送信ドメイン認証 標準装備

送信ドメイン認証は、メール送信者情報の「なりすまし」の有無をドメイン単位で判別し、認証する仕組みです。
共用レンタルサーバーでは、以下送信ドメイン認証が設定されています。

SPF Sender Policy Framework

メールの送信元サーバーのIPアドレスと照合し、一致することで、正当な送信元であることを認証する仕組みです。
送信元となるサーバーのIPアドレスや、IPアドレスにひもづいているホスト名の情報をDNSサーバーに TXTレコードで設定します。
CPIでは、提供しているサーバーやサービスに関するIPアドレスを内包する標準SPFを設定しています。

DKIM Domainkey Identified Mail

送信するメールに電子署名(秘密鍵)を付与し、DNSに設定されている公開鍵を用いて、認証する仕組みです。
CPIのメールサーバーで発行する電子署名(秘密鍵)に対する公開鍵を、標準でDNSに設定しています。

DMARC Domain-based Message Authentication, Reporting, and Conformance

SPF, DKIMで判定された結果にもとづいて、総合的に送信ドメインを認証する仕組みです。
判定した結果にもとづいて、送信メールの取り扱い（ポリシー）を「受領」「隔離」「拒否」の中から指定します。
CPIでは、ポリシーを"受領"としているDMARCを標準で設定しています。

対象プラン

● 標準装備

	ビジネス スタンダード
SPF	●
DKIM	●
DMARC	●

ご注意事項

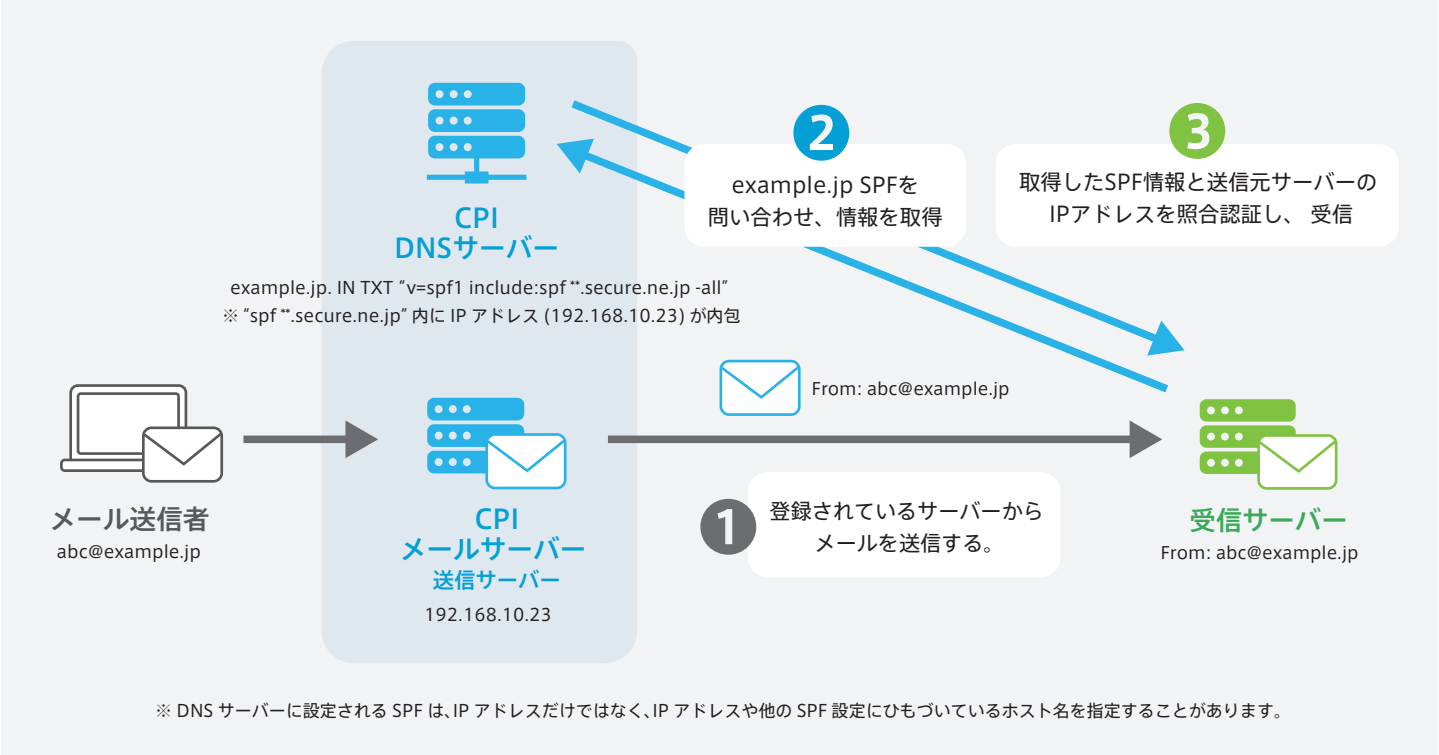
- CPI のメールサーバーご利用時のみ設定可能。
- CPI の DNS サーバーをご利用の場合において、標準で設定されます。
- CPI 以外の DNS サーバーへの設定も可能です。設定内容につきましてはお問い合わせください。
- CPI の DNS サーバーをご利用で、CPI 以外で発行した送信ドメイン認証 (SPF、DKIM、DMARC) の 設定をご希望の場合は、別途 DNS サーバーレンタルのご契約が必要となります。

