NETSCOUT

狙われる日本、実データから推測する サイバー攻撃

２０１９年１２月９日（月）

ネットスカウトシステムズ株式会社
シニアシステムズエンジニア
藤原哲士（フジワラサトシ）

アジェンダ

- 日本と世界のサイバー脅威の比較
- DDoS攻撃とその被害
- 過去の国際イベントでのDDoS攻撃
- 直近の日本におけるDDoS攻撃と想定される手法
- DDoS攻撃への対処方法
- ネットスカウトシステムズのデータ分析の紹介（ATLAS）

NETSCOUT

日本と世界のサイバー脅威の比較

日本と世界のサイバー脅威状況

2018年に経験したインシデント	世界	日本
DDoS攻撃によるインターネット接続の輻輳	40%	39%
DDoS脅威、攻撃による脅迫	34%	**40%**
通常のトラフィックの増加、スパイクによるインターネット接続の輻輳	29%	**34%**
自ネットワーク上のボット化、感染したホスト	17%	25%
ランサムウェア	32%	29%
悪意のある部内者	26%	14%
企業ネットワークにおけるAPT（Advanced Persistent Threat）	24%	25%
産業スパイ、データ漏洩	21%	13%
法規制管理対象データの漏洩	20%	8%
法規制管理対象外データの漏洩	21%	10%
侵害されたIoT	17%	11%
偶発的なデータ損失	40%	39%
偶発的な基幹サービスの機能停止	28%	25%

特に**DDoS関連のインシデント経験率が高い**結果となった。

情報漏洩関連のインシデントは世界と比べて低い傾向。

ネットスカウトシステムズ WISR第14版より

日本と世界のサイバー脅威状況

ハイスコア項目の考察

- **DDoS脅威・攻撃による脅迫**
  - ✓ 検知技術の導入が進んでおり、他国に比べてDDoSの検知率が高い
  - ✓ Eコマース（インターネットビジネス）の成長

- **通常のトラフィックの増加、スパイクによるインターネット接続の輻輳**
  - ✓ DDoSだとわからない”隠れDDoS”の攻撃を受けている可能性が高い（後述）
  - ✓ この”隠れDDoS”の相談は昨今急増している

日本と世界のサイバー脅威状況

- **自ネットワーク上のボット化、感染したホスト**
  - ✓ ITの普及率の高さに比例して脆弱なデバイス（IoT等）が多数接続されている
  - ✓ 攻撃の踏み台になっている脆弱なデバイス、野良サーバー等が増加していることで攻撃発信元となっている

NETSCOUT

DDoS攻撃とは

そもそもDDoS攻撃とは？？

DDoS攻撃とは

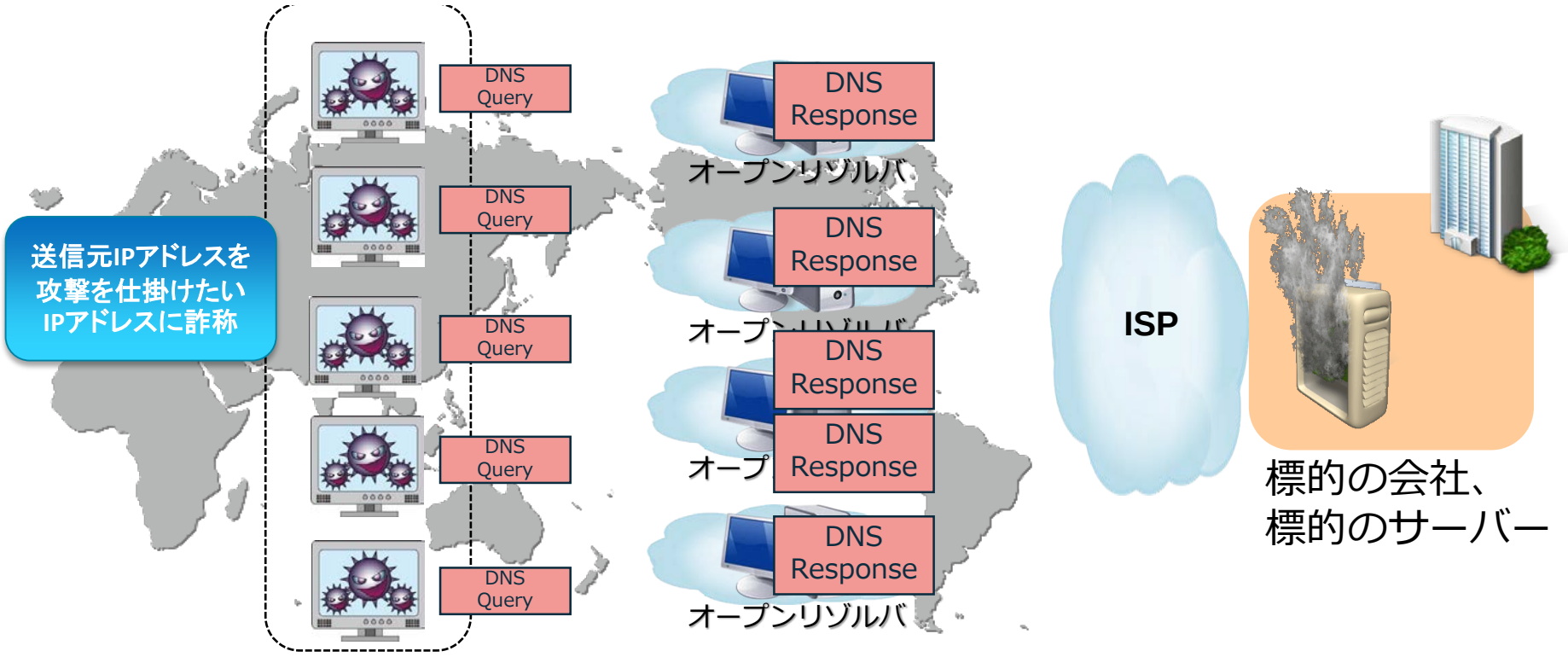
- インターネットに公開されているサービスが標的
- サービスを停止に追い込むことが目的
- （主に）マルウェアに感染したデバイスが発信源

