送信者ドメイン レピュテーション フィルタリング

この章は、次の項で構成されています。

送信者ドメインレピュテーションフィルタリングの概要

シスコの送信者ドメイン レピュテーション（SDR）は、送信者のドメインおよびその他の属性に基づいて電子メールメッセージのレピュテーションの判定を提供するクラウド サービスです。

Cisco Talos の送信者ドメイン レピュテーション（SDR）は、送信者のドメインおよびその他の属性に基づいて電子メールメッセージのレピュテーションの判定を提供するクラウドサービスです。

ドメイン ベースのレピュテーション分析では、共有 IP、ホスティングまたはインフラストラクチャ プロバイダーのレピュテーションよりも詳しい情報を調べることでより高いスパム検出率を達成し、完全修飾ドメイン名（FQDN）や Simple Mail Transfer Protocol（SMTP）通信およびメッセージ ヘッダーのその他の送信者情報に関連する特徴に基づいて判定を取得します。

詳細については、シスコのカスタマー連携プログラム（http://www.cisco.com/go/ccp）のセキュリティ トラックで、Cisco Talos の送信者ドメイン レピュテーション（SDR）のホワイト ペーパーをご覧ください。

（注）

- SDR のホワイト ペーパーにアクセスするには、シスコのカスタマー連携プログラムのアカウントを作成する必要があります。
- Cisco IPAS のクレームについては、Cisco Technical Assistance Center（TAC）のサポート リクエストを開いて SDR のクレームを送信してください。

SDR 判定

以下の表に、SDR 判定の名前、説明、推奨処置を記載します。

表 *1 : SDR* 判定

判定名	[説明（Description）]	推奨処置
非常に問題がある（Awful）	最も問題のあるレピュテーション判定です。 ブロッキングのしきい値がこの判定のみに設定されている場合、検出漏れ（FN）が発生し、セキュリティよりも配信が優先されます。	メッセージをブロックする。
不良（Poor）	推奨されるブロッキングのしきい値です。 これにより、検出漏れ（FN）と誤検出（FP）の長所と短所のバランスを取ることができます。Talos は SDR を調整し、「不良」または「非常に問題がある」の判定のいずれかを持つメッセージが SDR によってブロックされるようにします。 この判定でブロッキングをしない場合はセキュリティよりも配信が優先されますが、お客様はこの判定に基づいてブロックしない場合の検出漏れを許容することになります。	メッセージをブロックする。

判定名	[説明（Description）]	推奨処置
汚染されている（Tainted）	疑わしい送信者レピュテーションです。 これらの判定に基づくブロッキングは積極的で、Talos では推奨されていません。配信よりもセキュリティが優先されますが、この判定に基づいてブロックすると、許容できる誤検出が発生します。	アプライアンスに設定されている他のエンジンでメッセージをスキャンする。
弱い（Weak）	ニュートラルな判定を除外した弱いインジケータに関連付けられる多くのドメイン（正規および混在使用を含む）に一般的な判定です。Talos は、この判定でのブロッキングを推奨していません。 配信よりもセキュリティが優先されますが、この判定に基づいてメッセージをブロックする場合、（Talos の基準で）許容できない数の誤検出が発生します。	アプライアンスに設定されている他のエンジンでメッセージをスキャンする。

判定名	[説明（Description）]	推奨処置
不明（Unknown）	送信者が新しく登録したドメインか、SDR が認識できないドメインを使用しています。この判定不可能なステータスのドメインに対して、Talos は詳細な分析を実行してすばやく判定を確立します。Talos は、この判定でのブロッキングを推奨していません。この判定でブロックすると、しきい値をこの判定に調整した場合の多くの誤検出を許容することになります。Talos では、「不明」の判定でメッセージを検疫することを推奨しています。 Talos がドメインを調査するため、メッセージが後続のエンジンにスキャンされる前に、メッセージの配信が少し遅延します。	メッセージを検疫し、検疫の終了後、アプライアンスに設定された他のエンジンでメッセージをスキャンする。
ニュートラル	送信者が新しいドメインを使用しておらず、送信者のベストプラクティスに従っている場合に通常期待される判定です。送信者のベストプラクティスには、SPF を使用する、DKIM 署名を使用する、スパムを送信しないなどがあります。	メッセージを許可し、アプライアンスに設定されている他のエンジンでスキャンする。
良好	送信者が、メッセージにDKIM署名（「`From:` ヘッダー ドメインに並列」）がある認定済みのドメインを使用している稀な判定です。	メッセージを許可し、アプライアンスに設定されている他のエンジンでスキャンする。

