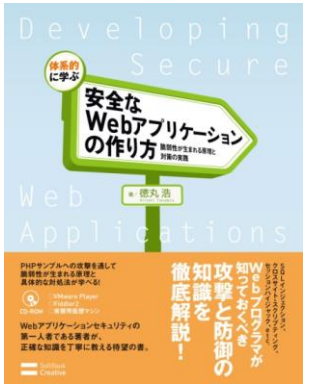
危険なWebサイトのライフサイクルの現状と施策について

HASHコンサルティング株式会社
徳丸 浩
twitter id: @ockeghem

HASH Consulting

徳丸浩の自己紹介

- 経歴
  - 1985年 京セラ株式会社入社
  - 1995年 京セラコミュニケーションシステム株式会社(KCCS)に出向・転籍
  - 2008年 KCCS退職、HASHコンサルティング株式会社設立
- 経験したこと
  - 京セラ入社当時はCAD、計算幾何学、数値シミュレーションなどを担当
  - その後、企業向けパッケージソフトの企画・開発・事業化を担当
  - 1999年から、携帯電話向けインフラ、プラットフォームの企画・開発を担当
    Webアプリケーションのセキュリティ問題に直面、研究、社内展開、寄稿などを開始
  - 2004年にKCCS社内ベンチャーとしてWebアプリケーションセキュリティ事業を立ち上げ
- 現在
  - HASHコンサルティング株式会社　代表　　http://www.hash-c.co.jp/
  - 独立行政法人情報処理推進機構　非常勤研究員 http://www.ipa.go.jp/security/
  - 著書「体系的に学ぶ 安全なWebアプリケーションの作り方」(2011年3月)
  - 技術士（情報工学部門）



問題意識

- 2008年頃からサイト間格差の拡大を実感
  - セキュリティ格差社会
- インターネットは繋がっている
- 情報だけが繋がつているのではなく、安全性についても相互に「繋がり」がある
- ゆえに、「重要なウェブサイト」だけを安全にすれば良いわけではない
- 安全でないサイトに足を引っ張られて、安全なはずのサイトまでも、安全でなくなる事態が発生する
  - パスワードリスト攻撃
  - DNS amp攻撃
  - 水飲み場攻撃
  - …

ウェブサイトが「加害者」になる状況の例

- Gambler型マルウェアの感染源になる
- パスワードリスト攻撃に悪用されるアカウント情報の流出
- いわゆる「水飲み場攻撃」
- ソフトウェア配布サイト、アップデートサイトの改ざんによるもの
- レンタルサーバーの他のユーザに影響を及ぼしてしまうもの（シンボリックリンク攻撃等）
- 迷惑メールの配信に悪用される
- その他、多くの改ざん事件

不正アクセス・不正ログインの原因

- 脆弱性の悪用
  - Webアプリケーションの脆弱性が原因
    - SQLインジェクション、クロスサイト・リクエストフォージェリ(CSRF)…
  - プラットフォームの脆弱性が原因
    - PHP、Tomcat、Apache Struts
    - OpenSSL (Heartbleed)
- 認証を突破
  - 管理者パスワードが推測される、デフォルトパスワードのまま
    - Tomcatの管理機能等
  - 管理者端末がマルウェアに感染（水飲み場攻撃等）
    - Evernote、Twitter、Yahoo! Japan(?)
  - 利用者の認証が突破される
    - パスワードリスト攻撃
    - 辞書攻撃、リバースブルートフォース攻撃（JAL、ANA、github…）

なぜ脆弱なWebアプリが作られるか?

発注者の問題

責任と契約について

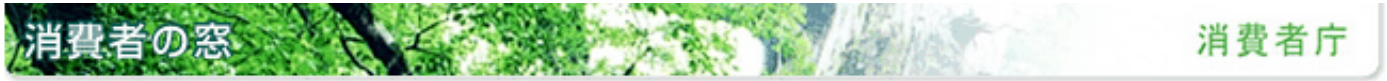
- ウェブアプリケーションの脆弱性の責任は発注者か開発者か
  - 発注者に責任というのが主流のよう
  - ただし、判例があるわけではないので要注意
- 経産省の「モデル契約書」では、以下のような記述がある

なお、本件ソフトウェアに関するセキュリティ対策については、具体的な機能、遵守方法、管理体制及び費用負担等を別途書面により定めることとしている（第50 条参照）。**セキュリティ要件をシステム仕様としている場合には**、「システム仕様書との不一致」に該当し、本条の「瑕疵」に含まれる。
（セキュリティ） 第50 条 乙が納入する本件ソフトウェアのセキュリティ対策について、甲及び乙は、その具体的な機能、遵守方法、管理体制及び費用負担等を協議の上、別途書面により定めるものとする。

- 発注者は自衛のために要求仕様にセキュリティ要件を盛り込んでおくべきだが…

参照 http://www.meti.go.jp/policy/it_policy/softseibi/index.html

【参考】製造物責任（PL）法では…



製造物責任（PL）法について

製造物責任法とは

製品の欠陥によって生命，身体又は財産に損害を被ったことを証明した場合に，被害者は製造会社などに対して損害賠償を求めることができる法律です。本法は円滑かつ適切な被害救済に役立つ法律です。

具体的には，製造業者等が，自ら製造，加工，輸入又は一定の表示をし，引き渡した製造物の欠陥により他人の生命，身体又は財産を侵害したときは，過失の有無にかかわらず，これによって生じた損害を賠償する責任があることを定めています。また製造業者等の免責事由や期間の制限についても定めています。

製造業者，消費者がお互い自己責任の考え方も踏まえながら，製品の安全確保に向けて一層の努力を払い

製造物責任法

問1　この法律

答え　この法律では製造物を「製造又は加工された動産」と定義しています。一般的には，大量生産・大量消費される工業製品を中心とした，人為的な操作や処理がなされ，引き渡された動産を対象とします。ですから，不動産，未加工農林畜水産物，電気，ソフトウェアといったものは該当しないことになります。

不動産，未加工農林畜水産物，電気，ソフトウェアといったものは該当しないことになります。

http://www.consumer.go.jp/kankeihourei/seizoubutsu/pl-j.html より引用

典型的な要件定義書の例（1）

５ 受託業務の内容
受託業務は基本設計書に基づいて実施する。

（１） 機能要件整理
新システムの機能を「別表１ 新システム機能一覧」に示す。
基本設計書を踏まえ、必要となる機能要件を整理し、システム機能要件書としてまとめる。
受託者から機能要件について提案がある場合は、山梨県教育委員会及び受託者双方の協議により提案の受け入れ及び内容を決定する。

