

## 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」(P.4-2)
- 「Outlook プラグインの基本設定」(P.4-3)
- 「Reporting Plug-in」(P.4-5)
- 「Encryption Plug-in」(P.4-9)
- 「ロギング設定の変更」(P.4-12)
- 「診断ツールを使用したトラブルシューティング」(P.4-13)
- 「Cisco IronPort Email Security Plug-in のアンインストール」(P.4-16)

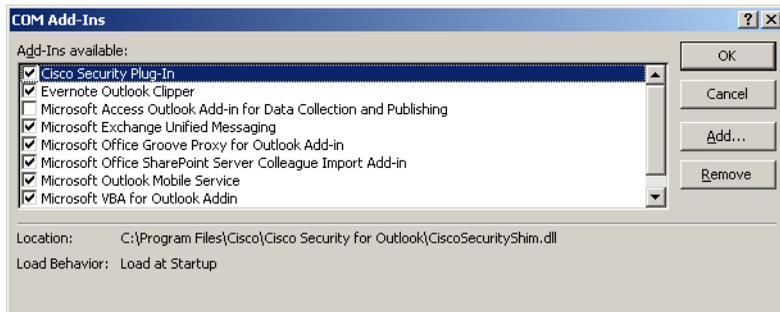
# Cisco IronPort Email Security Plug-in for Outlook の一般的な設定

