Cisco Domain Protection ユーザーガイド

初版：2022 年 12 月 19 日

シスコシステムズ合同会社

www.cisco.com/jp

シスコは、世界各国に 200 を超えるオフィスを開設しています。

各オフィスの住所、電話番号、FAX 番号は当社の Web サイト

（www.cisco.com/jp/go/offices）をご覧ください。

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1

ミッドタウン・タワー

www.cisco.com/jp

更新日：2022 年 12 月 16 日（金曜日）

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。ソフトウェアライセンスまたは限定保証書が見つからない場合は、CISCO 代理店に連絡してコピーを入手してください。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

データはすべて「現状のまま」提供され、CISCO, INC は、明示、黙示、法定を問わず一切の保証を行いません。これらの保証には、正確性、商品適格性、特定目的への適合性、非侵害性の黙示的保証、または履行の過程、取引の過程、使用もしくは取引から生じるあらゆる保証が含まれますが、これらに限定されません。また、CISCO, INC は、代替の物品の調達費用、または利益、データ、もしくはビジネスの損失、または特殊な損害、または間接的、付随的、懲罰的、もしくは結果的に生じる損害について一切の責任を負いません。

いかなる場合においても、CISCO およびその供給者は、このマニュアルの使用または使用不可によって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性が CISCO またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

目次

第 1 章

はじめに

サービス規約

組織内のユーザーがドメイン保護を使用する場合は、事前に必ずCisco サービス規約（TOS）を確認して同意する必要があります。TOS は、次の 2 つの方法のいずれかで提示されます。

- ほとんどの組織の場合、ドメイン保護に最初にログインするユーザーが初めてログインすると、TOS が表示されます。初めてログインしたときに TOS に同意する必要があります。
- マスター販売契約を結んでいる組織の場合、TOS の管理と同意はドメイン保護アプリケーションの外部で Cisco 販売チームによって行われます。

第 2 章

ドメイン保護の新機能

Cisco は、問題の修正から既存の機能の改善、新しい機能の追加まで、常にドメイン保護製品の改善に取り組んでいます。このセクションでは、ドメイン保護の機能の変更について説明します。また、製品の機能に必ずしも関連しているわけではありませんが、ドキュメントの更新についても説明します。

リリース	日付	更新の詳細
2022.12	2022 年 12 月	• **システムドメイングループ**のネームサーバーなしの定義を追加しました。「「ドメイングループ」 ページ 133」を参照してください。
2022.10	2022 年 10 月	• カスタム送信者を指名する機能が [送信者（Senders）] ページで使用できなくなったため、その内容を扱うドキュメントを管理者およびユーザーガイドから削除しました。 • マイナーな編集と修正。 • ヨーロッパと EMEA のお客様向けに、ブランド保護の新しいドメイン「www.bp.agari-eu.com」を発表。
2022.04	2022 年 4 月	• 「ドメインレビュー」ページに DMARC、DKIM、BIMI、SPF のホスティングステータスの詳細を追加しました。「「ドメインステータスの確認」 ページ 100」を参照してください。 • マイナーな編集と修正。
2022.02	2022 年 2 月	• 現在のアプリケーション UI に一致するようにすべての画像を更新しました。
2022.01	2022 年 1 月	• 新しい「SPF ルックアップレコード」ページ。「「Cisco での SPF レコードのルックアップ」 ページ 41」を参照してください。 • 「「電子メールトラフィックレポート」 ページ 116」ページの更新：電子メールの送信に使用する ISP の詳細を追加しました。 • 「「ドメインステータスの確認」 ページ 100」ページの更新：ドメインステータスの概要のルックアップとエラーメッセージの詳細を追加しました。 • [設定（Configure）] > [ドメインの管理（Manage Domain）] から BIMI をプレビューできなくなりました。新しいステップで更新しました。「「ブランドマーク識別子のプレビュー」 ページ 113」を参照してください。 • 「「BIMI レコードの作成」 ページ 112」ページのマイナーな編集と修正。 • 新しいページ「「Cisco での BIMI レコードのホスティングの停止」 ページ 115」。 • 「「エグゼクティブ概要」 ページ 108」に業界平均の計算について説明する注記を追加しました。
2021.03	2021 年 3 月	BP ワークフローの図を追加しました。「「ドメイン保護について」 ページ 15」を参照してください。

リリース	日付	更新の詳細
2020.12	2020 年 12 月	マイナーな編集。
2010.10	2020 年 10 月	その他の編集と修正。
2020.09	2020 年 9 月	その他の編集とマイナーな更新。
2020.08	2020 年 8 月	• 着信 DMARC 可視化を追加しました。「「DMARC の仕組み」 ページ 25」を参照してください。 • [設定(Configure)] メニューから脅威フィードホワイトリストのページにアクセスする方法について説明する更新を追加しました。「「設定メニューからのホワイトリストへのアクセス」 ページ 124」を参照してください。
2020.04	2020 年 4 月	新しい [エグゼクティブレポート(Executive Reports)] ページには、ドメインインフラストラクチャのいくつかの主要な側面に関する概要のレポートが掲載されています。「「エグゼクティブ概要」 ページ 108」を参照してください。
2020.03	2020 年 3 月	この更新には、いくつかのドキュメントのマイナーバグ修正が含まれています。
2020.02	2020 年 2 月	この更新には、ドメイン保護のドキュメントに対する次の改善が含まれています。 • ユーザーに割り当てることができるロールに対して修正が行われました。1 つのロールの名前が変更され、新しいロールが追加されて文書化されました。「「ユーザーアカウント設定」 ページ 146」を参照してください。 • ドメイン保護脅威フィード機能を文書化しました。詳細については、「「脅威フィード」 ページ 124」を参照してください。 • ドメイン保護監査証跡を検索する方法を文書化しました。「「組織アクティビティの検索」 ページ 142」を参照してください。
2019.12	2019 年 12 月	インフラストラクチャ アップグレードの一環として製品スタイルシート(CSS)にいくつか修正を加えました。これにより、ダイアログボックスのタイトルテキストが背景と対照的になって読みやすくなりました。このドキュメントのスクリーンショットを更新しました。

リリース	日付	更新の詳細

2019.11	2019 年 11 月	この 11 月のドキュメントリリースでは、次のようなコンテンツの改善に重点を置いています。
		• このガイドを再編成しました。概要を示すセクションでは、以下のような主題を取り上げています。
		  • 電子メール規格
		  • reject への移行（DMARC）
		  • reject 移行後の送信電子メールエコシステムのモニタリング
		• 識別子アライメントについてのセクションを追加しました。「「識別子アライメントについて」 ページ 58」を参照してください。
		• アラートをホワイトリストに登録する方法についてのセクションを追加しました。「アラートのホワイトリスト登録」を参照してください。
		• SPF レコード長についてのセクションを追加しました。「「SPF レコード長」 ページ 34」を参照してください。
		• 脅威フィードに関する情報を追加しました。「「脅威フィード」 ページ 124」を参照してください。

2019.10	2019 年 10 月	• ドメイン保護の URL を修正しました。 • Cisco の従業員がドメイン保護ユーザーアカウントに変更を加えることができないことを明確にしました。「「ユーザーアカウント」 ページ 145」を参照してください。
2019.04	2019 年 4 月	• DKIM の管理とホスティング Cisco は、DKIM レコードをホストする機能を追加しました。ドメイン保護は、Cisco がホストする DKIM レコードを管理できるようになりました。ドメイン保護の DKIM 管理では、ドメインに使用されている既存の DKIM キーを検出できます。Cisco は、DMARC、SPF、DKIM に関連するすべての DNS レコードをホストできるようになりました。詳細については、「「Cisco での DKIM レコードのホスティング」 ページ 65」を参照してください。

第 3 章

ドメイン保護について

Cisco Domain Protection™ は、ブランドの所有権を保護する場合に便利です。フィッシャやスパマーなど、本人になりすました偽の電子メールを送信して電子メールを悪用する者から顧客を保護できます。ドメイン保護では、そのために送信メール認証を簡単かつ完全に取得できます。この認証は、すべてのドメインと、それらのドメインからメッセージを送信するすべてのユーザーを対象とする、DMARC ポリシーによって確立された認証です。

DMARC（Domain-based Message Authentication, Reporting & Conformance）は、電子メール認証、ポリシー、レポートのプロトコルです。広く展開されている SPF（Sender Policy Framework）および DKIM（DomainKeys Identified Mail）プロトコルを基礎として、不正な電子メールからドメインを保護するべく、次の方法で改善とモニタリングを実施しています。

- 作成者（「From:」）ドメイン名へのリンクを追加します。
- 受信者が認証失敗を処理するためのポリシーを公開します。
- 受信者から送信者に報告します。

このガイドでは、DMARC を紹介します。また、Cisco Domain Protection を使用して組織に DMARC を実装するプロセスをガイドし、DMARC ステータスを最新の状態に保つ方法について説明します。ここで取り上げるトピックは次のとおりです。

- SPF、およびドメインの SPF DNS レコードの構築。「「SPF：Sender Policy Framework」 ページ 32」を参照してください。
- DKIM、およびドメインの DKIM DNS レコードの構築。「「DomainKeys Identified Mail（DKIM）」 ページ 58」を参照してください。
- DMARC、およびドメインの DMARC DNS レコードの構築。「「DMARC の実装」 ページ 82」を参照してください。
- モニターから拒否への DMARC の移行。「「拒否への移行」 ページ 98」を参照してください。
- Cisco での DNS レコードのホスティング。
- ドメイン、送信者、IP アドレスの変更など、ドメインの継続的なモニタリング。
- 電子メールトラフィックレポート。「「電子メールトラフィックレポート」 ページ 116」を参照してください。
- アラート（アラートの登録など）。「「アラート」 ページ 129」を参照してください。
- ドメイン保護管理（ユーザーアカウントやユーザーロールなど）。

対象読者

このガイドは、組織の DMARC の管理に着手している電子メール管理者を対象としています。

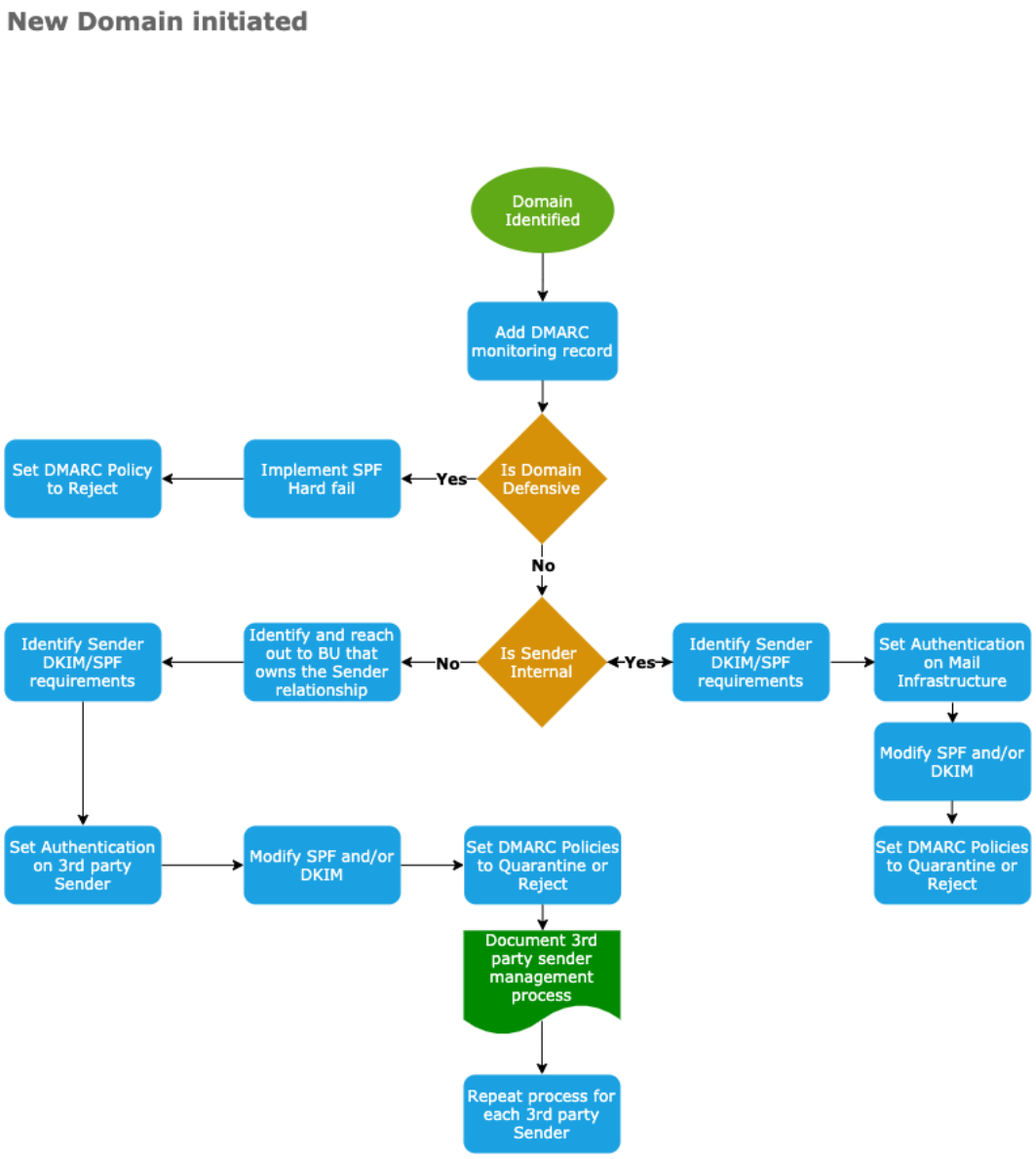
必要に応じた支援による DIY アプローチ

ドメイン保護とこのガイドを使用することにより、ドメインの DMARC ポリシーのセットアップ、管理、および保守のプロセス全体を容易に実行できます。

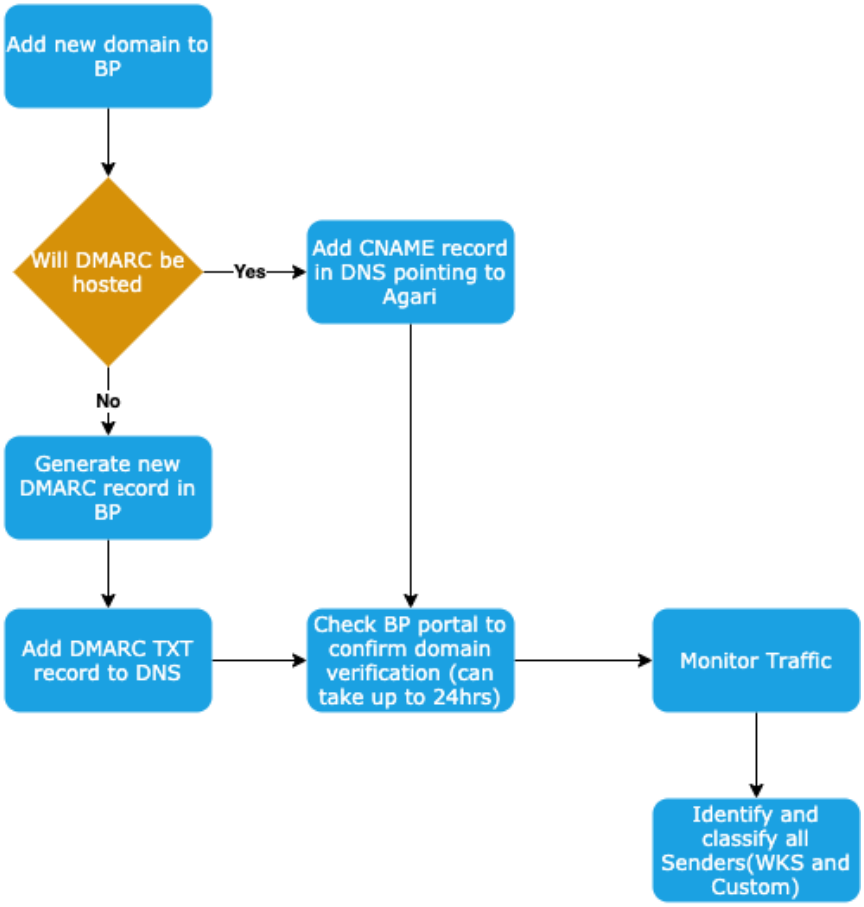
ドメイン保護は、ユーザーのブランドを持つ電子メールに関するデータの可視化を実現するとともに、そのデータを有意義な方法で分析するツール、DMARC を実装するためのさまざまなファイルを生成するツール、およびユーザー インターフェイスから有効にできないタスクを実行するために役立つヒントを提供します。

ブランド保護ワークフロー

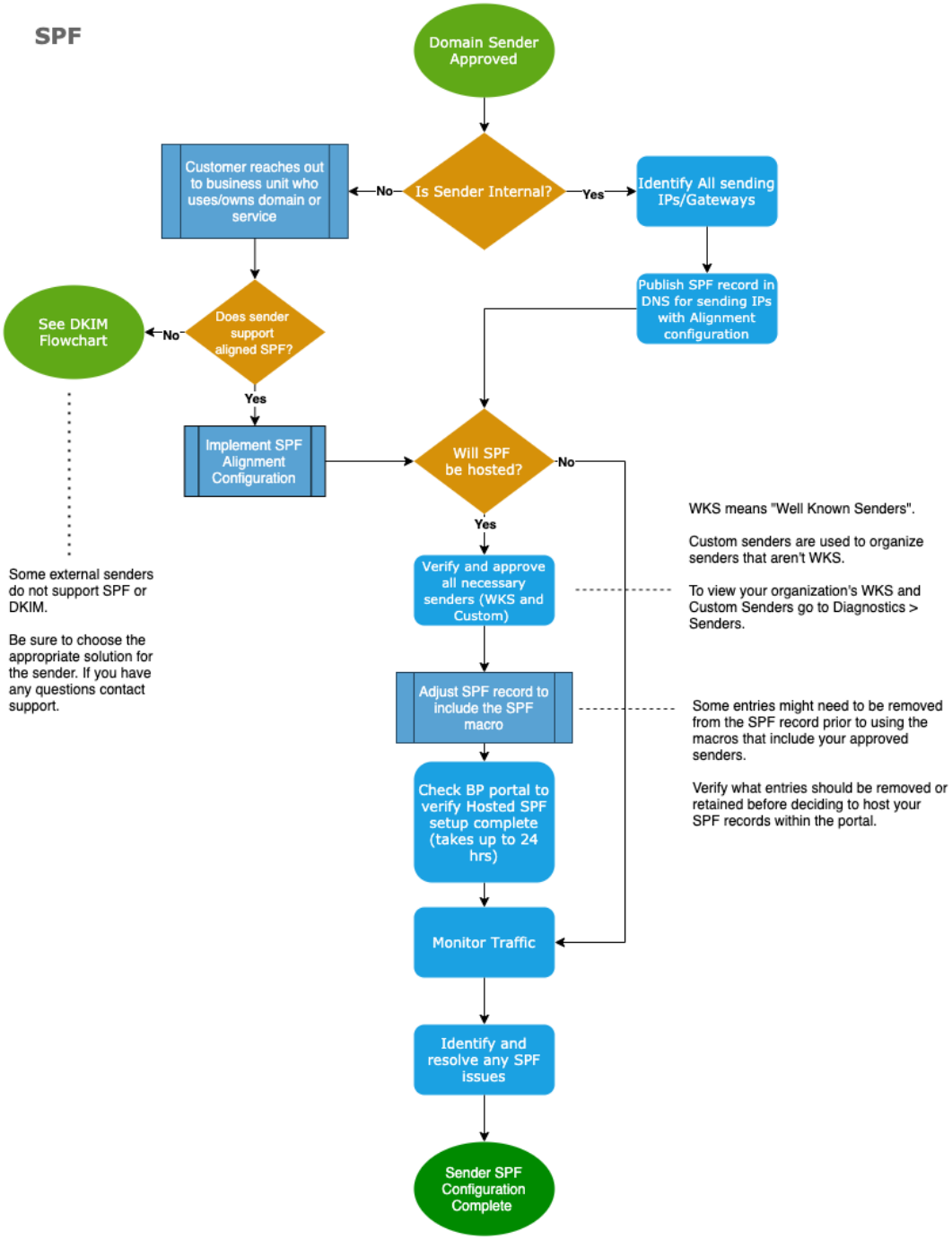
次の図は、基本的なドメイン保護ワークフローを示しています。

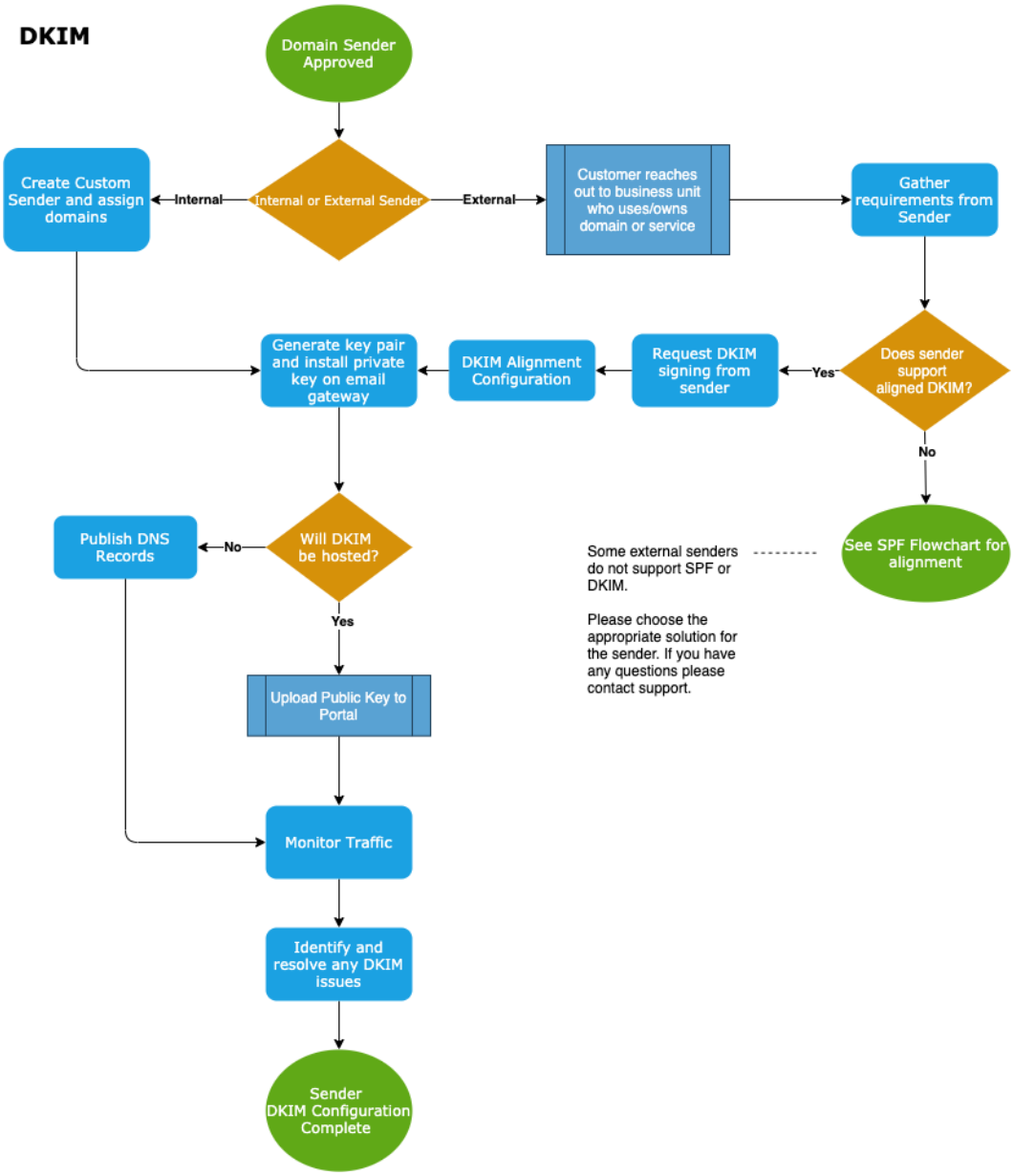


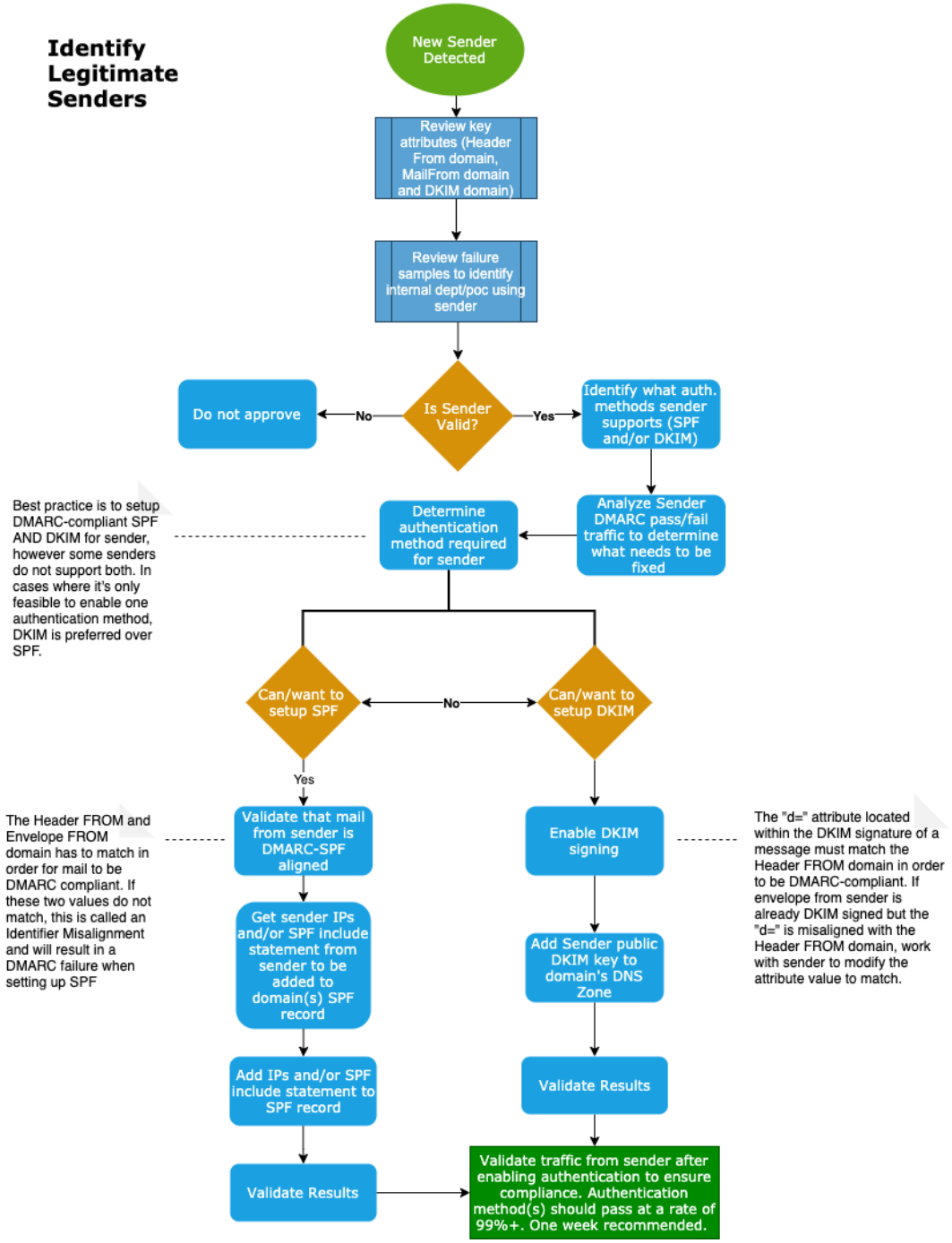
DMARC



NOTE: We can also verify domains without using a DMARC record, if DNS SOA is the same as other domains, in which case BP will assume you also own it.


SPF
Domain Sender Approved
Is Sender Internal?
No
Yes
Customer reaches out to business unit who uses/owns domain or service
Identify All sending IPs/Gateways
Publish SPF record in DNS for sending IPs with Alignment configuration
Does sender support aligned SPF?
No
See DKIM Flowchart
Yes
Implement SPF Alignment Configuration
Will SPF be hosted?
No
Yes
Verify and approve all necessary senders (WKS and Custom)
Adjust SPF record to include the SPF macro
Check BP portal to verify Hosted SPF setup complete (takes up to 24 hrs)
Monitor Traffic
Identify and resolve any SPF issues
Sender SPF Configuration Complete
Some external senders do not support SPF or DKIM.
Be sure to choose the appropriate solution for the sender. If you have any questions contact support.
WKS means "Well Known Senders".
Custom senders are used to organize senders that aren't WKS.
To view your organization's WKS and Custom Senders go to Diagnostics > Senders.
Some entries might need to be removed from the SPF record prior to using the macros that include your approved senders.
Verify what entries should be removed or retained before deciding to host your SPF records within the portal.


DKIM
Domain Sender Approved
Internal or External Sender
Internal
External
Create Custom Sender and assign domains
Customer reaches out to business unit who uses/owns domain or service
Gather requirements from Sender
Does sender support aligned DKIM?
Yes
No
Request DKIM signing from sender
DKIM Alignment Configuration
Generate key pair and install private key on email gateway
See SPF Flowchart for alignment
Some external senders do not support SPF or DKIM.
Please choose the appropriate solution for the sender. If you have any questions please contact support.
Will DKIM be hosted?
No
Yes
Publish DNS Records
Upload Public Key to Portal
Monitor Traffic
Identify and resolve any DKIM issues
Sender DKIM Configuration Complete



DMARC について

DMARC（Domain-based Message Authentication, Reporting, and Conformance）は、業界コンソーシアムの DMARC.org が電子メール チャネルを保護するために 2012 年に公開したオープン電子メール標準です。DMARC は、すでに確立されている電子メール認証標準を拡張するものであり、電子メール送信者が電子メール受信者に対して、送信している電子メールが本当に自分からのものであることを伝える唯一の方法です。

DMARC により、電子メールを送信する企業は、次のことが可能になります。

- ユーザー自身のインフラストラクチャから送信されたメッセージやサードパーティから送信されたメッセージを含め、それらの企業の電子メール送信ドメインの正当なすべての電子メールメッセージおよび送信元を認証できます。
- 電子メールメッセージに対するアクションをメールボックスプロバイダーに指示する明示的なポリシーを公開できます。ポリシーでは、本物であることが証明されたメッセージを受信トレイフォルダに送信するように指示できます。本物でないことが証明されたメッセージは、迷惑メールフォルダに送信するか完全に拒否することができます。これにより、不用心な受信者が攻撃から保護されます。
- 誰が企業のドメインからメールを送信しているのかがわかるようになり、電子メールストリームに関するインテリジェンスを得ることができます。このデータは、顧客に対する脅威を特定するだけでなく、気付かない可能性のある正当な送信者を発見するためにも役立ちます。

経緯：DMARC の必要性

電子メールは、その重要性、普遍性、および耐久性にもかかわらず、これまで決して安全なものではありませんでした。

セキュリティに関するこれまでの試みでは、他者のアイデンティティを使用して電子メールを送信できるという電子メールの基本的な欠陥を解決できませんでした。この脆弱性のために、世界で最も高い評価を得ているブランドの力が犯罪者に利用されています。それらの犯罪者は、電子メールにより、ほとんどすべてのブランドを利用してスパム メールやフィッシング メールを送信し、マルウェアをインストールして、顧客に直接的な損害を与えるとともに、企業が何年もかけて築き上げたブランド エクイティを失わせます。

Facebook、Apple、JPMorgan Chase、PayPal などの世界で最も賞賛されているブランドの多くでは、顧客とブランドを保護するために DMARC 標準が採用されています。

DMARC を使用する企業は、それらの企業のドメイン名を使用して送信される正当なメールと不正なメールに関する前例のない可視性を獲得します。DMARC の驚くべき機能により、ユーザーからのものであると主張してサードパーティ、ビジネス ユニット、攻撃者などから送信されるさまざまなメール ストリームのすべてを把握できるようになります。DMARC を採用した企業への全体的な影響は、ブランド エクイティの維持、電子メール詐欺に関するカスタマー サポート コストの削減、および企業の電子メール チャネルにおける信頼と関与の回復です。

世界の受信トレイの 70 % で有効になっており、最先端のセキュリティを実装するブランドでも採用されているオープン スタンダードの DMARC は、インターネット規模の電子メール保護を実現し、電子メール サイバー攻撃による正当なブランドの不正使用を防止する唯一のソリューションです。

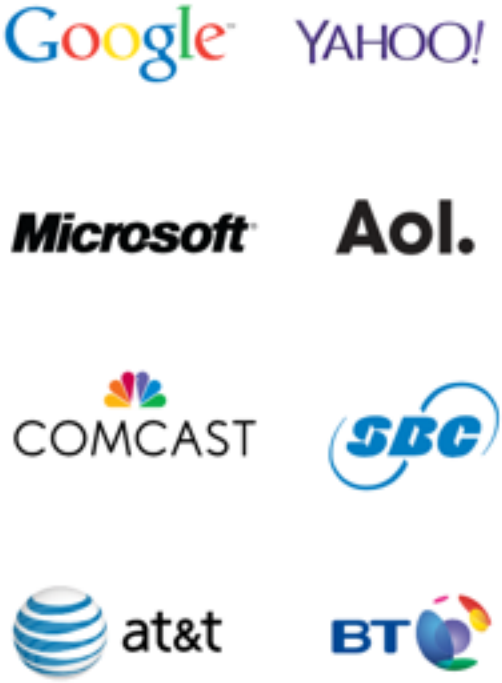
DMARC の支持者

DMARC は、世界最大の送信者、受信者、および業界のコンソーシアムによって支持されています。世界中の 25 億以上のメールボックスが DMARC に対応しています。

DMARC 標準を支持する世界最大規模の電子メール送信者には、以下の組織が含まれます。

DMARC を支持している送信者。

DMARC 標準を支持する世界最大規模の電子メール受信者には、以下の組織が含まれます。



DMARC を支持している受信者。

さらに、DMARC 標準は、以下の政府機関および産業通商組織によって支持されています。

政府機関

NIST：米国国立標準技術研究所
https://www.nist.gov/ [英語]

FTC：米国連邦取引委員会
https://www.ftc.gov/ [英語]

GOV.UK：https://www.gov.uk/ [英語]

業界団体

OTA：Online Trust Alliance
https://otalliance.org/ [英語]

M3AAWG：Messaging Malware Mobile Anti-Abuse Working Group
https://www.m3aawg.org/ [英語]

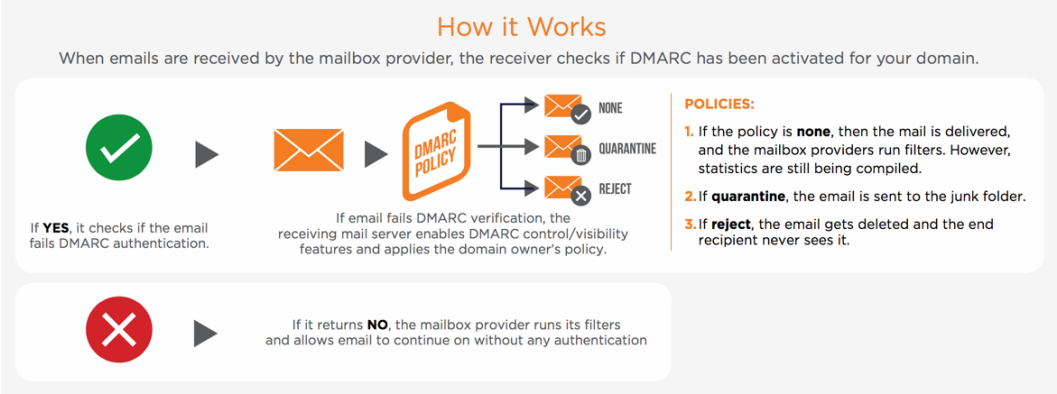
DMARC.org：https://dmarc.org/ [英語]

FS-ISAC：Financial Services Information Sharing and Analysis Center
https://www.fsisac.com/ [英語]

NH-ISAC：National Health Information Sharing and Analysis
https://nhisac.org/ [英語]

DMARC 強制とは

組織の DMARC ポリシーを設定することによって、ユーザーは電子メール送信者として、メッセージが保護されていることを示すことができます。このポリシーにより、DMARC に含まれるいずれかの認証方式に合格した（または合格しなかった）場合のアクションが受信者に通知されます。



DMARC の仕組み。

DMARC の利点

- ブランド保護

犯罪者は自分の利益のために他者のドメインを利用しようとしており、その対策は待ったなしの状態です。その犯罪行為がフィッシングであれ、マルウェアの拡散であれ、あるいは迷惑なスパムであったとしても、それらの攻撃によってブランドは損害を被ります。

- 電子メールの配信可能性の向上

正当なメッセージであっても、受信者が正当なメッセージと不正なメッセージを識別できなければスパム フォルダに入れられる可能性があります。

DMARC を導入することにより、不正なメッセージを排除すると同時に、正当なメッセージの配信可能性を向上させることができます。

- サービス コール

顧客は、そもそもフィッシング メッセージを受け取ることがなければ、そのようなメッセージに関して電話や電子メールで問い合わせることはありません。Cisco のお客様では、フィッシングメッセージが多かったドメインで拒否ポリシーを公開した後に 60 人のスタッフを別の場所に再配置できた事例があります。

- サイバー攻撃のリスクの可視性

自社に代わって電子メールを送信しているすべてのサードパーティ企業を把握できていますか。サードパーティ送信者は必要ですが、顧客、従業員、またはパートナーの詳細情報をサードパーティに提供するたびに、サイバー攻撃のリスクが増大します。DMARC を使用すると、代行送信するすべてのサードパーティを把握し、それらが電子メールのベスト プラクティスに準拠していることを確認できます。

着信上の利点

DMARC を実装することにより、ある種の着信電子メールの脅威（BEC など）も防ぐことができます。

BEC とは

ビジネス メール詐欺（BEC）は、攻撃者が会社の役員になりすまして、不正な代替口座への電信送金を要求する偽装電子メールを送信する着信上の脅威です。この攻撃を防がなければ、多くの場合、侵入され、被害者のクレデンシャルにアクセスされます。

特性

- ソーシャルエンジニアリングとデジタル偽装を活用しています。
- 悪意のあるリンク、コンテンツ、マルウェアのいずれも含まれていません。
- 主要なセキュア電子メールゲートウェイを容易に回避します。

DMARC と着信上の脅威：部分的な解決策

DMARC を適切に設定することにより、攻撃者が、「差出人」アドレスを使用して、保護されたドメインから発信されたように見える電子メールを送信するフィッシング攻撃を防ぐことができます。これは、発信フィッシングを防ぐためには最適ですが、着信トラフィックの許容される解決策とはなりません。

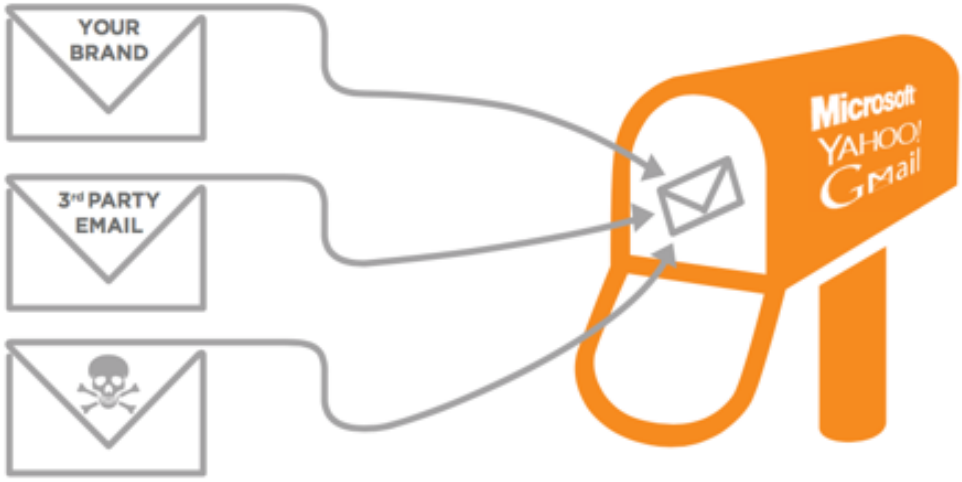
DMARC ポリシーによる着信上の脅威の防止：

着信偽装の手法	DMARC による対処
直接/同一ドメインのスプーフィング	可
表示名のスプーフィング	不可
類似したドメインのスプーフィング	不可

DMARC は BEC や高度な着信上の脅威に部分的に対処できますが、あらゆる形式の送信者アイデンティティの偽装を識別する包括的なレイヤによってゲートウェイ保護を強化する必要があります。

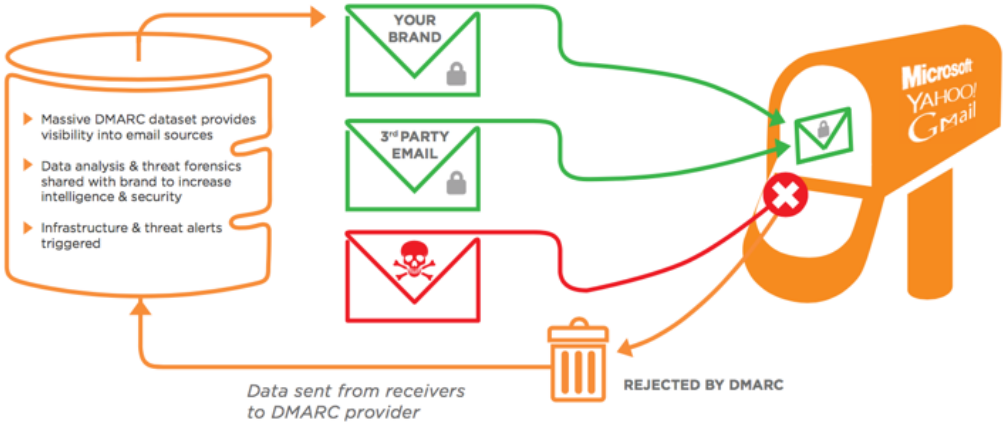
DMARC の利点：実装する前と後

DMARC を使用しない場合、ブランドは、電子メールの送信にドメインがどのように使用されているのかを十分に把握できません。



DMARC の実装前。

DMARC は、すべての電子メール トラフィックを可視化した後に、認証されていない電子メールを処理する方法を受信者に指示します（これらのすべてをメール フローの外部で実現）。



DMARC の実装後。

DMARC の仕組み

DMARC モデルでは、ポリシー公開のメカニズムとして DNS が使用されます。DMARC レコードは、DMARC 固有の名前空間で TXT DNS レコードとしてホストされます。DMARC 名前空間は、DMARC に準拠させる電子メール ドメインの前に「_dmarc.」を付加することによって作成されます。たとえば、「example.com」という電子メール ドメインが DMARC レコードを公開する場合は、「_ dmarc.example.com」で TXT レコードの DNS クエリを発行することにより、DMARC レコードが取得されます。

DMARC 仕様では、送信者の電子メール ドメインから送信されたものであると主張する電子メールの処理方法を通知するために受信者が使用するパラメータを含むポリシー レコードを、送信者が公開できます。DMARC によって実現される機能は次のとおりです。

- 柔軟なポリシー。DMARC モデルでは、電子メール送信者は次の 3 つのポリシーのいずれかを、基盤となる認証チェックに合格しなかった電子メールに適用するポリシーに指定できます。

DMARC ポリシー オプション

DMARC ポリシーの設定	構文	受信者によるアクション
なし（「モニタ」）	p=none	「p=none」ポリシーは、ポリシーを適用する必要がないことを意味します。つまり、ドメイン所有者は DMARC チェックに合格しなかった場合のアクションを受信者に依頼しません。このポリシーは、「モニタ」ポリシーと呼ばれる場合もあります。このオプションは、送信者が単に受信者からのフィードバックを収集する場合に使用されます。このポリシーにより、ドメイン所有者は、SPF/DKIM を導入していなくてもドメインを使用するメッセージに関するレポートを受け取ることができます。それによって、たとえば、ドメインが悪用されているかどうかを判断できます。メッセージの処理方法は変更されませんが、ドメイン所有者は、どのメールがそのドメイン名のもとで送信されているのかをある程度把握できるようになります。まだ SPF または DKIM を導入していない場合は、レポート機能を利用するために、まず DMARC ポリシーを公開することから着手してください。
検疫	p=quarantine	検疫ポリシーでは、認証チェックに合格しなかった電子メールは、疑念を持って処理する必要があります。検疫ポリシーは、受信者に「DMARC に合格しなかったメッセージを追加の処理のために隔離しておく」ことを指示します。ほとんどの受信メール システムでは、これらのメッセージがエンドユーザーのスパム フォルダに格納されます。これにより、エンドユーザーがさらに何らかの形でスパム対策の監視を強化したり、「不審なもの」としてタグ付けすることにつながったりする可能性があります。
拒否	p=reject	DMARC チェックに合格しなかったメッセージは受け入れられません。

- サブドメイン固有のポリシー。DMARC レコードでは、最上位のドメインとサブドメインに異なるポリシーを指定できます（「p=」タグと「sp=」タグを使用）。
- ポリシーの段階的公開。DMARC レコードには、DMARC ポリシーが適用される電子メールストリームの量を指定する「パーセンテージ」タグ（「pct=」）を含めることができます。この機能を使用すると、送信者は、十分な運用経験が得られて「100% カバレッジ」に移行するまで、段階的に強化されたポリシーを試すことができます。
- 識別子アライメントの柔軟性。DMARC 仕様では、ドメイン所有者は、識別子配置のセマンティックを制御できます。ドメイン所有者は、SPF と DKIM の両方で生成される認証済みドメイン識別子に関して、厳密なドメインの一致が必要かどうか、あるいは親ドメインとサブドメインのいずれかまたは両方が一致していると見なすことができるかどうかを指定できます。
- フィードバックの制御。DMARC レコードには、電子メール ドメイン所有者に送信されるフィードバックに関して、場所、頻度、および形式を指定するパラメータが含まれています。

DMARC と Cisco Domain Protection によって追加される機能

DMARC は、SPF と DKIM によって提供される機能に重要な機能を追加します。

- SPF と DKIM の認証に合格しなかった場合のアクションに関する柔軟なポリシー オプション：これは悪意のある電子メールを排除するために必要でありながら SPF 仕様と DKIM 仕様に「欠けている部分」です。
- ユーザーのドメイン名を使用するすべての電子メール送信者に関するデータを収集する機能：DMARC では、ユーザーが選択したアドレスに XML 形式のデータが送信されます。

電子メール データの量が一般に非常に多いことなどのために、DMARC で生成される XML データは処理が難しい場合があります。データの処理と分析においては、次のような要件に注意してください。

- 傾向を可視化するには、データを全体として分析する必要があります。
- 送信者の詳細情報を分析するには、個別の電子メールを利用できる必要があります。
- 脅威と正当な送信者の両方に関する洞察を得るには、履歴データを保存する必要があります。

Cisco のデータ分析は、電子メールの量が世界最大規模の送信者の協力を得て行われており、その恩恵をユーザーに提供しています。それは、ユーザーが DMARC からのデータを解釈して理解するために役立ちます。また、Cisco では、ユーザーインターフェイスの外部で実行する必要のあるすべての関連タスクに関して、適切にフォーマットされたファイルの作成を支援しています。

ドメイン保護は、次のように、プロトコル間の欠けている部分を埋めます。

- 電子メールエコシステムの業界理解に基づく解釈をレポートします。
- 実際のサンプル電子メールメッセージを可視化します。
- 実装の主要手順のガイダンスを提供します。

ホストされた DNS レコード

Cisco は、DMARC、SPF、DKIM の各レコードをホストできます。Cisco が DMARC、SPF、KIM の各レコードをホストするというのは、ドメイン保護で加えた変更が DNS で迅速、安全、かつ自動的に更新されるということです。

通常、DMARC、SPF、DKIM で何か変更を加えたら、レコードが変更されたドメインごとに 1 つずつ自身のホストレコードを手動で更新する必要があります。これには不要な作業が多数発生することがあります。ドメインの数が多い場合には特にそうです。たとえば、DMARC の場合、p=none（モニター）から始めて、次に検疫に進み、最後に拒否に到達することが目標です。管理しているドメインが 1,000 個ある場合を考えてみます（ドメイン保護では可能です。Business Fraud Protection では 5 個のドメインに制限されています）。この場合、DMARC の移行ごとに 1,000 個の DNS レコードを変更する必要があります。

次に、Cisco が DMARC（および SPF と DKIM）レコードをホストしているとします。ドメインの数は同じく 1,000 個で、そのすべてをモニターから検疫に移行したいと考えています。ドメイン保護では、そのようなドメインの DMARC レコードにその変更を一度に加えることができます。また、Cisco が DMARC レコードをホストしている場合は、1,000 個すべてのドメインに対してその変更が自動的に（かつ迅速かつ安全に）行われます。

