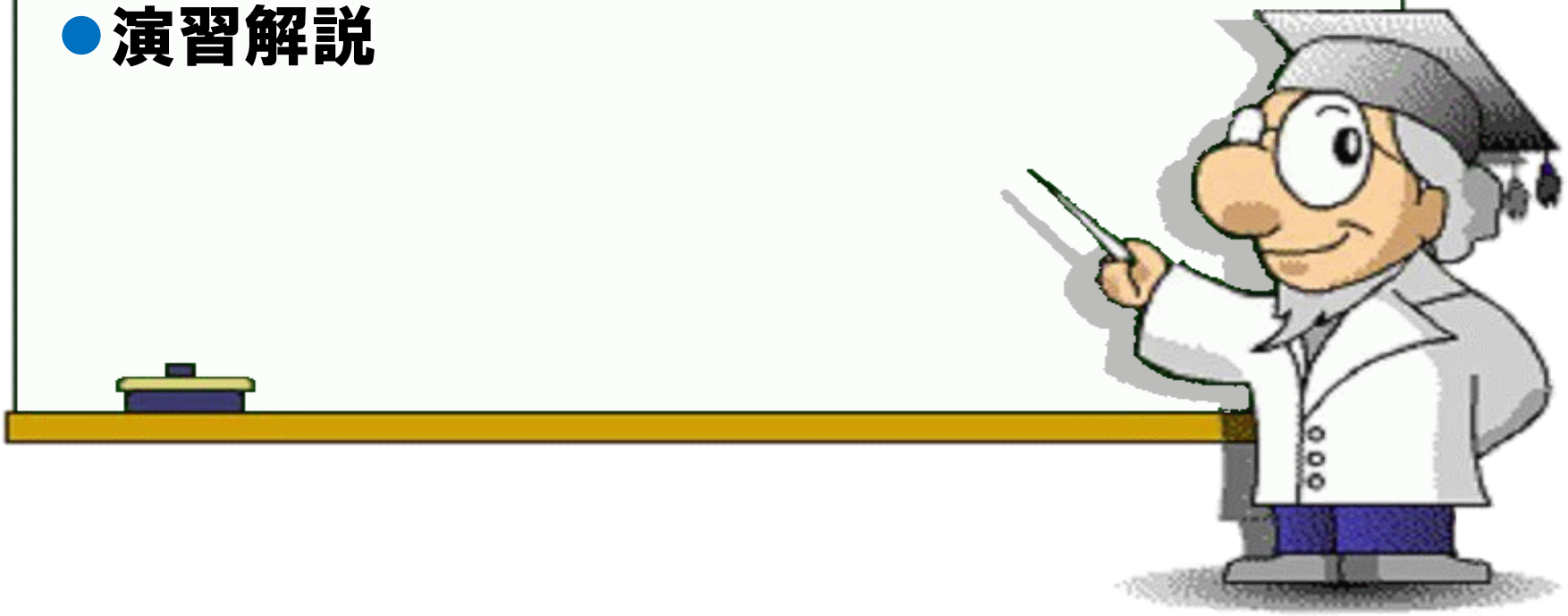
AppGoatを利用した集合教育補助資料
－ディレクトリ・トラバーサル編－

独立行政法人情報処理推進機構（IPA）
セキュリティセンター

内容

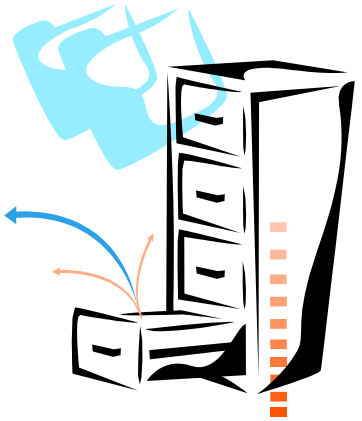
- 脆弱性の原理解説・基礎知識
- 脆弱性の発見方法
- 演習：ファイル情報の漏えい
- 演習解説



ディレクトリ・トラバーサルとは？

- フォルダ（ディレクトリ）を遡り、任意のファイルにアクセスする脆弱性。
- ウェブアプリケーションは複数のフォルダで構成されており、そのフォルダでパスの解釈に問題があることで生じる。
- （../）【一つ上のフォルダに移動する】

