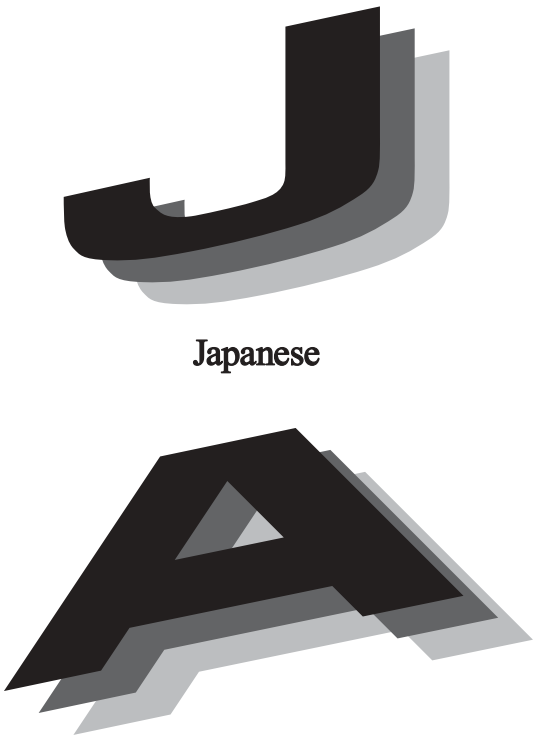
技術文書 04-101



リモートサービス セキュリティガイド

2004年 3 月
(社) 日本画像医療システム工業会
セキュリティ委員会
保健医療福祉情報システム工業会
セキュリティ委員会

はじめに

医療分野の IT 化が、ネットワークを介した医療情報のやりとりを可能にし、シームレスな医療環境が実現できるようになりました。例えば、医療施設間連携であり、医療機関の内部に保存されている診療情報を外部の医療機関で参照し、継続的な診療を実現するものです。遠隔医療もこの一種です。

また、医療機関外とのネットワーク化により、医療機関内の機器やシステムと保守サービスベンダとをネットワークで結び、保守管理サービスを遠隔で行うことも可能となりました。この遠隔保守（以下「リモートサービス」）により医療機関における機器およびシステムは、故障時などのダウンタイム短縮など、より円滑な運用が可能となります。

ただし、ネットワーク化で利便性が高まるとともに、外部の悪意を持った存在による個人情報の大量持出しや、医療システムの運用妨害などのリスクも高まりました。これらのリスクから個人情報や機器を保護することがネットワークセキュリティです。個人情報保護法も成立し、医療機関、ベンダともネットワークセキュリティに関する関心が向上しています。

本ガイドは、以上のような状況を踏まえ、ネットワークを介したリモートサービスを題材に、医療機関の機器およびシステム内に有する個人情報を保護するためのリスク分析・管理手法の説明、そして技術的および運用的セキュリティ対策について以下の順に述べています。

１）医療分野におけるリモートサービスの概要、セキュリティ対策の必要性
２）一般的なリモートサービスの運用モデルの提示と、それに基づいたリスク分析
３）それらのリスクに対する技術的および運用的セキュリティ対策例の紹介
４）リモートサービスに関するセキュリティ運用・マネジメントのポイント

本ガイドは、単にリモートサービス導入の際に留まらず、医療機関、ベンダそれぞれにおけるセキュリティ対策立案時に参考として頂くことを目的としています。少しでもお役に立てば幸いです。

２００４年3月
リモートサービスセキュリティWG

(社)日本画像医療システム工業会
セキュリティ委員会
保健医療福祉情報システム工業会
セキュリティ委員会

目　次

第１章　医療分野におけるリモートサービス

１－１．リモートサービスの概要

最近の各種検査装置、各種情報システムは自己診断機能を有しており障害の早期発見、鑑別などにも有用な情報を提供しています。更に、通信機能を持つ装置・システムも増え、自己診断機能の有用性を高めたり、様々な利便性を提供したりできるようになりました。以下、これらの機能を利用して行なわれるリモートサービスの具体例についてご紹介します。

（１）障害対応

医療機関のユーザが装置･システムに異常を発見してベンダのサポート窓口に連絡した時や、自己診断機能で異常がベンダのサポート窓口に自動通知された時などにリモートサービスを用いると、サポート担当者が直接対象装置・システムへネットワーク接続をして、短時間で現象を正確に確認し異常箇所を絞り込むことが可能となります。ハードウェア障害であれば何らかの現地作業が必要となりますが、ハードウェア的な問題でなければ直接復旧させることが可能な場合もあります。

（２）予防保守

装置・システムの自己診断機能を定期的に動作させることにより、機能の一部または全体が使えなくなる重大な障害を引き起こすような徴候を、事前に検出できることがあります。異常が検出された場合には、その記録を装置・システムの内部に蓄積しますが、リモートサービスを使うとベンダサポート窓口から定期的に自己診断機能の記録を確認したり、装置の自動メール発信機能等を用いてベンダのサポート窓口に直接伝えたりすることが可能となります。

（３）ソフトウェア改訂

異常の原因がソフトウェアである場合や、あるいは特に異常はなくても何等かの機能向上でソフトウェアを更新する必要がある場合は、リモートサービスによって遠隔地から直接改訂・更新作業を行うことが可能です。

１－２．リモートサービスの必要性

医療機関側もベンダ側もリモートサービスにより様々なメリットを得ることができます。以下、具体例を示します。

（１）ダウンタイムの大幅短縮

リモートサービスを用いない場合は、ベンダから派遣された現地保守サービス員は現象の詳細把握を行い、場合によっては採取した情報を持ち帰り、その上で必要な部品を入手して改めて現地に赴くことになります。リモートサービスを用いた場合は、あらかじめ異常個所の特定、対応策を検討してから現地保守サービス員を派遣することができるので、能率的で、ダウンタイムも大幅に短縮することができます。

（２）障害を予防することも可能

自己診断機能などにより装置やシステム自体で、稼働状態をモニタし、定期的に交換が必要な部品の交換時期を知らせたり、故障につながる微細な異常を早期に把握し、診療時間外にメンテナンスをしたりできます。

（３）保守費用の大幅低減

以上のように、ベンダからの保守サービス員が実際に医療機関に出向く頻度が大幅に減るため、また、ベンダのサービス拠点を集約することが可能となるため、保守サービスを実現するための費用が低減でき、結果的に医療機関が支払う保守契約費用の低減に通じます。

（４）現場職員の対応も低減

障害によるダウンタイムが大幅に短縮されることで、医療機関側の手間も減ることになります。

以上のように、リモートサービスには様々なメリットがあり、医療サービスの安定した提供のために重要な機能です。

１－３．本ガイドの対象範囲

本ガイドは、リモートサービスが実運用されるとき、ベンダのリモートサービスセンタから医療施設内に設置された保守対象機器にアクセスすることにより発生する個人情報に対する脅威の可能性を、許容できるレベル内に維持するためのセキュリティに関するガイドです。リモートサービスによる個人情報に対する脅威の事例を図１－１に示しました。個人情報に対する脅威は、大きく 3 つに分類することができます。１つ目は、リモートサービスセンタ内の端末からリモートサービス対象機器に至る通信経路上を流れる個人情報に対する脅威です。2 つ目は、リモートサービスセンタ内で参照・保存・印刷される個人情報に対する脅威です。3 つ目は、保守対象機器で参照･保存される個人情報に対する脅威です。

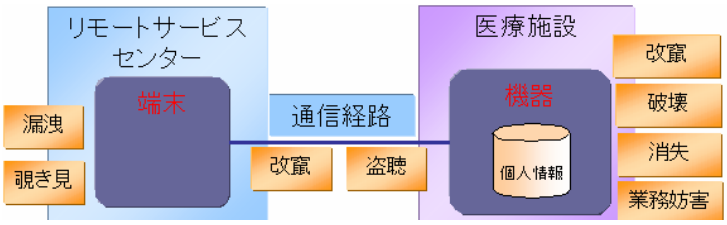


図１－１　リモートサービスにおける個人情報に対する脅威

本ガイドでは、これらの 3 種類の脅威に対して個人情報を保護するための技術的および運用的セキュリティ対策の具体的な要件について述べます。ただし、保守対象機器の個人情報保護については、リモートサービスセンタから遠隔操作することにより発生する可能性のある脅威のみを対象としています。つまり、保守対象機器上で、医療機関の職員やベンダの保守サービス員等が操作することにより発生する可能性のある脅威は本ガイドの対象外としています。また、通信経路としては、リモートサービスセンタと医療施設が ISDN 回線等を経由して直接接続するような場合だけでなく、インターネットなどのパブリックネットワークを経由してリモートサービスセンタと医療施設が接続するような場合も想定しています。ただし、通信経路に関しては、特定の通信方式を想定するのではなく、あくまで一般的な概念として検討しています。ISDN 回線、公衆電話回線、専用線、CATV 回線、といった物理的な通信手段に固有な問題については言及しません。

個人情報保護法の考え方には、リモートサービスにおいても医療機関の個人情報を保護する最終責任者は医療機関であり、医療機関は、その医療機関にリモートサービスを提供する全てのベンダに対して、リモートサービスによりその医療機関の個人情報が危険にさらされるリスクが、許容できるレベル内に維持できていることを確認・点検する義務を有している、という趣旨が見受けられます。そこで、本ガイドは、個人情報を保護するために適切な情報セキュリティマネジメントを行う医療機関とベンダを対象として、情報セキュリティマネジメントを発展させることに主眼を置いています。

１－４．略語集

以下に本ガイドで登場する略語の意味を紹介します。（一部、日本語がないものも含む）

COCIR:the European Coordination Committee of the Radiological and Electromedical Industry、欧州放射線医用電子機器産業連合会

HIPAA: The Health Insurance Portability and Accountability Act、医療保険の携行と責任に関する法律

HCF : Health Care Facility、医療機関(施設)

JAHIS:Japanese Association of Healthcare Information Systems Industry、保健医療福祉情報システム工業会 (http://www.jahis.jp)

JIRA:Japan Industries Association of Radiological Systems、日本画像医療システム工業会（http://www.jira-net.or.jp）

NEMA: National Electrical Manufacturers Association、 米国電子機器工業会

PHI : Protected Healthcare Information、保護対象の医療情報

RSC: Remote Service Center、リモートサービスセンタ

SPC : Security & Privacy Committee　NEMA,COCIR,JIRA の合同ワーキンググループ。セキュリティとプライバシ保護に関するガイドラインの検討を行なっている。

VPN: Virtual Private Network、仮想的な専用通信回線

第２章　リモートサービスセキュリティの課題

２－１．個人情報保護とリモートサービス

（１）医療機関における個人情報保護

個人情報保護法の成立により、日本においてもプライバシ保護について、医師による守秘義務という専門家による守秘から、患者本人による情報のコントロール権の確立の時代に移行しつつあります。医療機関においては個人情報について、管理の徹底、患者に対する漏洩リスクの説明、目的外使用を行なわないことの徹底を行うことが必要になってきています。「保健医療分野の情報化にむけてのグランドデザイン」の第一次提言においては、医療分野における個人情報保護に関し以下のように述べています。

「情報セキュリティおよび個人情報保護は、保健医療分野のみの問題ではなく、高度情報通信社会における共通の社会基盤である。従って、保健医療分野における対応は、e-Japan 重点計画に記載された施策に加えて、保健医療分野の特殊性を配慮して対策をたてる必要がある。」

医療情報は個人情報の中でも特に重要な情報であるため、その取扱は慎重かつ確実でなければなりません。

（２）個人情報保護の責任と対策

米国の HIPAA 法では、医療機関における情報管理責任者を置くことが義務付けられ、医療機関から個人情報が漏洩した場合、理由のいかんにかかわらず、医療機関の責任となるよう定めています。日本においても医療分野における個人情報保護のガイドラインが策定され、医療機関の責任者は個人情報保護について自らの責任において実施することが義務付けられることとなります。そのため、医療機関自らがきちんとした情報管理を実施しなければなりません。

しかし、日本においては、医療機関の情報管理について医療機器や医療情報システムの納入ベンダに任せきりの事例がみられます。医療機関が自ら情報管理を行なうという観点からみれば、医療機関の責任者にとっては、ベンダに任せきりにしたがために適切な危機管理を行うことが困難になる可能性があります。また、ベンダにとっても本来医療機関が負うべき管理責任を負うこととなり、情報漏洩などの事故が生じた場合の責任の所在が問題になる恐れもあります。こういった状況を打開するために、個人情報保護法の成立を機会として医療機関主体の情報管理体制への見なおしを実施するのが望ましいと考えられます。

（３）個人情報保護とリモートサービスの両立のために

前節で述べたとおり、個人情報を適切に守るためには医療機関は医療機関の責任において、セキュリティ対策を実施する必要があります。

現在の多くの医療機関において実施されているのは、院内における管理規定を定め、適切な管理を実施する運用的対策と、情報システムにセキュリティ対策を施し、個人情報を守

る技術的対策です。特にネットワークセキュリティ対策においては、多くの医療機関において、「外部ネットワークとの接続を許可しない」「VPN を利用する」などの対策が施され、外部のクラッカーなどがインターネット経由では侵入できないように工夫しています。しかしそれら対策を施し、外部からの侵入対策は完璧に近いと言われている医療機関においても唯一、外部からのアクセスを許すルートが存在します。それがリモートサービス用回線です。

リモートサービス回線経由でシステムベンダの保守要員がシステムにアクセスできることは、迅速な機能回復のために必要なこととして認められてきました。医療機関、ベンダの双方にメリットがあるリモートサービスは、個人情報保護法が成立し、医療分野における個人情報保護のガイドラインが提示された以降も必要なサービスであることに疑いはありません。医療機関は、自らの責任で安心してリモートサービスを利用できるようにするために、リモートサービスについて正しく理解し、適切な契約、技術的なセキュリティ対策、運用上の対策などを実施する必要があります。医療機関とリモートサービスを行うベンダのそれぞれの責任の明確化や、個人情報保護法の遵守のために、より安全な仕組みを構築することが重要です。医療機関、ベンダの双方がそれぞれの守るべき義務を正しく認識し、合意の下に適切なリモートサービスを行うことが望まれます。

２－２．リモートサービスにおけるセキュリティの現状

現在のリモートサービスにおいては、個別の公衆回線を利用したダイアルアップによるリモートアクセスを利用しているケースが大半だと考えられます。しかし最近では、安価なADSL 回線等ブロードバンドを利用してインターネット接続を行うことが広く普及してきており、リモートサービスも今後はこの形態が増えてくると予想されます。各ベンダが提供するリモートサービスの形態と、そのセキュリティ対策の現状を紹介します。

（１）リモートサービスの形態と技術的なセキュリティ対策

（A）公衆交換網接続を利用したリモートサービス

HCF 側では、ダイアルアップサーバ機能を提供する専用機等を設置します。この機器はモデム・TA 等によって公衆交換網と接続し、RSC 側リモート端末からのアクセスを待ちます。ISDN ダイアルアップルータのように、１台ですべての機能を行う通信機器もよく利用されています。

