



# ホワイトハッカーの第一歩：

# Pythonでサーバへの侵入テストを試みる

## インターネット接続について

本セッションではインターネット上のサンプルサーバを利用します。

## ファイルのダウンロードについて

チュートリアル申し込みページからリンクを用意しました。

<https://www.mta.gr.jp/tutorial/index.html>

## 第42回医療情報学連合大会 チュートリアルB-1 日本Mテクノロジー学会主催

群馬大学医学部附属病院 システム統合センター

鳥飼 幸太

熊本大学病院 総合臨床研究部 研究データ管理センター

山ノ内 祥訓

トレンドマイクロ株式会社

松山 征嗣

オリンパス株式会社

鈴木 克明

東京大学医学部附属病院 企画情報運営部

土井 俊祐

# VPN接続のためのクライアントソフトのインストール

- VPN脆弱性攻撃のハンズオンのため、以下のソフトウェアのインストールをお願いいたします。
- FortiClientについて
  - ダウンロードリンク<https://www.fortinet.com/support/product-downloads#vpn>

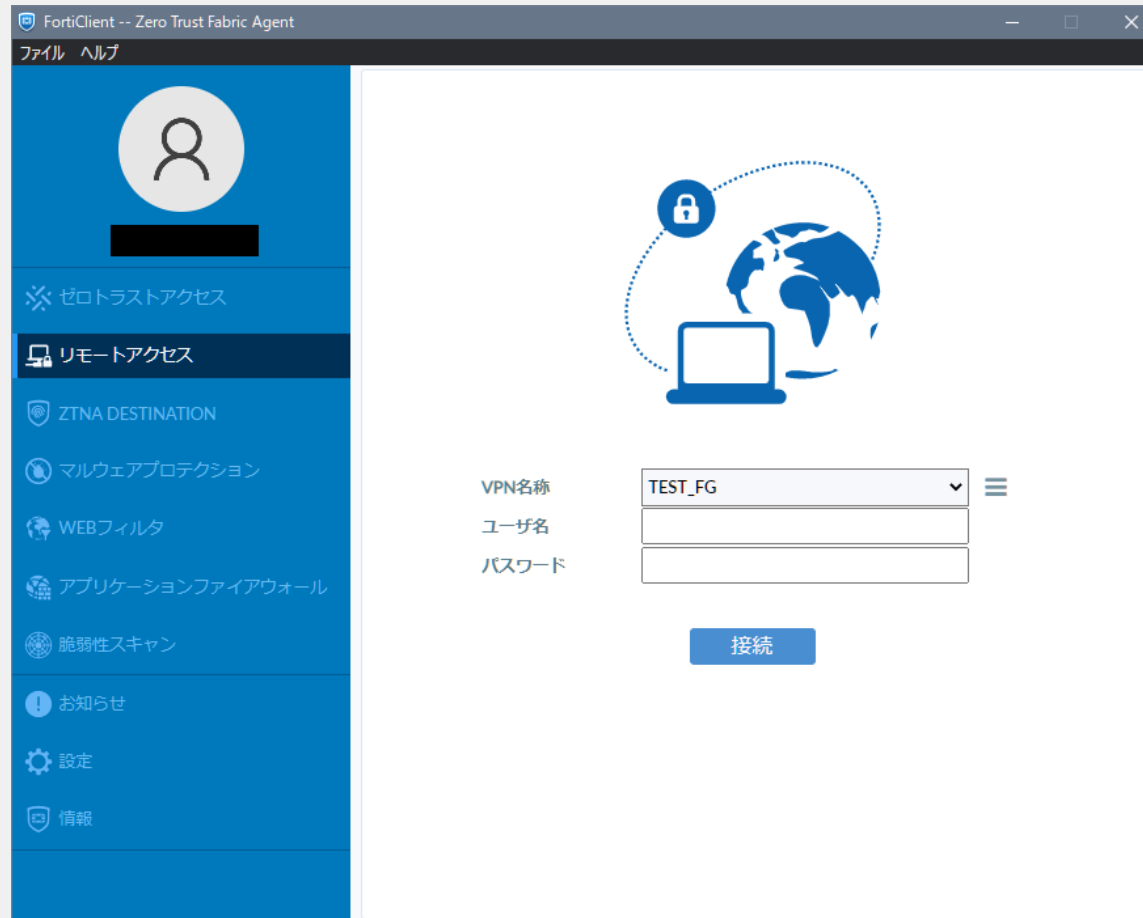
注意) “**FortiClient VPN**”の項目よりダウンロード下さい（こちらが無償版となります）



# VPN設定に接続について

- FortiClientのVPN設定(Windowsの場合)

- インストール後にFortiClientのコンソールを起動し、“リモートアクセス”を選択します。
- VPN名称の右側にある“≡”をクリックし、“新規接続の追加”を選択します。



# VPN設定に接続について

- FortiClientのVPN設定(Windowsの場合)
  - VPN接続を行う以下の情報を入力します。
    - 組織名：任意の文言を入力願います。  
(この例では“TEST-FG”)
    - リモートGW：  
接続先のFGのIP(10.0.0.254)を入力願います。
    - ポートの編集：チェックを入れます。
    - ポート番号：10443を入力します。
- 全て入力したら保存をクリックします。

The screenshot shows the FortiClient interface with the 'New VPN Connection' dialog box open. The dialog has three tabs: 'SSL-VPN', 'IPsec VPN', and 'XML'. The 'SSL-VPN' tab is selected. The following fields are highlighted with red boxes:

- 接続名**: TEST-FG
- リモートGW**: 10.0.0.254
- ポートの編集**:  (checked)
- ポート番号**: 10443

Other visible fields and options include:

- 説明**: (empty)
- クライアント証明書**: なし
- 認証**:  ユーザ名入力,  ユーザ名を保存
- VPNトンネルのシングルサインイン (SSO) を有効化
- IPv4/IPv6デュアルスタックアドレスを有効化

Buttons at the bottom: キャンセル, 保存



# VPN設定に接続について

- FortiClientのVPN設定(Windowsの場合)
- VPN名称に先ほど指定した

接続プロファイルを指定し、ユーザアカウントとパスワードを入力し、“接続”ボタンを押します。

画面右下のFortiClientアイコンに、  
鍵マークがつくとVPN接続状態となります。



※初回接続時は証明書エラーが出力されますが  
接続可能です。

(ビルドインの証明書を使っているためです)