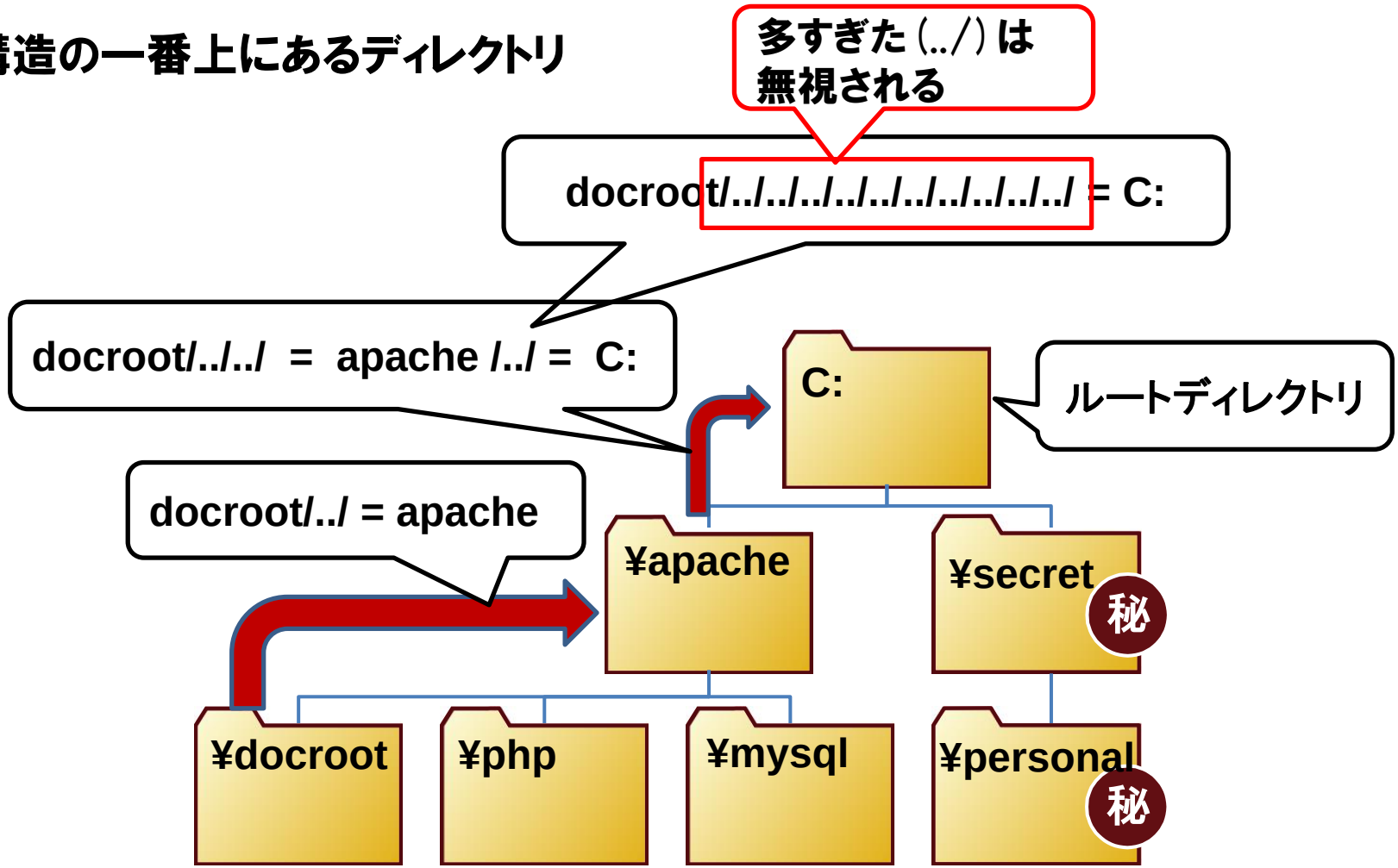
  を用いてフォルダを遡る。



ディレクトリの基礎知識

ルートディレクトリ

