VPN サービスにおける不正利用検知の試み

鳩野 逸生

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

概要 神戸大学においては，全学生・教職員に対して VPN 接続サービスが提供されており，学外における教育・研究に幅広く利用されているが，一方で不正に利用される一定のリスクを抱えている．本稿では，神戸大学において提供している VPN 接続サービスの不正検知を，接続記録の接続元の国を分析することにより検出した事例について報告する．

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) 接続サービスを, 全学生・教職員に提供している．本 VPN 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開発したので報告する．

2 VPN サービスの提供環境

神戸大学においては，全学生，教職員に対して，(1) ログイン ID, (2) ネットワーク ID, (3) メール ID という 3 種類の ID を発行している．各 ID は，それぞれ (1) のログイン ID は，教育用端末や主要な情報システム (学生の場合は, 学務システム，教職員の場合は，会計システムなど)，(2) のネットワーク ID は, VPN 接続サービスや, 全学無線 LAN サービス等のネットワーク接続サービス, (3) のメール ID は大学が提供するメールサービスでメールの送受信に利用するためのもので

Table 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

あり，それぞれ異なった ID/パスワードをつけることができる．これは，各サービスを利用する際の状況がサービスによってかなり異なると考えられるため，一つの ID が漏洩することですべてのサービスの不正利用につながるリスクを低減することを目的に導入されたものである．

神戸大学における VPN サービスは，F5 ネットワーク社の BigIP APM 2000 における SSL-VPN 方式を, (2) のネットワーク ID を用いることによって提供している [1].

3 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，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．

