医用画像システム部会 2023年度成果報告会

特別講演
リモートサービスセキュリティガイドラインと SDSサンプルの解説

一般社団法人 日本画像医療システム工業会
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

本日の内容

1. サイバーセキュリティ対策の状況
   - 厚労省から医療機関への要請内容
   - 安全管理GLの遵守事項

2. リモートサービスにおけるサイバーセキュリティ対応
   - リモートサービスセキュリティガイドライン（RSS-GL)
   - リモートサービスのSDSサンプル

サイバーセキュリティ対策の状況

- 最近のサイバー攻撃動向（IPA編「情報セキュリティ白書2023」）

  - 企業・団体におけるランサムウェア被害の増加
  - 攻撃者の組織化、分業化
    - ランサムウェア攻撃をサービスとして提供する「RaaS(Ransomware as a Service)」の普及

- 医療機関への攻撃と侵入経路（各事案の報告書より）
  - 徳島県つるぎ町立半田病院　2021年10月
    - 医療機器のメンテナンス等で接続するVPN装置の脆弱性を悪用した侵入か
  - 大阪急性期・総合医療センター　2022年10月
    - 業者の給食システムにリモート保守のために設置したVPN機器より侵入

国のサイバーセキュリティ対策

- サイバーセキュリティ基本法（2015年1月施行）
  - サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定
- 医療分野のサイバーセキュリティ対策について（厚生労働省）

  （https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html）
  - 医療機関がサイバー攻撃を受けた際の厚生労働省連絡先
  - 医療法施行規則の一部を改正する省令について
  - 医療機関等におけるサイバーセキュリティ対策の強化について
  - 医療情報システムの安全管理に関するガイドライン第6.0版
  - 医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

サプライチェーンリスク全体の確認

- 自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

https://www.mhlw.go.jp/content/10808000/001079508.pdf

医療情報システムの安全管理に関するガイドライン　第6.0版 企画管理編

１２．サイバーセキュリティ 【遵守事項】

- ① サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。
- ② 医療機関等において整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。
- ③ サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。
- ④ サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認する。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。
- ⑤ サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。

https://www.mhlw.go.jp/content/10808000/001102575.pdf

４．５　リスク評価とリスク管理

- なお、医療情報システムの安全管理上のリスク評価、リスク管理を実施するに当たっては、医療情報システム・サービス事業者から技術的対策等の情報を収集することが重要である。
- 例えば、総務省・経済産業省が定めている「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」における「サービス仕様適合開示書」や日本画像医療システム工業会（JIRA）の工業会規格（JESRA）及び保健医療福祉情報システム工業会（JAHIS）のJAHIS標準となっている「『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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリスト等を参考に、当該事業者から情報提供していただく等により、当該事業者と医療情報システムの安全管理上のリスクについて共通の理解を得た上で、リスク管理に関する合意形成（リスクコミュニケーション）を図ることが求められる。

https://www.mhlw.go.jp/content/10808000/001102570.pdf

本日の内容

１．サイバーセキュリティ対策の状況

– 厚労省から医療機関への要請内容

– 安全管理GLの遵守事項

２．リモートサービスにおけるサイバーセキュリティ対応

– リモートサービスセキュリティガイドライン（RSS-GL）

– リモートサービスのSDSサンプル

JIRA　リモートサービスセキュリティWG

- JIRA セキュリティ委員会　リモートサービスセキュリティWG（RSS-WG)
  - 活動内容
    - JAHIS（一般社団法人 保健医療福祉情報システム工業会）セキュリティ委員会と合同のWG
    - 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検討
  - 成果
    - JESRA TR-0034*C リモートサービスセキュリティガイドライン Ver.3.1
    - ISO TS11633-1:2019 Information security management for remote maintenance of medical devices and medical information systems – Part 1:Requirements and risk analysis

リモートサービスセキュリティガイドライン（RSS-GL)

- JESRA TR-0034*C リモートサービスセキュリティガイドライン Ver.3.1
  - 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の手法に従ったリスクマネジメントの実施例を提示
  - 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（特に患者の医療情報）を安全かつ効率的な保護を実現

本日の内容

1．サイバーセキュリティ対策の状況
- 厚労省から医療機関への要請内容
- 安全管理GLの遵守事項

2．リモートサービスにおけるサイバーセキュリティ対応
- リモートサービスセキュリティガイドライン（RSS-GL）
- リモートサービスのSDSサンプル

リモートサービスのSDS

- 医療情報システムの安全管理に関するガイドライン　第6版　概説編
  - 「医療情報システムの安全管理上のリスク評価、リスク管理を実施するに当たっては、医療情報システム・サービス事業者から技術的対策等の情報を収集することが重要」
  - 「『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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリスト等を参考に、当該事業者から情報提供」

