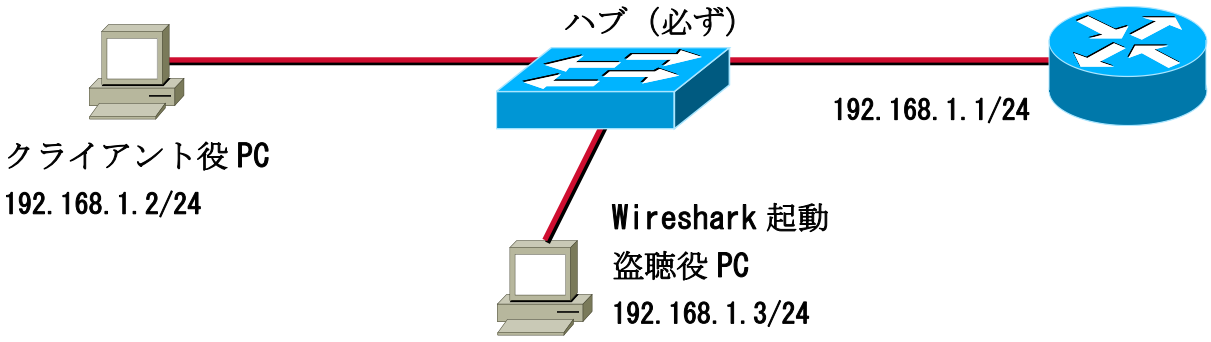
セキュリティ通信(SSH)

Linux の時間に学習しましたが Telnet はプレーンテキスト(平文)でデータ送信を行います。その為にスニッファ(盗聴)を行われると全ての通信が丸見えとなります！今回は危険な Telnet と安全な SSH の実習をします。

※課題 No.09 あり ！

① 以下の配線をして下さい(クライアント PC と盗聴 PC の共有も可)



※残念ながら、シュミレーション(Cisco Packet Tracer)では出来無いので確認だけ・・・

② 2 台の PC 間で ping が飛ぶことを確認

③ 盗聴 PC で Wireshark を起動して ping のキャプチャー

※ プロトコルが ICMP であることを確認

④ クライアント PC からルータへ Telnet アクセス

⑤ 盗聴 PC で Wireshark 停止。Wireshark のログを確認して、ユーザ名とパスワードか平文で流れていることの確認♪

※telnet はとても有名ですが実務で使用するのはとても危険です！ただ LAN 内でしたら使用されることも多いです。

・・・では安全な通信は無いの？
→“SSH” (Cisco、Linux、Windows)や“SDM(Cisco)”、“リモートデスクトップ(Windows)”、“VNC(Linux、Windows)”が有ります。

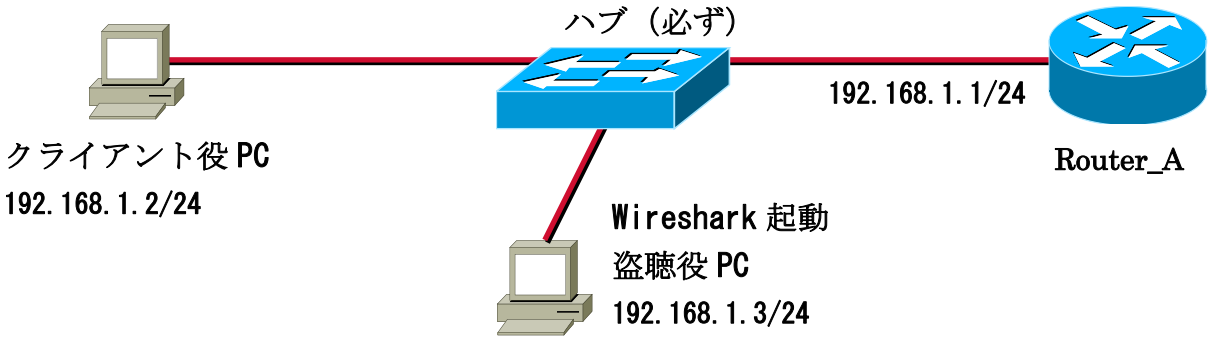
[1]SSH で接続する

SSH（セキュアシェル）は、ネットワークデバイスへセキュアなターミナルエミュレーション接続を確立するために使用されるプロトコルです。SSH を使用してルータを管理することができます。

Telnet では、クライアントとサーバ間の認証や暗号化を行うことができません。つまり、ネットワーク上に流れるトラフィックをスニファを使用することで傍受されてしまう恐れがあります。SSH は、Telnet と同様に TCP/IP ベースのプロトコルで、セキュアな接続ができることから、Telnet に取って代りつつあります。

