2026年度 JIRA-JAHIS合同報告会
― 医療機器におけるサイバーセキュリティ対策 ―

「リモートサービスセキュリティ ガイドライン（RSS-GL）の紹介」



一般社団法人 日本画像医療システム工業会（JIRA)
医用画像システム部会　セキュリティ委員会　RSS-WG主査　西田慎一郎

本日ご理解いただきたいこと

- リモートサービスは、医療機器の保守性や現場の利便性を高める一方、医療機関のネットワークや患者情報にアクセスする可能性があるため、設計段階から運用・終了時まで一貫したセキュリティ管理が必要です。
  - 昨今のサイバー攻撃では、リモートサービスのアクセスポイントから侵入されるケースが多く見られ、ネットワーク機器のセキュリティ管理は必須。ただ、それだけでなく製品、ネットワーク、認証、運用、保守員、委託先等を含めて管理が必要
  - また、利便性と安全性のバランスを、リスクに応じて決定することも重要

- そのためには、国際標準となっている情報セキュリティ管理システム（ISMS）の利用が効果的です。

リモートサービスセキュリティガイドライン（RSS-GL）は、
　リモートサービスのモデル化を行い、そのモデルに対して
　ISMS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。
その実施例に倣うことにより、情報資産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。

RSS-GL 概要

- 規格名
  - リモートサービスセキュリティガイドライン（Guideline for the Security of Remote Servicing）
    - 日本画像医療システム工業会規格(JESRA)　TR-0034*E
    - JAHIS標準　25-003
- 目的
  - 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すことで、医療機関の管理者、及び遠隔保守を行うベンダが、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ることです。
  - リモートサービス事業者がISMSを構築する際に、本書のリスクマネジメントの実施例を参考にして実施いただくことを想定しています。
- 適用範囲
  - 本ガイドラインは医療分野のリモートサービスに関するセキュリティのガイドラインを示します。
- 入手方法
  - JIRA及びJAHISのホームページより無償で入手可能です。入手資格はありません。
- メンテナンス
  - JIRA及びJAHISの両工業会のセキュリティ委員会が合同でWGを設立し、必要に応じて改訂、補足文書等の作成、セミナーなどの普及活動等を行っています。

RSS-GL 改訂履歴

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・合意事項及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 ユーザーズガイドの改定に伴う見直しを行った。
2022/10	Ver. 3.1a	参照しているガイドライン等の改定や廃止に伴い、当該箇所の修正を行い、最新の安全管理ガイドラインの内容に沿うよう見直しを行った。
2024/11	Ver. 4.0	引用規格である JIS Q 27001:2023(ISO/IEC27001:2022)、JIS Q 27002:2024(ISO/IEC 27002:2022)、最新の安全管理ガイドラインの内容に沿うよう見直しを行った。
2025/4	Ver.5.0	参照している経済産業省および総務省の「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」が改定されたことに伴い、当該箇所の修正を行った。

厚労省・安全管理GLの記載

- 医療情報システムの安全管理に関するガイドライン第7.0版　システム運用編
  10.2 リモートメンテナンスにおける安全管理対策
    表10-1 リモートメンテナンスにおいて実施すべき事項
      「人的・運用関連のリスク」の注釈として以下の記載あり。

医療機関等は、事業者がリモートメンテナンスをする場合には、適時、実施状況を確認することが求められる。
事業者が行うリモートメンテナンスについては、「リモートサービス セキュリティガイドライン」が一般社団法人保健医療福祉情報システム工業会(JAHIS)より示されているので、上記の確認において参考となる。
なお、同ガイドラインは適宜改定しているため、最新の版を参照することが求められる。

RSS-GLの内容紹介

RSS-GL 目次

1. 適応範囲
2. 引用規格・引用文献
3. 用語の定義
4. 記号および略語

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
    - 5.2 法的適合性
    - 5.3 契約・合意事項
    - 5.4 リモートサービスのライフサイクルにおける義務と責務
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
    - 6.2 リモートサービスにおける情報セキュリティ方針
    - 6.3 標準的事例におけるリスクの評価
    - 6.4 標準的事例における管理すべきリスク
    - 6.5 本ガイドラインに記載のないリスクの識別
    - 6.6 リスク対応
    - 6.7 セキュリティ監査と外部監査の推奨
7. 運用モデル
    - 7.1 運用モデル
    - 7.2 故障時の対応
    - 7.3 定期保守・定期監視
    - 7. 4ソフトウェアの改訂
8. リスク分析とセキュリティ対策
    - 8.1 リスク分析
    - 8.2 セキュリティ対策方針の決定(安全管理措置の例)
    - 8.3 セキュリティ対策
9. 技術的・制度的変化への対応

