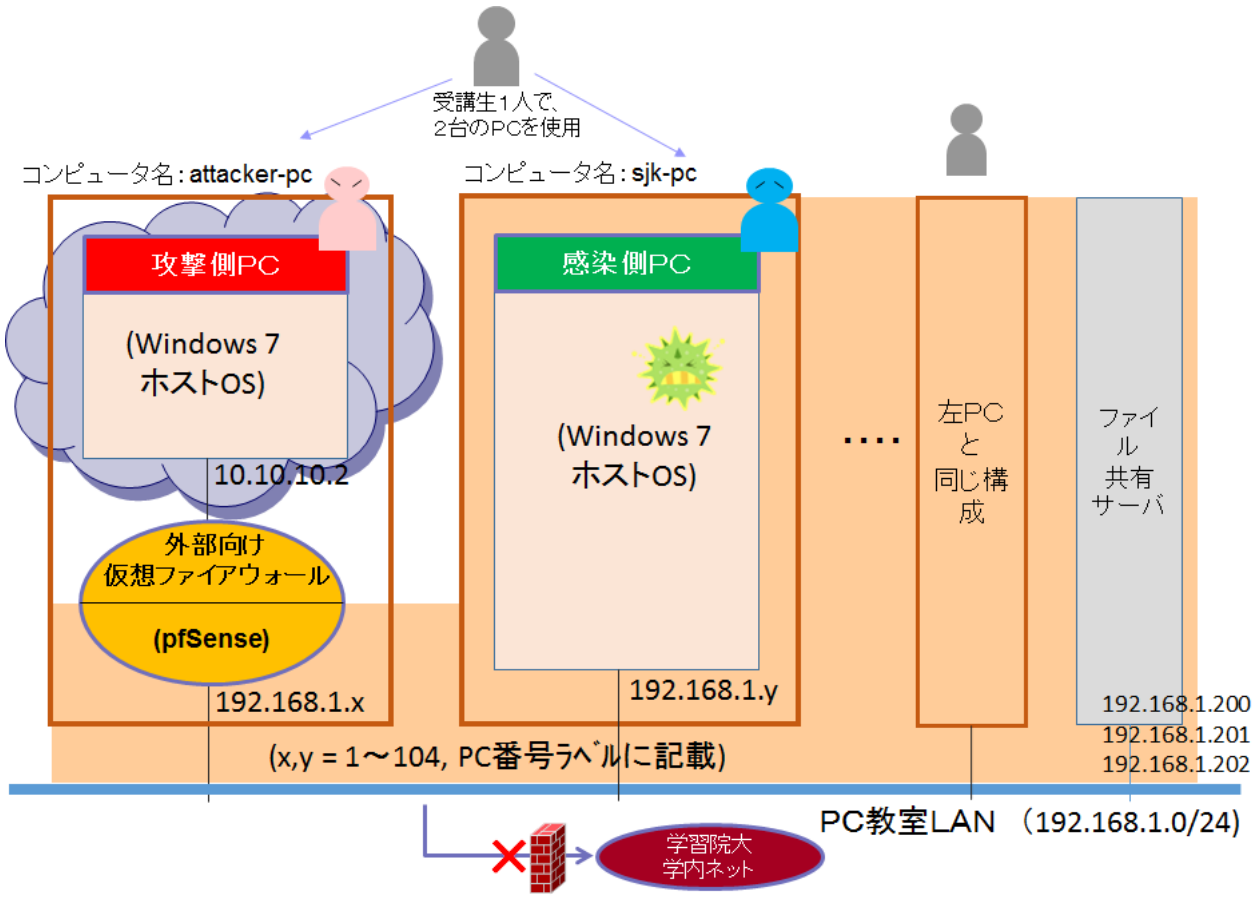
A-2「標的型攻撃を受けているらしいとの連絡があった時の調査と対応の演習」

実習環境について

- ■ 攻撃側 PC（attacker-pc）と感染側 PC（sjk-pc）の 2 台の PC を使用します。
- ■ 攻撃側 PC（attacker-pc）から感染側 PC（sjk-pc）操作してみましょう。



実習の進め方

【実習１】初期潜入
・感染側 PC を RAT に感染させましょう。
・攻撃側 PC から感染側 PC をリモート操作しましょう。

【実習２】基盤構築
・攻撃側 PC からのリモート操作で、感染側 PC に内部調査ツール（nmap）をインストールしましょう。

【実習３】内部侵入・調査
・攻撃側 PC からのリモート操作で nmap を実行し、感染側 PC の内部ネットワークの調査を実施しましょう。

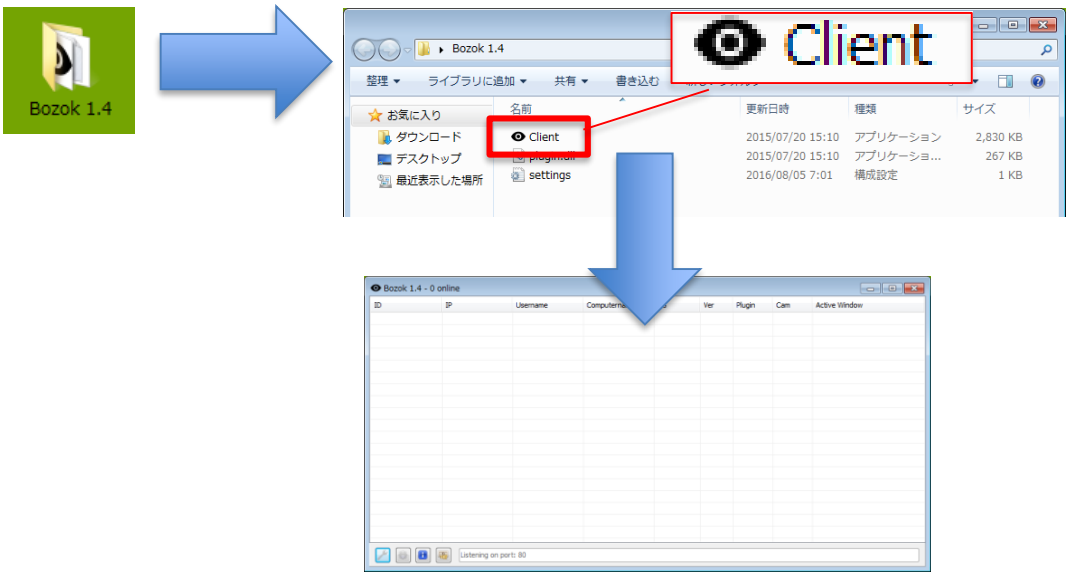
~~【実習４】撤収~~
~~・攻撃側 PC からのリモート操作で、感染側 PC で動いている RAT を停止しましょう。~~

