# DDoS攻撃10年の歴史を振り返る

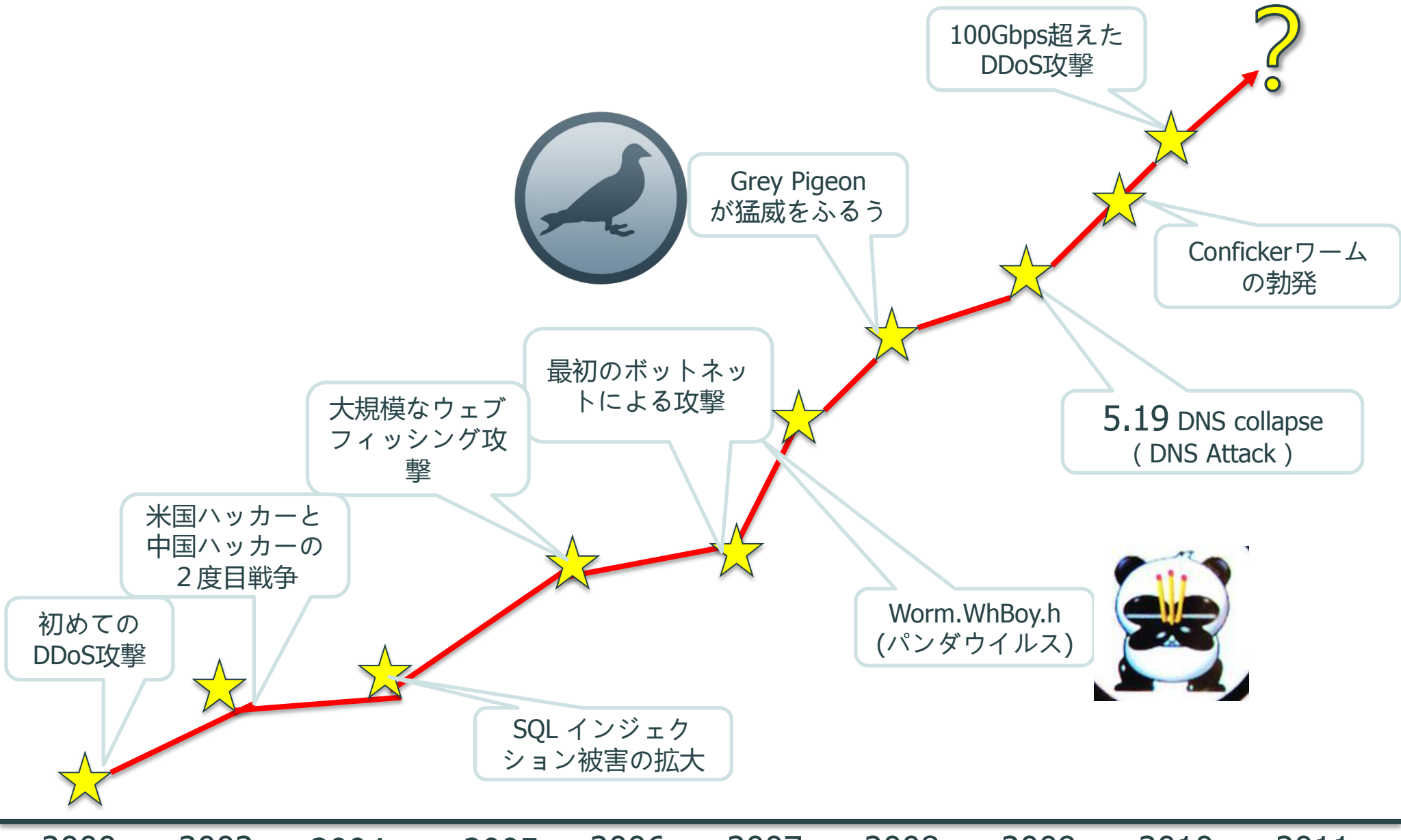
NSFOCUS 顧　茂林
gumaolin@nsfocus.co.jp

1 中国でのDDoS攻撃の変遷

2よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス

