

## リモートアクセス(Telnet)

Telnet : インターネットやイントラネットなどでネットワークに接続されたコンピュータを遠隔操作する為の標準方式。そのために使用されるプロトコル。Telnet サーバを立ち上げてあるコンピュータに他のコンピュータから Telnet クライアントを使ってログオンし、そのコンピュータの目の前にいるのと同じように操作することが出来ます。

※ドラマやアニメでハッカーがターゲット PC に不正アクセスする時に使っている方法の 1 つです♪  
今日は Telnet を使って Linux サーバを乗っ取ってみよう！！

昨年習ったと思いますが、Telnet は非常に単純な通信であり暗号化もされておらず、セキュリティ上問題があるため現在は非推奨となり、ssh に置き換えられています。しかし、製造業など現場によっては telnet でないといけないようなケースもままあり、完全には駆逐されきっていないのが実際ですので一応、理解しておきましょう！

### (1) Telnet サーバの確認

```
[hal@motobe ~]$ rpm -q telnet-server
```

パッケージ telnet-server はインストールされていません。

### (2) telnet クライアントおよび telnet サーバのインストール

```
[hal@motobe ~]$ sudo yum -y install telnet-server telnet
```

```
[hal@motobe ~]$ rpm -q telnet-server
```

telnet-server-0.17-85.el9.x86\_64 ←telnet サーバ

```
[hal@motobe ~]$ rpm -q telnet
```

telnet-0.17-85.el9.x86\_64 ←telnet クライアント

### (3) telnet 起動

```
[hal@motobe ~]$ sudo systemctl start telnet.socket
```

※サービスの確認

```
[hal@motobe ~]$ sudo systemctl list-units
```

( 以下略～ )

telnet.socket loaded active listening Telnet Server Activation Socket

( 以下略～ )

### (4) Firewall 設定

```
[hal@motobe ~]$ sudo firewall-cmd --add-service=telnet --zone=public
```

success

```
[hal@motobe ~]$ sudo firewall-cmd --list-services
```

cockpit dhcpv6-client http ssh telnet

※セキュリティ上 --permanent は付けない方がいいかも

## (5) Linux での確認

```
[hal@motobe ~]$ telnet localhost
```

```
Trying ::1...
```

```
Connected to localhost.
```

```
Escape character is '^'.
```

```
Kernel 5.14.0-252.el9.x86_64 on an x86_64
```

```
motobe login: hal
```

```
Password: ←パスワードは見えません
```

```
Last login: Sun May 14 21:28:26 on tty2
```

```
[hal@motobe ~]$ pwd
```

```
/home/hal
```

```
[hal@motobe ~]$
```

