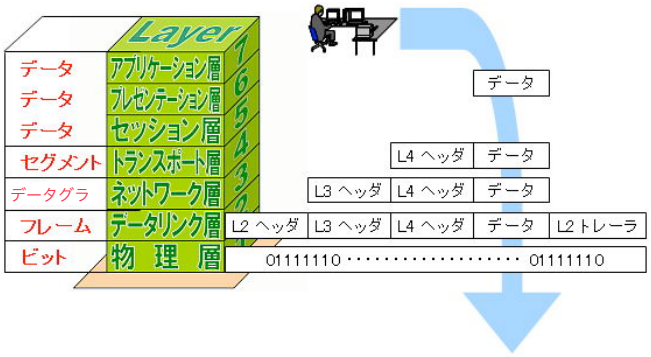
情報セキュリティ特論II 資料

UDP・TCP とファイアウォール

2023.1

UDP (user datagram protocol) の役割

UDPはOSI第4層のプロトコルの一つであるが，TCP（後述）と異なり，リアルタイム性を損なう確認応答や再送、輻輳制御機能がない。そのため，リアルタイム性が要求されるインターネット電話やビデオ転送などに用いられている。確認応答などの機能が必要な場合は上位層で実装する必要がある。

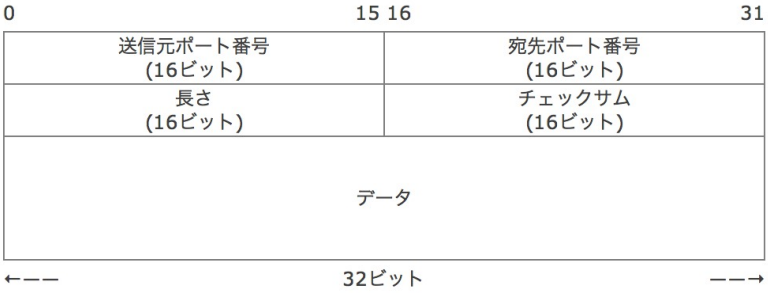


http://atnetwork.info/tcpip/tcpip24.html より

UDPセグメントの構造

UDPセグメントはUDPヘッダ部とデータ部からなる。

データ長の最大は 65507バイト（最大IPデータグラム長 65535 - IPヘッダ 20 - UDPヘッダ 8）である。



http://atnetwork.info/tcpip/tcpip30.html より

フィールド	説明
送信元ポート番号(16bit)	送信元のアプリケーションを識別するための番号 0～65535。 返信を要求しないUDPセグメントの場合は、送信元ポート番号を0にする。
宛先ポート番号(16bit)	宛先のアプリケーションを識別するための番号 0～65535。
長さ(16bit)	UDPセグメントの長さ。データ部分の長さを加えたバイト数。
チェックサム(16bit)	チェックサム計算のでは、UDP擬似ヘッダ(12bytes)、UDPヘッダ(8bytes)、UDPペイロードの3つを使用する。※UDP擬似ヘッダは、チェックサムの計算時にだけに使われる仮想的なヘッダ。
データ	UDPのデータ部。

TCP (transmission control protocol) の役割

TCPはOSI第4層のプロトコルの一つであり，上位アプリケーションとネットワークの先にあるアプリケーション間での仮想回線を確立する役割がある。そのために，セグメント分割と再組み立て，ウィンドイングによる効率的なセグメントの転送，輻輳制御，セグメントの再送などの機能を持つ。

TCPセグメントの構造

TCPセグメントはTCPヘッダ部とデータ部からなる。

フィールド	説明
送信元ポート番号(16bit)	送信元のアプリケーションを識別するための番号(1～65535)。
宛先ポート番号(16bit)	宛先のアプリケーションを識別するための番号(1～65535)
シーケンス番号(32bit)	送信するデータ1バイトごとにシーケンス番号を1つずつ増やす。
確認応答番号(32bit)	受信が完了したデータ位置のシーケンス番号＋1を返す。 ACKフラグがONの場合にのみ、ACK番号フィールドを有効とする。
ヘッダ長(4bit)	TCPデータが始まる位置を表すフィールド=TCPヘッダのサイズ。
URG(1bit)	URG　・・・　urgent：緊急。1でON。
ACK(1bit)	ACK　・・・　acknowledge 有効なACK番号がTCPヘッダに含まれていることを示すフラグ。TCPの3ウェイハンドシェイク時の一番最初を除き、他の全てのTCPセグメントは、ACKのフラグはON。
PSH(1bit)	PSH　・・・　push 受信したデータをすぐにアプリケーションに引き渡すように要求するためのフラグ。
RST(1bit)	RST　・・・　reset　　TCP接続を中断、拒否したい場合にセットされるフラグ。
SYN(1bit)	SYN　・・・　synchronize TCPの3ウェイハンドシェイク時のオープン処理の開始に双方のそれぞれがSYNフラグがONにして、ACK番号を同期させる。以降のパケットにはセットされない。
FIN(1bit)	FIN　・・・　finis　　TCP接続を終了させるためセットされるフラグ。
ウィンドウサイズ(16bit)	受信側のウィンドウサイズを相手に伝えるために利用されるフィールド。 単位はバイトで、最大65535バイト。0は、データを受信不可を表す。
チェックサム(16bit)	TCPセグメントの整合性を検査するための検査用データが入るフィールド。
緊急ポインタ (16ビット)	URGフラグが1の場合のみ有効。 緊急データの場所を表す。
オプション	TCP接続の特性を設定するために利用される可変長のフィールド。MSSのやり取りなどに利用される。32ビットの倍数になるように、必要に応じて最後にパディング（0）。
データ	TCPのデータ部。タイムアウトして切断されないようにデータを含まないTCPヘッダだけのパケットを送る場合もある。

