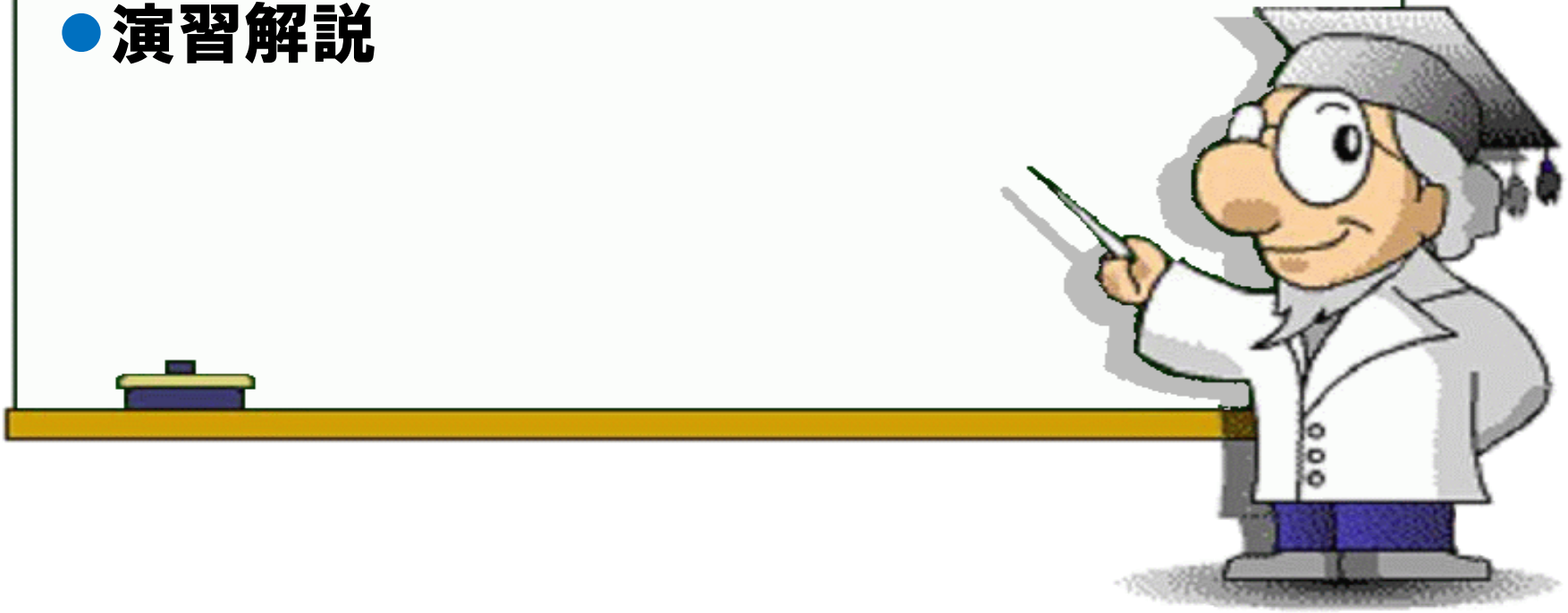
IPA Better Life with IT

AppGoatを利用した集合教育補助資料 －クロスサイトリクエストフォージェリ編－

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（演習1）

- 脆弱性の原理解説・基礎知識
- 脆弱性の発見方法
- 演習1：意図しない命令の実行
- 演習解説

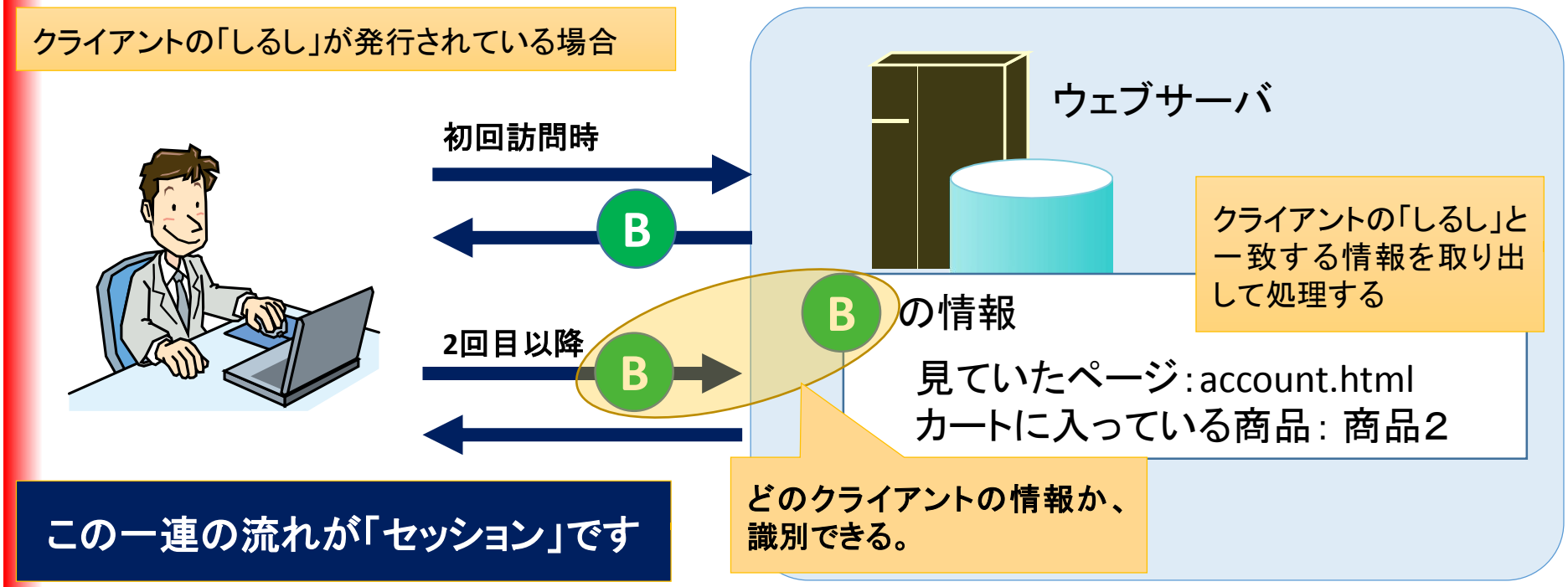


クロスサイト・リクエスト・フォージェリ（CSRF）とは？

- CSRF（Cross Site Request Forgeries）＝ サイトを横断してリクエストを偽造
- セッションIDを悪用し、ウェブサイトにログインしている利用者に意図しない操作をさせる攻撃
- わかりやすく言うと、通常ログイン者しか実行できない操作を、攻撃者が不正に操作する攻撃
- 過去にはCSRFを悪用された可能性がある事件も
  - ✓ 横浜市のサイトに犯行声明が投稿され、大学生が誤認逮捕されてしまった事件（2012年6月）