※ログイン出来ました！

## (6) Windows での確認

### ①Windows のコマンドプロンプト

```
C:\Users¥moto>telnet 192.168.42.2
```

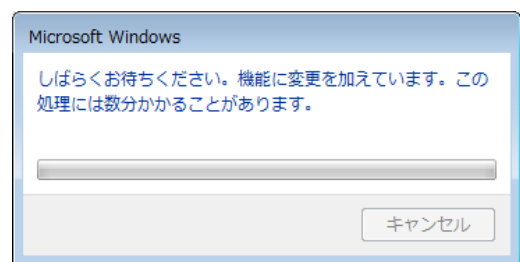
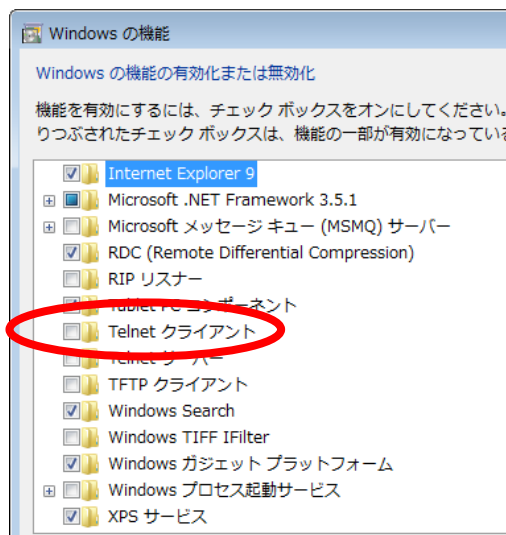
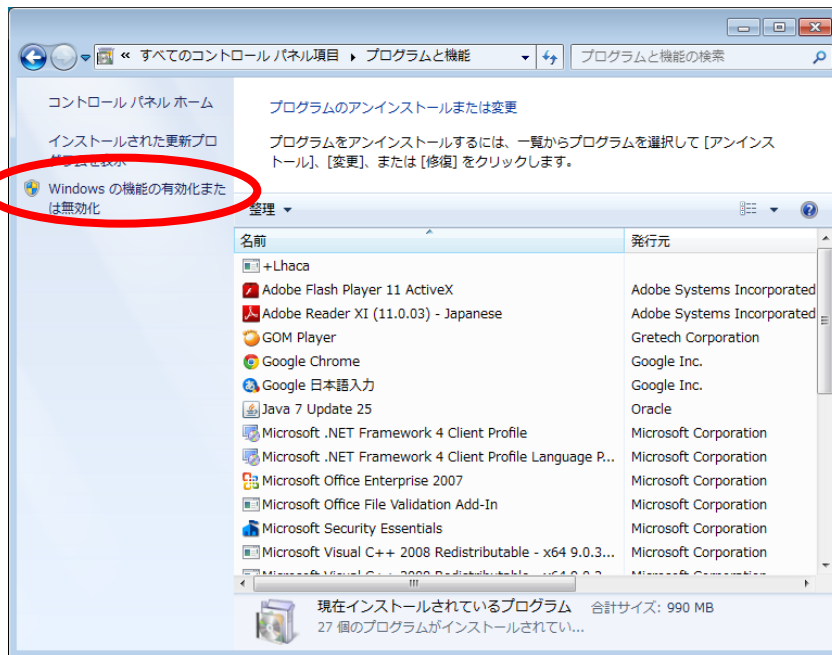
'telnet' は、内部コマンドまたは外部コマンド、  
操作可能なプログラムまたはバッチ ファイルとして認識されていません。

※Window10、8、7 はセキュリティで telnet が使用できなくなっています。 ←皆さんは昨年インストールしたかも

### ②Telnet のインストール

**【コントロールパネル】 → 【プログラムと機能】 → 【 Window 機能の有効化または無効化】 → 【 telnet クライアント 】のチェック**





③もう一度 Windows からログイン

C:\Users\moto>telnet 192.168.221.128

Kernel 5.14.0-252.el9.x86\_64 on an x86\_64

motobe login: hal

Password: ←パスワードは見えません

Last login: Sun May 14 23:03:03 from localhost

[hal@motobe ~]\$ pwd

/home/hal

ログイン成功！

適当に Linux を乗っ取ってみましょう！

## ④ログインしているユーザの確認

[hal@motobe ~]\$ **who**

```
hal      seat0      2023-05-14 21:28 (login screen)
hal      tty2       2023-05-14 21:28 (tty2)
hal      pts/1      2023-05-14 23:03 (localhost)
hal     pts/2      2023-05-14 23:16 (::ffff:192.168.221.1)
```

