

情報セキュリティ基礎

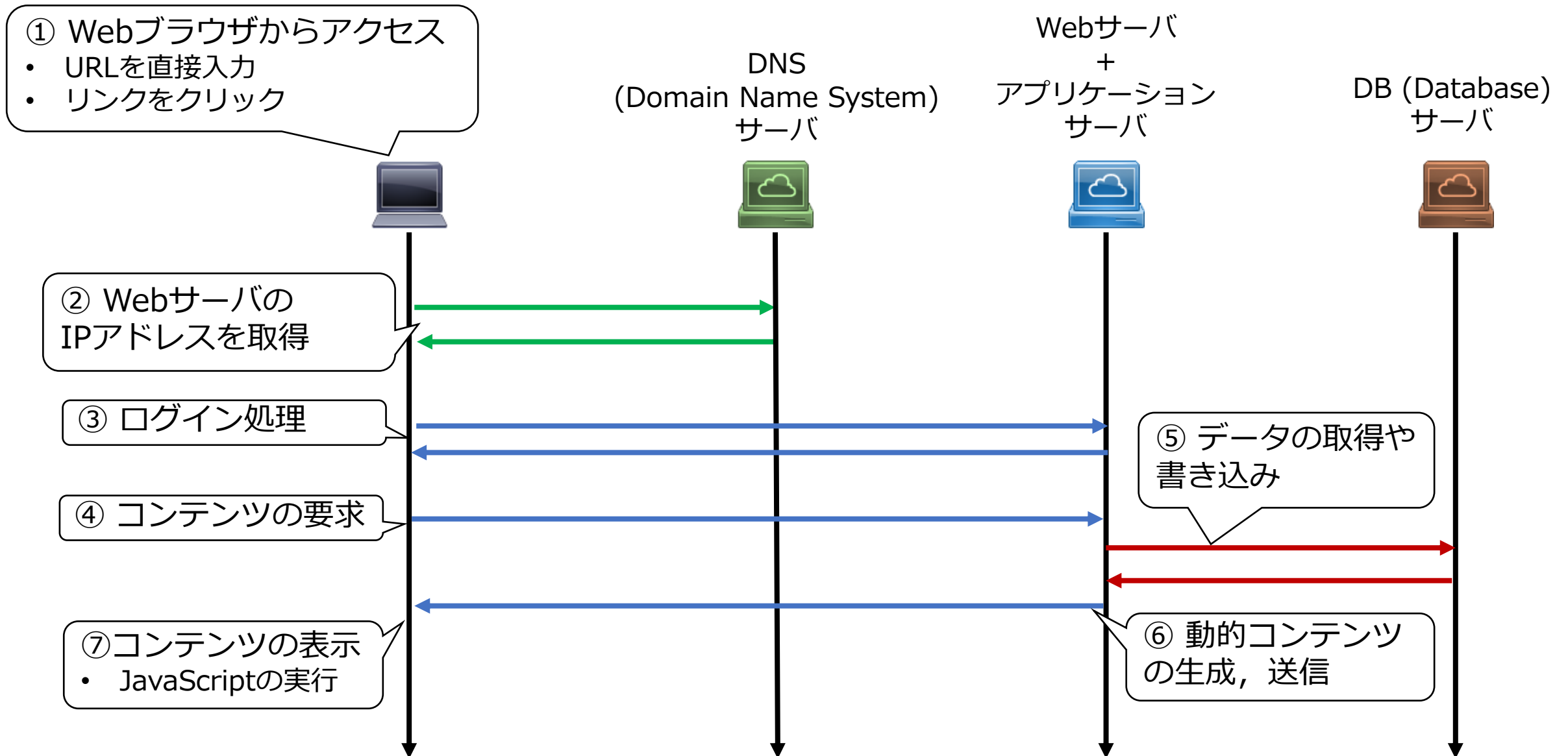
第5回 アプリケーションの通信に関する脅威（1）

藤本 章宏

今回の目標

- HTTPの動作について確認する
- HTTPのセッション管理における脅威について
簡単な演習を通し確認する

Webサービスにおける典型的な通信の流れ



URL (Universal Resource Locator)

