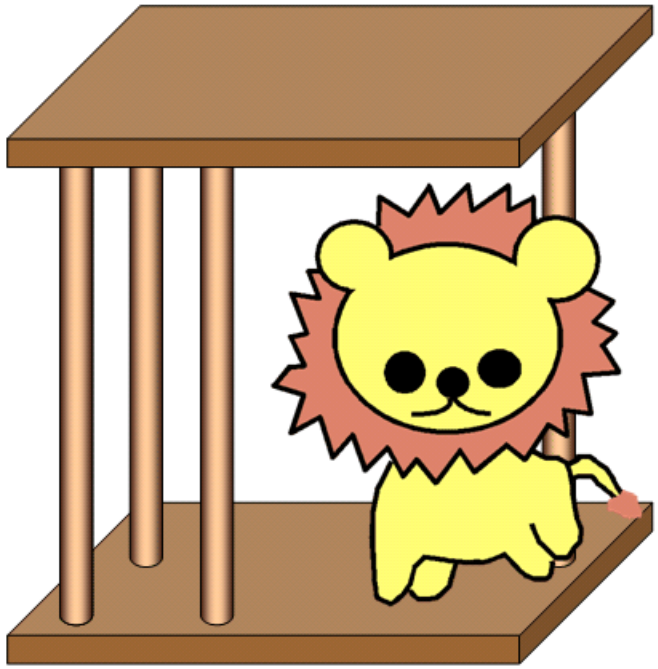
WAF入門
～原理･効果･限界～



2008年9月27日

徳丸　浩

アジェンダ

- WAFとはなにか
- 商用WAFについて
- 防御の実際
- まとめ(WAFとどう付き合うか)

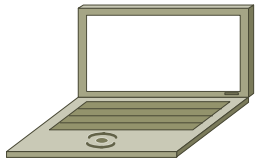
Copyright © 2008 HASH Consulting Corp.

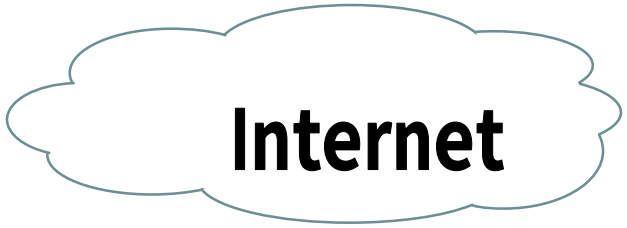
WAFとはなにか

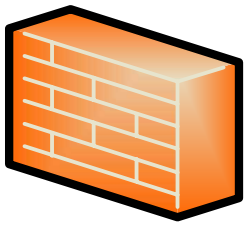
- HTTPリバースプロキシ方式で Webアプリの攻撃から防御するツールと考えると分かりやすい
  - mod_proxy, mod_waffulなどは例外
- WAFの防御戦略
  - 入力値検証
    - ホワイトリスト
    - ブラックリスト
    - 不正な文字エンコード、特殊文字(ヌルなど)
  - 画面遷移の検証
    - 外部からの入り口
    - 内部の遷移
  - 値の保護
    - Cookie
    - Hidden / Radio Button …

Copyright © 2008 HASH Consulting Corp.

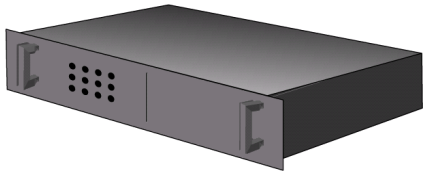
WAFの配置







Firewall



WAF

リバースプロキシ型
透過型(ブリッジ型、ルータ型)

Web Server

Copyright © 2008 HASH Consulting Corp.

本日のデモ環境

Web Application (Perl CGI)

vmware

CentOS

VMware Player

Microsoft Windows xp

WAF (JPSecure SiteGuard)

vmware

SiteGuard

CentOS

VMware Player

BurpSuite1.1

Copyright © 2008 HASH Consulting Corp.

WAFの変遷

ソフトウェアタイプ

旧Sanctum AppShield →WatchFire → F5(ディスコン)
旧KaVaDo InterDo →Protegrity(日本では販売停止)
F-Secure Site Guard →(スピンアウトしてJP-Secureに)
Kanatoko Guardian@JUMPERZ.NET(オープンソース)

アプライアンス

旧MagniFire TrafficShield →F5 BIG-IP Application Security Manager
旧Teros Secure Application Gateway
→Citrix Application Firewall
NetContinuum NCシリーズ →Barracuda Web Site Firewall
→Barracuda Web Application Controller
SecureSphere Imperva

Copyright © 2008 HASH Consulting Corp.