配布資料訂正

【実習 1】初期潜入

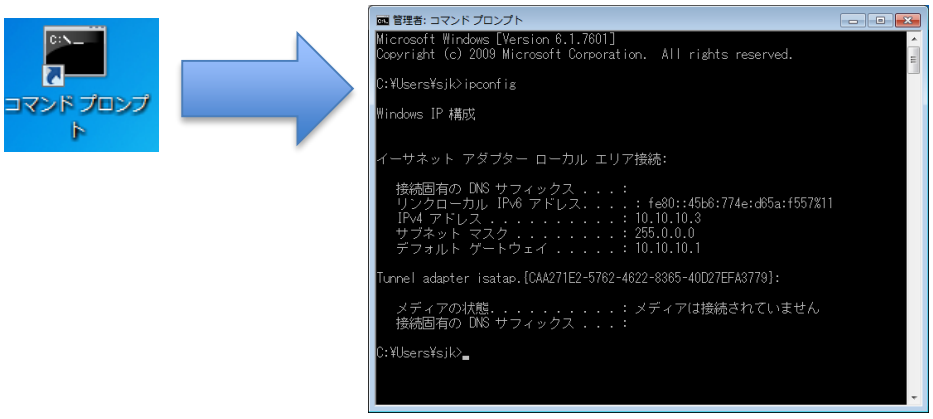
攻撃側 PC 操作

1. RAT コントローラーの起動
   攻撃側 PC のデスクトップにある“Bozok 1.4”を開き、中にある“Client.exe”をダブルクリックして起動します。”Bozok 1.4 – 0 Online”のウィンドが開くが、何も表示されないことを確認します。



感染側 PC 操作

2. 感染側 PC のデスクトップにあるコマンドプロンプトのショートカットを使ってコマンドプロンプトを開きます。コマンドプロンプトの画面が表示されたら、”**ipconfig**”コマンドを使って感染側 PC のネットワーク設定を確認しましょう。

