて添付ファイルをフィルタ処理するには、[ファイルサイズによる添付ファイルのフィルタ] セクションで、[サイズによる添付ファイルフィルタを有効にする] をオンにします。

   注意： 添付ファイル当たりのファイルサイズを指定できるほか、すべての添付ファイルの合計サイズを指定することもできます。サイズの上限をバイト (B)、キロバイト (KB)、またはメガバイト (MB) 単位で設定します。単一の添付ファイルのファイルサイズまたはすべての添付ファイルの合計 (すべての添付ファイルの合計ファイルサイズ) を指定します。

4. [ファイルサイズによる添付ファイルのフィルタ] のフィルタ処理を次の中から 1 つ選択します。[放置]、[隔離]、[削除]、[メールをブロック]、[承認のためにメールを転送]、または [指定する時間帯に配信]

   注意： [指定する時間帯に配信] を選択した場合は、送信する曜日と時刻を指定します。

5. [ファイルタイプによる添付ファイルのフィルタ] セクションで、[ファイルタイプによる添付ファイルフィルタを有効にする] チェックボックスをオンにします。

   InterScan では、200 種類を超えるファイル形式のコンテンツ (Notes のデータベース形式を含む) と添付ファイルとして使用される可能性のあるさまざまなファイルタイプを開き、整理して、検索できます。

   a. 検索するファイルタイプを、[すべてのファイルタイプ]、[指定]、[指定するファイルタイプを除くすべて] から選択します。

      [指定] または [指定するファイルタイプを除くすべて] を選択すると、次の操作を実行できます。

      - InterScan ファイルタイプデータベースを編集する
      - 実際のファイルタイプ、実際のファイルタイプのグループ、または拡張子名に基づいて、新しいエントリを入力するか、 をクリックしてファイルタイプを選択する

      注意： Domino では、添付ファイルのファイル名がメールメッセージ本文中に埋め込まれていることがあります。本文の検索によって、ファイル名に含まれる指定の単語が検出されます。

   b. フィルタ処理を [放置]、[隔離]、[削除]、[メールをブロック]、または [承認のためにメールを転送] から選択します。

c. 圧縮ファイルを検索するには、[圧縮ファイルの内部に対する添付ファイルフィルタを有効にする] を選択します。初期設定では、サーバのパフォーマンスを最適化するためにこのオプションは無効になっています。

6. [除外設定] セクションの [許可する添付ファイル名] に、フィルタ処理から除外する添付ファイルの名前を入力します。複数のファイル名または拡張子名を指定する場合、ワイルドカード文字 (* または ?) を使用できます。エントリ間は、セミコロン (;) で区切ります。

   [許可する添付ファイル名] に指定したファイル名または拡張子名は、添付ファイルのフィルタ処理条件より優先されます。

7. [通知] セクションで、ファイルが添付ファイルフィルタに一致したときの通知オプションを選択します。
8. [メールのスタンプ] セクションで、適切なメールスタンプの設定を定義します。
9. [保存して閉じる] をクリックします。

コンテンツフィルタの設定

コンテンツフィルタによって、管理者が定義する明示的なルールに基づいて InterScan がメッセージの内容をフィルタ処理する方法が定義されます。

企業秘密のリーク、侮辱的または不適切な言葉遣い、競合他社または敵国との不審な接触がないかをチェックすることなど、コンテンツセキュリティにはさまざまな形があります。

注意： 検索は、Microsoft Office および Adobe Portable Document Format に対応しています。

[コンテンツフィルタ] タブでは、一般的なルールと詳細なルールを定義できます。詳細については、104 ページを参照してください。

コンテンツフィルタオプションを設定するには

1. [検索オプション] で、[コンテンツフィルタ] タブをクリックします。
2. [メール検索ルールを有効にする] チェックボックスをオンにします。
   - 一致するルールが見つかった後に他のルールの処理を停止するには、[メールがこのルールに一致した場合、後続のルールを処理しない (終了フラグを有効)] チェックボックスをオンにします。
3. [コンテンツフィルタを有効にする] チェックボックスをオンにします。
4. [コンテンツフィルタ] セクションで、[新規コンテンツフィルタの作成] (132 ページ) または [既存コンテンツフィルタの追加] (134 ページ) を選択します。
5. [処理] セクションで、[内容が不適切なメールへの処理] を選択して、検索処理を指定します。

6. [通知] セクションで、メッセージについての適切な通知とフィルタ処理のオプションを選択します。

   指示または説明を追加するには、通知にフィルタの説明を加えます。
   例 : 詳細については、Domino の管理者に確認してください。

7. [保存して閉じる] をクリックします。

コンテンツフィルタの新規作成

コンテンツフィルタを新規作成するには、[コンテンツフィルタ] タブを使用します。

コンテンツフィルタを新規作成するには

1. [コンテンツフィルタ] タブで [新規コンテンツフィルタの作成] をクリックします。
2. [フィルタ名] に、新規コンテンツフィルタの名前を入力します。
3. 使用可能な式に対して比較する項目の選択] セクション で、キーワードと比較するメッセージの部分 ([件名]、[送信者]、[宛先]、[Cc]、[メール本文]、[添付ファイルの内容]、[添付ファイル名]) を選択します (詳細については、105 ページの「キーワード」を参照してください)。

図 4-25. コンテンツフィルタの新規作成

4. 選択部分すべてがコンテンツフィルタのキーワードと一致する場合のみ、一致を返すよう設定するには、[上記で選択した対象がすべて一致する場合にコンテンツフィルタに一致] を選択します。
5. [キーワード] で、コンテンツフィルタ処理に使用するキーワードを作成するか、追加します。詳細については、134 ページの「新規キーワードの作成」または 135 ページの「既存のキーワードを利用した新規キーワードの追加」を参照してください。
   - メッセージ内のキーワード数が指定値を超えた場合に迷惑メールに対する処理を実行するように指定するには、[メッセージで使用されているキーワードの種類が次の値を超えた場合にコンテンツフィルタに一致] にその指定値を示す整数を入力します。
   - メッセージ内のキーワードの合計数が指定値に一致した場合に迷惑メールに対する処理を実行するように指定するには、[.OCCUR. の頻度　(回数)] にその指定値を示す整数を入力します。
   - メッセージ内のキーワード間の語数が指定値を超えた場合に迷惑メールに対する処理を実行するように指定するには、[.NEAR. の近接値　(語数)] にその指定値を示す整数を入力します。

   注意： .OCCUR. と .NEAR. がキーワードに使用されている場合は、論理演算子には AND が使用されます。
6. [保存して閉じる] をクリックします。

コンテンツフィルタの削除

すべてのまたは特定のコンテンツフィルタを削除するには、[コンテンツフィルタの削除] を使用します。

コンテンツフィルタを削除するには

1. 削除するフィルタをクリックします。
2. [コンテンツフィルタの削除] をクリックします。
3. すべてのコンテンツフィルタを削除するには、[すべて削除] をクリックします。

コンテンツフィルタが削除され、変更についてリアルタイムメール検索タスクを実行するよう促されます。

既存フィルタを利用した新規コンテンツフィルタの追加

検索するメッセージ部分を定義するコンテンツフィルタを作成して、それを他のコンテンツフィルタの要素として使用できます。たとえば、件名ヘッダ検索用、添付ファイル検索用、およびメール全体検索用のコンテンツフィルタを 1 つずつ作成してから、これらのフィルタを基にしてコンテンツフィルタを作成できます。

新規コンテンツフィルタを追加するには

1. [コンテンツフィルタ] ワークスペースで、[キーワードの追加] ボタンをクリックします。
2. [キーワードの追加] 画面で、追加するキーワードをクリックします。複数のキーワードを選択できます。
3. [OK] をクリックします。

注意： コンテンツフィルタに追加するキーワードが多すぎると、フィルタが予想以上に複雑になることがあります。設定するキーワードは、コンテンツフィルタあたり 1、2 語にすることを推奨します。

新規キーワードの作成

フィルタ処理する単語、フレーズ、コンセプトそれぞれに対して、キーワードを新規に作成します。あるいは、複数の検索条件を 1 つの複合キーワードに結合することもできます。

ヒント： コンテンツフィルタに追加する条件が多すぎると、フィルタが予想以上に複雑になることがよくあります。作成するキーワードは、コンテンツフィルタあたり 1、2 語にすることを推奨します。

キーワードを新規作成するには

1. [コンテンツフィルタルール] ワークスペースで、[新規キーワードの作成] をクリックします。[新規キーワード] 画面が表示されます。
2. [定義] セクション の [キーワード] に、フィルタ処理するキーワード (単語またはフレーズ) を論理演算子で結合して入力します。論理演算子の使用方法の詳細については、[新規キーワード] 画面の最下部にあるヘルプセクションを参照してください。

注意： 本バージョンの InterScan では、コンテンツフィルタに正規表現を使用できます。たとえば、クレジットカード番号をフィルタ処理する場合、.REG. を使用して、次のように入力します。

Visa、MasterCard、および JCB の場合

```
.REG.(6011|5[1-5]¥d{2}|4¥d{3}|67¥d{2})([:space:]|¥.|¥¥|¥||-)?¥d{4
}([:space:]|¥.|¥¥|¥||-)?¥d{4}([:space:]|¥.|¥¥|¥||-)?¥d{4}
```

3. 大文字と小文字を区別した照合を有効または無効にします。
4. [保存して閉じる] をクリックします。

ヒント： メール検索ルールで新しいキーワードを有効にする前に、まず、そのキーワードをテストして、予期しない結果が発生しないことを確認します。また、処理として [削除] ではなく [隔離] を選択します。

既存のキーワードを利用した新規キーワードの追加

既存キーワードをテンプレートとして再利用して、新規キーワードを追加できます。

新規キーワードを追加するには

1. [コンテンツフィルタ] タブで既存のコンテンツフィルタを 1 つ選択して、[既存コンテンツフィルタの追加] をクリックします。
2. [コンテンツフィルタの追加] 画面で、使用するコンテンツフィルタを選択します。キーワードは複数個選択できます。
3. [OK] をクリックします。

ヒント： 1 つのメール検索ルールに設定するコンテンツフィルタが多すぎると、ルールが予想以上に複雑になる場合があります。設定するコンテンツフィルタは、メール検索ルールあたり 1 つか 2 つにすることをお勧めします。

情報漏えい対策

本バージョンの InterScan では、情報漏えい対策フィルタを使用してメールコンテンツ内の機密データを検出できます。コンプライアンスパターンは、社会保障番号 (SSN)、クレジットカード番号 (CCN)、電話番号など、構造化されたコンテンツでの使用に適しています。

たとえば、クレジットカード番号は一般に 16 桁形式の「xxxx-xxxx-xxxx-xxxx」で示されるため、パターンベースの検出に適しています。

注意： 検索は、Microsoft Office および Adobe PDF に対応しています。データベースではメールデータベースのみ検索されます。

[情報漏えい対策] で、情報漏えい対策テンプレートとデータ識別子を管理できます。

情報漏えい対策テンプレートの管理

[設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] から情報漏えい対策テンプレートの追加、削除、コピー、インポート、エクスポート、および表示を実行できます。パターンとキーワードを使用してカスタムテンプレートを作成できます。このテンプレートには複数のパターンとキーワードを含めることができます。

カスタムテンプレートを追加するには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. [追加] をクリックします。
3. [名前] と [説明] を入力します。
4. [一致条件] セクション で、[データ識別子] として [パターン] または [キーワード] を選択します。
5. 既存のものを選択するか、新しいキーワードまたはパターンをインポートまたは追加して、>> をクリックし、[一致条件] ウィンドウに追加します。
6. [テンプレート定義に追加する] をクリックします。
7. [保存して閉じる] をクリックします。

情報漏えい対策テンプレートを削除するには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. カスタムテンプレートを選択して、[削除] をクリックします。

情報漏えい対策テンプレートをコピーするには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. 1 つ以上のテンプレートを選択して、[コピー] をクリックします。

情報漏えい対策テンプレートをインポートするには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. [インポート] をクリックして、.dat 形式のテンプレートを選択します。

情報漏えい対策テンプレートをエクスポートするには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. ［エクスポート］をクリックします。

情報漏えい対策テンプレートを表示するには

1. [設定] → [情報漏えい対策] → [情報漏えい対策テンプレート] をクリックします。
2. 表示するテンプレートをダブルクリックします。

> **注意：** 変更できるのはカスタム情報漏えい対策テンプレートのみです。事前定義されたテンプレートは変更できません。

データ識別子

[設定] → [情報漏えい対策] → [データ識別子] からキーワードとパターンの追加、削除、コピー、インポート、エクスポート、および表示を実行できます。

キーワードを追加するには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. [追加] をクリックして [キーワード] を選択します。
3. [名前] と [説明] を入力します。
4. 適切な条件を選択します。
5. [サブキーワード] セクションで [名前] と [説明] を入力します。
6. 必要に応じて [大文字 / 小文字の区別] を選択します。
7. [追加] をクリックします。
8. サブキーワードを追加する手順を繰り返します。[インポート] をクリックしてサブキーワードを追加することもできます。
9. サブキーワードを削除するには、キーワードを選択して [削除] または [すべて削除] をクリックします。
10. [保存して閉じる] をクリックします。

パターンを追加するには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. [追加] をクリックして [パターン] を選択します。
3. [名前] と [説明] を入力します。
4. 適切な [タイプ] を選択します。
5. [パターン] を入力して、[大文字 / 小文字の区別] をどちらにするか選択します。
6. [表示のパターン] と [例] を入力します。

7. 適切な [検証] を選択します。
8. [保存して閉じる] をクリックします。

キーワードまたはパターンをコピーするには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. 1 つ以上のキーワード / パターンを選択します。
3. [コピー] をクリックします。

キーワードまたはパターンをインポートするには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. [インポート] をクリックし、.dat ファイルを選択します。

キーワードまたはパターンをエクスポートするには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. ［エクスポート］をクリックします。

注意： エクスポート時にはすべてのキーワードとパターンが結合されます。

キーワードまたはパターンの [表示順] パラメータを設定するには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. [表示順] をクリックして、[識別子]、[パターン]、[キーワード] から適切なオプションを選択します。

情報漏えい対策テンプレートを表示するには

1. [設定] → [情報漏えい対策] → [データ識別子] をクリックします。
2. キーワードまたはパターンを 1 つ選択し、それをダブルクリックして開きます。

注意： 変更できるのはカスタム情報漏えい対策テンプレートのみです。事前定義されたテンプレートは変更できません。

情報漏えい対策フィルタの設定

ここでは、情報漏えい対策フィルタを設定するために必要な手順について説明します。

情報漏えい対策フィルタオプションを設定するには

1. [検索オプション] で、[情報漏えい対策フィルタ] タブをクリックします。
2. [情報漏えい対策フィルタを有効にする] チェックボックスをオンにします。
3. [情報漏えい対策フィルタ] セクションで、次のオプションを選択します。
   - 情報漏えい対策フィルタの作成
   - 既存の情報漏えい対策フィルタの追加
   - フィルタの削除
   - すべて削除
4. 情報漏えい対策 (DLP) フィルタを作成するには
   a. [情報漏えい対策フィルタ] で [情報漏えい対策フィルタの作成] をクリックします。情報漏えい対策フィルタの画面が表示されます。
   b. [フィルタ名] に、新規フィルタの名前を入力します。
   c. [件名]、[送信者]、[宛先]、[Cc]、[メール本文]、[添付ファイルの内容]、[添付ファイル名] から、確認したいメールの部分を含むチェックボックスを選択します。
   d. [情報漏えい対策テンプレートの選択] セクションで、既存のリストからテンプレートを選択し、>> をクリックして右側の [選択した情報漏えい対策テンプレートのいずれかに一致する] ウィンドウに追加します。さらにテンプレートを追加するには、この手順を繰り返します。
      - テンプレートのグループを指定して情報漏えい対策フィルタを作成するには、[追加] をクリックします。
      - 情報漏えい対策テンプレートを .dat 形式でインポートするには、[インポート] をクリックします。
5. [除外設定] セクションで、情報漏えい対策フィルタから除外するファイルの名前を入力します。
6. [処理] セクションで、[内容が不適切なメールへの処理] を選択して、検索処理を指定します。
7. [通知] セクションで、メッセージについての適切な通知とフィルタ処理のオプションを選択します。

   指示または説明を追加するには、通知にフィルタの説明を加えます。
   例 : 詳細については、Domino の管理者に確認してください。
8. [保存して閉じる] をクリックします。

スクリプトフィルタの設定

Notes のスクリプトをフィルタ処理する方法を定義するには、[スクリプトフィルタ] タブを使用します。

スクリプトフィルタオプションを設定するには

1. [検索オプション] → [スクリプトフィルタ] タブをクリックします。
2. [スクリプトフィルタを有効にする] チェックボックスをオンにします。
3. [文字列] セクションで、次のように、フィルタ処理する格納フォームおよびリッチテキストのホットスポットスクリプトを入力します。
   - [@ 関数文字列] には、式言語による有効な IBM Notes 関数を指定できます。例 :`prompt`
   - [@ コマンド文字列] には、式言語による有効な IBM Notes フォーマットのコマンドを指定できます。たとえば、次のようなポリシーを作成します。`[Execute]`、`[FileDatabaseDelete]`
   - [スクリプト文字列] には、OS の有効な LotusScript コマンドを指定できます。たとえば、次のようなポリシーを作成します。`shell`、`getobject`、`kill`、`rmdir`、`activate`
   - [@URLOPEN で呼び出される URL] では、式言語による有効な URLOPEN コマンドを開けます。
4. [処理] セクションで、必要に応じて、[検出時に処理を実行する場合は、該当するチェックボックスをオンにしてください。] で項目を選択します。
5.  をクリックして、[格納フォームのホットスポットおよびイベント] に対するフィルタ処理および [リッチテキストのホットスポット] に対する処理を設定します。

注意： リッチテキストのホットスポットに対する自動駆除処理により、不正な文字列を含んでいるコードセグメントが削除されます。その結果、ホットスポットを含んでいる文書全体が完全に隔離されるので、誤検出された文書を復元できます。[ホットスポットをポップアップメッセージに置換する] を選択すると、リッチテキストのホットスポットはポップアップメッセージで置き換えられます。

---

6. [通知] セクションで、ファイルがメッセージフィルタに一致したときの通知オプションを選択します。
7. [メールのスタンプ] セクションで、適切なメールスタンプの設定を定義します。
8. [保存して閉じる] をクリックします。

転送オプションの設定

承認を受けるためのメール転送先を設定するには、[転送オプション] タブを使用します。メッセージを配信してもよいかどうかは、指定された承認者が決定します。

転送オプションを設定するには

1. メール検索ルールで、[転送オプション] タブをクリックします。
2. [管理者] セクションの [検索済みメールを次のユーザに転送] で、  をクリックして承認者のメールアドレスを指定します。

注意： 管理者権限のあるアカウントでも、そのアカウントが InterScan データベースへのアクセスと役割で指定されていなければ、InterScan の機能にアクセスできません。

指定したアカウントに、InterScan データベースへの適切なアクセス権があることを確認してください。InterScan データベースへのアクセスを定義する方法の詳細については、77 ページの「InterScan データベースへのアクセスと役割の定義」を参照してください。

ヒント： 指定した承認者が対応可能かどうかを確認することをお勧めします。指定した承認者が対応できない場合は、メールの転送先として別のメールアドレスを設定します。

転送されてきたメッセージを承認するアカウントを 2 つ以上指定することもできます。1 人の承認者が不在の場合でも、他の指定アカウントで転送されてきたメッセージを処理できます。これによって、メッセージが紛失したり、失念されたりしないようになります。

---

3. [通知] セクションで、承認者がメッセージを拒否または承認したときの通知の件名を入力します。
4. [保存して閉じる] をクリックします。

検査証明 (ディスクレーマー) の挿入

メール検索通知に検査証明 (ディスクレーマー) を使用するために、実際の検査証明メッセージを定義するには、[検査証明] タブを使用します。

注意： InterScan では、Domino によるインターネットメールに検査証明を挿入できます。ただし、同一の検査証明名がある場合は、最初の検査証明のみが使用され、挿入されます。

ディスクレーマーを挿入するには

1. メール検索ルールで、[検査証明] タブをクリックします。
2. [検査証明 (ディスクレーマー) を有効にする] をオンにします。
3. [挿入する場所] を設定します。

   注意： フィルタ通知がメッセージに挿入される場合、本来はメッセージ本文の先頭に配置される検査証明は、フィルタ通知の後ろに配置されます。また、件名の検査証明は、メッセージの元の件名の後ろに挿入されます。

4. [名前] に、検査証明の名前を入力します。

   注意： 名前が同じ検査証明が追加されるのは 1 回のみです。

5. [件名] および [メッセージ本文] に、適切な指定情報を入力します。
6. [保存して閉じる] をクリックします。

ルール予約の設定

メール検索ルールまたはデータベース検索ルールの予約を設定するには、[検索スケジュール] タブを使用します。

予約を設定するには

1. 検索ルールで、[検索スケジュール] タブをクリックします。
2. 次の項目から、ルール予約を指定します。
   - 常時 — ルールが常時適用されます。
   - 指定 — 指定した日付、時刻、および時間帯の間、またはそれを除く時間帯に、ルールが適用されます。

3. [保存して閉じる] をクリックします。

手動検索の実行

ローカル Domino サーバ上のデータベース、またはローカルサーバに割り当てたドライブまたはディレクトリを持つリモートクライアントに対して、ウイルス検索を実行できます。

手動検索の実行方法には、次の 2 とおりがあります。

- Domino サーバコンソールの使用
- 設定データベースの使用

手動検索の起動方法の詳細については、以降のセクションを参照してください。

Domino サーバコンソールを使用した手動検索の実行

Notes データベースの検索は、Domino サーバコンソールから、または InterScan インタフェースを使用して手動で実行できます。

ローカルのハードディスクまたはマウントされたハードディスクにある Notes データベースは、ネットワークドライブも含めて、手動検索と予約検索の対象にすることができます。

データベースを Domino サーバコンソールから検索するには

次のコマンドを入力します。

load SMDdbs -manual { ディレクトリ名と database.nsf}

この {ディレクトリ名と `database.nsf`} は、検索するデータベースまたはディレクトリです。

指定したデータベース、または `notes.ini` の ***`Directory`*** セクションの下にある個々のディレクトリが検索されますが、設定データベースで使用可能な手動検索設定に従って検索されます。

ヒント： 複数のデータベースは、セミコロンで区切って指定します。たとえば、次のようなポリシーを作成します。

```
load SMDdbs -manual
database.nsf;database2.nsf;database3.nsf;folder/database4.nsf
```

