JAHIS

ＪＡＨＩＳ標準　１６－００３

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．３．０

２０１６年６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

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 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、2004 年度に JAHIS 標準「リモートサービスセキュリティガイド」(04-101)を、2006 年度に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」(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（04-101）とガイドライン（06-001）をガイドライン Ver.2.0（09-002）として統合しました。

今回の改定（Ver3.0）では引用規格である JIS Q 27001:2014(ISO/IEC 27001:2013)及び JIS Q 27002:2014(ISO/IEC 27002:2013)の改定に伴い、その反映を中心に、同じく引用している経済産業省ガイドライン(改定版)、JIPDEC の ISMS 最新ユーザガイドとあわせる等見直しを行いました。

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。

２０１６年６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

＜＜　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、本ガイドラインに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・運用についての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規約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。

目　　次

1. 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。

2. 引用規格・引用文献

(一財）日本規格協会・JIS Q 27001:2014(ISO/IEC 27001:2013）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

(一財）日本規格協会・JIS Q 27002:2014(ISO/IEC 27002:2013）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（平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号）
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf

(一財)日本情報経済社会推進協会情報マネジメント推進センター・ISMS ユーザーズガイド-JIS Q 27001:2014(ISO/IEC 27001:2013)対応　（お知らせと申し込み方法説明）
http://www.isms.jipdec.or.jp/JIP-ISMS111-30.html

3. 用語の定義

この文書では、以下の用語は以下の意味合いで使用している。

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。

4. 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, Electromedical and Healthcare IT Industry）
HCF	医療施設（Health Care Facility）
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（Japan Institute 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）

5. 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

個人情報の漏えい事故も世間の耳目を集め、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

「個人情報保護法」により、医療機関に対して患者個人情報である診療情報について、その保護についての義務が課せられています。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」に基づく監督を受け、ガイドラインを遵守するために必要な措置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。

「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、個人情報保護法上、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で特に留意すべき事項としては、

- **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**
  本書が参照するISMSでは”資産の移動には事前の許可が必要”とされており、情報も資産と見なされることから、SLAにおいてはデータ取得に関する手続きを合意しておくことが実用的です。
- **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**
- **緊急時、災害時における非常時対応の規定**

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。

6. 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。

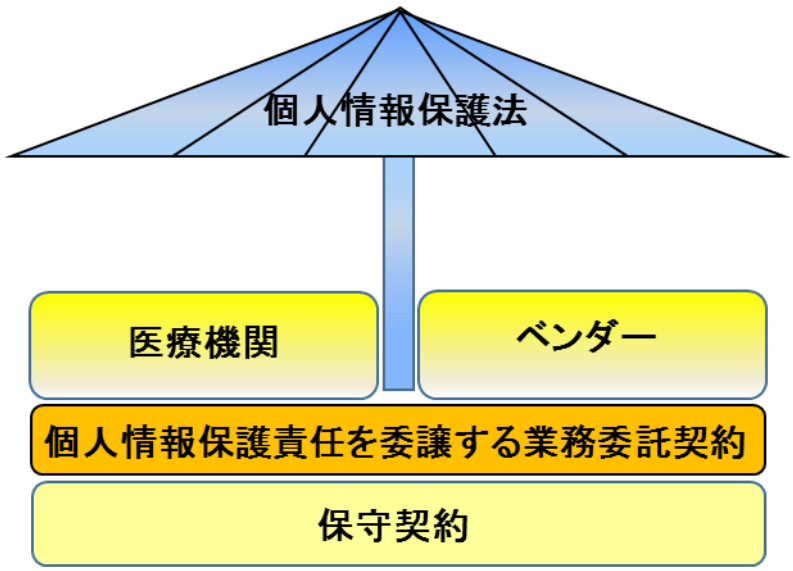

図６－１－１　日本のリモートサービスにおける個人情報保護の枠組み

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、情報セキュリティ方針（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。

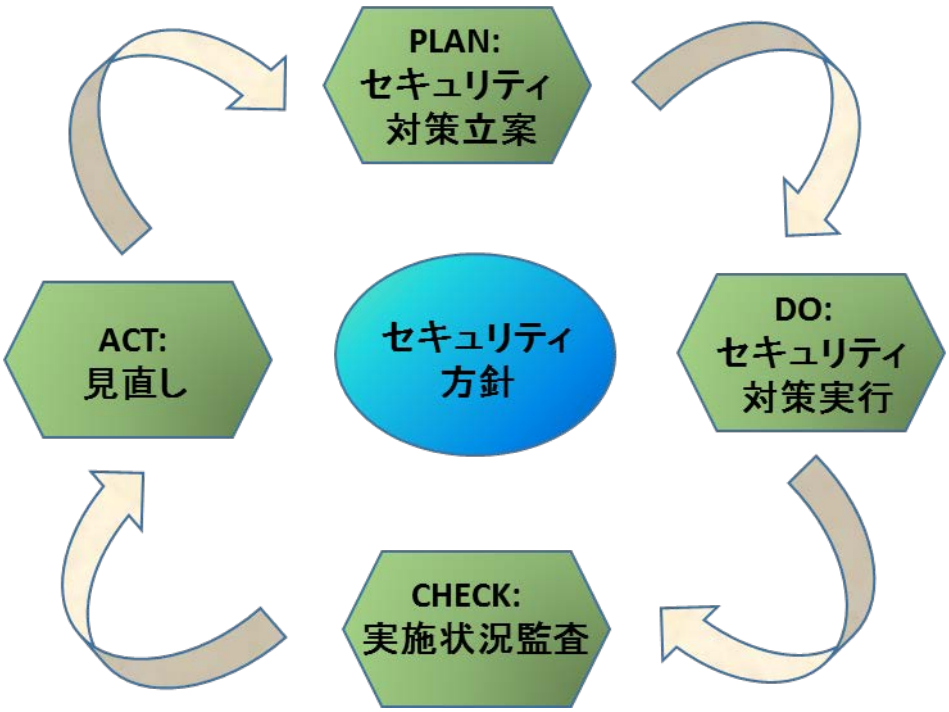

図６－１－２　情報セキュリティマネジメントシステム概念図

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方針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、情報セキュリティ方針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、情報セキュリティ方針の中には、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、情報セキュリティ方針および情報セキュリティ方針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。

- **情報セキュリティ方針**
- **リスク基準**
- **情報セキュリティ方針のマッピング**

- 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.情報セキュリティ方針

情報セキュリティ方針とは、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、情報セキュリティ方針は情報セキュリティに対する組織の意思を示し、方向付けをするものであり、組織の事業目的に沿っている必要があります。