着信 DMARC 可視化

この機能を使用すると、Agari 電子メールセンサーを介して会社が所有するドメインの着信電子メールを DMARC で可視化できます。

たとえば、Acme 社が Agari Brand Protection 製品内に複数のドメインを登録しているとします。そうしたドメインの 1 つが hr.acme.com で、会社の人事部門はこれを送信ドメインとして使用して、直接またはサードパーティサービスを介して従業員に人事関連の電子メールを配信しています。acme.com のユーザーが hr.acme.com から電子メールを受け取ると、センサーがこの電子メールを処理し、ドメイン保護製品内でこのドメインの DMARC 結果を得ます。DMARC が適用されているため、従業員がこれらの電子メールを受信していると確信が持てるようになります。

着信 DMARC 可視化を使用するには、Cisco フィッシング防御 にセンサーをセットアップする必要があります。「「着信メッセージのモニタリング」 ページ 136」を参照してください。

DMARC の実装

このガイドの残りの部分では Cisco Domain Protection による DMARC の実装プロセスについて詳しく説明しますが、大まかなプロセスは次のようなものです。ドメイン所有者が DMARC に準拠するには、これらの 3 つのアクティビティを実行する必要があり、これらを必要に応じて保護する予定のドメインごとに繰り返します。

DMARC レコードの公開

受信者からのフィードバックの収集を開始するには、DMARC レコードをドメイン名が「_dmarc.<your-domain.com>」の TXT レコードとして公開します。

“v=DMARC1; p=none; rua=mailto:dmarc-feedback@<your-domain.com>;

これにより、DMARC 準拠の受信者は、集約フィードバックを生成して「dmarc-feedback@<your-domain.com>」に送信します。「p=none」タグを使用すると、ドメイン所有者がフィードバックの収集にのみ関心があることを受信者に知らせることができます。

電子メール認証の導入：SPF と DKIM

SPF の導入手順には、電子メールドメインに代わって送信することを認可されたすべてのサーバを記述する SPF レコードの作成と公開が含まれます。小規模の組織では、一般に、単純な SPF レコードが使用されています。一方、複雑な組織は、多くの場合、さまざまなデータセンター、パートナー、およびサードパーティの送信者を認可する SPF レコードを保持しています。DMARC で提供される集約フィードバックは、SPF レコードのブートストラップ中に正当なサーバを特定するために役立つ場合があります。

DKIM を導入するには、ドメイン所有者が、電子メール サーバを設定して DKIM 署名を電子メールに挿入し、DNS で公開キーを公開する必要があります。DKIM は、広く利用され、主要なすべての電子メールベンダーでサポートされています。DMARC で提供される集約フィードバックを参照すると、DKIM 署名のない電子メールを送信するサーバーを特定できる場合があります。

識別子アライメントが適合していることの確認

DMARC で提供される集計フィードバックを使用すると、基盤となる認証テクノロジーが電子メールドメインと合致しない認証済みドメイン識別子を生成している場所を特定できます。アライメントの不一致が特定されたらすぐに修正できます。

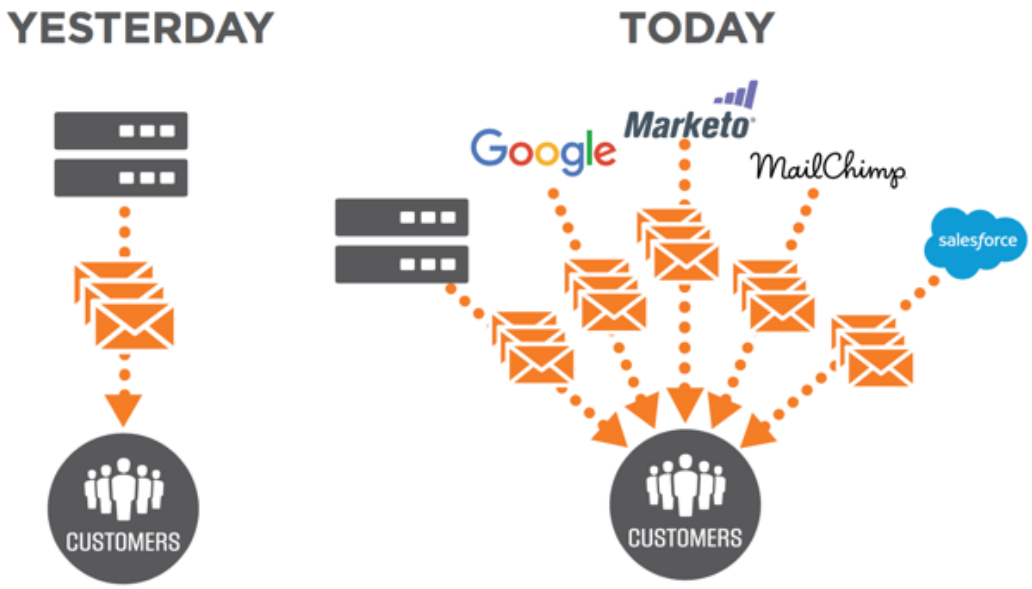
DMARC の実装を可視化するのが容易でない理由

低い可視性

ほとんどの企業では、DMARC レポートから集約データを取得するまで、電子メール エコシステムがどれほど複雑かが認識されません。標準のレポートは、ドメイン名、IP アドレス、および認証の詳細を示す個別の XML ファイルの形式で提供されます。この XML データを解析して可視化することができる多数のツールが存在しますが、ストリームの意味を理解し、ドメインの認証ステータスを向上させるために必要な後続のアクションを特定することは非常に難しく、電子メール フローを熟知しないとエラーが発生しやすくなります。

サードパーティ送信者の検出と許可

DMARC の導入過程で最も困難な部分は、すべてのサードパーティ送信者を把握し、正当な送信者が確実に正しく認証されるようにすることです。平均すると、顧客は Salesforce.com、Marketo、MailChimp などのサードパーティを通じて正当な電子メールの 64% を送信しています。



サードパーティ送信者の普及

「不適切な行為」のコスト

新しいメッセージング プラットフォームも登場していますが、電子メールは依然として組織のコミュニケーションとデジタル エンゲージメントの最も重要な手段でありつづけています。認証を不適切に設定すると、誤検出、配信可能性の問題、およびブランドの毀損が発生する可能性があります。配信不能な電子メールのビジネスへの影響が不明である場合や予測できない場合は、拒否ポリシーに移行する最後の手順を実行することが、非常に困難な見通しとなる可能性があります。

「正当な」電子メールの指定

Cisco Domain Protection と DMARC の仕様により、ブランドを悪用している可能性のある不正な送信者と区別して、ユーザーのドメイン「から」メールを送信する正当な（承認された）送信者を特定し、認可することができます。

必要な作業

DMARC の実装をするには、仕様の内容と使用方法をある程度専門的に理解する必要がありますが、管理やコミュニケーションも必要になります。ある程度の時間をかけることで、多くの場合、組織の内部と外部の両方の電子メール送信者を熟知できます。

「p=reject」の DMARC ポリシーへの移行

DMARC は、当初はドメインの DNS レコードに TXT レコードを追加することによって実装されます。このファイルに含まれるプロパティと値を編集すると、ユーザーが制御するドメインに DMARC がポリシーを適用する方法を指定することができます。

DMARC 実装プロセスの最終目標は、「p=reject」のポリシー（ポリシーは「p」というラベルを持つ）に移行することです。この拒否ポリシーは、電子メール受信者に、すべての非準拠電子メールを破棄する必要があることを通知します。ただし、DMARC 仕様には、メール フローに影響を与えることなく段階的に実装するためのさまざまなポリシーが含まれています。DMARC ポリシーの段階的な導入と強化を可能にすることが、この仕様を設計する上での主要な目標でした。「「DMARC の仕組み」 ページ 25」を参照してください。

サブドメインまたはドメインの単純な「モニタリング モード」レコードから始めます。このレコードは、DMARC 受信者に、ユーザーの（サブ）ドメインを使用して受け取るメッセージに関する統計情報を送信することを要求します。メッセージング インフラストラクチャにまだ SPF または DKIM を実装していなくても、この作業を行うことができます（ただし、それらを実装するまでは次のステップに進むことができません）。

SPF（「新しい SPF レコードの構築と提案」 ページ 39）と DKIM（「DomainKeys Identified Mail（DKIM）」 ページ 58）を導入すると、それらのチェックに合格したメッセージの数および送信元と、合格しなかったメッセージの数および送信元が報告されるようになります。これにより、正当なトラフィックのうち、それらで対処できた量とできなかった量を容易に把握し、問題のトラブルシューティングを行うことができます。また、不正なメッセージが送信された数とそれらの送信元も確認できるようになります。

正当なトラフィックのすべてまたは大部分が SPF と DKIM によって保護されていると思われる場合は、「検疫」ポリシーを実装できます。これにより、ユーザーのドメインを使用したメッセージでそれらのチェックのどちらにも合格しなかったものをローカルのスパム フォルダに相当する場所に入れるように DMARC 受信者に依頼できます。このポリシーを一定割合の電子メール トラフィックにのみ適用するように要求することもできます。この場合も、メッセージに何が起こっているのかを確認できる統計レポートが得られます。

いずれは、実装上の問題の解決具合に合わせて、ユーザーが望むペースでその割合を 100 % に増やすことができます。最後には、DMARC チェックに合格しなかったすべてのメッセージが顧客の受信トレイではなくスパム フォルダに入れられるようにする必要があります。

DMARC の前提条件

ドメイン保護を使用して DMARC の実装を開始する前に、次のタスクを実行する必要があります。

ドメイン保護にアクセスできることの確認

Cisco の担当者から、少なくとも 1 つのユーザーアカウントに、https://dmp.cisco.com にあるドメイン保護へのアクセスが提供されます。

Cisco のサポートにお問い合わせください（https://www.cisco.com/c/en/us/support/all-products.html）。

この 1 つのユーザー アカウントが管理者アカウントです。この最初のアカウントから追加のユーザー アカウント（委任された管理権限または読み取り専用権限用の異なるロールとアクセス許可を持つ）を作成できます。詳細については、「「ユーザーアカウント」 ページ 145」を参照してください。

ドメインリストの収集

組織のために保護するドメインおよびサブドメインのリストが必要です。このリストには、組織のプライマリドメイン、つまり組織に最も関連付けられているドメインおよび電子メールの送信に最もよく使用されるドメイン（たとえば、coltrane.net）を含めてください。さらに、組織が所有して維持する防御ドメインやテストドメイン（たとえば、blue.coltrane.net、coltrane-soprano.net、coltrane-tenor.net、a-love-supreme.net など）も含めることをお勧めします。過去の合併と買収の事例のほか、製品およびプロセスを区別するためにドメインが作成されて使用された特定の事例にも留意してください。

DNS を変更できる機能の取得

保護する予定のドメインのドメイン ネーム システム（DNS）レコードを変更する機能が必要です。DMARC 認証プロトコル（および SPF プロトコルと DKIM プロトコル）は、認証を実行するために DNS サービスに依存しています。ドメイン保護への最初のデータ フローの実現から、モニタから拒否への DMARC ポリシーの変更にいたるまで、ドメイン保護のプロセスの全体を通して、DNS を変更する必要があります。

ステークホルダーのリストの作成

組織のすべての発信電子メールを認証するプロセスには、組織の規模に応じて多数のグループが含まれる場合があります。たとえば、次のような事例が考えられます。

- マーケティングチームが、サードパーティ製ソフトウェアを使用して、潜在顧客に電子メールブラストを送信します。
- サポートチームが、既存の顧客と直接およびサポートソフトウェアを介して連絡を取ります。
- 事業継続チームが、注文の確認や領収書をバックエンドシステムから自動的に送信します。

すべてのチームが、組織の代わりに送信する電子メールの認証要件を（より厳格な DMARC ポリシーを有効にすると認証に適切に合格できなくなる場合には配信可能性の問題についても）認識する必要があります。早い段階で、またこのプロセス全体を通じて何度も、コミュニケーションをとるようにしてください。

参考資料

DMARC の基本概念を理解する場合に参考となる動画を提供しています。Patrick Peterson「DMARC Whiteboard Session」
https://www.brighttalk.com/webcast/10593/104965/dmarc-whiteboard-session-for-engineers

第 4 章

電子メール認証標準

電子メール認証標準には、SPF、DKIM、DMARC などがあります。

SPF : Sender Policy Framework

SPF（Sender Policy Framework、RFC 7208 として IEFT が 2014 年 4 月に公開。https://tools.ietf.org/html/rfc7208 を参照）は、Mail From: 電子メールアドレスでドメインを使用して電子メールを送信することが許可されるサーバーをドメイン所有者が指定できるようにする認証標準です。SPF により、受信者は、DNS へのクエリによって特定のドメインの認可済みサーバのリストを取得できます。認可されたサーバを介して電子メール メッセージが着信する場合、受信者は、その電子メールを正当なものと見なすことができます。

例「SPF : Sender Policy Framework」 上le.net. IN TXT “v=spf1 a mx -all”

SPF の DNS レコードの例

SPF は、電子メールのあらゆる使用例に最適な標準というわけではなく、メッセージが転送される場合には有用でないこともあります。SPF によって認証された Mail From:ドメインを電子メール受信者が容易に確認することはできません。

このフレームワークは、「5321.from」アドレス（「Mail From」、「Envelope From」、または「Return Path」とも呼ばれる）と認証済み送信 IP アドレスを結びつける認証プロセスを定義します。この認可は DNS の TXT レコードで公開されます。

受信者は、SMTP トランザクションの開始時に SPF をチェックし、5321.from ドメインと接続 IP アドレスを比較して、その接続 IP アドレスがそのドメインのメールの送信を認可されているかどうかを判断することができます。

ドメインの SPF レコードを公開することで、その公開レコードに含まれる IP アドレスからのみ電子メールを発信できることをアサートします。

SPF の詳細は次のとおりです。

- SPF レコードのシンタックス
- SPF レコード長
- SPF アライメント

SPF レコードのシンタックス

最も単純な SPF TXT レコードには、バージョン インジケータ、ドメインの許可された IP アドレス、および許可タイプが含まれます。

次に単純な SPF レコードの例を示します。

```
"v=spf1 ip4:198.51.1.137 -all"
```

v=spf1 はバージョンインジケータです。

198.51.1.137 は許可された送信 IP アドレス（IPv4 アドレス）です。

-all は、「198.51.1.137」という IP アドレスだけがそのドメインでメール送信が許可されているとアサートする許可タイプです。

IP アドレスの指定

SPF レコード内の認可済み IP アドレスは、いくつかの方法で定義できます。

ip4:191.51.1.137 や ip6:7939:a348:460d:966f:a986:d0ba:1e9a:c67e などの修飾子を前に付けることによって、1 つの IPv4 アドレスまたは IPv6 アドレスを指定できます。

CIDR 形式で IP アドレスの範囲を指定できます（例：ip4:191.51.1.137/29）。

送信ドメインの A レコードまたは MX レコードでもある任意の IP を指定できます。たとえば、「v=spf1 mx -all」により、送信ドメインの MX でもあるすべての IP が許可されます。

include: コマンドを使用して、他の SPF レコードを含めることができます。たとえば、include:_spf.google.com には Google の SPF レコードが含まれます。

メカニズムと修飾子には、評価時に DNS クエリが発生させるものとさせないものがあります。「include」、「a」、「mx」、「ptr」、および「exists」メカニズムと「redirect」修飾子には DNS クエリが必要です。1 つの SPF レコードでは、DNS の過負荷を回避するために、SPF 評価時のルックアップの総数を 10 に制限する必要があります。

許可タイプ

SPF レコードの最後のシンタックスにより、さまざまなタイプの認可方式を公開することができます。

SPF レコードの許可タイプ

ステートメント	結果	意味
+all	pass	すべてのメールが許可されます。
-all	fail	レコード内のいずれかのパラメータ（たとえば、IPv4、IPv6、MX）と合致するメールだけが許可されます。
~all	softfail	レコード内のパラメータと合致するかどうかにかかわらず、メールが許可されます。
?all	neutral	ポリシーステートメントはありません。

~all と -all の違い

DMARC 標準と SPF 標準が登場する前にも、Softfail（~）許可が使用されていました。そのおかげで、組織は、受信者によって許可の解釈と対処が異なる環境で発信 IP スペースをアサートするという考えに慣れることができました。

実際、DMARC とドメイン保護を導入していれば、データのモニタリングを続けながら、まずは Neutral 許可（「?all」）から始め、その後すばやく Softfail 許可（「~all」）に移行し、最終的に Fail 許可（「-all」）に移行できます。

[SPFの問題(What are my SPF problems?)]レポートを使用すると、ドメインの SPF レコードを変更するときにも、引き続きデータをモニターできます。

SPF レコード長

SPF(Sender Policy Framework)は DNS(ドメインネームシステム)レコードであり、DNS 仕様では DNS レコード文字列を 255 文字に制限しています。ただし、環境によっては複雑すぎて 255 文字に収まらない場合もあります。SPF を定義する仕様には DNS レコードに複数の文字列を含めることができるとも規定されているため、255 文字を超える SPF レコードを作成できます。技術的な詳細については、「RFC 4408」を参照してください。

具体的には次のとおりです。

> [RFC 1035] セクション 3.3.14 および 3.3 で定義されているように、単一のテキスト DNS レコード(TXT タイプまたは SPF RR タイプ)は、複数の文字列で構成できます。複数の文字列が含まれている公開レコードでは、その各文字列がスペースなしで連結されているかのように扱う必要があります。次に例を示します。
>
> IN TXT "v=spf1 .... first" "second string..."
>
> 次のようになっているものとして扱う必要があります。
>
> IN TXT "v=spf1 .... firstsecond string..."

単一の文字列が 255 文字を超えている SPF レコードまたは TXT レコードを作成しようとすると、BIND(DNS ソフトウェア)で「無効な rdata 形式:スペースが足りません」というようなエラーが生成されます。

追加の注意事項

- 512 バイトを超える DNS レスポンスにはわずかに望ましくない部分もあります。EDNS0(最近は全部ではないものの大多数の実装が対応しています)を装備していない場合、512 バイト(UDP パケットの制限)を超えるレスポンスは切り捨てられ、TCP で再試行するように求められるためです。できれば合計 512 バイト以内に収めるのが最適です。
- RDATA 自体は、含まれるすべての文字列のバイト単位の長さとペイロードの両方で構成され、合計で 65535 バイトを超えることはできません。この 64K という制限は、TXT レコードに固有のものではなく、あらゆるタイプの DNS レコードに見られる一般的な制限です。

例

次は、2 つの別個のテキスト文字列からなる単一の SPF レコードの例を示しています。

"v=spf1 ip4:156.77.0.0/16 ip4:63.88.61.0/24 ip4:216.30.177.0/24 ip4:74.86.131.74 ip4:63.76.9.0/24 ip4:63.251.90.0/24 ip4:69.25.31.0/24 ip4:216.74.162.0/24 ip4:216.197.69.0/24 ip4:66.35.231.0/24 ip4:204.3.170.225/32 ip4:64.94.179.244/30 ip4:64.94.179.217 ip4:212.118.254.242/31 ip4:208.86.144.242 ip4:204.90.130.118 ip4:204.90.130.121" " ip4:192.33.34.0/24 ip4:205.211.178.40/30 ip4:149.235.225.40/30 ip4:67.231.144.228 ip4:67.231.152.222 ip4:216.119.217.33 ip4:216.119.209.33 include:thirdparty.net -all"

次は、トラフィックの一部に関する独立したレコードの例を示しています。ドメインに DNS ルックアップがあまりない場合に便利です。

_spf.mydomain.com TXT v=spf1 ip4:156.77.0.0/16 ip4:63.88.61.0/24 ip4:216.30.177.0/24 ip4:74.86.131.74 ip4:63.76.9.0/24 ip4:63.251.90.0/24 ip4:69.25.31.0/24 ip4:216.74.162.0/24 ip4:216.197.69.0/24 ip4:66.35.231.0/24 ip4:204.3.170.225/32 ip4:64.94.179.244/30 ip4:64.94.179.217 -all

mydomain.com TXT v=spf1 ip4:212.118.254.242/31 ip4:208.86.144.242 ip4:204.90.130.118 ip4:204.90.130.121 ip4:192.33.34.0/24 ip4:205.211.178.40/30 ip4:149.235.225.40/30 ip4:67.231.144.228 ip4:67.231.152.222 ip4:216.119.217.33 ip4:216.119.209.33 include:thirdparty.net -all

SPF アライメント

ドメインに代わって送信が許可される IP アドレスのリストを SPF レコードでアサートするだけでなく、送信者と協力して、SPF のアライメントが正しく一致していることを確認する必要があります。

この調整を理解するには、SMTP プロトコルをある程度理解する必要があります。SPF の場合、RFC5321.MailFrom（「MAIL FROM」、「Envelope From」、または「Return Path」とも呼ばれる）のドメイン部分が、電子メール メッセージの本文（またはデータ部分）に表示されている From: アドレス（「Friendly From: アドレス」とも呼ばれる）と合致する場合に、ドメインが調整されていると見なされます。

ほとんどの場合、「Return-Path」ヘッダーが RFC5321.MailFrom ドメインを表示するために使用され、このヘッダーは、通常、ほとんどの電子メール クライアントで表示されません。

SMTP カンバセーションの例を次に示します。

1 S: 220 smtp.example.com ESMTP Postfix

2 C: HELO relay.example.com

3 S: 250 smtp.example.com, I am glad to meet you

4 C: MAIL FROM:<bob@example.com>

5 S: 250 Ok

6 C: RCPT TO:<alice@example.com>

7 S: 250 Ok

8 C: RCPT TO:<theboss@example.com>

9 S: 250 Ok

10 C: DATA

11 S: 354 End data with <CR><LF>.<CR><LF>

12 C: From: "Bob Example" <bob@example.com>

13 C: To: Alice Example <alice@example.com>

14 C: Cc: theboss@example.com

15 C: Date: Tue, 15 January 2008 16:02:43 -0500

16 C: Subject: Test message

17 C:

18 C: Hello Alice.

19 C: This is a test message with 5 header fields and 4 lines in the message body.

20 C: Your friend,

21 C: Bob

22 C: .

23 S: 250 Ok: queued as 12345

24 C: QUIT

25 S: 221 Bye

{サーバーが接続を切断します}

上記の例では、4 行目が RFC5321.MailFrom アドレスで、12 行目が Friendly From アドレス（通常、メール クライアントで表示される）です。この例では、ドメイン部分が SPF の目的に合わせてアライメントされていると見なされます。

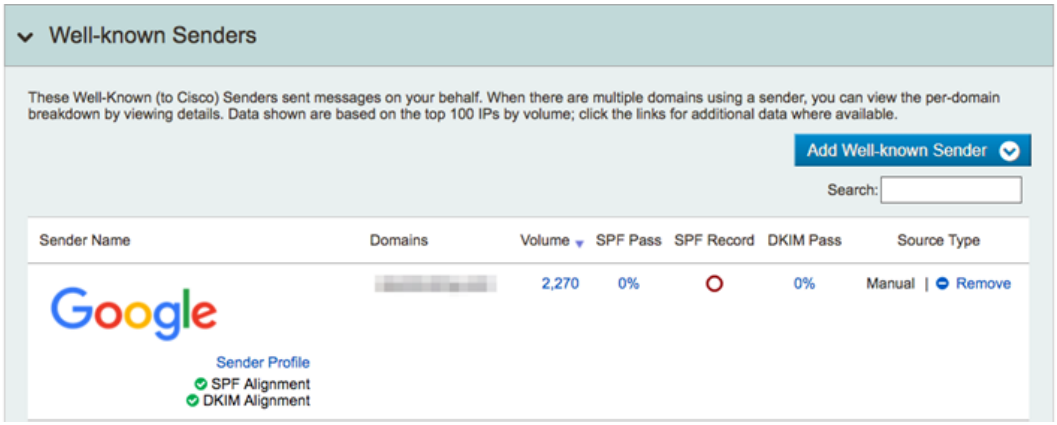
ウェルノウン送信者の SPF の例

この例に図示したシステムは、ここで説明した概念を実証するように設定されています。お使いのシステムとは外観が異なる場合があります。

Google

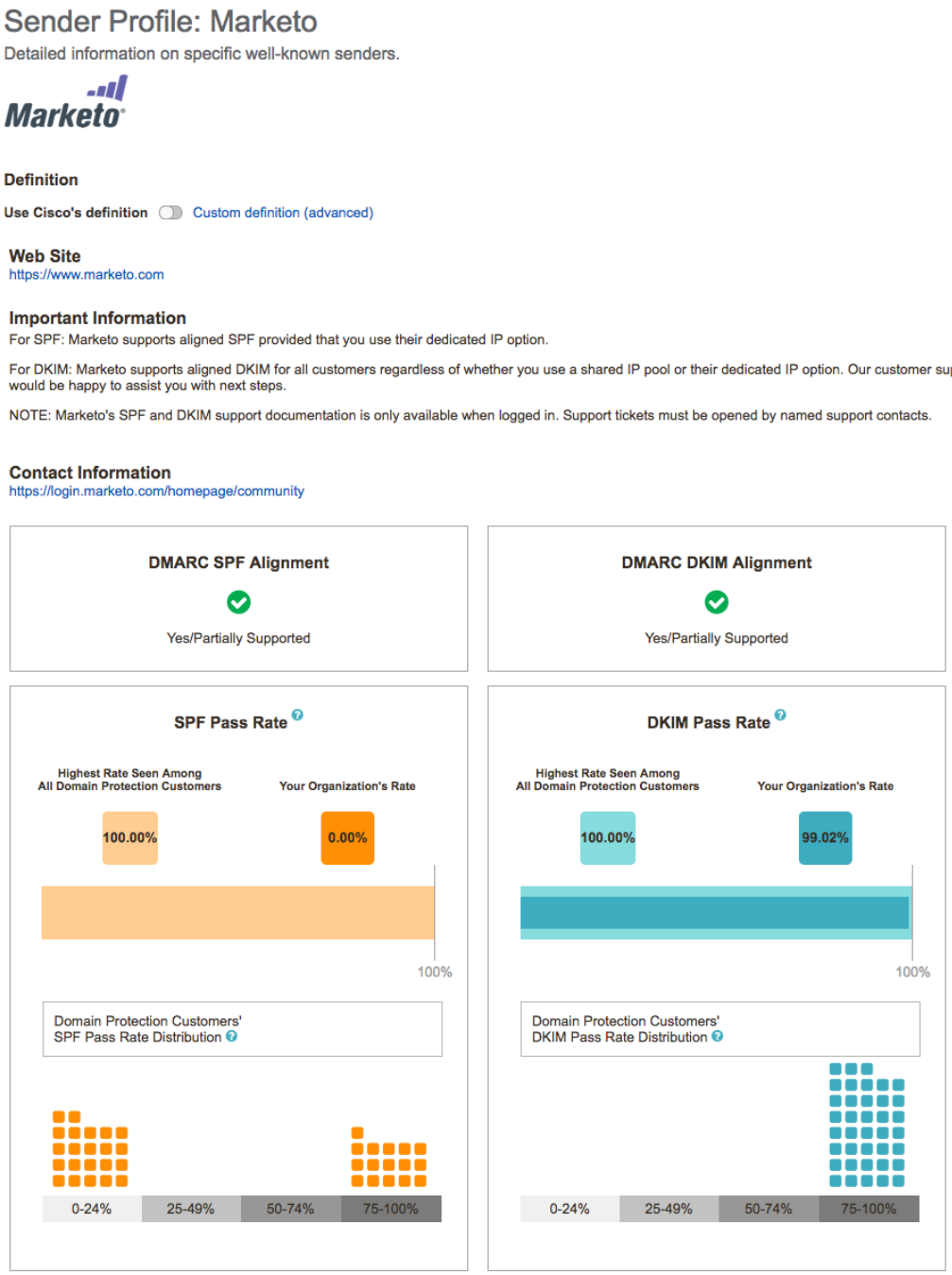
1. [診断（Diagnostics）] > [送信者（Senders）] に移動します。
2. [単一ドメイン（Single Domain）] を選択し、いずれかのドメインを選択して、そのドメインの送信者を表示します。

   Google を電子メール プロバイダーとして使用している場合（G Suite 環境など）は、送信者のリストに Google が含まれています。



   [SPFレコード（SPF Record）] 列は選択したドメインの SPF レコードが見つからなかったことを示していることに注意してください。

3. Marketo の [送信者プロファイル（Sender Profile）] リンクをクリックして、送信者に関する Cisco の情報を表示します。



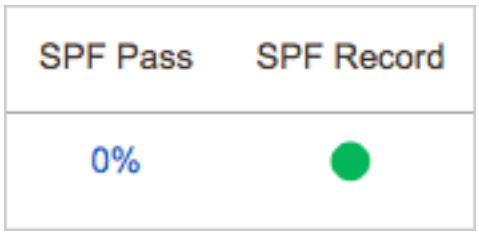
[送信者プロファイル（Sender Profile）] ページの上部にある [重要な情報（Important Information）] セクションには、送信者が SPF アライメントをサポートしているかどうかに関する情報と、サポートしている場合には SPF アライメントを実現するための指示が示されます（SPF の合格率や、Cisco の他の顧客がこの送信者と協力して SPF 認証を成功させたかどうかを確認することも可能です）。

[送信者プロファイル（Sender Profile）] ページのリンクをクリックすると、選択したドメインの SPF レコードに次が追加されていることを確認できます。

```
include:_spf.marketo.com
```

これにより、そのドメインに関して Marketo の IP アドレスが許可されます。

新しい SPF レコードは、有効になるまでに最大 48 時間かかる場合がありますが、通常、それよりも早く有効になります。有効になると、[SPFレコード(SPF Record)] インジケータが変化し、選択したドメインの SPF レコードに送信者が含まれたことが示されます。



[SPF合格(SPF Pass)] 列には、その送信者からのメッセージのうち、ドメインの SPF アライメントに合格したメッセージの割合が表示されます

(G Suite の場合は、SPF の調整を完了するために、G Suite の Postmaster ツールを使用してドメインを追加し、検証する。詳細については、https://support.google.com/mail/answer/6227174 を参照)。

承認済みの送信者を許可する場合は、その送信者をドメインの単一の SPF レコードに追加します。送信者ごとに個別の SPF レコードを作成しないでください。代わりに、SPF レコードを増やしてください(ただし、上記の 10 DNS メカニズム ルックアップに注意)。

カスタム送信者の SPF の例

カスタム送信者を使用すると、Cisco のウェルノウン送信者に含まれない送信者やサーバーを整理できます。組織によっては、オンプレミスに古いメールゲートウェイを設置して、レガシーシステム宛ての発信電子メールを送信している場合があります。ドメイン保護は、他の方法ではウェルノウン送信者に関連付けることができない IP アドレスをデフォルトでは [未割り当て(Unassigned)] カスタム送信者グループに分類します。このグループは、[送信者(Senders)] ページの下半分に表示されます。

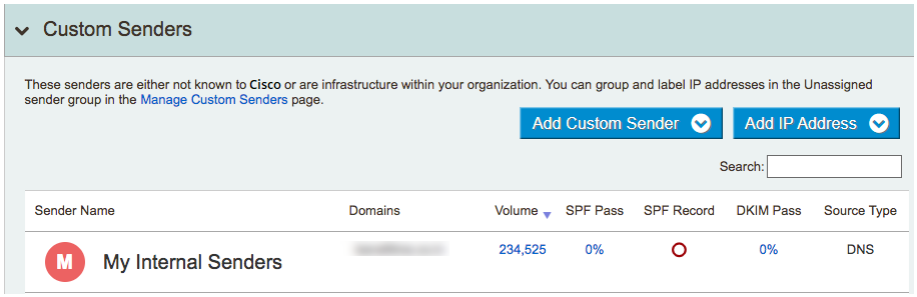
さまざまなビューやレポートでカスタム送信者をフィルタとして使用できます。たとえば、ユーザーがインフラストラクチャ内に所有するサーバーをカスタム送信者として分類できます。

新しいカスタム送信者を作成する方法

1. [設定(Configure)] > [カスタム送信者の管理(Manage Custom Senders)] に移動します。
2. [新しい送信者を追加(Add New Sender)] をクリックします。
3. 新しいカスタム送信者の名前を入力します。
4. Enter キーを押します。

作成したら、[未割り当て(Unassigned)] グループからカスタム送信者に IP アドレス/範囲を追加します。

たとえば、インフラストラクチャの内部 IP アドレスを [内部送信者(My Internal Senders)] という名前のカスタム送信者にグループ化したとします。



「「ウェルノウン送信者の SPF の例」 ページ 36」のウェルノウン送信者の場合と同様に、ページの [カスタム送信者（Custom Senders）] セクションで、このカスタム送信者からの電子メールトラフィックが見られることを確認でき、[SPFレコード（SPF Record）] インジケータには、送信者がまだドメインの SPF レコードに含まれていないことが示されます。

[設定（Configure）] > [カスタム送信者の管理（Manage Custom Senders）] ページに移動すると、そのカスタム送信者に関して定義されている IP アドレスのリストが表示されます。

IP アドレスを SPF レコードに追加するには、その IPv4 アドレスまたは IPv6 アドレスが含まれるように SPF レコードを変更します。次に例を示します。

```
ip4:192.168.1.67
```

（ここでは例として RFC 1918 アドレスを使用）

選択したドメインの SPF レコードが、Google、Zendesk、および「My Internal Senders」カスタム送信者グループの特定の IP アドレスを含むように変更されます。

```
v=spf1 include:_spf.google.com include:mail.zendesk.com ip4:192.168.1.67 ~all
```

CIDR 形式で IP アドレスの範囲を指定できます。

SPF レコードでアドレスを指定するための他のメカニズム（「a」、「mx」、「exists」など）もありますが、これらは高度であり、このドキュメントの範囲を超えています（たとえば、「ptr」メカニズムを SPF RFC 仕様で使用することは推奨されない）。これらのメカニズムの詳細については、https://en.wikipedia.org/wiki/Sender_Policy_Framework#Mechanisms を参照してください。

アライメントの確実な実行

IP アドレスをカスタム送信者からドメインに追加するだけでは、アライメントの実現が保証されません。当該のインフラストラクチャからメールを送信するシステムと連携して、RFC5321.MailFrom（「MAIL FROM」、「Envelope From」、または「Return Path」とも呼ばれる）が、電子メール メッセージの本文（またはデータ部分）に表示されている From: アドレス（「Friendly From: アドレス」とも呼ばれる）と合致することを確認する必要があります。

新しい SPF レコードの構築と提案

新しい SPF レコードを提示するプロセスは、保護する予定のすべてのドメインで同じです。概要レベルでのプロセスは次のとおりです。

1. ドメイン保護の［送信者（Senders）］ページを使用して、特定のドメインの送信者を特定します。
2. その送信者の SPF 指示を確認し、SPF レコードを公開します。
    - ベンダーが SPF をサポートしているかどうかを調べるには、ドメイン保護でウェルノウン送信者の送信者プロファイルを表示します。
    - 制御している IP アドレスを列挙するには、カスタム送信者のデータを使用します。
3. 送信者（ウェルノウン送信者またはカスタム送信者）と協力して、SPF アライメントが完了していることを確認します。
    - ［送信者（Senders）］ページと［分析（Analyze）］>［電子メール トラフィック（Email Traffic）］ページで進捗状況をモニタしてください。
4. 潜在的なすべての送信者を考慮してドメインの SPF レコードを更新/変更します。
    - 「「SPF レコードへの EasySPF™ Analyzer の使用」 ページ 51」を使用することもできます。
5. SPF レコードでドメインのすべての送信者が考慮されていることを確信できる場合は、「-all」ポリシーを使用するように SPF レコードを更新します。

保護するドメインごとに上記の手順を繰り返します。

次に、このプロセスの例をいくつか示します。

- 「ウェルノウン送信者の SPF の例」 ページ 36
- 「カスタム送信者の SPF の例」 ページ 38

参考資料

ここでは、ドメインの SPF 認証を有効にするプロセスを理解するために役立ついくつかの参考資料を示します。

Google G Suite の管理者ヘルプ：「SPF による送信者の認可」

https://support.google.com/a/answer/33786

Microsoft Office 365 のヘルプ：「スプーフィングを防止するために Office 365 で SPF を設定する」

https://technet.microsoft.com/en-us/library/dn789058(v=exchg.150).aspx

SPF の Wikipedia エントリ

https://en.wikipedia.org/wiki/Sender_Policy_Framework

RFC 7208：「Sender Policy Framework」［英語］

https://tools.ietf.org/html/rfc7208

Word to the Wise ブログ：「Authenticating with SPF: -all or ~all」［英語］

https://wordtothewise.com/2014/06/authenticating-spf/

Global Cyber Alliance：「Introduction to the Sender Policy Framework (SPF): A Closer Look」［英語］

https://www.youtube.com/watch?v=oEpU-iqBerI

SPF レコードの公開およびビジネスオーナーの特定

このプロセスのステップ 9 とステップ 10 は反復的な手順です。これらの手順では、多くの場合、組織のビジネスオーナーと協力してドメインの SPF レコードを公開および更新し、ドメイン レコードの包括性を確認します。

同様に、確信が持てるようになったら、SPF レコードを更新します。データのモニタリングを続けながら、まずは Neutral 認証（「?all」）から始め、次に Softfail 認証（「~all」）、そして Fail 認証（「-all」）へと移行します。

送信者が SPF をサポートしていない場合の対処

送信者によっては、専用 IP アドレスからアライメントされた SPF のみをサポートしている場合があります（送信者 Marketo など）。そのホストされたレコードで IP アドレスが認証されているかどうかをテストする場合は、「Ciscoでの SPF レコードのルックアップ」を参照してください。

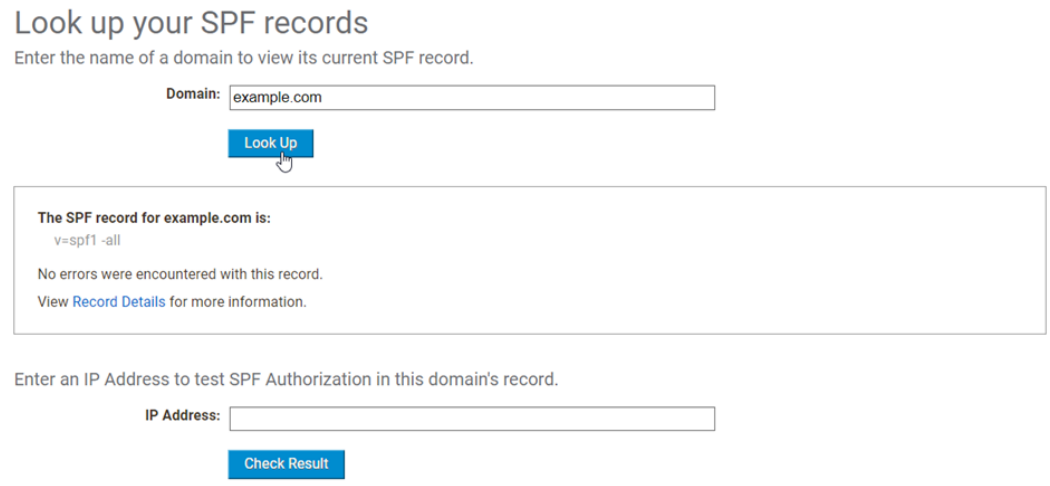
その場合、専用 IP オプションなしで DMARC に合格するには、調整済み DKIM 署名ドメインを使用し、DKIM によってメッセージに署名する必要があります。

SPF チェックと DKIM チェックのいずれかまたは両方に合格する場合、DMARC によって設定されたポリシーにも合致しているときは、DMARC チェックに合格したと見なされ、それ以外の場合は DMARC チェックに合格しなかったと見なされる、と DMARC 仕様で規定されていることに注意してください。

Cisco での SPF レコードのルックアップ

Cisco で SPF レコードをホストすることにした場合は、SPF ルックアップツールを使用して、そのホストされたレコードで IP アドレスが許可されているかどうかをテストできます。このツールは、特定の IP アドレスが Cisco で実際にホストされていることを検証する場合に便利です。

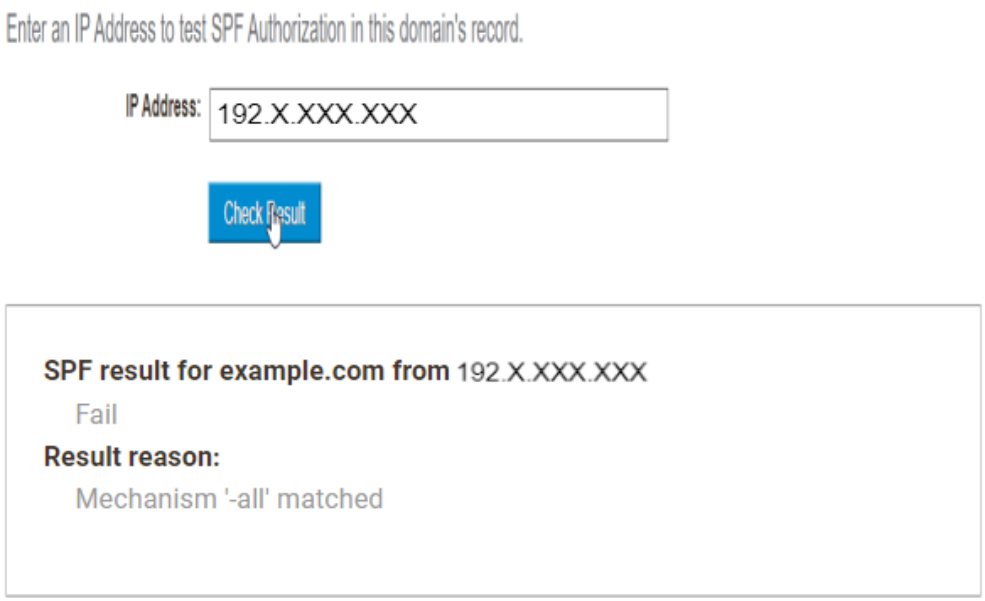
1. [ツール（Tools）] > [SPF] に移動します。
2. [ドメイン（Domain）] に入力します。
3. [ルックアップ（Lookup）] をクリックして、最初のレポートを表示します。



SPF ルックアップレコード

SPF レコードのテスト

1. [IPアドレス(IP Address)] に SPF をテストする IP アドレスを入力します。
2. [結果をチェック(Check Results)] をクリックして、レポートを表示します。



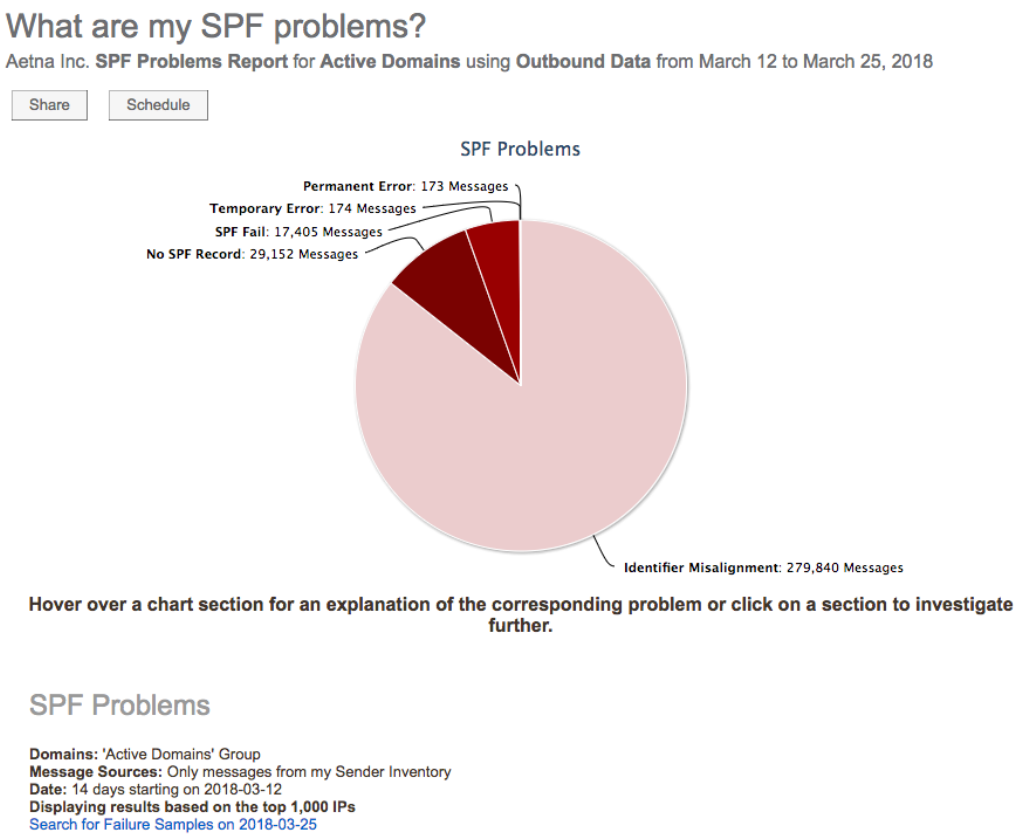
IP アドレスを使用した SPF のテスト

SPF の問題の特定

[SPFの問題(What are my SPF problems?)] レポートを使用すると、多くの場合、認証に関する作業を進め、特定のドメイン内の送信者ごとに包括的な SPF レコードを作成する際に、対処が必要な問題のドメインとカテゴリを特定できます。

[分析(Analyze)] > [電子メールトラフィック(Email Traffic)] に移動します。

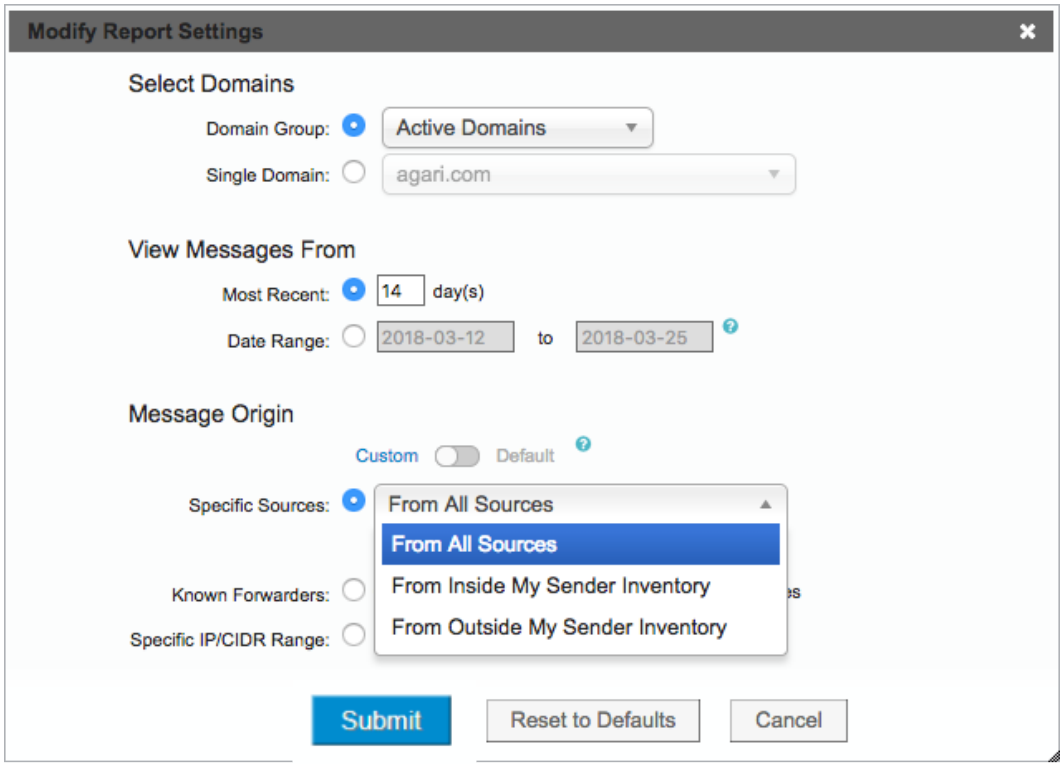
[SPFの問題(What are my SPF problems?)] をクリックして、最初のレポートを表示します。



[SPFの問題（What are my SPF problems?）] レポートの最上位画面。

多くの場合、最大の問題は、識別子の不整合です。

これらのレポートは、対象範囲を絞り込むように設定できることに注意してください（詳細については、「「電子メールトラフィックレポートの設定」 ページ 120」を参照してください）。たとえば次のように、過去 2 週間の単一ドメインのみを対象にした SPF の問題を表示できます。



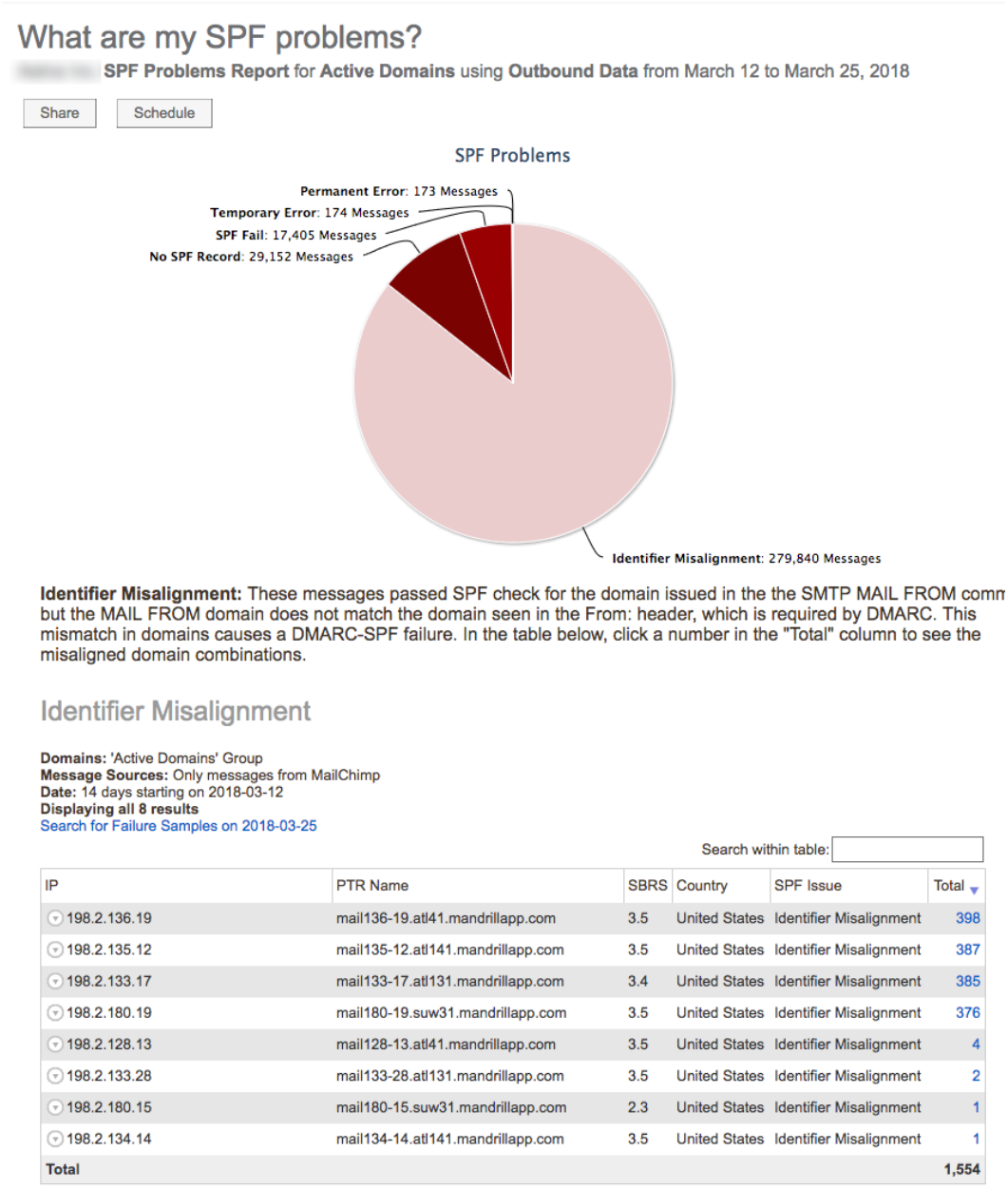
すべての送信元からのメッセージを探すように対象範囲を広げることで、送信者インベントリに含まれない送信者が [診断(Diagnostics)] > [送信者(Senders)] ページの [未承認(Unapproved)] タブに表示されるようになります。

問題を理解するために、このレポートの下部にある送信者のリストを調べてください。たとえば次のように、選択したドメインの送信者 MailChimp から送信されたメールに「識別子アライメント不一致」(Identifier Misalignment)の問題があることに気づく場合があります。

MailChimp	All Issues	1,546
	Identifier Misalignment	1,546

MailChimp での識別子アライメント不一致の問題。

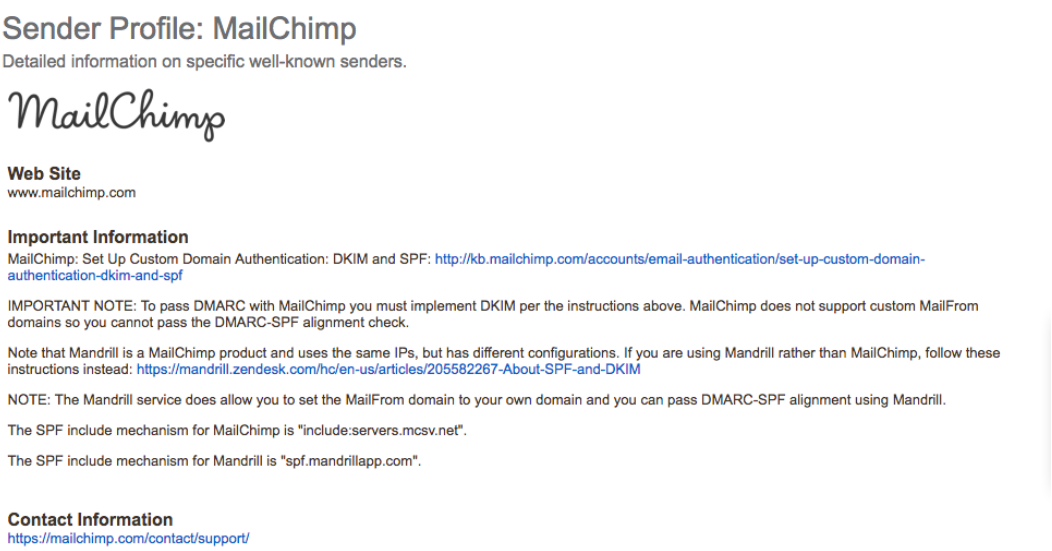
送信者 MailChimp から送信されたメッセージのリンクをクリックして、その送信者の詳細情報を確認します。



MailChimp での不整合の問題：詳細ビュー

このビューは、MailChimp から送信されたメッセージが調整に失敗していることを示しています（ドメインの SPF レコードに送信者 MailChimp の IP アドレスが追加されていると仮定）。

MailChimp の [送信者プロファイル（Sender Profile）] ページには、MailChimp と Mandrill（同じ IP アドレスを使用するが SPF の設定が異なる MailChimp 製品）の両方に関して SPF による認証を有効にすることに関する固有の注意事項が示されます。


Sender Profile: MailChimp

Detailed information on specific well-known senders.