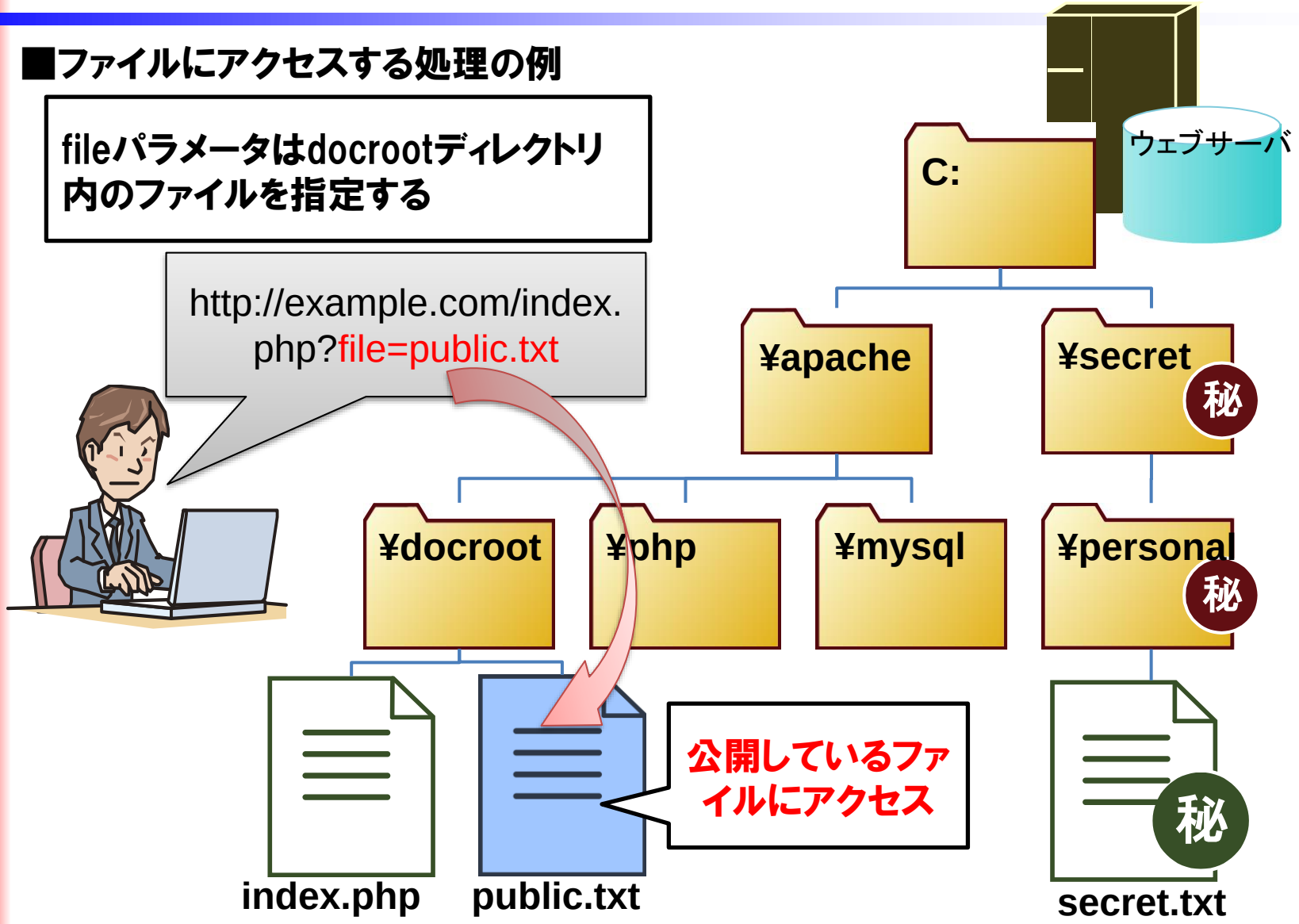
ツリー構造の一番上にあるディレクトリ



