応用情報技術者

試験対策テキストⅡ【システムの利用と開発編】

無料体験入学者用

TAC

はじめに

応用情報技術者試験(AP)は2009年春期より実施された試験区分です。対象者像は,

「高度IT人材となるために必要な応用的知識・技能をもち,
高度IT人材としての方向性を確立した者」

とされています。基本情報技術者試験(FE)で求められる基本的な知識に加え,さらに専門的・詳細な内容を含めた応用的知識が問われることになります。

本書は応用情報技術者試験の出題範囲であるテクノロジ系,ストラテジ系,マネジメント系のうち,テクノロジ系の周辺技術要素であるヒューマンインタフェース,マルチメディア,データベース,ネットワーク,情報セキュリティ,そしてシステム開発に関する分野の知識を網羅しています。その上で,読者の皆さんが効率よく学習が行えるよう,基礎的な用語や考え方を分かりやすく解説するように心がけました。

本書により,読者のみなさんが応用情報技術者試験に合格されることを願ってやみません。

TAC情報処理講座

目　次

(5)　ネットワーク層のその他のプロトコル

●ICMP

ICMP(Internet Control Message Protocol)とは，IPを利用した通信においてエラーメッセージや制御メッセージなどを転送するためのプロトコルである。ICMPが転送するメッセージの種類は複数ある。主要なメッセージとその意味を次に示す。

表3.10　ICMPのメッセージ

メッセージ	意　味
エコー応答	エコー要求に対する応答
宛先到達不能	送信元ホストにパケットが到達しない原因を通知する
リダイレクト	最適ルートが使用されていない場合に最適なルータを通知する
エコー要求	宛先ホストまでの到達確認
時間超過	TTL(Time To Live)値が0になったことを通知する

ICMPを利用したプログラムの一つに，pingコマンドがある。pingは，ICMPのエコー要求とエコー応答を利用してネットワークの到達確認を行うコマンドである。

ping 172.16.0.1

のようにIPアドレスを指定すると，そのIPアドレスに対してエコー要求を送信する。エコー要求を受け取ったホストはエコー応答を返すので，エコー応答を受け取れば，「少なくともネットワーク層(IP)レベルではつながっている(パケットが届く)と判断できる。また,「pingの応答は返ってくるのに通信ができない」のであればアプリケーションの設定ミスやサーバプログラムの異常などが，「pingの応答が返らない」のであれば，ネットワーク障害やルータまたはホストの設定ミスなどが考えられる。

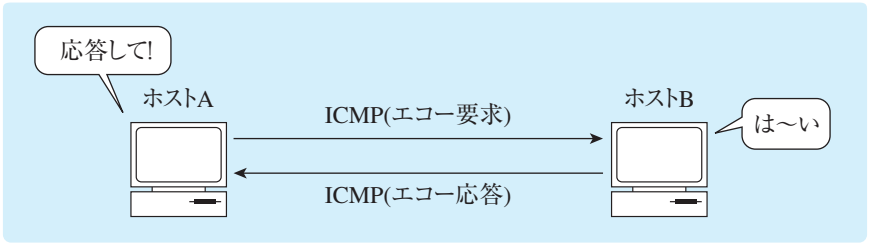


図3.48　ping

参考：traceroute

目的のIPアドレスまでに経由するルータを確認するコマンドにtracerouteとよばれるものがある。tracerouteは，IPヘッダーの生存時間(TTL)を1から順に増やしながらパケットを送付し，ルータがパケットを廃棄したときに通知されるICMP時間超過メッセージを用いて「パケットがどの経路(ルータ)を通るか」を確認する。

●ARP

データリンク層では，宛先(または中継先)までデータを届けるために宛先MACアドレスが必要となる。そこで，IPアドレスからMACアドレスを得るプロトコルのARP(Address Resolution Protocol)が用いられる。

ARPでは，ブロードキャスト(宛先MACアドレスはFF:FF:FF:FF:FF:FF)を利用してネットワーク中の全ノードに対して問合せ(ARP要求)を行い，目的のIPアドレスをもつノードのみがMACアドレスを回答(ARP応答)する。したがって，特殊な仕組みがない限り，ブロードキャストフレームが届かないノードのMACアドレスを得ることはできない。

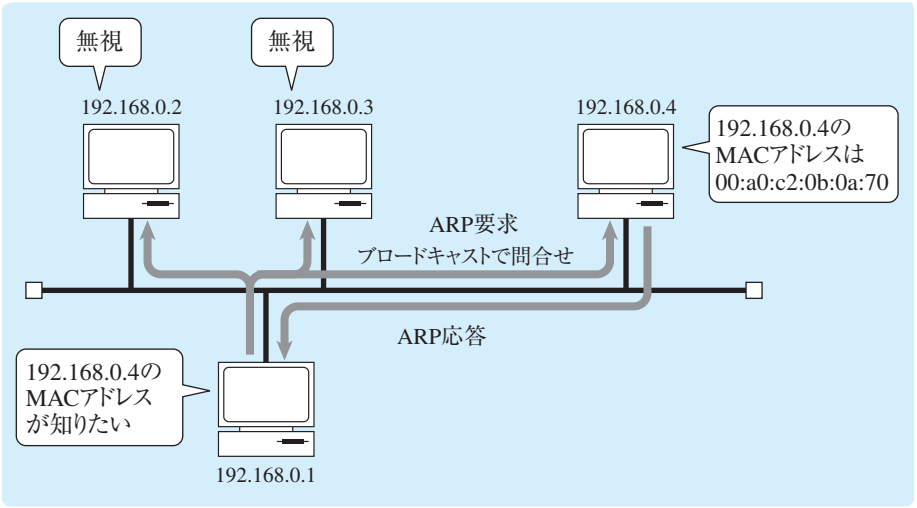


図3.49　ARP

なお，ARPによって得られたMACアドレスは一定時間“キャッシュ”として保持される。キャッシュに保持されたエントリーは，一定の時間が経過すると消去される。

●RARP

ARPの逆の処理，すなわち「MACアドレスからIPアドレスを知る」ためのプロトコルもあり，RARP(Reverse ARP)とよばれる。RARPは，電源を切った際にIPアドレスを保持できない装置が，電源投入時に自身がもつMACアドレスからIPアドレスを知るために用いられる。なお，ARPとRARPは，データリンク層のプロトコルと位置付けられることもある。

学習テーマ　3－7

TCPとUDP

(1)　トランスポート層プロトコルの役割

トランスポート層のプロトコルは，ネットワーク層が実現するエンドノード間の伝送路上で，データの順序制御や伝送誤りの訂正，再送の要求といった一定の品質を保つ制御を行う。

TCP/IPにおいては，TCP(Transmission Control Protocol)とUDP(User Datagram Protocol)がトランスポート層に該当し，それぞれが要求される品質に適した制御を行う。TCPとUDPは，通信データがどのアプリケーション(プロセス)で用いられるかを識別する役割も担う。

●ポート番号

ネットワークには複数のホストが接続され，各ホスト内では複数の通信アプリケーション(プロセス)が存在する。IPアドレスはホストを識別できるが，プロセスまでは識別できない。そこで，TCP/IPではプロセスを識別する16ビット(0 ～ 65,535)のポート番号を用いる。ポート番号は，トランスポート層のヘッダー(TCPヘッダーやUDPヘッダー)内で指定され，受信ホストはポート番号に基づいて「どのプロセスで処理をするか」を決定する。

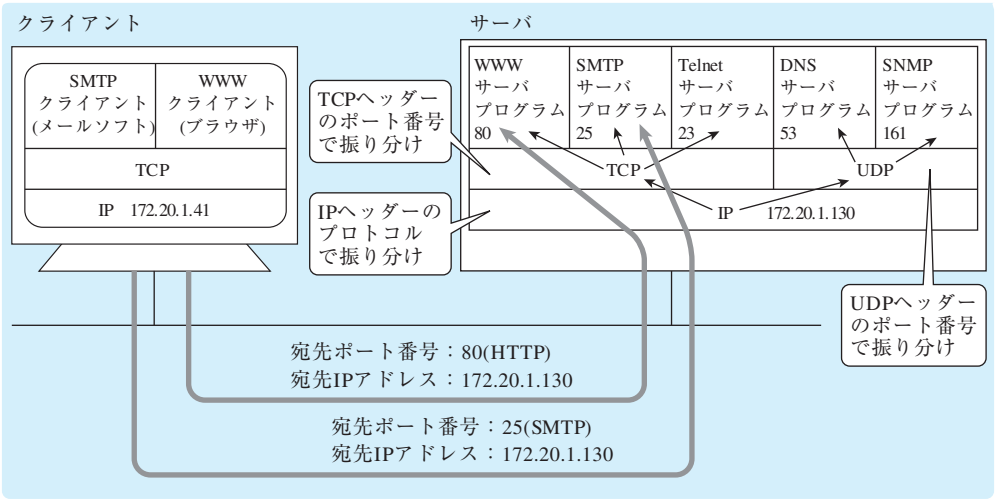


図3.50　ポート番号

・ウェルノウンポート番号

HTTPやSMTP，FTPなどの一般的なアプリケーションについては，あらかじめ標準的なポート番号が設定されている。これをウェルノウンポート番号という。主なウェルノウンポート番号を次に示す。なお，FTPのポート番号が二つあるのは，データの転送用(20)と制御用(21)で異なるポート番号を利用するためである。

表3.11　代表的なウェルノウンポート番号

ポート番号	内 容
20，21	FTP
22	SSH
25	SMTP
53	DNS
80	HTTP
110	POP3
443	HTTPS

通常，各サーバはウェルノウンポート番号を利用するため，クライアント側でポート番号を意識する必要はない。仮にサーバが利用するポート番号を変更すると，ポート番号を知らないクライアントはアクセスができなくなる。クライアントのポート番号は，ホスト内で矛盾が生じないようコネクション(通信の単位)ごとに動的に割り当てられる。

