Cisco IronPort Email Security Plug-in 7.1
管理者ガイド

Cisco IronPort Email Security Plug-in 7.1 Administrator Guide

2010 年 12 月 6 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco IronPort Email Security Plug-in 7.1 管理者ガイド

CONTENTS

CHAPTER 1

Cisco IronPort Email Security Plug-in の準備

ここでは、次の項目を取り上げます。

今回のリリースでの変更点

このリリースでは、頻繁に使用される電子メール セキュリティ プラグインを 2 つ（Cisco Encryption Plug-in および Cisco Reporting Plug-in）を組み合わせて使用します。Cisco Encryption Plug-in は電子メール プログラムからのメッセージの暗号化を、Cisco Reporting Plug-in はスパム、ウイルス、または誤って分類された電子メールの報告を可能にします。この 2 つのプラグインを組み合わせることにより、電子メール セキュリティ プラグインに簡単にアクセスして変更できるようになります。また、電子メール セキュリティ プラグインのインストールおよび更新プロセスが合理化されます。さらに、Cisco IronPort Email Security Plug-in には、Windows インストーラをベースにした標準インストーラが用意されています。このインストーラは、応答ファイルを使用したサイレント インストールなど、標準 Windows インストーラのコマンドライン オプションをサポートします。

サポートされている構成

次の設定がサポートされています。

Cisco IronPort Email Security Plug-in 7.1.x	Outlook 2003	Outlook 2007	Outlook 2010	Notes 6.x	Notes 7.x	Notes 8.0.x	Notes 8.5.x
XP 32 ビット	認定	認定	認定	認定	認定	認定	認定
XP 64 ビット	適合	適合	適合	適合	適合	適合	適合
Vista 32 ビット	認定	認定	認定	適合	適合	適合	認定
Vista 64 ビット	適合	認定	認定	適合	適合	認定	適合
Windows 7 32 ビット	認定	認定	認定	適合	適合	認定	認定
Windows 7 64 ビット	適合	認定	認定	適合	適合	適合	認定
Citrix	未サポート	未サポート	未サポート	未サポート	未サポート	未サポート	未サポート

（注） Cisco IronPort Email Security Plug-in には、Windows Installer 2.0 以降が必要です。

関連ドキュメント

Encryption Plug-in を使用するには、Cisco IronPort Encryption アプライアンスを実行し、Encryption Plug-in と連携するよう正しく設定する必要があります。Cisco IronPort Encryption アプライアンスの設定方法の詳細については、次のマニュアルを参照してください。

- 『*IronPort AsyncOS for Email Encryption User Guide*』。このマニュアルでは、電子メールの暗号化の設定について説明しています。設定したプラグイン設定と連携する暗号化アプライアンスの設定方法を理解するのに役立ちます。

Cisco IronPort Email Security の動作についての理解を深めるために、電子メールをスパム、ウイルス、または非スパムとして分類する方法に関する基本情報を確認することを推奨します。詳細については、次のマニュアルを参照してください。

- 『*Cisco IronPort AsyncOS for Email Configuration Guide*』。このマニュアルでは、スパムおよびウイルスからの保護について説明しています。スパムおよびウイルス対策プラグインを採用することにより、SenderBase ネットワークの有効性を高めることができます。電子メールに「スパム」、「ウイルス」、または「非スパム」のマークを付けると、フィルタの有効性を高め、すべての Cisco IronPort アプライアンスのパフォーマンスを向上させることができます。

このマニュアルの使い方

このマニュアルは、Cisco IronPort Email Security Plug-in の機能について理解するためのリソースとしてご使用ください。マニュアルの内容は論理的な順序で構成されていますが、すべての章を読む必要はありません。目次および「このマニュアルの構成」（P.1-4）を読んで、ご使用の設定に関連する章を確認してください。

このマニュアルは、PDF 形式で電子的に配布されます。このマニュアルの電子バージョンは、Cisco IronPort カスタマー サポート ポータルで入手できます。また、アプライアンスの GUI で [Help] ボタンをクリックすると HTML オンライン ヘルプ ツールにアクセスできます。

このマニュアルの構成

第 1 章「Cisco IronPort Email Security Plug-in の準備」では、IronPort セキュリティ プラグインの概要について説明し、ネットワーク セキュリティ設定で主要機能および役割を定義します。最新リリースの新機能、その他の情報リソース、およびサポート問い合わせ情報について説明します。

第 2 章「概要」では、Reporting Plug-in および Encryption Plug-in について説明します。ここでは、各ツールの概要を示します。

第 3 章「一括インストールの実行」では、一括インストールの実行方法について説明します。応答ファイルの作成、インストールの実行、インストール前のファイルの変更の手順を示します。

第 4 章「Cisco IronPort Email Security Plug-in for Outlook の設定および使用方法」では、Cisco IronPort Email Security Plug-in for Outlook の設定手順について説明します。レポート プラグインおよび暗号化プラグインの設定手順も示します。

第 5 章「Cisco IronPort Email Security Plug-in for Lotus Notes の設定および使用方法」では、Cisco IronPort Email Security Plug-in for Lotus Notes の設定手順について説明します。レポート プラグインおよび暗号化プラグインの設定手順、Lotus Notes メール プログラムからプラグインを使用する方法も示します。

付録 A「Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書」では、Cisco IronPort 製品のライセンス契約について詳しく説明します。

印刷時の表記法

書体	意味	例
AaBbCc123	コマンド、ファイル、およびディレクトリの名前。画面に表示される出力。	`Please choose an IP interface for this Listener.` `sethostname` コマンドは、IronPort アプライアンスの名前を設定します。
AaBbCc123	（画面に表示される出力に対する）ユーザ入力。	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**

AaBbCc123	マニュアルのタイトル、新規用語、強調する用語、およびコマンド ライン引数。コマンド ライン引数の場合、イタリック体のテキストは実際の名前または値のプレースホルダです。	『*IronPort Quickstart Guide*』をお読みください。
		
		IronPort アプライアンスでは、発信パケットを送信するためにインターフェイスを独自に選択する*必要があります*。
		
		`Before you begin, please reset your password to a new value.`
		`Old password:` **`ironport`**
		`New password:` *`your_new_password`*
		`Retype new password:`
		`your_new_password`

詳細情報の入手先

IronPort では、Cisco IronPort Email Security Plug-in について理解を深めるために次のリソースを用意しています。

IronPort 技術トレーニング

Cisco IronPort Systems 技術トレーニング サービスは、Cisco IronPort セキュリティ製品およびソリューションの評価、統合、導入、保守、およびサポートに必要な知識とスキルを得られるよう支援します。

次のいずれかの方法で Cisco IronPort 技術トレーニング サービスにお問い合わせください。

トレーニング：登録およびトレーニング全般に関するお問い合わせ先は次のとおりです。

- http://training.ironport.com
- training@ironport.com

認定：証明書および認定試験に関するお問い合わせ先は次のとおりです。

- http://training.ironport.com/certification.html
- certification@ironport.com

ナレッジ ベース

次の URL から Cisco IronPort カスタマー サポート サイトの Cisco IronPort ナレッジ ベースにアクセスできます。

`http://www.cisco.com/web/ironport/knowledgebase.html`

（注） サイトにアクセスするには Cisco.com のユーザ ID が必要です。Cisco.com のユーザ ID をお持ちでない場合は、`https://tools.cisco.com/RPF/register/register.do` で登録できます。

ナレッジ ベースには、Cisco IronPort 製品に関するトピックについて豊富な情報が用意されています。

一般に、項目は次のカテゴリのいずれかに分類されています。

- **手順：**手順の項目では、Cisco IronPort 製品を使用して何かを実行する方法について説明します。たとえば、アプライアンスのデータベースをバックアップおよび復元する手順を示します。

- **問題と解決策：**問題と解決策の項目では、Cisco IronPort 製品の使用時に発生する可能性があるエラーや問題に対処します。たとえば、製品の新バージョンにアップグレードしたときにエラー メッセージが表示された場合の対処方法を示します。
- **参考資料：**参考資料の項目では、特定のハードウェアに関連するエラー コードなどの情報を一覧表示します。
- **トラブルシューティング：**トラブルシューティングの項目では、Cisco IronPort 製品に関連する一般的な問題を分析し、解決する方法について説明します。たとえば、DNS で問題が発生した場合に実行する手順を示します。

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。フォーラムにトピックを投稿して質問したり、他のシスコ ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

`https://supportforums.cisco.com`

Cisco IronPort カスタマー サポート

本サポートは、1 年中いつでも電話、電子メール、またはオンラインで請求できます。Cisco IronPort カスタマー サポートのサービス レベル契約の詳細については、サポート ポータルをご覧ください。

カスタマー サポートの営業時間外に緊急のサポートを必要とする重大な問題を報告する場合は、次のいずれかの方法で Cisco IronPort にご連絡ください。

米国フリー ダイヤル：1 (877) 646-4766

サポート サイト：`http://www.cisco.com/web/ironport/index.html`

サポートをリセラーまたは別のサプライヤから購入された場合、製品のサポートについてはそのリセラーまたはサプライヤに直接お問い合わせください。

サード パーティ コントリビュータ

IronPort AsyncOS に含まれているソフトウェアの中には、FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc.、およびその他のサード パーティ コントリビュータのソフトウェア使用許諾契約の条件および通知に基づいて配布されているものがあり、これらの条件はすべて IronPort ライセンス契約に組み込まれています。

契約の全文については、次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

IronPort AsyncOS 内のソフトウェアの一部は、Tobi Oetiker 氏の書面による明示的な同意を得て、RRDtool をベースにしています。

このマニュアルの一部は、Dell Computer Corporation の許可を受けて複製されています。このマニュアルの一部は、McAfee, Inc. の許可を受けて複製されています。このマニュアルの一部は、Sophos Plc の許可を受けて複製されています。

Cisco IronPort Email Security Plug-in の概要

Cisco IronPort Email Security Plug-in は、Outlook または Lotus Notes 電子メール プログラムにレポートと暗号化のメニューをインストールします。レポート プラグインを使用すると、受信したメールのタイプについてフィードバックできます（スパム、フィッシング、ウイルス メールの報告など）。暗号化プラグインを使用すると、ツールバーに [Encrypt Message] ボタンが表示されます。このボタンにより、電子メール プログラムから暗号化された電子メールを送信できます。

Cisco Security Plug-in をインストールすると、Outlook メール クライアントまたは Lotus Notes メール クライアントのコンポーネントがイネーブルになります。この単一のインターフェイスにより、エンドユーザはシームレスに問題のある電子メールを報告したり、電子メール プログラムから暗号化された電子メールを送信したりできます。これらのプラグインを組み合わせると、インストールが簡単になり、ユーザが変更できる単一のインターフェイスが提供されます。

レポート プラグインおよび暗号化プラグインは、ツールバー ボタンと右クリック コンテキスト メニューを使用してフィードバックおよび暗号化されたメッセージを送信できる便利なインターフェイスです。レポート プラグインを使用してメッセージを報告すると、メッセージが送信されたことを示すダイアログ ボックスが表示されます。暗号化プラグインを使用すると、電子メール メッセージのメニュー バーに [Encrypt Message] ボタンが表示されます。送信者はこのボタンを使用して、メッセージが企業から送信される前に、暗号化されてセキュリティ保護されるメッセージに簡単にマークを付けることができます。暗号化プラグインの機能は、暗号化ライセンスがある Cisco IronPort Email Security アプライアンスがあり、正しく設定されているかどうかによって異なります。

CHAPTER 2

概要

Cisco IronPort Email Security Plug-in は、Reporting Plug-in、Encryption Plug-in を含む複数の Cisco IronPort Email Security Plug-in をサポートするフレームワークです。

ここでは、次の項目を取り上げます。

Cisco IronPort Email Security Plug-in

Cisco IronPort Email Security Plug-in は、2 つのよく使用される電子メール セキュリティ プラグイン（Reporting Plug-in および Encryption Plug-in）で構成されます。Cisco Email Security は、Outlook または Lotus Notes に導入できます。Cisco IronPort Email Security Plug-in を導入すると、次のアプリケーションのいずれかまたは両方がインストールされます。

- **Reporting Plug-in**：Reporting Plug-in を使用すると、Outlook および Lotus Notes のユーザは、スパム、ウイルス、フィッシング メッセージなど、一方的に送りつけられる不要な電子メール メッセージについて、Cisco IronPort Systems にフィードバックできます。詳細については、「Reporting Plug-in」（P.2-2）を参照してください。
- **Encryption Plug-in**：Encryption Plug-in を使用すると、電子メール メッセージのメニュー バーに [Encrypt Message] ボタンが表示されます。送信者はこのボタンを使用して、メッセージが企業から送信される前に、暗号化されてセキュリティ保護されるメッセージに簡単にマークを付けることができます。詳細については、「Encryption Plug-in」（P.2-2）を参照してください。

Reporting Plug-in

Reporting Plug-in を使用すると、Outlook および Lotus Notes のユーザは、スパム、ウイルス、フィッシング メッセージなど、一方的に送りつけられる不要な電子メール メッセージについて、Cisco IronPort Systems にフィードバックできます。Cisco IronPort Systems は、このフィードバックを利用して不要なメッセージが受信ボックスに配信されないようにフィルタを更新します。

誤って分類されたメッセージ（スパムとマークされた正当な電子メール メッセージ）を、[Not Spam] ボタンを使用して Cisco IronPort Systems に報告することもできます。Cisco IronPort Systems は、このレポートを利用してスパム フィルタを調整し、有効性を向上させます。

このプラグインは、ツールバー ボタンと右クリック コンテキスト メニューを使用してフィードバックを送信できる便利なインターフェイスです。メッセージを報告すると、メッセージが送信されたことを示すダイアログボックスが表示されます。送信したメッセージ データは、Cisco IronPort フィルタを改善するために自動システムによって使用されます。メッセージ データを送信することで、受信ボックス内の一方的に送りつけられる電子メールを減らすことができます。

Encryption Plug-in

Encryption Plug-in を使用すると、電子メール メッセージのメニュー バーに [Encrypt Message] ボタンが表示されます。送信者はこのボタンを使用して、メッセージが企業から送信される前に、暗号化されてセキュリティ保護されるメッセージに簡単にマークを付けることができます。Encryption Plug-in は、機能している設定済み Cisco IronPort Encryption アプライアンス、および Cisco IronPort Email Security アプライアンス（ネットワーク内にある場合）で動作するように設計されています。Encryption Plug-in に使用する設定は、これらのアプライアンスの設定と併せて設定する必要があります。これらのアプライアンスで同じ設定を使用しないと、暗号化されたメッセージの送信時に問題が発生することがあります。

