ARBOR NETWORKS

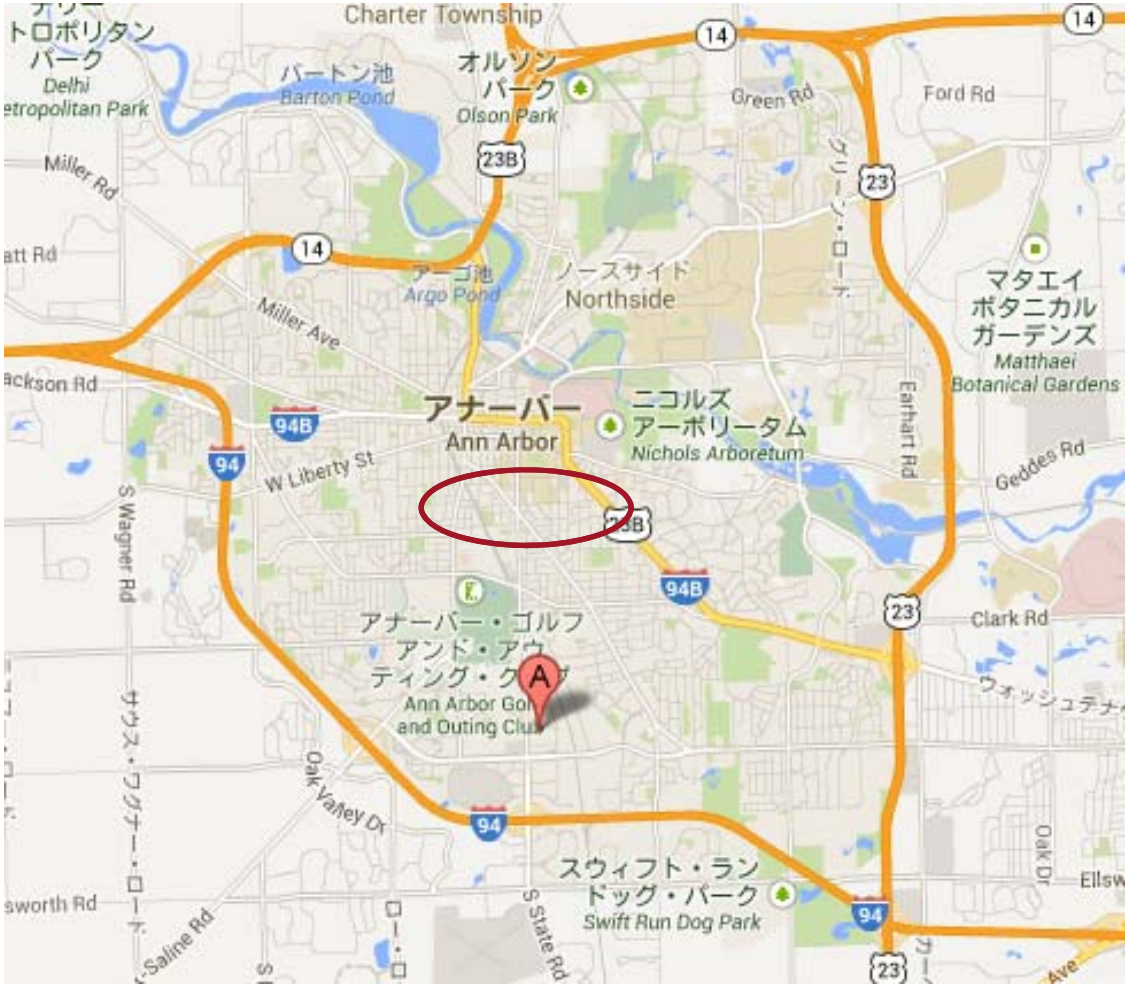
Internet Week 2013 – DDoS攻撃の実態と対策
～　DDoS攻撃の現状　～

Takashi Sasaki
SE Manager, Japan
tsasaki@arbor.net

ARBOR NETWORKS とは

ARBOR NETWORKS

ARBOR NETWORKS とは



ARBOR NETWORKS

ARBOR NETWORKS とは

ARBOR NETWORKS

ARBOR NETWORKS とは

本社所在地：米国マサチューセッツ州バーリントン

- 主要海外拠点：ロンドン、シンガポール、東京

日本法人：アーバーネットワークス株式会社

- 所在地：東京都千代田区神田淡路町
- 設立：2004年7月

沿革

- 1999年　米国マサチューセッツ州バーリントンで設立
- 2005年1月　1st ワールドワイド・インフラストラクチャ・セキュリティ レポート発表
- 2008年1月　エラコヤネットワークスを買収
- 2010年9月　ダナハーコーポレーションにより買収

事業内容

- 次世代データセンターおよびキャリア・ネットワーク向け、ネットワーク・セキュリティ/マネージメント・ソリューションの提供

主な製品

- Peakflow SP/TMS®（サービス・プロバイダ向けDDoS対策ソリューション）
- Pravail™ APS（Availability Protection System: エンタープライズ向けDDoS対策ソリューション）
- Pravail™ NSI（Network Security Intelligence: エンタープライズ向け内部脅威 検知ソリューション）

ARBOR NETWORKS

アジェンダ

DDoS攻撃の事例

DDoS攻撃の傾向

ARBOR NETWORKS

アジェンダ

DDoS攻撃の事例

DDoS攻撃の傾向

ARBOR NETWORKS

#OpIsrael　2013.4.7-

人道

ガザ地区攻撃に対する抗議

#OpIsrael

BY: ANONINDONESIA ON APR 7TH, 2013 | SYNTAX: NONE | SIZE: 0.18 KB | HITS: 590 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
1.  focus on this target for #OpIsrael
2.
3.  isoc.org.il
4.  cc.huji.ac.il
5.  81.91.161.69
6.  128.139.6.66
7.  128.139.34.240
8.  192.115.210.60
9.  149.20.56.132
10. 192.115.141.253
11. 192.5.4.1
12. 192.115.210.58
```

ARBOR NETWORKS

#OpTurkey 2013.6.4 -

自由主義

Anonymous declares #OpTurkey, attacks govt websites in support of protests

通信の検閲に対する抗議

Published time: June 02, 2013 19:47
Edited time: June 04, 2013 08:58

Get short URL

A demonstrator wears a Guy Fawkes mask as protestors clash with Turkish riot policemen during a protest against the demolition of the Taksim Gezi Park, in Taksim Square, in Istanbul (AFP Photo / Bulent Kilic)

The hacktivist group Anonymous has taken down the Turkish President's website, along with that of the country's ruling party, as operation #OpTurkey kicks off in support of the

Tags
Anonymous, Clashes, Internet, Mass media, Politics, Protest, Social networks,

ARBOR NETWORKS

#OpPetrol　2013.6.20 -

政治

国際石油・ガス産業に対する抗議

#OpPetrol

BY: A GUEST ON MAY 11TH, 2013 | SYNTAX: NONE | SIZE: 2.47 KB | HITS: 873 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
1.  Greetings Citizens of the World, We are Anonymous.
2.
3.
4.  It has been a long time coming, operation petrol, will be engaged on the 20th June 2013.
5.
6.  This operation will include the U S, Canada, England, Israel, Saudi Arabia (only Government), China, Italy,
    France, Germany, Kuwait (only government) and Qatar (only government).
7.
8.  As petrol is sold with the dollar currency of the U S we find this not acceptable when the oil should be sold at
    the country of Origin, making petrol a lot less then what you the citizens is paying for it
9.
10. Saudi Arabia you have betrayed your fellow believers with your cooper
    much pressure on families from around the world, you allow this to ha
11.
12. Back in time the middle east had no such currency as the dollar, it w
    agree with this paper currency idea and it is too the advantage of th
    with their taxes make it impossible to predict the price of gasoline,
    billionairs, continue to build on their obscene fortune.
13.
14. You may not already know, but in the future, electronic transfer of m
    way of all transactions by 2020.
15.
16. What you do not know, is when this occurs, just like in Syria, your g
    funds and retirement money at anytime they wish to steal it.
17.
18. The U S is known for creating war for the purpose of stealing Gold, s
    doing in Afghanistan still to this day, but you are not aware of this
```

ARBOR NETWORKS

#Opkillingbay 2013.11.x -

反日？

#OpKillingBay: Stop the Slaughter

BY: A GUEST ON NOV 8TH, 2013 | SYNTAX: NONE | SIZE: 3.37 KB | HITS: 794 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
1. Welcome World:
2. "TOKYO – The Japanese village notorious for the dolphin hunt documented in the film "The Cove" has slaughtered a
   pod of dolphins but spared the youngest animals, activists said Tuesday.
3.
4. Most of the dolphins caught by residents of the seaside village of Taiji on Monday were butchered Tuesday, except
   for two that will be sold to aquariums and six young animals that were released into the ocean, said Scott West, a
   member of the Sea Shepherd conservation group who is in Taiji as part of a campaign to protect the marine
   mammals.Leilani Munter, an environmental activist visiting Taiji from Charlotte, North Carolina, also witnessed
   the hunt and saw the dolphins being cut up in the slaugherhouse.
5.
6. "There is nothing to prepare you for seeing it in person. I saw these beautiful dolphins being driven into the
   cove, and they came out dead bodies," she told The Associated Press.
7.
8. For years, Taiji has held an annual dolphin hunt which begins in September and continues through March. It has
   traditionally sold the best-looking ones to aquariums and killed the rest.
```

ARBOR NETWORKS

#Opkillingbay