WAFの宣伝文句は目に余る

要件6.6対応はWAFの導入が必須要件
特に要件6.6の「Webアプリケーションに対する既知の攻撃に対する防御」においては、これまで「推奨する」にとどまっていたものが、2008年6月30日以降は「必須となり、WAF（Webアプリケーション・ファイアウォール）の導入が不可欠」に変わります。つまり何らかの形でカード決済に関わる処理を持つWebサイトにはWAFが必要になります。
http://www.f5networks.co.jp/solution/topics/pcidss/waf.html

6.6 Ensure that all web-facing applications are protected against known attacks by applying **either** of the following methods:
• **Having all custom application code reviewed for common vulnerabilities** by an organization that specializes in application security
• **Installing an application layer firewall** in front of web-facing applications.
Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

Copyright © 2008 HASH Consulting Corp.

ホワイトリスト防御の問題点

- 使える場所が限定される
  - 数値項目、メールアドレス、ID類、選択肢など
- ユーザのご入力後のフォローがなく、ユーザビリティが下がる(デモで)
- 設定が面倒(項目ごとに設定要)

- つまり、手間がかかる割りに、誰も嬉しくないというWAFの三重苦を象徴する結果に
  - 割高で　あてにならぬも　負担増

Copyright © 2008 HASH Consulting Corp.

ブラックリストこそ本命

- ブラックリストは使う場所をあまり選ばない
- ブラックリストで弾かれでもユーザには違和感は与えにくい…はず
  - 郵便番号欄に英字記号をうっかり入れたユーザには、親切にナビゲーションする必要がある
  - 住所欄に　”><script>alert .. を入れるような輩には厳しく対応して差し支えないww
- ブラックリストの管理が面倒なのはベンダー側であって、ユーザ側ではない
  (一方、ホワイトリストはユーザ側が面倒)

Copyright © 2008 HASH Consulting Corp.

難読化に対する神話

- JavaScriptやSQLの難読化により、WAFをすり抜けられるという発言があるが・・・
- 難読化はそれほどでもよ・・・

はみ出す部分

難読化を解く部分

```
z';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x440045004300...7200%20AS%20NVARCHAR(4000));EXEC(@S);--
```

出展:http://blogs.technet.com/neilcar/archive/2008/03/15/anatomy-of-a-sql-injection-incident-part-2-meat.aspx

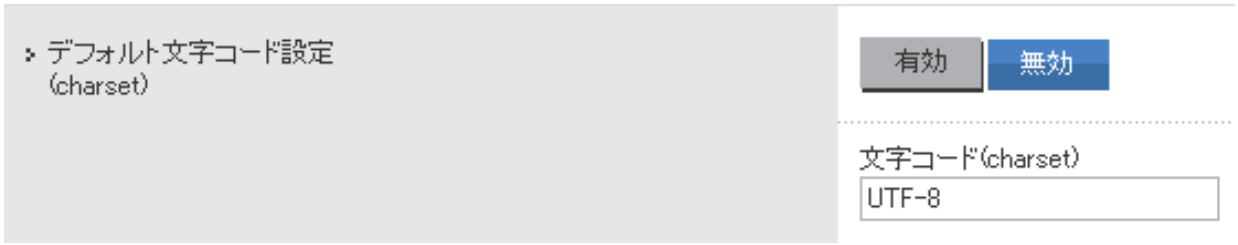
- 攻撃コードの目的は難読化できるが、
  - 文字列リテラルを「はみ出す」部分は難読化できない
  - 難読化を元に戻すコードは難読化できない
- まともなシグネチャなら、難読化されていても対応可能

Copyright © 2008 HASH Consulting Corp.

文字コードどうする?

