ARBOR NETWORKS

インターネット・セキュリティ最新動向と今後の展望
～2014年ワールドワイド・インフラストラクチャ・セキュリティ・レポート(WISR)第10版より～

Takashi Sasaki
SE Manager, Japan
tsasaki@arbor.net

Agenda

会社紹介

セキュリティレポートサマリー

アーバーネットワークスのソリューション

Agenda

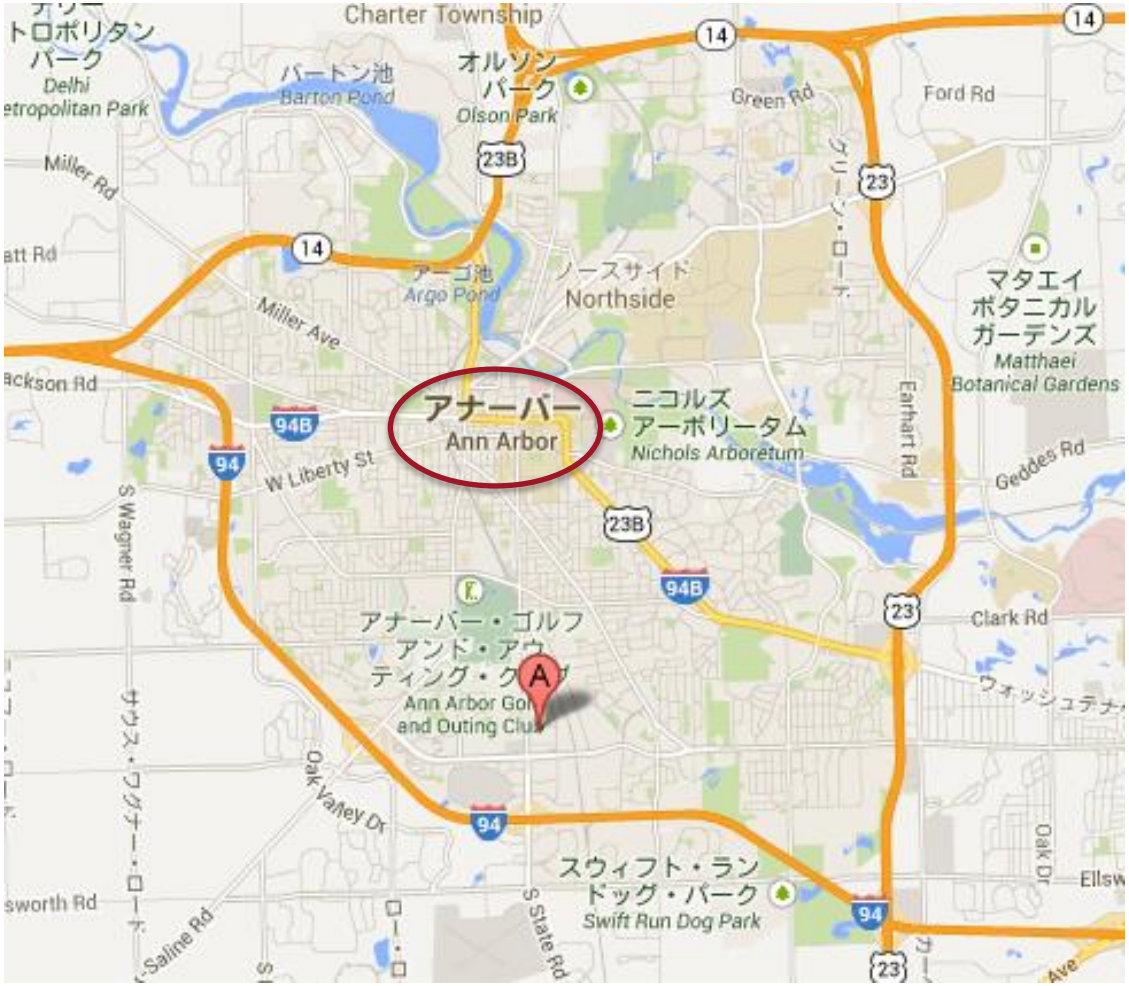
会社紹介

セキュリティレポートサマリー

アーバーネットワークスのソリューション

ARBOR NETWORKS とは

ARBOR NETWORKS とは



ARBOR NETWORKS とは

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

沿革

- 2000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
- 2013年9月　Packetloopを買収

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

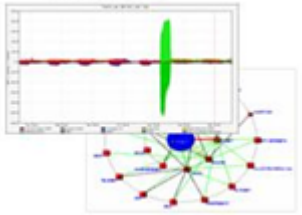
主な製品

- 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）
- Pravail™ SA（Security Analytics: セキュリティ分析ソリューション）

Arbor Networks とは ～14年間の軌跡～

2000
Arbor Networks設立
(ミシガン大学の
セキュリティ研究より)

2002
Peakflow SP
(Flowベース分析による業界初のキャリアクラスのDoS検知ソリューション)

2004

Peakflow SP
(ピアリング分析・
インフラの視認性)

2006
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

フィンガープリント・
シェアリング・
アライアンス (FSA)
& アクティブ・スレット・
フィード (ATF)

Peakflow SP TMS

DDoS Mitigation
市場に参入
(TMS 2700
：3Gbps)

2008
Peakflow SP TMS
10Gbps
DDoS Mitigation

ATLAS®
(世界初のグローバルな脅威分析)

2010
Peakflow SP TMS
40Gbps
DDoS Mitigation

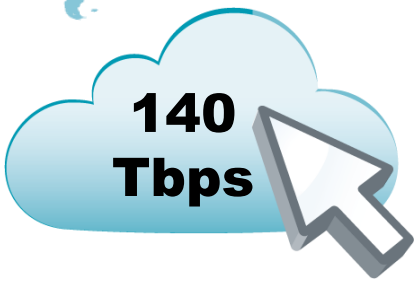
2012
INFONETICS RESEARCH
市場全体の61%の
シェアを持ちArborは
DDoS市場のリーダに
(インフォネティクス
リサーチ社より)

ARBOR NETWORKS

世界中最大級のネットワーク監視システム

90% Tier1サービスプロバイダの90%がARBORのお客様

107 ARBORの製品は107ヶ国に展開



35%のインターネット・トラフィックをATLASで監視

14 ARBORは革新的なセキュリティとネットワーク可視化技術を14年間に渡り提供

ARBORの市場ポジションはキャリア・エンタープライズ・モバイルのDDoS市場において61%のシェア
[Infonetics Research Dec 2011]

$16B 2011年 GAAP 売上高 [USD] $16Bのダナハーは ARBORの親会社として財政的支援を行う

ARBOR NETWORKS

ATLAS (Active Threat Level Analysis System：脅威レベル解析システム)

ATLAS®

Peakflow SP
Peakflow SP
ISP Network
DARKNET
ATLAS SENSOR

Peakflow SP
Peakflow SP
ISP Network
DARKNET
ATLAS SENSOR

Peakflow SP
Peakflow SP
ISP Network
DARKNET
ATLAS SENSOR

ATLAS DATA ASERT CENTER

http://atlas.arbor.net/

140 Tbps

ピーク時最大140Tbps の
インターネット・トラフィックを
ATLASで収集

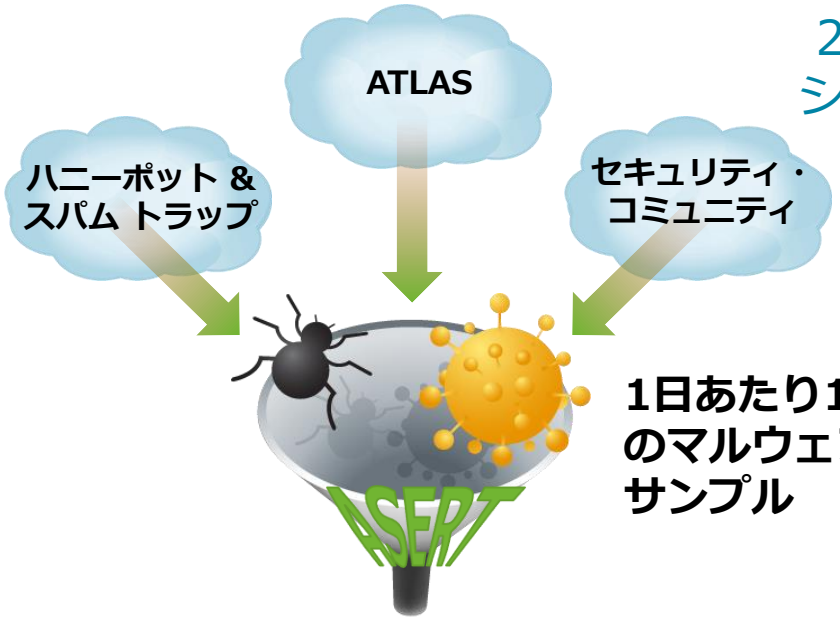
❶ 攻撃活動を発見し分類するためにダークネット空間でATLAS SENSORが展開される。

❷ ARBORのPeakflow、サードパーティおよび脆弱性のデータと組み合わせてATLAS DATA CENTERに送信される。

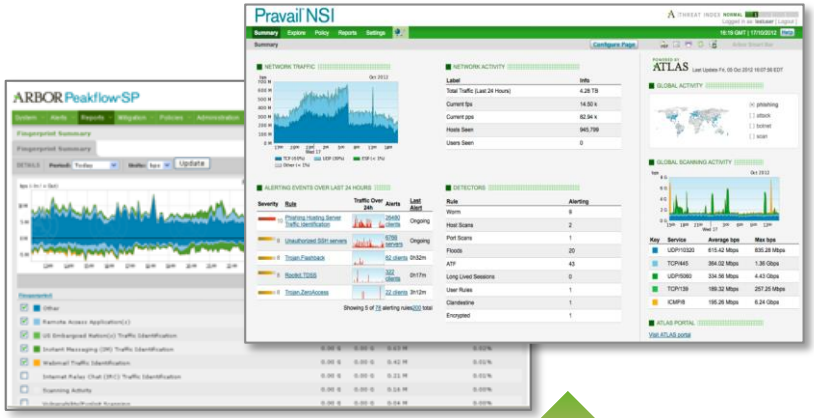
❸ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
・過去24時間の攻撃種類トップ
・過去24時間の攻撃における送信元など

ARBOR NETWORKS

ASERT (Advanced Threat にフォーカスした解析チーム)



20を超えるマルウェアの
シェアリング・パートナー



1日あたり10万個のマルウェア・サンプル

VM上のサンドボックスでマルウェアを実行
(C&Cサーバ、ボットネットなどの振る舞いを検出)

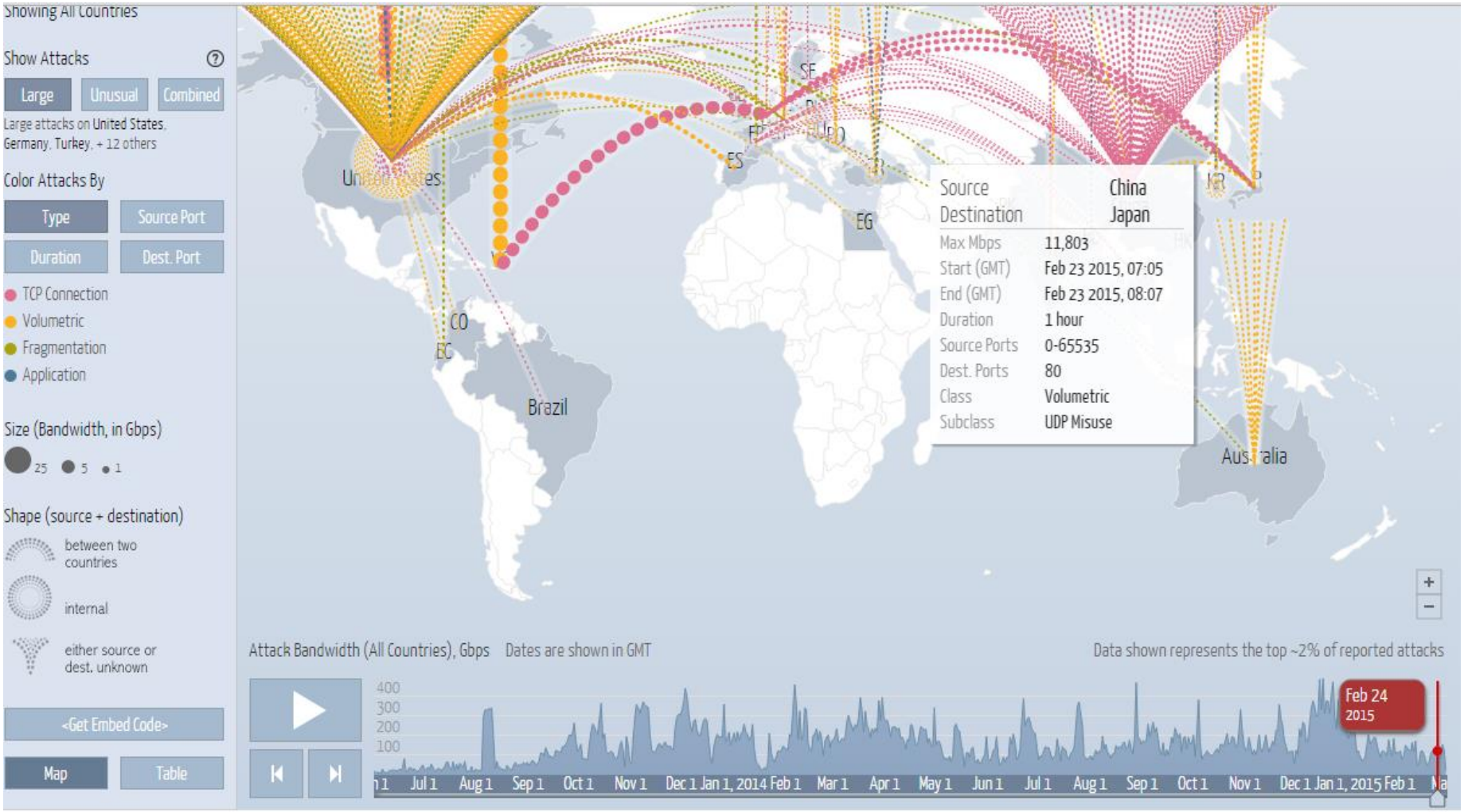
データベースに
レポートとPCAP
を保存

24時間毎に自動的に
分析・分類された
攻撃を追跡

ATF Fingerprints

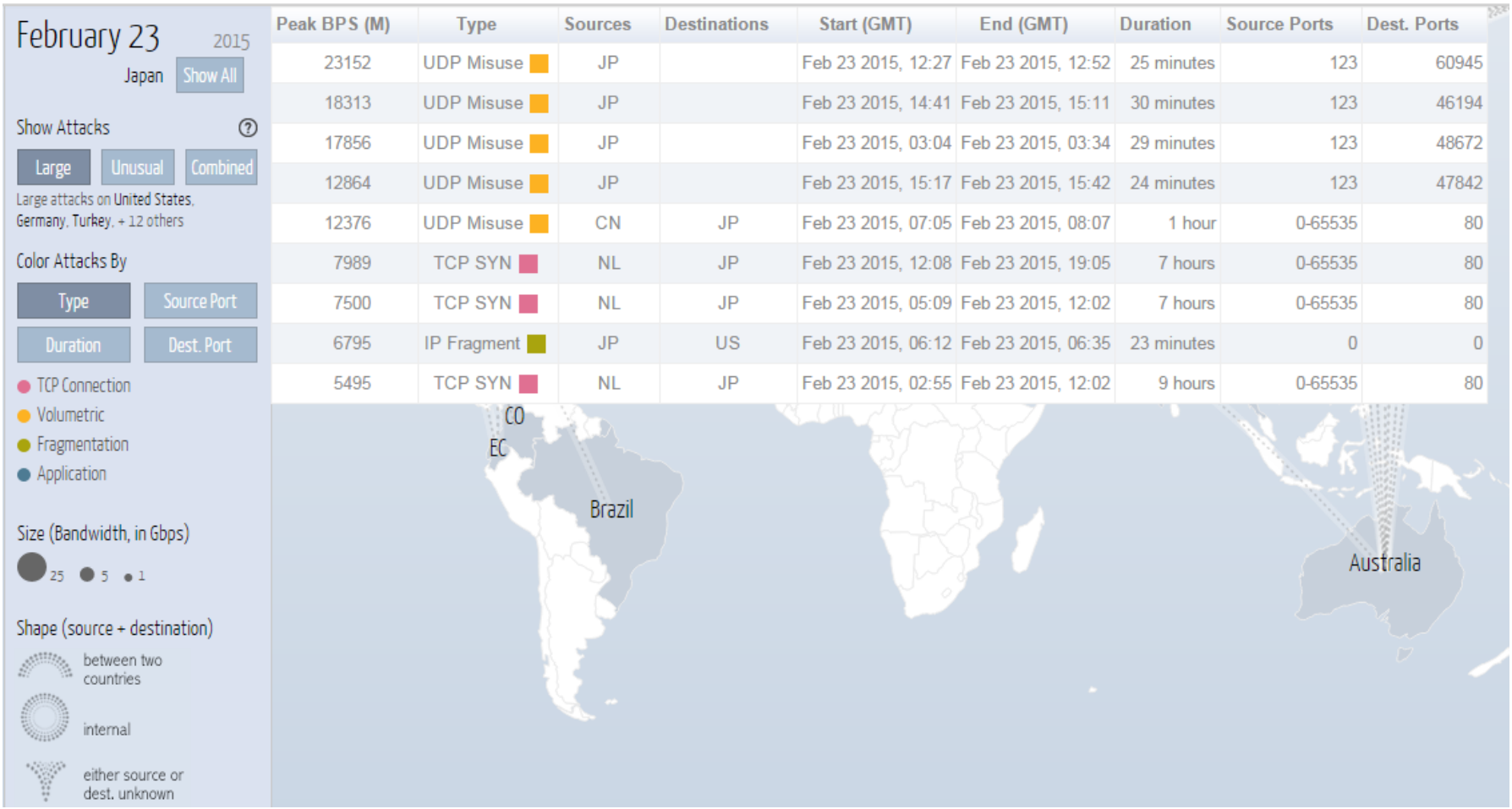
ARBOR NETWORKS

www.digitalattackmap.com



Privacy & Terms · Google ideas · ARBOR ·

www.digitalattackmap.com



Peak BPS (M)	Type	Sources	Destinations	Start (GMT)	End (GMT)	Duration	Source Ports	Dest. Ports
23152	UDP Misuse	JP		Feb 23 2015, 12:27	Feb 23 2015, 12:52	25 minutes	123	60945
18313	UDP Misuse	JP		Feb 23 2015, 14:41	Feb 23 2015, 15:11	30 minutes	123	46194
17856	UDP Misuse	JP		Feb 23 2015, 03:04	Feb 23 2015, 03:34	29 minutes	123	48672
12864	UDP Misuse	JP		Feb 23 2015, 15:17	Feb 23 2015, 15:42	24 minutes	123	47842
12376	UDP Misuse	CN	JP	Feb 23 2015, 07:05	Feb 23 2015, 08:07	1 hour	0-65535	80
7989	TCP SYN	NL	JP	Feb 23 2015, 12:08	Feb 23 2015, 19:05	7 hours	0-65535	80
7500	TCP SYN	NL	JP	Feb 23 2015, 05:09	Feb 23 2015, 12:02	7 hours	0-65535	80
6795	IP Fragment	JP	US	Feb 23 2015, 06:12	Feb 23 2015, 06:35	23 minutes	0	0
5495	TCP SYN	NL	JP	Feb 23 2015, 02:55	Feb 23 2015, 12:02	9 hours	0-65535	80