## (7) MAC での確認

MAC の端末で

**brew install telnet**

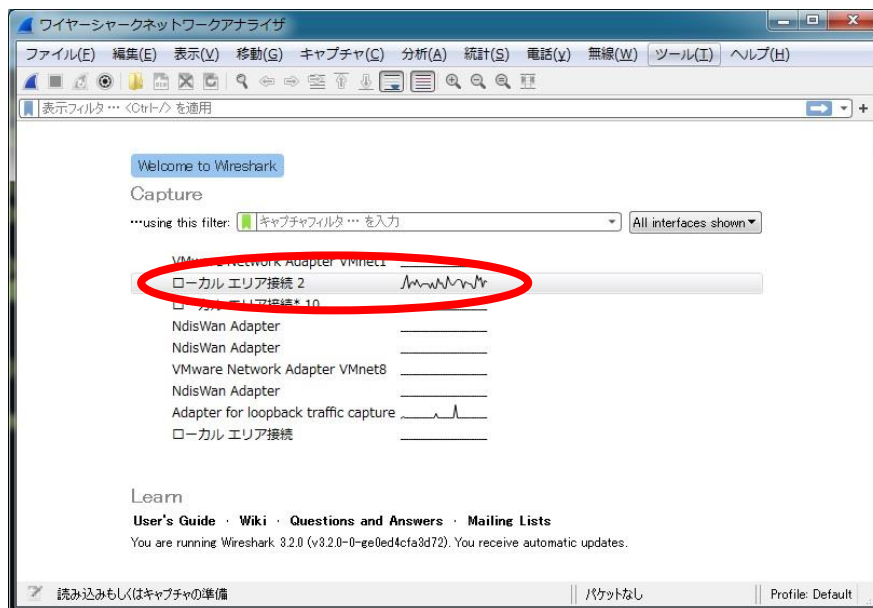
でインストール出来ます

※homebrew がインストール出来ていない方は先に **homebrew** をインストールしてください

## (8) Telnet の盗聴

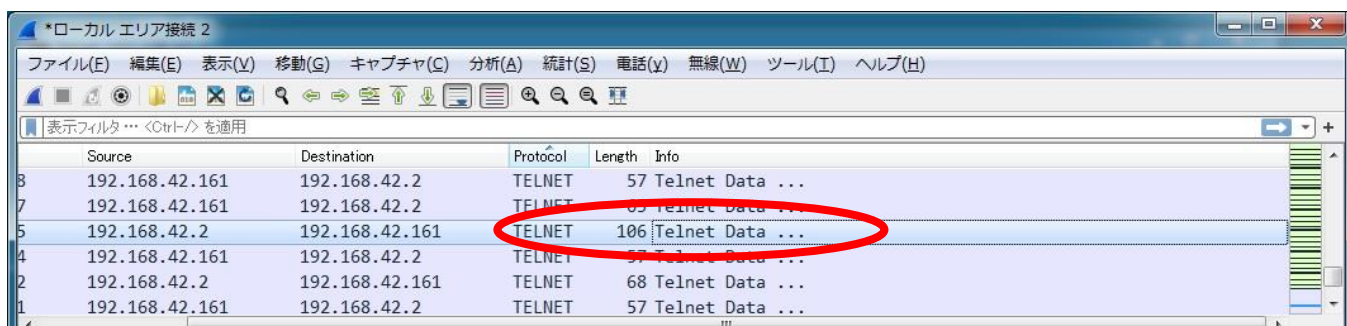
**Telnet は通信内容の暗号化をしません！！(超重要！！)** ←つまり、**内容が丸見え！！**

