DDoS観察日記

DDoSからACCSを守り続けた10年でみたものとは

NTTコミュニケーションズ株式会社
須藤　年章
2014年11月19日

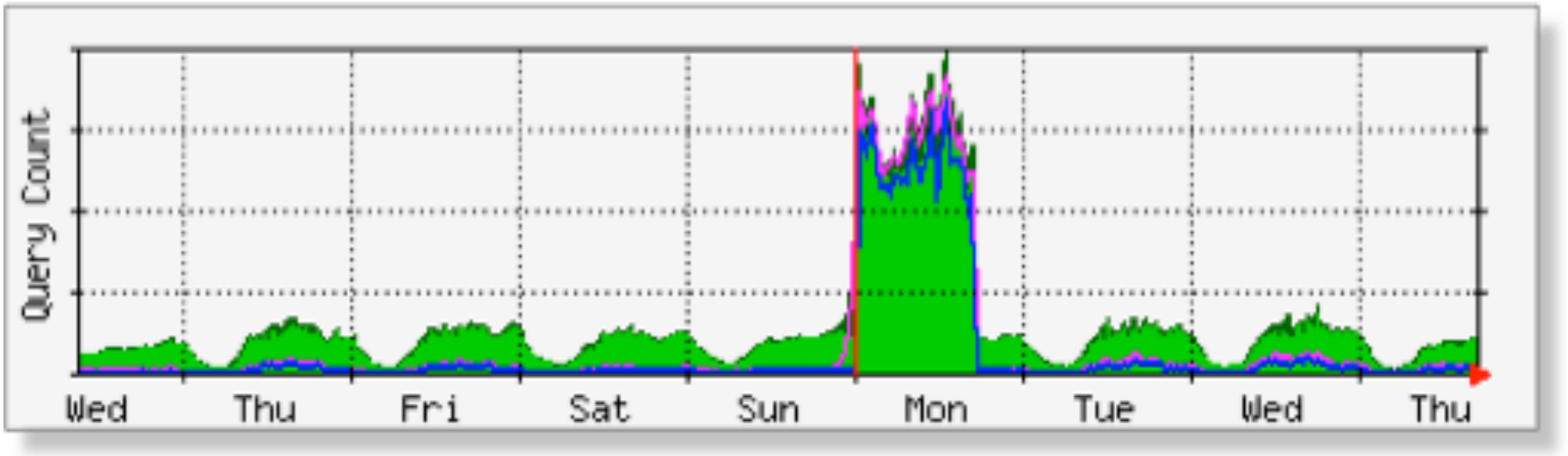
はじめに

- 現在もさまざまなサイバー攻撃が行われおりDDoS攻撃についても多くの被害を生んでいる
- 通信事業者、サイト管理者、エンドユーザー、Sier、セキュリティサービス運用などさまざまな立場でさまざまな苦労がつづいている
- ACCS DDoS事例では現在のセキュリティ対策につながるさまざまな対策、分析、体制や対応方法の議論と試行が行われてきた
- 実際に行われた対策を振り返るとともに現在および将来のセキュリティ対策へ繋げたい

DDoS観察日記

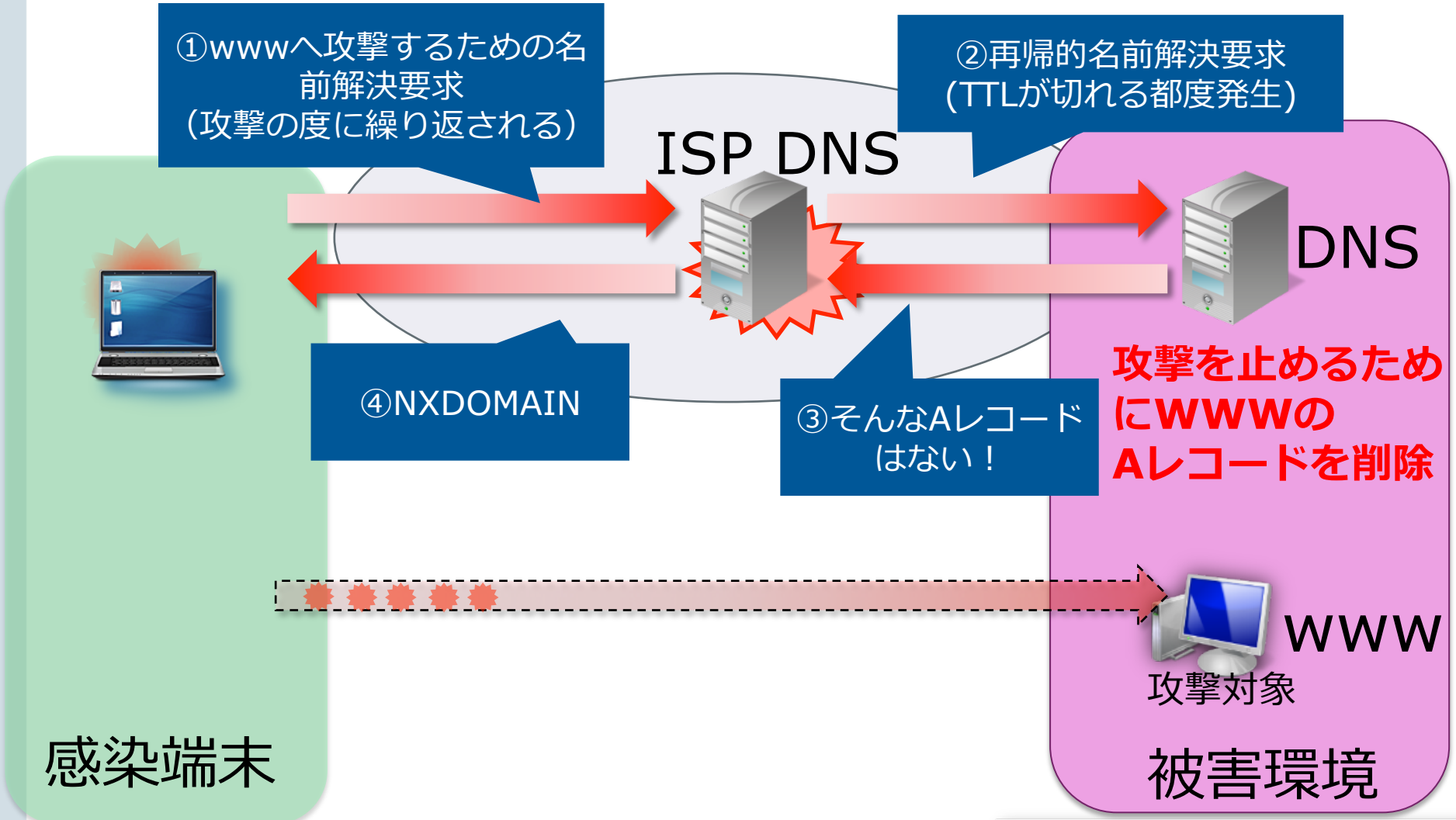
2004年4月5日　**発端**

- 2004年4月5日突然ISPが運用するDNS負荷が急上昇
- クエリが平常時6倍以上に跳上がる



当初、通信事業者目線ではDNSの異常クエリ増加として認識
ACCS？

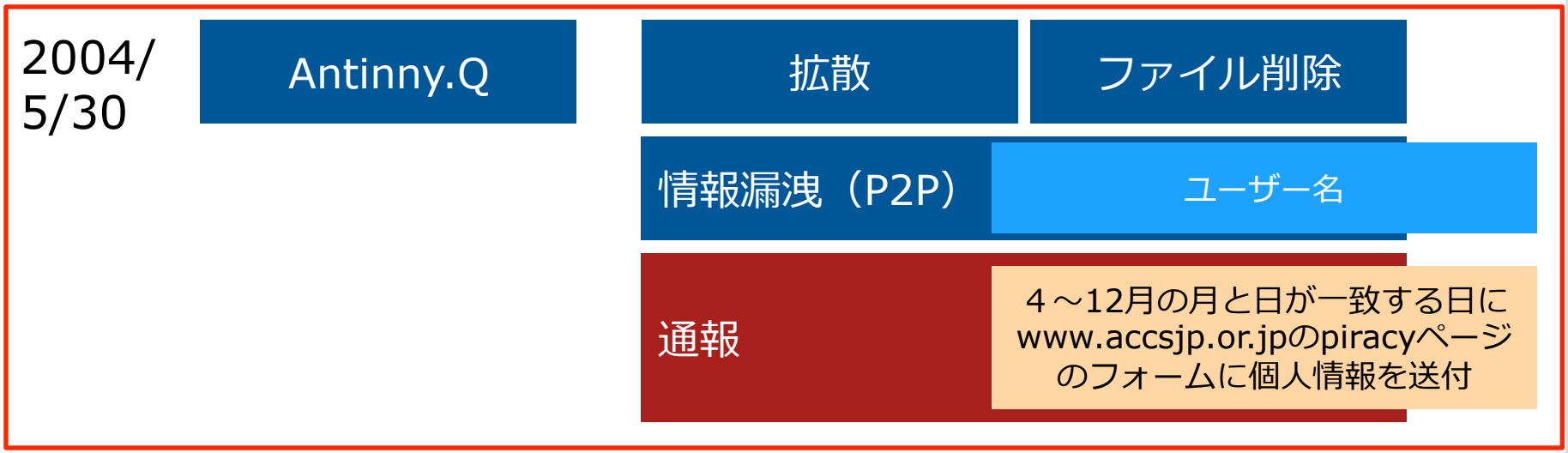
2004年4月5日　クエリ数急増の**原因**



2004年3月　背景にあったAntinny.Kの登場

2003/8/8	Antinny.A	エラーメッセージ表示	拡散
	Antinny.B		
	Antinny.C		
2004/3/18	Antinny.G	拡散	ファイル削除
		情報漏洩（P2P）	スクリーンショット、名前、組織、メールアドレス
2004/3/20	Antinny.K	拡散	
		情報漏洩（P2P）	スクリーンショット、名前、組織、メールアドレス
		通報	４～12月の月と日が一致する日にwww.accsjp.or.jpに個人情報をPOST

