Flash を用いた Covert Channel の視覚化

木下研究室　　新目　拓海 (200502753)

1　はじめに

現在、Social Network Service(SNS) は PC，モバイルともにインターネット上において急速な広がりをみせており，今後も一層の普及と発展が予想される．それに伴い，様々な問題が浮き上がってくる．その中の技術的な問題の一つとして，Covert Channel(隠れた経路) が挙げられる．Covert Channel とは一種の情報漏洩，改竄の可能性の示唆であり，これを一般に普及している Flash を用いて視覚化する事により，情報漏洩，改竄の経路を明確化させる事が可能となり，情報漏洩，改竄の発見や防止，解析等を早急かつ容易にさせる事ができる．本研究室では，SNS で起こりうる問題に対処すべく，covert channnel に関連する研究を年々行って来た．今回，その研究の一環として covert channnel の視覚化に着手し，本研究を行った次第である．

2　Covert Channel

ここまで Covert Channel という単語を度々使用してきた．Covert Channel とは何か，”はじめに”で既述したが Covert Channel とは一種の情報漏洩，改竄の可能性を示唆するものであり，訳すと隠れた経路という事になる．アクセス制御が既に施行された通信経路上での死角である．よって Covert Channel 自体が情報漏洩，改竄に必ずしも繋がるわけではなくあくまでも，可能性である事を明確にしておきたい．

次に，アクセス行列について説明する．アクセス行列とは，Subject が Object に対する read と write のアクセス権を表す行列であり，Covert Channel を示す事に用いる．図 1 は Covert Channel が存在するアクセス行列の例である．この図では S1 が O1 を read し，O1 を O2 へ write する．そして，S2 が O2 を read するという事を示している．問題は S2 は O1 を read する権限がないにも関わらず，S2 が read 可能な O2 を介して S1 から O1 を read している事にある．

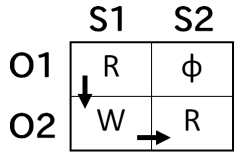

図 1: Covert Channel が存在するアクセス行列

3　視覚化プログラム作成

まず，視覚化にあたり，出力情報の既述には，汎用性の高い XML を利用する．アクセス行列が出力される am.xml とそのアクセス行列における covert channel が出力される cc.xml を用意した．この 2 つの XML ファイルの記述形式は同一であり，比較する事により，アクセス行列内の node 情報が covert channel であるかどうかを振り分ける．以下がその記述例であり，subject1 が object1 を read している事を示している．

```
<accessmatrix>
 <node>
  <name>subject1</name>
  <arc>
   <type>out</type>
   <label>read</label>
   <neighbornode>object1</neighbornode>
  </arc>
 </node>
</accessmatrix>
```

次に，このような XML 情報を読み込み，視覚化を行うプログラムには実行環境への依存度が低く，視覚化に最適な Flash を用いる．プログラミングには ActionScript3.0 を利用した．そして，作成した視覚化 Flash プログラムが図 2 であり，図 1 のアクセス行列をグラフ化したものである．

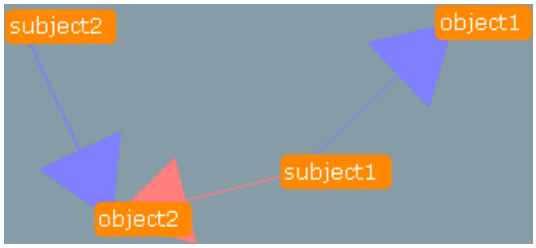

図 2: 視覚化 Flash プログラム実行

4　まとめ

Flash で視覚化プログラムを実行し，XML 情報を読み込み，その情報を基に，read 情報と write 情報の色分けを行い，使役される側へ矢印を引く事，アクセス行列内の covert channel 部を強調する事で covert channel の視覚化を行うことに成功した．これにより，アクセス行列の理解，covert channel の有無の確認が容易となった．

しかし，XML 情報が多いほどグラフ生成のための計算量，node の描画量が増大し，実行するハード側の問題としてフリーズや動作速度低下などの不具合が生じる可能性がある．