NTT-AT

サーバの過負荷対策を低コストで実現するサーバ制御ソフトウェア「ServDefense」

過剰トラヒックからサーバを防御する過負荷対策を簡易に

インターネットは、今やビジネスや生活のインフラといっても過言ではない。快適なサービスを提供するために、安定・堅牢なサーバ運用システムは不可欠だ。しかし一時的なアクセスの集中、あるいはDoS（Denial of Service）攻撃などの不正トラヒックが原因で、Webサーバ等が過負荷状態に陥り、動作が不安定になったり、ダウンしてサービスが提供できなくなったりすることがしばしば見受けられる。

このような過剰トラヒックからサーバを防御する方法として、これまで一般的には、侵入検知システム（IDS；Intrusion Detection System）／侵入防止システム（IPS；Intrusion Prevention System）の導入や、負荷分散装置によるサーバシステムの冗長化などの対策がとられている。しかし実際には、これら対策は以下のような課題を抱えている。

IDS/IPSでは、過剰トラヒックを検知した際に誤検知（正常トラヒックを誤って不正と判定）し、正常ユーザーへのサービスを誤って強制中断してしまう可能性があるため、遮断実行は人手で制御しているのが実情で、24時間人手による管理が必要となる。さらに、トラヒックやサーバの異常を検知してから実際に対処するまでに時間がかかり、問題の即時対応ができない。

一方、負荷分散システムは、サーバへのリクエスト量をベースに負荷を分散処理するものの、リクエストごとにサーバに及ぼす負荷の度合いが異なるためサーバリソースを有効活用できない。また、トラヒック集中のピーク時に合わせて事前に設計しておくことは実質的に不可能で、過剰トラヒックには対応することができない。

このような課題を解決するため、運用稼動を減らし簡易化できる過負荷対策システムが求められている。

NTTアドバンステクノロジ㈱
アクセスネットワーク事業本部
（左）ブロードバンドビジネス開発ユニット　熊澤　潤氏
（右）第一営業部　主査　塩井　桂氏

安定・堅牢にサーバを動作させる「ServDefense」

NTTアドバンステクノロジ（NTT-AT）では、既設のネットワーク設備をそのまま利用し、過剰トラヒックによるサーバのダウンや処理不能を防止し、サーバを安定・堅牢に動作させることができるソフトウェア「ServDefense」を販売している。

「ServDefenseは、NTT未来ねっと研究所が開発した“IPFICSER”技術を基に、NTT-ATが製品化し販売するソフトウェアです。既設サーバに実装することで、サーバの実稼動負荷を診断して稼動を最大限に保ちつつ安定運用を図るほか、不正アクセスを検知する侵入検知システム（IDS）との併用で、IDSからの検知結果を基にサーバ前段のネットワークスイッチを制御して自動的に過剰トラヒックを規制することができます。」（アクセスネットワーク事業本部　第一営業部　塩井 桂主査）

ServDefenseは、サーバが提供するサービスを安定して継続できるように、サーバでやり取りするトラヒックを制御するソフトウェアである。図1に示すように、サーバの稼動負荷状態（CPUリソースの消費状況）と、IDSからの不正アクセス情報を集約・評価し、設定してある制御レベルに応じた制御コマンドに