2004年5月　さらに**亜種**登場　Antinny.Q

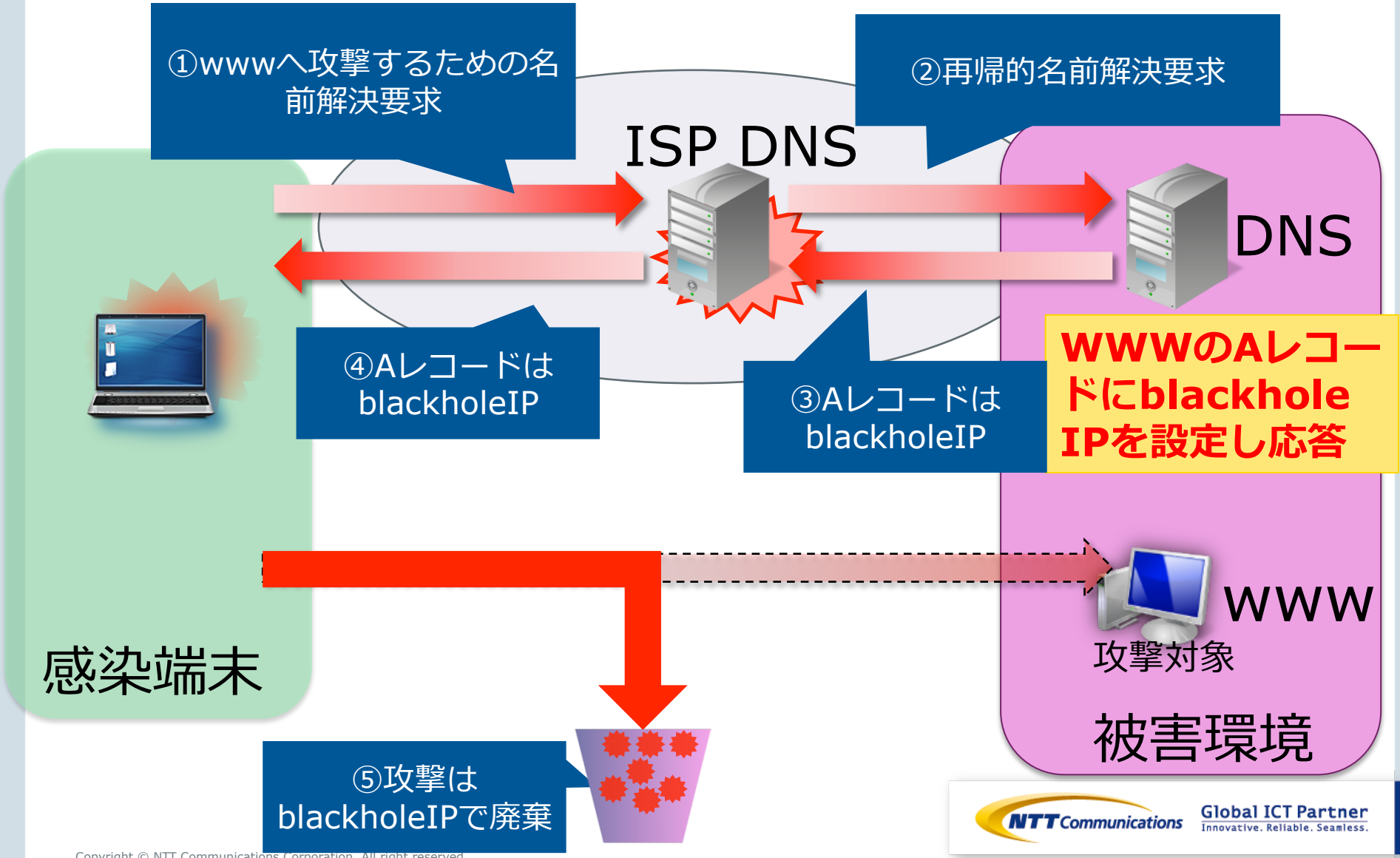


当初はwww.accsjp.or.jpに個人情報をHTTP POSTしてくるだけで**DDoSの効果しかなかった**

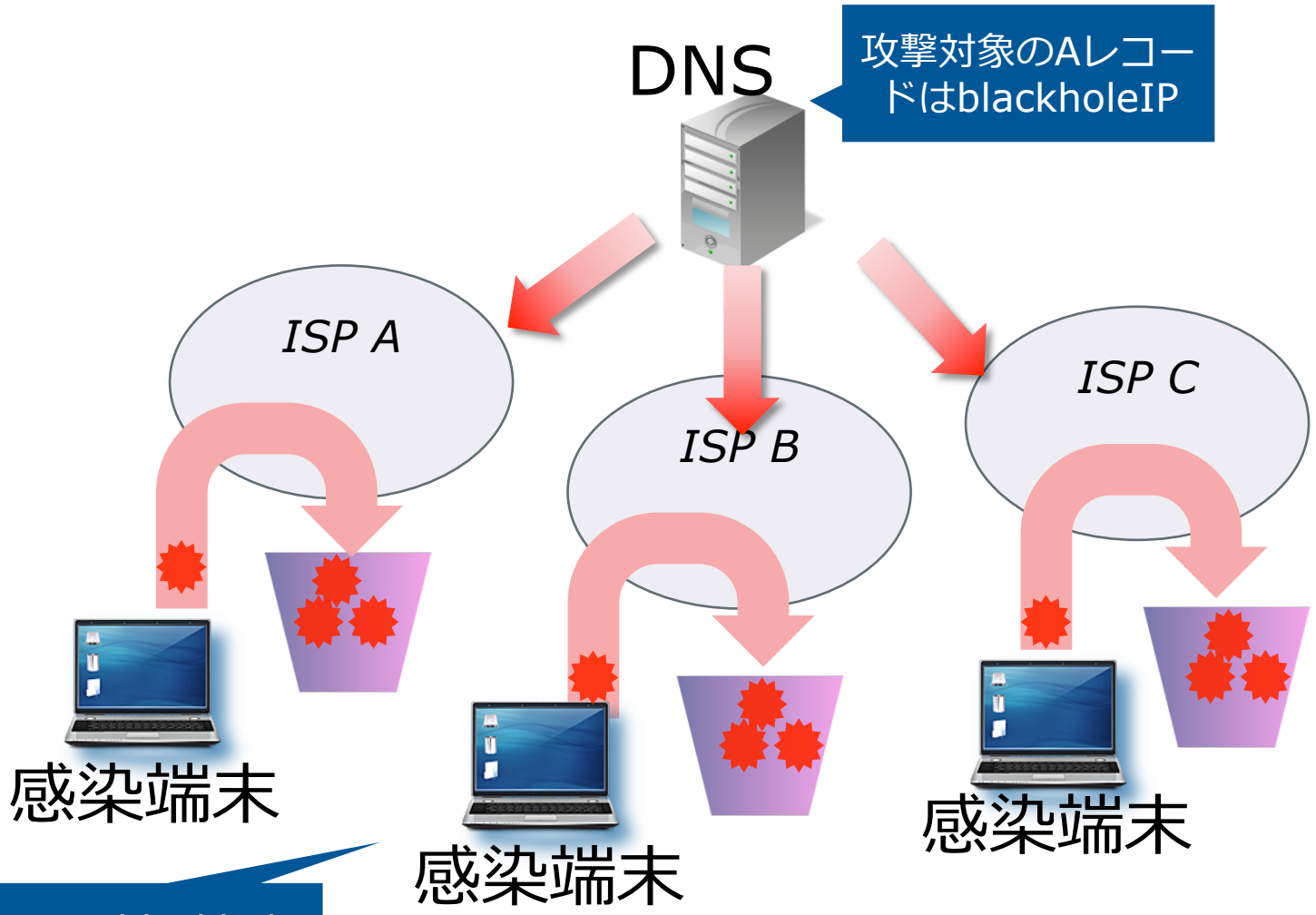
亜種はwww.accsjp.or.jpのpiracyページのフォームに情報を書き込む形に変更され**通報の意味をもった**