附属書 A リスクアセスメントシートの使い方
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

付録1　参考文献
付録2　作成者名簿

6. リモートサービスへのISMSの適用

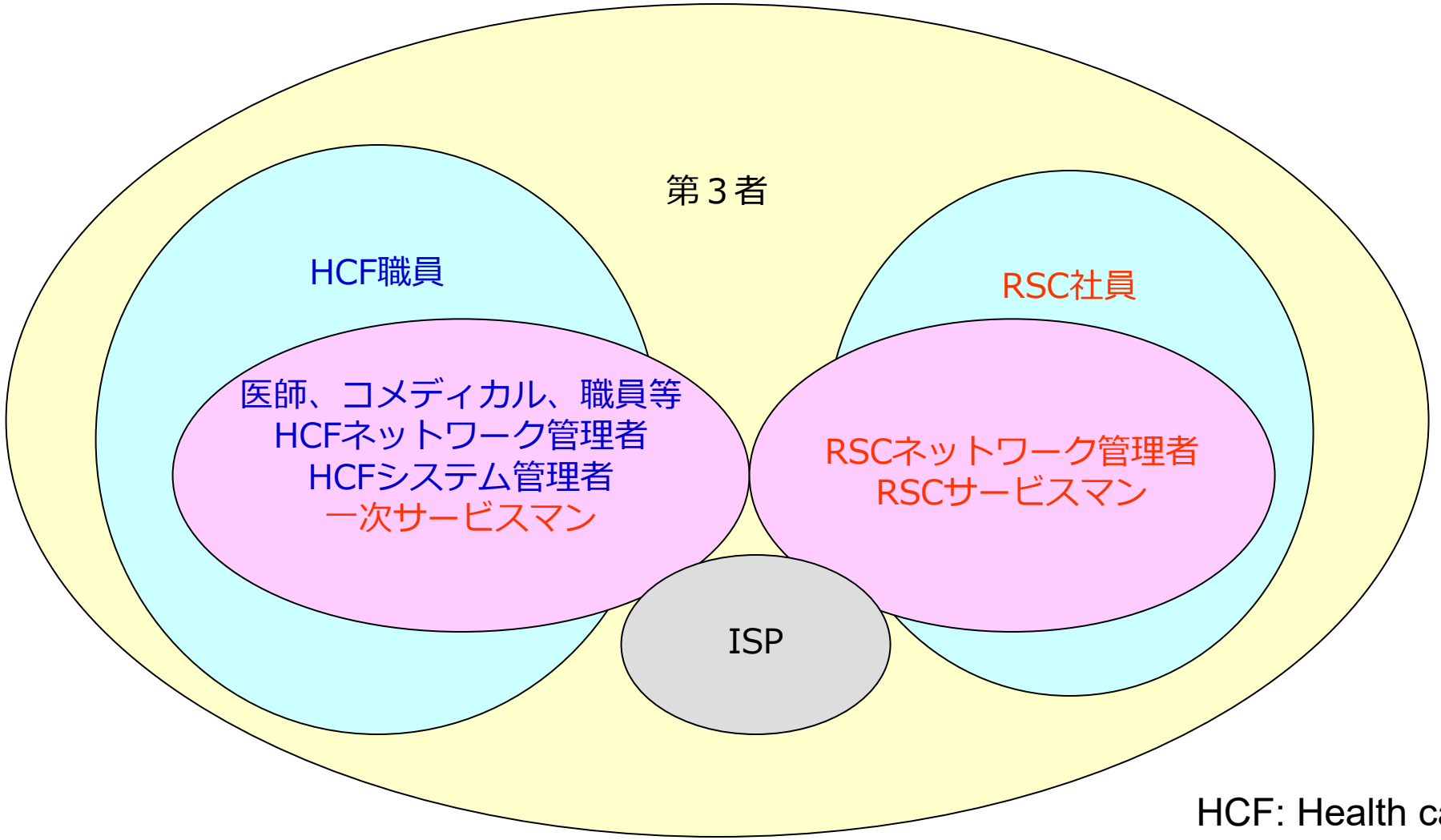
- リモートサービスのセキュリティ対策を構築するに当たり、RSS-WGでは以下のような考え方で整理を行った。

1. エンティティ（構成員要素）の関係整理
2. サイトの区分整理
3. ユースケースと業務フローの確定
4. 資産と脅威の洗い出し
5. リスク評価基準の設定
6. リスク評価

