ToMMo スーパーコンピュータを利用するための 遠隔セキュリティエリアの設置と運用

長瀬　祥子 [1),2)], 中村　直毅 [3),2),1)], 伊藤　和哉 [2)], 葭葉　純子 [2)]

平野　幸子 [1)], 齊藤　智 [1)], 木下　賢吾 [1),4)], 中山　雅晴 [2),3)], 冨永　悌二 [3),2)]

1) 東北大学 東北メディカル・メガバンク機構
2) 東北大学　医学系研究科 3) 東北大学病院 4) 東北大学　情報科学研究科

nagase@med.tohoku.ac.jp

Installation and operation of “Remote security areas” for the ToMMo Supercomputer

Sachiko Nagase [1),2)], Naoki Nakamura [3),2),1)], Kazuya Ito [2)], Junko Yoshiba [2)]

Sachiko Hirano [1)], Tomo Saito [1)], Kengo Kinoshita [1),4)]

Masaharu Nakayama [2),3)], Teiji Tominaga [3),2)]

1) Tohoku Medical Megabank Organization, Tohoku Univ.
2) Graduate School of Medicine, Tohoku Univ.
3) Tohoku University Hospital
4) Graduate School of Information Sciences, Tohoku Univ.

概要

東北メディカル・メガバンク機構（ToMMo）のスーパーコンピュータを利用するための遠隔セキュリティエリアの運用は、2016 年 12 月から開始した。遠隔セキュリティエリアを設置する際には、覚書を締結し、そこに定められたセキュリティ区画の要件を満たすことが必要で、生体認証や監視カメラの準備とともに、アクセスネットワークの準備を進めることとなる。覚書が締結され、セキュリティ区画・アクセスネットワークの準備が整うと、シンクライアント端末一式が遠隔セキュリティエリアに配送され、セキュリティ監査の実施、承認後にスーパーコンピュータを利用できるようになる。

遠隔セキュリティエリアからスーパーコンピュータへのアクセス拠点は、2019 年 9 月現在、東日本 14 拠点、西日本 7 拠点の合計 21 拠点と順調に増加している。遠隔セキュリティエリアからスーパーコンピュータを利用するためのアクセスネットワークの総通信量は、受信 1Mbps 以下、送信は最大でも 10Mbps 程度で、東日本・西日本どちらからでもストレスなく利用できるアクセス環境を提供できており、さらなる拠点数の増加にも十分に対応できる。今後は、コスト面に配慮しながらサポート体制を整え、遠隔セキュリティエリアからスーパーコンピュータの利用率の向上に繋がる取り組みを続けていく予定である。

1 はじめに

東北大学星陵キャンパス内に設置されている東北メディカル・メガバンク機構（以下、ToMMo）のスーパーコンピュータは、「個別化医療」「個別化予防」を達成するための情報解析とデータバンクの両方の機能を併せ持つ、複合データバンクの基盤としての役割を担っている。スーパーコンピュータに蓄積されている複合バイオバンクを構成するデータは、セキュリティレベルごとに区画を分けて格納されており、それぞれ異なる Firewall 配下のネットワークを割り当てることでセキュリティを担保したネットワークシステム内で解析が行われている [1]。

ToMMo では、全国各地にスーパーコンピュータを利用できる研究拠点を増やすため、スーパーコンピュータの分譲区画を、シンクライアント端末から安全に利用できる遠隔セキュリティエリアの運用を 2016 年 12 月から開始した [2]。

本稿では、遠隔セキュリティエリアの設置から利用までの仕組みとその運用について報告する。

2 遠隔セキュリティエリアの概要

2.1 スーパーコンピュータの利用

ToMMo スーパーコンピュータ（以下、スパコン）は、東北メディカル・メガバンク計画の未来型医療の推進に必要な研究開発に利用できる。メガバンク計画に基づく共同研究がスタートした場合、倫理申請と共同研究の申請を行うことで、スパコンの利用資格を満たす。スパコンには、公開区画、分譲・共同利用区画、内部解析用区画の 3 区画があり、共同研究では、分譲・共同利用区画のアカウントを ToMMo のゲノムプラットフォーム連携センター（以下、ゲノプラセンター）に申請することになる。

共同研究では、機微性の高い情報を扱うため、シンクライアント端末から仮想デスクトップ経由でスパコンに接続し、分譲・共同利用区画を利用する[1]。

また、シンクライアント端末の利用予定場所は、セキュリティ区画の条件を満たしている必要があり、学外の申請者は、星陵キャンパス内の共用端末室、または、遠隔セキュリティエリアを選択することができる。

2.2 遠隔セキュリティエリアの要件

遠隔セキュリティエリアにてスパコンの利用を希望する場合、遠隔セキュリティエリアを設置する組織の代表者が、情報エリア管理者（以下、エリア管理者）となり、「遠隔セキュリティエリアの利用手順書」等を参考にして、エリア設置の準備を進める。

