

第8章

利用者への周知





第 8 章 利用者への周知

メールを利用する際に、多くのエンドユーザはメールのなりすましを意識することは少ないと想定されます。しかし、エンドユーザが意識しないところで、送信ドメイン認証技術による影響を受ける可能性があります。

本章では、エンドユーザに、最低限意識して欲しいことについて解説します。

8.1 送信ドメイン認証技術とは

送信ドメイン認証技術とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術です。

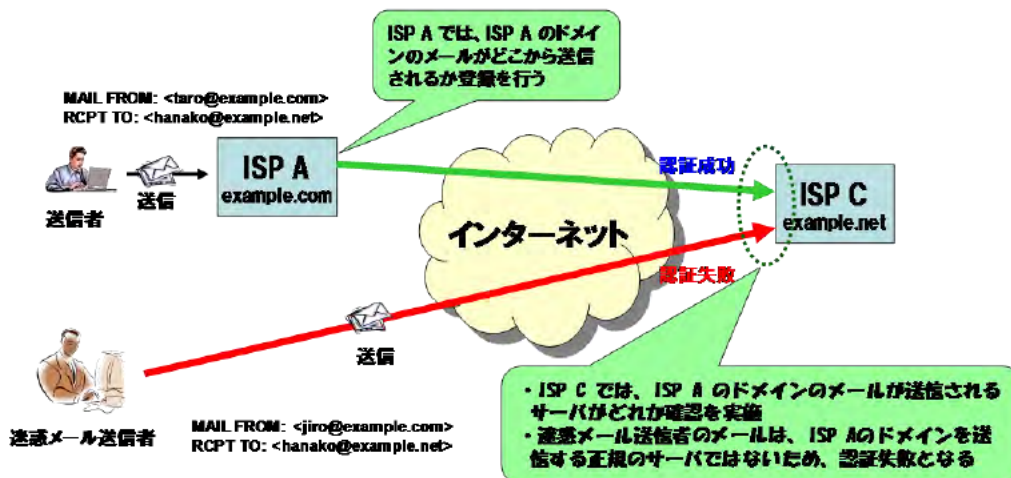
メールを普通郵便に例えるならば、送信ドメイン認証技術を用いたメールは、書留郵便のようなものと考えられます。ただし、決定的な違いは、郵便では、送信者が書留を意識して送信するのに対して、送信ドメイン認証技術では、送信側の該当ドメインのドメイン管理元で送信ドメイン認証技術を導入すれば、送信者が意識しなくても、送信ド

メイン認証技術に対応したメールとなることです。

しかし、書留郵便と異なり、送信ドメイン認証技術では、たとえ送信側で送信ドメイン認証技術を導入しても、受信側が対応していなければ、そのメールは、送信ドメイン認証技術に対応したメールとして受信されません。

エンドユーザは、各 ISP / ASP が提示する設定方法にしたがって利用していれば、意識しなくても、基本的には問題が発生することはありません。しかし、自分が利用しているメールについて、送信ドメイン認証技術を意識しないと問題が発生する場合もあるため、これらについて、以下で説明いたします。

なお、各 ISP / ASP が提供する迷惑メール対策のサービスには、本技術を用いたものも存在するため、迷惑メールに困っている場合は、サービスの内容を確認することも重要です。



図表 8-1 送信ドメイン認証技術の概要

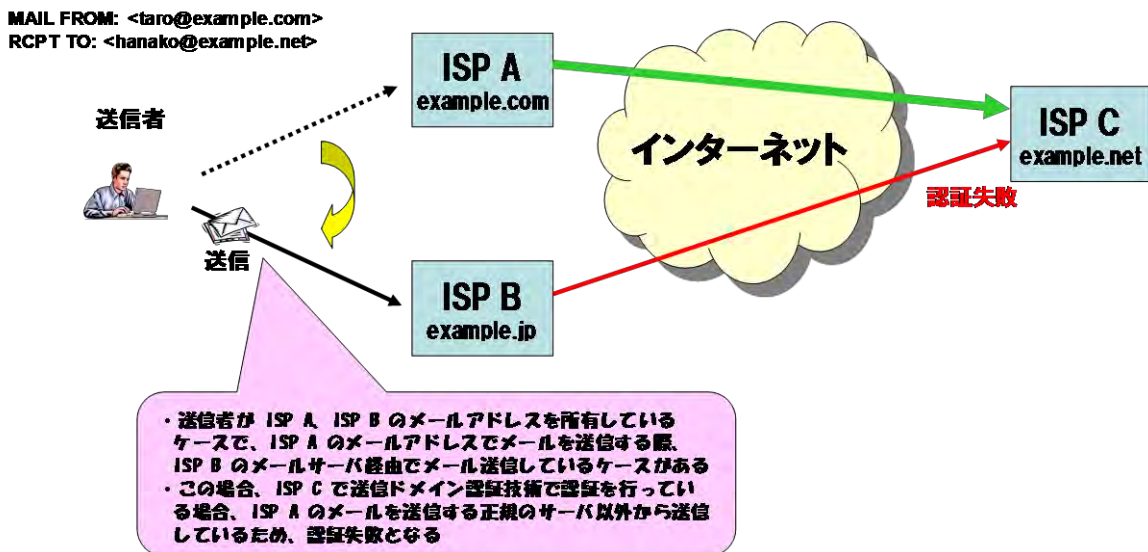
8.2 送信時の注意事項

多くのエンドユーザは、メールの送信時に、送信に用いるメールアドレスを偽装する（なりすます）ことはないと思定されます。しかし、会社などのアドレスを用いて、自宅から自分が契約している ISP 経由で送信すること等も想定されます。そのような送信方法は、厳格な管理を行う企業などでは禁止している場合が多いと思定されますが、実際にはメールクライアントソフトの設定を変更するだけで送信可能な場合もほとんどであり、事実としてこの利用方法は多数利用されているのが現実です。

