本当にあったセキュリティのおはなし [Enog29]

2014/11/7

NS・コンピュータサービス
小野澤　進

はじめに

ここ最近、セキュリティ関連のインシデントに遭遇する機会が

多くありましたので、内容についてまとめてみました。

みなさまも多く経験されているかと思いますが、

「うちはこんな対策してる」「これやってみれば？」

といった内容がありましたらアドバイスいただければと思いますm(__)m

agenda

- 最近あったセキュリティ的ないろいろ
  - ✓ ネットワーク
  - ✓ スパムメール
  - ✓ サーバ
  - ✓ マルウェア
- ためしてみた
- まとめ

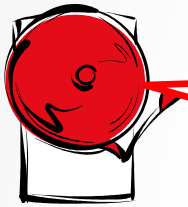
ネットワーク編
～そのパケット注文しましたっけ？～

最近あったセキュリティ的ないろいろ

2014年5月某日の昼下がり

～オペレーションルーム～

監視サーバ



BGPルータ対向アドレス応答が無くなったよ！

運用担当

ルータ自体は落ちていないようだが、
対向アドレスのPingがロストする

時を同じくして

～サポート宛の電話～

お客様A

なんかホームページの表示が遅いんですけど…

お客様B

そちらに預けているサーバへ接続できませんけど！

社員

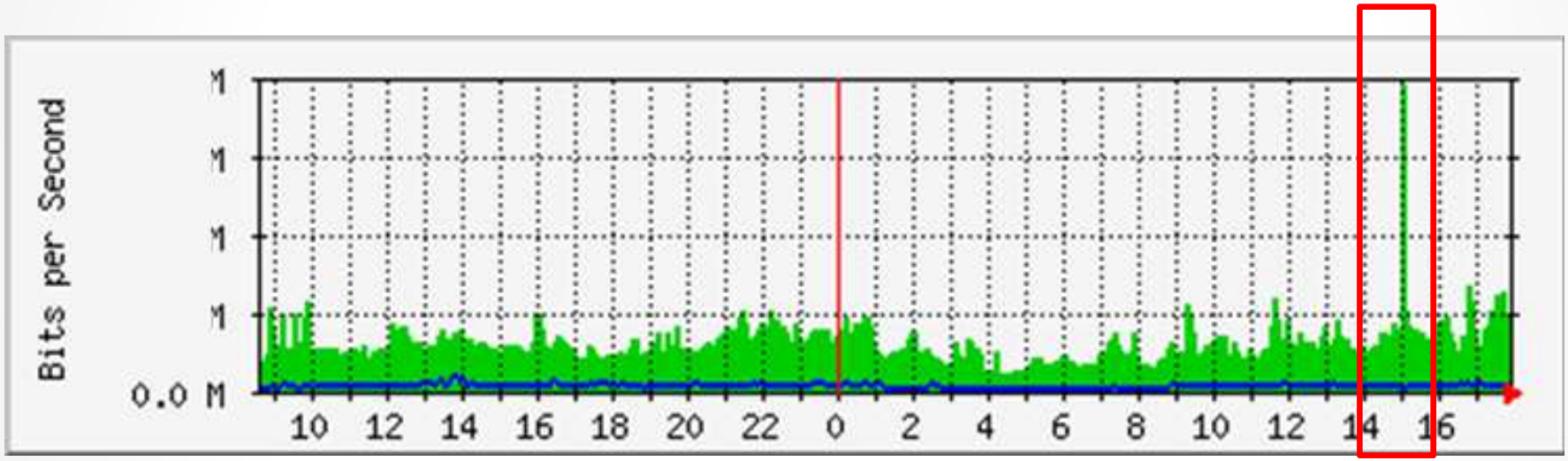
インターネット接続なんか遅い

申し訳ございません…
ただ今調査中です…

運用担当

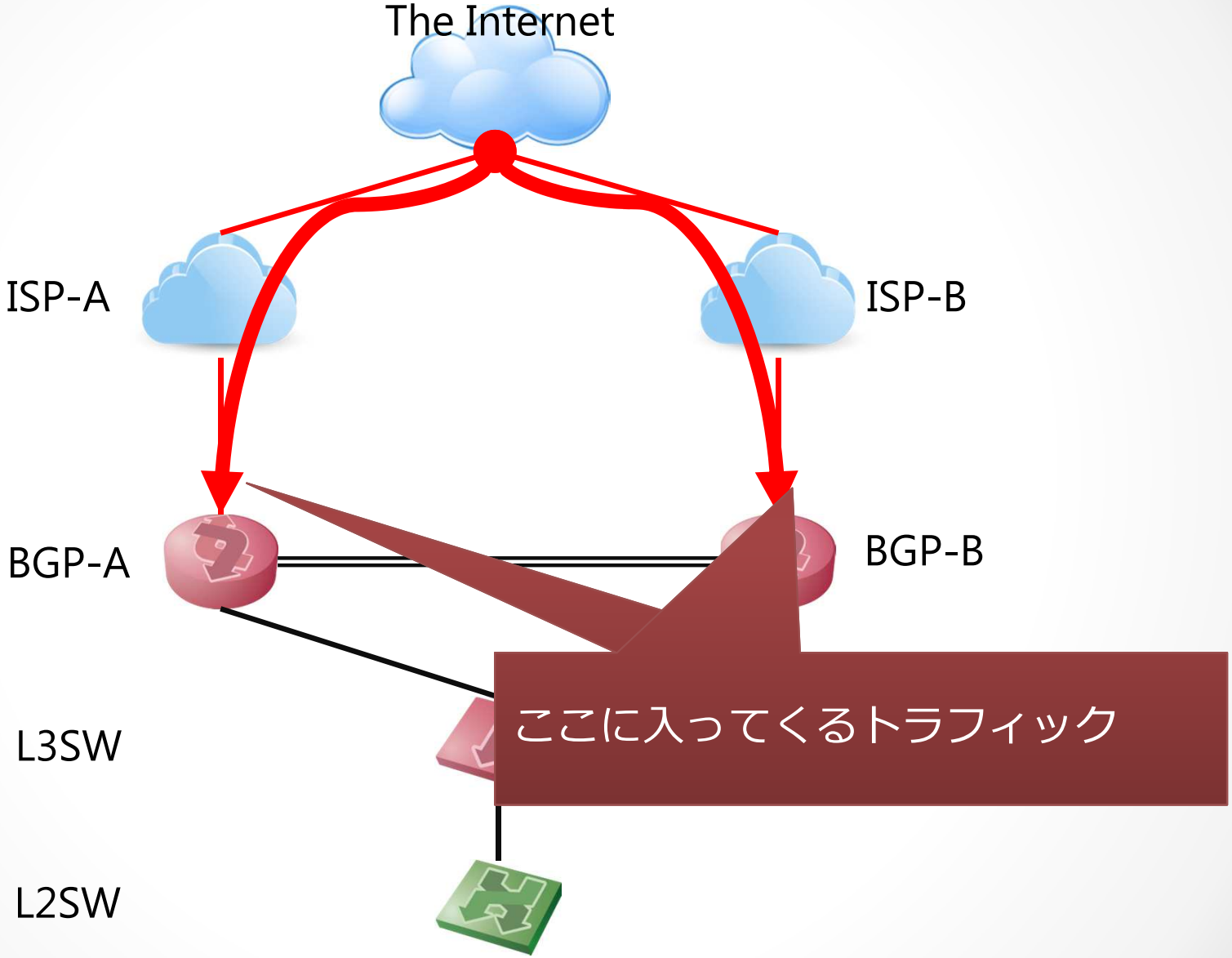
で、実際に起きていた事

上位ISPからの下りトラフィックが普段の4倍以上に！！！



その結果輻輳を起こし通信が遅くなっていました

超概要

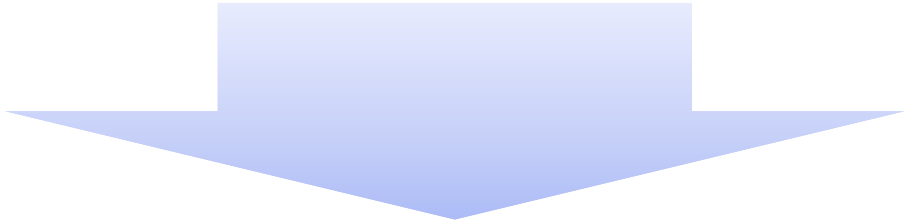


対応した事

どうも外部からのアタックが原因らしい

内部のネットワーク機器でフィルタをかけたとしても

トラフィックの流入は止まらない可能性がある。



上位ISPさんにお願いして該当トラフィックをブロック

していただきました。(というかすでにブロックして頂いていました...)

一体何が？

フィルタをかけていただいたパケットのIPアドレス・ポート等を確認した結果...

弊社でお預かりしているお客様サーバに対する、

“NTP Amplification攻撃” が発生していた事が分かりました。

NTP Amplification攻撃？

Network Time Protocol projectが提供するNTPDには、管理機能としてmonlistが実装されています。

この機能に対してクエリを発行すると、過去にNTPサーバとやり取りしたアドレスを最大600件返します。

→リクエストに対するパケットサイズの増幅が可能

monlistへのアクセスが適切に制限されていないサーバを踏み台にしたDDoS攻撃が最近流行しているらしい。

実際に確認してみる

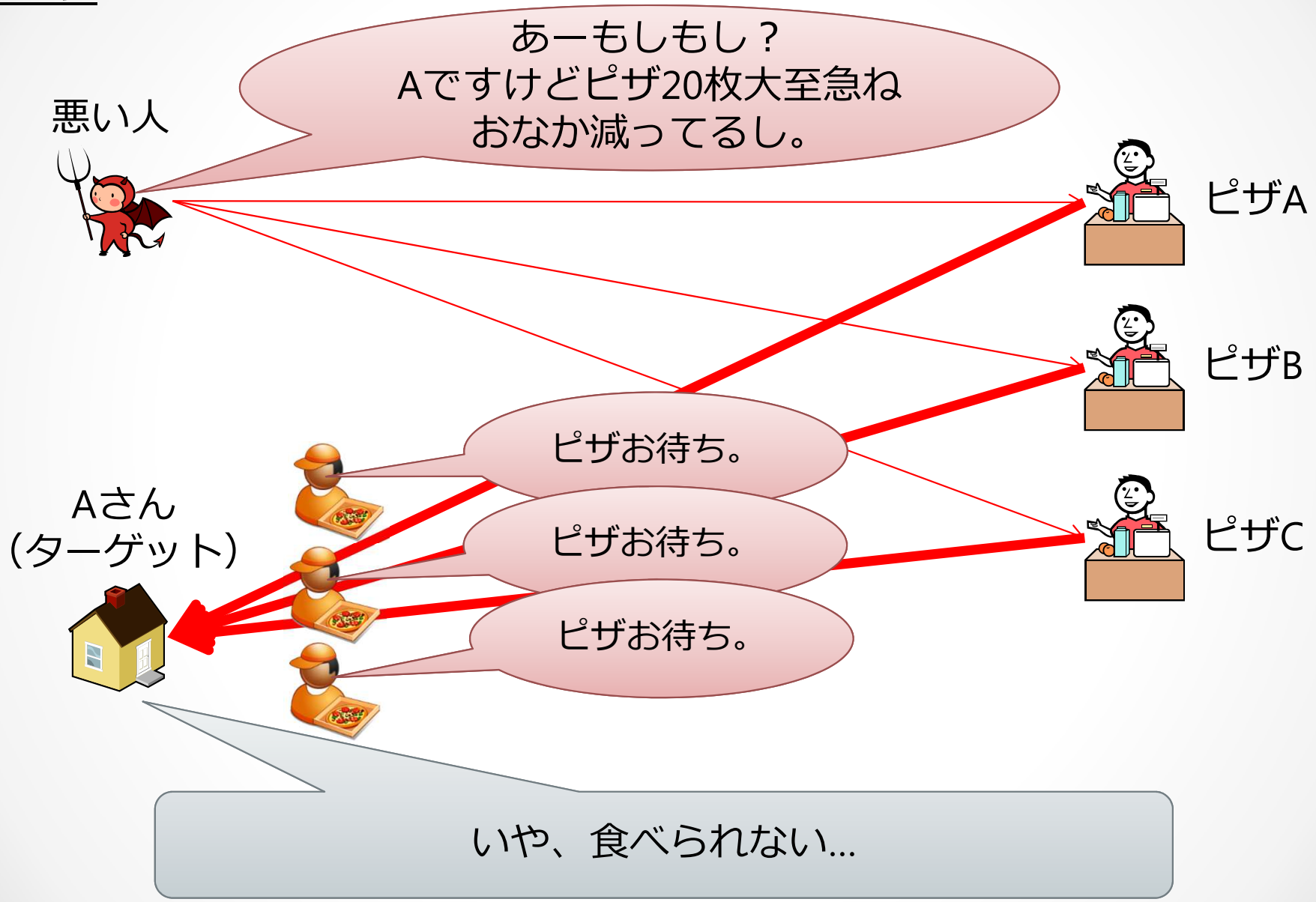
弊社のNTPサーバ上でmonlistを打ってみると以下のような応答

```
$ ntpdc -nc monlist localhost
remote address          port     local address          count      m     ver    code     avgint     lstint
===============================================================================
::1                     38083              ::1                4     7       2       0      10525          0
211.x.x                   694       172.16.x.x         58905165     3       3     180          0          0
210.x.x                   123       172.16.x.x            52079     3       4     180       1024          6
211.x.x                   123       172.16.x.x           495082     3       3     180         64          6
211.19.x.x                123       172.16.x.x           482563     3       3     180        129          7
211.19.x.x                123       172.16.x.x            71136     3       4     180        140          7
10.1.2.4                  123       172.16.x.x           236985     3       3       1        101          9
211.19.x.x                123       172.16.x.x           388211     3       4     180        126         14
211.19.x.x                123       172.16.x.x           609374     3       3     180         80         15
211.19.x.x                123       172.16.x.x           577696     3       3     180        328         16
...
```