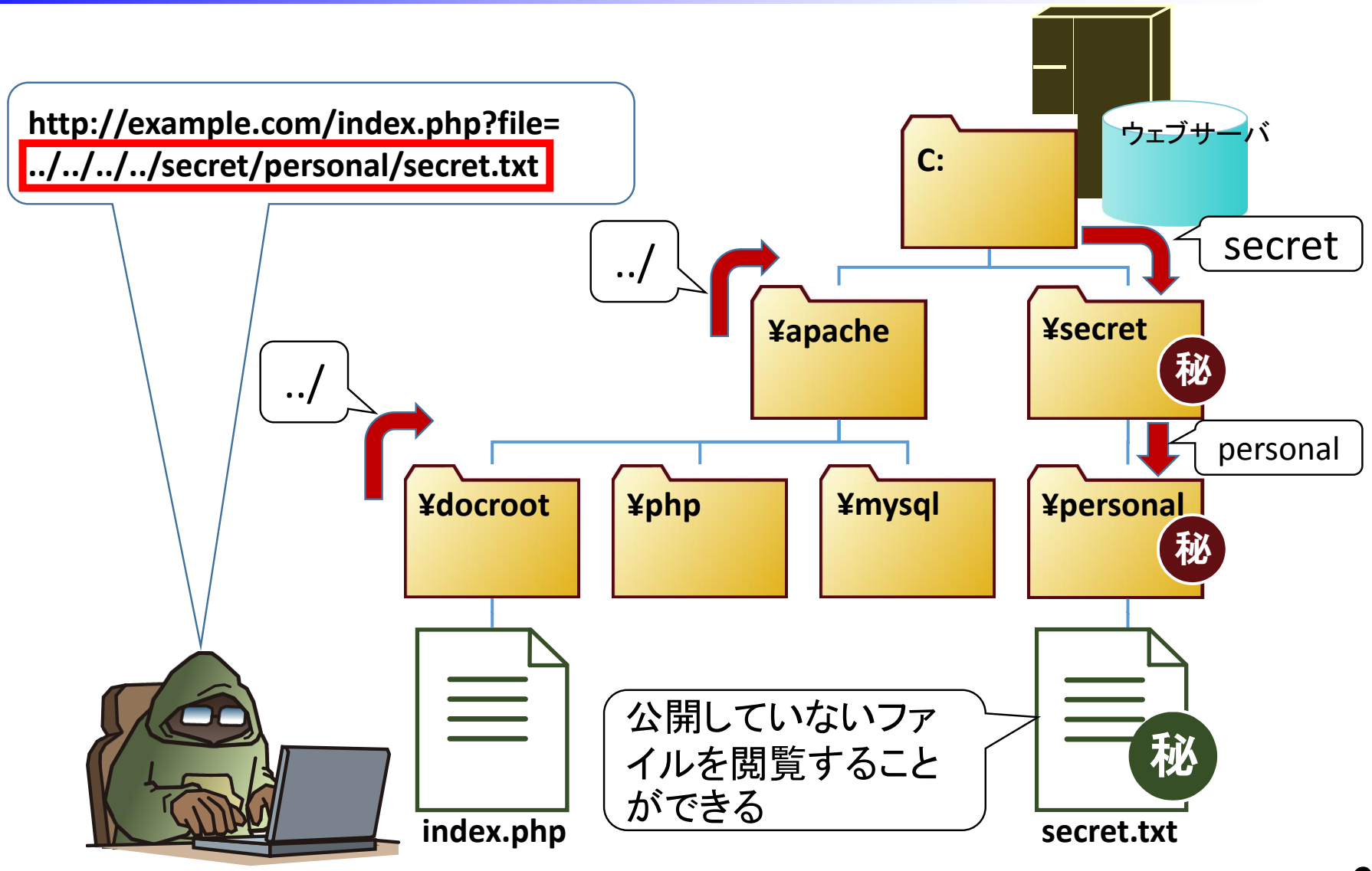
ディレクトリ・トラバーサルの攻撃イメージ
～公開されているファイルにアクセスする通常時の動作～

