InterScan™ Messaging Security Virtual Appliance 9.1 Sender Policy Framework 設定ガイド

1. はじめに

Sender Policy Framework (以下、SPF) は、送信者アドレスの偽装を防止するソリューションを提供するオープンスタンダードです。SPF を採用する組織は、「MAIL FROM」および「HELO」識別子で使用されるホストの DNS レコードを公開する必要があります。これにより、受信者はこれらのレコードを問い合わせることで、そのホストが特定ドメインのメールメッセージを送信することについて許可されているかどうかを特定できます。SPF の全仕様は、RFC 4408 に記載されていますので参考にしてください。

本書では、SPF のチェック処理を InterScan Messaging Security Virtual Appliance 9.1 (以下、IMSVA) に統合する方法について説明します。この統合には、Postfix SMTP アクセスポリシーの委任メカニズムを利用します。スクリプトが SPF チェックを実行し、Postfix へ特定の処理についてレポートを送ります。そのあと、Postfix が適切な処理を実行します。詳細については、http://www.postfix.org/SMTPD_POLICY_README.html を参照してください。

2. 有効化/無効化

• SPF を有効にするには

1. Postfix 設定を変更して、SPF チェックを Postfix のメールメッセージフローに組み込みます。

Postfix には、*master.cf* と *main.cf* の 2 つの主要な設定ファイルがあります。*master.cf* 設定ファイルは、クライアントプログラムをサービスに接続する方法や、サービスが要求されたときに実行するデーモンプログラムを定義します。Postfix の *main.cf* 設定ファイルは、Postfix メールシステムの処理を制御するパラメータの一部を指定します。

/opt/trend/imss/postfix/etc/postfix/master.cf で次のコメントを解除すると、SPF スクリプトが必要に応じて起動するようになります。

```
#SPFPolicyd     unix    -       n       n       -       0       spawn
#       user=imss    argv=/opt/trend/imss/postfix/etc/postfix/SPFPolicyd/SPFPolicyd.py
```

/opt/trend/imss/postfix/etc/postfix/main.cf で「smtpd_sender_restrictions」のパラメータに次のように「check_policy_service unix:private/SPFPolicyd」行を追記することで、「MAIL FROM」コマンドの受信後、Postfix で SPF チェックが実行されます。

```
smtpd_sender_restrictions =
  check_policy_service unix:private/SPFPolicyd
  check_policy_service inet:127.0.0.1:999
```

初期設定では、Postfix は 1,000 秒後に SPF チェックプロセスを停止します。この時間は、ポリシーデーモンの場合、少なくとも SMTP サーバプロセスと通信している間は実行が必要になる場合があるため短すぎます。SPF チェックプロセスの時間を延長するには、*main.cf* の次の行のコメントを解除します。

```
SPFPolicyd_time_limit = 3600
```

main.cf における SPF 関連設定の設定例を以下に記載します。

```
smtpd_sender_restrictions =
check_policy_service unix:private/SPFPolicyd
check_policy_service inet:127.0.0.1:999
SPFPolicyd_time_limit = 3600
127.0.0.1:999_time_limit = 3600
```

2. 次のコマンドを使用して Postfix サービスを再起動し、すべての変更を反映します。

```
# postfix restart
```

SPF チェックスクリプトのログは*/var/log/maillog* に書き込まれます。ログの各行の先頭は「SPFPolicyd」と表示されます。

SPF チェックが機能していることを確認するには、IMSVA の検索を正常に通過するメールメッセージを送信します。メッセージのヘッダに「Received-SPF」の記述があれば、SPF チェックスクリプトは正しく機能しています。

● SPF を無効にするには

SPF チェックを無効にするには、前のセクションで変更を加えた *master.cf* のエントリをコメント化し、*main.cf* の設定を削除します。次に Postfix サービスを再起動します。

3. 設定

スクリプトと同じフォルダ内にある *config.ini* ファイルは、メインの設定ファイルです。このファイルの形式は次のとおりです。

```
# Comments…
[section1]
Key1 = value1

[section2]
Key2 = value1, value2
```

3.1. 基本設定

次の表は、*config.ini* 内のすべてのキーについて詳細な使用方法を示しています。

注意:使用可能な値は「|」(パイプ)記号で区切られています。下線の付いた値が初期設定値です。複数値を設定できるパラメータでは、それらの値をカンマまたはスペースで区切って指定します。
例: example.com, example2.com

セクション	パラメータ	値	説明
globals	block_res	<テキスト> | 550 Service unavailable; SPF check unsuccessful and transaction closed due to the organization's policy.	メールメッセージがブロックされたかどうかを示す SMTP 応答コード。応答コードの「550」とメッセージの両方をカスタマイズできます。応答コードは、5 で始まる任意の有効桁数 3 桁の値にすることができます。応答コードとメッセージの間にスペースを忘れずに入れてください。
	check_helo	yes | no	HELO/EHLO 識別子の SPF チェックを実行する必要があるかどうかを指定します。HELO/EHLO 識別子は、MAIL FROM 識別子が空または無効である場合にチェックされます。
	enforce_domain	<ドメインのカンマまたはスペース区切りリスト>	ドメインの施行リストを指定します。このリストのドメインから送信されたメールメッセージには、「enforce_actions」セクションに定義された処理が適用されます。スパムメール送信者によって繰り返し偽造されるドメインを追加し、厳しい処理を適用して、メールシステムの保護を強化することができます。
	enforce_ip	<IP のカンマまたはスペース区切りリス	IP アドレスの施行リストを指定します。この使用方法は