→JIRAセキュリティ委員会では、リモートサービスのセキュリティ対応について
SDSによる情報提供をJIRA会員企業に推奨

→普及促進のために、JIRAのHPにてSDSサンプルを公開

リモートサービスのSDSチェックリストサンプル

JIRA 一般社団法人 日本画像医療システム工業会
Japan Medical Imaging and Radiological Systems Industries Association

Google 提供　会員ページ

Home ▸ 関係団体リンク ▸ サイトマップ ▸ お問い合わせ ▸ English

JIRAについて | 部会・委員会等 | 刊行物 | 展示会 | セミナー | トピックス

Home ＞ 刊行物 ＞ 指針・標準・基準等 ＞ セキュリティ

刊行物：指針・標準・基準等

工業会規格(JESRA) | モニタ | セキュリティ | 診断レポート | 動物 | COVID-19

セキュリティ

■ NEW 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
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）
- （3）ISMS準拠リスクアセスメント（テンプレート）
- （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.4.0) Rev.1

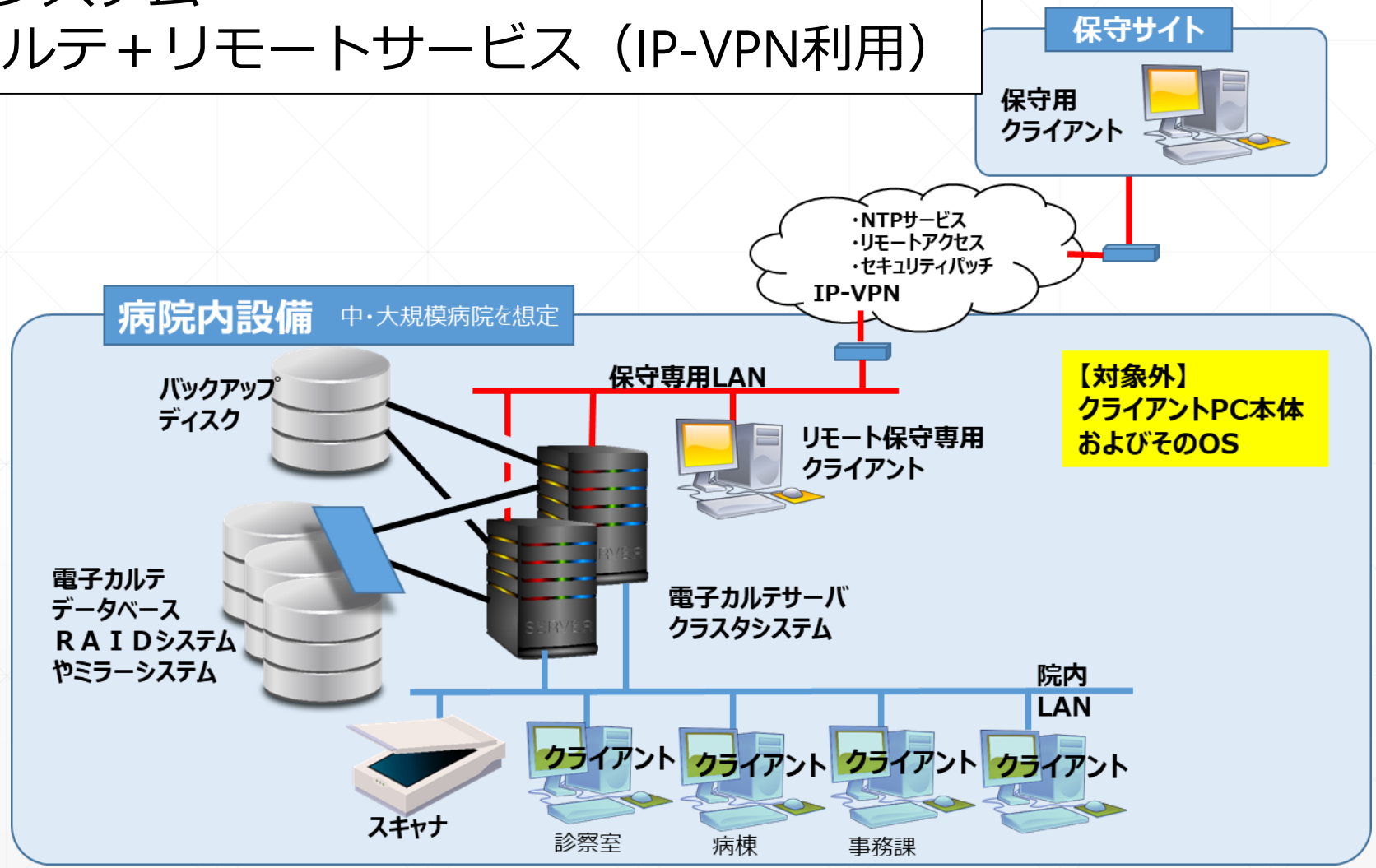
JIRAトップページより、
「刊行物」
→「指針・標準・基準等」
→「セキュリティ」