上記のようなエントリが600件表示されました ＝ 約48KByte

数百Byteのクエリが最大約200倍に増幅されて応答される。

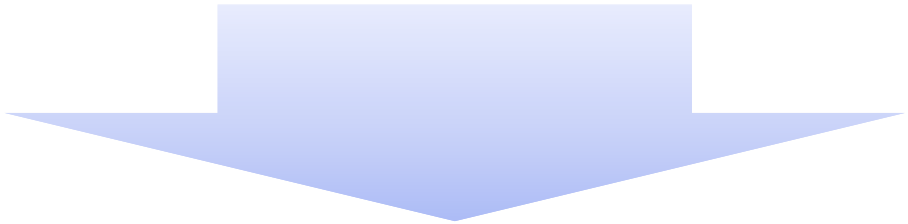
つまり


あーもしもし？
Aですけどピザ20枚大至急ね
おなか減ってるし。
悪い人
ピザA
ピザB
ピザC
ピザお待ち。
ピザお待ち。
ピザお待ち。
Aさん
(ターゲット)
いや、食べられない…

NTP Amplification攻撃②

同じような障害がこの後もあったのですが…

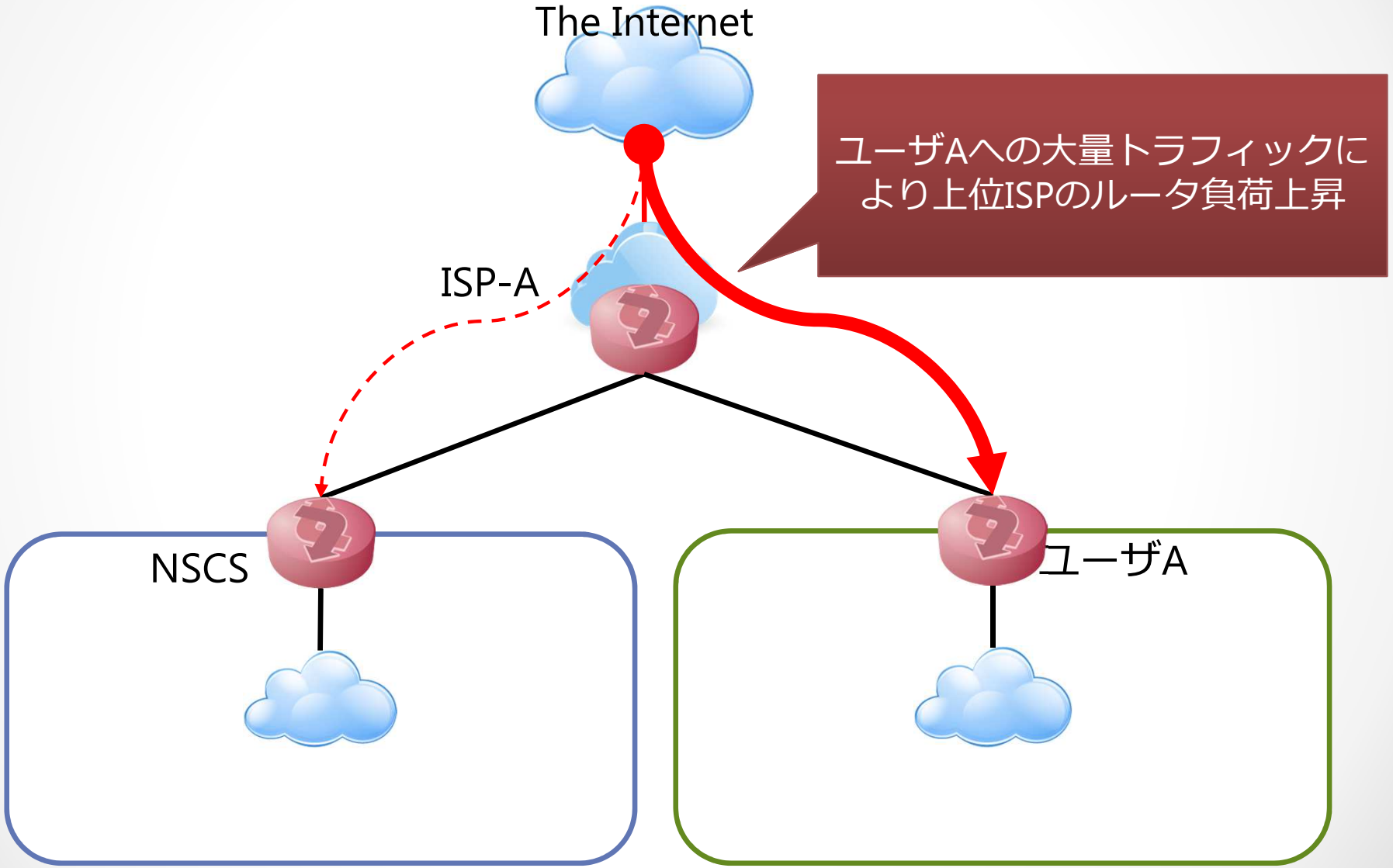
その時は弊社側トラフィックに異常は見当たらず。



上位ISPに確認したところ、別のユーザさんで同じ攻撃が発生し

ISP側のルータ負荷が上昇していたとの回答をいただきました

超概要②


The Internet
ユーザAへの大量トラフィックにより上位ISPのルータ負荷上昇
ISP-A
NSCS
ユーザA

対策って？

- 今回のようなケースは自前での対策は不可能か
  - 帯域リソース消費を狙ったタイプの攻撃...
  - 上位ISPに頼らざるを得ない？
- 標的とされにくくする方法はあるのか
- 自分たちが加害者にならない
  - サーバのパッチ適用、適切な設定
  - Source Address Validation(BCP38, BCP84)

NTPD上の対策

ntp.confに適切な設定、たとえば以下のような設定

- NTPの通信は基本すべて無視
- 限定的にアドレス許可かつクエリを制限

```
restrict default ignore
restrict 192.168.0.0 mask 255.255.255.0 noquery
```