```
1.  #OpKillingBay Target List
2.
3.  www.maff.go.jp/e/
4.  www.kantei.go.jp
5.  www.jnto.go.jp
6.  www.jpf.go.jp
7.  www.mofa.go.jp
8.  www.env.go.jp
9.  www.stat.go.jp
10. www.mof.go.jp
11. www.cao.go.jp
12. www.fsa.go.jp
13. www.npa.go.jp #fuckthepolice
14. www.soumu.go.jp
15. www.moj.go.jp
16. www.mext.go.jp
17. www.mhlw.go.jp
18. www.meti.go.jp
19. www.mlit.go.jp
20. www.shugiin.go.jp
21. www.sangiin.go.jp
22. www.courts.go.jp
23. www.town.taiji.wakayama.jp
```

ARBOR NETWORKS

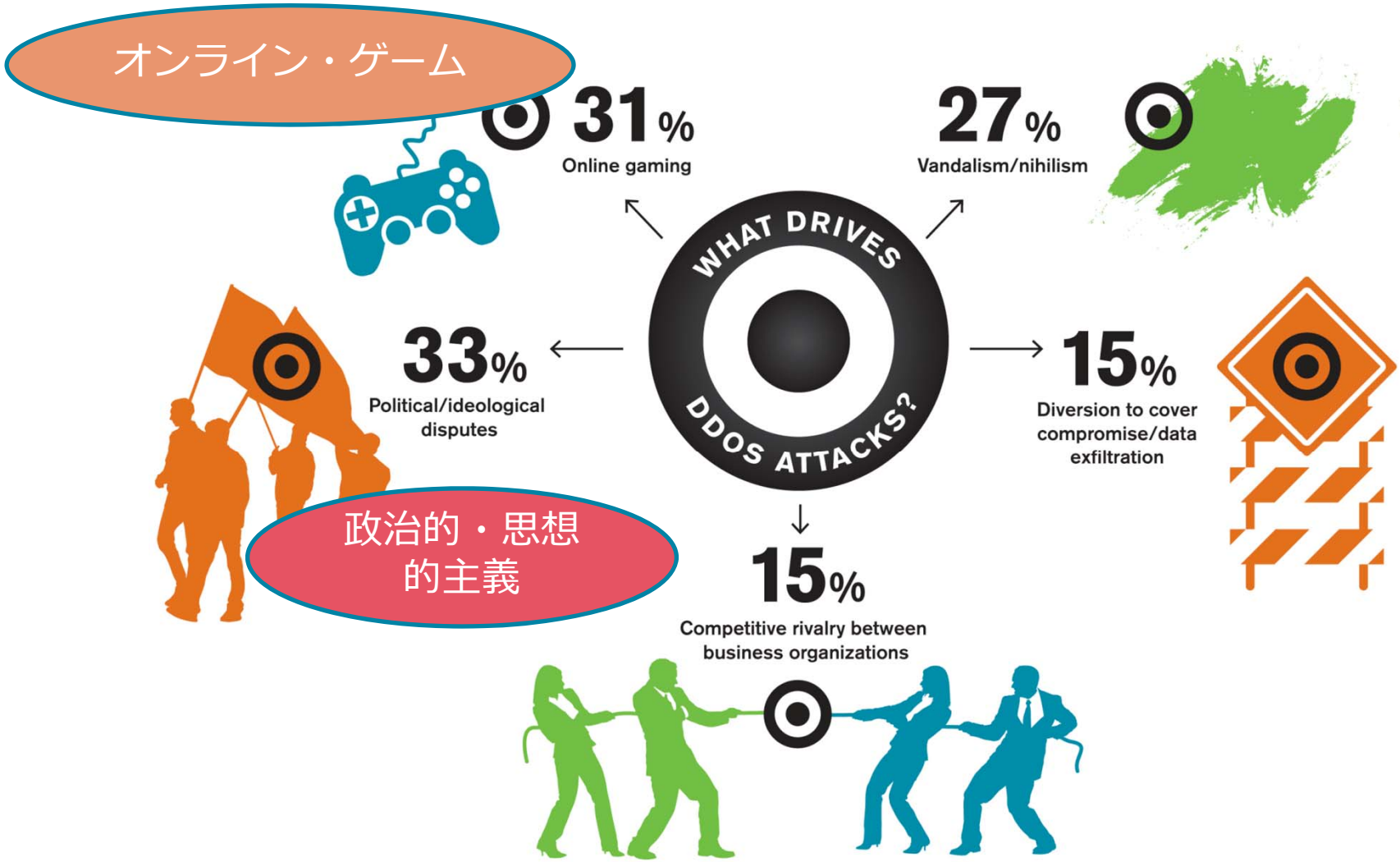
#Opkillingbay

アノニマス、イルカの屠殺に抗議するオペレーション #OpKillingBay を発表。ターゲットは「日本」。

アノニマスはイルカの屠殺に対する抗議を行うオペレーション「#OpKillingBay」を発表しました。抗議対象は日本でイルカ漁を推進している和歌山県太地町や政府機関で活動日時は不定期で抗議方法は合法にネット上で抗議するものからDDoS攻撃も行われる予定です。

ARBOR NETWORKS

DDoS攻撃に見られる動機の変化



ARBOR NETWORKS

イノセンス･オブ･ムスリム

宗教

イスラム教を誹謗中傷するビデオの公開

エジプト系アメリカ人

宗教が神聖なものではない国では物やお金が唯一の価値

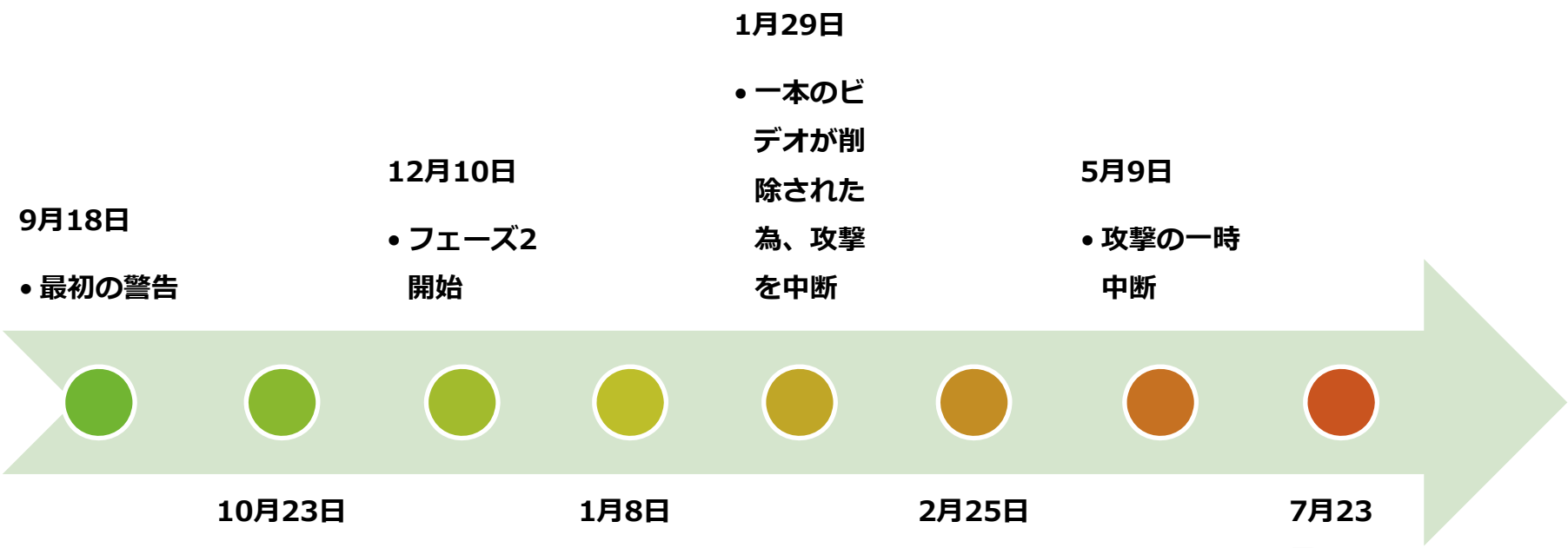
アメリカの銀行・金融関係へのDDoS攻撃

アメリカ政府がビデオを削除する決定を期待

ARBOR NETWORKS

Operation Ababil

“Izz ad-din Al qassam Cyber Fighters” は pastebin.comへの多くの功績を投稿



ARBOR NETWORKS

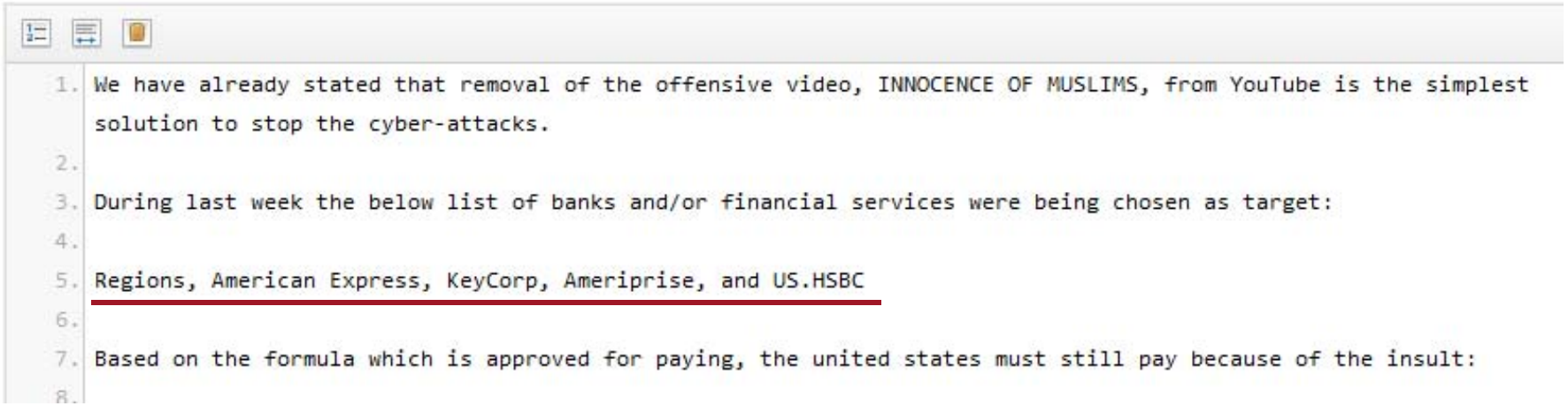
Operation Ababil

NAME / TITLE	ADDED	EXPIRES	HITS
Phase 4, Operation Ababil	Jul 23rd, 13	Never	1,030
Operation Ababil pauses this week, may 7th-9th	May 6th, 13	Never	2,215
Phase3/W9 Operation Ababil	Apr 30th, 13	Never	1,197
Phase3/W8 Operation Ababil	Apr 23rd, 13	Never	1,285
Phase3/W7 Operation Ababil	Apr 16th, 13	Never	908
Phase3/W6 Operation Ababil			
Phase3/W5 Operation Ababil			
Phase3/W4 Operation Ababil			
Phase3/W3, Operation Ababil			
Phase 3 / W 2, Operation Ababil			
Phase 3, Operation Ababil			
Operation Ababil, AlQASSAM ULTIMATUM			
Serious Warning, Operation Ababil			
Warning, Operation Ababil			

