JANOG35 Meeting

NTP Reflection Attackをとりまく状況と ISPにおける対応、NTP情報交換WGの活動報告

2015年1月15日

JANOG NTP 情報交換WG
高田　美紀
中島　智広

セッションのながれ

1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

6.上記についてのディスカッション

合計20分

1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

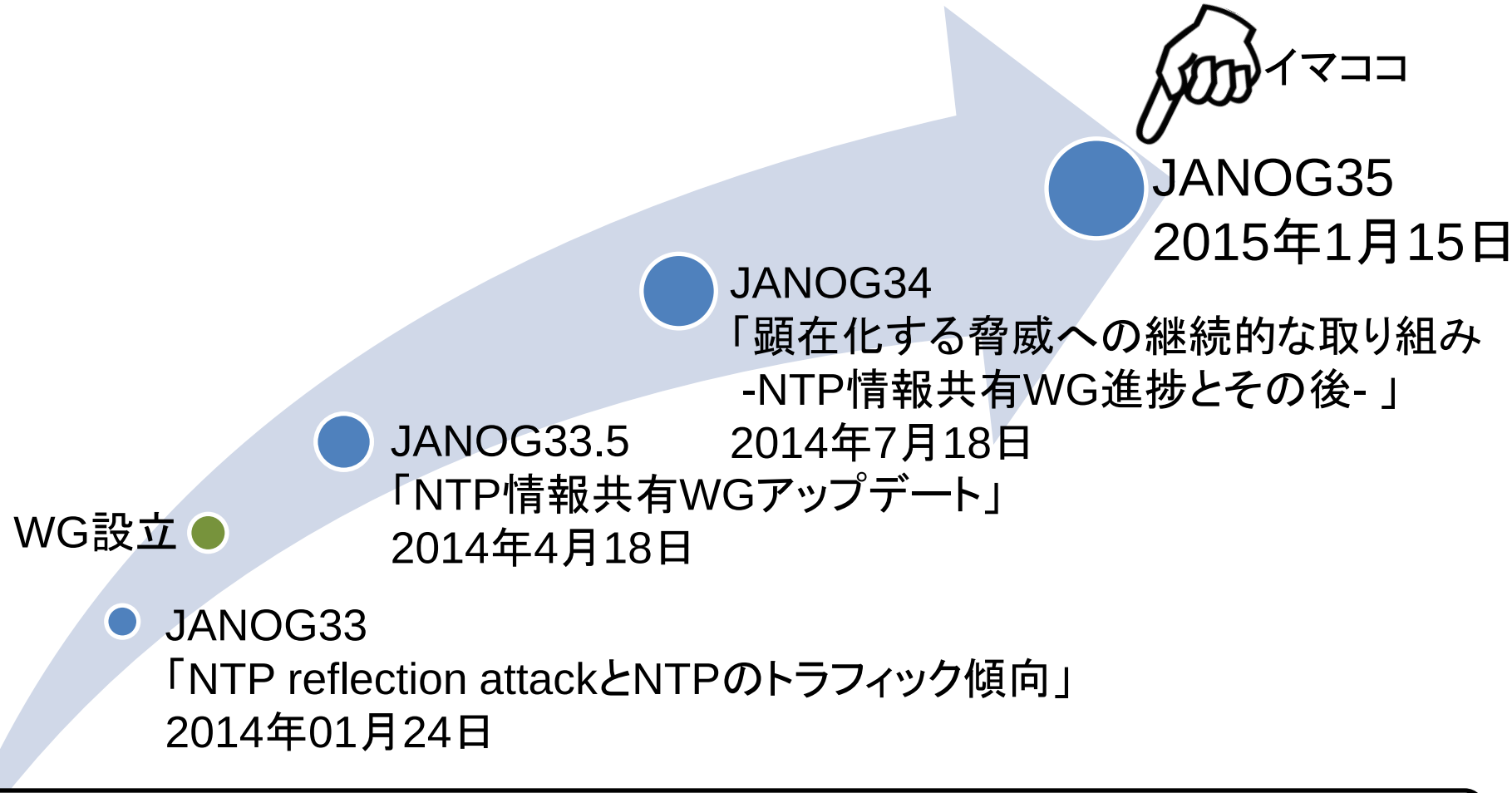
3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

