セコム IS研究所
Intelligent Systems Laboratory

XSS + CSRF対策編

JPNIC・JPCERT/CC
セキュリティセミナー2005
「Webのセキュリティ」

2005年10月6日

セコム IS研究所 新井 幹也

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

XSS + CSRF対策

Webアプリケーションの脆弱性である

本質的な対策はWebアプリケーション開発者が行う
Webアプリケーション脆弱性に対して各フェーズで対策

仕様策定・設計
- 製品・言語選定
- 認証方式
- セッション管理方式
- データベース設計
- リソース管理方式

実装
- 境界チェック
- 入出力チェック
- コードチェッカーの利用
- 変数初期化の励行

テスト
- 攻撃者の視点
- 検査ツールの活用

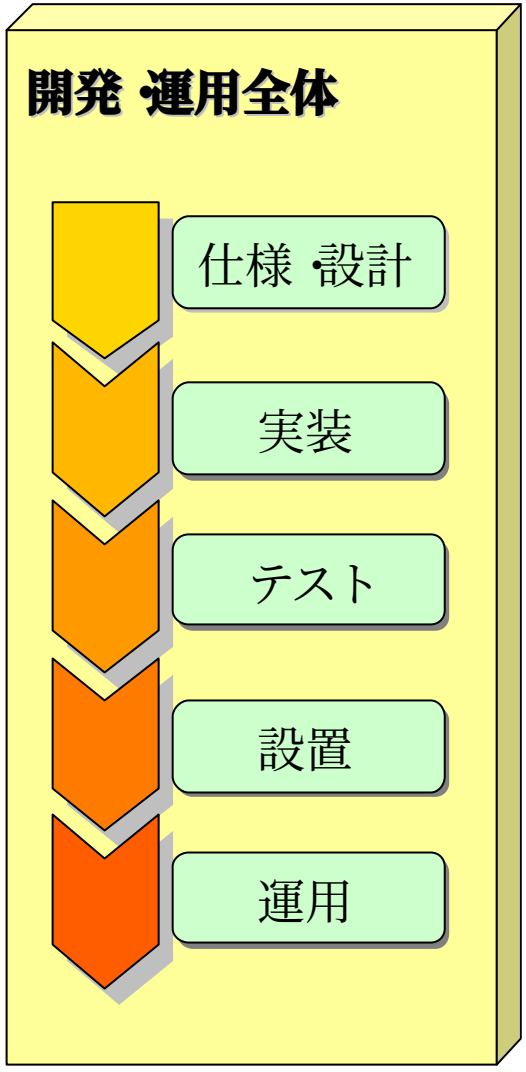
設置
- 各サーバ(Web, DB,…)の設定
- 不要なサービスの停止
- 要塞化
- ログ取得設定

運用
- 定期的な脆弱性診断
- パッチ管理・適用
- 稼動監視
- ログ監視
- 不正侵入監視
- 脆弱性情報収集

運用でできること、すべきことも多くある

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セキュアな開発・運用 各役割



要求仕様の段階では

- 顧客から求められている機能自体が脆弱でこれを悪用される恐れも…

→ 受注側が機能の危険性について説明でき、代替機能の提案までできると理想。**要求仕様を作成する役割の人**が機能が悪用されないかという視点を持っていることが重要。

