保健医療における遠隔サービス– 使用事例
並びに顧客及びサービス機関の責務

この白書は，NEMA/COCIR/JIRA 合同セキュリティ及びプライバシー委員会（SPC）
によって作成されたものである。

この白書は，MITA（NEMA の 1 部門である医用画像&技術提携），
COCIR（欧州放射線・医療電子機器産業連合会），
JIRA（日本画像医療システム工業会）
の承認を受けている。

2008 年 9 月

www.medicalimaging.org
事務局: MITA（医用画像&技術提携）
1300 North 17th Street, Suite 1752, Arlington, VA 22209, USA
電話: 001-703-841-3200，ファクス: 001-703-841-5900
事務局: Richard Eaton，電話: 001-703-841-3248，ファクス: 001-703-841-3348
電子メール: reaton@medicalimaging.org

目次

1. はじめに

医療機器は，情報技術（IT）にますます依存し，フィルムを用いる医用画像は，情報技術（IT）が診断情報の収集，流通，表示及び保存の主流になるにつれて衰退してきている。IT の多くの生産性向上機能の中には，ネットワーク接続を効果的に活用してハードウェアやソフトウェアへの遠隔サービスを提供する機能があるが，この機能によって使用できる時間が増加し，付加価値サービスが向上する。遠隔サービスとは，保健医療提供機関のシステム運用サイトとは離れた場所からハードウェア及び／又はソフトウェアシステムの保守を提供すること（一般的に外部電話会社又はデジタルネットワークプロバイダ接続を通じて）と定義付けられている。

遠隔サービス機能は，機器の標準設備の一部となっている。ここ数年にわたって，遠隔サービスは，初期の遠隔診断ツール（保守技術員に現場到着前に必要なパーツを提供するために使用される）から包括的遠隔保守サービスへと発展してきた。今日，製造業者の遠隔サービスの業務内容では、次のようなアプリケーションのメニューが提供されている。例えば、あたかもサービス要員が現場に来て点検するのと同様な支援、業務専用付加価値サービス及び予防的診断である。悪化させてしまうと突然の不測のシステム問題を生じ，使用不能となってしまうようなシステム状態の初期兆候を含むステータス情報は，標準的な自動メッセージによって伝えられる。これらのサービスは，すべて世界中のさまざまな場所にある販売業者のサービスセンターで実施される。

遠隔サービスの恩恵は，顧客にとっても製造業者にとっても明らかである。遠隔サービスは，移動時間を短縮し，また移動時間そのものをなくしてしまうことも少なくなく，さらにサービスコストも大幅に削減する。その結果，病院内のハイテク機器の生産性が向上する。顧客は，こういった恩恵を認めており，このサービスの新たな手法を受入れ，それを歓迎していが，一方で，患者の医療・診断システムを外部の遠隔サービス提供センターに接続する際に直面するデータのプライバシーやセキュリティの起こり得る問題に対する懸念を次第に深めつつある。したがって，遠隔アクセス提供中の情報の流れをセキュリティ保護することは，情報保護を維持し，これらの革新的技術への顧客の信頼を保つために欠かすことができない。

この白書では，関連データのセキュリティ及びデータのプライバシー要求事項を含む一連の使用事例について記載する。その使用事例で，製造業者が極めて重要なセキュリティ及び患者のプライバシー問題にどのように対処しているかを明らかにする。

遠隔サービスを利用している各機関は，適用法の要求事項を理解して，ある特定の医用 IT システムの遠隔サービス設備で利用できるセキュリティ及びプライバシーの管理手段を決定することが必要になる。この白書全体を通じて，“要求事項”という用語は，国家又は地域の法令から生じうる高レベルの一般的要求及び責務を表している。しかし，この白書は，法規又は法令の包括的なレビューを意図したものではない。それよりはむしろ，この白書は，セキュリティ及びプライバシーの管理の次善又は最善の手段に焦点を当てているので、これらの手段が保健医療 IT を基礎にしたシステムで合理的に利用できることが望ましい。この白書では，いつデータのプライバシー及びセキュリティの懸念が生じうるのか，及び製造業者は顧客が法的要求事項を満たせるよう支援するためにこれらの懸念をどのように管理しているかの具体例を示す。

この白書は，遠隔サービス機能をもつシステムで，保健医療の提供，例えば HIS（病院情報システム），PACS（医用画像保管通信システム），画像システム，放射線治療システム及び患者監視システムの一部となっているシステムすべてに適用される。

