安全性と柔軟性を備えたリモート保守接続環境の運用管理

長瀬祥子 [1)], 中村直毅 [2)], 白川宣行 [1)], 小川　諭 [1)], 齊藤　智 [1)], 木下賢吾 [3)]

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

nagase@med.tohoku.ac.jp

Operation and management of a network infrastructure for secure and flexible remote maintenance.

Sachiko Nagase [1)], Naoki Nakamura [2)], Nobuyuki Shirakawa [1)], Satoru Ogawa[1)], Tomo Saito[1)], Kengo Kinoshita[3)]

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

概要

東北メディカル・メガバンク機構では、個人情報や解析情報を扱うため安全性を重視したネットワークを管理している。このネットワークに接続した実験機器やサーバ等の保守のため、安全性と柔軟性を備えたリモート保守接続環境を構築し運用管理をしてきた。この発表では、これまでの運用管理状況について報告する。また、これまでの課題をまとめ、今後の運用と更改に役立てたい。

1 はじめに

東北メディカル・メガバンク機構（ToMMo）では、医療情報とゲノム情報を複合させたバイオバンクを構築しており、システムごとに異なる機密性が必要とされる個人情報や解析情報を扱っている。そこで、セキュリティポリシーの異なる複数の firewall （以下、fw）を組み合わせることで、同じ fw 内の通信や異なる fw 間の通信、クライアントからの通信をきめ細かに設定できるように Virtual LAN （以下、VLAN）を用いてネットワークを構築した[1]。一方、各 fw 内の VLAN に接続された機器を遠隔保守するため、機器の担当者のみが対象機器に接続できるリモート接続環境も構築した[2]。この環境では、安全性の高い認証を経て ToMMo 内の限定された VLAN にのみ接続することができ、監査証跡のために「いつ誰がどこからどこへ通信しているか」が通信ログとして記録されるようにリモート接続を構築している。本稿では、このリモート保守接続環境について、これまでの運用管理状況について報告する。

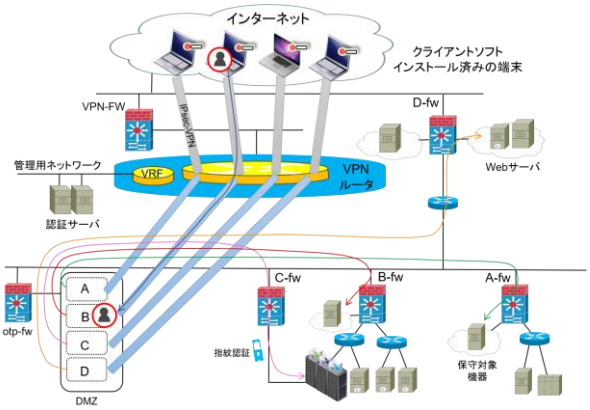

図1. ネットワーク構成

2　リモート保守接続環境

2.1 リモート接続の制御概要

このリモート接続環境では、ハードウェア・トークンが生成するワンタイムパスワード（One Time Password）と PIN コードの組み合わせで認証する方式でインターネットから Virtual Private Network へ接続する（以下 OTP-VPN と呼ぶ）。OTP-VPN では、ユーザ１名ごとに１アカウントを発行し、RSA SecurID ハードトークン SID 700（以下、トークン）のシリアル番号をアカウントに紐づけてユーザに提供する。ユーザは、ToMMo の

VPN ルータへのリモート接続の設定を埋め込んだクライアントソフト Cisco AnyConnect Secure Mobility Client（以下、AnyConnect）とトークンを受領し、PIN コード（4〜8 桁の英数字によるパスワード）を設定するとリモート接続が可能となる。ユーザは、アカウントと初回接続時に設定する PIN コードとトークンが 1 分毎に生成するワンタイムパスワード（6 桁の数字）を用いることによって、インターネットから ToMMo のネットワークに IPsec（IKEv2）による VPN 接続ができる（図 1）。VPN 接続時には、グループごとに 29〜24bit マスクの IP アドレス帯を割り当て、OTP-VPN 専用の fw（図 1 の otp-fw）のルールを設定することで対象機器の IP アドレスとポートのみにアクセスできる。その際、ユーザ間の通信はできないように VPN ルータで制御しセキュリティを担保している。

