

***e*TrustTM Antivirus Groupware Options**

ユーザガイド

7.1



Computer Associates®

G00502-1J

本書及び関連するソフトウェア プログラム(以下「本書」といいます。)は、お客様への情報提供のみを目的とし、Computer Associates International, Inc.(以下"CA")は本書の内容を予告なく変更、撤回することがあります。

CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、複製することはできません。本書は、CA が知的財産権を有する専有の情報であり、アメリカ合衆国及び日本国の著作権法並びに国際条約により保護されています。

上記にかかわらず、社内で使用する場合に限り、ユーザは本書の、合理的な範囲内の部数のコピーを作成できます。ただし CA のすべての著作権表示およびその説明を各コピーに添付することを条件とします。ユーザの認可を受け、ユーザが使用する本ソフトウェアのライセンスに記述されている守秘条項を遵守する、従業員、法律顧問、および代理人のみがかかるコピーを利用できます。

本書のコピーを作成する上記の権利は、本製品に対するライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、そのライセンスが終了した場合には、ユーザは CA に複製したコピーを返却するか、あるいは複製したコピーを破棄したことを文書で証明する責任を負います。

準拠法により認められる限り、CA は本書を現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対する不侵害についての黙示の保証を含むいかなる保証もしません。

また、本書の使用が直接または間接に起因し、逸失利益、業務の中断、営業権の喪失、業務情報の損失等いかなる損害が発生しても、CA は使用者または第三者に対し責任を負いません。CA がかかる損害について明示に通告されていた場合も同様とします。

本書及び本書に記載された製品は、該当するエンドユーザライセンス契約書に従い使用されるものです。

本書の制作者は Computer Associates International, Inc. です。

本書は、48 C.F.R. Section 12.212、48 C.F.R. Section 52.227-19 (c)(1) 及び (2)、または、DFARS Section 252.227.7013(c)(1)(ii)、または、これらの後継の条項に規定される「制限された権利」のもとで提供されます。

© 2004 Computer Associates International, Inc., One Computer Associates Plaza, Islandia, New York 11749. All rights reserved.

本書に記載された全ての製品名、サービス名、商号およびロゴはそれぞれ各社の商標またはサービスマークです。

目次

第 1 章: Exchange Option の紹介

Exchange Option の機能	1-1
メッセージング/グループウェア システムの理解	1-1
ネットワークと Exchange システムの保護	1-2
インストールに必要な条件	1-3
ハードウェアとソフトウェアの動作要件	1-3
インストールの手順	1-3
インストールのテスト	1-4

第 2 章: Exchange Option の使用法

リアルタイム スキャン	2-1
[リアルタイム メール オプションの設定]ダイアログ ボックスへのアクセス	2-1
スキャン オプションの使用法	2-2
スキャナ	2-2
検出	2-2
安全性レベル	2-3
ウイルスの処置	2-3
選択オプションの使用法	2-5
通常ファイル	2-6
圧縮ファイルのスキャン	2-6
プレスキャン ブロック	2-7
通知オプションの使用法	2-8
メッセージ送信者	2-8
メール システム管理者	2-9
返信用アドレス	2-9
Microsoft Exchange 2000 のオプションの使用法	2-9
メッセージの本文をスキャンする	2-10
事前スキャン	2-10
スキャンするスレッド数	2-10
スキャン タイムアウト	2-10
その他の各オプションの使用法	2-11
ログ サイズ	2-11

保存するバックアップ ログ数.....	2-11
ログの詳細レベル.....	2-12
システム イベント ログ.....	2-12
タイムアウト値.....	2-12
Exchange バックグラウンド スキャン.....	2-12

第 3 章: Lotus Notes/Domino Option の紹介

Lotus Notes/Domino Option の機能.....	3-1
メッセージング/グループウェア システムの理解.....	3-2
ネットワークと Lotus Notes/Domino Option システムの保護.....	3-2
インストールに必要な条件.....	3-3
ハードウェアとソフトウェアの動作要件.....	3-3
インストールの手順.....	3-3
インストールのテスト.....	3-3

第 4 章: Lotus Notes/Domino Option の使用法

リアルタイム メール オプションを使用した Lotus Notes/Domino Option のウイルス対策.....	4-1
スキャン オプションの使用法.....	4-2
スキャナ.....	4-2
検出.....	4-2
安全性レベル.....	4-3
ウイルスの処置.....	4-3
選択オプションの使用法.....	4-4
通常のコピー.....	4-5
圧縮ファイルのスキャン.....	4-5
プレスキャン ブロック.....	4-6
通知オプションの使用法.....	4-7
通知.....	4-7
カスタマイズ可能な警告メッセージ.....	4-8
カスタマイズ可能な警告メッセージの返信用アドレス.....	4-8

Exchange Option の紹介

eTrust™ Antivirus Option for Microsoft® Exchange Option (以下、「Exchange Option」)は、コンピュータ・アソシエイツのウイルス対策ソフトウェアと統合し、電子メール メッセージに添付された文書やフォルダ内で、ウイルスをスキャンします。このオプションは、感染した Microsoft Exchange の添付ファイルを自動的に修復します。Exchange Option はサーバを通過するすべてのメールをスキャンします。

Exchange Option は、Microsoft Exchange Server が常駐するサーバ上で稼働します。感染した電子メール添付ファイルを検出、修復、ブロックすることにより、感染が社内ネットワーク全体に広がることを防ぎます。

注: Exchange Option は、eTrust Antivirus 7.1 以降で動作します。

Exchange Option の機能

Exchange Option には、以下のような機能があります。

- **マクロ ウイルス アナライザ** – Word.Concept ウイルスや Excel Laroux ウイルスなど、急速に蔓延するマクロ ウイルスを検出し完全に除去します。添付文書をスキャンし、ウイルスを処理します。
- **ライブ スキャン** – メッセージングシステムを通常どおりに実行しながら、ユーザーの操作を妨げることなく、ウイルスをスキャンします。
- **簡単なオプション** – 検出オプションとログ オプションを簡単に指定できます(たとえば、感染ファイルの修復やログの詳細レベル)。

メッセージング/グループウェア システムの理解

Microsoft Exchange などの電子メッセージング システムは、今日の企業では情報伝達的手段として広く利用されています。また、メッセージング システムは多くの企業で、社内と社外の両方において情報や文書を共有する、必要不可欠な手段になっています。ところがこれらのシステムは、感染ファイルを取り込んで組織中に蔓延させる、セキュリティ上の盲点となってしまう可能性があり、データと生産性の両方が結果として危険にさらされてしまうおそれがあります。

ICSA® (International Computer Security Association) の調査によると、電子メール添付ファイルは最も一般的なウイルス感染源の 1 つです。マクロ ウイルス、ワーム、その他の悪意あるコードは、電子メールを媒体として侵入し、会社のシステムを少しずつ衰弱させます。

たとえば、Winword.Concept マクロ ウイルスと Melissa ウイルスが蔓延するまでに要した期間は、歴史上で最も最短でした。また、ICSA の別の調査では、検出された全ウイルスのうち 49%がマクロ ウイルスであると述べています。マクロ ウイルスは、Windows OS 上の Microsoft Word で使用される NORMAL.DOT テンプレート内に寄生します。Winword.Concept ウイルスが登場するまで、ウイルスのほとんどは、磁気メディアの実行可能領域 (つまりブート セクタ) またはファイル (.EXE、.COM、.BIN ファイルなど) にのみ寄生し感染していました。現在ではマクロ ウイルスが、ウイルスを拡散させる一般手段になっています。また、その他の有害なウイルスも蔓延しており、新種のウイルスは常に出現しています。

