

PHPカンファレンス2008

# 情報セキュリティの向上に役立つ IPA コンテンツ

独立行政法人 情報処理推進機構(IPA)  
セキュリティセンター

**永安 佑希允**

# 今日の内容

1. 情報セキュリティに関する IPA の取組み
2. 情報セキュリティに関するコンテンツの紹介
3. デモ:SQL インジェクションの脆弱性



## 情報セキュリティに関する IPA の取組み

# IPAのセキュリティ届出・相談窓口



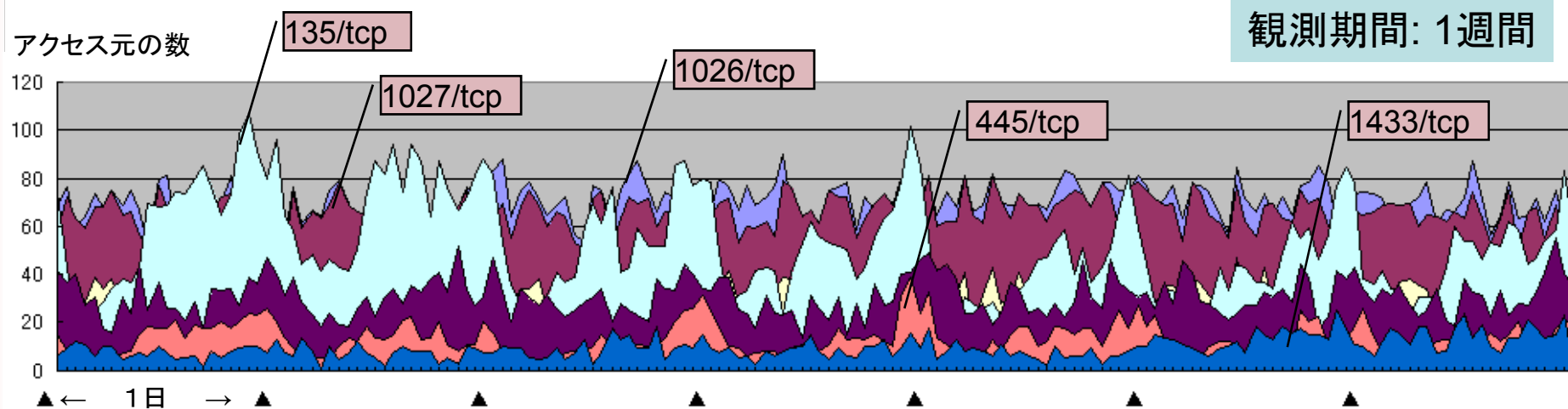
- 不正アクセスに関する届出  
<http://www.ipa.go.jp/security/ciadr/>
- コンピュータウィルス110番  
<http://www.ipa.go.jp/security/virus110/>
- 脆弱性情報の届出  
<http://www.ipa.go.jp/security/vuln/report/>

各届出の、統計情報等を定期的に公開しています

<http://www.ipa.go.jp/security/>

# インターネットに接続しているだけで…

## 典型的なネットワークトラフィック

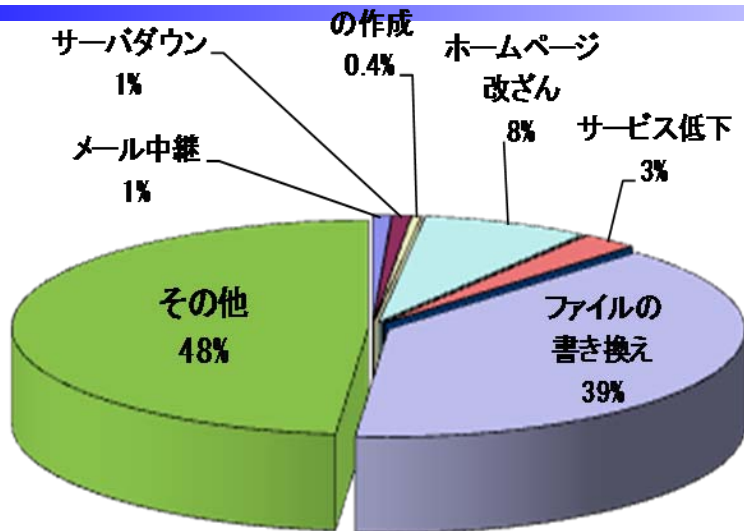


IPA インターネット定点観測 TALOT2 (2008/4/12-4/18) より

- 一般利用者の環境とほぼ同じ観測環境
- 一日あたり**259**個所の送信元から、約**690**件の一方的なアクセス(2008年4月)