- （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）
- （3）ISMS準拠リスクアセスメント（テンプレート）
- （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.4.0) Rev.1

https://www.jira-net.or.jp/publishing/security.html

リモート保守サービスのサービスモデル

サンプルSDSの想定システム
オンプレミス電子カルテ＋リモートサービス（IP-VPN利用）



リモートサービスのSDSサンプル（1/12）

サービス事業者による医療情報セキュリティ開示書（医療情報システムの安全管理に関するガイドライン第5.2版対応）

作 成 日	2023年10月4日
サービス事業者	リモートメンテナンス株式会社（仮称）
サービス名称	電子カルテシステムリモート保守サービス
バージョン	1.1

※本書式を作成したJAHIS/JIRAは、製品設計・設置・保守等の認証・試験・検査等は行っていません。また、特定の医療機関等における特定の目的・ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者/サービス事業者が全責任を負います。

診療録及び診療諸記録を外部に保存する際の基準(8.)					
1　診療録及び診療諸記録の外部保存を受託するか？(8.3)	該当	**非該当**		備考	-
1．1　保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.3.C1(1)～(5))	はい	いいえ	対象外	備考	-
1．2　保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.3.C2(1)～(9))	はい	いいえ	対象外	備考	-
医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践(6.2)					
2　扱う情報のリストを医療機関等に提示できるか？(6.2.C1)	**はい**	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（2/12）

組織的安全管理対策（体制、運用管理規程）(6.3)		
3　医療情報システムを運用する際に、医療情報システム安全管理責任者を設置しているか？(6.3.C1)	はい	いいえ　対象外　備考　-
4　医療情報システムを運用する際に、運用担当者を限定しているか？(6.3.C1)	はい	いいえ　対象外　備考　-
5　個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？(6.3.C2)	はい	いいえ　対象外　備考　-
6　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？(6.3.C3)	はい	いいえ　対象外　備考　-
7　医療機関等との契約に安全管理に関する条項を含めているか？(6.3.C4)	はい	いいえ　対象外　備考　-
8　個人情報を含む医療情報システムの業務をサービス事業者が外部委託する場合、その外部委託先との契約に再委託先を含めた安全管理に関する条項を含めているか？(6.3.C4)	はい	いいえ　対象外　備考　-
9　運用管理規程等において組織的安全管理対策に関する事項等を定めているか？(6.3.C5)	はい	いいえ　対象外　備考　-
物理的安全対策(6.4)		
１０　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？(6.4.C1)	はい	いいえ　対象外　備考　-
１１　個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？(6.4.C2)	はい	いいえ　対象外　備考　-
１２　個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？(6.4.C3)	はい	いいえ　対象外　備考　-
１２．１　入退出の事実を記録しているか？(6.4.C3)	はい	いいえ　対象外　備考　-
１２．２　入退者の記録を定期的にチェックし、妥当性を確認しているか？(6.4.C3)	はい	いいえ　対象外　備考　-
１３　個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置しているか？(6.4.C4)	はい	いいえ　対象外　備考　-
１４　個人情報が入力・参照できる端末に覗き見防止の機能があるか？(6.4.C5)	はい	いいえ　対象外　備考　-
１５　サービス事業者の管理端末に覗き見防止対策が取られているか？(6.4.C5)	はい	いいえ　対象外　備考　-

リモートサービスのSDSサンプル（3/12）

技術的安全対策(6.5)					
１６　権限を持たない者による不正入力を防止する対策が行われているか？(6.5.C1、6.5.C4)	**はい**	いいえ	対象外	備考	-
１７　アクセス管理の機能があるか？(6.5.C1)	**はい**	いいえ	対象外	備考	-
１７．１　利用者の認証方式は？(6.5.C1)(6.5.C13)					
・記憶（ID・パスワード等）	**はい**	いいえ	対象外	備考	-
・生体認証（指紋等）	はい	**いいえ**	対象外	備考	-
・物理媒体（ICカード等）	**はい**	いいえ	対象外	備考	1
・上記のうちの2要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	**はい**	いいえ	対象外	備考	2
・その他（具体的な方法を備考に記入してください）	はい	**いいえ**	対象外	備考	-
１７．１．１　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C14 (1)～(5))	**はい**	いいえ	対象外	備考	-
１７．１．１．１　他の手段と併用した際のパスワードの運用方法を運用管理規程に定めているか？(6.5.C14(1))	**はい**	いいえ	対象外	備考	-
１７．１．１．２　本人確認の実施の際、本人確認方法を台帳に記載しているか？(6.5.C14(2))	**はい**	いいえ	対象外	備考	3
１７．１．１．３　パスワードの有効期限が管理できるか？(6.5.C14(4))	**はい**	いいえ	対象外	備考	-
１７．１．１．４　文字列制限をチェックすることができるか？(6.5.C14(4))	**はい**	いいえ	対象外	備考	-
１７．１．１．５　類推しやすいパスワードをチェックすることができるか？(6.5.C14(5))	**はい**	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（3-1/12）