ここでは、ルータに SSH 接続を行う方法を紹介してゆきます。PC とルータとの接続は、下の図のようにします。

(クライアント PC と盗聴 PC の共有も可)



●IP アドレスを割り当てる

PC とルータが通信できるようにルータの Fa0(または Fa8)インタフェースに IP アドレスを割り当てる必要があります。

ここでは、ドメイン名は、適当に「hal.com」にしています。

Router(config)#hostname Router_A ←必ずルータ名を変更。デフォルトの名前(Router)ではエラーが出る

Router_A(config)#ip domain-name hal.com

Router_A(config)#interface f0
Router_A(config-if)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#no shutdown
Router_A(config-if)#exit

●ユーザアカウントを作成するユーザ名「ccna」、パスワード「osaka」でユーザアカウントを作成。

Router_A(config)#username ccna password osaka

Router_A(config)#line vty 0 4
Router_A(config-line)#login local
Router_A(config-line)#transport input telnet ssh
Router_A(config-line)#exit
RouterA(config)#ip ssh version 2 ←SSH のバージョン 2 に設定(初期はバージョン 1)

●ルータの RSA 暗号キーペアを生成する

デフォルトの暗号キーの数値は、512 ビットです。ここでは、1024 ビットで生成します。

```
Router_A(config)#crypto key generate rsa

The name for the keys will be: Router_A.ccna.com
Choose the size of the key modulus in the range of 360 to 2048 for your
```

```
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router_A(config)#
```

●show ip ssh

SSH が有効で、どのバージョンが使用されているかを確認するには、「show ip ssh」コマンドを使用します。

```
Router_A#show ip ssh
SSH Enabled - version 2.09
Authentication timeout: 120 secs; Authentication retries: 3
```

●盗聴 PC で Wireshark を起動

※SSH のアクセス確認の前に Wireshark を起動しておくこと。

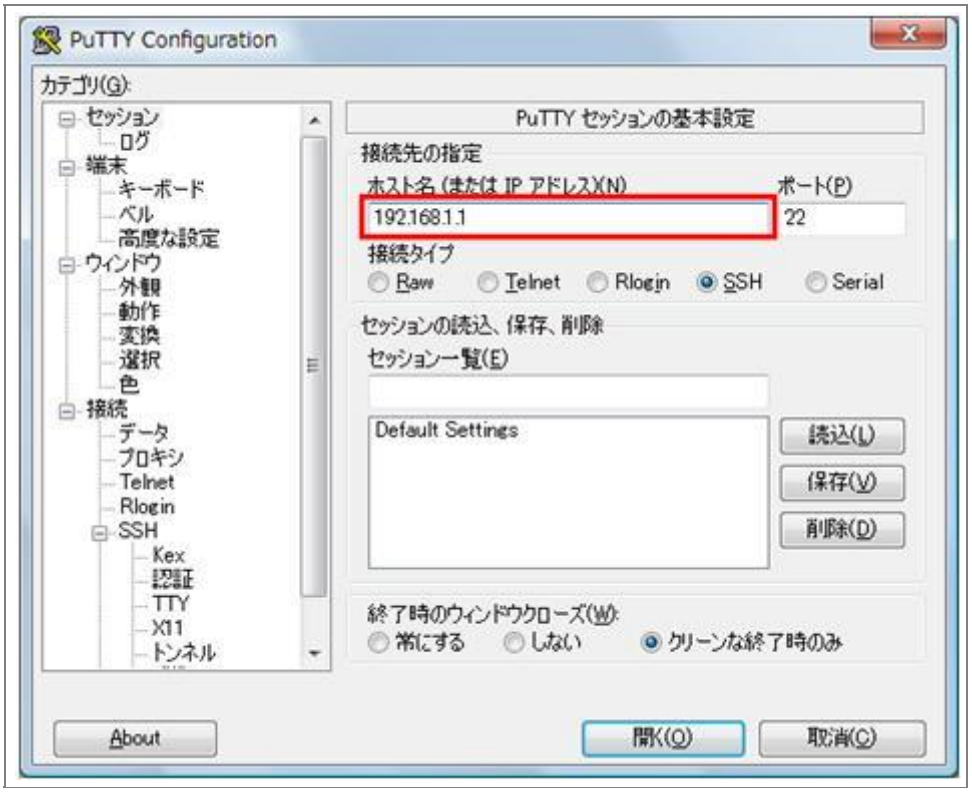
※残念ながら、シュミレーション(Cisco Packet Tracer)では出来無いので確認だけ・・・