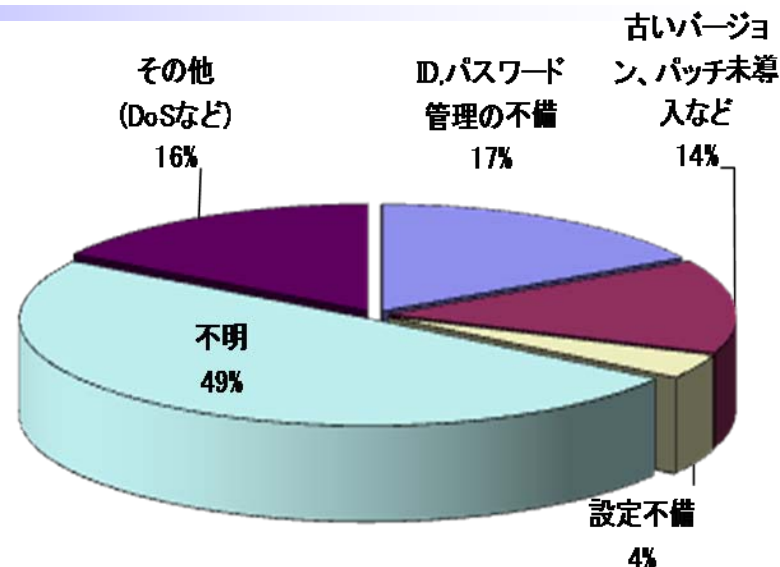
# 届出の被害とその原因

不正アカウント



## 2007年不正アクセス届出種別

- 届出件数は減少傾向
- 被害の件数自体はほとんど変わらず



## 2007年不正アクセス被害原因

- パスワード管理/パッチ未導入/設定不備が多い
- 不正アクセスの手口が巧妙化し原因究明が困難な事例が増えている

# 不正アクセスに関する考察

- ・ 狙われるのは特別なサイトではない

- ・ 既知の古い脆弱性
- ・ 推測され易い、弱いパスワード



**基本的な対策で十分防御可能！**

- ・ 「被害内容」として目立って来たもの

- ・ 他サイト攻撃用の踏み台として悪用された
- ・ 明らかに金銭を目的とした犯罪  
(個人情報奪取、オークション、オンラインゲーム)



**犯罪者がITを駆使し、悪用**

# 再確認：脆弱性って？

## ● 脆弱性(ぜいじゃくせい)とは

- ソフトウェア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルスなどの攻撃により、その**機能や性能を損なう原因**となり得る**セキュリティ上の問題箇所**のこと  
(出典：情報セキュリティ早期警戒パートナーシップガイドライン)

## ● 脆弱性を利用すると

- 問題点箇所を巧みに利用し、コンピュータの内部データ(情報)を盗んだり、書き換えたり、削除したり、また他のコンピュータへの同様の悪事を働くことが可能となる  
(これが**不正アクセス**であり、プログラム化して自動的に動作するのが**ウイルス**や**ボット**である)