（２） 詳細設計
① システム機能設計
⑥ セキュリティ設計
ウィルスや不正アクセス等、システムに対する脅威を明確にし、ユーザー認証、アクセス制御、権限管理等の観点から、具体的なセキュリティ対策を定義する。
設計内容をセキュリティ定義書としてまとめる。

新山梨県立図書館情報システム構築業務委託 仕様書
https://www.pref.yamanashi.jp/toshokan/documents/system/documents/03gyoumuitaku_shiyousho.pdf より引用

飛騨市図書館システムの購入仕様

3-2 ソフトウェアの必須要件

(1)セキュリティ

① 業務端末で使用できる本システムの機能は、認証レベルによつて異なるものとし、端末使用者を特定し不正操作防止の対策が施されていること。

② インターネットに接続するため、クラッカー防止、ウイルス対策等高いセキュリティ対策が確保されていること。

ふるさと宮崎人材バンクホームページ全面改修業務委託仕様書

４ その他システムに関すること
（１）セキュリティ対策について
① コンピュータウィルス対策を実施すること。
② データ漏えい・改ざん対策を実施すること。
③ アプリケーションはSQLインジェクションやクロスサイトスクリプティング対策などセキュリティ対策を施したプログラムを適用すること。

（２）運用・保守について
① セキュリティ（ウィルス対策、セキュリティパッチの適用等）に関しては常に最新の情報を入手し、その対策を実施すること。
② 日常のシステム監視を行い、異常がみられる場合は迅速に対応すること。
③ 必要なログは一定期間保存し、万一の場合には原因追求が的確に行えるようにすること。
④ バックアップはコンテンツの更新頻度等を考慮し、最適なタイミングで実施すること。また、障害発生後の迅速なリカバリが可能であること。

奈良市ホームページリニューアル業務委託仕様書

３－２ 検収

ウ　ホームページの改ざん防止等に資するため、Web アプリケーションの脆弱性の有無を診断すること。検査には、(財)地方自治情報センターのホームページ中、「ウェブ健康診断　仕様について」(https://www.lasdec.or.jp/cms/resources/content/1284/H20_web_kenko_shindan.pdf)　2.4　診断時に利用する診断項目毎の検出パターン(目安)、脆弱性有無の判定基準について　を元に全ての項目について、脆弱性が見つからないこと。また、Web健康診断の報告書を添付すること。

なお、試験に別途費用が発生する場合は受託者の負担とする。

コ SLA要件

3	信頼性	障害対応	一次通知（障害通知）		1時間以内	
			二次通知		2時間以内	
			リカバリポイント		前回バックアップ時点のデータ	
		セキュリティ	ウィルス定義ファイルの更新間隔		ベンダのリリース後、24時間以内	
			OSおよびミドルウェアのセキュリティパッチの適用間隔	セキュリティ関連のパッチ対応	ベンダのリリース後、7日以内に対応方針を報告	
				セキュリティ以外のパッチ対応	パッチ対応の必要性を精査し、必要と判断したパッチを四半期に一度まとめて評価実装	

http://www.city.nara.lg.jp/www/contents/1317628426069/files/itakushiyo.pdf より引用

開発者（受注者）の問題

開発者はどのようにIT知識を習得するか?

- 書籍
- インターネット検索
- Q&Aサイト
- 職場の先輩に聞く
- ・・・

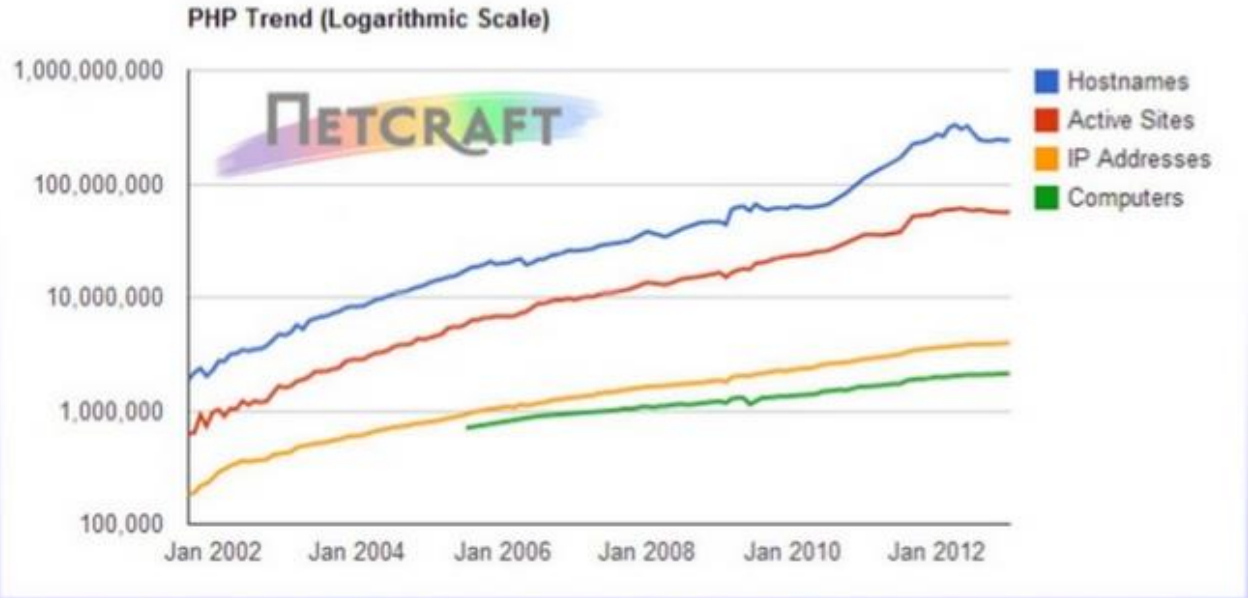
なぜPHP入門書に着目したか

- Webアプリの多くがPHPで記述されている
- 特に、手早くWebスクリプトを習得したい人にニーズがある
- PHP入門書そのものが非常に多い
- 「Yahoo!知恵袋」を見ていると、「なぜこんなソースを?」という書き方が多い
  - PHP入門書を読むと、「むむむ・・・」となる
- ある程度書けるようになったら、それ以上勉強しない and/or ググってすます、知恵袋で済ます人が多いと予想

