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。