設計の段階では

- セッション管理手法などの状態管理手法の選択を誤ると…

→ システムの設計や実装方針を決定する**アーキテクト**が、セキュアシステム構築のための知識や視点を持っていることが必要。

実装の段階では

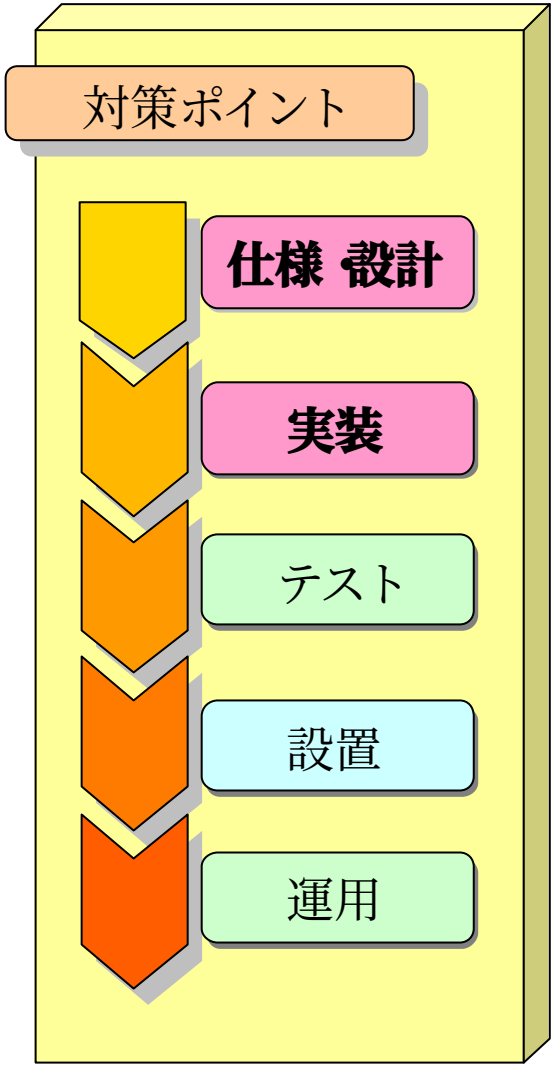
- SQLインジェクションやXSSを引き起こさないために…

→ **プログラマ**が悪意のある入力を排除するためのプログラミング技術に対して精通していることが必要。

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

XSS対策



入出力チェック

- 入力データ・出力データの明確な仕様策定
- 入出力値のチェック
  - 入力時のチェック
  - 出力時の変換
    - < → <、> → &gt など の変換
    - PHP :htmlspecialchars() など

セッション管理強化

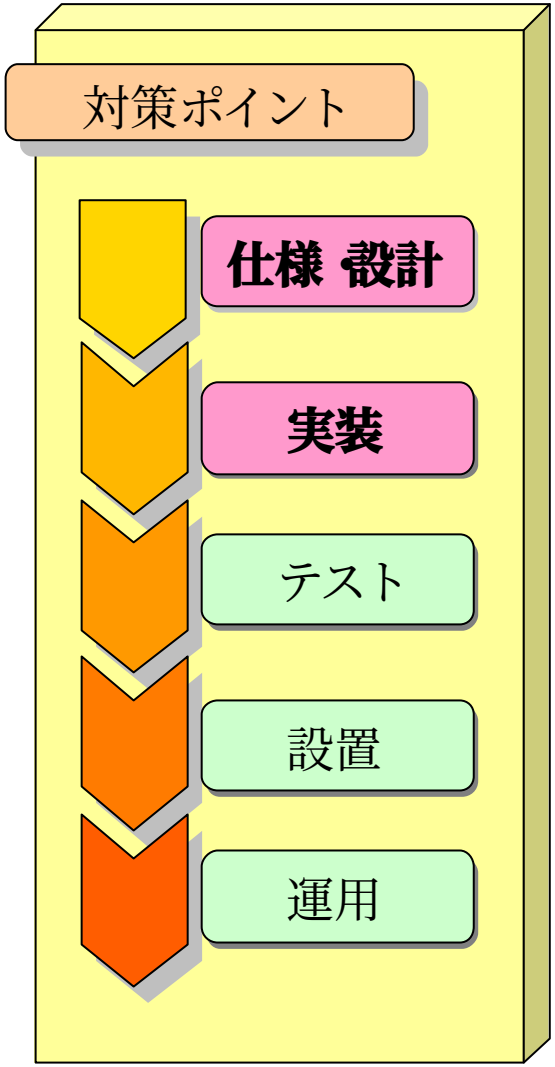
- HttpOnlyフラグの利用
  - JavaScriptからdocument.cookie の値を読めなくする
  - ただし、有効なのは IE6sp1以上

Set-Cookie: value=72w3er64twefs0;
expires=Wednesday,
09-Nov-99 23:12:40 GMT; **HttpOnly**