SPF 標準装備

メールの送信元サーバーのIPアドレスを照合し、一致することで、正当な送信元であることを認証する仕組みです。
送信元となるサーバーのIPアドレスや、IPアドレスにひもづいているホスト名の情報を
DNSサーバーに TXTレコードで設定します。

仕組み

① SPFに登録されている送信メールサーバーよりメールを送信する。
② 受信サーバーにて、受信したメールの送信元メールアドレスに関するSPFレコードをDNSサーバーに問い合わせる。
③ 送られてきたメールの送信サーバーのIPアドレスと、問い合わせで取得したSPF情報を照合し、一致することで受信する。



※ DNS サーバーに設定される SPF は、IP アドレスだけではなく、IP アドレスや他の SPF 設定にひもづいているホスト名を指定することがあります。

CPIにおけるSPF

- CPIの標準SPFは、CPIで提供しているサーバーやサービスに関するIPアドレスを内包した設定になっています。
- CPIレンタルサーバーにて、CPIのDNSサーバーを利用する申告をいただいた場合に、標準として設定します。
- CPIにおける標準SPF設定は、外部のDNSサーバーご利用時においても設定可能です。
  詳細な設定内容につきましてはお問い合わせください。

ご注意事項

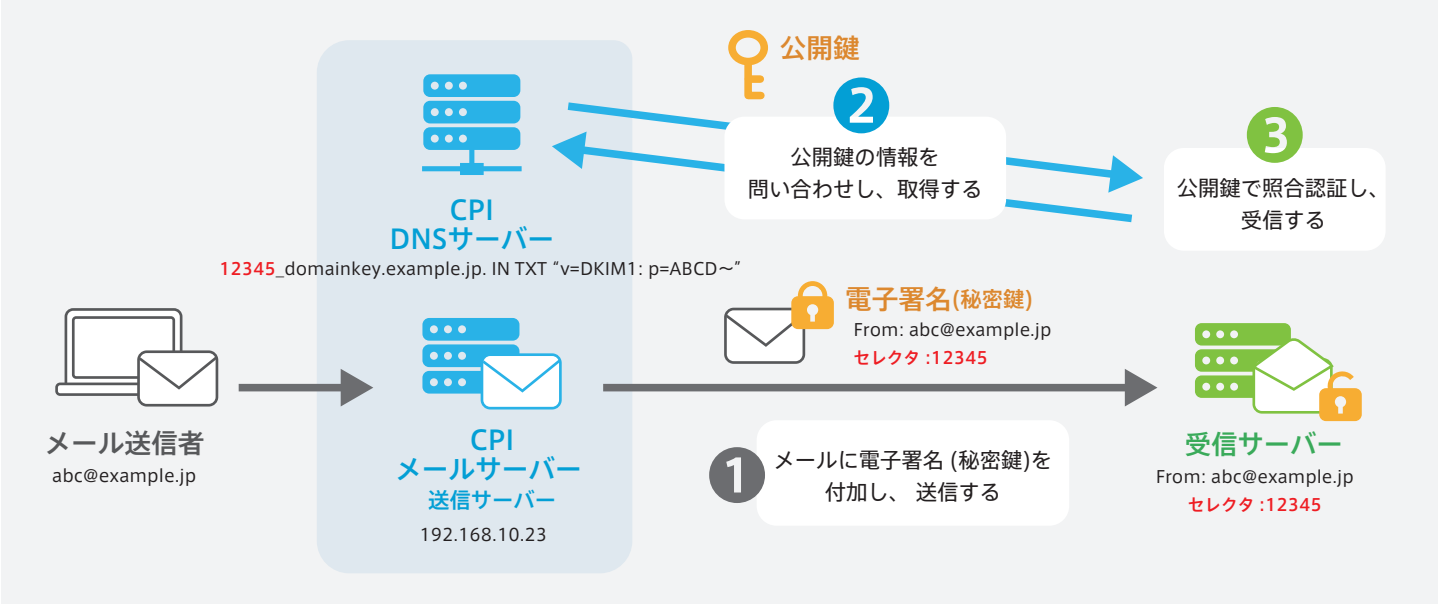
- CPIにおける標準SPF設定は、CPIサーバーより送信したメールに対して、有効な設定となります。
  CPI以外のサーバーより送信したメールは、CPIの標準SPFの適用外となります。

