パンデミック時のセキュリティポリシーと テレワーク用 VPN サービスの提供

柘植 朗 [1)], 村瀬 勉 [2)]

1) 名古屋大学　情報推進部
2) 名古屋大学　情報基盤センター

tsuge.akira@icts.nagoya-u.ac.jp

Official VPN Service for Tele-work with Day-by-day Security Policy Change in COVID-19 Pandemic

Akira Tsuge [1)], Tutomu Murase [2)]

1) Information Promotion Department, Nagoya University,
2) Information Technology Center, Nagoya University,

概要

COVID-19 パンデミック防止のため、名古屋大学でも非常事態の体制となり、多くの新しい試みがなされた。ここでは、テレワークのために、学外から大学の情報にアクセスするための VPN サービスの導入に関して、その経緯とセキュリティポリシーの変化について述べる。VPN サービスへの従来の要求や名古屋大学 VPN サービスの展開について述べる。特に、複数の VPN サービスメニューについて、利便性と認証セキュリティについて述べる。COVID-19 により、このサービスの展開がどのように変化したかについて時系列的に述べる。同時に、利便性とセキュリティリスクのトレードオフ(セキュリティポリシー)が、どのように変化したかについて述べる。VPN サービスの利用状況についても述べる。

1　はじめに

学内や企業内に閉じているサービスを学外や社外から利用するときなどに、VPN を用いることが多い。COVID-19 パンデミックの防止(以下、単に COVID-19)のため、名古屋大学でもロックダウンに近い状況になり、学外から学内のリソースにアクセスする要望が高まった。

今回の COVID-19 に対しては、学生のみならず一般事務職員も自宅での仕事(テレワーク)が原則となった時期があり、自宅から大学のリソースに安全にアクセスする必要が生じた。本学では、VPN を用いて、この要求に応えた。しかし、VPN は、利便性と共にセキュリティリスクも伴うアクセス方法である。そのため、セキュリティと利便性のトレードオフを考えて、導入の可否を判断する必要がある。利便性かセキュリティリスクのどちらに重きを置くかを決めるものをここではセキュリティポリシーと呼ぶ。

次章からは、まず、本学の VPN サービスについて紹介する。次に、サービス提供側において、VPN に対するセキュリティポリシーが、通常時と COVID-19 体制とで、どのように変化したかについて述べる。さらに、サービス受益側であるエンドユーザおよび学内専用サーバ管理のセキュリティポリシーが通常時と COVID-19 体制とで、どのように変化したかについて述べる。最後に、本学の今後の VPN サービスの発展について述べる。

2　学外から学内へのアクセス方法

ここでは、学外からのアクセス方法について現在入手できる方法を中心に簡単にまとめる。ここで、アクセス方法に必要な条件は、通信が他人に盗聴されても情報漏洩が無い(暗号化されている)こと、認証ができることである。

2.1 名古屋大学の公式 VPN に必要な条件

本学の VPN に必要な条件について述べる。一般的な VPN に要求される事項に加えて、セキュリ

ティと利便性について述べる。

まず、本学での学外からのリモートアクセスの現状について述べる。全てを正確に調査することはできなかったが、現状では概して次の 4 つの方法で、リモートアクセスがなされている。

1. SSH
2. 部局や研究室単位での SSL-VPN
3. 個人 PC での画面共有などのアプリ
4. 大学公式の SSL-VPN

このうち、1〜3 は、大学側として管理ができない。そのため、セキュリティ設定やログ保管の有無などで問題があるかもという危惧がある。セキュリティの観点からは、4 の公式 SSL-VPN に巻き取ることが望ましいと考えている。3 については、ファイヤウオールや NAT 越しに通信できるように、ランデブーポイントで接続していることによる、情報漏洩の危険性がある。

2.2 名古屋大学 公式 VPN の設計方針

上記 1〜3 の既存の方法を巻き取るためには、堅牢なセキュリティを具備すると共に、利便性の高い VPN を提供する必要がある。そこで、どの PC でも利用でき、特殊な設定をできるだけ避ける、という方針で SSL-VPN を選んだ。テレワークやリモートアクセスは、個人占有の PC から必ずしもおこなわれるとは限らないためである。例えば、共用されることもある大学の持ち出しノート PC といった PC からのアクセスも考慮する必要がある。また、電子証明書などを含む特殊なアプリケーションの導入などを行う方法もあるが、大学の教職員の様々な研究分野や利用法を考慮すると、汎用的な PC で汎用的に使える方法が望ましい。