これは，保健医療提供機関の IT の専門家に向けたものであり，IT インフラストラクチャ及びセキュリティ技術の基本的理解を前提としている。いつものことながら，特定のシステムに対するセキュリティ及びプライバシーの管理手段の完全な理解を得るために，販売業者が引き続き主な情報源となっている。

2. 使用事例

遠隔サービスの慎重な利用により，時間のかかる保守スタッフの現場訪問が回避される。突発的な重要な保守が必要な場合（又はそれを避けることができる場合）に，顧客にとっての最大の恩恵が実現される。この章は，スピードが重視される典型的な使用事例，及び医療の継続性に与えるシステム保守の影響を遠隔サービスがどのようにして最小限に抑えるかについて記載する。

2.1 オンデマンドサービス

2.1.1 偶発的データ削除

患者データが偶発的に削除されてしまった。例えば重大な状況では，その他のシステムの操作が行われる前に，削除されたデータを直ちに回復するのであれば，そのデータの回復がうまく行く公算が最も高い。回復プロセスが過度に遅延すると，保存装置の削除された領域が再使用され上書きされるため，このデータは，取り戻すことができない形で失われてしまう恐れがある。このようにデータが失われてしまうと，新たなに手動でデータを入力するか，又は患者への医療上の付帯リスクを伴う医療処置を繰り返さなければならないことがある。

2.1.2 医療処置中に遭遇する問題

一般的に，技術的な疑問又は問題は 1 日中いつ何時でも，医療処置の実施中にも起こりうる。これらの具体例では，内科医はその医療処置を止めなければならないか，又は短時間の機器のダウンタイム後に継続してよいかを，できるだけ迅速に決定する必要がある。遠隔サービス接続により，サービス機関が，技術的問題は直ちに解決できるか，又は長時間のダウンタイムを必要とするかを直ちに評価することができる。

2.1.3 システム故障後の再起動

保健医療 IT システムの故障は，保健医療提供場所でのワークフローに深刻な影響をもつことが少なくなく，一般的にシステムの再起動を必要とする。技術員による管理及び監視を受けて行う再起動は，遠隔で修正措置を実施することができ，したがってシステムのダウンタイムを最小限に抑え，さらに引き続きスムーズな稼働を確実なものとすることができる。そのような事例では，遠隔サービスがローカルのワークフロー妨害を低減し，同時に技術員を顧客の所在地に派遣する時間的遅延とコストを回避することができる。

2.1.4 リソース不足の場合のサポート

IT システムの継続的稼働は，機器のリソース又はスタッフの不足によって影響を受けることがある。これらの不足はそれぞれ，ローカルのワークフローを中断させることによって医療の提供を妨げる。

- 機器リソース不足：データ記憶領域の予期せぬ不足は，システムによるそれ以上のデータの取得又は処理を妨げる。追加の記憶ボリュームが利用できるようになるまで，一時的に外部の第三者へデータを電子的に転送することにより，そのようなリソース不足を補い，保健医療の提供の中断を短縮できる。
- スタッフ不足：スタッフの病気など予定外のスタッフ不足も，保健医療の提供を妨げる。製造業者がその遠隔サービスセンターから極めて重要な作業を管理・実行すること（例えば，バックアップを開始すること，又は現地のスタッフを指導することもあるかもしれない）でローカルプロセスを支援することができれば，悪影響が低減できる。

2.1.5 高度な問題固有監視

技術的問題の中には，散発的に発生し消失するものがある。これによって医療が中断し，問題の診断と解決が非常に困難なものになる。問題が再発した場合，ローカルシステムをさらに正確に監視し，ネットワーク接続を介して保守技術者に情報を与えることができる特殊なサービスツールの一時的使用が，遠隔サービスによって可能になる。これらの問題のいくつかは，ネットワーク接続問題から生じ，これは長期間(数日又は数週間の場合もある)のネットワークトラフィックの監視が必要となることがある。遠隔サービスがなければ，これらの問題を現場で解決するための時間的遅延及びコストは極めて多大なものとなるであろう。監視のその他の理由には，断続的なモーターの問題，温度の問題などが含まれる。