2.2 リモート保守接続申請

ToMMo に設置されている機器に対して学外からのリモート保守接続が必要な場合、下記を遵守できる場合に限ってトークンを提供している。

- ✓ アカウントの使い回しをしないこと。
- ✓ トークンの管理に責任を持つこと。
- ✓ ToMMo と交わした覚書の遵守事項に同意すること。

実際の手続きでは、機器が設置されている部門の責任者が、ToMMo の該当するネットワークの情報管理セキュリティ小委員会へリモート保守接続申請書を提出する。保守業者が学外からリモート接続を希望する場合は、保守業者と ToMMo の間で有効期間と遵守事項、秘密保持、責任体制を含む覚書（案）も提出する。この内容を小委員会で審議し承認された場合には、覚書の締結を事務で処理する。同時にネットワーク管理者は、リモート保守接続ができるようにユーザとグループを作成し、ネットワークやサーバを設定する。有効期間は毎年度末とし、年度毎に再申請による更新手続きを実施している。

3 運用

3.1 リモート保守接続申請状況

2016 年度から 14 件の新規のリモート接続の申請があり、年度更新を含むと延べ 61 申請があった。このうち 2 件は、OTP-VPN 接続を試したが、保守業者で導入しているリモート接続ツールでないと保守が難しいとの申し出があり、ホワイトリストで運用した。また 1 件は、保守業者の固定 IP とのみインターネット VPN の接続ができるように調整した。その結果、OTP-VPN による接続では、11 パターンの fw のルールと各種サーバの設定を行い、ToMMo の担当者ごとに 9 グループに分けて運用した。

3.2 リモート保守接続利用状況

2016 年 4 月から現在まで各月のリモート接続のアクセス数と利用者数の推移状況を図 2 に示す。1 ヶ月当たり最大接続数は、約 250 回であり、2016 年 4 月に 3 グループで運用が始まってから最大 9

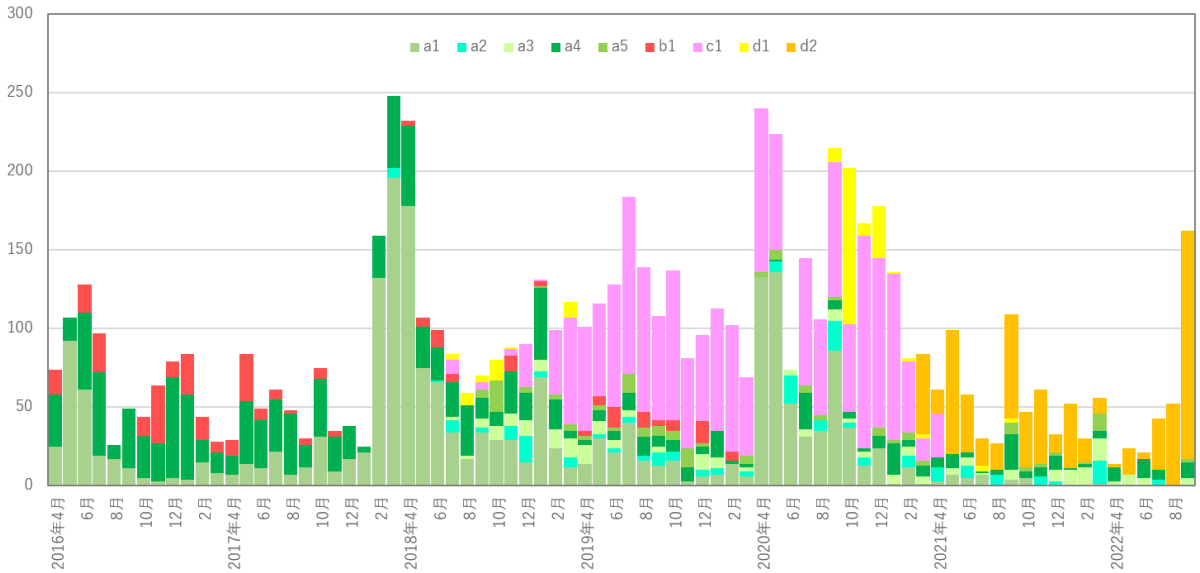

図2. グループごとの月別アクセス数

グループとなり、2022 年 9 月現在は 5 グループで運用している。新しい機器やシステムの導入時に新規申請があり、構築期間には多くのアクセスがあるが、運用期間に入るとアクセス数が減少する場合が多い。システム更改があると再びアクセス数が増加する傾向がある。新型コロナ対策による移動制限が始まった 2020 年春頃には、ユーザのアクセス回数が例年よりも多少増加したが、リモート接続環境が整っていたことで、機器の保守に大きな混乱を生じることなく事業を継続することができた。

