JAHIS標準 06-001

Japanese Association of Healthcare Information Systems Industry

リモートサービス
セキュリティガイドライン

2006年6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

リモートサービスセキュリティガイドライン

まえがき

医療の IT 化は医事会計システム、部門システム、オーダエントリシステム、電子カルテの順に整備され、今後、電子化された医療情報は、施設間連携などの医療行為のなかでやりとりされるだけでなく、ネットワークを介してシームレスに流通することが考えられます。特に医療機関と医療機器ベンダとをネットワークで結び、医療機器の保守を安全にかつ効率的に行うためには、扱う患者データ等の個人情報の持ち出しやシステムの運用妨害などのリスクを漏れなく把握し、医療機関と医療機器ベンダ双方がセキュリティ対策を講じていかなければなりません。

このような背景の中、JAHIS セキュリティ委員会では JIRA（社団法人　日本画像医療システム工業会）セキュリティ委員会と共同でリモートサービスセキュリティ WG を発足させ、医療分野における遠隔保守（リモートサービス）のあり方と、情報セキュリティマネジメントと個人情報保護の視点からリモートサービスのリスクアセスメントを研究し、医療機関と医療機器ベンダがそれぞれどのようなセキュリティ対策を取るべきかの検討を行ってきました。2003 年度には JAHIS 技術文書「リモートサービスセキュリティガイド」を完成させました。ガイド作成当時は、医療分野における情報セキュリティの対策や個人情報保護に対する指針が明確になっていなかった為に、JAHIS 標準となるガイドラインを作成することが難しく、セキュリティの啓蒙普及活動等を目的としたガイドを作成することとなりました。しかしながら現在では、情報セキュリティ及び個人情報保護に関する法律、指針・ガイドラインが明確となり、リモートサービスセキュリティの基準として、より踏み込んだ記載を行うことが可能となりました。そこで、当リモートサービスセキュリティ WG では、リモートサービスを安全に行うための実践的なガイドラインを作成し、医療機器およびシステム内に流通する個人情報を保護するための管理手法・リスク分析と、ISMS（情報セキュリティマネジメントシステム）という考え方におけるリモートサービスのセキュリティ対策のあり方についてまとめた「リモートサービスセキュリティガイドライン」を作成しました。

ガイドラインでは下記の事項について説明しています。

１）医療分野におけるリモートサービスのリスクマネジメントの必要性と範囲
２）リモートサービスにおけるセキュリティ要件とセキュリティの基本方針
３）一般的なリモートサービスの運用モデルにおけるリスク評価と残存リスク、リスク対応
４）リモートサービスにおけるリスクコントロールの目的と管理策
５）リモートサービスにおけるセキュリティ監査のあり方

本ガイドラインは、ネットワークを介したリモートサービスを題材とし、ISMS の最新動向を加味して、医療機器ベンダがリモートサービスを実施する際の基準を示すことを目的としています。本ガイドラインは、JAHIS 標準のガイドラインであり、厚生労働省から出されている安全管理ガイドラインの内容にも従っている為、記載されているセキュリティ対策の医療機関に対する説得性も高く、本ガイドラインの内容に従ったセキュリティ対策を施すことがより望ましいといえます。本ガイドラインが普及することによって、セキュリティ対策に対しての医療機器ベンダと医療機関の間での取り決めの際の拠り所となる基準ができ、これが医療ベンダと医療機関の双方に利益をもたらすこととなれば幸いです。

２００６年６月　　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

＜＜　告知事項　＞＞

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い本ガイドラインの準拠する旨を表現することは厳禁するものとします。

本ガイドラインならびに本ガイドラインに基づいたシステムの導入・運用についてあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

発行に寄せて

年々、医療機関が使用する機器やシステムのハードウェアはますます複雑になり、ファームウェアやソフトウェアの機能も増えつつある。それにともない、その保守や修理は、それぞれのベンダに特有な専門的な高度の知識が必要になってきている。そのため、ソフトウェアや交換可能なパーツに関連した保守や修理は、医療機関から遠く離れた場所にあるサービスセンタの専門スタッフが担当するリモートサービスが検討され実施されつつある。

リモートサービスには、顧客にとっての利点がいくつかある。最も重要なのが、保守や修理のための応答時間が短縮され、機器を利用できる時間が増える点である。さらに、オンサイト保守のための訪問が減ることから、リモートサービスは顧客にコストの軽減をもたらす。もう一つ、予想外の事故によるダウンタイムを避けるための定期保守・定期監視などのサービスが可能になる。さらに診療報酬請求マスターの変更やソフトウェアのバージョンアップ等の Live-update に相当する機能も実現できる。

リモートサービスは、サービス技術者が現場を訪れることなく、保守や修理作業を行うことを意味している。医療機関内でのオンサイトの保守・修理サービスにおいてでさえ、医療機関はベンダのサービスマンは特権アカウントや隠しコマンドでシステムを自由にいじれると思っている。まして、オンラインでメンテナンスを行う場合は知らない間に診療データを抜き出しているのではないかという医療機関側の不信感を払拭するのは難しい。また、保守・修理は通常な状態ではない非定常的運用を要求するので、そうした場合でも個人情報保護や電子保存の基準を満たす必要がある。リモートサービスを成功させるには、顔の見えないサービスに対するベンダと医療機関との間に信頼関係を構築し、維持することが大事である。サービス行為や結果が見えるようにすること、つまり透明性が重要視される。

本ガイドラインは、こうした状況を改善し、ベンダが適切に保守・修理を行っていることを保証し、その説明責任を果たすために有効である。そのために、

1）2004年3月策定の「リモートサービスセキュリティガイド」を、ISMSとプライバシ保護の視点からより技術的な内容を検討し、さらに「医療・介護関係事業者における 個人情報の適切な取扱いのためのガイドライン」、「個人情報の保護に関する法律についての 経済産業分野を対象とするガイドライン」あるいは「医療情報システムの安全管理に関するガイドライン」等を考慮したガイドラインである。
2）非常に多くの時間とコストが必要となるリスク分析（リスクアセスメント全般）について、ISO/IEC17799 に則ったリスクアセスメントモデル（添付の表：産業界として想

定する標準的な業務モデルを定義）を作成し、読者に活用してもらうこと。
3）リモートサービスセンターとして行うべき対策のベースラインを提示すること。
に主眼を置いて作成されている。

本ガイドラインが準拠している個人情報のガイドライン（「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」厚生労働省）では第Ⅲ章５節「個人データの第三者提供」の（５）「その他留意事項」で、

「第三者提供を行う場合のほか、他の事業者への情報提供であっても、①法令に基づく場合など第三者提供の例外に該当する場合、②「第三者」に該当しない場合、③個人が特定されないように匿名化して情報提供する場合などにおいては、本来必要とされる情報の範囲に限って提供すべきであり、情報提供する上で必要とされていない事項についてまで他の事業者に提供することがないようにすべきである。」

とされ、また、

「第三者提供に該当しない情報提供が行われる場合であっても、院内や事業所内等への掲示、ホームページ等により情報提供先をできるだけ明らかにするとともに、患者・利用者等からの問い合わせがあった場合に回答できる体制を確保する。」と規定している。つまり、リモートサービスにおいてもその実施および医療機関側は個人情報保護に対する対策をとっていることを必要に応じ患者へ説明する責任があり、委託先の監督義務がある。ベンダは委託先としてこれに対する対応を用意しておく必要がある。

その為には、ベンダとして「リモートサービス・セキュリティマネージメント」の確立が必要である。ＰＤＣＡサイクルをまわして、新規サービスにも機敏に対応できるマネージメントが必要である。「リモートサービス・セキュリティマネージメント」を確立し、コンプライアンス・プログラムを構築するには、先ず本ガイドラインの第３章および第４章で述べられているようにベンダの「セキュリティマネージメントに対する基本方針」が重要である。基本方針としては第１章で述べている前提条件の確認が重要である。「医療機関の許可により医療機関の機器にアクセスでき、医療機関が不都合と判断した場合にはいつでも切断することが出来る」ことや、どのようなサービスを行うのかその「サービスメニュー」の公開や個人情報の使用目的の特定も必要である。患者安全への配慮も重要である。

そもそもシステムを開発する段階でリモートサービスに適した設計にすべきである。例えば故障モード解析を行い、その状態に対応するログをあるエリアに保存し、通常はそのエリアだけにしかアクセスできないソフトウェア構造にする。また、やもえず生データを必要とする場合は出来るだけ個人名等を匿名化するとか、「安全管理のガイドライン」の６．９「外部と個人情報を含む医療情報を交換する場合の安全管理」で規定しているように「秘匿性の確保のための適切な暗号化」「通信の起点・終点識別のための認証」あるいは「リモ

ートログイン制限機能」への配慮も設計当初から必要である。

次にリスク分析とその対策が重要である。リスク分析は交通事故を避ける、あるいは盗難に遭わないようにする等への注意と同様に、それなりの訓練が必要で、リモートサービス関係者はその能力を養う必要がある。これは第３章、第４章よび付録１に基づいてＩＳＭＳ手法に従い、各ベンダの設計および運用の方針にそって適用するとシステマティックに行うことができる。個人情報保護に関しては第２章２項、電子保存に対しては同３項に従い、安全管理に関しては第４章に従って行う。また、サービスで入手した個人情報は目的以外には使用しないような運用管理をおこない、保守・修理終了後は破棄すべきである。このことは守秘義務契約等のサービス契約に含めるべきである。

さらに、本ガイドラインが準拠している「医療情報システムの安全管理に関するガイドライン」の６．８ には「情報システムの改造と保守」に関する要求事項が挙げられている。これらはリモートサービスを行う際にも医療施設側に義務づけられるのでベンダは委託先としてこれに対応する必要がある。ベンダはこれにそった契約書やサービス報告書を作成する必要がある。以下に「最低限のガイドライン」と「推奨されるガイドライン」を転記する。

１）「情報システムの改造と保守」に対する最低限のガイドライン

ａ）動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。

ｂ）メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、およびアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。

ｃ）そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。

ｄ）保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。

ｅ）保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。

ｆ）保守会社と守秘義務契約を締結し、これを遵守させること。

ｇ）保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対す

る十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。

h）リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること。

i）再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。

2）情報システムの改造と保守に対する推奨されるガイドライン

a）詳細なオペレーション記録を保守操作ログとして記録すること。

b）保守作業時には病院関係者立会いのもとで行うこと。

c）作業員各人と保守会社との守秘義務契約を求めること。

d）保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。

e）保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。

こうした「リモートサービス・セキュリティマネージメントの確立」を行うために参考になるのが、プライバシーマーク制度である。プライバシーマークは、JIS Q 15001 の要求事項およびその認定指針に基づき、個人情報保護のための体制を整備している施設に対して付与される。その要求事項は個人情報を保護するために必要な規定・体制・教育・監査・苦情処理等マネジメントシステムの構築から運用までに行うべき事項を具体的に示しているので、ＰＤＣＡのサイクルをまわし、スパイラルアップすることが出来る。この指針は医療機関が、個人情報保護を具体的に取り組む場合に利用することができるが、リモートサービスを行うベンダもマークを取得することをお勧めしたい。このマーク取得により医療機関の説明責任を支援し患者の信頼も得ることが出来る。実際、システム開発ベンダがマーク取得を始めている。

本ガイドラインにより、「リモートサービス・セキュリティマネージメント」が確立され、ベンダと医療機関との間に信頼関係が構築され、リモートサービスが促進され、医療機関もベンダもメリットが享受されることを期待したい。リモートサービスではサービス技術者がフェース・ツーフェースで築いてきた医療機関との友好関係が希薄になる等の弊害もあるがＩＰ－ＴＶ電話等でカバーする等の新たなビジネスモデルの工夫も必要になる。

本ガイドラインは適宜状況に応じ見直すことになっている。今後、各ベンダがこのガイドラインにもとづき実施し、その結果がフィードバックされ改訂される予定である。例えば、各ベンダの経験を集約し「リモートサービス・セキュリティマネージメントのコンプライアンス・プログラム・チェックリスト」、「医療機関とのリモートサービス・セキュリティ契約書」あるいは「リモートサービス報告書」等の雛形が追加され本ガイドラインもスパイラルアップされていくことを望みたい。

東京工業大学
喜多　紘一

目次

第１章　リモートサービスセキュリティガイドラインの必要性

１－１．背景

e-Japan 戦略が推し進められる中、保健・医療・福祉分野においても、電子カルテ等に代表される医療機関のコンピュータ化や、オンラインでのレセプト処理などが進められています。その一方で、コンピュータ化に伴う情報の電子化によって、情報システムや組織体におけるセキュリティ対策の不備に起因する様々な問題も生じています。これらは、情報システムへの不正侵入や機密情報の漏洩、情報システムに保存されているデータの改竄や破壊といった様々な脅威に対して、情報システムや組織の脆弱性により引き起こされたものです。

このような問題の発生を防止する方法の一つとして、情報セキュリティの効果的なマネジメントシステムを構築し、PDCA サイクルに基づいて運営管理していくための国際的なガイドラインとして、ISO/IEC17799 が作成されており、金融業、製造業を始め各分野にて普及しつつあります。また、これに基づいた「ISMS 認証基準」が（財）日本情報処理開発協会（以下、JIPDEC と表示）により作成されており、これに従った医療情報分野における解釈と実装のガイドとして、2004 年 11 月に「医療機関向け ISMS ユーザーズガイド」が出されています。

