インテグレーションPROXYサーバの開発
～セキュリティの第1歩はPROXYから～

1. 背景

いまやインターネットは、なくてはならない社会インフラとなる一方、セキュリティに関する脅威が大きな問題となっている。

特に、スパムメール大量配信やDDoS攻撃の踏み台とされるボットPCが急激に増加しており、世界でネットワーク接続されたコンピュータの25%（1億台）以上が、すでにボットネットに組み込まれているともいわれている。

ほとんどの人は、Java Scriptなどの接続先の命令によって動作するスクリプト言語を有効にした状態で、接続先の信頼性を意識することもなく、ホームページを閲覧しているという現状がある。大量の実行制御を行うスクリプト言語に脆弱性が存在することは不思議なことではなく、こうしたスクリプトが原因でボット感染する事例は非常に多い。

Webサーバなどのサーバソフトウェアについても脆弱性は多く存在し、Webサーバに不正侵入することにより、そのホームページを書き換え、閲覧者PCを次々とボット感染させるという行為が行われている。

2. 目的

こうした問題に対して、PROXYサーバという異なるコンピュータをインターネットとの間に挿入し、直接接続を禁止するというアプローチは、絶大な効果を発揮する。

最悪、クライアントPCがボット感染したり、スパイウェアなどの無断でネットアクセスを行うソフトウェアが実行された場合でも、それらはPROXYサーバの場所を探索することすら困難であり、また、PROXYサーバにアクセスできたとしても、PROXYサーバによって接続は拒否され、スパムメール大量配信やDDoS攻撃などを行うことは事実上不可能である。

サーバの脆弱性については、バッファオーバフローによる脆弱性を突く場合が多く、当然、PROXYサーバは、そうした不正リクエストの各種サーバへのフォワードは行わないため、未知のものを含めて、大部分の脆弱性は回避できる。

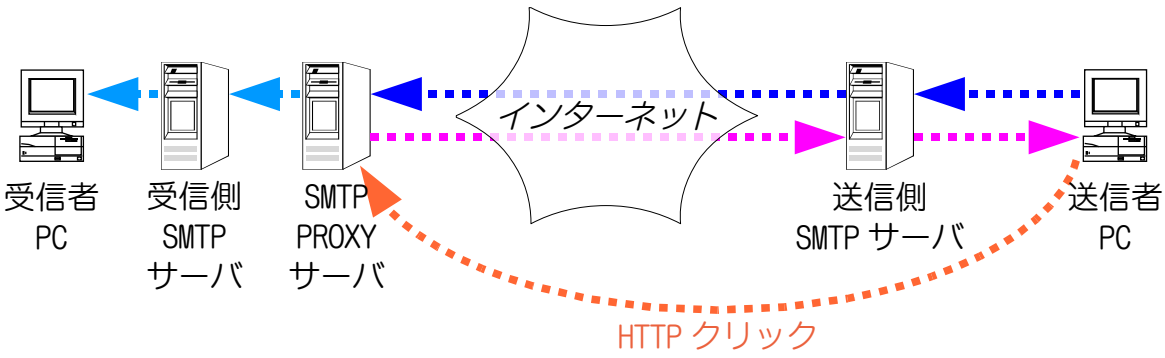
また、今回、PROXYとして、SMTPに対応し、本ソフトウェアの基盤技術となる異なるプロトコル(HTTP)との連携システムにより、多くの社会的損失へと波及するスパムメール問題に着実なメスを入れる。

3. 開発の内容

本ソフトウェアは、PROXY サーバ、リバース PROXY サーバ、Web サーバなど、多くのサーバ機能モジュールにより構成されている。今回の開発では、これら機能モジュールやコアモジュールの改良と、新たに PROXY として、SMTP 対応を行った。これにより、スパム対策と、暗号化や負荷分散対応を簡単に実現することができる。以下は、SMTP PROXY の主要機能の概説である。

3.1 URL クリック認証

SMTP として受信したメールの SMTP サーバへのフォワードを保留し、送信者（FROM アドレス）固有の URL を自動生成するとともに、送信者にその URL をメールで通知する。この URL に対してメール送信者がアクセス（メーラからクリック）することにより、SMTP PROXY は、Web サーバモジュールを介してこれを認識し、認証対象として、保留中のメールを通過させるという仕組みである。



3.2 おとりメールアドレス

通常、他人にメールを送信する場合、送信者ドメインの SMTP サーバにメール配信を依頼することで、受信者ドメインの SMTP サーバに自動配信される。しかし、スパマーはこうした SMTP サーバを利用することなく、直接、受信者ドメインの SMTP サーバに対してコネクションを張り、メールを送信する。これは、SMTP サーバの転送容量の限界や、管理者による転送拒否などにより、効率が悪いためである。また、スパマーは、送信元の特定を回避するため、ボットネットなどを利用し、次々と異なる IP アドレスからスパムメールの送信を行う。

しかしながら、大量配信という特性上、送信対象とするドメインの複数のユーザに対して、同じ IP アドレスから連続して送信が行われる場合が多い。このことから、メールの受信として使用することのない架空のメールアドレスを〝おとり〟として、スパマーの送信先リストに加えさせ、このおとりメールアドレスに対して送信を行う送信元 IP アドレスをスパマーとしてリアルタイムに補足する。これをスパム判定の要素として利用するという仕組みである。

