JANOG34 Meeting

顕在化する脅威への継続的な取り組み
-NTP情報共有WG進捗とその後-

2014年7月18日

JANOG NTP 情報交換WG

中島 智広

メッセージ

■昨今の脅威の多くは、古くから問題点を指摘されていたものが長年放置され顕在化した物です。**今後も放置されている諸問題が悪用され、顕在化していく**可能性が高いと言えます。

「攻撃は、有効性が広く認知されることでさらに流行します。」

■各組織の状況が違いすぎて一般化して、足並みをそろえて議論することは困難です。数多ある問題点、顕在化する前に**現状認識から始めましょう。**

当たり前の話ですが、重要なので繰り返し言います

NTP情報交換WG

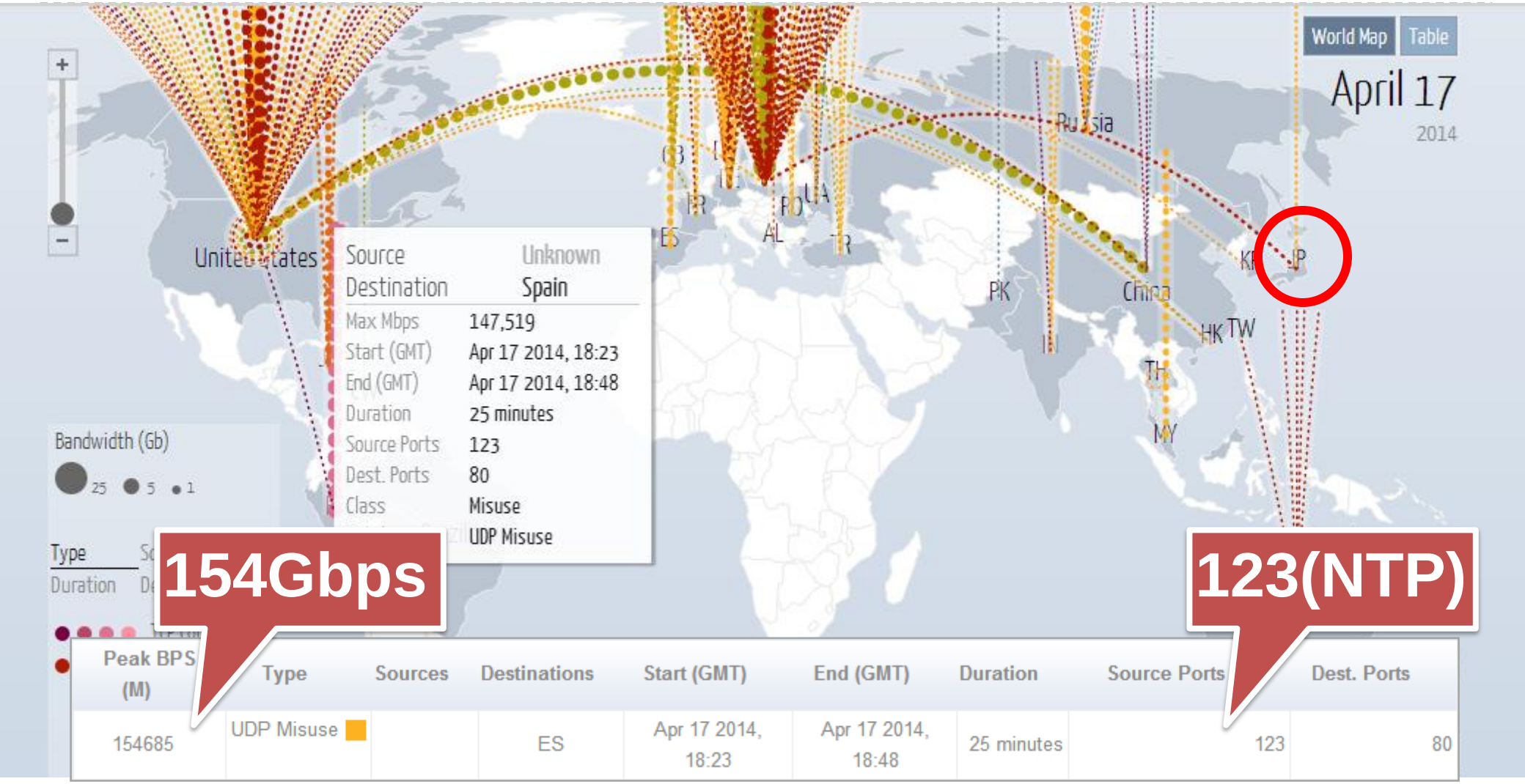
- 背景と問題意識(5分) 復習
- WG進捗(7分) アップデート

顕在化する脅威への継続的な取り組み

- 公開情報からみる現状 (5分) 本題