- 半端なShift_JIS
- 冗長なUTF-8
- みんなUTF-7が大好きだwww

- 不正な文字コードのチェックで対応可能
- デフォルト文字エンコードの設定



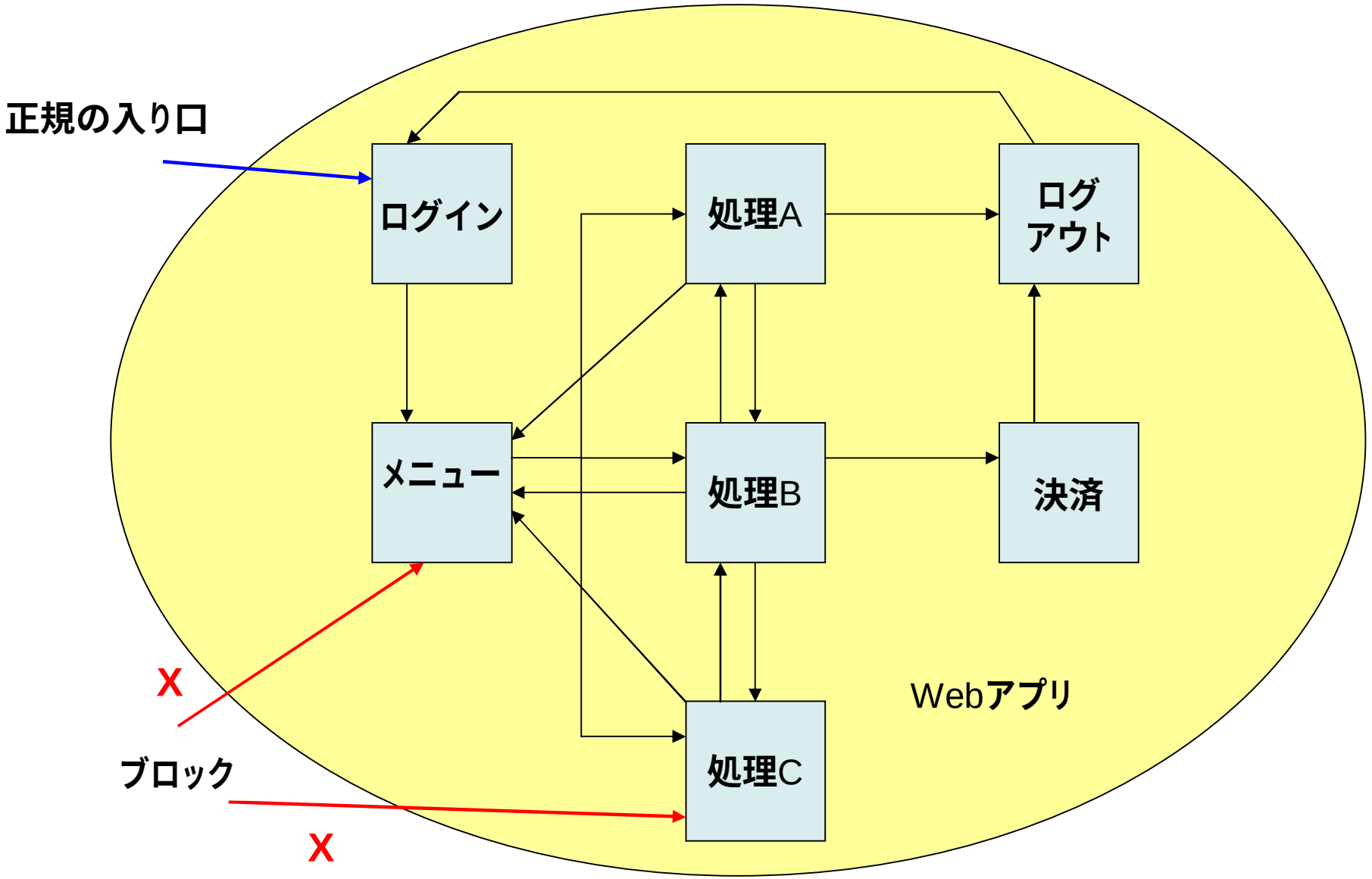
Copyright © 2008 HASH Consulting Corp.

画面遷移のチェックは・・・

- 画面遷移のチェックは二種類ある
  - 外部からの入り口となるページを限定し、それ以外のページは、外部からの遷移を拒否する
  - 内部の遷移も決まった遷移のみを許容する
- 運用上の問題が多い
  - ユーザにとっては不便
  - SEO上不利になる場合も
  - 内部遷移を厳重にチェックすると、戻るボタンが使えなくなる
- そのわりに防御効果が薄い(後述)

