JAHIS

ＪＡＨＩＳ標準　１４－００３

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

Ver.2.1

２０１４年７月

一般社団法人 保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

JAHIS/JIRA 合同リモートサービスセキュリティ作成 WG

ま　え　が　き

医療の ICT 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、電子カルテシステムの順に整備され、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交換されるようになりました。

医療機器の保守においても、医療機関と医療機器ベンダとをネットワークで結び、安全にかつ効率的に行うようになってきました。そのためには、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。

JAHIS セキュリティ委員会では JIRA（一般社団法人 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。

その成果として、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」（技術文書 04-101）を、2005 年度にはより踏み込んだ内容の JAHIS 標準「リモートサービスセキュリティガイドライン」（JAHIS 標準 06-001）を制定し、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示しました。

上記の 2 つの文書で示されたリモートサービスにおけるセキュリティマネジメントの考え方は、国内に限らずどこでも参考になることから、本 WG では 2008 年度に、これらの記述から日本固有の法令、制度等に係る部分を取り除いたものを国際標準とすることを考え、ISO/TC215 に提案し、ISO 参加各国の賛同を受け、同作業会議における審議と修正を経て、「ISO TR 11633 Part 1&2」として 2009 年度に出版されました。またその際に施された修正や新たに加えられた記述に、再度国内での固有の法令、制度等に関する記述を加え直し、従来のガイド（技術文書 04-101）とガイドライン（JAHIS 標準 06-001）をガイドライン Ver.2.0 として統合しました。

Ver.2.1 では 2011 年に JAHIS,JIRA 会員各社に実施したリモートサービス実態調査の結果を踏まえ、SLA（Service Level Agreement）のリモート保守に関連する内容、ネットワークインフラの発達に伴いユースケースとして常時接続を追加、および最新の状況を加味した内容に改版しました。

本ガイドラインが、医療情報システムにおける安全なリモート保守の普及・推進に多少とも貢献できれば幸いです。

2014 年 7 月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会
JAHIS/JIRA 合同リモートサービスセキュリティ作成 WG

目　次

第１章　適応範囲

本書では、医療機関内の情報機器・システムを遠隔保守するケースのモデル化を行い、そのモデルに対して ISMS（Information Security Management System）の手法に従ったリスクマネジメントの実施例を示しています。医療機関の管理者、および遠隔保守を行うベンダは、ここでの実施例に倣うことにより、情報資産（特に診療に関する患者の個人情報）を安全かつ効率的に保護することができるようになります。

本書は ISMS の適用方法を示すことを目的としているため、ISMS の手法そのものについては、最小限の説明しか行っていません。したがって、本書の内容を理解するためには、読者が ISMS の手法を既に習得しているか、または ISMS に関する詳細な文献を合わせて参照されることを想定しています。

第２章　引用規格・引用文献

日本規格協会・JIS Q 27001:2006(ISO/IEC 27001:2005) 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

日本規格協会・JIS Q 27002:2006(ISO/IEC 27002:2005) 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範

厚生労働省・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
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf

厚生労働省・医療情報システムの安全管理に関するガイドライン　第 4.2 版

http://www.mhlw.go.jp/stf/shingi/0000026088.html

経済産業省・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
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

第３章　用語の定義

アカウント

特定のコンピュータ システム、もしくはネットワークにアクセスするために「認証」される人を表現しており、権限属性をもつことがある。

アクセス制御

コンピュータセキュリティにおいて、ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすること。

アクセスログ

情報の作成、変更、参照、削除などの記録。

インシデント

情報セキュリティリスクが発現・現実化した事象。

インターフェース

プログラムや装置、操作者といった対象の間で情報のやりとりを仲介するもの。また、その規格。

改ざん

情報を管理者の許可を得ずに書き換える行為。

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。

サイト

本書におけるリモートサービス全体の領域を、リスク分析を行うために区分した単位。

常時接続

本書で言う常時接続とは、一般的に言われる常時ネットワーク接続されている状態のことだけではなく、医療施設、リモートサービスセンタ双方から適宜（医療施設側のネットワーク管理者の許可を都度必要とせずに）セッションを張ることができる接続形態のことをさす。

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。

相互運用性

異なったアプリケーションやシステム､構成コンポーネント間で情報の伝達または共有がなされ相互に接続、利用できる共通性を持つこと。

デバイス

コンピュータに搭載あるいは接続されるハードウェア。

保存性

記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されること。

第４章　記号および略語

このガイドラインでは、次の記号および略語・表記を用いる。

COCIR	欧州放射線医用電子機器産業連合会（the European Coordination Committee of the Radiological, and Electromedical and Healthcare IT Industry）
HCF	医療施設（Health Care Facility）
HIPAA	医療保険の携行と責任に関する法律（The Health Insurance Portability and Accountability Act）
ISMS	情報セキュリティマネジメントシステム（Information Security Management System）
ISP	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（Internet Service Provider）
JAHIS	一般社団法人　保健医療福祉情報システム工業会　（http://www.jahis.jp）（Japanese Association of Healthcare Information Systems Industry）
JIPDEC	一般財団法人 日本情報経済社会推進協会（JapanInstitute for Promotion of Digital Economy and Community）
JIRA	一般社団法人　日本画像医療システム工業会（http://www.jira-net.or.jp）（Japan Medical Imaging and Radiological Systems industries Association）
NEMA	米国電子機器工業会（National Electrical Manufacturers Association）
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	保護対象の医療情報（Protected Healthcare Information）
RSC	リモートサービスセンタ（Remote Service Center）
SPC	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。（Security & Privacy Committee）
VPN	仮想的な専用通信回線（Virtual Private Network）

第５章　リモートサービスセキュリティ

５．１　リモートサービスセキュリティとは

ここでは、本書が対象にするリモートサービスの例とそのメリットや考慮しなければならないセキュリティ上の問題について概説します。

本書における「医療情報システム」とは、厚生労働省発行の「医療情報システムの安全管理に関するガイドライン第 4.2 版」(以下、「安全管理ガイドライン」)が対象としているものです。

５．１．１　リモートサービスの概要

医療機関と外部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。

最近の各種検査機器、各種情報システムには、自己診断機能を有し障害の早期発見、障害箇所の特定、および障害内容などの情報を提供するものもあります。更に、通信機能を持ち、自己診断機能による情報を機器・システムから電子メールなどの手段で保守サービスベンダのリモートサービスセンタに送り対策することで機器・システムの可用性を高めたり、修正ソフトウェア等をリモートサービスセンタから医療機関に提供したりすることも可能になりました。

以下、これらのネットワーク接続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紹介します。

（１）障害対応

医療機関のユーザが機器・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、ベンダのサポート担当者が直接対象機器・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リモート作業で復旧させることが可能な場合もあります。ハードウェア的障害であったとしても、現地の作業員に適切な指示を送り共同して復旧させることが可能になります。

（２）予防保守のための情報収集

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兆候を、事前に検出できることがあります。機器の消耗部品の劣化度を監視している例もあります。

なんらかの兆候が検出された場合には、その記録を機器・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の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、機器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実現できます。これにより（１）に記載した障害対応に円滑に繋げることが可能になります。

（３）ソフトウェア改訂・更新

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予防保守やなんら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な場合があります。

５．１．２　リモートサービスの必要性

リモートサービスにより医療機関側もベンダ側も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

近年の医療機器・システムは技術的に高度化しており、保守サービス員の専門性も求められています。

リモートサービスを用いない場合の作業は、原則としてベンダから派遣された保守サービス員のみになります。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、専門知識のある保守サービス員があらかじめ異常個所の特定、対応策を検討してから保守サービス員の派遣が可能となったり、リモートサービスセンタから直接機器やシステムにアクセスして情報の収集ができるため、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。

また、ソフトウェアだけの問題であれば、直接リモート作業で復旧させることが可能な場合もあります。

（２）予防保守

自己診断機能などにより装置やシステム自体の稼働状態のモニタ内容をリモートで監視することで、交換が必要な部品の交換時期を予測したり、故障につながる微細な異常を早期に把握したり、より効率的な保守計画を設定できます。

（３）保守費用の大幅低減

（１）（２）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り、保守作業時間の削減が可能になります。この直接的費用削減も見込めます

が、ベンダのサービス拠点を集約することも可能となるため、保守サービスを実現するための費用が節減でき、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）医療機関側職員の対応も低減

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、医療機関にとって医療サービスの安定した提供のために有用です。

５．１．３　リモートサービスのリスク

個人情報保護法の成立を契機として、医療機関はもとより、患者側にも診療情報の保護についての関心が高まっています。

機器・システムの保守サービスに当たっては、患者個人情報を含む診療情報に触れる場合も多いことから、リモートサービスは、上記の様な長所も有る反面、ネットワーク上のリスクやリモートサービスを担う施設(リモートサービスセンタ)での不適切な情報取り扱いによる個人情報漏洩のリスクもあります。

