Cisco Domain Protection：最初の手順

公開日：2018 年 7 月 22 日

重要なプロジェクト チームのメンバーの確認

- **エグゼクティブ スポンサー**：重要な問題/プロジェクト障害のエスカレーション先です。
- **プロジェクトの所有者**：このプロジェクトの成功に責任を持ちます。
- **プロジェクト マネージャ**：このメンバーは主要な連絡先であり、組織へのインターフェイスとして機能します。また、プロジェクトを合意されたスケジュールに沿って確実に進めること、およびその他の内部グループや部門との協力に責任を持ちます。
- **導入エンジニア**：このメンバーは導入のエキスパートとなり、プロジェクトの主要な技術連絡先にもなります。
- **対象分野のエキスパート**：設計と統合へのインプットを提供する技術リーダーです。決定が組織のビジネス上の戦略に即していることを確認します。
  - DNS エンジニア
  - メッセージング アーキテクト
  - セキュリティ アーキテクト

最初の Customer Success コールの前に必要な手順

- **クイック スタート ガイドを確認**します。
- 組織が所有している**ドメインを特定して追加**します。成功させる最初の会議の少なくとも 1 週間前に Cisco に追加された、DMARC `p=none` レコードをもつ電子メールを送信するのに使用される少なくとも 1 つのドメインが必要になります。1 つだけ選択する場合は、組織のプライマリ電子メール ドメインを選択することをお勧めします。
  - `P=none` に **DMARC DNS レコードを作成**して、Cisco への DMARC レポートの送信を開始します。

    作成する DMARC エントリがわからない場合は、[ツール（Tools）] > [DMARC] を使用します。DMARC エントリのないドメインを検索し、クリックしてレコードを作成します。デフォルトの設定を使用するか独自に作成しますが、一旦 [続行（continue）] をクリックすると、コピーして DNS に直接貼り付けられる DMARC エントリが Cisco により提供されます。

  - メイン画面または [設定/ドメインの追加（Configure / Add Domains）] の [ドメインの追加（Add Domains）] ボタンを使用して、**Cisco にドメインを追加**します。
- **ドメインを優先順位付け**して、どれが最初に動作するかわかるようにします。最も重要なドメインとともに、問題のある場合はより影響の少ない、このプロセスの初期段階で動作する、影響を受けにくく複雑度の低いドメインを検討してください。
- 質問の**メモを作成**して、スケジュールされたコールの 1 ～ 2 日前に Customer Success エンジニアに送信します。即座に質問に対応できますが、準備を整えておくことができればセッションはより効果的になります。

最初の会議の前のオプション

Customer Success による会議の前にこれらの手順を完了すると実装が迅速化しますが、最初の会議中または会議後に完了することもできます。

- **トレーニング ビデオを視聴**、および/またはユーザ ガイドを参照します。
- プラットフォームを使用する必要のある、または電子メールのレポートを受信する必要のあるチーム メンバーの**ユーザ アカウントを作成**します。
- 組織が所有する**すべてのドメインを特定して追加**します（法務チームまたはドメイン レジストラに問い合わせるか、VewDNS.info などの Reverse Whois ツールを使用して、依然として組織に登録されている古い非アクティブなドメインを見つけることができます）。
  - すべてのドメインで **`p=none`** に **DMARC DNS レコードを作成**して、Cisco への DMARC レポートの送信を開始します。
  - メイン画面または [設定/ドメインの追加（Configure / Add Domains）] の [ドメインの追加（Add Domains）] ボタンを使用して、**ドメインを追加**します。
- 内部メッセージング インフラストラクチャに対して Agari で**カスタム送信者を作成**します。異なる電子メール プラットフォームに異なる個々のカスタム送信者を作成します。たとえば、Exchange サーバがあり、さらに複数の電子メール通知を送信するアプリケーション サーバがある場合、これらを個別に操作しレポートを作成するため、それぞれに対して異なるカスタム送信者を作成します。[カスタム送信者の設定/管理（Configure / Manage Custom Senders）] でこれを行います。
- プライマリ ドメインの送信者ページで**既知の送信者を承認**します。
- **防御ドメインを確認** – 少なくとも 2 週間分のレポート データにより、電子メール トラフィックのないドメインを確認します。一部の、特に最近登録されたドメインについては不確かである可能性がありますが、確実なドメインは電子メールを送信するものと想定されず、防御として指定され **`p=reject`** に設定される必要があります。また、「**`v=spf1 -all`**」の空の SPF エントリの設定をお勧めします。
- HR やマーケティングなど、組織の電子メールを送信する他のチームの**内部関係者とミーティング**を行い、彼らに影響を与える電子メール セキュリティ プロジェクトで作業していることを知らせます。最初の会議は非公式なものとなる可能性がありますが、これらのチームが電子メールを送信するのにどのツールを使用しているのかを知るための支援プロセスを開始し、これらのツールの管理所有者を見つけるプロセスを容易にするためのネットワーキングを開始します。