C11　不正アクセスパケットのシャボン玉による可視化

松谷　亜紀

1.　はじめに

近年 SNS やブログに代表されるインターネット上のユーザ参加型サービスの普及に伴い，一般利用者が増加しているが，ウィルスや不正アクセスといった脅威は未だ解消されていない．これらの攻撃の傾向や変化を検出し，対策に生かせるようにする必要があり，パケットを観測する多くの研究が行なわれている．例えば，不正アクセスパケットの振る舞いをアニメーションによって可視する[1]や，送信元 IP アドレスの分布から宛先に局所性があることを示した[2]などがある．しかし，これらの研究には観測期間とアドレス空間の関係が不明確であるという課題がある．

本研究では，不正アクセスパケットの観測データから，特定の送信元 IP アドレスが複数の宛先 IP アドレスにパケットを走査する様子を，シャボン玉によって表現する．シャボン玉の飛び方によって，不正アクセスパケットのスキャン先を明確にすることを目的としている．

2.　センサとログデータ

ネットワーク上でパケットを観測するホストをセンサとする．センサは受動的であり，届いたパケットに対して応答は行なわない．従って，センサで観測されたパケットはすべて不正アクセスパケットと仮定する．

ログデータは，日付，時間，標準時間，宛先 IP アドレス，プロトコル，送信元 IP アドレス，送信元ポート，宛先ポートから成る．本研究ではその中で送信元情報と宛先情報（IP アドレス，ポート番号）に注目し，可視化を行う．

3.　可視化システム

3.1 可視化軸

右側のメッシュが送信元，左側のメッシュが宛先を表す．可視化軸は，縦軸が IP の第 1 オクテット(32bit の上位 8bit, max=255)，奥行きがポート番号(max=65535)を表す．1 つのシャボン玉を右側から左側に移動させることによって，1 つの不正パケットの観測を表す．シャボン玉はセンサで観測された日付，時間順にアニメーションする．また，TCP や UDP といったプロトコルとの判別のために，ICMP パケットは，ポート番号の原点(0)を通る．

3.2 軸の回転

固定の角度からパケットの動向を見るのでは，ポート番号等の情報を読み取り難いことがある．そこで，軸の回転機能を実装し，任意の角度から見られるようにした．

3.3 システムの実装

本研究では主に java3D [3]のアニメーション機能を用いて可視化を行った．Alpha によりシャボン玉の出現や移動のスケジューリングを行い，Interpolator により実装している．

MouseBehavior によって，操作者が任意の視点で可視空間全体を回転させるようにした．また，シャボン玉が出現し，すぐに画面上から消えるのではなく，送信元地点と宛先地点に数秒程度留まった後にアクションさせることで，それらの情報が読み取り易くなるように工夫した．(図 1)

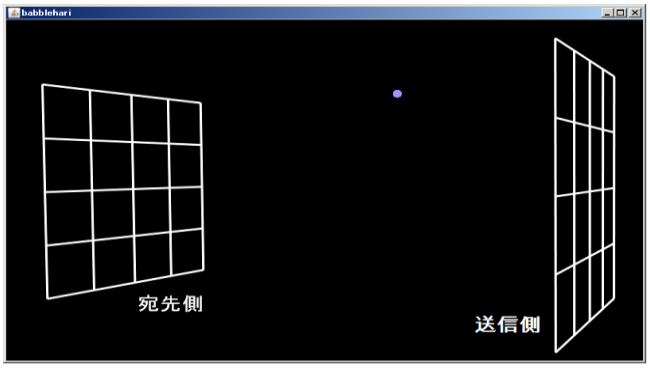

図 1.　不正パケットの可視化例

4.　おわりに

不正アクセスパケットが発信され，到着する様子を可視化した．これによりボットなどの影響によって，複数の送信元から同時に送られる不正アクセスパケットが飛ぶ様子を視覚的に捉えることができた．

今後の課題として，同時刻・近時刻に宛先側に到着したパケットが複数ある場合に，複数のシャボン玉が飛ぶようにし，実時間に沿ったパケットを可視化が挙げられる．

参考文献

[1]中尾ほか，「インシデント分析センタ nicter の可視化技術」，情報処理学会，CSEC2006，pp. 313-318，2006.

[2]石黒ほか，「インターネット上の不正パケットの送信元 IP アドレスの分布に関する分析」，情報処理学会，CSS2006，pp. 507-512，2006.

[3]林ほか，「java3D による 3 次元 CG プログラミング」，コロナ社.