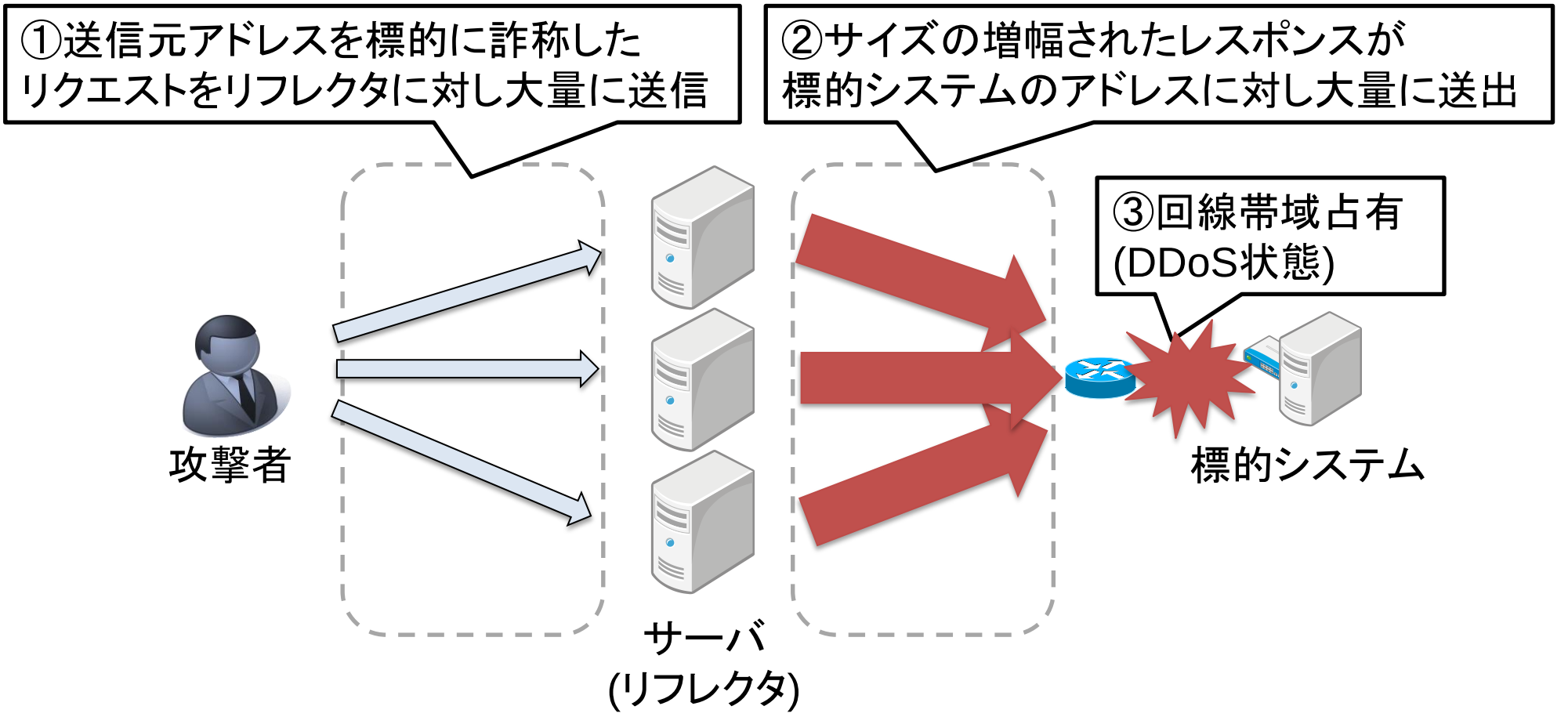
6.上記についてのディスカッション

[振り返り] これまでの経緯



JANOG33で取り組みをはじめてちょうど1年

[振り返り] UDPの送信元詐称を用いたDDoS攻撃

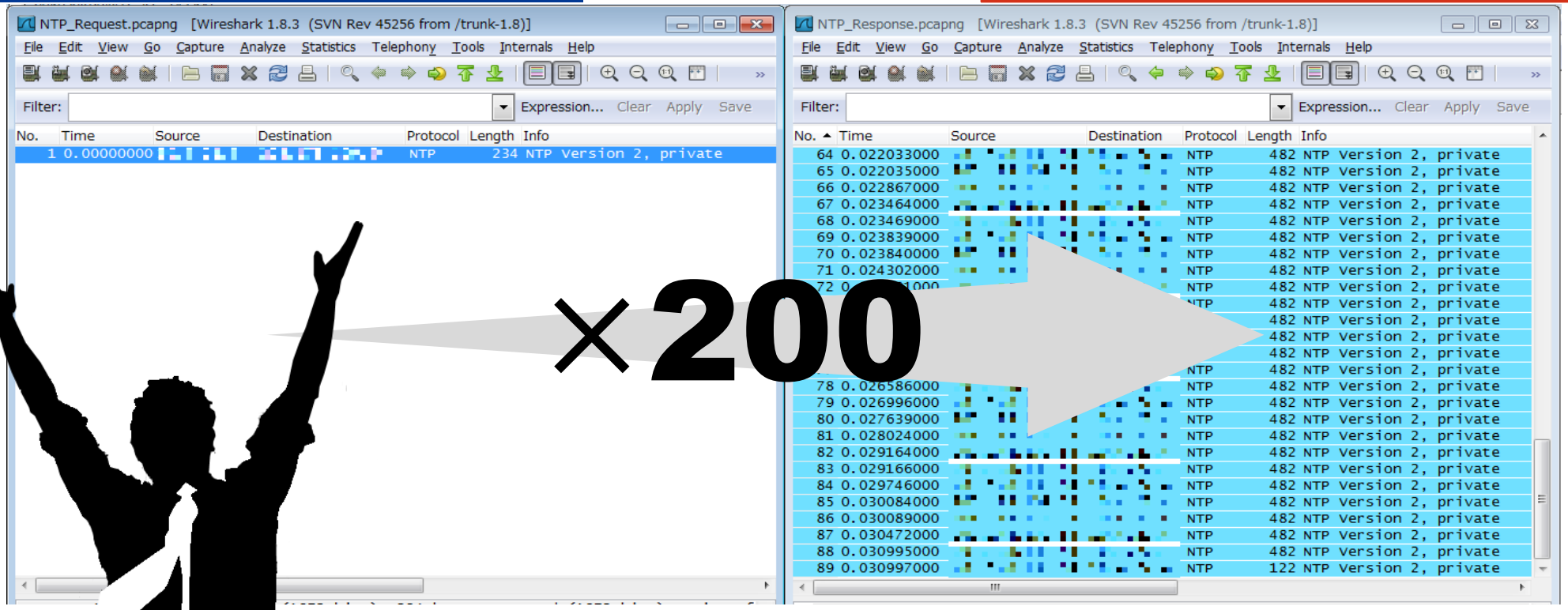