があまりにも量が多いため結局**DDoS**となった

2004年６月　対策



2004年６月　連携対策



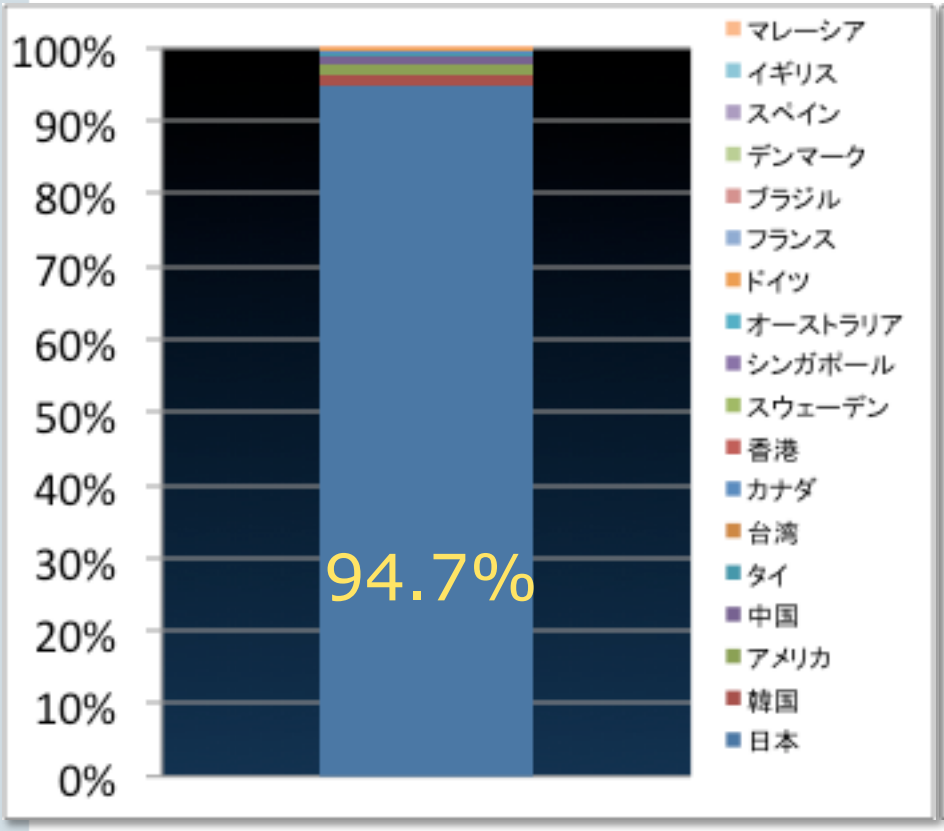
ここからが始まり

- **依然としてACCS殿のWebサーバはアクセスできない**
  - ISPのDNSサーバは救われたがDDoSには対応できていない
- **ACCS殿からの依頼に基づき通信状況の調査を行う**
  - 発生タイミング、手法は予測可能であるので実際のDDoS通信を詳細に観測、分析する
  - 検体、発生原因、攻撃元の調査・分析
  - DDoS対策手法の確立
  - 可能であれば一般的なDDoS対策手法として確立

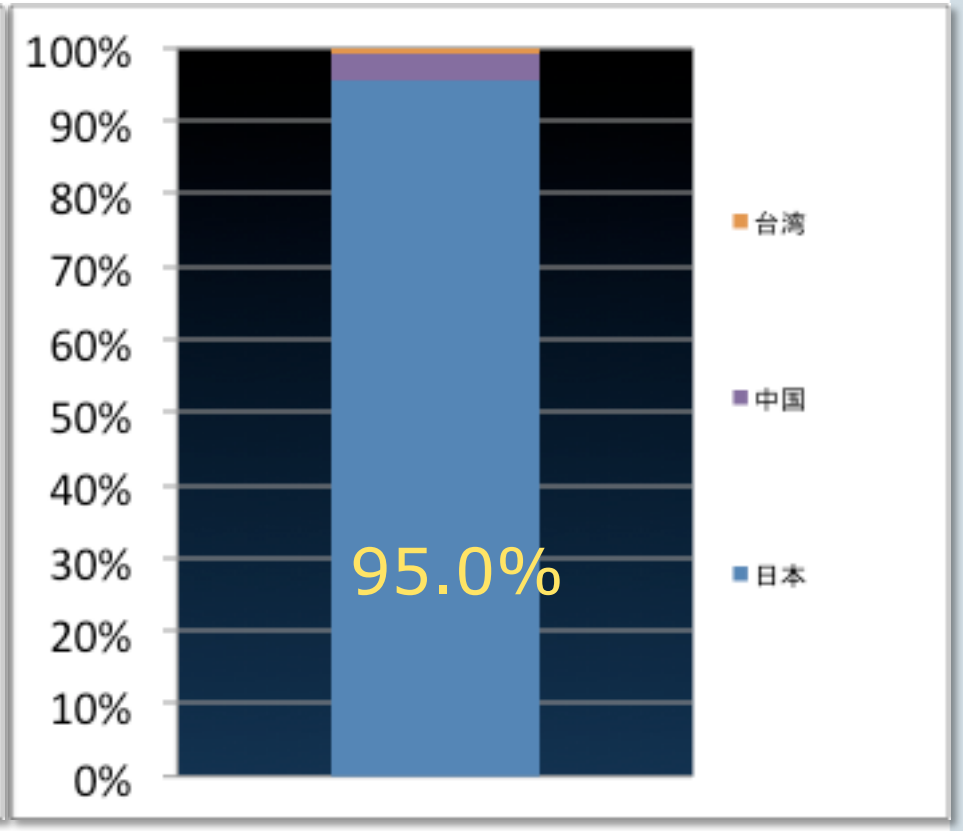
2004年8月　オンサイト調査

- 規模
  - 700Mbps
  - 30000～Request/Sec
- 攻撃内容
  - GET/POST floodのはずがsyn flood、connection floodが多い
  - トラフィックボリュームだけではなくsession table/メモリ枯渇問題を起こす攻撃の影響
  - 便乗攻撃
  - Netflow、sflowも利用したがL7までの解析が必要なので専用装置やフルキャプチャ利用に
  - 受けきる設備を準備することで対応できるかもしれないが釣り合うコストではない
- 攻撃元のほとんどが国内
  - リーチしやすい

攻撃元IPの**地理的**解析



2005/3



2014/10

ほとんどが国内からだが、アジア圏およびそれ以外の国からもわずかに

調査・分析 - 感染経路

- Winny,ShareなどのP2Pアプリケーション経由で流通しているアーカイブファイルにマルウェア実行ファイルが混入
- そのファイルをユーザーがダウンロードし実行することにより感染
- 後期にはDropper利用タイプも登場

調査・分析　- 主な感染方法

- **感染ファイルをユーザーに踏ませる工夫**
  - フォルダアイコンに偽装
  - 圧縮ファイルの解凍後に同一のファイル名＋.exe

    aaa.Zip
    ↓解凍
    aaa.avi、aaa.exe
  - ファイル名に空白文字を大量に含み拡張子をわかりにくくする

    新しいフォルダ　空白　.exe
  - RLO（unicode制御 Right to Left Override）

    hoge[U+2020e]TXT.EXE （実際のファイル名）→ hogeEXE.TXT（見た目のファイル名）
- **CD/DVD isoにマルウェア混入**
- **後期にはDropper利用や追加ダウンロード、亜種の自動生成など**

今現在も多用されている手法
（Zeus/Zbot等）

調査・分析 – 検体の静的解析、sandbox解析

- CnCレス
- 駆除されるまで、予めプログラムされた攻撃時間、攻撃対象に攻撃を続ける

機能追加、ターゲット変更はもないことからその日時に待ちかまえて対策できる

※ACCS以外を狙うのDDoSタイプAntinnyの後期にはCnC利用でDDoSや自動書き込みを行うタイプも登場

2005年1月　多面的対策開始

- 防御・被害者の救済
- 発生原因への対処

対処出来てもDDoSは発生しつづけ通信インフラやISPサービス等への影響はつづく
発生源が別のマルウェアに感染し新しい被害を生みつづける可能性が高い

- サイト側の対応
  - URL変えよう
  - DDoS対策
- エンドポイント対応
  - 駆除ツールの提供、駆除法方法の提供、サポート
  - アンチウィルス対応
- 通信事業者
  - 被害者からの申告に基づくユーザーリーチ
  - 通信の秘密、正当業務行為に関する議論（Telecom-ISAC等で）

2005年1月　URLの変更

www.accsjp.or.jp

www2.accsjp.or.jp

2005年3月　**亜種**の登場　**Trojan.Sientok**

2005/
3/21

Trojan.Sientok

DDoS

第一月曜日および4月～12月は月と日が一致するゾロ目の日にGET Flood

www2.accsjp.or.jp

2005/
4/?

