

IT講演会資料

攻撃者の手口を知り、被害に遭いにくくする

クロスサイトスクリプティングとセッションハイジャック編



今日の講演会で使うサイトです
スマホを持っている人はアクセスしてみよう！

http://.azurewebsites.net



こんな画面が
出てくるよ→

localhost:52545

あなたのお名前を教えてください。

お名前 OK

localhost:52545/Home

こんにちは、nakamura さん！

あなたのひみつを教えてください。

ひみつ OK

↓↓

を聞いたよ

実際に 起こった事件

2010年9月21日ITMedia社掲載の記事より抜粋
出典

<http://www.itmedia.co.jp/news/articles/1009/21/news111.html>

速報

🕒 2010年09月21日 22時33分 更新

Twitterの脆弱性突くコードが拡散 Webブラウザでのアクセス自粛呼び掛け

Twitterの脆弱性を突いたコードが急速に拡散し、意図しないツイートをしてしまうケースなどが多発。当面、WebブラウザからTwitterにアクセスしないなどの対策が必要だ。 **UPDATE**

[ITmedia]

21日23:10追記

Twitter公式ブログが脆弱性の修正を報告（[英文](#)）。だが全Twitterサーバに修正が反映されるまで時間がかかる可能性もあるため、当分は要注意。

Twitterの脆弱性を使ったコードが急速に拡散し、意図しないツイートをしてしまうケースなどが多発している。当面の対策として、WebブラウザからTwitter公式ホームページにアクセスしないなどの対策をセキュリティソフト会社やユーザー有志が呼び掛けている。

[Kaspersky Labのブログ](#)によると、Twitterに存在するクロスサイトスクリプティング（XSS）の脆弱性が原因。ツイートにスクリプトを埋め込んだり、外部サイトからスクリプトを呼び出すなどしてユーザーに実行させることが可能になっている。ユーザーにツイートを連鎖させるコードも出回っており、急速に広がっているようだ。

コードによっては、ログイン状態でWebブラウザからTwitterにアクセスしてコードを表示させただけで自動的に実行されてしまうものもあるため、（1）ログアウトする、（2）WebブラウザのJavaScriptを無効にする、（3）WebブラウザでTwitter公式ホームページにアクセスしない（安全が確認されているTwitterクライアントソフトを使う）——といった対策が必要。Twitterが公式に脆弱性を修正したとアナウンスするまでは要警戒だ。

クロスサイトスクリプティング

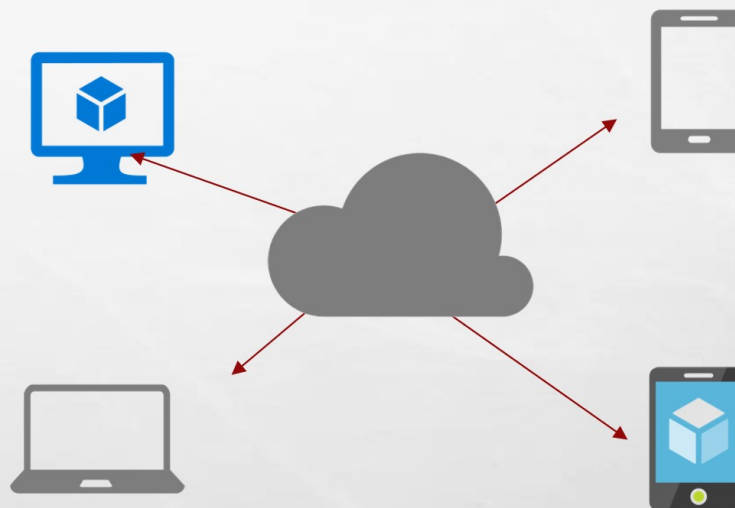
「クロスサイト（サイト横断）」という名称は歴史的なもので、初期に見されたXSSでは脆弱性のあるサイトと攻撃者のサイトを「サイト横断的」に利用して攻撃を実行する事から名づけられたもの

（Wikipedia クロスサイトスクリプティングより出典）

INTERNETの仕組み

インターネット

- 片一方からデータを送ると、反対側からデータが出てくる
- エンドシステムのみで動作している



URLについて

(Uniform Resource Locator)

- インターネット上のリソースに対する識別情報

<http://www.jmooc.jp/index.php>

アクセス方法
(スキーム)