2018 年より ToMMo の担当者に OTP-VPN 制御の権限移譲するため、次の権限を付与した。

- アカウントの開閉
- アカウントのロック解除
- PIN コードのクリア
- トークンの時刻同期

これにより、リモート接続時のトラブル対応をグループ内で迅速かつ円滑に行えるようになった。

4 課題と考察

4.1 リモート接続の要件の調整に際しての課題

ToMMo の機器への OTP-VPN 接続は、4 箇所の fw に設置された機器に対して 9 グループで実際に運用してきた。このように複数の fw への通信が必要になっても柔軟に対応できることを見据えて OTP-VPN の接続環境を構築し、様々なリモート接続の要望に応えることができた。要件を満たし使用を許可した 9 グループの内訳は、次の通りである（表 1）。

表 1. グループの内訳

fw（図 1）	グループ（図 2）	グループ数
A-fw	a1, a2, a3, a4, a5	5
B-fw	b1	1
C-fw	c1	1
D-fw	d1, d2	2
総計		9

このうち D-fw の 2 グループは、当初想定していなかった Web サーバや DB サーバの保守用途の要望に対応した（図 1: D-fw）。OTP-VPN 接続後に、Web サーバと DB サーバ宛の ssh 通信できるような環境を提供している。

一方、海外メーカーの大規模な機器やシステムでは、海外から不特定多数の保守人員によるリモート保守が必要となっており、そのリモート接続費用も保守契約に含まれていた。また、海外で勤務している保守人員にトークンを配布し安全に管理するように調整することは困難であった。そのため、本来であれば、統一したリモート接続方式を採用するのが望ましいが、業者が希望する商用のリモート接続管理ソフトウェアを条件付きで許容することにした。

リモート接続管理ソフトウェアを利用するには、当該機器からインターネット上のリモート接続管理ソフトウェアのサーバ向きの通信をホワイトリストで許可する必要があるとともに、通信ログからは、機器の遠隔操作の詳細を把握することはできない。そのため、リモート接続時に安全上の問題やインシデントが生じた際に、ToMMo の VLAN に影響が及ばないような考慮をするとともに、万が一の際には業者が責任を負うよう妥協点を図った。

【ホワイトリストで許可した例】

ToMMo の担当者が、踏み台となるサーバを別 VLAN に用意し、その踏み台サーバ経由でリモート接続を許可し、このアクセス履歴を監視することにした。

【インターネット VPN で許可した例】

リモート保守接続元と ToMMo の 2 地点間のみのインターネット VPN 接続環境を用意するため専用の VPN-IPsec 対応機器を設置し、この接続環境用の VLAN を保守対象機器の設置場所に伸ばした。ToMMo の担当者は、機器の遠隔保守メンテナンスが必要な時に、ToMMo の VLAN からインターネット VPN 用の VLAN に LAN ポートの接続を変更する。メンテナンスが完了したら ToMMo の VLAN に戻すという運用をしている。切替日時は、VLAN を設定しているネットワークスイッチのポートのダウンアップで記録している。

4.2 トークンの利用に際しての課題

OTP-VPN 導入の際には、有効期限が 5 年間のトークンを購入した。4 年目頃から電池の残容量が減るにつれて、トークンの時刻がずれて接続できない障害が発生した。トークンの時刻同期もグループごとに実施できるようにしていたため、利用者側の対応で調整することができ、原因が分かってからは大きな問題にはならなかった。また 2019 年に有効期限切れに伴い、トークンの更新を実施した。年度更新の手続きに合わせて、旧トークンを回収し新トークンを配布するという流れをグループごとに実施し、切り替えはスムーズに完了し