Phase/2,w/4; Operation Ababil	Jan 1st, 13	Never	3,686	None	-
Operation Ababil, Phase 2, Week 3	Dec 25th, 12	Never	1,665	None	-
الإسبوع / المرحلة الثانية...ا	Dec 18th, 12	Never	544	None	-
Phase 2/w2 Operation Ababil	Dec 18th, 12	Never	2,612	None	-
Phase 2 Operation Ababil	Dec 10th, 12	Never	8,888	None	-
المرحلة الثانية عمليات الأ...	Dec 10th, 12	Never	507	None	-
الاسبوع السادس لعمليات الا...	Oct 23rd, 12	Never	470	None	-
The 6th Week, Operation Ababil	Oct 23rd, 12	Never	2,477	None	-
الإسبوع الخامس، عمليات أب ! ...	Oct 16th, 12	Never	604	None	-
The 5th Week, Operation Ababil : 8 == 0 !	Oct 16th, 12	Never	6,239	None	-
الإسبوع الرابع لعمليات الأ...	Oct 9th, 12	Never	957	None	-
The fourth week, Operation Ababil	Oct 8th, 12	Never	5,830	None	-
Operation Ababil : second step over chase.com	Sep 19th, 12	Never	1,578	None	-
Operation Ababil : second step over chase.com	Sep 19th, 12	Never	4,969	None	-
بنك أمريكا وبورصة نيويورك ت...	Sep 18th, 12	Never	2,315	None	-
Bank of America and New York Stock Exchange under ...	Sep 18th, 12	Never	12,363	None	-

ARBOR NETWORKS

Operation Ababil



1. We have already stated that removal of the offensive video, INNOCENCE OF MUSLIMS, from YouTube is the simplest solution to stop the cyber-attacks.
2.
3. During last week the below list of banks and/or financial services were being chosen as target:
4.
5. Regions, American Express, KeyCorp, Ameriprise, and US.HSBC
6.
7. Based on the formula which is approved for paying, the united states must still pay because of the insult:
8.

すべてのビデオが削除されるまで
攻撃を続けると主張

ARBOR NETWORKS

Phases of Operation Ababil

- フェーズ 1 (2012年9月)
  - 1～2の銀行が同時に攻撃された
    主にHTTPにフラッド攻撃が組み合わされた
- フェーズ 2 (2012年12月)
  - 3～5の銀行が同時に攻撃された
    デフォルトのHTTPとSSLにフラッド攻撃が
    組み合わされた
- フェーズ 3 (2013年2月)
