企業がDMARCを セットアップする方法

企業が認証マーク証明書（Verified Mark Certificate：VMC）を発行できるようになるには、最初にDMARC（Domain-based Message Authentication, Reporting & Conformance）に準拠する必要があります。本書では、DMARCを正しく導入するために必要な手順について詳しく説明します。

digicert®

digicert®

DMARCとは？

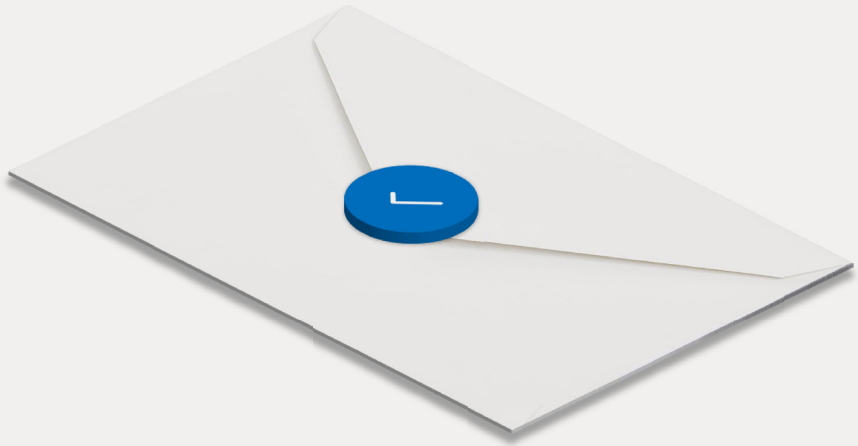
DMARCは、Eメール認証、ポリシー、およびレポートプロトコルで、これによって企業は自社のドメインがなりすましやフィッシング詐欺などに不正使用されるのを防ぐことができます。

概要

- DMARCは、DNSに保存されるTXTレコードで、Eメールの受信者が受信したメールの信頼性をチェックできるようにします。
- 企業の既存のインバウンド認証プロセスに適合し、メールがメール受信者の知る送信者と「一致」しているか判断できるようにします。
- 企業は、「不信」なメールの処理方法を3つのオプションから選択できます。

- “p = none”（何もしない）
- “p = quarantine”（隔離する）
- “p = reject”（拒否する）

- DMARCが正しく機能するには、事前にSPF（Sender Policy Framework）およびDKIM（DomainKeysIdentified Mail）プロトコルがセットアップされている必要があります。
- 企業のDMARCレコードは、既存のインターネットベースの「ツール」（例えば、valimail.com）から確認できます。



より安全なEメール認証はDMARCで始まる

DMARCの目標は、送信者と受信者が相互に連携を図り、送信者のメール認証の慣例を改善し、受信者が認証されていないメッセージを拒否できるシステムを構築することです。

digicert®

なぜDMARCなのか？

DMARCを導入することで、企業は4つの重要なメリットを享受できます。

1. セキュリティ

Eメールドメインの不正使用をブロックすることで、スパム、詐欺、フィッシングから保護します。

2. 可視性

インターネット上の誰が（何が）自分のドメインを使用してEメールを送信しているか、詳細なレポートを取得できます。

3. 配信率

配信率が5～10%向上し、EメールにSPAMのフラグが付けられるのを回避します。

4. ブランドの保護

アイデンティティをターゲットにした攻撃からブランドを保護します。

顧客の42%は、企業を装った攻撃者によるフィッシング詐欺にあった後、その企業と関わる可能性が低くなります。

digicert

SPFのセットアップ方法：

1. ドメインからEメールを送信するために使用されるIPアドレスを収集します。
   - Webサーバ
   - 社内メールサーバ
   - ISPのメールサーバ
   - サードパーティーのメールサーバ
2. **送信側ドメインと非送信側ドメインの両方のリストを作成します。**
3. **テキスト編集プログラム（Notepad ++、Vim、Nanoなど）を使用して、各ドメインのSPFレコードを.txtで作成します。**

