実施日 2024 年 11 月 17 日

コンピュータ科学実験 b

ソフトウェア実験 第 1,2 週 調査課題

学生番号: 102210017
氏名: 安藤 駿
共同実験者: 太田 充洋, 草島 悠伸, 阪口 修吾

1　調査課題 1 TCP, IP パケットのヘッダ情報

1.1　TCP パケットのヘッダ情報

TCP ヘッダの構造は図 1 に示すようになっている.

送信元ポート番号は, 16 ビットのフィールドで、0〜65535 の範囲の値が使用され, パケットを送信したアプリケーションを識別するために使用される. 宛先ポート番号も 16 ビットのフィールドで, パケットが送信されるアプリケーションやサービスを識別するために使用する.

シーケンス番号は, 32 ビットのフィールドで, TCP セグメントのデータ部が元データの何バイト目の位置のものかを表すために使用される.

確認応答番号は, 2 ビットのフィールドで、受信側が「次に受信することを想定しているシーケンス番号」を送信側に伝えるために使用される.

データオフセットは, TCP ヘッダのサイズは可変長のため, 受信側にヘッダとデータの境目を正しく伝えるために, データフィールドの開始位置を表す、4 ビットのフィールドである.

予約は, 6 ビットのフィールドで, 将来のために予約されている. 現在は使用していないため「0」がセットされる.

制御ビットには, 1 ビットのフィールドが 6 つある. URG（Urgent Pointer）は, 1 の場合は緊急ポインタフィールドが有効であることを示す. 0 の場合は, 緊急ポインタフィールドの値も 0 になる. ACK（Acknowledgement Number）は, 1 の場合は確認応答番号フィールドが有効であることを示す. つまり, 1 の場合は確認応答番号フィールドに 0 以外の値がセットされている. 0 の場合は, 確認応答番号フィールドの値も 0 になる. コネクション確立時の最初の SYN パケット以外は, 必ず 1 でなければならない. PSH（Push）は, データを即座にアプリケーションに転送するよう指示するために使用される. 送信側 TCP は, プッシュ機能が指示されるまでデータを送信バッファにためて, 自分の都合が良いときに送信できる. RST（Reset）は, コネクションのリセットである. 通常は 0 がセットされているが, コネクションを一方的に強制終了させるときなどに 1 をセットして送信する. SYN（Synchronize）は, コネクション確立時に使われる. このビットが 1 の場合, コネクションの確立を要求するとともに, シーケンス番号に格納されている数字でシーケンス番号を初期化する. FIN（Fin Flag）は, 1 の場合以後送信するデータがないことを示す. 通信が終了し, コネクションを切断したい場合に使用する.

ウインドウは, 16 ビットのフィールドで, 受信バッファの空きサイズを受信側が送信側に通知するために使用される. 送信側では通知された値に従って, 送信パケット数を調整する.

チェックサムは, 16 ビットのフィールドでエラーチェックのためのフィールドである.

緊急ポインタは, 16 ビットのフィールドで, データ部に緊急データが含まれているときに緊急データの位置を受信側に伝えるために使用される.

オプションは, 必要に応じてオプションを追加できる任意のフィールドである.

パディングは, TCP ヘッダは 32 ビットの倍数と決められているため, 必要に応じて TCP ヘッダのサイズを調整するために使用される.

