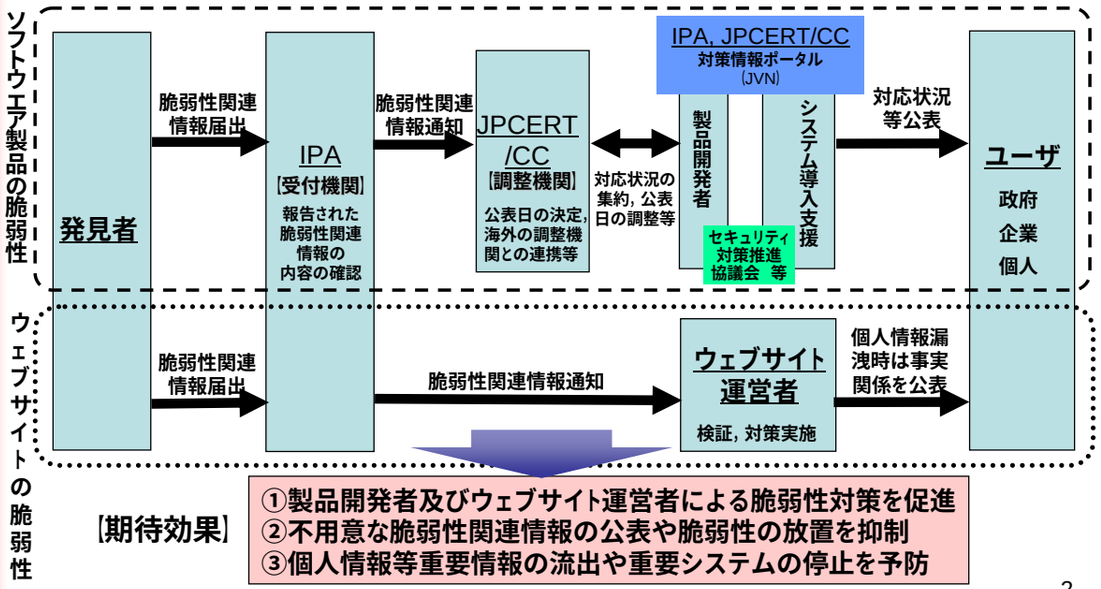
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