Powered by **Google Ideas**. DDoS data ©2013, **Arbor Networks, Inc.**

Agenda

会社紹介

セキュリティレポートサマリー

アーバーネットワークスのソリューション

ワールドワイド・インフラストラクチャ・セキュリティ・レポートについて

Peakflow SP

ATLASセンサー

ハニーポット

顧客への
サーベイ

ATLAS Data Center

ASERTによる分析

ARBOR SERT
Security Engineering & Response Team

WISR

ARBOR NETWORKS

今年はWISR10周年になります

セキュリティの脅威、懸念、及び緩和・検知の戦略や技術に対するセキュリティコミュニティへの調査の10年

この期間に渡り、調査範囲と回答者は大きく広がりました

いくつかの明確な継続的な動向や、いくつかの新しい実態が毎年観測されています

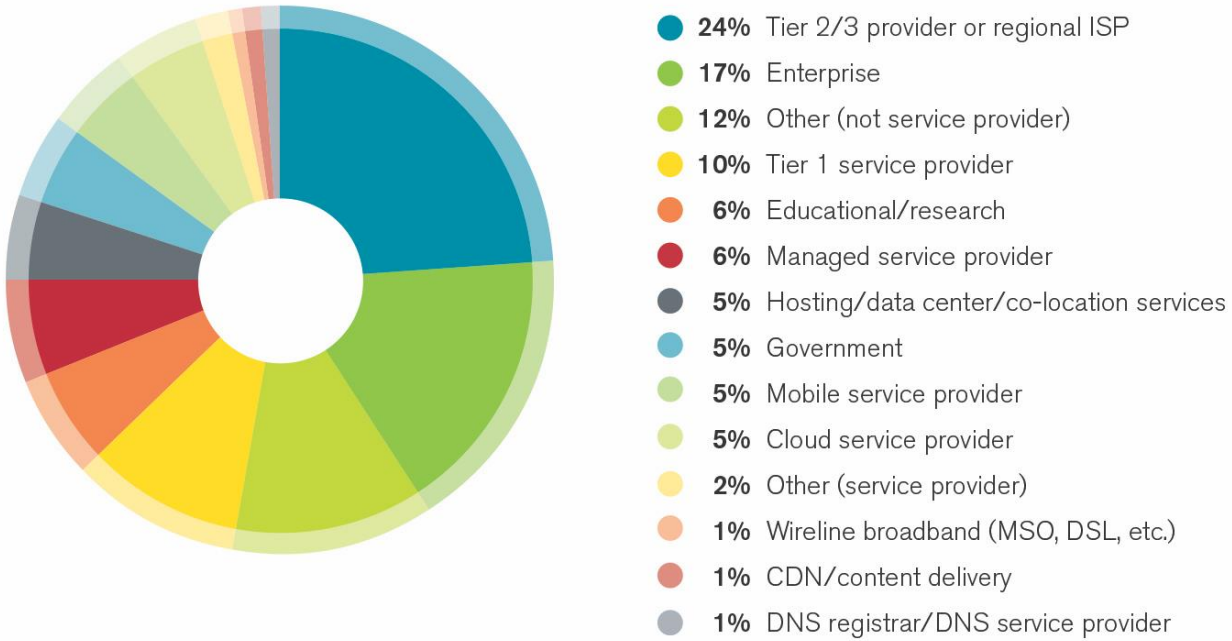
セキュリティの脅威の進化と、それらに対抗する我々の手段にとって、とても貴重なデータの積み上げになっています

`多くのものは変わりましたが、多くの人々は同じままです'

ARBOR NETWORKS

調査分布– 主要ビジネス

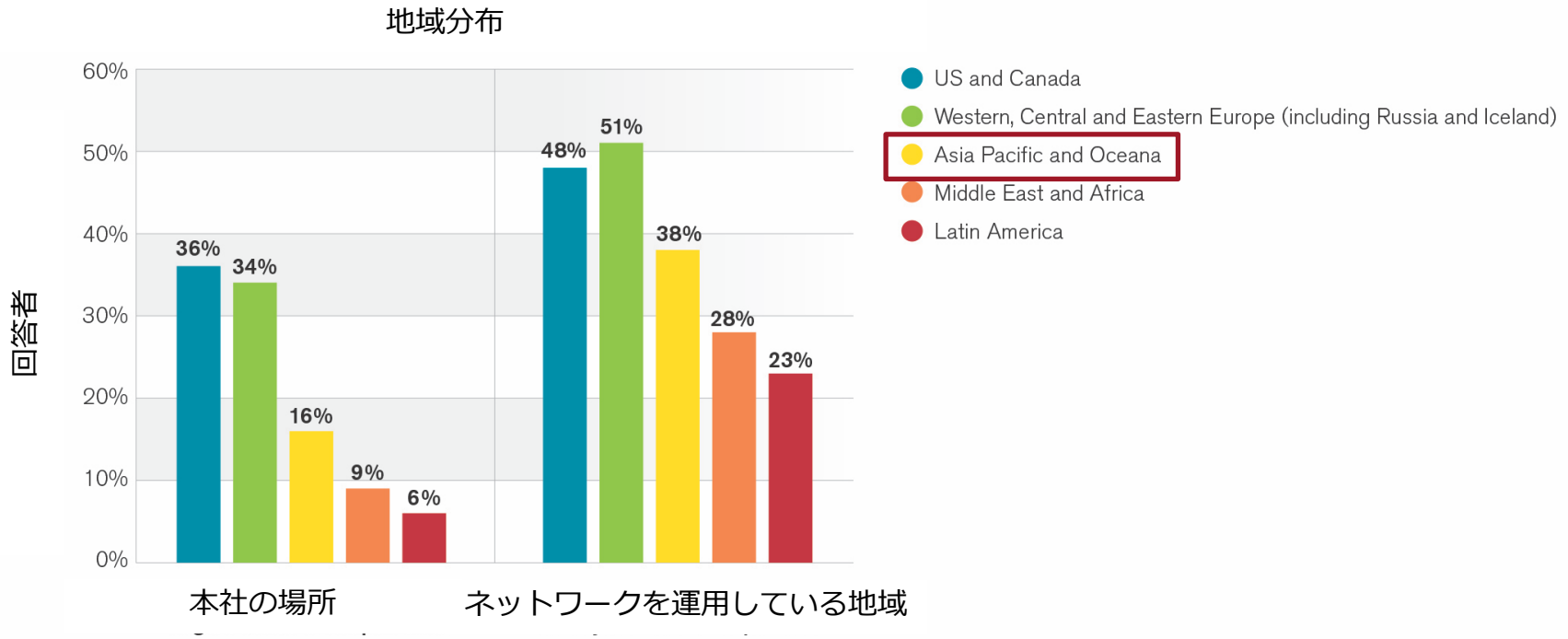
回答者の主要ビジネス



Source: Arbor Networks, Inc.

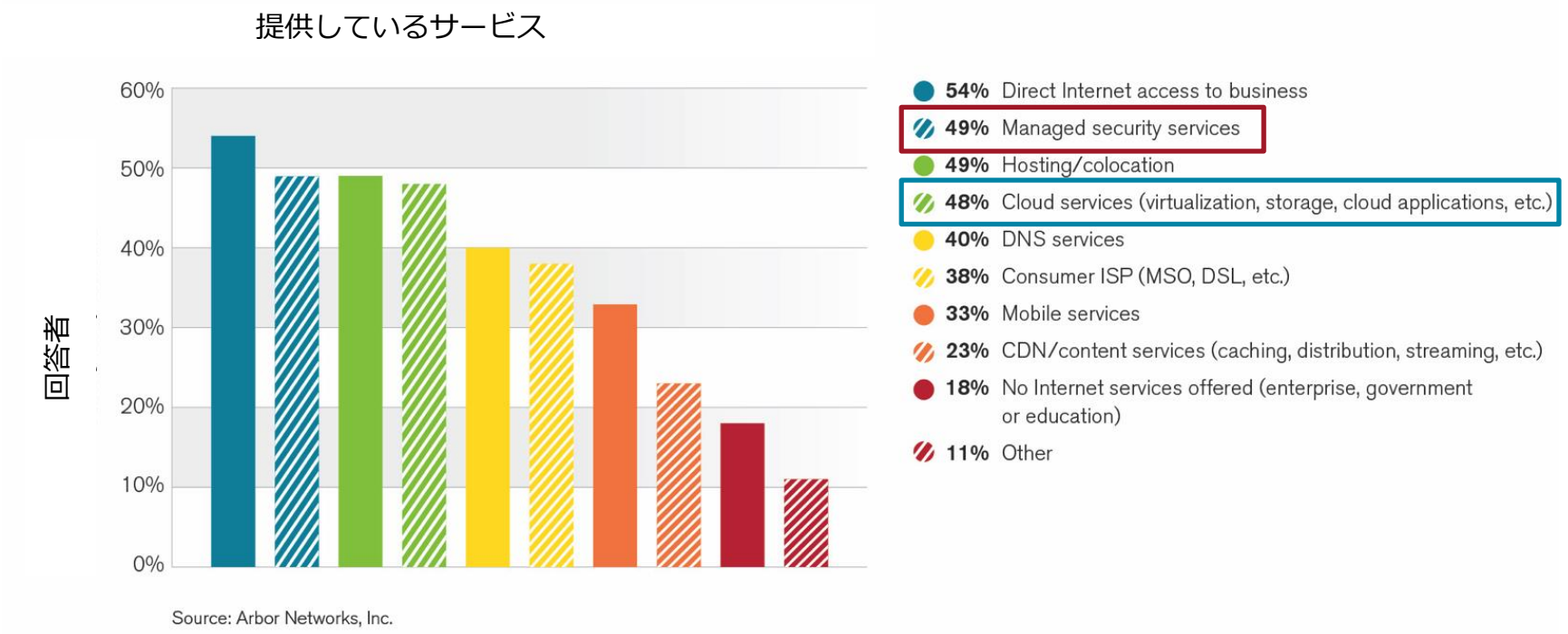
- 調査は2014年10月に行われました
- 287の回答を複数のビジネスマーケットから得ています
- 60%がインターネットサービスプロバイダになります

調査分布– 地域



- 今回はアメリカ/カナダがトップの地域で、前回のヨーロッパから変わりました
  - その他の地域は前回とほぼ同じです
- 回答者の70%はネットワーク、セキュリティ、又はオペレーションの技術者です

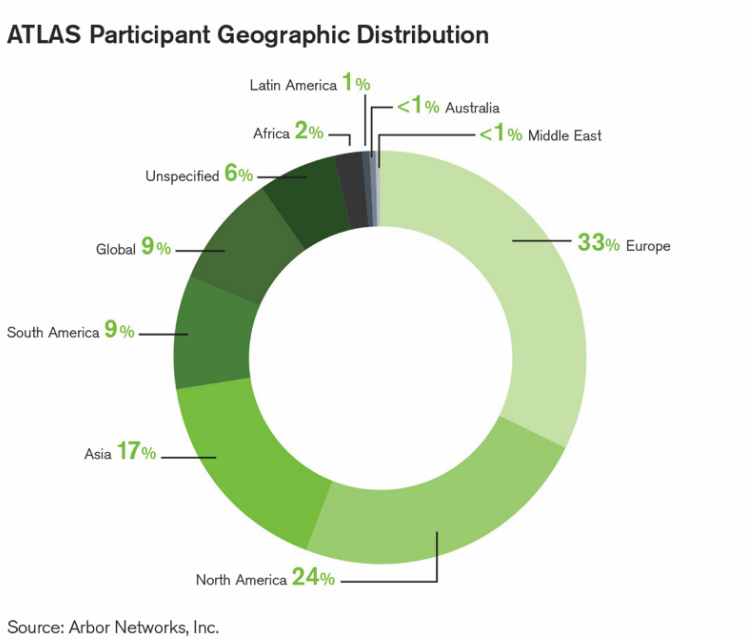
調査分布– 提供サービス

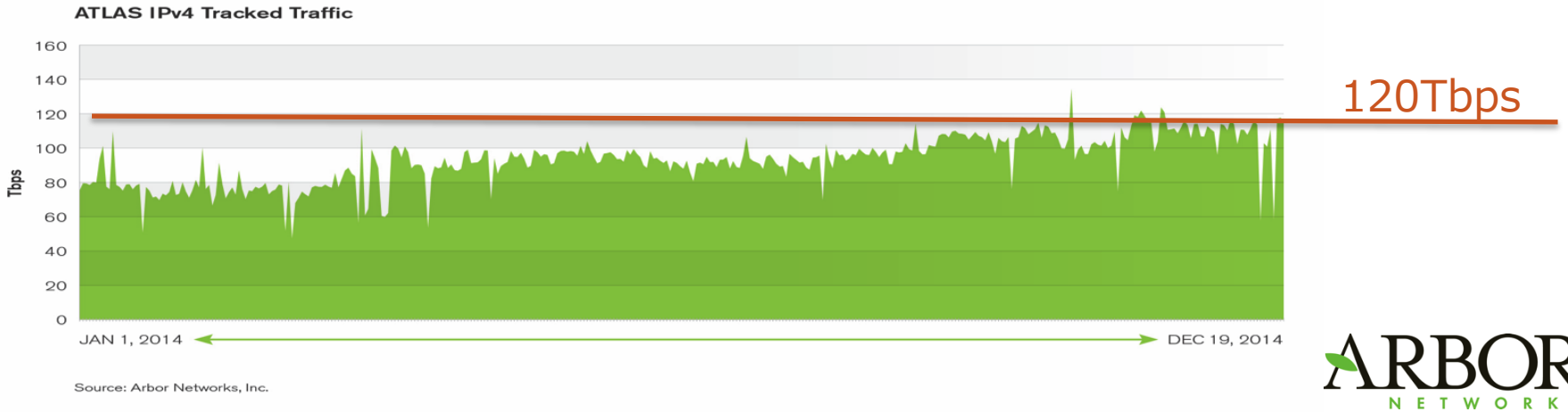


- 多くの回答者が複数のサービスを提供しています
- 法人向けインターネットアクセス、ホスティング、コロケーション、マネージド・セキュリティサービスが多くを占めています
  - マネージドセキュリティサービスは前回6位から2位へと大きく上昇しています
- 全体的にそれぞれのサービスを提供してる割合が減少しています

ATLAS の分布

- ATLASは非常に貴重なデータをアーバーの顧客と幅広いセキュリティ・コミュニティに提供しています
- 330社以上の参加顧客
  - 32% ヨーロッパ
  - 24% 北米
  - **17% アジア**
  - 9% 南米
  - 9% その他
- 最大で120Tbpsのモニタリング





主な調査結果

2014年のDDoS: リフレクション攻撃の年でした…

- 最大攻撃サイズは引き続き上昇しています
- とても大きな攻撃が多数報告又は観測されています
- 攻撃の回数は再び跳ね上がっています
- 多くの報告者はクラウドサービスが影響を受けたことを指摘しています
- 攻撃に対抗する手段として、ACLよりIntelligent DDoS Mitigation Solutions (IDMS) を使うという報告の数が初めて上回りました