[2]パケットをキャプチャーして、暗号化されていることを確認

①PuTTY を使用してルータに SSH アクセス　　←Linux でやりましたね

SSH をクリックし、「優先する SSH のプロトコルバージョン」に「2」をしています。SSH サーバの SSH のバージョンが 1 の場合でも、PuTTY クライアントでは、接続できるようになっています。

IP アドレスに、「192.168.1.1」を入力し、「開く」を押します。



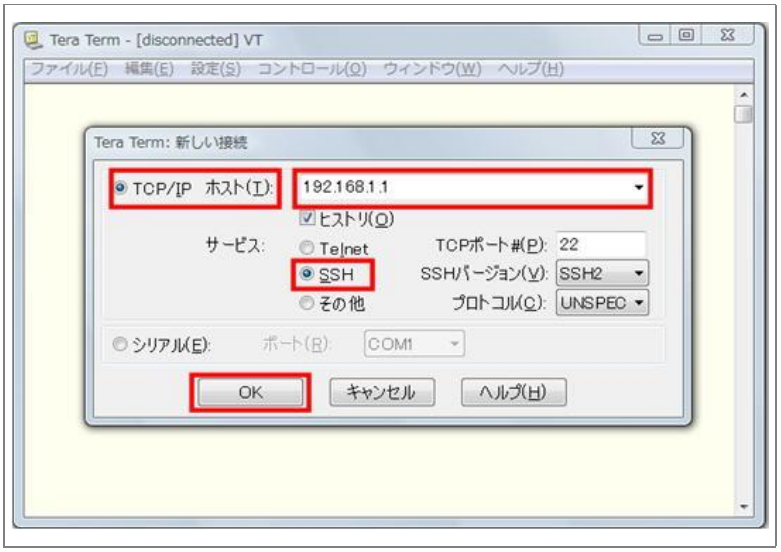
ログインプロンプトで、ユーザ名に「ccna」、パスワードに「osaka」を入力してログインします。

ログイン後は、いつものようにターミナル操作を行うことができます。

このように Linux と同じく Cisco ルータやスイッチでは、簡単に SSH を使用した接続ができるようになっています。

② Tera Term を使用して SSH アクセス ←Tera Term は今回コンソールで使用中の為、使いません

「Tera Term」は、シリアルを経由したターミナル接続だけでなく、Telnet や SSH の接続もサポートしています。「TCP/IP ホスト」を選択し、宛先に「192.168.1.1」を、サービスに「SSH」を選択して「OK」ボタンをクリックします。



