◆SMTP リレーとは!? 今さら聞けないメール配信の基礎知識
2017.12.08
https://baremetal.jp/blog/2017/12/08/468/

目次

メールの配送に使われる SMTP
顧客向けに新商品のお知らせメールを一斉に送りたい、あるいは会員登録したユーザーに対してメールで通知したいといったケースにおいて、遅延が生じて相手に届くまで時間がかかったり、そもそも相手に届かなかったりするトラブルは珍しくありません。このような事態が生じる理由として、送信に利用するメールサーバの処理能力不足や、迷惑メールとして誤って判断されて破棄されるといったことが挙げられます。

メールの配送に使われる SMTP
顧客向けに新商品のお知らせメールを一斉に送りたい、あるいは会員登録したユーザーに対してメールで通知したいといったケースにおいて、遅延が生じて相手に届くまで時間がかかったり、そもそも相手に届かなかったりするトラブルは珍しくありません。このような事態が生じる理由として、送信に利用するメールサーバの処理能力不足や、迷惑メールとして誤って判断されて破棄されるといったことが挙げられます。

こうした問題を回避し、迅速かつ確実に大量メールを送信するサービスとして提供されているのが「SMTP リレーサービス」などと呼ばれているものです。いわゆるメールの送信代行サービスですが、通常のメールサーバを使った送信と何が違うのでしょうか。それを知る前に、まずはメール送信に利用されるプロトコルである、「SMTP」（Simple Mail Transfer Protocol）について理解しておきましょう。

パソコンのメールソフトで作成したメールは、次の図のように流れて相手まで届きます。

(画像 stpm1.png)

このようにメールを送信する際、自分が使うメールソフトが送信用メールサーバにメールを転送するとき、そして送信側メールサーバから相手の受信側メールサーバへとメールを転送するために使われるのが SMTP です。

SMTP を使って送信するメールは、「エンベロープ」と「メールヘッダ」、そして「メール本文」の 3 つで構成されています。エンベロープとはもともと封筒という意味で、ここには送信元と宛先の情報が記録されています。メールヘッダにあるのは送信日時や送信元、宛先、件名などの情報です。なお送信元と宛先の情報は、エンベロープとメールヘッダの両方にありますが、SMTP サーバが利用するのはエンベロープに記載された内容です。ただエンベロープの内容をユーザーが記載する必要はなく、メールソフトがメールヘッダの情報を使ってエンベロープを作成します。

(画像 stpm2.png)

DNS で相手サーバを特定してメールを配信

さて、メールソフトからメールを受け取った送信サーバは、そのメールを転送するサーバを特定しなければなりません。この際に使われるのは「DNS」（Domain Name System）です。インターネット上で通信先を特定する際に使われる IP アドレスと、ドメイン名と呼ばれる名前を変換するための仕組みが DNS であり、たとえば Web サイトにアクセスする際、Web ブラウザのアドレスバーに「baremetal.jp」などと入力するでしょう。これがドメイン名で、Web ブラウザは OS を通じて、指定されたドメイン名に対応する IP アドレスを DNS サーバに問い合わせます。

DNS サーバにはメールサーバのドメインも登録することが可能であり、その情報は「MX レコード」と呼ばれます。メール送信のサーバは、メールを別のサーバに転送する必要が生じると、エンベロープに記載された宛先メールアドレスのドメイン名（@の右側部分）をチェックし、そのドメイン名に対応する IP アドレスを DNS サーバに問い合わせるわけです。こうして相手先のサーバが確定すると、SMTP で接続してメールの転送を行います。では、宛先として指定されたユーザーがメールを受け取る際にはどうするのでしょうか。ここで使われるのは「POP3」（Post Office Protocol version 3）や「IMAP4」（Internet Message Access Protocol version 4）といったプロトコルです。

SMTP でメールを受け取ったサーバは、それをいったんストレージに保存します。これを取り出すために使うのが POP3 や IMAP4 で、メールソフトからサーバに接続し、自分宛に届いたメールを取得します。なお POP3 と IMAP4 ではメールを管理する場所が異なり、POP3 ではメールソフトがあるパソコン側、IMAP4 ではサーバ側で管理します。SMTP を使った基本的なメール配送の仕組みはインターネット黎明期から変わりませんが、迷惑メールの増加にともなって徐々に新たな仕組みが追加されるようになります。

大量メール配信を妨げる迷惑メール対策

インターネット上におけるメールの送受信では SMTP（Simple Mail Transfer Protocol）が使われています。この SMTP はシンプルであり、誰でも自由にメールを送信できる特徴がありますが、それを逆手に取って広まったのが迷惑メールです。宣伝や詐欺などを目的として、無差別かつ大量に送信される迷惑メールは、インターネット社会において大きな問題であり、これまでさまざまな対策が講じられてきました。その 1 つとして挙げられるのが、ISP などによるメールの送信制限です。これは一定時間内に送信できるメール量を制限し、それを超えた場合にはメールの送信が不可能になるという仕組みです。通常のメール利用では、1 時間に数百通ものメールを送信するといったことはないでしょう。そこで短時間での大量のメール送信は迷惑メールの送信を行っていると判断し、メールの送信を拒否するというわけです。

