輪読会 #1

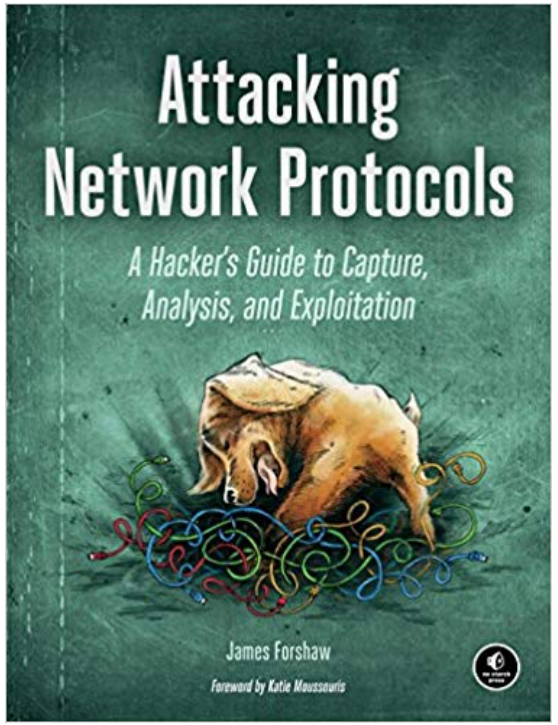
Attacking Network Protocols #1

The Basics Of Networking

ed

本書の紹介

- 著者｜James Forshaw
  - Google Project Zero に参加しているセキュリティ研究者
    - Google の脆弱性発見チーム
    - 「macOS」にゼロデイ脆弱性ーグーグルのProject Zeroが情報公開
  - Microsoft から $100,000 の賞金を獲得



- 攻撃者の観点からネットワークを調査, 脆弱性発見, 悪用し, 最終的に保護について解説
  - パケットキャプチャ, 操作, なりすまし, 独自のキャプチャフレームワーク作成, コードのリバーシング, パスワードクラッキング, トラフィック復号化, DoS, SQLインジェクション, メモリ破壊による脆弱性の悪用, トラフィックの再ルーティング, 圧縮, データフローの制御

