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

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)

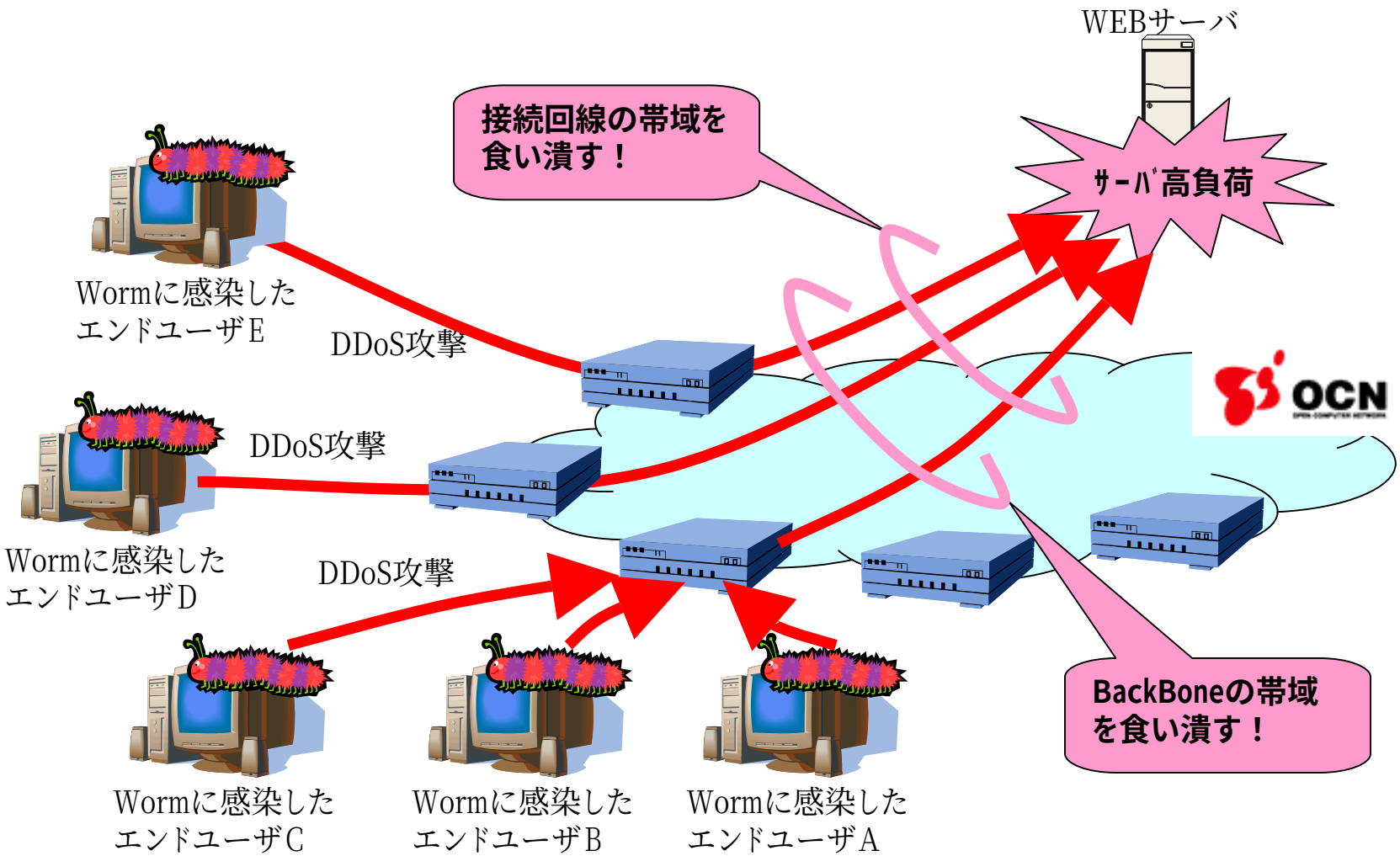
Netskyとは

- **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。**

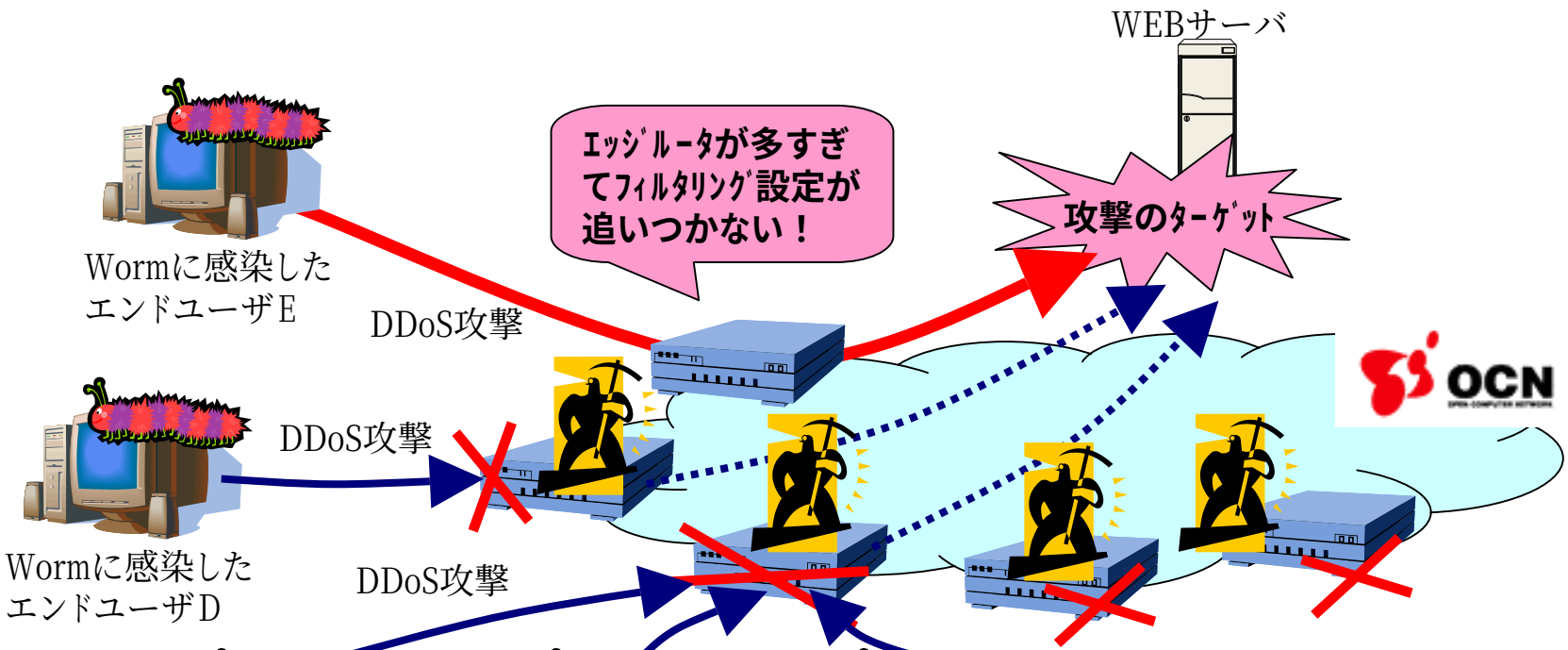
  http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.Q&VSect=T

  (トレンドマイクロ株式会社様のページ)