公衆交換網接続を利用する上では、通信回線に以下の特徴があります。

・ HCF と RSC との間の１対１での通信路が確保できる
・ ISDN の場合、フルデジタル化された交換網接続であるため盗聴が困難である

これらの特徴を生かし、技術的な以下の対策によりセキュリティの確保を行っているのが現状です。

（ア） 発信者番号の固定
　　コールバック認証もしくは発信者番号指定認証機能の利用
（イ） ユーザ認証
　　ワンタイムパスワードやパスワードの暗号化の利用
（ウ） 通信ログの確認
　　不正アクセスの有無の確認

（B）インターネット接続を利用したリモートサービス

HCF 側においては、固定グローバル IP アドレスを使用したインターネット常時接続環境を提供する専用機を設置します。RSC 側では、インターネット接続環境を用意し、インターネットを介して HCF 側と接続します。これは通常のインターネット接続時と同様であり、公衆交換網接続のような１対１対応の通信でないため、HCF と RSC 間の通信やユーザ認証方式にはさらに多くの技術が利用されています。以下に例をあげます。

（ア） ファイヤウォールの設置
（イ） ウィルスチェックツール等の利用
（ウ） VPN を利用した通信
　　通信経路の暗号化
（エ） さまざまなユーザ認証の利用
　　ワンタイムパスワードやパスワードの暗号化の利用
　　デジタル証明書の利用、等

（２）リモートサービス運用におけるセキュリティ対策

各ベンダは、個人情報の保護やシステムの安全な運用を行うために、運用規定を設けているのが一般的です。以下にその規定の例を挙げます。

（ア） RSC 操作要員に関する規定
（イ） RSC リモート端末を許可された要員以外に操作されないような対策規定
（ウ） RSC リモート端末が増設・移動される場合の規定
（エ） モバイルからのアクセスに関する規定

（３）HCF 側と RCF 側との契約

万一の事故等への対応として、以下の規定を設けている場合があります。

（ア） HCF と RSC との責任範囲の規定
（イ） 守秘義務に関する契約の締結

以上のように、リモートサービスにおけるセキュリティ対策には色々な手段があります。各ベンダは独自の規定によりこれらの手段を用いて、セキュリティの確保を行っているのが現状です。しかし、ベンダによりその方法が異なるため、HCF 側ではセキュリティのための必要経費が今後増大していくことと同時にそのセキュリティレベルを一定以上に維持することがさらに難しくなっていくことが予想されます。

２－３．セキュリティ対策の現状における問題

リモートサービスにおけるセキュリティ対策の現在の実施状況を省みると、いくつかの問題点が挙げられます。

第一に、現状では各社のリモートサービスにおいて、RSC から HCF までのネットワーク経路、リモート接続のためのハードウェアの種類およびアクセス手順、サービスを行なうツール、セキュリティポリシ、運用規程等が異なっている（ほぼ同じでも内容が開示されていないため同等に扱えない）ところが問題です。そのため、HCF 側では RSC ごとにアクセスポイントを準備する必要があり、設備費、維持管理といった手間が膨大になってしまいます。またアクセスポイントが多いということは、セキュリティホールの出現の可能性を増大させることにつながります。この問題を回避するためには、RSC ごとに異なっているこれらの仕様を、あるレベルまで標準化することが必要です。

第二の問題点は、セキュリティ対策を実装する上でのコストがどこまで許容できるかということです。過大なセキュリティ対策を行なっていくとセキュリティは十分に守られるかもしれませんが、リモートサービスにかかるコストは増大し続け、これが HCF 側、RSC 側双方の運営に支障をきたしてしまう恐れがあります。逆にあまりコストをかけないためにセキュリティレベルが低くなりセキュリティホール化することは、絶対に避けなければいけません。これを解決するためには、標準的なセキュリティガイドラインを作成し、リモートサービスにおけるセキュリティレベルを明確にし、かつ適切なコストでそれが実現できるようにすることが重要です。

第三は、現状の運用体制では、万が一個人情報が漏れた場合の HCF と RSC の責任範囲が明確になっていない、という点です。このような状況になっているのは、今までリモートサービスというものが一般的に RSC 主導で行なわれており、HCF 側の関与が低かったことが一因です。責任範囲を明確にするために、RSC 側のセキュリティ対策内容を明確にし、ここまでは RSC 側の責任範囲だが、それ以外のことは HCF 側の責任である等、責任の分界をはっきりさせ、契約に反映させておくことが重要です。そのために RSC においては、自身のセキュリティ対策を文書化し、外部に対して開示できるようなものにしておかなければなりません。

これらの問題は、日本だけでなく全世界的に取り組み、解決していかなければなりません。なぜなら、各社の医療装置・システムは国内だけでなく全世界に輸出されており、輸出対象国ごとの個人情報保護の法律に対して個々にセキュリティ対策を立てることは、ベンダ側に非常に重い負担とコストを発生させることになるからです。また現在のようなインターネット社会においては、国境をまたいでのリモートサービスというものも、近い将来行なわれていくのは間違いなく、RSC と HCF が異なる国に存在するケースも一般的になる可能性があります。したがって、日本国内だけで通用する、あるいは認められるセキュリティ対策では意味が無く、グローバル（特に米国、EU）に通用する対策を纏め上げていくことが、本当に有用なセキュリティ対策を実現する上で重要になってくるのです。

２－４．国際的な標準化に向けて

医療情報関連のシステムに対するセキュリティについて、国際的な団体での検討が進められており、ISO/TC215 WG4 や DICOM WG14 などで具体的な標準規格などの提案が行われています。これらの規格・ガイドラインは、ネットワークシステムにおける技術的対策について述べたものですが、実際のセキュリティの確保については技術的手段では不十分であり、組織的な運用手段での対策を合わせて行うことが必要であるとされています。この観点から、医療機関およびシステムを提供するベンダでの運用について述べたガイドラインが必要であるとされています。

米国では、HIPAA の 2003 年からの施行により、医療機関のセキュリティ対策が急がれており、画像医療機器分野においても技術的対策だけでなく組織的対策を含めたセキュリティ、特にプライバシ保護のためのガイドラインの策定が急務となっています。このため、米国での画像医療機器分野を含む工業会である NEMA（米国電子機器工業会）が先導し、欧州の COCIR および我が国の JIRA に呼びかけ、画像医療システムに関するセキュリティの共通ガイドラインを検討するための合同ワーキンググループの立ち上げを行いました。この WG は NEMA/COCIR/JIRA Joint Security and Privacy Committee（略称 SPC）と称し、これまでにいくつかのガイドライン・白書を出版しています。その中の一つが「リモートサービスに関するセキュリティおよびプライバシ要件（Privacy and Security Requirements for Remote Servicing）」です。

この SPC のガイドラインでは、医療機関内の画像医療機器を中心とした装置に対するリモートサービスを、外部のベンダから行う際の基本的なセキュリティ対策について、技術的および運用上の対策の双方が述べられています。技術的な対策の特徴として、医療機関のネットワークに対する外部接続に起因する脅威を削減するために、外部からのアクセスポイントを１つに限定し、リモートサービスを行う複数のベンダで共有することが提案されています。このようにすることにより、医療機関でのアクセスポイントに関するセキュリティの管理が１つに絞られ、セキュリティ管理コストを削減すると同時にリモートサービス方式を統一することで一定レベルのセキュリティを確保し安全性を高めることができます。

本ガイドの策定に当っては、SPC の「リモートサービスのセキュリティ」ガイドラインを始めとした国際的な標準化の動向について検討段階で十分考慮を行っており、我が国の個人情報保護法への対応を含んだ形で、検討を行ってきました。

第３章　リモートサービスにおけるリスク分析

３－１．リモートサービスの運用モデル

リモートサービスにおける基本的な運用モデルとして、次の３つのユースケースを考えました。

（１）故障時の対応
HCF 内の機器に障害が生じ、HCF 側からの連絡に基づき、RSC 側から HCF 内の保守対象機器にアクセスを行い、障害対応を行うものです。

（２）定期保守・定期監視
HCF 側からの了解の元に、RSC 側から HCF 内の保守対象機器に対して定期的にアクセスを行い、対象機機の監視および保守作業を行うものです。

（３）ソフトウェアの改訂
RSC 側から HCF 内の保守対象機器に対してアクセスを行い、保守対象機器のソフトウェアの更新を行うものです。

これらのユースケースでは、HCF 内の保守対象機機と内部ネットワーク、HCF と RSC(リモートサービスセンタ）を結ぶ外部ネットワーク、そして RSC 内の内部ネットワークと機器とから構成されるシステムを想定しています。（図３－１－１）

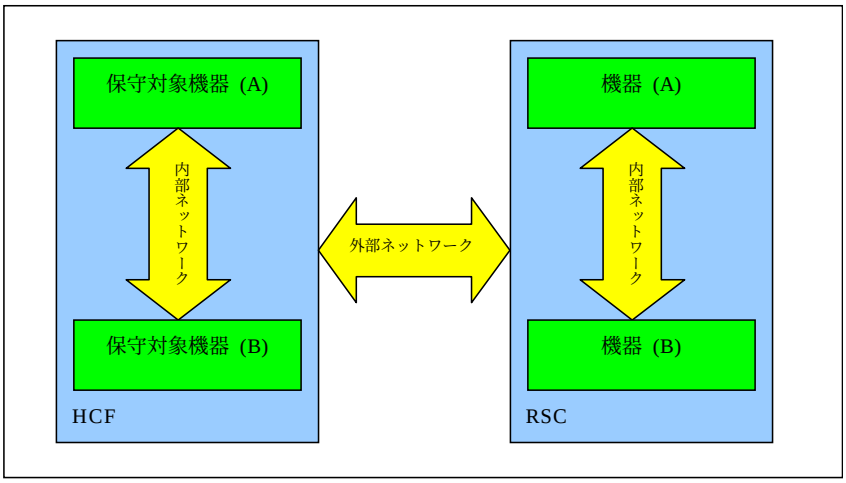


図３－１－１　リモートサービスのシステムの想定

３－１－１．故障時の対応

故障時の対応におけるワークフローを図３－１－２に示します。

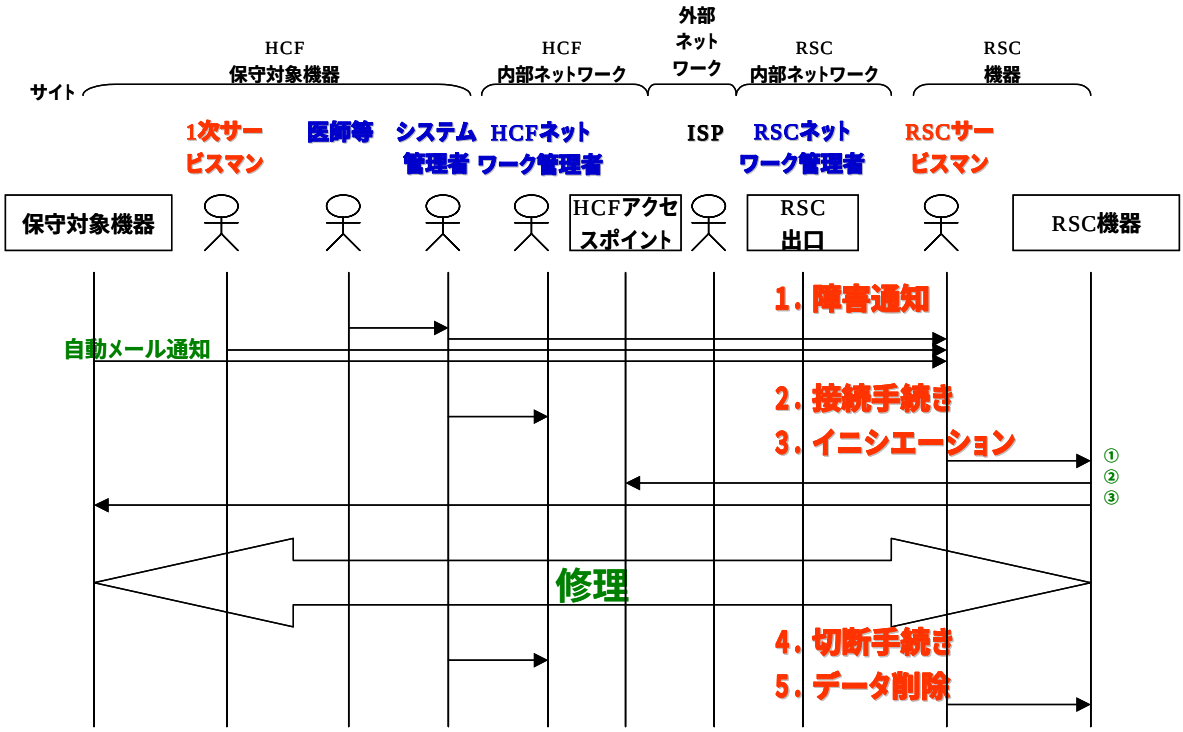


図３－１－２　故障時の対応のワークフロー

手順は次のようになります。

（１） RSC が HCF からの問題発生の連絡を受ける（電子メールによる自動通知の場合もある）。

（２） RSC から HCF にリモートサービスのためのネットワーク接続を申請する。

（３） RSC からネットワーク接続のためのイニシエーションを行う。

（４） RSC サービスマンがネットワークを介して、調査、対策、確認を行う。

（A）自己診断プログラムの実行

（B）当該機器からの関連情報の取得

（ア）動作ログ

（イ）画像データ

（ウ）設定ファイル／システムコンフィグレーション

（エ）データベース内容

（C）問題を切り分ける。

（D）問題がソフトウェア起因の場合には、当該機器の変更・更新作業を行う。

（ア）設定ファイル変更

（イ）ソフトウェア更新

（ウ）データ修復

（Ｅ）問題がハードウェア起因の場合には、１次サービスマンに連絡し故障部品の手配・交換を依頼する。
（Ｆ）修理後の動作確認を行う。

（５） RSC から HCF へ作業結果の報告を行う。
（６） RSC がリモートサービスのためのネットワーク接続の切断を行う。
（７） RSC が HCF にリモートサービスのためのネットワーク接続切断を申請する。
（８） RSC 側に PHI 情報を転送した場合には、それらの PHI 情報を全て削除する。