セッションとは？

- セッション： ウェブサイトへの要求から応答までの一連の流れ
- セッションID： クライアントを識別するためのしるし

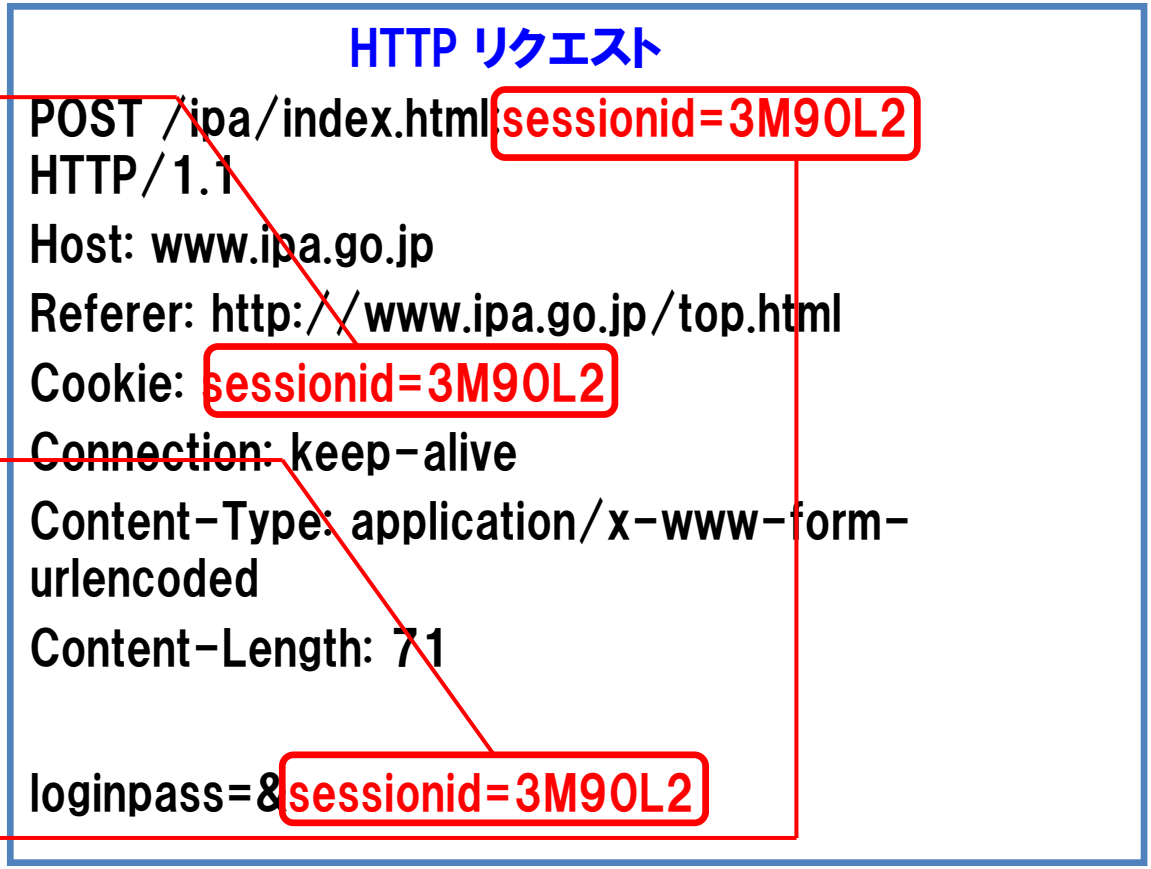


その操作が本人かどうかの確認に利用される

セッション ID をウェブサイトに運ぶ方法は？

- セッション ID を運ぶ方法は以下の3つ

1. Cookie
2. POST メソッド
3. GET メソッド

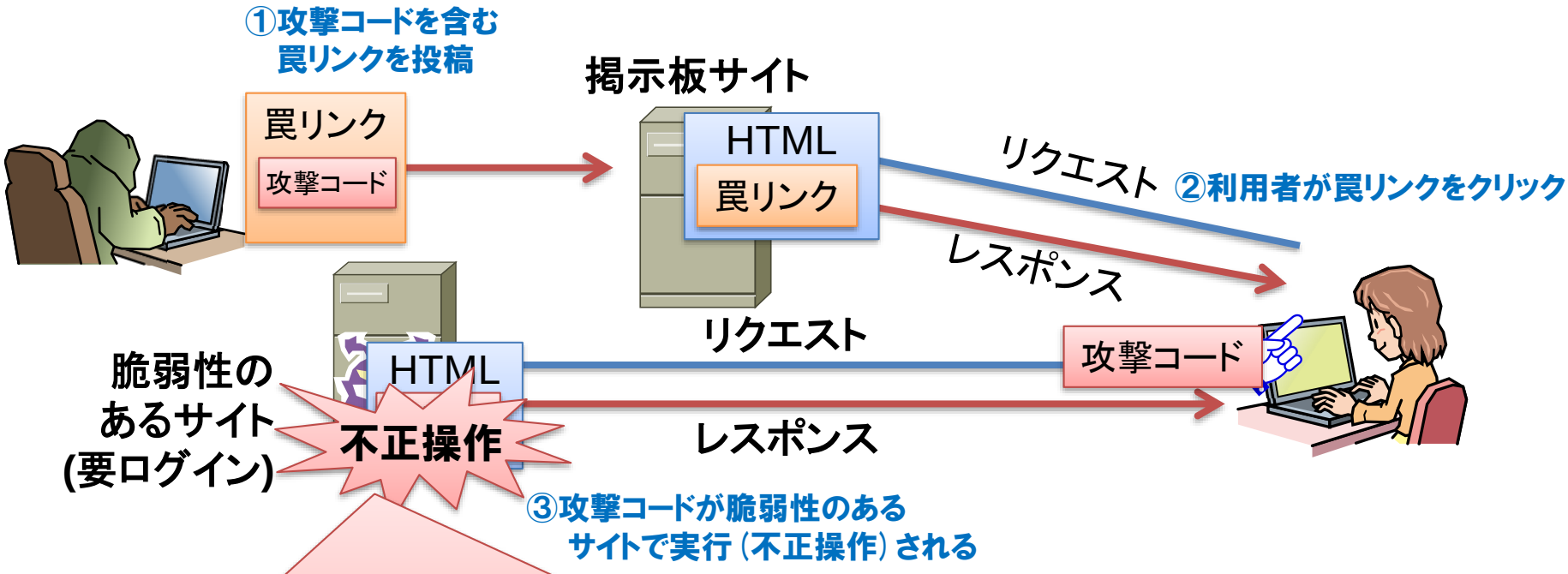


GETメソッドは暗号化できないURL部分にセッションIDを保持するため、盗聴された場合対策できない⇒非推奨の方法

CSRFの攻撃方法

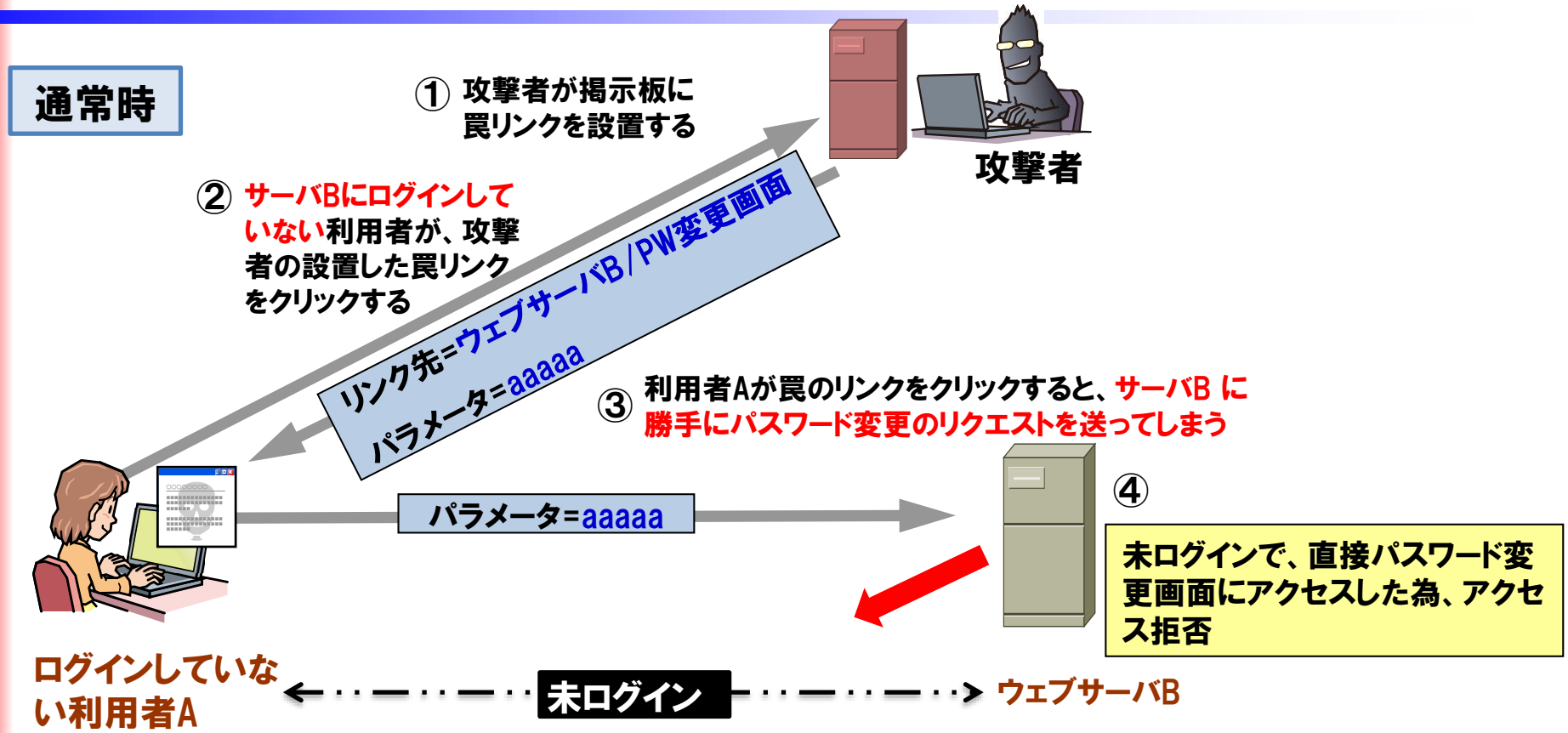
IPA

●ログインが必要なサイトで不正に操作



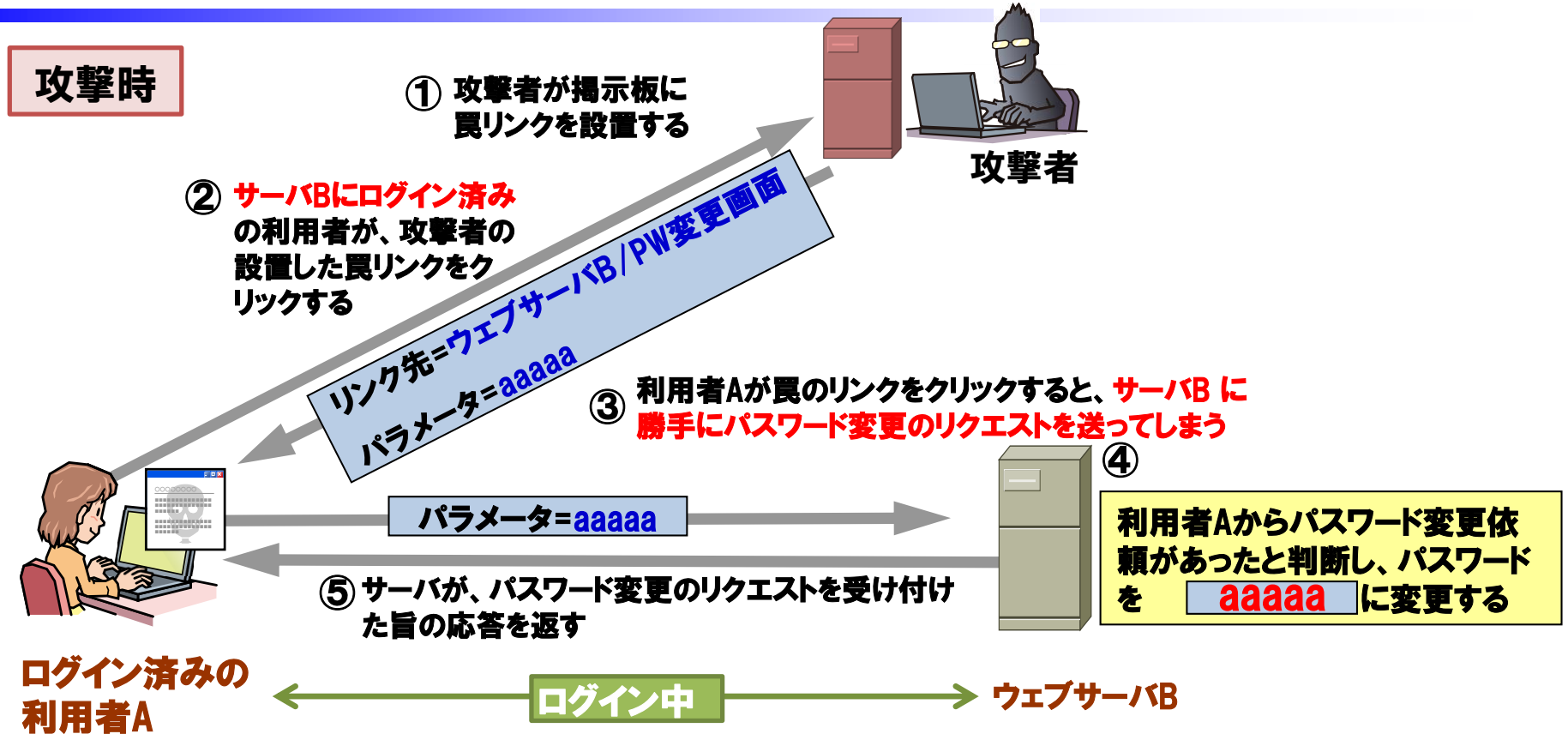