近代的な保健医療提供機関の高度に相互接続された IT 環境においては，1 つの技術的問題の原因となる個別のシステムの特定は簡単ではない。往々にして，数個のシステムが原因となって問題を引き起こしている。問題の原因を切り離すために，関係する製造業者すべてによる同時・協調的な調査が求められる。遠隔サービスにより，このような困難な問題を解決するために必要な関係者すべてのタイムリーで費用効率の高い連携が可能になる。

2.1.6 アプリケーション支援

新たなシステム又はアプリケーションの導入は，技術スタッフが新たな機能をどのように最大限に引き出すかを学ぶ期間が必ず必要である。この学習時間を短く保ち，システムの利用を最適化することにより，医療の質が改善される。遠隔サービスツールにより，システムの専門家は，“あたかもサービス要員が現場に来て点検するのと同様な支援”セッション中に技術スタッフを指導することができる。画面を共に見ること及び指導する者－指導を受ける者との会話によって，保健医療機関内部で極めて短時間で専門知識を高めることができる。操作上の質問，問題又は力量不足は，遠隔サービス接続を活用することにより当人だけを支援するという方法で短時間に解決することができる。

2.2 定期的サービス

上記の使用事例は，医用 IT サービスへの遠隔サービスの慎重な適用を通じて保健医療提供機関が得る恩恵の明らかな例をいくつか示している。提供される医療の品質は，医療提供機関が患者のデータの保護と同時に高レベルのシステム利用頻度（稼働率）を保証された場合に改善される。この恩恵は，次に由来する：

- システムの利用頻度の向上により，医療診断及び治療の時間が増え，重要システムがダウンした場合に必要となる間違いが発生しやすい“その場しのぎの対処”が回避される。完全に稼働可能なシステムにより，医療スタッフは患者への高品質な保健医療サービスの提供に専念することができる。
- 遠隔アクセスのための製造業者のサービススタッフの効率的な利用。遠隔サービスツールにより，製造業者は世界各地のいくつかのサービスセンターに少人数のスタッフを置いておき，そのスタッフのアクセスを注意深く管理・監視を行う。これにより，セキュリティ管理手段を実施し，患者データにアクセスする必要のあるサービス技術者数を最小限に抑える。この限定的なグループ及びそのグループのサービス技術者の保健医療提供機関システムへのアクセスをすべて監視することができることで，施設内の実際の現場へのオンコールスタッフの訪問よりも，さらに管理された環境をもたらし，したがってセキュリティ及びプライバシーのリスク緩和に役立つ。

2.2.1 ソフトウェアのダウンロード及び／又はシステム更新並びに試験

システムの遠隔サービスの接続可能性により，迅速なシステム更新，パッチング，及びその他のソフトウェアの部分的変更を行うための最高の機会が提供される。これは，顧客サービス技術者の現場到着前に，先行段階的なダウンロードとして実施することや，遠隔更新セッションの一部とすることが

できる。更新又はシステムの部分的変更を遠隔で行う場合，顧客のサービスセンターは，臨床スタッフと慎重に連携を取って，システムを臨床サービスから切り離し，保守業務完了後に臨床サービスを復旧させる方法を定めなければならない。適切な医療機器規則に整合させるため，遠隔サービスセンターは，更新後の現場での完全な検証を確実なものとするために現地での支援が必要となる場合がある。この場合，施設の技術スタッフは，始動前試験を実施する際に支援を求められることがある。

2.2.2 技術的問題を回避するためのシステム監視

近代的な遠隔サービスの提供には，IT システムの定期的稼働中に IT システムの医療利用を妨げることなくシステムの技術パラメータを監視することが必要となる。このステータス情報の通信は，医用システムから起動されることが多く，保護されたネットワークを介した通信によってシステム状態情報が自動的に遠隔サービスセンターに転送され点検を受ける。遠隔サービススタッフは，システムステータス分析システムからアラートが送信されてこない限り，実際に保健医療機関のシステムにログオンすることはない。例えば，稼働時間，アーカイブの利用可能な保存ボリュームなどのパラメータが故障の可能性や故障に近い状態を示す値を示した場合，早期の対策を予定に組み込むことができる。こういった対策を実施することにより，保健医療提供機関を予定外・不測のダウンタイムから守り，現場の柔軟性や意思決定を確保して，保健医療の品質及び継続性を確実なものとする。