メッセージングシステムでは、ファイルが通常のファイルシステムとしてでなくデータベース形式で格納されているため、ウイルス対策製品において特殊な問題が生じます。ウイルス対策製品自体は、そのようなシステムをスキャンできません。ただし、Exchange Option には、データベースの障壁をくぐり抜けて Microsoft Exchange など、サーバベースのメッセージングシステムのスキャンと修復を完璧に実行する、独自の機能が提供されています。この機能によって、マクロ ウイルスやほかの悪意ある感染ファイルは、必ずしも企業のメッセージング/データベース システムへの脅威ではなくなります。

ネットワークと Exchange システムの保護

Exchange システムとネットワーク全体を新種のウイルスから確実に保護するには、以下を実行します。

- Exchange Option とウイルス対策ソフトウェアをインストールした後、すぐに最新のシグネチャ ファイルをダウンロードします。コンピュータ・アソシエイツでは常時、新種のウイルスを検出しシグネチャ ファイルをアップデートしています。このため、最新のシグネチャ ファイルを使用することで、最新の保護機能を確実に利用できるようになります。
- すべての実行ファイルを読み込み専用に変更します。これで実行ファイルが感染しにくくなります。
- フロッピー ディスクからファイルをコピーする前に、ディスクに対してウイルス スキャンを実行します。
- ウイルス スキャンが問題なく実行された後、コンピュータ・アソシエイツの BrightStor などのバックアップ ツールを使用して、ご使用のワークステーションのバックアップを実行します。この処理を実行すると、ファイルでウイルスが検出されて駆除できなくなった場合でも、バックアップしたファイルを使用できます。
- コンピュータ・アソシエイツのテクニカル サポートのサイト (<http://www.caj.co.jp/support>) を定期的に参照してください。
- 最新のウイルス情報を提供するコンピュータ・アソシエイツのオンライン ウイルス対策ニュースレター (無料) を購読することもできます。

インストールに必要な条件

インストールする前に、必要なソフトウェアとハードウェアが準備できていることを確認してください。また、ご使用の Exchange Option アカウントに、適切なユーザ権限を設定しておく必要があります。

ハードウェアとソフトウェアの動作要件

Exchange Option をインストールして使用するには、以下のソフトウェアとハードウェアが必要です。

- 以下の Windows オペレーティング システムがサポートされています。
 - Windows NT 4.0 (SP4 またはそれ以上のサービス パックを適用済み)
 - Windows 2000 Server ファミリ (SP1 またはそれ以上のサービス パックを適用済み)
 - Windows 2003 Server ファミリ
- 以下の Exchange Server がサポートされています。
 - Exchange Server 5.5 (SP3 および Hotfix (MSKB Q248838) またはそれ以上のサービス パックを適用済み)
 - Exchange 2000 (SP1 以上を適用済み)
 - Exchange 2003
- Exchange Server を実行中のマシンにインストール済みの eTrust Antivirus 7.1 以降
- Exchange Server に 1MB のディスク空き容量、2MB の空きメモリ、および Intel プロセッサ

インストールの手順

最初に、eTrust Antivirus 7.1 ソフトウェアのインストールを実行します。次に、Microsoft Exchange Option を Microsoft Exchange Server にインストールするために、CD-ROM を CD-ROM ドライブに挿入します。セットアップ ウィザードの指示に従ってインストールを完了してください。

ICF ファイルを使用してカスタマイズ可能なインストール

製品をインストールする前に、InXSetup.ICF ファイルを使用して、インストール オプションとデフォルトのリアルタイム設定を設定できます。あらかじめ設定することによって、インストール時にすべてのマシンで必ず同じリアルタイム ポリシーが適用されるため、1 つのイメージを複数のマシンに適用できます。

サンプルの InXSetup.ICF ファイルは、製品 CD-ROM に収録されています。使用可能な設定とオプションの詳細は、このファイルを参照してください。共有ドライブやバッチ プログラムからインストール プログラムを無人で実行するように選択した場合は、すべての設定が InXSetup.ICF ファイルから取得されます。サイレント セットアップは、以下のコマンドを使用して実行できます。

```
SETUP /s.
```

インストールのテスト

EICAR テスト標準を使用して、コンピュータ・アソシエイツ Email Option のインストールをテストできます。EICAR (European Institute for Computer Antivirus Research) が開発した EICAR 標準を使用すると、感染ファイルとして検出される、テスト用の未感染の電子メール添付ファイルを作成できます。

以下は、EICAR 標準 Antivirus テスト ファイルのサンプル コードです。このコード行をテキスト ファイルにコピーします。

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

テキスト ファイルを EICAR.COM という名前で保存します。ファイルのサイズは 69～70 バイト程度になります。

EICAR.COM ファイルを Microsoft Exchange の電子メールに添付します。コンピュータ・アソシエイツ電子メール オプションによって添付ファイルが検出され、スキャン結果ファイル (AV-ScanReport.txt) が電子メールに添付されます。

テストの実施後、EICAR.COM ファイルを削除します。

Exchange Option の使用法

この章では、Microsoft Exchange Option のリアルタイム スキャンの特徴と、電子メールやメールボックス データベースでの感染からシステムを保護する方法について説明します。このオプションは、通常のファイルに対して使用できるリアルタイム ウイルス対策機能を使って、ご使用の電子メール システムを保護します。

コンピュータ・アソシエイツのウイルス対策製品の管理者ビューから、電子メール オプションを管理する方法の詳細については、『管理者ガイド』を参照してください。

リアルタイム スキャン

Exchange Option は、システムトレイ内の[リアルタイム]オプションを使用したリアルタイム スキャンと設定変更をサポートします。

[リアルタイム メール オプションの設定]ダイアログ ボックスへのアクセス

[リアルタイム オプションの設定]ダイアログ ボックスにアクセスするには、以下の操作を実行します。

1. システムトレイにある、コンピュータ・アソシエイツのウイルス対策ソフトウェアのアイコンを右クリックします。
2. ポップアップ メニューの[メール オプション]を選択します。

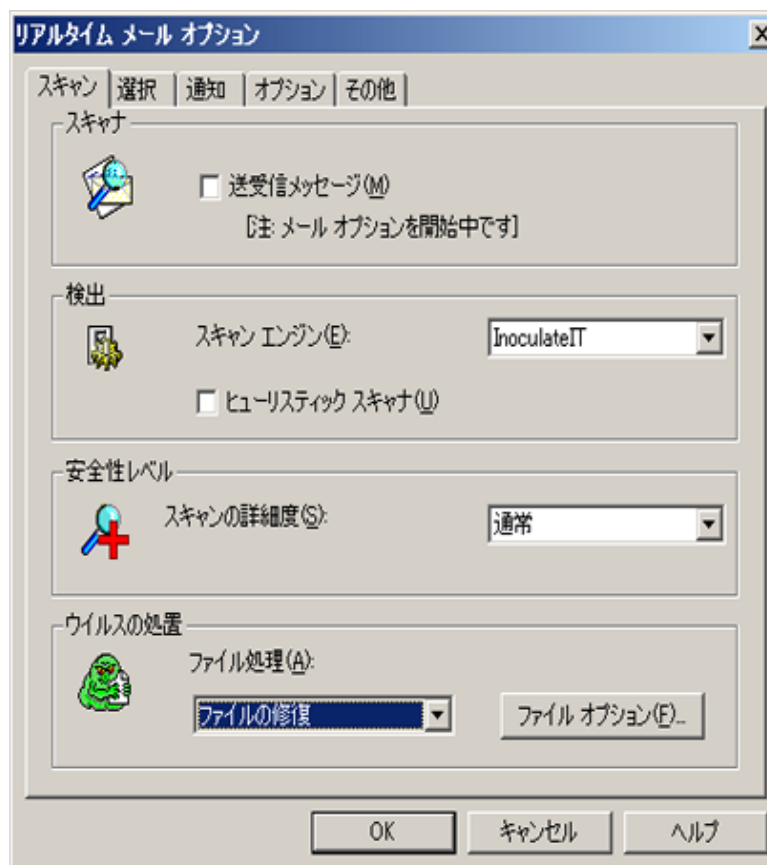
[リアルタイム メール オプション]が表示されます。

電子メール リアルタイム スキャンを管理するには、以下のオプションを使用できます。

- スキャン
- 選択
- 通知
- オプション
- その他

スキャン オプションの使用法

スキャン オプションは、[スキャン]タブに表示されます。これらのオプションで、スキャン エンジンを選択し、安全性レベルを指定し、希望のファイル操作を実行し、特定のオプションを有効にすることができます。