プラグインのインストール

ユーザ グループ向けに Cisco IronPort Email Security Plug-in をインストールする場合、サイレント インストールを実行できます。サイレント インストールでは、エンド ユーザに入力を要求することなくインストールを実行できます。Cisco IronPort Email Security Plug-in のサイレント インストールを実行するには、応答ファイル（インストール プロセス中に提示されるすべての質問に対する応答が含まれるテキスト ファイル）を作成する必要があります。この応答ファイルを使用して、Systems Management Server（SMS）や System Center Configuration Manager（SCCM）などの Systems Management ソフトウェアによってインストールを実行します。サイレント インストールの詳細については、第 3 章「一括インストールの実行」を参照してください。

Cisco IronPort Email Security Plug-in の設定

Cisco IronPort Email Security Plug-in のインストール後、Outlook の場合は [Tools] > [Options] >[Cisco Email Security] メニューから、Lotus Notes の場合は [Actions] > [Cisco Email Security] メニューから、設定を変更できます。

Reporting Plug-in または Encryption Plug-in を変更することも、両方のプラグインに影響を及ぼす汎用オプションを変更することもできます。たとえば、Encryption Plug-in と Reporting Plug-in の両方でロギングをイネーブルにしたり、電子メールに暗号化のマークを付ける方法を変更したりできます（これらの設定は Cisco IronPort Encryption アプライアンスに対応している必要があります）。

Outlook の設定を変更する場合は、第 4 章「Cisco IronPort Email Security Plug-in for Outlook の設定および使用方法」を参照してください。

Lotus Notes の設定を変更する場合は、第 5 章「Cisco IronPort Email Security Plug-in for Lotus Notes の設定および使用方法」を参照してください。

CHAPTER 3

一括インストールの実行

この章では、複数のデスクトップに一括インストールを実行する方法について説明します。ここでは、次の項目を取り上げます。

概要

ユーザ グループ向けに Cisco IronPort Email Security Plug-in をインストールするには、ローカル サイレント インストールを実行して、インストール中に使用する応答ファイルを作成する必要があります。サイレント インストールでは、エンド ユーザに入力を要求することなくインストールを実行できます。Cisco IronPort Email Security Plug-in の一括インストールを実行するには、応答ファイル（インストール プロセス中に提示されるすべての質問に対する応答が含まれるテキスト ファイル）を作成する必要があります。この応答ファイルを使用して、Systems Management Server（SMS）や System Center Configuration Manager（SCCM）などの Systems Management ソフトウェアによってインストールを実行します。

一括インストールを実行する基本的な手順は次のとおりです。

1. セキュリティ プラグイン（Desktop Encrypt Plug-in for Outlook、Desktop Flag Plug-in for Outlook、IronPort Plug-in for Outlook、IronPort Plug-in for Lotus Notes など）を構成する旧バージョンのプラグインをアンインストールします。または、Cisco IronPort Email Security Plug-in の現在実行しているバージョンをアンインストールします。
2. インストールする前に、Outlook または Lotus Notes をシャット ダウンします。
3. ローカル バージョンのインストールを実行して応答ファイルを作成し、応答ファイルが正しく作成されたことを確認します。「応答ファイルの作成」（P.3-2）を参照してください。
4. 応答ファイルが作成されたら、ローカル マシンにインストールした Cisco IronPort Email Security Plug-in をアンインストールします。次のステップでプラグインを再インストールして応答ファイルをテストします。
5. 作成した応答ファイルを使用して、ローカル マシンでインストールを実行します。Outlook または Lotus Notes に正しくインストールされたことを確認します。
6. インストールを確認したら、System Center Configuration Manager（SCCM）などの Systems Management ソフトウェアを使用して目的のコンピュータに一括インストールを実行します。SCCM を使用してインストールを実行するには、「SCCM を使用した一括インストールの実行」（P.3-4）を参照してください。

応答ファイルの作成

応答ファイルを作成するには、応答をファイルに記録する特別なオプションを使用してプラグインのインストールを実行します。記録された応答を使用して応答ファイルが作成されたら、インストール中に応答ファイルを使用して Cisco IronPort Email Security Plug-in をインストールするすべてのコンピュータでインストールに関する一連の質問に自動的に応答できます。

ステップ 1　応答ファイルを作成するには、**/r** キー オプションを使用してコマンド ラインからインストールを実行します。**/r** キー オプションは、結果を応答ファイルに記録するように InstallShield に指示します。デフォルトでは、InstallShield は応答ファイルを次の名前で次の場所に保存します。

c:¥windows¥setup.iss

ステップ 2　応答ファイルの場所を指定するには、**/f1** オプションを使用します。**/f1** オプションにより、代替応答ファイル名およびパスを指定できます。たとえば、コマンドラインから次のコマンドを実行すると、InstallShield は応答を C ドライブの *install_034.iss* ファイルに書き込みます。

C:¥Users¥user1¥Desktop¥CiscoEmailSecurity.7.1.0.34.exe /r /f1"C:¥install_034.iss"

C:¥Users¥user1¥Desktop¥CiscoEmailSecurity.7.1.0.34.exe は .exe ファイルへのパスです。

/s /v /qn /f1 のように、キーの間（各スラッシュの前）にスペースがあることを確認します。

.exe ファイル名および *.iss* ファイル名はファイル名の例です。.exe ファイル名が上記のファイル名と異なっていても、インストールには影響しません。

各インストール ステップを実行すると、一括インストール中に応答として使用される応答ファイルに応答が保存されます。

ヒント　**/f1** オプションを使用してパスとファイル名を変更する場合は、絶対パスを入力することを推奨します。また、応答ファイルの作成時に **/f1** オプションを使用した場合は、サイレント インストールを実行するときに応答ファイルへのパスを指定する必要があります（**/s** オプションを使用）。

ステップ 3　*install_file.iss* が作成されたことを確認します。

ステップ 4　*install_file.iss* が作成されたことを確認したら、プラグインをアンインストールします（コマンド ライン パラメータおよびキーを使用しない）。

ステップ 5　ローカル コンピュータでインストーラを実行して応答ファイルをテストします。そのためには、コマンド ラインから次を実行します。

C:¥Users¥user1¥Desktop¥CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"C:¥install_034.iss"

/s - は setup.exe をサイレントにします。

/v - は MSI パッケージにパラメータを渡します。

/qn - は *setup.exe* 以外をサイレントにします。

/f1 - は、ここにある応答ファイルを使用します。

ステップ 6　電子メール プログラム（Outlook または Lotus Notes）を開いて、Cisco IronPort Email Security Plug-in が正しくインストールされたことを確認します。

（注）　*install_file.iss* が作成されると、Cisco IronPort Email Security Plug-in を更新するときに使用することもできます。

SCCM を使用した一括インストールの実行

インストールを開始する前に、Cisco IronPort Email Security Plug-in をインストールするクライアント マシンで次の手順を完了します。

- クライアント マシンに .Net 3.5 をインストールします（インストール プロセスでは不足しているフレームワークを必要に応じてダウンロードしてインストールしますが、事前に .Net 3.5 をインストールしておくとインストールがより迅速に行えます）。
- Outlook または Lotus Notes をシャット ダウンします。
- Cisco IronPort Email Security Plug-in の現行バージョンをアンインストールします（インストールされている場合）。
- セキュリティ プラグイン（Desktop Encrypt Plug-in for Outlook、Desktop Flag Plug-in for Outlook、IronPort Plug-in for Outlook、IronPort Plug-in for Lotus Notes など）を構成する旧バージョンのプラグインをアンインストールします。
- *install_file.iss* ファイルが作成されていることを確認します。「応答ファイルの作成」（P.3-2）を参照してください。

インストールを開始する前に、SCCM で次の条件を満たしていることを確認します。

- Cisco IronPort Email Security Plug-in をインストールするクライアントのリストの収集を作成したこと。

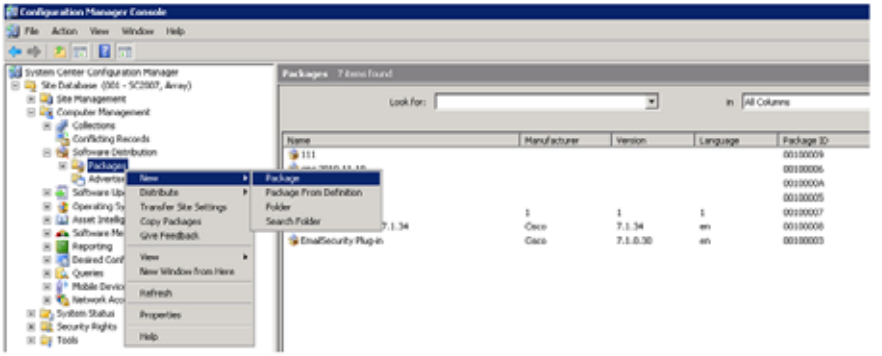
インストールの実行手順

ステップ 1　ネットワーク共有フォルダを作成し、ユーザがアクセスできるようにします。

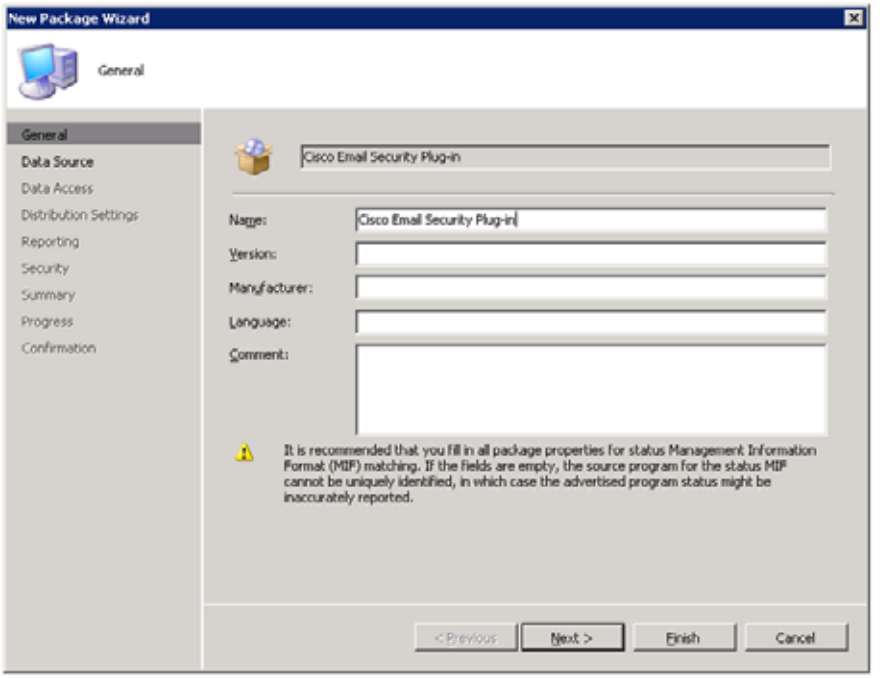
ステップ 2　インストーラと *install_file.iss* ファイルをこのフォルダに配置します。

ステップ 3　SCCM 管理ツールを開きます。

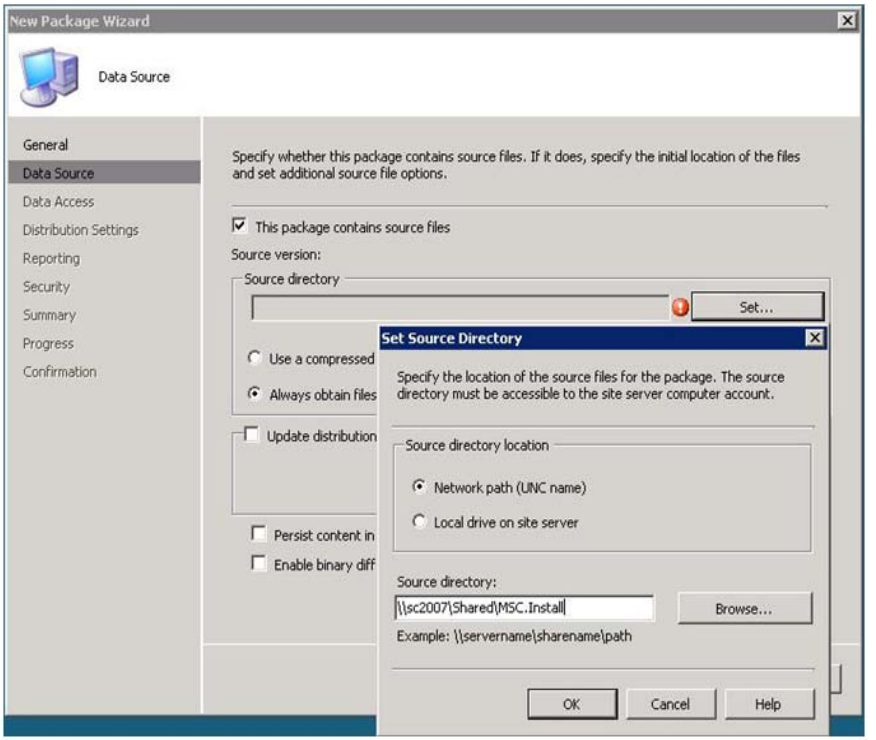
ステップ 4　新しいソフトウェア配布パッケージを作成します。



ステップ 5　パッケージ名を入力して、[Next] をクリックします

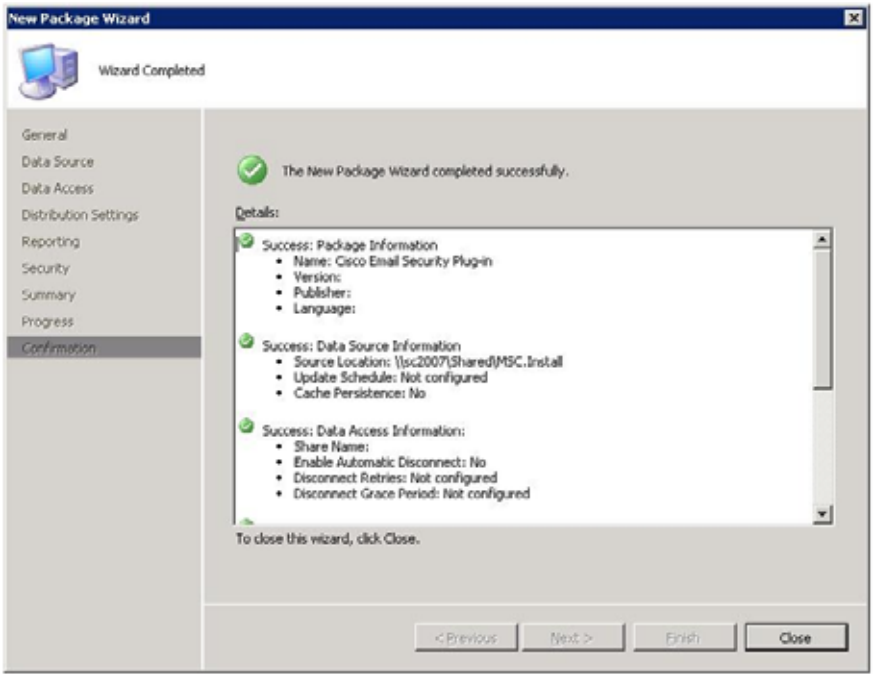


ステップ 6　ネットワーク共有フォルダへのパスを入力して、ステップ 1 で作成したネットワーク ソース ディレクトリを指定します。フォルダへのパスを入力するか、フォルダを参照します。[Next] をクリックします。

