

Trend Micro InterScan™ for Domino



管理者ガイド



本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、GateLock、VSAPI、eDoctor、eManager、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、Certified Rescue Partner、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、RBL+、Phish Checker、スパイバスター、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPSは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 1999-2007 Trend Micro Incorporated. All rights reserved.

P/N ISDFFF-AE0103 (2007/07)

目次

はじめに

バージョン 3.0 の新機能	12
対象プラットフォーム	17
対象読者	17
ドキュメントの表記規則	17

第 1 章：製品の概要

製品の概要	20
InterScan の機能 (スタンダード版)	22
InterScan の機能 (スイート版)	23
InterScan の機能	24
InterScan の構成要素	26
検索の種類	26
メール検索	27
リアルタイムデータベース検索	27
手動と予約によるデータベース検索	28
ポリシー、ルール、フィルタの概要	29
InterScan のルール	30
InterScan のフィルタ	31
InterScan によるセキュリティ戦略	32
ポリシーベースのウイルス対策計画	32
ポリシーベース環境におけるルールとフィルタの実装の計画	33

第 2 章：InterScan のインストール

導入計画	36
試験的な導入	37
導入の準備	38
対象サイトの選択	38
ロールバック計画の作成	38
インストールと評価	39
バージョン 2.5x または 2.6x からのアップグレード	39
推奨システム要件	40
InterScan のインストール	44

インストールの準備	45
英語以外の環境での InterScan のインストール (i5/OS および OS/400 プラットフォームのみ)	50
セットアップモード	51
セットアップオプション	52
ウィザードベースのインストールの実行	53
サイレントインストールの実行	66
コンソールベースのインストールの実行	71
Domino サーバの起動	83
他のウイルス対策製品を使用している場合の注意	85
InterScan のアクティベーション	85
アクティベーションコード	85
アクティベーションの実行	86
製品版へのアップグレード	87
EICAR によるインストールのテスト	87
インストール後のファイルとフォルダの確認	88

第 3 章： InterScan 用 Control Manager エージェントのインストール

InterScan 用 Control Manager エージェントのインストール	90
バージョン 2.5x または 2.6x からのアップグレード	90
インストールの準備	91
公開鍵 (E2Epublic.dat) の入手	92
セットアップモード	92
ウィザードベースのインストールの実行	94
コンソールベースのインストールの実行	103
Control Manager エージェントのインストールの確認	110
Control Manager エージェントインストール後の InterScan ファイルおよびフォルダの確認	111

第 4 章： 基本設定

InterScan のインタフェースの概要	114
ヘルプデータベースおよびヒントへのアクセス	115
インストール後の手動検索の実行	116
Notes ワークスペースへの InterScan データベースアイコンの追加	116
データベースへの署名	117
InterScan データベースへのアクセス権およびロールの定義	118
InterScan データベースへのアクセス	120

Notes クライアントを使用したデータベースへのアクセス	120
Web ブラウザを使用したデータベースへのアクセス	122
Web アクセスの制限事項	123
Web アクセスするためのインターネットパスワードの設定	124
その他のデータベースへのアクセス	124

第 5 章： 検索タスクの設定

ポリシーベースのウイルス対策計画	128
ポリシーベースのウイルス対策	129
ポリシーの管理	130
ポリシーの作成	130
ポリシーの変更	132
ポリシーの削除	132
信頼するクラスターサーバの設定	133
ルール作成	136
メール検索ルールの作成	136
最も厳しいルールの適用	139
一般の設定	140
データベースのリアルタイム検索ルールの作成	142
データベースの予約検索ルールの作成	145
ルールの整理	148
ルールの優先度の変更	149
ルールの演算子	149
フィルタについて	150
フィルタ処理の順序	150
スパムメールフィルタ (スイート版のみ)	152
コンテンツフィルタ	154
キーワード	155
スパムメールフィルタの設定	156
検索オプションの設定	159
ウイルス検索の設定	159
検索制限の設定	162
メッセージフィルタの設定	163
コンテンツフィルタの設定	164
既存フィルタを利用したコンテンツフィルタの追加	167
新規キーワードの作成	167
既存キーワードを利用したキーワードの追加	168

添付ファイルフィルタの設定	169
スクリプトフィルタの設定	172
転送オプションの設定	174
検査証明の挿入	175
検索スケジュールの設定	176
手動データベース検索の実行	176
Domino サーバコンソールからの手動検索の実行	176
設定データベースからの手動検索の実行	177
手動検索の停止	179

第 6 章： 管理の設定

すべてのサーバの概要の表示	182
[サーバ設定] 画面	183
サーバ設定の作成	184
サーバ設定の変更	184
サーバ設定の設定	185
検索に使用するディレクトリの設定	185
検索に使用するメモリサイズの設定	186
プロキシサーバの設定	187
サーバタスクモニタの有効化	188
サーバイベントのモニタ	188
初期設定の文字セットの指定	189
その他の設定	189
[管理] 画面	192
データベース設定	192
Domino Administrator からのタスクの表示	193
Domino 6 Web Administrator ページへの統合	193
アクセス制御リストのエントリの新規作成と適用	194
ライセンスプロファイルの作成	195
ライセンスプロファイルの削除	195

第 7 章： アップデート

ウイルス対策 / コンテンツセキュリティコンポーネントの概要	198
アップデートの実行	199
手動アップデート	199
予約アップデートルールを使用した自動アップデート	200
特定のコンポーネントの自動配信	202

アップデートの設定	204
コンポーネントの選択	204
ダウンロード元の設定	206
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を設定	208
 第 8 章： 通知	
通知の概要	210
通知のカスタマイズ	211
メールスタンプ (安全スタンプ) の使用	213
通知の設定	214
通知の配信方法の設定	214
検索通知の設定	216
アップデート通知の設定	216
 第 9 章： ログデータベースおよび隔離データベース	
ログデータベースの使用	220
InterScan のログの管理	220
ログ削除の有効化 / 無効化	222
ウイルスログの予約削除	223
ウイルスログの手動削除	225
統計とグラフの表示	227
統計の生成、表示、およびエクスポート	227
グラフの生成および表示	228
隔離データベースの使用	231
隔離メッセージまたは隔離添付ファイルの表示	231
隔離メッセージの再送信	232
隔離文書の復元	233
隔離された項目の削除の有効化および無効化	234
隔離ログの予約削除	235
隔離ログの手動削除	236
 第 10 章： Trend Micro Control Manager からの管理	
Control Manager について	240
主要な機能	240
Control Manager からの集中管理	241
Control Manager エージェントについて	242

トレンドマイクロ 大規模感染予防サービスについて	243
Control Manager を使用した InterScan の管理	244
Control Manager 管理コンソールへのアクセス	244
Control Manager 管理コンソールからの InterScan の設定	245
有効な大規模感染予防ポリシーの表示	247
期限切れ大規模感染予防ポリシーの削除	248

第 11 章： アンインストール

InterScan のアンインストール	250
InterScan の自動アンインストール	250
ウィザードベースのアンインストール	250
コンソールベースのアンインストール	253
単一または共有 InterScan の手動アンインストール	256
InterScan 用 Control Manager エージェントのアンインストール	261
ウィザードベースでのアンインストール	261
コンソールベースでのアンインストールの実行	263
TMI のアンインストール	264

第 12 章： トラブルシューティング

インストールログおよびアンインストールログの場所	268
AIX および Solaris 版における Control Manager サーバへの登録の問題	269
保留メールの問題	269
一般的な保留メールの問題	269
システムメールボックス内の保留メールの検索および配信	270
アップデートの問題	270
予約検索 / アップデートの問題	272
破損した InterScan データベースの修復	272
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	274
InterScan タスクのデバッグ	275
デバッグレベル	276
デバッグ結果	276
InterScan 用 Control Manager エージェントのデバッグ	277
デバッグログの収集	278
InterScan のエラーメッセージについて	281

第 13 章： 製品サポート情報

サポートサービスについて	288
製品 Q&A のご案内	289
セキュリティ情報	290
セキュリティ情報の入手先	290
トレンドマイクロへのウイルス解析依頼	291
ウイルス解析サポートセンター「TrendLabs」	291
 付録 A： Domino 環境での脅威について	
不正プログラムの概要	294
ウイルス	294
ワーム	296
トロイの木馬	296
ジョークプログラム	297
Notes 環境での不正プログラムの拡大	297
 付録 B： Control Manager エージェントのチェックリスト	
 付録 C： ファイルおよびフォルダー一覧	
Windows サーバにインストールされるファイル	302
Linux/Solaris/AIX サーバにインストールされるファイル	304
i5/OS および OS/400 サーバにインストールされるファイル	306
 付録 D： バージョン 2.6 および 3.0 の機能比較	

はじめに

この管理者ガイドでは、Trend Micro InterScan for Domino 3.0 (以下、InterScan) のインストールとアンインストール手順、および InterScan の機能を設定する方法について説明します。

InterScan 管理者ガイドで説明する主な項目は次のとおりです。

- 「製品の概要」— InterScan の機能の概要、およびこのリリースで提供される新機能について説明します。
- 「InterScan のインストール」— InterScan のインストール方法について説明します。
- 「InterScan 用 Control Manager エージェントのインストール」— InterScan 用 Control Manager エージェントのインストール方法について説明します。
- 「基本設定」— InterScan インストール後の推奨される設定手順について説明します。
- 「検索タスクの設定」— InterScan で Domino 環境を保護するため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。
- 「管理の設定」— サーバステータスの監視、Domino サーバ / サーバグループの設定、データベース管理の設定の手順を説明します。
- 「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更新する手順を説明します。
- 「通知」— InterScan 通知を送信する手順を説明します。
- 「ログデータベースおよび隔離データベース」— それぞれの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。
- 「Trend Micro Control Manager からの管理」— Trend Micro Control Manager を使用して InterScan を管理する方法を詳しく説明します。
- 「アンインストール」— InterScan をアンインストールする手順を説明します。

- 「トラブルシューティング」— 問題が発生した場合の対応策を説明します。
- 「製品サポート情報」— 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。

- 「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。
- 「Control Manager エージェントのチェックリスト」— InterScan の操作の最適化とパフォーマンスの最大化に役立つベストプラクティスを示します。
- 「ファイルおよびフォルダー一覧」— InterScan および InterScan 用 Control Manager をインストールした際に作成されるファイルおよびフォルダについてまとめてあります。
- 「バージョン 2.6 および 3.0 の機能比較」— InterScan 3.0 と旧バージョン 2.6 との機能の比較についてまとめてあります。

バージョン 3.0 の新機能

InterScan は、Domino 環境向けの強固なウイルス対策機能とコンテンツセキュリティ機能を備えています。InterScan スイート版は、ヒューリスティックベースの検索や、許可する送信者 / ブロックする送信者リストのマッチング、および署名データベースに基づく最新の検出機能を備えています。また、カスタマイズ可能なスパムメールフィルタおよびコンテンツフィルタ機能を備えており、組織のニーズに応じて利用できます。バージョン 3.0 における高機能化により、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。

注意： Windows、Linux、Solaris、および AIX 版向けにはスイート版のみの提供となります。i5/OS および OS/400 プラットフォーム向けにはスタンダード版のみの提供となります。

また、i5/OS および OS/400 プラットフォーム向け製品は英語版での提供となります。

InterScan 3.0 には、次の新機能があります。

- 「コマンドラインからの自動 (サイレント) インストールのサポート」

-
- 「ポリシーベースの設定」
 - 「InterScan データベースのユーザインタフェースの改良」
 - 「カスタマイズ可能なスパムメールフィルタ」
 - 「新しい検索オプション」
 - 「検索オプション設定に一致したメッセージの遅延配信または転送」
 - 「クラスタを構成するサーバに対する信頼」
 - 「Lotus Instant Messaging/Web Conferencing 通知のサポート」
 - 「通知のカスタマイズに役立つタグのサポート」
 - 「統計の向上」
 - 「新しいデバッグレベルの採用」
 - 「トレンドマイクロの新しい製品登録システムのサポート」
 - 「Domino 5.x のサポート停止」

コマンドラインからの自動 (サイレント) インストールのサポート

事前に記録された応答ファイル (インストールスクリプト) を使用して、複数の InterScan サーバでサイレントインストールまたはサイレントアップデートを実行することにより、簡単に自動化されたインストールを実現できます。

詳細については、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。

ポリシーベースの設定

ポリシーベースの設定は、メール検索、リアルタイムデータベース検索、予約データベース検索、および予約アップデートに適用されます。ポリシーにより、InterScan がスパムメールとデータベースを検索する方法、および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予約に基づいてアップデートする方法が決まります。ポリシーを使用すると、既存の設定と同じ設定または類似の設定をサーバグループに適用することで、管理の手間を省くことができます。

詳細については、128 ページの「ポリシーベースのウイルス対策計画」を参照してください。

InterScan データベースのユーザインタフェースの改良

InterScan の設定データベース、アップデートデータベース、ログデータベース、および隔離データベースのユーザインタフェースが改良され、管理と保守が容易になりました。

詳細については、114 ページの「InterScan のインタフェースの概要」を参照してください。

カスタマイズ可能なスパムメールフィルタ

InterScan では、スパムメールを検出するときに、スパムメール検索エンジンを使用して学習ベースのルールが適用されます。また、ユーザが許可した送信者からのメッセージを自動的に通過させるとき、およびブロックと指定されている送信者からのメッセージをブロックするときにも、同様のルールが適用されます。

スパムメール対策機能の設定方法については、156 ページの「スパムメールフィルタの設定」を参照してください。

新しい検索オプション

本バージョンでは、次のような検索オプションが追加されています。

- **トレンドマイクロの推奨処理** — 不正プログラムのタイプを識別し、そのタイプがコンピュータシステムまたは環境に感染する方法に基づいて、推奨される処理を提示します。

ウイルスなどの不正プログラムは、悪意のあるコード、複製、およびペイロードの各タイプに分類されます。ウイルスが検出されると、そのウイルスカテゴリに推奨されている処理（駆除、隔離、削除）が実行されるので、ユーザ環境の脆弱な個所を保護できます。

- **スクリプトフィルタの設定** — 設定済みユーザによって文書内のホットスポットが署名されている場合は、スクリプト検索が省略されます。
- **ファイルタイプまたはそのグループによる検索およびブロック**
- **20 レベルまでの圧縮ファイルの検索とブロック**

詳細については、150 ページの「フィルタについて」を参照してください。

検索オプション設定に一致したメッセージの遅延配信または転送

検索とフィルタの処理に、「転送」と「遅延配信」という 2 つの処理が追加されました。

-
- 転送 — 設定した承認者から承認を得るためにメッセージを転送することです。たとえば、メール管理者または部署のマネージャを承認者として設定します。転送されたメッセージに対し、承認者は配信を許可するか、ブロックすることができます。
 - 遅延配信 — メッセージを予約設定に従って配信することです。

InterScan の処理の詳細については、174 ページの「転送オプションの設定」を参照してください。

クラスタを構成するサーバに対する信頼

ポリシーを使用すると、クラスタネットワークを効率的に管理できます。クラスタサーバ間の関係を信頼するためのポリシーを設定します。

詳細については、133 ページの「信頼するクラスタサーバの設定」を参照してください。

Lotus Instant Messaging/Web Conferencing 通知のサポート

InterScan は、Lotus Instant Messaging/Web Conferencing (以前の名称は Sametime Connect) 通知の機能を備えており、ウイルス検出、フィルター一致、アップデート、ポリシー関連イベントなどを管理者に通知します。ポリシー作成時に、Lotus Instant Messaging の IP アドレス、ユーザ名、およびパスワードを指定します。これにより、管理者は Lotus Instant Messaging から InterScan 通知を受信できます。

詳細については、214 ページの「通知の配信方法の設定」を参照してください。

注意：この新機能は、Windows 版でのみ提供されます。

通知のカスタマイズに役立つタグのサポート

検出されたウイルス、ウイルスパターンファイルと検索エンジンのバージョンなどの詳細情報を通知に記述するにはタグを使用します。

詳細については、211 ページの「通知のカスタマイズ」および 214 ページの「通知の設定」を参照してください。

統計の向上

InterScan ログデータベースでは、次の統計が得られます。

- ウイルス検索
- 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памメールフィルタ
- 大規模感染予防フィルタ
- フィルタ
- 転送されたメッセージ

さらに、ログデータベースの情報が棒グラフで表示されます。

詳細については、227 ページの「統計とグラフの表示」を参照してください。

新しいデバッグレベルの採用

InterScan の SMDreal、SMDdb、SMDmon の各タスク向けに 3 つのデバッグレベルが提供され、より細部にわたるデバッグが可能になりました。

詳細については、275 ページの「InterScan タスクのデバッグ」を参照してください。

トレンドマイクロの新しい製品登録システムのサポート

従来のシリアル番号に代わり、アクティベーションコードを使用して製品をインストールします。

詳細については、85 ページの「InterScan のアクティベーション」を参照してください。

対象プラットフォーム

InterScan はマルチプラットフォーム対応製品です。現時点でリリースされている日本語版製品は、Windows 版、Linux 版、AIX 版、および Solaris 版です。i5/OS および OS/400 版は英語版のみ提供されています (2007 年 6 月現在)。

対象読者

InterScan のマニュアルは、セキュリティシステムと、Lotus Domino のメールおよび情報共有システム機能の管理について基本的な知識を持つ読者を対象としています。管理者ガイドと Domino ベースのオンラインヘルプは、Domino 管理者およびネットワーク管理者を対象としています。

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、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

表 1. 本書で使用している表記規則

製品の概要

Trend Micro InterScan for Domino 3.0 (以下、InterScan) は、Lotus/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します。

スイート版では、画期的なスパムメール対策技術やシステムによるコンテンツフィルタを利用した新たな保護レイヤを提供しています。スイート版では、リアルタイムでメール検索を実行してから、スパムメール検出やコンテンツフィルタを実行します。

この章で説明する項目は次のとおりです。

- 20 ページの「製品の概要」
- 26 ページの「検索の種類」
- 29 ページの「ポリシー、ルール、フィルタの概要」
- 32 ページの「InterScan によるセキュリティ戦略」
- 32 ページの「ポリシーベースのウイルス対策計画」

製品の概要

InterScan により、ウイルス、不正コード、不要なデータ、およびスパムメールが、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システムをリアルタイムで保護します。不正プログラムの検索は、メモリ内で実行され、それにより、検索速度が著しく向上します。

InterScan は、ネイティブな Domino サーバアプリケーションとして動作するように設計されているので、管理者にとって親しみやすく、直感的に使用できるインタフェースを備えています。InterScan の設定インタフェースは、Domino サーバに統合されており、Notes ワークステーション、Web ブラウザ、または Domino 管理クライアントによるリモート管理をサポートしています。

InterScan は、次のプラットフォームで動作します。

- Microsoft Windows
- Sun Solaris
- x86 プラットフォームの Red Hat Enterprise Linux および Novell SUSE Linux
- IBM AIX
- IBM i5/OS および IBM OS/400

スタンダード版では様々なモードでのウイルス検索とコンポーネントアップグレードが提供されます。スイート版では、さらにコンテンツフィルタとスパムメールフィルタの機能も利用できます。

注意： Windows、Linux、Solaris、および AIX 版向けにはスイート版のみの提供となります。i5/OS および OS/400 プラットフォーム向けにはスタンダード版のみの提供となります。また、i5/OS および OS/400 プラットフォーム向け製品は英語版での提供となります。

InterScan は、トレンドマイクロの集中管理コンソールである Trend Micro Control Manager (以下、Control Manager) と互換性をもち、それによってウイルス対策とコンテンツセキュリティ保護を統合的なソリューションにすることができます。

管理者は、検索対象とするデータベースを特定でき、感染していない文書を感染ファイルで上書きしないようにユーザを保護します。データベースの手動検索により、既存の感染ファイルを駆除します。

InterScan を使用することにより、管理者が企業のメールポリシーを適用し、総合的なサーバ効率を改善し、ウイルス大規模感染を抑制する手助けとなります。管理者は、特定のファイルタイプをブロックし、メッセージをブロック / 遅延配信したり、メッセージに優先度を設けたりするルールを作成できます。企業のポリシーを実行して、複数の方法で不正プログラムのインシデントを処理できます。

- 感染ファイルを隔離してから、駆除などの処理を実行
- ファイルがウイルスに感染していて駆除されていない旨を伝える通知とともに、感染アイテムを対象受信者に送信
- 感染ファイルを削除
- 感染ファイルをブロックしてその配信を阻止
- 管理者に警告を送信

マルチスレッドの検索エンジンと、検索に使用されるメモリのサイズを設定できる検索用メモリを使用することにより、処理速度を向上し、サーバのパフォーマンスへの影響を最小限に抑えられます。管理者はまた、検索不要なサーバを指定することで、検索時間を短縮できます。

InterScan の機能 (スタンダード版)

InterScan スタンダード版には、次のような機能があります。

- マルチスレッドのメモリ内検索による処理速度の向上
- 実際のファイル形式のサポートによる不正プログラム検索と添付ファイルのブロック
- 複数の InterScan を Domino パーティションサーバにインストール可能
- 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
- 圧縮ファイル検索時の解凍後のファイルサイズ制限やメール本文検索の有効化など、カスタマイズ可能な検索オプション
- 検索の詳細なオプション
 - ◆ データベースの手動検索および予約検索に対して増分検索オプションを設定すると、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ます。増分検索では、新規文書および新たに変更された文書のみが検索されます。
 - ◆ InterScan はスクリプト検索を実行して、被害を受ける前にソースから不正なコードを除去します。
 - ◆ 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
- 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設定するポリシーとルールを作成
- 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、Lotus Instant Messaging/Web Conferencing 通知のサポート (Windows プラットフォームのみ)
- Control Manager を経由した積極的な大規模感染予防

注意： i5/OS および OS/400 プラットフォーム向け製品では、Control Manager との連携機能は提供されません。

- マルチサーバ環境向けの信頼するサーバの設定。これで複数のサーバを構成することにより、信頼するサーバでは検索済みのメールが再検索されなくなります。この結果、検索に必要な時間とリソースを節約できます。
- 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
- さまざまなイベントを記録するログ機能とレポート作成機能 (統計とグラフを含む)

InterScan の機能 (スイート版)

注意： Windows、Linux、Solaris、および AIX 版向けにはスイート版のみの提供となります。i5/OS および OS/400 プラットフォーム向けにはスタンダード版のみの提供となります。

InterScan のスイート版では、スタンダード版の全機能のほかに次の追加機能を利用できます。

- スпамメールフィルタ
- メールの内容を件名または本文でフィルタ処理する機能
- .txt 形式、.html 形式、.rtf 形式、および Microsoft Office 文書の添付ファイルの内容を検索する機能
- Microsoft Office ファイルからマクロの除去を有効 / 無効にする機能

表 1-1 は、スイート版とスタンダード版の主な機能を比較したものです。

機能	スタンダード版	スイート版
ウイルス対策	○	○
スパムメール対策	×	○
コンテンツフィルタ		
件名 / 本文 / .txt、.html、.rtf 形式ファイル	×	○
Microsoft Office ファイル	×	○

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
アップデート	○	○
Control Manager エージェント	○	○

表 1-1. InterScan のスタンダード版とスイート版の機能の比較

InterScan の機能

トレンドマイクロの検索エンジンでは、ルールベースの方式とパターンマッチング方式のほか、MacroTrap 技術を採用しています。この技術により、マクロウイルスが検出、削除されます。ウイルスパターンファイルおよび検索エンジンは、頻繁に自動アップデートされ、Web からダウンロードでき、その際、InterScan をシャットダウンする必要はありません。

InterScan では、図 1-1 で示されるように、さまざまなエントリポイントで添付ファイルと文書の内容が検索され、駆除されます。

- Domino メールサーバで、メールの添付ファイルをリアルタイムに検索します。
- データベースイベントを監視し、文書を閉じる直前に添付ファイルを検索します。
- 複製中に、データベースと変更データを検索します。
- メールボックスと Domino データベースにある既存の添付ファイルを検索し、感染ファイルを除去します。

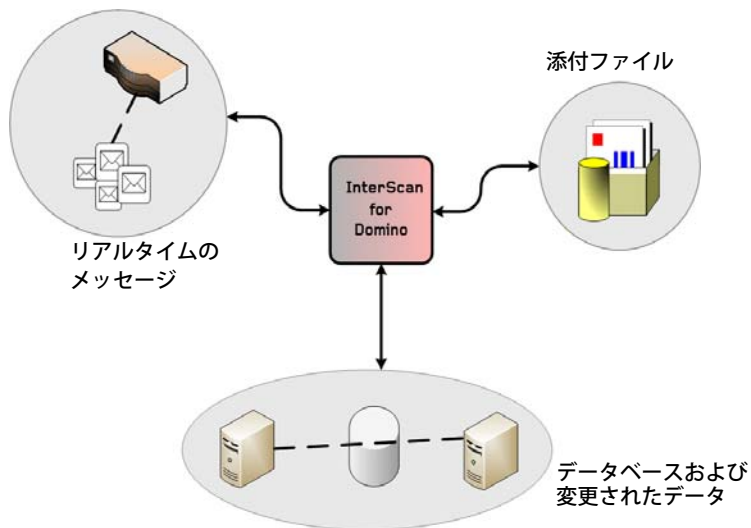


図 1-1. InterScan の保護の仕組み

InterScan では、包括的な活動ログが保持されて、感染ファイルごとに以下の詳細が記録されます。

- 感染源、ウイルス名、送受信者
- 受信日時
- ウイルス検出内容
- 実行した処理

Java ベースのグラフにより、管理者は企業全体でウイルスによる感染の有無を識別できます。Notes のデータベース複製機能によりさまざまなサーバのログを統合できます。

InterScan の構成要素

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 のエントリ

検索の種類

InterScan では、Domino のメール配信タスクが処理したメッセージ、データベース、文書、およびディレクトリが検索対象となります。これらの項目は、指定したポリシーで定義されているフィルタとルールに基づいて処理されます。詳細については、128 ページの「ポリシーベースのウイルス対策計画」を参照してください。

注意：InterScan では、インストール完了後ただちに Domino サーバを保護できるように、初期設定のポリシーが用意されています。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
- パスワード保護された圧縮ファイル
- 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。

- メール検索
- リアルタイムデータベース検索
- 手動と予約によるデータベース検索

メール検索

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。ユーザは、他の Notes ユーザや外部の送信元から送信される不正プログラムから保護されます。

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、すべてのデータベースにおいて、または検索範囲を指定したデータベース内のどのデータベース文書が保存されるときでも、その変更をリアルタイムに監視できます。すべてのまたは選択したデータベースのリアルタイム監視が実行され、他のサーバの複製先または複製元に指定されているデータベースが検索およびフィルタ処理されます。

効率化のために、変更された文書だけがチェックされ、不正プログラムがただちに検索されます。検索が完了するとその文書は閉じられて、次の文書でレプリケータタスクが実行されます。トレンドマイクロでは、高速で正確なこの方法を採用しています。この方法は、低速で費用のかかる電話回線を介してリモートサーバとの複製処理を行う場合に特に有用です。

リアルタイムデータベース検索によって複製プロセス全体が中断されることはありません。感染ファイルの保存だけが防止され、その後の文書の複製は影響を受けません。

Domino サーバにデータベースと頻繁にアップデートされるファイルが多数格納されている場合、リアルタイムデータベース検索は時間がかかり、CPU の多くを占有することがあります。オーバーヘッドを最小限にするために、ウイルスに感染しやすいデータベースのみをリアルタイム検索することをお勧めします。たとえば、ユーザ側で作成し、更新されるデータベースは、プログラム側で作成または更新されるデータベースよりも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にある文書と添付ファイルは、メール検索によって保護されているので、検索し直す必要はありません。

変更頻度が低いデータベースを保護するには、手動または予約によるデータベース検索を実行します。

手動と予約によるデータベース検索

手動と予約による検索は、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 オブジェクトや不正スクリプトも含め、すべてのタイプをウイルス検索できます。

注意： InterScan は、手動で mail.box データベースを検索する際にメール検索タスクを起動し、設定を適用します。手動検索が起動しているときにメール検索タスクが実行されていない場合は、メッセージが Domino サーバコンソールに表示され、ログファイルに記録されます。

予約検索と手動検索で増分検索を指定すると、新規文書または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。検索対象を絞ることによって、サーバのリリースと検索時間を節約できます。

警告： 増分検索の場合、古いパターンファイルで検出できなかったウイルスが存在する場合があります。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。

Domino 環境における脅威については、付録 A「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、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 InterScan で実行する方法を定義するポリシーを作成できます。InterScan により、サーバごとに 1 件のポリシーが実装されます。InterScan のインストールが正常に終了した時点で、サーバには初期設定のポリシーが割り当てられます。インストール直後の初期設定のポリシーには、リアルタイムのメール検索ルールが設定されています。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。InterScan では、サーバにポリシーが適用されます。複数のサーバに同じポリシーを適用することにより、プラットフォームの異なるサーバ間でも設定を共有することができます。
- ルールでは以下の事項が定義されます。
 - ◆ リアルタイムでのメールの検索方法
 - リアルタイムデータベース検索の実行方法
 - リアルタイムでないデータベース検索をいつ開始するか
 - 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をいつ実行するか
 - 通知の配信方法

ルールはポリシーごとにいくつでも定義できます。ただし、ルールが増えるほど、メッセージ 1 通の検査に要する時間も長くなります。

- ルールは、複数のフィルタで構成されます。これらのフィルタによって、メッセージと添付ファイルに対する検索処理が実際に定義されます。

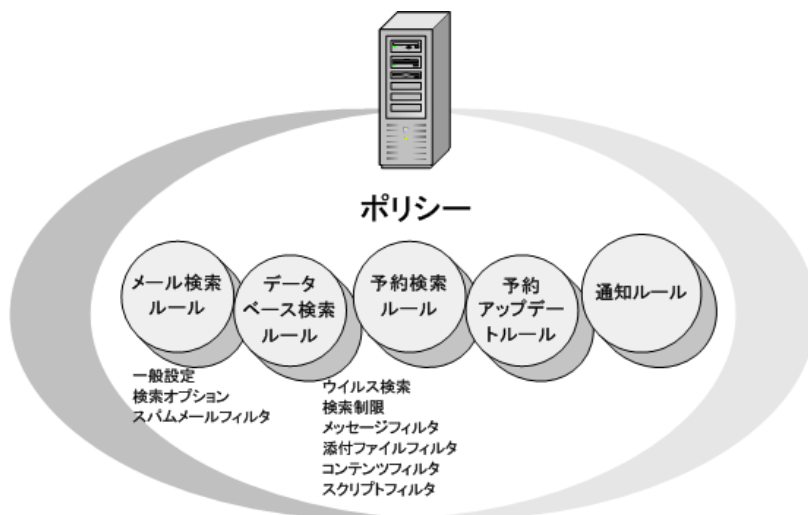


図 1-2. ポリシー、ルール、フィルタの関係

InterScan のルール

InterScan では、5 種類のルール (表 1-2) を利用できます。これらのルールによって、メッセージとデータベースの検索方法が定義されます。

ルールの種類	InterScan による実行方法の定義
メール検索ルール	メッセージの内容と添付ファイルをリアルタイムに検索してフィルタ処理します。メール検索ルールを作成するには、136 ページを参照してください。
データベース検索ルール	データベースをリアルタイムに検索します。リアルタイムデータベース検索ルールを作成するには、142 ページを参照してください。
予約検索ルール	予約に基づいてデータベースを検索します。予約データベース検索ルールを作成するには、145 ページを参照してください。

表 1-2. ルールの種類

ルールの種類	InterScan による実行方法の定義
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をアップデートします。予約アップデートルールを作成するには、200 ページを参照してください。
通知ルール	通知を配信します。通知ルールを作成するには、210 ページを参照してください。

表 1-2. ルールの種類

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) のサブセットです。これらのフィルタによって、メッセージ、添付ファイル、およびその内容に対する検索処理が実際に定義されます。フィルタオプションには次の種類があります。

フィルタオプション	適用対象
メッセージフィルタ	各種メッセージタイプ
添付ファイルフィルタ	不適切な添付ファイル
ウイルス検索	ウイルスなどの不正プログラム
検索制限	圧縮、暗号化などの処理を施された添付ファイル。ウイルス検索を有効にしておく必要があります。
コンテンツフィルタ	管理者が定義した明示的なルールに基づく、内容が不適切なメッセージ
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あるメッセージ

表 1-3. InterScan のフィルタオプション

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 の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 環境における不正コードの侵入場所と侵入方法 (たとえば、メール、Domino データベース内文書への添付ファイル、不正スクリプト)

ポリシーベースのウイルス対策計画

InterScan に搭載されているポリシーベースの機能を使用して、標準のウイルス対策とコンテンツセキュリティの設定を確立し、維持管理することをお勧めします。ポリシーを策定すると、次のことができます。

- ウイルス対策設定とアップデート設定を繰り返し作成すること、およびその他の管理作業の自動化
- 環境内サーバの管理の簡易化

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くグループポリシーの作成

共通のロールを持つサーバを複数備える大規模ネットワークでは、サーバごとに同じウイルス対策を設定するより、共通して適用できる設定セットを一度作成する方が、設定に要する時間と維持管理の手間を大幅に削減できます。

初期設定のポリシーに基づくポリシーを策定することにより、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、29 ページの「ポリシー、ルール、フィルタの概要」を参照してください。

- 特定の管理範囲にあるすべての Domino サーバに割り当てるためのグループポリシーの作成

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。
 - ◆ すべての Domino メールサーバ向けに共通の保護としてリアルタイムのメール検索を要求するポリシー
 - ◆ 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、およびそのサーバに適用する保護、アップデート、および通知の方法のセットを決定します。たとえば、あるメールサーバを保護するポリシーを作成してから、メールサーバとして機能している他のサーバに適用できます。

- 特定の Domino サーバに割り当てるための独自ポリシーの作成

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、予約検索ルールがある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。

ポリシーベース環境におけるルールとフィルタの実装の計画

Domino 環境における最適なウイルス対策とスパムメール対策に必要なルールとフィルタを実装するために、次の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用のリアルタイム検索ルールの作成
- 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の導入 (推奨されるファイルタイプのリストは 169 ページの表 5-1、「ブロックが推奨されるファイルの拡張子」を参照)

- すべてのデータベースで使用するリアルタイムデータベース検索ルールの作成

ヒント： ユーザのメールファイル、Domino のシステムデータベース、および更新頻度が低いその他のデータベースは検索対象から除外することをお勧めします。これにより、常に変更するデータベースに対するサーバリソースの割り当てがしやすくなります。

- 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用の予約アップデートルールの作成
- すべての Domino データベース用の予約データベース検索ルールの作成
- スпамメール対策を実装するために InterScan のスイート版を購入
 - ◆ スпамメール対策の有効化とスパムメール検出時の処理の指定
 - ◆ IT セキュリティポリシーに基づくフィルタレベルの設定
 - ◆ 許可する送信者とブロックする送信者の有効化と指定

また、システム上で実行するタスクの適切な数についても検討してください。InterScan のタスクの詳細については、26 ページの「**検索の種類**」を参照してください。

InterScan のインストール

この章では、Trend Micro InterScan for Domino 3.0 (以下、InterScan) の全サポートプラットフォーム上でのインストール方法について説明します。InterScan 用 Control Manager エージェントをインストールする予定の場合は、最初に InterScan をインストールしてください。

また、InterScan を使用するためのシステム要件のほか、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。

この章で説明する項目は次のとおりです。

- 36 ページの「導入計画」
- 37 ページの「試験的な導入」
- 39 ページの「バージョン 2.5x または 2.6x からのアップグレード」
- 40 ページの「推奨システム要件」
- 44 ページの「InterScan のインストール」
- 83 ページの「Domino サーバの起動」
- 85 ページの「InterScan のアクティベーション」
- 87 ページの「EICAR によるインストールのテスト」
- 88 ページの「インストール後のファイルとフォルダの確認」

導入計画

注意： i/5 OS および OS/400 版では、他のプラットフォーム向け InterScan 日本語版と本バージョン間における、InterScan 関連データベースの複製はサポートしていません。

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。InterScan をネットワークに導入する際は、さまざまな要素を考慮する必要があります。

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設定データベースとログ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 でのみ変更できるようにします。
- マスターのログデータベースから InterScan ログデータベースへの Push 複製を開始します。これにより、ウイルスなどの不正プログラム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、マスターのアップデートデータベースからアップデートデータベースに Pull 複製できるようにするかどうかを決定します。Pull 複製を有効にした場合は、中央の Domino サーバのみをトレンドマイクロのアップデートサーバに接続して最新コンポーネントをダウンロードします。その他のサーバではダウンロード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、206 ページの「ダウンロード元の設定」を参照してください。

- AIX 5.1 プラットフォーム上で InterScan を使用する場合は、APAR (Authorized Program Analysis Report) IY29345 の問題に対する修正プログラムがインストール済みであることを確認してください。この修正プログラムがインストールされていることを確認するには、コマンドプロンプトで「instfix -ik IY29345」と入力します。修正プログラムがインストールされていない場合は、次の Web サイトからプログラムをダウンロードしてインストールします。
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY29345> または、問題の回避策として Domino サーバのスタートアップスクリプトに次の 1 行を追加してください。AIXTHREAD_MNRATIO=1:1

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。試験的なインストールにより、次が可能になります。

- InterScan への習熟度向上
- 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による、導入プロセスの試行と改善、および導入計画が企業の事業要件と一致しているかの検証
- 各種機能の稼働状況および本格的な導入後に必要になるサービスレベルについての確認
- 改善が必要な設定の特定

試験的な導入を実施するには

1. 導入の準備をします。
2. 対象とするサイトを選択します。
3. ロールバック計画を作成します。
4. インストールを実施し、その結果を評価します。

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。周辺サーバ、すなわちスポークでは、ハブサーバから InterScan の設定を 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。
- ハブサーバから周辺サーバ、周辺サーバからハブサーバに 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

InterScan 以外に実稼働環境での使用を計画している他の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 3.5 (以下、Control Manager) など)、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。IT リソースのほか、地域的な企業ポリシーも考慮するようにします。

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、およびパフォーマンス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。

この評価結果は、実稼働環境への導入に反映させることができます。

バージョン 2.5x または 2.6x からのアップグレード

注意： Solaris 版、i5/OS および OS/400 版では、旧バージョンからのアップグレードに対応していません。

InterScan 2.x から 3.0 にアップグレードする際は、次の点を考慮します。

1. 開いている Notes クライアントをすべて閉じます。
2. InterScan データベース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。
3. Control Manager を使用している場合は、既存の Control Manager エージェントを事前にアンインストールしてください。
4. InterScan 2.x のシリアル番号が有効期限内であっても、InterScan 3.0 を使用するには、InterScan 3.0 のアクティベーションコード (85 ページを参照) を入手する必要があります。
5. InterScan 2.x がインストールされているアップグレード対象のサーバにパーティションサーバが含まれる場合は、インストールの際にすべて指定します。

競合が発生しないように、セットアッププログラムによって InterScan 2.x のプログラムが InterScan 3.0 のプログラムに変更されます。

推奨システム要件

企業ネットワークは、企業自体がそうであるように、それぞれが独自の性格を持っています。したがって、ネットワークの複雑さに応じて、ネットワークに対する要件はさまざまに変化します。ここでは、Domino サーバ用の InterScan を使用するための最小要件と推奨要件について説明します。

InterScan を使用するシステムの最小要件を表 2-1 に示します。

ハードウェア/ソフトウェアの仕様	最小要件
プラットフォーム	Winodws 版: Microsoft Windows Server 2003 Microsoft Windows 2000 Server/Advanced Server Service Pack 3 以上 Microsoft Windows NT 4.0 ServerService Pack 6a Linux 版: Red Hat Linux 7.2、Advanced Server 2.1/3.0 SUSE LINUX 7.2、8.0、Enterprise Server 8.0 UnitedLinux 1.0、powered by UnitedLinux 1.0 Solaris 版: Solaris 8、9、10 AIX 版: AIX 5.3、5.2、5.1 注意 :AIX 5.1 を使用する場合は、APAR IY29345 に対する修正プログラム、または問題に対する回避策を適用する必要があります。 i5/OS、OS/400 版: i5/OS V5R3、OS/400 V5R2 注意 :Lotus Domino 6.5.x サーバに i5/OS、OS/400 版をインストールする前に、IBM PTF をインストールする必要があります。Lotus Domino 6.5.x サーバで i5/OS、OS/400 版をインストールするにあたって必要なソリューション ID 27067、IBM PTF については、製品 Q&A (http://www.trendmicro.co.jp/esolution/) を参照してください。 注意 :Control Manager コンソールから InterScan を管理するには、Control Manager サーバに Control Manager 3.5 以降を適用しておく必要があります。