また、個人情報に関する法整備が遅れていた日本においても、個人情報の保護に関する法律（以下、個人情報保護法と記述）が2005年の4月に施行され、個人情報保護への関心が高まっています。これによって、この法律に定められている内容を満たせば、個人情報を扱ってよいことが法的に認められたこととなり、従来とは違い、どのような規則に従って個人情報を取り扱えばよいかが明確になりつつあります。これを受けて、2004年6月に経済産業分野を対象とした個人情報保護に関するガイドラインである「個人情報の保護に関する法律についての経済産業分野を対象としたガイドライン」が経済産業省より発表されました。保健・医療・福祉分野では、個人情報を多く扱うばかりでなく、機微な個人情報を扱うことが多いため、個人情報保護法への対応も複雑なものとならざるをえません。こうした状況を受けて、厚生労働省から、保健・医療・福祉分野における個人情報保護の指針である「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」が2004年11月に発表されています。

さらに、医療分野における電子保存のガイドラインである、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」及び「診療録等の外部保存に関するガイドライン」についても見直しが図られ、2つのガイドラ

インの内容を見直して、1つのガイドラインとしてまとめた「医療情報システムの安全管理に関するガイドライン」が2005年3月に厚生労働省より出され、ISMSや個人情報保護の動向も考慮した形で、診療録等のデータを電子保存する場合の具体的な指針が示されることとなりました。このガイドラインでは、ベンダが通信回線を経由して行う遠隔保守（以下、リモートサービスと記述）に関しても具体的な指針が示されており、リモートサービスを実施するに際して医療機関はベンダに対して上記ガイドラインを遵守させる監督責任があります。

以上で述べたように、医療機関は医療情報システムでの個人情報保護も含めた情報セキュリティ対策について、これまで以上に厳しい対応が求められ、これら法律や指針・ガイドラインに従う必要があります。

１－２．目的

JAHIS セキュリティ委員会では JIRA（財団法人　日本画像医療システム工業会）セキュリティ委員会と共同でリモートサービスセキュリティ WG を発足させ、2003 年度に「リモートサービスセキュリティガイド」の作成を行いました。このときには、医療分野における情報セキュリティの対策や個人情報保護に対する指針が明確になっていなかった為に、ガイドラインを作成することが難しく、セキュリティの啓蒙普及活動等を目的としたガイドを作成することとなりました。しかしながら現在では、１－１にて述べた通り、情報セキュリティ及び個人情報保護に対する法律、指針・ガイドラインが明確となり、リモートサービスセキュリティの基準として、より踏み込んだ記載を行うことが可能となっています。この為、リモートサービスセキュリティ WG では、リモートサービスセキュリティの基準を記載したガイドラインの作成を行いました。

本ガイドラインでは、ネットワークを介したリモートサービスを題材とし、ISMS の最新動向を加味して、ベンダがリモートサービスを実施する際の基準を示すことを目的としています。なお、本ガイドラインは、リモートサービスに対してベンダが独自のセキュリティ対策を施すことを否定しているものではありません。但し、その場合は、医療機関に対してセキュリティ対策の正当性を説明する責任が発生することとなります。本ガイドラインは、JIRA/JAHIS の工業会により認定されたガイドラインであり、厚生労働省から出されている「医療情報システムの安全管理に関するガイドライン」の内容にも従っている為、記載されているセキュリティ対策の医療機関に対する説得性も高く、本ガイドラインの内容に従ったセキュリティ対策を施すことがより望ましいといえます。本ガイドラインが普及することによって、セキュリティ対策に対してのベンダと医療機関の間での取り決めの際の拠り所となる基準ができ、これがベンダと医療機関の双方に利益をもたらすこととなれば幸いです。

１－３．対象範囲

本ガイドラインでは、リモートサービスに関して、個人情報取扱事業者としての医療機関とリモートサービスを提供するベンダとが最低限実施すべき「組織的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」、「人的安全管理措置」について解説します。

本ガイドラインの適用は、次のことが前提となります。

- 医療機関とベンダとの間で取り交わされる委託契約書または覚書等の中に、本ガイドラインで述べる安全管理措置の内容を明記します。
- 医療機関は、リモートサービス回線のアクセスポイントとなる医療機関側のネットワーク機器を管理します。したがって、医療機関がそのネットワーク機器を操作しない限り、リモートサービス回線は利用できませんので、リモートサービス回線を経由して保守作業を行っている間のみを対象として安全管理措置が必要となります。
- 医療機関は、医療機関の保有する個人情報がリモートサービスにより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点検・確認します。

なお、本ガイドラインで述べる安全管理措置は、１－４に述べる運用モデルを前提として検討されていますので、１－４に述べる運用モデルに当てはまるらない場合には情報セキュリティマネジメントシステム(以下、ISMS と略します。Information Security Management System)の考え方に則り、リスクアセスメントの見直しを行い、自己責任において適切な安全管理措置を別途導入する必要があります。

１－４．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(Healthcare Facility)内の機器に障害が生じ、HCF 側からの連絡に基づき、RSC(Remote Service Center)側から HCF 内の保守対象機器にアクセスを行い、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、対象機器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。

それぞれのユースケースは、HCF（医療機関）内の保守対象機器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１－４－１）

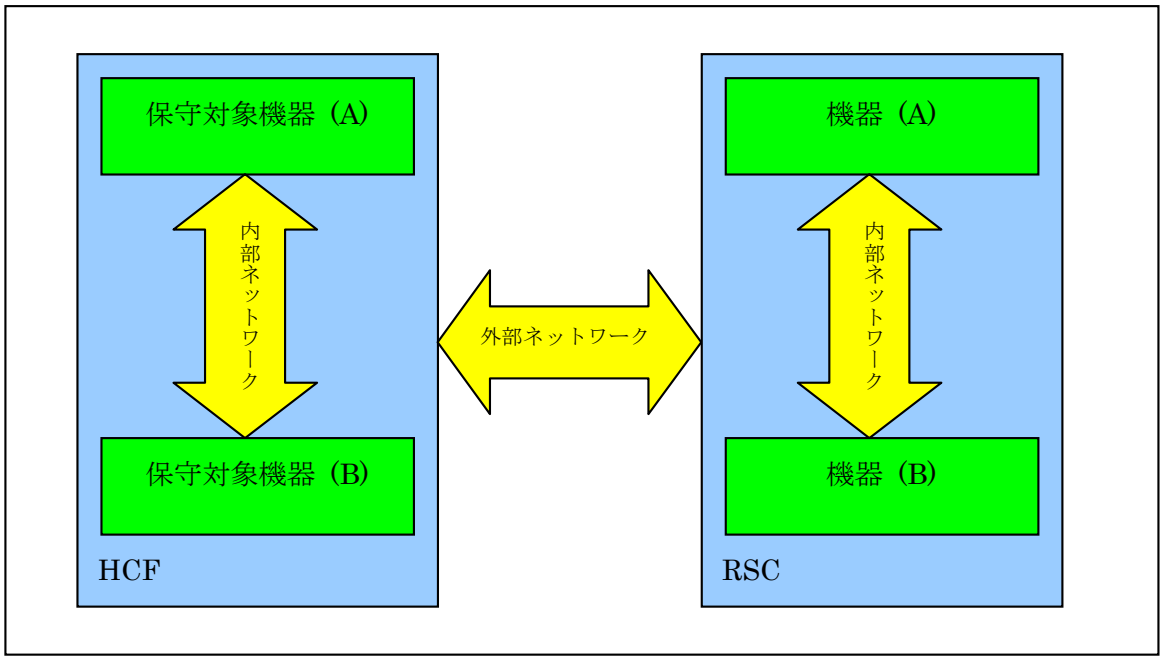

図１－４－１　リモートサービスのシステムの想定

１－４－１．故障時の対応

故障時の対応におけるワークフローを図１－４－２に示します。

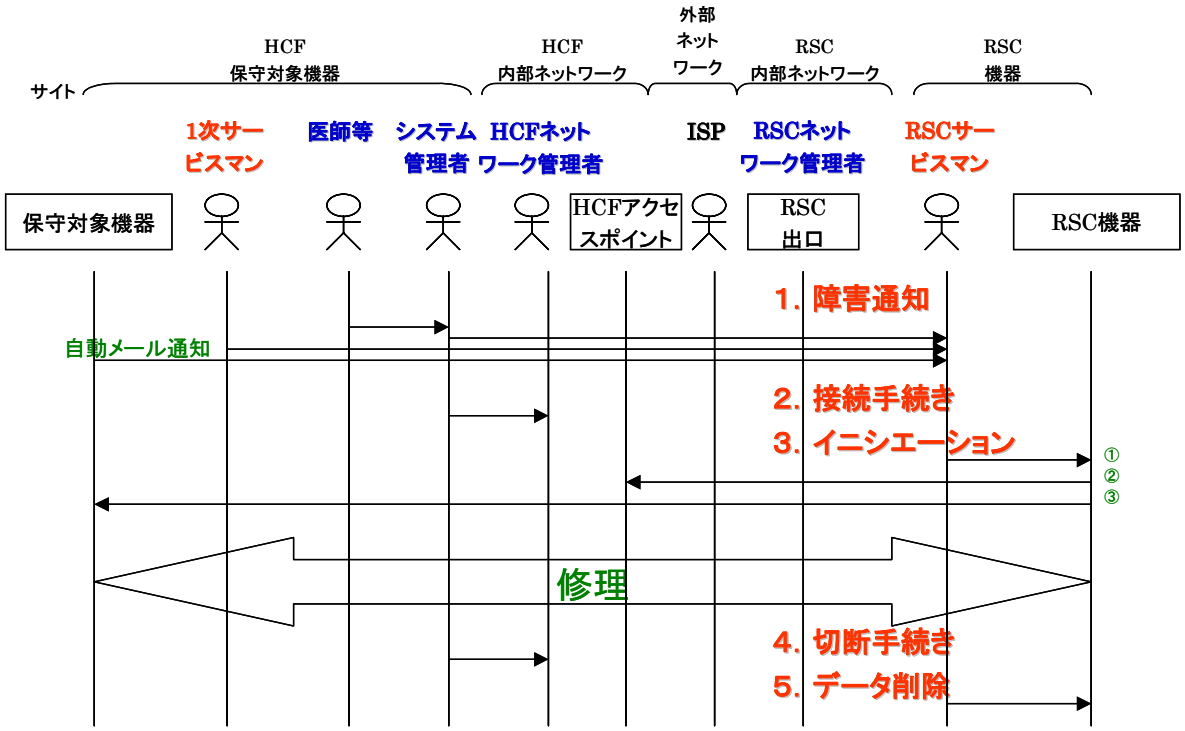

図１－４－２　故障時の対応のワークフロー

手順は次のようになります。

（１）　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）　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。（図中①→②→③）

（４）　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） HCF へ作業結果の報告を行う。

（６） 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） 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。

１－４－２．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１－４－３に示します。

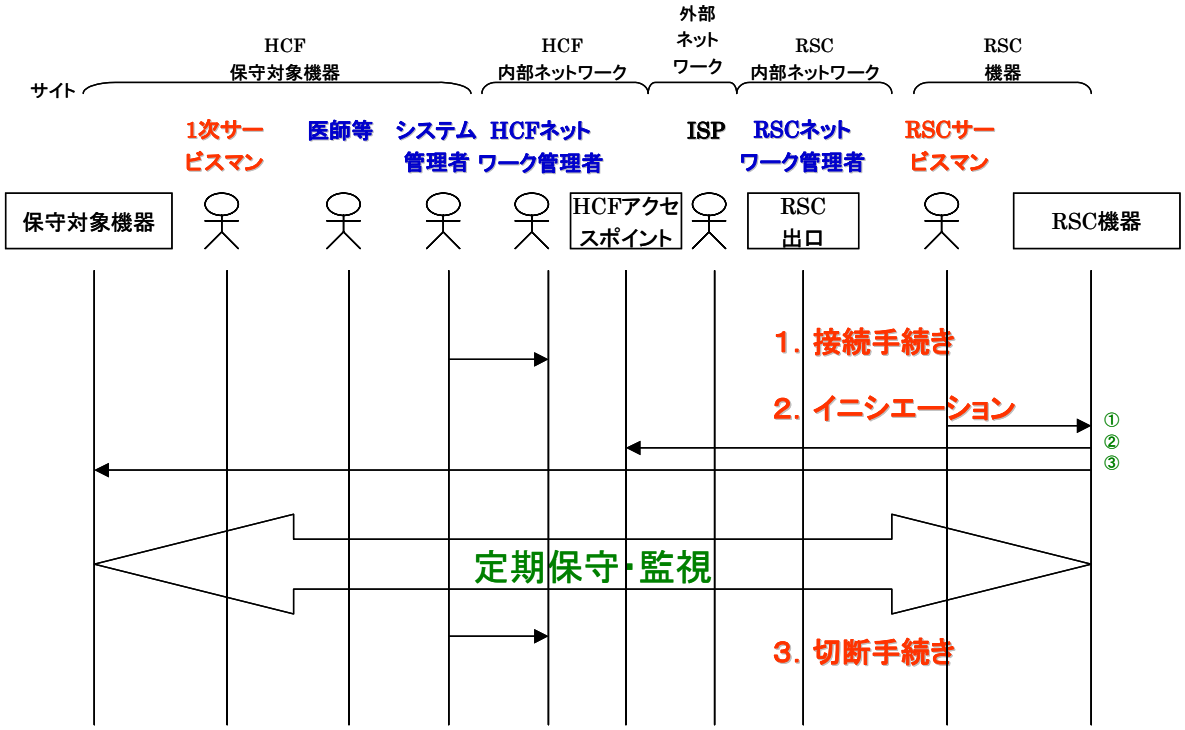

図１－４－３　定期保守・定期監視のワークフロー

手順は次のようになります。

（１）　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。（図中①→②→③）

（３）　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）　HCF へ作業結果の報告を行う。

（５）　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）　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。