  - 6つ以上の銀行が同時に攻撃された
    異なる特徴は、アプリケーション攻撃の
    デフォルトがHTTPSに変化

標的を絞り込んだマルチ・ステージ & マルチ・ベクトルのDDoS攻撃

- PHP、WordPress & Joomla サーバーへの侵入
- 複数ベクトルによる同時攻撃
  - GET およびPOSTアプリ層のHTTP、HTTPSに対する攻撃
  - DNSクエリのアプリ層への攻撃
  - UDP、TCP SYNによるフラッド攻撃およびICMPを始めとするIPプロトコル攻撃

DDoS Attacks on Banks Resume

Experts Warn Botnet Getting Stronger

By Tracy Kitten | February 26, 2013 | Follow Tracy @FraudBlogger

Credit Eligible Email Tweet Like Share Get Permission

WELLS FARGO PNC CapitalOne BB&T usbank HSBC SUNTRUST CHASE Bank of America REGIONS

Izz ad-Din al-Qassam Cyber Fighters has launched a new wave of **distributed-denial-of-service** attacks against U.S. banks and credit unions, and experts say institutions can expect more incidents in the coming days.

Just after 10 a.m. ET on Feb. 25, the opening day of **RSA Conference 2013**, a handful of U.S. banking institutions were reportedly targeted as part of the latest attacks.

KrebsonSecurity
In-depth security news and investigation

19 DDoS Attack on Bank Hid $900,000 Cyberheist

FEB 13

A Christmas Eve cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than $900,000.

At approximately midday on December 24, 2012, organized cyber crooks began moving money out of corporate accounts belonging to **Ascent Builders**, a construction firm based in Sacramento, Calif. In short order, the company's financial institution – San Francisco-based **Bank of the West** – came under a large distributed denial of service (DDoS) attack, a digital assault which disables a targeted site using a flood of junk traffic from compromised PCs.

ユニークな特徴を持つ攻撃

- 個々の発信源から毎秒驚異的な量のパケットを送出
- 業界内の複数の企業に対して攻撃を実行
- 攻撃効果をリアルタイムで監視
- ミティゲーションに応じて素早くベクトルを修正する機動性

ARBOR NETWORKS

DDoSとは？

DDoS = サービス停止・不能 = サーバーへの攻撃