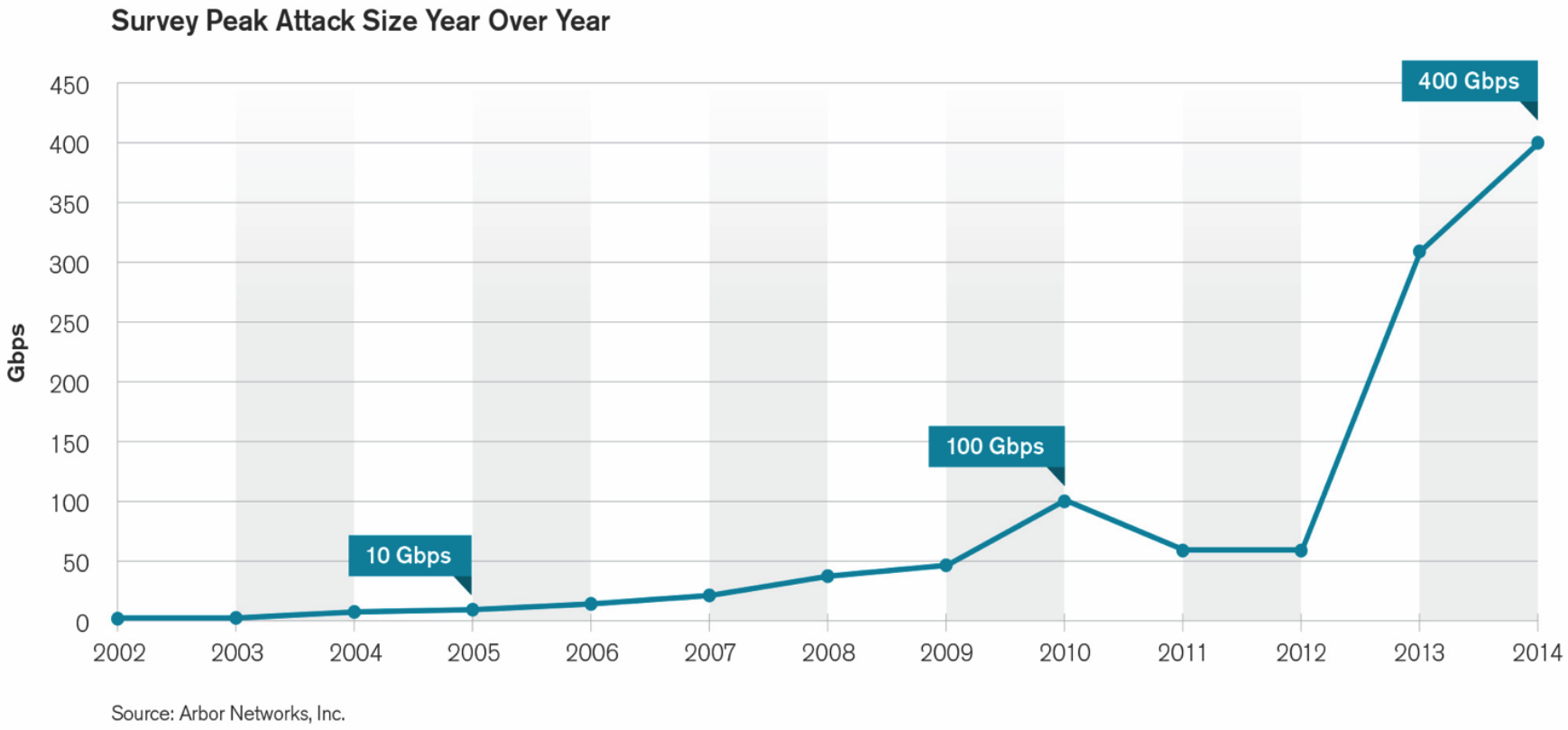
企業ネットワークセキュリティ

- 今年はISP、企業、官公庁、教育機関からのデータになります
- 半分の回答者のみが、セキュリティインシデントに対して合理的な準備をしていました
- すべての回答者において、DDoSは最大のセキュリティ脅威となっています
- 半分の回答者がDDoS攻撃を経験し、又、インターネット回線が飽和する攻撃の割合が非常に多かったと報告しています
- 今後はAPTが最大の懸念事項となっています

主な調査結果

IPv6	•トラフィックは大きく伸びているが、それでもまだ著しい量ではない (IPv6はIPv4の1%) •3/4近いサービスプロバイダーは、いくつかのお客様にIPv6サービスを提供しています
データセンター	•DDoS攻撃により収益を失った数が大きく増えています •DDoS攻撃を報告した2/3の回答者は、38%の攻撃はインターネット帯域を逼迫するものであったとしています •DDoS防御の為にIDMSとACLを使う事が大きく上昇しています
DNS	•懸念される傾向としてDNSセキュリティに対する取り組みが減少しています •回答者の僅かがDDoSによる顧客への影響があったと報告しています。
セキュリティ対策	•殆どの回答者が専任のリソースを確保していますが、依然として新規雇用や雇用確保が問題になっています •なりすまし対策やDDoS対策のリハーサルが削減されていることが懸念されます
モバイル	•LTEは幅広く導入されています •少数の回答者がセキュリティ事案のために顧客が影響を受けたとしています •攻撃はインフラに向けられて行われ、Gi/SGiが影響をうけています

最大攻撃の飛躍的な伸び



- 報告された最大の攻撃は400Gbpsであり、300Gbps, 200Gbps, 170Gbpsと続きます
- 100Gbps以上の攻撃が複数報告されていますが、このグラフでは最大攻撃のみ表しています。

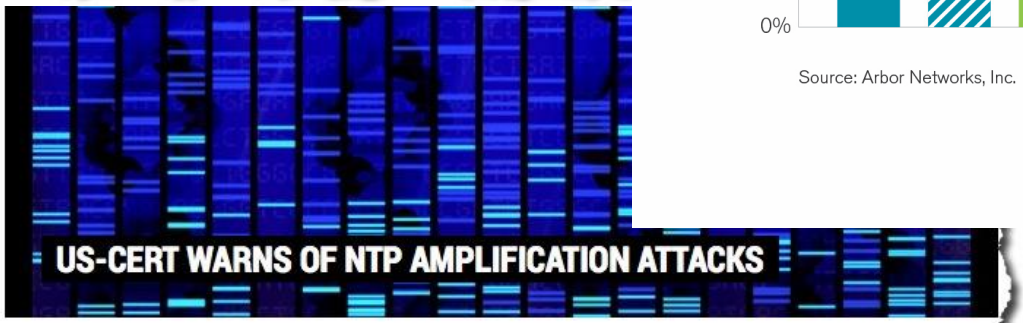
2014年はリフレクション攻撃の年でした.....

How DERP Was Able to Take Down Origin, League of Legends

January 9, 2014 - GamePolitics Staff

Ars Technica offers
insights into why th
denial-of-service (D
out EA's Origin serv
Battle.net, and Leag
particularly potent.
the DDoS attacks us
method to amplify t
being sent in order
online games to a h

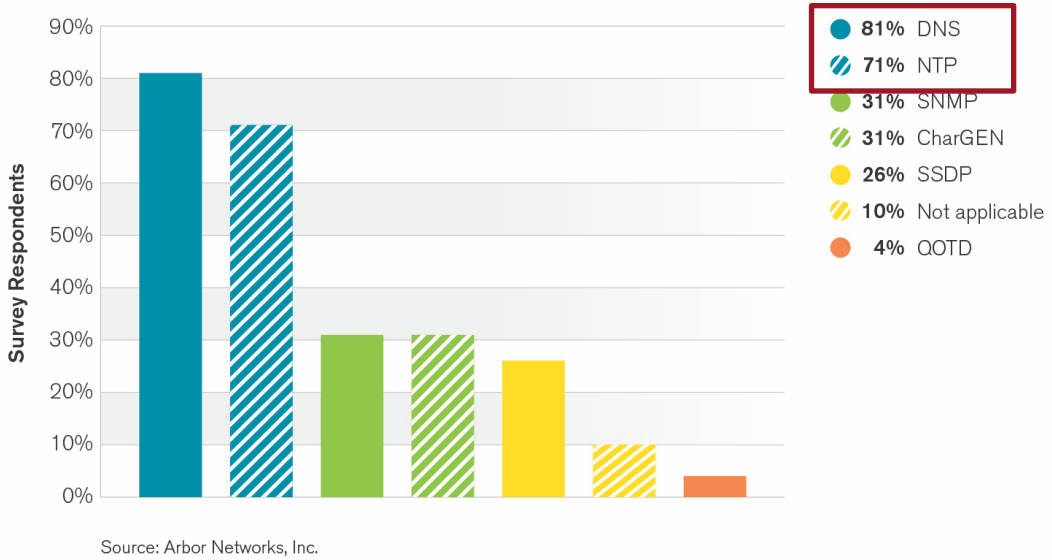
The hacking group
the Network Time P
attack; NTP is gene
synchronize comput
the correct local tim
the power of its DD
requests to the servers while pretending to be the gaming service th



by Michael Mimoso Follow @mike_mimoso January 14, 2014 , 12:45 pm

US-CERT has issued an advisory that warns enterprises about distributed denial of service attacks flooding networks with massive amounts of UDP traffic using publicly available network time protocol (NTP) servers.

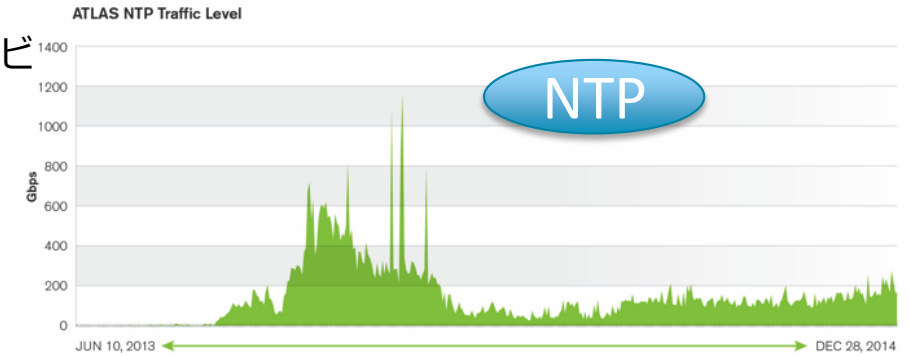
リフレクション/アンプ攻撃に使用されたサービス

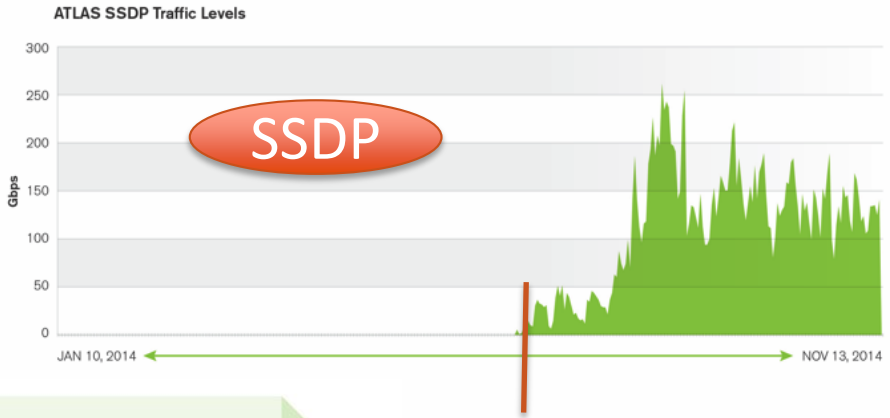


Source: Arbor Networks, Inc.

2014年はリフレクション攻撃の年でした…

- DNSは歴史的に反射・増幅攻撃に使われる主要のサービスでした
- NTPは2014年著しく広まりました
  - 100Gbps以上の攻撃が93回、200Gbps以上の攻撃は5回
- SSDPは7月以降著しく増えました
  - 25000回/月の攻撃が10,11,12月に観測されています
  - 最大は131Gbpsでした
- 他のプロトコルも依然として懸念されます





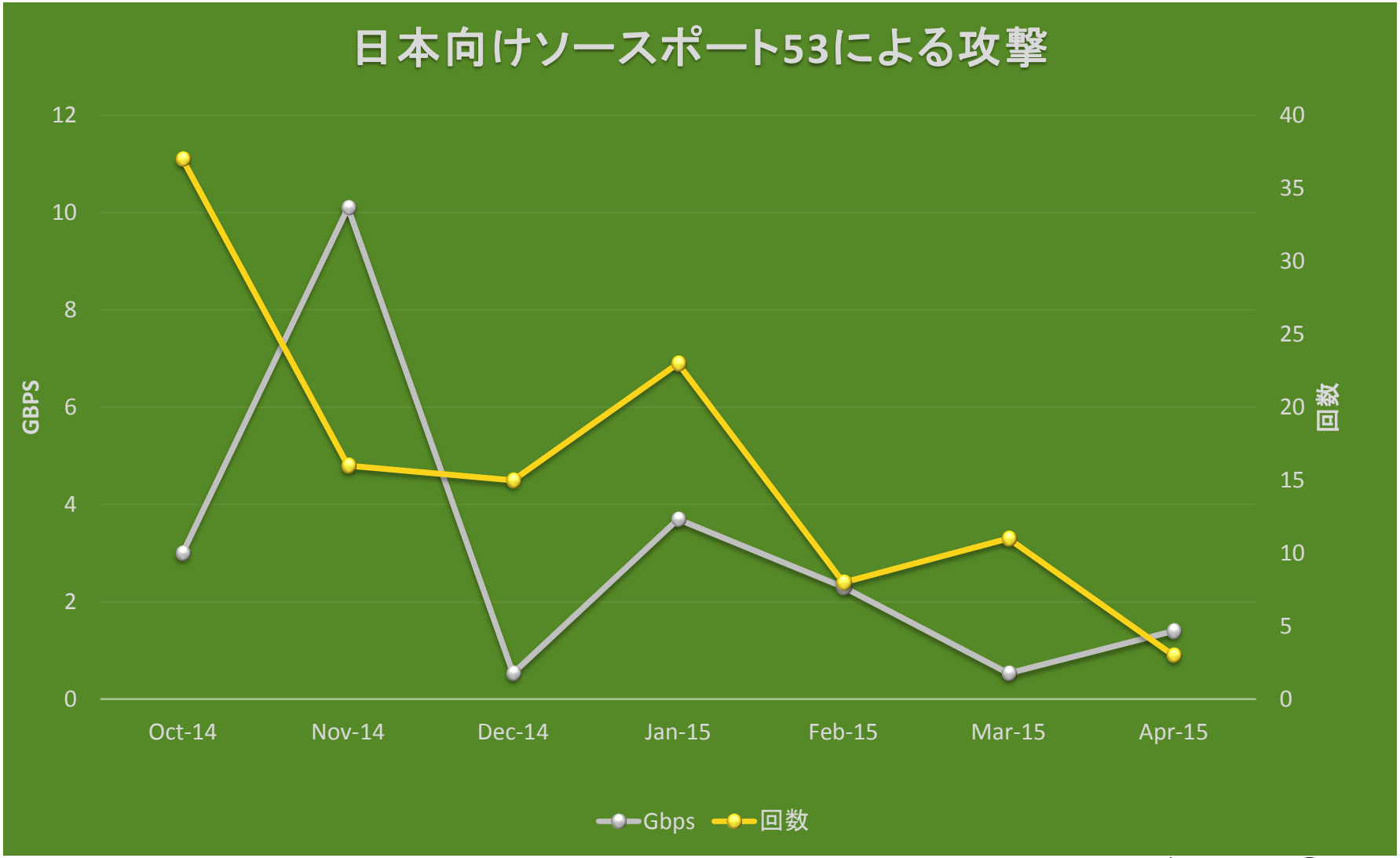
2014年7月

Exploited Protocols

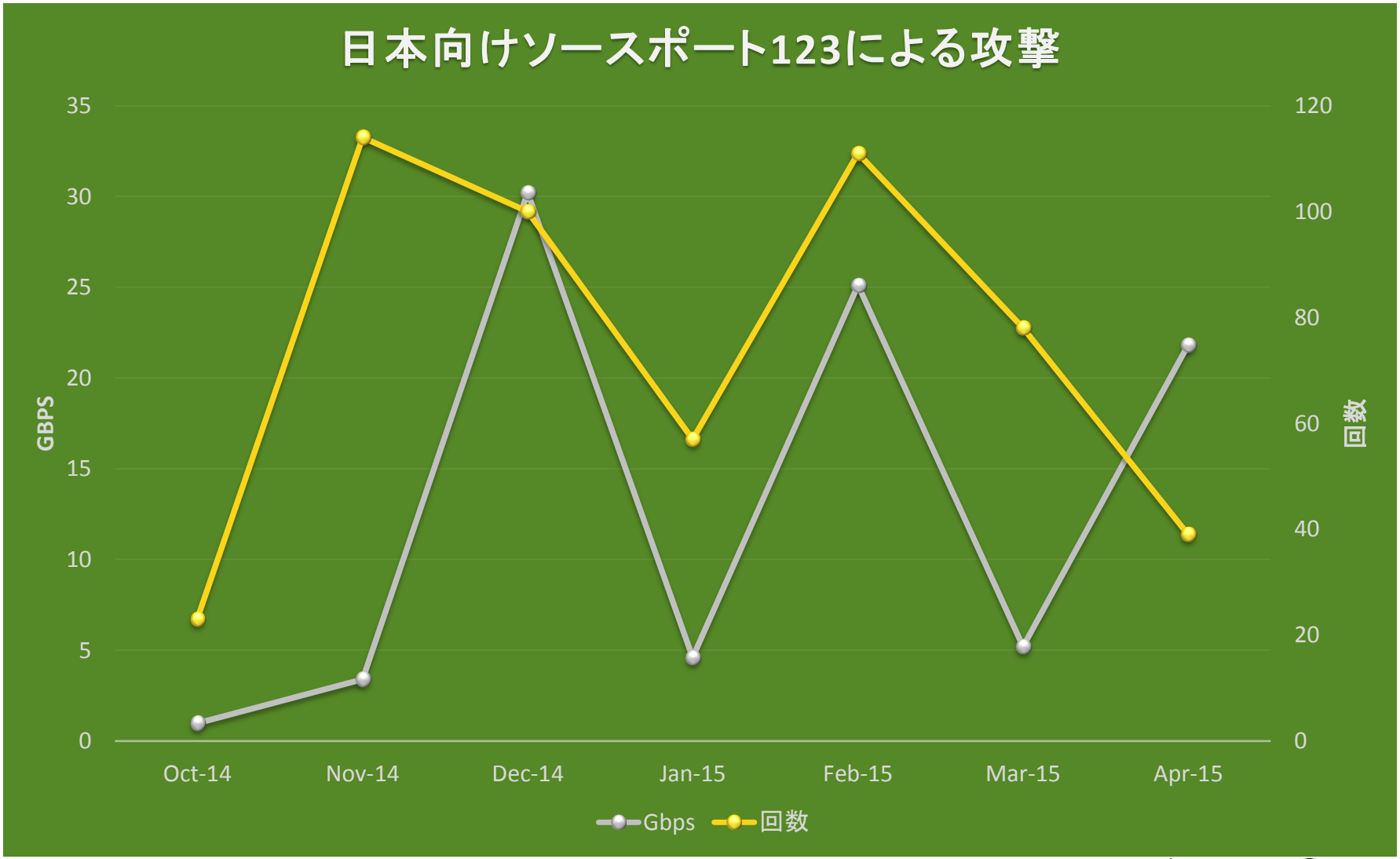
Protocol	Overall % Q1	Overall % Q2	Overall % Q3	Overall % Q4	Max Attack
DNS (53)	2%	4%	4%	Less than 1%	104.28 Gbps
NTP (123)	14%	6%	5%	7%	325.05 Gbps
SSDP (1900)	Less than 1%	Less than 1%	4%	9%	131.2 Gbps
SNMP (161)	Less than 1%	Less than 1%	Less than 1%	Less than 1%	18.61 Gbps
Chargen (19)	1%	1%	2%	1%	96.27 Gbps