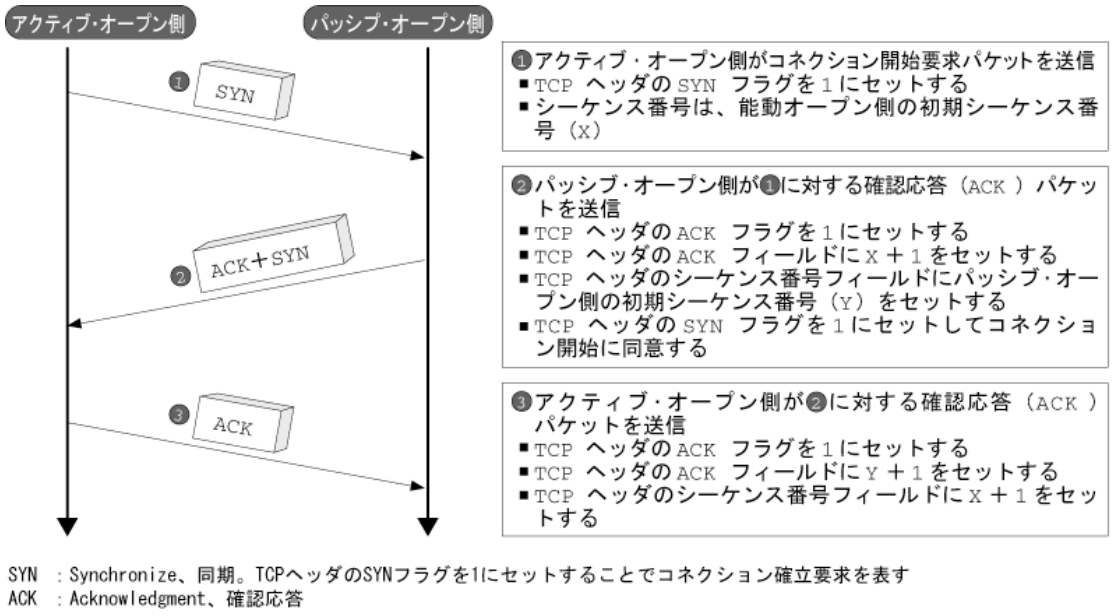
http://atnetwork.info/tcpip/tcpip29.htmlより

ポート番号の種類 (http://ja.wikipedia.org/wiki/ポート番号)

種類	範囲	内容
WELL KNOWN PORT NUMBERS	0番 - 1023番	一般的なポート番号
REGISTERED PORT NUMBERS	1024番 - 49151番	登録済みポート番号
DYNAMIC AND/OR PRIVATE PORTS	49152番 - 65535番	自由に使用できるポート番号

TCPセッションの確立 (3way handshake)

TCP通信は，コネクション型の通信なので，相手側との通信をはじめるにあたり３ウェイ・ハンドシェイクという方法で「セッシンの確立」をする。



3ウェイ・ハンドシェーク

http://dictionary.rbbtoday.com/Details/term1259.html より（リンク先消失）

セッションが確立された後で，上位層（アプリケーション間）の通信（http, smtp など）が行われる。

ネットワークのアクセス制御

TCP/IP 通信：IPアドレス＋ポート番号で接続先のサービスを指定する
デーモン daemon - 自律的に動いているサービス
スーパーデーモンとしての inetd, xinetd と tcp_wrapper
well known port 0-1023 (http:80, smtp:25, ssh:22,,,)
/etc/services というファイルに記述がある

ファイアウォール （firewall: 防火壁）

独立した機器としても存在するが， OS の一機能としても動作させられる（ホストレベルのファイアウォール）
パケットフィルタ（ip_tables, ipfw, pf など）は，サーバの「要塞化」の基本
また，「プロクシサーバ」を使った制御方法もある
「コンテンツ・フィルタリング」のような通信内容で制御が必要な場合

