tracerouteと公開ネットワーク管理情報を用いたIP geolocation

2009SE203　二井谷 はるか
指導教員：後藤 邦夫

1　はじめに

現在，traceroute コマンドを用いて得た目的ホストまでの通信経路情報は，障害の発生場所を特定したり，データを集めてネットワークトポロジを作成し，地域間でどのような通信が行われているのか調べるなど幅広く活用することが可能である．traceroute.org [2] などの Web サイトを用いることで簡単に指定したホストまでのネットワーク経路を知ることができる．さらに，使用する Web サイトによっては Google マップ [1] などの地図情報を利用して，その経路を視覚的に認識することが可能である．

利用する Web サイトや使用するタイミングによって traceroute 結果が異なる可能性もある点が traceroute における問題点である．

そこで，本研究では利用する Web サイトによる traceroute 結果の違いに着目し，複数の Web サイトから traceroute を行い，それぞれの結果を比較して経路情報を求めることを目的とする．住所など場所の判定にはホスト名に含まれる場所に関する情報や，whois を用いる．

2　システムの提案

この節ではシステムの流れについて説明する．本研究では図 1 の構造を持つシステムを作成する．

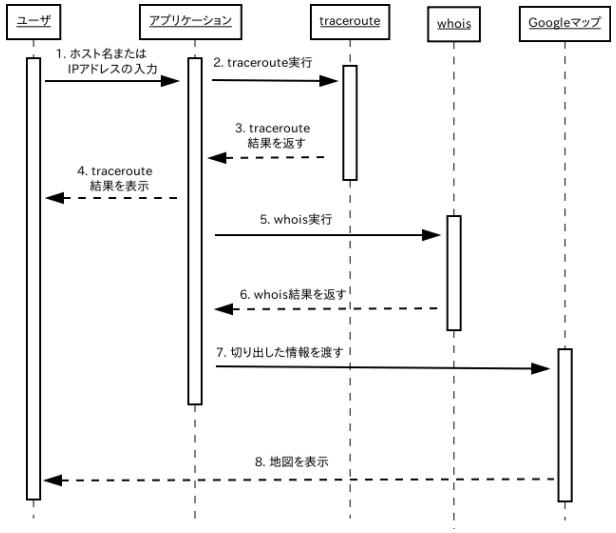

図 1　ユーザ入力から結果が返る流れを表すシーケンス図

1. ホスト名または IP アドレスの入力
ユーザはアプリケーションのトップページより宛先ホスト名または IP アドレスを入力する．

2. traceroute 実行
ユーザが入力したホスト名について，複数 Web サイトで traceroute を実行する．例えば 3 つの Web サイトを用いる場合，図 2 のようになる．

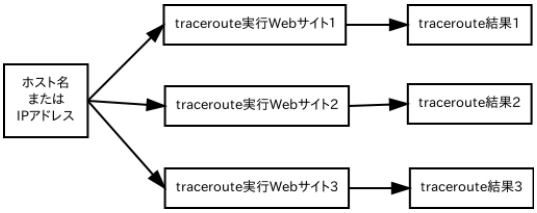

図 2　複数 Web サイト traceroute 実行例

3. traceroute 結果を返す
traceroute した結果をアプリケーション側に返す．この時 図 3 のように traceroute の経由地すべてと目的地を 1 箇所ずつ，さらにこれ以降 traceroute 結果の順番通りに区別する．そして，traceroute 経由地にあるルータのサブドメインから地名など場所が特定できる情報の検索を実行する．

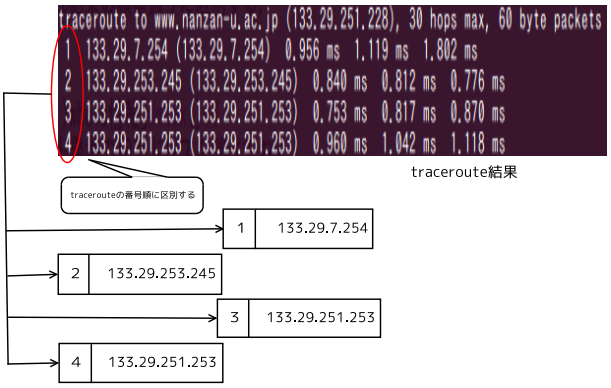

図 3　traceroute 結果の区別

4. traceroute 結果を表示
ここまでに求めたすべての traceroute 結果をユーザが確認できるように表示する．

5. whois 実行
宛先ホストの IP アドレスと，サブドメインから経路推定できなかった経由地について whois を実行する．

6. whois 結果を返す
whois 情報は organization または adress など，Google マップで場所が特定できる情報を切り出す．

7. 切り出した情報を渡す
切り出した情報を 1 つずつ Google マップへ送り，経由地は経由地，宛先は目的地として格納する．

8. 地図を表示
Google マップのルート乗り換え案内を用いて目的地と経由地を順番通りに線でつないだ結果を表示する．

3　実装

この節では作成したプログラムについて述べる．プログラムは PHP と HTML で作成する [4].