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策



セッション管理強化

- リファラをチェックする
  - Webアプリケーションの遷移上、存在しないパスを通ることが無いように設計し、存在しないパス上からの遷移を受け付けない
- 予測困難な情報を利用
  - 遷移前のページに、予測困難な情報をいれ、遷移後のページにおいて一致を調べる

その他

- GETよりPOSTの利用
  - 根本対策ではないが…
- 画像を利用した入力確認
  - CAPTCHAの利用

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策
POSTへの変更の考察

JavaScriptの利用により、自動的にPOST送信されることがある。

→ 実例：「はまちちゃん Ver.3」

http://www.example.com/cgi-bin/1.cgi?n=名前&m=メッセージ&v=1

```
<body onLoad="document.commit.submit.click();">
<form name=“commit" method="post" action="http://www.example.com/cgi-bin/1.cgi">
<input name=“n” type=“hidden” value=“名前”></td>
<input name=“m” type=“hidden” value=“メッセージ”></td>
<input name=“v” type=“hidden” value=“1”></td>
<input type="submit" name="submit">
</form>
```

効果が無いわけではない

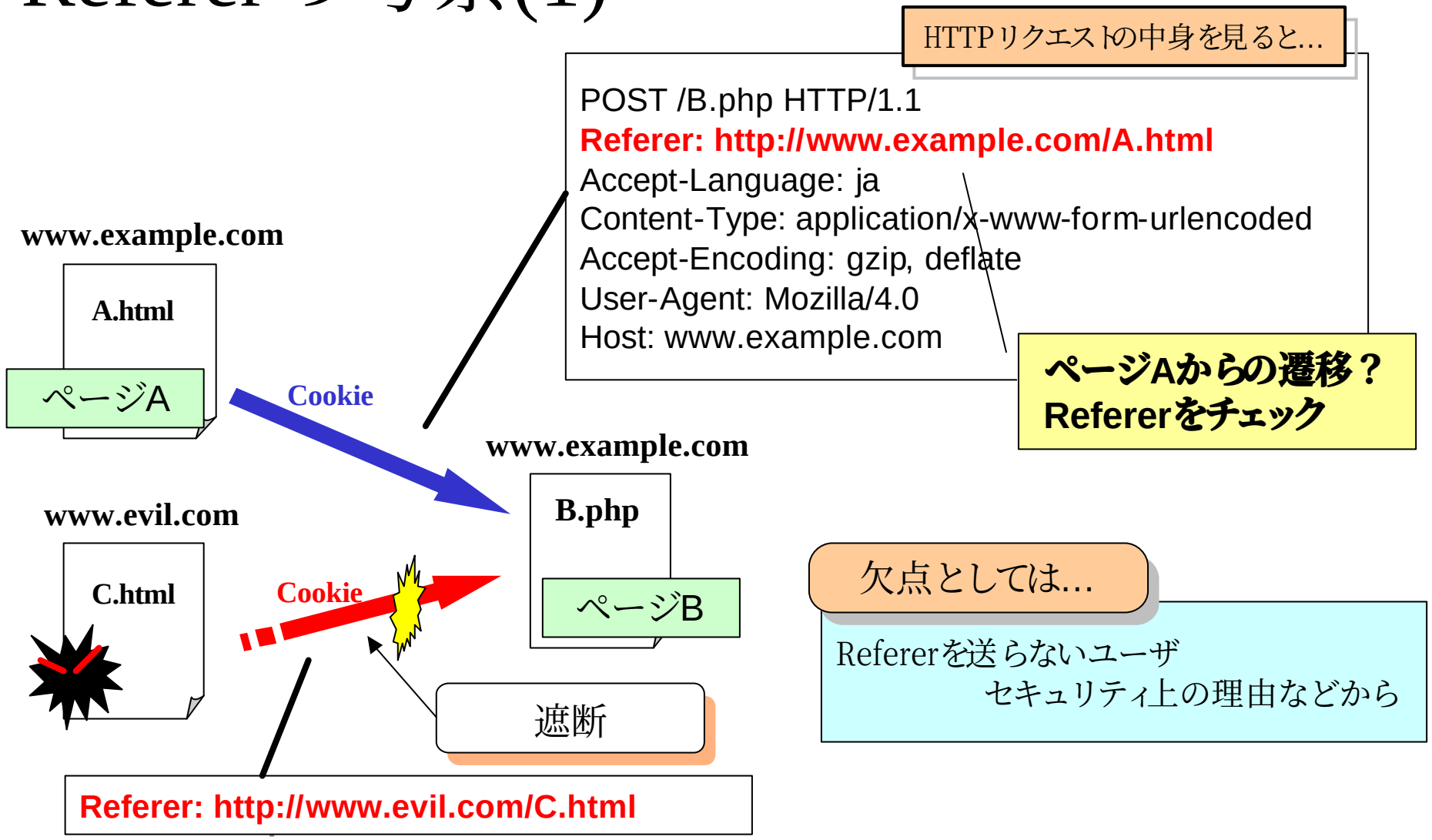
単純なリンクやIMGタグを利用した方法では攻撃が実現しなくなり、脆弱性悪用のための敷居が上がる