MailChimp

Web Site
www.mailchimp.com

Important Information
MailChimp: Set Up Custom Domain Authentication: DKIM and SPF: http://kb.mailchimp.com/accounts/email-authentication/set-up-custom-domain-authentication-dkim-and-spf

IMPORTANT NOTE: To pass DMARC with MailChimp you must implement DKIM per the instructions above. MailChimp does not support custom MailFrom domains so you cannot pass the DMARC-SPF alignment check.

Note that Mandrill is a MailChimp product and uses the same IPs, but has different configurations. If you are using Mandrill rather than MailChimp, follow these instructions instead: https://mandrill.zendesk.com/hc/en-us/articles/205582267-About-SPF-and-DKIM

NOTE: The Mandrill service does allow you to set the MailFrom domain to your own domain and you can pass DMARC-SPF alignment using Mandrill.

The SPF include mechanism for MailChimp is "include:servers.mcsv.net".

The SPF include mechanism for Mandrill is "spf.mandrillapp.com".

Contact Information
https://mailchimp.com/contact/support/

次の方法で問題のカテゴリを絞り込むことができます。

- ドメインによって
- ウェルノウン送信者によって
- カスタム送信者によって

ドメインごとに、[送信者(Senders)] ページと [SPFの問題(What are my SPF problems?)] レポートビューを使用して、包括的な送信者リストと、各ドメインの SPF レコードにある送信者の対応するエントリを確認できます。

ホストされた SPF

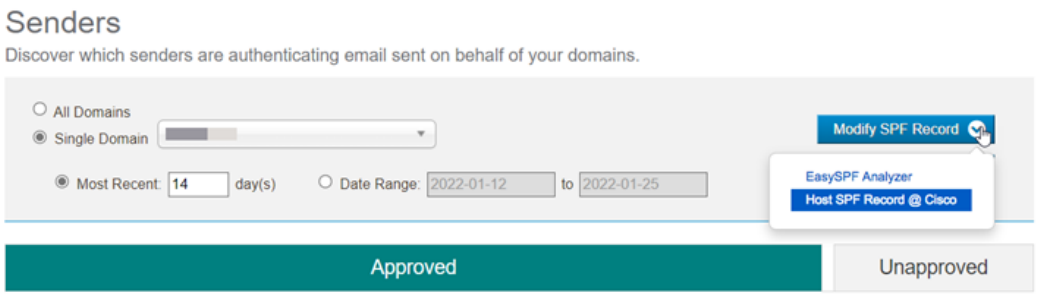
Cisco は、代わりに SPF レコードをホストできます。Cisco で SPF レコードをホストするように選択すると、組織で DNS を手動で変更する必要がなくなるため遅延なく送信者を承認できる一方、SPF レコードを迅速かつ正確に公開することですばやく認証作業を終えることができます。ホストされた SPF を使用する場合、Cisco の電子メール クラウド アイデンティティを活用し、安心して、わずか数回のクリックでドメインの電子メールを認証できます。

次の操作を実行できます。

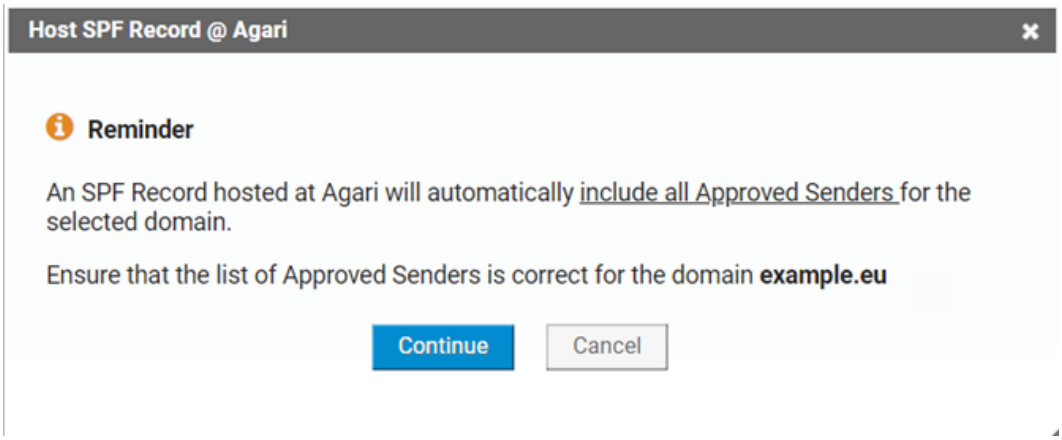
- 「Cisco での SPF レコードのホスティング」 下
- 「Cisco での SPF レコードのホスティングの停止」 ページ 50

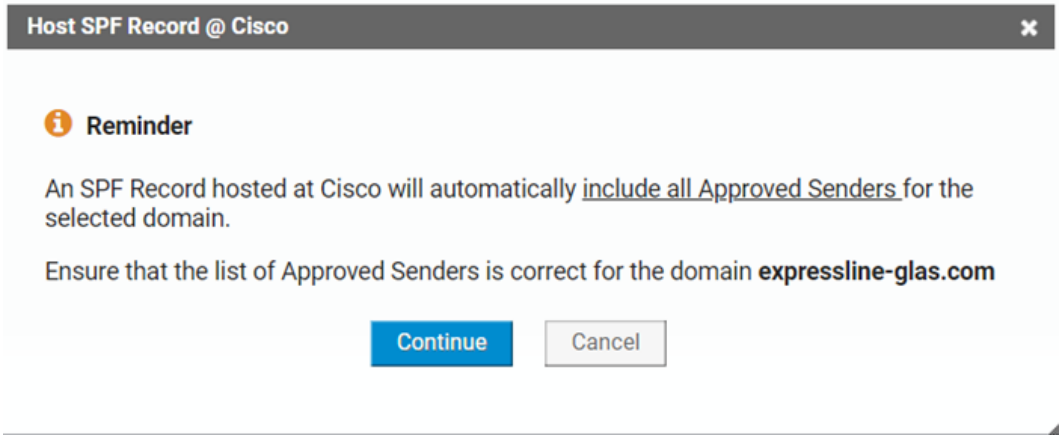
Cisco での SPF レコードのホスティング

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. 1 つのドメインを選択して、そのドメインで承認されている送信者を表示します。ドメインの SPF レコードを Cisco でまだホストしていない場合は、右側のボタンに [SPFレコードの変更(Modify SPF Record)] と表示されます。ドメインの SPF レコードを Cisco ですでにホストしている場合は、右側のボタンに [ホスティングの停止(Stop Hosting)] と表示され、続行できなくなります。
3. [SPFレコードの変更(Modify SPF Record)] > [Cisco でのSPFレコードのホスティング(Host SPF Record @ Cisco)] をクリックします。



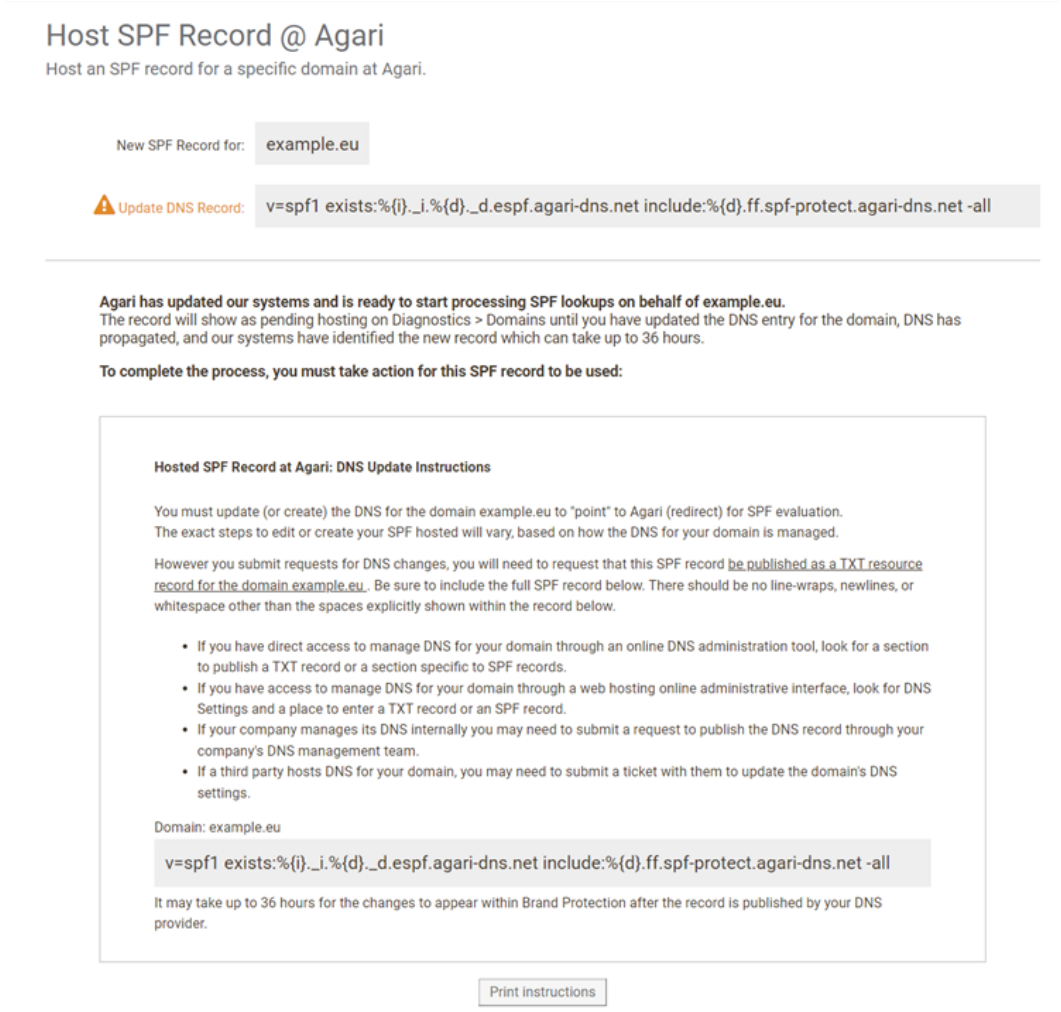
リマインダにより、選択したドメインのすべての承認済み送信者が Cisco に含まれることが通知されます。



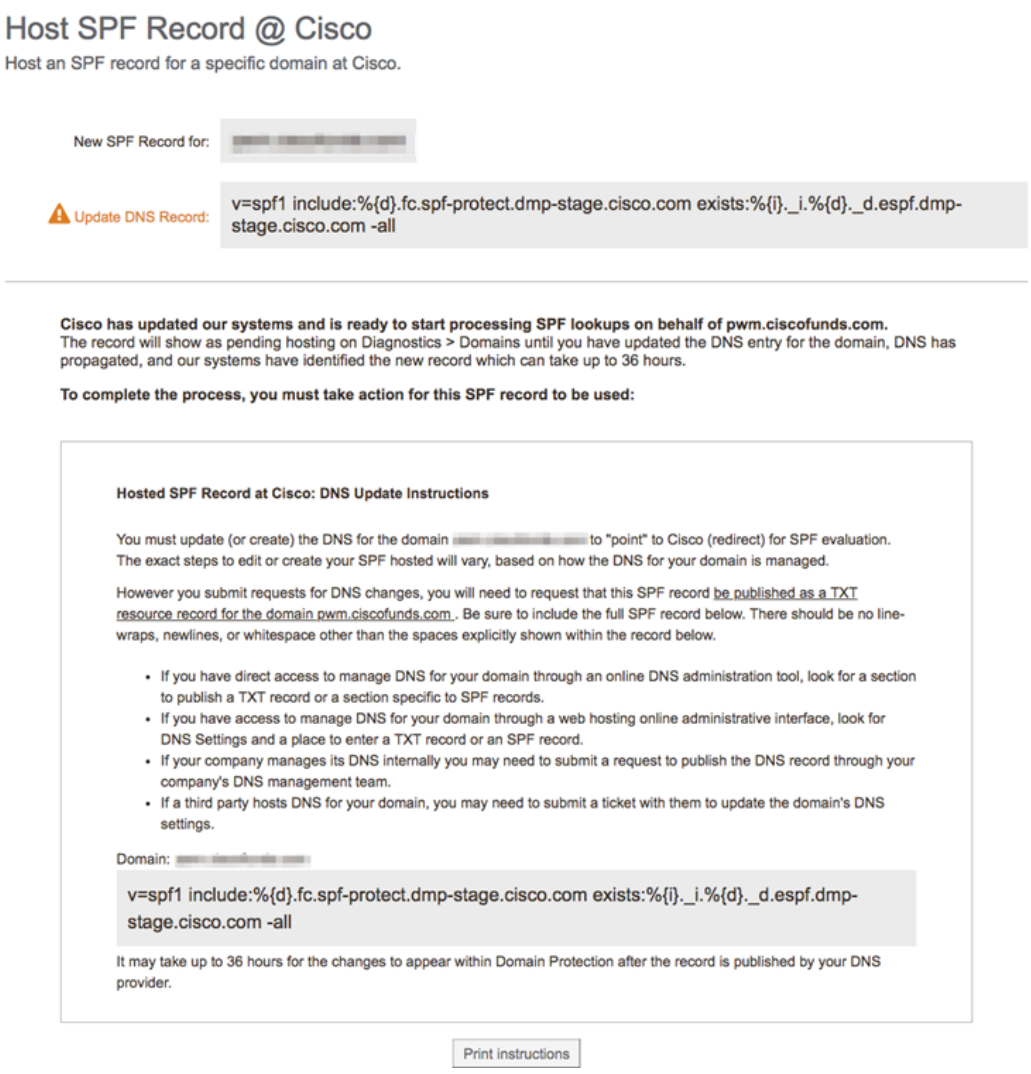


4. [続行(Continue)]をクリックして、ドメインの SPF レコードのホストを開始します。

画面に表示される指示に従って処理を完了します。



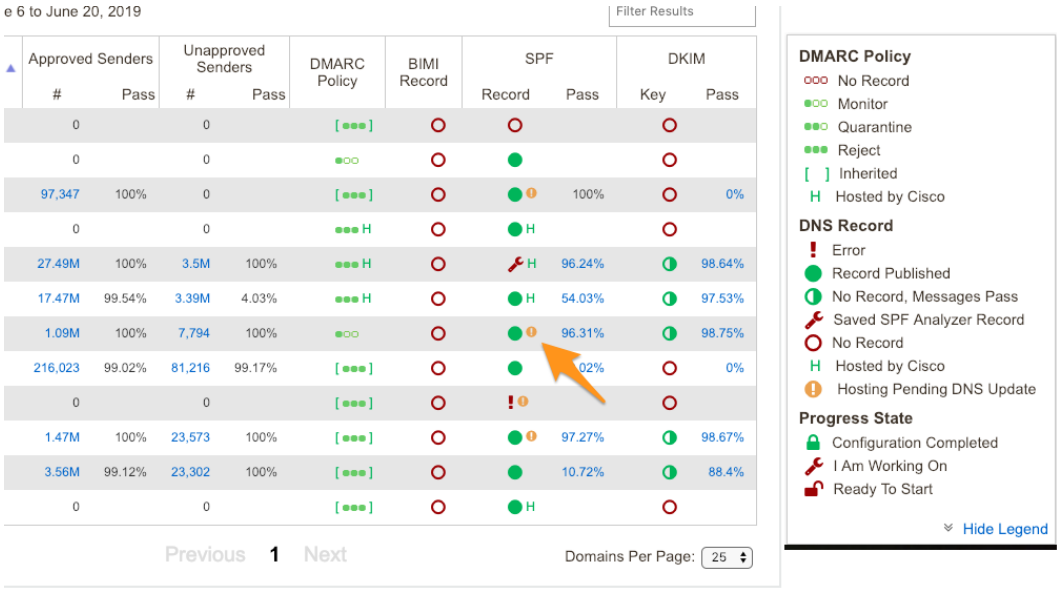
ホストされた SPF の指示。



ホストされた SPF の指示。

SPF レコードを使用するためのアクションを実行する必要があります。SPF 評価のために Cisco を「指す」(リダイレクトされる)ように DNS を更新してください。

Cisco で SPF レコードをホストすることを選択すると、そのステータスが [診断(Diagnostics)] > [ドメイン(Domains)] ページに反映されます。

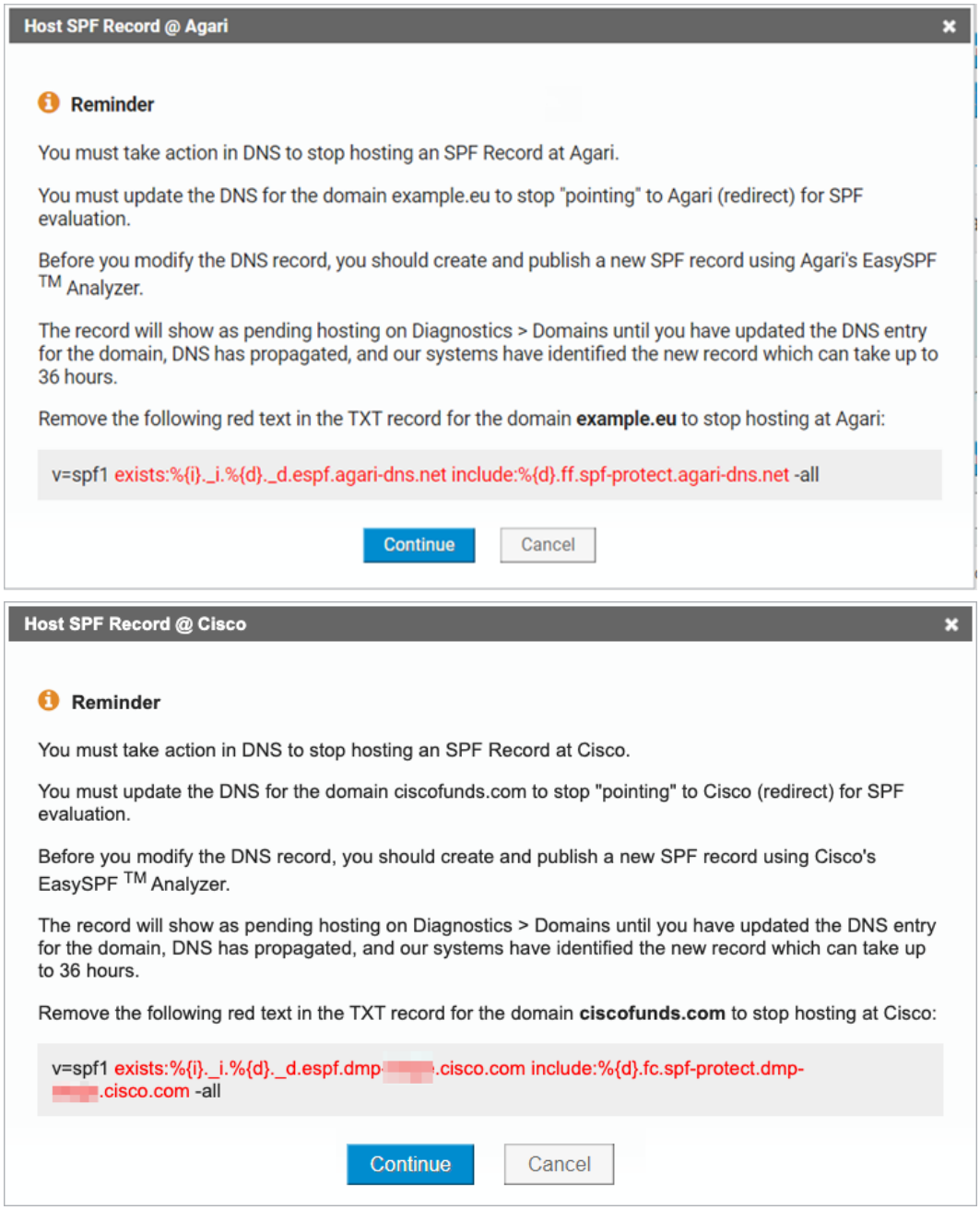


保留中の DNS 更新のホスト。

Cisco での SPF レコードのホスティングの停止

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. 1 つのドメインを選択して、そのドメインで承認されている送信者を表示します。ドメインの SPF レコードを Cisco でホストしている場合は、右側のボタンに [ホスティングの停止(Stop Hosting)] と表示されます。ドメインの SPF レコードを Cisco でまだホストしていない場合は、右側のボタンに [SPFレコードの変更(Modify SPF Record)] と表示され、続行できなくなります。
3. [ホスティングの停止(Stop Hosting)] をクリックします。

ユーザー自身の DNS インフラストラクチャ内で SPF レコードのホストを開始するために必要な手順を通知する警告が表示されます。



Cisco での SPF レコードのホスティングの停止

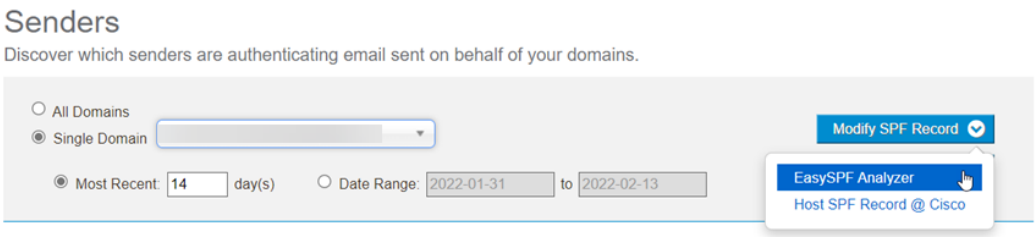
4. [続行(Continue)]をクリックします。

SPF レコードへの EasySPF™ Analyzer の使用

独自の SPF レコードをホストしている場合は、EasySPF™ Analyzer を使用して、既存の SPF レコードを分析したり、承認済み送信者に基づいて新しい SPF レコードを作成したりできます。

EasySPF Analyzer は、Cisco でホストされていないドメインに対してのみ使用できます。

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. 単一のドメインを選択します。
3. [SPFレコードの変更(Modify SPF Record)] > [EasySPF Analyzer] をクリックします。



EasySPF Analyzer では、次の 3 つのステップで SPF レコードを作成または変更できます。

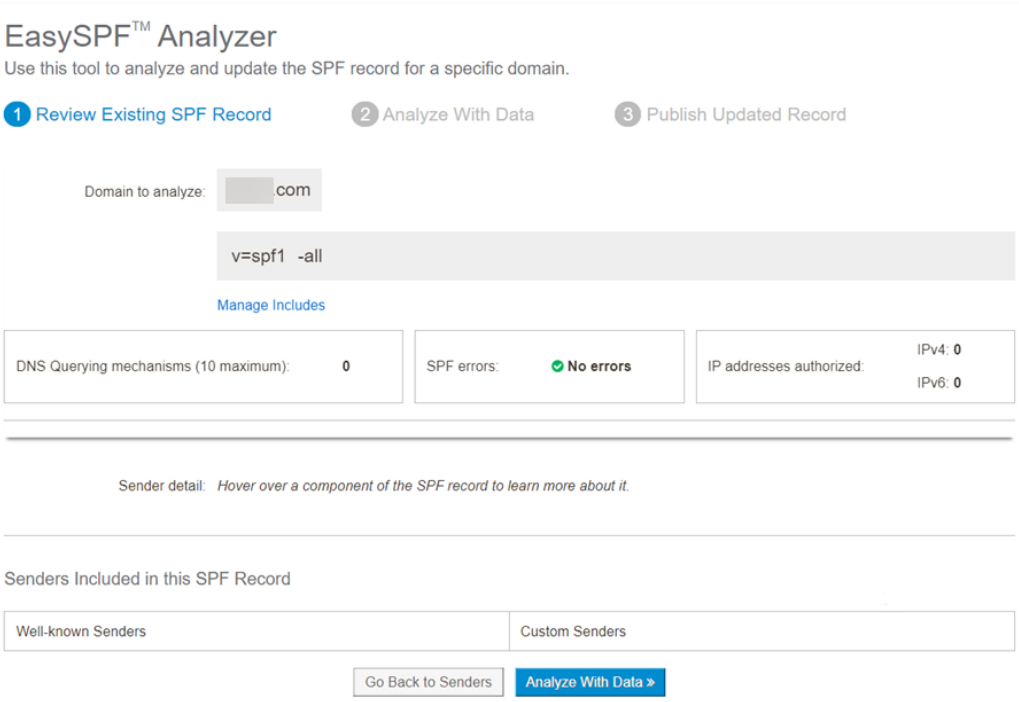
1. 既存の SPF レコードを確認します(ある場合)。
2. 送信者データを分析します。
3. 更新したレコードを公開します。

既存の SPF レコードの確認

EasySPF Analyzer の最初の手順では、既存の SPF レコードを確認します。次の点に注目してください。

- SPF レコード内で識別された送信者。
- 許可された IP アドレスの数。
- DNS クエリメカニズムの数。
- 既存のレコードのシンタックスエラー。

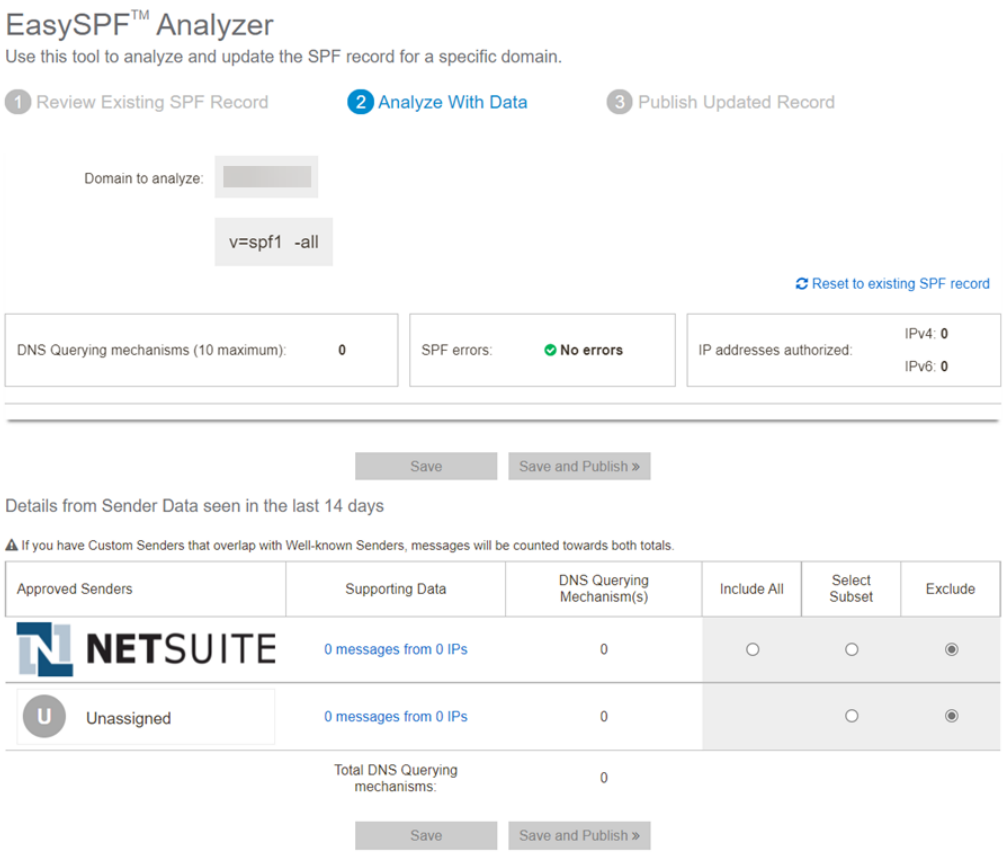
SPF レコードのコンポーネントにマウスのカーソルを合わせると、詳細情報が表示され、メカニズム コンポーネント間の接続や、選択したドメインの承認済み送信者との関係を確認できます。



EasySPF Analyzer：ステップ 1

送信者データの分析

1. ［データによる分析（Analyze with Data）］をクリックし、現在の SPF レコードを変更します。



EasySPF Analyzer：ステップ 2

このビューでは、次の操作を実行できます。

- [支援データ（Supporting Data）] リンクをクリックし、そのドメインに関してその送信者から送信されたメッセージを確認します。

  多くの場合、サードパーティ送信者から専用の IP アドレスを購入しています。ユーザーの SPF レコードでの送信者の定義（この場合）を、より少ない IP アドレスのグループに絞り込むことができます。支援データビューで、その送信者からのメッセージの送信に使用された IP アドレスの数を確認できます（さらに詳細な情報を確認することも可能）。

  ドメインのウェルノウン送信者およびカスタム送信者ごとに、[支援データ（Supporting Data）] リンクによって次の情報が表示されます。

  - IP アドレス：メッセージの発信元 IP アドレス
  - 送信者のインクルード メカニズムによって参照されている IP アドレス
  - PTR 名（ポインタ レコード）：IP アドレスのホスト名
  - 送信者ベースのレピュテーション スコア（SBRS）
  - 国：IP アドレスの地理的な場所
  - SPF 合格率（%）
  - DMARC 合格率（%）

- DMARC 合格量
- 電子メールの総量

- [含める(Include)]、[サブセットを含める(Include Subset)]、または [含めない(Exclude)] をクリックして、ドメインの SPF レコードに含まれている各送信者の定義を変更します。

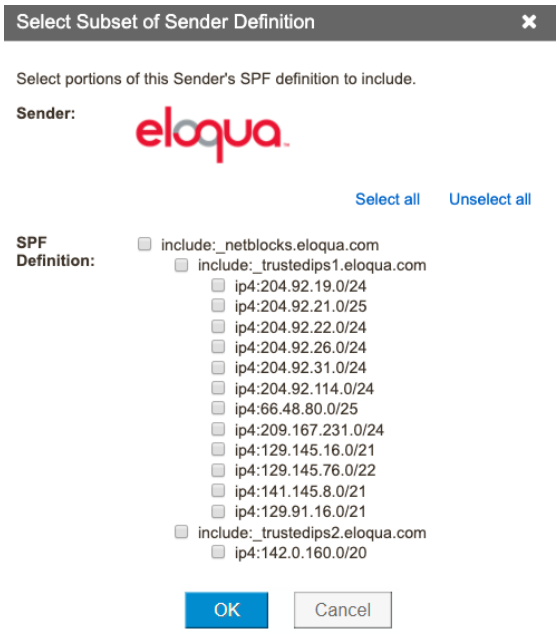
  変更を加えると、ページの上部に表示されている変更された SPF レコードの追加と削除が更新されます。

  SPF レコードの変更。

インクルード メカニズムから明示的な IP アドレスまたは範囲に変更すると、DNS クエリ メカニズムが更新されます。

いつでも既存の SPF レコード(現在 DNS にあるもの)にリセットして、加えた変更を削除できます。

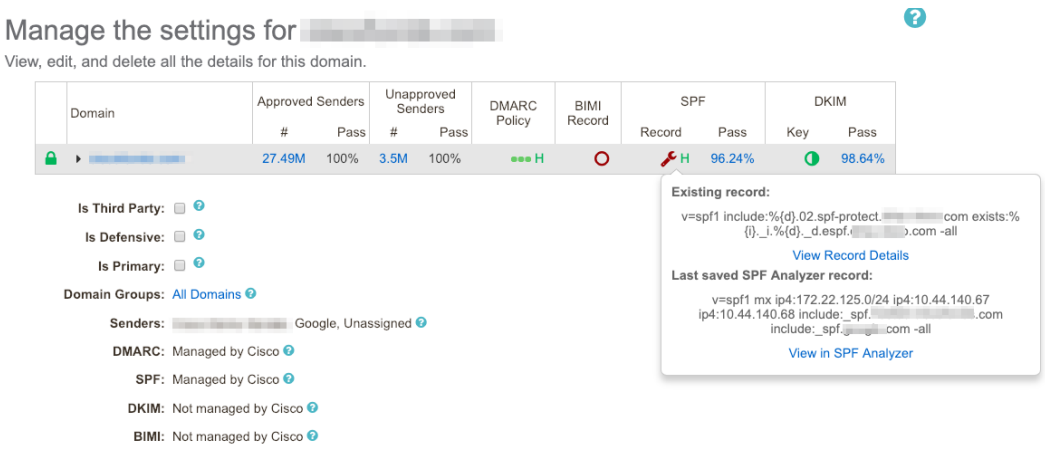
ウェルノウン送信者定義の特定のサブセットを編集すると、インクルード ステートメントが一連の IP アドレスに「フラット化」されます。



  ウェルノウン送信者定義のサブセットの選択。

2. 次をクリックします
   - [保存(Save)] をクリックしてステップ 2 に進み、SPF レコードの変更を続行します。
   - [保存して公開(Save And Publish)] をクリックして、ステップ 3 の「更新したレコードの公開」に進みます。

作業中の変更されたレコードを保存する場合は、[分析(Analyze)] > [ドメイン(Domains)] > [ドメインの詳細(Domain Detail)] ページのリンクをクリックすると、変更されたビューに戻ることができます。

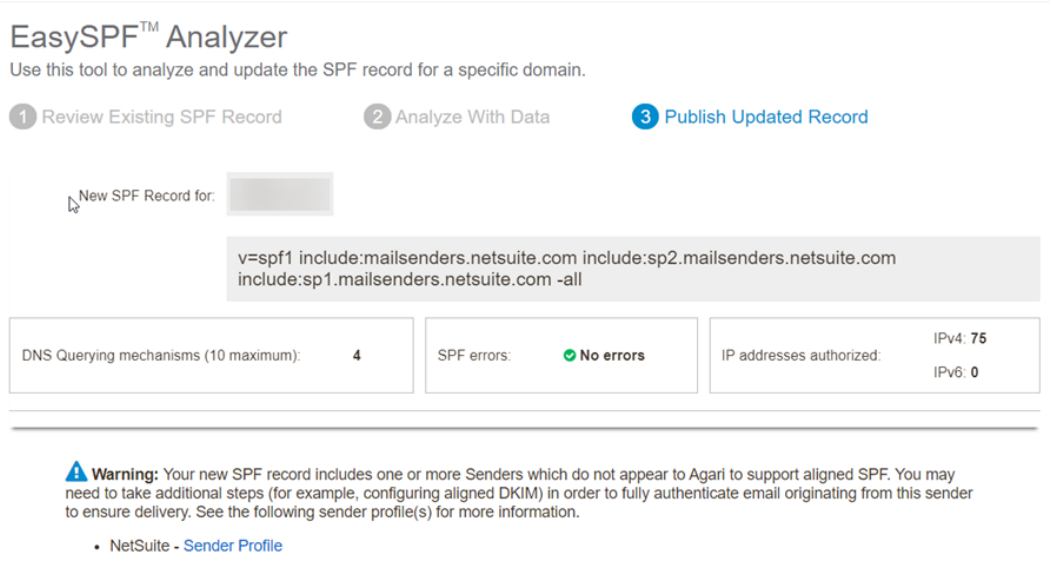


ドメインの保存済みの EasySPF Analyzer レコード。

更新したレコードの公開

[公開(Publish)] ボタンをクリックすると、EasySPF Analyzer のステップ 3 に進み、変更された SPF レコードが表示されます。

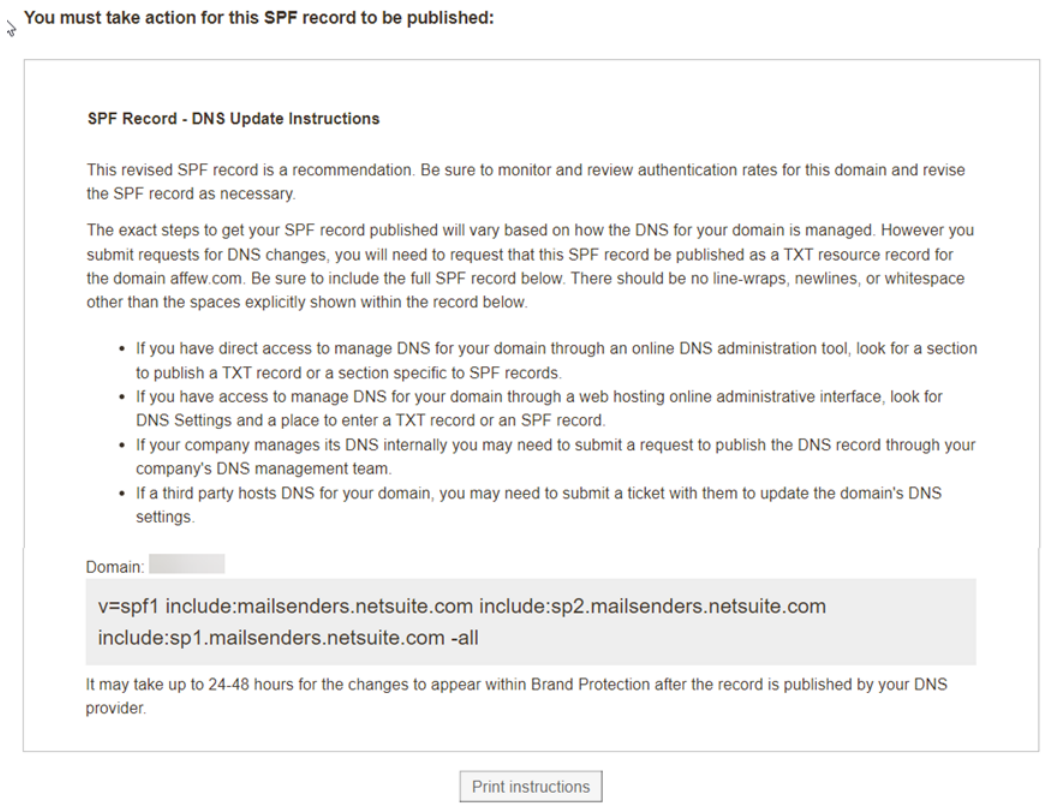
アライメントされた SPF 電子メールを送信しないと Cisco が認識している送信者のメカニズムを含めた場合は、「アライメントされていない送信者に関する警告」を確認する必要がある場合があります。その場合は、その送信者の [送信者プロファイル(Sender Profile)] ページにアクセスし、その送信者からのメッセージを完全に認証するために追加のアクションが必要かどうかを判断してください。



EasySPF Analyzer:ステップ 3(上部)

ページの下部には、新しい SPF レコードと、DNS で SPF レコードを作成するための指示が含まれます。

指示の印刷に適したバージョンを作成するには、[指示の印刷(Print Instructions)] をクリックします。



EasySPF Analyzer：ステップ 3（下部）

DKIM：DomainKeys Identified Mail

DKIM（Domain Keys Identified Mail、2018 年 1 月に RFC 8301 として公開）は、ドメイン名と電子メールメッセージを暗号によって関連付ける認証標準です。送信者は、電子メール メッセージに暗号署名を挿入します。受信者は、これを、DNS によってホストされる公開キーを使用して検証することができます。検証に成功した場合、DKIM は（SPF とは異なり）、転送に耐えられる優れた信頼性を持つドメイン レベルの識別子を提供します。

```
selector._domainkey.example. net IN TXT “v=DKIM1; k=rsa; p=public key data”
```

DKIM の DNS レコードの例

短所：DKIM は、送信メッセージごとに暗号署名を必要とし、一般に SPF よりもセットアップ作業が複雑になります。DKIM は、メーリングリストを通じて送信されるメッセージのように、内容が転送中に変更される場合には役に立ちません。

DKIM の実装

「「トラフィックのモニタリング」 ページ 86」で説明されているモニタリングツールは、この章での作業に必要な情報を直接提供します。つまり、そのモニタリングの結果を使用して、ドメインのサードパーティ送信者を特定し、それらの送信者の認証方式（SPF 認証と DKIM 認証のいずれかまたは両方）を有効にします。

ドメイン保護では、メール フローに関する情報を DKIM の有効化に役立てることができます。

DomainKeys Identified Mail（DKIM）

DomainKeys Identified Mail（DKIM）は、RFC 6376 として公開されています（https://tools.ietf.org/html/rfc6376 [英語] を参照）。

DKIM は、電子メールを送信してデジタル署名を行うユーザーのための標準化された方法を定義します。これにより、受信者は実際の電子メールの送信者が誰であるのか、および送信中にメッセージが改ざんされなかったかどうかを高い確度で確認できます。DKIM は、各ドメインからのすべての送信メールにデジタル署名を付ける方法を電子メールの送信者に提供することで SPF を補完します。DKIM は、世界中の主要な電子メール ボックス プロバイダーによってサポートされており、DMARC に組み込まれた 2 つの基本的な認証方式の 1 つとなっています。

DomainKeys Identified Mail（DKIM）により、署名ドメインを持つユーザー、役割、または組織はドメインとメッセージを関連付けることでメッセージに対する責任を主張できます。DKIM は、メッセージの署名者のアイデンティティに関する問題をメッセージの作成者とされるユーザーから切り離します。責任の主張は、暗号署名を使用し、（DNS で）直接署名者のドメインをクエリして適切な公開キーを取得することで検証されます。

概要：DKIM には暗号化が含まれる

DKIM を使用してメッセージに署名を付けるときは、公開キーと秘密キーのペアを作成します。

キー ペアを作成したら、DNS で公開キーを公開し、秘密キーを使用してメッセージのハッシュ（「署名」）部分を作成します。

受信者は、DKIM 署名付きメッセージを受信すると各自の署名を送信者の秘密キーと照合します。一致があると、そのメッセージは DKIM 署名に合格したと見なされます。

DMARC では DKIM 識別子アライメントが必要

DMARC 仕様は、DKIM 合格の概念を広げます。

DMARC-DKIM に合格するためのメッセージの条件は、次のとおりです。

- メッセージに有効な DKIM 署名が付いていること

  かつ

- メッセージの署名済みの内容が変更されていないこと

  かつ

- DKIM 署名ドメインが DMARC で要求された送信元ドメインと一致していること

識別子のアライメント不一致は、メッセージが DKIM 署名ドメインの DKIM チェックに合格したものの、DKIM 署名ドメインが DMARC で要求された送信元ドメインと一致していない状態であると定義されています。このようなドメインの不一致は、DMARC-DKIM の失敗の原因になります。

識別子アライメントについて

DMARC では、メッセージが DKIM または SPF 検証に合格するだけでなく、その識別子ドメインが「アライメント一致」である必要があります。識別子アライメントでは、SPF によって認証されたドメイン（通常は MailFrom ドメインですが、MailFrom が空であった場合には HELO ドメインにすることもできます）と、DKIM によって認証されたドメイン（DKIM-Signature ヘッダーの d= フィールドに示されている DKIM 署名ドメイン）を「ヘッダー From」ドメ

インに関係付けることができます。電子メールクライアントのユーザーは、このドメインの方をよく目にします。「strict」アライメントモードでは、ドメインが完全に一致する必要があります。「relaxed」アライメントモードでは、ドメインを同じ組織ドメインの異なるサブドメインにすることができます。

SPF の場合、メッセージは SPF チェックに合格する必要があり、From: ヘッダーのドメインは SPF の検証に使用されるドメインに一致する必要があります（strict アライメントの場合は正確に一致する必要があり、relaxed アライメントの場合（デフォルト）はサブドメインにすることができます）。「「SPF アライメント」 ページ 35」も参照してください。