WormによるDDoS攻撃



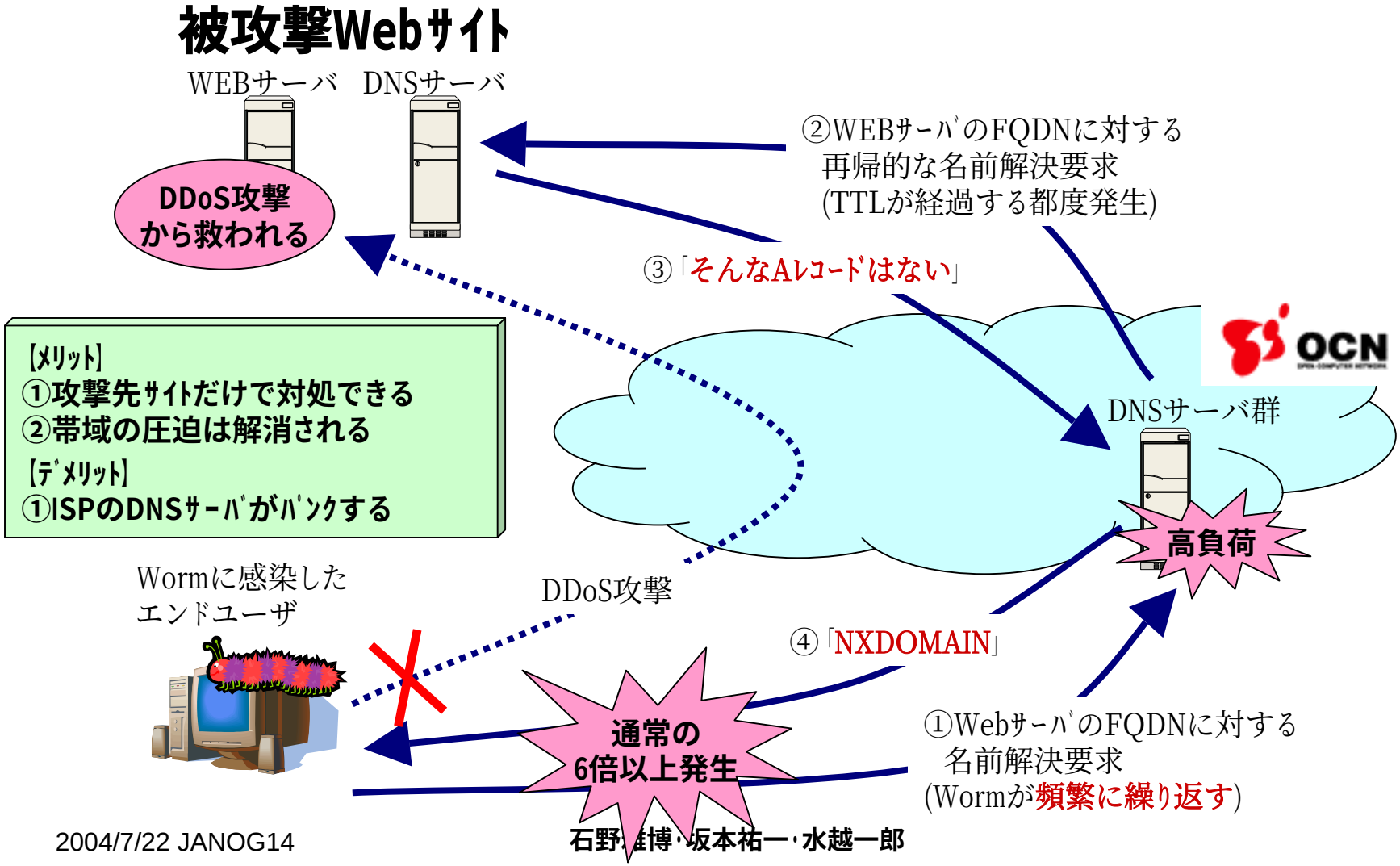
もしfilteringで立ち向かうと．．．



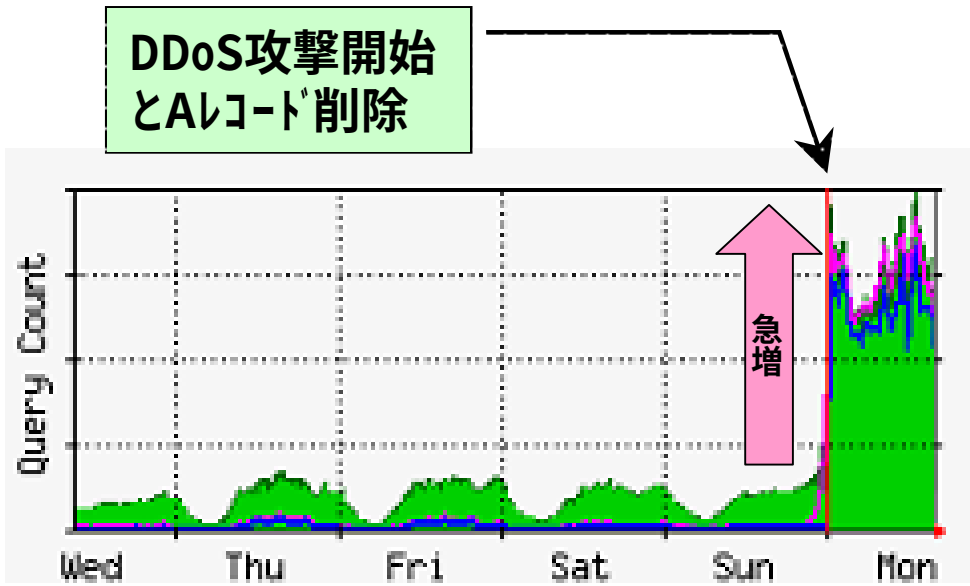
【メリット】
①ISP側だけで対処できる

【デメリット】
①一般的に、設定してもきりがない
→ 回避策については後半で…

サイト側でAレコードを削除すると．．．



ISP側DNSではquery処理が急増



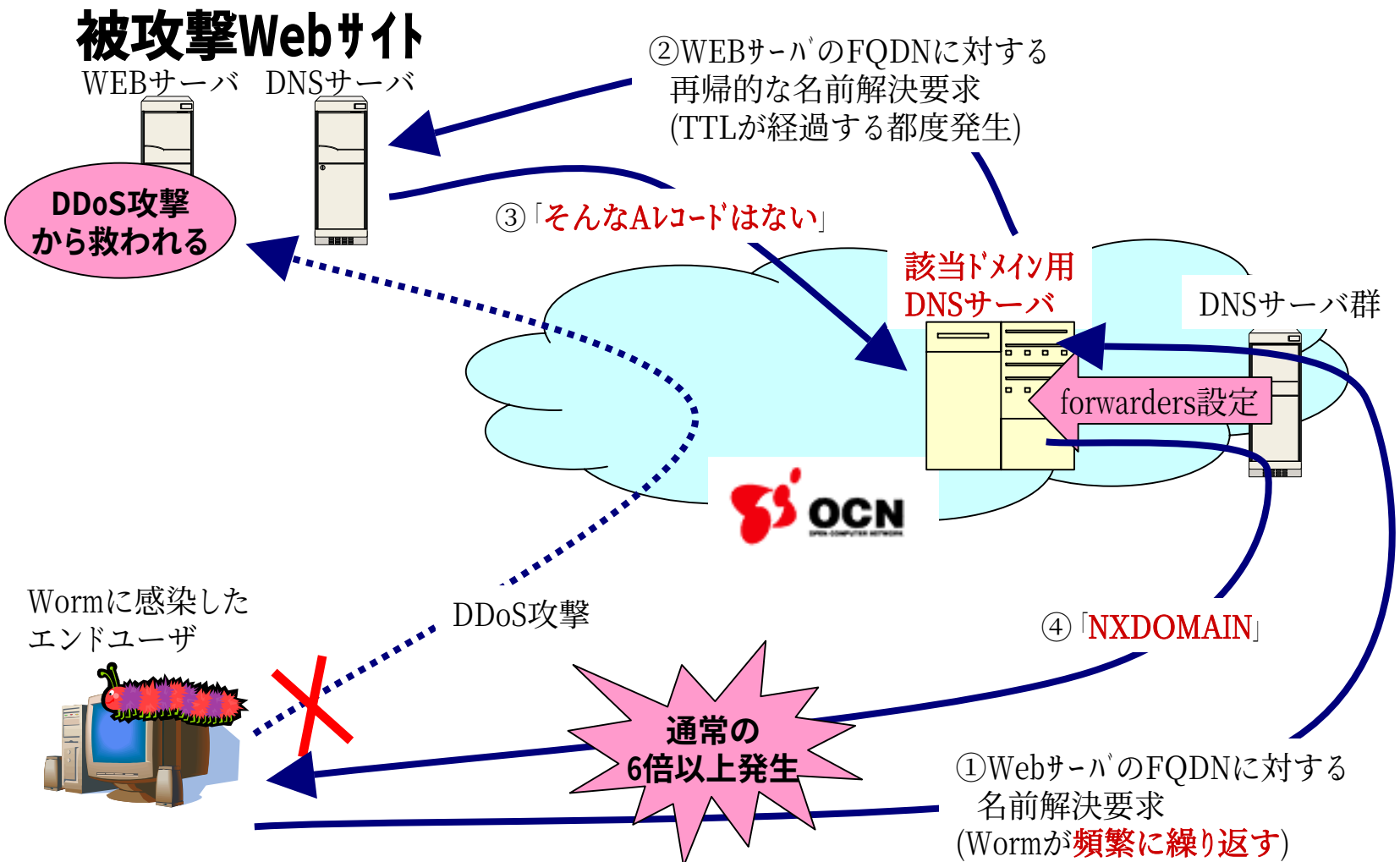
縦棒：query総数
折線：NXDOMAIN数

4/5(月)
Antinny活動日

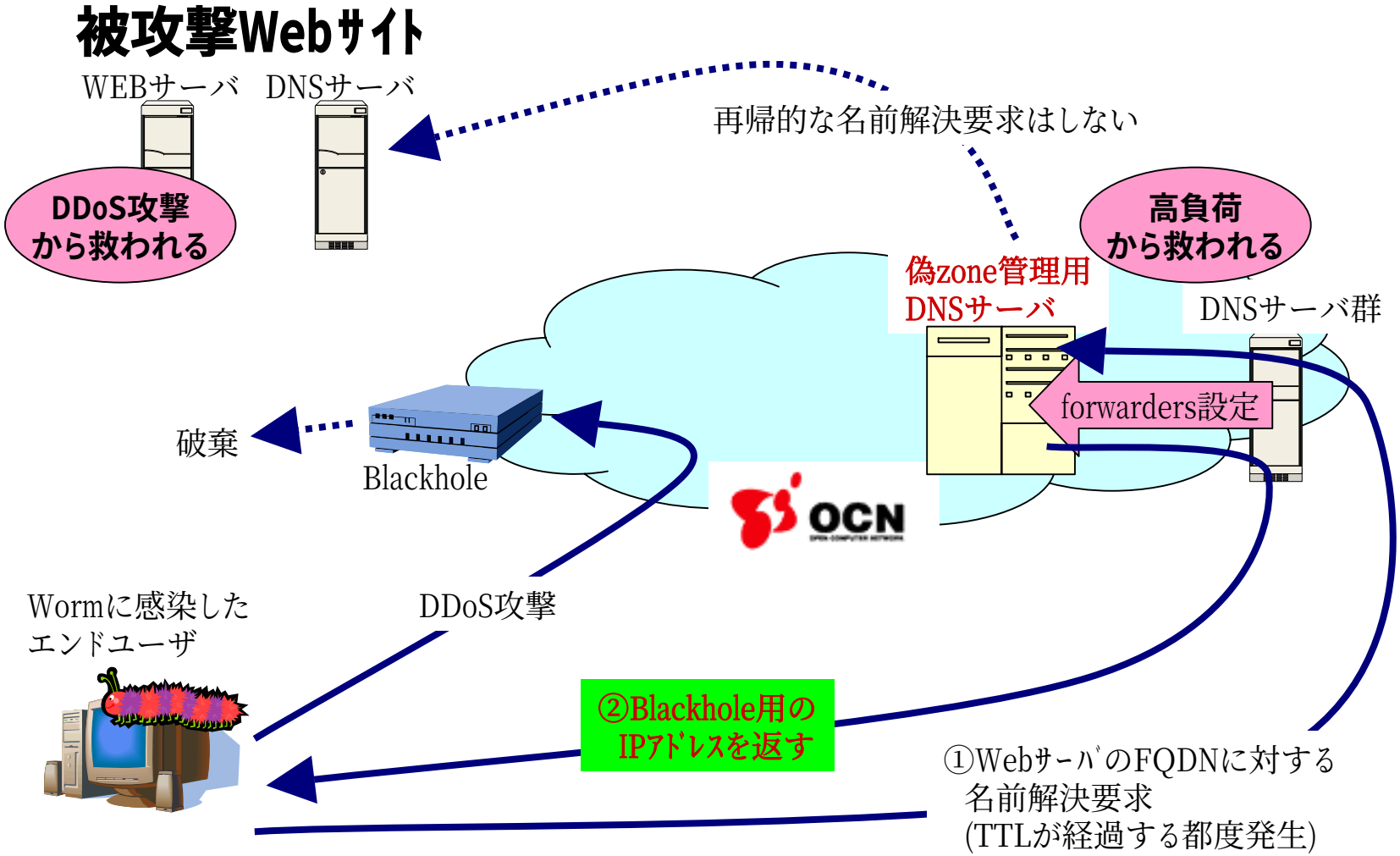
当日わかったこと

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

まずは該当ﾄﾞﾒｲﾝ処理用ｻｰﾊﾞをたてた

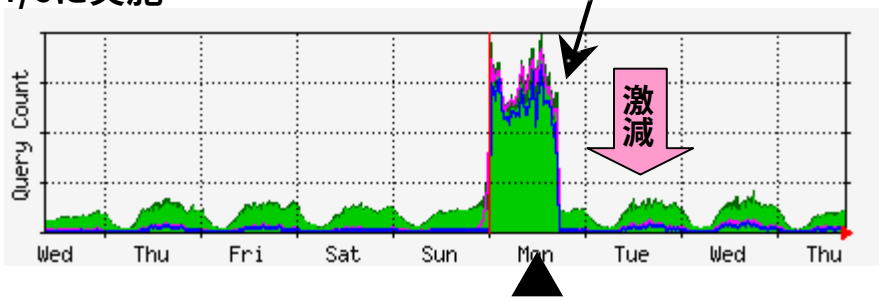


そしてBlackholeｱﾄﾞﾚｽの応答を開始．．．