ARBOR NETWORKS

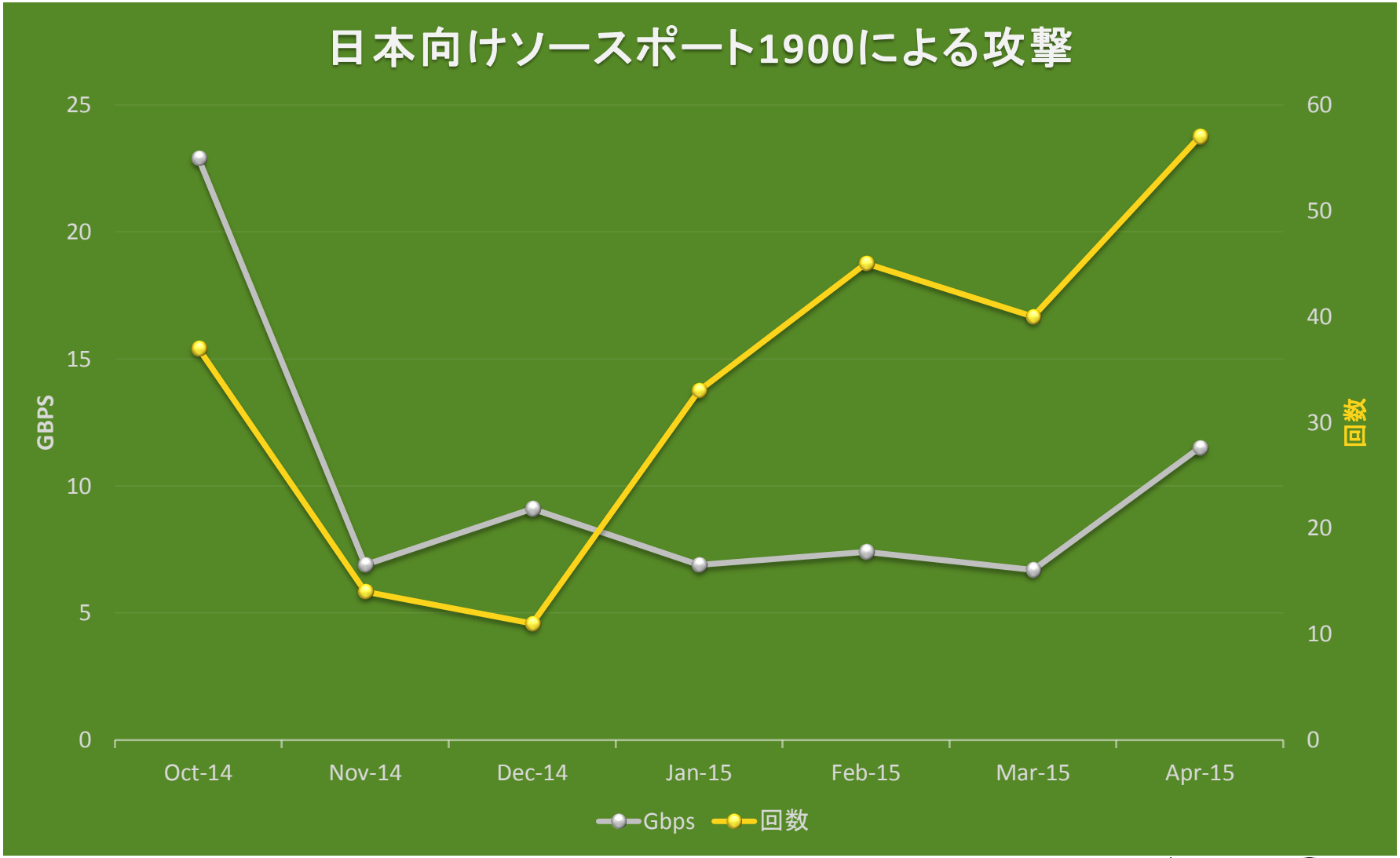
2014年はリフレクション攻撃の年でした…



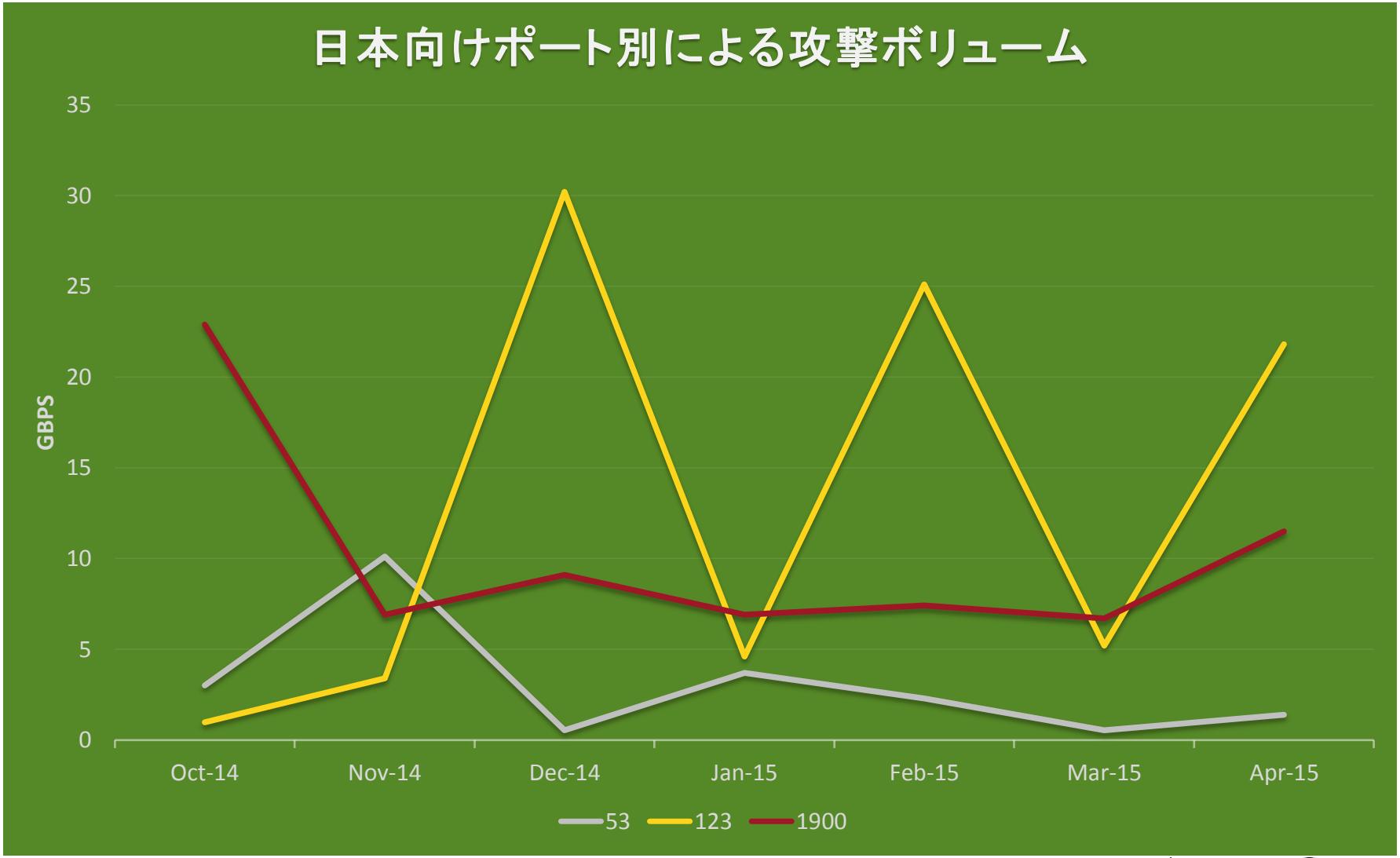
2014年はリフレクション攻撃の年でした…



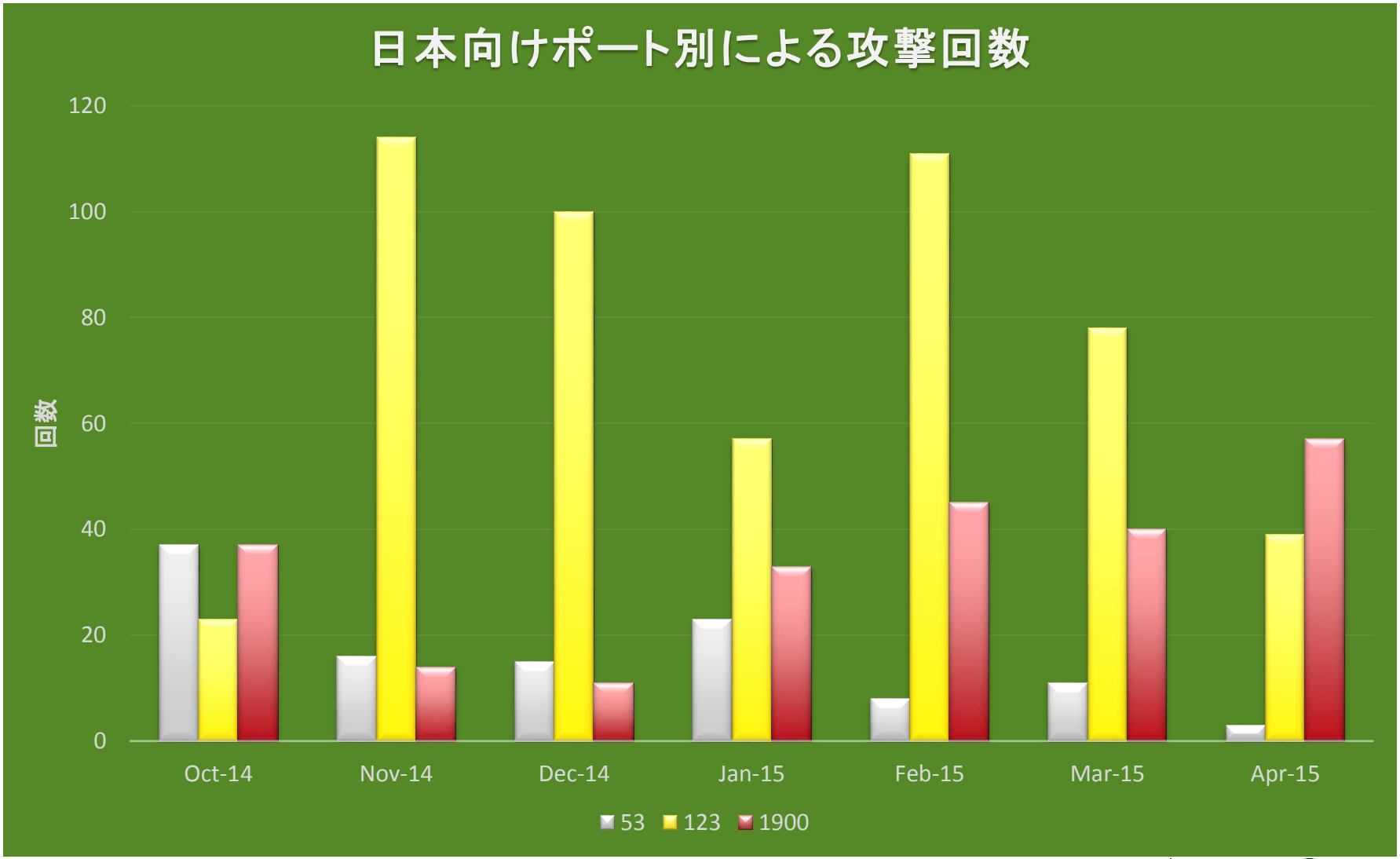
2014年はリフレクション攻撃の年でした…



2014年はリフレクション攻撃の年でした…

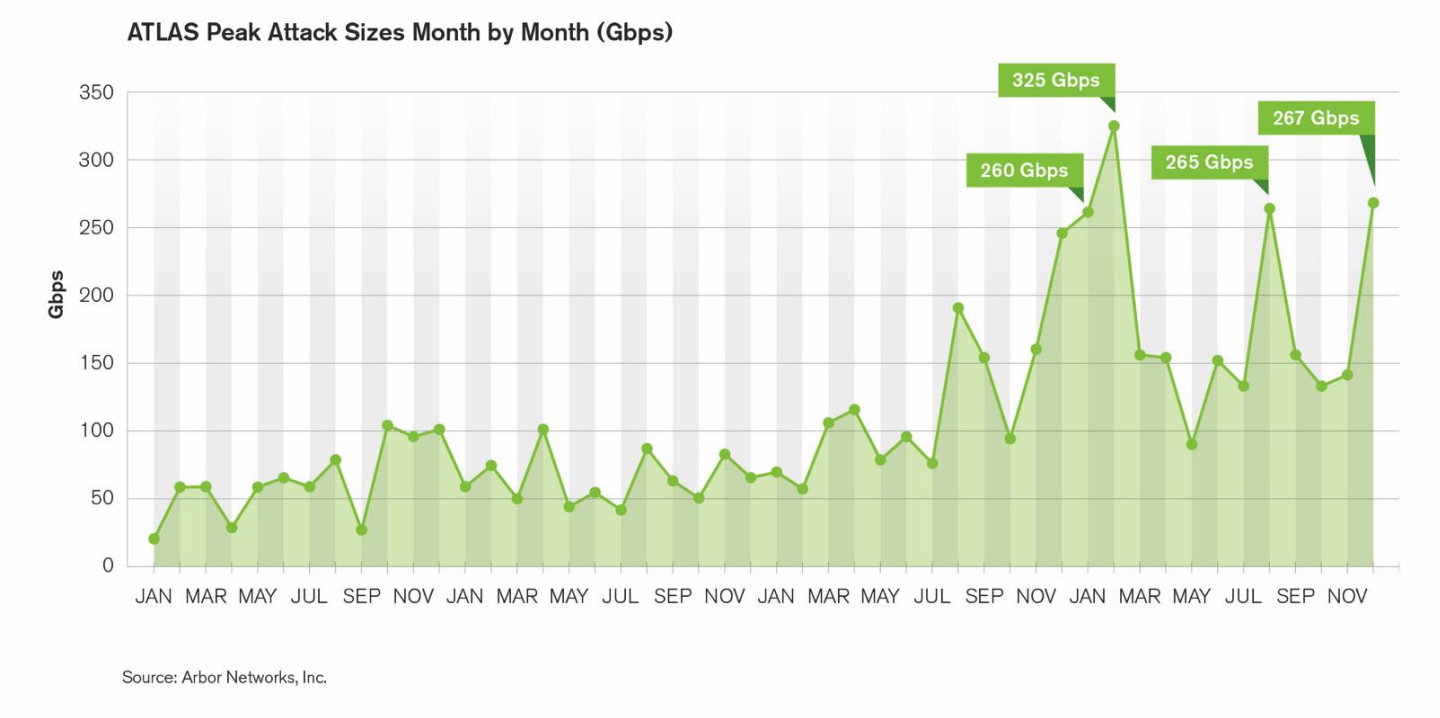


2014年はリフレクション攻撃の年でした…

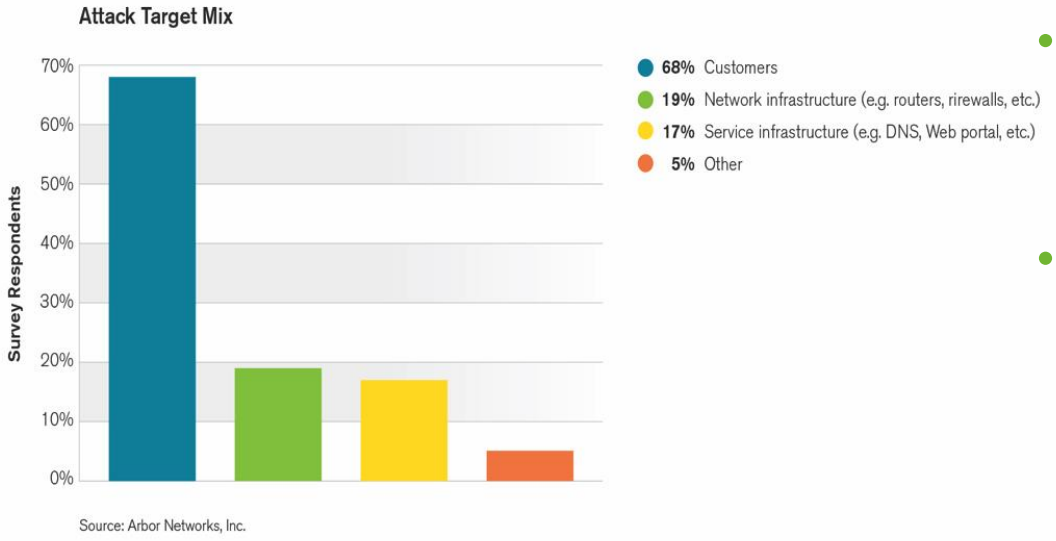


ATLAS – 前例の無い大容量の攻撃

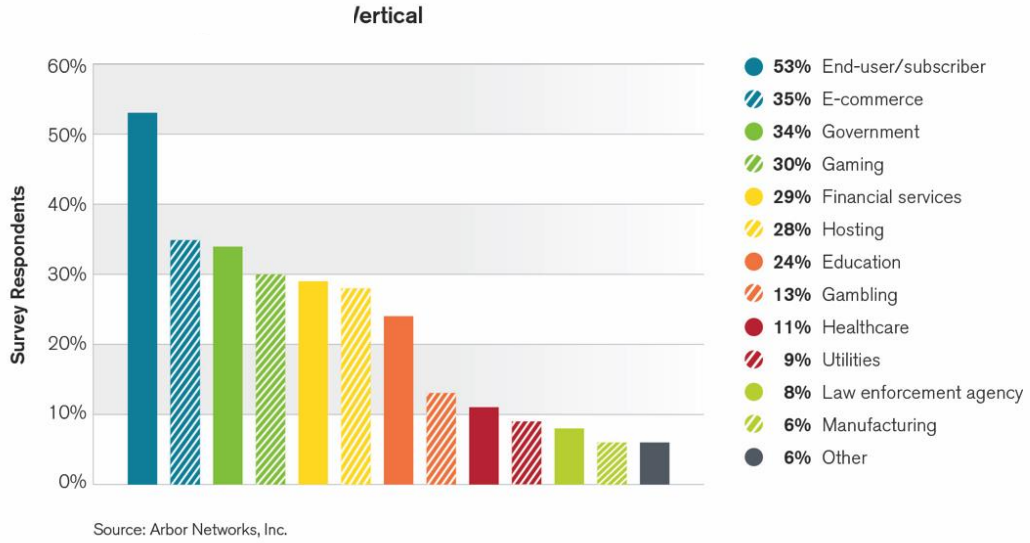
- 観測された最大の攻撃は325Gbpsで、前回と比較して32%上昇
  - 2014年1月、2月、8月、12月の最大の攻撃は、2013年の最大の攻撃より大きかった
- ATLASでは2013年と比較して、2014年は100Gbpsを超える攻撃を4倍以上観測



