L-087

IRCにおける新たな識別子の提案
Proposal of new identifier in IRC

丸山 洋平† 松澤 智史‡ 武田 正之‡
Yohei Maruyama Tomofumi Matsuzawa Masayuki Takeda

概 要

インターネット上のチャットシステム，IRC(Internet Relay Chat) 上において，違う時間帯に異なるIPアドレスから接続しているが，使うニックネームと入るチャンネルが同じユーザがいた場合，なりすましの可能性がある．また，なりすましでないとしてもこれらの接続が同一ユーザからのものなのかを判断するのは非常に困難である．本研究ではそういったなりすましの可能性を段階に分けて調査し，なりすましの可能性がある接続が多かったので，それを明確に区別できるような新しい識別子を提案する．

1. はじめに

インターネット上でのチャットシステムIRC(Internet Relay Chat)[1] において，違う時間帯に異なるIPアドレスからIRCサーバへと接続し，同じニックネームを使って同じチャンネルにJOINしたIRCクライアントがあった場合，そのIRCクライアントはなりすまし [2] をしている，もしくはされている可能性がある．

1.1 IRCにおけるなりすまし問題

IRCではチャンネルにJOINする際，IRCクライアント側にはIRCサーバからJOINしたユーザのニックネームの他に，usernameとIPアドレスの情報が送信されてくる．そのため，動的IPを使うユーザに対して，悪意のある第三者がそのユーザと同一のニックネームを使ってJOINした場合，他のユーザはJOINしてきたユーザが本人かどうかの区別が付かなくなってしまう．このような状況下において，チャンネルで自動的に，もしくはチャンネル内のユーザが手動で+op(オペレータ権限を配布) してしまうと，悪意のあるユーザがそのチャンネルの乗っ取り [3] をすることが可能となってしまう．

1.2 なりすましの可能性

ニックネームとJOINしているチャンネルが同じで，IPの異なるIRCクライアント全てでなりすましが発生しているとは限らないが，これらの接続がなりすましかどうか，または同一ユーザからの接続かどうかを判断するのは非常に困難である．そこで，現状のIRCネットワーク内でなりすましの可能性があるユーザがどれほどいるのかを調べ，その判断基準を段階分けすることでなりすましの可能性を考察を行った．

2. なりすましユーザの調査

今回はIRCネットワーク上よりユーザのニックネーム，接続IPアドレス，参加しているチャンネルの情報を取得し，なりすましの可能性があるユーザの調査を行なった．調査の内容については以下に記す．

2.1 調査内容

2.1.1 なりすましの可能性があるユーザ情報の抽出

1.1でも述べたが，なりすましを行なうユーザは，対象としたユーザとニックネーム，JOINするチャンネルを同じものにする．そこで任意の2人のユーザ情報に着目したとき，

1. 使用されているニックネームが同じ
2. 同じチャンネルに1つ以上JOINしている
3. IPアドレスが異なる

以上の条件を満たすユーザの情報を「なりすましを試みた可能性があるユーザの情報」とみなして抽出する．

2.1.2 なりすましの段階分け調査

以上のユーザ情報の抽出を行なった上で，なりすましを試みた可能性があるデータに対してそのドメインネームに着目し，以下のような判断基準を設ける．

1. ニックネームとJOINしているチャンネルが同じで，接続しているドメインネームが異なるものを取り出す．これを判断レベル1とする．
2. トップレベルドメインだけが完全一致するドメインネームを残す．これを判断レベル2とする．
3. 以降，判断レベルを1上げるごとにセカンドレベルドメイン，サードレベルドメイン…と比較範囲を広げて完全一致するドメインネームを残す．

例えば，同じニックネームを使っていた以下の3つのIPアドレスがあったとする．(つまり判断レベル1ではなりすまし可能性があるIP数が3)

```
(1) xxx.yyy.tus.ac.jp
(2) efg.hij.kkk.lll.com
(3) mno.pqr.sss.ne.jp
```

まず，トップレベルドメインに着目したとき，(2)は他との区別が付くのでこれを除くと，判断レベル2でのなりすまし可能性があるIP数は2，さらにセカンドレベルドメインを見ると(2)と(3)が除けるので，レベル3でのなりすまし可能性があるIP数は0となる．

以上のような基準に基づいて判断を行っていき，1レベル毎の判断が終了した時点で残っている(なりすましでないとは特定できない)IPの数を調査していく．

†東京理科大学 大学院 理工研究科 情報科学専攻
‡東京理科大学 理工学部 情報科学科

2.2 調査対象及び調査期間

今回の調査に当たっては，無作為に選んだ IRC ネットワークの Friend Chat[4] と irc.cre.jp[5] を対象とし，2005 年 6 月 25 日〜7 月 7 日までの期間で 1 時間ごとに取得したユーザ情報を調査対象に用いた．