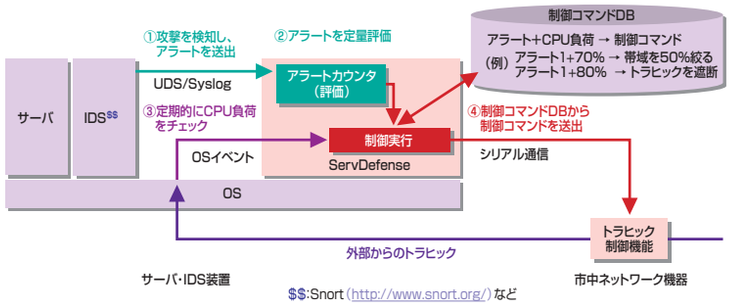

図１　ServDefenseの主要技術：サーバ負荷・アラート連動型トラヒック制御

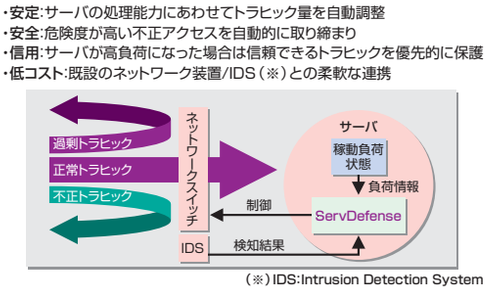

図２　ServDefenseの４つのポイント

よってトラヒックを自動的に調整することで、サーバのリソースを最大限に活用しつつ安定した運用を可能にしている。

「ポイントは、過負荷によるサービス提供不能を避けつつ、正常トラヒックを可能な限り受け入れるという点です。単純にトラヒックを規制するのではなく、サーバの正常な運用が難しくなってきた時にトラヒックを規制することを基本としています。」（アクセスネットワーク事業本部 ブロードバンドビジネス開発ユニット　熊澤 潤氏）。つまり、DoSのような大量パケットによる攻撃に対しては、サーバが過負荷とならない限りトラヒック規制は行わず、サーバが過負荷となった時点で、IDSが検知した不正トラヒックから優先的に規制する仕組みとなっている。

安定・安全・信用・低コストを実現

ServDefenseの最大の特長は、図２に示すように、安定・安全・信用・低コストを実現したことにある。

CPUの稼動状況を直接モニタリングし、サーバの処理能力に合わせてトラヒック量を自動調整することで、サーバのリソースを最大限に活用しつつ安定した運用が可能であるほか、フリーIDSのSnortなど、不正侵入検知システムとの併用で、危険度が高い不正アクセスからサーバを防御することが可能である。また、サーバが高負荷になった際には信頼できるトラヒックを優先的に保護するため、ユーザーの信用を得ることができる。さらに、既設のサーバに実装でき、しかもサーバ負荷・アラート連動型トラヒック制御技術によって高スキル管理者も不要なため、低コストで運用が可能である。加えて、汎用入出力インタフェースを採用しているため、既設のネットワーク装置／IDSとの柔軟な連携が可能で、導入コストの削減、マルチベンダ化を実現できる。

表１に、IDS/IPSや負荷分散装置との機能比較を示す。ServDefenseは、①サーバの実稼動に応じた制御、②トラヒック監視、③サーバの監視結果とトラヒック監視結果を総合的に判断してトラヒックを制御できるという点に大きな優位性がある。なお、単位時間当りのリクエスト量（処理量）を増やせるという優位性を持つ負荷分散装置とServDefenseを組み合わせることで、より可用性の高いサーバの過負荷対策が可能だ。

ServDefenseは以上のような特長に加え、税込み価格30万円と安価であることから、Web、FTP等のサーバ運用・管理など、幅広い分野での適用が期待される。

表１　類似製品との機能比較

	カテゴリ	IDS/IPS	ServDefense	負荷分散装置	ServDefense＋負荷分散装置
サーバ監視	単位時間当たりのリクエスト数に応じたトラヒック制御	×	×	○	○
	サーバの実稼動に応じた制御	×	○	×	○
トラヒック監視	進入検知結果に応じたトラヒック制御	○	○	△	○
	検知結果の集約制御と、集約結果に応じたトラヒック制御	△	○	×	○
サーバ監視結果とトラヒック監視結果の組み合わせに応じたトラヒック制御		×	○	×	○
トラヒック制御	アドレス情報に基づく遮断	○	スイッチ依存	○	○
	コネクション切断要求の送信	○	○	○	○
	帯域制限、優先度制御	×	スイッチ依存	○	○
	不正パケットの即時廃棄	○	△※1	○	△　※1
	トラヒック分流	×	×	○	○

※１　不正パケットの即時破棄が必要な場合は、アンチウィルスソフト等を併用する。

お問い合わせ先
NTTアドバンステクノロジ㈱
アクセスネットワーク事業本部
ServDefense担当
TEL：045-826-6485
E-mail：servdefense@ntt-at.co.jp