

第3章

ネットワークインフラストラクチャ

▼ 学習のポイント

この章では、ネットワーク基盤に焦点を当てます。ケーブリング、ネットワーク機器、プロトコルのぜい弱性と脅威、ネットワークセキュリティを強化（ハードニング）するツールやセキュリティ対策について説明します。

3》1 ネットワークモデル

3》2 ネットワークの設計要素と構成

3》3 ワイヤレスネットワークの脅威・セキュリティ対策

3》4 TCP/IP への脅威・ぜい弱性とセキュリティ対策

3》5 ポートとプロトコルへの脅威と、セキュリティ対策

3》6 ネットワークセキュリティ強化用のネットワークセキュリティツール

3

1

ネットワークモデル

3-1-1 OSI 参照モデルと DoD モデル

ここでは、ネットワークモデルの中から OSI 参照モデルと DoD モデルを説明します。

■ OSI 参照モデル

OSI (Open Systems Interconnection/開放型システム間相互接続) 参照モデルは、ISO が OSI プロトコルの開発に使用した参照モデルで、ISO/IEC 7498-1 に定義されています。

OSI プロトコルは、各メーカー（ベンダ）の独自ネットワークプロトコルを相互接続するために開発されたプロトコルです。

OSI 参照モデルは、OSI プロトコルの機能を階層構造で示すモデルで、通信機能を 7 階層（レイヤ/Layer、L1 ~ L7 のように表記）に分け、各層ごとに標準的な機能を定義しています。

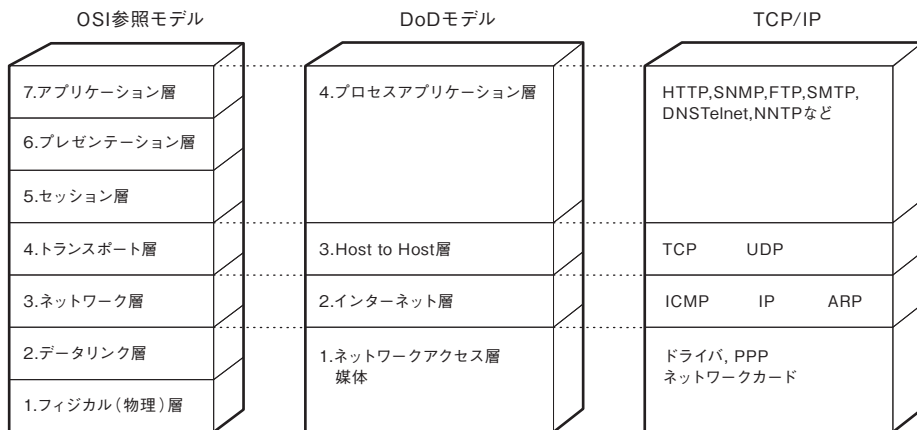


図 3-1 ネットワークモデルと TCP/IP の対応

■ DoD モデル

DoD モデルは、DoD（アメリカ国防総省：The Department of Defense）の 4 層モデルは、OSI 参照モデルの開発以前の 1974 年に定義され、インターネット（The Internet）プロトコル群、TCP/IP の開発に使用されています。DoD モデルは、日本では TCP/IP モデ

ルと呼ばれていることが多いようです。Host to Host層はトランスポート層と呼ばれる場合もあります。また OSI 参照モデルと DoD モデルを合成した5階層のモデルを TCP/IP モデルとしているケースもあります。

図 3-1 は、OSI 参照モデルと DoD モデル、TCP/IP プロトコル群の対応関係を示しています。ネットワーク媒体は、階層の中には含まれず、その下にあります。(これは ISO/IEC 7498-1 の定義によるものです。)

TCP/IP を中心とした解説では、DoD モデルが、下位層を中心とした解説では OSI 参照モデルが利用されることが多いようです。

3》1-2 ネットワークモデルと PDU 名の関係

■ プロトコルデータユニット (PDU)