設定データベースを使用した手動検索の実行

設定データベースを使用して、手動データベース検索を開始します。

今すぐ検索を実行するには

1. InterScan 設定データベースを開きます。
2. 左側のメニューで、[処理] → [手動検索] の順にクリックします。
3. 作業領域で、[編集] をクリックします。
4. [一般] タブをクリックします。
5. [増分検索] セクションで、[増分検索を有効にする] をオンにします。
6. [検索時間] セクションで、検索時間を分単位で指定します。

   注意： 検索時間を「0」に設定すると、すべてのデータベースの検索が終了するまで手動検索タスクが実行されます。

7. [検索するデータベース] タブをクリックして、次のように、検索するデータベースを設定します。
   - すべてのデータベース — Domino データディレクトリに格納されているデータベースをすべて検索します。サブディレクトリも対象となります。
   - 指定するデータベース — ディレクトリとデータベースのリストに基づいて、特定のデータベースを検索します。

     指定したディレクトリに含まれるフォルダも対象とする場合は、[サブディレクトリも含む] を選択します。
   - 検索から除外するデータベース — 指定したデータベースは検索しません。

     [追加]、[削除]、および [すべて削除] の各ボタンを使用して、リストにあるデータベースを操作します。
8. [検索オプション] タブをクリックして、必要に応じて検索オプションを設定します。
9. 通知テンプレートを定義します。

10. [今すぐ検索] をクリックします。

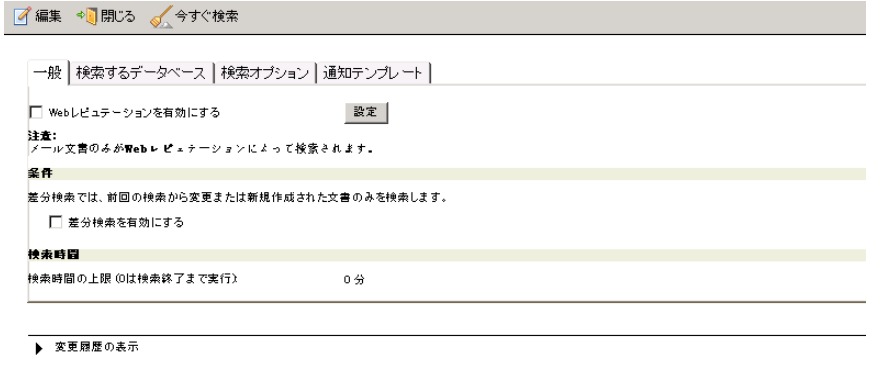


図 4-26. 今すぐ検索を実行する ID には、サーバコンソールコマンドを発行するための適切な権限が必要です。

11. [保存して閉じる] をクリックして、手動検索設定を保存します。

手動検索の手動による停止

自動的に終了する前に手動データベース検索を手動で停止する場合は、問題なく検索タスクが終了するように、Domino サーバコンソールで次のコマンドを発行します。

```
tell SMDdbs quit
```

現在の文書の検索が完了すると、検索が停止します。

第 5 章

管理の設定

[概要]、[サーバ設定]、[Control Manager エージェント設定]、および [管理] の各オプションには、設定データベースからアクセスできます。これらのオプションを使用すると、InterScan for IBM Domino (以下、InterScan) 5.6 サーバ情報を指定したり、InterScan データベースの管理容易性とパフォーマンスを最適化するための機能を設定したりできます。

第 5 章で説明する項目は次のとおりです。

すべてのサーバの概要の表示

設定データベースには、検索タスクのステータスの概要、および InterScan と OS に関する情報が含まれています。

すべてのサーバの概要を表示するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで [概要] をクリックします。

図 5-1.　[ステータス] 表示には、現在のサーバのステータスが表示されます。

3. 次のいずれかを実行します。
   - 使用可能なすべてのサーバの概要を表示するには、[すべてのサーバの概要を表示] をクリックします。
   - <F9> キーを押して、表示内容を更新します。

ヒント： お使いの環境で Trend Micro Control Manager (以下、Control Manager) を使用している場合は、管理コンソールから [製品ステータス] タブを選択して、InterScan のステータスを表示することもできます。

[サーバ設定] メニューオプションの指定

設定データベースの [サーバ設定] を使用し、Domino サーバまたは Domino サーバグループの次の設定を定義します。

- 検索中に一時ファイルを保存するために使用するディレクトリ
- 検索に使用するメモリサイズ
- コンポーネントのダウンロードと製品のアクティベーションに使用するプロキシサーバの設定
- Web レピュテーションの設定に使用されるローカルスマートスキャンソース
- InterScan イベントの種類と、それらのイベントを Domino サーバコンソールを使用して表示するかどうか
- InterScan タスクが異常終了した場合の管理者への通知
- InterScan がディスクレーマーに使用する文字セットを見つけられなかった場合に使用する初期設定の文字セット
- マルチスレッド検索、信頼するウイルス対策済みサーバ、警告用イメージ、メッセージルーティングなど、その他の設定

サーバ設定ルールの作成

サーバ設定ルールを作成するには、InterScan 設定データベースの [サーバ設定] メニューを使用します。

ヒント： サーバ設定ルールは、サーバまたはサーバグループごとに作成します。

サーバ設定ルールを作成するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[設定] → [サーバ設定] の順にクリックします。
3. 作業領域で、[サーバ設定の作成] をクリックします。
4. サーバ設定ルールの適用先のサーバまたはサーバグループを指定します。
5. 検索に使用するディレクトリを設定します (150 ページの「検索ディレクトリの設定」を参照)。
6. 検索に使用するメモリサイズを設定します (151 ページの「検索に使用するメモリサイズの設定」を参照)。

7. InterScan がコンポーネントのダウンロードや製品のアクティベーションに使用するプロキシサーバを設定します (152 ページの「プロキシサーバの設定」を参照)。
8. ローカルスマートスキャンソースを設定します (152 ページの「ローカルスマートスキャンソースの設定」を参照)。
9. InterScan が Domino サーバコンソールを介して通知をトリガするイベントを設定します (154 ページの「サーバイベントの監視」を参照)。
10. サーバタスクモニタを有効にします (155 ページの「サーバタスクモニタの有効化」を参照)。
11. InterScan がメッセージの文字セットを検出できないときに使用する、初期設定の文字セットを指定します (155 ページの「初期設定の文字セットの指定」を参照)。
12. その他の設定を行います (156 ページの「その他の設定」を参照)。
13. [保存して閉じる] をクリックします。

サーバ設定ルールの変更

サーバ設定ルールを変更するには、InterScan 設定データベースの [サーバ設定] メニューを使用します。

サーバ設定ルールを変更するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[設定] → [サーバ設定] の順にクリックします。
3. 作業領域で、「サーバ設定ルール」文書をダブルクリックするか、[編集] をクリックします。
4. 設定を変更します。
5. [保存して閉じる] をクリックします。

サーバ設定ルールの設定

サーバ設定ルールのプロパティを設定するには、[作業ディレクトリ]、[検索用メモリ]、[プロキシ設定]、[ローカルスマートスキャンソース]、[イベントログ]、[タスクモニタ]、[地域オプション]、および [その他] の各タブを使用します。

検索ディレクトリの設定

InterScan が検索中に一時ファイルを保存するために使用するディレクトリを設定するには、[作業ディレクトリ] タブを使用します。

作業ディレクトリを設定するには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[作業ディレクトリ] タブをクリックします。
3. Domino データディレクトリに関連付けるディレクトリを入力します。
4. [保存して閉じる] をクリックします。

検索に使用するメモリサイズの設定

InterScan がファイルを検索するために割り当てるメモリのサイズを設定するには、[検索用メモリ] タブを使用します。

メモリベースの検索に割り当てる適切なメモリを決定するには、次のガイドラインに従います。

- 環境内のほとんどのメッセージおよび文書の添付ファイルに十分なメモリ量を割り当てます。

  組織で受信する添付ファイルの 90% が 2MB 未満の場合、メモリベースの各検索タスクには 2MB のみを割り当てることができます。最適な結果を得られなくなるので、このサイズ指定にはメッセージサイズの平均は使用しないでください。
- 組織で、添付ファイルサイズの上限値を設定している場合は、その値を使用できます。
- 圧縮ファイルは、検索の前に解凍する必要があります。

  圧縮ファイルでなく、解凍後のファイルに適切なメモリ容量を割り当てます。
- Domino サーバですべての InterScan タスクによって使用されるメモリ量の合計を考慮します。

  たとえば、それぞれ 5MB のメモリが必要な SMDreal タスクを 3 つ実行している場合、InterScan で 15MB のメモリを使用していることになります。予約検索 (SMDdbs) の実行時には、これを実行するためのメモリも、メモリ量の合計に追加する必要があります。
- Domino サーバのメモリのサイズと利用状況を確認します。メモリの利用状況を判別する方法の詳細については、Domino のドキュメントを参照してください。

  メモリに余裕がない環境では、メモリベースの検索によるパフォーマンスの向上よりも、InterScan にメモリを割り当てたことによるパフォーマンスの低下の方が大きくなります。

ほとんどの組織では、InterScan タスクごとに初期設定値の 5MB の割り当てが適しています。

検索用メモリのサイズを設定するには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[検索用メモリ] タブをクリックします。
3. 検索の種類ごとに、メモリサイズを示す数字を MB 単位で入力します。

4. [保存して閉じる] をクリックします。

プロキシサーバの設定

Web レピュテーション、Control Manager エージェント、コンポーネントのダウンロード、および製品のアクティベーションに使用するプロキシサーバを設定するには、[プロキシ設定] タブを使用します。

注意： Control Manager エージェント用、または「予約アップデート」文書または「手動アップデート」文書でのコンポーネントのダウンロード用に、初期設定以外のプロキシサーバを指定できます。174 ページの「コンポーネントダウンロード用プロキシサーバの設定」を参照してください。

プロキシサーバを設定するには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[プロキシ設定] タブをクリックします。
3. [プロキシサーバを使用する] を選択します。
4. プロキシサーバのプロトコル (HTTP、Socks4、Socks5、HTTPS など) を選択します。
5. プロキシサーバの [アドレス] またはホスト名を入力します。
6. プロキシサーバの [ポート] 番号を入力します。
7. プロキシ認証に使用する [ユーザ名] と [パスワード] を入力します。
8. [保存して閉じる] をクリックします。

ローカルスマートスキャンソースの設定

[ローカルスマートスキャンソース] タブを使用して、Web レピュテーションに使用するローカルのスマートスキャンソースを設定します。

ローカル Smart Protection Server のフィルタオプションを追加するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. [追加] をクリックして、次のいずれかを実行します。
   - [サーバの名前またはアドレス] フィールドにローカル Web レピュテーションサーバの名前または IP アドレスを入力します。

- [Web レピュテーションサービスのポート] フィールドにサーバポートを入力します (デフォルトポートは 5274)。

4. [保存して閉じる] をクリックします。

ローカル Smart Protection Server のオプションを編集するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. [Smart Protection Server リスト] で使用可能なサーバのいずれかをダブルクリックします。
   - [サーバの名前またはアドレス] フィールドで、ローカル Web レピュテーションサーバの名前または IP アドレスを変更します。
   - [Web レピュテーションサービスのポート] フィールドのサーバポートを変更します (デフォルトポートは 5274)。
4. [保存して閉じる] をクリックします。

ローカル Smart Protection Server のオプションを削除するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. [削除] をクリックしてサーバを選択し、[OK] をクリックします。
4. [保存して閉じる] をクリックします。

ローカル Web レピュテーションサーバの優先度オプションを変更するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. 変更するサーバ優先度を選択して、[トップに移動] をクリックします。
4. [保存して閉じる] をクリックします。

通知メールを設定するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. [受信者] フィールドで管理ユーザの名前を入力または選択します。
4. [Web レピュテーションサービスが次の場合に通知を送信する :] で次のいずれかを選択します。
   - **使用不可**
   - **使用可能**
5. デフォルトの [件名] を使用するか、必要に応じてカスタマイズします。

6. [保存して閉じる] をクリックします。

プロキシサーバを設定するには

1. [サーバ設定] をクリックし、サーバ設定オプションを開きます。
2. [ローカルスマートスキャンソース] タブをクリックします。
3. 次のいずれかを選択します。
   - **プロキシサーバを使用しない**
   - **サーバ設定のプロキシサーバを使用する**
   - **次のプロキシサーバ設定を使用する**
4. [次のプロキシサーバ設定を使用する] を選択した場合は、次を実行します。
   - プロキシサーバプロトコルを選択します (HTTP、Socks4、または Socks5)。
   - プロキシサーバの [アドレス] または [ホスト名]、および使用する [ポート] を入力します。
   - 必要に応じてプロキシ認証用のユーザ名とパスワードを入力します。
5. [保存して閉じる] をクリックします。

注意： ローカル Web レピュテーションは HTTPS プロトコルのプロキシサーバをサポートしていません。

サーバイベントの監視

次のイベントを監視して Domino サーバコンソールに表示、または書き出すには、[イベントログ] タブを使用します。

- **ウイルス検出** — InterScan がウイルスなどの不正プログラムを検出した場合の情報を提供します。
- **新しい設定の適用** — InterScan が自身のデータベースに新しい設定を適用した場合の情報を提供します。
- **新しいコンポーネントのダウンロード** — InterScan がウイルス対策コンポーネントまたはコンテンツセキュリティコンポーネントをダウンロードした場合の情報を提供します。
- **新しいコンポーネントの適用** — InterScan がコンポーネントを適用または配信した場合の情報を提供します。

サーバイベントを監視するには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[イベントログ] タブをクリックします。
3. InterScan で監視するイベント、および Domino サーバコンソールにログを表示するかどうかを選択します。
4. [保存して閉じる] をクリックします。

サーバタスクモニタの有効化

タスクが異常終了した場合に InterScan から管理者に通知を送信するかどうかを定義するには、[タスクモニタ] タブを使用します。

サーバタスクモニタを有効にするには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[タスクモニタ] タブをクリックします。
3. [タスクが異常終了した場合に管理者に通知を送信する] を選択します。
4. [管理者] で、入力するか  をクリックして、通知を受信する管理者を指定します。
5. [件名] および [本文] に、通知メッセージに関する適切な情報を入力します。
6. [保存して閉じる] をクリックします。

初期設定の文字セットの指定

InterScan がディスクレーマー用の文字セットを検出できないときに使用する初期設定の文字セットを指定するには、[地域オプション] タブを使用します。

検査証明 (ディスクレーマー) を挿入するには、143 ページの「検査証明 (ディスクレーマー) の挿入」を参照してください。

初期設定の文字セットを指定するには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[地域オプション] タブをクリックします。
3. リストから、適切な [初期設定の文字セット] を選択します。

4. [保存して閉じる] をクリックします。

その他の設定

マルチスレッド検索、信頼するウイルス対策済みサーバ、警告用イメージ、およびメールルーティングを設定するには、[その他] タブを使用します。

その他の設定を行うには

1. サーバ設定ルールを作成 (149 ページの「サーバ設定ルールの作成」を参照) または変更 (150 ページの「サーバ設定ルールの変更」を参照) します。
2. 作業領域で、[その他] タブをクリックします。
3. [マルチスレッド検索] セクションで、次のようにメール検索およびデータベース検索に使用するマルチスレッドの数を整数で入力します。
   - リアルタイムメール検索のスレッド数
   - リアルタイムデータベース検索のスレッド数
   - 手動データベース検索のスレッド数

   ヒント： 検索ごとの値を 1 から 20 までの値に設定します。リアルタイムメール検索とリアルタイムデータベース検索の合計スレッド数を 20 未満に設定する必要があります。

   検索ごとのスレッド数を 5 に設定することをお勧めします。

4. [信頼するウイルス対策済みサーバ] セクションで次の設定を行います。
   - **SMTP サーバ** — SMTP サーバの IP アドレスまたはサーバ名を入力します。
   - **Domino サーバ** — サーバ名を入力するか、  をクリックしてメニューから選択します。

   注意： 他の Domino サーバがウイルスなどの不正プログラムに感染することを防止するために、信頼するサーバでウイルス対策およびコンテンツセキュリティ保護が行われていることを確認します。

   警告： **添付ファイルが削除された場合は、警告のビットマップは表示されません。**

5. InterScan リアルタイムタスクが実行されていない場合にメールの配信を無効にするには、[メール検索] セクションで、[メール検索タスク (SMDreal) が実行されていない場合はメールを配信しない] を選択します。

   ヒント： このオプションは有効にすることをお勧めします。次の警告および注意の情報を参照してください。

   警告： **このオプションは、初期設定で InterScan セットアッププログラムによって有効になります。InterScan タスクのロードに失敗した場合や SMDreal が誤ってアンロードされた場合でも、Domino サーバはメッセージを配信し続けます。検索されていないメッセージに、大規模感染につながるウイルスやその他の脅威が含まれる可能性があります。**

   注意： [メール検索タスク (SMDreal) が実行されていない場合はメールを配信しない] が無効になっていて、SMDreal がまだロードされていない場合、検索されていないメッセージが Domino ルータによって配信されます。これによってウイルスやその他の脅威の大規模感染が発生する可能性があります。

6. [タスクの除外] で、リアルタイムデータベース検索から除外する Domino タスク名を入力します。たとえば、次のようなポリシーを作成します。`compact; fixup; updall; update`

   ヒント： このオプションは、検索パフォーマンスの向上に役立ちます。

7. [保存して閉じる] をクリックします。

Control Manager エージェントの設定

以前のバージョンの InterScan および Control Manager で使用されていた Trend Micro Management Infrastructure (TMI) プロトコルが InterScan でサポートされなくなったため、InterScan と Control Manager 間の通信では新しいプロトコルが使用されます。InterScan のインストールの完了後、Control Manager エージェントを登録できます。次に、Control Manager エージェントを設定する方法を説明します。

注意： Control Manager エージェントは、インストールプロセス中に自動的にインストールされます。

Control Manager エージェント設定を作成または変更するには

1. 左側のメニューから、[設定] → [Control Manager エージェント設定] の順に選択します。
2. 作業領域で、[Control Manager エージェント設定の作成] をクリックします。

   注意： 既存の設定を変更するには、[Control Manager エージェント設定] 画面で、変更する設定をダブルクリックして、[編集] をクリックします。

3. [適用先サーバ] にサーバ名を入力するか、  をクリックして選択します。
4. [Control Manager の設定] セクションで、[Control Manager サーバに InterScan for IBM Domino を登録する] をオンにします。
5. [Control Manager サーバ] セクションで、[サーバアドレス] および [ポート] 番号を該当するフィールドに入力します。
6. Web 認証を使用する場合は、[Web サーバ認証] セクションで、[ユーザ名] および [パスワード] を入力します。
7. プロキシサーバを使用する場合は、[プロキシ設定] セクションで、[Control Manager サーバへの接続にプロキシサーバを使用する] をオンにして、次のオプションから選択します。
   a. [サーバ設定のプロキシサーバを使用する] を選択すると、サーバ設定に指定されているプロキシサーバが使用されます。
   b. [別のプロキシサーバを使用する] を選択した場合は、次のように、サーバ設定で指定されているものとは別のプロキシサーバを指定します。
      - プロキシサーバのプロトコル (HTTP、Socks4、Socks5、HTTPS など) を選択します。
      - プロキシサーバの [アドレス] またはホスト名を入力します。
      - プロキシサーバの [ポート] 番号を入力します。
      - プロキシ認証に使用する [ユーザ名] と [パスワード] を入力します。

8. [保存して閉じる] をクリックします。

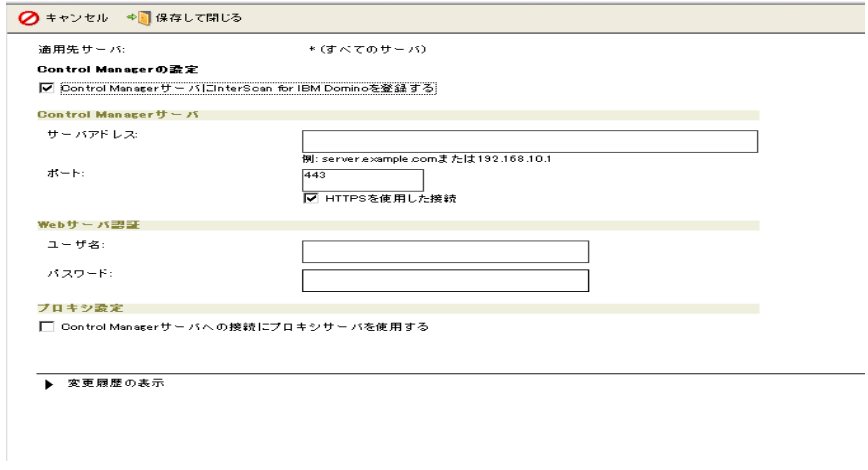


図 5-2. [Control Manager エージェント設定] 画面

Deep Discovery Advisor の設定

InterScan と Deep Discovery Advisor との通信には、標準 HTTPS プロトコルと認証用の API キーが使用されます。ここでは、InterScan で Deep Discovery Advisor を設定する方法について説明します。

Deep Discovery Advisor を設定するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[設定] → [Deep Discovery Advisor の設定] の順にクリックします。
3. 作業領域で、[Deep Discovery Advisor の作成] をクリックします。

注意： 既存の設定を変更するには、[Deep Discovery Advisor の設定] 画面で、変更する設定をダブルクリックして、[編集] をクリックします。

---

4. [適用先サーバ] にサーバ名を入力するか、 をクリックして選択します。
5. [InterScan for IBM Domino を Deep Discovery Advisor に登録する] を選択します。

6. [Deep Discovery Advisor] セクションで、適切なフィールドにサーバアドレス、ポート番号、および API キーを入力します。

   注意： Deep Discovery Advisor の API キーがわからない場合は、Deep Discovery Advisor 管理者に問い合わせて API キーを取得してください。

7. [通知] セクションの [Deep Discovery Advisor が次の場合に通知を送信する] でいずれかを選択します。
   - **使用不可**
   - **使用可能**

   デフォルトの [件名] を使用するか、必要に応じてカスタマイズします。
8. プロキシサーバを使用する場合は、[プロキシ設定] セクションで [Deep Discovery Advisor への接続にプロキシサーバを使用する] を選択し、次のいずれかを選択します。
   - **サーバ設定のプロキシサーバを使用する**
   - **別のプロキシサーバを使用する**