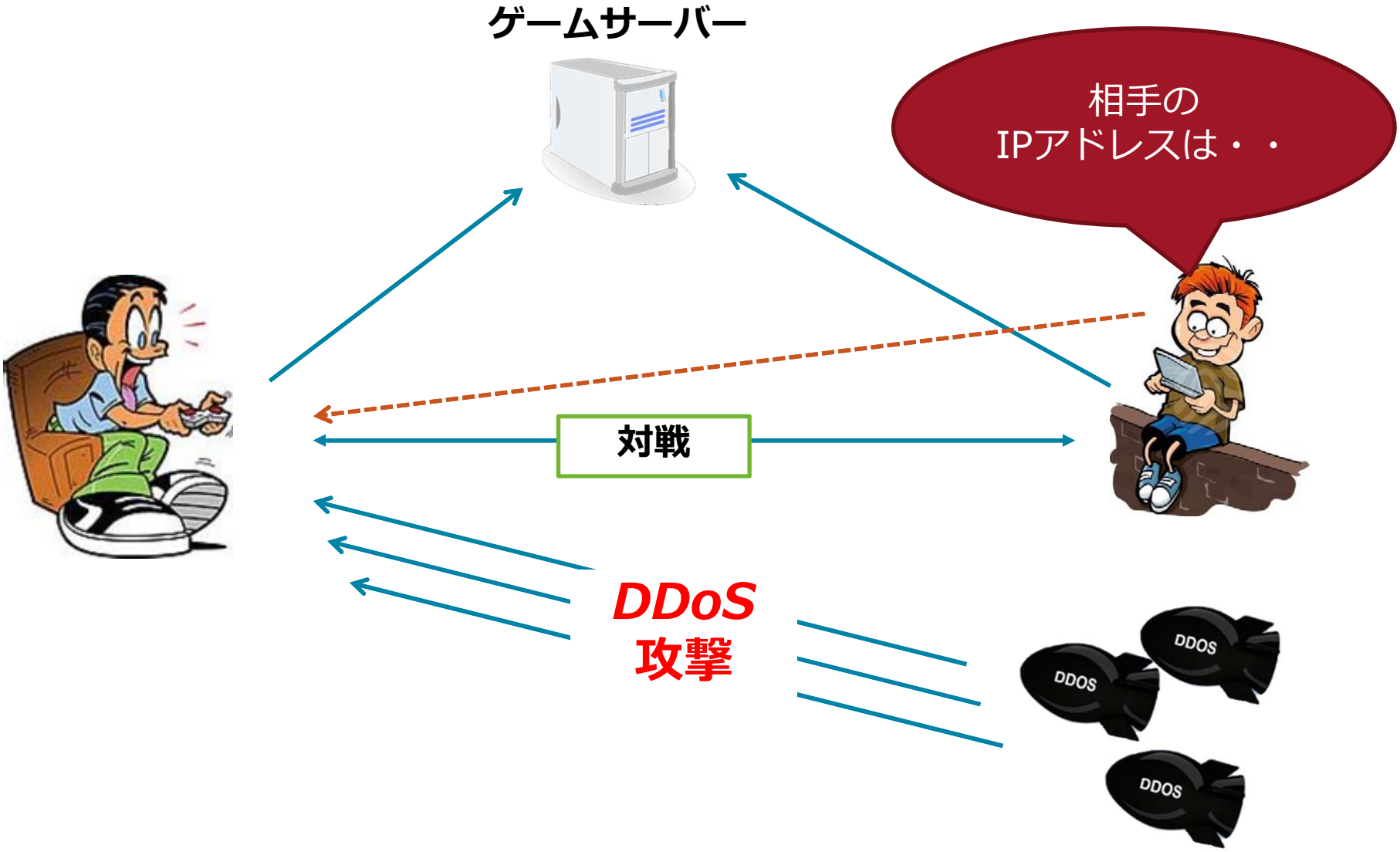
ハッキング等を紛らわすための目的

個人の趣味

ARBOR NETWORKS

オンラインゲームでのDDoS攻撃

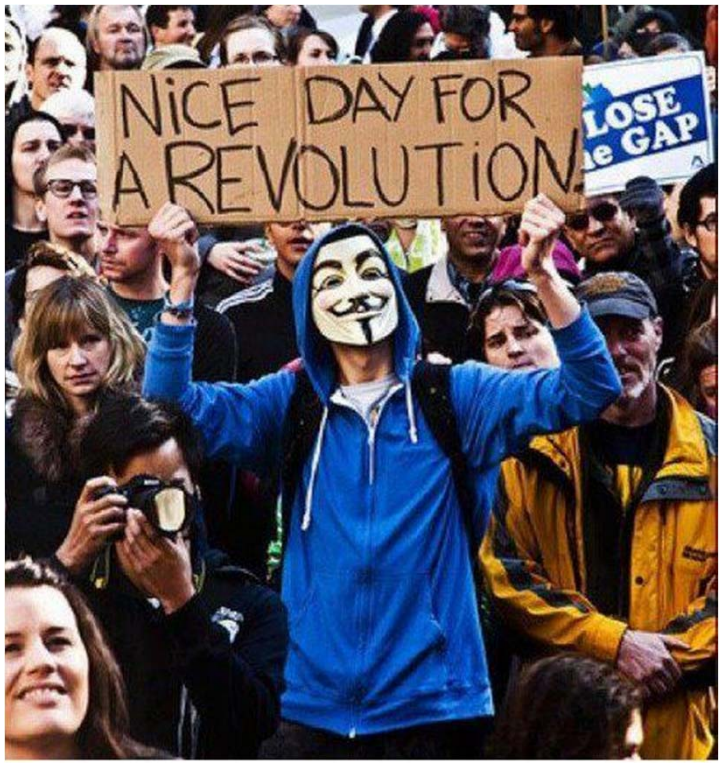
趣味



ARBOR NETWORKS

DDoS 攻撃の攻撃者像

- **12 歳**　オハイオ州で**コンピュータを学ぶ中学生**
- 13 歳　ソーシャルネットワークに飽きたホームスクールで学ぶ少女
- 15 歳　ウェブサイト改変集団に参加するブラジルの少年
- 16 歳　プログラミングを学ぶ東京の高校生
- 18 歳　高校をドロップアウトしたウクライナの学生
- 19 歳　授業での学習を実践したくなった学生
- 20 歳　毎日の単調な仕事に飽きたTaco Bellの従業員
- 21 歳　国際的なカーディングリングで働くマリの男性
- **23 歳**　副収入を得ようとしたポーランドの**主婦**
- 24 歳　手当たり次第に企業に攻撃を仕掛けようとしたハッカー
- 25 歳　韓国陸軍の兵士
- 26 歳　イラク軍の契約兵士
- 28 歳　出産間近の中国の公務員
- 29 歳　特定の政治的主張を猛進するオレゴンの完全菜食主義者
- 30 歳　ハッカーから足を洗えなかった女性ペンテスター
- **31 歳**　稼動中のサイトの脆弱性を見つけた**セキュリティ研究者**
- 32 歳　自暴自棄になったニュージーランドのアルコール依存症患者
- 34 歳　社内に攻撃のチャンスを見つけた従業員
- 35 歳　MI6の職員
- 36 歳　FSB（ロシア連邦保安庁）の職員と思われる領事館職員
- **40 歳**　5年間昇給がないことに不満を抱いた**事務職員**
- 42 歳　企業のCEOのスキャンダルを探る私立探偵
- 43 歳　ホストを感染させるごとに報酬を得るマルウェア製作者
- 45 歳　テロリストグループのメンバー
- **55 歳**　コーポレートインテリジェンスのコンサルタント



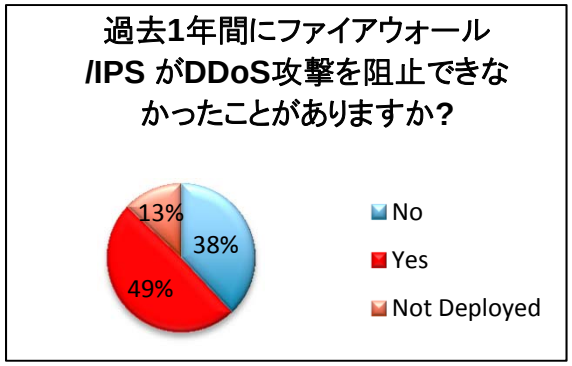
ARBOR NETWORKS

DDoS攻撃に関する誤った認識

「当社はファイアウォール/IPSで万全のDDoS攻撃対策ができている」

実際は

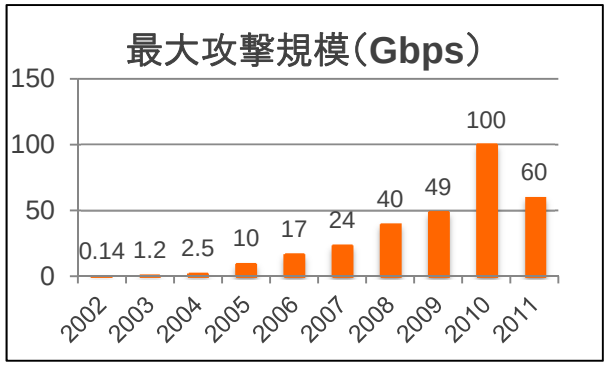
大規模データセンターのほとんどが、DDoS攻撃によってファイアウォール/IPSが無効化された経験を持つ



「十分な帯域幅があるので、DDoS 攻撃を
吸収できる」

実際は

数ギガビット級の攻撃が一般的になり、最大規模のネットワークでも麻痺させることが可能



「当社のような会社を攻撃する者などいないだろう」

実際は

ほとんどのデータセンターが毎年、DDoS攻撃によるダウンタイムを余儀なくされている

参照： Arbor Networks ワールドワイド・インフラストラクチャ・セキュリティレポート

ARBOR NETWORKS

Enterprise Lessons Learned

何がこれらの攻撃を
成功させたのか?

CHALLENGES

- 攻撃者はリアルタイムに戦術を変更
- ターゲットとする脆弱な
  銀行アプリケーションのSSLに対する
  L4/L7攻撃を使用
- いくつかのDBとミドルウェア障害
  によるログイン・サブシステムの枯渇
- インラインのFirewall/IPS/ADC
  は効果的ではない
  * ADC (Application Delivery Controller)
- キャリア/MSSP における補償の限界
- 多重層DDoS防御の欠如

何を変更する必要があるか?
我々はどのように助けられるか?

RECOMMENDATIONS

- 攻撃面を減らす
- 企業は、DDoS防御に
  投資しなければならない
  - DDoS防御のリハーサル
  - 可用性の維持に焦点を当てる
  - 効果的にMSSPと協力する