スキャナ

[送受信メッセージ]チェック ボックスをオンにし、電子メール オプションによるリアルタイム スキャンを有効にします。このオプションが無効になっていると、電子メールは保護されません。

検出

スキャン エンジンは、感染の検出に使用する専用のプロセッサです。デフォルトのスキャン エンジンは、大部分の設定に適しています。通常、ユーザがこの設定を変える必要はありません。このオプションは主に、大企業の熟練ユーザを対象としています。

ドロップダウン矢印を使用してスキャン エンジンを選択してください。

ヒューリスティック スキャナ

[ヒューリスティック スキャナ]チェック ボックスをオンにし、ヒューリスティック スキャン エンジン を有効にします。ヒューリスティック スキャン エンジン は、まだシグネチャが隔離も登録もされていないウイルスがないかどうかをスキャンします。

安全性レベル

スキャンの[安全性レベル]を[通常]または[詳細]モードに設定できます。ファイル を完全にスキャンする標準的な方法は、[通常]モードです。

[通常]モードでは検出できないウイルスの存在が疑われる場合は、[詳細]モードを使用します。[詳細]モードでは、ウイルス研究所での検出のように、活動していないウイルスや、故意に変更されているウイルスをも検出できます。なお、[詳細]モードは、[通常]モードに比べてかなり時間がかかります。

注: 特殊な状況のもとでは、[詳細]モードによって誤認警告が出される可能性もあります。従って、[詳細]モードを標準のスキャン オプションとした場合は、[レポートのみ]オプションを指定してください。

ウイルスの処置

処置オプションでは、感染検出時の処置を指定します。感染ファイルをどう処置するかを決める前に、感染があるかどうかをまず調べる場合には、[レポートのみ]を選択してください。ウイルス感染が発見された時点で、その後の処理を選択できます。

ファイル処理

ファイル処理を設定することによって、感染への処置を指定できます。以下のファイル処理が可能です。

ファイル処理	説明
レポートのみ	感染の検出時にレポートします。ウイルスが発見されると、ウイルスはレポートおよび元のファイルとともにパッケージ化されます。そのパッケージが元の添付ファイルと置き換えられ、指定された受信者に送信されます。
ファイルの削除	感染ファイルがレポート ファイルで置き換えられます。
ファイル名の変更	このオプションを指定すると、感染添付ファイルは、レポート ファイルを含む ZIP ファイルと AVB 拡張子を使って名前が変更された添付ファイルに置き換えられます。ウイルスが検出されたファイルの名前が 2 バイト文字の (アジア系言語の文字セットを使用している) 場合は、InfectedFile という名前に変更されます。ファイルが修復された場合は、CuredFile という名前に変更されます。

ファイル処理	説明
ファイルの移動	感染ファイルを、現在のディレクトリから移動先ディレクトリ (...¥Program Files¥CA¥Trust¥Antivirus¥Move) に移動します。添付ファイルはレポートファイルと置き換えられ、元のファイルは移動先フォルダに移動されます。ファイルはコンピュータ・アソシエイツのウイルス対策ソフトウェアの arctemp ディレクトリにリストアされます。リストアされたファイルを保存しておきたい場合、[シグネチャ アップデート]の無効化や、OS のシャットダウン、アンロードが発生する前に、ファイルを移動してください。ファイルは、リストアされても、宛先の受信者の電子メールに送信されません。
ファイルの修復	感染ファイルの自動修復を試みます。[スキャン オプション] ボタンをクリックすると、駆除処理オプションを表示し、[ファイルの修復] オプションを実行する方法を指定できます。レポート ファイルと元の添付ファイルとのパッケージが常に作成されます。 感染ファイルが修復された場合でも、感染ファイルを削除することをお勧めします。

駆除処理オプションの使用法

駆除処理オプションでは、マクロ ウイルスおよびトロイの木馬ウイルスをどう処理するか、また駆除の実行前または実行後に何を行うかを指定します。

[駆除処理オプション] ダイアログ ボックスには以下のオプションがあります。

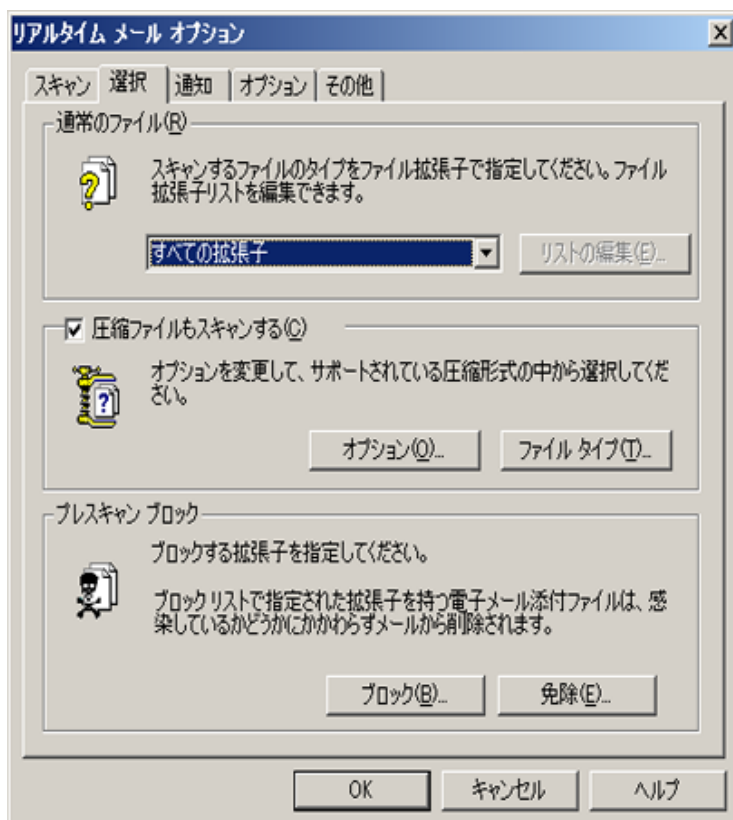
駆除処理オプション	説明
駆除前の処理	駆除しようとする前に、ファイルを移動先ディレクトリにコピーします。
トロイの木馬ウイルス/ワームに対する処理	トロイの木馬またはワーム ウイルスが発見された場合、感染ファイルを削除し、レポート ファイルと置き換えます。
駆除失敗時の処理	駆除に失敗した場合、感染ファイルの移動や名前変更などの処理は行われません。[ファイル処理] で指定した処理が行われます。[レポートのみ] と同じファイル処理はありません。
マクロ ウイルスに対する処理	ファイルから感染マクロのみを取り除くか、すべてのマクロを取り除くかを、選択できます。

カスタマイズ可能な警告メッセージ

ウイルス検出時のユーザ表示テキストを変更できます。警告メッセージをカスタマイズするには、テキスト エディタを使用して、mrtconfig.ini ファイルのメッセージ文字列を編集します。使用可能なメッセージ文字列とオプションの詳細については、インストール ディレクトリの mrtconfig.ini ファイルを参照してください。