Blackhole導入でquery数激減!

4/5に実施

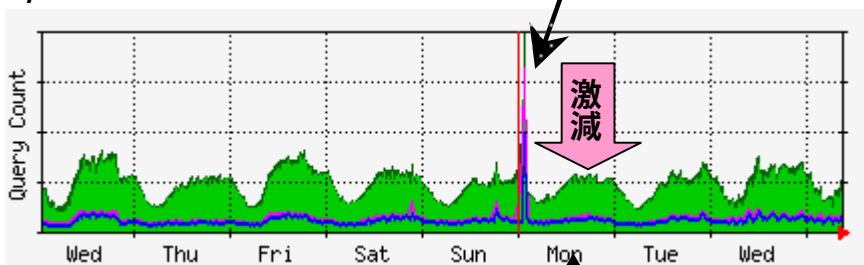


4/5(月)

Blackholeｱﾄﾞﾚｽを有効化

DNSｻｰﾊﾞの高負荷対策として非常に有効！

5/3にも同じ対策を実施



5/3(月)

Blackholeｱﾄﾞﾚｽを有効化

縦棒：query総数
折線：NXDOMAIN数

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ﾚｺｰﾄﾞを変更すると、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ﾚｺｰﾄﾞ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）

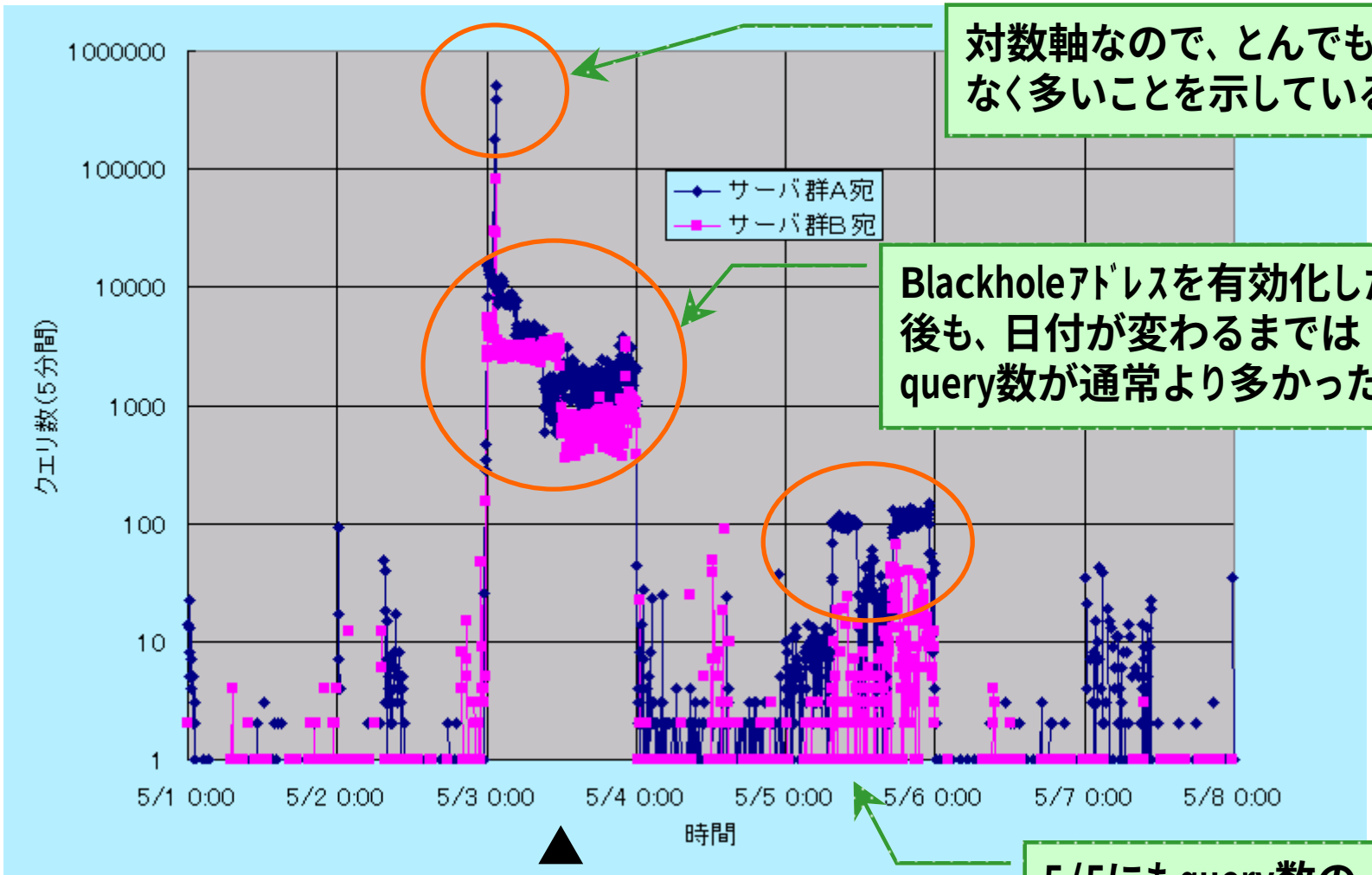
- 今後はﾜｸﾁﾝﾒｰｶとISPが密接に連繋して、Wormの詳細な挙動に関する情報を共有できる体制にしていきたい。

(調査：NTT情報流通プラットフォーム研究所)