# 中国でのDDoS攻撃の変遷



# 中国ではDDoS攻撃が100Gbpsを超えた！

一発で100Gを超える攻撃

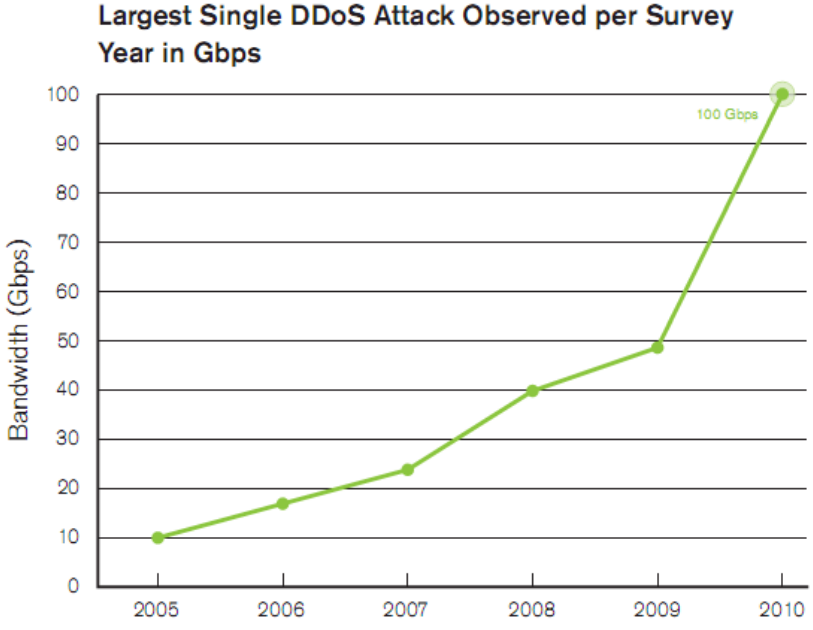



*Figure 1*
Source: Arbor Networks, Inc.

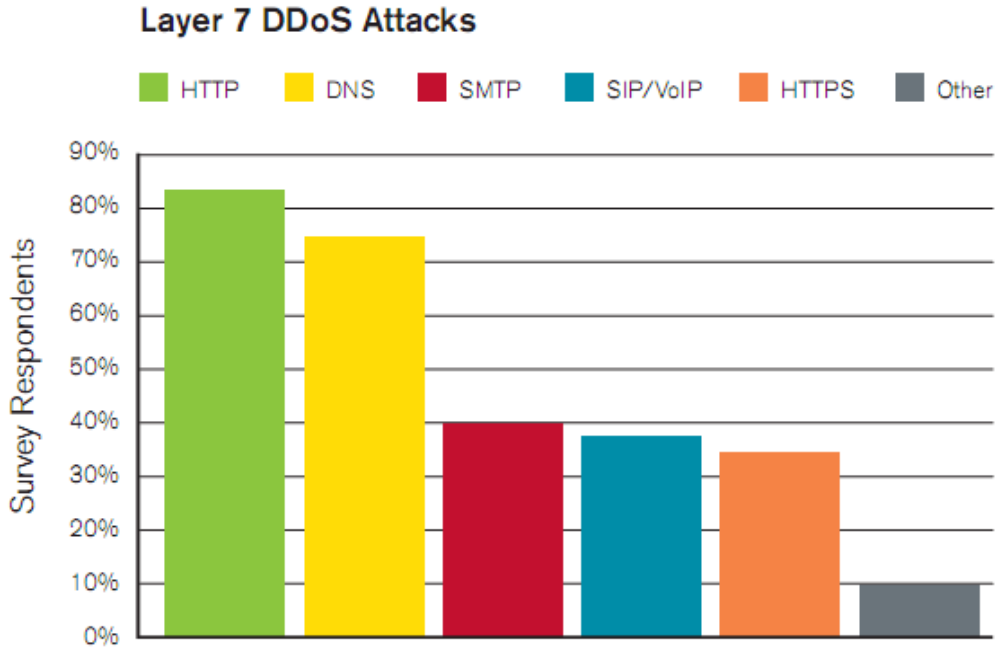



*Figure 8*
Source: Arbor Networks, Inc.