もしくはmonlist機能を無効化してしまう

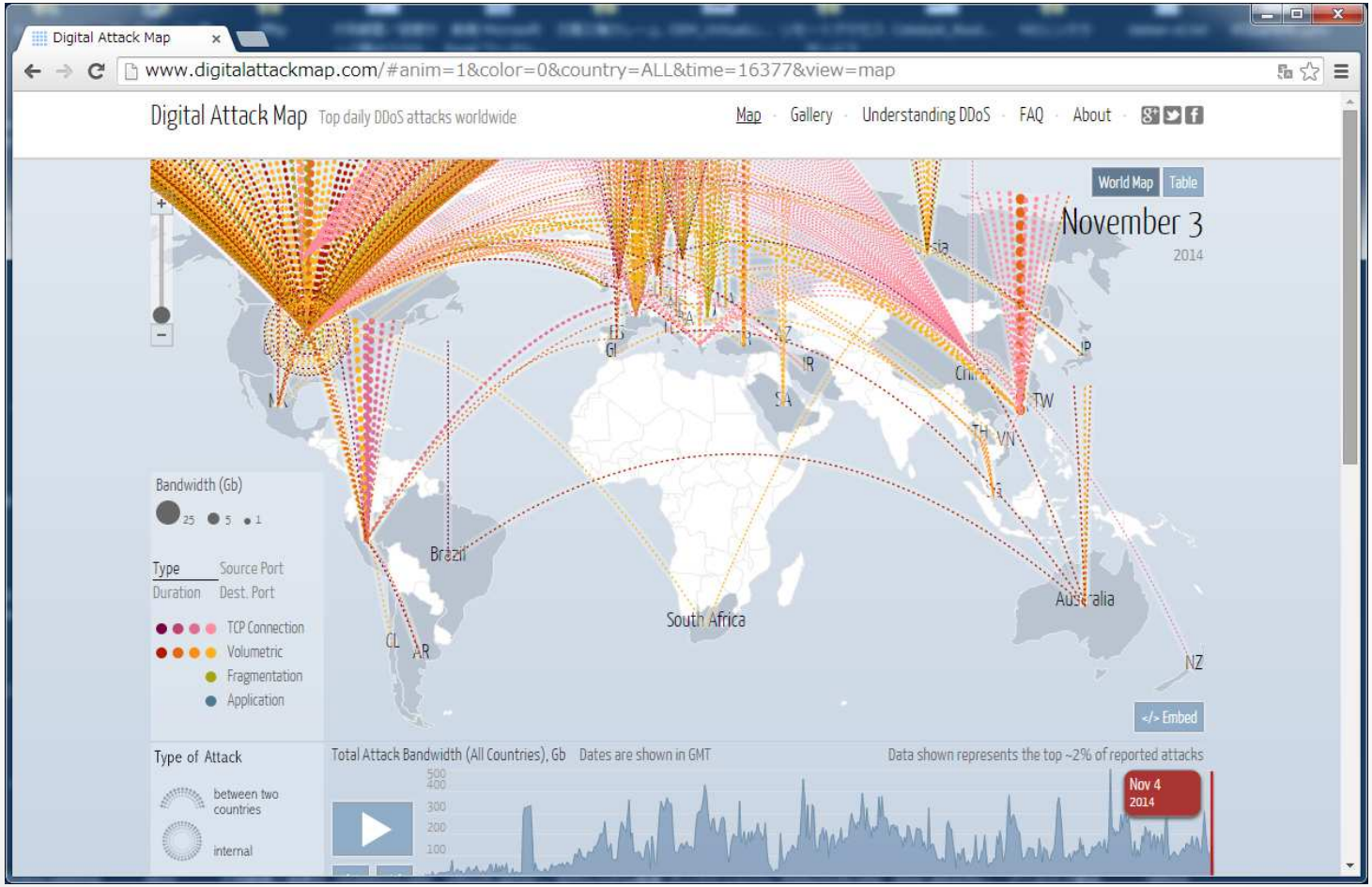
```
disable monitor
```

＃パッケージのアップデート？（対策済みの安定版はリリース済？）

Digital Attack Map

■アーバーネットワークスがデータ提供しているDDoS可視化ツール

http://www.digitalattackmap.com/



スパムメール編
～そのメールどうしても届けたいのか～

• • •

最近あったセキュリティ的ないろいろ

2014年10月某日

～サポート宛の電話～

お客様A

そちらのスパム対策サービスを使用しているけど、
最近スパムメールが多いのですが…

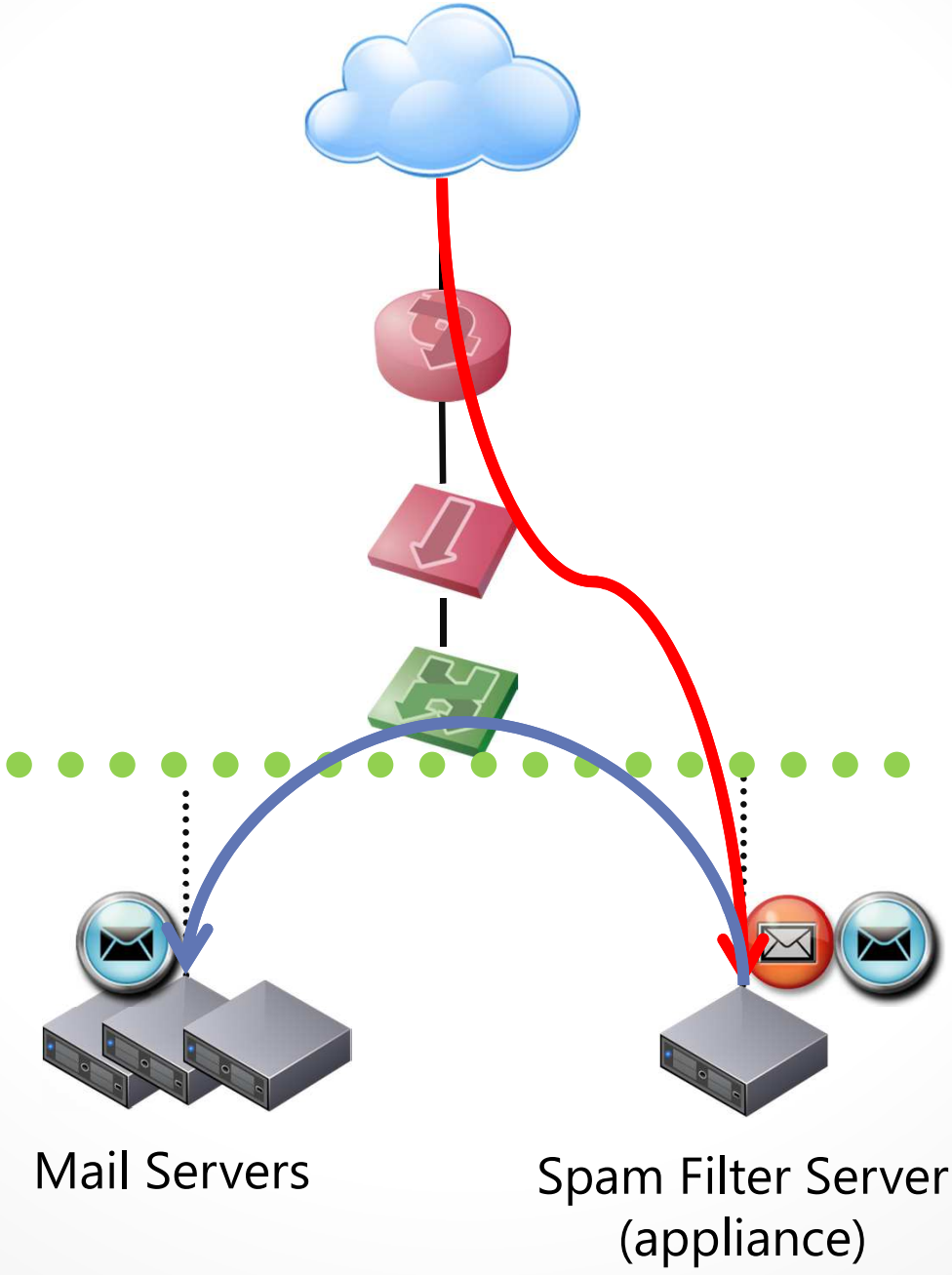
社員

社内アドレスに最近迷惑メールが多い…

調査します…

運用担当

超概要



いまのフィルタ

- CBL等Realtime Blackhole List(RBL)を参照したSMTPフィルタ
  - SMTP接続段階でのブロック
- メール本文中の不正なURLを検出して隔離
  - URLデータベースはメーカにより日々更新
- RPDエンジンによるスキャン
  - サンプリングデータをもとにスパムらしさを評価、検出