     [別のプロキシサーバを使用する] を選択した場合は、次を実行します。
     - プロキシサーバプロトコルを選択します (HTTP、Socks4、Socks5、または HTTPS)。
     - プロキシサーバの [アドレス] またはホスト名、および使用する [ポート] を入力します。
     - 必要に応じてプロキシ認証用のユーザ名とパスワードを入力します。
9. [保存して閉じる] をクリックします。

フィルタリストの管理

InterScan 5.6 では、フィルタリストデータベース (smlists.nsf) にフィルタリストが保存されます。リストには、迷惑メール対策ツールの承認する送信者とブロックする送信者のリスト、および Web レピュテーションの承認する URL のリストが含まれます。ここでは、データベースでのフィルタリストの管理方法について説明します。

フィルタリストを管理するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[フィルタリストデータベース] をクリックしてフィルタリストデータベースを開きます。

3. [Web レピュテーションの承認する URL]、[迷惑メール対策ツールのブロックする送信者]、または [迷惑メール対策ツールの承認する送信者] をクリックします。

図 5-3.　Web レピュテーションの URL の管理

4. 次のいずれかを実行します。
   - 承認する URL を追加するには、[追加] をクリックします。
   - 承認する URL を削除するには、[削除] をクリックします。
   - 承認する URL をインポートするには、[インポート] をクリックします。
   - 承認する URL をエクスポートするには、[エクスポート] をクリックします。

注意： [迷惑メール対策ツールのブロックする送信者] または [迷惑メール対策ツールの承認する送信者] をクリックした場合は、[追加] ボタンと [削除] ボタンだけが有効になります。

管理メニューオプションの設定

ライセンスプロファイルの作成やアクセス制御リストの新しいエントリの適用など、InterScan データベースの追加プロパティを定義するには、設定データベースの [管理] メニューを使用します。

InterScan データベースへの Notes データベースプロパティの適用

[管理] → [データベース設定] の順に選択して設定するオプションには、データベースプロパティへのショートカットが用意されています。

設定データベースを使用して、次のプロパティを InterScan データベースに設定して適用できます。

- [データベースを開く] ダイアログへの表示

  [データベースを開く] ダイアログに表示されるデータベースリストに InterScan データベースを追加するには、このオプションを有効にします。そこから除外するには、このオプションを無効にします。

- データベースカタログへの表示

  Notes データベースカタログ検索に InterScan データベースを追加するには、このオプションを有効にします。そこから除外するには、このオプションを無効にします。

- SSL による Web アクセス

  Notes R8 以降では、安全な通信を確保するために SSL (Secure Socket Layer) 2.0 以降がサポートされています。Web 経由で SSL を使用して InterScan データベースにアクセスできるようにするには、[データベースのプロパティ] ダイアログを使用する代わりに、設定データベースを使用してこのオプションを有効にします。

- 複製

  InterScan データベースを他のサーバに複製できるようにするには、このオプションを選択します。

Notes データベースプロパティを InterScan データベースに設定、適用するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[管理] → [データベース設定] の順にクリックします。
3. 作業領域で、Domino サーバを入力するか、  をクリックして選択します。
4. それぞれの InterScan データベースのプロパティを [有効]、[無効]、または [変更なし] に設定します。
5. [設定の適用] をクリックします。

注意： 設定データベースの設定によって、前回保存した設定が上書きされます。

アクセス制御リスト (ACL) のエントリの新規作成と適用

Domino サーバ上で InterScan データベースのアクセス制御を作成、適用するには、設定データベースを使用します。

アクセス制御リストのエントリを新規作成し、適用するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[管理] → [アクセス管理] の順にクリックします。
3. 作業領域で、[新規エントリの作成] をクリックします。
4. Domino サーバまたは Domino サーバグループに対するアクセス制御リストのエントリを入力するか、  をクリックして指定します。
5. リストからユーザタイプを選択します。
6. InterScan データベースを選択し、権限を設定します。
7. [詳細] をクリックし、リストからアクセスレベルを選択し、パブリック文書の表示または作成を有効にします。
8. [保存して閉じる] をクリックし、[アクセス制御リストへの適用] をクリックします。

Domino Administrator からのタスクの表示

Domino Administrator から InterScan タスクを表示できるようにするには、設定データベースを使用します。

Domino Administrator からタスクを表示できるようにするには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[管理] → [Domino Administrator] の順にクリックします。
3. 作業領域で、[domadmin.nsf にコピー] をクリックします。

ライセンスプロファイルの作成

ライセンスプロファイルを作成して、InterScan 製品版のアクティベーションまたはサポート契約の更新作業を完了させるには、設定データベースを使用します。

ライセンスプロファイルを作成するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. [管理] → [製品ライセンス] の順にクリックします。
3. 作業領域で、[ライセンスプロファイルの作成] をクリックします。
4. 表示されたフィールドに、71 ページの「InterScan の登録とアクティベーション」を入力します。
5. [保存して閉じる] をクリックします。

ライセンスプロファイルの削除

古いまたは期限切れの InterScan バージョンのライセンスプロファイルを削除するには、設定データベースを使用します。

注意： 体験版を製品版にアップグレードするには、まず新しいライセンスプロファイルを作成し、次に古いプロファイルを削除します。

ライセンスプロファイルを削除するには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. [管理] → [製品ライセンス] の順にクリックします。
3. 作業領域で、削除するライセンスプロファイルを選択します。
4. [ライセンスプロファイルの削除] をクリックします。

プロファイルを削除するかどうかを確認するメッセージが表示されます。 [OK] をクリックし、ライセンスプロファイル表示に戻ります。

ヒント： プロファイルを誤って削除した場合、削除されたプロファイルのアクティベーションコードを使用して新しいプロファイルを作成してください。

第 6 章

アップデート

InterScan for IBM Domino (以下、InterScan) 5.6 では、ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントを、自動または手動でアップデートできます。

第 6 章で説明する項目は次のとおりです。

ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントの概要

次の InterScan のウイルス対策コンポーネントとコンテンツセキュリティコンポーネントは、推奨されるアップデートの頻度が高い順に示されています。

- **ウイルスパターンファイル** — 不正なプログラムによるファイルの感染を検出して駆除します。

  特に大きな損害を与える不正プログラムによる感染が広がっていることが判明した場合、トレンドマイクロはその不正プログラムの検出ルーチンを発見次第、ただちに新しいパターンファイルを公開します (通常は数時間以内)。
  新しいウイルスが発見されると、トレンドマイクロではそのパターンを解析し、情報をパターンファイルに組み込みます。感染力の高い新しいウイルスは毎日のように発見されるため、トレンドマイクロでは必要性や脅威のリスクに応じて頻繁にウイルスパターンファイルの新しいバージョンをリリースしています。
- **スパイウェアパターンファイル** — 個人情報を密かに収集する隠しプログラムを検出します。
- **IntelliTrap パターンファイル** — リアルタイム圧縮のアルゴリズムを使用してウイルスフィルタを回避しようとするウイルスを検出します。IntelliTrap は、メールの添付ファイルとして着信するリアルタイム圧縮された実行可能ファイルをブロックし、他の不正プログラムの特性とこれらのファイルを照合することによって、ユーザのネットワークにウイルスが侵入するリスクを軽減します。
- **IntelliTrap 除外パターンファイル** — IntelliTrap パターンファイルに追加した除外設定の適用対象を検出します。
- **ウイルス検索エンジン** — 活動しているウイルスと不正プログラムをすべて検出します。
- **スパムメール検索エンジン** — 一方的に送られてくる広告メール (UCE) または大量のメール (UBE) を検出します。
- **スパムメール判定ルール** — スパム定義が収められているアップデート可能ファイルに基づいて迷惑メールを検出します。

  32/64 ビットマルチスレッド検索エンジンおよびパターンマッチングと呼ばれる処理を使用して、ファイルがリアルタイムでチェックされます。また、ウイルス検索エンジンでは、数多くのヒューリスティック検索テクノロジが採用されているため、未確認の新しいウイルスも検出することができます。変種 / 亜種のマクロウイルス、Nimda、CodeRed などのマスメーリング型ウイルス、マクロウイルス、ポリモーフィック型 (ミューテーション型) ウイルス、トロイの木馬、DDos 攻撃などもすばやく識別します。
- **URL フィルタエンジン** — メールに含まれる危険な URL や迷惑な URL を検出します。

ウイルス検索エンジンには、ディスク容量を節約できるように、古いウイルスパターンファイルを自動的に削除する機能があります。また、パターンファイルの増分アップデート機能もあり、帯域幅の消費の抑制に役立ちます。

- **高度な脅威検索エンジン** — 文書の悪用を含め、従来とは異なる脅威がないかどうかファイルを確認します。
- **InterScan アプリケーション** — Service Pack リリースなど、製品固有のコンポーネントです。

ヒント： ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントをアップデートして、最新のウイルスと不正プログラムの脅威に対する保護を維持することをお勧めします。

ただし、コンポーネントをアップデートできるのは、登録済みのユーザのみです。詳細については、71 ページの「InterScan の登録とアクティベーション」を参照してください。

コンポーネントのアップデート

InterScan のコンポーネントは、次の 2 つの方法でアップデートできます。

- 手動
- 自動

コンポーネントの手動アップデート

手動アップデートを実行するには、設定データベースの [アップデート] を使用します。

コンポーネントを手動でアップデートするには

1. InterScan 設定データベースを開きます (78 ページの「InterScan データベースへのアクセス」を参照)。
2. 左側のメニューで、[処理] → [手動アップデート] の順にクリックします。
3. 作業領域で、[編集] をクリックします。
4. [コンポーネント] セクションで、アップデートするコンポーネントをオンにします (複数可)。
5. [オプション] セクションの [適用方法] および [プラットフォーム] で、適切なオプションを選択します。

6. [ダウンロード元] タブをクリックします。
7. [ダウンロード元] セクションで、適切なオプションを選択します。
8. [プロキシ設定] タブをクリックします。
9. [プロキシ設定] セクションで、コンポーネントのダウンロードに使用するプロキシサーバ設定を指定します。
10. [通知] タブをクリックします。
11. [管理者への通知] セクションで、必要に応じて通知設定を定義します。
12. [保存] をクリックして、手動アップデート設定を保存します。
13. [アップデート] をクリックします。

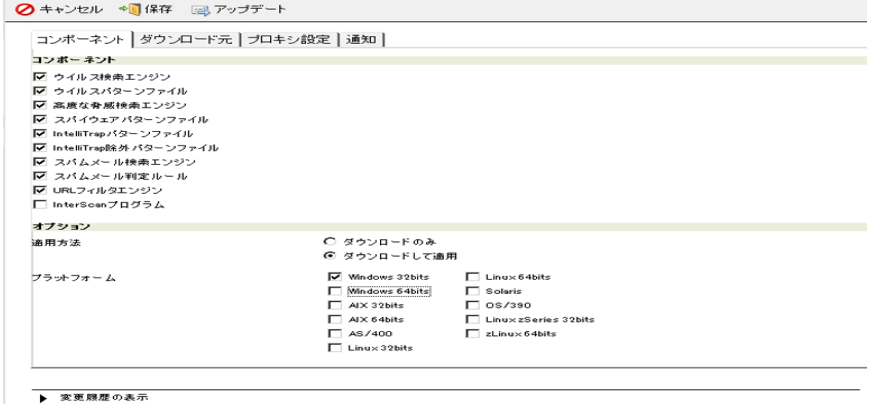


図 6-1. **[アップデート] をクリックして、最新のウイルス対策コンポーネントとコンテンツセキュリティコンポーネントをダウンロードします。**

予約アップデートルールを使用したコンポーネントの自動アップデート

コンポーネントを自動的にアップデートするには、予約アップデートルールを作成します。予約アップデートルールにより、特定の時刻に最新のコンポーネントをダウンロードする方法を定義します。

コンポーネントを自動的にアップデートするには

1. ポリシーを作成 (83 ページの「ポリシーの作成」を参照) または変更 (85 ページの「ポリシーの変更」を参照) します。
2. [設定] → [ポリシー] → [編集] / [新規ポリシーの作成] → [予約アップデート] タブをクリックします。
3. [予約アップデートを有効にする] をオンにします。
4. 自動配信するコンポーネントを設定します (170 ページの「特定のコンポーネントの自動配信」を参照)。
5. [新規ルールの作成] をクリックします。
6. [新規予約アップデートルール] 文書の [一般] タブで、一般的な設定を指定します。
   - [ルール識別子] セクションで、[名前] に予約アップデートの名前を指定します。
   - [適用] セクションで、[上位ポリシーのすべてのサーバ] または [指定するサーバ] を選択して をクリックし、リストからサーバを選択します。
7. [コンポーネント] タブをクリックします。
8. [コンポーネント] セクションで、アップデートするコンポーネントをオンにします。

図 6-2. 予約アップデートルールの作成とアップデートするコンポーネントの指定

9. [ダウンロード元] タブをクリックします。

10. [ダウンロード元] セクションで、適切なオプションを選択します (172 ページの「ダウンロード元の設定」を参照)。
11. [プロキシ設定] タブをクリックします。
12. [プロキシ設定] セクションで、コンポーネントのダウンロードに使用するプロキシサーバ設定をします (174 ページの「コンポーネントダウンロード用プロキシサーバの設定」を参照)。
13. [通知] タブをクリックします。
14. [管理者への通知] セクションで、必要に応じて通知設定を定義します (182 ページの「アップデート通知の設定」を参照)。

> **注意：** 予約アップデートルールの通知は、[通知] タブでポリシーに設定されたメールアドレスに送信されます。

15. [アップデートスケジュール] タブをクリックして、予約アップデートを実行する [実行時刻]、[実行間隔]、および [曜日] を設定します。
16. 作業領域の [予約複製] をクリックして Notes のアドレス帳を起動し、予約複製を設定します (Notes のヘルプの [複製] ページを使用するを参照してください)。
17. [保存して閉じる] をクリックします。スケジュールに基づいてコンポーネントがアップデートされます。

特定のコンポーネントの自動配信

ダウンロード元とダウンロードオプションによっては、最新のコンポーネントをすべて自動的に配信できます。特定のコンポーネントのみを配信するように設定するには、[コンポーネント配信を有効にする] を選択して、配信するコンポーネントを指定します (複数指定可)。InterScan では、最新のコンポーネントが次のようにダウンロードされ、配信されます。

1. ダウンロード元に利用可能な最新コンポーネントがあるかどうか確認します。
2. 利用可能な最新コンポーネントがあれば、アップデートデータベースにダウンロードします。
3. アップデートデータベースから最新コンポーネントを [適用先サーバ] の [一般] 設定で指定されているサーバに配信します。

特定のコンポーネントを自動的に配信するには

1. ポリシーを作成 (83 ページの「ポリシーの作成」を参照) または変更 (85 ページの「ポリシーの変更」を参照) します。
2. [設定] → [ポリシー] → [編集] / [新規ポリシーの作成] → [予約アップデート] タブをクリックします。

3. [コンポーネント配信を有効にする] を選択して、[設定] をクリックします。
4. [コンポーネントの配信設定] 画面の [コンポーネントの配信] セクションで、自動的に配信するコンポーネントを選択します。
5. [オプション] セクションで、[パターンファイル履歴の保持 : [x] パターンファイル] および [検索エンジン履歴の保持 : [x] 検索エンジン] に、InterScan で保存しておくパターンファイル数および検索エンジン数を示す値を入力します。

   注意 : ウイルスパターンファイルと検索エンジンファイルは、かなりのディスク容量を占めることがあるので、最新バージョンのほかに保存しておく旧バージョンの数は、ウイルスパターンファイルで 3 つ前まで、検索エンジンファイルで 2 つ前までとすることをお勧めします。ウイルスパターンファイルまたは検索エンジンファイルがアップデートされると、古いコンポーネントから順に削除されます。

6. [OK] をクリックして、画面を閉じます。
7. [保存して閉じる] をクリックして、配信設定を適用します。

アップデート設定

アップデート設定には、次の項目があります。

- アップデートするコンポーネント
- ダウンロード元
- コンポーネントダウンロード用のプロキシサーバ

アップデートするコンポーネントの選択

アップデートするコンポーネントを選択するには、[コンポーネント] タブを使用します。

ダウンロードするコンポーネントを選択するには

1. 「予約アップデートルール」文書または「手動アップデート」文書で、[コンポーネント] タブをクリックして、ダウンロードするコンポーネントを選択します (167 ページの「自動」または 167 ページの「手動」を参照)。
2. [コンポーネント] セクションで、ダウンロードするコンポーネントをオンにします。
3. [オプション] セクションで、パターンファイル履歴の保持 : [x] パターンファイルおよび検索エンジン履歴の保持 : [x] 検索エンジンに、InterScan で保存しておくファイル数を示す値を入力します。

注意： ウイルスパターンファイルと検索エンジンファイルは、かなりのディスク容量を占めることがあるので、最新バージョンのほかに保存しておく旧バージョンの数は、ウイルスパターンファイルで 3 つ前まで、検索エンジンファイルで 2 つ前までとすることをお勧めします。ウイルスパターンファイルまたは検索エンジンファイルがアップデートされると、古いコンポーネントから順に削除されます。

4. [適用方法] で、プログラムのアップデートを適用する方法として [ダウンロードのみ] または [ダウンロードして適用] を選択します。

ヒント： この 2 つのオプションを交互に適用する際は、注意が必要です。[ダウンロードのみ] オプションを使用してからアップデートを実行する場合、最新コンポーネントはアップデートデータベースにダウンロードされます。次に設定を [ダウンロードして適用] に変更すると、アップデートデータベースにあるコンポーネントがすでに最新のため、コンポーネントはダウンロードされません。これによって、[適用先サーバ] の [一般] 設定で指定されているサーバに最新コンポーネントが適用されなくなります。この場合、[ダウンロード元] に [複製データベース] を使用して、最新コンポーネントをその他のサーバに適用します。

5. [プラットフォーム] から適切なオプションを選択します。
6. [保存して閉じる] をクリックします。

ダウンロード元の設定

ダウンロードするコンポーネントを設定するには、[ダウンロード元] タブを使用します。

ダウンロード元を設定するには

1. 「予約アップデートルール」文書または「手動アップデート」文書で、[ダウンロード元] タブをクリックして、次のいずれかのダウンロード元を選択します (167 ページの「自動」または 167 ページの「手動」を参照)。
   - **複製データベース** — InterScan サーバにより、新しいパターンファイルが InterScan の中央サーバから自動的に pull 複製されます。

     このモデルでは、ハブサーバとなる InterScan サーバが新しいアップデートをダウンロードし、スポークの InterScan サーバすべてが中央のハブサーバからそれを自動的にプルして取得します。

[ダウンロードのみ] が設定されている場合でも、コンポーネントはスポークサーバに配信 (適用) されます。

注意： IBM Domino では、アップデートデータベースは自動的に複製されません。接続文書を Domino ディレクトリに作成して、複製方向と中央サーバを指定します。中央サーバは、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。

- **トレンドマイクロのアップデートサーバ** — InterScan サーバにより、最新のコンポーネントがトレンドマイクロのアップデートサーバから自動的にダウンロードされます。

注意： InterScan の初期設定では、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードする場合は常に、デジタル署名の確認が実行されます。署名ファイル (`*.sig`) によって、トレンドマイクロのアップデートサーバからのコンポーネントのダウンロードが安全であることが確認されます。

コンポーネントをアップデートするには、トレンドマイクロのアップデートサーバを使用するのが最も簡単です。マルチサーバ環境では、各 InterScan サーバが個別にトレンドマイクロのアップデートサーバをポーリングし、コンポーネントのアップデートがないか確認するように設定できます。または、1 台の InterScan サーバをアップデートをダウンロードするためのハブサーバとして指定し、スポークの InterScan サーバでは複製機能を使用してアップデートをプルして取得することもできます。

ヒント： アップデートに関する問題のトラブルシューティングについては、227 ページの「アップデートに関する問題」を参照してください。

- その他のインターネット上のサーバ — InterScan サーバは、ウイルスパターンファイルと検索エンジンをトレンドマイクロの Web サイト以外のサーバからダウンロードできます。たとえば、ローカルイントラネットの Web サイトからダウンロードできます。

  [アドレス] に、独自の「アップデートサーバ」の URL または UNC パスを入力します。

注意： UNC で指定するアップデート元は、InterScan for IBM Domino Windows 版のみに適用されます。その他のアップデートサーバからアップデートするには、最新コンポーネントを配置する場所に、対応する署名ファイル (`*.sig`) を保存しておく必要があります。`*.sig` ファイルがないと、アップデートに失敗します。

---

2. [保存して閉じる] をクリックします。

コンポーネントダウンロード用プロキシサーバの設定

InterScan サーバでインターネットへのアクセスにプロキシサーバが必要な場合は、[プロキシ設定] タブを使用します。

プロキシサーバを設定するには

1. 「予約アップデートルール」文書または「手動アップデート」文書で、[プロキシ設定] タブをクリックします。
2. インターネットへの接続にプロキシサーバが必要な場合は、[プロキシ設定] セクションで [プロキシサーバを使用する] を選択します。
3. [サーバ設定のプロキシサーバを使用する] か、[別のプロキシサーバを使用する] かを選択します。
4. 別のプロキシサーバを使用する場合、プロキシサーバの [プロトコル] を選択し、次の項目を指定します。
   a. プロキシサーバの [アドレス] またはホスト名、および使用する [ポート] を指定します。
   b. プロキシ認証に使用する [ユーザ名] と [パスワード] を入力します。
5. [保存して閉じる] をクリックします。

第 7 章

通知

InterScan for IBM Domino (以下、InterScan) 5.6 では、メール、添付ファイル、または文書中にウイルスまたは脅威となるその他の感染が検出されたとき、メールまたは IBM Instant Messaging and Web Conferencing を介して、指定された宛先に自動的に警告を送信できます。たとえば、Domino 管理者、感染ファイルが検出されたことの通知を必要とする担当者、メールの送信者、または受信者が通知先となります。

第 7 章で説明する項目は次のとおりです。

InterScan 通知の概要

メッセージまたはデータベースに不正なプログラムが検出されたとき、Domino 管理者、組織内外の送信者または受信者、データベース所有者、その他のインターネットメールアドレスやアドレス帳のメンバーなど、指定した宛先に自動的に通知を送信できます。

注意： スパムの問題につながる可能性があるため、外部送信者への通知を使用する場合は注意が必要です。

InterScan には次の通知カテゴリがあります。

- 検索通知は、メッセージまたはデータベースからメール検索、データベース検索、または予約検索ルールがトリガされるたびに送信されます。
- アップデート通知は、InterScan が予約アップデートを実行したとき、またはユーザが手動アップデートを実行したときに送信されます。
- Web レピュテーションサーバのステータス通知