以下に、リスクを考える上でのテーマを挙げます。

（１）ネットワーク上の問題

ネットワーク化で利便性が高まるとともに、ネットワーク上の悪意を持った存在(個人や組織)による個人情報の大量持ち出しや、情報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。医療機関とリモートサービスセンタ間をつなぐネットワークの種別や通信事業者の選定によって、このセキュリティに関する内容も変わってきます。

「安全管理ガイドライン 6.11 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」には、ネットワークの種類毎にそのリスクや対策が書かれており、リモートサービス(リモートメンテナンス)を含めての安全管理措置の要求事項が書かれています。

（２）リモートサービスセンタでの情報管理

リモートサービスの実施者は医療機関内には居ません。すなわち、医療機関側の責任者の目の届かない所からの情報アクセスによる作業のため、リモートサービスセンタ自身が医療機関側から信頼を貰えるセキュリティ対策をとる必要があります。

リモートサービスをすることによる機器・システムへの極端な負荷増などの悪影響は排除しなければなりません。このことの説明も必要です。

許可されたサービス員以外のアクセスの制限、メンテナンス作業に用いた医療機関からの情報の安全な管理と破棄作業、その記録などが求められます。

サービスベンダ自身あるいはリモートサービスセンタがプライバシマーク（JIS Q 15001）や ISMS 認定を受けていることは、信頼に値することの目安になります。

「安全管理ガイドライン 6.8 情報システムの改造と保守」には、リモートサービス(リモートメンテナンス)による作業を含めての安全管理措置の要求事項が書かれています。

（３）責任のあり方

業務委託契約を締結しているサービスベンダは医療機関から監督を受ける立場になり、（２）で述べた安全管理を実施していることの説明、場合によっては証明が必要になります。

リモートサービスは通信回線事業者が提供するネットワークを介して行われるのが一般的です。この場合、医療機関、サービスベンダ、通信回線事業者の各組織間の責任分界点の定義、障害発生時の対応責任、すなわち責任の明確化が必要です。

「安全管理ガイドライン 4 電子的な医療情報を扱う際の責任のあり方　4.3 例示による責任分界点の考え方の整理」には、リモートサービス(リモートメンテナンス)を含めての要求事項が書かれています。

以上の様に、ネットワーク上の問題だけでなく、リモートサービスセンタでの情報管理、責任のあり方も含めたリモートサービスにおける情報資産の保護がリモートサービスセキュリティです。

５．２　法的適合性

５．２．１　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、厚生労働省により「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「安全管理ガイドライン」が制定されており、医療機関等においてその遵守が求められています。

リモートサービスは、対象となる医療機器、医療情報システムの保守等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ります。その場合、リモートサービスの受託が医療機関等からみた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おいては、医療機関から「医療事業者ガイドライン」、ならびに「安全管理ガイドライン」に対する遵守を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。

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。しかし、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など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、とくに医療機関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、医療機関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。

５．２．２　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、電子保存を行う際に以下の三基準を確保することです。通称 e-文書法に対する厚生労働省の省令においてこの考え方が示されてされています。

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。リモートサービスにおいても同様の対策が必要になります。

５．２．３　「安全管理ガイドライン」への対応

保守作業における脅威については、「安全管理ガイドライン」6.8 節の B. 考え方、では以下のように示されています。

- **個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等**
- **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**

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）**

上記の考え方は、C 項最低限のガイドラインに具体的な対策としてまとめられており、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作業時の医療機関等の関係者からの監督

などの要請に対し対応する必要があります。

また、C 項では通常の保守における要求事項に加え、「リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業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。

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、①作業者が直接医療機関等の関係者の監督下にいない、②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、「安全管理ガイドライン」6.8 で挙げられている対策だけでなく、6.11「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」に記載された、ネットワークを利用する際の追加対策が必要です。

５．３　契約・合意事項

前項でも述べましたが、リモートサービスは医療機器や医療情報システムに対する保守作業のひとつのサービス形態であり、その実施においては保守契約を結んで行われます。保守契約の中では、保守サービスの内容や、料金・支払い条件等が定められます。これまでは、保守契約の中で保守サービスの内容や水準（達成目標等）について厳密に定義されていないケースが多かったですが、最近は、こういった保守サービス内容や水準の合意事項を明確に示したSLA(Service Level Agreement)を含むケースが増えてきています。

SLAは、サービス利用者と提供者の間でのサービス内容についての合意事項を文書化したものです。「合意」ですので、一方的な通知事項ではありません。また、一式に纏った文書でなくても良く、諸々の契約や合意を記載した文書中に該当内容が散在している事でも構いません。サービス内容について双方の合意を示す文書内容の総称です。

リモートサービスについてのSLAには、リモートサービスの一般的事項のほか、「５．１．３　リモートサービスのリスク」、「５．２　法的適合性」を踏まえた内容が記載されている必要があります。

一般的事項とは、提供サービスの責任組織構成、サービス時間帯、応答性能、保守サービスの手順などです。

本書が対象とする医療情報システム特有の事項としては、

- **利用者が監督責任を果たすに必要な提出文書類や監査に関する事項**
- **利用者、提供者および関与する事業者毎の責任分界**
- **提供者が保守に必要なデータを取得する場合の手続き**
- **提供者の取得データの保管・分析・利用後の破棄に関する安全性確保策（例えば、保管データへのアクセス権限管理、ログの保存期間、など）**
- **提供者から利用者への報告方法や提出内容**

などが挙げられます。

SLA作成時には、総務省発行の「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドラインに基づくSLA参考例」
（http://www.soumu.go.jp/main_content/000095028.pdf）が参考になります。なお、この例はASP・SaaSによる診療録の作成、その保存、およびそれに伴うサービスを主にしており、この中の全事項がリモートサービスに必要ということではありません。

第６章　リモートサービスへの ISMS の適用

６．１　セキュリティ要件

６．１．１　セキュリティ対策の全体的な方針

日本のリモートサービスにおける個人情報の保護は、図 6-1-1 に示すような枠組みで行われています。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、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になります。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。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ます。

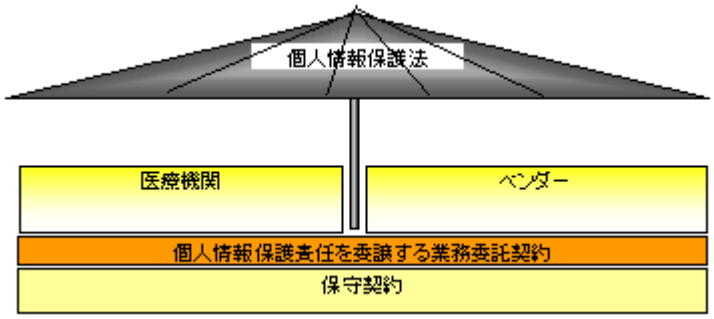

図６－１－１　日本のリモートサービスにおける個人情報保護の枠組み

リモートサービスの業務委託契約において個人情報保護という観点からは、「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。個人情報保護法において「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 6-1-2 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、6.1.2 節

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。

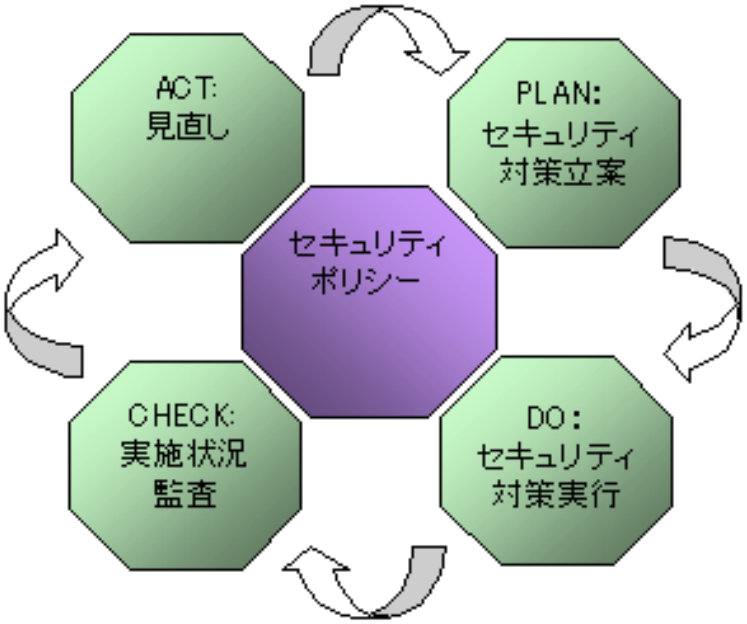

図６－１－２　情報セキュリティマネジメントシステム概念図

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ー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。

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、継続的な情報収集およ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およ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。

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**
- **セキュリティ対策基準**
- **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（6.7 節）**

