第5章 ISPでの対応

第 5 章　ISP での対応

本章では、ISP が送信ドメイン認証技術を導入する場合に考慮すべき事項について解説します。

ISP が運用するメールシステムは、2.1 で解説したような構成となっており、提供するサービスの規模にもよりますが、概ねメールの送信側と受信側でそれぞれのメールの流れがあります。ここでは、送信ドメイン認証技術の導入に際し、ISP として、メールの送信側及び受信側のそれぞれで行うべき作業や検討すべき事項について解説します。

5.1　ISP のメールサービスの概要

ISP のメールサービスは、ISP が管理する固定的なドメイン名を用いたメールアドレスを顧客に提供し、インターネットへのメールの送信と顧客宛のメールを受信します。受信したメールは、メールアドレスごとにメールスプールに格納されます。メールスプール上の受信メールは、顧客が MUA や、ウェブメール機能を提供している場合はウェブブラウザなどを利用して閲覧します。

ISP はドメインを管理している場合が多いので、SPF レコードの設定や DKIM の公開鍵の設定など、DNS 上に必要となる作業を自社で行えるため、送信ドメイン認証技術の導入が比較的容易であるといえます。また、メールスプールも管理していますので、例えば送信ドメイン認証技術で認証が失敗したメールを通常閲覧できる領域と別の場所に保管したり、認証が成功した特定のドメインからのメールを優先的に受信させるなど、フィルタサービスの機能拡充に応用することも可能です。

5.2　送信側の対応

5.2.1　概要

ISP が送信するメールは、一般の企業や各種組織のドメイン名を利用して送信されるメールに比べて、その規模が大きかったり、利用目的が多様であることにより様々な種類のメールが送受信される、という特徴があります。送信ドメイン認証技術を送信側で導入し、ISP を経由しない詐称されたメールを区別できるようにすることは、ISP のドメイン名の信頼度を向上させるために非常に重要です。

送信ドメイン認証技術は、送信者情報が偽装されているかどうかを確認可能とする技術なので、送信側で送信ドメイン認証技術を導入することにより、迷惑メールの多い ISP のドメイン名が、逆に迷惑メールの送信元として判断されてしまう可能性もあります。ISP から日々大量に送信されるメールの中に、メールの受信者にとって迷惑メールとなるようなメールが含まれていないか、それらが誰から送信されているのかを管理することも重要です。自社のドメイン名に対して迷惑メールを送信するドメインとしての評判が下がらないように、何らかの監視等の管理が必要です。

5.2.2　送信ドメイン認証技術の導入

5.2.2.1　SPF/Sender ID の導入

ネットワーク方式の送信ドメイン認証技術である SPF / Sender ID を送信側で導入するためには、メールに利用しているドメインについて、3.2.4 で解説した SPF レコードの記述が必要です。

SPF レコードには、メールの出口であるホストのグローバル IP アドレスが含まれるような、ネットワークアドレスや IP アドレス、ドメイン名などを記述します。これらの出口には、通常の送信用のホスト以外に、例えば、受信側が一時的に受け取らなかった場合に移される再配送用のホストや、メールサービスで利用しているドメイン名を使った顧客向けの連絡用の送信用メールサーバなども含める必要があります。

5.2.2.1.1　サブドメイン利用時の注意

メールサービスに、複数のドメイン名が利用できるようになっている場合には、それぞれのドメインについて SPF レコードを記述する必要があります。

また、複数のドメイン名を利用している場合で、それぞれがサブドメインの構成となっており、それらの親ドメインをメールサービスに利用していないときは、注意が必要です。SPF レコードが記述されていないドメイン名は、詐称されても受信側で判定できませんので、よく目にするドメイン名の認証結果が fail / softfail などの認証失敗でない場合には、誤解を与えてしまう可能性がありますので、3.2.3 と 4.1.2.2 で解説したとおり、以下のように、メールに利用しない親ドメインの場合は、明示的にすべて認証が失敗するような SPF レコードを宣言した方が良いでしょう。

```
example.jp              TXT "v=spf1 -all"
apple.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
peach.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
mango.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
```