- セッションIDが発行済み（ログイン済み）の場合不正操作
- セッションIDが未発行（未ログイン）の場合処理されない

ウェブアプリケーション側でリクエストを識別する仕組みがないと［セッション切断時］



セッション切断している為、パスワード変更できず

ウェブアプリケーション側でリクエストを識別する仕組みがないと



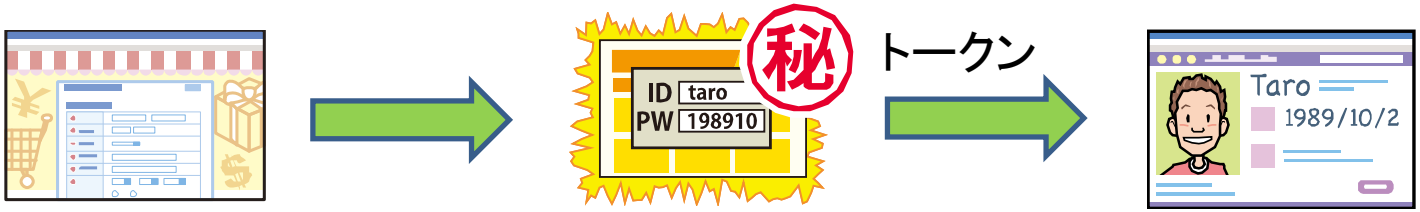
利用者の意図に反して、設定を変更されてしまう

クロスサイトリクエストフォージェリを発見するために

IPA
AppGoat
～突いてみますか？脆弱性！～

- トークンの有無を確認する
- トークンって何？
  - ✓ 第三者が知りえない秘密情報

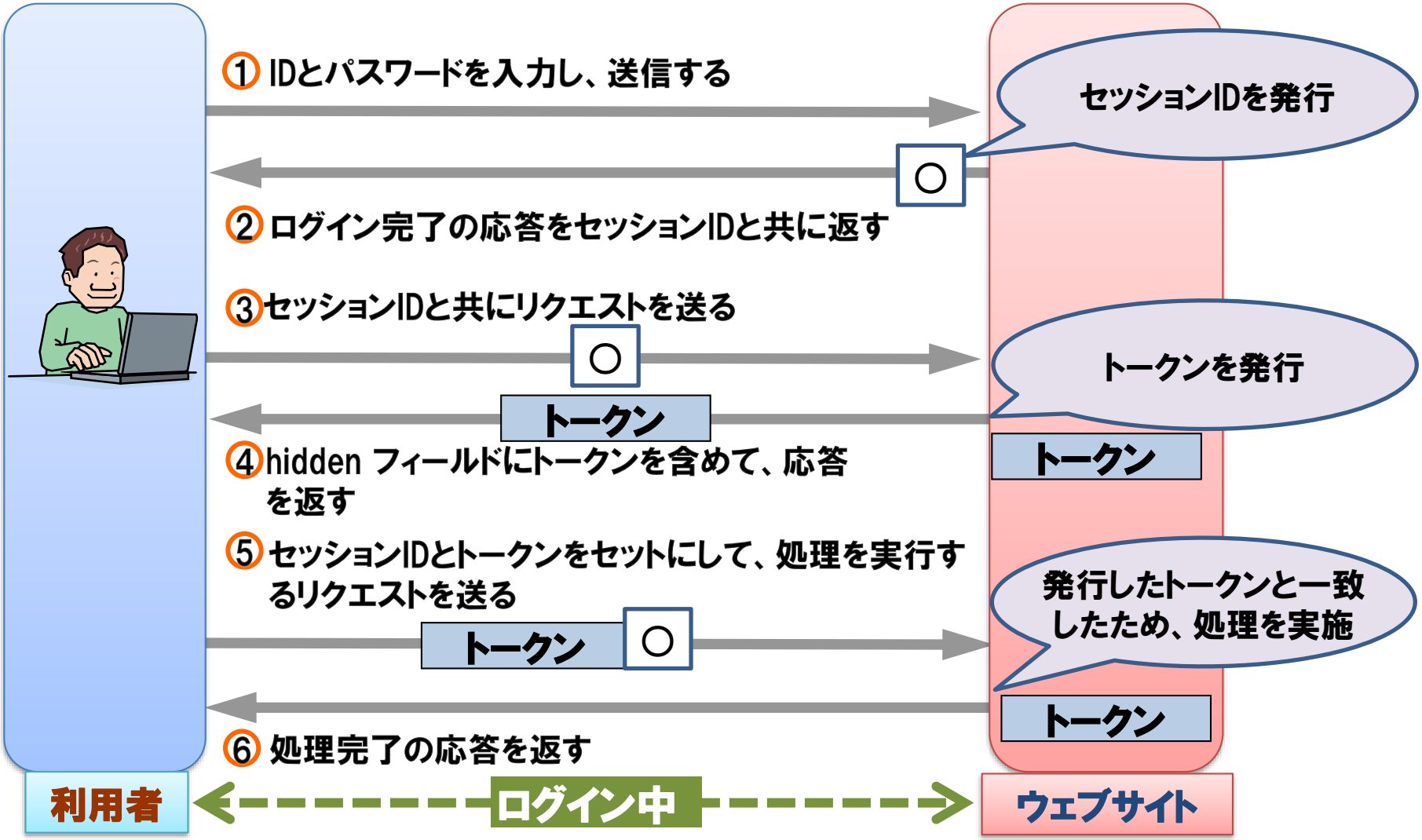
  - ✓ 登録ページや注文ページなどで発行し、利用者が意図したリクエストかを判別する