	備考記載欄
1	リモート保守センターの居室について、ICカード（社員証）による入退室管理を実施している
2	システムに対するID/パスワード認証を実施し、居室にはICカードによる認証を実施している
3	システム管理側でパスワードの再発行をする際には、運用管理規定に定められた本人確認を実施し、台帳に記入している
4	ICカードの盗難紛失等の対応の臨時カード発行ルール、およびパスワード忘れ時のパスワード再発行ルールを規定している
5	利用者とはRSCの保守作業者を指し、契約者の直接閲覧は出来ないが必要に応じ監査の際に開示ができる
6	非常時にはBCPに基づきリモートサービスを停止し、回復時に通常運用で再開させる
7	医療機関等に送付するファイルについては無害化処理を実行する。医療機関等からは実行ファイルは受け取らない。

リモートサービスのSDSサンプル（4/12）

１７．２　利用者の職種･担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	**はい**	いいえ	対象外	備考	-
１７．３　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	-
１７．３．１　アクセスログを利用者が確認する機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	5
１７．３．２　アクセスログへのアクセス制限ができるか？(6.5.C8)	**はい**	いいえ	対象外	備考	-
１７．３．３　アクセスログへのアクセス制限機能がない場合、不当な削除/改ざん/追加等を防止する運用的対策を講じているか？(6.5.C8)	はい	いいえ	**対象外**	備考	-
１７．４　アクセス記録（アクセスログ）機能が無い場合、利用者が監査できる形でサービス事業者が業務日誌等に操作の記録を行っているか？(6.5.C7)	はい	いいえ	**対象外**	備考	-
１８　時刻情報の正確性を担保する仕組みがあるか？(6.5.C9)	**はい**	いいえ	対象外	備考	-
１９　不正なソフトウェアが混入していないか確認しているか？(6.5.C10、6.5.C11)	**はい**	いいえ	対象外	備考	-
２０　システムにメールの送受信機能がある場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(6.5.C12)	はい	いいえ	**対象外**	備考	-
２１　システムでファイル交換機能を使用する場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(6.5.C12)	**はい**	いいえ	対象外	備考	7
２２　無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C15)	はい	いいえ	**対象外**	備考	-
２３　IoT機器を使用する場合、IoT機器により患者情報を取り扱うことに関する運用管理規程を定めた上で、医療機関等に開示できるか？(6.5.C16(1))	はい	いいえ	**対象外**	備考	-
２３．１　ウェアラブル端末や在宅設置のIoT機器を利用する場合、患者のリスク等に関する説明資料を提供できるか？(6.5.C16(2))	はい	いいえ	対象外	備考	-
２３．２　IoT機器のセキュリティアップデートを必要なタイミングで適切に実施できるか？(6.5.C16(3))	はい	いいえ	対象外	備考	-
２３．３　使用が終了または停止したIoT機器の接続を遮断できるか？(6.5.C16(4))	はい	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（4-1/12）

	備考記載欄
1	リモート保守センターの居室について、ICカード（社員証）による入退室管理を実施している
2	システムに対するID/パスワード認証を実施し、居室にはICカードによる認証を実施している
3	システム管理側でパスワードの再発行をする際には、運用管理規定に定められた本人確認を実施し、台帳に記入している
4	ICカードの盗難紛失等の対応の臨時カード発行ルール、およびパスワード忘れ時のパスワード再発行ルールを規定している
5	利用者とはRSCの保守作業者を指し、契約者の直接閲覧は出来ないが必要に応じ監査の際に開示ができる
6	非常時にはBCPに基づきリモートサービスを停止し、回復時に通常運用で再開させる
7	医療機関等に送付するファイルについては無害化処理を実行する。医療機関等からは実行ファイルは受け取らない。