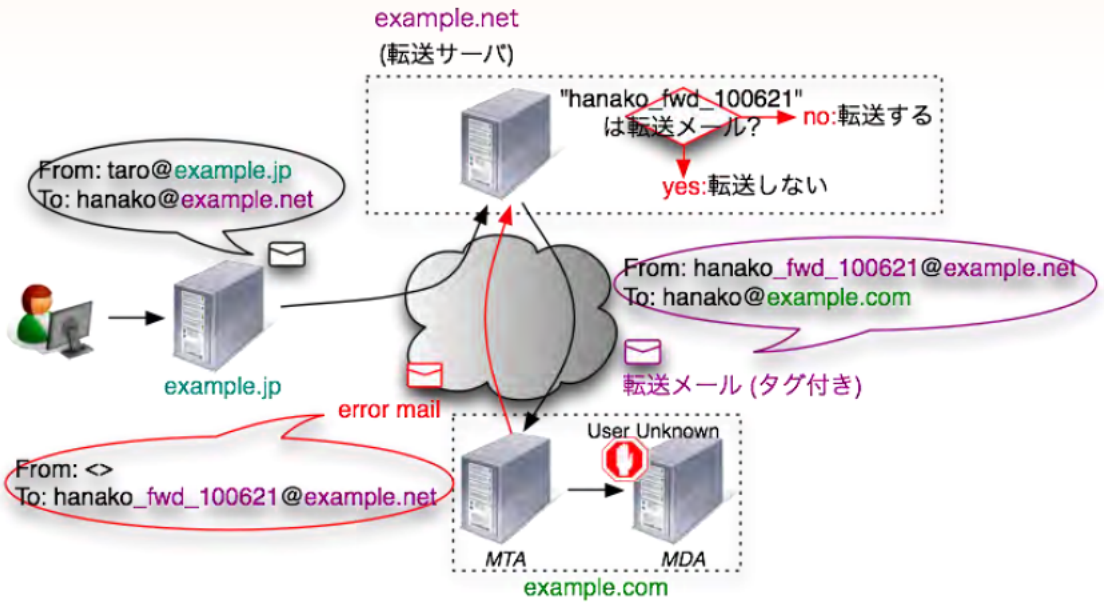
図表５－１　サブドメインがある場合の SPF レコードの例

5.2.2.1.2　転送処理

一度受信したメールを、あらかじめ設定された別のメールアドレスへ送信する転送機能は、古くから提供されてきた機能の一つですが、 4.2.1.2 で解説したとおり、ネットワーク方式の送信ドメイン認証技術との相性は良くありません。すなわち、現在提供されている多くの転送機能は、転送時のリバースパスに元々の送信者のリバースパス情報をそのまま使いますので、転送先での SPF の認証は失敗してしまいます。

転送設定は、メールの利用者がそれぞれ設定しますし、転送先のメール利用者は転送者と同一であることが一般的です。そのため、転送先のメール受信設定で、転送元からのメールが SPF の認証が失敗しても受け取るようなフィルタ等の設定が可能であれば、受け取ることは可能になります。

SPF の場合は、送信者情報としてリバースパス を利用しますので、4.2.1.2 で解説したとおり、転送時に送信元の情報を利用するのではなく、転送者のメールアドレスを設定し直すことによりこの問題は回避できます。ただし、単純にリバースパスを書き換えてしまうと、転送先で受け取れなかった場合やエラーメールなどが、ループしてしまう可能性があります。そのため、転送時に書き換えるメールアドレスは、ローカルパート部分に何らかの印となるような文字列を別途挿入し、通常の受信メールと転送メールの戻りメールとを区別できるような工夫も考えられます。通常の受信メールは転送し、転送したメールが戻ってきた場合には、そのまま転送せずに利用者のメールボックスに格納するなどです。



図表５－２　転送時の処理の例

転送先のメールシステムが Sender ID で認証している場合も、単純に受信したメールを転送したときには、認証が失敗します。転送時には、転送者のメールアドレスを Resent-From ヘッダに記述することで、転送先の Sender ID の認証時に送信者情報として認識されることになります。メール形式を定義する規格である RFC5322 では、転送のような再送信されるメールについては、Resent-From ヘッダなどの Resent- ヘッダを追加すべきと示されています。