インターネット上の資源の位置を指定するための識別子

例 1

<https://133.42.55.12:10203/login/index.html>

<https://www.wakayama-u.ac.jp/aic/news/2023110700026/>

スキーム :
アクセスするための手続き

ホスト :
リソースを管理しているコンピュータ
ドメイン名 (IPアドレス) [: ポート番号]

パス :
リソースの (特にサーバ内の)
位置

例 2

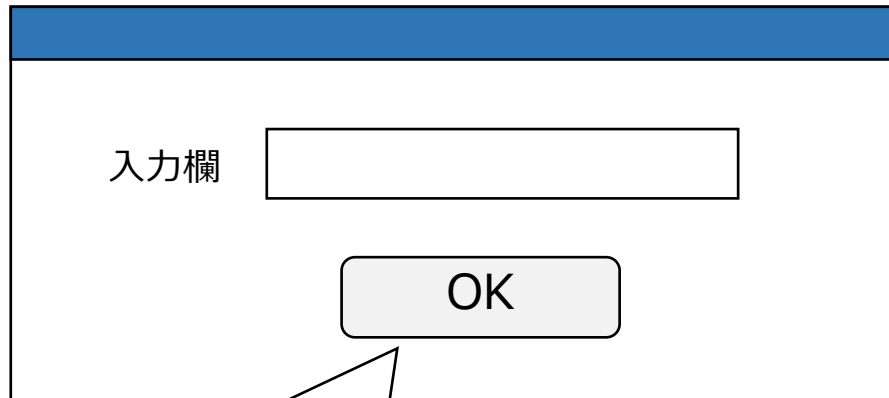
<mailto:fujimoto@wakayama-u.ac.jp>