- 更に、国際標準や行政からのガイドライン等を参照し、発生可能性のあるリスクに対する対策案を提示している。

- **JIS Q 27001:2023(ISO/IEC 27001:2022)**
  情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項
- **JIS Q 27002:2024(ISO/IEC 27002:2022)**
  情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策
- 【個人情報保護委員会・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ダンス
- 【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 6.0版**
- 【個人情報保護委員会】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

RSS-GL エンティティ



HCF: Health care facility
RSC: Remote service center
ISP: Internet service provider

RSS-GL　サイト

医療機関、リモートサービス提供社を以下の5サイトに区分している

■RSC（Remote Service Center）
（1）RSC機器：
RSC運用管理責任者／RSCサービスマン
（2）RSC内部ネットワーク：
RSC運用管理責任者／RSCネットワーク管理者

■外部ネットワーク
（3）外部ネットワーク
外部ネットワーク提供事業者

■HCF（Health Care Facility）
（4）HCF内部ネットワーク：
HCF運用管理責任者／HCFネットワーク管理者、HCFシステム管理者
（5）HCF保守対象機器：
HCF運用管理責任者／HCFシステム管理者

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、3つのユースケースで整理を行った。

（1）故障時の対応（修理）

- 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

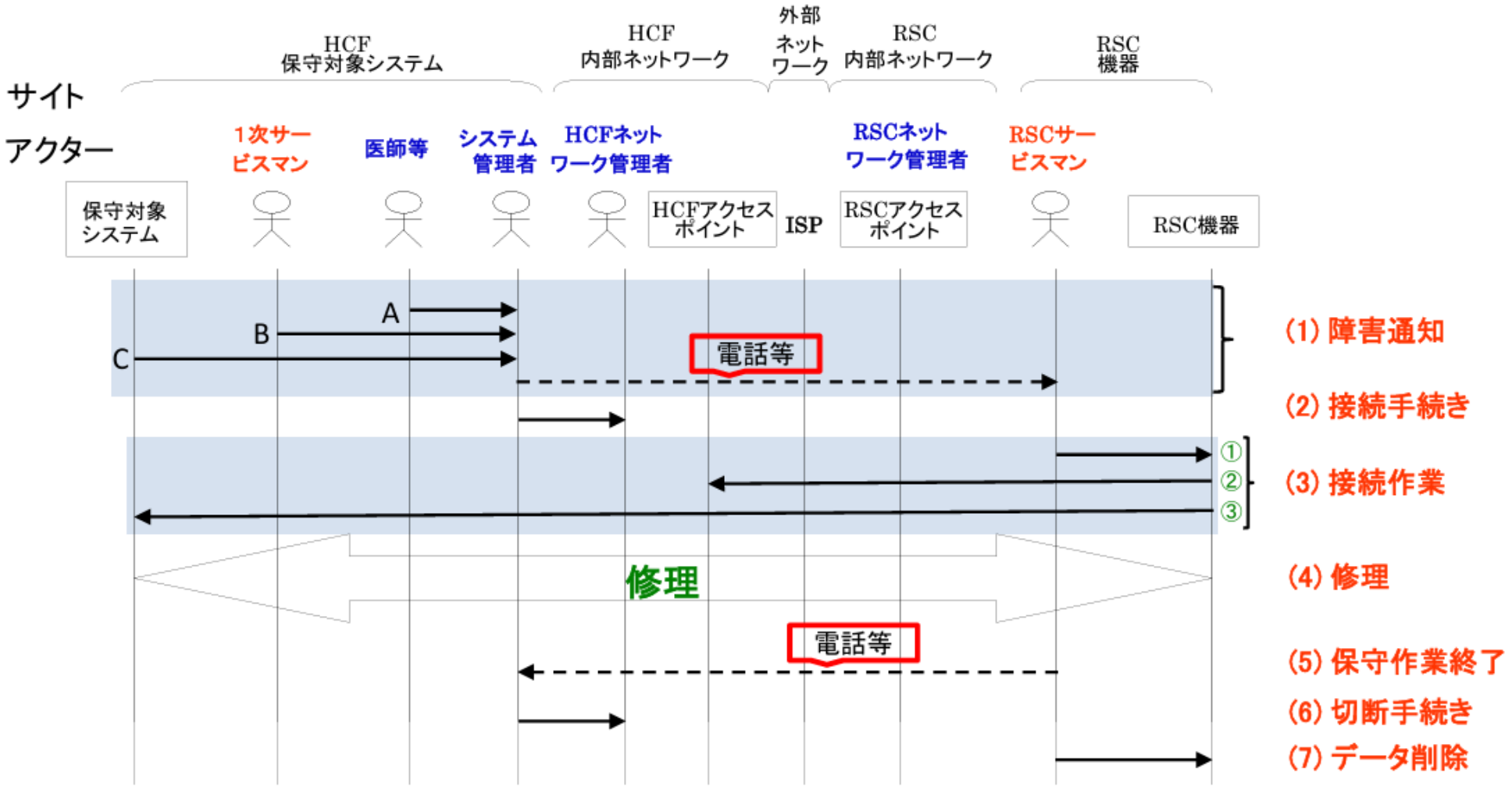
