神戸大学における緊急事態宣言時における VPN の運用と利用状況

鳩野 逸生

神戸大学 情報基盤センター
hatono@kobe-u.ac.jp

Operations and Status of Utilization of VPN Service in Kobe University during the State of Emergency for COVID-19 was Declared

Itsuo Hatono

Information Science and Technology Center, Kobe Univ.

概要

2020 年 4 月上旬に新型コロナウイルス流行に対する緊急事態が発令され，神戸大学の教職員の大多数が在宅勤務となり，学生は遠隔講義等による学習を余儀なくされた．本稿では，緊急事態への対応の中で，本学で利用している VPN 装置の運用面での対応とユーザの利用状況にについて報告する．

1 はじめに

神戸大学では 2014 年 4 月から F5 社製 BigIP-APM 2000[3] を用いた VPN サービスを学内の教職員・学生に提供してきており, 学外から学内の情報資源にアクセスするために利用してきた．2017 年 1 月に導入した KHAN2017[2] から，各研究室などの割り当てられたプライベートネットワークへのアクセスを，各プライベートネットワークの管理者が許可するを可能とする機能の導入を行って現在に至っている．2020 年初頭から発生した新型コロナウイルスの国内流行に伴い実施された大学内での活動制限への対応に際して重要な役割を果たした．

本稿では，大学内での活動制限に対応するために実施した VPN 装置の運用変更および利用状況にについて報告する．

2 VPN の運用状況

2.1 通常時の運用

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, 教務システム，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 [3]．認証成功後，認証基盤が提供する LDAP サービスを通じて取得される属性により, 教職員ユーザと学生ユーザに分類し異なった通信制限をかけている．例えば，学生ユーザは VPN サービス接続後も, 学内教職員向け Web ページや会計システムなど教職員のみが利用できるサービスにはアクセスすることができない．本学の BigIP APM 装置においては，同時 500 ユーザが利用できるライセンスが導入されている (学生ユーザ 250, 教職員ユーザ 250 に当初分割).

また，2018 年 1 月に導入された KHAN2017 においては, 各研究室のプライベートネットワークへのアクセスを, それぞれのネットワーク管理者が指定できる機能を導入して運用している．本機能は，認証成功後，BigIP 装置からプライベートネットワーク管理システムへ問い合わせを行い，認証に成功した ID に許可されたプライベートネットワークへのアクセスを許可する ACL を自動的に挿入することにより実現している．

2.2 緊急事態宣言後の運用

新型コロナウイルス流行に伴い，兵庫県下において 2020 年 4 月 7 日から 5 月 6 日までの外出自粛を要請する「緊急事態宣言」が政府から発令されたことに対応して，神戸大学においては，同日に, (1) 学生は，原

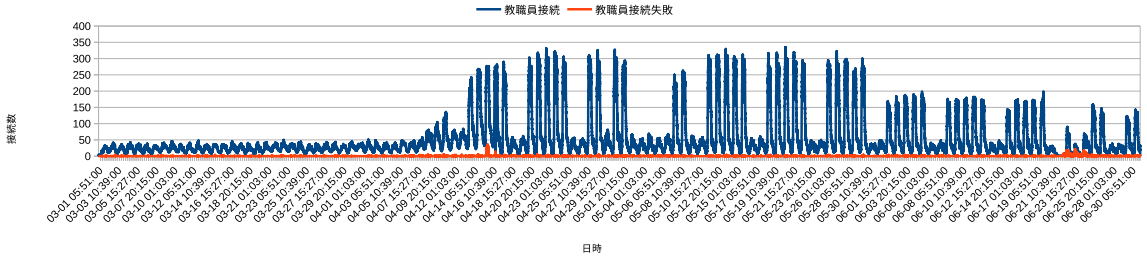

図 1　2020 年 4-6 月における教職員ユーザの接続数の推移 (1 分毎)

