

# サイトにおけるセキュリティと パーミッションの関係

～情報漏えいの脅威とその対策について～

2008年9月15日

カゴヤ・ジャパン株式会社

吉岡和彦

# 自己紹介

吉岡和彦(よしおかかずひこ)

カゴヤ・ジャパン株式会社(データセンター・レンタルサーバー)

システム開発・保守・運用

- コントロールパネル
- サーバー連携システム・社内システム

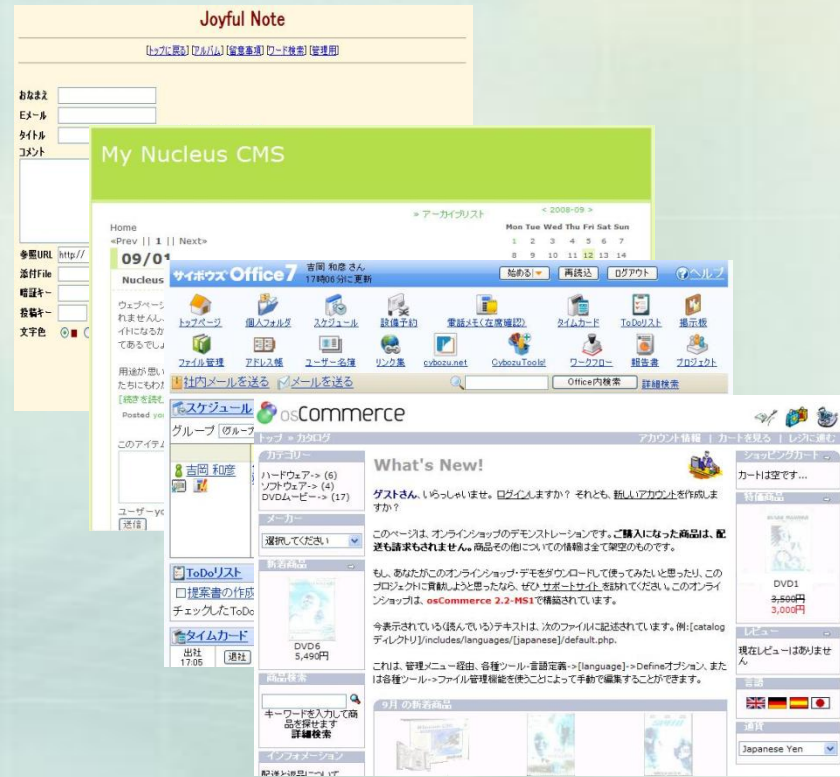
# テーマ

1. Webアプリケーションが扱うデータ
2. 情報漏えいの脅威
3. パーミッション設定による  
具体的なセキュリティ対策

**WEBアプリケーションが扱うデータ**

# WEBアプリケーションの種類

- 掲示板/チャット
- ブログ/CMS
- グループウェア
- ショッピングカート



# WEBアプリケーションが扱う データの種類

- 掲示板/チャット ⇒ 意見/会話
- ブログ/CMS ⇒ 日記/コーポレート
- グループウェア ⇒ スケジュール・社員
- ショッピングカート ⇒ 販売履歴・顧客データ

Q.情報漏えいという観点から見た場合

# 情報漏えいの脅威

# 情報漏えいしても問題ないデータ

- 記事データ
- 個人の日記等

→ 公開されているデータ

# 情報漏えいで問題となるデータ

- スケジュール/社員情報
- 販売履歴/顧客情報

→ 非公開のデータ

→ プライバシーに関わるデータ

# 情報漏えい時のコスト(1)

## 賠償金予想

(※賠償金は1人¥5,000～¥30,000を想定)

