

ファイアーウォール製品調査

2002.12

ファイアーウォールの分類

● パケットフィルタリング型

- IPパケットのヘッダ情報(IPアドレス、ポート番号など)といった静的ルールで判断し、不正アクセスを防ぐ。
- OSI基本参照モデルで例えると、ネットワーク層で動作するファイアウォールである。(ルータやスイッチのアクセスリストなどと同様。)

● ステートフルパケットフィルタリング型

- パケットフィルタリングを拡張した方式。IPパケットのヘッダ情報だけでなく、時間や履歴といった、動的ルールで判断する。単純にパケット単位でフィルタリングするのではなく、アプリケーションレベルで双方向の通信をチェックして、パケットを通過させるか否かを判断する。
- OSI基本参照モデルの3層(IPヘッダ情報)と4~7層(ペイロード情報)を参照する。

● アプリケーションゲートウェイ型

- 通信を中継するプロキシプログラムを利用し、内部ネットワークとインターネットの間で直接通信をできないようにする方式。
- アプリケーション層のファイアウォールである。(プロキシサーバと同様の動作。)

分類別ファイアウォール比較

	パケットフィルタリング型	ステートフルパケットフィルタリング型	アプリケーションゲートウェイ型
長所	<ul style="list-style-type: none">・高いパフォーマンス・アプリケーションに依存しない	<ul style="list-style-type: none">・高いパフォーマンス(パケットフィルタリングよりは低速)・アプリケーションに依存しない・IPヘッダ情報とペイロード情報を参照することで、セキュリティレベルを強化	<ul style="list-style-type: none">・アプリケーション層で詳細にアクセス制御を実行するため、高いセキュリティレベルを実現(ex: FTP のGet は許可するが、Put は許可しないなど)・アプリケーションレベルのログが取得できる(ex:URLなど)
短所	<ul style="list-style-type: none">・ルールの定義が煩雑になりやすい・IPヘッダ情報のみで判断するため、セキュリティレベルが低い・アプリケーションレベルでのアクセス制御ができない	<ul style="list-style-type: none">・高負荷時にステートテーブル更新処理がボトルネックになる場合がある	<ul style="list-style-type: none">・パフォーマンスが悪い・各アプリケーションプロトコルごとに個別のプロキシプログラムが必要

製品動向

・IPSec NAT 対応

- 従来、IPSec標準ではNATに対応できなかったが、最近ではIPSec環境でもNATなどのアドレス変換を併用できる製品が増加している。
- 標準化が検討されている。(インターネットドラフト(RFC となる前の段階))
 - “UDP Encapsulation of IPsec Packets”(<http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-05.txt>)

・VPN

- VPN機能は、ほぼすべてのファイアーウォールが標準装備している。
- アメリカ政府がDESの後継として採用したAES(Advanced Encryption Standard)対応の製品が増加している。

・アプライアンス型

- ISP、IDCなど大規模バックボーンユーザの需要に応えるため、下記項目を考慮して開発を進めている。
 - ・電源の二重化
 - ・ロードバランスと二重化構成
 - ・暗号化のみ専用ボードで処理 など

・個人ユーザ向けファイアーウォール

- パーソナルファイアーウォールの普及。
- WindowsXPではファイアーウォール機能(ダイヤルアップ接続時にデフォルトでファイアウォール機能が作動する)が搭載された。