InterScan は管理者、送信者、または受信者に通知を個別に送信します。Domino から元のメッセージを受信者に送信できる場合、その受信者への通知は元のメッセージに追加されます。

通知メッセージには、ユーザが設定したタグに基づいたイベント固有の情報を含めることができます。たとえば、検索通知に不正プログラムの名前、InterScan が実行した処理、感染ファイルの名前を記載できます。

通知のカスタマイズ

InterScan では次の 2 種類の通知タグを使用します。

- フィルタベースのタグは、[検索オプション] タブで利用できます。

  フィルタ通知をカスタマイズするには、次のタグを使用します。

検索オプション	タグ	戻り値
セキュリティリスク検索	%FILE%	感染ファイルのファイル名
	%DETECTION%	検出された不正プログラムの名前
	%ACTION%	検索処理
APT 対策フィルタ	%FILE%	感染ファイルのファイル名
	%DETECTION%	検出された不正プログラムの名前
	%ACTION%	検索処理

検索オプション	タグ	戻り値
検索制限	%FILE%	感染ファイルのファイル名
	%CAUSE%	一致する検索制限オプション
	%ACTION%	検索処理
メッセージフィルタ	%CAUSE%	一致するメッセージフィルタオプション
	%ACTION%	フィルタ処理
添付ファイルフィルタ	%FILE%	感染した添付ファイルのファイル名
	%CAUSE%	一致する添付ファイルフィルタオプション
	%ACTION%	フィルタ処理
コンテンツフィルタ	%CONTENT_FILTER_NAME%	一致するコンテンツフィルタ
	%MAILPART%	コンテンツフィルタに一致したメッセージの部分 : ヘッダ、メッセージ本文または添付ファイル
	%ACTION%	フィルタ処理
スクリプトフィルタ	%FORM_PART%	スクリプトフィルタに一致したメッセージの部分
	%KEYWORDS%	一致するキーワード
情報漏えい対策フィルタ	%DLP_FILTER_NAME%	一致する情報漏えい対策フィルタ
	%MAILPART%	コンテンツフィルタに一致したメッセージの部分 : ヘッダ、メッセージ本文または添付ファイル
	%ACTION%	フィルタ処理

- ルールベースのタグは、InterScan ルールで使用されます。

  メール検索、データベース検索、予約検索、および予約アップデートルールで使用する通知テンプレートをカスタマイズするには、次のタグを使用します。

タグ	戻り値
%DATABASE%	データベース名
%version%	パターンファイル / 検索エンジンのバージョン
%SERVER%	Domino/InterScan サーバ
%SENDER%	検索ルールに一致したメッセージの送信者

タグ	戻り値
%RECIPIENTS%	検索ルールに一致したメッセージの受信者
%SUBJECT%	検索ルールに一致したメッセージの件名ヘッダ
%SEND_TIME%	メッセージが送信された時刻 (hh:mm 形式)
%FINAL_ACTION%	最後に実行された検索 / フィルタ処理
%MATCHING_FILTER%	一致するフィルタ
%SCAN_TIME%	InterScan でメッセージが検索された時刻 (hh:mm 形式)
%PRODUCTVERION%	InterScan for IBM Domino のバージョン
%PATTERNVERSION%	ウイルスパターンファイルのバージョン
%SCANENGINEVERSION%	ウイルス検索エンジンのバージョン
%RULENAME%	ルール名
%RULENUMBER%	ルールの優先度
%ADMIN_FILTER_INFORMATION%	管理者に送信する通知のために選択したフィルタベースのタグを統合します。
%OWNER_FILTER_INFORMATION%	データベース所有者に送信する通知のために選択したフィルタベースのタグを統合します。
%INTERNAL_FILTER_INFORMATION%	Domino アドレス帳に記録されている送信者または受信者に送信する通知のために選択したフィルタベースのタグを統合します。
%EXTERNAL_FILTER_INFORMATION%	Domino アドレス帳に記録されていない送信者または受信者に送信する通知のために選択したフィルタベースのタグを統合します。
%OS%	プラットフォーム (たとえば、Windows)
%COMPONENT%	ウイルス対策コンポーネントまたはコンテンツセキュリティコンポーネント

注意： 通知テンプレートによって、指定したフィルタベースのタグが統合された後、通知設定ポリシーを使用して通知が配信されます (180 ページの「通知の配信方法の設定」を参照)。<<and>> などの文字を通知テンプレートに挿入しないでください。これらの文字を挿入すると、解析エラーが発生し、これらの文字で囲まれた内容が通知に表示されなくなります。

メールスタンプ (安全スタンプ) の使用

InterScan 通知以外に、メールスタンプを定義することで InterScan の処理についてただちにユーザに知らせることもできます。

メールスタンプは、件名ヘッダに通常のテキストとして付加されます。たとえば、次のようにメッセージの件名ヘッダをカスタマイズできます。

[InterScan 通知] このメールにウイルスは検出されませんでした。

検索ルールまたはアップデートルールで使用できる [検索オプション] タブに従って、メッセージの件名または本文の一部としてメールスタンプを次のように定義できます。

[検索オプション] タブ	利用可能なメールスタンプ
セキュリティリスク検索	次のことを実行できます。 • セキュリティリスクが検出された場合、警告を元のメールに挿入します。 • メールが安全な場合、メッセージを元のメールに挿入します。 件名ヘッダまたはメッセージ本文の末尾にメールスタンプを挿入します。
APT 対策フィルタ	件名の先頭にスタンプを挿入できます。
検索制限	件名の先頭にスタンプを挿入できます。
メッセージフィルタ	件名の末尾にスタンプを挿入できます。
添付ファイルフィルタ	件名の末尾にスタンプを挿入できます。
スクリプトフィルタ	件名ヘッダの末尾またはメッセージ本文の先頭にメールスタンプを挿入します。

適用可能なフィルタの安全スタンプの定義については、次のリンク先を参照してください。

- **スパムフィルタ**のスタンプについては、108 ページを参照してください。
- **Web レピュテーション**のスタンプについては、108 ページを参照してください。
- **セキュリティリスク検索**のスタンプについては、124 ページを参照してください。
- **APT 対策フィルタ**のスタンプについては、125 ページを参照してください。
- **検索制限**のスタンプについては、127 ページを参照してください。
- **メッセージフィルタ**のスタンプについては、127 ページを参照してください。

- **添付ファイルフィルタ**のスタンプについては、131 ページを参照してください。
- **スクリプトフィルタ**のスタンプについては、141 ページを参照してください。

InterScan 通知の設定

脅威となるコンテンツまたは迷惑メールが検出された場合や、ウイルス対策またはコンテンツセキュリティコンポーネントを最新バージョンにアップデートした場合に通知を送信するように InterScan を設定できます。

InterScan 通知の設定の詳細については、以降のセクションを参照してください。

通知の配信方法の設定

InterScan では、メールまたは IBM Instant Messaging および Web Conferencing を介して通知を送信できます。通知に使用する方法を設定するには、[通知] タブを使用します。InterScan は、Windows イベントログにも通知を送信します。

通知の配信方法を設定するには

1. ポリシーを作成 (83 ページの「ポリシーの作成」を参照) または変更 (85 ページの「ポリシーの変更」を参照) します。
2. 作業領域で、[通知] タブをクリックします。
3. 文書をダブルクリックするか [編集] をクリックして、次の内容を設定します。
   a. [設定] セクションの [返信アドレス] に、アドレスを入力するか、 をクリックして指定します。
   b. [Sametime サーバのホスト名 /IP アドレス] を入力して、IBM Instant Messaging and Web Conferencing のアカウントに通知を送信するよう InterScan を設定します。
   c. アカウントの [Sametime 送信者ユーザ名] を入力します。
   d. アカウントの [Sametime 送信者パスワード] を入力します。
   e. メッセージがフィルタ設定に一致したときに、メールおよび IBM Instant Messaging and Web Conferencing のさまざまな受信者に通知を送信するには、[管理者] セクションで、[イベントごとに通知受信者を指定する] を選択します。これを選択しない場合、管理者のメールアドレスと IBM Instant Messaging および Web Conferencing のアカウントのみに通知が送信されます。
4. [保存して閉じる] をクリックします。

Windows イベントログに関する InterScan の設定

Windows イベントログのアプリケーションカテゴリに通知を書き込むように InterScan を設定できます。

Windows イベントログに通知を配信するように InterScan を設定するには

- Domino コンソールを開き、次のコマンドを入力します。

  set config SMDWriteOSEventLog=1

注意： テキストエディタを使用して ***notes.ini*** ファイルを変更する場合は、変更内容を反映するために Domino サーバを再起動する必要があります。

InterScan 通知の設定

InterScan 通知のコンテンツを定義するには、[通知テンプレート] タブを使用します。ルールごとに通知テンプレートを定義します。

検索通知を設定するには

1. メール検索ルール、データベース検索ルール、または予約検索ルールで、[通知テンプレート] タブをクリックします。
2. [追加 >>] をクリックして、管理者宛て通知、内部の送信者 / 受信者宛て通知、および外部の送信者 / 受信者宛て通知のタグを追加します。

注意： 管理者宛ての通知は、[通知] タブでポリシーに設定したメールアドレスに送信されます (180 ページの「通知の配信方法の設定」を参照)。

検索通知によっては、ウイルス対策コンポーネントおよびコンテンツセキュリティコンポーネントの変数の値として「該当なし」が割り当てられる場合があります。コンポーネントの値が「該当なし」の場合、これは、データベース検索またはメール検索の際にフィルタではそのようなコンポーネントは使用されなかったという意味です。たとえば、添付ファイルフィルタでは、メッセージをフィルタ処理する際に検索エンジンもウイルスパターンファイルも使用されません。このため、メッセージが添付ファイルフィルタ設定に一致した場合に検索通知に %PATTERNVERSION% が設定されていると、この変数の値が「該当なし」になります。

---

3. [保存して閉じる] をクリックします。

アップデート通知の設定

コンポーネントがアップデートされたときに通知が送信されるように設定するには、[通知] タブを使用します。

アップデート通知を設定するには

1. 「予約アップデートルール」文書または「手動アップデート」文書で、[通知] タブをクリックします (168 ページの「予約アップデートルールを使用したコンポーネントの自動アップデート」または 167 ページの「コンポーネントの手動アップデート」を参照)。
2. [管理者] でアップデート通知の受信者を入力するか  をクリックして選択します。
3. アップデートされたときにアップデート通知送信の対象となるコンポーネントを選択します。
   - ウイルス対策コンポーネントまたはコンテンツセキュリティコンポーネントを選択します (166 ページの「ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントの概要」を参照)。
   - 選択したコンポーネントがアップデートできないときに通知を送信するには、[アップデートに失敗した場合に通知] を選択します。

     コンポーネントのダウンロードを試みる [試行回数] を入力します。この試行回数を超えると、通知が送信されます。

     注意： 1 回の試行時間は 120 秒です。
4. [件名] に、アップデート通知のメッセージの内容を入力します。
5. [保存] をクリックします。

第 8 章

ログデータベースおよび隔離データベース

第 8 章では、InterScan for IBM Domino (以下、InterScan) 5.6 のウイルスログと隔離ログの表示と削除、およびウイルス統計の生成について説明します。

第 8 章で説明する項目は次のとおりです。

ログデータベースの使用

InterScan では、その動作のすべてがログに保持され、ログデータベース（***smvlog.nsf***）に書き込まれます。

ログは、貴重なシステム情報源です。ログのエントリを調べると、メッセージ、共有データベース、複製トランザクションから、どのような不正なプログラムが InterScan で検出されているかがわかります。

サーバが扱うトラフィックの量と発見された不正プログラムの数によっては、ログデータベースが膨大なサイズになる場合があります。ログを手動で削除するか、定期的にログを自動削除するように InterScan を設定します。

InterScan ログデータベースの左側のメニューから、メール検索ログとデータベース検索ログを表示できます。

図 8-1.　InterScan ログデータベースのメイン画面

[統計] 画面で、InterScan の動作を集約して表示できます。

注意： マルチサーバ環境では、すべての InterScan サーバのログをまとめて管理する単一の中央サーバを設置した方が好結果が望める場合があります。Pull 処理による複製のみで周辺サーバからログを収集する中央 Domino サーバの設置をお勧めします。

Trend Micro Threat Connect ポータルへのアクセス

Threat Connect はトレンドマイクロのグローバルなインテリジェントネットワークを基盤としたクラウドベースのサービスであり、関連する実用的かつ豊富な脅威情報を提供するように設計されています。

InterScan 5.6 では、ウイルスログの [詳細] リンクをクリックすることで、Trend Micro Threat Connect ポータルにアクセスし、脅威に関する最新情報を取得することができます。脅威をトレンドマイクロのグローバルな脅威情報に関連付けることで、その攻撃プロファイルに対して適切な処理を施すことができます。

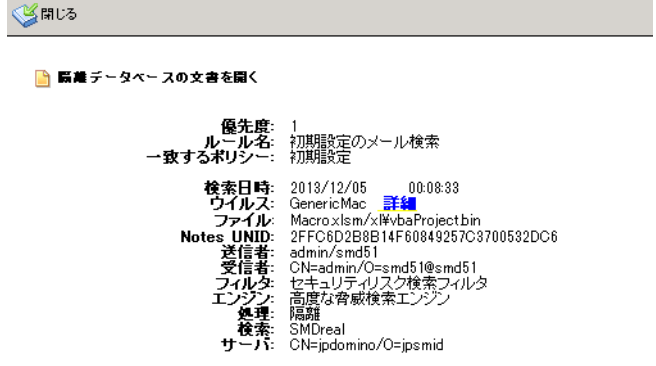


図 8-2. InterScan のウイルスログ

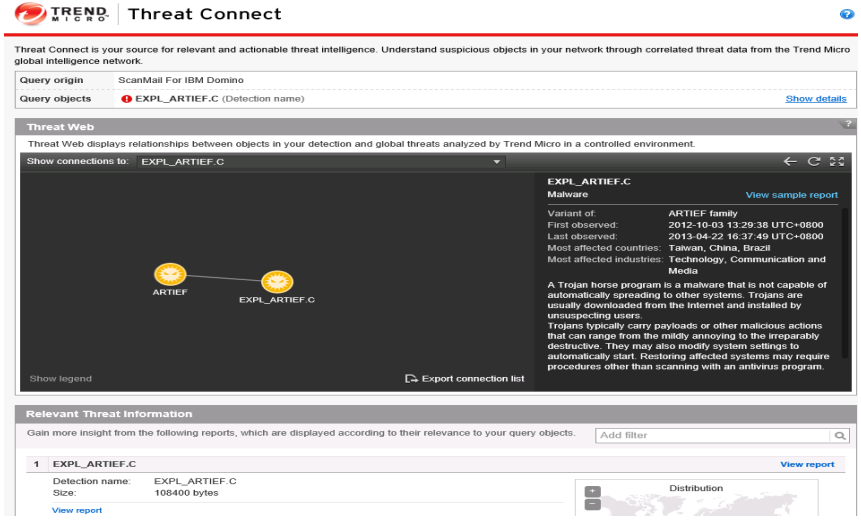


図 8-3. Threat Connect ポータルのウイルスの詳細

InterScan ログの管理

InterScan ログデータベースには、さまざまな設定が可能なオプションが用意されています。設定できる内容として、ウイルスログの保管期間、ログの定期予約メンテナンス、ウイルスログと隔離ログの手動削除、ハブサーバにウイルスログを複製するための接続などがあります。

InterScan ログにアクセスし、その内容を表示するには、InterScan ログデータベースを使用します。

ログの検索

ログデータベースで、検索条件を設定してログを検索できます。

ログ検索タスクを設定するには

1. 次のいずれかの操作を実行して、ログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. [ログクエリ] → [検索] の順に選択します。

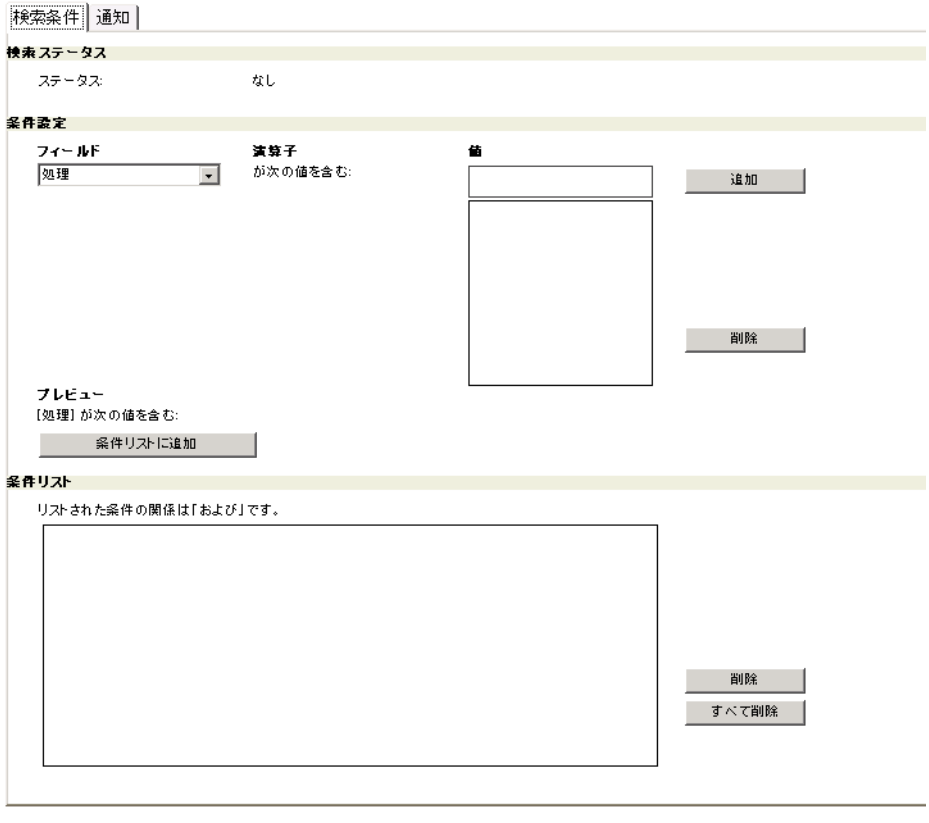


図 8-4. 検索条件の設定

3. [検索条件] タブで、検索条件を設定します。

- [検索ステータス] セクション : 検索タスクのステータス ([なし]、[タスク実行中]、[タスク完了]) が表示されます。
- [条件設定] セクション : 条件リストに条件を追加します。

  条件を追加するには、フィールドを選択して値を入力し、[追加] をクリックして値を追加してから、[条件リストに追加] をクリックします。
- [条件リスト] セクション : 現在の検索に対して設定されている条件のリストが表示されます。

  条件を削除するには、条件リストから条件を選択し、[削除] をクリックします。既存のすべての条件を削除するには、[すべて削除] をクリックします。

4. [通知] タブで、メール通知を有効にします。
   a. [検索の完了時に管理者に通知します] チェックボックスをオンにします。
   b. 通知メールの受信者を選択します。
   c. 通知メールの件名と本文を入力します。

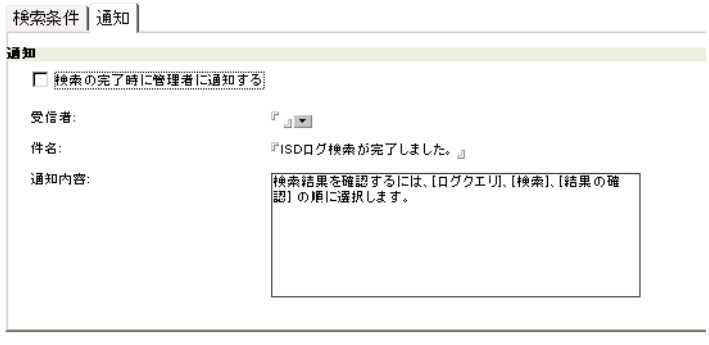


図 8-5. メール通知の有効化

ログを検索するには

1. 処理バーの [検索] をクリックします。
2. [更新] をクリックして、検索が完了したかどうかを確認します。
3. 検索が完了したら、[結果の確認] をクリックして検索結果を確認します。

   結果をクリアするには、[結果のクリア] をクリックします。

注意： ログ検索機能で実行できる検索タスクは一度に 1 つだけです。つまり、別のタスクを実行中に新しいタスクを開始することはできません。新しいタスクを開始すると、前のタスクの検索結果は自動的に削除されます。

自動削除の有効化 / 無効化

ログ削除を有効または無効にするには、ログデータベースを使用します。ログ削除を有効にしておくと、InterScan で自動的に削除できます。

ログを自動的に削除するには

1. 次のいずれかの操作を実行して、ログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. 削除を有効にするログ、または無効にするログを選択します。
3. [自動削除を有効] または [自動削除を無効] をクリックします。

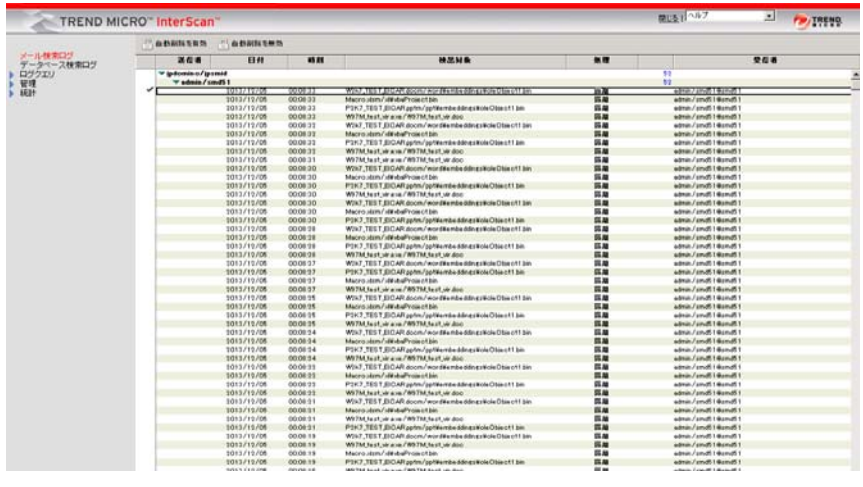


図 8-6. ログデータベースからのログ削除の有効化 / 無効化

注意： 数多くのログの削除を有効にする前に、それらが保管不要であるか確認することをお勧めします。

ウイルスログの自動削除

指定した保管期間を経過したウイルスログを自動的に削除するように InterScan を予約設定するには、ログデータベースを使用します。この機能は、Domino サーバで大量のトラフィックを処理する場合に便利です。

