

# ISPにおけるDDoS対応について ～DNSの活用とネットワークの立場から～

石野 雅博 (NTTコミュニケーションズ, OCN)

坂本 祐一 (NTTコミュニケーションズ, OCN)

水越 一郎 (NTTコミュニケーションズ, OCN)

# はじめに

- WormのDDoS攻撃がISPに与える影響
- Antinnyに対してOCNがDNSでやったこと
- ネットワーク管理者が見ていないといけないこと

# Netskyとは

- 自身のSMTP機能を使って増殖する。
- 特定日に特定のサイトへDDoSを仕掛ける。
- 以下のサイトがとても参考になります。

[http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM\\_NETSKY.Q&VSect=T](http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.Q&VSect=T)

(トレンドマイクロ株式会社様のページ)

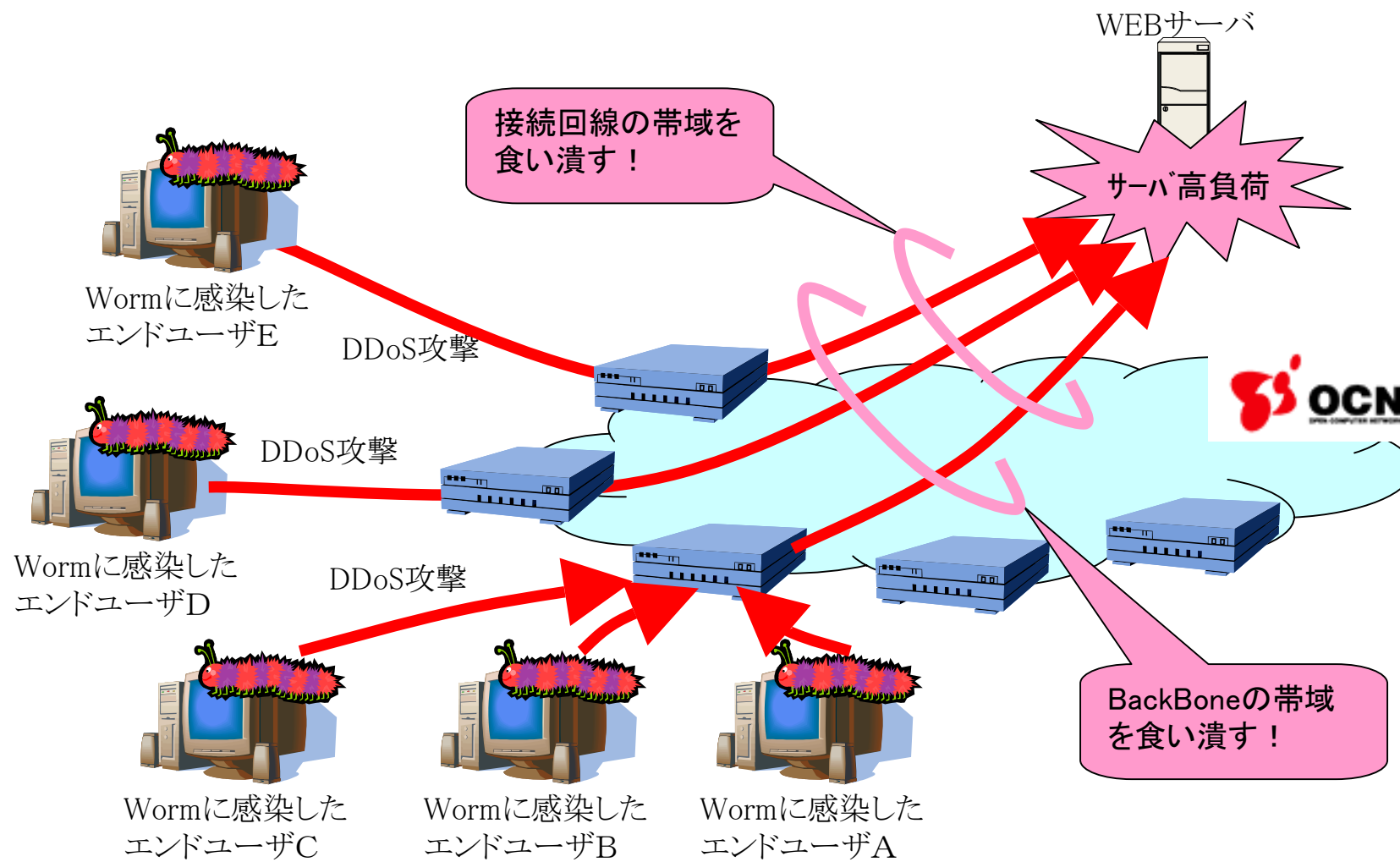
# Antinnyとは

- Winnyでファイルを送りつけて繁殖する。
- 特定日に特定のサイトへDDoSを仕掛ける。
- 以下のサイトがとても参考になります。

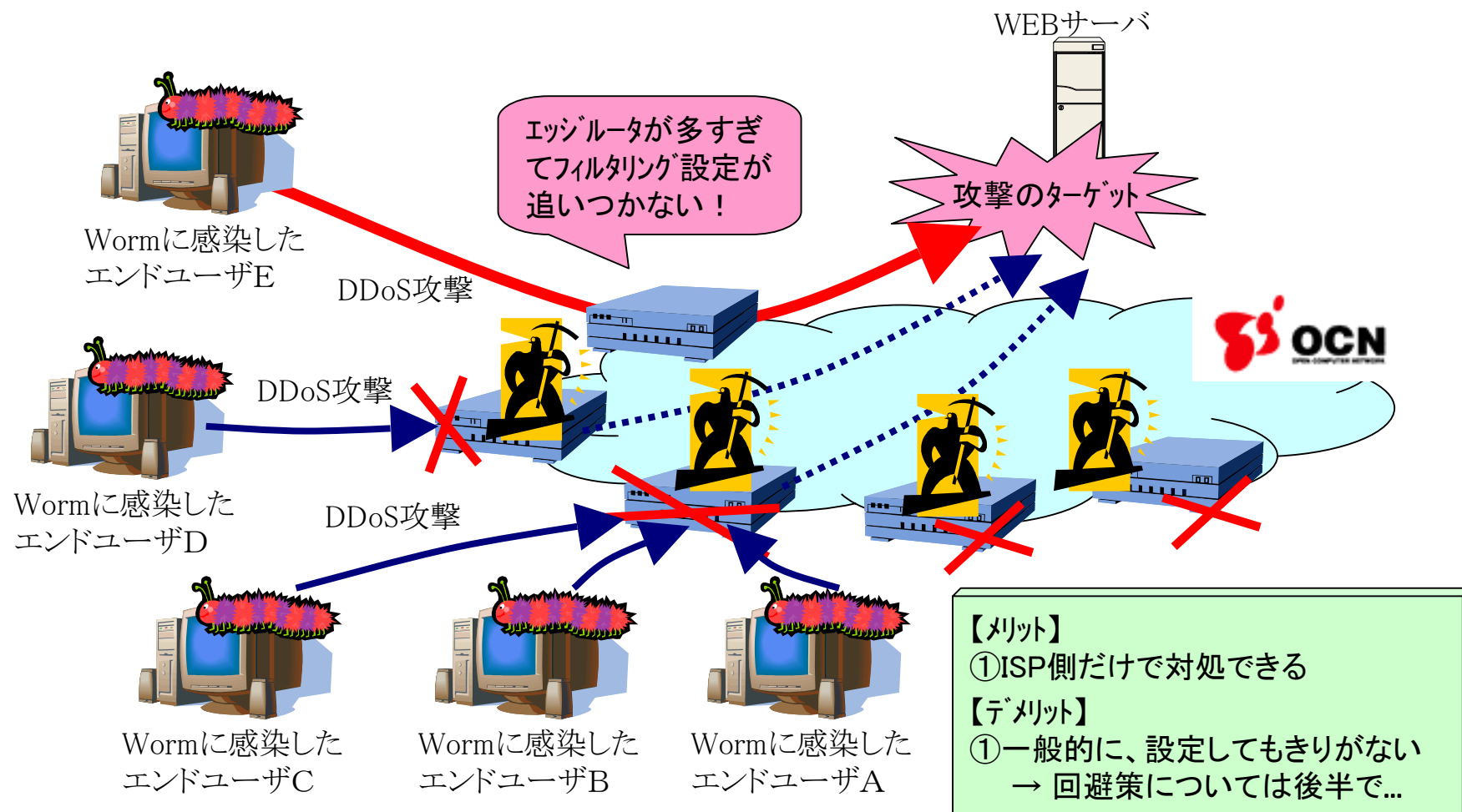
<http://www.symantec.com/region/jp/sarcj/data/w/w32.antinny.k.html>

(株式会社シマンテック様のページ)

