SPC 承認用

最終ドラフト

リモートサービスインターフェイス -- ソリューション (A): デジタル証明書を用いたインターネット経由の IPSec ー バージョン 2

[バージョン 2 で NAT を追加]

Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)
オリジナル: 2003-04-02
最終バージョン: 2003-07-08

www.nema.org/medical/spc
Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
Secretary: Stephen Vastagh tel:703-841-3281 fax:703-841-3381 E-mailto:ste_vastagh@nema.org

(このページは、SPC ならびに NEMA、COCIR、JIRA が承認作業を行う際に参照しやすいように提供されている。承認済み最終ドキュメントでは、このページは削除される。)

これまでの変更のまとめ

以下の変更は、3 つの協会が承認した後で、ソリューション A (バージョン 1) の文書に対して SPC が提案したものである。これらの変更は、"修正ソリューション A"の 2003 年 4 月 2 日のオリジナルドラフトにおいて認められた。

3.1 節 - 項目 12 を 2048 ビット RSA から 1024 ビット RSA 証明書に変更する。この用途に対する最低限の鍵長としては、1024 ビットが妥当かつ適切であると考えられる。

3.2 節 - 段落 6 の最後を、証明書ペアは構成される各 VPN トンネルに対してのみ必要であることを示すように変更する。これは、若干あいまいであった元の文章を明確にするものである。

バージョン 2 における変更のまとめ

"ソリューション A (バージョン 1)"に対して以下の変更が行われた。

第 1 節 - 第 3 段落の中間部分を、NATを使用すればすべてのHCFでソリューションAを実現できることを示すように変更した。

第 3.4.0 節 - HCFまたはRSCのどちらのアクセスポイントからでもトンネルを開始できることを示す段落を追加した。HCFアクセスポイントの動的アドレス指定に関する段落を追加した。

第 3.4.1 節 - HCFのアクセスポイントを装置が存在するネットワークの近くに配置できることを追加した。

第 3.4.2 節 - NATの使用に関する情報を追加した。

第 3.4.2.1 節 - NATの使用とプライベートアドレス指定に関する新しい節。

第 3.4.2.2 節 - NATとグローバルアドレス指定に関する新しい節。

第 3.4.2.3 節 - HCFの追加管理に関する新しい節。

第 8 節 - 用語集。上記の新しい節で出現する新しい用語を追加した。

目次

1. 目的 1
2. 概要 2
2.1 通信ネットワーク 2
2.2 リモートサービスセンター (RSC) 3
2.3 医療施設 (HCF) 3
3. 通信ネットワーク 4
3.1 IPSec (v4) を用いたVPN 4
3.2 トンネルを確立する際のアウトオブバンド証明書配信を用いたRSCとHCFの手動認証 7
3.3 パフォーマンス要件 8
3.4 アクセスポイントの構成 8
3.4.1 ファイアウォール、フィルタ、ルーティングルール 9
3.4.2 ネットワークアドレス変換 10
4. リモートサービスセンター 12
4.1 RSCの管理 12
4.2 技術的手段 12
4.2.1 RSCのネットワークアーキテクチャ 12
4.2.2 責任追跡性の保護 13
4.2.3 個人識別可能な患者データの取り扱い 13
4.2.4 RSCをバイパスするリモート接続の禁止 13
5. 医療施設 14
6. 監査記録 15
6.1 医療装置 15
6.2 アクセスポイント 15
6.3 RSC 15
7. 結論 16
8. 用語集 17
9. 付録 19
9.1 ドメイン名ルックアップ 19
9.2 Dynamic Host Configuration Protocol (DHCP) 19
9.3 ネットワークアドレス変換 (NAT) 19
9.4 リスクの軽減 19

1. 目的

リモートサービスは、ベンダー固有のリモートサービスセンターから医療装置に対する保守およびサービス作業を実施するための、革新的な手段である。医療施設の外部にデータが送信される可能性があるので、セキュリティに対する脅威の可能性に対処して、送信されるデータの可用性、機密性、および完全性を保証する必要がある。NEMA/COCIR/JIRA Security and Privacy Committee (SPC) は、米国、ヨーロッパ、日本における適切な法的要件を収集し、共通する要件群を抽出し、ホワイトペーパー「Security and Privacy Requirements for Remote Servicing」を発行した。このホワイトペーパーは、NEMA、COCIR、およびJIRAからすでに包括的な承認を得ている。このホワイトペーパーでは、アクセスポイントのペア、つまりリモートサービスセンター (RSC) と医療施設 (HCF) の間で認証、監査記録、および暗号化を使用するアーキテクチャが提案されていた。今日使用されている複数のカスタマイズされたソリューションを、単一の標準化された接続に置き換えるようになっていた。

第 2 のホワイトペーパーの目的は、SPC の勧告に従って、実現が可能であり、妥当で、実際的な 1 つのソリューションを定義することである。このソリューションのことを"ソリューション (A)"と呼ぶことにする。このドキュメントでは、暗号証明書を使用してインターネット経由で IPSec を構成する方法、およびアウトオブバンド方式で証明書を配布する方法について説明する。さらに、HCF と RSC におけるサポート条件を定義する。ベンダーおよび医療施設は、このドキュメントに従うことで、既製の装置を使用して単一のアクセスポイントを構成できる。

SPCの勧告に適合する技術ソリューションは他にも多くあることは了解している。ソリューション (A) は、サービスを必要とする大部分のサイトで有効である。ただし、**さまざまな理由でソリューション** (A) **を簡単に実装できない**サイト、またはソリューション (A) が経済的ではないサイトが存在する。日本では、IPアドレス空間に制限があり、NATの管理コストが高いため、このソリューションは一般的ではないと考えられる。**しかし、サイトでNATを行うことができ、RSCとHCFがそれを管理できる場合は、このソリューションは、小規模、中規模、そして大規模なHCFに対して有効である。**一部の国では、暗号化が法律で制限されている。SPCは、このような特殊な条件によりよく対応するソリューションを新たに開発する予定である。

このホワイトペーパーは、IT 専門家を対象としており、IT インフラストラクチャおよびセキュリティ技術の知識を前提としている。読者は、ファイアウォール、侵入検出、アンチウイルス、仮想専用線 (VPN)、IPSec、ネットワークアドレス変換 (NAT)、ルーティング、監査管理などの概念に関する実務的な知識を有している必要がある。