PHPとは？

参考

- PHPは主にWebアプリケーションに使用されるスクリプト言語
- 1995年の誕生以来、Webと共に成長
- 244M サイト (39%)のWebサーバーでPHPが実行されている
- TIOBE Programming Community Index：スクリプト言語で1位



http://news.netcraft.com/archives/2013/01/31/php-just-grows-grows.html

http://www.slideshare.net/hirokawa/php-con2013ub より引用


PHP
逆引きレシピ
261
PHP
逆引きレシピ
2
315
いきなり はじめる
PHP
作って動かす 速習コース!
気づけば プロ並み
PHP
ショッピングカート作りにチャレンジ!
同時に MySQLも マスター!!
PHP
よくわかる PHPの教科書
プロになるための
PHP
プログラミング入門
Web開発の基礎から フレームワーク活用まで
かんたんWebプログラミング!
これから始める人の
PHP
学習帖
PHP MYSQL FORM
作りながら基礎から学ぶ
PHP
によるWebアプリケーション入門
HTMLのみのシンプルなページが…
変わる過程を体験、学習できます!
基礎からの
PHP
いますぐ 学習が始められます!!
徹底攻略
PHP5
技術者認定[上級]試験
問題集
PHP プロフェッショナルによる書き下ろし
348
大充実の解説
効率的な
Webアプリケーション
の作り方
—PHPによるモダン開発入門—
今すぐ導入!
PHP×PostgreSQL
改訂版
最強Webシステム
PHP
徹底構築
実用
Webアプリの正しい
作り方
Webアプリケーション
構築入門

PHP入門書にセキュリティを求めるのか?

- セキュリティのことは後回しでも良いのでは?
  - 一応Yes
- しかし、できる限り、最初から正しい方法を教えた方が良い
- 「あなたが習ってきたPHPは間違っている」というのも酷
- いつセキュリティを学ぶの?
  - ~~今でしょ~~
  - 永遠にセキュリティを学ばない人が多いと予想
  - 最初に学ぶ時点で、できるだけ安全な方法を学んで欲しい

どのPHP本が売れているか?

いきなりはじめるPHP~ワクワク・ドキドキの入門教室~ 谷藤賢一、河原健人 (2011/12/9)

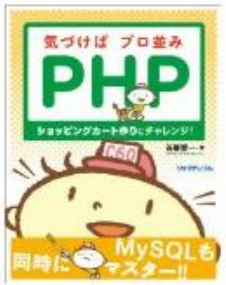
¥ 1,890 大型本 プライム

21時間以内にご注文いただくと、2013/11/29 金曜日までにお届けします。

こちらからもご購入いただけます - 大型本

¥ 1,623 中古品 (7 出品)

★★★★½ (50)



気づけばプロ並みPHP~ショッピングカート作りにチャレンジ! 谷藤賢一、河原健人 (2013/10/15)

¥ 2,625 大型本 プライム

16時間以内にご注文いただくと、2013/11/29 金曜日までにお届けします。

こちらからもご購入いただけます - 大型本

¥ 2,489 中古品 (3 出品)

★★★★½ (7)

よくわかるPHPの教科書 たにぐち まこと (2010/9/14)

¥ 2,604 単行本(ソフトカバー) プライム

21時間以内にご注文いただくと、2013/11/29 金曜日までにお届けします。

4点在庫あり。ご注文はお早めに。

¥ 1,905 Kindle版

今すぐダウンロード

こちらからもご購入いただけます - 単行本(ソフトカバー)

¥ 1,188 中古品 (22 出品)

★★★★☆ (60)

PHP超入門 ~誰でもできるプログラム~ 河口 英悟 (2013/6/4)

¥ 100 Kindle版

今すぐダウンロード

★★★★★ (1)

PHPエンジニア養成読本〔現場で役立つイマドキ開発ノウハウ満載!〕(Software Design plus) 新原 雅司、原田 康生、小山 哲志、田中 久輝 (2013/9/13)

¥ 2,079 大型本 プライム

16時間以内にご注文いただくと、2013/11/29 金曜日までにお届けします。

★★★★½ (4)

PHP逆引きレシピ 第2版 (PROGRAMMER'S RECiPE) 鈴木 憲治、山田 直明、山本 義之、浅野 仁 (2013/10/22)

¥ 2,940 単行本(ソフトカバー) プライム

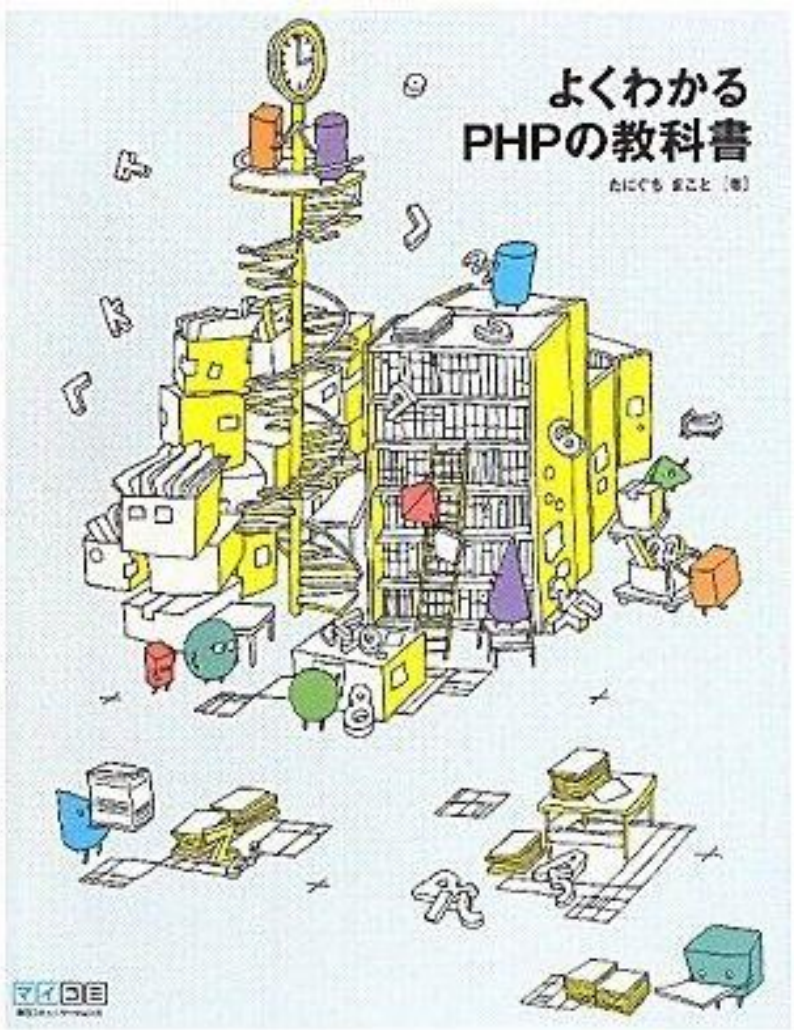
21時間以内にご注文いただくと、2013/11/29 金曜日までにお届けします。