5.2.2.2　DKIM の導入

DKIM は、送信するメールそれぞれに電子署名を追加して送信元を明らかにします。3.4.3 で解説したとおり、電子署名は、メール本文（ヘッダとメール本文の内容）のハッシュ値の計算、公開鍵暗号技術による電子署名の作成という処理を、メール送信のたびに行います。そのため、これまでのメール送信時より負荷が高くなることが予想されますので、導入時にある程度設備に余裕があるかどうかを確認する必要があります。設備負荷は、電子署名の作成に利用するアルゴリズムとも関連しますので、それとも合わせて検討が必要です。

次に、どのメールに対して電子署名を行うかの判断については、送信者情報が偽装されていないかを確認するという送信ドメイン認証技術の目的を考えると、基本的にはすべての送信メールを対象に電子署名を付与することが望ましいでしょう。自 ISP 宛に送信するメールなど、送信者が明確に判断できるような場合もありますが、そのメールが転送されて外のメールシステムに届くような場合も考える必要があります。

5.2.3　迷惑メールの管理

多くのユーザが利用する ISP のメールサービスでは、自身のドメイン名の評判を下げないような運用を心がける必要があります。

例えば、迷惑メールが自社のメールサーバを経由して送信されていた場合には、その迷惑メールの受信側からの申告により、ブラックリストに登録され、以降そのブラックリストを利用しているメール受信側に通常のメールも含めた全ての届かなくなってしまうことが考えられます。近年の迷惑メールの増加傾向により、こういった迷惑メール対策を行うメール受信者は増えていますし、送信ドメイン認証技術の普及によりドメイン名による受信制御が行われることが予想されます。

そのための対策としては、以下の事項が考えられます。

5.2.3.1　送信側の迷惑メール対策

迷惑メールの送信元となる ISP と判断されないためには、そもそも迷惑メールが外部に送信されないような仕組みがあれば良いことになります。現在、多くの ISP ではメール受信時に迷惑メールかどうかを判定する迷惑メールフィルタを提供しています。こういったフィルタがメールの内容から判断するタイプのものであれば、それを送信時にも適用し、迷惑メールを送信しようとしている場合に保留することによって、外部への送信を抑制することができます。

しかし、迷惑メール判定には誤判定が発生しますし、送信されなかったことが送信者に通知できない場合に問題となる可能性がありますので、利用者のサポートは十分に行う必要があります。また、送信側にもフィルタを導入することで新たな費用が発生する可能性もありますので、費用対効果なども含めて検討する必要があります。

5.2.3.2　送信者の特定とその対策手順の確立

迷惑メールが ISP のメールサーバから送信される可能性を完全に排除することは困難ですので、問題を大きくしないためにも、仮に迷惑メールが送信されても、受信者からの連絡があった場合などには、その迷惑メールを誰が実際に送信したのかを判断する仕組みが重要になります。

送信者を特定するには、メール送信時に送信者の認証を ID とパスワードによって行う SMTP-AUTH を導入し、メールヘッダやメール送信ログに、その AUTH ID を記録するなどして、誰が実際に送信したかを調べる方法があります。最近では、不正プログラム (マルウェア) に感染して、利用者が知らない間に外部から制御されて迷惑メールを送信することが問題となっており、SMTP-AUTH にも対応したマルウェアが現れているのではないかともいわれています。そのため、AUTH ID を利用して迷惑メール送信者を特定し、利用者への通知及び解決のためのサポートを行うことは、顧客保護の意味でも重要になってきます。また、迷惑メールの大量送信を抑制するために、AUTH ID 単位で、一定時間内に送信できるメール数を制限する方法があります。

5.2.3.3　送信者情報を変更できないような仕組み

送信ドメイン認証技術で送信者情報として使われるのは、リバースパスと From ヘッダアドレスのドメイン部分となります。受信側で送信ドメイン認証が失敗しないためには、これらが正しい情報となっている必要がありますので、顧客からメールが投稿された場合に、これらの情報が認証失敗するものになっていないかどうかを、配送前に確認すると良いでしょう。

メール投稿時に指定されたこれらの情報が、あらかじめ送信ドメイン認証に失敗することが分かった場合に、ISP が取りうる対応方法の例を以下に示します。

(a) メールの投稿そのものを受け付けない (エラー応答する)
(b) リバースパスの場合、ISP のドメイン名のメールアドレスに付け替える
(c) From ヘッダアドレスの場合、Sender ヘッダなどに ISP のドメイン名のメールアドレスを追加する

