

## SQLインジェクション対策について

1. SQL インジェクションの問題と脅威
2. SQL インジェクションの仕組みと対策
3. 攻撃の痕跡を見つける
4. まとめ

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  
谷口 隼祐

## 1. SQLインジェクションの問題と脅威

# こんなニュース聞いたことありませんか

- クレジットカード番号や個人情報の漏えい
  - 音響機器・楽器販売サイト
  - 健康食品や医薬品販売サイト
  - 化粧品販売サイト
- ウイルス感染などを引き起こすウェブサイトの改ざん
  - ウイルス対策ソフト開発会社
  - 自動車情報サイト
  - 政府関連のウェブサイト
  - 家庭用ゲーム会社のウェブサイト(米国)



**共通点**

**SQLインジェクション攻撃による被害**

# オンラインゲームにおける問題

- ウイルス感染を引き起こすように、ゲームの公式サイトが改ざんされてしまう (2008年5月、7月)\*
- ブログ運営サイトで、多数のゲーム関連ブログにゲームのアカウントを盗むウイルスが貼りつけられていた\*

\* 公式のアナウンスはないが、SQLインジェクションの脆弱性をついた攻撃の可能性はある

アカウント、アイテム、仮想通貨などのオンラインゲームで扱う情報を現実の通貨で売買する行為 (Real Money Trade) が存在している



- それらの情報を手に入れることができれば、**お金**になる
- 一部の人は、不正をしてでも情報入手したいと考える

パスワードを盗むウイルスの40~50%は、オンラインゲームのパスワードを狙ったウイルスとの報告もある  
(米国マカフィー)