表 2-1. システムの最小要件

ハードウェア/ソフトウェアの仕様	最小要件		
Lotus Domino	サポートバージョン:	7.0	6.5.x
	Windows	○	○
	Linux x86	×	○
	Solaris	○	○
	AIX	○	○
	i5/OS、OS/400	×	○
CPU	Windows/Linux 版: Intel Pentium プロセッサ以上 Solaris 版: Sun SPARC (32/64 ビット) AIX 版: POWER 3 RS64、POWER 2、POWER、PowerPC i5/OS、OS/400 版: IBM iSeries サーバ、IBM AS/400 サーバ上の PowerPC (RISC)		
メモリ	Windows/Linux/Solaris 版: 256MB AIX 版、i5/OS、OS/400 版: 512MB		

表 2-1. システムの最小要件 (続き)

ハードウェア/ソフトウェアの仕様	最小要件
ディスク空き容量	Winodws 版: プログラムファイル用に 200MB 一時ファイル用に 100MB 各 Domino サーバパーティション用に 55MB Linux 版: プログラムファイル用に 125MB 一時ファイル用に 285MB 各 Domino サーバパーティション用に 50MB Solaris 版: プログラムファイル用に 155MB 一時ファイル用に 280MB 各 Domino サーバパーティション用に 60MB AIX 版: プログラムファイル用に 150MB 一時ファイル用に 300MB 各 Domino サーバパーティション用に 50MB i5/OS、OS/400 版: プログラムファイル用に 250MB 一時ファイル用に 600MB 各 Domino サーバパーティション用に 65MB * インストールに必要なディスク空き容量は、お使いの環境に依存します。
ファイルシステム	Winodws 版: NT File System (NTFS) パーティション
モニタ	すべてのプラットフォーム: 解像度 1024 x 768、256 色以上の VGA モニタ
コンポーネントのアップデート	すべてのプラットフォーム: コンポーネントダウンロードのためのインターネットアクセス

表 2-1. システムの最小要件 (続き)

ハードウェア/ソフトウェアの仕様	最小要件
その他	AIX 版: xIC C++ Runtime 6.0 VisualAge C++ for AIX 5 をインストールすることを強くお勧めします。 i5/OS、OS/400 版: Java Developer Kit (ライセンスプログラム 5722JV1)、バージョン 1.2 と Host Servers オプション (ライセンスプログラム 5722SS1 オプション 12) がインストール、実行されていること

表 2-1. システムの最小要件 (続き)

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。最新の情報については弊社の「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。

InterScan のインストール

InterScan をインストールする前に、以下に挙げる項目に目を通してください。

インストールを円滑に進めるために、事前に実施しておく作業がいくつかあります。また、次の点を考慮してください。

- InterScan 3.0 をインストールした後では、InterScan 2.x を上書きインストールできなくなります。
InterScan 2.x に戻すには、InterScan 3.0 をアンインストールして (250 ページを参照) InterScan 2.x を新規にインストールする必要があります。InterScan 2.x のインストール方法については、InterScan 2.x のマニュアルを参照してください。
- 同一の Domino サーバ上で動作しているパーティションに、InterScan 2.x と 3.0 の両方をインストールすることはできません。
- InterScan 3.0 をインストールする前、およびアンインストールする前に、Domino サーバを停止する必要があります。

- パーティションサーバについては、パーティションごとに InterScan が必要です。

注意：Solaris 版、i5/OS および OS/400 版では、旧バージョンからのアップグレードインストールはできません。必ず旧バージョンを一度アンインストールした後、に本バージョンをインストールしてください。

インストールの準備

InterScan をインストールする前に、次の作業を実行します。

1. 管理者 (Windows プラットフォーム)、root ユーザ (Linux、Solaris、AIX プラットフォーム)、または機密保護担当者 (i5/OS および OS/400 プラットフォーム) としてログオンします。

i5/OS および OS/400 プラットフォームの場合、システム値「QALWOBJRST」が「*ALL」に設定されていることを確認します。

- a. CL コマンドエントリで、「CHGSYSVAL SYSVAL (QALWOBJRST)」と入力します。
- b. [New value] オプションに「*ALL」と入力します。

英語以外の環境でのインストールの場合は、残りのインストールの準備を行う前に、50 ページの「英語以外の環境での InterScan のインストール (i5/OS および OS/400 プラットフォームのみ)」にリストされた作業を実行します。

2. Lotus Domino 6.5.x サーバに i5/OS および OS/400 版をインストールする前に、IBM PTF をインストールする必要があります。Lotus Domino 6.5.x サーバで i5/OS、OS/400 版をインストールするにあたって必要なソリューション ID 27067、IBM PTF については、製品 Q&A (http://esupport.trendmicro.co.jp/supportjp/supportcentral/supportcentral_adv_ja.do) を参照してください。
3. AIX バージョン 5 以降の場合、x1C C++ Runtime 6.0 以降をインストールします。x1C C++ Runtime 6.0 は次の IBM サイトからダウンロードできます。
http://www-1.ibm.com/support/docview.wss?rs=2030&context=SSJT9L&dc=D400&uid=swg24008374&locc=en_US&cs=utf-8&lang=en

4. notes.ini の格納場所を確認します。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 の格納場所を確認してください。
5. Domino データディレクトリと Domino プログラムディレクトリのパスを確認します。
6. 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。デフォルトグループは管理者です。
7. 次のコマンドの 1 つを実行してディスク空き容量を確認します。
 - Linux, Solaris, AIX の場合、df -k コマンドを実行します。
 - i5/OS および OS/400 の場合、CL コマンド **dspsyssts** を使用して最低 900 MB の空き容量があることを確認します。
8. / (ルート) マウントポイントに最低限必要なディスク空き容量があることを確認します。
9. 開いている Notes クライアントをすべて閉じます。
10. 開いている Notes アカウントセッションをすべて閉じます。

注意： who コマンドを実行して、クライアントセッションを特定します。
InterScan 2.x からアップグレードする前、または InterScan 3.0 をはじめてインストールする前に、それらのセッションをすべて閉じる必要があります。

Linux, AIX, または Solaris のユーザセッションをリモートで終了するには、次のコマンドを実行します。

```
# who
# ps t {terminal session}
# kill -HUP {pid}
i5/OS または OS/400 のユーザセッションをリモートで終了するには次の CL コマンドを入力します。
wrksrjob user(*all) status(*active) jobtype(*interact) astlvl(*basic)
「4」を入力してから、<Enter> キーを押してユーザセッションをリモートで終了します。
```

11. 次の作業を実行する前には、Domino サーバを停止します。
 - InterScan 3.0 をはじめてインストールする場合
 - InterScan 2.x からアップグレードする場合
 - InterScan 3.x をアンインストールする場合
12. InterScan のアクティベーションコードを準備しておきます。
 アクティベーションコードの詳細については、86 ページを参照してください。
13. InterScan のセットアップファイルの権限を確認します (UNIX 系システムのみ)。

InterScan のセットアップファイルの権限を確認するには

- a. コマンドラインで次のコマンドを実行します。

ls -l {パス / ファイル名}

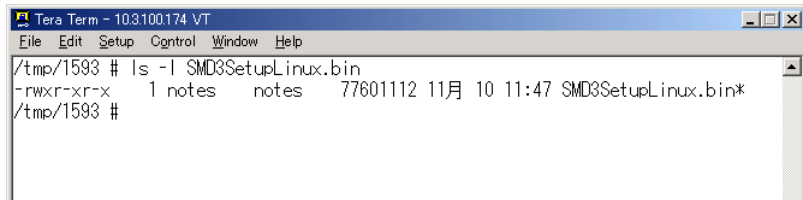
各パラメータの意味は次のとおりです。

- パスは、InterScan のセットアップファイルが格納されているディレクトリです。
- ファイル名は、InterScan のセットアップファイルの名前で、拡張子まで含みます。

例:

```
# ls -l /tmp/installers/SMD3SetupLinux.bin (Linux 版)
# ls -l /domino/installers/SMD3SetupAIX.bin (AIX 版)
# ls -l /domino/installer/SMD3Setupsolaris.bin
(Solaris 版)
$ ls -l /domino/installers/setup.jar(use qsh)
(i5/OS.05/400 版)
```

このコマンドを実行すると、図 2-1 のような結果が得られます。



```

Tera Term - 10.3.100.174 VT
File Edit Setup Control Window Help
/tmp/1593 # ls -l SMD3SetupLinux.bin
-rwxr-xr-x  1 notes  notes   77601112 11月 10 11:47 SMD3SetupLinux.bin*
/tmp/1593 #

```

図 2-1. InterScan のセットアップファイルの権限の確認

ls -l コマンドは指定したファイルの長いリスト形式を表示します。各ファイルの名前のほか、ファイルタイプ、権限、ハードリンク数、所有者名、グループ名、サイズ (バイト)、およびタイムスタンプ (または修正時刻) を印刷します。

この例では、10 文字コードの最初の文字がファイルタイプを示します。次の 9 文字はファイルについての権限を示します。権限 -rwxr-xr-x root root は、root ユーザによる読み取り、書き込み、実行権限、root グループのメンバーによる実行、読み取り権限、およびシステム上のその他のユーザによる実行権限を意味します。

ロングファイル名とファイル権限の詳細については、各プラットフォームのマニュアルを参照してください。

ヒント: UNIX 系システムでは、通常のユーザは自分の \$HOME ディレクトリと /tmp ディレクトリにのみ書き込みアクセス権を持ちますが、Microsoft Windows NT システムのユーザは、アクセス権が特に拒否されている場合を除いて、すべてのディスクに対するアクセスができます。Domino サーバは通常のユーザとして実行されるので、ファイルとディレクトリの所有関係を正確に設定するようにしてください。

- b. InterScan のインストールに使用するアカウントに十分なファイル権限がない場合には、**# chmod {###} { ファイル名 }** を実行して、ファイルへのアクセス権限を修正してください。

各パラメータの意味は次のとおりです。

- {###} は、ファイルの読み取り、書き込み、実行権限を示します (コードのリストと対応する権限については、表 2-2 を参照してください)。
- ファイル名は、InterScan のセットアップファイルの名前です。

コード	権限
7	すべて
6	読み取りと書き込み
5	読み取りと実行
4	読み取りのみ
3	書き込みと実行
2	書き込みのみ
1	実行のみ
0	なし

表 2-2. chmod コードと権限

例:

Linux 版: # `chmod 755 SMD3SetupLinux.bin`

AIX 版: # `chmod 755 /domino/installers/SMD3SetupAix.bin`

Solaris 版: # `chmod 775 SMD3Setupsolaris.bin`

i5/OS、OS/400 版: \$ `chmod 755 /domino/installers/setup.jar(use qsh)`

この例では、このアカウントにすべての権限、グループに実行と読み取り権限、およびその他のアカウントに実行権限が与えられます。

ヒント：上記コマンドを InterScan のセットアップファイルのあるディレクトリで実行します。または、コマンド実行時にファイルパスを含めます。

例 :# `chmod 755 /temp/installers/SMD3SetupLinux.bin`

対象サーバの準備が整っていることを確認したら、InterScan プログラムファイルをインストールし、InterScan データベースをセットアップします。

英語以外の環境での InterScan のインストール (i5/OS および OS/400 プラットフォームのみ)

i5/OS および OS/400 プラットフォーム上の英語以外の環境で InterScan をインストールするには

インストールを開始する前に、次を確認します。

- CCSID のユーザプロファイル設定が 37 であること
- ユーザプロファイル設定の場所が /QSYS.LIB/en_US.LOCALE であること
- the notes.ini CCSID が 819 であること

次の作業を実行します。

1. CL コマンドエントリで「CHGUSRPRF USRPRF(USERNAME)」と入力してから、<F4> キーを押します。例: `chgusrprf usrprf(qsecofr)`
2. 追加のパラメータを入力するには、<F10> キーを押します。
3. [コード化文字セット ID...] オプションを選択して、値を 37 に変更します。

4. [ロケール] オプションを選択して、値を /QSYS.LIB/en_US.LOCALE に変更します。

注意： この作業により言語環境が英語に変更されます。その後、端末とサーバの通信が英語になるため、あらかじめ i5/OS サーバに英語用のサブシステムを作成しておく必要があります。英語用のサブシステムを用意しないと、端末からログインできなくなります。

5. <Enter> キーを押して変更を保存します。
6. CL コマンドエントリで「90」と入力して、サインオフします。
7. コンソールウィンドウのメニューより、[通信] → [構成] を開きます。
8. [ホスト・コード・ページ] のプルダウンより、[037 米国] を選択し、[OK] をクリックします。
9. サインオンします。
10. CL コマンド、QSH を実行します。
11. Domino データパスにディレクトリ変更します。
12. notes.ini ファイルをバックアップします。「cp notes.ini notes1.ini」を入力します。
13. notes.ini の CCSID を変更します。「setccsid 819 notes.ini」と入力します。

InterScan のインストールが完了したら、設定を元の値に戻すことができます。

セットアップモード

次のいずれかの方法で 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 — グラフィカルユーザインタフェースをサポートしているサーバに InterScan をインストールする際に、ユーザに各種情報の入力を求めます。

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。詳細については、53 ページを参照してください。

- サイレントインストール — わずかなコマンド入力だけで、InterScan をインストールできます。

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。応答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。詳細については、66 ページを参照してください。

- コンソールベースのインストール — グラフィカルユーザインタフェースをサポートしていないサーバに InterScan をインストールする際に、ユーザが操作しながらインストールを進めます。

Windows 以外の各プラットフォームに InterScan をセットアップするときは、この方法を使用できます。詳細については、71 ページ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 種類が用意されています。

- 新規インストール — InterScan をはじ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。

セットアッププログラムによって、目的のサーバにインストールされている InterScan が検出されると、インストールオプションの確認画面が表示されます。InterScan 3.0 をはじめてインストールする場合、この画面は表示されません。

ウィザードベースのインストールの実行

該当の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。

グラフィカルユーザインタフェースから InterScan 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-ROM からインストールする場合は、CD-ROM 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. 次のいずれかのファイルを実行して、セットアッププログラムを起動します。

OS	セットアッププログラム
Windows	setupwin32.exe
Linux	SMD3SetupLinux.bin
Solaris	SMD3Setupsolaris.bin
AIX	SMD3SetupAIX.bin

ウィザードの初期化画面に続いて、次の画面が表示されます。

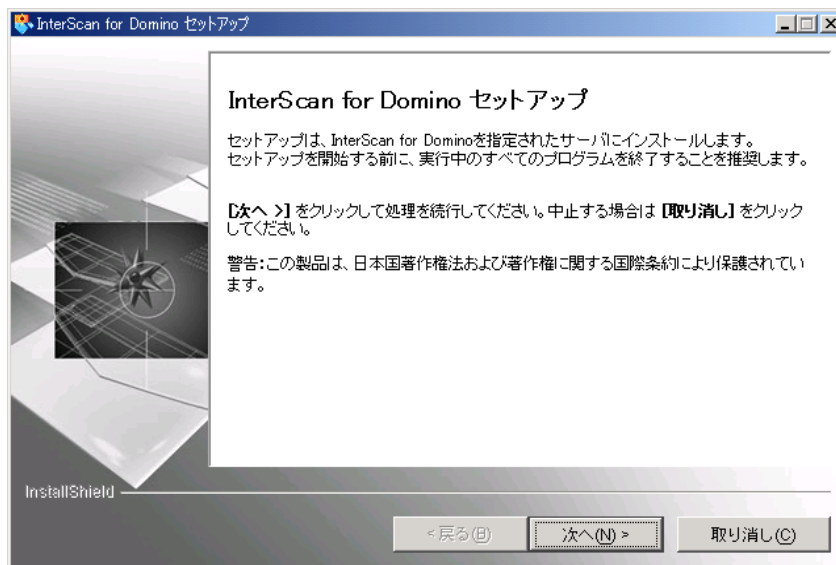


図 2-2. インストール開始画面

注意： ウィザードベースの InterScan のインストール手順の説明では、Windows 版で取得したスクリーンショットを使用しています。

3. [次へ] をクリックします。次の画面が表示されます。

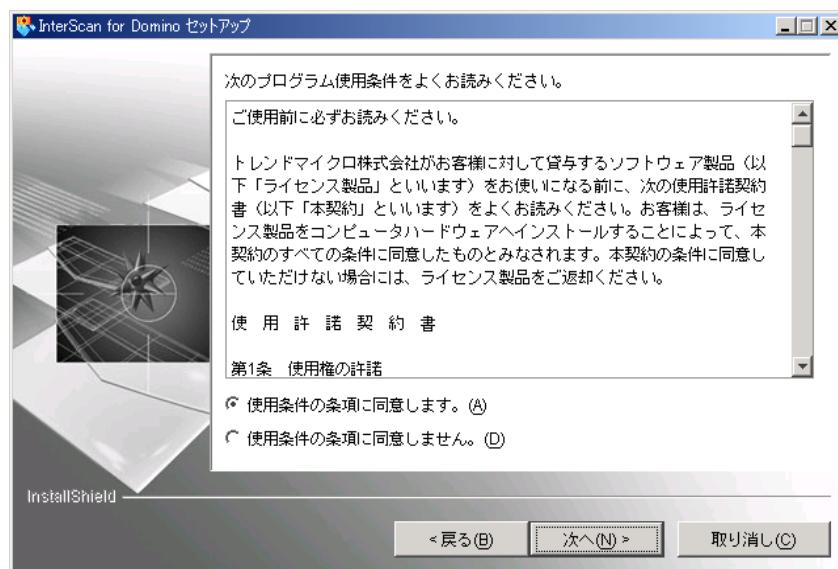


図 2-3. 使用許諾契約書画面

[使用条件の条項に同意します] を選択してインストールを続けます。使用許諾契約書の条項に同意しない場合は、[使用条件の条項に同意しません] をクリックします。インストールは中断されます。

4. [次へ] をクリックします。セットアッププログラムによって、インストール先のサーバの設定が確認されます。

サーバに InterScan 2.x または InterScan 3.0 がインストールされていない場合は、既存のセットアップオプション画面は省略され、製品のアクティベーション画面へ直接進みます。

対象サーバの InterScan のインストール状況に応じて、次のオプションのいずれか 1 つまたは複数が表示されます。

- アップグレード — インストール済みの InterScan をアップグレードします。
- インストールとアップグレード — すでにインストール済みの InterScan 3.0 をアップグレードし、追加した Domino サーバに InterScan 3.0 をインストールします。
- インストール — 追加した Domino サーバに InterScan 3.0 をインストールします。

図 2-4 の画面から、すべてのパーティションサーバに整合性のとれた InterScan セットアップを行うことができます。

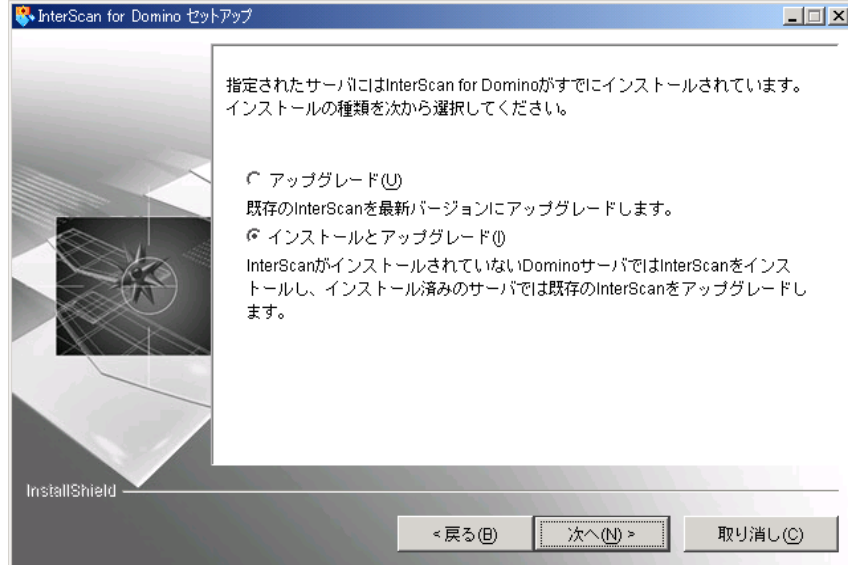


図 2-4. インストールとアップグレード画面

図 2-5 の画面から、追加した Domino サーバに同じバージョンの InterScan をインストールすることができます。

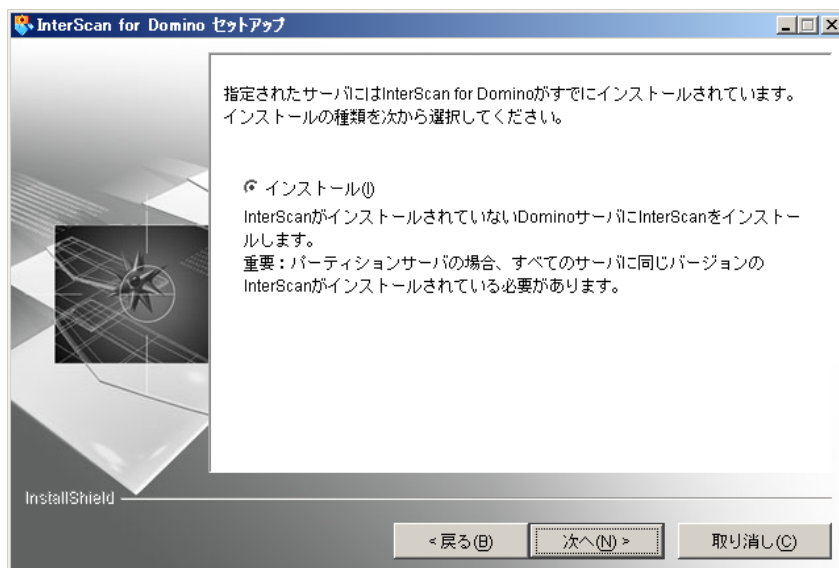


図 2-5. インストールセットアップ画面

詳細については、52 ページの「セットアップオプション」を参照してください。

5. 図 2-6 の製品のアクティベーション画面では、「アクティベーションコード」を入力して InterScan をアクティベートするか、この画面を省略して後で設定データベースを使用してアクティベートするかを選択することができます。

注意： InterScan 2.x のシリアル番号が有効期限内であっても、InterScan 3.0 に移行した場合は、InterScan 3.0 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。

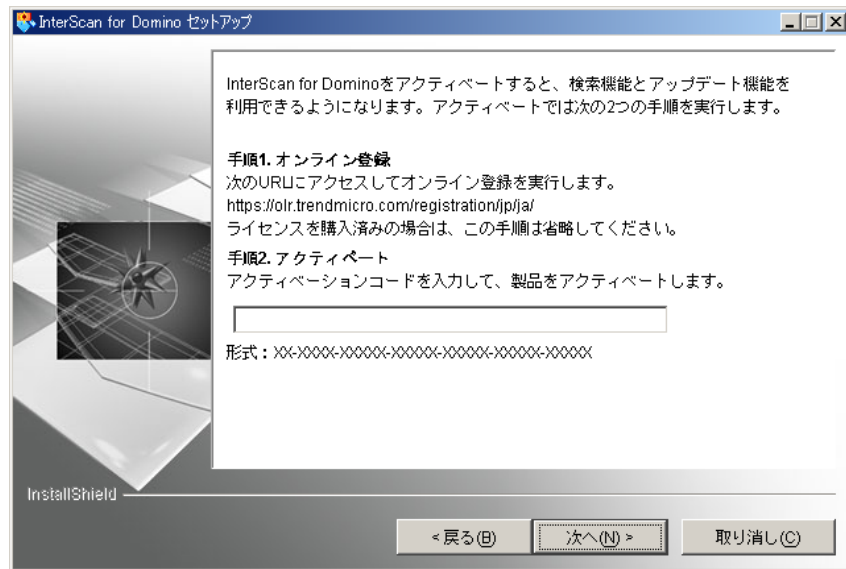


図 2-6. 製品のアクティベーション画面

「アクティベーションコード」を入力または貼り付けるか (85 ページを参照)、[次へ] をクリックして製品のアクティベーションを省略します。次のいずれかを実行します。

- すぐにアクティベート:

アクティベーションコードを入力してすぐに InterScan をアクティベートします。InterScan のすべての機能を利用するには、製品版アクティベーションコード (85 ページを参照) を入力する必要があります。

- 設定データベースを使用して後でアクティベート：

アクティベーションコードを入力せず、次の画面に進みます。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。インストールファイルがローカルの作業ディレクトリに抽出された後、Domino サーバの選択画面が表示されます。

7. Domino サーバの選択画面で次のいずれかをクリックします。

- 追加 — InterScan をインストールするサーバの notes.ini を指定します。このとき、パーティションサーバの notes.ini も同時に指定します。
- 削除 — リストからサーバを削除します。

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。

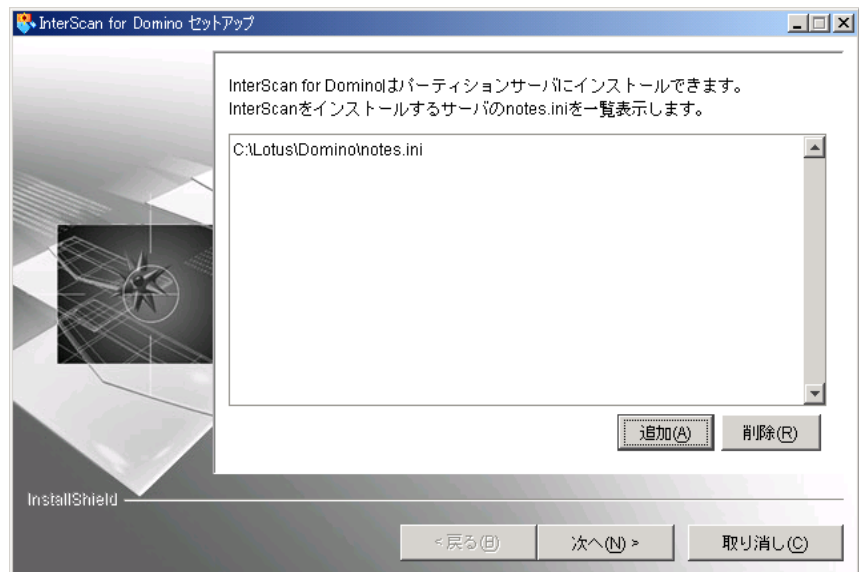


図 2-7. インストール先サーバリスト

8. [次へ] をクリックします。図 2-8 に示すように、Domino のプログラムディレクトリとデータディレクトリが示された画面が表示されます。

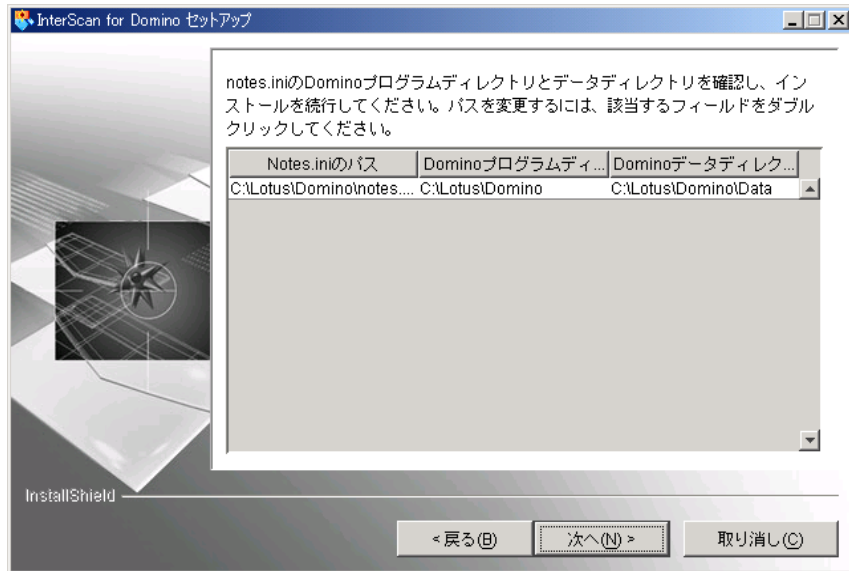


図 2-8. インストール先サーバの確認

セットアッププログラムによって、Domino プログラムディレクトリとデータディレクトリのパスが検出されます。

指定した notes.ini に記されていないパスを指定する場合は、空の項目をダブルクリックして正しいディレクトリ名を入力します。

注意： 指定された Domino プログラムディレクトリに Domino プログラムが含まれているかどうかインストールプログラムによってチェックされます。指定されたプログラムディレクトリが無効な場合は、エラーメッセージ「Domino プログラムディレクトリまたはデータディレクトリのパスが無効です。パスを確認して再度実行してください。」が表示されます。

9. [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。
- セットアッププログラムの初期設定では、隔離データベースを除くすべての InterScan データベースが複製対象として選択されています。初期設定を変更する場合には、複製する InterScan データベースを選択または選択解除します。

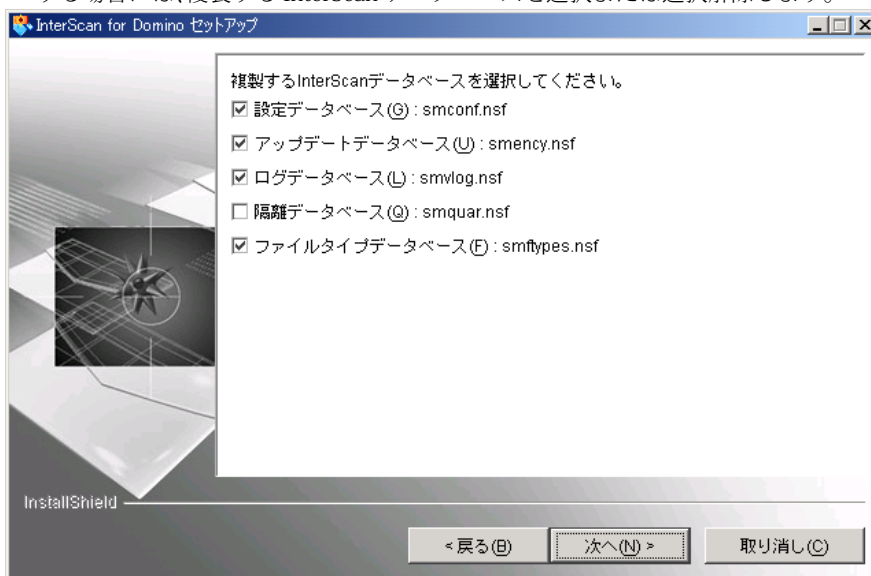


図 2-9. 複製する InterScan データベースの設定

複数のサーバ上で InterScan をインストールし、データベースを複製する場合、2 つ目以降のサーバにおいて設定データベースの複製を無効にすることができます。1 つのサーバをプライマリサーバまたは管理サーバとして選択し、その他のすべてのサーバに複製します。

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。

10. [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が、初期設定ポリシーを取得する必要があります。初期設定ポリシーが取得されていない場合は、新規ポリシーを作成した後で SMDreal タスクをリロードしてください。

注意： SMDreal タスクが正常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。インストール終了後、すべてのサーバが初期設定ポリシーまたはユーザ指定の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。

11. [次へ] をクリックします。InterScan データベースを管理するアカウントの指定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)、各サーバの管理者アカウントを入力します。

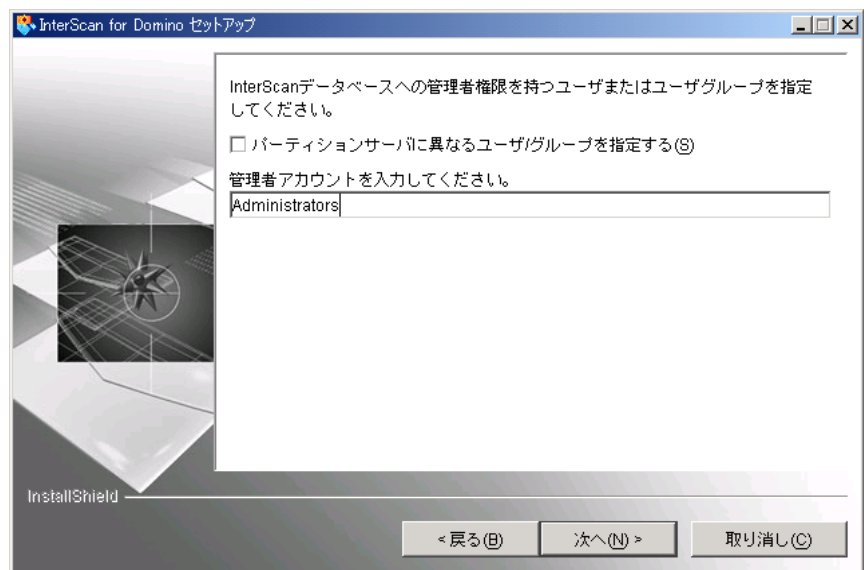


図 2-10. 管理者アカウントの指定画面

12. [次へ] をクリックします。図 2-11 の InterScan データベースへの署名画面が表示されます。

次のいずれかを実行します。

- セットアップでは InterScan データベースに署名しない場合は、[データベースの署名を省略する] を選択します。

この場合は、インストール終了後に手動で InterScan データベースに署名します。

- 単一の ID を使用して InterScan データベースに署名するには、[すべての対象サーバに対して単一の ID ファイルを使用する] を選択します。

[ID] 列に ID ファイルのフルパスを入力するか、[参照] をクリックして目的の ID ファイルのパスを指定します。次にパスワードを入力します。

- パーティションごとに異なる ID で InterScan データベースに署名するには、[対象サーバ/パーティションに対して異なる ID を使用する] を選択します。

[ID] 列に ID ファイルのフルパスを入力するか、[参照] をクリックして目的の ID ファイルのパスを指定します。次にパスワードを入力します。

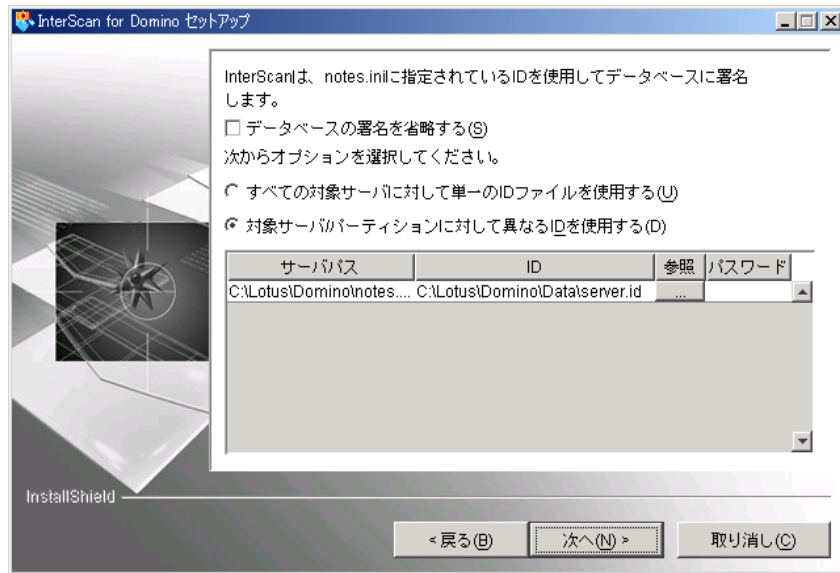


図 2-11. InterScan データベースへの署名画面

注意： 指定したアカウントが存在しない場合には、インストール完了時に作成します。アカウントには管理者権限があることを確認してください。

13. [次へ] をクリックします。インストールが始まります。

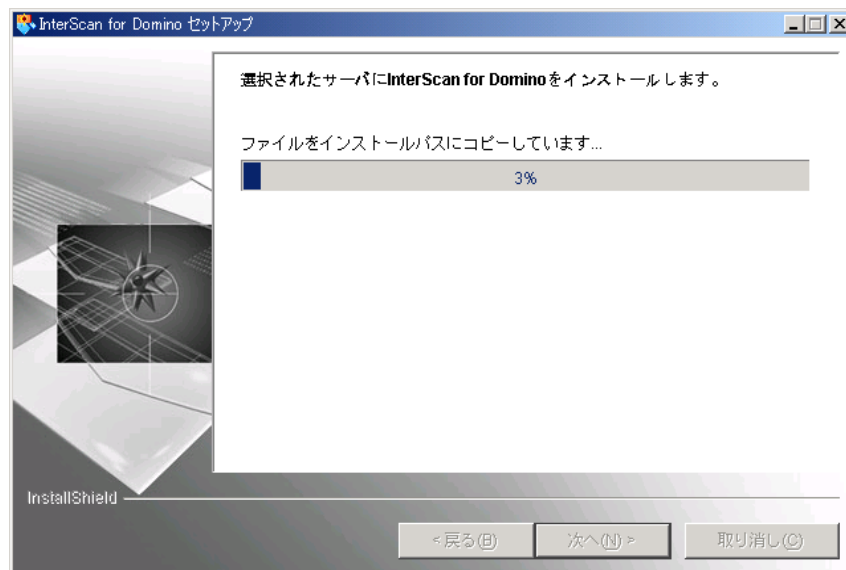


図 2-12. 選択したサーバに InterScan をインストール中

14. [終了] をクリックしてセットアップウィンドウを閉じます。

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、87 ページの「EICAR によるインストールのテスト」を参照してください。

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、85 ページの「他のウイルス対策製品を使用している場合の注意」を参照してください。

サイレントインストールの実行

サイレントインストールでは、事前に記録された応答ファイル (インストールスクリプト) を使用して、複数の InterScan サーバに簡単に自動化されたインストールを実行できます。

このインストール処理を開始する前に、次のことを実行します。

- 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は、40 ページの「推奨システム要件」を参照してください。
- 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。この処理を実行しないと、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作成して、複数のサーバに対する 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記録したスクリプトファイルです。インストールスクリプトをテキストエディタで編集し、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することが可能です。

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、コマンドコンソールから次の適切な情報を入力して、インストール時の構成をインストールスクリプトに記録します。
 - Windows 版の場合

setupwin32 -options-record { スクリプトパスおよびファイル名 }

例 :

setupwin32 -options-record c:\smd silent.txt

注意：サイレントインストールのスクリプトファイルの記録時に、KDE などの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。

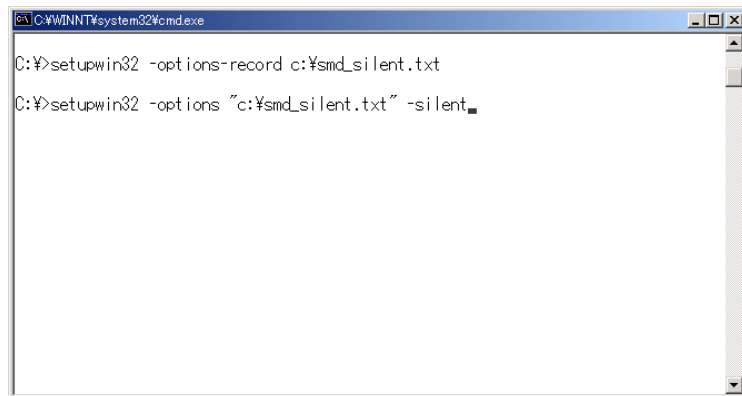


図 2-13. Windows サーバでの InterScan のインストールの記録

- Linux/Solaris/AIX 版の場合 (コンソールベースのインストール)

**./SMD3Setup{ プラットフォーム }.bin -console
-options-record { パスおよびスクリプトファイル名 }**

{ プラットフォーム } を、Linux、Solaris、または AIX に置き換えます。

例：

```
./SMD3Setupsolaris.bin -console -options-record  
/tmp/silent.txt
```

- i5/OS および OS/400 版の場合

```
java -cp ./setup.jar  
run -console -options-record ./smd_silent.txt
```

2. インストールスクリプトの記録が終了したら、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。

- Windows 版の場合

```
setupwin32 -options "{ パスおよびスクリプトファイル名 }"  
-silent
```

例：

setupwin32 -options "c:\smd_silent.txt" -silent

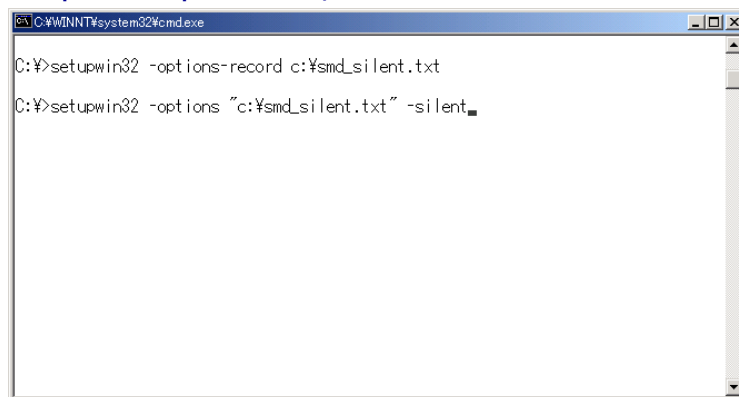


図 2-14. InterScan のサイレントインストール (Windows の例)