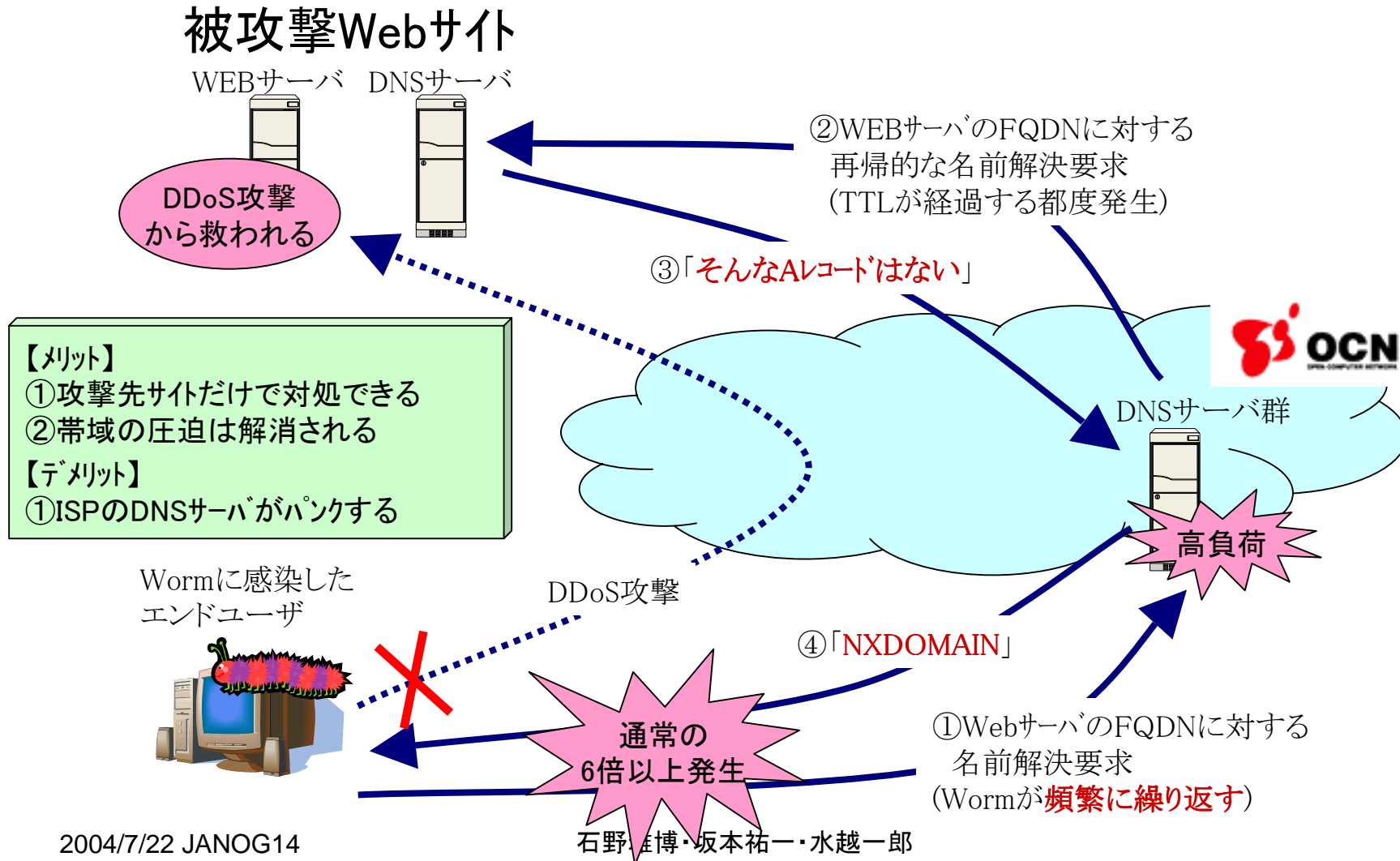
# WormによるDDoS攻撃



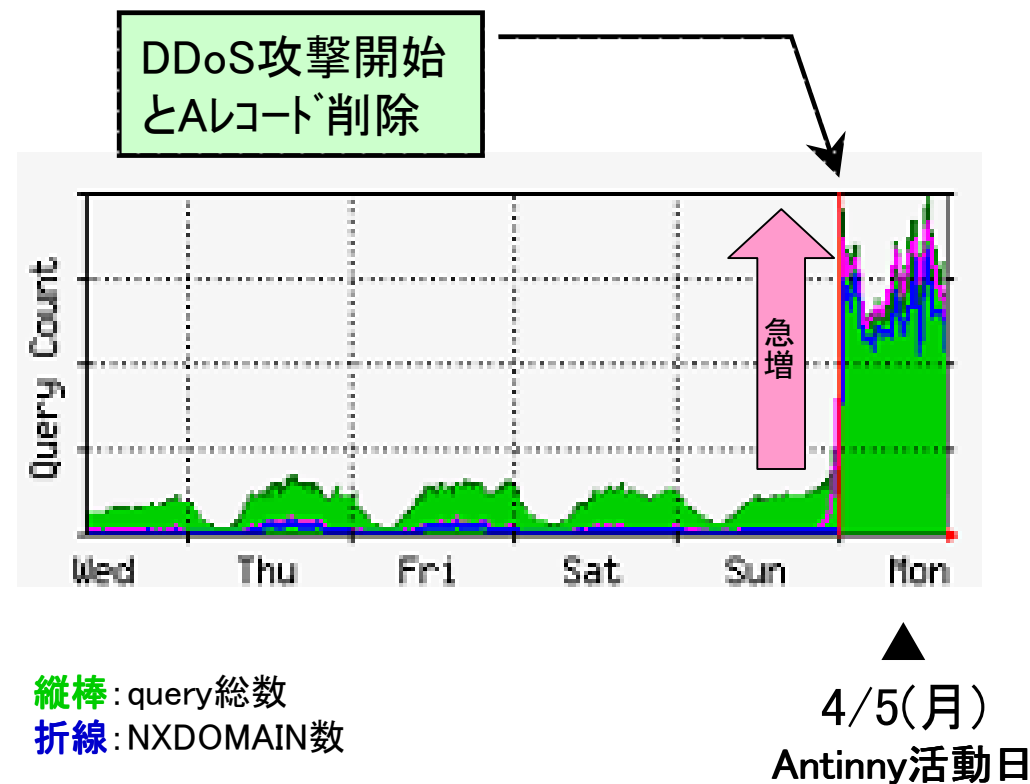
# もしfilteringで立ち向かうと...