・通信の識別

TCP/IPでは，

送信元IPアドレス，宛先IPアドレス，送信元ポート番号，宛先ポート番号

の組合せによって各通信(どのホスト間のどのプロセス間の通信か)を識別できる。要求パケットに対する応答パケットは，IPアドレス，ポート番号ともに送信元と宛先が入れ替わる。よって，通常はサーバからの応答パケットは，送信元ポート番号がウェルノウンポート番号となる。

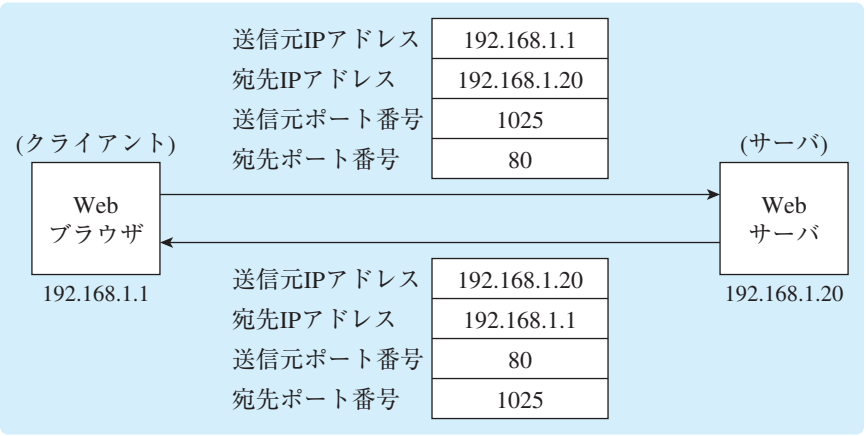


図3.51　IPアドレスとポート番号の関係

【ポイント】

TCPとUDPの役割

→一定の品質(信頼性やスループット)を保つための制御

→上位層(アプリケーション)の特定

(2)　TCP

●TCP の概要

TCP(Transmission Control Protocol)は，コネクション型のトランスポート層のプロトコルであり，コネクションを確立して確認応答やフロー制御などの機能を提供する。このため，信頼性が要求される通信に多く用いられる。TCP におけるデータの伝送単位はセグメントという。

●TCP ヘッダー

TCP では，ヘッダーに含まれる各フィールドの値を用いて信頼性を確保するために必要な制御を実現する。TCP のヘッダーフォーマットを次に示す。

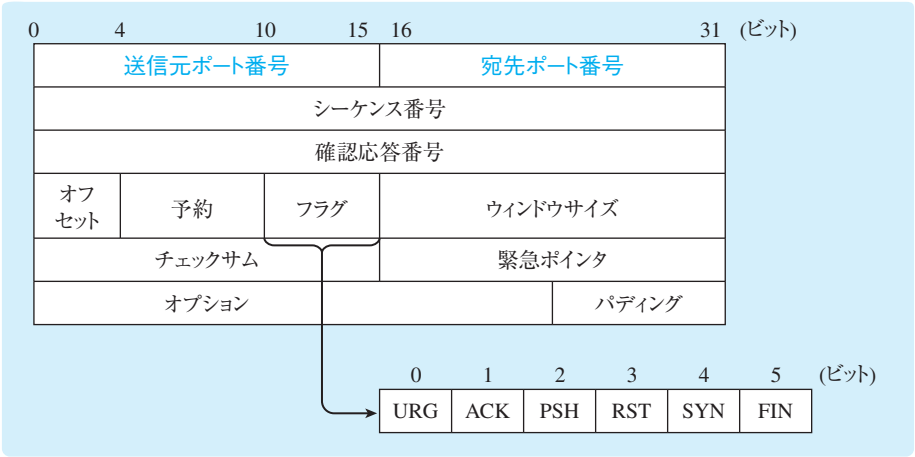


図3.52　TCP のヘッダーフォーマット

●コネクション管理

TCP では，通信に先立って TCP コネクションとよばれる論理的な通信路を確立し，通信終了時にそれを解放する。このコネクションを確立するためには TCP ヘッダー中の SYN フラグと ACK フラグが用いられ，コネクションを解放するために FIN フラグと ACK フラグが用いられる。

コネクション確立から切断までの流れを次に示す。ここで，図中の「SYN = 1」と「ACK = 1」はそれぞれ SYN フラグ，ACK フラグが1に設定された TCP セグメントの送信を表す。この動作は，

① SYN （確立要求）
② ACK + SYN （①への応答＋確立要求）
③ ACK （②への応答）

という三つのセグメントのやりとりで行われることから，スリーウェイハンドシェイクという。

なお，SYN は“SYNchronous（同期）”を，ACK は“ACKnowledge（肯定応答）”NAK は“Negative AcKnowledge（否定応答）”を表す。

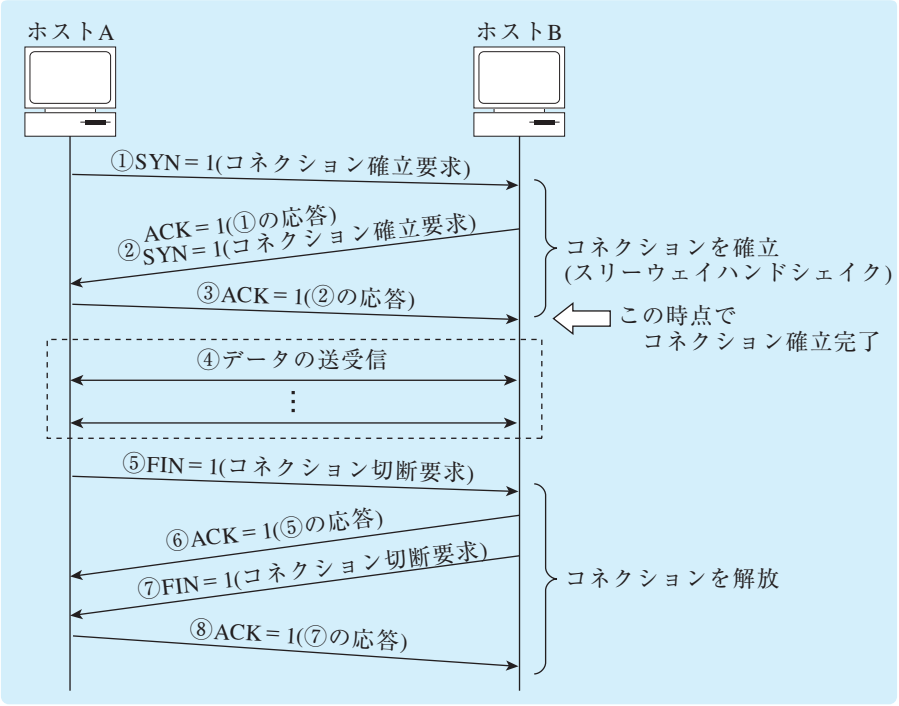


図3.53　コネクション管理

参考：確認応答

TCPでは，シーケンス番号を用いて送受信するセグメントを識別する。シーケンス番号はそれぞれのセグメントに付与される連続番号であり，正しく送受信が行われるとデータのバイト数だけ加算される。たとえば，1,000バイトのデータを送信すれば，次に送信するセグメントのシーケンス番号は1,000加算された値となる。

また，受信側のホストは，ACKフラグに1を，確認応答番号フィールドに「次に受信すべきシーケンス番号」を設定したセグメントを送信元ホストに送信する。これにより，送信元のホストはどのセグメントまで正しく受信されたかを確認でき，ACKが返ってくれば確認応答番号に示された次のセグメントを送信する。また，一定時間内にACKが返らない場合や同じ確認応答番号が返ってきた場合は，エラーやデータの消失などが生じたとみなして再送する。

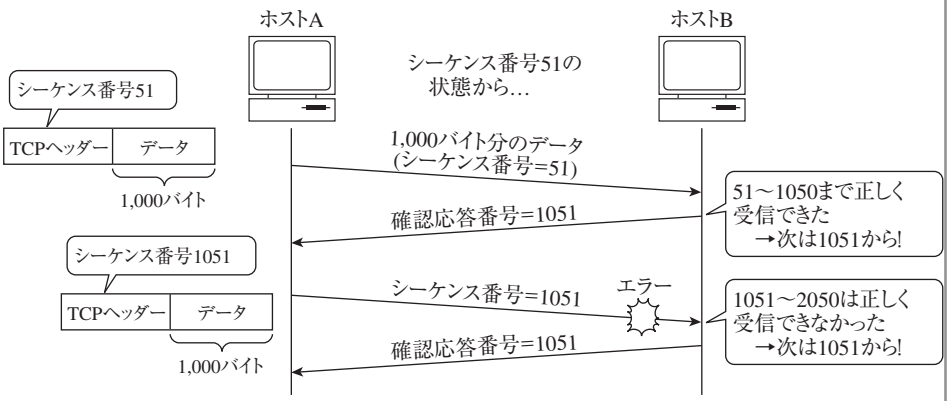


図3.54　確認応答番号

学習テーマ　4－8
ファイアウォール

●ファイアウォールの概念

ファイアウォールは，ネットワークの境界でアクセス制御を行うことにより，インターネットなどの外部ネットワークから，社内LANなどの内部ネットワークを保護する仕組みである。ファイアウォールは，「パケットフィルタリング型」と「アプリケーションゲートウェイ型」に大別されるが，いずれも「どの通信を許可し，どの通信を禁止するか」というルール(ポリシー)に基づいてアクセス制御を行う。

●パケットフィルタリング

パケットフィルタリング型のファイアウォールは，パケットフィルタリングの機能を利用しており，パケットに含まれるIPアドレスやポート番号といった情報をフィルタリングテーブル(ACL：Access Control List；アクセス制御リスト)と照合し，パケットの通過(フォワーディング)や遮断(フィルタリング)を制御する。

パケットフィルタリングでは，特定可能な「IPアドレス」と「ポート番号」を用いて，要求パケットと応答パケットの両方を制御する。たとえば，「内部のWebサーバへのHTTP通信のみを許可」する場合，内部のWebサーバへのHTTP要求と，内部のWebサーバからのHTTP応答のみを許可すればよい。仮に，WebサーバのIPアドレスが123.45.67.89であれば，パケットに含まれるヘッダーの内容は次のようになる。