■ファイルにアクセスする処理の例

fileパラメータはdocrootディレクトリ内のファイルを指定する



ディレクトリ・トラバーサルの攻撃イメージ
～公開されていないsecret.txtにアクセス～

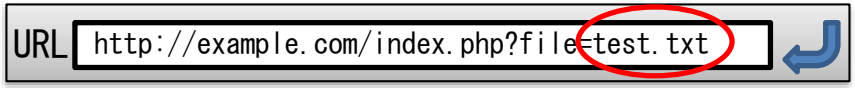


ディレクトリトラバーサルを発見するために

IPA AppGoat ～突いてみますか？脆弱性！～

- **脆弱性が存在する箇所を発見する**

  ポイント：ウェブの中でファイルやディレクトリを指定している箇所を確認する

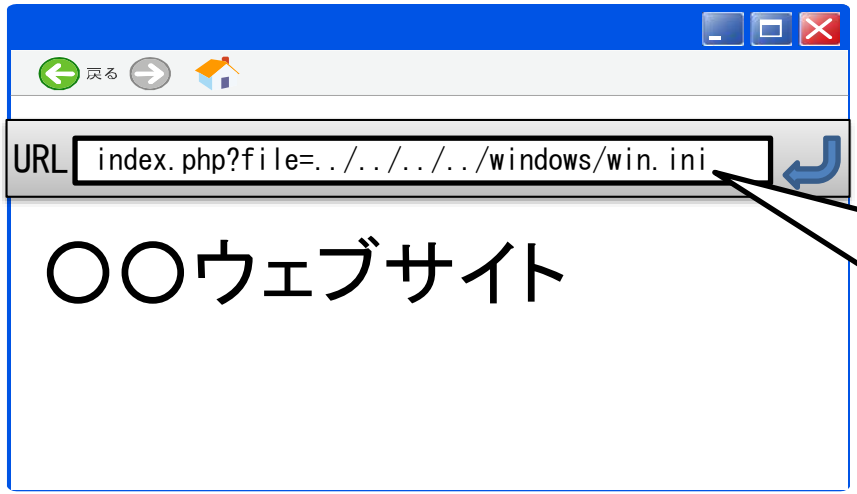


URLパラメータ

■WebサーバがWindows系OSの場合

「../../../../../../../../windows/win.ini」

公開していないファイル

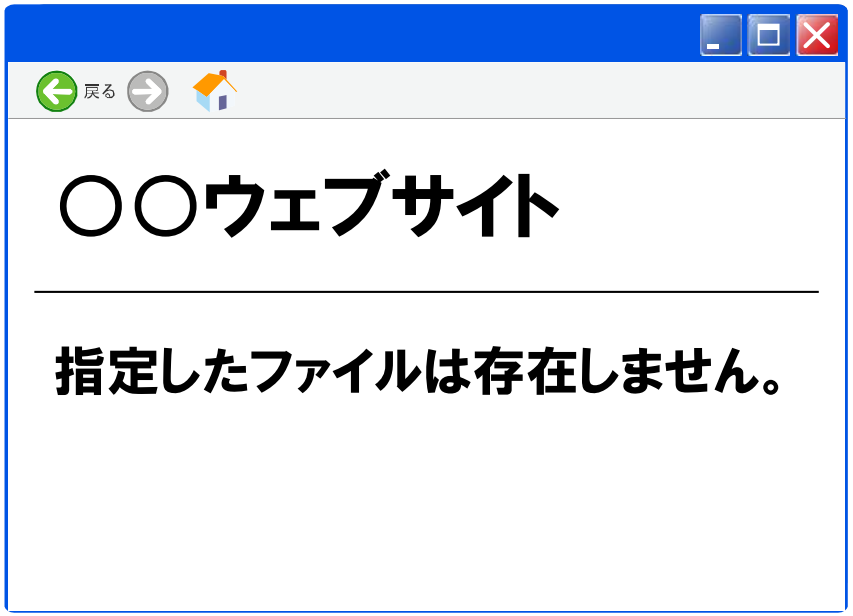


ウェブサイト内のURLのパラメータに、検出パターンを入力して送信する

ディレクトリトラバーサルを発見するために

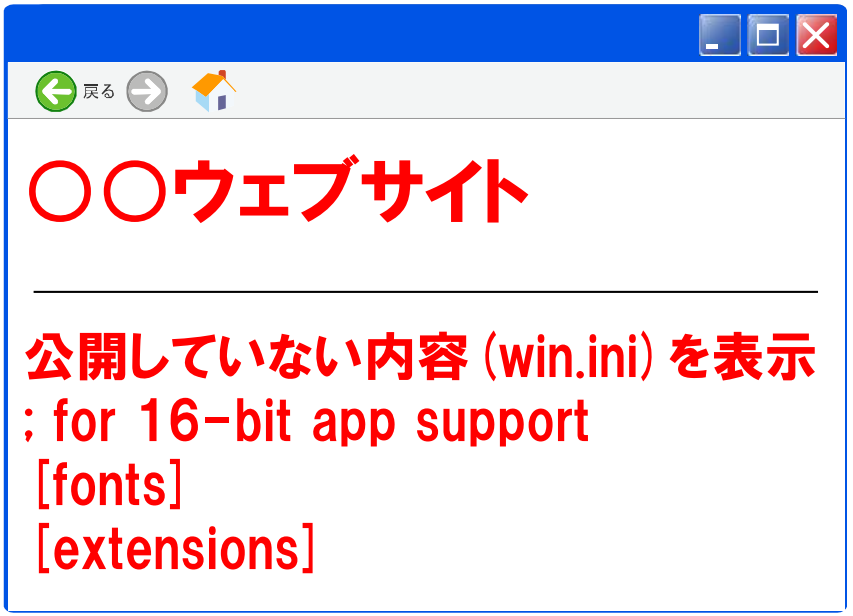
IPA
AppGoat
～突いてみますか？脆弱性！～

【正常】