# サイト側で勝手にAレコードを削除されると...



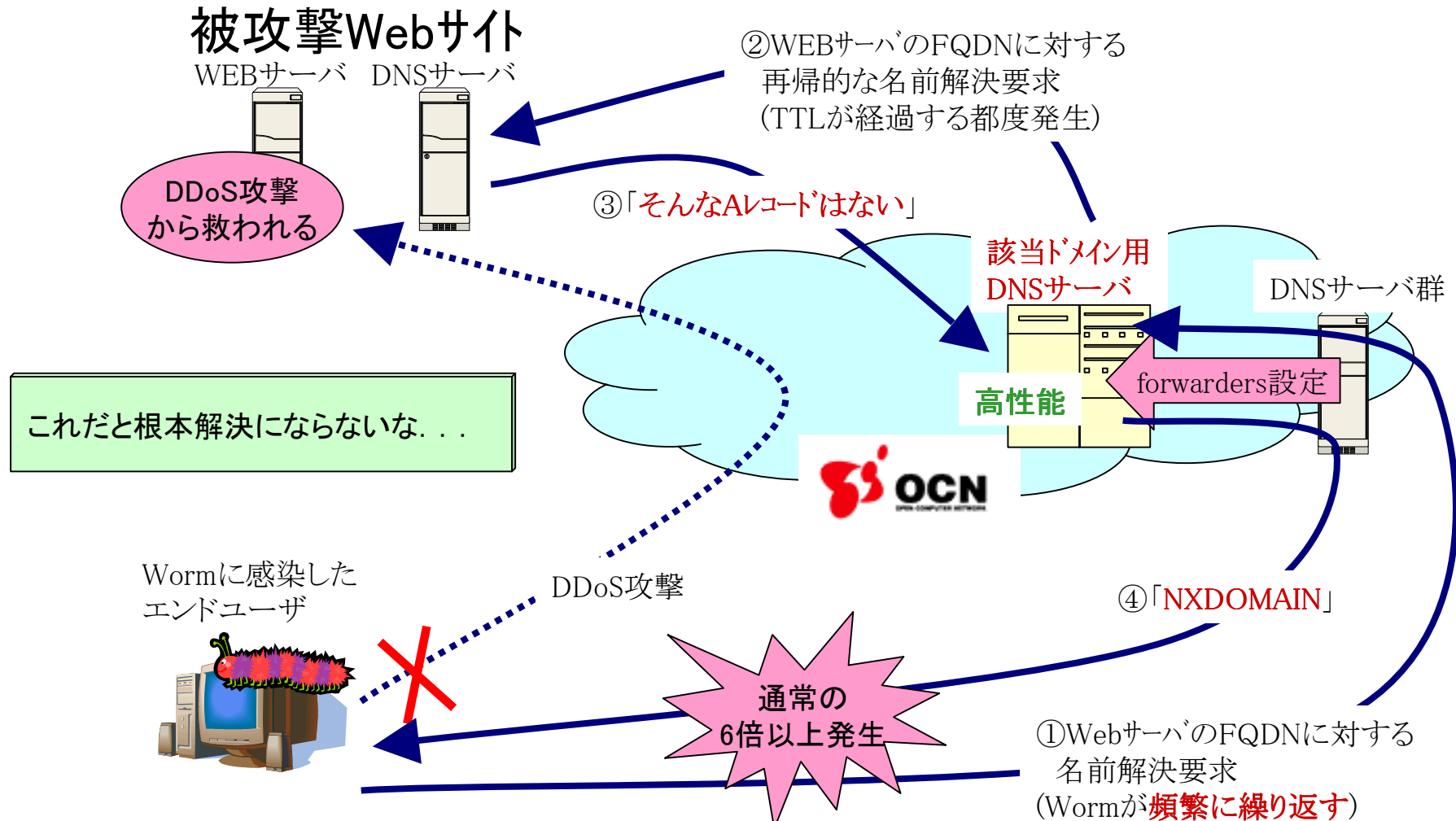
# ISP側DNSではquery処理が急増



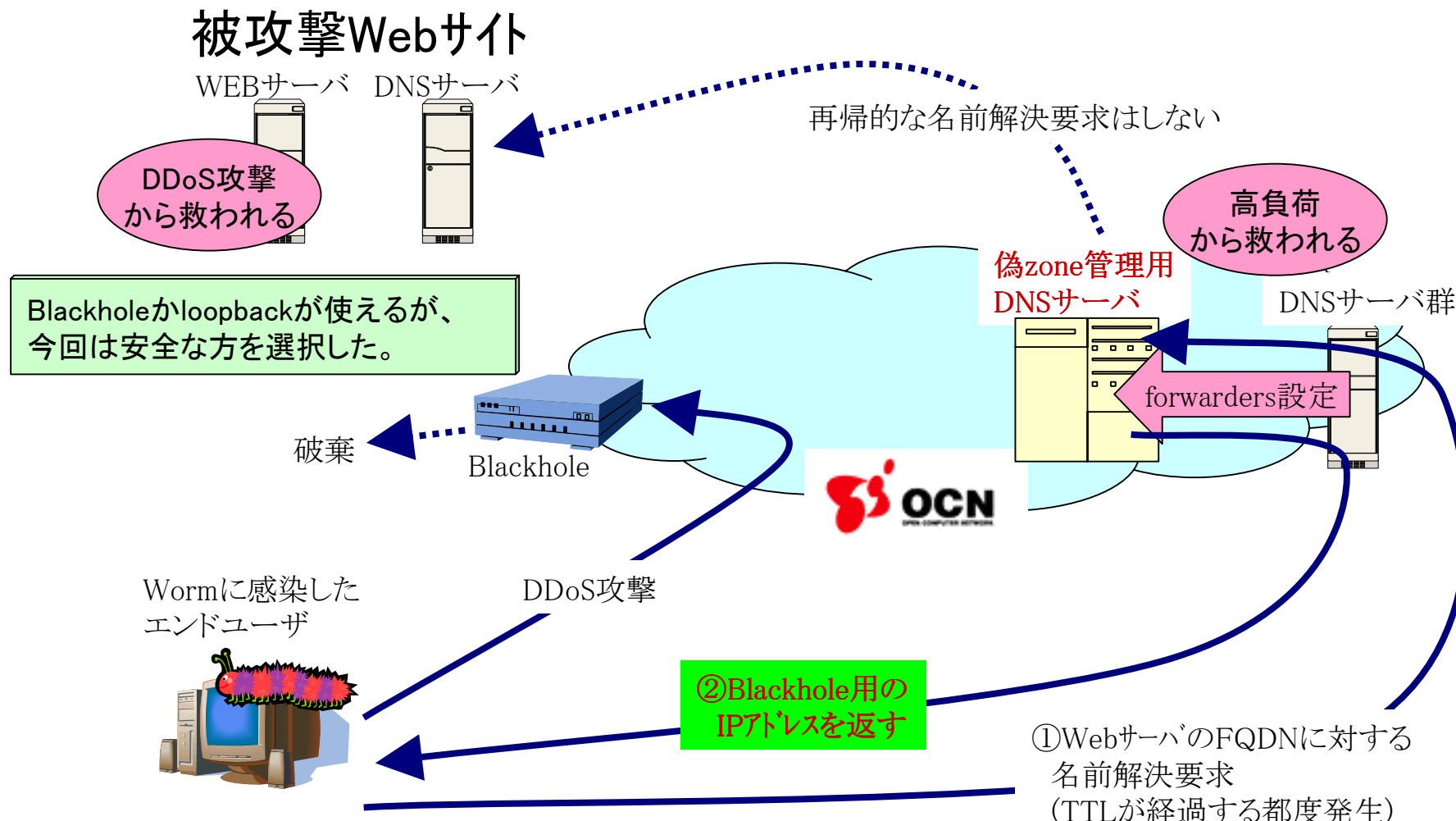
# 当日起きたできごと

- 被攻撃サイトの管理者はAレコードを削除することでDDoS攻撃を回避することができる。
- でも、各ISP側DNSサーバへの影響が非常に大きいからやらないで！

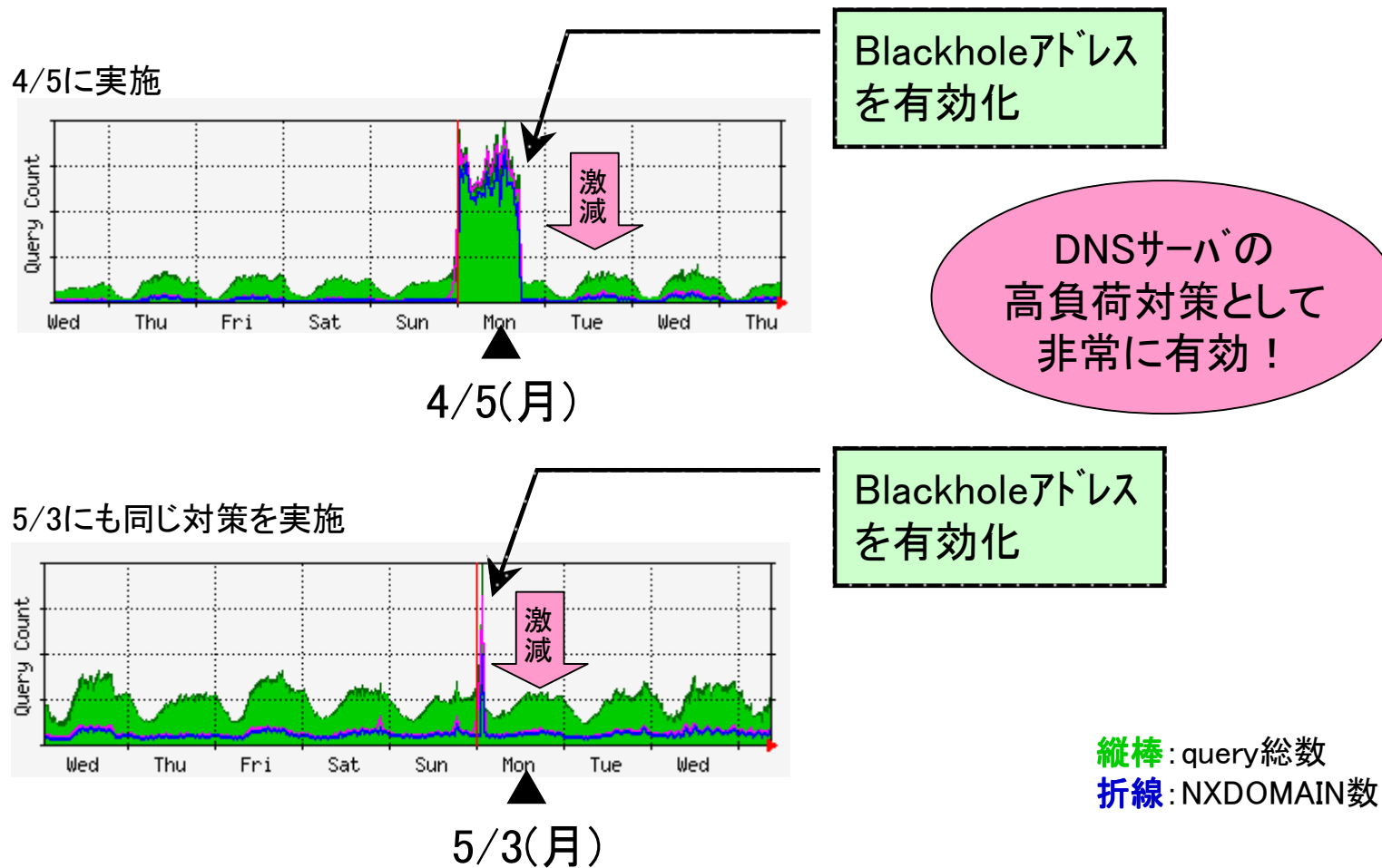
# まず該当ドメイン処理用サーバをたてたが



# そしてBlackholeアドレスの応答を開始...



# Blackhole導入でquery数激減!



## 勝手に偽の情報を応答してもいいの？

- ISP側の都合だけで勝手にAレコードを変更すると、各Webサイト管理者の意図に反してしまうことになりかねない。
- 今回はWebサイト側ですでにAレコードが無効化されていたため、ISP側で偽の情報を応答しても社会的な影響は大きくないと考える。

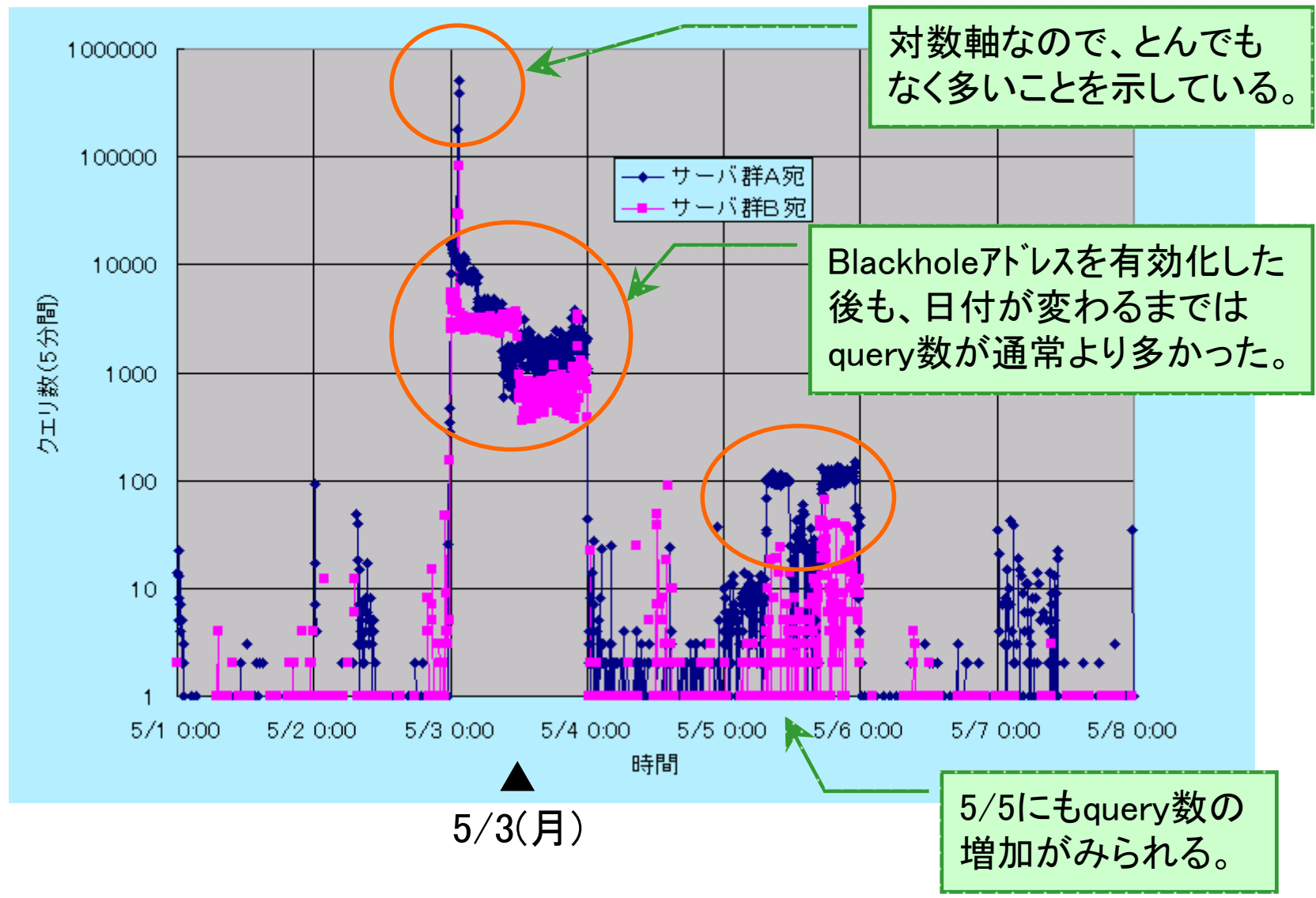
## Antinny.K発生は4/4や5/5のはずでは？

- Antinny.BやAntinny.Jが第1月曜日に発病するらしい、との情報も... (確たる証拠はつかめていない)
- 今後はワクチンメーカーとISPが密接に連繋して、Wormの詳細な挙動に関する情報を共有できる体制にしていきたい。