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。

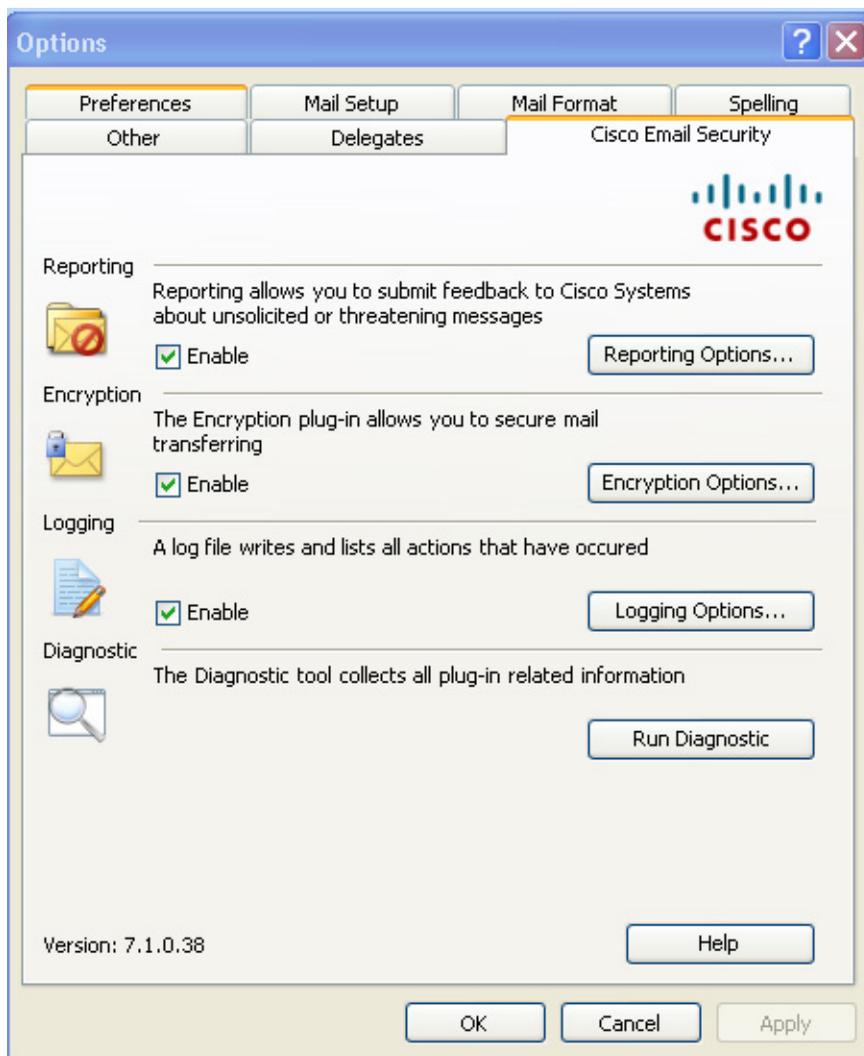
## Outlook プラグインの基本設定

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

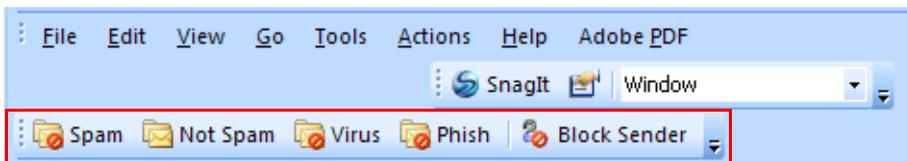
## 概要

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。

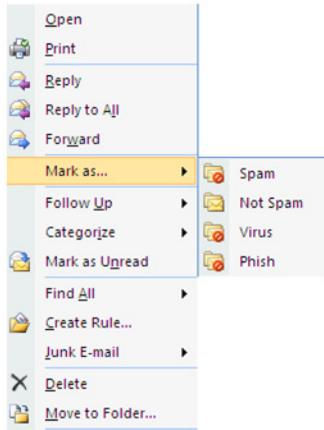
## シスコへのフィードバック

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)。

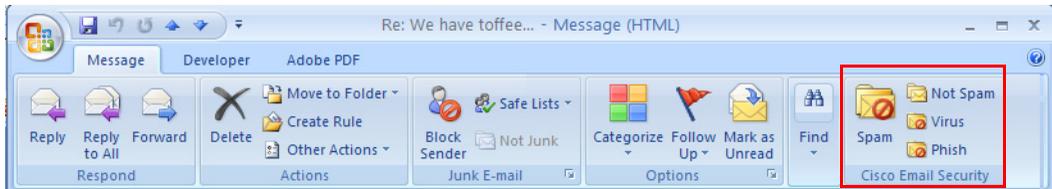


これらのボタンを使用して、スパム、ウイルス、およびフィッシング メールを報告します（フィッシング攻撃とは、不正な偽装 Web サイトにリンクしている電子メールです。この Web サイトは、受信者にクレジットカード番号、口座の名義人名とパスワード、社会保障番号など、個人の金融情報を漏洩させるように作られています。たとえば、*infos@paypals.com* から個人の銀行口座情報を不正に要求する電子メールが送信されてくる場合があります）。

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）。

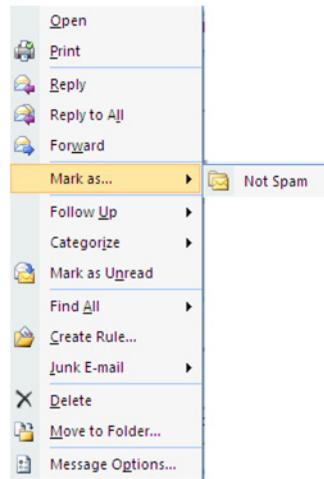


受信した電子メールがスパムであると誤って分類された（つまり、フィルタリングされ、[Spam] フォルダに配信された）場合、[Not Spam] ボタンをクリックして誤分類された電子メールを報告できます。これにより、この送信者からのメールは今後スパムとして分類されることはありません。

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。

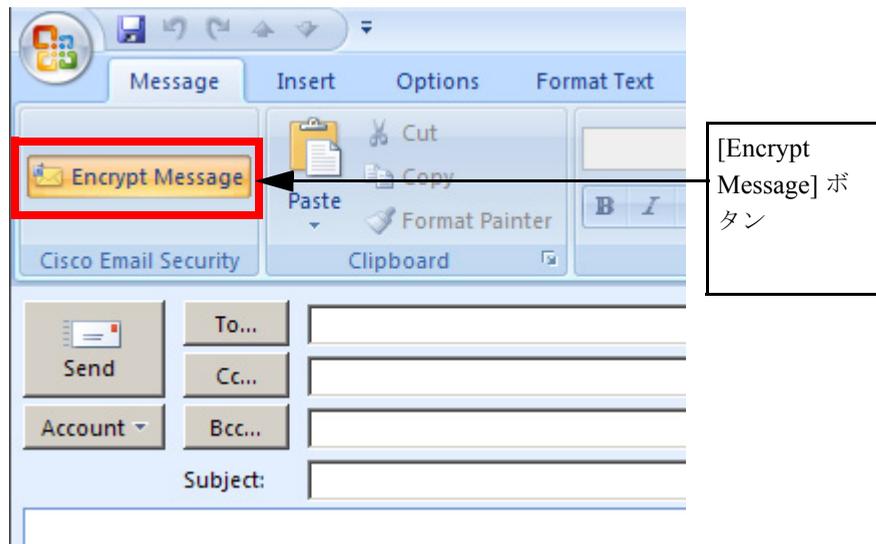
次のいずれかの方法で電子メールに暗号化のマークを付けることができます。

- [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りますを示します（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。