リモートサービスの情報セキュリティ方針は組織全体の情報セキュリティ方針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。

情報セキュリティ方針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/IEC27001:2013 として発効しています。

情報セキュリティ方針を作成するにあたり、そのフォーマットを ISO/IEC27001:2013 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/IEC27001:2013 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 114 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.リスク基準

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方針に従い、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

「リスク基準」を策定する必要があります。リスク基準にはリスクを受容するかどうかの判断基準であるリスク受容基準と、リスクアセスメントを実施するための基準が含まれます。

リスク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
- アクセスポイントに対する Dos 攻撃

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.情報セキュリティ方針のマッピング

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。そこで必要なのは情報セキュリティ方針のマッピングです。

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、ベンダの情報セキュリティ方針を評価し、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、両組織の情報セキュリティ方針を比較し、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**

情報セキュリティ方針の項で述べたように、両者が ISO/IEC27001:2013 に基づいたセキュリティ方針の策定を行っていれば、両者の比較は容易です。114 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、マッピングを行った結果としてベンダ側の情報セキュリティ方針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情報セキュリティ方針を、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）バックアップ媒体

- 磁気テープ
- ハードディスク
- DVD
- Blu-ray

（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
- 秘密分散
- RAID

（5）経路上のデータの保護

- 公衆網（ISDN など）
- IP-VPN
- インターネット VPN

（6）不正アクセスの監視・防御

- IDS
- IPS

（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情報セキュリティ方針

ISO/IEC 27001:2013 を JIS 化した JIS Q 27001:2014 の「5.2 方針」には、情報セキュリティ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。

> **トップマネジメントは、次の事項を満たす情報セキュリティ方針を確立しなければならない。**
>
> **a) 組織の目的に対して適切である。**
>
> **b) 情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。**
>
> **c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。**
>
> **d) ISMS の継続的改善へのコミットメントを含む。**
>
> **（JIS Q 27001:2014　5.2 方針　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情報セキュリティ方針には、情報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附属書 A および B を参照して

ください。

附属書 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（JIS Q 27001:2014）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、14 の管理分野と、114 の管理策から構成されています。14 の管理分野は以下のとおりです。

①情報セキュリティのための方針群

情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制及び規制に従って規定

②情報セキュリティのための組織

組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを規定。モバイル機器の利用やテレワーキングに関しても規定

③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、雇用前、雇用期間中、雇用の終了及び変更時の雇用条件、意識向上、教育及び訓練、責任及び義務について規定

④資産の管理

資産を特定し保護する責任、情報の重要度に応じての分類、媒体の取扱いについて規定

⑤アクセス制御

アクセス制御方針、利用者アクセス管理、利用者の責任、アプリケーションのアクセス制御について規定

⑥暗号

機密性、真正性及び/又は完全性を保護するための暗号の適切かつ有効な利用について規定

⑦物理的及び環境的セキュリティ

物理的セキュリティ境界、入退室管理、装置の設置及び保護等について規定

⑧運用のセキュリティ

運用手順書の文書化及び管理、マルウェアからの保護、バックアップ、ログ取得及び監視、ソフトウェアの管理、技術的脆弱性の管理、監査について規定

⑨通信のセキュリティ

ネットワークのセキュリティ管理、情報の転送時のセキュリティについて規定

⑩システムの取得、開発及び保守

情報システムへのセキュリティ要求事項。開発及びサポートプロセスのセキュリティ、試験データについて規定

⑪供給者関係

供給者関係における情報セキュリティ、供給者のサービス提供の管理を規定

⑫情報セキュリティインシデント管理

情報セキュリティインシデント管理のための責任及び手順、報告、評価及び決定、対応、学習、証拠収集について規定

⑬事業継続マネジメントにおける情報セキュリティの側面

情報セキュリティ継続の計画。実施、レビューや、情報処理施設の冗長化を規定

⑭遵守

法的及び契約上の遵守事項、プライバシ保護、情報セキュリティのレビューについて規定

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

6.6.1.リスク対応とは

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

6.6.2.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 13-009「JAHIS ヘルスケア分野の監査証跡メッセージ規約 V2.0」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。

7. 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 7-1A)

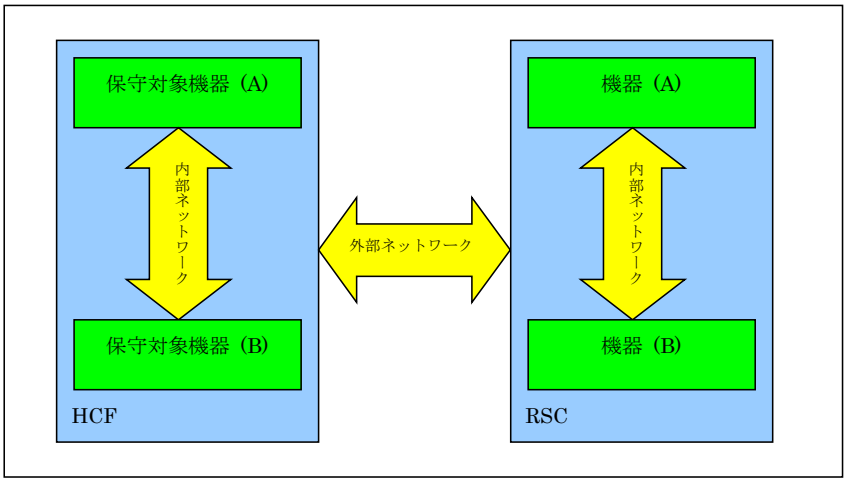

図７－１A　リモートサービスのシステムの想定

また外部のサービスを使用した接続形態であってもベンダの責任範囲内にありセキュリティが担保されていれば、その外部サービスは RSC 内部として見なします。（図 7-1B）