登録ページ　確認ページ　登録完了ページ

  - ✓ トークンはhiddenフィールドに埋め込んで送信する
    - hiddenフィールド：秘密情報などを格納するために使われる

トークンの基礎知識



クロスサイトリクエストフォージェリを発見するために

IPA
AppGoat
～突いてみますか？脆弱性！～

- トークンをどうやって確認するの？
- ✓URL内やウェブページのHTMLソース内にje0tecsm6cvqae6c9oneinqc44といった不規則な英数字の**値がない**ことを確認する

このような値がなければクロスサイトリクエストフォージェリの脆弱性の可能性

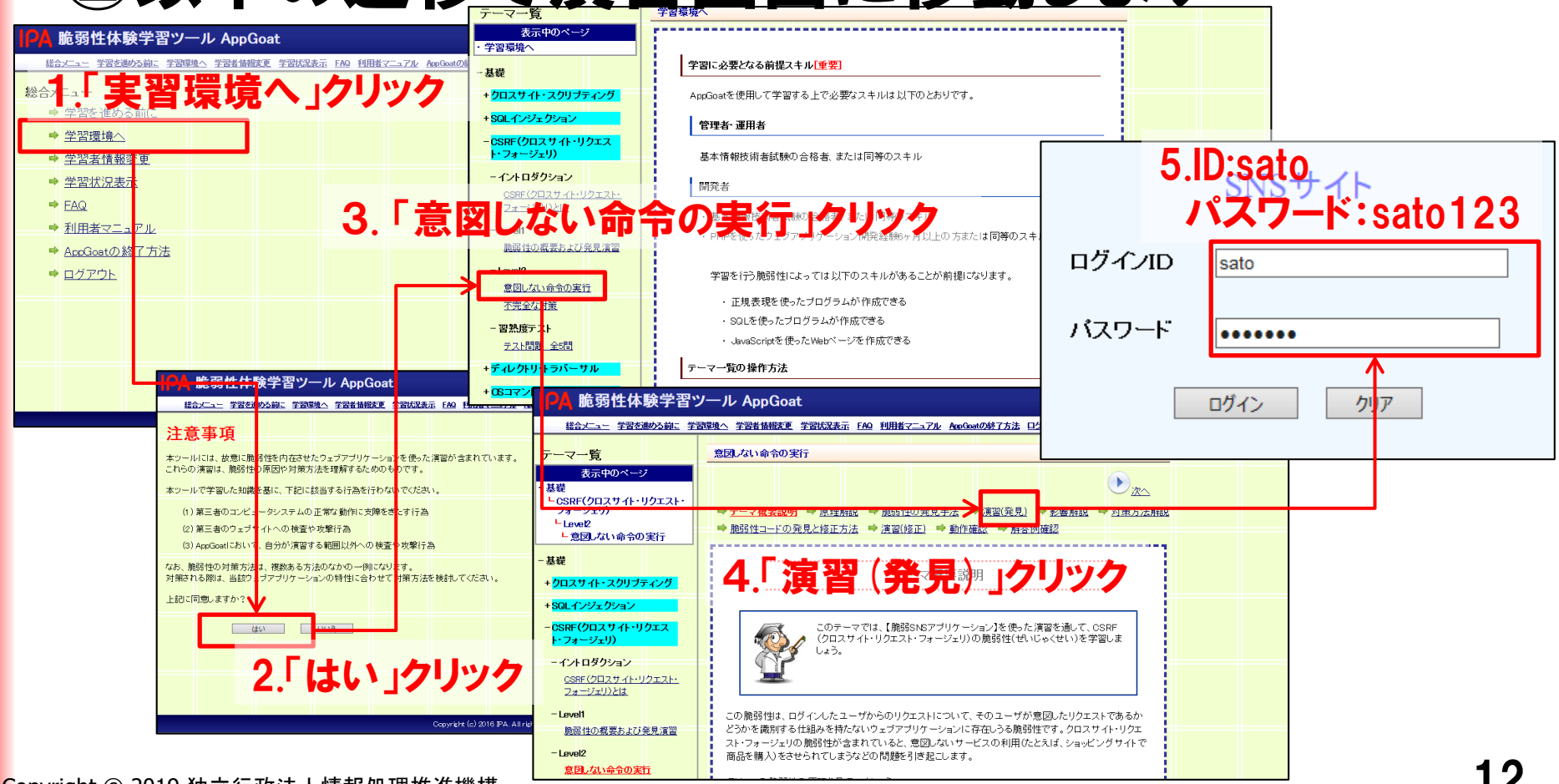
```
<div id="purchase_main" class="center">

    <form method="get" id="form_purchase" action="/Users/user01/Web/Scenario3201/                bond.php">
        <input type="hidden" name="page" value="8" />
        <input type="hidden" name="token" value="2a8b0169e6b8c43a32d4aa80b7e783df4fa375dd4bffefb9e9932701675e232e" />
        <div>
            <span class="must">*</span><span class="bold">口座番号選択</span>
            <span class="right">
                <select name="account_id" id="account_id" onchange="display()">
                    <option value="0">      --</option>
                                                                    <option value="1000001">1000001</option>
                                                                    <option value="1000002">1000002</option>
```