DDoS攻撃とは

DDoS攻撃とは

（例）DNSアンプ攻撃

- 世界中にあるオープンリゾルバを踏み台
- ネットワーク帯域を輻輳させる攻撃



DDoS攻撃って
受けるとマズいの？？

DDoS攻撃の被害

1. サイト停止による売り上げへの影響

例)
1時間あたり平均100万の売上が
あるサイトでDDoSにより10時間
のダウンが発生
(AM 9:00 – 19:00)

被害額 = **1000万円**

DDoS攻撃の被害

2. 対応に追われる従業員のコスト

例)
時給1,500円のコールセンター・スタッフ
30名を10時間超過で拘束(超過割増 1.5x)

被害額 = **67万5千円**

例)
時間単価5,000円のITスタッフ3名を
10時間超過で拘束(深夜割増 2x)

被害額 = **30万円**

モチベーションダウンによる離職も！

DDoS攻撃の被害

3.企業のイメージダウンによるビジネス機会損失

例)
ライフタイムバリュー５千万円の顧客3社が
競合他社に乗り換えた場合

被害額 = **1億５千万円**

例)
新規顧客の機会逸失

被害額 = **予測不能**

DDoS攻撃の被害

インターネット通信障害のお知らせ

2019.10.30　お知らせ

◆2019/10/09掲載（2019/10/30 10：35更新）

全国エリアの一部マンションにて、断続的に通信の異常が発生しております。

発生日時：2019/10/02(水) 20:00頃～
現　　象：DDos攻撃による大量のデータ受信で通信高負荷となり、ネットワークが不安定
影　　響：全国エリアの一部マンション
対策状況：マンションの共有部設置機器の順次交換（攻撃自体への対処も並行継続）
※正式な日程が決まり次第、マンション掲示板等へお知らせを掲示いたします。
※共有部設置機器の交換実施
ネットワーク機器も再起動が
お試しください。

事態の収束に向けて攻撃自体
対象マンションの共有部設置
実施しておりますので、復旧
何卒お願い申し上げます。
お客様へは大変ご迷惑をお掛

※文章長尺緩和のため、攻撃
現象再発の説明を削除いたし

※現象について当初は「サイ
厳密には「DDos攻撃」とな

『[redacted]サーバー』本日AM6:50頃～AM7:21頃までのDDoS攻撃の影響によるアクセス障害について

(2019年10月20日　掲載)