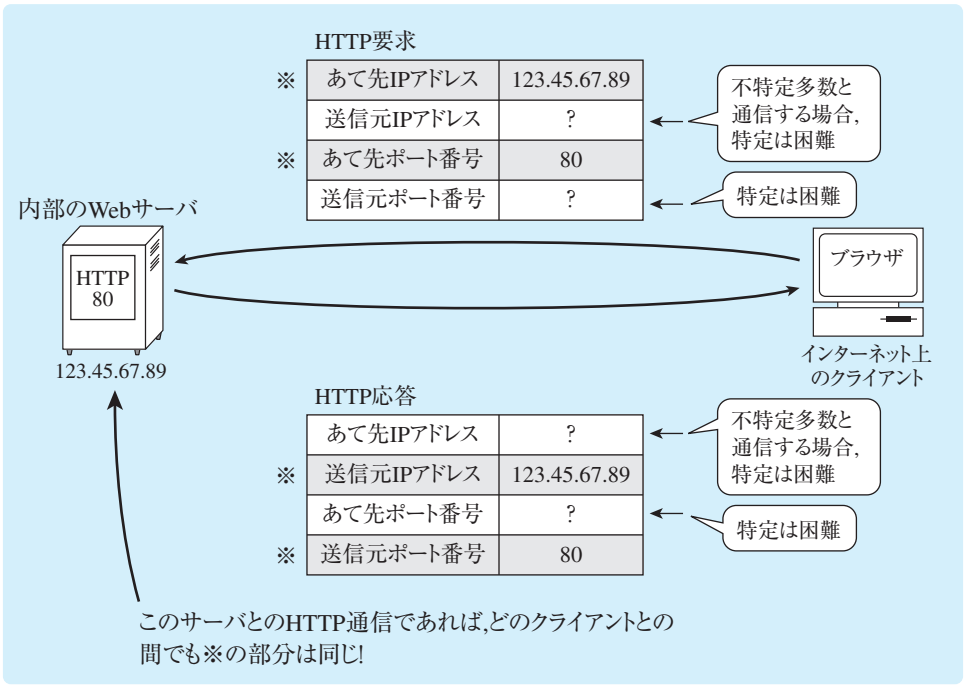
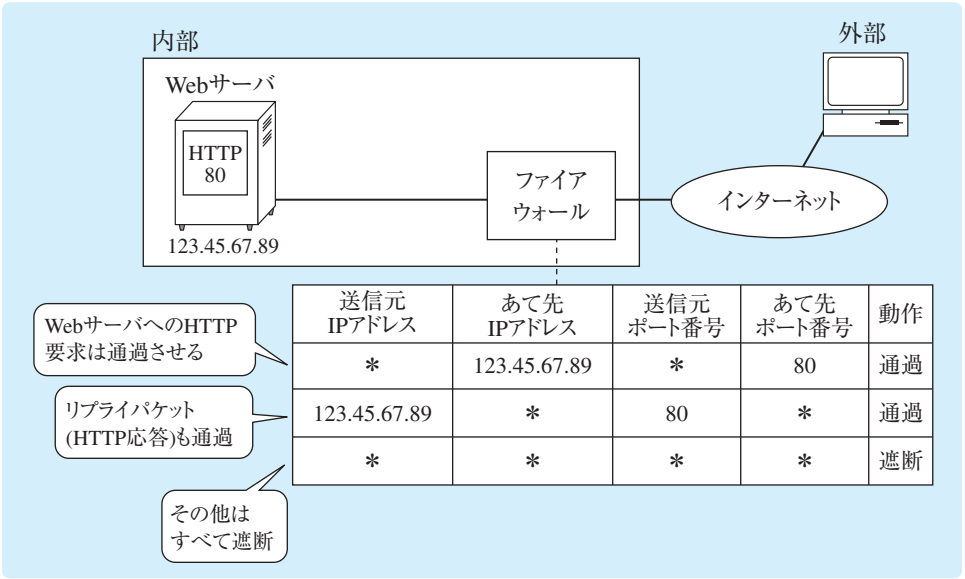


図4.20　HTTP通信におけるヘッダー情報

したがって，フィルタリングテーブルには以下のようなルールを設定すればよい。以下のルールでは，フィルタリングテーブルは上の行から順に検査し，条件に合致する行が見つかった時点で対応する動作を行う。‘*’は制限を行わないことを表す。



送信元 IPアドレス	あて先 IPアドレス	送信元 ポート番号	あて先 ポート番号	動作
*	123.45.67.89	*	80	通過
123.45.67.89	*	80	*	通過
*	*	*	*	遮断

図4.21　フィルタリングテーブルの設定例

このように，パケットフィルタリングによってアクセス制御を行う場合，リプライ(応答)パケットについても設定が必要となる。なお，クライアント側のポート番号として「1024以上(ウェルノウンではないポート番号)」を指定する場合もある。

> **参考：関門ルータ**
> パケットフィルタリング機能はルータがもつ基本的な機能であり，パケットフィルタリング型のファイアウォールのことを関門ルータ(スクリーニングルータ)という場合もある。

●パケットフィルタリングの欠点

パケットフィルタリングは，パケットのヘッダー情報のみを検査し，パケットの内容については検査しない。このため，

・IPアドレスやポート番号を偽造したパケット
・悪意のデータ(脆弱性への攻撃やウイルス)を含むパケット

は，通過させてしまう可能性がある。

たとえば，「自社内のPCからインターネット上のWebサーバへのHTTP通信のみを許可する」場合を考えると，フィルタリングテーブルは次のようになる。

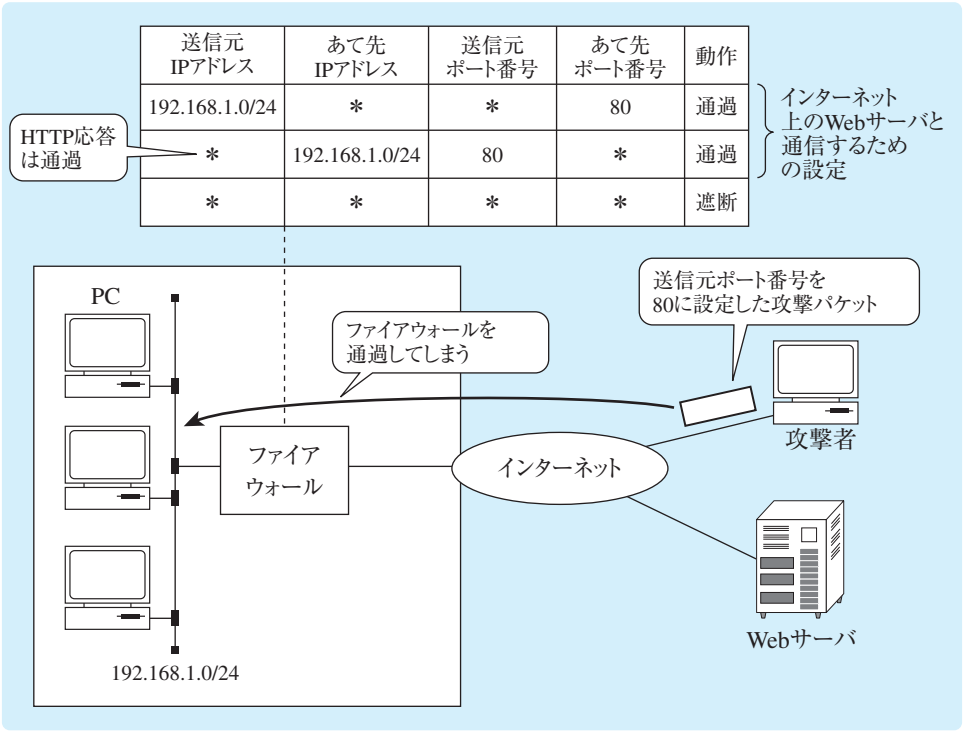


図4.22　攻撃パケットの通過

この例では，送信元ポート番号が80(HTTP応答)の内部向けのパケットは通過させる設定になっている。したがって，送信元ポート番号を80に設定した攻撃パケットは，ファイアウォールがHTTP応答と判断して通過させてしまう。

【ポイント】

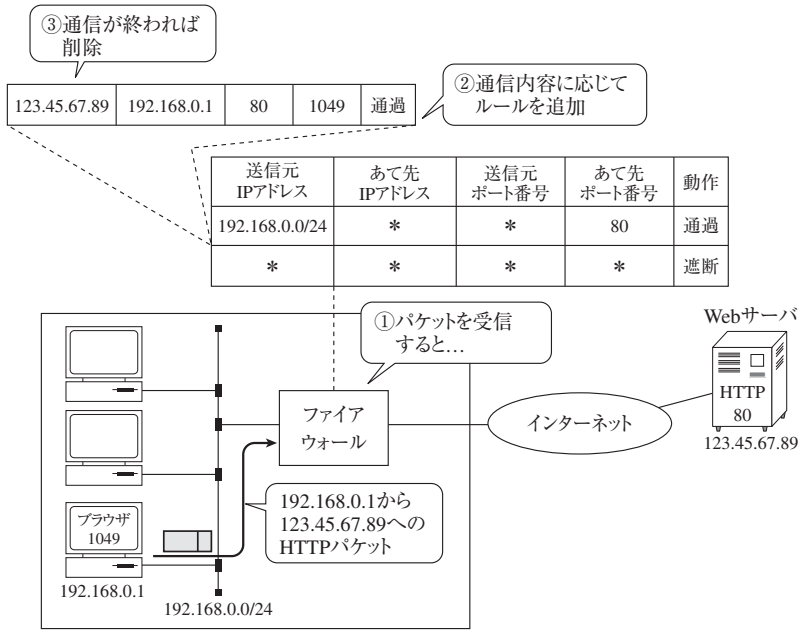
パケットフィルタリング

　パケットのヘッダー情報に基づいてパケットの通過／遮断を判断

　パケットの内容(データ)に基づく制御は不可能

参考：動的パケットフィルタリング

動的パケットフィルタリング(ダイナミックパケットフィルタリング)は，要求パケットに対するルールのみを定義しておき，要求パケットが到着すると，それを通過させるとともに「応答パケットを通過させるルールを動的に追加する」方式である。これにより，応答パケットを偽造した攻撃パケットはファイアウォールの通過が困難になる。