リモートサービスのSDSサンプル（5/12）

人的安全対策(6.6)					
２４　従業者との間で、雇用時または契約時に守秘義務契約を結んでいるか？（6.6.C1(1)）	はい	いいえ	対象外	備考	-
２５　従業者に対し、定期的に個人情報管理に関する教育訓練を行っているか？（6.6.C1(2)）	はい	いいえ	対象外	備考	-
２６　従業者の退職後または契約終了後における個人情報保護に関する規程が従業者との契約に含まれているか？（6.6.C1(3)）	はい	いいえ	対象外	備考	-
２７　就業規則等には守秘義務違反に対する包括的な罰則規定が含まれているか？（6.6.C2(1)a）	はい	いいえ	対象外	備考	-
２８　保守作業等で医療情報システムに直接アクセスする作業を行う際には、作業者・作業内容・作業結果を医療機関等に報告できるようになっているか？（6.6.C2(1)b）	はい	いいえ	対象外	備考	-
２９　清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っているか？（6.6.C2(1)c）	はい	いいえ	対象外	備考	-
３０　業務の一部を外部委託する場合に、外部委託先に対し、自らに課しているのと同等の個人情報保護に関する対策を施す義務を、契約によって担保しているか？（6.6.C2(1)d）	はい	いいえ	対象外	備考	-
３１　やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行っているか？(6.6.C2(2))	はい	いいえ	対象外	備考	-
情報の破棄(6.7)					
３２　ユーザに提示できる情報種別ごとの破棄の手順があるか？(6.7.C1)	はい	いいえ	対象外	備考	-
３２．１　手順には破棄を行う条件を含めているか？(6.7.C1)	はい	いいえ	対象外	備考	-
３２．２　手順には破棄を行うことができる従業者の特定を含めているか？(6.7.C1)	はい	いいえ	対象外	備考	-
３２．３　手順には破棄の具体的な方法を含めているか？(6.7.C1)	はい	いいえ	対象外	備考	-
３３　情報処理機器自体を破棄する場合、必ず専門的な知識を有する者が行うこととし、残存し、読み出し可能な情報がないことを報告できるか？(6.7.C2)	はい	いいえ	対象外	備考	-
３４　破棄を外部委託した場合、外部委託業者の監督及び守秘義務契約に準じた監督責任の下、情報の破棄を確認しているか？(6.7.C3)	はい	いいえ	対象外	備考	-
３５　不要になった個人情報を含む媒体の破棄を、運用管理規程に定めているか？(6.7.C4)	はい	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（6/12）

医療情報システムの改造と保守(6.8)					
３６　改造や保守に関する動作確認で個人情報を含むデータを使用する場合、作業員と守秘義務契約を交わしているか？(6.8.C1)	**はい**	いいえ	対象外	備考	-
３７　作業員はサービス事業者自身が定めた運用管理規程に従い、改造や保守に関する業務を行っているか？(6.8.C1)	**はい**	いいえ	対象外	備考	-
３８　運用管理規程には作業終了後に動作確認で使用した個人情報を含むデータを消去する規定が含まれているか？(6.8.C1)	**はい**	いいえ	対象外	備考	-
３９　改造や保守に用いるアカウントは、作業員個人の専用アカウントを使用しているか？(6.8.C2)	**はい**	いいえ	対象外	備考	-
４０　改造や保守に関する作業の記録として、個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を医療機関等に提供できるか？(6.8.C2)	**はい**	いいえ	対象外	備考	-
４１　アカウント情報の外部流出等による不正使用の防止に努めているか？(6.8.C3)	**はい**	いいえ	対象外	備考	-
４２　作業員の離職や担当替え等に対して速やかに保守用アカウントを削除しているか？(6.8.C4)	**はい**	いいえ	対象外	備考	-
４３　改造や保守を外部委託している場合、保守要員の離職や担当替え等の際に報告を義務付けているか？(6.8.C4)	**はい**	いいえ	対象外	備考	-
４３．１　報告に応じてアカウントを削除する管理体制ができているか？(6.8.C4)	**はい**	いいえ	対象外	備考	-
４４　メンテナンスを実施する場合は、事前に医療機関等に作業申請を提出できるか？(6.8.C5)	**はい**	いいえ	対象外	備考	-
４５　メンテナンス終了時に、速やかに医療機関等に作業報告書を提出できるか？(6.8.C5)	**はい**	いいえ	対象外	備考	-
４６　保守を外部委託する場合、保守事業者 と守秘義務契約を締結しているか？(6.8.C6)	**はい**	いいえ	対象外	備考	-
４７　個人情報を含むデータを組織外に持ち出す際に、医療機関等の責任者の承認を得ることが運用管理規程に定められているか？(6.8.C7)	はい	いいえ	**対象外**	備考	-
４８　リモートメンテナンスによる改造・保守を行う場合は、アクセスログを収集するか？(6.8.C8)	**はい**	いいえ	対象外	備考	-
４９　リモートメンテナンスにおいて、医療機関等へ送付等を行うファイルは、送信側で無害化処理が行われているか？(6.8.C9)	**はい**	いいえ	対象外	備考	
５０　保守業務を外部委託している場合、外部委託事業者にも自らと同等な義務を求め、契約しているか？(6.8.C10)	**はい**	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（7/12）