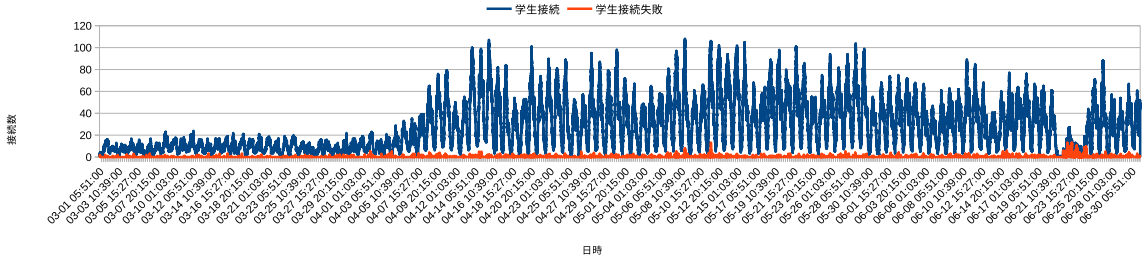

図 2　2020 年 4-6 月における学生ユーザの接続数の推移 (1 分毎)

則として自宅待機の上，不要不急の外出を避けること．(2) 教職員は，可能な限り在宅勤務を行うこと．という緊急の学長メッセージが発表された．これにより，学部学生の入構禁止，研究および大学の業務継続に必要な最小限の教員, 職員, 大学院生のみ入構可能となった [1].

3　緊急事態宣言時における運用変更

神戸大学においては，会計システム，グループウェアなどの業務に必要な情報システムを学外から利用する場合には VPN サービスを利用することが必要な運用を行っていたため，4 月 7 日以降アクセスが急増し，接続可能な同時アクセス数がオーバーして接続できないケースが多発していた．接続状況を調査したところ，4 月中旬の状況では, 利用者が特に急増しているのは教職員であり，学生ユーザ数も増加はしているが，上限まではまだ余裕がある状態であった．また，VPN へ繋がりにくくなったためか一旦接続したらそのまま接続したままにするケースも多く，余計に繋がりにくくなっていると推測された．しかも，現在導入している BigIP APM2000 装置は最大 同時 500 ユーザまでしか拡張できず，同時アクセス数増加を実施するためには，機器を更新するしかなかったが，機器の更新を短時間に行うことは不可能であった．学生の遠隔学習をサポートする LMS や教務システムは，VPN を介さず直接インターネットからアクセスすることが可能であったため，本稿の内容には含めていない．

そのため，以下に示す設定変更で対応可能な対応を 4 月 16 日に実施した．

1. 連続接続時間を 3 時間に制限する (3 時間経過すると接続が切断される).
2. 教職員ユーザの同時接続数を 350, 学生ユーザの同時接続数を 150 に変更する.
3. 事務系用プライベートネットワークへのアクセスを限定的なユーザにのみ許可可能な機能の導入を行う (Windows Remote Desktop のみ利用可能).

3. は, 学内に設置された PC でのみ実施可能で，大学業務を継続する上で必要最小限な業務 (給与計算, 学内業務システムのメンテナンス) に限って許可する運用とした．最小限とした理由は，通常時は学内の事務系プライベートネットワークに接続された PC で実施することが前提となっている業務 (神戸大学では事務業務を自宅で行うことを前提とした環境は整備していない) を，自宅で行うにあたって必要な環境 (貸出 PC など) が用意できないことと，情報セキュリティ維持のためのルール等が全く存在しなかったためである．事務系ネットワークへのユーザ許可を限定したユーザに許可するにあたっては，短期間のみ有効な一時アカウントを発行し，ユーザ毎の許可 ACL を投入するプログラムに，許可された一時アカウントでログインした時のみ事務系ネットワークへの許可 ACL を投入するようにロジックを変更することにより対応した．

4　2020 年 4 月から 8 月までの運用状況

以上のような状況において，VPN サービスの利用状況を BigIP APM が出力する log 情報を解析することによって実施した．

4.1 利用者の推移

図 1 および 2 に，2020 年 3 月から 6 月末までの, 一分毎の接続数の推移を示す．図中の「接続失敗」は，認証は成功したが IP アドレスが割り付けられなかった接続であることを示すものとする．教職員および学生とも 4 月 7 日前後から接続数が増加し始め，4 月 16 日から急増している．4 月 16 日から急増したのは事務職員の緊急事態宣言中の勤務体制が実施されるのにやや時間を要したためであると推測される．4 月 16 日には接続失敗数が増加している．4 月 16 日までの教職員ユーザの最大接続数は 250 であることを考えると, 常に 100 名程が接続できなかったと考えられる．

