セキュリティ対策（迷惑メール）取り組み事例の紹介

メールの送信元チェック（S25R）による迷惑メール対策

大阪歯科大学

大阪歯科大学では、インターネットゲートウェイでウイルスをチェックしていたが、月に３千件を超えるアラート（警告・確認・注意）やスパムメールも大量に届いていることから、この対策としてスパムメールを防御する「＊S25R」と呼ばれる対策を取ることで効果をあげている。

１．実施規模

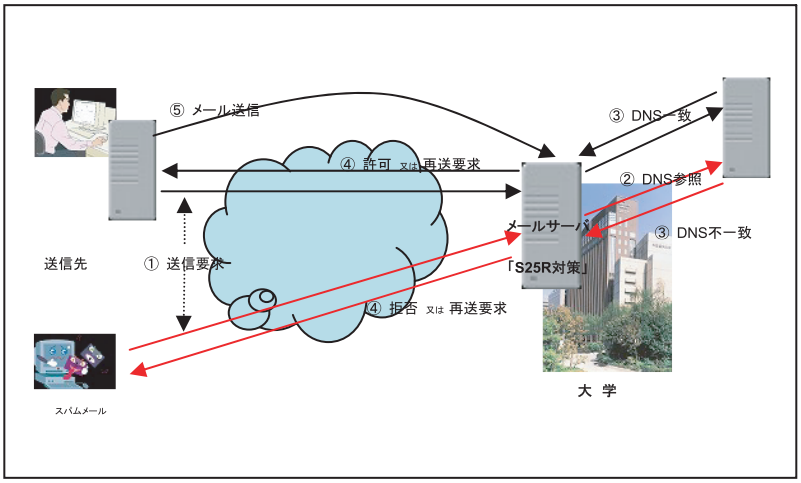
８６９人（学部生・大学院生）＋３８１人（教職員）

２．導入の経緯

２００４年頃から多い月では３千件を超えるアラートが出ることも珍しくなく、スパムメールも大量に届いていることから、スパム対策としてブラックリストの利用を検討したが、まだ信頼性が低くリスト参照に DNS の負荷がかかることから、メールハブ（中継）サーバで SMTP セッション時の応答時間を遅らせるという対策をとった。しかし、この対策だけではスパムメールは減少するものの、正規メールの受信遅延や、重複受信などの問題が生じていた。この問題解決のため、「S25R」対策を実施した。

３．導入の形態、内容と効果

導入は、メールサーバ上でメールの送信元をチェックしてスパムメールを防御する「S25R」方式を採用した。正規のメールサーバは、通常は固有の IP アドレスが割り当てられているが、スパムメールの送信元ホスト名の多くは、送信元の組織情報(ドメイン情報)が消されていたり、無秩序な英数字で表記されているなどの特徴があることから、送信元の IP アドレスから特定される組織名を調べた上で、一致しないものについては受信を拒否する、いわゆる DNS の逆引きによる対策である。この対策の結果、ゲートウェイで処理するコンピュータ・ウイルスのアラートが激減している。



４．今後の課題

この「S25R」も万能ではなく、ISP や ASP でのメール運用などにより、少数ではあるが正規のメールが届かないということが生じている。運用上で必ず注意しなければならないのが、常にログを監視しなければいけないということである。正規のメールサーバは何度か再送を繰り返すので、一旦受信を拒否したメールが再送されてきた場合は、必要ならホワイトリストに追加するなど誤検知した場合の対策が必須となる。

＊正式名称は、Selective SMTP(port25) Rejection で、開発者の浅見秀雄氏の論文が「阻止率 99%のスパム対策方式の研究報告」として公開されています。
http://gabacho-net.jp/anti-spam/anti-spam-system.html