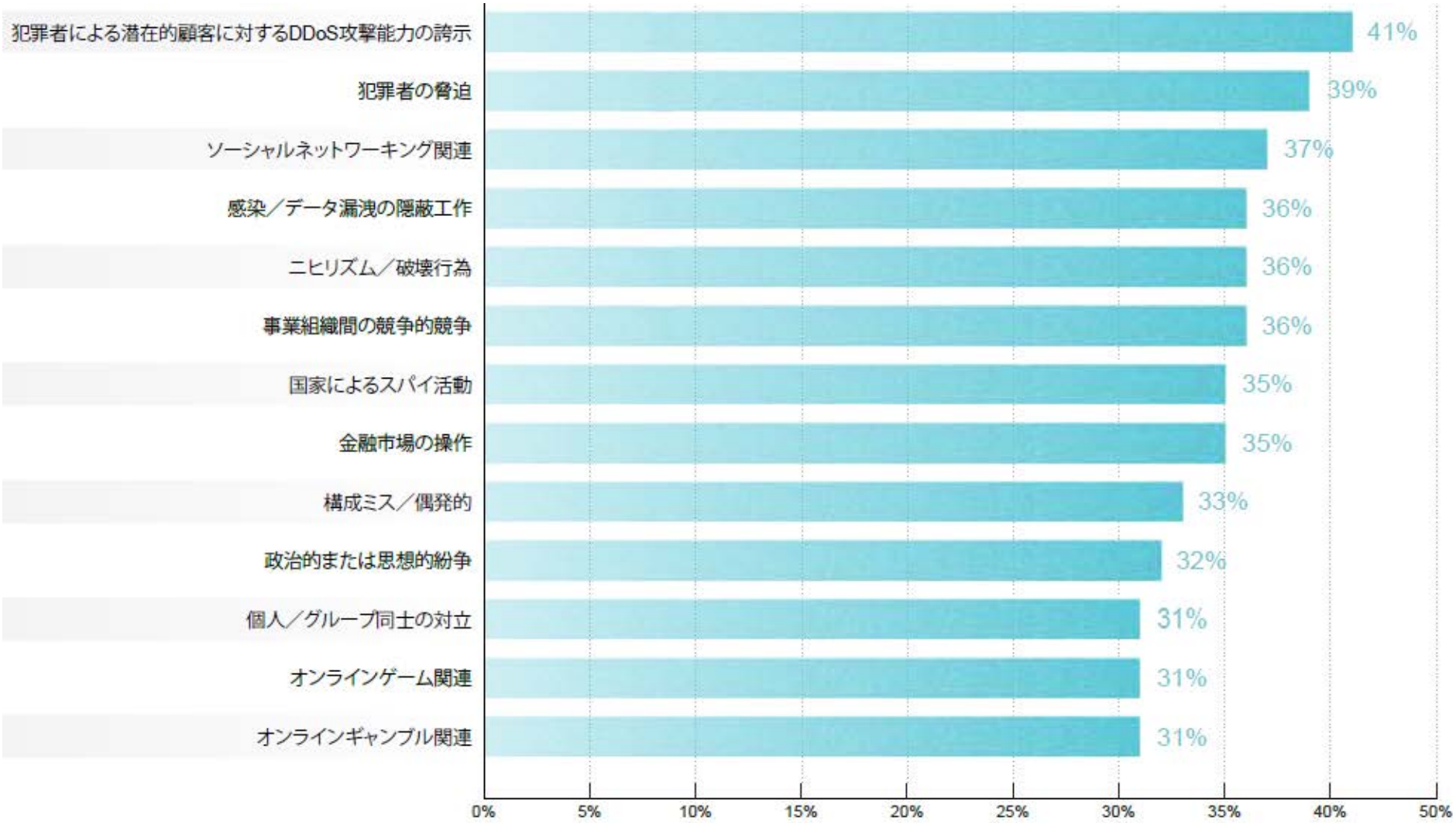
『[redacted].jpサーバー』において
本日AM6:50頃～AM7:21頃まで
DDoS攻撃の影響により、サーバーにアクセスできなくなる障害が発生しておりました。