   例1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all

   例2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all
4. **SPFをDNSに公開します。**

   DNSを管理している場合は、SPFテキストを含む新しいTXTレコードを追加するだけです。

   DNSを管理していない場合は、レコードを追加するようサーバ管理者に依頼します。
5. DNSにレコードが追加されたら、SPFチェックツールを使用して確認します。

SPFとは？

未承認の送信者による詐欺行為に遭わないようにします。

SPFは、ドメインベースのEメール認証のコンセプトを開拓した規格です。ドメイン所有者がそのドメインを名乗ってEメールを送信することを認めたサーバのIPアドレスを承認することでなりすましを防ぎます。リストにないIPアドレスのメールサーバがそのドメインを使用してメールを送信しようとした場合、SPF認証に合格しません。

digicert®

DKIMのセットアップ方法：

1. **DKIMセレクターを選択します。**
   これは、単純なユーザー定義のテキスト文字列で、ドメイン名に追加され、DKIM公開鍵（「standard」など）を識別するために使用します。

   例：“standard._domain.example.com” = ホスト名

2. **ドメイン用の公開鍵/秘密鍵ペアを生成します。**
   - Windowsユーザーは、PUTTYGenを使用できます。
   - Linux、Macユーザーは、ssh-keygenを使用できます。

3. **新しいTXTレコードを作成して公開します。**
   DNS管理コンソールから、前述の鍵ペアの公開鍵を使用して新しいレコードを作成します。

   例： v=DKIM1; p=YourPublicKey

DKIMとは？

送信中にEメールが改ざんされるのを防ぐ

DKIMは、公開鍵/秘密鍵暗号を使用して、Eメールメッセージに署名するためのメール認証基準です。

DKIMを使用して、EメールがDKIM鍵の関連付けられたドメインから送信されたこと、さらに送信中に変更されていないことを確認します。

DMARC監視モードのセットアップ

1. **SPFとDKIMが正しくセットアップされていることを確認します。**
2. **DNSレコードを作成します。**

   DMARC “TXT”レコードの名前は、「_dmarc.your_domain.com」のようにする必要があります。

   例：“v=DMARC1;p=none; rua=mailto:dmarcreports@your_domain.com”

   ドメインのDNSを管理している場合は、SPFやDKIMレコードと同様に「p=none」（監視モード）のDMARCレコードを作成します。

   DNSを管理していない場合は、DNSプロバイダーにDMARCレコードの作成を依頼します。
3. **DMARCチェックツールを使用してDMARCレコードをテストします。**

   注意：通常、レプリケーションに24～48時間掛かります。
   DMARCチェックツール

digicert®

DMARC監視モードとは？

ドメインから何が送信されているかを可視化できます。

レポートモードにすると、ドメイン所有者はそのドメインに関するEメールのトラフィックを含むDMARCレポートを確認できます。

このレポートでは、DMARCが完全な適用モードになったときに、隔離または拒否される可能性のある失敗メッセージを識別します。さらに、DMARCレポートには、監視対象のドメインからEメールを送信しているすべてのシステムとサービスに関する情報が表示されます。

注意：監視モードでは、どのレベルの適用もできません。認証に失敗したメールは正常に配信され、DMARCの実装中に潜在的な混乱を回避できます。

digicert®

DMARC .TXTレコードに使用される一般的なタグ

タグ名	必須/省略可	意味
V	必須	プロトコルのバージョン
P	必須	プロトコルのバージョン
PCT	省略可	フィルターの対象になるメッセージの割合（%）
RUA	省略可	集計結果のレポートURI
SP	省略可	そのドメインのサブドメインに関するポリシー

digicert®

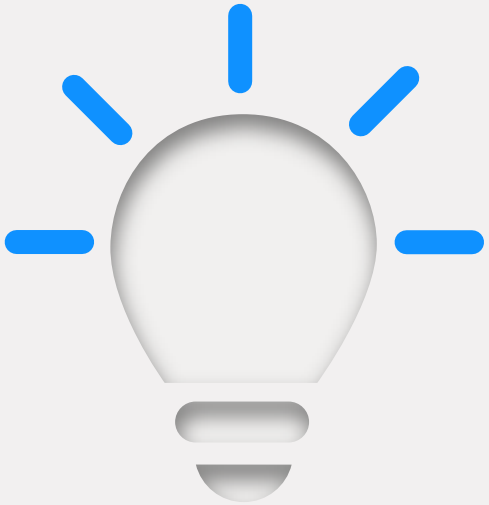
DMARCレポートが提供するのはどのような情報か？

このレポートは、どれだけ多くの詐欺メッセージがそのドメインを使用しているか、そのメッセージの送信元はどこか、さらにDMARCの「隔離」または「拒否」ポリシーによって阻止されたかどうかをドメイン所有者に示します。