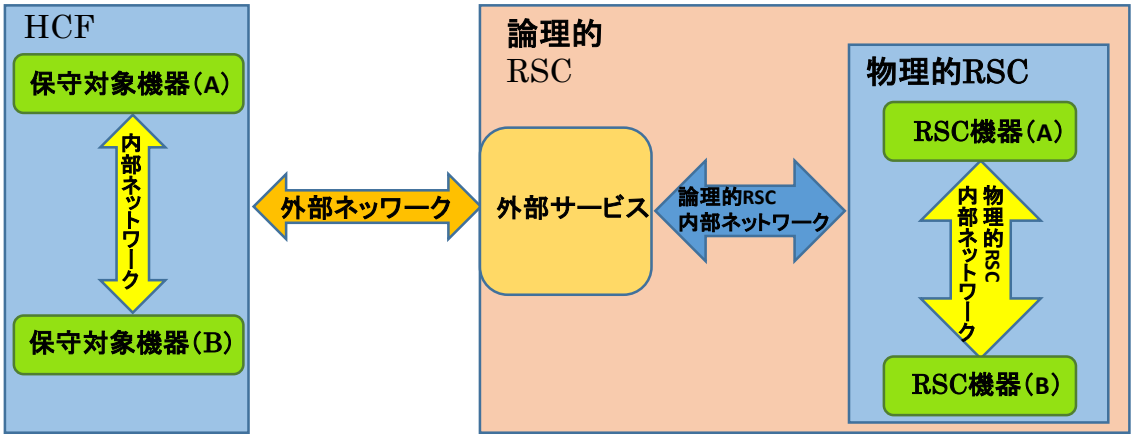

図７－１B　リモートサービスのシステムの想定（外部サービス使用の場合）

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。

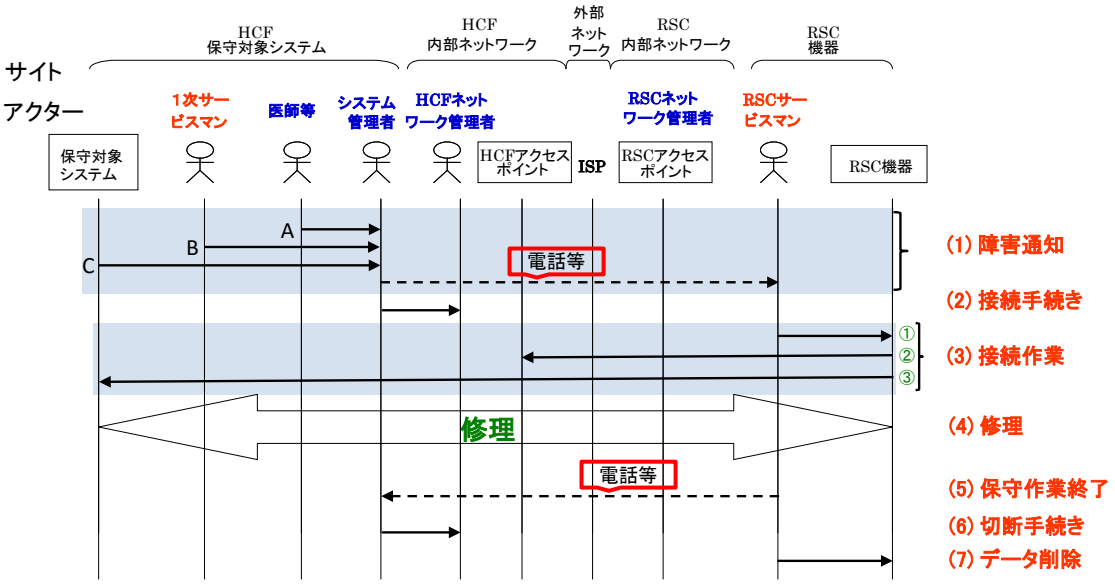

図７－１－１　故障時の対応のワークフロー

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。

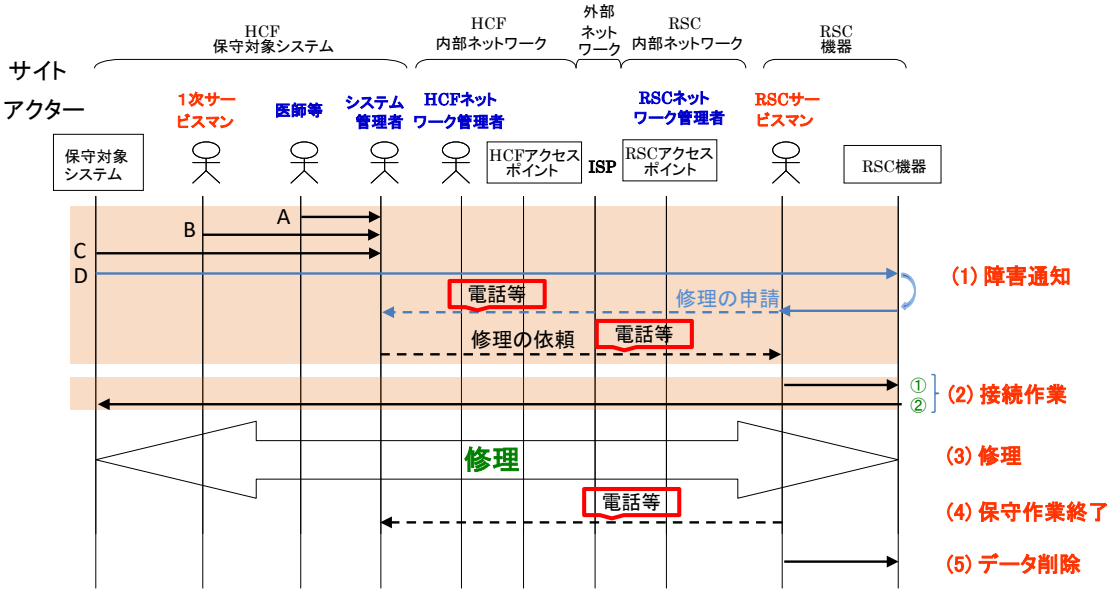

図７－１－２　常時接続における故障時の対応のワークフロー

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 AP 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。