６．１．２　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。

（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（6.1.6 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 ISO 化されており、ISO/IEC27001 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 ISO/IEC27001 に従うのは第三者評価を受けるために非常に有効です。ISO/IEC27001 においては、リスク対応のための管理項目および管理策が 133 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。

６．１．３　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。

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。

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の禁止
- 許可範囲以外の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。

６．１．４　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、リモートサービスセンタと医療機関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 ISO/IEC27001 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。133 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。

６．１．５　ソリューションの選定

対象となるリモートサービスセンタ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、リモートサービスセンタ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。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。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。

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。

（１）リモートサービス室入室時の認証

- **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）リモートサービス機器ログイン時の認証

- **ワンタイムパスワード**
- **IC カード**
- **PKI**
- **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**

６．１．６　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

- **アクセスポリシ**
- **ユーザ登録の規定**
- **特権管理**
- **カードやパスワードの管理**
- **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

- **施設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

- **バックアップ作業規定**
- **メディア保管規定**
- **処分規定**

（５）VPN、IDS、FW、PROXY 等のセキュリティ装置

- **各種設定および変更規定**
- **シグネチャ、パターンファイルなどの情報の更新規定**
- **チューニングの規定**
- **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

- **仕事の定義**
- **人員採用審査やポリシ**

- **秘密保持合意文書**

（９）教育・訓練

（１０）その他

- **バージョンアップ、パッチ処理の規定**
- 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の整合性チェック

６．２　リモートサービスにおけるセキュリティ基本方針

ISO/IEC 27001:2005 を JIS 化した JIS Q 27001:2006 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，その目的および適用範囲，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およ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，標準類および適合する要求事項の簡潔な説明
> 1)法律上およ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)ウイルスおよび他の悪意のあるソフトウェアの予防および検出
> 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および特定責任の定義
> 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およ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 Q 27001:2006　3.1.1　情報セキュリティ基本方針文書　より引用）

これらの事項をリモートサービスセキュリティ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。

リモートサービスセキュリティでのセキュリティ基本方針には、セキュリティに関する技術的・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医療機器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。

６．３　標準的事例におけるリスクの評価

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の評価を行い、セキュリティ対策を行なうものです。自身でリスクの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の評価を実施し、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属書 A および B を参照してください。

付属書 B のリスクアセスメントシートは、日本情報経済社会推進協会（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/IEC27001 および 27002、ならびに JIS Q 27001 および 27002 に準拠しており、11 の管理分野と、133 の管理策から構成されています。11 の管理分野は以下のとおりです。

①情報セキュリティ基本方針
経営者による組織横断的なセキュリティポリシの発行、および支援について規定

②情報セキュリティのための組織
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人的資源のセキュリティ
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

⑥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

⑦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

⑧情報システムの取得、開発および保守
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

⑨情報セキュリティインシデントの管理
情報セキュリティの脆弱性が明らかになった際の改善に関する規定

⑩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

⑪コンプライアンス（順守）
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

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。

６．４　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。

- **リモートサービスセンタ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**

６．５　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。

６．６　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 6-6-1 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８章にて詳しく解説します。

表６－６－１　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

６．６．１　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、その完全な対策のためにはコストがかかりすぎるあるいは対策不可能な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。ここで医療機関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。

医療機関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、リモート

サービスセンタ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。リモートサービスセンタでは、本章で解説した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。医療機関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、残存リスクを見直していきます。

６．７　セキュリティ監査と外部監査の推奨

６．７．１　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。実際の評価に当たっては適切な監査を行うための監査証跡の取得が重要になります。監査証跡の重要性については、MEDIS-DC 発行の「個人情報保護に役立つ監査証跡ガイド」が参考になります。また、監査証跡の詳細については、JAHIS 標準０９－００３「JAHIS ヘルスケア分野の監査証跡メッセージ規約 V1.1」を参考にして必要な監査ログを取得することを推奨します。

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、医療機関、リモートサービスセンタ両者にとって有益な施策といえます。

６．７．２　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。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。医療機関、リモートサービスセンタ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　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。なお、本章以降、リモートサービス対象機器が設置されている医療施設のことをHCF(Health Care Facility)、リモートサービス用機器が設置されているリモートサービスセンタのことをRSC(Remote Service Center)と略して表記します。

（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。

これらのユースケースでは、HCF 内の保守対象機器と内部ネットワーク、HCF と RSC 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 7-1)

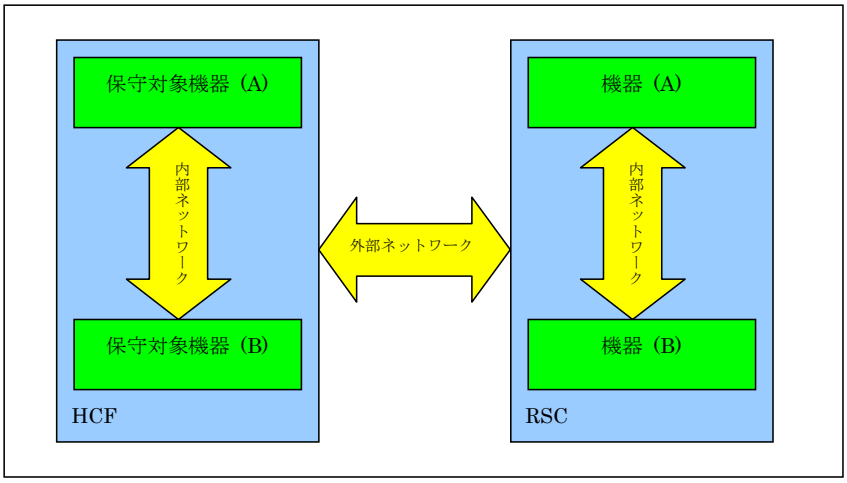

図７－１　リモートサービスのシステムの想定

７．１　故障時の対応

７．１．１　故障時の対応（HCF がアクセスポイントを制御するケース）

故障時の対応におけるワークフローを図 7-1-1 に示します。

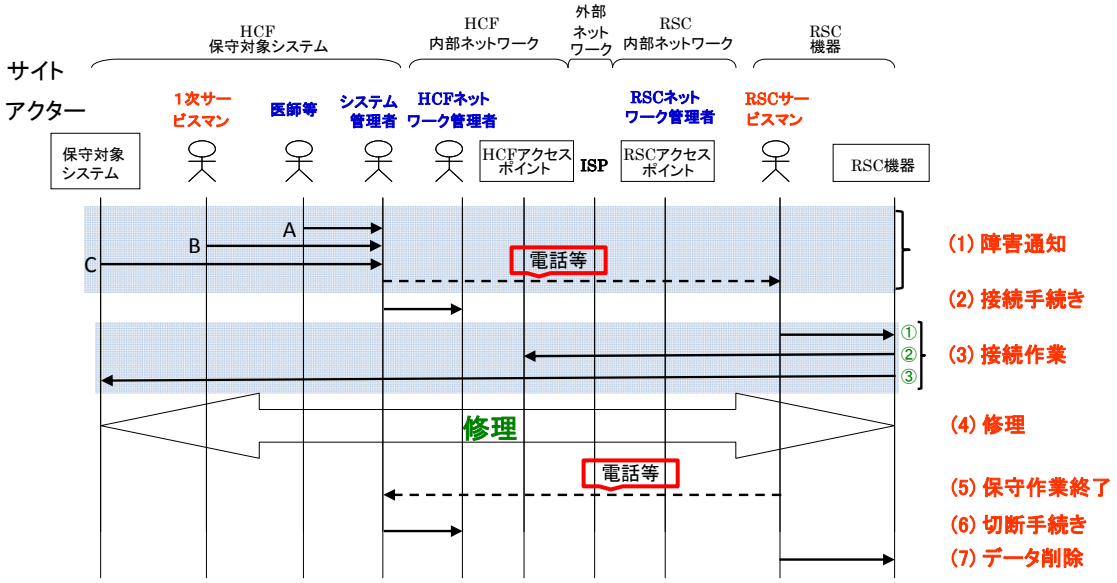

図７－１－１　故障時の対応のワークフロー

手順は次のようになります。

（１）　HCF のシステム管理者が問題発生の連絡を受け、RSC サービスマンへ電話等で通知する

HCF 内での連絡のパターンは以下 A、B、C を想定している。

A：医師等から HCF のシステム管理者に連絡する場合

B：HCF で作業中の 1 次サービスマンから HCF のシステム管理者に連絡する場合

C：保守対象システムから HCF のシステム管理者にアラートが発呼される場合

（２）　システム管理者が RSC から HCF のへのリモートサービスのためのネットワーク接続を HCF ネットワーク管理者へ申請する。

（３）　RSC から HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器から HCF アクセスポイントに接続