- Linux/Solaris/AIX 版の場合

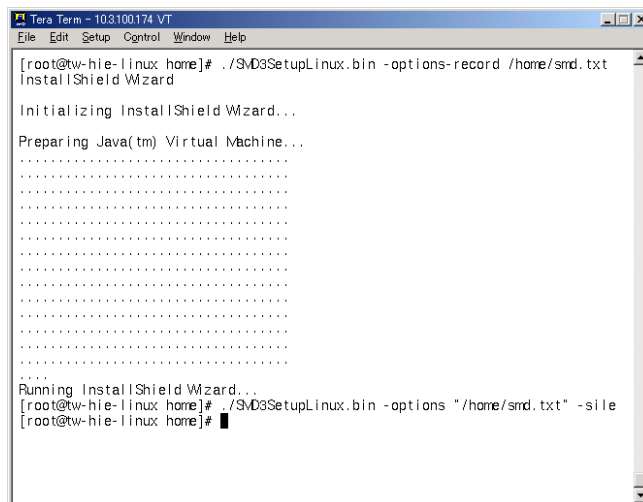


図 2-15. InterScan のサイレントインストール (Linux の例)

ログファイル setuplog.txt を開いて、インストール結果を確認します。インストールが正常に実行された場合は、このファイルに「[yyyy.mm.dd hh:mm:ss] [Inf] Installation on {notes.ini path} is successfull.」というメッセージが記録されています。また、次のポップアップメッセージが表示されます。

**InterScan for Domino のサイレントインストールが終了しました。
/opt/trend に作成されているログ(Setuplog.txt)を参照し、インストール結果を確認してください。**

「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。

コンソールベースのインストールの実行

次の Windows 以外のプラットフォームでは、コンソールベースのインストールがサポートされます。

プラットフォーム	カーネルバージョン	参考 URL
Solaris 8、9、10	該当なし	http://jp.sun.com
Red Hat Enterprise Linux AS/ES 2.1/3.0	2.4.18 2.4.13 2.4.10 2.4.9 2.4.8 2.4.7 2.4.5 2.4.4 2.4.3	http://www.jp.redhat.com
SUSE 7.2 SUSE Linux Enterprise Server 8	2.4.18 2.4.13 2.4.10 2.4.9 2.4.8 2.4.7 2.4.5 2.4.4 2.4.3 2.4.2	http://www.suse.com
AIX 5.3、5.2、5.1	該当なし	http://www-6.ibm.com/jp/servers/eserver/pseries/aix/
i5/OS V5R3 OS/400 V5R2	該当なし	http://www-900.ibm.com/cn/servers/eser/product/series.shtml

システム要件の詳細については、表 2-1 を参照してください。

ヒント：Linux 版、Solaris 版、または AIX 版ではウィザードベースのインストールを使用することができます。詳細については、53 ページを参照してください。

セットアップの前に実行する作業については、45 ページの「インストールの準備」を参照してください。

コマンドラインから InterScan をインストールするには

注意： 表示されているコンソールベースのインストール画面は、Linux 版です。

1. 次のいずれかの方法で、セットアッププログラムがあるフォルダに移動します。
 - InterScan の製品 CD-ROM がある場合は、CD-ROM をコンピュータに入れて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. 次のコマンドを入力して、コンソールベースのインストールを開始します。

プラットフォーム	セットアッププログラム
Linux	./SMD3SetupLinux.bin -console
Solaris	./SMD3Setupsolaris.bin -console
AIX	./SMD3SetupAIX.bin -console
i5/OS、 OS/400	java -cp ./setup.jar run -console

ヒント： コンソールベースのセットアップでは、既存の設定をそのまま使用する場合は <Enter> キー を押し、次の手順に進む場合は「1」を入力します。セットアップを中止する場合は、「3」を入力します。

セットアップが始まり、開始メッセージが表示されます。

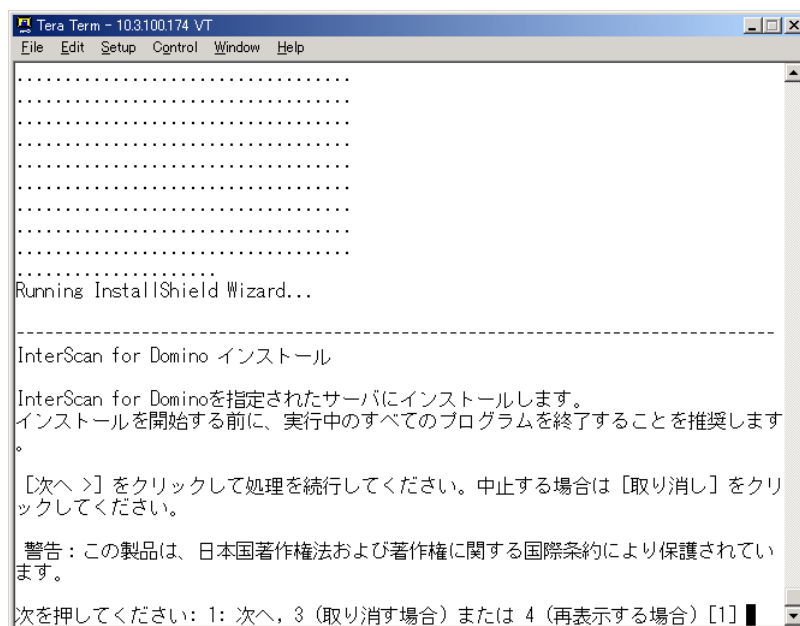


図 2-16. インストール開始画面

ほとんどの画面では、次の数値入力による操作が可能です。

- 0: 既存の設定をそのまま使用します。
 - 1: 次の画面に進みます。
 - 2: 前の画面に戻ります。
 - 3: セットアップを中止します。
 - 4: 現在の画面を再表示します。
3. 「1」を入力して InterScan のインストールを開始します。
 4. 使用許諾契約画面が表示されます。<Enter> キーを押して処理を続行します。
 5. 使用許諾契約のプロンプトで、使用条件の条項に同意する場合は「1」を入力します。同意しない場合は「2」を入力し、次に「3」を入力してインストールを中止します。

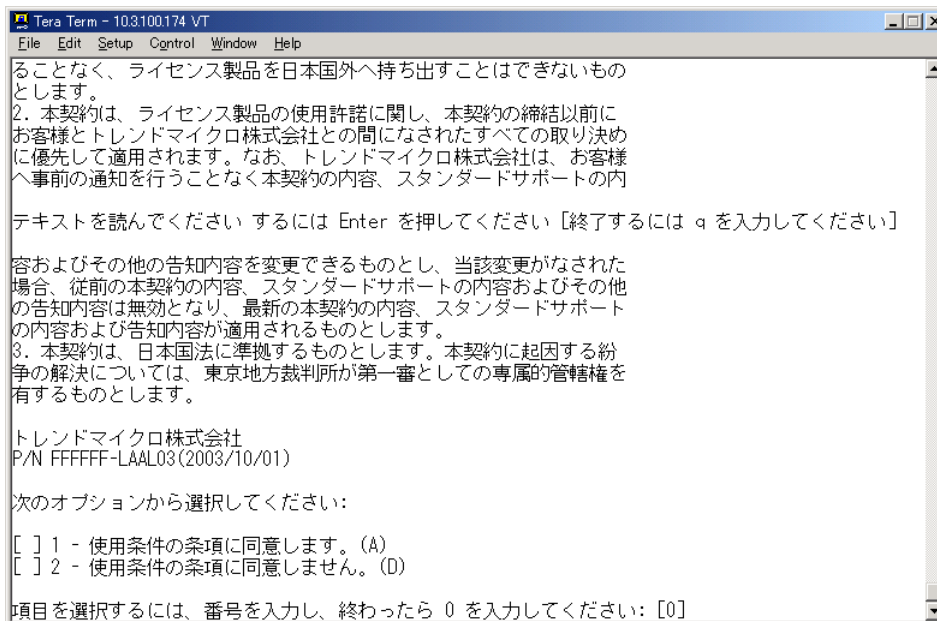


図 2-17. InterScan の使用許諾契約同意画面

6. 製品のアクティベーション画面では、アクティベーションコードを入力して InterScan をアクティベートできます。また、この画面では入力せず、インストール後に設定データベースからアクティベートすることもできます。

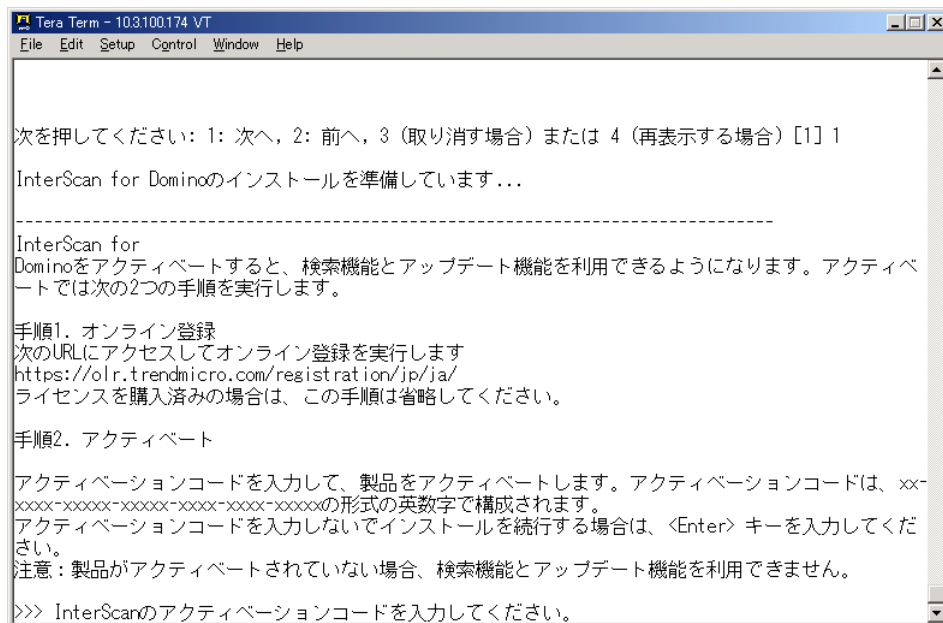


図 2-18. 製品のアクティベーション

次のいずれかを実行します。

- すぐにアクティベート:

アクティベーションコードを入力してすぐに InterScan をアクティベートします。InterScan のすべての機能を利用するには、製品版アクティベーションコードを入力する必要があります。

- 後でアクティベート:

この手順を省略して後でアクティベートすることもできます。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。

7. Domino サーバでは、現在インストールされている InterScan が一覧表示されます。

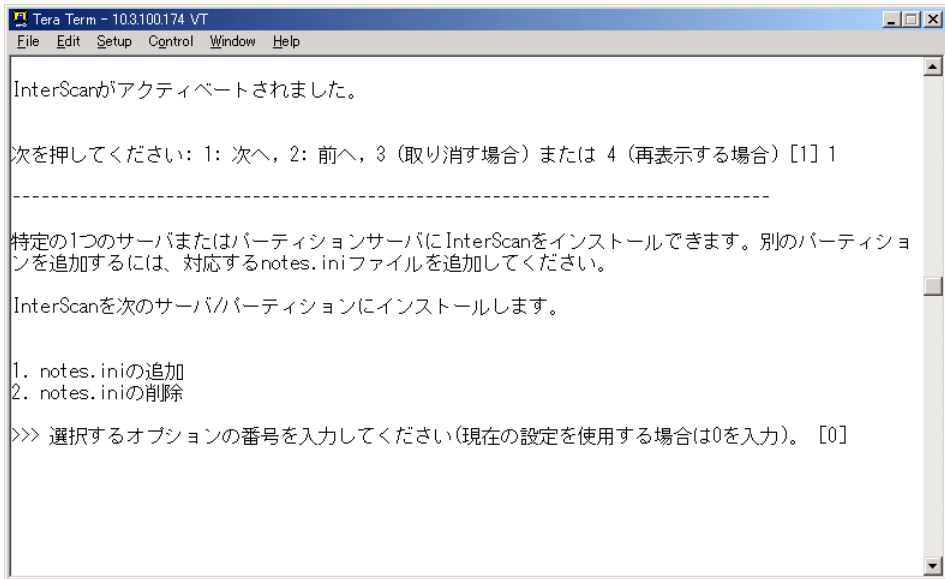


図 2-19. 現在インストールされている Domino サーバー一覧

次のいずれかを実行します。

- notes.ini を追加して目的の Domino サーバを指定する場合は、「1」を入力します。

例: /lotus/notesdata/notes.ini

(Linux、Solaris、AIX、i5/OS、OS/400 版)

- notes.ini を削除して Domino サーバまたはパーティションに InterScan がインストールされないようにする場合は、「2」を入力します。

指定された Domino プログラムディレクトリに Domino プログラムが含まれているかどうかインストールプログラムによってチェックされます。指定されたプログラムディレクトリが無効な場合は、次のエラーメッセージが表示されます。

Domino プログラムディレクトリまたはデータディレクトリのパスが無効です。パスを確認して再度実行してください。

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ごとに InterScan をインストールします。

8. Domino プログラムパスまたは Domino データパスを変更するために使用できるオプションのインデックス番号を選択します。

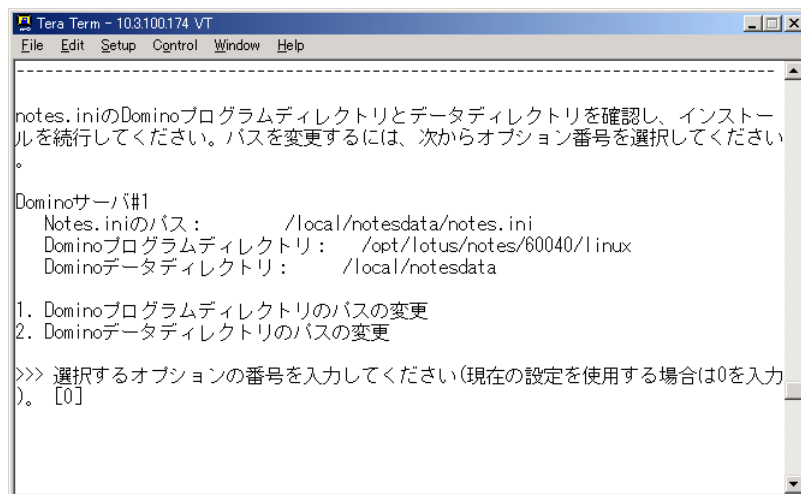


図 2-20. Domino サーバのプログラムディレクトリとデータディレクトリの指定

セットアップオプションによって、インストール先のサーバが解析されます。この解析では、インストールされている InterScan の情報がないか確認され、その結果が表示されます。

既存バージョンの InterScan 3.0 がインストールされているサーバの場合は、アップグレードが実行されます。InterScan がインストールされていないサーバの場合は、InterScan が新規にインストールされます。

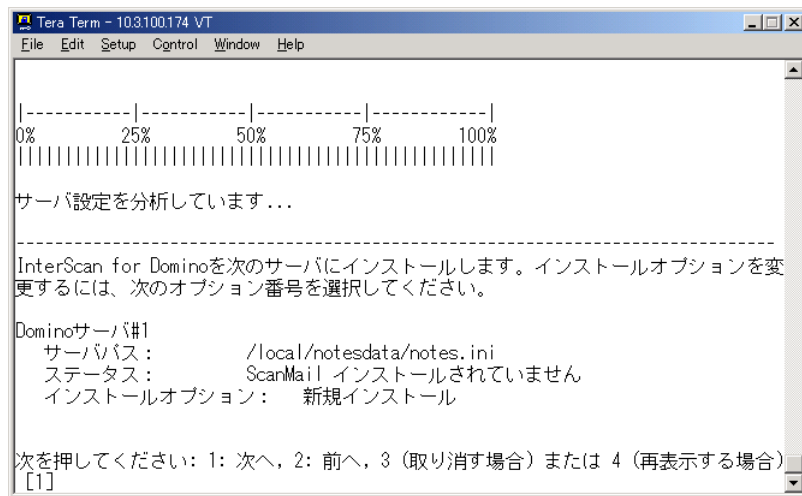


図 2-21. 設定の解析 — InterScan をはじめてインストールする場合

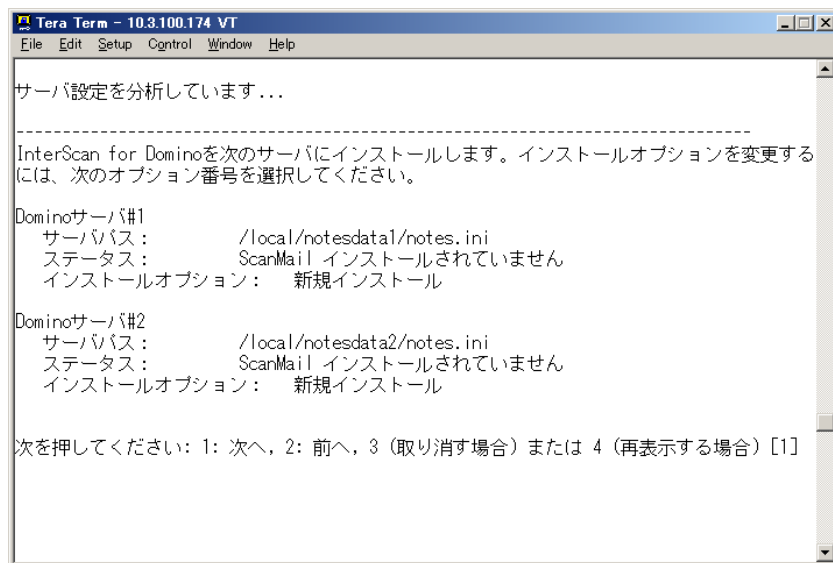


図 2-22. 設定の解析結果

9. データベース複製の設定画面では、複製できる InterScan データベースをセットアップ時に選択します。

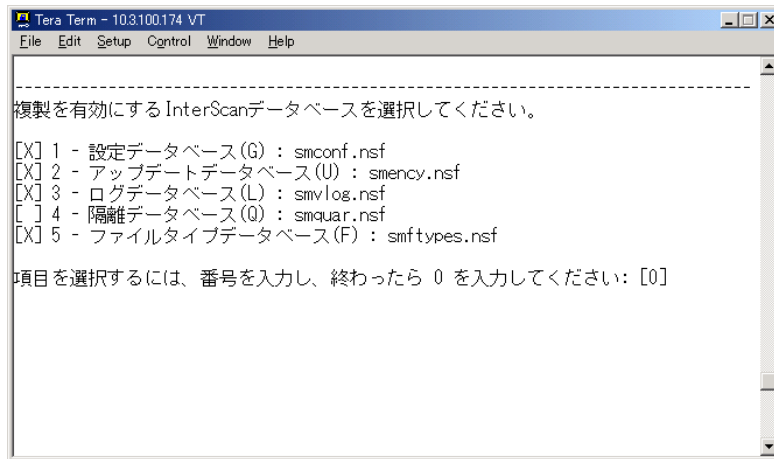


図 2-23. データベース複製の設定

セットアッププログラムの初期設定では、隔離データベースを除くすべての InterScan データベースが複製対象として選択されています。初期設定を変更する場合には、複製する InterScan データベースを選択または選択解除します。複数のサーバ上で InterScan をインストールし、データベースを複製する場合、2 つ目以降のサーバにおいて設定データベースの複製を無効にすることができます。1 つのサーバをプライマリサーバまたは管理サーバとして選択し、その他のすべてのサーバに複製します。

注意： インストール終了後、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。

10. 初期設定ポリシーを受け入れるかどうかを選択します。

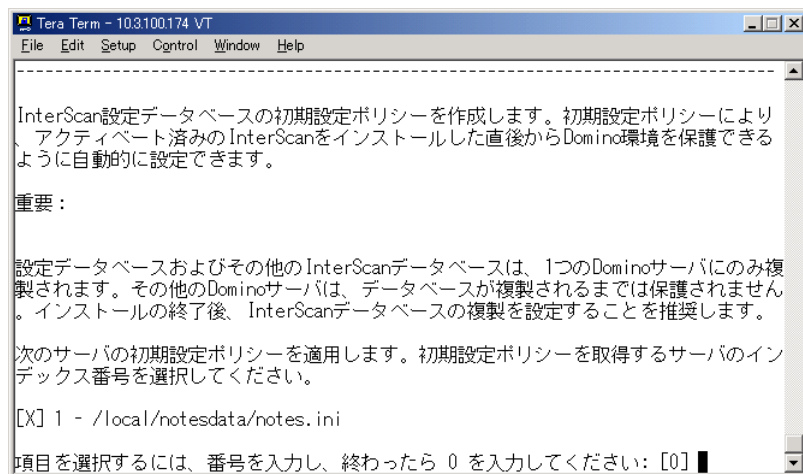


図 2-24. 初期設定ポリシーの受け入れ

11. InterScan 管理者の設定画面では、次のいずれかを実行します。

- すべての InterScan データベースに対する管理者権限を持つユーザの名前を入力します。たとえば、notes_admin 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、各サーバの管理者アカウントを入力します。

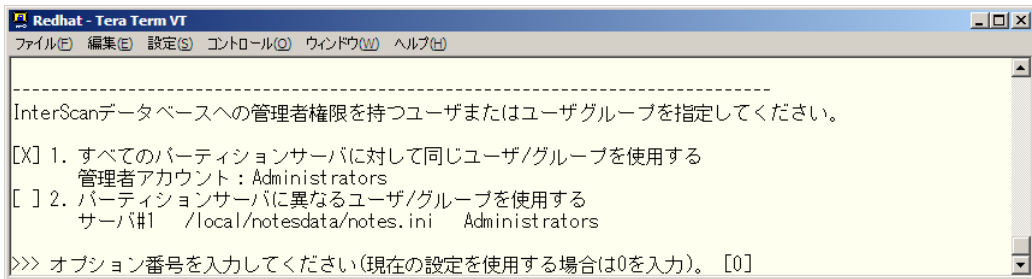


図 2-25. 管理者アカウント設定

注意： 指定したアカウントが存在しない場合には、インストール完了時に作成します。アカウントには管理者権限があることを確認してください。

12. InterScan データベースへの署名画面では、次のいずれかを実行します。

- [データベースへの署名を省略する] を選択して InterScan データベースへの署名を後日行う場合は、「2」を入力します。

この場合は、インストール終了後に手動で InterScan データベースに署名します。方法については、117 ページの「データベースへの署名」を参照してください。

- [すべての対象サーバに対して単一の ID ファイルを使用する] を選択し、単一の ID を使用して InterScan データベースに署名するには、「3」を選択します。

フルパス付きの ID とパスワードを入力します。

- [対象サーバ / パーティションに対して異なる ID を使用する] を選択し、パーティションごとに異なる ID で InterScan データベースに署名するには、「4」を選択します。

フルパス付きの ID とパスワードを入力します。

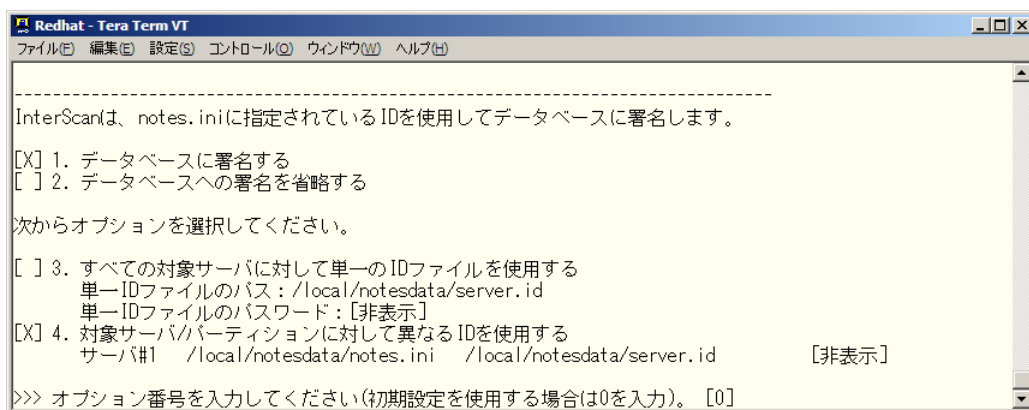


図 2-26. データベースへの署名画面

InterScan のコンポーネントがインストール先のサーバにコピーされます。

13. インストールが終了した後、<Enter> キーを押してセットアップを終了します。

これで InterScan のインストールが終了しました。

Domino サーバの起動

InterScan のインストールが終了した後は、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、87 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、「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]→[Lotus Applications]→[Domino Server] の順に選択します。

Linux/Solaris/AIX プラットフォームで Domino サーバを起動するには

1. 次のコマンドを実行して環境変数を設定します。これにより、Domino やその他のアプリケーションがハングアップするのを防ぐことができます。
(LinuxThread を使用してる Linux プラットフォームのみ)

```
export LD_ASSUME_KERNEL=2.2.5
```

2. root アカウントではなく、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。これを確認するには、コマンド `whoami` または `id` を実行します。
3. Domino データディレクトリ (例: `/local/notesdata`) に切り替えます。コマンドプロンプトで次のコマンドを入力して、Domino サーバを起動します。

```
server
```

— または —

```
server -jc &
```

ヒント： シェル環境をカスタマイズしていない場合には、次のコマンドを実行して Domino のスタートアップスクリプトを実行してください。

```
/opt/lotus/bin/server
```

i5/OS および OS/400 プラットフォームで Domino サーバを起動するには

CL コマンド、`strdomsvr` を実行します。

Domino サーバの起動方法の詳細については、Domino のマニュアルを参照してください。

他のウイルス対策製品を使用している場合の注意

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、検索の競合が発生するのを避けるため、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ます。「検索に使用する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してください。

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 のアクティベーション

InterScan の機能を利用するには、インストール時またはインストール後に InterScan データベースで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」はご購入の製品に同梱されています。詳細については購入元にお問い合わせください。

アクティベーションコード

InterScan のアクティベーションコードには、次の 3 種類があります。

- 体験版アクティベーションコードを使用すると、30 日間、InterScan の機能をすべて使用できます。体験期版の有効期間中は、不正プログラムとスパムメールのフィルタ処理、検索、コンポーネントのアップデートが可能です。体験版アクティベーションコードの有効期限が切れると、InterScan のタスクはロードできませんが、Domino 環境の保護機能はすべて無効となります。

- スタンダード版アクティベーションコードを使用すると、コンテンツフィルタおよびスパムメールフィルタを除く機能を実装できます。スタンダード版ではあらゆるモードでのウイルス検索とコンポーネントアップグレードが提供されます。ただし、コンテンツフィルタとスパムメールフィルタは使用できません。
- スイート版アクティベーションコードを使用すると、コンテンツフィルタおよびスパムメールフィルタを含む InterScan の機能をすべて実装できます。

注意： Windows、Linux、Solaris、および AIX 版向けにはスイート版のみの提供となります。i5/OS および OS/400 プラットフォーム向けにはスタンダード版のみの提供となります。

InterScan では、設定されている有効期限の残り日数が Domino サーバのコンソールに表示されます。有効期限が切れる前に新しいアクティベーションコードを入手し、Domino 環境を継続して保護できるようにすることをお勧めします。

アクティベーションの実行

製品パッケージに同梱されているアクティベーションコードを使用して InterScan をアクティベートし、アップデートされたプログラムコンポーネントのダウンロード機能など、InterScan のすべての機能を利用可能にします。

設定データベースからアクティベートを実行するには

1. 設定データベースを開きます。
2. メインメニューで、[管理]→[製品ライセンス] の順に選択します。
3. ライセンスプロファイルを作成します (195 ページの「ライセンスプロファイルの作成」を参照)。
4. インストールで作成されたライセンスプロファイルを削除します (195 ページの「ライセンスプロファイルの削除」を参照)。

製品版へのアップグレード

InterScan を体験版から製品版にアップグレードした後、アクティベートして、体験期間が過ぎた後も継続して使用できるようにします。InterScan をアクティベートし、アップデートされたプログラムコンポーネントのダウンロード機能など、InterScan のすべての機能を利用可能にします。

製品版にアップグレードするには

1. 製品版アクティベーションコードを入手します。
2. ライセンスプロファイルを作成します (195 ページの「ライセンスプロファイルの作成」を参照)。
3. 体験版用のライセンスプロファイルを削除します (195 ページの「ライセンスプロファイルの削除」を参照)。

EICAR によるインストールのテスト

EICAR 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 (European Institute for Computer Antivirus Research) 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。このファイルはウイルスではなく、自己複製機能也没有。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 文字の文字列を入力します。
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。

インストール後のファイルとフォルダの確認

InterScan と Control Manager 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。

- 302 ページの「Windows サーバにインストールされるファイル」
- 304 ページの「Linux/Solaris/AIX サーバにインストールされるファイル」
- 306 ページの「i5/OS および OS/400 サーバにインストールされるファイル」

InterScan 用 Control Manager エージェントのインストール

Trend Micro Control Manager (以下、Control Manager) は、複数の InterScan をインストールしている場合、または複数のトレンドマイクロ製品の使用している場合、ウイルス対策とコンテンツセキュリティ対策を統合することができる集中管理コンソールです。

InterScan 用の Control Manager エージェントをインストールすると、Control Manager コンソールから、ウイルスログの分析や、ウイルスパターンファイルおよび検索エンジンの一括アップデートが可能になります。

注意：Control Manager エージェントは、i5/OS では使用できません。

この章では、InterScan 用 Control Manager エージェントのインストール方法について説明します。この章で説明する項目は次のとおりです。

- 90 ページの「InterScan 用 Control Manager エージェントのインストール」
- 94 ページの「ウィザードベースのインストールの実行」
- 103 ページの「コンソールベースのインストールの実行」
- 110 ページの「Control Manager エージェントのインストールの確認」
- 111 ページの「Control Manager エージェントインストール後の InterScan ファイルおよびフォルダの確認」

InterScan 用 Control Manager エージェントのインストール

Control Manager エージェントをインストールするときは、次の点を考慮します。

- InterScan for Lotus Notes 用の Control Manager エージェントがインストールされている場合、InterScan for Domino 用の Control Manager エージェントを別にインストールする必要があります。
- Domino サーバに他のウイルス対策製品用の Control Manager エージェントがインストールされていても、InterScan 用 Control Manager エージェントを別途インストールする必要があります。
- InterScan を実行しているサーバごとにエージェントを 1 つインストールします。
- Domino パーティションサーバに対しては、パーティションごとに Control Manager エージェントをインストールする必要があります。
- InterScan のセットアップでは Domino サーバを停止しておく必要があるのに対し、Control Manager エージェントのセットアップでは Domino サーバを起動しておく必要があります。そのため、まずすべてのパーティションに InterScan をインストールし、その後サーバを起動してすべてのエージェントをインストールします。
- Control Manager では、さまざまなプラットフォームに配置された管理下の製品を一括してアップデートできます。

バージョン 2.5x または 2.6x からのアップグレード

Control Manager を使用している場合、InterScan for Domino 用の Control Manager エージェントをインストールする前に InterScan 2.5 または 2.6 用の既存の Control Manager エージェントをアンインストールします。InterScan for Domino をインストールする前に、既存の Control Manager エージェントをアンインストールすることをお勧めします。まず InterScan for Domino をインストールしてから Control Manager エージェントの最新バージョンをインストールします。

インストールの準備

InterScan 用 Control Manager エージェントをインストールする前に、次の作業を実行します。

- エージェントをインストールする InterScan サーバの管理者アカウントまたは同等の権限を持つアカウントを確認します。
- 管理者権限の Control Manager のユーザ ID を入手します。

注意：Control Manager エージェントのインストールに使用した Control Manager アカウントは削除しないでください。このアカウントを削除すると、Control Manager サーバへのエージェントの再登録ができなくなります。

- Domino サーバと Control Manager サーバ間の通信に telnet コマンドを使用する際、Control Manager サーバとネットワーク環境が適切に対話していることを確認します。次のポートをテストします。
 - ◆ TELNET <Control Manager の IP アドレス>
 - ◆ HTTP
 - ◆ 10198
 - ◆ 10319
 - ◆ SSL
- エージェントを登録する Control Manager サーバの公開鍵を入手して、その場所を確認します (i5/OS、OS/400 版の InterScan for Domino では不要)。

注意：他のトレンドマイクロ製品用の Control Manager エージェントがインストールされていても、InterScan 用のエージェントを別にインストールする必要があります。ただし、他の製品が登録されている Control Manager サーバに InterScan を登録する場合は、公開鍵を入手する必要はありません。Domino サーバ上に他製品の Control Manager エージェントが存在する場合、Control Manager の通信インフラストラクチャは共有されるため、新たにインストールされることはありません。

- サーバに固有の情報を収集するときは、299 ページの「Control Manager エージェントのチェックリスト」を印刷し、確認すると効果的です。

注意： AIX 版、Solaris 版、i5/OS および OS/400 版では、InterScan for Lotus Notes 2.6 用 Control Manager エージェントから InterScan for Domino 3.0 用 Control Manager エージェントへのアップグレードをサポートしていません。InterScan for Lotus Notes 2.6 用 Control Manager エージェントを事前にアンインストールしてから InterScan for Domino 3.0 用 Control Manager エージェントをインストールしてください。

公開鍵 (E2EPublic.dat) の入手

Control Manager エージェントは、公開鍵 E2EPublic.dat を使用して、自身の登録先となる Control Manager サーバを特定します。この鍵は、Control Manager エージェントをインストールするときに必要です。

E2EPublic.dat を入手するには

1. Control Manager 管理コンソールにアクセスします (244 ページを参照)。
2. メニューの [製品] をクリックします。
3. メインメニューで、[製品エージェントの追加 / 削除] をクリックします。

[公開鍵] を右クリックしてから、[対象をファイルに保存] をクリックします。エージェントのインストールプログラムからアクセスできる場所に、E2EPublic.dat ファイルを保存します。

セットアップモード

InterScan 用 Control Manager エージェントのインストールでは、次のセットアップモードを選択できます。

- ウィザードベースのインストール – グラフィカルユーザインタフェースをサポートしているサーバに InterScan 用 Control Manager エージェントをインストールする際に、ユーザに各種情報の入力を求めます。

ウィザードベースのインストールでは、エージェントのインストールを容易にするインタフェースが順次表示されます。94 ページを参照してください。

- コンソールベースのインストール – グラフィカルユーザインタフェースをサポートしていないサーバに Control Manager エージェントをインストールする際に、ユーザが入力しながらインストールを進めます。

Windows 以外の各プラットフォームに InterScan 用 Control Manager エージェントをセットアップするときは、この方法を使用します。103 ページを参照してください。

ウィザードベースのインストールの実行

Control Manager をインストールするプラットフォーム用の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。i5/OS および OS/400 版では、グラフィカルインタフェースベースのインストールはサポートされていません。

InterScan 用 Control Manager エージェントをグラフィカルユーザインタフェースからインストールするには

注意： ウィザードベースのインストール手順の説明では、Windows 版の InterScan 用 Control Manager エージェントのセットアップで表示されるスクリーンショットを使用しています。

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。
 - 製品 CD-ROM からインストールする場合は、Control Manager エージェントのフォルダ (cmagent) 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、コンピュータ内でそのファイルを格納したフォルダに移動します。通常、このフォルダは InterScan のインストールプログラムが格納されているディレクトリのサブディレクトリ \cmagent です。
2. 次のいずれかのファイルを実行して、セットアッププログラムを起動します。

プラットフォーム	セットアッププログラム
Windows	smd3-windows-cmagent.exe
Linux	CMAgent3SetupLinux.bin
Solaris	CMAgent3Setupsolaris.bin
AIX	CMAgent3SetupAix.bin

3. プログラムが起動すると、InstallShield の開始画面が表示され、図 3-1 に示すインストール開始画面が表示されます。



図 3-1. [[InterScan for Domino 用 Control Manager エージェント セットアップ] - 開始画面

4. [次へ] をクリックします。図 3-2 に示す使用許諾契約画面が表示されます。

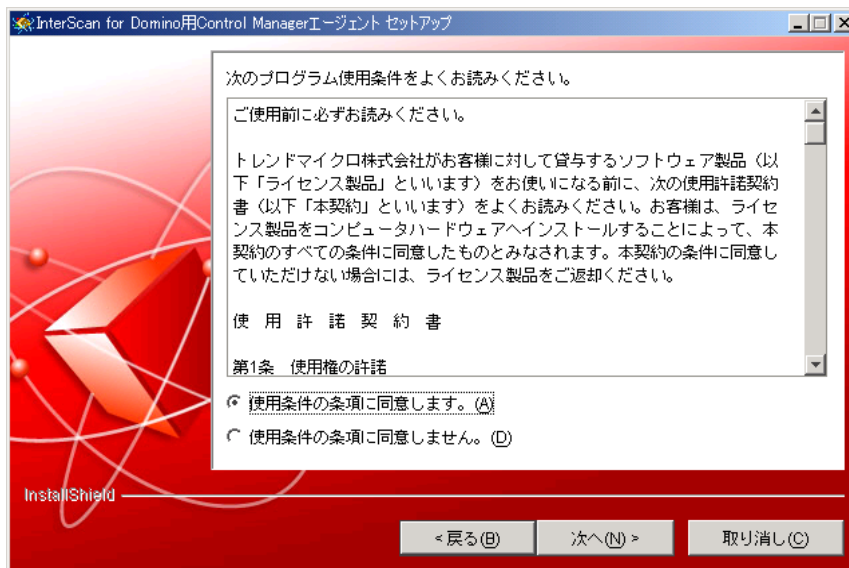


図 3-2. [InterScan for Domino 用 Control Manager エージェント セットアップ] - 使用許諾契約画面

使用許諾契約をすべて読み終えたら、[使用条件の条項に同意します] 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、[使用条件の条項に同意しません] をクリックします。インストールは中止されます。

5. [次へ] をクリックします。インストールファイルがローカルの作業ディレクトリに抽出された後、Domino サーバ解析画面 (図 3-3) が表示されます。

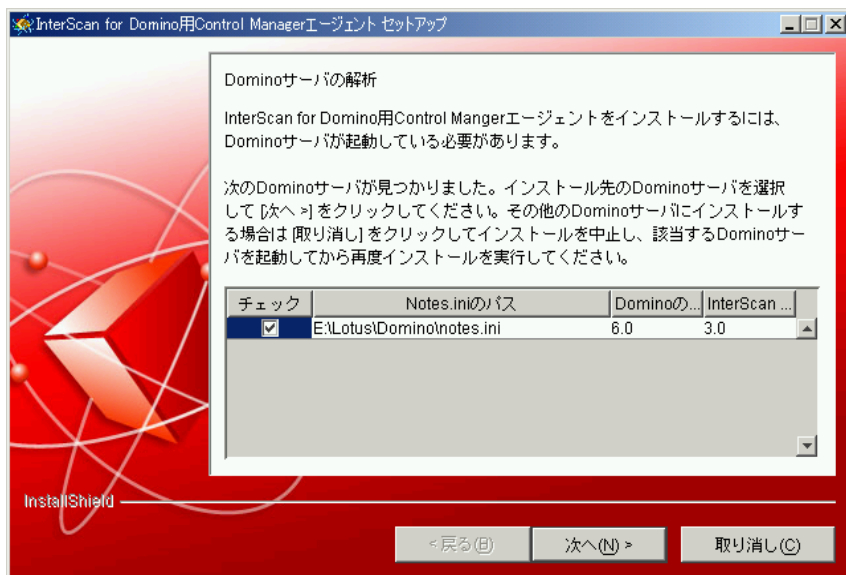


図 3-3. [InterScan for Domino 用 Control Manager エージェント セットアップ] - Domino サーバ解析画面

Control Manager エージェントをインストールするサーバを選択するには、対象サーバのチェックボックスをオンにして [次へ] をクリックします。

選択したサーバに、同じバージョンの Control Manager エージェントがすでにインストールされており、新規インストールが実行されていない場合、このままインストールを続行するかどうかを確認するメッセージが表示されます。

- 新しい Domino サーバ用の Control Manager エージェントをインストールする場合は、[はい] をクリックします。
- サーバに対する変更は何も行わずにインストールプロセスを終了する場合は、[いいえ] をクリックします。

注意： Trend Micro Management Infrastructure (TMI) がサーバにすでにインストールされている場合、既存の TMI が使用されるため、手順 5 と 6 は省略されます。TMI の詳細については、242 ページの「Control Manager エージェントについ

て」を参照してください。

6. Windows 版のみ [次へ] をクリックすると、図 3-4 に示すメッセージルーティングパス設定画面が表示されます。Control Manager サーバと InterScan サーバ間で送受信されるメッセージのルーティングを指定します。

受信メッセージのパスを設定するには

[受信メッセージの送信先] を選択し、次のいずれかのオプションを選択します。

- すべてのホスト — すべての送信元からのメッセージを受け入れます。
- IP ポート転送 — [ファイアウォール IP] にファイアウォールの IP アドレスを入力し、[ポート] に Control Manager との通信のために開かれているポート番号を入力します。
- プロキシサーバ — プロキシサーバを使用する場合に選択します。

