IPAへの脆弱性情報の届出

はせがわようすけ
hasegawa@openmya.hacker.jp
Microsoft MVP for Windows - Security
(2005.10-2006.09)

注意事項

悪用厳禁!!

・違法行為はしないように!

・モラルある行動を

脆弱性って何？

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその**機能や性能を損なう原因となり得る安全性上の問題箇所**。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

ソフトウェア等脆弱性関連情報取扱基準

(平成16年度経済産業省告示 第235号)

脆弱性関連情報の届出制度

- 2004年7月より開始
- ソフトウェア製品、Webアプリケーションについて受付
- 受付機関はIPA
- 調整機関はJPCERT/CC

届出の対象

- **ソフトウェア製品**
  OSやブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタやICカード等のソフトウェアを組み込んだハードウェア等

- **Webアプリケーション**
  インターネット上のウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステム

「脆弱性関連情報に関する届出について」より
http://www.ipa.go.jp/security/vuln/report/index.html

どうやって届け出るの？

- 電子メールまたはWebフォームから報告
- ソフトウェア製品とWebアプリで報告の書式が異なる
- Webフォームでの届出は手元に控えが残らない

届出の記入例

IPAの提供しているサンプルを見てみよう

不受理の例

こんなのは不受理になります

- ❖ 最新版では修正されている脆弱性
- ❖ 海外で提供されているWebアプリケーション
- ❖ 具体的な脅威が想定できないもの

➔ バグか脆弱性かの判断は誰がするの？

脆弱性じゃないけど受理

MUAの仕様がフィッシングに利用される

```
From: info@card.example.com
Reply-To: info@card.example.com
      <hasegawa@openmya.hacker.jp>
Subject: カード番号を連絡下さい
```

返信した場合に、宛先欄でアドレスが
表示されず、表示名のみ

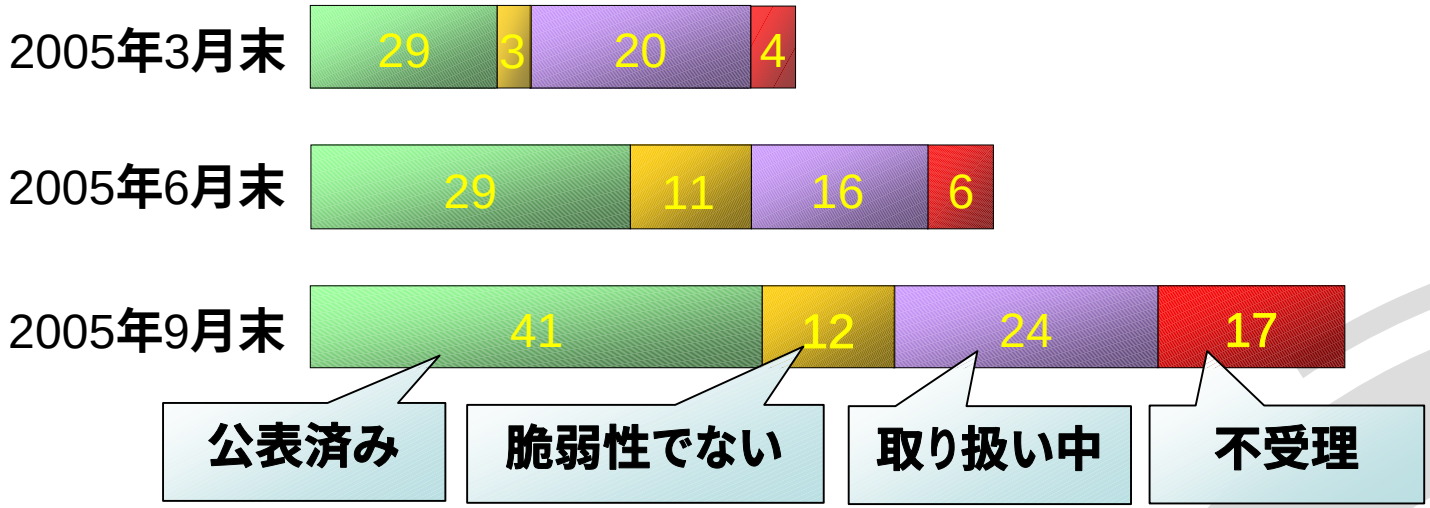
脆弱性じゃないけど受理

- 届出時点で「脆弱性ではない」と明記
- 開発元は「仕様である」との返答
- IPAから開発元に対して仕様変更の検討を依頼

➔ 脆弱性でなくても脅威が想定できればできれば受理されることもある

最近、不受理が増えてる？

ソフトウェア製品の脆弱性の推移



ソフトウエア等の脆弱性関連情報に関する届出状況
[2005 年第3 四半期 (7 月～9 月)]
http://www.ipa.go.jp/security/vuln/report/documents/vuln2005q3.pdf

最近、不受理になった例

- **報告内容**
  あるアプリケーション上でAというファイルを開こうとすると、Bというファイルが開かれてしまう。AおよびBには、実行可能なマクロを含めることが可能。
- **IPAからの回答**
  もともと許可されたファイルを開くことが可能になるだけ。

とはいえ・・・

- 不受理でも開発元へ情報提供
- 同種の脆弱性が多ければ受理
- 不受理でも脅威をきちんと説明できれば受理されるかも？

まとめ？

- 制度自体は非常に有効
- 疑問は遠慮なく問うべき
- 脆弱性情報のさらなる周知

まっちゃ１３９紹介

- Webサイト
  - http://matcha139.hiemalis.org/
- メーリングリスト
  - http://ml.s-lines.net/mailman/listinfo/matcha139
- 勉強会
  - 3〜4ヶ月に一度、京都を中心に勉強会を開催
  - 開発系の話、管理運用系の話、若手教育の話など