## ①「Wireshark」を用いて本格的なパケットのキャプチャ(盗聴?)を行きましょう！



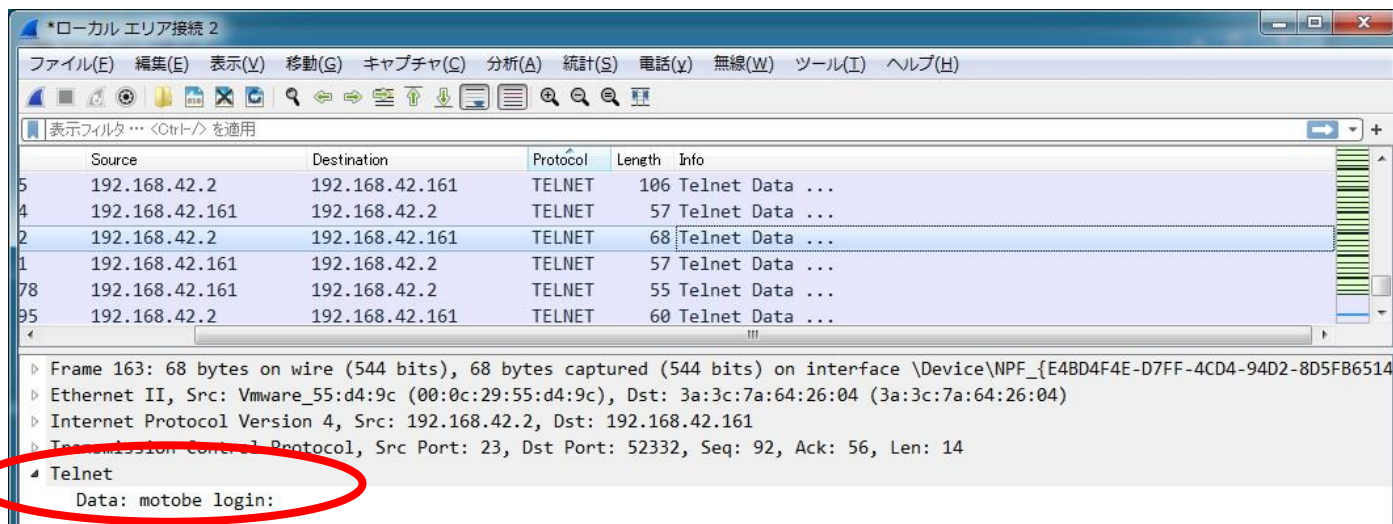
メニュー「ファイル」の下にある赤い四角(停止)を選択

停止後 → 「Protocol 別に並び替え」 または 「表示フィルタ欄に **Telnet** と入力」



	Source	Destination	Protocol	Length	Info
8	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
7	192.168.42.161	192.168.42.2	TELNET	55	Telnet Data ...
5	192.168.42.2	192.168.42.161	TELNET	106	Telnet Data ...
4	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
2	192.168.42.2	192.168.42.161	TELNET	68	Telnet Data ...
1	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...

「Telnet Data」内の「Telnet」をクリックして中身を確認(盗聴)



	Source	Destination	Protocol	Length	Info
5	192.168.42.2	192.168.42.161	TELNET	106	Telnet Data ...
4	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
2	192.168.42.2	192.168.42.161	TELNET	68	Telnet Data ...
1	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
78	192.168.42.161	192.168.42.2	TELNET	55	Telnet Data ...
95	192.168.42.2	192.168.42.161	TELNET	60	Telnet Data ...

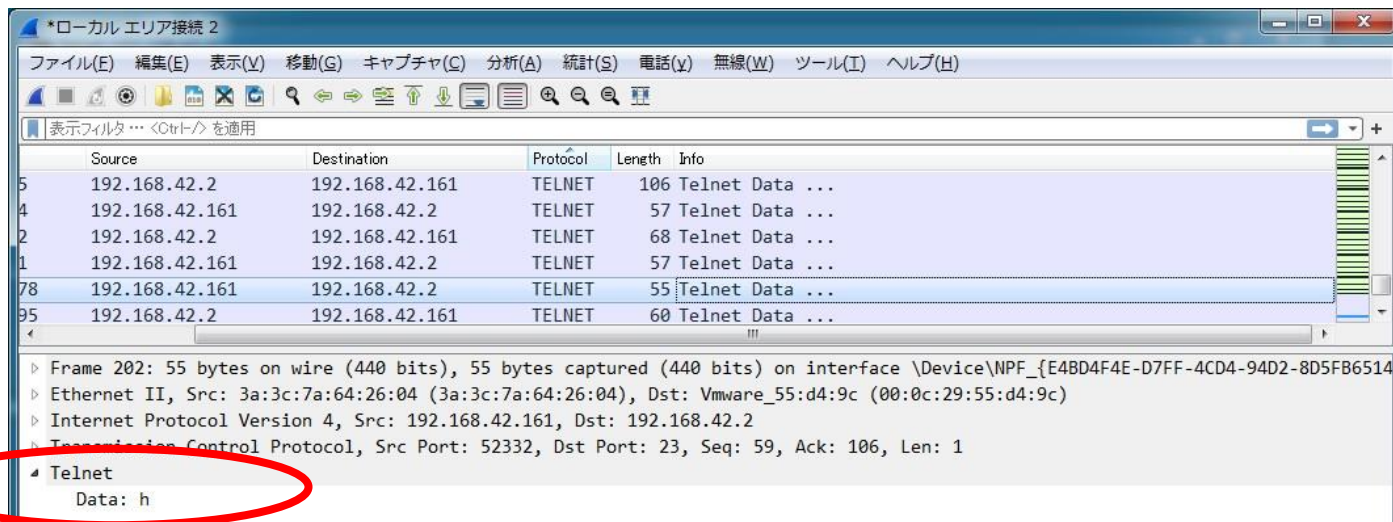
▶ Frame 163: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF\_{E4BD4F4E-D7FF-4CD4-94D2-8D5FB6514}