## 5月のquery状況を分析してみました

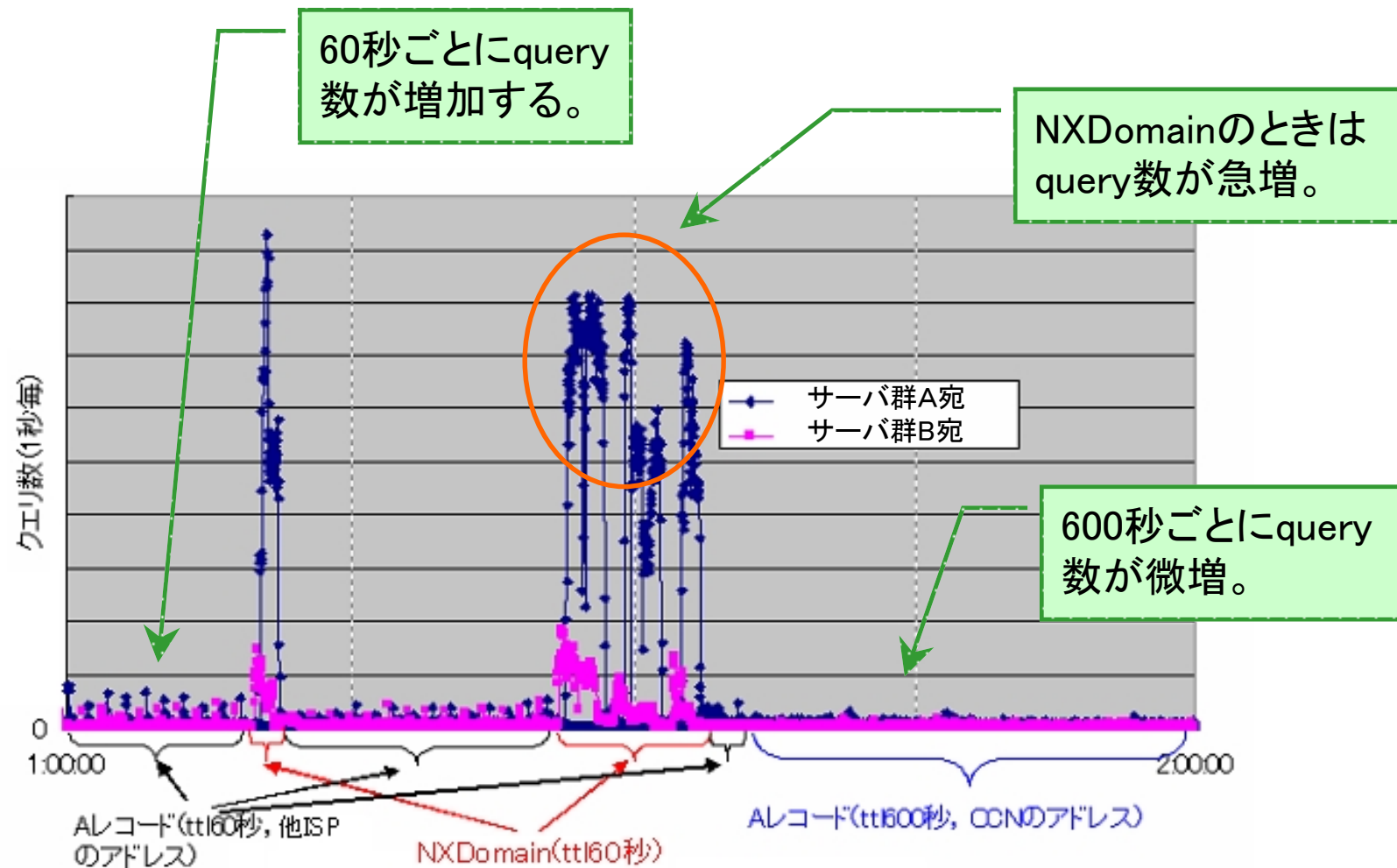
- クエリ数が最も多かったのは5/3
- 5/3 1:10am, 1:30am付近にスパイクが存在  
(次ページのグラフを参照)
- 上記ピークはACCS様側でNXDomainを返すようにした期間と一致
- 以降、"accsjp.or.jp"が含まれるクエリを対象にした解析を示す。

(調査:NTT情報流通プラットフォーム研究所)



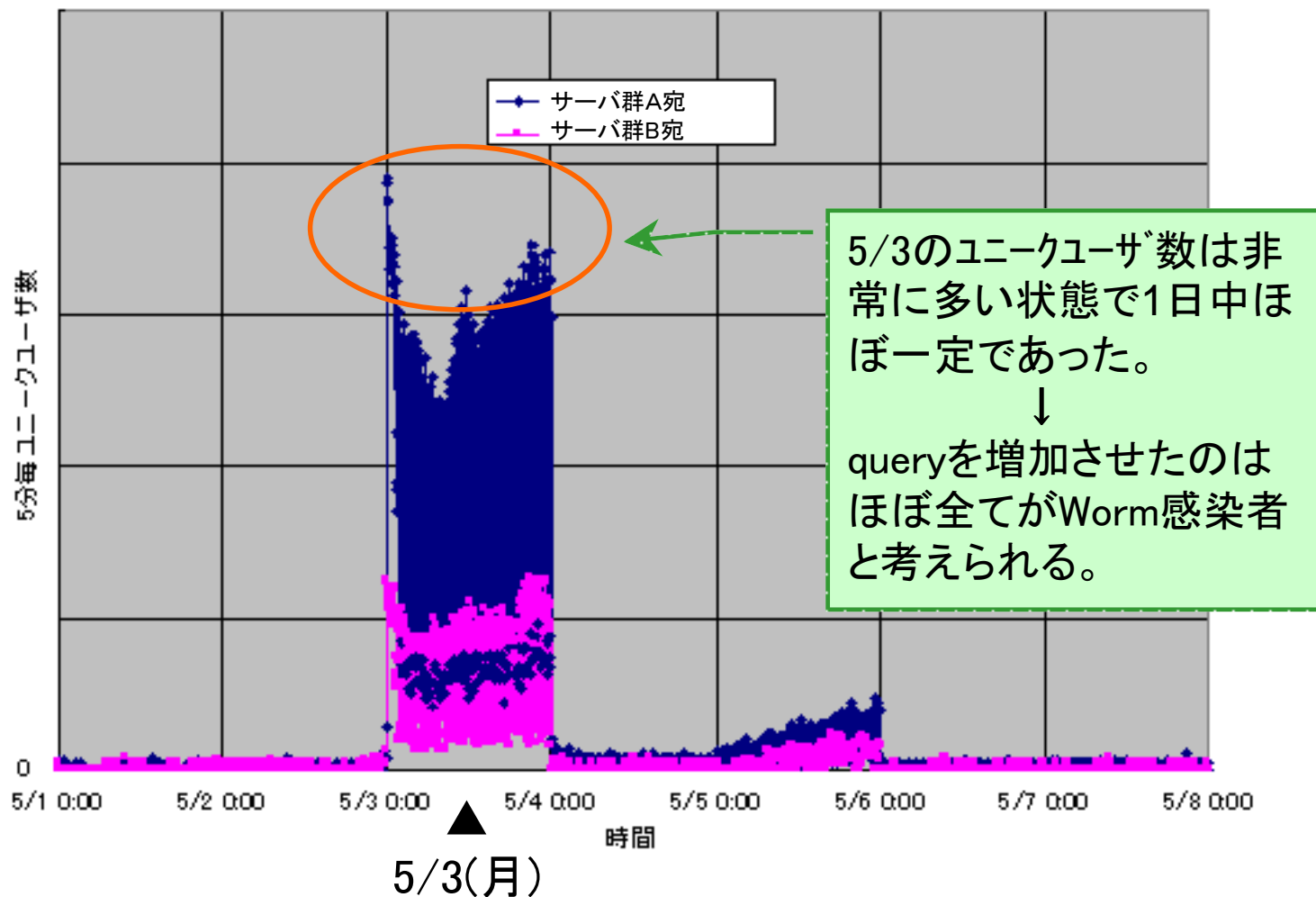
(調査:NTT情報流通プラットフォーム研究所)

# 5/3 0:00~1:00の1秒毎クエリ数



(調査:NTT情報流通プラットフォーム研究所)