ネットワークモデルの各層でやり取りされる「プロトコル (制御情報) とデータ」の組み合わせは、プロトコルデータユニット (PDU/Protocol Data Unit) と呼ばれます。PDU には名前 (PDU 名) が付けられています。ネットワークモデルごと、ネットワーク階層ごとに PDU 名は異なりますが、おおまかに全てを「パケット」と呼ぶこともあります。

■ OSI 参照モデルの PDU 名

OSI 参照モデルの PDU 名は、データリンク層 (2 層) では「フレーム」、ネットワーク層 (3 層) では、「パケット」、トランスポート層 (4 層) では「セグメント」と呼ばれます。

■ DoD モデルの PDU 名

DoD モデルの PDU 名は、ネットワークアクセス層の上位部分は、OSI 参照モデルのデータリンク層と同じく「フレーム」、インターネット層 (OSI 参照モデルのネットワーク層) では「データグラム」、Host to Host 層 (OSI 参照モデルのトランスポート層) からはプロトコルが TCP の場合は「セグメント」、UDP の場合は「パケット」、プロセス/アプリケーション層 (OSI 参照モデルの 5~7 層) では、プロトコルが TCP の上位プロトコルの場合は「ストリーム」、UDP の上位プロトコルの場合は「メッセージ」と呼ばれます。

現在は OSI 参照モデルに基づいた PDU 名で呼ばれることが多いですが、文献によって呼ばれ方は様々です。

階層	OSI 参照モデル		階層	DoD モデル		
	機能 モジュール	PDU 名		機能 モジュール	TCP の PDU 名	UDP の PDU 名
5 ~ 7	セッション層以上	データ	4	アプリケーション層	ストリーム	メッセージ
4	トランスポート層	セグメント	3	Host to Host 層	セグメント	パケット
3	ネットワーク層	パケット	2	インターネット層	データグラム	
2	データリンク層	フレーム	1 の 上位部	ネットワーク アクセス層上位部	フレーム	

図 3-2 ネットワークモデルと PDU 名

■ カプセル化した通信

コンピュータ間で通信されるデータは、送信側では、アプリケーション層で受信先のアプリケーション層でどのように処理するべきかを指示したプロトコル（制御情報）ヘッダを追加し、1つ下の階層の機能を実行する手続きに渡されます。ネットワークプロトコルの各階層で、通信データをどのように処理するべきかを指示したプロトコル（制御情報）ヘッダが、上位層の PDU の前に追加され、1つ下の階層の機能を実行する手続きに渡されます。

次々にプロトコル（制御情報）ヘッダを追加されたデータは、各階層の異なるプロトコルにカプセル化され、最後は電気信号に変換されてネットワーク内を受信先まで転送されます。