[プロキシサーバ設定] をクリックして、プロキシサーバを設定します。

送信メッセージのパスを設定するには

[送信メッセージのルーティング] を選択し、次のいずれかの方法を選択します。

- サーバに直接送信する
- プロキシサーバを設定する

[プロキシサーバ設定] をクリックしてプロキシサーバを設定します。

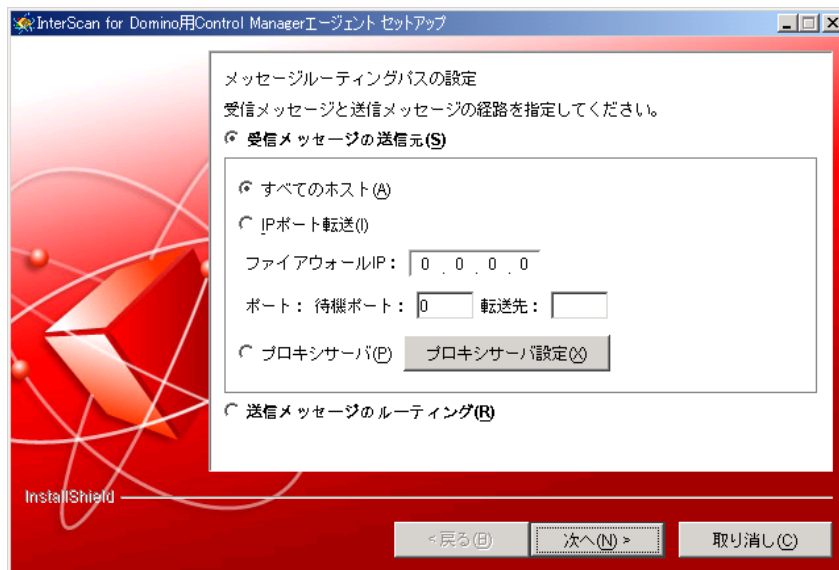


図 3-4. [InterScan for Domino 用 Control Manager エージェント セットアップ] - メッセージルーティングパス画面

[次へ] をクリックします。

7. [次へ] をクリックすると、図 3-5 に示す公開鍵の指定画面が表示されます。[インポート] をクリックします。エージェントを登録する Control Manager サーバの公開鍵 (E2EPublic.dat) を指定して、[開く] をクリックします。

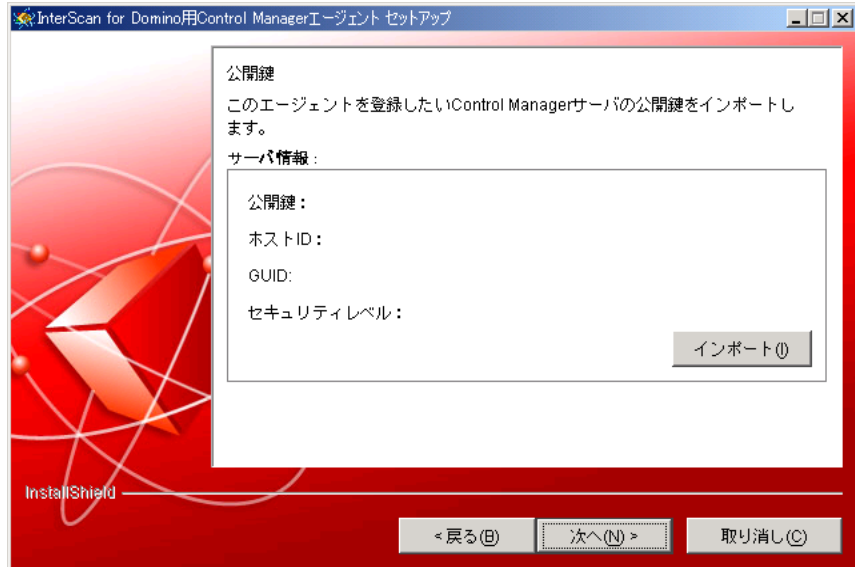


図 3-5. 公開鍵インポート選択画面

- Windows 版では、Control Manager エージェントによって公開鍵ファイルがインポートされ、公開鍵ファイルに含まれている情報の一部がサーバ情報ビュー画面に表示されます。
- Linux 版、AIX 版、および Solaris 版では、インストールプログラムによって公開鍵ファイルがインポートされますが、サーバ情報ビュー画面は表示されません。

8. [次へ] をクリックします。図 3-6 に示す Control Manager サーバ登録画面が表示されます。

[ユーザ ID]フィールドに、root 権限の Control Manager アカウントの名前を入力します。

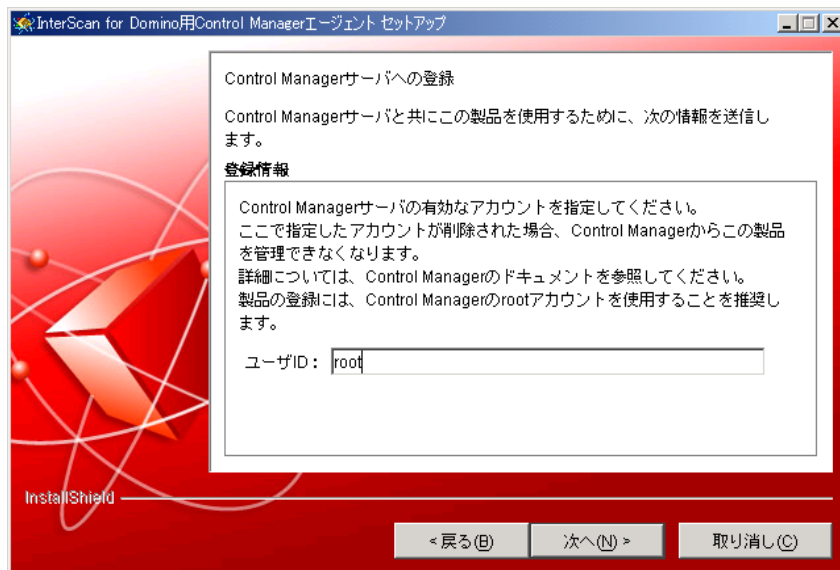


図 3-6. [InterScan for Domino 用 Control Manager エージェント セットアップ] - Control Manager サーバ登録画面

9. [次へ] をクリックします。[管理下の製品名] フィールドをダブルクリックして、Control Managerの製品ディレクトリに表示する管理下の製品名を指定します。



図 3-7. [InterScan for Domino 用 Control Manager エージェント セットアップ] - Domino サーバチェック結果画面

警告： 上記の手順で指定したユーザ ID が Control Manager サーバから削除されると、製品を管理できなくなります。

10. [次へ] をクリックします。エージェントのインストール画面で、インストール状況を監視します。
11. 最後の画面で [終了] をクリックします。

これで Control Manager エージェントがインストールされました。110 ページを参照して、Control Manager エージェントが正常にインストールされたことを確認します。

コンソールベースのインストールの実行

InterScan for Domino が Linux、Solaris、AIX、i5/OS および OS/400 プラットフォームで稼動している場合、コンソールベースの InterScan 用 Control Manager エージェントのインストールを実行できます。インストールの流れはウィザードベースのセットアップとほぼ同じですが、手順 5 については Windows プラットフォームのみに適用されます。

Control Manager エージェントをコマンドラインからインストールするには

注意： コンソールベースの InterScan のインストール手順の説明では、Solaris 版のスクリーンショットを使用しています。

1. 次のいずれかの方法で、セットアッププログラムがあるフォルダに移動します。
 - 製品 CD-ROM がある場合は、CD-ROM をコンピュータに入れて InterScan for Domino フォルダの \cmagent サブ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、サーバの \cmagent サブフォルダに移動します。

2. 次のコマンドを入力して、コンソールベースのインストールを開始します。

プラットフォーム	セットアッププログラム
Linux	<code>./CMAgent3SetupLinuxbin -console</code>
Solaris	<code>./CMAgent3Setupsolaris.bin -console</code>
AIX	<code>./CMAgent3SetupAix.bin -console</code>
i5/OS、 OS/400	<code>java -cp /QIBM/Prod/Data/Java400/jt400ntv.jar:./setup.jar run -console</code>

セットアッププログラムが起動し、開始メッセージが表示されます。

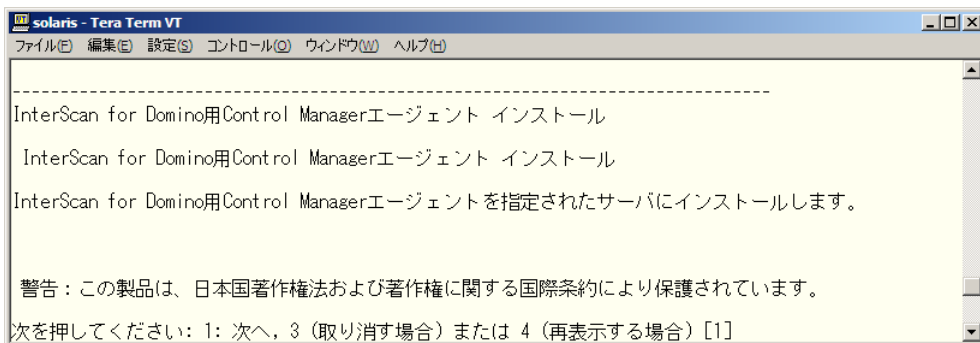


図 3-8. Control Manager エージェントのセットアップ開始画面

ヒント： コンソールベースのセットアップでは、既存の設定をそのまま使用する場合は <Enter> キーを押し、次の手順に進む場合は「1」を入力します。セットアップを中止する場合は、「3」を入力します。

ほとんどの画面では、次の数値入力による操作が可能です。

- 0: 既存の設定をそのまま使用します。
- 1: 次の画面に進みます。
- 2: 前の画面に戻ります。
- 3: セットアップを中止します。
- 4: 現在の画面を再表示します。

3. 「1」を入力して、Control Manager エージェントのセットアップを開始します。

4. 使用許諾契約画面が表示されます。<Enter> キーを押して処理を続行します。

使用許諾契約のプロンプトで、[I accept the terms of the license agreement.] を選択して Control Manager エージェントをインストールする場合は、「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。

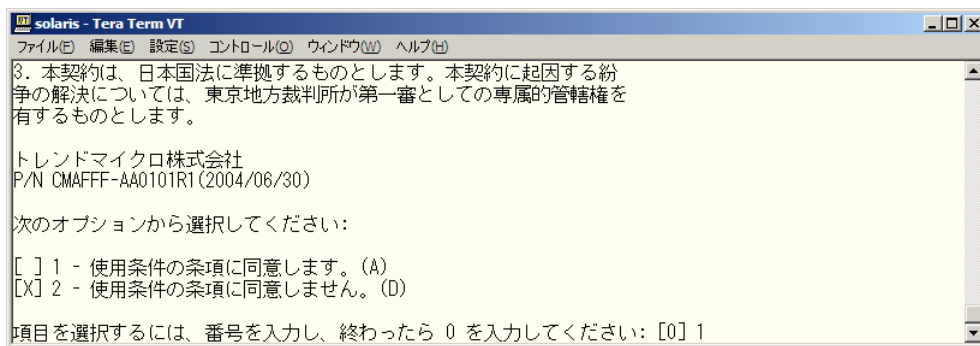


図 3-9. Control Manager エージェントの使用許諾契約

セットアッププログラムによって、インストールファイルがローカルの作業ディレクトリに抽出されます。

5. (i5/OS および OS/400 版では、この手順は省略します。)公開鍵のプロンプトで、公開鍵ファイル名とそのディレクトリパスを入力します。

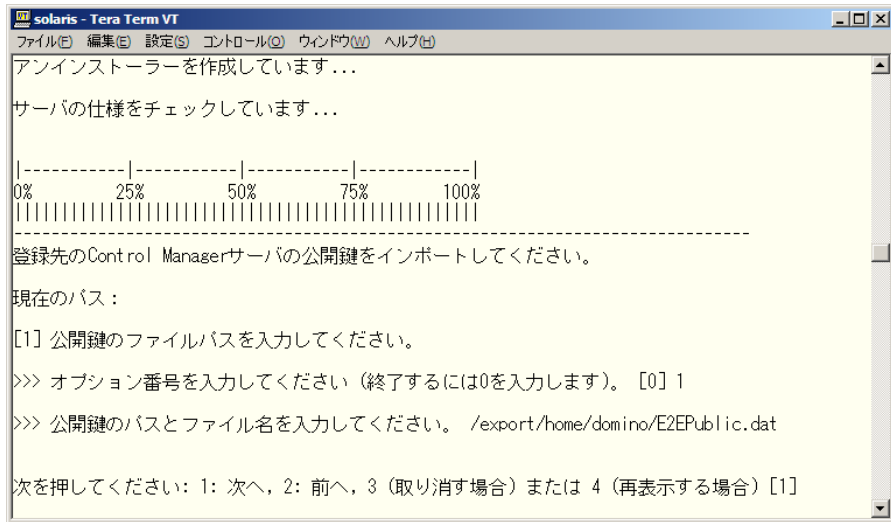


図 3-10. 公開鍵

注意： Domino サーバにすでに TMI がインストールされている場合、エージェントは既存の TMI を使用するので、手順 5 は省略されます。

6. Control Manager エージェントを i5/OS または OS/400 にインストールする場合は、Control Manager サーバの IP アドレスを入力するよう求められます。Control Manager サーバで初期設定ポート (80) 以外の HTTP ポートを使用している場合は、IP アドレスにポート番号を追加します。<Control Manager サーバの IP アドレス>:<ポート番号> の形式で入力してください。
- IP アドレスを入力したら、次に「0」を入力して設定を確定します。IP アドレスを変更する場合は、「1」を入力します。

7. Domino サーバの解析画面で、インストール先サーバのインデックス番号を入力します。たとえば、サーバ 1 を設定するには「1」を入力します。

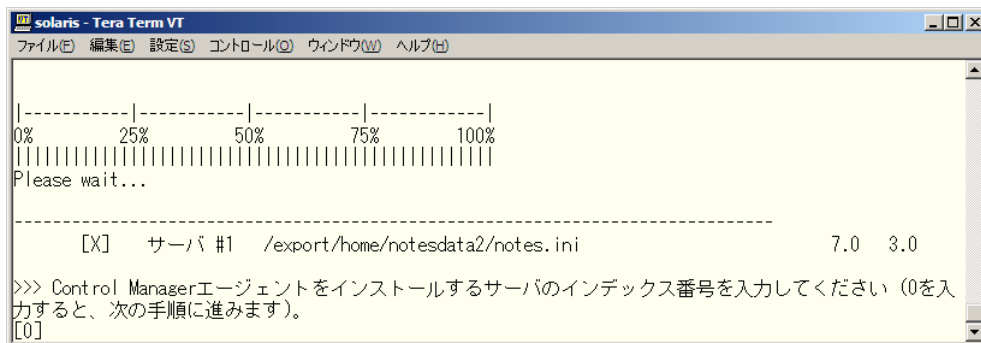


図 3-11. Domino サーバの解析

8. 登録情報画面で、InterScan を Control Manager サーバに登録する際に使用する、root 権限の Control Manager アカウントを入力します。

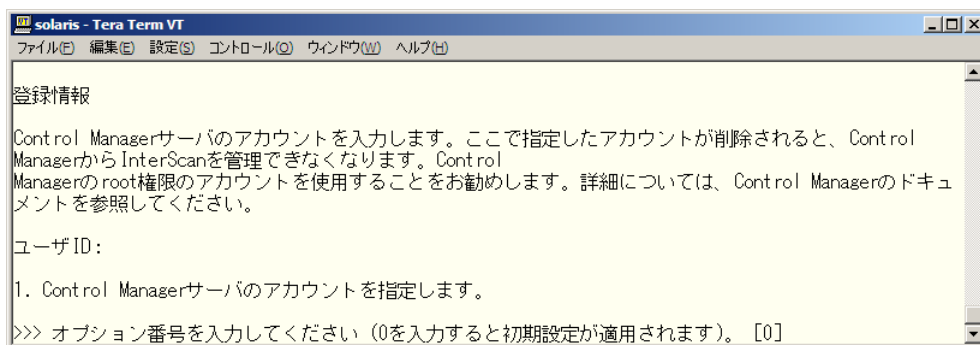


図 3-12. Control Manager サーバの登録情報

注意： 上記の手順で指定した Control Manager ユーザ ID が Control Manager サーバから削除されると、Control Manager で製品を管理できなくなります。

9. 管理下の製品名画面で、Control Manager の製品ディレクトリに表示する InterScan の製品名 (エンティティ名) を入力します。

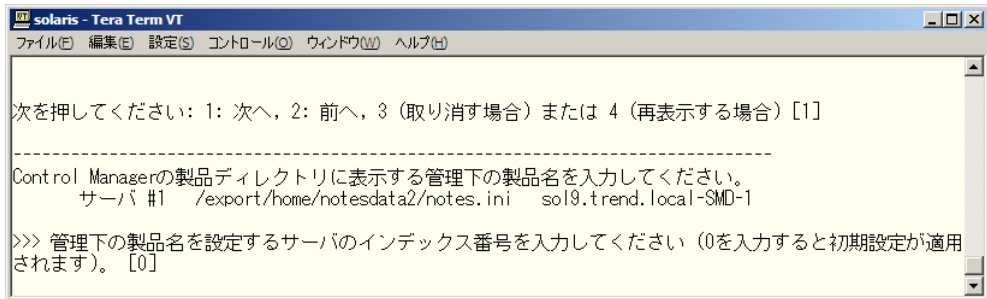


図 3-13. 管理下の製品名

ヒント: InterScan サーバの用途を的確に表現するような製品名を割り当てると便利です (例: SMD_NYmail1)。インストールプログラムによって生成された名前を確認します (名前は notes.ini の後に出力されます)。システム環境によって設定されたホスト名がヌルの場合は、意味のあるエンティティ名を入力します。名前にスペースは使用できません。

10. 「1」を入力して、Control Manager エージェントのセットアップを開始します。

11. <Enter> キーを押してセットアップを完了します。

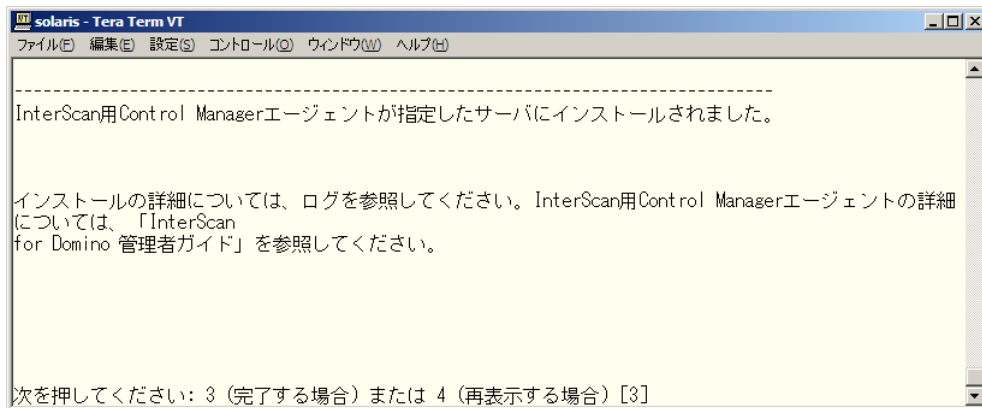


図 3-14. インストール完了

110 ページを参照して、Control Manager エージェントが正常にインストールされたことを確認します。

Control Manager エージェントのインストールの確認

エージェントが正常にインストールされていることを確認するには、Control Manager 管理コンソールにアクセスして、目的の製品が Control Manager に正しく登録されているかどうか、および製品ディレクトリに管理下の製品として一覧表示されているかどうかを調べます。

Control Manager エージェントが正常にインストールされたことを確認するには

1. Control Manager 管理コンソールにアクセスします (244 ページを参照)。
2. メインメニューの [製品] をクリックします。
3. メインメニューで、リストから [管理下の製品]を選択し、[表示] をクリックします。

製品ディレクトリの [新規エンティティ] フォルダに InterScan の管理下の製品のアイコンが表示されます。

InterScan の管理下の製品が表示されない場合は、次の手順を試します。

1. 製品ディレクトリを更新します。メインメニューの右上角にある [更新] アイコンをクリックします。
2. InterScan サーバから Control Manager サーバに ping コマンドを送信し、両サーバが正常に接続されていることを確認します。
3. InterScan サーバ上で Trend Micro Management Infrastructure サービスを再起動します。

4. InterScan 用 Control Manager エージェントを再インストールします。詳細については、90 ページの「InterScan 用 Control Manager エージェントのインストール」を参照してください。

注意： Domino サーバの ID ファイルがパスワードで保護されている場合、Control Manager エージェントをインストールしても、エージェントは実行されません。この問題の解決方法については、トレンドマイクロのサポートチームにお問い合わせください。

Control Manager エージェントインストール後の InterScan ファイルおよびフォルダの確認

InterScan と Control Manager 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。

- 302 ページの「Windows サーバにインストールされるファイル」
- 304 ページの「Linux/Solaris/AIX サーバにインストールされるファイル」
- 306 ページの「i5/OS および OS/400 サーバにインストールされるファイル」

基本設定

この章では、Trend Micro InterScan for Domino 3.0 (以下、InterScan) のインストール後およびアクティベーション後に行う設定作業について説明します。

この章で説明する項目は次のとおりです。

- 114 ページの「InterScan のインタフェースの概要」
- 115 ページの「ヘルプデータベースおよびヒントへのアクセス」
- 116 ページの「インストール後の手動検索の実行」
- 116 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」
- 118 ページの「InterScan データベースへのアクセス権およびロールの定義」
- 117 ページの「データベースへの署名」
- 118 ページの「InterScan データベースへのアクセス権およびロールの定義」
- 120 ページの「InterScan データベースへのアクセス」

InterScan のインタフェースの概要

InterScan のインタフェースの画面は、次のようになっています。

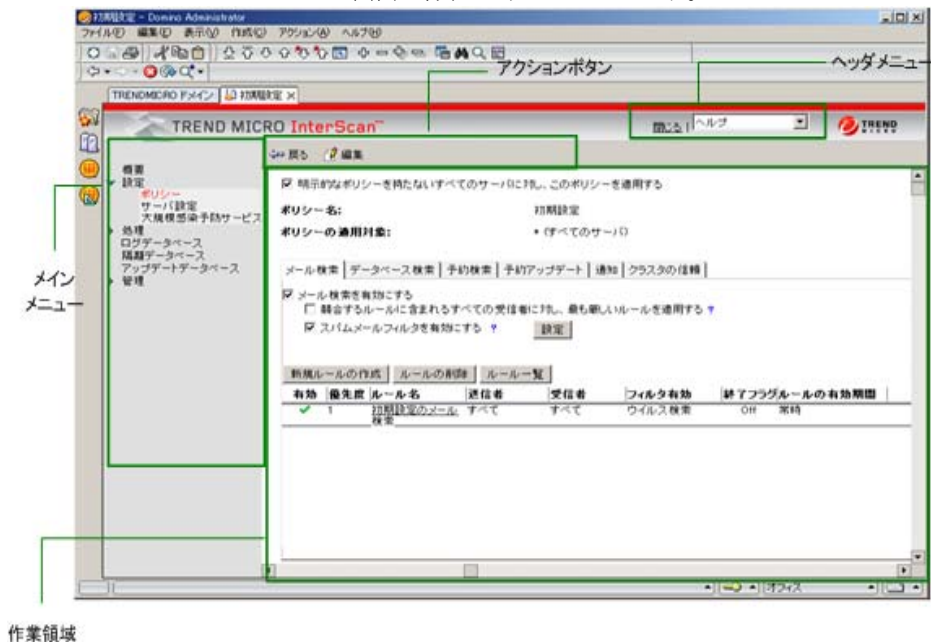


図 4-1. InterScan のインタフェース

このインタフェースには、次の領域があります。

領域	目的
アクションボタン	設定の編集や前に表示されていた文書に戻るなど、特定の処理を実行できます。
ヘッダメニュー	InterScan の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あります。
メインメニュー	InterScan の各機能や他の InterScan データベースへのショートカットを提供します。
作業領域	InterScan インタフェースの中心となる領域で、ここで InterScan の各種オプションを設定できます。

ヒント：InterScan データベースの表示には、1024 x 768 ピクセルの画面領域の使用が適しています。

ヘルプデータベースおよびヒントへのアクセス

InterScan ヘルプデータベースには、InterScan の基本機能に関する情報が記載されており、関連トピックへの相互参照リンクがあります。各項目の [操作手順] セクションでは、一般的な設定の方法が説明されています。InterScan の操作方法について不明な点がある場合は、この [操作手順] を参照してください。

ヘルプデータベースおよびヒントへのアクセス

- InterScan データベースのヘッダメニューから、[オンラインヘルプ] を選択します。

- オプションのヒントを表示するには、下線付きのラベル、またはオプションの後に置かれている  アイコンをクリックします。

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、ヒントは利用できません。

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索して駆除することをお勧めします。手動検索については、176 ページの「手動データベース検索の実行」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ドライブ上にある 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、145 ページの「データベースの予約検索ルールの作成」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]→[データベース]→[開く] の順にクリックします。
2. [ファイル名] フィールドにパスとファイル名を入力するか、またはリストから選択します。

3. [開く] をクリックします。

注意：Domino を使用している場合、InterScan 管理者データベースを smadmR5.nsf ワークスペースに追加します。

Notes のワークスペースの詳細については、Lotus Notes ヘルプの Notes ワークスペースに関するトピックを参照してください。

データベースへの署名

次の場合は、適切な 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への署名を省略し、はじめてデータベースに署名する場合
- インストール時にデータベースへの署名に使用した ID と別の ID を割り当てる場合

InterScan データベースに署名するには

1. InterScan データベースへの署名に使用する ID を切り替えるには、Lotus 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. Domino Administrator を起動し、InterScan サーバを選択した後、[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] ウィンドウで [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、操作を終了します。

InterScan データベースへのアクセス権およびロールの定義

InterScan データベースへのアクセス権を定義するには、Notes クライアントを使用します。アクセス権を定義することにより、InterScan の機能へのアクセスを制限することができます。

注意： Domino の管理者権限のアカウントであっても、そのアカウントが InterScan データベースに対してアクセス権とロールを持たない場合には、InterScan の機能にアクセスできません。

InterScan データベースへのアクセス権を定義するには

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]→[データベース]→[アクセス制御] の順に選択します。
3. [アクセス制御リスト] ウィンドウの [基本] タブで、データベースの初期設定のアクセス権を [管理者] から [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: なし
InterScan 管理者は、LocalDomainServers や OtherDomainServers とともに、[-Default-] と同じリスト内で、[ユーザー] または [グループ] として表示される必要があります。
4. InterScan 管理者、InterScan サーバ、LocalDomainServer、または OtherDomainServer が[ユーザー]、[サーバー]、[グループ] に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] ウィンドウで、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ったまで前述の操作を繰り返します。
- d. 終了した後 [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。
- ユーザタイプ: 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、続けて下記に示すアクセス権限を割り当てます。

ユーザー、サーバー、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
Anonymous	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

表 4-1. InterScan データベースのアクセス制御リスト

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」以上のアクセス権が必要です。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 (223 ページを参照)。Default ユーザに対しては、どのチェックボックスもオンにしません。

7. 設定データベース (smconf.nsf) については、[ロール] グループで [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。

ロールの割り当てと Notes データベースへのアクセスを調整する方法については、Notes のヘルプにある「ローカルデータベースのアクセスを制御する」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 2 つの方法でアクセスできます。

- Domino クライアントを使用する方法
- Web ブラウザを使用する方法

Notes クライアントを使用したデータベースへのアクセス

Notes クライアントから InterScan の機能に素早く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] メニューから [データベース] を選択し、[開く] をクリックします。
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 smd フォルダ内の [InterScan 設定] (smconf.nsf) を選択します。

5. [開く] をクリックします。

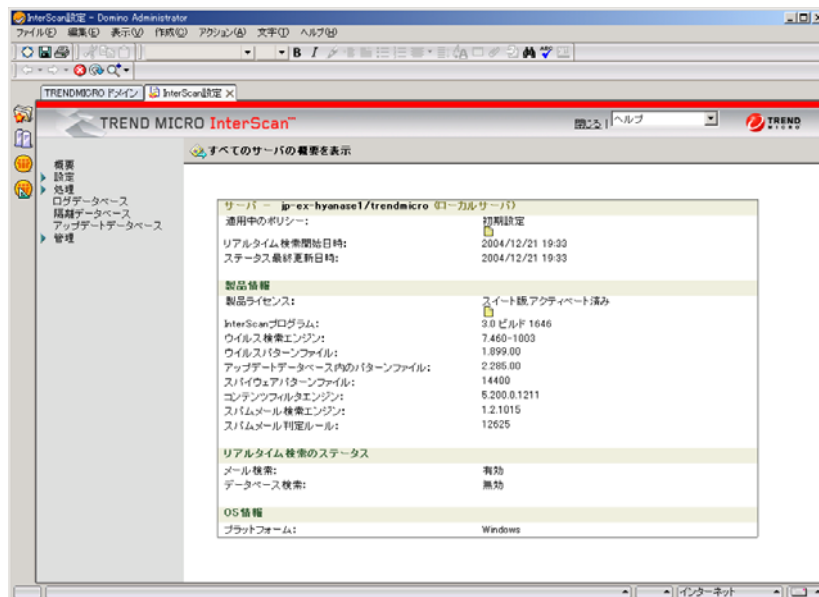


図 4-2. [概要] が設定データベースの初期設定の最初のページとして表示されます。

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。

Web ブラウザを使用したデータベースへのアクセス

Domino サーバ R6 以降を使用し、Notes/Domino HTTP タスクを実行していれば、InterScan の設定データベース、隔離データベース、ログデータベース、アップデートデータベース、およびヘルプデータベースに Web ブラウザからアクセスできます。これは、Domino サーバ文書がデータベースへのアクセスに Web ブラウザを使用することを許可しているためです。

Domino は、InterScan をパスワードでセキュリティ保護します。システム管理者はアドレス帳の HTTP パスワードで各ユーザのパスワードを設定できます。詳細については、124 ページの「Web アクセスするためのインターネットパスワードの設定」を参照してください。アクセス制御リストにより、Notes のワークスペースから設定した場合と同じようにアクセスが制御されます。

Web ブラウザを使用して InterScan データベースにアクセスするには

1. Web ブラウザを開きます。
2. アドレスフィールドに、次の URL を入力します。

`http://{Domino server}/smd/smconf.nsf`

{Domino server} は、Domino サーバのホスト名または IP アドレスです。

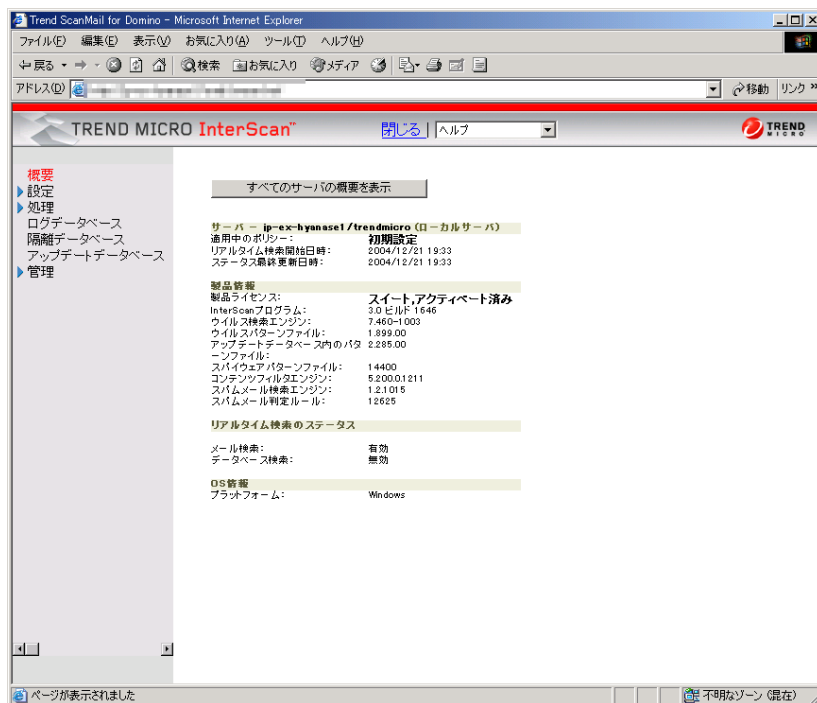


図 4-3. Web ブラウザを使用した InterScan データベースへのアクセス

Web アクセスの制限事項

Web ブラウザを使用して InterScan にアクセスする場合、次の制限があります。

- 作成したポリシー、ルール、およびフィルタは、設定する前に保存する必要があります。
- 設定データベースでは、次のメニューを使用できません。
 - [管理]→[データベース設定]
 - [管理]→[Domino Administrator]

- ログデータベースでは、次のメニューを使用できません。
 - [統計]→[ログ統計]
 - [統計]→[データベース検索履歴]
 - [統計]→[手動削除]

Web アクセスするためのインターネットパスワードの設定

Web ブラウザから安全に InterScan にアクセスできるよう、インターネットパスワードを設定します。InterScan では、Domino のパスワード認証方式を使用してデータベースへのアクセスを制限します。

InterScan データベースへのアクセスに使用するインターネットパスワードを設定するには

1. サーバにあるアドレス帳を開き、アクセスを割り当てるユーザを選択します。
2. [インターネットパスワード] フィールドにパスワードを入力します。
3. [保存して閉じる] をクリックします。

インターネットパスワードに関する詳細については、Lotus Notes/Domino のマニュアルを参照してください。

その他の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. 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

検索タスクの設定

この章では、Trend Micro InterScan for Domino 3.0 (以下、InterScan) における検索タスクの設定方法について説明します。社内のさまざまな個人やグループ向けにポリシーを設定して、不正プログラムやスパム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。

この章で説明する項目は次のとおりです。

- 128 ページの「ポリシーベースのウイルス対策計画」
- 130 ページの「ポリシーの管理」
- 136 ページの「ルールの作成」
- 148 ページの「ルールの整理」
- 150 ページの「フィルタについて」
- 159 ページの「検索オプションの設定」
- 176 ページの「手動データベース検索の実行」

ポリシーベースのウイルス対策計画

InterScan に搭載されているポリシーベースの機能を使用して、標準のウイルス対策とコンテンツセキュリティの設定を確立し、維持管理することをお勧めします。ポリシーを策定すると、次のことができます。

- ウイルス対策設定とアップデート設定を繰り返し作成すること、およびその他の管理作業の自動化
- 環境内サーバの管理の簡易化

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くグループポリシーの作成

共通のロールを持つサーバを複数備える大規模ネットワークでは、初期設定ポリシーに基づくポリシーを使用することで設定に要する時間と維持管理の手間を大幅に削減できます (29 ページの「ポリシー、ルール、フィルタの概要」を参照)。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。

- 特定の管理範囲にあるすべての Domino サーバに割り当てるためのグループポリシーの作成

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。

- ◆ すべての Domino メールサーバ向けに共通の保護としてリアルタイムのメール検索を要求するポリシー
- ◆ 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、およびそのサーバに適用する保護、アップデート、および通知の方法のセットを決定します。たとえば、あるメールサーバを保護するポリシーを作成してから、メールサーバとして機能している他のサーバに適用できます。

- 特定の Domino サーバに割り当てるための独自ポリシーの作成

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、予約検索ルールがある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、次のようにして行われます。

1. InterScan の一般、検索タスク、アップデート、通知オプションを定義するポリシーを作成します。詳細については、29 ページの「ポリシー、ルール、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。詳細については、183 ページの「[サーバ設定] 画面」を参照してください。
3. 同期スケジュールを設定して、環境内の他のサーバに複製するためのポリシーを有効にします。

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設定データベース (smconf.nsf) を追加する必要があります。
[概要] 画面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。詳細については、「すべてのサーバの概要の表示」を参照してください。

注意：サーバ間で複製が正常に実行されるようにするには、データベースの ACL リストに対象のサーバを追加し、管理者権限を付与します。詳細については、194 ページの「アクセス制御リスト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

ポリシーを管理するには、設定データベースを使用します。

ポリシーの作成

ポリシーを作成するには、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. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[設定]→[ポリシー] の順に選択します。

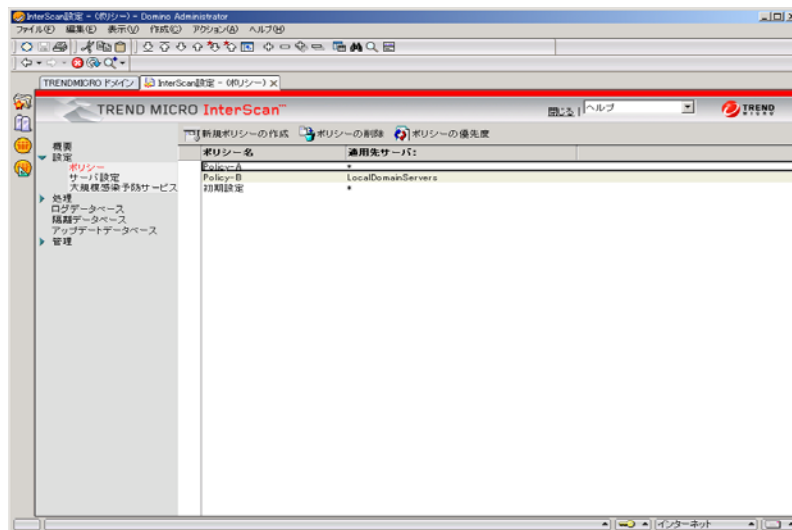


図 5-1. ポリシー画面

3. [新規ポリシーの作成] ボタンをクリックします。

4. ポリシー名を入力します。

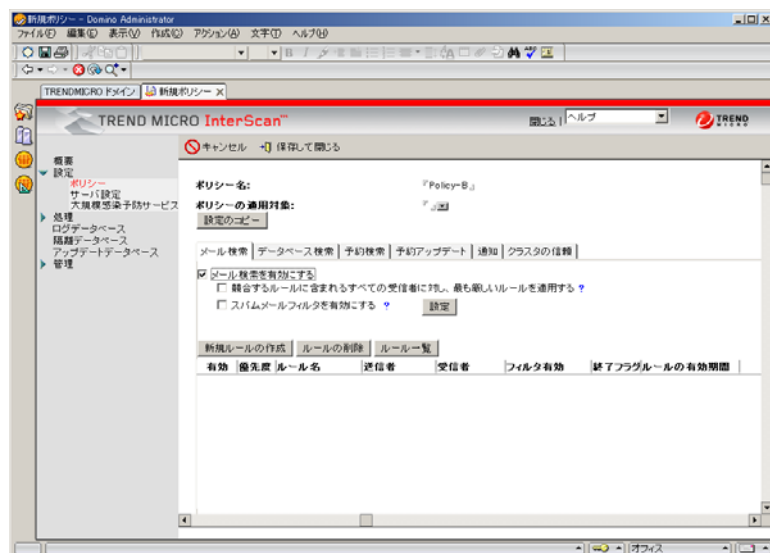


図 5-2. 新規ポリシーの作成

5. ポリシーを適用するサーバまたはサーバグループを、リストから選択するかまたは入力します。

注意： Domino を使用している場合、サーバグループのタイプが [多目的] に設定されている必要があります。

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] では、ポリシー名と適用対象のサーバまたはサーバグループを除いて、コピー元のポリシーと同じ内容のポリシーが作成されます。

7. メール検索ルールを作成します (136 ページを参照)。
8. データベース検索ルールを作成します (142 ページを参照)。

9. 予約検索ルールを作成します (145 ページを参照)。
10. 通知の配信方法を定義します (214 ページを参照)。
11. クラスタの信頼を定義します (133 ページを参照)。
12. [保存して閉じる] をクリックします。

ポリシーの表示画面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、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. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[設定]→[ポリシー] の順に選択します。
3. 作業領域で、対象のポリシーをダブルクリックします。
4. 次のタブを使用して各項目を設定します。[メール検索] タブ (136 ページ)、[データベース検索] タブ (142 ページ)、[予約検索] タブ (145 ページ)、[予約アップデート] タブ (200 ページ)、[通知] タブ (215 ページ)、または [クラスタの信頼] タブ (133 ページ)。
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、設定データベースを使用します。

ポリシーを削除するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[設定]→[ポリシー] の順に選択します。[ポリシー] 画面が表示されます。

3. 削除するポリシーを選択します。
4. 作業領域で削除するポリシーを選択し、[ポリシーの削除] をクリックします。

注意： InterScan の初期設定ポリシーは削除できません。

信頼するクラスタサーバの設定

選択したポリシーを適用するサーバを表示して、クラスタグループ内のサーバを選択するには、[クラスタの信頼] タブを使用します。

注意： 初期設定のポリシーを特定のクラスタグループに適用することはできません。
初期設定のポリシーの [クラスタの信頼] タブでは、クラスタの信頼を設定できません。