[演習] AppGoatの準備

①AppGoatを起動します

②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

IPA

AppGoat ～突いてみますか？脆弱性！～

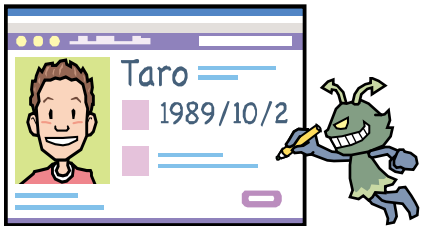
- **演習テーマ：**

  「意図しない命令の実行」

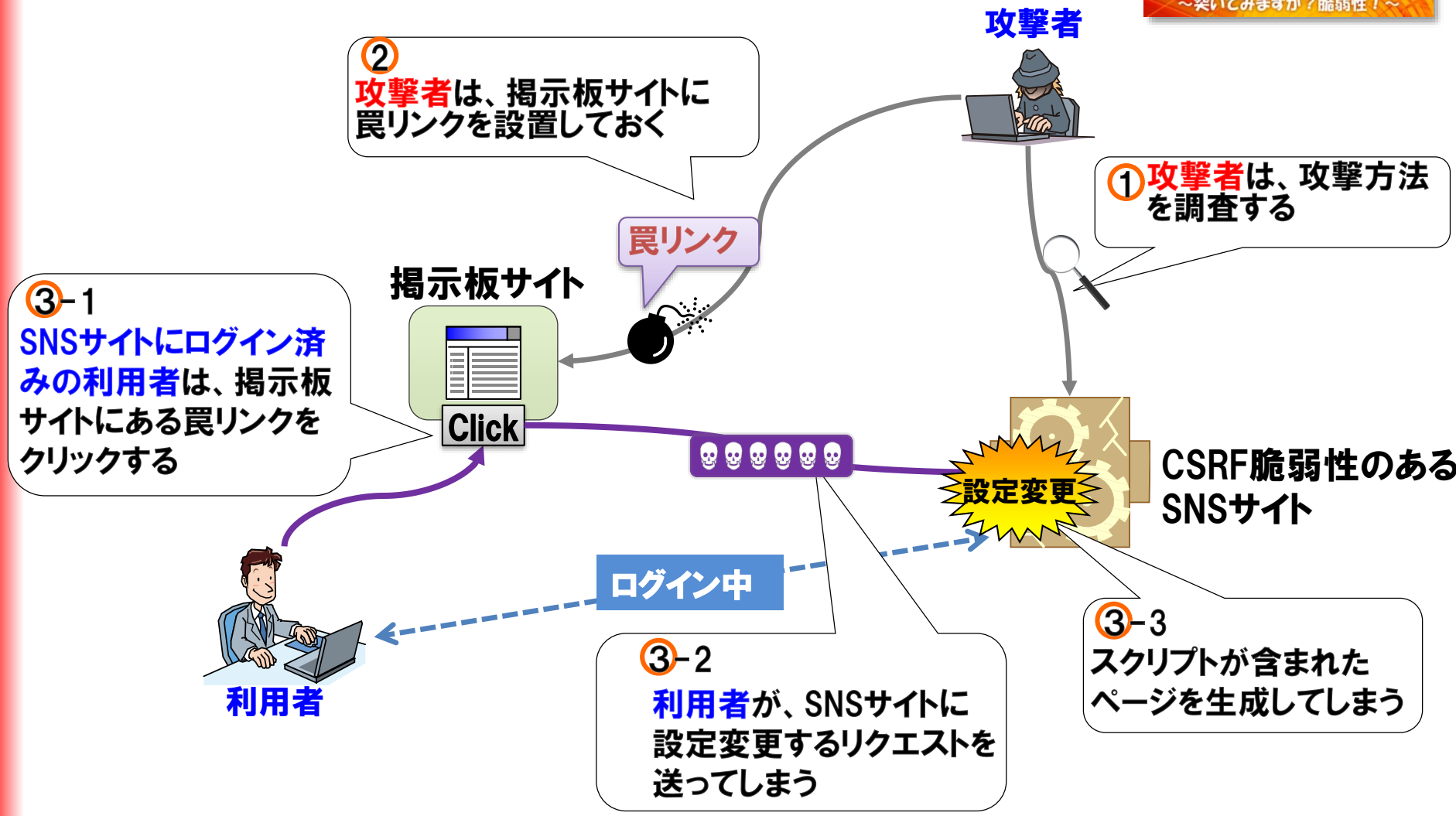
- **ミッション：**

  他人のSNSの設定を変更してみましょう

Congratulations!!演習の目標を達成しました。



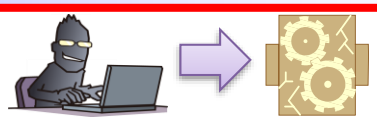
[演習] 疑似攻撃のイメージ



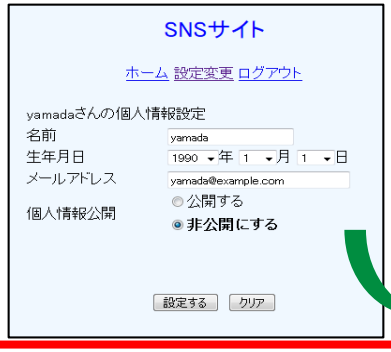
[演習] 演習の進め方

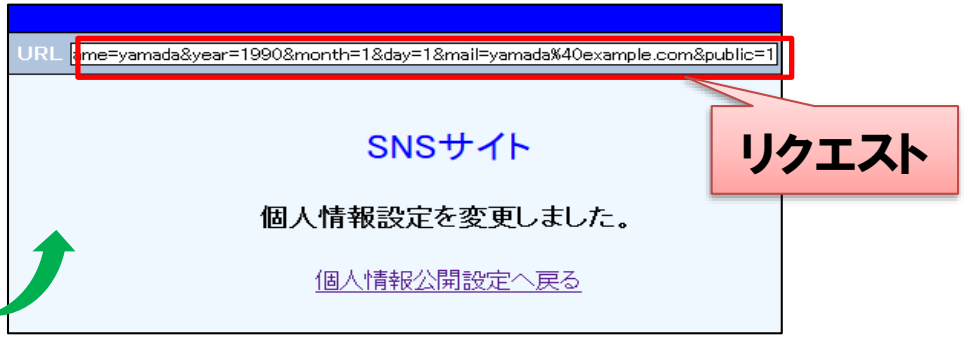
IPA

AppGoat ～突いてみますか？脆弱性！～

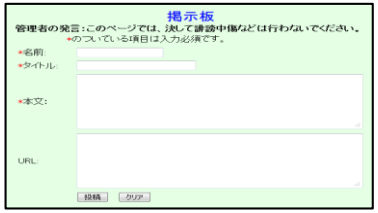


- **Step1：攻撃準備を行う**
  - ・SNS（satoさん）にログインし、設定変更（公開設定）を行う際のリクエストを確認する（※特殊な演習なため、トークンの確認は不要です）

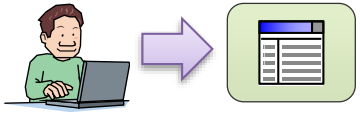




- **Step2：掲示板にアクセスし、設定変更を行うリンクを設置する**
  - ・設定変更（公開設定）を行うリンクを掲示板に投稿する
  - ※分からない場合は、ヒントを参照してください。



- **Step3:攻撃を確認してみる**



  - ・SNS（yamadaさん）にログインした状態で、掲示板のリンクをクリックしてみる

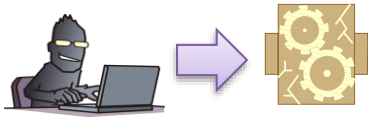
演習

IPA

演習はじめてください。

※演習が終わったら次のページで解説を行います。

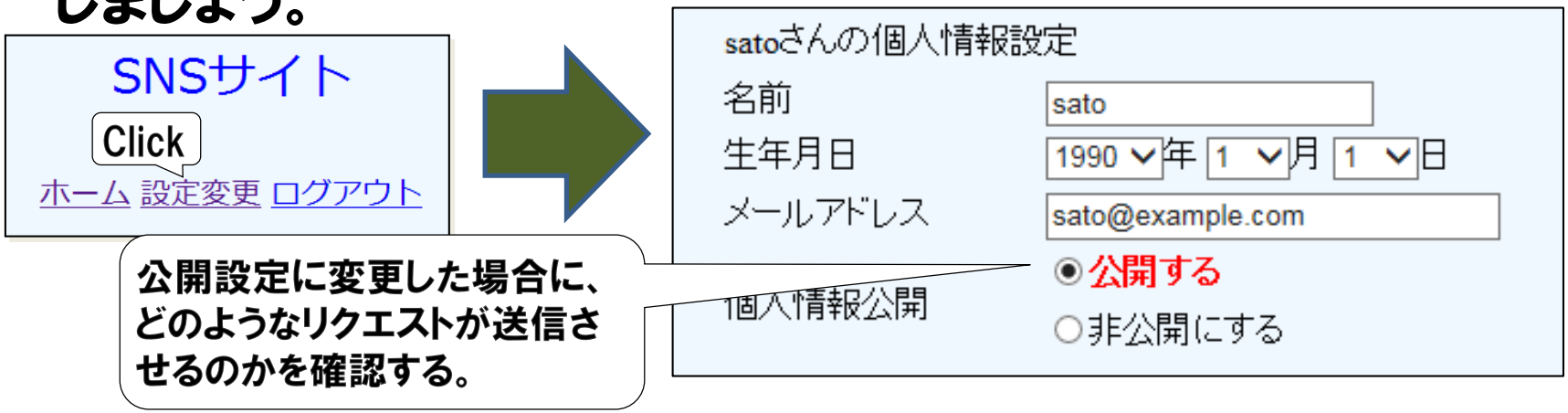
[Step1] どのようなリクエストを送っているか確認する



IPA

AppGoat ～突いてみますか？脆弱性！～

- 設定変更する際にどのようなリクエストを送信しているのか確認しましょう。



送信されるリクエスト

```
http://IPアドレス/Users/ログインID/Web/Scenario1321/VulSoft/sns.php?page=4&secret_token=b5c3181f0f833ba46f27c7fa0e1faee089344ba797ee580b5bff33ff68327519&name=yamada&year=1990&month=1&day=1&mail=yamada@example.com&public=1
```

「個人情報公開」の設定を変更するためのパラメータ

補足：secret_tokenパラメータがあるため、トークンが存在するように見えますが、演習のために無効化しています。
トークンが存在しない（脆弱性が存在する）前提での演習となります。