堅牢なセキュリティのためには、多段階・多要素認証が欠かせない。今回は、大学の認証と email を用いた二段階認証を用いた。現場での認証の最大の課題は、初期設定における本人確認であると思われる。VPN の場合にも、初期設定のための本人確認の工数の問題を回避したい。そのため、本学で導入している CAS 認証を利用して、email による二段階認証をまず実現した。すでに CAS 認証においては、本人確認の上で認証が行われているため、VPN で新たな認証を行う必要が無い。これにより、CAS 認証と email へのアクセスの両方が同時に漏洩しない限り、利便性が高くセキュアな VPN を実現することができた。

また、必要性の高い人に限定することでセキュリティリスクを低減する。本学の VPN では、ユーザを大学院生と教職員に限定している。一部の学部生(例えば研究室に配属されている学部生)は、各研究室のネットワーク責任者が許可すれば、後述する研究室 LAN 用 VPN を利用することができる。

3 名古屋大学 VPN サービス

大学公式の VPN について、その機能を紹介する[1]。

名古屋大学 VPN サービスには、用途に応じて 3 種類のサービスを提供しており、それぞれについて特徴を述べる。

次に、セキュリティの要である二段階認証について方式を述べる。

最後に、インシデント発生時の調査や、ユーザの利用履歴をトラッキングするためのログについて、保存方法を述べる。

3.1 用途に応じた 3 種類のサービス

3.1.1 NICE 用 VPN

名古屋大学の全学的なキャンパス情報ネットワーク（NICE）につながる VPN サービスである。

この VPN を使うと、学内の無線 LAN に接続するのと同じように、NICE につながった状態になる。

学内限定に公開しているサービスのほとんどを利用できるが、一部のサービスはセキュリティまたは規約上、この VPN からの接続を禁止している。

なお、利用できるのは大学院生、および教職員であり、学部学生は利用できないようにしている。授業に必要なサービスは学外公開しており、学内限定のサービスを利用する必要がないと判断したためである。

3.1.2 研究室 LAN 用 VPN

研究室のプライベートなネットワーク（Secure NICE）につながる VPN サービスである。

この VPN を使うと、研究室内のネットワークにつながった状態になる。

この VPN を利用するには、はじめに Secure NICE の利用者が VPN の利用申請を行う。Secure NICE の利用者は、VPN を利用できるユーザの事前登録が必要であり、研究室内のユーザのみに利用を限定することができる。