最近の脆弱性関連情報の届出事例とその解決策

IPAセキュリティセンター
情報セキュリティ技術ラボラトリー
田原 美緒

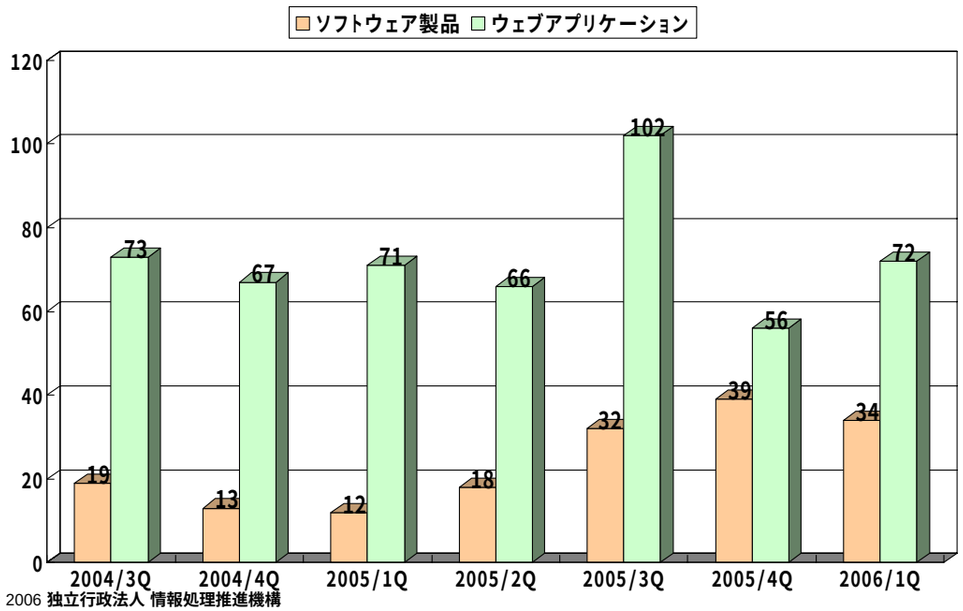
「情報セキュリティ早期警戒パートナーシップ」について

- 「情報セキュリティ早期警戒パートナーシップ」ご存知ですか？



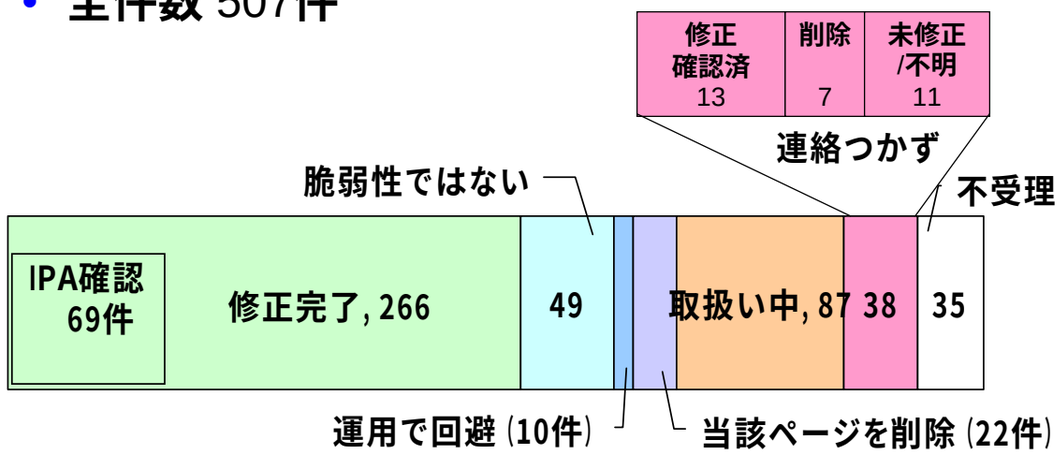
届出件数の推移

- 届出件数の推移 (2004年7月～2006年3月31日)



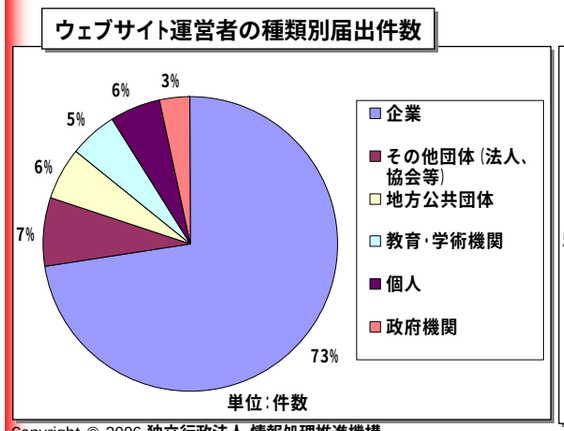
ウェブアプリケーション届出の対応状況

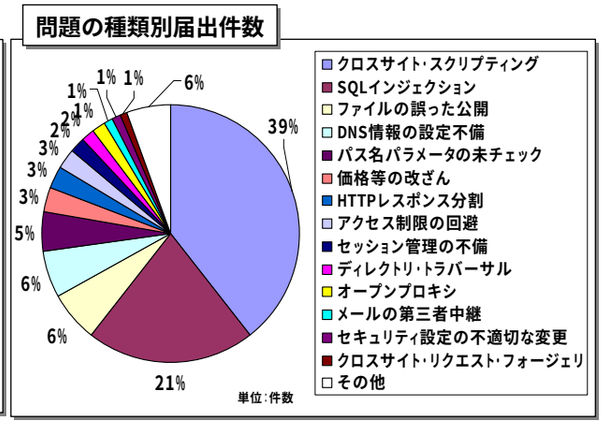
- 2006年3月31日 17:00時点
- 全件数 507件



受理した届出の内訳

- クロスサイト・スクリプティングの問題に関する届出が最多だが、SQLインジェクションの問題の問題も増加
- 届出全体の約3/4は企業ウェブサイトの問題





目次

- 不受理の届出および修正以外で取扱いを終了した届出について
- 脆弱性分類ごとの届出事例
- 届出から見るウェブアプリ脆弱性への対策
- IPAの運用上の課題とお願い事項

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

不受理の届出および修正以外で取扱いを終了した届出について

不受理の届出

- 主に日本国内からのアクセスを想定していない
- 届出内容から問題がないことが確認できた
  - 発見者の確認ミス
  - 「可能性」段階の届出で実際は問題がないことが明確
- 脆弱性かどうか判断できない
  - 情報が少ない、具体的でない
  - 発見者に質問しても返ってこない
- 問題はあるが、本枠組みの脆弱性とは言いがたい
  - 個人情報の入力フォームで通信が暗号化されてない！
  - オンラインショップアプリのソースコードが見える
  - サイトが改竄されている

修正以外で取扱いを終了した届出

- 脆弱性がないことを確認
  - 「可能性」の段階で届け出られた問題が、実際にはなかったというもの
- システム上の修正・変更ではなく運用で回避
  - バックエンドで、人が確認している（価格等の改ざん）
  - パスワード変更の呼びかけを強化（初期パスワードの不備）
- 当該ページを削除
  - 必要がないファイルだったため削除
  - 修正方法がわからないため削除