送信者ドメインレピュテーションに基づいてメッセージをフィルタリングする方法

手順	操作手順	詳細情報
ステップ 1	Cisco E メール セキュリティ ゲートウェイで SDR フィルタリングを有効化します。 （注） AsyncOS 12.0 にアップグレードすると、SDR クエリがデフォルトで有効化されます。	Cisco E メール セキュリティ ゲートウェイでの送信者ドメイン レピュテーション フィルタリングの有効化 （5 ページ）
ステップ 2	SDR に基づいてメッセージを処理するためのメッセージまたはコンテンツ フィルタを設定します。	送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 （6 ページ）
ステップ 3：	SDR に基づいてメッセージをフィルタ処理するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチします。	受信メール ポリシーへのコンテンツ フィルタのアタッチ （11 ページ）

Cisco E メール セキュリティ ゲートウェイでの送信者ドメイン レピュテーション フィルタリングの有効化

（注） AsyncOS 12.0 にアップグレードすると、SDR クエリがデフォルトで有効化されます。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [有効化（Enable）] をクリックします。

ステップ 3 [送信者ドメインレピュテーションフィルタリングの有効化（Enable Sender Domain Reputation Filtering）] をチェックします。

ステップ 4 （任意）SDR サービスによって、メッセージの追加の属性によって SDR を確認する場合は [追加属性を含める（Include Additional Attributes）] をチェックします。

このオプションを有効にすると、メッセージの次の追加属性が SDR の確認に追加され、有効性が向上します。

- 「`Envelope From:`」ヘッダー、「`From:`」ヘッダー、および「`Reply-To:`」ヘッダーに存在する電子メールアドレスのユーザ名の部分。
- 「`From:`」ヘッダーと「`Reply-To:`」ヘッダーの表示名。

ステップ 5 （任意）レピュテーション クエリーがタイムアウトになるまでの経過秒数を入力します。

（注） SDR クエリのタイムアウト値を変更すると、メール処理のパフォーマンスに影響を与える可能性があります。

ステップ 6 （任意）アプライアンスで「Envelope From：」ヘッダーのドメインのみに基づく SDR の確認をスキップする場合は、[Envelope Fromのドメインに基づいてドメイン例外リストと一致] をチェックします。

ステップ 7 [送信] をクリックします。

ステップ 8 （任意）「SDR には追加属性契約が含まれます」のメッセージを許可する場合は [同意（I Agree）] をクリックします。

（注） 「SDR には追加属性契約が含まれます」のメッセージは、[追加属性を含める（Include Additional Attributes）] オプションを選択した場合のみ表示されます。

ステップ 9 [確定する（Commit）] をクリックして変更を保存します。

次のタスク

SDR に基づいてメッセージを処理するためのメッセージまたはコンテンツ フィルタを設定します。送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 （6 ページ） を参照してください。

送信者ドメインレピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージフィルタの設定

以下のいずれかの方法で ‘Domain Reputation’ のメッセージまたはコンテンツ フィルタを使用して、SDR に基づいてメッセージをフィルタ処理し、そのようなメッセージに対して適切なアクションを実行できます。

- 送信者のドメインの判定
- 送信者のドメインの経過時間
- 送信者のドメインがスキャン不可

関連項目

- メッセージ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング （7 ページ）
- コンテンツ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング （9 ページ）

