一般口演
# 一般口演12
# ネットワーク・システム開発
2017年11月21日(火) 16:15 ～ 17:45 B会場 (12F 会議室1202)

[2-B-3-OP12-2] 遠隔セキュリティルームからスーパーコンピュータへの接続サービスの展開事例

長瀬 祥子[1,2], 中村 直毅[2,1], 伊藤 和哉[2], 葭葉 純子[2], 齊藤 智[1], 木下 賢吾[1], 冨永 悌二[2,1] （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）

東北メディカル・メガバンク機構（以下、 ToMMo）では、全国各地に設けられる ToMMoのセキュリティ要件を満たす遠隔セキュリティルームにおいて、シンクライアント端末から ToMMoのスーパーコンピュータの一区画にアクセスする接続サービスの提供を2016年12月から開始している。

著者らは平成28年度大学病院情報マネジメント部門連絡会議において、遠隔セキュリティルームの接続サービスを全国各地に展開するにあたり、1. 安全なネットワーク網の構築、2. 全国各地の大学や研究所など様々な組織へのサービス提供、3.サービス提供のための運用保守体制について比較・検討をおこない、サービス利用者が、所属組織のネットワーク管理者を頼らずに、簡単かつ安全に接続することができるアウトソーシングによる VPN接続サービスの展開について報告した。本サービスでは、 NTT東日本が提供するフレッツ VPNワイドとそのオプションサービスのレンタルルータを用いて、安全なネットワーク接続を東日本エリアにおいて展開した。しかし、西日本エリア（富山県、岐阜県、静岡県以西の30府県）へ本サービスを展開するためには、接続構成や運用体制などさまざまな課題を抱えていた。

本稿では、 ToMMoのスーパーコンピュータと遠隔セキュリティルームをネットワークで接続する VPN接続サービスを全国各地へ提供するためのネットワーク構築のうち、東日本エリアから西日本エリアへも拡張する際に検討した IP-VPN網の東西接続の問題を中心に、サービス提供のための回線費用や保守運用体制について比較・検討した内容を述べる。また、東日本エリアから西日本エリアへネットワークを拡張し全国均一となるネットワーク接続サービスを提供するための構築事例として、実際のサービス展開に至った過程と運用状況を報告する。

©一般社団法人 日本医療情報学会

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 －

長瀬祥子[*1*2]、中村直毅[*2*1]、伊藤和哉[*2]、葭葉純子[*2]、
齊藤　智[*1]、木下賢吾[*1*3]、冨永悌二[*2*1]
*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　情報科学研究科

Service of a supercomputer that can be accessed from remote security areas
- A deployment case throughout eastern and western Japan -

Sachiko Nagase[*1*2], Naoki Nakamura[*2*1], Kazuya Ito[*2], Junko Yoshiba[*2],
Tomo Saito[*1], Kengo Kinoshita[*1*3], Teiji Tominaga[*2*1]
*1 Tohoku Medical Megabank Organization, Tohoku University,
*2 Graduate School of Medicine, Tohoku University,
*3 Graduate School of Information Sciences, Tohoku University

Tohoku Medical Megabank Organization (ToMMo) has been started to service of a supercomputer that can be accessed from remote security areas in eastern Japan, December 2016. We considered about operation and management of the service, which is necessary to construct secure network, and to provide various research organizations all around Japan. Then, we decided to use outsourced VPN connection service of NTT EAST with rental VPN router. This service can be easily applied by users of remote security area in eastern Japan without a network administrator. However, there were some problems about network, cost and management to deploy the service for additional remote security area in all around Japan. Because, the IP-VPN network between NTT EAST and NTT WEST is separated, we had to use the connection service at high cost if more than 10 connections in a session. Therefore, we decided to construct IP-VPN within 10 connections per a session. We will plus another session each 10 connections if more than 10 connections have been connected. We conclude this is the minimum cost of our service.

Keywords: VPN (Virtual Private Network), supercomputer, remote security area.