※障害発生時間は1分程度のずれがある場合がございます。

現在は復旧しておりますが、
ご迷惑をおかけして申し訳ございませんでした。

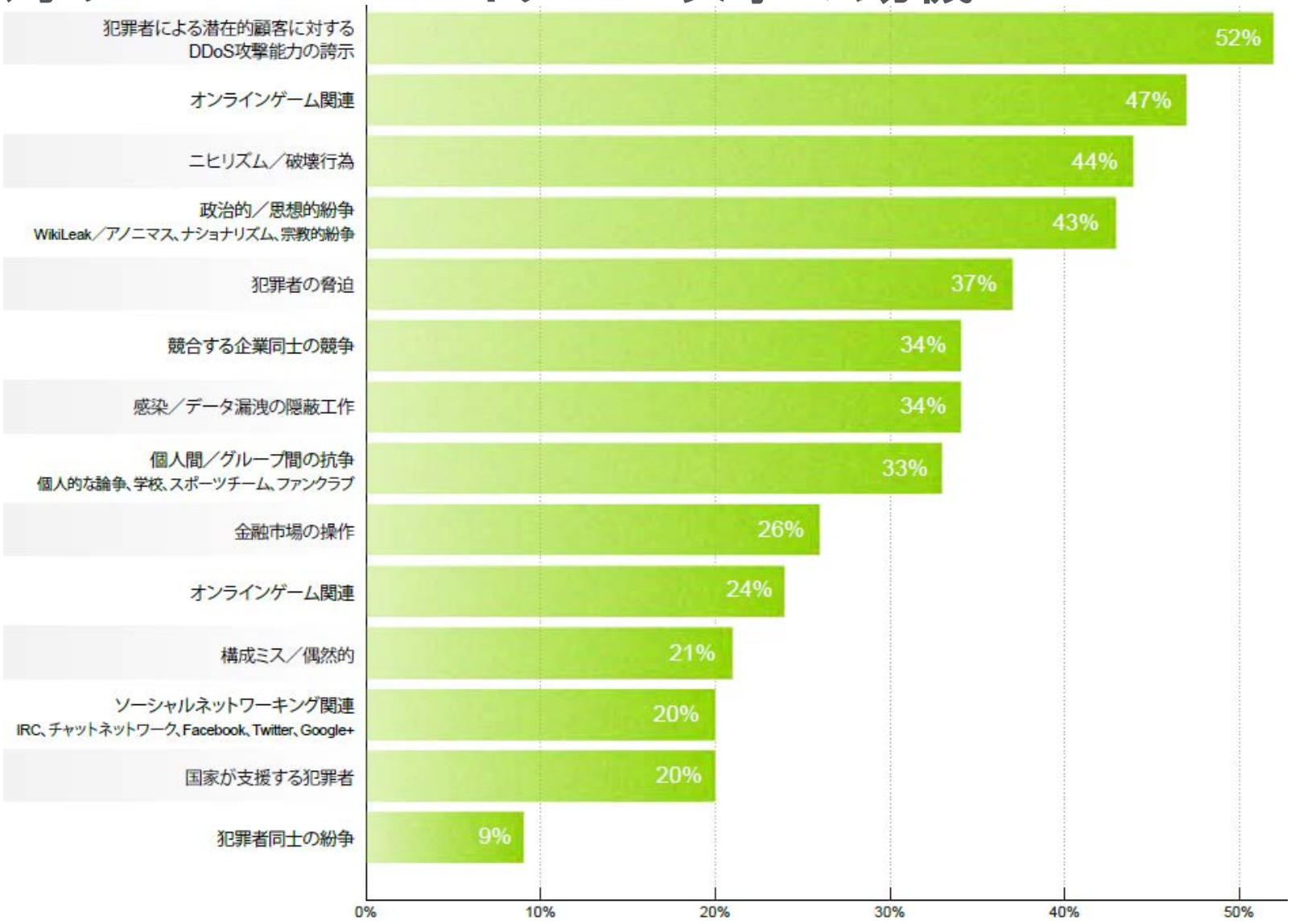
※DDoS攻撃 ... 複数のネットワークから特定のサーバーに対して大量のデータを送りつけ、
ネットワークやサーバーの停止を狙う攻撃手法。

対企業　攻撃の動機



ネットスカウトシステムズ WISR第14版より

対サービスプロバイダー　攻撃の動機



ネットスカウトシステムズ WISR第14版より

NETSCOUT

過去の国際イベントにおける DDoS攻撃

ブラジルを襲ったDDoS攻撃

組織的なキャンペーン	• アノニマス、LizardSquad、PoodleCorp • JavaScriptやToRネットワークを使用した巧妙なツール • 選手応援のソーシャルメディアを狙うキャンペーン
アプリケーション層攻撃	• Slowloris – HTTP Slowリクエスト • Ack-Psh Flood • Http-Getリクエスト
大規模ボリューム攻撃	• 平均攻撃サイズ：200Gbps以上 • 最大攻撃サイズ：540Gbps
使用された技法	• GREカプセル化攻撃（ACL/フィルターをバイパス） • ACKフラッド • UDPフラッド – ポート443および80 • ICMPエコー・リクエスト・フラッド

攻撃者のメッセージ

Anonymous Brasil
13 h ·

Agora você também pode nos ajuda
os passos abaixo e bem vindo a fes

Esse programa foi d
sistema windows, le
necessário o uso de
a rede tor.

Tutorial:

1 - Acesse
https://www.torproje
6.0.2/torbrowser-ins
instale o navegador
2 - Acesse
http://www.megafile
ympddos.rar e baixe
opolympddos.rar (lir
3 - Execute o TOR B
mensagem de que e
4 - Abra o arquivo o
depois abra ddos.ex
5 - Clique nos botõe
site para "Atacar". U

mensagem de que ele está ativo.
4 - Abra o arquivo opolympddos.rar, e depois abra ddos.exe
5 - Clique nos botões com o endereço do site para "Atacar". Uma janela do CMD será aberta.
6 - Quanto mais vezes clicar no botão, mais janelas de ataque serão abertas.
7 - Divirta-se indo jantar/viajar/trabalhar enquanto seu computador faz todo trabalho de forma anônima e segura.