- あるべき論とギャップ(5分) 論点

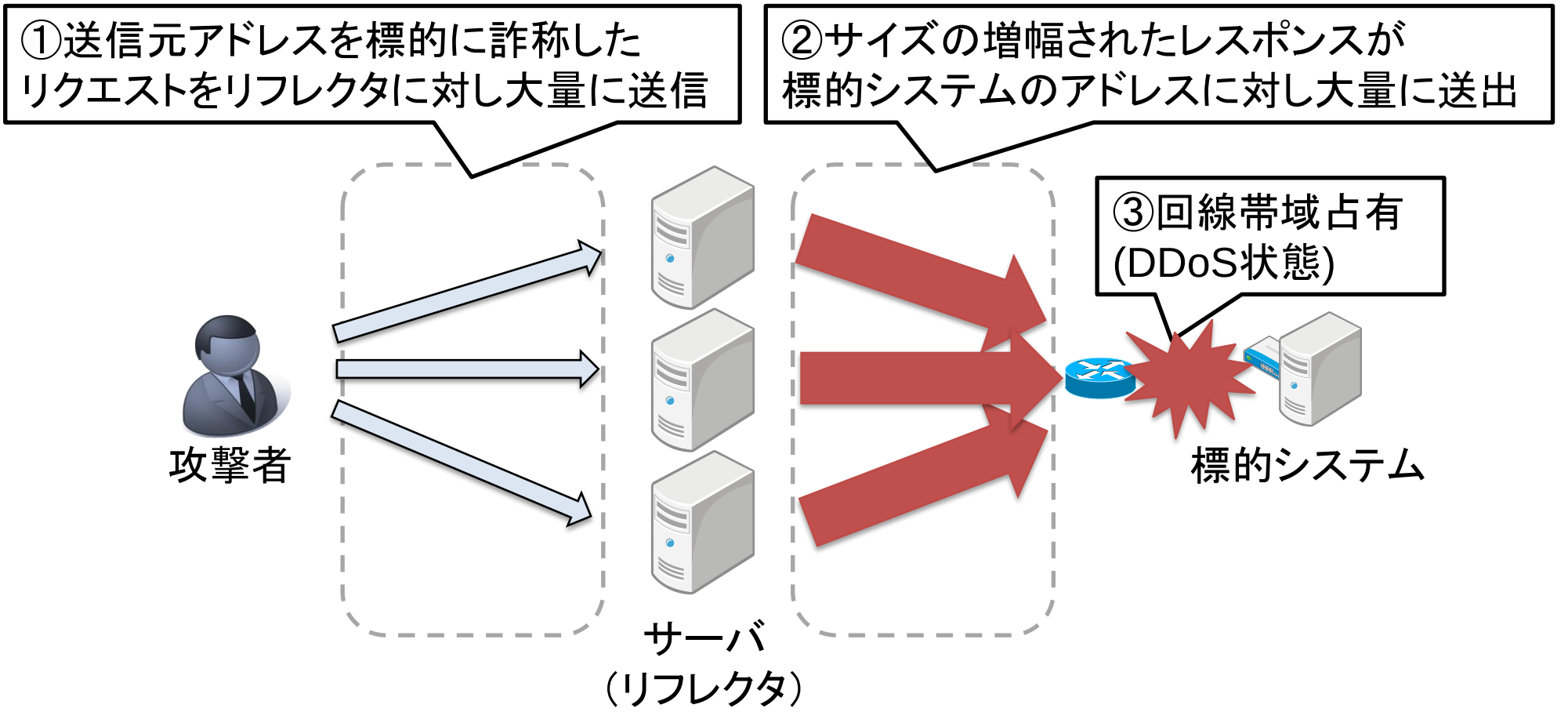
ディスカッション(18分) 混ぜる

とある日の世界の様子@JANOG33.5



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

UDPパケット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

悪用されがちなプロトコル/サービスの増幅率

Protocol	Amplification Factor	Vulnerable Command
NTP	556.9	monlist
CHARGEN	358.8	-
DNS	28 to 54	any など
SNMP	6.3	getbulkなど

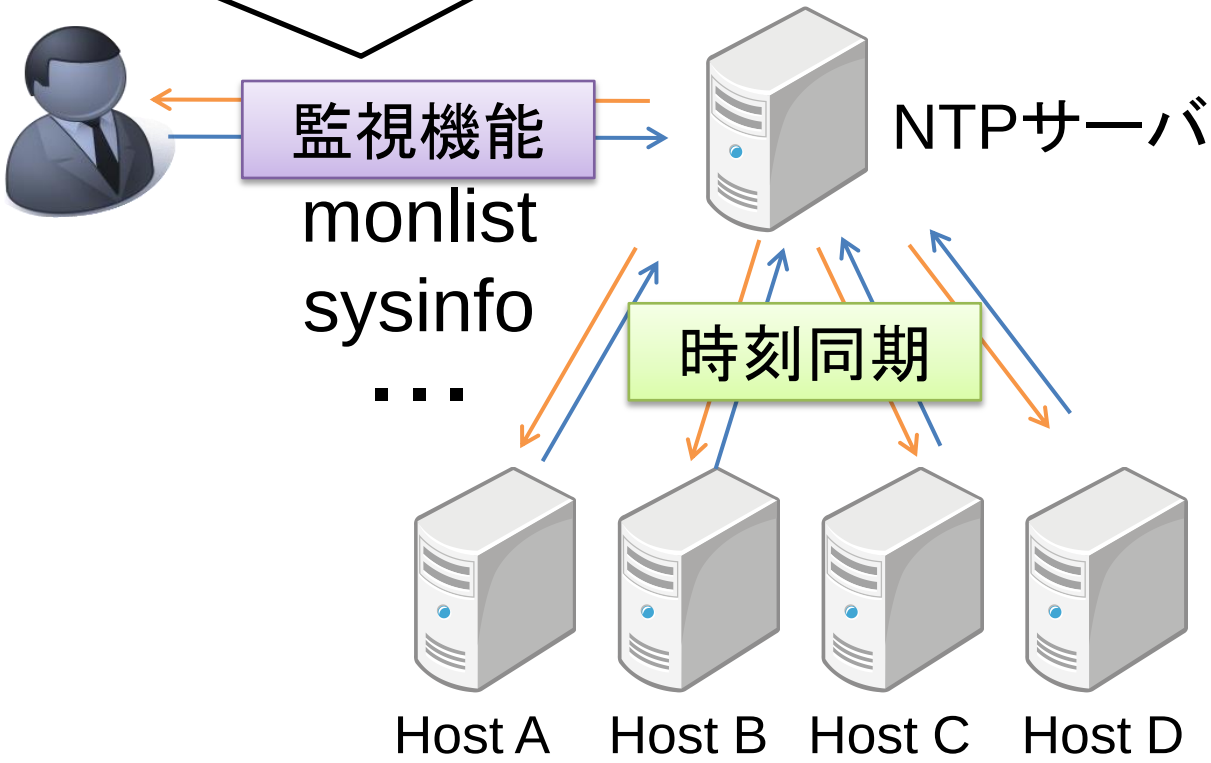
https://www.us-cert.gov/ncas/alerts/TA14-017A より抜粋