３－１－２．定期保守・定期監視

定期保守・定期監視におけるワークフローを図３－１－３に示します。

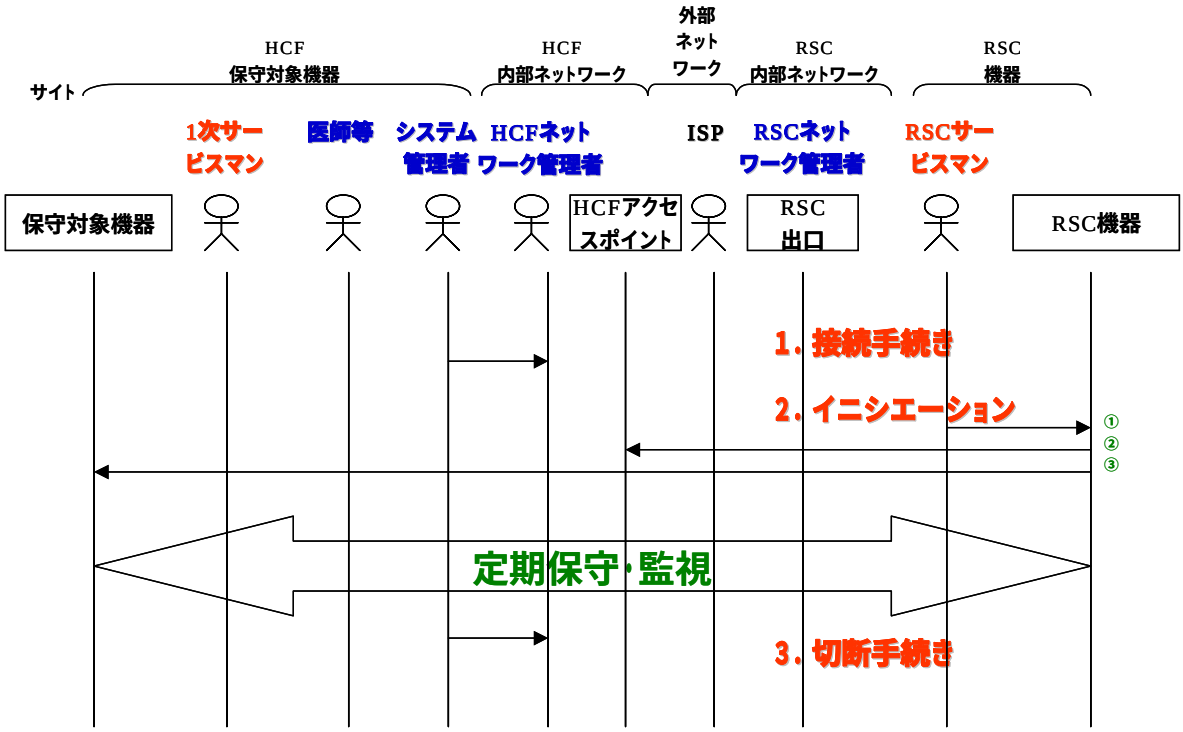


図３－１－３　定期保守・定期監視のワークフロー

手順は次のようになります。

（１） RSC が HCF にリモートサービスのためのネットワーク接続を申請する。
（２） RSC からネットワーク接続のためのイニシエーションを行う。
（３） RSC サービスマンが定期点検作業・定期監視作業を行う。
　（A）自己診断プログラムの実行
　（B）各種ログの確認
　（C）画質（精度）チェック
　（D）稼動情報の取得
（４） RSC が HCF へ作業結果の報告を行う。
（５） RSC がリモートサービスのためのネットワーク接続の切断を行う。
（６） RSC が HCF にリモートサービスのためのネットワーク接続切断を申請する。
（７） RSC 側に PHI 情報を転送した場合には、それらの PHI 情報を全て削除する。

３－１－３．ソフトウェアの改訂

ソフトウェアの改訂におけるワークフローを図３－１－４に示します。

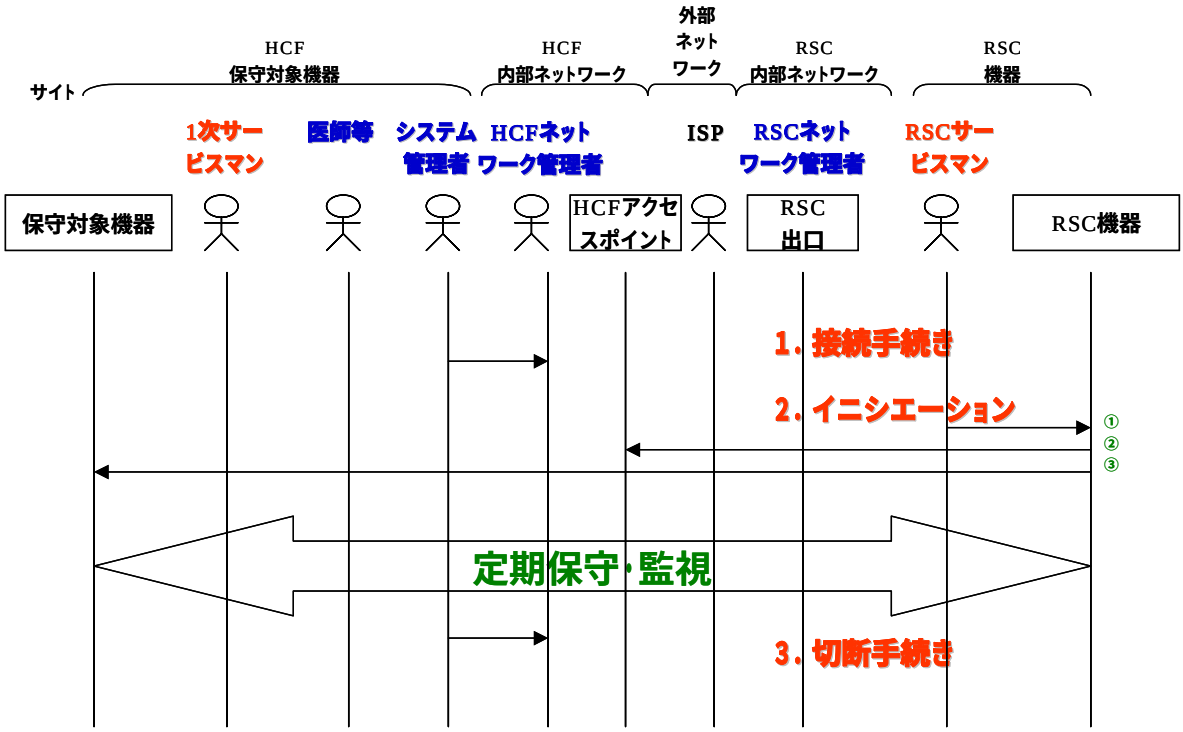


図３－１－４　ソフトウェアの監視のワークフロー

手順は次のようになります。

（１） RSC が HCF にリモートサービスのためのネットワーク接続を申請する。
（２） RSC からネットワーク接続のためのイニシエーションを行う。
（３） RSC サービスマンがソフトウェアの改訂を行う。
　（A）ソフトウェアの入替え
　（B）設定変更
　（C）動作確認
（４） RSC が HCF へ作業結果の報告を行う。
（５） RSC がリモートサービスのためのネットワーク接続の切断を行う。
（６） RSC が HCF にリモートサービスのためのネットワーク接続切断を申請する。
（７） RSC 側に PHI 情報を転送した場合には、それらの PHI 情報を全て削除する。

３－２．リスク分析

本章では、前章で述べたリモートサービスにおける基本的な運用モデルの中で、責任者の管理範囲に基づくサイトの分類別に資産を洗い出し、それに対する脅威と脆弱性を分析します。

３－２－１．リスク分析の考え方と基準

（１）考え方

HIPAA 法では、医療機関内のリスクについては、その医療機関の情報管理責任者がセキュリティを考える必要があると定めています。したがって、その範囲外と情報をやりとりするときには、それを取り出してセキュリティを考える必要があります。

本分析は、HCF/RSC 間の契約を補完する資料またはガイドとして位置付けます。

管理範囲が病院の場合の分析は、別途、病院毎に行う必要があります。

（２）サイトの分類

サイトは下記のように分類します。

RSC 機器
RSC 内部ネットワーク
外部ネットワーク
HCF 内部ネットワーク
HCF 保守対象機器

（３）脅威の対象範囲の定義

脅威の対象範囲を下記のように定義します。

HCF サイトの関係者（医師等、HCF システム管理者、HCF ネットワーク管理者、HCF 職員、一次サービスマン）を除いた脅威をおこなう者の、リモートサービスで扱う PHI に対する HCF サイトの外からの脅威、を対象範囲とします。

対象範囲外となる“ HCF サイトの関係者 ”といえども、HCF サイトの外からの脅威となる行為をした場合は第３者とみなします。

例外として、リモートサービスの有無に拘わらず存在する下記のものを除外します。

HCF 側の対策となるリスク（但し、保守対象機器は含まない）
PHI を扱う機器やソフトウェアの可用性にかかわる脅威
コンピュータウィルスにかかわる脅威
採用・教育・訓練にかかわる要員の脅威

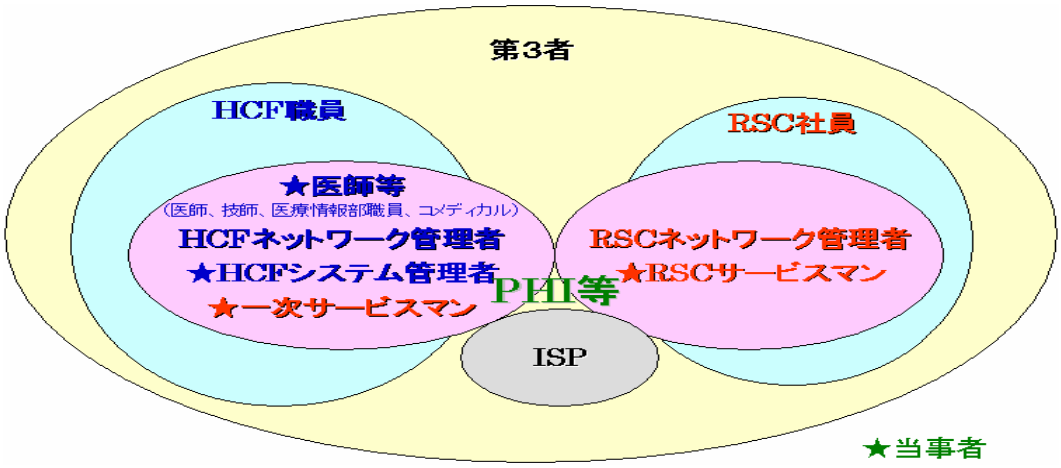


図３－２－１　リモートサービスのアクタ

（４）セキュリティ要件

各脅威が侵害するセキュリティ要件は下記のものを考えます。

（A）機密性：覗き見/盗用、不正ログイン/成りすまし、持出などによる暴露に対する脆弱度合い

（B）完全性：改ざん、差換え、消去によるねつ造や否認に対する脆弱度合い

（C）可用性：故障、災害、ケーブル不通・サービス妨害によるサービス不能に対する脆弱度合い

３－２－２．リモートサービスにおけるリスク分析

以上の考え方と基準に従ったリスク分析の詳細については、付録１に記載してありますので参照してください。

３－３．セキュリティ対策

３－２では、リモートサービス参照モデルに対するリスク分析を、サイトに分けて行いましたが、脅威から資産を守るためには、リスク分析をおこなうだけでなく、適切なセキュリティ対策を講じることがとても重要です。そこで、それぞれのリスクに対して、技術的対策と運用的対策を考える必要があります。

本章では、責任者の管理範囲であるサイト毎に、どのようなセキュリティ対策が有効か、技術的対策と運用的対策に分けて述べます。さらに、サイトにかかわらず、全般的にとるべきセキュリティ対策を述べます。

３－３－１．RSC 機器における対策

RSC 機器における対策（案）を表３－１に示します。

表３－１　RSC 機器における対策

サイト	ガイド			リスク
	VPN対策の有無	技術的対策	運用的対策	
RSC機器管理（SPC対象）			入室管理	保守権限の無い第三者による画面の覗き見、不正ログインによる情報の盗用
		操作の記録	記録の監査 守秘義務の徹底 身元調査	RSCサービス員のRSC機器内PHIの盗用
		自動ログオフ		RSC保守員のPHI削除忘れによる漏洩
		アクセス管理	権限管理（ユーザ/特権ログイン）	権限の無い者からの不正ログイン
			パスワードの定期的変更	
			複数人によるRSC機器の点検	RSC機器の異常状態、持ち出し
			PHI記録紙のシュレッダ廃棄	修理の都合で残された記録の覗き見
			複数人による入室管理	RSCサービス員による記録の持ち出し
	VPN対策あり	アクセス管理		VPN設定情報の盗用
（SPC対象外）		Computer Virus対策	IRT（緊急事態対応体制）	バックドアやPHI盗用プログラムの挿入
			RSCサイトと道路の距離確保	漏洩電磁波の解析
			保守点検	機器故障によるPHI漏洩
			バックアップ機器の施錠保管	持ち出し
			防災対策	被災によるPHI漏洩
			事業継続計画	事業終了時のデータ漏洩
			教育・技能基準	誤操作、誤設定によるPHI情報の漏洩

３－３－２．RSC 内部ネットワークにおける対策

RSC 内部ネットワークにおける対策（例）を表３－２に示します。

表３－２　RSC 内部ネットワークにおける対策（例）

サイト	ガイド			リスク
	VPN対策の有無	技術的対策	運用的対策	
RSC内部ネットワーク（SPC対象）		RSC機器のルート制御		外部経路からの不正ログインによる、RSC側経路上のPHI漏洩
		RSC出口におけるアクセス管理		
		ネットワークの分離		
		強制経路（FW）		
		フィルタリング		
		ポートの保護		
			IRT（緊急事態対応体制）	外部経路からの不正ログインによる、RSC側経路上のPHI漏洩
		アクセス管理	権限管理（ユーザ/特権ログイン）	外部経路からの不正ログインによる、RSC側経路上のPHI漏洩
			パスワードの定期的変更	外部経路からの不正ログインによる、RSC側経路上のPHI漏洩
			RSC側内部経路点検	経路上のPHI盗用
			複数人によるRSC側内部経路点検	管理者の経路上のRSC側ネットワーク機器経由の覗き見によるPHI盗用
			複数人による施錠保管	管理者によるRSCネットワーク側のPHI盗用
			PHI記録紙のシュレッダ廃棄	管理者以外のPHI記録紙覗き見、持ち出し
			入室管理	権限の無い者の入室による、PHI記録紙の覗き見、持ち出し
			PHI記録媒体の施錠保管	管理者以外のPHI記録媒体の持ち出し
			PHI記録媒体の複数人による施錠保管	管理者単独のPHI記録媒体の持ち出し
RSC内部ネットワーク（SPC対象外）		Computer Virus対策	IRT（緊急事態対応体制）	バックドアや情報の盗用プログラムの挿入によるPHI漏洩
			ネットワーク機器の施錠保管	管理者以外のネットワーク機器持ち出しによるPHI漏洩や機器の破壊
			複数人による施錠保管	管理者単独のネットワーク機器持ち出しによるPHI漏洩や機器の破壊
			シールを貼る	タンパリング
			RSCサイトと道路の距離確保	漏洩電磁波の解析
			定期的なネットワーク機器や環境の保守点検	ネットワーク機器の故障によるリモートサービス不能
			防災対策	ネットワーク機器の被災によるリモートサービス不能
			身元調査	収賄によるPHI情報の漏洩
			教育・技能基準	誤設定によるPHI情報の漏洩
	VPN対策あり		認定暗号アルゴリズムと安全な鍵配送方式の採用	暗号化データの解読によるPHI情報の漏洩

３－３－３．外部ネットワークにおける対策

外部ネットワークにおける対策（例）を表３－３に示します。

表３－３　外部ネットワークにおける対策（例）

サイト	ガイド			リスク
	VPN対策の有無	技術的対策	運用的対策	
外部ネットワーク			ISPとの外部委託契約による責任分界の明文化	ISP側ネットワーク機器の故障、被災、破壊によるリモートサービス不能
				ISP側ネットワーク機器の環境設備の故障、被災、破壊によるリモートサービス不
	VPN対策あり		認定暗号アルゴリズムと安全な鍵配送方式の採用	暗号化データの解読によるPHI情報の漏洩