この考え方を応用してTCPセッション(あるいはUDP擬似セッション)の状態を記憶し，セッション状態と矛盾するようなパケットを破棄するといった，より高度な制御を行う方式を，ステートフルパケットインスペクション(SPI)という。

●アプリケーションゲートウェイ

アプリケーションゲートウェイ(ALG：Application Level Gateway)は，プロキシサーバの機能を利用する方式のファイアウォールである。クライアントからの通信要求を受けると，それが許可された通信であれば，通信を代替することによってアクセス制御を行う。

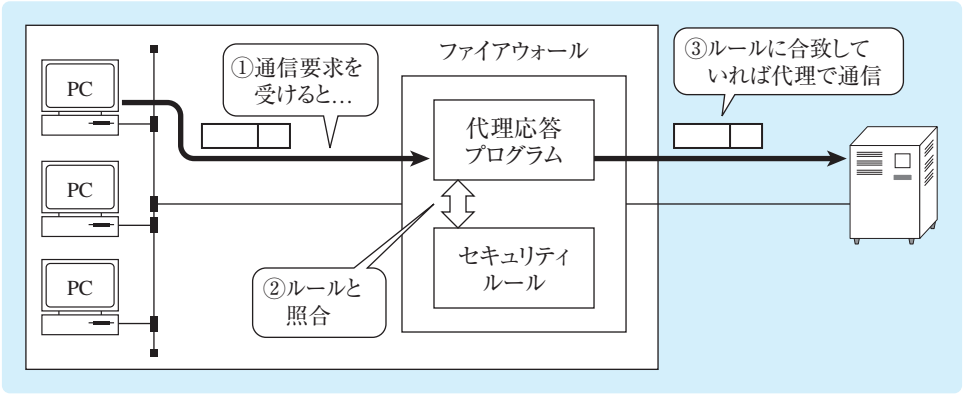


図4.23　アプリケーションゲートウェイ

アプリケーションゲートウェイは，アプリケーション層の情報を参照・解析してアクセス制御を行うことができる。このため，HTTPのパケットに含まれるURLを検査して特定のURLへの接続を禁止する，特定のコマンド(操作)を禁止する，といったパケットフィルタリングでは不可能な制御が可能である。

●ファイアウォールとサーバの配置

ファイアウォールとネットワークの接続構成は様々であり，サーバを設置する領域として，内部セグメント，外部セグメント，DMZ(DeMilitarized Zone：非武装地帯)などがある。現在では，DMZにサーバを配置することが多い。

表4.15　サーバを設置する領域

設置する領域	特徴
外部セグメント	ファイアウォールと外部接続用ルータの間にあるネットワーク。バリアセグメントともいう。サーバが乗っ取られても内部への攻撃はファイアウォールで防げるが，サーバ自体はファイアウォールで保護できない
内部セグメント	ファイアウォールの内側にある保護されたネットワーク。サーバはファイアウォールで保護できるが，サーバが乗っ取られるとすべてのネットワークに被害が及ぶ可能性がある。このため，内部でのみ利用されるサーバ(非公開サーバ)などを配置する
DMZ	外部からも内部からもファイアウォールを介してアクセス可能なネットワーク。サーバをファイアウォールで保護でき，サーバが乗っ取られても内部への攻撃はファイアウォールで防げる

DMZに公開サーバを配置した例を次に示す。ここで，“○”は通信の許可(ただし許可されたものに限定)を表し，“×”は通信の拒否を表す。これらは絶対的なものでなく，システムの構成，サーバの配置，要件，セキュリティポリシーなどによって異なる。

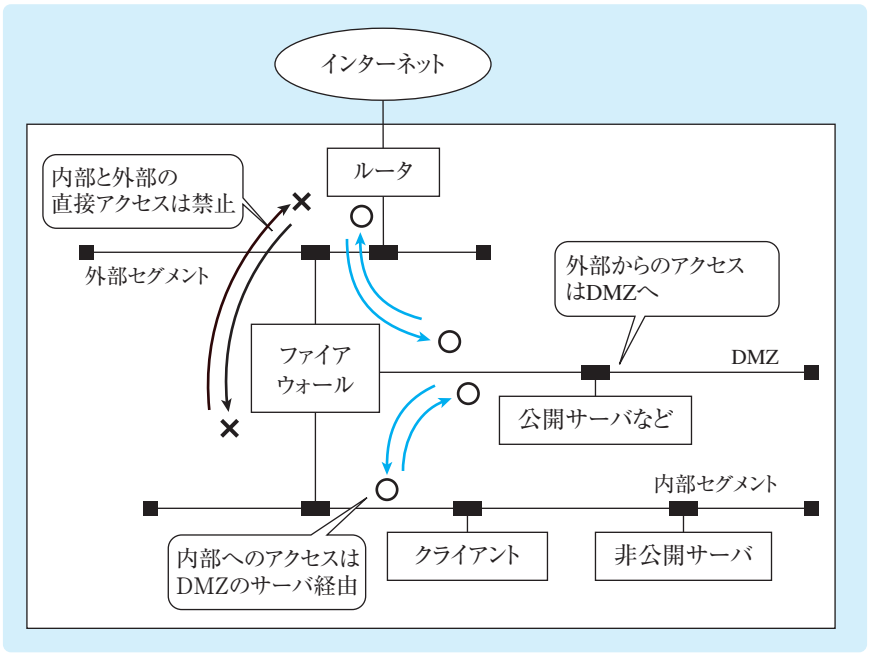


図4.24　DMZを用いたアクセス制御の例

●IDS(侵入検知システム)

ファイアウォールでは，すべての不正なアクセスを遮断できるとは限らない。そこで，IDS(Intrusion Detection System；侵入検知システム)が用いられることもある。IDSは，システムを監視し，不審なアクセスを検出した場合は管理者に警告を発する仕組みである。IDSは，その監視対象によりNIDS(ネットワーク型IDS)とHIDS(ホスト型IDS)に大別される。

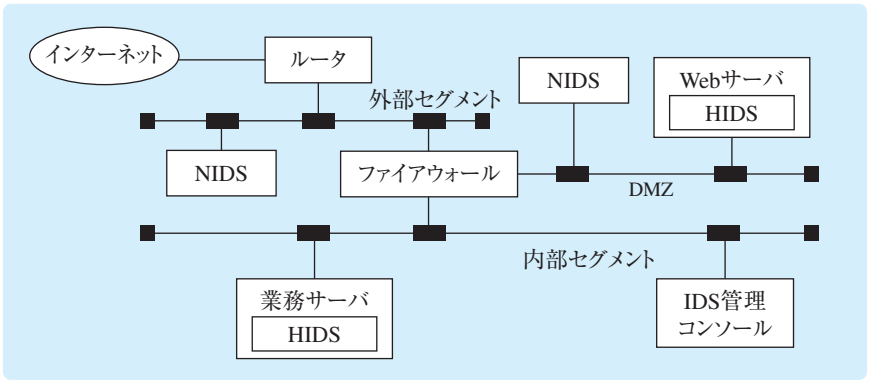


図4.25　IDSの配置

(a)　NIDS

NIDSはネットワーク中(回線上)を流れるパケットを監視し，不正アクセスが検出された場合は管理者に警告する。NIDSは，監視対象によって設置場所が異なる。

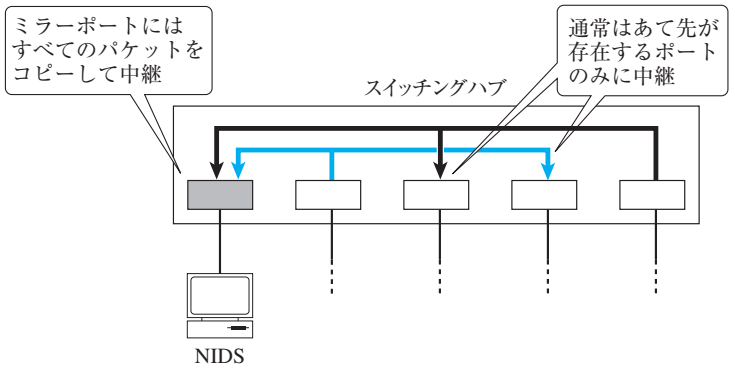
表4.16　IDSの設置場所と監視対象の例

IDSの設置場所	監視対象
ファイアウォールの外側	ファイアウォールがブロックする攻撃を含んだすべての攻撃
ファイアウォールの内側	内部の利用者が行う攻撃
DMZ	ファイアウォールを通過した，公開サーバをターゲットとした攻撃

NIDSは，パケットをリアルタイムで受信・解析・記録するために高い性能が要求される。このため，どのような攻撃を対象とするのかの絞り込みや，配置場所の検討が重要になる。

参考：ポートミラーリング

NIDSは，ネットワーク中を流れるパケットをすべて監視できる場所に設置する必要があるが，スイッチングハブはあて先ノードが存在するポートにしかパケットを転送しない。そこで，NIDSやネットワークアナライザ(LANのパケットを解析する装置)を利用する場合は，ポートミラーリング機能を利用することが多い。ポートミラーリング機能は，監視対象のポートを流れるパケットを特定のポート(ミラーポート)にも転送する機能である。



(b)　HIDS

HIDSは，監視対象のホストにインストールされ，監視対象のホストが受信したパケットや監視対象のホストに対する操作などを監視し，不正アクセスが検出された場合は管理者に警告する。ログの内容，ファイルの変更，システムコールなどに基づいた制御や暗号化通信への対応も可能であるが，監視対象のホスト以外への攻撃は検出できない。また，監視対象となるホストの負荷が高くなる可能性もある。