5月のquery状況を分析してみました

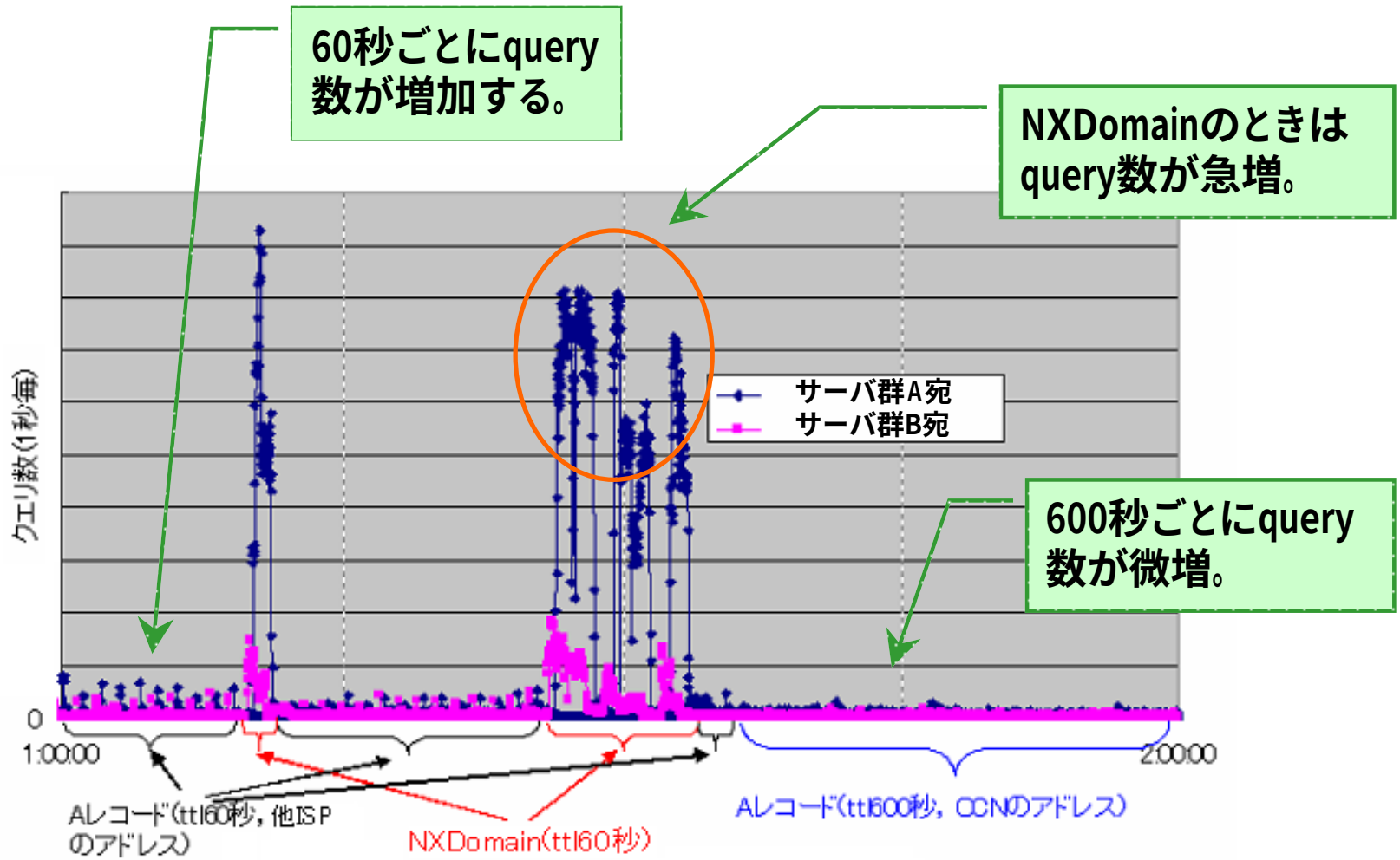
- クエリ数が最も多かったのは5/3
- 5/3 1:10am, 1:30am付近にスパイクが存在 (次ページのグラフを参照)
- 上記ピークはACCS様側でNXDomainを返すようにした期間と一致
- 以降、"accsjp.or.jp"が含まれるクエリを対象にした解析を示す。

(調査：NTT情報流通プラットフォーム研究所)



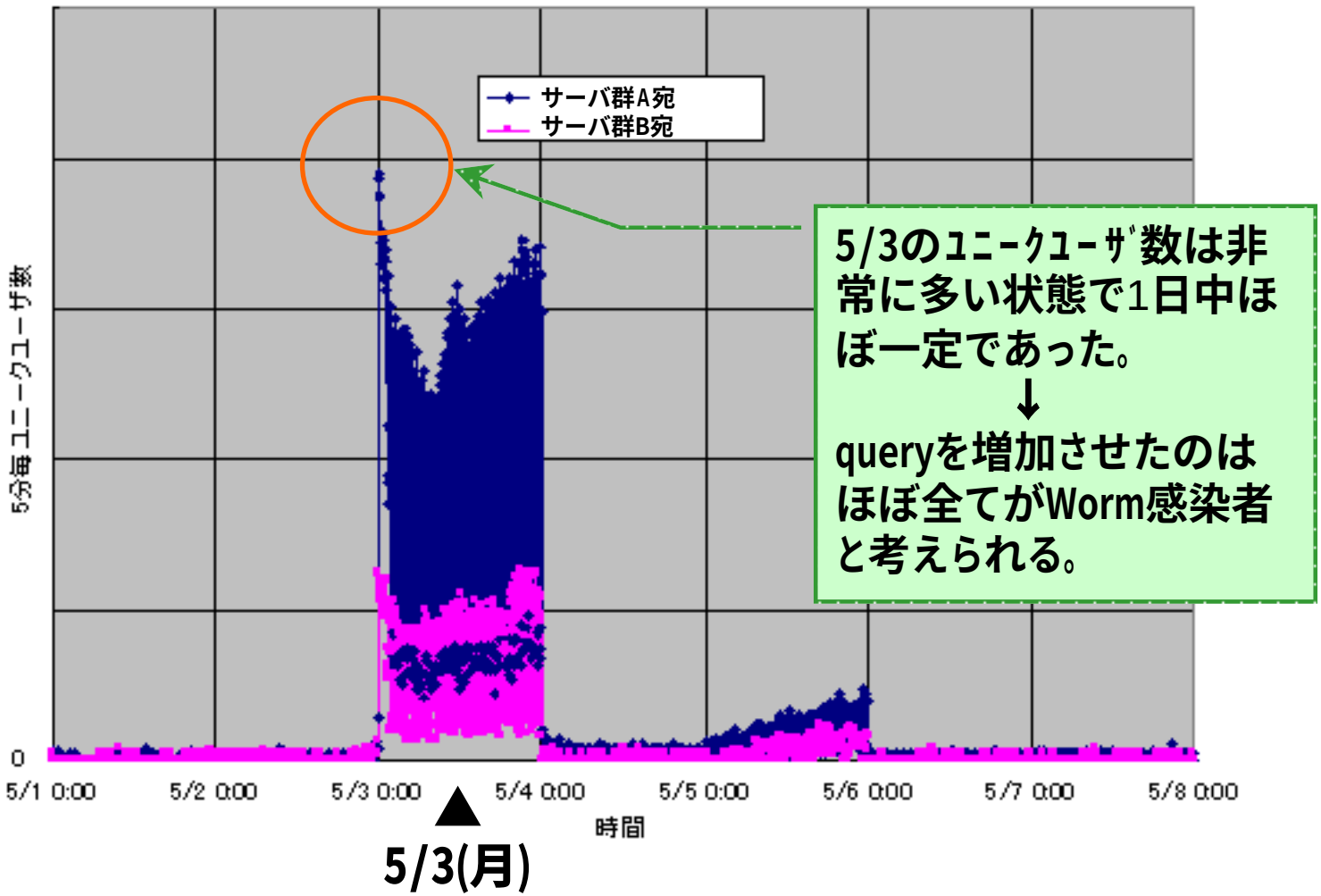
(調査：NTT情報流通プラットフォーム研究所)