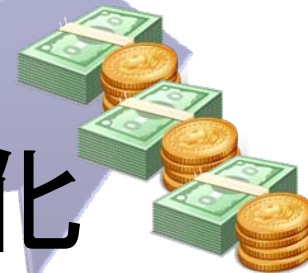
# オンラインゲームと SQL インジェクション

## SQLインジェクションの位置づけ



現金化

RMT



高価値データの取得

- ・ SQLインジェクション

被害

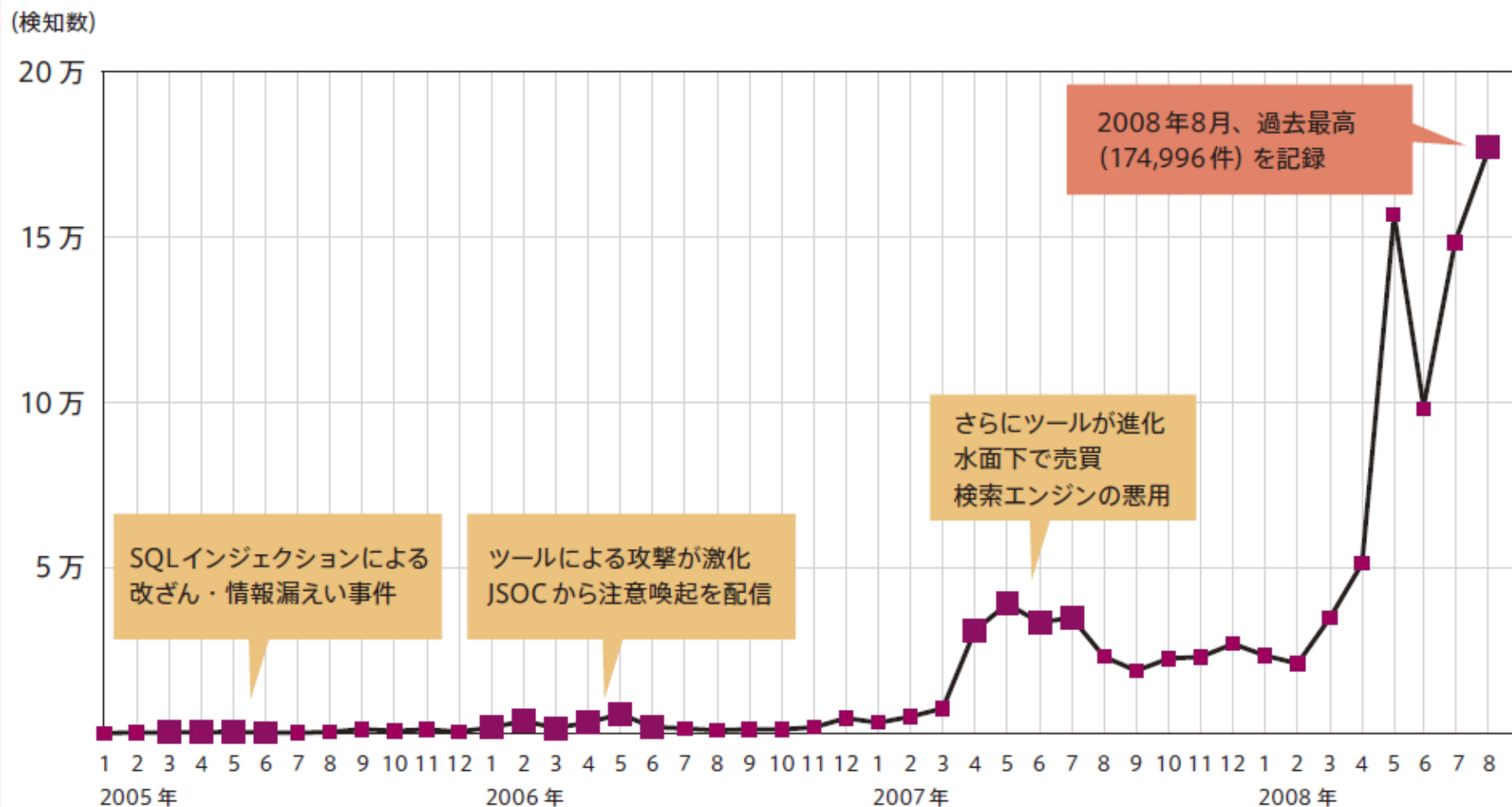
オンラインゲームのアカウント情報が漏えいしてしまう

ウェブサイトが改ざんされ、ウェブサイト閲覧者をウイルス感染させてしまう → アカウント情報が漏えい

参考: ITpro 急増するSQLインジェクション攻撃  
攻撃の背後にはRMT市場の拡大あり

<http://itpro.nikkeibp.co.jp/article/COLUMN/20080930/315843/>

# SQLインジェクションの攻撃傾向



出典: 株式会社ラック「侵入傾向分析レポート Vol.11」より  
[http://www.lac.co.jp/info/jsoc\\_report/\\_vol11.html](http://www.lac.co.jp/info/jsoc_report/_vol11.html)