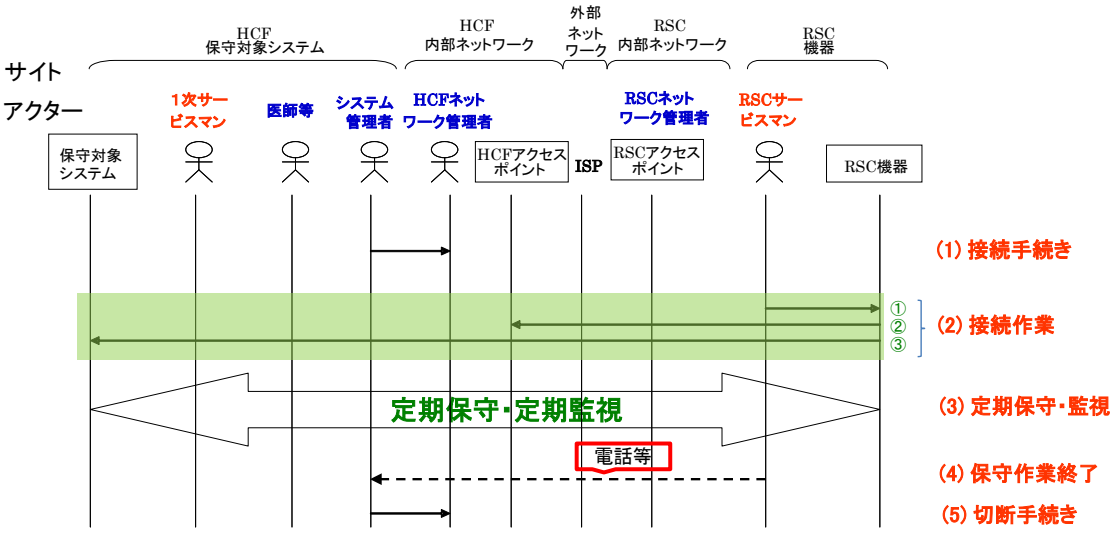

図７－２－１　定期保守・定期監視におけるワークフロー

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 が常時接続のケース）

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。

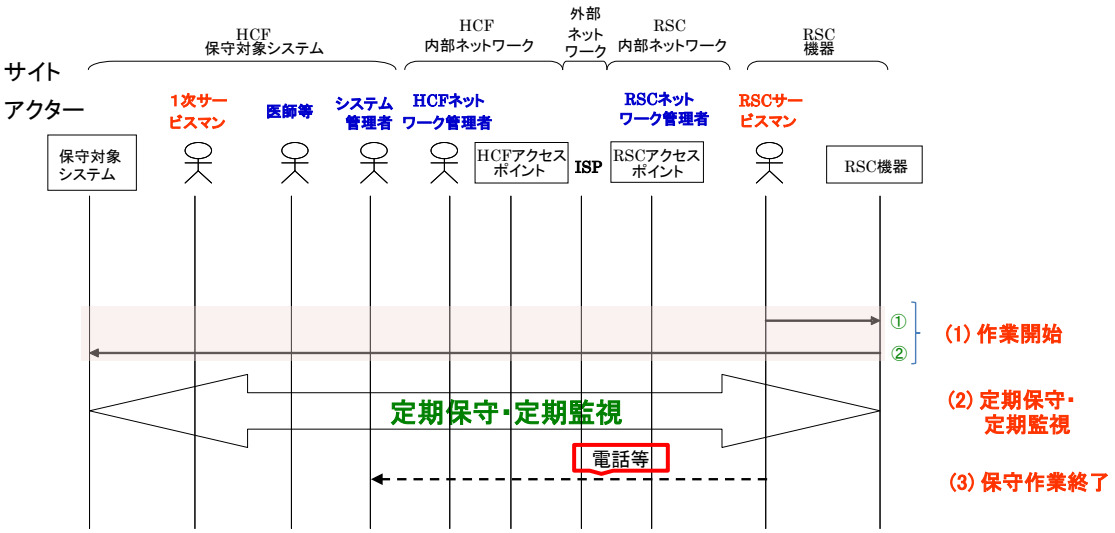

図７－２－２　定期保守・定期監視（常時接続）のワークフロー

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 AP 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。

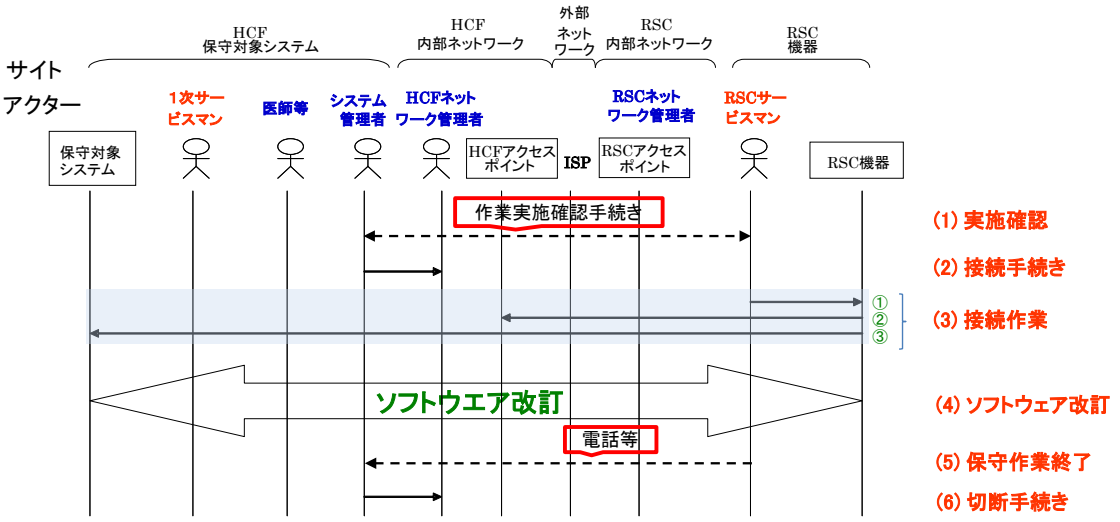

図７－３－１　ソフトウェアの改定のワークフロー

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 が常時接続のケース）

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。

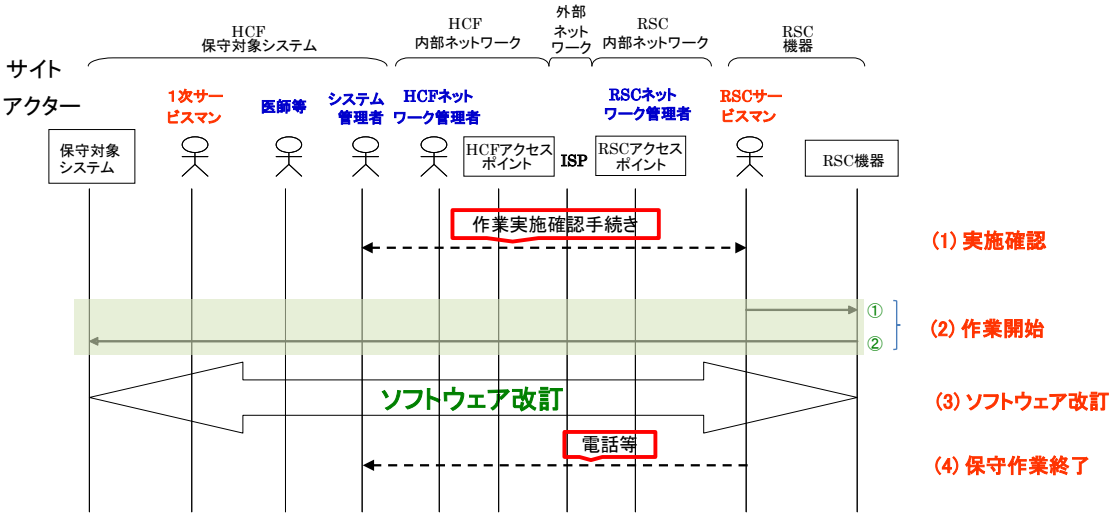

図７－３－２　ソフトウェアの改訂（常時接続）のワークフロー

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。

8. 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、その範囲外と情報の通信を行うときには、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対策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、リスク分析は HCF 毎に別途、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サイトになります。