３－３－４．HCF 内部ネットワークにおける対策

HCF 内部ネットワークにおける対策（例）を表３－４に示します。

表３－４　HCF 内部ネットワークにおける対策（例）

サイト	ガイド			リスク
	VPN対策	技術的対策	運用的対策	
HCF内部ネットワーク（SPC対象外）		HCF機器のルート制御		外部経路からの不正ログインによる、HCF側経路上のPHI漏洩
		HCF出口におけるアクセス管理		
		ネットワークの分離		
		強制経路（FW）		
		フィルタリング		
		ポートの保護		
			IRT（緊急事態対応体制）	外部経路からの不正ログインによる、HCF側経路上のPHI漏洩
			パスワードの定期的変更	外部経路からの不正ログインによる、HCF側経路上のPHI漏洩
				内部経路からの不正ログインによる、HCF側経路上のPHI漏洩
		アクセス管理	権限管理（ユーザ/特権ログイン	内部経路からの不正ログインによる、HCF側経路上のPHI漏洩
			内部経路点検	内部経路からのタッピングによる、HCF側経路上のPHI漏洩
			複数人による内部点検	内部経路からの管理者によるタッピングによる、HCF側経路上のPHI漏洩
			複数人による施錠保管	管理者のネットワーク機器経由の覗き見による、HCF側経路上のPHI漏洩
				管理者のネットワーク機器持ち出しによるPHI漏洩や機器の破壊
			シュレッダ廃棄	管理者以外のメモやプリントアウトの紙の持ち出し、覗き見によるPHIの暴露
			入室管理	管理者以外のメモやプリントアウトの紙の持ち出し、覗き見によるPHIの暴露
			媒体の複数人による入室管理	管理者のメモやプリントアウトの紙の持ち出しによるPHIの暴露
			媒体の複数人による施錠保管	管理者によるバックアップ媒体の持ち出
		コンピュータウィルス対策	IRT（緊急事態対応体制）	バックドアや情報の盗用プログラムの挿入によるPHI漏洩
			ネットワーク機器の施錠保管	管理者以外のネットワーク機器持ち出しによるPHI漏洩や機器の破壊
			シールを貼る	タンパリング
			HCFサイトと道路の距離確保	漏洩電磁波の解析によるPHIの暴露
			定期的な保守点検、バックアッ	ネットワーク機器の故障によるリモートサービス不能
				ネットワーク機器の環境設備の故障やケーブルの不調によるリモートサービス
			防災対策	ネットワーク機器の被災によるリモートサービス不能
				ネットワーク機器の環境設備の被災によるリモートサービス不能
			施錠保管	ネットワーク機器の破壊によるリモートサービス不能
				ISP側ネットワーク機器の環境設備の破壊によるリモートサービス不能
				管理者以外によるバックアップ媒体の持ち出し
			身元調査	収賄によるPHI情報の漏洩
			教育・技能基準	誤設定によるPHI情報の漏洩
HCF内部ネットワーク（SPC対象）	VPN対策あり		ルート制御	外部経路からの不正ログインによる、HCF側経路上のPHI漏洩

３－３－５．HCF 保守対象機器における対策

HCF 保守対象機器における対策（例）を表３－５に示します。

表３－５　HCF 保守対象機器における対策（例）

サイト	ガイド			リスク
	VPN対策の有	技術的対策	運用的対策	
HCF保守対象機器（SPC対象）		アクセス管理(ログイン)	権限管理（ユーザ/特権ログイン）	外部経路からの関係者以外の不正ログイン、なりすまし
			パスワードの定期的変更	
		操作の記録	記録の監査	外部経路からのRSCサービスマンによるPHI盗用
			守秘義務の徹底、身元調査	
		アクセス管理(書込み禁止、消去禁止)		外部経路からのRSCサービスマンによるPHI捏造
HCF保守対象機器（SPC対象外）		アクセス管理(ログイン)	パーティション	オンサイトでの関係者以外による画面の覗き見、不正ログインによる情報の盗用
			クリアデスク	
		操作の記録	記録の監査	オンサイトでの関係者によるＨＣＦ機器内PHIの盗用
			守秘義務の徹底	
			身元調査	
			複数人による施錠管理	権限のあるものの記録の持ち出し
		Computer Virus対策	IRT（緊急事態対応体制）	PHI盗用プログラムの挿入
			シール	タンパリング
			サイトと道路の距離確保	漏洩電磁波の解析によるPHI暴露
			保守点検、バックアップ	機器故障によるサービス不能
			防災対策、事業計画	被災によるサービス不能
			施錠保管	破壊によるサービス不能
			教育･技能基準	誤入力によるサービス障害

第４章　日本におけるリモートサービスのあり方

４－１．医療機関とベンダの役割分担

これまでリモートサービスのセキュリティは各ベンダの判断と責任の下で実装されてきました。これは、HCF がベンダとの保守契約を締結することで、リモートサービスにおけるセキュリティの確保を HCF がベンダに委任していたとみなすことが出来ます。ここで、問題となるのは次のような点です。

（１）ベンダが実施しているセキュリティ対策が十分であることを第三者が理解できる形で明文化していない。
（２）現在のセキュリティ対策は技術面の対策が中心で、管理面の対策が必ずしも十分であるとはいえない。
（３）問題が発生した後の対応については、ほとんど検討されていない。
（４）コンピュータウィルスなどの広範な脅威については検討されていない。

今後個人情報保護法により、個人の医療情報セキュリティに対する最終的な責任者は HCF となり、リモートサービスのセキュリティ維持も HCF が責任を持って実施していくことになることを想定し、HCF とベンダの役割分担について説明します。

まず､リモートサービスにおけるセキュリティ確保のための技術的な実装はいままでどおりベンダが行います。医療装置へのリモートサービスのための機能の実装はベンダが行うしかないからです。ここでベンダが考慮すべき点は、各ベンダがそれぞれ異なったセキュリティ技術を実装すると、リモートサービスの普及を妨げることになることです。HCF はベンダごとにリモートサービスのアクセスポイントを準備することになり、セキュリティ管理が複雑化しセキュリティホールの要因になります。そのため、広く使われている標準的なセキュリティ技術を各ベンダが共通して採用し、実装することが望ましいでしょう。

また技術面の対策だけでなく管理面の対策も重要です。これは HCF、RSC 双方に必要です。BS7799 のようなセキュリティポリシ策定の国際標準に基づいて、現状の情報セキュリティマネジメントシステムを明文化し、セキュリティポリシの比較や対応付けができるようにするとともに、リモートサービスにおけるセキュリティの最低基準を明確にすることが重要となります。

HCF は、自身のセキュリティポリシの策定および対策を行うとともに、ベンダが開示するリモートサービスにおけるセキュリティポリシ、セキュリティ対策状況を検討・評価し、ベンダとの間で運用の遵守や秘守に関しての契約を結びます。これによりリモートサービスのセキュリティが確保されたことになります。

４－２．SPC における合意事項

リモートサービスにおけるセキュリティの確保の最終的な責任が HCF 側にあるとしても、RSC 側の技術的および組織的な対策の責任が無くなる訳ではありません。RSC を提供する側のベンダの団体である前述の SPC では、リモートサービスのセキュリティに関するガイドラインを策定しました。これは、「Security and Privacy Requirements for Remote Servicing（リモートサービスにおけるセキュリティとプライバシの要件)」という文書にまとめられています。なお、この文書は、米国 NEMA、欧州 COCIR そして日本 JIRA の３極の画像医療システム関連工業会でそれぞれ検討・承認されています。

この中で、リモートサービスを行うシステムのモデルが提案されています（図４－２－１)。それは、HCF に設置されている複数のベンダの装置・システムに対するリモートサービスは、単一のアクセスポイントを各 RSC で共有して、それぞれの装置にアクセスするというものです。

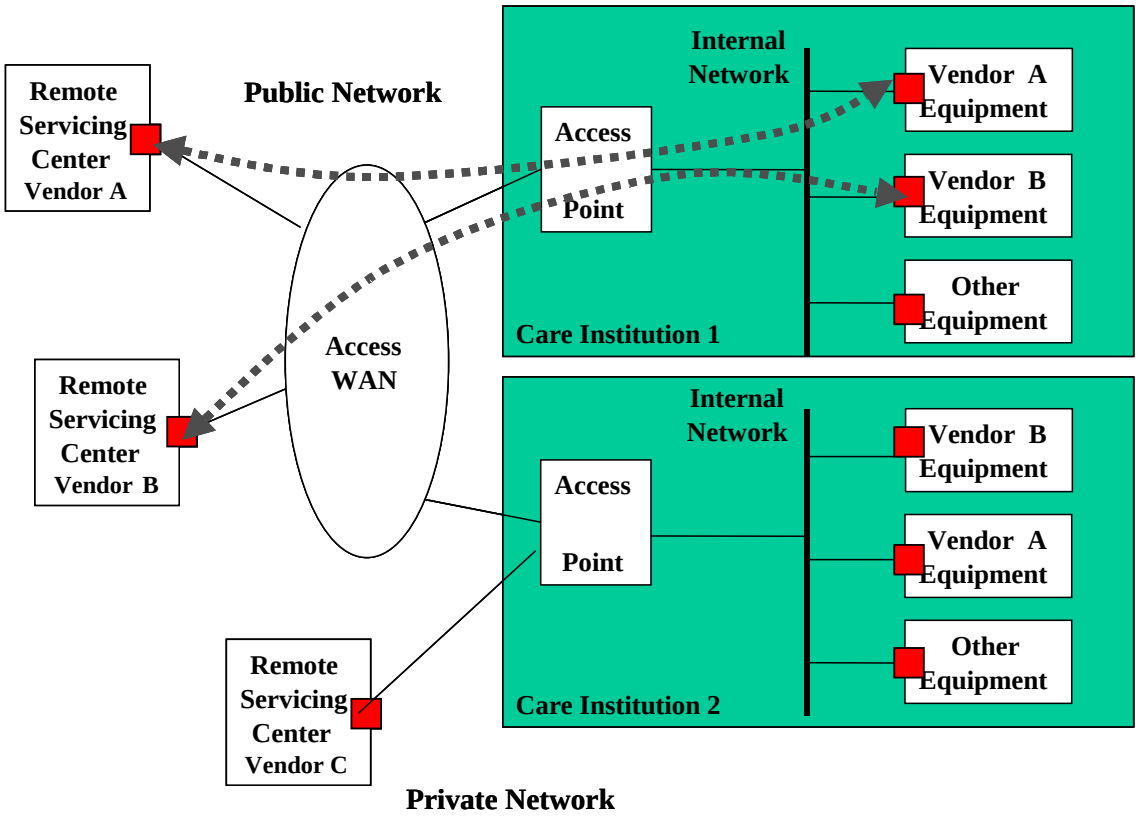


図４－２－１　リモートサービスシステムのモデル

従来のリモートサービスでは、各ベンダは、リモートサービスを行う装置ごとに電話あるいは ISDN 回線を設置していました。その回線を通じて、各社の RSC からそれぞれの装置・システムにアクセスし、リモートサービスを実施していたわけです。このため、多くの機器を有する HCF では多数のアクセスポイントが存在することになり、その部分の管理を十

全に行わないと、外部からの不正アクセスという脅威に、システムがさらされかねません。また、リモートサービスを提供するベンダにとっても、回線を使用する料金の負担は無視できないものになってきています。

この様な状況を改善するために、SPC のガイドラインでは、単一に統合したアクセスポイントの管理だけをきちんと行えば、施設内のネットワークシステムの安全が保てるモデルを提案しました。アクセスポイントには、インターネットを通じて接続することにより、通信の費用も安く済むことになり、リモートサービスにおいて多量のデータを回収する場合でも、高速に行えることになります。

しかしながら、インターネットの利用においては、リモートサービスで行う通信上の、患者氏名などの個人情報が含まれるかもしれないデータが、第三者にのぞき見られる可能性があります。また、不正な第三者から、このアクセスポイントに接続され、HCF 内のネットワークに不正アクセスされる可能性もあります。

この様な問題を防ぐために、SPC のガイドラインでは、セキュリティを確保しプライバシを守るための以下の対策を示しています。

- アクセスポイントへの接続時に認証を行い、誰がアクセスポイントに接続しているかを HCF 側がわかるようにします。
- 接続している RSC が自分の装置・システムにだけアクセスできるようにします。
- HCF 側は、手動で、RSC からの接続を切断できます。
- リモートサービスでの接続内容は、RSC、アクセスポイント、リモートサービス対象機器の 3 カ所で、アクセス記録を取ります。
- HCF と RSC の間のネットワークでは、暗号化などの手段を用い、個人情報が漏洩しないようにします。
- 出来る限り、患者様の個人情報は、個人の特定が出来ないように変換します。個人情報を転送した場合にそなえて、RSCでは、その個人情報を守るためのセキュリティポリシと運用管理規定を定め、従業員に対する教育と秘密保持の契約を結びます。また、個人情報データの安全な廃棄を行います。

SPC のガイドラインでは、以上の対策をとり、適切な運用を行うことにより、リモートサービスを実施したことによるセキュリティレベルの低下やプライバシの漏洩などの問題は、防ぐことが可能である、としています。

SPC のガイドラインでは、とるべき対策について述べているだけで、具体的な技術的なソリューションについては述べていません。このため、実際にリモートサービスを行う際に、単一のアクセスポイントを複数の RSC で共有するためには、その接続の技術的な統一を図っておく必要があります。

第５章　セキュリティ対策の策定

５－１．全体的な方針

日本のリモートサービスにおける個人情報の保護は、図５－１に示すような枠組みで行われる見通しです。個人情報保護法における個人情報取扱事業者である医療機関は、個人情報保護法で定める義務と責任を負うことになります。リモートサービスにおいては、リモートサービスセンタから医療施設内に設置された対象機器にネットワークを介してアクセスすることになりますので、医療機関は、リモートサービスを提供するベンダに対しても、個人情報保護のための適切な措置を求める必要があります。具体的には、医療機関がベンダと締結する保守契約もしくは覚書の中で、ベンダ内においても適切な措置を講じなければならない旨の項目を記載することが考えられます。これにより、医療機関は、契約・覚書を通してベンダに保守作業に伴う個人情報保護に関する義務と責任を分与することになります。また、米国 HIPAA 法のように、保守契約とは別に医療機関がベンダに対して個人情報保護のための業務委託契約を結ぶことを求めるケースも考えられるでしょう。いずれにしても、個人情報保護に関する最終責任者である医療機関と、個人情報保護に関する責任を分与されたベンダは、双方が適切な情報セキュリティマネジメントシステムを構築し、個人情報を適正に取り扱うことが求められるわけです。

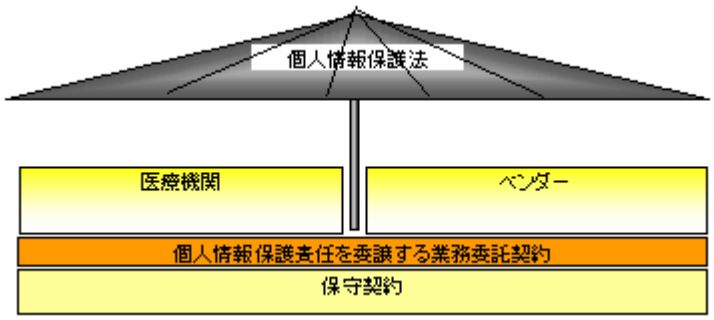


図５．１　日本のリモートサービスにおける個人情報保護の枠組み

リモートサービスにおける個人情報保護という観点においては、「安全管理措置」、「第三者提供の制限」などの条項が重要になります。「安全管理措置」として、医療機関が個人情報の安全管理のために必要かつ適切な措置を講じる義務が述べられており、「第三者提供の制限」では情報提供時の本人の事前同意を義務付けています。