2. 概要

図 1 に示すように、3 つの領域について考える必要がある。

1. 通信ネットワーク (インターネット)
2. リモートサービスセンター (RSC)
3. 医療施設 (HCF)

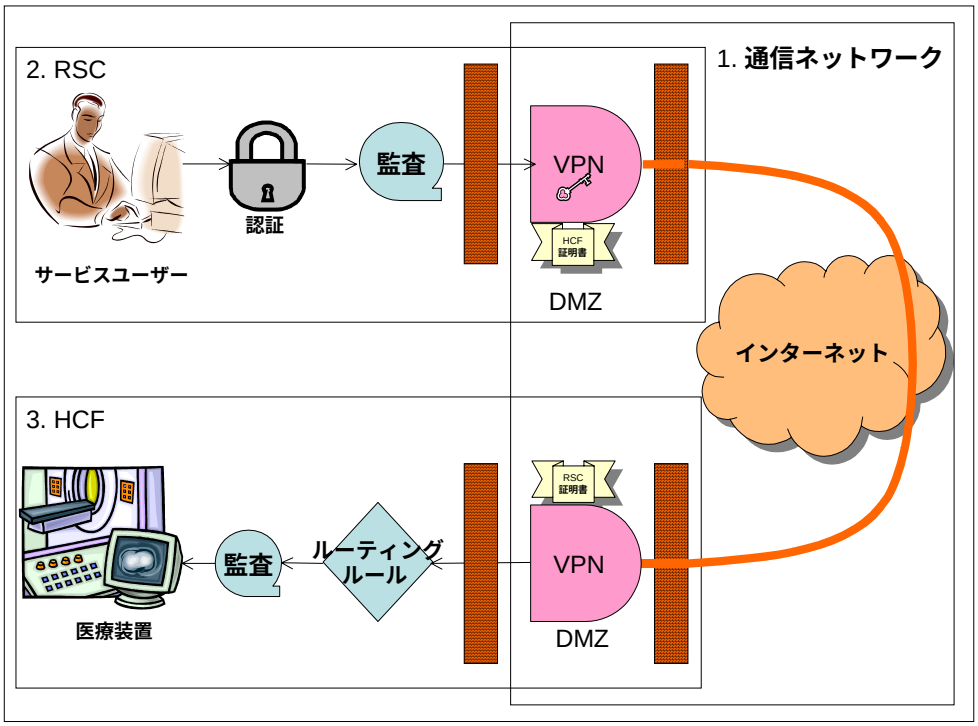

図 1: ベンダーの RSC と HCF の間の安全な接続のためのスキーマ

2.1 通信ネットワーク

ソリューション (A) では、RSC と HCF の間で使用されるネットワークはインターネットである。インターネットは公衆網なので、データを傍受されたり、ネットワーク上を移動中のデータを改竄されたりするリスクがある。

ソリューション (A) は、インターネット接続をすでに保有している施設を対象としている。このソリューションは、既存のインターネット接続に追加する必要のあるインフラストラクチャを最低限に抑えた、比較的低コストのものである。多くの HCF には、すでにインターネットインフラストラクチャがある。インターネット接続がなく、ソリューション (A) を利用したい施設に対しては、DSL やケーブルタイプのアクセスを通して利用できる低コストのインターネット接続ソリューションがある。

IP (インターネットプロトコル) には、インターネット (または他の安全でないネットワーク) 上を伝送されるデータを保護する機能が本来備わっていないので、RSC

と HCF の間の通信を保護するための構成要素の 1 つは、IPSec (IP Security) プロトコルを使用することである。IPSec プロトコルは、暗号セキュリティサービスを用いた安全なプライベート通信に対応している。

2.2 リモートサービスセンター (RSC)

RSC は、接続先の各医療施設の論理的な延長部分になるので、特に危害を加えられやすい場所である。したがって、ファイアウォール、侵入検出、アンチウイルス検出などの機能を使用して、RSC を十分に保護する必要がある。さらに、各ベンダーの技術者は RSC に対する認証を受け、そこでのすべての活動を追跡されなければならない。ソリューション (A) では、RSC およびネットワークアクセスポイントが責任を負うので、既存の医療装置を変更する必要はない。

以下の節では、サービス担当者の認証、アクセスポイントでのアクセス制御、および監査記録を通して、個々の責任追跡性が維持される仕組みの概要について説明する。

2.3 医療施設 (HCF)

HCF もまた、患者個人の身元がわかる大量のデータを処理および保管するので、非常に危害を受けやすい場所である。ソリューション (A) では、医療施設が必要な予防手段を講じて施設とネットワークを保護することが求められている。これには、ファイアウォール、侵入検出、部門分離、交換網、アンチウイルス技術などの要素が含まれる。インターネットアクセスは、許可されたユーザー、システム、およびプロトコルに制限されなければならない。個人の識別が可能な患者データへのアクセスを許可することの法的必要性、リスク、およびメリットを比較検討する最終的な責任は HCF にある。この基本的な責任は、世界中の行政規則によって強調されている。各地域の規則の例としては、米国の HIPAA、ヨーロッパの EC 95/46 とその各国固有の実施、および日本の HPB 517 などがある。

以下の節では、ソリューション (A) が成功するために必要なセキュリティとプライバシーの構成要素の概要について説明する。HCF 内のセキュリティについて詳細に考察するのではなく、リモートサービスの安全を確保するために不可欠な構成要素について考える。HCF は、示されているものより強力なセキュリティを実施してもかまわない。

3. 通信ネットワーク

この節では、RSC のインターネット接続ポイントと HCF のインターネット接続ポイントの間で VPN 接続を安全に確立して維持するために必要な接続コンポーネントについて説明する。

ソリューション (A) で提案されている通信ネットワークは、以下の機能を備えている。

- 証明書による強力な認証
- RSC と HCF の組み合わせごとに設定されるルーティングとフィルタリングのルールの形式でのアクセス制御
- 個別の責任追跡性の提供に利用できる、アクセスポイントにおける監査記録