情報 及び 情報機器の持ち出し 並びに 外部利用 について(6.9)					
５１　持出機器を提供しているか？(6.9)	該当	**非該当**		備考	-
５１．１　持出機器においてソフトウェアのインストールを制限する機能があるか？(6.9)	はい	いいえ	対象外	備考	-
５１．２　持出機器において外部入出力装置の機能を無効にすることができるか？(6.9)	はい	いいえ	対象外	備考	-
５１．３　外へ持ち出す際、情報に対して暗号化等の対策を行うことができるか？(6.9.C7)	はい	いいえ	対象外	備考	-
５１．４　持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	はい	いいえ	対象外	備考	-
５２　提供するサービスに係わる情報及び情報機器の持ち出しについて、リスク分析を実施しているか？(6.9.C1)	**はい**	いいえ	対象外	備考	-
５３　サービス事業者が情報及び情報機器を持出する場合があるか？(6.9.C1)	**該当**	非該当		備考	-
５３．１　リスク分析の結果を受けて、情報及び情報機器の持ち出しに関する方針を運用管理規程に定めているか？(6.9.C1)	**はい**	いいえ	対象外	備考	-
５３．２　持ち出した情報及び情報機器の管理方法を定めているか？(6.9.C2)	**はい**	いいえ	対象外	備考	-
５３．３　情報を格納した媒体及び情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか？(6.9.C3)	**はい**	いいえ	対象外	備考	-
５３．４　自社方針・規則等で定めた盗難、紛失時の対応を従業員等に対して周知徹底し、教育を行っているか？(6.9.C4)	**はい**	いいえ	対象外	備考	-
５３．５　情報機器について、起動パスワード等を設定しているか？(6.9.C6)	はい	いいえ	**対象外**	備考	-
５３．６　パスワード設定においては、適切なパスワード管理措置を行っているか？(6.9.C6)	**はい**	いいえ	対象外	備考	-
５３．７　サービス事業者が外へ持ち出す際、情報に対して暗号化等の対策を行っているか？(6.9.C7)	**はい**	いいえ	対象外	備考	-
５３．８　医療機関等または医療機関等に委託されたサービス事業者が、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	はい	いいえ	**対象外**	備考	-
５４　情報の管理者は情報機器・媒体の所在について台帳を用いる等して管理しているか？(6.9.C5)	**はい**	いいえ	対象外	備考	-
５５　個人保有の情報機器の利用を禁止しているか？(6.9.C10)	**はい**	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（8/12）

災害、サイバー攻撃等の非常時の対応(6.10)					
５６　医療機関等に提供可能なサービス事業者のBCP手順書が用意されているか？(6.10.C1、6.10.C2)	**はい**	いいえ	対象外	備考	-
５７　非常時アカウント又は、非常時にも医療サービスを継続して提供できる機能を持っているか？　(6.10.C4)	はい	いいえ	**対象外**	備考	6
５７．１　「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるか？ (6.10.C4(1))	はい	いいえ	対象外	備考	-
５７．２　非常時機能を有している場合、非常時機能が定常時に不適切に利用されることがないよう適切に管理及び監査できる情報を提供できるか？(6.10.C4(2))	はい	いいえ	対象外	備考	-
５７．３　非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更できるか？ (6.10.C4(3))	はい	いいえ	対象外	備考	-
５７．４　標的型メール攻撃等により医療情報システムに不正ソフトウェアが混入した場合、関係先への連絡手段を準備しているか？(6.10.C4(4))	はい	いいえ	対象外	備考	-
５８　重要なファイルをバックアップしているか？(6.10.C4(5))	はい	いいえ	**対象外**	備考	-
５８．１　バックアップは数世代、複数の方式で実施しているか？(6.10.C4(5))	はい	いいえ	対象外	備考	-
５８．２　数世代、複数方式のバックアップの一部は不正ソフトウェアの混入による影響が波及しないように管理されているか？ (6.10.C4(5))	はい	いいえ	対象外	備考	-
５８．３　バックアップからの復元手段が整備されているか？(6.10.C4(5))	はい	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（9/12）