③　RSC 機器と保守対象機器とのネットワーク接続が確立

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

（例）

・自己診断プログラムの実行

・当該機器からの関連情報の取得

・問題の切り分け

・当該機器の変更・更新作業

・１次サービスマンに連絡し故障部品の手配・交換の依頼

・修理後の動作確認

（５） RSC サービスマンから HCF のシステム管理者にリモート保守作業終了の連絡を行う。

（６） HCF のシステム管理者が、リモートサービスのためのネットワーク切断を HCF ネットワーク管理者へ申請する。

（７） RSC 側に PHI を転送した場合には、RSC サービスマンがそれらの PHI を全て削除する。

７．１．２　故障時の対応（HCF と RSC が常時接続されているケース）

故障時の対応におけるワークフローを図 7-1-2 に示します。

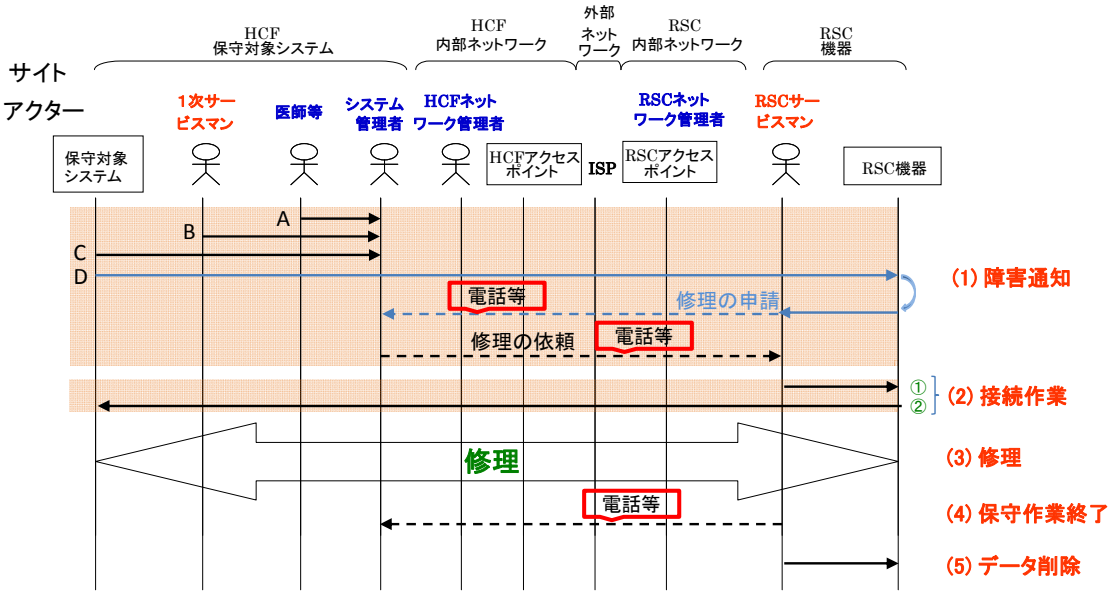

図７－１－２　常時接続における故障時の対応のワークフロー

手順は次のようになります。

（１）　HCF のシステム管理者が問題発生の連絡を受け、RSC サービスマンへ電話などで通知する（パターン A, B, C）。あるいは、保守対象システムから常時接続回線を通じて RSC 機器にアラートが発呼され RSC サービスマンから HCF のシステム管理者へ電話などで修理依頼を行う（パターン D）。

HCF 内での連絡のパターンは以下 A、B、C を想定している。

A：医師等から HCF のシステム管理者に連絡する場合

B：HCF で作業中の 1 次サービスマンから HCF のシステム管理者に連絡する場合

C：保守対象システムから HCF のシステム管理者にアラートが発呼される場合

（２）　RSC から HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器と保守対象機器とのネットワーク接続が確立

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

（例）

・自己診断プログラムの実行

・当該機器からの関連情報の取得

・問題の切り分け

・当該機器の変更・更新作業

・１次サービスマンに連絡し故障部品の手配・交換の依頼

・修理後の動作確認

（４）　RSC サービスマンから HCF のシステム管理者にリモート保守作業終了の連絡を行う。

（５）　RSC 側に PHI を転送した場合には、RSC サービスマンがそれらの PHI を全て削除する。

７．２　定期保守・定期監視

７．２．１　定期保守・定期監視（HCF がアクセスポイントを制御するケース）

定期保守・定期監視におけるワークフローを図 7-2-1 に示します。

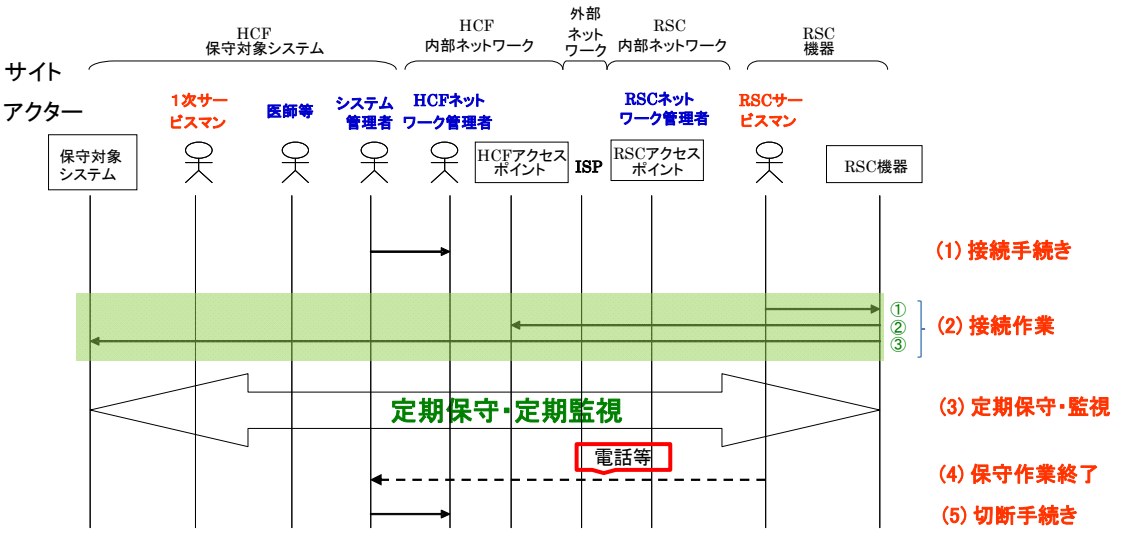

図７－２－１　定期保守・定期監視におけるワークフロー

手順は次のようになります。

（１）　HCF のシステム管理者が、RSC から HCF へのリモートサービスのためのネットワーク接続を HCF ネットワーク管理者へ申請する。

（２）　RSC から HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器から HCF アクセスポイントに接続

③　RSC 機器と保守対象機器とのネットワーク接続が確立

（３）　RSC サービスマンが定期点検作業・定期監視作業を行う。

（例）

・自己診断プログラムの実行

・各種ログの確認

・画質（精度）チェック

・稼動情報の取得

（４）　RSC サービスマンから HCF のシステム管理者にリモート定期保守・定期監視作業終了の連絡を行う。

（５）　HCF のシステム管理者がリモートサービスのためのネットワークの切断を HCF ネットワーク管理者へ申請する。

７．２．２　定期保守・定期監視（HCF と RSC が常時接続されているケース）

定期保守・定期監視（常時接続）におけるワークフローを図 7-2-2 に示します。

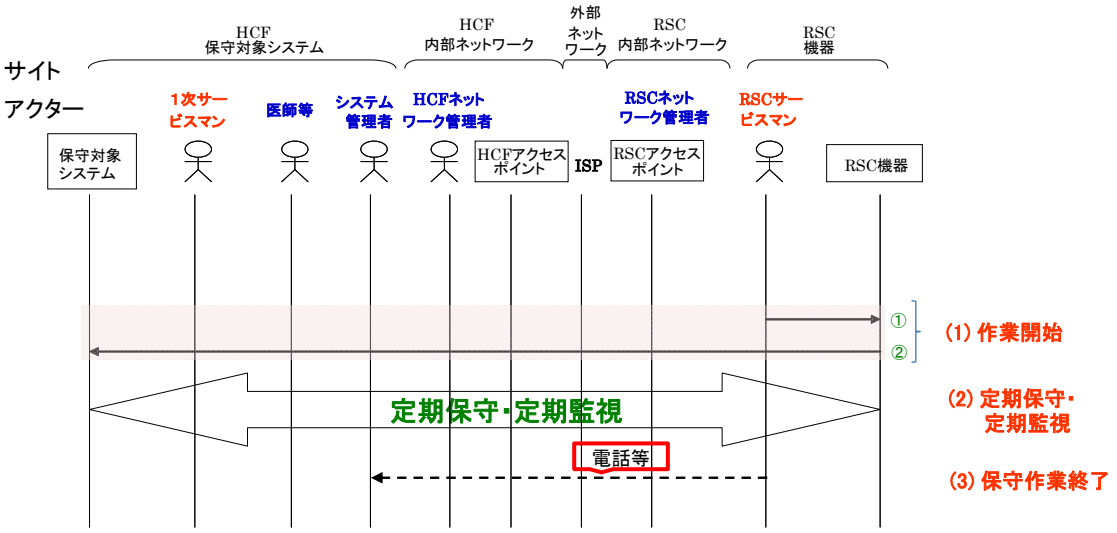

図７－２－２　定期保守・定期監視（常時接続）のワークフロー

手順は次のようになります。

（１）　RSC から HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器と保守対象機器とのネットワーク接続が確立