3. 遠隔サービスの範囲

3.1 国際的見地

医療機器製造業者は世界的に事業を営んでいる。製造業者は，世界中に数多くの遠隔サービスセンターを置き，ファーストレベル及びセカンドレベルの製品サポートを提供している。特定の製品についてのサードレベルの深い知識は，1か所の製造拠点又は研究開発拠点にあることも少なくない。リアルタイムでネットワークに接続されている遠隔サービスの非常に素晴らしいメリットは，製造業者のサポート組織がすぐさま 3 つのレベルの専門家すべてから回答を得られることである。この速さが，コストと時間の両方を節減する。技術的問題を解決するために必要な技術の専門家は，地球の反対側にいてもよいのである。今日，すべての技術的問題に対処するよう訓練された専門家が各国にいることを期待するのは現実的ではない。そういった専門家がコスト効率とサービス効率の高い方法で世界各地に分散し，保健医療提供機関に必要なサービスを最大限に提供している。

3.2 遠隔サービスに関連するリスク

遠隔サービスによって得られる恩恵は，データ及びシステムのセキュリティとプライバシーのリスクを伴っている。セキュリティリスクには，データ又はシステムの機密保護，完全性，又は稼働率に対する潜在的危険が含まれる。プライバシーの危険は，セキュリティ違反（機密性の喪失）による個人情報の制御不能を意味することが少なくない。使用者の中には，遠隔アクセスが潜在的な不正アクセス及びユーザの医用 IT システムに損害を与えるシステム侵入につながることを懸念している可能性がある。

原則的に，IT システムへの保護されていない又は設定が不十分なネットワークアクセスは，悪意のある個人に，何の制約もなくその人物側にはほとんどリスクもなくアクセスを試みる可能性を与える。さらに，1 システム上に確認された脆弱性を，同種の多くのシステム上で再び利用することができる。遠隔サービスに起こりうるシステムセキュリティ侵害の可能性は，大きく 2 つの問題発生源に区分することができる。

- 臨床スタッフと遠隔サービス専門家との間の誤った通信によって起こる意図的ではない行為で，保守対象のシステムの取り違え（例えば，誤ったネットワークアドレス）など単純なものが多い。そのような事態は，現場での保守を実施時ではなく，遠隔でシステムにアクセスする際に起こる可能性が高い。

- 悪意のある個人が自身の目的のためにネットワークアクセスを利用してシステムを悪用する

意図的な破壊的又は隠れた行為。熟練したハッカー，又は技術に傾倒した 10 代の若者でさえも安全だと思われたシステムにアクセスし，使用し，又は悪質なソフトウェアによって，損害を与えてきたことが知られている。

意図的でない行為又は意図的な不正行為の可能性が高まったことは，遠隔サービスの提供に使用される IT インフラストラクチャを導入する際に，製造業者もユーザも無視すべきではない。適切な遠隔サービスは，サービス提供機関と保健医療機関との境界線を越えるため，セキュリティとプライバシーは共同責任であり，高いレベルの協力と信頼を必要とする。保健医療提供機関に課せられた使命の中で，医師の倫理綱領を医用 IT システムの役割に結び付け，SPC は医用 IT システムの最も重要な 3 つの特性を認識するにいたった。それは（優先順で），(1) 安全性，(2) 有効性，及び (3) プライバシーである。これが，医用 IT システムを維持する上での SPC の優先事項の指針であり，当方の医療の提供に対する脅威についての措置をまとめ上げるのに役立っている。

3.2.1 患者の安全性に対する脅威

患者及び臨床スタッフの安全性に影響を与える行為は，最も懸念されるものである。こういった行為は，機械部品の動作，機械操作の変更（X 線量，エネルギー配給などに影響を与える），治療の中断若しくは早期開始，又は個人の医療記録の変更によって生じる可能性がある。いずれも，患者や医療スタッフに対する重大な安全性リスクを招く恐れがある。

3.2.2 有効な医療に対する脅威

あらゆるネットワーク化された装置については，システム及びそのシステムがもつデータの利用頻度に関連するリスクが存在する。ウィルス，トロイの木馬，ワームの伝搬を通じた医用 IT システムに対する直接的な悪意ある攻撃，サービス拒否攻撃，又はさらにそのシステムを利用して他のシステムへアクセスを行うことが，最も一般的なセキュリティの侵害である。

