VPN/認証プロキシサービスの利用状況監視

鳩野 逸生

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

1. はじめに

神戸大学においては，学外で活動する，学生および教職員に対して，学内向けに提供されている情報システムおよびサービスに学外からセキュアにアクセスすることを可能とするサービスとして VPN(Virtual Private Network) 接続サービスと認証プロキシサービスを, 全学生・教職員に提供している．こららのサービスは，一月あたり延べ数千人が利用している．

一方で，学外からの利用を前提としている VPN サービス，認証プロキシサービスは, 常に不正利用されるリスクにさらされている．これは，電子ジャーナルなど大学における教育・研究に対して提供されているサービスが, 大学によってかなり格差がある, などの背景によるものであると推察される．

2013 年末に，外部機関から神戸大学が提供する VPN サービスに対して不正利用の試みが行われている可能性がある，という指摘があったことから，VPN 接続の接続記録を，接続元 IP が存在すると推定される国の遷移，という観点から検査することを可能としたプログラムを VPN サービス，認証プロキシ向けに開発したので報告する．

2. VPN の利用状況

現 VPN 装置が稼働開始した 2014 年 6 月から 9 月までの延べ利用者数を Table 1 に示す. なお，2014 年 6 月以前までは，同じく F5 ネットワーク社製の FirePass 装置により VPN サービスを提供しており，同程度に利用されていた．Table 1 に示すように教職員，学生とも広く利用されていることが推察される．

また，学外からの VPN 接続の多くは日本国内からであるが，学生・教職員にかかわらず海外からの利用も多く見られる．Table 2 に海外からの利用状況を示す．Table 2 から,

表 1: VPN サービスの利用者数

日時	延べ利用者数	教職員	学生
2014 年 09 月	11,898	3,958	7,940
2014 年 08 月	11,476	3,499	7,977
2014 年 07 月	17,569	3,280	14,289
2014 年 06 月	11,819	2,276	9,503

表 2: VPN の国外からの利用状況

年月	アクセス元の国・地域
2014 年 6 月	Australia, Austria, Canada, China, Denmark, Finland, Germany, Hong Kong, India, Indonesia, Italy, Kenya, Korea, Republic of, Malaysia, New Zealand, Norway, Singapore, Spain, Thailand, United Kingdom, United States, Vietnam
2014 年 7 月	Australia, Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, Hong Kong, India, Indonesia, Italy, Kenya, Korea, Republic of, Malaysia, Netherlands, Norway, Singapore, Spain, Switzerland, Taiwan, Thailand, Turkey, Uganda, United Kingdom, United States
2014 年 8 月	Andorra, Argentina, Australia, Bangladesh, Belgium, Canada, China, Denmark, Finland, France, Germany, Guam, India, Indonesia, Italy, Kenya, Korea, Republic of, Malaysia, Morocco, Nepal, Netherlands, Norway, Palau, Philippines, Russian Federation, Singapore, Spain, Switzerland, Taiwan, Thailand, Uganda, United Kingdom, United States, Vietnam
2014 年 9 月	Austria, Bangladesh, Belgium, Bolivia, Canada, China, Cote D'Ivoire, Denmark, Finland, France, Germany, Greece, Guam, India, Italy, Kenya, Korea, Republic of, Lao People's Democratic Republic, Malawi, Malaysia, Nepal, Netherlands, New Zealand, Norway, Philippines, Poland, Russian Federation, Singapore, Spain, Switzerland, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Kingdom, United States, Uzbekistan, Vietnam