Table 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

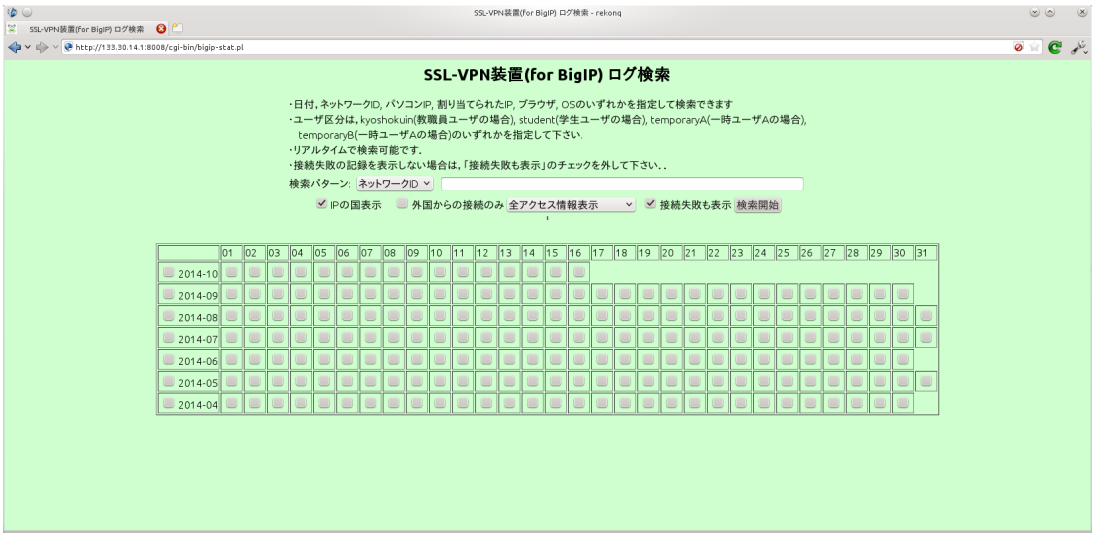


Fig. 1 接続情報検索画面例

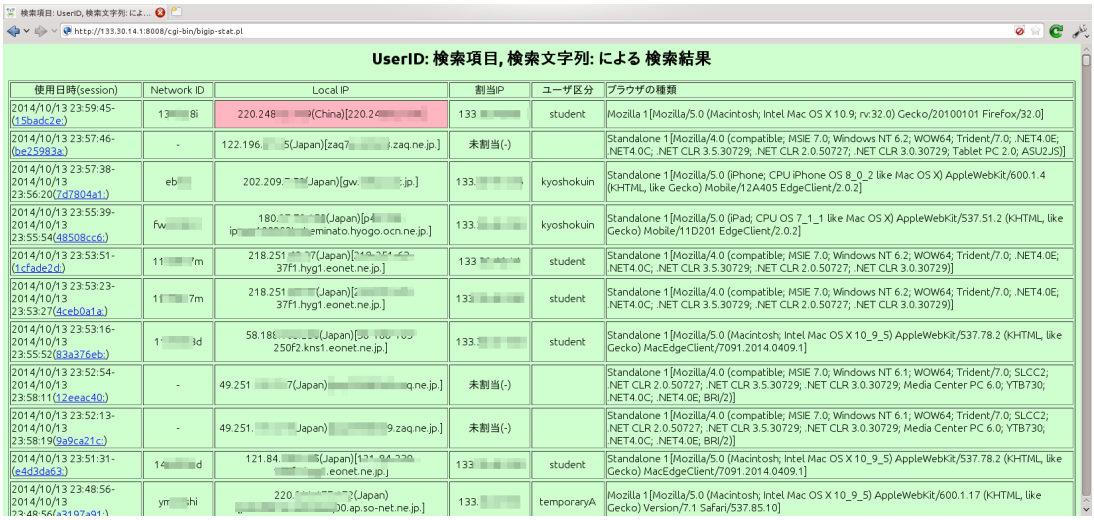
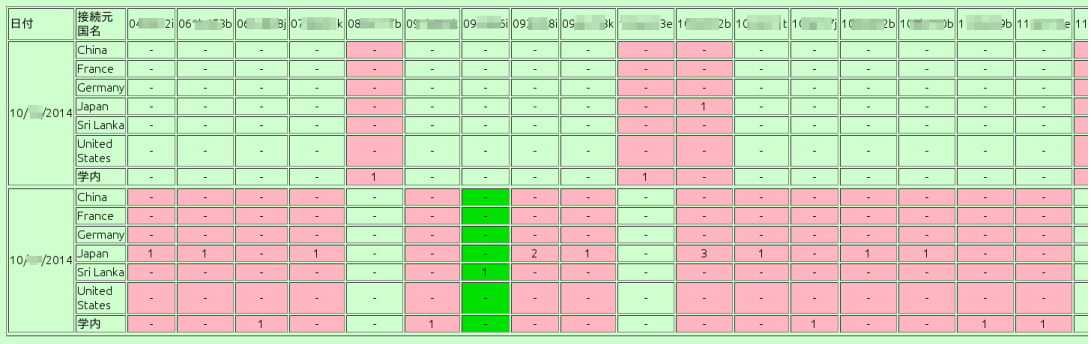


Fig. 2 接続情報一覧



日付	接続元国名	04 2i	06 3b	06 8j	07 k	08 b	09	09 5i	09 8i	09 3k	3e	1 2b	10 t	10 j	10 2b	10 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

4 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．

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．

5 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

Fig. 5 不正利用の検知

(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.

6 まとめと今後の課題

本稿では, VPN サービスのサポートを目的として開発したユーザ接続状況検索表示機能を, 不正利用検知に拡張して利用した事例について報告した. 神戸大学において本稿で示すような監視を行っていることを学内に周知できた点で不正利用の一定の抑止力になることが期待される.

しかし, 国内と海外で同時利用していない場合や国内で ID を多人数で利用している場合など, すべてのケースで検知できるわけではないのは明らかであり, 今後検知機能の強化が望まれる. 一般には, 定期的に利用状況を目視し, 長期間の海外からの利用に関しては利用者の所在の確認などの作業が必要であると考えられる.

また, 目視による確認作業の作業量を減少させるため, 以下の拡張を行うことを検討している.

- GeoIP パッケージは, 都市も検知できる機能を持っているため (ただし有償), 現在国レベルで判定している接続元の地理的位置を都市レベルに広げる. ただし, 精度や接続形態によって IP からの位置情報推定が無意味なケースもあるため十分な検討が必要である.
- 他のサービス (メール送受信など) の利用状況と照合して不正検知を行う.

[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.

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