（pcap, 2018）

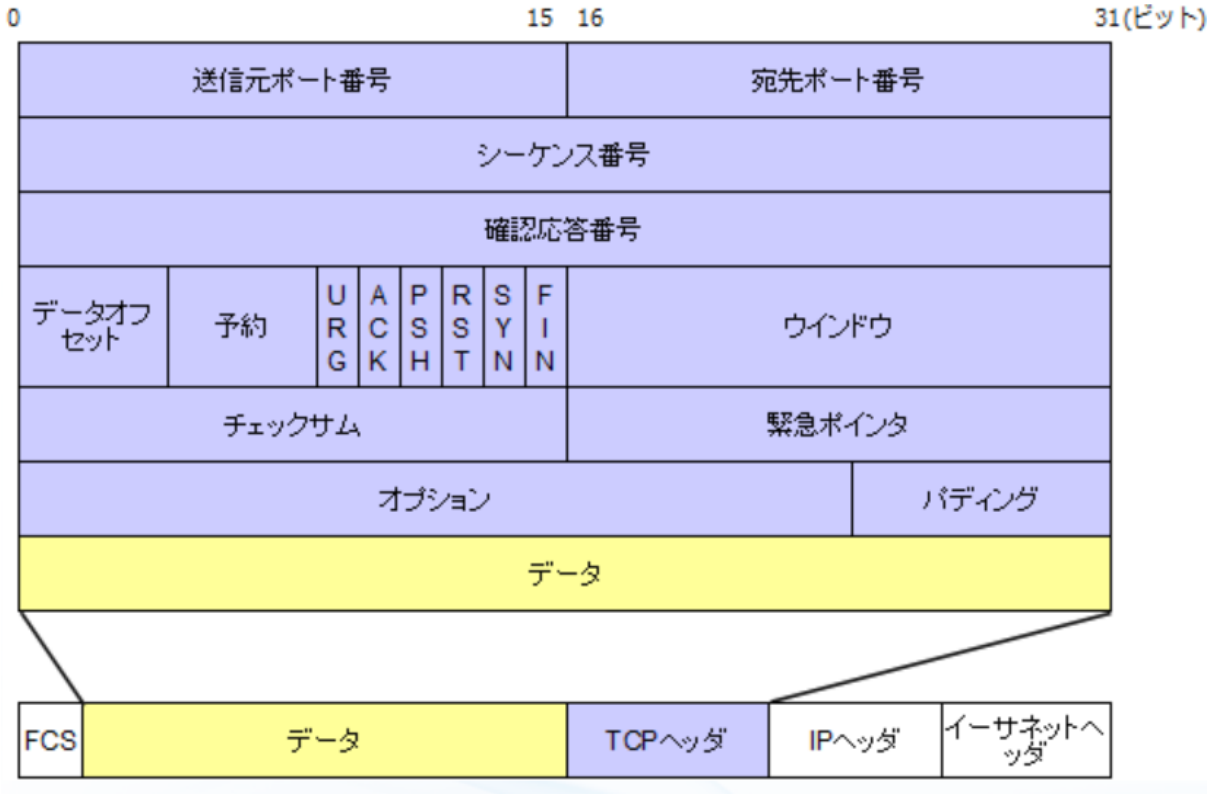

図 1　TCP ヘッダの構造

1.2　IP パケットのヘッダ情報

IP ヘッダの構造は図 2 に示すようになっている.

バージョンは, IP のバージョンである. IPv4 の場合は「4」がセットされる.

IP ヘッダ長は, 4 ビットのフィールドで, IP ヘッダのサイズを 4 で割った値がセットされる.

サービスタイプ（Type Of Service）は, TOS フィールドとも呼ばれ, QoS を行う場合に利用される.

IP データグラム長は, IP データグラム（IP ヘッダ + データ）のサイズをバイト単位で表す. IP 自体は最大 65,535 バイトまで扱うことができるが, 実際の IP データグラムのサイズはデータリンク層のプロトコルが扱える MTU に依存する.

ID（Identification）, フラグ, フラグメントオフセットは, データリンク層の MTU を超えるような大きいパケットが生成された場合, IP はデータリンク層の MTU に合わせてパケットを分割する. 分割されたパケットは受信側ホストで再構築される. 受信側でパケットが正しく再構築できるように必要な情報を提供するのが, ID, フラグ, フラグメントオフセットとなる.

生存時間（Time To Live:TTL）は, TTL と呼ばれ, 8 ビットのフィールドであり, パケットがネットワークに存在できる時間を秒数で表す. TTL の値は, 送信元ホストによって初期値が設定され, ルータがパケットを中継するたびに中継処理にかかった秒数（1 秒未満の場合は 1）ずつ減らされる.