機能が正常に稼働してエラー処理が実行。

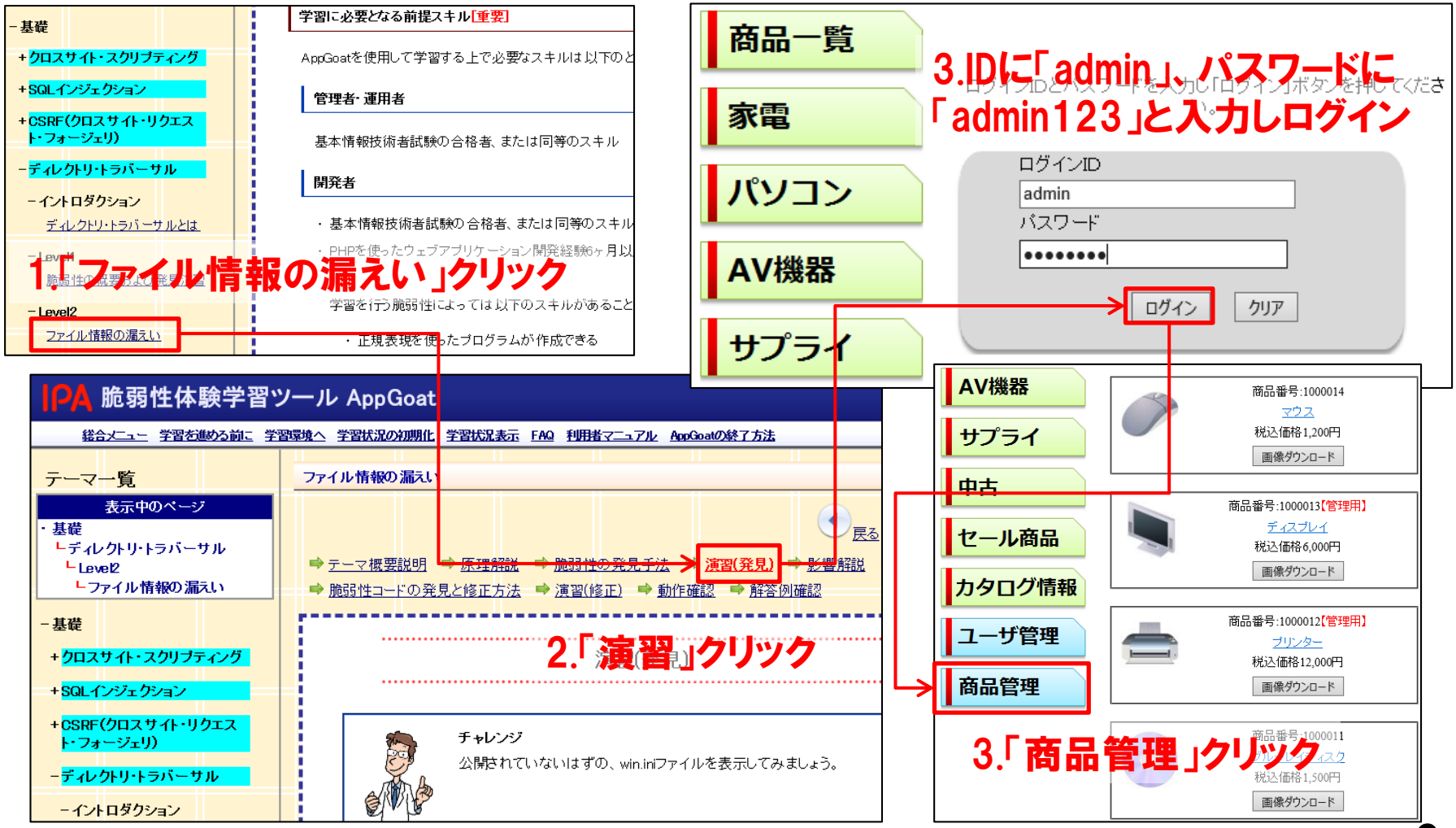
【脆弱性あり】



本来見えていけない情報が表示されたら、脆弱性ありと判定。

[演習] AppGoatの準備

以下の遷移で演習画面に移動します



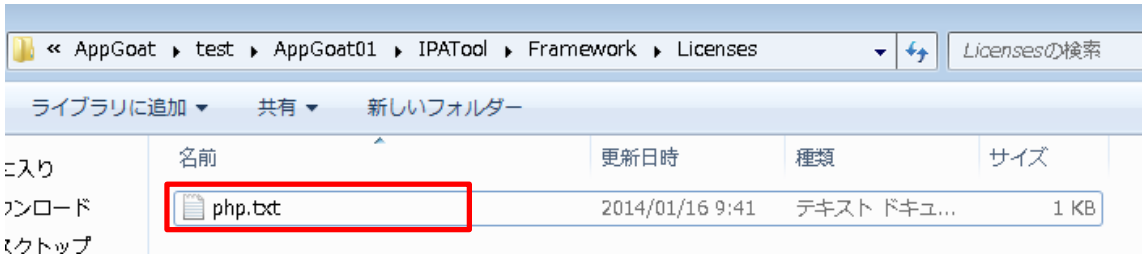
[演習] AppGoatを用いた疑似攻撃体験

- 演習テーマ：

  「ファイル情報の漏えい」

- ミッション：

  公開されていないファイル（php.txt）の表示!



※AppGoatの演習はwin.iniの表示までですが、応用として
IPATool内のフォルダも表示させましょう！

[演習] 演習の進め方

IPA

AppGoat
～突いてみますか？脆弱性！～

- **Step1：脆弱性がある箇所を特定する**
  - ・ログイン後の商品管理画面の商品登録ボタンを押して動作を確認する。
  - ・win.iniにアクセスできる脆弱性のある箇所を確認する。
- **Step2：脆弱性を突く攻撃を考える**
  - ・ php.txtファイルにアクセスするURLを考える。
- **Step3:脆弱性を突いてみる**
  - ・Step2で考えたURLにアクセスする。