- ¥5,000 × 10万人 = 5億円
- ¥3,000 × 10万人 = 30億円
- 上記 + 人件費 + メディア(告知)費用

# 情報漏えい時のコスト(2)

表 1 : 2007 年 個人情報漏えいインシデント 概要データ

漏えい人数	3,053 万 1,004 人
インシデント件数	864 件
想定損害賠償総額	2 兆 2,714 億 1,060 万円
一件当たりの漏えい人数 <sup>※1</sup>	3 万 7554 人
一件当たり平均想定損害賠償額 <sup>※1</sup>	27 億 9,386.3 万円
一人当たり平均想定損害賠償額 <sup>※2</sup>	3 万 9,017 円

(引用)日本ネットワークセキュリティ協会

2007年度情報セキュリティインシデントに関する調査報告書

<http://www.jnsa.org/result/2007/pol/incident/index.html>

# パーミッション設定による 具体的なセキュリティ対策

# Webアプリケーションの セキュリティ対策

- SQLインジェクション防止
- クロスサイトスクリプティング防止
- パラメータ改ざん防止
- ：
- パーミッション設定

# なぜ今、パーミッションか

■ 設定が甘くてもプログラムは動く！

→ (パーミッション設定が) 疎かになりがち

⇒ **ずさんな管理の実状が存在する！**

(※情報漏えいしてもおかしくない)

# (パーミッション設定が) 疎かになりがちなる理由

- サイトの見た目に影響しない
- クライアントに説明しても分からない
  - Q. 情報漏えいした場合 ⇒ クライアントは何と言うか??
- 昔からのなごり

⇒ 逆に言えば…

**手軽に情報漏えい対策**

# 説明の対象とする環境

- 共用サーバー
- OS:Linux系
- CGIプログラムである(\*\*\*.cgi)
- Webサーバーに、  
CGIWrap または suEXEC 機能が  
実装されている (mod\_ruid,他…)  
⇒setuid,setgidする機能

# (補足)CGIWrap や suEXECとは

CGIをファイルのオーナー権限で  
実行できるwrapper(仲介)プログラム

※汎用的なパーミッションよりも、セ  
キュアなパーミッション設定が可能

※セキュリティのチェックが行われる  
⇒オーナー,グループ,ディレクトリ

# (補足)CGIWrap や suEXEC機能が ない場合(利用していない場合)

## [サーバー内]

Aさん



[会員ID/PW]

(マスター)



認証

Webサーバーさん  
(他人)



Aさんのサイト  
(会員ログインフォーム)



ID/PW 入力

共用サーバーであれば、同じサーバー内の全ユーザーが、  
Aさん所有のデータ(マスターのID/PW)を読み取ることが可能！

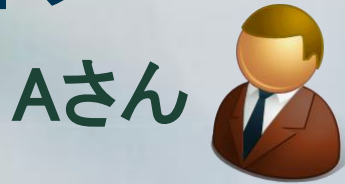
インターネットアクセス

※Aさんから見た他人

⇒ 同じサーバー内の全ユーザー

# (補足)CGIWrap や suEXEC機能が ある場合 (機能を利用する場合)

[サーバー内]



[会員ID/PW]

(マスター)



認証



Aさんの権限  
(オーナー)



Aさんのサイト  
(会員ログインフォーム)



ID/PW 入力

インターネットアクセス

※Aさんの権限のみでデータを  
やりとり可能なため、安全

# パーミッションのおさらい

## パーミッションは3ケタの数値

ターゲット

オーナー

グループ

その他

権限

呼出 (4)

呼出

呼出 (4)

書込 (2)

書込

書込

実行 (1)

実行

実行 (1)

現在の属性

705

# パーミッションによって 情報漏えいの可能性あり！

## 情報漏えいの可能性がある例

- 『CGIプログラム』のパーミッションが、  
**755** or **705** ...etc...
- 『データファイル』のパーミッションが、  
**644** or **604** ...etc...

# パーミッションによって 情報漏えいする理由

下記のようなパーミッション設定に  
なっている

■ 755 or 644 ...etc...