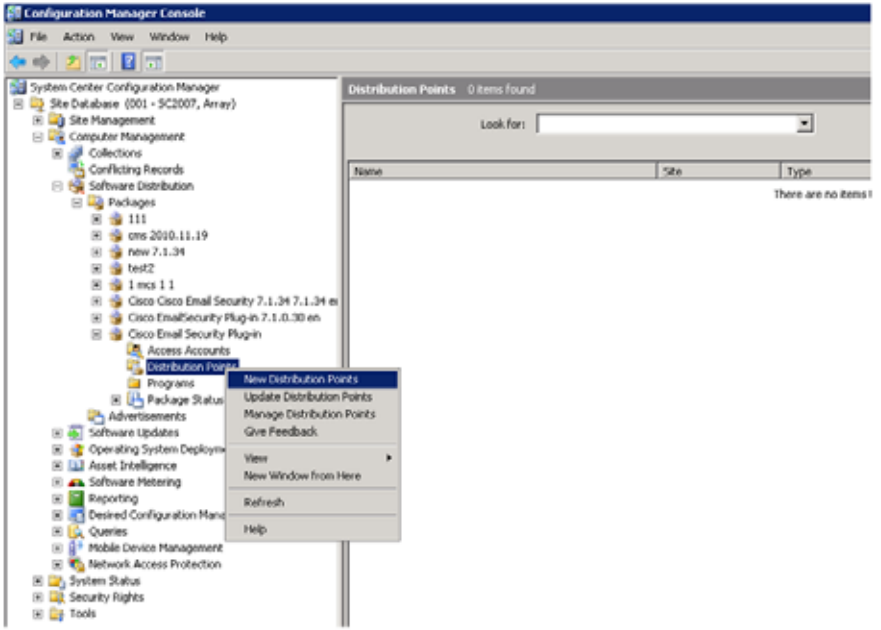


ステップ 7　[New Package Wizard] で次のステップに進み、[Next] をクリックします。

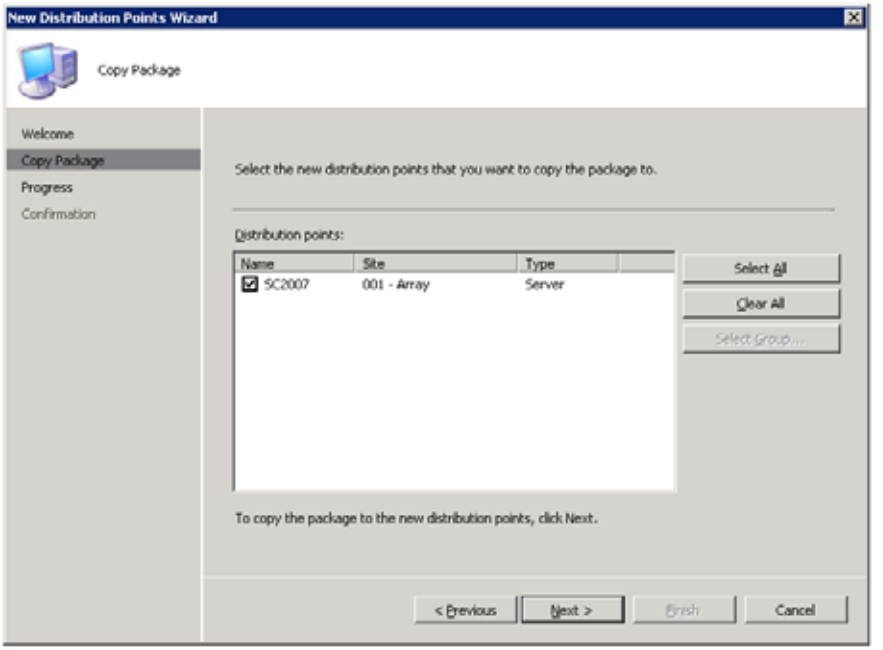
ステップ 8　[New Package Wizard] が正常に完了したことを確認して、[Close] をクリックします。



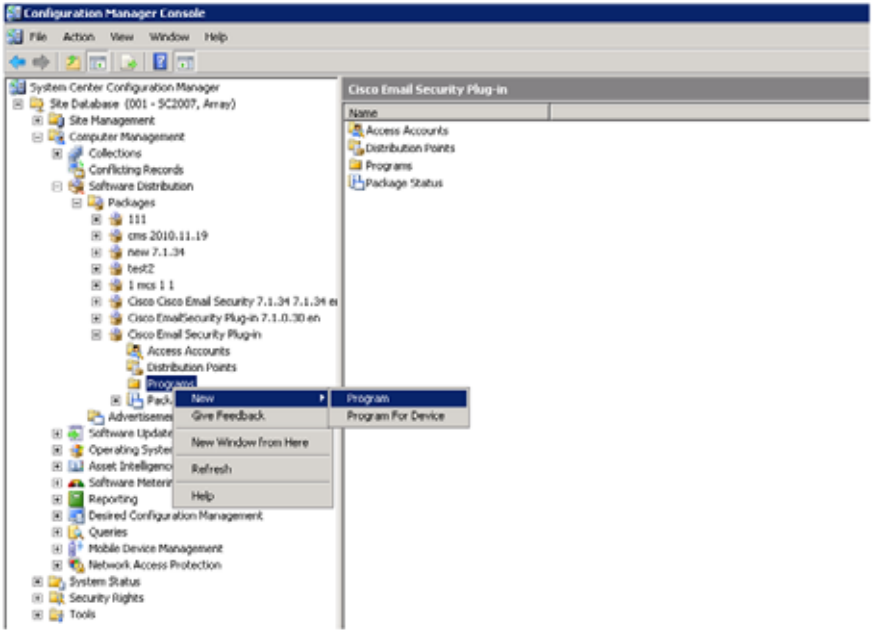
ステップ 9　新しい分散ポイントを作成し、[Welcome] ページの [Next] をクリックします。



ステップ 10　新しい分散ポイントを選択します。[New Distribution Points Wizard] で以降のページをクリックして、[Close] をクリックします。



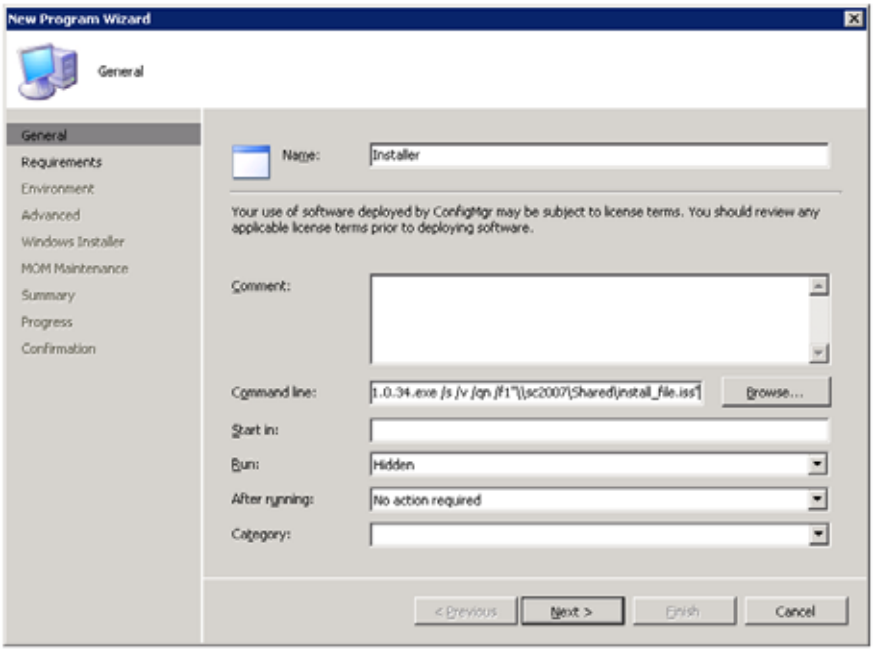
ステップ 11　新しいプログラムを作成します。



ステップ 12　コマンド ラインで、プログラム名と次のコマンドを入力します。

¥¥sc2007¥Shared¥CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"¥¥sc2007¥Shared¥install_file.iss"

¥¥sc2007¥Shared¥CiscoEmailSecurity.7.1.0.34.exe は、ネットワーク共有フォルダ内の .exe ファイルへのフル ネットワーク パスです ("¥¥sc2007¥Shared¥install_file.iss")。



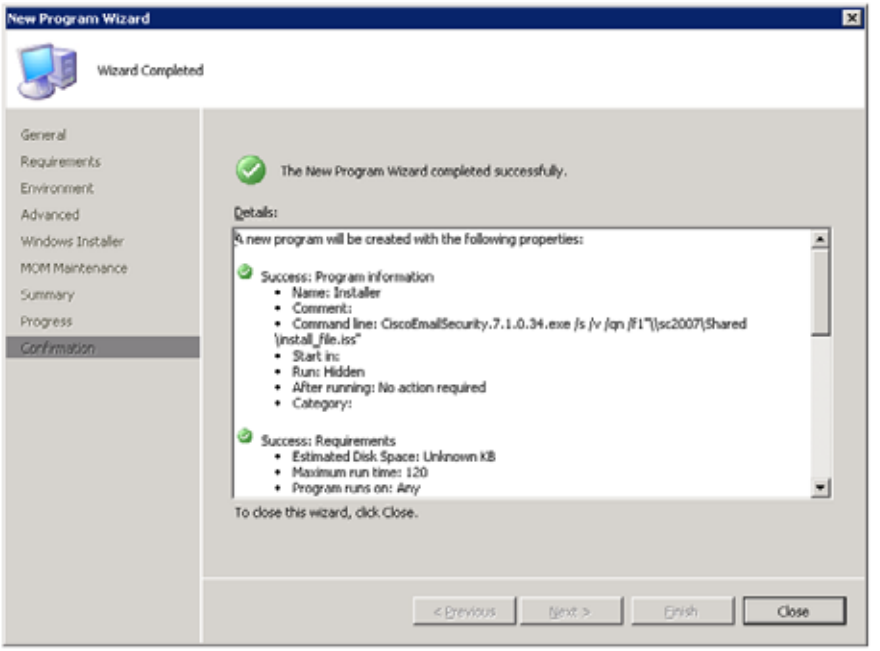
ステップ 13　[Run] フィールドで [Hidden] を選択し、[Next] をクリックします。

ステップ 14　要件ページをクリックして、[Next] をクリックします。

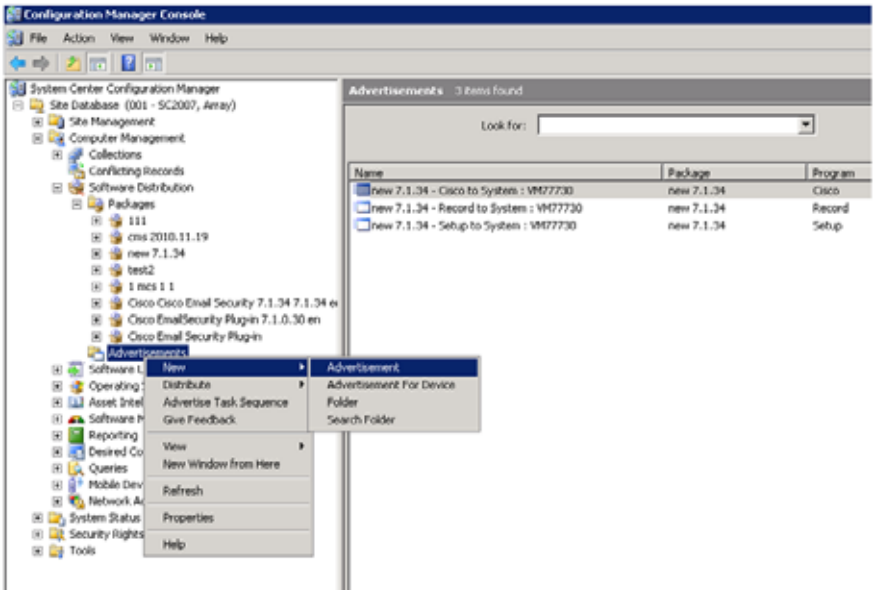
ステップ 15　次の環境オプションを選択します。

- [Program can run]：ユーザのログイン時に限ります。
- [Run mode]：ユーザの権限で実行するか、またはユーザが新しいソフトウェアのインストールに必要な権限を持っていない場合は管理権限で実行します。