教職員ユーザの最大接続数を 350 に拡張した 4 月 17 日以降は，接続失敗数も通常に戻っており，接続障害は発生していなかったものと考えられる[*1]．6 月 21 日から数日間接続失敗が増加しているのは, この期間神戸大学の対外接続回線に障害が発生していたためである．

図 3 に, 設定変更を実施した前後の利用状況 (4 月 15 日から 4 月 17 日) のユーザの利用状況の詳細を締め明日．4 月 15 日においては，利用者数が 250 より少し上で頭打ちになっており，接続できなかったユーザがかなりいたことが推定される．一方, 4 月 17 日は同時接続 300 名近くまでは到達しているものの頭打ちになっているような状況は見当たらない．以上のことから今回の設定変更で全く接続できないという事態は回避できたものと思われる．

図 4 に，教職員ユーザの接続時間毎の接続数の推移 (1 日毎の集計) を示す．接続時間の最大値が 3 時間であるにもかかわらず 180~240 分のレンジが 0 でない理由は，本集計における接続時間は, 接続開始のログが記録された時間から接続終了のログの時間差で計算しており，VPN 内部で管理している接続時間より認証や IP 割り当てに要する時間の分だけ長めになっているためであると考えられる．一方でこのレンジに含まれている接続は，放置されてシステムにより時間制限で切断されたものと考えられ，かなりのユーザが接続を切らずに作業を行っていると推測される．

4.2 事務業務への利用

図 5 に, 2020 年 4-6 月における業務システム (グループウェア，会計業務システム) の利用セッション数 (1 時間毎の集計) を示す．本学では ACL を logging オプション付きで記述しているため，すべてのアクセスについて IP アドレスとポートが記録される．本稿では，該当業務システムへのアクセスが記録されているセッション数をカウントしている．図 5 から，緊急事態宣言後の在宅勤務開始に伴い, グループウェアの利用セッション数が大幅に伸びていることが分かる．

会計業務システムの利用数も若干増えているがグループウェアほどでないのは，VPN を介して利用できる機能が, Web インタフェースによる物品購入依頼や出張申請 (主なユーザは教員) であるためであると思われる．

6 月に入って全体の接続数が減少しているのは, 6 月に入って事務職員の在宅勤務体制が緩和されたものによると思われる[*2]．教員は，普段から VPN を通じてグループウェアや会計業務システムを利用しており，3 月中の利用状況が教員の利用状況であると推測される．すなわち, 4 月以降の増加分のほとんどは事務系職員の在宅勤務によるものである可能性が高い．

図 6 に, 事務系ネットワーク内に接続された PC への RDP 接続数を示す．許可した対象が給与計算業務と業務用情報システムのメンテナンス業務だけであり，ごく少数に留まっている．4 月末にやや接続数が増加しているのは，給与計算業務のために接続したためであると思われる．

5 教育研究における利用

図 7 に，教育研究用プライベートセグメントへのアクセスを行ったセッション数を示す．4 月 7 日の緊急事態宣言後，急増していることがわかる．しかし，教職員ユーザほどは増加していない．潜在的には需要は大きかったことは予想されるが，在宅で研究を行う準備ができる準備が十分にできていなかったことが要因ではないかと想像している[*3]．

また, 図 8 に, VPN を介した学内への RDP(Remote desktop 接続) の状況を示す．まだ学内のグローバル上に設置された PC への RDP 接続が残っており，教育研究用プライベートへ移行していない研究室が少なからず存在していることを示している．

6 運用状況の考察

4 月 17 日の運用変更後，VPN の接続障害は発生しなかったことから，今回の緊急事態宣言においては最低限の対応ができたものと判断している．もし，教職員・学生のそれぞれの利用最大数の変更後も，同時接続数不足による接続障害が発生した場合は，更に最大接続時間を短縮することにより対応することを計画していた．