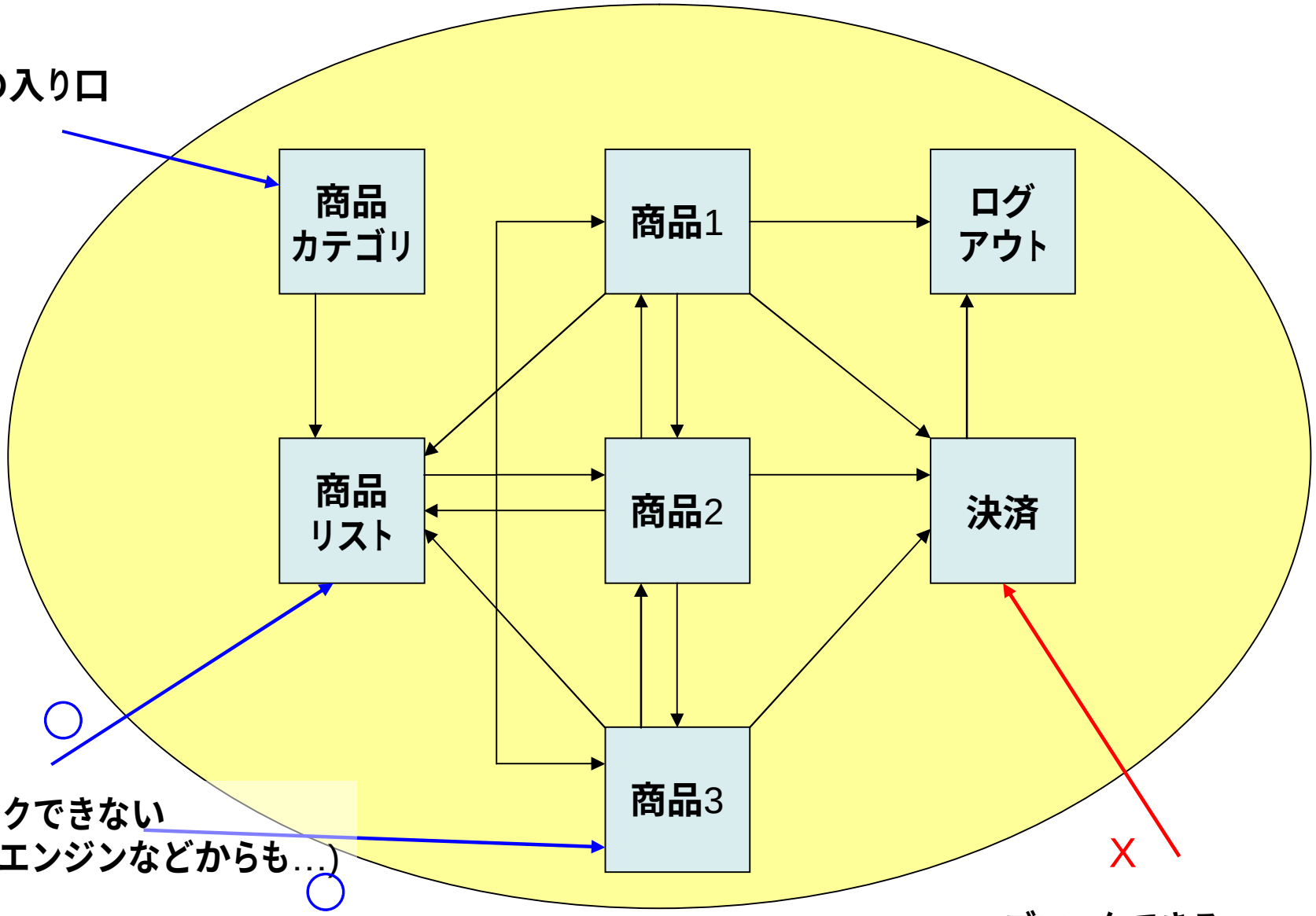
Copyright © 2008 HASH Consulting Corp.

業務システムの場合は外部からの入り口を制限できる



Copyright © 2008 HASH Consulting Corp.

ECサイトの場合は外部からの入り口を制限しにくい



Copyright © 2008 HASH Consulting Corp.

画面遷移チェックの防御効果

- あまり期待できない
- 能動的攻撃の場合(SQLインジェクションなど)
  - 正規の入り口から入っていけばいいだけ
  - 自動化攻撃にはある程度は期待できるかも
- 受動的攻撃の場合(XSS、CSRFなど)
  - これに期待したいわけだが・・・
  - IFRAME要素などで、順につついていけば貫通
  - CSRF対策には、専用の機能を
    (例:Gurdian@JUMPERZ.NET by Kanatoko)
- 続きはデモで

Copyright © 2008 HASH Consulting Corp.

WAFをどう使うか

- WAFによる防御が完全でないことは誰もが認めるところ
- 基本はプログラミング上の対策
- 完全でないものに、高額な費用と多大な手間を掛けることはナンセンス
- 保険的な対策と割り切る
- 安い、あるいは無料のWAFを手間を掛けずに導入する
- WAFも *ゆるふわ* がよい?

Copyright © 2008 HASH Consulting Corp.

ご清聴ありがとうございました

Copyright © 2008 HASH Consulting Corp.