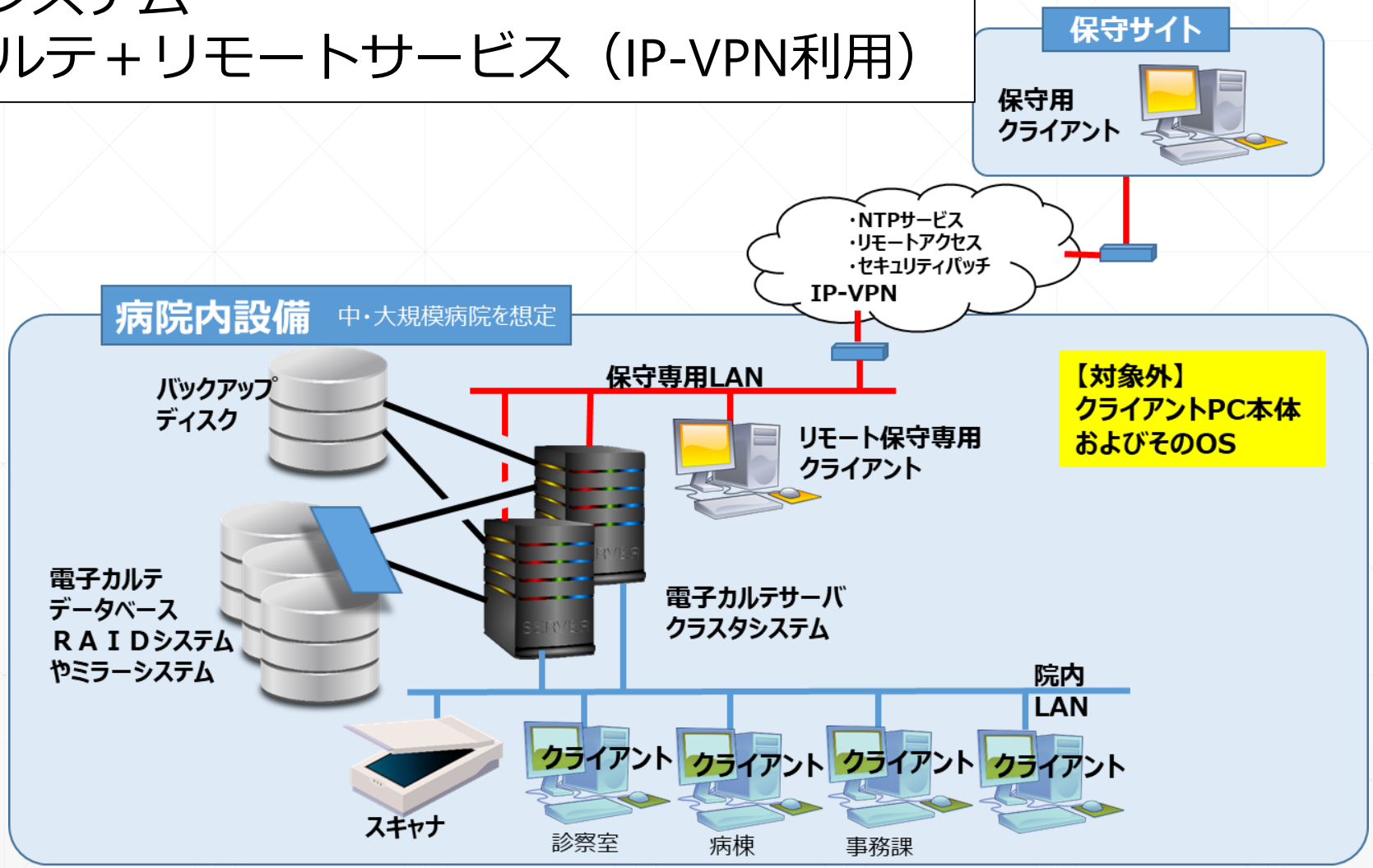
外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理(6.11)

５９～６３の質問は、提供するサービスで利用している通信方式について確認するものです。通信方式によって対策すべき項目が異なりますので、対応している通信方式それぞれに対して確認が必要です。対応する通信方式に「該当」とし、対応していない通信方式を「非該当」としてください。

５９	通信方式として専用線に対応しているか？(6.11)	該当	**非該当**		備考	-
５９．１	提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考	-
５９．２	採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-
６０	通信方式として公衆網に対応しているか？(6.11)	該当	**非該当**		備考	-
６０．１	提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考	-
６０．２	採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-
６１	通信方式としてIP-VPNに対応しているか？(6.11)	**該当**	非該当		備考	-
６１．１	提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	**はい**	いいえ	対象外	備考	-
６１．２	採用する認証手段が定められているか？(6.11.C2)	**はい**	いいえ	対象外	備考	-
６２	通信方式としてIPsec-VPN ＋IKEに対応しているか？(6.11)	該当	**非該当**		備考	-
６２．１	セッション間の回り込み等の攻撃への適切な対策をしているか？(6.11.C11)	はい	いいえ	対象外	備考	-
６２．２	採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-
６３	チャネル・セキュリティとしてTLS1.2以上のクライアント認証に対応しているか？(6.11)	**該当**	非該当		備考	-
６３．１	サーバ/クライアントともに「TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行っているか？(6.11.C11)	**はい**	いいえ	対象外	備考	-
６３．２	セッション間の回り込み等による攻撃への適切な対策を実施しているか？(6.11.C11)	**はい**	いいえ	対象外	備考	-