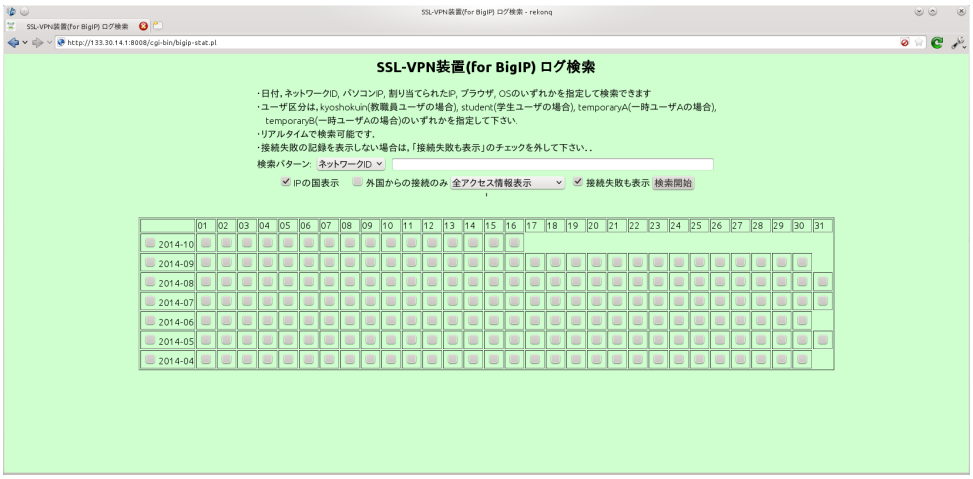


Fig.1: 接続情報検索画面例

いわゆる先進国から発展途上国まで多様な国・地域からの利用が定常的にあることがわかる.

3. VPN 接続状況監視

VPN を利用するにあたっては，PC に接続用ソフトウェアあるいはブラウザのプラグインをインストール必要がある．VPN 装置の利用状況の確認および接続トラブル発生時のサポートを目的とし，BigIP 装置が出力するログ情報を解析して表示するプログラムを開発し利用している．開発にあたっては，事務職員が利用することを前提とし，神戸大学における利用者区分, 接続元 IP, 割当 IP, 利用接続ツール種別などの情報が，日時毎に検索できるようにした.

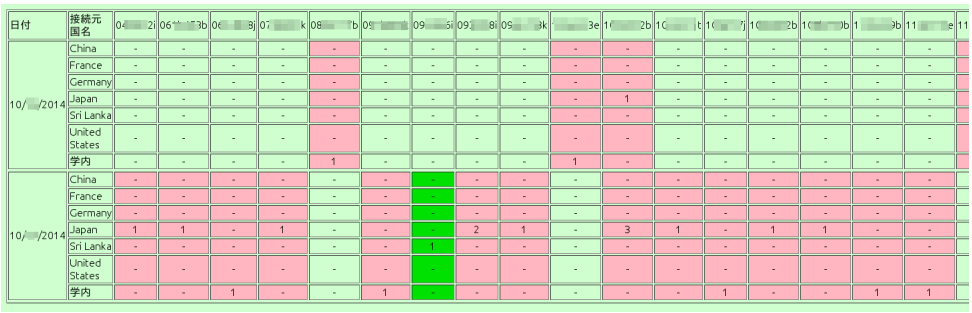
BigIP 装置の管理コンソールにおいても同種の情報を検索できる機能を利用できる. しかし，事務職員から利用しにくい，長期間のデータを VPN 装置内に保持することが困難であることから学内で開発した.

Fig. 1 に，日付/ID 名等による検索画面，Fig. 2 および 3 に，それぞれ接続情報一覧および表で出力した例を示す．Fig. 3 において，国内および国外からのアクセスがあった場合，それぞれ異なった背景色で表示される．緑の部分は，対応する日付において列に対応するユーザからスリランカからのアクセスが一回あったということを示している．もし，同一日に国外と国内からアクセスがあった場合は，背景色は赤で表示される.