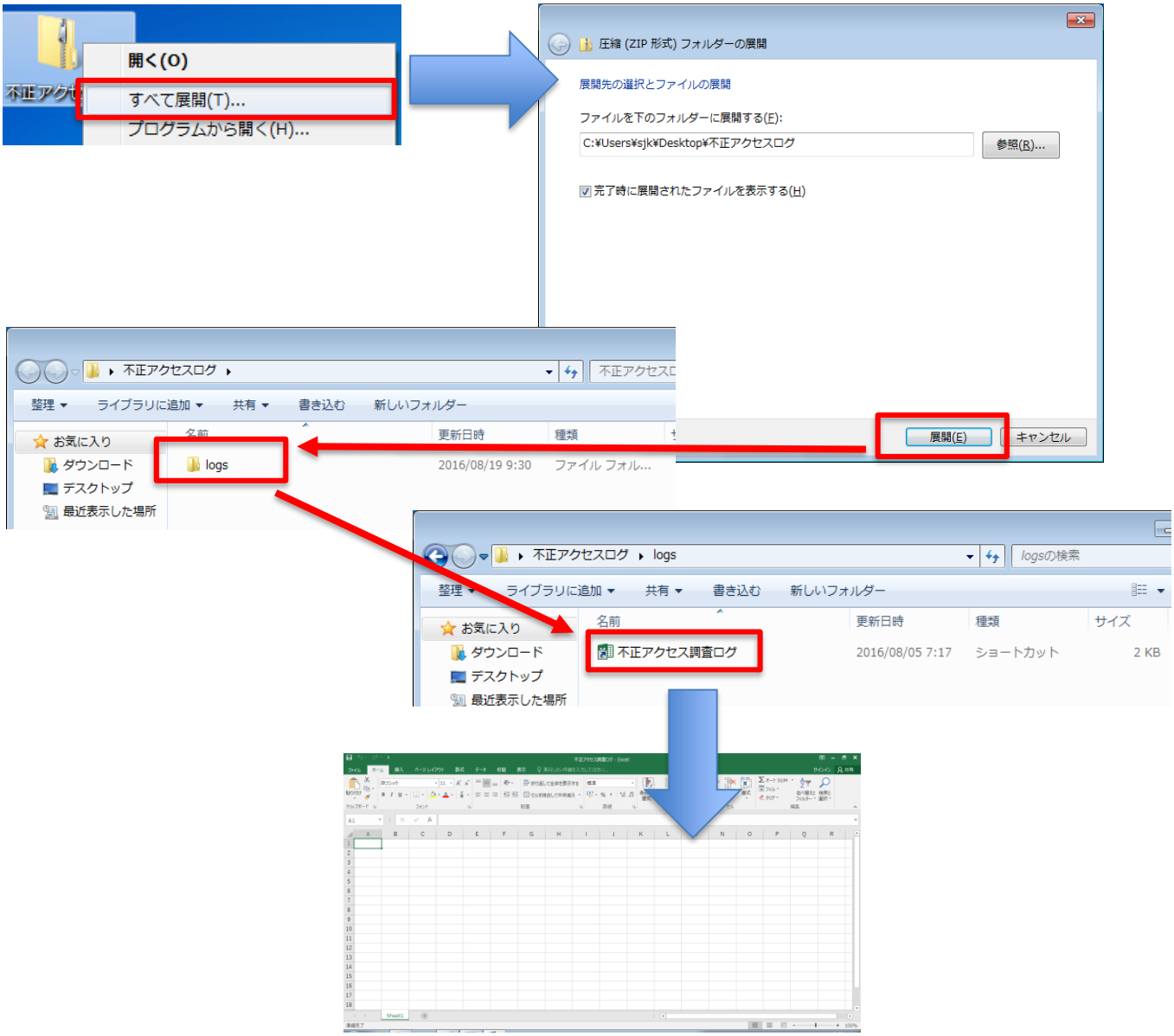


■ 演習 1　感染側 PC のネットワーク設定を記録しましょう。(ipconfig コマンドを使用)

IP アドレス	（例）192.168.1.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	（例）192.168.1.1

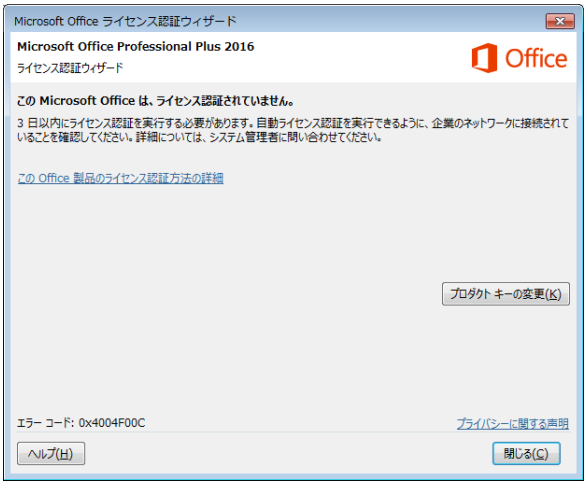
3. RAT に感染

感染側 PC のデスクトップにある“不正アクセスログ.zip”を解凍します。解凍されたフォルダにある”logs”フォルダを開いて、”**不正アクセス調査ログ.xlsx**“をダブルクリックします。空の Excel が開くことを確認します。