パス「fujimoto@wakayama-u.ac.jp」で表されるリソースにmailtoという手続きでアクセス

GETメソッドとPOSTメソッド

どちらのメソッドを使っても
サーバに情報を渡すことができる

例：フォーム内容の送信



OKボタンを押すと
入力内容をサーバに送信

GETメソッドでも
POSTメソッドでも送信可能

GETメソッド

- 入力内容に紐づいた情報を閲覧したい場合に使う
例：検索キーワード
- URLの後ろに入力内容が付加

GET /a.html?input=xxx HTTP/1.1

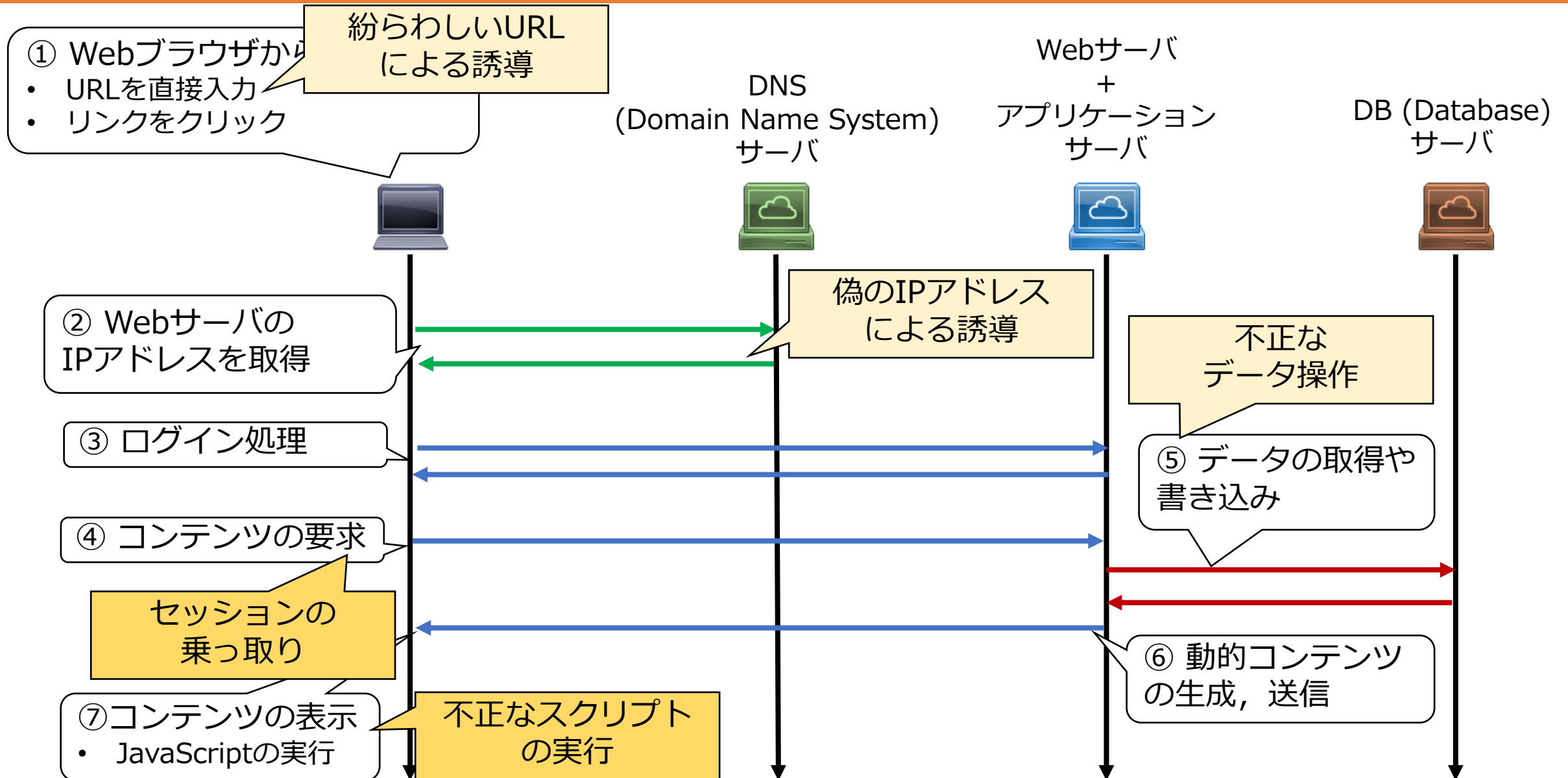
クエリストリング (URLパラメータ)

