

eTrust[®] Inoculate//[™] Microsoft Exchange Option

ユーザガイド



Computer Associates[™]

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製、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。

© 2002 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	1-2
ネットワークと Exchange システムの保護	1-3
インストールの要件	1-3
ハードウェアとソフトウェアの要件	1-3

第 2 章: Exchange Option の使用法

リアルタイム スキャン	2-1
スキャン オプションの使用法	2-2
検出	2-2
安全性レベル	2-3
感染の処置	2-3
メール オプションを有効にする	2-5
システム イベント ログを有効にする	2-5
バックグラウンドスキャンを有効にする	2-5
選択オプションの使用法	2-6
通常のコピー	2-7
圧縮ファイルをスキャン	2-7
タイムアウト値を指定	2-9
トレース ファイルのサイズを指定	2-9
デバッグ レベルを指定	2-9
フィルタ オプションの使用法	2-10
プレスキャンブロック	2-10
ログ オプションの使用法	2-11

索引

Exchange Option の紹介

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のためのオプション製品であり、電子メールメッセージに添付された文書内やフォルダ内で、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 が常駐するサーバの上で稼働します。電子メールの感染した添付物を検出、修復、遮断することにより、感染が会社全体に広がるのを防ぎます。

注：Windows NT 上で Exchange Option を使用する場合は、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バージョン 6.0 (SP1) 以降が必要です。

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伝染するマクロ 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、ウイルスを処理した後、アラートを送信します。
- 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も、ユーザの操作を妨げることなく、ウイルスをスキャンします。
- 使いやすいオプション
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 など電子メッセージング システムは、今日の企業では情報のやり取りに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ための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が、ウイルスに感染しそこから組織じゅうに蔓延させてしまうためのセキュリティ上の穴となってしまうことがあり、結果的にデータと生産性の両方を危険にさらす恐れがあります。

ICSA® (International Computer Security Association)の調査によれば、電子メールの添付ファイルが最もありふれたウイルス感染源の1つとのこと。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 ウイルスは、歴史上、最も短期間で蔓延しました。また、ICSA の別の調査では、検出された全ウイルスの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、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常套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現れています。

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。しかし 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、独自の機能があります。この機能により、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、以下のことをしてください。

- Exchange Option とウイルス対策ソフトウェアをインストールしたら、すぐに最新のシグネチャ ファイルをダウンロードしてください。CA 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取り専用を設定してください。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、フロッピー ディスクをウイルス スキャンしてください。
- ウイルス スキャンを問題なく実行した後に、BrightStor Enterprise Backup や ARCserve 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をとってください。こうしておけば、あるファイルでウイルスが検出され、それを修復できなくなっても、代わりに、バックアップしておいたファイルが使用できます。
- 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）を購読してください。

インストールの要件

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 Microsoft 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。

- Windows NT 4.0 以降
- Exchange Server 5.5 (SP4)、または Exchange 5.5 (SP3) およびホットフィックス (MSKB Q248838)
- 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 バージョン 6.0 (SP1) 以降
- Exchange Server 用に少なくとも 40MB のディスク空き容量
- Exchange Option を実行する Exchange Server

Exchange Option の使用法

この章では、Microsoft Exchange Option 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解説します。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 ウィ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。