3.2.3 個人情報（医療プライバシーを含む）の保護に対する脅威

支払い情報の誤用，識別情報の盗用，V.I.P 情報の開示，保険金詐欺，重要な治療情報の喪失，－これらすべてが医用 IT システムのネットワーク接続に付随する潜在的脅威である。こういった事態は，患者の安全性及び治療の有効性と比較すれば二次的なものと見なすことができるが，個人データの開示は，患者にとっても保健医療提供機関及び機器製造業者にとっても深刻である。

この白書は，医用 IT システムが医療機器規制指針に従って開発されたことを前提としている。こういった規則の下では，遠隔でサービスを提供する手段は，医療機器の安全性と有効性を目的として計画，設計及び試験が行われることが望ましい。これには，安全でセキュリティ保護された運用を可能にするための技術面，運営管理面及び物理面の管理が含まれる。

医用 IT システムが医療機器規則の対象となっていなかった場合，保健医療施設はシステム製造業者と協力して，安全性，有効性，セキュリティ（プライバシーを含む），相互運用性及びその他の機能的要求事項を適切に管理するリスク管理計画を作成した方がよい。

こういった種類のシステムがネットワーク（例えば，遠隔サービス）に接続されている場合にそのシステムを管理する際の支援策として，規格団体が ISO 専門委員会 215 と IEC 62A 分科委員会 62A の合同作業部会を編成し，新たな規格 IEC 80001“医療機器を組み込んだ IT ネットワークへのリスク管理の適用”を作成した。この規格は，こういったシステムのネットワーク接続のリスク管理の基本的なプロセスを示すことになる。この規格は 2010 年に正式な IEC 規格となることが見込まれている。

4. 患者データへのアクセス

遠隔アクセスセッションは，1 回の遠隔サービス提供セッション中に患者データにアクセスするか又はアクセス可能かによって分類することができる。この分類は，上記に参照した使用事例及びシステムの技術的性能には無関係である。

4.1 患者データへのアクセスを伴わない遠隔保守

システム状態の自動的報告の場合，システムステータス情報だけが転送される。例えば，保守上の注意を必要とするようなコンポーネントの問題や範囲外の操作を予見するためのシステムパラメータの監視がこれに当たる。データのプライバシー保護の立場から，また顧客の立場からも同様に，これが理想的な状況である。

システムの中には，リモートサービス要員による点検前に，データの匿名化を可能にするよう設計されたものがある。例えば，DICOM 画像の品質は，DICOM ヘッダー内に付随する患者識別情報が送信前に上書き又は消去されたとしても調べることが可能である。そのような匿名化機能は問題診断のためにデータを送信する前のオプションとして医用 IT システムに組み込むことができる。

4.2 患者データへのアクセス：可能又は必須である場合

医用 IT システムを診断して補修するためにさらに多くのシステム専門知識が求められる場合，医用 IT システム内部のすべてのコンポーネントとデータへのアクセスが必要となることがある。“何が起こったのか”についての情報を収集する際，最初の電話サービス連絡（第 1 階層サービス又は問題明確化段階と呼ぶ）中に患者データへのアクセスがある可能性は低い。しかし，いったん機器の専門家（第 2 階層），又はさらに工場を本拠地とする技術者（第 3 階層）が呼ばれると，綿密な調査に，患者データへのアクセスを含め広範な内部システムへのアクセスが必要になることが往々にしてあるようである。

遠隔サービスを通じた通常の第 2 階層及び第 3 階層への一歩踏み込んだアクセスが行われるようになったのは，この方法で機器を診断することが，サービス技術者への情報を最大限にして，それによってサービスの提供に要する時間的遅延とコストを低減するからである。しかし，ある医用 IT システムのサービスを行う際，医療利用の性質上，サービスを行うために個人情報を送信することが求められる可能性がある。例えば，PACS（医用画像保管通信システム）には，画像関連の医療記録のデータベースが含まれている。PACS の構成及びローカルでの利用によっては，投与データ及び完全な病歴も含めて，患者について利用できるデータの一部又はすべてをも PACS に含まれることがある。PACS データベース（又はその他のあらゆるデータベース）は，包括的な患者データで構成できるため，患者データへのアクセスが行われる可能性が非常に高い。さらに，問題専用監視ファイル（2.1.5 を参照）を用いる問題の解決には，患者データを見ることが必要になることもある。

