SenderBase Network Participation

この章は、次の項で構成されています。

SenderBase Network Participation の概要

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、電子メールのレピュテーション サービスです。

SenderBase ネットワークに参加しているお客様は、使用するすべてのサービスの機能向上のため、シスコが客様の組織の集約された電子メール トラフィックの統計情報を収集することを許可します。参加は任意です。シスコは、メッセージ属性の要約データおよび Cisoco 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を収集します。たとえば、シスコは、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。

SenderBase との統計の共有

手順

ステップ 1 [セキュリティサービス（Security Services）] > [SenderBase] に移動します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

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、（Cisco アンチスパム 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コンテキスト適応スキャン エンジン（CASE）

が使用されます。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。

ステップ 4 （任意）プロキシ サーバをイネーブルにして、SenderBase Information Service と統計データを共有します。

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、パスフレーズ、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、アップグレードおよびアップデートをダウンロードするためのサーバ設定を参照してください。また、CLI の **updateconfig** コマンドを使用して同様の設定を行うこともできます。

FAQ

シスコは、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、シスコ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。シスコが収集した、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 Cisco 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、シスコに提供された、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（後述のシスコは、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。 （6 ページ）を参照してください）。

次の表では、「人間にわかりやすい」形式でサンプルのログ エントリを説明しています。

表 *1 : Cisco* 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
隔離サイズ（Quarantine Size）	500 MB
隔離可能メッセージ数	現在 50 件のメッセージを隔離可能
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隔離
隔離されたメッセージのウイルス スコアの合計	120
隔離されたメッセージ数	30（平均スコア 4）
最大隔離時間	12 時間
アンチウイルス結果との相関による隔離理由および隔離解除理由で分類した、アウトブレイク隔離メッセージ数の内訳	.exe ルールにより 50 件を隔離 手動で 30 件を隔離解除。このうち 30 件すべてがウイルス陽性
隔離解除の際に実行されたアクションで分類した、アウトブレイク隔離メッセージ数の内訳	10 件のメッセージは隔離解除後に添付ファイルを削除
メッセージ隔離時間の合計	20 時間

表 *2 :* 送信者 *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

項目	サンプルデータ
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定によるメッセージ数	スパム 500 件、スパムなし 300 件
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	「.exe」添付ファイル 300 件
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	50 ～ 55 K の範囲に「.exe」添付ファイルが 30 件

項目	サンプルデータ
ファイルレピュテーションサービス（AMP クラウド）にアップロードされた添付ファイルの数	1110個のファイルをファイル レピュテーション サービスにアップロード
ファイルレピュテーションサービス（AMP クラウド）にアップロードされたファイルの判定	10 個の悪意のあるファイルが検出 100 個のファイルが正常と判断 1000個のファイルはレピュテーション サービスでは不明
ファイルレピュテーションサービス（AMP クラウド）にアップロードされたファイルのレピュテーション スコア	50 個のファイルのレピュテーション スコアは 37 50 個のファイルのレピュテーション スコアは 57 1 個のファイルのレピュテーション スコアは 61 9 個のファイルのレピュテーション スコアは 99
ファイルレピュテーションサービス（AMP クラウド）にアップロードされたファイルの名前	example.pdf testfile.doc
ファイルレピュテーションサービス（AMP クラウド）で検出されたマルウェア脅威の名前	トロイの木馬 - テスト

表 *3:* メッセージごとに共有される統計情報

メッセージ ID	内部メッセージ識別子 - 10010
受信者数	メッセージの受信者数 - 15
拒否された受信者数	無効であることが判明し、拒否された受信者数 - 5
ウイルス対策の判定	ウイルス対策エンジンから受信した判定。
AMP 判定	Advanced Malware Protection エンジンからの判定でマルウェア陽性の場合。
大容量メール	メッセージが「ヘッダー繰り返し回数」のメッセージ フィルタ ルールに一致した場合。
内部 Ironport スパム対策データ	メッセージが Ironport スパム対策エンジンにスキャンされた場合の、Ironport スパム対策スコアとメッセージ識別子。

（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。

AsyncOS 8.5 for Email以降、IronPort Anti-Spam機能またはIntelligent Multi-Scan機能がアクティブで、SenderBase Network Participationがイネーブルの場合、AsyncOSは製品の有効性を向上させるために次の手順を実行します。

- メッセージの特定のヘッダーの繰り返しに関する情報を収集して、収集した情報を暗号化し、暗号化した情報をヘッダーとして個々のメッセージに追加します。

  お客様はこのように処理されたメッセージを、分析のためにシスコに送信できます。各メッセージは、専門家チームによってレビューされ、製品の有効性を向上させるために使用されます。分析のためにシスコにメッセージを送信する手順については、誤って分類されたメッセージのシスコへの報告を参照してください。

- 送信者のSBRSに関係なく、スパム対策スキャンのためにCASEにメッセージのランダムサンプルを送信します。CASEは、これらのメッセージをスキャンして、その結果を製品の有効性の向上に利用します。AsyncOSは、アイドル状態の場合のみにこのアクションを実行します。その結果、このフィードバックメカニズムによるメッセージ処理への大きな影響はありません。

シスコは、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。

- Cisco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Cisco SenderBase Networkサーバに送信されます。
- お客様のデータはすべて、シスコ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シスコ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、シスコ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 Cisco アプライアンスのパフォーマンスに影響はありますか。

シスコは、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、（Cisco アンチスパム 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コンテキスト適応スキャン エンジン（CASE）が使用されます。

（注） SenderBase Network への参加を選択すると、「本文スキャン」が各メッセージに対して実行されます。これは、メッセージに適用されたフィルタなどのアクションにより本文スキャンが起動されたかどうかに関係なく実行されます。本文スキャンの詳細については、本文スキャン ルールを参照してください。

その他ご質問がありましたら、シスコ カスタマー サポートまでお問い合わせください。シスコサポートコミュニティ 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。

シスコ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、ご協力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 エンジニアまたはシスコ カスタマー サポートにお問い合わせください。

その他の方法でデータを共有できますか。

翻訳について
このドキュメントは、米国シスコ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。