どんなメールがフィルタをすり抜けているのか

- サンプル1

```
Received: from unknown (HELO ary058.localhost) (103.232.15.114)
 by xxx.xxx.xxx.xxx with ESMTP; 3 Nov 2014 01:14:52 +0900
 Received: by ary058.localhost (Postfix, from userid 1002)
 id CADB9BA175; Mon, 3 Nov 2014 01:11:21 +0900 (JST)
 Received: from localhost (unknown [10.190.116.153])
 by localhost (Postfix) with ESMTP id 5F6101048CDF
 for <sample@example.jp>; Mon, 3 Nov 2014 01:11:20 +0900 (JST)
 MIME-Version: 1.0
 Content-Type: multipart/related;
 boundary="=_40e5d6439a2bec00af9b933b02ceddb7"
 To: < sample@example.jp>
 From: 佐久間瞳<nrzbims9ex32@ug53nhrhs09t.pink>
 Subject: sample@example.jp様　私も直ぐ会える人の方がいいです♪
 Message-Id: <20141102161120.5F6101048CDF@mybmfyzw.ownpcip>
 Date: Mon, 3 Nov 2014 01:11:20 +0900 (JST)

 --=_40e5d6439a2bec00af9b933b02ceddb7
 Content-Type: multipart/alternative;
 boundary="=_08b0634309f7b756c0f3ae3e4fe114fb"

会える人募集してるの見つけてメールしちゃいました♪
```

どんなメールがフィルタをすり抜けているのか

- サンプル2

```
Received: from unknown (HELO ary053.localhost) (103.232.13.61)
 by xxx.xxx.xxx.xxx with ESMTP; 31 Oct 2014 05:10:23 +0900
 Received: by ary053.localhost (Postfix, from userid 1002)
 id E8B38B8C31; Fri, 31 Oct 2014 05:10:24 +0900 (JST)
 Received: from localhost (unknown [10.144.242.45])
 by localhost (Postfix) with ESMTP id 453701048CA5
 for <sample2@example.jp>; Fri, 31 Oct 2014 05:10:18 +0900 (JST)
 MIME-Version: 1.0
 Content-Type: multipart/related;
 boundary="=_0337ac8d5d83aa62b139d72f28c1cc2a"
 To: <sample2@example.jp>
 From: 乾春華<avzwk4zzsx8o@uafyh7o09lz7.red>
 Subject: sample2@example.jpさん…？　ですよね？違ったらすみません！
Message-Id: <20141030201018.453701048CA5@dkodrj.etddmf>
 Date: Fri, 31 Oct 2014 05:10:18 +0900 (JST)


 sample2@example.jp さん


 携帯が故障してしまって代替機使ってるんですけど…
```

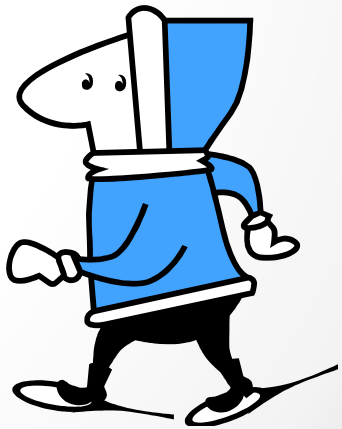
特徴

- RBLに登録されていない、登録されにくいIPから送信
  - RBLを利用したSMTP接続段階でのブロックがされにくい
- 送信元アドレス(ドメイン)を頻繁に変更して送信
  - ドメインやメールアドレスでのフィルタが難しい
  - フィルタデータベースの更新もいたちごっこ

このようなメールを“スノーシュースパム”と呼ぶそうです

スノーシュースパム？

- スパムメールの発信元を分散させてフィルタリングをすり抜ける
  - 「スノーシュー」＝「かんじき」が荷重を分散させて雪に沈まない仕組みをたとえたもの
  - 数をばらまく攻撃から、標的を絞った攻撃へ(量より質)
  - ２～３年前から急増



対策？

- フィルタ基準を厳しく設定するか
  - SPFとかTarpittingとか
  - 誤判定？検証はできるのだろうか。
- 個人的には…
  - 「スパムを受け取らない」ことではなく

    「スパムでないメールを確実に受け取る」事が重要

そのほかにもこんなメール

- サンプル3

件名：【告発通知】
送信元： sample@example.jp
送信先： sample@example.jp
本文(抜粋)：

貴殿が以前購入及びインターネット内で観覧又はダウンロードした違法わいせつ物の製造・販売に関与した、数グループが当団体と被害者児童の保護者及び被害者女性の働きかけにより、平成25年度に組織的処理法違反・児童買春・児童ポルノ禁止法違反により警視庁に摘発されました。

この度、被害者児童及び保護者と、性犯罪女性被害者のさらなる拡大を防止する為、購入者に対しても事件証拠（購入履歴・金融機関履歴等）を提出し告発致します。

告発を取り下げたい者は本メール到着後から翌日の電話受付時間内に当団体に必ず電話にてご連絡ください。
メールでのご返答は受け付けておりませんので携帯電話等からお電話ください。
期日を過ぎた場合、いかなる状況でも即時即告発いたします。

