CHAPTER 13

SenderBase Network Participation

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

System Setup Wizard（GUI）および `systemsetup` コマンド（CLI）で、SenderBase ネットワークへの参加に同意できます。IronPort は、組織の電子メール トラフィックを集約した統計情報を収集します。これには、メッセージ属性の要約データおよび IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報のみが含まれています。たとえば、IronPort は、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。

この章は、次の内容で構成されています。

共有のイネーブル化

ご使用の IronPort アプライアンスの統計情報を SenderBase ネットワークと共有するには、次の手順を実行します。

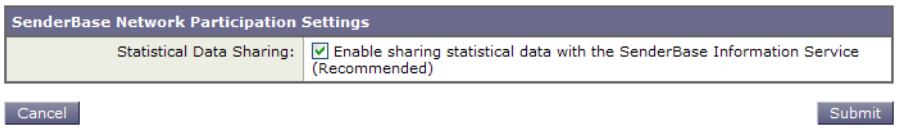
ステップ 1　[Security Services] > [SenderBase] ページにアクセスします。

図 13-1　[Security Services] > [SenderBase] ページ

（注）　システム セットアップ中にライセンス契約書に同意していない場合（「手順 2：[System]」（P.3-54）を参照）は、このページの表示は異なります。グローバル設定を編集できるようにするには、[Security Services] > [SenderBase] ページで [Enable] をクリックして、ライセンス契約を読み、同意する必要があります。

ステップ 2　[Edit Global Settings] をクリックします。

図 13-2　[Security Services] > [SenderBase] ページ：編集



ステップ 3　ボックスをチェックして、SenderBase Information Service との統計データの共有をイネーブルにします。このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。イネーブルにした場合、（IronPort

Anti-Spam スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集に Context Adaptive Scanning Engine（CASE）が使用されます。

ステップ 4　任意で、SenderBase Information Service との統計データ共有用に、プロキシ サーバをイネーブルにできます。ルールのアップデートを取得するようにプロキシ サーバを定義する場合は、追加で表示されるフィールドに、プロキシ サーバに接続する際に使用する認証済みのユーザ名、パスワード、および特定のポートも設定できます。これらの設定を編集する方法については、「システム時刻」（P.15-541）を参照してください。また、CLI の `senderbaseconfig` コマンドを使用して同様の設定を行うこともできます。

よくあるご質問

IronPort は、プライバシーが重要であると認識しており、プライバシーを考慮してサービスを設計および操作しています。SenderBase Network Participation に登録した場合は、IronPort は組織の電子メール トラフィックに関する集約した統計情報を収集しますが、個人を特定できる情報を収集したり、使用したりすることはありません。IronPort が収集した、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます。

なぜ参加する必要があるのですか。

SenderBase Network に参加していただくことで、IronPort がお客様に役立てるようになります。スパム、ウイルス、およびディレクトリ獲得攻撃などの、電子メールをベースとした脅威が組織に影響を及ぼすことを止めるには、IronPort とデータを共有していただくことが重要になります。参加が特に重要になる例として、次のような場合があります。

- お客様の組織を特に標的とした電子メール攻撃では、提供したデータがお客様自身を保護する主要な情報源となります。
- お客様の組織が、最初に新しいグローバルな電子メール攻撃を受けた組織の 1 つであった場合、IronPort と共有したデータにより、新しい脅威に対応するスピードが大幅に向上します。

どのようなデータを共有するのですか。

データは、メッセージ属性の要約情報および IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報です。メッセージの本文すべてを収集するわけではありません。繰り返しになりますが、IronPort に提供された、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます（後述の「IronPort は、共有されたデータがセキュアであることをどのように確認していますか。」（P.13-426）を参照してください）。

表 13-1 および表 13-2 に、「人間にわかりやすい」形式でサンプルのログ エントリを説明します。

表 13-1　IronPort アプライアンスごとに共有される統計情報

項目	サンプル データ
MGA ID	MGA 10012
タイムスタンプ	2005 年 7 月 1 日午前 8 時～午前 8:05 のデータ
ソフトウェア バージョン番号	MGA バージョン 4.7.0
ルール セットのバージョン番号	アンチスパム ルール セット 102
アンチウイルス アップデート間隔	10 分ごとにアップデート
検疫エリアのサイズ	500 MB
検疫可能メッセージ数	現在 50 件のメッセージを検疫可能
ウイルス スコアしきい値	脅威レベル 3 以上のメッセージを検疫
検疫されたメッセージのウイルス スコアの合計	120
検疫されたメッセージ数	30（平均スコア 4）
最大検疫時間	12 時間
アンチウイルス結果との相関による検疫理由および検疫解除理由で分類した、Outbreak 検疫メッセージ数の内訳	.exe ルールにより 50 件を検疫 手動で 30 件を検疫解除。このうち 30 件すべてがウイルス陽性
検疫解除の際に実行されたアクションで分類した、Outbreak 検疫メッセージ数の内訳	10 件のメッセージは検疫解除後に添付ファイルを削除
メッセージ検疫時間の合計	20 時間