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



5/3のﾕﾆｰｸﾕｰｻﾞ数は非常に多い状態で1日中ほぼ一定であった。

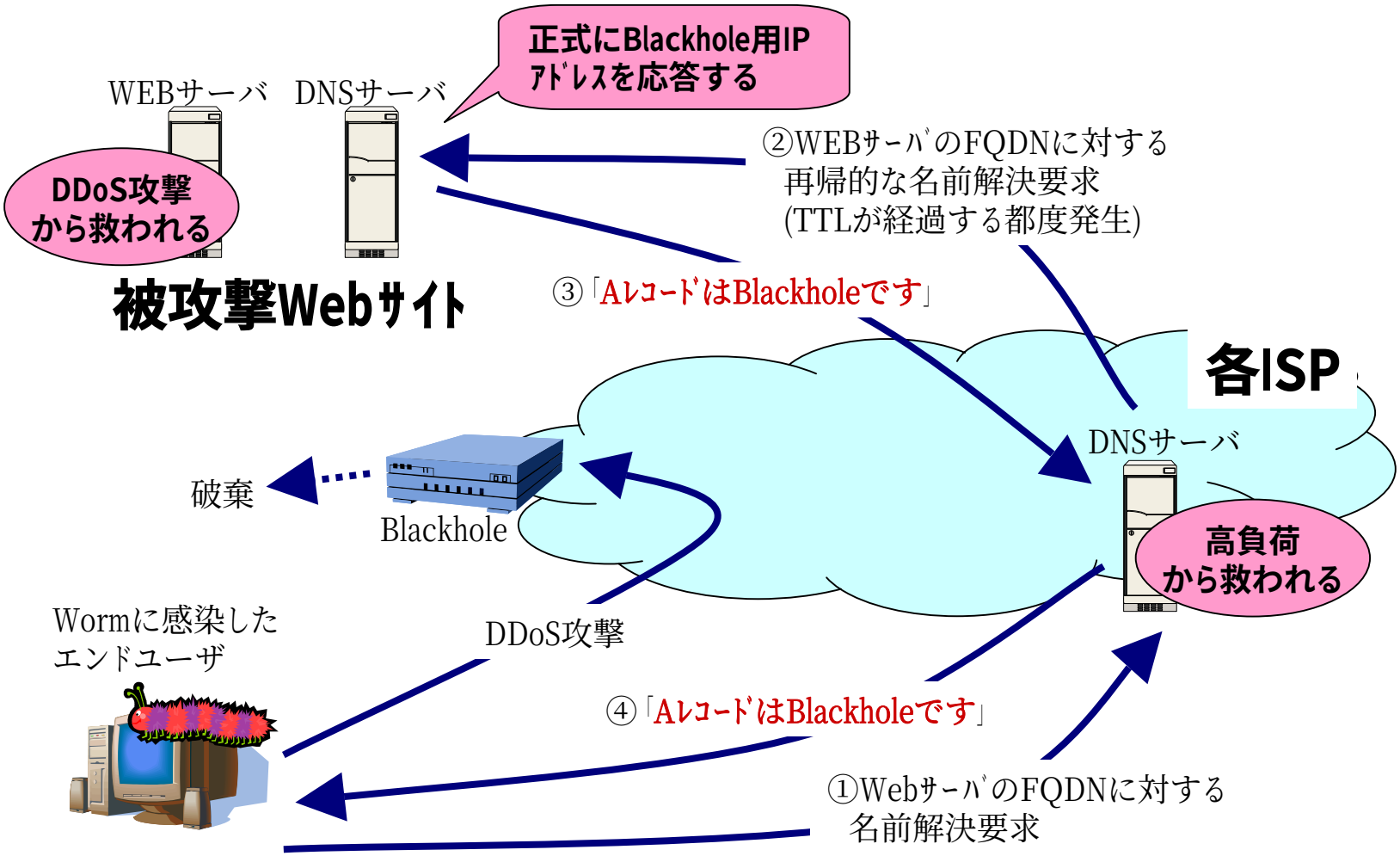
↓

queryを増加させたのはほぼ全てがWorm感染者と考えられる。

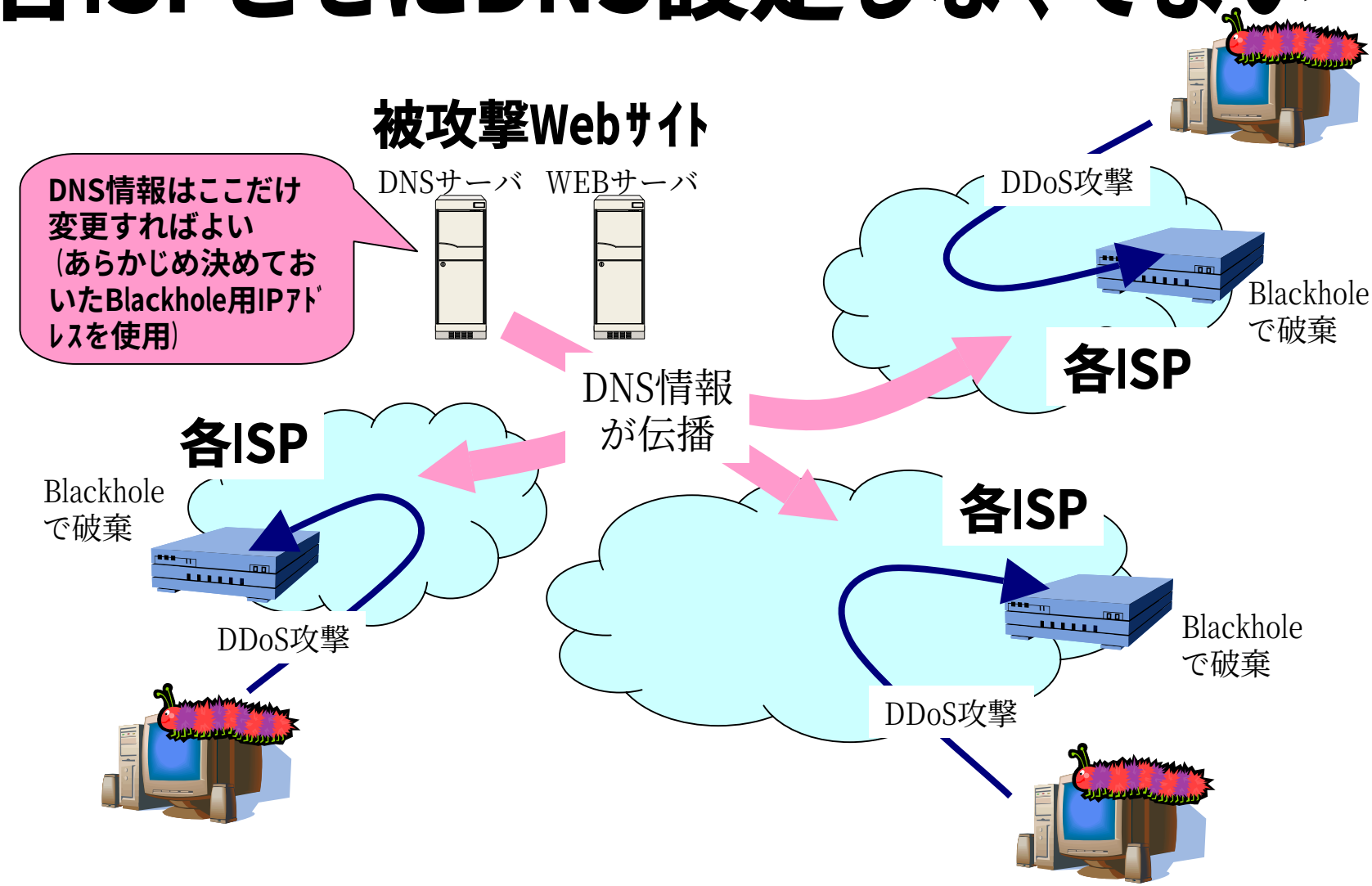
6月にも活動期がくる

- 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ｻｰﾊﾞ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？

攻撃先が自らBlackholeを名乗る



各ISPごとにDNS設定しなくてよい



攻撃先や他ISPの協力で実現

- Telecom-ISAC Japanを通じて連繋。

  https://www.telecom-isac.jp/

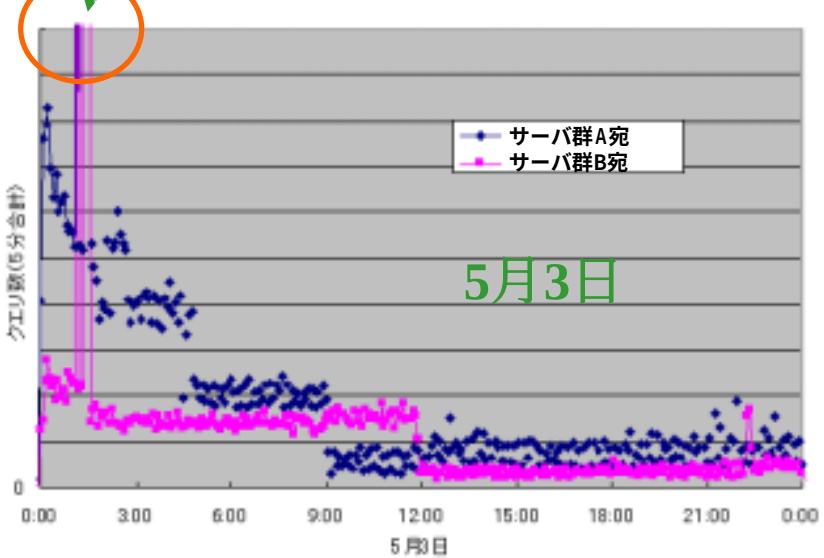
- 被攻撃ｻｲﾄ側がAﾚｺｰﾄﾞとしてBlackhole用IPｱﾄﾞﾚｽを応答する。
- 各ISPではそのIPｱﾄﾞﾚｽ宛のﾊﾟｹｯﾄを自ﾈｯﾄﾜｰｸ内で破棄するように設定。
- 今回はBlackhole用IPｱﾄﾞﾚｽをOCNのｱﾄﾞﾚｽ帯から一時的に用意した。