サーバ編
～穴があったら入ってくる～

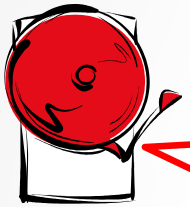
• • •

最近あったセキュリティ的ないろいろ

2014年某日

～オペレーションルーム～

監視サーバ



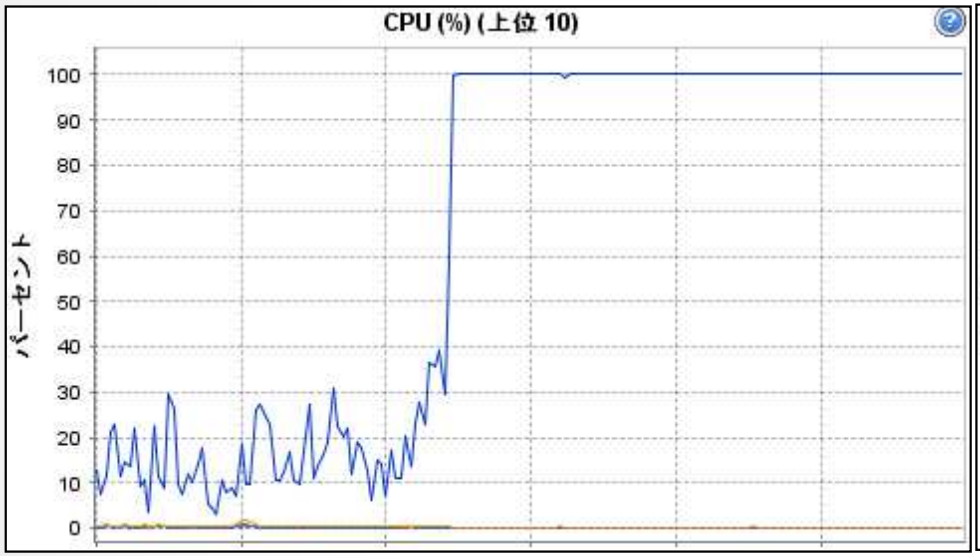
○○社のWebページが閲覧できません
WebサーバのCPU負荷も高いです

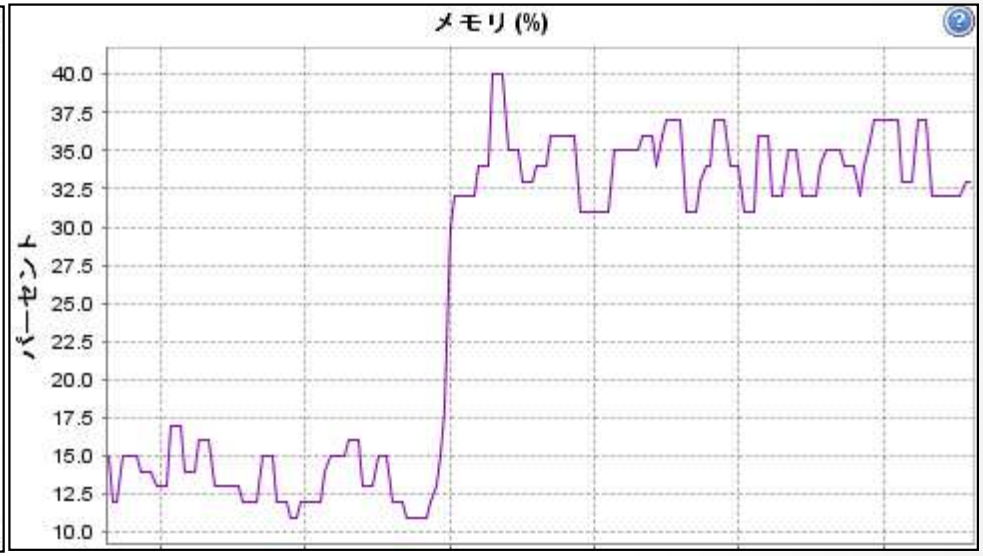
調査。。調査。。

運用担当

サーバを外からのぞく

対象のサーバはVMware上の仮想マシン、vSphere上の状態は…





明らかに負荷が高いですね…

サーバの中は…

```
-bash-3.2$ w
 16:07:28 up 293 days,  7:22,  2 users,  load average: 41.69, 37.96, 35.68
```

何がそんなに仕事をしているのか

```
-bash-3.2$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
～一部省略
apache     366  6.4  1.3  57640 40552 ?        S    16:03   0:21 /usr/sbin/httpd
apache     516  5.8  1.3  58136 41080 ?        S    16:03   0:17 /usr/sbin/httpd
apache     610  5.1  1.3  58464 41612 ?        S    16:03   0:14 /usr/sbin/httpd
apache     611  3.9  1.3  58004 40984 ?        S    16:04   0:11 /usr/sbin/httpd
…httpd 沢山！
```

そんなに人気サイトなのか。

サーバの中は②…

Apacheのアクセスログを見てみる

```
162.xx.xx.xx - - [2014:16:30:57 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:31:00 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
199.xx.xx.xx - - [2014:16:30:59 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:30:54 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
162.xx.xx.xx - - [2014:16:30:53 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:31:00 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:30:59 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:31:00 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
204.xx.xx.xx - - [2014:16:31:01 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
162.xx.xx.xx - - [2014:16:31:00 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
162.xx.xx.xx - - [2014:16:31:02 +0900] "POST /xmlrpc.php HTTP/1.0" 200 523 "-"
```

可能性として

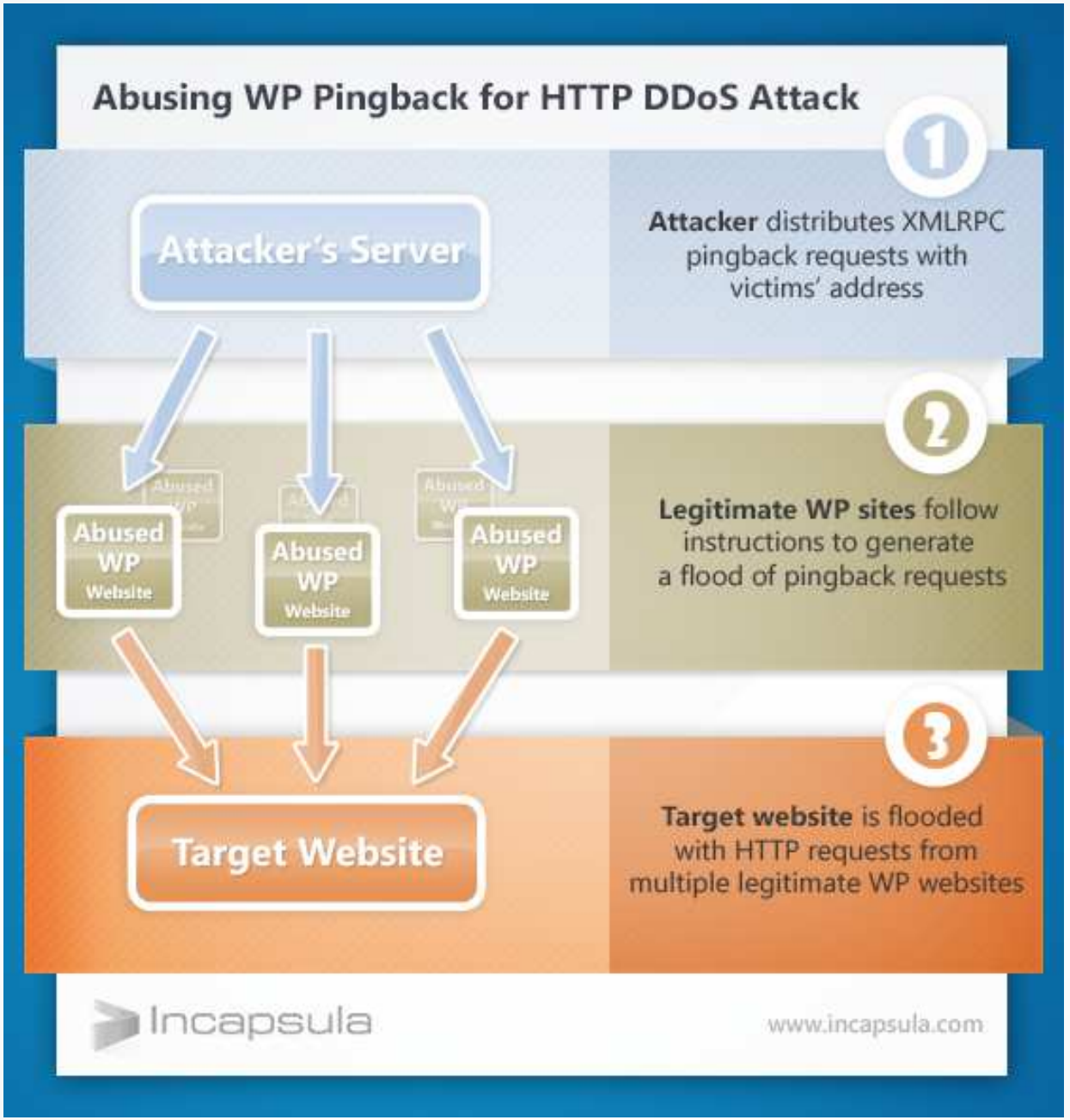
このWebサイトはCMSとしてWordPressを使用している。

XML-RPCを悪用され特定の Web サイトに対して攻撃を仕掛けているのでは？

もしくは攻撃を受けている？

※XML-RPCは本来はコンテンツ所有者が自分の投稿にリンクが張られたことを通知する「Pingback（ピンバック）」機能で利用されている

※あくまで調査時に出てきたもので別の脆弱性である可能性もあり



出典：Incapsula

その他
～こまかいもの～

・・・

最近あったセキュリティ的ないろいろ

マルウェア

Game Over Zeus (GOZ) …

金融機関関連情報を窃取するなどの機能がある危険性の高い不正プログラム。GOZに感染した端末を使用して金融機関の正規のウェブサイトへ通信を行うと、当該利用者の口座から不正送金が行われてしまう。