UserID: 検索項目, 検索文字列: による 検索結果

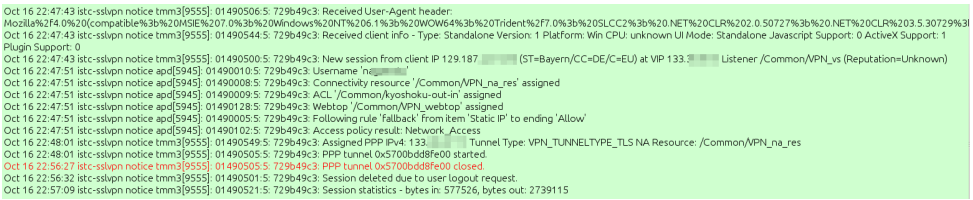
使用日時(session)	Network ID	Local IP	割当IP	ユーザ区分	ブラウザの種類
2014/10/13 23:59:45-(15badc2e:)	13 8i	220.248 (China)[220.24	133.	student	Mozilla 1[Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:32.0) Gecko/20100101 FireFox/32.0]
2014/10/13 23:57:46-(be25983a:)	-	122.196. 5(Japan)[zaq7 .zaq.ne.jp.]	未割当(-)		Standalone 1[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729; Tablet PC 2.0; ASU2JS)]
2014/10/13 23:57:38-2014/10/13 23:56:20(7d7804a1:)	eb	202.209. (Japan)[gw. .jp.]	133.	kyoshokuin	Standalone 1[Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12A405 EdgeClient/2.0.2]
2014/10/13 23:55:39-2014/10/13 23:55:54(48508cc6:)	fw	180. (Japan)[p4 ip eminato.hyogo.ocn.ne.jp.]	133.	kyoshokuin	Standalone 1[Mozilla/5.0 (iPad; CPU OS 7_1_1 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko) Mobile/11D201 EdgeClient/2.0.2]
2014/10/13 23:53:51-(1cfade2d:)	11 7m	218.251 7(Japan)[37f1.hyg1.eonet.ne.jp.]	133.	student	Standalone 1[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)]
2014/10/13 23:53:23-2014/10/13 23:53:27(4ceb0a1a:)	11 7m	218.251 (Japan)[37f1.hyg1.eonet.ne.jp.]	133.	student	Standalone 1[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)]
2014/10/13 23:53:16-2014/10/13 23:55:52(83a376eb:)	1 id	58.18 (Japan)[250f2.kns1.eonet.ne.jp.]	133.	student	Standalone 1[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.78.2 (KHTML, like Gecko) MacEdgeClient/7091.2014.0409.1]
2014/10/13 23:52:54-2014/10/13 23:58:11(12eeac40:)	-	49.251 7(Japan) q.ne.jp.]	未割当(-)		Standalone 1[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; YTB730; .NET4.0C; .NET4.0E; BRI/2)]
2014/10/13 23:52:13-2014/10/13 23:58:19(9a9ca21c:)	-	49.251. Japan) 9.zaq.ne.jp.]	未割当(-)		Standalone 1[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; YTB730; .NET4.0C; .NET4.0E; BRI/2)]
2014/10/13 23:51:31-(e4d3da63:)	14 d	121.84. 5(Japan)[.eonet.ne.jp.]	133.	student	Standalone 1[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.78.2 (KHTML, like Gecko) MacEdgeClient/7091.2014.0409.1]
2014/10/13 23:48:56-2014/10/13	yn hi	220. (Japan) 0.ap.so-net.ne.jp.]	133.	temporaryA	Mozilla 1[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/600.1.17 (KHTML, like Gecko) Version/7.1 Safari/537.85.10]

Fig.2: 接続情報一覧



日付	接続元国名	04 2	06 3b	0 8j	07 k	08 b	09	09 5	09 8i	09 3k	3e	1 2b	1 t	1 j	1 2b	1 0b	1 9b	11 e	11
10/ /2014	China	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	France	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Germany	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Japan	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	
	Sri Lanka	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	United States	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	学内	-	-	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	
10/ /2014	China	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	France	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Germany	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Japan	1	1	-	1	-	-	-	2	1	-	3	1	-	1	1	-	-	
	Sri Lanka	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	
	United States	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	学内	-	-	1	-	-	1	-	-	-	-	-	-	1	-	-	1	1	