(c)　IDSの課題

NIDSとHIDSは，監視対象や監視方法が異なるため，用途に適したIDSを導入し，必要に応じて両者を組み合わせる必要がある。また，攻撃と正常なアクセスを100%区別することは難しく，正常なアクセスを不正アクセスとみなすフォールスポジティブ（偽陽性）や，不正アクセスを正常なアクセスとみなすフォールスネガティブ（偽陰性）といった誤検知が発生し得る。

参考：IPSとハニーポット

IDSは，原則として不正なアクセスを検出し，通知するだけである。これに対して，不正なアクセスを遮断するシステムをIPS(Intrusion Prevention System：侵入防止システム)という。

また，不正アクセス手法の分析や保護対象のサーバから目を逸らさせることを目的とし，一見すると脆弱に見える(実際は強固に構築された)“おとり”のサーバを用意することがある。このような手法またはおとりのサーバを，ハニーポットという。

参考：ペネトレーションテスト

構築したファイアウォールやIDSといったセキュリティシステムについて，弱点の発見や，実際に機能するかの確認を目的とした擬似侵入テストをペネトレーションテストという。

参考：UTM（Unified Threat Management）

UTM（統合脅威管理）とは，ファイアウォールの機能に加え，後述のVPN装置やアンチウイルス，IDS/IPS，コンテンツフィルタといった総合的なセキュリティ機能を有する装置である。UTMに搭載される機能は製品によって異なるが，少なくともファイアウォール機能を有し，インターネットとの接続境界に設置される製品がほとんどである。

学習テーマ　4－9

マルウェア対策

マルウェアは，悪意をもって作成された不正なプログラムを指す。以前はコンピュータウイルスともよばれていた。マルウェアの種類には，次のようなものがある。

表4.17　マルウェアの種類と特徴

種類	特徴
マクロウイルス	ワープロや表計算といったアプリケーションのマクロ機能を利用し，データファイルに感染する不正プログラム
ワーム	単体での動作が可能であり，システム上で自身を複製して自己増殖する機能を持つ不正プログラム
トロイの木馬	単体での動作が可能であり，有用なプログラム(ユーティリティやゲームなど)を装って実行されるのを待つ不正プログラム
スパイウェア	ユーザーの行動履歴や個人情報を収集するプログラム。有用なプログラムの一機能として含まれる場合もある。
ボット	感染したコンピュータを乗っ取り，C&Cサーバ(攻撃指示用のコンピュータ)の指示に従って遠隔操作する不正プログラム。主にスパムメールの送信やDDoS攻撃の踏み台として利用される。ボットに感染したコンピュータで構成したネットワークをボットネットという。
ランサムウェア	システムのハードディスクドライブを暗号化するなど，システムの使用を不可能あるいは制限し，利用者に身代金を支払うよう促すメッセージを表示する不正プログラム
ダウンローダ	別の不正プログラムなどをダウンロードすることによって自身の変化や機能拡張などを行う不正プログラム
RAT(Remote Access Trojan)	攻撃者からの指示に従って感染したコンピュータを不正に操作するプログラム。RATは主に標的型攻撃に用いられ，より高度な情報の窃取などを行う点がボットと異なる

マルウェアは，攻撃者が金銭を得るために利用されることも多い。MITB攻撃（Man In The Browser攻撃）は，マルウェアを用いた中間者攻撃の一つであり，金融機関との通信を検出するとWebブラウザの通信を乗っ取ってデータの盗聴や改ざんを行う。MITB攻撃に対しては，利用者がWebブラウザで入力した情報とサーバが受信した情報に差がないことを検証するトランザクション署名などが有効になる。また，感染したコンピュータの計算資源（CPUなど）を不正に使用して暗号資産を得るための計算（マイニング）を行う手法を，クリプトジャッキングという。マルウェアへの感染だけでなく，不正なJavaScriptを組み込んだWebサイトを訪問することでクリプトジャッキングが行われることもある。

●マルウェア対策の基礎

マルウェアは，有用なプログラムや安全なデータを装う，OSやアプリケーションの脆弱性を利用してWebサイトの閲覧や電子メールのプレビューによって自動実行する，LANやUSBメモリを経由して自己増殖(感染)するといった手段で感染する。このため，怪しいWebサイトを閲覧しない，電子メールに添付されたファイルなどの出所が不明なファイルを不用意に開かない，安易にプログラムをダウンロードしないといった基本的な行動に加え，

・OSやアプリケーションの脆弱性を解消するための修正プログラム(セキュリティパッチ)を適用してOSやアプリケーションを最新の状態に保つ

・マルウェア対策ソフト(ウイルス対策ソフト)を利用する

といった対策が重要になる。ソフトウェアを入手する際は，プログラムコードに開発元のデジタル署名を付与するコードサイニングによって，開発元が作成し，改ざんされていないことを確認するという方法もある。

●マルウェア対策ソフト(ウイルス対策ソフト)

マルウェア対策ソフトは，次のような検出手法でマルウェアを検出する。

表4.18　マルウェアの検出手法

コンペア法	安全に保管されている原本と検査対象を比較する。
チェックサム法	情報に符号(チェックサム)を用いる。
パターンマッチング法	特徴的なマルウェアのコードが登録された定義ファイルを用いて検出する。
ビヘイビア法	マルウェアによって引き起こされる動作パターンを監視して検出する。

代表的な検出手法であるパターンマッチング法では，マルウェアの特徴的な部分を定義したパターンファイル(シグネチャファイル，ウイルス定義ファイル)と検査対象のファイルを比較する。パターンファイルに登録されていないマルウェアは検出できないので，パターンファイルを常に最新に保つことが重要になる。ビヘイビア法のように動的な解析を伴う場合は，実環境とは隔離された仮想的な領域上で動作させ，悪影響の拡散を防ぐ。このような領域をサンドボックスという。いずれの方法であっても，正常なファイルをマルウェアと判断する偽陽性(フォールスポジティブ)や，マルウェアを正常なファイルと判断する偽陰性(フォールスネガティブ)といった誤検知が発生し得る。また，ウイルス(マルウェア)側も，対策ソフトによる検知をすり抜けるように工夫してくる場合もある。以下に例を示す。

ポリモーフィック型：自身の複製時に異なる鍵で暗号化を行い，内容を変化させる

メタモーフィック型：自身の複製時に「同機能を実現する別のコード」に変化する

ファイルレスマルウェア：実行ファイルが補助記憶装置に保存されず，主記憶装置上で攻撃を行う

●企業におけるマルウェア対策

企業内では，マルウェアの感染に加えて組織内部での感染拡大を防ぐことも重要になる。このため，不用意に見知らぬファイルを開かない，USBメモリはマルウェアチェックされた承認されたものだけを使用する，といった基本的な対策を周知・徹底する人的な対策も重要となる。

また，OSやアプリケーションのセキュリティパッチを定期的に適用して最新の状態を保つ，PCなどの機器にマルウェア対策ソフトを導入するといった基本的な対策も重要である。ネットワークの境界付近やメールサーバなどでマルウェアチェックを行うことも効果的であるが，感染経路はネットワーク経由のみとは限らないので，PCなどの末端の機器にマルウェア対策ソフトを導入することは必須といえる。

万が一，コンピュータがマルウェアに感染した場合の対応手順は，すべての要員が理解し，遵守する必要がある。近年はネットワーク経由で感染を拡大するマルウェアも多いので，不審な挙動を発見したら初動としてLANケーブルを抜くなどしてコンピュータをネットワークから切断し，感染拡大を防いだ上でシステム管理者に連絡して指示を仰ぐ。

システム管理者は，影響範囲を局所化した上で，被害状況の分析やマルウェアの除去，システムの回復などを行う。この際，主記憶装置上にある情報(実行しているマルウェアやデータなど)は電源を切ってしまうと失われてしまうので，安易に電源を切るべきではない場面もある。

マルウェアに感染した場合，マルウェアを駆除したとしても破壊されたデータは復旧しない。このため，データを定期的にバックアップしておくことが重要になる。ランサムウェアなどは，アクセス可能な範囲のファイルを暗号化してしまうので，バックアップしたデータが被害を受けないような対策も重要である。具体的には，バックアップしたデータを保管するサーバや機器はネットワーク経由でアクセス可能な状態としないことに加え，バックアップしたデータはWORM(Write Once Read Many)のような書き換えが不可能な記録媒体に記録する，3-2-1ルールに従うなどの方法がある。3-2-1ルールとは，

・データは「オリジナル」「コピー1」「コピー2」の3つ用意する
・2つのコピーはそれぞれ異なる媒体に保存する
・コピーのうちいずれか1つを遠隔地に保存する

とルールに基づいてバックアップ運用を行うものであり，バックアップの理想とされる。

●マルウェアを利用した攻撃手法

(a) ガンブラー(Gumblar)

ガンブラーとは，Webサイトの改ざんとマルウェアを組み合わせ，Webサイトを閲覧した不特定多数のコンピュータをマルウェアに感染させる手法の総称である。ガンブラーでは正規のWebサイトを改ざんして攻撃用サイトに誘導し，OSやアプリケーションソフトの脆弱性を突いて攻撃するようなマルウェア(攻撃コード)をダウンロードさせる。閲覧者のコンピュータに脆弱性が存在すれば，そのコンピュータはマルウェアの侵入を許してしまい，マルウェアに感染する。このようなWebサイトを閲覧しただけでマルウェアに感染するような手法をドライブバイダウンロードという。

このような攻撃に対しては，ウイルス対策ソフトを導入してパターンファイルを最新の状態に保つ，OSやアプリケーションソフトのセキュリティパッチを適用して脆弱性を解消する，といった基本的な対策が重要になる。

(b) 標的型攻撃

機密情報の窃取などを目的として特定の組織（企業や官公庁）を狙った攻撃を標的型攻撃という。標的型攻撃の手法はさまざまであるが，主にソーシャルエンジニアリングの手法を用いた偽装メールとマルウェアを組み合わせた標的型攻撃メールを用いたものが多い。

標的型攻撃メールは，攻撃者は事前に標的となる組織や取引先などの関連組織などに関する情報を調査して作成される偽装メールであり，一般的には次のような特徴が挙げられる。