これまで、多くのメールサービスでは、これら送信者情報の指定方法については比較的緩やかな運用をしていました。そのため、このような対応を急激に行うと、利用者にとって混乱の原因になりかねませんので、事前の周知が重要になります。

また、DKIM の場合も From ヘッダアドレスのドメイン名とは無関係ではありませんので、DKIM-Signature ヘッダに示される送信者情報のドメインと異なるようなことがある場合は、同様に何らかの対策が必要になります。

5.2.3.4　エラーメール処理

受信したメールが宛先不明で配送できなかった場合は、メールの送信者にエラーメールを送信する必要があります。エラーメールは、リバースパスに指定されたメールアドレスに送信されます。迷惑メールの多くは、このリバースパスを詐称する場合が多いので、結果として不要なエラーメールがメールアドレスを詐称された側に大量に送信されることになります。

ISP では、決まったドメインを使ってメールサービスを提供しますので、詐称に使われる可能性が比較的高いドメイン名である一方、不特定多数にサービスを提供していることもあり、宛先不明となる迷惑メールも多く、結果として不要なエラーメールを多数送信している可能性もあります。こうした不要なエラーメールを抑制するためには、次の対策があります。

(a) メールの受信時点で宛先が存在するかを確認して存在しない場合は受け取らない
(b) 受信時に送信ドメイン認証技術で認証が失敗した場合にエラーメールを送信しない

(a) の対策のために、メールの受信時に、宛先が存在するかを確認するには、顧客管理を行っているシステム (データベースなど) とリアルタイムで問合せできることが必要です。メールシステムの構成として、

メールスプールが存在するかどうかで宛先不明かどうかを MTA ではなく、MDA が判断している場合には、システムの変更が必要になります。また、メール受信時に宛先不明かどうかを SMTP 上の応答として返すことになりますので、送信側でその応答を確認することにより、実在するメールアドレスかどうかを簡単に調べることができてしまいます。よく使われるローカルパートの文字列を総当たり的に指定して実在するメールアドレスを取得する攻撃は、辞書攻撃 (DHA: Directory Harvesting Attack) と呼ばれます。これを防ぐためには、一定数以上の宛先不明が発生した場合に、以後の SMTP 処理を継続しない、という方法があります。

宛先不明時にエラーメールを返す送信先は、詐称されていない実際の送信元です。そのため、送信ドメイン認証技術で認証が失敗した送信先、例えば SPF / Sender ID で認証結果が fail / softfail となった送信元や、DKIM で認証が失敗した場合や、ADSP で fail/discard であったような送信元には、エラーメールを送信する必要はありません。このため、(b) の対策を実施することも考えられます。

5.3　メール受信側としての検討

5.3.1　概要

第３章で解説したとおり、送信ドメイン認証技術を用いることにより、メールの受信側が認証を行うことで、そのメールが本当にそのドメインから発信されたかどうかを判定することができます。送信ドメイン認証技術は、送信側の対応も必須ではありますが、受信側が対応を進めることは送信側の導入モチベーションにも繋がるものです。そのため、送信ドメイン認証技術の普及に向けてのよいサイクルを生むためにも、ISP では積極的に受信時の認証およびラベリングを行うべきであり、受信したメールを適切に取り扱う努力を行っていることを、利用者・送信者へアピールしていくことが望まれます。

5.3.2　利用する送信ドメイン認証技術の選定

受信時に利用する送信ドメイン認証技術を選定する場合には､4.1.1 を参考にします。送信ドメイン認証技術を複数導入すれば、ドメインの正当性の判断に利用できる情報は増えますが、認証のために必要な追加コストが増加する場合があります。特に ISP の場合、取り扱うメールの通数が一般的な企業に比べ多くなりますので、機能を追加する設備の規模も大きくなると考えられます。現状のネットワーク構成やハードウェアを考慮しながら、段階的に送信ドメイン認証技術を導入していくことが現実的でしょう。

5.3.3　メールの配送制御

改めての説明になりますが、送信ドメイン認証技術は、あくまでも「特定の送信元から確かに送信されたかどうか」を機械的に判断するための技術であり、認証結果とメールのコンテンツは何の関係もないものです。ISP では多様な利用者にサービスを提供するという性質上、送信ドメイン認証技術での認証結果の取り扱いについては、特に慎重になるべきです。

