【TOPIC】

神戸大学の 2013 年第一四半期における情報セキュリティ状況

情報基盤センター
ネットワーク基盤研究部門/CISO 補佐
鳩野逸生

1. はじめに

2012 年度には，情報セキュリティに関する事件が数多く報道されたことは記憶に新しい．中でも，PC からの脅迫に対する誤認逮捕, 外交問題と関連したサイバー攻撃などが大きなものとしてあげられる．本稿では，2013 年第一四半期における神戸大学に向けられているサイバー攻撃の状況について概要を報告する．

2. サイバーアタック監視のための情報取得

神戸大学においては，セキュリティ維持のために，対外接続用 Firewall, 学内 Web サーバ (対外公開用) 防護用の Web Cache 装置が設置されている．これらの装置では，通信の防護の他に学外からの通信状況の把握ができるようなっており，定期的に監視している．また，ネットワーク上で以下のような学外からの通信のモニタリングを行っている[1]．

- 基幹ルータにおけるサンプリングによるパケット取得[2]．
- 対外接続通信のミラーリングポートの監視による，http 通信ログの取得．
- KAISER サーバにおける処理記録 (メール，Web サーバ，KUMA サーバなど)．

取得したデータは，一定期間保存するとともに統計処理され, 神戸大学内の情報基盤の利用状況分析に用いるとともにセキュリティ状況の把握およびインシデント対応に活用している．

3. 主なサイバーアタック

3.1 Web サーバへのサイバーアタック

対外接続用 Web Cache 装置のアクセス記録によると，Web アプリケーションの既知の脆弱性を狙ったと思われるアクセスがほぼ毎日全学の IP アドレスへ向けて実施されている．対象がはっきりと特定できるものは以下の通りである．

- phpmyadmin (mysql の Web による操作インタフェース) における脆弱性を持つバージョンや設定ミス探査
- Tomcat 管理プログラムの設定ミス探査など様々な Web アプリケーションの探査
- WordPress, MovableType のバージョン取得 (脆弱性を持つバージョンの探査?)

特に，phpmyadmin に対するアタックは，ここ数年にわたり継続しており神戸大学内でも数件被害にあっている．いずれも単純な設定ミスあるいは脆弱性を持つ古いバージョンを利用していたためであった．**図 1** に典型的な phpmyadmin を狙ったアタックを示す．Web サーバの管理者にあたっては，CMS(Contents Management System) 等の導入の際にプラグインとして意図せずインストールされていることがあるため，正しくサーバが拒否をしているかログを定期的に確認することが望まれる[3]．

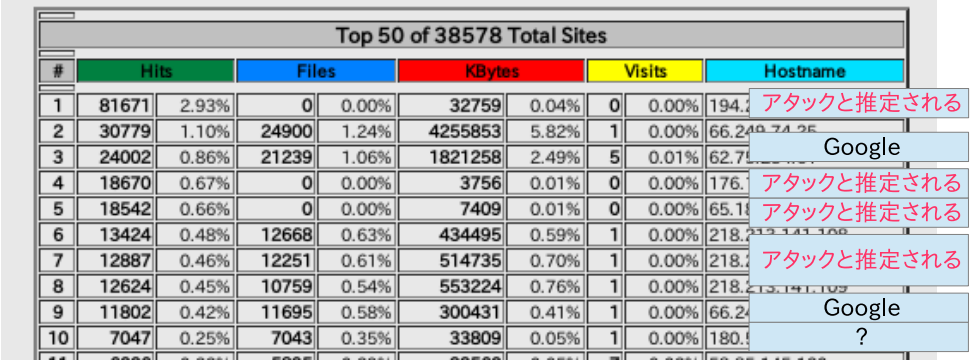
```
5.xx.yy.121 - - [18/Mar/2013:06:48:52 +0900] "GET //admin/phpmyadmin/scripts/setup.php HTTP/1.1" 404 515 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:48:55 +0900] "GET //typo3/phpmyadmin/scripts/setup.php HTTP/1.1" 404 517 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:48:57 +0900] "GET //phpmyadmin/scripts/setup.php HTTP/1.1" 404 514 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:48:57 +0900] "GET //phpmyadmin1/scripts/setup.php HTTP/1.1" 404 514 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:48:58 +0900] "GET //phpmyadmin2/scripts/setup.php HTTP/1.1" 404 514 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:48:59 +0900] "GET //xampp/phpmyadmin/scripts/setup.php HTTP/1.1" 404 517 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:49:02 +0900] "GET //phpmyadmin/scripts/setup.php HTTP/1.1" 404 514 "-" "-"
5.xx.yy.121 - - [18/Mar/2013:06:49:40 +0900] "GET //phpmy-admin/scripts/setup.php HTTP/1.1" 404 514 "-" "-"
```