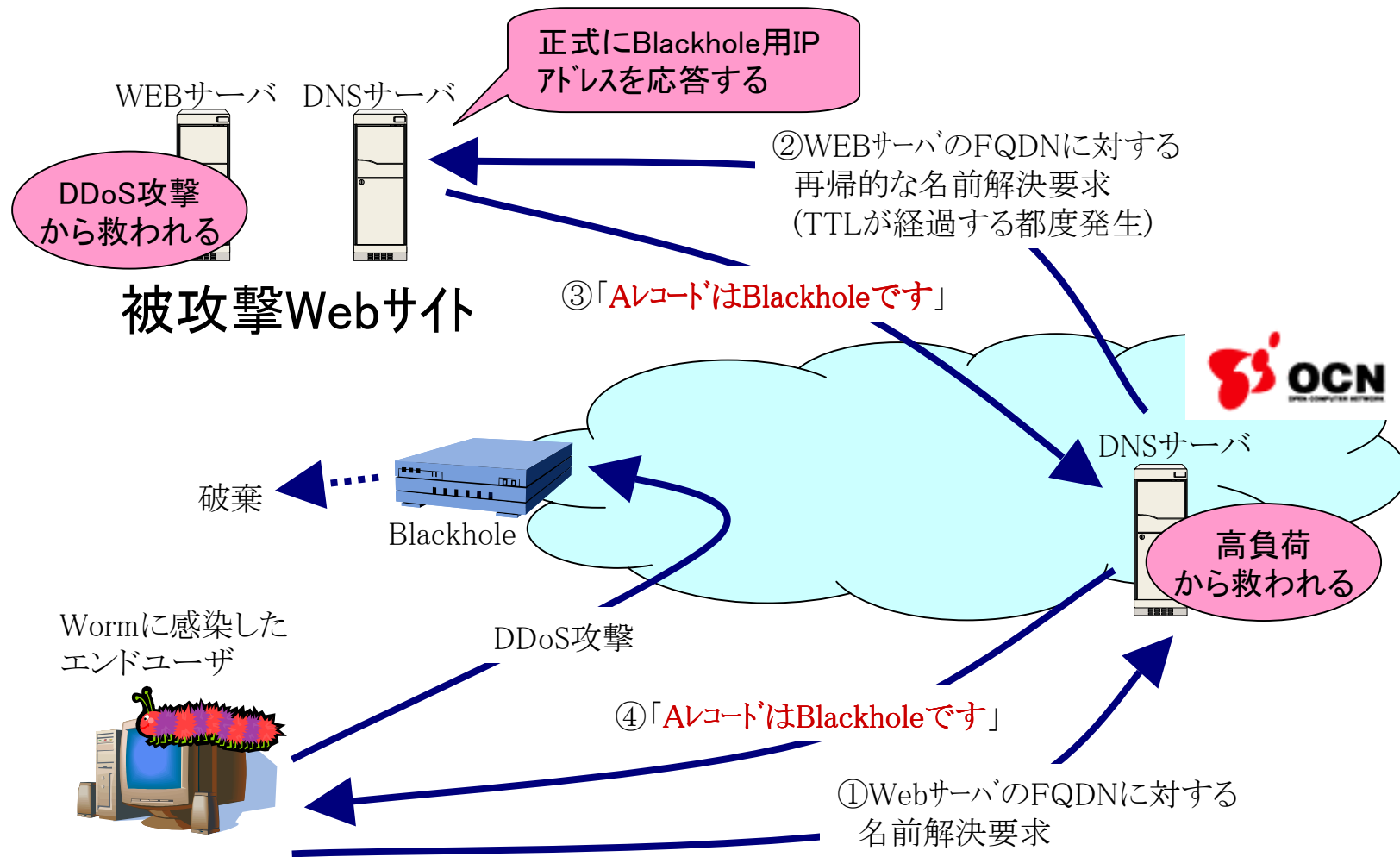
# 5/1~5/7一週間のユーザ数時系列



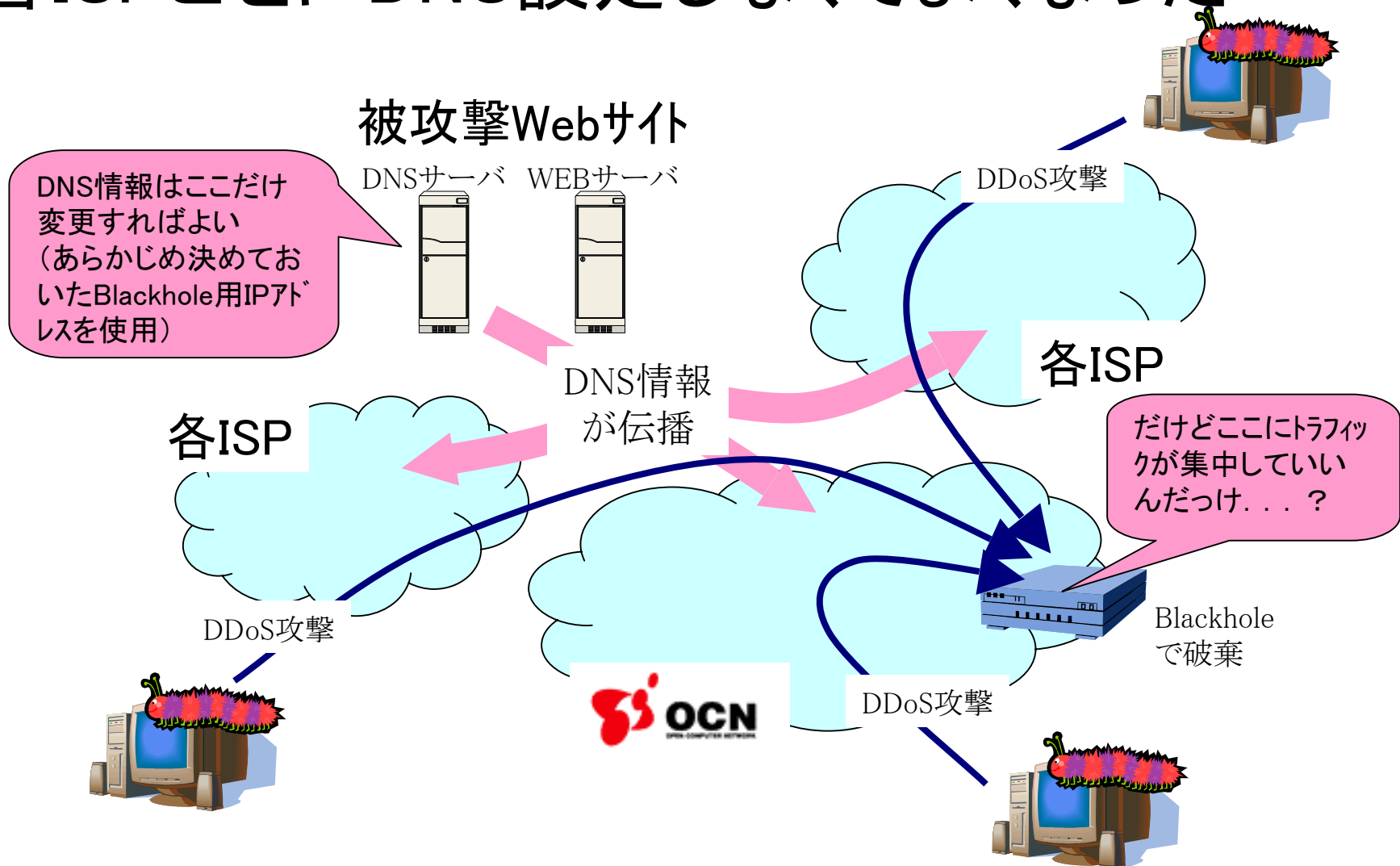
## 6月も7月も、これからも活動期がくる

- 他のISPでも同様の問題を抱えているはず。
- 各ISPが所有する全DNSサーバで偽応答を設定する、というのは結構大変な作業。
- では、どうすればよいか？

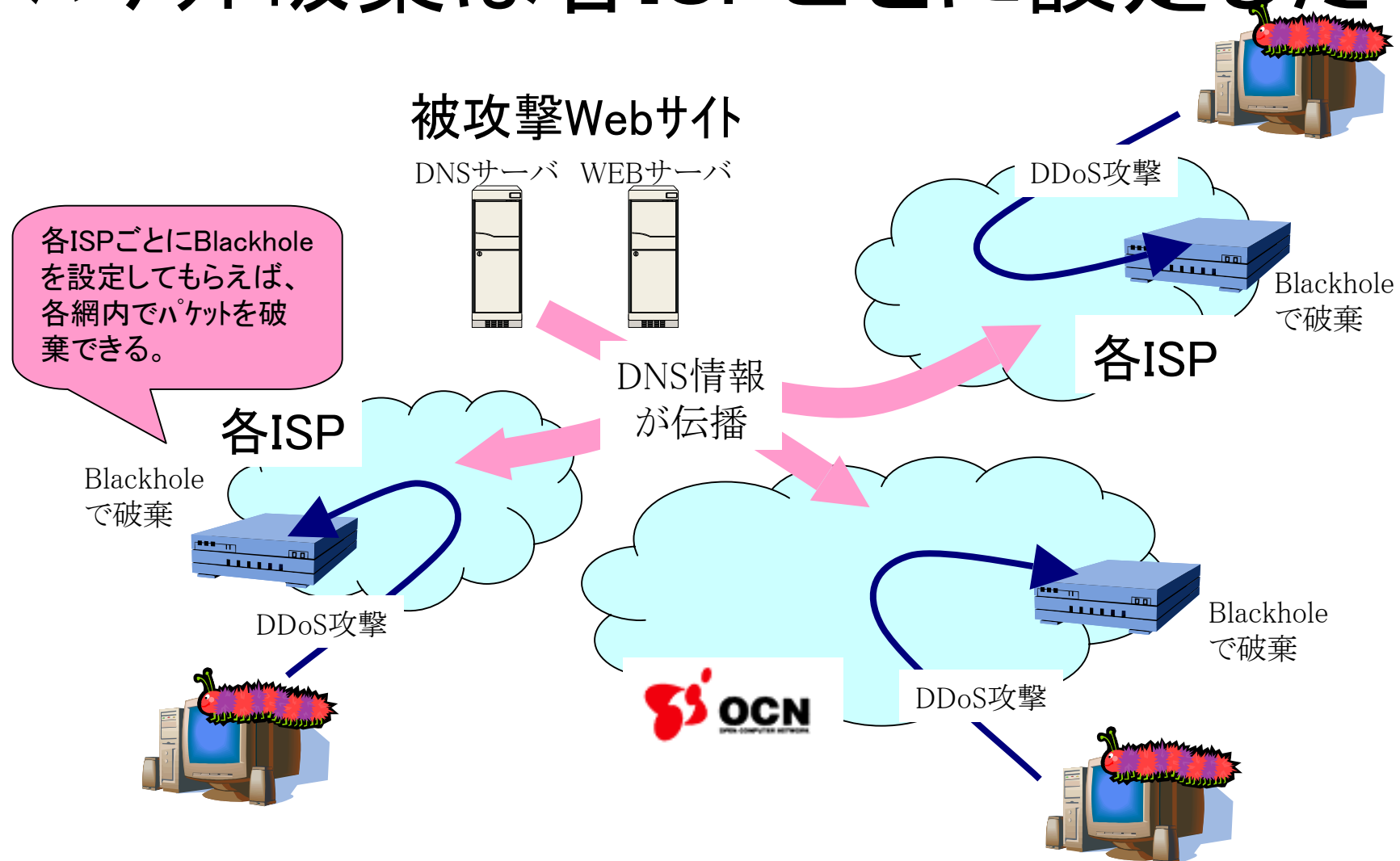
# サイト側にBlackholeの応答を依頼



# 各ISPごとにDNS設定しなくてよくなった



# パケット破棄は各ISPごとに設定した

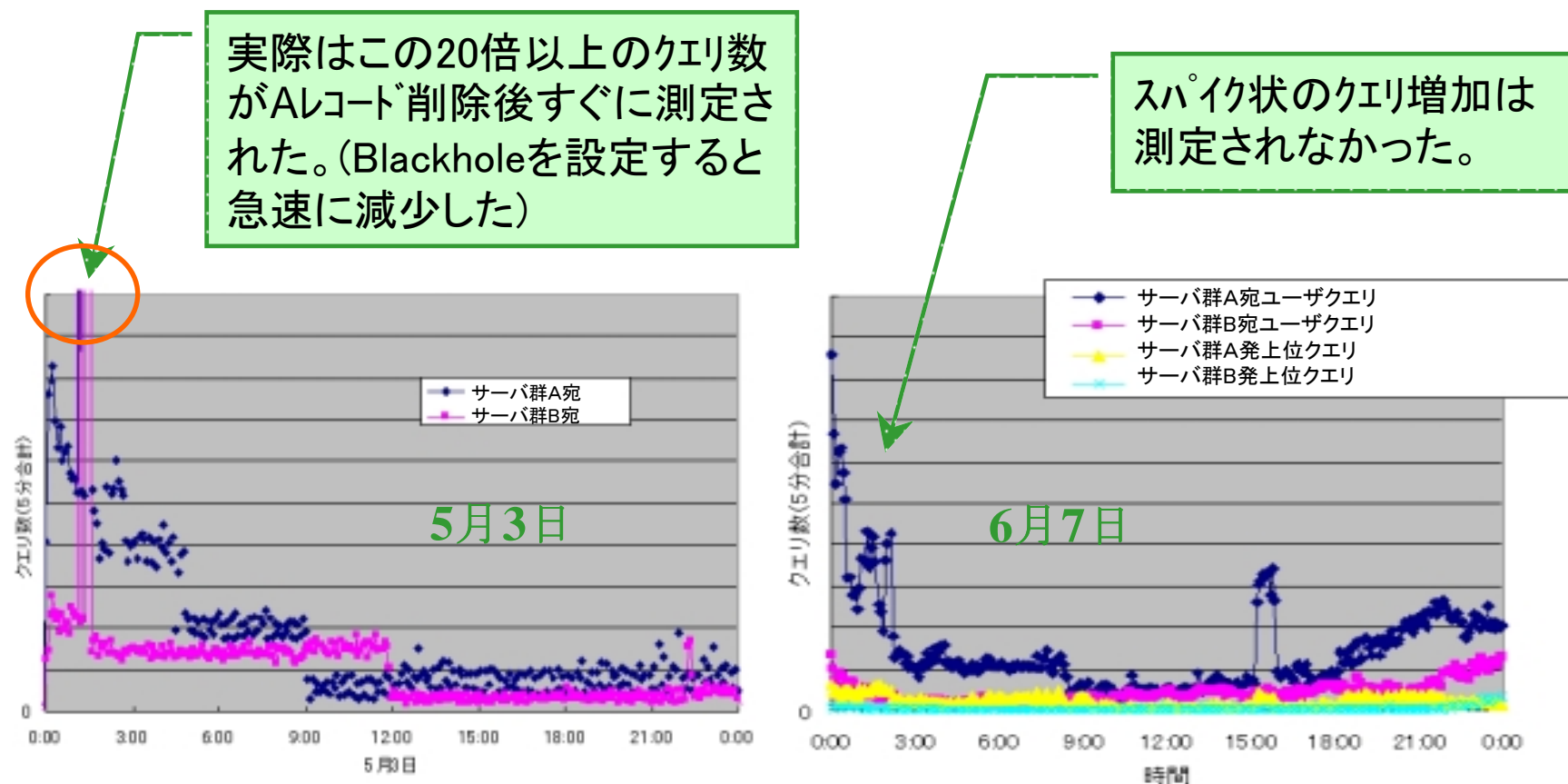