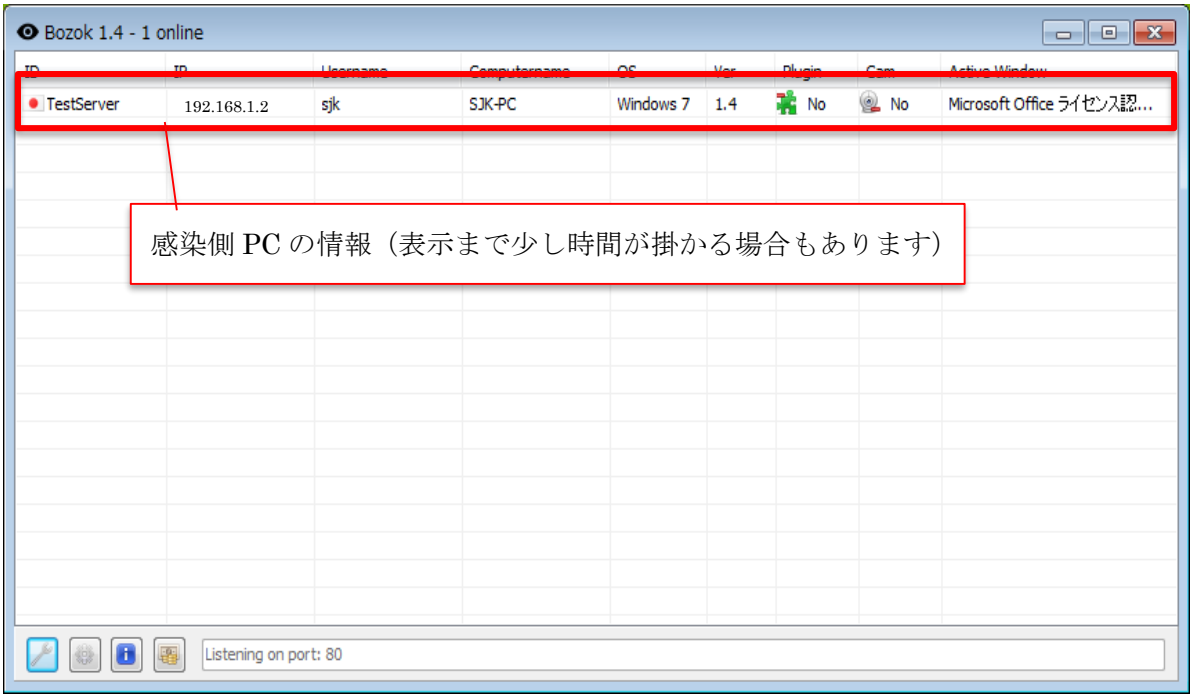
（補足）

右の様に“Microsoft Office ライセンス認証ウィザード”が表示された場合は、”**閉じる(C)**“を押してして終了してください。



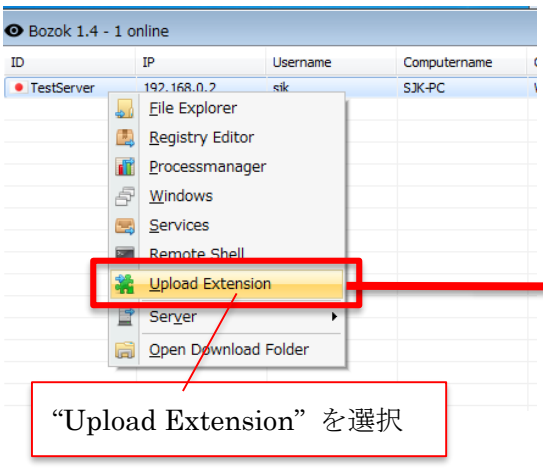
攻撃側 PC 操作

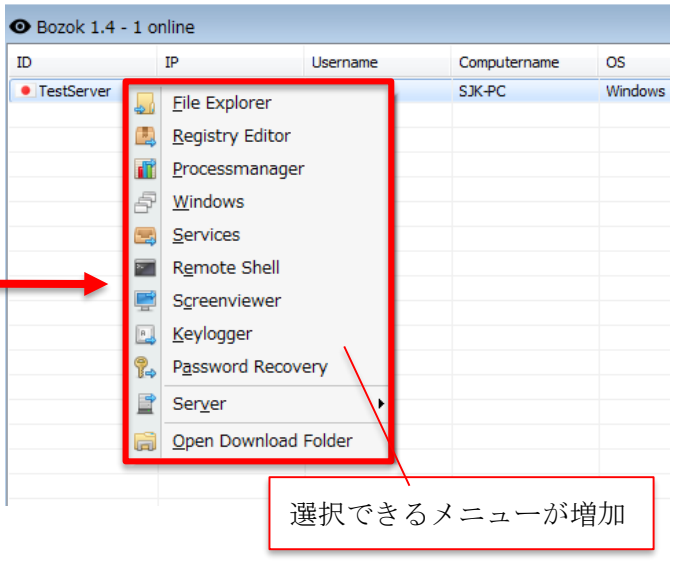
4. RAT コントローラーの感染側 PC の補足
RAT コントローラーに感染側 PC の情報が表示されます。演習 1 で記録した IP アドレスが表示されていることを確認しましょう。



感染側 PC を補足することができたら、攻撃側 PC から様々な操作を RAT コントローラー経由で実行できます。RAT コントローラーの設定をした後、4 つの攻撃操作を行いましょう。

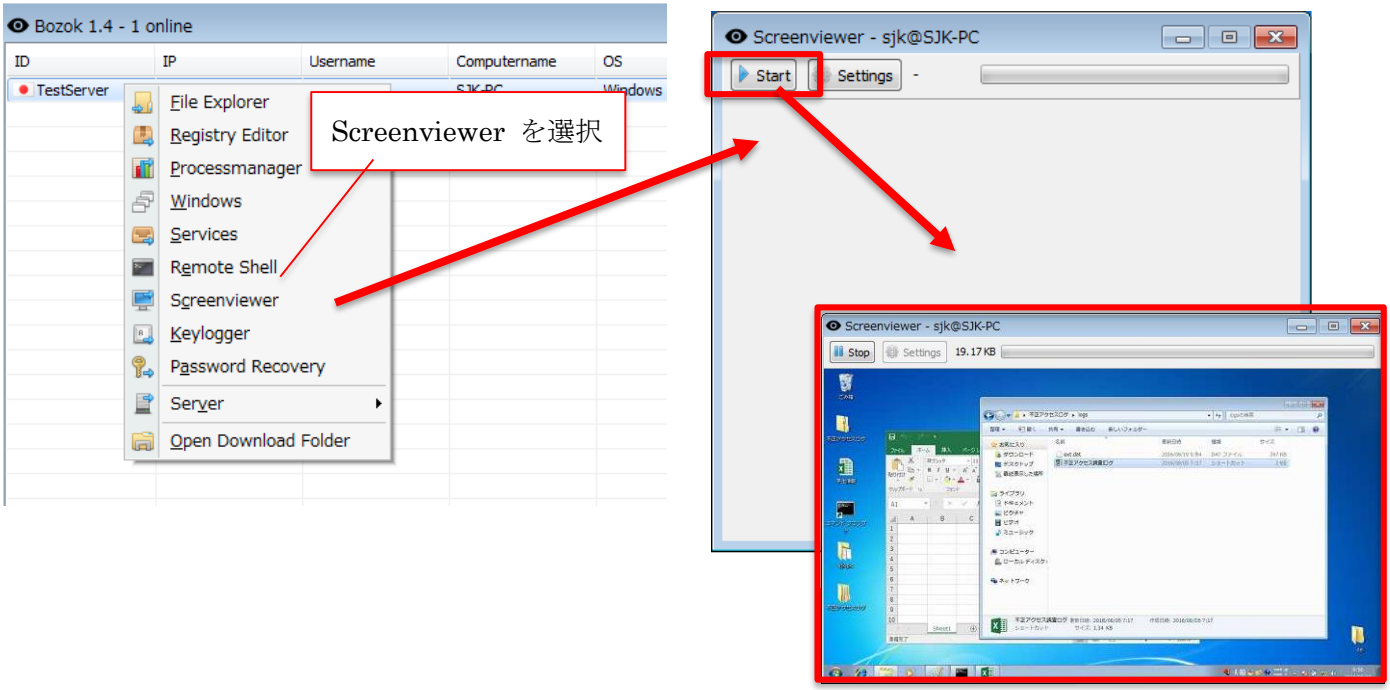
5. RAT コントローラーの設定
感染側 PC を選択し、右クリックで表示されるメニューから ”Upload Extension” を選択します。再度右クリックでメニューを表示すると、内容が増えていることがわかります。





≪攻撃操作１≫ 感染側 PC のデスクトップ画面をモニターする

1. Screenviewer の起動
   感染側 PC を選択し、右クリックメニューから “Screenviewer” を選択し起動します。[Start] を押すことで、感染側 PC のモニターが開始されます。モニターを終了する場合は [Stop] を押します。