3.1 IPSec (v4) を用いた VPN

IPSec プロトコルは、図 2 に示すように、インターネット上に仮想専用線 (VPN) をセットアップし、RSC と HCF に対するアクセスポイント間に暗号化されたトンネルを確立する機能を提供する。VPN は、一方の端の他の端に対する認証、データの完全性、データの機密性、VPN が搬送するトラフィックに対するリプレイ攻撃の防御を保証する。以下で説明するように構成した場合、IPSec はネットワーク層でトラフィックを保護し、サービスアプリケーションに対しては透過的に動作する。

以下は、IPSec を使用して VPN を確立するための、ハードウェア、ソフトウェア、および構成に関する要件である。IPSec ベンダー間の相互運用性に関するこれまでの問題を考えて、以下のオプションおよび機能のリストが推奨される。

1) すべての装置 (ハードウェアおよびソフトウェア) は、IPSec [RFC 2401] 対応の通信をサポートしなければならない。
2) IPSec の実装は、相互運用の可能性を高めるため、標準に準拠していることを ICSA Labs によって承認されなければならない。
3) 透過性と最大限の保護を実現するため、IPSec はトンネルモードで使用しなければならない。
4) AH (認証ヘッダー) [RFC 2402] は、認証、完全性、およびリプレイ防御を提供する。
5) ESP (暗号ペイロード) [RFC 2406] は、ペイロードまたはデータのレベルでの認証、機密性、完全性、およびリプレイ防御を提供する。
6) システムは、暗号化アルゴリズムおよび鍵の長さとして少なくとも 3DES (Triple Data Encryption Standard) [RFC 2405] を使用して構成されなければならない。
7) システムは、データ認証および完全性として少なくとも SHA-1 (Secure Hashing Algorithm 1) [RFC 2404] を使用して構成されなければならない。
8) IPSec Security Association (SA) 鍵は、24 時間ごと、またはデータ 1GB ごとに、ネゴシエーションし直さなければならない。

9) Perfect Forward Secrecy (PFS) を必ず実施しなければならない。
10) IKE (Internet Key Exchange) [RFC 2407、2409] は、AH と ESP に必要な認証鍵の通信をセットアップする。
11) メインモードを必ず使用しなければならない。アグレッシブモードを使用してはならない。
12) エッジ間認証は、1024 ビット RSA の公開鍵/秘密鍵を使用して実現される。
13) 公開鍵は、BER エンコード化 x.509 証明書 (後述参照) を使用するアウトオブバンド方式を通して配布される。

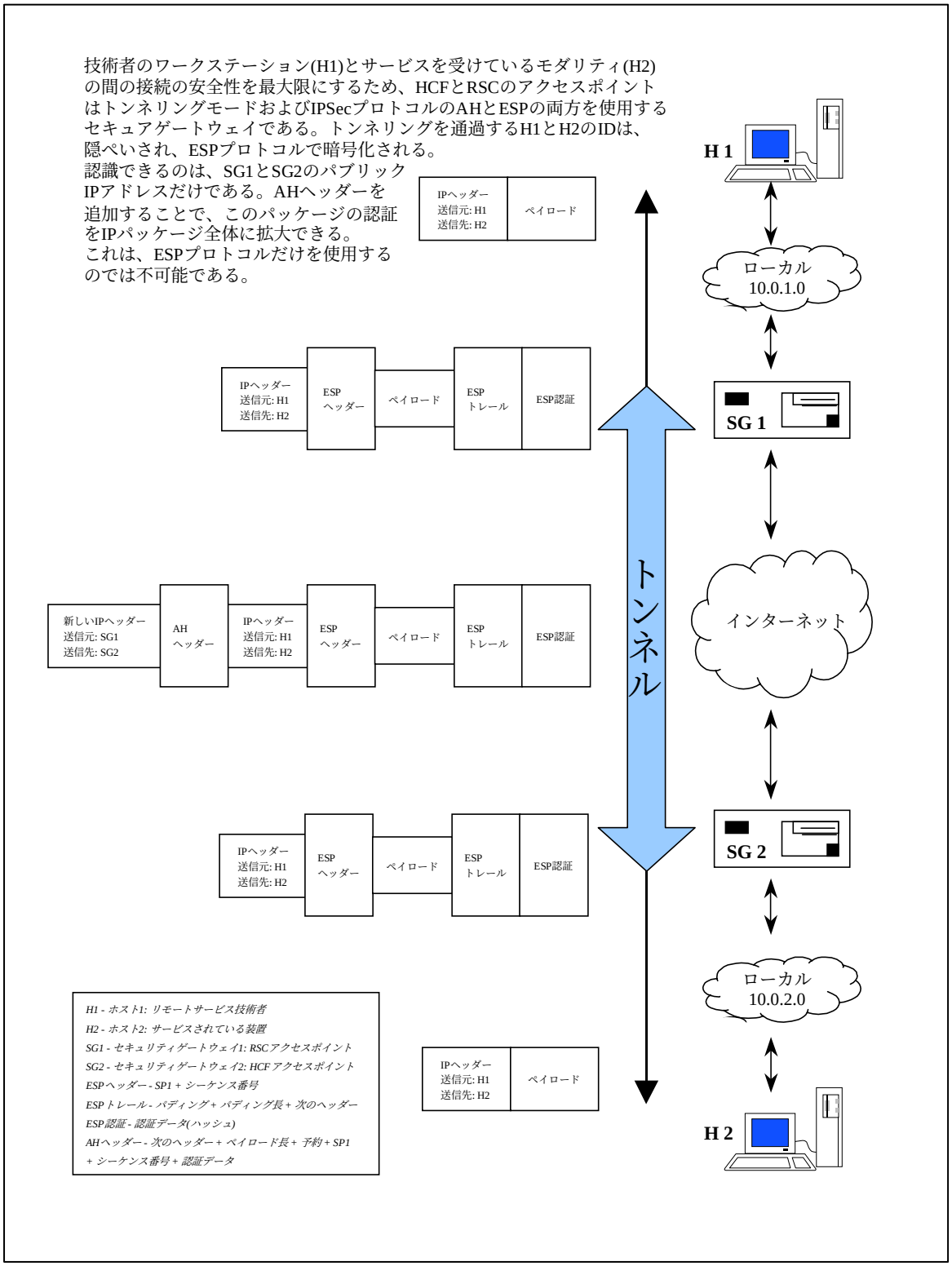
技術者のワークステーション(H1)とサービスを受けているモダリティ(H2)の間の接続の安全性を最大限にするため、HCFとRSCのアクセスポイントはトンネリングモードおよびIPSecプロトコルのAHとESPの両方を使用するセキュアゲートウェイである。トンネリングを通過するH1とH2のIDは、隠ぺいされ、ESPプロトコルで暗号化される。
認識できるのは、SG1とSG2のパブリックIPアドレスだけである。AHヘッダーを追加することで、このパッケージの認証をIPパッケージ全体に拡大できる。
これは、ESPプロトコルだけを使用するのでは不可能である。
IPヘッダー 送信元: H1 送信先: H2
ペイロード
H 1
ローカル 10.0.1.0
IPヘッダー 送信元: H1 送信先: H2
ESP ヘッダー
ペイロード
ESP トレール
ESP認証
SG 1
トンネル
新しいIPヘッダー 送信元: SG1 送信先: SG2
AH ヘッダー
IPヘッダー 送信元: H1 送信先: H2
ESP ヘッダー
ペイロード
ESP トレール
ESP認証
インターネット
IPヘッダー 送信元: H1 送信先: H2
ESP ヘッダー
ペイロード
ESP トレール
ESP認証
SG 2
ローカル 10.0.2.0
H1 - ホスト1: リモートサービス技術者
H2 - ホスト2: サービスされている装置
SG1 - セキュリティゲートウェイ1: RSCアクセスポイント
SG2 - セキュリティゲートウェイ2: HCFアクセスポイント
ESPヘッダー - SP1 + シーケンス番号
ESP トレール - パディング + パディング長 + 次のヘッダー
ESP認証 - 認証データ(ハッシュ)
AHヘッダー - 次のヘッダー + ペイロード長 + 予約 + SP1 + シーケンス番号 + 認証データ
IPヘッダー 送信元: H1 送信先: H2
ペイロード
H 2