メッセージ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング

送信者ドメインの判定に基づいてメッセージをフィルタ処理

（注） 推奨されるブロッキングのしきい値は「Poor」です。SDR 判定の詳細は、SDR 判定 （2 ページ）を参照してください。

構文：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

それぞれの説明は次のとおりです。

- `'drop_msg_based_on_sdr_verdict'` は、メッセージ フィルタの名前です。
- `'sdr-reputation'` は、ドメイン レピュテーション メッセージ フィルタのルールです。
- `'awful'`、`'poor'` は、SDR に基づいてメッセージをフィルタ処理するための送信者のドメイン判定の範囲です。
- `'domain_exception_list'` は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。
- `'drop'` は、メッセージに適用されるアクションです。

例

以下のメッセージでは、SDR 判定が 'Unknown' の場合、メッセージが検疫されます。

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

送信者ドメインの経過時間に基づいてメッセージをフィルタ処理

構文：

```
<msg_filter_name>
if sdr-age (<‘unit'>, <‘operator'> <‘actual value’>)
{<action>}
```

それぞれの説明は次のとおりです。

- ‘sdr-reputation' は、ドメイン レピュテーション メッセージ フィルタのルールです。
- 'sdr_age'は、SDR に基づいてメッセージをフィルタ処理するために使用される送信者ドメインの経過時間です。
- ‘unit' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための ‘days’、‘years’、‘months’、'weeks' オプションです。
- ‘operator'は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための比較演算子です。
  - – >（次の値より大きい）
  - – >=（次の値以上）
  - – <（次の値より小さい）
  - – <=（次の値以下）
  - – ==（次の値と等しい）
  - – !=（次の値と等しくない）
  - – Unknown
- ‘actual value'は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するために使用される数字です。

例

以下のメッセージでは、送信者ドメインの経過時間が不明な場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

以下のメッセージでは、送信者ドメインの経過時間が1ヵ月よりも短い場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

送信者ドメインのスキャン不可能性に基づいてメッセージをフィルタ処理

構文：

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

それぞれの説明は次のとおりです。

- 'sdr-unscannable' は、ドメイン レピュテーション メッセージ フィルタのルールです。

  'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下のメッセージでは、メッセージが SDR チェックに不合格の場合、メッセージが検疫されます。

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

コンテンツ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング

始める前に

- （任意）ドメインのみが含まれたアドレス リストを作成します。作成するには、Web インターフェイスの [メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] ページに移動するか、CLI で addresslistconfig コマンドを使用します。詳細については、メール ポリシーを参照してください。
- （任意）ドメインの例外リストを作成します。詳細については、ドメインの例外リストの作成 （10 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [ドメインレピュテーション（Domain Reputation）] をクリックします。

ステップ 6 SDR に基づいてメッセージをフィルタ処理するために、以下のいずれかの条件を選択します。

- 判定範囲を選択し、SDR サービスから受け取った判定に基づいてメッセージをフィルタ処理するには [送信者ドメインレピュテーション判定（Sender Domain Reputation Verdict）] を選択します。

  （注） 推奨されるブロッキングのしきい値は「Poor」です。SDR 判定の詳細は、SDR 判定 （2 ページ）を参照してください。

- [送信者ドメインの経過時間（Sender Domain Age）] を選択し、比較演算子を選択します。数字を入力し、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための期間を選択します。
- [送信者ドメインレピュテーションスキャン不可（Sender Domain Reputation Unscannable）] を選択し、SDR の確認に失敗したメッセージをフィルタ処理します。

ステップ 7 （任意）Cisco E メール セキュリティ ゲートウェイで、SDR に基づくメッセージのフィルタ処理を避けるホワイトリスト ドメインのリストを選択します。

ステップ 8 [アクションの追加（Add Action）] をクリックして、SDR に基づいてメッセージに実行する適切なアクションを設定します。

ステップ 9 変更を送信し、保存します。

ドメインの例外リストの作成

ドメインの例外リストは、ドメインのみが含まれるアドレスのリストで構成されています。ドメインの例外リストを使用して、Cisco E メール セキュリティ ゲートウェイで設定したメールポリシーにかかわらず、すべての受信メッセージに対する SDR チェックをスキップできます。

（注） 特定のメール ポリシーで受信メッセージに対する SDR コンテンツ フィルタ アクションをスキップする場合は、ドメイン レピュテーション コンテンツ フィルタでドメインの例外リストを選択する必要があります。

