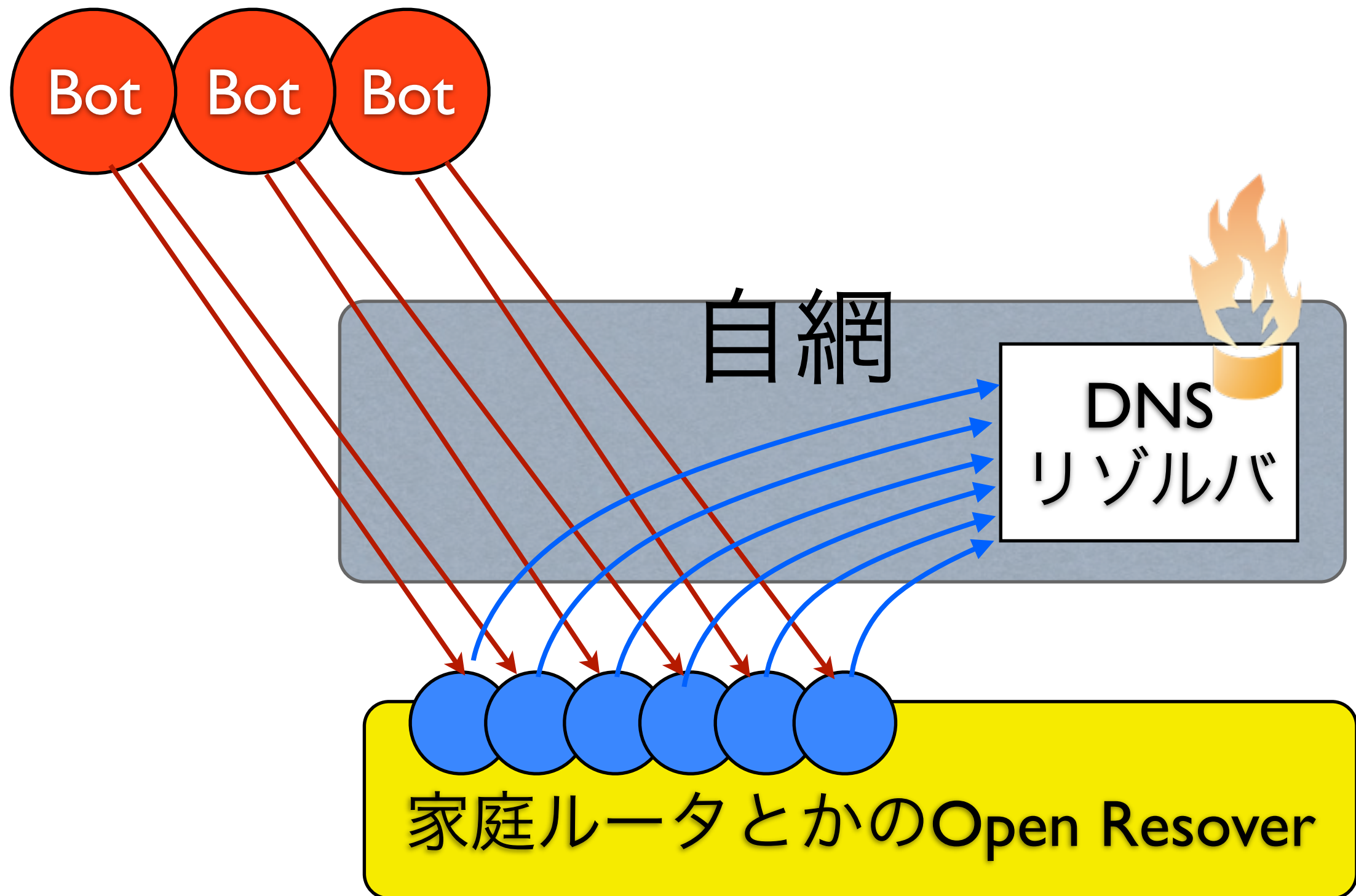


オープンソースでキめる DDoSトラヒック分析

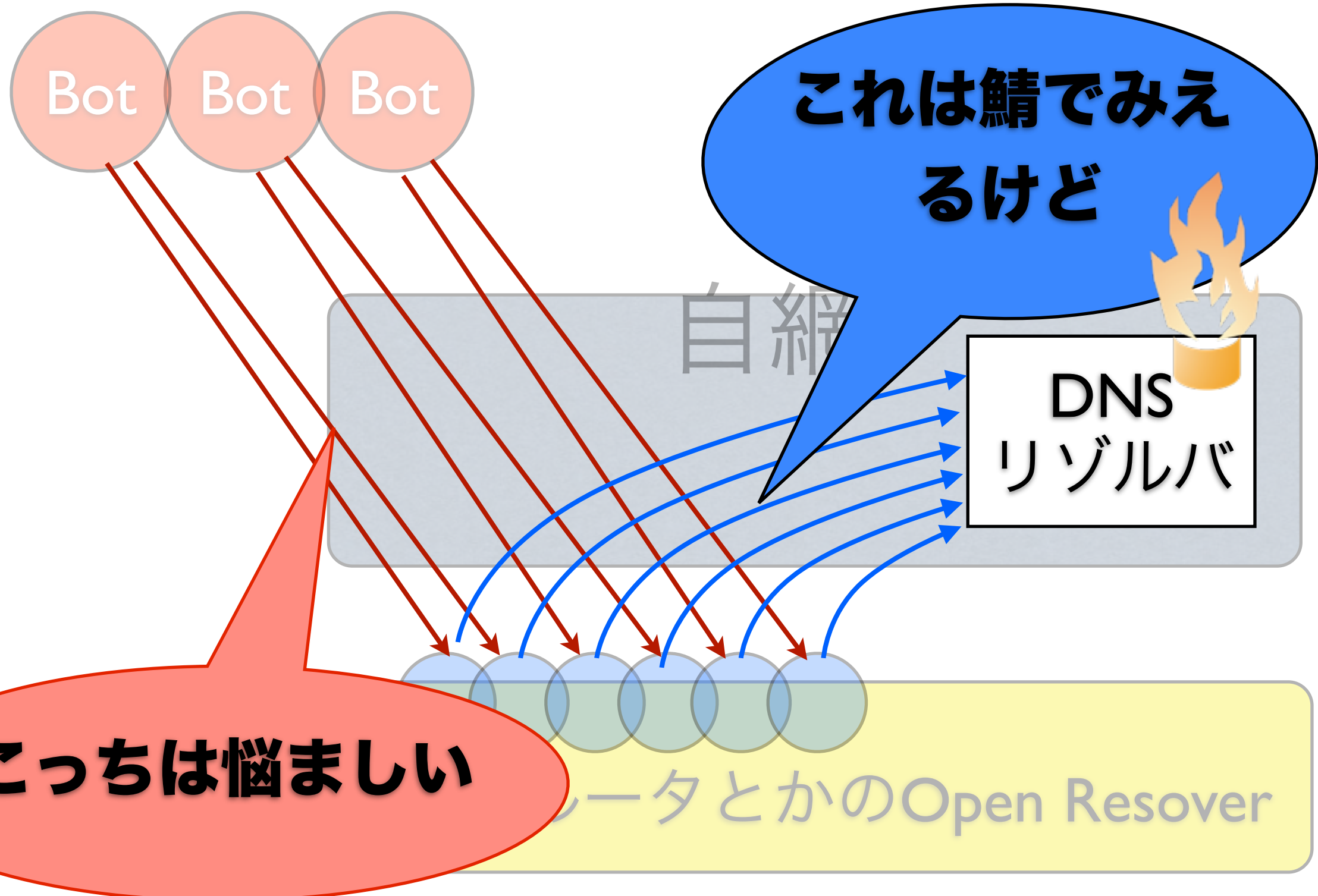
田島弘隆(Genie Networks)

JANOG34
Jul.2014

NTP/DNS attack多し



「あやしいパケットを監視しましょう」 っていうけど。。。



DBに突っ込む

stamp_inserted	ip_src	ip_dst	port_dst	packets	bytes
-----+	-----+	-----+	-----+	-----+	-----
2014-07-18 04:14:00	100.0.0.1	10.0.0.13	53	10179896	371162832
2014-07-18 04:14:00	100.0.0.2	10.0.0.12	54	10173829	370799712
2014-07-18 04:14:00	100.0.0.1	10.0.0.11	53	10140321	372540530
2014-07-18 04:14:00	100.0.0.2	10.0.0.13	54	10121036	376238388
2014-07-18 04:14:00	100.0.0.1	10.0.0.12	53	10132434	374899934
2014-07-18 04:14:00	100.0.0.2	10.0.0.11	54	10170474	371333024
2014-07-18 04:13:00	100.0.0.1	10.0.0.11	53	11107253	409788396
2014-07-18 04:13:00	100.0.0.2	10.0.0.13	54	11058126	403499564
2014-07-18 04:13:00	100.0.0.1	10.0.0.12	53	11055127	404444180
2014-07-18 04:13:00	100.0.0.2	10.0.0.11	54	11109750	405448137
2014-07-18 04:13:00	100.0.0.1	10.0.0.13	53	11053489	405154962

トラヒックグラフ

外部サービスに任せる

Google code Code Playground

[Tell us what you think](#) | [Sign in](#)



攻撃の通知

外部サービスにまかせる



コンセプト

- **全部自前で実装しない**
- **他と連携する仕組みを用意する**
- **各部分は得意なサービスにまかせる**