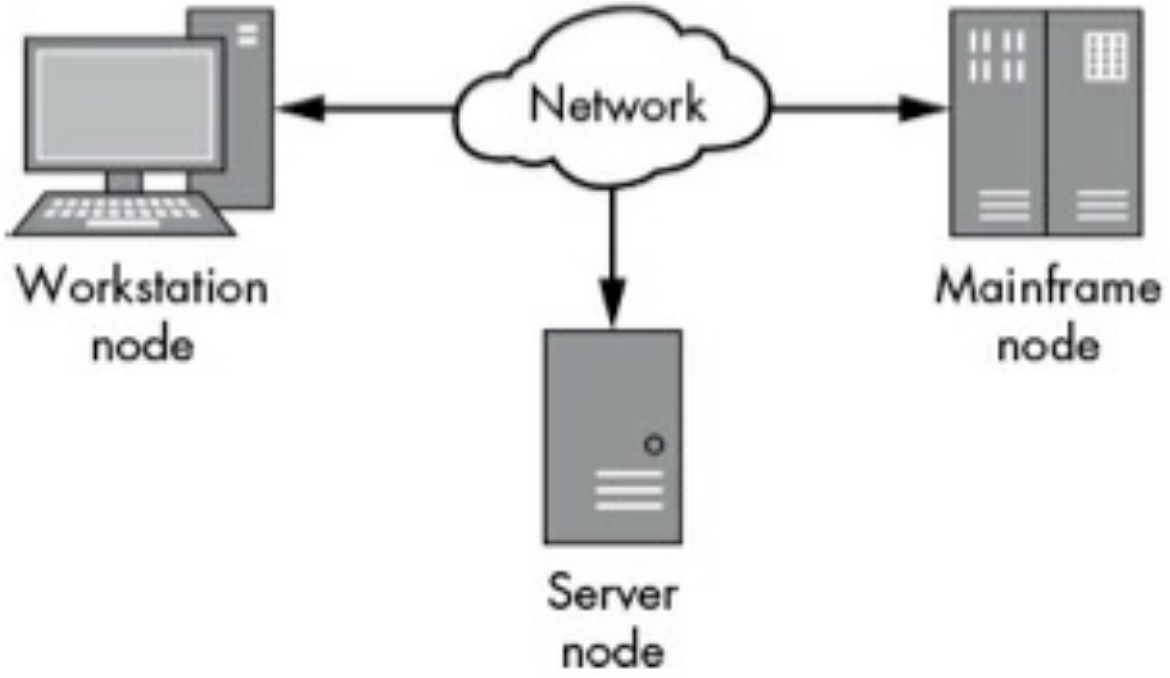
攻撃の前に, ネットワークとは何か？

情報共有のため互いに接続された２台以上のコンピュータのセット

ノードはOS, ハードが異なってもプロトコルに従う限り正しく通信可能

プロトコル性質例

- セッションの確立, 維持, 終了
- アドレスによるノード識別
- フロー制御
- データ到着順序保証
- エラー検知と修復
- データの形式と変換



インターネットプロトコルスイート

インターネットを成立させている一連のプロトコル

アプリケーション層

ユーザアプリケーションと対話

トランスポート層

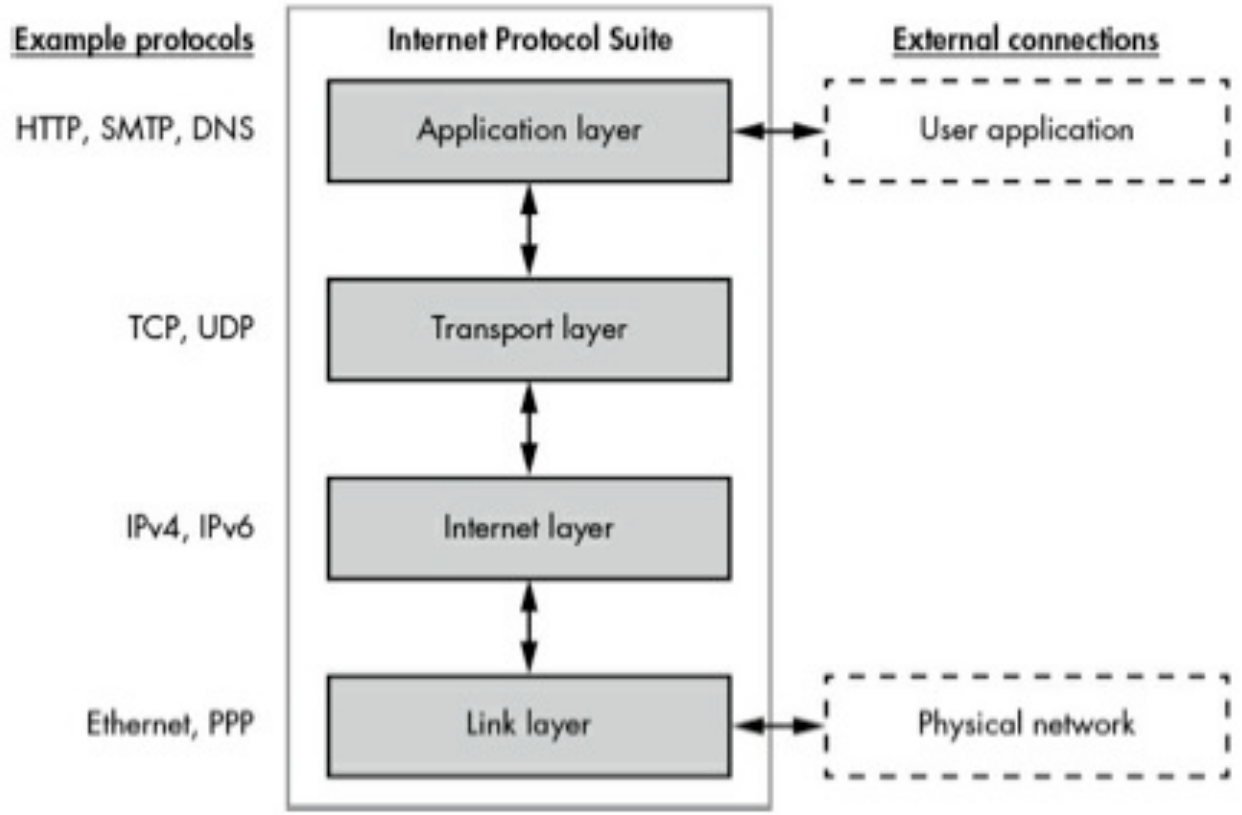
