FPGAによるパケットフィルタリング処理の高速化

長尾 宗胤†　　冨澤 眞樹†
前橋工科大学工学部†

1. はじめに

近年，インターネットは電気や水道と並ぶ社会基盤の一つとしての役割を担うようになってきた．同時に，インターネットに対するサイバー攻撃の脅威も大きくなっているのが現状である．

サイバー攻撃の一つである DoS 攻撃は，攻撃対象のシステムに対し過大な負荷をかけ，その正常な稼動を妨害する悪質な行為であり，対策が急務となっている．

本稿では DoS 攻撃に焦点を当て，NIC（Network Interface Card）にハードウェア(FPGA)によるパケットフィルタリング機能を付加し，処理速度の高速化と攻撃検出精度の向上を実現するための手法について提案する．

2. DoS 攻撃の防御手法

DoS 攻撃からシステムを防御する手法として，IPS(Intrusion Prevention System)と呼ばれる装置を使用する手法と，ソフトウェアを使用する手法がある．

IPS による防御手法は図 1 に示すように，IPS をネットワーク上にインラインで設置し，ネットワークを流れるパケットを検査対象とし，DoS 攻撃を検知・防御する手法である．

ソフトウェアによる防御手法は図 2 に示すように，保護対象サーバに DoS 攻撃の検知・防御を行う防御モジュールをインストールし，大量のアクセスを行うクライアントからのトラヒックを遮断することにより，システムを保護する．

この手法では，サーバプロセスの稼動状態や，システムが記録するログなどを検査対象とし，攻撃を検知した場合はその原因となっているトラヒックを遮断する．

一般に広く利用されている Web サーバである Apache では，DoS 攻撃からサーバを保護する機能は，モジュールとしてサーバ本体とは別に配布されている．（例：mod_dosdetector） このように，防御モジュールはサーバソフトウェアのサブセットとして提供されることが多いため，サーバソフトウェアごとに防御モジュールをインストールする必要がある．

次項では，ソフトウェアとパケットフィルタリング機能を付加した NIC により，DoS 攻撃対策を行うアプローチについて述べる．

Speed-up of packet filtering by FPGA.
†Toshitsugu NAGAO, † Masaki TOMISAWA
†Dept. of Engineering, Maebashi Institute of Technology.

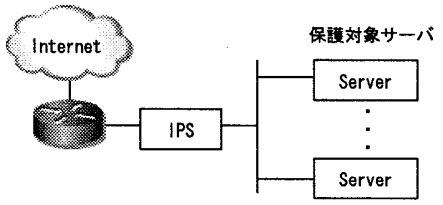

図1　IPS による防御

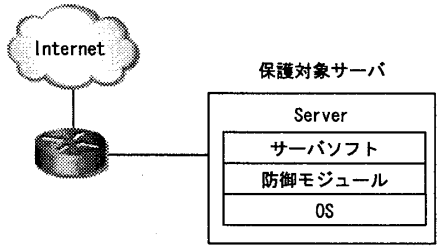

図2　ソフトウェアによる防御

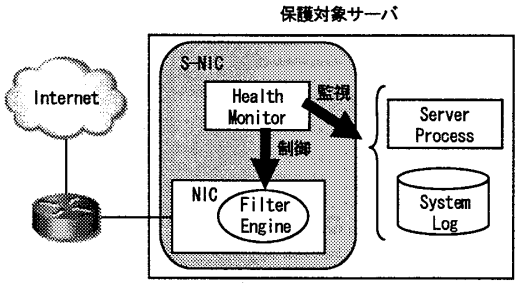

図3　S-NIC のシステム構成

3. パケットフィルタリング機能を付加した NIC による DoS 攻撃対策

本稿で提案する手法は，パケットフィルタリング機能を付加した NIC と，保護対象の内部状態を監視するソフトウェア(Health Monitor)を組み合わせることにより，DoS 攻撃からシステムを保護するものである．我々はこの手法を

Secure な NIC から「S-NIC（エスニック）」と命名した．S-NIC のシステム構成を図 3 に示す．

NIC には，FPGA を使用して構成する Filter Engine を搭載し，レイヤ 3 レベルのパケットフィルタリングをハードウェアにより行う．Health Monitor は，従来のホストベース IDS をベースにしたもので，システムログやサーバプロセスの稼動状態などを監視し，DoS 攻撃の検出と Filter Engine の制御を行う．S-NIC による DoS 攻撃の防御プロセスを次に示す．