NTPの増幅率は圧倒的

NTP monlist

Remote Address	Port	Local Address	count	m	ver	rstr	avgint	lstint
Host A	xxxx	X.Y.Z.A	xxx	x	x	0	xxxxx	xxxxx
Host B	xxxx	X.Y.Z.B	xxx	x	x	0	xxxxx	xxxxx
Host C	xxxx	X.Y.Z.C	xxx	x	x	0	xxxxx	xxxxx
Host D	xxxx	X.Y.Z.D	xxx	x	x	0	xxxxx	xxxxx

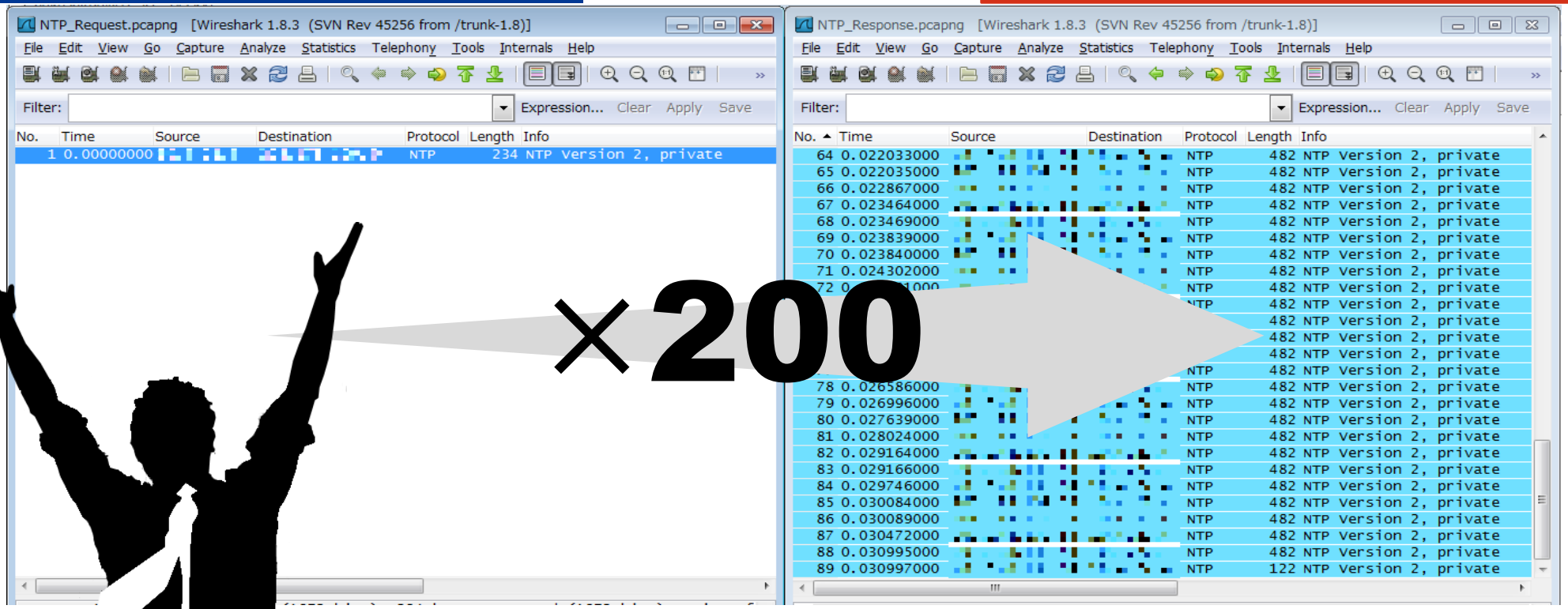
最大600件
=44,000Byte