注意： 削除を有効にしたログが自動的に削除されます。

ログファイルを自動的に削除するには

1. 以下のいずれかの手順でログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. ログデータベースの左側のメニューから、[管理] → [削除設定] の順にクリックします。 [自動削除設定] と [手動削除] の画面が表示されます (図 8-7)。

図 8-7. [自動削除設定] と [手動削除]

3. [自動削除設定] セクションで、[次の日数を経過したログを削除する] をオンにします。
4. InterScan にログを保持する期間を日数で入力します。
5. InterScan で保持する削除レコードの件数を [保持する削除レコード数] に入力します。

6. [保存して閉じる] をクリックします。

ウイルスログの手動削除

ウイルスログを手動で削除するには、ログデータベースを使用します。

ログを手動で削除するには

1. 次のいずれかの操作を実行して、ログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. ログデータベースの左側のメニューから、[管理] → [削除設定] の順にクリックします。 [自動削除設定] と [手動削除] の画面が表示されます (図 8-7 を参照)。
3. [手動削除] セクションで、次のいずれかの操作を実行します。
   - ログデータベースに存在する既存のログをすべて削除する場合は、[すべてのログを削除] を選択します。
   - 選択したログを削除する場合は、[指定したログを削除] を選択します。
     i. [参照] をクリックして、[ログファイル] ウィンドウを開きます。
     ii. 削除するログを選択します。
     iii. [OK] をクリックします。
4. [今すぐ削除] をクリックします。

注意： 削除が有効になっているウイルスログのみが削除されます。

統計とグラフの表示

[統計] オプションでは、サーバ上のメールおよびデータベースのウイルスログの数値での概要を生成できます。この統計には、不正プログラムの総数が、駆除済み、削除済み、隔離済み、放置に分類されて表示されます。また、セキュリティリスク検索、APT 対策フィルタ、メッセージフィルタ、添付ファイルフィルタ、コンテンツフィルタ、スクリプトフィルタ、スパムフィルタ、Web レピュテーション、情報漏えい対策フィルタ、大規模感染予防フィルタ、および転送されたメッセージの結果に関する統計を生成するオプションもあります。

統計の生成、表示、およびエクスポート

ログ統計を生成、表示するには、ログデータベースを使用します。

ログ統計を生成、表示、およびエクスポートするには

1. 次のいずれかの操作を実行して、ログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. ログデータベースの左側のメニューで、[統計] → [ログレポート] の順にクリックします。
3. 作業領域で、すべての統計または表示する特定の統計を選択します。
4. [表の表示] から、表示する表を選択します。
   - **すべて**
   - **セキュリティリスク検索**
   - **APT 対策フィルタ**
   - **メッセージフィルタ**
   - **添付ファイルフィルタ**
   - **コンテンツフィルタ**
   - **情報漏えい対策フィルタ**
   - **スクリプトフィルタ**
   - **スパムフィルタ**
   - **Web レピュテーション**
   - **大規模感染予防フィルタ**
   - **転送されたメッセージ**
5. 目的のログが保存されているサーバを選択します (複数選択可)。
6. [範囲] として、[すべて]、[本日]、[過去 1 週間]、[過去 1ヵ月間]、または [指定する日付] を選択します。
7. [ログ数値反映] をクリックすると、選択したログを要約したレポートの作成が始まります。
8. 作業領域で、[エクスポート] をクリックして、生成されたデータを `*.csv` ファイルにエクスポートします。

注意： `*.csv` ファイルを開くには、Microsoft Excel などの表計算アプリケーションを使用します。

CSV 形式で出力されたログファイルの表示

Microsoft Excel を使用すると、エクスポートした InterScan ログを使いやすい形で表示できます。

Microsoft Excel を使用して、*.csv にエクスポートした InterScan ログを表示するには

1. Microsoft Excel を開きます。
2. エクスポートした *.csv ファイルを開きます。
3. 列ヘッダをクリックして、データの先頭列をハイライトします。
4. メインメニューで [データ] → [区切り位置] の順に選択し、表示されるウィザードに従って操作します。
   - [カンマやタブなどの区切り文字によってフィールドごとに区切られたデータ] を選択して、[次へ] をクリックします。
   - [タブ] チェックボックスをオフにします。[カンマ] をオンにし、[文字列の引用符] で [なし] を選択します。
   - ウィザードの最後の画面では何も変更せずに、[完了] をクリックします。
5. 同じデータをもう一度インポートして表の体裁を直さなくてもすむように、文書を *.xls の Excel ファイルで保存します。

グラフの生成と表示

[統計] → [トップ 10] オプションを使用して、次のいずれかのグラフを棒グラフのレイアウトで生成できます。

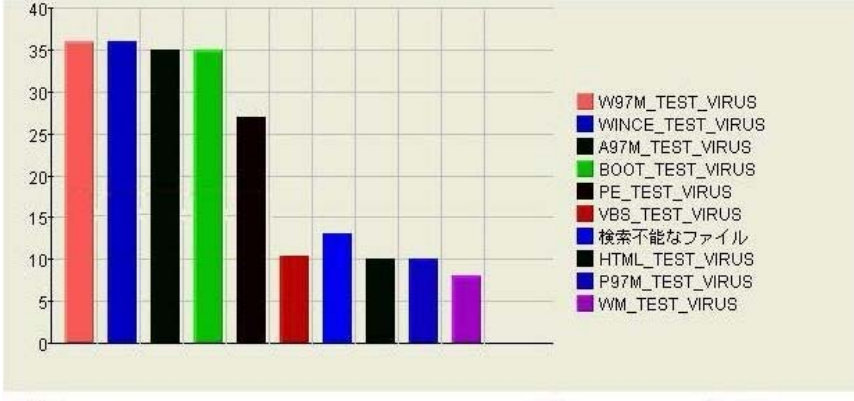
- **ウイルスグラフ** — 検出件数が上位 10 件に入るウイルスを示します。
- **サーバグラフ** — 感染検出件数が上位 10 位に入るサーバの情報を示します。
- **ユーザグラフ** — メールを介してウイルスを送付した回数が上位 10 位に入るユーザの情報を示します。
- **データベースグラフ** — 感染件数が上位 10 位に入るデータベースの情報を示します。

ログ統計を生成、表示するには

1. 以下のいずれかの手順でログデータベースを開きます。
   - InterScan の左側のメニューから、[ログデータベース] を選択します。
   - ***smvlog.nsf*** を開きます。
2. ログデータベースの左側のメニューから、[統計] → [トップ 10] を選択します。
3. 作業領域で、生成、表示するグラフの種類を選択します。

4. 日付として [すべて] またはいずれかの日付範囲を選択します。
5. [グラフの生成] をクリックします。

   画面には、上位 10 位の値を示す棒グラフと、これらの値が全件数の中で占める比率が表示されます。ログデータベースにログが存在しない場合は、棒グラフにはデータは表示されません。



ウイルス	件数	パーセント
W97M_TEST_VIRUS	36	16.14%
WINCE_TEST_VIRUS	36	16.14%
A97M_TEST_VIRUS	35	15.70%
BOOT_TEST_VIRUS	35	15.70%
PE_TEST_VIRUS	27	12.11%
VBS_TEST_VIRUS	13	5.83%
検索不能なファイル	13	5.83%

図 8-8.　検出グラフの例

隔離データベースの使用

InterScan 隔離データベース (smquar.nsf) には、コンテンツ違反、不正プログラム違反、またはスパム違反のために隔離されたメッセージのコピーが保存されます。

サーバが扱うトラフィックの量と、InterScan で検出された不正プログラムの量によっては、隔離データベースが膨大なサイズになる場合があります。InterScan では、不正プログラムが検出されると、感染メールおよび添付ファイルは隔離され、smquar.nsf データベースに新規文書として保存されます。

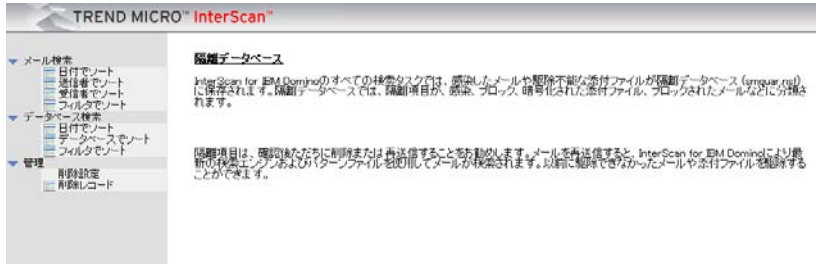


図 8-9.　隔離データベースのメイン画面

隔離アイテムを「x」日ごとに自動的に削除するように、InterScan を設定します (198 ページの「隔離アイテムの自動削除」を参照)。または、隔離データベースから隔離アイテムを手動で削除することもできます (199 ページの「隔離アイテムの手動削除」を参照)。

隔離されたメッセージ、文書、および添付ファイルの表示

隔離アイテムにアクセスし、その内容を表示するには、InterScan 隔離データベースを使用します。

メール検索で隔離された添付ファイルを表示するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 左側のメニューから、[メール検索] を選択し、次の基準に従ってアイテムを表示します。
   - **日付でソート** — 日付を基準にして、InterScan で隔離されたすべてのメッセージを表示します。
   - **送信者でソート** — 送信者を基準にして、InterScan で隔離されたすべてのメッセージを表示します。

- **受信者でソート** — 受信者を基準にして、InterScan で隔離されたすべてのメッセージを表示します。
- **フィルタでソート** — フィルタを基準にして、InterScan で隔離されたすべてのメッセージを表示します。

データベース検索で隔離された添付ファイルを表示するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 左側のメニューから、[データベース検索] を選択し、次の基準に従ってアイテムを表示します。
   - **日付でソート** — 日付を基準にして、InterScan で隔離されたすべてのメッセージを表示します。
   - **データベースでソート** — データベースを基準にして、InterScan で隔離されたすべてのメッセージを表示します。
   - **フィルタでソート** — フィルタを基準にして、InterScan で隔離されたすべてのメッセージを表示します。

隔離メッセージの再送信

隔離メッセージとは、InterScan のリアルタイムメール検索タスクで隔離されたメッセージです。InterScan では、隔離メッセージを再送信できます。

隔離メッセージを再送信するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 隔離データベースの左側のメニューから、[メール検索] → [日付でソート]、[送信者でソート]、[受信者でソート]、または [フィルタでソート] を選択します。
3. 再送信する、メール検索で隔離されているメッセージを選択します。
4. 作業領域で、[再送信を有効] をクリックします。
5. 再送信できるように設定したメッセージには、アイコン が表示されます。アイコン がないアイテムは、再送信が無効になっています。
6. [再送信] をクリックしてメッセージを再送信します。

隔離文書の復元

隔離文書とは、InterScan のリアルタイム検索タスク、手動検索タスク、または予約データベース検索タスクで隔離された文書です。InterScan では、隔離文書を復元できます。

警告： 隔離文書の復元では細心の注意を払います。不正プログラムが含まれる文書を復元して開くことができますが、これによってウイルスの大規模感染を招くおそれがあります。

隔離文書を復元するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 隔離データベースの左側のメニューから、[メール検索] または [データベース検索] を選択します。
   - [メール検索] の場合、[日付でソート]、[送信者でソート]、[受信者でソート]、または [フィルタでソート] を選択します。
   - [データベース検索] の場合、[日付でソート]、[データベースでソート]、または [フィルタでソート] を選択します。
3. 作業領域で、隔離文書を選択して [再送信を有効] をクリックし、[再送信] をクリックします。

隔離アイテムの削除の有効化 / 無効化

隔離アイテムの削除を有効または無効にするには、隔離データベースを使用します。アイテムの削除を有効にしておくと、InterScan で自動的に削除できます。

隔離アイテムを自動的に削除するには

1. 以下のいずれかの手順で隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 削除を有効にする隔離アイテム、または無効にする隔離アイテムを選択します。

3. [自動削除を有効] または [自動削除を無効] をクリックします。

図 8-10. 隔離アイテムの削除の有効化 / 無効化

注意： 削除を有効にする前に、それらの隔離アイテムが本当に保管不要であるか確認することをお勧めします。

隔離アイテムの自動削除

指定した保管期間を経過した隔離アイテムを自動的に削除するように InterScan を予約設定するには、隔離データベースを使用します。この機能は、Domino サーバで大量のトラフィックを処理する場合に便利です (図 8-11 を参照)。

図 8-11. [自動削除] と [手動削除] の画面

注意： 削除を有効にした隔離アイテムが自動的に削除されます。

メール検索またはデータベース検索で隔離されたアイテムを自動的に削除するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 隔離データベースの左側のメニューから、[管理] → [削除設定] の順に選択します。
3. [自動削除を有効にする] をオンにして、次のいずれかのオプションを選択します。
   - [次の日数を経過した隔離メールを削除] をオンにして、メールを削除するまで InterScan で保管する日数を入力します。
   - [次の日数を経過した隔離データベース文書を削除] をオンにして、データベース文書を削除するまで InterScan で保管する日数を入力します。
4. [保持する削除レコード数] に、InterScan の削除レコードフォルダで保管する削除レコード数 (0 ～ 100) を入力します。

   注意： 削除されたメール検索およびデータベース検索は、[管理] → [削除設定] → [保持する削除レコード数] で保管が設定されている削除レコード数に基づいて、削除レコードフォルダに保管されます。

5. [保存して閉じる] をクリックします。

隔離アイテムの手動削除

隔離アイテムを手動で削除するには、隔離データベースを使用します。

隔離アイテムを手動で削除するには

1. 次のいずれかの操作を実行して、隔離データベースを開きます。
   - 設定データベースの左側のメニューから、[隔離データベース] を選択します。
   - ***smquar.nsf*** を開きます。
2. 隔離データベースの左側のメニューから、[管理] → [削除設定] の順に選択します。
3. 作業領域で、次のいずれかを実行します。
   - 隔離データベースにある既存のアイテムをすべて削除する場合は、[隔離文書をすべて削除] を選択します。
   - 選択したアイテムを削除する場合は、[選択した隔離文書を削除] を選択します。
     i. [参照] をクリックして、[ログファイル] ウィンドウを開きます。

ii. InterScan で削除する隔離アイテムを選択します。

iii. [OK] をクリックします。

4. [今すぐ削除] をクリックします。

注意： 削除を有効にした隔離アイテムのみが削除されます。

Deep Discovery Advisor 隔離データベースの概要

InterScan の APT 対策検索タスクでは、InterScan Deep Discovery Advisor 隔離データベース (`smddtas.nsf`) を使用して、疑わしいファイルが添付されたメッセージを一時的に保存します。この添付ファイルは分析のために Deep Discovery Advisor にアップロードされ、その分析結果に基づいて、APT 対策フィルタによりメッセージまたは添付ファイルに対して事前設定処理が行われます。

注意： データが失われる可能性があるため、一時隔離データベース内のメッセージは手動で削除しないことをお勧めします。

隔離されたメッセージの表示

隔離アイテムにアクセスし、その内容を表示するには、Deep Discovery Advisor 隔離データベースを使用します。

メール検索またはデータベース検索で隔離された添付ファイルを表示するには

1. `smd` フォルダの InterScan Deep Discovery Advisor 隔離データベース (`smddtas.nsf`) を開きます。
2. 左側のメニューで、[メール検索] または [データベース検索] を選択し、一時的に隔離されたメッセージを表示します。
3. レコードをダブルクリックして詳細を表示します。

第 9 章

Trend Micro Control Manager からの管理

Trend Micro Control Manager　(以下、Control Manager) は、トレンドマイクロのウイルス対策製品とサービスを 1 つのウイルスセキュリティおよびコンテンツ管理ソリューションに統合する集中管理システムです。

第 9 章で説明する項目は次のとおりです。

Control Manager について

Control Manager は、トレンドマイクロおよびサードパーティのウイルス対策およびコンテンツセキュリティのための製品とサービスを、ゲートウェイ、メールサーバ、ファイルサーバ、企業デスクトップの各レベルで管理する集中管理コンソールです。Control Manager の Web ベースの管理コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティのための製品とサービスを 1 か所で監視できます。

Control Manager には、企業ごとに異なる要件をより良く満たせるように、スタンダード版とエンタープライズ版が用意されています。

- スタンダード版は、企業のウイルス対策やコンテンツセキュリティの管理を可能にする高度な管理機能と設定機能を提供します。
- エンタープライズ版は、大企業や各種サービスプロバイダを対象にしています。エンタープライズ版では、スタンダード版の機能に加えて、階層管理コンソールのサポートやレポート作成などさまざまな高度な機能が提供されます。

主な機能

Control Manager の主な機能は次のとおりです。

- 集中管理により、管理者はネットワークにインストールされているトレンドマイクロのソフトウェアを、場所やプラットフォームにかかわらず、単一のコンソールから設定、監視、および保守できます。
- 柔軟でスケーラブルな構成により、ウイルスおよびコンテンツセキュリティに関する企業ポリシーの管理を簡素化できます。
- ジョブの委任を実現する階層構造により、管理者はアクセス制御を決定でき、ユーザごとに、階層の異なる末端レベルへのアクセスを割り当てることができます。
- 大規模感染予防サービスは、攻撃に対する予見的な保護サービスを提供し、ファイル名やファイルの特定の詳細に基づいて不正コードをブロックします。また、新しい脅威を検出して駆除するために、新しいパターンファイルの開発も行われています。
- 脆弱性診断は、ネットワークのセキュリティリスクを診断するサービスで、既知のウイルスや不正プログラムによる攻撃に対するシステムの脆弱性を検索し、その脆弱性を排除するために推奨する処理を示します。

- エージェントが不要なダメージクリーンナップサービス (DCS) は、感染を診断し、ワームやトロイの木馬など、不正な残存プログラムによる影響からシステムを修復する、包括的なクリーンナップサービスを提供します。これにより、システム管理者は、ローカルのクライアントマシンにソフトウェアをインストールすることなく、容易にシステムから不正なプログラムを駆除できます。

Control Manager と InterScan の連携

Control Manager は、複数の Domino サーバを持つ組織や、InterScan for IBM Domino (以下、InterScan) 5.6 以外にも他のトレンドマイクロ製品を使用している組織で役立つツールです。InterScan を Control Manager と連携させることの主な利点は次のとおりです。

- 一元化されたウイルスログの作成
- 高機能なレポートと分析オプション
- トレンドマイクロ 大規模感染予防サービスによる、ウイルスの大規模な感染に対する迅速な予防措置の発動
- 集中ライセンス管理コンソール
- 一元化されたコンポーネント配信

Control Manager Management Communication Protocol の概要

InterScan と Control Manager 間の通信では、Trend Micro Control Manager Management Communication Protocol (MCP) という新しいプロトコルが使用されます。InterScan では、以前のバージョンの InterScan と Control Manager で使用されていた Trend Micro Management Infrastructure (TMI) プロトコルはサポートされなくなりました。

InterScan のインストール後、Control Manager エージェントを登録できます。InterScan では、Control Manager からの Web コンソールのリダイレクションがサポートされます。InterScan 製品コンソール用のユーザ名とパスワードを使用して、Control Manager 製品コンソールから InterScan 製品コンソールに直接アクセスします。

トレンドマイクロ大規模感染予防サービスの概要

注意： InterScan では、リアルタイム検索が有効になっていないと、大規模感染予防サービスは適用されません。

大規模感染予防は、管理対象製品でウイルスの大規模感染が検出されたが、利用できるパターンファイルがない危機的な局面で使用されます。このような局面では、システム管理者は組織内の各所との複雑な連絡に長い時間を費やすことになります。ときには組織が世界中に分散しているために、一元的な管理が不可能なこともあります。

大規模感染予防サービスでは、新しい脅威に関する通知を配信するとともに、攻撃の進行時にはシステムのステータスに関する包括的なアップデートを継続的に配信します。新しい脅威が識別されると、ウイルスに関する詳細なデータとともに、脅威に対処するための定義済み処理および検索ポリシーがただちに配信されるので、企業はウイルスを短時間で封じ込めて感染の拡大を防止できます。

また、大規模感染予防サービスでは、中央で推奨ポリシーを配信および管理することにより、通信不良の可能性を排除してポリシーを適用し、攻撃の発生時にそれに対処するための情報を配信します。

大規模感染予防サービスでは、Control Manager を経由して自動または手動でポリシーをダウンロードして配信できるため、トレンドマイクロの世界的なセキュリティリサーチおよびサポートネットワークである TrendLabs の専門家から、ネットワーク上の重要なアクセスポイントに情報を直接インポートできます。

このサービスでは、ネットワーク上の重要な箇所に置かれたトレンドマイクロ製品を使用して、企業全体の調整と大規模感染管理が提供されます。この重要な箇所とは、たとえば、インターネットゲートウェイ、メールサーバ、ファイルサーバ、キャッシュサーバ、クライアント、リモートユーザ、ブロードバンドユーザ、サードパーティ製企業用ファイアウォールです。

Control Manager を使用した InterScan の管理

ネットワーク上の任意のコンピュータから InterScan の管理対象製品を設定するには、Control Manager 管理コンソールにアクセスします。

Control Manager 管理コンソールへのアクセス

管理コンソールには、次の 2 つの方法でアクセスできます。

- Control Manager サーバ上で直接アクセスする方法
- 互換性のあるブラウザを使用してリモートにアクセスする方法

Control Manager サーバから管理コンソールにローカルにアクセスするには

1. [スタート] メニューから [プログラム] → [Trend Micro Control Manager] → [Trend Micro Control Manager] の順にクリックします。
2. [ユーザ名] と [パスワード] を入力します。
3. <Enter> キーを押します。

コンソールにリモートにアクセスするには

1. ブラウザのアドレスフィールドに次の URL を入力して、サインイン画面を開きます。

   https://{ ホスト名 }/webapp/login.aspx

   ここで、{ ホスト名 } は、Control Manager サーバの完全修飾ドメイン名 (FQDN)、IP アドレス、またはサーバ名です。

   https://{ ホスト名 }/WebApp/index.html (Control Manager 5.5 の場合)

   https://{ ホスト名 }/webapp/login.aspx (Control Manager 6.0 の場合)
2. [ユーザ名] と [パスワード] を入力します。
3. <Enter> キーを押します。

Control Manager 管理コンソールからの InterScan の管理

Control Manager 管理コンソールは Web ベースのコンソールで、これを使用すると、互換性のある Web ブラウザを通して任意のコンピュータから Control Manager を管理できます。互換性のあるブラウザのリストについては、Control Manager 管理者ガイドまたはオンラインヘルプを参照してください。