→ GET・POSTどちらを使うか設計時点で場面に応じた充分な考慮が必要

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策
Refererの考察(1)



Copyright © 2005 SECOM Co., Ltd. All rights reserved.

CSRF対策 Refererの考察(2)

セコムIS研究所 Intelligent Systems Laboratory

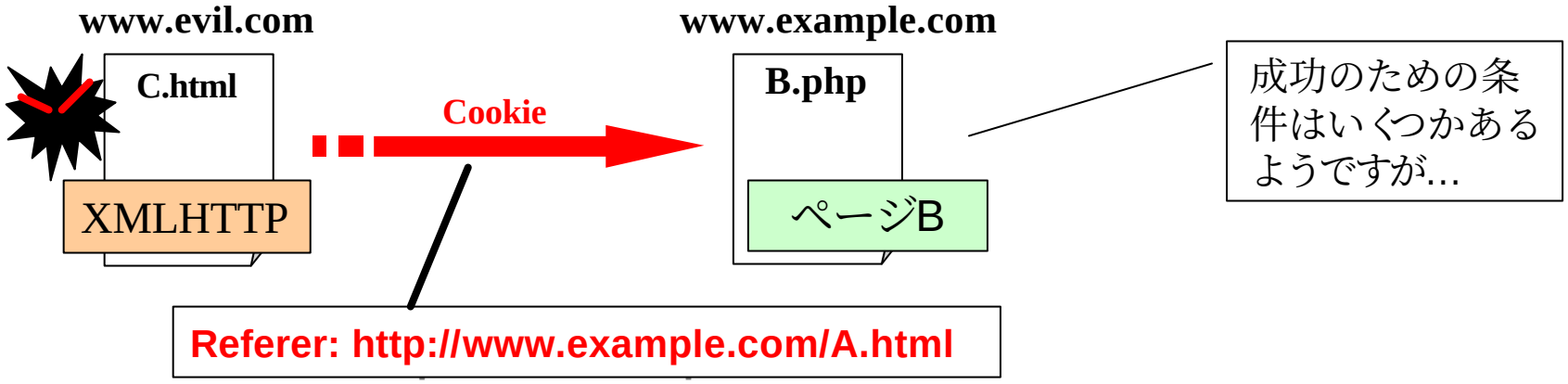
脆弱性情報

IE6にパッチ未提供の脆弱性、HTTP Request偽装の恐れ(2005/09/27　INTERNET Watchより)

IEにまたパッチ未公開の脆弱性--セキュリティ専門家が警告(2005/09/29　CNET Japanより)