[*1] 同時接続数に余裕がある場合でも一定確率で接続障害は常時発生している．

[*2] 緊急事態宣言中は, 70% が在宅勤務可能なことを目指した勤務体系となっていた．6 月に入ってからは 50% に緩和された．

[*3] 研究室の計算機を利用するための学生ユーザが急増した場合は，今回の VPN 装置の運用変更でも対応が困難であったことが予想される．

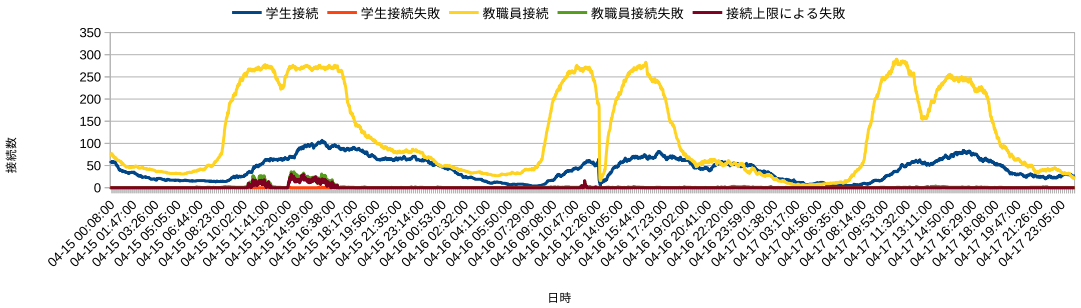

図 3　VPN 装置運用変更前後の利用状況

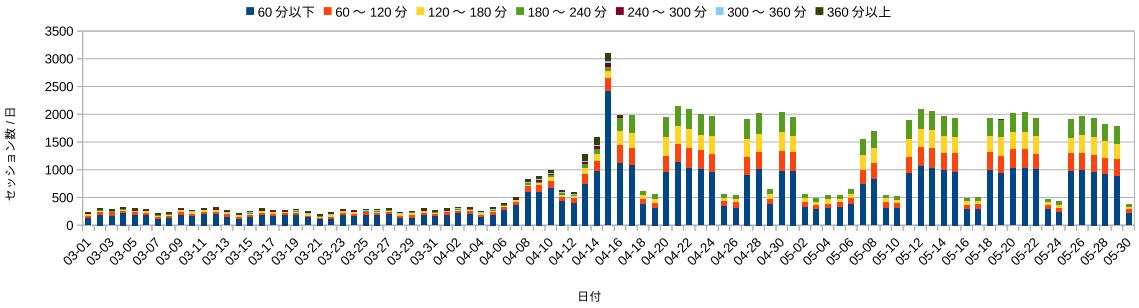

図 4　2020 年 4-6 月における教職員ユーザの接続時間の推移 (1 日集計)

一方で，最大接続時間が 3 時間という運用には不満も多かったという意見も聞かれた．可能ならば，もっと多くの同時接続が可能な機種への更新が望まれる．緊急事態宣言が出されていた 4 月，5 月におけるユニークなユーザ数は，それぞれ 4,716 名および 5,081 名であった．通常の利用者数は，同時 1,500 名前後であったことから，接続時間無制限という設定で 4,5 月を運用するためには，ライセンス数は，3 倍程度 (1,500 名) 必要であると思われる．

7　終わりに

本稿では，2020 年 4 月の新型コロナ対策のための緊急事態宣言発令時における神戸大学における VPN 装置の設定変更と運用状況について述べた．今後，BCP などに VPN による業務維持をもっと具体的に記述しておくとともに，VPN 装置の増強が必要であると思われる．

現状，事務系職員が利用可能な PC は，在宅勤務を考慮した運用は行われていない．さらに本格的な在宅勤務を行うためには，主要な業務に対する PC の VDI 化などの仮想化が必要であるとともに，在宅勤務のセキュリティを考慮した運用ルールの策定が必須である．また，学生の利用状況から見て，研究においてVPN 装置の利用は想像していたより増加しなかった．今後は教育研究用プライベートシステムの機能についてさらに学内に広報していく必要がある．

参考文献

[1] 神戸大学:　https://www.kobe-u.ac.jp/NEWS/info/2020_04_07_01.html(2020 年 9 月現在)

[2] 鳩野逸生，伴好弘，伊達浩典, 北内一行, 神戸大学におけるキャンパスネットワークの更新および全学無線 LAN サービスと統合した研究室向けプライベートネットワークの導入, 情報処理学会研究報告, 2018-IOT-43, 2018

[3] F5 Networks: Access Manager, https://f5.com/jp/products/big-ip/access-manager, (2018 現在)