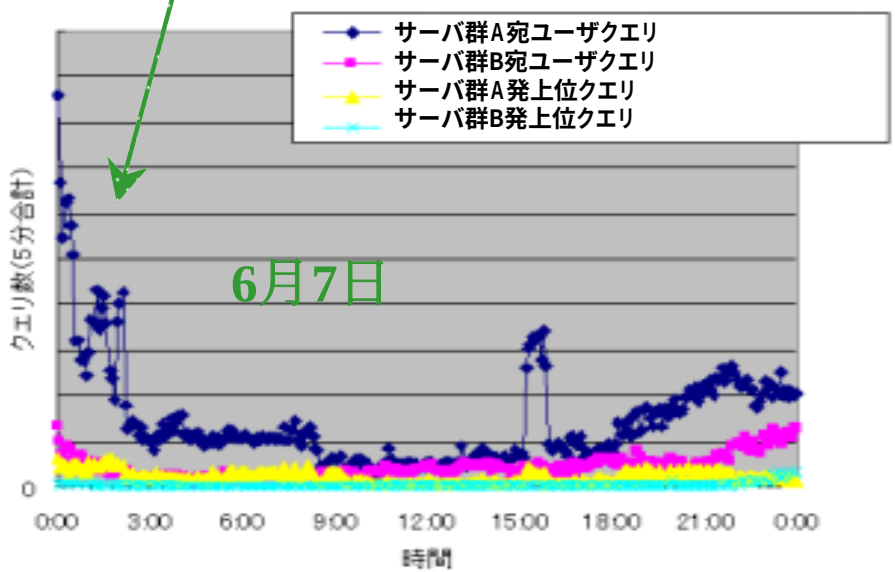
(調査：NTT情報流通プラットフォーム研究所)

5月の対策よりも効果的でした

実際はこの20倍以上のｸｴﾘ数がAﾚｺｰﾄﾞ削除後すぐに測定された。(Blackholeを設定すると急速に減少した)

ｽﾊﾟｲｸ状のｸｴﾘ増加は測定されなかった。





今後のことについて

- 今後どのようにDDoSに対応していくべきか、JANOG14(in宮崎)で話し合いましょう！

NWでのDDosパケット破棄方法

① 各ｴｯｼﾞﾙｰﾀでﾀｰｹﾞｯﾄIPをFilter!

でも処理能力が厳しいかも・・・・・・

①´各ｴｯｼﾞﾙｰﾀでﾀｰｹﾞｯﾄIPをNullStatic!

でもIPが変わる度に変更はしんどい・・・

② BlackholeﾙｰﾀでﾀｰｹﾞｯﾄIPを引き込む!

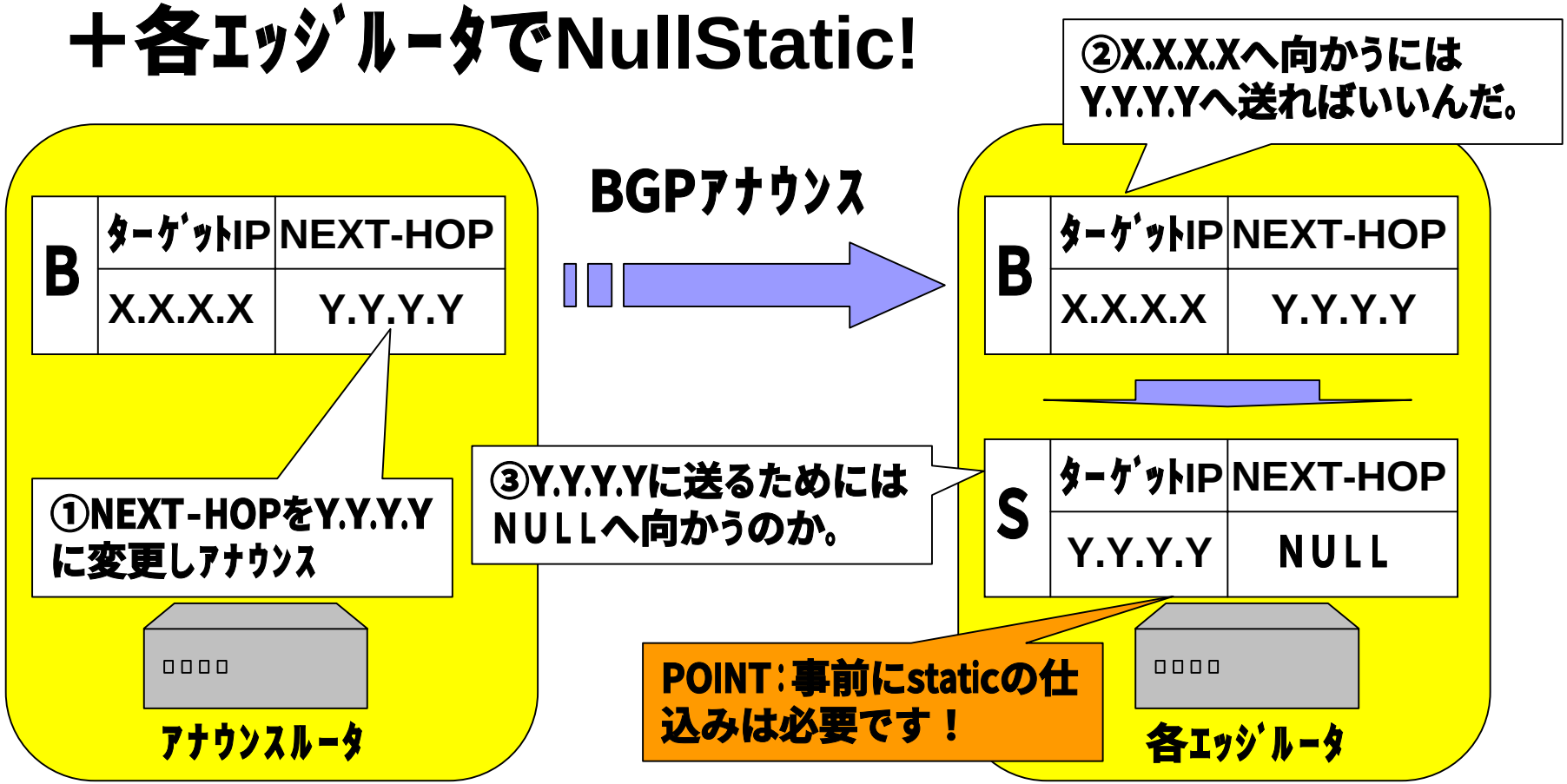
一手に引き受けてNWは大丈夫??・・・

③ BGPｱﾅｳﾝｽﾙｰﾀでﾀｰｹﾞｯﾄIPをBGPでｱﾅｳﾝｽ!
＋各ｴｯｼﾞﾙｰﾀでNullStatic!

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

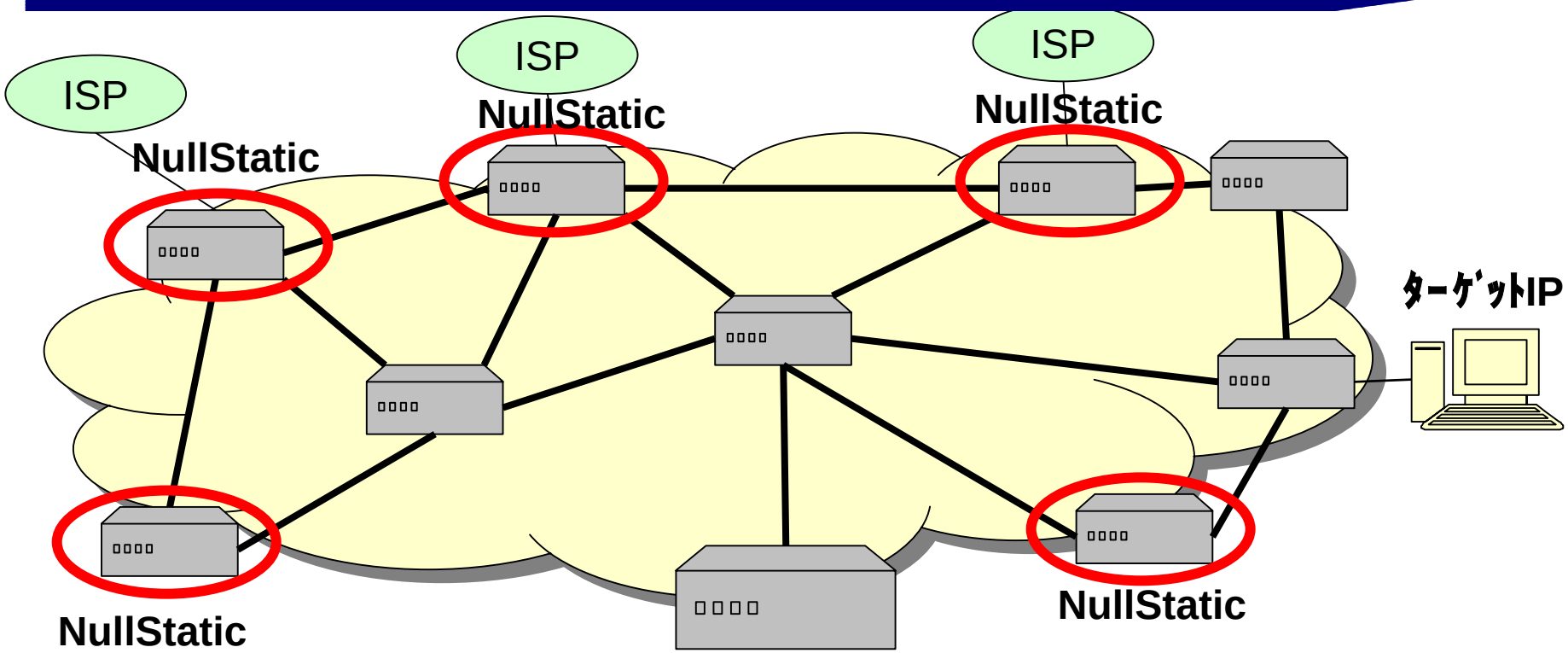
NWでのDDosパケット破棄方法

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!