5.3.3.1　配送前制御に関する注意

送信ドメイン認証技術による認証結果を利用した受信側のアクションで特に注意すべきなのが、認証結果による配送方法の取扱いです。4.1.3 で解説したとおり、送信ドメイン認証技術では、受信者の意図しないメーリングリスト経由での再配送や送信時ポリシーの記述ミスなどによって認証が失敗する場合もあります。特に、ISP ではさまざまな受信者による利用シーンが考えられるため、送信ドメイン認証技術による認証結果だけを利用して、一律にメールの受信を拒否したり破棄したりする取り扱いをしてはなりません。ただし、以下の場合にはこの限りではありません。

(a) 受信設備の高負荷による緊急避難など限定的対応の場合
(b) エンドユーザからの個別の同意がある場合

(b) による場合には､エンドユーザに対してリスクについて十分な説明を行うとともに、簡易に機能を解除させたり、個別に回

避できるような機能を設けるなどの機能的配慮もした上で、個別に同意を取って提供しなければなりません 。

5.3.3.3　ホワイトリストやドメインレピュテーションの活用

4.1.4.3 で示したとおり、送信ドメイン認証の結果と、ISP が事前に用意したホワイトリストやドメインの評判（ドメインレピュテーション）情報と照合することもできます。照合結果によって、メールに特別なマークを付与したり、迷惑メール判定を実施せずにフィルタを通過させたりするなどの活用方法が考えられます。また、サービスの利用者が個別にドメインを設定することにより、Web ブラウザや MUA 上でのフォルダ振分けなどに利用できるようにするサービス形態も考えられます。

ISP が他組織により提供されるホワイトリストやレピュテーション情報を利用する場合は、自組織のポリシーと一致しないことも十分に考えられるので注意が必要です。そのため、これらホワイトリストやレピュテーション情報は、自組織でコントロールができる権利もしくは機能を持つタイプのものでなければなりません。

5.3.3.4　認証結果の可視化による利用者のユーザビリティ向上

利用者が認識できるように認証結果の表示を行うためには、Web ブラウザ経由や MUA 経由など、表示領域を任意に制御できるような環境でメールを閲覧する必要があります。

一部の ISP では Web ブラウザ上でメールを利用できるサービスを提供していますが、このような環境の場合、画面インターフェース中に認証に利用したドメイン名や認証結果、ホワイトリストなどとの照合結果を分かりやすく表示させることが可能です。一方 MUA ではこのような画面表示に標準的に対応しているクライアントはまだほとんど存在していません。

送信ドメイン認証結果を分かりやすく表示するアプリケーション環境が整い、利用者が積極的に利用できるよう、ISP として可能な取り組みを推進することが好ましいといえます。

5.4　ユーザ周知

送信ドメイン認証を導入する場合には、導入した結果として発生する影響について、ユーザに周知する必要があります。周知の方法は、メールや郵便物で行う方法もありますが、最低限ホームページでの周知は実施するべきです。

なお、ユーザへの周知内容は、各社の対応内容によっても異なりますが、ユーザは送信ドメイン認証という技術の理解をすることが困難な場合も多いと想定されるため、表現方法や影響をよりわかりやすくする工夫が必要です。特に、「送信ドメイン認証技術」という表現にこだわらず、ユーザの理解を得られる表現を使うことも重要です。

5.4.1　送信側の対応

ユーザによるメールの利用方法により認証が失敗してしまう場合として、送信側では、ユーザが自社のサーバ（MSA）経由で送信アドレスを該当ドメイン以外で送信した場合と、ユーザが自社のサーバ以外のサーバから該当ドメインのメールを送信したケースの２つがあります。後者については、自社の管理外の問題であるため、ユーザに対して必ずしも説明する必要はないとも思えますが、前者と合わせて説明することが望ましいものです。

また、送信側の対応について、導入した技術と期待される効果を説明することが推奨されます。

5.4.2　受信側の対応

受信側の対応については、どの技術を採用しているかを説明する必要があります。

認証結果をラベリングとして記述する場合には、ラベリングの確認方法を、代表的なメールクライアントの設定方法について説明することが推奨されます。また、フィルタサービスを提供する場合には、該当のサービスの利用方法に加えて、利用した場合の影響について説明することが必要です。特に、ユーザにはドメイン詐称に対する認識が少ないため、どのような送信方法のメールがフィルタリングされるかを図解なども用いて説明することが推奨されます。