リクエストに対するレスポンスの**増幅率**が高く、**踏み台が多い**ほど効率的

[振り返り] NTP monlistコマンドの検証結果

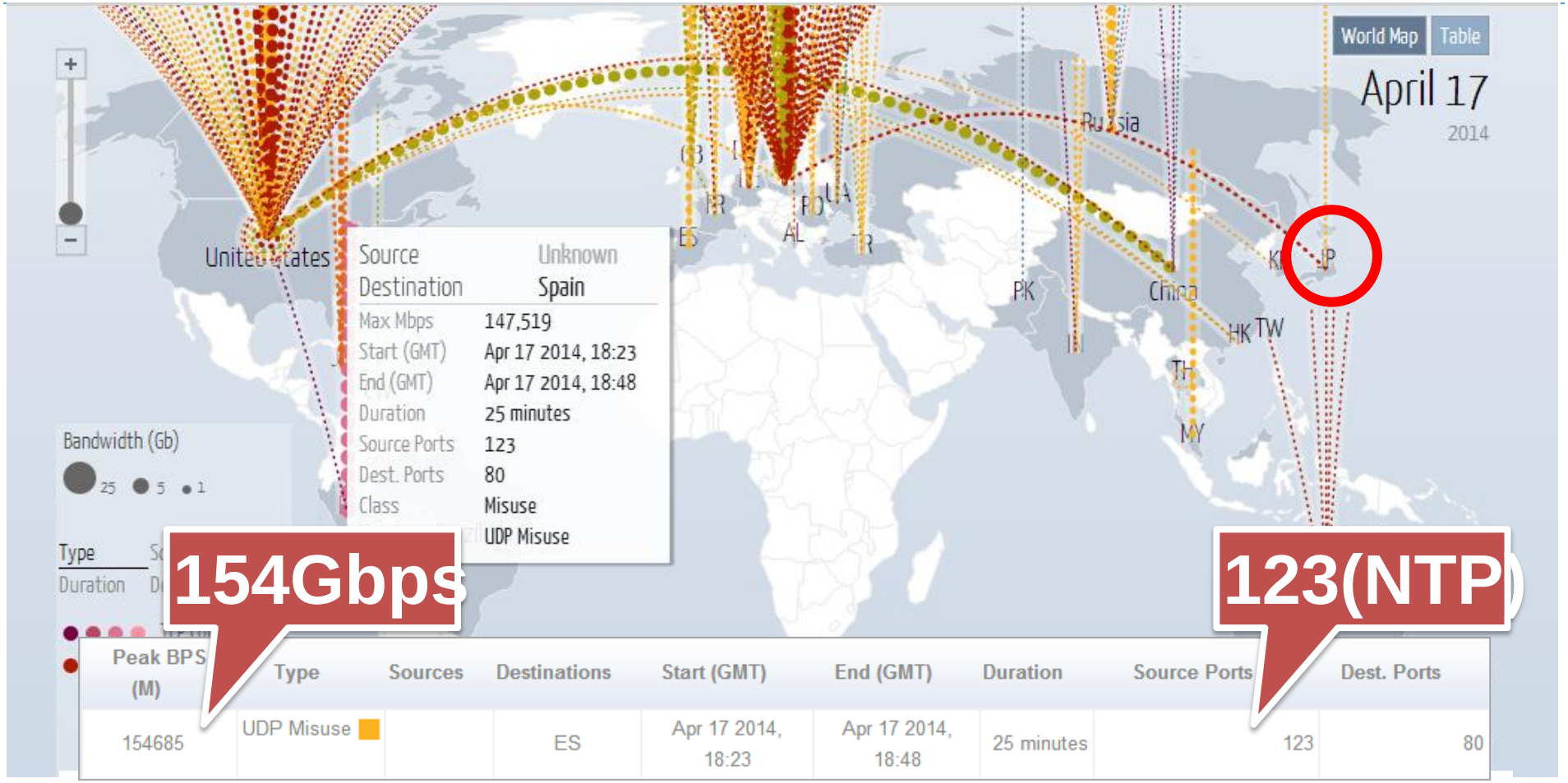
Request 234Byte

Response 44000Byte



増幅率が高いため、DDoS攻撃への悪用が極めて効果的

[振り返り] 実際の攻撃の観測



(引用元)Digital Attack Map Top daily DDoS attacks worldwide, http://www.digitalattackmap.com/