DKIM の場合、メッセージは DKIM チェックに合格する必要があり、有効な署名の d=ドメインは From: ヘッダーのドメインに一致する必要があります（strict アライメントの場合は正確に一致する必要があり、relaxed アライメントの場合はサブドメインにする必要があります）。

SPF と DKIM が認証に合格した場合でも、識別子がアライメント一致でないと、DMARC は失敗します。

識別子アライメントで使用される用語は次のとおりです。

- ヘッダー From ドメイン：メールアドレスのドメイン部分で、電子メールクライアントに表示される「From:」フィールドでエンドユーザーが最もよく目にするものです。同じ「From:」フィールドには表示名もよく表示されますが、それとは異なります。たとえば、電子メールクライアントに「From: Cisco <donotreply@blah.cisco.com>」と表示されることがあります。この例では、「Cisco」は表示名、「cisco.com」は組織ドメインであり、「blah.cisco.com」は From ヘッダーの実際のドメインです。
- SPF ドメイン：この識別子は、SPF 認証メカニズムによって使用されます。通常、これは SMTP カンバセーションの mail-from に使用されるドメインです。ただし、mail-from が空の場合（バウンスや OOO 通知などのシナリオと同様）、受信者は通常、メッセージ送信の HELO/EHLO に指定されたホストで SPF に合格するかどうかをチェックします。
- DKIM ドメイン：この識別子は、DKIM 認証メカニズムによって使用されます。DKIM-Signature ヘッダーの「d=」タグに指定されたドメインです。
- DKIM 公開キー：メッセージ内の DKIM 署名を復号するために使用される鍵です。この「d=」ドメインと、同じく DKIM-Signature ヘッダーにある DKIM セレクタ（「s=」）とを組み合わせて、DNS ルックアップを実行すると見つかります。公開キーは、厳密に言うと、DNS の {s}._domainkey.{d} という TXT ロケーションにあります。s と d は、電子メールメッセージの DKIM-Signature ヘッダーにあります。

DKIM の参考資料

ここでは、ドメインの DKIM 署名を有効にするプロセスを理解するのに役立ついくつかの参考資料を示します。

Google G Suite Administrator Help、「About DKIM」

https://support.google.com/a/answer/174124?hl=en [英語]

Microsoft Office365 ヘルプ、「DKIM を使用して、Office 365 のカスタムドメインから送信される送信電子メールを検証する」

https://technet.microsoft.com/en-us/library/mt695945

OpenDKIM：

http://opendkim.org/ [英語]

DKIM の Wikipedia エントリ：

https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail [英語]

RFC 6376、「DomainKeys Identified Mail (DKIM) Signatures」

https://tools.ietf.org/html/rfc6376 [英語]

Word to Wise ブログ、「A DKIM primer resurrected」

https://wordtothewise.com/2016/04/a-dkim-primer-resurrected/ [英語]

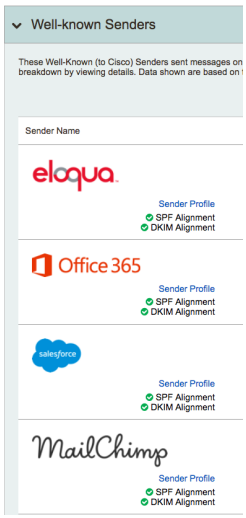
サードパーティオーナーへの DKIM 署名のリクエスト

特定のドメインに使用する各サードパーティ送信者の DKIM を有効にするには、次のプロセスを繰り返す必要があります。

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. 個々のドメインを選択します。

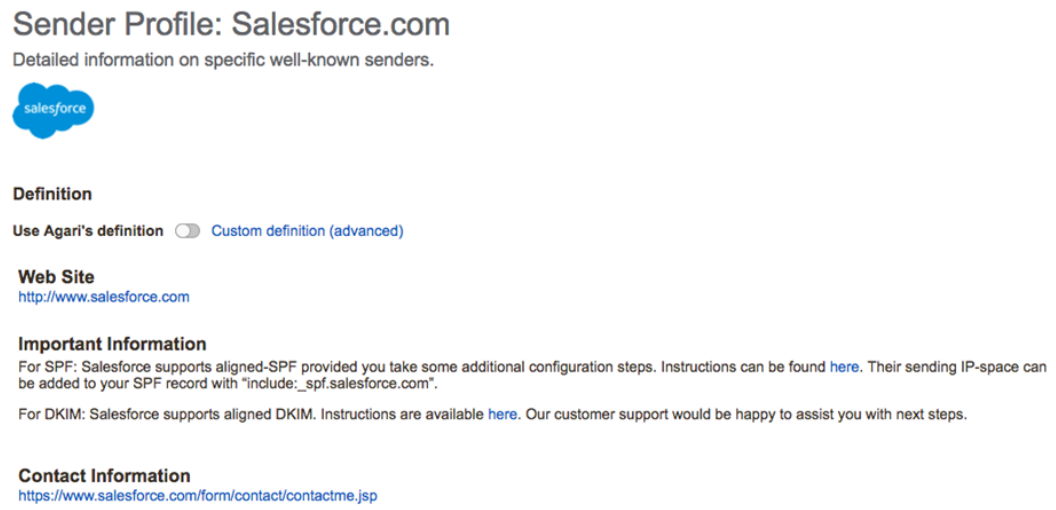
   承認済みのウェルノウン送信者が、ページの上部にリストされます。

   この例では、Salesforce がいずれかのドメインに対して承認されたウェルノウン送信者であると想定しています。



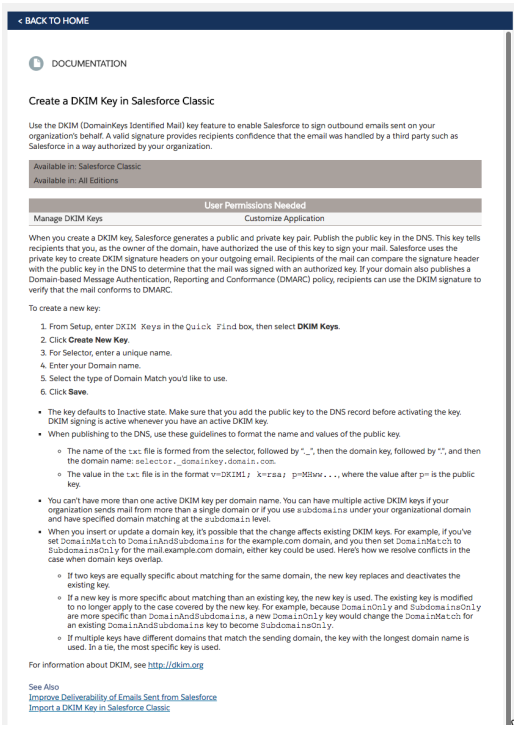
送信者 Salesforce とその送信者プロファイルのリンク

3. Salesforce の [送信者プロファイル(Sender Profile)] リンクをクリックして、Salesforce の DKIM 機能について学習します。



Salesforce の送信者プロファイルの詳細

4. DKIM 指示のリンクをクリックします。ユーザーのドメインに代わって Salesforce が送信するメッセージの DKIM 署名を有効化する手順のページ（https://help.salesforce.com/articleView?id=emailadmin_create_dkim_key.htm）にリダイレクトされます。



Salesforce DKIM ドキュメント

すべてのサードパーティ送信者用の DKIM キーの実装

（「「サードパーティオーナーへの DKIM 署名のリクエスト」（前のページ）」の Salesforce の例に示されているような）各送信者のドキュメントを読むと、そのプロセスにはよく次の手順が含まれています。

- キー ペアの生成
- ドメインのセレクタの選択
- DNS での公開キーの公開

DKIM キーの仕様では、次のように定義されています。

- TXT ファイルの名前はセレクタから作成され、その名前の後には「._」、ドメイン キー、「.」、ドメイン名が続きます。例：selector._domainkey.domain.com。
- TXT ファイルの値は、v=DKIM1; k=rsa; p=MHww... の形式になります。p= の後の値は、公開キーの内容です。

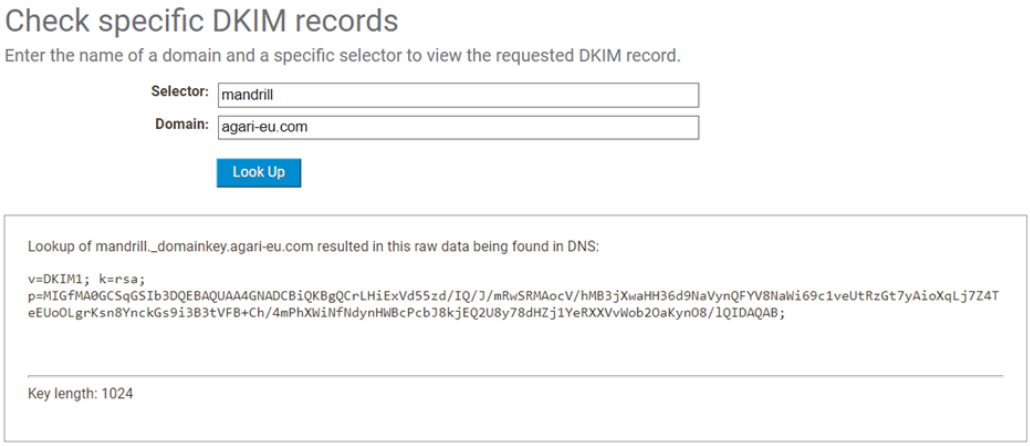
これで、選択したドメインで承認を取得している次の既知の送信者に対する手順を進めることができます。承認を取得している次の既知の送信者に対して上記の手順を繰り返し、状況に応じて DNS TXT レコードを更新します。

多くのサードパーティ送信者は、デフォルトで DKIM 署名を有効にしています。たとえば、Microsoft Office 365 と Google G Suite では、送信メッセージの DKIM 署名が自動的に有効になります。

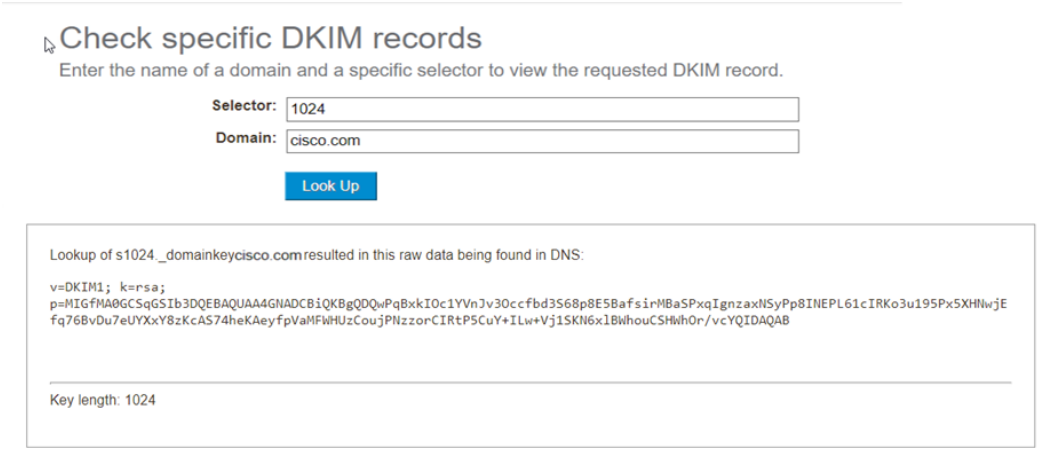
すべてのサードパーティ送信者の DKIM の検証

Cisco Domain Protection（または MX ツールボックス（https://mxtoolbox.com/dkim.aspx [英語]）などの公開されているツール）により、DNS で DKIM レコードが正しく公開されていることを確認できます。

1. [ツール（Tools）] > [DKIM] に移動します。
2. ドメイン名とセレクタを入力します。次に例を示します。



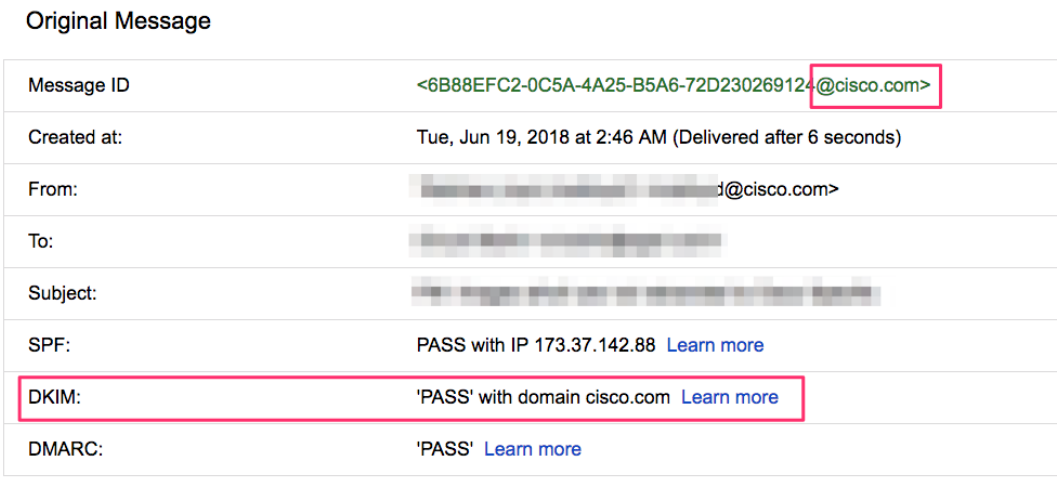
DKIM レコードの確認



DKIM レコードの確認

受信メッセージのヘッダーを調べることにより、サードパーティが正しく署名を付けていることを確認できます。たとえば、Gmail クライアントの場合、メッセージの [メッセージのソースを表示（Show Original）] を選択すると、SPF、DKIM、および DMARC の認証結果が表示されます。

この例のメッセージは、Salesforce.com の送信インフラストラクチャから送信されたものです。なお、Gmail クライアントでは DKIM 合格の認証結果が表示されます。