プロトコルは, 8 ビットのフィールドであり, 上位層のプロトコルを番号で表す.

ヘッダチェックサムは, 16 ビットのフィールドで, 受信側でエラーチェックを行うための値がセットされる.

送信元アドレス（Sorce Address）, 宛先アドレス（Destination Address）は, それぞれ 32 ビットのフィールドで, 送信元の IP アドレスと宛先 IP アドレスがセットされる.

オプションは, 可変長のフィールドで, テストやデバッグなどを行うときに使用される.

パディングは, オプションフィールドが 32 ビットの整数倍にならない場合に、IP ヘッダサイズの調整のために 0 が挿入される使用される.

（pcap, 2018）

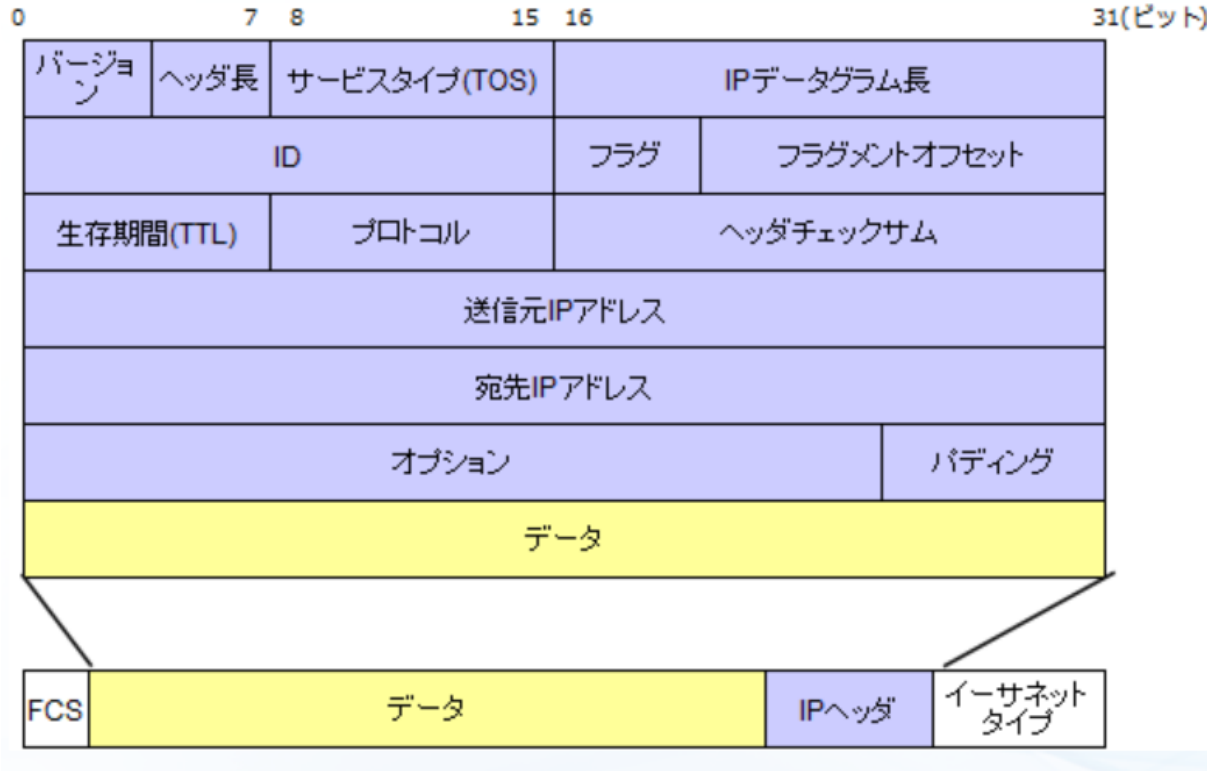

図 2　IP ヘッダの構造

2　調査課題 2 TCP/IP 通信におけるブロードキャスト

2.1　ブロードキャストの役割

ブロードキャストとは, ネットワークに接続されている全ての機器に対して, 同じ情報を一度に送信する通信方式のことである.