DDoSは日常的に観測

1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

6.上記についてのディスカッション

総務省研究会および関連団体における見解の公開

■概要

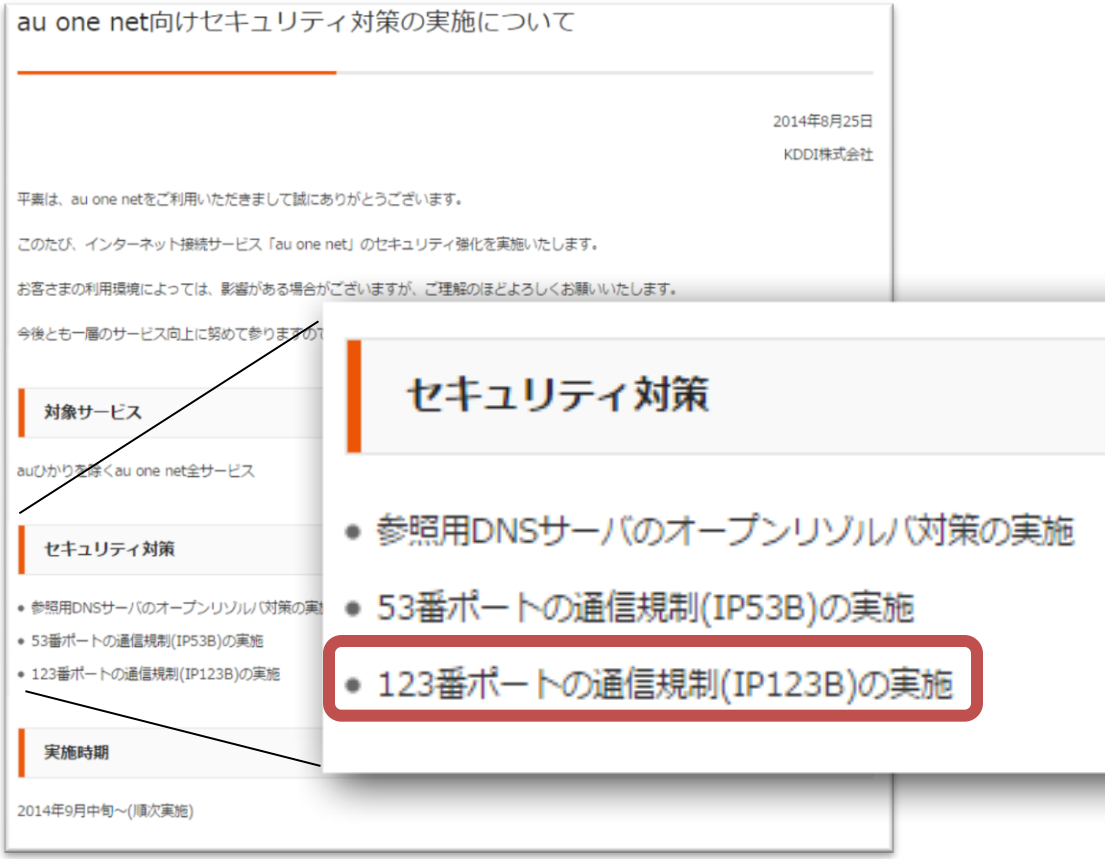
- NTPやDNSをはじめとする大量通信を用いた攻撃への対処とその適法性について言及
- とはいえ「個々の判断は実際の状況に応じて個別になされるべきものである。」という位置づけ

■原典

- 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」
  http://www.soumu.go.jp/main_content/000283608.pdf
- 「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン第三版」
  http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf

フィルタリング実施をアナウンスする事業者の登場

■セキュリティ対策の一環としてフィルタリングの実施を公に表明



原典：http://www.au.kddi.com/information/notice_internet/service/20140825-01/

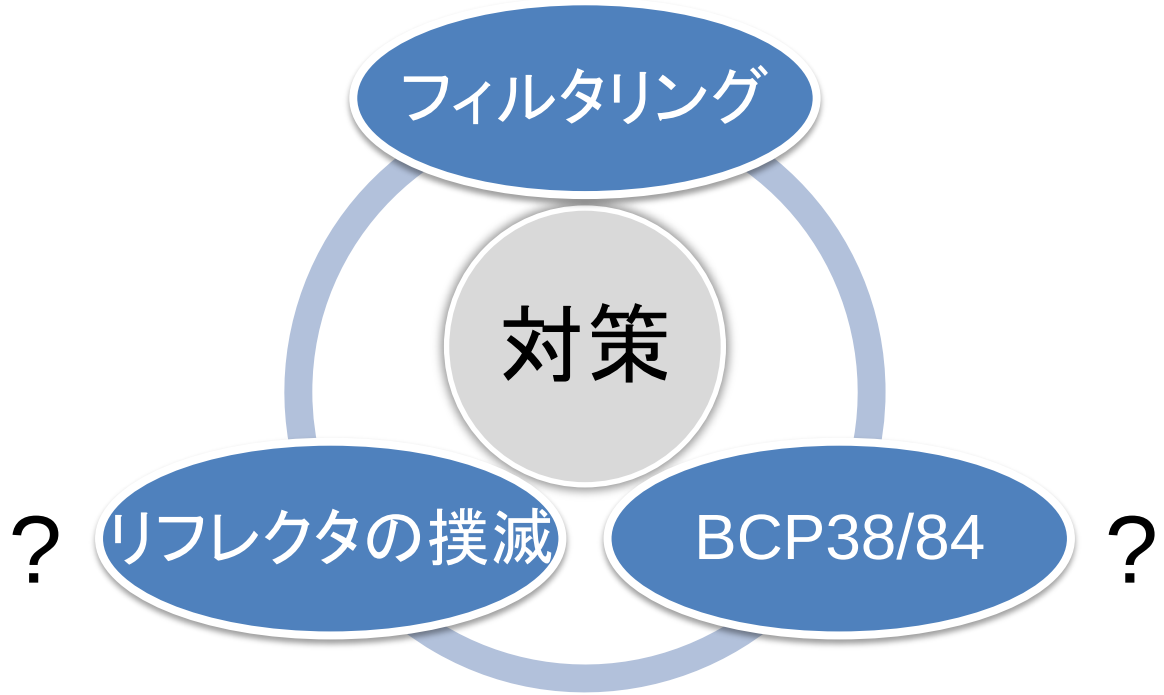
考察1

- 総務省の研究会をはじめとする場で対処方法に対する議論で、フィルタリング実施の後ろ盾となる一定の解釈がなされた

- フィルタリングできるできないの是否の問題から、どのように実装できるかの現場の問題に一段階ブレイクダウン
- 各社の実施状況や検討状況は不明であり、実装や実施のベストプラクティスはまだ導き出されていないと考えられる