医療機関は、保守契約あるいは業務委託契約等において、個人情報保護の最終責任者として、ベンダに対する義務を明文化すると同時に、適切な情報セキュリティマネジメントシステムを構築しなければなりません。

図５－２は、情報セキュリティマネジメントシステムの概念を示したものです。情報セキュリティマネジメントシステムとは、セキュリティポリシ（Security Policy、５．２章参照）の下に、セキュリティ対策を具体化して（Plan）、それらのセキュリティ対策を実行し

（Do）、それらのセキュリティ対策が確実に実行されていることを監査し（Check）、必要に応じて見直し（Act）を行うための一連の PDCA サイクルを運行する仕組みのことです。

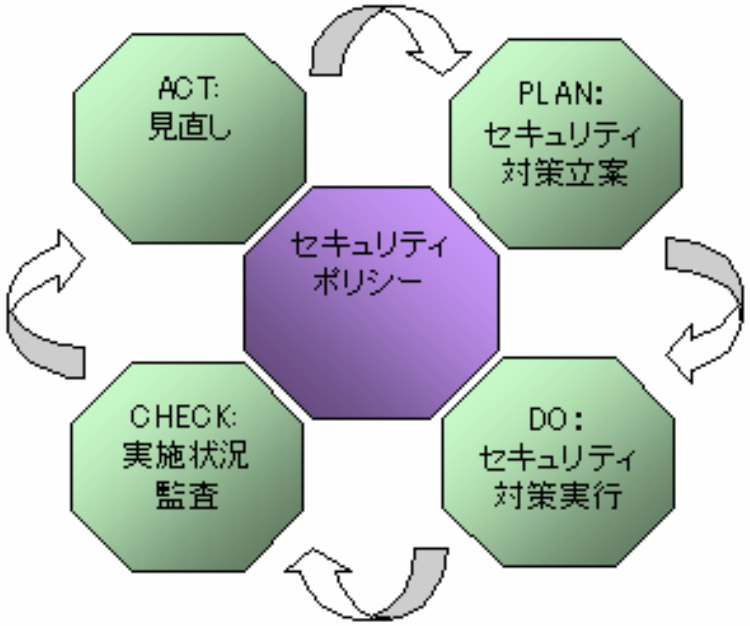


図５－２　情報セキュリティマネジメントシステム概念図

医療機関とベンダは、それぞれ適切な情報セキュリティマネジメントシステムを構築することが必要となりますが、リモートサービスにおける個人情報保護のセキュリティ対策を考える上では、医療機関はリモートサービスを提供する全てのベンダとの間で情報セキュリティマネジメントシステムの整合という作業を行わなければなりません。リモートサービスは、ある意味で医療機関とリモートサービスを提供するベンダのそれぞれのネットワークをつなげてしまうものです。このようにネットワークがつながったことにより、これまで存在していなかったセキュリティホールができてしまう危険性を秘めているのです。もしこのネットワークの一部にセキュリティホールがあれば、このネットワークにつながっている医療機関や他のリモートサービスベンダのネットワークをも危険に陥れることになってしまいます。このことにより、医療機関は、主導的にリモートサービスを提供する全てのベンダの情報セキュリティマネジメントシステムを整合させて、セキュリティホールができていないことを確認するとともに、各ベンダのセキュリティレベルが適切に保たれていることを確認しなければなりません。

次節以降では、情報セキュリティマネジメントシステムを整合させるために、遵守すべき項目を中心に、以下の具体的な内容について述べていきます。

・　セキュリティポリシ
・　セキュリティ対策標準
・　セキュリティポリシのマッピング
・　ソリューションの選定
・　運用実施規定

・ セキュリティ監査基準
・ セキュリティ監査と監査証跡

５－２．セキュリティポリシ

セキュリティポリシとは、ある組織においてセキュリティに対してどのように取り組むかについての意思を明確化したものです。情報セキュリティマネジメントシステムとして適切な管理、運用を行うためには、セキュリティポリシは情報資産を守るための基本方針や実施すべき対策を文書化したものであることが求められます。

セキュリティポリシは一般的には以下の階層に分けられます。

（１）基本方針（ポリシ）
「社会、職員に対する組織の目標とセキュリティ方針（対象･重要性分類･推進体制等）」
この部分は経営層がどのような方針でセキュリティに取り組んでいくかの宣言を記述する部分です。

（２）対策基準（スタンダード）
「管理策（コントロール）」
この部分は実際に守るべき規定を具体的に記述する部分です。管理策には、リスク分析作業も含みます（５－３で説明しています）。

（３）実施手順（プロシージャ）
「作業指示書、手順書」
この部分は対策基準を実施するための詳細手順を具体的に記述する部分です（５－６で説明しています）。

リモートサービスのセキュリティポリシは組織全体のセキュリティポリシにおける基本方針を踏襲しつつ、リモートサービスにおいて特に意識しなければならない事象について規定する必要があります。たとえば、基本方針として職員以外のアクセスを禁止していたとしても、リモートメンテナンス要員がアクセスするための仕組みが必要です。また、リモートサービスにおいて社会的・制度的に要求されるセキュリティ要件に対し、その組織がどのように対処するかについて具体的に記載していくこととなります。すなわち、保健医療分野において厚生労働省が規定する個人情報保護やネットワークセキュリティの指針をもとに、医療機関以外の組織とデータのやりとりが発生するという前提でその対処を規定することとなります。

セキュリティポリシは単に策定すれば良いと言うものではなく、策定（Plan）されたポリシに基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Act）していかねばなりません。PDCA サイクルを適切に廻しながら改善活動を伴う継続的な運用を行うことが重要です。このようなプロセスモデルを採用した情報セキュリティマネジメント規格が 2002 年度版 BS7799 です。BS7799 のガイドラインに相当する部分が既に ISO 化されており、ISO17799 として発効しています。

セキュリティポリシを作成するにあたり、そのフォーマットを 2002 年版 BS7799-2（管理策）に従うのは第三者評価を受けるために非常に有効です。BS7799-2 においては、リスク対応のための管理項目及び管理策が 127 項目定められており、そこから選択するか追加の管理策を策定することとなります。定められた管理項目から管理策を選択することは、他の組織とのポリシマッピングにおいても両者の比較対象項目が明確になるため有用です。

５－３．セキュリティ対策基準

医療機関およびリモートサービスセンタを運営するにあたっては、情報セキュリティポリシで策定した基本ポリシに従い、実際に守るべき行為および判断の基準を具体的に述べる「セキュリティ対策基準（スタンダード）」を策定する必要があります。

さまざまな脅威の例として、保守サービス員へのなりすまし、保守サービス員によるドキュメント・アカウント名・パスワード等の不正取得、リモートメンテナンス回線からの侵入、同回線盗聴、総当たりによるダイアルアップ回線用電話番号の露見、などがあります。これらに対して、保守サービス提供組織や要員の管理体制の確立、サービス提供者側および利用者側双方での確実な識別と認証、リモートサービスに対する監視と監査、許可範囲以外のコマンド使用やファイルアクセスの拒否などの管理策（コントロール）が必要です。

セキュリティ対策基準を策定するにあたり、事前にリスクを分析する必要があります。具体的には、まず、リモートサービスを行う場合の具体的な作業の流れ（ワークフローと呼びます）をモデル化し、情報資産の管理責任者の責任範囲に基づいて、物理的な区分（サイトと呼びます）ごとに情報資産を定義します。次に、それらの情報資産に対して、機密性、完全性、可用性の観点から、考えられる脅威やリスクと、それらによる脆弱性を洗い出していきます。さらに、それらの脆弱性を脆弱度、影響度、発生度などの観点から評価して、脆弱性の優先度付けを行います。最後に、個々の脆弱性を抑制、防止・予防、検出、回復、維持、消去・廃棄するための管理策を具体化していくことになります。なお、管理策としては、ハードウェアやソフトウェアなどを導入して行う技術的対策と、手続きや規則などを設けて行う組織的・管理的対策があります。

ISO17799 では１０のマネジメント領域を定めています。

（１） 組織的・管理的領域

①セキュリティポリシ
　経営者による組織横断的なセキュリティポリシの発行、及び支援について規定

②セキュリティ組織
　セキュリティを確保するための組織作り（セキュリティフォーラムの設置など）について規定

③資産の分類および管理
　組織の資産を保護するための資産目録や資産分類（極秘、部外秘など）について規定

④人的セキュリティ

人的な問題によるリスクを軽減するため、業務責任、採用時の審査、採用条件、教育などについて規定

⑤事業継続管理
各種障害（事故、災害などを含む）における回復対策、予防対策による事業継続管理（影響分析、継続計画など）について規定

⑥適合性
知的所有権、記録の保管、プライバシ保護など法的要求事項への準拠について規定やセキュリティポリシと技術準拠のレビュー（内部監査）について規定

（２） 技術的領域

①物理的および環境的セキュリティ
入退出管理、施設(事務所、居室など)、装置の設置などのセキュリティについて規定

②通信および運用管理
情報処理システムの管理・運用を健全に実施するため、操作手順書の整備、運用の変更管理、セキュリティ問題管理、不正ソフトウェア対策、バックアップなどについて規定

③アクセス制御
情報へのアクセス制御、利用者のアクセス管理、特権管理、ネットワークにおけるアクセス制御などについて規定

④システム開発およびメンテナンス
健全な開発・運用のため、システムへのセキュリティ要件、アプリケーションプログラムに対するセキュリティ要件情報の秘匿・認証、暗号鍵の管理などについて規定

IT の発展速度は極めて速いため、ある時に講じた最高の情報セキュリティ対策が、将来にわたっても最高のものとして永続することは一般的には期待できません。その時々のハードウェア、ソフトウェアの導入は、導入時には適切な対策となっているかもしれませんが、継続性は保証されていません。情報セキュリティ対策は、ガイドラインを基に情報セキュリティポリシを策定することによって完結する一過性の取り組みではなく、情報セキュリティポリシの策定およびそれに続く日々の継続的な取り組みによって確保される性質のものであることを十分に認識することが大切です。

また、情報セキュリティポリシの中には、継続的な情報収集及びセキュリティ確保の体制を構築しておくこと、また「いかに破られないか」のみならず、「破られたときどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に構築しておくことが重要です。

さらには、情報セキュリティポリシ及び情報セキュリティポリシに関連する実施手順等の規定類を定期的に見直すことによって、所有する資産に対して新たな脅威が発生していないか、環境の変化はないかを確認し、継続的に対策を講じていくことが必要です。特に、情報セキュリティの分野では、技術の進歩や不正アクセスの手口の巧妙化に鑑み、早いサイクルで見直しを行っていくことが重要です。

５－４．セキュリティポリシのマッピング

異なる組織間で情報の共有ややりとりが発生する場合、セキュリティ対策にレベルの差があった場合には、全体のセキュリティレベルが低いほうに引き下げられてしまいます。リモートサービスにおいては、RSC と HCF の間で情報のやりとりが発生しますので、両者間のセキュリティ対策の差が問題になります。そこで必要なのはセキュリティポリシのマッピングです。

医療機関は個人情報取扱事業者として責任ある立場にありますので、ベンダとリモートサービス契約を実施するにあたり、ベンダのセキュリティポリシを評価し、セキュリティレベルが下がらないようにしなければなりません。セキュリティレベルが下がらないかどうかは、両組織のセキュリティポリシを比較し、医療機関における要件を満たしているかを医療機関が判断しなければなりません。特に、以下についての十分なチェックが必要です。

・適切なリスクアセスメントがなされているか
・リスク対応のための管理目的、管理策は適切か

セキュリティポリシの項で述べたように､両者が BS7799-2 に基づいたセキュリティポリシの策定を行っていれば、両者の比較は容易です。127 項目のうちどの管理策を採用しているのかが明確になっているので管理策の分類などで混乱することを避けることが出来ます。ベンダ、医療機関のどちらか、もしくは双方が独自の管理策を採用していた場合には独自の管理策についてどのような脅威に対する管理策なのかを明確にした上で、比較検討することとなります。

脅威と管理策は１対１で対応するものではなく、一つの脅威に複数の管理策で対応したり、複数の脅威に一つの管理策で対応したりすることも可能です。そのため、単に同じ管理策を採用しているかだけではなく、それぞれの脅威に対してどのような管理策で対応しているかについて全体を把握した上で、複数の管理策全体としてのセキュリティレベルのギャップを評価しなければなりません。

もしも、ポリシマッピングを行った結果としてベンダ側のセキュリティポリシが医療機関の要求レベルに満たない場合、要求レベルに見合うような改善（Act）が行われなければ契約すべきではありません。

５－５．ソリューションの選定

前章までは、リモートサービスを行うにあったってのリスク分析やセキュリティ対策、セキュリティポリシについて述べてきましたが、実際に SPC の提案であるリモートサービスセキュリティガイドラインを採用する場合、対象となる施設の形態や環境により対策を考え、それに沿ったソリューションを選ぶ必要があります。対象となる RSC にどのソリューションを導入するのが最適かという点については、RSC の規模や採用しているネットワーク、投入金額により異なります。ただ最も気をつけなくてはいけない点は、サービスのシステム全体をポリシなどで決めたセキュリティレベル以上のものとするということです。一箇所でもセキュリティレベルが低くなると、他の部分でセキュリティを高くしても意味がなくなるからです。

（１）RSC 室入室時の認証
　　IC カード
　　生体認証（指紋、指静脈、網膜、虹彩、音声、人相、血流パターンなど）

（２）RSC 機器ログイン時の認証
　　ワンタイムパスワード:
　　IC カード
　　USB キー
　　生体認証（指紋、指静脈、網膜、虹彩、音声、人相、サイン、血流パターンなど）

（３）バックアップ装置
　　磁気テープ
　　ハードディスク
　　CD-R
　　DVD

（４）ハードディスク上のデータの保護
　　ハードディスクのデータの暗号化

（５）経路上のデータの保護
　　VPN
　　IP-VPN
　　インターネット VPN

（６）不正アクセスの監視
　　IDS

（７）アクセスポイントにおいての制御

ファイヤウォール
PROXY
認証

ここに記載されたさまざまなセキュリティソリューションを導入するのも重要ですが、それを使いこなすための運用方法を決めたり、運用する人の教育をしたりすることは、導入したセキュリティソリューションの機能を最大限に発揮させることに繋がります。従って、運用に必要なコストも充分に考慮して、適切なソリューションを導入する必要があります。また、セキュリティソリューション導入の根本となるセキュリティポリシを、十分に検討して策定することが大切です。

５－６．運用実施規定

対策基準を実施するにあたり、情報セキュリティマネジメントシステムを確立して、それを維持していく必要があります。そこで、リスク評価および要求されるシステムの保証の度合いに基づいて管理策を選択し、それらの実施にあたって運用ルールを決定し、運用実施規定として文書として明文化します。明文化することにより、担当者の役割や手順の周知徹底が図れるとともに、担当者変更においてもスムーズな引継ぎができます。