# SQLインジェクションの脅威

- データベースを直接操作されてしまう



- 秘密情報、個人情報等の漏えい

直接情報を盗まれる

- データベースに格納していたクレジットカード情報の漏えい
- ゲームなどのアカウント情報の漏えい

- 重要情報の改ざん、破壊

間接的に情報を盗まれる

- ウェブサイト上にウイルスを埋め込まれる
- 攻撃者に都合の良い情報に書き換える



## 2. SQLインジェクションの仕組みと対策

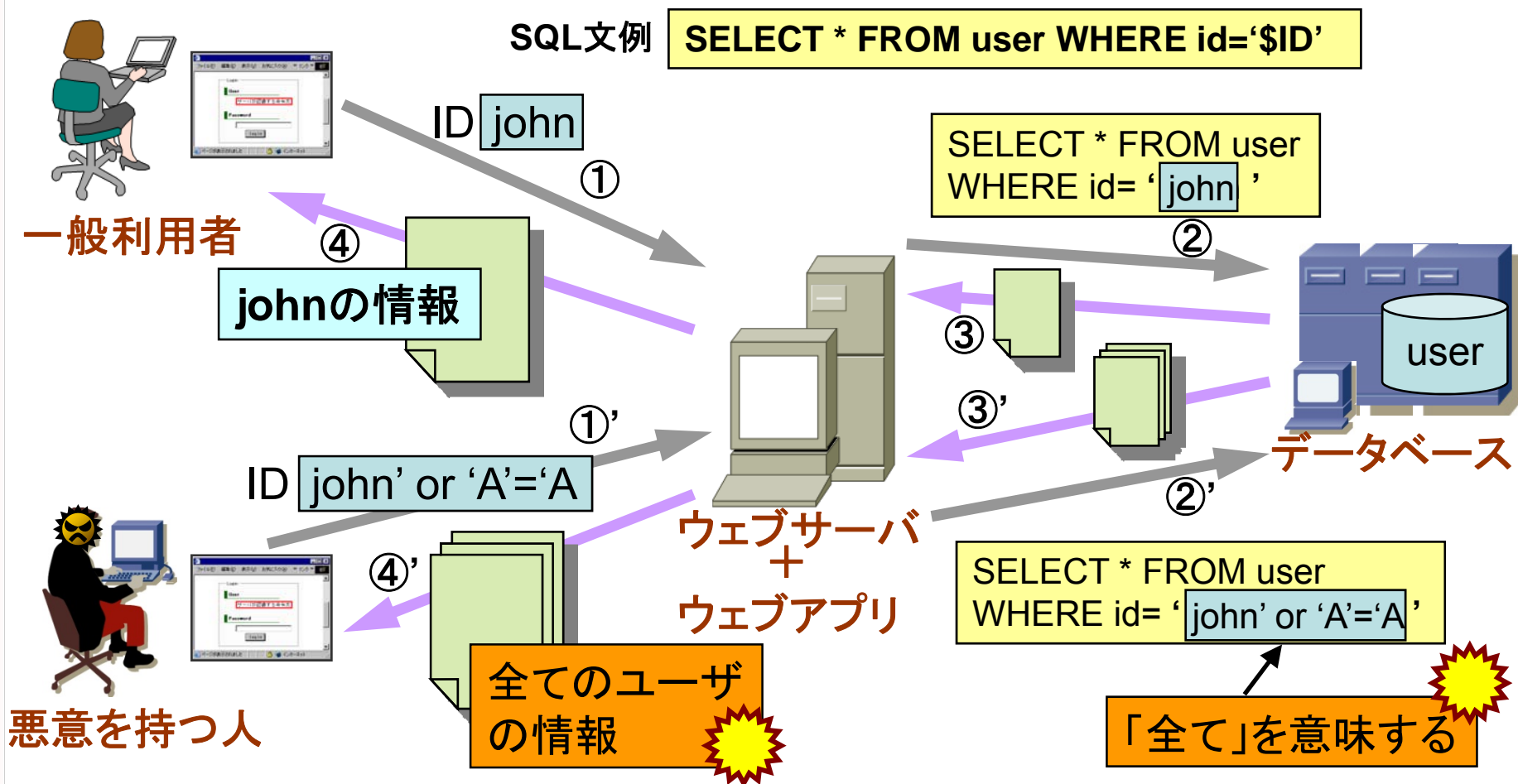
# SQLインジェクションとは？

- どのような問題？
  - データベースを不正に操作されてしまう問題
    - セキュリティ上の弱点(脆弱性)のひとつ
- 影響を受けるシステムの構成は？
  - データベースと連携しているシステム
    - 特にウェブサーバ上で動作するウェブアプリケーションに多く存在する
- 原因は？
  - データベースへの命令の組み立て方に問題



※SQL : リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。

# SQLインジェクションの仕組み



**・データベースから重要な情報が盗まれてしまう**

# SQLインジェクション対策

## ウェブアプリケーションのプログラム上の問題

### • 根本的解決

「脆弱性の原因を作らない実装」を実現

#### – エスケープ処理

##### • バインド機構の利用

– プレースホルダ、バインド変数、準備された文(Prepared Statement)