（２）　RSC サービスマンが定期点検作業・定期監視作業を行う。

（例）

・自己診断プログラムの実行

・各種ログの確認

・画質（精度）チェック

・稼動情報の取得

（３）　RSC サービスマンから HCF のシステム管理者にリモート定期保守・定期監視作業終了の連絡を行う。

７．３　ソフトウェアの改訂

７．３．１　ソフトウェアの改訂（HCF がアクセスポイントを制御するケース）

ソフトウェアの改訂におけるワークフローを図 7-3-1 に示します。

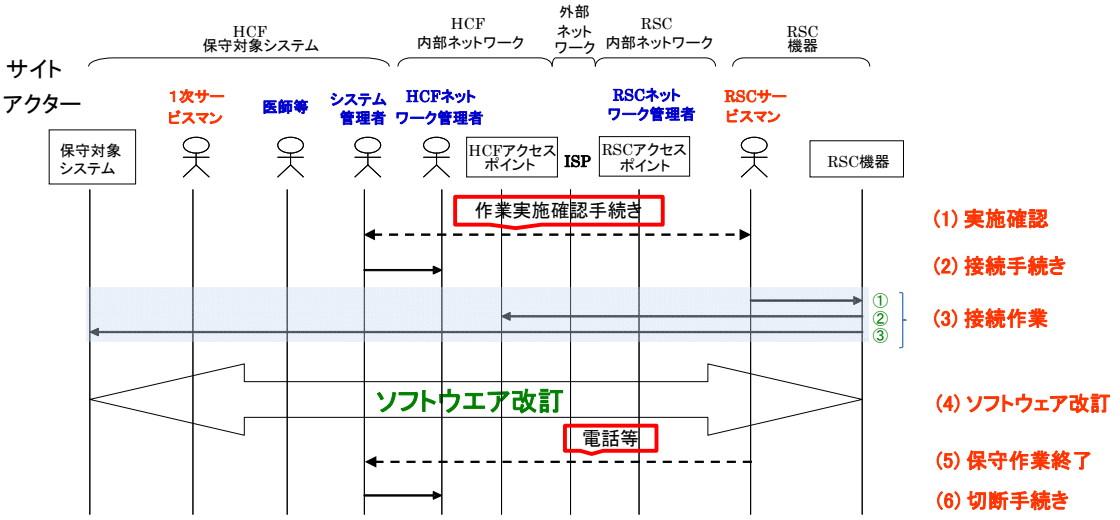

図７－３－１　ソフトウェアの改定のワークフロー

手順は次のようになります。

（１）　HCF のシステム管理者と RSC サービスマン間で作業実施の確認手続きを行う。

（２）　HCF のシステム管理者が、HCF ネットワーク管理者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 HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器から HCF アクセスポイントに接続

③　RSC 機器と保守対象機器とのネットワーク接続が確立

（４）　RSC サービスマンがソフトウェアの改訂作業を行う。

（例）

・ソフトウェアの入替え

・設定変更

・動作確認

（５）　RSC サービスマンが HCF のシステム管理者にソフトウェア改訂の作業終了報告の連絡を行う。

（６）　HCF のシステム管理者がリモートサービスのためのネットワークの切断を HCF ネットワーク管理者へ申請する。

７．３．２　ソフトウェアの改訂（HCF と RSC が常時接続されているケース）

ソフトウェアの改訂におけるワークフローを図 7-3-2 に示します。

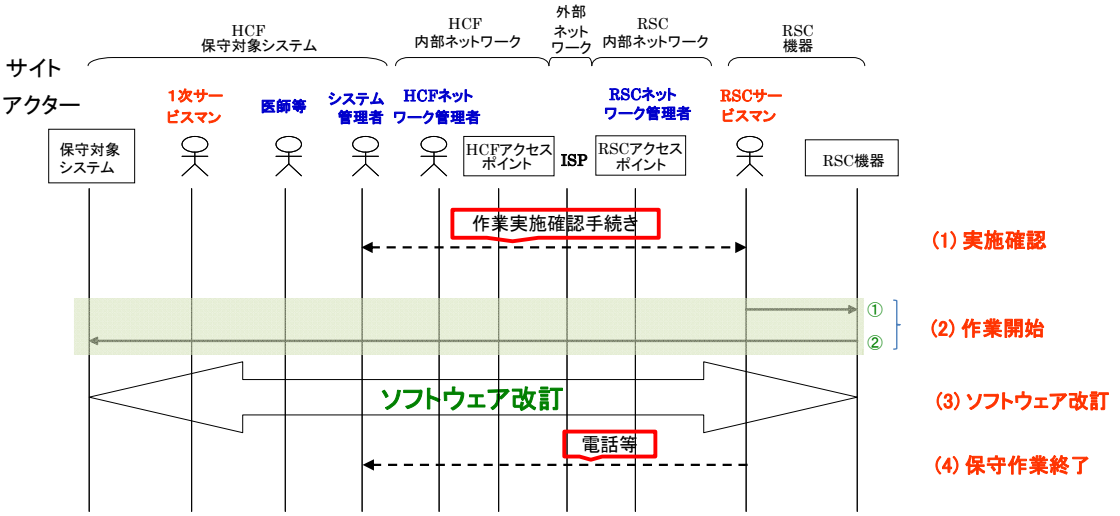

図７－３－２　ソフトウェアの改訂（常時接続）のワークフロー

手順は次のようになります。

（１）　HCF のシステム管理者と RSC サービスマン間で作業実施の確認手続きを行う。

（２）　RSC から HCF にネットワーク接続を以下の手順で実行する。

①　RSC サービスマンが RSC 機器を操作

②　RSC 機器から HCF アクセスポイントに接続

③　RSC 機器と保守対象機器とのネットワーク接続が確立

（３）　RSC サービスマンがソフトウェアの改訂作業を行う。

（例）

・ソフトウェアの入替え

・設定変更

・動作確認

（４）　RSC サービスマンが HCF のシステム管理者にソフトウェア改訂の作業終了報告の連絡を行う。

第８章　リスク分析とセキュリティ対策

８．１　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、サイト毎に資産を洗い出し、それに対する脅威と脆弱性を分析します。

８．１．１　リスク分析の考え方と基準

（１）考え方

HCF 内のリスクについては､その HCF の情報管理責任者が対策を考える必要があります。したがって、その範囲外と情報をやりとりするときには、RSC と HCF 間のネットワーク形態や、リモートサービスをおこなう際の物理的な環境等などを考慮してセキュリティを講じる必要があります。

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 HCF の場合の分析は、別途、HCF 毎に行う必要があります。

（２）適応範囲

本ガイドラインの運用モデルにおける ISMS の適用範囲は下記の箇所になります。

- **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 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 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 関係者”といえども、HCF 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。

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

- **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**
- **バグあるいは機器等の設定不備によるリスク**
- **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**

（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。

- **機密性:覗き見／盗用、不正ログイン／成りすまし、持ち出しなどによる暴露に対する脆弱度合い**
- **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**
- **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**

（５）影響性

情報資産に対する脅威が顕著化した場合に、経営や業務遂行にどの程度の影響があるかを定量化します。影響の度合いが業務に対し無視できる程度から、業務遂行に支障をきたす重大な影響がでる可能性があるものまでを考慮します。

（６）発生可能性

リスクの発生可能性は、HCF および RFC の保守要員の人数や、リモートサービスで利用する回線の種類により異なります。リモートメンテナンスに要する経過時間や、モニタ画面に接近できる保守要員の物理的な制限の有無、回線のサービス品質などを考慮して、リスクの発生可能性を定量化します。

８．１．２　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。

８．２　セキュリティ対策方針の決定(安全管理措置の例)

８．２．１　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「医療事業者ガイドライン」と「安全管理ガイドライン」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、およ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」）」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確認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。

８．２．２　リモートサービスの安全管理措置

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 21 年 10 月 9 日厚生労働省・経済産業省告示第 2 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。

（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。

③ 個人データの取扱状況を一覧できる手段の整備

④ 個人データの安全管理措置の評価、見直しおよび改善

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。

（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。
- 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、紙の覗き見や持ち出し、RSC 機器やディスクの持ち出しを防止すること。

② 盗難等の防止

- 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ち出しを防止すること。
- 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ち出しを牽制すること。
- 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。
- 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。
- 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ち出しを防止すること。

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ち出し、破壊によるサービス不能を防止すること。）
- 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ち出しを牽制、RSC ネットワーク機器経由の PHI の暴露を防止すること。
- 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。
- シールにより、タンパリング痕跡を検出すること。