これは，製造業者の技術的手段によって個人データを見させないようにする能力を制限する。こういった状況について，保健医療提供機関及び遠隔サービスセンターの両者によって，技術的解決策ではなく運営管理上の解決策が定められ適用されなければならない。適切な方針によって，明確な手続き，契約条件，行為の監査，及びその他の管理手段を定めなければならない。このような手段の実施により，サービスセッション中にアクセスされるデータを保護し，機器の補修を効率的に進めることが可能になる。

5. 遠隔サービスに関する技術的及び組織的解決策

遠隔サービスに関する技術的及び組織的方針と手続きは，遠隔サービスセッション中に患者データへのアクセスがない場合は制限を最少にすることができるが，患者データにアクセス可能か，又はアクセスする場合には，より厳しく制限しなければならない。情報のセキュリティを管理するため

に必要な組織的な方針及び手続きには，ある程度の相互信頼と信用を必要とし，そういった相互信頼や信用は遠隔サービスセンターが ISO 27001“情報技術－－セキュリティ技術－－情報セキュリティマネジメントシステム－要求事項”に記載されたような確立されたセキュリティ管理手段に一致した方法で事業を営んでいれば容易に達成できる。

この章は，サービスを提供する企業が遭遇しがちな顧客の要望集を収録し，遠隔サービス機関によって実施された解決策をできる限り記載している。これは，遠隔サービスの提供についての最初の SPC 白書“遠隔サービスの提供に対するセキュリティ及びプライバシー要求事項”（2001 年 11 月）に記録したものと全く同じではあるが，新たな顧客セキュリティ推奨事項が含まれている。この章は，製造業者及び顧客のそれぞれに対してセキュリティ管理手段を実施する責任の所在を詳しく説明する表 1 で締めくくられている。

5.1 組織的方針及び手続き

組織的方針及び手続きは，その保護のもとで遠隔サービスを実施することができるよう定めるものである。世界的に整合化された一連の方針に信頼を置くことができることは，製造業者にとっても顧客にとっても明らかに必要である。

国際的な規則は多くの細かい部分で異なるため，この白書は，完全かつ世界的に受け入れられた一連の方針を示すことはできない。しかし，現在，医用 IT システム及び遠隔サービスセッション中にアクセスされる医療データの両方を防護するために用いられている一連の組織的な慣行を記載する。

その目的は，システムとそのデータのセキュリティを維持しながら，合理的なコストで有効なサービスを提供することである。組織的方針及び手続きは，多くの場合，危機管理責任者，個人情報保護管理責任者，遠隔サービスセンター経営陣，及び法規制職員が関与し，細部にわたって交渉を行うことが可能である。

これらの組織的方針及び手続きには，次のようなものが含まれる。

- 遠隔サービスセッションは，電子的又は視覚的傍受によって起こりうる不正アクセスを避けるために管理手段が全部整えられている状態で，セキュリティを保護された場所から，適用法に従って実施されるという条件
- サービススタッフは，方針により情報を機密に保持しなければならない（かつ，そういった方針に従って訓練を受ける）という条件
- 保護されたデータ（個人データ，医療情報など）は，必ず契約による合意に従って，アクセス及び処理が行われるという指令
- 誰がどういった条件でサービス行為の監査記録を取得することが可能か，及び製造業者はどの位の期間，その記録を保持するのかを定める明確な条件
- 顧客の所在地と製造業者の遠隔サービスセンターとの間で，接続可能性の問題を解決するための仕組み
- プロセス，管理手段及び個人データに関連する活動の定期的監視
- 各機関が遠隔サービス開始前に，その機関が自身の規制要求事項を満たしていることを自ら検証すること

5.2 技術的慣行

5.2.1 接続権限の付与

顧客の機器に保存されている患者データへのアクセスの可能性を含め，顧客システムへの接続は，有効かつ情報を与えられた上での顧客の事前の承諾が必要である。これには，次のいずれかが含まれる。

- 顧客のシステムの継続的な監視及び／又は予防保守に対する長期的権限の付与

- 特定のサービスの 1 つの事例に必要となることが見込まれる短期的権限の付与

サービス契約書には次の項目が記載されることがある。
- 前もって定めたシステムへのアクセスタイミング
- 予防（予測）保守のための定期的アクセス及びオフピークアクセス
- 顧客が，遠隔サービスが行われているときを（視覚的な合図によって）知ることができること
- 顧客が，サービスセッションを拒否及び／又は切断できること