論よりRun！

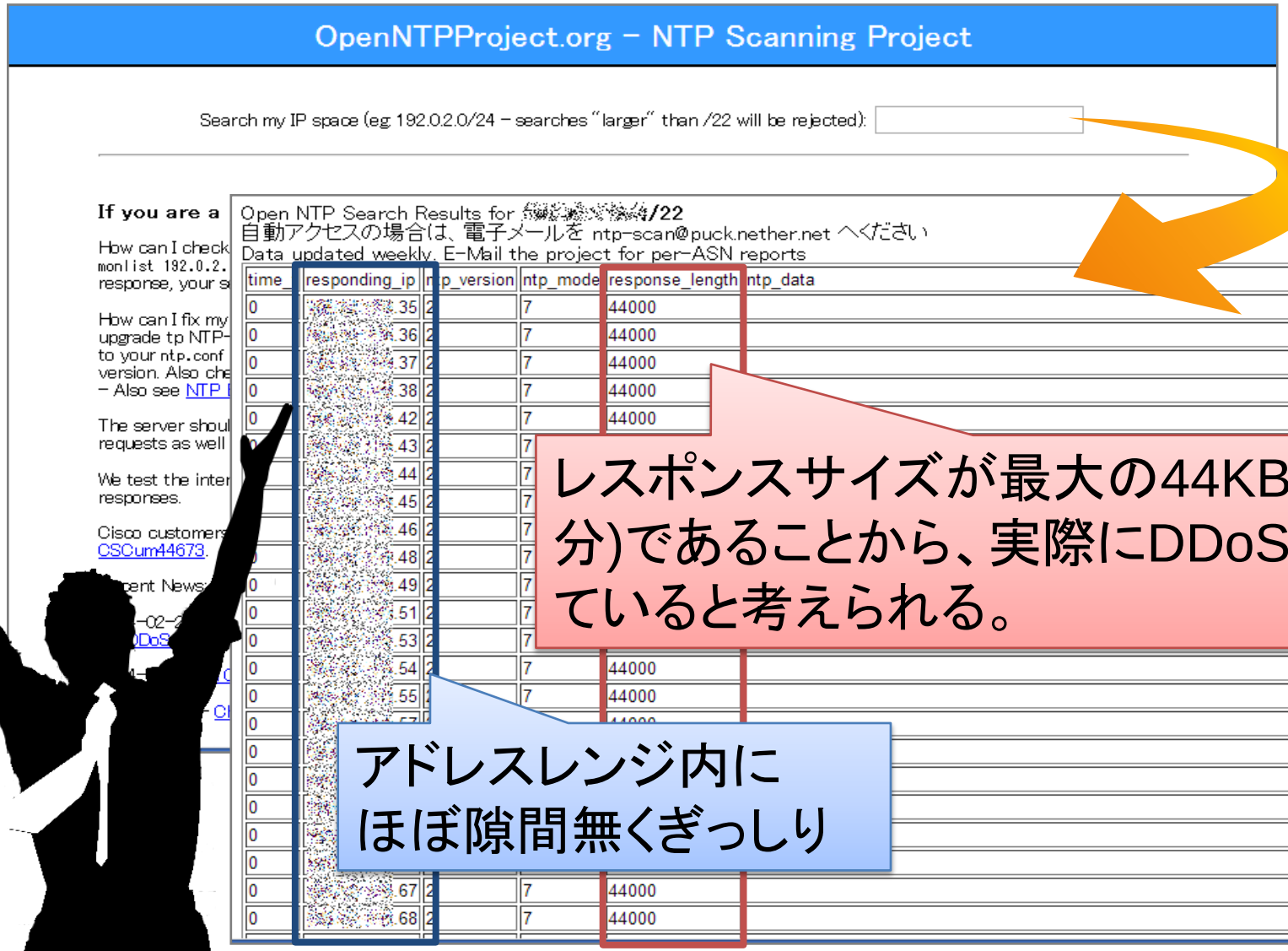
Request 234Byte

Response 44000Byte



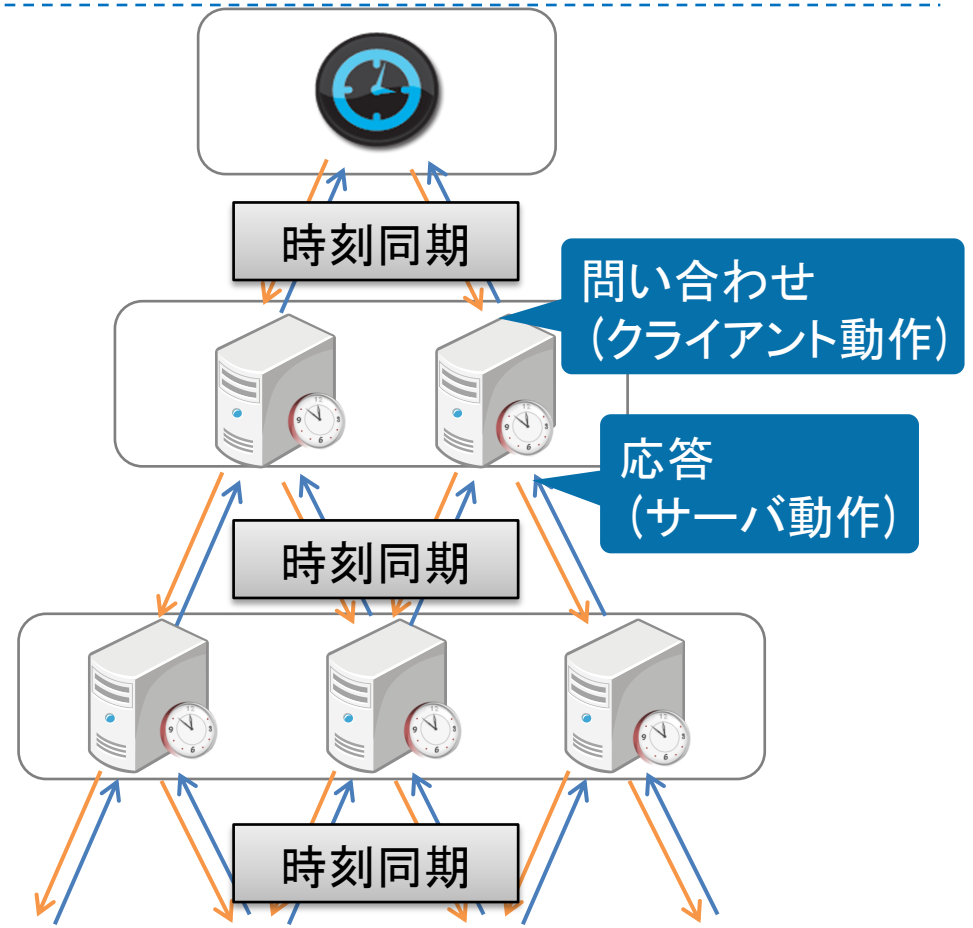
CloudFlare事例：平均 **87Mbps**/1リフレクタ

おびただしい数の踏み台



原因考察：管理者の理解不足と、デフォルト設定

- NTPデーモンは、クライアントでもありサーバでもある
- NTPデーモンはサーバ/ネットワーク機器のみならず、ありとあらゆる機器で利用されている
- NTPデーモンを積極的にメンテナンスする動機は稀、サーバ以外ではなおさら