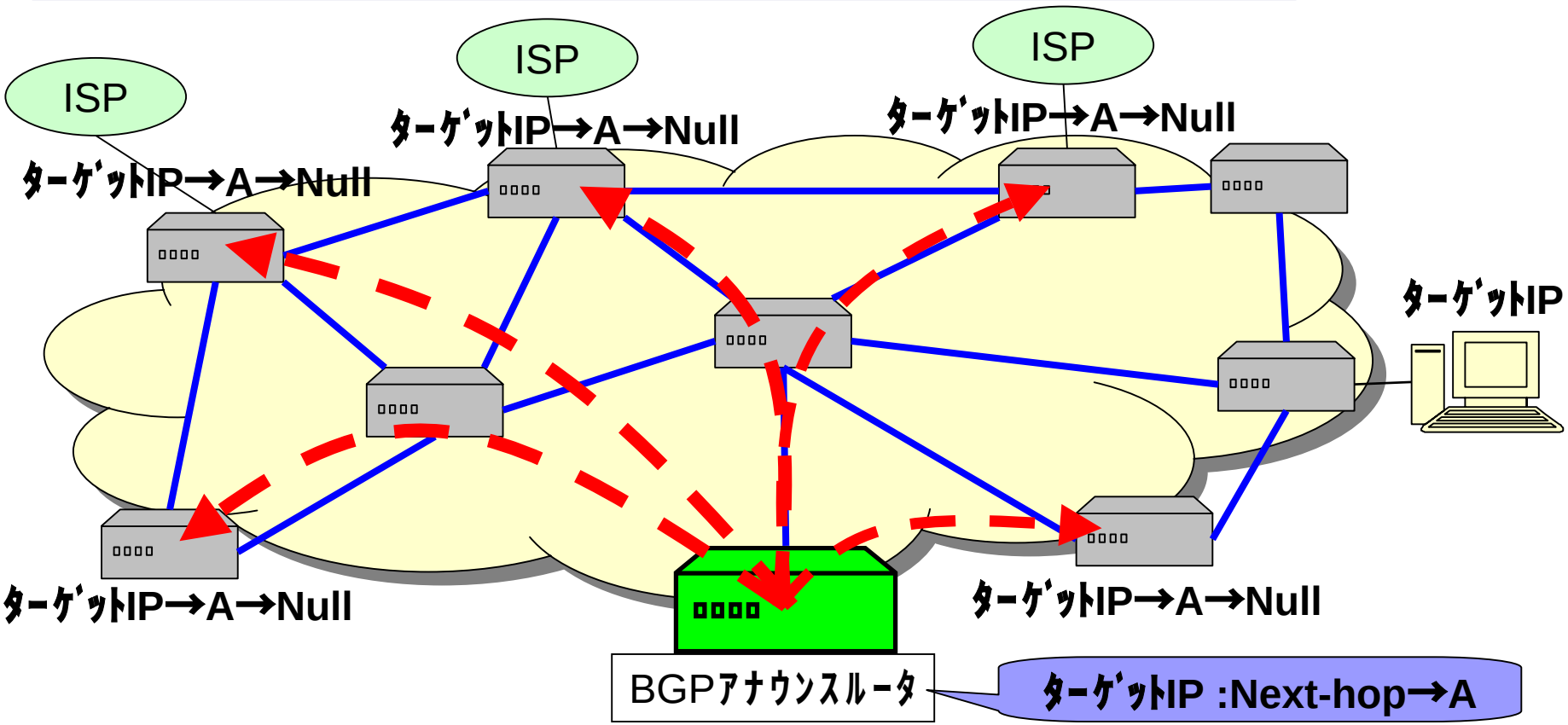
NWでのDDosパケット破棄方法

①ｴｯｼﾞにあるBGPﾙｰﾀに未使用IP (=A) へのNullStaticを書きます。



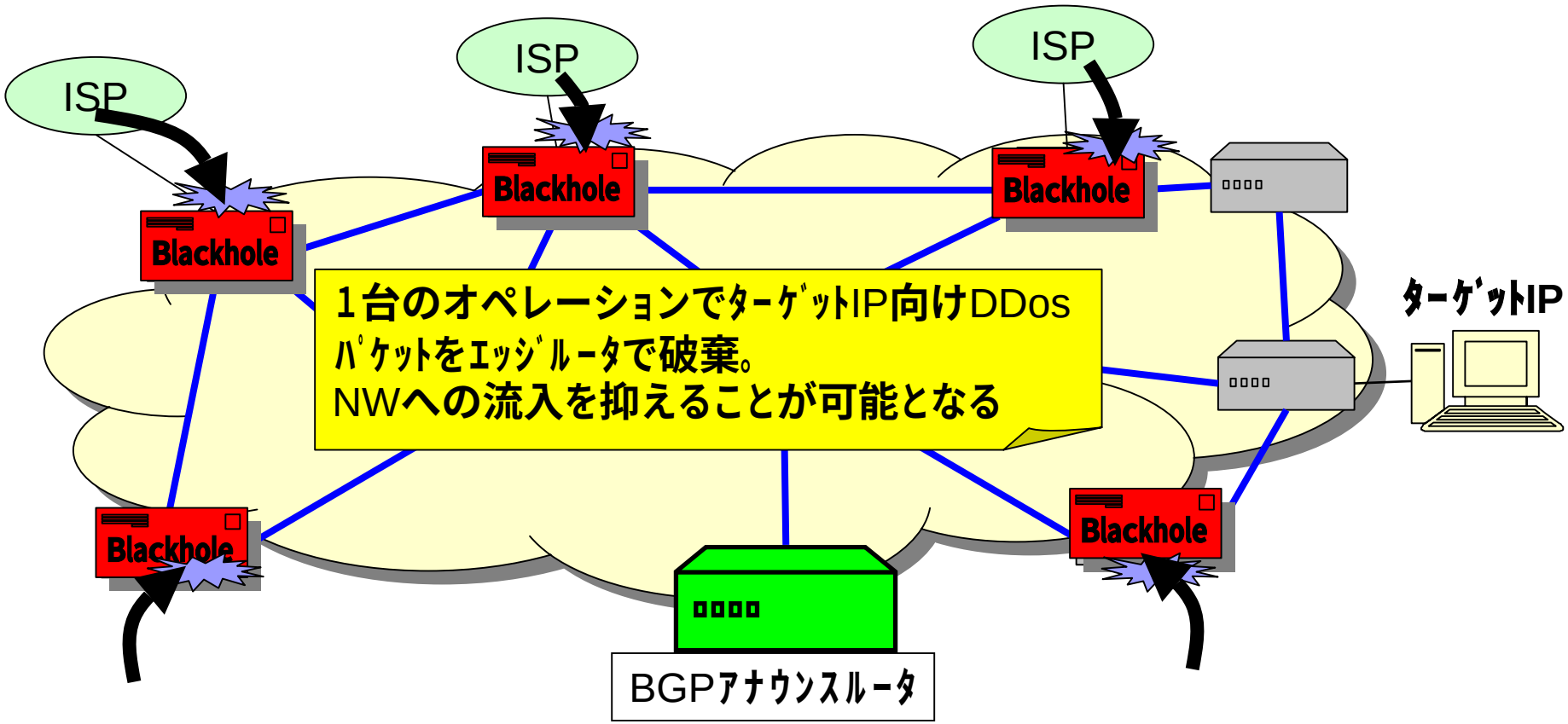
NWでのDDosパケット破棄方法

②BGPｱﾅｳﾝｽﾙｰﾀにて、ﾀｰｹﾞｯﾄ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ﾀｰｹﾞｯﾄIPを Filter	・LOGで何か分かる かも	・ﾀｰｹﾞｯﾄ毎に再設定 ・処理能力が不安
①´ﾀｰｹﾞｯﾄIPを NULL(Discards)	・網内帯域は圧迫無	・ﾀｰｹﾞｯﾄ毎に再設定 ・破棄ﾊﾟｹｯﾄ観測NG
②ﾀｰｹﾞｯﾄIP引込	・ﾀｰｹﾞｯﾄが変わっても簡単に変更 ・破棄ﾊﾟｹｯﾄ観測可能	・帯域圧迫 ・自分が死亡
③BGPでｱﾅｳﾝｽ +ｴｯｼﾞでNULL	・ﾀｰｹﾞｯﾄが変わっても簡単に変更 ・網内帯域は圧迫無	・破棄ﾊﾟｹｯﾄ観測NG