ブロードキャストは, ネットワークに接続されたデバイス（コンピュータ、プリンタ、ルータなど）を検出するために利用される. 例えば, DHCP クライアントが IP アドレスを取得する際, ネットワーク内の DHCP サーバを見つけるためにブロードキャストを使用する.

また, 新しいデバイスがネットワークに接続した際, IP アドレスを取得するために DHCPDISCOVER

メッセージをブロードキャストする. その結果, DHCP サーバが応答し、デバイスに適切な IP アドレスが提供される.

（e-words, 2023）

2.2 ブロードキャストの特徴

ブロードキャストの特徴は, 一度のデータ送信でネットワークに接続された多数の機器に同時に情報を届けることができることである.

この特徴は、いくつかの場面でメリットをもたらす.

まず, 送信元が受信先の機器のアドレスを個別に知らなくても, 情報を届けられることである. これは, ネットワークに接続されている機器の数が多い場合や, 接続状況が流動的な場合に特に有効である. 例えば, 大規模な社内ネットワークや, 不特定多数の機器が接続する公共 Wi-Fi などでも, それぞれの機器のアドレスを把握していなくても, ブロードキャストを使えば情報を確実に届けることができる.

また, 一度の送信ですべての機器に情報を届けられるため, 送信側の負担が軽減されるというというメリットもある. 個別にデータを送信する場合と比べて、ネットワークの負荷を大幅に減らすことができる. これは, ネットワークの帯域幅が限られている場合や, リアルタイム性が求められるシステムにおいて大きな利点になる.

しかし, デメリットもある. ブロードキャストは, ネットワークに接続されているすべての機器に対して, データを送信してしまう. これは, 必要なデータを受け取る機器にとっては効率的であるが, 関係のない機器にとっても同様の処理が発生することになるので, ットワーク全体の情報量が過剰になり, 処理速度の低下を招く可能性がある.

また, 攻撃者がブロードキャストを利用して, ネットワーク内のすべてのデバイスに不正なパケットを送信する可能性があり, セキュリティが脆弱になることなどの問題が生じることもある.

（netanzen, 2024）

3 調査課題 3

PC1（192.168.200.2）から PC2（10.10.1.20）への SSH 接続において、TCP パケットが目的地に到達するまでの過程を説明する.

3.1 PC1 からの送信情報

TCP/IP プロトコルを使用して、PC1 は SSH（ポート番号 22）の通信を開始する.

パケットに含まれている情報は, 送信元 IP アドレス（192.168.200.2）, 送信元ポート（動的に割り当てられる）, 宛先 IP アドレス（10.10.1.20）, 宛先ポート（22）などである.

3.2 ARP プロトコルによる MAC アドレス解決

PC1 が最初に ARP プロトコルを使用して、ルータ（デフォルトゲートウェイ）の MAC アドレスを取得する．これにより、Ethernet フレームに適切な宛先 MAC アドレスが設定される．

3.3 LAN ルータ（192.168.200.1）での処理

PC1 から受信したパケットをチェックし、宛先 IP（10.10.1.20）が異なるネットワークに属していると判断する．ルーティングテーブルを参照し、パケットを FW 構築実験用ルータ（192.168.100.1）に転送する．

3.4 FW 構築実験用ルータ（192.168.100.1）の処理

192.168.100.1 のファイアウォール（icesc01）が受信パケットを検査する．SSH 通信（TCP 22 番ポート）が許可されている場合のみ、転送を実行する．

パケットを教育用計算機システムネットワーク（10.10.0.0/16）に送信する．

3.5 教育用計算機システムネットワークへの到達

192.168.100.1 から送信されたパケットが、教育用計算機システムネットワーク内のルータ（icesc20, IP: 10.10.1.255）に到達する．ルータ（icesc20）はパケットを最終的な宛先 PC2（10.10.1.20）に転送する．