選択オプションの使用法

選択オプションでは、スキャン対象として設定または除外するファイルの拡張子の種類、スキャンする圧縮ファイルの種類、およびプレスキャンブロックを選択できます。



通常ファイル

すべての拡張子のファイルをスキャンすることも、含めるか除外するファイルの拡張子を選択することもできます。

スキャンするファイルの拡張子	説明
すべての拡張子	[すべての拡張子]オプションを選択すると、すべてのファイル拡張子がスキャン対象に含まれます。
指定された拡張子のみ	[指定された拡張子のみ]オプションを選択すると、[リストの編集]ボタンが有効になります。[リストの編集]ボタンをクリックして、[指定された拡張子のみ]ダイアログ ボックスを開きます。スキャンしたいファイルの拡張子をファイル拡張子のリストに追加するか、またはリストからファイル拡張子を削除します。
指定された拡張子を除くすべて	[指定された拡張子を除くすべて]オプションを選択すると、[リストの編集]ボタンが有効になります。[リストの編集]ボタンをクリックして、[指定された拡張子を除くすべて]ダイアログ ボックスを開きます。スキャンしたくないファイルの拡張子をファイル拡張子のリストに追加するか、またはリストからファイル拡張子を削除します。
リストの編集	[指定された拡張子のみ]オプションまたは[指定された拡張子を除くすべて]を選択した場合、[リストの編集]ボタンをクリックすることにより、スキャン対象の特定のファイル拡張子を選択および除外するダイアログ ボックスを表示します。

圧縮ファイルのスキャン

圧縮ファイルのスキャンする場合は、[圧縮ファイルもスキャンする]オプションを選択します。オプションを変更し、使用可能な圧縮ファイルの種類をリストから選択できます。

オプション

圧縮ファイルを管理するオプションがもう 1 つあります。このオプションを選択すると、スキャン パフォーマンスが向上します。[圧縮ファイルもスキャンする]グループ内の [オプション]ボタンをクリックして、[圧縮ファイル オプション]ダイアログ ボックスを表示します。感染ファイルの発見時に圧縮ファイルのスキャンを停止させるには、このオプションを選択します。

ファイル タイプ

サポートされている、スキャン可能な圧縮ファイルの種類は以下のとおりです。

- ARJ
- GZIP
- JAVA アーカイブ
- LHA
- Microsoft キャビネット ファイル
- Microsoft 圧縮ファイル
- MIME
- UNIX 間のエンコード形式ファイル (UUEncode)
- ZIP
- RAR
- UNIX 圧縮ファイル (.Z)
- リッチ テキスト形式 (.RTF)
- TNEF カプセル化電子メール ファイル

プレスキャン ブロック

[プレスキャン ブロック]オプションでは、配信をブロックするか、またはブロックから除外する電子メール添付ファイルの拡張子を指定できます。

ブロック

[ブロック]をクリックすると、[ブロック拡張子リスト]ダイアログ ボックスが開きます。[ブロック拡張子リスト]ダイアログ ボックスを使用すると、ブロックする拡張子のリストに、電子メール添付ファイルの拡張子を追加できます。

除外

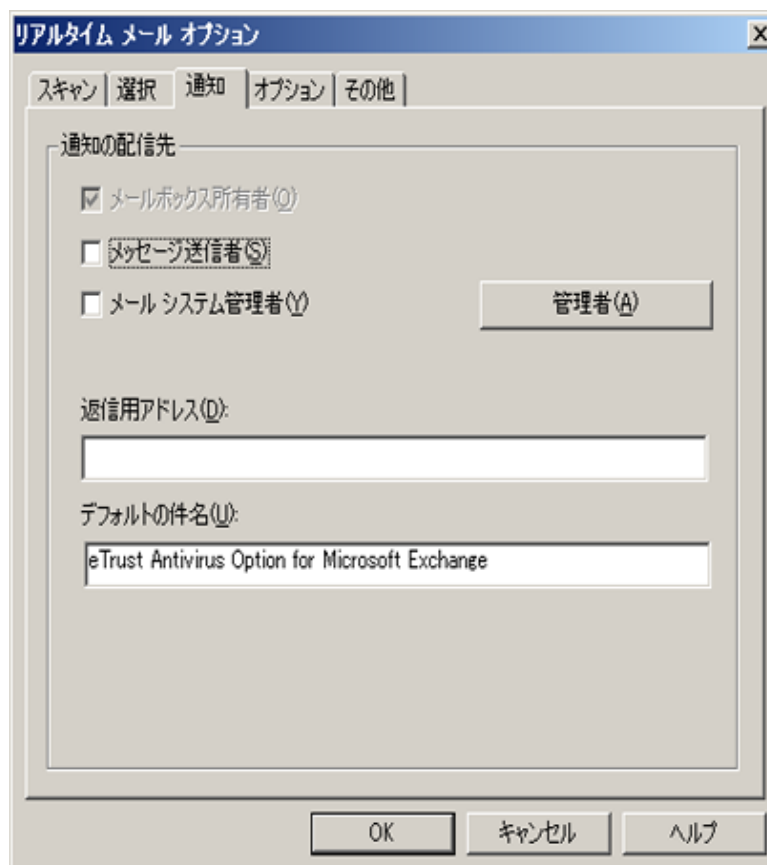
[除外]ボタンをクリックすると、[ブロックから除外]ダイアログ ボックスが開きます。[ブロックから除外]ダイアログ ボックスを使用すると、除外リストに含める電子メール添付ファイルを指定できます。ファイルの末尾の文字列も指定できます。たとえば `virus.com` と指定すると、`myvirus.com` と `another_virus.com` はブロックから除外されます。

拡張子はブロックされて、ファイル名が除外されている電子メール添付ファイルは、添付先の電子メールとともに配信されます。添付ファイルは配信される前にスキャンされます。

注: スペルは正確でなければなりません。

通知オプションの使用法

[通知]タブを使用すると、感染の通知先および通知の件名を設定できます。デフォルトで、受信者には常に通知します。受信者以外に対する通知には、感染に関する情報のみが含まれ、感染した添付ファイルや電子メールは含まれません。



メッセージ送信者

このオプションを選択すると、感染した電子メールの送信者に通知できます。

メール システム 管理者

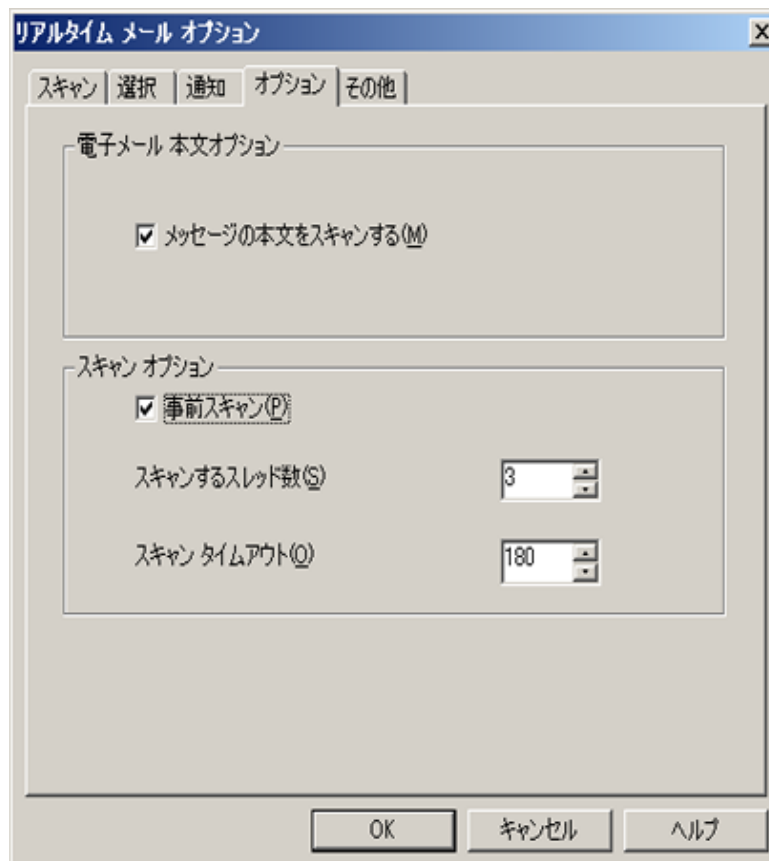
このオプションを選択すると、感染のシステム管理者に通知されます。管理者のリストに入力するには、[管理者]をクリックします。