Trojan.Sientok
亜種

DDoS

第一月曜日にGET Flood

www2.accsjp.or.jp
www3.accsjp.or.jp
www0.accsjp.or.jp
www1.accsjp.or.jp
ww2.accsjp.or.jp
ww3.accsjp.or.jp
2www.accsjp.or.jp
accsjp.or.jp
www.accsjp.or.jp

www2に追従！しかもDDoS機能に特化！
また変えるかもしれないから予めwww3とかも爆撃

2005年3月　エンドポイント対策

- **感染 PC の改善救済**
  - Antinnyワームの駆除ツールを作成
  - Telecom-ISAC Japan 会員ISPが連携し、ACCSサイトへ攻撃とみなされるユーザー数千人にメール等で連絡を開始

数%のユーザーの反応はあったが、目立った攻撃減にはつながらず

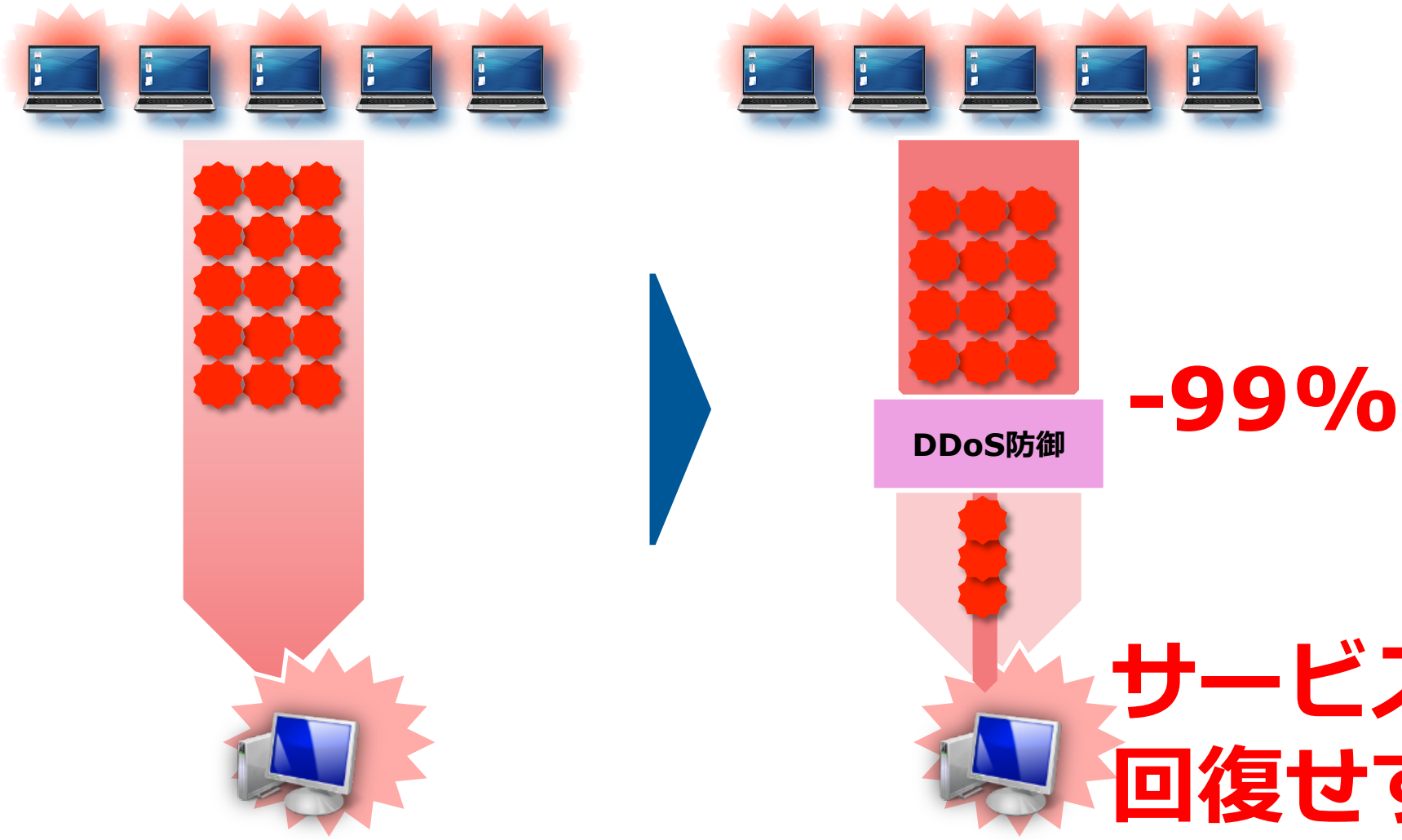
もっと受け入れられやすい注意喚起方法は？
強制的に駆除する仕組みは？

2005年3月　DDoS対策準備

オンサイト調査およびトラフィックLearningにより閾値、機能の調整

- 基本的なDDoS対策機能
  - Syn flood対策
  - Ssyn flood対策
  - Connection flood対策
  - GET/POST flood対策
- Antibot
  - L4レベル　Syn proxy/Syn cookie
  - L7レベル　HTTP正常性
  - L4-L7 遅延挿入（Tarpitting的な）
  - L4-L7 強制再送
- 帯域制御、シェーピング

2005年3月　DDoS対策開始



21

DDoS対策のゴールとは

トラフィックボリュームの削減	OK
サービス回復	NG

DDoSトラフィック状況

- 基本的なDDoS対策
  - Syn flood対策
  - Ssyn flood対策
  - Connection flood対策
  - GET/POST flood対策

- 大量性を伴うDDoSは防御可能
- 閾値にかからない低レート通信
- ゆるやかなconnection flood
- SlowRead,SlowPost
- 不完全リクエスト

- Antibot
  - Syn proxy/Syn cookie
  - 遅延挿入（Tarpitting的な）
  - L4/L7強制再送

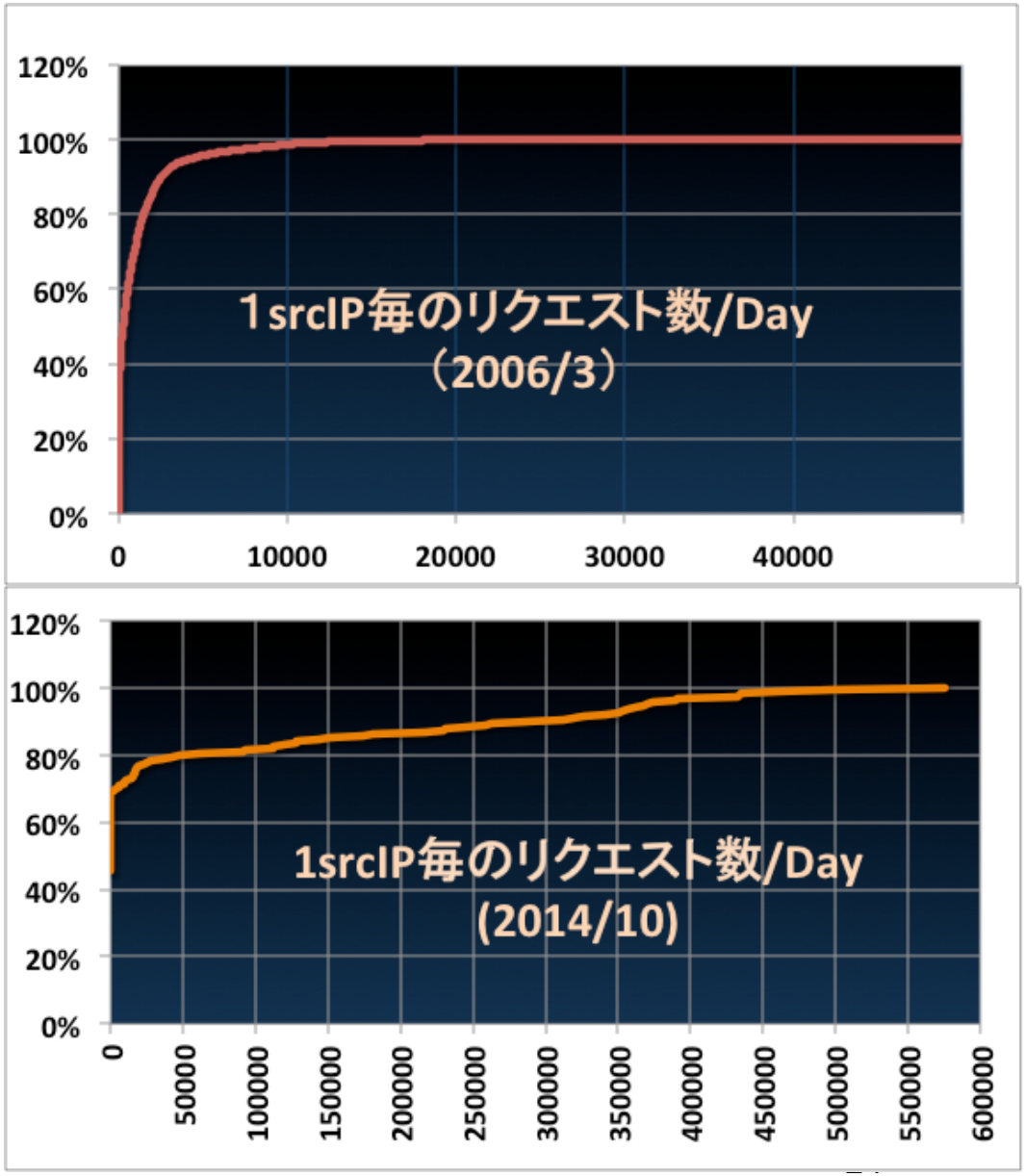
- 有効性は大いに認められたが、なぜかすり抜ける通信あり

- 帯域制御

- インフラを守るためにボリュームを抑えるという意味では有効だが正常通信を巻き込みサービス回復できない

この段階の対策効果ではすり抜けるトラフィックはサーバーの性能要件を超えておりDDoSは成立し続けている

1ソースIPあたりの攻撃量の累積度分布



- ほとんどが低レート通信
- 2014の方が10倍以上のトラフィックを吐いているユーザーの数が増えているのは通信環境がよくなったせい？再感染？

対策が有効に働かないトラフィックの発生原因分析

- **ユーザー環境の問題**
  - PC、ブロードバンドルータの性能、通信品質、バグ
- **通信環境の問題**
  - 低速／品質の悪い通信回線
  - モバイル通信
- **エンドポイントに近い側でのセキュリティ対策の影響**
  - Firewall、proxy
- **DDoS対策が攻撃力を助長**
  - TCP再送の誘発
  - 守っているはずのサーバー向け通信を不完全にしてしまう