3.1.3 事務 LAN 用 VPN

研究室 LAN 用 VPN を拡張したものであり、事務用端末専用の LAN につながる VPN サービスである。

この VPN を使うと、事務 LAN 内のネットワークにつながった状態になる。

研究室 LAN 用 VPN と同様、利用できるユーザは事前登録が必要である。

また、事務 LAN 内のセキュリティレベルが高いサーバは、この VPN から直接的には接続できないようになっている。

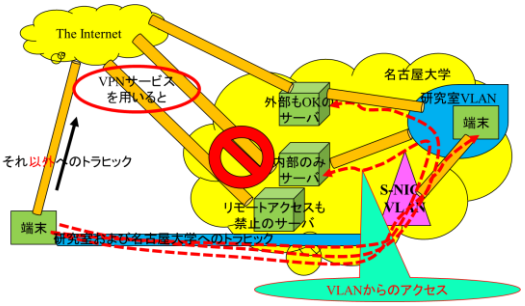

図 1 VPN の経路

3.2 二段階認証

現状の二段階認証である、CAS 認証と email を組み合わせた方式は、次の順番で実現している。

1.利用者は VPN ポータル画面にブラウザでアクセスする。

図 2 二段階認証（手順 1）

2.利用開始をクリックすると、CAS 認証の画面が表示され、名古屋大学 ID とパスワードの認証を行う。

図 3 二段階認証（手順 2）

3.CAS 認証が成功するとメールアドレスの入力をし、VPN アカウント発行をクリックする。

図 4 二段階認証（手順 3）

4.入力したメールアドレス宛に、ランダムなトークンを含む VPN アカウント確認用 URL が送付される。

図 5 二段階認証（手順 4）

5.利用者はメールを受信し、VPN アカウント確認用 URL にアクセスする。

6.CAS 認証の画面が表示され（同じブラウザであればシングルサインオンで本画面はスキップされる）、名古屋大学 ID とパスワードの認証を行う。

7.CAS 認証が成功すると、VPN 用の ID とパスワードが画面に表示される。

図 6 二段階認証（手順 7）

8.ブラウザまたはアプリで、VPN ゲートウェイ

にアクセスし、VPN 用の ID とパスワードを入力する。

図 7 二段階認証（手順 8）

9.認証が成功すると、VPN の利用が開始される。

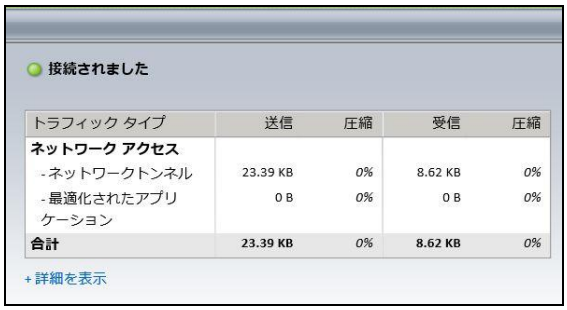

図 8 二段階認証（手順 9）

3.3 ログ保存

VPN ポータル画面では、VPN アカウント発行時のログを取得し、VPN ゲートウェイでは VPN の開始と終了のログを取得している。

それらのログは、別のサーバに転送し、約 1 年間保存している。

VPN ゲートウェイでは、VPN 用の ID が記録されており、それだけでは誰が利用したかを判別できないため、VPN アカウント発行時のログと紐付けてユーザを特定する必要がある。

現状では紐付けが自動でできていないため、手作業でログを紐付ける必要がある。紐付けの自動化は、運用コストの低減になるため、今後の課題である。

4 セキュリティと VPN サービスの展開

VPN も含めてネットワークアクセスにおける利便性とセキュリティについてのトレードオフに関しては、議論は尽きない。このトレードオフは、一般的には人為的に決まるものであり、通常は、経営トップや最高情報セキュリティ責任者（CISO）が決める。それをここでは、セキュリティポリシーと呼ぶ。CISO は、そのようなセキュリティポリシーに基づき、すなわち、潜在的被害の大きさを考慮したセキュリティリスクと、利便性を天秤に掛け、トレードオフに判断を下す。

COVID-19 禍の前後で、この利便性とセキュリティリスクに関して、どのようなセキュリティポリシーが導入されたか、すなわちどのような判断が行われたかを、時系列的に述べる。

4.1 COVID-19「前」の本学の VPN のセキュリティ評価

当初 VPN サービスは、試行の扱いであり、前述の NICE 用 VPN のみでスタートした。セキュリティのため、前述の二段階認証を実装した。ユーザの利便性を考慮して、認証後 24 時間の継続的な接続が可能であった。

しかしながら、継続利用時間は、3 時間に短縮された。二段階認証のセキュリティ的な問題を指摘され、さらに、接続が切れたら再接続すれば良いだけとの指摘もあり、セキュリティ面を重視しての判断であった。

また、利便性を考慮して前述の研究室 LAN 用 VPN と事務 LAN 用 VPN の開発を行ったが、これらのサービスは、セキュリティの強化が優先であるとの理由で、サービスインは棚上げとなった。そこで、多要素認証の実装を検討した。多数の方式のなかから、MS365 をベースにした Azure AD を用いた TOTP 方式を有力候補とした。多要素認証においては、認証の堅さと実装・運用コストを考慮することが重要である。MS365 は本学が既に導入していること、大学の ID そのものを Azure 側に提示する必要が無いことなどの利点と、追加費用なしに認証機能が使えることの利点とで、採用に至った。

この時点で、利便性とセキュリティを天秤に掛けたとき、圧倒的にセキュリティに重きが置かれるセキュリティポリシーであった。そのため、VPN サービスは、NICE 用 VPN のみで、なおかつ「試行」という状態でサービスを提供していた。この時点では、サービスの本格化および多機能化のためには、多要素認証実装が必須であった。この多要素認証の実装途上、前述の MS365 を用いた方式の仕様をほぼ定めた後、COVID-19 禍が発生した。