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

脆弱性分類ごとの届出事例

よくある届出、届出事例について

クロスサイト・スクリプティング

- よくある届出
  - 入力フォームにスクリプトを入力してみたら、次画面で実行された
  - URL中の引数がそのままHTMLソースに反映されているため、そこにスクリプトを入れてみたら実行された
- 届出事例
  - 外部サイトへのリンクに使用するリダイレクタの引数にスクリプトを入力すると、リンク先のページを表示する前の確認ページでスクリプトが実行される

SQLインジェクション

- よくある届出
  - SQLエラー画面を見つけた、表示された
    - 検索結果から
    - URLの末尾が欠けた状態でアクセスしたら表示された
    - 何も入力せずにログインボタンを押したら表示された
    - Cookieを無効にして操作したら表示された
- 届出事例
  - SQL 文そのものがURLパラメータに含まれている
    - 商品券のサイトで絞込検索結果をブックマークしようとしたが、できなかったためHTMLのソースを表示したところ、以下の記述を発見した

```
<input type="hidden" name="SQL" value="SELECT a.*
FROM ...省略... ">
```

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

- よくある届出
  - hiddenの値に、ファイル名が直接書いてある
    - 過去に話題になった事例と同じファイル名なので同じ問題があるのでは？

```
<input type= "hidden" name="file" value="foo.csv">
```

    - “../ ”をつけたら他のページが閲覧できた
- 届出事例
  - URL内のパラメータにファイル名が使われていた
    - パラメータに“../ ”を含ませたら、含ませないときと同じファイルが表示された
    - パラメータの最後に“ / ”や “/. ”をつけたら、そのファイルが開けない旨のエラーが表示された
    - パラメータに“../ ”を含むファイル名が含まれていた

価格等の改ざん

- よくある届出
  - hidden の値に価格が含まれている

```
<input type="hidden" name="goods" value="パーティーバッグA">
<input type="hidden" name="price" value="20000">
```


HTTPレスポンス分割

- よくある届出
  - URLに含まれる文字列が、HTTP 応答ヘッダの location: フィールドにそのまま含まれる。ためしにURL末尾に“%0d%0aSet-Cookie:test”を付けてみたら、Cookieが発行された

セッション管理の不備

- よくある届出
  - セッションの管理に秘密情報が使われていない
    - hiddenの値でセッション管理をしているようだが、その値が第三者でも入手できる情報だった
    - Cookieでセッション管理をしているようだが、含まれる値がユーザIDのみである
    - URL内にIDが含まれており、IDを変えることで他のユーザの関連操作ができる
  - セッション管理情報の推測が容易
    - 複数アカウントを作成したら、Cookieに含まれるセッション管理情報の生成規則がわかってしまった

セッション管理の不備（続き）

- 届出事例
  - パスワードリマインダ機能で、「秘密のパスワード」がなくても、新しいパスワードをセットできた
    - hiddenの値でセッション管理
    - その値はユーザID さえわかれば誰でも入手できる情報だった
  - ウェブメールのURLにID、パスワード（暗号化）が含まれていた（Refererから発見）

メールの第三者中継

- よくある届出
  - hiddenの値に送信先アドレスが書かれており、そこを変更して他の宛先にメール送信が可能
- 届出事例
  - 地方自治体サイトの「あなたの携帯電話にURLをメールで送る」という機能で、hiddenの値にSubjectが書かれており、書き換え可能だった

    → そもそも宛先アドレスは自由設定で、Subject、結果的に本文が利用者から設定可能

DNS情報の設定不備

- よくある届出
  - DNSの情報を調べていて発見
    - DNS サーバに不適切な情報が登録されているため、第三者がそのドメイン名の持ち主であるかのようにふるまえてしまう

      → ウェブやメールの横取り、フィッシング詐欺

ファイルの誤った公開

- よくある届出
  - 個人情報のようなファイルが公開されている
  - 公開を意図していないと思われるディレクトリの一覧が見える
    - メールアドレスを検索したらファイルに当たった
    - ディレクトリを遡ったら、それらしいファイルがあった
  - コンテンツ管理画面が認証もなく公開されている
- 届出事例
  - アクセス解析用のcgiが使われており、公開されているアクセス解析データに到達できた。そこから「社員のページ」というページにアクセスできた

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

届出から見る
ウェブアプリ脆弱性への対策

出力時に正しく処理する

- ページ生成時のhtmlのエスケープ処理 (クロスサイト・スクリプティング)
  - 入力内容をチェックして置換・削除する処理は、抜けが発生することもある
    例：クロスサイト・スクリプティングの対策のために、入力値から<script> を削除する場合、<Script △>で抜けてしまった
- HTTPレスポンスヘッダ作成時に改行コードを削除 (HTTPレスポンス分割)