リソースが存在するホスト

対象ホスト内のリソース

ブラウザ



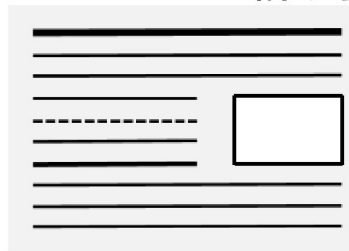
ブラウザの役割 HTMLの解釈と描画(レンダリング)

HTMLファイル

```
<!DOCTYPE html>  
<html lang="ja">  
...  
<body>  
...  
</body>  
</html>
```

解釈

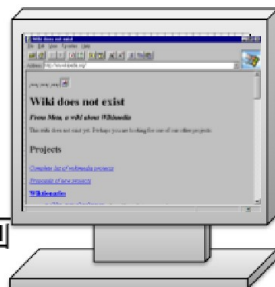
ドキュメントの構成要素



ビットマップディスプレイ

ピクセル(点)ごとに色(光)の発色を制御する方式のディスプレイ

描画

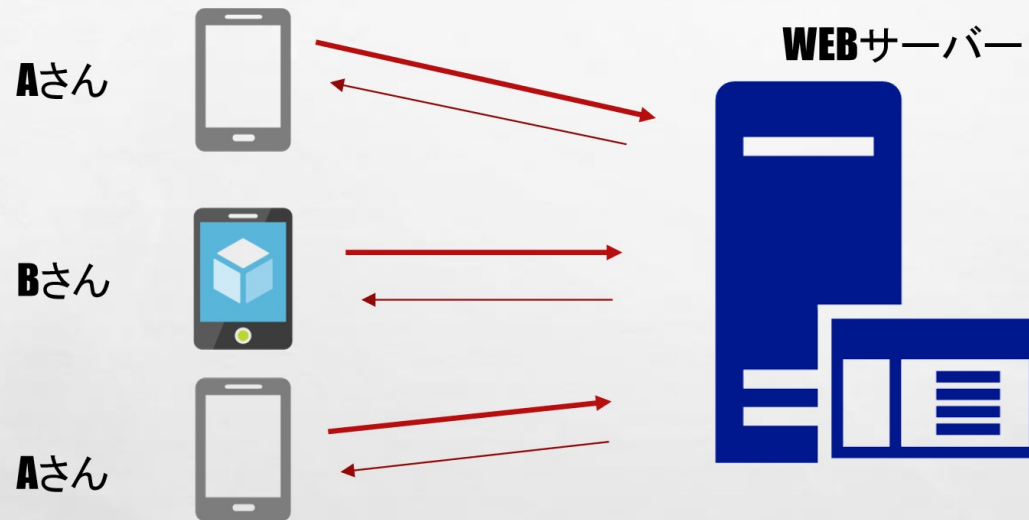


レンダリング

Htmlタグを自デバイス内で描画する

慶應義塾大学環境情報学部 村井純 教授
gakko 講義 インターネット より出典

STATE LESSとSTATE FULプロトコルとCOOKIE

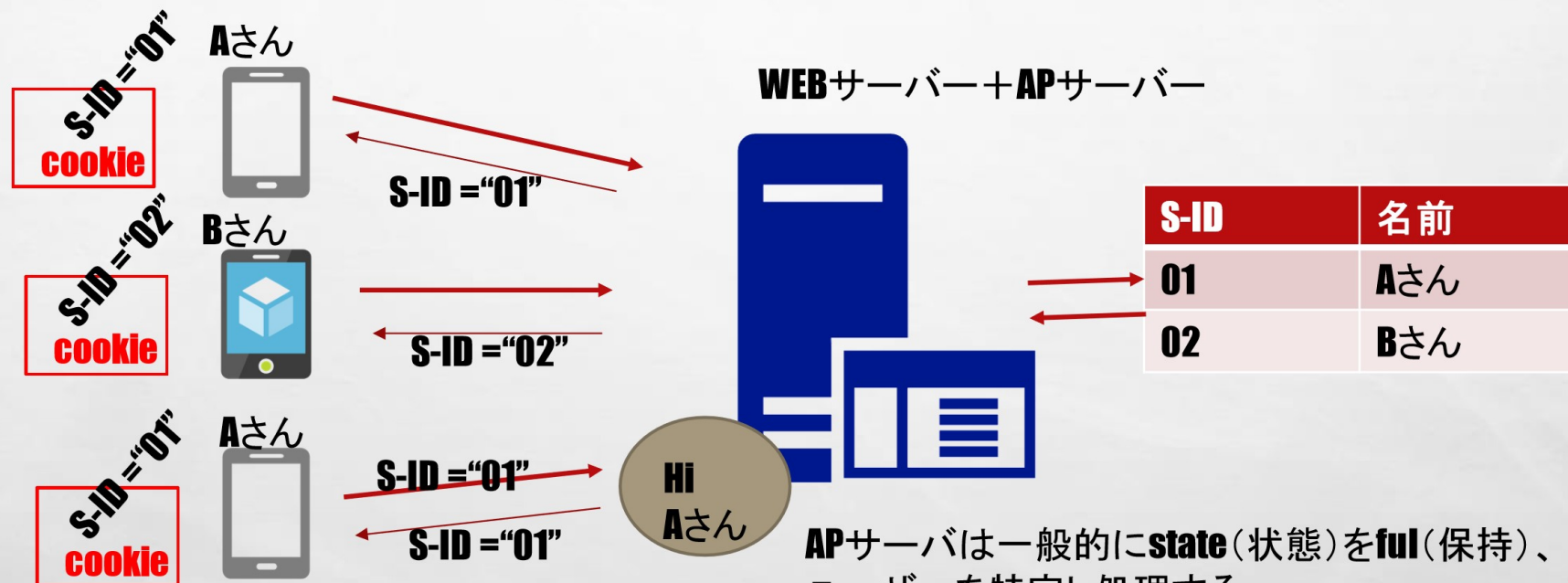


WEBサーバは1回のリクエストに対し1回のレスポンスを返すのみ

インターネットとの代表的な通信プロトコル**http(s)**は

state (状態)を**less** (保持しない)

STATE LESSとSTATE FULプロトコルとCOOKIE



APサーバは一般的に**state**(状態)を**ful**(保持)、ユーザーを特定し処理する
その方法としてサーバーは相手先毎に**key**を発行して、クライアントはその**key**を**cookie**に格納、その後のアクセスはそれを用いることで自身を特定させる

用意した**WEB**アプリケーション

主催者が用意したサイト

攻撃者が用意したサイト

localhost:52545

あなたのお名前を教えてください。

お名前

localhost:52545/Ho

こんにちは、nakamura さん！