Anonymous Brasil retweetou
Anonymous Center @AnonymousCenter · 39 min
#Anonymous
#OpOlympicHacking
e/KU1Z5T-vFE4
s Begin.
tebin.com/WTN6J1Qh

2016年ブラジルを襲ったDDoS攻撃

当日会場のみでの投影

ブラジルを襲ったDDoS攻撃の変遷

当日会場のみでの投影

GREフラッド攻撃

当日会場のみでの投影

ICMPフラッド攻撃

当日会場のみでの投影

Slowloris攻撃

当日会場のみでの投影

2020年　狙われる東京

当日会場のみでの投影

ブラジルのその後（回数）

当日会場のみでの投影

NETSCOUT

直近の日本における DDoS攻撃と想定される手法

直近の日本におけるDDoS攻撃

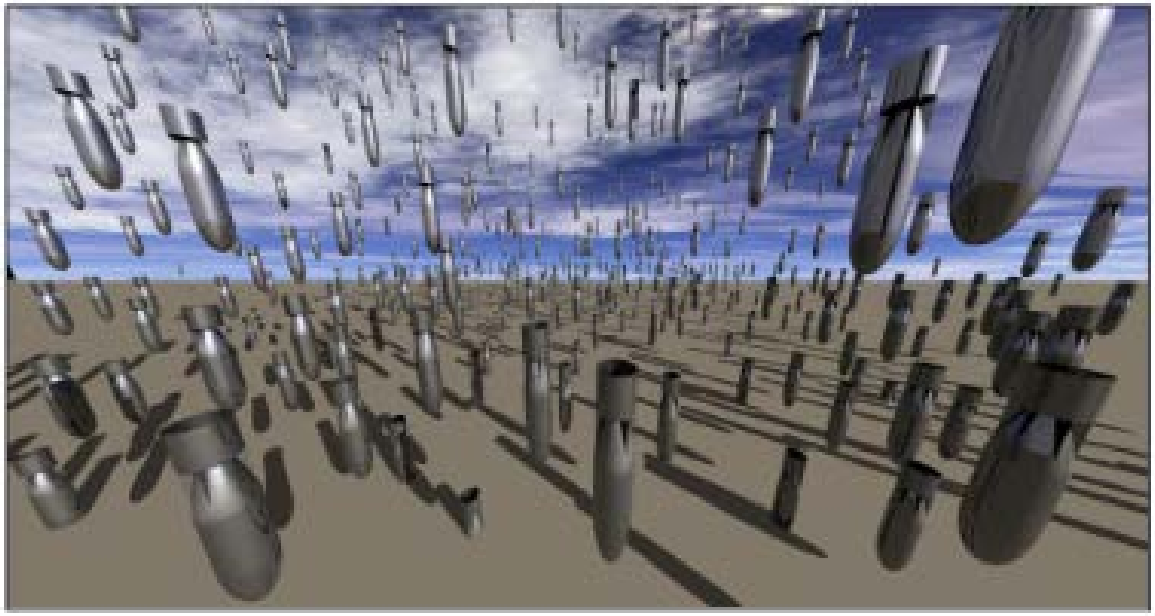
当日会場のみでの投影

カーペットボンビング（絨毯爆撃）攻撃

従来のDDoS攻撃

