V. セキュリティ対策の具体例

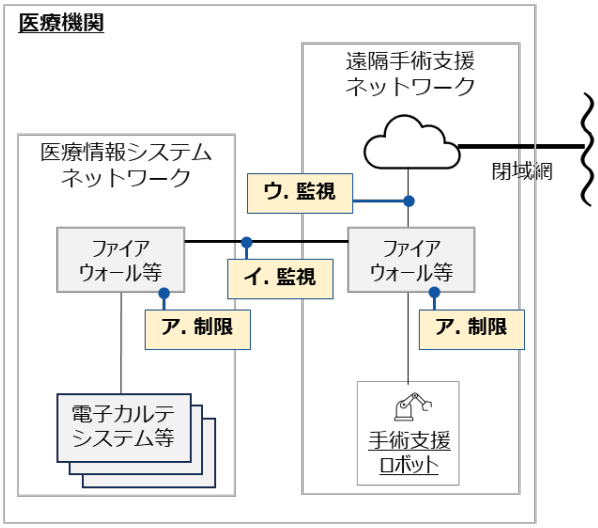
令和 4 年度国立研究開発法人日本医療研究開発機構（AMED）「高度遠隔医療ネットワーク研究事業」における『手術支援ロボットを用いた遠隔手術の実現に向けた実証研究』の中でセキュリティ対策の具体例について検討を行った。

本ガイドラインは、両施設間や手術支援ロボット事業者間を閉域通信ネットワーク等のセキュアなネットワークを用いることで遠隔手術環境の閉域性を高めた構成を前提としている。しかしながら、今後の遠隔手術の利用方法の発展に伴い、医療情報システムネットワークとの接続や手術支援ロボット事業者以外との多様な外部への接続も想定される。その場合、重大なセキュリティ事案が発生する危険性を有するため、次のように情報セキュリティ対策に留意して遠隔手術を行う必要がある。

なお、遠隔手術環境をセキュリティ監視する場合、セキュリティ監視機器が手術支援ロボットの操作に必要な通信等を認識できることや複数ネットワークの効率的な監視にあたって、各ネットワーク機器と物理的に近距離へ設置することなどを考慮する必要がある。

（1）施設内接続の留意点

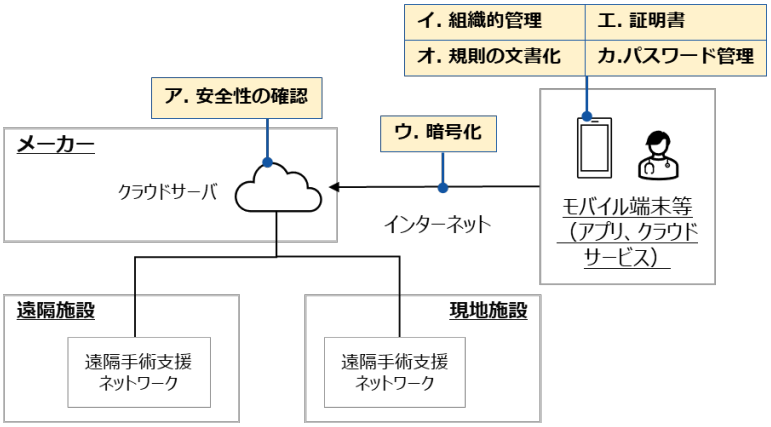
情報連携の目的で医療情報システム等と遠隔手術環境を接続するケースが想定される。



図：施設内接続イメージ

1) 遠隔手術環境と医療情報システムネットワーク等を接続する場合、医療情報システムネットワーク等においてもファイアウォール等により宛先／送信元 IP アドレスや使用ポート番号を可能な限り限定すること。
2) 遠隔手術環境と医療情報システムネットワークを接続する必要がある場合は、医療情報システムネットワーク側と遠隔手術支援ネットワーク間で不適切なアクセスの監視等の情報セキュリティ対策を講じること
3) 現地施設と遠隔施設の遠隔手術支援ネットワーク間で不適切なアクセスの監視等の情報セキュリティ対策を講じること。