（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、個人データおよ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 個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。
- 遠隔コンピュータシステムへの接続は、認証されること。

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。

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およ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、正規の利用者登録および登録削除の手続きがあること。パスワードの割当ては、正規の管理手続きによって統制すること。

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。

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および防止の管理策、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。

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およ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。
- 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およ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。
- 一連の合意された標準類，手順およ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。

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およ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。

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およ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。

（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 雇用契約時における従業者との非開示契約の締結、および委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結

- 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。
- 組織のセキュリティ基本方針および手順に違反した従業員に対する、正式な懲戒手続きを備えていること。

② 従業者に対する内部規程等の周知・教育・訓練の実施

- 組織の基本方針および基準について、組織のすべての従業員およ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。

８．３　セキュリティ対策

8.1および8.2節では、リモートサービスの運用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。

本節では、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。

８．３．１　RSC 機器における対策

RSC 機器における対策（例）を表 8-3-1 に示します。

表８－３－１　RSC 機器における対策（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

８．３．２　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 8-3-2 に示します。

表８－３－２　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

８．３．３　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 8-3-3 に示します。

表８－３－３　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

８．３．４　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 8-3-4 に示します。

表８－３－４　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

８．３．５　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 8-3-5 に示します。

表８－３－５　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９章　技術的・制度的変化への対応

本書は、2013 年 12 月時点でのセキュリティに関する技術状況および、関連省庁から提示されている法令等に適用しうるガイドラインとして作成されました。参照している法令等につきましては、「第 2 章　参照規格」に列挙しております。

個人情報の保護に関する要求事項については、社会情勢の変化や技術の進歩等によって変わり得るものです。それらの変化に応じて法制度についても改訂が行われる可能性があります。

本書は国際的なセキュリティ標準である ISO/IEC27001 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・制度的変化が大きい場合には、リスク分析の手法や適応する対策を見直す必要が生じると考えられます。このため、本書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。

附属書 A リスクアセスメントシートの使い方

付属書B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。表３に示すとおり、機密性、完全性、可用性の視点から脆弱性を数値化し、それぞれに該当する脅威が顕著化しリスクが発生した場合の影響度とこれが生じる発生可能性により評価しています。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,持ち出し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,持ち出し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,持ち出し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

※ リスク評価＝脆弱性（機密性・完全性・可用性）×影響性×発生可能性

附属書 B　ISMS 準拠リモートサービスリスクアセスメント表

情報セキュリティ管理基準				資産と脅威の対象範囲													
章	項	目的	コントロール	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
A.5.情報セキュリティ基本方針	A.5.1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方向性及び支持を、事業上の要求事項、関連する法令及び規則に従って規定するため。	・情報セキュリティ基本方針文書は、経営陣によって承認され、全従業員及び関連する外部関係者に公表し、通知すること。 ・情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当、及び有効であることを確実にするためにレビューすること。	—	—	—	—	—	—	—	—	—	—	—	—
A.6.情報セキュリティのための組織	A.6.1内部組織	組織内の情報セキュリティを管理するため	・経営陣は、情報セキュリティの責任のに関する明りょうな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持すること。 ・情報セキュリティ活動は、組織のなかの、関連する役割及び職務機能をもつさまざまな部署の代表が、調整すること。 ・すべての情報セキュリティ責任を、明確に定めること。 ・新しい情報処理設備に対する経営陣による認可プロセスを定め、実施すること。 ・情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに	—	—	—	—	—	—	—	—	—	—	—	—
	A.6.2外部組織	外部組織によってアクセス、処理、通信、又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。	・外部組織がかかわる業務プロセスからの、組織の情報及び情報処理施設に対するリスクを識別し、外部組織にアクセスを許可する前に適切な管理策を実施すること。 ・顧客が組織の情報又は資産にアクセスする前に、明確にしたすべてのセキュリティ要求事項に対処すること。	—	—	—	—	—	—	—	—	—	—	—	—
			・組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理に関わる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げること。	36	C1	m	—	（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できる。
								（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。
								（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きる。
				37	C1	n	—	（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できる。
								（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。
								（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きる。
A.7.資産の管理	A.7.1資産に対する責任	組織の資産の適切な保護を達成し、維持するため。	・すべての資産を明確に識別し、また、重要な資産すべての目録を作成し維持すること。 ・情報及び情報処理施設と関連する資産のすべてについて、組織のなかに、その保有者を指定すること。 ・情報及び情報処理施設に関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施すること	—	—	—	—	—	—	—	—	—	—	—	—
	A.7.2資産の分類	情報の適切なレベルでの保護を確実にするため。	・情報は、組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から分類すること。 ・情報に対するラベル付け及び取扱いに関する適切な一連の手順は、組織が採用した分類体系に従って【作成】策定し、実施すること。	—	—	—	—	—	—	—	—	—	—	—	—
A.8.人的資源のセキュリティ	A.8.1雇用前	従業員、契約相手及び第三者の利用者がその責任を理解し、求められている役割にふさわしいことを確実にするとともに、盗難、不正行為、又は施設の不正使用のリスクを低減するため。	・従業員、契約相手及び第三者の利用者の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に従って定義し、文書化すること。 ・従業員、契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は、関連のある法令、規則及び倫理に従って行うこと。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行われること。	—	—	—	—	—	—	—	—	—	—	—	—
			・従業員、契約相手及び第三者の利用者は、契約上の義務の一部として、情報セキュリティに関する、これらの者の責任及び組織の責任を記載した雇用契約書に同意し、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
								（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
							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。
			・経営陣は、組織の確立された方針及び手順に従ったセキュリティの適用を従業員、契約相手及び第三者の利用者に要求すること。	—	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A8.人的資源のセキュリティ	A8.2雇用期間中	従業員、契約相手及び第三者の利用者の、情報セキュリティの脅威及び諸問題、並びに責任及び義務に対する認識を確実なものとし、通常の業務の中で組織の情報セキュリティ基本方針を維持し、人による誤りのリスクを低減できるようにすること。	・組織のすべての従業員並びに、関係するならば、契約相手及び第三者の利用者は、職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け、また定めに従ってそれを更新すること。	19	A1	h	—	（脆弱性）誤入力l、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l、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。
	A8.3雇用の終了または変更	従業員、契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にすること。	・雇用の終了又は変更に関する責任は、明確に定義し、割り当てること。 ・すべての従業員、契約相手及び第三者の利用者は、雇用、契約又は合意の終了時に、自らが所有する組織の資産すべてを返却すること。 ・すべての従業員、契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正すること。	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。
			・セキュリティ違反を犯した従業員に対する正式な懲戒手続きを備えること	—	—	—	—	—	—	—	—	—	—	—	—
A.9.物理的及び環境的セキュリティ	A9.1セキュリティを保つべき領域	組織の施設及び情報に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	・情報及び情報処理施設を含む領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いること。	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C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。
			・セキュリティを保つべき領域は、認可されたもの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	m	—	（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。
				27	B1	n	—	（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						
				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。
								（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に繋がる						
				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。
				58	E1	e	—	（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						
			・火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し、適用すること。	—	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A.9.物理的及び環境的セキュリティ	A9.1セキュリティを保つべき領域	組織の施設及び情報に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	・オフィス、部屋、及び施設に対する物理的セキュリティを設計し、適用すること。 ・セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用すること。	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RSCネットワーク機器経由のPHIの暴露を防止できる。
				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(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)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牽制できる。
							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)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の暴露を防止できる。
				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に繋がる	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)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)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)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を牽制できる。
				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阻止して媒体の持出を牽制できる。
				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。
			・一般の人が立ち寄る場所(例えば、荷物などの受渡し場所)及び、敷地内の、許可されていない者が立ち入ることもある場所を管理し、また、可能ならば、認可されていないアクセスを避けるために、それらの場所を、情報処理施設から離すこと。	—	—	—	—	—	—	—	—	—	—	—
	A9.2装置のセキュリティ	資産の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。	・装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護すること。	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。
								(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。
			・装置は、支援ユーティリティの不具合による、停電、その他の故障から保護すること。 ・データを伝送する又は情報サービスを支援する通信ケーブル及び電源ケーブルの配線は、傍受又は損傷から保護すること。 ・装置は、可用性及び完全性を継続的に維持することを確実とするために、正しく保守すること。 ・構外にある装置に対しては、構外での作業に伴った、構内での作業とは違ったリスクを考慮に入れて、セキュリティを適用すること。	—	—	—	—	—	—	—	—	—	—	—
			・記憶媒体を内蔵した装置は、処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又は問題が起きないように上書きしていることを確実にするために、すべてを点検する	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。	—
	(A.11.1)その他の管理策	認可されていない利用者のアクセス、並びに情報及び情報処理施設の損傷又は盗難を防止するため。	(A.11.3.1～3) ・パスワードの選択及び利用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること。 ・利用者は、無人状態にある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。 ・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、並びに情報処理設備に対するクリアスクリーン方針を適用すること。	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できる。
			・装置、情報またはソフトウェアは、事前の認可なしでは、構外に持ち出さないこと。	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲											
章	項	目的	コントロール	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
A10.通信及び運用管理	A10.1運用の手順及び責任	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。	・操作手順は、文書化して維持していくこと。また、その手順は、必要とするすべての利用者に対して利用可能とすること。	—	—	—	—	—	—	—	—	—	—	—
			・情報処理設備及びシステムの変更は、管理すること。	—	—	—	—	—	—	—	—	—	—	—
				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。
				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。
				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。
				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	—							
			・職務及び責任範囲は、組織の資産に対する、認可されていない又は意図しない変更又は誤用の危険性を低減するために、分割すること。	—	—	—	—	—	—	—	—	—	—	—
			・開発施設、試験施設、及び運用施設は、運用システムへの認可されていないアクセス又は変更によるリスクを【軽減】低減するために、分離すること	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。
	A10.2第三者が提供するサービスの管理	第三者の提供するサービスに関する合意に沿った、情報セキュリティ及びサービスの適切なレベルを確保し、維持するため。	・第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義、及び提供サービスレベルが、第三者によって実施、運用及び維持されることを確実にすること。 ・第三者が提供するサービス、報告及び記録は、定期的に監視し、レビューすること。また、監査も定期的に実施すること。 ・関連する業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、サービス提供の変更（現行の情報セキュリティ方針、手順、及び管理策の保守・改善を含む）を管理すること。											
	A10.3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	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。 ・新しい情報システム及び改訂版・更新版の受入れ基準を確立し、開発中及びその受入れ前に適切なシステム試験を実施すること。	—	—	—	—	—	—	—	—	—	—	—
	A10.4悪意あるコード及びモバイルコードからの保護	ソフトウェア及び情報の完全性を保護するため。	・悪意のあるコードから保護するために、検出、予防及び回復のための管理策、並びに利用者に適切に意識させるための手順を実施すること。 ・モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うこと。また、認可されていないモバイルコードを実行できな	15	A1	e	—		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									
				44	D1	l								
				55	E1	e								
	A10.5バックアップ	情報及び情報処理【施設】設備の完全性及び可用性を維持するため。	・情報及びソフトウェアのバックアップは、合意されたバックアップ【の個別】方針に従って定期的に取得し、【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		—	（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に繋がる						
				27	B2	n								
				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に繋がる						
				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						
				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						