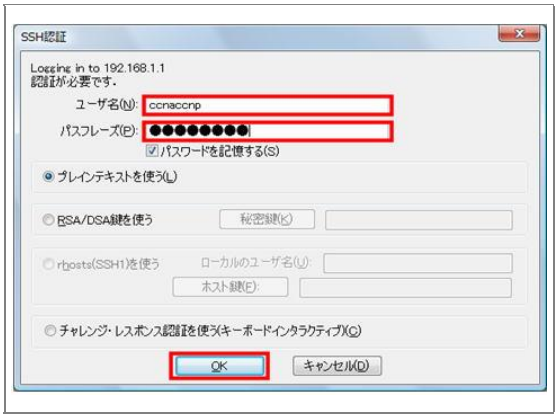
「セキュリティ警告」が表示されます。「続行」をクリックします。

「SSH 認証」では、以下のように入力します。

ユーザ名： ccna

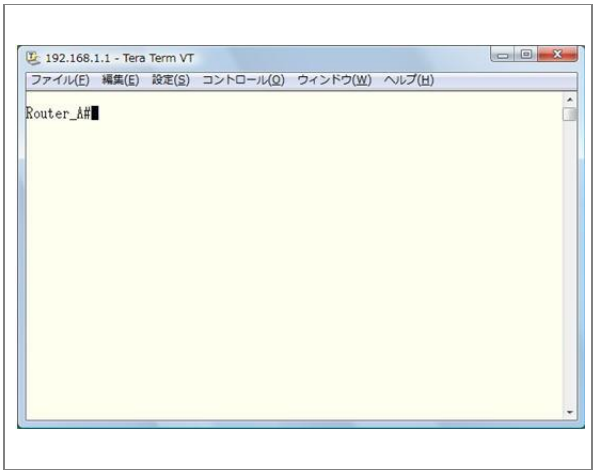
パスフレーズ： osaka

入力が終わったら、「OK」ボタンをクリックします。



※ユーザ名が ccnaccnp になっているのは気にしないで下さい

下のように、SSH での接続が確立されます。



③ MAC の方は　　←Linux でやりましたね

Terminal を開く

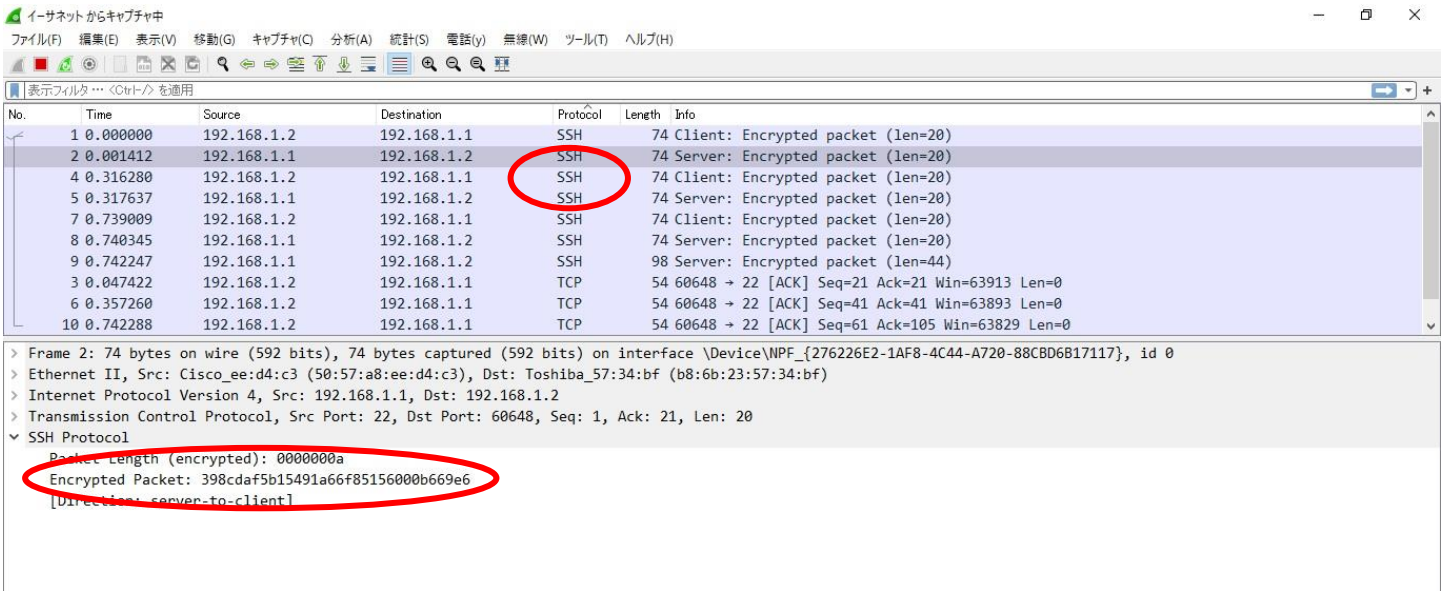
※Terminal は、「アプリケーションフォルダ」内の「ユーティリティフォルダ」にインストールされています。

ssh -l hal (Cisco の IP アドレス)

でアクセス出来ます

④ 暗号化の確認

Wireshark で暗号化されていることを確認して下さい！



[3] 課題 09

(1) NT43 Cisco 資料 05 静的ルーティングと動的ルーティング(RIP)(11 月 27 日)

NT43 Cisco 資料 06 Telnet と SSH(12 月 4 日)

←SSH の所のみ。Wireshark は出来ません

の NW を完成。

現在の設定の保存

```
motobe#copy  running-config  startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

(2) ルータ A の設定を以下に変更(ルータ B は変更しなくて構いません)

① ルータ名を「出席番号自分の名前」 ←(例)55Motobe
※ルータ A の名は必ず変更すること。変わっていない場合は未提出扱いとします！
② 「enable シークレット」を「kawata」
③ 「コンソールのパスワード」を「motobe」

(3)課題提出

以下のデータを課題提出サーバに提出 [motobe.shigekazu] → [NT43] → [01]

・Cisco Packet Tracer を「出席番号自分の名前.pkt」で保存提出 (例)55 元部重和.pkt

●課題 No.09

主題：「Cisco ルータ基本設定」

日付：12 月 11 日(深夜 12 時) 教員：元部 重和

※「出席番号自分の名前.pkt」を課題提出サーバ 01 に提出。

以上！