１－４－３．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１－４－４に示します。

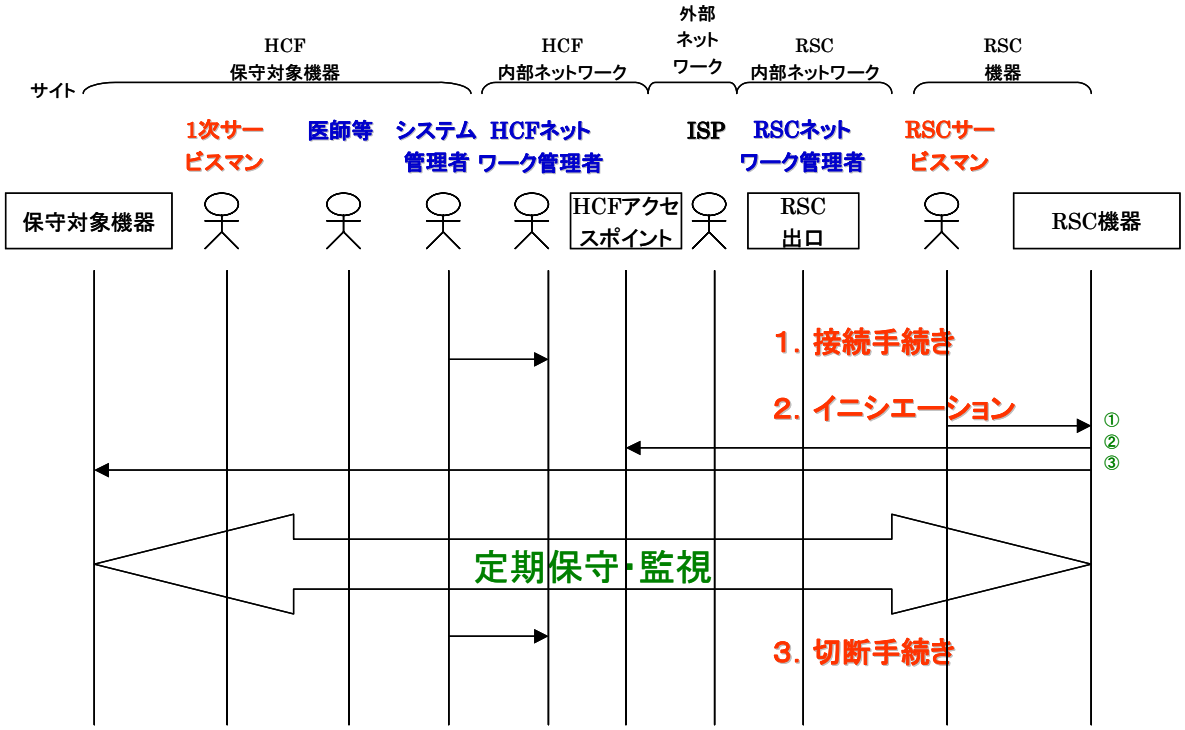

図１－４－４　ソフトウェアの監視のワークフロー

手順は次のようになります。

（１）　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。（図中①→②→③）

（３）　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）　HCF へ作業結果の報告を行う。

（５）　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）　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。

１－４－４．リスクアセスメント実施時の条件

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情報資産を洗い出し、それに対する脅威と脆弱性を分析しています。ここで扱う情報資産の重要度は、すべて同じレベルであると想定しています。

分析は、下記のサイトごとに行っています。

- 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

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三者とみなします。

例外として、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(Protected Healthcare Information)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

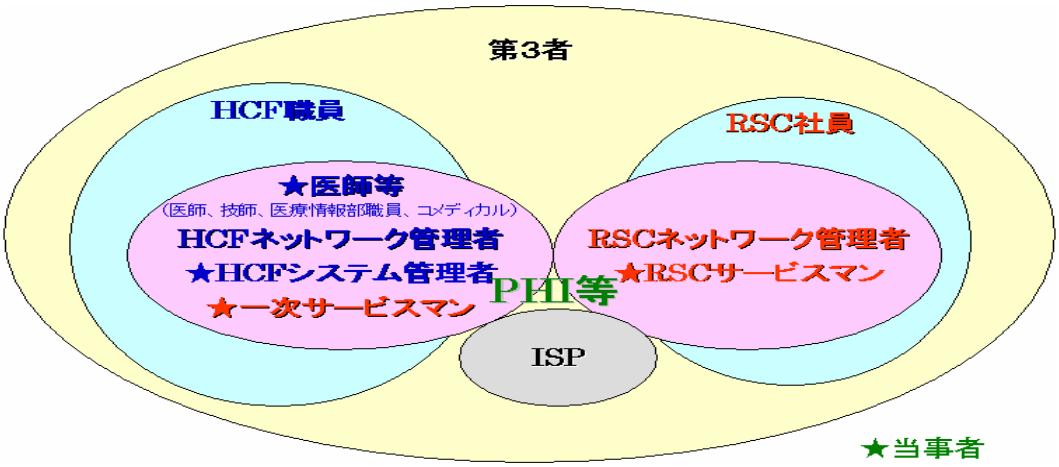

図１－４－５　リモートサービスのアクタ

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

１－５．略語集

以下に本ガイドライン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)

ISMS : Information Security Management System、情報セキュリティマネジメントシステム

ISP : Internet Service Provider、インターネット・プロバイダ、インターネット・サービス・プロバイダ

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)

JIPDEC : Japan Information Processing Development Corporation、財団法人　日本情報処理開発協会

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

PDCA : Plan（計画）、Do（実施）、Check（検証）、Act（行動）のマネジメントサイクル

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要件

２－１．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普及してきており、この形態を利用したリモートサービスを実現していきたいが、どのようにセキュリティを確保するか、どのように安全性を説明するかといった課題があるように思います。さらに実際の医療機関ではリモートサービスを必要とするシステムは複数あり、それらのセキュリティレベルのばらつきをどのようにボトムアップし、かつ、管理するかという課題もあるように思います。以下、順に説明します。

（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、以下の技術的対策によりセキュリティの確保を行っています。

（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、ネットワークに関する管理規定
（ウ）　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
（エ）　RSC がリモートサービスを行う際の記録、授受データの処理に関する規定
（オ）　RSC リモート端末が増設・移動される場合の規定
（カ）　モバイルからのアクセスに関する規定

また、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
（ウ）　リモートサービス業務の監査方法に関する取り決め

（３）マルチベンダ化によるセキュリティ上の課題

実際の HCF には複数の病院情報システムが存在し、それぞれのリモートサービスにおけるセキュリティ対策は異なっています。複数のシステムが同じネットワーク上に存在する場合、右図（**図２－１－１**）に示すようにもっともセキュリティレベルが低いシステムが全体としてのレベルを決定します。

このように無条件に病院情報システムのリモートサービスを導入させることは HCF 側のセキュリティレベルを一定以上に維持することを困難にするばかりか、セキュリティ確保のための必要経費が増大していくことになります。その対策としては、２つの方法が考えられます。

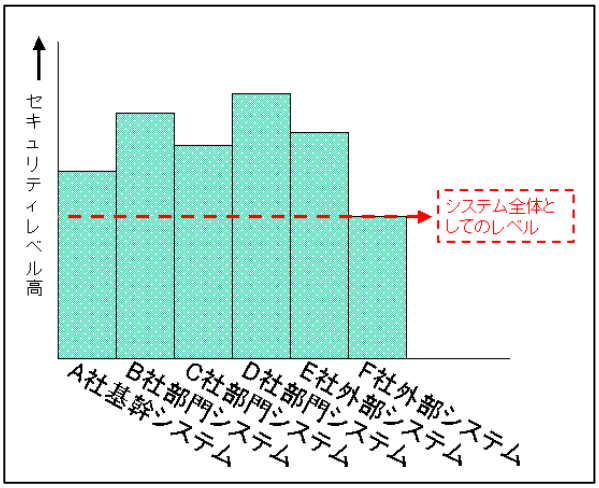

図２－１－１　全体のセキュリティレベル

（A）　複数システムの HCF 側アクセス口を１つにまとめ、経路制御、モニタを厳重に行う方法。

（B）　セキュリティレベルの低い病院情報システムは、基幹ネットおよび他のシステムと Firewall などで論理的に切り離すことにより、影響を最小限に制限する方法。

いずれにしても HCF 全体でリモートサービスに関する利便性とリスクのバランスが最適となるように計画し、管理する必要があります。

（４）リモートサービスと説明責任

個人情報保護法の施行により、医療機関は法律上において個人情報取扱事業者となります。医療機関は患者に対して行う業務、導入しているシステムを管理する必要があり、その延長線上でリモートサービスの管理、またサービスを提供するベンダの管理も行うことになります。リモートサービスを行うベンダは自己の保守体制、リモートサービスのためのシステムについて後述するように詳細に分析し、説明できるようなセキュリティレベルを確保し、かつ説明資料を用意する必要があります。

２－２．個人情報保護とリモートサービス

2005 年 4 月より、「個人情報保護法」が全面施行され、医療機関に対して個人情報である診療情報について、その保護についての新たな義務が課せられるようになりました。また、診療情報は、その取扱いにより一層の留意が求められるため、厚生労働省より「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（以下「医療事業者ガイドライン」）」および「医療情報システムの安全管理に関するガイドライン（以下「システムガイドライン」）」が制定されており、医療機関および関連業者においてその遵守が求められています。

個人情報保護法では、個人情報を取り扱う個人情報取扱事業者が、その個人情報の安全管理に関する義務を負っており、その事業者から委託を受けて個人情報を取り扱う受託業者についての義務規定は、定められてはいません。しかしながら、「医療事業者ガイドライン」では、医療機関に対し、個人情報の取扱いを委託する場合についての留意事項を以下のように定めています。

・個人情報を適切に取り扱っている事業者を委託先（受託者）として選定する
・契約において、個人情報の適切な取扱いに関する内容を盛り込む（後略）
・受託者が、委託を受けた業務の一部を再委託することを予定している場合は、再委託を受ける事業者の選定において個人情報を適切に取り扱っている事業者が選定されるとともに、再委託先事業者が個人情報を適切に取り扱っていることが確認できるよう契約において配慮する
・受託者が個人情報を適切に取り扱っていることを定期的に確認する
・受託者における個人情報の取扱いに疑義が生じた場合（中略）には、受託者に対し、説明を求め、必要に応じ改善を求める等適切な措置をとる

リモートサービスにおいては、対象となる医療機器、医用情報機器の保守やサービスが主たる業務ですが、その遂行の際にそれらの機器に含まれる患者情報などの個人情報に触れる可能性がある場合には、個人情報の取扱いの委託に該当する可能性が高いと言えます。従ってリモートサービスを提供する業者に於いては、医療機関から上記の要件が求められることを前提に、リモートサービスにおけるセキュリティ対策をとるべきです。すなわち、

・個人情報を適切に取扱う対策がとられていることを示すこと
・個人情報の取扱いに関する内容を契約に含めること
・再委託先について、選定の妥当性の説明、適正な個人情報の取扱いを確認できること
・個人情報を適切に取扱っていることを定期的に示すこと

・問題が生じた際に適切な対応をとること

などが、必要となります。

また、「システムガイドライン」では、6.8 節に「情報システムの改造と保守」の項があり、リモートサービスについても、「リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること。」との安全措置が、最低限のガイドラインとして示されており、対応が必須とされています。

民間業者が対象である個人情報保護法では、委託業務に関しては委託する側の監督責任が定められているだけで、受託側の責任は明確にはなっていませんが、個人情報保護法と同時に成立・施行された「独立行政法人等の保有する個人情報の保護に関する法律」では、第七条の２項において、「個人情報の取扱いの委託」を受けた者についても安全管理措置の実施が明確に課せられており、第六章において懲役を含む罰則も定められています。リモートサービス業務も、上述の「個人情報の取扱いの委託」に該当する可能性が高いため、国立病院機構や国立大学附属病院でのリモートサービス業務については、その点に留意する必要があります。

また、都道府県立や市町村立などの公立病院では、それぞれの地方公共団体が制定した個人情報保護に関する条例が適用されるため、それぞれの条文の内容について留意が必要です。

以上のように、個人情報保護法の全面施行にともない、明確な個人情報保護の対策を行うことが求められており、とくに医療施設の監督者と直接の対面を伴わないリモートサービスに於いては、医療施設側の信頼を得られるだけの安全対策を行うことが必要であると言えます。

２－３．電子保存三原則とリモートサービス

電子保存三原則とは、平成11年4月の厚生省（当時）健康政策局長、医薬安全局長、保険局長の連名による「診療録等の電子媒体による保存について」通知において示されているもので、電子保存を行う際に、以下の三基準を確保することです。

①**真正性**　正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、および混同が防止されていること
②**見読性**　電子媒体に保存された内容を権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること
③**保存性**　記録された情報が、法令等で定められた期間にわたって、真正性を保ち、見読可能にできる状態で保存されること

法令に保存義務が定められている診療録等の電子保存を行っている医療機関は、装置やネットワーク機器などによる技術的な対策と、組織や人による運用的な対策を組み合わせて、これらの基準を確保していなければなりません。もちろん、医療機関が装置・ベンダに委託して行う保守作業においても同様に基準が確保されていなければなりません。保守作業の場合、委託先の保守要員が管理者モードで直接診療情報に触れる可能性があり、十分な対策が必要になります。

保守作業における電子保存三原則に対する脅威については、厚生労働省が平成 17 年 3 月に出した「医療情報システムの安全管理に関するガイドライン」で以下のように示されています。