返信用アドレス

通知を配信できない場合は、このアドレスに再配信されます。

Microsoft Exchange 2000 のオプションの使用法

[オプション]タブでは、Microsoft Exchange 2000 Server での電子メールのスキャンについてカスタム設定を選択できます。適切なオプションを選択して、Microsoft Exchange 2000 Server でのコンピュータ・アソシエイツのウイルス対策ソフトウェアのパフォーマンスをチューニングできます。



メッセージの本文をスキャンする

このチェック ボックスをオンにすると、電子メール メッセージの本文をスキャンできます。

事前スキャン

このチェック ボックスをオンにすると、Microsoft Exchange のキュー スキャンの優先順位付けを有効にできます。予防型スキャンを無効にすると、項目はユーザまたはオンデマンド スキャナによって直接アクセスされた場合にのみスキャンされるか、バックグラウンド スキャン スレッドによってスキャンされます。

スキャンするスレッド数

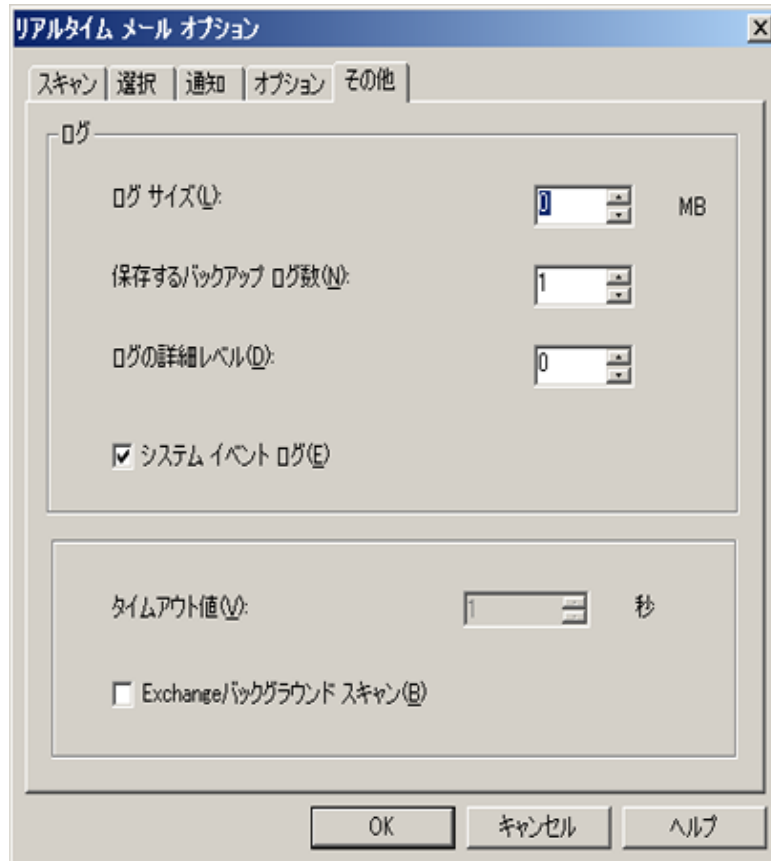
ドロップダウン メニューから選択することにより、グローバル スレッド プールのスレッド数を変更できます。スキャン スレッド数を増やすと、システムのパフォーマンスに悪影響を及ぼす可能性があります。Microsoft ではデフォルト値を推奨しています。

スキャン タイムアウト

タイムアウト値を秒数で指定できます。ドロップダウン矢印を使用すると、値を選択できます。負荷の高いシステムでは、タイムアウトまでの時間が長くなるように指定できます。

その他の各オプションの使用法

[その他]タブでは、その他の各種オプションを指定できます。ログ オプションでは、ログのサイズ、保存しておくログの数、ログの詳細レベルを指定できます。また、このタブでは、システム イベント ログの有効化、タイムアウトの指定、およびバックグラウンド スキャンの有効化を行うことも可能です。



ログ サイズ

ドロップダウン矢印を使用すると、希望のログ サイズを選択できます。選択した値はログ ファイルの大きさを MB 単位で表します。

保存するバックアップ ログ数

ドロップダウン矢印を使用すると、保存するログの数を選択できます。ログは、InXScan#####.log または StoreVS(2)#####.log (#####は 0000、0001 など) という形式で、eTrust Antivirus ソフトウェアのインストール先ディレクトリに保存されます。

ログの詳細レベル

ドロップダウン矢印を使用すると、ログの詳細レベルを指定できます。

- 0 = ログに記録しない
- 1 = 感染ファイルのみに関するログ
- 2 = 全スキャンファイルに関するログ

システム イベント ログ

このオプションでは、感染添付ファイルの発見時にアプリケーション イベント ログ内にイベントを作成する電子メール オプションを有効に設定できます。

注:このオプションがオンの場合にウイルスの攻撃があると、アプリケーション イベント ログが迅速に発行されます。

タイムアウト値

タイムアウト値を指定する場合は、スキャンが完了するまでスレッドが待機できる最長時間(秒数)を指定します。指定したタイムアウト期間内にスキャンが完了しない場合は、メッセージの表示やメッセージへのアクセスが不可能になります。ドロップダウン矢印を使用すると、値を選択できます。頻繁にタイムアウトになる場合は、タイムアウト値を大きくします。

注:このオプションはExchange 5.5 でのみ使用できます。

Exchange バックグラウンド スキャン

このオプションでは、未スキャンの添付ファイルの場所を情報ストアが特定するために添付ファイル テーブルをスキャンする必要があるか、またはバージョンが変更されたかどうかを指定できます。

注:Exchange 5.5 では、オプションは一時的に(0~60 秒)停止し、再開します。Exchange 2000 または 2003 では、そのようなことは起きません。

注:バックグラウンド スキャンによって、サーバのパフォーマンスが著しく低下する場合があります。コンピュータ・アソシエイツはExchangeサーバではバックグラウンド スキャンを有効にしないことをお勧めします。

Lotus Notes/Domino Option の紹介

eTrust Antivirus Lotus Notes/Domino Option は、コンピュータ・アソシエイツのウイルス対策ソフトウェアと統合し、文書や電子メール添付ファイル内でウイルスをスキャンします。感染した Lotus Notes の添付ファイルを自動的に検出できます。このオプションを使用すると、感染が検出された場合にホスト メッセージングシステムを通してユーザに通知されます。

注: Lotus Notes/Domino Optionは、コンピュータ・アソシエイツのeTrust Antivirus 7.1以降で使用してください。

Lotus Notes/Domino Option の機能

Lotus Notes/Domino Option には以下の機能があります。

- **メール スキャン** – Lotus Notes/Domino Option は Notes サーバ上に常駐します。Notes メールを通して送信された感染ファイルを、すべて検出し処理します。ウイルスからの保護は自動かつ継続的です。
- **マクロ ウイルス アナライザ** – Word Concept ウイルスなど、急速に蔓延するマクロ ウイルスを検出し完全に除去します。添付文書を切り離し、検査し、再添付します。修復処理を選択して適用した場合は、感染した添付ファイルを再添付し、ウイルスを処理してアラートを送信します。
- **ライブ スキャン** – この機能は、メッセージング システムがオンラインであっても、ユーザの作業を妨害することなくウイルスをスキャンします。
- **簡単なオプション** – 検出オプションとアラート オプションを簡単に指定できます (たとえば、感染ファイルを修復してアラートをシステム管理者に送るなど)。
- **通知オプション** – この機能で、感染電子メールをメールボックスに受信したユーザ、感染電子メールを送信したユーザ、または Lotus Notes 管理者に、ウイルス通知を送信するオプションを設定できます。また、ウイルスを含むメールに通知を直接添付することもできます。