信頼するクラスタサーバを設定するには

1. ポリシーを作成 (136 ページを参照) または変更 (132 ページを参照) します。

2. [クラスタの信頼] タブをクリックします。

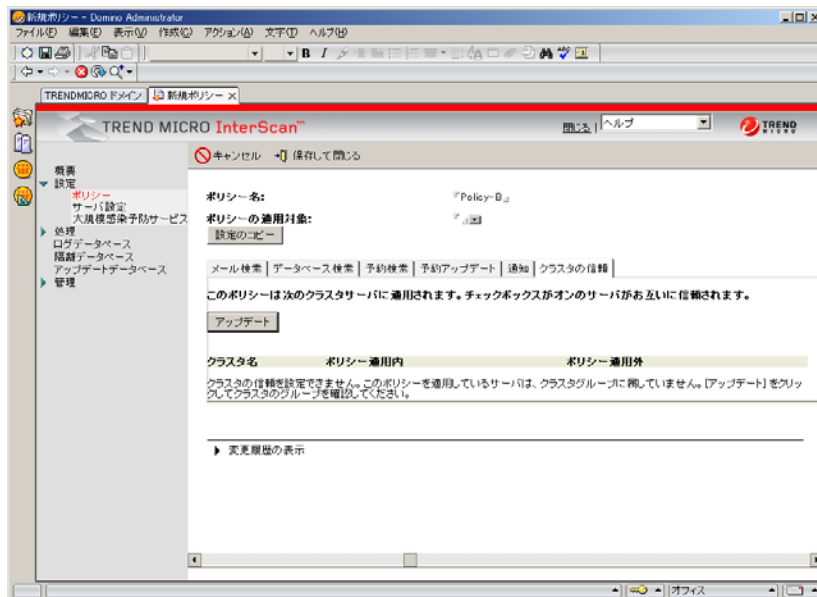


図 5-3. クラスタグループ内のサーバを一覧表示する [クラスタの信頼] 画面

3. 次のいずれかを実行します。

- [クラスタの信頼] 画面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展開して、表示を更新します。
- [クラスタの信頼] 画面にサーバが表示されている場合は、クラスタサーバの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] 画面には、[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 5-4 を参照してください。

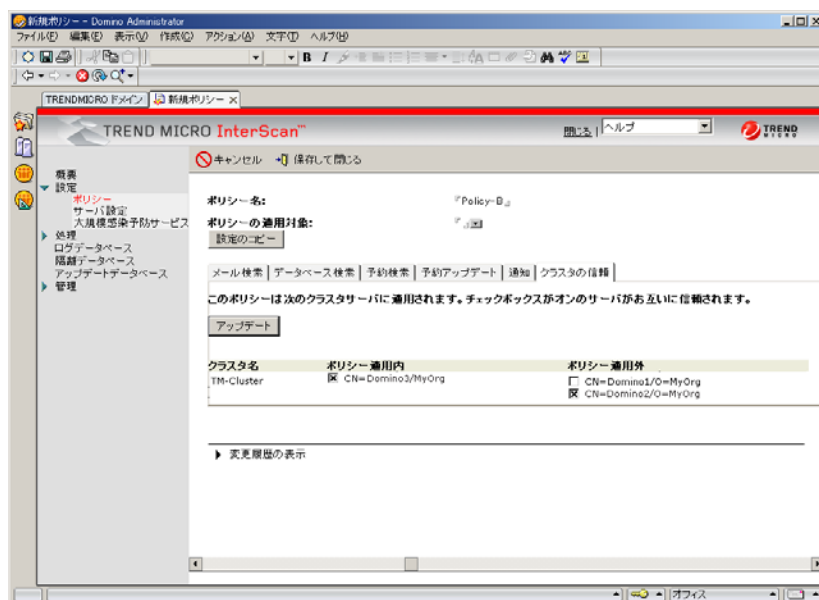


図 5-4. クラスタの信頼の設定例

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、予約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：ルールを作成する際には、smdreal が起動していて、ステータスが「Idle」になっていることを必ず事前に確認してください。

ヒント：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ことがよくあります。ポリシーごとに複雑なルールを 1 つか 2 つ作成するよりは、単純なルールを複数作成することをお勧めします。

メール検索ルールの作成

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 (136 ページを参照) または変更 (132 ページを参照) します。

2. 作業領域で、[メール検索] タブをクリックします。

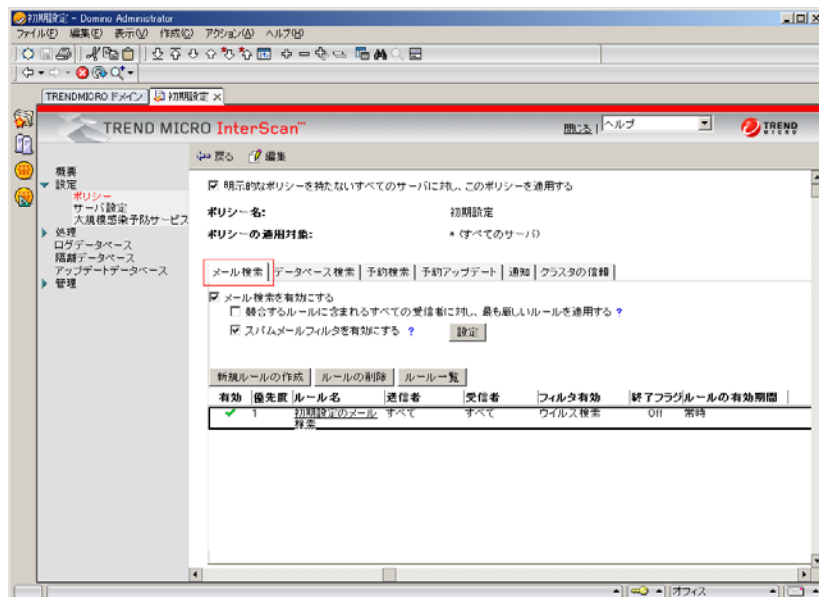


図 5-5. [メール検索] タブでは、メール検索が定義されます。

3. 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適用されるようにするには、[競合するルールを持つすべての受信者に対し、最も厳しいルールを適用する] チェックボックスをオンにします。詳細については、139 ページを参照してください。
4. スイート版を使用している場合は、[スパムメールフィルタを有効にする] チェックボックスをオンにし、[設定] をクリックしてスパムメール対策の設定を指定できます (詳細については、156 ページを参照)。
5. [新規ルールの作成] をクリックします。

6. メールに一致するルールが見つかったとき、その他のルールを処理せずに処理を確定する場合は、[新規メール検索ルール] 画面の [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：複数のルールが適用される状況では、このように終了フラグを有効にすることで、メール検索のパフォーマンスを向上させることができます。

7. [一般] タブでルール名を指定します。
8. 一般の設定を指定します (140 ページを参照)。
9. [検索オプション] タブをクリックし、メッセージを検索してフィルタ処理する方法を設定します。
- ウイルス検索 (159 ページを参照)
 - 検索制限 (162 ページを参照)
 - メッセージフィルタ (163 ページを参照)
 - 添付ファイルフィルタ (169 ページを参照)
 - コンテンツフィルタ (164 ページを参照)
 - スクリプトフィルタ (172 ページを参照)

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。その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。

10. 検索通知を設定します (216 ページを参照)。
11. [転送オプション] を設定します (174 ページを参照)。
12. [検査証明] タブをクリックして、検査証明を設定します (175 ページを参照)。
13. [検索スケジュール] タブをクリックして、検索スケジュールを設定します (176 ページを参照)。
14. [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

[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]
チェックボックスをオンにすることにより、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」には、次の設定があります。

[一般]: [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」には、次の設定があります。

[一般]: [指定する受信者] = user@domain.com

user@domain.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

All of Accounting と user@domain.com を宛先とする、7MB の添付ファイル入りの受信
メッセージが届いた場合、次のような処理が行われます。

- [最も厳しいルールの適用] が有効になっていると、そのメッセージは All of Accounting グループのどのユーザにも受信されません。
- [最も厳しいルールの適用] が無効だと、user@domain.com 以外のすべてのユーザ
が、メッセージと添付ファイルを受信します。

このオプションを無効にした場合、最も厳しい検索ルールはグループ内の特定のユーザーに適用されます。

ヒント： アドレスグループ名を正確で漏れがないように指定することにより、グループ内の個人に適切なポリシーを適用できます。

一般の設定

メール検索ルールで許可する送信者と受信者、および除外する送信者と受信者を設定するには、メール検索の [一般] タブを使用します。

メール検索ルールの一般的な項目を設定するには

1. メール検索文書の [一般] タブをクリックします。
2. [ルール識別子] で、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 (例: 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] グループで、対象となる送信者を選択します。
 - a. ルールで許可する送信者を選択します。
 - 指定した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。

[指定する送信者] を選択した場合、次の設定を行います。

 - Notes のユーザー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 (例: user@domain.com)。

- 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 (例: *@domain)。

b. ルールで除外する送信者を指定します。

- [受信者] グループで、対象となる受信者を選択します。

a. 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。

[指定する受信者] を選択した場合、次の設定を行います。

- 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 (例: user@domain.com)。
- 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 (例: *@domain.com)。

b. 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、このルールの処理時に使用する演算子を選択します (149 ページを参照)。

4. 送信者または受信者、あるいはその両方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] を選択する場合は、必要に応じて [優先度を低く設定]、[指定する時間帯に配信] チェックボックスをオンにします。

注意： 初期設定では、Domino サーバからの優先度の低いメッセージのルーティングは、午前 0 時～午前 6 時の間に行われます。

5. メッセージの送信者に通知を送信するには、[送信者への通知] をクリックします。

- a. 件名を入力します。
- b. メッセージを新たに入力していきます。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。

設定は、[メール検索] タブに表示されます。たとえば、ルール名、優先度、送信者と受信者の許可と除外、予約、終了フラグの各設定、および有効になっている検索オプションなどです。

データベースのリアルタイム検索ルールの作成

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 (136 ページを参照) または変更 (132 ページを参照) 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。

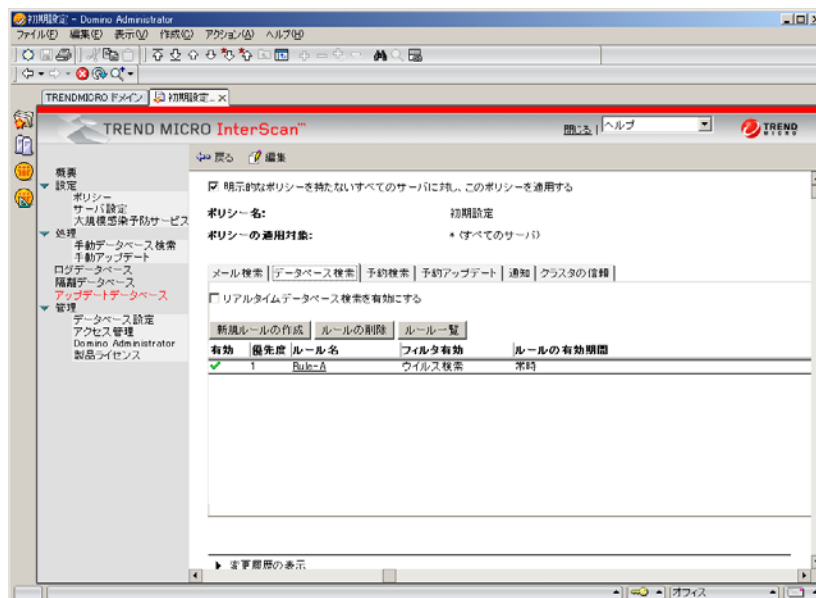


図 5-6. データベース検索ルールを作成

3. [新規ルールの作成] をクリックします。
4. [新規データベース検索ルール] 画面でルール名を指定します。
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。

注意： Linux 版、AIX 版、Solaris 版、または i5/OS および OS/400 版の InterScan を使用している場合は、パスおよびデータベース名が大文字 / 小文字の区別も含めて正しいかどうか確認してください。パスおよびデータベース名が正確でない場合、InterScan の検索対象にすることができません。

6. [検索オプション] タブをクリックして、データベースを検索する方法を設定します。設定項目は次のとおりです。
 - ウイルス検索 (159 ページを参照)
 - 検索制限 (162 ページを参照)
 - スクリプトフィルタ (172 ページを参照)
7. [通知テンプレート] をクリックして、検索通知を設定します (216 ページを参照)。
8. [検索スケジュール] タブをクリックして、検索スケジュールを設定します (176 ページを参照)。
9. [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ときだけでなく、開かれているときには常にリアルタイム検索を実行するように InterScan を設定するには、`notes.ini` ファイルのエントリを次のように設定します。

`SMDEnableOpenEvent=1`

データベースの予約検索ルールを作成

データベースの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 (136 ページを参照) または変更 (132 ページを参照) します。
2. 作業領域で、[予約検索] タブをクリックします。

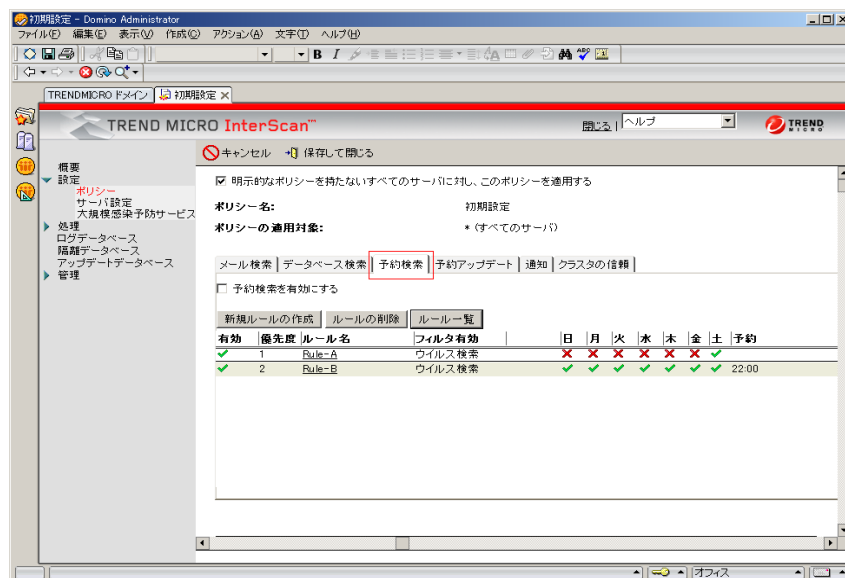


図 5-7. [予約検索] タブ

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] 画面の [一般] タブで一般的な設定を指定します。
 - a. ルール名を指定します。

- b. 検索の 1 日当たりの実行回数、持続時間、および曜日を設定します。
- c. 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節約できます。前回の検索以降に作成または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] という 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。
 - 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、特定のユーザ、ユーザグループのメールデータベースまたはデータベースを検索します。

[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。

注意： Linux 版、AIX 版、Solaris 版、または i5/OS および OS/400 版の InterScan を使用している場合は、パスおよびデータベース名が大文字 / 小文字の区別も含めて正しいかどうか確認してください。パスおよびデータベース名が正確でない場合、InterScan の検索対象にすることができません。

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。

- ウイルス検索 (159 ページを参照)
- 検索制限 (162 ページを参照)
- スクリプトフィルタ (172 ページを参照)

7. 検索通知を設定します (216 ページを参照)。

8. [検索スケジュール] タブをクリックして、検索スケジュールを設定します。

- a. [実行時刻] を設定します。この時刻から予約検索ルールが実行されます。例：06:00 AM、04:00 AM - 05:00 AM

注意： [実行時刻] フィールドを空白にした場合、予約検索は無効になります。

- b. [検索時間の上限] フィールド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. ルールを実行する曜日を入力するか、 をクリックしてリストから選択します。

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。その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。

ルールの整理

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ルールを整理するには、[ルール一覧] 画面を使用します。

閉じる 上へ 下へ ルールの有効化 ルールの無効化						
	有効	優先度	ルール名	送信者	受信者	有効なフィルタ
メール検索		1	初期設定のメール検索	すべて	すべて	ウイルス検索
データベース検索		1	Rule-A			ウイルス検索
予約検索		1	Rule-A			ウイルス検索
		2	Rule-B			ウイルス検索
予約アップデート		1	Update-A			

- 図 5-8. 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。
- 各ルールを有効化または無効化するには、[ルールの有効化] ボタンまたは [ルールの無効化] ボタンを使用します。

次のガイドラインに従ってルールの構成を考慮する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 は優先度 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。[メール検索] のルールでは、[ル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ったら、ルール比較はそれ以上実施されず、指定された処理が実行されます。

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 番めのルールではじ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が節約できます。

- 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、予約アップデートのルールの優先度を変更するには、[ルール一覧] 画面を使用します。[ルール一覧] 画面には、ルールの有効化または無効化を設定するための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、ルールを選択して  をクリックします。
 - ルールの優先度を下げるには、ルールを選択して  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@domain.com, 2@domain.com, 3@domain.com

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

フィルタについて

フィルタは、検索ルールの子セットです。InterScan の検索動作を実際に定義しているのはフィルタです。

フィルタ処理の順序

ルール内の [検索オプション] タブで、フィルタを設定することができます。

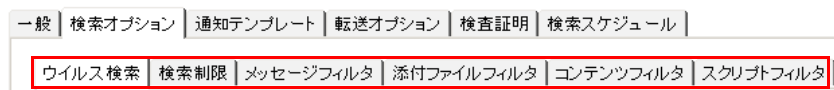


図 5-9. [検索オプション] タブ

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、次の表のタブを使用します (この表の順序でフィルタが適用されます)。

順序	フィルタ	検索処理の適用対象
1	メッセージフィルタ	各種メッセージタイプ
2	添付ファイルフィルタ	不適切な添付ファイル
3a	検索制限	圧縮、暗号化などの処理を施された添付ファイル 注意： [検索制限] の設定を適用するには、ウイルス検索を有効にしておく必要があります。
3b	ウイルス検索	ウイルスなどの不正プログラム
4	コンテンツフィルタ	管理者が定義した明示的なルールに基づく、内容が不適切なメッセージ
5	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あるメッセージ

注意： スпамメールフィルタを設定しておく、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メールフィルタ (156 ページ)。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. 一般的な設定 (140 ページ)
3. [検索オプション] タブで有効になっているフィルタ

スパムメールフィルタ (スイート版のみ)

注意： Windows、Linux、Solaris、および AIX 版向けにはスイート版のみの提供となります。i5/OS および OS/400 プラットフォーム向けにはスタンダード版のみの提供となります。

スパムメール検索エンジンによるスパムメールフィルタ機能を使用すると、次のコンポーネントに基づいてスパムメールをブロックできます。処理の対象となるメールは、Domino サーバのアドレス帳の LocalDomainServers に属していないユーザにより送信されたメールです。コンポーネントは、ルール内の [一般] タブで設定できます。

順序	コンポーネント	提供方法	説明
1	許可する送信者	ユーザ定義	内容に関係なく受け付けるメッセージの送信元のリスト。 その他のメッセージに対しては、事前に設定した処理が実行されます。
2	ブロックする送信者	ユーザ定義	内容に関係なくスパムメールとみなすメッセージの送信元のリスト。 その他のメッセージは、受け付けられません。
3	ルールファイル	トレンドマイクロ	ヒューリスティックファイルと URL 署名ファイルで構成されます。承認する送信者もブロックす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提供するスパムメール判定ルールに基づいてフィルタ処理を行います。

注意： 承認する送信者もブロックする送信者も設定されていない場合、トレンドマイクロのルールファイルが使用されます。

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。次の表に、スパムメール検索エンジンがメッセージをスパムメールとみなすタイミングとその方法を示します。

フィルタレベル	しきい値
高	4.5
中 (初期設定)	5
低	7

各項目の説明は次のとおりです。

- フィルタレベルは、スパムメールをフィルタ処理する際のスパムメール検索エンジンの感度を定義します。
- しきい値は、スパムメールスコアの許容最大値を定義します。

スパムメール検索エンジンは、スパムメールスコアの合計値がしきい値以上の場合、そのメールをスパムメールとして処理します。しきい値未満の場合、次の順番のフィルタ処理に進みます (150 ページの表を参照)。

次に例を挙げます。

```

Lotus Domino Server: E3/tmase
07/19/2004 12:21:15 AM SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:16 AM SMTP Server: Message 0059D67D received
07/19/2004 12:21:16 AM SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:17 AM 15.200: Spam triggered
07/19/2004 12:21:17 AM Router: Message 0059D67D delivered to user1/tmase
07/19/2004 12:21:24 AM SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:24 AM SMTP Server: Message 0059D9F2 received
07/19/2004 12:21:24 AM SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:26 AM 15.200: Spam triggered
07/19/2004 12:21:26 AM Router: Message 0059D9F2 delivered to user1/tmase
07/19/2004 12:21:31 AM SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:31 AM SMTP Server: Message 0059DC79 received
07/19/2004 12:21:31 AM SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:32 AM 3.726: passed(not Spam)
07/19/2004 12:21:32 AM Router: Message 0059DC79 delivered to user1/tmase
07/19/2004 12:21:33 AM SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:33 AM SMTP Server: Message 0059DD56 received
07/19/2004 12:21:33 AM SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:34 AM 24.300: Spam triggered
07/19/2004 12:21:34 AM Router: Message 0059DD56 delivered to user1/tmase
>

```

図 5-10. スパムメールスコアの例

この例では、フィルタレベルは「中」に設定されています。線で囲まれた項目が、スパムメールスコアです。最初のスパムメールスコアは、15.20 で、これはしきい値「5」を超えています。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はスパムメールとみなされます。一方、2 つめのスパムメールスコアは、3.726 で、これはしきい値に達していません。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メールとみ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、156 ページを参照してください。

コンテンツフィルタ

コンテンツフィルタでは、管理者によって定義されたルールに基づいてメッセージの内容を確認し、条件に一致した場合の処理を定義します。

企業秘密の漏えい、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、素早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
- メール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が現れる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、大量メール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、一致とはみなされません。

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、167 ページを参照してください。

注意： Windows、AIX、または i5/OS および OS/400 プラットフォームにおいて、2 バイト文字セットを使用している場合は、ワイルドカード .WILD. は無効になります。

スパムメールフィルタの設定

スパムメールをスパムメール検索エンジンによって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。スパムメールフィルタの概要については、152 ページを参照してください。[スパムメールフィルタの設定] 画面には、不適切なメッセージのフィルタ処理に適用するヒューリスティック検出レベルや、[許可する送信者] および [ブロックする送信者] のリストを定義するオプションがあります。

注意： [スパムメールフィルタ] および [コンテンツフィルタ] 機能は、InterScan スイート版でのみ利用可能です。詳細については、85 ページの「アクティベーションコード」を参照してください。また、InterScan のスパムメールフィルタはメール検索のみに適用されます。

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] チェックボックスをオンにし、[設定] をクリックします。[スパムメールフィルタの設定] ウィンドウが表示されます。

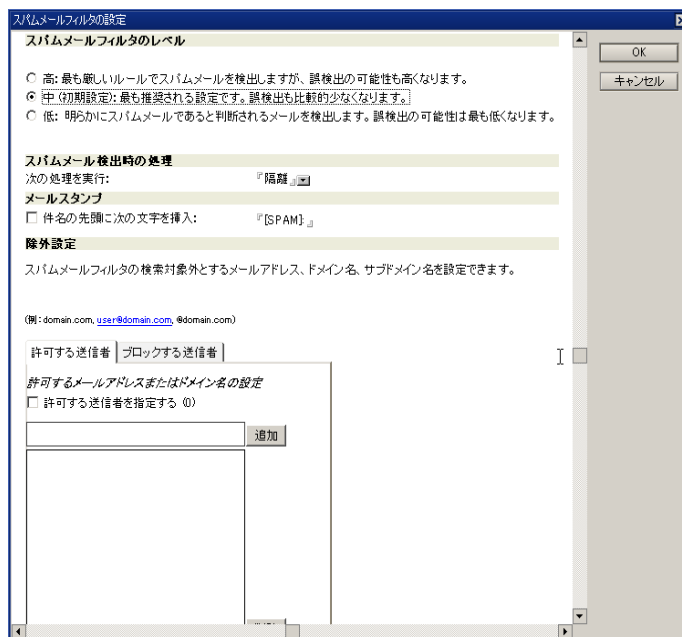


図 5-11. スパムメールフィルタ設定画面

2. [スパムメールフィルタのレベル] を設定します。

- 高 — 最も厳しいスパムメール検出レベル

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がスパムメッセージとしてフィルタ処理されてしまうことを指します。

- 中 — 初期設定

ある程度高いレベルのスパムメール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 — 最も寛容なスパムメール検出レベル

明らかにスパムメール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. [スパムメール検出時の処理] を設定します。スパムメールに対する処理として [放置]、[隔離]、[ブロック] のいずれかを選択します。

4. [メールスタンプ] について設定します。[件名の先頭に次の文字を挿入] チェックボックスをオンにすることにより、スタンプとして入力した文字をスパムメールの件名に追加できます。

5. [許可する送信者] と [ブロックする送信者] を有効化して、それぞれのリストに含める送信者を指定すると、誤検出の可能性を最小化できます。

- [許可する送信者] タブをクリックし、[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。削除するには、リストからメールアドレスまたはドメインを選択した後、[削除] をクリックします。

- [ブロックする送信者] タブをクリックし、[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。

拒否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。削除するには、メールアドレスまたはドメイン選択した後、[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提供する判定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、152 ページの「スパムメールフィルタ (スイート版のみ)」を参照してください。

6. 次のいずれかを実行してスパムメールフィルタの設定を保存します。

- Notes インタフェースの場合：画面右上の [OK] をクリックし、[保存して閉じる] をクリックします。

— または —

- Web インタフェースの場合: [保存] をクリックします。

検索オプションの設定

検索動作を設定するには、ルール内の [検索オプション] タブを使用します。

ウイルス検索の設定

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、[ウイルス検索] タブを使用します。

ウイルス検索オプションを設定するには

1. [検索オプション] で、[ウイルス検索] タブをクリックします。
 2. [ウイルス検索] タブで、ウイルス検索オプションを設定します。
 - a. 検索するファイルを指定します。次のオプションから選択します。
 - すべて(推奨) — 除外するファイルで指定したもの以外のすべてのファイルを検索します。
- 検索対象からの除外を実際のファイルタイプに基づいて指定するには、[検索から除外する実際のファイルタイプ] フィールド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ます。また、ファイル名または拡張子に基づいて除外を指定することもできます。その場合は、[検索から除外するファイル名 / 拡張子] フィールド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ます。

- 指定するファイル — 選択されたファイル名または拡張子に基づいて検索します。

ファイル拡張子名の初期設定リストが表示されます。検索対象のファイル名または拡張子を新たに指定するには、[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ます。

b. 選択できる詳細オプションは、次のとおりです。

- 圧縮ファイル — 圧縮ファイルを検索します。

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 で検索できる圧縮ファイルタイプのリストについては、製品 Q&A を参照してください。

- 埋め込みオブジェクト — OLE を検索します。

InterScan では、MIME、UUencode、または BINHEX の形式でエンコードされたバイナリ添付ファイルを検索できます。

- Microsoft Office 文書内のマクロ — Microsoft Office ファイル (例: *.doc、*.xls) にマクロが含まれていないか検索します。

マクロ検出時の処理を選択します。

c. 感染ファイルに対する [処理] を設定します。

- **トレンドマイクロの推奨処理** — 不正プログラムのタイプを識別し、トレンドマイクロのパターンファイルに基づいて、識別されたタイプがコンピュータシステムまたは環境に感染する方法に対応した推奨処理を自動的に提示します。[隔離]は、ウイルス駆除不能な項目に対する初期設定の処理です。

[トレンドマイクロの推奨処理] を選択した場合は、ウイルス駆除不能な Microsoft Office ファイルに対する処理も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ことがあります。このようなファイルは検出時に駆除不能とみなされます。[駆除不能なウイルスへの処理] で選択した処理は、Microsoft Office ファイルにのみ適用されます。他のすべてのファイルタイプに対しては、パターンファイルに定義されている処理が適用されます。

- **指定する処理** — 不正プログラムのタイプに応じて InterScan が取る処理を選択します。

注意： 圧縮ファイルのウイルス処理を無効にしている場合、不正プログラムを含む圧縮ファイル全体に対して、検出された不正プログラムに指定された処理が実行されます。圧縮ファイルの駆除処理が有効になっている場合は、個別の不正プログラムに対して処理が実行されます。

[その他の不正プログラムへの処理] が設定されていない場合、[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] の設定が適用されます。[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、脅威を有効にして、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] を有効にして [駆除] を選択した場合、検出された大量メール配信ウイルスが自動的に削除されます。

- d. [通知] を設定します。不正プログラム検出時、駆除不能時、または感染ファイルに対する処理の実行時に送信する通知先、通知内容を設定します。
- e. [メールスタンプ] を設定します。

3. [保存して閉じる] をクリックします。

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. 各オプションを設定します。
 - 解凍ファイルサイズが次の上限を超えた場合 — 解凍時のファイルサイズの上限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] の値を選択して、検索対象とする圧縮レベルの上限を設定します。[圧縮レベルの上限] を「3」に設定した場合、圧縮レベル数が 2 (圧縮後、再圧縮) 以上の圧縮ファイルが検索されます。

注意： 初期設定では、InterScan で検索できる圧縮レベルの上限値は 20 です。

- パスワードで保護された圧縮ファイル — パスワードで保護された圧縮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を自動的に検索できるようにします。
3. [通知] を設定します。ファイルが検索制限の設定に一致した場合の通知先、通知内容を設定します。
 4. [メールスタンプ] を設定します。
 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

暗号化されたメッセージまたは分割されたメッセージに対する処理を定義するには、[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] 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出時の処理を定義します。
 - メッセージサイズが次の条件に一致する場合 — 検索を省略して、指定制限値の条件に一致するメッセージに対する指定処理を自動的に実行できるようにします。
サイズ制限値をバイト (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ルール — 検索を省略して、同じドメインにいるユーザー間で送受信した暗号化メッセージに対する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 — 検索を省略して、暗号化された受信メッセージに対する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 — 検索を省略して、暗号化された送信メッセージに対する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 — 検索を省略して、分割されたメッセージに対する指定処理を自動的に実行できるようにします。
4. [通知] を設定します。ファイルがメッセージフィルタに一致した場合の通知先、通知内容を設定します。
5. [メールスタンプ] を設定します (このメールスタンプは暗号化メッセージに対してのみ有効です)。
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設定

コンテンツフィルタでは、管理者によって定義されたルールに基づいてメッセージの内容を確認し、条件に一致した場合の処理を定義します。

企業秘密の漏えい、侮辱的または不適切な言葉遣い、競合他社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： AIX 版、i5/OS および OS/400 版では、Microsoft Office 文書の検索はサポートしていません。

[コンテンツフィルタ] タブでは、一般的なルールや詳細なルールを定義できます。詳細については、154 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. [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。
3. 新規コンテンツフィルタを作成する (164 ページを参照) か、既存のフィルタをコンテンツフィルタリストに追加します (167 ページを参照)。
4.  をクリックして、コンテンツフィルタ設定に一致したメールの検出時の処理を指定します。
5. [通知] を設定します。メールがコンテンツフィルタ設定に一致した場合の通知先、通知内容を設定します。
フィルタに関する説明を通知に挿入することで、追加の指示や説明を組み込みます。
例：詳細については、Domino 管理者に問い合わせてください。
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] タブの [新規コンテンツフィルタの作成] ボタンをクリックします。
2. [新規コンテンツフィルタ] 画面でコンテンツフィルタの名前を入力します。
3. [フィルタの対象] で、フィルタ処理して、指定したキーワードと比較するメッセージの部分 (例: [件名]、[From]、[To]、[メール本文]) を選択します。キーワードの詳細については、155 ページの「キーワード」を参照してください。



図 5-12. コンテンツフィルタの新規作成

比較する部分として選択した対象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を検出するように設定する場合は、[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] チェックボックスをオンにします。

4. コンテンツのフィルタ処理に使用するキーワードを作成するか (167 ページを参照)、または追加します (168 ページを参照)。
 - メッセージ内のキーワード数が指定値を超えた場合に不適切な内容のメールに対して実行する処理を指定するには、[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らコンテンツフィルタに一致] フィールドに整数を入力します。
 - 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不適切な内容のメールに対して実行する処理を指定するには、[.OCCUR. の頻度 (回数)] フィールドに整数を入力します。
 - 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不適切な内容のメールに対して実行する処理を指定するには、[.NEAR. の近接値 (語数)] フィールドに整数を入力します。

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。

5. [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

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] タブを使用します。

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選択し、[OK] をクリックします。
2. [コンテンツフィルタの削除] ボタンをクリックします。

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] ボタンをクリックします。

コンテンツフィルタが削除され、リアルタイム検索タスクに変更が通知されます。

既存フィルタを利用したコンテンツフィルタの追加

メッセージのどの部分を検索するかを定義した「ベース」コンテンツフィルタをいくつか作成しておいて、これをコンテンツフィルタの要素として繰り返し利用できます。たとえば、件名検索用、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。

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] の作業領域で [既存するコンテンツフィルタの追加] ボタンをクリックします。
2. 追加する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。

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よくあります。設定するキーワードは、コンテンツフィルタ当たり 1、2 語にすることをお勧めします。

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当たり 1、2 語にすることをお勧めします。

新規キーワードを作成するには

1. [コンテンツフィルタ] タブで対象のコンテンツフィルタをダブルクリックして開き、[新規キーワードの作成] ボタンをクリックします。
2. [新規キーワード] 画面で、フィルタ処理するキーワード (語句またはフレーズ) 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、画面下部にあるヘルプセクションを参照してください。
3. [大文字 / 小文字の区別] を有効または無効に設定します。
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。

既存キーワードを利用したキーワードの追加

既存キーワードをテンプレートとして再利用して、キーワードを追加できます。

キーワードを追加するには

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] ウィンドウで、使用するキーワードをクリックします。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: メール検索ルールに追加するキーワードが多すぎると、ルールが予想以上に複雑になることがよくあります。設定するキーワードは、メール検索ルール当たり 1、2 個にすることをお勧めします。

添付ファイルフィルタの設定

メール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。

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	バッチ処理ファイル
.BIN	バイナリファイル
.CLA	Java クラスファイル (通常は *.CLASS ですが、*.CLA という短縮形もあります)
.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	Microsoft 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)

表 5-1. ブロックが推奨されるファイルの拡張子

拡張子	説明
.HTM .HTML	ハイパーテキストマークアップ言語
.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

表 5-1. ブロックが推奨されるファイルの拡張子

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] で、[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] チェックボックスをオンにします。
 3. 添付ファイルのフィルタ処理条件を設定します。
 - ファイルサイズで添付ファイルをフィルタ処理するには、[サイズ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。

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。サイズの制限値をバイト (B)、キロバイト (KB)、またはメガバイト (MB) 単位で設定します。
 - ファイルタイプで添付ファイルをフィルタ処理するには、[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、添付ファイルとして使用されると考えられる 200 種類を超えるファイル形式のコンテンツを開き、整理して、検索できます。Notes のデータベース形式も同様に処理できます。
- 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 [指定を除くすべて] を選択すると、次の操作が可能になります。
- InterScan のファイルタイプデータベースを編集できます。
 - 実際のファイルタイプ、実際のファイルタイプグループ、または拡張子名に基づいて、ファイルタイプを入力するか、または  をクリックして選択します。

注意： Domino では、添付ファイルのファイル名がメール本文中に埋め込まれていることがあります。そのため、ファイル名に含まれる指定単語を見つけるために、本文が検索されることがあります。

- b. [処理]フィールドに[放置]、[隔離]、[削除]、[ブロック]、または [承認のためにメールを転送] から、フィルタ処理を選択します。
 - c. 圧縮ファイルを検索する場合は、[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] チェックボックスをオンにします。サーバーのパフォーマンスを最適化するため、初期設定ではこのオプションは無効になっています。
4. フィルタ処理から除外する添付ファイル名を、[許可された添付ファイル] フィールドで指定します。複数のファイル名または拡張子を指定するには、ワイルドカード文字 * または ? を使用します。エントリ間は、セミコロン (;) で区切ります。
- [許可された添付ファイル] フィールドで指定されたファイル名または拡張子は、添付ファイルのフィルタ処理条件より優先されます。
5. [通知] を設定します。添付ファイルが添付ファイルフィルタに一致した場合の通知先、通知内容を設定します。
6. [メールスタンプ] を設定します。
7. [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

Lotus 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] で、[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. フィルタ処理する格納フォームと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、次のような Lotus 式言語による有効な Lotus Notes 関数を指定できます。例：prompt
 - [@ コマンド文字列] には、次のような Lotus 式言語による有効な Lotus Notes のコマンドを指定できます。例：[Execute]、[FileDatabaseDelete]
 - [スクリプト文字列] には、OS で有効な次のような LotusScript コマンドを指定できます。例：shell、getobject、kill、rmdir、activate
 - [@URLOPEN で呼び出される URL] では、次のような Lotus 式言語による有効な URLOPEN コマンドを指定できます。例：offensivesite.com、www.offensivesite.com
4.  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、リッチテキストのホットスポットに対するフィルタ処理を設定します。

注意： ホットスポットに対する [自動駆除] 処理により、悪意のある文字列を含んでいるコードセグメントが削除されます。文書全体が隔離されるため、誤検出された場合は、文書を復元可能です。[ホットスポットをポップアップメッセージに置換する] チェックボックスをオンにすると、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。

格納フォームに対する [自動駆除] 処理は、現時点では使用できません。格納フォームのホットスポットおよびイベントに対しては、[削除:格納フォームを削除] 処理を選択することをお勧めします。

5. [通知] を設定します。ファイルが検索制限の設定に一致したときの通知先、通知内容を設定します。
6. [メールスタンプ] を設定します。
7. [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。メールを配信してもよいかどうかは、指名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.  をクリックして、[検索済みメールを次のユーザに転送] フィールドに承認者のメールアドレスを指定します。

注意： アカウントに管理者権限がある場合でも、InterScan データベースへのアクセス権とロールを持たない場合には、InterScan の機能にアクセスできません。

指定したアカウントが InterScan データベースへの適切なアクセス権を持ってい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権については、118 ページを参照してください。

ヒント： 指定された承認者が不在でないことを確認してください。指定された承認者が不在になる場合は、別の承認者のメールアドレスも転送先に設定しておくことをお勧めします。

承認者のアドレスは少なくとも 2 つ指定することをお勧めします。1 人の承認者が不在の場合でも、もう 1 人の承認者が処理することができ、メールの紛失や処理もれを防ぐことができます。

3. [通知] を設定します。承認者によってメールが承認または拒否した場合の通知件名を入力します。
4. [保存して閉じる] をクリックします。

検査証明の挿入

メール検索を行ったことに対する通知として検査証明を挿入するには、[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、検査証明の名前が同じ場合、検査証明が挿入されるのは 1 度だけです。

検査証明を挿入するには

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] チェックボックスをオンにします。
3. 検査証明の詳細を設定します。

注意： 本文では、[メッセージ本文の先頭] を選択している場合に、フィルタ通知がメッセージに挿入される場合、検査証明はフィルタ通知の後に挿入されます。また、件名では、元のメッセージ件名の後に検査証明が挿入されます。

4. 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. 件名とメッセージ本文の検査証明の内容を入力します。
6. [保存して閉じる] をクリックします。

検索スケジュールの設定

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。

検索スケジュールを設定するには

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. 期間を設定します。
 - 常時 — ルールが常時適用されます。
 - 指定 — 指定した期間にルールが有効または無効であることをオプションから選択します。指定期間の詳細 (曜日、期間、タイムゾーン) を設定します。
3. [保存して閉じる] をクリックします。

手動データベース検索の実行

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保存されている Notes データベースに対して、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 種類があります。

- Domino サーバコンソールを使用する方法
- 設定データベースを使用する方法

手動検索の実行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 サーバコンソールからの手動検索の実行

Notes データベースは、Domino サーバコンソールまたは InterScan インタフェースで手動検索できます。

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。

Domino サーバコンソールから手動検索を実行するには

次のコマンドを入力します。

```
load SMDdbs -manual {directory name and  
database.nsf}
```

ここで、{directory name and database.nsf} は、検索するディレクトリまたはデータベース名です。

指定されたデータベースまたは notes.ini の Directory セクションにある関連するディレクトリが検索されます。

ヒント：複数のデータベース名は、セミコロン (;) で区切ります。例：

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

設定データベースからの手動検索の実行

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。

設定データベースから手動検索を実行するには

1. 設定データベースを開きます。
2. メインメニューで、[処理]→[手動データベース検索] の順に選択します。
3. 作業領域で、[編集] をクリックします。

4. [一般] タブをクリックして、[増分検索を有効にする] チェックボックスをオンにし、検索時間を指定します。

注意： 検索の最長実行時間を [検索時間] に分単位で入力します。「0」と入力した場合、すべて完了するまで検索を実行します。

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の下位にあるフォルダも含めるには、[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。