- Webサーバのログに (URLとして) 入力内容が残る

POSTメソッド

- 入力内容を登録したい場合や、入力内容进行处理した結果が欲しい場合に使う
例：ユーザ登録, ログイン処理
- 入力内容はメッセージボディに記載され送信される
- Webサーバのログには残らない

攻撃者が狙うポイント



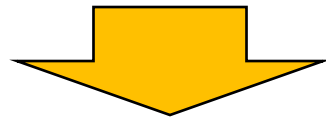
HTTPにおけるセッション管理

HTTPは元々ステートレス (=過去のやり取りを覚えてない)

- 1組のリクエスト・レスポンスで処理が完結
 - ✓ 設計をシンプルにでき, サーバの負担が少ない
 - ✓ 複数のサーバ間での負荷分散が容易
- 静的なWebページを表示するだけならば, ユーザの情報は不要

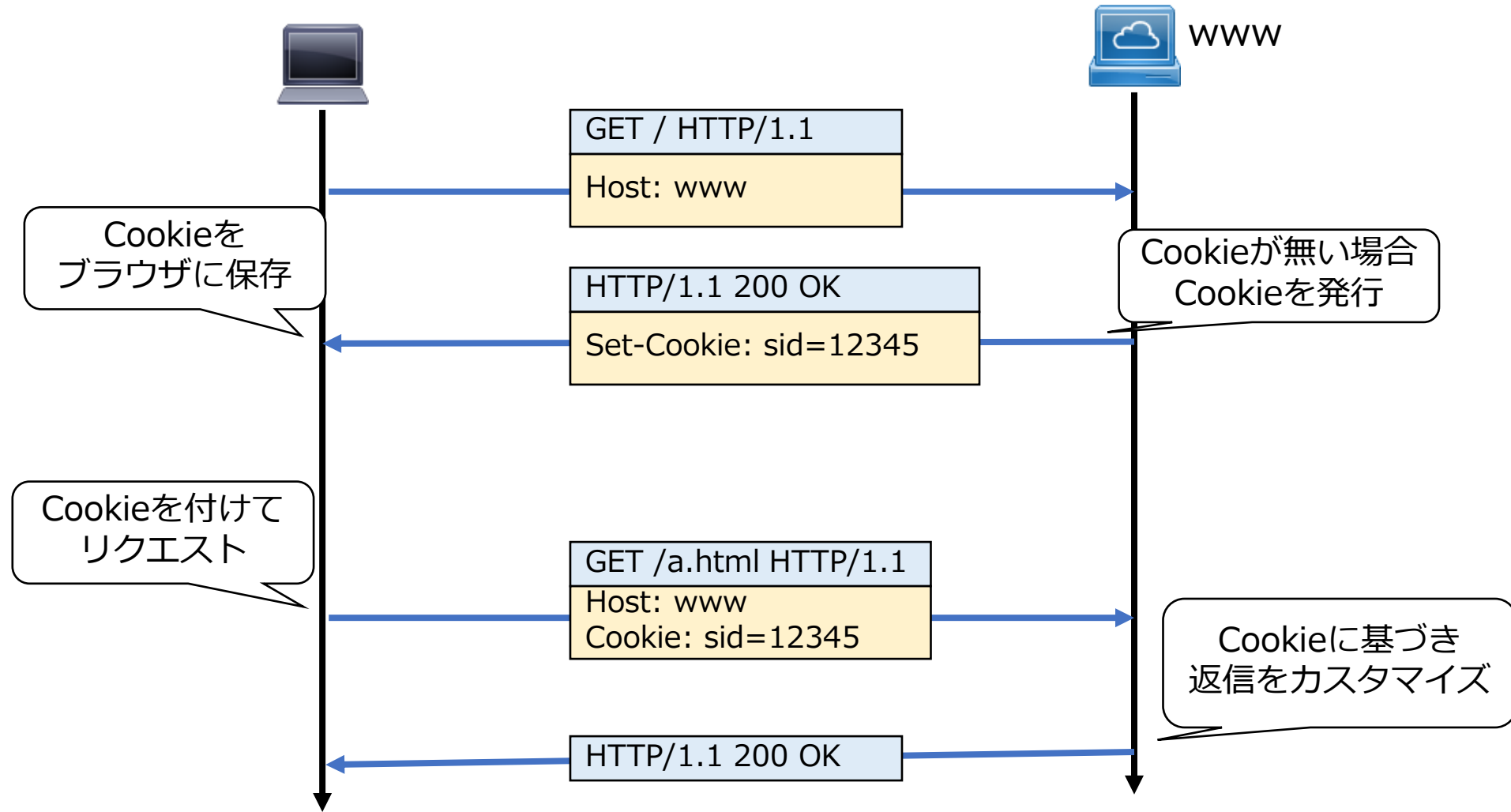
ステートレスのままだと, 複雑なサービスを実現できない

例: ショッピングサイトを作ろうとしても, 買い物カゴの中身を覚えておけない