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)ダイアログへのアクセス

以下に示す、システム トレイ内のコンピュータ・アソシエイツのウィルス対策ソフトウェアのアイコンを右クリックしてください。



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]ダイアログが表示されます。

以下のタブ オプションを使って電子メール リアルタイム スキャンを管理できます。

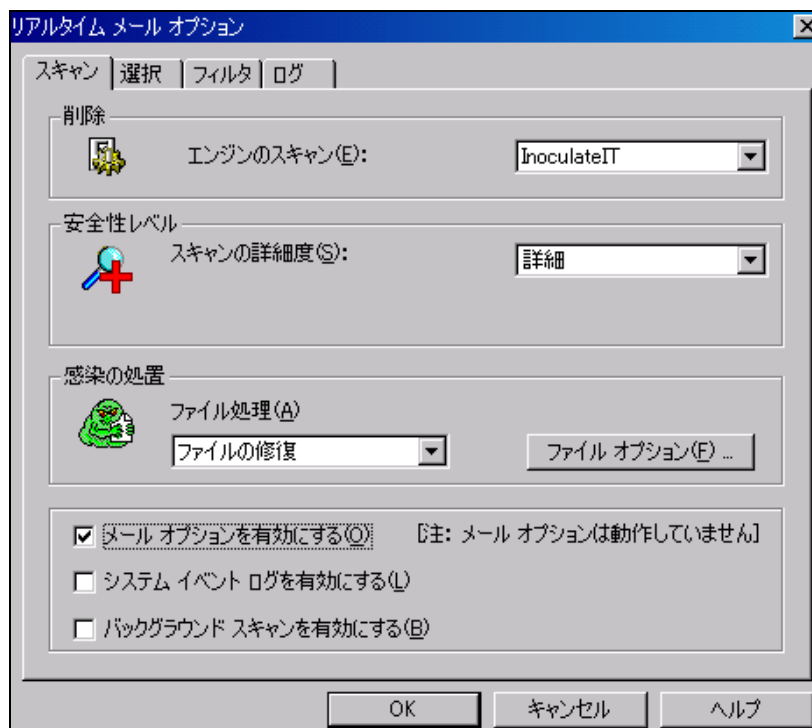
- スキャン
- 選択
- フィルタ
- ログ

この章では、電子メール スキャンを管理するこれらのオプションの使用法について説明します。

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。

[スキャン]タブで使用できるオプションについて以下に説明します。



検出

スキャン エンジンは、感染の検出に専用のプロセッサです。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。通常、ユーザがこの設定を変える必要はありません。このオプションはおもに、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。

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感染の疑いがある場合には、[詳細]モードを使用してください。[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。ただし、[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： 環境によっては、[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。このため、[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。

感染の処置

[感染の処置]オプションでは、ウイルス感染の発見時にそのウイルスを処理する方法を指定します。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たい場合には、[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

ウイルス感染への処置として、ファイル処理を設定してください。以下のようなファイル処理があります。

ファイル処理	説明
レポートのみ	ウイルス感染が発見されると、レポートが発行されます。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、感染した添付ファイルは、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。
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 Move サブディレクトリに移動します。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 Move フォルダに移動されます。ファイルは CA 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は、オプション[シグネチャのアップデート]の無効化や、OS のシャットダウン、アンロードを引き起こす何らかのことが行われる前に、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、意図された受信者の電子メールに戻されはしません。

ファイル処理	説明
ファイルの修復	<p>感染ファイルを自動的に修復しようとしています。[ファイル オプション] ボタンをクリックすることにより、[駆除処理オプション]を表示し、[ファイルの修復]オプションの処理方法を指定してください。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。</p> <p>感染ファイルが修復された後でも、感染ファイルを削除し、元のファイルを、バックアップまたはインストール ディスクからリストアすることをお勧めします。</p>

駆除処理オプション

[駆除処理]オプションでは、マクロ ウイルスとトロイの木馬ウイルスの感染を処理する方法と、駆除の試行前と試行後に行う処理を指定できます。

[駆除処理オプション]ダイアログ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 Move ディレクトリにコピーします。
トロイの木馬/ワーム処置	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。
駆除に失敗した場合の処理	<p>駆除に失敗した場合、感染ファイルを Move ディレクトリに移動するか、ファイルの拡張子を AVB に変更するか、または両方を行います。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 Move フォルダに移動されます。ファイルは CA 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、オプション[シグネチャのアップデート]の無効化や、OS のシャットダウン、アンロードを引き起こす何らかのことが行われる前に、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、意図された受信者の電子メールに戻されはしません。[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。</p>
マクロ ウイルス処置	ファイルから感染マクロだけを取り除くか、すべてのマクロを取り除くかを、選択できます。