DDoS：攻撃対象

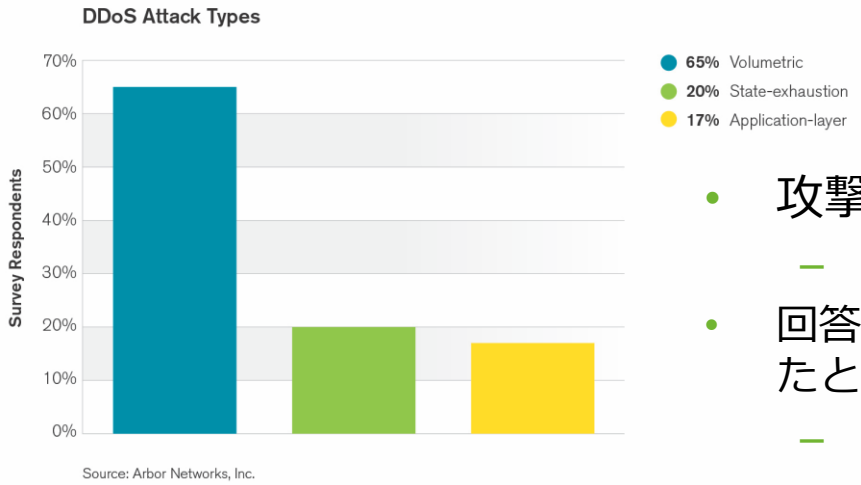


- 回答者の顧客がもっとも共通する攻撃のターゲット
- インフラに対する攻撃の割合は引き続き上昇しています



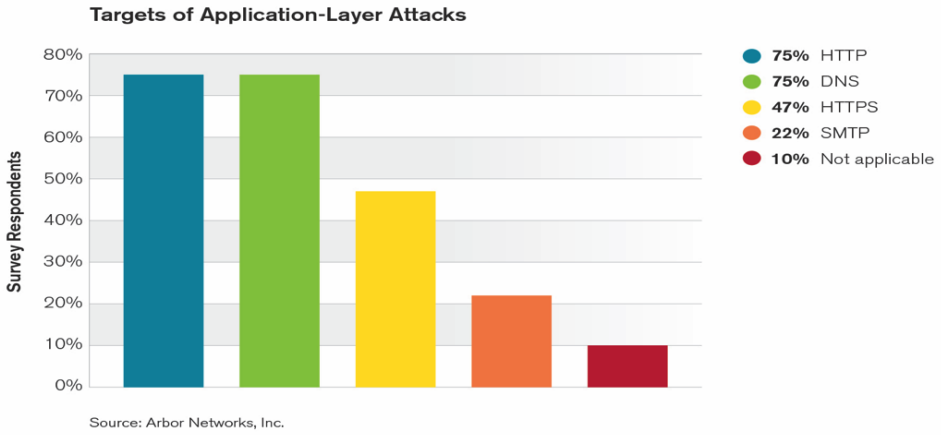
- 昨年と変わらず、エンドユーザーとイーコマースがトップ
- 金融関係は、官公庁、オンラインゲームに続き5位へ

DDoS：攻撃のタイプ

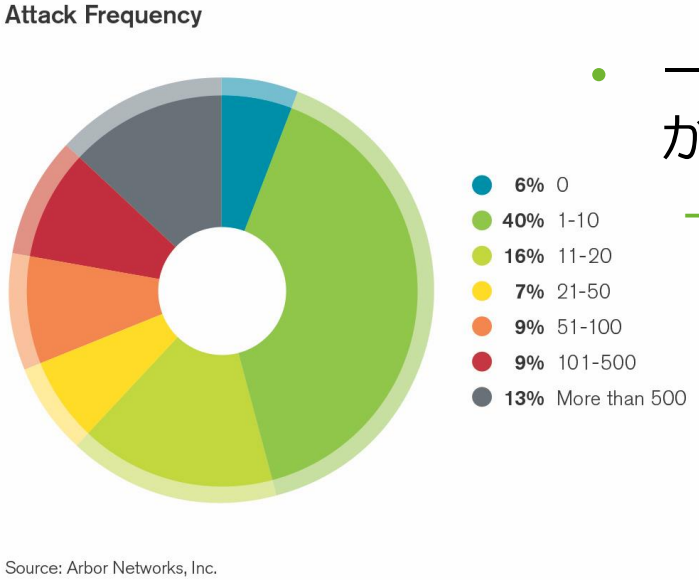


- 攻撃の65%はボリュームによる攻撃でやや上昇
  - リフレクション攻撃が多かったことによる
- 回答者の9割がアプリケーションレイヤー攻撃を受けたと回答
  - アプリケーションレイヤー攻撃の割合としては4%減少

- HTTPとDNSはアプリケーションレイヤー攻撃のトップ
- HTTPSに対する攻撃は、回答者の割合が低下



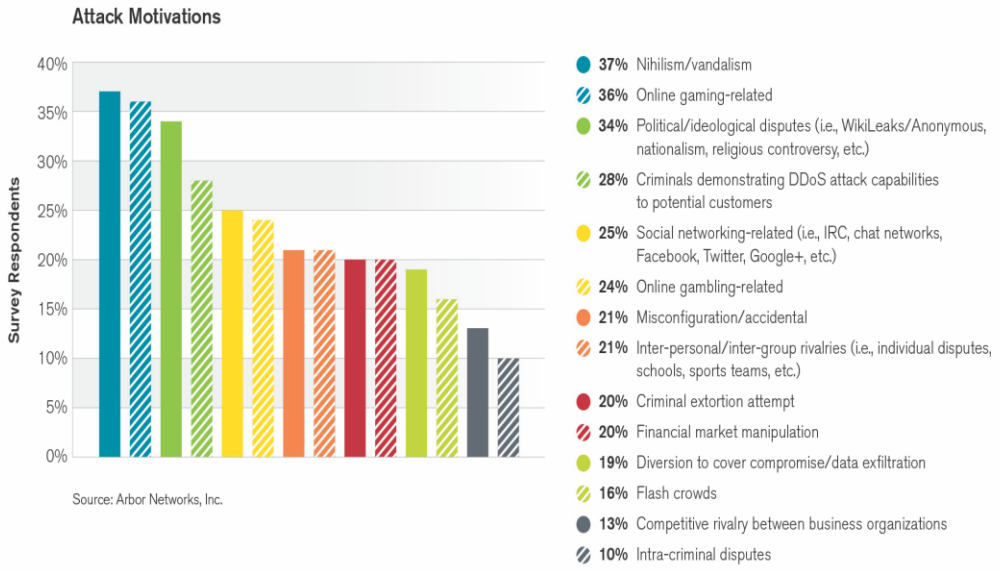
DDoS：動機と頻度



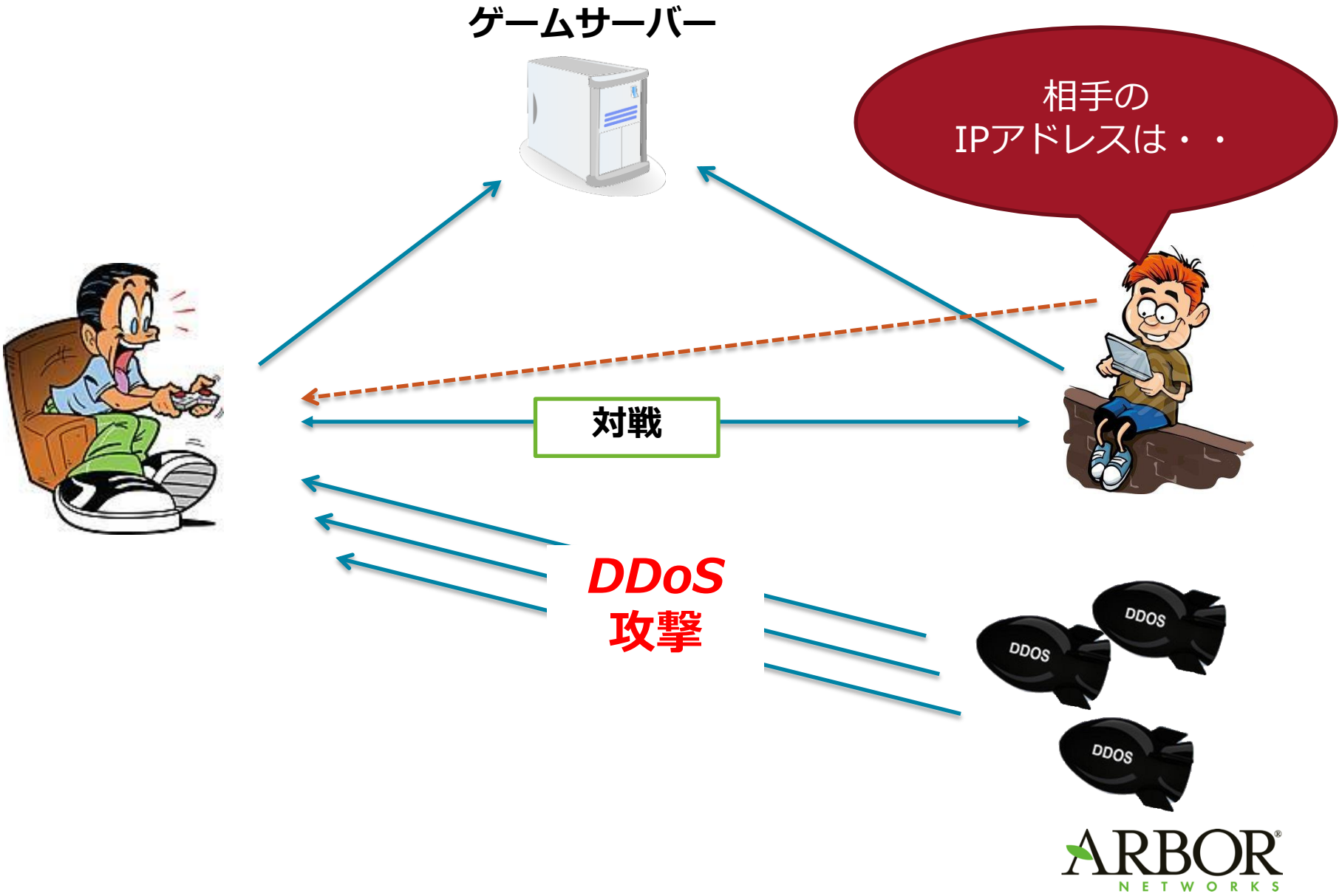
- 一ヶ月に21回以上攻撃を受けたという回答が著しく上昇
  - 今回　38%　前回　25%

- トップ3の攻撃の動機は前回と同じ
  - イデオロギー、ハクティビズム、社会的・政治的主義・主張、が主な要因

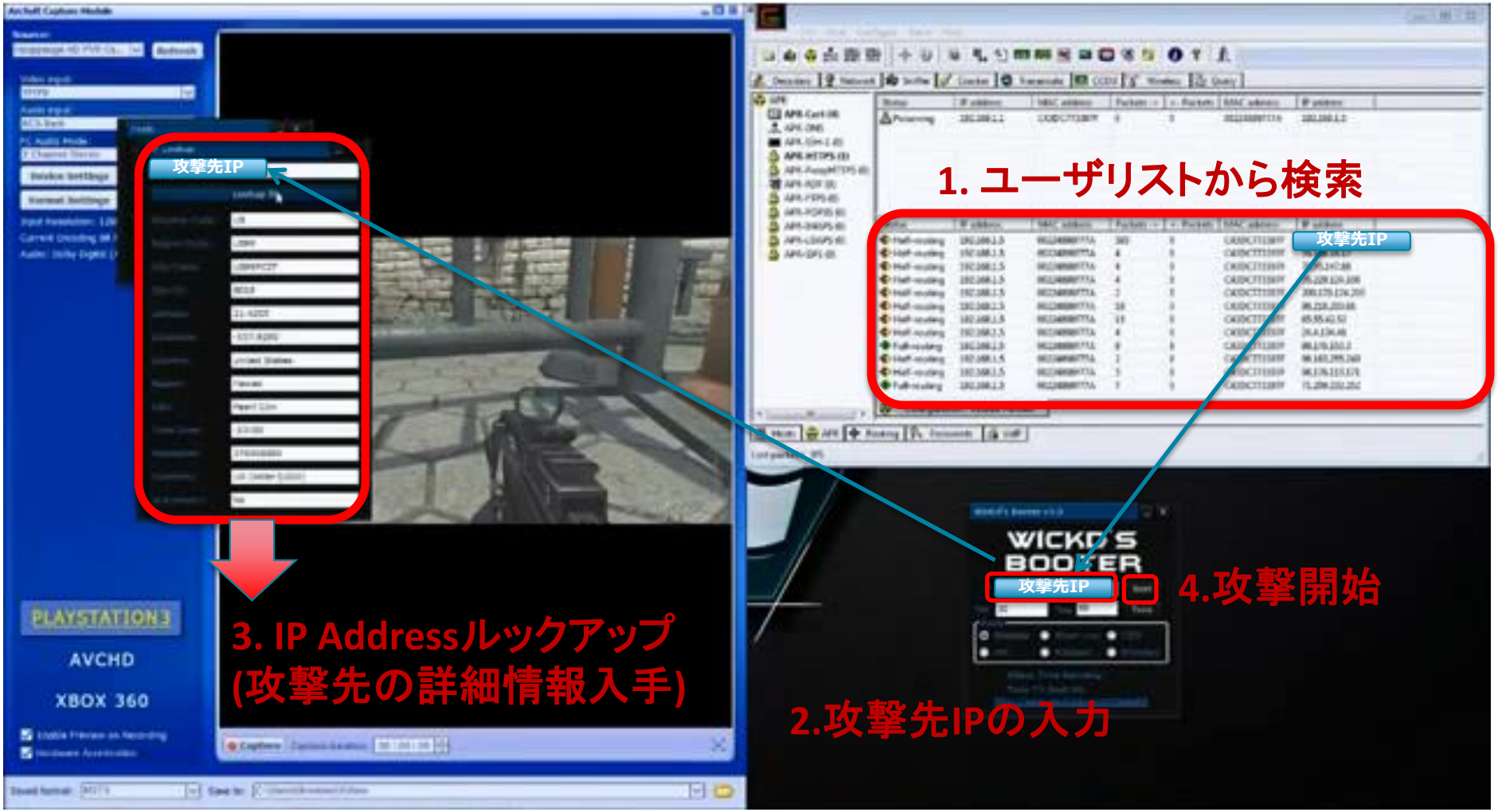
- ゆすりや、市場操作、偽装工作を動機とする攻撃は引き続き上昇しています



オンラインゲームでのDDoS攻撃



オンラインゲームでのDDoS攻撃



Mt.Gox (2013年4月)

◎攻撃の対象

電子通貨 (ビットコイン) の世界最大の取り引きサイト

◎攻撃による影響

1BTCの価値が急騰したタイミングで攻撃が発生し取引を12時間停止させた。攻撃後、価値は1/5の50ドルまで下落した。

Mt.Gox (2013年4月)

◎攻撃の特徴

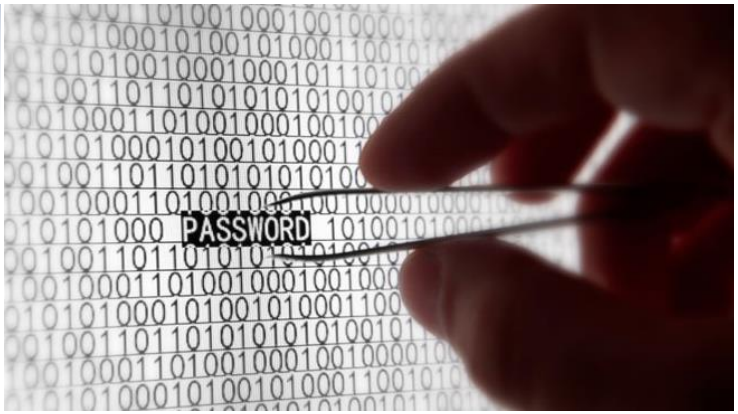
DDoS攻撃と同時期にハッキングの被害も受ける。
データベースに不正にアクセスされBitcoinの財布を扱うサービスを無期限で停止する。

April 4th, 2013, 10:55 GMT · By Eduard Kovacs

Instawallet Hacked, Mt. Gox Hit by Major DDOS Attack

In wake of Bitcoin spike, Instawallet halts service and Mt. Gox "eats" DDOS

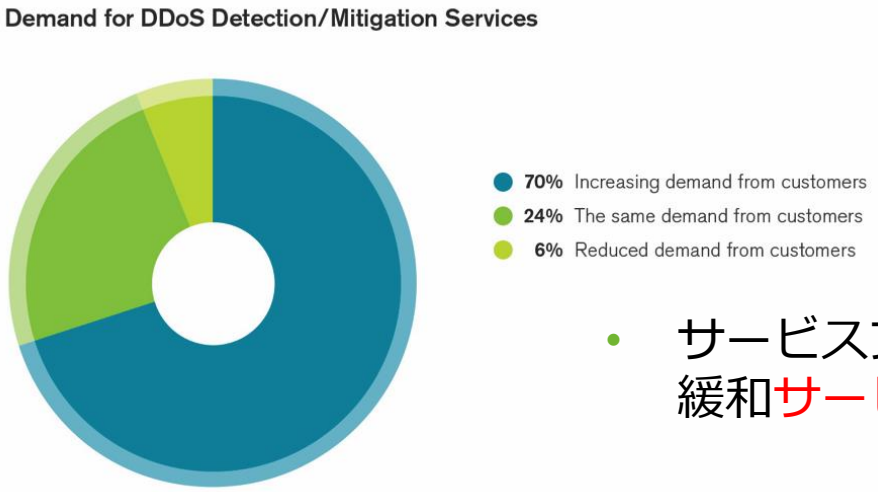
Instawallet will reimburse accounts with less than 50 BTC—good luck if you're over.