DKIM Domainkey Identified Mail 標準装備

送信するメールに電子署名(秘密鍵)を付与し、DNSに設定されている公開鍵を用いて、認証する仕組みです。
送信メールサーバー側に電子署名(秘密鍵)の発行機能を有していることが必須となります。
ドメインまたは、送信サーバー（メールサービス）ごとに、電子署名(秘密鍵)と公開鍵の情報が異なります。

仕組み

① 送信メールサーバーにて、電子署名(秘密鍵)を付与し、メールを送信する。
② 受信サーバーにて、送られたメールに関する公開鍵をDNSサーバーに問い合わせる。
③ 取得した公開鍵とメールに付与された電子署名(秘密鍵)を照合・認証して、メールを受信する。



CPIにおけるDKIM

メールサーバー

- CPIメールサーバーにて、電子署名 (秘密鍵) をつけて送信します。

DNSメールサーバー

- CPIメールサーバー専用のDKIMは、標準として、CNAMEレコードで設定します。
  ※ CNAME レコードで指定のホスト名で、公開鍵を設定してあります。
- CPI 以外の DNS サーバーをご利用の場合も設定可能です。詳細な設定内容につきましてはお問い合わせください。

ご注意事項

- CPIにおけるDKIM設定は、CPIメールサーバーからの送信時のみ有効となります。
  CPI以外のメールサーバーから送信されたメールは、CPIにおけるDKIM設定の適用外となります。
- 現在CPIにおいては、共用レンタルサーバー(ビジネス スタンダード)にのみDKIMに対応しております。
  共用レンタルサーバー(ビジネス スタンダード)以外のプランには対応しておりません。