- **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 外部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 外部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かか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在化した場合に、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をおよぼす可能性があるものまでを考慮します。

（6）発生可能性

リスクが発生する可能性は、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、リスクが発生する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、附属書 A、B 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情報には患者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かかわらず、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（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、「安全管理ガイドライン」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 26 年 12 月 12 日厚生労働省・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。

（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。

（3）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

- シュレッダ等の破砕機を用い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、第三者、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。

（4）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。**

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

9. 技術的・制度的変化への対応

本書は、2016 年 1 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表（附属書 B）の使い方

附属書 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 を扱うソフトウェア
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ェア
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

また、附属書 B ではリモートサービスにおける脅威分析を「表１」の A1～E1 に対し、以下のとおり示しております。

１．RSC 機器

（１）資産

・メモリ・ディスク・画面上の PHI

・メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

・メモリ・ディスク・画面上の PHI のバックアップ媒体

・PHI を扱うソフトウェア

・PHI を扱う機器

・PHI を扱う機器の環境設備

（電源・防災設備を指します。但し機器、ネットワーク機器は含みません。）

・PHI を扱う操作者

・暗号アルゴリズムと鍵と鍵配送方式（VPN 対策実施の場合）

（２）脅威

（A）メモリ・ディスク・画面上の PHI

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

（B）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

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

（C）メモリ・ディスク・画面上の PHI のバックアップ媒体

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

（D）PHI を扱うソフトウェア

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

（E）PHI を扱う機器

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

（F）PHI を扱う機器の環境設備

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

（G）PHI を扱う操作者

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

（H）暗号アルゴリズムと鍵と鍵配送方式

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

（3）脆弱性

（A）メモリ・ディスク・画面上の PHI

RSC 側当事者以外のオンサイトでの脆弱性

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

RSC 側当事者のオンサイトでの脆弱性

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

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

外部経路からの脆弱性

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

内部経路 (RSC ネットワーク管理者以外から) の脆弱性

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

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

内部経路 (RSC ネットワーク管理者から) の脆弱性

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

(B) メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

RSC 当事者以外のオンサイトでの脆弱性

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

RSC 側当事者のオンサイト

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

(C) メモリ・ディスク・画面上の PHI のバックアップ媒体

RSC 側当事者以外のオンサイトでの脆弱性

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

RSC 側当事者のオンサイトでの脆弱性

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

(D) PHI を扱うソフトウェア

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

(E) PHI を扱う機器

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

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

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

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

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

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

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

(F) PHI を扱う機器の環境設備

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

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

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

(G) PHI を扱う操作者

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

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

(H) 暗号アルゴリズムと鍵と鍵配送方式

(内部経路の VPN 対策をしている場合)

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

2．RSC 内部ネットワーク

(1) 資産

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

（2）脅威

（A）RSC 内部ネットワークの PHI

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

（B）通信トレースのメモやプリントアウトの紙

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

（C）通信トレースのバックアップ媒体

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

（D）ネットワーク機器のソフトウェア

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

（E）ネットワーク機器

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

（F）ネットワーク機器の環境整備

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

（G）ネットワーク機器の操作者

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

（H）暗号アルゴリズムと鍵と鍵配送方式

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

（3）脆弱性

（A）RSC 内部ネットワークの PHI

外部経路からの脆弱性

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

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

RSC ネットワーク管理者以外の内部経路からの脆弱性

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

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

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

RSC ネットワーク管理者の内部経路からの脆弱性

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

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

（B）通信トレースのメモやプリントアウトの紙

RSC 側当事者以外のオンサイトでの脆弱性

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

RSC 側当事者のオンサイトでの脆弱性

・(前提）監視または修理の都合で当該資産を残した時、(脆弱性）RSC ネット

ワーク管理者による持出 C が行われると、PHI の（脅威）暴露 C に繋がります。

（C）通信トレースのバックアップ媒体

RSC 側当事者以外のオンサイトでの脆弱性

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

RSC 側当事者のオンサイトでの脆弱性

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

（D）ネットワーク機器のソフトウェア

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

（E）ネットワーク機器

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

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

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

・（脆弱性）RSC 側ネットワーク機器やケーブルの漏洩電磁波が解析 C されると、PHI の（脅威）暴露 C に繋がります。

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

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

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

（F）ネットワーク機器の環境整備

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

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

・（脆弱性）RSC 側ネットワーク機器の環境設備が破壊 A されると、リモート

サービスの（脅威）サービス不能 A に繋がります。

（G）ネットワーク機器の操作者

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

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

（H）暗号アルゴリズムと鍵と鍵配送方式

（内部経路の VPN 対策をしている場合）

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

3．外部ネットワーク

（1）資産

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

（2）脅威

（A）外部ネットワーク上の PHI

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

（B）通信トレースのメモやプリントアウトの紙

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

（C）通信トレースのバックアップ媒体

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

（D）ネットワーク機器のソフトウェア

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

（E）ネットワーク機器

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

（F）ネットワーク機器の環境整備

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

（G）ネットワーク機器の操作者

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

（H）暗号アルゴリズムと鍵と鍵配送方式

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

（3）脆弱性

（A）外部ネットワーク上の PHI

前提（VPN 対策）により脅威は無視できるため省略します。

（B）上記通信トレースのメモやプリントアウトの紙

前提（VPN 対策）により脅威は無視できるため省略します。

（C）上記通信トレースのバックアップ媒体

前提（VPN 対策）により脅威は無視できるため省略します。

（D）ネットワーク機器のソフトウェア

前提（VPN 対策）により脅威は無視できるため省略します。

（E）ネットワーク機器

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

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

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

（F）ネットワーク機器の環境整備

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

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

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

(G) ネットワーク機器の操作者

前提 (VPN 対策) により脅威は無視できるため省略します。

(H) 暗号アルゴリズムと鍵と鍵配送方式

(内部経路の VPN 対策をしている場合)