標的のみを攻撃

カーペットボンビングDDoS攻撃

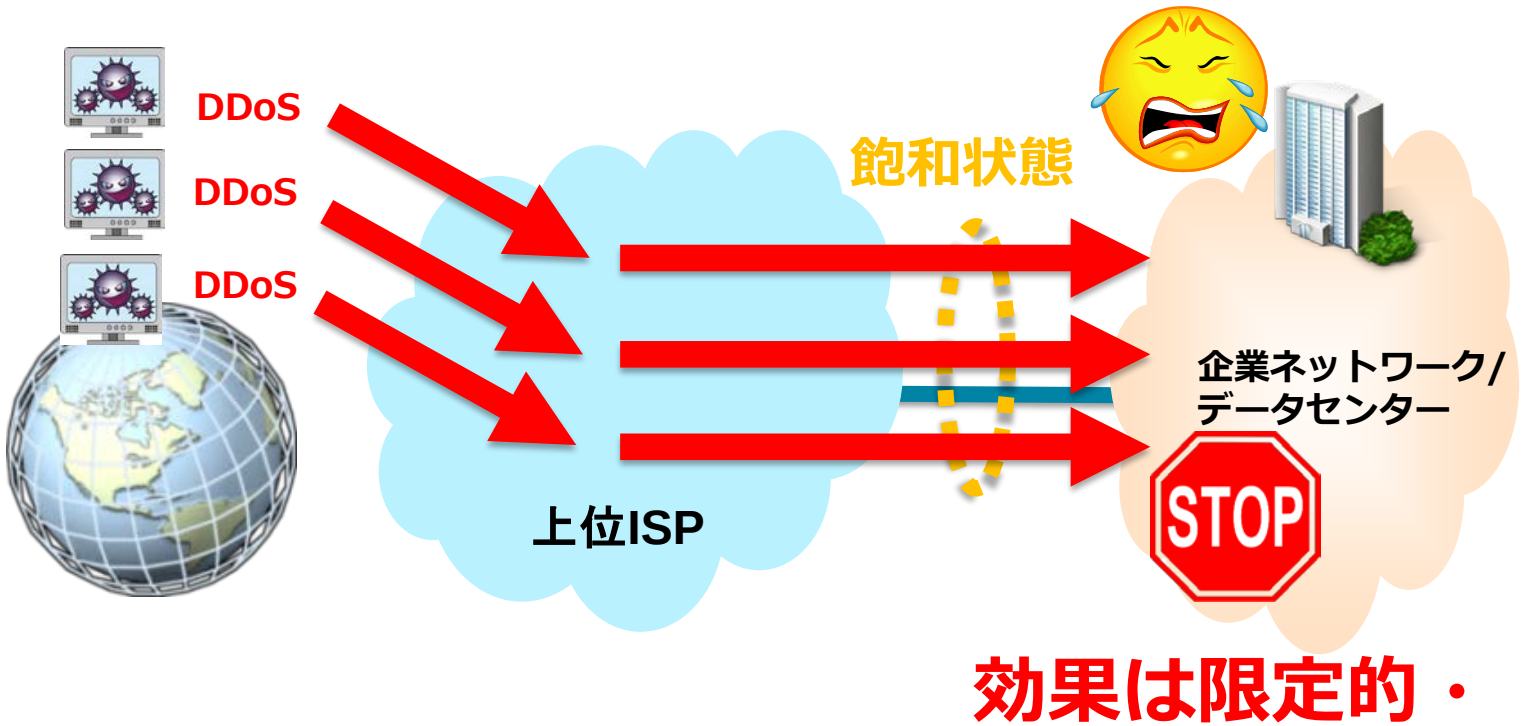


ネットワーク全体を攻撃する手法
（一般的には検知が難しい）

NETSCOUT

DDoS攻撃への対処方法

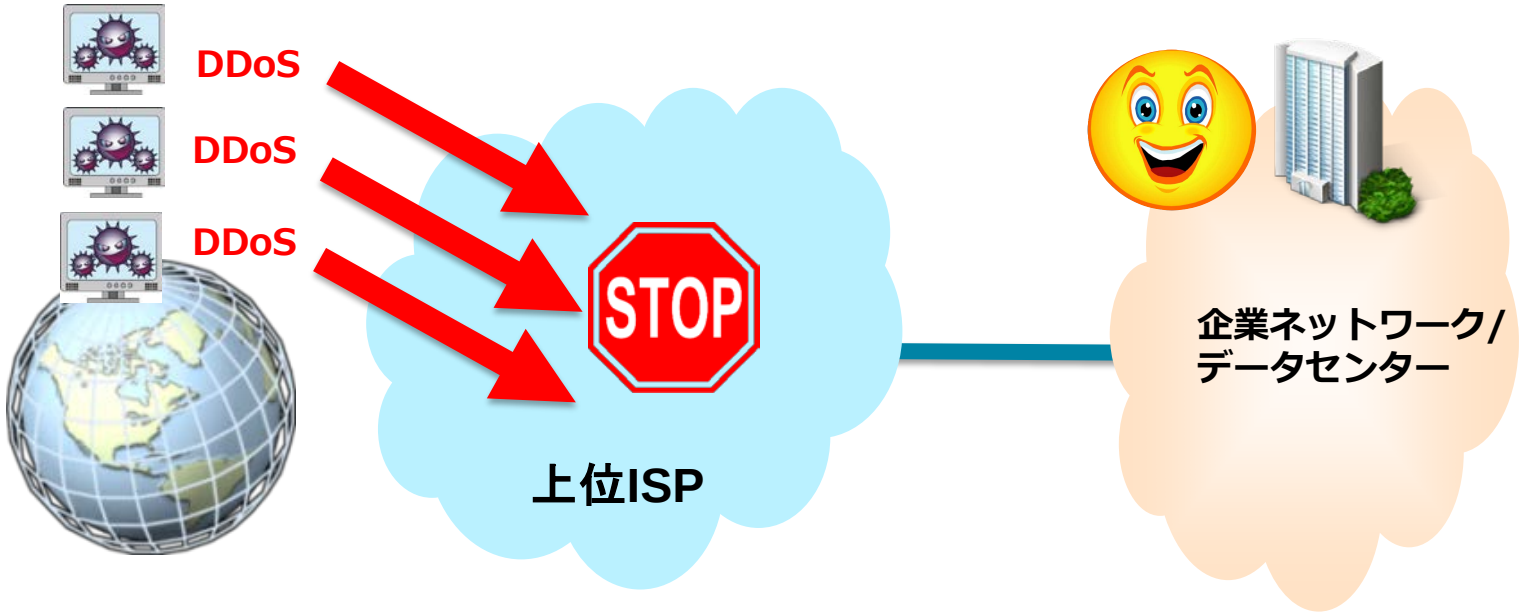
DDoS対策



効果は限定的・・・

ボリューム型DDoS攻撃の場合、エンドユーザとのインターネットアクセスリンクが飽和

DDoS対策



ボリューム型DDoS攻撃を防御できるのは
上位ISPだけ！

まず始めるべきDDoS対策

ボリューム型DDoS攻撃

まずは契約しているISPさんに相談してください

契約しているISPさんがDDoS対策サービスを行っているのか、

可能であればサービス内容、約款等を読むことをお勧めします。

ブラジルに学ぶDDoS緩和･防御成功への道

- イベント開会式の数か月前から攻撃は開始された。
  - IoTボットネットからの大規模ボリューム攻撃
