

eTrust[®] Antivirus Lotus Notes / Domino 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: 概要

Lotus Notes Domino 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
ネットワークの保護と Lotus Notes/Domino Option システム	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: 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	2-1
スキャン オプションの使用法	2-2
検出	2-3
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	2-4
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
フィルタ オプションの使用法	2-8
プレスキャンブロック	2-8
通知の配信先	2-9

索引

Lotus Notes/Domino Option は、文書内の感染と電子メール メッセージの添付ファイルでの感染を、弊社のウイルス対策ソフトウェアでスキャンできるようにするための、仲介役を果たします。感染した Lotus Notes の添付ファイルを自動的に検出できます。このオプションはまた、感染が検出されるとホスト メッセージング システムを通してユーザに通知します。

注： Windows NT 上で Lotus Notes/Domino 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。

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 ウィルス アナライザ

Word.Concept ウィルスなど急速に伝染するマクロ ウィ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。このときウイルスが処置され警告が送信されます。

- 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。

- 使いやすいオプション

検出と警告のオプションは簡単に指定できます（たとえば、感染ファイルを修復して警告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、感染ファイ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急速に蔓延させてしまうため、セキュリティ上の穴に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。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、検出されたすべてのウイルスの49パーセントがマクロ 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) にも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、急速に感染を広げ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へと保存された場合、弊社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。

ネットワークの保護と Lotus Notes/Domino Option システム

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、以下のことをしてください。

- 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書き込み禁止に設定してください。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 ディスクからどのファイルをコピーするときも、コピーの前にフロッピー ディスクをウイルス スキャンしてください。
- ウィルス スキャンを問題なく実行した後に、BrightStor Enterprise Backup または 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 ウィ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 Lotus Notes/Domino 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

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 以降
- Lotus Server 4.6x または R5
- ベースとなる弊社のウイルス対策ソフトウェア 6.x SP1 に適合する Lotus Notes/Domino
- Lotus Server の場合は、2MB 以上のディスク空き容量のほかに、Lotus Notes/Domino Option を実行できる十分なディスク スペース

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、弊社ウイルス対策ソフトウェア付属の『管理者ガイド』で説明されています。

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、ほかのユーザに感染ファイルを送ろうとするまさにそのときを補足するので、感染が広がる前に防げます。

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、弊社のウイルス対策メールボックスを通過してから、Lotus Notes/Domino Option サーバに送られます。弊社のウイルス対策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し、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て、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・アソシエイツのウイ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]を選択してください。[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

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 エンジンとは、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。システム管理者はこの設定を変更できます。

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。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できます。感染があるかどうかを調べてから、感染した電子メール添付ファイルをどう処置するかを判断したい場合は、[レポートのみ]を選択してください。電子メール添付ファイルに感染がある場合は、Lotus Notes/Domino Option を使って 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あります。

ファイル処理	説明
レポートのみ	感染が検出されたときにそれをレポートします。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	感染ファイルが見つかったら、その名前を AVB 拡張子に変更します。同名の感染ファイルがある場合は、数字を 1 ずつ増やした拡張子が付けられます (#.AVB の形式で。たとえば、FILE.0.AVB、FILE.1.AVB)。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。

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。
ファイルの修復	感染ファイルの自動修復を試みます。[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。 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。

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 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 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ます。
駆除に失敗した場合の処理	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、またはその両方を行います。[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。