◎攻撃内容

「"Layer7"のDDoS攻撃を受け、正当なトラフィックと悪意のあるトラフィックか見分けることが困難だった」と同社はコメントを残している。

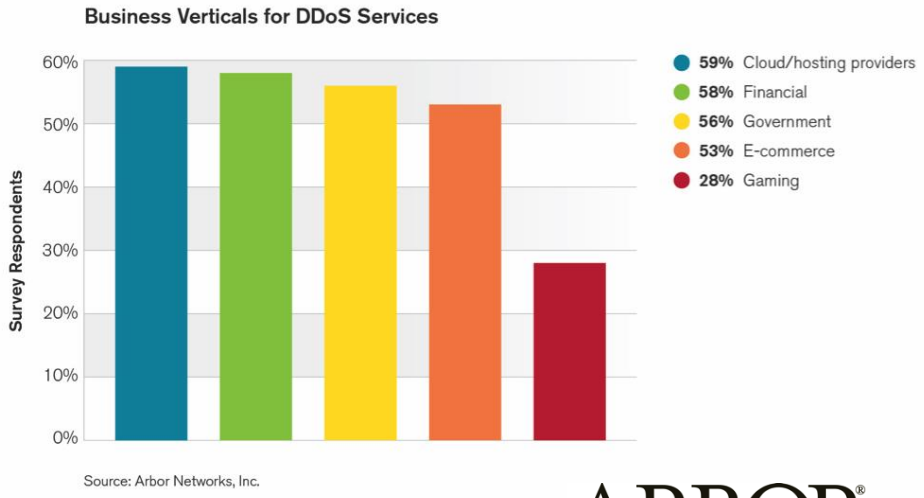
DDoS：ISPの顧客にとって必要なもの



Source: Arbor Networks, Inc.

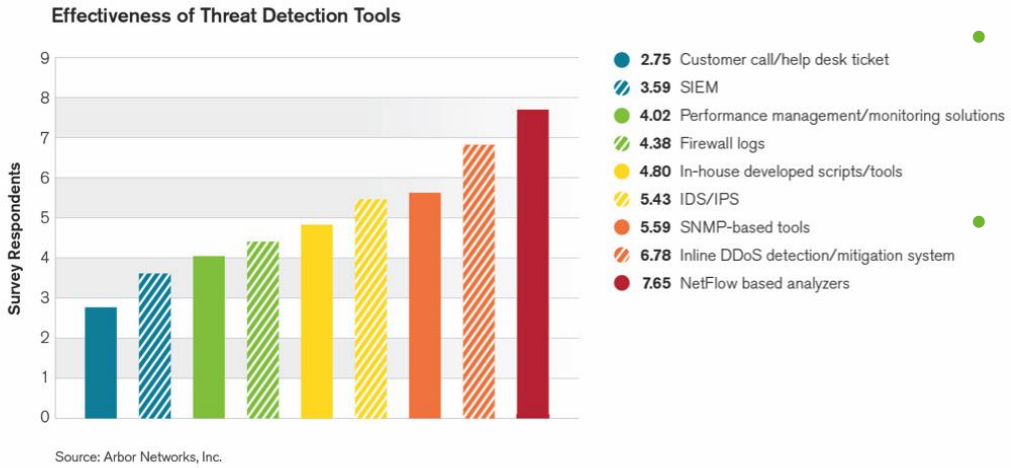
- サービスプロバイダの70%は顧客からDDoSの検知・緩和サービスについての要望が増えていると回答

- クラウド・ホスティングプロバイダーがDDoSサービスを最も意識している
  - クラウドに向けられた攻撃が、前回19%に対し29%に上昇していることにも裏付けられる）
- 金融関係、官公庁、イーコマースも同様



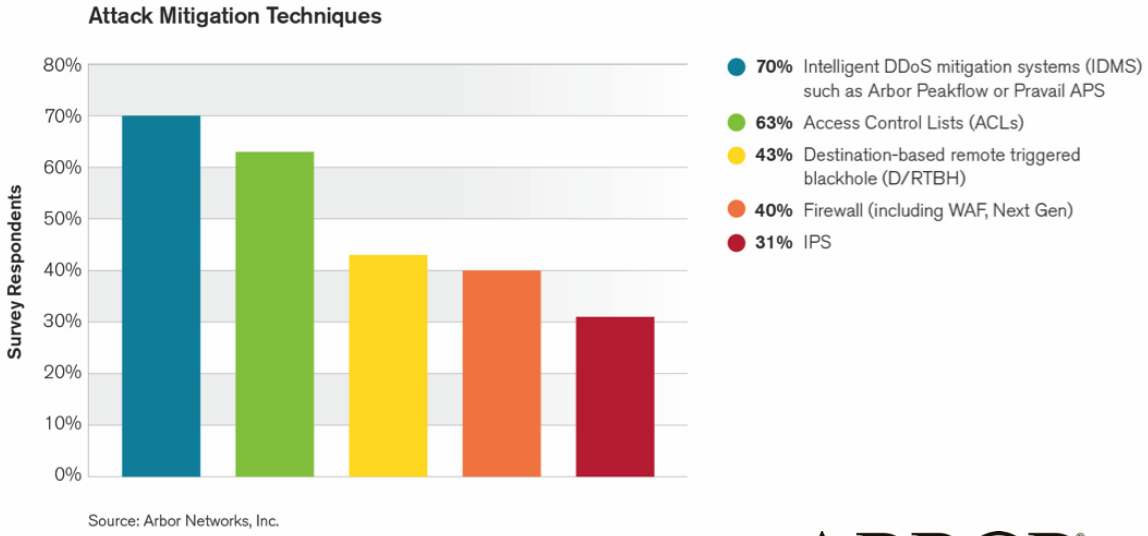
Source: Arbor Networks, Inc.

ISPでの脅威の検知と緩和

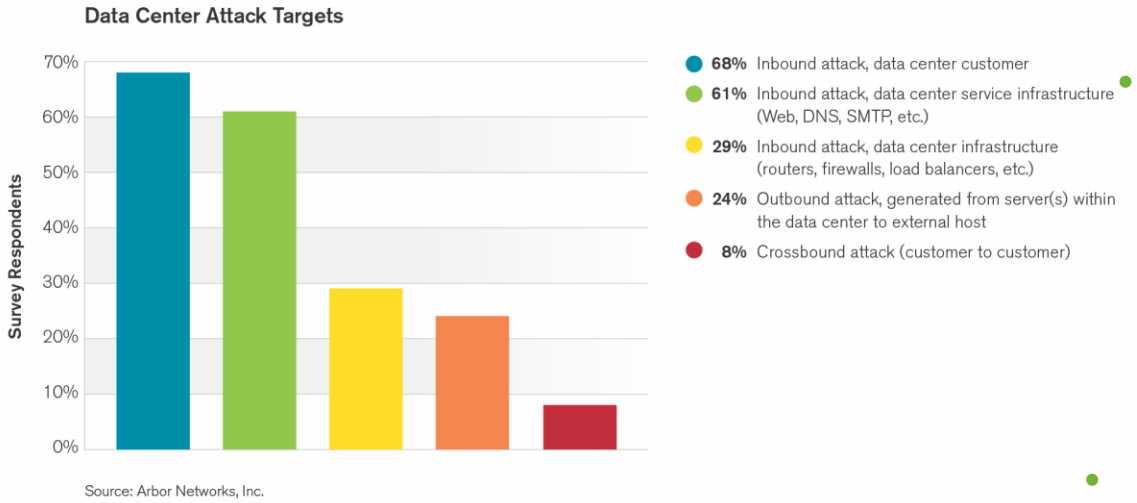


- NetFlowによる解析が最も効果的で、かつ最も一般的に導入されている脅威の検知方式
- ファイヤーウォールは2番目に多く導入されている脅威検知方式であるにも関わらず、有効性という視点では6位

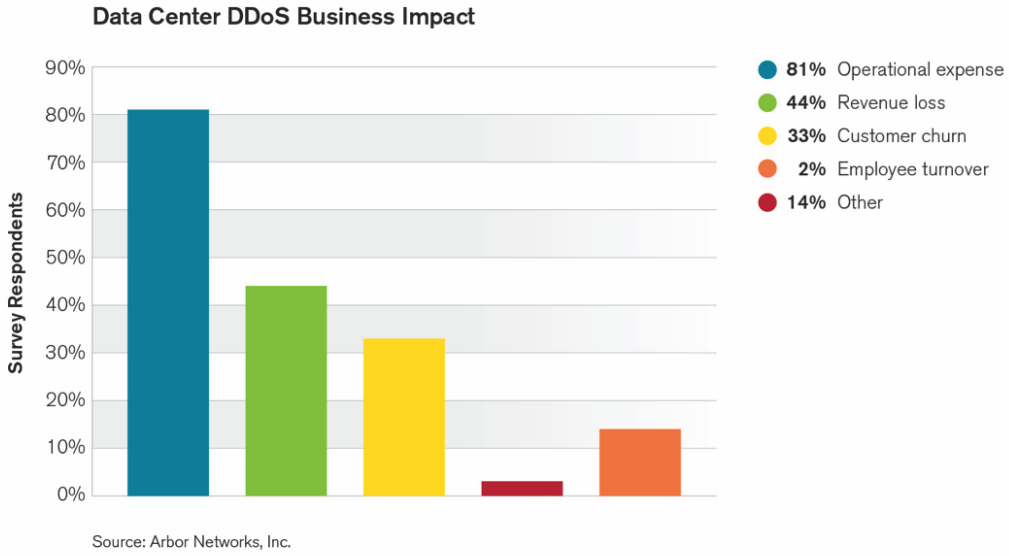
- IDMSがACLを超え、最も一般的な緩和方式に
- ファイヤーウォールは今回さらに順位をさげました
- 20分以内に緩和動作を行える回答者の割合が、60%に増えました



データセンターにおけるDDoS攻撃とその影響

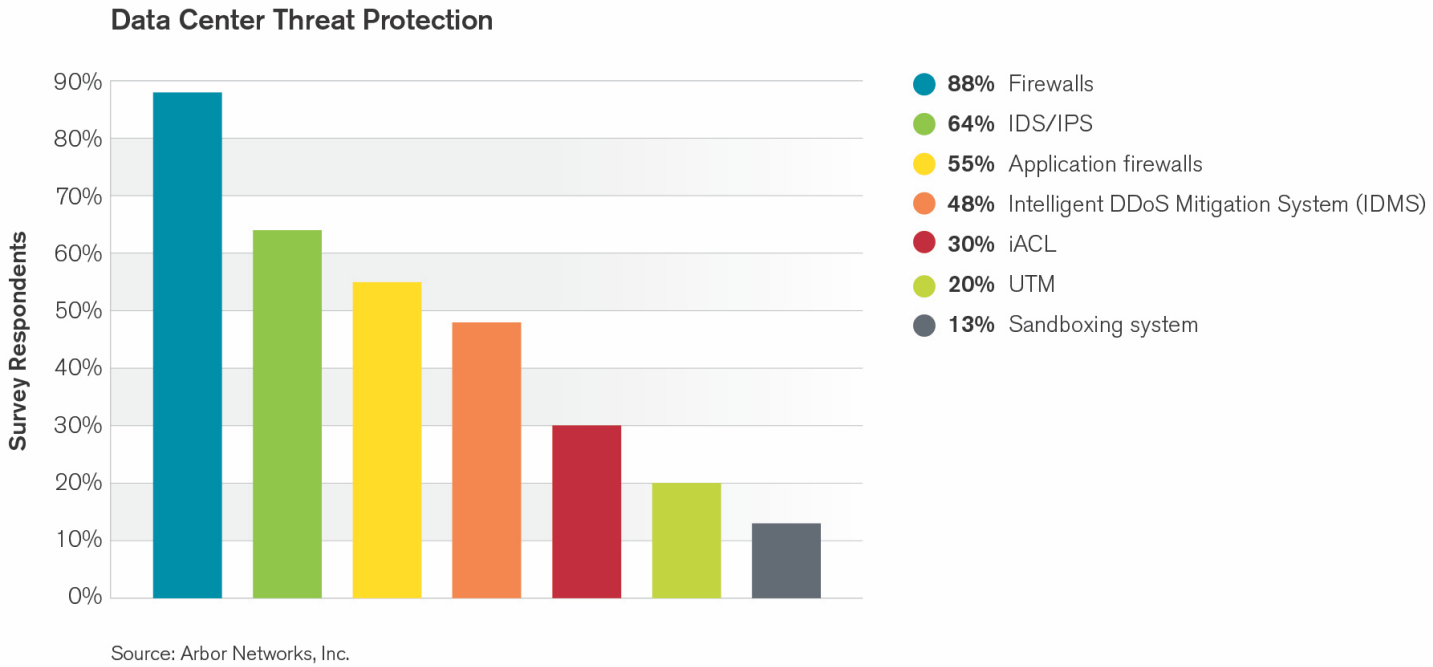


- 最も共通する攻撃対象は、インフラより現状では顧客になっている



- 前回同様38%は攻撃がインターネット帯域に達することを経験
- 昨年は81%が運用経費がビジネス上の最大の問題としている
- 売り上げ損失の割合が、前回と比較し27%から44%へと大きく上昇

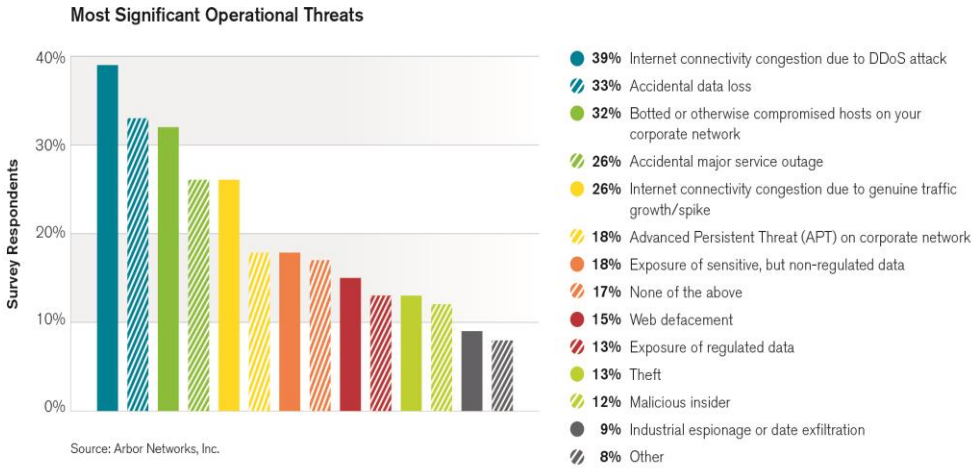
データセンタの保護



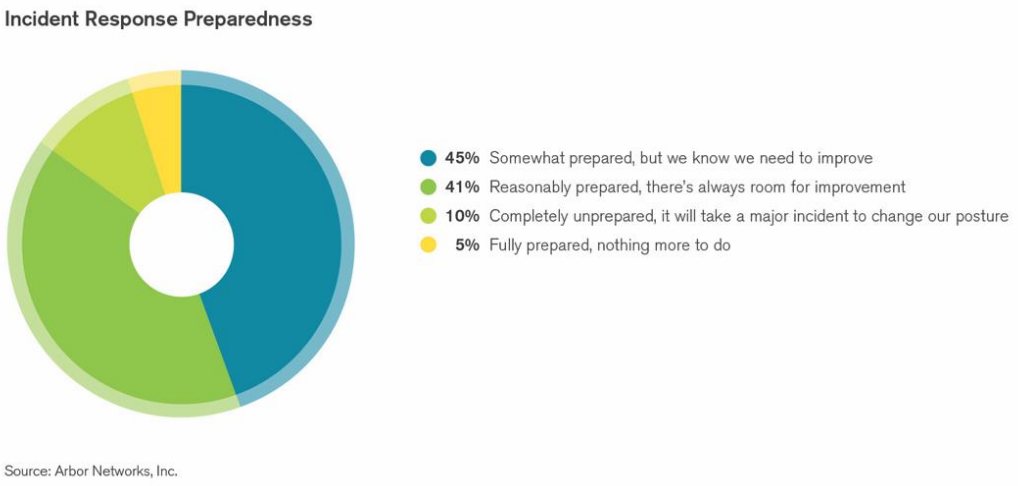
- ファイヤーウォール、IDS/IPS、アプリケーションファイヤーウォールが依然トップ3の導入されているセキュリティ技術
- IDMSが6%から48%へ、又ACLが13%から30%へ大きく上昇
- 49%がDDoSの為にファイヤーウォールがダウンしたと回答
- 37%が標準又はオプションとしてDDoS防御サービスを提供し、21%は多段でのサービスも提供

