JANOG38 BoF議論まとめ

増え続けるDDoS攻撃に対抗するために
事業者間で協力してできることBoF

JANOG38 BoF まとめ

■ 増え続けるDDoS攻撃に対抗するために事業者間で協力してできることBoF

■ 開催日

- 2016.07.06 17:00-18:00 JANOG38 沖縄

■ 参加者について

- 参加者層
  - ✓ 全体 87名
  - ✓ ISP, IXP, DC, CSP, エンタープライズ, 学術
  - ✓ DDoS対策提供者: 30名程度
  - ✓ DDoS対策利用者: 30名程度

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

今あるサービスについて

1. RTBH(Remote Triggered blackhole)
2. ACL
3. 増設による対策(CDN等)
4. クラウド型DDoS対策(緩和サービス)

提供者側から見て、利用者から見て、メリット/デメリットや要望についてのコメントはありますか？

今あるサービスについて(会場コメント)

- RTBHの頻度はどのくらいなのか？
  - 多い時では1日に何十回というケースも
- RTBHのスケーラビリティは？
  - パケットを捨てる動作については、null0に落とすのでそこまでキツイわけではない
- RTBHは攻撃が実際止まっているかがわからないが、IXPからも一部流れ込んでくるので、それで攻撃が止まったか判断することはある
- 日本は特定国(中国・韓国)からのDDoS攻撃が特に多いので、国でRTBHまでしなくて良いが、shapingの機能は欲しい
- ISPの立場では、Blackholeで止めればよいと考えていたが、コンテンツプロバイダとしては、RTBHは何も守っていないことになるので、緩和する対策が欲しい
- RTBHはIPv4だと簡単だが、IPv6になると複数アドレスを指定する必要があるので、単位が/128は適切なのか考えたい

事業者間の連携について

1. 利用者と提供者の連携
   - 仕様の統一は必要だと思いますか
   - どのようにしたらより上手く連携できますか

2. 提供者間の連携
   - 必要だと思いますか
   - 必要だとしたらどのような形が考えられますか

事業者間の連携について(会場コメント)

- 事業者連携のケースでは、DDoS攻撃のトラフィックを減らすことで、2次ISPへのトランジット収入が下がるという側面も考えないといけない
- 攻撃をいつ受けるかわからないので、保険のようなサービスで解決をするというのもありうるのでは
  - 保険にしてしまうと、結局攻撃者の思惑通りとなってしまう
- 事業者連携のケースはいつか必要となるので今のうちから考えておかないといけない

DDoS攻撃/対策の今後について

1. DDoS攻撃はいつまで続くのか
   - 防御側不利の状況はいつまで

2. 今後のあるべき対策
   - 対策手法への理解は十分か
   - DDoS対策のコストと仕様は見合っているのか

3. DDoS対策事業者への期待
   - SOCなどマネジメントの充実
   - コスト/競合環境
   - Scrubbing centerの場所
   - 仕様の統一

DDoS攻撃/対策の今後について(会場コメント)

- DDoS攻撃はもう止まらないし無くならないのでは
- 攻撃のブローカー(booter)だけでなく、bot用PCの提供などのエコシステムが出来上がっており、その中の一つのところを規制するようなやり方だけではうまくいかない
- ネット上でクラウドサービス型のDDoS防御を比較出来るサービスがある
  - その比較は都合が悪いことは隠されており、実際に導入してみると上手くいかないことがある。特にトラフィックの戻しはトラブルが多い
- 攻撃を止める場所についてはなるべく分散している方がよいが、日本のトラフィックの在り方に適した形があると思われる