（2）定期保守・定期監視

- 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、対象機器の監視及び保守作業を行うもの

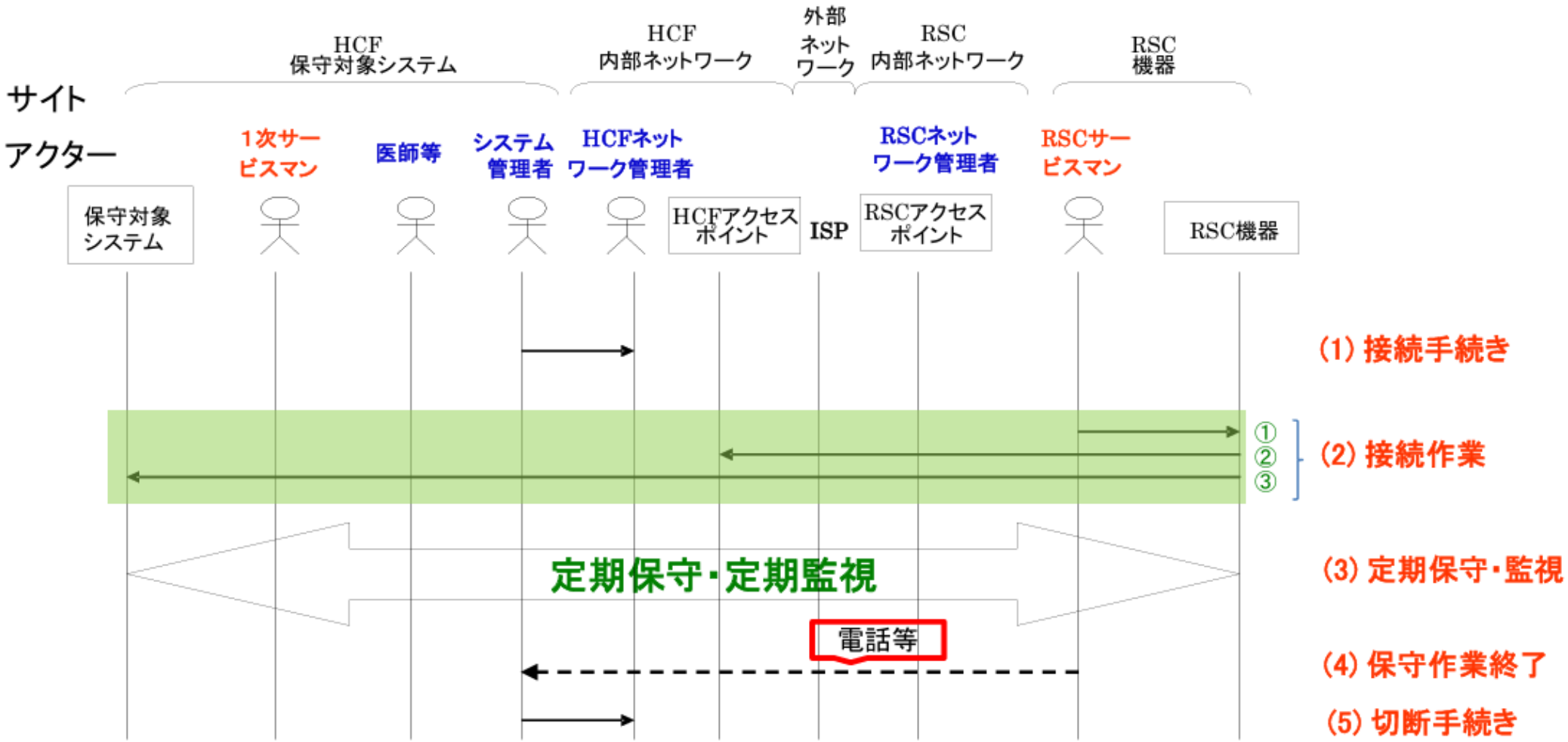
（3）ソフトウェアの改訂

- 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

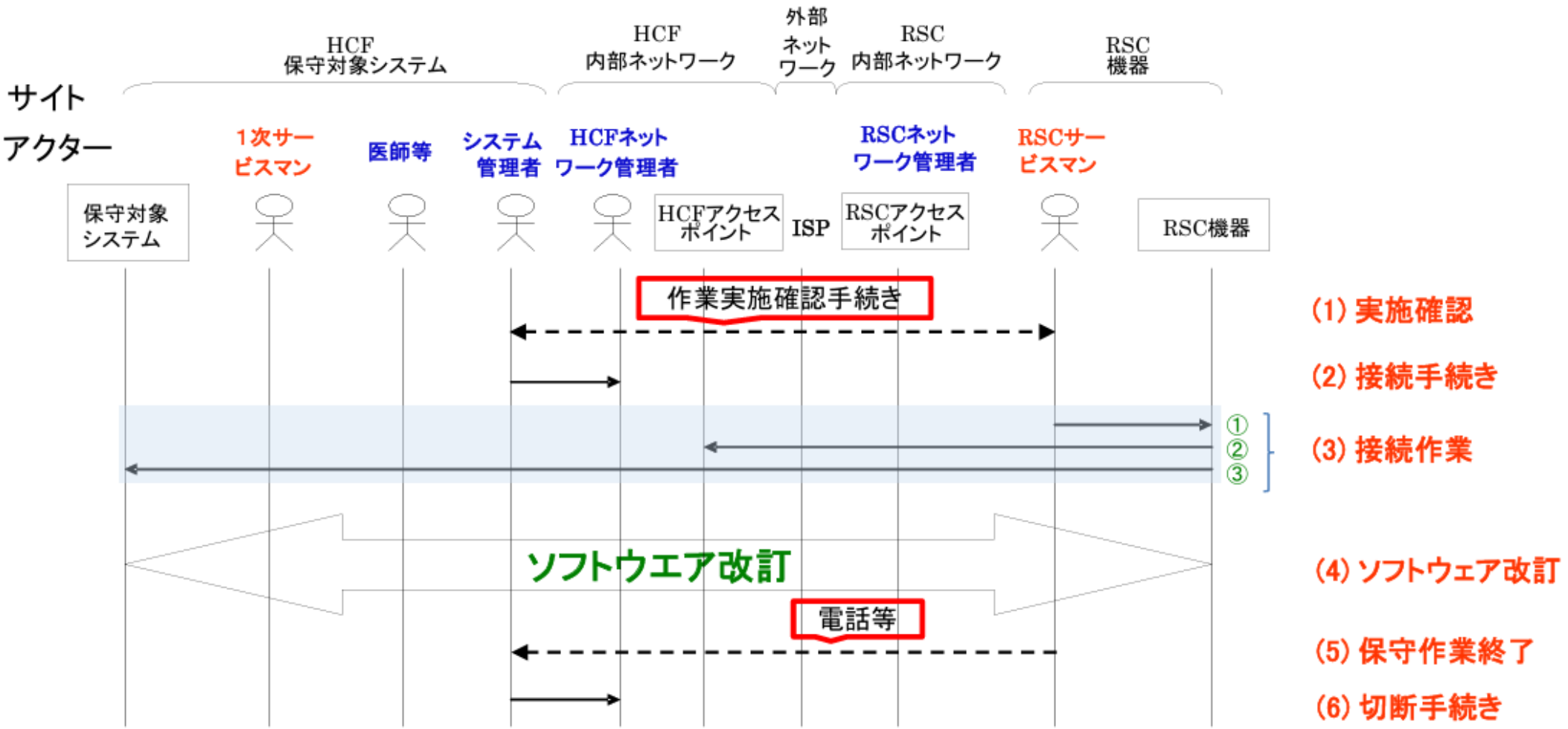
7．2　故障時の対応フロー



7．3　定期保守・定期監視


HCF
保守対象システム
HCF
内部ネットワーク
外部
ネット
ワーク
RSC
内部ネットワーク
RSC
機器
サイト
アクター
1次サー
ビスマン
医師等
システム
管理者
HCFネット
ワーク管理者
RSCネット
ワーク管理者
RSCサー
ビスマン
保守対象
システム
HCFアクセス
ポイント
ISP
RSCアクセス
ポイント
RSC機器
(1) 接続手続き
①
②
③
(2) 接続作業
定期保守・定期監視
(3) 定期保守・監視
電話等
(4) 保守作業終了
(5) 切断手続き