企業・官公庁・教育機関
ネットワークの脅威とインシデントレスポンス

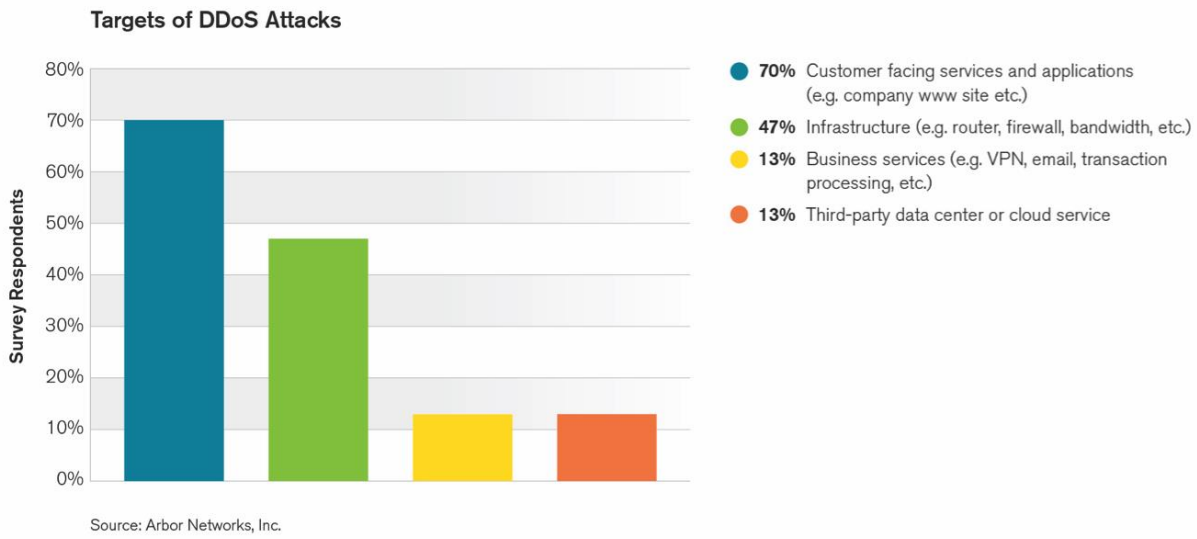
- 脅威のトップ: DDoS攻撃、偶発的なデータ損失、ボット化したホスト
  - ISPも企業ネットワークが、最も脅威であるDDoSによって帯域が輻輳したことを報告



- 20%近い回答者がAPTを経験
  - 翌年に向け半分以上の回答者が懸念を示しています
- 組織の10%がインシデントの取り扱いに全く準備できていないと回答
- 回答者の半分以上が準備中の状況



企業から見たDDoS攻撃

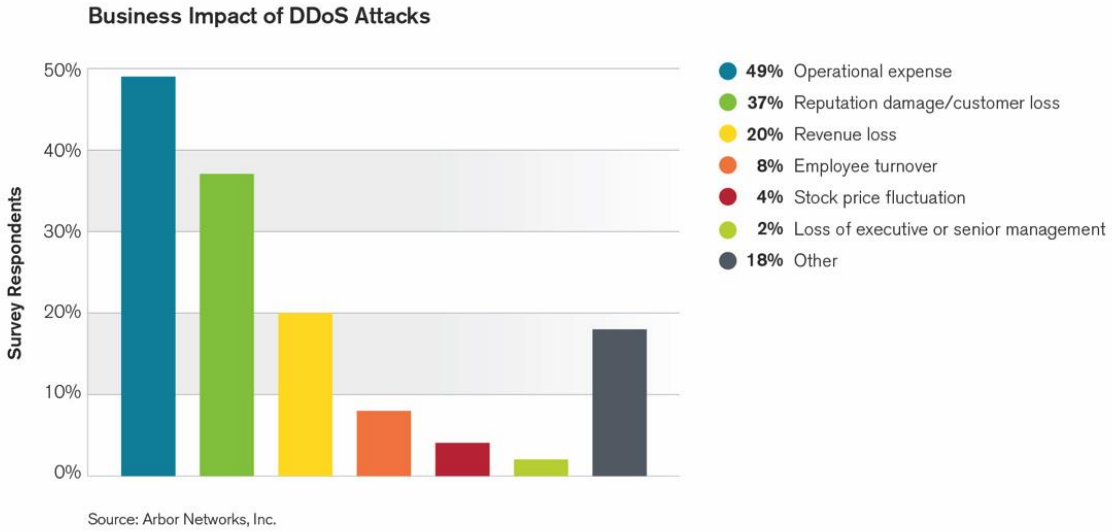


回答者の半分近くが攻撃を受け、うち40%はインターネット接続が飽和

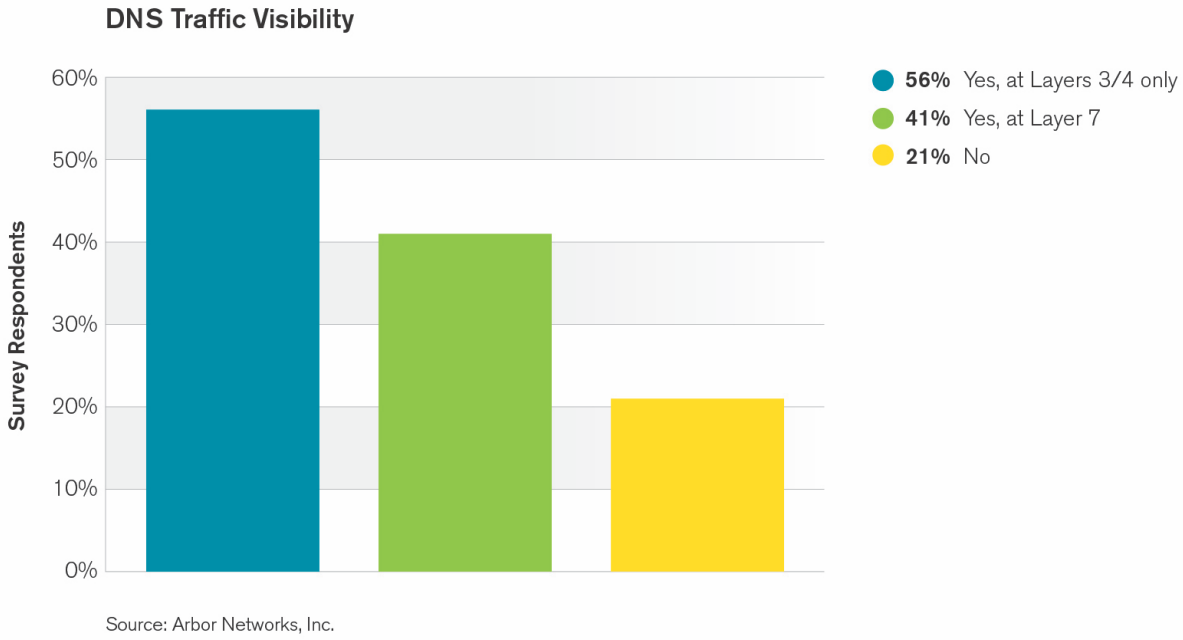
攻撃対象の29%はアプリケーションレイヤー

- 81% HTTP
- 58% DNS, 57% HTTPS

- DDoSにより33%以上がファイヤーウォールのダウンを経験
- 運用経費、信用損失、収益減がビジネスにおける最も大きな影響

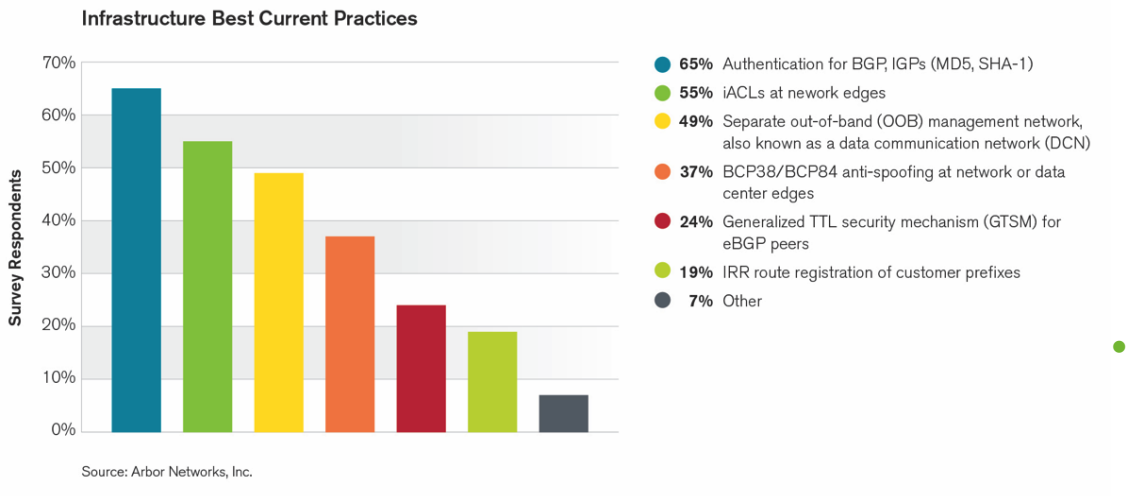


DNSは依然セキュリティ対策がされていません

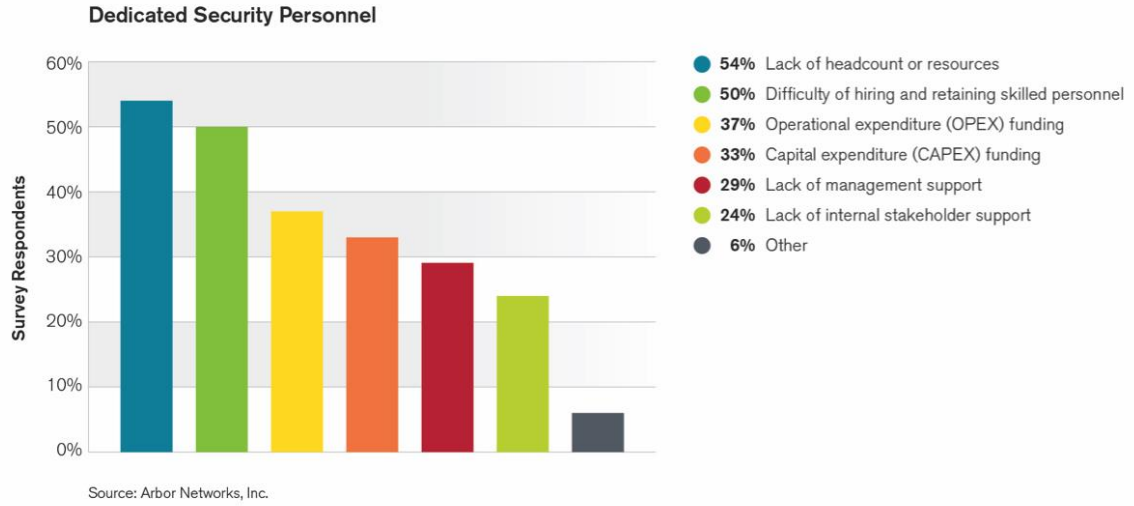


- DNSに対し正式な責任を持つセキュリティグループがないとした回答者は、引き続き上昇し33%に達しています
- 回答者の17%がDDoSによって顧客が影響を受けたとし、これは前回の36%から減少しています
  - 攻撃者は他のプロトコルへ関心を持ち始めています
- レイヤー7の視認性は41%となり前回の37%、2012年の27%から改善されています

BCP（現時点における最善の実践）



- IP詐称防止（BCP38/84)を導入している回答者の割合が減少しています
  - リフレクション攻撃に対して大きな懸念となっています
- DDoS防御をトレーニングしている割合は引き続き減少しています

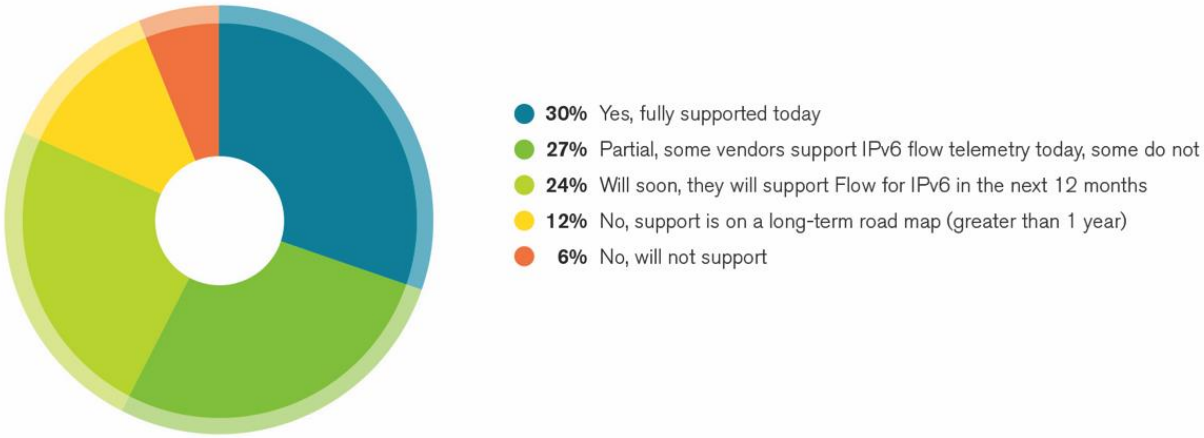


回答者の94%は専任のセキュリティリソースを確保

組織に対する課題は、立ち上げたチームをそのまま継続すること（新規雇用、雇用保持をすることが大きな問題）

IPv6はまだ幅広く普及していない・・・

IPv6 Flow Telemetry



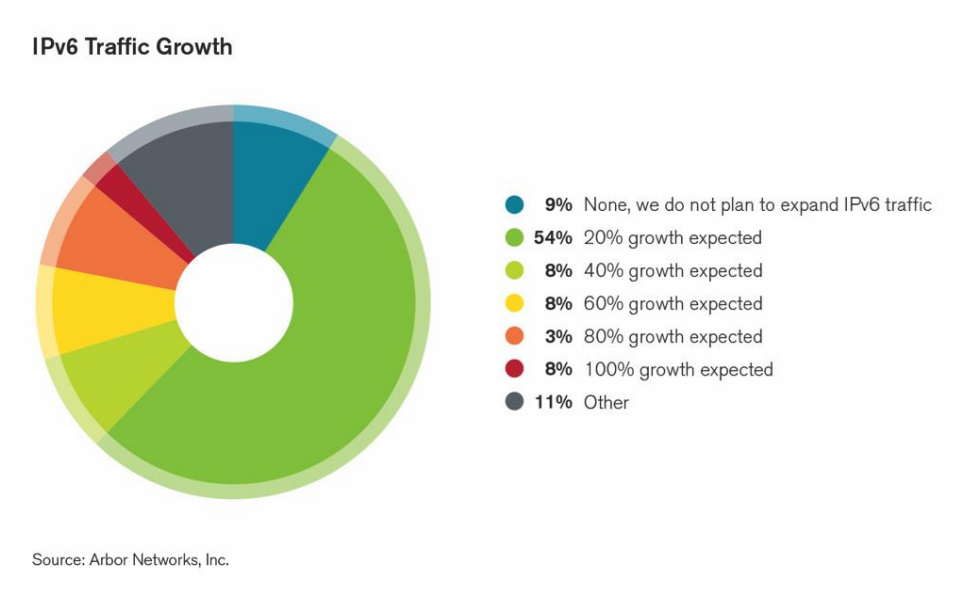
Source: Arbor Networks, Inc.

IPv6 Visibility

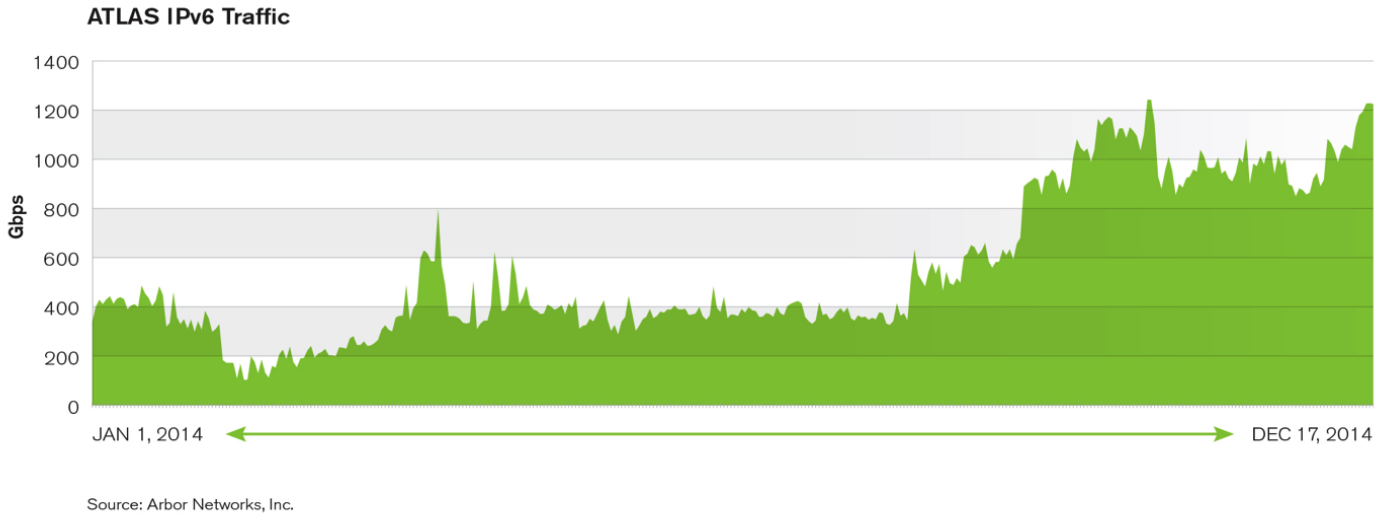
Source: Arbor Networks, Inc.