注意： Linux 版、AIX 版、Solaris 版、または i5/OS および OS/400 版の InterScan を使用している場合は、パスおよびデータベース名が大文字 / 小文字の区別も含めて正しいかどうか確認してください。パスおよびデータベース名が正確でない場合、InterScan の検索対象にすることができません。

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。

- ウイルス検索 (159 ページを参照)
- 検索制限 (162 ページを参照)
- スクリプトフィルタ (172 ページを参照)

7. [通知テンプレート] タブをクリックして、検索通知を設定します。

8. [ScanNow] をクリックします。

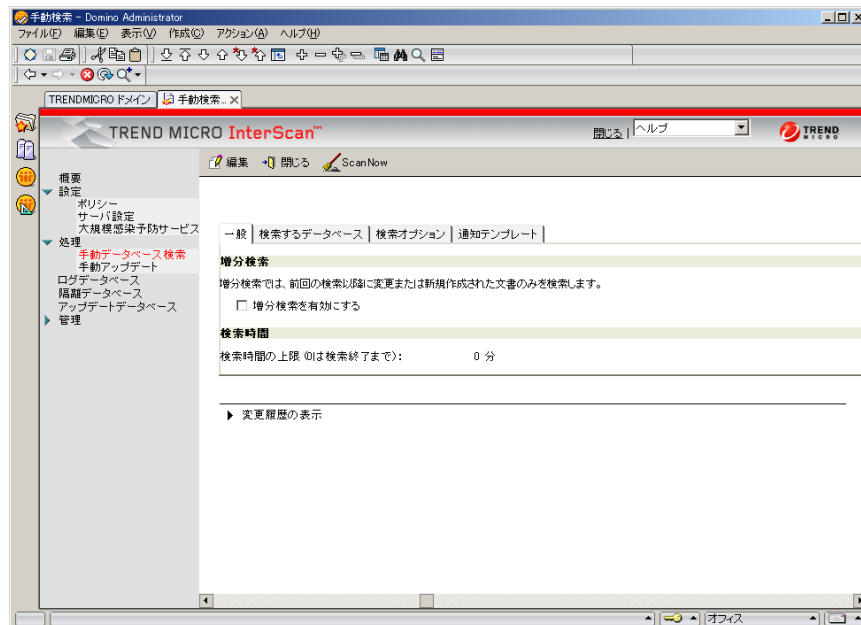


図 5-13. 手動データベース検索を実行する Notes ID は、サーバコンソールコマンドを発行することのできる適切な権限が必要です。

9. [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。

手動検索の停止

手動データベース検索を、自動終了する前に中止するには、Domino サーバコンソールで次のコマンドを実行して、検索タスクを正常に終了させます。

```
tell SMDbbs quit
```

現在の文書の検索が完了すると、検索が停止します。

管理の設定

Trend Micro InterScan for Domino 3.0 (以下、InterScan) では、[概要]、[サーバ設定] および [管理] の新しいメニューが提供されます。これらのオプションを使用して、InterScan サーバ情報を表示したり、InterScan データベースの管理性やパフォーマンスを最適化することができます。

この章で説明する項目は次のとおりです。

- 182 ページの「すべてのサーバの概要の表示」
- 183 ページの「[サーバ設定] 画面」
- 192 ページの「[管理] 画面」

すべてのサーバの概要の表示

設定データベースの [概要] 画面には、検索タスクのステータスの概要や、InterScan と OS の情報が表示されます。

すべてのサーバの概要を表示するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで [概要] をクリックします。

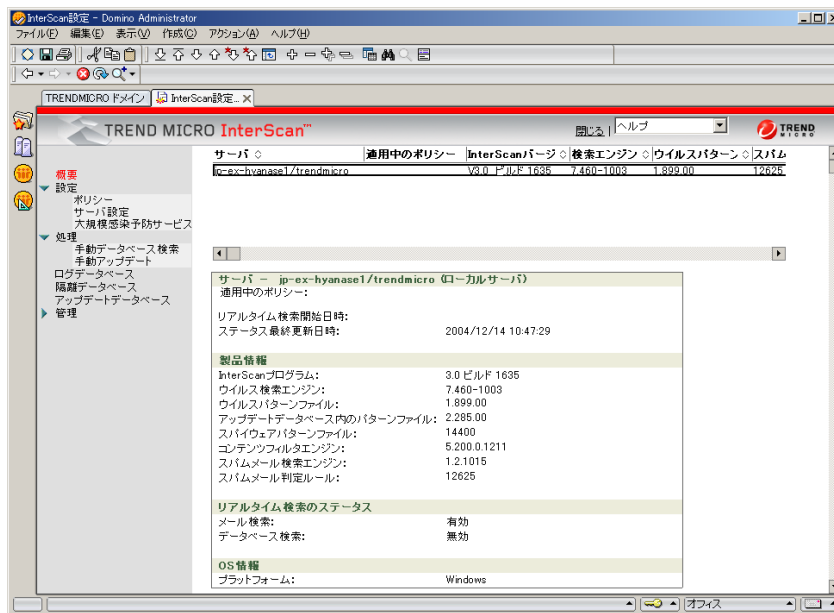


図 6-1. すべてのサーバのステータス概要

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。
 - 表示されている情報を更新するには、<F9> キーを押します。

ヒント: Trend Micro Control Manager をインストールしている場合は、管理コンソールから [製品ステータス] タブにアクセスし、InterScan のステータスを確認することもできます。

[サーバ設定] 画面

設定データベースの [サーバ設定] 画面を使用し、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。

- 検索に一時的に使用される作業ディレクトリ
- 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
- InterScan イベントの種類と、それらが Domino サーバコンソールを通じて表示される条件
- InterScan タスクが異常終了した場合の管理者への通知
- InterScan が検査証明に使用する文字セットを見つけ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、警告用画像、メッセージルーティングなど、その他の設定

サーバ設定の作成

サーバ設定を作成するには、設定データベースの [サーバ設定] 画面を使用します。

ヒント：サーバ設定は、サーバまたはサーバグループごとに作成してください。

サーバ設定を作成するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[設定]→[サーバ設定] の順に選択します。
3. 作業領域で、[サーバ設定の作成] をクリックします。
4. サーバ設定を適用する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 (185 ページを参照)。
6. 検索に使用するメモリサイズを設定します (186 ページを参照)。
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 (187 ページを参照)。
8. 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 (188 ページを参照)。
9. サーバタスクモニタを有効にします (188 ページを参照)。
10. 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 (189 ページを参照)。
11. その他の設定を行います (189 ページを参照)。
12. [保存して閉じる] をクリックします。

サーバ設定の変更

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

サーバ設定を変更するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[設定]→[サーバ設定] の順に選択します。
3. 作業領域で、サーバ設定ルール of 文書を開き、ダブルクリックするか、または [編集] ボタンをクリックします。
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。

サーバ設定の設定

サーバ設定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]、[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。

検索に使用する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. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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. 検索の種類ごとに、Domino データディレクトリを基準にした相対パスで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。

- 環境内にあるほとんどのメッセージや文書を処理できるメモリ容量を割り当てます。
添付ファイルの 90% が 2MB 未満である環境の場合、メモリベースの個々の検索タスクに割り当てるメモリ容量は 2MB で済みます。最適な結果を得るためには、メモリサイズを決定する際に平均メッセージサイズを使用しないでください。
- 添付ファイルのサイズに上限を設けている組織の場合は、その値を使用してください。
- 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 サーバ上のすべての InterScan タスクで使用されるメモリ容量の合計を考慮します。
たとえば、5MB のメモリを割り当てた SMDreal タスクを 3 つ実行している場合、InterScan は 15MB のメモリを使用します。予約検索 (SMDdbs) の実行時には、そこで使用されるメモリも合計容量に加える必要があります。
- Domino サーバ上のメモリのサイズと使用率を確認します。メモリの使用率の確認方法については、Domino のマニュアル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ほうが大きくなります。

大半の組織では、InterScan タスクごとに 5MB という初期設定値が適しています。

検索メモリサイズを設定するには

1. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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

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するには、[プロキシ設定] タブを使用します。

注意： 予約アップデートまたは手動アップデート文書でコンポーネントをダウンロードするときに、初期設定以外のプロキシサーバを指定できます。詳細については、208 ページの「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を設定」を参照してください。

プロキシサーバを設定するには

1. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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、およびポート番号を指定します。
6. 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。
7. [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

InterScan のタスクが正常に終了しなかった場合に 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. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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. 通知を受け取る管理者を入力するか、 をクリックして設定します。
5. 通知メッセージの件名と本文を入力します。
6. [保存して閉じる] をクリックします。

サーバイベントのモニタ

次のイベントを監視して Domino サーバコンソールに表示するには、[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. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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. Domino サーバコンソールにログを表示させたいイベントに対応する [Domino サーバコンソール] チェックボックスをオンにします。
4. [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 が検査証明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。

検査証明を挿入する方法については、175 ページ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. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) 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、警告用画像、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. サーバ設定を作成 (184 ページを参照) または変更 (184 ページを参照) します。
2. 作業領域で、[その他] タブをクリックします。

3. メールおよびデータベース検索に使用するスレッドの数を表す整数を入力します。

ヒント：スレッドの数には、1 ～ 20 までの値を指定してください。リアルタイムのメール検索スレッドとリアルタイムのデータベース検索スレッドの合計は、20 以下とする必要があります。

検索ごとのスレッド数として、「5」をお勧めします。

4. 入力するか  をクリックして、ウイルス対策済みの SMTP サーバおよび Domino サーバを選択します。

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。

5. ウイルスなどの不正プログラムが検出された場合や、[添付ファイルフィルタ] タブの設定 (169 ページを参照) の処理によって添付ファイルがブロックされた場合、通知に挿入する警告用画像 (たとえば、*.gif、*.jpg、*.bmp) を Domino データディレクトリに属する smd フォルダに保存されている画像から指定します。

Domino データディレクトリの smd フォルダに保存されている画像を指定します。

6. [警告用画像] で、[既存のアイコンの後ろに警告用画像を挿入] または [添付ファイルの中身を空白で置き換える] を選択します。

注意：InterScan では、Notes メールから元のファイルのアイコンを削除することはできません。[添付ファイルの中身を空白で置き換える] を選択した場合、InterScan は空白からなる 2 バイトのファイルで添付ファイルを置換します。

7. InterScan リアルタイム検索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] チェックボックスをオンにします。

ヒント： この設定を有効にすることをお勧めします。この項目の設定にあたっては、次の警告と注意を参照してください。

警告： 初期設定では、このオプションは選択されています。何らかの理由で InterScan が停止した場合や、メール検索 (SMDreal) タスクが意図せずアンロードされた場合、Domino サーバではメッセージの処理と配信を停止します。そのため、検索されなかったメッセージには、大規模感染につながるウイルスなどの不正プログラムが含まれる可能性があります。

注意： Linux 版、Solaris 版、AIX 版、i5/OS 版、または OS/400 版の InterScan を使用している場合、サーバのハードウェア仕様によっては、SMDreal タスクのロードに時間がかかる場合があります。InterScan は最初にスパムメール検索エンジンをロードしてから他のタスクをロードします。[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] オプションが選択されずに、SMDreal がまだロードされていない期間、Domino は検索されていないメールを配信します。そのため、この期間にウイルスが広がる可能性があります。

8. [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。例：compact; fixup; updall; update

ヒント： 検索処理の速度向上のために、このオプションを有効にすることをお勧めします。
この機能は Windows 以外のプラットフォームで有効です。

9. [保存して閉じる] をクリックします。

[管理] 画面

ライセンスプロファイルの作成や新しいアクセス制御リストの適用など、InterScan データベースのデータベースプロパティを定義するには、設定データベースの [管理] 画面を使用します。

データベース設定

[管理]→[データベース設定] オプションでは、データベースプロパティに対するショートカットを提供します。

設定データベースを使用して、次のプロパティを InterScan データベースに適用します。

- **[データベースを開く] ダイアログへの表示**

Notes の [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**

安全な通信を確保するために SSL (Secure Socket Layer) バージョン 2.0 以降がサポートされています。[データベース] ダイアログを使用する代わりに、SSL で Web を介して InterScan データベースにアクセスするためにこのオプションを有効にするには、設定データベースを使用します。

- **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。

各 InterScan データベースに Notes データベースプロパティを適用するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューから、[管理]→[データベース設定] の順に選択します。
3. 作業領域で、Domino サーバ名を入力するか  をクリックして選択します。
4. 各 InterScan データベースのプロパティに対する処理を、[有効]、[無効]、または [変更なし] から選択します。
5. [設定の適用] をクリックします。

注意： 設定データベースを完全に閉じるまでは、設定は反映されません。

Domino Administrator からのタスクの表示

Domino Administrator から InterScan タスクを管理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. 設定データベースを開きます (120 ページを参照)。
2. メインメニューから、[管理]→[Domino Administrator] の順に選択します。
3. 作業領域で、[domadmin.nsf にコピー] をクリックします。

Domino 6 Web Administrator ページへの統合

InterScan を Domino 6 Web Administrator ページに統合するには、設定データベースを使用します。

InterScan を Domino 6 Web Administrator ページに統合するには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューから、[管理]→[Domino Administrator] の順に選択します。
3. 作業領域で、[webadmin.nsf にコピー] をクリックします。

アクセス制御リスト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. 設定データベースを開きます (120 ページを参照)。
2. メインメニューから、[管理]→[アクセス管理] の順に選択します。
3. 作業領域で、[新規エントリの作成] をクリックします。
4. アクセス制御リストに加えたい Notes ID を [アクセス制御リストのエントリ] に入力するか  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] をクリックします。
9. [アクセス制御リストへの適用] をクリックします (文書を保存しただけでは、設定は適用されません)。

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 のアクティベーションを実行するには、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. 設定データベースを開きます (120 ページを参照)。
2. [管理]→[製品ライセンス] の順に選択します。
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「アクティベーションコード」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

ライセンスプロファイルを作成して、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。詳細については、87 ページを参照してください。

ライセンスプロファイルを削除するには

1. 設定データベースを開きます (120 ページを参照)。
2. [管理]→[製品ライセンス] の順に選択します。
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。

プロファイルの削除を確認するメッセージが表示されます。[OK] をクリックして、[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てしまった場合は、削除し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することで復元できます。

アップデート

Trend Micro InterScan for Domino 3.0 (以下、InterScan) 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。

この章で説明する項目は次のとおりです。

- 198 ページの「ウイルス対策 / コンテンツセキュリティコンポーネントの概要」
- 199 ページの「アップデートの実行」
- 204 ページの「アップデートの設定」

ウイルス対策 / コンテンツセキュリティコンポーネントの概要

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を、推奨アップデート頻度の高い順に次に示します。

- ウイルスパターンファイル — 悪意のあるファイルによる感染を検出して、処理します。

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。新しいウイルスは日々作成されているため、パターンファイルは頻繁にアップデートされます。

- スパイウェアパターンファイル — 個人情報などを密かに収集する隠しプログラムを検出します。
- スпамメール判定ルール — スпамメール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、スパムメールを検出します。
- 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。

32 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、データ内のウイルスの有無をチェックします。さらに、トレンドマイクロの検索エンジンは、多数の高度なアルゴリズムを活用して、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 攻撃などをすばやく識別します。

検索エンジンには、古いウイルスパターンファイルの自動消去ルーチンが組み込まれており、ディスクスペースの管理に役立ちます。また、増分パターンファイルアップデート機能も備えており、これは帯域幅の管理に役立ちます。

- スпамメール検索エンジン — 一方的に送られてくる広告メールまたは大量のメールを検出します。

- InterScan プログラム — 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ユーザだけです。詳細については、85 ページの「InterScan のアクティベーション」を参照してください。

アップデートの実行

InterScan のコンポーネントは、必要に応じて手動で、またはスケジュールを指定して自動でアップデートできます。

- 手動
- 自動

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] 画面を使用します。

コンポーネントを手動でアップデートするには

1. 設定データベースを開きます (120 ページを参照)。
2. メインメニューで、[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. アップデートするコンポーネントを選択します (複数選択可)。
5. ダウンロード元を設定します。

6. 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を設定します。
7. アップデート通知を定義します。
8. [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。
9. [アップデート] をクリックします。

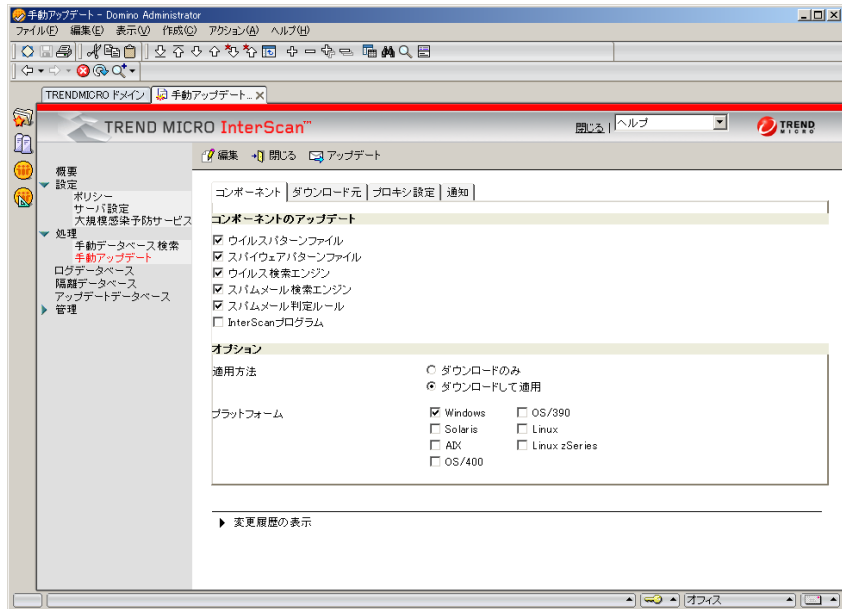


図 7-1. アップデートの設定

予約アップデートルールを使用した自動アップデート

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 (130 ページを参照) または変更 (132 ページを参照) します。

2. 作業領域で、[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] を選択します。
4. 自動配信するコンポーネントを設定します (202 ページを参照)。
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の [一般] タブで、次の項目を指定します。
 - 予約アップデートのルール名を指定します。
 - [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 (複数選択可)。
7. ダウンロードするコンポーネントを選択します。

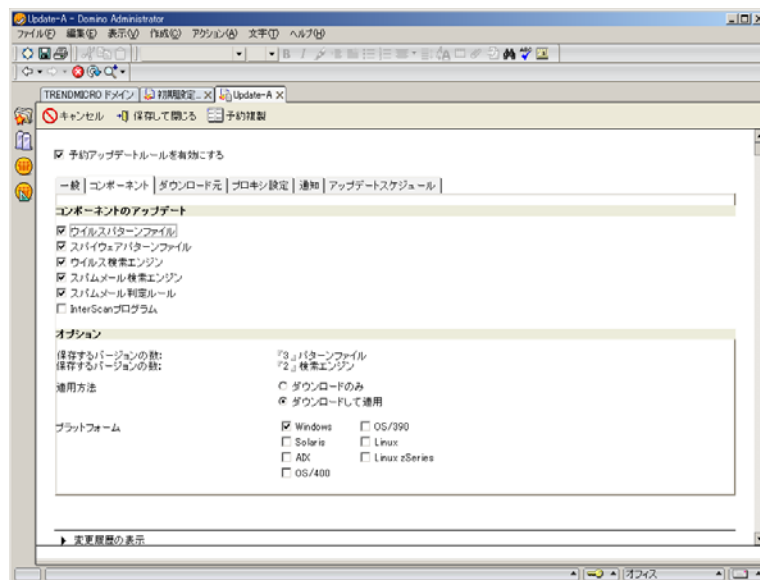


図 7-2. コンポーネントの選択

8. ダウンロード元を設定します (206 ページを参照)。
9. 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を設定します (208 ページを参照)。

10. アップデート通知を定義します (216 ページを参照)。

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

11. [アップデートスケジュール] タブをクリックして、予約アップデートの実行時刻、実行間隔 (分)、および曜日を設定します。
12. [予約複製] ボタンをクリックして Domino ディレクトリを起動し、予約複製を設定します。Notes のヘルプの「複製をスケジュールする」を参照してください。
13. [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)。最新のコンポーネントは、次の手順でダウンロードされて配信されます。

1. ダウンロード元に最新のコンポーネントがないか、InterScan によってチェックされます。
2. 最新の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されます。
3. 最後に、最新のコンポーネントが、アップデートデータベースから [一般] タブで指定されたサーバに配信されます。

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 (130 ページを参照) または変更 (132 ページを参照) します。
2. 作業領域で、[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] 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] ウィンドウで、自動的に配信するコンポーネントを選択します。
5. 保存するパターンファイルと検索エンジンのバージョン番号を、[保存するバージョンの数] フィールドに入力します。

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、多く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、ウィンドウを閉じます。
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。

アップデートの設定

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

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 (199 ページを参照) または手動アップデート (199 ページを参照) 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。
2. [コンポーネント] で、ダウンロードするコンポーネントを選択します。
3. 次のダウンロードオプションを設定します。
 - a. 保存するウイルスパターンファイルと検索エンジンのバージョン番号を、[保存するバージョンの数] フィールドに入力します。

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、多く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。

- b. プログラム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た後でアップデートを実行すると、最新のコンポーネントがアップデートデータベースにダウンロードされます。その後で、設定を [ダウンロードして適用] に変更すると、コンポーネントのダウンロードは実行されません。すでに最新のコンポーネントがアップデートデータベースに格納されているからです。そのため、[一般] タブで指定されたサーバに最新のコンポーネントが適用されることはありません。この場合は、複製データベースをダウンロード元として使用し、最新のコンポーネントをダウンロードして他のサーバに適用します。

- c. ダウンロードしたコンポーネントを適用するプラットフォームを選択します。

4. [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

コンポーネントのダウンロード元を設定するには、[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 (199 ページを参照) または手動アップデート (199 ページを参照) 画面で [ダウンロード元] タブをクリックして、次のダウンロード元のいずれかを選択します。

- 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 の中央サーバからの Pull 処理で自動的に複製されます。

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 Pull 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： 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 (<http://smln-p.activeupdate.trendmicro.co.jp/activeupdate/japan>) からダウンロードされます。

注意： InterScan では、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ダウンロードの際、初期設定でデジタル署名のチェックが行われます。デジタル署名ファイル (*.sig) を使用することにより、トレンドマイクロのアップデートサーバからの安全なダウンロードが実現します。

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 サーバをダウンロード用のハブサーバとして指定し、周辺の InterScan サーバでは複製機能を使用してコンポーネントを Pull 取得することもできます。

ヒント： アップデート問題のトラブルシューティングについては、270 ページの「アップデートの問題」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] フィールドに、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 パスは Windows 版でのみ指定できます。

最新コンポーネントが含まれるフォルダに、適切なデジタル署名ファイル (*.sig) が置かれている必要があります。デジタル署名ファイルが存在しない場合、ダウンロードは失敗します。

2. [保存して閉じる] をクリックします。

コンポーネントのダウンロードに使用するプロキシサーバを設定

インターネットにアクセスするためのプロキシサーバが InterScan で必要な場合は、[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 (199 ページを参照) または手動アップデート (199 ページを参照) 画面で、[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、[プロキシサーバを使用する] を選択します。
3. [プロキシ設定] にある [プロキシサーバを使用する] か、または [別の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、および使用するポートを指定します。
6. 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。
7. [保存して閉じる] をクリックします。

通知

Trend Micro InterScan for Domino 3.0 (以下、InterScan) ではメール、添付ファイル、文書中にウイルスその他の感染が検出されたとき、メールまたは Lotus Instant Messaging/Web Conferencing (以前の名称は Sametime Connect) 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、通知先として Domino 管理者、データベースの所有者、メールの送信者、受信者などを指定できます。

この章で説明する項目は次のとおりです。

- 210 ページの「通知の概要」
- 213 ページの「メールスタンプ (安全スタンプ) の使用」
- 214 ページの「通知の設定」

通知の概要

メールまたはデータベース文書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： 外部の送信者に通知を送信する場合は、必要以上に多くの宛先に通知を送信しないよう注意が必要です。

通知には次の 2 種類のカテゴリがあります。

- 検索通知は、メール検索、データベース検索、予約検索のルールで指定した条件に該当する不正なプログラムが検出されたときに送信されます。
- 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、またはユーザーが手動アップデートを実行したときに送信されます。

InterScan は、指定した宛先に個別に通知を送信します。メール検索処理後、そのメールが受信可能な場合、通知メッセージは受信メールのメッセージに追加表示されます。

通知メッセージには、ユーザーが設定したタグに基づいたイベント固有の情報を表示させることができます。たとえば、検索通知には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 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、メール検索の [検索オプション] タブで利用できます。

InterScan では、通知タグを使用して通知内容をカスタマイズできます。

検索オプション	タグ	値
ウイルス検索	%FILE%	感染したファイルの名前
	%DETECTION%	検出された不正プログラムの名前
	%ACTION%	検出時の処理
検索制限	%FILE%	感染したファイルの名前
	%CAUSE%	一致する検索制限オプション
	%ACTION%	検出時の処理
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名前
	%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の名前
	%MAILPART%	コンテンツフィルタに一致したメッセージの部分 : 件名、メール本文、添付ファイルの内容、添付ファイル名
	%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
	%CAUSE%	一致するスクリプトフィルタオプション
	%KEYWORDS%	一致するキーワード

- 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 / 予約検索の [通知テンプレート]、予約アップデート / 手動アップデートの [通知] で使用されるタグ。

タグ	値
%SERVER%	Domino/InterScan サーバ
%SENDER%	検索ルールに一致したメールの送信者
%RECIPIENTS%	検索ルールに一致したメールの受信者
%SUBJECT%	検索ルールに一致したメールの件名
%SEND_TIME%	メールが送信された日時 (年月日および時刻)
%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 でメールが検索された日時
%PRODUCTVERSION%	InterScan for 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%	[検索オプション] で、管理者への通知に指定した情報 (タグを含む)
%OWNER_FILTER_INFORMATION%	[検索オプション] で、データベース所有者への通知に指定した情報 (タグを含む)
%INTERNAL_FILTER_INFORMATION%	[検索オプション] で、内部の送信者 / 受信者への通知に指定した情報 (タグを含む)
%EXTERNAL_FILTER_INFORMATION%	[検索オプション] で、外部の送信者 / 受信者への通知に指定した情報 (タグを含む)
%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： 通知テンプレートは、指定されたフィルタベースのタグ情報をまとめてから、ポリシー通知設定を使用して通知を配信します (214 ページを参照)。通知テンプレートに << や >> のような文字は挿入しないでください。こうした文字は、解析エラーを引き起こし、これらの文字に

はさまれた内容は通知に表示されません。

メールスタンプ (安全スタンプ) の使用

通知以外に、メールスタンプによって InterScan の処理を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、次のようにメールの件名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。

各検索ルールの [検索オプション] タブでは、次のようにメールの件名または本文の一部としてメールスタンプを定義できます。

[検索オプション] タブ	利用可能なメールスタンプ
ウイルス検索	次の設定が可能です。 • ウイルスが検出された場合、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。 件名またはメール本文の末尾にメールスタンプを挿入します。
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。

[検索オプション] タブ	利用可能なメールスタンプ
スクリプトフィルタ	件名の末尾またはメール本文の先頭にメールスタンプを挿入します。 ホットスポットを、ポップアップメッセージ形式のメールスタンプに置換することもできます。

各フィルタで利用できる安全スタンプの設定方法については、次を参照してください。

- スпамメールフィルタ: 158 ページ
- ウイルス検索: 161 ページ
- 検索制限: 162 ページ
- メッセージフィルタ: 163 ページ
- 添付ファイルフィルタ: 172 ページ
- スクリプトフィルタ: 173 ページ

通知の設定

危険なコンテンツや迷惑メールの検出時、またはウイルス対策コンポーネントやコンテンツセキュリティコンポーネントの最新バージョンへのアップデート時に、通知を送信するように設定できます。

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 Sametime を介して通知を送信できます。通知方法を設定するには、[通知] タブを使用します。

通知の配信方法を設定するには

1. ポリシーを作成 (130 ページを参照)、または変更 (132 ページを参照) します。
2. 作業領域で、[通知] タブをクリックします。
3. 作業領域をダブルクリックするか、[編集] ボタンをクリックして、次の内容を設定します。
 - a.  をクリックするか、[返信アドレス] に送信者として通知に表示されるアドレスを入力します。
 - b. [Sametime サーバのホスト名 /IP アドレス]、[Sametime 送信者ユーザ名]、[Sametime 送信者パスワード] を入力し、Sametime のアドレスに通知が送信されるように設定します。
 - c. メールまたはデータベース文書が検索またはフィルタ処理されたとき、各イベントごとに異なる受信者へ、メールまたは Sametime で通知を配信するには、[イベントごとに通知受信者を指定する] を選択し、個別に受信者のアドレスを設定します。これを選択しない場合は、管理者のメールまたは Sametime の受信者に通知が送信されます。

注意： Sametime 通知は Windows 版でのみ使用できます。

4. [保存して閉じる] をクリックします。

検索通知の設定

通知内容を定義するには、[通知テンプレート] タブを使用します。通知テンプレートは、ルールごとに設定します。

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. 管理者、内部または外部のメール送信者 / 受信者、データベースの所有者への通知の件名または通知内容を設定します。タグが表示されているフィールドでは、タグを選択し、[追加] ボタンをクリックして、タグを追加することができます。

注意： 管理者宛ての通知は、ポリシーの [通知] タブで設定したメールアドレスに送信されます。詳細については、214 ページの「通知の配信方法の設定」を参照してください。

検索通知のコンポーネント情報の一部が「該当なし」と表示される場合があります。これは、メール検索、データベース検索、または予約検索において、そのコンポーネントが使用されなかったことを意味します。たとえば、添付ファイルフィルタではメール検索の際に検索エンジンとウイルスパターンファイルを使用しません。そのため、添付ファイルフィルタの検索通知に変数「%PATTERNVERSION%」を使用している場合、その値は「該当なし」と表示されます。

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方法は、次のとおりです。

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 (200 ページ) または予約アップデート (199 ページ) で、[通知] タブをクリックします。
2. 手動アップデートの場合、[管理者] フィールド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. 手動アップデートまたは予約アップデートの [通知] タブをクリックし、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 (198 ページを参照)。
 - 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： InterScan では、1 回の試行に 120 秒間を割り当てます。

4. アップデート通知に使用するメッセージを [件名] フィールドに入力します。
5. [保存して閉じる] をクリックします。

ログデータベースおよび隔離データベース

この章では、Trend Micro InterScan for Domino 3.0 (以下、InterScan) のログおよび隔離ログの表示と削除、および統計の生成について説明します。

この章で説明する項目は次のとおりです。

- 220 ページの「ログデータベースの使用」
- 231 ページの「隔離データベースの使用」

ログデータベースの使用

InterScan では、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、重要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検出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、定期的にログを削除するように InterScan を設定します。

InterScan のログは、次の設定に基づいて表示できます。

- 処理、日付、ユーザ、検出名 (不正プログラム名)、ルールに基づくグループ別
これらグループのいずれかについて、1 日単位、1 週間単位、または 1 か月単位で記録を表示できます。すべての日付の記録を表示することもできます。
- サービス (メール検索またはデータベース検索) に基づくグループ別

また、[統計] 画面では 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効率が良い場合があります。複製のみで周辺サーバからログを収集 (Pull 処理) する中央 Domino サーバの設置をお勧めします。

InterScan のログの管理

ログデータベース (smvlog.nsf) 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、ログの予約削除、手動削除、複製などがあります。

ログの内容を表示するには、ログデータベースを使用します。

ログを表示するには

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。
 - 設定データベースのメインメニューで [ログデータベース] をクリックします。
 - ログデータベースを直接開きます。
2. 次の基準に従って、表示するログを選択し、整理します。
 - 処理 — InterScan で実行された処理を基準にログを表示します。
 - 日付 — ウイルスなどの不正なプログラムが InterScan で検出された日付を基準にログを表示します。
 - ユーザ — 安全でないメッセージやスパムメールの受信者を基準にログを表示します。
 - 検出名 — 検出されたウイルスなどの不正なプログラムの名前を基準にログを表示します。
 - ルール — 不正プログラムやスパムメールを検出したルールの名前を基準にログを表示します。
 - データベース — データベース検索で生成されたログを表示します。
 - メール — メール検索で生成されたログを表示します。
3. 次のいずれかを選択します。
 - ログを表示する期間を選択します。
全日付、本日、過去 7 日間、または過去 30 日間の表示を選択します。
 -  をクリックして、フィールドの昇順または降順で並べ替えます。

ログ削除の有効化 / 無効化

ログを自動的に削除することができます。ログの削除を有効にすると、指定した条件でログが自動的に削除されます。また、手動削除においても、必要なときに指定した条件でログを削除することもできます。

注意： 隔離データベースから隔離ログを削除すると、同じレコードがログデータベースから自動的に削除されます。

隔離ログ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メインメニューで [ログデータベース] をクリックします。
 - ログデータベースを直接開きます。
2. 削除を有効化または無効化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。

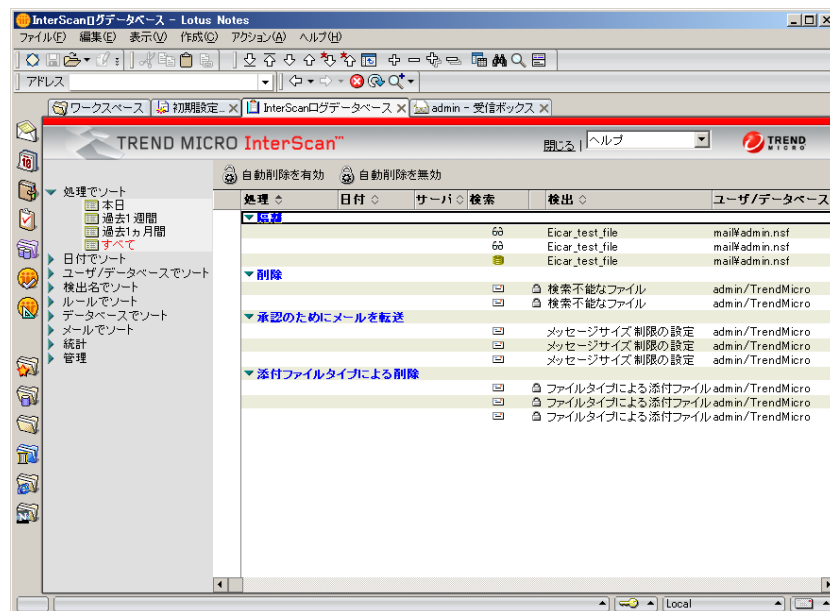


図 9-1. ログデータベースからのログ削除の有効化 / 無効化

注意：多数のログを一度に削除する場合は、それらのデータが保管不要なデータかどうかを事前に確認することをお勧めします。

ウイルスログの予約削除

指定した保管期間を経過したログを自動的に削除するようにできます。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：InterScan では、削除を有効にしたログを自動的に削除します。

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。
 - 設定データベース内のメインメニューで、[ログデータベース] をクリックします。
 - ログデータベースを直接開きます。
2. ログデータベース内のメインメニューで、[管理] → [予約削除] の順に選択します。[予約削除] 画面が表示されます。

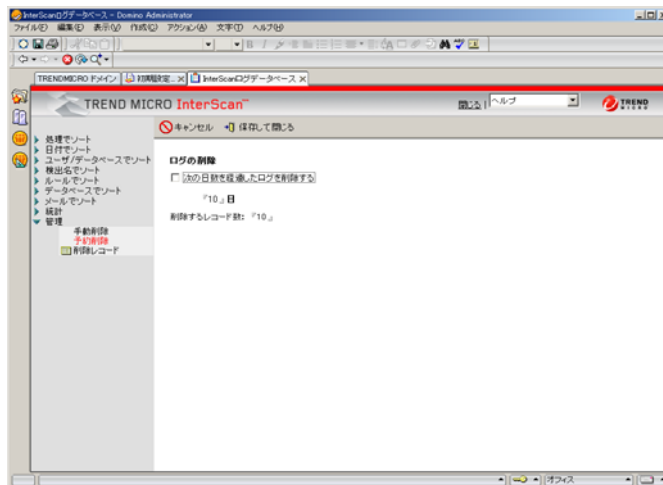


図 9-2. ログの予約削除の設定

3. [次の日数を経過したログを削除する] チェックボックスをオンにします。
4. ログを保持する期間を日数で入力します。
5. 保持するレコードの件数を入力します。

6. [保存して閉じる] をクリックします。

注意： InterScan が SUSE LINUX Enterprise Server 8 (Service Pack 3) サーバ上で稼動している場合、ウイルスログが自動的に削除されないことがあります。ウイルスログを自動的に削除できず、次のエラーメッセージが Domino コンソールに表示されることがあります。

AMgr:Agent 'Delete log files (Auto)' in 'smd/smvlog.nsf' does not have proper execution access, cannot be run

このエラーが発生した場合は、Domino Administrator を使用して、手動でログデータベースに server.id の署名をしてください。

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。

ログファイルを手動で削除するには

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。
 - 設定データベースのメインメニューで [ログデータベース] をクリックします。
 - ログデータベースを直接開きます。

2. ログデータベース内のメインメニューで、[管理] → [手動削除] の順に選択します。[手動削除] 画面が表示されます。



図 9-3. ログの手動削除

3. 次のいずれかを実行します。
- ログデータベースに存在する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。
 - a. [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。
 - b. 削除するログを選択します。
 - c. [OK] をクリックします。
4. [今すぐ削除] をクリックします。
- 削除するように指定したログのみが削除されます。

統計とグラフの表示

ログ統計オプションを使用すると、サーバ上のメールおよびデータベースのログに関する数値情報を作成できます。この統計は、駆除、削除、隔離、放置、ブロックに分類されて表示されます。また、ウイルス検索、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、スパムメールフィルタ、大規模感染予防フィルタ、転送されたメッセージの統計を生成するオプションも用意されています。

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. 以下のいずれかの手順でログデータベースを開きます。
 - 設定データベースのメインメニューで [ログデータベース] をクリックします。
 - ログデータベースを直接開きます。
2. ログデータベース内のメインメニューで、[統計] → [ログ統計] の順に選択します。
3. [ウイルス検索]、[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памメールフィルタ]、[大規模感染予防フィルタ]、[転送されたメッセージ] の各統計をすべて選択するか、表示する特定の統計をこれらの中から選択します。
4. 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)。
5. 表示する期間の範囲を選択します。
6. [ログ数値反映] をクリックすると、選択したログのレポートが作成されます。
7. [エクスポート] をクリックすると、生成されたデータが *.csv ファイルにエクスポートされます。

*.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。

Microsoft Excel による *.csv にエクスポートしたログの表示

Microsoft Excel を使用すると、エクスポートした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したがって操作します。
 - i. [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。
 - ii. [タブ] チェックボックスがオンになっている場合は、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、[次へ] をクリックします。
 - iii. ウィザードの最後の画面では何も変更せず、[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。

グラフの生成および表示

[トップ 10 グラフ] オプションを使用すると、各種データを表す次のような棒グラフを生成できます。

- ウイルスグラフ — 検出件数が上位 10 位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。

グラフを生成、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。
 - 設定データベース内のメインメニューで、[ログデータベース] をクリックします。
 - ログデータベースを直接開きます。
2. ログデータベース内のメインメニューで、[統計] → [トップ 10 グラフ] の順に選択します。
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. 表示する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、棒グラフにはサンプルデータが表示されます。

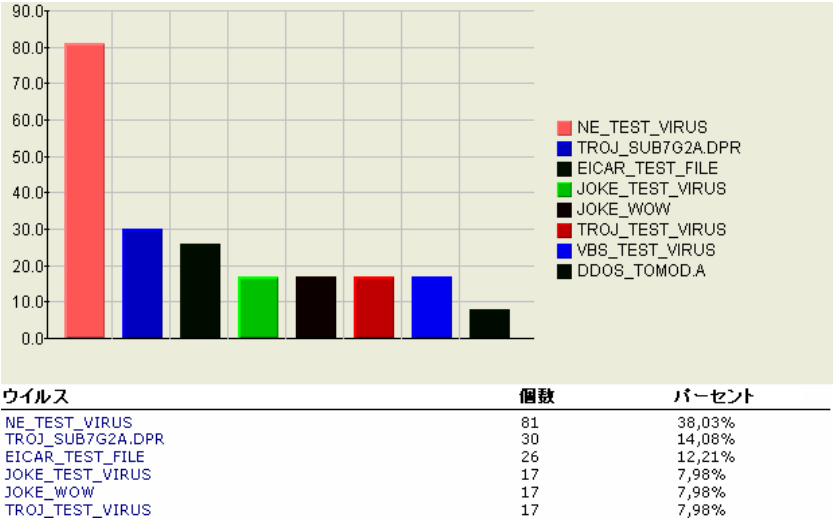


図 9-4. グラフの例

隔離データベースの使用

隔離データベース (smquar.nsf) には、ウイルス検索、検索制限、フィルタールール、スパムメールフィルタによって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、隔離するたびにログが生成され、smquar.nsf データベースに新規文書として保存されます。