1. はじめに

東北大学星陵キャンパス内の東北メディカル・メガバンク機構（ToMMo）に設置されているスーパーコンピュータは情報解析とデータバンクの両方の機能を有し、個別化医療や個別化予防の達成を目的としている 1)。そして、ToMMo では、このスーパーコンピュータを利用できる拠点を日本全国の研究機関に設置することを目指して 2016 年 12 月からサービスを開始した。利用者は、各拠点に設置されたシンクライアント端末からスーパーコンピュータの分譲区画にアクセスすることで、遠隔地からでもスーパーコンピュータ内のゲノム情報などの機微性の高い情報を安全に扱うことができる。この際、各拠点のシンクライアント端末は、生体認証や監視カメラが整備され高いセキュリティ要件を満たした ToMMo の遠隔セキュリティエリアにのみ設置することができる 2)。今後，全国どこの拠点から接続することになった場合でも同じようにスーパーコンピュータへ安全にアクセスできる接続サービスを展開する必要がある。

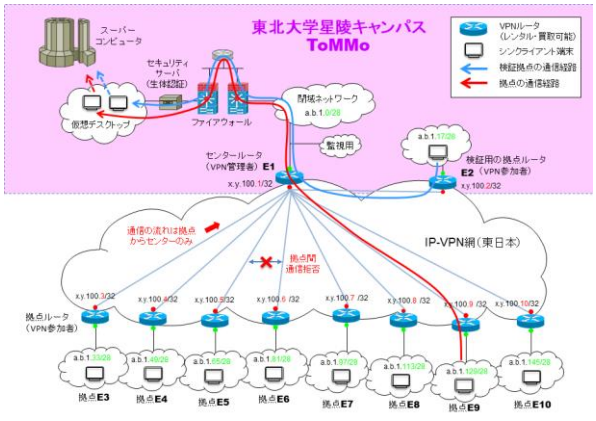

図 1　VPN 接続サービスの概要

遠隔セキュリティエリアからスーパーコンピュータに接続するために構築した VPN 接続サービスの概要を図 1 に示す。ToMMo に設置したセンタールータは、東日本エリアに 9 地点の遠隔拠点を追加することを想定して設計した。新規に遠隔拠点を追加する際には、VPN ルータの IP アドレスや割り当てるサブネット、IPsec のトンネル情報などの VPN 接続に必要なパラメータは、ToMMo で予め構築したものを利用する。新規利用者は、最寄りの NTT 営業担当者を ToMMo に連絡する。ToMMo で受けた連絡を ToMMo の NTT 営業担当に伝えると、申し込みに必要な事項が記入された申請書が ToMMo に届く。ToMMo では VPN 接続に必要なパラメータを申請書に補完し NTT に返却することで新規利用者の申し込みが完了する。そして、NTT の工事が終わると新規利用者はレンタルルータを用いた VPN 接続サービスを開始できる 3)。

サービスが開始されると、遠隔地でレンタルした拠点ルータと ToMMo のセンタールータは IP-VPN 網内の IPsec トンネルを介して接続される。これにより、遠隔セキュリティエリアの拠点ルータ配下のシンクライアント端末は、ファイアウォールを介してスーパーコンピュータの仮想デスクトップ用セキュリティサーバに接続できるようになる（図 1 赤矢印：拠点の通信経路）。また、様々な接続時のトラブルに対処するため、シンクライアント端末の動作確認ができるように、9 地点の遠隔拠点のうちの1拠点を遠隔セキュリティエリアと同じ構成で ToMMo 内に設置してある（図 1 青矢印：検証拠点の通信経路）。

2. 目的

遠隔セキュリティエリアの接続サービスを全国各地に展開するにあたり、1. 安全なネットワーク網の構築、2. 全国各地の大学や研究所などへのサービスの提供方法、3.サービス提供のための運用保守体制、の三点について、比較・検討してきた。そして、各拠点でのサービス利用者が、利用者の所属する組織のネットワーク管理者に頼ることなく、簡単かつ安全に接続することができるアウトソーシングによる VPN 接続サービスの展開について著者らは報告した 3)。このサービスでは、NTT 東日本が提供するフレッツ VPN ワイドとそのオプションサービスのレンタルルータを用いて、セキュアな IP-VPN の閉域ネットワーク接続を展開している。しかし、東日本エリア(新潟県、山梨県、長野県以東の 17 都道府県)だけではなく、西日本エリア(富山県、岐阜県、静岡県以西の 30 府県)へ本サービスを展開し、さらに拠点数を増やしていくためには、接続構成や運用体制、運用費用面でさまざまな課題や問題点を抱えている。これらの問題を克服するため、東日本エリアでの VPN 接続サービスの現状を解析し、西日本エリアへの VPN 接続サービスを展開するための手法を確立する必要がある。そして、西日本エリアでも安価で効率的かつ安全に運用できるシステムを構築することが本稿の目的である。