NTPの階層構造

管理者が意識して制限しなければ、自ずとリフレクタになる

問題意識

- 100Gbps級だけでなく1Gbps級も十分な脅威
  - 5Mbps➔1Gbpsは容易に発生可能、
    サーバのNICはまだまだ1Gbps

- 危険性を訴えるだけでは誰も得をしない、
  技術的方法論だけで無く、収束へのアプローチが必要

- 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
  必要な人に、必要な情報が、伝わる記述で

NTP情報交換WG

- 背景と問題意識(5分) 復習
- WG進捗(7分) アップデート

顕在化する脅威への継続的な取り組み

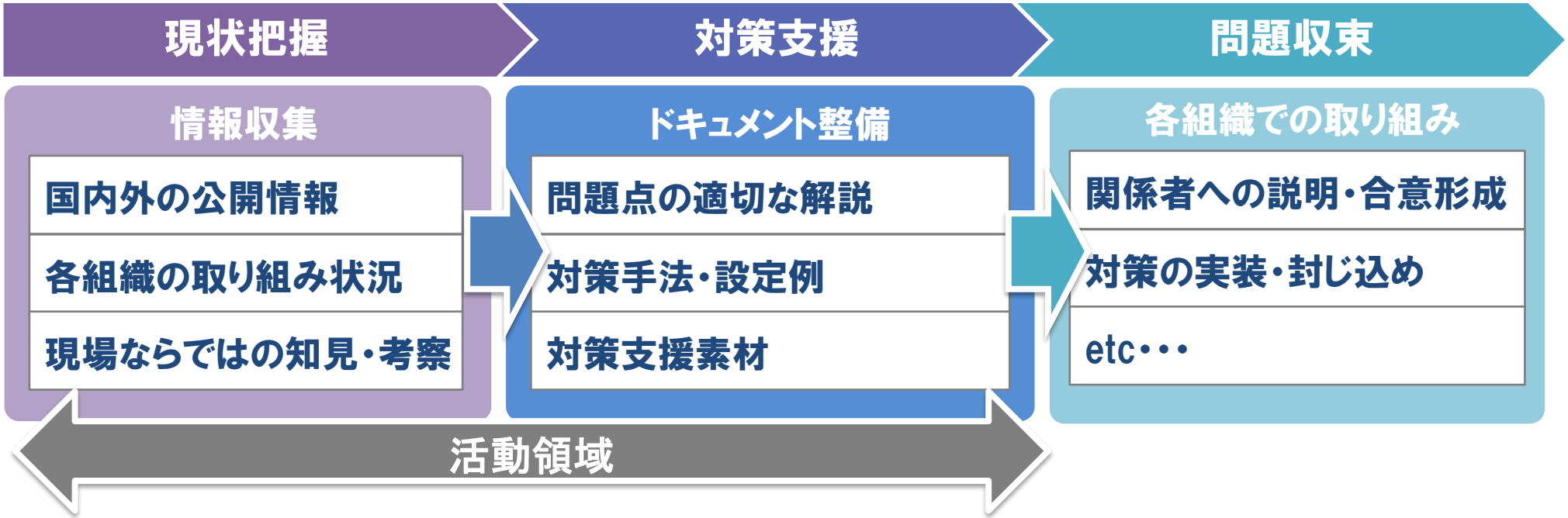
- 公開情報からみる現状 (5分) 本題
- あるべき論とギャップ(5分) 論点

ディスカッション(18分) 混ぜる

NTP 情報交換WG 概要

■目的

- ●NTP を用いたDDoS攻撃の現状把握を行い、
  ドキュメント整備を通じて対策を支援し、問題の収束に資する



活動スタンス

■スコープ

- UDPパケットの送信元詐称を用いたDDoS攻撃はNTPだけの問題ではないが、まずは悪用が容易かつ破壊力の高いNTPを喫緊の脅威ととらえ焦点を絞って活動

■スケジュール

- ~~ドキュメント整備はJANOG34を目処に完了させたい~~ **m(_ _)m**
- 少々時間がかかってもきちんと使えるドキュメントを整備、タイミングが遅れ、世の中に必要とされなくなったとして、それはそれで幸いなこと

活動経過

■第1回ミーティング(2014年2月14日)

- 持ち寄った情報で議論、叩き台文書を作成することになる

■第2回ミーティング(2014年3月28日)

- 叩き台文書(A4×9枚)を元に議論、成果物の骨子を確定
- 「詳解編」の執筆を割り当て、JPCERT/CC担当者との情報共有

■第3回ミーティング(2014年5月1日) Update!