▶ Ethernet II, Src: Vmware\_55:d4:9c (00:0c:29:55:d4:9c), Dst: 3a:3c:7a:64:26:04 (3a:3c:7a:64:26:04)

▶ Internet Protocol Version 4, Src: 192.168.42.2, Dst: 192.168.42.161

▶ Transmission Control Protocol, Src Port: 23, Dst Port: 52332, Seq: 92, Ack: 56, Len: 14

▶ Telnet  
 Data: motobe login:



	Source	Destination	Protocol	Length	Info
5	192.168.42.2	192.168.42.161	TELNET	106	Telnet Data ...
4	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
2	192.168.42.2	192.168.42.161	TELNET	68	Telnet Data ...
1	192.168.42.161	192.168.42.2	TELNET	57	Telnet Data ...
78	192.168.42.161	192.168.42.2	TELNET	55	Telnet Data ...
95	192.168.42.2	192.168.42.161	TELNET	60	Telnet Data ...

▶ Frame 202: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF\_{E4BD4F4E-D7FF-4CD4-94D2-8D5FB6514}

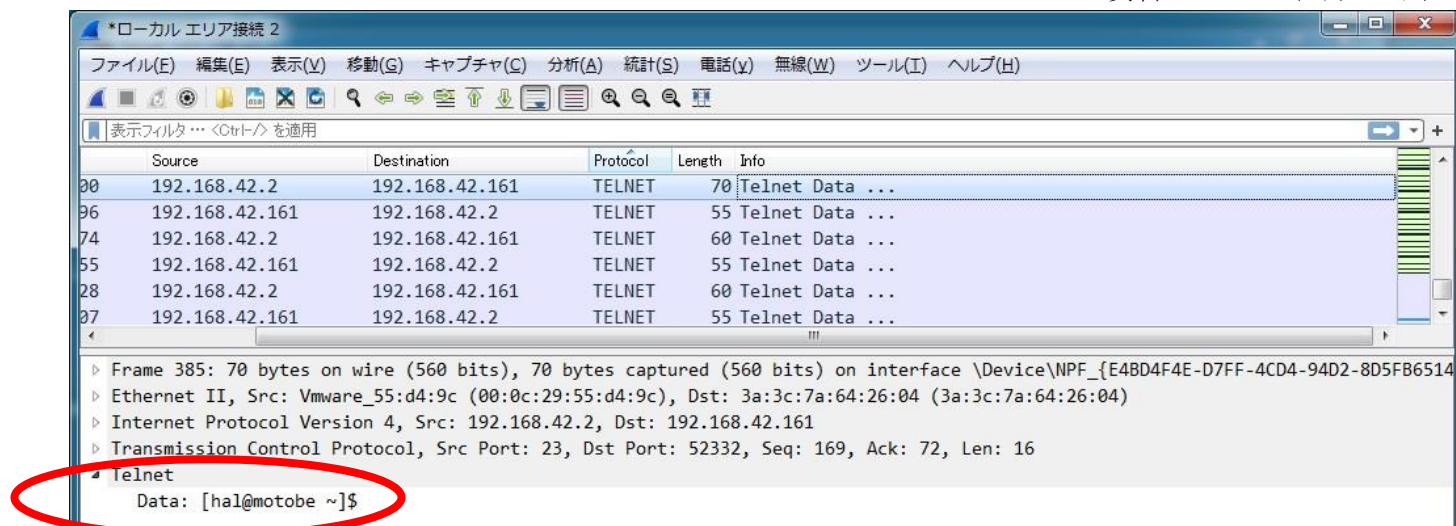
▶ Ethernet II, Src: 3a:3c:7a:64:26:04 (3a:3c:7a:64:26:04), Dst: Vmware\_55:d4:9c (00:0c:29:55:d4:9c)

▶ Internet Protocol Version 4, Src: 192.168.42.161, Dst: 192.168.42.2

▶ Transmission Control Protocol, Src Port: 52332, Dst Port: 23, Seq: 59, Ack: 106, Len: 1

▶ Telnet  
 Data: h





※見ての通り、通信内容がマル見え！

では安全な通信はないの？ → 暗号化して安全な通信を行う **SSH** や **VPN** 等があります！

以上！