##### • バインド機構以外でのエスケープ

– エスケープ関数

(Perl の DBI quote() や PHP の dbx\_escape\_string())

– 置き換え演算子等で自己エスケープ処理  
( s/'"/g; など)

# 根本的解決

## ・ エスケープ処理の実施

特別な意味を持つ記号文字が普通の文字として解釈されるように処理する

例：' → ''（同じ文字の繰り返し）

\$p='foo' or 'a'='a' の場合：

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

変数中の '（シングルクォート）が、普通の文字として解釈される

# エスケープ処理の実装例（根本的解決）

- ・ バインド機構を利用（例: Perl DBI）
  - 独自の処理でエスケープ処理をする必要がなくなる

```
$sth = $dbh->prepare(  
    "SELECT id, name, tel, address, mail FROM usr  
    WHERE uid=? AND passwd=?");  
$sth->execute($uid, $passwd);
```

バインド変数

プレースホルダ

参考：セキュアプログラミング講座

第6章 入力対策 SQL注入: #1 実装における対策

<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/502.html>

# 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」

- エラーメッセージを非表示にする
  - 詳細なデータベースに関するエラーメッセージをウェブページに表示させない
  - エラーを表示するとしても、内容は最小限に
- データベースアカウントの権限見直し
  - 「権限全部入り」のアカウントは使わない
    - 権限を必要最小限にすれば、防げる攻撃もある
- その他の対応
  - 収集する情報を見直す
  - DBに格納する情報を見直す
  - パスワードはそのまま保存しない

# SQLインジェクションの対策のまとめ

- SQL文の組み立てには必ずエスケープ処理を実装する
  - バインド機構を推奨
- その他の対策については、「安全なウェブサイトの作り方」、「セキュアプログラミング講座」を参照



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>

IPA セキュア・プログラミング講座

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

## 3. 攻撃の痕跡を見つける

# iLogScannerの紹介

- SQLインジェクションやクロスサイト・スクリプティング等の攻撃の有無を調査
- ウェブサーバのログから解析
- 被害を受けていないか自己チェックするために利用