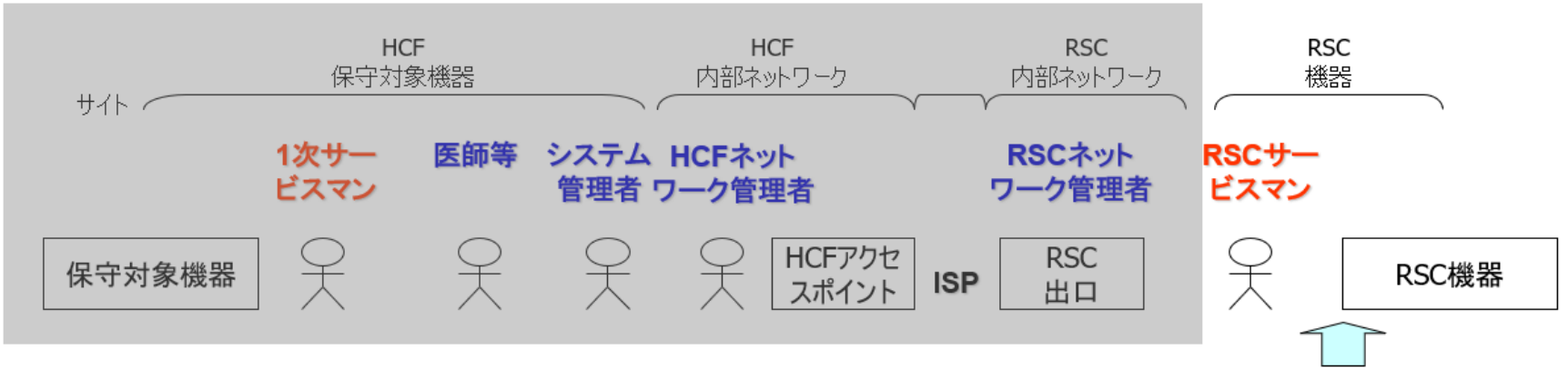
7．4　ソフトウェアの改訂



8．リスク分析とセキュリティ対策

- リスク分析
  - 運用モデルのサイト別に資産を洗い出し、それに対する脅威と脆弱性を分析
- リスク分析の考え方
  - HCF内のリスクは、HCFの情報管理者が検討
  - サイトの管理範囲がHCFの場合、HCF毎に別途行う必要あり
  - リモートサービスの有無にかかわらず存在するリスク（マルウェア脅威等）は、本GLの適用範囲外
  - 附属書A、Bにリモートサービスのリスク分析（例）を記載
- セキュリティ対策方針の決定
  - 組織的・人的・物理的・技術的安全管理措置
- セキュリティ対策
  - 技術的対策と運用的対策について、サイト別の対策(例)を記載

RSC機器でのリスクアセスメント（1例）



資産	番号	脅威（C:機密性,I:完全性,A:可用性）
メモリ・ディスク・画面上のPHI情報	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
上記PHI情報のメモやプリントアウトの紙	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
上記PHI情報のバックアップ媒体	14	修理の都合で記録した媒体の持出Cによる暴露C
PHI情報を扱うソフトウエア	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
PHI情報を扱う機器	16	持出C,タンパリングC,漏えい電磁波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
PHI情報を扱う機器の環境設備*1	18	故障A,被災A,破壊Aによるサービス不能A
PHI情報を扱う操作者	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
暗号アルゴリズムと鍵と鍵配送方式	1a	暗号化データの解読Cによる暴露C

9. 技術的・制度的変化への対応

- 本ガイドラインは、2026年4月時点でのセキュリティに関する技術状況及び、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
  - 2026年6月に発出された厚生労働省「医療情報システムの安全管理に関するガイドライン　第7.0版」には未対応
- 本ガイドラインは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
  - 特定の技術や製品に依存していない
  - 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あり
- このため、本ガイドラインの内容については適宜見直し、必要に応じて改訂
  - 安全管理GL第7版対応を今後進めてまいります。

RSS-GL Ver.5で追加された項目

5.4. リモートサービスのライフサイクルにおける義務と責任
  5.4.1. 契約前の合意形成及び契約中の合意の維持
  5.4.2. 通常時の義務
  5.4.3. 危機管理対応時の義務及び責任
  5.4.4. 合意形成における要求事項