図 2: IPSec の構成

3.2 トンネルを確立する際のアウトオブバンド証明書配信を用いた RSC と HCF の手動認証

RSC は、適切な HCF アクセスポイントと接続していることを極めて確実に認識しなければならない。同様に、HCF は適切なベンダーが認証を受けていることを認識しなければならない。このリモートサービスアーキテクチャを強力なものにしているのは、このような相互認証である。ただし、この強力な IPSec エッジ間認証は、接続の中で両方のアクセスポイントとインターネットの間の部分に限られる。RSC からサービスを受けている医療装置までの通信パス全体に認証能力を与えるために必要な拡張については、RSC と HCF の構成に関する節で説明する。

この提案では、強力な認証を実現するための手段として公開鍵/秘密鍵の技術の使用を選択している。認証機関 (Certificate Authority : CA) によって署名されたデジタル証明書を使用することで、秘密鍵の保有者を認証できる。したがって、秘密鍵は、鍵ペアの所有者に対して秘密でなければならない。秘密鍵は保護しなければならず、所有者に管理を任せてはならない。

多くの証明書配布方法が提案されているが、結局、その多くには相互運用性の問題がある。一部の施設は証明書機能を所有して独自の証明書生成方法を使用することを望み、他の施設は一般の認証機関 (CA) を使用するようになると思われる。

相互運用性の問題を避けるため、自動的ではない手段 (アウトオブバンド) で証明書を配布するよう提案する。HCF は、通信相手の各ベンダーに関連付けられた少数の証明書だけを必要とし、他の HCF の証明書は必要ないので、この方法は実現可能であると考えられる。また、各 RSC が必要とするのは、自分たちがサービスを行う各 HCF の証明書だけである。つまり、さまざまなサイトにおける鍵の数は百万単位ではなく百の単位であり、必要な証明書と鍵の数が少ないのでロジスティックや拡張性の問題は発生しないものと考えられる。したがって、このソリューションでは PKI を使用することも実装することもない。

このように、HCF と RSC は証明書の作成方法を自由に選択できる。署名機関としては、病院が管理する CA、ベンダーが管理する CA、または信頼できる第三者が考えられる。証明書の有効期間は 2 年以下でなければならない。

証明書は、その特定のエッジ間 VPN 接続のみに対する信頼できる証明書として配布および挿入される。IPSec の実装は、証明書チェーンまたは失効リストをチェックする必要はない。どちらの処理も、HCF と RSC の間の手動による"アウトオブバンド"の配布と通信によって行われる。鍵ペアが損傷したおそれがある場合は、手動で失効させ (アンインストール)、新しい鍵ペアを作成し、新しい証明書を発行して、インストールする。SPC は、VPN トンネル構成ごとに証明書を作成することを推奨する。

証明書を使用することの強みは、証明書自体を開示されないよう保護する必要はなく、証明書の信憑性は認証機関の証明書までつながっている信用のチェーンを通して証明できることである。証明書のこのような特性により、認証情報の配布に対して過剰な保護手段は必要ない。

ただし、公開鍵基盤 (PKI) は成熟した技術なので、認証は PKI を使用するさらに安全な方式へと発展する必要がある。

3.3 パフォーマンス要件

通信ネットワークは、128Kbps の定格スループットを提供する必要がある。パケットを暗号化する処理には時間がかかり、暗号化を待つ間に、伝送時間に未使用のギャップが発生する場合がある。さらに、暗号化されたデータは圧縮率が低いので、リンクレベルでの圧縮によるメリットが小さくなる。この要件では、帯域幅の保証は要求されていない。予想される多数の同時セッションをサポートするパフォーマンスのレベルを推奨するためのものである。

HCF は、RSC が IPSec の接続性をテストしてリンクを確立できることを確認しようとする場合があることを認識しておく必要がある。両当事者は、このようなイベントを調整して障害警報が発生しないようにする必要がある。これは、サービスを必要とするイベントが発生しても患者の安全に影響がないことを保証するための追加手段である。

3.4 アクセスポイントの構成

第 3 節でこれまで説明したように、RSC と HCF に対するアクセスポイントは VPN のエンドポイントである。VPN 自体は、リプレイ防止、サイトの相互認証、および送信されるメッセージの完全性と機密性の機能を備えている。セキュリティの侵害を防ぐためには、アクセスポイントを適切に構成する必要がある。両方のアクセスポイントにおいて同じ技術的手段を使用できる場合であっても、具体的な構成は、VPN によってもたらされるリスクの評価を行った後でないと定義できない。