メール オプションを有効にする

このオプションでは、メール オプションによるリアルタイム スキャンを有効にできます。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。

システム イベント ログを有効にする

このオプションでは、感染した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メール オプションを有効にできます。

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。

バックグラウンド スキャンを有効にする

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。

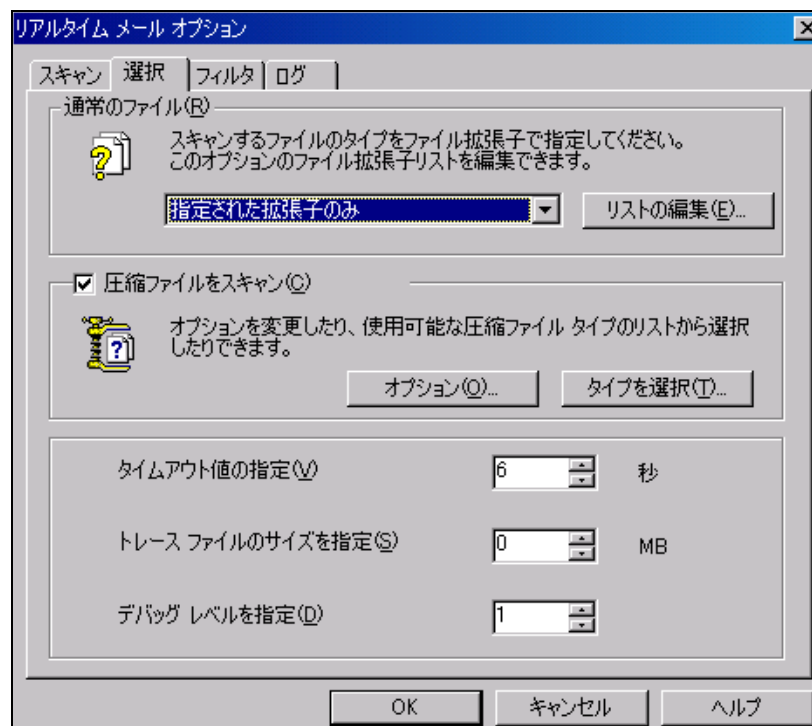
このオプションを変更（無効か有効）するとメール オプションが無効になり、続いて再開されます。再開までの時間は0～60 秒の範囲です。

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。

選択オプションの使用法

[選択]オプションでは、ファイルの拡張子を選択して、それをスキャンに含めるか除外するかを指定できます。また、タイムアウト値、トレース ファイルのサイズ、デバッグ レベルを指定できます。

[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]ボタンをクリックすることにより、[指定された拡張子のみ]ダイアログを開いてください。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てください。
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]ボタンをクリックすることにより、[指定された拡張子を除くすべて]ダイアログを開いてください。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てください。
リストの編集	[指定された拡張子のみ]または[指定された拡張子を除くすべて]オプションを選択した場合、[リストの編集]ボタンをクリックすることにより、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を表示してください。

圧縮ファイルのスキャン

圧縮ファイルのスキャンしたい場合は、[圧縮ファイルのスキャン]オプションを選択する必要があります。オプションを変更し、使用可能な圧縮ファイルタイプのリストから選択することができます。

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。[圧縮ファイルをスキャン]グループ内の[オプション]ボタンをクリックすることにより、[圧縮ファイル オプション]ダイアログを表示してください。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てください。

タイプを選択

スキャン可能な現在サポートされている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)
- Microsoft インストーラ形式ファイル (.MSI)
- Microsoft Office 文書の埋め込みファイル

タイムアウト値を指定

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して選択します。

トレース ファイルのサイズを指定

トレース ファイルのサイズをメガバイト (MB) 単位で指定できます。デフォルト値の 0 ではトレースが行われません。コンピュータ・アソシエイツのテクニカル サポートから指示されない限り、トレースを有効にしないでください。選択するにはドロップダウン矢印を使用してください。