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A10.通信及び運用管理	A10.6ネットワークセキュリティ管理	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。	・ネットワークを脅威から保護するために、また、処理中の情報を含め、ネットワークを用いた業務用システム及び業務用ソフトウェアのセキュリティを維持するために、ネットワークを適切に管理し、制御すること。 ・組織が自ら提供するか外部委託しているかに関わらず、すべてのネットワークサービスについて、セキュリティ特性、サービスレベル及び管理上の要求事項を特定し、いかなるネットワークサービス合意書にもこれらを盛り込むこと。	21	B2	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	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						
								(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						
								(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						
				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						
				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						
	A10.7媒体の取扱い	資産の認可されていない開示、改ざん、除去、又は破壊、並びにビジネス活動の中断を防止するため。	・取り外し可能な媒体の管理のための手順は、備えること。	—	—	—	—	—	—	—	—	—	—	—
			媒体が不要になった場合は、正式な手順を【利用して】用いて、【安全、かつ、確実】セキュリティを保ち、かつ安全に処分すること。	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。
				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。
			・情報の取扱い及び保管についての手順は、その情報を認可されていない開示又は誤用から保護するために、確立すること。 ・システム文書は、認可されていないアクセスから保護すること。	—	—	—	—	—	—	—	—	—	—	—
	A10.8情報の交換	組織内部で交換した及び外部と交換した、情報及びソフトウェアのセキュリティを維持するため。	・あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えること。 ・組織と外部組織との間の情報及びソフトウェアの交換について、両者間での合意が成立すること。 ・情報を格納した媒体は、組織の物理的境界を越えた配送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。 ・電子的メッセージ通信に含まれた情報は、適切に保護すること。 ・業務用情報システムの相互接続と関連がある情報を保護するために、個別方針及び手順を策定し実施すること	—	—	—	—	—	—	—	—	—	—	—
	A10.9電子商取引サービス	電子商取引サービスのセキュリティ、及びそれらサービスのセキュリティを保った利用を確実にするため。	・公衆ネットワークを経由する電子商取引に含まれる情報は、不正行為、契約紛争、認可されていない開示及び改ざんから保護すること。 ・オンライン取引に含まれる情報は、不完全な通信、誤った通信経路設定、認可されていないメッセージの変更、認可されていない開示、認可されていない複製又は再生を未然に防止するために、保護すること。 ・認可されていない変更を防止するために、公開されているシステム上で利用可能な情報の完全性を保護すること。	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A.11.アクセス制御	A11.1アクセス制御に対する業務上の要求	情報へのアクセスを制御するため。	・アクセス制御方針は、アクセスについての業務上及びセキュリティ要求事項に基づいて確立し、文書化し、レビューすること。	—	—	—	—	—	—	—	—	—	—	—
	A11.2利用者のアクセス管理	情報システムへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	・すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えること。	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。	—
							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機器にはつながない）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	—
							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。	—
				21	B1	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機器にはつながない）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	—
							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機器にはつながない）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	—
							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。	—
				41	D1	p	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	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	—
							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の差換えが行われると、（脅威）ねつ造に繋がる	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。	—
				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	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の差換えが行われると、（脅威）ねつ造に繋がる	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。	—
			・特権の割当て及び利用は、制限し、管理すること。	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）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	（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	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。
							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の差換えが行われると、（脅威）ねつ造に繋がる	3→2	3	1	9→6	—	（管理策）権限管理（アクセス管理）は、「アクセス管理」と組合せで使われる管理策である。
							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）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。
							外部経路 RSC側当事	（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の差換えが行われると、（脅威）ねつ造に繋がる	3→2	3	1	9→6	—	（管理策）権限管理（アクセス管理）は、「アクセス管理」と組合せで使われる管理策である。
				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→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。
			・パスワードの割当ては、正式の管理【手続き】プロセスによって管理すること。 ・管理者は、正式のプロセスを使用して、利用者のアクセス権を定められた	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲													
章	項	目的	コントロール	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
A.11.アクセス制御	A11.3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	・パスワードの選択及び利用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること。	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	B1	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。
							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						
				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）HCF側ネットワーク機器の成りすましを防止できる。
				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に繋がる	3→2	3	1	9→6	—	
							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						
				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	（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	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。
							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。
			・利用者は、無人状態にある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。	—	—	—	—	—	—	—	—	—	—	—
	A11.4ネットワークのアクセス制御	ネットワークを利用したサービスへの認可されていないアクセスを防止するため。	・利用することを特別に認可したサービスへのアクセスだけを、利用者に提供すること。	—	—	—	—	—	—	—	—	—	—	—
			・特定の場所及び装置からの接続を認証するための手段として、自動の装置識別を考慮すること。	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）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	—
				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	—
								（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。	—
			・遠隔利用者のアクセスを管理するために、適切な認証方法を利用すること。	—	—	—	—	—	—	—	—	—	—	—
			・診断用及び環境設定用ポートへの物理的及び論理的なアクセスは、制御すること。	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）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	—
				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	—
			・情報サービス、利用者及び情報システムは、ネットワーク上、グループごとに分割すること。 ・共有ネットワーク、特に、組織の境界を越えて広がっているネットワークについて、アクセス制御方針及び業務用ソフトウェアの要求事項に沿って、利用者のネットワーク接続能力を制限すること(11.1参照)。 ・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、ルーティング制御の管理策をネットワークに対して実施すること。	—	—	—	—	—	—	—	—	—	—	—	—
	A11.5オペレーティングシステムのアクセス制御	オペレーティングシステムへの、認可されていないアクセスを防止するため。	・オペレーティングシステムへのアクセスは、セキュリティに配慮したログオン手順によって制御すること。 ・すべての利用者は、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、また、利用者が主張する同一性を検証するために、適切な認証技術を選択すること。 ・パスワードを管理するシステムは、対話式とすること、また、良質なパスワードを確実とするものであること。 ・システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理すること。 ・一定の使用中断	—	—	—	—	—	—	—	—	—	—	—
	A11.6業務用ソフトウェア及び情報のアクセス制御	業務用ソフトウェア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。	・利用者及び支援要員による情報及び業務用ソフトウェアシステム機能へのアクセスは、既定のアクセス制御方針に従って、制限すること。 ・取扱いに慎重を要するシステムは、専用の（隔離された）コンピュータ環境を持つこと。	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A.11.アクセス制御	(A.10.10)監視	認可されていない情報処理活動を検知するため。	・利用者の活動、例外処理、及び情報セキュリティ事象を記録した監査ログを取得すること、また、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、保持すること。 ・ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護すること。 ・システムの実務管理者及び運用担当者の作業は、記録すること。 ・障害のログを取得し、分析し、また、障害に対する適切な処置を講じること。	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。	—
				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)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。	—
							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。	—
			・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、及び監視活動の結果を定めに従ってレビューすること。	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。
				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盗用,差換えを抑制できる。
			・組織又はセキュリティ領域内の関連するすべての情報処理システム内のクロックは、合意された正確な時刻源と同期させること。	—	—	—	—	—	—	—	—	—	—	—
	A11.7モバイルコンピューティング及びテレワーキング	モバイルコンピューティング及びテレワーキング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。	・モバイルコンピューティング・通信設備を用いた場合のリスクから保護するために、正式の方針を備え、適切なセキュリティ対策を採用すること。 ・テレワーキングのための方針、運用計画及び手順を策定し、実施すること。	—	—	—	—	—	—	—	—	—	—	—
A.12.情報システムの取得、開発及び保守	A12.1セキュリティ要求事項の分析及び仕様化	セキュリティは情報システム【における必須の要素となっている】の欠くことのできない部分であることを確実にするため。	新しい情報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を記述した文書では、セキュリティの管理策についての要求事項を仕様化すること。	—	—	—	—	—	—	—	—	—	—	—
	A12.2業務用ソフトウェアでの正確な処理	業務用ソフトウェアにおける情報の誤り、消失、認可されていない変更又は誤用を防止するため。	・業務用ソフトウェアに入力するデータは、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。 ・処理の誤り又は故意の行為によって発生する情報の破壊を検出するために妥当性確認の機能を業務用ソフトウェアに組み込むこと。 ・業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し、また、適切な管理策を特定し実装すること。 ・業務用ソフトウェアからの出力データ【について】は、保存された情報の処理が正しく、かつ、状況に対して適切であることを確実にすること	—	—	—	—	—	—	—	—	—	—	—
	A12.3暗号による管理策	暗号手段によって、情報の機密性、真正性又は完全性を保護するため。	・情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施すること。	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									
				39	C1	b								
			・暗号技術の組織における利用を支援するために、かぎ管理を実施すること。	—	—	—	—	—	—	—	—	—	—	—
	A12.4システムファイルのセキュリティ	システムファイルのセキュリティを確実にするため。	・運用システムに関わるソフトウェアの導入を管理する手順を備えること。 ・試験データは、注意深く選択し、保護し、管理すること。 ・プログラムソースコードへのアクセスは、制限すること。	—	—	—	—	—	—	—	—	—	—	—
	A12.5開発及び支援プロセスにおけるセキュリティ	業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。	・変更の実施は、正式な変更管理手順の使用によって、管理すること。 ・オペレーティングシステムを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要な業務用ソフトウェアをレビューし、試験すること。 ・パッケージソフトウェアの変更は、抑止し、必要な変更だけに限ること。また、すべての変更は、厳重に管理すること。 ・情報の漏えいの可能性を抑止すること。 ・組織は、外部委託したソフトウェア開発を監督し、監視すること。	—	—	—	—	—	—	—	—	—	—	—
	A12.6技術的ぜい弱性管理	公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。	・利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。また、そのようなぜい弱性に組織がさらされている状況を評価し、それと関連するリスクに対処するために、適切な手段を講じること。	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準				資産と脅威の対象範囲												
章	項	目的	コントロール	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
A.13.情報セキュリティインシデントの管理	A13.1情報セキュリティの事象及び弱点の報告	情報システムに関連する情報セキュリティの事象及び弱点を、時機を失しない是正処置を講じることができるやり方で連絡することを確実に	・情報セキュリティ事象は、適切な管理者への連絡経路をとおして、できるだけ速やかに報告すること。 ・すべての従業員、契約相手並びに第三者の情報システム及びサービスの利用者に、システム又はサービスのなかで発見した又は疑いをもったセキュリティ弱点は、どのようなものでも記録し、また、報告するように要求すること。	—				—	—	—	—	—	—	—
	A13.2情報セキュリティインシデントの管理及びその改善	情報セキュリティインシデントの管理に、一貫性のある効果的な取組み方法を用いることを確実にするため。	・情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、責任体制及び手順を確立すること。 ・情報セキュリティインシデントの形態、規模及び費用を定量化し監視できるようにする仕組みを備えること。 ・情報セキュリティインシデント後の個人又は組織への事後処置が法的処置(民事又は刑事)に及ぶ場合には、関係する法域で定めている証拠に関する規則に従うために、証拠を収集、保全及び提出すること。					—	—	—	—	—	—	—
A.14.事業継続管理	A14.1事業継続管理における情報セキュリティの側面	情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、さらに、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。	・組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う、管理された手続を、策定し、維持すること。 ・業務プロセスの中断を引き起こしうる事象は、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに、特定す	—	—	—	—	—	—	—	—	—	—	—
			・重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施すること。	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						
			・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、情報セキュリティ上の要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持すること。 ・事業継続計画が最新で効果的なものであることを確実にするために、定めに従って試験・更新すること。	—	—	—	—	—	—	—	—	—	—	—
A.15.コンプライアンス	A15.1法的要求事項の順守	法令、規則又は契約上のあらゆる義務、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	・各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を、明確に定め、文書化し、また、最新に保つこと。 ・知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、法令、規則及び契約上の要求事項の順守を確実にするための適切な手順を導入すること。 ・重要な記録は、法令、規則、契約及び業務上の要求事項に従って、消失、破壊及び改ざんから保護すること。 ・個人データ及び個人情報の保護は、関連す	—	—	—	—	—	—	—	—	—	—	—
	A15.2セキュリティ方針及び標準の順守、並びに技術的コンプライアンス	組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。	・管理者は、セキュリティ方針及び標準類への順守を達成するために、自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすること。 ・情報システムを、セキュリティ実施標準の順守に関して、定めに従って点検すること。	—	—	—	—	—	—	—	—	—	—	—
	A15.3情報システム監査に対する考慮事項	情報システム監査手続の有効性を最大限にするため、及び情報システム監査手続への／からの干渉を最小限にするため。	・運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意されること。 ・情報システム監査ツールの誤用又は悪用を防止するために、それらのツールへのアクセスは、抑制すること。	—	—	—	—	—	—	—	—	—	—	—