メッセージのヘッダーを調べると、Salesforce が適切な DKIM ヘッダーを挿入したことがわかります。

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
  d=cisco.com; i=@cisco.com; l=5289592; q=dns/txt;
  s=iport; t=1529401619; x=1530611219;
  h=from:to:subject:date:message-id:references:in-reply-to:
   mime-version;
  bh=wwnGqrNevIbPG97FceJsWcspPFmLJJludpJAODKqgzM=;
  b=Cr5VTd6UKKVC8ixQr4G/FwA3gOWTezZNM8YYUpDf/06uxRm1lepYH9XF
   exxCsMcmhtauyH7CUXFfl2csTgWOnutzrhWhIU3p01U2fX821e8VXH1eI
   bDnRiQb9C+gaVVgv27MRcpmaJZCnxOaBjJUC/Ubs5Go+vZE+tfADyXX/0
   o=;
```

d=cisco.com：ドメインは cisco.com です。

s=iport sfdc：セレクタは「iport**sfdc**」です。

h=... – ハッシュの決定に使用したヘッダー

bh=... メッセージの本文のハッシュ

b=... – メッセージの内容に含まれる実際のデジタル署名

送信エージェントがスタンプを付けた DKIM ヘッダーの内容と構造の詳細については、https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail#Technical_details [英語] を参照してください。

ゲートウェイでの DKIM の有効化

特定のドメインに使用する各 E メール ゲートウェイの DKIM を有効にするには、以下のプロセスを繰り返す必要があります。

多くの場合、[診断（Diagnostics）] > [送信者（Senders）] ページでは各自のインフラストラクチャの E メール ゲートウェイがカスタム送信者として表示されます。

送信メールを送信する E メール ゲートウェイをホストしている場合は、次の 4 つの手順で DKIM を実装する必要があります。

ステップ 1：ドメインを決定する

E メール ゲートウェイから送信メールを送信できるすべてのドメインを決定します。[診断（Diagnostics）] > [ドメイン（Domains）] ページ（とカスタム ドメイン グループ）が包括的なドメイン セットの特定に役立つ場合があります。

ステップ 2：キーペアを作成する

次に、ツールを使用して DKIM の公開キーと秘密キーのペア、およびポリシーレコードを作成します。公開キーは、DKIM ポリシーレコードとともに公開する DNS レコードに含めるキーです。

秘密キーは、電子メールゲートウェイ（MTA/電子メール送信システム）にインストールされる長いキーです。送信メールを送信すると、送信 E メール ゲートウェイによって DKIM 署名が追加されます。

キー ペアを作成するときは、いくつかのオンライン ツールが役に立ちます。キー ペアの作成に使用できるオンライン ツールには、次のようなものがあります。

https://port25.com/dkim-wizard/ [英語]

http://dkimcore.org/tools/keys.html [英語]

https://www.dnswatch.info/dkim/create-dns-record [英語]

「DKIM キー ジェネレータ」または「DKIM キー ウィザード」を検索すると、さらに結果が表示されます。

ステップ 3：DKIM 情報を含む DNS レコードを公開する

電子メールの送信に使用するすべてのドメインの DKIM 情報を含む DNS テキスト レコードを作成します。これらのレコードは、公開される各送信ドメインの DNS レコードに挿入されます。ドメインごとに新しいレコードを作成することに注意してください。

Cisco はドメインの DKIM レコードをホストできます。そのためには引き続きドメインにネームサーバー（NS）レコードを追加する必要がありますが、DKIM レコード自体は Cisco がホストしているため、ドメイン保護で加えた変更は自動的に公開され、今後自分で DNS レコードを操作する必要はありません。

ステップ 4：ゲートウェイで DKIM 署名を有効にする

DKIM 署名を有効にする手順は、ゲートウェイによって異なります。以下に一般的なゲートウェイモデルのドキュメントのリンクを示します。

- IronPort：https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide/b_ESA_Admin_Guide_chapter_010101.html
- Symantec：https://support.symantec.com/en_US/article.HOWTO126432.html
- Postfix：https://petermolnar.net/howto-spf-dkim-dmarc-postfix/

Cisco での DKIM レコードのホスティング

DKIM レコードを Cisco にホストした場合、ドメイン保護で DMARC レコードに影響を与える変更を加えたときに、レコードが迅速、安全、かつ自動的に更新されます。

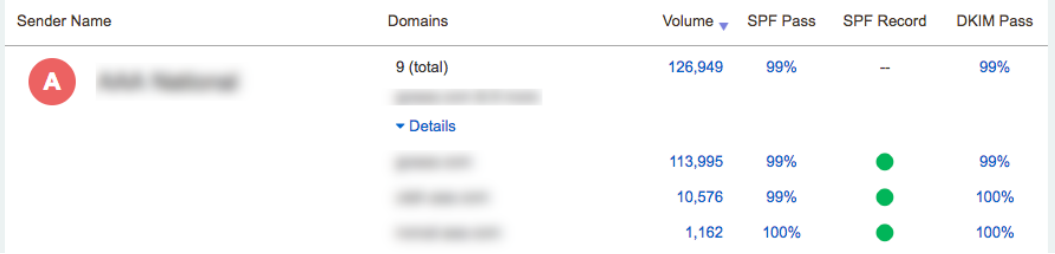
1. [診断（Diagnostics）] > [送信者（Senders）] に移動します。
2. 単一のドメインを選択します。
3. [DKIMキーをモニター（Monitor DKIM Keys）] をクリックします。
    - [ホストされたDKIMキーの管理（Manage Hosted DKIM Keys）] ページに移動した場合、このドメインの DKIM キーは Cisco によってすでにホストされています。
    - [DKIM管理（DKIM Management）] ページに移動した場合、このドメインの DKIM キーは Cisco によってホストされません。
4. [DKIM管理（DKIM Management）] ページで作業している場合は、ドメインの DKIM キー情報を確認してください。DKIM キーがない場合は、[新しいキーを追加...（Add New Key for...）] をクリックして、ドメインの新しい DKIM キーを追加できます。
5. [ホスティングを開始する準備ができました（I' m ready to start hosting）] をクリックします。
6. DKIM 情報を確認します。一部のセレクタでは、Cisco で CNAME レコードと TXT レコードのどちらをホストするかを選択できます。
    - [CNAME]（デフォルト）：CNAME キーはサードパーティによってホストされることが多く、サードパーティがドメインの DKIM キーに変更を加えた場合、Cisco によって自動的に検出されます。
    - [TXT]：ドメインの DKIM キーを常にそのままにしておきたい場合にのみ、これを選択します。サードパーティが DKIM キーに加えた変更は、Cisco によって自動的に検出されません（これは、CNAME レコードを使用するオプションが使用可能な場合に共通することではありませんが、CNAME が使用可能でない場合にはデフォルトとなります）。
7. [ホスティングの開始（Start Hosting）] をクリックします。

この時点で、ドメインホストにあるネームサーバー情報（NS レコード）を更新する必要があります。表示されるページで、NS レコードに必要な情報が得られます。

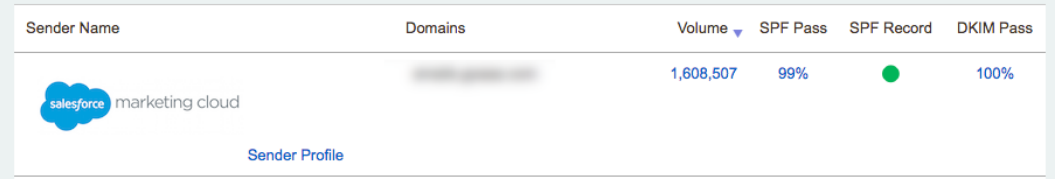
DNS を更新してそれが伝播されると、[ドメインのDMARCステータスの診断（Diagnose the DMARC status of your domains）] ページ（[診断（Diagnostics）] > [ドメイン（Domains）]）で、DKIM 列内の記号の横に「H」が表示されます（ H）。DNS を更新するまで、ホスティング保留中の記号（ ）が DKIM 列に表示されます。

DKIM が機能していることの検証

ドメインの DKIM 署名が有効になると、[送信者（Senders）] ページに結果が表示されます。次の例では、[DKIM 合格（DKIM Pass）] 列が更新され、カスタム送信者 A から送信されたメッセージのドメインに関する DKIM 合格の結果が表示されます。



ウェルノウン送信者の結果も表示されます。次の例は、送信者 Salesforce Marketing Cloud から送信された電子メールの DKIM 合格の結果を示しています。

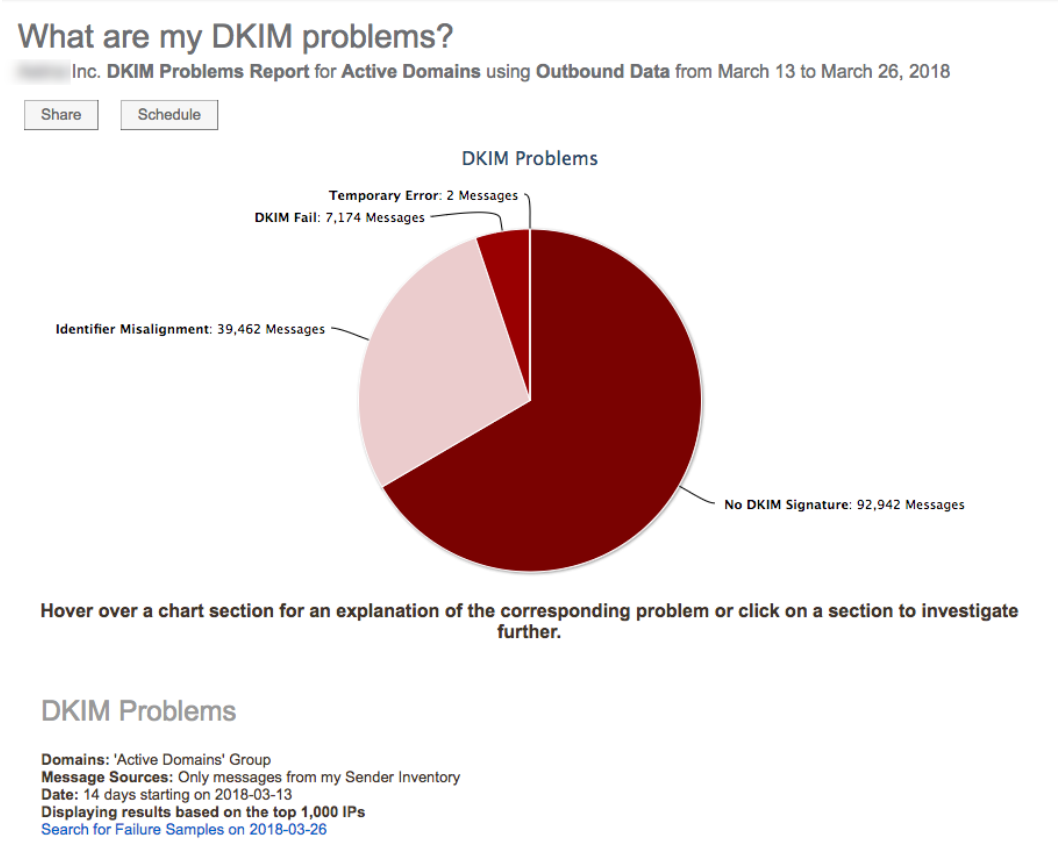


[DKIM合格（DKIM Pass）] 列に示されているいずれかの結果のリンクをクリックすると、次のセクションで説明する [DKIMの問題（What are my DKIM Problems?）] レポートの結果が表示されます。

DKIM の問題の特定

[DKIMの問題（What are my DKIM Problems?）] レポートを使用すると、認証の作業を進め、特定のドメインの送信者ごとに DKIM 署名を取得する際に、対処が必要な問題のドメインとカテゴリを特定できる場合がよくあります。

1. [分析（Analyze）] > [電子メールトラフィック（Email Traffic）] に移動します。
2. [DKIMの問題（What are my DKIM Problems?）] をクリックして、最初のレポートを表示します。



[DKIMの問題(DKIM Problems)]レポートの最上位画面

DKIM の問題の例

多くの場合、識別子のアライメント不一致が「DKIM 署名なし」(メッセージに DKIM の署名がまったく付いていない状態)の次に大きな問題となります。なお、左上の [設定の変更(Modify Settings)] ボタンを使用すると、範囲を絞り込んだり、このレポートをフィルタ処理したりできます(たとえば、1 つのドメインに関する過去 2 週間の DKIM の問題だけを表示することが可能です)。詳細については、「「電子メールトラフィックレポートの設定」 ページ 120」を参照してください。

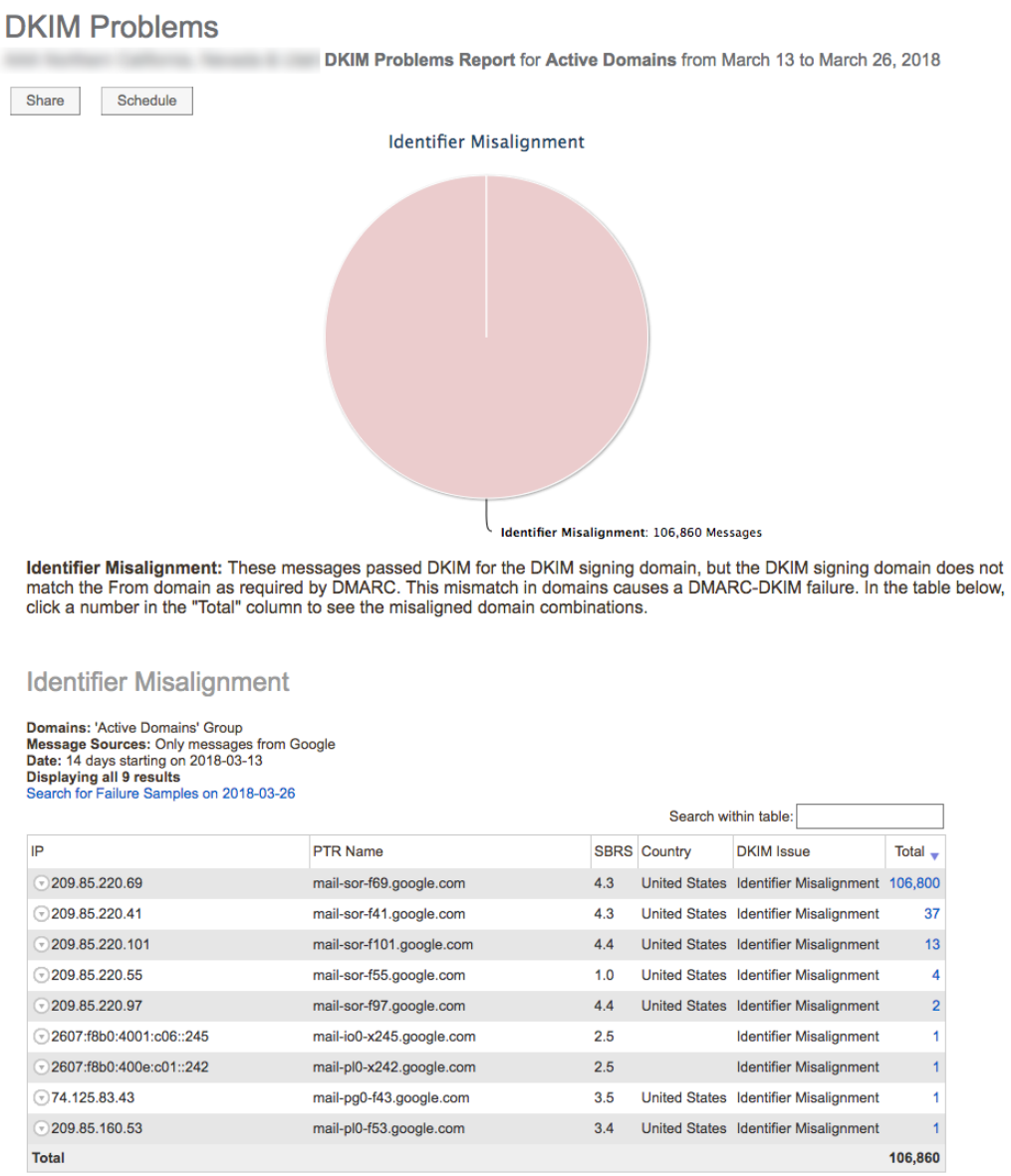
たとえば、[すべての送信元から(From All Sources)] のメッセージを調べるために範囲を広げることができます。[送信者インベントリに含まれない送信者(Senders outside your Sender Inventory)] は、[診断(Diagnostics)] > [送信者(Senders)] ページの [未承認(Unapproved)] タブに表示されます。

問題を理解するために、このレポートの下部にある送信者のリストを調べてください。たとえば以下のように、選択したドメインに関して、送信者 Google から送信されるメールに「識別子のアライメント不一致」と「DKIM 署名なし」の問題があることがわかる場合があります。

Sender	DKIM Issues	Total
Google	**All Issues**	**107,981**
	Identifier Misalignment	106,858
	No DKIM Signature	1,057
	DKIM Fail	66

Google に関する識別子アライメント不一致の問題

送信者 Google から送信されたメッセージのリンクをクリックし、その送信者の詳細情報を確認します。

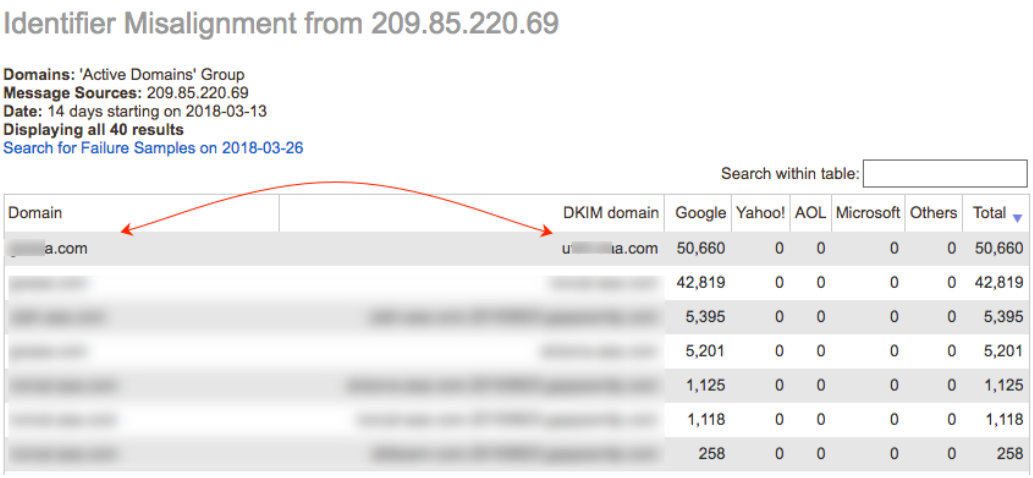


Google に関するアライメント不一致の詳細ビュー

ビューには、Google から送信されたメッセージが整合していないことが示されます。実際、整合の問題の大部分は 1 つの IP アドレス（209.85.220.69、mail-sor-f69.google.com）に原因があります。

IP アドレスのリンクをクリックしてさらに詳細を確認します。

この例では、問題の大部分（5 万超）の原因が DKIM キーと整合していない 1 つのドメインにあります。



次の方法で問題のカテゴリを絞り込むことができます。

- DKIM 署名なし（特定のドメインの送信者に DKIM 署名を付ける必要があります）
- 識別子のアライメント不一致（特定のドメインに使用されている署名キーを送信元ドメインと整合させる必要があります）

ドメインごとに、[送信者（Senders）] ページと [DKIMの問題（What are my DKIM problems?）] レポートビューを使用して、各ドメインのすべての送信者に系統的に DKIM 署名を付けることができます。

レポートの共有または登録

[DKIMの問題（What are my DKIM Problems?）] レポートを他のユーザーに送信したり、一定の間隔で電子メールバージョンのレポートを受け取ったりできます。詳細については、「「電子メールトラフィックレポートの共有」 ページ 121」と「「電子メールトラフィックレポートのスケジュール」 ページ 121」を参照してください。

レポートをスケジュールする場合、レポートの範囲は常に現在のビューになることに注意してください。たとえば、ドメインの包括的な DKIM レコードを作成するプロセスを進める際に、レポートの範囲を広げたバージョン（すべてのドメインのすべての送信者）を受け取ると同時に、レポートの範囲をビジネスオーナーに絞り込んだバージョンのレポート（1 つのドメインの 1 つの送信者）を定期的に送信できます。

EasyDKIM アナライザ

ドメイン保護EasyDKIM アナライザを使用すると、既存の DKIM レコードを分析したり、承認済み送信者に基づいて新しい DKIM レコード作成したりできます。

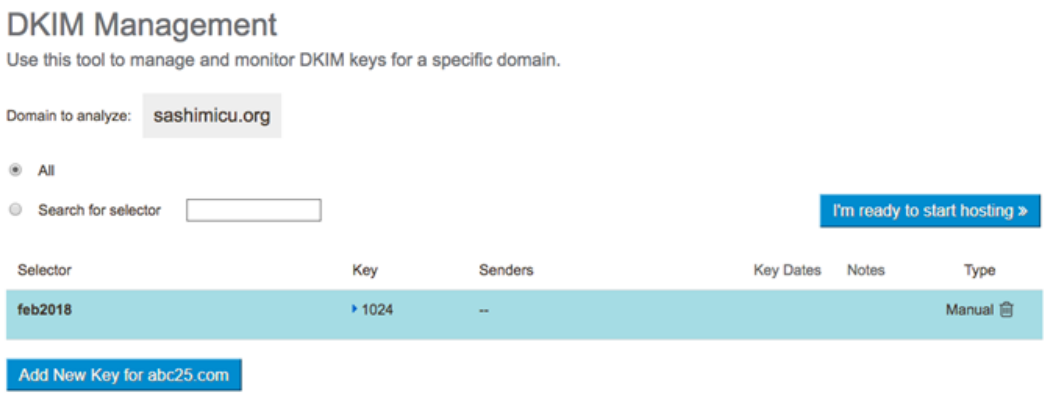
EasyDKIM アナライザでのドメインの DKIM キーの表示

ドメイン保護の EasyDKIM アナライザは、ドメインの DKIM レコードに関する情報を表示し、変更を加える場合に便利です。また、まだ DKIM レコードをホストしていなければ、Cisco に DKIM レコードを簡単にホストできます。

1. [診断（Diagnostics）] > [送信者（Senders）] に移動します。
2. 単一のドメインを選択します。
3. [DKIMキーをモニター（Monitor DKIM Keys）] をクリックします。

[ホストされたDKIMキーの管理(Manage Hosted DKIM Keys)] ページに移動した場合、このドメインの DKIM キーは Cisco によってすでにホストされています。[DKIM管理(DKIM Management)] ページに移動した場合、このドメインの DKIM キーは Cisco によってホストされません。どちらの場合も、ここに表示される内容と実行できる操作は、DKIM ホスティングに関連することを除き、同じです。

[ホストされたDKIMキーの管理(Manage Hosted DKIM Keys)]/[DKIM管理(DKIM Management)] ページでは、ドメインの DKIM キー情報が各キーの詳細とともに表にリストされます。デフォルト表示では、ドメインの集約データとフォレンジックデータを生成元とする DKIM キーが、ドメインの検証後にドメイン保護によって表示されます。[セレクタを検索(Search for selector)] オプションボタンをクリックし、セレクタの全部または一部を入力して、その入力内容でリストをフィルタ処理します。



[DKIM管理(DKIM Management)] ページの例。

DKIM キー情報は、ドメイン保護に手動で入力した場合、背景が青色になります。

次の表では、[DKIM管理(DKIM Management)] ページでドメインの DKIM キーごとに使用可能な情報について説明します。

項目	説明
[セレクタ(Selector)]	DKIM 署名の s= の部分。
[キー(Key)]	キーの長さをビット単位で示します。数値をクリックすると、DNS の DKIM レコードの詳細が表示されます。DKIM レコードが CNAME DNS レコードにある場合、詳細は **CNAME:** で始まります。キーの長さの横に (黄色か赤色)または アイコンが表示されることもあります。これは、DKIM レコードに問題があることを示しています。 アイコンは、DNS の DKIM レコードに欠落した部分が 1 つ以上あることを示しています。 は、キーのローテーションが始まってから過度の時間が経過したことを示しています(黄色の場合は 60 ～ 90 日、赤色の場合は 91 日以上)。詳細については、いずれかのアイコンをクリックしてください。
[送信者(Senders)]	ドメインにこの DKIM キーを使用する送信者をリストします。 をクリックすると、DKIM キーの送信者が表示されます。送信者名の横にあるエンベロープアイコン( )は、送信者が既知のメールボックスプロバイダーであり、この DKIM セレクタによるメッセージの発信元ではない可能性があることを示しています。
[主要な日付(Key Dates)]	送信者の横にある をクリックすると、ドメインの送信者から送られたメッセージにドメイン保護によって DKIM キーが最初に表示された日にちと、最近表示された日にちを確認できます。
[注記(Notes)]	参考のためにドメインの DKIM レコードに関するメモを入力できます。 をクリックすると、メモを追加、編集、または削除できます。
[タイプ/編集	ドメインの DKIM レコードが Cisco によってホストされていない場合、この列の表題は [タイプ

項目	説明
(Type/Edit)]	(Type)] であり、その情報はドメインのレコードのタイプです。通常、これは DNS になります。 ドメインの DKIM レコードが Cisco によってホストされている場合、この列の表題は [編集 (Edit)] です。 アイコンをクリックすると、DKIM レコードを編集できます。

ドメイン保護でモニターするドメイン DKIM レコードの追加

ドメイン保護にまだ表示されていないドメインの DKIM レコードがある場合は、手動で追加できます。

その DKIM レコードのセレクタを知っている必要があります。

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. 単一のドメインを選択します。
3. [DKIMキーをモニター(Monitor DKIM Keys)] をクリックします。
4. [[DomainName]の新しいキーを追加(Add New Key for [DomainName])] をクリックします。
5. 追加する DKIM キーのセレクタを入力します。
6. [検索(Lookup)] をクリックします。DKIM レコードを調べて間違いがないことを確認します。
7. [DKIMキーを追加(Add DKIM Key)] をクリックします。

DKIM キーが [ホストされたDKIMキーの管理(Manage Hosted DKIM Keys)]/[DKIM管理(DKIM Management)] ページに追加されます。キー情報は、背景が青色で、[タイプ(Type)] 列に [手動(Manual)] と表示されるため、ドメイン保護によって自動的に検出されたキーではなく手動で追加されたキーであることがわかります。

DMARC : Domain-based Message Authentication, Reporting, & Conformance

DMARC(Domain-based Message Authentication, Reporting & Conformance、RFC 7489 として 2015 年 3 月に公開)は、SPF および DKIM と連携して機能する電子メール認証標準であり、電子メールに長い間不足していた機能をもたらします。つまり、電子メールドメインがどのように使用および悪用されているかを送信者が把握することを可能にします。既存の認証テクノロジーを組み合わせてセキュアな電子メールチャネルを作成する方法が規定されており、受信者には認可されていない電子メールを安全に処分する方法に関する明確な指示が提供されます。しかも、これらのすべてがインターネット規模で実現されます。

DMARC の DNS レコードの例:

_dmarc.domain.com. IN TXT “v=DMARC1; p=reject; rua=mailto:d@rua.cisco.com; ruf=mailto:d@ruf.cisco.com;”

DMARC は DKIM と SPF に基づいて保護とレポートの両方を提供。

着信 DMARC 可視化機能を使用すると、Agari 電子メールセンサーを介して会社が所有するドメインの着信電子メールを DMARC で可視化できます。これにより、サードパーティ送信者によるものも含め従業員に送信している電子メールは、DMARC 認証に合格していると確信が持てるようになります。「「DMARC の仕組み」 ページ 25」を参照してください。

モニターポリシーでの DMARC レコードの公開

モニターポリシーでの DMARC レコードの公開は、ドメイン保護において非常に早い段階で行う手順の一つです。これは、ドメイン保護への最初のデータフローを実現する手法でもあります。また、これによって間接的に、ユーザーがドメインの所有者であることを Cisco に示すことができます。DMARC ポリシーは、DNS でテキスト（TXT）リソース レコード（RR）として公開され、特定のドメインから受信した電子メールが非適合メールであった場合に電子メール受信者が実行する必要のあるアクションを通知します。

保護する予定のドメインごとに、「none」フラグが設定されたポリシーで DMARC レコードを公開します。このレコードは、受信者から Cisco へのデータレポートの送信を要求します。その後、ドメイン保護を使用してデータを分析し、必要に応じてメール ストリームを変更することができます。

ポリシーに「none」フラグが設定された DMARC レコードは、メール フローや、そのドメインから送信されるメッセージの配信可能性に影響を与えません。「none」フラグはドメインからの電子メールを認証するプロセスの手始めの手順であり、これによって分析用のデータを収集できるようになります。この後、ドメインの SPF と DKIM を実装し、送信者を認可する（このガイドの以降の手順）ことで、DMARC ポリシーのフラグをより厳格なもの（「検疫」や最終的には「拒否」）に変更できます。

モニターポリシーで DMARC レコードを公開するには、次の手順を実行します。

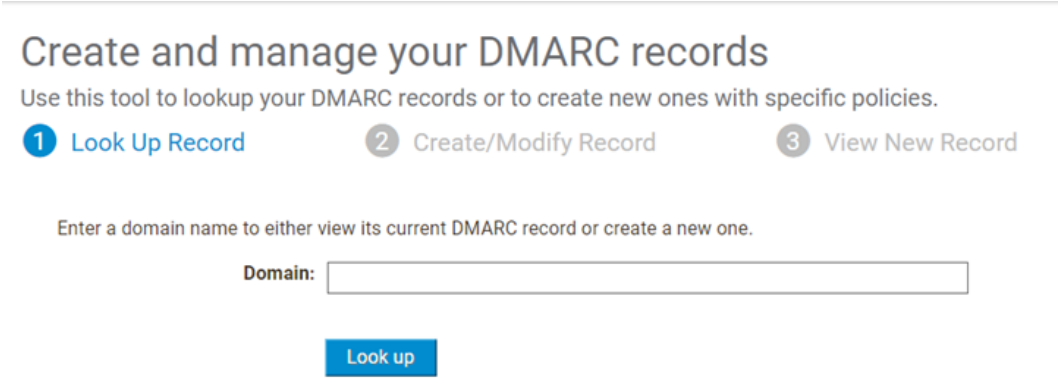
- 「DMARC Builder による DMARC レコードの作成」 次のページ）
- 「DNS での DMARC レコードの公開」 ページ 75
- 「DMARC ポリシー公開のための組織ドメインの追加」 ページ 77

DMARC Builder による DMARC レコードの作成

ドメイン保護の DMARC Builder により、任意のドメインの DMARC ポリシーレコードを検索できます。次に、DMARC Builder を使用して、そのドメインの有効な DMARC レコードのテキストを変更または作成することができます。最後に、DMARC Builder は、ドメインの DNS プロバイダーと、DMARC レコードの公開方法に関する情報を提供します。

(このガイドでは、独自の DNS インフラストラクチャを編集することを前提としています。Cisco で DMARC レコードをホストする方法については、Cisco サポートにお問い合わせください)

1. [ツール(Tools)] > [DMARC] に移動します。



DMARC Builder のステップ 1

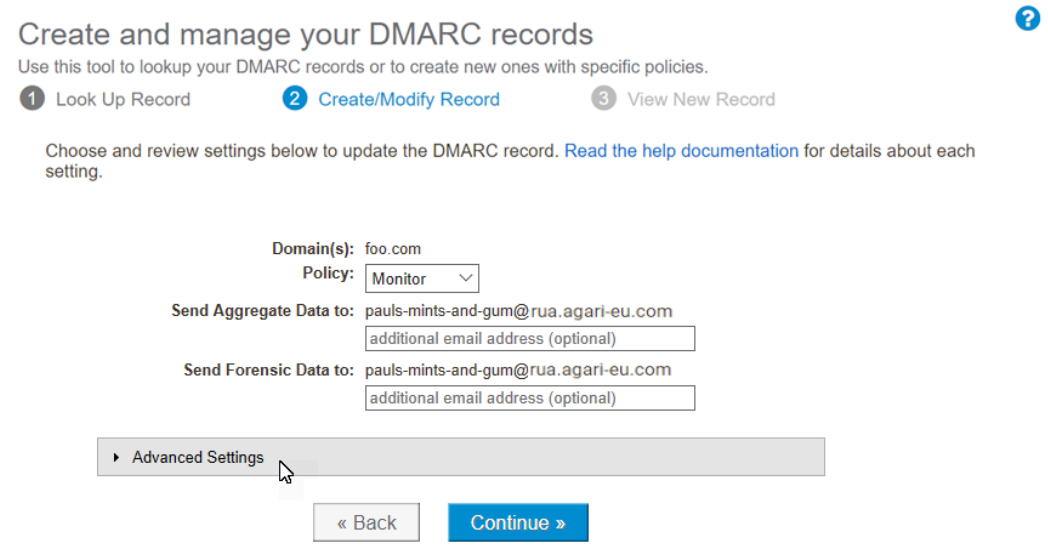
2. ドメイン名を入力します。
3. [検索(Look up)] をクリックして、ドメインの現在の DMARC レコードを表示するか、新しいドメインを作成します。ドメインに DMARC ポリシーがない場合は、新しい DMARC レコードを作成するオプションか、Cisco で新しい DMARC レコードをホストするオプションが表示されます。

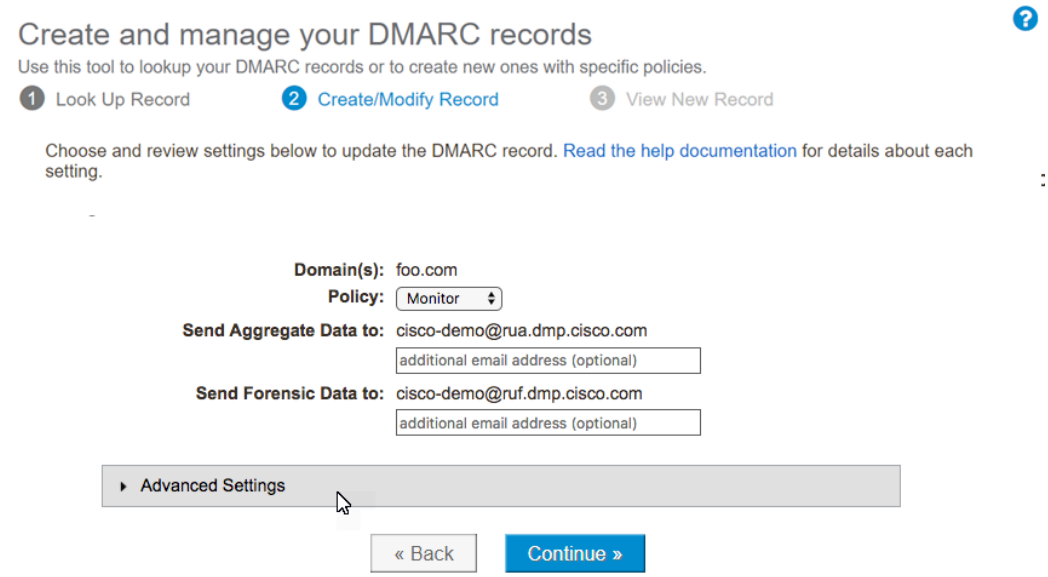
4. [新しいDMARCレコードを作成(Create new DMARC record)] をクリックします。
5. DMARC レコードの設定を入力します。詳細については、「「DMARC Builder の設定」 ページ 79」を参照してください。
6. [続行(Continue)] をクリックします。
7. [指示の作成(Create Instructions)] をクリックします。次の手順で使用するテキストファイル(.txt)がダウンロードされます。

ドメイン保護で保護する予定のドメインごとに繰り返してください。

DMARC の例

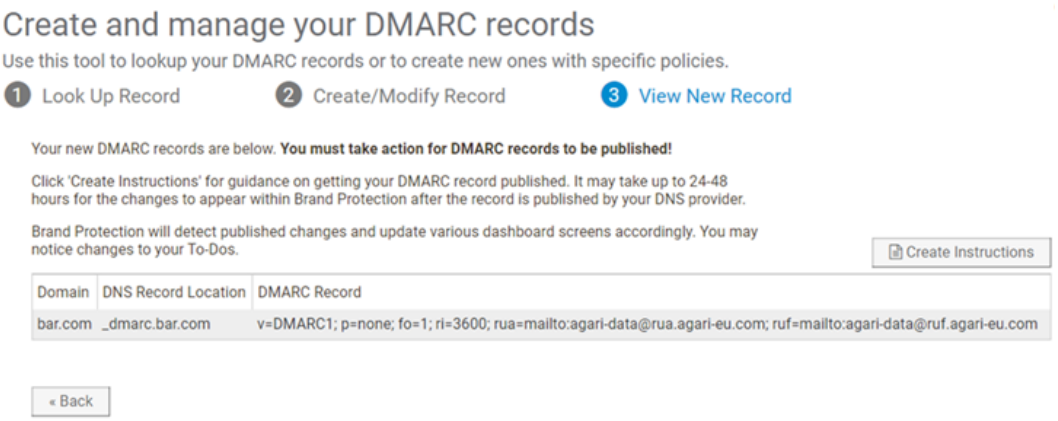
この例では、ドメインは「foo.com」、ポリシーは「モニター」、レポートデータを送信する Cisco の電子メールアドレスは「cisco-demo@rua.cisco.com」と「cisco-demo@rufcisco.com」です。

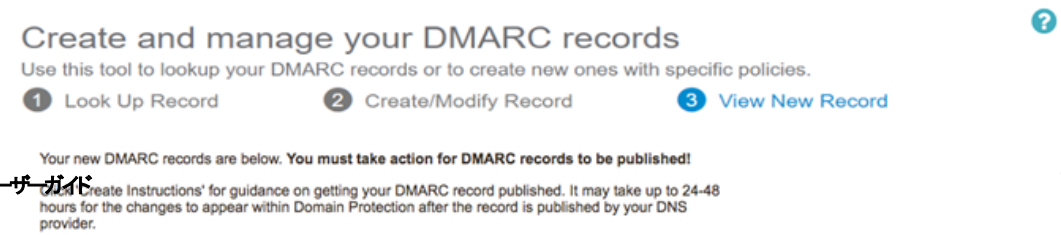




DMARC Builder のステップ 2

この DMARC レコードは、ドメイン「bar.com」用です。





DMARC Builder のステップ 3

次のパラメータを定義します。

- [DNSレコードの場所（DNS Record Location）]：_dmarc.bar.com 用に DNS テキストレコードがインストールされている必要があります。
- **v=DMARC**：これは DMARC 仕様のバージョン 1 です。
- **p=none**：このレコードのポリシー（p=）は「なし」（モニター専用ポリシー）です。
- **fo=1**：ドメイン所有者に DMARC 失敗レポートを送信するためのディレクティブ。認証/アライメントの脆弱性が見つかった場合（アライメント一致（合格）以外のものが生成された場合）は 1 です。
- **ri=3600**：レポート間隔（ri=）は 3600 秒（1 時間に 1 回）である必要があります。
- **rua=**organization_name**@rua.cisco.com**：**集約**情報の送信先となるレポートユーザー電子メールアドレス（rua=）です。このアドレスは組織に固有のものであり、Cisco がデータを受信するためのメカニズムです。
- **ruf=**organization_name**@ruf.cisco.com**：**フォレンジック**情報が送信先となるレポートユーザー電子メールアドレス（ruf=）です。このアドレスは組織に固有のものであり、Cisco がデータを受信するためのメカニズムです。

DNS での DMARC レコードの公開

ドメイン用の適切な形式の DMARC レコードが作成されたので、ドメインの DNS レコードを更新する必要があります。

DMARC レコードを公開する正確な手順は、ドメインの DNS の管理方法によって異なります。ただし、DNS 変更の要求を送信する場合、この DMARC レコードを TXT リソース レコードとして公開するように要求する必要があります。「「DMARC Builder による DMARC レコードの作成」 ページ 73」のリストにある [DNSレコードの場所（DNS Record Location）] セクションに示されているように、「_dmarc」を前に付けることによって作成されたサブドメインでレコードを公開する必要があります。引用符内のすべてを含む完全な DMARC レコード（引用符自体は不要）が含まれていることを確認してください。その後のレコードに明示的に示されているスペース以外の折り返し文字、改行文字、または空白文字が含まれないようにしてください。

（注）

- オンライン DNS 管理ツールによるダイレクト アクセスによってドメインの DNS を管理する場合は、TXT レコードを公開するためのセクションまたは DMARC レコードに固有のセクションを探してください。
- Web ホスティング オンライン管理インターフェイスによるアクセスによってドメインの DNS を管理する場合は、DNS 設定と、TXT レコードまたは DMARC レコードを入力する場所を探してください。
- ユーザーの社内で DNS を管理している場合は、社内の DNS 管理チームを通じて DNS レコードの公開要求を送信する必要がある可能性があります。
- サードパーティがドメインの DNS をホストしている場合は、ドメインの DNS 設定を更新するためにサードパーティにチケットを送信する必要がある可能性があります。

おめでとうございます。

DNS プロバイダーによって DMARC レコードを公開した後、ドメイン保護内で変更が反映されるまでに最大 24 ～ 48 時間かかる場合があります。

Cisco での DMARC レコードのホスティング

DMARC レコードを Cisco にホストした場合、ドメイン保護で DMARC レコードに影響を与える変更を加えたときに、レコードが迅速、安全、かつ自動的に更新されます。

新しい DMARC レコードの追加（「「DMARC Builder による DMARC レコードの作成」 ページ 73」を参照）と Cisco での DMARC レコードのホスティングを一度にまとめて行うことはできません。

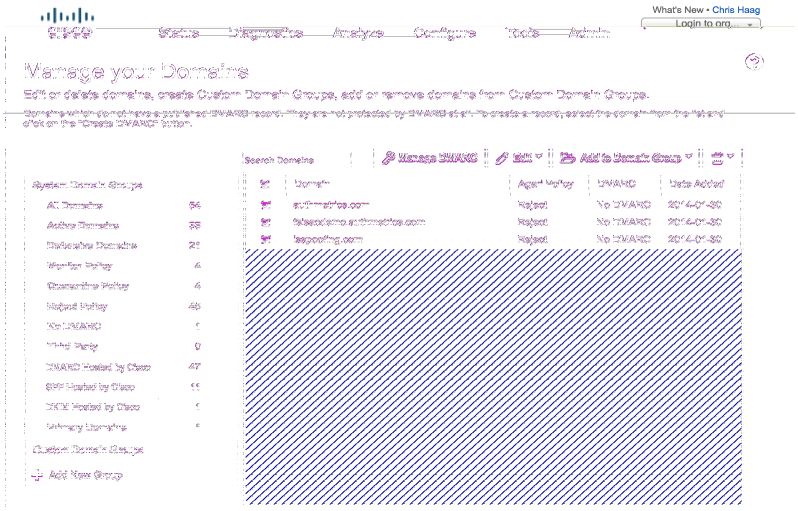
ドメインが検証されたら、Cisco でそのドメインの DMARC レコードをホストできます。

1. [設定（Configure）] > [ドメインの管理（Manage Domains）] に移動します。
2. [すべてのドメイン（All Domains）] をクリックします。
3. [DMARCのホスティング（DMARC Hosted）] 列を [なし（No）] にして、1 つ以上のドメインを選択します。
4. [DMARCの管理（Manage DMARC）] をクリックします。
5. [Cisco でDMARCレコードのホスティング（Host DMARC Record at Cisco）] をクリックします。
6. [ホスティング手順を取得（Get Hosting Instructions）] をクリックします。これにより、次のステップに必要な情報が記載されたテキストファイルがダウンロードされます。
7. ドメインごとに、DNS レコードに新しい CNAME レコードを作成します。ダウンロードしたファイルには、各ドメインのエントリがあります。ドメインごとに、ホストレコードに CNAME レコードを追加します。[名前（Name）] にはファイルに記載された [DNSレコードの場所（DNS Record Location）] 値を使用し、[レコード（Record）] にはファイルに記載された [CNAMEレコード（CNAME Record）] 値を使用します。文字やキャリッジリターンなどを追加せずに、現状のまま値をコピーします。

この最後のステップは、ドメイン保護の外部で実行され、Cisco が DMARC のレコードをホストできるようにするために必要です。

DMARC レコードがないドメイン用にホストされる DMARC レコードの作成

1. [設定（Configure）] > [ドメインの管理（Manage Domains）] に移動します。
2. [DMARCなし（No DMARC）] をクリックします。



3. Cisco で DMARC レコードをホストするドメインを選択します。
4. [DMARCの管理（Manage DMARC）] をクリックします。
5. ドメインの DMARC 設定を確認します。

6. [Cisco でDMARCレコードのホスティング（Host DMARC Record at Cisco）] をクリックします。
7. [ホスティング手順を取得（Get Hosting Instructions）] をクリックします。これにより、次のステップに必要な情報が記載されたテキストファイルがダウンロードされます。
8. ドメインごとに、DNS レコードに新しい CNAME レコードを作成します。ダウンロードしたファイルには、各ドメインのエントリがあります。ドメインごとに、ホストレコードに CNAME レコードを追加します。[名前（Name）] にはファイルに記載された [DNSレコードの場所（DNS Record Location）] 値を使用し、[レコード（Record）] にはファイルに記載された [CNAMEレコード（CNAME Record）] 値を使用します。文字やキャリッジリターンなどを追加せずに、現状のまま値をコピーします。

DMARC ポリシー公開のための組織ドメインの追加

ドメイン保護で保護する予定のすべてのドメイン用の p=None ポリシーで DMARC レコードを公開した場合は、この手順をスキップできます。これらのドメインは、Cisco によって自動的に追加され、検証されます。

p=None ポリシーをまだ公開していないドメインがある場合は、ドメイン保護でそのドメインを追加します。ドメイン保護では、ほとんどのアクティビティがドメインを中心に行われます。この手順のアクティビティにより、ドメイン保護は組織に関連付けられているドメインを認識します。

1. [ステータス（Status）] > [保護（Protection）] に移動します。
2. [ドメインを追加（Add Domains）] をクリックします。

3. ドメインに関する情報を入力します。

[ドメインを追加する方法（How do you want to add your domains?）]	1 つ以上のドメインを入力するか、ドメイン情報が含まれているファイルをアップロードします。 • [ドメインを入力（Type in your domain(s)）] を選択し、テキストフィールドに 1 つ以上のドメインをカンマで区切って入力します。 • [ドメイン名のファイル（txtまたはcsv）をアップロード（Upload a file of domain names (txt or csv)）] を選択し、[ファイルを選択（Choose File）] をクリックして、1 つ以上のドメイン名がカンマで区切られて記載されたファイルを選択します。
[これらのカスタムドメイングループに追加（Add to these Custom Domain Groups）]	フィールド内をクリックして、1 つ以上のドメイングループにドメインを追加します（「「ドメイングループ」 ページ 133」を参照してください）。 また、[新しいグループを追加（Add a new group）] をクリックして、新しいドメイングループを作成することもできます。
[Cisco ポリシーを設定（Set the Cisco Policy）]	これにより、追加するドメインの DMARC ポリシーレベルが決まります。
[防御としてマーク（Mark as Defensive）]	防御ドメインは、電子メールを送信しない会社ドメインに似ていますが、他のユーザーが所有しないようにするために所有するドメインです。
[サードパーティとしてマーク（Mark as Third Party）]	サードパーティドメインは、コンテンツと電子メールがサードパーティによって管理されているドメインです。サブドメインでよく見られます。たとえば、warriors.nba.com などです。
[プライマリとしてマーク（Mark as Primary）]	できるかぎり早く拒否に移行したい重要なドメインです。

4. [ドメインを追加（Add your domains）] をクリックします。

確認メッセージが表示されます。この時点で、Ciscoは組織がこれらのドメインを担当していることを検証します。これには、最大 24 時間かかる場合があります。

[設定（Configure）] > [未検証のドメイン（Unverified Domains）] に移動して、未検証のドメインをリストできます。

未検証ドメインとは

ポリシーを指定し、検証済みドメインのデータのみを表示することができます。

Cisco の担当者は、システムドメインにアップロードされたドメインを管理する準備ができたことを確認するためのアクションを実行して、ドメインを検証します。Cisco は、未検証のすべてのドメインを定期的にチェックして、そうしたドメインの検証を可能にする変更が加えられたかどうかを確認します。検証対象のドメインを再送信して、ドメインの再チェックを早めることができます。

ドメインを最も迅速に検証済みにする方法は、ドメインの DMARC レコードを公開することです。これを行う場合は、「「DNS での DMARC レコードの公開」 ページ 75」を参照してください。Cisco は、この方法を強くお勧めします。ドメインの DMARC レコードを公開するには、ドメインの DNS エントリを変更する必要があります。これは、ユーザーがドメインに対する権限を持っていることを示すもう一つの方法です（Cisco は、システムに入力されたすべてのドメインを検証することにより、間違ってまたは不注意によって入力されたドメインがないことを確認できます）。

Cisco がドメインを検証したら、DMARC レコードをホストするよう Cisco に依頼できます。詳細については、「「Cisco での DMARC レコードのホスティング」 ページ 76」を参照してください。ドメインの DMARC レコードが Cisco によってホストされると、ドメイン保護で DMARC レコードに影響を与える変更が行われた場合、それを DMARC レコードに迅速、安全、かつ自動的に反映させることができます。

DNS と検証に関する追加のオプション

ドメインの DNS ネームサーバーレコード（NS レコード）を更新します。これにより、Cisco はそれを組織に関連付けることができるようになります。ドメインの DNS が外部 DNS プロバイダーによって管理されている場合は、これを実行できない可能性があります。

例：ユーザーが cat.com をドメイン保護に登録しようとしているとします。ユーザーの組織に関して dog.com が Cisco によってすでに承認されており、cat.com の NS レコードが ns1.dog.com である場合、Cisco はユーザーが cat.com に対する権限を持っていることを信用できます（ユーザーのものであるとシスコが把握しているドメインによって cat.com の DNS が制御されているため）。

ドメインの DNS メール エクスチェンジャ レコード（MX レコード）を更新します。これにより、Cisco はそれを組織に関連付けることができるようになります。これは、実行できない場合があります（ドメインに関して電子メールがどのようにホストされているかによって異なる）。

例：ユーザーが cat.com をドメイン保護に登録しようとしているとします。ユーザーの組織に関して dog.com が Cisco によってすでに承認されており、cat.com の MX レコードが mail1.dog.com である場合、Cisco はユーザーが cat.com に対する権限を持っていることを信用します（cat.com に送信されるすべての電子メールが、ユーザーのものであるとシスコが把握しているドメインに向けられるため）。

DMARC Builder の設定

DMARC ポリシーにより、送信者は自身の電子メールが SPF や DKIM で保護されていることを示し、いずれの認証方法にも合格しなかった場合の対処方法（メッセージの検疫や拒否など）を受信者に指示できます。ドメイン保護の DMARC Builder により、任意のドメインの DMARC ポリシーレコードを検索できます。次に、DMARC Builder を使用して、そのドメインの有効な DMARC レコードのテキストを変更または作成することができます。DMARC Builder は、ドメインの DNS プロバイダーと、DMARC レコードの公開方法に関する情報も提供します。

このトピックでは、DMARC Builder のすべての設定について説明します（[詳細設定（Advanced Settings）] はオプションであり、デフォルトで推奨設定になっています。これらの設定は変更しないことをお勧めします）。

設定	説明
[ドメイン（Domain(s)）]	DMARC レコードを作成または変更するドメインの名前。1 つのドメイン名やドメイン名のカンマ区切りリストを入力できます。
[ポリシー（Policy）]	ヘッダー From アドレスにドメイン所有者のドメインが含まれている受信メッセージで DMARC チェックに合格しなかったものに関して、ドメイン所有者が電子メール受信者に実行することを要求するアクション。次を選択します。 • [なし（None）]：これは、DMARC チェックに合格しなかったメッセージに関して特別なアクションを実行せず、ドメインの DMARC レコードで指定されているレポート アドレスに DMARC データを送信するように、受信者に指示します。注：これは、この手順で選択することが推奨されるポリシーです。 • [検疫（Quarantine）]：これは、DMARC チェックに合格しなかったメッセージを受信者のスパム フォルダ（またはその他の、不審なメッセージを確認できる隔離されたエリア）に入れるように、受信者に要求します。

設定	説明
	• [拒否(Reject)]:これは、DMARC チェックに合格しなかったすべてのメッセージを拒否し、そのアクションを DMARC データでレポートするように、受信者に要求します。受信者は、拒否されたメッセージを入手できません。
[集約データの送信先(Send Aggregate Data to)]	DMARC 集約データの送信先となる電子メールアドレス。DMARC Builder では、Cisco のレポートアドレスがデフォルトで設定されています。Cisco のアドレスに加えて、別のレポートアドレスを指定することもできます。どちらも DMARC レコードに表示されます。DMARC 受信者は両方のアドレスにレポートデータを送信する必要があります。
[フォレンジックデータの送信先(Send Forensic Data to)]	DMARC フォレンジックデータの送信先となる電子メールアドレス。DMARC Builder では、Cisco のレポートアドレスがデフォルトで設定されています。Cisco のアドレスに加えて、別のレポートアドレスを指定することもできます。どちらも DMARC レコードに表示されます。DMARC 受信者は両方のアドレスにレポートデータを送信する必要があります。 警告:フォレンジックデータは、DMARC チェックに合格しなかったメッセージのリアルタイムフローです。そのデータ量は非常に多くなる場合があり、また非常に散発的である場合もあります。このフィールドで独自のレポートアドレスを追加すると、ローカルメールサーバーで問題が発生する可能性があります。
詳細設定	
[レポート形式(Report Format)]	DMARC フォレンジックレポートの形式を指定します。DMARC 仕様では AFRF と IODEF の両方が許可されていますが、現在 DMARC 受信者から送信される形式は AFRF のみです。
[DKIM識別子アライメント(DKIM identifier alignment)]	DKIM でサブドメインがどのように処理されるかを定義します。次を選択します。 • [緩和(Relaxed)]:DKIM 署名ドメインとヘッダー From ドメインが相互のサブドメインになることができます。 • [厳格(Strict)]:DKIM 署名ドメインとヘッダー From ドメインは完全に一致する必要があります。
[SPF識別子アライメント(SPF identifier alignment)]	SPF でサブドメインがどのように処理されるかを定義します。次を選択します。 • [緩和(Relaxed)]:MailFrom ドメインとヘッダー From ドメインが相互のサブドメインになることができます。 • [厳格(Strict)]:MailFrom ドメインとヘッダー From ドメインは完全に一致する必要があります。
[次の%に適用(Apply to %)]	これは、ポリシーの適用先となるドメインからのメッセージの割合です。たとえば、ここに「拒否」ポリシーと 50% を指定した場合、拒否ポリシーは受信者からのメッセージのうち DMARC 認証に失敗したランダムな 50% にのみ適用されます。
[レポートインターバル(Reporting Interval)]	DMARC 仕様では、時間間隔をさまざまに変えた DMARC 集約レポートをリクエストできます。ただし実際には、現在実装されているどの DMARC でもレポートは 24 時間単位でのみ送信されます。
[サブドメインポリシー(Subdomain Policy)]	デフォルトでは、ドメインの DMARC ポリシーは、すべてのサブドメインに適用されます。DMARC では、必要に応じてサブドメインに異なるポリシーを適用できます。指定したすべてのサブドメインポリシーが、「すべて」のサブドメインに適用されます。特定のサブドメインに異なるポリシーを適用する場合は、そのサブドメイン専用の DMARC レコードを公開します。

設定	説明
[フォレンジックレポートオプション（Forensic Report Options）]	どの失敗条件であればフォレンジックレポートを受信してもよいかを DMARC 受信者に指示できます。Customer Protect は、デフォルトでは SPF または DKIM が失敗したら必ずレポートを送信するようにこれを設定します。この設定を、SPF と DKIM の両方が失敗した場合にのみレポートを送信するように変更できます。

第 5 章

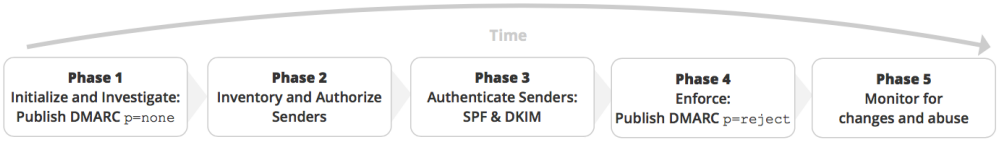
DMARC の実装

このセクションでは、組織で DMARC を実装するプロセスについて説明します。

全体的なプロセス

Cisco は、DMARC と電子メール認証の実装支援で業界をリードする製品です。

そのプロセスには、おおまかには次の 5 つのフェーズがあります。



DMARC を実装するフェーズ

Cisco Domain Protection を使用してユーザーのすべてのドメインからの電子メールを認証するための Cisco のベストプラクティスは通常、以下に示す特定のステップで構成されます。

Cisco Domain Protection の実装の全体的なプロセス

フェーズ	ステップ
フェーズ 1	1.ドメイン保護へのアクセスを取得し、Cisco の入門トレーニングを受ける
	2. DMARC レコードをモニタ ポリシーで公開する
	3.ドメインをポータルに追加する
フェーズ 2	4.トラフィックをモニタする
	5.ターゲットドメインを特定する
	6.すべての送信者を特定して分類する（ウェルノウンとカスタム）
	7.すべてのサードパーティ送信者を追跡するスプレッドシートを作成する

フェーズ	ステップ
フェーズ 3	8. 新しい SPF レコードを提示する
	9. 新しい SPF レコードを公開する
	10. 社内のビジネス オーナーを特定する
	11. サードパーティ オーナーに DKIM 署名を要求する
	12. すべてのサードパーティ送信者用の DKIM キーを実装する
	13. すべてのサードパーティ送信者に関して DKIM が機能していることを確認する
	14. 電子メール ゲートウェイで DKIM 署名を有効にする
	15. 電子メール ゲートウェイで DKIM が機能していることを確認する
フェーズ 4	16. すべてのビジネス オーナーから承認を得る
	17. DMARC レコードを拒否に移行する（Cisco が最終確認のために使用）
フェーズ 5	18. アラートとレポートを確認する

ステップ 2 とステップ 4 ～ 18 は、保護する予定の組織内のドメインごとに繰り返すプロセスと考えることができます。

一部のドメインでは、このプロセスを迅速に完了できます。たとえば、ユーザーが所有しているものの、正当な電子メールの送信に使用する予定のない、防御ドメインや内部ドメインなどです。

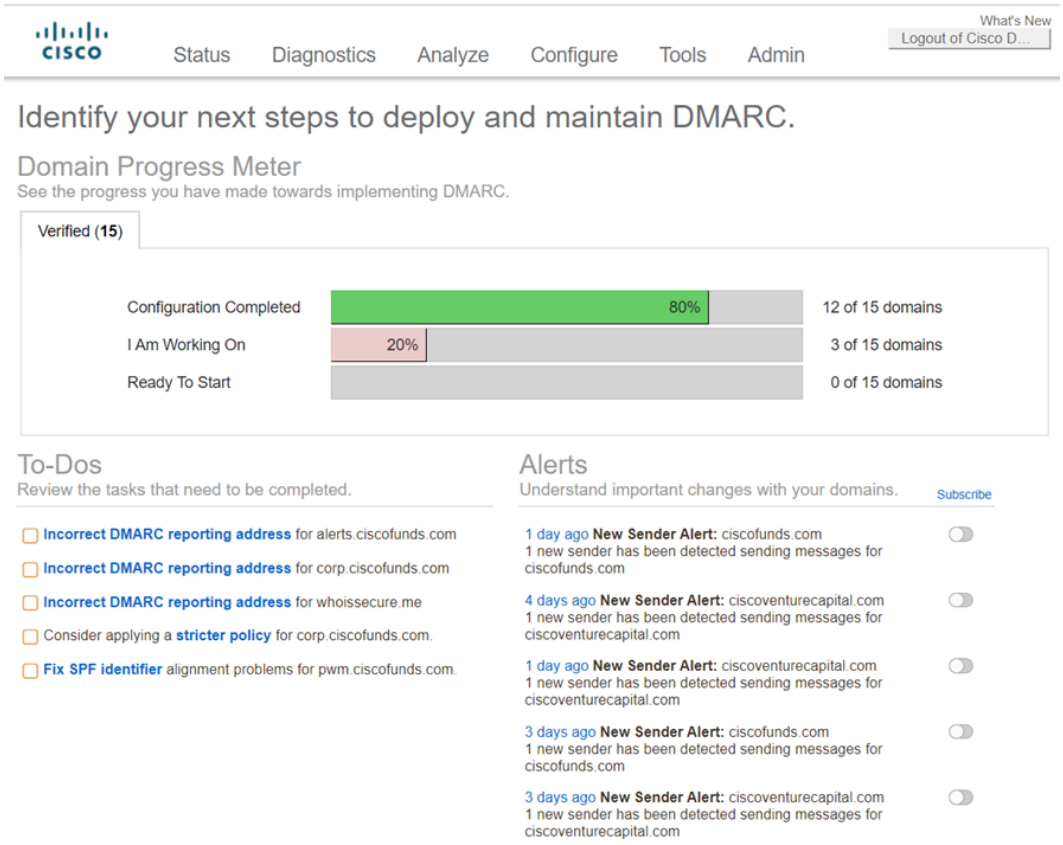
その他のドメイン（プライマリドメインや、非常に大きな容量のドメインなど）では、プロセスの各手順を系統的に完了し、必要に応じて変更をステークホルダーに伝える必要があります。

以下の章では、各手順を理解して完了するための支援を提供します（特に Cisco Domain Protection で利用可能な支援データを使用）。

ダッシュボード

Cisco Domain Protection にログインすると、ダッシュボード設定ページが開き、次の項目が表示されます。

- [ドメイン進捗状況メーター（Domain Progress Meter）]：ドメインの設定のステータスを表示します。
- [To-Do（To-Dos）]：DMARC 展開ステータスに基づいて完了することが推奨されているタスクとアクションがリストされます。Cisco Domain ProtectionTo-Do を手動で処理する必要はありません。自動的に表示され、完了したタスクに基づいて毎日再計算されます。
- [アラート（Alerts）]：登録できるアラート。詳細については、「「アラート」 ページ 129」を参照してください。

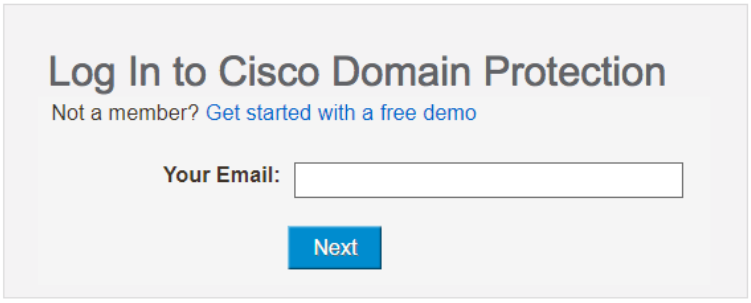


ログイン情報とトレーニングの取得

開始とオンボーディングの一般的なプロセスの一環として、Cisco Domain Protection にアクセスする方法の手順を入手する必要があります。

このキックオフミーティングでは、https://dmp.cisco.com での Cisco Domain Protection へのアクセス権が Cisco の担当者から付与されます。

Cisco から初期アカウントログイン情報が記載された電子メールが届きます。このアカウントは、組織が管理に使用する最初のアカウントです。今後組織のユーザーアカウントを追加で作成する場合は、このアカウントを使用します。



ドメイン保護のログイン。

サポートへの問い合わせ

アクセス権をまだ受け取っていない場合は、Cisco サポート（https://www.agari.com/support/）にお問い合わせください。

高度なトピック

この段階で考慮する必要がある項目は次のとおりです。

- ドメイン保護には、ユーザーアカウントに異なるレベルのアクセス権を付与する、ロールベースの権限付与およびアクセス制御（RBAC）が含まれています。読み取り専用ユーザー、監査専用ユーザー、ポータル内のレポートの管理のみが可能なユーザーなどを作成してみることをお勧めします。権限の詳細については、「「ユーザーアカウント」 ページ 145」を参照してください。
- ドメイン保護にサインインすると、組織に固有の URL（例：https://organization_name. dmp.cisco.com）にリダイレクトされます。
- Cisco では、プログラムを使用して製品の一部にアクセスするための API を提供しています。API ドキュメンテーションにアクセスするには、ユーザーアカウントを作成し、そのユーザーに API アクセス権を付与する必要があります。
- Cisco では、サービスプロバイダーから開始（SP 開始）するか ID プロバイダーから直接開始（IdP 開始）するシングルサインオン（SSO）もサポートしています。組織の SSO 設定の詳細については、「「シングルサインオン（SSO）」 ページ 149」を参照してください。

管理者アカウント（およびユーザー作成権限を持つ後続のアカウント）は、作成されたユーザーのパスワードをリセットできます。

トラフィックと送信者のモニタリング

ドメインの DMARC レコードが正常に作成されて公開されると、データが Cisco Domain Protection に表示されるようになります。

これで、電子メールトラフィックのモニタリング、保護するドメインの特定、すべての送信者の特定と分類、そして最後にすべてのサードパーティ送信者を追跡するためのスプレッドシートの作成を行うプロセスを開始できます。

トラフィックのモニタリング

DMARC レポートデータ（集約およびフォレンジック）のドメイン保護への送信が開始されると、トラフィックをモニターするプロセスを開始できます。Cisco のあるお客様に、DMARC レポートデータに基づいてトラフィックをモニターできるプロセスに関連して次のように言われたことがあります。「Cisco にはハッとさせられました。まるで暗い部屋で電気をつけたようなものでした」。

ほとんどの場合、有意義なデータセットを得たいのであれば、少なくとも 2 週間以上のデータを収集することをお勧めします。

DMARC レポートデータでは、次の情報を得ることができます。

- ドメインに代わって電子メールを送信している送信者。
- インベントリの送信元（IP アドレス）。
- そうした電子メールが SPF および DKIM 認証チェックに合格しているかどうか。

ただし、そのためにはまず、トラフィックを一定期間モニターする必要があります。この期間は、組織の規模や複雑さによって異なります。たとえば、組織では、領収書や注文確認の電子メールは毎日送信するものの、サードパーティ送信者を利用したマーケティングキャンペーンの送信はそれほど頻繁ではなく、別の部門による別のサードパーティ送信者からのニュースレターの送信はさらに散発的であるといった場合があります。一部の正当なサードパーティ電子メールのニュースレター、キャンペーン、またはその他のタイプのイベントは、月に 1 回、四半期に 1 回、または年に 1 回の頻度で発生する場合があるため、最初の 2 週間の期間内にキャプチャされない可能性があることを考慮する必要があります。ほとんどの企業では、DMARC レポートから集約データを取得するまで、電子メール エコシステムがどれほど複雑かが認識されません。

重要な点として、ユーザーに代わるすべてのサードパーティ送信者のデータを収集できたこと、またそのためにドメインのすべての潜在的な送信者に対して認証をセットアップ可能であることを確信できる期間にわたってデータをモニターする必要があります。