ただ、自社サービスの会員向けに一斉に案内メールを送りたい、あるいはユーザ自身によるパスワード再設定処理のためにシステムから自動でメールを送信したいなど、正当な理由で一定時間内に大量のメールを送信したいこともあります。このような場面では、迷惑メール対策が大きな足かせとなるのです。ドメイン認証と呼ばれる迷惑メール対策も広まっています。これは送信者のメールアドレスのドメイン名が偽装されていると判断した場合にメールの受信を拒否する仕組みです。迷惑メールの多くがドメイン名を偽装したメールアドレスを利用しているため、有効な対策の 1 つであると言えます。

なお SMTP サーバは誰でも自由に構築することが可能であり、プロトコル上は自分で構築した SMTP サーバを使ってメールを送信することも不可能ではありません。ただ現在は、送信者から SMTP サーバへメールの送信設定を行う際に、送信者のアカウント名やパスワードが正しい利用者であることを確認してから送信をする、SMTP 認証（SMTP Authentication）を行なっているケースが一般的ですのでこうした方法でのメール送信は現実的ではないでしょう。

また、迷惑メールだと判断されなかったとしても、SMTP サーバの処理能力不足、あるいは帯域不足によって遅延や不着が生じる恐れがあります。EC サイトにおける商品購入確認メールなど、迅速かつ確実に相手に届けたいといった場合、こうした問題が生じればビジネスに悪影響を及ぼすことにもなりかねません。

参考：迷惑メール対策のための SPF レコードの書き方

ビジネスでの大量メール配信をサポートする SMTP リレーサービス
このように、迷惑メール対策やシステム上の要因から、大量のメールを送信するのは難しいのが現状です。そこで、こうした課題を解決するサービスとして提供されているのが、SMTP リレーなどと呼ばれているメール配信に特化したサービスです。これらのサービスが SMTP リレーなどと呼ばれているのは、バケツリレーのように複数のサーバを介してメールを配送する SMTP の仕組みを使っているためです。SMTP が生まれた当初は、相手のサーバと直接通信できるとは限らなかったため、別のサーバを介して相手のサーバにメールを配送するといったことが行われていました。たとえば、直接通信することができない組織 A と組織 C でメールを送受信する際、両者に接続している組織 B のサーバがメールを中継するといった形です。

現在では相手の組織のメールサーバと直接メールを送受信することが一般的で、別の組織のメールサーバを介することはほとんどありません。ただ SMTP には、メールを中継して送信する機能が残っており、SMTP リレーサービスではこの仕組みを使います。具体的には、自社のメールサーバに対して SMTP リレーサービスを提供している SMTP サーバを中継するように設定します。これにより、相手のメールサーバに直接送信するのではなく、SMTP リレーサービスを使って送信できるようになるわけです。こうしたサービスで使われる SMTP サーバは、大量のメール送信を可能にしているだけでなく、Gmail などのサービスや各携帯通信キャリア、ISP などから信頼を得ることで、大量のメールを送信しても確実に相手に届くようにしています。

大量のメールを確実に送信するため、技術的な工夫も盛り込まれています。たとえばリンクが提供するメール配信サービスである「ベアメール」では、処理を複数のサーバに分散するロードバランサーを使い、複数の SMTP サーバを使ってメールを送信するようにしているほか、広帯域のネットワークを使ってインターネットに接続しています。

自社で SMTP サーバを構築する場合、メンテナンスやセキュリティ対策といった適切な運用管理はもちろん、IP アドレスの評判を指標化した「IP レピュテーションスコア」を常に高く維持する必要があります。このスコアはメールの到達率に大きく関係しています。例えば、使用歴が浅い IP アドレスは十分な配信実績があるとみなされず、IP レピュテーションスコアも低い状態にあり、受信側にメールをブロックされやすくなります。自社でサーバを構築するケースには、こうした IP レピュテーションを意識した運用がなされていないと到達率が上がらないというリスクが伴います。

また、メルマガなどで一斉に大量のメールを送る際、メールサーバのスペックや ISP 側での送信数の制限によっ

ては、きちんと処理しきれずに配信遅延、もしくは配信がされないといったことも起こりえます。

ベアメールでは、「SMTP リレーをする」といった利用方法だけでなく「SMTP サーバとして使う」こともでき、自社で送信サーバを構築する際に生じるこうした課題を解決することができます。

メールはビジネスの幅広い領域で使われており、内容によっては遅延や不達が大きな影響を及ぼすことも考えられます。こうした不安を解消する上で、ベアメールは極めて有効な解決策となります。もし大量メールの送信で遅延や不達に悩んでいるのであれば、ぜひ利用を検討してみましょう。