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

4. HCF 内部ネットワーク

(1) 資産

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

(2) 脅威

(A) HCF 内部ネットワーク上の PHI

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

(B) 通信トレースのメモやプリントアウトの紙

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

(C) 通信トレースのバックアップ媒体

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

（D）ネットワーク機器のソフトウェア

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

（E）ネットワーク機器

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

（F）ネットワーク機器の環境整備

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

（G）ネットワーク機器の操作者

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

（3）脆弱性

（A）HCF 内部ネットワーク上の PHI

外部経路からの脆弱性

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

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

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

内部経路（HCF ネットワーク管理者以外から）の脆弱性

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

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

・(脆弱性) 内部経路からの HCF ネットワーク管理者以外の者による HCF 側

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

内部経路（HCF ネットワーク管理者から）の脆弱性

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

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

（B）上記通信トレースのメモやプリントアウトの紙

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

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

（C）上記通信トレースのバックアップ媒体

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

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

（D）ネットワーク機器のソフトウェア

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

（E）ネットワーク機器

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

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

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

・（脆弱性）HCF 側ネットワーク機器やケーブルの漏洩電磁波が解析 C されると、PHI の（脅威）暴露 C に繋がります。

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

・（脆弱性）HCF 側ネットワーク機器が被災 A すると、リモートサービスの（脅

威）サービス不能 A に繋がります。

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

（F）ネットワーク機器の環境整備

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

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

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

（G）ネットワーク機器の操作者

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

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

5．HCF 保守対象機器

（1）資産

・メモリ・ディスク・画面上の PHI

・メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙
（持ち込んだドキュメントや媒体は対象外）

・メモリ・ディスク・画面上の PHI のバックアップ媒体
（持ち込んだドキュメントや媒体は対象外）

・PHI を扱うソフトウェア

・PHI を扱う機器

・PHI を扱う機器の環境設備
（電源・防災設備を指します。但し機器、ネットワーク機器は含みません。）

・PHI を扱う操作者

・暗号アルゴリズムと鍵と鍵配送方式

（2）脅威

（A）メモリ・ディスク・画面上の PHI

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

（B）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

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

（C）メモリ・ディスク・画面上の PHI のバックアップ媒体

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

（D）PHI を扱うソフトウェア

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

（E）PHI を扱う機器

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

（F）PHI を扱う機器の環境設備

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

（G）PHI を扱う操作者

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

（3）脆弱性

（A）メモリ・ディスク・画面上の PHI

HCF 側当事者以外のオンサイトでの脆弱性

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

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

・（脆弱性）オンサイトでの第３者、HCF 職員、HCF ネットワーク管理者、他

社一次サービスマンによる画面の覗き見 C が行われると、保守対象機器内の PHI が盗用 C され（脅威）暴露 C に繋がります

HCF 側当事者のオンサイトでの脆弱性

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

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

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

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

外部経路（RSC 側当事者以外）からの脆弱性

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

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

外部経路（RSC 側当事者）からの脆弱性

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

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

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

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

内部経路の脆弱性

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

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

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

ねつ造 I に繋がります。

（B）メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙

医師等以外からの脆弱性

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

医師等からの脆弱性

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

（C）メモリ・ディスク・画面上の PHI のバックアップ媒体

医師等以外からの脆弱性

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

医師等からの脆弱性

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

（D）PHI を扱うソフトウェア

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

（E）PHI を扱う機器

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

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

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

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

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

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

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

（F）PHI を扱う機器の環境設備

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

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

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

(G) PHI を扱う操作者

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

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

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			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	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情報セキュリティのための方針群	A.5.1情報セキュリティのための経営陣の方向性	情報セキュリティのための経営陣の方向性及び指示を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。	A.5.1.1	情報セキュリティのための方針群	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員並びに関連する外部関係者に通知しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.5.1.2	情報セキュリティのための方針群のレビュー	情報セキュリティのための方針群は、あらかじめ定めた期間で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
A.6情報セキュリティのための組織	A.6.1内部組織	組織内で情報セキュリティの実施および運用に着手し、これを統制するための管理上の枠組みを確立するため。	A.6.1.1	情報セキュリティの役割及び責任	全ての情報セキュリティの責任を定め、割り当てなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.6.1.2	職務の分離	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離しなければならない。											
			A.6.1.3	関連当局との連絡	関係当局との適切な連絡体制を維持しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.6.1.4	専門組織との連絡	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組まなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.6.2モバイル機器およびテレワーキング	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。	A.6.2.1	モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.6.2.2	テレワーキング	テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.7人的資源のセキュリティ	A.7.1雇用前	従業員及び契約相手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ため。	A.7.1.1	選考	全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行われなければならない。また、この確認は、事業上の要求事項、アクセスあれる情報の分類及び認識されたリスクに応じて行わなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.7.1.2	雇用条件	従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。	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,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。
									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。
						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	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
						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。
	A.7.2雇用期間中	従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。	A.7.2.1	経営陣の責任	経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.7.2.2	情報セキュリティの意識向上、教育及び訓練	組織の全ての従業員、及び関係する場合には、契約相手は、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及び訓練を受けなければならず、また、定めに従ってその更新を受けなければならない。	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。
			A.7.2.3	懲戒手続	情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備えなければならない。	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。
	A.7.3雇用の終了及び変更	雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。	A.7.3.1	雇用の終了又は変更に関する責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び職務を定め、その従業員又は契約相手に伝達し、かつ、遂行させなければならない。	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。

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲												
章	項	目的	項番	条文	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.8資産の管理	A.8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	A.8.1.1	資産目録	情報及び情報処理施設に関する資産を特定しなければならない。また、これらの資産の目録を、作成し、維持しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.1.2	資産の管理責任	目録の中で維持される資産は、管理されなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.1.3	資産利用の許容範囲	情報の利用の許容範囲、並びに情報及び情報処理施設と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、実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.1.4	資産の返却	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
	A.8.2情報分類	組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。	A.8.2.1	情報の分類	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.2.2	情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.2.3	資産の取扱い	資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
	A.8.3媒体の取扱い	媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。	A.8.3.1	取外し可能な媒体の管理	組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.8.3.2	媒体の処分	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分しなければならない。	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。
			A.8.3.3	物理的媒体の輸送	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
A.9アクセス制御	A.9.1アクセス制御に対する業務上の要求事項	情報及び情報処理施設へのアクセスを制限するため。	A.9.1.1	アクセス制御方針	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.9.1.2	ネットワーク及びネットワークサービスへのアクセス	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
	A.9.2利用者アクセスの管理	システム及びサービスへの、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。	A.9.2.1	利用者登録及び登録削除	アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。	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。	—
			A.9.2.2	利用者アクセスの提供	全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者のアクセスの提供についての正式なプロセスを実施しなければならない。				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。	—
						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。	—
									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。	—
						41	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。	—
									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。	—
						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。	—
						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）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。	—
			A.9.2.3	特権的アクセス権の管理	特権的アクセス権の割当及び利用は、制限し、管理しなければならない。	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	（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）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。
						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）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。