Fig.3: 接続情報一覧表 (一部)



```
Oct 16 22:47:43 istc-sslvpn notice tmm3[9555]: 01490506:5: 729b49c3: Received User-Agent header:
Mozilla%2f4.0%20(compatible%3b%20MSIE%207.0%3b%20Windows%20NT%206.1%3b%20WOW64%3b%20Trident%2f7.0%3b%20SLCC2%3b%20.NET%20CLR%202.0.50727%3b%20.NET%20CLR%203.5.30729%3
Oct 16 22:47:43 istc-sslvpn notice tmm3[9555]: 01490544:5: 729b49c3: Received client info - Type: Standalone Version: 1 Platform: Win CPU: unknown UI Mode: Standalone Javascript Support: 0 ActiveX Support: 1
Plugin Support: 0
Oct 16 22:47:43 istc-sslvpn notice tmm3[9555]: 01490500:5: 729b49c3: New session from client IP 129.187. (ST=Bayern/CC=DE/C=EU) at VIP 133.3 Listener /Common/VPN_vs (Reputation=Unknown)
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490010:5: 729b49c3: Username 'na
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490008:5: 729b49c3: Connectivity resource '/Common/VPN_na_res' assigned
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490009:5: 729b49c3: ACL '/Common/kyoshoku-out-in' assigned
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490128:5: 729b49c3: Webtop '/Common/VPN_webtop' assigned
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490005:5: 729b49c3: Following rule 'fallback' from item 'Static IP' to ending 'Allow'
Oct 16 22:47:51 istc-sslvpn notice apd[5945]: 01490102:5: 729b49c3: Access policy result: Network_Access
Oct 16 22:48:01 istc-sslvpn notice tmm3[9555]: 01490549:5: 729b49c3: Assigned PPP IPv4: 133. Tunnel Type: VPN_TUNNELTYPE_TLS NA Resource: /Common/VPN_na_res
Oct 16 22:48:01 istc-sslvpn notice tmm3[9555]: 01490505:5: 729b49c3: PPP tunnel 0x5700bdd8fe00 started.
Oct 16 22:56:27 istc-sslvpn notice tmm3[9555]: 01490505:5: 729b49c3: PPP tunnel 0x5700bdd8fe00 closed.
Oct 16 22:56:32 istc-sslvpn notice tmm3[9555]: 01490501:5: 729b49c3: Session deleted due to user logout request.
Oct 16 22:57:09 istc-sslvpn notice tmm3[9555]: 01490521:5: 729b49c3: Session statistics - bytes in: 577526, bytes out: 2739115
```

Fig.4: SSLVPN 装置が出力する情報

本機能の開発においては perl 言語を用い，BigIP 装置が出力する, Fig. 4 に示すような接続記録を解釈することにより実現している．Fig.4 に示す情報を適切に解釈するためには BigIP 装置の設定に関する知識が必要であり，事務職員が対応することは現実的ではない．また，IP アドレスから，発信元の国名を推定するために，GeoIP パッケージ [2] を用いている．

また，Fig. 2 右端の「ブラウザの種類」欄の情報から，利用者の接続環境 (PC/OS の種類) を推定することができ，接続トラブル時のユーザサポートに利用している．

4. 不正利用検出事例

2013 年末，外部から神戸大学の VPN 装置が不正利用されている可能性が外部から指摘された. VPN 装置のアクセス記録は，FirePass 時代からのものも含めて 3 年以上保存しているが，2012 年-2013 年の記録に対して本機能を用いて調査を実施した．不正利用か否かの判定にあたっては,「一定の期間に渡って，同一日に国内と国外から接続記録が存在する」を判断基準とした．単に同一日に複数の国からの接続という基準では，同一日に移動中である可能性もあり，前述の基準に合致する接続を最終的に不正である可能性が高いと判断して，担当部署に該当期間におけるユーザの在校の有無の確認を依頼した．不正利用の検出例を Fig. 5 に示す．Fig. 5 において，赤が背景の部分において同日に学内からの利用 (認証付情報コンセント)[1] あったにも関わらず，外国からのアクセスも数回観測していることを示している．