- 結果的に閾値にかからない低レートDDoSの発生
- 意図的ではなく結果論としてSlowRead、SlowPost、不完全通信状態を生み出している

多層防御で

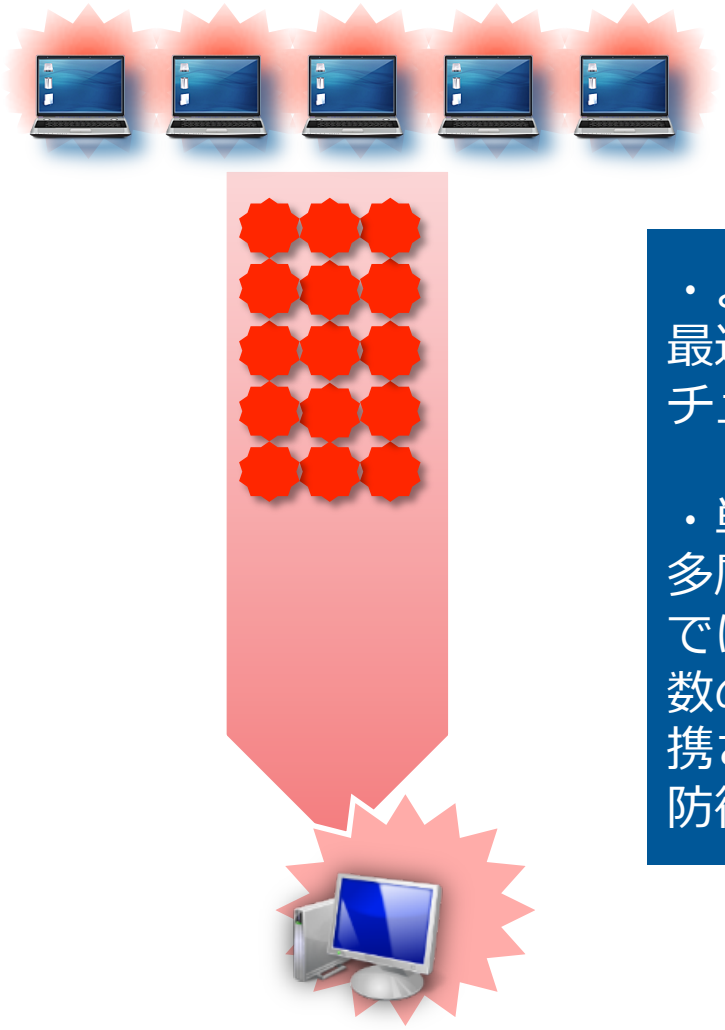
ロ 対策機能が有効に機能できない問題

- ロ 単独装置内の多層防御機能ではなく、異なる機能の装置を多層に組み合わせることで対策効果の改善と効率化を図る
- ロ 各装置、各機能の得意分野を有効に機能させるような多層化

ロ セキュリティ対策装置自体の過負荷対策

- ロ 装置の性能、機能を有効に発揮するために多層にすることで装置自体を守る

2005年 4月～　チューニング後DDoS対策リベンジ



攻撃対象（被害サイト）

・より環境に最適化したチューニング

・単体装置の多層防御機能ではなく、複数の装置を連携させて多層防御

攻撃対象（被害サイト）

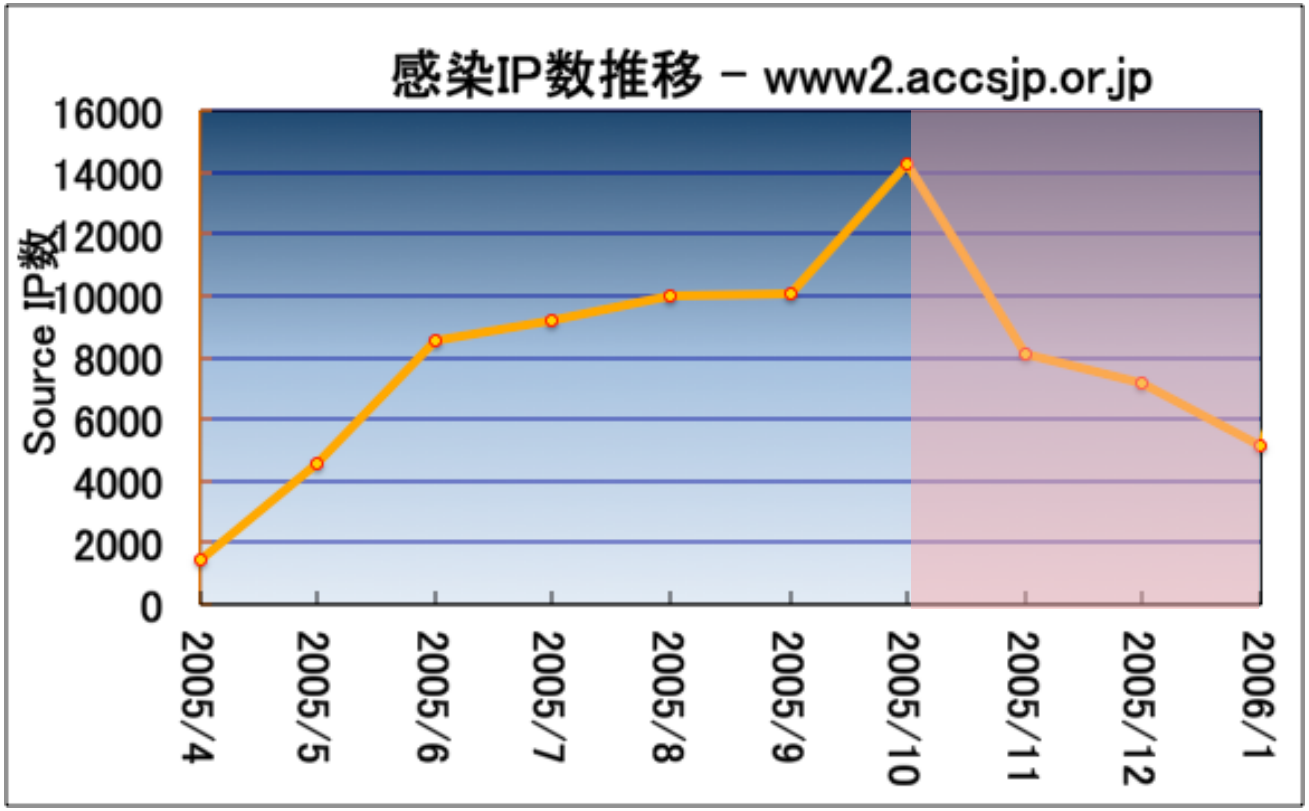
-99.98%

サービス回復

27

2005年10月　**さらなる**エンドポイント対策

2005年11月　マルウェア**駆除**



悪意のあるソフトウェア削除ツールでの対応
（11万台のPCから20万のAntinnyを駆除）
半減させることができた！それでも半減にとどまる
でも、このままいけば終わりが見えるかもと期待！