このようなリスクの中でも、特に、偽装 (なりすまし、など) 攻撃、および VPN リンクを利用して他の施設に侵入する悪意を持った者について考える。この節では、アクセスポイントが必要なセキュリティ水準を保証するための最低限の要件について説明する。リスク評価の結果、他の技術的または手順的な要件が明らかになる場合がある。

また、VPNアクセスポイントのどちらかの側がトンネルを開始できることにも注意する必要がある。推奨される構成およびセキュリティ手段では、両当事者の合意に基づき、HCFまたはRSCのどちらかがトンネルを開始できる。

RSCは静的なグローバルIPアドレスを使用することが推奨される。HCFもVPN装置に静的グローバルIPアドレスを割り当てると多くのメリットがあるが、このソリューションは、ISPがHCFのVPN装置に動的にIPアドレスを割り当てる場合にのみ機能する。この場合は、HCFがRSCの対応するVPN装置の静的IPアドレスを認識してトンネルを開始し、デジタル証明書を使用して認証を行うことで、トンネルを安全に確立できる。

3.4.1 ファイアウォール、フィルタ、ルーティングルール

少なくとも、アクセスポイントはフィルタとルーティングルールを使用して、接続の試みを制限しなければならない。このようなルールは、ベンダーごとに異なってもかまわない。このようにすることで、HCF はベンダーごとにアクセスできる医療装置を制御でき、RSC は装置から送信されたメッセージの送り先を制御できる。

RSC と HCF のアクセスポイントはどちらも、固有のルーティングルールを使用して、自分のネットワーク内から送信されたパケットだけがアクセスポイントを通過するようにしなければならない。これにより、VPN を介した通信を制限し、ある HCF が共通の RSC を通して別の HCF にアクセスすること、またはその逆を防ぐ。また、不正なインターネットトラフィックが VPN を使用することを防ぐ。

アクセスポイントは、一次ファイアウォールの背後で、二次ファイアウォールの前面に構成することが強く推奨される。この位置は、一般に DMZ ("非武装地帯") と呼ばれる。DMZ を適切に構成すると、事前スクリーニングと事後スクリーニングによる縦深防御が実現され、セキュリティが強化される。一次ファイアウォールと二次ファイアウォールの実際の実装は、最適なソリューションの構成要素である。HCF には、選択した方法を使用して組織内のインターネットリスクを減少させる最終的な責任がある。

HCFには、論理的に切り離された (VLANなど)、または物理的に切り離された (大学のネットワークと病院など)、複数のネットワークが存在する場合があることに注意する必要がある。場合によっては、VPNアクセスポイントが、ベンダーの装置が存在するネットワークの近くに配置されることがある。つまり、放射線部門ネットワークなどの内部ネットワークの周辺に、VPN装置が実際に配置される場合がある。RSCのトンネルがHCFのDMZを通して内部のネットワークまでルーティングされ、そこでVPNトンネルが終了する可能性がある。そこから、トラフィックはサービスが必要な特定の装置までルーティングされる。すでに指摘したように、HCFアクセスポイントをどこに配置する場合であっても、アクセスポイントは一次ファイアウォールの背後で二次ファイアウォールの前面に置くことが推奨される。

3.4.2 ネットワークアドレス変換

今日のイントラネットでは、ネットワークアドレス変換 (NAT、RFC 1631) がごく一般的に使用されている。エッジ間認証はインターネットでルーティング可能な IP アドレスに対して行われるので、このホワイトペーパーで提案されている IPSec の構成は、NAT の影響が及ぶ範囲の外で終了する。この場合、NAT は、サービスを受ける医療装置までのアクセスパスに対応していなければならない。このような NAT ルールは、前述したように、IPSec 認証に固有であってもかまわない。

NATを使用することで、このソリューションはどのようなサイトでも動作するようになる。適切に実装されたNATルールは、すべてのサイトにおいて個々の装置を一意に識別できるだけでなく、RSCまたはHCFによって設けられているデフォルトのルーティングポリシーも扱うことができる。ただし、サービス対象装置に対してNATが正しく動作するためには、サービスを受けるHCFの装置に対して静的なIPアドレスを割り当てる必要があることに注意しなければならない。割り当てるIPアドレスはプライベートでもグローバルでもかまわないが、装置を起動/再ロードするたびに変化してはならない。

ほとんどのサイトでは、サーバータイプまたはネットワークタイプの装置には静的なIPアドレスを割り当て、エンドユーザーのパーソナルコンピュータ、ワークステーション、またはラップトップコンピュータに対してはDHCP (Dynamic Host Configuration Protocol) を使用できる。DHCPは装置に対してIPアドレスを動的に割り当てる手段であるが、これは、基本的に、装置を起動するたびにIPアドレスが異なることを意味する。また、DHCPはある装置に対するIPアドレスを確保しておくためにも使用できるが、これは静的なIPアドレスの割り当てと似ている。DHCPを使用して静的なIPアドレスを割り当てる場合は、このソリューションが機能する。DHCPが動的なIPアドレスを割り当てる場合には、このソリューションは面倒なものになる。NAT処理に関する以下の説明では、VPNトンネルを通してリモートでサービスを受ける装置には静的なIPアドレスが割り当てられているものとする。

3.4.2.1 プライベートアドレス指定でのNAT

多くのHCFはプライベートアドレス指定 [Address Allocation of Private Address Space, RFC-1918] を使用しており、プライベートアドレス指定は複数のサイトで使用できるので、異なるHCFが内部ネットワーク内で同じアドレス指定方式を使用している場合がある。その結果、異なるHCFにある装置に同じアドレスが割り当てられる可能性がある。正しいHCFと装置にルーティングしてサービスを行うためには、RSCは、すべてのHCFの個々の装置を一意に識別するために使用できるアドレスのブロックを管理する必要がある。このようなIPアドレスは、HCFにおいて使用されているものとは別のプライベートアドレス範囲でもかまわない。RSCがNATの割り当てを管理する場合には、RSCはHCFの個々の装置に対して正