3.6 PC2 での受信

PC2（10.10.1.20）が SSH パケットを受信し、TCP 接続の確立を試みる．成功すると、SSH 接続が開始される．

3.7 ルーティング情報

各ルータ（各班用ルータ, FW 構築実験用ルータ）はルーティングテーブルを保持しており, 宛先 IP アドレスに基づいて次に転送すべきネットワークインターフェースを判断する．

各ネットワーク間をつなぎ、パケットを目的地まで確実に届ける．

3.8 ブロードキャストの役割

ネットワーク内で新しいデバイスの IP アドレスを解決する際, ARP（Address Resolution Protocol）でブロードキャストが利用される．例えば, PC1 が「各班用ルータの MAC アドレス」を取得するために ARP リクエストを送信し, その応答を得る形で通信が開始される．

4　調査課題 4 DNS の詳細

4.1　DNS（Domain Name System）とは

DNS（Domain Name System）とは, インターネットなどの IP ネットワーク上でドメイン名と IP アドレスの対応関係を管理するシステムである. 利用者が単なる番号列である IP アドレスではなく, 日常使っている言語の文字を組み合わせた認識しやすいドメイン名で, ネットワーク上の資源にアクセスすることができるようになる.

例えば, ある企業が「198.51.100.1」という IP アドレスの割り当てを受けて Web サーバと電子メールサーバを運用する場合, Web サイトの URL は「https://198.51.100.1/」のようになり, 代表メールアドレスは「info@198.51.100.1」のような表記になる. これは人間にとっては覚えたり伝達したり入力したりしにくい.

また, 接続事業者を切り替えるなどして IP アドレスが替わるとこれらのアドレスもすべて変更となり, 記録物を書き直したり関係者に改めて通知・告知しなおさなければならなくなってしまう.

そこで,「example.co.jp」というドメイン名を取得し, ホスト名として「www.example.co.jp」を「198.51.100.1」に,「〜@example.co.jp」のメールアドレスを管理するメールサーバのアドレスを「198.51.100.1」に対応付けておけば, これらの問題を解決できる.

4.2　DNS の基本的な仕組み

DNS クライアント（リゾルバ）が, ユーザーがウェブサイトにアクセスする際に, 最初に DNS リクエストを送信する. そして, DNS サーバーが, このリクエストを受け取り、適切な IP アドレスを返すことで, ドメイン名と IP アドレスが対応付けされる.
（e-words, 2023）

4.3　DNS のセキュリティ強化の動向

DNS のセキュリティ強化のための技術として, DNSSEC がある. DNSSEC（Domain Name System Security Extensions）は, DNS データの完全性と認証を提供するための技術である.

この技術により, DNS の応答が改ざんされていないことを確認できる. 具体的には, DNS リソースレコード（RR）の応答にデジタル署名を追加し, リゾルバが署名を検証することで, 偽の DNS レコード（例: フィッシング攻撃による偽サイトのリダイレクト）を防止することができる.
DNSSEC では、DNS レコードにデジタル署名を追加する. これにより、DNS データが正当であるかどうかを確認するための署名が生成される.
公開鍵と秘密鍵のペアを使用して, DNS データを署名する. ドメインの権威 DNS サーバーは, 秘密鍵を使って DNS レコードを署名し, その署名を含む応答をリゾルバに返す. DNS レコードに署名するために使用され, 秘密鍵が漏洩しないように厳重に管理される. DNS リゾルバが DNS レコードの署名を検証するために

使用され, 公開鍵は DNS レコードに含まれているか, 上位の権威サーバーから取得される.
（nesuke, 2023）

5　調査課題 5 暗号化を行うプロトコル

5.1　SMTP

SMTP（Simple Mail Transfer Protocol）は, メールを送信するために使われるプロトコルのことである.