# 他ISPの協力で実現

- Telecom-ISAC Japanを通じて連繋。  
<https://www.telecom-isac.jp/>
- 今回はBlackhole用IPアドレスをOCNのアドレス帯から一時的に用意した。
- 各ISPではそのIPアドレス宛のパケットを自ネットワーク内で破棄するように設定。

(調査:NTT情報流通プラットフォーム研究所)

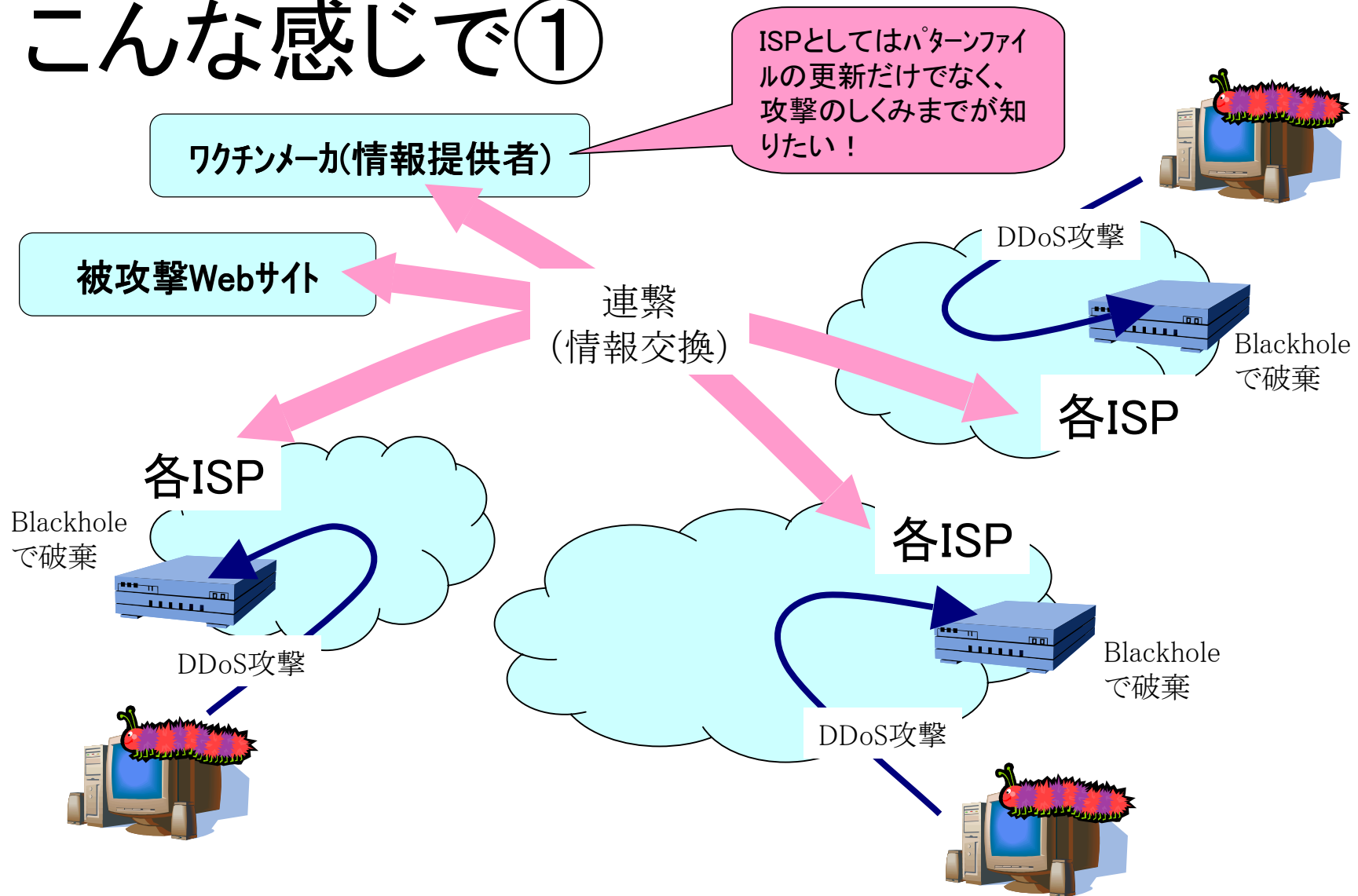
# 5月の対策よりも効果的でした



# 今後の話①

- 6月・7月の対処方法が大変効果的でした。他のISPさんも一緒にやってみませんか？
- 今後は、  
(a)被攻撃サイト (b)ISP (c)ワクチンメーカー  
が連繋してDDoS対応ができるよう、脅威情報の集約と展開に関する新しいスキームを構築しませんか？