> ・ 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
> ・ 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
> ・ 保存性の点では、意図的な媒体の破壊および初期化や、オペレーションミスによる媒体の初期化やデータの上書き等
>
> （6.8　情報システムの改造と保守　B．考え方）

これらの脅威に対する対策については以下のように示されています。

> これらの脅威からデータを守るためには、医療機関の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。
>
> （6.8　情報システムの改造と保守　B．考え方）

以上より、保守作業を行うベンダは、保守作業先の医療機関から出される①守秘義務契約の締結、②保守要員の登録、③作業計画報告の提出、④作業時の病院関係者からの監督などの要請に対し対応する必要があります。

リモートサービスも保守作業のひとつのサービス形態ですが、作業者が直接病院関係者の監督下にいない、リモート接続する経路上のセキュリティ対策が必要等、現地で行う保守作業にはない脅威が想定されます。そのため、「医療情報システムの安全管理に関するガイドライン」で挙げられている対策だけでなく、リモートサービス向けの追加対策が必要です。

本ガイドラインでは、リモートサービスにおける脅威を検討し、それらに対する対策について述べています。リモートサービスを行うベンダは、本ガイドラインの内容にしたがい、電子保存三原則を脅かさないように、医療機関の監督の下で適切な対策を実施してください。

２－４．情報セキュリティマネジメントとリモートサービス

情報セキュリティマネジメントシステム(ISMS)とは、セキュリティポリシの下に、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 を運行する仕組みのことです。

ISMS の一般的事柄は ISO/IEC17799　として国際的標準化がなされており、これに沿ってシステム構築・運用を行うことが、便宜的であると言えます。また、患者さんや医療評価機関等に説明を行うに当たっても、説得性を持った手法となります。図２－１－１に ISMS 構築の一般的ステップを記します。

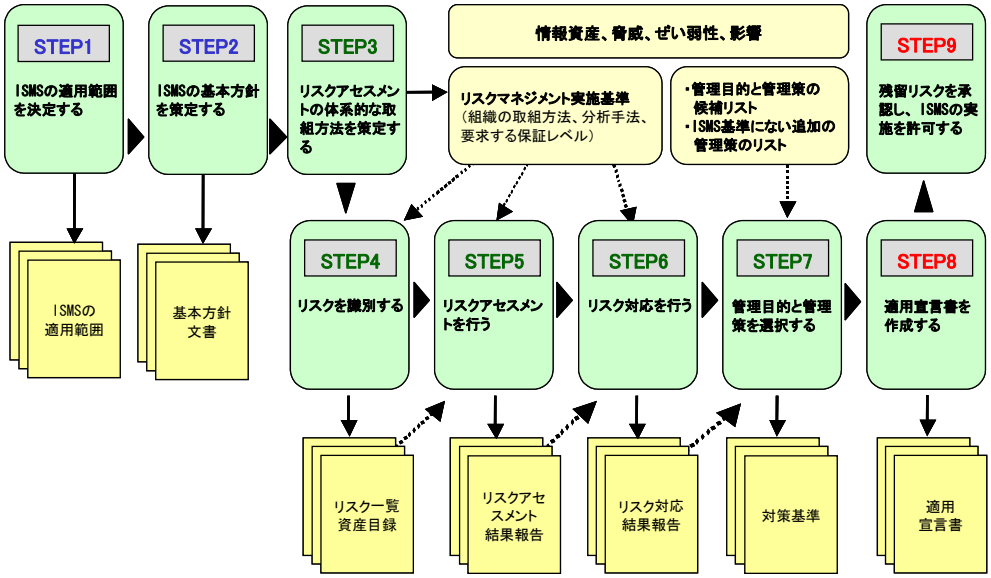

図２－１－１　ISMS 構築の一般的ステップ
（JIPDEC　医療機関向け ISMS ユーザーズガイドから）

以下に、ISMS の考え方に沿って、リモートサービスにおける個人情報のセキュリティ対策を述べます。

医療機関とリモートサービスを提供するベンダは、それぞれ適切な情報の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ベンダとの間で情報のセキュリティマネジメントを整合させる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、医療機関とリモートサービス提供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が内在しています。

リモートサービスは独立した組織である医療機関とリモートサービスセンター(RSC)間にまたがる行為であり、一組織内のシステム構築とは異なった問題があり、ゼロベースでRSS を考えることは、医療機関と RSC の双方にとって負担になることが考えられます。この点、既に定まった手法である ISMS を利用することが効率よく実施するための近道と言えます。

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、RSC 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、個人情報のための適切な措置を求める必要があります。

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のセキュリティマネジメントシステムと整合させて、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。情報の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は、以下項目を文書化し遵守していく必要があります。

・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
・運用実施規程
・セキュリティ監査基準
・セキュリティ監査と監査証跡

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、RSC 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。医療機関は保守契約あるいは業務委託契約等において、個人情報の最終責任者として、ベンダに対する監督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。

本 WG の 2003 年度の成果である「リモートサービスセキュリティガイド」には、ISMS 方式でリスク分析と対策例示がなされています。従って、この内容をベースにして不足部分があれば追加することで RSS を構築することが、医療機関と RSC のどちらにもメリットをもたらすものと考えます。

第３章　リモートサービスへの ISMS の適用

３－１．本ガイドラインにおける ISMS の適用範囲

１－４に述べた運用モデルでの ISMS の適用範囲は下記の箇所になります。

・ 医療機関内の保守対象機器
・ 医療機関の内部ネットワーク
・ 医療機関側におけるリモートサービスアクセスポイントからRSCまでの経路
・ RSCの内部ネットワーク
・ RSCにおける機器管理

下記の事項はリモートサービスの有無に拘らず存在するリスクですので、本章の ISMS 適用範囲からは除外します。

・ HCF 側で対策対象とすべき、リモートサービス対象機器以外のリスク
・ 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

３－２．RSS でのセキュリティ基本方針

ISO/IEC 17799 を JIS 化した JIS X 5080 の「3.1.1　情報セキュリティ基本方針文書」には、基本方針に含まれる事が望ましい内容が以下の様に規定されています。

a）情報セキュリティの定義，その目的及び適用範囲，並びに情報共有を可能にするための機構としてのセキュリティの重要性
b）情報セキュリティの目標及び原則を支持する意向声明書
c）組織にとって特に重要なセキュリティ基本方針，原則，標準類及び適合する要求事項の簡潔な説明
1）法律上及び契約上の要求事項への適合
2）セキュリティ教育の要求事項
3）ウイルス及び他の悪意のあるソフトウェアの予防及び検出
4）事業継続管理
5）セキュリティ基本方針違反に対する措置
d）　セキュリティ事件・事故を報告することも含め，情報セキュリティマネジメントの一般的責任及び特定責任の定義

> e）基本方針を支持する文書（例えば，特定の情報システムについてのより詳細なセキュリティ個別方針及び手順又は利用者が従うことが望ましいセキュリティ規則）の参照情報
>
> （JIS X 5080:2002　3.1.1　情報セキュリティ基本方針文書　より引用）

これらの事項を RSS に則して当てはめてみると、システムの可用性を確保しつつ、患者個人情報保護と電子化情報の電子保存 3 原則(法的保存義務のある書類の真正性、見読性、保存性確保)を図ることになります。

RSS でのセキュリティ基本方針には、RSS に関する技術的・組織的・人的・物理的安全措置に関する内容が明記される必要があります。

以下の説明は、大規模な総合医療施設を想定して記述されています。大規模の医療施設では、リモートサービスを受ける RSC が複数の部門に存在することが有り得るため、その統一的な管理方針が必要になります。施設規模や運用形態がこれとは違う場合では、同様な趣旨が満たされることが目的ですから、適宜実態に則した形態で運用を行うことが大切です。

３－３．標準的事例におけるリスク評価

リスクアセスメントにおいては、情報資産に対して

① どのような脅威が存在するのか
② 脅威の発生の可能性や頻度はどの程度か
③ 脅威が顕在化したときにどの程度の影響を受けるか

について分析を行ないます。

分析の手法は大きくは以下の四つに分類されています。

（１）ベースラインアプローチ

標準やガイドラインに基づいてリスク分析を行なう手法です。あらかじめ業界などで標準的なリスク評価を行いセキュリティ対策を行なうものです。自身でリスク評価を行なう必要がないため費用面、期間面で有利ですが、標準的なリスクと自身の組織のリスクの適合性がどの程度かが大きな問題となります。

（２）詳細リスク分析

詳細のリスク分析を実施することにより厳密なリスク評価を実施し、適切な管理策を選

択するものです。リスクアセスメントには必要な人材の確保を含め多大なコストと時間を必要とします。

（３）組み合わせアプローチ

ベースラインアプローチと詳細リスク分析を組み合わせるもので、両方のメリットを享受できます。

（４）非形式的アプローチ

組織や担当者の経験や判断によりリスクを評価するものです。方法が構造化されていないため結果の第三者評価が難しい側面があります。

リモートサービスは医療機関とリモートサービスセンターという異なる組織をまたがる業務なので、リスク分析も両者が合意できるものでなければなりません。本ガイドラインでは、JAHIS、JIRA の両工業会が想定する標準的なユースケースについてモデル化を行い、そのモデルに関するリスクアセスメントを実施しています。このリスクアセスメント結果を利用することで、（１）のベースラインアプローチや（３）の組み合わせアプローチによるリスク分析が可能になります。リスクアセスメントの結果は付録を参照してください。

この表では、リモートサービスセキュリティガイドにおいてリスクアセスメントを実施した結果について、日本情報処理開発協会（JIPDEC）の ISMS 認証基準（Ver2.0）における詳細管理策のリストから適切な管理目的と管理策を選定し、反映したものとなっています。この詳細管理策のリストは ISO/IEC17799 ならびに JIS X5080 に準拠しており、10 の管理分野と、36 の管理目的、127 の管理策から構成されています。

ここで規定されている対策は JAHIS、JIRA の両工業会としてリモートサービスを実施する上で最低限遵守すべき内容について規定したものです。個人情報の管理者である医療機関からみて、リモートサービスセンターがこのガイドラインに準拠しているかどうかを評価し、もしリモートサービスセンターがこのガイドラインを満たしていない場合には適切な対策をとるように要請すべきです。また、医療機関自身のセキュリティレベルが本ガイドラインを下回っているようであれば、必要な対策を実施する必要があるでしょう。リモートサービスベンダー各社においては、本ガイドラインを遵守できるように必要な対策を実施することが期待されます。

３－４．標準的事例における管理すべきリスク

ここでは、個人情報保護の観点からリモートサービス利用時において特に注意しなければならないリスクについていくつか例をあげて解説します。これらのリスクに対する十分な対策を実施することが重要です。もちろん、ここで挙げたリスクはあくまで例であり、これ以外のリスクが重要でないということではありません。

（１）医療機関の管理する個人情報をリモートサービスセンター内で取り扱う場合

この場合に特に注意が必要なのは当事者以外の人間による情報の漏洩です。システムに対する不正アクセスだけではなく、作業中に発生する画面上の情報や紙に印字される情報などについても十分な配慮が必要です。主なリスクとして以下のものが挙げられます。

・RSC 内部の当事者以外の画面などの覗き見
・第三者委託における委託先での漏洩
・データ解析時に発生するログやプリントした紙、キャッシュなどからの漏洩
・ネットワークの経路上の漏洩

（２）管理者権限で医療機関の保守対象機器にアクセスする場合

この場合に特に注意が必要なのはオペレータのミスや悪意をもった不正アクセス（許されたオペレーション以外のオペレーションをすること）です。主なリスクとして以下のものが挙げられます。

・オペレーションミスによる保守対象機器内のデータの破壊
・悪意を持った破壊活動による保守対象機器内のデータの破壊
・保守対象機器を踏み台にした内部侵入による、より重要な情報の漏洩や破壊

（３）ソフトウェアのアップデートを行なう場合

この場合に特に注意が必要なのは不正なソフトウェアやウイルスなどが保守対象機器に組み込まれてしまうことです。主なリスクとして以下のものが挙げられます。

・不正なソフトウェアによる保守対象機器内のデータの漏洩や破壊
・ウイルスの内部侵入による、より重要な情報の漏洩や破壊

３－５．本ガイドラインに記載のないリスクの識別

本ガイドラインにおいては JAHIS、JIRA が標準的と考えるモデルに関するリスクアセスメントを行なっていますので、それ以外の事例については対象範囲としていません。もし、本ガイドラインが想定しているモデルとは異なる業務モデルの場合、本ガイドラインのリスクアセスメント結果は流用可能ですが、全てをカバーできない可能性があります。この場合、組み合わせアプローチにより、本ガイドラインに記載のないリスクについて詳細リスク分析を行なう必要があります。

詳細リスク分析におけるリスクアセスメントの方法については「リモートサービスセキュリティガイド」に詳しく説明されていますので、そちらを参照してください。「リモートサービスセキュリティガイド」の手法を用いることで、ベースラインのガイドラインと同一の手法を取ることとなりますので、全体を容易に統合することができます。

３－６．リスク対応

リスク対応とは、リスクアセスメントの結果想定されるリスクに対してどのような対応をするかを定め、実施することをいいます。リスク対応には下記の表３－６－１の選択肢があり、必要に応じてそれらを組み合わせて行ないます。

通常のリスクマネジメントにおいては、これらのどれか一つを選択するということではなく、リスクの重要度や対策の容易性などから総合的に判断し、これらの対策を組み合わせて実施します。特に個人情報保護法などの法律やガイドラインで定められた情報資産のリスク対応についてはリスクコントロールを行なうことが法律や通知などで求められているものがあります。このような場合には、リスクファイナンスなどの解決方法がとれませんので、積極的にリスクコントロールを行なわなければなりません。もしくは、リスク回避策をとり、法律で対象となっている個人情報をリモートサービスでは一切扱わないという対策も一つの解です。