各受信者からのレポートは、XMLファイルで、次のフィールドで構成されています。

- 各IPアドレスからのメッセージ数
- これらのメールがDMARCポリシーによってどのように処理されたか
- これらのメッセージに対するSPFの結果
- これらのメッセージに対するDKIMの結果

XMLレポートは表示できますが、そのままでは不便です。ドメイン所有者は、Valimailまたはその他のDMARCサービスプロバイダーのDMARCレポートプロセッサを使用してください。



DMARCレポートを使用する4つの方法

適用を開始する前に適切なベースラインを取得します。

1.不適切とマークされたトラフィックを識別します。

2.DMARCによって不適切のフラグを付けられた適切なEメールを探します。適用を開始すると、ポリシーによっては、これらのメールが「拒否」または「隔離」される可能性があります。

3.不適切というフラグが付けられたEメールの正当性を明確にするために、可能性のあるシステム/アプリケーションの所有者と連絡を取ります。

4.必要に応じて、これまで含まれなかった正当なIPアドレスの許可リストを作成しSPFレコードを更新します。

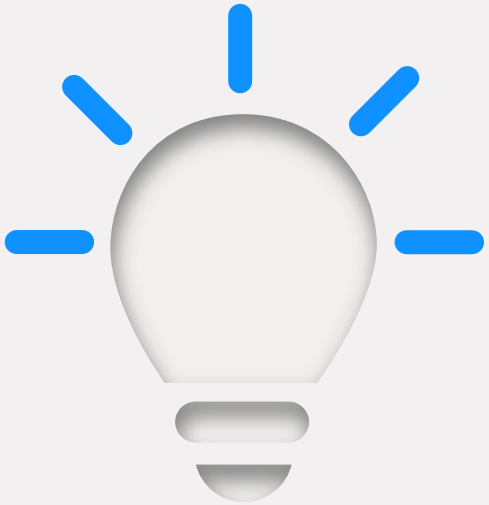
適用する前にDMARCレポートを使用して環境を整える

DMARCレポートの分析には時間が掛かります。しかし、ドメイン所有者が送信者を見過ごしたり、誤認したりした場合、DMARCポリシーが適用に設定された時点で「正当」なメールをブロック（「隔離」または「拒否」）する可能性があり、その結果さらに時間のかかる問題が発生して、業務を妨げることになるかもしれません。

その代わりに、DMARCの適用を開始する前にいくつかの内部タスクを行うことをお勧めします。

- DMARCレポートで特定されたすべてのEメール送信者と関係者から指摘された他のすべての送信者のリストを作成します。
- 各サービス/Eメール送信者の所有者を特定します。
- 送信サービスを、承認、未承認、悪意があるのいずれかに分類します。
- DMARCレポートに表示されない可能性のある送信者が他にもいるかどうかを関係者の協力を得て特定します。
- 新しい送信者を識別するたびに、関係者に連絡します。
- 新しく正当なEメール送信者のIPアドレスが見つかるたびに、SPFレコードを更新します。

digicert®



適用前コミュニケーションの推奨

より良い導入のための5つのヒント

- 関係者と共有する実装ポリシーを文書化する。
- DMARCタスクが処理できないほど大量であったり、支援が必要な場合は、ValimailなどのDMARCサポートプロバイダーに連絡する。
- DMARCレポートから得た新しい結果は使用可能になり次第通知する。
- 内部プロジェクトとしてDMARCの実装を開始する。
- 経営陣をプロジェクトのメインスポンサーにする。