（１）情報にアクセスするための管理
　　（Ａ）アクセスポリシ
　　（Ｂ）ユーザ登録の規定
　　（Ｃ）特権管理
　　（Ｄ）カードやパスワードの管理
　　（Ｅ）認証できなかった場合の規定

（２）物理的セキュリティの規定
　　（Ａ）施設とそこを出入りするためのセキュリティ規定

（３）ネットワークへのアクセス制御

（４）バックアップ装置
　　（Ａ）バックアップ作業規定
　　（Ｂ）メディア保管規定
　　（Ｃ）処分規定

（５）VPN、IDS、FW、PROXY 等のセキュリティ装置
　　（Ａ）各種設定および変更規定
　　（Ｂ）シグネチャ、パターンファイルなどの情報の更新規定
　　（Ｃ）チューニングの規定
　　（Ｄ）ログのチェック規定

（６）保守サービスのコール手順

（７）リモートメンテナンス業務規定

（８）サービス員の服務規程
　　（Ａ）仕事の定義
　　（Ｂ）人員採用審査やポリシ
　　（Ｃ）秘密保持合意文書

（９）教育・訓練

（１０）その他

（A）バージョンアップ、パッチ処理の規定

（B）問題発生時や規定を外れた場合の連絡報告処置等の規定

（C）規定の整合性チェック

５－７．セキュリティ監査基準

（１）セキュリティ監査

セキュリティ監査とは、情報セキュリティの維持・向上を図るためのものであり、セキュリティ対策を総合的に評価・検討することです。またセキュリティ監査は、内的脅威と外的脅威からの具体的なリスクの算出にとても有効な手段です。

セキュリティ監査には、管理者が自ら行う内部監査と、第三者による外部監査があります。外部監査とは、ソリューションプロバイダや、セキュリティ専門のコンサルティング業者、監査法人系のコンサルティング業者などに外部委託し、セキュリティ監査を実施するものです。外部委託先は技術的に信頼のできる企業を選定すべきであることはいうまでもありません。例えばISMSやプライバシマークを取得している企業を選ぶことも良いでしょう。

（２）セキュリティ監査の実施

セキュリティ監査を実施するためには、まず監査担当者を決めます。セキュリティポリシの運用状況を監査するにあたり、情報セキュリティに係る監査の知識並びに実務能力を有する人を選ぶことが一般的です。選ばれた監査担当者は、客観的な評価者としての立場を堅持すると共に、監査対象へ改善勧告した事項について、その実施報告を求める権限を有します。

監査担当者は、監査の対象を明確にしなければなりません。監査対象は、医療施設のセキュリティポリシとリモートサービスセンタのセキュリティポリシのマッピングから決定されます。同時に監査対象の責任者は、監査担当者の協力要請に応じなければなりません。また、監査実施中の監査作業の妨害、虚偽の報告及び事実の隠蔽をしてはいけません。

セキュリティ監査には、セキュリティポリシに従って定期的な実施計画が必要です。計画内容は、リモートサービスにテーマを限定した監査を適宜実施するものとすることができます。このとき、リモートサービスの運用及び情報資産の取扱がポリシどおり実施されていることを監査します。一般に監査終了後に監査結果報告書を作成します。監査結果報告書には、監査対象、監査内容、監査結果、指摘事項及び改善勧告等を盛り込むことが大切です。

監査担当者は、監査結果報告書に基づき監査対象に改善勧告を行います。監査対象は、監査担当者より指摘を受けた事項について可及的速やかに改善しなければなりません。

このようなセキュリティ監査を盛り込んだ PDCA サイクルを繰り返すことによって、利用者も含めリモートサービスに関わる人たちのセキュリティ対策に対する意識も高まり、より良いシステムへの更新が可能となります。

５－８．セキュリティ監査と監査証跡

HCF、RSC それぞれのシステム活動を常時記録して検査を行う機構を監査コントロールと呼んでいます。この監査コントロールが実装されることにより、HCF では正しいリモートメンテナンスが行われているかを確認することができ、また RSC においてもプライバシ侵害などのセキュリティインシデントが発生した際の有効な資料となるなど、多くのメリットがあります。特に円滑なセキュリティ監査を実施するために必要となるデータを監査証跡と言い、以下のような構成になっています。

■監査証跡　…　監査コントロールがシステムの信頼性や安全性の確保に結びついているかを事後に実証するための手段
・トランザクション証跡（データ処理の内容や相互の処理結果を追跡できる記録と仕組み）
・アクセス証跡（資源へのアクセスについて因果関係を事後に追跡するための記録と仕組み）

監査証跡とは、いわば時系列的な多くの監査証拠（ログ）の連鎖です。監査証拠によって監査証跡が組み立てられ、その監査証跡と監査コントロールによってシステムのセキュリティおよびプライバシに関わる行動をモニタできるのです。また、セキュリティインシデントが発生した場合、監査データが医療情報を含むオリジナルデータを再構築できる唯一のものとなります。

例えば、医療情報に関わる監査証拠（ログ）には以下のようなものがあります。
・画像、データ記録の入力、患者履歴、保険データなどへのアクセス
・データの編集（変更、更新など）
・データ移動（ネットワークや電子媒体を介したデータエクスポート）
・データの印刷
・データの削除
・ユーザのログイン、ログアウトの成功と失敗
・ウイルス検出

具体的に監査証跡は、誰が、いつ、何を、どのシステムで実施したかを記録することを目的とします。ここで注意することは、ネットワーク上のデータを収集するだけではその量は膨大なものとなってしまい、効果的な監査が出来なくなる恐れがあることです。収集するデータの質と量をコントロールすることも必要となってきます。すなわち、追跡可能な記録または証拠が監査証跡の要件であることから、一連の追加情報のない、事象そのものだけの監査証跡にはほとんど価値はありません。時間やユーザ情報などの具体的データが必要となります。

さて、このようにして作成された監査証跡の保存はどのようにすればよいのでしょうか。

監査証跡の性質上、限られた人だけのアクセスに限定することが重要となってきます。この監査証跡へのアクセス管理は、通常のアクセス管理機構と同様のものでなければなりません。同時に、監査証跡は累積データであることから、変更を許すものであってはならないのです。また、保存期間については業務上の有用性や法的な要件で大きく差があり、HCF/RSC ともに異なるポリシをとる可能性があります。これらの問題に対しては、セキュリティポリシのマッピングを行う際に十分に吟味されなければなりません。

細かに設計された監査コントロールであっても、それらはセキュリティ違反やプライバシ侵害を検出するだけであり、それらは既に起きてしまったインシデントのデータであることを認識していなければなりません。セキュリティ監査からの改善勧告をどのようにシステムに反映させていくか、が重要なプロセスです。

第６章　リモートサービスセキュリティの実際の運用

第５章において文書化された運用実施規程にしたがって実際の運用を行っていきます。このとき必要に応じて手順書、指示書、マニュアルなども作成し、確実に運用が行なわれるようにしてください。

また、運用結果を記録（証跡）として残しておかなくてはいけません。どのようなものを記録するかはセキュリティポリシや、それに基づく運用実施規程により決められます。これらの記録は、ISMS が確実にかつ効率的に運用されたことの証拠になります。記録の様式は紙媒体であっても電子媒体であってもかまいませんが、電子媒体の場合、情報セキュリティの観点から機密性、完全性、可用性に留意して管理しておかなければいけません。

第７章　第三者機関を利用した公的監査の推進

「情報セキュリティ監査」とは、企業や政府などの情報セキュリティ対策について、専門的知識を有する人が客観的に評価を行う手法です。情報セキュリティ監査は専門性の高い分野であることから、自らの対策を行うことが重要であるとともに外部の専門家を有効に活用することも重要です。外部監査を導入することでより確実な情報セキュリティマネジメントを実現できます。外部監査には以下のようなメリットがあります。

（１）自らでは気付きにくい情報セキュリティの欠陥の指摘を受けることが可能

的確な内部監査体制を構築していても、内部監査スタッフに十分な情報セキュリティやシステム監査に対する知識が備わっていないことも考えられます。知識不足や経験不足による見落としや誤りを避けるために、専門的知識を持った外部スタッフによる監査を行うことが有効です。

（２）自らでは構築が難しい「情報セキュリティマネジメント」の確立が可能

ISMSの適切な運用という視点からは「自己満足的な運用」に陥らないことが重要です。専門家による外部監査を活用し、セキュリティマネジメントそのものに対する適正化のための指摘を受けることも非常に有効です。

（３）第三者（他の医療機関や患者など）に対しての信頼の獲得

内部監査だけで「本当に正しく運用が行われている」ことを証明することは非常に難しいため、何らかの第三者評価が必要です。勿論、ISMS全体について認証を受けることが最も効果的ですが、ISMSの認証取得は非常に高いハードルであり簡単には取得できません。しかし、ISMSの認証取得のためのステップとしても外部監査を受けることは有効であり対外的な評価や信頼につながるといえます。

外部監査を行うためには「情報セキュリティ管理基準」を策定する必要があります。外部監査を行うということであれば「情報セキュリティ管理基準」は国際的に採用されている策定プロセスに準拠していることが望ましく、その規範を2002年度版BS7799に求めることは有用です。適切な監査ルールに基づき外部監査を実施することは、ISMSの認証取得にもつながるため、個人情報保護などの観点から社会的評価を得ることを目指す組織であれば積極的に外部監査を採用することを推奨します。

第８章　本ガイドの技術的・制度的変化への対応

本ガイドは、2003 年 3 月時点でのセキュリティに関する技術状況および法令をはじめとする個人情報保護に関する制度において、適用しうるガイドとして制定しました。

セキュリティの技術に関しては、セキュリティを守る側とそれを破ろうとする側とのせめぎ合いの様相を呈しており、お互いに相手の技術を超えようとすることが行われており、技術的対策はより高度なものへと進んで行かざるを得ません。また、法制度についても、それらの状況の変化に応じて改訂が行われる可能性があります。

本ガイドは特定の技術に依存したガイドラインではありませんので、技術の変化に伴って適用できなくなるものではありませんが、技術的・制度的な変化が大きい場合には、見直す必要が生じると考えられます。このため、本ガイドの内容については適宜見直し、必要に応じて改訂を行っていきます。

付録

付録１　リスク分析（例）

１．RSC 機器

（１）資産

メモリ・ディスク・画面上の PHI

メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

メモリ・ディスク・画面上の PHI のバックアップ媒体

PHI を扱うソフトウェア

PHI を扱う機器

PHI を扱う機器の環境設備

（電源・防災設備を指します。但し機器、ネットワーク機器は含みません。）

PHI を扱う操作者

暗号アルゴリズムと鍵と鍵配送方式（VPN 対策実施の場合）

（２）脅威

（A）メモリ・ディスク・画面上の PHI

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
11	オンサイトでの削除忘れ C、覗き見 C/盗用 C、RSC 機器の不正ログイン C/成りすまし C による暴露 C
12	経路からの盗用 C、RSC 機器の不正ログイン C/成りすまし C による暴露 C

（B）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
13	修理の都合で記録を残した紙の覗き見 C、持出 C による暴露 C

（C）メモリ・ディスク・画面上の PHI のバックアップ媒体

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
14	修理の都合で記録した媒体の持出 C による暴露 C

（D）PHI を扱うソフトウェア

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
15	バックドアや情報を盗み出すプログラムの挿入 I による暴露 C

（E）PHI を扱う機器

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
16	持出 C、タンパリング C、漏洩電磁波 C による暴露 C
17	故障 A、被災 A、破壊 A によるサービス不能 A

（F）PHI を扱う機器の環境設備

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
18	故障 A、被災 A、破壊 A によるサービス不能 A

（G）PHI を扱う操作者

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
19	収賄による暴露 C、誤入力 I、誤消去 A によるサービス障害 A

（H）暗号アルゴリズムと鍵と鍵配送方式

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
1a	暗号化データの解読 C による暴露 C

（3）脆弱性

（A）メモリ・ディスク・画面上の PHI

RSC 側当事者以外のオンサイトでの脆弱性

●リスク番号 1000

（脆弱性）オンサイトでの第３者、RSC 社員、RSC ネットワーク管理者による、画面の覗き見 C や RSC 機器の辞書攻撃等を用いた不正ログイン C や漏洩パスワードを用いた成りすまし C が行われると、（脅威）PHI の暴露 C に繋がります。

RSC 側当事者のオンサイトでの脆弱性

●リスク番号 1001

（脆弱性)オンサイトでの RSC サービスマンによる RSC 機器内 PHI の盗用 C が行われると、（脅威）暴露 C に繋がります。

●リスク番号 1002

（脆弱性）オンサイトでの RSC サービスマンによる PHI の削除忘れ C があると、PHI の（脅威）想定外の暴露 C に繋がります。

外部経路からの脆弱性

●リスク番号 1010

（脆弱性）外部経路からの全ての者による RSC 機器の辞書攻撃等を用いた不正ログイン C や漏洩パスワードを用いた成りすまし C が行われると、RSC 機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

内部経路（RSC ネットワーク管理者以外から）の脆弱性

●リスク番号 1011

（脆弱性）内部経路からの第３者、RSC 社員、RSC ネットワーク管理者による RSC 機器の辞書攻撃等を用いた不正ログイン C が行われると、RSC 機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 1012

（脆弱性）内部経路からの第３者、RSC 社員、RSC ネットワーク管理者による RSC 機器の漏洩パスワードを用いた成りすまし C が行われると、RSC 機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

内部経路（RSC ネットワーク管理者から）の脆弱性

●リスク番号 1013

（脆弱性)内部経路からの RSC サービスマンによる RSC 機器内 PHI の盗用 C が行われると、（脅威）暴露 C に繋がります。

（Ｂ）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

RSC 当事者以外のオンサイトでの脆弱性

●リスク番号 1100

（前提）修理の都合または分離不可で当該資産を残した時、（脆弱性）第３者、RSC 社員、RSC ネットワーク管理者による覗き見 C、持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

RSC 側当事者のオンサイト

●リスク番号 1101

（前提）修理の都合または分離不可で当該資産を残した時、（脆弱性）RSC サービスマンによる持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

（Ｃ）メモリ・ディスク・画面上の PHI のバックアップ媒体

RSC 側当事者以外のオンサイトでの脆弱性

●リスク番号 1200

（前提）修理の都合または分離不可で当該資産を残した時、（脆弱性）第３者、RSC 社員、RSC ネットワーク管理者による持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

RSC 側当事者のオンサイトでの脆弱性

●リスク番号 1201

（前提）修理の都合または分離不可で当該資産を残した時、（脆弱性）RSC サービスマンによる持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

（Ｄ）PHI を扱うソフトウェア

SPC 対象範囲外ですが、以下の脆弱性の例があります。

●リスク番号 1300（SPC 対象範囲外）

（脆弱性）バックドアや情報を盗み出すプログラムが挿入 I されると、PHI の（脅威）暴露 C に繋がります。

（Ｅ）PHI を扱う機器

SPC 対象範囲外であるが、以下の脆弱性の例があります。

●リスク番号 1400（SPC 対象範囲外）

（脆弱性）RSC サービスマン以外の者による RSC 機器やそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 1401（SPC 対象範囲外）