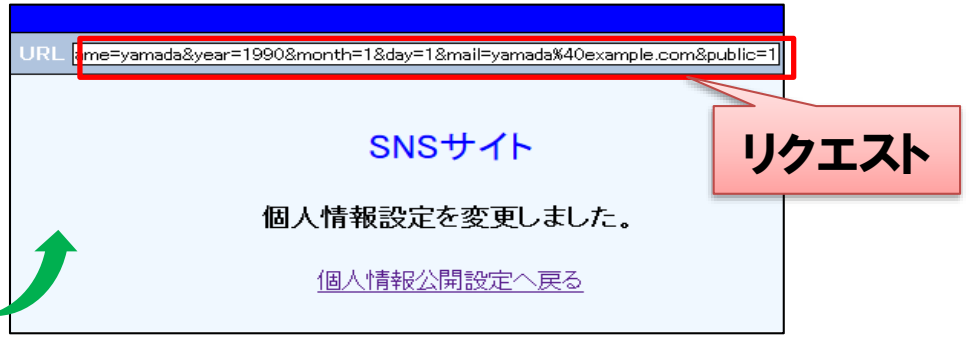
[演習] 演習の進め方

IPA

AppGoat ～突いてみますか？脆弱性！～

Step1：攻撃準備を行う

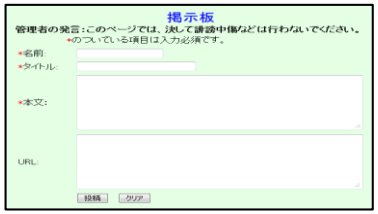
・SNS（satoさん）にログインし、設定変更（公開設定）を行う際のリクエストを確認する



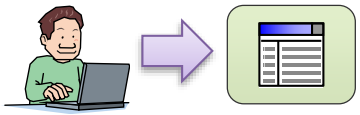
Step2：掲示板にアクセスし、設定変更を行うリンクを設置する

・ 設定変更（公開設定）を行うリンクを掲示板に投稿する

※分からない場合は、ヒントを参照してください。



Step3:攻撃を確認してみる



・SNS（yamadaさん）にログインした状態で、掲示板のリンクをクリックしてみる

[Step2] 
罠リンクのURLを考える

IPA
AppGoat
～突いてみますか？脆弱性！～

- SNSサイトのCSRF脆弱性を突いて、「個人情報公開」の設定を「公開する」に変更するURLを考えてみましょう。

1. 前スライドで確認したリクエストから、「個人情報公開」の設定を変更するパラメータを確認します。赤字が該当のパラメータです。

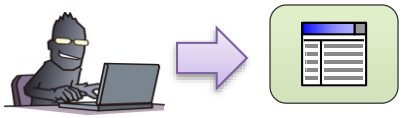
確認したリクエスト

http://IPアドレス/Users/ログインID/Web/Scenario1321/VulSoft/sns.php?page=4&secret_token=b5c3181f0f833ba46f27c7fa0e1faee089344ba797ee580b5bff33ff68327519&name=yamada&year=1990&month=1&day=1&mail=yamada@example.com&public=1