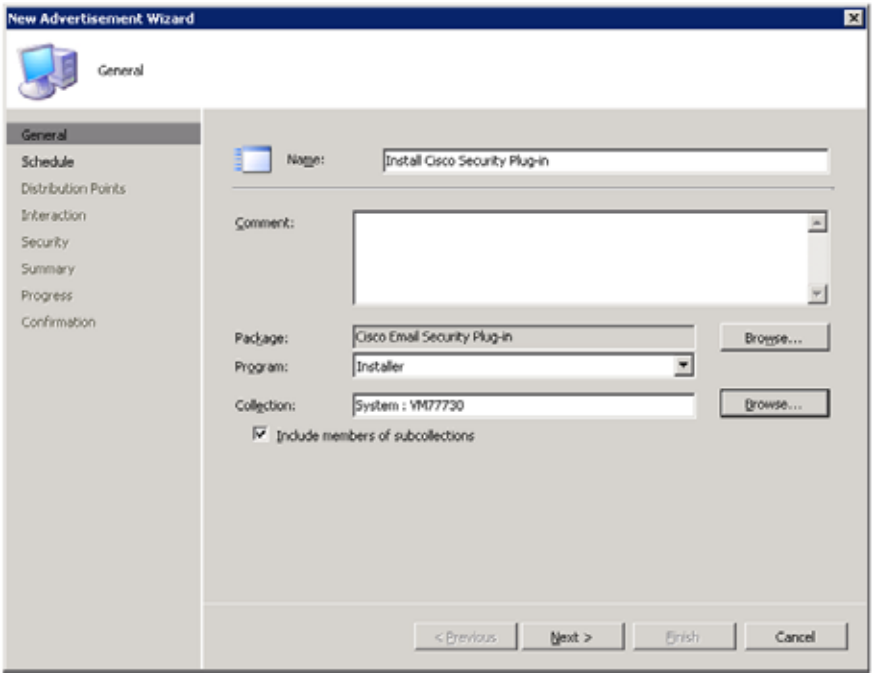
ステップ 16　[New Program Wizard] が正常に完了したことを確認して、[Close] をクリックします。



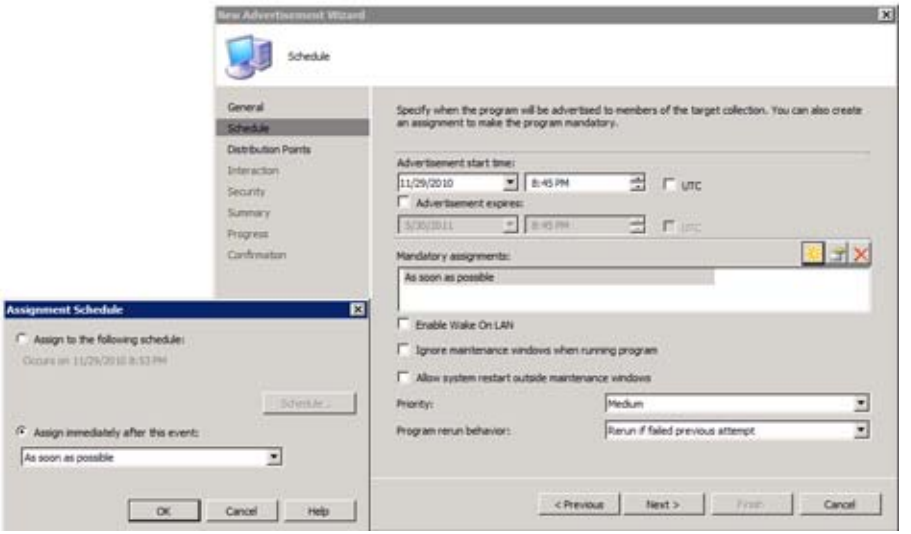
ステップ 17　新しいアドバタイズメントを作成します。



ステップ 18　名前を入力し、作成したパッケージとプログラムを選択します。プラグインをインストールするクライアントのグループが含まれる収集を選択します。[Next] をクリックします。



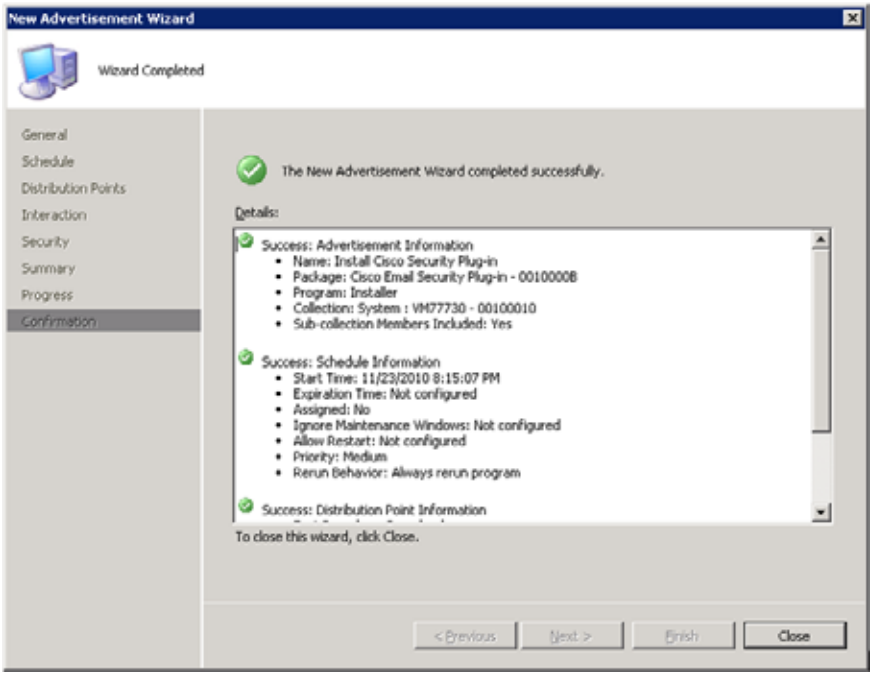
ステップ 19　割り当てを必須として設定します。[Next] をクリックします。



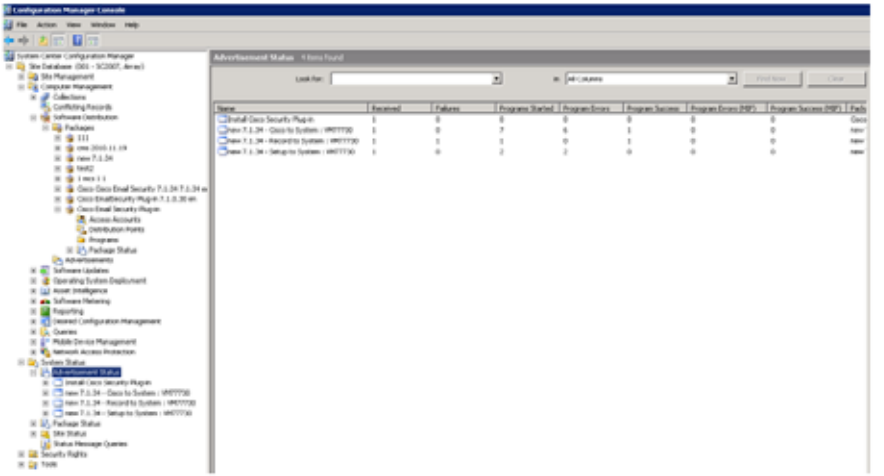
ステップ 20　必要に応じてスイッチを選択します。ただし、接続が遅い場合プログラムが起動しないので [Do Not Run Program] を選択しないでください。[Next] をクリックします。

ステップ 21　[New Advertisement Wizard] をクリックし、[Next] をクリックします。

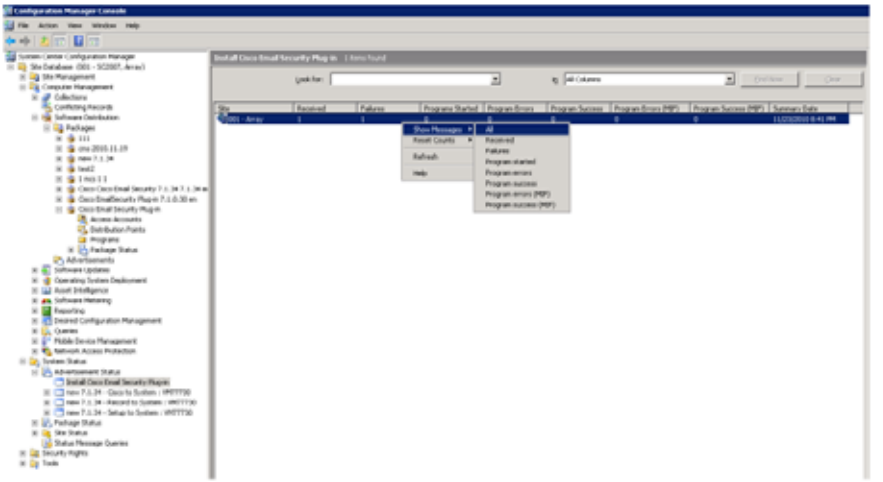
ステップ 22　[New Advertisement Wizard] が正常に完了したこと示す確認を表示して、[Close] をクリックします。



ステップ 23　[Advertisement Status] ウィンドウで [Advertisement Status] を表示します。



ステップ 24　アドバタイズメント レポートを作成して詳細を表示するには、コンテキスト メニューで [Show message] > [All] を選択します。エラーが発生した場合は、レポートを調べてエラーが発生した場所を確認できます。



プラグインのコンフィギュレーション ファイルの変更

Cisco IronPort Email Security Plug-in をインストールすると、設定データが作成され、次の XML ファイルに保存されます。

- **CommonConfig.xml**：ロギング情報など、Reporting Plug-in と Encryption Plug-in の両方に共通する基本的な設定データが保存されます。
- **Reporting.xml**：報告可能な最大メール サイズなど、Reporting Plug-in に関連する設定データが保存されます。
- **Encryption.xml**：フラグを付ける方法（たとえば、件名の文字列や x ヘッダー）など、Encryption Plug-in に関連する設定データが保存されます。

Cisco IronPort Email Security Plug-in インストーラを使用すると、デフォルトのコンフィギュレーション ファイルを変更できます。別のコンフィギュレーション ファイルを使用して、インストールに関する基本機能を変更することもでき

ます。たとえば、暗号化コンフィギュレーション ファイルでファイルにフラグを付ける方法を変更できます（この変更は、暗号化アプライアンスでもこの方法を変更できる場合に限り行います）。また、レポート コンフィギュレーション ファイルで、報告用の最大メール サイズ、報告後にファイルのコピーを保持するかどうかなどのデフォルト オプションの一部を変更できます。メイン コンフィギュレーション ファイルでは、ロギングをイネーブルまたはディセーブルにしたり、ログ レベルを変更したりできます。

カスタム コンフィギュレーション ファイルを使用する場合は、次の構文を使用してコマンド ラインから特別なキーを追加する必要があります。

```
CiscoEmailSecurity-7.0.0.005.exe /s
/v"UseCustomConfigs=\"\\smsarray\SMSClient\config\"" /qn
/"f1CiscoEmailSecurity.7.0.0.005.iss"
```

UseCustomConfigs コマンド ライン パラメータを使用すると、カスタム コンフィギュレーション ファイルを使用でき、インストール時に使用するコンフィギュレーション ファイルが保存されているフォルダへのパスを指定できます。

デフォルトでは、プラグインは Outlook および Lotus Notes の次の場所にある %appdata% ディレクトリ内のコンフィギュレーション ファイルをインストールします。

%appdata%\Cisco\Cisco IronPort Email Security Plug In\Outlook

%appdata%\Cisco\Cisco IronPort Email Security Plug In\LotusNotes

UseCustomConfigs コマンド ライン パラメータを使用すると、インストール用の独自のコンフィギュレーション ファイルの名前と場所を指定できます。ただし、有効性を維持するために元のファイルの構造を保持する必要があります。デフォルトのコンフィギュレーション ファイルは、config.zip ファイル内に配置されています。フォルダを作成する場合は、必ずファイルの構造を保持し、Outlook または Lotus Notes いずれかのコンフィギュレーション ファイルのサブフォルダを含めます（Outlook プラグインだけをインストールする場合は LotusNotes のフォルダを省略できます。また、LotusNotes プラグインだけをインストールする場合は Outlook のフォルダを省略できます）。

CHAPTER 4

Cisco IronPort Email Security Plug-in for Outlook の設定および使用方法

この章では、Cisco IronPort Email Security Plug-in for Outlook で利用可能な機能について説明します。Cisco IronPort Email Security Plug-in には、Outlook 電子メール プログラムと連携する数種類のセキュリティ プラグインが含まれます。ここでは、次の項目を取り上げます。

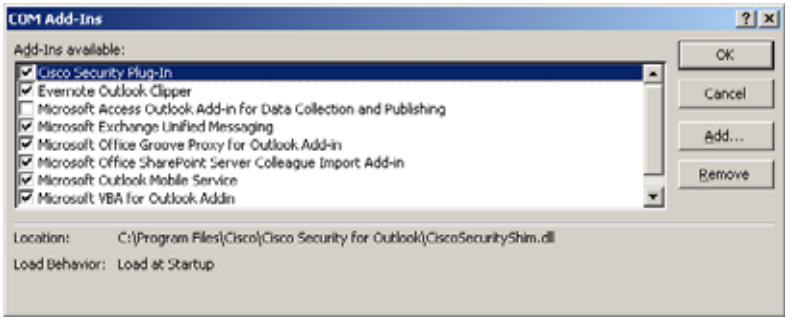
Cisco IronPort Email Security Plug-in for Outlook の一般的な設定

Cisco IronPort Email Security Plug-in は、Encryption Plug-in、Reporting Plug-in などの Cisco プラグインをサポートするプラットフォームです。Cisco IronPort Email Security Plug-in の一般的な設定は、[Options] ページで行います。

イネーブル / ディセーブル

デフォルトでは、Cisco IronPort Email Security Plug-in はインストール時にイネーブルになります。Cisco IronPort Email Security Plug-in をディセーブルにする場合は、次の手順を実行します。

- Outlook 2003/ 2007 では、[Tools] > [Options] > [Cisco Email Security] を選択します。
- Outlook 2010 では、[File] > [Options] > [Add-ins] を選択します。次に、[Manage] ドロップダウン リストから [COM Add-Ins] を選択し、[Go] をクリックします。



[COM Add-Ins] ウィンドウで、[Cisco IronPort Email Security Plug-in] チェックボックスをオフにして [OK] をクリックします。

Outlook プラグインの基本設定

基本設定は [Cisco Email Security] タブで設定します。Outlook 2003/2007 で [Cisco Email Security] タブを開くには、[Tools] > [Options] > [Cisco Email Security] を選択します。