- 可用性に対する脅威に焦点を当て、
  コンプライアンス対策の義務付け
- DDoS防御は、事業継続計画（BCP）
  の一部でなければならない

ARBOR NETWORKS

MSSP Lessons Learned

何がこれらの攻撃を
成功させたのか?

CHALLENGES

- 組織の硬直
- 大きな組織のお役所仕事
- 機敏なオペレーションの限界
- 最適応答を適用するための
  ターゲット理解の欠如
- クロスファンクショナル協力の欠如
- 利用可能なすべてのミティゲーション
  オプションに対する理解の欠如

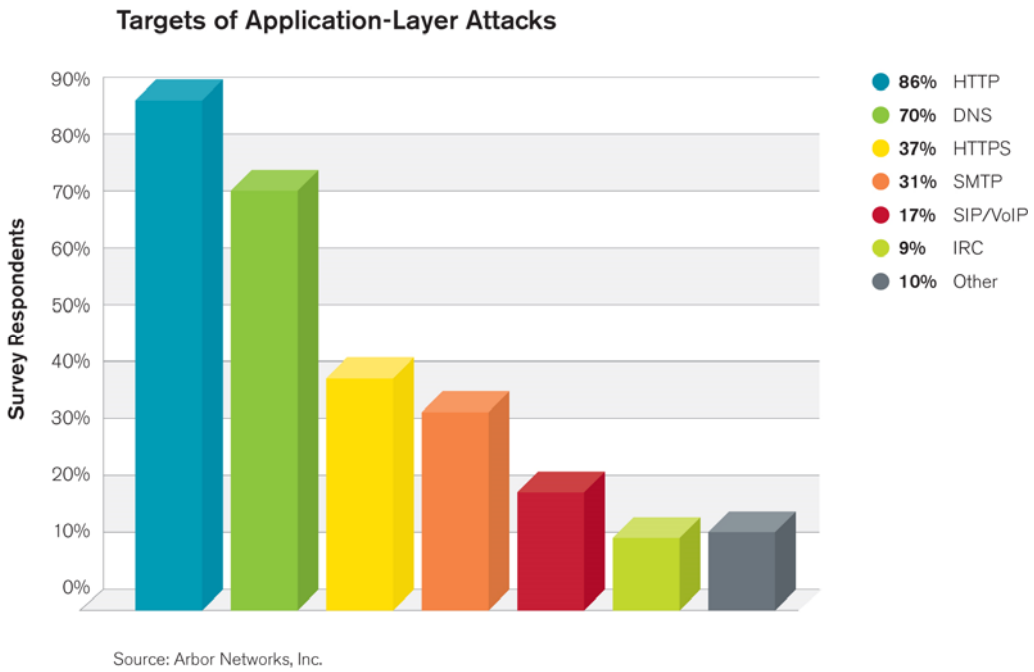
何を変更する必要があるか?
我々はどのように助けられるか?

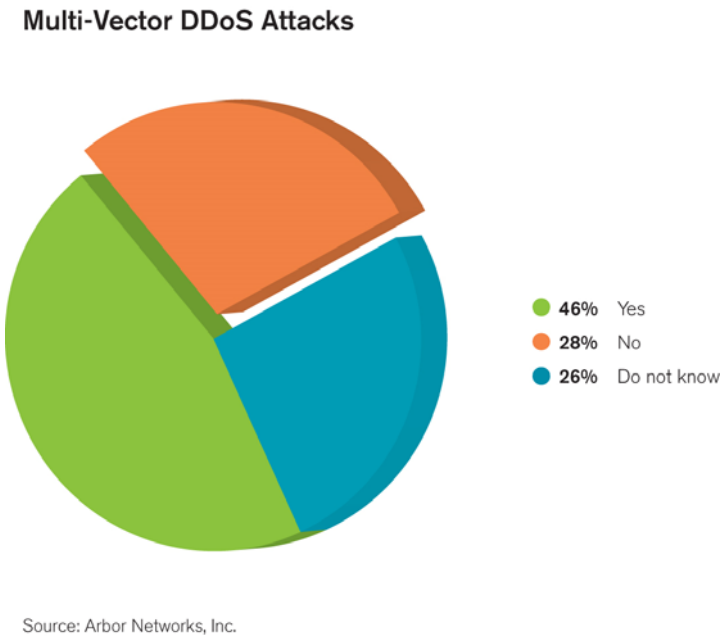
RECOMMENDATIONS

- 複数ベクトル、複数顧客への大きな攻撃に
  対処する大容量モデル
- 動的にミティゲーション能力を展開する
- ソフトウェア導入のスピードを上げる
- 脅威ミティゲーションに関する多くの教育
- ツールとCountermeasureのカスタマイズ
- ミティゲーション・シナリオの
  オペレーションと練習
- オペレーション境界を取り除く

ARBOR NETWORKS

アプリケーション層 / 複数の手法を用いた攻撃が増加





- アプリケーション層への攻撃では、**HTTP および DNS**サービスへの攻撃が大部分を占める
- また、HTTPS に対する攻撃も前年より増加
- 回答者の半数近くが**複数の手法**を用いた攻撃を経験しており、前年と比べ **60% 増加**
  - 複数の手法を用いた攻撃に効果的に対処するためには、複数のレイヤで防御システムを構築することが要求される
  - 2012年第4四半期に起こった米国の金融サービス機関を標的とした攻撃は、最たる例

ARBOR NETWORKS

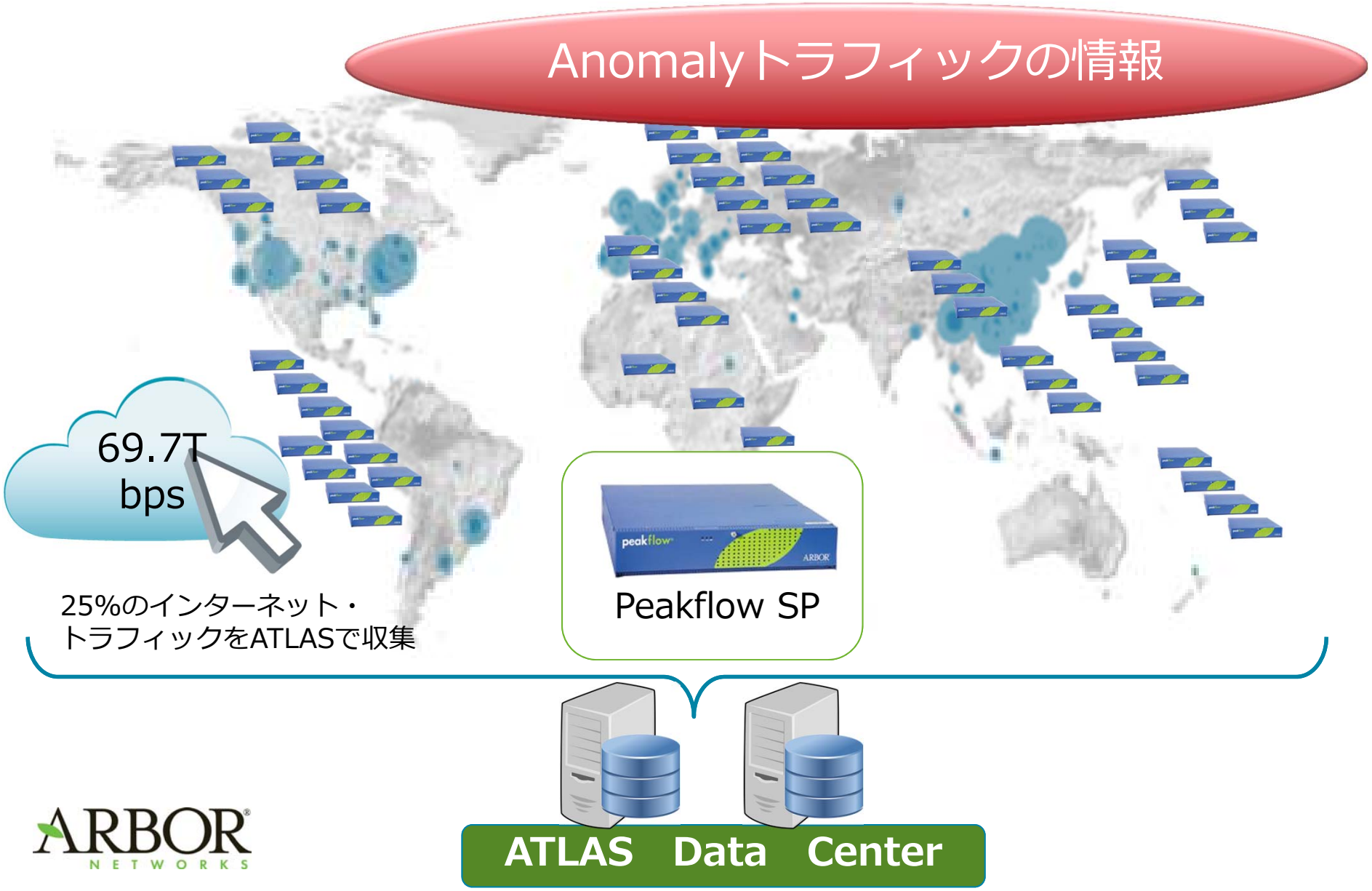
アジェンダ

DDoS攻撃の事例

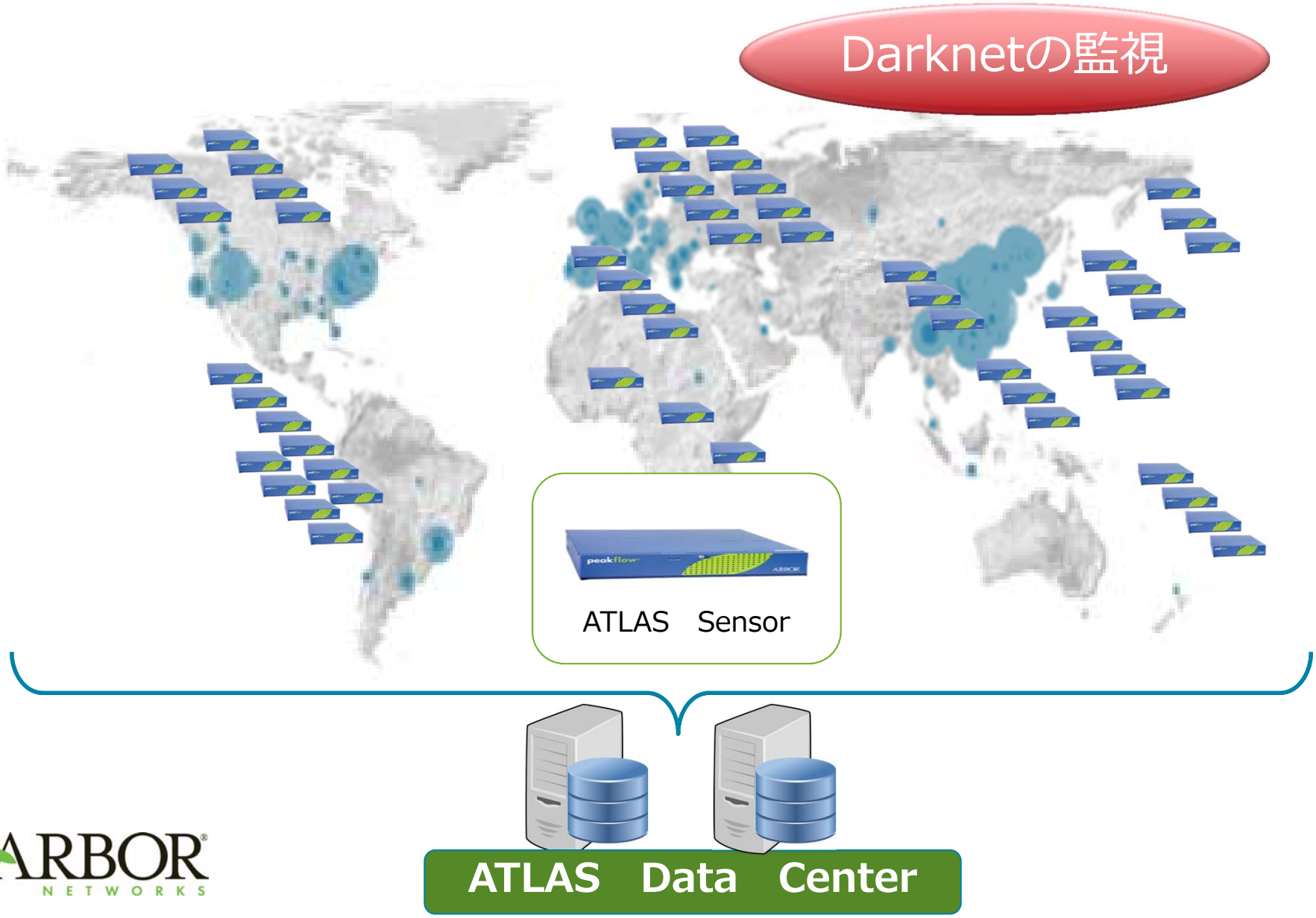
DDoS攻撃の傾向

ARBOR NETWORKS

ARBOR　Peakflow SP



ARBOR　ATLAS Sensor



Arbor ATLAS – インターネットトレンド

- 275以上のISPからリアルタイムにデータを共有
  - 一時間毎に自動的にXMLファイルをHTTPSでATLASへ送信
  - 匿名性を持ったファイルで、下記の情報のみが含まれる
    - 顧客の地域（アジア、ヨーロッパ等）
    - プロバイダー種別（Tier1, Tier2,コンテンツプロバイダー,ケーブル等）
- データはFlow / BGP / SNMP の相関関係から生成
  - Arbor Peakflow SP プロダクトの持つデータ
    - リアルタイムでのFlow/BGP
    - 実ライブトラフィック
    - Network / Router / Interface 等のTraffic Reporting
    - 脅威の検知(DDoS / 感染しているSubscriber)
      - 複数の検知手法

- ATLASは現在最大約69.7Tbpsのトラフィックをモニタリングしています
  - これはインターネットトラフィックの多くの割合を占めます

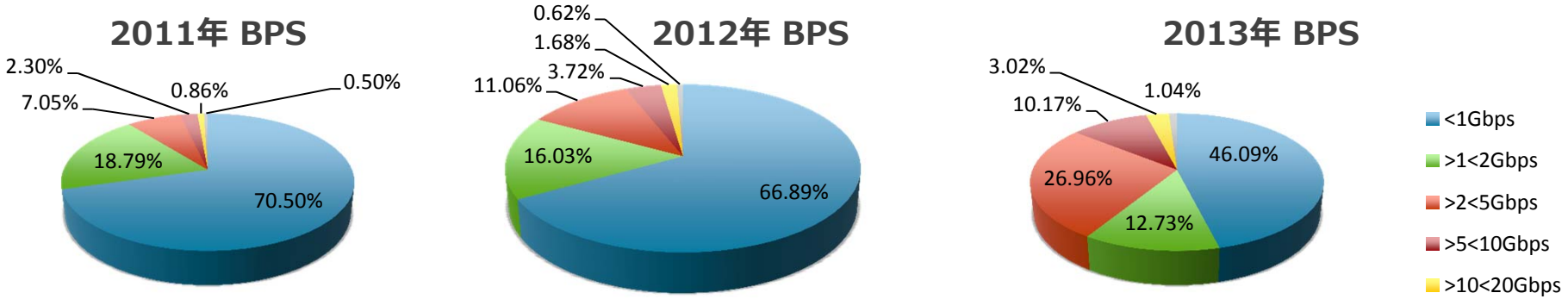
ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

BPSの大きい攻撃が引き継続き増えています。

- 1Gbpsを超える攻撃の割合が上昇
  - 21%（2010）> 29.5%(2011) -> 33.1%(2012)-> 53.91%(2013)
- 最近の傾向に反して1Mpps以下の割合が再上昇