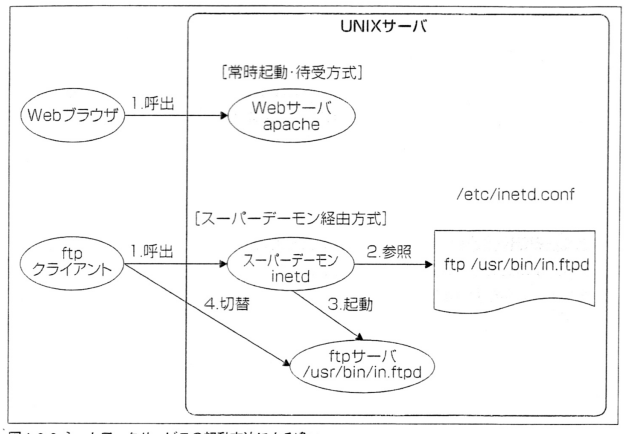


図4-2-3 ネットワークサービスの起動方法による違い

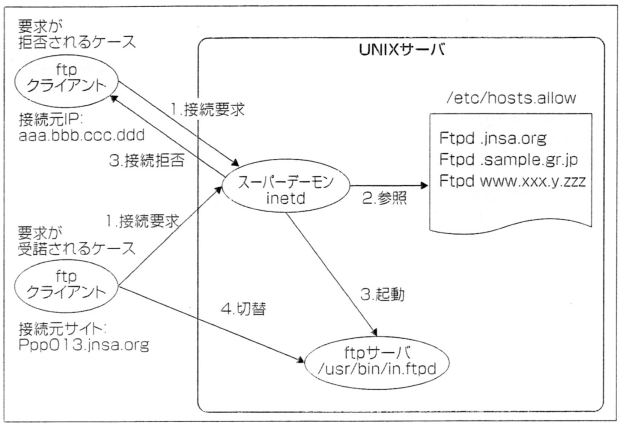


図4-2-5 inetd + tcp_wrappers でアクセス制御をするしくみ

ネットワークサービスの違い（左）とtcp wrapper によるアクセス制御（右）

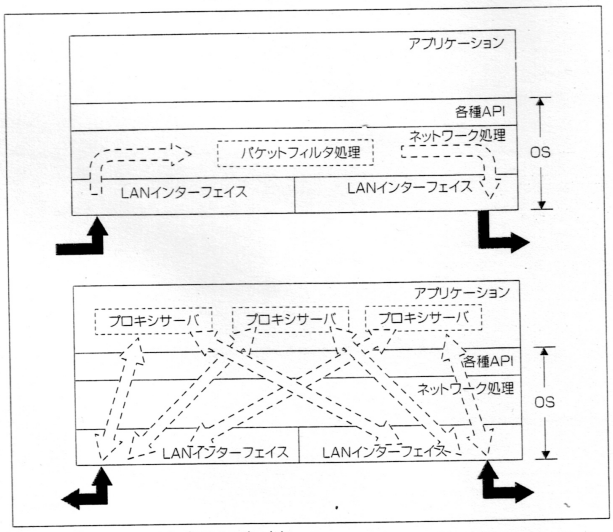
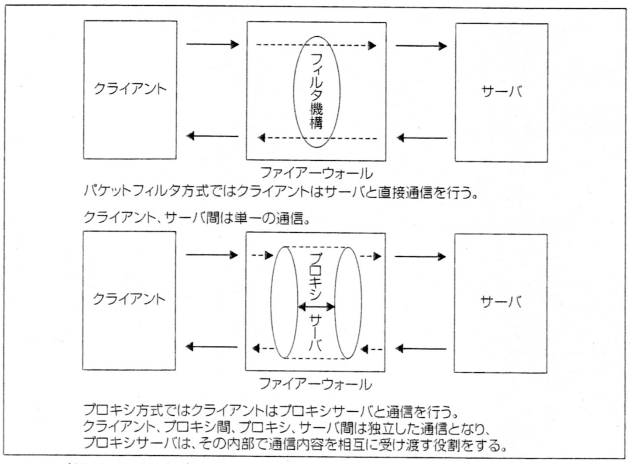


図5-2-1 パケットフィルタとプロキシの違い(1)



パケットフィルタとプロキシの違い(2)

パケットフィルタ (packet filter) とプロキシ（代理） (proxy)

ファイアウォール (firewall) の動作

「ファイアウォール」とは，ホストやネットワーク間の通信を選択的に通過させるシステムの総称。

「SYNフラグの検査によるTCPコネクション確立の拒否」のように，通信データの特定部分を検査して動作させる。

基本的には， IPアドレス，ポート番号，SYNフラグ等で，パケットを選択的に通過させる。

５層以上の通信内容によって通信を選択的に通過させるファイアウォールは，「アプリケーション・ファイアウォール」という。

ルール番号	パケット数	バイト数	ルール
04200	535	26264	deny log tcp from 59.32.0.0/11 to any setup via fxp0
07100	651	38704	deny log tcp from 61.128.0.0/10 to any setup via fxp0
50800	0	0	deny log ip from 218.212.0.0/16 to any dst-port 25 setup via fxp0

ファイアウォール設定とログの例（ipfw)

SYNフラグの検査による通信の拒否

「SYNフラグ」は， TCP パケットの一部に含まれている情報なので，このフラグがオンになっているパケットを通過させない処理をすることで，通信を開始させないようにできる。