エリア管理者が所属する組織（または、遠隔セキュリティエリアを設置する組織）は、ToMMo と「遠隔セキュリティエリアの利用についての覚書」を締結する必要がある。

覚書に定める利用環境では、遠隔セキュリティエリアの出入口を、クライアント端末で用いる生体認証（現状は、指紋認証）と異なる種類の生体認証による入室管理の制御下で常時施錠、及び、監視カメラ（図 1）で入退室を録画することが課せられている。

これは、星陵キャンパス内の共用端末室と同等のセキュリティ要件となっている。共用端末室は、エリア設置前から利用できるので、実際に仕様を確認して設置を検討することが可能である。

図 1 共用端末室の入退室管理（左:虹彩認証装置、右：監視カメラ）

2.3 クライアント端末の要件

クライアント端末は、ゲノプラセンターでキッティング済みのシンクライアント端末と周辺機器一式を貸し出すこととなるので、覗き見防止の対策がとられた設置場所が必要となる（図 2）。

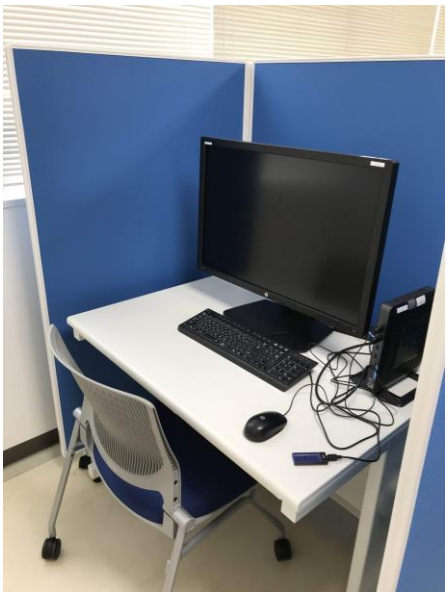

図 2 シンクライアント端末一式

2. 4 アクセスネットワークの要件

覚書が締結された場合、全国どこの大学や民間の研究機関でも一律のサービスを提供できることを考慮し、ToMMo では、NTT 東日本と NTT 西日本が提供するフレッツ光ネクストのアクセス回線とフレッツ・VPN ワイド（以下、VPN ワイド）によるバーチャルプライベートネットワークを介してスパコンにアクセスできるネットワークを構成した [3]。

2019 年 8 月現在のアクセスネットワークの概要を図 3 に示す。ToMMo では、センタールータのアクセス回線として、フレッツ光ネクストファミリー・ハイスピードタイプを契約している。この回

線は、データ受信最大 200Mbps、データ送信最大 100Mbps のベストエフォート型となっている。

ToMMo のセンタールータの WAN 側は、VPN ワイドプラン 10 の VPN 管理者（E1, E11）と VPN 参加者（E2～E20, W1～W10）の間を PPPoE と IPsec で接続する（図 3）。センタールータの LAN 側は、学内のシンクライアント端末と同じ仮想デスクトップに接続して利用するように構成されている。

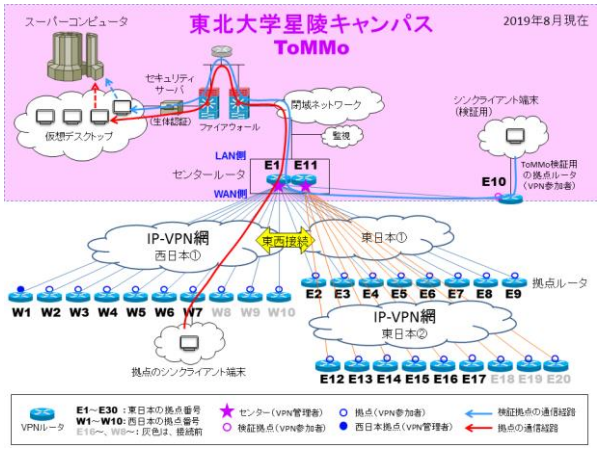

図 3 アクセスネットワークの概要

遠隔セキュリティエリアの拠点ルータは、エリア管理者が、「ToMMo の遠隔セキュリティエリア設置希望」を最寄りの NTT 東日本もしくは NTT 西日本の担当者に連絡して、手軽に申し込めるようになっている。最寄りの NTT 担当者が、ToMMo の NTT 東日本営業担当者と連携し、レンタルルータの申請書に必要なパラメータを記載したものを用意して、ゲノプラセンターを介して申し込みが完了する。その後、回線工事が行われ、レンタルルータが拠点に設置されれば、アクセスに必要なネットワークの準備は完了となる。