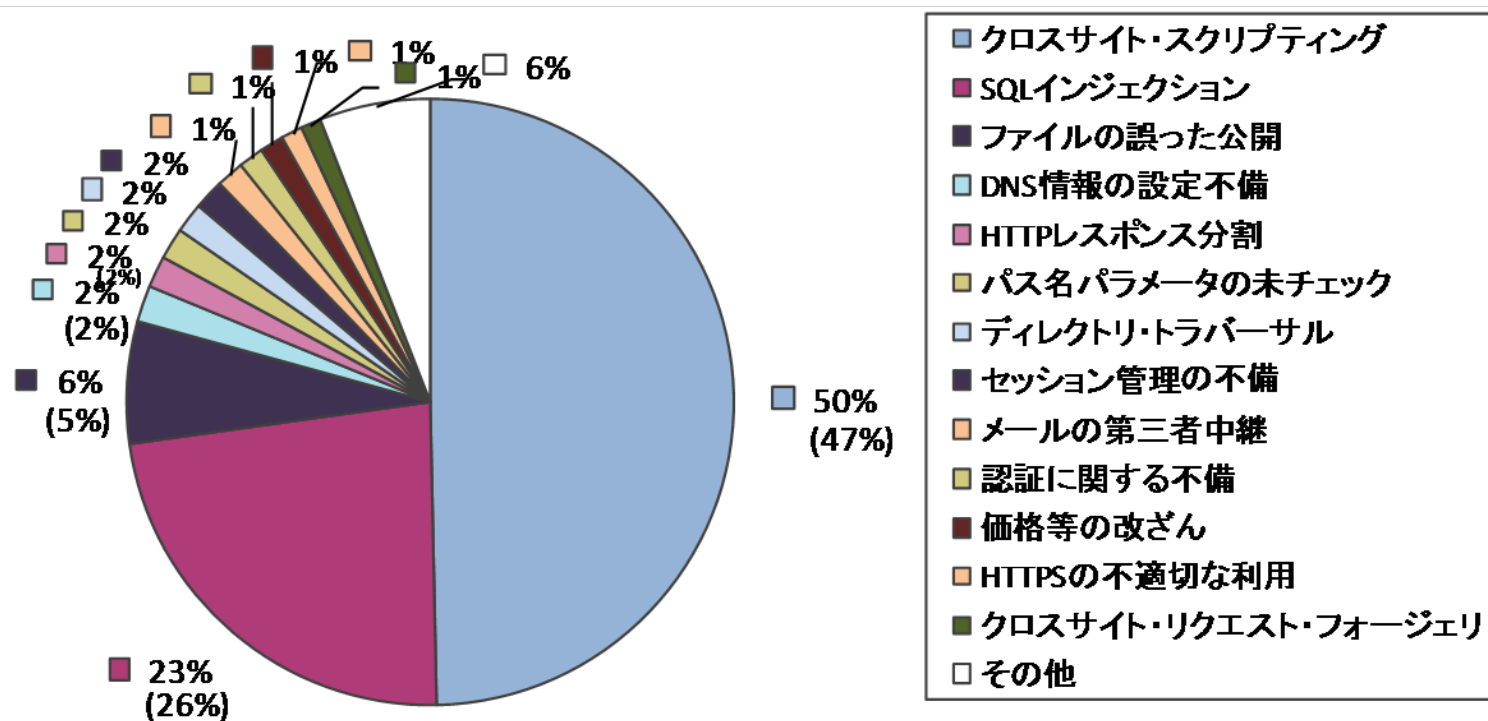
## ● 脆弱性対策は根本的なセキュリティ対策

- セキュリティ対策としてウイルスなどの対策も十分必要だが、脆弱性を無くすことが最も重要！！



# ウェブアプリケーションの脆弱性届出

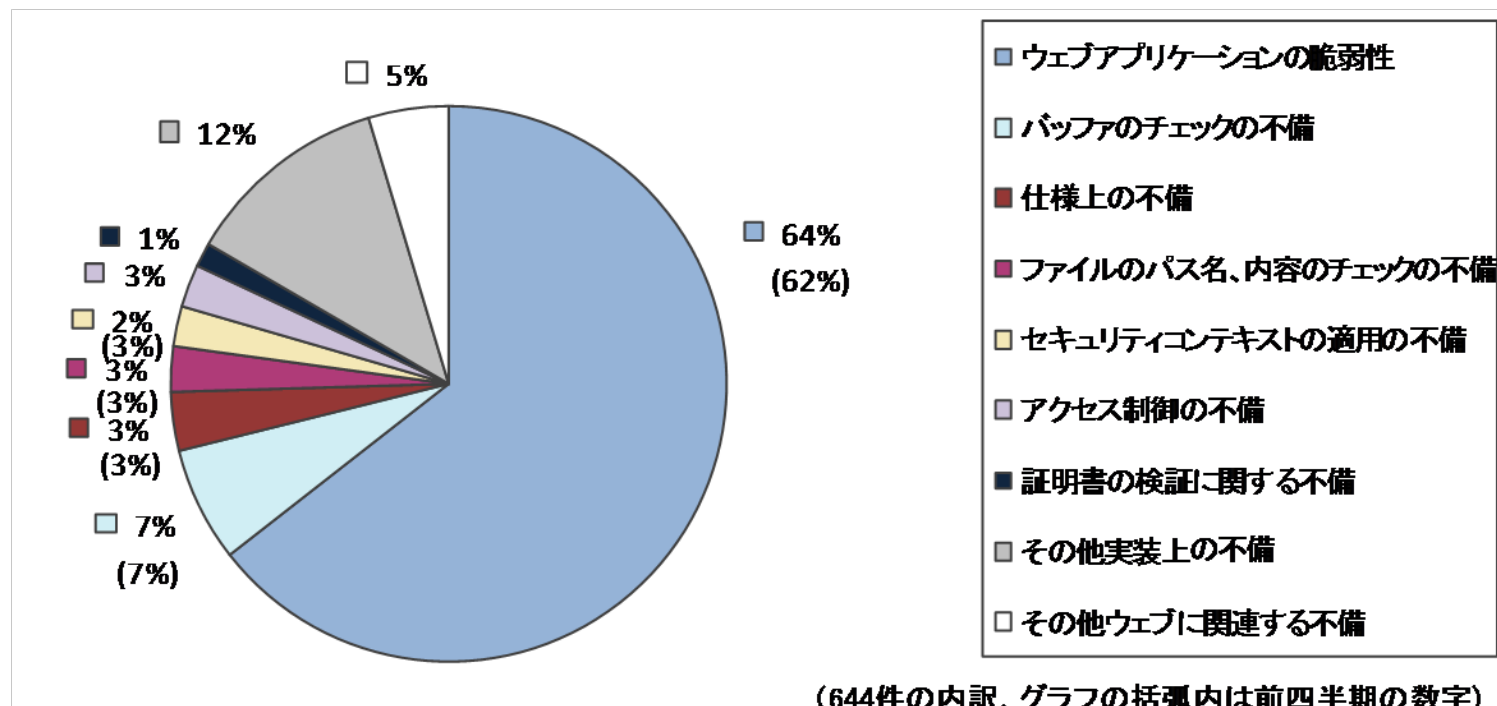
- クロスサイト・スクリプティングとSQL インジェクションで7割以上
- うっかり作りこみやすく、また発見されやすい