しくルーティングできなければならない。特定の範囲のIPアドレスをVPNネットワーク経由でルーティングすることができ、安全ではないインターネットネットワークに至る異なるゲートウェイにルーティングしないようにするため、RSCにおいてルーティングルールの追加が必要になる場合がある。このようなIPアドレスのプライベートな範囲が、誤って安全ではないインターネットにルーティングされたとしても、オープンなインターネットネットワークを通してプライベートアドレスが正しくルーティングすることはできないので、リスクは最低限に抑えられる。データは単に破棄されるだけである。

3.4.2.2 NATとグローバルアドレス指定

一部のHCFでは、独自のグローバルIPアドレスを使用して各サーバータイプ装置に割り当てる場合がある。グローバルアドレスを使用すると、各装置は世界的に一意に識別される。グローバルアドレスは、それを所有するHCFまでインターネットを正しく移動できるので、RSCは、自分のネットワークにルーティングルールを入力し、RSCのVPNゲートウェイからHCFのVPNゲートウェイまでトラフィックをルーティングできる。その後、HCFのルーターは、このグローバルIPアドレスを使用して、RSCのサービス技術者を最終的な装置まで直接ルーティングできる。グローバルアドレスではNATは必要ないが、NATを使用した方がRSCにとっては簡単な場合がある。NATを使用すると、グローバルアドレス指定を使用するサイトに対するデフォルトゲートウェイに入力する必要のあるルーティングルールの値が簡単になる場合がある。さらに、VPN接続のセットアップに対して一貫性を維持するため、RSCがNATを引き続き使用することを望む場合がある。繰り返しになるが、HCFがネットワークでグローバルアドレスを使用する場合は、NATは必ずしも必要ないが、NATを使用すれば、RSCのネットワーク管理作業が簡単になる。

3.4.2.3 追加されるHCFセキュリティ管理機能

NATとグローバルアドレス指定方式またはプライベートアドレス指定方式を使用すると、HCFは新たなセキュリティ管理を実施できる。たとえば、1 対 1 のNATステートメントを設定すると、RSCからサービス対象の特定の装置に対する接続を制限できる。つまり、RSCの接続は、HCFのネットワークまたはサブネットの全体ではなく、対象の装置に限定される。また、HCFは、内部ファイアウォールで新たなセキュリティルールを実装してアクセスを制限したり、新たなポートやプロトコルフィルタリングを実装したりできる。

複数のRSCがソリューション (A) を使用して、すべてのHCFサイトにあるサービスの必要なすべての装置を一意に識別することで多数のHCFサイトに対応するには、ネットワークアドレス変換テーブルを適切に管理および保守する必要がある。また、あるRSCが別のRSCと同じ範囲のプライベートIPアドレスを使用して装置

を識別しないようにするためには、HCFはNATルールについて認識している必要がある。

4. リモートサービスセンター

ベンダーは、RSC-LAN を確実に管理および運用する最終的な責任を負っている。3.5 節では、RSC-LAN のすぐ外側で終了するアクセスポイントの構成について説明した。この節では、RSC-LAN においてソリューション (A) の確実な実装が保証されるために必要な作業と技術について指摘する。RSC に対しては、個別の状況に応じて、ここで示す推奨事項を満足できる水準まで拡張することが推奨される。

4.1 RSC の管理

RSC には、自分の VPN アクセスポイントと LAN を適切に管理してその完全性を保証する責任がある。この責任は、米国内の HCF と接続する際には HIPAA 法において要求される Business Associate Agreements により、他の国では HCF とベンダーの間に要求または推奨されるその国固有の取り決めにより、いっそう大きくなる。このような取り決めでは、HCF は、通常、個人の識別が可能な患者データの取り扱いに関する具体的なルールを示す。このような要因は、RSC が独自のリスク評価を行う契機となる。考慮する必要のあるその他の問題としては、たとえば、リスク緩和計画、監査やユーザーアクセス管理に対する規定を含む内部セキュリティポリシー、要員のトレーニングなどがある。

アクセスポイントの構成を変更するときは、HCF との連絡 (おそらくはアウトオブバンドでの) に注意する必要がある。構成の変更を行おうとするときに VPN リンクにアクティブなセッションが存在しないようにし、承認された変更を同期をとって行うようにするには、この連絡が非常に重要である。RSC は、HCF の権限を持つ者だけが変更を要求できるよう、ポリシーを作成し、手順に従う必要がある。

常に可能な限り患者のデータから個人が識別されないようにしなければならないが、個人が識別されないようあらゆる努力を払っても、データの中にまだ識別情報が残る場合がある。RSC は、個人識別情報を排除されたデータについても取り扱い方針を作成する必要があり、その中ではデータの保管、処理、追跡、および最終的な破棄の方法について規定しなければならない。

4.2 技術的手段

4.2.1 RSC のネットワークアーキテクチャ

RSC のネットワークは、前述したようにインターネットから切り離すだけでなく、ベンダー自身のイントラネットからも切り離して、患者の識別可能なデータが許可なく開示されるリスクを最低限にしなければならない。

RSC は、インターネットおよびベンダーのイントラネットから RSC を分離する内部セキュリティシステムを実装する必要がある。

4.2.2 責任追跡性の保護

対象 HCF に対する VPN にアクセスする前に、各個別 RSC ユーザーの ID と認証およびすべての活動を追跡する監査記録を通して、技術者個人の責任追跡性を RSC において維持しなければならない。
以下の推奨事項を RSC において実現する必要がある。

- RSC は、セッションに関係する各サービス担当者を識別しなければならない。
- VPN に対するアクセスを含むすべての RSC リソースを使用する前に、提示された各 RSC ユーザーの ID を認証しなければならない。
- RSC は、サービスのためのアクセスと行動を追跡するログファイルを保持しなければならない (6.3 節で詳しく説明)。
- RSC のすべてのリソースに対するアクセスは、担当者が変わったなら (再割り当て、終了など)、直ちに取り消されなければならない。
- サービスを受けているシステムから別のシステムへの HCF の承認を受けない移動は、ポリシーと手順により管理されなければならない。
- RSC の文書化されたポリシーでは、HCF の要求 (サービス要求、証明書管理、パスワード変更など) を認証するために使用する方法が指定されていなければならない。