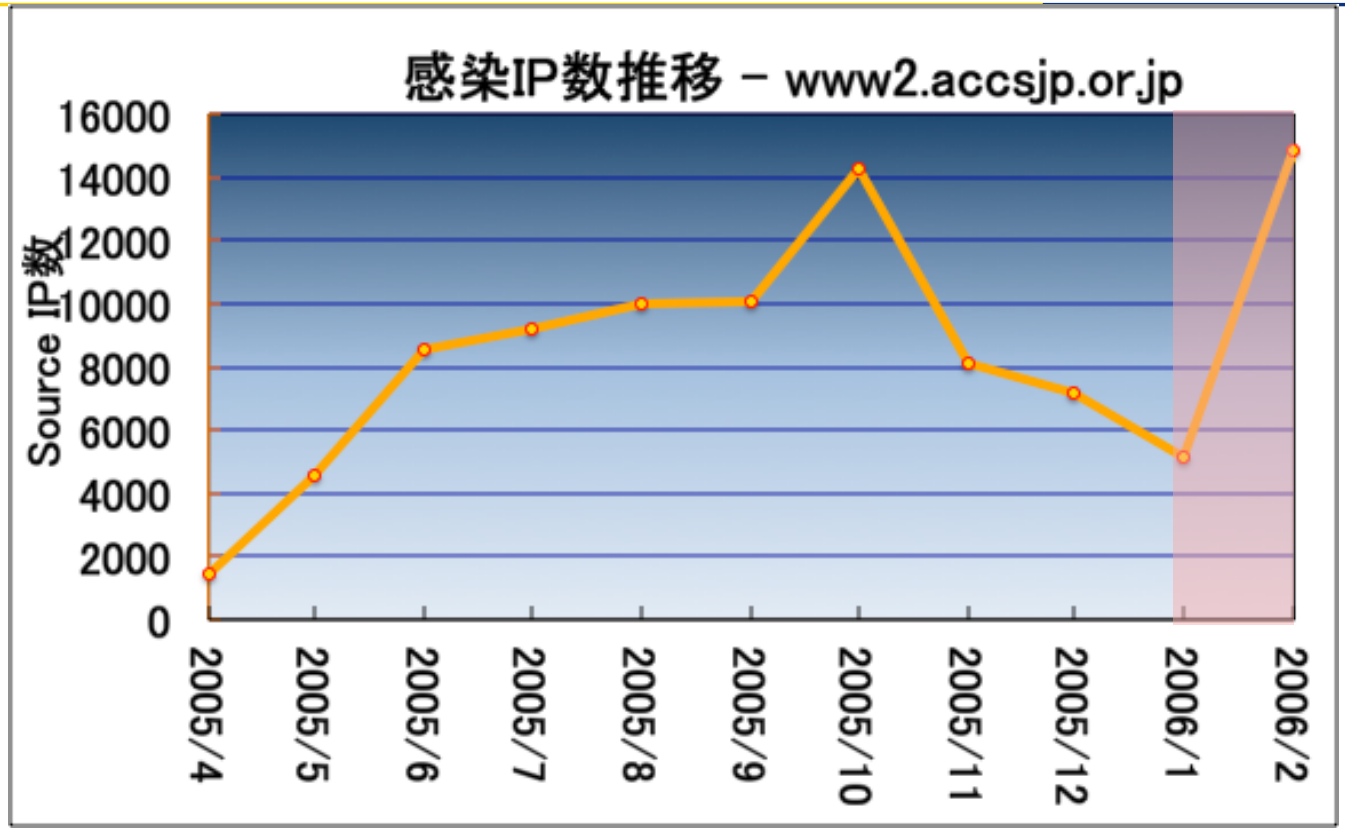
2006年1月　**がしかし**さらなる亜種の登場Antinny.AX

2006/1/28

Antinny.AX		
	拡散	ファイル削除
	情報漏洩（P2P）	スクリーンショット、名前、officeドキュメント、メールアドレス、P2Pアプリ情報等
	プロセス管理ツールの強制停止	dropper
	DDoS	月曜日であり、日付が 1 から 6 日までの間にある場合にwww.accsjp.or.jpとwww2.accsjp.or.jpにGET Flood

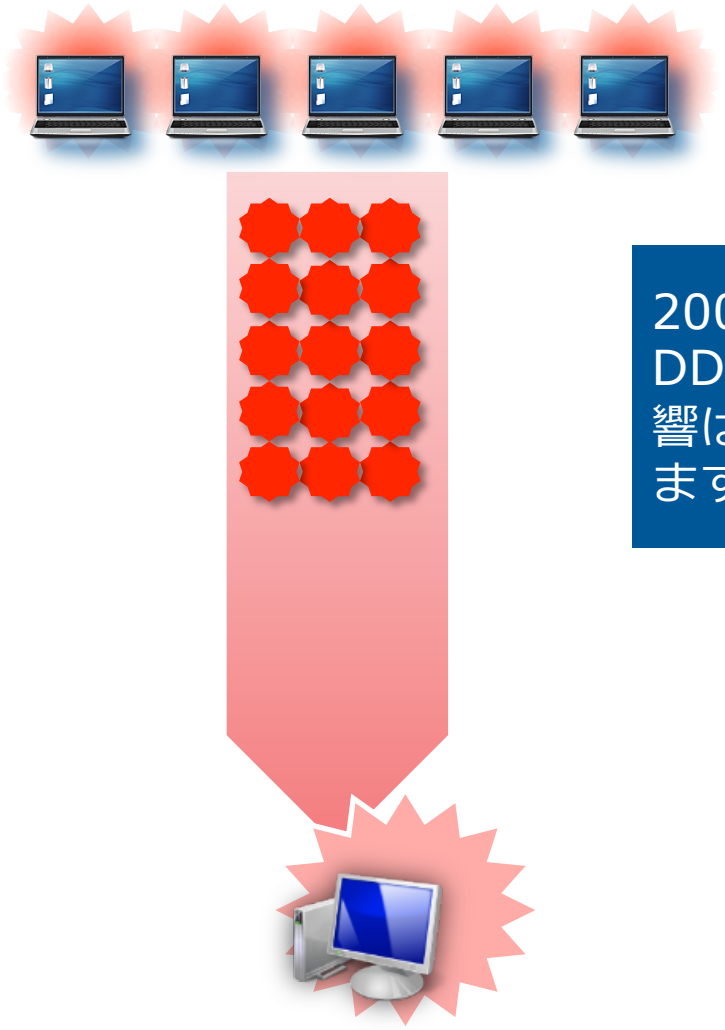
高機能化がすすむ中なぜか特定DDoS機能付き
www.accsjp.or.jp、www2.accsjp.or.jpを狙い撃ち