- ブラジルの銀行、通信会社、政府機関およびゲーム会社が（LizardStressorを介して）攻撃された。（2016年6月ASERTブログの掲載記事で報告） 最大時400Gbpsを超えるDDoSを観測。
- ワールドカップとイベント開会前の攻撃行動は、キャリア事業者にとってはイベント本番に対しての予行練習となった。
- 事前準備をしっかりと行うことが、大規模かつ複雑な攻撃への対処につながる。逆に事前準備を怠ると、全て攻撃者の思いのままになる。

NETSCOUT

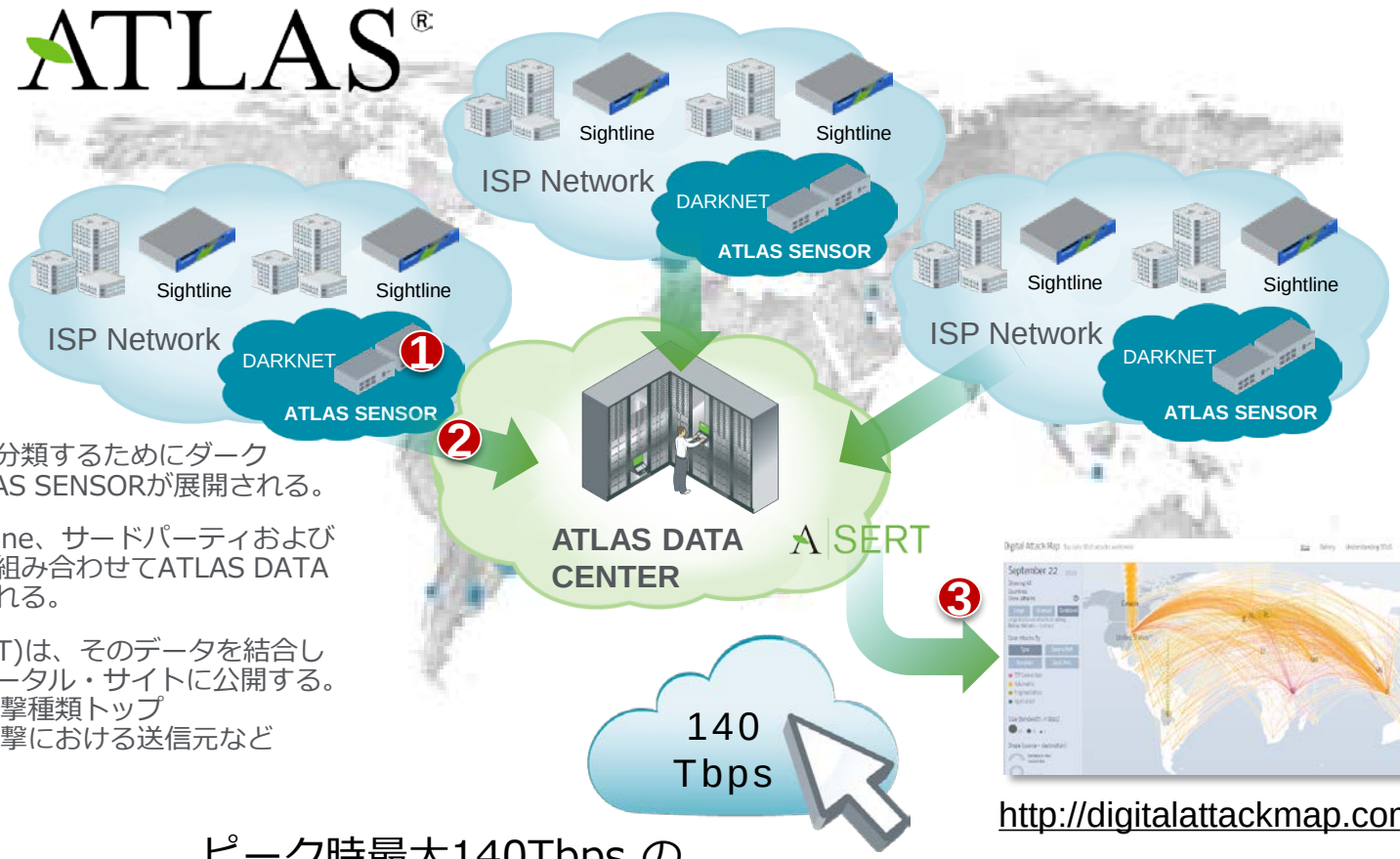
ネットスカウトシステムズのデータ分析の紹介（ATLAS）

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

- ネットスカウトが有する世界最大級の
  トラフィックモニタリングシステム
- 世界中のISPによる善意のデータ共有
- インターネットの生のトラフィックを分析
- Digital Attack Mapとしてデータをフィードバック