クライアント，サーバー間接続を規定

インターネット層

ネットワークのアドレッシングを規定

データリンク層

LAN 内のノード間通信を規定

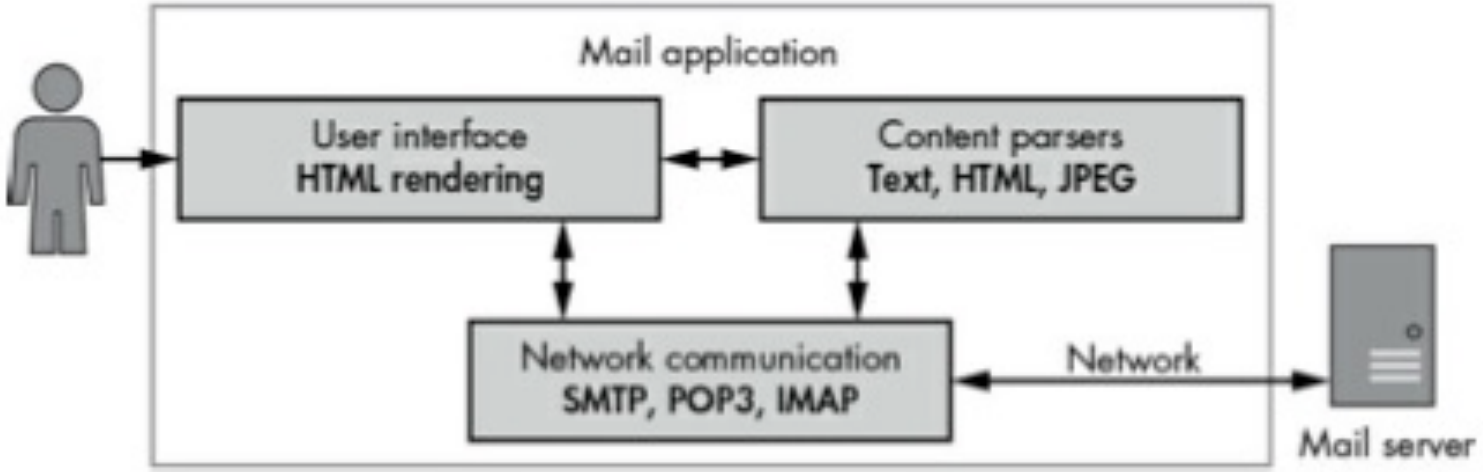


ユーザアプリケーション｜Mail

アプリケーション｜ユーザにサービスを提供する関連機能の集合

メール｜ネットワークを介したメッセージの送受信

- Network Communication｜ネットワークを介して通信（SMTP, POP3）
- Content Parsers｜受信データから内容を抽出（本文としてテキストデータ, 動画像）
- User Interface｜ユーザにデータを表示（Webブラウザ内でHTMLメールを表示）