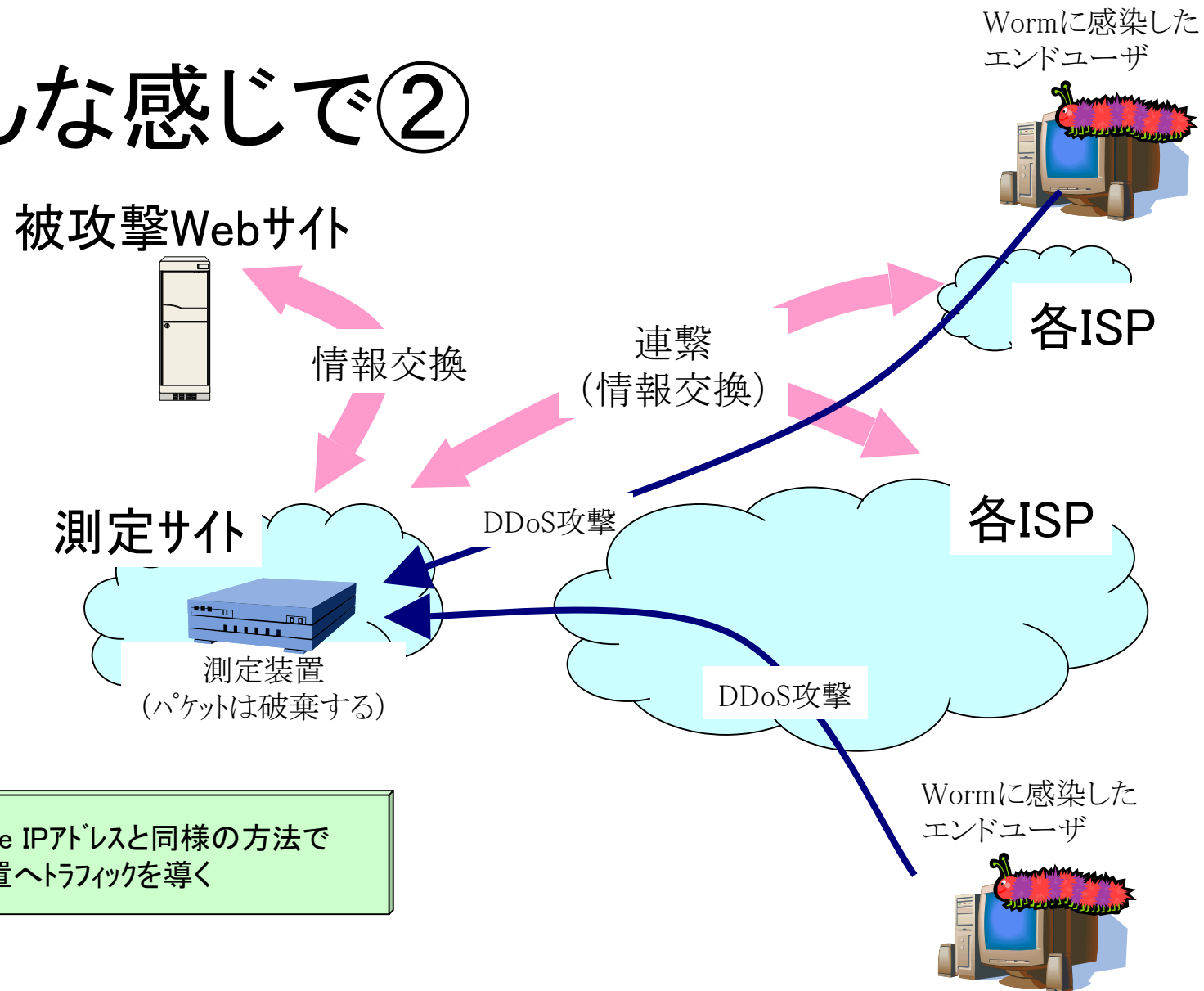
# こんな感じで①



## 今後の話②

- 将来的にはBlackholeアドレスのところにDDoS状況を測定できる装置を設置できれば、
- Wormの挙動解析やISPのエンタープライズ対応に役立てることが可能になる。
- 測定装置をどこに置くのか、誰が解析するべきかという点については整理が必要。

# こんな感じで②



Blackhole IPアドレスと同様の方法で  
測定装置へトラフィックを導く

## 今後の話③ 最後に紹介させていただきます...

- WebサーバへのDDoSトラフィックを分散し、性能面でDDoS耐性を高めるためにはAkamai技術の導入も有効かと...
- ちなみに弊社でも以下のサービスをご提供いたしております。

**「Broadband CDN powered by Akamai」**

**<http://www.ntt.com/cdn/index.html>**

# NWでのDDosパケット破棄方法

## ① 各エッジルータでターゲットIPをFilter!

でも処理能力が厳しいかも……

## ①' 各エッジルータでターゲットIPをNullStatic!

でもIPが変わる度に変更はしんどい……

## ② BlackholeルータでターゲットIPを引き込む!

一手に引き受けてNWは大丈夫??……

## ③ BGPアナウンスルータでターゲットIPをBGPでアナウンス! + 各エッジルータでNullStatic!

参照 : <http://www.nanog.org/mtg-0402/morrow.html>

# NWでのDDosパケット破棄方法

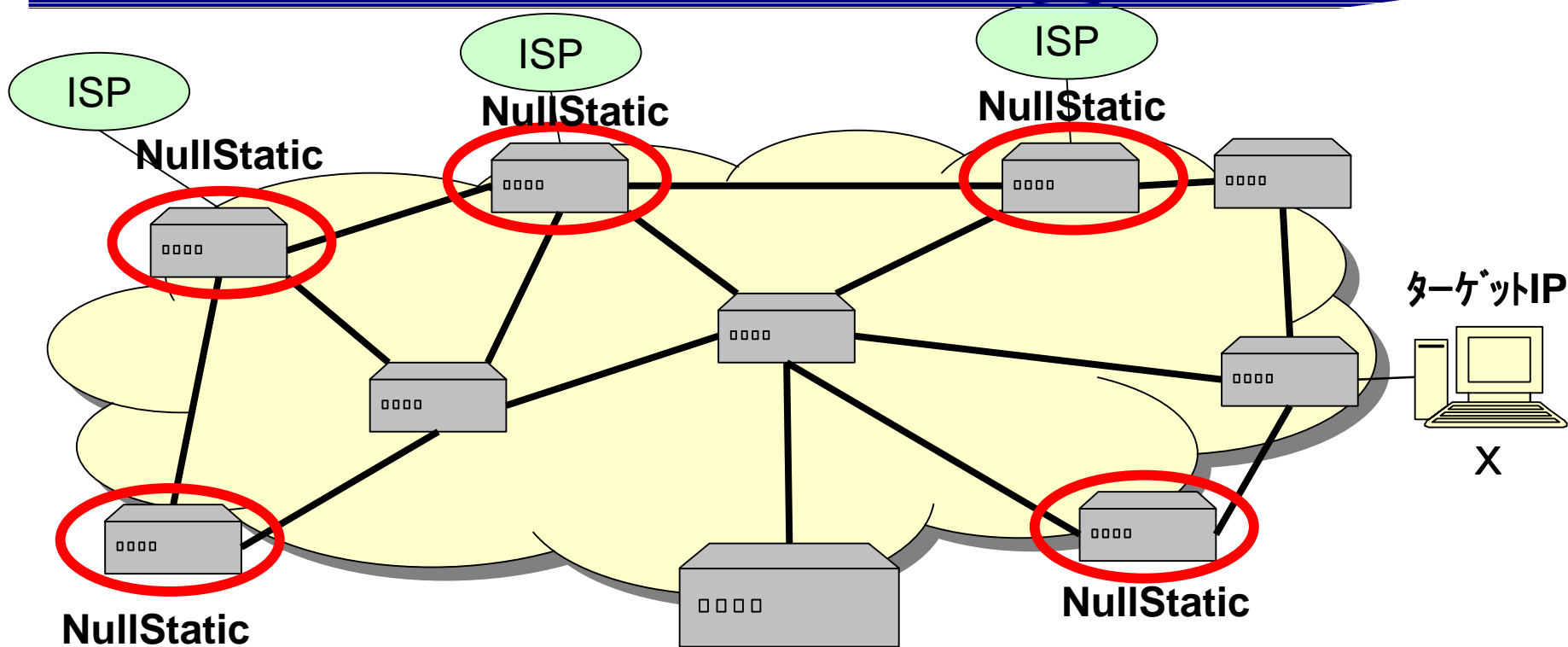
## ③BGPアナウン斯拉ータでターゲットIPをBGPでアナウン!