DNS攻撃はもっとも容易なDDoS攻撃手口になってしまった！

1 中国でのDDoS攻撃の変遷

2よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス

# よく見られるDDoS攻撃

**大流量型の攻撃**：
攻撃トラフィックのソース：
・テスト用機器
・ハイパフォーマンスサーバーとソフト
・IDC


**トラフィックの特徴：**
・まったくランダムなSource IPまたはある決まった範囲での
ランダムなIP
・スリーハンドシェイクができない
・1Gbpsから70Gbpsにまで及ぶトラフィック

**防御方法：**
・従来のリバースプロクシを使って偽装IPからのパケットを
ドロップする
・ただし大量のリバースプロクシトラフィックにより、
アップリンク帯域が逼迫

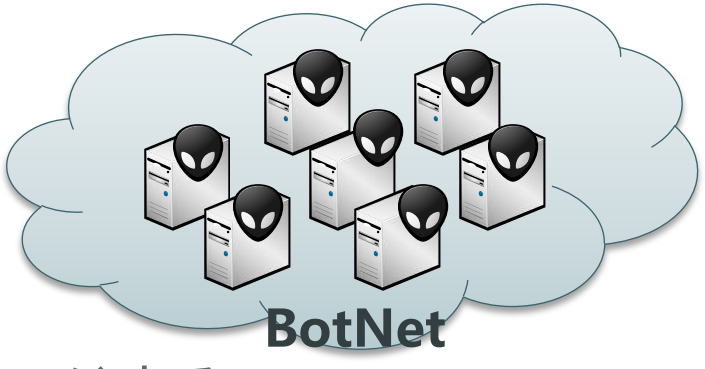
# よく見られるDDoS攻撃

**実IPからの中規模の攻撃：**

・Botnet
・Proxy Server

**攻撃の特徴：**

・スリーハンドシェイクは完了する
・主にＨＴＴＰのサビースをターゲットにする
・100M程度の攻撃トラフィック




**防御方法：**

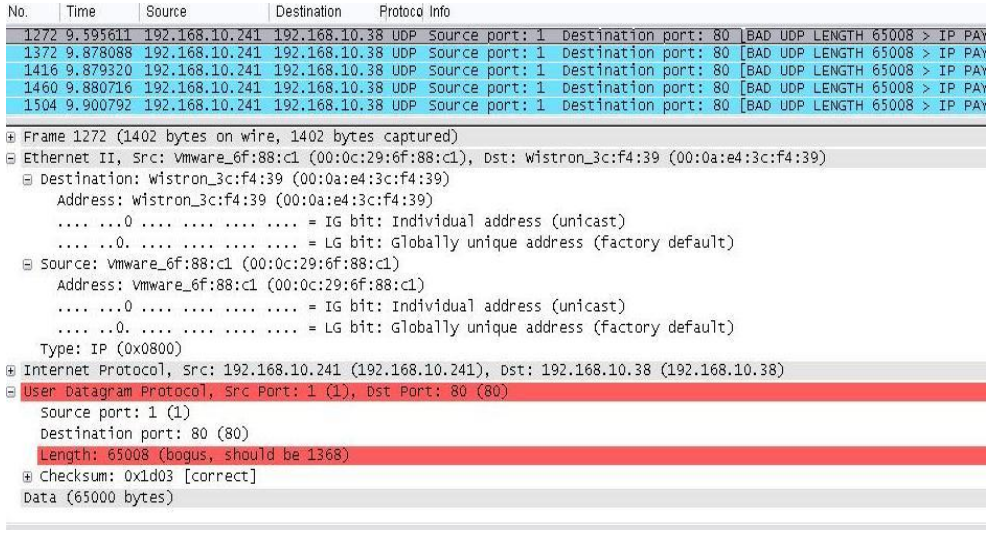
・SYN-Cookieのチェック
・アプリケーション層のデータチェック
・シグネチャを使ってパケットフィルタリングする