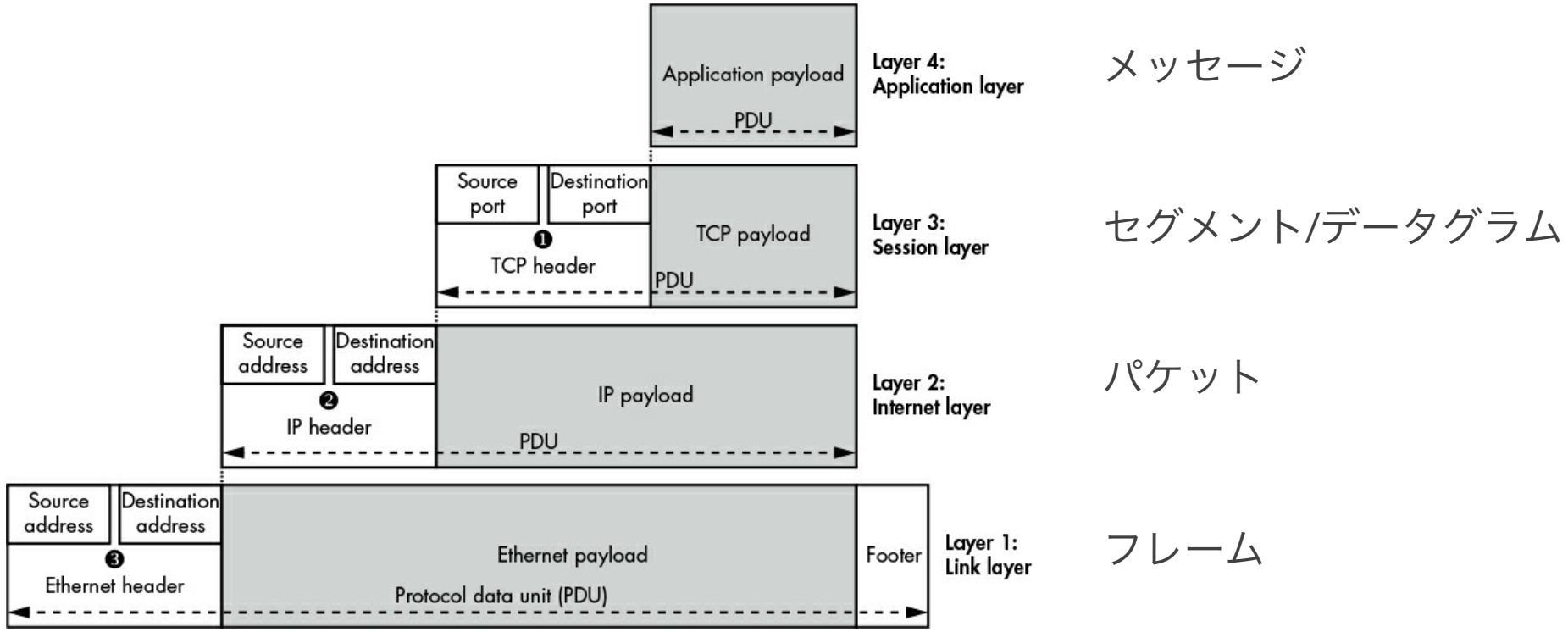


データのカプセル化

各層は上層からのデータをカプセル化するため，レイヤー間で通信可能

プロトコルデータユニット(PDU)｜各層で送受信されるデータ

先頭にデータ送信に必要なデータ，末尾にエラーチェック情報

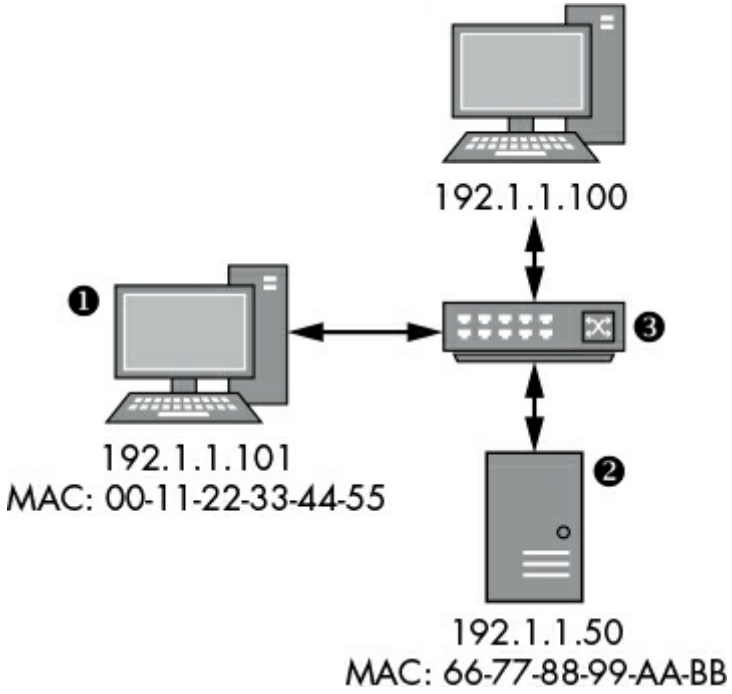


データ転送

1 から 2 に Internet Protocol を用いてデータを送信

3 のスイッチは全ノード間でフレームを転送

* スイッチはリンク層のみで稼働するため IP アドレスは不要



1. 1 の OS はセグメントを src: 192.1.1.101, dst: 192.1.1.50 でカプセル化しパケット生成
2. 1 の OS はパケットをフレームとしてカプセル化
   - ただし，宛先 MAC アドレスが不明
   - IP から MAC アドレス特定のため ARP リクエストをネットワーク全域に送信
   - レスポンス受信後, src: 00-11-22-33-44-55, dst: 66-77-88-99-AA-BB からフレーム生成し送信
3. 3 のスイッチはフレーム受信後, 宛先ノードへ転送
4. 2 の OS はフレームからパケットを取り出し，正当性確認後，IPペイロードを上層へ渡す

ネットワークルーティング