図 1: phpmyadmin を狙った攻撃の例

図 2 に，2013 年 2 月 13 日における学外から学内への Web アクセスにおいて, Web アクセス数が多い順に並べたアクセス元 IP のうち，上位 10 位分を示す．Hits(Web アクセス) 数が多く，Files(実際に取得したファイル) が 0 あるいは非常に少ないものは攻撃を意図したものと考えられる．また，2013 年に入ってか

[1] 学内通信状況の監視も実施しているが本稿では触れない．
[2] パケット取得には sflow を用いている．
[3] 対外公開申請を行っている Web サーバでは必ず観測されているはず．

らの状況としては，**サーバのレスポンスヘッダ (コンテンツにつけられる Web サーバの状況を示すデータ) のみを取得するアクセス**が急増している点が特徴的である．意図は不明であるが，サーバの状況を調査し，攻撃の準備をしているものと疑わざるを得ない．



Top 50 of 38578 Total Sites

#	Hits		Files		KBytes		Visits		Hostname	
1	81671	2.93%	0	0.00%	32759	0.04%	0	0.00%	194.2	アタックと推定される
2	30779	1.10%	24900	1.24%	4255853	5.82%	1	0.00%	66.249.74.25	Google
3	24002	0.86%	21239	1.06%	1821258	2.49%	5	0.01%	62.75	
4	18670	0.67%	0	0.00%	3756	0.01%	0	0.00%	176.1	アタックと推定される
5	18542	0.66%	0	0.00%	7409	0.01%	0	0.00%	65.1	アタックと推定される
6	13424	0.48%	12668	0.63%	434495	0.59%	1	0.00%	218.2	
7	12887	0.46%	12251	0.61%	514735	0.70%	1	0.00%	218.2	アタックと推定される
8	12624	0.45%	10759	0.54%	553224	0.76%	1	0.00%	218.2	
9	11802	0.42%	11695	0.58%	300431	0.41%	1	0.00%	66.24	Google
10	7047	0.25%	7043	0.35%	33809	0.05%	1	0.00%	180.5	?

図 2: Web アクセスが多い送信元 IP のランキング

3.2 SSH サーバへのサイバーアタック

定期的に学外から対外公開サーバ上の ssh サーバに対してアタックが行われている．注意していただきたいのは，**学外から ssh サーバへアクセス可能な状態で, 数 10 分から数時間経過するとほぼ 100%パスワードに対する辞書攻撃が始まる**，という点である．また，辞書攻撃に当たっては，従来英語における「名前」が使用される場合がほとんどであったが，直近の攻撃では,「日本人の名前」も多く使われるようになってきている (**図 3**)．よりクラックされる可能性が高くなっていると考えられる．ssh サーバの運用に当たっては，ID/Password だけに頼らず，IP によるアクセス制限をかけるなどの対処が必須であると考える．

```
Mar 28 04:02:28 133.30.xx  Failed password for taisa from yy port 45600 ssh2(0)
Mar 28 04:02:31 133.30.xx  Failed password for taii from yy port 45674 ssh2(0)
Mar 28 04:02:33 133.30.xx  Failed password for kose from yy port 46146 ssh2(0)
Mar 28 04:02:36 133.30.xx  Failed password for namie from yy port 46217 ssh2(0)
Mar 28 04:02:39 133.30.xx  Failed password for koizumi from yy port 46690 ssh2(0)
Mar 28 04:02:41 133.30.xx  Failed password for amuro from yy port 46763 ssh2(0)
Mar 28 04:02:44 133.30.xx  Failed password for yasuo from yy port 47222 ssh2(0)
Mar 28 04:02:47 133.30.xx  Failed password for taisho from yy port 47698 ssh2(0)
Mar 28 04:02:49 133.30.xx  Failed password for root from yy port 47764 ssh2(0)
Mar 28 04:02:52 133.30.xx  Failed password for asura from yy port 48234 ssh2(0)
Mar 28 04:02:55 133.30.xx  Failed password for agatamori from yy port 48303 ssh2(0)
```