こちらからもご購入いただけます - 単行本(ソフトカバー)

¥ 2,700 中古品 (1 出品)

★★★★★ (3)

よくわかるPHPの教科書



- 発売日: 2010/9/14
- Amazonランキング:5,889
- 価格: ¥2,604-

機能	対応
クラス	×
SQL	○ (MySQL)
メール	○
アップロード	○
認証	○
サンプル	一行掲示板

本書の特徴

- カラー図版を多数用いた親しみやすい版組み
- 全ページカラー!
- 「ジャパネットたにぐち」と異名をもつ軽妙な語り口
- 初歩の入門から、DB、ファイルアップロード、メール送信、認証など一通りの機能開発が学べる
- コードはゆるい感じ

本書を読んでの所感

- セキュリティには一応の配慮をしている
- SQL呼び出しはmysql関数 + mysql_real_escape_stringによるエスケープ
  - mysql関数は、PHP5.5で非推奨になったが、本書発行時点では決まっていなかったので仕方がない
  - とは言え、本書の内容が古くなった感はある
  - MySQLに特化した記述が気になる（文字列リテラルをダブルクォートで囲むなど）
- XSS対策は配慮しているが抜けもある
- CSRF対策はしていない

SQLインジェクションはどうか

```
// ここまでで、認証済みであるこの検査が済んでいる
$id = $_REQUEST['id'];
// 投稿を検査する
$sql = sprintf('SELECT * FROM posts WHERE id=%d',
        mysql_real_escape_string($id));
$record = mysql_query($sql) or die(mysql_error());
$table = mysql_fetch_assoc($record);
if ($table[‘member_id’] == $_SESSION[‘id’]) { // 投稿者の確認
  // 投稿した本人であれば、削除
  mysql_query('DELETE FROM posts WHERE id=' .
mysql_real_escape_string($id)) or die(mysql_error());
}
```

しかし、DELETE FROM
文なので表示はない

ここにSQLインジェクション

SQL文のエラーが起こるか否かで情報を盗む

- SQLインジェクションにより実行されるSQL文の例

  DELETE FROM posts WHERE id=18-(SELECT id FROM members WHERE id LIKE char(49) ESCAPE IF(SUBSTR((SELECT email FROM members LIMIT 1,1),1,1)>='M', 'a', 'ab')))
- WHERE句の中 18-(SELECT … WHERE …)
- 中のWHERE句は
  LIKE 述語にESCAPE句がある
- ESCAPE句はIF関数により、membersの1行目の1文字目が’M’以上の場合’a’、それ以外の場合’ab’
- SQL文の文法上、ESCAPE句は1文字以外だとエラー
- この結果を繰り返すことによって、対象文字列を絞り込む
  →ブラインドSQLインジェクション

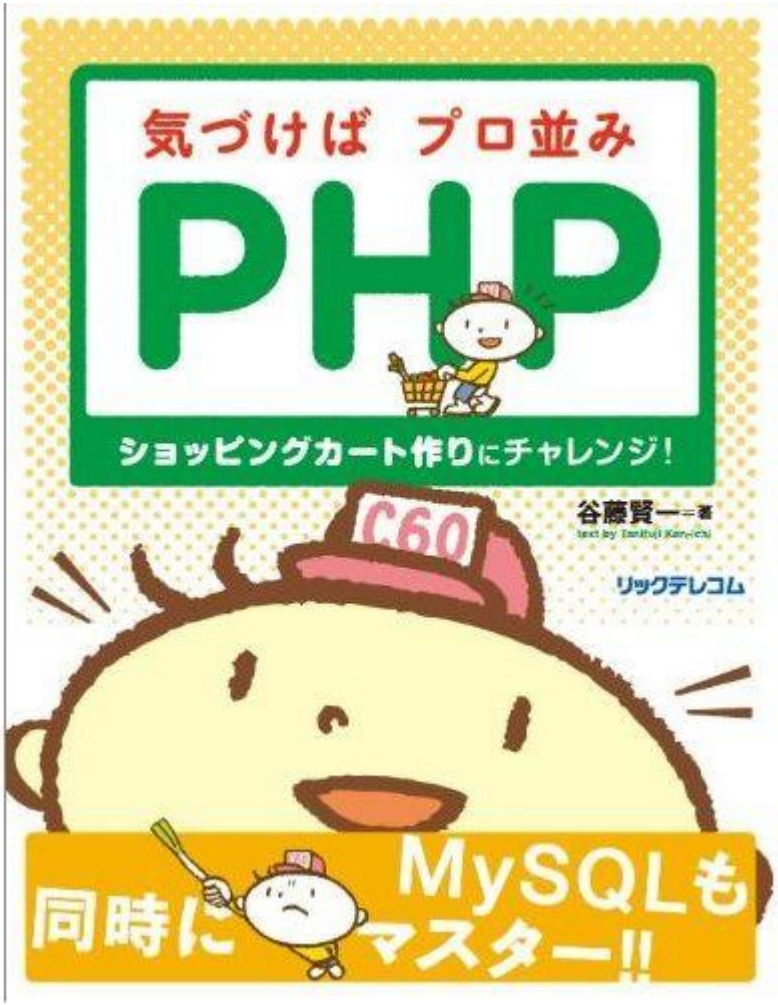
CSRFはどうか?

```
005:  if (isset($_SESSION['id']) && $_SESSION['time'] + 3600 > time()) {
006:    // ログインしている 省略
014:  } else {
015:    // ログインしていない
016:    header('Location: login.php'); exit();
017:  }
018:
019:  // 投稿を記録する
020:  if (!empty($_POST)) {
021:    if ($_POST['message'] != '') {
022:      $sql = sprintf('INSERT INTO posts SET member_id=%d, message="%s",
   reply_post_id=%d, created=NOW()',
023:        mysql_real_escape_string($member['id']),
024:        mysql_real_escape_string($_POST['message']),
025:        mysql_real_escape_string($_POST['reply_post_id'])
026:      );
027:      mysql_query($sql) or die(mysql_error());
028:
029:      header('Location: index.php'); exit();
030:    }
031:  }
```