メッセージング/グループウェア システムの理解

Lotus Notes などの電子メッセージング システムは、今日の企業では情報伝達手段として広く利用されています。また、メッセージング システムは多くの企業で、社内と社外の両方において情報や文書を共有する、必要不可欠な手段になっています。ところがこれらのシステムは、感染ウイルスを取り込んで組織中に急速に蔓延させる、セキュリティの盲点になってしまう可能性があり、データと生産性の両方が結果として危険にさらされてしまうおそれがあります。

ICSA® (International Computer Security Association) の調査によると、電子メール添付ファイルは最も一般的なウイルス感染源の 1 つです。この急速な成長率は過去 10 年で 2 倍以上になりました。ICSA によって実施された 1996 年の調査では、検出されたウイルスの 49% がマクロ ウイルスであると述べられています。マクロ ウイルスは、NORMAL.DOT (Windows 版 Microsoft Word 6.0 以上で実行される) に寄生します。Winword.Concept ウイルスが登場するまで、ウイルスのほとんどは、磁気メディアの実行可能領域 (つまりブート セクタ) またはファイル (.EXE、COM、BIN ファイルなど) にのみ寄生し感染していました。ICSA によると、よく知られているラブレター ウイルスはマスメーラであり、急速に蔓延する可能性を持っています。このウイルスは、電子メール メッセージに添付された VBS ファイルとして受信されます。

ドキュメントがメッセージからハードディスク ドライブへと保存された場合、コンピュータ・アソシエイツのソリューションのようにユーザをウイルスから保護できるクライアント/サーバ ウイルス対策ソフトウェアは少数です。ただし、Lotus Notes のようなサーバベースのメッセージング システムをスキャンおよび修復できるのは、弊社が提供するような統合型ソリューションだけです。統合型ソリューションを使用すれば、会社のメッセージング/データベース システムは Winword Concept やその他のマクロ ウイルスの脅威にさらされずに済みます。

ネットワークと Lotus Notes/Domino Option システムの保護

Lotus Notes/Domino Option システムとネットワーク全体を新種のウイルスから完全に保護するには、以下の操作を実行します。

- Lotus Notes/Domino Option とウイルス対策ソフトウェアをインストールした後、すぐに最新のシグネチャ ファイルをダウンロードします。コンピュータ・アソシエイツでは常時、新種のウイルスを検出しシグネチャ ファイルをアップデートしています。このため、最新のシグネチャ ファイルを使用することで、最新の保護機能を確実に利用できるようになります。
- すべての実行ファイルを読み込み専用を設定します。これで実行ファイルが感染しにくくなります。
- フロッピーディスクからどのファイルのコピーするときも、コピーの前にフロッピーディスクに対してウイルススキャンを実行します。
- ウイルス スキャンを問題なく実行した後に、コンピュータ・アソシエイツの BrightStor などバックアップ ツールを使用して、ご使用のワークステーションのバックアップ処理を実行します。この処理を実行すると、あるファイルでウイルスが検出されて駆除できなくなっても、バックアップしたファイルを使用できます。

- コンピュータ・アソシエイツのテクニカル サポートのサイト (<http://www.caj.co.jp/support>) を定期的に参照してください。
- 最新のウイルス情報を提供するコンピュータ・アソシエイツのオンライン ウイルス対策ニュースレター (無料) を購読することもできます。

インストールに必要な条件

インストールする前に、必要なソフトウェアとハードウェアが準備できていることを確認してください。

ハードウェアとソフトウェアの動作要件

Lotus Notes/Domino Option をインストールして使用するには、以下のソフトウェアが必要です。

- Windows NT 4.0、Windows 2000 Server、Windows 2000 Advanced Server、Windows XP Professional、または Windows 2003 Server。
- Lotus Domino Server/Client バージョン 4.65、5.07、5.08、5.09、5.010、または 6。
- Lotus Notes Server を実行中のマシンにインストール済みの eTrust Antivirus 7.1 以降。
- Lotus Notes Server に、2MB のディスク空き容量、2MB の空きメモリ、および Intel プロセッサ。

インストールの手順

最初に、eTrust Antivirus 7.1 ソフトウェアのインストールを実行します。次に、Lotus Notes/Domino Option を Lotus Notes Server にインストールするため、CD-ROM を CD-ROM ドライブに挿入します。インストール画面が表示された後、Lotus Notes インストール オプションを選択し、セットアップ ウィザードの指示に従ってインストールを完了します。

インストールのテスト

EICAR テスト標準を使用して、コンピュータ・アソシエイツ電子メール オプションのインストールをテストできます。EICAR (European Institute for Computer Antivirus Research) が開発した EICAR 標準を使用すると、感染ファイルとして検出される、テスト用の未感染の電子メール添付ファイルを作成できます。

以下は、EICAR 標準 Antivirus テスト ファイルのサンプル コードです。このコード行をテキスト ファイルにコピーします。

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

テキスト ファイルを EICAR.COM という名前で保存します。ファイルのサイズは 69～70 バイト程度になります。

EICAR.COM ファイルをテスト用の電子メールに添付します。コンピュータ・アソシエイツ電子メール オプションにより、添付ファイルが検出され、スキャン結果ファイル (AvReport.txt) が電子メールに添付されます。

テストの実施後、EICAR.COM ファイルを削除します。

Lotus Notes/Domino Option の使用法

この章では、Lotus Notes/Domino Option を使用して、電子メールやメールボックスデータベースに隠れている可能性のある感染を検出する方法について説明します。感染の検出後の処理については、eTrust Antivirus に付属の『管理者ガイド』を参照してください。

リアルタイム メール オプションを使用した Lotus Notes/Domino Option のウイルス対策

企業のウイルス対策の鍵は、リアルタイムスキャンにあります。リアルタイム スキャンは、他のユーザに感染ファイルを送ろうとするタイミングでウイルスを捕捉するため、感染が広がるのを防止できます。

サーバベースのメール システムとして、Lotus Notes/Domino Option 内のすべての電子メールは、eTrust Antivirus メールボックスを通過した後、Lotus Notes/Domino サーバに送られます。eTrust Antivirus ソフトウェアは侵入してくる感染を捕らえるバリアをサーバ上に張り巡らせて、サーバとユーザの両方を感染から守ります。

Lotus Notes/Domino Option は、システムトレイ内の[リアルタイム]オプションを使用したリアルタイム スキャンと設定変更をサポートします。

[リアルタイム メール オプションの設定]ダイアログボックスへのアクセス

システムトレイにある、eTrust Antivirus ソフトウェアのアイコンを右クリックします。

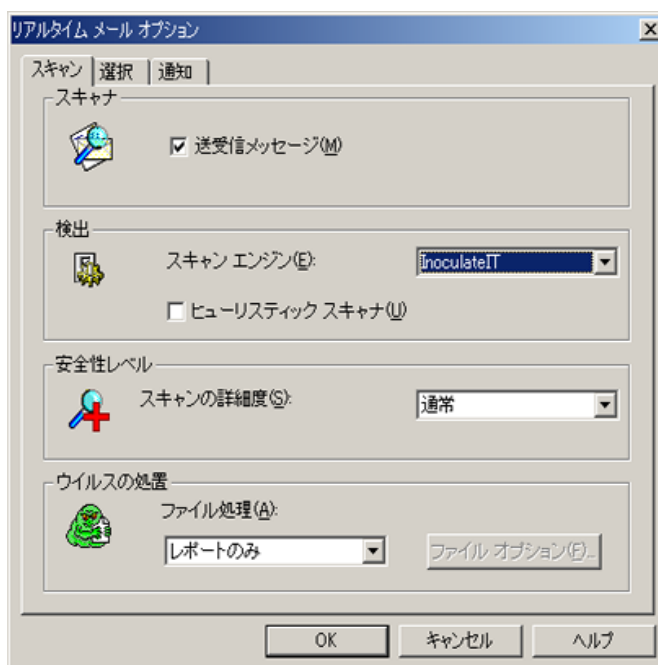
オプションメニューが表示されます。[メール オプション]を選択します。[リアルタイム メール オプション]ダイアログ ボックスが表示されます。