実際のphp.txtファイルと表示された情報を比較してみましょう

演習

IPA

演習はじめてください。

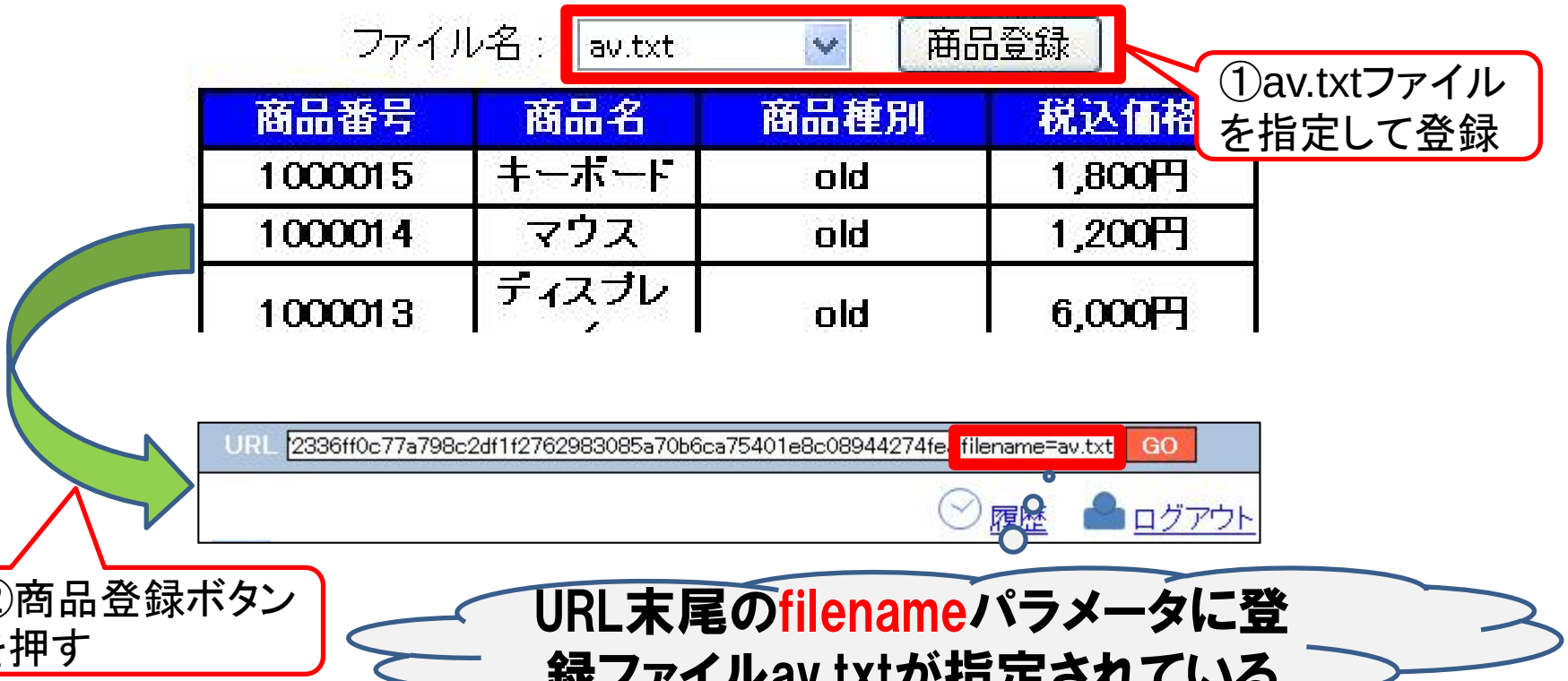
[Step1] 脆弱性がある箇所を特定する

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

URLにファイル名を指定しているようなパラメータがないか探してみましょう

- 商品管理画面の商品登録ボタンを押してみましょう。



URL末尾のfilenameパラメータに登録ファイルav.txtが指定されている

[Step1]  脆弱性がある箇所を特定する

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

win.iniファイルのパスは、C:¥Windows¥win.ini

- (../) を使ってルートディレクトリに遡りwin.iniにアクセス

http://(URL省略)&filename=../../../../../../../../Windows/win.ini

多すぎた(../)は
無視される

=

C:/Windows/win.ini ファイルを呼び出す

[Step1]  脆弱性がある箇所を特定する

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

- **win.iniにアクセスするURLを作成**

ヒント3

・URL欄に次のURLを入力します。
「http://ホスト名:ポート番号/Users/アカウント名/Web/Scenario1421/VulSoft/netshopping.php?page=15&token=トークン&filename=../../../../../../../../../../../windows/win.ini」

・URLに埋め込むトークンは商品管理ページのソースのhidden属性のtokenに格納されています。すでにURLにトークンが入っている場合もありますが、必ずソースのhidden属性のtokenからコピーします。

トークンは「商品管理」ページのソースを表示し、
<input type="hidden" name="token" value="トークン" />
と書かれている箇所から取得することができます。

[Step1]  
脆弱性がある箇所を特定する

IPA
AppGoat
～突いてみますか？脆弱性！～

演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

- 作成したURLを、トークンを取得したページのURL欄に入力してアクセスします。

URL 9e162a43f804a91375988e8ba&filename=../../../../../../../../../../../../windows/win.ini GO

- 画面にwin.iniの情報が表示されることを確認できます。

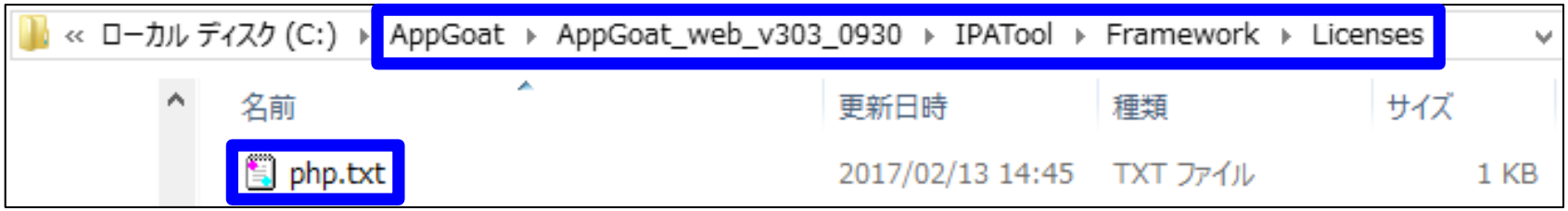
[Step2] php.txtにアクセスするURLを考える

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

ルートディレクトリに遡り、php.txtファイルにアクセスしましょう

- (../) を使ってルートディレクトリに遡りphp.txtファイルにアクセス



多すぎた (../) は無視される

http://(URL省略)&filename=../../../../../../../../../[保存したフォルダ名]/AppGoat_web_v303_XXXX/IPATool/Framework/Licenses/php.txt