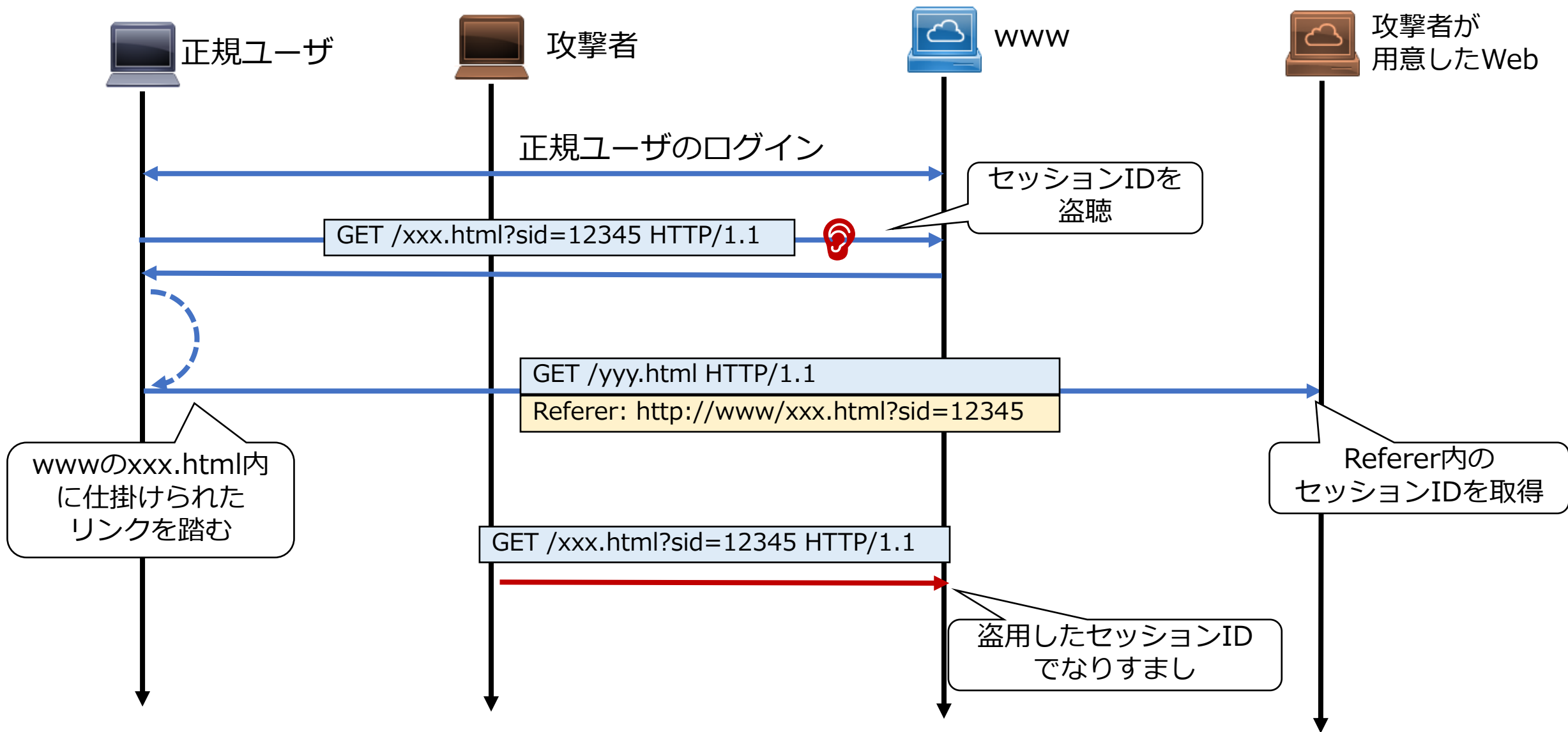
- サーバからのレスポンスにユーザ情報を格納
 - ✓ 典型的な例では, ユーザIDやセッションID
- リクエスト時に, ユーザ情報を提示
 - ✓ サーバは提示された情報を元にリクエストを処理

Cookieを用いたユーザ情報のやりとり



メリット : 情報交換が容易.ユーザ情報を一定期間, ブラウザに保管可能
デメリット : Cookieの取り扱いによっては攻撃に利用される

セッションIDの盗用



演習：Cookieの盗用

ログイン済みのセッションIDがわかった場合、
本当になりすませるでしょうか？

- ① Webブラウザのシークレットモードを開く
 - Ctrl + Shift + N で開くと思います
- ② 演習用Webサイトにアクセスして、
ログイン画面が表示されることを確認
- ③ F12キーを押して、開発者ツールを開く