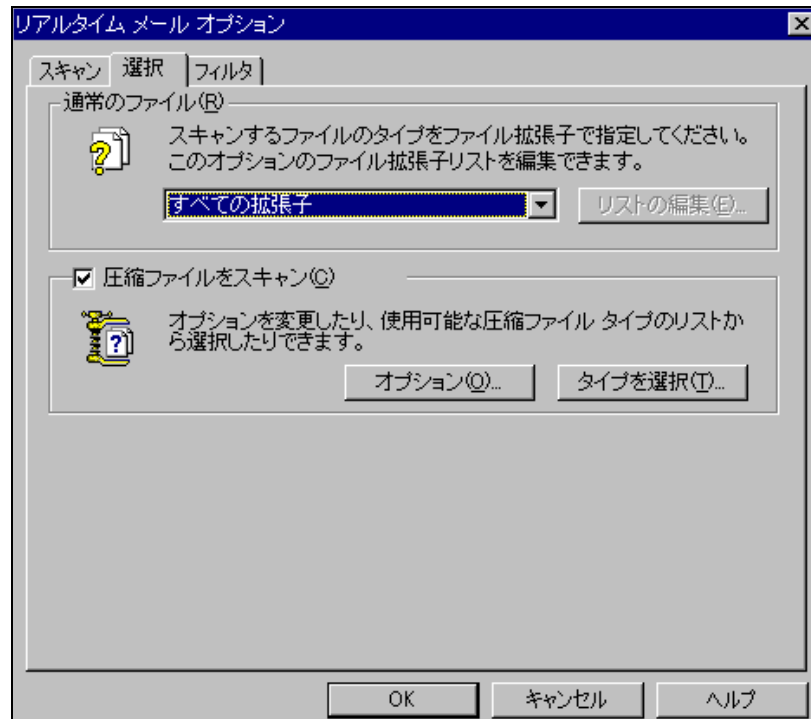
メール オプションを有効にする

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。

選択オプションの使用法

[選択]オプションでは、ファイル拡張子を選択して、それをスキャンに含めるか除外するかを指定できます。

[選択]タブで使用できるオプションを以下に説明します。



通常のファイル

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]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、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。

圧縮ファイルをスキャン

圧縮ファイルをスキャンしたい場合は、[圧縮ファイルをスキャン]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したりできます。

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。

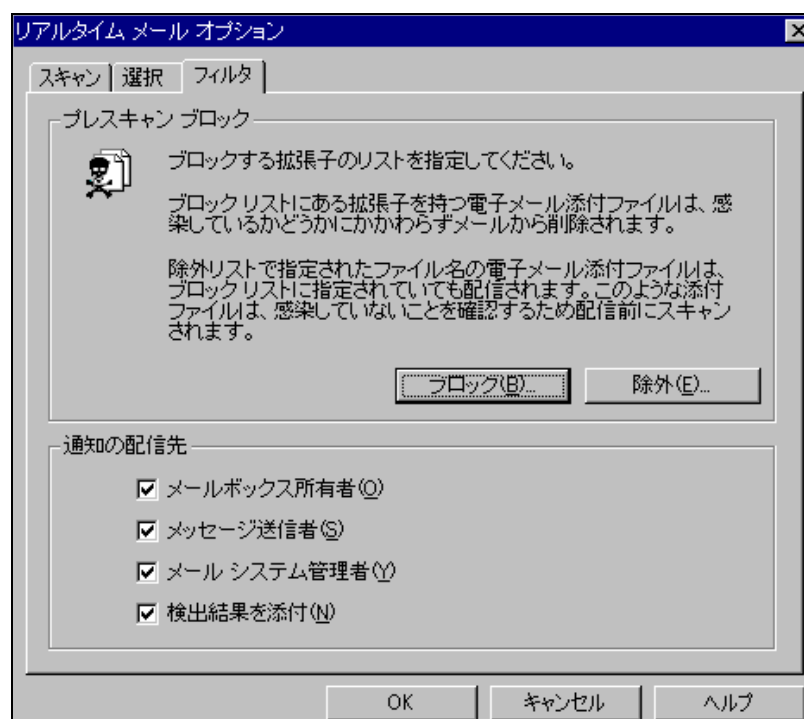
- ARJ
- GZIP
- JAVA アーカイブ
- LHA

- 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)
- TNEF カプセル化電子メール

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

[ブロック]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。

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。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。

通知の配信先

[通知の配信先]の下のオプションを選択するには、使用するオプションの隣にあるボックスにチェックマークを付けてください。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、メールの添付ファイルに感染の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とれます。
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。

索引

L

Lotus Notes Option

概要, 1-1

機能, 1-1

Lotus Notes Server, 2-1

A

圧縮ファイル

オプション, 2-6

スキャン, 2-6

タイプを選択, 2-6

I

移動、ファイル処理, 2-4

インストールの要件, 1-3

カ

拡張子

ブロックから除外, 2-9

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, 2-3

スキャン タブ, 2-1

セ

選択オプション

[選択]タブ, 2-5

ツ

通常のファイルのスキャン, 2-6

通常モード, 2-3

通知オプション, 2-9

テ

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, 2-4

ネ

ネットワークの保護, 1-3

フ

ファイル拡張子

指定された拡張子のみ, 2-6

指定された拡張子を除くすべて, 2-6

すべて, 2-6

リストの編集, 2-6

ファイル処理, 修復, 2-4

ファイル名変更, ファイル処理, 2-3

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