本ガイドラインでは、ISMS の考え方に基づいて積極的にリスクコントロールを行なうことを推奨しています。具体的な対策については４章にて詳しく解説します。

表３－６－１　リスクへの対応

リスクに対処する方法

リスクコントロール
積極的に損害を小さくする対策（管理策）を採用する
・リスク予防
脅威や脆弱性を少なくするための対策を実施する
・損害の極小化
リスクが発生したときの損害を少なくするための対策を実施する

リスク保有
組織としてリスクを受容する対応
・リスクファイナンス
引当金を積むなどの対応を行う
・何もしない

リスク移転
契約等により他社に移転する対策
・リスクファイナンス
損害保険や責任賠償保険などに加入しリスクを移転する
・アウトソーシング
情報資産そのものや情報セキュリティ対策を外部に委託する

リスク回避
適切な対策が見出せない場合の対応
・業務の廃止
業務そのものをやめてしまう
・情報資産の破壊
管理対象物をなくしてしまう

第４章　管理目的と管理策の選択

４－１．リモートサービスの安全管理措置に関する全体的な方針

リモートサービスにおいて流通するデータには患者データ等の個人情報が含まれる可能性があることから、HCF は厚生労働省から提示されている「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（平成 16 年 10 月)」と「医療情報システムの安全管理に関するガイドライン（平成 17 年 3 月)」で要求されている内容を、RSC と共に実現していかなければなりません。

HCF と RSC は、安全なリモートサービスを実現するための適切なセキュリティ対策を行うために、リスクアセスメントの結果からその重要度に応じ管理策を選択します。RSC は個人情報取扱事業者であるなしに関わらず、HCF からリモートサービスを監督される立場にあり外部委託業者として HCF が求める安全なリモートサービスを提供しなければなりません。

本章ではこれら組織的、物理的、技術的、及び人的な安全管理措置について、リモートサービスを行う際に HCF と RSC がそれぞれどのような対策を実施していくかを具体的に示しています。本 WG の成果物であります本ガイドライン付録の「ISMS 準拠リモートサービスリスクアセスメント表（以下、「リスクアセスメント表」)」およびリモートサービスセキュリティガイドを参照していただくことで、リモートサービスを構築するときに行うリスクアセスメントに要する作業時間を削減できることと期待しています。

すでに運用されているリモートサービスについても、このリスクアセスメント表を活用していただき、自ら行ったリスクアセスメントが適切であるかどうかを監査していただくことを推奨いたします。

また、リモートサービスを締結する際の守秘義務等に関する契約や、HCF への作業の報告については、「医療情報システムの安全管理に関するガイドライン」の第６章を参照ください。

４－２．リモートサービスにおける安全管理措置

本節では、リスクアセスメント表の各要件を「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 16 年 6 月 厚生労働省経済産業省告示第 4 号)」（以下、「経済産業省ガイドライン」）にて示されている安全管理措置として講じなければならない事項の各項目へ対応付けています。本節中の丸数字項目は、経済産業省ガイドラインで示されています安全管理措置として講じなければならない事項の丸数字項目と対応しています。同じく、（要件番号：____）はリスクアセスメント表に記載の要件番号と対応しています。

４－２－１．リモートサービスにおける組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規定や手順書を整備運用し、その実施状況を確認することをいいます。

①　個人データの安全管理措置を講じるための組織体制の整備

②　個人データの安全管理措置を定める規程等の整備と規程等に従った運用

ISP 側の保守点検、バックアップ、防災対策、事業継続計画、施錠保管を明文化して責任の分界を明確にすることによって、サービス不能を防止すること。（要件番号：12）

③　個人データ取扱台帳の整備

④　個人データの安全管理措置の評価、見直し及び改善

⑤　事故又は違反への対処

防災対策、事業継続計画によって、災害を予防し、災害による被害損失の最小化と早期回復を可能とすること。（要件番号：114）

４－２－２．リモートサービスにおける物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいいます。

①　入退館（室）管理の実施

・パーティション等により、関係者以外の立ち寄りを抑止すること。(要件番号:26)

・入室管理により、権限の無い者の入室を阻止して画面の覗き見や不正ログインや成りすまし、紙の覗き見や持出、RSC 機器やディスクの持出を防止すること。(要件番号：27)

②　盗難等に対する対策

・シュレッダ廃棄により資産を消去することによって、権限の無い者による紙の覗き見や持出を防止すること。(要件番号：27)

・複数人管理による入室管理により権限の有る者の単独入室を防止し、RSC サービスマンによる単独入室を阻止して紙の持出を牽制すること。(要件番号：29)

・道路とサイトの距離の確保により漏洩電磁波の受信を防止し、PHI の暴露を防止すること。(要件番号：31)

・ログオフ時の自動消去により人的ミスを防止し、RSC サービスマンの PHI の削除忘れを防止すること。(要件番号：36)

・クリアデスクにより無人時の資産の放置を防止し、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紙の覗き見や持出を防止すること。(要件番号：37)

③　機器・装置等の物理的な保護

・施錠保管により、権限の無い者による接触を阻止して媒体の持出、破壊によるサービス不能を防止すること。(要件番号：27)

・複数人管理による施錠保管により権限の有る者の単独接触を防止し、RSC サービスマンによる単独接触を阻止して媒体や RSC 機器やディスクの持出を牽制、RSC ネットワーク機器経由の PHI の暴露を防止すること。(要件番号：29)

・RSC 側内部経路点検により、経路上のタッピング痕跡を検出すること。(要件番号：29)

・シールにより、タンパリング痕跡を検出すること。(要件番号：31)

４－２－３．リモートサービスにおける技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置のことをいいます。

①　人データへのアクセスにおける識別と認証

・遠隔地からの利用者のアクセスには、認証を行うこと。（要件番号：72）

・遠隔コンピュータシステムへの接続は、認証されること。（要件番号：73）

②　個人データへのアクセス制御

・利用者には､ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること。（要件番号：70）

③　個人データへのアクセス権限の管理

・複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること。（要件番号：64）

・パスワードの割当ては、正規の管理手続によって統制すること。（要件番号：66）

④　個人データのアクセスの記録

・情報処理設備の使用状況を監視する手順を確立すること。（要件番号：90）

⑤　個人データを取り扱う情報システムについての不正ソフトウェア対策

・悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること。（要件番号：47）

⑥　個人データの移送・送信時の対策

・データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること。（要件番号：33）

・共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと。（要件番号：77）

・一連の合意された標準類，手順及び方法に基づく鍵管理システムを，暗号技術の利用を支援するために用いること。（要件番号：103）

⑦　個人データを取り扱う情報システムの動作確認時の対策

・装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること。（要件番号：34）

⑧　個人データを取り扱う情報システムの監視

・極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、か

つ検査すること。（要件番号：48）

４－２－４．リモートサービスにおける人的安全管理措置

人的安全管理措置とは、従業者に対する業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいいます。

①　雇用契約時及び委託契約時における非開示契約の締結

・従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること。（要件番号：18）

・組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること（要件番号：25）

②　従業者に対する教育・訓練の実施

・組織の基本方針及び基準について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと。（要件番号：20）

第５章　残存リスクの承認

残存リスクとは、リスク評価によって算出されるすべてのセキュリティリスクのうち、意図的に残したものや識別困難なもの、その対策を完全に行うためには高額となってしまうリスクのことを指します。リスクコントロールとリスクファイナンスを行っても、依然として必ず残ってしまう残存リスクについては経営的な理由からも経営層が適切と判断し承認する必要があります。ここで HCF がこの残存リスクを承認するということは、ISMS に準拠したリスクアセスメントによって構成されたリモートサービスを許可するという宣言となります。

HCF はリモートサービス全体の契約の中で、残存リスクについて承認し、RSC はそれらの残存リスクに留意したリモートサービスを行っていきます。特に RSC では、第４章で扱うリモートサービスにおけるリスク分析の結果にあるように、患者情報等の個人情報が漏洩するリスクが完全にはなくなりません。HCF はこのことを理解し、厚生労働省のガイドラインなどを参考にして、実際のリモートサービスにおいて適切なセキュリティ対策が行われていることを監査していきます。

第６章　セキュリティ監査のガイドライン

６－１．リモートサービスにおけるセキュリティ監査

セキュリティ監査の目的は、セキュリティに係わるリスクマネジメントが効果的に実施され、リスクアセスメントに基づく適切なコントロールが行われていることを確認することです。またセキュリティ監査は、情報セキュリティ管理基準の全体的な適合性を監査するものでもありますが、リモートサービスに焦点を当てて監査することも可能です。リモートサービスにおけるセキュリティ監査においても、リモートサービスのリスクアセスメントに基づく適切な管理策（コントロール）が整備され運用されていることを検証および評価します。

また、このセキュリティ監査を通してセキュリティ上の安全基準を評価することは、リモートサービスの堅牢性を高めるための有効な判断材料となることからも、HCF、RSC 両者にとって有益な施策といえます。

６－２．第三者機関によるセキュリティ監査の推奨

情報セキュリティ監査を内部監査として行うには次のような問題点が考えられます。

- リスクアセスメントから漏れてしまうリスクに気付きにくい
- 監査員が客観性・独立性にかける
- 専門的な知識が要求されることから監査員の養成に時間がかかる
- 監査報告を外部へ開示する際にその形式を作ることが難しい

以上のことから、高い専門知識を有する監査人に客観的に評価してもらう外部監査を導入することが考えられます。リモートサービスセキュリティガイドにおいても紹介していますが、適切な監査ルールに基づいた外部監査を実施することは、ISMS やプライバシーマークの認証取得にもつながり、個人情報保護などの観点から社会的評価を得ることにもなります。HCF、RSC それぞれのセキュリティ監査報告の信頼性のギャップを極めて小さくするためにも、外部監査を採用することを推奨いたします。

第７章　本ガイドラインの技術的・制度的変化への対応

本ガイドラインは、2005 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して関連省庁から提示されているガイドライン等に適用しうるガイドラインとして制定しました。

個人情報の保護についての考え方は、法の施行後の状況や社会情勢の変化に応じた技術の進歩等によって変わり得るものです。また、法制度についても、それらの変化に応じて改訂が行われる可能性があります。

本ガイドラインは国際的なセキュリティ標準である ISO/IEC17799 の情報セキュリティマネジメントの考え方を元に作成されたものであり、特定の技術や製品に依存す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、本ガイドライン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。

参照規格および法規

本ガイドラインで扱う規格および法規について、参考となる参考文献、法令等を以下に示します。

医療機関のセキュリティに関するガイドライン等

・「保健医療分野のプライバシーマーク制度　参考資料集」
財団法人医療情報システム開発センター　2003.07
http://privacy.medis.jp/book.html（入手案内）

・「保健医療分野のプライバシーマーク関連情報」
財団法人医療情報システム開発センター　2003.07

・「リモートサービスセキュリティガイド」
（社）日本画像医用システム工業会　2004.03

・「SPC 文書」
NEMA（米国電気機器製造者協会）、COCIR（欧州放射線医用電子機器産業連合会）、JIRA（日本画像医用システム工業会）の Joint Security and Privacy Committee（通称：SPC）による作成文書
http://www.nema.org/prod/med/security/（英文版）

ISMS に関する参考資料

・「JIS X 5080:2002 情報セキュリティマネジメントガイド」
日本規格協会　2003.04

・情報システム部門責任者のための情報セキュリティブックレット
IPA/ISEC　2001.03
http://www.ipa.go.jp/security/fy12/contents/bookletB.pdf

・情報セキュリティ監査基準（Ver.1.0）
経済産業省　2003.04
http://www.meti.go.jp/feedback/downloadfiles/i30326fj.pdf

・情報セキュリティ監査研究会報告書
経済産業省　2003.03
http://www.meti.go.jp/feedback/downloadfiles/i30326bj.pdf

・ISMS 認証基準（Ver.2.0）
JIPDEC　2003.04
http://www.isms.jipdec.or.jp/doc/JIP-ISMS100-20.pdf

・ISMS 適合性評価性制度の概要（パンフレット）
JIPDEC　2003.06
http://www.isms.jipdec.jp/doc/v2ismspanf.pdf

・医療機関向け ISMS ユーザーズガイド
JIPDEC　2004.11
http://www.isms.jipdec.jp/doc/JIP-ISMS114-10.pdf

・「情報セキュリティマネジメントの国際規格」
日本規格協会　2003.03
http://www.webstore.jsa.or.jp/lib/lib.asp?fn=/iso/iso01_42.htm

・「BS7799-2:2002(Specification for information security management system　情報セキュリティマネジメントシステムー仕様及び利用の手引)」英和対訳版
日本規格協会

・「ISO/IEC 17799:2000(ISO/IEC 17799:2000 Code of practice for information security management)」英和対訳版
日本規格協会

・「JIS X 5080:2002(ISO/IEC 17799:2000(Information technology -Code of practice for information security management)情報技術ー情報セキュリティマネジメントの実践のための規範」
日本規格協会

・情報セキュリティポリシーに関するガイドライン
内閣官房情報セキュリティセンター
http://www.bits.go.jp/

・情報セキュリティ対策の資料
IPA/ISEC
http://www.ipa.go.jp/security/

個人情報保護に関する資料

・個人情報の保護に関する法律
首相官邸　平成 15 年 5 月 30 日法律第 57 号
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/index.html

・民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン
旧通商産業省告示 98 号　1997.3.4
http://www.gip.jipdec.or.jp/policy/infopoli/privacy.html