・実際の組織名や個人名などを送信者名として詐称する。
・件名，本文，添付ファイル名を工夫し，業務連絡などを装う。
・PDFファイルや文書ファイルなどに偽装したマルウェアを開くよう，あるいはマルウェアをダウンロードさせる不正サイトに接続するよう誘導する。

添付されたマルウェアは，不特定多数の利用者に無差別に送付されるものではなく，その組織への攻撃に最適化されているため，ウイルス対策ソフトでのパターンマッチングによる検出が難しい。さらに，バックグラウンドで次のような活動を行う。ファイルの破壊や改ざんといった目立った活動を行わない場合，感染に気づくことも難しくなる。

・バックドアの作成
・外部のC&C(Command & Control)サーバに対するコネクトバック通信
・システムに関する情報（システム構成など）の取得
・取得した情報の外部への送信
・新たなマルウェアのダウンロードや機能拡張
・ネットワーク経由の感染・拡散
・USBメモリ経由での隔離されたクローズ系システムへの侵入

コネクトバック通信とは，感染した端末がC&Cサーバにアクセスし，攻撃者がそれに応答する形で端末に接続するバックドア通信のことである。この通信にはHTTPやHTTPSが用いられることが多く，一見すると通常のWebアクセスと見分けるのが難しいため，ファイアウォールを通過しやすくなる。

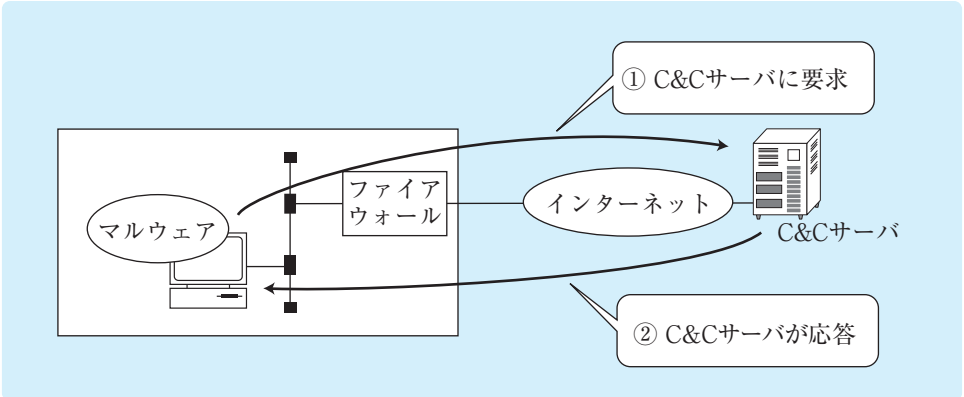


図4.26　コネクトバック通信

標的型攻撃で用いられる手法は特別に新しいものではなく，ソーシャルエンジニアリングやダウンローダ，ドライブバイダウンロード，バックドア，マルウェア，USBワーム，ゼロデイ攻撃など，既存の技術を組み合わせたものである。ただし，標的となる組織に対して長期的に調査や攻撃を行い，攻撃手法を最適化していく点が従来のものとは異なる。このような標的に特化した手段で長期的に行う攻撃をAPT(Advanced Persistent Threat)ともいう。

このほかにも，標的となる組織の従業員が頻繁に閲覧するサイトを改ざんして攻撃コードを埋め込み，アクセス時にマルウェアをダウンロードさせるような手法も用いられる。これを水飲み場型攻撃という。

標的型攻撃を防ぐためには，不審な添付ファイルを開かない，URLを安易にクリックしない，OSやアプリケーションソフトのセキュリティパッチを適用して最新に保つ，重要情報はネットワークから隔離するといった従来どおりの技術的対策や利用者教育などが重要となる。これらを確実に実施したとしてもシステムへの侵入を確実に防止できるとは限らないので，重要情報が組織外部(インターネット)に出て行くことを防止する出口対策も重要となる。

出口対策の一つに，プロキシサーバで認証を行う認証プロキシを利用するというものがある。この際，マルウェアが認証情報を窃取しないよう，PCには認証情報を保存しないといった対策も考慮する。

学習テーマ　4－10

インターネットセキュリティ

(1)　HTTP における認証

●HTTP 基本認証

HTTP はそれ自体が基本認証 (basic 認証) とよばれる認証機能をもつため，Web サイトや特定のディレクトリなどに対して，ユーザー ID とパスワードによるアクセス制限を設定できる。

ただし，この基本認証では，ユーザー ID とパスワードは平文で送信される。このため，盗聴される可能性もあり，アクセス制御が重要なシステムでは SSL/TLS によって通信内容を暗号化することが望ましい。また，多くのブラウザは，基本認証によって入力されたユーザー ID やパスワードを記憶する機能をもつ。このため，複数人で 1 台のパソコンを共有するような場合は，パスワードを記憶させないように設定しておく必要がある。

(2)　SSL/TLS

●SSL/TLS の機能

SSL(Secure Sockets Layer) やその後継規格である TLS(Transport Layer Security) は，TCP/IP モデルにおけるアプリケーション層とトランスポート層の間に位置し，アプリケーションプロトコルに対して次のような機能を提供するセキュリティプロトコルである。

表 4.19　SSL/TLS の機能

サーバ認証， クライアント認証	サーバ (またはクライアント) が提示する証明書を検証し，通信相手を認証する。どちらか一方の認証 (あるいは両方とも認証しない) も可能であり，WWW においては，サーバ認証が行われることが多い
暗号化	アプリケーションプロトコルのデータを暗号化する
メッセージ認証	メッセージ認証符号を用いて，改ざんを検出する

SSL/TLS はトランスポート層に TCP を用いるさまざまなアプリケーションプロトコルの下位層として利用することができる。Web においては，上位層に HTTP を利用する HTTPS(HTTP over TLS) が主に用いられ，ウェルノウンポート番号として 443 が用いられる。

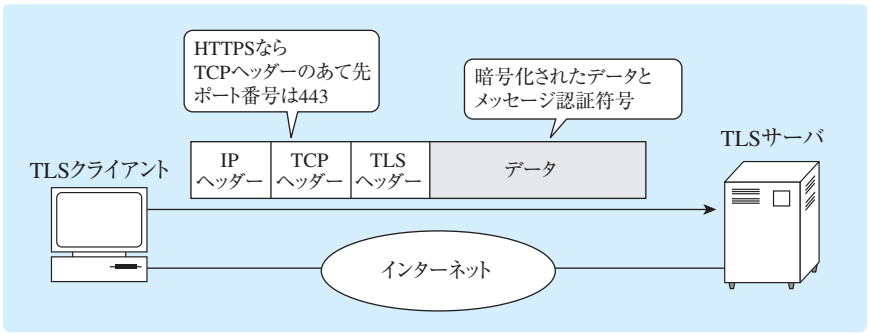


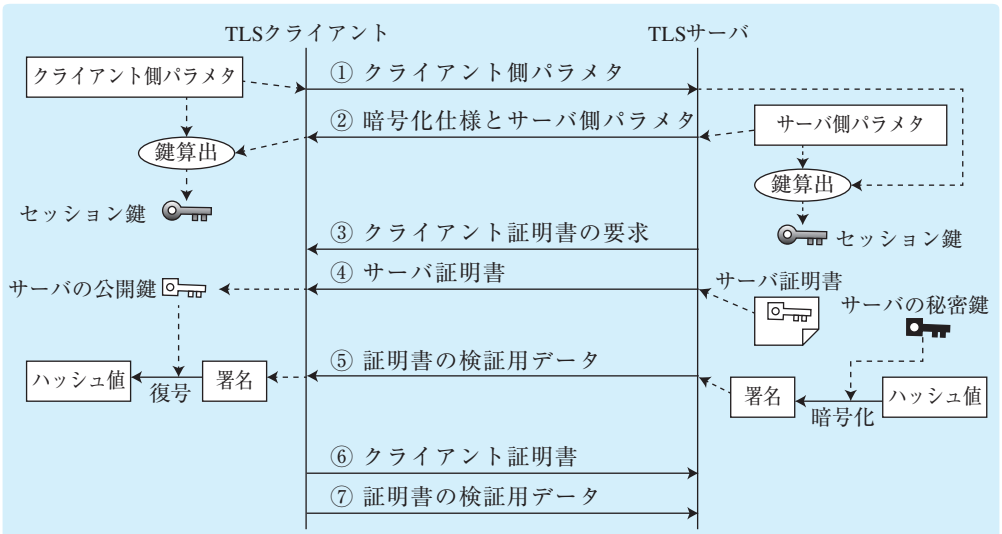
図4.27　TLSを利用した通信

●TLSの通信手順

TLSでは，通信に先立って

・利用するTLSのバージョンや暗号化アルゴリズムなどについての合意
・鍵交換（使用するセッション鍵の合意と生成）
・通信相手の認証（サーバ認証，クライアント認証）

などが行われる。これをハンドシェイクという。ハンドシェイクの詳細な手順は，SSLを含むTLSのバージョンや認証の有無などによって異なる。また，通信内容の暗号化に用いられるセッション鍵は，DH（Diffie–Hellman）鍵交換を応用して生成される。DH鍵交換とは，クライアントとサーバでパラメタとなる乱数を交換し，公開鍵暗号の理論によって第三者に推測不可能な共通鍵を生成する方法である。



注記1：③，⑥，⑦はクライアント認証を行う場合に，サーバ認証と同様の手順で行われる。
注記2：検証用データの基となるハッシュ値は，それまでに送受信されたメッセージから生成される。

図4.28　TLSの通信シーケンス

●SSL/TLSを利用する場合の留意点

SSL/TLSは現状では十分なセキュリティを確保することができるため，通信内容の保護に関しては大きな問題はない。ただし，SSL/TLSを利用する場合は以下の点に注意する必要がある。

・SSL/TLSの利用による処理性能の低下

SSL/TLSを利用すると，証明書の交換やセッション鍵の生成などの処理が発生する。処理件数によってはサーバには大きな負荷がかかるため，SSL/TLSを利用するサーバには高い処理能力が要求される。このため，必要に応じてSSLアクセラレータ(TLSアクセラレータ)とよばれる「SSL/TLSの処理を行う専用装置」を用いて負荷を分散する。