電子メール リアルタイム スキャンを管理するには、以下のタブ オプションを使用できます。

- スキャン
- 選択
- 通知

スキャン オプションの使用法

スキャン オプションを使用すると、メール オプションの有効化、スキャン エンジンの選択、安全性レベルの指定、ファイル処理の実行などを行えます。



スキャナ

[送受信メッセージ]チェック ボックスをオンにし、電子メール オプションによるリアルタイム スキャンを有効にします。このオプションが無効になっていると、電子メールは保護されません。

検出

スキャン エンジンは、感染の検出専用のプログラムです。インストール時に、ご使用の構成に適したスキャン エンジンが自動的に選択されます。

ドロップダウン矢印を使用すると、InoculateIT スキャン エンジンまたは Vet スキャン エンジンのいずれかを選択できます。

ヒューリスティック スキャナ

[ヒューリスティック スキャナ]チェック ボックスをオンにし、ヒューリスティック スキャン エンジンを有効にします。ヒューリスティック スキャン エンジンは、まだシグネチャが隔離も登録もされていないウイルスがないかどうかをスキャンします。

安全性レベル

スキャンの[安全性レベル]は[通常]または[詳細]モードに設定できます。ファイルを完全にスキャンする標準的な方法は、[通常]モードです。

[通常]モードでは検出できないウイルスの存在が疑われる場合は、[詳細]モードを使用します。[詳細]モードでは、ウイルス研究所での検出のように、活動していないウイルスや、故意に変更されているウイルスをも検出できます。なお、[詳細]モードは、[通常]モードに比べてかなり時間がかかります。

注: 特殊な状況のもとでは、[詳細]モードによって誤認警告が出される可能性もあります。したがって、[詳細]モードを標準のスキャン オプションとした場合は、[レポートのみ]オプションを指定します。

ウイルスの処置

処置オプションでは、感染検出時の処置を指定します。感染があるかどうかを調べた後で、感染した電子メール添付ファイルの処置を指定したい場合は、[レポートのみ]を選択します。電子メール添付ファイルに感染がある場合は、Lotus Notes/Domino オプションを使用して AvReport.txt という電子メール添付ファイルを挿入できます。このレポートは感染に関する情報を示します。

ファイル処理

ファイル処理を設定することによって、感染への処置を指定できます。以下のファイル処理が可能です。

ファイル処理	説明
レポートのみ	感染の検出時にレポートします。ウイルスが発見されると、感染ファイルをどう処置するかを選択できます。
ファイルの削除	感染ファイルを削除します。
ファイル名の変更	感染ファイルの検出後に、ファイル名を AVB 拡張子に変更します。ファイルは、名前が AVB タイプの拡張子に変更された後は、スキャンされません。ウイルスが検出されたファイルの名前が 2 バイト文字の(アジア系言語のフォントを使用している)場合は、一時ファイルに変更されます。
ファイルの移動	感染ファイルを、現在のディレクトリからホームディレクトリの移動先サブディレクトリに移動します。
ファイルの修復	感染ファイルの自動修復を試みます。[スキャン オプション]ボタンをクリックすると、駆除処理オプションを表示し、[ファイルの修復]オプションを実行する方法を指定できます。 感染ファイルが修復された場合でも、感染ファイルを削除することをお勧めします。

駆除処理オプションの使用法

駆除処理オプションでは、マクロ ウイルスおよびトロイの木馬ウイルスをどう処理するか、また駆除の実行前または実行後に何を行うかを指定します。

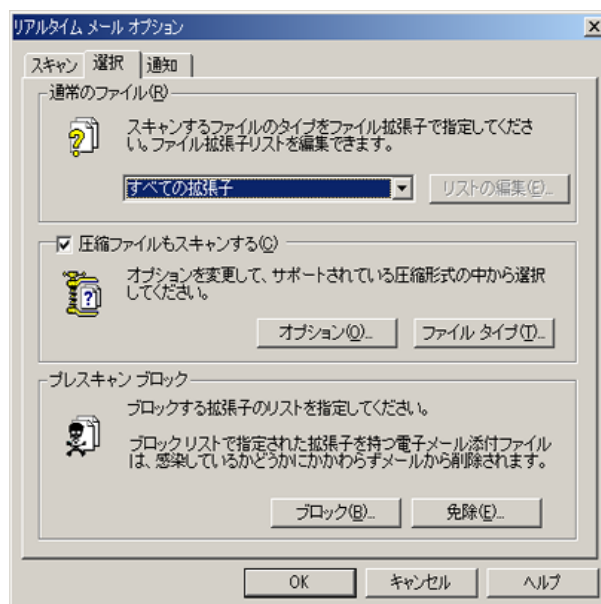
[駆除処理オプション]ダイアログボックスでは、以下のオプションを使用できます。

駆除処理オプション	説明
駆除前の処理	駆除しようとする前に、ファイルを移動先ディレクトリにコピーします。
トロイの木馬ウイルス/ワームに対する処理	トロイの木馬またはワーム ウイルスが発見された場合、感染ファイルを削除します。
駆除失敗時の処理	駆除に失敗した場合、感染ファイルを移動先ディレクトリに移動するか、ファイルの拡張子を AVB に変更します。[処理なし]オプションを選択することにより、ファイルを処理しないことも可能です。
マクロ ウイルスに対する処理	ファイルから感染マクロのみを取り除くか、すべてのマクロを取り除くかを、選択できます。

選択オプションの使用法

選択オプションでは、スキャンの対象として設定または除外するファイルの拡張子の種類、スキャンする圧縮ファイルの種類を選択できます。

[選択]タブで使用できるオプションを以下に説明します。



通常ファイル

すべての拡張子のファイルをスキャンすることも、含めるか除外するファイルの拡張子を選択することもできます。

スキャンするファイルの拡張子	説明
すべての拡張子	[すべての拡張子]オプションを選択すると、すべてのファイル拡張子がスキャン対象に含まれます。
指定された拡張子のみ	[指定された拡張子のみ]オプションを選択すると、[リストの編集]ボタンが有効になります。[リストの編集]ボタンをクリックして、[指定された拡張子のみ]ダイアログ ボックスを開きます。スキャンするファイルの拡張子をファイル拡張子のリストに追加するか、またはリストからファイル拡張子を削除します。
指定された拡張子を除くすべて	[指定された拡張子を除くすべて]オプションを選択すると、[リストの編集]ボタンが有効になります。[リストの編集]ボタンをクリックして、[指定された拡張子を除くすべて]ダイアログ ボックスを開きます。スキャンしないファイルの拡張子をファイル拡張子のリストに追加するか、またはリストからファイル拡張子を削除します。
リストの編集	[指定された拡張子のみ]オプションまたは[指定された拡張子を除くすべて]を選択した場合、[リストの編集]ボタンをクリックすることにより、スキャン対象の特定のファイル拡張子を選択および除外するダイアログ ボックスを表示します。

圧縮ファイルのスキャン

圧縮ファイルのスキャンする場合は、[圧縮ファイルもスキャンする]オプションを選択します。オプションを変更し、使用可能な圧縮ファイルの種類をリストから選択できます。

オプション

圧縮ファイルを管理するオプションがもう 1 つあります。このオプションを選択すると、スキャン パフォーマンスが向上します。[圧縮ファイルもスキャンする]グループ内の[オプション]ボタンをクリックして、[圧縮ファイル オプション]ダイアログ ボックスを表示します。感染ファイルの発見時に圧縮ファイルのスキャンを停止させるには、このオプションを選択します。[アーカイブに感染処理を適用する]オプションも選択できます。