### +各エッジルータでNullStatic!



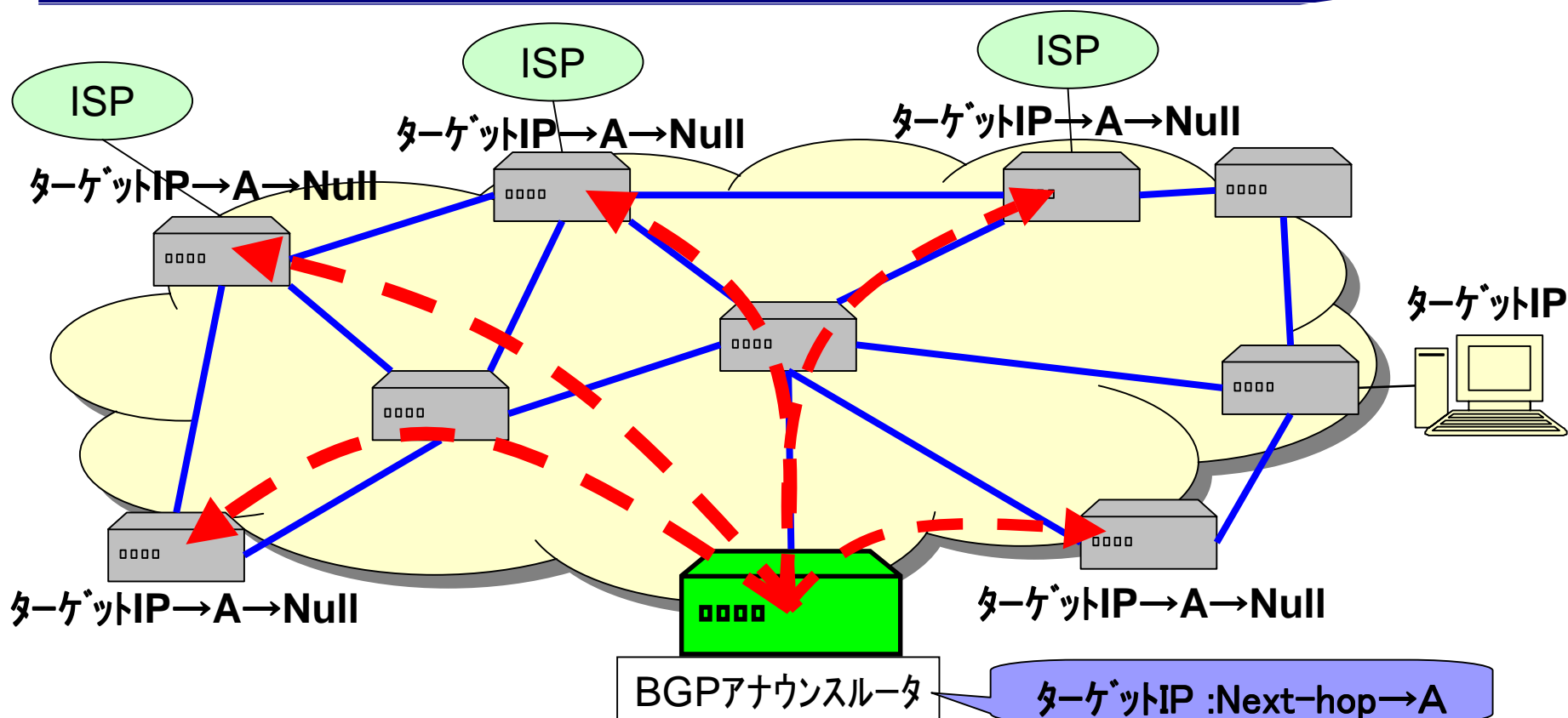
# NWでのDDosパケット破棄方法

①エッジにあるBGPルータに未使用IP (=A) へNullStaticを書きます。



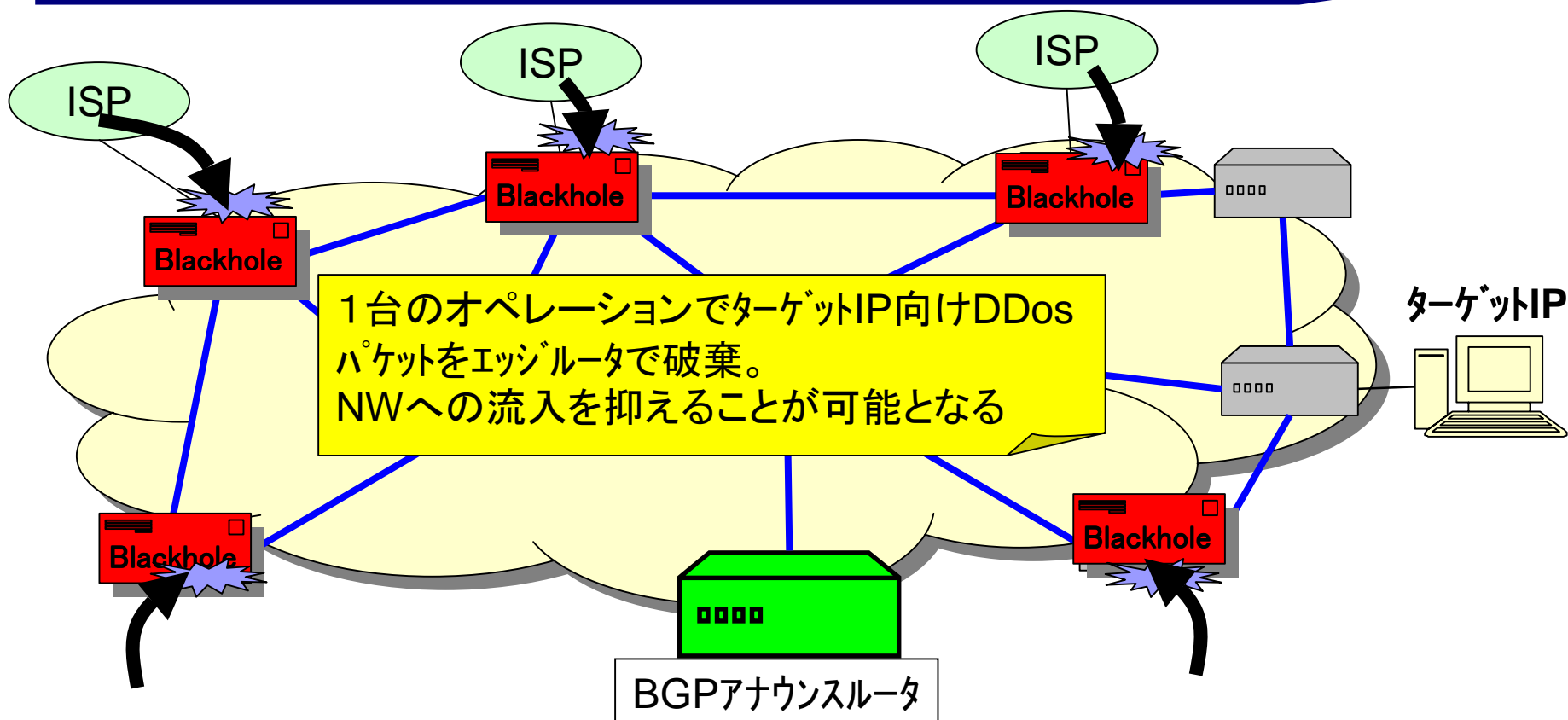
# NWでのDDosパケット破棄方法

②BGPアナウン斯拉ータにて、ターゲットIPのnext-hopを①で設定した未使用IPに付け替えてアナウンス開始します。



# NWでのDDosパケット破棄方法

③BGP経路受信したルータがたちまちBlackholeルータへ変身します。



# パケット破棄方法のまとめ

方式	メリット	デメリット
①ターゲットIPをFilter	<ul style="list-style-type: none"> <li>・LOGで何か分かる?</li> <li>・網内帯域は圧迫無</li> </ul>	<ul style="list-style-type: none"> <li>・ターゲット毎に再設定</li> <li>・処理能力が不安</li> </ul>
①`ターゲットIPをNULL(Discards)	<ul style="list-style-type: none"> <li>・網内帯域は圧迫無</li> <li>・処理はACLより軽い</li> </ul>	<ul style="list-style-type: none"> <li>・ターゲット毎に再設定</li> <li>・破棄パケット観測NG</li> </ul>
②ターゲットIP引込	<ul style="list-style-type: none"> <li>・ターゲットが変わっても簡単に変更</li> <li>・破棄パケット観測可能</li> </ul>	<ul style="list-style-type: none"> <li>・帯域圧迫</li> <li>・自分が死亡</li> </ul>
③BGPでアナウンス+エッジでNULL	<ul style="list-style-type: none"> <li>・ターゲットが変わっても簡単に変更</li> <li>・網内帯域は圧迫無</li> </ul>	<ul style="list-style-type: none"> <li>・破棄パケット観測NG</li> <li>※nanogでは続き有</li> </ul>

# DDos/WORM発生時の注意ポイント

- CPU的に・・・(攻撃(伝染)時に大量パケットをだすので)
  - ・ bps (トラフィック量)
  - ・ pps (パケット数)

## ● 物理帯域圧迫していませんか？

特定のIFに対してトラフィックが膨大となり、パケットdrop等が発生

## ● パケットピンポンしていませんか？

帯域は大したことないけれどパケット数が膨大な場合がある

icmpTimeExceeded数を監視すればどこで発生しているか特定は可能

# DDos/WORM発生時の注意ポイント

- **メモリー的に・・・**（攻撃（伝染）時にランダムな所を狙うので）
  - ・NATセッション数
  - ・ルーティングCache数

## ●セッションオーバーしていませんか？

NATテーブルが上限に来て新規セッションは接続できないかも

## ●Cacheテーブルが膨れていませんか？

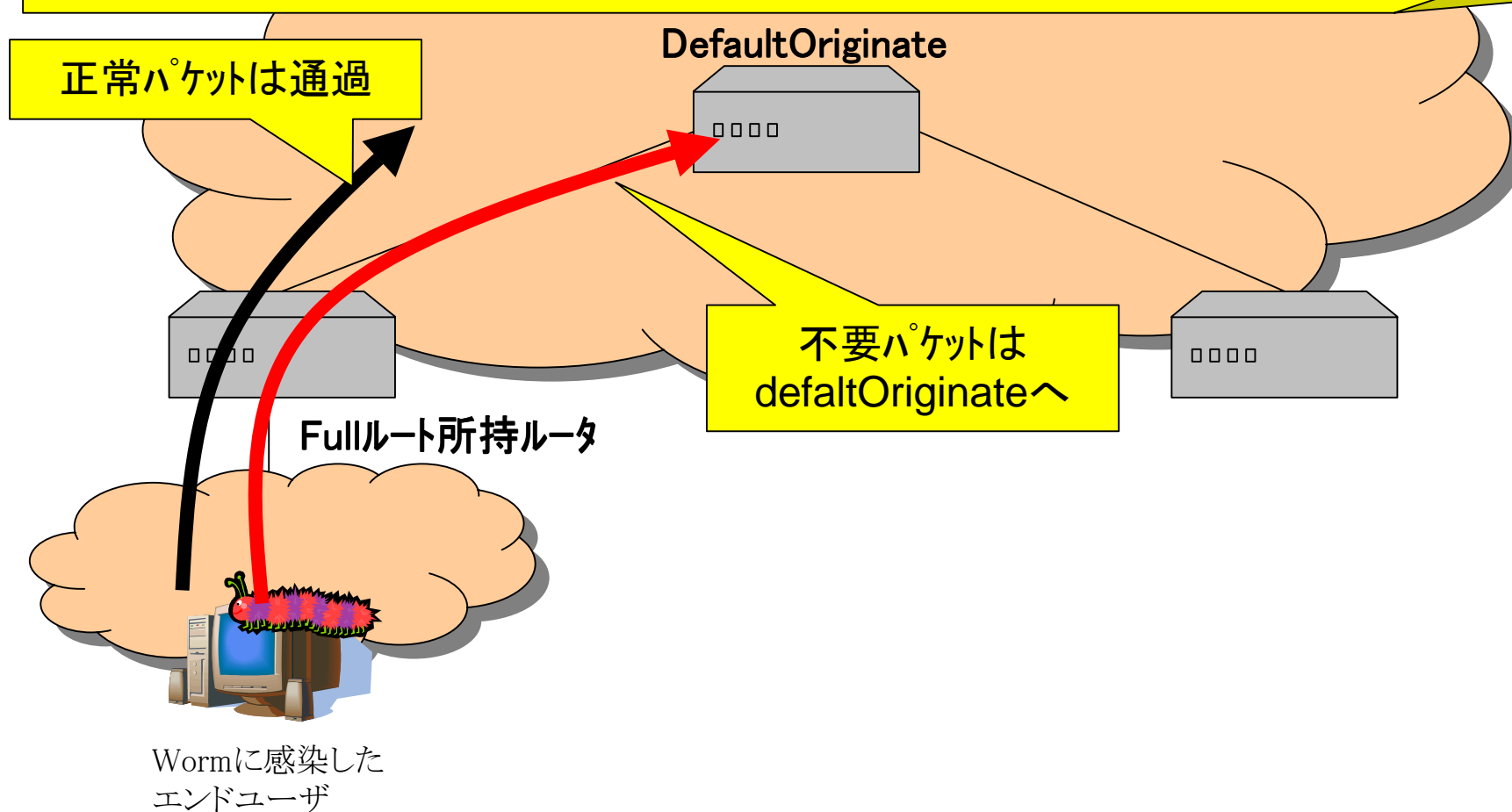
Cacheへのエントリー数によりメモリ不足かも

## ●CacheのHIT率が落ちていませんか？

枯渇することにより処理性能が落ちてるかも

# (参考) 不要パケットを用いたワーム観察方法

- ・ワーム感染のパケットは感染活動のため不特定IPへのspoofingを行う傾向
- ・Fullなルートを持ったルータではDefaultに向かう通信はありえない



# (参考) 不要パケットを用いたワーム観察方法

- ・Fullルートを持ったルータに渡りを設置し、defaultルートを書いてトラフィック迂回
- ・SW等でIDS向けにミラーし、パケットmonitorを実施