2013 年から 2014 年にかけて本機能を用いることにより 3 件の不正利用を検知している．

5. 認証プロキシサービスの国外からの利用状況

Fig.6 に，2015 年 4 月から 11 月に外国から認証プロキシサービスを利用したユーザの一覧を示す．本サービスは認証として Basic 認証を用いているためセキュリティ上の問題があり，可能な限り VPN サービスを利用するようにユーザに勧めているため，外国からの利用者数も少なくなっている．しかし，VPN サービスを利用するためにはプラグインまたは接続のためのアプリケーションをインストールする必要があり，接続トラブルが一定数発生するのが現状である．そのための代替手段として，認証プロキシサービスを打ち切ることができない．

6. 認証プロキシサービスの接続状況監視

認証プロキシに対してはたびたび大規模な辞書攻撃が行なわれるが，現在利用している BlueCoat 社の製品は一定数認証が失敗すると一定時間該当の IP からのアクセスを凍結する機能がある．比較的辞書攻撃には耐性があるものと考えられるが，辞書攻撃以外の経路で ID およびパスワードが流出することも考慮し，外国からのアクセスに対して，Fig.7 のように，外国からのアクセス状況, 認証が失敗している ID の一覧および認証が失敗している ID に対するアクセス元 IP の一覧を一日に一度メールで管理者に通知するプログラムを作成し運用している．

監視にあたっては，外国からのアクセスを見ただけでは不正かどうか判定できないため，ユーザの属性 (教員，職員，職種) や他サービス (メール，無線 LAN など) の利用状況と比較した上で不正利用かどうかを推定し，所属部局に問い合わせた上で最終判断している．本監視により，数カ月に一件ほどの不正利用が発見されている (2015 年度).

[1] 学内の有線認証付情報コンセントサービスのために同一の装置を利用している．

	Asia/Pacific Region	-	-	-
	Australia	-	-	-
	Austria	-	-	-
	Belgium	-	-	-
	Canada	-	-	-
	[redacted]	2	-	-
	Denmark	-	-	-
	France	-	-	-
	Germany	-	-	-
	Guam	-	-	-
	Hong Kong	-	-	-
	India	-	-	-
	Indonesia	-	-	-
	Italy	-	-	-
11/18/2013	Korea, Republic of	-	-	-
	Malaysia	-	-	-
	Morocco	-	-	-
	Netherlands	-	-	-
	Norway	-	-	-
	Palestinian Territory	-	-	-
	Philippines	-	-	-
	Portugal	-	-	-
	Singapore	-	-	-
	Switzerland	-	-	-
	Thailand	-	-	-
	Turkey	-	-	-
	United Kingdom	-	-	-
	United States	-	-	-
	Vietnam	-	-	-
	学内	4	1	-
	Algeria	-	-	-
	Asia/Pacific Region	-	-	-