（脆弱性）RSC サービスマンによる RSC 機器やそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 1402（SPC 対象範囲外）
（脆弱性）RSC 機器がタンパリング C されると、PHI の（脅威）想定外の暴露 C に繋がります。
●リスク番号 1403（SPC 対象範囲外）
（脆弱性）RSC 機器の漏洩電磁波が解析 C されると、PHI の（脅威）暴露 C に繋がります。
●リスク番号 1410（SPC 対象範囲外）
（脆弱性）RSC 機器が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。
●リスク番号 1411（SPC 対象範囲外）
（脆弱性）RSC 機器が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。
●リスク番号 1412（SPC 対象範囲外）
（脆弱性）RSC 機器が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（F）PHI を扱う機器の環境設備
SPC 対象範囲外ですが、以下の脆弱性の例があります。
●リスク番号 1500（SPC 対象範囲外）
（脆弱性）RSC 機器の環境設備が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。
●リスク番号 1501（SPC 対象範囲外）
（脆弱性）RSC 機器の環境設備が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。
●リスク番号 1502（SPC 対象範囲外）
（脆弱性）RSC 機器の環境設備が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（G）PHI を扱う操作者
SPC 対象範囲外ですが、以下の脆弱性の例があります。
●リスク番号 1600（SPC 対象範囲外）
（脆弱性）収賄 C が行われると、PHI の（脅威）暴露 C に繋がります。
●リスク番号 1601（SPC 対象範囲外）
（脆弱性）誤入力 I、誤消去 A が行われると、リモートサービスの（脅威）サービス障害 A に繋がります。

（H）暗号アルゴリズムと鍵と鍵配送方式
（内部経路の VPN 対策をしている場合）
●リスク番号 1700
（脆弱性）暗号アルゴリズムや鍵や鍵配送方式の強度が不足 C していると、暗号化データが解読され PHI の（脅威）暴露 C に繋がります。

２．RSC 内部ネットワーク

（１）資産

・RSC 内部ネットワークの PHI
・上記通信トレースのメモやプリントアウトの紙
・上記通信トレースのバックアップ媒体
・ネットワーク機器のソフトウェア
・ネットワーク機器
・ネットワーク機器の環境整備
・ネットワーク機器の操作者
・暗号アルゴリズムと鍵と鍵配送方式（VPN 対策実施の場合）

（２）脅威

（A）RSC 内部ネットワークの PHI

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
21	経路の覗き見 C、RSC 側ネットワーク機器の不正ログイン C／成りすまし C、タッピング C による暴露 C

（B）通信トレースのメモやプリントアウトの紙

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
22	監視記録紙の覗き見 C、持出 C による暴露 C

（C）通信トレースのバックアップ媒体

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
23	監視記録媒体の持出 C による暴露 C

（D）ネットワーク機器のソフトウェア

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
24	バックドアや情報を盗み出すプログラムの挿入 I による暴露 C

（E）ネットワーク機器

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
25	持出 C、タンパリング C、漏洩電磁波 C による暴露 C
26	故障 A、被災 A、破壊 A によるサービス不能 A

（F）ネットワーク機器の環境整備

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
27	故障 A、被災 A、破壊 A、ケーブル不通 A によるサービス不能 A

（G）ネットワーク機器の操作者

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
28	収賄による暴露 C、誤設定 C による暴露 C

（H）暗号アルゴリズムと鍵と鍵配送方式

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
29	暗号化データの解読 C による暴露 C

（３）脆弱性

（A）RSC 内部ネットワークの PHI

外部経路からの脆弱性

●リスク番号 2000

（脆弱性）外部経路からの全ての者による RSC 側ネットワーク機器の辞書攻撃等を用いた不正ログイン C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 2001

（脆弱性）外部経路からの全ての者による RSC 側ネットワーク機器の漏洩パスワードを用いた成りすまし C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

RSC ネットワーク管理者以外の内部経路からの脆弱性

●リスク番号 2002

（脆弱性）内部経路からの RSC ネットワーク管理者以外の者による RSC 側ネットワーク機器の辞書攻撃等を用いた不正ログイン C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 2003

（脆弱性）内部経路からの RSC ネットワーク管理者以外の者による RSC 側ネットワーク機器の漏洩パスワードを用いた成りすまし C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 2004

（脆弱性）内部経路からの RSC ネットワーク管理者以外の者による RSC 側経路のタッピング C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

RSC ネットワーク管理者の内部経路からの脆弱性

●リスク番号 2005

（脆弱性）内部経路からの RSC ネットワーク管理者による RSC 側経路のタッピング C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 2006

（脆弱性）RSC ネットワーク管理者による RSC 側ネットワーク機器経由の覗き見 C が行われると、RSC 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

（B）通信トレースのメモやプリントアウトの紙

RSC 側当事者以外のオンサイトでの脆弱性

●リスク番号 2100

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）RSC ネットワーク管理者以外の者による覗き見 C、持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

RSC 側当事者のオンサイトでの脆弱性

●リスク番号 2101

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）RSC ネットワーク管理者による持出 C が行われると、PHI の（脅威）暴露 C に繋がります

（C）通信トレースのバックアップ媒体

RSC 側当事者以外のオンサイトでの脆弱性

●リスク番号 2200

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）RSC ネットワーク管理者以外による持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

RSC 側当事者のオンサイトでの脆弱性

●リスク番号 2201

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）RSC ネットワーク管理者による持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

（D）ネットワーク機器のソフトウェア

SPC 対象範囲外であるが、以下の脆弱性の例があります。

●リスク番号 2300（SPC 対象範囲外）

（脆弱性）バックドアや情報を盗み出すプログラムが挿入 I されると、PHI の（脅威）暴露 C に繋がります。

（E）ネットワーク機器

SPC 対象範囲外であるが、以下の脆弱性の例があります。

●リスク番号 2400（SPC 対象範囲外）

（脆弱性）RSC ネットワーク管理者以外の者による RSC 側ネットワーク機器やメールサーバ及びそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 2401（SPC 対象範囲外）

（脆弱性）RSC ネットワーク管理者による RSC 側ネットワーク機器やメールサーバおよびそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 2402（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器がタンパリング C されると、PHI の（脅威）想定外の暴露 C に繋がります。

●リスク番号 2403（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器やケーブルの漏洩電磁波が解析 C される

と、PHI の（脅威）暴露 C に繋がります。

●リスク番号 2410（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 2411（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 2412（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（F）ネットワーク機器の環境整備

SPC 対象範囲外であるが、以下の脆弱性の例があります。

●リスク番号 2500（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器の環境設備が故障 A したり、ケーブルが不通 A となったりすると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 2501（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器の環境設備が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 2502（SPC 対象範囲外）

（脆弱性）RSC 側ネットワーク機器の環境設備が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（G）ネットワーク機器の操作者

SPC 対象範囲外であるが、以下の脆弱性の例があります。

●リスク番号 2600（SPC 対象範囲外）

（脆弱性）収賄 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 2601（SPC 対象範囲外）

（脆弱性）誤設定 C が行われると、PHI の（脅威）想定外の暴露 C に繋がります。

（H）暗号アルゴリズムと鍵と鍵配送方式

（内部経路の VPN 対策をしている場合）

●リスク番号 2700

（脆弱性）暗号アルゴリズムや鍵や鍵配送方式の強度が不足 C していると、暗号化データが解読され PHI の（脅威）暴露 C に繋がります。

３．外部ネットワーク

（１）資産

・外部ネットワーク上の PHI

・上記通信トレースのメモやプリントアウトの紙

・上記通信トレースのバックアップ媒体

・ネットワーク機器のソフトウェア
・ネットワーク機器
・ネットワーク機器の環境整備（電源・防災設備を指す。）
・ネットワーク機器の操作者
・暗号アルゴリズムと鍵と鍵配送方式 (VPN 対策実施の場合)

（２）脅威

（A）外部ネットワーク上の PHI

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
31	前提としている VPN 対策有りのため、脅威は無視可能

（B）通信トレースのメモやプリントアウトの紙

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
32	前提としている VPN 対策有りのため、脅威は無視可能

（C）通信トレースのバックアップ媒体

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
33	前提としている VPN 対策有りのため、脅威は無視可能

（D）ネットワーク機器のソフトウェア

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
34	前提としている VPN 対策有りのため、脅威は無視可能

（E）ネットワーク機器

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
35	前提としている VPN 対策有りのため、無視可能
36	故障 A、被災 A、破壊 A によるサービス不能 A

（F）ネットワーク機器の環境整備

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
37	故障 A、被災 A、破壊 A、ケーブル不通 A によるサービス不能 A

（G）ネットワーク機器の操作者

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
38	前提としている VPN 対策有りのため、無視可能

（H）暗号アルゴリズムと鍵と鍵配送方式

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
39	暗号化データの解読 C による暴露 C

（３）脆弱性

（Ａ）外部ネットワーク上の PHI

前提（VPN 対策）により脅威は無視できるため省略します。

（Ｂ）上記通信トレースのメモやプリントアウトの紙

前提（VPN 対策）により脅威は無視できるため省略します。

（Ｃ）上記通信トレースのバックアップ媒体

前提（VPN 対策）により脅威は無視できるため省略します。

（Ｄ）ネットワーク機器のソフトウェア

前提（VPN 対策）により脅威は無視できるため省略します。

（Ｅ）ネットワーク機器

●リスク番号 3000

（脆弱性）ISP 側ネットワーク機器が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 3001

（脆弱性）ISP 側ネットワーク機器が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 3002

（脆弱性）ISP 側ネットワーク機器が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（Ｆ）ネットワーク機器の環境整備

●リスク番号 3100

（脆弱性）ISP 側ネットワーク機器の環境設備が故障 A したり、ケーブルが不通 A となったりすると、リモートサービスの（脅威）サービス不能 A に繋がる。

●リスク番号 3101

（脆弱性）ISP 側ネットワーク機器の環境設備が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 3102

（脆弱性）ISP 側ネットワーク機器の環境設備が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（Ｇ）ネットワーク機器の操作者

前提（VPN 対策）により脅威は無視できるため省略します。

（Ｈ）暗号アルゴリズムと鍵と鍵配送方式

（内部経路の VPN 対策をしている場合）

●リスク番号 3200

（脆弱性）暗号アルゴリズムや鍵や鍵配送方式の強度が不足 C していると、暗号化データが解読され PHI の（脅威）暴露 C に繋がります。

４．HCF 内部ネットワーク

（１）資産

・HCF 内部ネットワーク上の PHI
・上記通信トレースのメモやプリントアウトの紙
・上記通信トレースのバックアップ媒体
・ネットワーク機器のソフトウェア
・ネットワーク機器
・ネットワーク機器の環境整備（電源・防災設備を指す。）
・ネットワーク機器の操作者

（２）脅威

（A）HCF 内部ネットワーク上の PHI

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
41	経路の覗き見 C、HCF 側ネットワーク機器の不正ログイン C/成りすまし C、タッピング C による暴露 C

（B）通信トレースのメモやプリントアウトの紙

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
42	監視記録紙の覗き見 C、持出 C による暴露 C

（C）通信トレースのバックアップ媒体

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
43	監視記録媒体の持出 C による暴露 C

（D）ネットワーク機器のソフトウェア

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
44	バックドアや情報を盗み出すプログラムの挿入 I による暴露 C

（E）ネットワーク機器

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
45	持出 C、タンパリング C、漏洩電磁波 C による暴露 C
46	故障 A、被災 A、破壊 A によるサービス不能 A

（F）ネットワーク機器の環境整備

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
47	故障 A、被災 A、破壊 A、ケーブル不通 A によるサービス不能 A

（G）ネットワーク機器の操作者

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
48	収賄による暴露 C、誤設定 C による暴露 C

（3）脆弱性

（A）HCF 内部ネットワーク上の PHI

外部経路からの脆弱性

●リスク番号 4000（SPC 対象範囲外）

SPC 対象範囲外であるが、以下の脆弱性の例があります。

（脆弱性）外部経路からの他社 RSC 当事者を含む RSC 当事者以外の者による HCF 側ネットワーク機器の辞書攻撃等を用いた不正ログイン C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 4001（SPC 対象範囲外）

SPC 対象範囲外であるが、以下の脆弱性の例があります。

（脆弱性）外部経路からの他社 RSC 当事者を含む RSC 当事者以外の者による HCF 側ネットワーク機器の漏洩パスワードを用いた成りすまし C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 4002

（脆弱性）外部経路からの他社 RSC サービスマン、RSC サービスマンによる HCF 側ネットワーク機器の辞書攻撃等を用いた不正ログイン C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

内部経路（HCF ネットワーク管理者以外から）の脆弱性

SPC 対象範囲外ですが、以下の脆弱性の例があります。

●リスク番号 4003（SPC 対象範囲外）

（脆弱性）内部経路からの HCF ネットワーク管理者以外の者による HCF 側ネットワーク機器の辞書攻撃等を用いた不正ログイン C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 4004（SPC 対象範囲外）

（脆弱性）内部経路からの HCF ネットワーク管理者以外の者による HCF 側ネットワーク機器の漏洩パスワードを用いた成りすまし C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 4005（SPC 対象範囲外）

（脆弱性）内部経路からの HCF ネットワーク管理者以外の者による HCF 側経路のタッピング C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

内部経路（HCF ネットワーク管理者から）の脆弱性

SPC 対象範囲外ですが、以下の脆弱性の例があります。

●リスク番号 4006（SPC 対象範囲外）

（脆弱性）内部経路からの HCF ネットワーク管理者による HCF 側経路のタッ

ピング C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 4007（SPC 対象範囲外）

（脆弱性）HCF ネットワーク管理者による HCF 側ネットワーク機器経由の覗き見 C が行われると、HCF 側経路上の PHI が盗用 C され（脅威）暴露 C に繋がります。

（B）上記通信トレースのメモやプリントアウトの紙

●リスク番号 4100（SPC 対象範囲外）

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）HCF ネットワーク管理者以外による覗き見 C、持出 C が行われると、（脅威）PHI の暴露 C に繋がります。

●リスク番号 4101（SPC 対象範囲外）

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）HCF ネットワーク管理者による持出Cが行われると、（脅威）PHIの暴露Cに繋がります。

（C）上記通信トレースのバックアップ媒体

●リスク番号 4200（SPC 対象範囲外）

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）HCF ネットワーク管理者以外による持出 C が行われると、（脅威）PHI の暴露 C に繋がります。

●リスク番号 4201（SPC 対象範囲外）

（前提）監視または修理の都合で当該資産を残した時、（脆弱性）HCF ネットワーク管理者による持出Cが行われると、（脅威）PHIの暴露Cに繋がります。

（D）ネットワーク機器のソフトウェア

●リスク番号 4300（SPC 対象範囲外）

（脆弱性）バックドアや情報を盗み出すプログラムが挿入 I されると、PHI の（脅威）暴露 C に繋がります。

（E）ネットワーク機器

●リスク番号 4400（SPC 対象範囲外）

（脆弱性）HCF ネットワーク管理者以外の者による HCF 側ネットワーク機器やメールサーバ及びそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 4401（SPC 対象範囲外）

（脆弱性）HCF ネットワーク管理者による HCF 側ネットワーク機器やメールサーバ及びそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 4402（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器がタンパリング C されると、PHI の（脅威）想定外の暴露 C に繋がります。

●リスク番号 4403（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器やケーブルの漏洩電磁波が解析 C される

と、PHI の（脅威）暴露 C に繋がります。

●リスク番号 4410（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 4411（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 4412（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（F）ネットワーク機器の環境整備