2006年1月　**さらなる**亜種の登場のせいで振り出しに



多数の亜種の登場により駆除前と同等のレベルまで増加
アンチウィルスやupdateしていない人の多さ。。。
何度も同じ手に引っかかって再感染する人たちの多さ。。。

2006年2月　**でも**DDoS対策は継続的に有効



攻撃対象（被害サイト）

2005/4以降はDDoS自体の影響は抑えられてます

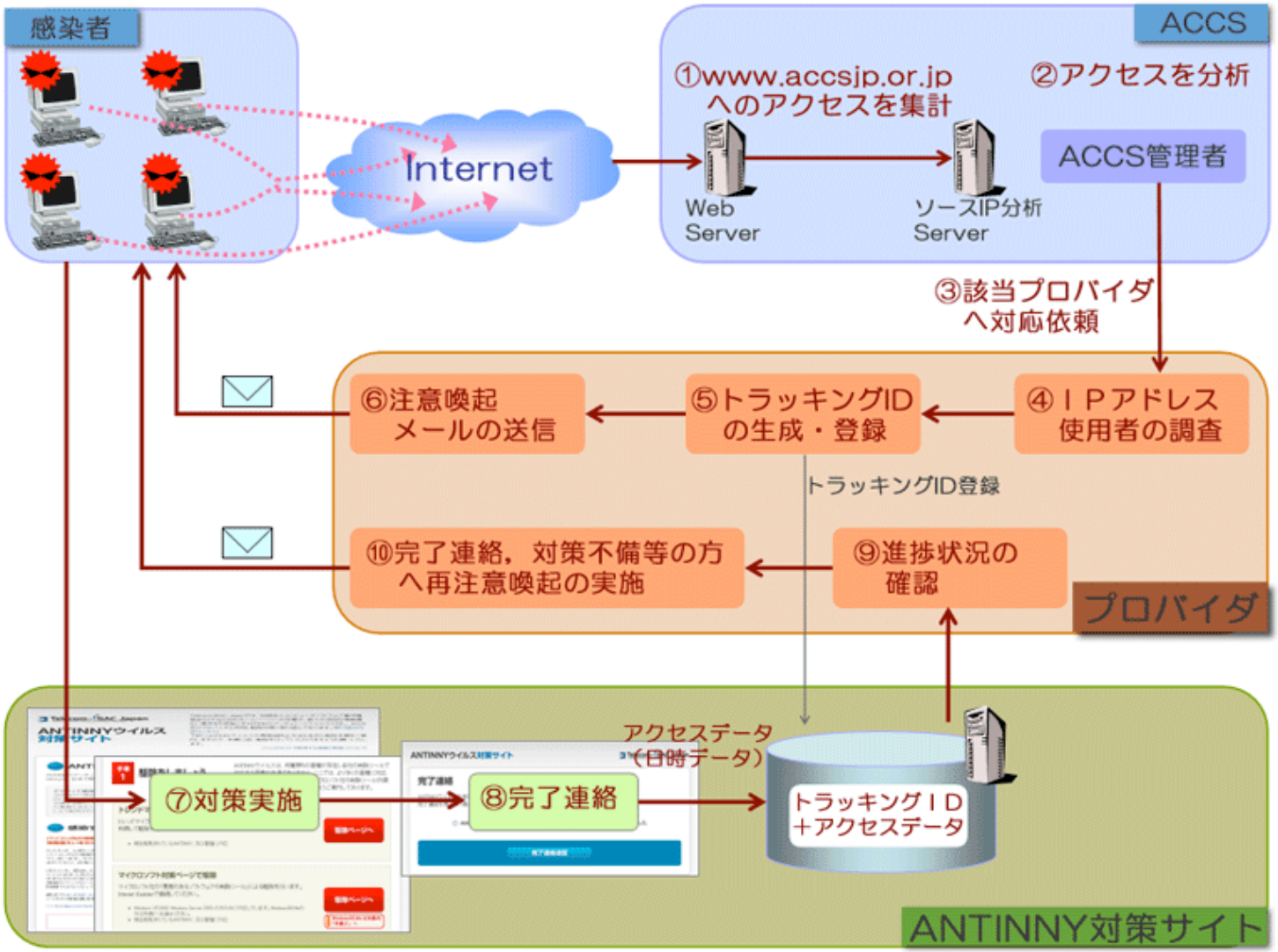
攻撃対象（被害サイト）

-99.98%

サービス回復

32

2006年3月　さらなるISP連携による注意喚起の実施



https://www.telecom-isac.jp/news/news20060315.html

その後。。。

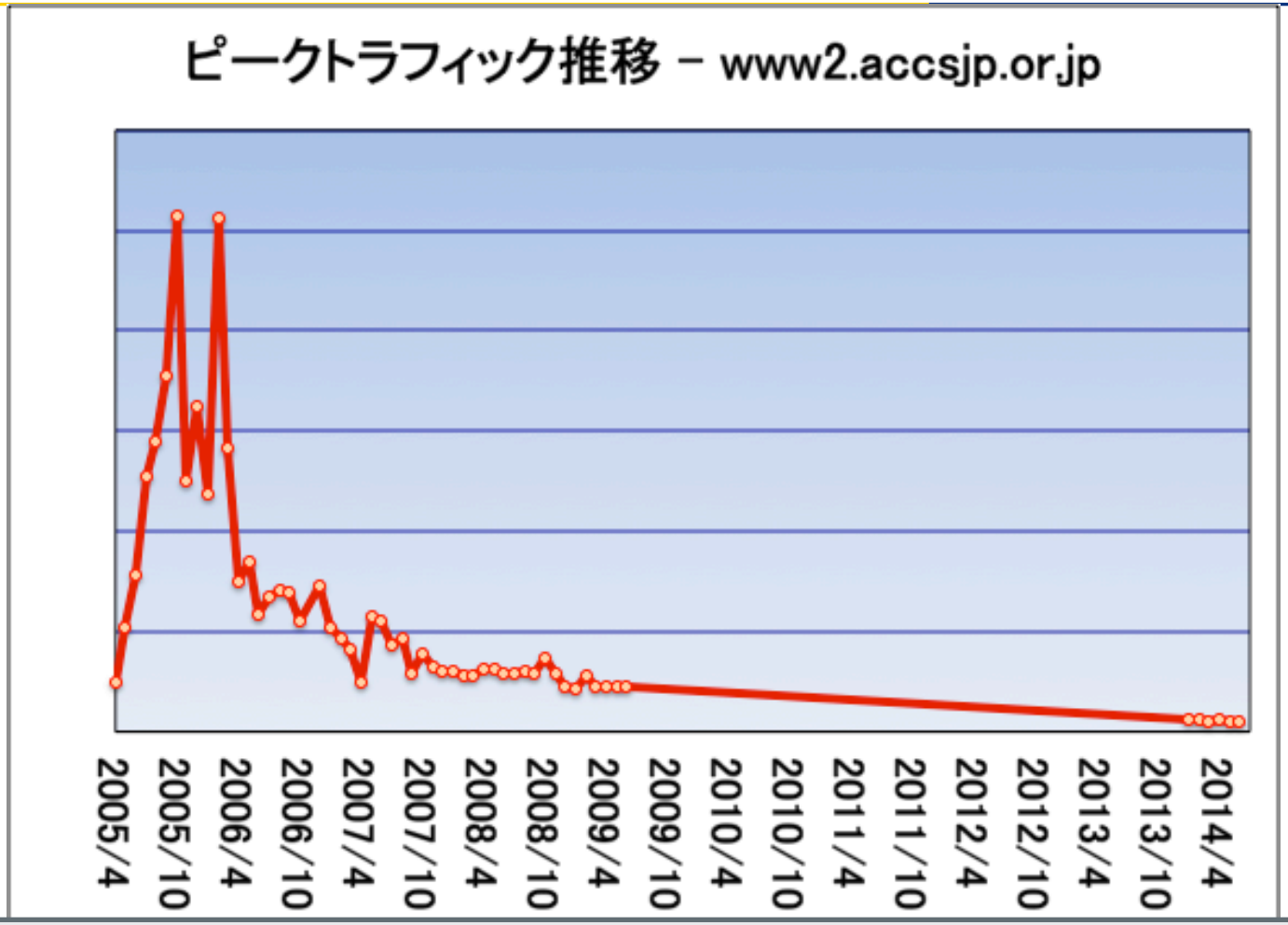
2006年3月以降　順調に

- ISP連携による注意喚起、アンチウィルスの対応とそれ以後該当のDDoS機能を持つ亜種が登場していないせいか順調に減
- ただし0にはなっていない

10年間の記録

- 9年かけて5%まで縮小も**未だに0にならず**

10年間の記録

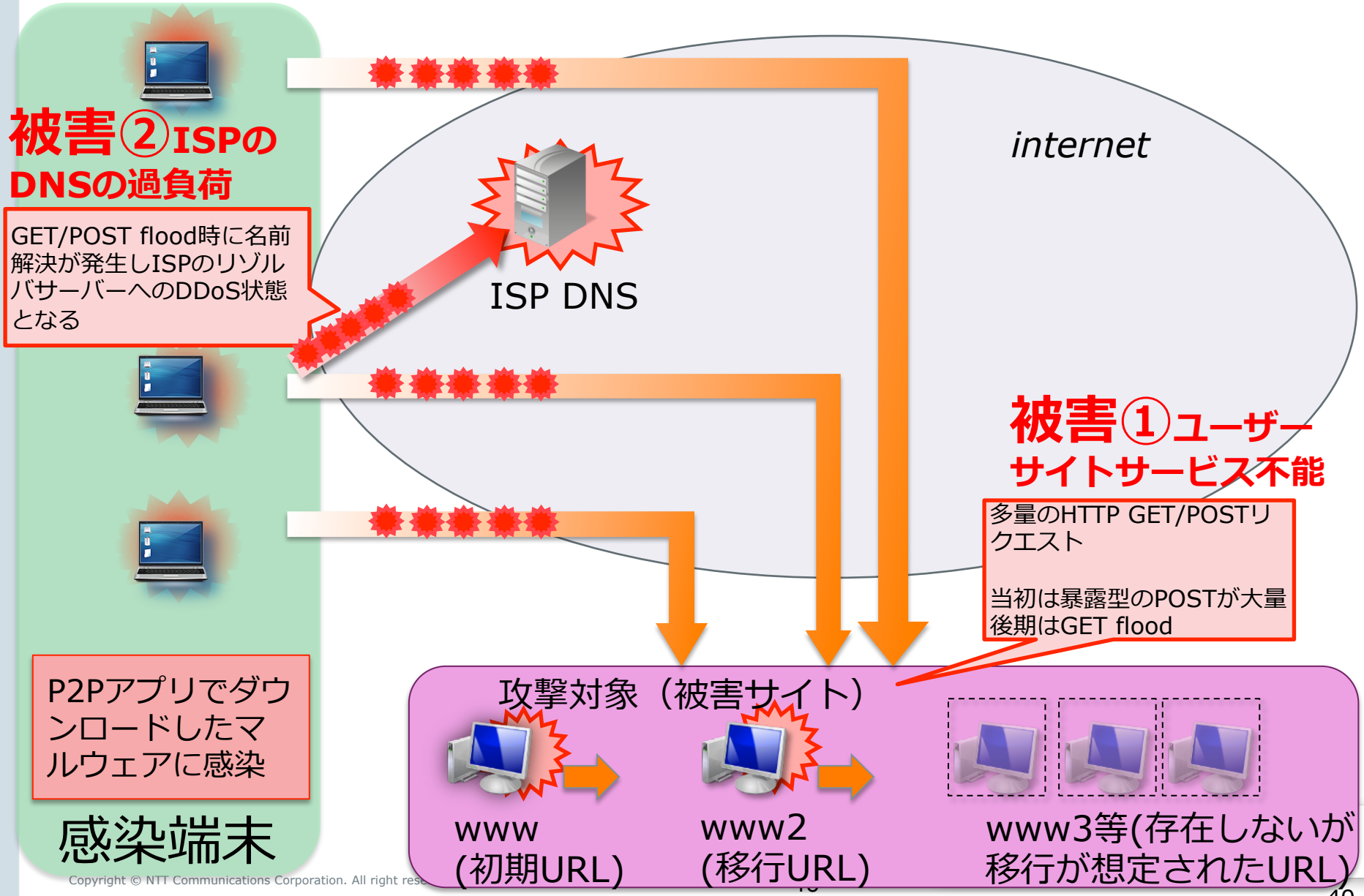


- 9年かけて0.5%まで縮小も**未だ0にならず**
- 影響はほぼない規模に

影響は限りなく小さくなっているが感染端末は０になっておらず攻撃は続いている

攻撃まとめ

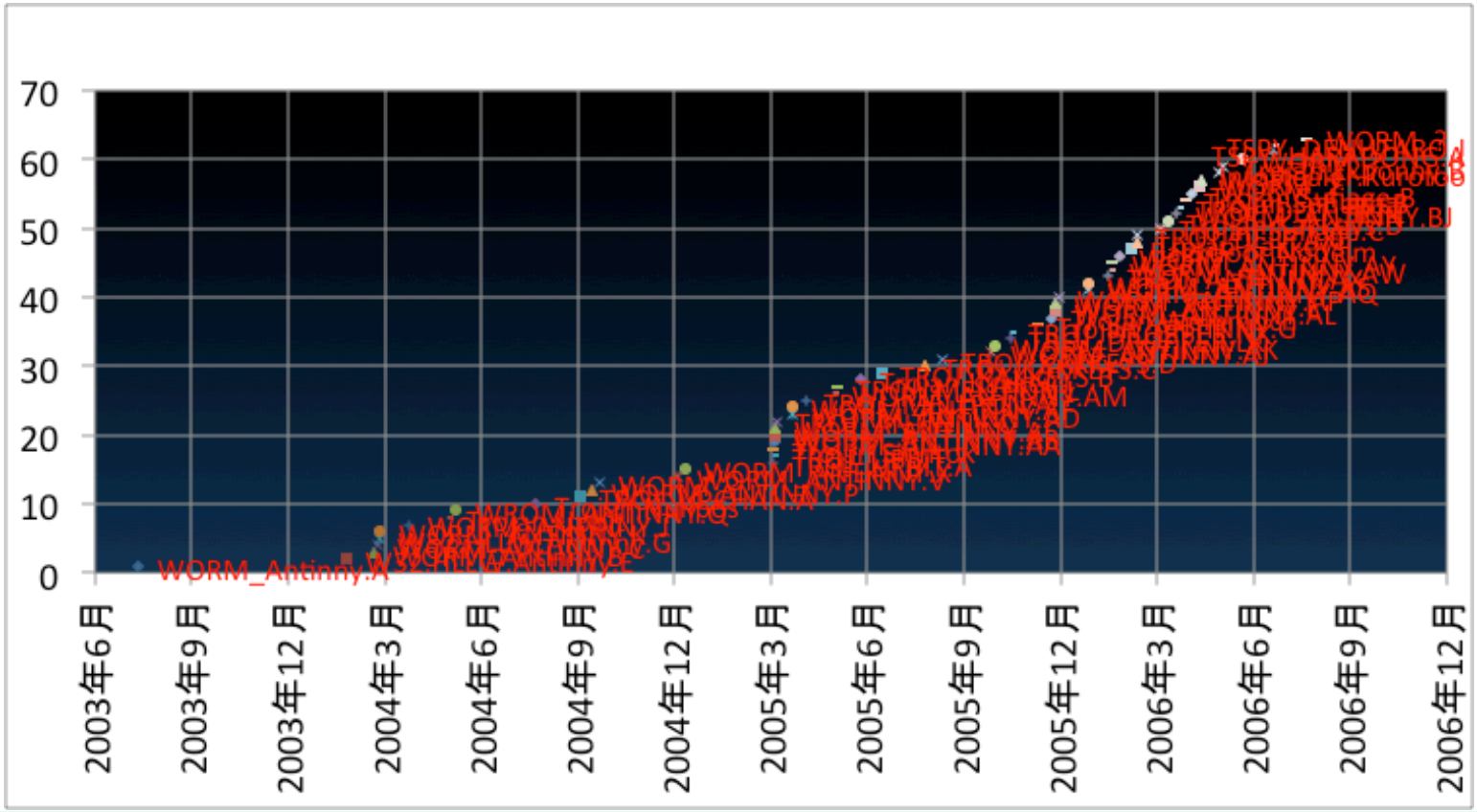
発生した被害まとめ



エンドポイント端末の改善の重要さと大変さ

- エンドユーザーの感染しやすさ、対策不足、再感染問題は永遠の問題だが
- のこっている攻撃元の正体は不明
  - 10年間OSのアップデートもアンチウィルスも入れてない
  - PC・OSの買い替え、アップグレードサイクルで０になることを期待していたが。。
  - 再感染？
- 攻撃パワーが10倍になっているように見えるものも
  - 回線速度UP？
- Antinny以外にもたくさん感染してる可能性が高い問題

代表的な関連マルウェアの発生時期



機能面のバリエーションは多く近年のbotやマルウェアと遜色ない
発生する被害も似ている

対策まとめ・課題

多角的対策

分析	**□ R&D的な内容** DDoS分析 攻撃原因マルウェアの分析 実際の攻撃を利用したDDoS対策の実験
防御	**□ DDoS対策機能の導入** 攻撃被害者側で防御
攻撃元の対処	**□ 被害者申告に基づくＩＳＰから感染者へのリーチ** 連携体制の確立 マルウェア対策ポータルを構築し駆除情報を提供 駆除ツールの提供 駆除進捗の確認追跡
情報共有・連携	□ 攻撃情報や対策情報の共有、公開

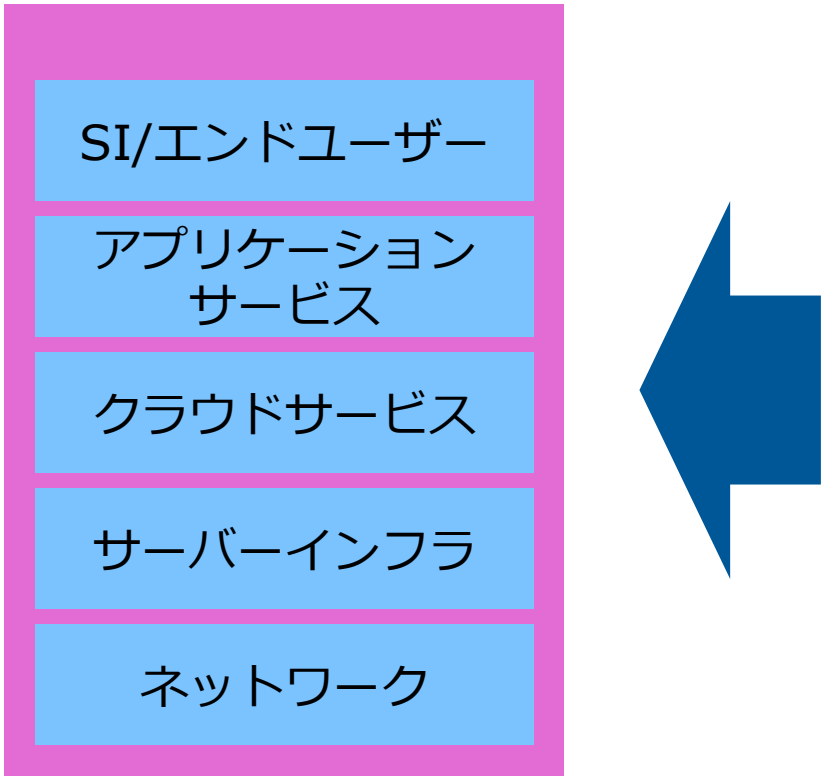
立場によりできることは異なる

	対応	課題