InterScan 用 Control Manager エージェントは、Control Manager サーバからコマンドを受け取り、それらを実行するように InterScan に指示します。たとえば、Control Manager 管理コンソールで [タスク] → [検索エンジンの配信] の順に選択した場合、Control Manager エージェントは最新の検索エンジンを配信するように InterScan に指示します。

管理コンソールから InterScan を管理するには

1. Control Manager 管理コンソールにアクセスします (205 ページの「Control Manager 管理コンソールへのアクセス」を参照)。
2. 左側のメニューから、[製品] を選択します。
3. 製品ディレクトリで「ISD」フォルダを展開し、次の操作を実行します。

InterScan ステータスを確認するには

1. 作業領域で、[ステータス] をクリックし、現在表示されているステータスを更新します。

   [製品ステータス] 画面には、製品情報、コンポーネントステータス、OS 情報、エージェント環境情報、および製品ライセンス情報が表示されます。

InterScan を設定するには

1. 作業領域で、[設定] をクリックします。
2. 表示される製品リストから InterScan を選択します。InterScan 設定データベースの Web コンソールが表示されます。

   注意： 必要に応じて、設定データベースへのアクセスに使用するユーザ名とパスワードを入力します。InterScan に設定されているパスワードについては、管理者にお問い合わせください。

3. Notes クライアントインタフェースから設定する場合と同じように、InterScan を設定します。

スパムメール判定ルール、検索エンジン、ライセンスプロファイル、またはパターンファイルを配信するには

1. 作業領域で、[タスク] をクリックします。
2. リストから次のいずれかのタスクを選択します。
   - スパムメール判定ルールの配信
   - 検索エンジンの配信
   - ライセンスプロファイルの配信
   - パターンファイル / クリーンナップテンプレートの配信
3. 適切なオプションを選択して、[配信開始] をクリックします。
4. [OK] をクリックします。

セキュリティログおよび情報漏えい対策ログを表示するには

1. 作業領域で、[ログ] をクリックします。
2. 表示するログの種類を選択します。
   - **セキュリティ脅威情報**には、すべてのウイルスログイベント、コンテンツセキュリティ違反、スパム違反ログ、およびメールやデータベースで検出されたウイルスが記録されます。
   - **情報漏えい対策情報**には、リアルタイムのメールやメールが格納されているデータベースで検出された情報漏えい対策イベントが記録されます。
     i. 表示するログの種類を選択した後、重大度やイベントなどの検索パラメータを指定します。
     ii. [クエリ] をクリックして、クエリを開始します。
     iii. [CSV 形式で保存] をクリックすると、画面上のデータをカンマ区切り形式のファイルにエクスポートできます。
   - CSV 形式へのログのエクスポート

CSV 形式でログをエクスポートするには

1. [CSV 形式でエクスポート] をクリックします。
   [ファイルのダウンロード] ダイアログボックスがポップアップ表示されます。
2. [保存] をクリックします。
3. [別名で保存] 画面で、ファイルの保存場所を指定します。
4. ［保存］をクリックします。

*.CSV ファイルを開くには、Microsoft Excel などの表計算アプリケーションを使用します。

有効な大規模感染予防ポリシーの表示

注意： InterScan では、リアルタイム検索が有効になっていないと、大規模感染予防サービスは適用されません。

有効な大規模感染予防ポリシーを表示するには、次の 2 つの方法があります。

- 設定データベースを使用する方法
  a. InterScan 設定データベースを開きます。
  b. 左側のメニューで、[設定] → [大規模感染予防サービス] の順にクリックします。
  有効な大規模感染予防ポリシーの詳細が作業領域に表示されます。

- Control Manager 管理コンソール (Control Manager 5.5) の [サービス] 画面を使用する方法 (Control Manager 6.0 の場合は [管理] → [大規模感染予防サービス])

  a. Control Manager 管理コンソールにアクセスします (205 ページを参照)。

  b. メインメニューで [サービス] をクリックします。

  c. 左側のメニューで、[サービス] の下にある [大規模感染予防サービス] をクリックします。

  この画面では、最上位の脅威およびステータス情報を最新に保つために、表示が自動的に更新されます。

第 10 章

アンインストール

第 10 章では、Domino 環境から InterScan for Lotus Domino (以下、InterScan) 5.6 および InterScan 用 Trend Micro Control Manager (以下、Control Manager) エージェントを削除する方法について説明します。

第 10 章で説明する項目は次のとおりです。

InterScan の削除

InterScan は、インストール先のすべてのプラットフォームで自動的にまたは手動で削除できます。

- ウィザードを使用して InterScan をアンインストールできます。
- 自動的にアンインストールすることをお勧めしますが、手動で削除することもできます。

InterScan を削除する前に

1. エンドユーザメール隔離 (EUQ) を無効化します。そうしないと、Windows 64 ビット OS でのアンインストールの際、メールデータベーステンプレートファイルに適用された変更がロールバックされないことがあります。
2. Domino サーバをシャットダウンします。

InterScan の自動削除

InterScan がインストールされている OS に応じて、次のアンインストール手順を実行します。

ウィザードベースのアンインストールの実行

InterScan のウィザードベースのアンインストールでは、アンインストールプロセスに沿って手順が表示されます。

InterScan 5.6 Windows 版の削除

グラフィカルデスクトップ環境を使用して InterScan の自動アンインストールを実行するには

1. [スタート] → [プログラム] → [InterScan for IBM Domino] → [InterScan for IBM Domino 5.6 のアンインストール] の順にクリックします。アンインストール準備の進行状況を示す画面が表示されます。

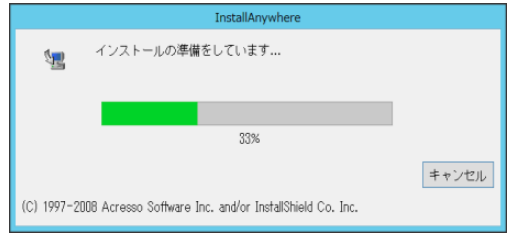


図 10-1.　　アンインストールの進捗画面

2. アンインストール準備の進行状況を示す画面が完了すると、[Trend Micro InterScan for IBM Domino 5.6 のセットアップにようこそ] 画面が表示されます。[次へ] をクリックします。[Domino サーバの選択] の手順に進みます。

図 10-2.　　[ようこそ] 画面

3. [Domino サーバの選択] の手順で、InterScan を削除するサーバを選択し、[アンインストール] をクリックします。

図 10-3. InterScan をアンインストールするサーバの選択

4. アンインストールプロセスを開始すると、アンインストール実行の進行状況を示す画面が表示されます。

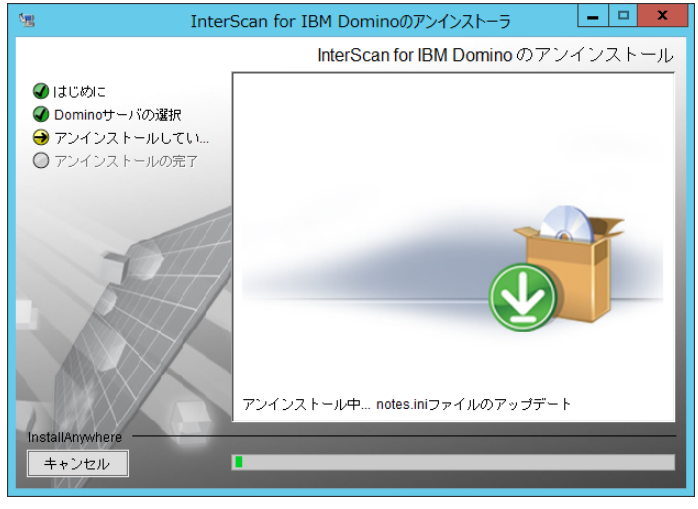


図 10-4. InterScan のアンインストール

5. アンインストールプロセスが完了すると、[アンインストールの完了] 画面が表示されます。[完了] をクリックします。図 10-5 を参照してください。

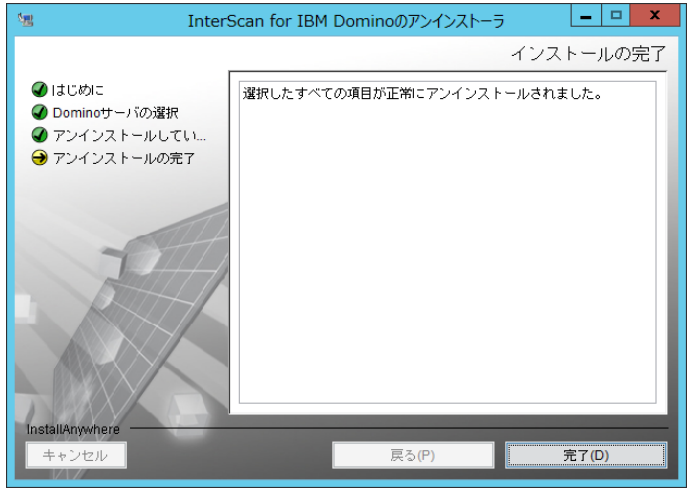


図 10-5.　　アンインストールの完了

注意： Windows プラットフォームでは、Windows の [スタート] → [コントロール パネル] → [プログラムの追加と削除] → [InterScan for IBM Domino] を順に選択することによって、InterScan を削除することもできます。

InterScan 5.6 Linux 版の削除

InterScan 5.6 を削除するには、次の手順を実行します。

1. ターミナルを開き、InterScan のインストールパスの下の ***uninstall*** フォルダに移動します (たとえば、`/opt/trend/SMID/uninstall`)。
2. **./uninstaller** コマンドを使用して、アンインストールファイル (***uninstaller***) を実行します。

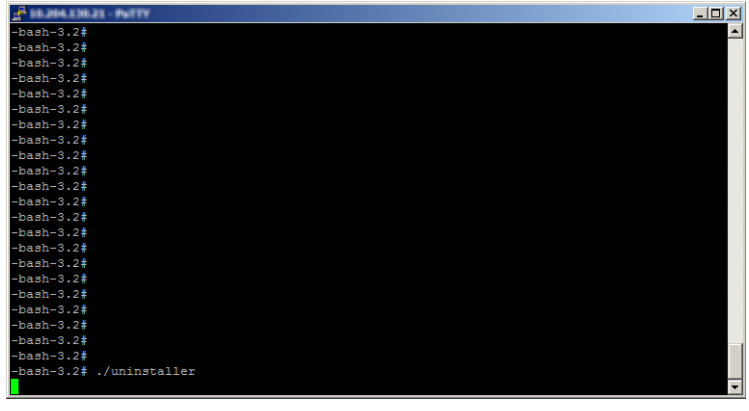


図 10-6.　　アンインストールファイルの実行

InterScan のアンインストールの [ようこそ] 画面が表示されます。

図 10-7.　　[ようこそ] 画面

3. **<Enter>** キーを押します。**[Domino** サーバの選択 **]** 画面が表示されます。

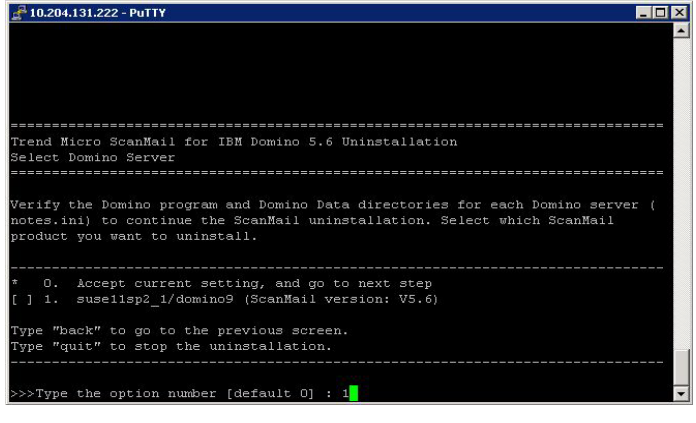


図 10-8.　　インストール済みの Domino サーバを表示した選択画面

図 10-8 の画面では、インストール済みのすべての Domino サーバが一覧表示されています。削除または保持する Domino サーバを選択または選択解除します。

Domino サーバを選択または選択解除するには

a. 該当する番号を入力します。たとえば、図 10-8 の画面に表示されているリストで、**suse11sp2_1/domino9** という名前のサーバを選択する場合は、「*2*」を入力します。

b. **<Enter>** キーを押します。

4. 現在の設定をそのまま使用して、選択済みの Domino サーバのアンインストールを開始する場合は、「*0*」(ゼロ) を入力します。

5. **<Enter>** キーを押します。概要画面が表示され、アンインストール対象の選択された Domino サーバが一覧表示されます。

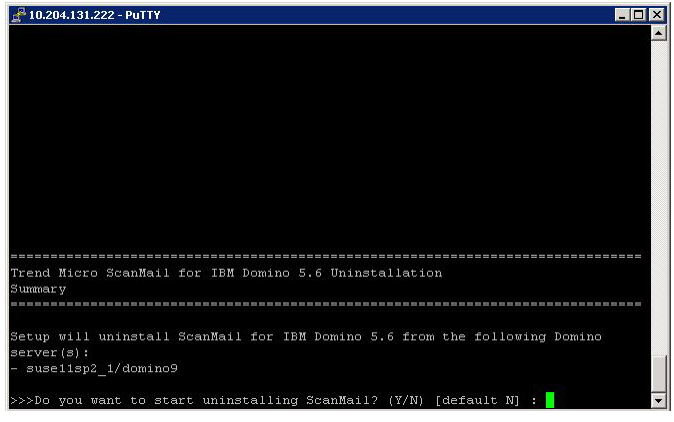


図 10-9. 概要画面

6. 「*Y*」または「*y*」を入力して、**<Enter>** キーを押します。アンインストールが始まります。

アンインストールプロセスが完了すると、画面にアンインストールの完了メッセージが表示されます。

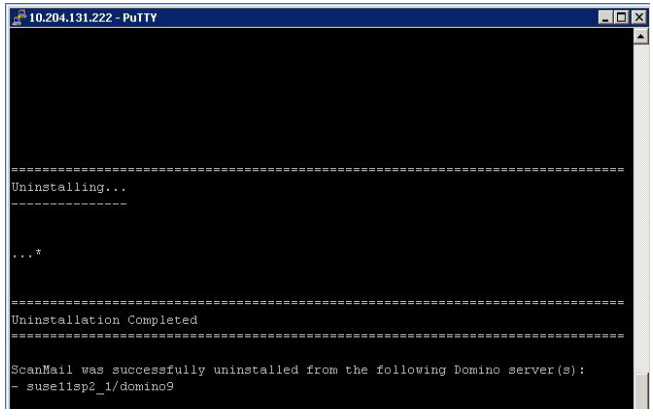


図 10-10.　アンインストールの完了

InterScan の単一または共有インストールの手動削除

InterScan を自動削除できなかった場合、手動で InterScan を削除できます。ただし、InterScan を手動で削除しようとする前に、自動的に削除する方法を試してみることをお勧めします。

サーバに InterScan の複数インストールが設定されており、これらのインスタンスをすべて手動でアンインストールする場合、その手順は単一インストールの InterScan を手動で削除する場合と同様です。

各インスタンスのインストール情報とファイルパスはすべて ***smdsys.ini*** (Windows の場合) または ***smdsysV3.ini*** (Linux の場合) に記録されています。また、これらの ini ファイルには、[SMDConfx] のインスタンスが複数含まれます。

Windows に対する単一または共有 InterScan インストールの削除

単一または共有 InterScan インストールを手動で削除するには

ヒント : InterScan のファイルおよびフォルダ構造については、付録 B「ファイルおよびフォルダー一覧」の B-248 ページの表 B-1 を参照してください。

1. InterScan がインストールされているサーバで、***smdsys.ini*** を見つけ、テキストエディタを使用して開きます。後続の手順の実行時には、参照できるようにこのファイルを開いたままにしておきます。

   以降の手順では、次のパラメータを参照します。

   - DomSvr{X}DominoBinPath
   - DomSvr{X}DataPath
   - DomSvr{X}NotesIniPath
   - ProductPath

   注意 : DomSvr{X} は InterScan インスタンスを表しており、{X} は InterScan インストールの番号を表します。
   対象サーバに InterScan インストールが 1 つしかない場合、DomSvr{X} は DomSvr0 です。InterScan インストールが複数ある場合、{X} は 1 ずつ増えます。つまり、DomSvr0 が 1 つ目のインスタンス、DomSvr1 が 2 つ目のインスタンスというように続きます。

次に、InterScan インスタンスが複数設定されている Windows サーバの ***smdsys.ini*** の例を示します。

```
[SMDConf] ¥¥1 つ目の InterScan インスタンスを示しています
ProductPath=C:¥TrendMicro¥1¥ScanMail for Domino
DomSvrISMDCount=2 ¥¥1 つ目の InterScan インスタンスのパーティション
サーバの数を示しています
ProductVersion=V5.6 ¥¥InterScan のバージョンが 5.6 であることを示して
います
InstallType=32-bit ¥¥32 ビットの InterScan であることを示しています
DomSvrISMDSecs=DomSvr0,DomSvr1 ¥¥1 つ目の InterScan インスタンスの
パーティションサーバを示しています
[DomSvr0] ¥¥1 つ目の InterScan インスタンスの 1 つ目のパーティションサー
バを示しています
DomSvr0NotesIniPath=C:¥IBM¥Domino1¥Data1¥notes.ini
DomSvr0DominoBinPath=C:¥IBM¥Domino1
DomSvr0DataPath=C:¥IBM¥Domino1¥Data1
DomSvr0DominoVersion=0
DomSvr0SMDVersion=5.6
[DomSvr1] ¥¥1 つ目の InterScan インスタンスの 2 つ目のパーティションサー
バを示しています
w=C:¥IBM¥Domino1¥Data2¥notes.ini
DomSvr1DominoBinPath=C:¥IBM¥Domino1
DomSvr1DataPath=C:¥IBM¥Domino1¥Data2
DomSvr1DominoVersion=0
DomSvr1SMDVersion=5.6

[SMDConf0] ¥¥2 つ目の InterScan インスタンスを示しています
ProductPath=C:¥TrendMicro¥2¥ScanMail for Domino
DomSvrISMDCount=1 ¥¥2 つ目の InterScan インスタンスのパーティション
サーバの数を示しています
ProductVersion=V5.6
DomSvrISMDSecs=DomSvr2 ¥¥2 つ目の InterScan インスタンスのパーティ
ションサーバを示しています
[DomSvr2] ¥¥2 つ目の InterScan インスタンスの 1 つ目のパーティションサー
バを示しています
DomSvr2NotesIniPath=C:¥IBM¥Domino2¥Data1¥notes.ini
DomSvr2DominoBinPath=C:¥IBM¥Domino2
DomSvr2DataPath=C:¥IBM¥Domino2¥Data1
DomSvr2DominoVersion=0
DomSvr2SMDVersion=5.6
```

2. Domino バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、DomSvr{X}DominoBinPath で指定されたディレクトリに移動し、次に該当する InterScan ファイルを探して削除します。
   - Windows サーバ上にある DominoBinPath InterScan ファイル (B-248 ページの表 B-1 を参照)。
3. DomSvr{X}DataPath に指定されているディレクトリに移動し、次の InterScan インストールフォルダおよび作業フォルダを削除します (B-248 ページの表 B-1 を参照)。
4. DomSvr{X}NotesIniPath で指定された ***notes.ini*** をテキストエディタで開き、次を実行します。
   a. ServerTasks セクションを見つけて、次の項目を削除します。
      - SMDemf
      - SMDreal
      - SMDsch
      - SMDmon
      - SMDcm
   b. EXTMGR_ADDINS セクションを探し、SMDext 項目を削除します。
   c. ScanMailInstallPath セクションを探し、ファイルパスも含め、その行全体を削除します。
5. ***notes.ini*** を保存して閉じます。
6. ***smd.ini*** を削除します。このファイルは、DomSvr{X}DominoBinPath で指定されたパスにあります。
7. InterScan バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、ProductPath に指定されたフォルダを削除します。このフォルダには、VSAPI とスパムメール対策で使用するウイルスパターンおよび検索エンジンファイルなど InterScan ファイルが保存されています。
8. InterScan インストールログが保存されているフォルダに移動し (226 ページの「インストールログおよびアンインストールログの確認」を参照)、ログファイルを削除します。
9. Windows サーバにインストールされた InterScan では、次のタスクを実行します。
   a. レジストリを開いて、次のアンインストールキーを削除します。

      HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥ScanMail for Domino

   b. C:¥Documents and Settings¥All Users¥ スタートメニュー¥ プログラムから Trend Micro InterScan for IBM Domino フォルダを削除します。この処理によって、[スタート] メニューから InterScan プログラムフォルダが削除されます。
   c. レジストリエディタを閉じます。
10. ***smdsys.ini*** で、指定された InterScan インスタンスをインストールするパーティションサーバの情報を削除および修正します。
    - DomSvrISMDCount

- DomSvrISMDSecs
- DomSvrX (InterScan インスタンスのパーティションサーバに関連する情報を削除)

InterScan バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、***smdsys.ini*** 内の SMDConfx インスタンスを削除します。

すべての InterScan インスタンスを対象のサーバから削除する場合は、***smdsys.ini*** を削除します。

11. Domino サーバを再起動します。

Linux に対する単一または共有 InterScan インストールの削除

ヒント : InterScan のファイルおよびフォルダ構造については、付録 B「ファイルおよびフォルダ一覧」の B-248 ページの表 B-1 を参照してください。

1. InterScan がインストールされているサーバで、***smdsysV3.ini*** を見つけ、テキストエディタを使用して開きます。後続の手順の実行時には、参照できるようにこのファイルを開いたままにしておきます。

   以降の手順では、次のパラメータを参照します。

   - DomSvr{X}
   - ProductPath

注意 : DomSvr{X} は InterScan インスタンスを表しており、{X} は InterScan インストールの番号を表します。

対象サーバに InterScan インストールが 1 つしかない場合、DomSvr{X} は DomSvr0 です。InterScan インストールが複数ある場合、{X} は 1 ずつ増えます。つまり、DomSvr0 が 1 つ目のインスタンス、DomSvr1 が 2 つ目のインスタンスというように続きます。