DDos／WORM発生時の注意ポイント

- ＣＰＵ的に・・・(攻撃(伝染)時に大量ﾊﾟｹｯﾄをだすので)
  - ・ｂｐｓ(ﾄﾗﾋｯｸ量)
  - ・ｐｐｓ(ﾊﾟｹｯﾄ数)

●物理帯域圧迫していませんか？

特定のIFに対してﾄﾗﾋｯｸが膨大となり、ﾊﾟｹｯﾄdrop等が発生

●ﾊﾟｹｯﾄﾋﾟﾝﾎﾟﾝしていませんか？

帯域は大したことないけれどﾊﾟ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）時にﾗﾝﾀﾞﾑな所を狙うので）
  ・NATｾｯｼｮﾝ数　　・ﾙｰﾃｨﾝｸﾞCache数

●ｾｯｼｮﾝｵｰﾊﾞｰしていませんか？

NATﾃｰﾌﾞﾙが上限に来て新規ｾｯｼｮﾝは接続できないかも

●Cacheﾃｰﾌﾞﾙが膨れていませんか？

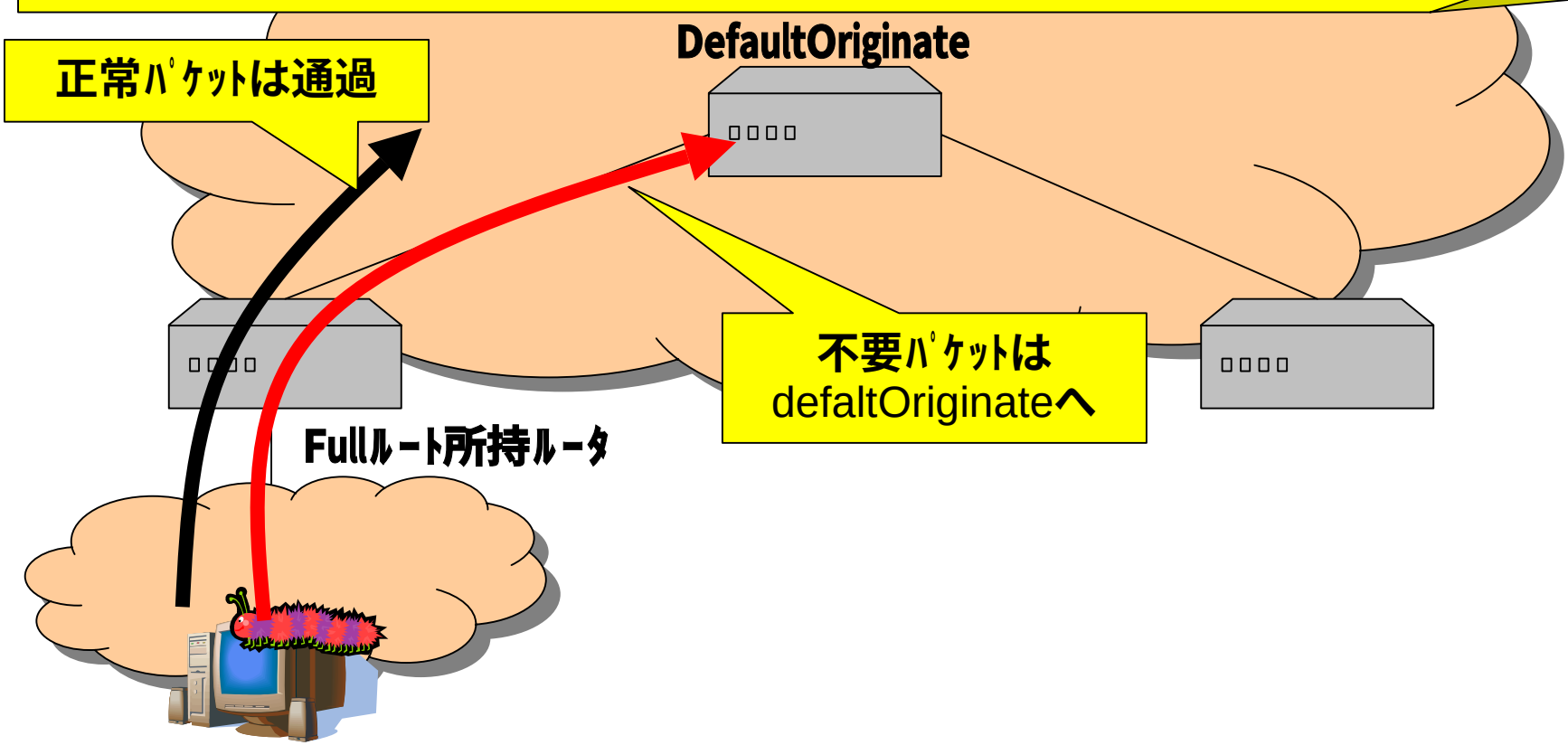
Cacheへのｴﾝﾄﾘｰ数によりﾒﾓﾘ不足かも

●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

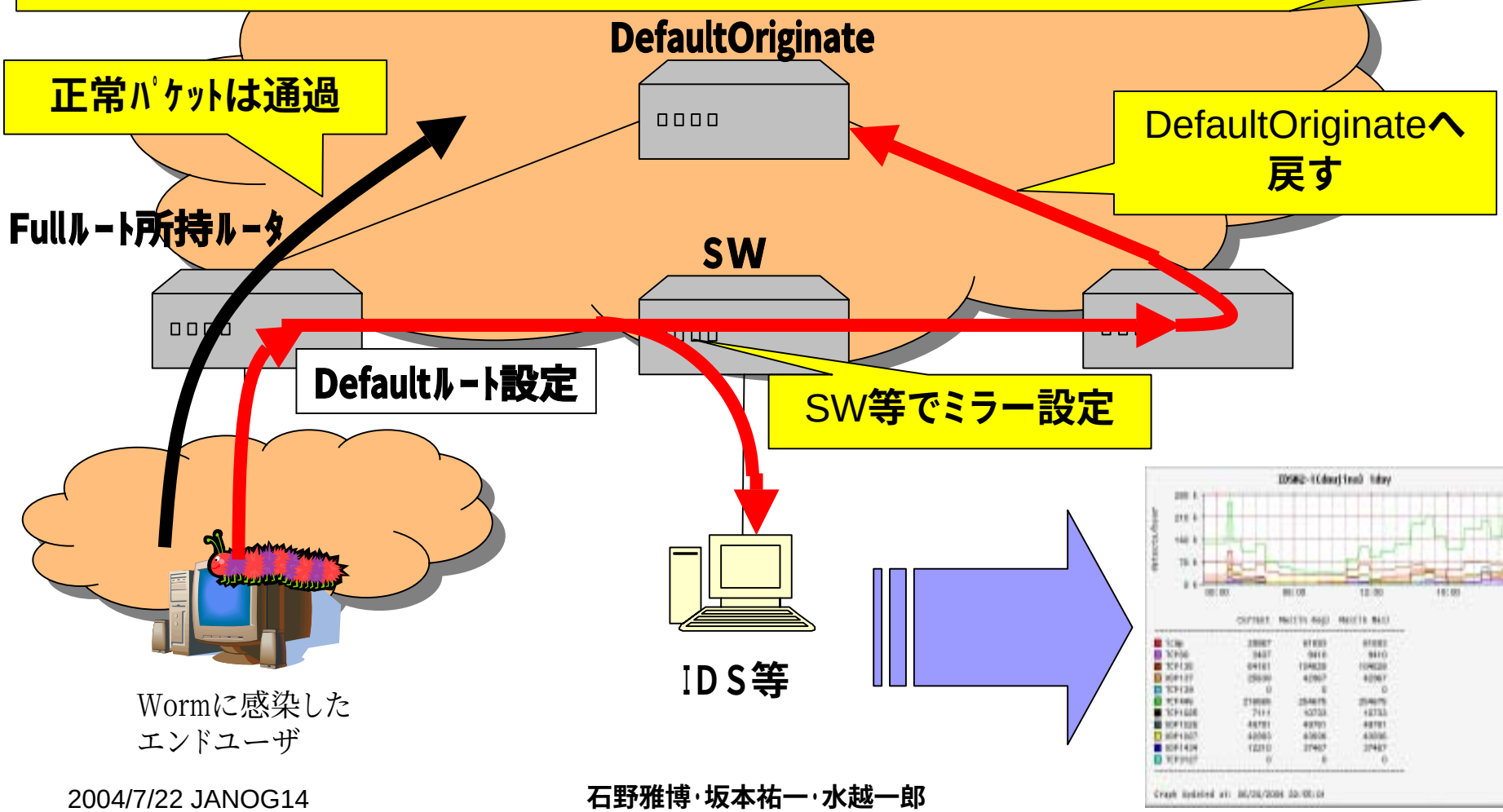
(参考) 不要ﾊﾟｹｯﾄを用いたﾜｰﾑ観察方法

・ﾜｰﾑ感染のﾊﾟ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) 不要ﾊﾟ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ﾋｯｸ迂回
・SW等でIDS向けにミラーし、ﾊﾟｹｯﾄmonitorを実施



石野雅博･坂本祐一･水越一郎