3.1　ユーザ入力

図 4 は，traceroute を実行するためのユーザ入力画面である．

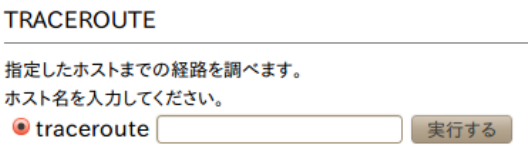

図 4　ユーザ入力画面

ユーザがテキストボックスにホスト名を入力し実行ボタンを押すと，ローカルホストで traceroute が実行される．traceroute 実行結果は，ログファイル tracelog.txt に保存される．

3.2　情報の切り出し

以下のプログラムは上記で作成したログファイルを読み込み，情報の切り出しを行うプログラムの一部である．

```
......(略)......
1: foreach($trace_res as $lineno => $value){
2: print "$lineno = $value<br>";
3: $fields = preg_split('/[ ]+/', $value);
4: foreach($fields as $no => $tvalue){
5: if($no==2){
6: $domain[$lineno]=$tvalue;
7: }
8: else if($no==3){
9: $ipaddr[$lineno] \\
              = str_replace("(", "", $tvalue);
10:$ipaddr[$lineno] = str_replace(")", \\
                        "", $ipaddr[$lineno]);
......(略)......
}
```

プログラム行と合わせ，次に情報切り出しの手順を示す．

- 1: traceroute ホップ数ごとの分割を$lineno で行う．
- 3: $fields で$lineno の空白ごとの分割を行う．
- 5: $no==2 のときの$fields をドメイン情報として切り出す．
- 8: $no==3 のときの$fields を IP アドレス情報として切り出す．

例えば

$lineno[2] = 2 fw.seto-private (10.8.1.254) 1.342 ms 0.967 ms 0.896 ms

の場合，

$fields[0] = 2, $fields[1] = fw.seto-private,
$fields[2] = (10.8.1.254)
.....
$domain[2] = fw.seto-private,
$ipaddr[2] = 10.8.1.254

が代入される．

4　実験，評価

実装したプログラムを実行すると図 5 の結果が得られる．例として yahoo.co.jp を指定して実行した場合を示す．

```
0 = traceroute to 124.83.187.140 (124.83.187.140), 30 hops max, 60 byte packets
DOMAIN: 124.83.187.140
IPADDR: 124.83.187.140,

1 = 1 10.64.6.254 (10.64.6.254) 1.491 ms 1.777 ms 3.797 ms
DOMAIN: 10.64.6.254
IPADDR: 10.64.6.254

2 = 2 fw.seto-private (10.8.1.254) 1.342 ms 0.967 ms 0.896 ms
DOMAIN: fw.seto-private
IPADDR: 10.8.1.254
```

図 5　プログラム実行結果 (一部抜粋)

上記結果より，ドメイン名，IP アドレスを用意した変数に切り出して代入することに成功した．DOMAIN に IP アドレスが入ってしまうことがあるが，サブドメインによる経路推定の段階で IP アドレスかサブドメインかを判定するので，この段階では問題ないものとする．

今回の実験で成功したことと残った問題点を次に示す．

- 図 4 より入力したホスト名から自動で traceroute を実行することができた．しかし，ローカルホストでの traceroute のみである．
- ドメイン名と IP アドレスの切り出しについては出来ていたことが確認できた．
- wget コマンドを用いて Web サイト (UltraTools[3]) に接続することに成功した．しかし，返り値を受け取り，位置を特定することが出来なかった．

5　おわりに

本研究では，複数 Web サイトを用いた traceroute 結果の地図表示の実現を目指して必要なプログラムを検討し，その一部を実装した．今後の課題として主に次の点が挙げられる．

- wget を用いて traceroute，whois 結果を求める具体的なプログラムを完成する．
- ユーザによる入力から地図表示まで自動化させる．
- ルート乗換案内に依存しない Google マップ上での表示を可能にする．

上記の点を改善することで，より実用的なシステムになると考える．

参考文献

[1] Google: Google マップ (accessed Jan. 2013). http://maps.google.co.jp/.

[2] Kernen, T.: traceroute.org (accessed Jan. 2013). http://www.traceroute.org/.

[3] Neustar, I.: UltraTools (accessed Jan. 2013). https://www.ultratools.com/.

[4] Rasmus Lerdorf, Kevin Tatroe, P. M.: プログラミング PHP 第 2 版，Vol. 1, 株式会社オライリー・ジャパン (2007).