(1,492件の内訳、グラフの括弧内は前四半期の数字)

# ソフトウェア製品の脆弱性届出

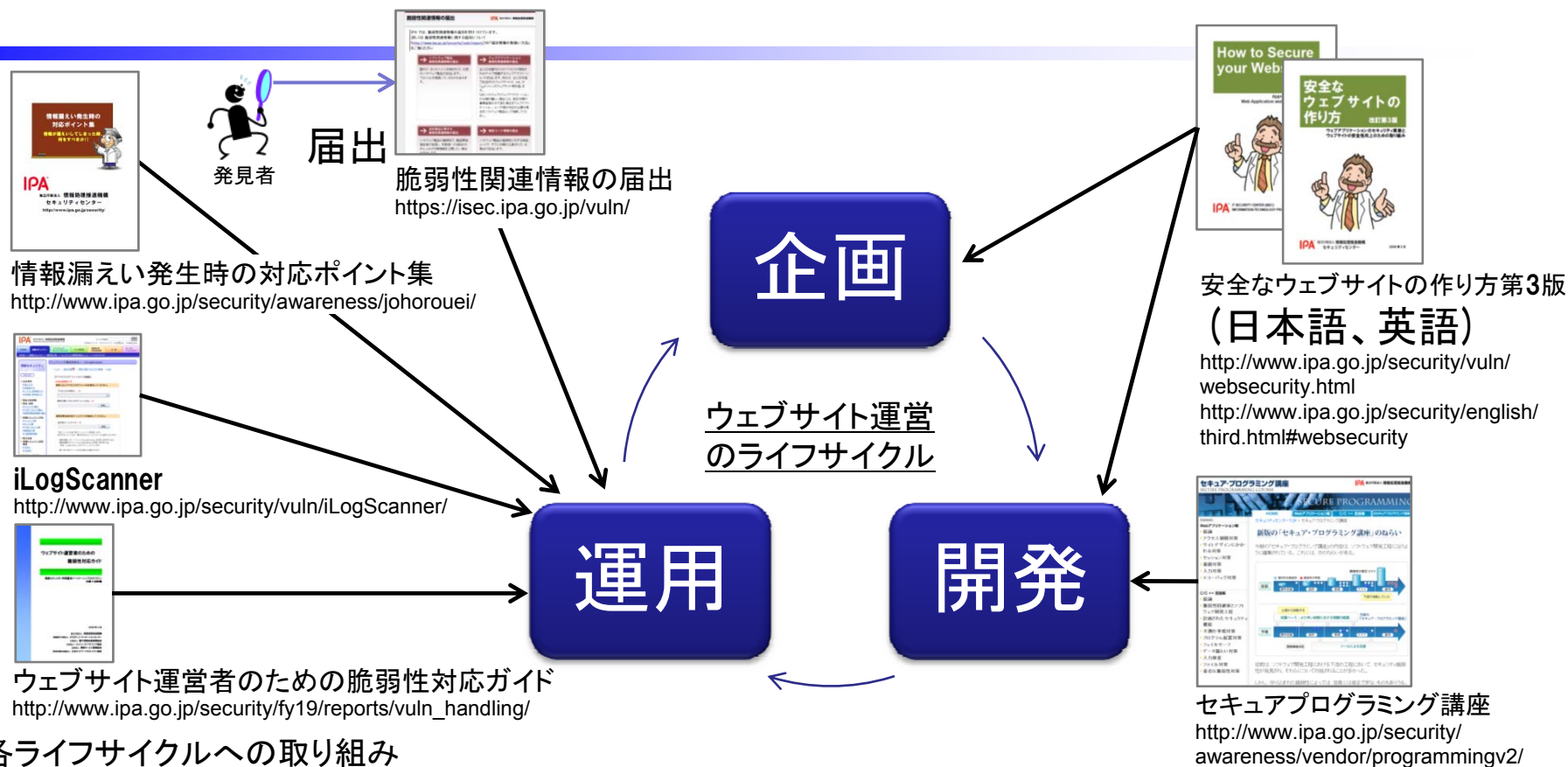
- ウェブアプリ(CGI/CMS等)の届出が多い
- 半分近くがクロスサイト・スクリプティング
  - ウェブアプリ以外でもウェブ技術を利用するものが多い