次に、InterScan インスタンスが複数設定されている Linux サーバの ***smdsysV3.ini*** の例を示します。

```
[SMDConf] ¥¥1 つ目の InterScan インスタンスを示しています
ProductPath=/ibm2/linux/trend/SMID
ProductVersion=V5.6 ¥¥InterScan のバージョンが 5.6 であることを示しています
InstallType=64-bit ¥¥64 ビットの InterScan であることを示しています
DomSvrISMDCount=1 ¥¥1 つ目の InterScan インスタンスのパーティションサーバの数を示しています
DomSvrISMDSecs=DomSvr0 ¥¥1 つ目の InterScan インスタンスのパーティションサーバを示しています
DomSvr0=/ibm2/linux/notesdata0/notes.ini

[SMDConf0] ¥¥2 つ目の InterScan インスタンスを示しています
ProductPath=/ibm1/trend/SMID
ProductVersion=V5.6
InstallType=64-bit
DomSvrISMDCount=2 ¥¥2 つ目の InterScan インスタンスのパーティションサーバの数を示しています
DomSvrISMDSecs=DomSvr1,DomSvr2 ¥¥2 つ目の InterScan インスタンスのパーティションサーバを示しています
DomSvr1=/ibm1/notesdata1/notes.ini
DomSvr2=/ibm1/notesdata0/notes.ini

[SMDConf1] ¥¥3 つ目の InterScan インスタンスを示しています
ProductPath=/ibm2/trend/SMID
ProductVersion=V5.6
InstallType=64-bit
DomSvrISMDCount=1 ¥¥3 つ目の InterScan インスタンスのパーティションサーバの数を示しています
DomSvrISMDSecs=DomSvr3 ¥¥3 つ目の InterScan インスタンスのパーティションサーバを示しています
DomSvr3=/ibm2/notesdata0/notes.ini
```

2. Domino バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、Domino バイナリディレクトリに移動し、次に該当する InterScan ファイルを探して削除します。
   - Linux サーバ上の Domino プログラムディレクトリ (ibmpow) にある InterScan ファイル (B-249 ページの表 B-2 を参照)
3. Domino データディレクトリに移動し、次の InterScan インストールフォルダおよび作業フォルダを削除します。
4. DomSvr{X} で指定された ***notes.ini*** をテキストエディタで開き、次を実行します。
   a. ServerTasks セクションを見つけて、次の項目を削除します。
      - SMDemf

- SMDreal
- SMDsch
- SMDmon
- SMDcm

b. `EXTMGR_ADDINS` セクションを探し、`SMDext` 項目を削除します。

c. `ScanMailInstallPath` セクションを探し、ファイルパスも含め、その行全体を削除します。

5. ***notes.ini*** を保存して閉じます。
6. InterScan バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、`ProductPath` に指定されたフォルダを削除します。このフォルダには、VSAPI とスパムメール対策で使用するウイルスパターンおよび検索エンジンファイルなどの InterScan ファイルが保存されています。
7. InterScan インストールログが保存されているフォルダに移動し (226 ページの「インストールログおよびアンインストールログの確認」を参照)、ログファイルを削除します。
8. ***smdsysV3.ini*** で、指定された InterScan インスタンスをインストールするパーティションサーバの情報を削除および修正します。
   - DomSvrISMDCount
   - DomSvrISMDSecs
   - DomSvrX (InterScan インスタンスのパーティションサーバに関連する情報を削除)

   InterScan バイナリを共有するすべてのパーティションサーバから InterScan のインスタンスを削除する場合は、***smdsysV3.ini*** 内の `SMDConfx` インスタンスを削除します。

   すべての InterScan インスタンスを対象のサーバから削除する場合は、***smdsysV3.ini*** を削除します。
9. Domino サーバを再起動します。

第 11 章

トラブルシューティング

第 11 章では、InterScan for IBM Domino (以下、InterScan) 5.6 で発生する可能性のある問題を解決する方法を説明します。

第 11 章で説明する項目は次のとおりです。

インストールログおよびアンインストールログの確認

次の表は、InterScan のインストールログとアンインストールログを示しています。

表 11-1. インストールログおよびアンインストールログ

プラットフォーム	保存場所とファイル名	説明
Windows	%windir%¥temp¥smdins.log	InterScan のインストールログ
	%windir%¥temp¥smdunins.log	InterScan のアンインストールログ
Linux	/var/log/smdins.log	InterScan のインストールログ
	/var/log/smdunins.log	InterScan のアンインストールログ

保留メールに関する問題

ここでは、保留メールに関するさまざまな問題に対処する方法について説明します。

保留メールに関する一般的な問題

保留されたメールの問題を迅速に解決するには、次の情報を判断し、収集します。

- メールボックス
- InterScan 一時ファイル。作業ディレクトリの完全なパスについては、設定データベースの [サーバ設定] 画面を参照してください。
- SMDreal デバッグファイル
- 実行されている SMDreal タスクの数

システムメールボックスの保留メールの検索と解放

SMDreal が手動で停止されている場合など、状況によっては、いくつかの検索不能メールがシステムのメールボックス `mail.box` に保留されていることがあります。このような場合は、システムのメールボックスを手動で検索して、保留されているメールを解放します。

システムのメールボックスを検索して、保留メールを解放するには

1. SMDreal サーバタスクをロードして、このスタータスが `idle` (アイドル状態) になっていることを確認します。
2. [処理] → [手動検索] → [検索するデータベース] の順に進み、検索対象リストに `mail.box` を追加します。
3. [今すぐ検索] をクリックするか、Domino コンソールで smddbs をロードします。システムのメールボックス内のすべてのメッセージが検索され、すべての保留メッセージが解放されます。

注意： システムのメールボックスの手動検索では、現在有効な InterScan ポリシーに設定されているルールが使用されます。

アップデートに関する問題

ダウンロード元からウイルス対策コンポーネントとコンテンツセキュリティコンポーネントをダウンロードするようにダウンロード元を設定している場合に、最新コンポーネントをダウンロードできないことがあります。172 ページの「ダウンロード元の設定」および 166 ページの「ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントの概要」を参照してください。

予約検索または予約アップデートに関する問題

スケジューラが予約時間に起動できなかった場合、InterScan の予約検索または予約アップデートを再実行することはできません。この問題の回避策は次のとおりです。

1. ***`notes.ini`*** にサーバ開始タスクとして smddbs または smdupd を追加します。
2. 予約検索または予約アップデートの設定に指定されているものと同じ設定を使用して、手動検索または手動アップデートの設定を指定します。

   毎晩実行されるバックアップ時など、Domino サーバが再起動するときに、smddbs または smdupd によって、予約検索または予約アップデートと同じ検索タスクまたはアップデートタスクが実行されます。

破損した InterScan データベースの復元

何らかの理由で InterScan データベースが破損した場合、データベースで整合性チェックを実行することによってデータベースの復元を試行できます。これを行うには、Domino サーバコンソールで次のコマンドを入力します。

load fixup { データベースのパスおよびファイル名 }

たとえば、破損した設定データベースを修復する場合、管理者は Domino サーバコンソールから次のコマンドを発行する必要があります。

load fixup smd¥smconf.nsf

データベースを復元できない場合は、データベースを再作成することもできます (228 ページの「データベーステンプレートを使用した InterScan データベースの再作成」を参照)。

注意： データベースの再作成によって元の内容が復元されるわけではありません。

データベーステンプレートを使用した InterScan データベースの再作成

InterScan データベースが破損し、復元不可能な場合は、対応する InterScan データベーステンプレートを使用して破損したデータベースを再作成します。

注意： InterScan データベースを再作成した場合、元の内容は復元されません。破損したデータベースが設定データベースの場合、管理者は、ポリシー、ルール、およびフィルタを再定義する必要があります (または、ローカルの設定データベースを再作成してから、別の InterScan サーバから設定データベースを複製します)。

InterScan データベースを再作成するには

1. 再作成するデータベースのテンプレート (`*.NTF`) を入手し、Domino データディレクトリに置きます。
2. Notes クライアントを起動し、InterScan データベースを含む [ワークスペース] タブを開きます。InterScan アイコンを Notes のワークスペースに追加する方法の詳細については、76 ページの「Notes ワークスペースへの InterScan データベースアイコンの追加」を参照してください。

3. 修復する InterScan データベースを選択します。
4. メインメニューから、[ファイル] → [アプリケーション] → [設計の置換] の順にクリックします。 [データベース設計の置換] ウィンドウが表示されます。
5. [テンプレートサーバー] をクリックします。
6. リストから対応するサーバをクリックして、[OK] をクリックします。
7. [詳細テンプレートの表示] チェックボックスをオンにします。
8. テンプレートリストから、破損したデータベースに対応する InterScan テンプレートを選択します。
9. [置換] をクリックします。InterScan のインストール時に使用した ID を使用してテンプレートファイルが署名されていなかった場合は、新しいデータベースにこの ID を使用して署名します。

Deep Discovery Advisor エージェントの問題

Deep Discovery Advisor エージェントが Deep Discovery Advisor に接続しない場合は、次の手順を実行します。

1. InterScan サーバが Deep Discovery Advisor に接続していることを確認します。
2. Deep Discovery Advisor 設定で API キーを確認します。詳細な設定手順については、159 ページの「Deep Discovery Advisor の設定」を参照してください。

注意： Deep Discovery Advisor の API キーがわからない場合は、Deep Discovery Advisor 管理者に問い合わせて API キーを取得してください。

InterScan タスクのデバッグ

次のいずれかのデバッグ手順を実行します。

InterScan の `SMDreal`、`SMDdbs`、`SMDmon`、`SMDsch` または `SMDcm` の各タスクをデバッグするには

Domino コンソールで次のコマンドを入力し実行します。

```
tell { 検索タスク } quit
load { 検索タスク } -debug { レベル }
```

{ レベル } は、1、2、3 のいずれかです。

InterScan の `EMfilter` タスクをデバッグするには

a. `notepad.exe` などのテキストエディタを使用して ***`notes.ini`*** を開きます。

ヒント： Domino または InterScan の `*.ini` ファイルの変更は慎重に行います。元の設定に戻すことができるように ***`notes.ini`*** のバックアップを作成しておきます。

---

b. ***`notes.ini`*** の最後のエントリとして次のパラメータを追加します。

```
SMDEMDEBUG=1
```

c. ***`notes.ini`*** を保存して閉じます。

デバッグレベル

InterScan の検索タスクでは、次のデバッグレベルを使用します。

レベル	説明
1	重大なエラーのみを表示
2	省略したデバッグ情報を表示
3	詳細なデバッグ情報を表示

注意： Extension Manager と Extension Manager フィルタのデバッグレベルは設定できません。

デバッグ結果

検索タスクのデバッグでは、次の命名規則によりログがファイルに書き込まれます。

`{ サーバタスク名 }_{yyyymmdd}.dbg`

ここで、

`{ サーバタスク名 }` は、InterScan タスクの名前です。
`{yyyymmdd}` は、ログファイルが生成された年月日です。

例 :

- Windows: nSMDreal_20040211.dbg

その他のデバッグログは次のとおりです。

- Extension Manager タスクの SMDEXT.dbg
- Extension Manager フィルタタスク (SMDEMF) の SMDEMF.dbg
- InterScan データベース設定デバッグログの <Domino データ >¥SMDTemp¥dbsetup.log

  InterScan では、Domino データディレクトリに属する ¥SMDtemp フォルダにすべてのデバッグファイルが保存されます。

InterScan のエラーメッセージの概要

Domino サーバコンソールに表示される可能性のある最も一般的な InterScan メッセージについて、次の表で説明します。

メッセージ	原因	対処方法
SMDreal: メッセージキューを作成できません。Domino サーバを再起動してください。	Domino サーバが正常に動作していない可能性があります。	Domino サーバを再起動します。
SMDreal: 共通メッセージを初期化できません。SMDreal をアンロードしてから再ロードしてください。	メッセージファイルがありません。	InterScan をいったんアンインストールし、再インストールします。
SMDreal: 検索エンジンを初期化できません。検索エンジンおよびパターンファイルを確認してください。	検索エンジンまたはパターンファイルがありません。 ***smconf.nsf*** にポリシー文書が含まれていません。	InterScan をいったんアンインストールし、再インストールします。 ***smconf.nsf*** にポリシーを作成し、smdreal を再ロードします。
SMDreal: ***notes.ini*** に Extension Manager がありません。InterScan を再インストールしてください。	誤ったインストールパッケージを使用して InterScan がインストールされました。または、InterScan が手動で削除されました。	InterScan をいったんアンインストールし、再インストールします。

メッセージ	原因	対処方法
SMDreal: アクティベーションコード番号が不正です。設定データベースを介して InterScan をアクティベートした後、SMDreal を再ロードしてください。	InterScan のインストール中にアクティベーションコードが入力されていません。または、無効なアクティベーションコードが入力されました。	[InterScan 設定データベース] → [管理] → [製品ライセンス] 文書の順にクリックして、有効なアクティベーションコードを入力します。71 ページの「InterScan の登録とアクティベーション」を参照してください。
SMDreal: 体験版の試用期間は終了しています。レジストレーションキーを取得して、InterScan をアクティベートしてください。	インストール中に体験版アクティベーションコードが入力されました。このアクティベーションコードの有効期限はすでに終了しています。	
SMDreal: ポリシーをロードできません。設定データベースを確認してから SMDreal を再ロードしてください。	設定データベースが破損している可能性があります。	InterScan を再インストールします。
SMDreal: メッセージデータベースをロードできません。***smmsg.nsf*** を確認してから SMDreal を再ロードしてください。	***smmsg.nsf*** (InterScan メッセージデータベース) が破損している可能性があります。	
SMDdbs: データベースのリスト設定が無効です。手動検索または予約検索のルール設定でデータベースリストを確認してください。	設定データベースのデータベースリストの形式が正しくありません。	[リアルタイムデータベース検索] 文書、[予約検索] 文書、または [手動検索] 文書の [検索するデータベース] リストを確認します。複数のエントリはセミコロンで区切ります。
SMDreal: Domino ディレクトリを読み取れません。サーバステータスを確認してください。	Domino サーバの完全修飾名 (FQDN) が空です。または、その他の Domino 設定が正しくありません。	Domino の設定を修正します。

メッセージ	原因	対処方法
SMDreal: データベース { データベース名 } を開けません。設定データベースでデータベース名を確認してください。	InterScan がデータベース内で特別な文書を検索しようとしましたが、データベースを開けませんでした。InterScan が検索する前にデータベースが削除された可能性があります。	必要な処理はありません。
SMDdbs: データベース検索設定を読み取れません。設定データベースを確認してください。	データベース検索の設定が正しくありません。	データベース検索ルールを確認します (94 ページの「リアルタイムデータベース検索ルールの作成」を参照)。
SMDupd: 複数の SMDupd インスタンスを実行できません。	予約アップデートタスク、手動アップデートタスク、または Control Manager サーバからのアップデートタスクが同時に実行されました。	1 つのアップデートタスクが終了した後、次のアップデートタスクを実行します。
SMDupd: 無効なパラメータです。	アップデートタスクは、3 つの異なるダウンロード元でトリガされたアップデートを表す 4 種類の形式パラメータのみを受け入れます。パラメータが必要な形式に従っていない場合に、このメッセージが表示されます。	「手動検索」文書または予約アップデートルールを確認します (144 ページの「手動検索の実行」または 167 ページの「コンポーネントのアップデート」を参照)。
SMDupd: アップデートタスクを初期化できません。	正しいアップデート設定を取得できないか、トレンドマイクロのアップデートサーバを呼び出せません。	
SMDupd: 接続をセットアップできません。ネットワーク接続を確認してください。詳細については、[InterScan ヘルプ] → [トラブルシューティング] を参照してください。	トレンドマイクロのアップデートサーバへの接続を確立できません。	ネットワーク接続、およびプロキシサーバの接続と設定を確認します。詳細については、<InterScan のインストール先パス >¥AU_Log¥TmuDump.txt を参照してください。

メッセージ	原因	対処方法
SMDupd: コンポーネントをダウンロードできません。サーバのステータスを確認してください。詳細については、[InterScan ヘルプ] → [トラブルシューティング] を参照してください。	ネットワークが混雑しています。または、ダウンロードコンポーネントの整合性チェックを実行できません。	詳細については、<InterScan のインストール先パス >¥AU_Log¥TmuDump.txtを参照してください。
SMDupd: コンポーネントをアップデートできません。アクティベーションコードの有効期限が切れています。	アクティベーションコードの有効期限が終了しています。	
SMDupd: 最新バージョンにアップデートできません。詳細については、[InterScan ヘルプ] → [トラブルシューティング] を参照してください。	トレンドマイクロのアップデートサーバへの接続を確立できません。 または、ダウンロードコンポーネントの整合性チェックを実行できません。	ネットワーク接続、およびプロキシサーバの接続と設定を確認します。 詳細については、<InterScan のインストール先パス >¥AU_Log¥TmuDump.txt を参照してください。
SMD Loader: 実行可能ファイルはサイズの上限 { サイズの上限 } を超えています。	実行可能ファイルのパス名が長すぎます。サブディレクトリの階層が深すぎることや長いファイル名を使用していることが原因である可能性があります。	短いパス名のディレクトリに InterScan を再インストールしてください。
SMD Loader: 最新プログラムのディレクトリが見つかりません。	notes.ini に ***ScanMailInstallPath*** パラメータが見つかりません。インストールが完了していない、または InterScan のファイルが手動で削除された可能性があります。	InterScan を再インストールします。 または、正しい ScanMailInstallPath パラメータとその値を ***notes.ini*** に追加します。

メッセージ	原因	対処方法
SMD Loader: 最新プログラムのディレクトリ {パス} を参照できません。	`ScanMailInstallPath` で指定されたパス名が無効なパスまたは無効なディレクトリです。	InterScan を再インストールします。 または、正しい `ScanMailInstallPath` パラメータとその値を ***`notes.ini`*** に追加します。
SMD Loader: 動的ライブラリ「%s」をロードできません。 SMDsch: スケジュールタスク「%s」を開始できません。	動的ライブラリをロードできません。これは、そのファイルがないか破損している場合、またはそのファイルに対する十分な権限がない場合に発生します。	InterScan を再インストールするします。または、有効なファイルを取得して Domino サーバ上の破損したファイルを上書きします。

第 12 章

サポート情報

トレンドマイクロは、ユーザの期待を超えるサービスとサポートの提供に尽力しています。ここでは、テクニカルサポートを受ける方法について説明します。サポートを受けるには、お使いの製品を登録する必要があることに注意してください。

第 12 章で説明する項目は次のとおりです。

製品サポート情報

InterScan for IBM Domino のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポート サービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービスの継続をご希望される場合は、契約満了前に更新されることをお勧めします。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

製品 Q&A

`http://esupport.trendmicro.co.jp/corporate/search.aspx`

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

トレンドマイクロ「セキュリティ情報」

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

`http://jp.trendmicro.com/jp/threat/index.html`

管理コンソールからセキュリティ情報 Web サイトにアクセスすることもできます。セキュリティ情報 Web サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから [セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出 / 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「セキュリティデータベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

```
http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=jp
```

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

```
http://inet.trendmicro.co.jp/esolution/attach_agreement.asp
```

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs （トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 箇所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 A

Domino 環境での脅威について

InterScan for IBM Domino (以下、InterScan) 5.6 は、既知および亜種の不正プログラムによる侵入と感染から、IBM Notes 環境のコンピュータを保護します。

この付録で説明する項目は次のとおりです。

不正プログラムの概要

不正プログラムとは、ユーザが予期していない「不正な活動」を行うプログラムのことです。ウイルスは不正プログラムの一形態です。不正プログラムのその他の例として、トロイの木馬、ワーム、バックドア、DoS 攻撃エージェント、ジョークプログラム、およびその他のより細かいカテゴリに分類される不正コードがあります。

ウイルスは、「不正 (malicious)」と「ソフトウェア (software)」という 2 つの語から作られたマルウェア (malware) とも呼ばれる大規模な不正プログラムグループの一部でしかありません。「不正」と言う場合、プログラムがユーザの認識または同意の範囲外で実行されていることを意味します。不正プログラムをすべてウイルスと呼ぶことは、実際には自動車以外の乗り物もあるのに、路上で見たあらゆる種類の乗り物を自動車と呼ぶようなものです。

「ウイルス」という言葉が、あらゆる種類の不正コードという意味で使用される場合があります。しかし、これは正確ではなく、不正コードがすべてウイルスというわけではありません。

不正なコードを表現するには、「不正プログラム (malware)」が最も適切です。不正プログラムには、次のような多くのサブカテゴリが含まれます。

- ウイルス
- ワーム
- トロイの木馬
- ジョークプログラム

以下で、各サブカテゴリについて説明します。

ウイルス

コンピュータウイルスは、増殖機能を持つコードセグメントです。通常、ウイルスはファイルに感染することによって増殖します。ファイルに感染したウイルスは、それ自身のコピーをファイルに付加し、ファイルが実行されたときに自身も起動するようなロジックを作り上げます。また、この場合、感染したファイルが他のファイルへの感染力を持つようになります。

一般的に、ウイルスには次の 3 種類があります。

- ファイル感染型

  ファイル感染型ウイルスにはさまざまな種類があります。DOS ウイルス、Windows ウイルス、マクロウイルス、およびスクリプトウイルスです。これらはすべて異なる種類のホストファイルまたはプログラムに感染する点を除いて、共通の特徴を持っています。

- ブート

  ブートウイルスは、ハードディスクのパーティションテーブルやハードディスクとフロッピーディスクのブートセクタに感染します。

- 不正スクリプト

  不正スクリプトは、Visual Basic スクリプトや JavaScript などのスクリプトプログラム言語で記述されたウイルスであり、通常、HTTP 文書に埋め込まれています。
  VB スクリプト (Visual Basic スクリプト) ウイルスおよび JavaScript ウイルスは、Microsoft の Windows スクリプトホストを利用して動作し、他のファイルに感染します。Windows スクリプトホストは Windows 98 や Windows 2000 などの Windows OS で使用可能なため、これらのウイルスは、Windows Explorer から `*.vbs` または `*.js` ファイルをダブルクリックするだけで活性化されます。
  スクリプト型ウイルスの特性は何でしょうか。アセンブリタイプのプログラミング知識が必要なプログラミングバイナリウイルスとは異なり、ウイルス作成者はスクリプト型ウイルスをテキストとしてプログラミングします。スクリプトウイルスは高度なプログラミングを必要とせず、可能な限り小さなコードで機能を達成できます。また、Windows に事前定義されているオブジェクトを使用し、感染したシステムの数多くの領域に容易にアクセスできます。この結果、ファイル感染やマスメーリングなどで感染を広げます。さらに、コードがテキストであるため、他人でも簡単に読むことができ、コードを模倣できます。この理由により、多くの不正スクリプトには、改変された複数の亜種が存在します。
  たとえば、「I love you」ウイルスが出現してまもなく、ウイルス対策製品の供給メーカーは、元のコードの変形されたコピーを検出しました。このコピーは、さまざまな件名行やメッセージ本文で拡散するウイルスでした。