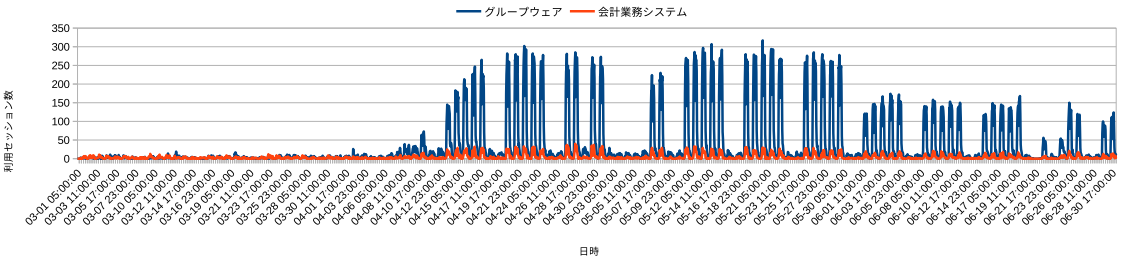

図 5　2020 年 4-6 月における業務システムの利用セッション数

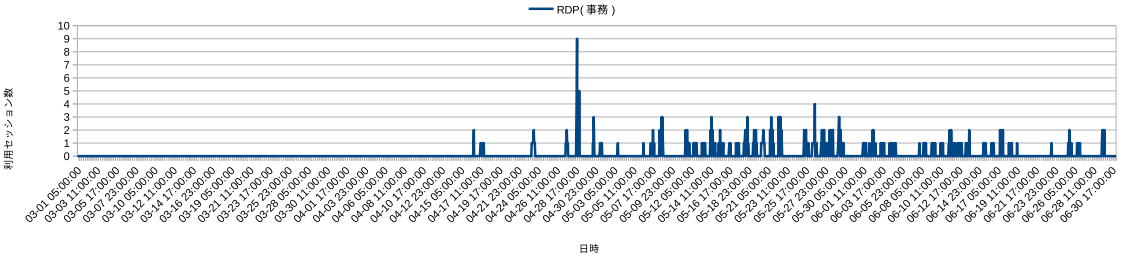

図 6　2020 年 4-6 月における事務系への RDP 接続数

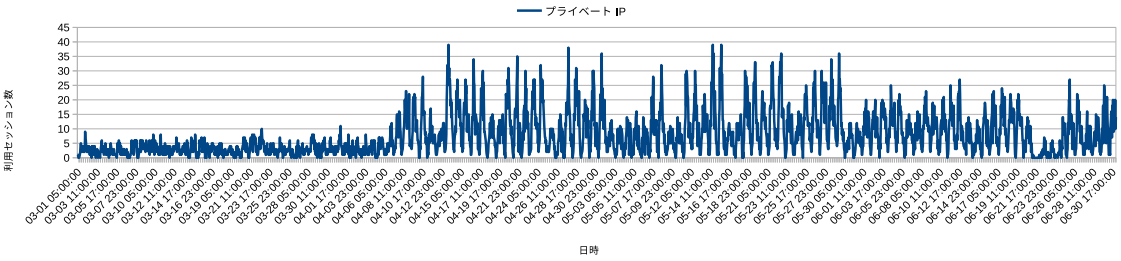

図 7　2020 年 4-6 月におけるプライベートアクセス利用セッション数

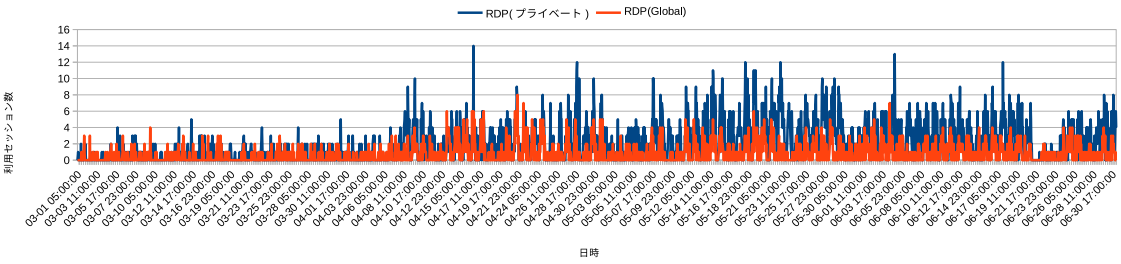

図 8　2020 年 4-6 月における教育研究系への RDP 接続数