付録 1：参考文献

＜医療機関のセキュリティに関するガイドライン等＞

財団法人医療情報システム開発センター・保健医療分野のプライバシマーク制度 参考資料集

http://privacy.medis.jp/book201110.html

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

http://privacy.medis.jp/

SPC 文書（英文版）

http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/

＜ISMS に関する参考資料＞

日本規格協会・JIS Q 27001:2006 情報セキュリティマネジメントガイド

IPA/ISEC・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

http://www.ipa.go.jp/security/fy12/contents/bookletB.pdf

経済産業省・情報セキュリティ監査基準（Ver.1.0）

http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf

経済産業省・情報セキュリティ監査研究会報告書

http://www.meti.go.jp/policy/netsecurity/downloadfiles/i30326bj.pdf

JIPDEC・ISMS 認証基準（Ver.2.0）

JIPDEC・ISMS 適合性評価性制度の概要（パンフレット）

http://www.isms.jipdec.jp/doc/v2ismspanf.pdf

JIPDEC・医療機関向け ISMS ユーザーズガイド

http://www.isms.jipdec.jp/doc/JIP-ISMS114-21.pdf

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

＜個人情報保護に関する資料＞
首相官邸・個人情報の保護に関する法律
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/index.html

旧通商産業省告示・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
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/

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

付録 2：作成者名簿

JAHIS/JIRA 合同リモートサービスセキュリティ作成 WG 委員名簿

作成者（五十音順）

岡田　康	東芝医療情報システムズ(株)	
大田　晃康	日本光電工業(株)	
下野　兼揮	(株)グッドマン	
西田　慎一郎	(株)島津製作所	◎JIRA 主査
野津　勤	(株)システム計画研究所	
葉賀　功	コニカミノルタ（株)	
平田　泰三	シーメンス・ジャパン(株)	
藤咲　喜丈	日本光電工業(株)	
松本　義和	サイバートラスト(株)	◎JAHIS 主査
茗原　秀幸	三菱電機(株)	

改定履歴		
日付	バージョン	内容
2006/06/01	V1.0	最初のバージョン
2009/09/01	V2.0	技術文書「リモートサービスセキュリティガイド」を統合し、全体として当該箇所をISO/IEC27001に沿った内容に修正した。
2014/01/31	V2.1	契約・合意事項およびリモートサービスの運用モデルを追加した。

（ＪＡＨＩＳ標準　１４－００３）
２０１４年　7月発行

リモートサービスセキュリティガイドラインＶｅｒ．２．１

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070