→ Secuniaよりアドバイザリ
Microsoft Internet Explorer "XMLHTTP" HTTP Request Injection

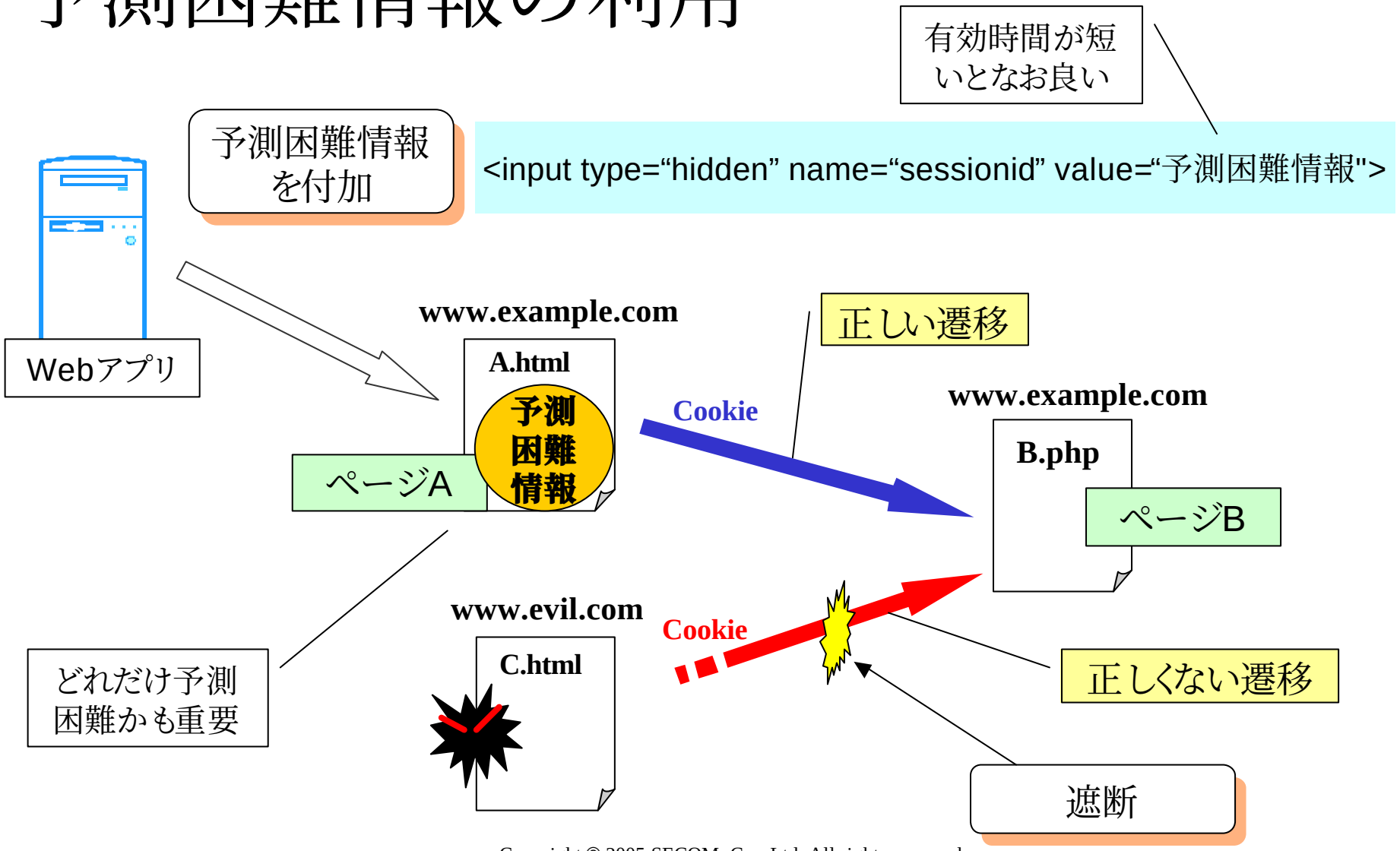
→ 詳細な情報は…
websecurity@webappsec.org への2005/09/25の投稿
“Exploiting the XmlHttpRequest object in IE ”



Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策
予測困難情報の利用



Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策
CAPTCHAの考察(1)