デバッグ レベルを指定

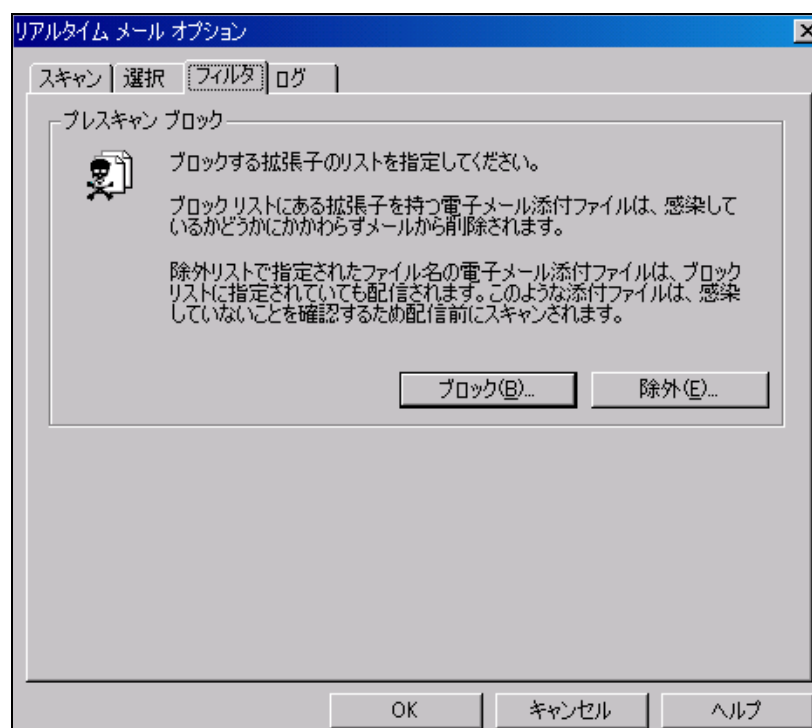
デバッグ レベルは 1~3 の範囲で指定できます。選択するにはドロップダウン矢印を使用してください。

レベル	定義
1	最小限の情報。通常、メール オプションの開始時と停止時。
2	中間の情報。すべての STOREVS.DLL デバッグ情報を含む。
3	1 と 2 のすべての情報と、ARCLIB.DLL 内と INOSCAN.DLL 内のすべての情報を含む。

フィルタ オプションの使用法

[フィルタ]タブでは、メール ボックスへの配信を拒否するか、または配信拒否から除外する電子メールの添付ファイルの拡張子を指定できます。

[フィルタ]タブ オプションについては以下に説明します。



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の添付ファイルの拡張子を指定できます。

ブロック

このボタンをクリックすることにより、[ブロック対象拡張子リスト]ダイアログを開いてください。[ブロック対象拡張子リスト]ダイアログにて、ブロックする拡張子のリストに、電子メールの添付ファイルの拡張子を追加してください。ファイルの末尾の文字列も指定できます。たとえば virus.com は、myvirus.com と another_virus.com をブロックします。ブロック リストにある拡張子を持つ電子メールの添付ファイルは、[ファイル処理]の設定にかかわらず、メールから除去されます。

除外

[除外]ボタンをクリックすることにより、[ブロックから除外]ダイアログを開いてください。[ブロックから除外]ダイアログにて、除外リストに含める、電子メールの添付ファイルを指定してください。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。