- サービスプロバイダーの回答者の66%以上はIPv6を導入しているが、企業・官公庁・教育機関では33%のみがIPv6を導入していると回答
- サービスプロバイダの75%近くがIPv6サービスを利用している加入者を持っていると回答しているが、IPv6サービスの利用率加入者と企業ユーザー含めてまだ25%以下

IPv6 の普及に対する期待と実態

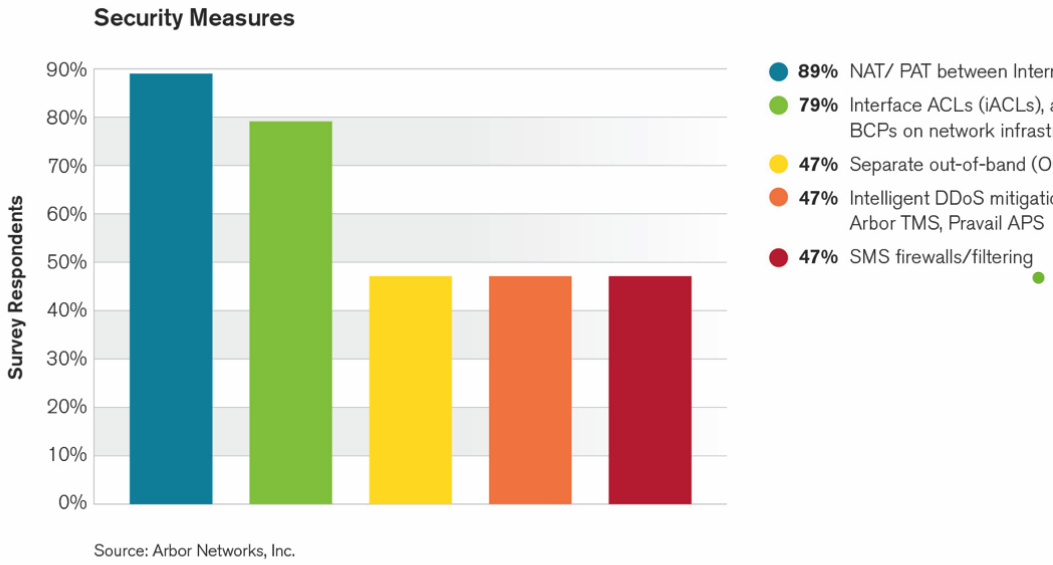


- IPv6トラフィックの報告された最大の通信ボリュームは80Gbpsで前回（20Gbps)から4倍の上昇
- ATLASではネイティブIPv6トラフィックが約3倍に増えた事を確認し、そのときのピークは1.24Tbpsに達しています



モバイル・セキュリティ

- 回答者の17%は加入者がセキュリティによる問題で通信できなくなったことを経験しています
- 回答者の75%は加入者の不正アクセス（マルウェア感染）をネットワーク上で検知することができません
- MNOsでは依然としてiACL/NAT/PATがiACLs最も一般的な防御方法として用いられているものの、その他の技術についても大きく上昇しています



36%の回答者が不完全な実装によるモバイルアプリケーションがサービスに影響を与えた事を経験しています

まとめ

- アーバーネットワークスは10年間にわたりWISRの取り纏めを行ってきました。そしていくつかの大きな変化が起きています
  - ネットワークの使い方が変わり、ネットワークも変わりました
  - 回答者が大きく増えました
  - 多種多様な回答者構成
  - 幅広い質問内容

- WISRはOpSecコミュニティでの所見、経験、及び懸念に対する非常に価値のある財産となります
  - 進行しているトレンドの見極め
  - 予期しない振る舞いの変化

- 目的は変わりません
  - 幅広いコミュニティへの支援
  - 共通の問題に対する解決策の共有

Agenda

会社紹介

セキュリティレポートサマリー

アーバーネットワークスのソリューション

アーバーネットワークスのソリューション

大規模ネットワークのモニタリング

企業ネットワークのモニタリング

Peakflow SP

DDoS防御

Pravail NSI

インターネット

Pravail APS

企業ネットワーク/
データセンター

不正アクセス遮断

Peakflow TMS

Pravail SA

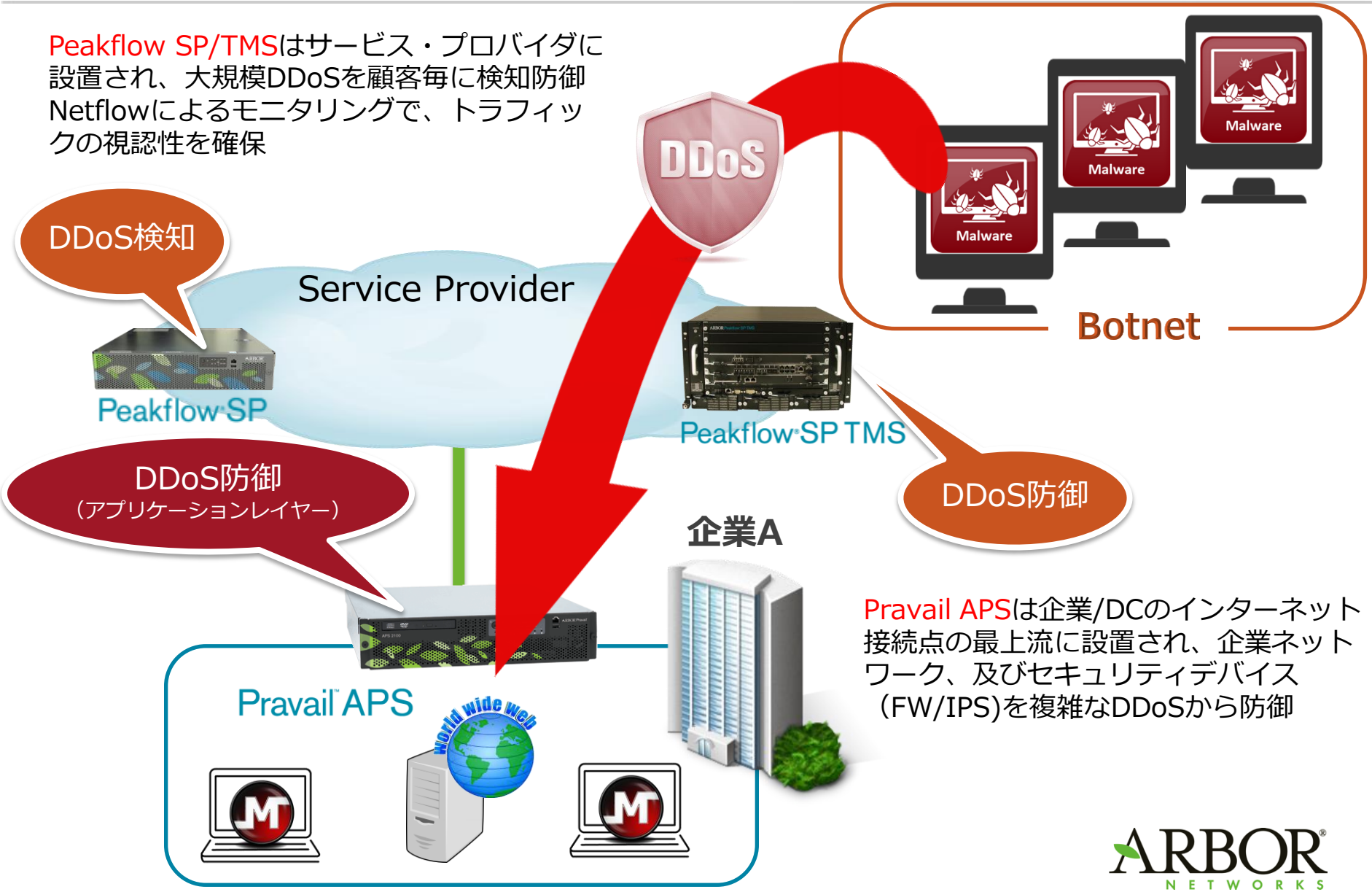
DDoS攻撃・検知/防御

APT/高度な攻撃・マルウェア感染・
ゼロディ攻撃検知・対策

ARBOR NETWORKS

DDoS攻撃対策ソリューション

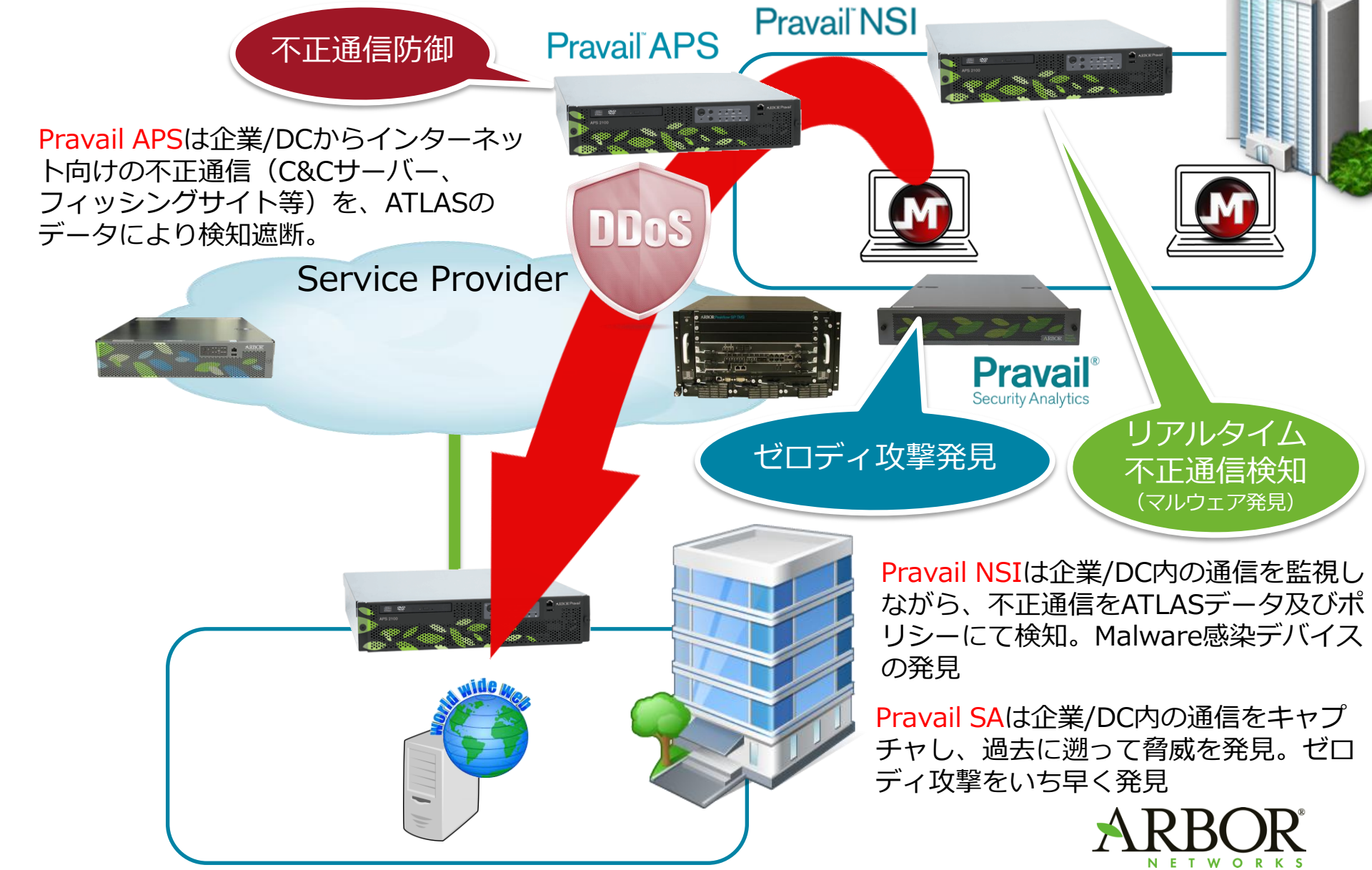
Peakflow SP/TMSはサービス・プロバイダに設置され、大規模DDoSを顧客毎に検知防御
Netflowによるモニタリングで、トラフィックの視認性を確保



Pravail APSは企業/DCのインターネット接続点の最上流に設置され、企業ネットワーク、及びセキュリティデバイス（FW/IPS)を複雑なDDoSから防御

高度な脅威検知・対策ソリューション

企業A



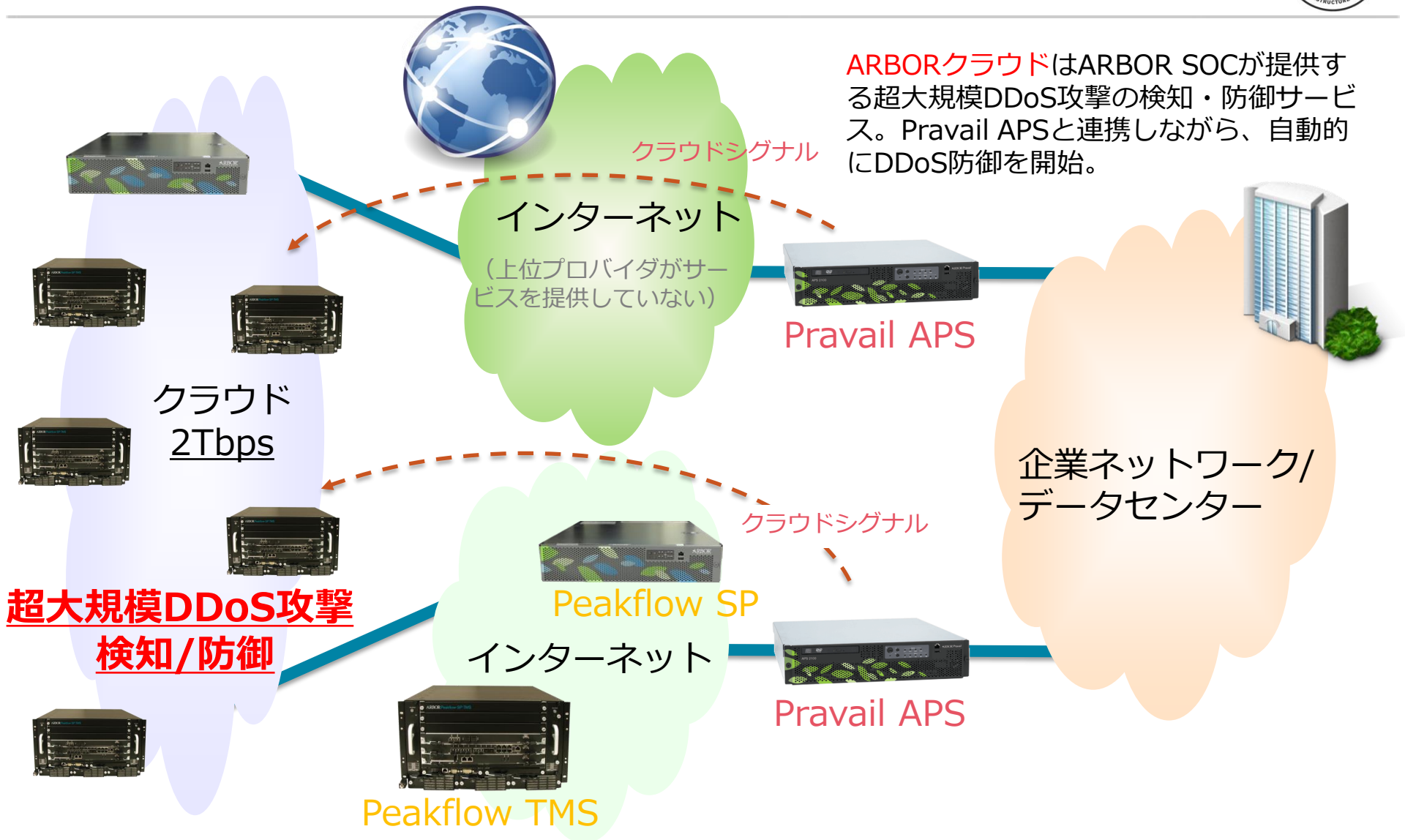
Pravail APSは企業/DCからインターネット向けの不正通信（C&Cサーバー、フィッシングサイト等）を、ATLASのデータにより検知遮断。

Pravail NSIは企業/DC内の通信を監視しながら、不正通信をATLASデータ及びポリシーにて検知。Malware感染デバイスの発見

Pravail SAは企業/DC内の通信をキャプチャし、過去に遡って脅威を発見。ゼロディ攻撃をいち早く発見

ARBOR NETWORKS

超大規模DDoS攻撃対策ソリューション



ご清聴ありがとうございました

お問い合わせ
Arbor Networks
電話：03-3525-8040
Email：japan@arbor.net