Fig.5: 不正利用の検知

ユーザ	2015/04	2015/05	2015/06	2015/07	2015/08	2015/09	2015/10	2015/11
ユーザ1		Japan:25; United States:4060		Italy:1				
ユーザ2					Switzerland:256			
ユーザ3		Australia:223						
ユーザ4	Japan:33732; France:26317	France:14317; Japan:40759; Taiwan:2108			Japan:60416; France:44370	Japan:77931; France:20809		
ユーザ5					United States:147			
ユーザ6		China:392						
ユーザ7		United States:313						
ユーザ8		Indonesia:8479	Indonesia:1813	Indonesia:12627	Indonesia:866	Indonesia:2324	Indonesia:8475	Indonesia:823
ユーザ9						Japan:7742; Austria:2395		United States:284; Japan:19848
ユーザ10					Thailand:65; Japan:962			
ユーザ11					China:7			
ユーザ12				United States:340				
ユーザ13	Indonesia:15017	Indonesia:11769	Indonesia:19155	Indonesia:26357	Indonesia:21696	Indonesia:17615	Indonesia:3637	Indonesia:11735
ユーザ14			China:6	China:7	China:4		China:11	China:71
ユーザ15		China:8						
ユーザ16		Japan:46472; United States:15606	United States:9972; Japan:5447					
ユーザ17		China:82						
ユーザ18	China:143							
ユーザ19		Japan:866; Vietnam:1060				Vietnam:1303	Vietnam:1576	Vietnam:773; Japan:1147
ユーザ20					Japan:25338; Korea, Republic of:119			
ユーザ21			Japan:8427; Germany:2883					Japan:1710; Guam:442
ユーザ22						Indonesia:1175		
ユーザ23	China:13							
ユーザ24						Korea, Republic of:51	Korea, Republic of:79; Japan:91787	
ユーザ25	Japan:216321; Taiwan:3885			United Kingdom:2161; Japan:165549			Japan:174280; Spain:3021	
ユーザ26							India:3065	
ユーザ27	Germany:1815							
ユーザ28	France:703		France:5094					
ユーザ29					Japan:4; Taiwan:12	Taiwan:1		
ユーザ30						Germany:52779	Germany:36701	Germany:53119
ユーザ31							Japan:3240; Vietnam:1001	
ユーザ32					Japan:25200; Australia:98047	Australia:31915; Japan:191707		
ユーザ33	United States:127							

Fig.6: 認証プロキシサービスの外国からの利用状況

```
Mon Dec  7 08:00:10 2015: 認証プロキシーへの外国からアクセス状況（Mon Dec  7 08:00:10 2015: 1日）!

外国からあるいは複数国からアクセスがあるユーザの UID

.-----------------------------------------------.
| UID    | Normal | Fail | Country:AccessCount |
+--------+--------+------+---------------------+
| xxxxxx |     10 |    6 | Indonesia:16        |
| yyyyyy |    413 |   79 | Germany:492         |
'--------+--------+------+---------------------'


List of Attacked ID
.-----------------------------------------.
| ID                              | Count |
+---------------------------------+-------+
| %20                             |   101 |
| 091kxxxx                        |    29 |
   (略)
| shyyyy                          |    37 |
| abcddddddddddddd6@xxxxxx.ne.jp |     1 |
'---------------------------------+-------'


List of Attacker IP
.-------------------------------------------------------------------------------------------------------------------------.
| IP              | FQDN                                                | Country        | Count | Attacked IDs                    |
+-----------------+-----------------------------------------------------+----------------+-------+---------------------------------+
|   36.52.xxx.yyy | xxxxxxxxxxxxxxxxxxxxxxx.ne.jp.                      | Japan          |     1 |                        xxxxxxxx |
|   203.202.zzz.x | yyyyyyyyyyyyyyy.ne.jp.                              | Japan          |   725 | None                            |
   (略)
|     36.12.x.yyy | ddddddddddddddddddddd.ne.jp                         | Japan          |     1 | zzzzzzzzz@xxxxxxo.ne.jp         |
|  185.21.zzz.zzz | eeeeeeeeeeeee.com.                                  | United Kingdom |    55 | axxxxxxx                        |
'-----------------+-----------------------------------------------------+----------------+-------+---------------------------------'
```

Fig.7: 認証プロキシの外国からの利用状況

7. おわりに

本稿では，VPN と認証プロキシの利用状況及び不正利用監視について報告した．今後は，他サービス利用状況も含めた総合的な監視を行い，不正利用の早期検知を行っていく必要がある．

参考文献

[1] F5Networks 社，https://f5.com/products/big-ip, 2014 年現在
[2] Maxmind 社, GeoIPlite パッケージ, http://geolite.maxmind.com/, 2014 年現在