(1) Health Monitor が，ログやプロセスの動作状態から，DoS 攻撃を検出する．
(2) Health Monitor は，攻撃元の IP アドレスを Filter Engine に通知する．
(3) Filer Engine は，Health Monitor から通知された IP アドレスをメモリ内のブラックリストに登録し，攻撃元 IP アドレスからのパケットを遮断する．
(4) ブラックリストに登録された IP アドレスからのトラヒック量を測定し，DoS 攻撃が終了したらブラックリストの登録を解除する．

この手法を導入することにより，期待される効果は次のとおりである．

・パケットフィルタリング処理をハードウェア化することにより，サーバのリソースを消費することなく高速なパケットフィルタリング処理が可能となる．
・サーバの内部状態に着目したパケットフィルタリングが可能となり，攻撃検出精度の向上が期待できる．
・従来，サーバソフトウェアごとに実装されていた防御モジュールを統合することができ，汎用的な DoS 攻撃対策が可能となる．

4. Apache に適用した場合の考察

ここでは Apache が稼動している Web サーバが DoS 攻撃を受けたときと同じ状況を作り出し，本稿で提案する手法の有効性について考察する．

4.1 実験方法

実験に使用したネットワークの構成図を図 4 に示す．Web サーバには Apache2.2.3 を使用し，最大同時接続数(MaxClients)の値を小さくして，意図的にパフォーマンスを低下させ，DoS 攻撃の影響を受けやすいように設定した．攻撃側には Web サーバの負荷試験ツールである「JMeter」を使用して，1 秒間あたり 100 のリクエストを送信するリロード攻撃を行った．

リロード攻撃とは，DoS 攻撃に使用される手口の一つで，Web サーバの処理能力を超える接続要求を送信し，サーバの正常な稼動を妨害する手法である．

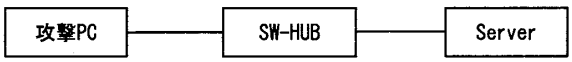

図 4　実験環境の構成

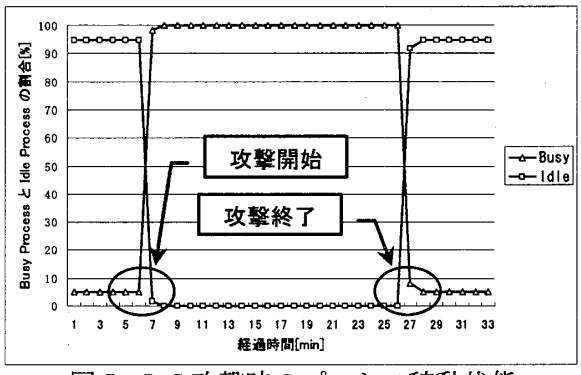

図 5　DoS 攻撃時のプロセス稼動状態

4.2 実験結果

リロード攻撃を行った際の Apache のプロセスの状態を図 5 に示す．この図から，攻撃を受け始めるとすぐにアイドル状態のプロセスが無くなり，全プロセスがリロード攻撃によるリクエストの処理に費やされていることがわかる．

4.3 考察

実験結果から分かるように，リロード攻撃を行った際には，プロセスの稼動状態が大きく変化する．S-NIC ではこの変化を Health Monitor で検出し，NIC で攻撃元からのパケットを遮断する．これにより，DoS 攻撃の影響を最小限にとどめることが可能になる．

5. まとめ

本稿では，ハードウェアを使用したパケットフィルタリングによる DoS 攻撃の検出・防御手法について提案した．現在，S-NIC の実現に向けて研究を継続中である．

参考文献
[1]警察庁：DoS/DDoS 対策について
http://www.cyberpolice.go.jp/server/rd_env/pdf/DDoS_Inspection.pdf
[2] 出雲教郎：DoS 攻撃対策製品の仕組みと特徴
http://www.atmarkit.co.jp/fsecurity/special/61dos/dos01.html
[3] 小倉秀敏：IPS の実装方法と防御技術とは
http://www.atmarkit.co.jp/fsecurity/special/59ips/ips01.html
[4] 田中慎司：Apache における DoS 攻撃対策手法
Software Design 2007 年 9 月号　技術評論社