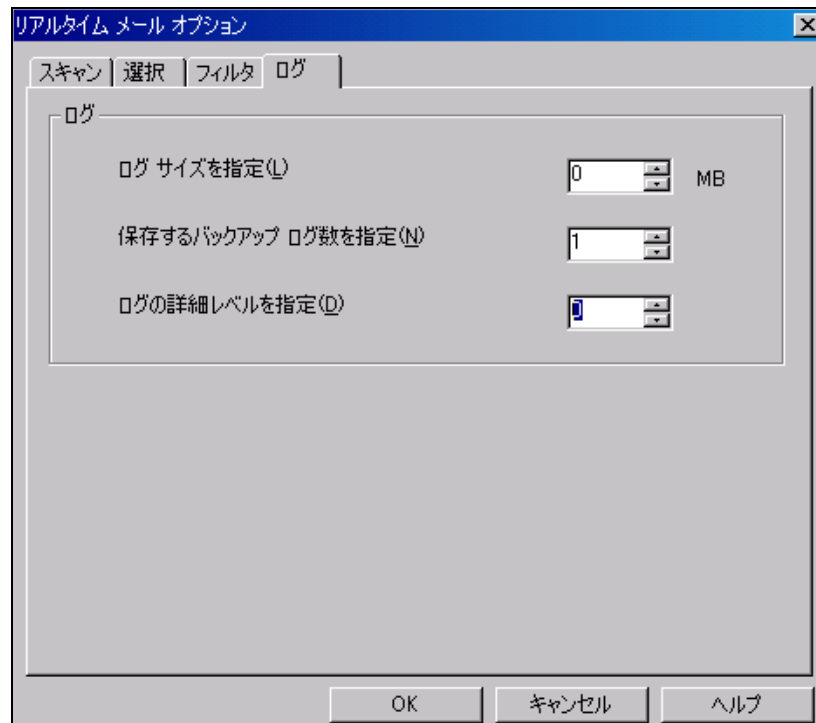
拡張子はブロックされているが、ファイル名が除外されている電子メールの添付ファイルは、添付先の電子メールとともに配信されます。添付ファイルは配信される前にスキャンされます。

注： スペルは正確でなければなりません。

ログ オプションの使用法

[ログ]タブでは、ログのサイズ、保存しておくバックログの数、ログの詳細レベルを指定できます。

[ログ]タブ オプションについて以下に説明します。



ログ サイズを指定

ドロップダウン矢印を使用して任意のログ サイズを選択してください。選択した値はログ ファイルの大きさをメガバイト単位で表します。

保存するバックアップ ログ数を指定

ドロップダウン矢印を使用して、保存しておきたいログの数を指定してください。ログは、InXO####.log (####は 0000、0001 など) という形式で、ウイルス対策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。

ログの詳細レベルを指定

ドロップダウン矢印を使用してログの詳細レベルを指定してください。

- 0 = 感染ファイルに関するログ
- 1 = 全スキャン ファイルに関するログ
- 2 = 現在はレベル 1 と同じ

索引

M

Microsoft Exchange Option
機能, 2-1
紹介, 1-1

A

圧縮ファイル
オプション, 2-8
スキャン, 2-7
タイプを選択, 2-8

アンチウイルス ニュースレター, 1-3

I

移動, ファイル処理, 2-3

インストールの要件, 1-3

カ

拡張子
スキャンをブロックする, 2-10
ブロックから除外, 2-11

ク

駆除処理オプション, 2-4

サ

削除
ファイル処理, 2-3

シ

シグネチャ ファイルのダウンロード, 1-3

システムトレイ
メール オプションへのアクセス, 2-1

詳細モード, 2-3

処置オプション, 2-3

ス

スキャン エンジン, 2-2

スキャン タブ, 2-1

セ

選択オプション

[選択]タブ, 2-6

ツ

通常ファイルのスキャン, 2-7

通常モード, 2-3

テ

テクニカル サポート, 1-3

電子メールの保護を行う

 メール オプションを有効にする, 2-5

ネ

ネットワークの保護, 1-3

ハ

配信拒否, 2-10

バックアップ システム, 1-3

フ

ファイル拡張子

 指定された拡張子のみ, 2-7

 指定された拡張子を除くすべて, 2-7

 すべて, 2-7

 リストの編集, 2-7

ファイル処理, 修復, 2-4

ファイル名の変更, ファイル処理, 2-3

ブロック拡張子, 2-10

メ

メール オプションへのアクセス, 2-1

メール オプション メニュー, 2-1

メッセージング システム, 1-2

モ

モード

 通常または詳細, 2-3

ヨ

要件

 ハードウェアとソフトウェア, 1-3

レ

レポートのみ, ファイル処理, 2-3