- 「詳解編」の進捗と内容レビュー、公開へ向けての議論
- 次の成果物「設定編」の進め方の議論

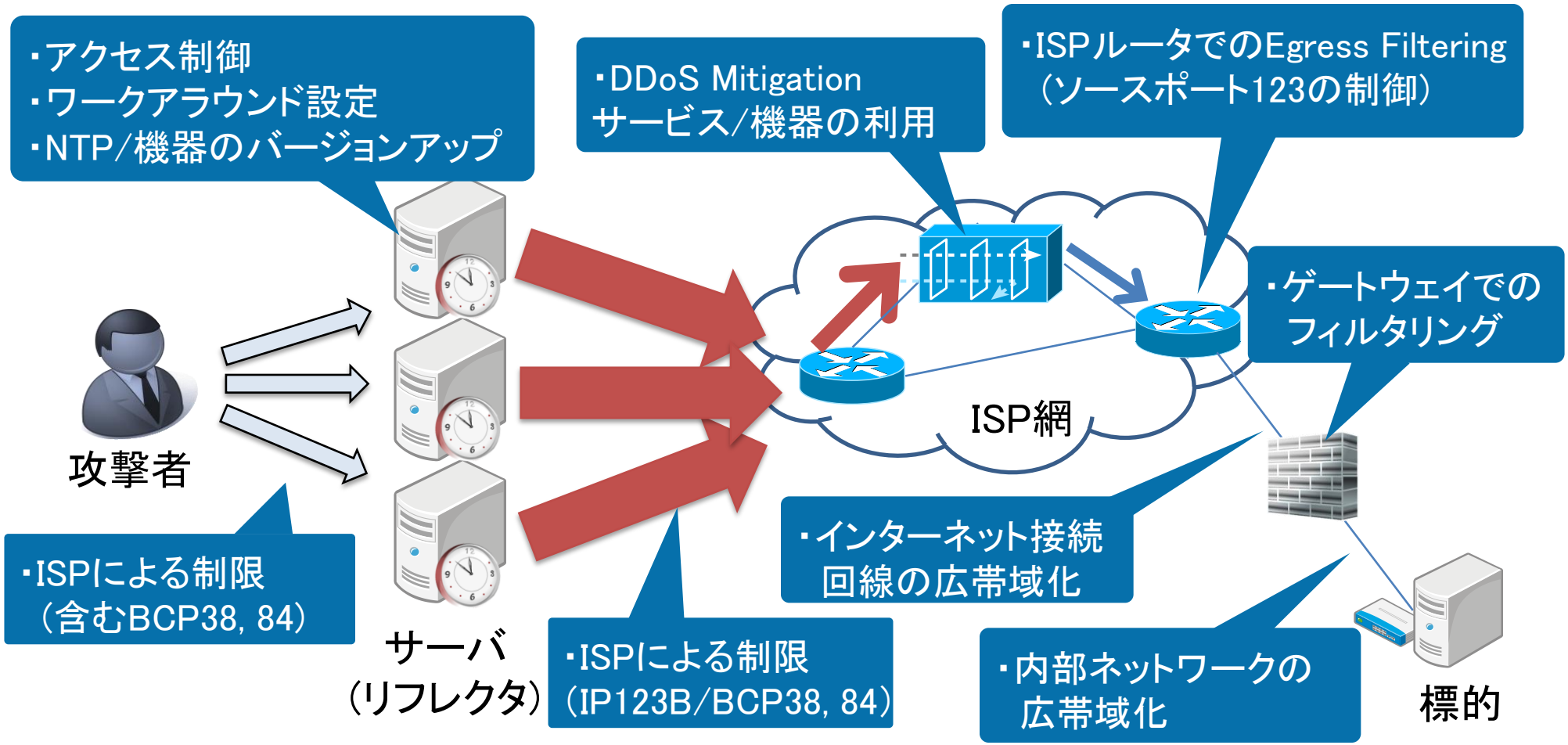
成果物構成

1.詳解編	A4 10頁超の長めの文書。これさえ読めば、課題と取り組むべき内容をひと通り把握できる。対象はエンジニアや、情報システム担当者。
2.設定編	具体的な設定例や対策例を、機器種別ごとに整理。対象は、エンジニア。
3.簡易解説編	取り組みに理解を示してもらい、協力を得るための読みやすい資料。A4一枚。対象はITに疎い関係者及びエンドユーザ。
4.テンプレート編	関係者への説明や合意形成に利用可能なテンプレート。対象はxSP事業者。

成果物と進捗

#	成果物名	進捗	状況
1	詳解編	 95%	公開レビューまであと一歩
2	設定編	 10%	大方針は固まるが、 ニーズの再確認が必要
3	簡易解説編	 0%	詳解編が完成してから検討
4	テンプレート編	 0%	未検討

余談：対策ポイントの全体像（?）

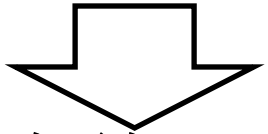


技術論だけでなくインシデント対応の話もある

余談：95%ルールとモチベーション

■状況の変化

- ●(過去)DDoSはコストが高いため長時間継続することは希



- ●(現在)95%ルールで救えなくなってきていないか？
  - ・DDoSを受ける場合：5%=1.5日
  - ・リフレクションに悪用される場合：定常的なトラヒック増

■仮説

- ●きちんとOpenNTP/OpenResolver対策を進めた組織には、目に見えない形でコストメリットが出ているのではないか？
- ●トランジットを売る側からすると・・・