・政府　個人情報保護法制度化専門委員会 Web ページ
http://www.kantei.go.jp/jp/it/privacy/houseika/

・プライバシーマーク事務局 Web ページ
JIPDEC
http://privacymark.jp/

付録

付録１　ISMS 準拠リモートサービスリスクアセスメント表

本 ISMS 準拠リモートサービスリスクアセスメント表は、「サイトと前提（表１）」と「資産の分類（表２）」、「リスク評価表（表３）」を併用することにより、リモートサービスを構成する際に行うリスクアセスメントを効果的に行うことができます。しかし、これらはあくまで本ガイドラインが示すユースケースにおけるリスクアセスメントであるため、本表中の「－」で表示されている項目についても十分な検討が必要です。

表１．サイトと前提

表中記号	サイトと前提
A1	RSC 機器 ・スタンドアロンを強制しない ・複数の HCF に対応する可能性がある ・リモートアクセス時には、個人の ID でなく組織の ID を使用することがある ・RSC 側には PHI は存在しないはず。
A2	内部経路の VPN 対策をしている場合
B1	RSC 内部ネットワーク ・論理的にアイソレーションしている
B2	内部経路の VPN 対策をしている場合
C1	外部経路の VPN 対策をしている場合
D1	HCF 内部ネットワーク ・アクセスポイントは集約する ・アクセスポイントは複数のベンダが同時に利用することがある ・リモートサービスとして修理／定期保守／稼動監視／ソフトウエア改版を行う ・リモートサービスを行う都度セッションを確立する（常時確立は想定しない） ・リモートサービスを行う都度接続手続きと切断手続きを行う ・イニシエーションは RSC->HCF とし、逆方向は認めない ・リモートアクセス時には個人識別はできなくてもよい。
E1	HCF 保守対象機器 ・病院の性格上入室管理を前提としない

表２．資産の分類

表中記号	資産内容
a	メモリ・ディスク・画面上の PHI
b	暗号アルゴリズムと鍵と鍵配送方式
c	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
d	メモリ・ディスク・画面上の PHI のバックアップ媒体
e	PHI を扱うソフトウエア
f	PHI を扱う機器
g	PHI を扱う機器の環境設備
h	PHI を扱う操作者
i	RSC 内部ネットワーク上の PHI
j	上記通信トレースのメモやプリントアウトの紙
k	上記通信トレースのバックアップ媒体
l	ネットワーク機器のソフトウエア
m	ネットワーク機器
n	ネットワーク機器の環境設備
o	ネットワーク機器の操作者
p	HCF内部ネットワーク上の PHI

表３．リスク評価表

	点数	評価基準
機密性	1	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対して脆弱性が無視できる
	2	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対してやや脆弱である
	3	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対して極めて脆弱である
完全性	1	改ざん,差換え,消去によるねつ造や否認に対する脆弱性が無視できる
	2	改ざん,差換え,消去によるねつ造や否認に対してやや脆弱である
	3	改ざん,差換え,消去によるねつ造や否認に対して極めて脆弱である
可用性	1	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性が無視できる
	2	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してやや脆弱である
	3	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して極めて脆弱である
影響性	1	経営・業務遂行に影響が無視できる
	2	経営・業務遂行に影響がでる可能性がある
	3	経営・業務遂行に重大な影響がでる可能性がある
発生可能性	1	起こる可能性が無視できる
	2	起こる可能性が少ない
	3	起こる可能性が多い

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性(C;機密性、I;完全性、A;可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
1.セキュリティ基本方針	1.1情報セキュリティ基本方針	情報セキュリティのための経営陣の指針及び支持を規定するため	1) 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること	1	—	—	—	—	—	—	—	—	—	—	—
			2) 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること	2	—	—	—	—	—	—	—	—	—	—	—
2.組織のセキュリティ	2.1情報セキュリティ基盤	組織内の情報セキュリティを管理するため	1) セキュリティを主導するための明りょうな方向付け及び経営者による目に見える形での支持を確実にするために、運営委員会を設置すること。運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること	3	—	—	—	—	—	—	—	—	—	—	—
			2) 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を設置すること	4	—	—	—	—	—	—	—	—	—	—	—
			3) 個々の資産の保護に対する責任及び特定のセキュリティ手続きの実施に対する責任を、明確に定めること	5	—	—	—	—	—	—	—	—	—	—	—
			4) 新しい情報処理設備に対する経営陣による認可手続を確立すること	6	—	—	—	—	—	—	—	—	—	—	—
			5) 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること	7	—	—	—	—	—	—	—	—	—	—	—
			6) 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること	8	—	—	—	—	—	—	—	—	—	—	—
			7) 情報セキュリティ基本方針の実施を、他者が見直すこと	9	—	—	—	—	—	—	—	—	—	—	—
	2.2第三者によるアクセスのセキュリティ	第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため	1) 組織の情報処理施設への第三者のアクセスに関連づけてリスクを評価し、適切な管理策を実施すること	10	—	—	—	—	—	—	—	—	—	—	—
			2) 組織の情報処理施設への第三者アクセスにかかわる取決めは、正式な契約に基づくこと	11	—	—	—	—	—	—	—	—	—	—	—
	2.3外部委託	情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため	1) 情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述されること					—	(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に繋がる	3→2	2	2	12→8	—	(管理策)外部委託契約(保守点検、バックアップ)は、(機能)ISP側の保守点検、バックアップを明文化して責任の分界を明確にすることによって、故障の予防し、(効果)サービス不能を防止
									(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に繋がる	3→2	2	1	6→4	—	(管理策)外部委託契約(防災対策、事業継続計画)は、(機能)ISP側の防災対策を明文化して責任の分界を明確にすることによって災害を予防し、(効果)サービス不能を防止できる。
					36	C1	m		(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に繋がる	3→2	2	1	6→4	—	(管理策)外部委託契約(施錠保管)は、(機能)ISPとの間の契約において、ISP側の施錠管理を明文化して、責任の分界を明確にすることによって破壊を予防し、(効果)サービス不能を防止で
									(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となると、リモートサービスの(脅威)サービス不能Aに繋がる	3→2	2	2	12→8	—	(管理策)外部委託契約(保守点検、バックアップ)は、(機能)ISP側の保守点検、バックアップを明文化して責任の分界を明確にすることによって、故障の予防し、(効果)サービス不能を防止
									(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に繋がる	3→2	2	1	6→4	—	(管理策)外部委託契約(防災対策、事業継続計画)は、(機能)ISP側の防災対策を明文化して責任の分界を明確にすることによって災害を予防し、(効果)サービス不能を防止できる。
				12	37	C1	n	—	(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に繋がる	3→2	2	1	6→4	—	(管理策)外部委託契約(施錠保管)は、(機能)ISPとの間の契約において、ISP側の施錠管理を明文化して、責任の分界を明確にすることによって破壊を予防し、(効果)サービス不能を防止で
3.資産の分類及び管理	3.1資産に対する責任	組織の資産の適切な保護を維持するため	1) 情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持すること	13	—	—	—	—	—	—	—	—	—	—	—
	3.2情報の分類	情報資産の適切なレベルでの保護を確実にするため	1) 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響(例えば、情報への認可されていないアクセス又は情報の損傷)を考慮に入れておくこ	14	—	—	—	—	—	—	—	—	—	—	—
			2) 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること	15	—	—	—	—	—	—	—	—	—	—	—

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性(C;機密性、I; 完全性、A; 可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
4.人的セキュリティ	4.1職務定義及び雇用におけるセキュリティ	人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため	1) セキュリティの役割及び責任は、組織の情報セキュリティ基本方針で定められたとおりに、職務定義書のなかに文書化すること	16	—	—	—	—	—	—	—	—	—	—	—
			2) 常勤職員を採用するときは、提出された応募資料の内容を検査すること	17	—	—	—	—	—	—	—	—	—	—	—
			3) 従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること		11	A1	a	RSC側当事者	(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に繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)RSCサービスマンによる盗用を抑制できる。
					12	A1	a	内部経路	(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に繋がる						
					19	A1	h	—	(脆弱性)収賄Cが行われると、PHIの(脅威)暴露Cに繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)収賄による盗用を抑制できる。
					28	B1									
					28	B2									
					48	D1	o								
					51	E1	a	HCF側当事者	(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に繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)一次サービスマンの盗用を抑制できる。
									(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にねつ造に繋がる	3	3	1	9	—	(管理策)守秘義務は、(機能)操作者の不正行為を牽制するので、(効果)医師等の盗用,差換えを抑制できるが、これだけでは効果が薄い。
					52	E1	a	外部経路 RSC側担当	(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に繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)RSCサービスマンの盗用を抑制できる。
								内部経路	(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に繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)医師等,HCFシステム管理者,一次サービスマンの盗用,差換えを抑制できる。
					53	E1	c	医師等	(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に繋がる	3	3	1	9	—	(管理策)守秘義務は、(機能)操作者の不正行為を牽制するので、(効果)医師等の盗用を抑制できるが、これだけでは効果が薄い。
					59	E1	h	PHIを扱う操作者	(脆弱性)収賄Cが行われると、(脅威)PHIの暴露Cに繋がる	3→2	3	1	9→6	—	(管理策)守秘義務や身元調査(資質の確認)は、(機能)操作者の不正行為を牽制したり予防するので、(効果)収賄による盗用を抑制できる。
			4) 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること	19	—	—	—	—	—	—	—	—	—	—	—
	4.2利用者の訓練	情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事の中で利用者が組織のセキュリティ基本方針を維持していくことを確実にするため	1) 組織の基本方針及び基準について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと		19	A1	h	—	(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に繋がる	3→2	3	2	18→12	—	(管理策)教育,技能基準は、(機能)操作者の資質を向上し維持するので、(効果)誤入力,誤消去によるサービス障害を予防できる。
					28	B1		—	(脆弱性)誤設定Cが行われると、PHIの(脅威)想定外の暴露Cに繋がる	3→2	3	2	18→12	—	(管理策)教育,技能基準は、(機能)操作者の資質を向上し維持するので、(効果)誤設定による想定外の暴露を予防できる。
					48	D1	o								
					59	E1	h	PHIを扱う操作者	(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に繋がる	3→2	3	2	18→12	—	(管理策)教育,技能基準は、(機能)操作者の資質を向上し維持するので、(効果)誤入力,誤消去によるサービス障害を予防できる。
	4.3セキュリティ事件・事故及び誤動作への対処	セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため	1) セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること	21	—	—	—	—	—	—	—	—	—	—	—
			2) 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること	22	—	—	—	—	—	—	—	—	—	—	—
			3) ソフトウェア誤動作を報告する手順を確立すること	23	—	—	—	—	—	—	—	—	—	—	—
			4) 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること	24	51	E1	a	HCF側当事者	(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に繋がる	3→2	3	1	9→6	—	(管理策)監視下の操作は、(機能)単独操作を防止するので、(効果)HCFシステム管理者による盗用,差換えを牽制できる。
			5) 組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること	25	—	—	—	—	—	—	—	—	—	—	—
5.物理的及び環境的セキュリティ	5.1セキュリティが保たれた領域	業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため	1) 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること	26	51	E1	a	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)パーティションは、(機能・効果)関係者以外の立ち寄りを抑止する管理策である。
			2) 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によってセキュリティの保たれた領域を保護すること		11	A1	a	—	(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、RSC機器内のPHIが盗用Cされ(脅威)暴露Cに繋がる	3→2	3	1	9→6	—	(管理策)入室管理は、(機能)権限の無い者の入室を防止するので、(効果)第3者,RSC社員,RSCネットワーク管理者の入室を阻止して画面の覗き見や不正ログインや成りすましを防止できる。
					13	A1	c	当事者以外	(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に繋がる	3→2	3	1	9→6	—	(管理策)入室管理は、(機能)権限の無い者の入室を防止するので、(効果)第3者,RSC社員,RSCネットワーク管理者による入室を阻止して紙の覗き見や持出を防止できる。
					14	A1	d	当事者以外	(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に繋がる	3→2	3	1	9→6	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)第3者,RSC社員,RSCネットワーク管理者による接触を阻止して媒体の持出を防止できる。
					16	A1	f	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)入室管理は、(機能)権限の無い者の入室を防止するので、(効果)RSCサービスマン以外の者の入室を阻止してRSC機器やそのディスクの持出を防止できる。
					17	A1	f	—	(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に繋がる	3→2	2	1	6→4	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)破壊によるサービス不能を防止できる。
					18	A1	g	—	(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に繋がる						
					22	B1	j	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)入室管理(通信トレース機器室)は、(機能)権限の無い者の入室を防止するので、(効果)RSCネットワーク管理者以外の者による入室を阻止して紙の覗き見や持出を防止できる。
					23	B1	k	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)RSCネットワーク管理者以外の者による接触を阻止して媒体の持出を防止できる。
					25	B1	m	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)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を防止できる。
					26	B1		—	(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に繋がる	3→2	2	1	6→4	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)破壊によるサービス不能を防止できる。
						B2	m								
					27	B1		—	(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に繋がる						
					27	B2	n								
					42	D1	j	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)シュレッダ廃棄は、(機能)資産を消去するので、(効果)HCFネットワーク管理者以外の者による紙の覗き見や持出を防止できる。 (管理策)入室管理(通信トレース機器室)は、(機能)権限の無い者の入室を防止するので、(効果)HCFネットワーク管理者以外の者による入室を阻止して紙の覗き見や持出を防止できる。
					43	D1	k	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)HCFネットワーク管理者以外の者による接触を阻止して媒体の持出を防止できる。
					45	D1	m	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)入室管理は、(機能)権限の無い者の入室を防止するので、(効果)HCFネットワーク管理者以外の者入室を阻止して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を防止できる。
					47	D1	n	—	(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に繋がる	3→2	2	1	6→4	—	(管理策)施錠保管は、(機能)権限の無い者の接触を防止するので、(効果)破壊によるサービス不能を防止できる。