4.2.3 個人識別可能な患者データの取り扱い

個人を識別できる患者データの HCF からの取得について、RSC を制限するためのあらゆる処置が行われなければならない。サービス作業を行うために、患者の識別可能なデータを取得することが必要になる場合がある。この処理は、各地域の規則に従って行われなければならない。このデータを VPN を通して取得する場合は、HCF と RSC の間の契約による合意に従って、注意深く管理されなければならない。

4.2.4 RSC をバイパスするリモート接続の禁止

すべてのサポート担当者は、RSC によって設定されたセキュリティアーキテクチャとインフラストラクチャを使用して、HCF にリモートで接続しなければならない。これは、サポート担当者の PC から HCF への直接リモート接続を可能にすることで、監査記録、認証、ファイアウォール保護、およびこのホワイトペーパーで説明されているすべての構成要素をバイパスできないようにするためである。

5. 医療施設

HCF は、患者の個人識別が可能なデータのセキュリティとプライバシーに対して、最終的な責任を負う。そのため、各施設は、リスク評価を行い、セキュリティとプライバシーに関する施設固有のポリシーと手順を作成する必要がある。HCF が、このような評価を実施しなければならない。この節は、そのような作業の代わりになるものではない。ただし、手順を作成する必要のある場所を指摘し、ソリューション (A) の実装を成功させるために必要な技術について説明する。HCF に対しては、以下の推奨事項を満足できる状態になるまで変更することが推奨される。

VPN アクセスポイントの完全性を管理して保証することは、HCF の責任である。第 3 節では、アクセスポイントの構成について説明した。HCF の判断によっては、この作業をアウトソーイングしてもかまわない。RSC の観点から前述したように、アクセスポイントの構成を変更するときは、事前に RSC と連絡を取ることが重要である。構成を変更しようとするときに VPN リンクにアクティブなセッションが存在しないようにし、合意された手順に従って承認された変更を同期をとって行うようにするには、この連絡が非常に重要である。

ソリューション (A) は安全な環境に依存する。VPN が接続される HCF のイントラネットは、ファイアウォール、侵入検出、アンチウイルス管理などを使用して、セキュリティの脆弱性から適切に保護しなければならない。さらに、HCF のネットワークアーキテクチャは、伝送するデータの完全性を保証し、リソースに対するアクセスを管理し、トラフィックの機密性を保護する必要がある。このホワイトペーパーで説明されているアーキテクチャでは、イントラネットの暗号化は提案もしくは要求されていないことに注意すること。

サービスを受ける医療装置は、病院ネットワーク経由でのリモートアクセスをサポートしなければならない。また、IPSec トンネルにアクセスし、それを通して通信できる必要がある。装置が病院のネットワークに接続されていない場合は、このホワイトペーパーで説明するソリューションを使用してリモートサービスを行うことはできない。

6. 監査記録

監査記録は、個人の責任追跡性の重要な構成要素である。個人識別が可能な患者データが存在する可能性のある装置のサービスにおいて実行されたアクションは、監査の記録を用いることで、特定の RSC の特定の個人まで追跡できる。SPC リモートサービスインターフェイスアーキテクチャの目的は、サービスを受ける装置に対して新たな要件を課すことなく、このような責任追跡性を提供することである。これは、必要な責任追跡性を提供しながら現在の装置に対する HCF の投資を保護するので、このアーキテクチャの成功にとって重要な要素である。

すべての監査ログエントリには、日付と、少なくとも 1 秒の精度のタイムスタンプが記録されなければならない。異なる場所にある異なるシステムでログファイルが作成されていてもログファイルを証拠としての能力を持つものにするためには、正確なタイムスタンプが重要である。このホワイトペーパーでは、ログファイルのフォーマット、保存、通信、またはアクセスについては言及されていない。この種の問題については、SPC、IHE、HL7、DICOMなどの他の業界および標準化グループが作業している。医療画像における監査については、SPCの文書「Security And Privacy Auditing In Health Care Information Technology」を参照されたい。

6.1 医療装置

既存の医療装置に対する新しい要件はない。監査ログ機能は、その医療装置に対する本来の規定に従って使用する必要がある。

6.2 アクセスポイント

このホワイトペーパーでは、アクセスポイント自体に対する具体的な要件は規定されていない。RSC または HCF では、アクセスポイントが備えている監査機能を必要に応じて使用する必要がある。

6.3 RSC

RSC では、HCF およびその個人識別が可能な患者データに対するアクセスに関するサービス担当者の行動を追跡する監査ログを保持しなければならない。この監査ログは、妥当な範囲で可能な限り具体的でなければならず、以下の情報が含まれていなければならない。

- サービスユーザー個人の ID
- 医療装置の IP アドレスとポート番号 (または NAT で変換されたアドレス)
- 接続および切断の日付と時刻
- 実行された作業の記述 (アクセスとアクションなど) (手動の場合がある)
- アクセスの試みの成功または失敗

7. 結論

これは、SPC リモートサービスインターフェイスのホワイトペーパーに準拠する実現可能な複数のソリューションの中の、妥当な 1 つのソリューションである。これは単なる技術ソリューションではないということを理解することが非常に重要である。本当に安全なリモートサービス機能を実現するためには、HCF と RSC は、指摘されているように技術を実装すると共に、ポリシーと手順を変更する必要がある。