また、予め設計した拠点数（10 拠点）を超えて、遠隔セキュリティエリアの設置の見込みが出てきた場合には、ToMMo で新たに VPN ワイドプラン 10 を申込み、VPN 管理者に払い出される PPPoE のユーザ ID とともに設計情報をセンタールータに反映させる工事が必要となる。

2.3 端末のキッティングとセキュリティ監査

遠隔セキュリティエリアのセキュリティ区画整備とネットワークの準備が完了すると、ToMMo では、セキュリティ監査を実施する。監査に合格すると、エリア管理者と同じ組織のエリア利用者は、シンクライアント端末からスパコンに接続できる。

そのため、ToMMo のゲノプラセンターでは、スパコンを利用するためのシンクライアント端末一式のキッティング作業を行う。基本設定を実施し、ToMMo の検証拠点 E10 を用いて動作確認が取れた後、配布先で利用する IP アドレスを端末に設定してキッティングが完了する。キッティングされた端末は、セキュリティ監査に間に合うように遠隔セキュリティエリアに配送される。

遠隔セキュリティエリアでは、受け取ったシンクライアント端末を設置し、この端末を NTT が設置したレンタルルータに接続することでスパコンへアクセスできるようになっている。

セキュリティ監査を受け、監査で承認されるとスパコンの利用申請により発行された ID パスワードを入力し、さらに指紋認証することで、スパコン接続用の仮想デスクトップにログインできる（図 3）。

図 4 東日本と西日本のアクセス拠点数

3 運用

3.1 アクセス拠点

ToMMo のセンタールータ（E1, E11, E21）と検証環境（E10）を除くと、2019 年 9 月現在、東日本 14 拠点、西日本 7 拠点の合計 21 拠点において、遠隔セキュリティエリアのアクセスネットワークの接続が完了となっている（図 4）。

2017 年当初は、西日本と東日本の IP-VPN 網間を接続するための東西接続の費用が 10 拠点を超えると大幅に増えてしまうため、図 5A のような見込みを立てた [2]。結果として、西日本は、2017 年 1 月に、最初の拠点が接続してから現在まで 10 拠点以内で納まっているため、必要最低の費用で運用している（図 5B）。

一方、東日本の拠点は順調に増加しており、2018 年 3 月に 20 拠点まで拡張し、2019 年 9 月に 30 拠点を見越した工事を行った。この拠点追加の工事は、他の拠点に全く運用影響を与えることなく実施できた。

東日本の場合、VPN ワイドの 10 拠点のうち 1 拠点（図 3 の E11）を ToMMo に割り当て、セッシ

ョンを増やして接続している。VPN ワイドのプラン 30 に移行する場合と比べて、月額費用は半額以下で構成しており、当初の見込み（図 5A）の範囲内の必要最低限のコストで運用できている（図 5B）。

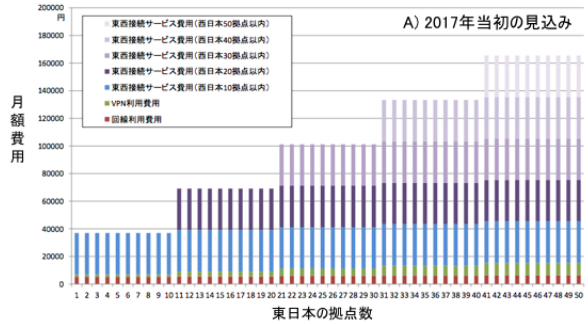

図 5A 東日本 VPN 管理者の運用コスト（2017 年当初の見込み）

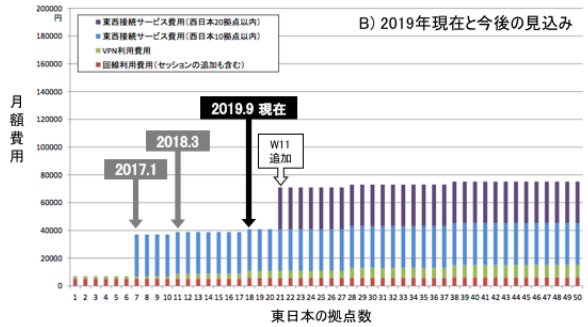

図 5B 東日本 VPN 管理者の運用コスト（2019 年現在と今後の見込み）

3.2 アクセスネットワークの通信

過去 1 年間分の ToMMo センタールータの WAN 側（拠点側）の通信は、1 日平均で受信 0.2Mbps 程度、送信 1.2Mbps 以内で推移している（図 6A）。また、2019 年 8 月以降は、送信量が増加しており利用が増えている。仮想デスクトップの利用では、センターから拠点のシンクライアント端末に画面転送しているため、受信量に比べて送信量が多いと考えられる。