図 3: 辞書攻撃の様子ー日本人名が使用されている

3.3 メールサーバへのサイバーアタック

メールサーバに対しては，学外から定期的に以下のアタックがかけられている．

- 第三者中継 (認証無しに学外から学外へメールがリレーされること) の可能性チェック．
- 送信時に認証を行っているメールサーバに対する辞書攻撃 (**図 4**).

ssh サーバの場合と同様に，辞書攻撃に対する対処が必要である．しかしメールサーバの場合，IP などによるアクセス制限が困難である場合がある．基本的にメールサーバのログを定期的に監視して，不正な認証による中継が行われていないかチェックする必要がある．辞書攻撃によるパスワードクラッキングを許して大量メールの中継を許した場合，神戸大学から発信されるメール自体が拒否されるようになる可能性があり，十分な注意が必要である[4]．メールサーバの送信認証を行うには，平文による認証は行わず，暗号化された認証を用いることが必要である．

3.4 メールによるサイバーアタック

10~15 年前と比較すると，メールによって送られてくるコンピュータウイルスの数自体は減少している．2013 年 2 月中旬から 3 月中旬にかけて，情報基盤センターで設置しているメールセキュリティアゲートウェイプライアンスでは 約 500 通ウイルス付きメールを検知して検疫処理を行っている．しかし，一定確率でアプライアンスで検知できなかったとウイルス付きメールが学内に送付されていることを確認している．本

[4] 数年前に, aol.com から数日メールの配送が拒否されるという事態が発生した.

```
Jan 21 08:13:11 XX postfix/smtpd[24921]: warning: zzz.com[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:11 XX postfix/smtpd[24921]: warning: xxx.com.x[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:12 XX postfix/smtpd[24921]: warning: unknown[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:12 XX postfix/smtpd[24921]: warning: zzz.com[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:13 XX postfix/smtpd[24921]: warning: xxx.com.x[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:17 XX postfix/smtpd[24921]: warning: unknown[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:17 XX postfix/smtpd[24921]: warning: zzz.com[aaa.28.138.41]: SASL LOGIN authentication failed: authentication failure
Jan 21 08:13:18 XX postfix/smtpd[24921]: warning: xxx.com.x[aaa.28.bbb.41]: SASL LOGIN authentication failed: authentication failure
```

図 4: メールサーバへの辞書攻撃の様子

学のアプライアンスは，大手のアンチウイルスソフトメーカ製のものを採用しているため，PC 上のアンチウイルスソフトでも検知できない可能性が高く，アンチウイルスソフトを導入したからといって安心できない状況であることには変わりない．

一方で，迷惑メールは, 約 70 万通 (1 ヶ月間のメール総数は約 750 万通) 検知してブロックしており，深刻な状況は継続している．また，いわゆるフィッシングメールも数多く送られてきている．多くは，外国での詐欺を前提にしたものであるが，2013 年 1 月に 日本の東京 UFJ 銀行を騙ったフィッシングメールが全国的にばらまかれたことは記憶に新しい．神戸大学にも大量に送付されたが，情報基盤センターのメールサーバの通信ログから送信元を調べると, 一定の IP からではなく，世界中の各地から同時に送付されていることが判明した．これは，**遠隔操作ウイルスに感染した世界中の PC から一斉に発信している**ということではないかと考えられる[5]．

今後,「標的型」のフィッシング/ウイルスメールはより巧妙化する可能性があり，添付ファイル付きあるいはリンクを伴う HTML メールの操作には細心の注意が必要である．

4. 終わりに

本稿では，2013 年第一四半期における情報セキュリティの状況について概説した．特に，遠隔操作ウイルス感染 PC からの脅迫メッセージを投稿したという事件で誤認逮捕が発生したように，サイバー犯罪に対する司法当局の対応は不安定であり，注意を要する．また,「岡崎市立中央図書館事件」[1] では，クローリングソフトウェアを開発して運用していた技術者が不正アクセスとして逮捕されるという事態も発生しており，大量アクセスを伴う「インターネットの教育研究利用」も注意が必要であることを浮き彫りした．

今後，セキュリティ状況は大きく変化する可能性が高く，注視して対策を講じていく必要がある．

参考文献

[1] http://astand.asahi.com/magazine/wrnational/special/2011012800004.html

[5] 幸いにも神戸大学内からは送信されていないと思われる