# 特殊なDDoS攻撃

**偽メッセージによる大規模な攻撃トラフィック：**
異なる攻撃ターゲットごとに、攻撃がばれないように
攻撃のメッセージを偽装する。
例： ソースIPを偽装
TTL,Port,SNなどの偽装
コンテンツの偽装

**防御の考え方：**
UDPのサービスでは、どんな方法でもソースIPアドレスが偽装されて
いれば、スリーハンドシェイクができない

**防御方法**：
- リバースプロクシ
- SYN-Cookieのチェック
- 自動学習(Smart Technology)



# BotNetによる攻撃

**Botnet**

大量なゾンビPCから構成され、通信可能で、
リモートコントロールできるネットワーク

**特徴:**

- コントロールが可能
- 悪意を持って拡散
- 同じ動きをする悪意のある行動が一つのボットマスター
  からたくさんのゾンビPCに拡散

**脅威:**

- DDoS攻撃
- Spam
- Phishingと成りすまし
- 情報搾取

**Botの分類：**

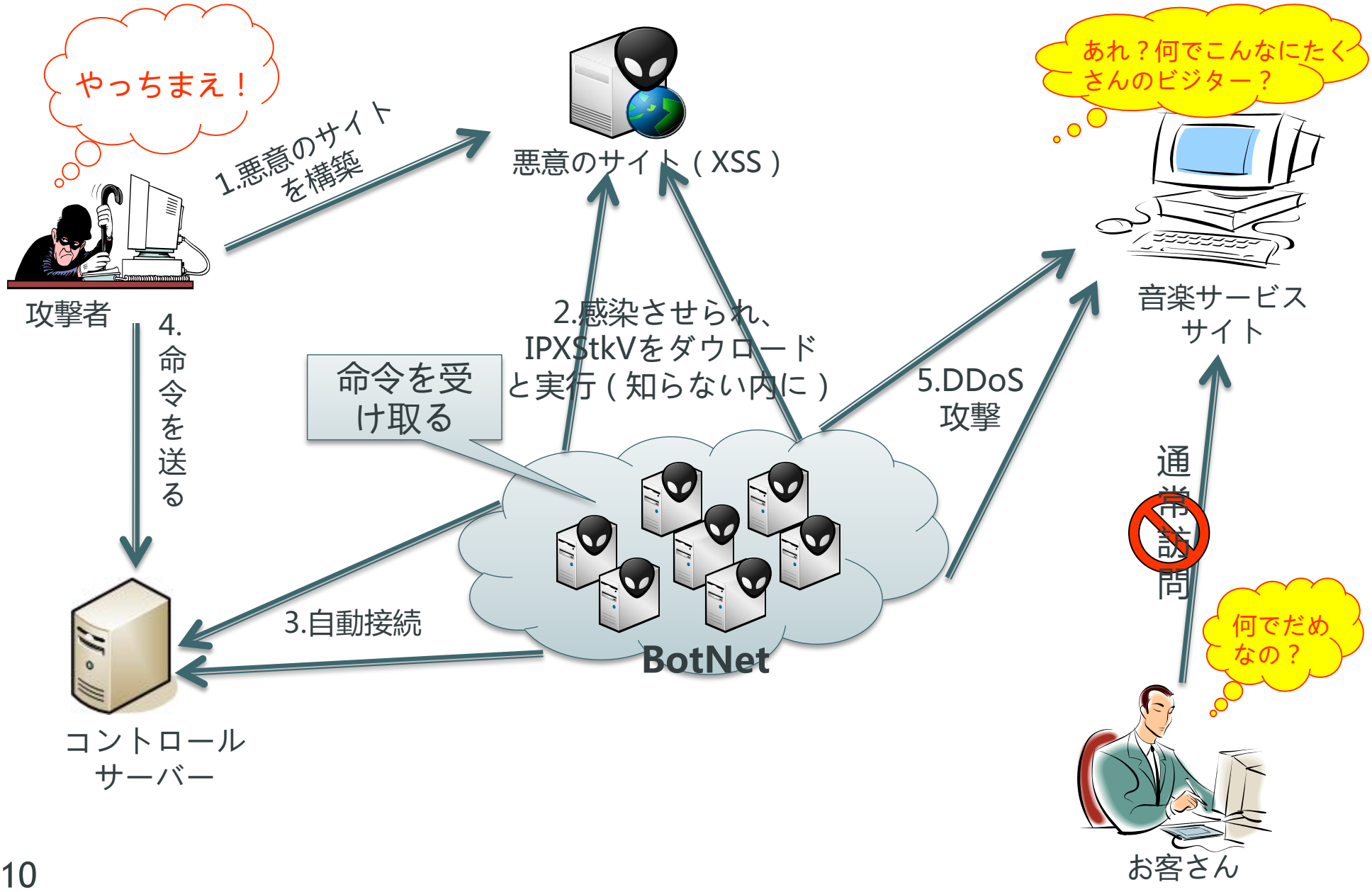
- IRC Bots
- P2P Bots
- HTTP Bots
- DNS Bots

# Mariposa Botnet

Mariposa Botnet infected 14,000,000 computers in 31901 cities of 190 countries all over the world.

