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

Cisco Talos の送信者ドメインレピュテーション（SDR）は、電子メールのエンベロープおよびヘッダーに入力されたドメインに基づいて、電子メールメッセージのレピュテーション判定を提供するクラウドサービスです。たとえば、HELO/EHLO 文字列、エンベロープとヘッダーの「From」アドレス、「Reply-to」アドレス、および「List-Unsubscribe」ヘッダーに含まれるドメインが使用されます。

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。

AsyncOS 14.2.x リリース以降、送信者のドメインの期間経過オプションは、送信者の成熟度に置き換えられます。送信者の成熟度は、送信者のレピュテーションを確立するための重要な機能です。送信者の成熟度は、スパムを分類するために、複数の情報源に基づいて自動的に生成され、「Whois-based domain age」とは異なる場合があります。送信者の成熟度は 30 日の制限に設定されており、この制限を超えるとドメインは電子メール送信者として成熟していると見なされてそれ以上の詳細は提供されません。

このリリース以降、メッセージの送信者ヘッダーを受信した後に、追加の送信者ドメイン レピュテーション チェックが実行されます。（電子メールゲートウェイで）構成された SDR 拒否レベルに一致する脅威レベルのメッセージは拒否されます。

（注） このリリース以降、[SDR ドメインのエージ（SDR Domain Age）] 設定済みフィルタは、[SDR 送信者の成熟度（SDR Sender Maturity）] フィルタに自動的に更新されます。[送信者の成熟度（Sender Maturity）] の値が無効なフィルタは、アップグレード後に「非アクティブ」としてマークされます。メッセージまたはコンテンツフィルタを確認し、適宜変更してください。

（注） 送信者の成熟度機能は、電子メールゲートウェイの現在の時刻を使用して、ログに送信者の成熟度情報を表示し、必要なフィルター条件と照合します。電子メールゲートウェイがタイムゾーンに基づいた正しい時刻で設定されていることを確認してください。

AsyncOS 14.2.x リリースにアップグレードすると、コンテンツまたはメッセージフィルタ、レポート、およびメッセージトラッキングの従来の SDR 判定は、次のように新しい SDR 判定に置き換えられます。

- 信頼できない
- 要検討
- ニュートラル
- 好ましい
- 信頼できる
- 不明

新しい SDR 判定ごとに実行できる推奨されるアクションの詳細については、「SDR 判定 （3 ページ）」を参照してください。

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	推奨処置
信頼できない	最も問題のあるレピュテーション判定です。 最も安全な推奨されるブロッキングしきい値です。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。
要検討	この判定は、誤検出（FP）率が低く、比較的安全ですが、すべての組織にとって安全であるとは限りません。 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、結果的に検出漏れが発生することになります。	電子メールゲートウェイ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。ブロックは確認後にのみ行います。詳細については、送信者ドメイン レピュテーション ポリシーの調整 （6 ページ）を参照してください。
ニュートラル	正当なドメインと混合使用のドメインに割り当てられる最も一般的な判定であり、好ましい判定を受けることを妨げる脆弱性指標が関連付けられます。	電子メールゲートウェイ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	推奨処置
好ましい	送信者は、新しいドメインではない公正なドメインを使用しています。送信者は、SPFの使用、DKIM署名、DMARCの使用、スパムを送信しないなど、送信者のベストプラクティスに従っています。	電子メールゲートウェイ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。
信頼できる	送信者が、メッセージがDKIMによって認証される（「From:」ヘッダードメインに並列）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ます。 後続のエンジンをバイパスする方法の詳細については、「skip-spamcheck」、「skip-viruscheck」などのメッセージフィルタルールを使用します。メッセージフィルタを使用した電子メール ポリシーの適用の「メッセージフィルタ アクション」セクションを参照してください。
不明（Unknown）	送信者は、SDR が認識しないドメイン、またはレピュテーションの確立に使用できないドメインを使用しています。	電子メールゲートウェイ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。

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。	電子メール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）

手順	操作手順	詳細情報
ステップ 2	（オプション）電子メールゲートウェイの SDR 設定を確認して、適切な SDR ポリシーを確立します。	送信者ドメイン レピュテーション ポリシーの調整 （6 ページ）
ステップ 3	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 （7 ページ）
ステップ 4	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 （12 ページ）

電子メール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）電子メールゲートウェイで「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（Match Domain Exception List based on Domain in Envelope From）] をチェックします。

ステップ 7 **範囲スライダ**を動かして、SMTP カンバセーションレベルでメッセージを許可または拒否するために必要な SDR 判定範囲を選択します。

（注） AsyncOS 14.x 以降にアップグレードした後、デフォルトでは範囲スライダは「Untrusted」判定を示します。「Untrusted」判定のメッセージはすべて、SMTP カンバセーションレベルでドロップされます。

（注） 「Favorable」判定は送信者が認証済みドメインを使用していることを示すため、メッセージを拒否するために「Favorable」判定を選択することはできません。

ステップ 8 [送信] をクリックします。

ステップ 9 （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 10 [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

電子メールゲートウェイの SDR 設定を確認して、適切な SDR ポリシーを確立します。送信者ドメイン レピュテーション ポリシーの調整 （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 ポリシーの調整

SDRは、各判定に対してデフォルトの動作を推奨します。ただし、組織にとって検出漏れと誤検出を最適に調整することが不可欠である場合は、指定の手順に従って、セキュリティ要件に基づいて SDR ポリシーを調整します。