・通信内容に基づく制御

SSL/TLSに限らず，通信を暗号化した場合は通信内容が第三者に傍受される可能性を低減できる反面，その内容を解析することも困難になる。このため，ウイルスを検出するためのウイルスチェックや不正な通信内容を遮断するコンテンツフィルタなどは，正常に機能しなくなる。また，HTTPのメッセージボディやcookieなどにセッションIDなどを格納してセッション維持を行うようなケースでも，暗号化を解除しないと制御ができなくなってしまう。

(3)　電子メールの暗号化と署名

送信元からあて先まで電子メールの内容を暗号化する場合，「電子メールを送信する前にメッセージを暗号化する」ことが基本となる。このために，S/MIMEやPGPなどが用いられる。

S/MIME(Secure MIME)は，PKIとMIMEの仕組みを利用して電子メールに暗号化とデジタル署名の機能を提供するプロトコルであり，ハイブリッド暗号方式でメールメッセージの暗号化を行う。暗号化されたメールメッセージや署名，暗号化された公開鍵などは，MIMEの機能を用いて添付ファイルの形で送受信される。このため，S/MIMEに対応していないメールソフトでは，署名のみを行ったメールであればメッセージを読むことは可能だが，署名を検証することはできない。

なお，S/MIMEで暗号化を行う場合，送信者の公開鍵で暗号化された共通鍵と，受信者の公開鍵で暗号化された共通鍵の両方が格納される。これは送信者と受信者の双方がメールを復号できるようにするためである。

> 参考：PGP
>
> PGP（Pretty Good Privacy）は，S/MIMEと同様にハイブリッド暗号方式を用いてメールメッセージの暗号化やデジタル署名などを実現する仕組みである。PGPは，認証局のような公開鍵の所有者を保証する仕組みをもたない。公開鍵に対して所有者を保証するための署名を，各ユーザーが相互に付加することによって公開鍵を信頼する。このような仕組みを，信頼の輪という。

(4)　メールサーバにおけるセキュリティ

●電子メールの不正中継対策

メールの送信に用いられるSMTPは，元々は認証機能をもっていなかった。このため，詐欺や広告の送信などを目的に不特定多数の宛先に無差別にメールを送信するスパムメール(迷惑

メール)が問題となっている。スパムメールの送信には，他者が所有するメールサーバを踏み台に用いることが多い。仮に自社のメールサーバが踏み台に利用されると，メールサーバのリソースが不正に利用されるだけでなく，スパムメールの送信元と見なされて社会的信用を失う恐れもある。スパムメールの踏み台として利用されないための対策として，リレー制限やSMTP-AUTHの利用などが挙げられる。

(a)　リレー制限

自社のメールサーバが「外部(社外)からのメールをさらに外部へ中継する」ことを許可した状態(オープンリレーと呼ばれる)になっていると，スパムメールを送信する踏み台として自社のメールサーバが利用されるリスクが高まる。このような電子メールの不正中継(第三者中継ともいう)を防ぐためには，メールサーバに電子メールの中継を制限するリレー制限を設定する方法が効果的である。具体的には，内部(社内LANなど)から発信された電子メールは外部(社外など)へ転送するが，外部から発信された電子メールは外部に転送しないように設定を行うことにより，電子メールの不正中継を防ぐことが可能となる。

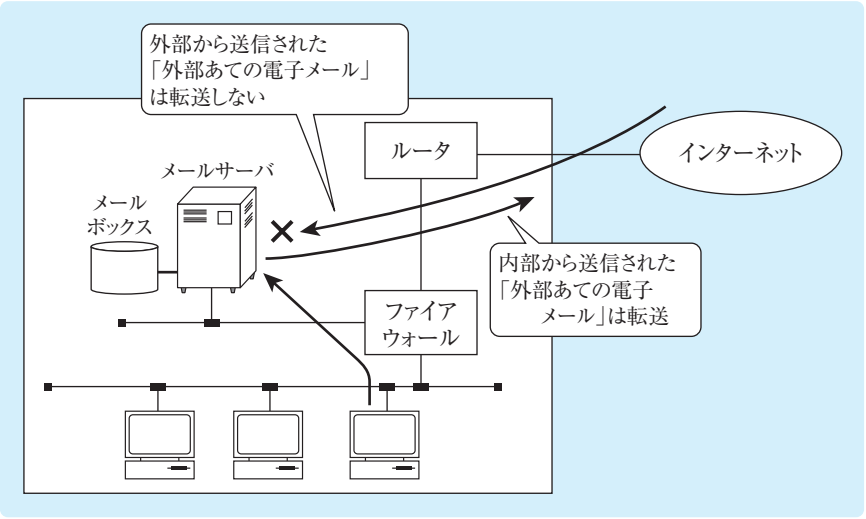


図4.29　電子メールのリレー制限

また，メールサーバを分離することによって不正中継対策のルールを単純化し，メールボックスへの攻撃を防ぐ効果が期待できる。たとえば，外部用メールサーバと内部用メールサーバを用意して，次のように設定することが考えられる。

・外部用メールサーバは外部から送られた内部向けの電子メールを内部用メールサーバに転送し，内部用メールサーバから転送された電子メールのみを外部に転送する
・内部用メールサーバは，(クライアントマシンの)各メールソフトから送られてきた外部向け電子メールのみを外部用メールサーバに転送し，外部用メールサーバから転送された電子メールと内部でやりとりされる電子メールをメールボックスに蓄積する

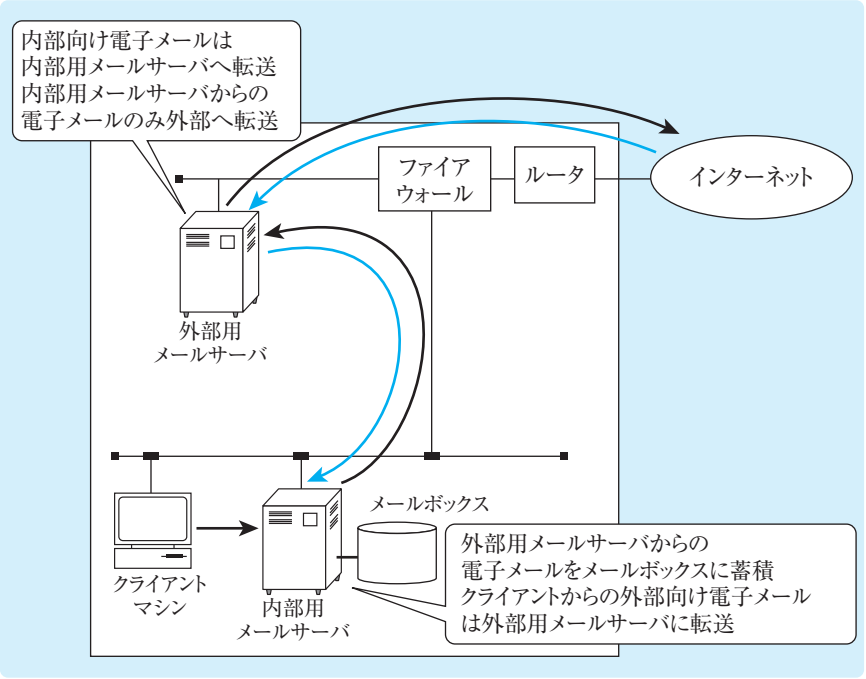


図4.30　メールサーバの分割

このほかにも，「送信用のメールサーバと受信用のメールサーバを別にする」，「メールマガジン配送用など，大きな負荷がかかるメールサーバは別に用意する」など，メールサーバの負荷分散やセキュリティリスクの分散などを目的に，メールサーバの分割を行うこともある。

(b)　SMTP-AUTH

SMTP-AUTH(SMTP AUTHentication)は，SMTPそのものに認証機能を追加したSMTPの拡張仕様である。ユーザーは認証に成功した場合のみ，電子メールを送信できる。SMTP-AUTHでは，25番(SMTP)ではなく，サブミッションポートとよばれる587番のポート番号を用いる。

現在では，悪意ある顧客やボットに感染したPCなどが自社のドメインからスパムメールを送信するのを防ぐため，自社のメールサーバを経由せずにインターネットに出ていくSMTP通信(ポート番号は25)を遮断するISPが多い。これをOP25B(Outbound Port25 Blocking)という。OP25Bではサブミッションポートによるメール送信はブロックしないので，正当なメールアカウントをもつ利用者は問題なく他のISPのメールサーバを利用することができる。

(c)　送信ドメイン認証

電子メール送信者のアドレスがなりすまされておらず，信頼できるネットワーク領域(ドメイン)から送信されていることを証明することを，送信ドメイン認証という。送信ドメイン認証を実現する技術には，送信元ドメインのDNSサーバにメールサーバのIPアドレスを登録・公開しておき，受信側がそれを参照・確認するSPF(Sender Policy Framework)や，メールサーバがメールに署名するDKIM(DomainKeys Identified Mail)などがある。

SPFでは，メールの送信元となる組織が，自ドメインからメールを送信するサーバのIPアドレスをDNSサーバのTXTレコードに登録しておく。このレコードをSPFレコードという。

受信側のメールサーバは，メールを受信すると送信元ドメインのDNSサーバにSPFレコードを問い合わせ，メールの送信元となるIPアドレスがSPFレコードに含まれているかを確認する。SPFレコードに含まれている場合は，メールは正規のメールサーバから送信されたと判断する。含まれていない場合は，メールサーバがなりすまされていると判断する。

DKIM(DomainKeys Identified Mail)では，送信元の組織がDNSサーバに公開鍵を登録しておき，送信側メールサーバが電子メールのヘッダーにデジタル署名を付加する。受信側メールサーバは，デジタル署名を公開鍵で検証し，メールサーバがなりすましでないかを確認する。

