

■ #15_通信の約束事 : プロトコル_まるみえ HTTP_ゲームの通信を見る

せっかくなので、WireSharkを使って、ネットワークゲームの通信をのぞいてみましょう。今回、ゲームの通信が非常に見やすいと定評のある、某“艦〇れ”を題材にしてみましょう。

1. “艦〇〇れ〇〇〇〇”って？

スマホが広まった初期に開発されたソーシャルゲームです。ソーシャルゲームなので、ブラウザ上で提供された AdobeFlash の環境を使ったゲームです。

iPhone で動かないとか、コラボキャラが異常に強すぎるとか、台湾の漫画が本家だとか、当時いろいろ話題になりましたが、実はクライアントとサーバ間の通信が非常にわかりやすいと話題になったゲームでもあります。

2018 年 8 月に、AdobeFlash の環境から、HTML5 に環境が移行し、動作環境が広がったのですが、やっぱり iPhone でな動かない模様。

第 2 期になり、通信の解析は多少難しくなったのですが、基本的には同じと考えていいでしょう。

では、WireShark を起動して、ブラウザから“艦〇れ”起動してみます。起動には DMM GAMES のアカウントが必要です、Yahoo などで、使い捨ての一時的なアカウントを作成してからの方がいいかもしれません。

※一応大人ページに分かれていますが、“R18 的”、“肌色成分”が多いゲームがたくさんあります。
気をつけてください。

2. なぜ“艦〇れ”は、通信が見やすいのか？

それは、ゲーム内の通信がほぼ“平文”で行われていたためです。当時は“セキュリティ”への意識も低く、あまり気にしていなかったのですが、チートされまくりでカオスな状態になりました。

現在は、先にも書いたように第 2 期として AdobeFlash から HTML5 へ移行し、一部セキュリティの改善が見られますが、基本的な枠組みはあまり変わらないため、今回教材として利用します。

また、提供元の DMM GAMES のサイト自体は HTTPS 化されていますが、“艦〇れ”のページは HTTPS 化しておらず見やすい事もあります。

DMM GAMES : <https://games.dmm.com/>

“艦〇れ” サイト : http://www.dmm.com/netgame/social/-/gadgets/=/app_id=854854/

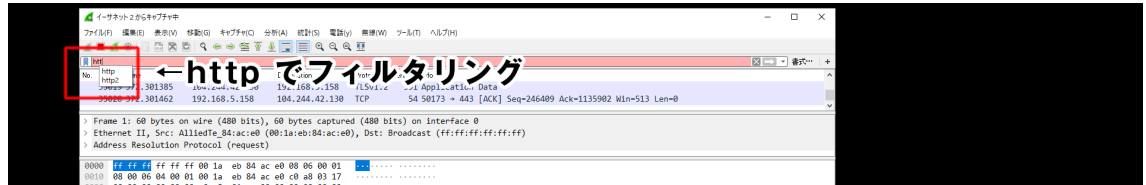
3. キャプチャリング手順

それでは、“艦これ” サイトを開いて、Wireshark も起動しておきます。

3.1. WireShark で何を見るのか

これから、“艦これ” の通信をのぞいてみます。WireShark でキャプチャ開始すると、例によって関係ない通信もキャプチャしてしまい、何のことやらになります。

“艦これ” は通信に “HTTP” を利用していますので、まずは “HTTP” でフィルタリングをかけることにします。



そうすると緑色の HTTP 通信の結果だけが表示されます、それにしても、GET とか POST とか、やたら見慣れたキーワードがたくさん出てきます。

“艦これ”の通信は基本的に POST していますので、先ほどのフィルタリングに POST を追加しておきます。

```
http.request.method == POST
```

これで、ゲーム内を移動すると、そのたびにリストに通信内容がリスティングされます。Info の欄を見ると、なんとなくどのページの通信が分かりそうですね。

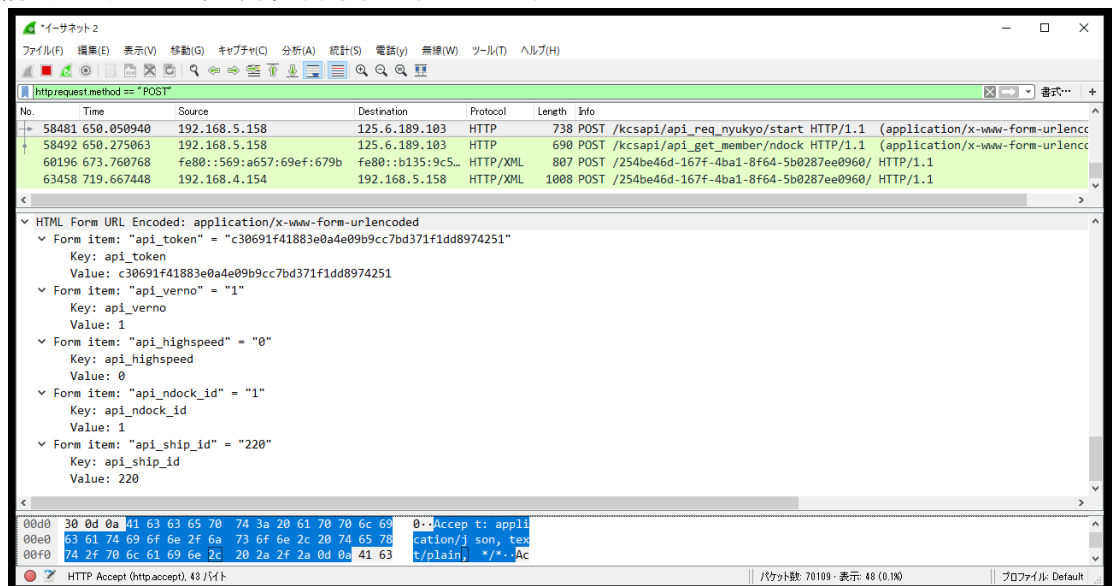
3.2. 修理の様子を見てみます

では、簡単なところから。適当に戦闘して修理をしてみます。そうすると

```
/kcsapi/api_req_nyukyo/start HTTP/1.1 ....
```

という項目があると思いますので、そこをクリックして、HTML Form URL Encoded: の欄を見てみましょう。何やら気になるキー名がちらほらありますね。

ここに自分の都合のよいキーや数字を入れると、結果を操作することができます。あくまで “できる” ということで、自分のプログラムのデバッグ以外の目的でやってはいけません。



3.3. いろいろググると・・・

ここに、これ以上書けないのですが、キーの解析結果なんかもちまたにあふれてるのですね。

今回は、ゲームの通信の現状を把握することが目的ですが、知れば知るほど怖くなりますね。現在は暗号化された HTTPS が主流になってきますが、それはそれで暗号化・複合化のオーバーヘッド、デバッグが困難になることなど、開発者にとって手間がかかる事が多くなる事を考えると憂鬱です。

現在はその切り替え時期なので、今のうちにいろいろ勉強しておくといいかもしれません。

参考資料：興味ある人はこんなの見ると面白いかも

○チェックポイント・キーワード：特に変わりなし



- ・HTTP
- ・SSL/TSL
- ・平文
- ・パケットキャプチャ
- ・再構成
- ・8つのメソッド： GET、POST は特に！
- ・CS(クライアント-サーバシステム)

図は [かわいいフリー素材いらすとや](#)