SPF を実装して メールのなりすましを防ぐ方法

SPF とは何か？

SPF（Sender Policy Framework）はメール送信ドメインの認証技術のひとつで、送信者のドメインの詐称を防ぎ、送信ドメインの正当性を検証することができます。

SPF により、ドメインの所有者がそのドメインからメールを送信するために使用するメールサーバーを指定することができます。電子メールを送信する企業は、ドメインネームシステム（DNS）で SPF レコード（TXT RR）を発行します。このレコードリストには、そのドメインを利用して電子メールを送信することが許可されている IP アドレスが含まれています。

電子メールの受信者は、DNS 内の「envelope from」（Mail From、Mfrom、return-path などとも表記）ドメイン名を調べて SPF レコードを検証します。このドメインを利用して電子メールを送信している IP アドレスが SPF レコードに記載されていない場合、そのメッセージは SPF 認証に失敗します。

SPF で保護されたドメインは犯罪者にとって魅力的でなくなるため悪用されることが少なくなり、結果としてスパムフィルタによってブラックリスト化されにくくなります。

メール詐欺は、送信元を詐称して送られることが多いため、送信元の IP アドレスの正当性を検証することが重要になります。SPF は他の送信ドメイン認証方式に比べて、既存システムに影響を与えずに早期に導入することができる技術です。

SPF で認証された送信元とユーザーが目にする送信者メール（HEADER FROM）と同一かを検証する DMARC と併用することにより、さらに効果的になりすましメールを阻止することができます。

SPF の実装手順

ステップ 1: 電子メールを送信するために使用されている IP アドレスを収集

自社のドメインからメールを送信するために使っているメールサーバーを特定します。（Web サーバー、オフィス内のメールサーバー、ISP のメールサーバー、サードパーティのメールサーバーなど）これは意外に難しい作業になる可能性がありますので、DMARC レポートを利用することをお勧めします。詳しい情報は、このキットに含まれる DMARC テンプレートを参照してください。

ステップ 2: 送信するドメインのリストを作成

企業では多くのドメインを所有している可能性があります。これらのドメインのいくつかは、電子メールを送信するために使用されており、その他はそうではありません。

自社が管理するすべてのドメインで SPF レコードを作成することが重要です。非送信ドメインも同様です。何故でしょう？ サイバー犯罪者があなたの送信ドメインが全て SPF で保護されていることを確認した後にまず行う事は、非送信ドメインを偽装しようとすることだからです。

ステップ 3:
自社の SPF レコードの作成

正当な送信者を認証するために、v = spf1（バージョン 1）タグの後に IP アドレスを記載してください。

たとえば : v=spf1 ip4:1.2.3.4 ip4:2.3.4.5

自社のドメインに代わって電子メールを送信する第三者を認証したい場合は、SPF レコードに自社の IP アドレス、A レコードまたは「include」ステートメントを追加する必要があります。（include:thirdparty.com など）すべての認証 IP を追加した後、レコードの最後に HardFail の場合には -all、SoftFail の場合には ~ all タグを追加します。Proofpoint ではそれが最も安全であるとの理由から、-all タグを推奨しています。

SPF レコードは、長さが 255 文字を超えることはできません。また、10 個以上の追加の DNS ルックアップを含む事もできないため、注意してください。以下はレコードの例です :

v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all

電子メールを送信しないドメインでは、SPF レコードは -all を除いて、全ての修飾子を除外します。以下は非送信ドメインのレコード例です。

v=spf1-all

ステップ 4:
DNS に SPF を公開

メールボックスプロバイダから参照できるように、DNSサーバーの管理者と協力してenvelope fromドメインのSPFレコードをDNSに公開します。もし123-regやGoDaddyのようなホスティングプロバイダを使用している場合は、このプロセスは非常に簡単です。

もしDNSレコードがISPによって管理されているか、またはよくわからない場合は、IT部門に連絡してサポートを依頼して下さい。

一般的には、特定のDNSロケーションのコントロールがメールサービスプロバイダに委任されている場合、彼らが御社に代わってドメインを送信するためのSPFレコードを公開します。

詳細は proofpoint.com/jp でご確認ください。