または

Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] を選択します。

[Cisco Email Security] タブ

レポート、暗号化、およびロギングをイネーブルにするには、このタブで [Enable] チェックボックスをオンにします。さらに設定を行うには、[Reporting Options...]、[Encryption Options]、または [Logging Options...] ボタンをクリックします。問題解決時に診断ツールを使用すると、Cisco IronPort Email Security Plug-in でレポートを実行して、シスコのサポートに送信することもできます。

Reporting Plug-in

レポート設定により、Reporting Plug-in をイネーブルまたはディセーブルにできます。Reporting Plug-in を使用すると、受信した電子メールがスパム、フィッシング攻撃、またはウイルスの場合や、スパム（「ハム」と呼ばれることもあります）であると誤って分類された場合に、シスコに報告できます。

Cisco IronPort Email Security Reporting Plug-in for Outlook は、Outlook の [Options] ページで設定できます。

Reporting Plug-in for Outlook 2003/2007 をイネーブルにするには、[Tools] > [Options] > [Cisco Email Security] タブを選択し、[Cisco Email Security] タブの [Reporting] フィールドで [Enable] チェックボックスをオンにします。

または

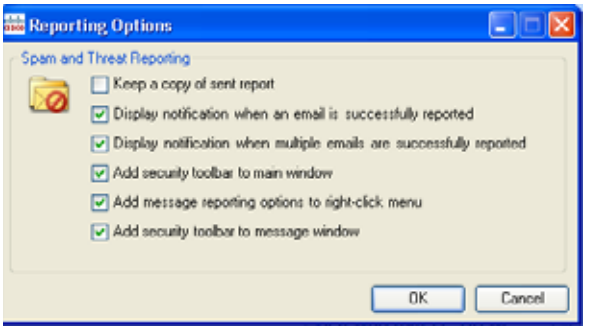
Reporting Plug-in for Outlook 2010 をイネーブルにするには、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] タブを選択し、[Cisco Email Security] タブの [Reporting] フィールドで [Enable] チェックボックスをオンにします。

[Reporting Options]

Outlook 2003/2007 で [Reporting Options] ページにアクセスするには、[Tools] > [Options] > [Cisco Email Security] タブを選択し、[Reporting Options] ボタンをクリックします。

Outlook 2010 で暗号化設定を変更するには、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] を選択し、[Reporting Options] ボタンをクリックします。

[Reporting Options] ページ



オプション

ここでは、設定可能なレポート オプションについて説明します。

- [Keep a copy of sent report] : デフォルトでは、スパムまたはウイルスの電子メール メッセージや、スパムまたはウイルスであると誤って分類された電子メール メッセージをシスコに報告すると、送信した報告電子メールは削除されます。このオプションを選択すると、電子メールは削除されません。
- [Display notification when an email is successfully reported] : 電子メールをスパムやウイルスとして報告すると、Outlook で正常に報告されたことを示すメッセージをダイアログボックスに表示できます。このオプションをオフにすると、このダイアログボックスは表示されません。
- [Display notification when multiple emails are successfully reported] : 複数の電子メールをスパム、ウイルス、フィッシング、非スパムとして報告すると、Outlook で正常に報告されたことを示すメッセージをダイアログボックスに表示できます。このオプションをオフにすると、このダイアログボックスは表示されません。
- [Add security toolbar to main window] : デフォルトでは、Cisco IronPort Email Security Plug-in をインストールすると、プラグイン ツールバーが Outlook のメイン ウィンドウに追加されます。このオプションをオフにすると、このツールバーは Outlook のメイン ウィンドウに追加されません。
- [Add message reporting options to right-click menu] : デフォルトでは、Cisco IronPort Email Security Plug-in をインストールすると、Reporting Plug-in のメニュー項目が Outlook の右クリック コンテキスト メニューに追加されます。このオプションをオフにすると、このメニュー項目は右クリック コンテキスト メニューに追加されません。
- [Add security toolbar to message window] : デフォルトでは、Cisco IronPort Email Security Plug-in をインストールすると、プラグイン ツールバーが電子メール メッセージ ウィンドウに追加されます。このオプションをオフにすると、このツールバーは電子メール メッセージ ウィンドウに追加されません。

Reporting Plug-in for Outlook の使用方法

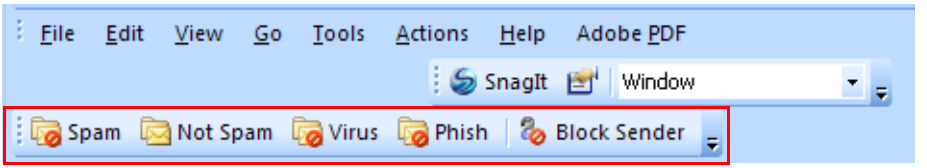
概要

Cisco IronPort Email Security Plug-in for Outlook を使用すると、受信ボックスに受信したスパム、ウイルス、またはフィッシング メールについてシスコにフィードバックできます。電子メール メッセージが誤って分類される場合（たとえば、スパムとして処理する必要がある場合など）、シスコに報告できます。シスコは、このフィードバックを利用して不要なメッセージが受信ボックスに配信されないようにフィルタを更新します。

このプラグインは、スパム、ウイルス、フィッシング、または誤って分類された電子メールを報告できるように、Outlook のメニュー バーおよび右クリック メッセージ メニューに便利なインターフェイスを提供します。電子メールを報告すると、レポートが送信されたことを示すメッセージが表示されます。報告したメッセージは、シスコの電子メール フィルタの改善に使用され、受信ボックスに一方的に送りつけられるメールを減らすことができます。

シスコへのフィードバック

このプラグインにより、Outlook に [Spam]、[Not Spam]、[Virus]、[Phish]、および [Block Sender] ボタンを含む新しいツールバーが追加されます（[Block Sender] は迷惑メール ボックスの電子メールはブロックしません）。



これらのボタンを使用して、スパム、ウイルス、およびフィッシング メールを報告します（フィッシング攻撃とは、不正な偽装 Web サイトにリンクしている電子メールです。この Web サイトは、受信者にクレジット カード番号、口座の名義人名とパスワード、社会保障番号など、個人の金融情報を漏洩させるように作られています。たとえば、*infos@paypals.com* から個人の銀行口座情報を不正に要求する電子メールが送信されてくることがあります）。

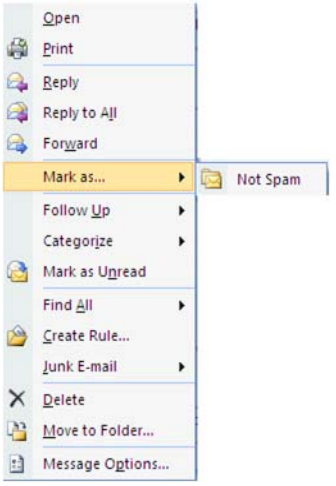
右クリックすると表示されるコンテキスト メニューを使用して、スパム、誤分類されたメール、ウイルス、フィッシングを報告することもできます。

メッセージ ウィンドウのボタンを使用して、スパム、ウイルス、フィッシング、誤分類されたメールを報告できます（誤分類されたメールとは、スパム、ウイルス、またはフィッシングであると誤ってマークが付けられたメールです）。

受信した電子メールがスパムであると誤って分類された（つまり、フィルタリングされ、[Spam] フォルダに配信された）場合、[Not Spam] ボタンをクリックして誤分類された電子メールを報告できます。これにより、この送信者からのメールは今後スパムとして分類されることはありません。

また、[Junk Email] フォルダのメッセージに誤分類とマークを付けるには、メッセージ ウィンドウの [Not Spam] ボタンをクリックします。

右クリック コンテキスト メニューを使用して、誤って分類されたメールにマークを付けることもできます。



Encryption Plug-in

暗号化設定は、[Cisco Email Security] ページにあります。Outlook 2003/2007 で暗号化設定を変更するには、[Tools] > [Options] > [Cisco Email Security] を選択し、[Encryption Options] をクリックします。

Outlook 2010 で暗号化設定を変更するには、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] を選択し、[Encryption Options] ボタンをクリックします。

Encryption Plug-in をイネーブルまたはディセーブルにするには、[Cisco Email Security] タブの [Encryption] フィールドで [Enable] チェックボックスをオンまたはオフにします。

[Encryption Options]

オプション

暗号化された電子メールを送信するオプション

送信メールを暗号化する場合、電子メールに暗号化のマーク（「フラグ」）を付ける必要があります。これにより、システム管理者によって作成されたフィルタは暗号化する必要があるメッセージを識別できます。

警告　システム管理者に連絡せずに、電子メールに暗号化のフラグを付ける方法を変更しないでください。これらの方法では Cisco IronPort Encryption アプライアンスの設定を変更して適切に動作するようにする必要があり、この変更を行えるのはシステム管理者だけです。

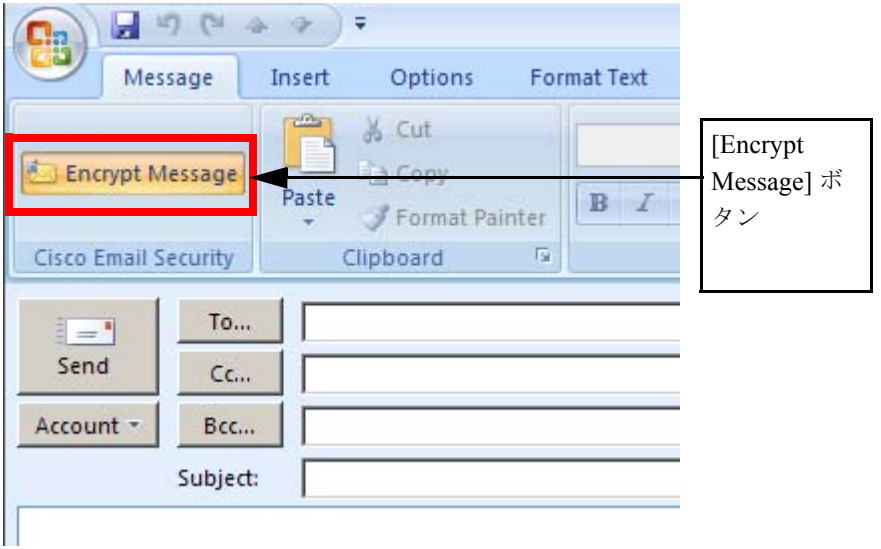
次のいずれかの方法で電子メールに暗号化のマークを付けることができます。

- [Flag Subject Text]：送信メールの [Subject] フィールドにテキストを追加して、電子メールに暗号化のフラグを付けることができます。[Subject] フィールドの先頭にテキストを入力して、電子メールを暗号化する必要があることを示します（デフォルト値は *[SEND SECURE]* です）。
- [Flag X-header name/value]：送信メールに x ヘッダーを追加して、電子メールに暗号化のフラグを付けることができます。1 つめのフィールドに x ヘッダーを入力します（デフォルト値は *x-ironport-encrypt* です）。2 つめのフィールドに *true* または *false* を入力します。*true* を入力した場合、指定された x ヘッダーのメッセージが暗号化されます（デフォルト値は *true* です）。

- **Outlook の秘密度に関するヘッダー** Outlook では、秘密度に関するヘッダーを追加して電子メールの暗号化を示すフラグをメッセージに付けることができます。この方法を選択すると、Outlook の秘密度に関するヘッダーを使用して電子メールに暗号化のマークを付けることができます。

暗号化された電子メールの送信

安全な電子メールを送信するには、電子メールの作成中に [Encrypt Message] ボタンを選択します。安全なメッセージを送信する前に、次のように [Encrypt Message] ボタンが選択されていることを確認します。

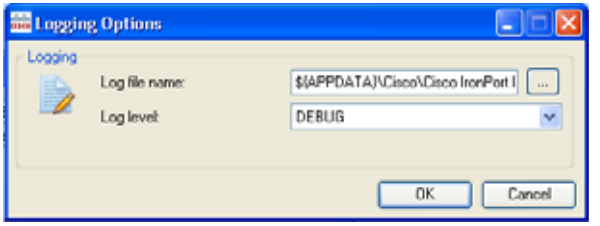


[Encrypt Message] ボタンは、電子メールの作成時に使用できます。

ロギング設定の変更

[Logging Options] ページを開くには、[Logging Options...] をクリックします。

[Logging Options]



オプション

[Logging] メニューから次のオプションを設定できます。

[Log file name]

%appdata%\Cisco に保存されるログ ファイルの名前を指定できます。ログ ファイル名には .log 拡張子が必要です。

[Log level]

ログ レベルは、ログ ファイルに記録される情報を指定します。次のいずれかのログ レベルを選択できます。

- [ERROR] : エラー メッセージおよび例外状況をログに記録します。
- [WARN] : [ERROR] で記録されるメッセージおよび警告メッセージがログに記録されます。
- [INFO] : 基本情報およびその他のステータス メッセージがログに記録されます。自動更新プロセスのステータス メッセージがログに記録されます。[WARN] および [ERROR] で記録されるメッセージもすべてログに記録されます。
- [DEBUG] : 設定に関する詳細情報がログに記録されます。[ERROR]、[WARN]、および [INFO] のすべてのエラー メッセージ、および問題のトラブルシューティングに役立つ可能性がある情報がログに記録されます。

特定の状況に必要なトラブルシューティングのレベルに基づいてログ レベルを変更できます。たとえば、Cisco IronPort Email Security Plug-in に関する問題が発生した場合、ログ レベルを [DEBUG] に設定すると、開発者が問題を再現して診断を実行できるように最大限の情報を提供できます。

診断ツールを使用したトラブルシューティング

Cisco IronPort Email Security Plug-in には、問題のトラブルシューティング時にシスコのサポートを支援する診断ツールが用意されます。診断ツールはプラグインから重要なデータを収集します。このデータをシスコのサポートに送信して問題解決を支援できます。

エラーが発生した場合や、修復プロセスでは解決できない Cisco IronPort Email Security Plug-in に関する問題が発生した場合に、診断ツールを使用します。また、診断ツールを使用すると、不具合の報告時にシスコのエンジニアと重要情報を共有することもできます。

注：エラーが発生した場合、トラブルシューティングのヒントの「Diagnostic」の項を参照してください。

Cisco IronPort Email Security 診断ツールにより収集されるデータ

診断ツールは、ご使用のコンピュータから次の情報を収集します。

- 一部の COM コンポーネントに関する登録情報
- 環境変数
- Cisco IronPort Email Security Plug-in の出力ファイル
- Windows および Outlook に関する情報
- システム ユーザ名および PC 名
- その他の Outlook プラグインに関する情報