世界的に蔓延していることからFBIなどが中心となり、当該不正プログラムのネットワークを崩壊させる作戦を実施中。

bash

2014年9月

環境変数の処理に問題があり、任意の OS コマンドを実行されるbashの脆弱性 (CVE-2014-6271他)が発覚

基本すべてのLinux系サーバに対してアップデートを適用

httpdログにこの脆弱性を利用された形跡が残っていたものも…。

ためしてみた(かった事)
～時間足りませんでした～

• • •

ごめんなさい

障害の時

何が起こっている(いた)のか調査しますよね。

その時確認するのはログ

(CPU、トラフィックなどもパフォーマンスログとして)

でも、何も起こっていない時はあまり見ない

普段から活用できる形にできないか

探してみた

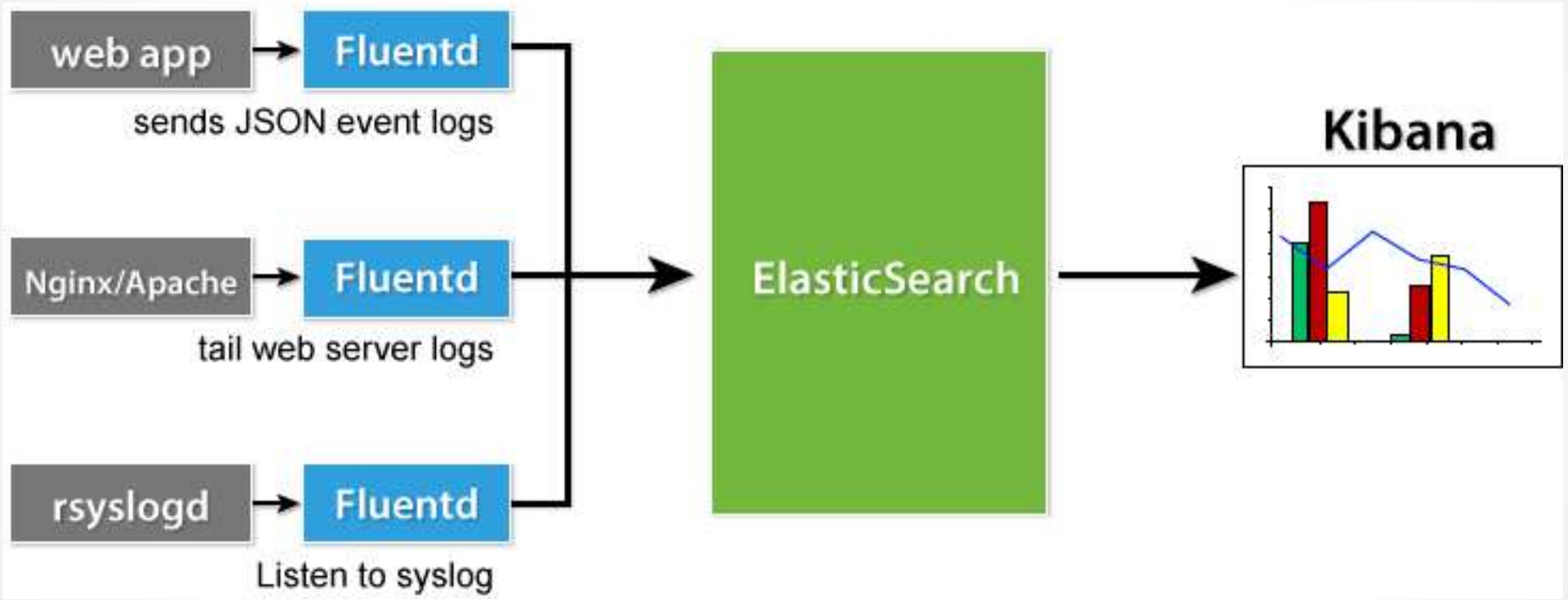
「fluentd + elasticsearch + Kibana」を利用したログの可視・解析が流行っているらしい。

ログを集めて

解析・検索して

表示する

概念図


web app
Fluentd
sends JSON event logs
Nginx/Apache
Fluentd
tail web server logs
rsyslogd
Fluentd
Listen to syslog
ElasticSearch
Kibana