(644件の内訳、グラフの括弧内は前四半期の数字)

## 情報セキュリティに関する コンテンツの紹介

# ウェブサイトの脆弱性に対する IPA の取組み



## 各ライフサイクルへの取り組み

ライフサイクル全体に対する取り組み



情報セキュリティ白書2008



知っていますか？脆弱性



安全なウェブサイト運営入門

# 「安全なウェブサイトの作り方」



- IPA が実際に脆弱性として判断しているものを記載
- ウェブアプリケーションに関する届出件数の約 9 割を網羅
- 有効性を確認済みの修正例
- 失敗事例
- チェックリスト

安全なウェブサイトの作り方 改訂第3版

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

# 取り上げている ウェブアプリケーションの問題

1. SQL インジェクション
2. OS コマンド・インジェクション
3. パス名パラメータの未チェック／ディレクトリ・トラバーサル
4. セッション管理の不備
5. クロスサイト・スクリプティング
6. CSRF (クロスサイト・リクエスト・フォージェリ)
7. HTTP ヘッダ・インジェクション
8. メールの第三者中継
9. アクセス制御や認可制御の欠落

# 根本的解決と保険的対策

- 根本的解決
  - 「脆弱性の原因を作らない実装」を実現。
  - その脆弱性による攻撃を完全に無効化。
  - 可能な限り、根本的解決を行うのが望ましい。
- 保険的対策
  - 攻撃による影響を低減する「セーフティネット」。
  - 脆弱性の原因は依然として残る。
  - 保険的対策のみに頼る取組は望ましくない。

# 取り上げていない問題

1. PHP Remote File Inclusion
2. NULL バイト攻撃 (NULL Byte Attack)
3. register\_globals に関する問題
4. PHP4 サポート終了

# 「セキュア・プログラミング講座」

- 上流工程（要件定義、設計）から脆弱性対策



# 「セキュア・プログラミング講座」

1. 総論
2. アクセス制御対策
3. サイトデザインにかかわる対策
4. セッション対策
5. 暴露対策
6. 入力対策
7. エコーバック対策

セキュア・プログラミング講座

<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html>

# 「iLogScanner」

## 解析結果のレポート例

**47件のSQLインジェクション攻撃を検出**

**攻撃成功は0件**

**攻撃成功の可能性は検出されなかった。**

解析結果

- 終了ステータス: 成功
- 解析日時: 2008/04/07 14:22
- 解析対象ファイル: access\_log, access\_log.2, access\_log.5, access\_log.6, access\_log.8, access\_log.9
- 検出数 : 計 47件

検出したWebサイトへの攻撃について、下記に検出結果を記載します。

検出対象脆弱性	攻撃があったと思われる件数	攻撃が成功した可能性の高い件数
SQLインジェクション	47	0

脆弱性が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。  
※この結果に該当するアクセスログはiLogScanner\_20080407\_\*.logです。

**検出対象脆弱性の説明と対策**

**SQLインジェクション**

「SQLインジェクション」は、データベースと連携を行うWebアプリケーションにおいて、SQL文を改ざんされ、意図していないデータベース操作が実行されてしまう問題です。データベース操作を行うSQL文を、ユーザからの入力値を用いて構成している場合に、想定外の入力を行うことによりSQL文の書き換えを行います。この脆弱性が存在する場合、アプリケーションが使用するデータベースアカウントの権限で、データベース操作を実行することが可能になります。不正にデータベースが操作されることにより、情報の漏洩、不正な更新・削除によるデータベースの破壊などの影響が考えられます。実行可能な操作はアプリケーションが使用するデータベースアカウントの権限に依存するため、不必要に大きな権限が与えられている場合、不正なプログラムの埋め込みなど、さらに被害が広がる可能性があります。  
[http://www.ipa.go.jp/security/vuln/vuln\\_contents/sql.html](http://www.ipa.go.jp/security/vuln/vuln_contents/sql.html)

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

## 解析結果のログ例

解析結果ログの見方

ログファイル名  
[[行番号] [脆弱性種別] [攻撃が成功した可能性が高い] [該当するアクセスログ]]