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	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アクセス制御	A.9.2利用者アクセスの管理	システム及びサービスへの、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。	A.9.2.3	特権的アクセス権の管理	特権的アクセス権の割当及び利用は、制限し、管理しなければならない。				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	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。
			A.9.2.4	利用者の秘密認証情報の管理	秘密認証情報の割当ては、正式な管理プロセスによって管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.2.5	利用者アクセス権のレビュー	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.2.6	アクセス権の削除又は修正	全ての従業員及び外部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なければならず、また、変更に合わせて修正しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.9アクセス制御	A.9.3利用者の責任	利用者に対して、自ら秘密認証情報を保護する責任をもたせるため	A.9.3.1	秘密認証情報の利用	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求しなければならない。	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。
									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						
						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						
									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	—	（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						
						41	D1	p								
						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。
									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。
						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。
	A.9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	A.9.4.1	情報へのアクセス制限	情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.4.2	セキュリティに配慮したログオン手順	アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.4.3	パスワード管理システム	パスワード管理システムは、対話式でなければならず、また、良質なパスワードを確実とするものでなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.4.4	特権的なユーティリティプログラムの使用	システム及びアプリケーション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、厳しく管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.9.4.5	プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスは、制限しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.10暗号	A.10.1暗号による管理策	情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。	A.10.1.1	暗号による管理策の利用方針	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、実施しなければならない。	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								
			A.10.1.2	鍵管理	暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.11物理的及び環境的セキュリティ	A.11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理アクセス、損傷及び妨害を防止するため。	A.11.1.1	物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。	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。
			A.11.1.2	物理的入退管理策	セキュリティを保つべき領域は、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保護しなければならない。	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。
						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。
						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。

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	コントロール	脅威番号	サイト前提	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物理的及び環境的セキュリティ	A.11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理アクセス、損傷及び妨害を防止するため。	A11.1.2	物理的入退管理策	セキュリティを保つべき領域は、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保護しなければならない。	26	B1 B2	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 B2	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。
										（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。
						47	D1	n	—	（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	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						
A.11物理的及び環境的セキュリティ	A.11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理アクセス、損傷及び妨害を防止するため。	A.11.1.3	オフィス、部屋及び施設のセキュリティ	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、適用しなければならない。	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。
						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。
										（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1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。
						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1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。
			A.11.1.4	外部及び環境の脅威からの保護	自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.1.5	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する手順を設計し、適用しなければならない。	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。

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	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物理的及び環境的セキュリティ	A.11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理アクセス、損傷及び妨害を防止するため。	A.11.1.5	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する手順を設計し、適用しなければならない。				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。
						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。
			A.11.1.6	受渡場所	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理しなければならない。また、可能な場合には、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さなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.11物理的及び環境的セキュリティ	A.11.2装置	資産の損失、損傷、盗聴又は劣化、及び組織の業務に対する妨害を防止するため。	A.11.2.1	装置の設置及び保護	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し、保護しなければならない。											
						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。
										（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。
						25	B1	m	—	（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。
										（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。
						45	D1	m	—	（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。
										（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。
						56	E1	f	—	（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。
			A.11.2.2	サポートユーティリティ	装置は、サポート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しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.3	ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.4	装置の保守	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にするために、正しく保守しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.5	資産の移動	装置、情報又はソフトウェアは、事前の許可なしでは、構外に持ち出してはならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.6	構外にある装置及び資産のセキュリティ	構外にある資産に対しては、構外での作業に伴った、構外での作業とは異なるリスクを考慮に入れて、セキュリティを適用しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.7	装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての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、又はセキュリティを保って上書きしていることを確実にするために、検証しなければならない。	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.11.2.8	無人状態にある利用者の装置	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しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.11.2.9	クリアデスク・クリアスクリーンの方針	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しなければならない。	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。

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲												
章	項	目的	項番	条文	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.12運用のセキュリティ	A.12.1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。	A.12.1.1	操作手順書	操作手順書は、文書化し、必要とする全ての利用者に対して利用可能にしなければな	—	—	—	—	—	—	—	—	—	—	—
			A.12.1.2	変更管理	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理しなければならない。	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	—							
			A.12.1.3	容量・能力の管理	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・調整しなければならず、また、将来必要とする容量・能力を予測しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.12.1.4	開発環境、試験環境及び運用環境の分離	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセスまたは変更によるリスクを低減するために、分離しなければならない。	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。
	A.12.2マルウェアからの保護	情報及び情報処理施設がマルウェアから保護されていることを確実にするため。	A.12.2.1	マルウェアに対する管理策	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施しなければならない。	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）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	l								
						44	D1	l								
						55	E1	e								
	A.12.3バックアップ	データの消失から保護するため。	A.12.3.1	情報のバックアップ	情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に実施し、検査しなければならない。	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、ケーブルが不適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									
						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、ケーブルが不適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						
	A.12.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	A.12.4.1	イベントログ取得	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューしなければならない。	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」と組合せて使われる管理策である。	—
			A.12.4.2	ログ情報の保護	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しなければならない。	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						
			A.12.4.3	実務管理者及び運用担当者の作業ログ	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューしなければならない。	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」と組合せて使われる管理策である。	—
									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）記録（イベントの要求者・種類・日時等）は、「内部監査」と組合せて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1が行われると、（脅威）暴露C,ねつ造に繋がる	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」と組合せて使われる管理策である。	—
			A.12.4.4	クロックの同期	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.12.5運用ソフトウェアの管理	運用システムの完全性を確実にするため。	A.12.5.1	運用システムに関わるソフトウェアの導入	運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.12.6技術的ぜい弱性の管理	技術的ぜい弱性の悪用を防止するため。	A.12.6.1	技術的ぜい弱性の管理	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しなければならない。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なければならない。さらに、それらと関連するリスクに対処するために、適切な手段をとらなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.12.6.2	ソフトウェアのインストールの制限	利用者によるソフトウェアのインストールを管理する規則を確立し、実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.12.7情報システムの監査に対する考慮事項	運用システムに対する監査活動の影響を最小限にするため。	A.12.7.1	情報システムの監査に対する管理策	運用システムの検証を伴う監視要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.13通信のセキュリティ	A.13.1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情報処理施設の保護を確実にするため。	A.13.1.1	ネットワーク管理策	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御しなければならない。	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、遠隔診断ポートの保護がある。	—
						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）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。	—
										（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。	—