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性（C:機密性、I: 完全性、A: 可用性）	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
					54	E1	d	医師等以外	（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に繋がる	3→2	3	1	9→6	—	（管理策）施錠保管は、（機能）権限の無い者の接触を防止するので、（効果）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接触を阻止して媒体の持出を防止できる。
					56	E1	f	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）施錠保管は、（機能）権限の無い者の接触を防止するので、（効果）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を防止できる。
					57	E1	f	—	（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に繋がる	3→2	2	1	6→4	—	（管理策）施錠保管は、（機能）権限の無い者の接触を防止するので、（効果）破壊によるサービス不能を防止できる。
				27	58	E1	g	—	（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に繋がる						
			3) セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること	28	—	—	—	—	—	—	—	—	—	—	—
			4) セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること		13	A1	c	RSC側当事者	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による入室管理は、（機能）権限の有る者の単独入室を防止するので、（効果）RSCサービスマンによる単独入室を阻止して紙の持出を牽制できる。
					14	A1	d	RSC側当事者	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）RSCサービスマンによる単独接触を阻止して媒体の持出を牽制できる。
					16	A1	f	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）RSCサービスマンによるRSC機器やそのディスクの持出を牽制できる。
								内部経路RSCネットワーク管理者以外	（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に繋がる	3→2	3	1	9→6	—	（管理策）RSC側内部経路点検は、（機能・効果）経路上のタッピング痕跡を検出する管理策である。
								内部経路RSCネットワーク管理者	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人によるRSC側内部経路点検は、（機能・効果）複数人で経路上のタッピング痕跡を検出する管理策である。
					21	B1	i		（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	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）RSCネットワーク管理者による単独接触を阻止してRSCネットワーク機器経由のPHIの暴
					22	B1	j	—	（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	3→2	3	1	9→6	—	（管理策）複数人管理による入室管理（通信トレース機器室）は、（機能）権限の有る者の単独入室を防止するので、（効果）RSCネットワーク管理者による単独入室を阻止して紙の持出を牽制
					23	B1	k	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）RSCネットワーク管理者による単独接触を阻止して媒体の持出を牽制できる。
					25	B1	m	—	（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及びそのディスクの持出Cが行われると、PHIの（脅威）	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）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及びそのディスク
								内部経路HCFネットワーク管理者以外	（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に繋がる	3→2	3	1	9→6	—	（管理策）HCF側内部経路点検は、（機能・効果）経路上のタッピング痕跡を検出する管理策である。
								内部経路HCFネットワーク管理者	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人によるHCF側内部経路点検は、（機能・効果）複数人で経路上のタッピング痕跡を検出する管理策である。
					41	D1	p		（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	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）HCFネットワーク管理者による単独接触を阻止してHCFネットワーク機器経由のPHIの暴
					42	D1	j	—	（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	3→2	3	1	9→6	—	（管理策）複数人管理による入室管理（通信トレース機器室）は、（機能）権限の有る者の単独入室を防止するので、（効果）HCFネットワーク管理者による単独入室を阻止して紙の持出を牽制
					43	D1	k	—	（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	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）HCFネットワーク管理者による単独接触を阻止して媒体の持出を牽制できる。
					45	D1	m	—	（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）	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）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
					54	E1	d	医師等	（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）医師等による単独接触を阻止して媒体の持出を牽制できる。
				29	56	E1	f		（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に繋がる	3→2	3	1	9→6	—	（管理策）複数人管理による施錠保管は、（機能）権限の有る者の単独接触を防止するので、（効果）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を牽制できる。
			5) 品物を受け渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること	30	—	—	—	—	—	—	—	—	—	—	—

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性(C:機密性、I:完全性、A:可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
	5.2装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること		16	A1	f	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)道路とサイトの距離の確保は、(機能)漏洩電磁波の受信を防止するので、(効果)PHIの暴露を防止できる。
					25	B1	m	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)シールは、(機能・効果)タンパリング痕跡を検出できる管理策である。
									(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に繋がる	3→2	3	1	9→6	—	(管理策)道路とサイトの距離の確保は、(機能)漏洩電磁波の受信を防止するので、(効果)PHIの暴露を防止できる。
					45	D1	m	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)シールは、(機能・効果)タンパリング痕跡を検出できる管理策である。
									(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に繋がる	3→2	3	1	9→6	—	(管理策)道路とサイトの距離の確保は、(機能)漏洩電磁波の受信を防止するので、(効果)PHIの暴露を防止できる。
					56	E1	f	—	(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に繋がる	3→2	3	1	9→6	—	(管理策)シールは、(機能・効果)タンパリング痕跡を検出できる管理策である。
				31					(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に繋がる	3→2	3	1	9→6	—	(管理策)道路とサイトの距離の確保は、(機能)漏洩電磁波の受信を防止するので、(効果)PHIの暴露を防止できる。
			2) 装置は、停電、その他の電源異常から保護すること	32	—	—	—	—	—	—	—	—	—	—	—
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること	33	—	—	—	—	—	—	—	—	—	—	—
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること	34	—	—	—	—	—	—	—	—	—	—	—
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること	35	—	—	—	—	—	—	—	—	—	—	—
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	36	11	A1	a	RSC側当事者	(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に繋がる	3→2	3	1	9→6	(管理策)ログオフ時の自動消去は、(機能)人的ミスを防止するので、(効果)RSCサービスマンのPHIの削除忘れを防止できる。	—
	5.3その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること	37	53	E1	c	医者等以外	(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,他社ー次サービスマン,ー次サービスマン,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に繋がる	3→2	3	1	9→6	—	(管理策)クリアデスクは、(機能)無人時の資産の放置を防止するので、(効果)第3者,HCF職員,HCFネットワーク管理者,他社ー次サービスマン,ー次サービスマン,HCFシステム管理者による紙の覗き見や持出を防止できる。
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできな	38	—	—	—	—	—	—	—	—	—	—	—

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性（C:機密性、I:完全性、A:可用性）	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
6.通信及び運用管理	6.1運用手順及び責任	情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと	39	—	—	—	—	—	—	—	—	—	—	—
			2) 情報処理設備及びシステムの変更について管理すること	40	—	—	—	—	—	—	—	—	—	—	—
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立すること		15	A1	e	—	（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に繋がる	3→2	3	2	18→12	—	（管理策）IRT（緊急事態対応体制）は、（機能）新種のコンピュータウィルスによる被害から回復するための管理策であるので、（効果）バックドアや情報を盗み出すプログラムによる被害から
					21	B1 B2	i	外部経路	（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に繋がる	3→2	3	1	9→6	—	（管理策）IRT（緊急事態対応体制）は、（機能・効果）不正アクセスによる被害から早期回復するための管理策である。
					24	B1	l	—	（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に繋がる	3→2	3	2	18→12	—	（管理策）IRT（緊急事態対応体制）は、（機能）新種のコンピュータウィルスによる被害から回復するための管理策であるので、（効果）バックドアや情報を盗み出すプログラムによる被害から
					41	D1	p	外部経路	（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に繋がる	3→2	3	1	9→6	—	（管理策）IRT（緊急事態対応体制）は、（機能・効果）不正アクセスによる被害から早期回復するための管理策である。
				41	44	D1	l	—	（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に繋がる	3→2	3	2	18→12	—	（管理策）IRT（緊急事態対応体制）は、（機能）新種のコンピュータウィルスによる被害から回復するための管理策であるので、（効果）バックドアや情報を盗み出すプログラムによる被害から早期回復できる。
					55	E1	e	—							
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮す	42	—	—	—	—	—	—	—	—	—	—	—
			5) 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明確に定め、文書化するこ	43	16	A1	f	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）シールは、（機能・効果）タンパリング痕跡を検出できる管理策である。
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れ	44	—	—	—	—	—	—	—	—	—	—	—
	6.2システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること	45	—	—	—	—	—	—	—	—	—	—	—
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること	46	—	—	—	—	—	—	—	—	—	—	—
	6.3悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること		15	A1	e	—	（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に繋がる	3→2	3	2	18→12	（管理策）コンピュータウィルス対策は、（機能）コンピュータウィルスを検出し駆除するので、（効果）バックドアや情報を盗み出すプログラムを検出し駆除できる	—
					24	B1									
				47	44	D1	l								
					55	E1	e								
	6.4システムの維持管理(Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること		17	A1	f	—	（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に繋がる	3→2	2	2	12→8	—	（管理策）保守点検、バックアップは、（機能）故障の予防であり、（効果）サービス不能を予防できる。
					18	A1	g	—	（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に繋がる						
					26	B1 B2	m	—	（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に繋がる						
					27	B1	n	—	（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となると、リモートサービスの（脅威）サービス不能Aに繋が						
					27	B2									
					46	D1	m	—	（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に繋がる						
					47	D1	n	—	（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となると、リモートサービスの（脅威）サービス不能Aに繋が						
					57	E1	f	—	（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に繋がる						
				48	58	E1	g	—	（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に繋がる						
			2) 運用担当者は、自分の作業の記録を継続すること	49	—	—	—	—	—	—	—	—	—	—	—
			3) 障害については報告を行い、是正処置を取ること	50	—	—	—	—	—	—	—	—	—	—	—
	6.5ネットワークの管理	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること					内部経路 RSCネットワーク管理者以外	（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に繋がる	1	3	1	3	（対策不要）	
									（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に繋がる						
									（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に繋がる						
								内部経路 RSCネットワーク管理者	（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に繋がる						
					21	B2	i		（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に繋がる						
					22	B2	j	—	（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覗き見C、持出Cが行われると、PHIの（脅威）暴露Cに繋がる						
									（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						
					23	B2	k	—	（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に繋がる						
									（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に繋がる						
					24	B2	l	—	（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に繋がる	1	3	2	6	（対策不要）	
					25	B2	m	—	（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に繋がる	1	3	1	3		
									（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に繋がる						
									（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に繋がる						
									（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に繋がる						
				51	28	B2	o	—	（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						
	6.6媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること		—	—	—	—	—	—	—	—	—	—	—
			2) 媒体が不要となった場合は、安全、かつ、確実に処分すること		13	A1	c	当事者以外	（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に繋がる	3→2	3	1	9→6	—	（管理策）シュレッダ廃棄は、（機能）資産を消去するので、（効果）第3者,RSC社員,RSCネットワーク管理者による紙の覗き見や持出を防止できる。
					22	B1	j	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）シュレッダ廃棄は、（機能）資産を消去するので、（効果）RSCネットワーク管理者以外の者による紙の覗き見や持出を防止できる。
				52	42	D1	j	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）シュレッダ廃棄は、（機能）資産を消去するので、（効果）HCFネットワーク管理者以外の者による紙の覗き見や持出を防止できる。

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性(C:機密性、I:完全性、A:可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	54	—	—	—	—	—	—	—	—	—	—	—
			4) 認可されていないアクセスからシステムに関する文書を保護すること	55	—	—	—	—	—	—	—	—	—	—	—
	6.7情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換(電子的又は人手によるもの)については、ある場合には正式な契約として、合意を取り交わすこと	56	—	—	—	—	—	—	—	—	—	—	—
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護するために管理策を適用すること	57	—	—	—	—	—	—	—	—	—	—	—
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護するために管理策を適用すること	58	—	—	—	—	—	—	—	—	—	—	—
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	59	—	—	—	—	—	—	—	—	—	—	—
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること	60	—	—	—	—	—	—	—	—	—	—	—
			6) 電子的に公開した情報の完全性を保護するように注意すること	61	—	—	—	—	—	—	—	—	—	—	—
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策をもつこと	62	—	—	—	—	—	—	—	—	—	—	—

