DKIM を設定して メールのなりすましを防ぐ方法

DKIM とは何か？

DKIM（DomainKeys Identified Mail）は、電子署名を用いて送信ドメインの認証をおこなう仕組みです。

攻撃者はメールコンテンツを改変 (例えば振り込み依頼であれば攻撃者の口座情報に変更) し、受信者をだますことがあります。DKIM を使用することで、受信側がコンテンツが改ざんされていないかを検証することができます。

送信者は、電子メールのどの要素を署名プロセスに含めるかを決定します。メッセージ全体（ヘッダーと本文）を含めるか、電子メールヘッダーの 1 つ以上のフィールドだけに集中するかを決めることができます。DKIM 署名の対象要素が転送中に変更された場合、DKIM 署名は認証に失敗するため、改ざんを検知することができます。

しかし、DKIM だけではメールのなりすましを効果的に防ぐことはできません。そのため、DKIM とともに、DKIM で検証されたメール送信元が、ユーザーが目にする送信者メール (MAIL FROM) と同一かを検証する DMARC と併用することを奨励しています。

DKIMとDMARC の組み合わせのほかに、SPF と DMARC の組み合わせによるメールなりすまし対策も効果的です。

DKIM の設定手順

ステップ 1: すべての送信ドメインを特定する

すべての送信ドメインのリストを作成し、メールの送信に以下のどれが使用されているかを確認してください。

- Web サーバー
- 社内のメールサーバー（Microsoft Exchange など）
- ISP のメールサーバー
- 自社のブランドに代わってメールを送信するために使用される他のメールサーバー

ステップ 2: メールサーバーに DKIM をインストールして設定する

すべての送信メールを DKIM で署名する必要があるため、自社のメールサーバーに専用の DKIM パッケージをインストールする必要があります。利用中のプラットフォームに対応した DKIM ソフトウェアがあるかどうかを確認するには、DKIM.org をチェックするか、ベンダーに確認してください。電子メールサービスプロバイダーを使用している場合は、DKIM レコードの設定時に彼らと協力して作業する必要があります。

ステップ 3: 公開鍵と秘密鍵のペアを作成する

オンラインウィザードまたはメールサーバー独自の鍵生成プログラムを使用して、DKIM 公開鍵 / 秘密鍵ペアとポリシーレコードを作成します。公開鍵は DNS レコードに含めて公開され、秘密鍵は MTA/ 電子メール送信システムにインストールされます。openssl を使って自身で鍵を作成することもできます :

- 認証する From: ドメインを入力します。
- セレクタ名を入力します。この名前は、「marketing」や「newsletter」など、送信するメールの種類を表すものにします。
- また、鍵長が 1024 ビット以上であることを確認してください。ほとんどのプロバイダーにはこれ以下のオプションはありませんが、自身のツールを使用している場合は 1024 ビット以上に設定します。

ステップ 4: 公開鍵を公開する

DKIMウィザードでセレクタレコードが表示されます。このレコードには、ドメインとセレクタ名の組み合わせである公開鍵を格納するDKIMサブドメインが含まれます。

たとえば、marketingのセレクタを持つdomain.comの公開鍵は、marketing._domainkey.domain.comに格納されます。その公開鍵を、ドメインのTXTレコードとして登録します。ほとんどのユーザーは、システム管理者と協力してこれを公開する必要があるでしょう。ホストされたソリューションを使用している場合は、管理インターフェース内でこれを設定できます。

ステップ 5: 秘密鍵を保存する

秘密鍵はウィザードによって生成されるため、DKIM パッケージで指定されている場所に保存する必要があります。この秘密鍵は、絶対に誰かと共有したり、流出させたりしないようにして下さい。さもなければ、セキュリティが損なわれてしまいます。

ステップ 6: メールサーバーを設定する

合併や買収が行われると、新しい従業員が急増し、重要なリソーシステムを適切に構成する必要があります。サーバーのインストール手順を参照するか、ベンダーに問い合わせてください。

ステップ 7：テスト実行

システム上ですべての設定が正常に完了した場合、次のステップはテストです。

鍵または鍵ペアが侵害された場合に備えて、できる限りの対策としてキーローテーションを検討する必要があります。

プルーフポイントは、6 ヶ月毎のキーローテーションをお勧めしています。適正に認証を維持したい場合、プルーフポイントに連絡して下さい。DKIM 署名の管理をお手伝いします。

詳細は proofpoint.com/jp でご確認ください。