

SPF レコードでメールのなりすましを防止する

組織のドメインが偽装メールに利用されないように対策をする

送信元のドメインを偽ってメールを送る行為は「なりすまし」と呼ばれます。組織で使用しているドメインホストに Sender Policy Framework (SPF) レコードを設定しておくことで、メールが正規の送信元から届いたものであり、なりすましでないことを受信者に確認してもらうことができます。

G Suite のお申し込み時にドメインを Google パートナー (GoDaddy.com、eNom.com、DomainDiscount24.com) から購入されたお客様は、SPF レコードの設定が不要な場合があります。詳しくは、[ドメインホストによって管理される設定](#)をご覧ください。

ドメインホストに SPF TXT レコードを追加する

ドメインホストには、ウェブトラフィックをドメインに対応付けるテキスト情報 (DNS レコード) が登録されています。SPF TXT レコードにはドメインからのメール送信が許可されているメールサーバーが登録されており、ここに含まれていないサーバーから届いたメールは、受信サーバー側で迷惑メールとみなされる可能性があります。

メモ: ドメインに設定できる SPF レコードは 1 つだけですが、そのレコードに複数のサーバーを登録できます。詳しくは、[SPF レコードに複数のサーバーを登録する](#)をご覧ください。

1. (Google 管理コンソールではなく) ドメインホストでドメイン アカウントにログインします。
2. ドメインの DNS レコードの更新を行うページに移動します。
「DNS 管理」、「ネームサーバー管理」、「詳細設定」といったページを探してください。
3. TXT レコードを探し、ドメインに SPF レコードが設定されているかどうかを確認します。
SPF レコードは「v=spf1」で始まります。
4. ドメインに SPF レコードが設定されている場合は削除します。設定されていない場合は、手順 5 に進みます。
5. 次の値を使用して TXT レコードを作成します。
 - **名前 / ホスト / エイリアス** - 「@」と入力するか、空白のままにします。
ドメインに設定されている他の DNS レコードを参考に入力してください。
 - **有効期間 (TTL)** - 3600 と入力するか、デフォルトのままにします。
 - **値 / 応答 / 参照先** - v=spf1 include:_spf.google.com ~all と入力します。
6. レコードを保存します。

ここで設定した SPF レコードが 48 時間以内に有効になります。