これらはどのような種類であれ、基本的なしくみは同じです。ウイルスには、明示的にそれ自身をコピーするコードが含まれます。通常、ファイル感染型の場合、ユーザが感染したプログラムを誤って実行すると、コンピュータの制御を握るために何らかの改変を行います。ウイルスコードの実行が終了すると、多くの場合、制御は元のホストプログラムに返され、感染したファイルには異常がないような印象をユーザに与えます。

クロスプラットフォーム型のウイルスも存在する点に注意してください。こうした種類のウイルスは、異なるプラットフォーム (Windows と Linux など) にあるファイルに感染可能です。ただし、こうしたウイルスは非常にまれで、その機能をすべて発揮することはめったにありません。

ワーム

コンピュータワームは、自分自身またはそのセグメントの機能コピーを他のコンピュータシステムに感染させる機能を持つ自立型プログラムです。通常、感染の拡大はネットワーク接続またはメールの添付ファイルを通じて行われます。ウイルスと異なり、ワームは自分自身をホストプログラム

に付加する必要はありません。ワームは通常、伝播に、メールや Microsoft Outlook などのアプリケーションを使用します。自分のコピーを共有フォルダに置いたり、Kazaa などのファイル共有システムを利用することもあります。これらのフォルダのファイルはユーザによってダウンロードされる可能性が高いので、ワームの拡大を狙うことができるためです。また、ICQ、AIM、mIRC、その他のピアツーピア (P2P) プログラムなどのチャットアプリケーションを利用するワームも存在します。

トロイの木馬

トロイの木馬は、破壊性のあるプログラムです。一見、無害なように見えるだけでなく、興味をそそるような形 (ゲームやグラフィックアプリケーションなど) で送られてくるソフトウェアに潜んでいます。トロイの木馬が破壊的なペイロードを持たない場合があるかも知れません。そのかわり、システムまたはネットワーク全体のセキュリティを脅かすルーチンを隠し持っている可能性があります。こうした種類のトロイの木馬は、バックドア型のトロイの木馬とも呼ばれます。

トロイの木馬は、複製しない不正プログラムです。つまり、自身を複製することはなく、ユーザがトロイの木馬のコピーを他のユーザに送ることを当てにしています。このような性質から、コンピュータゲームやグラフィックソフトウェアのような魅力的なソフトウェアの内部に潜んで、初級ユーザが他のユーザに送信することを利用する場合があります。

ジョークプログラム

ジョークプログラムは、多くの場合、悪意のない一般的な実行可能プログラムです。ウイルス作成者は、コンピュータユーザをからかうためにジョークプログラムを作成します。データを破壊する意図はありませんが、経験の浅いユーザが誤ってデータの損失につながる操作を実行する可能性があります。たとえば、古いバックアップからファイルを復元したり、ドライブをフォーマットしたり、ファイルを削除したりするといった操作です。

ジョークプログラムは普通の実行可能プログラムであるため、他のプログラムに感染したり、コンピュータシステムやデータに損害を与えることはありません。たまに、マウス、キーボード、その他のデバイスを一時的に再設定するジョークプログラムもあります。しかし、ジョークプログラムの実行が終了するか、ユーザがコンピュータを再起動すると、コンピュータは元の状態に戻ります。ジョークプログラムは、通常無害である反面、組織に余計な経費負担を強いることがあります。

Web レピュテーション

Web レピュテーション機能が InterScan で提供されるようになりました。Web レピュテーション機能は、Web ページユーザのアクセスの安全性の確保、および不正プログラム、スパイウェア、ユーザをだまして個人情報を提供させるよう設計されているフィッシング詐欺などの Web からの脅威の排除に役立ちます。InterScan の Web レピュテーション機能では、評価レーティングに従って、メールに含まれる不正な URL が特定されます。また、管理者は Web レピュテーションのリストに URL を追加できます。115 ページの「Web レピュテーションの設定」を参照してください。

Web レピュテーションを有効にすると、トレンドマイクロのサーバにクエリを実行して、Web ページのリンク、ドメインと IP アドレスの関連性、スパム送信元、スパム内のリンクなど複数の情報源と相互に関連付けられているレーティングを取得します。Web レピュテーションでは、レーティングをオンラインで取得するため、有害なページをブロックするための最新情報を使用できます。Web レピュテーションは、ユーザによる不正な URL へのアクセスの防止に役立ちます。Web レピュテーションは、メッセージ本文に URL が含まれるメールを受信したときに、トレンドマイクロのサーバにクエリを実行して、評価レーティングを取得します。設定に応じて、Web レピュテーションで、不正な URL が含まれるメールの隔離、削除、またはタグ付けを実行できます。

Notes 環境に不正プログラムが拡大するしくみ

InterScan では、Notes クライアント環境が最も脆弱となる次の 3 つの侵入ポイントが継続的に検索、保護されます。

- メール送信 — InterScan では、すべての送受信メールおよびそれらの添付ファイルに対してリアルタイム検索が実行され、ユーザのシステムに不正プログラムが侵入しないように、または、他のユーザ (顧客など) のシステムに感染しないように阻止します。
- クライアントデータベースへのアクセス — InterScan では、変更されたデータベースファイルがリアルタイムで監視され、保存されているデータベース文書にウイルスが格納されないように阻止します。

- 複製 — InterScan では、Notes データベースを通じて変更されたすべてのファイルがリアルタイムでチェックされ、ウイルスが他の Notes サーバから複製されないようにします。

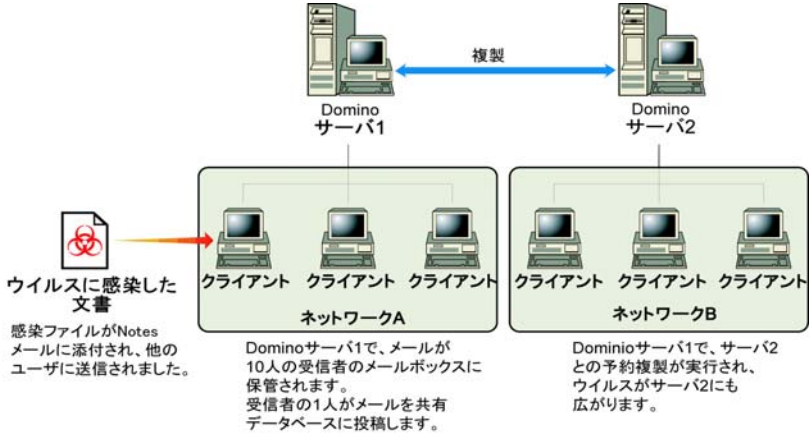


図 A-1.　Notes 環境でのウイルス感染文書の拡大

リアルタイム検索に加え、InterScan ではすべてのデータベースやメールの添付ファイルに対して手動検索または予約検索を実行し、ウイルスの再感染を防ぎます。InterScan の検索の概要については、「検索の種類」を参照してください。

付録 B

ファイルおよびフォルダー一覧

付録 B には、InterScan for IBM Domino (以下、InterScan) 5.6 のファイルとフォルダ構造の一覧を記載しています。これらのファイルとフォルダは、アプリケーションのインストールが正常に終了するとすぐに利用できます。

イントールログとアンインストールログの一覧については、226 ページの「インストールログおよびアンインストールログの確認」を参照してください。

InterScan Windows 版

Windows サーバに InterScan と Control Manager エージェントを正常にインストールしたときに作成されるファイルのリストについては、表 B-1 を参照してください。

表 B-1.　Windows サーバで使用できる InterScan のファイルとフォルダ

ファイル / フォルダ	説明
...¥IBM¥Domino ...ndbsetup.exe ...nSMDcm.exe ...nSMDdbs.exe ...nSMDDTAS.exe ...nSMDEUQ.exe ...nSMDemf.exe ...nSMDext.dll ...nSMDmon.exe ...nSMDreal.exe ...nSMDsch.exe ...nSMDsupp.exe ...nSMDupd.exe ...smd.ini	InterScan ローダ、フィルタ、Extension Manager、エンドユーザメール隔離、dbsetup、および InterScan 設定のファイルを格納
...WINDOWS¥smdsys.ini	InterScan のメイン設定ファイル。
...¥Program Files¥Trend Micro¥ScanMail for Domino	InterScan の初期設定のインストールフォルダ。
...¥engine	Trend Micro スパムメール検索エンジン (TMASE) とウイルス検索エンジンのフォルダを格納
...¥engine¥atse	トレンドマイクロの高度な脅威検索エンジンを格納
...¥engine¥tmase	TMASE を格納
...¥engine¥tmufe	URL フィルタエンジンが含まれます。
...¥engine¥vsapi	トレンドマイクロの検索エンジンを格納
...¥pattern	TMASE とウイルス検索ルール / パターンのフォルダを格納
...¥pattern¥tmase	TMASE のルールファイルを格納

表 B-1. Windows サーバで使用できる InterScan のファイルとフォルダ (続き)

ファイル / フォルダ	説明
...¥pattern¥vsapi	ウイルスパターンファイル、スパイウェアパターンファイル、および IntelliTrap パターンファイルが含まれます。
...¥program	InterScan の Readme ファイル、およびバイナリファイルと設定ファイルのフォルダが含まれます。
...¥program¥V5.#.#.####	InterScan のバイナリファイルと設定ファイルを格納
...¥Uninstall	InterScan のアンインストールプログラムを格納
...IBM¥Domino¥Data¥smd	Domino データディレクトリ内に、InterScan データベースとテンプレートを格納
...IBM¥Domino¥Data¥smdtemp	Domino データディレクトリ内に、セットアップの ***dbsetup.log***、および InterScan の検索タスクで使用される一時ファイルを格納
...IBM¥Domino¥Data¥smd¥smtemp	検索対象の一時ファイルを解凍するための InterScan フォルダ

InterScan Linux 版

Linux サーバに InterScan と Control Manager エージェントを正常にインストールしたときに作成されるファイルのリストについては、表 B-2 を参照してください。

表 B-2. Linux サーバで使用できる InterScan のファイルとフォルダ

ファイル / フォルダ	説明
/etc/smdsysV3.ini	InterScan のメイン設定ファイル
/opt/trend/SMID/	InterScan の初期設定のインストールフォルダ。ただし、インストールは、他の任意のフォルダで実行できます。
.../engine/atse	トレンドマイクロの高度な脅威検索エンジンを格納
.../engine/tmase	TMASE を格納
.../engine/vsapi	トレンドマイクロの検索エンジンを格納
.../pattern/tmase	TMASE のルールファイルを格納

表 B-2. Linux サーバで使用できる InterScan のファイルとフォルダ (続き)

ファイル / フォルダ	説明
.../pattern/vsapi	ウイルスパターンファイル、スパイウェアパターンファイル、および IntelliTrap パターンファイルを格納
.../engine/tmufe	URL フィルタエンジンを格納
.../program	InterScan の Readme ファイル、およびバイナリファイルと設定ファイルのフォルダを格納
.../program/V5.#.#.####	InterScan のバイナリファイルと設定ファイルを格納 ここで、 • .#.# (最初の 2 つの #) はマイナーバージョンを示します。 • .#### (最後の 4 つの #) はビルド番号を示します。
/opt/lotus/notes/latest/ibmpow ...libsmdext.a ...smdcm ...smddbs ...smddtas ...smdeuq ...smdemf ...smdmon ...smdreal ...smdsch ...smdsupp ...smdupd	Domino プログラムディレクトリの InterScan 設定ファイル、バイナリファイル、およびデータベースファイルを格納。ただし、Domino プログラムディレクトリには、他の任意のフォルダを指定することができます。
.../smd	Domino データディレクトリ内に、InterScan データベースとテンプレートを格納
.../smdtemp	Domino データディレクトリ内に、セットアップの ***dbsetup.log***、および InterScan の検索タスクで使用される一時ファイルを格納
.../smd/smtemp	検索対象の一時ファイルを解凍するために使用される InterScan の Domino データディレクトリ内の初期設定フォルダ

付録 C

バージョン 5.5 およびバージョン 5.6 の機能比較

次の表は、InterScan for Lotus Domino (以下、InterScan) 5.5 と InterScan for IBM Domino 5.6 の比較を示しています。ただし、情報は各バージョンリリース当初のものです。

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較

機能	InterScan 5.5	InterScan 5.6
インストール / プラットフォームのサポート		
Domino 6.5.x のサポート	なし	なし
Domino 6.0.x のサポート	なし	なし
Domino 5.0.13a、5.0.12、5.0.11 のサポート	なし	なし
Domino 7.0.2、7.0.3、8.0 のサポート	なし	なし
Domino 8.0.1、8.0.2、8.5、8.5.1、8.5.2、8.5.3、8.5.4、9 のサポート	あり	あり
Linux 32 ビットおよび 64 ビットのサポート	あり	あり
クラスタサーバのサポート (各サーバ上のタスクと信頼を伴う完全なサポート)	あり	あり
パーティションサーバのサポート	あり	あり
複数のパーティションへの同時インストール	あり	あり
すべてのプラットフォームへのスクリプト化された / サイレントインストール	あり	あり
インストール時の複製の準備	あり	あり
インストール時のアクセス制御リストの設定	あり	あり
インストール時のデータベースへの署名	なし	なし
代替 ID/ パスワードを使用したデータベースへの署名または署名の省略	なし	なし
プラットフォーム間での設定データベースの複製	あり	あり
インストールのパラメータ化のサポート	あり	あり
複数インスタンスのサポート	あり	あり
新しい Trend Micro Control Manager および Management Communication Protocol (MCP) エージェントのサポート	あり	あり
サポートされる Domino アプリケーション		
IBM Domino データベース (.nsf)	あり	あり
IBM Domino Web Access (以前の iNotes Web Access)	制限あり	制限あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
ネイティブ 64 ビットのサポート	あり	あり
製品のアクティベーション		
トレンドマイクロのオンライン登録システム	あり	あり
アクティベーションコードの使用	あり	あり
アクティベーションコード (情報漏えい対策付きスイート)	あり	あり
検索 (一般)		
マルチスレッド検索	あり	あり
マルチスレッド検索タスク	あり	あり
アドウェア / スパイウェアに対する個別処理	あり	あり
メール検索		
リアルタイム検索	あり	あり
高度な脅威検索	あり	あり
メール送信者 / 受信者に基づいたメール検索ルール	あり	あり
除外するユーザ / グループに対する個別の検索設定	あり	あり
設定内容と時間を変えて複数指定できる予約検索	あり	あり
検出時のウイルス駆除	あり	あり
検出時の処理の設定	あり	あり
ネストされた圧縮ファイルの検索時の検索レベルの選択	あり	あり
MIME/HTML 本文のスクリプトウイルスの検索	あり	あり
不正な Notes スクリプト、ホットスポット、および URL の検索	あり	あり
署名ベースの検索	あり	あり
信頼するウイルス対策済みサーバの再検索回避のサポート	あり	あり
埋め込み OLE オブジェクトの選択的検索	あり	あり
IntelliTrap のサポート	あり	あり
Microsoft Office 2007 のサポート	あり	あり
Microsoft Office 2010 のサポート	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
RAR、SFX、CHM、NSIS、および ZIP SFX ファイルの解凍アルゴリズムのサポート	あり	あり
スパムメール対策		
スパム対策のサポート	あり	あり
エンドユーザメール隔離	あり	あり
指定したユーザ / グループに対するエンドユーザメール隔離の有効可	なし	あり
メールテンプレートへのエンドユーザメール隔離の導入	なし	あり
Web レピュテーション		
Web レピュテーションのサポート	あり	あり
ローカル Web レピュテーションのサポート	あり	あり
Web レピュテーションの通知	なし	あり
アドウェアの検出		
検出時の処理の設定	あり	あり
スパイウェアの検出		
検出時の処理の設定	あり	あり
メール / 帯域幅の管理		
承認のためのメールの転送	あり	あり
ファイルタイプによるグループ分けの選択	あり	あり
APT 対策フィルタ	あり	あり
実際のファイルタイプによる添付ファイルブロックの設定 (個々のファイルタイプ)	あり	あり
Microsoft Office マクロに対する処理の設定	あり	あり
拡張子またはファイル名による添付ファイルブロックの設定	あり	あり
実際のファイルタイプによる添付ファイルブロックの設定 (グループ)	あり	あり
Microsoft Office 文書からのマクロの除去	あり	あり
指定のスケジュールに基づいたメールの遅延	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
サイズに基づいたメールのブロック	あり	あり
優先度を低くする機能	あり	あり
添付ファイルの実際のファイルタイプに基づいたメールのブロック	あり	あり
添付ファイルのファイル名または拡張子名に基づいたメールのブロック	あり	あり
コンテンツフィルタ		
メッセージヘッダフィールドの検索	あり	あり
メッセージ本文のテキストのフィルタ処理	あり	あり
メッセージの添付ファイル内のテキストのフィルタ処理	あり	あり
正規表現のサポート	あり	あり
Microsoft Office 2007 ファイルのサポート	あり	あり
Microsoft Office 2010 ファイルのサポート	あり	あり
上限が 20 レベルの OLE 埋め込み層検索の追加サポート	あり	あり
ヒューリスティック検索テクノロジの使用	あり	あり
許可する / ブロックする送信者リストのサポート	あり	あり
フィルタレベルの設定	あり	あり
ルールファイルの使用	あり	あり
リアルタイム検索	あり	あり
予約検索	あり	あり
手動検索	あり	あり
リアルタイム検索設定が複数ある場合の期間の設定	あり	あり
リアルタイム検索でのスクリプト検索のサポート	あり	あり
指定の期間内の予約検索 (検索時間の上限)	あり	あり
設定が異なる複数の予約検索のサポート	あり	あり
完了しなかった検索の再開	あり	あり
予約検索でのスクリプト検索のサポート	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
設定データベースからの検索スケジュールの設定	あり	あり
情報漏えい対策フィルタ		
メッセージヘッダフィールドの検索	あり	あり
メッセージ本文のテキストのフィルタ処理	あり	あり
メッセージの添付ファイル内のテキストのフィルタ処理	あり	あり
Microsoft Office 2007/2010 ファイルのサポート	あり	あり
上限が 20 レベルの OLE 埋め込み層検索の追加サポート	あり	あり
ヒューリスティック検索テクノロジの使用	あり	あり
すべての情報漏えい対策フィルタから除外するファイル名の指定	あり	あり
フィルタレベルの設定	あり	あり
ルールファイルの使用	あり	あり
リアルタイム検索	あり	あり
予約検索	あり	あり
手動検索	あり	あり
リアルタイム検索設定が複数ある場合の期間の設定	あり	あり
リアルタイム検索でのスクリプト検索のサポート	あり	あり
指定の期間内の予約検索 (検索時間の上限)	あり	あり
設定が異なる複数の予約検索のサポート	あり	あり
完了しなかった検索の再開	あり	あり
予約検索でのスクリプト検索のサポート	あり	あり
設定データベースからの検索スケジュールの設定	あり	あり
管理		
R6/5 Administrator クライアントおよび Notes クライアントとの完全な連携	なし	なし
Lotus Notes 7/8 のサポート	あり	あり
IBM Notes 9 のサポート	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
Web インタフェースを使用したリモート管理	あり	あり
Notes クライアントからのリモート管理	あり	あり
ユーザインタフェースでのフレームの使用と最新のトレンドマイクロ規格への準拠	あり	あり
ユーザインタフェースを使用したサーバステータスの監視	あり	あり
サーバタスクの監視	あり	あり
タスクステータスの監視	あり	あり
サーバおよびサーバグループ間でのサーバ設定およびウイルス対策ポリシーの共有	あり	あり
処理を定義するためにユーザが定義し管理するルール	あり	あり
ユーザおよびグループに基づいたルールの定義	あり	あり
ポリシーに依存しないサーバ設定	あり	あり
Notes インタフェースから設定可能な役割ベースのアクセス制御	あり	あり
ボタン 1 つの情報コレクタ (サポートツール)	あり	あり
ウイルス対策コンポーネントおよびコンテンツセキュリティコンポーネントのアップデート		
手動アップデート	あり	あり
コンポーネントの選択および定期的な予約アップデートの設定	あり	あり
トレンドマイクロのアップデートサーバを使用したパターンファイルの自動アップデート	あり	あり
トレンドマイクロのアップデートサーバを使用した検索エンジンの自動アップデート	あり	あり
トレンドマイクロのアップデートサーバを使用したプログラムの自動アップデート	あり	あり
アップデート後のパターンファイル / 検索エンジンの整合性チェック	あり	あり
アップデート後の製品の整合性チェック	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
トレンドマイクロのスパムメール検索エンジンに対する部分的および完全なパターンファイルのダウンロードのサポート	あり	あり
IntelliTrap パターンファイルのアップデートのサポート	あり	あり
通知オプション		
通知のカスタマイズ	あり	あり
IBM Instant Messagingを使用した通知 (InterScan for Domino Windows 版のみ)	あり	あり
送信者、受信者、または管理者への通知	あり	あり
内部ユーザと外部ユーザへの別々の通知	あり	あり
リッチテキストによるメッセージの設定	あり	あり
MIME メールへの通知挿入のサポート	あり	あり
メッセージ件名への安全スタンプの挿入	あり	あり
Notes メッセージ本文への安全スタンプの挿入	あり	あり
SMTP メッセージ本文への安全スタンプの挿入	あり	あり
複数の検査証明 (ディスクレーマー) のサポート	あり	あり
メールが複数のサーバを通過する際の 1 つの検査証明 (ディスクレーマー) の挿入	あり	あり
検査証明 (ディスクレーマー) の位置設定のサポート	あり	あり
隔離		
種類、保存期間、および保持する記録に基づいた隔離ログの自動削除	あり	あり
隔離アイテムの再送信 / 復元のサポート	あり	あり
隔離アイテムの転送のサポート	なし	あり
ログ / 統計		
Microsoft Excel スプレッドシートへの統計のエクスポート	あり	あり
ログの自動削除	あり	あり
感染したメッセージの送信者の特定	あり	あり
感染ファイルの特定	あり	あり

表 C-1. InterScan 5.5 と InterScan 5.6 の機能の比較 (続き)

機能	InterScan 5.5	InterScan 5.6
Threat Connect 情報ポータルへのアクセスのサポート	あり	あり
受信者情報の記録	あり	あり
脅威に対する処理の記録	あり	あり
グラフィカルなメール統計 / レポート	あり	あり
ログ検索	なし	あり

索引

英数字

あ

か

さ

た

は

ま

ら

わ