ドメインの例外のリストを使用するための条件

SDR チェックをスキップするには、デフォルトで、メッセージの「`Envelope From:`」ヘッダー、「`From:`」ヘッダー、および「`Reply-To:`」ヘッダーが同じで、ドメイン例外リストに設定されているドメインと一致する必要があります。アプライアンスで「Envelope From：」ヘッダーのドメインのみに基づく SDR の確認をスキップする場合は、ドメイン レピュテーションの設定ページで [Envelope Fromのドメインに基づいてドメイン例外リストと一致] を選択します。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [ドメインの例外リスト（Domain Exception List）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 ドメインのみが含まれている必要なアドレス リストを選択します。

ステップ 4 変更を送信し、保存します。

次のタスク

CLI で `domainrepconfig` コマンドを使用してドメインの例外リストを作成することもできます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

受信メールポリシーへのコンテンツフィルタのアタッチ

SDR に基づいてメッセージをフィルタ処理するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチできます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 2 コンテンツ フィルタの下のリンクをクリックします。

ステップ 3 [コンテンツフィルタを有効にする（カスタマイズ設定）（Enable Content Filters (Customize Settings)）] を確実に選択します。

ステップ 4 SDR に基づいてメッセージをフィルタリングするために作成したコンテンツ フィルタを選択します。

ステップ 5 変更を送信し、保存します。

送信者ドメインレピュテーションフィルタリングおよびクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、SDR フィルタリングとメール ポリシーを有効化できます。

メッセージ トラッキングの送信者ドメイン レピュテーション詳細の表示

メッセージ トラッキングを使用して、SDR に基づくメッセージの詳細を表示できます。

始める前に

- E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージ トラッキングを有効にするには、Web インターフェイスで [セキュリ

ティサービス（Security Services）] > [メッセージトラッキング（Message Tracking）] ページに移動します。

- SDRに基づいてメッセージをフィルタリングするためのコンテンツまたはメッセージフィルタが動作していることを確認します。

手順

ステップ 1 [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] に移動します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [メッセージイベント（Message Event）] の下の [送信者ドメインレピュテーション（Sender Domain Reputation）] をクリックします。

ステップ 4 必要な SDR 判定を選択して、SDR サービスから受け取った判定に基づいてメッセージを表示します。

ステップ 5 （任意）SDR チェックに失敗した場合にメッセージを表示するには [スキャン不可（Unscannable）] をチェックします。

ステップ 6 （任意）必要な SDR の脅威カテゴリを選択して、脅威カテゴリに基づいてメッセージを表示します。

ステップ 7 [検索（Search）] をクリックします。

アラートの表示

以下の表では、SDRに対して生成されるアラート、アラートの説明、アラートの重大度を記載します。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.IMH.SENDER_DOMAIN_LOOKUP_FAILURE_ALERTS	The SDR lookup failed. Reason - <$reason> 警告。SDR クエリが失敗した場合に送信されます。	**‘reason’** - SDR クエリが失敗した理由。

ログの表示

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

SDR フィルタリングのログ エントリの例

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

送信者ドメイン レピュテーションの認証の失敗

この例のログは、SDR サービスに接続する際の認証失敗のために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Authentication failure.
```

ソリューション

CLI で `sdradvancedconfig` コマンドを使用すると、Cisco E メール セキュリティ ゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメイン レピュテーションのリクエストのタイムアウト

この例のログは、SDR サービスと通信する際のリクエスト タイムアウトのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Request timed out.
```

ソリューション

SDR リクエストがタイムアウトになると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

送信者ドメイン レピュテーションの無効なホスト

この例のログは、Cisco E メール セキュリティ ゲートウェイで無効な SDR サービス ホストが設定されたために SDR に基づいてフィルタ処理されなかったメッセージが表示しています。

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Invalid host configured.
```

ソリューション

CLI で `sdradvancedconfig` コマンドを使用すると、Cisco E メール セキュリティ ゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメインのレピュテーションの一般的なエラー

この例のログは、不明なエラーのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Unknown error.
```

ソリューション

不明なエラーが発生すると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。