●リスク番号 4500（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器の環境設備が故障 A したり、ケーブルが不通 A となったりすると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 4501（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器の環境設備が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 4502（SPC 対象範囲外）

（脆弱性）HCF 側ネットワーク機器の環境設備が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（G）ネットワーク機器の操作者

●リスク番号 4600（SPC 対象範囲外）

（脆弱性）収賄 C が行われると、（脅威）PHI の暴露 C に繋がります。

●リスク番号 4601（SPC 対象範囲外）

（脆弱性）誤設定 C が行われると、PHI の（脅威）想定外の暴露 C に繋がります。

５．HCF 保守対象機器

（１）資産

・メモリ・ディスク・画面上の PHI

・メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

（持ち込んだドキュメントや媒体は対象外）

・メモリ・ディスク・画面上の PHI のバックアップ媒体

（持ち込んだドキュメントや媒体は対象外）

・PHI を扱うソフトウェア

・PHI を扱う機器

・PHI を扱う機器の環境設備

（電源・防災設備を指します。但し機器、ネットワーク機器は含みません。）

・PHI を扱う操作者

・暗号アルゴリズムと鍵と鍵配送方式

（２）脅威

（A）メモリ・ディスク・画面上の PHI

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
51	オンサイトでの削除忘れ C、覗き見 C/盗用 C、保守対象機器の不正ログイン C/成りすまし C、差換え I による暴露 C、ねつ造 I
52	経路からの盗用 C、保守対象機器の不正ログイン C/成りすまし C、差換え I による暴露 C、ねつ造 I

（B）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
53	業務で記録を残した紙の覗き見 C、持出 C、差換え I による暴露 C、ねつ造 I

（C）メモリ・ディスク・画面上の PHI のバックアップ媒体

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
54	業務で記録した媒体の持出 C、差換え I による暴露 C、ねつ造 I

（D）PHI を扱うソフトウェア

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
55	バックドアや情報を盗み出すプログラムの挿入 I による暴露 C

（E）PHI を扱う機器

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
56	差換え I、持出 C、タンパリング C、漏洩電磁波 C によるねつ造 I、暴露 C
57	故障 A、被災 A、破壊 A によるサービス不能 A

（F）PHI を扱う機器の環境設備

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
58	故障 A、被災 A、破壊 A によるサービス不能 A

（G）PHI を扱う操作者

脅威番号	脅威（C:機密性、I:完全性、A:可用性）
59	収賄による暴露 C、誤入力 I、誤消去 A によるサービス障害 A

（３）脆弱性

（A）メモリ・ディスク・画面上の PHI

HCF 側当事者以外のオンサイトでの脆弱性

●リスク番号 5000（SPC 対象範囲外）

（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマンによる保守対象機器の辞書攻撃等を用いた不正ログイン C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5001（SPC 対象範囲外）

（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマンによる保守対象機器の漏洩パスワードを用いた成りすまし C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5002（SPC 対象範囲外）

（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマンによる画面の覗き見 C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります

HCF 側当事者のオンサイトでの脆弱性

●リスク番号 5003（SPC 対象範囲外）

（脆弱性）オンサイトでの一次サービスマンによる保守対象機器内 PHI の盗用 C が行われると、（脅威）暴露 C に繋がります。

●リスク番号 5004（SPC 対象範囲外）

（脆弱性）オンサイトでの一次サービスマンによる保守対象機器内 PHI の差換え I が行われると、（脅威）ねつ造 I に繋がります。

●リスク番号 5005（SPC 対象範囲外）

（脆弱性）オンサイトでの HCF システム管理者による保守対象機器内 PHI の盗用 C、差換え I が行われると、（脅威）暴露 C、ねつ造 I に繋がります。

●リスク番号 5006（SPC 対象範囲外）

（脆弱性）オンサイトでの医師等による保守対象機器内 PHI の盗用 C、差換え I が行われると、（脅威）暴露 C、ねつ造 I に繋がります。

外部経路（RSC 側当事者以外）からの脆弱性

●リスク番号 5010（(SPC 対象範囲外）

（脆弱性）外部経路からの RSC 側当事者以外の者による保守対象機器の辞書攻撃等を用いた不正ログイン C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5011（SPC 対象範囲外）

（脆弱性）外部経路からの RSC 側当事者以外の者による保守対象機器の漏洩パスワードを用いた成りすまし C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

外部経路（RSC 側当事者）からの脆弱性

●リスク番号 5012

（脆弱性）外部経路からの他社 RSC サービスマンによる保守対象機器の辞書攻撃等を用いた不正ログイン C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5013

（脆弱性）外部経路からの他社 RSC サービスマンによる保守対象機器の漏洩パスワードを用いた成りすまし C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5014

（脆弱性）外部経路からの RSC サービスマンによる保守対象機器内 PHI の盗用 C が行われると、（脅威）暴露 C に繋がります。

●リスク番号 5015

（脆弱性）外部経路からの RSC サービスマンによる保守対象機器内 PHI の差換え I が行われると、（脅威）ねつ造 I に繋がります。

内部経路の脆弱性

●リスク番号 5016（SPC 対象範囲外）

（脆弱性）内部経路からの第３者、HCF 職員、HCF ネットワーク管理者による保守対象機器の辞書攻撃等を用いた不正ログイン C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5017（SPC 対象範囲外）

（脆弱性）内部経路からの第３者、HCF 職員、HCF ネットワーク管理者による保守対象機器の漏洩パスワードを用いた成りすまし C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります。

●リスク番号 5018（SPC 対象範囲外）

（脆弱性）内部経路からの医師等、HCF システム管理者、一次サービスマンによる保守対象機器内 PHI の盗用 C、差換え I が行われると、（脅威）暴露 C、ねつ造 I に繋がります。

（Ｂ）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

医師等以外からの脆弱性

●リスク番号 5100（SPC 対象範囲外）

（前提）医師等が業務で当該資産を残した時、（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマン、一次サービスマン、HCF システム管理者による覗き見 C、持出 C が行われると、（脅威）PHI の暴露 C に繋がります。

医師等からの脆弱性

●リスク番号 5101（SPC 対象範囲外）

（脆弱性）オンサイトでの医師等による持出 C、差換え I が行われると、（脅威）PHI の暴露 C、ねつ造 I に繋がります。

（Ｃ）メモリ・ディスク・画面上の PHI のバックアップ媒体

医師等以外からの脆弱性

●リスク番号 5200（SPC 対象範囲外）

（前提）医師等が業務で当該資産を残した時、（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマン、一次サービスマン、HCF システム管理者による持出 C が行われると、（脅威）PHI の暴

露 C に繋がります。

医師等からの脆弱性

●リスク番号 5201（SPC 対象範囲外）

（脆弱性）オンサイトでの医師等による持出 C、差換え I が行われると、（脅威）PHI の暴露 C、ねつ造 I に繋がります。

（D）PHI を扱うソフトウェア

●リスク番号 5300（SPC 対象範囲外）

（脆弱性）バックドアや情報を盗み出すプログラムが挿入 I されると、PHI の（脅威）暴露 C に繋がります。

（E）PHI を扱う機器

●リスク番号 5400（SPC 対象範囲外）

（脆弱性）HCF システム管理者以外の者による保守対象機器やそのディスクの持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 5401（SPC 対象範囲外）

（脆弱性）HCF システム管理者による保守対象機器やそのディスクの持出 C、差換え I が行われると、PHI の（脅威）暴露 C、ねつ造 I に繋がります。

●リスク番号 5402（SPC 対象範囲外）

（脆弱性）保守対象機器がタンパリング C されると、PHI の（脅威）想定外の暴露 C に繋がります。

●リスク番号 5403（SPC 対象範囲外）

（脆弱性）保守対象機器の漏洩電磁波が解析 C されると、PHI の（脅威）暴露 C に繋がります。

●リスク番号 5410（SPC 対象範囲外）

（脆弱性）保守対象機器が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 5411（SPC 対象範囲外）

（脆弱性）保守対象機器機器が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 5412（SPC 対象範囲外）

（脆弱性）保守対象機器機器が破壊 A されると、リモートサービスの（脅威）サービス不能 A に繋がります。

（F）PHI を扱う機器の環境設備

●リスク番号 5500（SPC 対象範囲外）

（脆弱性）保守対象機器の環境設備が故障 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 5501（SPC 対象範囲外）

（脆弱性）保守対象機器の環境設備が被災 A すると、リモートサービスの（脅威）サービス不能 A に繋がります。

●リスク番号 5502（SPC 対象範囲外）

（脆弱性）保守対象機器の環境設備が破壊 A されると、リモートサービスの（脅

威）サービス不能 A に繋がります。

（G）PHI を扱う操作者

●リスク番号 5600（SPC 対象範囲外）

（脆弱性）収賄 C が行われると、（脅威）PHI の暴露 C に繋がります。

●リスク番号 5601（SPC 対象範囲外）

（脆弱性）誤入力 I、誤消去 A が行われると、リモートサービスの（脅威）サービス障害 A に繋がります。

付録２　情報セキュリティ監査規程作成時の留意点

１．情報セキュリティ監査の目的

情報セキュリティ監査とは、情報セキュリティの維持・向上を図るためのものであり、監査及び点検に関し、セキュリティポリシに準じた事項を定める必要があります。

２．点検

（１）点検担当者

情報セキュリティ対策に関する点検は、情報資産を取扱う人が自ら行います。情報セキュリティ責任者は、点検を担当する者（以下「点検担当者」という）を任命します。

（２）計画の立案

点検担当者は、セキュリティポリシに準じた頻度で点検の実施計画を立案します。実施計画は、（１）の情報セキュリティ責任者の承認を得る必要があります。

（３）点検の実施基準

点検担当者は、セキュリティポリシの内容のうち、該当するシステムに関連する事項を十分配慮して、点検用資料を作成します。

（４）点検の実施

点検担当者は、点検用資料の作成にあたって、医療情報システム管理部署に協力を要請することができます。また、点検資料に基づき、被監査システムのスタッフ等にアンケート等を用いた調査を行うことが望まれます。点検対象に情報システムが含まれるリモートサービスには、前述のほか、当該システムの脆弱性を検査します。

（５）報告

点検担当者は、点検終了後、点検結果報告書を作成し、被監査システムの情報セキュリティ担当者に報告します。情報セキュリティ担当者は、情報セキュリティ委員会に監査対象の点検結果を報告します。

（６）改善

情報セキュリティ担当者は、点検結果に基づいて、問題点を明確にし、それを改善します。

（７）点検の実施頻度

点検の実施頻度は、セキュリティポリシに準じたものです。

３．監査

（１）監査担当者の指名

セキュリティポリシの運用状況を監査する人（以下「監査担当者」という）は、情報セキュリティ責任者が指名する人とすることが一般です。監査担当者は、次に掲げる条件を満たす人であることが求められます。

・被監査対象と独立性を保つことのできる人
・情報システムの基本的知識を有する人
・情報セキュリティに係る監査の知識並びに実務能力を有する人

（２）監査担当者の職務倫理・守秘義務

監査担当者は、客観的な評価者としての立場を堅持しなければなりません。また、監査担当者は、自己に対する倫理的要請を自覚するとともに、的確かつ誠実な監査の実践を通じて内外の信頼に応えなければなりません。同時に、正当な理由がない限り職務上知り得た秘密を漏らし又は不当な目的に利用してはいけません。なお、監査担当者としての監査担当職務を離任後も同様です。

（３）監査担当者の責任・権限

監査担当者は、次に掲げる責任及び権限を有します。

・自らの判断に対する根拠を明確にする責任
・被監査対象に対して資料の提出を求めることのできる権限
・被監査対象へ改善勧告した事項について、その実施報告を求めることのできる権限

（４）監査の対象

監査担当者は、監査の対象を明確にしなければなりません。

監査対象は、セキュリティポリシに準じ決定します。委託先事業者においては情報システムの委託業務に係る情報セキュリティの実施状況が対象となります。

（５）被監査システム責任者の義務

被監査システムの責任者は、監査担当者の協力要請に応じなければなりません。また、監査作業の妨害、虚偽の報告及び事実の隠蔽をしてはいけません。

（６）計画の立案

監査担当者は、定期的に情報セキュリティ監査の実施計画を立案します。計画内容は、リモートサービスにテーマを限定した監査を適宜実施するものとすることができます。実施計画は、情報セキュリティ責任者の承認を得ることが必要となります。

（７）監査の実施基準

情報セキュリティ監査では、セキュリティポリシに準じたリモートサービスの運用及び情報資産の取扱が実施されていることを監査します。

（８）監査の実施

監査担当者は、一般に監査計画に基づき情報セキュリティ監査を実施します。監査

実施にあたっては、監査項目及び監査方法を明確にした監査用書類を準備します。監査実施は、被監査システムに立入り、利用者等へのヒアリング及び資料調査等により行います。

（９）報告

監査担当者は、一般に監査終了後に監査結果報告書を作成します。監査結果報告書には、監査対象、監査内容、監査結果、指摘事項及び改善勧告等を盛り込むことが大切です。監査担当者は、監査結果報告書は情報セキュリティ責任者の承認を受けます。また、監査担当者は、監査結果報告書を情報セキュリティ委員会に事後報告します。

（１０）改善

監査担当者は、一般に監査結果報告書に基き被監査部門に改善勧告を行います。被監査システムは、監査担当者より指摘を受けた事項について可及的速やかに改善されることが望まれます．また、監査担当者は、一定期間内に改善勧告について被監査システムの実施状況を確認することが一般的です。

監査担当者は、情報共有にシステム全体の情報セキュリティ維持及び向上に有効であると判断した場合、監査結果の一部を被監査対象内において公開することができます。

（１１）臨時監査

監査担当者は、情報セキュリティ責任者より特に指示を受けた場合に、臨時的に監査を行うことができます。

（１２）外部監査

監査担当者は、自らが行う監査のほか、情報セキュリティ責任者の承認を受けた場合に、外部の事業者による外部監査を実施することができます。

（１３）監査結果報告書の保管

監査担当者は、監査結果報告書を保管・保存しなければなりなせん。

（１４）監査の実施頻度

監査の実施頻度は、セキュリティポリシに準じたものです。

付録３　リモートサービスセキュリティWG　委員名簿（あいうえお順）

青木　尚　　（三菱電機）
梅澤　昭生　（横河電機）
桑野　聡　　（グッドマン）
佐藤　成樹　（富士写真フイルム）
佐藤　能行　（富士総合研究所）
篠田　英範　（東芝）
島西　聡　　（東芝医用システムエンジニアリング）
清水　学　　（グッドマン）
武智　洋　　（横河電機）
手島　文彰　（東芝）
野津　勤　　（横河電機）
西田　慎一郎（島津製作所）
原嶋　茂夫　（横河電機）
藤咲　喜丈　（日本光電）
松本　義和　（グッドマン）
茗原　秀幸　（三菱電機）
山内　香里　（横河電機）
吉村　仁　　（コニカ）

（技術文書 04-101）

リモートサービスセキュリティガイド

2004年３月

発行：(社) 日本画像医療システム工業会
セキュリティ委員会

保健医療福祉情報システム工業会
セキュリティ委員会

〒105-0001　東京都港区虎ノ門１丁目19-9
（虎の門TBLビル　6F）
TEL：03-3506-8010　FAX：03-3506-8070