5.2.2 遠隔サービスセンターの適切な識別及び認証

保健医療施設は, その医用 IT システムにアクセスしている個人について知っておくべき要求事項がある。サービスは，高度な訓練を受けた個人の集合の中で共有される行為であるため，この要求事項は 2 段階のプロセスで満たすことができる。まず，製造業者は，遠隔サービス提供センターへのアクセスを制限し，サービスセッションを実施できる権限を付与した訓練済みのサービススタッフだけに限定する管理手段をもたなければならない。世界的な多種機器操作では，製造業者の管理手段が，アクセスを既知の選択した的確な技術者の集合に制限することが多い。サービスを実施する人物の実際の識別情報は，遠隔サービスセンターで管理され，監査される。次に，医用 IT システムが遠隔サービス設備に接続しているとき，その遠隔サービス提供センター自体の明確な識別及び認証が存在しなければならない。正しくサービスセンターを識別し認証するための見込みのある技術的解決策は，以前，SPC 白書“遠隔サービスインタフェース－解決策 A：デジタル証明書を用いるインターネット上の IPSec（インターネット・プロトコル・セキュリティ）”（第 2 版，2003 年 12 月）の中に掲載された。

顧客の中には現場の各システム上で複数のサービス技術者を個人的に識別することを求める者がおり, 上記の管理手段はその要望に取って代わることを意図していた。このような個別のログオンを可能にすることは，システムの複雑な機能を必要とし，サービスコストを大幅に増加させるであろう。

5.2.3 監査証跡

サービス行為は，適切な詳細度で記録することが望ましい。一般的に，これは自動監査記録によって実現されることになるが，特定の状況では，作業報告書も妥当な場合がある。記録は，サービスセッション中に不正行為が開始されたかを検証するための事後調査を支援する役目を果たすことが望ましい。記録によって，データのセキュリティとデータのプライバシーのレベルを上げるためにさらなる分析が必要な事例を検出しやすくすることが望ましい。サービス行為を記録するための仕組み及び記録された特定の細目は販売業者に任せるものの，保健医療施設は，要請次第，監査記録をレビューする機会を得ることが望ましい。SPC は，適切な保存期間として 1 年を推奨する。

監査記録は，次を含むことが望ましい。

- 事象の日付と時間（開始／終了）
- 業務を実施するサービス技術者まで行為を遡るに十分な一意の識別名
- アクセスされたシステムの一意の識別名
- 実施された操作行為及び診断行為の識別（例えば，インストールしたパッチ，変更した構造，ダウンロードした画像（識別されていない，又は識別された），データベースの補修，どのようなサービスツールが始動されたか）
- アップロード及び／又はダウンロードしたファイルの識別（例えば，単なるファイル名）

個人情報を記載することは追加的な防護と管理手段が必要となるため，監査記録が患者を識別する情報を含めることは望ましくない。SPC では，個人データ又は ePHI（電子個人医療情報）が含まれる可能性が高いことから，サービスセッション中にいかなる種類のキーストロークロギングも行わないよう推奨する。

監査記録への操作者情報の記載に対するニーズがあると感じられることが少なくない。管轄区域によっては，操作者の名前及び操作時間を記載することが個人データを構成することを理解することが重要である。記録がこの個人データを含める場合，新たな防護及び管理手段の必要性を生じる。

5.2.4 患者データのセキュリティ保護された機密（暗号化された）の転送及び保存

遠隔サービス行為を実施する際に最も重要な要求事項は，患者のデータを機密に扱うことである。患者データの機密転送を確実なものとする確立した技術は存在する（SPC 白書“遠隔サービスインタフェースー解決策 A：デジタル証明書を用いるインターネット上の IPSec（インターネット・プロトコル・セキュリティ）”（第 2 版，2003 年 12 月）を参照）。今日，VPN，TLS，SSL，SSL-VPN などその他の技術が，必要とされるレベルのデータのプライバシーとデータのセキュリティを保護するまでに成熟している。さらに，現地の規則が，暗号化方式若しくは変調長さ，又はその機関のネットワーク内での暗号化の利用についても，その最終決定に影響を及ぼす可能性がある。

遠隔サービスセンターでの個人データのあらゆる保存は，特定のサービス事例を解決するために必要な保存に制限することが望ましい。遠隔サービス個人データ保存の防護手段には，高度なセキュリティ手段が含まれること，及びデータの完全な暗号化を検討することが望ましい。