サイト管理者／SI	• 設備増強 • 対策技術の導入 • 対策サービスの利用	• 導入コストの問題 （大規模サイト向けソリューションはあっても、中小規模サイトでは導入しづらいことが多い）
通信事業者	• 自社設備・サービスへ影響を防ぐための対応 • 被害者申告を元にした各種対応 • セキュリティサービスの提供	• 中小規模向けへの提供コスト • ユーザー毎にカスタマイズ • より高度なSOCレベルの解析と対応が必要な質の攻撃への対応

攻撃情報、予兆情報の共有による対策の検討
→その情報を使うモチベーション、情報の信ぴょう性と責任

サービス提供形態の変化

- 通信事業者といっても様々な形態が存在しプレーヤーの多様化と連携の複雑化がすすむ



・一つのサービスのそれぞれの層を異なる通信事業者が提供している場合

・インフラは海外、上位層は国内事業者

・各層に直接提供、ローミングや再販など複雑な提供事業者の関係性がある場合

・エンドユーザーとの関係

ユーザー環境の問題

- 古いOSを使い続ける理由
  - 性能は十分、特に買い換える必要性がない
  - PCはデジカメや音楽プレーヤーの母艦として使いたいだけ
  - 使い続けたいハードウェアやソフトウェアが古いOSでしか使えない
- アップデートできない
  - 「アップデートしてください」→「10年前の機器やソフトにアップデートファイルはないです」
  - PCだけではなくネットワーク機能をもったさまざまな機器

- セキュリティ機能が強化されても使ってもらえなければ意味がない
- 時代とともにユーザー環境がPC、スマホ、タブレット、クラウドなどに変化し、仮想化やソフトウェア化が進む時代のソフトウェアすべてのセキュリティ対策は難しそう

ユーザーのセキュリティ意識

- ユーザーにどうやって声を届けるか？
  - 「スパム？とどいてるよ。無視してるから大丈夫」「迷惑メールフィルタ？みればわかるからなくても大丈夫」
  - 「ああ、この変なメッセージはたぶん、○○くんの電話帳が盗まれたんだろうな。ふーん。」
  - 当然予防に対するモチベーションはない

- ネットワークやインフラ層を意識しない、アプリを使ってるだけ、コンパネ操作でなんできる感覚しかないユーザー層
- 正しい設定例を公開しても届かないし届いても理解してもらえない
- 若年層～中高齢層など各層で事情は異なるためそれに応じた分析と対応が必要
- 声が届かなくても意識していなくても守られるアーキテクチャの提供が必要なのか？対策側の意識と対策手法の変革も必要

まとめ

- マルウェア感染による個人端末からの情報漏えいや標的型攻撃、マルウェア感染した個人端末や、乗っ取られたLinuxサーバーを踏み台にしたDDoSも日常的に発生している
- 今回の事例で実現し有効性が確認できた手法、体制の基本的な考え方はさまざまな対策に応用できる
- 達成できなかったことや課題も同じ
- サービスの多様化、ネットワーク環境の変化、利用者の変化など時代に応じた、サービスへのセキュリティ機能の実装や、対策・対応方法、新しい連携体制の検討を続けていく必要がある

ご清聴ありがとうございました