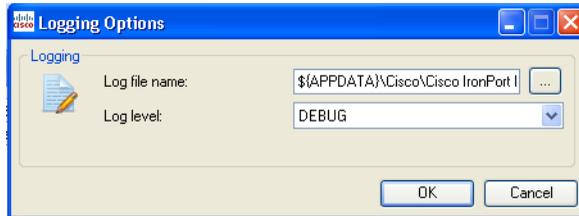


[Encrypt Message] ボタンは、電子メールの作成時に使用できます。

## 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 ユーザー名および PC 名
- その他の Outlook プラグインに関する情報

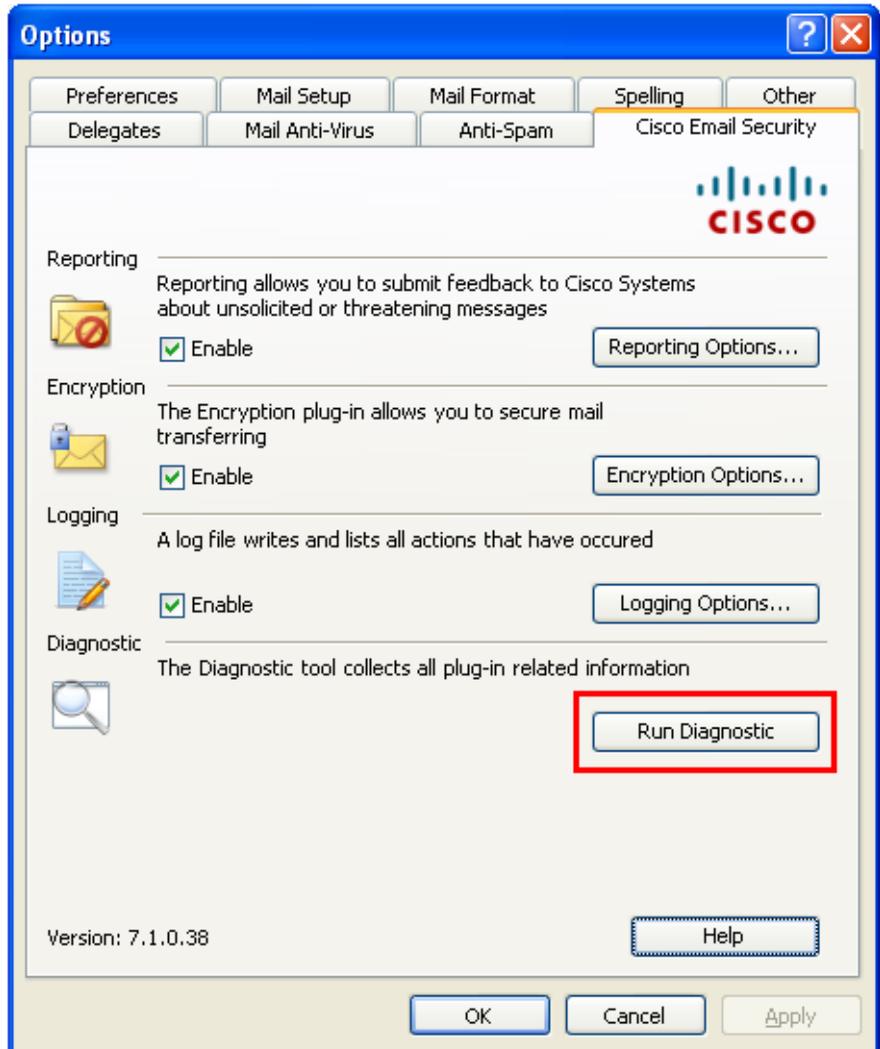
## Cisco IronPort Email Security 診断ツールの実行

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。