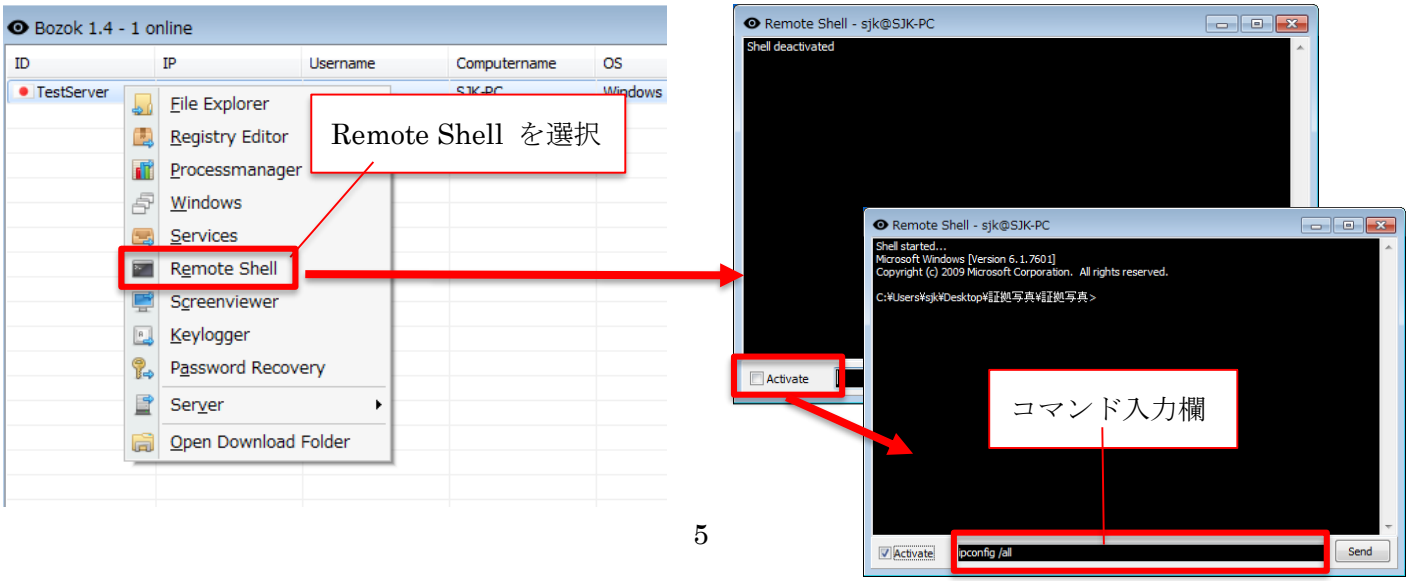


■ 演習２　感染側 PC の画面をモニターできましたか？

画面モニター可否	可	・	否

≪攻撃操作２≫ 感染側 PC のネットワーク情報、及びシステム情報を窃取する

1. Remote Shell の起動
   感染側 PC を選択し、右クリックメニューから “Remote Shell” を選択し起動します。**[Activate] にチェックを入れることで**、感染側 PC のコマンドプロンプトを起動した状態と同じになります。コマンド入力欄にコマンドを入力し、[Send] を押すことで画面に結果が返ってきます。



■ 演習３　感染側 PC のネットワーク情報を調べましょう。（ipconfig コマンドを使用）

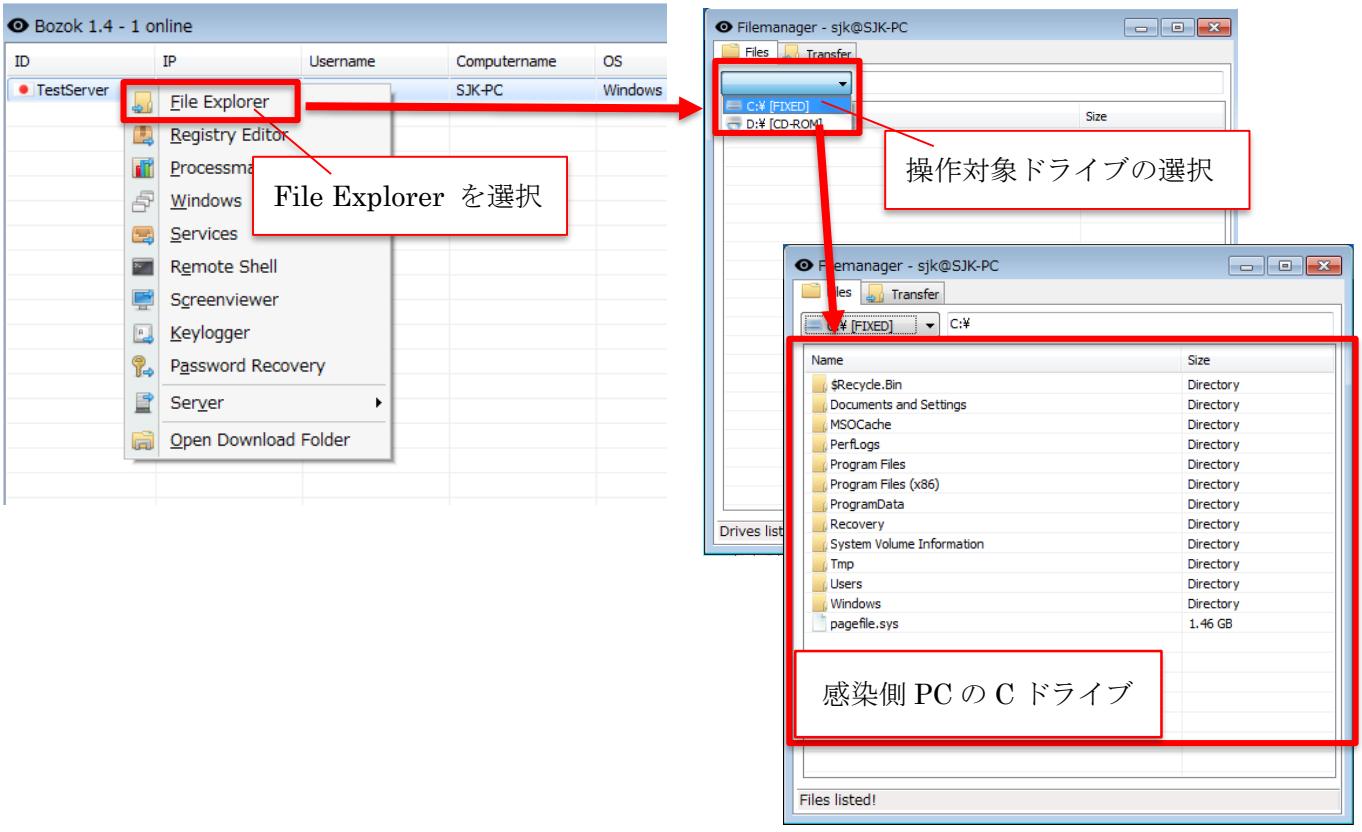
IP アドレス	（例）192.168.1.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	（例）192.168.1.1