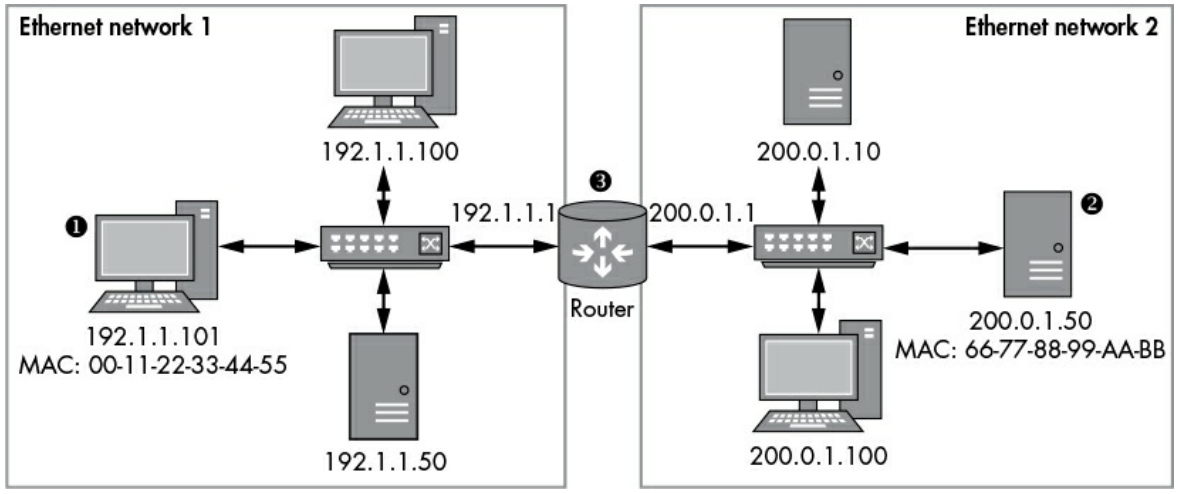
イーサネットは全ノードが同一ローカルネットワークに直接接続

インターネット上の全ノードを直接接続は非現実的

独立なネットワーク同士を接続し，アドレス範囲によって識別

1 から 2 に Internet Protocol を用いてデータを送信

IPアドレスとサブネットマスクから判断可能



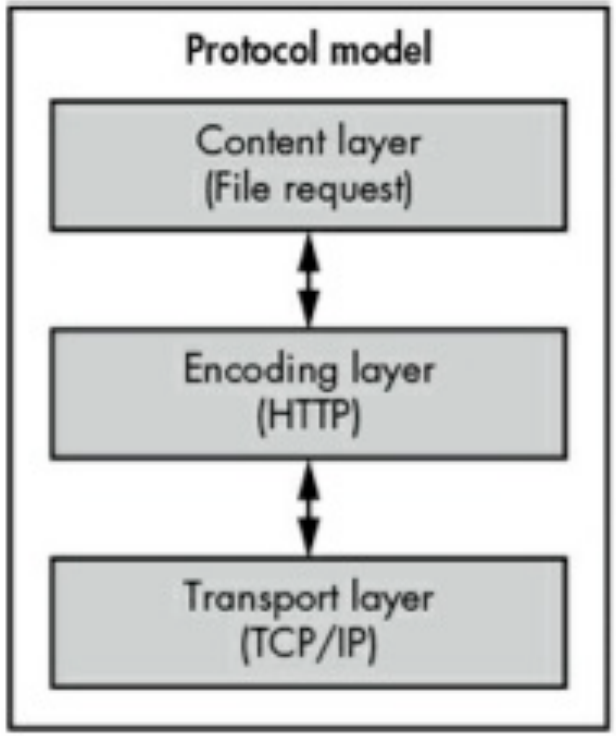
1. 1 はセグメントを src: 192.1.1.101, dst: 200.0.1.50 でカプセル化しパケット生成
2. 1 はパケットをフレームとしてカプセル化
   - 宛先アドレスが自ネットワーク外のため自ルーティングテーブルを参照
     * 200.0.1.50 宛パケットは192.1.1.1 が取り扱い可能と知っている
   - 192.1.1.1 の MAC アドレスを知るため ARP 送信
   - レスポンス受信後, src: 00-11-22-33-44-55, dst: [Router MAC Address] からフレーム生成し送信
3. 3 のルーターはフレーム受信後, パケットを取り出し, 宛先アドレスを確認後, 転送
   - ルーター宛でないと判断
   - 200.0.1.50 の MAC アドレスを検索しフレーム生成
   - ネットワーク2に送信