2. 必要最低限のパラメータのみ残すと下記のようなリクエストになります。下記のリクエストが送信されるように罠リンクを設置します。

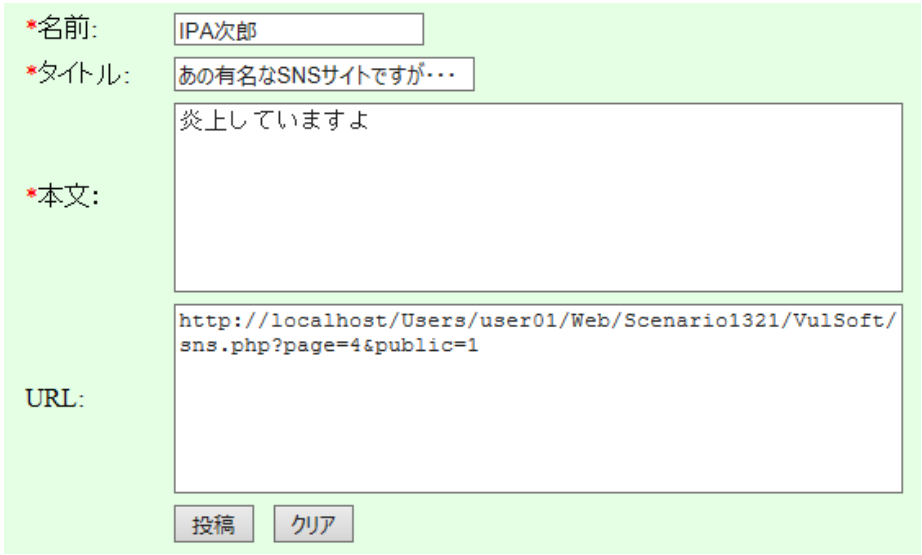
罠リンクのURL

http://IPアドレス/Users/ログインID/Web/Scenario1321/VulSoft/sns.php?page=4&public=1

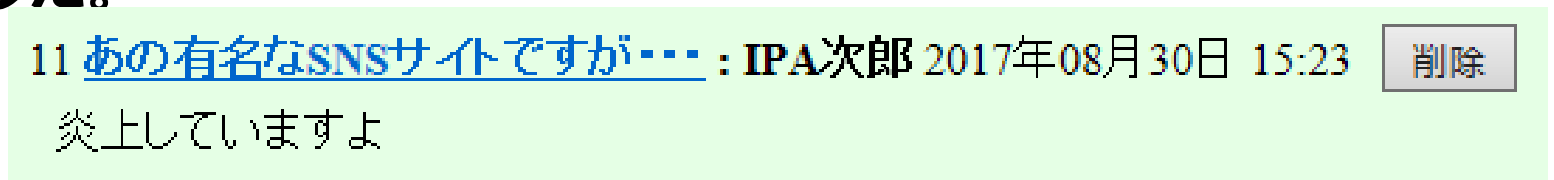
[Step2]  罠リンクを掲示板サイトに投稿する

IPA AppGoat ～突いてみますか？脆弱性！～

1. **攻撃者の立場になり**、掲示板に罠のリンクを作成します。罠のリンクには、先ほど作成したURLを入力します。

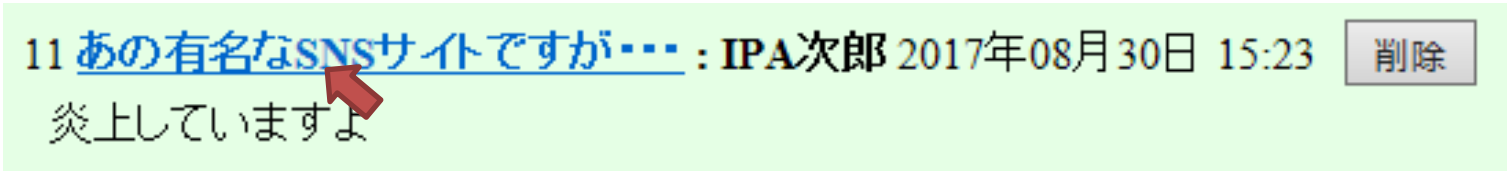


2. 「投稿」ボタンを押下します。これで罠リンクの設置が完了しました。

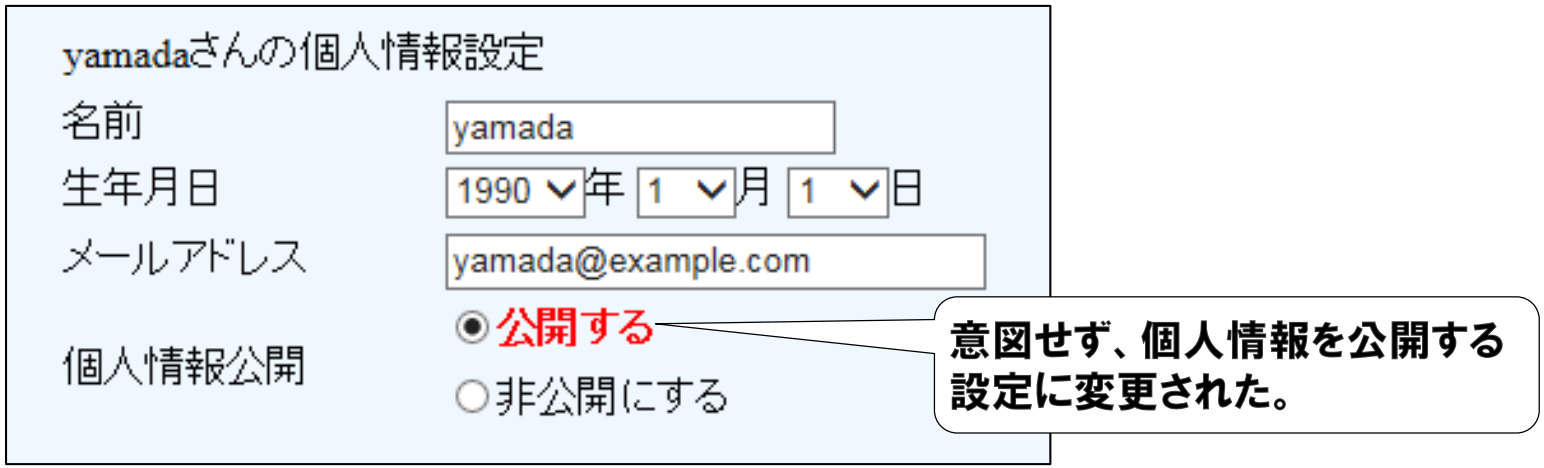


[Step3]  設定変更されてしまうことを確認する

1. （SNSサイトにログインした）利用者の立場になり、罠のリンクをクリックし、SNSサイトにアクセスします。



2. その結果、利用者のSNS設定情報が変更されます。

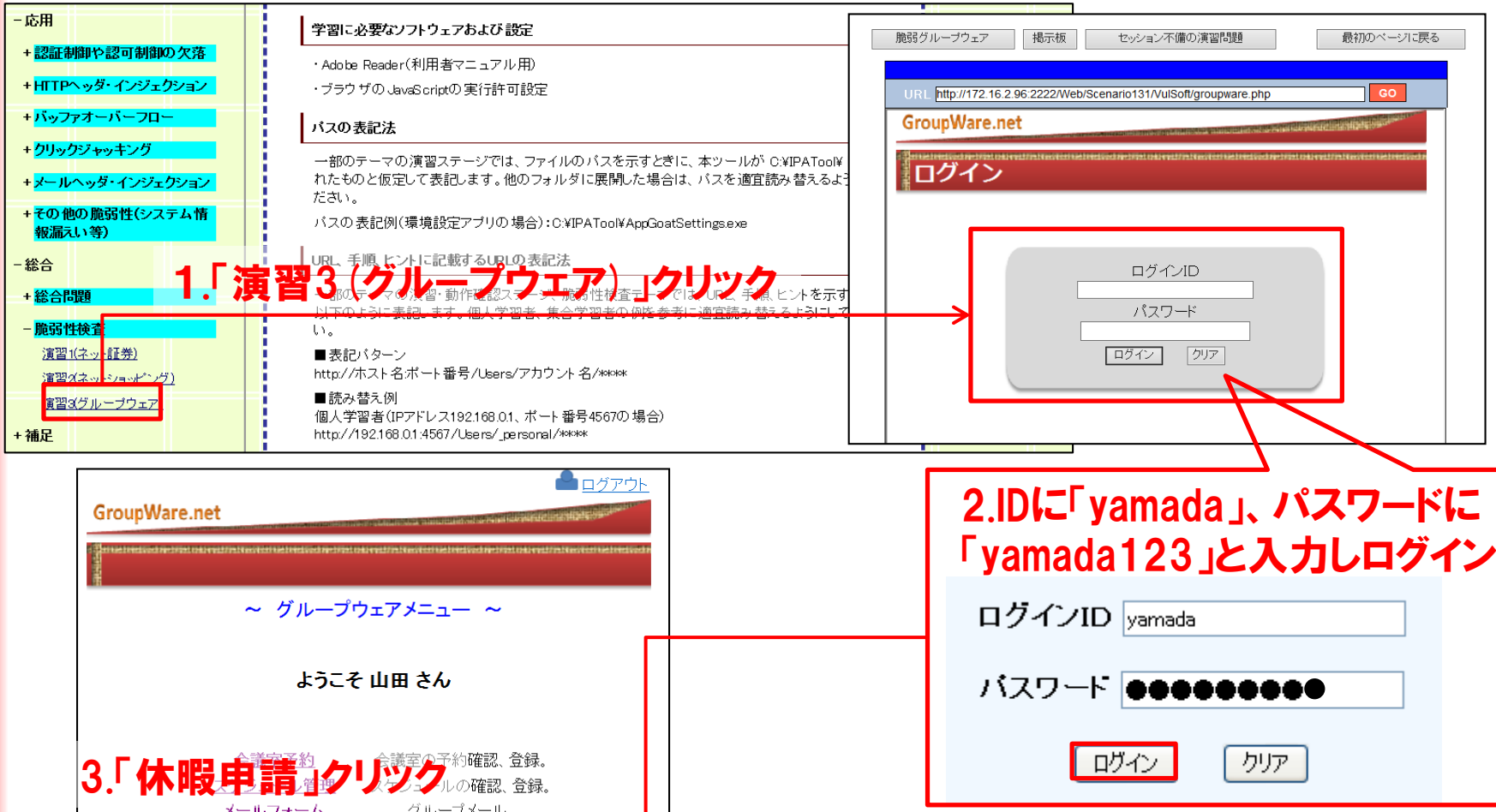


内容（演習2）

- 演習2：演習3（グループウェア）
- 演習解説
- 対策方法

[演習] AppGoatの準備

①以下の遷移で演習画面に移動します

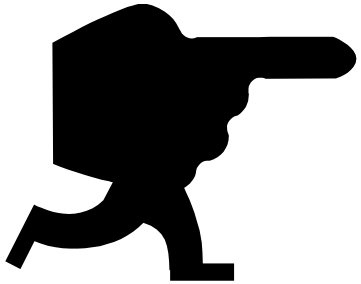


[演習] AppGoatを用いた疑似攻撃体験

IPA
AppGoat
～突いてみますか？脆弱性！～

- **演習テーマ：**

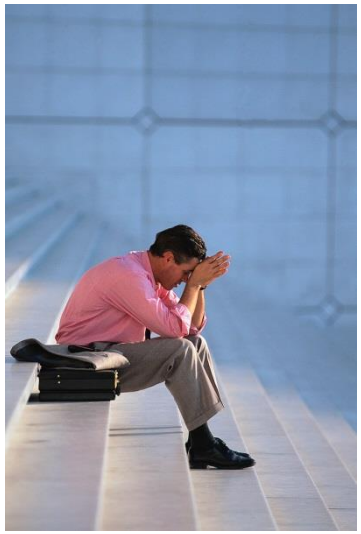
  「意図しない命令」



- **ミッション：**

  意図しない休暇申請の操作

Congratulations!!演習の目標を達成しました。



[演習] 演習の進め方

IPA
AppGoat
～突いてみますか？脆弱性！～

- Step1：脆弱となる箇所を特定する
  - ・リクエスト（URL）にトークンが含まれずに処理を実施できてしまう操作を発見してみましょう

- Step2：掲示板にアクセスし、登録変更を行うリンクを設置する

- Step3:攻撃を確認してみる
  - ・SNSにログインした状態で、掲示板に設置したリンクにアクセスしてみましょう。

演習

IPA

演習はじめてください。

※演習が終わったら次のページで解説を行います。

[Step1] 
トークンを送らずに処理ができてしまう操作を確認する

IPA
AppGoat
～突いてみますか？脆弱性！～

演習の手順

処理を実行する際のURLにトークンが含まれているか確認しましょう

- 休暇申請書を作成し、URLを確認してみましょう。

```
http://IPアドレス/Users/ログインID/Web/Scenario3401/VulSoft/
groupware.php?page=8&token=0197f33f7b071d855608a0e3a92381b
b144b3cad6a1298e3e6e69e506b8749a1&start_time=2017%2F09%2F
01&end_time=2017%2F09%2F08&date=6&type=%E5%85%A8%E6%97%A
5%E4%BC%91%E6%9A%87&reason=%E7%A7%81%E7%94%A8&comment=
&save=%E7%94%B3%E8%AB%8B%E6%9B%B8%E3%81%AE%E4%BD%9C%E6
%88%90
```

- 演習用に数個休暇申請書を作成してみましょう。
- 休暇申請を削除するURLを確認してみましょう。

```
http://IPアドレス/Users/ログインID/Web/Scenario3401/VulSoft/
groupware.php?page=8&holiday_id=1&delete=%E5%89%8A%E9%99%A4
```