  (http://www.digitalattackmap.com/)

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



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 NetscoutのSightline、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。

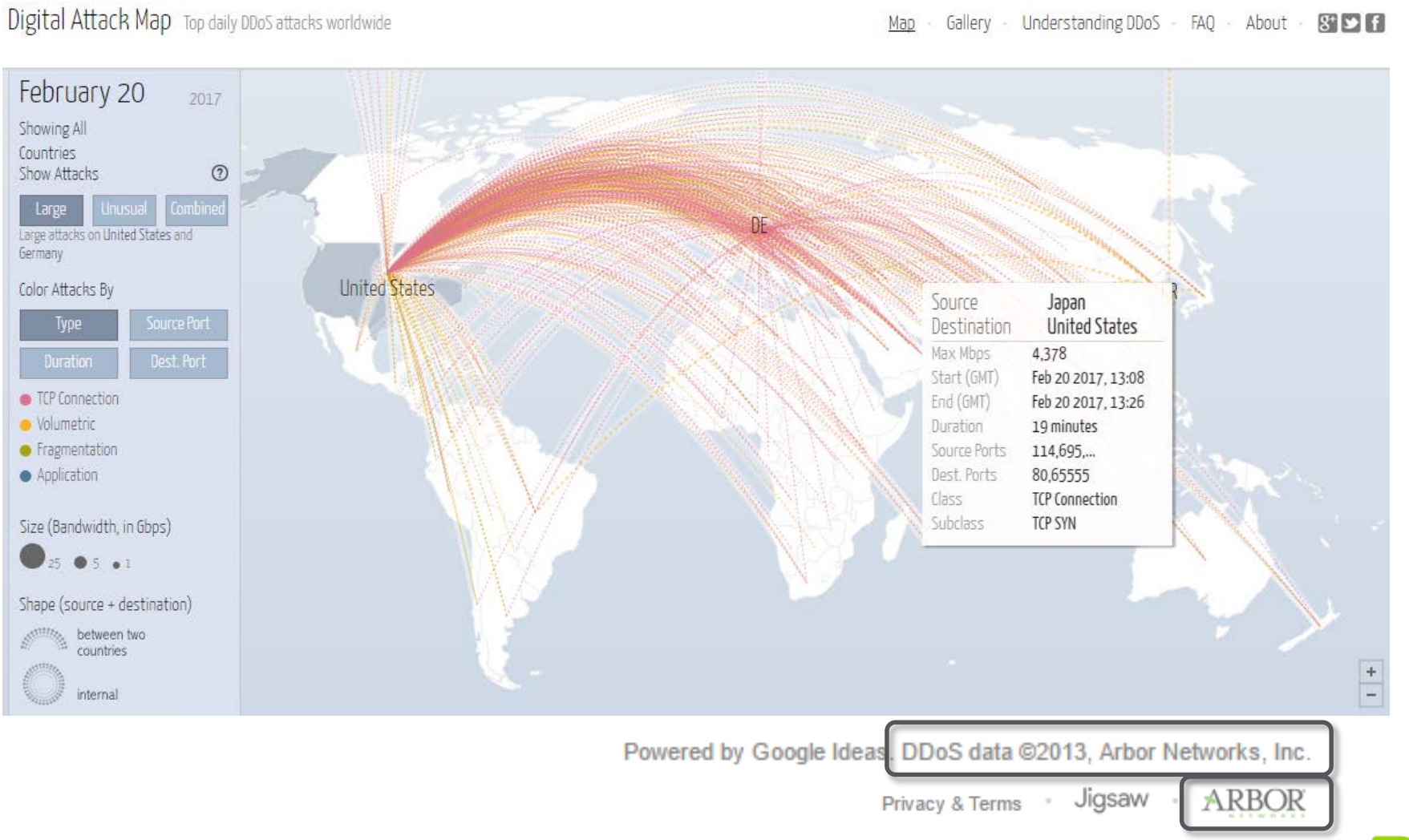
❸ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
・過去24時間の攻撃種類トップ
・過去24時間の攻撃における送信元など

http://digitalattackmap.com/

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

Digital Attack Map

http://www.digitalattackmap.com/



Thank You.

www.netscout.com