

「安全なウェブサイトの作り方」 を読もう

2008/12/27

FM-Tokyo ライトニングトーク発表資料

松尾 篤（株式会社エミック）

Webアプリケーションを
安全に作っていますか？

カスタムWebで開発を
始める前に

「安全なウェブサイトの
作り方」を読みましよう

はじめに

- Webサイトの「安全上の欠陥」（脆弱性）が狙われる事件が後を絶たない現状

安全上の欠陥があると 起こりうる問題

- Webサイトの内容が改ざんされる
 - Webページにウイルスが埋め込まれる
 - Webサイトから個人情報盗まれる
- etc.

狙われる対象は 多岐にわたる

- オペレーティングシステム (OS)
 - Webサーバー
 - Webアプリケーション
- etc.

なかでも

Webアプリケーションは

- 個別に独自開発される場合が多いため、セキュリティ対策は個別に実施する必要がある
- 安全に作っておかなければ安全に運用することは極めて困難

安全に作らなければ いけないものの

- そもそも安全に作ることを意識していない
- 何が問題なのか分からない
- 安全に作る方法が分からない
- そもそもどうすればいいのか分からない

安全なウェブサイトの 作り方

- 独立行政法人 情報処理推進機構（略称：IPA）が公開している資料
- 2008年12月現在、最新版は改訂第3版
- 日本語版だけでなく英語版も公開

<http://www.ipa.go.jp/security/vuln/websecurity.html>

何が書かれているのか

- Webアプリケーションにおける主な脆弱性の種類や発生しうる脅威、解決方法等
- Webサイト全体の安全性を向上するための指針、対策
- 問題となる実装の失敗例

XSSでよくある失敗例

- エスケープ処理の未実施

例) `<?php echo $_GET['param']; ?>`

- 応答結果で文字コードの未指定

etc.

実際に読んでみる

まとめ

- FileMakerのカスタムWeb公開機能を使う前に「安全なウェブサイトの作り方」を必ず読みましょう
- カスタムWebだけでなくWebビューアを利用する前にも是非読みましょう