※ 各項目はタブ区切りになります  
※※ 攻撃が成功した可能性が高い場合、「●」が付きます  
以下、解析結果ログ

access_log.3	脆弱性種別	攻撃が成功した可能性	該当するアクセスログ
6891	SQLインジェクション	-	118.64 -- [02/Mar/2008:20:00:00]
6892	SQLインジェクション	-	118.64 -- [02/Mar/2008:20:00:00]
6893	SQLインジェクション	-	118.64 -- [02/Mar/2008:20:00:00]
9020	SQLインジェクション	-	128.138 -- [03/Mar/2008:04:00:00]
9033	SQLインジェクション	-	197.234 -- [03/Mar/2008:04:00:00]
9035	SQLインジェクション	-	197.234 -- [03/Mar/2008:04:00:00]
9036	SQLインジェクション	-	197.234 -- [03/Mar/2008:04:00:00]
9048	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9049	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9050	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9051	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9052	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9053	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9059	SQLインジェクション	-	70.21 -- [03/Mar/2008:04:00:00]
9060	SQLインジェクション	-	70.21 -- [03/Mar/2008:04:00:00]
9061	SQLインジェクション	-	70.21 -- [03/Mar/2008:04:00:00]
9070	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9071	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9072	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9083	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9094	SQLインジェクション	-	3.183 -- [03/Mar/2008:04:00:00]
9119	SQLインジェクション	-	70.21 -- [03/Mar/2008:04:00:00]
9121	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9182	SQLインジェクション	-	197.234 -- [03/Mar/2008:04:00:00]
9514	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9515	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9516	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9548	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
9549	SQLインジェクション	-	5.193.190 -- [03/Mar/2008:04:00:00]
75149	SQLインジェクション	-	5.193.190 -- [04/Mar/2008:00:00:00]
75150	SQLインジェクション	-	5.193.190 -- [04/Mar/2008:00:00:00]
75151	SQLインジェクション	-	5.193.190 -- [04/Mar/2008:00:00:00]
76374	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
76375	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
76551	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
76552	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
77202	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
77203	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
77204	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]
77561	SQLインジェクション	-	165.64 -- [04/Mar/2008:16:00:00]

**攻撃元のIPアドレス**

**攻撃のあった時刻**

ウェブサイトの脆弱性検出ツール iLogScanner

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

# 「iLogScanner」の利用例

- IPA で公開している OSS iPedia のアクセスログを解析
- 最近SQL インジェクションがますます急増

## 1.解析対象のウェブサイト

- ・IPA のOSS iPedia  
(オープンソース情報データベース)