ファイル タイプ

サポートされている、スキャン可能な圧縮ファイルの種類は以下のとおりです。

- ARJ
- GZIP
- JAVA アーカイブ
- LHA
- Microsoft キャビネット ファイル
- Microsoft 圧縮ファイル
- MIME
- UNIX 間のエンコード形式ファイル (UUEncode)
- ZIP
- RAR
- UNIX 圧縮ファイル (.Z)
- リッチ テキスト形式 (.RTF)
- TNEF カプセル化電子メール ファイル

プレスキャン ブロック

[プレスキャン ブロック]オプションでは、配信をブロックするか、またはブロックから除外する電子メール添付ファイルの拡張子を指定できます。

ブロック

[ブロック]ボタンをクリックして、[ブロック拡張子リスト]ダイアログボックスを開きます。[ブロック拡張子リスト]ダイアログボックスで、ブロックする拡張子のリストに、電子メール添付ファイルの拡張子を追加します。

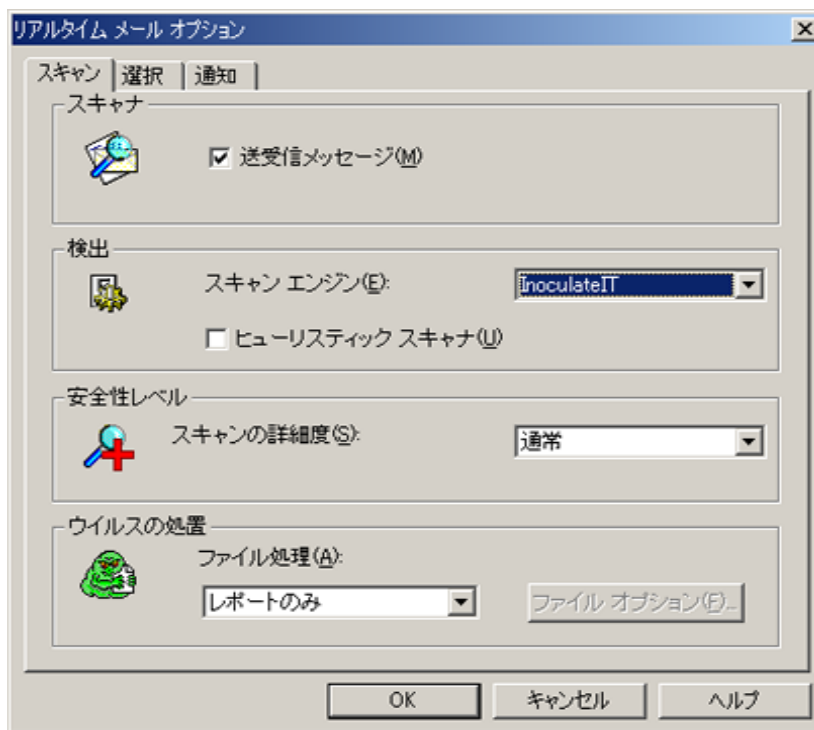
除外

[除外]ボタンをクリックして、[ブロックから除外]ダイアログ ボックスを開きます。[ブロックから除外]ダイアログボックスで、除外リストに含める電子メール添付ファイルを指定します。拡張子はブロックされ、ファイル名が除外されている電子メール添付ファイルは、添付先の電子メールとともに配信されます。添付ファイルは配信される前にスキャンされます。

注: スペルは正確でなければなりません。

通知オプションの使用法

[通知]タブを使用すると、通知オプションを指定できます。



通知

[通知]の下のおプションを選択するには、使用するオプションのチェックマークをオンにします。ウイルス対策ソフトウェアは、メッセージング システムで感染が検出されると、Lotus Notes/Domino Option のメール システムを使用して、ユーザによって指定された種類の通知を送信します。

メールボックス所有者

感染ファイルが添付されたメールの受信者に通知します。これは、メールに感染ファイルが添付されている可能性があることを受信者に知らせるためのよい方法です。このオプションを常にオンにしておいてください。

メッセージ送信者

感染メールの送信者、または感染が含まれるデータベースの作成者に通知します。このオプションの使用により、感染ファイルの送信元を追跡し、送信元のメールボックス所有者に通知することができます。

メール システム管理者

ネットワークセキュリティが脅かされた可能性があることを管理者に知らせます。これにより管理者はネットワークの安全確保に必要な処置を行えます。

検出結果を添付

検出結果を添付ファイルとして電子メールメッセージに添付します。内容は、感染ファイルの情報、行われた処置、修復されたかどうかなどです。

カスタマイズ可能な警告メッセージ

ウイルス検出時のユーザ表示テキストを変更できます。警告メッセージをカスタマイズするには、テキスト エディタを使用して、`virushdr.txt` ファイルのメッセージ文字列を編集します。使用可能なメッセージ文字列とオプションの詳細については、インストール ディレクトリの `virushdr.txt` ファイルを参照してください。また、[デフォルトの件名]ボックスの文字列または `nRTstr.ini` ファイルの `SUBJECT_FOR_INFECT`ION の値を更新すると、警告メッセージの件名をカスタマイズできます。

カスタマイズ可能な警告メッセージの返信用アドレス

メッセージを正常に配信できなかった場合に、警告メッセージを適切なアドレスに返信できます。返信用アドレスをカスタマイズするには、[返信用アドレス]ボックスの文字列を編集するか、テキスト エディタを使用して、`nRTstr.ini` ファイルの `RETURN_ADDRESS` の値を編集します。

索引

L

Lotus Notes Option

インストールに必要な条件, 3-3

概要, 3-1

機能, 3-1

Lotus Notes サーバ, 4-1

M

Microsoft Exchange 2000 のオプション

[オプション]タブ, 2-10

Microsoft Exchange Option

インストールに必要な条件, 1-3

機能, 2-1

紹介, 1-1

あ

圧縮ファイル

オプション, 2-7, 4-6

スキャン, 2-7, 4-6

い

移動、ファイル処理, 2-4, 4-4

う

ウイルス対策ニュースレター, 1-3

か

拡張子

ブロックから除外, 2-8, 4-7

き

キュー スキャンの優先順位付け

Microsoft Exchange 2000, 2-11

<

駆除処理オプション, 2-4, 4-4

さ

削除、ファイル処理, 2-4, 4-4

し

シグネチャファイルのダウンロード, 1-2

システムトレイ

メール オプションへのアクセス, 4-1

システムのバックアップ, 1-2

修復、ファイル処理, 2-4, 4-4

[詳細]モード, 2-3, 4-3

処置オプション, 2-3, 4-3

す

スキャン エンジン, 2-2, 4-2

[スキャン]タブ, 4-1

スレッドをスキャンする

Microsoft Exchange 2000 での変更, 2-11

せ

選択オプション
[選択]タブ, 4-5
選択タブ, 2-6

つ

通常のファイルのスキャン, 2-7, 4-6
[通常]モード, 2-3, 4-3

て

テクニカル サポート, 1-3

と

動作要件
ハードウェアとソフトウェア, 1-3, 3-3

ね

ネットワークの保護, 1-2, 3-2

ふ

ファイル拡張子
指定された拡張子のみ, 2-7, 4-6

指定された拡張子を除くすべて, 2-7, 4-6
すべての拡張子, 2-7, 4-6
リストの編集, 2-7, 4-6

ファイル処理
移動, 2-4, 4-4
削除, 2-4, 4-4
修復, 2-4, 4-4
ファイル名の変更, 2-4, 4-4
レポートのみ, 2-3, 4-3

ファイル名の変更、ファイル処理, 2-4, 4-4

め

メール オプションへのアクセス, 4-1
[メール オプション]メニュー, 4-1
メッセージング システム, 1-1, 3-2

も

モード
[通常]または[詳細], 2-3, 4-3

れ

レポートのみ、ファイル処理, 2-3, 4-3