余談：思っていること

- 非公開のDDoS攻撃事例を共有したところで
  興味・関心を満たす以上のものはない

- 対策手法やインシデント対応の知見、ノウハウを
  共有してこそ価値がある、やらない理由の共有はマイナス

- 日本は、世界的に見ても1回線当たりで送出可能なトラヒック
  が大きいため、攻撃の踏み台として非常に魅力的ではないか

これからも

■問題収束はみなさんと力をあわせて取り組んで行く必要があります。上手く収束させていくために改めて協力して行きましょう。組織の大小関係ありません。

NTP情報交換WG

- 背景と問題意識(5分) 復習
- WG進捗(7分) アップデート

顕在化する脅威への継続的な取り組み

- 公開情報からみる現状 (5分) 本題
- あるべき論とギャップ(5分) 論点

ディスカッション(18分) 混ぜる

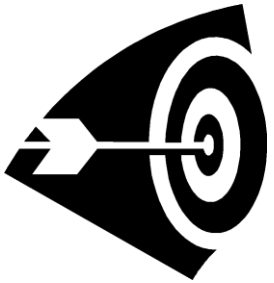
攻撃者の特徴と攻撃の傾向

■目的別に攻撃者を分類すると…

- 愉快犯型・劇場型
- 金銭目的型
- 政治目的型（Hacktivism）
- 諜報活動・サイバー戦争型

■攻撃タイプで分類すると…

- 攻撃対象を絞った攻撃が多発
- 無差別型から標的型へのシフト傾向



ごく最近のDDoS事例

2014年06月12日 07時50分 更新

EvernoteやFeedly、DDoS攻撃で一時ダウン――金銭の要求も

EvernoteやFeedlyが相次いで障害に見舞われた。Feedlyは攻撃を止める条件として金銭を要求されたという。

2014年06月23日 14時19分 更新

DDoS攻撃で停止の「ファンタシースターオンライン2」、再開できず　「攻撃規模、極めて大きい」

DDoS攻撃を受けてサービス停止中の「ファンタシースターオンライン2」（PSO2）が、23日になってもアタックがやまず、再開できない状態に。

Emerging Threat - Anonymous - Operation Petrol (June 20 2014)

Created: 13 Jun 2014 • Updated: 13 Jun 2014

MSS Global Threat Response　SYMANTEC EMPLOYEE

+1
1 Vote

Symantec. | Official Blog

(補足)日本企業も具体的な対象として注意喚起された

ポイント

- 明確な目的(金銭、主義主張)

- 攻撃手法の複合化傾向(コンビネーション)
  - 例)NTPとDNSとCHARGENとSYN FLOODとSlowLoris、etc…

- 攻撃の長時間・長期間(断続)化

➔それらを支える攻撃インフラの低コスト化(仮説)

攻撃の敷居が下がり、効果・旨味が増している

頭の痛い話

- あれもこれもそれもやらないといけません
  - IP***Bというだけでもない
  - BCP38, 84ですら十分ではない
- 思考停止、したくなりますよね?