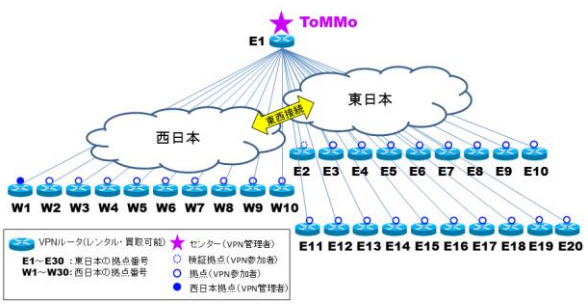

図 2 センタールータ1セッションの場合の VPN 論理構成

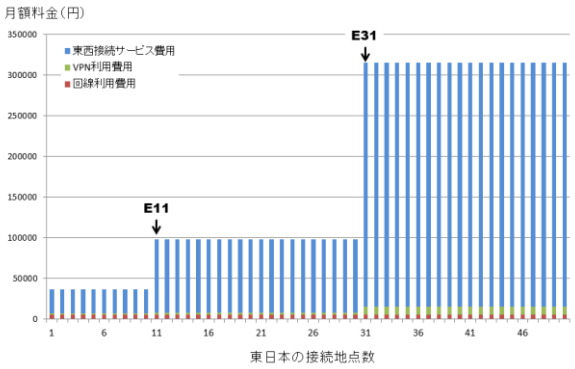

図 3 接続地点数による VPN 管理者の月額料金
(全拠点を1セッションでセンタールータに接続する場合)

3. 方法

全国を網羅した VPN 接続には、NTT 東日本と NTT 西日本間の通信が必要であるため，東西接続サービスを利用してシステムを構築する(図 2)。VPN 管理者が東西接続サービスを利用することで、東日本エリアの VPN 管理者が管理している IP-VPN 網と西日本エリアの VPN 管理者が管理している IP-VPN 網の間で通信することが可能となる。

西日本エリアの最初の接続拠点(図 2 :W1)が VPN 管理者となることで、その後の拠点は、VPN 参加者として西日本エリアの IP-VPN に接続できる。西日本エリアでは、VPN 管理者(W1)でも VPN 参加者(W2～W10)でも拠点ルータは全て ToMMo のセンタールータ(E1)と IPsec のトンネルを張るスター型のネットワーク構成とする。

IP-VPN の同じセッションで東日本エリアの接続拠点を増やす場合、VPN 管理者の月額利用料金は、図 3 のように、ToMMo を含めた接続拠点が 10 拠点を超えた時点(E11～)と 30 拠点を超えた時点(E31～)で大幅に増額する。つまり、東日本エリアと西日本エリアの接続地点がそれぞれ 10 地点以上になった時、ネットワーク拡張にともなう費用が増加する。今回の VPN 接続サービスでは、各拠点ルータからセンタールータへの通信のみが必須であり、拠点間の通信は拒否するように設定している(図 1)。つまり、拠点ルータはセンタールータにさえ接続できれば良いので、図 2 のように拠点ルータ同士を全て同じ IP-VPN セッションに集約させる意味はない。従って、東日本エリアで 10 拠点を超える際には、30 拠点用のプランに移行するのではなく、新たに、10 拠点分の IP-VPN のセッションを追加して運用する方式を取る(図 4)。

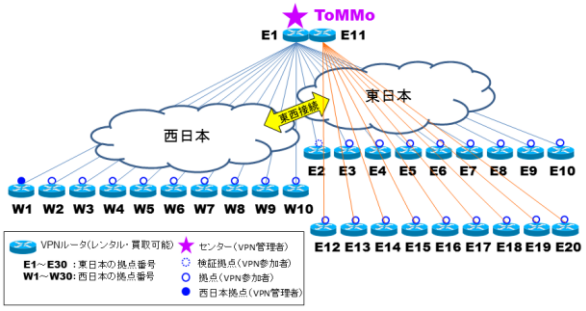

図 4 センタールータ 2 セッションの場合の VPN 論理構成

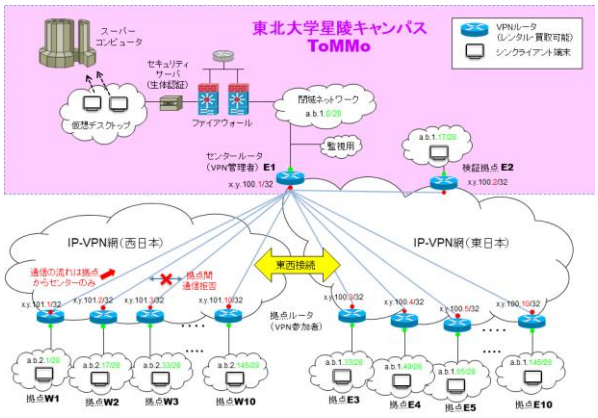

図 5 東日本エリアと西日本エリアを東西接続で繋いだ VPN 接続サービスの概要

4. 結果

3 章で述べた方式に従いシステムを構築した(図 5)。ネットワーク設計とセンタールータの設定及び拠点ルータの設定は、遠隔拠点が NTT 西日本管内でも、NTT 東日本を介して、アウトソーシングできた。また、保守体制では、東日本・西日本