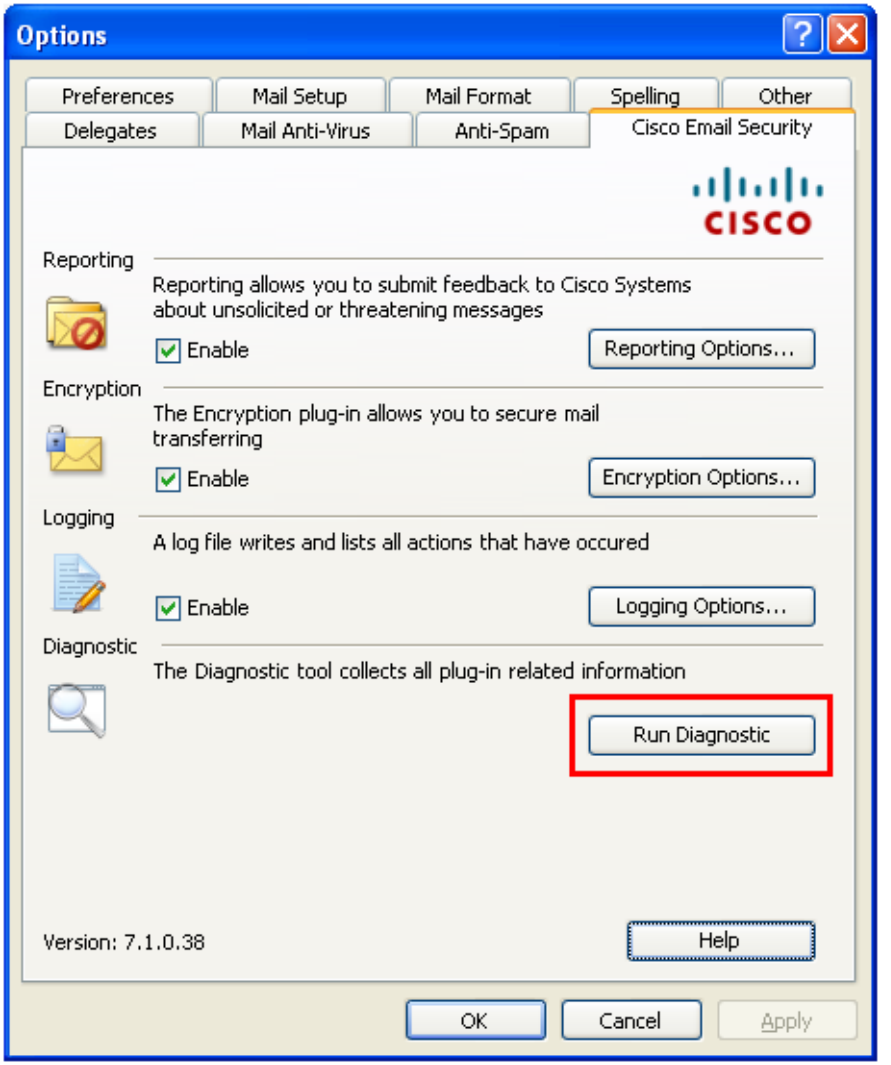
Cisco IronPort Email Security 診断ツールの実行

Cisco Email Security 診断ツールは次の場所のいずれかから実行できます。

- **Cisco Email Security の [Options] タブから**。通常は、Cisco Email Security の [Options] タブから診断ツールを実行します。
- **Program Files¥Cisco IronPort Email Security Plug-in フォルダから**（通常は C:¥Program Files¥Cisco¥Cisco IronPort Email Security Plug-in）。これは Cisco IronPort Email Security Plug-in がインストールされているフォルダです。
- **[Start Menu] > [All Programs] > [Cisco IronPort Email Security Plug-in] > [Diagnostic Tool] から。**

Outlook の [Options] ダイアログからの診断ツールの実行

Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] タブを選択し、[Run Diagnostics] をクリックします。Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] を選択し、[Run Diagnostics] をクリックします。



1. 診断ツールがデータを収集するまで数秒間待ちます。

2. 診断ツールがデータを収集し終わったら、データが正常に収集されたことを示すメッセージが表示されます。

CiscoDiagnosticReport.zip ファイルに移動して、システム管理者またはシスコのサポート担当者にファイルを手動で送信できます。

Program Files からの診断ツールの実行

Cisco IronPort Email Security Plug-in がインストールされているフォルダ（通常は C:¥Program Files¥Cisco¥Cisco IronPort Email Security Plug-in）に移動して、*Cisco.EmailSecurity.Framework.Diagnostic.exe* ファイルをクリックします。

[Start] メニューからの診断ツールの実行

診断ツールを実行するには、[Start] > [Programs] > [Cisco IronPort Email Security Plug-in] を選択します。[Diagnostic Tool] をクリックします。レポートを表示するには、[Go to Report] をクリックします。レポートは、zip ファイル *CiscoDiagnosticsReport.zip* に保存されます。

Cisco IronPort Email Security Plug-in のアンインストール

Cisco IronPort Email Security Plug-in をアンインストールするには、[Control Panel] > [Add/Remove Program] を選択するか、setup.exe プログラムを実行します。

アンインストール中、次の項目が削除されます。

- プラグインによって作成されたすべてのレジストリ エントリ
- [Add/Remove Program] に一覧表示されるプラグインのエントリ
- プラグインに関連するファイル
- プラグイン ツールバー（Outlook から削除）

（注）　プラグインをアンインストールしても Outlook のパフォーマンスには影響しません。

Cisco IronPort Email Security Plug-in for Outlook のアンインストール手順

Cisco IronPort Email Security Plug-in for Outlook をアンインストールするには、次の 2 つの方法があります。

- [Start] > [Control Panel] > [Add/Remove Programs] をクリックします。[Cisco IronPort Email Security Plug In] を選択して、[Remove] をクリックします。

  または

- プラグイン設定ファイル（プラグインのインストールに使用したファイル）をダブルクリックし、[Remove] オプションを選択して、Cisco IronPort Email Security Plug-in をアンインストールします。

CHAPTER 5

Cisco IronPort Email Security Plug-in for Lotus Notes の設定および使用方法

この章では、Cisco IronPort Email Security Plug-in for Lotus Notes で利用可能な機能について説明します。Cisco IronPort Email Security Plug-in には、いくつかの共通の電子メール セキュリティ プラグインが含まれます。ここでは、次の項目を取り上げます。

Cisco IronPort Email Security Plug-in for Lotus Notes の一般的な設定

Cisco IronPort Email Security Plug-in for Lotus Notes は、次のような Cisco IronPort Email Security Plug-in をサポートするフレームワークです。

- Reporting Plug-in：このプラグインは、スパム、ウイルス、フィッシング攻撃の電子メールや、スパムであると誤って分類された電子メールの報告に使用します。
- Encryption Plug-in：このプラグインは、暗号化された安全な電子メールの送信に使用します。

Cisco IronPort Email Security Plug-in は、[Options] ページで設定できます。[Options] ページにアクセスするには、[Actions] > [Cisco Email Security] を選択します。

[Cisco Email Security Options] ページ

レポート、暗号化、およびロギングをイネーブルにするには、このタブで各オプションの [Enable] チェックボックスをオンにします。さらに設定を行うには、[Reporting Options...]、[Encryption Options...]、または [Logging Options...] ボ

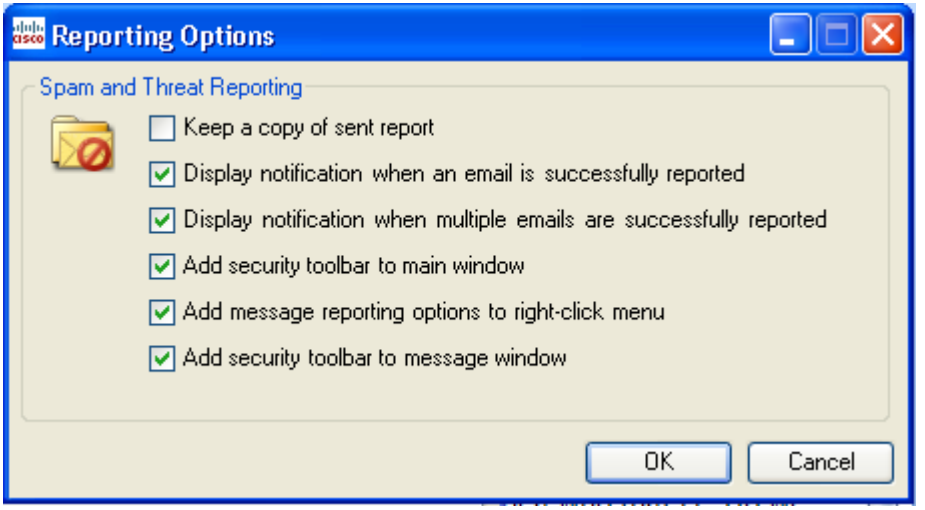
タンをクリックします。問題解決時に診断ツールを使用すると、Cisco IronPort Email Security Plug-in でレポートを実行して、シスコのサポートに送信することもできます。

Reporting Plug-in

[Options] ダイアログ

Reporting Plug-in を使用すると、受信した電子メールがスパム、フィッシング攻撃、ウイルスの場合や、スパムであると誤って分類された場合に、シスコに報告できます。

Cisco Email Security Reporting Plug-in for Lotus Notes は [Options] ダイアログで設定できます。[Reporting Options] ページにアクセスするには、[Actions] > [Cisco Email Security Options] を選択し、ダイアログの [Reporting] タブを選択します。



オプション

ここでは、変更可能なレポート オプションについて説明します。

[Keep a copy of sent report]

デフォルトでは、スパムまたはウイルスの電子メール メッセージや、スパムまたはウイルスであると誤って分類された電子メール メッセージをシスコに報告すると、送信した報告電子メールは削除されます。このオプションを選択すると、電子メールは削除されません。

[Display notification when an email is successfully reported]

電子メールの報告時に、このオプションを選択すると電子メールが正常に報告されたことを示す通知アラートを表示できます。

[Display notification when multiple emails are successfully reported]

複数の電子メールの報告時に、このオプションを選択するとすべての電子メールが正常に報告されたことを示す通知アラートを表示できます。

[Add security toolbar to main window]

このオプションを使用すると、セキュリティ ツールバーがメイン ウィンドウに追加されます。

[Add message reporting options to right-click window]

このオプションを使用すると、メッセージ レポート オプションが右クリック ウィンドウに追加されます。

[Add security toolbar to message window]

このオプションを使用すると、セキュリティ ツールバーがメッセージ ウィンドウに追加されます。

Reporting Plug-in for Lotus Notes の使用方法

Cisco Email Security Reporting Plug-in for Lotus Notes を使用すると、受信ボックスに受信したスパム、ウイルス、またはフィッシング メールについてシスコにフィードバックできます。シスコは、このフィードバックを利用して不要なメッセージが受信ボックスに配信されないようにフィルタを更新します。

Lotus Notes でスパム、ウイルス、フィッシング、または誤って分類された電子メールを報告するようにメイン メニュー バーから設定できます。電子メールを報告すると、レポートが送信されたことを示すメッセージが表示されます。報告したメッセージは、シスコの電子メール フィルタの改善に使用され、受信ボックスに一方的に送りつけられるメールを減らすことができます。

Encryption Plug-in

暗号化オプションの設定

Encryption Plug-in の設定は [Cisco Email Security Options] ダイアログで変更できます。暗号化設定を変更するには、[Actions] > [Cisco Email Security Options] を選択し、[Encryption Options] をクリックします。

オプション

暗号化された電子メールを送信するオプション

送信メールを暗号化する場合、電子メールに暗号化のマーク（「フラグ」）を付ける必要があります。これにより、システム管理者によって作成されたフィルタは暗号化する必要があるメッセージを識別できます。

警告　システム管理者に連絡せずに、電子メールに暗号化のフラグを付ける方法を変更しないでください。これらの方法では Cisco IronPort Encryption アプライアンスで変更を行う必要があり、この変更を行えるのはシステム管理者だけです。

次のいずれかの方法で電子メールに暗号化のマークを付けることができます。

- [Flag Subject Text] : 送信メールの [Subject] フィールドにテキストを追加して、電子メールに暗号化のフラグを付けることができます。[Subject] フィールドの先頭にテキストを入力して、電子メールを暗号化する必要があることを示します（デフォルト値は *[SEND SECURE]* です）。
- [Flag X-header name/value] : 送信メールに x ヘッダーを追加して、電子メールに暗号化のフラグを付けることができます。1 つめのフィールドに x ヘッダーを入力します（デフォルト値は *x-ironport-encrypt* です）。2 つめのフィールドに true または false を入力します。*true* を入力した場合、指定された x ヘッダーのメッセージが暗号化されます（デフォルト値は *true* です）。

Encryption Plug-in の使用方法

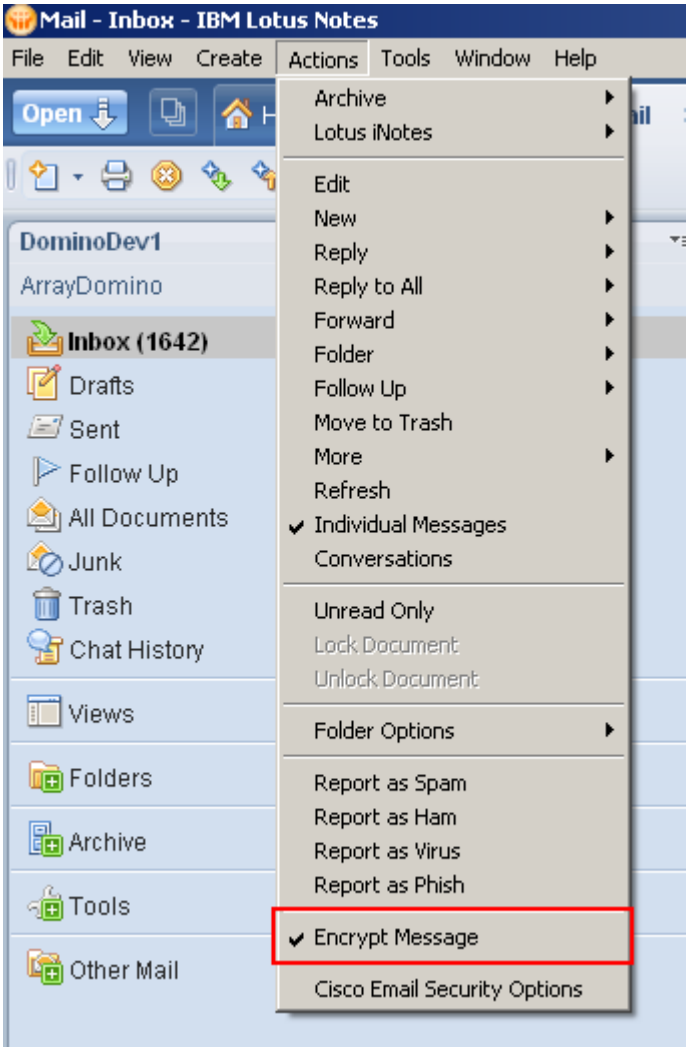
概要

Encryption Plug-in を使用すると、Lotus Notes 電子メール プログラムから暗号化した電子メールを送信できます。安全な電子メールを送信する場合、Cisco Email Security Encryption Plug-in は暗号化のマークが付けられた電子メールを安全に送信し、目的の受信者だけがそのメールを読めるようにします。