CSRF脆弱性
対策していない

続きはデモで

気づけばプロ並みPHP



- 発売日: 2013/10/15
- Amazonランキング:5,117
- 価格: ¥2,625-

機能	対応
クラス	×
SQL	○ (MySQL/PDO)
メール	○
アップロード	○
認証	○
サンプル	ショッピングサイト

本書の特徴

- 「いきなりはじめるPHP~ワクワク・ドキドキの入門教室~」（通称『谷藤本』）の続編にあたる
- ショッピングサイトの基本機能であるショッピングバスケット作りを通じて、「プロ並み」を目指す…らしい
- PHP習得を通じて、多くの方の就業支援を目指している

本書を読んでの所感

- 「いきなり始める～」から継承した分かりやすさ
- PHPの書き方としては古臭いもの（10年前くらい・・・）
- バリデーションはほぼしていない
- SQL呼び出しはすべてPDOのプレースホルダを用いている(Good!)
- XSS対策のHTMLエスケープは、入力時にまとめて行っている(Bad!)
- クロスサイト・リクエストフォージェリ(CSRF)対策はしていない
- パスワードはソルトなしMD5で保存
  - "一度MD5で暗号化されてしまうと、スーパーコンピュータでも簡単には解読できません"

PHP入門書に関するまとめ

- PHPの入門書には課題のあるものが多い
- 「わかりやすさ」を全面に出した書籍にその傾向が…
- セキュリティ以前のコードの品質が低い
- 入力を直ちにHTMLエスケープする場合が多い
- せめて以下をお願いしたい
  - SQLはプレースホルダで、接続時に文字コードを指定
  - HTMLのエスケープは出力時に、文脈に応じて
  - できればCSRF対策も説明して（控えめなお願い）
- でも、良書も増えてきたよ
- PHP逆引きレシピ第2版は本当にすごい
- ネット検索なんかせずに逆引きレシピ2版を見るといいよ

Google検索、Q&Aサイト

「SQLインジェクション対策」でGoogle検索して上位15記事を検証した

■「SQLインジェクション対策」でGoogle検索して上位15記事を検証した 514 users ★★★★★ 36★

このエントリでは、ネット上で「SQLインジェクション対策」でGoogle検索した結果の上位15エントリを検証した結果を報告します。

SQLインジェクション脆弱性の対策は、既に「安全なSQLの呼び出し方」にファイナルアンサー（後述）を示していますが、まだこの文書を知らない人が多いだろうことと、やや上級者向けの文書であることから、まだ十分に実践されてはいないと思います。

この状況で、セキュリティのことをよく知らない人がSQLインジェクション対策しようとした場合の行動を予測してみると、かなりの割合の人がGoogle等で検索して対処方法を調べると思われます。そこで、以下のURLでSQLインジェクション対策方法を検索した結果の上位のエントリを検証してみようと思い立ちました。

- http://www.google.co.jp/search?q=SQLインジェクション対策

どこまで調べるかですが、以前NHKスペシャルで"グーグル革命"の衝撃が放送された際に話題になった印象的な言葉「グーグル検索で…上位15位に入らなければこの世に存在しないのと同じです」にならい、少し多いですが「この世に存在する」上位15位までを調べてみました。

http://d.hatena.ne.jp/ockeghem/20111109/p1 より引用

「SQLインジェクション対策」でGoogle検索して上位15記事を検証した(結論)

まとめ

「SQLインジェクション対策」でGoogle検索した上位15件の内容を検証しました。

ここまで説明したように、上位15件の中には、SQLインジェクションの対策手法を説明した上質の文書はあまりありません。12位の「 PHPでのSQLインジェクション対策 – エスケープ・クォート編 – Let's Postgres 」はとても良い解説ですが、初心者には少し難しいと思います。

初心向けの解説としては、VOYAGE GROUP須藤さんの素晴らしいブログ記事「Webアプリケーションとかの入門本みたいのを書く人への心からのお願い。」がおすすめです。現役バリバリのWebエンジニアがこれを書いたところに圧倒的な説得力があります。この記事は、次のように始まります。

> SQLインジェクションについて書くときに以下のメッセージを必ず含めて欲しいです。
>
> - 単にプリペアドステートメントを使え
> - 絶対に文字列結合でSQLを構築しようとしてはいけない
> - IPAの「安全なSQLの呼び出し方」を読むこと
>
> *http://d.hatena.ne.jp/ajiyoshi/20100409/1270809525*

素晴らしい。以上の引用をもって、本エントリ全体のまとめに代えたいと思います。

http://d.hatena.ne.jp/ockeghem/20111109/p1 より引用

ベストアンサーに脆弱性がある例は珍しくない

ベストアンサーに選ばれた回答

sebumihaさん

SQLの検索～表示の部分のソースを見せていただけますか？

'textfield'のくくりがバッククォート「`」でなくシングルクォーテーション「'」になっていますね。

```
$sql = "SELECT * FROM table WHERE textfield = '$Cid'";
```

或いは

```
$sql = "SELECT * FROM table WHERE `textfield` = '$Cid'";
```

としてみてください。

SQLインジェクション脆弱性有り
…最近は改善されつつある

Y! ナイス！ 0

回答日時：2009/6/23 22:36:11 編集日時：2009/6/24 16:33:38 違反報告

http://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q1427570179 より引用

プラットフォームの脆弱性

Struts1に脆弱性

注意喚起情報

Apache Struts 2の脆弱性が、サポート終了のApache Struts 1にも影響
～国内でいまだ大量稼働するStruts 1利用企業に、直ちに緩和策を～

2014年04月24日

株式会社ラック サイバー・グリッド研究所は、Apache Struts 2 に存在するとされた、リモートの第三者による任意のコード実行を許す脆弱性(CVE-2014-0094)と同様の問題がApache Struts 1 においても存在していることを確認しました。(2014/05/01 追記) この問題には、4月30日付けで、共通脆弱性識別子CVE-2014-0114が割り当てられました。

Apache Strutsは、Apacheソフトウェア財団のApache Strutsプロジェクトで開発とサポートがおこなわれているオープンソースでのJava Webアプリケーションフレームワークです。

現在は、Struts 2 がサポートされていますが、2008年10月4日に最終版が公開され、2013年4月5日でサポート終了となった、Struts 1 においても、同様の脆弱性が存在します。しかし、Struts 1 はサポート終了しており、当該プロジェクトからは公式なアナウンスは出ておらず、今後正規の更新プログラムの提供もされないものと考えられます。

一方、Struts 1 が稼働しているWebサイトは、官公庁や公益法人、銀行などを含め国内に数多く存在しており、提供ベンダーからの個別サポートなど個々で特別な対応を行ってない限り攻撃に関して脆弱な状態のままと推測されます。