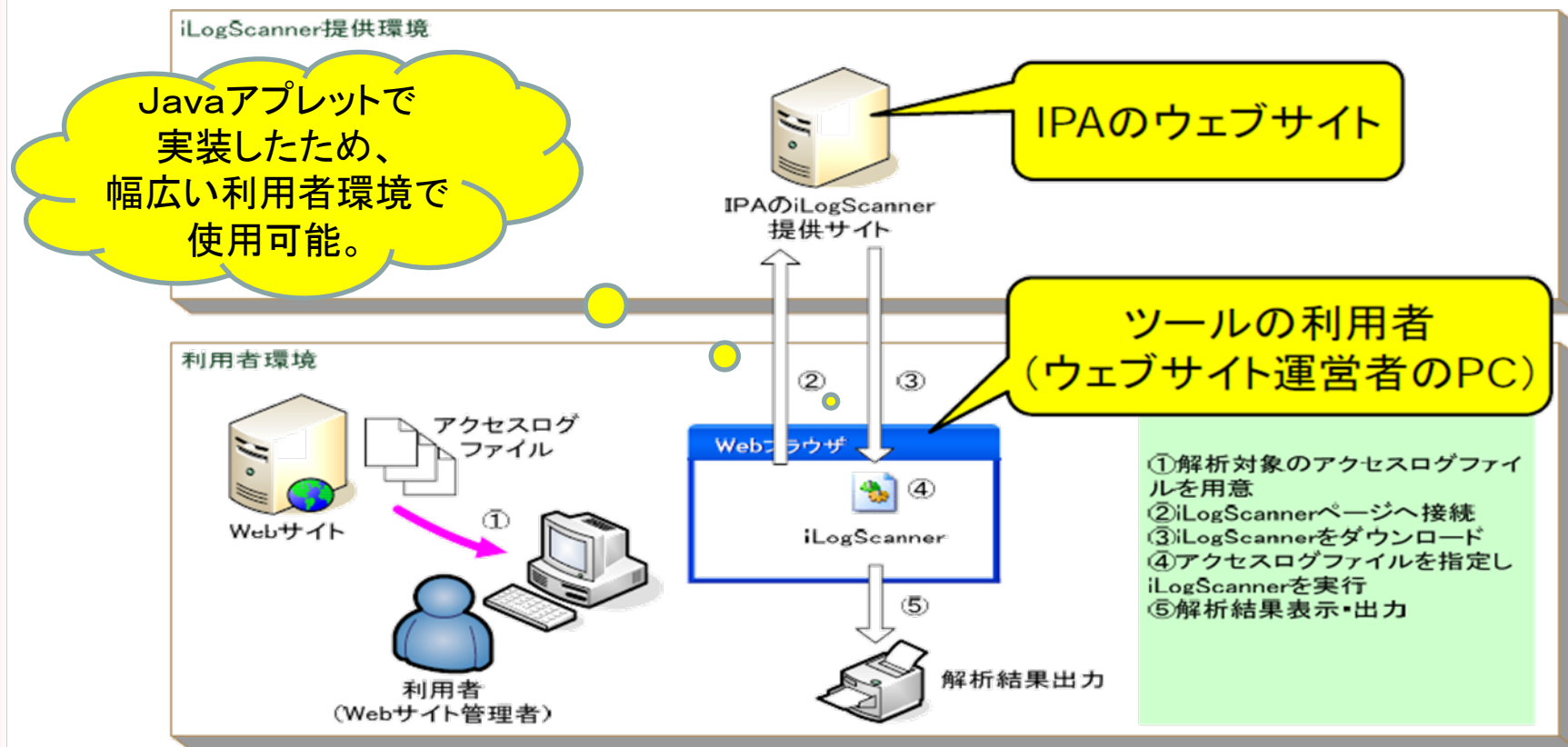


図1. 脆弱性検出ツールの利用イメージ



# iLogScannerの利用例

- IPA で公開しているウェブサイトの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

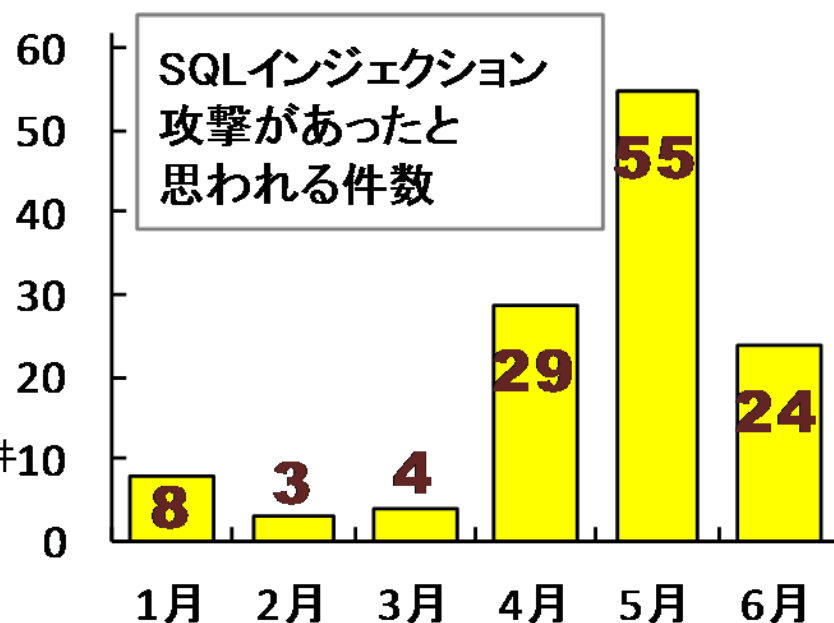
## 3.「iLogScanner」の解析結果

(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

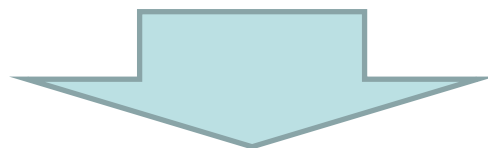
## 4.ログの詳細調査結果

- 攻撃に成功した件数:0件



# 自組織内での活用

iLogScannerでSQLインジェクション攻撃の痕跡がないかどうか確認してみてください



- 攻撃が検出された場合
  - 特に攻撃が成功した可能性が検出された場合は、ウェブサイトの開発者やセキュリティベンダーに相談されることを推奨します
- 攻撃が検出されない場合
  - 「検出されない＝脆弱性が存在しない」というわけではないので、引き続き脆弱性対策を実施してください

## 4. まとめ

# 全体のまとめ

- SQLインジェクション攻撃は増加しており、さまざまな被害が発生している
  - アカウントやクレジットカード情報の漏えい、不正サイトへの誘導やウイルス感染を目的としたウェブサイト改ざんなど
- 根本的解決は、ウェブアプリケーションでのエスケープ処理の実施
  - SQL文に出力する際にバインド機構を用いてエスケープ処理を行うことを推奨
- まずはiLogScannerで調査をして、攻撃されていないかどうか確認してみてください

# 付録：情報セキュリティ対策関連情報

## 脆弱性の理解

- 「知っていますか？脆弱性(ぜいじゃくせい)」- アニメで見るウェブサイトの脅威と仕組み -

詳細はこちら

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

## 脆弱性を作らないために

- 「安全なウェブサイトの作り方 改訂第3版」

詳細はこちら

[http://www.ipa.go.jp/security/vuln/documents/website\\_security.pdf](http://www.ipa.go.jp/security/vuln/documents/website_security.pdf)

- 新版「セキュア・プログラミング講座」

詳細はこちら

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

- 「TCP/IPに係る既知の脆弱性に関する調査報告書 改訂第3版」

詳細はこちら