⇒「他人」or「グループ」に対して、  
読込権(4) が付与されている

# お情報漏えいに対して 効果的なパーミッション設定

「他人」&「グループ」に対する  
読込権を付与しない(書込権・実行権も)

(例) [700] : `***.cgi`

[600] : 重要なデータファイル  
設定ファイル

[700] : ディレクトリ (CGIのみが参照する...)

# パーミッション変更の注意点

正しく設定しないとプログラムが  
動作しなくなる

## ※トラブルの例

⇒CGIWrap や suEXEC 環境でないのに、  
700,600のようなパーミッションを設定し  
てしまった

# パーミッション設定の補足(1)

設定対象は CGIプログラムと  
そのデータファイルに限らない

※重要なデータファイル単体をサーバー上に  
アップロードする場合でも、他人・同じグループ  
に読み取られるパーミッションにはしない

(大体のサーバーで、ファイルアップロード時の  
パーミッションが標準で644となっている為、忘れがち)

# パーミッション設定の補足(2)

## パーミッション設定で、解決できない ケース

- CGIWrap/suEXEC 環境でない  
(※一概には言えませんが)
- PHPスクリプト(『\*\*\*.php』)である  
(※オーナー権限で動作するサーバーもあります)

# おさらい

## 効果的なパーミッションの設定

- 700 : CGI
- 600 : 重要なデータファイル  
CGIの設定ファイル
- 700 : CGIのみが参照するディレクトリ

# おさらい(補足)

## よくわからない場合は…

- CGI : 755 → 705 → 700
- データファイル : 644 → 604 → 600  
設定ファイル
- ディレクトリ : 777 → 707 → 700

# まとめ

- **パーミッションの設定だけで、セキュリティリスクを減らすことができる**  
(ケースもある)
- **パーミッションの設定により生じるセキュリティリスクの把握が大事**  
→ 可能であれば、セキュリティポリシーを策定してください

**(おまけ)**

**WEBアプリケーションの  
セキュリティ対策2**

# おまけ1：パーミッション以外での セキュリティ強化

- 専用サーバーを使う(VPSも有効)
- スクリプトのCGI化(`php`→`cgi` 等)
- `suphp`, `mod_ruid`,,,

# おまけ2：WEBアプリケーションのバージョンアップ適用タイミング

- セキュリティパッチの場合  
→ **すぐに適用**
- 不具合修正・機能更新の場合  
→ **様子見でもOK**

(公開後に不具合が出る可能性がある為、過去の実績を参考にしてもよい)

ありがとうございました

# パーミッション設定の補足(3)

## グループに対するパーミッション

- 殆ど(ほぼ全て)のレンタルサーバーでは、グループに対する権限(パーミッション)を付与する必要はありません

⇒グループが利用されるケースは、ないと考えられる

# パーミッション設定の補足(4)

『**CGIのみが参照するディレクトリ ⇒ 700**』に関連する補足です

- CGIが参照するディレクトリであっても、ブラウザから(URLで)直接アクセスされるファイル(HTMLや画像等。CGIプログラムも含む)が直下・または下位に存在する**ディレクトリ**の場合は、ディレクトリのパーミッションを**705 or 755**としてください

[理由]

ブラウザから(URLで)直接アクセスされるファイルへは、まずWebサーバー(他人)の権限で、対象ファイルの(存在や権限等の)チェックが行われる為

⇒他人(その他)に、「アクセス対象のファイルが存在するディレクトリの中を参照する権限」を付与する必要がある

[補足]

これは必要なことであり、データファイルや設定ファイルに対するパーミッションが正しく設定されていれば、ディレクトリのパーミッション設定に起因する情報漏えいの可能性は、ありません

# ご意見・お問い合わせ

今回お話(補足)した内容は、Linuxのユーザーの概念・CGIWrapやsuEXEC等の機能に基づいています

スライドやお話させて頂いた内容で、不明な部分がある場合、またはフィードバックを頂けます場合は、下記アドレスまでメールを頂ければ幸いです

[yoshioka@kagoya.com](mailto:yoshioka@kagoya.com)