昨年発見されたStruts 2 の脆弱性の多くが攻撃に悪用された実績からして、攻撃は必ず発生する前提で対応する必要があると考えます。

http://www.lac.co.jp/security/alert/2014/04/24_alert_01.html より引用

国税庁Webサイト、一部でサービス停止 - Apache Struts脆弱性の影響で

[2014/04/26]

国税庁は4月25日、「確定申告書作成コーナー」「e-Taxソフト(Web版)」「NISA(日本版ISA)コーナー」のサービス停止を発表した。これらのサービスには、オープンソースのJava Webアプリケーションフレームワーク「Apache Struts1」が利用されており、脆弱性があるとしてセキュリティ会社ラックが注意喚起を行なっている。

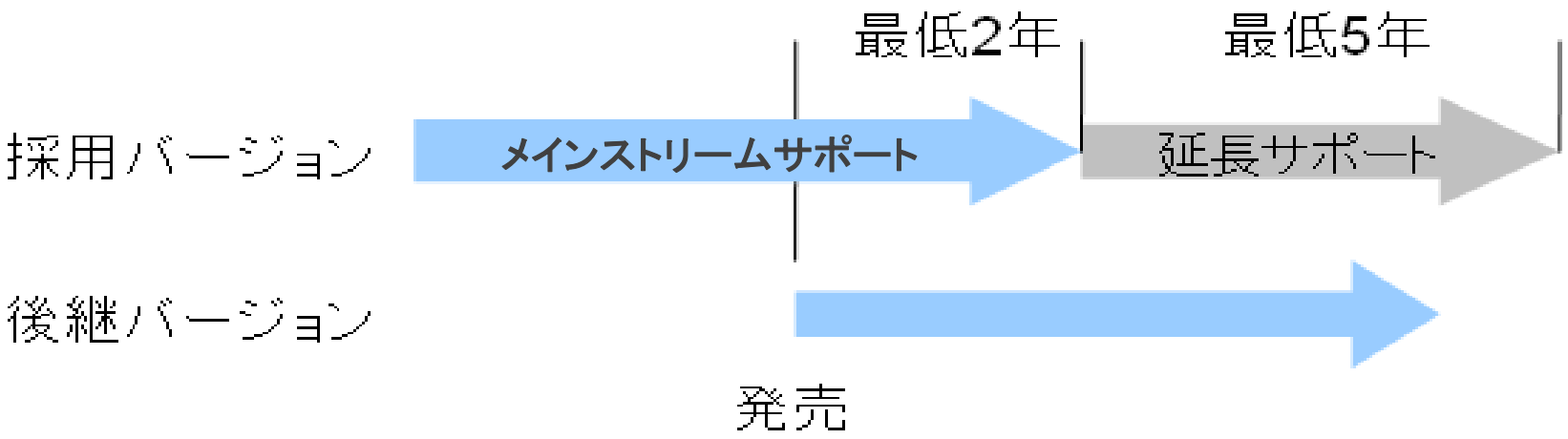
同庁によると、脆弱性に関する情報が出たのち、全てのサービスを確認したところ、前述の3サービスにStruts1が使用されていたという。なお、通常のe-Taxソフトや源泉徴収票等作成ソフトといったその他サービスは引き続き利用できるという。

国税庁では、停止しているこれらのサービスについて「対応を検討中」としており、対応が完了するまでの間は、代替手段でのサービス利用を行なうよう呼びかけている。

サポートライフサイクルポリシーとは

- サポートライフサイクルポリシーとは、製品サポートについてのサポートポリシーを文書化したもの
- 厳密な契約ではないが、購入者に対する「約束」と考えられる
- マイクロソフト社の取り組みが有名
  - 2002 年 10 月に最初に発表
  - 2004 年 6 月に更新
  - 詳しくは次のスライドで…

マイクロソフト社のサポートライフサイクルポリシー



メインストリームサポート	次のうちいずれか長い方 ・製品発売から5年 ・後継製品の発売から2年
延長サポート	次のうちいずれか長い方 ・メインストリームサポート終了から5年 ・2番目の後継製品の発売から2年

・マイクロソフト社のサポートポリシーでは、**最新の製品を使う限り、7年間のサポートが保証されている（追加費用無し）**

日本IBMのサポートライフサイクルポリシー

- 分散ソフトウェア製品（IBM プログラムのご使用条件（IPLA）に基づくソフトウェア製品）について：
- 2008年2月以降、Lotus, Information Management, Rational, Tivoli および WebSphere ブランドのIPLA製品の大多数は、エンハンスト・サポート・ライフサイクル・ポリシーの製品として発表され、製品が使用可能となった日（GA日）から**最低5年間のサポートを提供**する。
  - ある製品のコンポーネントとなっている同梱されているソフトウェアは、全て同じサポート期間となる。
  - 少なくともサポート終了日の12カ月前には、サポート終了（EOS）のお知らせをする。顧客は、サポート終了前に新しいバージョンへの移行を検討。 また、サポート終了日は、4月または9月のいずれかとなる。
  - サポート期間の情報は、全て一つのサイトで提供している。
- スタンダード・サポート・ライフサイクル・ポリシーの製品は、製品が使用可能となった日（GA日）から最低3年間のサポートを提供する。

※GAから5年では、稼働期間中のパッチ提供が打ち切られる可能性がある

Request for Comments: Release Process(PHP)

- Yearly release cycle
  - 3 years release life cycle
  - 2 years bug fixes only
  - 1 year security fixes only
- 下図のように、PHP5.x（2番目の数字）を使い続けるのは、2～3年が限度

Example time line with only one major version at a time

```
**** pre release phase
++++ release lifetime with all bug fixes, no feature addition
---- release lifetime security  fixes only
D    EOL
Version Time ->
       2011        2012        2013        2014        2015        2016        2017
        |     |     |     |     |     |     |     |     |     |     |     |     |
5.3     +++++++++++++-----D
5.4     |*****++++++++++++++++++++++++++-----------D
5.5     |     |     |******++++++++++++++++++++++++-----------D
5.6     |     |     |     |     |******++++++++++++++++++++++++-----------D
6.0     |     |     |     |                 |******++++++++++++++++++++++++-----------D
6.1     |     |     |     |                             |******++++++++++++++++++++++++-----------D
```