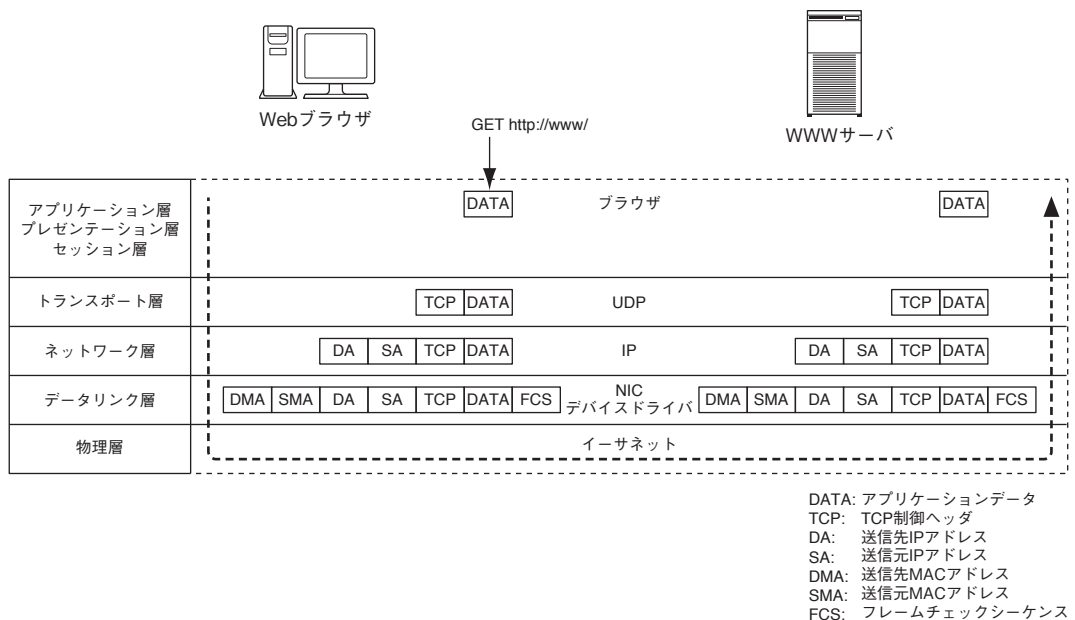


図 3-3 カプセル化した通信

受信側では、電気信号を一定のフォーマットにあわせて数値に変換し、送信元の各ネットワーク階層のヘッダ内容を、送信元と同じネットワーク階層（同位層）の手続きで送信元の指示に従って処理され、その階層で処理したプロトコルヘッダを除いたPDUを上位層に渡し、カプセル化を解きながら各階層のプロトコルを処理します。

Q 1

DoS 攻撃、DDoS 攻撃に用いられるものはどれですか？

- A. MITM
- B. ボットネット
- C. Null セッション
- D. リプレイ

Q 2

スタティック NAT の外側と内側のマッピングについて正しい説明はどれですか？

- A. スタティック NAT は多対 1 のマッピングを使う
- B. スタティック NAT は 1 対多のマッピングを使う
- C. スタティック NAT は 1 対 1 のマッピングを使う
- D. スタティック NAT は多対多のマッピングを使う

Q 3

代表的な NIDS はどれですか？

- A. Snort
- B. Nessus
- C. John the Ripper
- D. Wireshark

Q 4

ドメイン登録を最長 5 日間まで公開する手法はどれですか？

- A. DNS ポイズニング
- B. スプーフィング
- C. ドメインハイジャック
- D. Kiting

A 1 B

DoS、DDoS 攻撃には乗っ取られたゾンビ PC で構成されるボットネットが利用されることがあります。MITM はマンインザミドル攻撃、Null セッションは Windows マシンに列挙を仕掛ける手法、リプレイは再生攻撃のことで DoS、DDoS とは異なります。

A 2 C

スタティック NAT は、内部のマシン上で外部に公開するサービスを提供する場合外側から内側へのアクセスを許可するために、NAT の外側の IP アドレスと、内部のマシンの IP アドレスの 1 対 1 のマッピングを使います。

A 3 A

Snort は、代表的な NIDS です。Nessus はぜい弱性検査ツール、John the Ripper は、パスワードクラッカー、Wireshark はプロトコルアナライザーです。

A 4 D

カイトイングは、最長 5 日間の無料の登録猶予期間だけドメイン名を公開して利益を得ようとする手法です。スプーフィングはなりすまし、ドメインハイジャックスプーフィングの一種で、ドメイン名の所有者になりすましてドメイン名を支配下に置く攻撃です。DNS ポイズニングは、DNS キャッシュを汚染する攻撃で、DNS スプーフィングにも利用されます。

チェックポイント

- ★ケーブルとネットワーク構成要素の特徴
- ★ワイヤレス LAN のぜい弱性と対策
- ★TCP/IP のポート番号とプロトコルの関係
- ★プロトコルやシステムのぜい弱性を利用した攻撃の特徴
- ★ネットワークセキュリティツールの特徴

★この章は次の試験分野に対応しています。

試験分野	出題比率
システム セキュリティ	21%
ネットワーク インフラストラクチャ	20%
アクセス制御	17%
アセスメントと監査	15%
暗号化技術	15%
組織面でのセキュリティ	12%