⇓

php.txtファイルを呼び出す

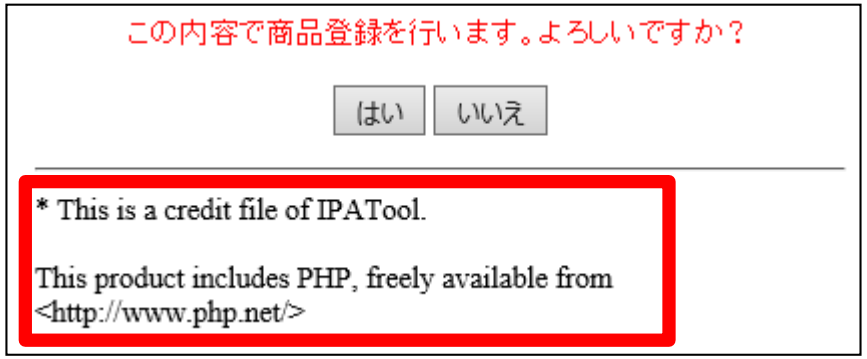
[Step3] Step2のURLにアクセスしファイルを確認する

演習の手順

Step2で作成したURLにアクセスしてみましょう

- 作成したURLを、トークンを取得したページのURL欄に入力してアクセスします。

- 画面にphp.txtの情報が表示されることを確認できます。



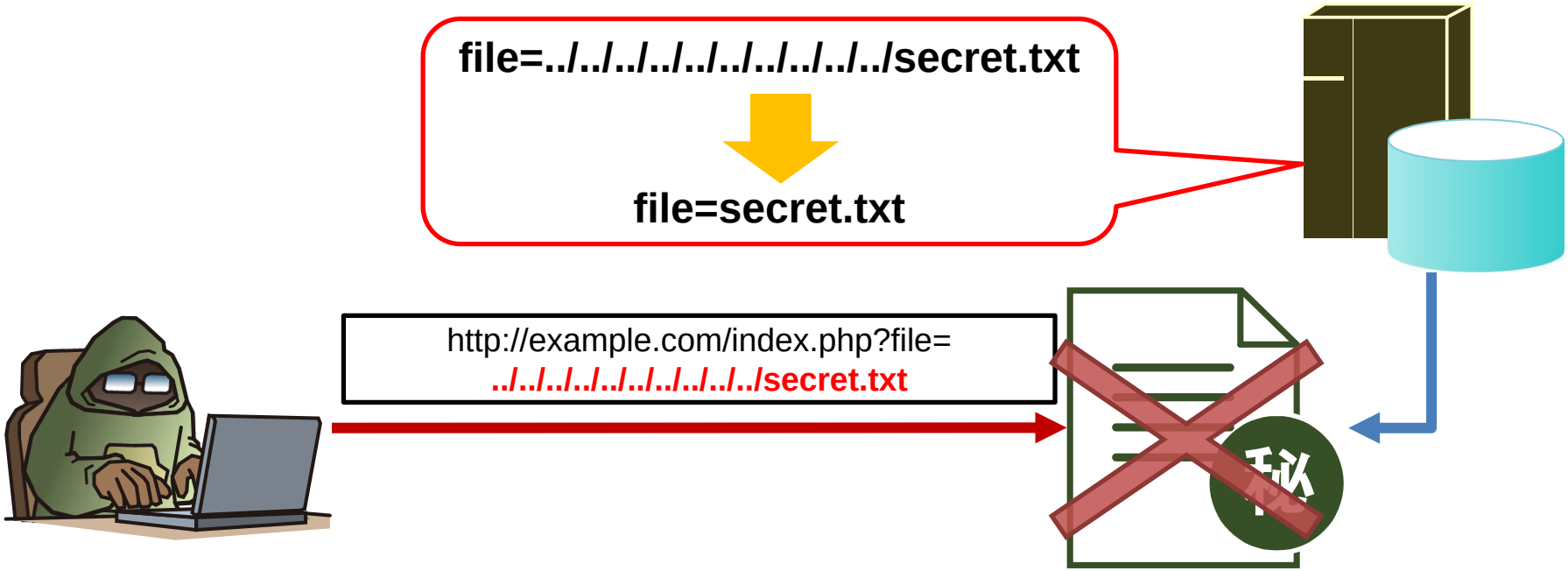
原因の解説

IPA

対策方法

対策のポイント

- ファイル名の指定でディレクトリ名が含まれないようにする



ディレクトリ・トラバーサル脆弱性の対策

- 根本的解決
  - ファイル名にディレクトリ名が含まれないようにする

    PHPではbasename関数を使用することで、ファイル名のみを取得できる。
  - ファイル名を直接指定する実装を避ける
- 保険的対策
  - アクセス権限の設定を正しく管理する。

以上で、

ディレクトリ・トラバーサルの解説は終了です。