■ 演習４　感染側 PC のシステム情報を調べましょう。（systeminfo コマンドを使用）

ホスト名	SJK-PC
OS 名	Microsoft Windows 7 Enterprise
登録されている所有者	sjk
システムモデル	20AUA1NLJP

≪攻撃操作３≫ 感染側 PC に対してファイルのダウンロード（窃取）を実行してみる

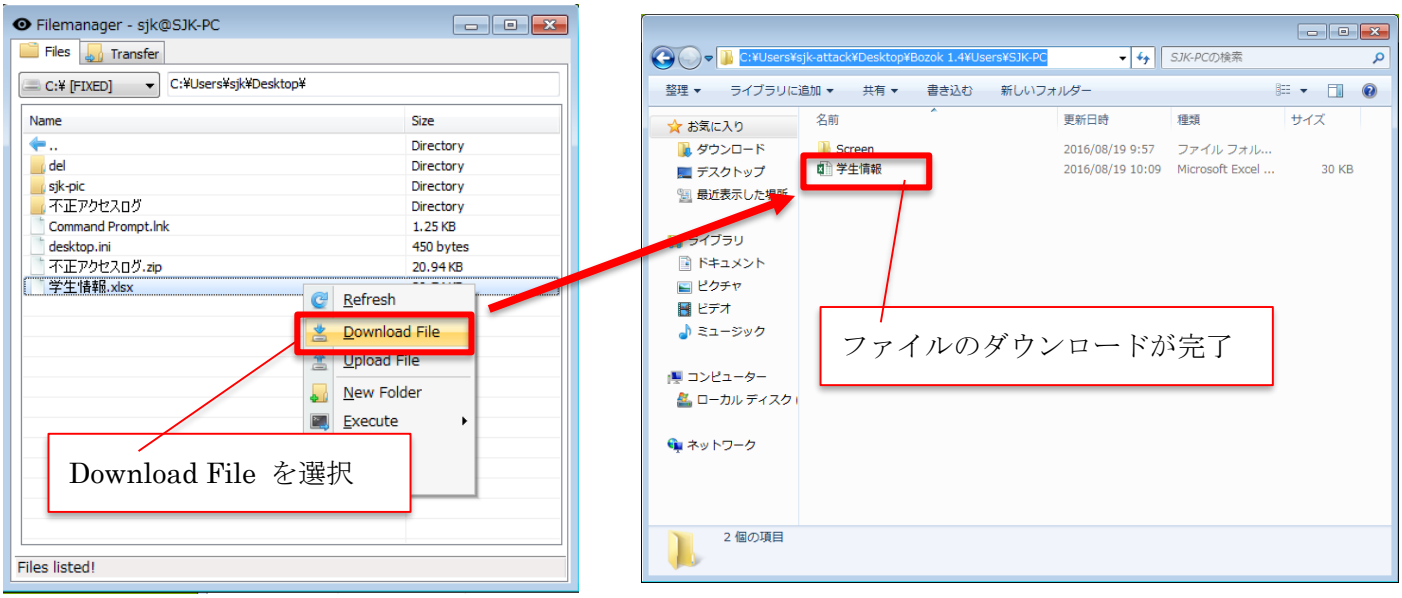
1. File Explorer の起動
   感染側 PC を選択し、右クリックメニューから “File Explorer” を選択し起動します。対象ドライブから “C:¥[FIXED]” を選択することで、感染側 PC の C ドライブの情報が表示されます。



2. 感染側 PC 内のファイル窃取

感染側 PC の C ドライブ情報が表示されたら、後はフォルダをクリックしていけばそれぞれの中を確認することができます。ここでは [Users]-[sjk]-[Desktop] フォルダ内にある“ **学生情報.xlsx** ”ファイルを攻撃側 PC にダウンロードします。

対象のファイルを選択し、右クリックメニューから［Download File］を選択するだけで、攻撃側 PC のデスクトップにある [Bozok 1.4]-[Users]-[SJK-PC] 内にファイルがダウンロードされます。