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	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通信のセキュリティ	A.13.1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情報処理施設の保護を確実にするため。	A.13.1.2	ネットワークサービスのセキュリティ	組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定しなければならず、また、ネットワークサービス合意書にもこれらを盛り込まなければならない。				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						
						21	B2	i		（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						
						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による持出Cが行われると、PHIの（脅威）暴露Cに繋がる						
						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						
						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に繋がる						
			A.13.1.3	ネットワークの分離	情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離しなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.13.2情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	A.13.2.1	情報転送の方針及び手順	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備えなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.13.2.2	情報転送に関する合意	合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱わなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.13.2.3	電子的メッセージ通信	電子的メッセージ通信に含まれた情報は、適切に保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.13.2.4	秘密保持契約又は守秘義務契約	情報保護に対する組織の要件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、定めに従ってレビュー し、文書化しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.14システムの取得、開発及び保守	A.14.1情報システムのセキュリティ要求事項	ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。	A.14.1.1	情報セキュリティ要求事項の分析及び仕様化	情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項を含めなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.1.3	アプリケーションサービスのトランザクションの保護	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護しなければならない。 ― 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 ― 認可されていないメッセージの複製又は再生	—	—	—	—	—	—	—	—	—	—	—
	A.14.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	A.14.2.1	セキュリティに配慮した開発のための方針	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.2	システムの変更管理手順	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	オペレーティングプラットフォー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、重要なアプリケーションをレビュー し、試験しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.4	パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は、抑止しなければならず、必要な変更だけに限らなければならない。また、全ての変更は、厳重に管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.5	セキュリティに配慮したシステム構築の原則	セキュリティに配慮したシステムを構成するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.6	セキュリティに配慮した開発環境	組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.14.2.7	外部委託による開発	組織は、外部委託したシステム開発活動を監視し、監視しなければならない。	—	—	—	—	—	—	—	—	—	—	—

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲											
章	項	目的	項番	条文	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.14.2.8	システムセキュリティの試験	セキュリティ機能(functionality)の試験は、開発期間中に実施しなければならない。											
			A.14.2.9	システムの受入れ試験	新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
	A.14.3試験データ	試験に用いるデータの保護を確実にするため。	A.14.3.1	試験データの保護	試験データは、注意深く選定し、保護し、管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
A.15供給者関係	A.15.1供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため。	A.15.1.1	供給者関係のための情報セキュリティの方針	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要件事項について、供給者と合意し、文書化しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.15.1.2	供給者との合意におけるセキュリティの取扱い	関連する全ての情報セキュリティ要求事項を確立しなければならず、また、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意しなければならない。				—	（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。
						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きる。
										（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、ケーブルが不適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。
						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きる。
			A.15.1.3	ICTサプライチェーン	供給者との合意には、情報通信技術(ICT)サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
	A.15.2供給者のサービス提供の管理	供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。	A.15.2.1	供給者のサービス提供の監視及びレビュー	組織は、供給者のサービス提供を定常的に監視し、レビューし、監視しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.15.2.2	供給者のサービス提供の変更に対する管理	関連する業務情報、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、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
A.16情報セキュリティインシデント管理	A.16.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取り組みを確実にするため。	A.16.1.1	責任及び手順	情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.2	情報セキュリティ事象の報告	情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.3	情報セキュリティ弱点の報告	組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.4	情報セキュリティ事象の評価及び決定	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.5	情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.6	情報セキュリティインシデントからの学習	情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.16.1.7	証拠の収集	組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
A.17事業継続マネジメントにおける情報セキュリティの側面	A.17.1情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない。	A.17.1.1	情報セキュリティ継続の計画	組織は、困難な状況(adverse situation)（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。	—	—	—	—	—	—	—	—	—	—	—	—
			A.17.1.2	情報セキュリティ継続の実施	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し維持しなければならない。	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						

情報セキュリティ管理基準			ISO/IEC 27001:2013（JIS Q 27001:2014）			資産と脅威の対象範囲										
章	項	目的	項番	条文	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.17事業継続マネジメントにおける情報セキュリティの側面	A.17.1情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない。	A.17.1.2	情報セキュリティ継続の実施	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し維持しなければならない。	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						
			A.17.1.3	情報セキュリティ継続の検証、レビュー及び評価	確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証しなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.17.2冗長性	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするため、プロセス、手順及び管理策を確立し、文書化し、実施し、維持しなければ	A.17.2.1	情報処理施設の可用性	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。	—	—	—	—	—	—	—	—	—	—	—
A.18順守	A.18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、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。	A.18.1.1	適用法令及び契約上の要求事項の特定	各情報システム及び組織について、全ての関連する法令、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を、明確に特定し、文書化し、また、最新に保たなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.1.2	知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規則及び契約上の要求事項の遵守を確実にするための適切な手順を実施しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.1.3	記録の保護	記録は、法令、規則、契約及び事業場の要求事項に従って、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.1.4	プライバシー及び個人を特定できる情報（PII）の保護	プライバシー及びPIIの保護は、関連する法令及び規則が適用される場合には、その要求に従って確実にしなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.1.5	暗号化機能に関する規制	暗号化機能は、関連する全ての協定、法令及び規則を遵守して用いなければならない。	—	—	—	—	—	—	—	—	—	—	—
	A.18.2情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され、運用されていることを確実にするため。	A.18.2.1	情報セキュリティの独立したレビュー	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.2.2	情報セキュリティのための方針群及び標準の順守	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—
			A.18.2.3	技術的順守のレビュー	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューしなければならない。	—	—	—	—	—	—	—	—	—	—	—

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＞
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 参考図書
http://privacy.medis.jp/book201110.html

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・情報セキュリティ管理基準（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）

大田 晃康	日本光電工業(株)
梶山 孝治	(株)日立製作所
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	シーメンスヘルスケア(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
2006/6	Ver. 1.0	初版
2009/12	Ver. 2.0	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。
2014/7	Ver. 2.1	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。
2016/6	Ver. 3.0	引用規格である JIS Q 27001:2014(ISO/IEC27001:2013)、JIS Q 27002:2014(ISO/IEC 27002:2013)、経済産業省ガイドライン（改定版)、JIPDEC の ISMS 最新ユーザガイドの改定に伴う見直しを行った。

（ＪＡＨＩＳ標準　１６－００３）
２０１６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Ｖｅｒ．３．０

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