安全な電子メールの送信

メール システムで安全な電子メールを送信するには、[Actions] メニューの [Encrypt Message] をオンにします。

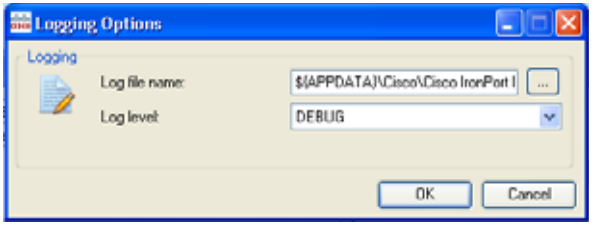
安全なメッセージを送信するには、次のように [Encrypt Message] がオンになっていることを確認します。



[Logging Options] の変更

[Logging Options] ページを開くには、[Logging Options...] をクリックします。

[Logging Options]



オプション

[Logging] メニューから次のオプションを設定できます。

[Log file name]

%appdata%\Cisco に保存されるログ ファイルの名前を指定できます。ログ ファイル名には .log 拡張子が必要です。

[Log level]

ログ レベルは、ログ ファイルに記録される情報を指定します。次のいずれかのログ レベルを選択できます。

- [ERROR] : エラー メッセージおよび例外状況をログに記録します。
- [WARN] : [ERROR] で記録されるメッセージおよび警告メッセージがログに記録されます。
- [INFO] : 基本情報およびその他のステータス メッセージがログに記録されます。自動更新プロセスのステータス メッセージがログに記録されます。[WARN] および [ERROR] で記録されるメッセージもすべてログに記録されます。
- [DEBUG] : 設定に関する詳細情報がログに記録されます。[ERROR]、[WARN]、および [INFO] のすべてのエラー メッセージ、および問題のトラブルシューティングに役立つ可能性がある情報がログに記録されます。

特定の状況に必要なトラブルシューティングのレベルに基づいてログ レベルを変更できます。たとえば、Cisco IronPort Email Security Plug-in に関する問題が発生した場合、ログ レベルを [DEBUG] に設定すると、開発者が問題を再現して診断を実行できるように最大限の情報を提供できます。

トラブルシューティングと診断

ここでは、Cisco IronPort Email Security Plug-in for Lotus Notes の使用中に発生する可能性がある一般的なエラー、およびそれらのエラーを修正するためのトラブルシューティングのヒントを示します。

（注）　同じエラー メッセージが数回表示され、このエラーによって Cisco IronPort Email Security Plug-in for Lotus Notes の機能が影響を受ける場合、修復プロセスを実行してみてください。修復プロセスを実行しても同じエラーが発生する場合は、「Cisco Email Security 診断ツール」を使用してシスコにフィードバックする手順を実行してください。

一般的な起動エラー

コンフィギュレーション ファイルの初期化中に発生するエラー

Outlook の起動時に次のメッセージが表示されることがあります。

- 「Error occurred during Cisco IronPort Email Security Plug-in configuration file initialization.Some settings set to default values.」
- 「Error during reading configuration for Reporting component.Some settings set to default values.」
- 「Error during reading configuration for Encryption component.Some settings set to default values.」

上記のエラー メッセージは、コンフィギュレーション ファイル（*%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes\CommonConfig.xml*）の一部の値が破損した場合に表示されます。

解決策

プラグインは破損したコンフィギュレーション ファイルをデフォルト値に戻します。引き続きエラー メッセージが表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正します。

コンフィギュレーション ファイルが見つからない。設定がデフォルト値に設定される。

Outlook の起動時に次のエラー メッセージのいずれかが表示されることがあります。

- 「Cisco IronPort Email Security Plug-in configuration file not found.Settings set to default values.」
- 「Configuration file for Encryption component was not found.Settings set to default values.」
- 「Configuration file for Reporting component was not found.Settings set to default values.」

解決策

プラグインは破損したコンフィギュレーション ファイルをデフォルト値に戻します。引き続きこのエラー メッセージが表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正します。

メッセージ報告エラー

無効な電子メール アドレス

Lotus Notes で [Report as Spam]、[Report as Virus]、[Report as Phish]、または [Report as Not Spam] ボタンをクリックすると、次のメッセージが表示されることがあります。

「Invalid address for report type.Please update configuration file.」（レポート タイプに無効なアドレスです。コンフィギュレーション ファイルを更新してください。）

このエラー メッセージは、Reporting Plug-in を使用していて、報告しようとしている電子メールの形式が不適切な場合に表示されます。スパムおよびフィッシング メールを報告できるように（および正当なメールを「非スパム」として報告できるように）、Reporting Plug-in ファイルを修正する必要があります。

解決策

%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes フォルダ内のレポート設定を確認します。その設定を削除して、修復プロセスを実行してデフォルト値に戻します。

Cisco IronPort Email Security Plug-in for Lotus Notes ファイルの修復

1. [Control Panel] > [Add or Remove Programs] を選択します。
2. プログラムの一覧で Cisco IronPort Email Security Plug-in を見つけて、[Change] をクリックします。
3. Lotus Notes が終了していることを確認します。
4. Cisco IronPort Email Security Plug-in インストーラを選択して、[Repair] オプション ボタンをクリックします。
5. [Next] をクリックします。インストーラの修復プロセスが実行されます。
6. エラーの原因になったアクションを実行します。修復プロセスの実行後も同じエラーが発生する場合、診断ツールを使用してシスコにフィードバックする手順を実行してください。

Cisco Email Security 診断ツール

問題を十分に分析するために必要な詳細情報をシスコに送信できる、Cisco IronPort Email Security Plug-in 用の診断ツールが用意されています。エラーが発生した場合や、修復プロセスでは解決できない Cisco IronPort Email Security Plug-in に関する問題が発生した場合に、診断ツールを使用します。また、診断ツールを使用すると、不具合の報告時にシスコのエンジニアと重要情報を共有することもできます。

エラーが発生した場合、トラブルシューティングのヒントの「Diagnostic」の項を参照してください。

Cisco Email Security 診断ツールにより収集されるデータ

診断ツールは、ご使用のコンピュータから次の情報を収集します。

- 一部の COM コンポーネントに関する登録情報
- 環境変数

- Cisco Email Security の出力ファイル
- Windows および Lotus Notes に関する情報
- システム ユーザ名および PC 名
- その他の Lotus Notes プラグインに関する情報

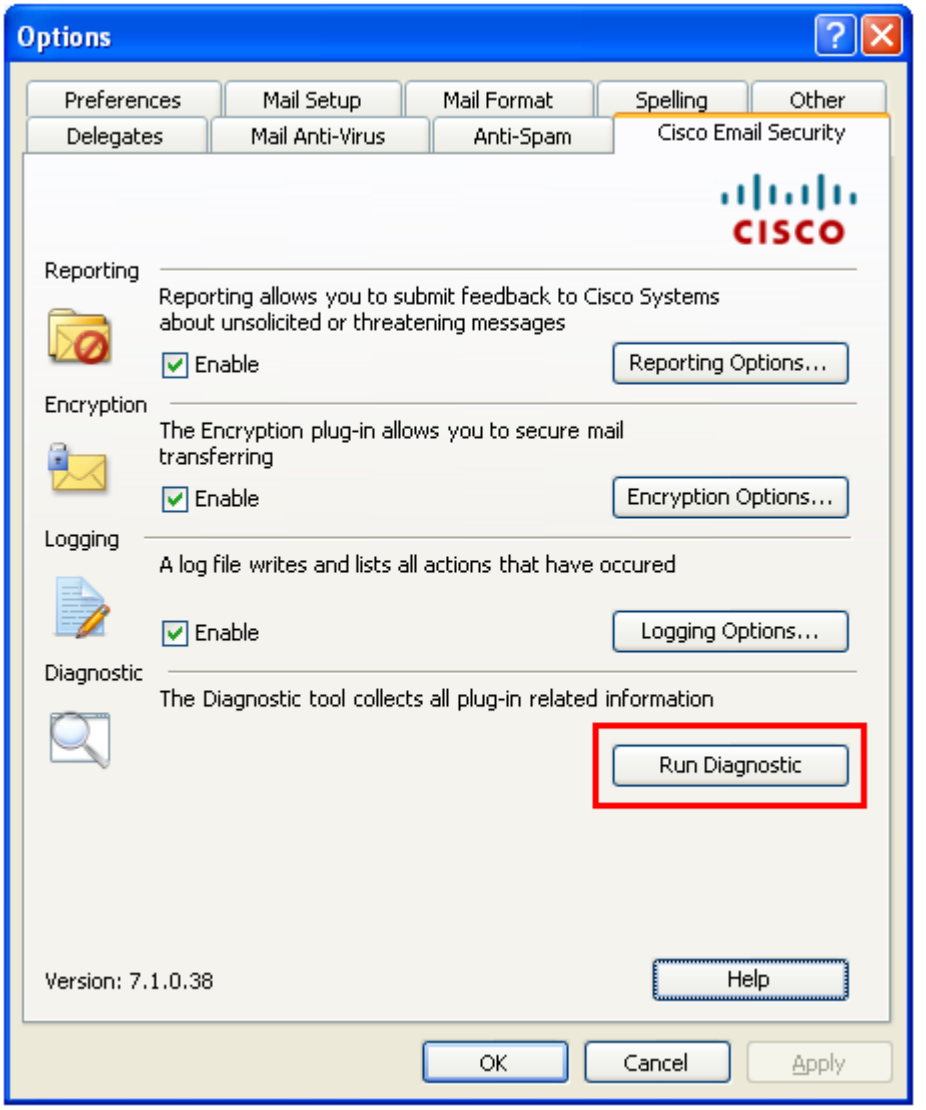
Cisco Email Security 診断ツールの実行

Cisco Email Security 診断ツールは次の場所のいずれかから実行できます。

- **Cisco Email Security の [Options] ダイアログから**：通常、Cisco Email Security の [Options] ダイアログから診断ツールを実行します。診断ツールにアクセスするには、[Actions] > [Cisco Options] を選択します。
- **Program Files\Cisco IronPort Email Security Plug-in フォルダから**（通常は C:¥Program Files¥Cisco¥Cisco IronPort Email Security Plug-in）：これは Cisco IronPort Email Security Plug-in がインストールされているフォルダです。

[Options] ダイアログからの診断ツールの実行

[Actions] > [Cisco Email Security Options] を選択して、[Run Diagnostics] をクリックします。診断ツールがデータを収集するまで数秒間待ちます。



診断ツールがデータを収集し終わったら、データが正常に収集されたことを示すメッセージが表示されます。診断ツールは、*CiscoDiagnosticReport.zip* という zip ファイルにデータを保存します。

[Go to Report] をクリックして *CiscoDiagnosticReport.zip* ファイルに移動し、システム管理者またはシスコ セキュリティ管理者にファイルを手動で送信できます。

Program Files からの診断ツールの実行

診断ツールを実行するには、[Start] > [Programs] > [Cisco Email Security for Lotus Notes] を選択します。または、Cisco Email Security がインストールされているフォルダ（通常は C:¥Program Files¥Cisco¥Cisco IronPort Email Security Plug-in）に移動して、*Cisco.EmailSecurity.Framework.Diagnostic.exe* ファイルをダブルクリックします。

アンインストール

Cisco IronPort Email Security Plug-in をアンインストールするには、[Control Panel] の [Add/Remove Program] を使用するか、setup.exe プログラムを実行します。

アンインストール中、次の項目が削除されます。

- プラグインによって作成されたすべてのレジストリ エントリ
- [Add/Remove Program] に一覧表示されるプラグインのエントリ
- プラグインに関連するファイル

（注） プラグインをアンインストールしても Lotus Notes のパフォーマンスには影響しません。

プラグインのアンインストール手順

Cisco IronPort Email Security Plug-in をアンインストールするには、次の 2 つの方法があります。

- [Start] > [Control Panel] > [Add/Remove Programs] をクリックします。Cisco IronPort Email Security Plug-in を選択し、[Remove] をクリックします。

  または

- プラグイン設定ファイル（プラグインのインストールに使用したファイル）をダブルクリックし、[Remove] オプションを選択して、Cisco IronPort Email Security Plug-in をアンインストールします。

APPENDIX A

IronPort エンド ユーザ ライセンス契約書

この付録の内容は、次のとおりです。

Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書

すべてのユーザに対する警告：本ソフトウェア（以下で定義）のライセンスについて、以下の法的な契約書（「契約書」）を注意深くお読みください。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様（個人または単一の実在者のいずれかを指し、総称して「お客様」と呼びます）は、デラウェア州法人である Cisco IronPort Systems, LLC（以下「IronPort」）とお客様（総称して「両当事者」と呼びます）との間の以下の契約に従い、その当事者となることに同意したことになります。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様は（A）お客様がお客様の会社を代表する権限を正式に与えられており、（b）お客様の会社を代表して本契約の条件に同意することを表明し、それによって契約が成立します。お客様またはお客様が代表する会社（総称して「お客様」と呼びます）が本契約の条件に同意しない場合は、キャンセル ボタンをクリックするか、質問に「N」を入力し、即座に（ただし後述のとおり納品日から 30 日以内に）、IronPort または本ソフトウェアの提供元である販売代理店に通知し、本ソフトウェアに対して支払った代金の全額の返金を受けてください。