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性（C:機密性、I:完全性、A:可用性）	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
7.アクセス制御	7.1アクセス制御に関する業務上の要求事	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定義し、文書化すること	63	—	—	—	—	—	—	—	—	—	—	—
	7.2利用者のアクセス管理	情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること		12	A1	a	内部経路	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）第3者,RSC社員,RSCネットワーク管理者による不正ログインを防止できる。	—
					21	B2	i	外部経路	（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に繋がる	3→2	3	1	9→6	（管理策）ルート制御（RSC機器にはつなげない）は、（機能・効果）RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理（ログイン）、ネットワークの分離・強制経路（FW）・フィルタリング、遠隔診断ポートの保護がある。	—
						B1	i	内部経路 RSCネットワーク管理者以外	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）RSCネットワーク管理者以外の者による不正ログインを防止できる。	—
					41	D1	p	外部経路	（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に繋がる	3→2	3	1	9→6	（管理策）ルート制御（RSC機器にはつなげない）は、（機能・効果）RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理（ログイン）、ネットワークの分離・強制経路（FW）・フィルタリング、遠隔診断ポートの保護がある。	—
						D1	p	内部経路 HCFネットワーク管理者以外	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）HCFネットワーク管理者以外の者による不正ログインを防止できる。	—
					51	E1	a	当事者以外	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）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不正ログインを防止できる。	—
								HCF側当事者	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（書込み禁止,ファイル消去禁止）は、（機能）権限の無い者の書込み禁止,ファイル消去を防止するので、（効果）一次サービスマンによる差換えを防止できる。	—
					52	E1	a	外部経路 RSC側当事者	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）他社RSCサービスマンによる不正ログインを防止できる。	—
									（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（書込み禁止,ファイル消去禁止）は、（機能）権限の無い者の書込み禁止,ファイル消去を防止するので、（効果）RSCサービスマンによる差換えを防止できる。	—
								内部経路	（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に繋がる	3→2	3	1	9→6	（管理策）アクセス管理（ログイン）は、（機能）権限の無い者の操作を防止するので、（効果）第3者,HCF職員,HCFネットワーク管理者による不正ログインを防止できる。	—
			2) 特権の割り当て及び使用は、制限し、管理すること	64	12	A1	a	内部経路	（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に繋がる	3→2	3	1	9→6	—	（管理策）権限管理（ユーザ/特権ログイン）は、「アクセス管理」と組合せで使われる管理策である。
					21	B1	i	内部経路 RSCネットワーク管理者以外	（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に繋がる						
					41	D1	p	—	（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に繋がる						
								当事者以外	（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						
					51	E1	a	HCF側当事者	（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に繋がる						
					51	E1	a	外部経路 RSC側当事者	（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に繋がる						
								外部経路 RSC側当事者	（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に繋がる						
					52	E1	a	内部経路	（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に繋がる						
			3) パスワードの割当ては、正規の管理手続によって統制すること	66	—	—	—	—	—	—	—	—	—	—	—
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に	67	—	—	—	—	—	—	—	—	—	—	—
7.3利用者の責任	認可されていない利用者のアクセスを防止するため		1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと		12	A1	a	—	（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に繋がる	3→2	3	1	9→6	—	（管理策）パスワードの定期的な変更は、（機能）パスワードの強度を維持するので、（効果）RSC機器の成りすましを防止できる。
					21	B2	i	外部経路	（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に繋がる	3→2	3	1	9→6	—	（管理策）パスワードの定期的な変更は、（機能）パスワードの強度を維持するので、（効果）RSC側ネットワーク機器の成りすましを防止できる。
						B1	i	内部経路 RSCネットワーク管理者以外	（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に繋がる						
					41	D1	p	外部経路	（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	3→2	3	1	9→6	—	（管理策）パスワードの定期的な変更は、（機能）パスワードの強度を維持するので、（効果）HCF側ネットワーク機器の成りすましを防止できる。
								内部経路 HCFネットワーク管理者以外	（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に繋がる						

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲						リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件		脆弱性(C:機密性、I:完全性、A:可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例	
					51	E1	a	当事者以外		(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	3→2	3	1	9→6	—	(管理策)パスワードの定期的な変更は、(機能)パスワードの強度を維持するので、(効果)保守対象機器の成りすましを防止できる。	
					52	E1	a	外部経路 RSC側当事者 内部経路		(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に繋がる (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に繋がる	3→2	3	1	9→6	—	(管理策)パスワードの定期的な変更は、(機能)パスワードの強度を維持するので、(効果)保守対象機器の成りすましを防止できる。	
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	69	—	—	—	—		—	—	—	—	—	—	—	
	7.4ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	70	—	—	—	—		—	—	—	—	—	—	—	
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること			B1		外部経路		(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に繋がる	3→2	3	1	9→6	(管理策)ルート制御(RSC機器にはつなげない)は、(機能・効果)RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理(ログイン)、ネットワークの分離・強制経路(FW)・フィルタリング、遠隔診断ポートの保護がある。	—
					21	B2	i										
					41	D1	p	外部経路		(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に繋がる	3→2	3	1	9→6	(管理策)ルート制御(RSC機器にはつなげない)は、(機能・効果)RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理(ログイン)、ネットワークの分離・強制経路(FW)・フィルタリング、遠隔診断ポートの保護がある。	—
				71						(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に繋がる	3→2	3	1	9→6	(管理策)ルート制御は、(機能・効果)経路を強制し接続機器を指定する管理策である。	—
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	72	—	—	—	—		—	—	—	—	—	—	—	
			4) 遠隔コンピュータシステムへの接続は、認証されること	73	—	—	—	—		—	—	—	—	—	—	—	
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること			B1		外部経路		(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に繋がる	3→2	3	1	9→6	(管理策)ルート制御(RSC機器にはつなげない)は、(機能・効果)RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理(ログイン)、ネットワークの分離・強制経路(FW)・フィルタリング、遠隔診断ポートの保護がある。	—
					21	B2	i										
					41	D1	p	外部経路		(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に繋がる	3→2	3	1	9→6	(管理策)ルート制御(RSC機器にはつなげない)は、(機能・効果)RSC機器のリモート接続を禁止する管理策である。なお、一般的なネットワーク管理策としては、RSC側ネットワーク機器、特にRSC出口におけるアクセス管理(ログイン)、ネットワークの分離・強制経路(FW)・フィルタリング、遠隔診断ポートの保護がある。	—
				74													
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	75	—	—	—	—		—	—	—	—	—	—	—	
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	76	—	—	—	—		—	—	—	—	—	—	—	
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと	77	—	—	—	—		—	—	—	—	—	—	—	
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること	78	—	—	—	—		—	—	—	—	—	—	—	
	7.5オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	79	—	—	—	—		—	—	—	—	—	—	—	
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	80	—	—	—	—		—	—	—	—	—	—	—	
			3) すべての利用者(技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者)は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子(利用者ID)を保有すること	81	—	—	—	—		—	—	—	—	—	—	—	
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	82	—	—	—	—		—	—	—	—	—	—	—	
			5) システムユーティリティのために認証手順を使用すること	83	—	—	—	—		—	—	—	—	—	—	—	
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮すること	84	—	—	—	—		—	—	—	—	—	—	—	
			7) リスクの高い場所(例えば、組織のセキュリティ管理外にある公共又は外部領域)にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末は遮断されること	85	—	—	—	—		—	—	—	—	—	—	—	
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供すること	86	—	—	—	—		—	—	—	—	—	—	—	

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性（C:機密性、I:完全性、A:可用性）	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
	7.6業務用ソフトウェアのアクセス制御	情報システムが保有する情報への認可されていないアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	87	—	—	—	—	—	—	—	—	—	—	—
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	88	—	—	—	—	—	—	—	—	—	—	—
	7.7システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること		11	A1	a	RSC側当事者	（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に繋がる	3→2	3	1	9→6	（管理策）記録（イベントの要求者・種類・日時等）は、「内部監査」と組合せで使われる管理策である。	—
					12	A1	a	内部経路	（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に繋がる						
					51	E1	a	HCF側当事者	（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に繋がる	3→2	3	1	9→6	（管理策）記録（イベントの要求者・種類・日時等）は、「内部監査」と組合せで使われる管理策である。	—
								外部経路 RSC側担当	（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に繋がる	3→2	3	1	9→6	（管理策）記録（イベントの要求者・種類・日時等）は、「内部監査」と組合せで使われる管理策である。	—
				89	52	E1	a	内部経路	（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に繋がる	3→2	3	1	9→6	（管理策）記録（イベントの要求者・種類・日時等）は、「内部監査」と組合せで使われる管理策である。	—
			2) 情報処理設備の使用状況を監視する手順を確立すること。監視の結果は、定期的に見直すこと		11	A1	a		（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に繋がる	3→2	3	1	9→6	—	（管理策）内部監査（記録）は、（機能）記録から不正操作を検出する管理策であるので、（効果）RSCサービスマンの盗用を検出できる。加えて、この管理策は（機能）不正操作を牽制するので、（効果）RSCサービスマンによる盗用を抑制できる。
					12	A1	a		（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に繋がる						
					51	E1	a	HCF側当事者	（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に繋がる	3→2	3	1	9→6	—	（管理策）内部監査（記録）は、（機能）記録から不正操作を検出する管理策であるので、（効果）一次サービスマンの盗用を検出できる。加えて、この管理策は（機能）不正操作を牽制するので、（効果）一次サービスマンの盗用を抑制できる。
								外部経路 RSC側担当者	（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に繋がる	3→2	3	1	9→6	—	（管理策）内部監査（記録）は、（機能）記録から不正操作を検出する管理策であるので、（効果）RSCサービスマンの盗用を検出できる。加えて、この管理策は（機能）不正操作を牽制するので、（効果）RSCサービスマンの盗用を抑制できる。
				90	52	E1	a	内部経路	（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に繋がる	3→2	3	1	9→6	—	（管理策）内部監査（記録）は、（機能）記録から不正操作を検出する管理策であるので、（効果）医師等,HCFシステム管理者,一次サービスマンの盗用,差換えを検出できる。加えて、この管理策は（機能）不正操作を牽制するので、（効果）医師等,HCFシステム管理者,一次サービスマンの
			3) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること。コンピュータの時計は正しく設定すること	91	—	—	—	—	—	—	—	—	—	—	—
	7.8移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特別	92	—	—	—	—	—	—	—	—	—	—	—
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手配されていることを確実にすること	93	—	—	—	—	—	—	—	—	—	—	—
8.システムの開発及び保守	8.1システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にしなければならない	94	—	—	—	—	—	—	—	—	—	—	—
	8.2業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること	95	—	—	—	—	—	—	—	—	—	—	—
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	96	—	—	—	—	—	—	—	—	—	—	—
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮すること	97	—	—	—	—	—	—	—	—	—	—	—
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること	98	—	—	—	—	—	—	—	—	—	—	—
	8.3暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること		1a	A2		—	（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に繋がる	3→2	3	1	9→6	—	（管理策）認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用は、（機能）暗号化データの解読に対する強度を維持するので、（効果）暗号化されたPHIの解読を防止できる。
					29	B2									
				99	39	C1	b								
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	100	—	—	—	—	—	—	—	—	—	—	—
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用	101	—	—	—	—	—	—	—	—	—	—	—
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いること	102	—	—	—	—	—	—	—	—	—	—	—
			5) 一連の合意された標準類，手順及び方法に基づく鍵管理システムを，暗号技術の利用を支援するために用いること	103	—	—	—	—	—	—	—	—	—	—	—

ISMS準拠リモートサービスリスクアセスメント表

RSS WG

情報セキュリティ管理基準				資産と脅威の対象範囲					リモートサービスにおけるコントロール							
章	項	目的	コントロール	要件番号	脅威番号	サイトと前提	資産	脅威条件	脆弱性(C:機密性、I:完全性、A:可用性)	脆弱性	影響性	発生可能性	評価	技術的管理策例	運用的管理策例
	8.4システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするた	1) 運用システムでのソフトウェアの実行を管理すること	104	—	—	—	—	—	—	—	—	—	—	—
			2) 試験データを保護し，管理すること	105	—	—	—	—	—	—	—	—	—	—	—
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持すること	106	—	—	—	—	—	—	—	—	—	—	—
	8.5開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	107	—	—	—	—	—	—	—	—	—	—	—
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	108	—	—	—	—	—	—	—	—	—	—	—
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	109	—	—	—	—	—	—	—	—	—	—	—
			4) 隠れチャネル(Covert channels)及びトロイの木馬(Trojan code)の危険性から保護するために，ソフトウェアの購入，使用及び修正を管理し，検査すること	110	—	—	—	—	—	—	—	—	—	—	—
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いること	111	—	—	—	—	—	—	—	—	—	—	—
9.事業継続管理	9.1事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	112	—	—	—	—	—	—	—	—	—	—	—
			2) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること	113	—	—	—	—	—	—	—	—	—	—	—
			3) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること。重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること	114	17	A1	f	—	(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に繋がる	3→2	2	1	6→4	—	(管理策)防災対策、事業継続計画は、(機能)災害の予防であり、(効果)災害による被害損失の最小化と早期回復ができる。
					18	A1	g	—	(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に繋がる						
					26	B1 B2	m	—	(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に繋がる						
					27	B1 B2	n	—	(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に繋がる						
					46	D1	m	—	(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に繋がる						
					47	D1	n	—	(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に繋がる						
					57	E1	f	—	(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に繋がる						
					58	E1	g	—	(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に繋がる						
			4) すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組	115	—	—	—	—	—	—	—	—	—	—	—
			5) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること。事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること	116	—	—	—	—	—	—	—	—	—	—	—
10.適合性	10.1法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	117	—	—	—	—	—	—	—	—	—	—	—
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するように，適切な手続を実行すること	118	—	—	—	—	—	—	—	—	—	—	—
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	119	—	—	—	—	—	—	—	—	—	—	—
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	120	—	—	—	—	—	—	—	—	—	—	—
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための管理策を用いること	121	—	—	—	—	—	—	—	—	—	—	—
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために，法的な助言を求めること	122	—	—	—	—	—	—	—	—	—	—	—
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	123	—	—	—	—	—	—	—	—	—	—	—
	10.2セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること	124	—	—	—	—	—	—	—	—	—	—	—
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	125	—	—	—	—	—	—	—	—	—	—	—
	10.3システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意され	126	—	—	—	—	—	—	—	—	—	—	—
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること	127	—	—	—	—	—	—	—	—	—	—	—

付録２　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）

	倉垣　公一	セコム（株）
	島西　聡	東芝医用システムエンジニアリング（株）
	手島　文彰	東芝メディカルシステムズ（株）
	奈須　孝二	横河電機（株）
	西田　慎一郎	（株）島津製作所
	野津　勤	横河電機（株）
	藤咲　喜丈	日本光電工業（株）
◎主査	松本　義和	（株）グッドマンヘルスケアＩＴソリューションズ
	三浦　広毅	（株）三菱総合研究所
	茗原　秀幸	三菱電機（株）
	吉村　仁	コニカミノルタエムジー（株）

（JAHIS 標準　06-001）

２００６年　６月　発行

リモートサービスセキュリティガイドライン

発行元　保健医療福祉システム工業会
〒105-0001　東京都港区虎ノ門１丁目１９－９
（虎ノ門ＴＢビル６Ｆ）
電話　03-3506　　ＦＡＸ　03-3506-8070