3.3 使い捨て別名メールアドレス

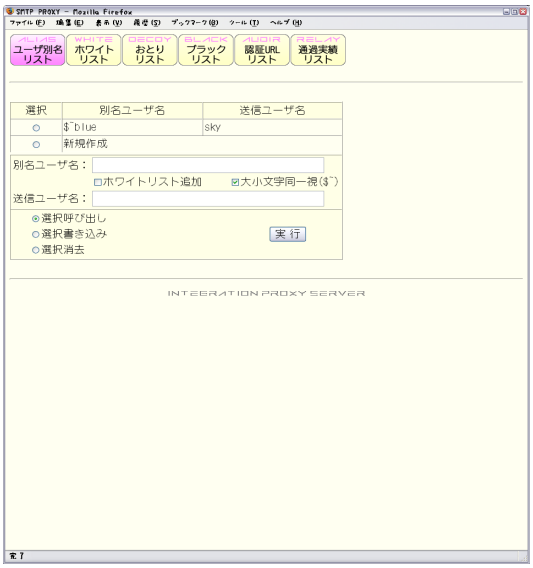
スパムメールが氾濫している現在、もはやメールボックスと同じメールアドレスを他人に通知すべきではない。信頼できる相手であっても、PC の脆弱性などによって、メールアドレスが漏洩することは珍しくない。よって、できるだけ通信相手ごとに、使い捨ての別名メールアドレスを作成し、スパムメールが届いた場合、その原因ルートを把握可能とするとともに、当該別名メールアドレスを削除することが、効果的なスパム対策である。

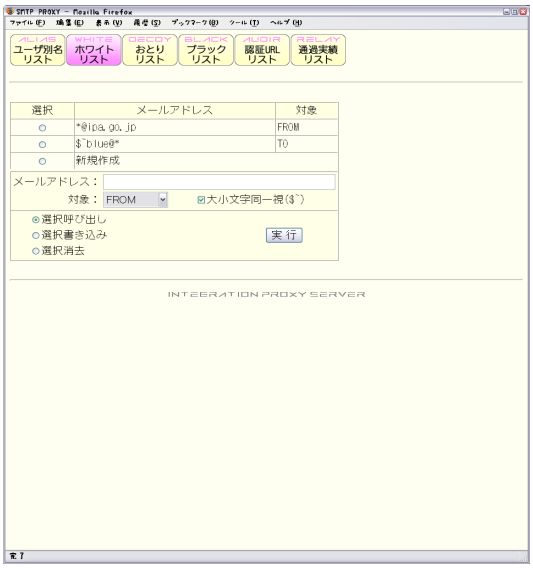
これをシステム管理者ではなく、ユーザ自身が、簡単なユーザインタフェースにより、登録、削除できる仕組みを実現した。

3.4 ホワイトリスト

これは、前述の「別名メールアドレス」と組み合わせて使用することが望ましい。メーリングリストなどの、通知 URL をクリックできない相手に対して有効であり、これに登録されているメールアドレス（FROM または TO の選択が可能）について、URL クリック認証を行うことなく、メールを通過させる。

これも、簡単なユーザインタフェースにより、ユーザ自身が、登録、削除できる。





3.5 セカンダリサーバ同期機能

スパム判定アルゴリズムでは、ALIAS(ユーザ別名リスト)、WHITE(ホワイトリスト)、DECOY(おとりリスト)、BLACK(ブラックリスト)、AUDIR(認証 URL リスト)、RELAY(通過実績リスト)の６つのリストが参照および更新される。

これらリスト群は、本ソフトウェア稼働サーバ間でリアルタイムに共有することができ、これにより、本ソフトウェア起動ホストを複数台、立ち上げ、負荷分散させることができる。通信プロトコルは、SSL 暗号化通信に対応しており、インターネットを経由したホスト間共有も可能である。

3.6 TLS 暗号化対応

RFC3207 による TLS に対応している。フォワード先 SMTP サーバの対応は必要なく、本システムにより、デコードしてフォワード可能である。接続元、フォワード先、またはその両方について、TLS 通信を行うかの設定ができる。

3.7 負荷分散、IPv6 対応

フォワード先 SMTP サーバを、複数指定することができ、その場合、負荷を分散して接続を行う。SMTP サーバの障害やメンテナンスにより接続できないサーバが含まれても、接続可能な SMTP サーバに対して、メールのフォワードを行う。

また、接続元、フォワード先について、どちらも、IPv4、IPv6、その両方の設定が可能である。接続元、フォワード先で異なる場合は、プロトコル変換を行う。

4. 従来の技術との相違

スパム対策は多く行われているが、異なるプロトコル(HTTP)の組み合わせをベースとする対策技術は、恐らく、このソフトウェアが初めてである。従来のメール内容や逆引きホスト名によるフィルタリングでは、誤判定により、必要なメールが到着しないという問題が発生するが、送信者に指定の URL をクリックさせるという手法では、クリックされることのないスパムメールを確実に排除することができる。

5. 期待される効果

SMTP PROXY は、本ソフトウェアの１つの機能である。セキュリティ対策として重要なのは、サーバサイト側、クライアント側ともに、PROXY サーバを導入することであり、このマルチプロトコル PROXY サーバが普及すれば、インターネット全体のセキュリティ向上が期待できる。

6. 普及の見通し

本ソフトウェアの普及は、セキュリティ対策の最適解が PROXY 導入にあるという理解の広がりに依存する。システムを直接、インターネットにさらすことの危険性と、PROXY によるその回避能力を解説してゆく必要がある。

7. 開発者名

大村研治(有限会社ジーエックス)
http://gxnet.jp/
http://gxnet.jp/gxs/