1. 定義

1.1「お客様のサービス」とは、お客様の内部的なビジネスを遂行することを目的とし、購入契約、評価契約、ベータまたはプレリリース契約、注文書、見積書、お客様と IronPort またはその販売代理店との間のその他同様の契約（以下「契約」）、ならびにシステム アーキテクチャおよびそのインターフェイスの概要が記載されている該当するユーザ インターフェイスおよび IronPort の標準システム ガイド ドキュメント（総称して「ライセンス文書」と呼びます）で規定されているとおり、お客様の製品を通じて可能となる、エンド ユーザに提供される、お客様の電子メールまたはインターネット サービスを意味します。

1.2「エンド ユーザ」とは、お客様のサービスを通じてインターネットへアクセスすること、もしくは電子メール サービスを利用することをお客様が承認した従業員、請負業者、またはその他の代理人を意味します。

1.3「本サービス」とは、（i）アップデートおよびアップグレードを含む、本ソフトウェアの機能の提供、および（ii）場合によって IronPort またはその販売代理店によるサポートの提供を意味します。

1.4 「本ソフトウェア」とは、（i）IronPort が所有し、IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されるソフトウェア、（ii）IronPort のサードパーティ ライセンサーによって提供され、IronPort のハードウェア製品で使用するためにお客様にライセンス付与された任意のソフトウェア、（iii）IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されたその他の任意の IronPort ソフトウェア モジュール、および（iv）それらに対するすべてのアップデートおよびアップグレードを意味します。

1.5「アップデート」とは、本ソフトウェアに大規模な新機能を追加せず、IronPort またはそのサード パーティ ライセンサーによってリリースされる、マイナー アップデート、エラー修正およびバグ修正を意味します。アップデートは、本ソフトウェアのリリース番号における小数点の右側の増加（たとえば、ソフトウェア 1.0 からソフトウェア 1.1 へ）により示されます。「アップデート」という用語は、IronPort またはそのサード パーティ ライセンサーにより個別の製品として販売およびライセンス付与されるアップグレードまたは新しいソフトウェア バージョンを明確に除外します。

1.6「アップグレード」は、本ソフトウェアに対する改訂を意味し、IronPort またはそのサードパーティ ライセンサーによりその独自の裁量でリリースされた場合に、新しい拡張機能を既存の機能に追加します。アップグレードは、本ソフトウェアのリリース番号における小数点の左側の増加（たとえば、ソフトウェア 1.x からソフトウェア 2.0 へ）により示されます。いかなる場合にも、アップグレードには、IronPort またはそのサード パーティ ライセンサーにより個別の製品として販売およびライセンス付与される本ソフトウェアの新しいバージョンは含まれません。

2. ライセンスの付与とデータ収集条件についての同意

2.1 ソフトウェアのライセンス。本ソフトウェアおよびライセンス文書を使用することにより、お客様は本契約の条件に従うことに同意し、お客様が本契約に準拠している限り、IronPort はお客様に、契約期間中、お客様のサービスをエンドユーザに提供することに関連してのみ、IronPort のハードウェア製品上でのみ本ソフトウェアを使用する非独占的、二次ライセンス不能、譲渡不能、世界的なライセンスを付与します。本ライセンスの期間と範囲は、ライセンス文書で別途規定します。本契約で明示する場合を除き、IronPort、IronPort の販売代理店、またはその各ライセンサーは、お客様に対し、いずれの本ソフトウェアにおける権利、権原、権益も付与しません。本ライセンスとすべての本サービスは同時に終結します。

2.2 データの使用についての同意とライセンス。本契約の第 8 項と、お客様への通知をもって IronPort により随時修正される可能性がある IronPort プライバシー声明（http://www.IronPort.com/privacy.html）に従い、お客様は、IronPort により随時修正される可能性があるライセンス文書に規定されているとおり、お客様からデータ（以下「データ」）を収集し使用することに同意し、そのライセンスを IronPort に付与します。データを使用してレポートまたは統計情報を生成する範囲において、データは全体としてのみ開示され、ユーザ名、電話番号、難読化されていないファイル名、電子メール アドレス、物理アドレス、およびファイルの内容など、エンド ユーザの識別情報をデータから推測できないようにするものとします。上記にかかわらず、お客様は、事前に書面または電子的な手段で通知することで、IronPort がデータを収集および使用する権利をいつでも終了させることができますが、かかる権利が終了した場合、お客様は本ソフトウェアまたは本ソフトウェアのコンポーネントを利用できなくなります。

3. 機密性。各当事者は、相手方当事者のすべての機密情報を、自身の同様の機密情報を保護するのと同じ程度に（また、いかなる場合にも妥当な程度の注意を払って）秘密に保持し、かかる機密情報を本契約で許された範囲でのみ使用することに同意します。本契約での「機密情報」とは、「機密」と表示された当事者の情報または開示元の当事者が独占的または機密として見なすことが妥当な情報を意味します。ただし、IronPort によって提供される本ソフトウェアの設計レビューおよびあらゆる製造前のリリースで開示されたデータ、本ソフトウェア、情報は、機密と表示されているどうかにかかわらず明らかに機密情報と見なされます。

4. 財産権、所有権。IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他の資料の権原および所有権、ならびに前記にかかわるすべての知的財産権（以下で定義）は、IronPort および/またはその上位ライセンサーの独占的所有物です。お客様ならびにその従業員および代理人は、IronPort またはその販売代理店によってお客様に提供された本ソフトウェアまたはその他の資料のコピーに現れる商標またはその他の所有権表記、説明文、記号またはラベルを削除または改変しないものとします。お客様は、本ソフトウェア

または本ソフトウェアによって生成される内部データファイルの変更、変換、営利目的での転売、配布、複製、機能拡張、適合、翻訳、逆コンパイル、リバースエンジニアリング、逆アセンブルを行ったり、本ソフトウェアまたは本ソフトウェアによって生成される内部データ ファイルのソースコードを特定したり、取得しようとしたり、本ソフトウェアまたはライセンス文書に基づいて二次的著作物を作成したりしないものとし、他者によるそのような行為を許可または承認しないことに同意します。別途書面で合意しない限り、本契約または関連するすべてのコンサルティングまたはプロフェッショナル サービス契約の履行途中に IronPort またはその上位ライセンサーによって作成または開発されたプログラム、発明、概念、文書、仕様、またはその他の文書化された資料または図面による資料および媒体は、すべての著作権、データベース権、特許、企業秘密、商標、著作者人格権、またはかかる作業の遂行に関連するその他すべての知的財産権（「知的財産権」）を含め、IronPort またはその上位ライセンサーに独占的に属するものとし、合衆国法典第 17 編（1976 年著作権法）の意味の範囲内でお客様のために有償で行われた作業とは見なさないものとします。

5. 制限付き保証と保証の放棄

5.1 制限付き保証。IronPort はお客様に対し、本ソフトウェアが適切にインストールされ正しく使用されている場合に、ライセンス文書に記載された仕様に相当程度に従うことを、納品日から 90 日間か、ライセンス文書に記載されている期間のうちの長いほうの期間（以下「保証期間」）にわたり保証します。本項に記載されている保証のいずれかの違反に対し、お客様の唯一の法的救済および IronPort の全責任は、保証期間内にお客様によって不適合が IronPort および/またはその販売代理店に報告された場合に限り、誤りまたは不適合をすみやかに修正することです。この保証は、お客様に対してのみ行われ、エンド ユーザまたは他の第三者への譲渡はできません。本項で定める保証の違反、または本契約の違反に対し、かかる違反が直接的または間接的に次のいずれかから、またはそれに関連して生じた場合、IronPort は一切の責任を負いません。（i）お客様または第三者による、本ソフトウェアの無許可の、不適切な、不完全な、または不適当なメンテナンスまたはキャリブレーション、（ii）第三者のハードウェア、ソフトウェア、サービスまたはシステム、（iii）本ソフトウェアまたは本サービスの許可のない変更または改造、（iv）本ソフトウェアの無許可の、もしくは不適切な使用もしくは操作、またはお客様が該当する環境仕様に従わなかった場合、（v）IronPort またはその販売代理店から随時提供されるアップデート、アップグレード、修正、改訂をインストールおよび/または使用しなかった場合。

5.2 保証の否認。本契約書の 5.1 項に記載されている明示的な保証は、本ソフトウェアまたは本サービスに関する唯一の保証を構成します。適用法によって許される最大の限度まで、IronPort は本契約上の本ソフトウェアと本サービスのライセンスを「現状のまま」付与します。本契約で明示的に規定しない限り、IronPort およびその上位ライセンサーは、明示、黙示または制定法上の（事実上

の、または法律の運用による）いかなる形の表明も保証も行わず、市場性または特定目的適合性の黙示的保証などを含むその他のあらゆる保証を明示的に否認します。IronPort もそのサード パーティ ライセンサーも、本ソフトウェアまたは本サービスが（1）不具合、エラー、バグを含まないこと、（2）本ソフトウェアの動作が中断しないこと、（3）本ソフトウェアの使用により得られるか得られる可能性がある結果または情報が正確で、完全で、信頼でき、安全であることを保証しません。

6. 責任制限。適用法で許される最大限度まで、いずれの当事者も相手方に対して、利益の損失、代替商品またはサービスの調達コスト、取引上の損失、使用またはデータの損失、事業の中断、またはあらゆる種類の間接的損害、特別損害、偶発的損害、結果的損害について、かかる当事者がかかる損害の可能性を示す事前通知を受け取っていた場合であっても、責任を負わないものとします。いかなる場合でも、本契約のいずれかの条項の下で生じる各当事者の責任は、かかる損害の請求が契約、不法行為、その他の法理論に基づくかどうかにかかわらず、そのような責任を生じさせる事象よりも前の 12 か月間に、本ソフトウェアまたは本サービスに対して支払われた総額を超えないものとします。

7. 契約の期間および終了。本契約の期間（「契約期間」）は、ライセンス文書で規定するものとします。IronPort が本契約またはライセンス文書の重要な条項を履行しなかった場合、お客様は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に本契約を終了させることができます。お客様が本契約またはライセンス文書の重要な条項を履行しなかった場合、IronPort は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に返金することなく本契約を終了させることができます。本契約は、次の場合に、いずれかの当事者により、いつでもただちに通告なく終了させることができます。（i）相手方当事者によるまたは相手方当事者に対する債務超過、管財人管理または破産手続き、またはかかる当事者の負債の調停のためのその他の訴訟手続、（ii）相手方当事者による債権者への一括譲渡、（iii）相手方当事者の解散。本契約が終了または満了した場合、第 2 項で付与されたライセンスはただちに終了します。お客様は、本契約が終了または満了してから 30 暦日以内に、本契約の下で IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他すべての資料またはドキュメントのすべてのコピーを IronPort またはその販売代理店に返却または破棄するものとします。

8. 米国 政府による権利の制限、輸出管理。本ソフトウェアおよび付随するライセンス文書は、該当する DFAR 227.7202 および FAR 12.212 に従い、それぞれ「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア文書」と見なされます。米国政府による本ソフトウェアおよび付随するライセンス文書の使用、変更、複製、リリース、実行、表示、開示は、本契約の条項のみによって決定され、本契約の条項によって明示的に許される範囲を除き禁止されます。本ソフトウェアおよびライセンス文書は米国の輸出管理規則に従って輸出し

なければならず、米国の法律に反する行為は禁止されることを、お客様は認めます。お客様は、米国輸出管理局もその他の連邦政府関係機関も、お客様が輸出する権利の停止、取り消し、拒否をしていないことを表明します。お客様は、お客様が本ソフトウェアを核兵器、科学兵器または生物兵器、ミサイル技術に関連して使用せず、これらの関連する最終使用のために譲渡しないことを表明します。ただし、米国政府により、規制または特定のライセンスによって許可されている場合を除きます。お客様は、米国およびその他の国におけるあらゆる輸入および輸出規制、その他の適用法に従うのは、最終的にお客様の責任であることを認め、IronPort またはその販売代理店が、元の販売国内でお客様に最初に販売した後はいかなる責任も負わないことを認めます。

9. 雑則。本契約は、法の抵触のルールを排除して、米国およびカリフォルニア州の法律に準拠します。国際物品売買契約に関する国連条約の適用は、明示的に除外されます。本契約に含まれるすべての規定は、両当事者間の代理関係、提携、その他の合同企業を構成するものと解釈されません。いずれの当事者も、下記による義務の不履行または履行遅延を理由とした責任を負わないものとします（金銭の支払いを除きます）。（i）米国の現在もしくは将来の法令または本契約に適用される法律の条項、（ii）電力供給の中断、インターネットの障害、ストライキ、品不足、暴動、反乱、火災、洪水、暴風雨、爆発、天災、戦争、テロ、政府の行動、労働条件、地震、またはかかる当事者の合理的な支配の及ばないその他の事由。本契約およびライセンス文書は、本ソフトウェアの使用に対するすべての権利を定め、両当事者間の完全な合意であり、本ソフトウェアおよびライセンス文書にかかわるその他のあらゆる通信に優先します。本契約の条件は、ライセンス文書、注文、当事者によって提出されたその他の書面との相違がある場合でも、相手方当事者によって正式に拒否されたかどうかにかかわらず、優先されます。本契約の変更は、IronPort の正式に認められた代表者が提供する書面での追記による場合を除き、禁止されます。ただし、IronPort は、お客様への通知により、IronPort プライバシー声明をその裁量においていつでも変更でき、その内容は http://www.IronPort.com/privacy.html に掲載されます。本契約のいずれの条項も、権利放棄されたものと見なされません。ただし、かかる権利放棄が書面により IronPort または IronPort の正式に認められた代表者によって署名されたものである場合を除きます。本契約のいずれかの条項が無効とされた場合であっても、本契約の残りの部分は完全な効力を維持するものとします。両当事者は、本契約書が英語のみで書かれていることは各自が希望したものであることを認めます。

10. IronPort の連絡先情報。お客様が何らかの理由で IronPort に連絡する必要がある場合の連絡先は次のとおりです。住所：IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066、電話：650.989.6500、FAX：650.989.6543。