

## 第 XXVII 部

### 迷惑メール低減に関する 技術開発と普及



## 第 27 部

## 迷惑メール低減に関する技術開発と普及

## 第 1 章 はじめに

antispam ワーキンググループでは、主にドメイン認証の普及に関して研究を進めている。本章では、2006 年度の研究成果について述べる。

## 第 2 章 SPF の普及に関する提案

antispam ワーキンググループの山本は、IAJapan の有害情報対策ポータルサイトについて、SPF を普及させるための提案を公開している。

- [http://www.iajapan.org/anti\\_spam/portal/Operation/Suggestion/sugg\\_a01\\_01.html](http://www.iajapan.org/anti_spam/portal/Operation/Suggestion/sugg_a01_01.html)

この提案を受け入れるサイトが増加すれば、SPF RR を宣言すれば、受け取る不用なエラーメールが低減する。

前述のように、この提案は SPF を普及させるために考え出されたが、最近 RBL (Real-time Black-list) の弊害を防止する意味でも有効であることがわかってきた。

## 第 3 章 RBL による弊害とその防止

RBL による弊害とは、本来届くべきはずの正当なメールが、RBL のせいで届かなくなることである。これを理解するためには、まずエラーメールの仕組みを理解する必要がある。

図 3.1 に示すように、これまで受信サーバの多くは、ユーザが存在しないときは、SMTP でユーザがないことを通知していた。エラーメールを生成し

送信するのは、受信サーバではなく、1 つ手前のユーザの不在を通知されたサーバである。

迷惑メール配送業者は、この種の受信サーバに対し、ハーベスティング攻撃をかけることにより、メールアドレスのリストを作成できる。つまり、適当なユーザ名宛のメールをこの受信サーバに送りつけ、受理されたらそのメールアドレスは存在し、ユーザの不在を通知されたら存在しないと判断する (図 3.2)。

このハーベスティング攻撃を防止するために、受信サーバに対策を施すサイトが増えてきた。すなわち、ユーザが存在してもメールを受け取り、ユーザが存在しない場合は自分自身でエラーメールを作成し送信するのである (図 3.3)。

この種の受信サーバは、不要なエラーメールを生成するという副作用を持つ。この副作用は、以下のようにして起こる。

図 3.4 において、「標的の企業」は受信サーバにハーベスティング攻撃の対策を施しているとする。また、迷惑メール配送業者は、この「標的の企業」に迷惑メールを送りつけることとする。迷惑メールの多くは、送信者が詐称されている。ここでは、「詐称された企業」のアドレスが悪用されていたとしよう。「標的の企業」は、迷惑メールを受け取り、もしユー

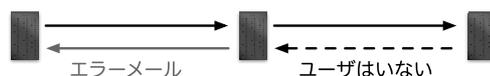


図 3.1. 古いタイプの受信サーバとエラーメールの生成

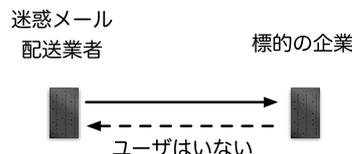


図 3.2. ハーベスティング攻撃

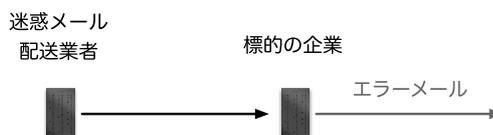


図 3.3. ハーベスティング攻撃の対策を施した受信サーバ

が存在しない場合、自身でエラーメールを生成し配送する。このときエラーメールは、迷惑メール配送業者ではなく、詐称された企業へ送信される。

このエラーメールは、「詐称された企業」にとって迷惑である。このため「詐称された企業」は、「標的の企業」を RBL に登録するかもしれない。

不幸にも「標的の企業」が RBL に登録された場合、その企業からのメールは、他のサイトに届かなくなる可能性がある。つまり、「標的の企業」が、ある企業にメールを送ろうとし、もしその企業が RBL を参照している場合、受け取りを拒否してしまう(図 3.5)。

これは机上の空論ではなく、実際に起こっている深刻な問題である。

もし、「詐称された企業」が SPF の普及に関する

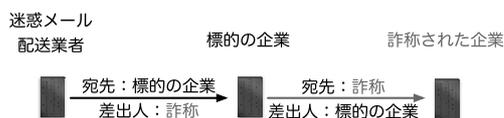


図 3.4. 不要なエラーメールの生成

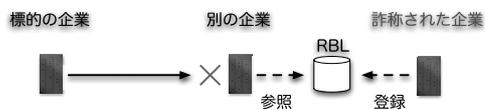


図 3.5. RBL によるメール受信の拒否



図 3.6. 不要なエラーメール送信の防止

提案を実装すれば、不要なエラーメールは生成しない(図 3.6)。このため、誤って RBL に登録される事故を防止できる。

---

第 4 章 SPF の普及に関する提案の実装

---

慶応大学の佐川は、SPF の普及に関する提案を Sendmail で実装し、パッチの形で公開している。

- <http://member.wide.ad.jp/wg/antispam/sm-dsn-supr/>

この実装は、Mew.org で運用されており、安定性と効果が確かめられている。

---

第 5 章 SPF の普及率

---

以上のように SPF の普及に関する提案は、RBL の弊害を防止することにも役立つことがわかった。この提案がうまく作用するためには、SPF RR を宣言するサイトがある程度存在しなければならない。

antispam ワーキンググループでは、JPRS の協力のもと、毎月 “.JP” における SPF の普及率を測定している。図 5.1 に 2007 年 1 月までの普及率の推移を示す。

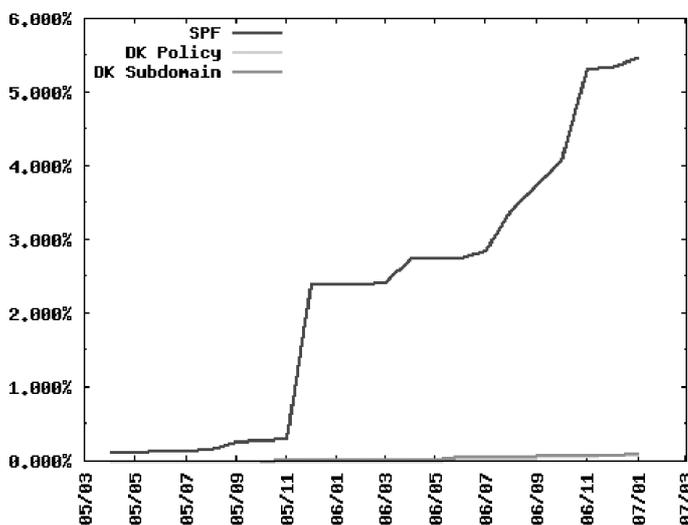


図 5.1. ドメイン認証の普及率の推移

2007年1月時点でのSPFの普及率は5.47パーセントである。

---

---

## 第6章 おわりに

---

---

SPFの普及に関し、サイト管理者ができることを列挙する。趣旨をよく理解し、ぜひ実行して頂きたい。

- メールの送信側：サイトのDNSでSPF RRを宣言する
- メールの受信側：受信サーバで提案を実装する。あるいは、ベンダーに実装するようにお願いする。