このような場合に、送信に用いたメールア

ドレスのドメインが送信ドメイン認証技術に対応している場合、そのメールはそのドメインのメールを許可されているサーバ以外からの送信となり、受信側でも送信ドメイン認証技術に対応していると、そのメールは送信者情報を偽装した（なりすました）メールと判定されます。仮にそう判定されると、受信側の機能によっては、該当のメールがフィルタリングされ、受信者に到達しない場合もあります。

したがって、このような方法でのメール送信は行わないことが賢明です。なお、このような事態を回避するために、一部のメールクライアントでは、“Sender アドレス” というものが設定できます。



図表 8-2 外部メールサーバ利用時の注意事項

第8章 利用者への周知

8.3 受信時の注意事項

送信ドメイン認証技術で認証されたメールは、あくまでも、送信されたメールアドレスのドメインのメールを許可された送信されたことが確認されているだけです。その内容まで信頼できる訳ではありません。したがって、送信されたメールの内容や送信者のアドレスを見て、問題ないメールか判断することが重要です。そのため、迷惑メール対策として利用する場合には、内容に基づくフィルタリングサービスなど、他のサービスと組み合わせる活用することが重要です。

迷惑メールの対策として、一部の ISP では、送信ドメイン認証技術を用いたフィルタサービスを提供しています（サービスの名称としては、「なりすましフィルタ」など、別の名称が用いられていることもあります。）。迷惑メ

ールの多くは、送信者情報を偽装している（なりすましている）ため、このフィルタが提供されている場合には、利用者側でも、積極的に導入することが推奨されます。

しかし、特別の使い方をする場合には、8.2で解説した問題のほか、8.4で解説するメール転送の課題などもあるため、場合によっては、その利用方法について注意が必要です。多くの ISP では、回避策を準備していることが多いため、利用の際は、利用している ISP の説明を確認することが推奨されます。

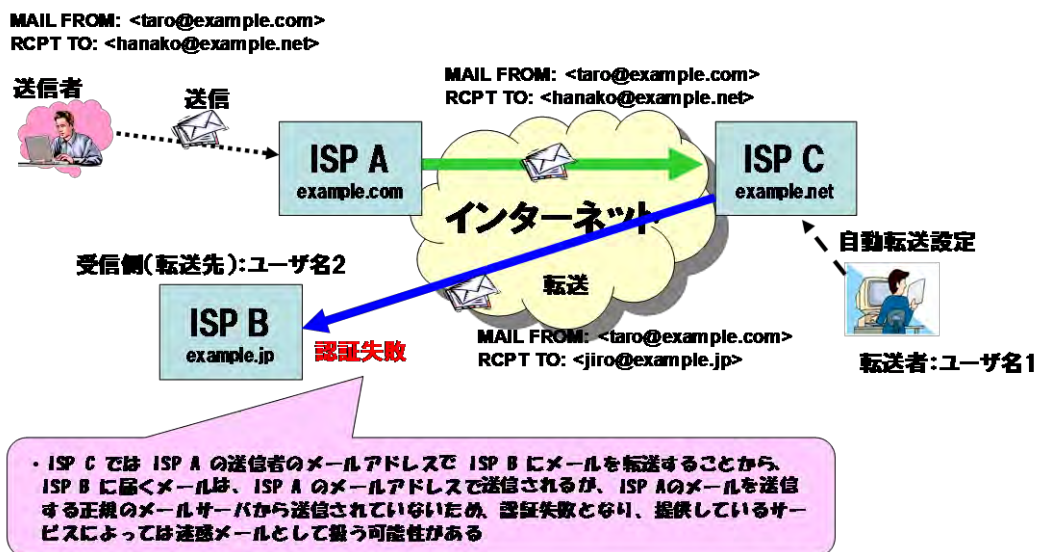
ただし、多くのエンドユーザは、特別な使い方をすることはないと考えられますので、基本的には、そのようなことを意識する必要はないと思われます。

8.4 メール転送時の注意事項

メールを転送する場合には、転送元のアドレスは、最初のメールの送信者のアドレスになるのが一般的です。このため使っているドメイン認証技術によっては、メールの転送が行われる場合に、受信側で送信ドメイン認証技術による確認をする場合に、送信者情報（転送元のアドレス）と送信に用いられたメールサーバ（転送者のサーバ）が異なることになるので、結果として、送信者情報を偽装した（メールアドレスをなりすました）メールを送信したと同じことになってしまい、転送先の送信ドメイン認証のフィルタを利用している場合などには、転送したメールが届か

なくなってしまう。

したがって、メール転送を行う場合には、転送先のサービスが送信ドメイン認証技術を採用しているか、メール転送時にどのようなアドレスを使っているか等を確認する必要があります。送信ドメイン認証技術を用いたフィルタを提供している多くのサービスでは、ホワイトリストのように、無条件で受信を許可する設定を可能にしており、事前に確認したアドレスをホワイトリストに登録すること等により、フィルタで拒否されなくすることも可能です。利用の際は、具体的な設定の方法等について、利用している ISP の説明を確認することが推奨されます。



図表 8-3 メール転送時の注意事項