  - 87%(2010) -> 65.07%(2011) -> 62.2%(2012) -> 77%(2013)

- 昨年と比較した平均攻撃サイズ
  - 2012:
  - 1.48Gbps (2011年と比較して20%の上昇)
  - 1.48Mpps (2011年と比較して11%の上昇
  - 2013 Q1/Q2/Q3:
  - 2.64 Gb/sec (2012年と比較して78%の上昇)
  - 982.16Kpps (2012と比較して34%の減少)



ARBOR NETWORKS

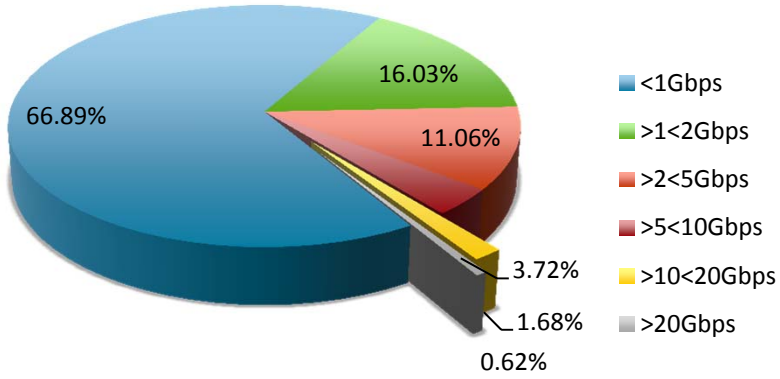
ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

BPSの大きい攻撃の割合が著しく上昇しています

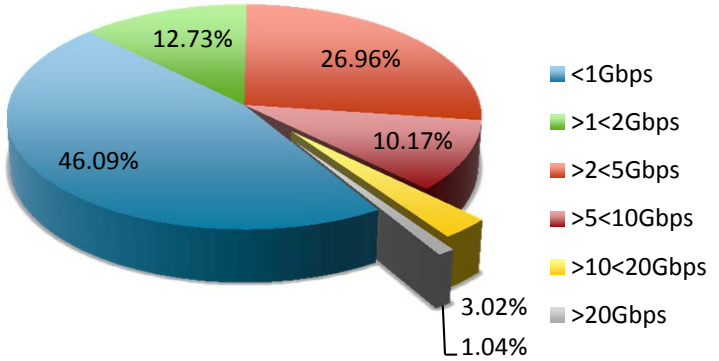
- 2012年と比較してこれまでに20Gbpsを超える攻撃回数を4.5倍以上観測
- 2-10Gbpsの攻撃割合が上昇
  - 9.3%(2011) 14.78%(2012) **37.1%**(2013)

- 10Gbpsを超える割合が非常に大きく増加
  - 2012年　2011年から69.4%の上昇
  - 2013年　2012年から**76.5%**の上昇
  - 10Gbpsを超える割合は**4.06%**
  - 10Gbpsを超える平均の攻撃サイズは**18.47Gbps**

2012年 BPS



2013年 BPS

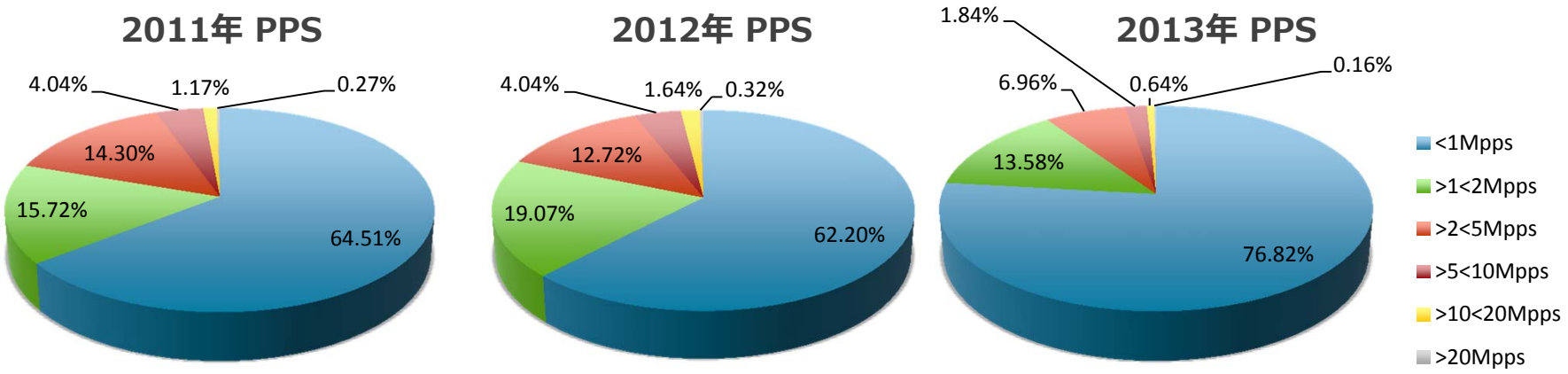


ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

*BPS*に焦点がおかれ、*PPS*は減少しています

- PPSの攻撃サイズは複数のレンジで減少:
  - 2-5Mpps –　12.7% (2012年)　7%　(2013年)
  - 5-10Mpps – 4%　(2012年)　1.84% (2013年)
  - 10Mpps –　1.96% (2012年)　0.8%　(2013年)

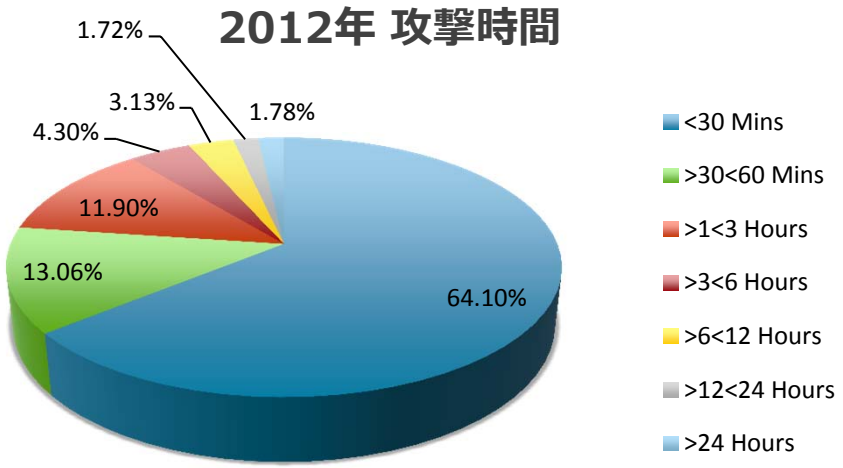


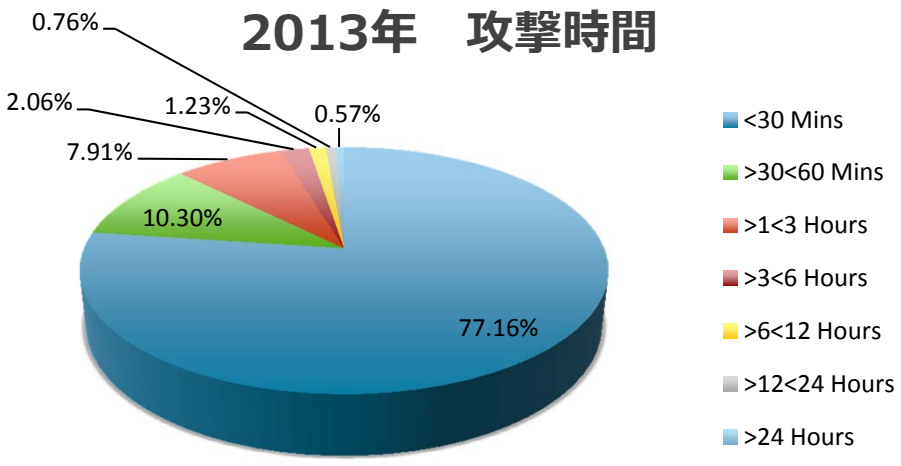
ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

短時間の攻撃がより一般的に

- 全体の約87.5%が1時間以下の攻撃
  - 2012と比較して10%もの上昇
- 平均の攻撃時間は2時間18分で、2012年と比較すると76分短縮
- 10GBpsを超える平均攻撃時間は2時間17分
- 12時間を超える攻撃割合は減少
  - 4.75%(2010), 3.7%(2011), 3.5%(2012), 1.3%(2013)





ARBOR NETWORKS

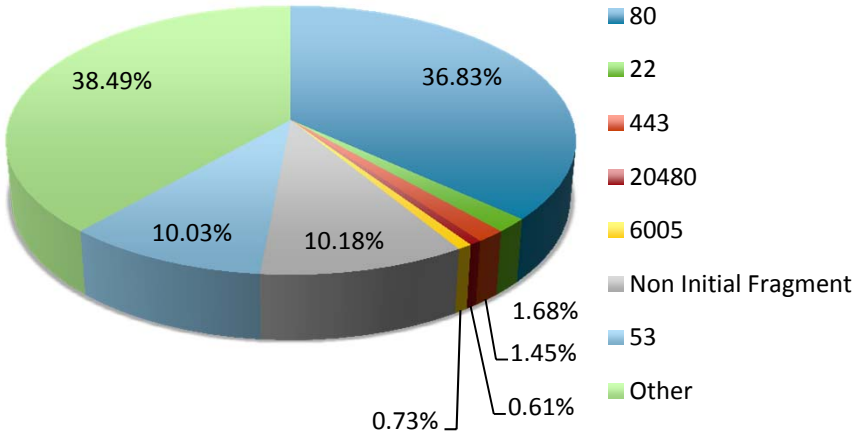
ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

フラグメントによる攻撃が大幅に増加

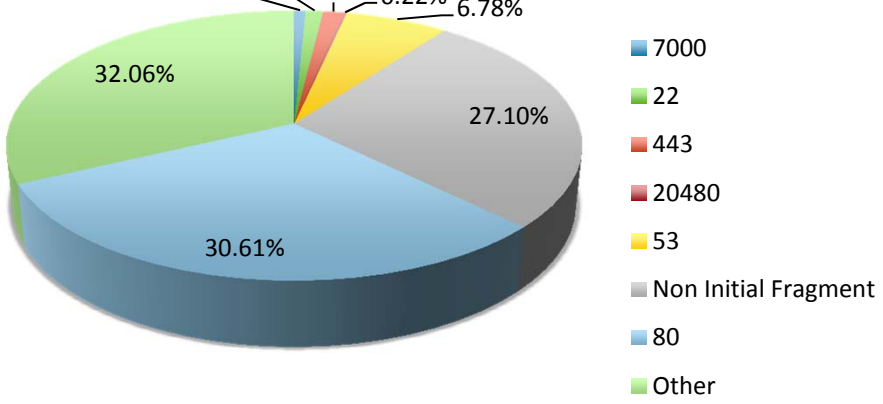
- ポート80番に対する攻撃が30.6%となり、2012年の36.8%から減少
- フラグメント（Port0）の攻撃は2012年の10.2%に対して27.1%となり大幅な上昇

- 10Gbpsを超える攻撃の55%がフラグメント（Port0)55% of attacks over 10Gb reported against port 0 (fragment)
- ポート443に対する攻撃はあまり変化なし
  - 1.45%(2012)/1.33%(2013)
- ポート53に対する攻撃は昨年の10%に対して、6.8%へ減少

2012年　ポート



2013年　ポート