DMARC Domain-based Message Authentication, Reporting, and Conformance 標準装備

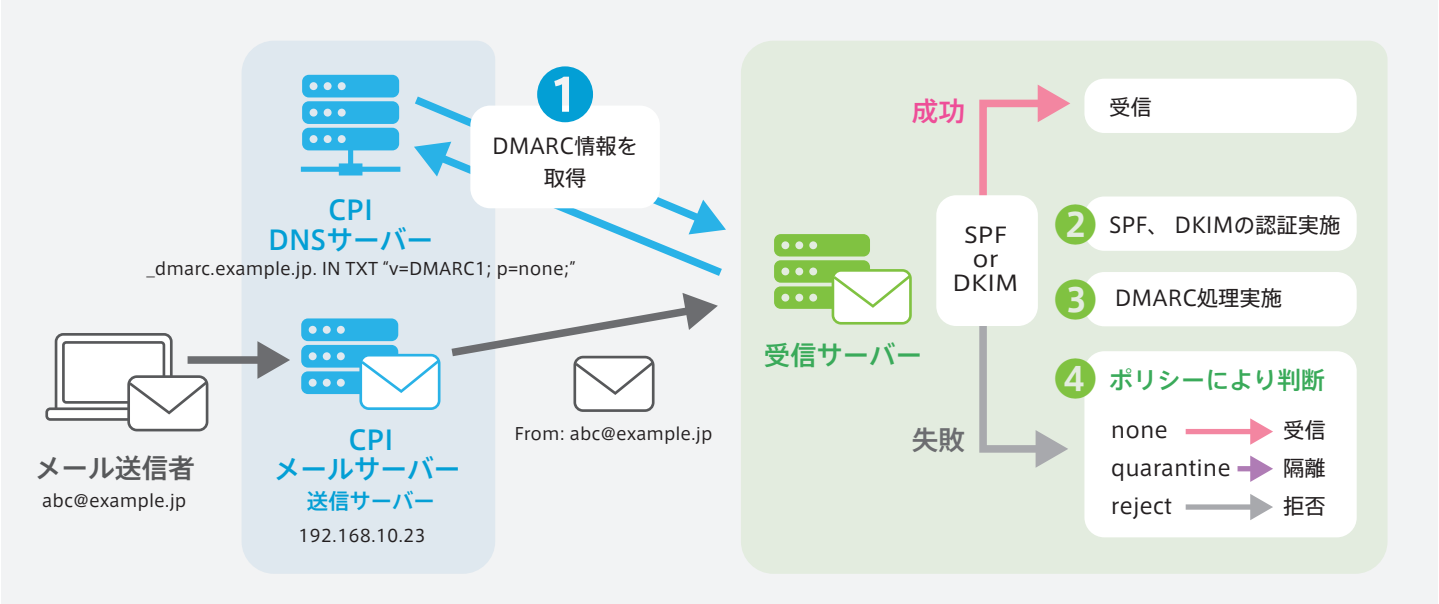
SPF、DKIMで判定された結果にもとづいて、総合的に送信ドメインを認証する仕組みです。
判定した結果にもとづいて、送信メールの取り扱い（ポリシー）を「受領」「隔離」「拒否」の中から指定します。
設定によっては、認証結果のレポートをメールで送信することも可能です。

仕組み

① DMARC の情報を DNS サーバーに問い合わせる。
② SPF、DKIM の認証を実施する。
③ SPF、DKIM の認証結果を基に DMARC 処理を実施する。
④ SPF、DKIM 認証が Fail(失敗) の場合、DMARC 設定の ポリシーによって、メールの取り扱い　(「受領」「隔離」「拒否」) を判断する。

ポリシー

- none　：そのままメールを受信
- quarantine　：受信サーバーの方式に従って、隔離
- reject　：メールの受信を拒否



CPIにおけるDMARC

- CPIにおける標準のDMARCは、以下のようにポリシー "none"(受領)で設定されます。
  例) _dmarc.example.jp. IN TXT "v=DAMRC1; p=none;"
- CPIの標準設定では、レポート送信設定等は行っていません。

ご注意事項

- CPIの標準設定では、ポリシー"none" (受領)のみが設定されます。レポート送信等、その他の設定はおこないません。
  レポート送信設定等の設定をご希望の場合は、別途、DNSサーバーレンタルのご契約が 必要となります。
- DMARCのレコードは、ドメイン名ごとに1つまでの制約があります。
  すでにDMARCレコードが設定されている場合、CPIにおける標準設定はいたしません。