■ 演習５　ファイル窃取は成功しましたか？

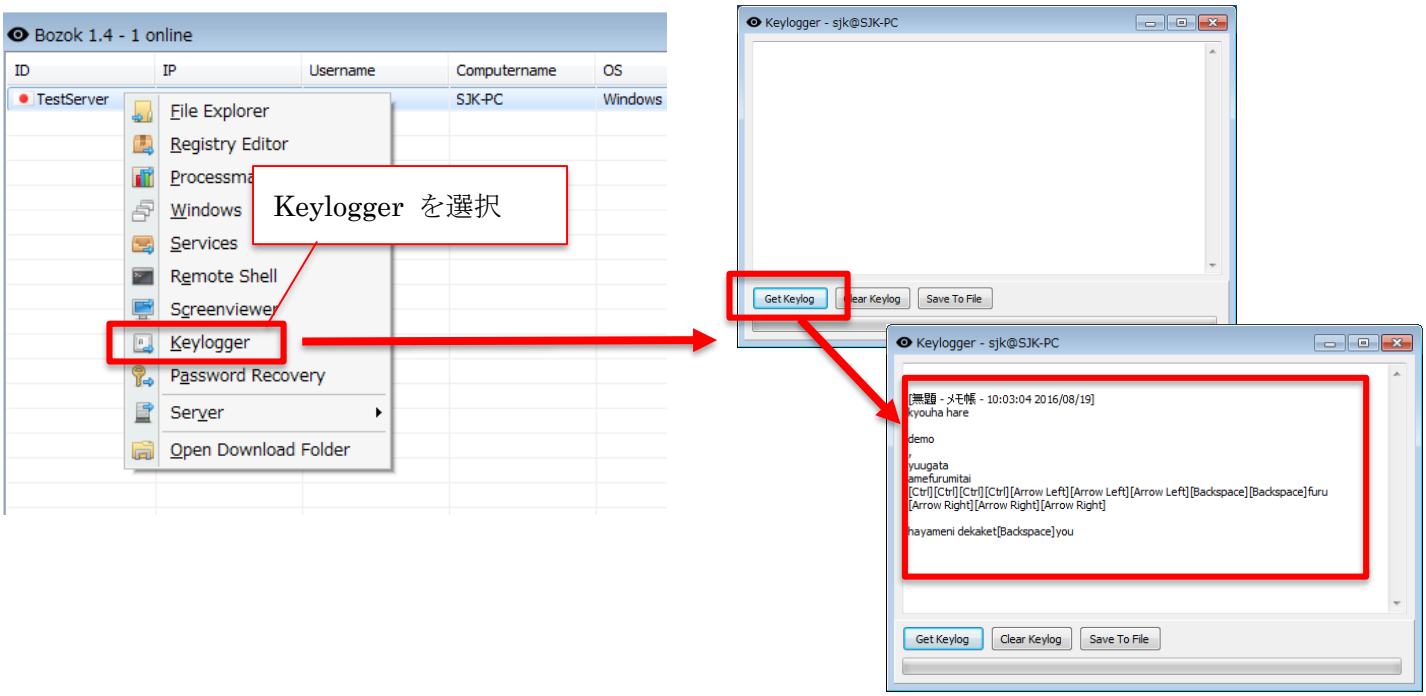
ファイル窃取	成功	・	失敗

■ 演習６　窃取したファイルにはどんな情報がありましたか？

窃取した情報	学生の個人情報 氏名、電話番号、メールアドレス、住所

≪攻撃操作４≫ 感染側 PC のキー入力情報を窃取する

1. Keylogger の起動
   感染側 PC を選択し、右クリックメニューから “Keylogger” を選択し起動します。[Get Keylog] を押すことで、RAT 起動後に感染側 PC で入力されたキー情報が表示されます。



■ 演習７　キー入力情報の窃取は成功しましたか？

キー入力情報窃取	成功	・	失敗

【実習２】基盤構築

攻撃側 PC 操作

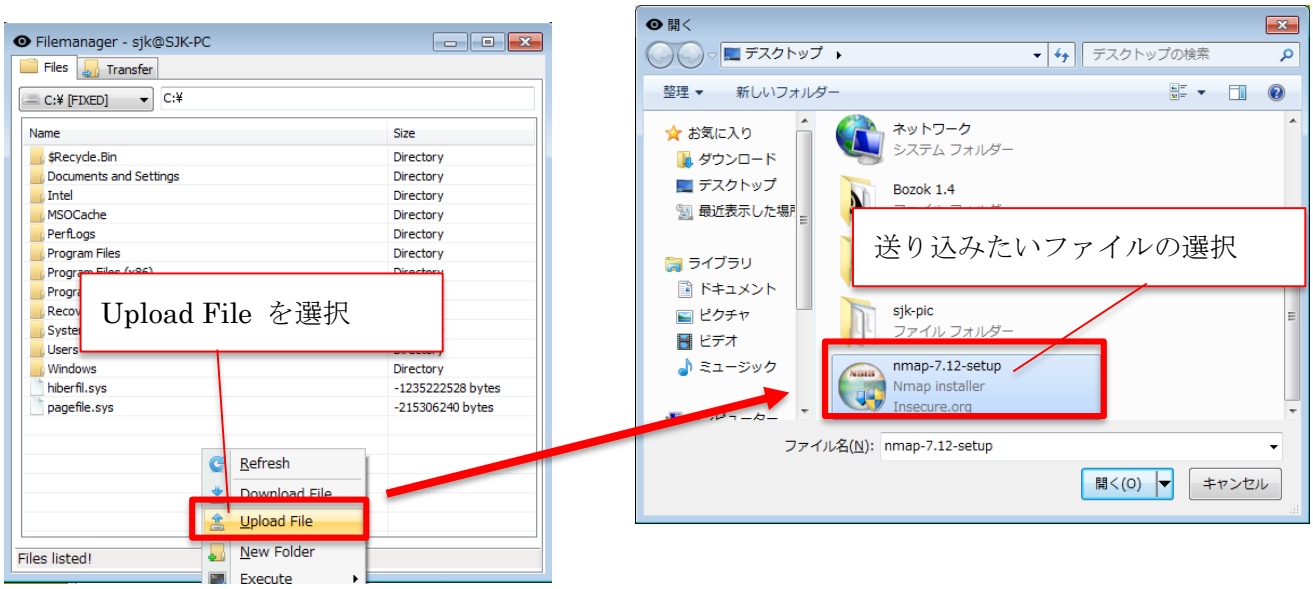
1. 感染側 PC のコマンド確認
   感染側 PC を選択し、右クリックメニューから “Remote Shell” を選択し起動します。[Activate] にチェックを入れた後コマンド入力欄に ”**nmap**“ と入力し、[Send] を押します。