考察2

■対症療法としてのフィルタリングについての議論が進む一方、根本療法としてのリフレクタの撲滅や、BCP38/84についての議論は進んでいないように見受けられる



1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

6.上記についてのディスカッション

3.ヒアリング活動の結果

得られた結果と課題

■WG活動の一環として事例や課題のヒアリングを実施

➔インシデントやその対応に関わる情報の取り扱いは難しく
オープンな場での情報共有は困難、このこと自体が課題

■事例の一部

- 観測トラヒック増加
- 機器の高負荷によるサービス断

■課題の一部

- フィルタリング実装箇所問題
- 網内のリフレクタをおおっぴらに調査していいのか問題

OpenXXXProjectの情報使えばいいじゃない・・・(ボソ

1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

6.上記についてのディスカッション

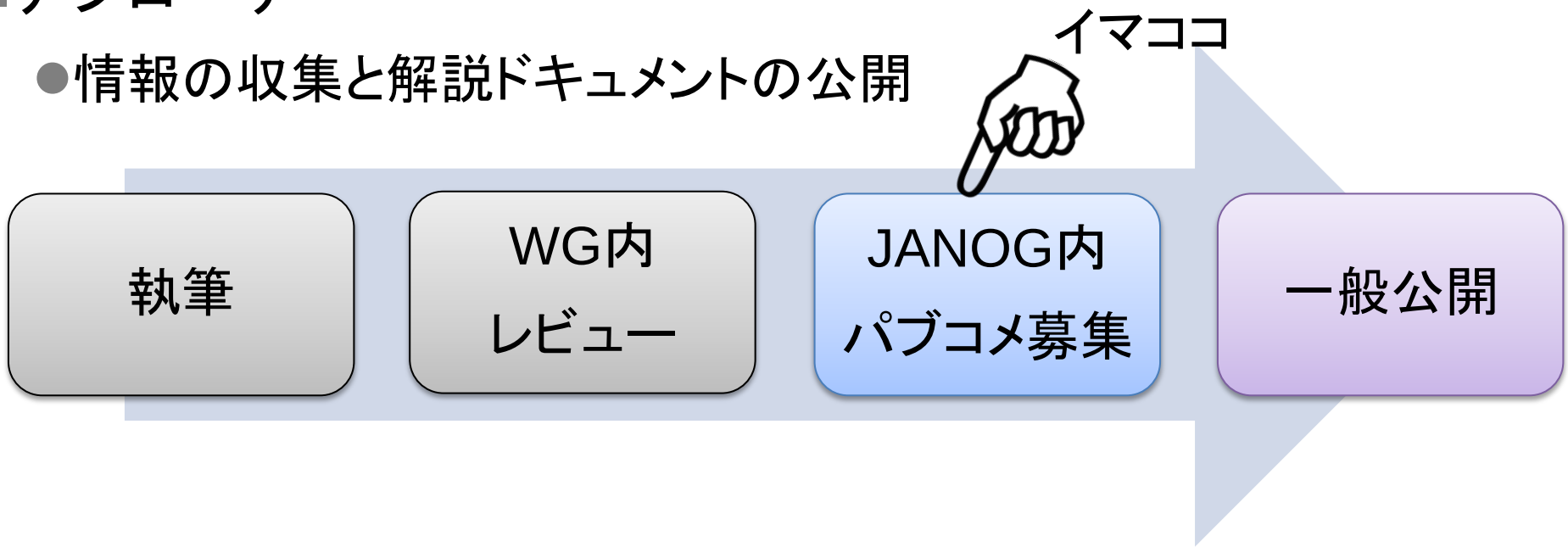
成果物の作成と公開

■問題意識

- 対策・啓蒙活動を進めていく上でのリファレンス先が不十分

■アプローチ

- 情報の収集と解説ドキュメントの公開



本プログラムのWebに公開しています

ドキュメント概要

問題点	海外および国内の事例の紹介とメカニズムの解説を通じて、本事象の問題点を解説
対策	事業者によって選択できる対策手法が異なる前提の下、全体像を示しつつ「攻撃から守る対策 」「悪用を防ぐ対策」を具体的に紹介
対応	実際にインシデントに直面した際の対応を「自社もしくは顧客のシステムが攻撃を受けた場合」「自社もしくは顧客のシステムが攻撃に悪用されている場合」に整理し紹介

特に期待するコメントのポイント

- 重要な観点の抜け漏れ
- 明らかな解釈・認識の違い

フィードバックの送付先などの詳細は
別途janog@janogに投げます。

まずは目を通してみてください！

1.はじめに – 背景の振り返り–

2.JANOG34以降の状況のアップデート

3.ヒアリング活動の結果

4.WG成果物の紹介とパブコメ募集のお願い

5.WGの今後の方向性についての報告

6.上記についてのディスカッション

WGを取り巻く状況と今後

■情報交換WGとしてのアプローチが困難な状況
- ●オープンな場で議論をすることは難しい
- ●議論した内容を共有することはさらに難しい

■一方で他のクローズドな場での議論は継続される予定
(例：先述の総務省研究会の第2次)

■これまでの活動とドキュメントの公開を以ってWGによる
現場レベルの情報共有は一定の役割を果たしたことになる

■WGとしての活動はいったんクローズし、
今後の情報発信は各所における議論をフォローし都度検討

ディスカッション前のまとめ

- JANOG以外のクローズドな場でも議論・検討が進む
- 公開ドキュメントにコメントをお願いします
- ドキュメント一般公開を以て情報共有WGは一旦クローズ
- 今後の情報発信は各所における議論をフォローし都度検討

帰社したら今回のJANOGの報告をしましょう(お約束)

ディスカッション

1. 事例・課題の共有
2. フィルタリング実装の検討進んでます?
   - 実装箇所(エッジ？コア？)
   - ブラックリスト/ホワイトリスト運用の必要性
   - 利用者に改めて告知する?しない?
3. 根本対策取り組んでます?
   - リフレクタ撲滅
   - BCP38/84
4. その他