「もしも」のときに

不正アクセス事例に学ぶホームページ管理（再）

大阪府産業デザインセンター
デザイン専門員　木下　敏夫

不正アクセス事例に学ぶホームページ管理（再）

- 不正アクセス発見
- その時どうした？
- その後どうした？

不正アクセス発見時の経緯

- bmb.oidc.jp のバージョンアップ作業時を実施中
- それまでアクセス出来ていたページが急に表示できなくなった。

不正アクセス発見時の経緯

- 幾つかの確認の結果　・・・
- .htaccess というファイルにこれまで見たことのない行が追加されているのを発見
- 不正アクセスによるサイト改竄が行われたと判断

そのときどうした？

- webサーバー機能を停止
- 大阪府産業デザインセンター川本氏に不正アクセスされている可能性を報告
- 原因究明の為、ログやコンテンツの保全をサーバー管理会社に連絡
- 会員及び閲覧者に対する情報提供
- 報道発表
- 原因究明を（地独）大阪府立産業技術総合研究所 に依頼

その後どうした？

- サーバー会社から不正アクセスを受けたHDDを提供してもらい丸ごとコピー
- コピーしたHDDを産技研で解析

で？

- 不正アクセスは
  - phpMyAdmin というツールの脆弱性を狙われた
  - 5月1日に最初の不正アクセスに成功している
  - それから2週間後にサイトの改竄を実施

```
----------------------------------------------------------------------------------------------------
Feb/2011:18:21:32 +0900] "GET //phpMyAdmin-2.8.2/scripts/setup.php      HTTP/1.1" 404 465 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
Mar/2011:17:32:19 +0900] "GET /phpMyAdmin/scripts/setup.php             HTTP/1.1" 200 14054 "-" "Mozilla/3.0 (compatible; Indy Library)"
May/2011:13:50:13 +0900] "GET /phpMyAdmin/scripts/setup.php             HTTP/1.0" 200 14033 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
May/2011:00:09:11 +0900] "GET /phpMyAdmin/scripts/setup.php             HTTP/1.0" 200 14033 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
May/2011:04:28:22 +0900] "GET /phpMyAdmin/scripts/setup.php             HTTP/1.1" 200 14054 "-" "Mozilla/3.0 (compatible; Indy Library)"
May/2011:14:22:29 +0900] "GET /phpMyAdmin/scripts/setup.php             HTTP/1.1" 200 14033 "-" "Mozilla/5.0 (Windows)"
May/2011:14:22:31 +0900] "POST /phpMyAdmin/scripts/setup.php            HTTP/1.1" 500 780 "-" "Mozilla/5.0 (Windows)"
----------------------------------------------------------------------------------------------------
```

で？

- phpMyAdminは
  - データベース管理の為のWebプログラム
  - サイト構築の際に自分たちで導入したもの
  - 利用後使わなくなったのでバージョンアップ等せず放置
  - 最新のバージョンであれば脆弱性対策がされていた

まとめると

- 被害拡大の防止の為に
  - 物理的切断
- 2次被害防止の為に
  - 情報公開
- 再発防止の為に
  - 原因究明
  - 啓蒙活動

ちなみに

- 不正アクセスの攻撃目標は無差別
  - プログラムで自動的に検索され目標にされる
- 不正アクセスと被害発生時期は、ずれることもある
  - 不正アクセスがあってから数か月後に発生することも
- データが回復できないこともある

ということで

- ホームページを公開している企業は
  - サーバーのセキュリティ対策の実施
  - CMS等の更新
  - バックアップの作成
  - 不必要なものを残さない
- 個人情報は
  - サーバーに残さない
  - 必要最低限の情報だけにする