[http://www.ipa.go.jp/security/vuln/vuln\\_TCPIP.html](http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html)

## ウェブサイトの事件を体験

- 「安全なウェブサイト運営入門」- 7つの事件を体験し、ウェブサイトを守り抜け！ -

詳細はこちら

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

# 情報セキュリティ対策関連情報(つづき)

## 脆弱性攻撃の状況把握

- ウェブサイトの脆弱性検出ツール iLogScanner

詳細はこちら

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

## 脆弱性が発見されたら

- ウェブサイト運営者のための脆弱性対応ガイド

詳細はこちら

[http://www.ipa.go.jp/security/ciadr/vuln\\_website\\_guide.pdf](http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf)

- 「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」

詳細はこちら

[http://www.ipa.go.jp/security/ciadr/vuln\\_announce\\_manual.pdf](http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf)

## 不正アクセスの被害を受けたら

- 不正アクセスに関する届出

詳細はこちら

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

# 情報セキュリティ対策関連情報(つづき)

## 利用者のセキュリティ対策

### ● ウイルス対策

詳細はこちら

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

- ・ウイルス対策ソフトや定義ファイルを最新にする
- ・OSやアプリケーションにセキュリティパッチを適用する
  - Windows 利用者は、Microsoft Update を定期的実施
  - メール、ブラウザ、PDF 閲覧ソフト、オフィスソフトにセキュリティパッチを適用する

### ● フィッシング (Phishing)対策

詳細はこちら

<http://www.ipa.go.jp/security/personal/protect/phishing.html>

- ・メールに記載されているリンクからアクセスするのではなく、お気に入りに登録したアドレスからホームページを見るようにする
- ・カード番号や暗証番号を入力するような依頼メールが届いた場合、情報を入力する前に、そのメールの真偽を確認する

ご清聴ありがとうございました