Source: Panda Security 2010 March

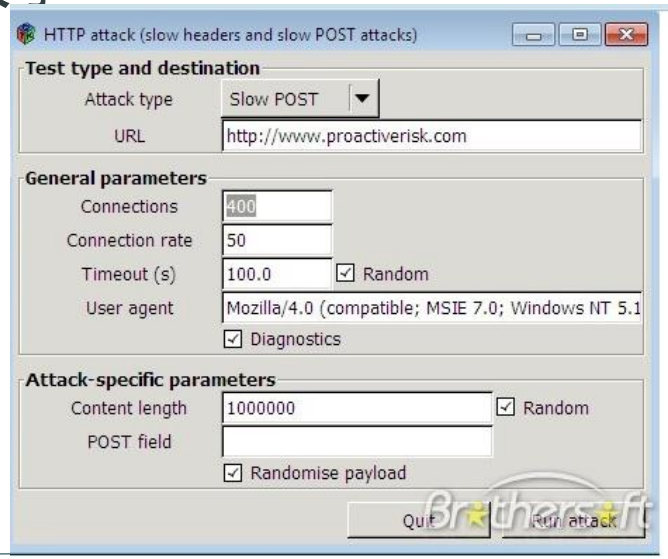
# Botnetによる攻撃の流れ図



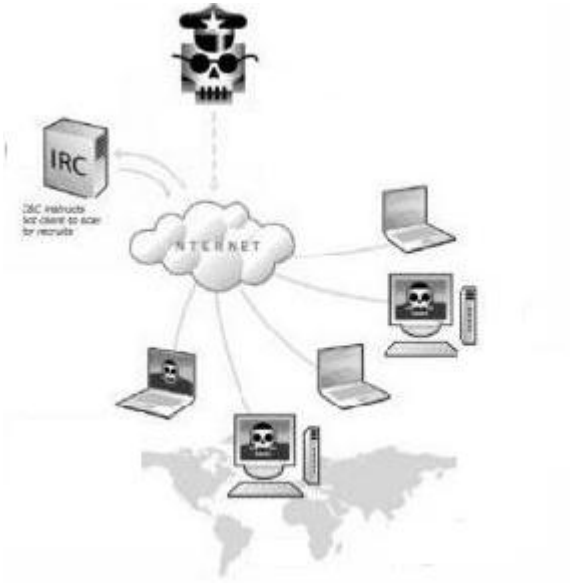