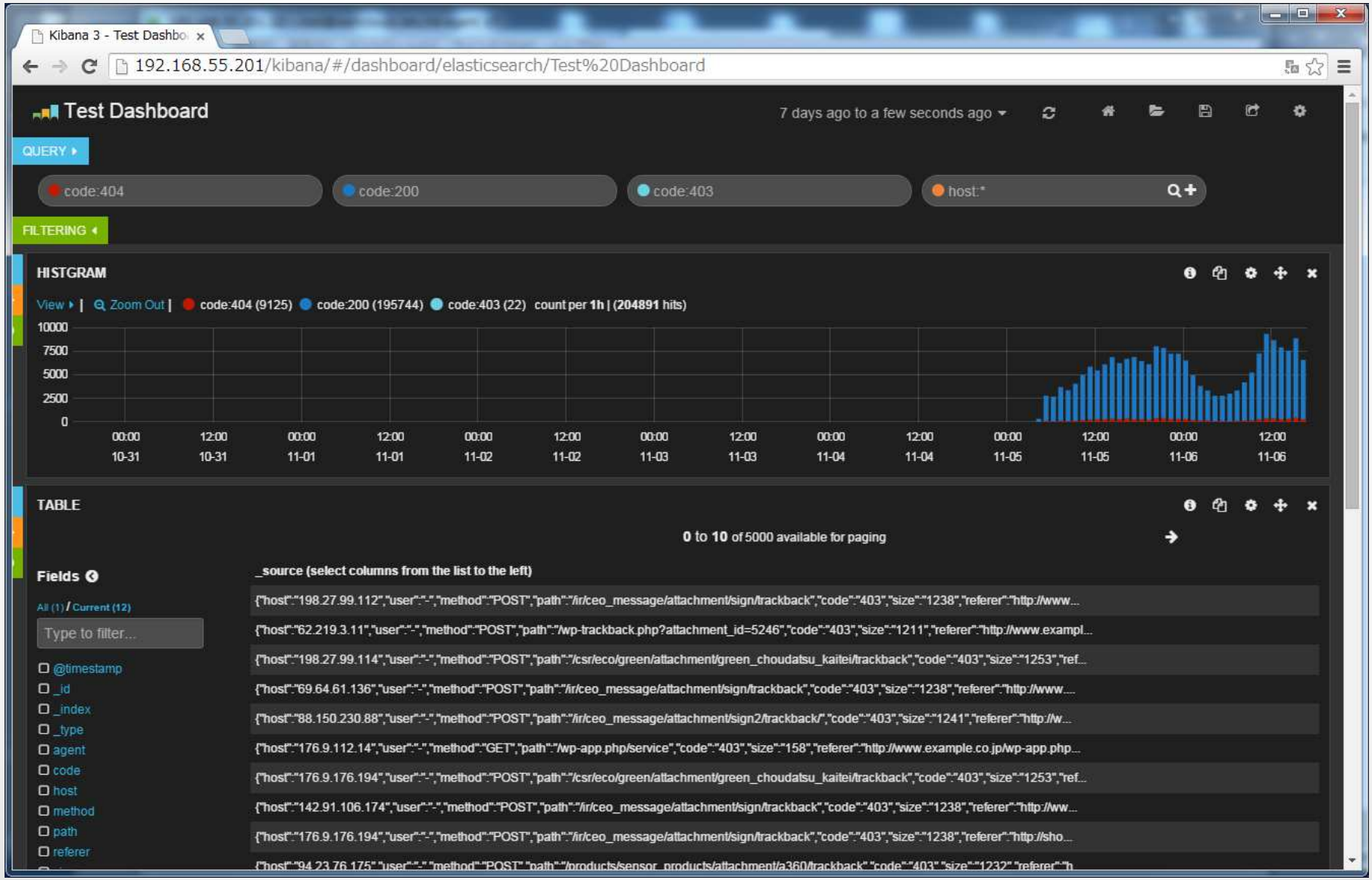
インストール

インストール自体は、公式ページやWeb上に公開されている情報を参考に比較的簡単にできました。

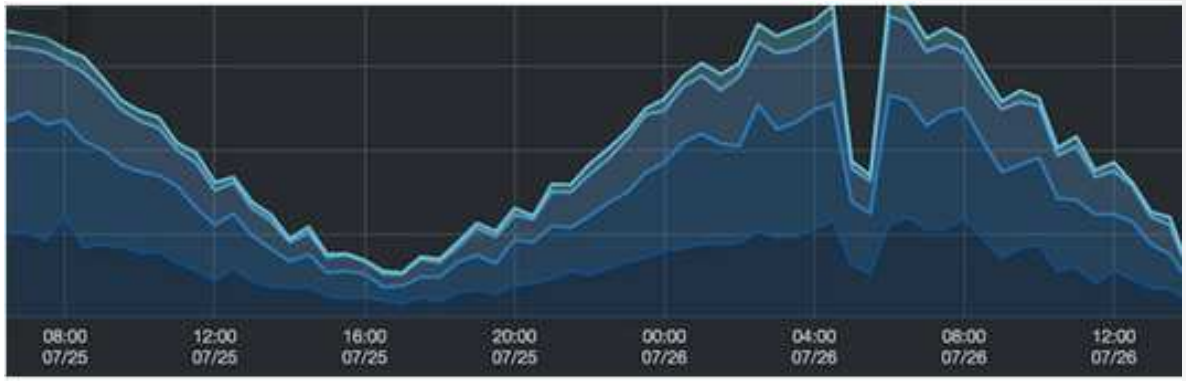
Fluentdの設定については、タグ付の概念やプラグインとの連携など

理解するのに少し時間がかかる印象です。

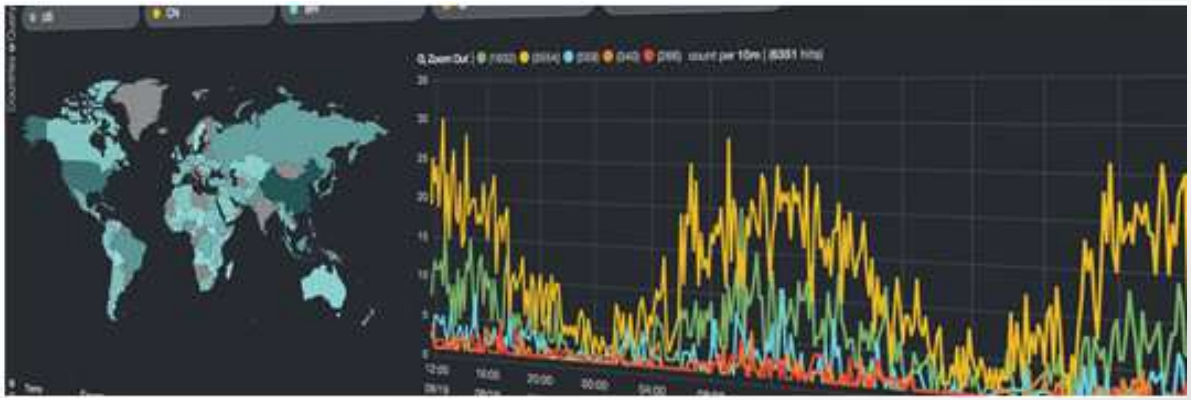
試しにいれてみた


Kibana 3 - Test Dashbo
192.168.55.201/kibana/#/dashboard/elasticsearch/Test%20Dashboard
Test Dashboard
7 days ago to a few seconds ago
QUERY
code:404
code:200
code:403
host:*
FILTERING
HISTGRAM
View | Zoom Out | code:404 (9125) code:200 (195744) code:403 (22) count per 1h | (204891 hits)
10000
7500
5000
2500
0
00:00 10-31
12:00 10-31
00:00 11-01
12:00 11-01
00:00 11-02
12:00 11-02
00:00 11-03
12:00 11-03
00:00 11-04
12:00 11-04
00:00 11-05
12:00 11-05
00:00 11-06
12:00 11-06
TABLE
0 to 10 of 5000 available for paging
Fields
All (1) / Current (12)
Type to filter...
@timestamp
_id
_index
_type
agent
code
host
method
path
referer
_source (select columns from the list to the left)
{"host":"198.27.99.112","user":"-","method":"POST","path":"/ir/ceo_message/attachment/sign/trackback","code":"403","size":"1238","referer":"http://www...
{"host":"62.219.3.11","user":"-","method":"POST","path":"/wp-trackback.php?attachment_id=5246","code":"403","size":"1211","referer":"http://www.exampl...
{"host":"198.27.99.114","user":"-","method":"POST","path":"/csr/eco/green/attachment/green_choudatsu_kaitei/trackback","code":"403","size":"1253","ref...
{"host":"69.64.61.136","user":"-","method":"POST","path":"/ir/ceo_message/attachment/sign/trackback","code":"403","size":"1238","referer":"http://www....
{"host":"88.150.230.88","user":"-","method":"POST","path":"/ir/ceo_message/attachment/sign2/trackback/","code":"403","size":"1241","referer":"http://w...
{"host":"176.9.112.14","user":"-","method":"GET","path":"/wp-app.php/service","code":"403","size":"158","referer":"http://www.example.co.jp/wp-app.php...
{"host":"176.9.176.194","user":"-","method":"POST","path":"/csr/eco/green/attachment/green_choudatsu_kaitei/trackback","code":"403","size":"1253","ref...
{"host":"142.91.106.174","user":"-","method":"POST","path":"/ir/ceo_message/attachment/sign/trackback","code":"403","size":"1238","referer":"http://ww...
{"host":"176.9.176.194","user":"-","method":"POST","path":"/ir/ceo_message/attachment/sign/trackback","code":"403","size":"1238","referer":"http://sho...

公式ページより


08:00
07/25
12:00
07/25
16:00
07/25
20:00
07/25
00:00
07/26
04:00
07/26
08:00
07/26
12:00
07/26


File types over time



機能の追加

プラグインが豊富なようなので、やりたいことがみつかるかも

http://www.fluentd.org/plugins

http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/modules-plugins.html

まとめ

- 最近アタック多い！
  - 以前とサーバやネットワーク構成は変わっていないのに…
  - 安易にツールが手に入り、誰でも簡単に攻撃ができる？
- 突然の障害は慌てる！
  - ログを活用して攻撃予兆となるようなアクセスを検知できないか
  - 攻撃に先回りして対応したい

おわり

ありがとうございました。