迷惑メールについて

株式会社アイ・シー・アイ

Internet &
Communication
Innovator

■迷惑メールとは、

メール受信者の同意なしに大量送信される広告・宣伝メールを一般的に「迷惑メール」といいます。
インターネット上では、無差別に送信される悪質なメールを別名「SPAMメール」とも呼んでいます。

以前の紙媒体で投函されていたダイレクトメールに比べ、「迷惑メール」の送信にはほとんどコストが掛からないというメリットがあり、爆発的に増加しました。

また、2000年以降は携帯電話の普及に伴って、携帯電話メールアドレス宛ての「迷惑メール」の増加も問題となりました。

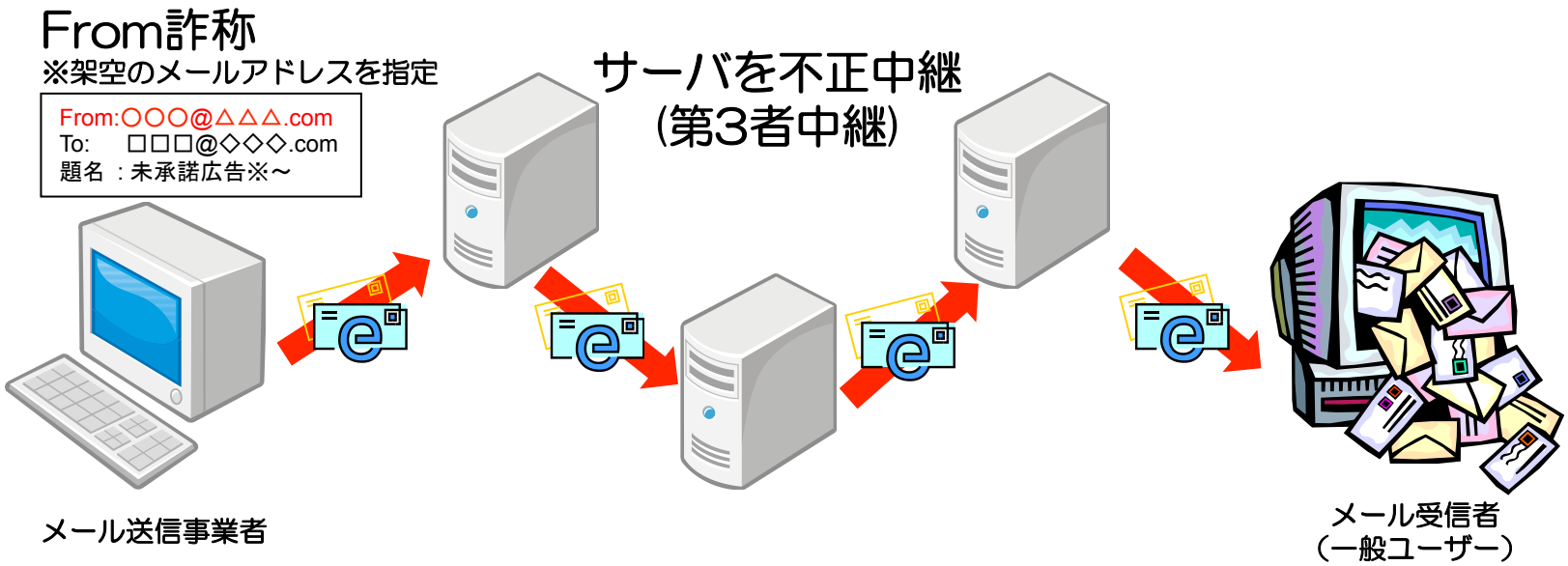
■迷惑メールの送信手段

メール送信事業者は迷惑メール送信専用のソフトを使用する事が多く、時代とともに高機能化しています。

送信手段としては、主に以下のようなものが挙げられます。

- ●送信メールアドレスの偽称（From詐称と呼ばれます）