複数のモデム接続ではなく単一のアクセスポイントに集中することで、内部ネットワークに対する HCF の制御が強化される。

8. 用語集

- 3DES ― Triple Data Encryption Method [RFC 2405] は暗号化を提供する。
- アクセスポイント ― IPSec VPN を実装するために使用されるハードウェアとソフトウェアの論理的な組み合わせ。
- アグレッシブモード ― 2 つのメインモード交換を組み合わせた鍵交換の IKE 方式。IPSec の実装ではアグレッシブモードはオプションである。
- AH ― Authentication Header (認証ヘッダー) [RFC 2402]。
- BER ― Basic Encoding Rules (基本符号化ルール) (ASN.1)。
- CA ― Certificate Authority (認証機関)。証明書の妥当性に関する相互に合意された機関。
- 証明書 ― デジタル証明書。
- COCIR ― European Coordination Committee of the Radiological and Electro-Medical Industry。ヨーロッパの画像装置ベンダーを代表する。
- 装置 ― リモートでサービスを受ける HCF の製品を定義するために使用される一般的な用語。
- **DHCP ― Dynamic Host Configuration Protocol (動的ホスト構成プロトコル)。装置にIPアドレスを割り当てるために使用されるプロトコル。**
- デジタル証明書 ― CA によって署名された暗号公開鍵。
- DMZ ― DeMilitarized Zone (非武装地帯)。敵対する勢力の間の地域を示す軍事用語からの流用。内部ファイアウォールと外部ファイアウォールの間に存在するネットワークで、リソースに対する管理されたアクセスを可能にするためにソフトウェアとハードウェアが配置される。
- ESP ― Encapsulated Security Payload (暗号ペイロード) [RFC 2406]。
- ファイアウォール ― 接続のスクリーニングのためのルーティングとフィルタリングを行うネットワーク装置。パケットの検査を行う場合もある。
- **グローバルアドレス ― インターネットでルーティング可能なアドレス。インターネット上のノードを一意に識別するIPアドレス。**
- HCF ― Health Care Facility (医療施設)。
- HIPAA ― 米国の法律。Health Insurance Portability and Accountability Act。
- IKE ― 以前の ISAKMP。Internet Key Exchange (インターネット鍵交換) [RFC 2407, 2409]。IPSec セッションを開始するために使用される認証とネゴシエーションのプロトコル。
- IPSec ― Internet Protocol Security (インターネットプロトコルセキュリティ) [RFC 2401]。
- **ISP ― Internet Service Provider (インターネットサービスプロバイダ)。インターネットへのアクセスを提供する会社。**
- JIRA ― Japan Industries Association of Radiological Systems (日本画像医療システム工業会)。日本の医療画像システムベンダーのグループ。
- メインモード ― IPSec の実装に必要な鍵交換の IKE 方式。
- NAT ― Network Address Translation (ネットワークアドレス変換) **[RFC 1631]**。

- ❖ **1 対 1 NAT ― あるIPアドレスを別の特定のIPアドレスに変換するためのマッピングの方式。**

- NEMA ― National Electrical Manufactures Association (北米電子機器工業会)。
- NEMA MII ― NEMA の Medical Imaging Informatics Section (医療画像情報セクション)。
- PFS ― Perfect Forward Secrecy。特定の IPSec SA の鍵が他の秘密鍵から生成されなかったことを保証する。
- PHI ― Protected Health Information。この文書では、一般に、保護された医療情報の任意の形式を指して使用される。
- PKI ― Public/Private Key Infrastructure (公開/秘密鍵基盤)。
- Preshared Key (事前共有鍵) ― セッションを開始するために IPSec によって手動で共有および使用される対称暗号鍵。
- **プライベートアドレス [RFC 1918] ― プライベートインターネット (LAN) で使用するために予約されているアドレスのブロック。**
- RSC ― Remote Service Center (リモートサービスセンター)。
- SA ― Security Association。IPSec 装置間で定期的に自動的にネゴシエートされるプロトコルと鍵のセット。
- SHA-1 ― Secure Hashing Algorithm 1 [RFC 2404]。データの認証と完全性を実現する。
- SPC ― Joint NEMA/COCIR/JIRA Security and Privacy Committee。
- ベンダー― リモートサービス機能を提供する医療装置の製造者。
- VPN ― Virtual Private Network (仮想専用線)。

9. 付録

この節では、いくつかの一般的な問題領域について指摘する。IPSec VPN、ファイアウォール、NAT、および DHCP を用いた医療装置のリモートサービスは、非常に複雑な構成である。これらの要素をすべて適切に構成すれば、ソリューションは機能する。以下で示す問題は、構成を誤る可能性のある一般的な領域である。

9.1 ドメイン名ルックアップ

リモートサービスは、RSC センターから HCF 内の医療装置に対して行われる。RSC の担当者は、医療装置のアドレスを正しく指定し、ネットワークインフラストラクチャにホスト名を解決させることができなければならない。

9.2 Dynamic Host Configuration Protocol (DHCP)

DHCP のようなプロトコルを使用する動的な IP アドレス割り当てを使用するのが一般的な方法である。この種の動的な割り当てでは、RSC が装置にアクセスできるようにすることが重要である。DHCP サーバーでは、NAT システムを適切に通知および更新する必要がある。適切に構成できるなら、DHCP を使用してもかまわない。

9.3 ネットワークアドレス変換 (NAT)

HCF がネットワーク内にネットワークアドレス変換 (NAT) を実装する場合は、リモートでサービスを受ける必要のあるすべての医療装置は、IPSec VPN に対して公開される NAT 変換を持つ必要がある。ネットワークインフラストラクチャ (代表的なものは DMZ) は、公開される NAT 変換が IPSec VPN だけに制限され、外部のファイアウォールを通してはアクセスできないことを保証できる。両側から IPSec VPN を通して使用されるすべての IP アドレスは、インターネットでルーティング可能なアドレスでなければならない。NAT 変換は、IPSec VPN の外側で行われなければならない。

9.4 リスクの軽減

ソリューション (A) によってリスクは十分に軽減されると考えられるが、リスクを軽減する方法を完全に公表する。

- PKI はまだ成熟していないため、相互運用性の問題が発生する可能性がある。
  - ❖ アウトオブバンド証明書配布を使用することで、この問題を軽減しようとしている。
- 特定のサービス担当者の認証は、RSC で行う。
  - ❖ 病院は、事後処理のために監査記録にアクセスできる。
- このソリューションでは、インターネット接続が必要である。
  - ❖ フレームリレー、ISDN、ケーブルモデムなどを利用する手頃なインターネットソリューションがある。HCF がこのリスクを受け入れる

場合は、ルータールールとフィルタリングを利用して、説明されているファイアウォール保護を実装できる。

- SCP のホワイトペーパー「Security and Privacy Requirements for Remote Servicing」では、手動切断の必要性が示されている。この概念を利用すれば、病院のスタッフはリモートサービスのセッションをリアルタイムで監視し、不審なセッションを終了させることができる。
    - ❖ このソリューションは、このような要件を支援または妨害するものではない。ネットワークトラフィックを監視することはできるが、プライバシーに関する決定を下すための適当なユーザーインターフェイスはない。