逆 PROXY 型 Web サーバ拡張システム

ーPROXY は最強のセキュリティ対策ー

1. 背景

インターネット人口の増加に呼応するかのように回線速度は向上し、いまや一般家庭にさえ光ファイバが普及する時代となった。しかしながら、多くのサイトのサーバ処理能力向上といえば、とても緩慢だといわざるを得ない。集中しがちな人々の関心によるトラヒック集中に備えることはおろか、普段のアクセスでさえストレスを感じるサイトは非常に多く、こうしたロス時間は、多忙な現代人には深刻な問題といえる。あるいは、経済的損失にさえ、波及しているといえるのではないだろうか。

インターネットの快適さ向上には、これら多くのサイトシステムの環境改善が必要であるが、技術的問題やコスト的問題を抱えるサイトは少なくない。

2. 目的

今後、ますます高度化するシステム環境を見据え、本プロジェクトでは、逆 PROXY を中心とした統合サーバの開発により、LAN と WAN を結ぶパイプラインのセキュアな集約と LAN 内分散性を図り、インターネット環境の向上を促進することを目的とする。

3. 開発の内容

システムのコアとなるセッション管理モジュールおよび、以下の機能群を開発した。

・逆 PROXY サーバ機能

後述の PROXY サーバに対して、逆 PROXY サーバは、サーバ側環境に配置され、クライアントからのリクエストにより Web サーバと情報交換を行い、それをリクエストを行ったクライアントに対して送信するというシステムである。Web サーバは、インターネットに直接さらされないため、脆弱性保護などによるセキュアなサイト環境が実現できるほか、負荷分散として複数台の Web サーバを配置し、サイトレスポンスを高速化するなどの効果がある。

こうした基本機能に加え、本機能では、SSL、IPv6 に対応し、デコードあるいはプロトコル変換したリクエストを、Web サーバに対して送信することができる。

・Web サーバ機能

HTTP プロトコルを解釈し、基本的な Web サーバとしての機能を実現する。

・負荷分散機能

サーバへの再接続処理について、複数台のサーバを接続先候補とし、負荷率の小さなサーバに対して優先的に接続する機能である。また、前述の Web サーバと逆 PROXY サーバを同時に起動することにより、サーバ負荷の小さなときには Web サーバとして処理し、サーバ負荷が大きくなると、逆 PROXY サーバとして外部 Web サーバに処理を分散させることができる。

・クライアント認証機能

Web サーバおよび逆 PROXY サーバとしての機能であり、ブラウザからのアクセスについて、ID とパスワードによりクライアントを認証し、Cookie などによりログイン状態を維持管理する機能である。ID とパスワードを要求する画面や、パスワード変更、エラーなどの画面は、html として自由にデザインできるほか、タイムアウトまでの秒数や、パスワードエラーによるアクセス制限などを設定することができる。

・ブラウザによるアカウント情報設定機能

　管理者は、ブラウザにより、アカウントの追加、削除、パスワード変更を行うことができる。パスワードは、指定のパスワードファイルに、ハッシュ値として保存される。

・パスワードサーバ機能

　パスワード情報を、異なるサーバ機器に配信する機能である。これにより、複数台のクライアント認証機能稼働サーバ間において、アカウント情報を共有させることができる。

・ログサーバ機能

　ログ情報を、集中管理するための機能である。これにより、複数台のサーバログを１個のファイルに集約することができる。

・ポートフォワード機能

　HTTP プロトコルを解釈することなく、ダイレクトに指定のサーバに再接続する機能である。再接続先サーバを複数指定することにり、負荷分散が可能である。

・PROXY サーバ機能

　インターネットでは、ブラウザなどのクライアントと、Web サーバなどのサーバが存在し、クライアントがサーバにアクセスすることによって、サーバとの情報交換が行われる。しかし、クライアント端末を直接インターネットにさらすことは、クライアント環境の脆弱性や不正アクセスなどの面でリスクが高い。こうした問題に対して、PROXY サーバは、クライアント側環境に配置され、クライアントからのリクエストを代行してインターネット上のサーバにアクセスし、受け取った情報を、リクエストを行ったクライアントに再送信するというものである。
　こうした基本機能に加え、本機能では、IPv6 プロトコル変換や、リクエスト内容に基づく、細かなアクセスコントロールを設定することができ、さらなるクライアントの安全性が確保できる。

4. 従来の技術との相違

複数台のサーバ機器への分散性と連携性、実行時における省メモリ性は、サーバソフトウェアとしてトップレベルの性能を持つ。

5. 期待される効果

Web サーバの脆弱性をプロテクトする効果や、指定ディレクトリに対するクライアント認証機能などにより、運用における多くの負担軽減が期待できる。

6. 普及の見通し

本開発成果は、オープンソースとして公開する予定であり、平易なユーザインタフェースを目指して開発していることから、環境向上を望むすべてのサイトが対象となる。また、逆 PROXY というアプローチにより、既存システムをほとんど変更することなく環境改善が実現できることから、保守的なサイト管理者にも受け入れやすく、広く普及することが期待できる。

7. 開発者名

大村研治(有限会社ジーエックス)
（参考）http://gxnet.jp/