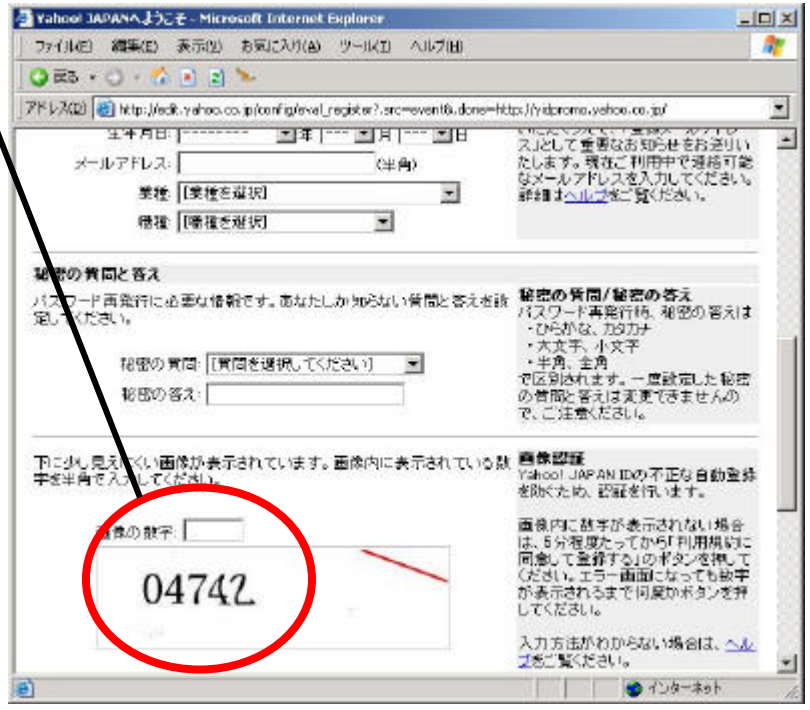
- Completed Automated Public Turing tests to tell Computers and Humans Apart
  - http://www.captcha.net/
- 人間なのか？コンピュータなのか？を見分ける手法