## 2.解析したログの期間

- ・2008年1月～6月

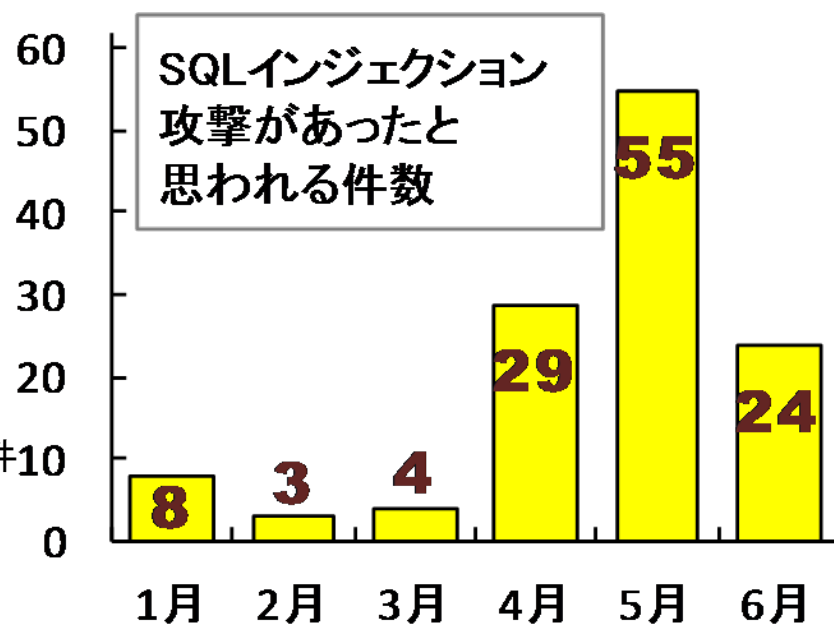
## 3.「iLogScanner」の解析結果

(1)攻撃があったと思われる件数:123件

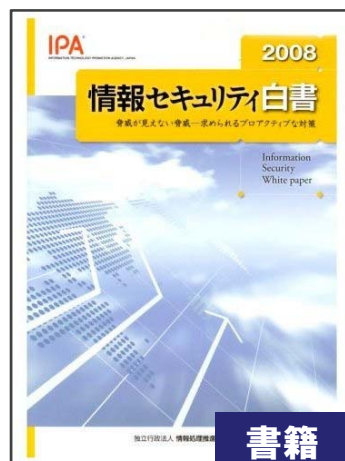
(2)攻撃が成功した可能性の高い件数:0件

## 4.ログの詳細調査結果

- ・攻撃に成功した件数:0件



# 「情報セキュリティ白書2008」



情報セキュリティ白書2008



同 第II部 10大脅威

- 2007年は脅威の「見えない化」がますます進んだ年
- 脅威が単独で利用されず、互いに関連し利用されている
- 単独でセキュリティ対策を行うのではなく、複合的かつ継続的な対策(PDCAサイクル)が求められている
- 中でも脆弱性対策には、開発設計時からの取り組みが重要

# 2007年の10大脅威

ますます進む「見えない化」

- 第1位 高まる「誘導型」攻撃の脅威
- 第2位 ウェブサイトを狙った攻撃の広まり
- 第3位 恒常化する情報漏えい
- 第4位 巧妙化する標的型攻撃
- 第5位 信用できなくなった正規サイト
- 第6位 検知されにくいボット、潜在化するコンピュータウイルス
- 第7位 検索エンジンからマルウェア配信サイトに誘導
- 第8位 国内製品の脆弱性が頻発
- 第9位 減らないスパムメール
- 第10位 組み込み製品の脆弱性の増加

情報セキュリティ白書2008 より

<http://www.ipa.go.jp/security/publications/hakusyo/2008/hakusyo2008press.html>



# 脆弱性について理解する



ウェブサイトにおける代表的な 10 種類の脆弱性について  
アニメーションで解説

<http://www.ipa.go.jp/security/vuln/7incidents/>



ウェブサイトの脆弱性による被害を中心とした7つの具体的な事件を  
題材に、ロールプレイング形式で体験的に学習

[http://www.ipa.go.jp/security/vuln/vuln\\_contents/](http://www.ipa.go.jp/security/vuln/vuln_contents/)

# 組織としてセキュリティに取り組む

- 情報セキュリティ対策ベンチマーク

設問に答えるだけで、自社のセキュリティレベルを他社との比較で診断することのできるシステム

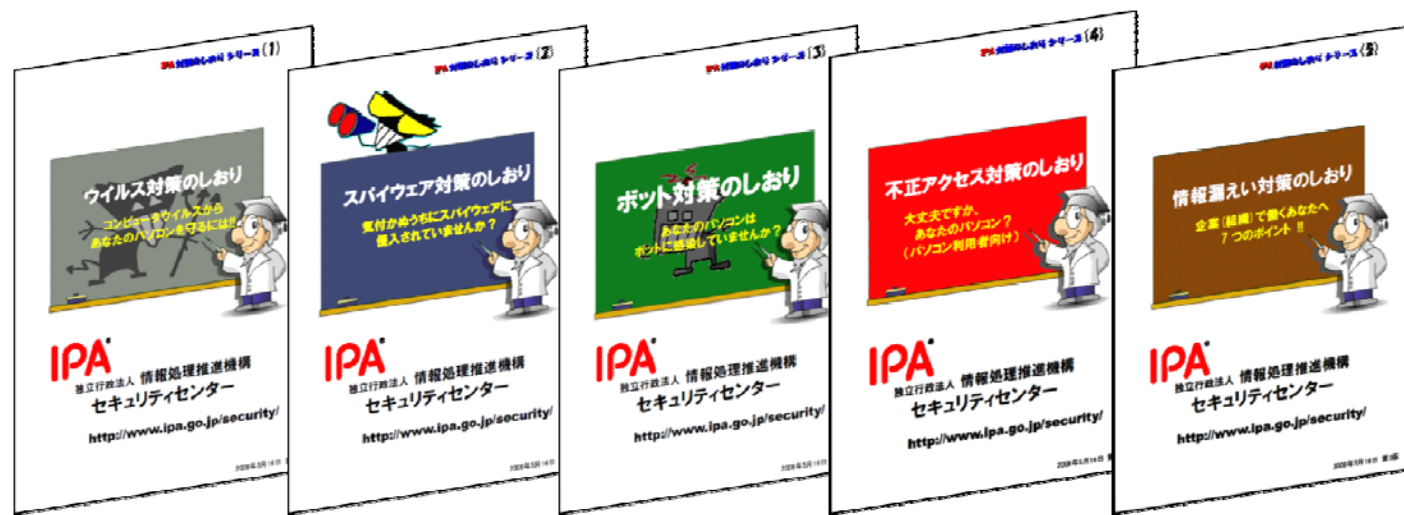
<http://www.ipa.go.jp/security/benchmark/>