- ●メールサーバの不正中継

上記以外に、ウイルス感染によって自分では気づかないうちにメール送信させる「Bot」というものもあります。



■迷惑メールへの対策①

迷惑メールへの代表的な対策として、以下のような手法が用いられています。

●ブラックリスト

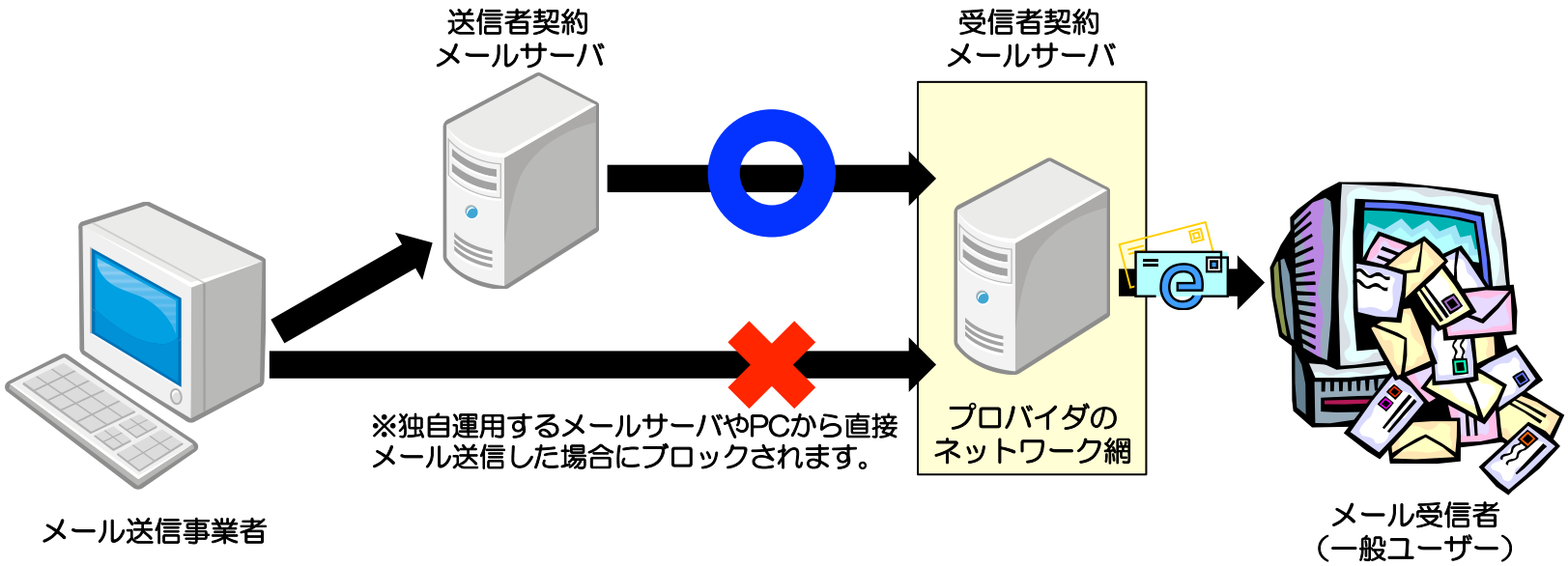
迷惑メールの送信元アドレスを登録し、そのアドレスから再度送信された場合、自動的にメールを削除する機能。

●メール内文字列検索

メールの題名や本文に特定の文字列を検出した場合、自動的にメールを削除する機能。

●Inbound Port 25 Blocking (IP25B) ※下図参照

メール送信者が契約しているメールサーバ以外からのメールを規制する機能。



■迷惑メールへの対策②

技術的な取り組みの他に、法律による取り組みも行われ、2008年12月からは「特定電子メールの送信の適正化等に関する法律」が施行されており、これを遵守しなかった場合は処罰が科せられます。