利用者が変更可能なパラメータの扱いに注意する

- type="hidden" で隠した値やURL内のパラメータが利用者に変更された結果、問題が発生することが多い
  - 特定のディレクトリのファイルしか扱えないようにする (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)
  - 利用者が変更する必要の無い値はプログラム内で持ち、公開する値も変換表などを使い、利用者が任意に値を書きかえられないようにする (メールの第三者中継、価格等の改ざん)

既存、標準の機能を利用する

- Prepared Statement (SQLインジェクション)
- パスからファイル名を抜き出すAPIなど (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)
- htmlエスケープ処理する関数 (クロスサイト・スクリプティング)
- ライブラリや既存の暗号アルゴリズム (セッション管理の不備)

他者が作成したCGIの利用に注意する

- 利用者に入力させた情報を公開フォルダに保管するようになっていないか？
  - パーミッションの設定やアクセス制御が必要（ファイルの誤った公開）
- 本来固定のパラメータの値を利用者が変えられるようになっていないか？
  - 問合せフォーム等では、利用者が送信先アドレスを変えられる必要はない（メールの第三者中継）

設定、運用、ポリシー等の問題

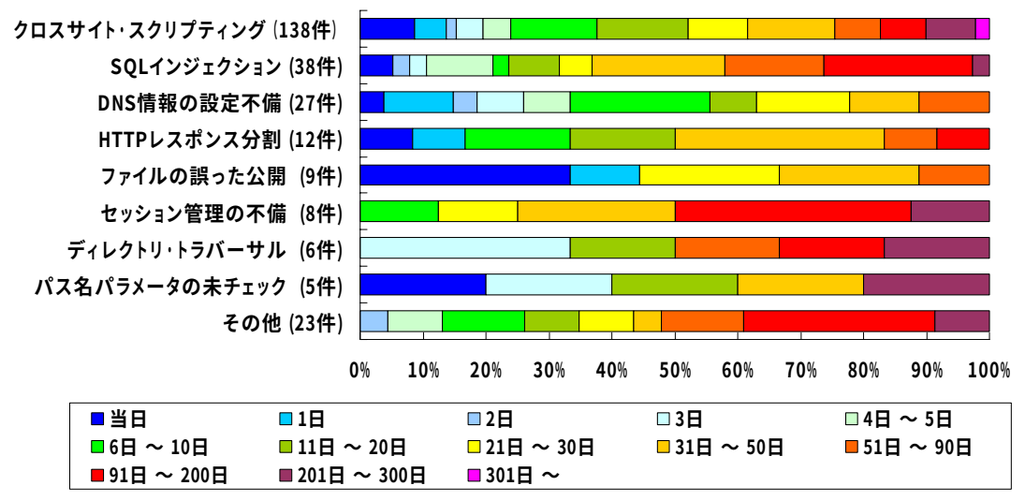
- パーミッション、アクセス制限の設定忘れ・誤設定（ファイルの誤った公開）
- 設定ミス、更新し忘れ（DNS 情報の不適切な設定）

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

IPAの運用上の課題とお願い事項

届出の修正に要した日数

- 2006年3月31日現在
  - 連絡当日に修正の報告があったものもある
  - 「セッション管理の不備」の修正は、時間がかかる傾向にある



修正が進まない背景…

- 話が伝わらない
  - 担当者までなかなかたどり着かない
  - 「うちは大丈夫」といった印象
- 予算獲得が困難？
  - 作った人が運用している場合は、その人さえ動ければOK
  - 作った人が別の場合は、誰が直す？新たに費用が必要
- 直し方がわからない
  - 昔作ってはもらったけど、開発者との関係が途絶えている
  - 連絡をもらっても、誰にいえばいいのかわからなくなっている
  - でも自分ではわからないし…

修正が進まない背景… (続き)

- 脅威が充分伝わっていない
  - XSS：Cookie 漏洩のイメージが強いが…
    - フィッシング詐欺への悪用
    - 表示されている情報の漏洩や変更
    - 利用者が入力する情報の漏洩
  - SQLインジェクション:個人情報漏洩のイメージが強いが…
    - 個人情報以外の情報の漏洩
    - データベース内の情報の改ざん
- IPAからもっと具体的でイメージしやすい情報を出していく
- 届出してくださる発見者の方もご協力を

届出で頂きたい情報

1) 脆弱性を確認したウェブサイトのURL
2) 脆弱性の種類
   一般的な名称や届出の四半期プレスで使っている名称
   なければ、その問題を的確に表していればOK
3) 脆弱性の発見に至った経緯
   どういう経路でたどった場合に、どういう動作をした/状態であったか
4) 脆弱性であると判断した理由
   なぜそれがセキュリティ上の問題であると判断したか
5) 脆弱性により発生しうる脅威
   誰に対してどんな被害が生じるか
   一般的な話ではなくそのサイトに特化した話で
6) ウェブサイトの連絡窓口
   サイトに記載されたアドレスやその他の窓口があれば
7) その他

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ご聴講ありがとうございました