# Http Get Flood 攻撃

## ページリフレッシュによる攻撃

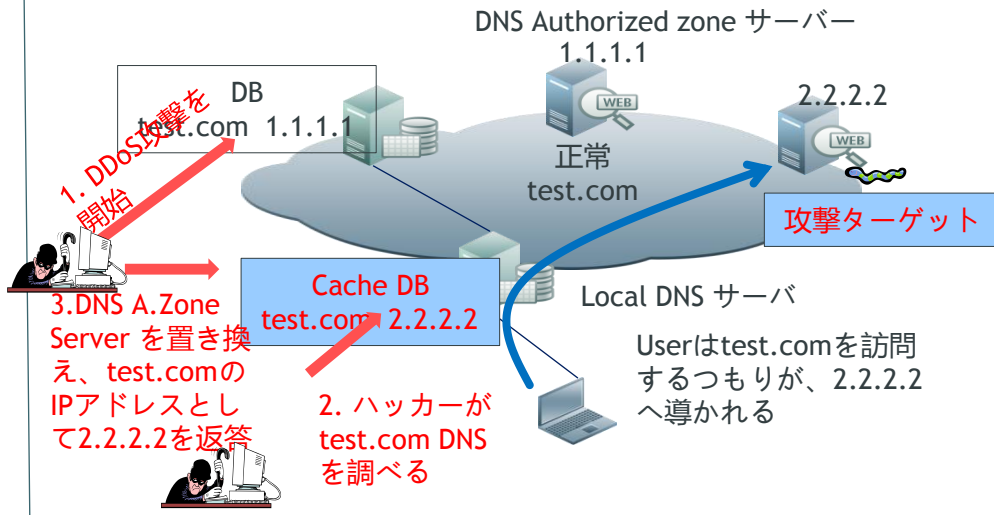

## 静的な攻撃



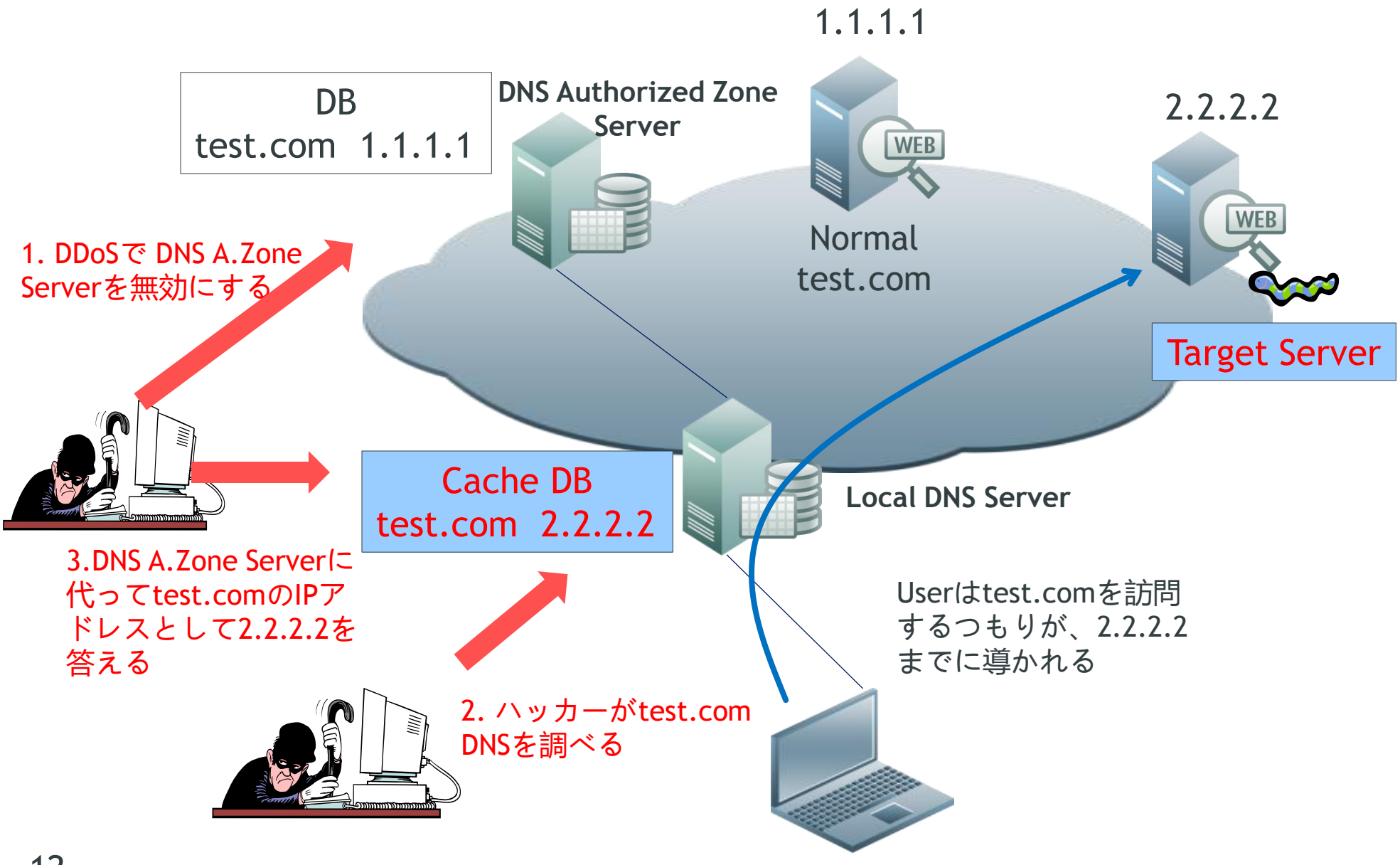

## 動的な攻撃




## DNSを利用する攻撃



# DNSポイズニング攻撃