SMTP は 1980 年代から使われている古いプロトコルで, 最初の仕様は IETF によって 1982 年に RFC 821 として規格化された. 幾度かの改訂を経て 2008 年に最新版の RFC 5321 が発行されている. 1994 年に追加された拡張機能やコマンド群は「ESMTP」（SMTP Service Extensions）と呼ばれることもある.

暗号化の仕組みには, STARTTLS などでがあり, これは, SMTP 通信の途中で TLS 暗号化を開始する方式である. 暗号化がサポートされていない場合は通常の通信にフォールバックする.
また, SMTPS（SMTP over SSL/TLS）は, 通信の開始時から TLS を使用して暗号化する方式である.
（baremail, 2021）

5.2　IMAP

IMAP（Internet Message Access Protocol）は、インターネットなどの IP ネットワークで標準的に用いられる, 電子メールを受信するためのプロトコルである. 利用者が自分宛ての電子メールを保管しているメール受信サーバにアクセスし, 新着を確認したり一覧から必要なものを選んで手元に受信する手順を定めている.

最も初期のバージョンは IETF が 1988 年に RFC 1064 として策定した IMAP2 だが, 正式名称は現在と異なり Interactive Mail Access Protocol だった. 1994 年に IMAP4 が RFC 1730 として策定され, このとき現在の名称に改められた. IMAP4 は最も普及したバージョンであり, 単に IMAP といった場合は IMAP4 を指すことが多い. IMAP4 には様々な拡張仕様が追加され, 2003 年には RFC 3501 として改訂されている.

暗号化の仕組みには, IMAP over SSL/TLS があり, これは, IMAP で TLS 暗号化を使用する方式である.
また, POP3 over SSL/TLS は, POP3 で TLS 暗号化を使用する方式である.
（e-words, 2021）

5.3　FTP

FTP（File Transfer Protocol）は, ネットワーク上でファイルを送受信する際に使用する通信プロトコルである.
FTP サーバーに作成したファイルをアップロードすることで, 新規の Web ページを追加できる. また, 既存ファイルの一部を書き換えたものをアップロードし, サーバー上の既存ファイルに上書きすれば, 公開済みのページの内容を更新することも可能である.

暗号化の仕組みには, FTPS（FTP Secure）があり, これは SSL/TLS を使用して通信を暗号化した FTP

の拡張版である.

また, SFTP（SSH File Transfer Protocol）は, SSH プロトコルを使用してセキュアな通信を行う別の方式である.

（kagoya, 2024）

参考文献

[1] pcap: *TCP* プロトコル.
https://pcap.it-mem.info/プロトコル/tcp プロトコル/ 2018.

[2] pcap: *IP* プロトコル.
https://pcap.it-mem.info/プロトコル/ip プロトコル/ 2018.

[3] e-words: ブロードキャスト.
https://e-words.jp/w/ブロードキャスト.html 2023.

[4] netanzen: ブロードキャストとは？ 誰でもわかるネットワーク通信の基本.
https://netanzen.jp/network/understanding-broadcast-a-basic-network-communication-method/ 2024.

[5] e-words: *DNS*【*Domain Name System*】ドメインネームシステム.
https://e-words.jp/w/DNS.html 2023.

[6] nesuke: 初心者にも分かりそうな *DNSSEC* の仕組みと機能.
https://milestone-of-se.nesuke.com/l7protocol/dns/dnssec-summary/ 2023.

[7] baremail: *SMTP* とは？ メール送受信の基礎知識と、*SMTP* サーバーの機能と課題.
https://baremail.jp/blog/2021/04/05/1217/ 2021.

[8] e-words: *IMAP*【*Internet Message Access Protocol*】*IMAP4*.
https://e-words.jp/w/IMAP.html 2020.

[9] kagoya: *FTP* とは？ 通信の仕組みやソフトについてわかりやすく解説.
https://www.kagoya.jp/howto/it-glossary/web/ftp/ 2024.