		ト>	「enforce_domain」とほぼ同じです。現在は IP v4 のみがサポートされています。特定の形式<x.x.x.x>を使用して IP アドレスを完全に一致させたり、サブネットマスクパターン<x.x.x.x>/<サブネットマスク長>を使用して一連の IP アドレスに一致させたりすることができます。
	log_level	0 | 1 | 2 | 3 | 4	ログレベルを定義します。5 つのログレベルがあります。 0: ログなし > ログは生成されません。 1: 標準 > 管理とメンテナンスの基本的な情報を提供します。 2: 詳細 > 元の SPF チェックの結果など、詳細情報を表示します。 3: 診断 > レベル 1 および 2 のすべての情報に加えて、使用中の設定を示します。 4: デバッグ > 最も詳細な情報で、トラブルシューティング時にのみ使用することをお勧めします。
	pass	bypass | tempblock | block	SPF クエリは、pass、neutral、softfail、fail、none、temperror、および permerror の 7 種類の結果を返すことができます。同じ名前のパラメータは、その対応する処理を定義します。使用可能な処理には、bypass、tempblock、および block があります。 Bypass: SPF チェックが実行されないことを意味します。 Tempblock: 一時的にメールをブロックする 4XX SMTP 応答を返します。 Block: メールをブロックする5XX 応答を返します。 Pass: 対象ホストがこのドメインのメッセージについて送信を許可されていることを意味します。
	neutral	bypass | tempblock | block	このホストの正当性が指定されていないことを意味します。
	softfail	bypass | tempblock | block	対象ホストはメッセージの送信を許可されていないが、処理を実行中で

			あることを意味します。
	fail	bypass | tempblock | block	対象ホストがメッセージの送信を許可されていないことを意味します。
	none	bypass | tempblock | block	ドメインに SPF レコードがないか、SPF レコードに結果が存在しないことを意味します。
	temperror	bypass | tempblock | block	一時的なエラーが発生したことを意味します。たとえば、ネットワーク接続の切断などがあります。
	permerror	bypass | tempblock | block	持続的なエラーが発生したことを意味します。たとえば、SPF レコードの形式が正しくない場合などがあります。
	prepend_header	yes | no	メッセージに「Received-SPF」ヘッダを挿入するかどうかを指定します。 **より詳細な管理やメッセージ分析のために、このヘッダを追加することをお勧めします。**
	tempblock_res	<テキスト> | 451 Service temporarily unavailable; SPF check unsuccessful and transaction closed due to the organization's policy.	メッセージが一時的にブロックされているかどうかを示す SMTP 応答コード。応答コードの「451」とメッセージの両方をカスタマイズできます。応答コードは、4 で始まる任意の有効桁数 3 桁の値です。応答コードとメッセージの間にスペースを忘れずに入れてください。
	white_domain	<ドメインのカンマまたはスペース区切りリスト>	ドメインの承認済みリストを指定します。このリストのドメインから送信されたメッセージは SPF チェックから除外されます。このリストには、信頼するドメインを追加できます。
	white_ip	<IP のカンマまたはスペース区切りリスト> | 127.0.0.1	ドメインの承認済みリストを指定します。このリストのアドレスから送信されたメッセージは SPF チェックから除外されます。このリストには、信頼するドメインを追加できます。
enforce_actions	pass	bypass | tempblock | block	「enforce_actions」セクションのパラメータは、施行リスト内のドメインと IP アドレスに対する処理を定義します。動作は、global 処理のものと同じです。
	neutral	bypass | tempblock	上記と同様

		| block	
	softfail	bypass | tempblock | block	上記と同様
	fail	bypass | tempblock | block	上記と同様
	none	bypass | tempblock | block	上記と同様
	temperror	bypass | tempblock | block	上記と同様
	permerror	bypass | tempblock | block	上記と同様

3.2.ドメイン固有の処理の設定

いくつかのドメインに特定の処理を適用することが必要になる場合があります。たとえば、ドメイン example.com には公開済みの SPF レコードがあり、SPF レコード内に存在しないホストを使用してメッセージを送信することができないとします。その場合、この SPF レコード内のホストからではないメッセージはブロックする必要があります。*config.ini* にセクションを追加することで、それらのメッセージをブロックできます。

```
[<ドメイン>.com]
none=block
```

ここで SPF クエリの結果が none になると、メッセージはブロックされます。他のクエリ結果に対する処理は global の処理と同じですが、必要に応じて無効にすることもできます。
ワイルドカードがサポートされています。たとえば、「*.example.com」を使用して、example.com とそのすべてのサブドメインに対する処理を定義できます。SPF チェックは、最もマッチするドメインを自動的に検索します。送信者アドレスが「postmaster@example.com」の場合、SPF チェックは最初に「[example.com]」を検索し、このセクションが存在しない場合は、「[*.example.com]」を検索します。　このセクションの優先度は、承認済みリストおよび施行リストよりも低くなります。

3.3. SPF とクラウドプレフィルタの併用

クラウドプレフィルタを使用している場合、外部からのメッセージはクラウドプレフィルタを経由して受信されます。接続元の IP アドレスは常にクラウドプレフィルタの IP アドレスであるため、正当なメッセージであったとしても SPF の認証に失敗します。
そのため、http://esupport.trendmicro.com/solution/ja-jp/1123515.aspxを参照してクラウドプレフィルタの IP アドレスを取得し、その IP アドレス（または IP アドレスの範囲）をパラメータ「white_ip」にすべて登録し、SPF の検証から除外してください。