を新設して、経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」と整合を取っている。

特に、5.4.4.では、医療機関との合意形成におけるリモートサービスベンダーへの要求事項を以下のようにまとめている。

- 医療機関等への適切な情報提供をSDS、SLA等で行うこと。その際、適切な共通理解が得られるよう医療機関等が容易に理解可能になるように努めること
- 合意形成にあたり、双方の運用管理を踏まえた形で役割分担を定め、その内容を情報提供に含めること
- 安全管理の妥当性について医療機関等と共通理解を得るために、安全管理に係る評価（リスクアセスメント）を行い、評価結果を医療機関等へ情報提供すること
- 医療情報を取り扱う事業者として最低限の適格性を医療機関等に示すため、情報セキュリティに係る公的な第三者認証等として、プライバシマーク認定または ISMS 認証を取得すること

RSS-GL参考資料の紹介

RSS-GL 参考資料

工業会規格(JESRA) | ディスプレイ（モニタ） | セキュリティ | 診断レポート | 動物 | COVID-19 感染予防

セキュリティ

■ リモートサービスセキュリティガイドラインに関する参考資料

JIRA/JAHIS合同リモートサービスセキュリティWGにて作成している「リモートサービスセキュリティガイドライン」に関する参考資料を公開します。
リスクアセスメント実施時、リモートサービスのSDS作成時等にご利用ください。

<ダウンロード>

- （1）ISMS準拠リモートサービスリスクアセスメント表（使用方法）
- （2）ISMS準拠リモートサービスリスクアセスメント表（見本）（2025年2月6日差し替え）
- （3）ISMS準拠リスクアセスメント（テンプレート）（2025年2月6日差し替え）
- （4）リモート保守サービスSLAサンプル_Ver.1.0 （しおり付き）
- （5）リモート保守サービスSLAサンプル解説付き
- （6）RSS_SDS_チェックリスト（SDS Ver.4.1) Rev.3.1a（2026年9月18日差し替え）

JIRA-HPの「セキュリティ」のページからダウンロードできます。

リモート保守サービスSLAサンプル

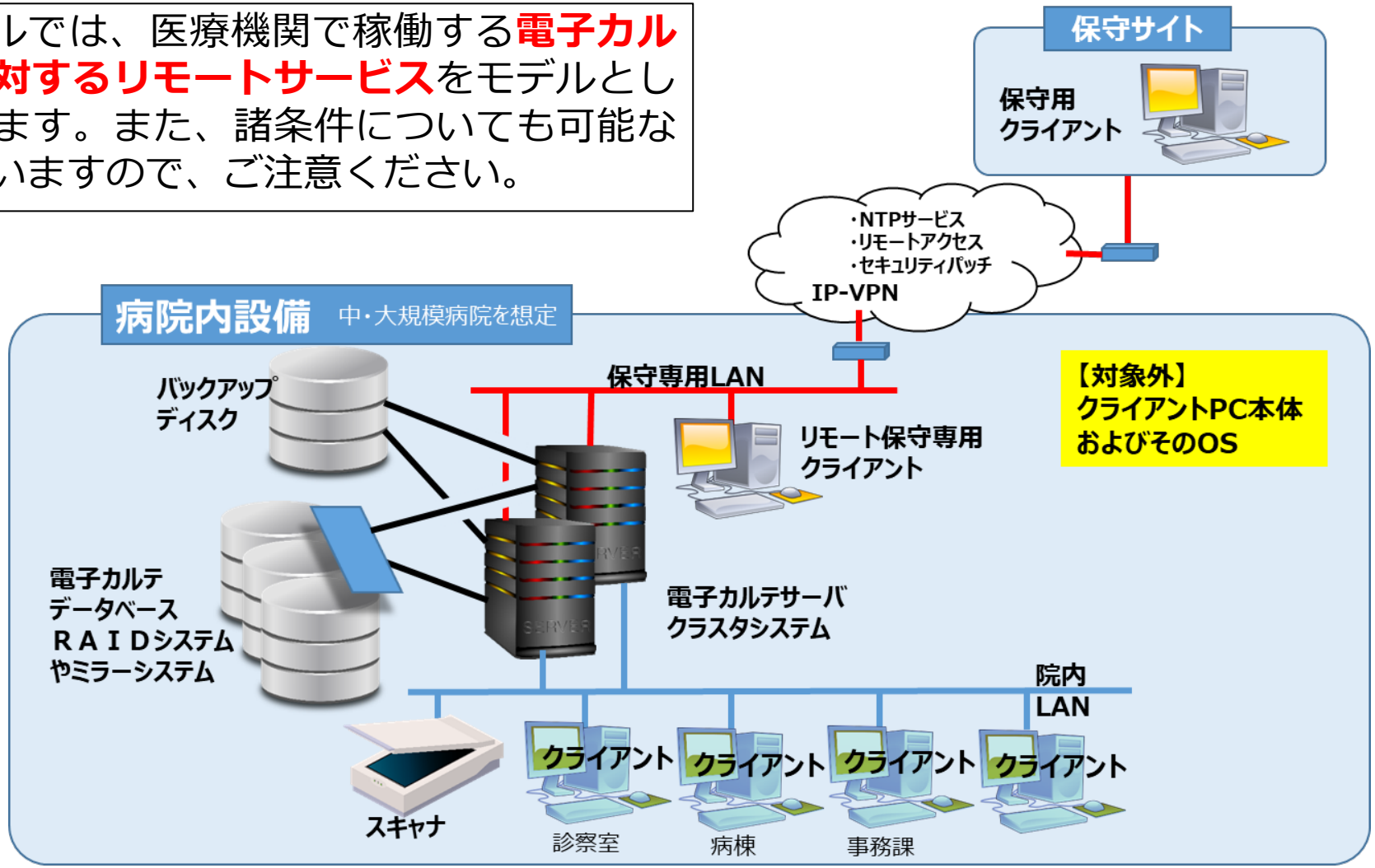
- 参考資料の「リモート保守サービスSLAサンプル」は、
  - リモートサービスセキュリティガイドラインにおいて定義されたサービスモデルを踏まえ、
  - サンプルのリモート保守サービスを仮定した上で、そのサービスのSLAを作成したものです。