手順

ステップ 1 SDR ポリシーアクションを 10 日間設定せずに、電子メールゲートウェイで SDR を有効にします。

ステップ 2 メッセージトラッキング機能を使用して、SDR 判定に基づいてメッセージを確認します。

詳細については、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（13 ページ）を参照してください。「Untrusted」または「Questionable」の判定を受けたメッセージを検索できます。

ステップ 3 メッセージトラッキング検索（手順2で実行）から取得したメッセージで、検出漏れまたは誤検出がないかどうかを確認します。

検出漏れとは、受信者のメールボックスに配信する必要があるが、「Questionable」または特に「Untrusted」という判定を受けたメッセージです。誤検出は、「Untrusted」判定は受けていないが、SDRに関連するメッセージ属性に基づいてブロックされることが予想されるメッセージです。

ステップ 4 （メッセージが「Untrusted」判定を受けたために検出漏れが発生した場合）Cisco TACでサポートチケットを開いた後で、「Untrusted」判定に基づいてメッセージをブロックするようにSDRポリシーを設定してください。

（注） Cisco Talosでは、ほとんどのユースケースで、「Untrusted」判定のメッセージがブロックされると想定されます。

ステップ 5 「Questionable」判定を受けたメッセージに検出漏れが存在する場合は、推奨される安全な「Untrusted」しきい値を使用します。

（注） 「Untrusted」しきい値を使用しない場合は、よりアグレッシブな「Questionable」しきい値に基づいてメッセージをブロックできます。詳細については、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 （7 ページ）を参照してください。

（注） 「Questionable」判定はスパムメッセージを送信する大量の送信者に関連付けられますが、これらの送信者が正当な（ほとんどの場合優先度の低い）大量の電子メールを配信している可能性もあります。セキュリティ要件に基づいて、確認後にメッセージをブロックすることが適切です。

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

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
- 送信者の成熟度
- 送信者のドメインがスキャン不可

（注） AsyncOS 14.2.x リリース以降、送信者のドメインの期間経過オプションは、送信者の成熟度に置き換えられます。送信者の成熟度は、SDR 判定にすでに組み込まれています。特別な使用例を除いて、送信者の成熟度に基づいてメッセージをフィルタリングすることは一般には推奨されません。

関連項目

- 送信者ドメイン レピュテーション ポリシーの調整 （6 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 （8 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 （10 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「Untrusted」です。SDR 判定の詳細についてはSDR 判定 （3 ページ）を、SDR ポリシーの調整については送信者ドメイン レピュテーション ポリシーの調整 （6 ページ）を参照してください。

構文：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['untrusted', 'questionable'], "<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。
- `'untrusted'`、`'questionable'` 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")}
```

送信者の成熟度に基づいてメッセージをフィルタ処理

（注） AsyncOS 14.2.x リリース以降、送信者のドメインの期間経過オプションは、送信者の成熟度に置き換えられます。送信者の成熟度は、SDR 判定にすでに組み込まれています。特別な使用例を除いて、送信者の成熟度に基づいてメッセージをフィルタリングすることは一般には推奨されません。送信者の成熟度は 30 日の制限に設定されており、この制限を超えるとドメインは電子メール送信者として成熟していると見なされてそれ以上の詳細は提供されません。

構文：

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

それぞれの説明は次のとおりです。

- 'sdr-maturity' は、送信者の成熟度のメッセージフィルタルールです。
- ‘unit' は、送信者の成熟度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、送信者の成熟度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、送信者の成熟度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、送信者の成熟度が不明な場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Maturity: if (sdr-maturity ("unknown", "")) {drop();}
```

以下のメッセージでは、送信者ドメインの成熟度が 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_Maturity: if (sdr-maturity ("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 （11 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「Untrusted」です。SDR 判定の詳細は、SDR 判定 （3 ページ）を参照してください。

- [送信者の成熟度（Sender Maturity）] を選択し、比較演算子を選択します。数字を入力し、送信者の成熟度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。

  （注） AsyncOS 14.2.x リリース以降、送信者のドメインの期間経過オプションは、送信者の成熟度に置き換えられます。送信者の成熟度は、SDR 判定にすでに組み込まれています。特別な使用例を除いて、送信者の成熟度に基づいてメッセージをフィルタリングすることは一般には推奨されません。送信者の成熟度は30日の制限に設定されており、この制限を超えるとドメインは電子メール送信者として成熟していると見なされてそれ以上の詳細は提供されません。

- [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）電子メールゲートウェイで、SDR に基づくメッセージのフィルタ処理を避ける許可リストに掲載された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

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。

[Envelope Fromのドメインに基づいてドメイン例外リストと一致（Match Domain Exception List based on Domain in Envelope From:）] オプションが無効で、「HELO:」、「RDNS:」、「Envelope From:」、「From:」、および「Reply-To:」のいずれかのドメインがドメイン例外リストに設定されている場合、SDR チェックはスキップされます。

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 [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。

（注） 電子メールゲートウェイで SDR ベースのコンテンツまたはメッセージフィルタを構成していない場合でも、SDR 判定に基づいてメッセージを追跡できます。

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リクエストのタイムアウト （14 ページ）
- 送信者ドメインのレピュテーションの一般的なエラー （15 ページ）

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。

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。