モニタリングの開始

[分析（Analyze）] > [電子メールトラフィック（Email Traffic）] に移動し、ドメイン保護で利用可能なレポートを確認します。

[電子メールトラフィックの分析（Analyze Email Traffic）] ページには、電子メール エコシステムに役立つビューを提供するための一般的な質問のリストがあります。こうしたレポートで表示できることと実行できることの詳細については、「「電子メールトラフィックレポート」 ページ 116」を参照してください。

こうしたレポートで、ビューとドリルダウンのすべての機能を実際に試してください。

次のステップ

非常に多数のレポート機能や非常に詳細なデータが提供されることにたじろがないでください。プロセスのこの時点では、プロジェクトの次のフェーズの戦略を策定するために必要な情報を収集しているにすぎません。

- 当面のターゲットとなる一連のドメインを特定します。
- ターゲットとなる一連のドメインの送信者メッセージング認証要件（SPF、DKIM）を特定します。
- メッセージングチームと協力して、ユーザー自身のメールインフラストラクチャで、ターゲットとなる一連のドメインの認証を設定します。
- サードパーティ送信者やビジネスユニットと協力して、ターゲットとなる一連のドメインの認証を設定します。

- ターゲットとなる一連のドメインの DNS SPF レコードや DNS DKIM レコードを変更します。
- 設定を確認します。

ターゲットとなる 1 つまたは複数のドメインの特定

ドメイン保護でデータをモニタする期間が経過したら、保護を開始するために、ターゲットとなる一連のドメインの特定を検討し始める必要があります。

たとえば、次のような戦略が考えられます。

- プライマリドメインまたは最大容量のドメインから開始します。

  プライマリドメイン（特定のサブドメインではなく）が、その企業からのすべての電子メール通信に使用される場合があります。たとえば、多くの場合、joe@foo.com といったアドレスの電子メールが、企業の日々の通信、つまり領収書や注文確認、ニュースレター、マーケティングキャンペーン、または CRM システムからのメッセージの送信に使用されます。

  このような場合は、プライマリドメインから作業を始めることをお勧めします。

- 防御ドメインから始めて、アクティブ ドメインへと進んでください。

  定義上、防御ドメインでは電子メールが送信されないため、厳格なポリシーによって比較的簡単にロックすることができます（ロックされていない未保護の防衛ドメインは、スパム送信者に悪用される潜在的な脅威にさらされています）。ドメイン保護のデータを使用すると、防御ドメインをカタログ化し、DMARC 拒否ポリシーにすばやく移行することができます。

  防御ドメインのポリシーを強化した後に、組織の正当なメールを送信することを意図したドメインに作業を集中することができます。

- 一貫性のある送信プロファイルまたは統一された送信プロファイルを使用して、ビジネス クリティカル ドメインまたはバックエンド システム自動化ドメインから作業を開始します。

  たとえば、組織が単一のサードパーティ送信者（たとえば、Zendesk）に属する単一のサブドメイン（たとえば、support.foo.com）からカスタマーサポートメールを送信する場合、先にこのドメインの認証を実装する方が作業が容易になる可能性があります。

- あるいは、ビジネスに不可欠でないものから始めます。

  逆に、ビジネス クリティカルな電子メールの配信を中断できない場合は、最初にマーケティング メールを送信するドメインから作業を開始することを検討します。これは、それらのスケジュールされたメーラーからの認証済み電子メールの送信に関する「移行期間」を特定する方が容易である場合があるためです。

どの戦略を選択する場合でも、「「ドメイングループ」 ページ 133」の説明に従って、[設定（Configure）] > [ドメインの管理（Manage Domains）] ビューを使用してドメインをグループ化する必要があります。

送信者の特定と分類

特定の一連のドメインに関して電子メール認証を実装するための戦略を定義できたので、それらのドメイン（および組織全体）の送信者の識別と分類を開始できます。

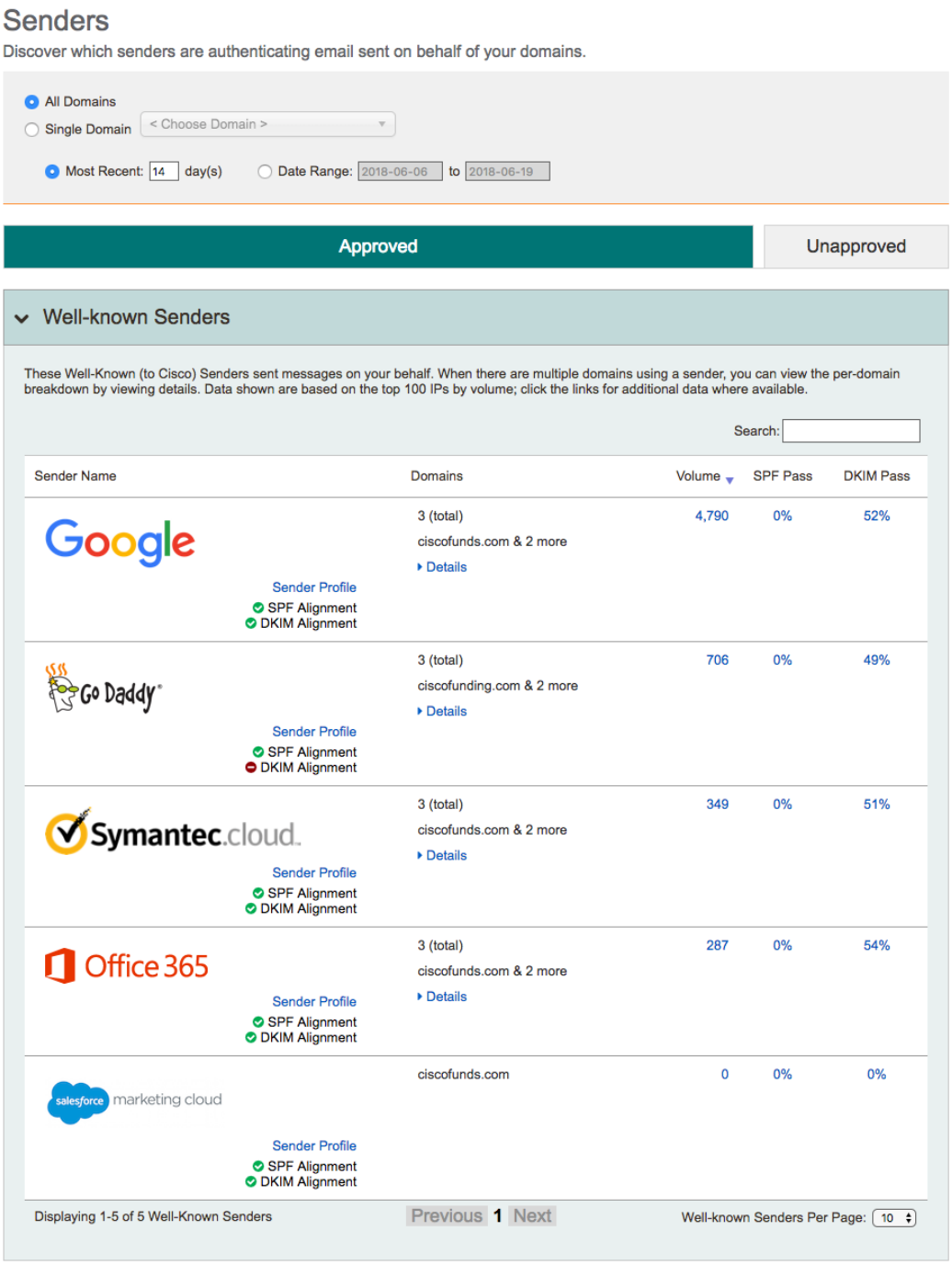
送信者

[送信者（Senders）] ページを使用すると、ドメイン保護システム内のすべてのドメインのウェルノウン送信者とカスタム送信者を整理して追跡できます。[送信者（Senders）] ページでは、シスコがユーザーの組織に関して正当であると見なしているウェルノウン送信者を確認できます。そうした送信者の IP アドレスを検出するために使用されたドメインと、それらを検出するためにシスコが使用した特定の DNS レコードソースも確認できます。[送信者（Senders）] ページを使用すると、システム内のすべてのドメインのウェルノウン送信者とカスタム送信者を整理して追跡できます。

送信者を表示するには、[診断（Diagnostics）] > [送信者（Senders）] に移動します。[送信者（Senders）] ページに表示される内容は次のとおりです。

- 承認済みのウェルノウン送信者とカスタム送信者。
- 未承認の送信者と IP アドレス。

デフォルトでは、ドメイン保護は、ウェルノウン サードパーティ送信者を、それらの送信インフラストラクチャによって認識します。たとえば、このビューでは組織が Marketo、Acxiom、Taleo、および Epsilon を正当なサードパーティ送信者として特定し、承認しています。



[送信者（Senders）] ページの [ウェルノウン送信者（Well-known Senders）] セクションの Marketo、Acxoim、Taleo、および Epsilon。

このページに移動した際に、承認済みおよび未承認の送信者が表示されなくても、心配はいりません。DNS で適切な認証情報がまだ公開されていないだけかもしれません。

[送信者(Senders)] ページの仕組み

ドメイン保護にデータが送られるようになると、組織全体の情報とドメインごとの情報が集約されます。ドメイン保護は、組織のすべての登録済みドメインの DNS レコードを調べて、組織に代わって正当なメッセージを送信している可能性の高い IP アドレスを判別します。

[承認済み(Approved)] タブにデータが表示されない場合は、[未承認(Unapproved)] タブをクリックして次の情報を確認します。

- 未承認のウェルノウン送信者
- 未承認の IP アドレス

[送信者(Senders)] ページのデータをドメインおよび日付でフィルタ処理できます。詳細については、「「送信者のフィルタ処理」 ページ 96」を参照してください。

[送信者(Senders)] ページの要点

ドメイン保護にデータが送られるようになると、組織全体の情報とドメインごとの情報が集約されます。[送信者(Senders)] ページを使用すると、システム内のすべてのドメインのウェルノウン送信者とカスタム送信者を整理して追跡できます。

[承認(approve)] をクリックして、正当なサードパーティウェルノウン送信者を [未承認(Unapproved)] タブから [承認済み(Approved)] タブに移動します(一方、組織でウェルノウン送信者を使用しないことになっている場合は、[無視(ignore)] をクリックして、無視する送信者のリストにそのウェルノウン送信者を移動できます)。このドメイン保護内で送信者を認可する操作([未承認(Unapproved)] から [承認済み(Approved)] への移動)は、ドメインに関して管理する SPF ポリシーと DKIM ポリシーの基礎となります(それらに反映されます)。次に、ドメインの承認済み送信者からのすべての電子メールを認証するための作業を行います。また、DMARC ポリシーは、認証に合格しなかったメッセージに対するアクションを受信者に指示します。

ここでは、次の操作が可能です。

- 「ドメインの送信者の承認」 下
- 「ドメインの送信者の無視」 ページ 92
- 「カスタム送信者への未承認の IP アドレスの追加」 ページ 95
- 「未承認の IP アドレスの無視」 ページ 95

ドメインの送信者の承認

ドメインに代わってメールを送信するエンティティのデータがドメイン保護に蓄積されるため、次のようにドメインごとにウェルノウン送信者を承認することをお勧めします。

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. [単一ドメイン(Single Domain)] をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているドメインがすべて含まれています。
3. [未承認(Unapproved)] タブをクリックします。

4. 未承認の送信者の名前をクリックして、その送信者に関する情報を確認し、承認しようとしている送信者に間違いないことを確認します。確認する必要がある主な事項は次のとおりです。
    - 未承認の送信者からどのくらいの量のトラフィックが送信され、そこに何か規則性があるか。一貫した頻度で送信している送信者は、正規の送信者であることが多いようです。
    - トラフィックを把握するために使用できる失敗サンプルデータはあるか。Failure Samples エクスプローラを使用してサンプルを入手できれば、未承認の送信者が正当に使用されている事例があるかどうかを判断できる可能性があります。
5. ブラウザの [戻る(Back)] ボタンをクリックします。
6. 引き続き送信者を承認する場合は、対応する [承認(Approve)] リンクをクリックします。
7. [送信者の追加(Add Sender)] ダイアログボックスで、IP スペース(IP アドレスとネットブロック)を確認します。この送信者が代わって電子メールを送信するドメインが他にもある場合は、[追加のドメインを選択(Select Additional Domains)] フィールドも表示されます。こうしたドメインについて個別に送信者を確認したくない場合は、この時点でそうしたドメインについてもこの送信者を承認できます。
8. [承認済みに追加(Add to Approved)] をクリックします。

ドメインへの送信者の追加

送信者がドメインに代わってトラフィックを送信する場合、プロセスの一部がその送信者を承認します(「「ドメインの送信者の承認」(前のページ)」を参照してください)。また、ドメイン保護がトラフィックを検出しなかったドメインの送信者を承認することもできます。

ウェルノウン送信者を追加するプロセスは、カスタム送信者を追加するプロセスとは若干異なります。

ドメインへのウェルノウン送信者の追加

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. [単一ドメイン(Single Domain)] をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているアクティブなドメインがすべて含まれています。
3. [承認済み(Approved)] タブをクリックします。
4. [ウェルノウン送信者(Well-known Senders)] セクションで、[ウェルノウン送信者を追加(Add Well-known Sender)] をクリックします。
5. 送信者を選択します。リストには、ドメインの未承認のウェルノウン送信者がすべて含まれています。
6. [承認済みに追加(Add to Approved)] をクリックします。

ドメインへのカスタム送信者の追加

1. [診断(Diagnostics)] > [送信者(Senders)] に移動します。
2. [単一ドメイン(Single Domain)] をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているアクティブなドメインがすべて含まれています。
3. [承認済み(Approved)] タブをクリックします。
4. [カスタム送信者(Custom Senders)] セクションで、[カスタム送信者を追加(Add Custom Sender)] をクリックします。
5. 送信者を選択します。このリストには、ドメインへのトラフィックがない未承認のカスタム送信者が含まれて

います。

6. [承認済みに追加(Add to Approved)]をクリックします。

ドメインの送信者の無視

自分が管理しているドメインに代わって送信者がメールを送信していて、ドメイン保護でそうした送信者を分類したくない場合は、そのドメインではその送信者を無視するようにドメイン保護に指示できます。

1. [診断(Diagnostics)]>[送信者(Senders)]に移動します。
2. [単一ドメイン(Single Domain)]をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているドメインがすべて含まれています。
3. [未承認(Unapproved)]タブをクリックします。
4. 未承認の送信者の名前をクリックして、その送信者に関する情報を確認し、無視しようとしている送信者に間違いないことを確認します。確認する必要がある主な事項は次のとおりです。
    - 未承認の送信者がフォワーダとして機能している可能性はありますか。ホスティングサービスとメールボックスプロバイダーがメッセージの転送に使用されることがありますが、比較的少量の場合がほとんどです。こうした送信者は、実際にトラフィックの発信元に使用する場合を除き、承認する必要はありません。
5. ブラウザの[戻る(Back)]ボタンをクリックします。
6. それでもドメインの送信者を無視する場合は、送信者の[無視(Ignore)]リンクをクリックします。
7. [送信者の無視(Ignore Sender)]ダイアログボックスで、[追加のドメインを選択(Select Additional Domains)]フィールドに、この送信者が代わって電子メールを送信する他のドメインが表示されます。こうしたドメインについて個別に送信者を確認したくない場合は、この時点でそうしたドメインについてもこの送信者を無視できます。
8. [無視リストに追加(Add to Ignore List)]をクリックします。

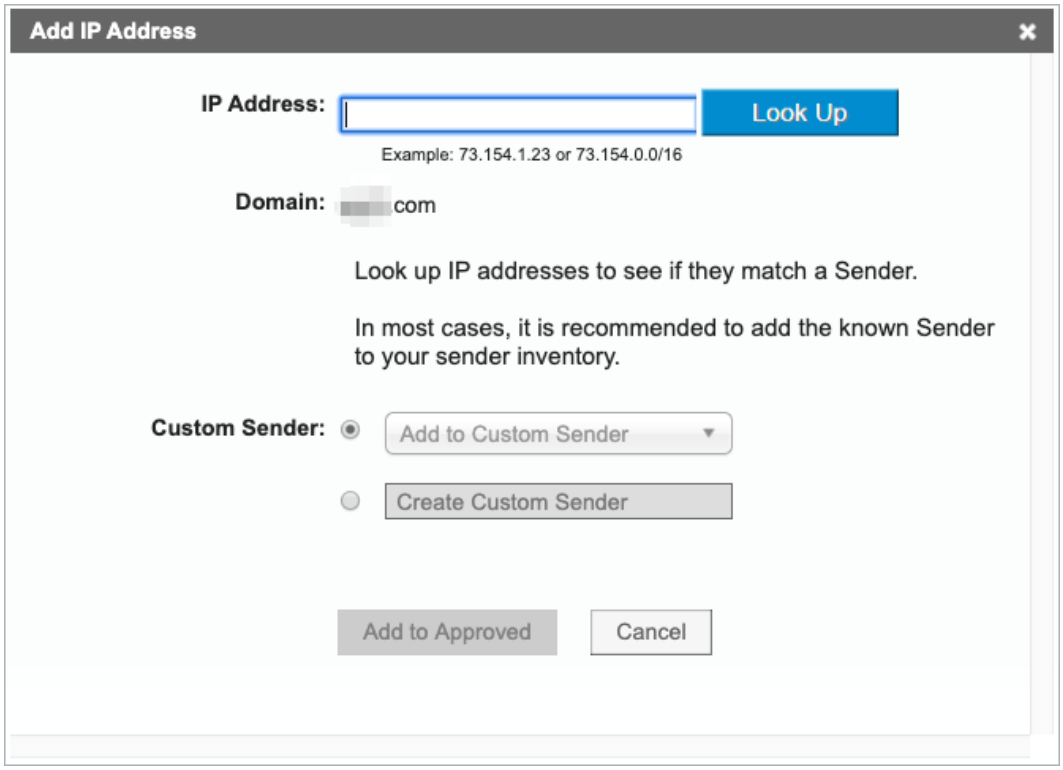
カスタム送信者への IP アドレスの追加

既存の顧客側の送信者に IP アドレスまたはネットブロックを手動で追加したり、それらを使用して新しい顧客側の送信者を定義したりできます。

同じ IP アドレスが複数のウェルノウン送信者または複数のカスタム送信者に同時に属することはできません。IP アドレス範囲(ネットブロック)のどの部分も、複数のウェルノウン送信者または複数のカスタム送信者に同時に属する(重複する)ことはできません。同じ IP アドレスまたは IP アドレス範囲の部分が、複数のウェルノウン送信者または複数のカスタム送信者に属する(重複する)ことはできません。

1. [診断(Diagnostics)]>[送信者(Senders)]に移動します。
2. [単一ドメイン(Single Domain)]をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているドメインがすべて含まれています。
3. [承認済み(Approved)]タブをクリックします。

4. [カスタム送信者（Custom Senders）] セクションで、[IPアドレスを追加（Add IP Address）] をクリックします。



5. [IPアドレス（IP Address）] フィールドに、単一の IP アドレスまたはネットブロック（IP アドレス範囲）を入力します。ネットブロックを入力する場合は、CIDR（Classless Inter-Domain Routing）表記にする必要があります。
6. [検索（Look Up）] をクリックします。

この時点で、いくつかの事態が発生する可能性があり、実行できるアクションはルックアップ結果によって異なります。

ルックアップ	ルックアップ結果	可能なアクション
IP アドレス	ウェルノウン送信者の定義にすでに含まれています。	何も実行しません。IP アドレスは承認済みの送信者に残ります。 • [キャンセル（Cancel）] をクリックします。 既存の承認済みカスタム送信者に IP アドレスを追加します。 1. [カスタム送信者に追加（Add to Custom Sender）] をクリックし、既存のカスタム送信者を選択します。 2. [承認済みに追加（Add to Approved）] をクリックします。 新しいカスタム送信者に IP アドレスを追加し、そのカスタム送信者を承認します。 1. [カスタム送信者を作成（Create Custom Sender）] をクリックし、カスタム送信者名を入力します。 2. [作成して承認（Create and Approve）] をクリックします。
IP アドレス	カスタム送信者の定義にすでに含まれています。	IP アドレスは、既存のカスタム送信者に追加することも、新しいカスタム送信者の作成に使用することもできません。異なるカスタム送信者に同じ IP アドレスを含めることはできません。[キャンセル（Cancel）] のみが可能です。

ルックアップ	ルックアップ結果	可能なアクション
IP アドレス	送信者は検出されませんでした。	既存の承認済みカスタム送信者に IP アドレスを追加します。 1. [カスタム送信者に追加(Add to Custom Sender)]をクリックし、既存のカスタム送信者を選択します。 2. [承認済みに追加(Add to Approved)]をクリックします。 新しいカスタム送信者に IP アドレスを追加し、そのカスタム送信者を承認します。 1. [カスタム送信者を作成(Create Custom Sender)]をクリックし、カスタム送信者名を入力します。 2. [作成して承認(Create and Approve)]をクリックします。
ネットブロック	ネットブロックは、複数のカスタム送信者をオーバーフローします(複数のカスタム送信者の定義にすでに含まれています)。	ネットブロックは、既存のカスタム送信者に追加することも、新しいカスタム送信者の作成に使用することもできません。異なるカスタム送信者に同じ IP アドレスまたはネットブロックのセクションを含めることはできません。[キャンセル(Cancel)]のみが可能です。
ネットブロック	ネットブロックは、1 つの承認済みのカスタム送信者をオーバーフローします(1 つの承認済みのカスタム送信者の定義にすでに含まれています)。	ネットブロックは、既存のカスタム送信者に追加することも、新しいカスタム送信者の作成に使用することもできません。異なるカスタム送信者に同じ IP アドレスまたはネットブロックのセクションを含めることはできません。[キャンセル(Cancel)]のみが可能です。
ネットブロック	ネットブロックは、1 つの未承認のカスタム送信者をオーバーフローします(1 つの未承認のカスタム送信者の定義にすでに含まれています)。	ネットブロックは、既存のカスタム送信者に追加することも、新しいカスタム送信者の作成に使用することもできません。異なるカスタム送信者に同じ IP アドレスまたはネットブロックのセクションを含めることはできません。[キャンセル(Cancel)]のみが可能です。
ネットブロック	ネットブロックはウェルノウン送信者をオーバーフローします。	ネットブロックを既存の承認済みのカスタム送信者に追加します。 1. [カスタム送信者に追加(Add to Custom Sender)]をクリックし、既存のカスタム送信者を選択します。 2. [承認済みに追加(Add to Approved)]をクリックします。 ネットブロックを新しいカスタム送信者に追加し、ネットブロックの送信者を承認します。 1. [カスタム送信者を作成(Create Custom Sender)]をクリックし、カスタム送信者名を入力します。 2. [作成して承認(Create and Approve)]をクリックします。
IP アドレス/ネットブロック	入力した IP アドレスまたは範囲が無効です。	アクションは有効になりません。[キャンセル(Cancel)]ボタンのみをクリックできます。有効な IP アドレスまたはネットブロックを再入力し、[ルックアップ(Look Up)]を再度クリックします。

カスタム送信者への未承認の IP アドレスの追加

電子メールの送信に使用する IP アドレスが組織の送信インフラストラクチャ（たとえば、組織が発信電子メールを送信するために所有し管理している専用のメール交換サーバー）の一部である可能性がある場合、ドメイン保護がそうした IP アドレスを分類することはできません。分類できず、ドメインに関連付けられていない IP アドレスをドメイン保護が認識すると、その IP アドレスは [送信者（Senders）] ページの [未承認のIPアドレス（Unapproved IP Addresses）] セクションにリストされます。特定のドメインで [未承認のIPアドレス（Unapproved IP Addresses）] セクションに認識された IP アドレスがフォワーダとも疑わしいとも判断されなかった場合は、その IP アドレスをカスタム送信者に追加することで分類できます。

1. [診断（Diagnostics）] > [送信者（Senders）] に移動します。
2. [単一ドメイン（Single Domain）] をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているドメインがすべて含まれています。
3. [未承認（Unapproved）] タブをクリックします。
4. [未承認のIPアドレス（Unapproved IP Addresses）] の [アクション可能（Actionable）] セクションで未承認の IP アドレスの名前をクリックし（場合によってはスクロールダウンする必要があります）、その IP アドレスに関する情報を調べて、承認したい IP アドレスに間違いないことを確認します。確認する必要がある主な事項は次のとおりです。
    - [IP情報（IP Information）] タブで、IP アドレスのホスト名と、DMARC 認証に合格した送信メッセージの数を確認します（後者の数が少ない場合は、設定を行う必要があります）。
    - [ドメイン（Domains）] タブで、この IP アドレスから送信されたメッセージの From ヘッダーにあるドメインがきちんと認識し管理しているドメインかどうかを確認します。
5. ブラウザの [戻る（Back）] ボタンをクリックします。
6. 引き続き IP アドレスを承認する場合は、対応する [承認（Approve）] リンクをクリックします。
7. [IPアドレスの追加（Add IP Address）] ダイアログボックスで、顧客側の送信者を選択します。
8. [承認済みに追加（Add to Approved）] をクリックします。

未承認の IP アドレスの無視

電子メールの送信に使用する IP アドレスが組織の送信インフラストラクチャ（たとえば、組織が発信電子メールを送信するために所有し管理している専用のメール交換サーバー）の一部である可能性がある場合、ドメイン保護がそうした IP アドレスを分類することはできません。分類できず、ドメインに関連付けられていない IP アドレスをドメイン保護が認識すると、その IP アドレスは [送信者（Senders）] ページの [未承認のIPアドレス（Unapproved IP Addresses）] セクションにリストされます。特定のドメインで [未承認のIPアドレス（Unapproved IP Addresses）] セクションに認識された IP アドレスがフォワーダとも疑わしいとも判断されなかった場合は、その IP アドレスを [無視（Ignored）] リストに追加して機能しないようにすることができます。

1. [診断（Diagnostics）] > [送信者（Senders）] に移動します。
2. [単一ドメイン（Single Domain）] をクリックし、ドメインを選択します。このリストには、ドメイン保護で管理しているドメインがすべて含まれています。
3. [未承認（Unapproved）] タブをクリックします。
4. [未承認のIPアドレス（Unapproved IP Addresses）] の [アクション可能（Actionable）] セクションで未承認の IP アドレスの名前をクリックし（場合によってはスクロールダウンする必要があります）、その IP アドレスに関する情報を調べて、承認したい IP アドレスに間違いないことを確認します。確認する必要がある主な事項は

次のとおりです。

- [IP情報(IP Information)] タブで、IP アドレスのホスト名と、DMARC 認証に合格した送信メッセージの数を確認します(後者の数が少ない場合は、設定を行う必要があります)。
- [ドメイン(Domains)] タブで、この IP アドレスから送信されたメッセージの From ヘッダーにあるドメインがきちんと認識し管理しているドメインかどうかを確認します。

5. ブラウザの [戻る(Back)] ボタンをクリックします。
6. それでも IP アドレスを無視する場合は、対応する [無視(Ignore)] リンクをクリックします。
7. [無視リストに追加(Add to Ignore List)] をクリックします。

送信者のフィルタ処理

[送信者(Senders)] ページ(「送信者」 ページ 88)をドメインおよび日付でフィルタ処理できます。このトピックでは、[送信者(Senders)] ページの上部にあるフィルタについて説明します。

フィルタ	説明
[ドメイン(Domains)]	次から選択してください。 • [すべてのドメイン(All Domains)](デフォルト):すべてのドメインに代わって電子メールを認証している送信者をすべて表示します。 • [単一ドメイン(Single Domain)]:選択したドメインに代わって電子メールを認証している送信者をすべて表示します。 単一ドメインを選択した場合、適切な権限を持っていれば、そのドメインの SPF レコードを変更できます。
[期間(Period)]	次から選択してください。 • [最新(Most recent)](デフォルト):入力した最新の日数中に電子メールを認証した送信者を表示します。 • [日付範囲(Date Range)]:選択した開始日から終了日までに電子メールを認証した送信者を表示します。

カスタム送信者のウェルノウン送信者への変換

カスタム送信者のネットブロックがウェルノウン送信者に一致するか重複している場合は、そのカスタム送信者をウェルノウン送信者に変換できます。Cisco が新しいウェルノウン送信者をドメイン保護に追加した場合に、一致が「検出」されると、よくこういうことが起きます。

ネットブロックが完全に一致している場合は、単に顧客側の送信者をウェルノウン送信者に変換し、カスタム送信者を削除するだけです。重複が見られる場合、つまりカスタム送信者のネットブロックの一部がウェルノウン送信者に一致し、他の部分は一致しない場合は、どのタイプの送信者にネットブロックを割り当てるか、いくつかオプションがあります。やるべきことを選択すると、あとはドメイン保護がすべての作業を行います。

1. [設定（Configure）] > [カスタム送信者の管理（Manage Custom Senders）] に移動します。
2. アイコンが表示されているカスタム送信者をクリックします。このアイコンは、カスタム送信者に既存のウェルノウン送信者と一致または重複するネットブロックが含まれていることを示しています。
3. 次をクリックします。
    - [ウェルノウン送信者を使用（Use Well-Known Sender）] をクリックして、対応するネットブロックを組織内のウェルノウン送信者として追加します。ネットブロックが完全一致ではなく重複している場合は、次のような結果になります。
    - [カスタム送信者を維持（Keep Custom Sender）] をクリックして、送信者の定義を現状のままにします。

送信者の定義を現状のままにすることにした場合は、アイコンがカスタム送信者に表示されたままとなり、今後いつでもウェルノウン送信者に変換できます。

IP アドレスの重複

カスタム送信者のネットブロックがウェルノウン送信者のネットブロックと重複する場合、3 つのケースが考えられます。次の表では、[ウェルノウン送信者を使用（Use Well-Known Sender）] を選択すると何が起こるのか、ケースごとに説明しています。

ケース	結果
すべてのカスタム送信者のネットブロックがウェルノウン送信者のネットブロックのサブセットです。	カスタム送信者は削除されて、組織内のウェルノウン送信者に置き換えられます。
ウェルノウン送信者のすべてのネットブロックがカスタム送信者のネットブロックのサブセットです。	ウェルノウン送信者が組織に追加されます。ネットブロックの定義がカスタム送信者の定義と一致した場合は、それも追加されます。カスタム送信者は残りますが、その定義にウェルノウン送信者と一致するネットブロックがあればそのネットブロックは削除されます。
カスタム送信者のネットブロックの一部がウェルノウン送信者のネットブロックの一部と同じです。	

すべての送信者の追跡

ドメイン保護に（直接、または DMARC p=none ポリシーを公開することで間接的に）入力したドメインと、一定期間データをモニターして [送信者（Senders）] ページから収集した情報を使用すると、組織で使用するすべてのサードパーティ送信者に関する情報を収集できるはずです。

外部のスプレッドシートを使用すると、この情報を簡単に追跡できます。例については、「「ドメインから送信者を追跡するスプレッドシートの例」 見開きページ」を参照してください。

このスプレッドシートの情報を使用して、適切な認証に必要な SPF レコードと DKIM キーを作成し、認証プロジェクトのステータスを内部で伝達します。

ドメインから送信者を追跡するスプレッドシートの例

ドメイン	送信者	内部連絡先	アカウントの詳細情報
foo.com	Marketo Zendesk CustomSender 1	bob@foo.com	
receipts.foo.com	Taleo MailChimp	jane@foo.com rita@foo.com	MailChimp アカウント 1
newsletters.foo.com	MailChimp	john@foo.com	MailChimp アカウント 2：「jim@foo.com」認証情報を使用（前の管理者）
help.foo.com	Freshdesk （SendGrid）	bill@foo.com	SendGrid
sales.foo.com	Toutapp （Marketo）	alex@foo.com	Marketo アカウント
foo.net	なし（防御ドメイン）	IT@foo.com	
fuuu.com	なし（防御ドメイン）	IT@foo.com	

上記のように、組織内のさまざまな部門が同じ送信者に複数のアカウントを使用している場合があります。送信者を複数のシステムタイプへの送信に使用している場合もあります。たとえば、SendGrid はメールサービスだけでなく、Freshdesk CRM サービスのメールインフラストラクチャも提供します。

拒否への移行

ドメインからの電子メールを認証するために必要な各ステップを繰り返し実行することになりますが、その際、Cisco Domain Protection のツールとレポートを使用して、進捗状況を整理して追跡できます。

- 「電子メールトラフィックの確認」 次のページ）
- 「ドメインステータスの確認」 ページ 100

こうしたツールとレポートを使用することにより、認証に十分な自信を持つことができるようになります。それにより、ドメインにさらに厳格なポリシーを適用できます。

拒否ポリシーに移行する前にデータを解釈するための支援が必要な場合は、Cisco カスタマーサポートにレビューを依頼してください。

Cisco の推奨事項は次のとおりです。

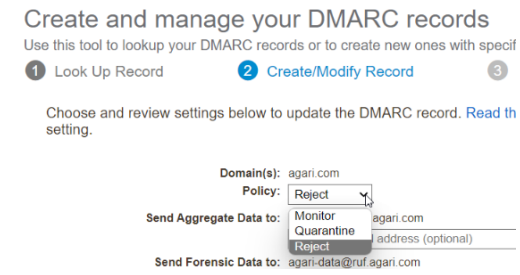
1. すべてのビジネスオーナーから承認を得る。

   強制ポリシーを有効にする前に、ドメインのすべての社内ビジネスオーナーに伝達済みであることを確認してください。単一のドメイン、送信者、ISP 受信者などからの配信に何か問題があれば、前述のレポートに記録されるため、問題を先取りできるはずです。

   「「すべての送信者の追跡」（前のページ）」で作成した問い合わせ先のリストを使用してください。

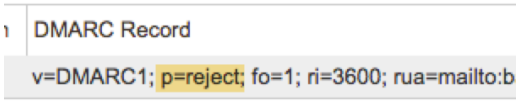
2. 選択したドメインの DMARC レコードを拒否ポリシーに移行させる。

ポリシーを更新して公開するプロセスは、「「DMARC Builder による DMARC レコードの作成」 ページ 73」で使用したプロセスと同じです。ただし、これまでに可視化を実現できたので、ポリシーを [拒否（Reject）] に設定できます。



DMARC ポリシーの [拒否（Reject）] への変更

変更されたポリシーには、p=Reject 表記が含まれます。



おめでとうございます。

このガイドを使用すると、組織内の 1 つまたは複数のドメインに関して強制（p=Reject）ポリシーを実装する手順を正常に管理できます。

DMARC により、ブランドをスプーフィングから自信を持って保護し、顧客の信頼を確保することができます。

電子メールトラフィックの確認

Cisco Domain Protection の電子メールトラフィックレポートは、いつ拒否に移行する準備ができるかを評価する場合に使用する一連のツールです。これらの各レポートは、DMARC の集計データとフォレンジック データからの貴重な洞察を提供します。これらは、Cisco Domain Protection ソリューションの有用性の象徴です。ほとんどのレポートには複数の「ドリル ダウン」ビューがあり、特定のメールのフローやエリアを詳しく調べて対処することができます。

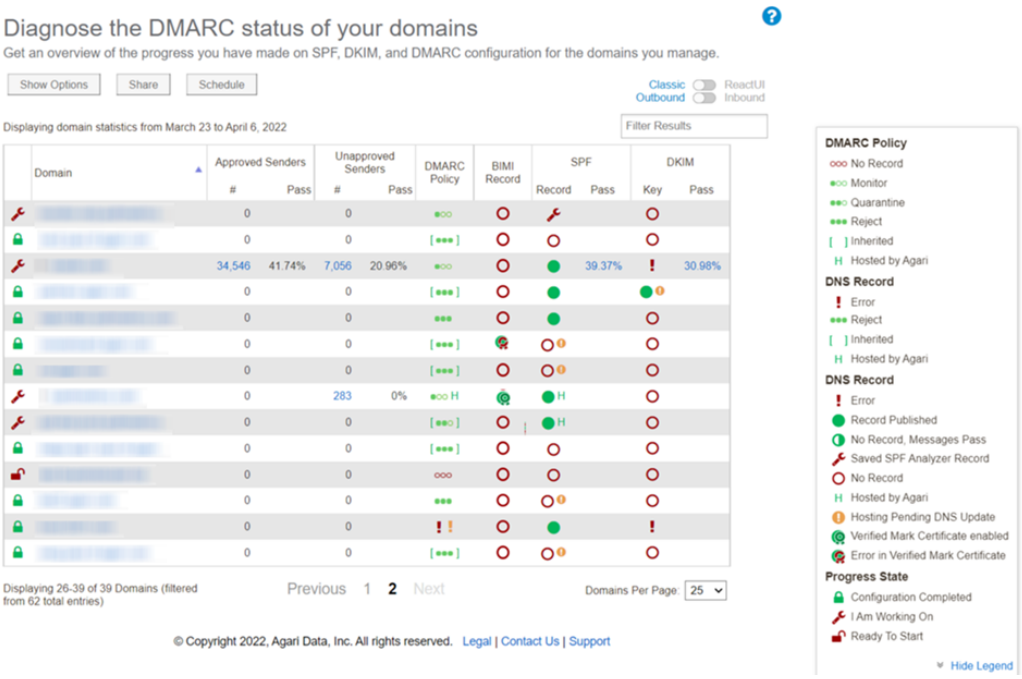
次の操作を実行できます。

- 任意のレポートのビューを設定します。詳細については、「「電子メールトラフィックレポートの設定」 ページ 120」を参照してください。
- 任意の列ヘッダーをクリックしてレポートビューを並べ替えます。
- グラフビューをフィルタ処理します。そのためには、グラフキー内の任意の項目をクリックして、ビューでその項目を有効または無効にします。
- レポートを共有およびスケジュールします。詳細については、「「電子メールトラフィックレポートの共有」 ページ 121」と「「電子メールトラフィックレポートのスケジュール」 ページ 121」を参照してください。

表示できるすべての電子メールトラフィックレポートについては、「「電子メールトラフィックレポート」 ページ 116」を参照してください。

ドメインステータスの確認

[診断ドメイン（Diagnostics Domains）] ページでは、管理しているすべてのドメインのステータスの概要を確認できます。



ドメインステータスの概要のルックアップ。

ドメインステータス	説明
[ドメイン（Domain）]	組織で管理しているドメインのリスト。
[承認済みの送信者（Approved Senders）]	組織によって承認されている送信者を発信元とする電子メールメッセージの数を表示します。「「送信者」 ページ 88」を参照してください。
[未承認の送信者（Unapproved Senders）]	組織によって承認されていない送信者を発信元とする電子メールメッセージの数を表示します。「「送信者」 ページ 88」を参照してください。
[承認済み/未承認の送信者 - 合格およびSPF/DKIM – 合格（Approved / Unapproved Senders – Pass & SPF / DKIM – Pass）]	選択したドメインの SPF と DKIM に合格した電子メールの割合を表示します。
[DMARCポリシー（DMARC Policy）]	ドメインの DMARC レコードステータスを示します。DMARC レコードステータスは次のとおりです。 • ! 赤い感嘆符は、DMARC レコードにエラーがあることを示します。 • ! オレンジ色の感嘆符は、一貫性のない DMARC レコードに問題があり、複数のレコードが公開されている可能性があることを示します。[DMARCポリシー（DMARC Policy）] をクリックすると、エラーの内容と最後にエラーが発生した時間が表示されます。 • ○○○ DMARC レコードが見つかりません。

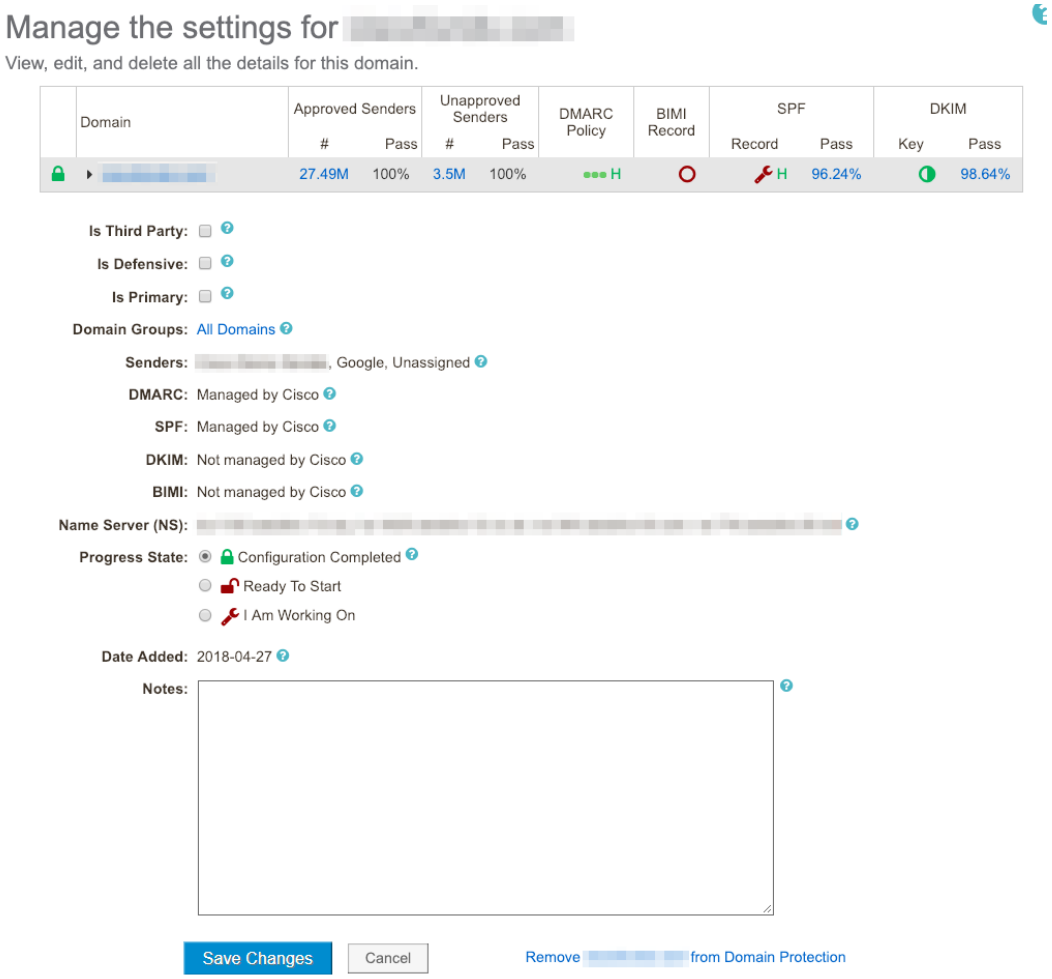
ドメインステータス	説明
	• [ ] DMARC ポリシーが親ドメインから継承されています。 • DMARC ポリシーが 、なし（[モニター（Monitor）]）に設定されています。 • DMARC ポリシーが [拒否（Reject）] に設定されています。 • DMARC ポリシーが [検疫（Quarantine）] に設定されています。 • 保留中の DNS 更新をホストしている DMARC レコードを示します。 • H DMARC は Cisco によってホストされています。
[BIMIレコード（BIMI Record）]	ドメインの BIMI レコードステータスを示します。BIMI レコードステータスは次のとおりです。 • 有効な BIMI レコードを示します。 • BIMI レコードが見つからないことを示します。 • ! 赤い感嘆符は、BIMI レコードにエラーがあることを示します。 • BIMI にリンクされている**検証済みマーク証明書**（VMC）が有効で使用可能であることを示します。 • 有効な BIMI にリンクされている**検証済みマーク証明書**（VMC）にエラーがあることを示します。 • 保留中の DNS 更新をホストしている BIMI レコードを示します。 • H BIMI が Cisco によってホストされています。
[SPFレコード（SPF Record）]	ドメインの SPF レコードステータスを示します。SPF レコードステータスは次のとおりです。 • 有効な SPF レコードを示します。 • SPF レコードが見つかりません。 • ! 赤い感嘆符は、SPF レコードにエラーがあることを示します。 • 保存済みまたは進行中の SPF レコードが SPF Analyzer によって作成されたことを示します。 • SPF Analyzer によって作成された SPF レコードは、Cisco によってホストされません。 • 保留中の DNS 更新をホストしている SPF レコードを示します。 • H SPF が Cisco によってホストされています。

ドメインステータス	説明
[DKIMキー（DKIM Keys）]	ドメインの DKIM レコードステータスを示します。DKIM レコードステータスは次のとおりです。 • 有効な DKIM レコードを示し、すべての DKIM キーが適切に設定されています。 • DKIM キーが見つかりません。 • DKIM キーに重大なエラーがあります。 • 保留中の DNS 更新をホストしている DKIM レコードを示します。 • DKIM が Cisco によってホストされています。

レコードをすばやくプレビューするには、DMARC、DKIM、BIMI、SPF のいずれかのステータスアイコンをクリックします。プレビューページで [レコードの詳細を表示（View Record Details）] をクリックして、選択したレコードの詳細ページを開きます。

ドメインの詳細ビュー

ドメインをクリックして、各ドメインとそのステータスの詳細を表示します。



ドメインの詳細ページ。

[ドメインの詳細(Domain Details)]には、組織に登録されているドメインのデータと特性の概要が示されます。一部の特性を編集したり、ドメインに関するメモを保存したりすることもできます。

ドメインの設定	説明
[サードパーティか(Is Third Party)]	このドメインは、サードパーティ送信者がユーザーに代わって電子メールを送信するために使用していますか。ドメインは、サードパーティが排他的に使用することもできますし、サードパーティトラフィックを混在させることもできます。Cisco がサードパーティ送信者を自動的に検出している場合は、このチェックボックスがすでにオンになっています。
[防衛か(Is Defensive)]	防御ドメインとは、登録されているものの、正規の電子メールの送信には使用されていないドメインです。Cisco では、悪用を防ぐために、防御ドメインを DMARC 拒否ポリシーで保護することを推奨しています。Cisco が防御ドメインであることを自動的に検出している場合は、このチェックボックスがすでにオンになっています。防御ドメインは、Defensive Domains システム グループに追加されます。
[プライマリか(Is Primary)]	プライマリドメインは、プロジェクトにとって優先度が高いと見なしたドメインです。プライマリドメインラベルの上位候補には、大量の電子メール、ブランド自体として使用されるもの、最初に注目したいドメインなどがあります。
[ブランドマーク識別子(Brand Mark Identifier)]	BIMI を使用していて、ブランドマーク識別子ファイルを保持している場合は、そのファイルを表示します。そうでない場合、このフィールドは非表示になります。

ドメインの設定	説明
[ドメイングループ（Domain Groups）]	このドメインが属しているドメイングループのリスト。
[送信者（Senders）]	最近このドメインでアクティビティを行った送信者のリスト。
[DMARC]	このドメインの DMARC レコード ホスティング ステータスを示します。DMARC レコードは、DNS インフラストラクチャ内でのみホストすることも、Cisco の DNS サーバーによってホストすることもできます。Cisco 側にあるこのドメインの DNS サーバーを自社 DNS サーバーの CNAME エントリで指定していれば、その DMARC レコードは Cisco でホストされていると見なされます。詳細については、「「Cisco での DMARC レコードのホスティング」 ページ 76」を参照してください。
[SPF]	このドメインの DMARC レコード ホスティング ステータスを示します。SPF レコードは、DNS インフラストラクチャ内でのみ管理することも、Cisco によってホストすることもできます。このドメインの公開された SPF レコードに「espf.cisco.com」を参照するインクルードが含まれている場合、ドメインの SPF レコードは Cisco でホストされていると見なされます。詳細については、「「ホストされた SPF」 ページ 46」を参照してください。
[DKIM]	このドメインの DKIM レコード ホスティング ステータスを示します。DKIM レコードは、DNS インフラストラクチャ内でのみ管理することも、Cisco によってホストすることもできます。すべてが「hosted-dkim.cisco.com」のサブドメインを指す NS レコードを公開すると、ドメインの DKIM レコードは Cisco でホストされていると見なされます。詳細については、「「Cisco での DKIM レコードのホスティング」 ページ 65」を参照してください。
[BIMI]	このドメインの BIMI レコード ホスティング ステータスを示します。BIMI レコードは、DNS インフラストラクチャ内でのみ管理することも、Cisco によってホストすることもできます。すべてが「hosted-bimi.cisco.com」のサブドメインを指す NS レコードを公開すると、ドメインの BIMI レコードは Cisco でホストされていると見なされます。詳細については、「「Cisco での BIMI レコードのホスティング」 ページ 114」を参照してください。
[ネームサーバ（NS）（Name Server（NS））]	ドメインの DNS レコードをホストするサーバ。

<table>
<tr><th>ドメインの設定</th><th>説明</th></tr>
<tr><td>[進捗状況（Progress State）]</td><td>ドメインの進捗状況は、現在作業中のドメイン、作業が完了したドメイン、および注意が必要なドメインを継続的に追跡するために役立ちます。ドメイン名の横にある星印をクリックすると、ドメインを [作業中（I Am Working On）]、[設定完了（Configuration Completed）]、または [開始可能（Ready To Start）] に設定できます。

進捗状況を使用すると、[ステータス（Status）] > [保護（Protection）] ページにある全体的な進行状況の [ドメイン進捗状況メーター（Domain Progress Meter）] の状態に影響します。

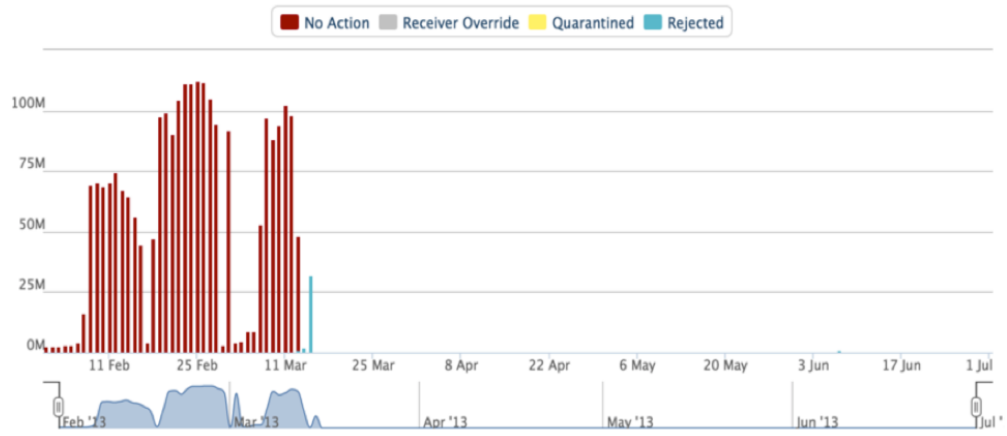
<table><tr><td>[設定完了（Configuration Completed）]</td><td>ドメインが完全に保護されており、Cisco が残りの問題を検出しなかった場合、Cisco によって自動的に [設定完了（Configuration Completed）] とマークされます。また、ドメインを保護するために予定されている作業がない場合は、ドメインを [設定完了（Configuration Completed）] とマークすることができます。ドメインを手動で [設定完了（Configuration Completed）] とマークする場合、ユーザーは、ドメインに解決の必要がない（または解決する意思のない）未解決の問題があることを認識しています。</td></tr><tr><td>[作業中（I Am Working On）]</td><td>このドメインを完全に保護された状態にするために、問題を解決する作業を行っている場合は、ドメインを [作業中（I Am Working On）] とマークします。たとえば、SPF レコードを更新するために、または DMARC ポリシーを拒否ポリシーに、DNS 変更要求を送信しており、変更が有効になるのを待っている場合などです。</td></tr><tr><td>[開始可能（Ready To Start）]</td><td>ほとんどのドメインは、この状態で開始されます。ドメインを完全に保護するために実行することを Cisco が推奨しているアクションがあります。ドメインの進捗状況を手動で変更することにより、そのドメインを [作業中（I Am Working On）] または [設定完了（Configuration Completed）] から [開始可能（Ready To Start）] に戻すことができます。</td></tr></table></td></tr>
<tr><td>[追加日（Date Added）]</td><td>ドメインが Cisco で承認され、組織に追加された日付。</td></tr>
<tr><td>[注記（Notes）]</td><td>自由形式のテキスト フィールドで、ドメインに関するメモを保存できます。単に、新しいテキストを追加または補足するか、関連性がなくなった既存のテキストを削除してください。</td></tr>
</table>

第 6 章

DMARC のモニタリング

拒否ポリシーを使用して 1 つ以上のドメインを有効にしたら、認証作業の利点の確認を開始する必要があります。

たとえば、この Cisco のお客様に関する [DMARCの傾向（What does my DMARC trend look like?）] レポートには、「ドメインを拒否ポリシーに移行した後に、スパム送信者が単に移動して、ドメインのスプーフィングの試みを止めた」ことが記録されています。



拒否ポリシーへの移行の利点

拒否へと移行すると、ドメイン保護は移行先で必要になる情報を引き続き提供します。これは重要なことです。電子メールインフラストラクチャが静的になることはなく、今後進化していくからです。[ステータス（Status）] メニューに用意されているページでは、次のような数多くの情報が得られます。

- 保護ステータス
- 脅威の状態
- 最新のアラート
- エグゼクティブ概要

ドメイン保護に用意されている数多くのツールでは、電子メールトラフィックに関するレポートやシステムの変更に関するアラートなど、電子メールインフラストラクチャに関する情報が得られます。これらの機能の詳細については、「「電子メールトラフィックレポート」 ページ 116」と「「アラート」 ページ 129」を参照してください。

次のステップ...

このガイドでは、組織に DMARC ポリシーを実装し、DMARC の実装後にモニタリングを開始する場合の基本事項について説明します。

次のようなドメイン保護の高度な機能の詳細については、Cisco サポートにお問い合わせください。

- ブランドなりすましの検出：特定のブランド識別文字列が DMARC 不合格メッセージに表示されるたびにアラートが生成されます。
- 脅威フィード：Cisco の脅威フィードをユーザーのテイクダウンベンダーと組み合わせて使用して、悪意のあるなりすましに迅速に対応する方法を学習します。
- API アクセス：他のセキュリティツールと連携するために、アプリケーション プログラミング インターフェイス（API）からドメイン保護の情報にアクセスします。
- SSO アクセス：シングルサインオン（SSO）機能からドメイン保護へのログインを有効にします。

第 7 章

エグゼクティブ概要

Cisco Domain Protection では、エグゼクティブ ダッシュボード ページから広範なレポートを利用できます。ダッシュボードには、次のレポートが含まれています。

- 停止された脅威：拒否または隔離された不審なメッセージの総数。
- 認証されたメッセージ：配信されたメッセージのうち認証に合格したメッセージの合計パーセンテージ。
- 保護されたドメイン：DMARC ポリシーに reject と定義されて保護されているドメインの数と、DMARC ポリシーに quarantine、monitor と定義されているドメインの数、または DMARC ポリシーがないドメインの数の比較。
- ポートフォリオ複雑性レポート：選択したドメイングループ（デフォルトは [アクティブなドメイン（Active Domains）]）と一致する、選択した期間のドメインの総数。比較のために、ユーザーの地域と業界のすべての顧客の平均が含まれています。
- 信頼スコア：電子メールがどの程度保護されているかを表すインデックス。スコアが 100 点満点であれば、送信したすべての電子メールが DMARC の reject ポリシーで保護されたことになります。比較のために業界の信頼スコアが表示されます。これは、ユーザーの業界と地域に属するすべての顧客の信頼スコアを平均したものです。
- DMARC メッセージ認証：指定された期間の DMARC の合格率と不合格率。比較のために、ユーザーの業界と地域のすべての顧客の平均が含まれています。
- 顧客保護率：正常に停止した不審なメッセージの割合。保護されていないドメインが攻撃されて、こうしたメッセージが配信されようになると、この比率は低下します。ドメインが保護されて、攻撃がブロックされるようになると、この比率は上昇します。比較のために、ユーザーの業界と地域のすべての顧客の平均が含まれています。
- ドメイン DMARC ポリシー、トレンド：ユーザーの組織全体で DMARC ポリシーの設定がどのくらい進行しているかを示す、指定された期間の月次ビュー。
- 高価値ドメイン：ボリュームが最も多く、最も保護されているドメイン。

このページでは、すべてのレポートの期間を選択できます。次から選択します。

- 3 ヵ月
- 6 ヵ月
- カスタム（開始日と終了日を選択します）

レポートの集約データには、現在の日付のデータや、組織からデータを蓄積し始めた日付よりも前のデータは含まれません。データは次のようにチャートに表示されます。

- 期間が 3 ヵ月および 6 ヵ月の場合、各データポイントは 1 ヵ月分のデータ。
- カスタムの場合、各データポイントは 1 ヵ月分のデータになり、最大 18 ヵ月前まで選択できます。開始日を組織でレポートデータの蓄積が始まった日付よりも前の日付に設定すると、各チャートの最上部に「…以降

（Since...）」と表示され、チャートのデータの最も早い日付が示されます。タブやページから離れてもリセットされず、ログアウトしたときにのみリセットされるという点では、カスタム日付範囲も「固定」です。

業界平均は、毎週日曜日の開始時（UTC 時間）に計算されます。このため、月の初日から最初の日曜日までは、エグゼクティブ ダッシュボードに業界平均が表示されません。

また、電子メールトラフィックレポートの場合と同様の方法で、このレポートページを共有して送信をスケジュールすることもできます。詳細については、「「電子メールトラフィックレポートの共有」 ページ 121」と「「電子メールトラフィックレポートのスケジュール」 ページ 121」を参照してください。

エグゼクティブ概要レポートの設定

1. [ステータス（Status）] > [エグゼクティブ概要（Executive Overview）] に移動します。
2. ドロップダウンメニューから [ドメイングループ（Domain Group）] を選択します。[アクティブなドメイン（Active Domains）] がデフォルトのシステムドメイングループです。また、作成したカスタムドメイングループ（[DMARCなし（No DMARC）] など）を選択することもできます。
3. [送信（Submit）] をクリックします。

この設定は、ページ上のすべてのレポートに適用されます。

第 8 章

ブランド インジケータ メッセージ識別

ブランド インジケータ メッセージ識別（BIMI）は、電子メールの受信者がユーザーエージェントに DMARC 認証メッセージとともにブランドロゴを表示できるようにするための新しい業界標準です。電子メールの受信者は、送信者のドメインが DMARC 検疫または拒否ポリシーを実装している場合にのみ、送信者の BIMI ブランドロゴを表示できます。その狙いは、ブランド認知を DMARC 認証と関連付けることです。