トークンが含まれていない

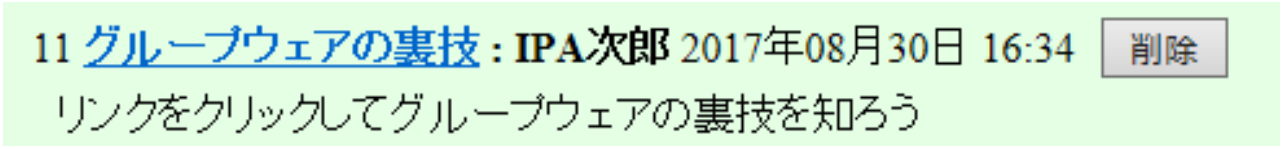
[Step2] 

罠リンクを掲示板サイトに投稿する

IPA AppGoat ～突いてみますか？脆弱性！～

1. **攻撃者の立場になり**、掲示板に罠のリンクを作成します。罠のリンクには、先ほど休暇申請を削除したURLを入力します。

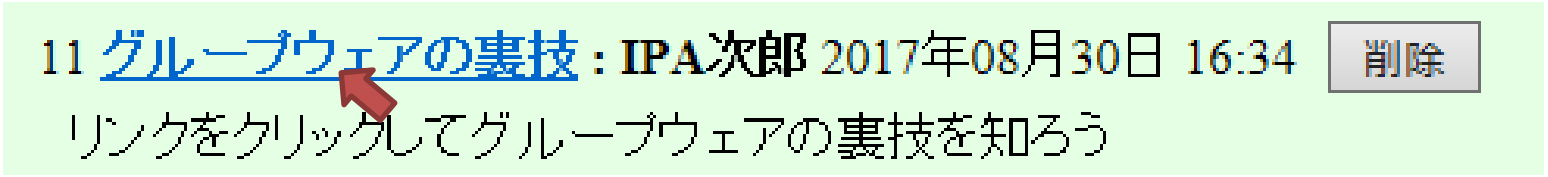
2. 「投稿」ボタンを押下します。これで罠リンクの設置が完了しました。



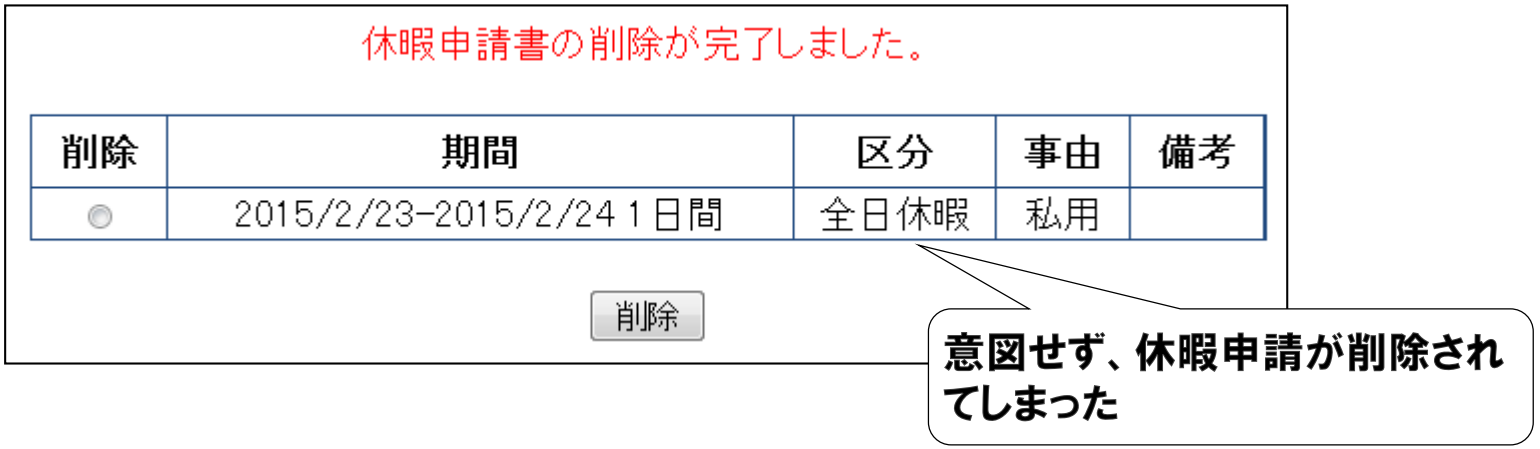
[Step3] 休暇申請が削除されることを確認する

IPA AppGoat ～突いてみますか？脆弱性！～

1. （グループウェアにログインした）利用者の立場になり、罠のリンクをクリックし、グループウェアにアクセスします。



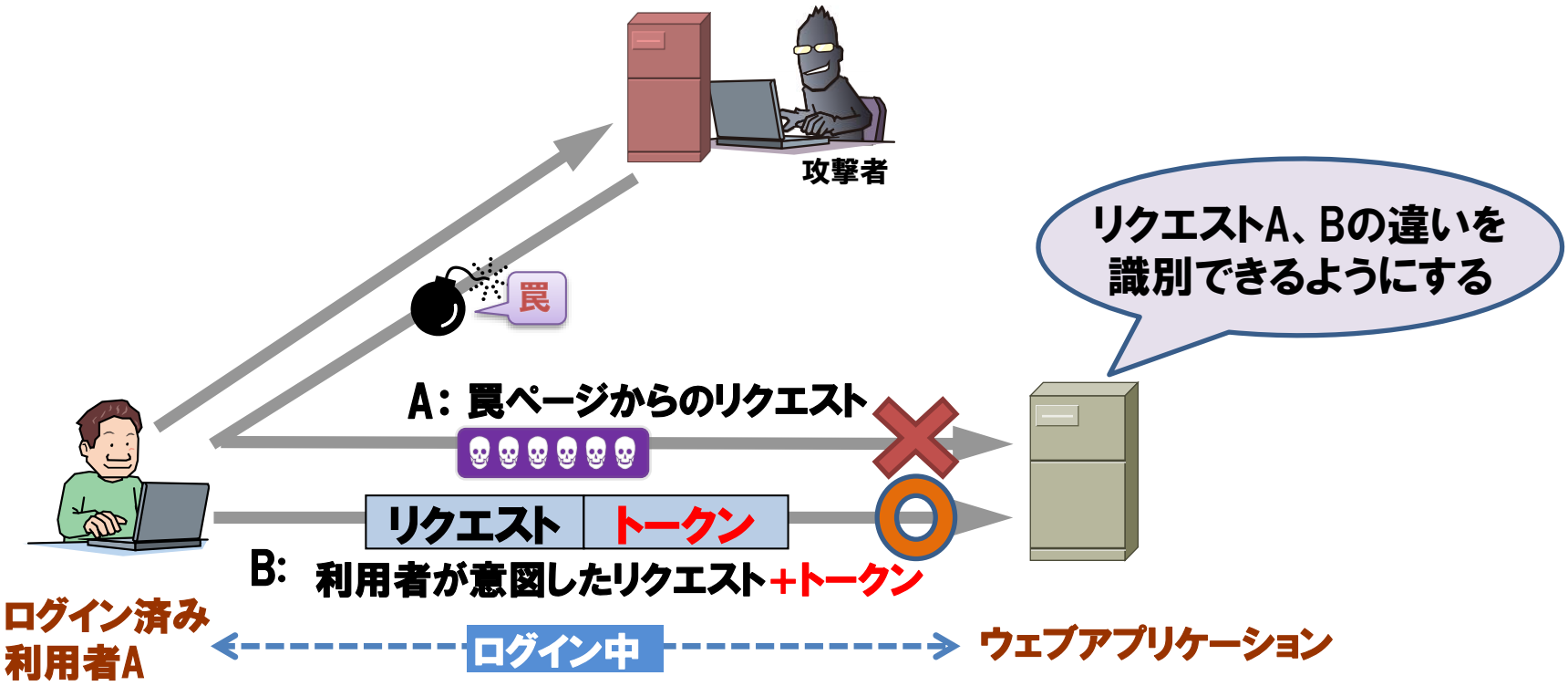
2. その結果、利用者の休暇申請が削除されてしまいます。



対策方法の解説

対策のポイント

- 罠ページを経由したリクエストと正規のリクエストを識別できるようリクエストにトークン（秘密情報）を付加する



対策方法

- リクエストに推測困難な秘密情報を埋め込む
  - 処理を実行する際に、秘密情報を要求し、その値が正しい場合のみに処理を実行する
    - ✓POSTメソッドで送る
      - ⇒GETメソッドで秘密情報を送付すると、外部サーバのアクセスログに秘密情報がRefererとして漏れる可能性がある

秘密情報が上記の条件を満たさないと、対策漏れが生じる可能性がある

以上で、
クロスサイトリクエストフォージェリの
解説は終了です。