5.3 遠隔サービスを実施する際に推奨される責任

この白書では，セキュリティ保護された遠隔サービスセッションには，保健医療機関及びサービス機関の双方による責任の履行が必要であることを述べている。表 1 は，遠隔サービスの提供に関連する技術的及び組織的な手段の実施に対するそれぞれの責任を示している。

表 1： 技術的及び組織的な手段の実施に対して推奨される責任

	推奨される実施責任	
管理手段	**保健医療機関**	**サービス機関**
組織的方針及び手続き（5.1）	IT システムサービス機関によって提供される標準契約条項には，一般的に高レベルの信頼性がある。	適用法に基づく標準契約を利用して，サービスセッション中又はその直前の個々の条項の複雑な管理を避けることが望ましい。
接続権限の付与（5.2.1）	サービス契約は，接続権限の付与に関する条項を含む。	遠隔サービスセンターは，顧客特有の契約要求事項を認識しなければならない（標準契約条項の使用が強く推奨されている）。

顧客の所在地での遠隔サービスセンターの適切な識別と認証(5.2.2)	サービス契約は，サービス機関に対して次を要求する。 - 訓練を受けた正当な個人に対する遠隔アクセスの権限付与を承認するためのプロセスをもつこと - すべてのサービス行為を識別された人物まで遡れること	遠隔サービスセンターは，サービススタッフの行為の監査を含め，サービススタッフの識別と権限付与を実施するための技術的及び運営管理上の管理手段をもつ。
監査証跡（5.2.3）	サービス契約は，サービス機関が調査を行えるだけの十分な細部の監査記録を保持することを要求している。契約に基づいて監査記録の監査が許可される。	遠隔サービスセンターで収集され，セキュリティ保護された監査記録は，1年間保存することが望ましい。記録は，顧客の監査を許可するような方法で維持される。
セキュリティ保護された（暗号化された）患者データの転送(5.2.4)	サービス契約言語は，サービス問題の解決に必要な患者データへのアクセスを制限する。	データの転送は記録され，データはセキュリティ保護された，場合によっては暗号化された形式で保管される。技術的管理手段及び運営管理上の管理手段が存在し，サービス問題の終了後のデータの破壊を確実なものとする。

6. 結論

遠隔サービスセンターから医用 IT システムへのサービスは，現在，世界中で毎日毎時行われている。遠隔サービスの効率的な提供は，システムの稼働率と性能を高め，機器の保守費用を節減する。しかし，遠隔アクセス機能には不正アクセスのリスク，システムのセキュリティ侵害及び医療情報の不適切な開示の危険が付きまとう。医療の継続性，契約による取決めを含めた適切な技術的及び組織的な手段が備えられなければならない。

最近の技術の進歩によって，医用 IT システムに対する遠隔サービスの提供をセキュリティ保護された効率的な方法で提供することが可能になっている。これらのサービスを提供するために用いられるツールや接続は，慎重な設計，継続的監視，新たに発生するリスクに対処しながら品質とセキュリティのレベルを維持するための改良が必要である。

この白書は，遠隔サービスにおける慣行のいくつかについて詳しく述べている。ネットワーク及び IT 機器の複雑さによって，顧客及び製造業者は，この保守の連携における自分たちの責任について，明確に理解しなければならなくなっている。

最終的な注意書きの 1 つが作成されている。1 つの団体として SPC は，今まで，遠隔サービスを可能にする技術的解決策に焦点を当ててきたが，引き続き製造業者が自社のシステムの遠隔サービスを提供するためのセキュリティ保護された解決策を提供していくことが重要である。

しかし，医用 IT システムの効率的なサービス提供に欠かせない情報の国境を越えた移動を管理することを意図した法律や規則に迅速に対応すべく，さらに継続的な取組みが行われなければならない。現在，個人データ保護のための国及び地域の法律が存在し，かつ進化し続けている。この白書の範囲を超えるものの，医療器機産業及び保健医療提供機関は，自分たちが遠隔サービスに与える影響を理解するよう一丸となって取り組むことが不可欠である。

製造業者は，セキュリティとプライバシーの管理手段をもち，遠隔サービスにおけるデータの流れを明確に示さなければならない。顧客機関は，自らのローカルデータ保護の責務を理解し，これを果たす必要がある。両者が一丸となって規則に適合するよう取り組み，立法者及び規制者と共にコスト効率の高い機器サービスの提供と質の高い保健医療を目指した実質的保護を達成しなければならない。