た。ハードウェア・トークンを利用する場合には、導入後にこのような手間も考慮する必要がある。

4.3 データの持ち出し・持ち込みに際しての課題

リモート接続の際のリスクには、データの持ち出しやマルウェアなどに感染した危険なファイルの持ち込みがある。覚書の遵守事項では規定しているものの意図せずにインシデントが発生する可能性がある。

そこで 2018 年度以降は、リモートデスクトップ接続用に Windows OS の仮想端末を用意し、その仮想端末を踏み台にして保守対象機器に接続できる環境を整備した（図 3）。Windows OS でデバイスを制御し、ToMMo の VLAN からのデータの出し入れは FTP サーバ経由のみに限定した（図 3 破線矢印）。FTP サーバでは、ウィルスチェックのリアルタイムスキャンを有効にし、必要に応じてファイルのアップロードとダウンロードを有効に設定する。一度アップロードしたファイルの削除は禁止し、アップロード後 1 週間経過したファイルは、圧縮して保管用ディレクトリに移動するようにスクリプトで処理した。

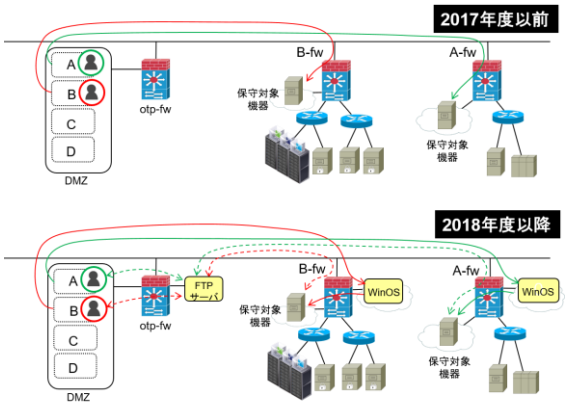

図3. FTPサーバによるデータの持ち出し・持ち込み管理

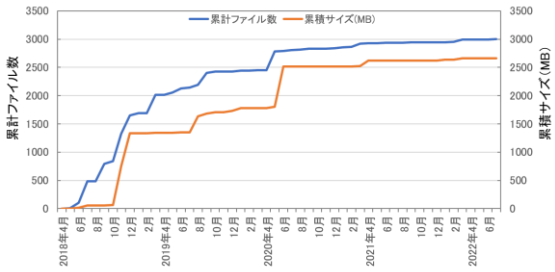

図4. データ持ち出し・持ち込みファイル数とサイズ

その結果、リモート接続先から FTP サーバ経由で持ち込まれたデータと持ち出されたデータの累計を図 4 に示す。１年に１回程度、大きなファイルのやり取りが多い時期があり、システムのアップデートなどの対応の様子が判る。また約４年間で 2.7GB 程度のデータの出し入れがあったが、現時点では特にインシデントは発生していない。

5 まとめ

本稿では、リモート保守接続環境の運用状況について報告した。OTP-VPN のリモート接続環境は本格運用から約 7 年が経過し、提供中のトークンの有効期限は 2024 年までである。

現在は、スマートフォンの普及もあり、ハードウェアを用いたワンタイムパスワード認証以外にもソフトウェアトークンや生体認証など多様な認証方式の選択肢も増えている。保守業者のリモート接続という用途では、ハードウェアを用いたトークンは、個人のスマートフォンに頼らずに利用でき、固有のパスワード（PIN コード）とワンタイムパスワードの二要素で認証でき、所有物認証にもなるというメリットがある。

本来、ToMMo へのリモート接続は、ToMMo で準備した OTP-VPN 接続に統一して運用できれば理想的であった。しかし、実際には、保守対象機器や保守契約内容は多岐に渡り、機器の新規導入や更改の時期も異なる。そのため、ToMMo の担当者にリモート保守接続申請の準備を速やかに実施してもらうことで要望を把握し、ToMMo のネットワークへのリスクが最小限になるよう案件ごとの対応を行ってきた。

今後は、リモート保守接続申請の状況を踏まえてより利便性が高く安全に接続できるリモート環境を検討していきたい。

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, 長田 俊明, 高畑 知香, 鈴木 麻里恵, 鈴木 みどり, 冨永 悌二: 安全性と柔軟性を備えたリモート接続環境の構築. 第 35 回医療情報学連合大会(第 16 回日本医療情報学会学術大会)論文集, 医療情報学 35 (Suppl.), 970～973, 2015.