隔離ログを x 日ごとに自動的に削除するように、InterScan を設定します（詳細については、223 ページの「ウイルスログの予約削除」を参照）。また、必要に応じて手動でログを削除します（詳細については、225 ページの「ウイルスログの手動削除」を参照）。

隔離メッセージまたは隔離添付ファイルの表示

隔離項目にアクセスし、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。

隔離メッセージまたは隔離添付ファイルを表示するには

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。
 - 設定データベース内のメインメニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。

2. 次の基準に従って、表示する隔離ログを選択します。
 - ウイルス検索 / 検索制限 — ウイルスなどの不正プログラムへの感染が検出されたために隔離されたメッセージを表示します。
 - 隔離されたメッセージ — コンテンツフィルタとスクリプトフィルタに基づいて隔離されたメッセージ、および検索制限に一致したために隔離されたメッセージを表示します。
 - 隔離された添付ファイル — 添付ファイルフィルタの条件に一致したために隔離された添付ファイルを表示します。
 - 暗号化メール — メッセージフィルタの条件に一致したために隔離されたメッセージを表示します。
 - 送信者 / 受信者
 - 受信者 — メッセージの受信者ごとに隔離された添付ファイルを表示します。
 - 送信者 — メッセージの送信者ごとに隔離された添付ファイルを表示します。
3. 次のいずれかを実行します。
 - 表示する期間を指定して、検索結果を整理します (全日付、本日、過去 7 日間、または過去 1 ヶ月の表示を選択)。
 -  をクリックして、フィールドの昇順または降順で並べ替えます。

隔離メッセージの再送信

隔離メッセージとは、メール検索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. 以下のいずれかの手順で隔離データベースを開きます。
 - 設定データベース内のメインメニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。
2. メインメニューで、再送信する隔離メッセージを選択します。
3. [再送信を有効] をクリックします。
4. 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。
 が表示されていないメッセージは再送信できません。
5. [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ってください。悪意のある動作を意図したコンテンツを含む文書を復元して開くと、ウイルスの感染を拡大するおそれがあります。

隔離文書を復元するには

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。
 - 設定データベース内のメインメニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。
2. メインメニューで、復元する隔離文書を選択します。

3. 作業領域で、隔離文書を選択して右クリックし、[コピー] を選択します。
4. 隔離文書を復元するデータベースを開き、コピーした文書を貼り付けます。

隔離された項目の削除の有効化および無効化

隔離された項目の削除を有効、または無効にするには、隔離データベースを使用します。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。削除を有効にしているログでも、手動でいつでも削除できます。

隔離ログ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メニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。
2. 削除を有効にする隔離項目、または無効にする隔離項目を選択します。

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。

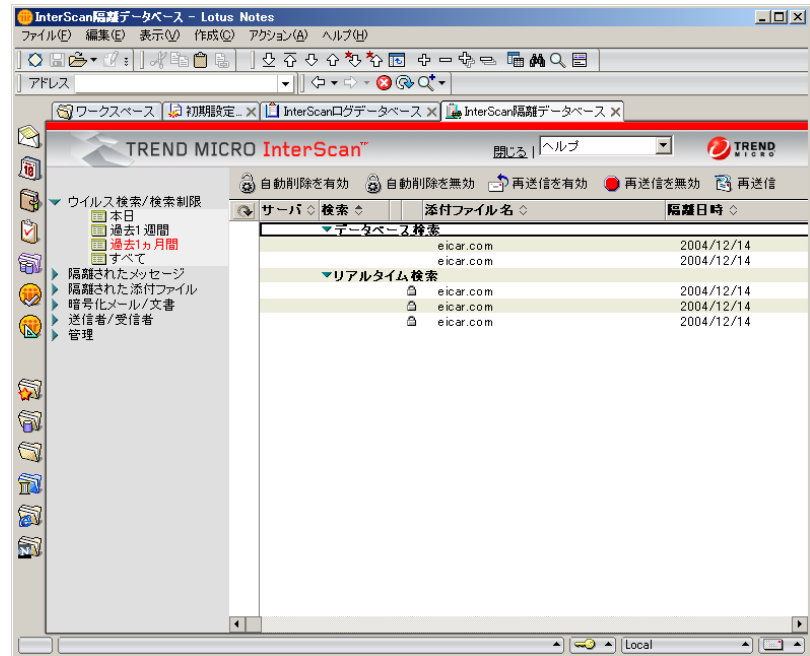


図 9-5. 隔離された項目の削除の有効化 / 無効化

注意： 削除を有効にする前に、それらが本当に保管不要なデータかどうかを事前に確認することをお勧めします。

隔離ログの予約削除

指定した保管期間を経過した隔離ログを自動的に削除するようにできます。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： InterScan では、削除を有効にした隔離ログを自動的に削除します。

隔離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隔離データベースを開きます。
 - 設定データベースのメニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。
2. 隔離データベース内のメインメニューで、[管理] → [予約削除] の順に選択します。
3. [自動削除を有効にする] を選択します。
4. 隔離された文書の種類を選択し、ログを保管する期間を日数で指定します。
5. 保持するレコードの件数を入力します。
6. [保存して閉じる] をクリックします。

隔離ログの手動削除

隔離ログを手動で削除するには、隔離データベースを使用します。

隔離ログファイルを手動で削除するには

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メニューで、[隔離データベース] をクリックします。
 - 隔離データベースを直接開きます。
2. 隔離データベース内のメインメニューで、[管理] → [手動削除] の順にクリックします。
3. 次のいずれかを実行します。
 - 隔離データベースにある存在するログ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。
 - 選択したログを削除する場合は、[選択した隔離文書を削除] を選択します。

- a. [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。
 - b. InterScan で削除する隔離ログを選択します。
 - c. [OK] をクリックします。
4. [今すぐ削除] をクリックします。
削除するように指定した隔離ログのみが削除されます。

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ツールです。

この章で説明する項目は次のとおりです。

- 240 ページの「Control Manager について」
- 242 ページの「Control Manager エージェントについて」
- 243 ページの「トレンドマイクロ 大規模感染予防サービスについて」
- 244 ページの「Control Manager を使用した InterScan の管理」

Control Manager について

Control Manager は、トレンドマイクロの製品とサービス、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製品を、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、ネットワーク上に展開したウイルス対策と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。

さまざまな企業のニーズに応えるために、Control Manager にはスタンダード版とエンタープライズ版があります。

- 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には、スタンダード版の機能に加え、カスケードコンソールのサポートやレポート機能などのさまざまな高度な機能が用意されています。

主要な機能

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。
- 階層構造により、管理者はアクセス制御を決定できます。
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。
- トレンドマイクロ 大規模感染予防サービス (以下、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を随時リリースしています。

- トレンドマイクロ 脆弱性診断サービス (以下、脆弱性診断サービス) では、ネットワークに潜むセキュリティ上の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からの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。
- トレンドマイクロ ダメージクリーンアップサービス (以下、ダメージクリーンアップサービス) では、感染を診断し、ワームやトロイの木馬など、残存する不正プログラムによって影響を受けたシステムを修復します。
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 からの集中管理

Control Manager は、複数の Domino サーバを持つ組織や、InterScan 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
- 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
- 一元化された設定コンソール
- 一元化されたコンポーネント配信

注意： Control Manager から配信できるのは、ウイルスパターンファイルおよび検索エンジンのみです。その他のコンポーネントは配信できません。

Control Manager エージェントについて

Control Manager から管理する 1 つの InterScan につき 1 つの Control Manager エージェントが存在し、次の処理を行います。

- コミュニケータを介して、Control Manager サーバからのコマンドを受信します。
- コミュニケータを介して、管理対象製品のステータスとログを収集し、それらを Control Manager に送信します。

コミュニケータは、メッセージ配信フレームワーク (MRF) ともいい、Control Manager システムの通信バックボーンとして機能します。これは、Trend Micro Management Infrastructure (TMI) のコンポーネントの 1 つです。コミュニケータでは、Control Manager サーバと管理対象製品との通信が処理されます。管理対象製品との通信では、Control Manager エージェントとコミュニケータとの通信処理が行われます。

Control Manager エージェントは、InterScan サーバにインストールされるアプリケーションの 1 つで、これによって Control Manager から製品の管理ができるようになります。エージェントは、管理対象製品およびコミュニケータと通信します。これにより、管理対象製品とコミュニケータを接続するコンポーネントとして機能します。そのため、InterScan と同じサーバに、InterScan 用の Control Manager エージェントをインストールする必要があります。

インストールが終了すると、Control Manager エージェントと TMI ファイルが次の場所に保存されます (Windows の場合)。

- **<root>:\Program Files\Trend Micro\ScanMail for Domino\CMAgent**
- **<root>:\Program Files\<Trend Micro または Trend>\Common\TMI**

Linux、Solaris、および AIX サーバの場合

- /opt/Trend/TMI
- /opt/Trend/SMD/CMAgent

i5/OS、OS/400 サーバの場合

- /qibm/UserData/Trend/TMI
- /qibm/UserData/Trend/SMD/CMAgent

トレンドマイクロ 大規模感染予防サービスについて

注意：メール検索が有効になっていない場合、大規模感染予防サービスは適用されません。また、大規模感染予防ポリシーによって配信される設定は、メール検索のみに適用されます。データベース検索には適用されません。

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時に、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、ウイルスやワームの大規模な発生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、感染の拡大を防止できます。

Control Manager を使用した InterScan の管理

Control Manager 管理コンソールを使用して、ネットワーク上の任意のコンピュータから InterScan を設定できます。

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でアクセスする方法

Control Manager サーバから管理コンソールにアクセスするには

- a. [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。
- b. 表示されるフィールドにユーザ ID とパスワードを入力します。
- c. [ログオン] をクリックします。

管理コンソールにリモートでアクセスするには

- a. ブラウザのアドレスフィールドに次の URL を入力して、ログオンページを開きます。
http://{host name}/ControlManager
{host name} 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。
- b. 表示されるフィールドにユーザ ID とパスワードを入力します。
- c. [ログオン] をクリックします。

Control Manager 管理コンソールからの InterScan の設定

Control Manager 管理コンソールは、Web ベースのコンソールです。これにより、互換性のある Web ブラウザを使用して、任意のコンピュータから Control Manager ネットワークを管理できます。互換性のあるブラウザのリストについては、Control Manager のマニュアル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]→[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。

InterScan の管理画面にアクセスするには

1. Control Manager 管理コンソールにアクセスします (244 ページを参照)。
2. メインメニューの [製品] をクリックします。
3. メインメニューで、リストから [管理下の製品] を選択し、[表示] をクリックします。
4. 製品ディレクトリを展開して、管理対象の InterScan のアイコンを選択します。
次のいずれかを実行します。

InterScan のステータスを確認するには

- 作業領域で、[製品ステータス] タブをクリックします。
[製品ステータス] 画面には、製品情報、コンポーネントのステータス、OS 情報、およびエージェント環境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] タブをクリックします。

2. 表示された製品リストから対象の InterScan を選択し、[次へ] をクリックします。設定データベースの Web コンソールが表示されます。
3. 必要であれば、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。
4. 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。

コンポーネントを配信するには

1. 作業領域で、[タスク] タブをクリックします。
2. [タスク] リストからタスクを選択し、[次へ] をクリックします。
3. [配信開始] をクリックして、最新のコンポーネントの InterScan サーバへの配信を開始します。

セキュリティログやイベントログを表示するには

1. 作業領域で、[ログ] タブをクリックします。
2. 表示するログの種類を選択します。
 - **セキュリティログ**には、ウイルス検出、コンテンツセキュリティ違反、ダウンロードトラフィック (HTTP、FTP)、メール、ファイルで検出されたウイルス、および Web セキュリティ違反などのイベントが記録されます。[セキュリティログ検索] 画面で、表示するログのイベントの種類を選択し、[クエリ] をクリックします。
 - **イベントログ**には、Control Manager サーバから管理対象製品に送信されたコマンド、管理対象製品のステータス変更イベントが記録されます。

注意： イベントログには、Control Manager サーバから管理下の製品に送信されたコマンドと、管理下の製品のステータス変更イベントが記録されます。

3. 重大度やイベントなどの検索パラメータを指定します。

4. [ログ表示] をクリックし、クエリを開始します。
5. [CSV 形式で保存] をクリックすると、画面上のデータを CSV 形式のファイルにエクスポートできます。

CSV 形式でログをエクスポートするには

1. [CSV 形式で保存] で [ファイルの表示] を右クリックし、[対象をファイルに保存] を選択します。
2. [名前を付けて保存] 画面で、ファイルの保存場所を指定します。
3. [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：メール検索が有効になっていない場合、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. 設定データベースを開きます。
 - b. メインメニューで、[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 管理コンソールから [サービス] ページを使用する方法
 - a. Control Manager 管理コンソールにアクセスします (244 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. メインメニューで、[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。

このページでは表示が自動的に更新され、最上位に常に最新の脅威およびステータス情報が表示されます。

期限切れ大規模感染予防ポリシーの削除

注意：リアルタイム検索が有効になっていない場合、大規模感染予防サービスは適用されません。

無効または期限切れの大規模感染予防ポリシーを削除するには、設定データベースを使用します。

大規模感染予防ポリシーを削除するには

1. 設定データベースを開きます。
2. メインメニューで、[設定]→[大規模感染予防サービス] の順にクリックします。
3. 作業領域で、[期限切れ大規模感染予防ポリシーの自動削除を無効にする] をクリックします。
4. [OK] をクリックし、確定します。

期限切れの大規模感染予防ポリシーは、設定データベースへの署名に使用した ID が次の条件に該当する場合に削除できます。

- 「編集者」以上の権限を持つ場合
- アクセス制御リストの文書の削除オプションが有効になっている場合

Control Manager エージェントによって、30 分ごとに大規模感染予防ポリシーの有効期限が確認され、期限切れのポリシーが削除されます。

アンインストール

この章では、Domino 環境から Trend Micro InterScan for Domino 3.0 (以下、InterScan)、および InterScan 用 Trend Micro Control Manager (以下、Control Manager)エージェントをアンインストールする方法について説明します。

この章で説明する項目は次のとおりです。

- 250 ページの「InterScan のアンインストール」
- 261 ページの「InterScan 用 Control Manager エージェントのアンインストール」

InterScan のアンインストール

InterScan は、次のような方法でアンインストールできます。

- Windows 版 /Linux 版 /Solaris 版 /AIX 版 – ウィザードベースのセットアッププログラムを使用
- Linux 版 /Solaris 版 /AIX 版 /i5/OS および OS/400 版 – コンソールベースのセットアッププログラムを使用

すべてのプラットフォームにおいて、InterScan を手動でアンインストールすることも可能ですが、ウィザードまたはコンソールベースのセットアッププログラムを使用してアンインストールすることをお勧めします。

InterScan をアンインストールする前に、次の処理を実行してください。

- Domino サーバと Notes クライアントが実行されている場合は、停止します。
- i5/OS および OS/400 プラットフォームでは、対象サーバが停止していることと、トレンドマイクロライブラリ内のすべてのジョブがロックされていないことを確認します。
- InterScan 用 Control Manager エージェントをインストールしている場合は、これを先にアンインストールします (261 ページの「InterScan 用 Control Manager エージェントのアンインストール」を参照)。

InterScan の自動アンインストール

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

ウィザードベースで InterScan をアンインストールするときは、グラフィカルインタフェースによるアンインストール手順の案内が示されます。

グラフィカルインタフェースを使用して InterScan をアンインストールするには

1. 次のいずれかの方法で、アンインストールプログラムに移動します。
 - Windows 版の InterScan をアンインストールする場合は、次のいずれかを実行してアンインストールプログラムを起動します。
 - [スタート] メニューから [プログラム]→[Trend Micro InterScan for Domino]→[InterScan for Domino のアンインストール] の順に選択します。
 - <root>:\Program Files\Trend Micro\ScanMail for Domino\Uninstall に移動します。
 - Linux 版、Solaris 版、または AIX 版の InterScan をアンインストールする場合は、次のディレクトリに移動します。
/opt/trend/SMD/Uninstall
2. 次のいずれかを実行してアンインストールプログラムを起動します。

プラットフォーム	アンインストールプログラム
Windows	uninstaller32.exe
Linux	SMD3UninstallerLinux.bin
Solaris	SMD3UninstallerSolaris.bin
AIX	SMD3UninstallerAix.bin

表 11-1. InterScan for Domino のアンインストールプログラム

3. [はい] をクリックし、InterScan のアンインストールを開始します。

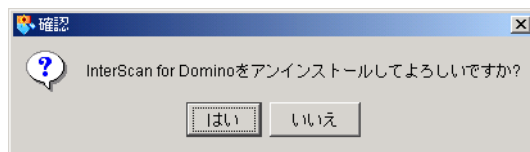


図 11-1. アンインストールの確認

4. サーバの選択画面で、InterScan をアンインストールするサーバを選択します。

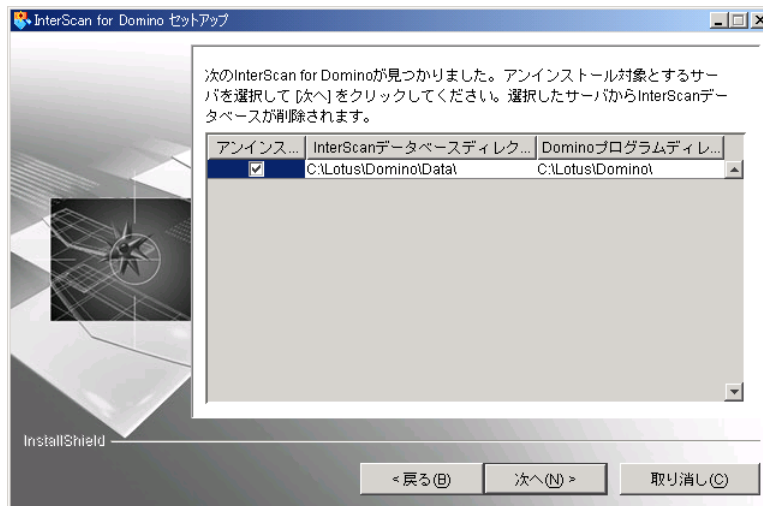


図 11-2. アンインストールする InterScan の選択

5. [次へ] をクリックします。

Domino データディレクトリの下にインストールされた共有プログラムファイルと標準プログラムファイルが削除されます。また、プログラムフォルダ、ディレクトリ、Windows レジストリに作成されたエントリ、および notes.ini に追加されたエントリも削除されます。

6. [終了] をクリックして、アンインストールを終了します。

7. AIX および Solaris プラットフォームで InterScan を使用している場合は、次のコマンドを実行して、セットアップログと空のプログラムフォルダを手動で削除します。

```
cd /opt/trend
```

```
rm smdins.log (InterScan のインストールログ)
```

```
rm smundins.log (InterScan のアンインストールログ)
```

```
rm cmains.log (Control Manager エージェントのインストールログ)
```

```
rm cmaunins.log (Control Manager エージェントのアンインストールログ)
```

```
rm -fr SMD
```

注意： Windows プラットフォームの場合は、[スタート]→[コントロールパネル]→[アプリケーションの追加と削除] の順にクリックし、[Trend Micro InterScan for Domino] を選択して InterScan をアンインストールすることもできます。

コンソールベースのアンインストール

Linux 版、AIX 版、および Solaris 版では、コンソールベースのアンインストールがサポートされます (Windows 版では動作確認されていません)。

コンソールから InterScan をアンインストールするには

1. InterScan のアンインストールプログラムを含むディレクトリ (通常は、`/opt/trend/SMD/Uninstall`) から、次のコマンドを実行します。

Linux 版の場合：

```
./SMDUninstallerLinux.bin -console
```

Solaris 版の場合：

```
./SMDUninstallerSolaris.bin -console
```

AIX 版の場合：

```
./SMDUninstallerAIX.bin -console
```

2. 「1」を入力し、InterScan をアンインストールします。
3. 複数の InterScan が存在する場合は、インデックス番号を入力し、対象の InterScan がインストールされているサーバを選択します。
4. 「3」を入力し、セットアップを終了します。

5. 次のコマンドを実行して、セットアップログと空のプログラムフォルダを手動で削除します。

```
cd /opt/trend
```

```
rm smdins.log (InterScan のインストールログ)
```

```
rm smundins.log (InterScan のアンインストールログ)
```

```
rm cmains.log (Control Manager エージェントのインストールログ)
```

```
rm cmaunins.log (Control Manager エージェントのアンインストールログ)
```

```
rm -fr SMD
```

注意： アンインストール後に Notes のワークスペースから InterScan アイコンが消えない場合は、各アイコンを右クリックし、表示されたメニューから [ワークスペースから削除] を選択します。また、notes.ini ファイルの InterScan エントリ (ScanMailInstallPath など) を手動で削除することもできます。

コマンドコンソールから InterScan のアンインストールを実行するには (i5/OS および OS/400)

1. InterScan アンインストールプログラムを含むディレクトリ (通常、/QIBM/UserData/trend/SMD/Uninstall) から、次のコマンドを実行します。

QShell

```
java -cp /QIBM/ProdData/Java400/jt400ntv.jar:  
/QIBM/UserData/trend/SMD/Uninstall/setup.jar run -console
```

CL コマンド

```
RUNJAVA CLASS(run) PARM('-console') CLASSPATH  
( '/QIBM/ProdData/Java400/jt400ntv.jar:/QIBM/UserData/trend  
/SMD/Uninstall/setup.jar')
```

2. 「1」を入力し、InterScan をアンインストールします。
3. 複数の InterScan が存在する場合は、インデックス番号を入力し、対象の InterScan がインストールされているサーバを選択します。

4. 「3」を入力し、セットアップを終了します。

単一または共有 InterScan の手動アンインストール

InterScan を自動アンインストールできなかった場合、手動で InterScan をアンインストールできます。ただし、手動でアンインストールする前に自動アンインストールを試みることをお勧めします。

サーバに複数の InterScan が共有インストールされていて、これらのすべてを手動でアンインストールする場合の手順は、共有されていない単一の InterScan を手動でアンインストールする手順とほぼ同じです。

各 InterScan のインストール情報とファイルパスはすべて `smdsys.ini` に記録され、`smdsys.ini` には複数の `[DomSvrX]` が含まれます。

単一または共有の InterScan を手動でアンインストールするには

ヒント： InterScan と Control Manager のファイルおよびフォルダ構造については、301 ページの「ファイルおよびフォルダー一覧」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` を探し、テキストエディタで開きます。内容を参照しながら、以降の手順を実行します。

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**
- **ProductID**

注意： 1 つの DomSvr{X} エントリは、1 つの InterScan を表します。{X} は、InterScan に対応する番号です。目的のサーバ上の InterScan インストールが 1 つのみの場合、DomSvr{X} は DomSvr0 となります。複数の InterScan インストールがある場合、DomSvr0 から始まり、DomSvr1、DomSvr2 と順に続きます。

複数の InterScan がインストールされた Windows サーバの `smdsys.ini` の例を次に示します。

[SMDConf]

DomSvrISMDCount=5 \\InterScan インストールの数を
示します

ProductID=1faa7e494dca845ffe3515a3b077fa29

ProductVersion=V3.0.0.1183

ProductPath=C:\Program Files\Trend
Micro\ScanMail for Domino\

[DomSvr0] \\1 番目の InterScan を示します

DomSvr0NotesIniPath=D:\Lotus\r6.5\Data2\notes.in
i

DomSvr0DominoBinPath=d:\lotus\r6.5\Prog\

DomSvr0DataPath=d:\lotus\r6.5\data2\

DomSvr0DominoVersion=0

DomSvr0SMDVersion=3.0

[DomSvr1] \\2 番目の InterScan を示します

DomSvr1NotesIniPath=D:\Lotus\R6\Data1\notes.ini

DomSvr1DominoBinPath=d:\lotus\r6\

DomSvr1DataPath=d:\lotus\r6\data1\

DomSvr1DominoVersion=0

DomSvr1SMDVersion=3.0

[DomSvr2] \\3 番目の InterScan を示します

DomSvr2NotesIniPath=D:\Lotus\R6\data2\notes.ini

DomSvr2DominoBinPath=d:\lotus\r6\

DomSvr2DataPath=d:\lotus\r6\data2\

DomSvr2DominoVersion=0

DomSvr2SMDVersion=3.0

2. DomSvr{X}DominoBinPath で指定されたディレクトリに移動し、InterScan のインストールファイルを削除します。

注意： InterScan のファイル一覧については、付録 C を参照してください。

3. DomSvr{X}DataPath で指定されたディレクトリに移動し、InterScan のインストールファイルおよび一時フォルダを削除します。

注意： InterScan のファイル一覧については、付録 C を参照してください。

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 セクションを探し、次の項目を削除します。

- **SMDemf**
- **SMDreal**
- **SMDsch**
- **SMDmon**

- 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. ProductPath で指定されたフォルダを削除します。このフォルダには、ウイルス検索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。
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ます (268 ページを参照)。

9. Windows サーバにインストールされた InterScan では、次の手順に従います。
 - a. レジストリを開き、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\\${ProductID}

{ProductID} は、smdsys.ini に記述されている ProductID の値です。
 - b. C:\Documents and Settings\All Users\Start Menu\Programs から、Trend Micro InterScan for Domino フォルダを削除します。これにより、[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. レジストリから、次の InterScan 製品キーを削除します。
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Domino
10. smdsys.ini を閉じた後、削除します。
11. i5/OS および OS/400 プラットフォームの場合のみ、CL コマンド go licpgm を使用し、「12」を入力して SMD ライセンスを削除します。
12. Domino サーバを再起動します。

InterScan 用 Control Manager エージェントのアンインストール

InterScan と Control Manager エージェントのいずれか、または両方をアンインストールする場合は、必ず先に Domino を停止します。Control Manager エージェントを先にアンインストールしてから製品をアンインストールし、最後に Trend Micro Management Infrastructure (TMI) をアンインストールします。Control Manager エージェントをアンインストールする際、他の Control Manager エージェントがサーバ上に存在しない場合は、Trend Micro Management Infrastructure (TMI) も自動的にアンインストールされます。TMI を手動でアンインストールする必要がある場合は、InterScan をアンインストールした後でアンインストールしてください。

注意： InterScan 用 Control Manager をアンインストールする際は、Domino サーバが起動している必要があります。

InterScan 用 Control Manager エージェントをアンインストールするには、次のいずれかの方法を実行します。

- ウィザードベースでのアンインストールの実行
- コンソールベースでのアンインストールの実行

ウィザードベースでのアンインストール

ウィザードベースで Control Manager エージェントをアンインストールするときは、グラフィカルインタフェースによるアンインストール手順の案内が示されます。

ウィザードベースでアンインストールを実行するには

1. 次のいずれかの方法で、アンインストールプログラムに移動します。
 - Windows 版の InterScan をアンインストールする場合は、<root>:\Program Files\Trend Micro\ScanMail for Domino\CMAgent\Uninstall\ に移動します。

ヒント：Windows のタスクバーから Control Manager エージェントをアンインストールすることもできます。[スタート]→[設定]→[コントロールパネル]→[アプリケーションの追加と削除] の順にクリックし、[Trend Micro InterScan for Domino] を選択します (Windows 2000 の場合)。

- Linux 版、Solaris 版、または AIX 版の InterScan をアンインストールする場合は、/opt/trend/SMD/CMAgent/Uninstall/ に移動します。
2. 次のいずれかのファイルを実行してアンインストールプログラムを起動します。

プラットフォーム	アンインストールプログラム
Windows	cmaunins32.exe
Linux	CMAgent3UninstallerLinux.bin
Solaris	CMAgent3UninstallerSolaris.bin
AIX	CMAgent3UninstallerAIX.bin

表 11-2. Control Manager エージェントのアンインストールプログラム

3. [はい] をクリックし、確定します。
4. アンインストールの終了後、[終了] をクリックします。

これにより、Control Manager エージェントがアンインストールされます。Control Manager 管理コンソールにアクセスし、管理対象の InterScan が製品ディレクトリに表示されていないければ、Control Manager エージェントは正しくアンインストールされています。

コンソールベースでのアンインストールの実行

Linux 版、Solaris 版、AIX 版、i5/OS または OS/400 版では、コンソールベースのアンインストールがサポートされています。

コンソールベースで Control Manager エージェントのアンインストールを実行するには (i5/OS および OS/400 版)

1. Control Manager エージェントのアンインストールプログラムを含むディレクトリ (通常は、/QIBM/UserData/trend/SMD/CMAgent/Uninstall/) から、次のコマンドを実行します。

```
java -cp
```

```
/QIBM/ProdData/Java400/jt400ntv.jar:/QIBM/UserData/trend/SMD/CMAgent/Uninstall/setup.jar run -console
```

2. 「1」を入力して、Control Manager エージェントをアンインストールします。
3. 「3」を入力し、セットアップを終了します。

これにより、Control Manager エージェントがアンインストールされます。Control Manager 管理コンソールにアクセスし、InterScan の管理対象製品が製品ディレクトリに表示されていない場合は、Control Manager エージェントは正しくアンインストールされています。

コンソールベースで Control Manager エージェントのアンインストールを実行するには (Linux 版、Solaris 版、または AIX 版)

1. Control Manager エージェントのアンインストールプログラムを含むディレクトリ (通常は、/opt/trend/SMD/CMAgent/Uninstall/) から、次のコマンドを実行します。

Linux 版の場合:

```
./CMAgent3UninstallerLinux.bin -console
```

Solaris 版の場合:

```
./CMAgent3UninstallerSolaris.bin -console
```

AIX 版の場合:

```
./CMAgent3UninstallerAIX.bin -console
```

2. 「1」を入力して、Control Manager エージェントをアンインストールします。
3. 「3」を入力し、セットアップを終了します。

これにより、Control Manager エージェントがアンインストールされます。Control Manager 管理コンソールにアクセスし、InterScan の管理対象製品が製品ディレクトリに表示されていないければ、Control Manager エージェントは正しくアンインストールされています。

TMI のアンインストール

Windows プラットフォームで InterScan を使用している場合、Domino サーバ上に他の Control Manager エージェントがインストールされていない場合は、TMI をアンインストールしてください。

i5/OS および OS/400 プラットフォームでは、エージェントがサーバからアンインストールされると、Control Manager エージェントのアンインストーラによって TMI がアンインストールされます。

TMI をアンインストールするには

1. Windows のタスクバーから、[スタート]→[設定]→[コントロールパネル]→[アプリケーションの追加と削除] の順にクリックします。
2. リストを下にスクロールして、[Trend Micro Management Infrastructure] を選択してから、[削除] および [はい] をクリックして TMI のアンインストールを開始します。
3. アンインストールの終了後、[閉じる] をクリックします。

トラブルシューティング

この章では、Trend Micro InterScan for Domino 3.0 (以下、InterScan) 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。

この章で説明する項目は次のとおりです。

- 268 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場所」
- 269 ページの「AIX および Solaris 版における Control Manager サーバへの登録の問題」
- 269 ページの「保留メールの問題」
- 270 ページの「アップデートの問題」
- 272 ページの「予約検索 / アップデートの問題」
- 272 ページの「破損した InterScan データベースの修復」
- 274 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」
- 275 ページの「InterScan タスクのデバッグ」
- 277 ページの「InterScan 用 Control Manager エージェントのデバッグ」
- 278 ページの「デバッグログの収集」
- 281 ページの「InterScan のエラーメッセージについて」

インストールログおよびアンインストールログの場所

InterScan および InterScan 用の Trend Micro Control Manager (以下、Control Manager) エージェントのログは、次のとおりです。

プラットフォーム	保存場所とファイル名	説明
Windows	<root>\smdins.log	InterScan のインストールログ
	<root>\smdunins.log	InterScan のアンインストールログ
	<root>\setuplog.txt	InterScan のサイレントインストールログ
	<root>\cmains.log	InterScan 用 Control Manager エージェントのインストールログ
	<root>\cmaunins.log	InterScan 用 Control Manager エージェントのアンインストールログ
Linux/Solaris/AIX	/opt/trend/smdins.log	InterScan のインストールログ
	/opt/trend/smdunins.log	InterScan のアンインストールログ
	/opt/trend/cmains.log	InterScan 用 Control Manager エージェントのインストールログ
	/opt/trend/cmaunins.log	InterScan 用 Control Manager エージェントのアンインストールログ
i5/OS、OS/400	/QIBM/UserData/trend/smdins.log	InterScan のインストールログ
	/QIBM/UserData/trend/smdunins.log	InterScan のアンインストールログ
	/QIBM/UserData/trend/cmains.log	InterScan 用 Control Manager エージェントのインストールログ
	/QIBM/UserData/trend/cmaunins.log	InterScan 用 Control Manager エージェントのアンインストールログ

表 12-1. インストールログおよびアンインストールログ

AIX および Solaris 版における Control Manager サーバへの登録の問題

InterScan のインストール後に Control Manager サーバへの登録に失敗することがあります。

次のコマンドを順に実行し、Trend Micro Management Infrastructure を再起動します。

1. `cd /opt/trend/TMI`
2. `./tmi stop`
3. `slibclean`
4. `./tmi start`

保留メールの問題

ここでは、さまざまな保留メールの問題の処理に関する情報を提供します。

一般的な保留メールの問題

保留されたメールの問題を迅速に解決するには、次の情報を収集し、判断します。

- Mail.box
- InterScan の一時ファイル (作業ディレクトリのパスは、設定データベースの [サーバ設定] 画面で確認できます)
- SMDreal のデバッグファイル
- 実行中の SMDreal タスクの数

システムメールボックス内の保留メールの検索および配信

SMDreal タスクが手動で停止されたといった理由でメール検索タスクが動作していない状況では、ウイルス検索されていないメールがシステムメールボックス (mail.box) 内に滞留する場合があります。

このような場合には、システムメールボックスを手動で検索し、保留メールが配信されるようにします。

システムメールボックス内の保留メールを検索し配信するには

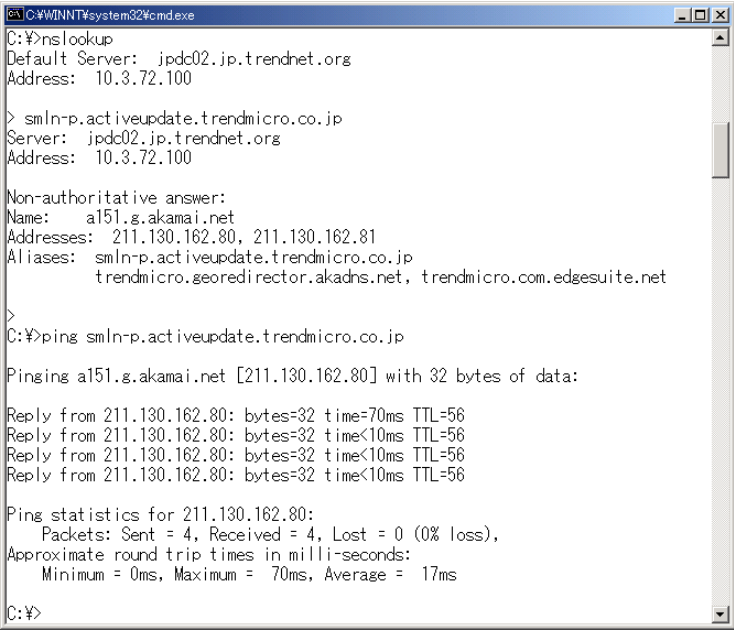
1. SMDreal サーバタスクをロードし、ステータスが「idle」になっていることを確認します。
2. [処理] → [手動データベース検索] → [検索するデータベース] の順にクリックし、mail.box をリストに追加します。
3. [ScanNow] ボタンをクリックします。または、Domino コンソールから smddbs タスクをロードします。システムメールボックス内のすべてのメッセージが検索され、保留されていたメールが配信されます。

注意：システムメールボックスの手動検索には、その時点でアクティブなメール検索ポリシー内のルールが適用されます。

アップデートの問題

コンテンツセキュリティコンポーネント (206 ページを参照) をダウンロードするようにダウンロード元を設定 (198 ページを参照) したにもかかわらず、最新コンポーネントをダウンロードできない場合、設定したダウンロード元に応じて次の手順を実行し、問題の原因を調べてください。

- [その他のインターネット上のサーバ] が選択されている場合は、最新コンポーネントの置かれているフォルダに適切なデジタル署名ファイル (*.sig) が存在することを確認してください。デジタル署名ファイルが存在しない場合、コンポーネントのダウンロードおよびアップデートは失敗します。
- [トレンドマイクロのアップデートサーバ] が選択されている場合は、Domino サーバからトレンドマイクロのアップデートサーバへの接続をチェックします。
 - a. nslookup を使用し、Domino サーバがトレンドマイクロのアップデートサーバの完全修飾ドメイン名 (FQDN) を解決できることを確認します。
 - b. Domino サーバから
<http://smln-p.activeupdate.trendmicro.co.jp/activeupdate/japan> に ping コマンドを実行します。



```

C:\WINDOWS\system32\cmd.exe
C:\>nslookup
Default Server: jpdco2.jp.trendnet.org
Address: 10.3.72.100

> smln-p.activeupdate.trendmicro.co.jp
Server: jpdco2.jp.trendnet.org
Address: 10.3.72.100

Non-authoritative answer:
Name: a151.g.akamai.net
Addresses: 211.130.162.80, 211.130.162.81
Aliases: smln-p.activeupdate.trendmicro.co.jp
          trendmicro.georedirector.akadns.net, trendmicro.com.edgesuite.net

>
C:\>ping smln-p.activeupdate.trendmicro.co.jp

Pinging a151.g.akamai.net [211.130.162.80] with 32 bytes of data:

Reply from 211.130.162.80: bytes=32 time=70ms TTL=56
Reply from 211.130.162.80: bytes=32 time<10ms TTL=56
Reply from 211.130.162.80: bytes=32 time<10ms TTL=56
Reply from 211.130.162.80: bytes=32 time<10ms TTL=56

Ping statistics for 211.130.162.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 70ms, Average = 17ms

C:\>
    
```

図 12-1. Domino サーバとトレンドマイクロのアップデートサーバ間の接続確認

- c. ポート 80 でトレンドマイクロのアップデートサーバに telnet 接続し、Domino サーバが HTTP 経由で接続できることを確認します。
 - d. <http://smln-p.activeupdate.trendmicro.co.jp/activeupdate/japan/server.ini>にアクセスして、server.ini ファイルをダウンロードできることを確認します。
- Domino コンソールをチェックし、SMDupd からエラーメッセージが返されるかどうかを確認します。

前述の措置を実行してもコンポーネントをアップデートできない場合は、SMDupd デバッグを有効にし（「InterScan タスクのデバッグ」を参照）、トレンドマイクロのテクニカルサポートにお問い合わせください。

予約検索 / アップデートの問題

スケジューラが予約時間中に起動しなかった場合は、InterScan の予約検索 / アップデートを再実行できません。この問題の回避策は次のとおりです。

1. **Notes.ini** で、スタートアップサーバタスクとして smddbs/smdupd を追加します。
2. [予約検索]/[予約アップデート] の設定で指定されている設定を使用して [手動検索]/[予約アップデート] の設定を指定します。

夜間のバックアップなどで、Domino サーバの再起動が行われると、smddbs/smdupd は予約検索 / アップデートと同じ検索 / アップデートタスクを実行します。

破損した InterScan データベースの修復

なんらかの原因で InterScan データベースが破損した場合は、データベースに対して整合性チェックを実行して修復を試みてください。整合性チェックを実行するには、Domino サーバコンソールで次のコマンドを実行してください。

```
load fixup {database}
```


たとえば、設定データベース (smcon.nsf) を修復するには、Domino サーバコンソールで次のコマンドを実行します。

load fixup smd/smconf.nsf

この手順でデータベースを修復できない場合は、データベースを再作成する必要があります (274 ページを参照)。ただし、データベースを再作成した場合、現在のデータベースに保存されている設定は失われます。

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

なんらかの原因で InterScan データベースが破損し、修復不能になった場合は、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、元の設定内容は復元されません。そのため、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、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た後、他の 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、次のディレクトリに置きます。
 - Domino R4 の場合 : Notes\Data
 - Domino R5/6 の場合 : Lotus\Domino\Data
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、118 ページの「InterScan データベースへのアクセス権およびロールの定義」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] → [データベース] → [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] のリストボックスを開きます。
6. リスト内の該当するサーバをクリックし、[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 のインストール中に使用した ID をテンプレートファイルの署名に使用していない場合は、この ID で新しいデータベースに署名します。