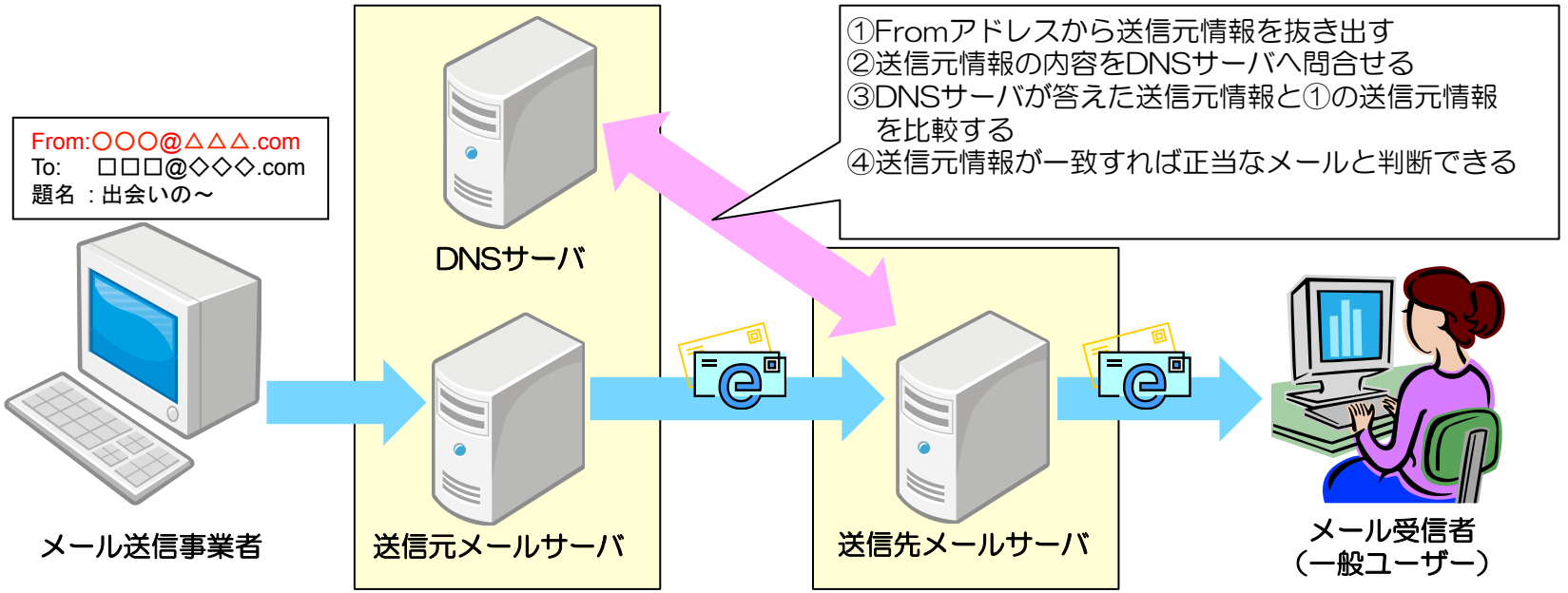
総務省
MIC Ministry of Internal Affairs and Communications

「特定電子メールの送信等に関するガイドライン」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/m_mail_081114_1.pdf

■迷惑メール対策の最新技術

近年、各インターネット通信事業者が迷惑メールへの対策として取り入れている技術として、「送信ドメイン認証」というものがあります。
ここでは「SPF・SenderID」「DKIM・DomainKeys」という2つの手段を紹介します。

●SPF（Sender Policy Framework）・SenderID



●DKIM（DomainKeys Identified Mail）・DomainKeys

メールの中に「電子署名」を付けておいて、送信先でその電子署名があるか、または検証の結果認証が成功するかによって、正当なメールであるかを判断でき、不正なメールの削除も可能です。
こちらの技術は、迷惑メール対策に有効な手段ですが、送信側・受信側双方で対応が必要なためまだまだ普及していないのが現状であり、多くの事業者で導入が急がれています。

■迷惑メールの今後と利用者による取り組み

今まで述べてきたように、迷惑メールに対して各インターネット通信事業者や政府機関など様々な対策を実施していますが、送信される迷惑メールの数はほとんど減少していないのが現状です。

その背景としては、メールの受信対象者であるユーザーが多種多様な通信機器の普及により増加していることと、迷惑メールを送信することによってメール送信事業者に利益が生まれ続けていることがあげられるでしょう。

メール利用者側で簡単に実施できる対策について、以下のようなものがありますので、是非有効に活用してみて下さい！

- インターネット通信事業者が提供しているセキュリティサービスを利用する
- セキュリティ（アンチウィルス）ソフトのフィルタリング機能を利用する
- メールソフトのフィルタリング機能を利用する
- 送付されてきた迷惑メールの配信停止依頼先へは絶対に連絡しない