- JNSA セキュアシステム開発ガイドライン

「Webシステム セキュリティ要求仕様(RFP)」編

[http://www.jnsa.org/active/2005/active2005\\_1\\_4a.html](http://www.jnsa.org/active/2005/active2005_1_4a.html)

# 脅威への対策のためのしおり



ウイルス対策

スパイウェア対策

ボット対策

不正アクセス対策

情報漏洩対策

ウェブ  
書籍

- 一般の家庭や企業向けに、情報セキュリティ上の様々な脅威への対策を分かりやすく説明したもの

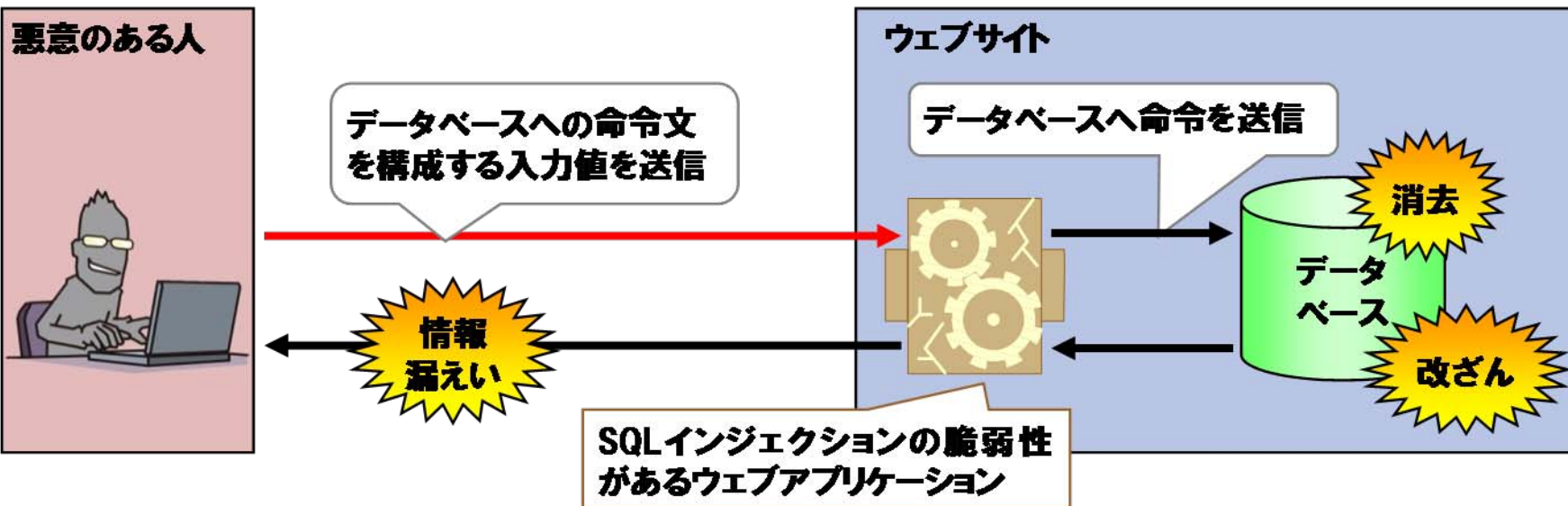
<http://www.ipa.go.jp/security/antivirus/shiori.html>

## デモ:SQL インジェクションの脆弱性

# SQLインジェクション

## SQL インジェクション

SQL インジェクションの脆弱性がある場合、悪意あるリクエストにより、データベースの不正利用をまねく可能性があります。



# なぜ SQL 文の挿入が可能だった？

- 特別な意味を持つ記号文字の扱いが不適切。  
' (シングルクォート) : テキスト文字の引用符

```
SELECT * FROM a WHERE id=' $p' ;
```

\$p=foo の場合 :

```
SELECT * FROM a WHERE id=' foo' ;
```

\$p='foo' or 'a'='a' の場合 :

```
SELECT * FROM a WHERE id=' foo' or 'a'='a' ;
```

変数中の記号文字が意味のある文字として解釈される。

# まとめ

- IPA では、ウェブサイト safely にする、さまざまなコンテンツを公開しています。
- 企画、開発、運用など、各段階で活用することができます。
- ぜひ、IPA のコンテンツを利用ください。

※ SQLインジェクションのデモで行った攻撃は、実際に稼働するウェブサイトに対しては、行わないでください。

**ご静聴ありがとうございました**

**ご質問を受け付けます**