4.2 COVID-19「後」の本学の VPN セキュリティ評価

COVID-19 禍発生後、3 月中旬には、教職員および学生のリモートアクセスの早急な実現が、必

須となった。4 月 6 日には、“名古屋大学の構成メンバーとしての自覚を持ち、自律的で理性的な行動を求む！”と題して、総長からのメッセージが発信された。リモートアクセスなどを利用して、教職員・学生が 3 密を避ける行動をとることが要求され、そのための IT ツールの充実化についても鋭意進めていることが述べられた。

そこで、4 月中旬までに、3 つの VPN サービスを全て正式サービスとして、全学に展開した。図 9 に最大同時接続ユーザ数を示す(1 日ののべ接続数は、これよりも遙かに多い数になっている)。4 月中旬から VPN ユーザ数は増加し、4 月末の連休直前でピークを迎えた。この時期、ロックダウン寸前の最も厳しい警戒レベルになっており、ほぼ、全員がテレワークのような状況であった。すなわち、大学に出勤しているのは、筆者らのような大学インフラの運用を担う、ごく限られた教員などに限定された。

この時点で、セキュリティに比べて利便性に重きが置かれるというセキュリティポリシーとなった。この状況下においては、VPN 無しでのテレワークでは、処理できることに限界があった。特に、経理や人事給与システムを止めることはバイタルな問題につながるため、担当事務職員が、これらのシステムおよびそのバックヤードへリモートアクセスできるサービスを提供する必要があった。この判断により、多くの VPN の利用がなされ、この正念場を乗り切れたと思われる。

5 今後の VPN の展開とセキュリティ

本原稿執筆時点では、with コロナという声も多く聞かれる小休止状況になった。政府の Go To トラベルなど、感染防止策と同時に、経済振興政策が実施されている状況である。本学でも、後期(秋学期)からの対面講義をアナウンスするなど、COVID-19 対策は、小休止を迎えた。

現在は、今後の新たなパンデミックやインフルエンザなどの他の感染症と COVID-19 の同時再流行などに備えた対策を進めつつある。多要素認証機能の早期実装、リモートアクセスでの情報漏洩防止のための VDI 機能導入および VPN サービスシステム全体の冗長化など、徐々にセキュリティや信頼性に重点を置いた取り組みに向かっている。

COVID-19 が終息していない状況では、多要素認証の導入に当たっての初期設定時の本人確認には、難しさを感じている。本来であれば、学生証や職員証で本人確認すべきところ、COVID-19 感染の恐れから、大学に来れない学生・職員の存在があるためである。ここでも、セキュリティポリシーにおいて、利便性のほうに重点が置かれるのであろう。

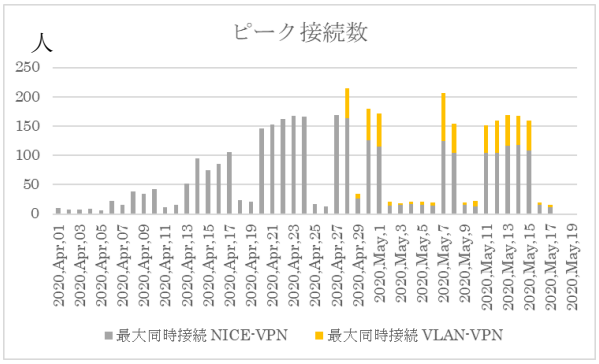

図 9 日毎の VPN の同時接続最大ユーザ数

6 おわりに

VPN サービスの展開を通して、COVID-19 によって、利便性とセキュリティリスクのどちらを重く見るかといったセキュリティポリシーの変化が顕著に見られた。リモートアクセスの重要度が低い平常時には、ポリシーはセキュリティリスクを重く見るため、VPN サービスの展開は遅々として進まなかった。COVID-19 後は、リモートアクセスの利便性が重く見られ、VPN サービスは急展開することになった。

このようなセキュリティポリシーの変化は、今回のような COVID-19 のみならず、この先も発生するであろう可能性が否定できないパンデミック禍においては、繰り返し発生すると思われる。広域で重大な自然災害などの場合にもこのようなセキュリティポリシーの変化は見られるであろう。

謝辞

名古屋大学 VPN サービスの構築に当たっては、情報連携統括本部の多くの人から多大な貢献をいただいたことをここに記して、深謝する。

参考文献

[1] 名古屋大学 VPN サービス
http://www.icts.nagoya-u.ac.jp/ja/services/