DMARC（および SPF と DKIM）と同じく、BIMI 指示はドメインの DNS レコードに追加されます。ドメイン保護では、ワークフローに検証機能が用意されているため、1 つ以上のドメインに対して BIMI 指示を簡単に作成できます。Cisco が BIMI レコードをホストしている場合でも、ドメイン保護はロゴの表示を自動的に管理します。

ブランド インジケータ メッセージ識別に関する RFC は現在（2019 年半ば）、IETF（Internet Engineering Task Force）でドラフト状態にあり、https://datatracker.ietf.org/doc/draft-blank-ietf-bimi/ で読むことができます。ドラフトとはいえ、精緻かつ具体的な内容になっていて、すでに導入が進んでいます。このドラフトでは、BIMI メカニズムを次のように規定しています。

> ドメイン所有者は、DNS 経由でドメインのブランド インジケータ アサーションを公開します。
>
> 次に、電子メールの受信者がメッセージを受信すると、以下のように処理します。
>
> a. 受信者は、DMARC のほか、内部のレピュテーション インデックスや自分で適用したいその他の独自の認証メカニズムを使用して、メッセージを認証します。
> b. 受信者は、対応する BIMI レコードと、インジケータ検証の証明を DNS に照会します。
> c. 電子メールとロゴの両方が認証されたら、受信者はメッセージにヘッダーを追加します。MUA（メールユーザーエージェント）は、このヘッダーを使用して、ドメイン所有者が推奨するブランドインジケータを判別できます。
>
> MUA は、自身のポリシーとユーザーインターフェイスに基づいて、必要に応じてブランドインジケータを取得して表示します。

インジケータ検証の証明は、マーク検証済み証明書によって提供されます。

BIMI レコードのシンタックス

BIMI レコード（アサーションレコード）は、_bimi という名前でサブドメインに存在する DNS TXT レコードであり、DNS ベースのキーレコードの tag-value シンタックスに従います。BIMI レコードは、次のタグで構成されます。

タグ	説明	値	注記
v=	バージョン。	BIMI1	このタグは必須です。このバージョンの BIMI と互換性がある実装にするには、値を BIMI1 にする必要があります。このタグの値は、正確に一致する必要があります。値が一致しない場合や存在しない場合は、取得されたレコード全体を無視する必要があります。リストの最初のタグである必要があ

タグ	説明	値	注記
			ります。
a=	BIMI 信頼機関。	• self • cert • mva	これらのオプションは、まだ使用できません。a= タグは、空白のままにする（a= とする）か含めないようにする必要があります。 このタグはオプションで、3 つの値のいずれかを取ります。その値を次に示します。 • self：検証オプションなし（タグを省略した場合と同じ）。 • cert：マーク検証済み証明書を指す https URL であり、この URL を使用してインジケータを検証できます。 • mva：API エンドポイントを指す https URL であり、ここから検証情報を照会できます。
l=	画像リソースへの URL。	http URL	このタグは必須ですが、その値は空でもかまいません。タグは小文字の「L」です。画像リソースは、SVG（スケーラブル ベクター グラフィックス）ファイルにする必要があります。プロトコルは https である必要があります。 グラフィックファイルは以下に準拠する必要があります。 • 正方形 • SVG • 白/透明の背景 • ロゴ/マークを空間の中央にできるだけ大きく配置する • テキストではなくアイコン

BIMI レコードの例：

v=BIMI1; a=; l=https://www.mycompany.com/bimi/brandlogo.svg;

BIMI レコードを使用して、拒否を示すことができます。推奨事項は次のとおりです。

> 「a」タグと「l」タグの両方が空の場合、BIMI への参加を明示的に拒否したことになります。これは、そもそも BIMI レコードを公開しないのとは大きく異なります。たとえば、組織のドメインでデフォルトのインジケータを使用できる場合には、サブドメインの参加を拒否できます。また、公開を拒否したセレクタを使用してメッセージが送信された場合、メッセージにインジケータが表示されません。他のセレクタを使用したメッセージであれば、正常に表示されます。
>
> 公開を明示的に拒否する場合は、次のようになります。
>
> v=BIMI1; a=; l=;

BIMI レコードのシンタックスは厳密で、大文字と小文字も区別されます。電子メールの受信者は、BIMI レコードでシンタックスエラーや大文字小文字のエラーが発生しても修正できません。必須のタグがない場合はエラーになります。v= タグで始まらないレコードや、現在の BIMI バージョンを識別しない v= タグで始まるレコードは、破棄する必要があります。

BIMI 実装

BIMI DNS レコードの形成方法に関する推奨事項は厳格ですが、BIMI の実装方法に関しては柔軟性があります。ドメイン所有者は受信者にブランドインジケータを表示してほしいと頼むことができますが、実際に表示するかどうかは受信者が選択できます。また、受信者は代替のインジケータを表示することもできます。推奨事項は次のとおりです。

ドメイン所有者は、1 つ以上のドメインで BIMI に参加することをアドバタイズする場合、そのドメインに DNS TXT レコードを追加します。その際、ドメイン所有者は自身のいずれかのドメインからのものとするメッセージを送信して、表示してほしいインジケータを MUA に具体的にリクエストします。

ドメイン所有者は、BIMI に参加しないことを選択することもできます。この場合、ドメイン所有者が行うのは、BIMI アサーションレコードを一切公開しないようにして、参加のアドバタイズを拒否することだけです。

BIMI メカニズムを実装している MUA は、ドメイン所有者が公開した BIMI ポリシーに準拠するよう最善の努力を尽くします。ただし、MUA はエンドユーザーに公開されるユーザーインターフェイスを最終的に制御できます。また、BIMI アサーションレコードに指定されているもの以外の代替インジケータを使用することも、インジケータをまったく使用しないこともできます。

BIMI レコードは、セカンドレベルドメインの直下にある default._bimi という名前のゾーンに公開する必要があります。たとえば、目的のセカンドレベルドメインが foo.com である場合、そのドメインの BIMI TXT レコードは default._bimi.foo.com に公開されます。

BIMI レコードの作成

ドメイン保護で管理しているドメイン（およびサブドメイン）に対してのみドメイン保護で BIMI レコードを作成できます。ドメイン保護で管理しているドメインを確認するには、[設定（Configure）] > [ドメインの管理（Manage Domains）] に移動し、[すべてのドメイン（All Domains）] をクリックします。

前提条件

- SVG（スケーラブル ベクター グラフィックス）形式のブランドロゴファイルが安全な（https）URL からアクセス可能な場所にあること。
- 上記への URL。

1. [ツール（Tools）] > [BIMI] に移動します。
2. ドメイン保護で管理しているドメインまたはサブドメインを入力します。
3. [検索（Look Up）] をクリックします。
4. [新しいBIMIレコードの作成（Create New BIMI Record）] をクリックします。
5. [ブランドマーク識別子（Brand Mark Identifier）] の値を入力します。これはリソースへの完全修飾 https URL であり、SVG（スケーラブル ベクター グラフィックス）ファイルにする必要があります。次に、[適用（Apply）] をクリックします。
6. 必要に応じて [BIMI証明書（BIMI Certificate）] の値を入力します。これは、検証のために照会できる証明書または API への完全修飾 https URL です。次に、[適用（Apply）] をクリックします。

7. [続行（Continue）] をクリックします。
8. [指示の作成（Create Instructions）] をクリックします。

拡張子が .txt のテキストファイルがコンピュータにダウンロードされます。保存場所は、ブラウザに設定したデフォルトのファイルダウンロード場所によって異なります。このファイルには、どのような DNS レコードをドメインに追加すればよいかを記載した指示と、コピーして貼り付けることができる BIMI に最適な TXT レコードが含まれます。

BIMI レコードの編集

BIMI レコードに使用するグラフィックリソース（スケーラブル ベクター グラフィックス（SVG）ファイルにする必要があります）と、BIMI 信頼機関への URL を変更できます。これらの値の詳細については、「「ブランド インジケータ メッセージ識別」 ページ 110」を参照してください。

1. [ツール（Tools）] > [BIMI] に移動します。
2. ドメイン保護で管理し、BIMI レコードがあるドメインまたはサブドメインを入力します。
3. [検索（Look Up）] をクリックします。
4. [BIMIレコードの変更（Modify BIMI Record）] をクリックします。
5. 必要な変更を加えます。
    - [ブランドマーク識別子（Brand Mark Identifier）] フィールドに、SVG グラフィックリソースへの完全修飾 URL を入力し、[適用（Apply）] をクリックします。
    - [BIMI証明書（BIMI Certificate）] フィールドに、必要に応じて証明書または API エンドポイントへの https URL を入力し、[適用（Apply）] をクリックします。
    - 値を削除するには、このフィールドを空白のままにし、[適用（Apply）] をクリックします。
6. [続行（Continue）] をクリックします。
7. [指示の作成（Create Instructions）] をクリックします。

拡張子が .txt のテキストファイルがコンピュータにダウンロードされます。保存場所は、ブラウザに設定したデフォルトのファイルダウンロード場所によって異なります。このファイルには、どのような DNS レコードをドメインに追加すればよいかを記載した指示と、コピーして貼り付けることができる BIMI に最適な最新の TXT レコードが含まれます。

ブランドマーク識別子のプレビュー

BIMI レコードを公開したら、ドメイン保護内からブランドマーク識別子が一部の電子メールクライアントでどのように見えるかをプレビューできます。

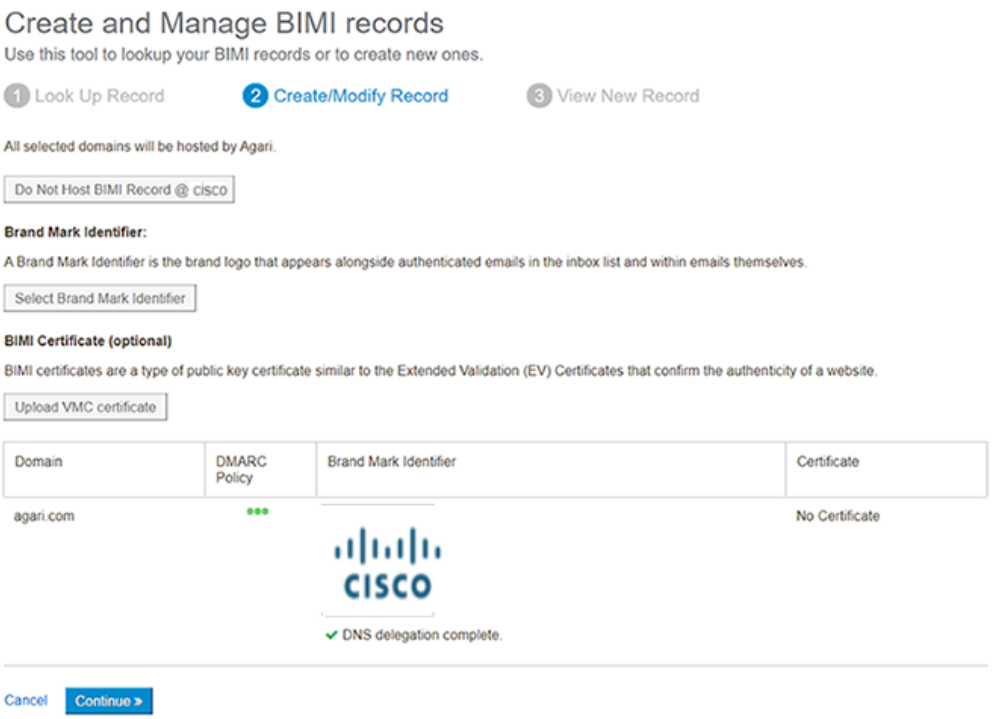
1. [ツール（Tools）] > [BIMI] に移動します。
2. ドメイン保護で管理しているドメインまたはサブドメインを入力します。
3. [検索（Look Up）] をクリックします。
4. [BIMIレコード（BIMI Record）] 列で、BIMI グラフィックをクリックします。

Cisco での BIMI レコードのホスティング

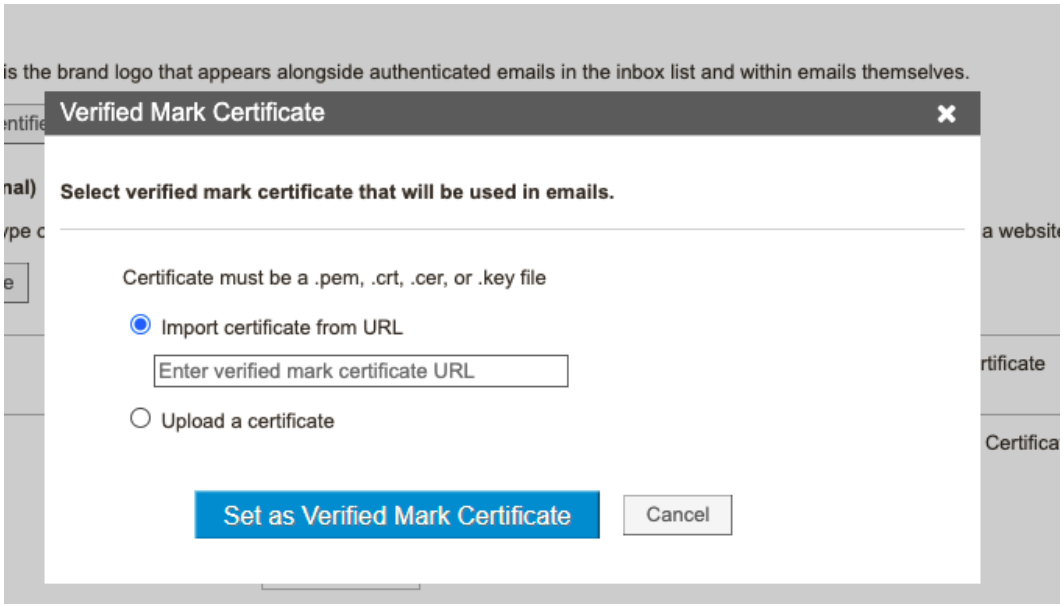
BIMI（ブランド インジケータ メッセージ識別）レコードを Cisco にホストした場合、ドメイン保護で BIMI レコードに影響を与える変更を加えたときに、レコードが迅速、安全、かつ自動的に更新されます。

Cisco にいつでもドメインの BIMI レコードをホストできますが、ドメインが DMARC 検疫または拒否にある場合を除き、電子メールの受信者は BIMI ブランドイメージを表示できません。

1. [ツール（Tools）] > [BIMI] に移動します。
2. ドメイン名を入力して、現在の BIMI レコードを表示するか、新しいレコードを作成します。
3. 結果の下にある [BIMIレコードの変更（Modify BIMI Record）] ボタンをクリックします。



4. [BIMI証明書（オプション）（BIMI Certificate（optional））] で、[VMC証明書をアップロード（Upload VMC certificate）] ボタンを選択します。新しいダイアログボックスが表示されます。

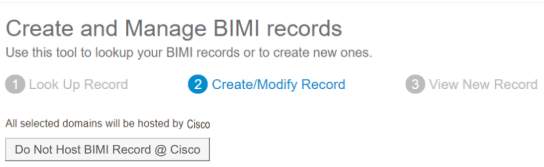


URL を入力して証明書をインポートしたり、証明書をファイルとしてアップロードしたりできます。

5. URL から証明書をインポートするには、フィールドに URL を入力します。
6. ファイルをアップロードするには、[証明書をアップロード(Upload a certificate)] を選択します。新しいダイアログボックスが開くので、コンピュータからファイルを選択するか、ファイルをドラッグアンドドロップしてアップロードできます。

Cisco での BIMI レコードのホスティングの停止

1. [ツール(Tools)] > [BIMI] に移動します。
2. ドメイン名を入力して、現在の BIMI レコードを表示するか、新しいレコードを作成します。
3. 結果の下にある [BIMIレコードを変更(Modify BIMI Record)] ボタンをクリックします。
4. [Cisco でBIMIレコードをホストしない(Do Not Host BIMI Record at Cisco)] をクリックします。



5. [続行(Continue)] をクリックします。
6. 次をクリックします。
   - Cisco で単一のドメインの BIMI レコードをホストする場合は、そのドメインの横にある [適用(Apply)] をクリックします。
   - Cisco ですべてのドメインの BIMI レコードをホストする場合は、[すべて適用(Apply All)] をクリックします。

第 9 章

送信メッセージのモニタリング

自分の代わりに電子メールを送信するすべてのドメインを reject に移行したら、ドメイン保護を使用して送信電子メールをモニターできます。ドメイン保護では、自分で明示的に送信したメッセージと自分の代わりに他者が送信した電子メールだけでなく、送信元が自分であると見なされたメッセージやそうでないと見なされたメッセージも可視化できます。そのため、ブランドを毀損しようとする攻撃を検出して対処できます。

電子メールトラフィックレポート

[電子メールトラフィックの分析（Analyze Email Traffic）] ページには、電子メール エコシステムに役立つビューを提供するための一般的な質問のリストがあります。各ビューは電子メールエコシステムに関する詳細なレポートであり、各レポートには情報のグラフとリストの両方が表示されます。

レポートを表示したときには、次のことができます。

- グラフのセクションにカーソルを合わせると、特定のデータを要約したポップアップが表示されます。
- グラフのセクションをクリックすると、そのデータサブセットでフィルタ処理されます。
- リスト内の任意のリンクをクリックすると、そのデータサブセットでフィルタ処理されます。
- 「電子メールトラフィックレポートの共有」 ページ 121
- 「電子メールトラフィックレポートのスケジュール」 ページ 121

使用可能なレポート

ドメイン保護には、発信電子メールトラフィックに関するさまざまなレポートが用意されています。

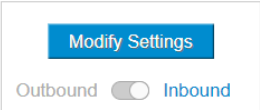
次の表は、表示できるレポートを示しています。レポートは 3 つのタイプに分類されます。

電子メールトラフィックレポートのリスト。

レポート名	着信
[全体像（The Big Picture）]	
[DMARCの傾向（What does my DMARC trend look like?）]	✅
[DMARC不合格のメッセージの処理方法（What's happening to messages failing DMARC?）]	✅
[SPFとDKIMでDMARCに合格しているメッセージ（What messages pass DMARC with SPF & DKIM?）]	✅
[電子メールの送信先のISP（Which ISPs do I send email to?）]	
[ドメインを使用する正当な電子メールの割合（How much email using my domains is	✅

レポート名	着信
legitimate?)]	
[修正可能なもの(Things I Can Fix)]	
[SPFの問題(What are my SPF problems?)]	✅
[DKIMの問題(What are my DKIM problems?)]	✅
[正当なメッセージの拒否(Are any legitimate messages being rejected?)]	✅
[把握していない正当なサブドメイン(What legitimate subdomains don't I know about?)]	✅
[スプーフィングの脅威(Who is Spoofing Me?)]	
[ブロックされたスプーフィング電子メール(How much spoofed email am I blocking?)]	✅
[スプーフィングに使用されているサブドメイン(What subdomains are being used to spoof me?)]	✅

[分析(Analyze)]>[電子メールトラフィック(Email Traffic)]ページには、発信電子メールトラフィックに関するレポートから着信電子メールトラフィックに関するレポートに切り替えるトグルがあります(デフォルト表示は[発信(Outbound)]です)。



各レポートのフィルタオプションを調整して、必要な情報を得るために役立てることができます。次の操作を実行できます。

- 1つのドメインまたはドメイン グループの各レポートをフィルタリングします。
- データ範囲をデフォルト値の2週間から増減させます。送信のトレンドとパターンがつかめるように日付範囲を90日といったもっと広い範囲に拡大することを推奨します(たとえば、四半期ごとに送信されるニュースレターのデータを表示する場合、期間が2週間というのは短すぎます)。
- メッセージ グループの細かさを変更します(毎日、毎週、または毎月)。
- 特定のレポートのメッセージ発信元を変更します。たとえば、一部のビューでは、特定のカテゴリのメッセージを含める(または除外する)と有意義である場合があります。

電子メールトラフィックレポートのビューをカスタマイズする方法の詳細については、「「電子メールトラフィックレポートの設定」ページ120」を参照してください。

ドメイン保護で電子メールトラフィックをモニターし始めたばかりであれば、まず次のレポートを確認すると、有用な情報を得ることができます。

DMARCの傾向(What does my DMARC trend look like?)

このレポートでは、メッセージのDMARC合格/不合格に関する一般的な傾向が示されます。すべてのドメインのすべての送信者からの認証が増えると、十分な量の電子メールがDMARCチェックに合格した時期を判断できます。これにより、自信を持って拒否ポリシーに移行できるようになります。

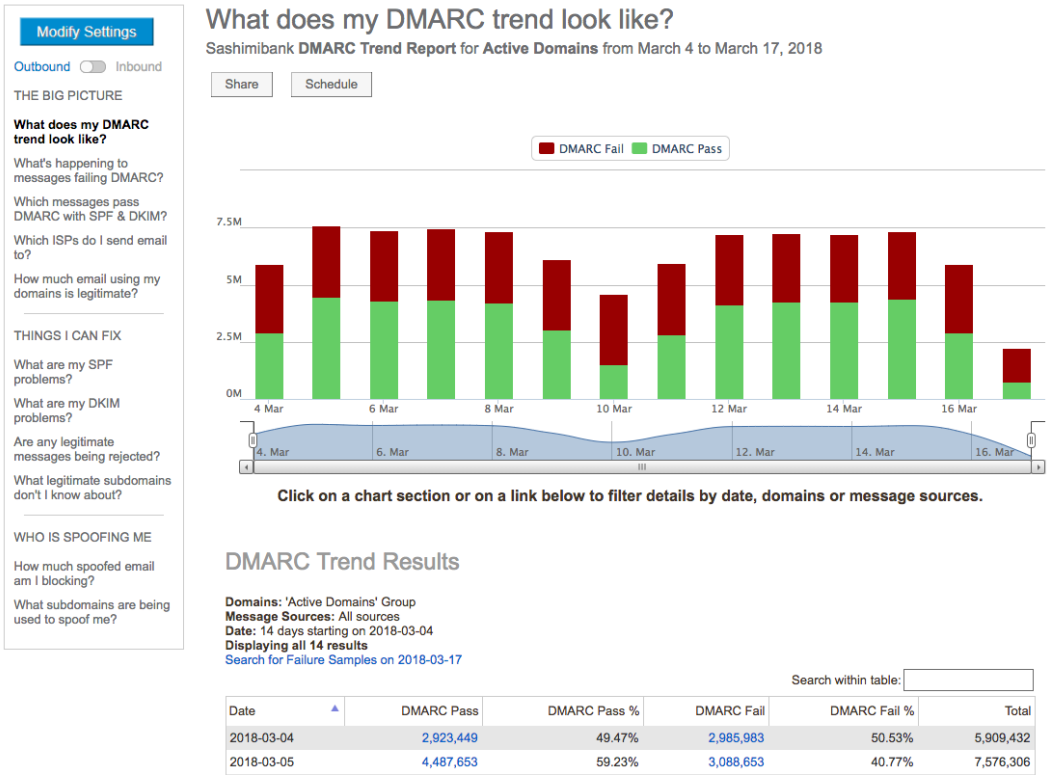
データのモニタリングの初期段階では、デフォルト表示である[DMARCの傾向(What does my DMARC trend look like?)]レポートが有用です。

この時点では、ドメイン保護へのデータを生成するドメインがわずかしかない場合があり、それらのドメインにどのような認証もない場合があります。

[DMARC合格(DMARC Pass)] 列または [DMARC不合格(DMARC Fail)] 列のいずれかのリンクをクリックして、特定のデータの詳細情報を確認します。

このビューで特定のドメインのリンクをクリックすると、選択した時間枠内で特定のドメインに代わって送信しているすべての IP アドレスのレポートが生成されます。

この表に示されている IP アドレスの [DMARC合格(DMARC Pass)] リンクをクリックすると、さらに詳細な情報を確認できます。



Active Domains グループの [DMARCの傾向(What does my DMARC trend look like?)] ビュー

DMARC不合格のメッセージの処理方法(What's happening to messages failing DMARC?)

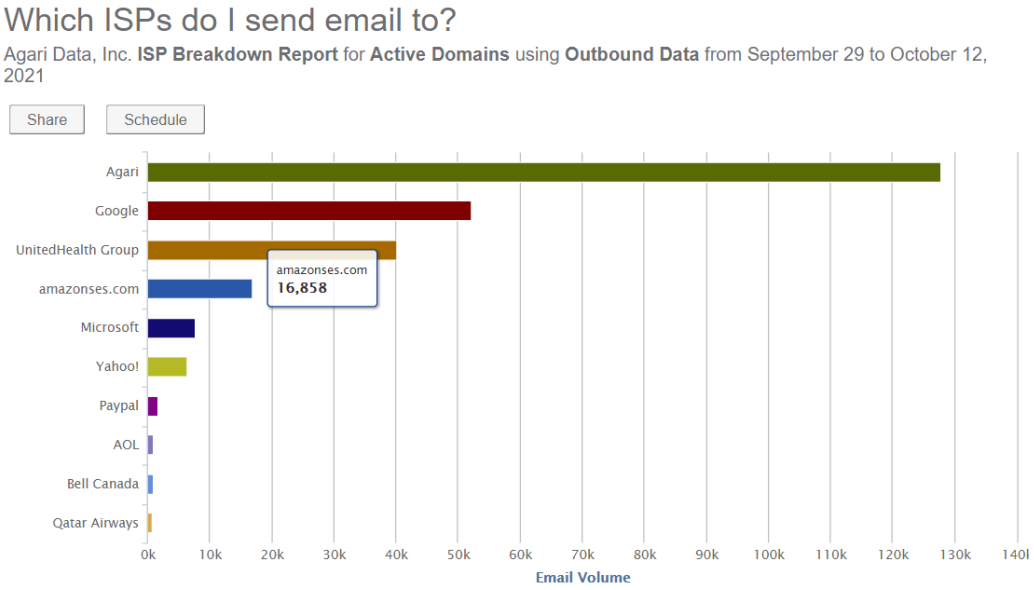
DMARC チェックに合格しなかったメッセージに関して、a)ポリシーと b)受信者のアクションに応じて、異なるアクションを実行できます。このビューを使用して、不合格のメッセージを調べ、さまざまな大規模受信者(Google、Yahoo、AOL、Microsoft など)がそれらをどのように処理しているのかを確認します。詳細を掘り下げ、不合格のメッセージをドメイン単位で調べることができます。

SPFとDKIMによってDMARCに合格しているメッセージ(Which messages pass DMARC with SPF & DKIM?)

逆に、このビューには、合格したメッセージ(DMARC に合格、SPF に合格、または両方に合格)がドメイン単位で示されます。このビューを使用して詳細を掘り下げ、認証チェックに関して各ドメインでどのようなアクションがとられたのかを確認できます。

電子メールの送信先のISP(Which ISPs do I send email to?)

このレポートには、特定の ISP によって報告されたすべてのメッセージが認証結果別に表示されます。



ドメインを使用する正当な電子メールの割合(How much email using my domains is legitimate?)

さらに別の回転式には、正当なメッセージと脅威メッセージの集約された量がドメイン単位で示されます。

正当なメッセージには、送信者インベントリ(つまり、承認済みの送信者リスト)内の IP アドレスから発信されたメッセージ(DMARC 認証の合格/不合格にかかわらず)が含まれます。DMARC 認証に合格した、送信者インベントリ外からのメッセージ(元の DKIM 署名を保持する自動転送メッセージなど)も含まれます。

脅威メッセージは、ユーザーの IP 空間外から発信され、DMARC 認証に合格しなかったメッセージです。

SPFの問題(What are my SPF problems?)、DKIMの問題(What are my DKIM problems?)

「「SPF の問題の特定」 ページ 42」と「「DKIM の問題の特定」 ページ 66」で説明しているように、これらのレポートを使用して、SPF および DKIM 認証の進捗状況やドメインに関する問題の詳細情報を掘り下げて調べることができます。

正当なメッセージの拒否(Are any legitimate messages being rejected?)

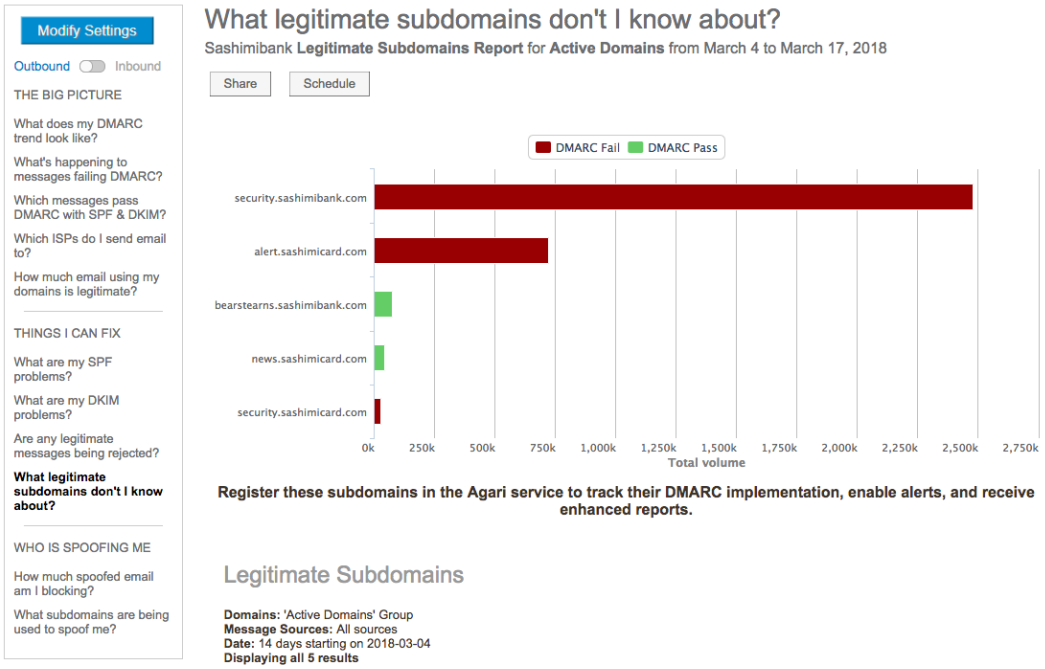
このレポートを使用して、DMARC ポリシーのために受信者で誤検出されたメッセージが拒否されているかどうかを判断します。

把握していない正当なサブドメイン(What Legitimate Subdomains Don't I Know About?)

このレポートを使用して、組織のメッセージを送信するために使用されているサブドメインを確認します。

このビューも、モニタリングの初期段階に有用なビューです。

このビューの結果により、電子メールの送信に使用されている可能性のあるプライマリドメインのサブドメインが明らかになる場合があります。



[把握していない正当なサブドメイン(What Legitimate Subdomains Don't I know about?)] ビュー。

このレポートの正当なサブドメインは、承認済みドメインについてのみレポートされます。

ブロックされたスプーフィング電子メール(How much spoofed email am I blocking?)

拒否ポリシーを実装すると、このレポートビューで強制ポリシーの利点を確認できます。

スプーフィングに使用されているサブドメイン(What subdomains are being used to spoof me?)

上記のサブドメインレポートと同様に、このビューを使用して、電子メールの送信を現在認可していないサブドメインを確認できます。DMARC 拒否ポリシーに移行する作業を行うために、ドメイン保護でサブドメインを防御ドメインとして登録します。

電子メールトラフィックレポートの設定

発信または着信電子メールトラフィックレポートを表示しているときには、必要な情報が得られるようにそのレポートを設定できます。

1. [電子メールトラフィックレポート(Email Traffic Reports)] ページ([分析(Analyze)] > [電子メールトラフィック(Email Traffic)])の左側の列で、レポートの名前をクリックし、[発信(Outbound)] または [着信(Inbound)] を選択します。
2. [設定を変更(Modify Settings)] をクリックします。
3. レポートに必要な変更を加えます。詳細については、「「電子メールトラフィックレポート設定」 ページ 122」を参照してください。

[デフォルトにリセット(Reset to Defaults)]をクリックして、カスタム設定を削除し、レポートをデフォルト設定に戻します。

4. [送信(Submit)]をクリックします。

電子メールトラフィックレポートの共有

[電子メールトラフィック(Email Traffic)]ページ([分析(Analyze)]>[電子メールトラフィック(Email Traffic)])で、任意のドメイン保護ユーザーとレポートを共有できます。

1. 左側の列で、共有するレポートの名前をクリックします。
2. 現在表示しているレポートと異なるレポートが必要な場合は、レポートを設定します。
    a. [設定を変更(Modify Settings)]をクリックします。
    b. レポート設定を変更します。詳細については、「「電子メールトラフィックレポート設定」見開きページ」を参照してください。
    c. [送信(Submit)]をクリックします。
3. [共有(Share)]をクリックします。
4. [宛先(To)]ドメイン保護フィールドで、レポートを受信するユーザーを選択します。
5. [含める(Include)]リストで、レポートに含める形式を選択します。デフォルトは、レポートへのリンクと、電子メールに添付される PDF(Adobe Acrobat)ファイルです。
6. 必要に応じて、自由形式のメモを追加します。
7. [メールの送信(Send Email)]をクリックします。

スケジュールされたすべてのレポートでは、レポートの作成時に、[レポート設定の変更(Modify Report Settings)]「電子メールトラフィックレポート設定」見開きページダイアログボックスで定義されている範囲が維持されることに注意してください。たとえば、ドメインの包括的な SPF レコードを作成するプロセスを進める際に、レポートの範囲を広げたバージョン(すべてのドメインのすべての送信者)を受け取ると同時に、レポートの範囲をビジネスオーナーに絞り込んだバージョンのレポート(1 つのドメインの 1 つの送信者)を定期的に送信できます。

電子メールトラフィックレポートのスケジュール

[電子メールトラフィック(Email Traffic)]ページ([分析(Analyze)]>[電子メールトラフィック(Email Traffic)])で、定義した間隔で任意のドメイン保護ユーザーにレポートを送信するようにスケジュールできます。

1. 左側の列で、共有するレポートの名前をクリックします。
2. 現在表示しているレポートと異なるレポートが必要な場合は、レポートを設定します。
    a. [設定を変更(Modify Settings)]をクリックします。
    b. レポート設定を変更します。詳細については、「「電子メールトラフィックレポート設定」見開きページ」を参照してください。
    c. [送信(Submit)]をクリックします。
3. [スケジュール(Schedule)]をクリックします。

4. [送信(Send)]フィールドで、レポートをいつ送信するかを選択します(レポートは現地時間の午前 0 時に送信されます)。次から選択してください。
    - [日次(Daily)]:レポートは毎日送信されます。
    - [週次(Weekly)]:レポートは選択した曜日に送信されます。デフォルトは月曜日です。
    - [月次(Monthly)]:レポートは、選択した月の日にちに送信されます。デフォルトは 1 日です。
5. [含める(Include)]リストで、レポートに含める形式を選択します。デフォルトは、電子メールに添付される PDF(Adobe Acrobat)ファイルです。
6. [宛先(To)]ドメイン保護フィールドで、レポートを受信するユーザーを選択します。デフォルトは、スケジュールされたレポートの作成者です。
7. [所有者(Owner)]フィールドで、レポート所有者で識別するドメイン保護ユーザーを選択します。デフォルトは、スケジュールされたレポートの作成者です。
8. 必要に応じて、レポートの [名前(Name)]を変更します。
9. [スケジュール(Schedule)]をクリックします。

スケジュールされたすべてのレポートでは、レポートの作成時に、[レポート設定の変更(Modify Report Settings)]「電子メールトラフィックレポート設定」下ダイアログボックスで定義されている範囲が維持されることに注意してください。たとえば、ドメインの包括的な SPF レコードを作成するプロセスを進める際に、レポートの範囲を広げたバージョン(すべてのドメインのすべての送信者)を受け取ると同時に、レポートの範囲をビジネスオーナーに絞り込んだバージョンのレポート(1 つのドメインの 1 つの送信者)を定期的に送信できます。

電子メールトラフィックレポート設定

このセクションでは、あらゆる種類の電子メールトラフィックレポートを表示するために定義できる設定について説明します。ビューを定義すると、電子メールトラフィックレポートを「電子メールトラフィックレポートの共有」(前のページ)または「電子メールトラフィックレポートのスケジュール」(前のページ)するときに使用できます。

設定	説明
[ドメインを選択(Select Domains)]	レポートに含めるドメインを決定します。次から選択してください。 • [ドメイングループ(Domain Group)](デフォルト)。システムドメイングループ(デフォルトはアクティブドメイン)またはカスタムドメイングループ(作成したドメイングループ)を選択します。 • [単一ドメイン(Single Domain)]。モニターするドメインのいずれかを選択します。
[メッセージを表示(View Messages from)]	レポートの期間を決定します。次から選択してください。 • [最新(Most Recent)](デフォルト)。過去何日分のレポートを生成するかを入力します(デフォルトは 14 日です)。 • [日付範囲(Date Range)]。開始日と終了日を選択します。 レポートの範囲を 428 日よりも長くすることはできません。つまり、[最新(Most Recent)]フィールドに 428 を超える数値は入力できません。また、[日付範囲(Date Range)] で 428 日より前の日付を選択することはできません。
[メッセージをグループ化(Message Grouping)]*	レポートデータをどのようにグループ化するかを定義します。日次(デフォルト)、週次(レポート範囲が 30 日以上の場合に使用可能)、または月次(レポート範囲が 90 日以上の場合に使用可能)にします。グループ化は、グラフとグラフに属する表の両方に適用されます。データをグループ化すると(またはグループ化しないと)、さまざまなレベルおよび粒度でレポート期間の

<table>
<tr><th>設定</th><th>説明</th></tr>
<tr><td></td><td>有益なインサイトを得ることができます。たとえば、年次レポートの場合、データを週次または月次のチャンクにグループ化すると、年間トレンドについて日次ビューよりも優れたビューを得ることができます。</td></tr>
<tr><td>[メッセージの発信元(Message Origin)]</td><td>レポート内のメッセージを複数の発信元特性でフィルタ処理できます。次から選択してください。
• [デフォルト(Default)](デフォルト):[カスタム(Custom)] 設定にデフォルトとして定義されるソース、フォワーダ、および IP アドレス/CIDR。
• [カスタム(Custom)]:次のカスタムフィルタのいずれかを選択します。
<table>
<tr><th>フィルタ</th><th>説明</th></tr>
<tr><td>[特定のソース(Specific Sources)](デフォルト)</td><td>レポートを特定のソースに限定します。次から選択してください。
• [すべてのソースから(From All Sources)](デフォルト):レポートには、すべてのメッセージが含まれます。
• [自分の送信者インベントリ内から(From Inside My Sender Inventory)]:レポートには、送信者インベントリ内のソースからのメッセージがすべて含まれるか(デフォルト)、送信者インベントリ内の送信者のリストに記載された単一の送信者からのメッセージが含まれます。
• [自分の送信者インベントリ外から(From Outside My Sender Inventory)]:レポートには、送信者インベントリ外のソースからのメッセージがすべて含まれるか(デフォルト)、送信者インベントリ外の送信者のリストに記載された単一の送信者からのメッセージが含まれます。
また、レポートから既知のフォワーダ IP アドレスを除外することもできます。</td></tr>
<tr><td>[既知のフォワーダ(Known Forwarders)]</td><td>レポートを既知のフォワーダ IP アドレスからのメッセージに限定します。</td></tr>
<tr><td>[特定のIP/CIDR範囲(Specific IP/CIDR Range)]</td><td>レポートを特定の IP アドレス、IP アドレス範囲、または CIDR からのメッセージに限定します。1 つまたは複数をカンマで区切って入力します。</td></tr>
</table>
</td></tr>
</table>

*[メッセージをグループ化(Message Grouping)] 設定は、以下のレポートにのみ使用できます。

- [DMARCの傾向(What does my DMARC trend look like?)]
- [DMARC不合格のメッセージの処理方法(What's happening to messages failing DMARC?)]
- [SPFとDKIMによってDMARCに合格しているメッセージ(Which messages pass DMARC with SPF & DKIM?)]
- [ドメインを使用する正当な電子メールの割合(How much email using my domains is legitimate?)]
- [正当なメッセージの拒否(Are any legitimate messages being rejected?)]
- [ブロックされたスプーフィング電子メール(How much spoofed email am I blocking?)]

脅威フィード

ドメイン保護の脅威フィードには、RUF データに基づくDMARC の失敗に関する詳細が表示されます。脅威フィード内の情報を使用すると、失敗サンプルで一連の脅威の攻撃と共通点を特定できます。

脅威フィードは、DMARC 失敗サンプルをリストにまとめたものです。各サンプルには、レポート環境に渡される特定の情報が含まれています。具体的には、いずれかのドメインから送信されたメッセージやいずれのドメインからも送信されなかったもののブランド識別子が含まれているメッセージのうち、DMARC に合格しなかったメッセージに関する情報です。

脅威フィードを使用して、次のことができます。

- フィルタを使用して、失敗サンプルから同じ IP アドレスや件名といった共通点を見つけて、一連の攻撃を特定できます。
- DMARC に失敗したメッセージ内の URL を特定できます。
- API エンドポイントを使用して、SIEM システムを電子メールデータと相互に関連付けられます。

[脅威フィード(Threat Feed)] ページのテーブルには、脅威フィード項目ごとに以下がリストされます。

- [カウント(Count)]:脅威フィードに URL が登場した回数。
- [URI]:メッセージ内の特定の URL。
- [Fromドメイン/電子メール送信元IP(From Domain/Email Source IP)]:From ヘッダー内のドメインと、そのドメインを表す IP アドレス。
- [件名(Subject)]:メッセージヘッダーに含まれる件名。
- [最終報告日(Last Reported)]:脅威が最後に報告された日付と時刻。
- [検出元(Detected By)]:脅威の検出方法。[検出元を含める:フィード電子メール内の脅威の発生源(Include detected by: threat source in feed emails)] 設定が有効になっている場合にのみ表示されます。詳細については、「「脅威フィード設定」 ページ 127」を参照してください。

[脅威フィード(Threat Feed)] テーブル内の各行は、失敗サンプルで見つかった URL を表します。同じドメインと同じ件名のメッセージに一意の URL が複数回見つかることがあります([カウント(Count)] 値が 2 以上になります)。また、同じドメインと同じ件名のメッセージに複数の URL が見つかることもあります([Fromドメイン/電子メール送信元IP(From Domain/Email Source IP)] 列と [件名(Subject)] 列の値が重複しています)。

脅威フィードの設定

1. [分析(Analyze)] > [脅威フィード(Threat Feed)] に移動します。
2. [脅威フィードの設定(Configure your Threat Feed)] をクリックします。
3. 脅威フィード設定を選択します。詳細については、「「脅威フィード設定」 ページ 127」を参照してください。
4. [完了(Done)] をクリックします。

設定メニューからのホワイトリストへのアクセス

URL をホワイトリストに登録すると、その URL を含むメッセージが脅威フィードに追加されなくなります。

[設定(Configure)] > [ホワイトリスト(Whitelist)] に移動して、画面を開きます。ここでは、次のことができます。

- 脅威フィードホワイトリスト登録アクションを使用してホワイトリストに登録された URL と、Agari によってホワイトリストに登録された URL がすべて記載されたリストを表示できます。
- URL をホワイトリストに手動で追加できます。

脅威フィードからホワイトリストへの URL の登録

脅威フィードの URL リストから直接 URL をホワイトリストに登録できます。

1. [分析(Analyze)] > [脅威フィード(Threat Feed)] に移動します。
2. [URI] 列内の URL をクリックします。
3. 次をクリックします。
    - [...ルートドメインまたはそのサブドメイン(...root domain or its subdomains)]: ルートドメインが含まれている URL をすべてホワイトリストに登録します。これは、Facebook などの共有サービスドメインの場合に選択できます。facebook.com のすべての URL をホワイトリストに登録するのではなく、your_company.facebook.com をホワイトリストに登録することをお勧めします。
    - [...クエリ文字列を除く正確なパス(...exact path, excluding the query string)]: 特定の URL のみをホワイトリストに登録します。これは、特定の完全修飾 URL とパス(facebook.com/safestuff など)が適切であることはわかっているものの、それでも facebook.com のみが含まれているメッセージを脅威フィードの対象と見なしたい場合に選択できます。

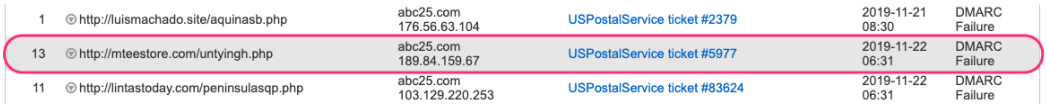
URL が緑色に変わり、ホワイトリストに登録されたことが示されます。

失敗サンプルの表示

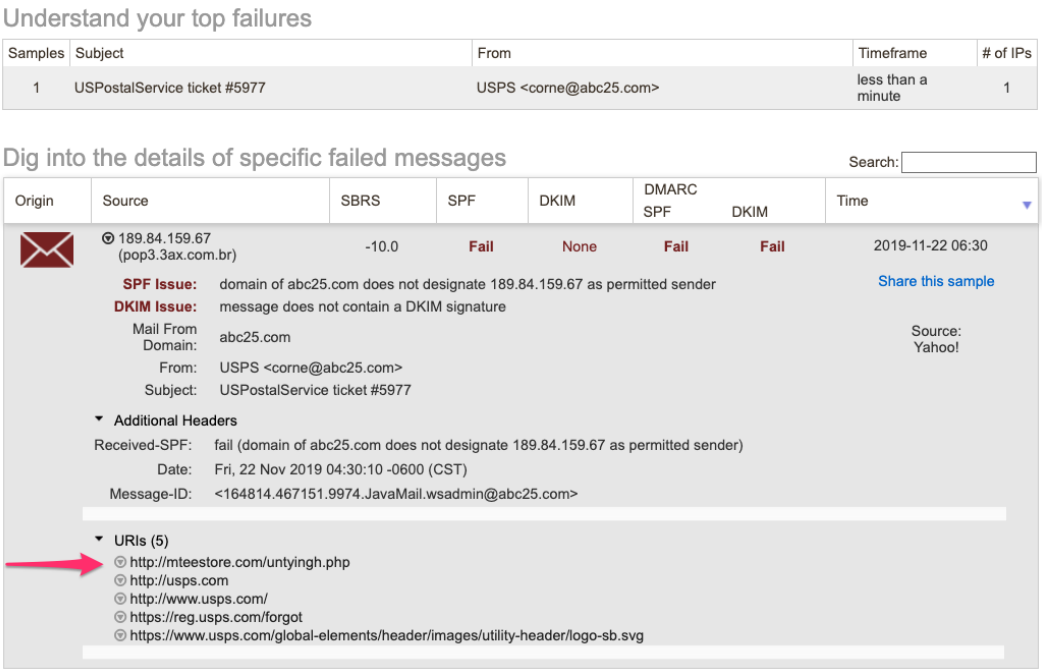
1. [分析(Analyze)] > [失敗サンプル(Failure Samples)] に移動します。

    または

2. [分析(Analyze)] > [脅威フィード(Threat Feed)] に移動します。[件名(Subject)] 列にあるリンクをクリックします。



この URL は、[Fromドメイン/電子メール送信元IP(From Domain/Email Source IP)] と [件名(Subject)] が同じ 13 個のメッセージに表示されています。



失敗サンプルには、複数の URL が含まれています。脅威として識別される URL であり、脅威フィードリストに表示されるものと同じです。また、メッセージが SPF または DMARC に合格しなかったことと、DKIM 署名がないことも確認できます。

失敗サンプルの共有

失敗サンプルを組織内の他のユーザーと共有して、分析してもらうことができます。

1. [分析（Analyze）] > [失敗サンプル（Failure Samples）] に移動します。

または

1. [分析（Analyze）] > [脅威フィード（Threat Feed）] に移動します。[件名（Subject）] 列内のリンクをクリックします。
2. 次をクリックします。
   - [共有（Share）]（ページ上部にあるボタン）：失敗レポート全体を共有します。複数のメッセージが記載されている場合があります。
   - [このサンプルを共有（Share this sample）]（特定のメッセージ内のリンク）：失敗レポート内の該当するメッセージだけを共有します。
3. [レポートの共有（Share Report）] ダイアログボックスで、共有に含める内容を選択します。
   - [リンク（Link）]（デフォルトで選択）：メッセージに含まれている失敗サンプルレポートへのリンク。
   - [PDF]（デフォルトで選択）：メッセージに添付されたレポートを生成した Adobe Acrobat バージョン。
   - [CSV]：メッセージにテキストファイル形式で添付されたカンマ区切り値バージョンのレポート。
   - [追加の注意事項を入力（Enter any Additional Notes）]：自由形式のフィールドで、レポートの受信者にとって有用な情報を入力できます。

[宛先:(To:)]フィールドに対して電子メールアドレスを追加または削除することはできません。失敗サンプルレポートは、すべてのドメイン保護ユーザーに送信されます。

4. [メールの送信(Send Email)]をクリックします。

脅威フィード設定

設定	説明
[脅威フィードを有効にする(Enable Threat Feed)]	脅威フィードを完全に有効または無効にします。この設定はデフォルトで有効になっています。
[後で再表示する脅威を再送信(Resubmit threats which are seen again after)]	認証失敗サンプルに繰り返し表示されるURIをいつ脅威フィードに再送信するかを指定します。次から選択してください。 • 2週間(デフォルト) • 1ヵ月 • 3ヵ月 脅威フィードに誤検出(ほとんどの場合正当なもの)や迷惑/スパムURLが多数含まれている場合、後者は実際の脅威ではなく通常はアクションを必要としないため、期間が長い方のいずれかを選択することをお勧めします。組織のほとんどはデフォルトの2週間で十分であり、それだけの期間があれば、必要なアクションを実行できなかったURLがあるかどうかを確認できます。アクションの実行にあたってリンク単位で課金し、契約で時間を制限しているテイクダウンベンダーを使用している場合には特にそうです。
[信号強度(Signal Strength)]	脅威フィードに含める脅威を指定します。次から選択してください。 • [すべての脅威を送信(Send all threats)]:ブランドになりすましているURIとDMARCに失敗している脅威の両方を含めます。信号強度が最も高い推奨の設定です。 • [ブランド識別子があるすべての脅威を送信(Send all threats with brand identifiers)]:ブランド識別子があるURIのみを含めます。 • [DMARCに失敗したすべての脅威を送信(Send all DMARC failure threats)](デフォルト):ブランド識別子があるURIを除外します。
[検出元を含める:フィード電子メール内の脅威の発生源(Include detected by: threat source in feed emails)]	[脅威フィード(Threat Feed)]テーブルに[検出元(Detected By)]列を表示するかどうかを指定します。[検出元(Detected By)]列では、脅威フィード送信を脅威の発生源に分類します。DMARCデータまたはブランドなりすましのいずれかを発生源にすることができます。
[ドメイン保護ホワイトリストにあるURIを除外(Exclude URIs on the Domain Protection Whitelist)]	ドメイン保護は、既知の正規URIパターンのグローバルなホワイトリストを維持します。この設定によって、ホワイトリストに登録されたURIが脅威フィードに表示されるかどうかが決まります。こうしたパターンと一致するURIが脅威フィードに送信されないようにする場合に選択します(デフォルト値)。
[ホワイトリストにあるURIを除外(Exclude URIs on my Whitelist)]	組織のホワイトリストにURIを追加できます。この設定によって、組織のホワイトリストに登録されたURIが脅威フィードに表示されるかどうかが決まります。こうしたパターンと一致するURIが脅威フィードに送信されないようにする場合に選択します(デフォルト値)。
[SBRSしきい値が次より大	SBRSは、電子メールメッセージの送信元IPアドレスに対するレピュテーションスコ

設定	説明
きい送信元からのURIを除外（Exclude URIs from sources with an SBRS threshold greater than）]	アです。SBRS 値の範囲は、-10（最悪）から +10（最高）です。送信元の SBRS が指定のしきい値よりも大きいメッセージから抽出された URI を除外できます。デフォルト値は 0 です。 たとえば、送信元の SBRS が非常に肯定的なメッセージから取得した URI を脅威フィードが無視するようにできます。
[電子メール受信者に脅威フィードを送信（Send Threat Feed to email recipients）]	指定した受信者に脅威フィード内の項目を送信するかどうかを指定します。有効な電子メールアドレスのカンマ区切りリストを入力します。このリストには、脅威フィードを直接受信できるようにするテイクダウンベンダーの電子メールアドレスを含める必要があります。 そのため、電子メールフィードが大量に発生する可能性があります。これは、個人の電子メールアドレスではなく、自動処理を行う場合にお勧めします。 電子メールメッセージに悪意のある URI が含まれることがあります。そうしたメッセージをスパム対策フィルタやウイルス対策フィルタからホワイトリストに登録してください。 脅威フィード電子メールメッセージ： • 199.255.192.0/22、199.127.232.0/22、54.240.0.0/18 の範囲にある送信元 IP アドレスから生成されます。 • Cisco <no-reply@cisco.com> の From ヘッダー電子メールを使用します。 • [フィード電子メールの件名：（Subject of feed emails:）] フィールドに指定した件名を使用します。
[フィード電子メールにヘッダー From:ドメインを含める（Include header From: domains in feed emails）]	URI の抽出元のメッセージに使用された From: ヘッダードメインを脅威フィード電子メールに含めるかどうかを指定します。デフォルトでは選択されていません。 これにより、悪用が発生したドメインの追加情報が得られます。通常は、このオプションを有効にすることをお勧めします。ただし、有効にすると、使用している有料サービスやサードパーティサービスで自動化プロセスが中断する場合を除きます。
[フィード電子メールに件名を含める（Include Subject: lines in feed emails）]	URI の抽出元のメッセージに使用された件名を脅威フィード電子メールに含めるかどうかを指定します。デフォルトでは選択されていません。 これにより、件名の共通点など悪用メッセージに関する追加情報が得られます。たとえば、いずれの件名にも「バイアグラ」や「アカウント」が含まれているといった情報です。通常は、このオプションを有効にすることをお勧めします。ただし、有効にすると、使用している有料サービスやサードパーティサービスで自動化プロセスが中断する場合を除きます。
[フィード電子メールの件名（Subject of feed emails）]	脅威フィード電子メールの件名を指定します。こうしたメッセージをフィルタ処理して、特定のフォルダに転送する場合に便利です。 デフォルトは「シスコシステムズ合同会社 の Cisco 脅威フィード」です。
[ヘッダーFrom:ドメインをホワイトリストに登録（Whitelist header From: domains）]	From ヘッダーで特定のドメインを使用しているメッセージ内にある URI を脅威フィードから省くかどうかを指定します。カンマ区切りリストに有効なドメイン名を入力すると、そのドメインからのメッセージに URI が含まれないようになります。 たとえば、ドメイン email.mycorp.com を社内の従業員が電子メールを送信するために使用しているとします。このドメインに対する認証に失敗した場合、有効な URL が多数含まれることがよくあります。そのため、組織の脅威フィードでは email.mycorp.com からのメッセージに URL を含めないようにすることをお勧めしま

設定	説明
	す。このオプションを選択し、テキストフィールドに email.mycorp.com と入力してください。
[Internet Identity(IID:「シスコシステムズ合同会社」を提供するターゲット)に脅威フィードを送信(Send threat feed to Internet Identity (target to provide IID: 'Cisco, Inc.'))]	テイクダウンベンダーが Internet Identity(IID、現在は Infoblox)である場合、このオプションを選択して、脅威フィード電子メールを送信することなく、IID に直接脅威フィードを送信できます。デフォルトでは選択されていません。

アラート

Cisco Domain Protection は、数多くのイベントについてアラートを生成します。たとえば、脅威や認証失敗の急増、新しい送信者とブランドなりすまし、顧客側の送信者の変更、SPF、DKIM、DMARC の各レコードの変更といったイベントです。こうしたアラートによって、すべてのドメインの認証ステータスを維持するために必要な情報を得ることができます。次の操作を実行できます。

- 「アラートの表示」見開きページ
- 「アラートへの登録」ページ 131
- 「アラートの設定」ページ 132

アラートのタイプ

このトピックでは、ドメイン保護が生成するすべてのアラートについて説明します。アラートの件名について新たに報告すべき内容があれば、各種アラートがそれぞれの頻度に応じて送信されます。午後 10 時(UTC)に、すべてのレポート購読者に向けて日次レポートの送信が始まります。

アラート	周波数	設定可能	説明
認証失敗スパイク	毎時	• しきい値 • 例外	過去 1 時間に送信者インベントリから受け取った DMARC 失敗サンプルの量が、事前設定された統計的しきい値を超えています。電子メールインフラストラクチャまたは認定サードパーティ送信者で SPF、DKIM、識別子アライメントに関する重大な問題が発生している可能性があります。このアラートは、アクティブなドメインの失敗サンプルデータを 1 時間ごとに評価します。
ブランドなりすましアラート	毎時	なし	他の人が所有しているドメインからのメッセージで、ブランドのなりすましである可能性があります。こうしたメッセージは、DMARC ポリシーで保護されません。このアラートは、ブランドなりすましの新たな脅威でないか、DMARC 以外のデータを 1 時間ごとに評価します。
カスタム送信者変更	イベント時	なし	送信者インベントリが変更されたため、カスタム送信者の IP 範囲が変更されました。
DKIM レコード変更	毎日	• 例外	いずれかのドメインに関連する DKIM レコードが変更されました。

アラート	周波数	設定可能	説明
DMARC レコード変更	• 毎時（アクティブなドメイン） • 毎日（防御ドメイン）	• 例外	いずれかのドメインに関連する DMARC レコードが変更されました。
インフラストラクチャ アラート	毎日	• しきい値 • 例外	送信者インベントリ内の任意のサーバーで MARC-DKIM または DMARC-SPF に失敗するメッセージの割合が、通常の日の失敗率よりも高くなっています。サーバーのアラート日付の全体的な失敗率の差は、通常の日の全体的な失敗率よりも少なくとも 10.0 パーセンテージポイント高くなっている必要があります。このアラートには、アクティブなすべてのドメインの DMARC 集約データが含まれています。
新しい DKIM セレクタ	毎日	• 例外	いずれかのドメインに関連する新しい DKIM セレクタが見つかりました。