DMARCを監視モードにしておく期間は？

この期間は、企業ごとに異なります。一般に、大規模な企業の方が小規模な企業よりも長い時間が掛かります。数週間から数か月の計画を立てましょう。

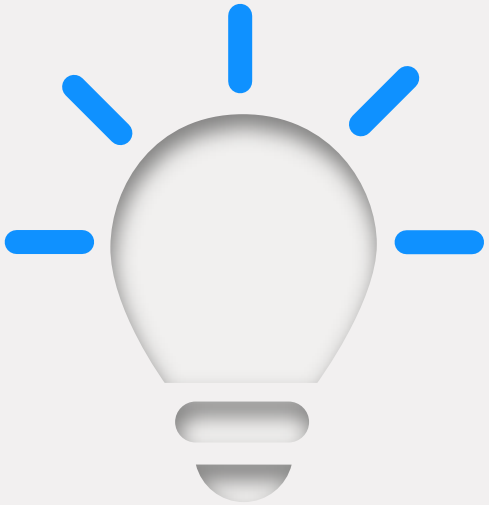
リストが完成し、承認された送信者がすべてマッピングされて、十分な情報が得られたら、検疫フェーズに移行する準備ができています。

検疫モードをオンにすると、認証に失敗したメッセージは隔離されます。通常、このメッセージはユーザーのスパムフォルダーに送られます。

DMARCの検疫の適用をセットアップする方法

1. **DNSサーバにログインし、DMARCレコードを検索します。**
2. **目的のドメインに関するDMARCレコードを開き、ポリシーを「p=none」から「p=quarantine」に更新します。**
   例：“v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@you_domain.com”
3. **フラグ「pct」（フィルターの対象になるメッセージの%）を追加します。10%から始めることをお勧めします。**
4. **フィルターされるメッセージの割合を徐々に上げていき、より安心できるようになってきたら、「pct=100」（100%）にします。**

注意：BIMIおよび認証マーク証明書標準を満たすには「pct=100」にする必要がありますが、独自のポリシーは「隔離」または「拒否」にすることができます。



フラグの働き：

- 「p=none」以外のポリシーが指定されている場合、そのポリシーは、「pct」フラグの割合に適用されます。
- 次に制限の少ないポリシーが残りに適用されます（例えば、「p=quarantine」および「pct=10」のDMARCレコードの場合、失敗したトラフィックの10%は隔離され、他の90%は正常に配信されます）。

フィルタリングが100%に到達したら、適用の最高レベルである「P=REJECT」に移行する準備ができています。

digicert

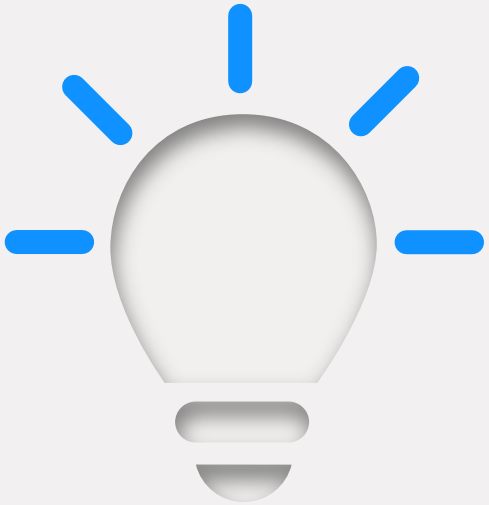
DMARCの拒否ポリシーのセットアップ方法

1. **DNSコンソールを使用してDMARCレコードを開きます。**
2. **「p=quarantine」から「p=reject」に変更します。**
   例：“v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports@you_domain.com
3. **レコードを保存します。**

ヒント：正当なEメールが拒否されたり削除されたりしないことを保証するために、この段階で監視を続けていることが特に重要です。

他に質問がありますか？今すぐcontactus@digicert.comに電子メールを送信するか、https：//www.digicert.com/jp/tls-ssl/verified-mark-certificates/にアクセスしてください。

© 2021 DigiCert, Inc. All rights reserved.DigiCertは、米国およびその他の国における DigiCert, Inc.の登録商標です。その他の商標および登録商標は、それぞれの所有者に帰属します。



拒否ポリシーはEメールにどのように作用するのか？

DMARCチェックに失敗したすべてのメッセージ（認証されないEメール）は、ブロック/削除され、メールの受信者がそのコピーを受け取ったり、削除されたことに気づくことはありません。