■ 演習８　感染側 PC に nmap コマンドはありましたか？

nmap の有無	有	・	無

2. 感染側 PC への nmap インストールファイルの混入
   感染側 PC に nmap インストールファイルを混入させます。攻撃側 PC のデスクトップ（[Users]-[sjk]-[Desktop]）にある “**nmap-7.12-setup.exe**“ を感染側 PC の C ドライブ直下に送り込みます。”File Explorer” で感染側 PC の C ドライブ直下に移動します。画面中ファイル名が表示されていない場所で右クリックメニューから [Upload File] を選択し、感染側 PC に送り込みたいファイル

（“ nmap-7.12-setup.exe “）を選択します。



3. 感染側 PC への nmap インストール

感染側 PC を選択し、右クリックメニューから “Remote Shell” を選択し起動します。[Activate] にチェックを入れた後、初めに感染側 PC の C ドライブ直下に移動するために、コマンド入力欄に ” **cd c:¥** “ と入力し、[Send] を押します。

次に “ nmap-7.12-setup.exe “ が感染側 PC の C ドライブ直下に混入されたことを確認するために、コマンド入力欄に “ **dir** “ と入力し、[Send] を押します。“ nmap-7.12-setup.exe “ があることを確認します。

最後にコマンド入力欄に “ **nmap-7.12-setup.exe /S** “ と入力し、[Send] を押します。

4. 感染側 PC のコマンド確認

“Remote Shell” のコマンド入力欄に ” **nmap** “ と入力し、[Send] を押します。

■ 演習９　感染側 PC に nmap コマンドはありましたか？

nmap の有無	有	・	無

【実習３】内部侵入・調査

攻撃側 PC 操作

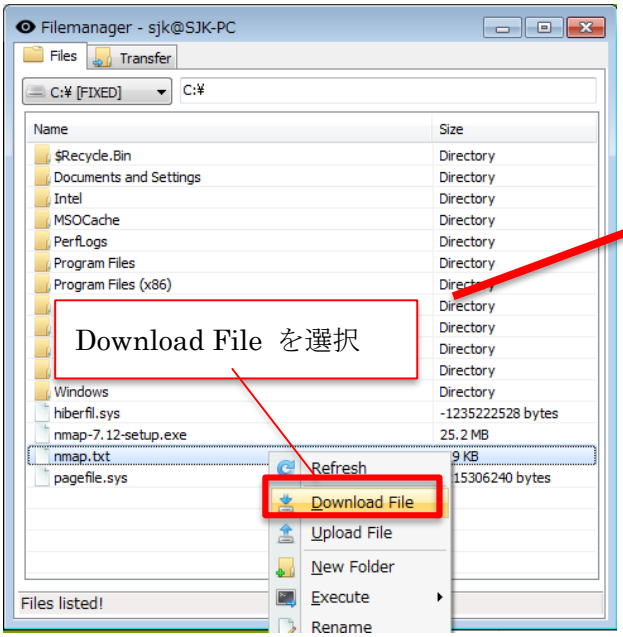
配布資料訂正

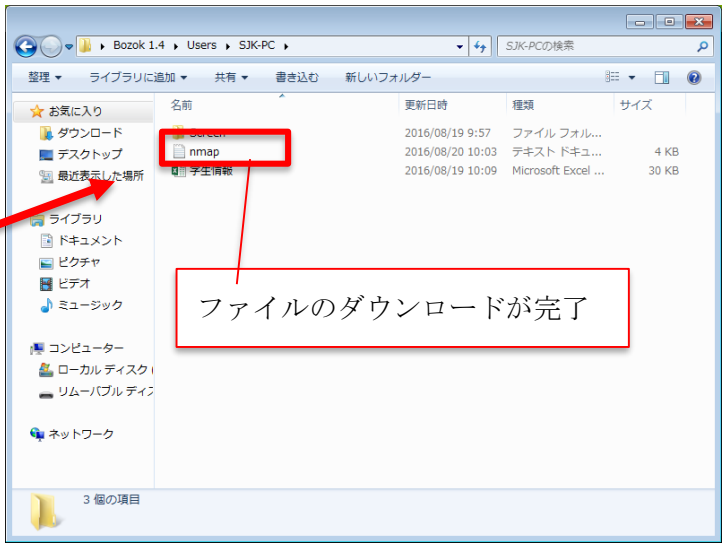
1. 感染側 PC の内部ネットワーク調査実行

   “Remote Shell” のコマンド入力欄に ” **nmap -F -O -P0 192.168.1.0/24 > nmap.txt** “ と入力し、[Send] を押します。（※この調査には時間が掛かります。）

2. 調査結果（nmap.txt）のダウンロード

   感染側 PC を選択し、右クリックメニューから “File Explorer” を選択し起動します。対象ドライブから “C:¥[FIXED]” を選択して感染側 PC の C ドライブの情報が表示し、目的のファイル（ nmap.txt ）を攻撃側 PC にダウンロードします。





■ 演習１０　nmap の調査結果からファイル共有サーバーを探し出し、サービスポートを書き出しましょう？

ファイル共有サーバーIP アドレス	（例）192.168.1.201
サービスポート	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 1025/tcp open NFS-or-IIS 1026/tcp open LSA-or-nterm 1027/tcp open IIS 1028/tcp open unknown 1029/tcp open ms-lsa 3389/tcp open ms-wbt-server 5357/tcp open wsdapi