管内とも、センタールータと拠点間のトンネルが切断した場合にアラートメールが配信されるよう、センター側のネットワーク保守を拡張した。フレッツ IP-VPN 網と拠点側の保守については、東日本管内も西日本管内も東西接続管内もすべて NTT 東日本と NTT 西日本にアウトソーシングした。

2017 年 9 月 6 日現在、東日本エリアで 6 拠点、西日本エリアで 2 拠点の遠隔セキュリティエリアにサービスを提供している。また、現在手続き中の追加拠点を考慮し、東日本エリアで 20 拠点まで、西日本エリアで 10 拠点までの VPN 接続サービスができるようにネットワーク構成を準備している。これに関わる費用増加を抑えるため、論理的に東日本エリアの拠点のみで構成される IP-VPN セッションを ToMMo のセンタールータに追加する方針である。これにより，東日本の拠点が 20 拠点まで増えても VPN 管理者の費用は、5 万円以下で運用できる（図 6 の青色）。

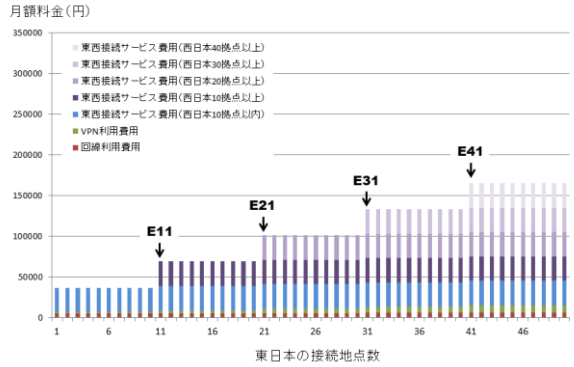

図 6　接続地点数による VPN 管理者の月額料金
（複数セッションに分けてセンタールータに接続する場合）

5. 考察

東西接続サービスを用いて東日本エリアと西日本エリアの双方の遠隔セキュリティエリアからスーパーコンピュータに接続する VPN 接続サービスが可能となった。この東日本エリアと西日本エリアは実質、全国を網羅している。

ToMMo では、全ての遠隔拠点との接続状況を把握できるようなネットワーク保守体制で、安定したサービスを提供している。具体的には、各拠点ルータとセンタールータ間の IPsec トンネルの切断や再接続を検知した際にアラートメールを配信するように設定している。スーパーコンピュータの担当者は、このメールを確認することで、各拠点と VPN の接続状態を把握できる。また、遠隔セキュリティエリアのシンクライアント端末からスーパーコンピュータに通信できないという申告があった場合には、ToMMo に設置した検証拠点のシンクライアント端末を用いて、スーパーコンピュータ担当者がサポートする。このサポートで解決しない場合や IPsec のトンネルが切断したままの場合には、遠隔拠点側のアクセス回線と VPN 回線及び、VPN ルータ（レンタル）の問題である。フレッツ回線とフレッツ VPN ワイドの契約では、各遠隔拠点からフレッツ故障受付のフリーダイアルで対応可能である。

6. まとめ

全国を網羅する商用回線として、フレッツ回線とフレッツ VPN ワイドを用いて、スター型の VPN 接続サービスを提供した。東日本エリアと西日本エリアにそれぞれ 10 拠点以上の接続拠点がある場合、単純に同じネットワークに拠点を追加する手法（図 3）に比べて、10 拠点ずつ追加する手法では月額料金の増加が段階的になり（図 6）、運用費用を抑えることができる。

今後、東日本エリアで 20 拠点、西日本エリアで 10 拠点を超える場合にも同様のネットワークの論理構成の変更と契約変更が必要となる。例えば、西日本エリアで 10 拠点を超える場合に、今回の手法を用いると、その時点から、図 6 の紫色の費用を加算できる。このように、拠点増加に伴い、必要最低限の費用で効率的なサービスを提供できる。また、物理構成をできるだけ変更せずに必要なタイミングで拡張することでネットワーク機器の導入コストを抑え、保守体制を維持した安定した運用が可能となる。

参考文献

1) ToMMo Super Computer [https://sc.megabank.tohoku.ac.jp/(cited 2017-Sep-7)]
2) 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.
3) 長瀬祥子，中村直毅，伊藤和哉ら. 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.