ようこそ **test** さん

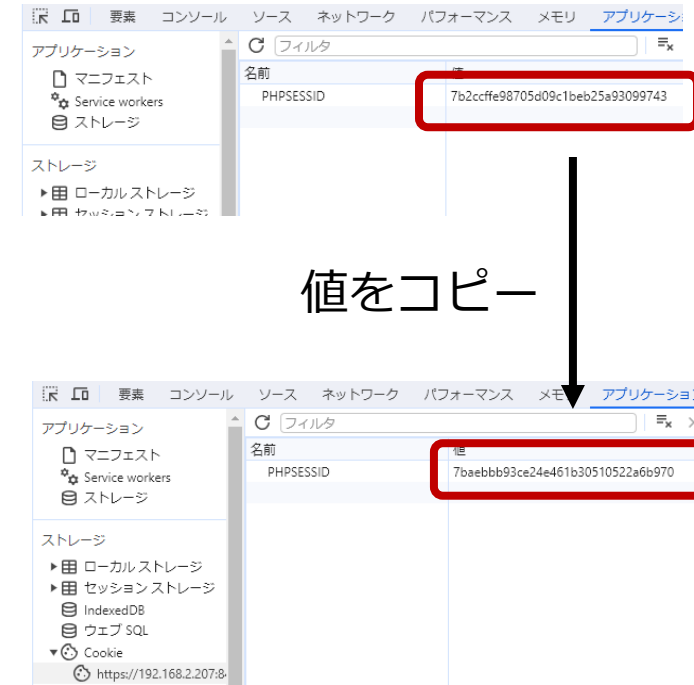
ログアウト

Login

Username

Password

Login

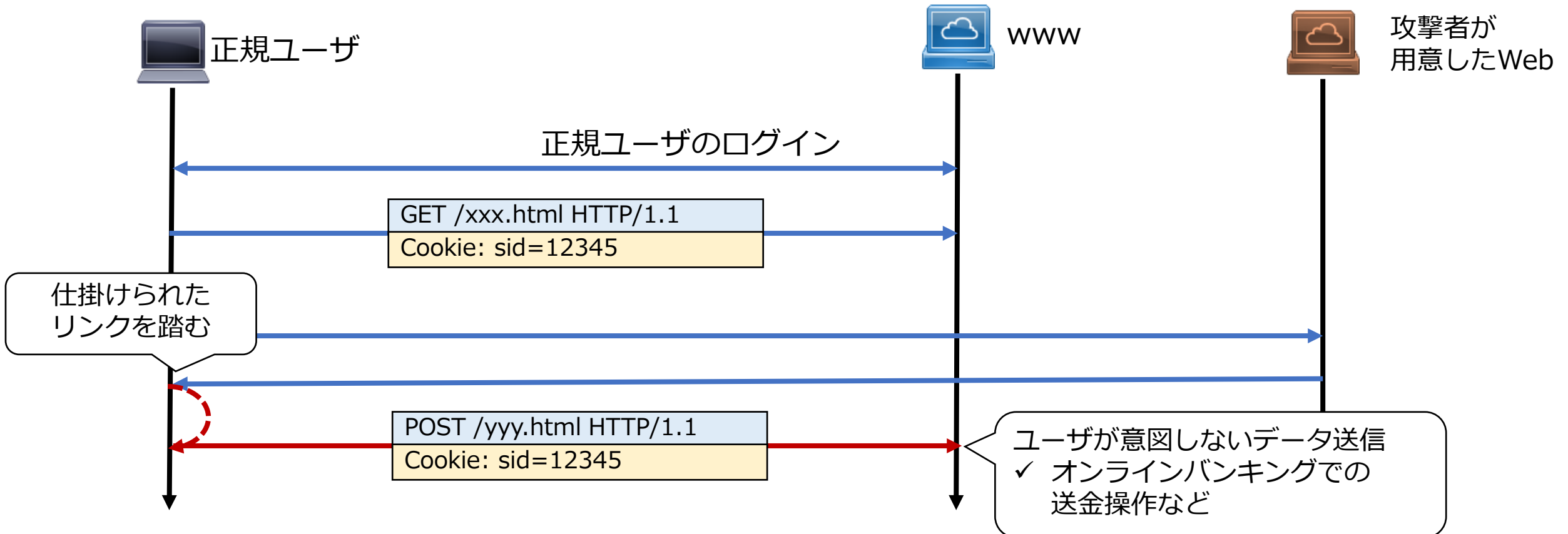


CSRF (Cross Site Request Forgery)

ログイン済みの状態が維持されることを悪用して、不正にリクエストを送信させる

✓ リクエストするのはユーザ自身

□ 攻撃者はセッションIDを取得する必要がない



不正にスクリプトが実行可能なWebサーバ

ユーザからの入力をそのまま埋め込んでしまうWebサーバ

期待される動作

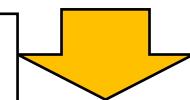
名前	aaa
e-mail	aaa@bbb.jp
登録	



名前	aaa
e-mail	aaa@bbb.jp
上記の内容で登録してもよろしいですか？	
OK	

不正な入力の場合

名前	<script> ~ </script>
e-mail	aaa@bbb.jp
登録	



HTMLの中身

```
<div>
名前 <script>alert()</script>
</div>
```

alert	
OK	