新しい送信者アラート	毎日	• しきい値 • 例外	送信者インベントリに属していない送信者が、ドメインに向けて送信しています。
新しいウェルノウン送信者	毎日	なし	新しいウェルノウン送信者がカスタム送信者と重複しています。
SPF レコード変更	毎日	• 例外	いずれかのドメインに関連する SPF レコード（またはインクルード）が変更されました。
脅威スパイク	毎時	• しきい値 • 例外	過去 1 時間に送信者インベントリの外部から受け取った DMARC 失敗サンプルの量が、事前設定された統計的しきい値を超えています。アラートに示されたドメインに対してフィッシング攻撃が開始されている可能性があります。
不正なネットブロック	毎日	なし	ウェルノウン送信者が未指定の IP アドレスを使用して送信したメッセージが検出されました。

アラートの表示

1. [ステータス（Status）] > [アラート（Alerts）] に移動します。

トリガーされたすべてのアラートがデフォルト表示にリストされます。

- 過去 1 週間
- すべてのドメイン
- すべてのアラートタイプ

アラートのリストをフィルタ処理できます。

アラートリストのフィルタ処理

1. アラートリストをフィルタ処理する場合は、表の上方にある次のいずれかのフィールドを変更し、[実行(Go)]をクリックしてフィルタを適用します。

アラートフィルタ	説明
1:開始日と終了日	デフォルトは、現在の日付の 1 週間前です。つまり、終了日は現在の日付で、開始日は現在の日付の 1 週間前の日付です。 いずれかのフィールドをクリックして、開始日または終了日に別の日付を選択します。
2:ドメイングループ	デフォルトは [すべてのドメイン(All Domains)] です。 フィールド内をクリックして 1 つ以上のシステムまたはカスタムドメイングループを選択し、そのグループに所属するドメインのアラートのみがリストに記載されるようにします。 1 つ以上のシステムまたはカスタムドメイングループを選択する場合は、[すべてのドメイン(All Domains)] 項目を削除する必要があることに注意してください。そうしないと、ドメイン保護は引き続きリスト内のすべてのドメインのアラートを表示します。
3:アラートタイプ	デフォルトは [すべてのアラートタイプ(All Alert Types)] です。 フィールド内をクリックして、1 つ以上のアラートタイプを選択し、そのタイプのアラートのみがリストに記載されるようにします。 1 つ以上のアラートタイプを選択した場合は、[すべてのアラートタイプ(All Alert Types)] 項目を削除する必要があることに注意してください。そうしないと、ドメイン保護は引き続きリスト内のすべてのアラートタイプのアラートを表示します。
4:ID またはドメイン	特定のアラート ID を入力してテーブル内の該当するアラートのみを表示したり、特定のドメインを入力してテーブル内の該当するドメインのすべてのアラートを表示したりできます。 文字を入力するたびに、テーブル内の項目がフィルタ処理されます。

アラートへの登録

ドメイン保護でアラートを表示する代わりに、アラートタイプに登録できます。アラートタイプに登録すると、そのアラートタイプのアラートがトリガーされるたびに、アラートの内容が記載された電子メールが届きます。

1. [ステータス(Status)] > [アラート(Alerts)] に移動します。
2. [登録の管理(Manage My Subscriptions)] をクリックします。
3. 登録するアラートタイプのスライダを右に移動します。選択内容は自動的に保存されます。

アラートの登録解除

1. [ステータス(Status)] > [アラート(Alerts)] に移動します。
2. [登録の管理(Manage My Subscriptions)] をクリックします。

3. 登録解除するアラートタイプのスライダを左に移動します。選択内容は自動的に保存されます。

アラートの設定

組織管理者ロールを持つユーザーのみがアラートを設定できます。

ブランドなりすましとカスタム送信者変更を除くすべてのアラートタイプで、ドメイングループを除外できます。

認証失敗スパイク、インフラストラクチャ アラート、新しい送信者アラート、脅威スパイクの各アラートタイプには、アラートしきい値を設定することもできます。

アラートタイプの設定を変更するときは注意が必要です。

- 例外リストでドメイングループを選択する場合は、このタイプのアラートを表示する必要があるドメインがグループに含まれていないことを確認してください。確信がない場合は、すべてのドメイングループでドメインを確認したうえで、ドメイングループを除外してください。
- しきい値によって、アラートの必要性に影響が出ないようにしてください。たとえば、しきい値が小さすぎると、アラートが数多く生成され、対処が必要なアラートを見失うおそれがあります。また、しきい値が大きすぎると、対処が必要な状況でアラートが生成されない可能性があります。

アラートを設定するには、次の手順を実行します。

1. [ステータス(Status)] > [アラート(Alerts)] に移動します。
2. [組織のアラート設定の管理(Manage Organization Alert Settings)] をクリックします。
3. [アラートタイプの設定(Alert Type Settings)] タブをクリックします。
4. アラートタイプの [(しきい値と)例外の編集(Edit (Threshold and) Exceptions)] リンクをクリックします。
5. 必要な変更を加えます。詳細については、以下の「アラート設定オプション」セクションを参照してください。
6. [保存(Save)]をクリックします。

アラート設定オプション

設定できるアラートタイプであれば、例外リストから 1 つ以上のドメイングループを除外できます。一部のアラートタイプでは、1 つ以上のドメイングループに対してしきい値を定義することもできます。

例外リスト

例外リストのドメイングループに属するドメインに対しては、アラートがトリガーされません。

[除外するドメイングループ(Domain groups to exclude)] フィールドで、フィールド内をクリックし、ドロップダウンリストから 1 つ以上のシステムまたはカスタムドメイングループを選択します。

[すべてのドメイン(All Domains)] は選択しないでください。選択すると、すべてのドメインがそのアラートタイプから除外され、そのタイプのアラートがトリガーされなくなります。

しきい値

しきい値(デフォルトは 100)を入力し、[ドメイングループ(Domain Groups)] フィールド内をクリックし、ドロップダウンリストから 1 つ以上のドメイングループを選択します。

[別のしきい値を追加（+ Add another threshold）] をクリックして、さらに他のドメイングループのしきい値を追加します。

組織アラート登録の管理

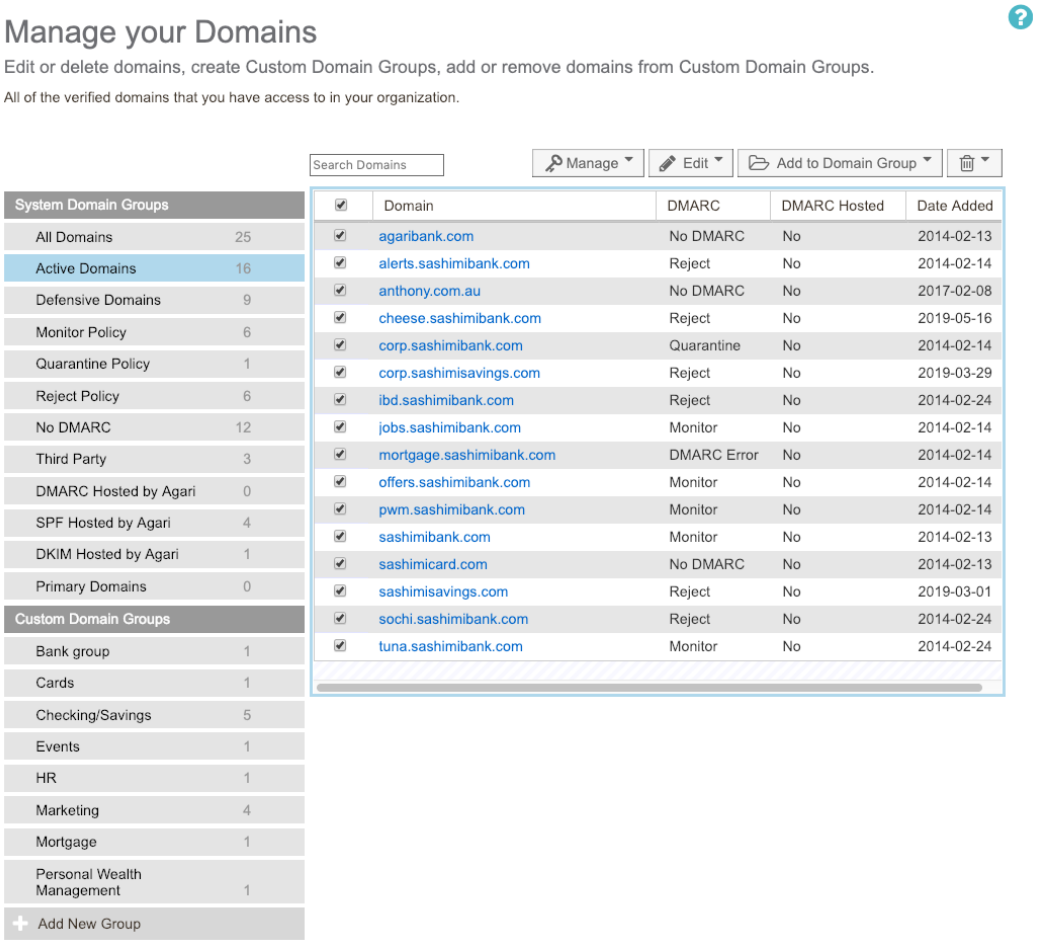
組織のすべてのドメイン保護ユーザーについて登録を管理（登録および登録解除）できます。組織管理者ロールを持つユーザーのみが、組織レベルで登録を管理します。

1. [ステータス（Status）] > [アラート（Alerts）] に移動します。
2. [組織のアラート設定の管理（Manage Organization Alert Settings）] をクリックします。
3. [サブスクライバ（Subscribers）] タブをクリックします。
4. いずれのユーザーでも、アラートタイプスライダを右にクリックすると、そのユーザーがそのアラートに登録され、アラートタイプスライダを左にクリックすると、そのユーザーがそのアラートから登録解除されます。選択内容は自動的に保存されます。

ドメイングループ

ドメイン保護では、カスタマイズ可能な方法でドメインをグループ化し、そうしたドメイングループを製品全体で使用できます。たとえば、1 つの部門が所有する一連のドメインをまとめて考慮する必要がある場合があります。ドメインを名前によってグループ化すると、グループ化されたドメインを使用して作業を進めることができ、多数のドメインによるリストを使用するよりも、作業が容易になります。ドメイングループは、ドメイン保護に習熟するほど役立つ強力な分類ツールです。

ドメインとドメイングループは、[設定（Configure）] > [ドメインの管理（Manage Domains）] ページで管理します。



ドメイングループのページの例

このページでは、すべてのアクティブドメインおよび防御ドメインを確認し、ドメイン分類用のカスタムドメイングループを作成し、ドメインユーザーへのアクセスを管理することができます。

システムドメイングループ

システムドメイングループは、事前定義された共通ドメインカテゴリであり、素早くアクセスできるため、ドメイン管理の改善に役立ちます。システムドメイングループは、動的にも作成されます。既存のシステムレベルのドメイングループのほかに、カスタムグループを追加できます。たとえば、「拒否ポリシー」グループには、組織内の、DMARC 拒否ポリシーを持つすべてのドメインが含まれます。Cisco がユーザーのドメインのいずれかで DMARC 拒否ポリシーを検出すると、そのドメインは自動的に「拒否ポリシー」グループのメンバーになります。このグループのドメインの追加または削除のためにユーザーは何もする必要がありません。

ドメインは複数の一意のグループに属することができます。

「アクティブ」ドメインと「防御」ドメイン：[防御としてマーク（Mark as Defensive）] が選択されていない限り、ドメインは「アクティブ」と見なされます。防御ドメインとは、メールフローが関連付けられていないドメインです。

サードパーティ：パートナーや代理店などの社外エンティティが管理するドメインです。

ネームサーバーなし：現在または最新の**ネームサーバールックアップ**で結果を返さなかったドメインです。

カスタムドメイングループ

カスタムドメイングループを使用すると、ドメインのグループを作成してワークフローをより適切に整理することができます。たとえば、上の図の例では、「Cards」ドメインで作業するチームと「Checking/Savings」ドメインで作業するチームを区別することができます。ドメインをグループ化すると、グループ化されたドメインを使用することで、多数のドメインによるリストを使用するよりも、作業が容易になります。また、ユーザーアカウントを作成する際に、そのユーザーが他のドメインを表示できないように制限することもできます。

ドメイングループの追加

1. [設定（Configure）] > [ドメインの管理（Manage Domains）] に移動します。
2. [カスタムドメイングループ（Custom Domain Groups）] リストの下部で、[新しいドメイングループを追加（Add New Domain Groups）] をクリックします。
3. 新しいドメイン グループの名前を入力します。
4. Enter キーを押します。
5. ドメインが含まれているドメイングループを選択します。
6. 1 つ以上のドメインを選択します。
7. [ドメイングループに追加（Add to Domain Group）] をクリックします。
8. 作成したドメイングループを選択します。
9. [適用（Apply）] をクリックします。

ドメイングループの削除

1. [設定（Configure）] > [ドメインの管理（Manage Domains）] に移動します。
2. 使用しないカスタムドメイングループにマウスのカーソルを合わせます。
3. ごみ箱のアイコンをクリックしてグループを削除します。
4. [OK] をクリックして確認します。

いったん削除したカスタムドメイングループは復元できません。

第 10 章

着信メッセージのモニタリング

着信 DMARC 可視化を実現するためには、Agari センサーが必要です。これを使用して、組織の電子メールストリームからメッセージごとの情報を収集し、Agari クラウドにテレメトリ情報をリレーして、DMARC 情報を集約します。

センサーには、次の 2 つのインストールオプションがあります。

·Agari ホステッド型センサー：ほとんどのお客様に推奨されるオプションです。ホステッド型センサーは、自動的にスケーリングされ、維持されます。Agari は、個別に管理される安全なクラウドでセンサーをホストします。

·オンプレミスセンサー：センサーは、オンプレミスにも展開できます。これは一般に、お客様が Cisco フィッシング防御 ソリューションを使用していて独自に Exchange サーバーを実行している場合にのみ推奨される設定です。これは、メールストアの近くにセンサーを配置した方が通常効率がよくなるためです。ただし、着信 DMARC には必要ありません。オンプレミスセンサーをホストする場合は、更新が利用可能になったら（「「着信メッセージのモニタリング」上」）センサーのインスタンスを明示的に更新し、メールの負荷が大きくなったらセンサーを手動で追加する必要があります。

詳細と、着信 DMARC およびセンサーセットアップを有効にする場合の支援については、Agari のサポートにお問い合わせください。

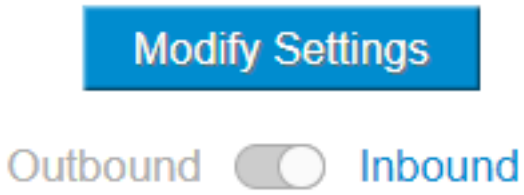
着信 DMARC 可視化をオンにする

ドメイン保護では、次の 2 つの場所でこの機能のオンとオフを切り替えることができます。

- [ドメイン（Domains）] ページの [診断（Diagnostics）]：

この切り替えで、[ドメイン（Domains）] リストでの着信メールと発信メールの表示をトグルします。

- [電子メールトラフィック（Email Traffic）] ページの [分析（Analyze）]



この切り替えで、着信メールと発信メールの分析の表示をトグルします。

第 11 章

管理

ドメイン保護の管理には、組織設定の定義、組織内のアクティビティの確認、組織内のドメイン保護ユーザーの管理などがあります。

組織管理者ロールを持っている場合にのみ、組織設定の変更、監査証跡の表示、およびユーザーの管理を行うことができます。

組織設定

[顧客組織の管理(Manage customer organizations)] ページで組織設定を管理します。ここでは、次のカテゴリに分かれた設定を構成します。

- 管理
- 組織
- ユーザーアカウント

組織設定を編集するには、[管理(Admin)] > [組織(Organization)] に移動し、[組織の詳細の編集(Edit Organization Details)] をクリックします。

組織管理者ロールを持っている場合にのみ、組織設定を変更できます。

設定	説明
	管理
[組織名(Organization Name)]	組織の名前。これは、監査証跡など組織に関して表示する情報がある場所に表示されます。組織名を変更する場合は、Cisco 担当者にお問い合わせください。
[シンボリック名(Symbolic Name)]	組織を一意に定義するために、当初設定された組織名から作成される一意の文字列です。この識別子は、システムによって使用され、ここにのみ表示されます。これは変更できません。
[サブドメイン(Subdomain)]	組織に固有のアプリケーション URL の一部。dmp.cisco.com のサブドメインです。 この値を変更する場合は十分に注意してください。ドメイン保護のリンク、ブックマーク、およびその他の接続が破損する可能性があります。
[作成日(Creation Date)]	組織が作成された日付と時刻が表示されます。 をクリックすると、現地時間と UTC(協定世界時)が切り替わります。
[注記(Notes)]	このフィールドを使用すると、組織に関する情報とその設定方法、あるいは表示したい情報を自由形式で追加できます。ここに入力した内容は、組織内のどのユーザーでも、組織設定ページを開いたときに表示されます。

設定	説明
	組織設定
[主要な管理担当者（Primary Administrative Contact）]	ここで組織内のユーザーを選択すると、管理作業に関する問い合わせはすべてそのユーザーがCisco から受信することになります。
[データコレクションポリシー（Data Collection Policy）]	個人識別情報（PII）を保持するか、メッセージや障害レポートから削除したうえでドメイン保護に保存するかを決定します。次を選択します。 • [利用可能なすべてのデータを収集（Collect All Available Data）]（デフォルト） • [変更されたデータを収集（Modified Data Collection）] [変更されたデータを収集（Modified Data Collection）] を選択した場合、すべての障害レポートから次の部分が取り除かれ、保持されず、回復できなくなります。 • メッセージ全文 • メッセージ本文に含まれる URL • 特定のヘッダーフィールド これらに PII が含まれる場合や、PII がエンコードされて識別が難しい場合があるため、これらを完全に削除してから、メッセージと障害レポートがドメイン保護に保存されます。このデータがない場合、URL スレッドフィードなどドメイン保護の一部の機能が組織で使用できなくなる可能性があります。 [利用可能なすべてのデータを収集（Collect All Available Data）] を選択すると、ドメイン保護では組織内の登録済みユーザーのみがデータにアクセスできるようになります。
[対処不可能なエラーを無視（Ignore non-actionable errors）]	DKIM エラーを判断する際に、DKIM レコードに v= 属性がなくても無視するかどうかを決定します。選択した場合、ドメインの DKIM レコードには v= 属性がなく、次のようになります。 • DKIM の重大な問題のリストにも軽微な問題のリストにも、DKIM レコードが記載されません。 • DKIM レコードは、有効なキーのリストに記載されるようになります。 ドメインの [DKIMキー（DKIM Key）] アイコンをクリックした場合。 また、v= 属性の欠落がドメインで発生した唯一の DKIM エラーである場合は、ドメインの [DKIMキー（DKIM Key）] アイコンの横にエラーインジケータ（!）が表示されません。 DKIM の仕様（https://www.ietf.org/rfc/rfc6376.txt）には v= 属性が必須の属性であると定義されていますが、DKIM レコードに v= 属性がなくても、DKIM は失敗しません。Cisco では DKIM レコードを扱う際にこの仕様に従うことを推奨していますが、ドメインの DKIM レコードにアクセスできない場合、DKIM レコードの更新は必ずしも容易なことではありません。管理するドメインの DKIM レコードを Cisco にホストするようにすると（「「Cisco での DKIM レコードのホスティング」 ページ 65」を参照）、DKIM レコードの更新が容易になります。
	ユーザーアカウント設定
[シングルサインオン（Single Sign-on）]	ユーザーがドメイン保護にアクセスする場合にユーザー名だけでなくパスワードも入力する必要があるかどうかや、ユーザーが既存の認証を使用できるかどうかを決定します。詳細については、「「シングルサインオン（SSO）」 ページ 149」および「「組織のシングルサインオンの有効化」 ページ 150」を参照してください。

設定	説明
[セッションが非アクティブならログオフ(Session Inactivity Logoff)]	ユーザーがドメイン保護にサインインしたままにできる時間を決定します。これを過ぎると、自動的にサインアウトします。デフォルトは 4 時間です。 自動ログオフの方法も選択します。次から選択してください。 • [相対(Relative)](デフォルト):[セッションが非アクティブならログオフ(Session Inactivity Logoff)] に設定された期間内にドメイン保護でアクションが行われないと自動的にログオフします。 • [絶対(Absolute)]:ログイン後に [セッションが非アクティブならログオフ(Session Inactivity Logoff)] に設定された期間が経過すると、自動的にログオフします。つまり、[セッションが非アクティブならログオフ(Session Inactivity Logoff)] のクロックは、ログイン時に開始され、ユーザーがアクションを行ってもリセットされません。この設定にすると、ユーザーがアクションを行っている最中にログオフする可能性があります。
[パスワードの有効期限(Password expiration)]	ユーザーが次に新しいパスワードを選択するまでの期間を決定します。デフォルトは [なし(Never)] です。
[ログイン試行失敗の最大回数(Maximum failed login attempts)]	ユーザーがログインに失敗できる回数を決定します。この回数を超えると、ロックアウトされ、新しいアクティベーションリンクを送信する必要があります。ログインの試行を制限しない場合は、[無効(Disable)] を選択します。デフォルト値は 5 です。
[パスワードポリシー(Password Policy)]	「組織設定」ページ 138でログイン時にパスワードの入力を必須にした場合(非 SSO)、パスワードの複雑さの最小要件を決定します。 ユーザーの次のパスワード要件を変更する場合は、要件に対応した値を入力します。 • 最小長(デフォルト:5) • 大文字の最小数(デフォルト:0) • 小文字の最小数(デフォルト:0) • 記号(英数字以外)の最小数(デフォルト:0) • 数値の最小数(デフォルト:0) Federal Risk and Authorization Management Program(FedRAMP)プロセスにより、ドメイン保護ユーザーが自身のパスワードを変更するときに、そのユーザーが以前に使用していた 24 個のパスワードのいずれにも変更できません。
[IP ベースのアクセス制御(IP-Based Access Control)]	ドメイン保護がどこからアクセスできるかを定義および制限します。 セキュリティを強化するために、ユーザーが定義した特定の IP アドレスセットからのみドメイン保護にアクセスするように規定できます。1 つ以上の IP アドレスまたは CIDR ブロックをスペースまたはカンマで区切って入力します。

[監査組織アクティビティ(Audit Organization Activity)] リンクをクリックすると、ユーザーのログイン/ログアウトや設定の変更などの情報が記録された組織の監査ログを表示できます。詳細については、「「組織アクティビティの表示」次のページ)」を参照してください。

監査証跡

ドメイン保護は、組織内のすべてのアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。組織と組織内の各ユーザーの両方のアクティビティがすべて、新しい順に [アクティビティログの監査（Audit the activity log）] ページにリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。

アイコン	アクティビティのカテゴリ
	ユーザーがドメイン保護 自体またはドメイン保護内の組織にサインインしたことを示します。
	ユーザーがドメイン保護 自体またはドメイン保護内の組織からサインアウトしたことを示します。
	ユーザーがユーザーアカウントを作成、編集、または削除したこと、あるいはシステムがタスクを実行したことを示します。
	ドメイン保護ユーザーか、またはドメインを管理するシステムによって、ドメインで作成、編集、削除、またはその他のアクションが実行されたことを示します。そうしたアクションに関する情報もあればリストされます。たとえば、ドメインのネームサーバーを変更すると、以前のネームサーバーと新しいネームサーバーの両方が監査ログに記録されます。
	ユーザーが送信者に対して作成、編集、削除、またはその他のアクションを実行したことを示します。
	ユーザーがレポートリクエストを作成したことを示します。
	ユーザーがドメイングループに対して作成、編集、削除、またはその他のアクションを実行したことを示します。
	送信者のインベントリが変更されたことを示します。
	ユーザーが、Cisco サービス規約（TOS）に同意する、組織設定を変更するなど、組織レベルのアクティビティを実行したことを示します。

組織アクティビティの表示

ドメイン保護は、組織内のすべてのアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。

組織のアクティビティを表示するには、組織管理者ロールが必要です。

1. [管理（Manage）] > [組織（Organizations）] に移動します。
2. [監査組織アクティビティ（Audit Organization Activity）] をクリックします。

ドメイン保護組織内のすべてのアクティビティが、新しい順にリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。詳細については、「「監査証跡」（前のページ）」を参照してください。ログの検索および使用方法の詳細については、ページの上部にある［ヘルプ（Help）］（  ）をクリックしてください。

［CSVをダウンロード（Download CSV）］をクリックして、ドメイン保護が追跡するイベントがすべて記載されたリストをカンマ区切り値（CSV）テキストファイルとしてダウンロードします。

組織アクティビティの検索

組織のアクティビティのリストを表示しているときに、リスト内を検索することもできます。次の 2 つの検索タイプを使用できます。

- 簡易テキスト検索：Web 検索エンジンと同じく、用語を入力すると、その用語が検索され、見つかれば検出されます。たとえば、ユーザー名を入力して、組織内でのそのユーザーのアクティビティのみを表示できます。
- クエリキー：特定のキーワードを入力して、リストを特定のアクションに絞り込むことができます。たとえば、レポートリクエストが作成されるたび、という具合です。

クエリキー

簡単に言うと、クエリキーとはドメイン保護の監査証跡によって追跡される項目のことです。さまざまなオブジェクトであり、ドット（.）で動詞とつなぐこともできます。クエリキーでは特定のオブジェクトに対するアクションを定義するため、検索フィールドでクエリキーを使用するときは、常にその前に action: を付けます。

ほとんどのクエリキーオブジェクトは、動詞の作成、更新、破棄と組み合わせることができます。技術的に言うと、「CRUD」アクションから「R」を差し引いたものです。一部のキーでは、他にもいくつか動詞を使用できます。

検索形式は action:*object*[.*verb*] です。

つまり、action: は必須で、その後にオブジェクト名を続けます（: の後にはスペースを入れません。オプションでドット（.）と有効な動詞を続けることができます）。

次に、すべてのクエリキーを示します。

bimi_record_source

追加の動詞：なし

説明：BIMI（「「ブランド インジケータ メッセージ識別」 ページ 110」を参照）レコードに加えられた変更。

例：action:bimi_record_source.create を検索すると、結果に「123 Inc.（admin@123.com）created the BIMI record 123.com」が含まれることがあります。

dkim_record_source

追加の動詞：なし

説明：DKIM（「「DomainKeys Identified Mail（DKIM）」 ページ 58」を参照）レコードに加えられた変更。

例：action:dkim_record_source.update を検索すると、結果に「123 Inc.（admin@123.com）updated the DKIM record abc123.com」が含まれることがあります。

domain

追加の動詞：なし

説明:ドメインレコードに加えられた変更。

例:action:domain.destroy を検索すると、結果に「123, Inc. (admin@123.com) deleted the domain ABC123.com」が含まれることがあります。

domain_sender

追加の動詞:なし

説明:送信者承認レコードに加えられた変更。このオブジェクトは、送信者がドメインに対して承認されると作成され、承認が取り消されると削除されます。自動化プロセスによくあることですが、ユーザーはドメインの送信者を手動で承認できます。また、送信者を手動で承認していた場合は、その承認を手動で取り消すことができます。これは、特に SPF レコードをホストしている場合に重要な意味を持ちます。ドメイン/送信者のすべての関係が手動で処理されるからです。

例:action:domain_sender.create を検索すると、結果に「123, Inc. automatically created the domain sender #<DomainSender:*hash*>」が含まれることがあります。

domain_set

追加の動詞: add_domains、remove_domains

説明:ドメイングループ(「「ドメイングループ」 ページ 133」を参照)レコードに加えられた変更。

例:action:domain_set.remove_domains を検索すると、結果に「123, Inc. (admin@123.com) modified the domain group third party」が含まれることがあります。

organization

追加の動詞: accept_agreement、reject_agreement、add_netblock_source、remove_netblock_source

説明:組織の情報または設定に加えられた変更。

作成アクションと破棄アクションは関係会社組織、つまりサブ組織を持つ組織でのみ実行されるアクションであるため、これらのアクションを監査証跡で確認できるのは関係会社組織のみです。

例:action:organization.accept agreement を検索すると、結果に「123, Inc. (admin@123.com) accepted the End_User License Agreement ABC123.com」が含まれることがあります。

organization_sender

追加の動詞:なし

説明:組織と送信者間の関係に加えられた変更。

このオブジェクトに影響を与えるためにユーザーが実行できる明示的なアクションはありません。organization_sender は、ドメインと送信者間の関係だけに基づいてセカンダリオブジェクトとして作成されます。これが作成されるのはドメインが初めて組織内の送信者に関連付けられたとき(送信者がドメインに対して承認されたとき)であり、削除されるのは送信者に関連付けられた組織内にドメインがなくなったときです。また、ドメインが送信者との関係を獲得または失うと更新されます。

例:action:organization_sender.destroy を検索すると、結果に「123, Inc. (admin@123.com) removed the sender New Sender」が含まれることがあります。

report_request

追加の動詞:なし

説明:レポートリクエストに加えられた変更。

例：action:report_request.destroy を検索すると、結果に「123, Inc. (admin@123.com) deleted the report request Daily Domain Diagnostic Report (123, Inc.) (csv, pdf)」が含まれることがあります。

sender

追加の動詞：なし

説明：送信者（「「送信者」 ページ 88」を参照）の定義に加えられた変更。

例：action:sender.destroy を検索すると、結果に「123, Inc. (admin@123.com) deleted the sender New Sender」が含まれることがあります。

sender_netblock

追加の動詞：

説明：ネットブロックの作成または削除。

sender_netblock オブジェクトには、更新動詞がありません。

例：action:sender_netblock.create を検索すると、結果に「123 Inc. (admin@123.com) created the sender netblock ###.###.###.###」（# はネットブロック内の数字）が含まれることがあります。

sender_netblock_source

追加の動詞：なし

説明：送信者のインベントリに加えられた変更。

例：何らかの動詞を含めて action:sender_netblock_source を検索すると、結果に「123, Inc. (automatically) modified ABC's Sender Inventory」が含まれることがあります。

user

追加の動詞： activated、login、logout、update_roles

説明：ユーザーアカウント、ユーザー アカウント アクティベーション、ユーザーログイン、またはユーザーログアウトに加えられた変更。

例：action:user.update または action:user.update_roles を検索すると、結果に「123, Inc. (admin@123.com) changed the roles for newuser123.com」が含まれることがあります。

検索の仕組み

検索フィールドへの文字入力を開始し、その後入力を一時停止または停止すると、ドメイン保護による検索が始まります。専門用語では、「starts with」検索と言います。特に同じ文字で始まるオブジェクトがいくつかあるという理由で、表示された検索結果を理解するには、この概念が重要です。

たとえば、前述のように、*.verb* はオプションです。しかし、該当するオブジェクトのすべての監査証跡エントリを確認する目的で action:sender_netblock を検索した場合、検索結果には sender_netblock_source オブジェクトの監査証跡エントリも含まれます。sender_netblock オブジェクトのエントリのみを表示するには、action:sender_netblock. というように動詞を含めずに . を追加します。

ユーザーアカウント

ユーザーアカウントでは、ドメイン保護ユーザーのログイン情報とアクセス機能を定義します。ドメイン保護は、ロールベース アクセス コントロール（RBAC）を使用しており、ドメイン保護機能にアクセスするためのロールを各ユーザーに 1 つ以上割り当てることができます。

Cisco のサポート担当者には、ドメイン保護 組織でユーザーアカウントを作成、有効化、編集、または削除するためのアクセス権がありません。

ユーザーアカウントの作成

ユーザーアカウントを作成できるのは、ユーザー管理者ロールを持つユーザーのみです。

1. [管理者（Admin）] > [ユーザー（Users）] に移動します。
2. [新規ユーザーを追加（Add New User）] をクリックします。
3. [氏名（Full Name）] と [電子メール（E-mail）] にそれぞれ氏名とアドレスを入力します。

   有効なメールアドレスを入力する必要があります。このメールアドレスが招待メールメッセージの送信先になります。招待メールメッセージには作成した新規ユーザーに固有のリンクが含まれ、ユーザーはそのリンクをクリックして自身の新規アカウントを検証する必要があります。
4. 他のユーザーアカウント設定を構成し、1 つ以上のユーザーロールを選択します。詳細については、「「ユーザーアカウント設定」見開きページ」を参照してください。
5. [新規ユーザーを招待（Invite New User）] をクリックします。

入力したメールアドレスに電子メールが送信されます。メールにはユーザーを検証するためのリンクが含まれ、検証されたユーザーはアカウントのパスワードを設定できます。

ユーザーアカウントの編集

1. [管理者（Admin）] > [ユーザー（Users）] に移動します。
2. ユーザーの名前をクリックします。
3. ユーザー情報と設定に必要な変更を加えます。詳細については、「「ユーザーアカウント設定」見開きページ」を参照してください。
4. [更新（Update）] をクリックします。

ユーザーアカウントの削除

1. [管理者（Admin）] > [ユーザー（Users）] に移動します。
2. ユーザーの名前をクリックします。
3. 左下にある [ドメイン保護から[username]を完全に削除（Delete [username] entirely from Domain Protection）] リンクをクリックします。
4. [OK] をクリックします。

ユーザーアクティビティの表示

ドメイン保護 は、組織内のすべてのユーザーのすべてのアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。

ユーザーのアクティビティを表示するには、組織管理者ロールが必要です。

1. [管理者(Admin)] > [ユーザー(Users)] に移動します。
2. ユーザー名の下にある [監査(Audit)] リンクをクリックします。

ドメイン保護組織内のすべてのユーザーアクティビティが、新しい順にリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。詳細については、「「監査証跡」 ページ 141」を参照してください。ログの検索および使用方法の詳細については、ページの上部にある [ヘルプ(Help)] ( ) をクリックしてください。

[CSVをダウンロード(Download CSV)] をクリックして、ドメイン保護が追跡するイベントがすべて記載されたリストをカンマ区切り値(CSV)テキストファイルとしてダウンロードします。

ユーザーアカウント設定

このトピックでは、ドメイン保護ユーザーアカウントの設定について説明します。

ユーザー情報

設定	説明
正式名称	ユーザーがログインしているときに各ページの上部に表示されるユーザーのフルネーム(ユーザーのリストに表示されるものと同じ)。アクティビティの監査ログにも表示されます。
E メール	ユーザーの電子メール アドレス。ユーザーのログイン クレデンシャルと、レポートおよびアラートの宛先アドレスに使用されます。この電子メール アドレスは、初期アクティベーション トークンが添付された招待電子メールに使用されることに注意してください。
デフォルト ダッシュボード	ログイン時にユーザーに表示されるダッシュボードを選択します。
セカンダリ認証	組織がシングルサインオン(SSO)を使用している場合、このオプションによって、セカンダリ認証(ユーザー名とパスワード)をオプションにするか必須にするかが決まります。このオプションを選択しないと、常に SSO が使用されます。そのため、サインイン時に SSO プロバイダーが利用できない場合は、アプリケーションにアクセスできません。このオプションを選択すると、さらに次の 2 つのオプションが表示されます。 • [SSOが失敗したときのみ(Only when SSO fails)]: SSO プロバイダーが利用できない場合、ユーザーはパスワードフィールドに入力するように求められます。 • [排他的(SSOで認証しない) (Exclusively (do not authenticate with SSO))]: ユーザーは、常にパスワードの入力を求められます(SSO は使用されません)。

ロール

ロールではユーザーがアクセスできるドメイン保護の機能を定義します。各ロールを定義するには特定かつ固有のアクセス権限が必要です。ユーザーごとに少なくとも 1 つのロールを選択する必要があります。

ロールリストは階層的であり、あるロールを選択すると、そのロールの下にあるすべてのロールが自動的に選択されます。ただし、下位のロールの権限が継承されることはありません。選択したロールの下にあるユーザーの個々のロールをクリアできますが、いくつかまとめてクリアした場合、ユーザーインターフェイスが想定外の動作をすることがあります。

ユーザーロールには、次の 2 つのカテゴリがあります。

- 管理者ロール：組織での設定を変更できます。
- 読み取り専用ロール：アラートを受信し、データを表示できます。

ロール	説明
	管理者のロール
組織の管理者	組織レベルの設定を管理します。これには、組織のパスワードルールの設定、セッションの有効期限の設定、データ収集ポリシーの設定、およびドメイン保護ユーザーの IP ベースのアクセス制御リストに関する制限の設定などがあります。
ドメインポリシー管理者	ドメインレベルの設定を管理します。これには、組織のドメインやカスタムドメイン グループの追加、編集、または削除と、組織の送信者インベントリの編集が含まれます。
脅威管理者	脅威レベルの設定を管理します。これには、組織の脅威フィードの設定と、組織の URI ホワイトリストの編集が含まれます。
ユーザー管理者	組織内のユーザーを管理します。これには、ユーザーの追加、編集、または削除が含まれます。 ユーザー管理者を作成するときは、この管理者がユーザーに付与できるロールのタイプを割り当てる必要があります（下記のロールの使用例を参照）。
	読み取り専用ロール
監査ユーザー	組織の監査ログと組織内のユーザーを表示します。
読み取り専用ユーザー	データを表示し、Web ポータルでレポートをスケジュールします。
レポートユーザー	スケジュールされたレポートとアラートを受け取ります。 このロールのみが単独で割り当てられているユーザーは、ドメイン保護で直接データを表示できません。このようなユーザーは、他のユーザーによってスケジュールされた電子メールによるレポートを受け取ったり、他のユーザーが登録した電子メールによるアラートを受け取ったり、登録されているレポートのリストを表示したりすることだけができます。 1 人の受信者ではなくメーリングリストにレポートや通知を送信する際に使用するアカウントを作成するには、通常どおりにユーザーを作成して招待してから、[ユーザー（Users）] リストでユーザーの名前をクリックして、そのユーザーを編集し、強力なパスワードを追加して [更新（Update）] をクリックすると、この疑似ユーザーがアクティブになり、レポートの受け取りに利用できるようになります。

ロール	説明
脅威フィード送信 API ユーザー	threat_feed_submissions エンドポイントからドメイン保護アプリケーション プログラミング インターフェイス（API）を介して脅威フィードデータのみを取得します。サードパーティのテイクダウンベンダーは、API に幅広くアクセスすることはできず、必要とする特定の情報にのみアクセスできます。そのため、サンプルデータに不具合があって個人情報にアクセスできてしまうといったことがありません。 このロールが割り当てられているユーザーアカウントには、このロールのみを割り当てる必要があります。このロールのみが割り当てられているユーザーアカウントは、ドメイン保護製品、その他の API、API ドキュメントにアクセスできません。 このロールを持つユーザーアカウントを使用して、脅威フィードデータの API にアクセスするには、管理者からアクセストークンとエンドポイント URL を入手します。

ドメインアクセス

デフォルトでは、新しいユーザーアカウントにはすべてのドメインへのアクセスが割り当てられます。

カスタムドメイングループにユーザーアクセスを割り当てることによって、ユーザーアクセスを特定のドメインに制限できます。

[ドメインアクセス（Domain Access）] の横にある矢印をクリックして、特定のドメイングループを選択します。

使用可能なドメイングループを確認し、リストから 1 つ以上のカスタムドメイングループを選択します。

ユーザーは次の操作のみを実行できます。

- ドメインに関する情報を表示する
- レポートのみを表示する
- アラートを受け取る

対象となるのは、選択したドメイングループに含まれるドメインのセットです。

たとえば、ドメイン固有のアクセス権を持つユーザーは、アクセス権のあるドメインに関連するデータしか表示できないため、電子メールトラフィック分析の [DMARCの傾向（What does my DMARC trend look like?）] にアクセスしたときのビューは、すべてのドメインへのアクセス権を持つユーザーが使用できるビューとは異なります。

ロールの例

ユースケースによっては、ロールを設定することになります。このトピックでは、その設定方法の例を示します。

電子メールでレポートとアラートを受け取れる読み取り専用ユーザーを作成

ユーザーの読み取り専用ロールをオンにすると、レポート受信者ロールもデフォルトでオンになります。電子メールによるレポートとアラートを受け取ることもできる読み取り専用ユーザーを作成するには、単にこれらのデフォルトを受け入れます。レポート受信者ロールをオフにすると、読み込み専用ユーザーは、レポートを送信するために使用可能なユーザーのリストに表示されず、アラートに登録できるユーザーのリストにも表示されません。

読み取り専用アクセス権を持ち、他の読み取り専用ユーザーを作成できるユーザー管理者を作成

ユーザー管理者を、そのユーザーの最上位アクセス ロールとしてオンにします。このユーザー管理者は、読み取り専用アクセス以下のアクセス権を持つユーザーのみを作成して管理できるようにするため、ユーザー管理者ロールの真下にある [ユーザーの管理（Manage Users）] チェックボックスで [すべての権限（All privileges）] オプションをオフにします。その後に、[読み取り専用（Read Only）] オプションと [レポート受信者（Report Recipient）] オプションをオンにします。このユーザーは、読み取り専用以下の権限を持つユーザーを作成して管理することができます。

他のユーザーの作成のみが可能なユーザー管理者を作成

他のユーザーを作成または編集することだけを目的とするユーザー管理者を作成します。このロールは、製品を使用してデータを表示したり、レポートやアラートを受け取ったりすることはできません。

新しいユーザーを作成した後に、作成したユーザーに対してユーザー管理者ロールをオンにして、ユーザー管理者の下で自動的にオンになっているすべてのロールをオフにします。ユーザー管理者ロールの下にある [ユーザーの管理（Manage Users）] ボックスで設定を変更しない限り、作成したユーザー管理者は、「すべての権限」を持つ他のユーザーを作成できます。

この新しいユーザー管理者が組織管理者とユーザー管理者を除くすべてのロールを作成できるようにするには、[x] を選択して [すべての権限（All Privileges）] を削除します。その後に、[ロールタイプの選択（Select Role Types）] 入力を使用して、組織管理者とユーザー管理者を除く各ロールをオンにします。

ドメイン設定は変更できるがユーザーの作成または編集ができないユーザーを作成

作成するユーザーに対してドメイン ポリシー管理者ロールをオンにします。ドメイン ポリシー管理者の下にあるすべてのロールがデフォルトでオンになります。このユーザーが他のユーザーを作成または編集できないようにするには、ユーザー管理者ロールをオフにします。

シングルサインオン（SSO）

ドメイン保護は現在、SAML 2.0 プロトコルを介して、組織内のユーザーを認証するためのシングルサインオン（「SSO」）メカニズムを有効化する機能が組み込まれています。

シングル サインオンを使用して、次のことを実行できます。

- 「ワンクリック」ログインの体験を作成する。既存の企業ログインアイデンティティ（アカウント）をドメイン保護のユーザー名にバインドできます。それによって、個別のドメイン保護のパスワードは必要なくなります。
- ユーザーアクセスを一元的に取り消す。従業員が退職した場合は、ドメイン保護へのアクセスをドメイン保護内で個別にではなくSSO プロバイダー内で削除できます。
- オプションのセカンダリ認証を提供する。特定のユーザー（たとえば、請負業者は ID プロバイダーシステムでは利用不可）を、ドメイン保護に保存されているログイン情報を使用して、排他的に認証できます（効果的にシングルサインオン メカニズムをバイパス）。また、SSO アイデンティティ サービスが失敗した場合でも、ドメイン保護のみに保存されているクレデンシャルを使用して、特定のユーザーを認証することができます。

組織のシングルサインオンの有効化

開始する前に、シングルサインオン プロバイダーから次の 2 つの情報を入手する必要があります。

- SAML 2.0 エンドポイント（HTTP）URL（ID プロバイダーシステムでは、「宛先」や「SAML 受信者」とも呼ばれます）
- パブリック証明書（X.509）

このタスクを実行するには、組織管理者ロールが必要です。

1. [管理者（Admin）] > [組織（Organization）] に移動します。
2. [組織の詳細を編集（Edit Organization Details）] をクリックします。
3. [ユーザーアカウント設定（User Account Settings）] セクションで、[シングルサインオンを有効にする（Enable Single Sign-On）] を選択します。
4. 確認メッセージで、[OK] をクリックします。
5. SSO パラメータを入力します。

シングルサインオン パラメータ	説明
[識別子フォーマット名を指定（Name Identifier Format）]	次から選択してください。 • urn:oasis:names:tc:SAML:1.1nameid-format:unspecified • urn:oasis:names:tc:SAML:1.1nameid-format:emailAddress • urn:oasis:names:tc:SAML:2.0nameid-format:persistent（デフォルト）
[SAML 2.0エンドポイント（HTTPリダイレクト）（SAML 2.0 Endpoint（HTTP Redirect））]	シングルサインオン プロバイダーから入手した SAML 2.0 エンドポイント URL を入力します。
[公開証明書（Public Certificate）]	シングルサインオン プロバイダーから受け取った証明書のテキスト全体を入力します。（コピーして貼り付けるのが最も簡単です）

6. [設定をテスト（Test Settings）] をクリックして、ID プロバイダーから提供されたエンドポイント URL と証明書の値を検証します。ドメイン保護は、指定の場所にある公開証明書認証情報で ID プロバイダーを呼び出します。

   まだログインしていない場合は、ID プロバイダーによる認証が必要です。
7. [設定の保存（Save Settings）] をクリックします。
8. 確認メッセージで、[OK] をクリックします。
9. [情報を更新（Update Information）] をクリックします。

この時点で、シングルサインオンは有効になり、次のことが行われます。

- 既存のすべてのユーザーに電子メールが届き、ドメイン保護にアクセスする際にはシングルサインオン ID プロバイダーのログイン情報を使用するように指示されます。
- ドメイン保護に現在ログインしているユーザーは、中断することなくセッションが継続されますが、今後ログインしようとすると ID プロバイダーのページが表示されます。

第 12 章

アプリケーション プログラミング インターフェイス

ドメイン保護 にはアプリケーション プログラミング インターフェイス（API）が組み込まれているため、組織内の開発者はドメイン保護 内のデータにプログラムでアクセスできます。

ドメイン保護 API のエンドポイントでは、クエリ単位で結果の量が制限されています。この制限は、APIドキュメントにエンドポイントごとに記載されています。

- ドメイン保護 API は、RESTful の原則に基づいて JSON データ表現で構築されています。
- クライアントは、OAuth 2.0 プロトコルを使用して、API リクエストを認証します。

ユーザーアカウントに、API クライアント ID とクライアントシークレットで構成される 1 つの API 認証情報を割り当てることができます。こうした認証情報で利用できるリソースとデータは、アカウント管理者がドメイン保護 ユーザーインターフェイスを使用してそのユーザーに割り当てた権限に直接結び付けられます。

Agari 開発者向けドキュメント（https://developers.agari.com/agari-platform）には、広範な情報が含まれています。ステップバイステップガイドとチュートリアルの両方があり、Agari API を対話形式で説明する完全なリファレンスとなっています。

API 認証情報の生成

ユーザーが Cisco Domain Protection API を使用できるようにするには、事前にそのユーザーの API（アプリケーション プログラミング インターフェイス）認証情報（API シークレットとも呼ばれます）を生成する必要があります。

ユーザー管理者ロールを持つユーザーのみが、API 認証情報を生成できます。

1. Cisco ドメイン保護 で、[管理者（Admin）] > [ユーザー（Users）] に移動します。
2. ユーザー名をクリックします。
3. [APIクライアントシークレット（API Client Secret）] セクションで、[API認証情報の生成（Generate API Credentials）] をクリックします。
4. API アクセス UID と認証情報を安全な場所にコピーして保存します。API をテストするときや、API 経由で Cisco 統合を使用しているときに、APIドキュメントページに入力する必要があります。

APIドキュメントの表示

ドメイン保護 API（アプリケーション プログラミング インターフェイス）ドキュメントを表示する場合は、事前にユーザーアカウントの API 認証情報を生成する必要があります。詳細については、「「API 認証情報の生成」 上」を参照してください。

1. ドメイン保護 ページの右上で、自分の名前をクリックし、[設定（Settings）] をクリックします。
2. ドメイン保護 の [APIドキュメント（API Documentation）] をクリックします。