マルチチャットプログラムの作成と TCP-DUMP によるパケット通信の解析

提出者：214　岡田久司
共同研究者：205　上嶋将大

1. 実験概要

インターネット通信、特にパケット通信について、データがどのように流れているかを調査する。そのために自らチャットプログラムを作成し、通信環境の違いによるパケットの違いを TCP-DUMP を用いて解析・考察する。TCP-DUMP による解析では、①自作チャットプログラムによる通信、②チャットサイト「Skype」による通信、③就活サイトや和英翻訳サイトなどのネットサーフィン時、この 3 つの環境で解析する。

2. 実験結果

チャットプログラムはウェブ上のサンプルプログラムを参考に完成させた。

以下に示すのは翻訳サイトにおける通信の TCP-DUMP による解析結果の一部である。

```
・・・
0x03a0:  6e74 656e 742d 4c65 6e67 7468 3a20 3132  ntent-Length:.12
0x03b0:  330d 0a0d 0a62 6566 6f72 653d 5468 6973  3....before=This
0x03c0:  2b69 732b 616e 2b61 7070 6c65 2e26 7762  +is+an+apple.&wb
0x03d0:  5f6c 703d 454e 4a41 2661 6674 6572 3d25  _lp=ENJA&after=%
0x03e0:  4533 2538 3125 3933 2545 3325 3832 2538  E3%81%93%E3%82%8
0x03f0:  4325 4533 2538 3125 4146 2545 3325 3832  C%E3%81%AF%E3%82
・・・
```

3. 実験考察・感想

TCP-DUMP による解析で、情報が平文で流れている場合と暗号化されて流れている場合があることが分かった。情報の秘匿性が求められるサービスは暗号化され、自作チャットプログラムや翻訳サイトは暗号化されていない。インターネット通信が日常生活に大きくかかわる現代において、インターネット通信の方法と、通信手段や暗号化技術の大切さを学ぶことができた。

反省点として、実験環境の準備に大きく時間を割かれた結果、解析できた環境はごくわずかとなってしまったことがあげられる。