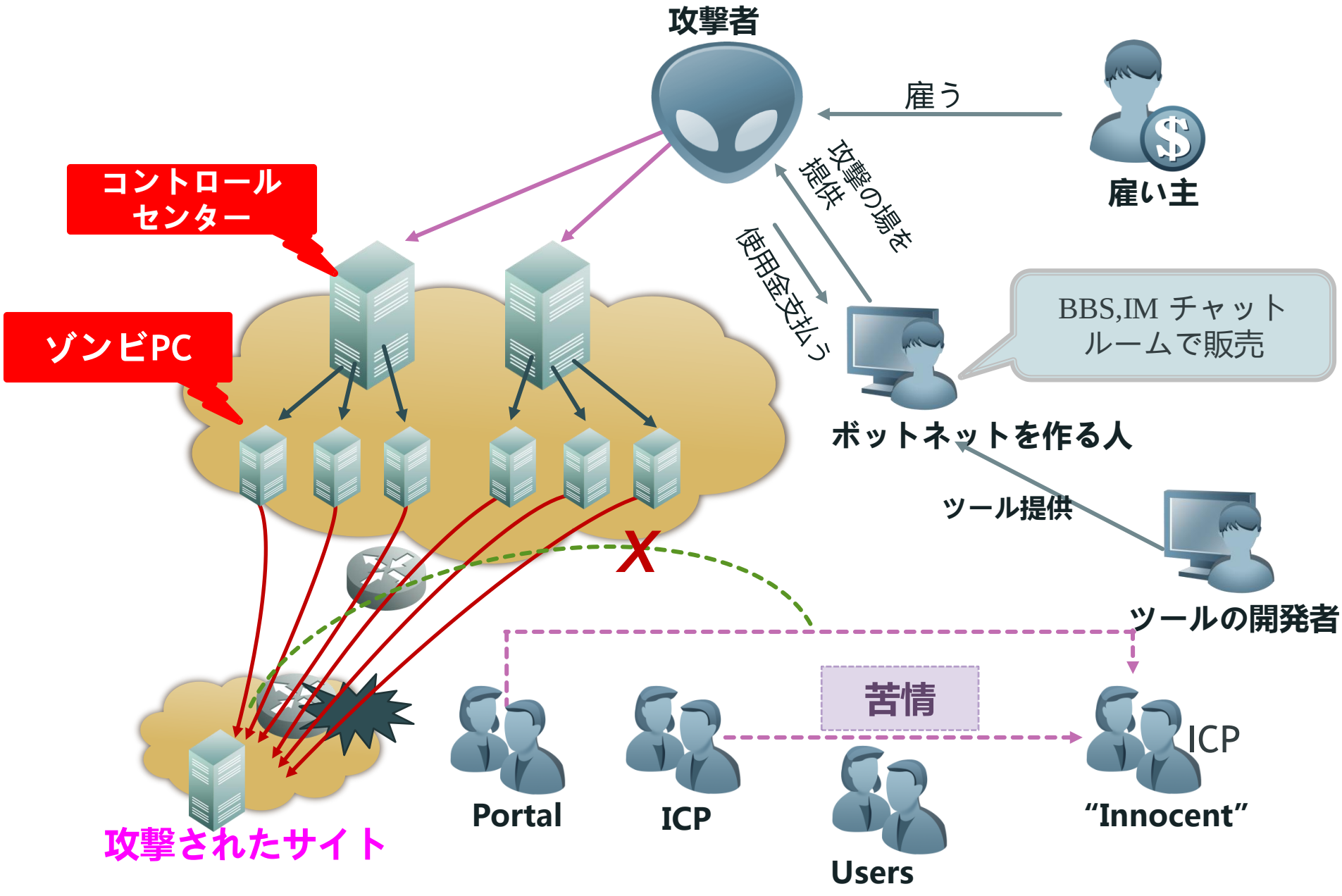


1 中国でのDDoS攻撃の変遷

2よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス

# DDoS 攻撃のアングラビジネス



# ご清聴どうもありがとうございました