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、SMDdb、SMDmon 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 {scan task} quit  
load {scan task} -debug {level}
```

{level} 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： *.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くことをお勧めします。

- b. 次のパラメータを notes.ini の最後のエントリとして追加します。

```
SMDMDEBUG=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 3 つ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。

{servertaskname}_{yyyymmdd}.dbg

各項目の説明は次のとおりです。

{servertaskname} 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
- Linux/Solaris/AIX: smdreal_20040211.dbg
- i5/OS、OS/400: SMDREAL_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: SMDEXT.dbg
- Extension Manager フィルタタスク (SMDEMF): SMDEMF.dbg
- InterScan データベースセットアップ: <Domino データ>\SMDTemp\dbsetup.log
- InterScan データベース移行: <Domino データ>\SMDTemp\dbmigrate.log

デバッグファイルはすべて、Domino データディレクトリ内の \SMD\SMDtemp\ フォルダに保存されます。

InterScan 用 Control Manager エージェントのデバッグ

注意: i5/OS および OS/400 プラットフォーム向け製品では、Control Manager との連携機能は提供されません。次の手順は、i5/OS および OS/400 以外のプラットフォーム上で InterScan をお使いの場合に参照してください。

InterScan 用 Control Manager エージェントをデバッグするには、entity.cfg を変更します。

ヒント: Control Manager の設定ファイル (*.xml または *.cfg 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、entity.cfg のバックアップを作成しておくことをお勧めします。

InterScan 用 Control Manager エージェントをデバッグするには

1. Domino データディレクトリにある entity.cfg をテキストエディタで開きます。

2. LOG_level パラメータを探し、その値を変更します。設定可能な値は次のとおりです。

レベル	説明
0	詳細なデバッグ情報を表示
2	エラーメッセージのみを表示

3. LOG_filename パラメータを探し、その値をデバッグログのファイル名に変更します。
4. entity.cfg を保存して閉じます。

LOG_filename に指定したファイル名を使用して、Control Manager エージェントのデバッグログが <root>\Program Files\Trend\Common\TMI\DbgLog フォルダに作成されます。

デバッグログの収集

InterScan が正常に動作しないなどの不測の事態が発生した場合は、トレンドマイクロのテクニカルサポートよりデバッグログの収集をお願いする場合があります。

Domino のデバッグログを収集するには

Domino データディレクトリ内に生成された NOTES.RIP をチェックします。

InterScan のデバッグログを収集するには

InterScan のサポートツールを起動します。次のいずれかを実行します。

- Domino サーバコンソールを使用し、次のコマンドを実行します。

load SMDSupp

- Windows エクスプローラ（Windows プラットフォーム上）を使用し、次のファイルをダブルクリックします。<root>:\Lotus\Domino\nSMDSupp.exe

- Linux のコンソールまたは Solaris の bash ターミナルから、次を実行します。

注意： Domino サーバのインストールに使用したアカウントを使用してログオンしてください。他のアカウントでログオンした場合は、エラーメッセージが表示され、サポートツールを起動できません。

- a. 次のコマンドを順に実行します。

```
# export LD_LIBRARY_PATH={Notes path}:{InterScan path}/program/latest
# export Notes_ExecDirectory={Notes path}
```

各項目の説明は次のとおりです。

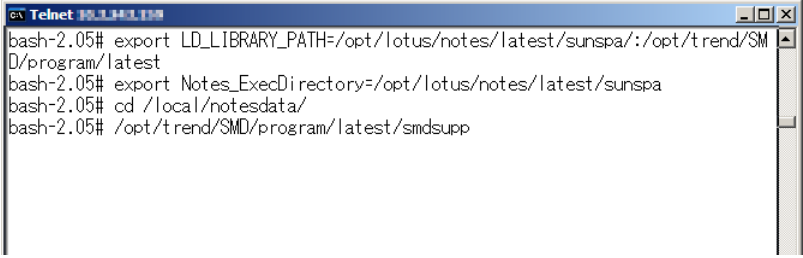
- {Notes path} は、Domino プログラムディレクトリの絶対パスです。
Linux の例： /opt/lotus/notes/latest/linux
Solaris の例： /opt/lotus/notes/latest/sunspa
- {InterScan path} には、InterScan のインストールディレクトリを指定します。
例： /opt/trend/SMD

- b. notes.ini のあるディレクトリに移動します。例： /local/notesdata

- c. InterScan のサポートツールを起動するには、次のコマンドを実行します。

```
# {InterScan path}/program/latest/smdsupp
```

コマンドの実行例については、図 12-2 を参照してください。



```
bash-2.05# export LD_LIBRARY_PATH=/opt/lotus/notes/latest/sunspa/:/opt/trend/SMD/program/latest
bash-2.05# export Notes_ExecDirectory=/opt/lotus/notes/latest/sunspa
bash-2.05# cd /local/notesdata/
bash-2.05# /opt/trend/SMD/program/latest/smdsupp
```

図 12-2. Solaris の bash ターミナルによる SMDsupp の実行

- i5/OS または OS/400 のメインメニュー（i5/OS および OS/400 プラットフォーム上）から次の CL コマンドを実行します。

- a. **chgcudir** を実行すると、notes.ini のあるディレクトリに移動します。例： /local/notesdata
- b. **ADDLIB LIB(QNOTES)**
- c. **ADDLIB LIB(QDOMINOxxx)**
xxx は、Domino 6.0.3 以降のバージョンです。
- d. **call trendmicro/smdsupp**

このツールにより、サーバタスクのデバッグログ、notes.ini、サーバのメールボックス、log.nsf および smconf.nsf が収集され、次のような命名規則で zip ファイルに保存されます。

SMDSuppyyyy-mm-dd.zip

このファイルは、Domino データディレクトリの \SMD\SMDtemp\ フォルダの下に置かれます。

注意： サポートツールにより、収集されたログはパスワード付きの圧縮ファイルに格納されます。収集されたログの内容を確認する場合は、パスワード「trendsmid」を使用して解凍してください。

InterScan のエラーメッセージについて

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: Unable to create message queue. Restart Domino server.	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: Unable to initialize common message. Unload and then reload SMDreal.	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: Unable to initialize scan engine. Check the scan engine and pattern file.	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 にポリシー関連文書が格納されていません。	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 でポリシーを作成し、smdreal を再ロードします。
SMDreal: Missing Extension Manager in notes.ini. Re-install ScanMail.	InterScan のインストールで、正しくないインストールパッケージを使用しました。または、InterScan が手動でアンインストールされました。	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。
SMDreal: Invalid Activation Code. Activate ScanMail via the Configuration Database and then reload SMDreal.	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。	[設定データベース] → [管理] → [製品ライセンス] → 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。「アクティベーションの実行」を参照してください。

メッセージ	原因	対処方法
SMDreal: The evaluation period has expired. Obtain a Registration Key and then activate ScanMail.	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ています。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: Unable to load policy. Check Configuration Database and then reload SMDreal.	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: Unable to load Message Database. Check smmsg.nsf and then reload SMDreal.	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: Invalid database list settings. Check the database list in the Manual or Scheduled scan rule setting.	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。	リアルタイム検索、予約検索、または手動検索の [検索するデータベース] リストをチェックします。複数のエントリはセミコロンで区切ります。
SMDreal: Unable to read Domino directory. Check server status.	Domino サーバの完全修飾ドメイン名 (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。
SMDreal: Cannot open database {database name}. Check the database name in the Configuration Database.	InterScan がデータベース内で特別な文書を検索しようとしたが、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。

メッセージ	原因	対処方法
SMDdbs: Cannot read Database Scan settings. Check Configuration Database.	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 チェックします (「データベース のリアルタイム検索ルールの作 成」を参照)。
SMDupd: Unable to run multiple SMDupd instances	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 スクを実行するように設定しま す。
SMDupd: Invalid parameter	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 (「手動データベース検 索の実行」を参照) または予約 アップデートルール (「アップ デートの実行」を参照) を チェックします。
SMDupd: Unable to initialize the update task	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: Unable to set up connection. Check network connection. Refer to ScanMail Help > Troubleshooting section for details.	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 チェックします。詳細について は、<InterScan のインストール 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: Unable to download components. Check server status or refer to ScanMail Help > Troubleshooting section for details.	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 のインストールパス>\AU_Log\TmuDump.txt を参照してください。
SMDupd: Unable to update component(s), the Activation Code already expired.	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: Unable to update to the latest version. Refer to ScanMail Help > Troubleshooting for details.	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チェックします。 詳細については、<InterScan のインストールパス>\AU_Log\TmuDump.txt を参照してください。
SMD Loader: The executable file exceeds the allowable maximum size {maximum size}	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: Unable to find the latest program directory	notes.ini に ScanMailInstallPath が見つかりません。これは、インストールが不完全であったり、InterScan ファイルが手動で削除されたために発生します。	InterScan を再インストールします。または、notes.ini にある ScanMailInstallPath パラメータとその値を修正します。

メッセージ	原因	対処方法
SMD Loader: Unable to browse the latest program directory {パス}	無効なパスまたはディレクトリが ScanMailInstallPath で指定されています。	InterScan を再インストールします。または、notes.ini にある ScanMailInstallPath パラメータとその値を修正します。
SMD Loader: Unable to load dynamic library "%s"	ダイナミックライブラリをロードできません。これは、そのファイルまたは依存するファイルがないか破損している、またはそのファイルに対する十分な権限がないために発生します。	InterScan を再インストールします。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。
SMDsch: Unable to start the scheduled task "%s"		

製品サポート情報

Trend Micro InterScan for Domino (以下、InterScan) 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。

この章で説明する項目は次のとおりです。

- 288 ページの「サポートサービスについて」
- 289 ページの「製品 Q&A のご案内」
- 290 ページの「セキュリティ情報」
- 291 ページの「ウイルス解析サポートセンター「TrendLabs」」

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「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、「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、契約満了前に必ず更新してください。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。

http://esupport.trendmicro.co.jp/supportjp/supportcentral/supportcentral_adv_ja.do

The screenshot displays the Trend Micro Product Q&A website. The top navigation bar includes links for Home, Products/Services, Purchase Information, Support (active), Security Information, Partners, and Company Information. The left sidebar contains a list of support-related links. The main content area is titled '製品Q&A' and includes a search section with a text input field for keywords, a dropdown for search scope (set to '全文'), and other filters like '製品' and 'バージョン'. A search button is located at the bottom right of the search section.

図 13-1. 製品 Q&A の Web サイト

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

セキュリティ情報の入手先

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://www.trendmicro.co.jp/vinfo/>

管理コンソールからセキュリティ情報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ウイルスデータベース検索サイトにアクセスして、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://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp>

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/supform.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。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 800 名以上 (2006 年 1 月現在) のスタッフがセキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客様に提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネジメントの英国規格 BS7799 (フィリピン) を取得しています

Domino 環境での脅威について

Trend Micro InterScan for Domino 3.0 (以下、InterScan) 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、Domino 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。

- 294 ページの「不正プログラムの概要」
- 297 ページの「Notes 環境での不正プログラムの拡大」

不正プログラムの概要

不正プログラムとは、ユーザが許可しない動作を実行するあらゆるプログラムを指します。ウイルスは不正プログラムの一形態です。その他の不正プログラムには、トロイの木馬、ワーム、バックドア、サービス拒否 (DoS) 攻撃エージェント、ジョークプログラムのほか、不正コードの小さなカテゴリがいくつかあります。

ウイルスは不正プログラムの一部に過ぎません。「不正」という言葉には、ユーザが認識できない動作や、意図しない動作を実行するという意味があります。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結び付けられることがしばしばあります。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。

実際のところ、不正プログラムというのが、不正コードを説明するには最適な言葉なのです。不正プログラムには、次のような多くのサブカテゴリがあります。

- 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。

- ファイル感染型ウイルス

ファイル感染型ウイルスは、DOS ウイルス、Windows ウイルス、マクロウイルス、不正スクリプトなど、さまざまな種類があります。これらは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、すべて共通の特徴を持っています。

- ブート感染型

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 98、Windows 2000 などの Windows OS では Windows スクリプトホストが利用可能なため、Windows エクスプローラから *.vbs ファイルまたは *.js ファイルをダブルクリックするだけでウイルスが起動します。

不正スクリプトの特徴は、アセンブリ型のプログラミング知識を必要とする他のプログラミングバイナリウイルスと異なり、ウイルス作成者が不正スクリプトをテキストでプログラミングできる点です。不正スクリプトは高度なプログラミングを必要とせず、可能なかぎ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、ファイル感染や大量メール配信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、元のコードを変更し、異なる件名やメール本文で感染を広げるコピーが検出されました。

これらはどのような種類であれ、基本的な仕組みは同じです。ウイルスには、明瞭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、コンピュータを制御するためになん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にも注意してください。この種類のウイルスは、異なるプラットフォーム (Windows と Linux など) の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を他のコンピュータシステムにコピーして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感染させる必要はありません。ワームは、Microsoft Outlook などのメールおよびアプリケーションを利用して感染を拡大することがよくあります。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ます。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あります。

トロイの木馬

トロイの木馬は、無害に見えるだけでなく、興味を引くような形態 (ゲームやグラフィックアプリケーションなど) のソフトウェアに潜む、破壊的なプログラムです。トロイの木馬には、破壊的なペイロードがない代わりに、システムやネットワーク全体のセキュリティを脅かすルーチンを持つものがあります。この種のトロイの木馬は、バックドア型と呼ばれることがあります。

トロイの木馬は、増殖しない不正プログラムです。自身で増殖することはせず、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で感染を拡大します。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、普通の実行可能プログラムで、通常悪意はありません。ウイルス作成者は、ユーザをからかう目的でジョークプログラムを作成します。ジョークプログラムには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データの損失につながる操作（古いバックアップからのデータ復元、ドライブのフォーマット、ファイルの削除など）を、誤って実行してしまう恐れがあります。

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。たまたま、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。

Notes 環境での不正プログラムの拡大

InterScan は、Notes クライアント環境で最も攻撃されやすい次の 3 つの侵入ポイントを常に監視し、保護します。

- メール送受信 — InterScan は、送受信されるメールのメッセージと添付ファイルをすべてリアルタイムで検索し、不正プログラムがユーザのシステムに侵入したり、顧客など他者のシステムに感染したりすることを防ぎます。
- クライアントによるデータベースアクセス — InterScan は、データベースファイルの変更をリアルタイムで監視し、ウイルスがデータベース文書内に保存されることを防ぎます。

- 複製 — InterScan は、Notes のデータベースレプリケートで変更されたファイルをすべてリアルタイムでチェックし、他の Notes サーバからウイルスが複製されることを防ぎます。

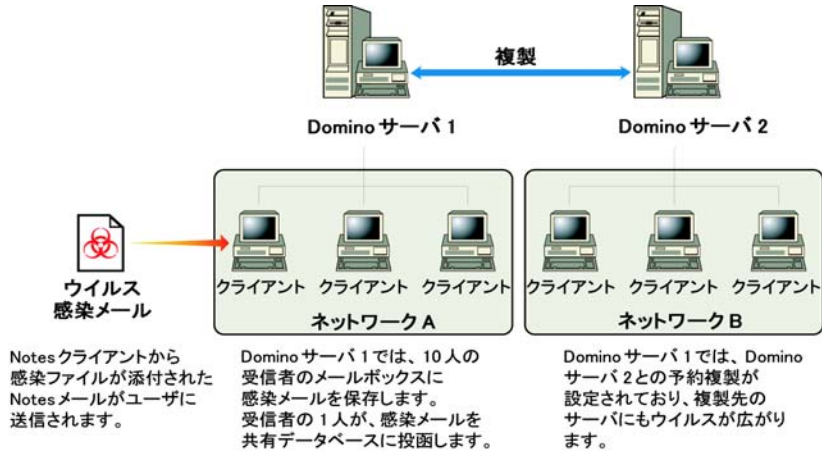


図 A-1. Notes 環境でのウイルス感染文書の拡大

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 の検索については、「検索の種類」を参照してください。

Control Manager エージェントの チェックリスト

この付録に示されている Trend Micro Control Manager (以下、Control Manager) エージェントのチェックリストを使用して、該当するシステム情報を記録します。将来、この情報が必要になることがあります。

必要な情報	例	設定値
Control Manager サーバ のユーザ ID	root	
公開鍵の場所	<Domino データ>\E2EPulic.dat	



root 権限の Control Manager アカウントの代わりに、どのアカウントを使用しても Control Manager エージェントをインストールできますが、削除されることのない root アカウントの使用をお勧めします。エージェントのインストール時に指定された Control Manager アカウントが削除されると、製品を管理できなくなるためです。

製品名	管理者レベルのアカウント	IP アドレス	ホスト名
例) InterScan	Admin	10.225.225.225	PH-antivirus

ファイルおよびフォルダー一覧

付録 D には、Trend Micro InterScan for Domino 3.0 (以下、InterScan) と Trend Micro Control Manager (以下、Control Manager) 3.5 のファイルとフォルダ構造のリストを記載しています。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。

インストールログとアンインストールログのリストについては、268 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場所」を参照してください。

Windows サーバにインストールされるファイル

表 C-C-1 と表 C-C-2 は、Windows サーバに InterScan と Control Manager エージェントが正常にインストールされたときに作成されるファイルのリストです。

ファイル / フォルダ	説明
... \Lotus \Domino nSMDext.dll nSMDemf.exe nSMDreal.exe nSMDsch.exe nSMDmon.exe nSMDdbf.exe nSMDupd.exe nSMDsupp.exe ndbsetup.exe nsmlnredID.dll ndbmigrate25.exe ndbmigrate26.exe smd.ini	InterScan ロード、フィルタ、Extension Manager、dbsetup、および InterScan の設定に関連するファイル
... WINNT \smdsys.ini	InterScan for Domino の主要な設定ファイル
... \Program Files \Trend Micro \ScanMail for Domino	InterScan for Domino のインストールフォルダ
... \engine	スパムメール検索エンジンとウイルス検索エンジンのフォルダを格納
... \engine \tmase	スパムメール検索エンジンを格納
... \engine \vsapi	ウイルス検索エンジンを格納
... \pattern	スパムメール検索エンジンとウイルス検索ルール / パターンのフォルダを格納
... \pattern \tmase	スパムメール判定ルールを格納
... \pattern \vsapi	ウイルスパターンファイルを格納

表 C-1. InterScan のファイルとフォルダ (Windows 版)

ファイル/フォルダ	説明
...\program	InterScan の Readme ファイル、およびプログラムファイルと設定ファイルのフォルダを格納
...\program\V3.#.#.####	InterScan のプログラム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
...\Lotus\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

表 C-1. InterScan のファイルとフォルダ (Windows 版)

ファイル/フォルダ	説明
...WINNT\cmasys.ini	Control Manager エージェントの主要な設定ファイル
...\Program Files\Trend Micro\ScanMail for Domino\CMAgent	Control Manager エージェントのインストールフォルダ。Control Manager エージェントのプログラムと設定ファイルを格納
...\Program Files\Trend Micro\ScanMail for Domino\CMAgent ¥ Uninstall	Control Manager エージェントのアンインストールプログラムを格納

表 C-2. Control Manager エージェントのファイルとフォルダ (Windows 版)

Linux/Solaris/AIX サーバにインストールされるファイル

表 C-C-3 と表 C-C-4 は、Linux/Solaris/AIX サーバに InterScan と Control Manager エージェントが正常にインストールされたときに作成されるファイルのリストです。

ファイル/フォルダ	説明
/etc/smdsys.ini	InterScan for Domino の主要な設定ファイル
/opt/trend/SMD/	InterScan for Domino のインストールフォルダ
.../engine/tmase	スパムメール検索エンジンを格納
.../engine/vsapi	ウイルス検索エンジンを格納
.../pattern/tmase	スパムメール判定ルールを格納
.../pattern/vsapi	ウイルスパターンファイルを格納
.../program	InterScan の Readme ファイル、およびプログラムファイルと設定ファイルのフォルダを格納
.../program/V3.#.#.####	InterScan のプログラムファイルと設定ファイルを格納 .## 先頭の 2 つの # はマイナバージョン .#### 末尾の 4 つの # はビルド番号
/opt/lotus/notes/latest/<OS の名前 > ...smddb ...smddbsh ...smdemf ...smd.ini ...smdmon ...smdreal ...smdsch ...smdsupp ...smdupd ...libsmdext.so ...libsmldnredid.so	次のいずれかの <OS の名前> がある Domino プログラムディレクトリの下に InterScan の設定ファイル、プログラムファイル、およびデータベースファイルを格納 Linux: linux Solaris: sunspa AIX: ibmpow

ファイル / フォルダ	説明
/local/notesdata/smd	InterScan のデータベースとテンプレートを格納
/local/notesdata/smdtemp	Setup dbsetup.log、および InterScan の検索タスクで使用する一時ファイルを格納

表 C-3. InterScan のファイルとフォルダ (Linux 版 /Solaris 版 /AIX 版)

ファイル / フォルダ	説明
/etc/cmasys.ini	Control Manager エージェントの主要な設定ファイル
/opt/trend/SMD/CMAgent	Control Manager エージェントのインストールフォルダ。Control Manager エージェントのプログラムファイルと設定ファイルを格納
.../CMAgent/Uninstall	Control Manager エージェントのアンインストールプログラムを格納
.../CMAgent/temp	一時ファイルを格納
Entity.cfg	Domino data フォルダ下に保存される、Control Manager エージェントの設定ファイルおよび一時ファイル
Entity.ini	Control Manger エージェントの実行時に使用するパラメータを格納する一時ファイル
Entity.tmp	Control Manger エージェントの実行時に使用するパラメータを格納する一時ファイル
/opt/trend/TMI	Trend Micro Management Infrastructure (TMI) のインストールフォルダ。TMI のプログラムファイルと設定ファイルを格納

表 C-4. Control Manager エージェントのファイルとフォルダ (Linux 版 /Solaris 版 /AIX 版)

i5/OS および OS/400 サーバにインストールされるファイル

表 C-C-5 は、i5/OS または OS/400 サーバに InterScan と Control Manager エージェントが正常にインストールされたときに作成されるファイルのリストです。

ファイル/フォルダ	説明
/etc/smdsys.ini	InterScan for Domino の主要な設定ファイル
/qibm/userdata/trend/smd/	InterScan for Domino のインストールフォルダ
.../engine/tmase	スパムメール検索エンジンを格納
.../engine/vsapi	ウイルス検索エンジンを格納
.../pattern/tmase	スパムメール判定ルールを格納
.../pattern/vsapi	ウイルスパターンファイルを格納
.../program	InterScan の Readme ファイル、およびプログラムファイルと設定ファイルのフォルダを格納
./V3.##.####	InterScan のプログラムファイルと設定ファイルを格納 .## 先頭の 2 つの # はマイナバージョン .#### 末尾の 4 つの # はビルド番号
/QIBM/ProdData/LOTUS/NOTES または /QIBM/ProdData/LOTUS/Domino### ...smd.ini ...smdemf.pgm ...smdreal.pgm ...smdsupp.pgm ...smddbs.pgm ...smdmon.pgm ...smdsch.pgm ...smdupd.pgm ...dbmigrate26.pgm ...dbsetup.pgm	Domino 6.0.3. より以前のバージョンでの使用 ### は、Domino 6.0.3 以降のバージョンです。 Domino プログラムディレクトリの下に InterScan の設定ファイル、プログラムファイル、およびデータベースファイルを格納
/local/notesdata/smd	InterScan のデータベースとテンプレートを格納

ファイル / フォルダ	説明
/local/notesdata/smdtemp	Setup dbsetup.log、および InterScan の検索タスクで使用する一時ファイルを格納

表 C-5. InterScan のファイルとフォルダ (i5/OS または 400 サーバ版)

バージョン 2.6 および 3.0 の機能比較

次の表は、Trend Micro InterScan for Domino 3.0、および旧バージョンの InterScan for Lotus Notes 2.6 の機能を比較したものです。

機能	バージョン 2.6	バージョン 3.0
インストール / サポートプラットフォーム		
Domino 7.0	○	○
Domino 6.5	○	○
Domino 6	○	×
Domino R5	○	×
クラスタサーバの信頼 (サーバごとのタスクのフルサポートと信頼)	×	○
パーティションサーバのサポート	○	○
複数のパーティションへの同時インストール	×	○
すべてのプラットフォームでのサイレントインストールのサポート	×	○
インストール時の複製の設定	×	○
インストール時のアクセス制御リストの設定	×	○
インストール時のデータベース署名	○	○
異なる ID/ パスワードを使用してのデータベース署名、または署名の省略	×	○
プラットフォームにまたがるデータベースの複製の設定	×	○
サポートされる Domino アプリケーション		
Lotus Domino データベース (.nsf)	○	○

表 D-1. バージョン 2.6 および 3.0 の機能比較

機能	バージョン 2.6	バージョン 3.0
Lotus Domino Web Access (旧 iNotes Web Access)	×	○
製品のアクティベーション		
シリアル番号の使用	○	×
2つのシリアル番号 (InterScan 用と、オプションで eManager 用)	○	×
トレンドマイクロの新しい製品登録システム	×	○
アクティベーションコードの使用	×	○
検索 (一般)		
マルチスレッドでの検出時の処理	×	○
マルチスレッドでの検索タスク	×	○
アドウェアとスパイウェアに対する個別の処理	×	○
メール検索		
リアルタイム検索	○	○
メール送信者 / 受信者に基づくメール検索ルール	×	○
除外設定による特定のユーザ / グループに対する処理の除外	×	○
スケジュールに基づく設定の変更	×	○
ウイルス検出時のウイルス駆除	○	○
ウイルス検出時の処理の設定	○	○
多重圧縮ファイルの検索 (設定データベースからの圧縮階層数の指定)	○	○
MIME/HTML メール本文のスクリプト検索	○	○
不正スクリプト、ホットスポット、URL の検索	○	○
署名ベースの検索	○	○
再検索を回避するための信頼するサーバの設定	○	○
埋め込み OLE オブジェクトの選択的な検索	○	○

表 D-1. バージョン 2.6 および 3.0 の機能比較 (続き)

機能	バージョン 2.6	バージョン 3.0
アドウェア検出		
ウイルス検出時の処理の設定	×	○
スパイウェア検出		
ウイルス検出時の処理の設定	×	○
メール配信 / 使用帯域幅の管理		
承認のための転送	×	○
設定データベースからのファイルタイプのグループ化	×	○
実際のファイルタイプによる添付ファイルに対する処理 (個々のファイルタイプ)	×	○
Microsoft Office のマクロに対する処理の設定	×	○
拡張子またはファイル名による添付ファイルに対する処理	○	○
実際のファイルタイプによる添付ファイルに対する処理	○	○
Microsoft Office 文書からのマクロの除去	○	○
スケジュールに基づいたメールの遅延配信	○	○
サイズによるメールのブロック	○	○
メールへの低い優先度の設定	○	○
添付ファイルの実際のファイルタイプに基づくメールのブロック	○	○
添付ファイルの拡張子またはファイル名に基づくメールのブロック	○	○
コンテンツフィルタ		
件名の検索	○	○
メール本文内のテキストの検索	○	○
添付ファイル内のテキスト検索	○	○
スパムメールフィルタ		
ヒューリスティック技術の採用	×	○

表 D-1. バージョン 2.6 および 3.0 の機能比較 (続き)

機能	バージョン 2.6	バージョン 3.0
許可する送信者 / ブロックする送信者のサポート	×	○
フィルタのレベルの設定	×	○
ルールファイルの使用	○	○
データベース検索		
リアルタイム検索	○	○
予約検索	○	○
手動検索	○	○
複数のリアルタイム検索設定の、時間帯による使い分け	×	○
リアルタイム検索におけるスクリプトフィルタのサポート	○	○
指定期間内での予約検索	×	○
複数の異なる設定による予約検索のサポート	×	○
終了しなかった検索の再開	×	○
予約検索におけるスクリプトフィルタのサポート	○	○
設定データベースによる予約検索スケジュールの設定	×	○
管理		
R5/6 Notes Administrator または Notes クライアントとの統合	○	○
Web インタフェースからのリモート管理	○	○
Notes クライアントからのリモート管理	○	○
トレンドマイクロの新デザイン標準を採用したユーザインタフェース	×	○
設定データベースからのサーバステータスの監視	×	○
サーバタスクの監視	×	○
タスクステータスの監視	×	○
複数のサーバおよびサーバグループ間でのウイルス対策設定の共有	×	○

表 D-1. バージョン 2.6 および 3.0 の機能比較 (続き)

機能	バージョン 2.6	バージョン 3.0
ユーザが定義したルールのサポート	×	○
ユーザ / グループに基づいたルールの定義	×	○
ポリシーベースのサーバ設定	×	○
Notes インタフェースから設定可能なロールベースのアクセス制御	×	○
サポート情報収集ツール	×	○
コンポーネントのアップデート		
手動アップデート	○	○
コンポーネントの選択と予約アップデートの繰り返し設定	×	○
トレンドマイクロのアップデートサーバからのウイルスパターンファイルの自動アップデート	○	○
トレンドマイクロのアップデートサーバからの検索エンジンの自動アップデート	○	○
トレンドマイクロのアップデートサーバからのプログラムファイルの自動アップデート	×	○
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	○	○
アップデート後の製品の整合性チェック	×	○
通知オプション		
カスタマイズ可能な通知	×	○
Lotus Instant Messaging/Web Conferencing (Sametime) 経由での通知	×	○
送信者、受信者、管理者への通知	○	○
内部ユーザと外部ユーザへの異なる通知	○	○
リッチテキストメッセージの設定	○	○
MIME メールへの通知の挿入	×	○
添付ファイルが削除された場合のホットスポットの置換	×	○
メール件名へのスタンプの挿入	○	○

表 D-1. バージョン 2.6 および 3.0 の機能比較 (続き)

機能	バージョン 2.6	バージョン 3.0
Notes メール本文へのスタンプの挿入	○	○
メール本文へのスタンプの挿入	×	○
複数の検査証明 (ディスクレーマー) のサポート	×	○
メールが複数のサーバを通過する際の、1 つの検査証明の使用	○	○
検査証明の挿入位置の指定	×	○
隔離データベース		
隔離された項目の自動削除	○	○
隔離された項目の再送信	○	○
ログデータベース		
CSV 形式ファイルへの統計のエクスポート	×	○
ログの自動削除	○	○
感染メールの送信者の識別	○	○
感染ファイルの識別	○	○
受信者情報の記録	○	○
実行された処理の記録	○	○
グラフィカルな統計レポート	○	○

表 D-1. バージョン 2.6 および 3.0 の機能比較 (続き)

索引

英数字

Control Manager

- InterScan の管理 245
- InterScan 用のエージェント 242
- エージェント 242
 - 処理 242
- エンタープライズ版 240
- 機能 240
- サーバ 240
- 使用 244
- スタンダード版 240
- 大規模感染予防 243
- 大規模感染予防ポリシー 247

Control Manager エージェント

- インストール 90、94
- インストールの確認 110
- インストールの準備 91
- 公開鍵 92
- 公開鍵の入手 92

Domino 6 Web Administrator 193

Domino R5 117

E2EPublic.dat 92

EICAR 87

InterScan

- 3.0 へのアップグレード 39、90
- アクティベート 85、87
- インストール
 - サイレントモード 66
- インタフェース 114
- エラーメッセージ 281
- 概要 19、20
- 機能 22、23
- 機能比較 309
- 検索の種類 26
- コンポーネント 26、197
- サイレントモードでのインストール 66
- システム要件 40
- 通常モードでのインストール 44
- 通知 209
- データベース
 - 再作成 274
 - 修復 272
- 登録 87

バージョン 3.0 の新機能 12

配置計画 36

ログ 220

InterScan のアンインストール 250

自動 250

LocalDomainServers 152

Microsoft Excel 228

Misc

警告用画像 190

ServerProtect 85

sig 207

smadmR5.nsf 117

smquar.nsf 231

SMTP 190

smvlog.nsf 220

TrendLabs 291

Web アクセス 192

InterScan データベース 122

あ

アクセス制御リストのエントリ 194

アクティベーションコード

InterScan 85

スイート版 86

スタンダード版 86

体験版 85

アクティベーションの実行 86

アクティベート

InterScan 87

アップデート

アップデート元 206

ウイルス対策コンポーネント 199

コンテンツセキュリティコンポーネント 199

コンポーネントの選択 204

自動 200

手動 199

プロキシサーバの設定 208

アップデート元。「アップデート」を参照

アンインストール

InterScan 250

自動 250

InterScan 用 Control Manager エージェント 261

インストール

InterScan 35

インストールの確認

Control Manager エージェント 88、110

InterScan のインストール 85

- インストールのテスト 87
- インタフェース 114
- ウイルス 294
- ウイルス対策。「コンポーネント」を参照
- ウイルス対策製品 85
- ウイルスパターンファイル 198
- ウイルスログの削除
 - 手動 225
 - 予約 223
- エクスポート
 - グラフ 228
 - 統計 227
- エラーメッセージ 281
- か**
- 拡大 297
- 隔離データベース 231
- 隔離メッセージ
 - 再送信 232
 - 表示 231
- 隔離メッセージの再送信 232
- 管理コンソール 245
- キーワード 155
- 機能比較 309
- グラフ 227
- 警告
 - Control Manager ユーザ ID 102
 - 隔離文書の復元 233
 - 実行されていないメールタスク 191
 - メールの配信 191
- 警告用画像 190
- 検索エンジン 198
- 検索スケジュールの設定 176
- 検索制限 31、151
- 検査証明 175
- 検査証明の挿入 175
- 公開鍵 92
- 誤検出 157
- このマニュアルの対象読者
 - 対象読者 17
- コンテンツセキュリティ。「コンポーネント」を参照
- コンテンツフィルタ 154
 - キーワード 155
- コンポーネント 198
 - InterScan アプリケーション 199

- ウイルスパターンファイル 198
- 検索エンジン 198
- 署名ファイル。「ウイルスパターンファイル」も参照
- スパイウェアパターンファイル 198
- スパムメール検索エンジン 198
- スパムメール判定ルール 198
- ダウンロードできない 270
- プログラムファイル 199
- コンポーネントのアップデート 199

さ

- サーバイベント 188
- サーバイベントのモニタ 188
- サーバ設定 181
 - 概要 183
- サーバタスクモニタ 188
- 作業ディレクトリ 185
- 作成
 - キーワード 167
 - コンテンツフィルタ 164
 - サーバ設定ルール 184
 - ポリシー 130
 - ルール 136
- システム要件 40
- 受信メッセージ 152
- 手動 28
- 手動アップデート 199
- 手動検索 116、176、177
 - Domino サーバコンソール 176
 - 手動による停止 179
 - 設定データベース 177
 - 停止 179
- ジョークプログラム 297
- 署名ファイル 207
- 署名ファイル。「ウイルスパターンファイル」も参照
- 処理
 - 駆除可能なウイルス 161
 - 駆除不能なウイルス 161
 - その他の不正プログラム 161
 - 特定の脅威 161
- 新機能 26
- 信頼するクラスタサーバ 133
- 信頼するサーバ 190
- 推奨システム要件 44
- スパイウェアパターンファイル 198

スパムメール検索エンジン 198

スパムメール判定ルール 198

スレッド 190

製品版へのアップグレード 87
設定

 アップデート通知 216

 ウイルス検索 159

 検索スケジュール 176

 検索制限 162

 検索通知 216

 コンテンツフィルタ 164

 スクリプトフィルタ 172

 スパムメールフィルタ 156

 スレッド数 190

 タスクの表示 193

 データベースプロパティ 192

 転送オプション 174

 添付ファイルフィルタ 169

 メール検索ルールの一般的な設定 140

 メッセージフィルタ 163

その他のインターネット上のサーバ 207

その他の設定 189

 Domino ルーティングの無効化 191

 ウイルス対策済みの SMTP サーバおよび Domino
 サーバ 190

 警告用画像 190

 スレッドの検索 190

 タスクの除外 191

た

大規模感染予防サービス 243

大規模感染予防ポリシー 247

 期限切れの削除 248

 表示 247

ダウンロード元 206

タグ 211

タスクの除外 191

注意

 Domino R5 117

 EICAR 87

 Extension Manager 276

 InterScan スイート版 156

 InterScan データベースの再作成 274

 InterScan の手動削除 257

 Notes データベースのプロパティ 193

 TMI 97

 圧縮レベル 162

アップデートデータベースの複製 206

ウイルスパターンファイルの履歴 203

管理者宛ての通知 216

キーワード 167

クラスタの信頼 135

検索エンジンの条件 146

検索エンジンの履歴 203

検索時間 178

検査証明 175

検査証明の挿入 175

検査証明の名前 175

コンポーネントのダウンロード 217

コンポーネントのダウンロードの試行 217

自動駆除処理 173

自動削除 223、235

初期設定のポリシー 26、133

初期設定のポリシーの削除 133

新規ルールの作成 148

信頼するサーバ 190

製品版へのアップグレード 195

設定のコピー 131

体験版のアップグレード 195

ダウンロードのみ 206

ダウンロード元 206

通知テンプレート 212

デバッグレベル 276

添付ファイル名 171

パーティションサーバ 59

パターンファイルの条件 146

ヒント 116

フィルタ処理順序 151

複製スケジュール 62

プロキシサーバ 187

ポリシーの作成 131

マルチサーバ環境 220

優先度の低いメッセージのルーティング 141

予約アップデート通知 202

リッチテキストのホットスポット 173

履歴 203、204

ログ削除 223、235

論理演算子 166

通知 209

 アップデート実行 210

 アップデート通知 216

 概要 210

 カスタマイズ 211

 検索実行 210

 検索通知 216

- 設定 216
- タグ 211
 - フィルタベースのタグ 211
 - ルールベースのタグ 212
- テンプレート 216
- 配信 214
- タグ。「通知タグ」を参照
- 通知のカスタマイズ 211
- データベース 220
 - 隔離 231
 - カタログ 192
 - 再作成 274
 - 修復 272
 - ログ 220
- データベースの再作成 274
- [データベースを開く] ダイアログ 192
- デジタル署名 207
- デバッグ 275
 - Control Manager エージェント 277
 - InterScan タスク 275
 - 結果 276
 - レベル 276
- デバッグログ 276
 - Control Manager エージェント 278
 - Domino 278
 - InterScan 278
 - 収集 278
 - チェック 276
- デバッグログの収集 278
- デバッグログのチェック 276
- 統計 227
- 登録
 - InterScan 87
- トラブルシューティング 267
- トロイの木馬 296
- は**
- はじめに 11
- 破損した InterScan データベースの修復 272
- 表記規則 17
 - 文書 17
- 表示
 - 隔離メッセージ 231
 - グラフ 228
 - サーバ概要 182
 - 統計 227
- ヒント
- Domino の脅威 29
- InterScan データベースの表示 115
- InterScan による処理 138
- InterScan のパフォーマンス向上 138
- アップデートのトラブルシューティング 207
- アップデートの問題 207
- アドレスグループ 140
- キーワード 168
- キーワードのテスト 168
- 厳しいルール 140
- 脅威 29
- 検索とフィルタ処理 138
- コンテンツフィルタ 168
- コンポーネント 199
- コンポーネントのアップデート 199
- 削除されたライセンスプロファイル 196
- 条件 167
- 新規ルール 138
- 設定ファイルの変更 275、277
- 複数のデータベース 177
- メール検索ルールの作成 138
- メッセージ検索 138
- 最も厳しいルールの適用 140
- ライセンスプロファイル 196
- ルールの作成 136
- ルールの条件 136、167
- ルールの命名 140
- ルール名 140
- フィルタ 31、150
- フィルタ処理
 - コンテンツ 31、151
 - 順序 150
 - スクリプト 31、151
 - スパムメール対策 156
 - メッセージ 31、151
- 不正プログラム 294
 - ウイルス 294
 - スクリプト 295
 - ファイル感染型 295
 - ブート 295
 - 拡大 297
 - ジョークプログラム 294
 - トロイの木馬 294
 - ワーム 294
- 脅威。不正プログラムを参照
- プロキシサーバ
 - コンポーネントダウンロード 208
- プロキシサーバの設定 187

プロキシ。「プロキシサーバの設定」を参照

ヘルプ **115**

ヘルプへのアクセス **115**

変更

 サーバ設定ルール **184**

棒グラフ **16**

ポリシー

 概要 **29**

 計画 **32、128**

 作成 **130**

 変更 **132**

ま

メール検索 **27**

メール検索ルール **140**

 一般的な設定 **140**

メールスタンプ **213**

メッセージの転送 **174**

メッセージフィルタ **31、151**

メモリサイズ **186**

文字セット **189**

や

予約データベース検索 **28**

ら

リアルタイム検索 **27**

ルール **30**

 サーバ設定 **184**

 作成 **136**

 通知 **31**

 データベース検索 **30**

 データベースのリアルタイム検索 **142**

 メール検索 **30**

 予約 **176**

 予約アップデート **31**

 予約検索 **30**

ログ **220**

 ウイルスログの削除 **223**

 手動 **225**

 予約 **223**

 管理 **220**

わ

ワーム **296**