2.3 調査結果

判断レベル毎で見たなりすましの可能性がある IP 数を，期間内に接続していた IP 全体に対する割合とあわせて表 1 に表し，その割合の推移を図 1 に表す．

表 1: 調査結果

判断レベル	なりすましらしき IP 数 (割合)	
	irc.cokage.ne.jp	irc.friend.td.nu
1	2115(60.14%)	8057(67.58%)
2	2069(58.83%)	7760(65.08%)
3	2061(58.60%)	7642(64.09%)
4	1994(56.70%)	7261(60.90%)
5	1802(51.24%)	6304(52.87%)
6	744(21.15%)	2291(19.21%)
7	401(11.40%)	1478(12.40%)
8	115(3.27%)	555(4.65%)
9	10(0.28%)	4(0.03%)
全体の IP 数	3517(100.00%)	11923(100.00%)

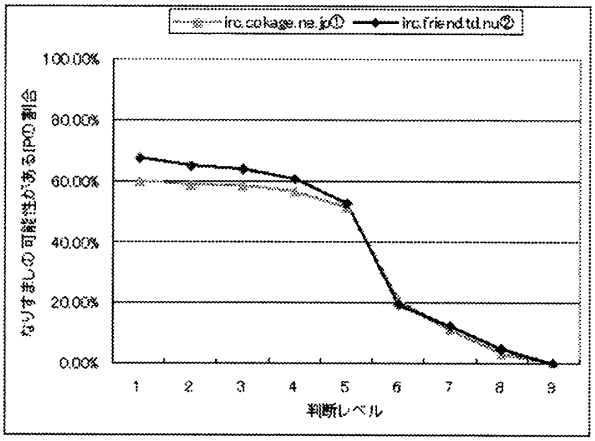

図 1: なりすまし可能性がある IP 数の割合推移

調査の結果，半分以上の接続に対してなりすましの可能性が見られ (ユーザの特定が出来ず)，その殆どが判断レベル 5 で調べてもなりすましの可能性がないとは言い切れないことが分かった．そこで本研究では，このようなユーザの判断を容易につけられる新しい識別子案を以下に提案する．

3. 新しい識別子の提案

IRC において，なりすましなどの疑いがあってユーザ特定が出来ない原因は，決定がユーザ側に依存するニックネームが識別子として用いられていることである．そこで，ニックネームを識別子とはせずに他の一意的な識別子を用いることが最良であると考えた．

そこで今回提議する草案は，IP アドレスと IRC サーバ接続時に開放しているポート番号を暗号化させたものを識別子として用いる方法である．なお，ニックネームはチャットにおけるユーザの名前として用い，ユーザの区別は新しい識別子を用いることで行う．

接続する IRC クライアントごとで IP アドレスと接続ポート番号の組み合わせは必ず一意であるので，この案を用いると識別子も IRC クライアントごとに一意に決まる．そのため，今回の調査でなりすましなのかどうか分からないユーザの区別がつけられるようになり，さらにはニックネームの衝突問題 [6] も解決することが出来る．

表 2: 従来と今回提議する識別子案の比較

	識別子	非識別子
従来	ニックネーム	IP アドレス
提案	暗号化した IP アドレスとポート番号	ニックネーム

4. おわりに

本研究では，IRC におけるユーザのなりすまし問題に焦点を当て，現状の IRC ネットワークにおいてなりすましではないとは言い切れないユーザがどれだけいるのかをまず調査し，さらにドメインネームの比較をして，どの時点で他のドメインネームと違うことが分かるかを調べた．その上で，それらのユーザがなりすましかどうかを可能な限り区別できるようにするための方法を提案した．

今回の提案はユーザ毎に一意である IP アドレスとポート番号をユーザの識別子にすることによって，なりすましであるかをどうかを明確にする．

参考文献

[1] C.Kalt: Internet Relay Chat Protocol, RFC2810 RFC2811 RFC2812 RFC2813, April 2000

[2] なりすまし [セキュリティ用語辞典]: http://www.atmarkit.co.jp/aig/02security/disguise.html

[3] チャンネル防衛について: http://www.ge-myu.net/irc/takeover.html

[4] Friend Chat IRC:http://www.friend.td.nu/

[5] irc.cre.jp:http://irc.cre.jp

[6] 丸山洋平, 松澤智史, 武田正之:IRC における Nickname 衝突問題回避方法の提案, 第 67 回情報処理学会 全国大会 4X-4, March 2005