それでは、攻撃者の思うつぼです

NTP情報交換WG

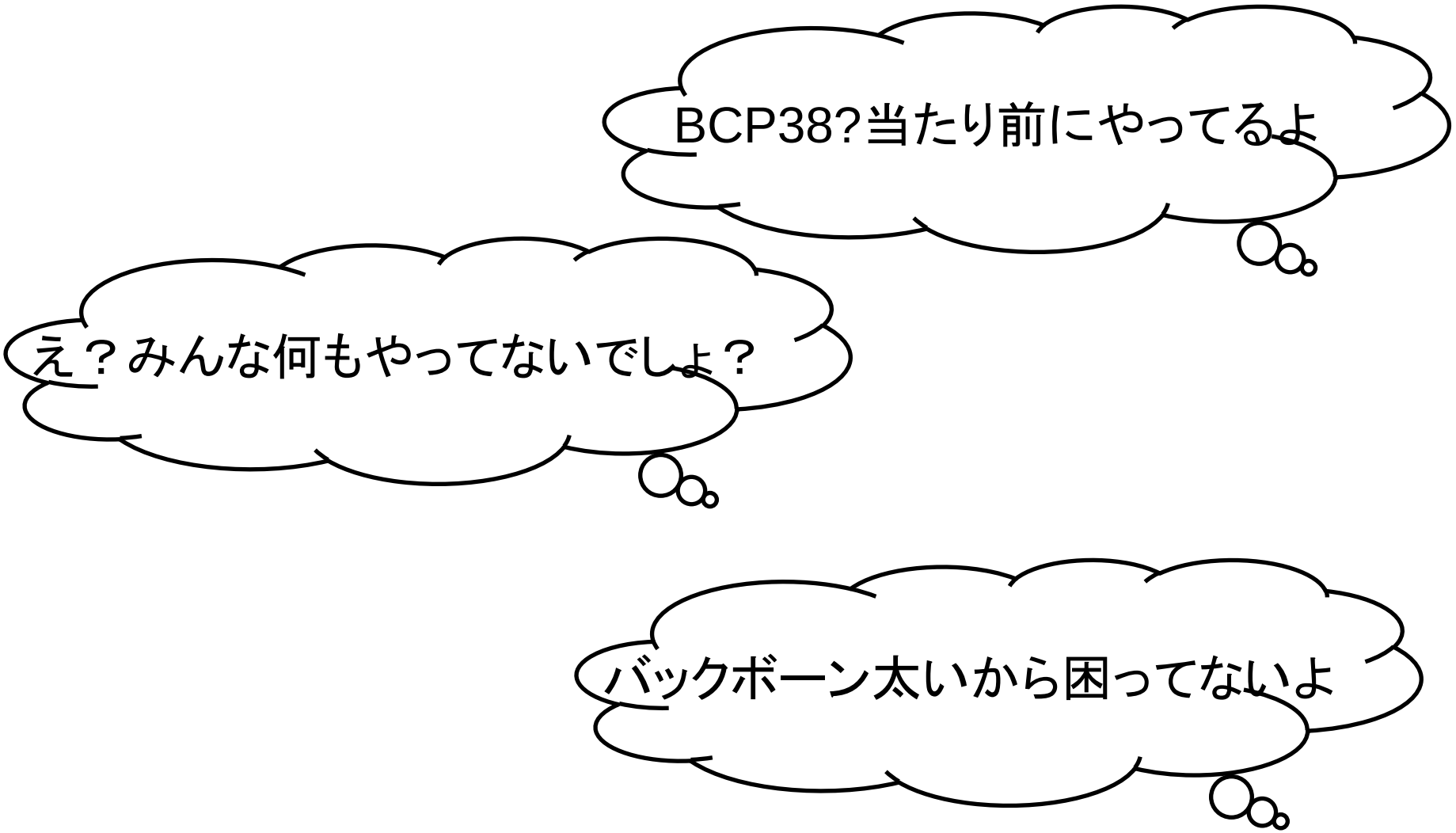
- 背景と問題意識(5分) 復習
- WG進捗(7分) アップデート

顕在化する脅威への継続的な取り組み

- 公開情報からみる現状 (5分) 本題
- あるべき論とギャップ(5分) 論点

ディスカッション(18分) 混ぜる

温度感、ぜんぜん違う・・・



喰らってみないと駄目なのか・・・?

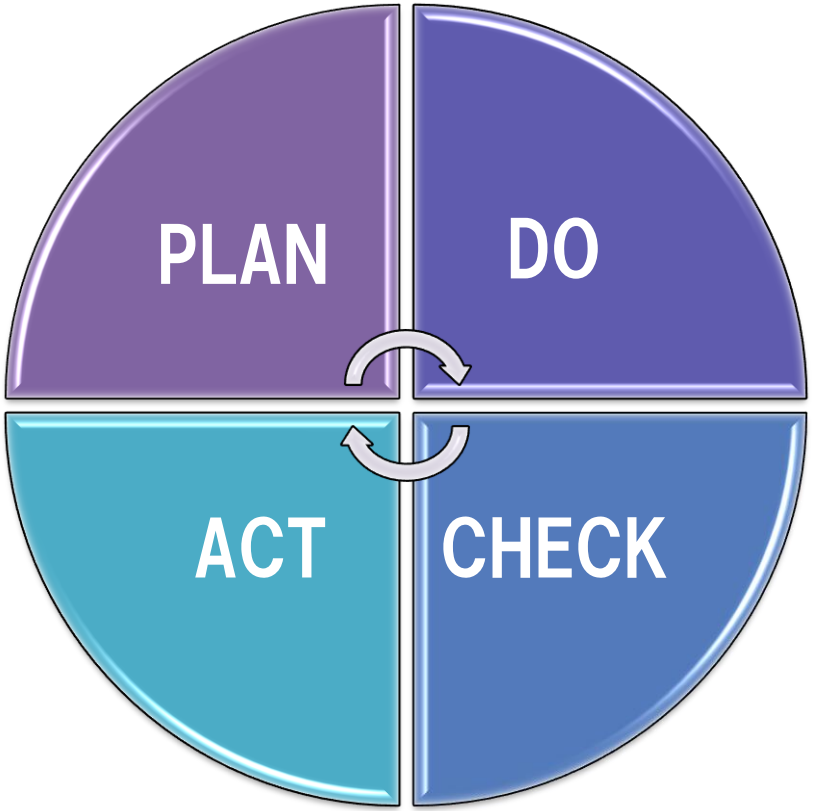
■JANOG34 Day0 BoF
「ブロッキング・フィルタリング ぶっちゃけBoF」
「我慢する?あきらめる?工夫する?大量攻撃トラフィック対応」
オープンリゾルバ悪用によるキャッシュDNSサーバ高負荷問題

Q.では、自社網にどのくらいオープンリゾルバがあるか把握してる方?

A.手を挙げたのは2割くらい・・・

問題意識を持ってBoFに来ている人でもこのくらい?

お願い



対策の実行までは難しくとも、現状把握だけはしましょう

ありがちな構図

■管理職/経営層

- ●何か起きてからでいいんじゃないか?
- ●他社がやっていないならやらなくていいんじゃない?
- ●当期の利益率を落としたくないから後回し

■現場担当者

- ●何か起きてからじゃ遅いよ・・・
- ●実際に目の当たりにしてるんだよ

ん?どっかで見た構図だぞ???

攻略のヒント

■潮目の変化を見逃さない
- ●管理職・経営層の異動
- ●世の中のインシデント

■定期的にいい続けること
- ●定点観測とアップデート
- ●定期的なイベント報告

まず、今回のJANOGの報告をしましょう

[再掲] メッセージ

■昨今の脅威の多くは、古くから問題点を指摘されていたものが長年放置され顕在化した物です。**今後も放置されている諸問題が悪用され、顕在化していく**可能性が高いと言えます。

「攻撃は、有効性が広く認知されることでさらに流行します。」

■各組織の状況が違いすぎて一般化して、足並みをそろえて議論することは困難です。数多ある問題点、顕在化する前に**現状認識から始めましょう。**

当たり前の話ですが、重要なので繰り返し言います

ディスカッション／コメント募集

- NTP情報共有WGへの期待・要望・苦情
  - いろいろあった方がいい、はわかるけど、何が本当に必要?
  - 何があれば対策進む?
- 各組織ごとの状況の違い、なんなんだろう?
- 改めてBest Current Practice(38/84以外も)について
  場を設けたら前向きにざっくばらんと議論できます?
- 顕在化寸前の放置されている次の課題ってなんでしょう?
- そのほか、言いたいことある人どうぞ！