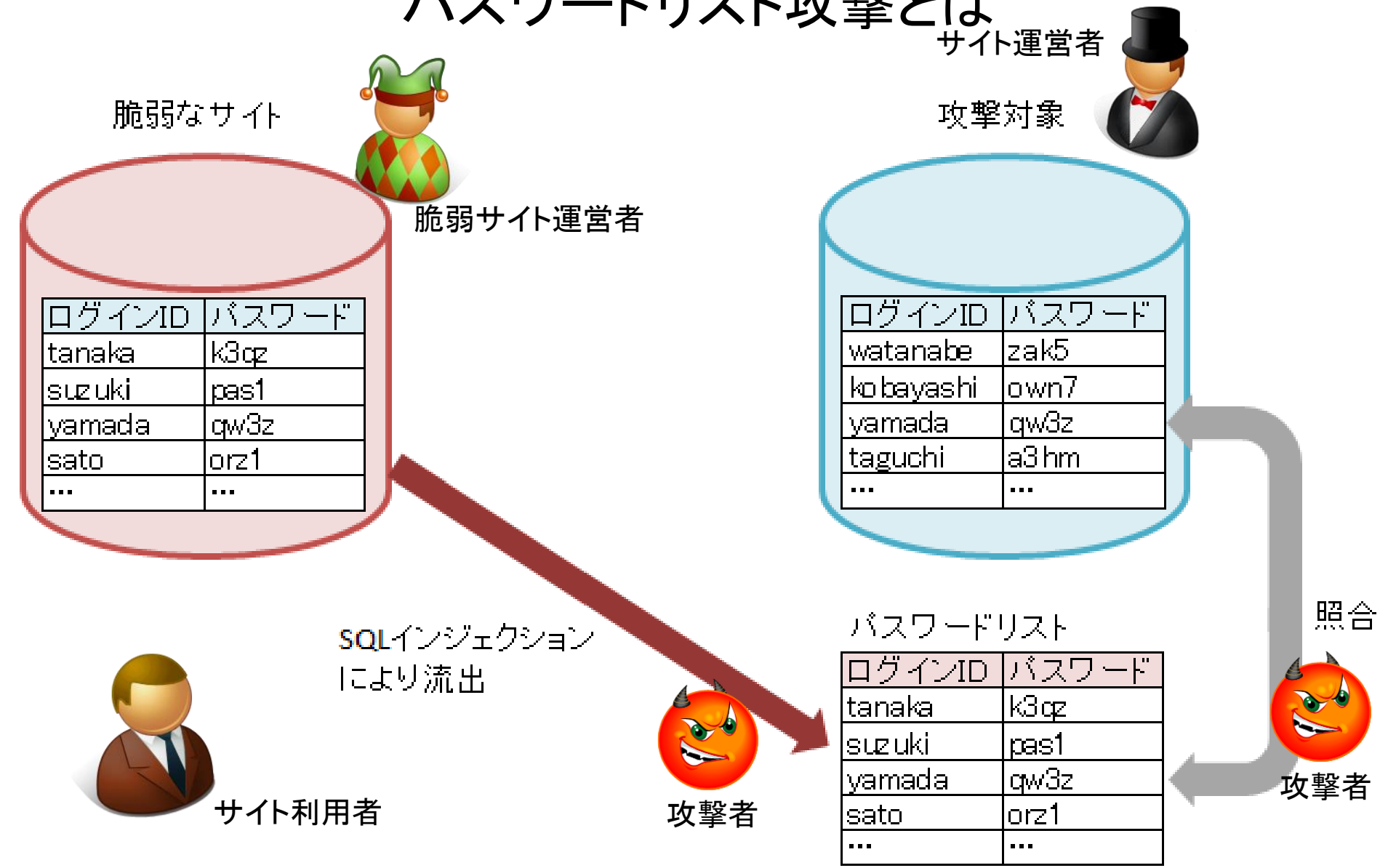
https://wiki.php.net/rfc/releaseprocess より引用

サポートライフサイクルポリシーまとめ

- サポートライフサイクルポリシーとは
- 製品選定時にサポートライフサイクルポリシーを確認すること
- サポート期間が足りないようなら、製品提供元と交渉する
- サポート計画を検討する
  - サポートの長い製品を選定する
    - PHPなどもRedHat/CentOSのパッケージで導入すれば10年サポートに
  - 途中でバージョンアップする計画を立てておく（予算も）
  - オープンソースソフトウェアの場合、バージョンアップにとことん付き合うというやり方ももちろんあり

パスワードリスト攻撃

パスワードリスト攻撃とは



Webサイトは「どこまでやれば」いいのか?

- パスワード認証に対する施策は、利用者の責任をサイト側が *救済する* 意味合いが強い
- Webサイトが *最低* しないといけないのは下記
  - ある程度長いパスワードをつけられること
  - SQLインジェクション等の脆弱性を排除すること
- 1文字のパスワードをつけられたら、それは脆弱性?
  - 従来の「タテマエ論」からすると、それはサイトの責任ではなく、利用者の責任
  - 他の人が知らないパスワードをつけるのは利用者の責任
- 大事なことなので大きな文字にしました

パスワードリスト攻撃の「登場人物」悪いのは誰?

パスワードをお
漏らししたサイト

パスワードリスト攻
撃を受けたサイト

脆弱なサイト

ログインID	パスワード
tanaka	k3qz
suzuki	pas1
yamada	qw3z
sato	orz1
…	…

攻撃対象

ログインID	パスワード
watanabe	zak5
kobayashi	own7
yamada	qw3z
taguchi	a3hm
…	…

SQLインジェクション
により流出

パスワードリスト

ログインID	パスワード
tanaka	k3qz
suzuki	pas1
yamada	qw3z
sato	orz1
…	…

照合

パスワードリスト攻撃により
不正ログインされた利用者

攻撃者

1番悪いのは…

- 攻撃者
- これは自明

2番目にわるいのは…

- パスワードをお漏らししたサイト
- 利用者からお預かりしたパスワードを漏えいした責任

3番目に悪いのは…

- パスワードリスト攻撃により不正ログインされた利用者
- パスワードの「使い回し」をしていた責任

1番悪くないのは…

- パスワードリスト攻撃を受けたサイト
- 追求されるほどの不備はないと考えられる

でも、利用者側にも言い分が

ぼく、パスワード認証にしてくれとは頼んでないもん!