(5)　Webサイトのセキュリティ対策

●Webサイト改ざん対策

Webサイトの運営においては，Webページの改ざんというリスクがつきまとう。Webサイトを改ざんするための手法は様々であるが，ここではサーバに保存されたWebページを改ざんする手法について解説する。

Webページを改ざんするためには，Webサーバに侵入して管理者権限などのWebページを書き換える権限を得る。このための代表的な手法として，次の二つが挙げられる。

・パスワードクラックや推測，盗聴などによってWebサーバに直接侵入する

・OSやWebサーバソフトの脆弱性を攻撃し，管理者権限を奪取する

このため，強固なパスワードを設定して定期的に変更する，ベンダーから公表される脆弱性情報を収集してセキュリティパッチを適用する，あるいは推奨された対応策を適用するなどの対策が必要になる。

●フィッシング対策

電子メールなどを用い，正規のWebサイトを装った偽のWebサイト（フィッシングサイト）に誘導してクレジットカード番号を窃取するといった詐欺行為をフィッシングという。フィッシングサイトは，巧妙に正規のWebサイトを装っているが，ドメイン名が異なっていたり，ドメイン名ではなくIPアドレスを用いていたりする。このため，URLに注意すれば被害にあうことは少なく，利用者側の対策が重要となる。

また，正規のドメイン名を用いて偽のWebサイトに誘導する手口もある。これをファーミングという場合もあり，実現する手法には次のようなものが挙げられる。

(a)　hostsファイルの書き換え

hostsファイルとは，ホスト名(ドメイン名)とIPアドレスの対応を記述したテキスト形式のファイルであり，DNSと同様にドメイン名に対応するIPアドレスを得るために用いられる。マルウェアの中には，正規のドメイン名へのアクセスを不正なサーバに誘導するために，hostsファイルを書き換えるものもある。また，特定のドメイン名への接続を防止するためにhostsファイルを悪用する場合もある。たとえば，ウイルス定義ファイルの提供元となるFQDNを，PC自身を表すIPアドレス（ループバックアドレス）である127.0.0.1に対応付けると，その機器は提供元のサイトにアクセスすることができず，ウイルス定義ファイルをダウンロードできなくなる。

(b)　DNSサーバへの不正侵入

DNSサーバに不正侵入されてゾーン情報のAレコードが書き換えられた場合も，正規のドメイン名へのアクセスが不正なサーバに誘導されてしまう。このような不正侵入を防ぐためには，Webサーバと同様にDNSサーバのセキュリティを確保するために適切なパスワード管理や脆弱性の解消などが重要となる。

(c)　DNSキャッシュポイズニング

クライアントからのDNS問い合わせを受け付けて，ゾーン情報を保持するDNSサーバ（コンテンツサーバ）に問合せを行うDNSサーバをキャッシュサーバという。DNSキャッシュポイズニングは，キャッシュサーバがもつキャッシュに偽りの情報を埋め込む攻撃である。具体的な手法としては，キャッシュサーバに問合せを依頼するとともに偽の回答を送りつけるなどがある。キャッシュサーバは，問合せを受けたドメイン名がキャッシュにあればコンテンツサーバへの問合せを行わないので，正規のドメイン名に対して不正なサーバのIPアドレスを回答してしまう。

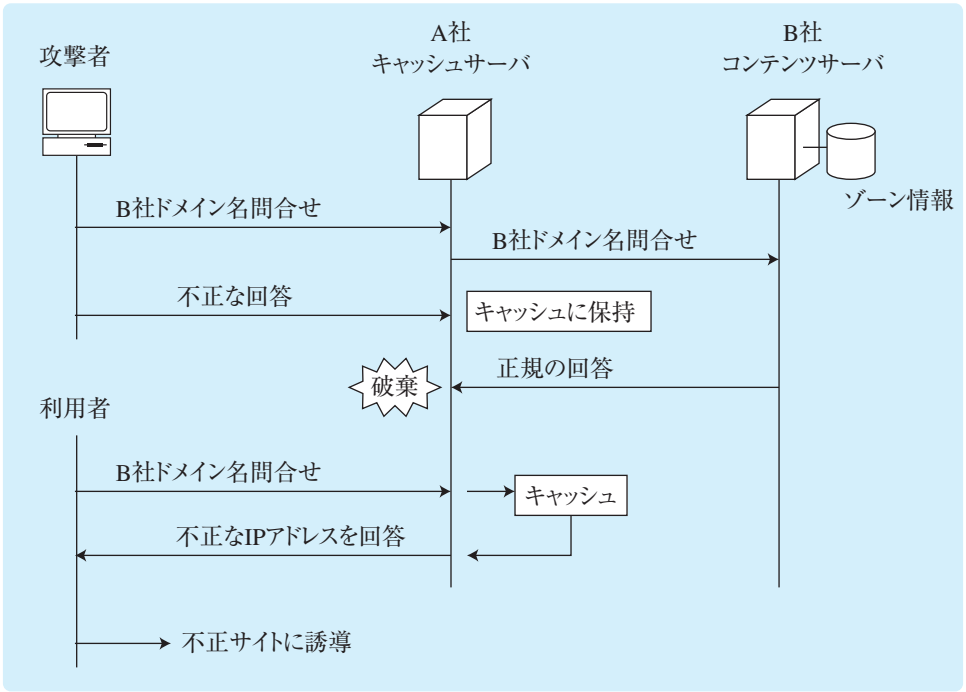


図4.31　DNSキャッシュポイズニング

外部（インターネット）からのDNS再帰問合せに応答するようなキャッシュサーバをオープンリゾルバという。オープンリゾルバは，DNSキャッシュポイズニングだけでなく，様々な攻撃にも利用されるため，自社のキャッシュサーバが外部（インターネット）からのDNS再帰問合せに応答しないよう設定する必要がある。また，キャッシュサーバが偽の回答を入手しないための技術としては，デジタル署名の仕組みを用いることによって正当なDNSサーバからの応答かをクライアント側が検証できるようにしたDNSSEC(DNS Security Extensions)などがある。

●DoS攻撃(Denial Of Service)

DoS攻撃とは，提供するサービスの妨害や停止を目的とした攻撃であり，大量のアクセスなどを発生させて過負荷をかける手法が代表的である。DoS攻撃のうち，ボットに感染したパソコンなど，多数の踏み台を利用して一斉にDoS攻撃を仕掛ける攻撃を，DDoS攻撃（Distributed DoS攻撃)ともいう。DoS攻撃及びDDoS攻撃は単なるアクセス集中と区別がつきにくく，ファイアウォールのパケットフィルタリングの設定だけで防御することは難しい。また，サーバのリソースを浪費させるDDoS攻撃とネットワーク帯域を浪費させるDDoS攻撃を組み合わせるなど，複数のDDoSを組み合わせる手法をマルチベクトル型DDoS攻撃という。DoS攻撃及びDDoS攻撃には，次のような手法がある。

表4.20　DDoS攻撃の手法

名称	内容
smurf攻撃	送信元を攻撃対象とし，宛先をブロードキャストとしたICMPエコー要求を送信する攻撃。攻撃対象には大量のICMPの応答パケットが送られる。
ICMP Flood攻撃	大量のICMPエコー要求を送信する攻撃。攻撃対象までの回線を過負荷状態にさせる。
SYN Flood攻撃	攻撃対象のサーバに対してTCPコネクションの確立を要求するSYNパケットを大量に送信する攻撃。
DNS水責め攻撃 ランダムサブドメイン攻撃	実在しない攻撃対象ドメインのサブドメイン名をランダムかつ大量に生成し，その問合せをオープンリゾルバに送信する攻撃。攻撃対象の権威サーバにはサブドメイン名に対する問合せが集中する。実在しないランダムなサブドメイン名を生成するため，DNS応答がキャッシュされない。
DNSリフレクタ攻撃 DNSリフレクション攻撃 DNS amp攻撃	送信元を攻撃対象に偽装したDNSの問合せを，大量にオープンリゾルバに送信する攻撃。攻撃対象には大量のDNS応答が集中する。DNSの応答は攻撃対象に送信されることから，オープンリゾルバが攻撃を反射しているように見える。また，DNSの応答は問合せよりもサイズが大きいので攻撃パケットのサイズを増幅させることができる。
NTPリフレクタ攻撃 NTPリフレクション攻撃	送信元を攻撃対象に偽装したNTPの問合せを，インターネット上の公開NTPサーバに送る攻撃。攻撃対象には大量のNTP応答が集中する。直前にNTP通信したホストの一覧を得るコマンド（monlistコマンド）を使用することにより，応答パケットのサイズを増幅させることができる。

DNSを用いたDDoS攻撃では，踏み台としてオープンリゾルバが利用される。自社のDNSサーバが踏み台として利用されないためにも，自社のDNSサーバはオープンリゾルバとしない設定とすべきである。この他にも，従量課金制のクラウドサービスを利用する企業に対して経済的な損失を与えるために，リソースを大量消費させるEDoS攻撃（Economic Dos攻撃）などもある。

> **参考：IPスプーフィング**
>
> 送信元のIPアドレスを偽装する手法をIPスプーフィングという。IPアドレスによる接続制限を回避する場合やDoS攻撃の攻撃元を隠蔽するなどの目的に用いられる。

(6)　その他のインターネットセキュリティ

●ダークネット

インターネット上で到達可能であるが使われていないIPアドレス空間を，ダークネットという。ダークネットはサイバー攻撃に用いられることも多く，国立研究開発法人 情報通信研究機構（NICT）では，サイバー攻撃の観測・分析システムであるNICTERによってダークネットを観測し，サイバー攻撃の動向やマルウェアの活動動向などを把握・分析している。

●ダークウェブ

インターネット上に存在するが，特定のソフトウェアや設定を使用しないとアクセスできないWebサイトやコンテンツをダークウェブといい，サイバー犯罪者の情報交換の場になっていることもある。ダークウェブを実現する仕組みの一つであるTorは，TCP/IPネットワークにおいて通信経路を匿名化する。Torブラウザなどのソフトウェアを使用することにより，Torによって構築されたネットワークにアクセスしたり，Torを経由して匿名性を保ったままインターネットにアクセスしたりすることが可能となる。