（２）クラウドサービス利用時の留意点

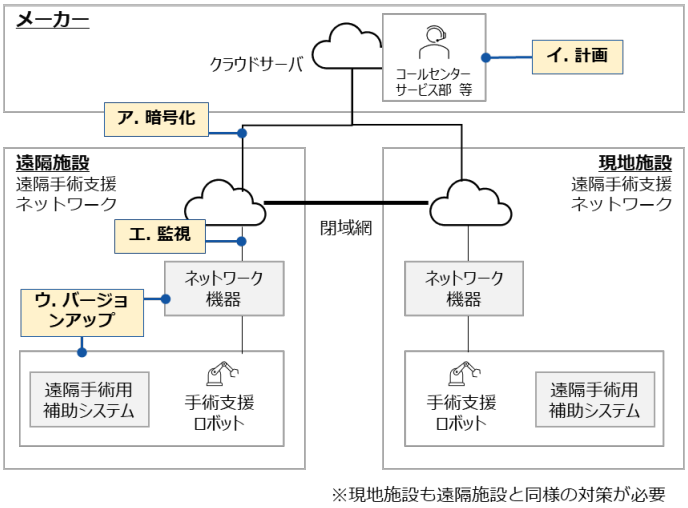


図：クラウドサービスの利用イメージ

1) 手術支援ロボット製造販売元が提供する、手術支援ロボットで行った手術の操作履歴等を確認できるクラウドサービスを利用する場合、当該サービスのリスク評価を踏まえて、医療情報の安全管理を確認すること。具体的には、利用するクラウド基盤の ISMAP 登録等の第三者評価･認証の有無や、当該サービスにおいて、アクセス管理（特権の管理、識別･認証情報の管理、物理セキュリティ等）、システムの開発・変更に係る管理（開発管理、変更管理）、システムの運用管理（脆弱性管理、障害管理、システム運用監視、ネットワーク管理、クラウドサービスにおける各種設定の逸脱監視、冗長性の確保等）、これらを委託している場合は、委託先における管理状況の把握を含めて確認すること。
2) 医療機関等が管理しない情報通信機器で、クラウドサービスにアクセスするモバイル端末等（例えば BYOD：Bring Your Own Device、個人保有の情報機器の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規程等に含めること。また、これに基づいて利用される情報通信機器について、利用の許諾状況も含めて、医療機関等が管理する情報通信機器と同様に、台帳管理等を行うこと。
3) クラウドサービスへ接続する場合、暗号化された通信を利用すること。
4) クラウドサービスへのアクセスにおいて、利用者の識別・認証を行い、利用者認証方法に関する手順やアカウントの管理について、規則、マニュアル等で文書化すること。
5) クラウドサービスへ個人情報を含む情報を保存する場合、接続する情報通信機器にクライアント認証を実装すること。
6) パスワードを利用者の識別・認証に使用する場合、第三者に推測されにくいものとするよう、安全性を考慮したパスワードを設定すること。

（３）保守管理接続の留意点

手術支援ロボットのメンテナンスや利用状況把握（モニタリング、ログの収集等）のため、手術支援ロボット事業者と保守回線を接続するケースが想定される。



図：保守管理接続イメージ

1) ロボットの保守管理等の目的で外部回線と接続する場合、利用する通信ネットワークに応じて、通信もしくは情報を暗号化すること。
2) 保守管理業務の内容に応じて、提供が必要な情報（手術支援ロボット等の機器の状態、操作実績や操作時間等の記録など)、アクセス方法および権限管理等のセキュリティ遵守事項について、保守業務の受託企業が保守管理計画書を作成し、管理者権限の扱い、アクセスする際のルールや手順を定め、施設の承認を得ること。
3) VPN 装置を用いる場合はファームウェアなどを最新に保ち、脆弱性のない状態を担保すること。IP アドレスについても、なりすましのリスクがゼロでないことに留意する必要がある。
4) 保守業務の受託企業と遠隔手術環境間で不適切なアクセスの監視等の情報セキュリティ対策を講じること。