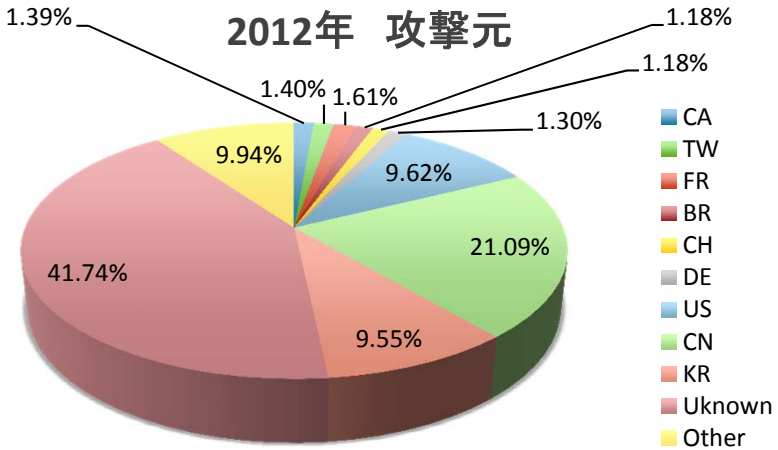


ARBOR NETWORKS

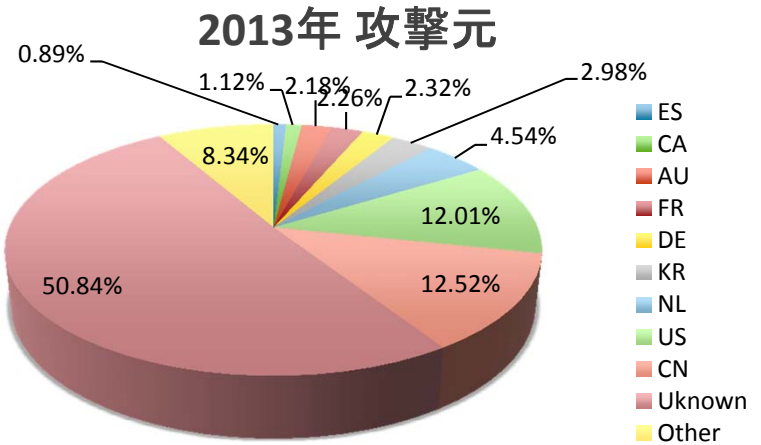
ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

攻撃元の観測

- 観測された攻撃の50.8%は 多くの分散されたソースとして攻撃元が識別不可
- 残りの49.2%の中でのトップ3の攻撃元は以下の通り
  - 中国：12.5% (21% 2012)
  - アメリカ：12% (9.6% 2012)
  - オランダ: 4.5% (2012年はTop10外)



- 10GBpsを超える攻撃元のランキングは異なります。
  - 中国：9.7% (10% 2012)
  - アメリカ：8.7% (10.4% in 2012)
  - ドイツ：2.1% (2012年はTop10外)
- 主な変化:
  - オランダは全体で第三位に
  - ドイツは10Gbps 以上で第三位に



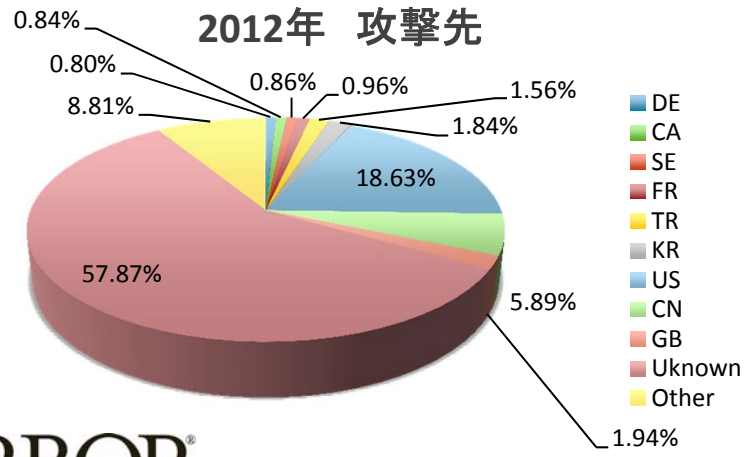
ARBOR NETWORKS

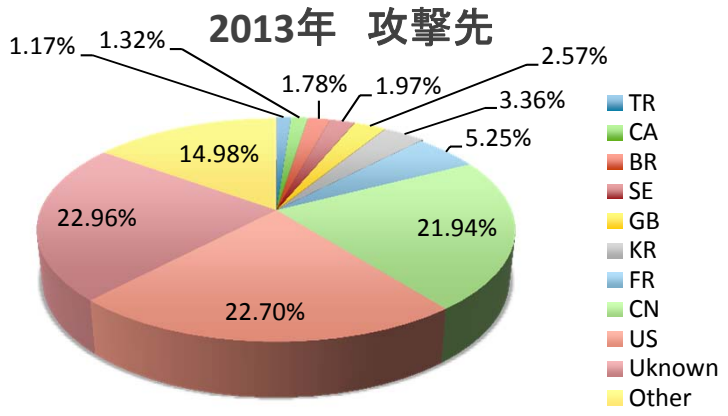
ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

攻撃先の観測

- 23%の攻撃先は識別不可
- 残り77%におけるトップ3の攻撃先は以下の通り
  - アメリカ：22.7% (19% 2012)
  - 中国：21.9% (6%　2012)
  - フランス：5.3% (1%　2012)

- 10GBpsを超える攻撃のランキングは異なります。
  - アメリカ：23.1% (25% in 2012)
  - 中国：21.8% (10.3% n 2012)
  - フランス: 5.4% (2.3% in 2012)
- 主な変化:
  - フランスが全体で第三位にI
  - 10Gbpsを超える攻撃では、イギリスが4位、韓国が5位に



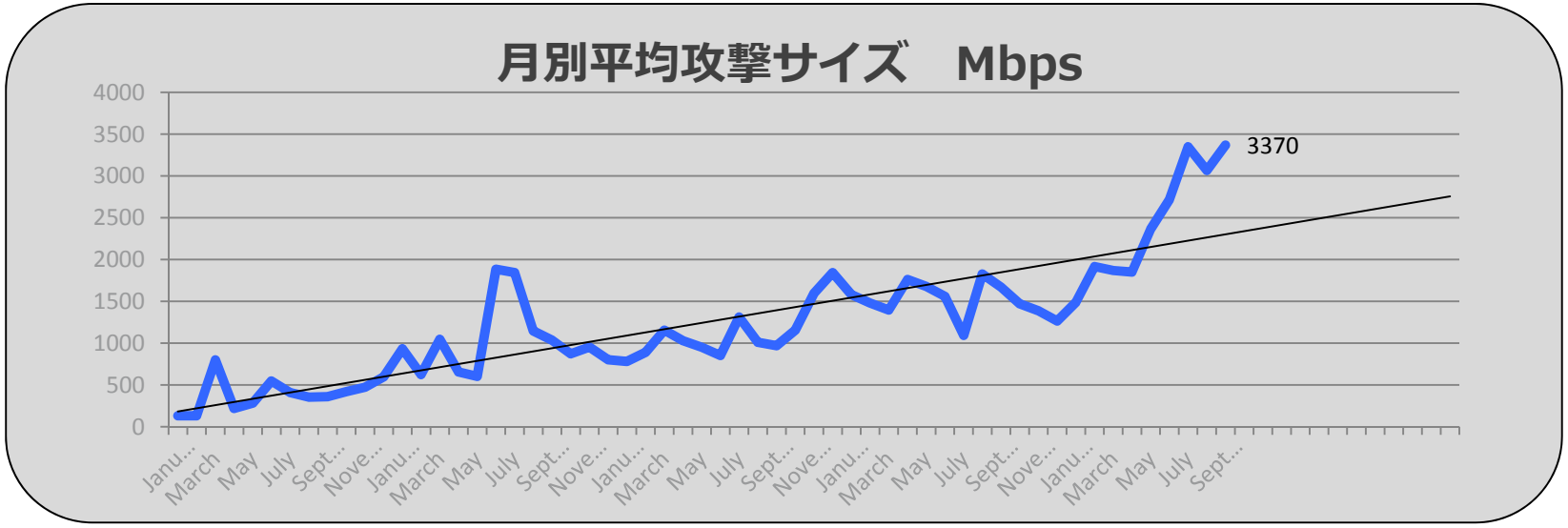


ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

*Bps*における平均攻撃サイズは引き続き上昇傾向

- 2013年9月における平均攻撃サイズは3.37Gbps
- 2013年Q3では常に３Gbps以上
- 2013年は平均攻撃サイズの伸びが非常に顕著

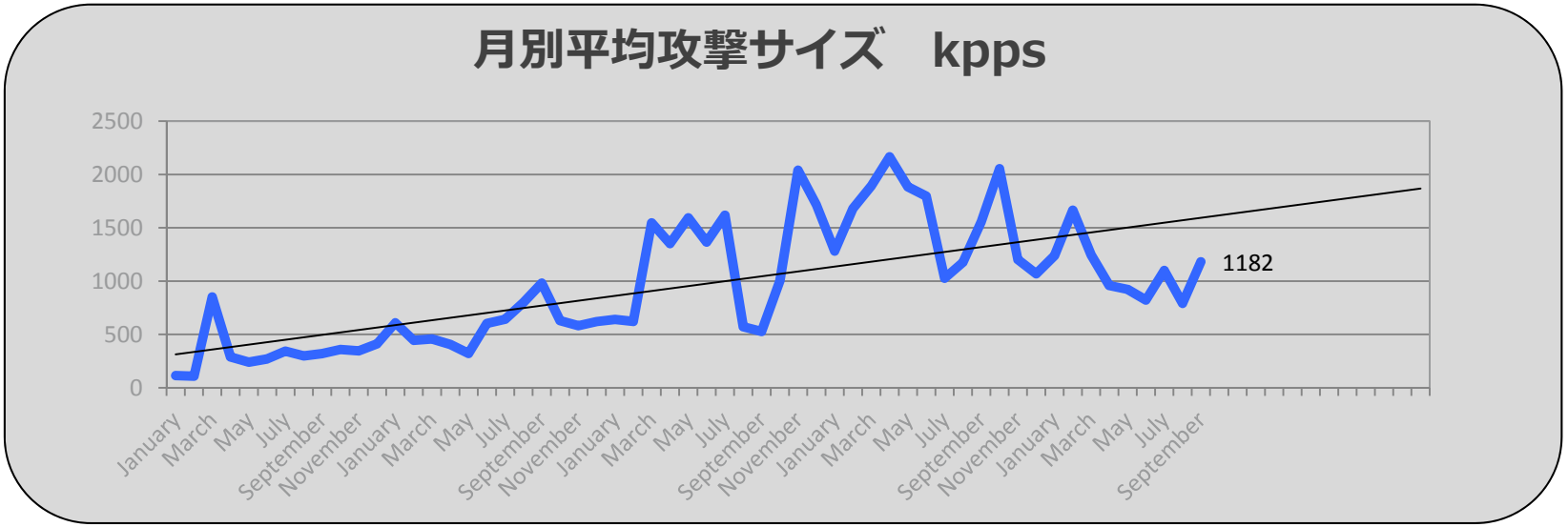


ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

*PPS*における平均攻撃サイズの傾向

- 2013年9月における平均攻撃サイズは1.18Mpps
- 2013年これまでにおいて、平均攻撃サイズは下降気味

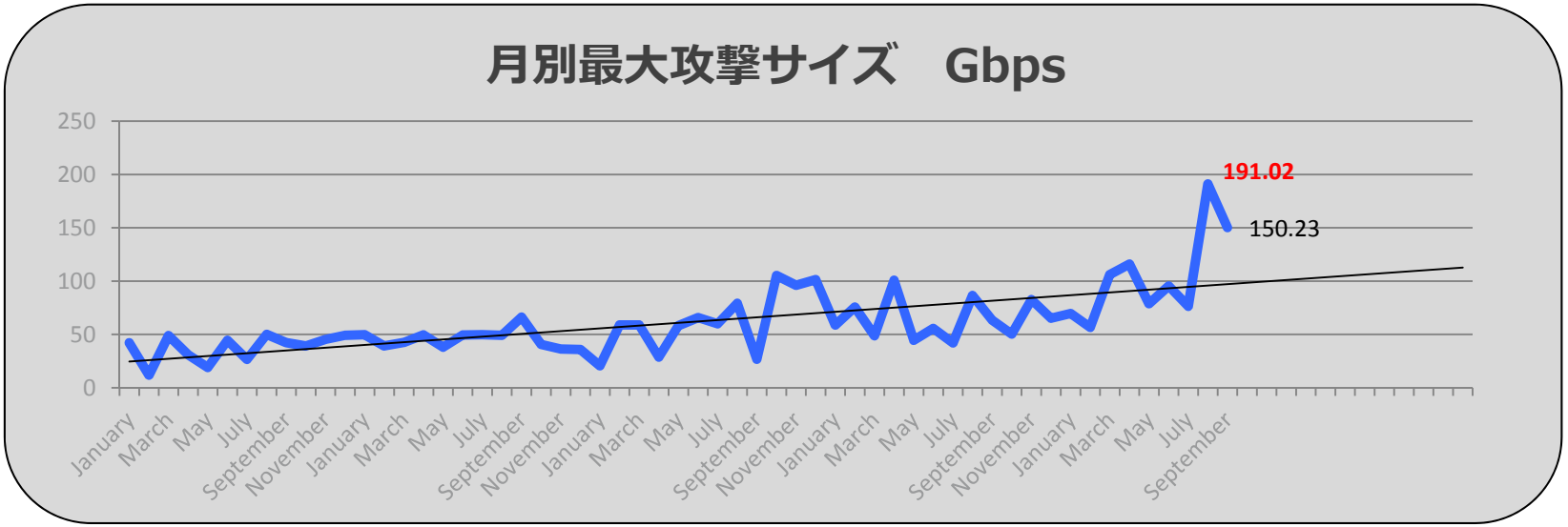


ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

*Bps*における最大攻撃サイズの傾向

- 2013年9月における最大攻撃サイズは150.23Gbps
- 断続的に100Gbps以上に上昇
- 8月には191Gbpsを観測

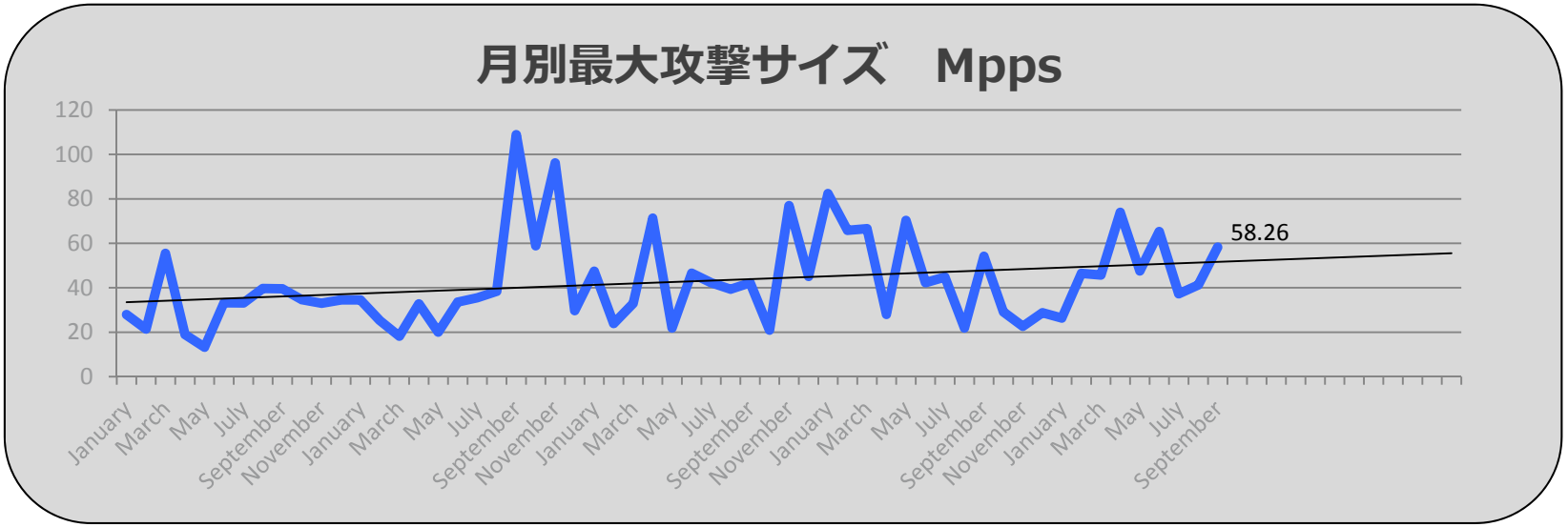


ARBOR NETWORKS

ATLAS　ワールドワイドで見る2013年のDDoS攻撃傾向

*pps*における最大攻撃サイズの傾向

- 2013年9月における最大攻撃サイズは58.26Mpps
- 月別の最大攻撃サイズは2012年に対して概ね似通った状況



ARBOR NETWORKS

ARBOR NETWORKS

ご清聴ありがとうございました

tsasaki@arbor.net