人間ならば読めるがコンピュータでは読みにくい、という特徴を利用する

ユーザ登録時などに人間が登録をしているのか自動化ソフトなどで登録しているのかを見分ける

http://en.wikipedia.org/wiki/Image:Captcha.jpgより

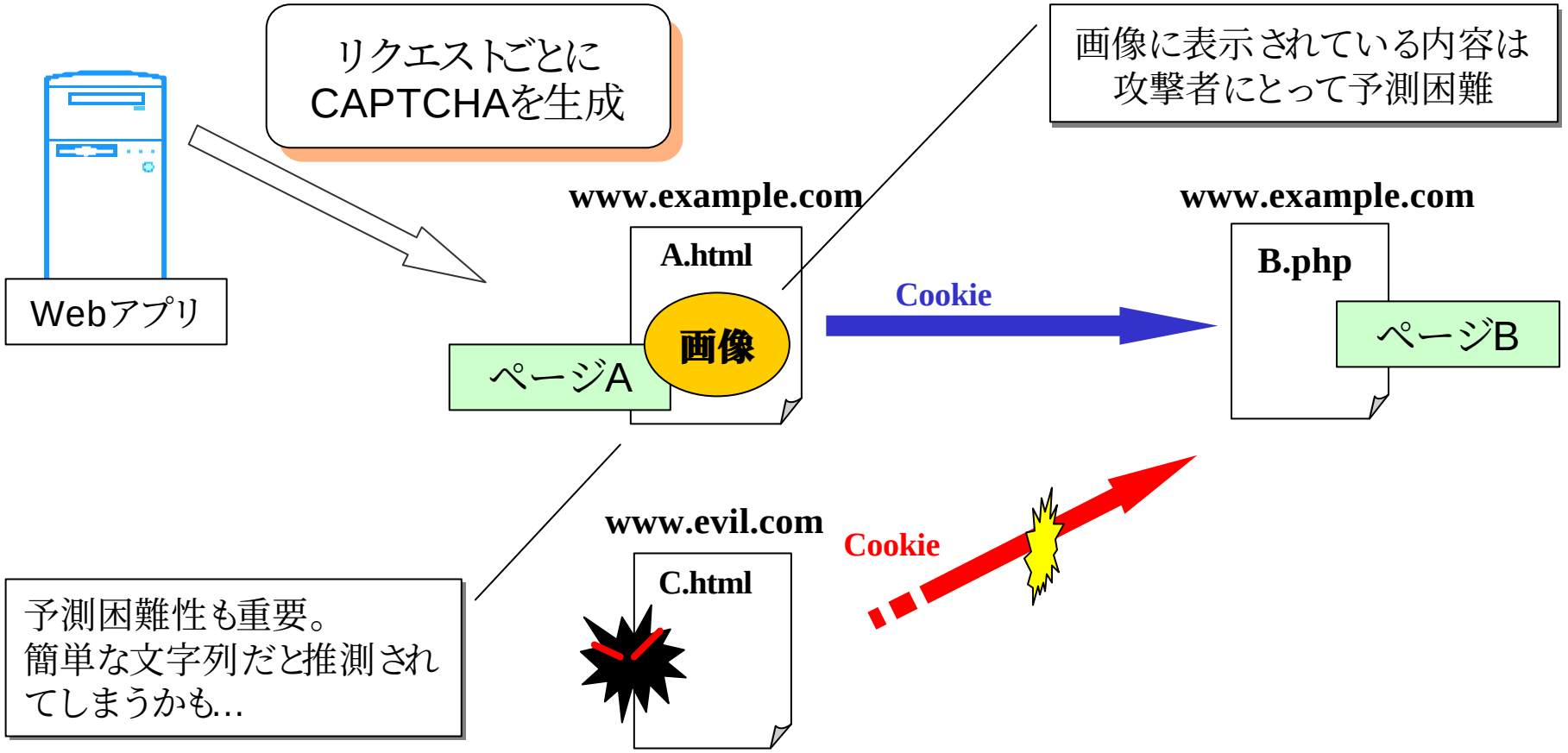
SMWM



http://edit.yahoo.co.jp/config/eval_register?.src=event&.done=http://yidpromo.yahoo.co.jp/

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

CSRF対策
CAPTCHAの考察(2)



Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

CSRF対策 重要なのは…

リスクとの関連

- CSRFの脆弱性を利用されることでどんなことが発生するか？
- 必ずしも全てのリクエストに対策を施す必要はないと考えられる
- 影響の大きな処理を行う箇所の対策

対策に利用する技術の可能性

- 取っていた対策が時間が経過するにつれて効果が下がってくる可能性も

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

Webアプリケーション脆弱性対策

セコムIS研究所
Intelligent Systems Laboratory

Webアプリ開発者

?セキュアな開発の推進
?脆弱性と対策の正確な知識

ネットワークオペレータ

•Webアプリのセキュリティ検査
•管理下Webアプリの脆弱性対策
?WAFの導入検討

一般ユーザ

?利用PC・Webブラウザの脆弱性除去
?脆弱性発見の際の届出

参考

ドキュメント

•OWASP Guide
•WASC Threat Classification
•ウェブサイトのセキュリティ対策の再確認を
～脆弱性対策のチェックポイント～

団体・コミュニティ

•WASF
•OWASP東京支部
•WebAppSec

制度

•脆弱性関連情報の取り扱い

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

参考

- ドキュメント
  - OWASP Guide
    - http://www.owasp.org/documentation/guide.html
  - WASC Threat Classification(脅威の分類)
    - http://www.webappsec.org/projects/threat/v1/WASC_TC-1.0.jpn.pdf
  - ウェブサイトのセキュリティ対策の再確認を～脆弱性対策のチェックポイント～
    - http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

Copyright © 2005 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

参考

- 団体・コミュニティ
  - WASF(Web Application Security Forum)
    - SQLインジェクション対策をまとめた文書を公開
      - http://www.wasf.net/wg-eval-sql200509.pdf
  - OWASP東京支部
    - 第一回のミーティングが開催
      - http://www.owasp.org/local/tokyo.html
  - WebAppSec
    - https://www.webappsec.jp/
- 脆弱性関連情報の取り扱い
  - http://www.ipa.go.jp/security/vuln/report/index.html

Copyright © 2005 SECOM Co., Ltd. All rights reserved.