リモート保守サービスのサービスモデル

サンプルSDSの想定システム
オンプレミス電子カルテ＋リモートサービス（IP-VPN利用）



リモートサービスのSDSサンプル（11/12）

６４　ネットワーク上において、改ざんを防止する対策を行っているか？(6.11.C1)	はい	いいえ	対象外	備考	-
６５　ネットワーク上において、盗聴を防止する対策を行っているか？(6.11.C1)	はい	いいえ	対象外	備考	-
６６　ネットワーク上において、なりすましへの対策を行っているか？(6.11.C1)	はい	いいえ	対象外	備考	-
６７　データ送信元と送信先において、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行っているか？(6.11.C2)	はい	いいえ	対象外	備考	-
６８　ネットワークの経路制御・プロトコル制御を行える機器または機能を有するか？(6.11.C4)	はい	いいえ	対象外	備考	-
６９　ネットワークの経路制御・プロトコル制御に関わる機器または機能は、安全性を確認できるようなセキュリティ対策が規定された文書を示すことができるか？(6.11.C4)	はい	いいえ	対象外	備考	-
７０　医療機関等との通信経路について回り込みが行われないように経路設定を行っているか？(6.11.C4)	はい	いいえ	対象外	備考	-
７１　送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施しているか？(6.11.C5)	はい	いいえ	対象外	備考	-
７２　暗号化を利用する場合、暗号化の鍵について電子政府推奨暗号のものを使用しているか？(6.11.C5)	はい	いいえ	対象外	備考	-
７３　脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等が提示できるか？(6.11.C6、6.11.C9)	はい	いいえ	対象外	備考	-
７４　医療機関等から委託をされた範囲において、脅威に対する管理責任の範囲を医療機関等に明確に示し、その事項を示す文書等を提示できるか？(6.11.C6)	はい	いいえ	対象外	備考	-
７５　リモートメンテナンスサービスを有しているか？(6.11.C8)	該当	非該当		備考	-
７５．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する仕組みを有しているか？(6.11.C8)	はい	いいえ	対象外	備考	-
７６　回線の可用性等の品質に関して問題がないことを確認し、明確に文書等の証跡を残し、医療機関等に提示できるか？(6.11.C9)	はい	いいえ	対象外	備考	-

リモートサービスのSDSサンプル（12/12）

７７　患者に情報を閲覧させる機能があるか？(6.11.C10)	該当 **非該当**	備考　-
７７．１　情報の閲覧のために公開しているサービスにおいて、医療機関等の内部システムに不正な侵入等が起こらないように対策を実施しているか？(6.11.C10)	はい　いいえ　対象外	備考　-
７７．２　医療機関等が患者等へ危険性や情報提供の目的について説明を行うために必要となる情報を資料として提示できるか？(6.11.C10)	はい　いいえ　対象外	備考　-
７７．３　説明資料では、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にしているか？(6.11.C10)	はい　いいえ　対象外	備考　-
保存が義務付けられている文書を扱っている場合のみ下記対象		
法令で定められた記名･押印を電子署名で行うことについて(6.12)		
７８　記名･押印が義務付けられた文書を扱っているか？(6.12.C1)	該当 **非該当**	備考　-
７８．１　HPKI対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の署名機能があるか？(6.12.C1)	はい　いいえ　対象外	備考　-
７８．２　HPKI対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の検証機能があるか？(6.12.C1)	はい　いいえ　対象外	備考　-
７８．２．１　特定の国家資格の確認を行う必要がある場合に、電子的に検証できる機能があるか？(6.12.C1)	はい　いいえ　対象外	備考　-
７８．３　総務省の「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供する認定のタイムスタンプが付与可能か？(6.12.C2)	はい　いいえ　対象外	備考　-

リモートサービスのSDSチェックリストサンプル

JIRA 一般社団法人 日本画像医療システム工業会
Japan Medical Imaging and Radiological Systems Industries Association

Google 提供　会員ページ

Home ▸ 関係団体リンク ▸ サイトマップ ▸ お問い合わせ ▸ English

JIRAについて | 部会・委員会等 | 刊行物 | 展示会 | セミナー | トピックス

Home ＞ 刊行物 ＞ 指針・標準・基準等 ＞ セキュリティ

刊行物：指針・標準・基準等

工業会規格(JESRA) | モニタ | セキュリティ | 診断レポート | 動物 | COVID-19

セキュリティ

■ NEW 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
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）
- （3）ISMS準拠リスクアセスメント（テンプレート）
- （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.4.0) Rev.1

JIRAトップページより、
「刊行物」
→「指針・標準・基準等」
→「セキュリティ」

- （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）
- （3）ISMS準拠リスクアセスメント（テンプレート）
- （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.4.0) Rev.1

https://www.jira-net.or.jp/publishing/security.html

ご清聴
ありがとう
ございました

JIRA
一般社団法人 日本画像医療システム工業会
Japan Medical Imaging and Radiological Systems Industries Association