- 本SLAサンプル作成にあたっては、
  - 総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の添付文書である「別紙1　ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」のSLAを基にしています。

- また、本SLAサンプルは、
  - SDSサンプルを作成するために設定したものであり、利用する各社はあくまで参考として自社サービスのSLAおよびSDS策定の参考としてください。

リモート保守サービスSLAサンプルのサービスモデル

本SLAサンプルでは、医療機関で稼働する**電子カルテシステムに対するリモートサービス**をモデルとして採用しています。また、諸条件についても可能な限り定義していますので、ご注意ください。



リモート保守サービスSLAサンプルの構成

A1. 本サービスの目的と対象
- A1.1. 本サービスの目的
- A1.2. 本サービスの提供範囲
- A1.3. 本サービスの提供時間

A2. 本SLAについて
- A2.1. 本サービスにおけるサービスレベル合意書の意義
- A2.2. 本サービスにおけるサービスレベル適用の考え方
- A2.3. 本SLAの適用期間
- A2.4. 本SLAの改定

A3. 前提条件
- A3.1. リスクマネジメント
- A3.2. サービス利用環境
- A3.3. サービス提供環境・運用に係る前提条件
- A3.4. 機器・ソフトウェアの品質
- A3.5. 準拠する法令・ガイドライン等
- A3.6. 守秘義務等
- A3.7. 監査

A4. 役割分担
- A4.1. システム構成上の役割分担と責任
- A4.2. 甲の業務上の役割分担と責任
- A4.3. 再委託事業者・連携対象事業者等
- A4.4. 連絡体制

A5. サービス仕様
- A5.1. ネットワークセキュリティに関するサービス仕様
- A5.2. 受託情報に関するサービス仕様

A6. 運用内容
- A6.1. 運用組織・規定等
- A6.2. 受託情報の取扱い
- A6.3. 運用仕様及びその指標
- A6.4. 非常時の対応
- A6.5. 報告事項・事前連絡
- A6.6. サポート

A7. サービスレベルに関する合意事項
- A7.1. サービスレベルの評価方法
- A7.2. サービスレベルマネジメント

※参照している総務省・経済産業省のガイドラインと同じ構成です。

リモートサービスセキュリティSDSチェックリスト

- 参考資料の「RSS_SDS_チェックリスト」は、
  - SLAサンプルで定義したサービスモデルとそのサービス内容について、SDSチェックシートを活用し必要項目をまとめたものです。
  - 各社のサービス仕様と照らし合わせる等、参考としてください。

- リモートサービスとSDSの位置づけ
  - 本説明での開示書（SDS）は、MDSと同じく厚生労働省の「医療情報システムの安全管理に関するガイドライン（以下、安全管理GL）」に基づいています。
  - 開示書（MDS/SDS）テンプレートでは、安全管理GL５.２版の章立て記載を残し、保守ベンダーによる対応可否の状況を問う質問項目を提示してあります。
  - ご利用の時点で、最新版のテンプレートをJIRA-HPの「「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド」よりご取得ください。

御清聴 ありがとうございました。