一応のまとめ

- パスワード認証のタテマエとして、パスワードの管理は利用者の責任という考え方がある
- でも、それ、無理だよね（本音）
- そもそも、パスワード認証にしてくれと頼んでないし…
- パスワード認証が崩壊すると、結局サイト運営者も困るし…
- そこで、サイト運営者側も頑張っている
- でも、サイト運営者側の努力だけでは解決しない
- どこかで折り合いがつけられれば…

ではどうしたらよいか？

課題と解決の方向性

- 発注者向け啓蒙
  - 脆弱性の責任は発注者にあり
  - 「地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Webアプリケーション）」…の試み
- 開発者向け啓蒙
  - 質問サイト、PHP入門書等は少しずつ改善が見られる
  - さらに「かみくだいた」解説が必要
  - 長期的には、免許制などの検討が必要ではないか?
- プラットフォームのライフサイクルとパッチ適用の問題
  - 従来は「（脆弱性が多いから）例えば、PHPを避ける」と言われたが
  - むしろ、長期のサポートと、パッチ適用の容易さを考慮すべきでは?
  - 「メンテナンス容易性」でプラットフォームを選択するべきでは?
- パスワードの問題
  - 新しい認証手段に期待

モデルプランのポイント

「セキュリティ保証期間」という期間を設け、
「脆弱性リスト」で示した脆弱性に限定して対処（脆弱性がないようにする）を求めている。

（万一運用時に脆弱性が発覚したら、追加費用なしで修補を求める）

セキュリティ保証期間＝5年間（稼働予定期間）

追加費用なし≠無償

“追加費用なし”の効用

- リスクの見積もりを提案者（ベンダー）に委ねている。

「自ら開発したソフト、選定したソフトで事後（セキュリティ保証期間中）に脆弱性が発覚するリスクを見込んで保守費用に対応費用を積んでおいてください」

- 地方公共団体の調達 ＝ ほとんど入札

…となれば、

  - 「(開発者は)できるだけセキュアなソフト開発をする」
  - 「(SIerは)できるだけセキュアなソフトを選定する」

というインセンティブが働く（保守費用を安くできるから）

- 地方公共団体だけでなく、他にも広がれば…

モデルプランの採用が進むと…

脆弱性を作り込まない開発体制（構築体制）整えている優秀なベンダーの製品の採用を促進し、そうでない製品を排除する方向に。

提案者にとってのモデルプランの意義

- セキュリティ施策について、何をどこまでやればよいかを明示
- セキュリティ施策の対応範囲を明確にする
  - 脆弱性対応、セキュリティ機能
  - セキュリティ検査
  - セキュリティ保証期間内の「追加費用無しで」の脆弱性修補
  - 選定ソフトウェアのパッチ適用の確認
- 「セキュリティ保証期間」の導入により、サイトの稼働期間を通じて安全を維持することを目指す
- 提案時に責任範囲を明確にすることにより、提案の「土俵」を統一し、公平なベンダー選定を目指す

RedHatのサポートライフサイクルポリシー

レッドハット、RHEL 5／6のサポート期間を10年に延長
基幹系システム向けサポートも拡大

レッドハットは、Red Hat Enterprise Linux 5／6のサポート期間を10年に延長した。基幹系システム向けサポートサービスの適用範囲も広げた。

[本宮学，ITmedia]

レッドハットは4月11日、Linuxディストリビューション「Red Hat Enterprise Linux」（RHEL）5／6のサポート期間を従来の7年から10年に延長 6を2020年

7年から10年に延長

RHEL 5／6のサポート期間は、全ての新機能や新ハードウェアに対応するフェーズ1（5年半）、いくつかの新機能やセキュリティアップデートに対応するフェーズ2（1年）、バグフィックスや重要なセキュリティアップデートに対応するフェーズ3（3年半）で構成される。RHEL 3／4のサポート期間は従来通り7年だが、オプションで3年間の延長サポートも提供するという。

米Red Hatのジム・トットン副社長兼 プラットフォーム事業部門長

http://www.itmedia.co.jp/enterprise/articles/1204/12/news016.html より引用

RedHatのサポートライフサイクルポリシー(Cont.)

Red Hat Enterprise Linux 5および6のライフサイクル：

Production 1 (approx. 5 1/2 years)					Production 2 (approx. 1 year)	Production 3 (approx. 3 1/2 years)				Extended Life Phase (approx. 3 years)		
Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Year 11	Year 12	Year 13

	Red Hat Enterprise Linuxのライフサイクル					
説明	運用1フェーズ	運用2フェーズ	運用3フェーズ	延長ライフサイクルフェーズ[7]	Extended Life Cycle Support (ELS) アドオン[9]	Extended Update Support (EUS) アドオン[9]
以前にリリースされた内容へのRed Hatカスタマーポータルからのアクセス	○	○	○	○	○	○
Red Hatカスタマーポータルを利用するセルフサポート	○	○	○	○	○	○
テクニカルサポート[1]	無制限	無制限	無制限	制限つき[10]	無制限	無制限
非同期のセキュリティErrata (RHSA)	○	○	○	×	○[9]	○[9]
非同期のバグ修正Errata (RHBA)[2]	○	○	○	×	○	○
マイナーリリース	○	○	×	×	×	×
更新されたハードウェアの有効化[3]	ネイティブ	制限つき[4]ネイティブ	仮想化を使用	仮想化を使用	仮想化を使用	仮想化を使用
ソフトウェア機能拡張[5]	○[6]	×	×	×	×	×
更新インストールイメージ	○	×[8]	×	×	×	×

RedHat/CentOSの現行バージョンはいつまで使える?

Red Hat Enterprise Linux 5			
一般的な利用可能開始日	運用1フェーズの終了日	運用2フェーズの終了日	運用3フェーズの終了日 (運用フェーズの終了)
2007年3月15日	2012年第4四半期	2014年第1四半期	2017年3月31日

Red Hat Enterprise Linux 6			
一般的な利用可能開始日	運用1フェーズの終了日	運用2フェーズの終了日	運用3フェーズの終了日 (運用フェーズの終了)
2010年11月10日	2016年第2四半期	2017年第2四半期	2020年11月30日

21. What is the suppo

~~CentOS 3~~	~~CentOS-3~~
~~CentOS 4~~	~~CentOS-4 updates until Feb 29, 2012~~
CentOS 5	CentOS-5 updates until Mar 31, 2017
CentOS 6	CentOS-6 updates until November 30, 2020

Red Hat EL5/CentOS5: 2017/3/31まで
Red Hat EL6/CentOS6: 2020/11/30まで

http://wiki.centos.org/FAQ/General#head-fe8a0be91ee3e7dea812e8694491e1dde5b75e6d

まとめ

- 脆弱なWebサイトが作られる原因を考察
- 発注、開発、運用、利用者に原因がある
  - つまり、全部☹
- 関係者が多いため、迅速な対応には限界がある
  - 発注者、開発者は徐々にではあるが改善の兆しが
  - 安かろう・悪かろうのサイトは減らない
  - 利用者のスキルは向上しない
- メンテナンス容易性・パッチ適用容易性からプラットフォームを選択する
  - 貧乏人はCentOSを使え（10年サポートだし…）
- セキュリティ格差社会は今後も拡大する
- 極力作らない、所有しない

Thank you