表 13-2　IP アドレスごとに共有される統計情報

項目	サンプル データ
アプライアンスのさまざまな段階におけるメッセージ数	アンチウイルス エンジンにより発見：100 アンチスパム エンジンにより発見：80
アンチスパムとアンチウイルスのスコア合計および判断	2,000（発見されたすべてのメッセージに対するアンチスパム スコアの合計）
さまざまなアンチスパム ルールおよびアンチウイルス ルールの組み合わせにヒットしたメッセージ数	100 件のメッセージがルール A および B にヒット 50 件のメッセージがルール A のみにヒット
接続数	20 SMTP 接続
受信者の総数および無効数	総受信者数 50 無効な受信者数 10
ハッシュされたファイル名：（a）	<one-way-hash>.zip という名前のアーカイブされた添付ファイル内で、ファイル <one-way-hash>.pif が検出
難読化されたファイル名：（b）	ファイル aaaaaaa.zip 内で、ファイル aaaaaaa0.aaa.pif が検出
URL ホスト名（c）	メッセージ内で www.domain.com へのリンクが検出
難読化された URL パス（d）	メッセージ内で aaa000aa/aa00aaa というパスを持つホスト名 www.domain.com へのリンクが検出
スパムおよびウイルス スキャン結果ごとのメッセージ数	スパム陽性 10 件 スパム陰性 10 件 スパムの疑い 5 件 ウイルス陽性 4 件 ウイルス陰性 16 件 ウイルス スキャン不可 5 件
さまざまなアンチスパムおよびアンチウイルス判断によるメッセージ数	スパム 500 件、ハム 300 件

表 13-2　IP アドレスごとに共有される統計情報（続き）

項目	サンプル データ（続き）
サイズ レンジ内のメッセージ数	30 ～ 35 K の範囲に 125 件
さまざまな拡張子タイプごとの数	300 個の「.exe」添付ファイル
添付ファイル タイプ、本当のファイル タイプ、およびコンテナ タイプの相関関係	100 個の添付ファイルの拡張子が「.doc」ですが、実際には「.exe」 50 個の添付ファイルが zip 内に含まれた「.exe」拡張子
拡張子および本当のファイル タイプと添付ファイル サイズの相関関係	30 個の添付ファイルが 50 ～ 55 K の範囲の「.exe」

(a) ファイル名は一方向ハッシュ（MD5）でエンコードされます。

(b) ファイル名は難読化された形式で送信されます。この形式では、すべての小文字の ASCII 文字（[a ～ z]）は「a」、すべての大文字の ASCII 文字（[A ～ Z]）は「A」、すべてのマルチバイト UTF-8 文字は（その他の文字セットにプライバシーを提供するため）「x」に、すべての ASCII 数字（[0 ～ 9]）は「0」に置換され、その他すべてのシングルバイト文字（空白文字、句読点など）はそのまま保持されます。たとえば、ファイル Britney1.txt.pif は Aaaaaaa0.aaa.pif と表示されます。

(c) IP アドレスと同様に、URL ホスト名はコンテンツを提供する Web サーバを指定します。ユーザ名およびパスワードのような、秘密情報は含まれません、

(d) ホスト名に続く URL 情報は、ユーザの個人情報が漏えいしないように難読化されています。

IronPort は、共有されたデータがセキュアであることをどのように確認していますか。

SenderBase Network への参加に同意すると、次のように処理されます。

IronPort アプライアンスから送信されたデータは、セキュアなプロトコル HTTPS を使用して IronPort SenderBase Network サーバに送信されます。

お客様のデータはすべて、IronPort で慎重に取り扱われます。このデータは、セキュアな場所に保存され、データへのアクセスは、企業の電子メール セキュリティ製品およびサービスの向上またはカスタマー サポートの提供のためにデータにアクセスする必要のある IronPort の従業員および請負業者に限られます。

データに基づいてレポートまたは統計情報が作成された場合、電子メールの受信者またはお客様の企業を特定する情報が、IronPort Systems 以外で共有されることはありません。

データを共有することで IronPort アプライアンスのパフォーマンスに影響はありますか。

IronPort は、ほとんどのお客様には若干のパフォーマンス上の影響があると認識しています。IronPort は、電子メール配信プロセスの一環として、既存のデータを記録します。その後、アプライアンス上でお客様のデータが集約され、通常 5 分ごとに SenderBase サーバに一括送信されます。HTTPS を介して転送されるデータの総サイズは、一般的な企業の電子メール トラフィック帯域幅の 1 % 未満と予想しています。

イネーブルにした場合、（IronPort Anti-Spam スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集に Context Adaptive Scanning Engine（CASE）が使用されます。

不明点は、IronPort カスタマー サポートまでお問い合わせください。「Cisco IronPort カスタマー サポート」（P.1-12）を参照してください。

その他の方法でデータを共有できますか。

IronPort がより高品質のセキュリティ サービスを提供できるようにするために、追加のデータの共有をお考えのお客様のために、追加データの提供を可能にするコマンドを用意しています。このより高レベルのデータ共有では、メッセージに含まれる添付ファイルの明確なファイル名、ハッシュされていないテキスト、および URL のホスト名も提供されます。この機能の詳細について関心をお持ちの場合は、システム エンジニアまたは IronPort カスタマー サポートにお問い合わせください。