1 日分の通信（図 6B）では、5 分間平均で送信 6Mbps を超える通信量があったことが判る。一方、受信は 0.5Mbps 程度で推移している。

また、一週間を通しての通信は、月曜日から金曜日までの平日日中帯が多く、平日でも昼休みの時間帯には通信量が減っていることが分かる（図 6B）。センタールータの WAN 側の通信量は、すべてのアクセス拠点の合計量を示しているが、1 拠点あたりの通信を観測すると、5 分間平均で受信は数十 Kbps 程度、送信は数百 Kbps～1.2Mbps 程度である。ToMMo では、センターとの通信にあまり帯域を消費しない仮想デスクトップを利用していることから、現状では、拠点数が増加しても、アクセスネットワークがボトルネックにならないことを確認している。

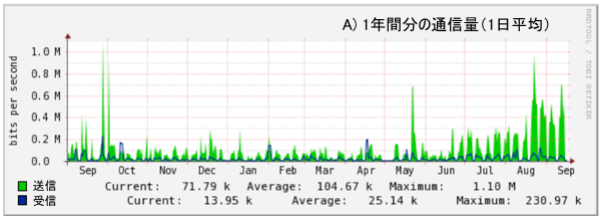

図 6A センタールータ（WAN 側）の 1 年間の通信量

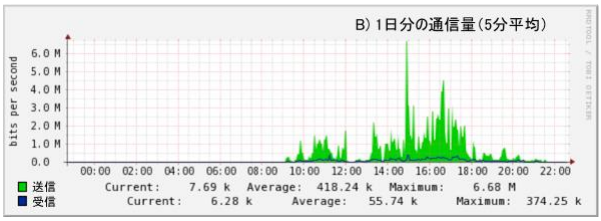

図 6B センタールータ（WAN 側）の 1 日の通信量

3.3 スパコンへの接続

アクセスネットワークを構築した当初、アクセス拠点のシンクライアント端末から仮想デスクトップにログインする際に、ログイン失敗や 40～50 秒程度の遅延が生じる不具合が発生した。この遅延は、ネットワークが DNS サーバを参照できない構成となっており、シンクライアント端末で名前解決のタイムアウトが生じていたことが原因であった。この不具合は、シンクライアント端末の hosts ファイルに接続先サーバのホスト名を記載するとともにサーバ証明書関連の設定を見直し、名前解決しないようにすることで解消した。これまでの運用の中で、これ以外には特に大きな問題は発生していない。

遠隔セキュリティエリアの利用状況は、エリア管理者とエリア利用者のアカウントから仮想デスクトップにログインした回数で集計しており、東日本のほうが西日本よりも利用頻度が高いことが分かる（図 7）。東日本の遠隔セキュリティエリアからのログイン回数は、1 ヶ月当たり最大 226 回で、月平均は 152 回であった。平日の利用者は、平均すると 7～8 名程度と予想される。

図 7 遠隔セキュリティエリアから仮想デスクトップへのログイン回数

4 まとめ

本稿では、ToMMo の遠隔セキュリティエリアを円滑に運用するための様々な取り組みについて述べた。

2019 年 9 月現在、東日本 14 拠点、西日本 7 拠点の計 21 拠点の遠隔セキュリティエリアの設置が進んでいる。東日本では、30 拠点までの増加を見込んで工事を完了しており、西日本は、11 拠点目の開通に合わせて、VPN 管理者の運用コストが増える見込み（図 5B）となっている。

遠隔セキュリティエリアからスパコンへのアクセスは、センターとの通信にあまり帯域を要求しない仮想デスクトップを利用しているため、アクセスネットワークの総通信量は、センタールータの WAN 側で受信 1Mbps 以下、送信は最大でも 10Mbps 程度に留まっており、東日本・西日本どちらからでもストレスなく利用できるアクセス環境を提供できている。従って、新たな遠隔セキュリティエリアの設置にも十分に対応できるようになっている。

今後は、トラフィックや利用者アクセスを監視しつつ、サポート体制を整え、既設および新設の遠隔セキュリティエリアからスパコンの利用率の向上に繋がる取り組みを進める予定である。

参考文献

[1] Takai-Igarashi T, Kinoshita K, Nagasaki M, et al. Security controls in an integrated Biobank to protect privacy in data sharing: rationale and study design. BMC Med Inform Decis Mak. 2017;17(1):100. doi:10.1186/s12911-017-0494-5.

[2] 長瀬祥子，中村直毅，伊藤和哉，葭葉純子，齊藤智他．遠隔セキュリティエリアからスーパーコンピュータへの接続サービス -全国展開の事例-．第 37 回医療情報学連合大会(第 18 回日本医療情報学会学術大会)論文集，2017，医療情報学 37 (Suppl.), 538-540.

[3] 長瀬祥子，中村直毅，伊藤和哉，葭葉純子，高畑知香他．アウトソーシングによる VPN 接続サービスの展開．平成 28 年度大学病院情報マネジメント部門連絡会議　ポスター抄録 p49-52, 2017.