あなたのひみつを教えてください。

ひみつ

↓↓

を聞いたよ

localhost:52545/Ho

こんにちは、nakamura さん！

あなたのひみつを教えてください。

ひみつ 本当はこんなことが...

↓↓

本当はこんなことが... を聞いたよ

[Click Here](#)

localhost

localhost:52545/Home

あなたの秘密は見せてもらいましたよ
1週間以内に 100,000円を子ども銀行に振り込みなさい。

収集したsessionは

mojiretuff2xvpu5r2jr4ykd1nrxb255 / tlensupw0vd3htxgopyfjwvx /
xkmntf0zrqeix0vvfoe4cc1r / 2uj2gyjudentl2dec5muiuhl /

[Go site](#)

攻撃者が設置したクロスサイト
スクリプティング
これをクリックするとセッションが
ハイジャックされる

攻撃者はハイジャックしたセッ
ションを使用して他者の情報を
盗み見る事ができる

どうしたらいい？

クロスサイトスクリプティングが仕掛けられる可能性があるサイトを撲滅することは難しい

- WEBをブラウジングしているときは、怪しいリンクやボタンはクリックしない
- クロスサイトスクリプティングは不特定多数のユーザーが書き込める箇所が一番危険
- 大切な情報を書き込むサイトでは、必要が無くなったら速やかにログアウトする
- ログインしたまま、別ドメインへのリンクをクリックしない

講師紹介



中村 茂

こんなことをしています…

- 世田谷区青少年喜多見地区委員会理事
- 世田谷区喜多見中部町会副会長
- 平成28年度 駒澤大学高等学校PTA(施檀会)会長
- 平成25年度 世田谷区喜多見中学校PTA会長

facebook: <http://www.facebook.com/mob.naka>

E-mail(PC) : mob.naka@gmail.com

Thank You