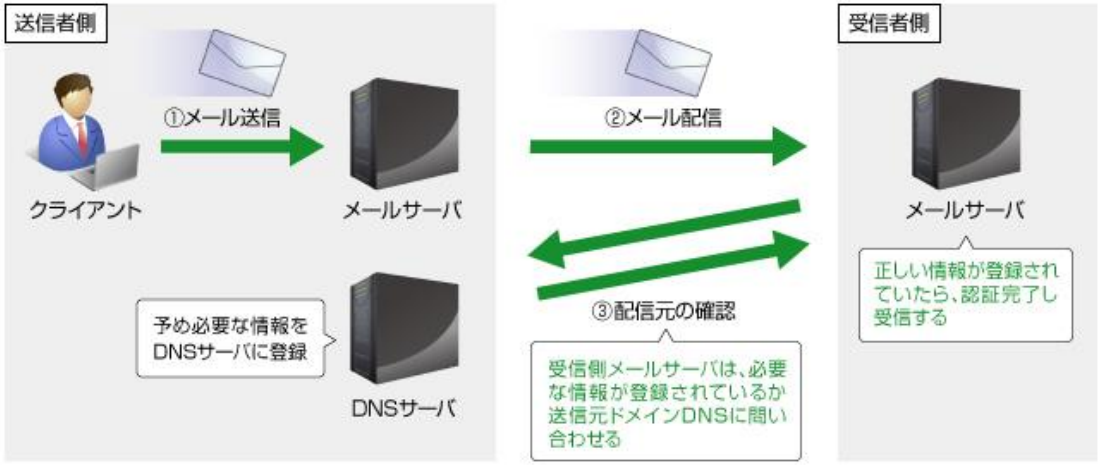
SPF（Sender Policy Framework）とは

メールの送信元ドメインが詐称されていないかを証明するための、インターネット技術標準（RFC）で定められる仕組みです。
メールの受信者側において、送信者側IPアドレス（サーバー）から来たメールは、送信者側ドメインから来た正常なメールであるかを確認するために用いられます。
SPFは、標的型攻撃メールや迷惑メールなどの「なりすましメール」の流通を抑止するための有効な手段の一つとされ、近年導入が強く推奨されています。



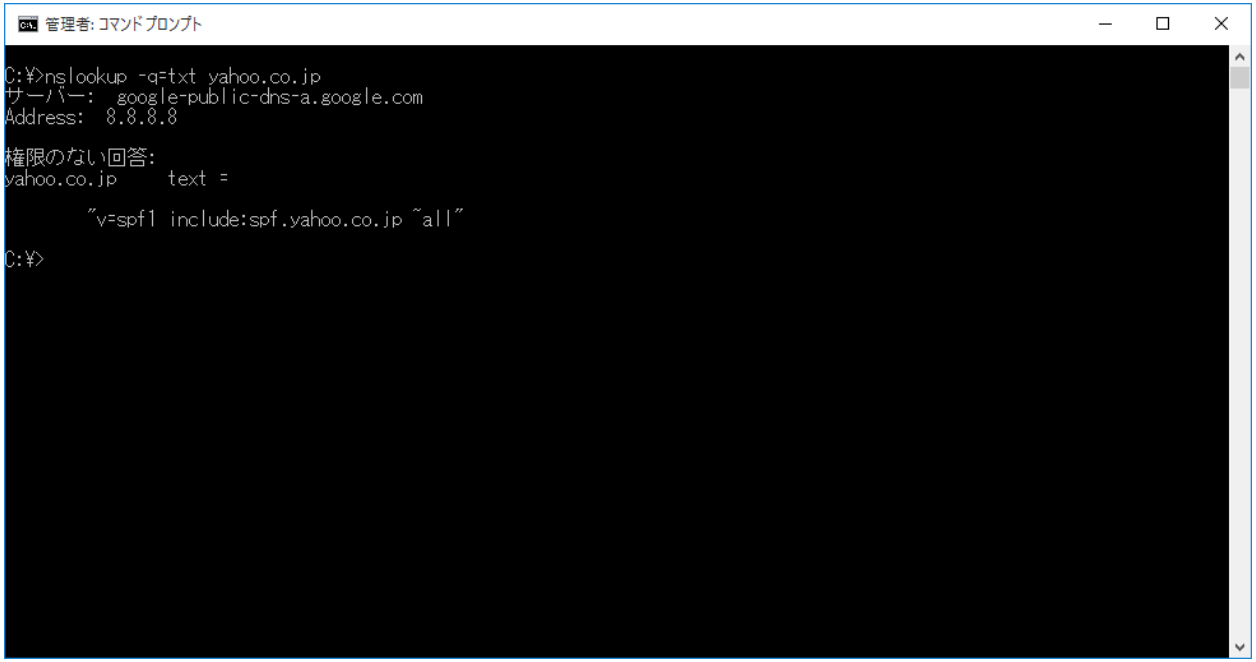
SPFの確認方法

■ 「Mailセキュリティ・クラウド」をご利用頂くにあたっては、DNSサーバでSPFレコードの追加登録が必要な場合がございます。
以下の手順に従いSPFレコードの追加登録可否をご確認ください。

コマンドプロンプトを起動して、下記コマンドを入力します。
nslookup -q=txt 【お客様ドメイン】

【例】：お客様ドメインが example.co.jp の場合
nslookup -q=txt example.co.jp

画面イメージ



Mailセキュリティ・クラウド ご利用にあたって

◆ 前項のコマンドの結果により、Mailセキュリティ・クラウドの利用可否が判明します

■「Mailセキュリティ・クラウド」をご利用いただくことが、不可のパターン

コマンドの結果で「v=spf1 include: ・・・ ~all（もしくは-all）」が表示される場合は、
SPFレコードが有効です。

【例】：お客様ドメインが example.co.jp の場合
exsample.co.jp text ="v=spf1 include: ・・・ ~all（もしくは-all）“

現行設定で「Mailセキュリティ・クラウド」をご利用頂くことは不可となります。
弊社サービスから中継されたメールは「なりすましメール」と判断され相手先から受信を拒否される可能性があります。
「サービス登録完了書」に記載されたSPFレコードを追加登録することで、正常なメールであると証明され受信が可能となります。

■ 「Mailセキュリティ・クラウド」をご利用いただくことが、可能なパターン

コマンド結果に「v=spf1 include:・・・ ~all（もしくは-all）」のような表示がされなければ、
SPFレコード追加登録の必要はありません。

現行の設定で「Mailセキュリティ・クラウド」をご利用頂くことが可能です。
ただし、今後SPFレコードを有効化する際には追加登録が必要となります。

総合情報漏えい対策ソリューション・ガーディアンウォール

GUARDIANWALL

製品情報　https://canon.jp/business/solution/it-sec/lineup/guardianwall

お問い合せ　https://canon.jp/business/solution/it-sec/lineup/guardianwall/contact