プロトコル解析のためのモデル

インターネットプロトコルスイートは分析目的では冗長

アプリケーションネットワークプロトコル分析のための独自モデルを導入

分析のため，アプリケーション固有のプロトコルの見通しが良くなる



通信目的を表現｜ファイル'image.jpg'に対してHTTPリクエスト送信

```
I would like to get the file image.jpg
```

表現方法｜取得ファイルを指定する HTTP GET 要求にエンコード

```
GET /image.jpg HTTP/1.1
```

```
4500 0043 50d1 4000 8006 0000 c0a8 0a6d
d83a d544 40e0 0050 5dff a4e6 6ac2 4254
5018 0102 78ca 0000 4745 5420 2f69 6d61
6765 2e6a 7067 2048 5454 502f 312e 310d
0a0d 0a                ...
```

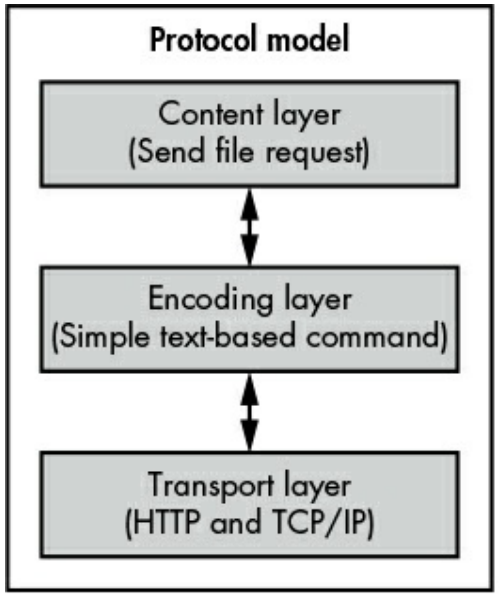
ノード間データ転送方式を表現｜HTTP GET リクエストは TCP/IP を通してリモートノード 216:58.213.68:80 へ送信

プロトコル解析のためのモデル（利用例）

状況｜マルウェアからのネットワークトラフィックを調査中

1. マルウェアはHTTPによりサーバー経由でクラッカーからコマンドを受信
2. クラッカーがマルウェアに，感染したコンピュータの全ファイル列挙を要求
3. クラッカーは特定のファイルをサーバーへアップロードするように要求

以上をクラッカー，マルウェアの対話方式の観点からプロトコル分析



通信目的を表現｜マルウェアが窃盗したファイル'secret.doc'をサーバーに送信

```
Sending file secret.doc with content 1122..
```

表現方法｜コマンドは'SEND'，ファイル名，データからなるテキスト文字列

```
SEND secret.doc 1122..
```

転送方式表現｜'%'を用いた標準のHTTPリクエストでコマンドを転送

```
GET /image.jpg?e=SEND%20secret.doc%11%22 HTTP/1.1
```

TCP/IP は重要ではなく，分析の必要があるプロトコルそうに焦点を合わせたモデル

まとめ

- ネットワークとは何か？
- インターネットプロトコルスイート
- ユーザーアプリケーション｜Mail
- データのカプセル化
- データ転送
- ネットワークルーティング
- プロトコル解析のモデル