健康で豊かな国民生活を保健医療福祉情報システムが支えます

セキュリティ委員会活動報告

2024年2月13日

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
委員長　茗原秀幸

サイバーセキュリティに対するセキュリティ委員会の対応

セキュリティ関連のJAHIS標準類を多数発行

保存が義務付けられた診療録等の電子保存ガイドライン：電子保存・外部保存システムにおけるベンダーの技術的対策を規定（安全管理GL6版の内容を反映した改定作業を実施中）

ヘルスケア分野における監査証跡のメッセージ標準規約：医療情報システムにおける監査証跡としてのメッセージを規定

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：安全管理GL対応状況を自ら説明するための開示書を規定（安全管理GL6版対応に向け改定作業を実施中）

リモートサービスセキュリティガイドライン：リモート保守などのサービスを実施する際のサービサーとして考慮すべき事項を規定（ISO27001:2018、ISO27002:2018対応の改定作業を実施中）

HPKI対応ICカードガイドライン：HPKI証明書をICカードに格納した場合のHPKIへのアクセスメソッドを規定
（リファランスの最新化や表現の正確性を確保する改定作業を実施中）

ヘルスケアPKIを利用した医療文書に対する電子署名規格：HPKIを利用して否認防止のための電子署名の手続きを規定（JAdESフォーマット対応を追加した改定作業を実施中）

HPKI電子認証ガイドライン：HPKIを利用して本人確認などの認証を行う際の考慮すべき事項を規定

シングルサインオンにおけるセキュリティガイドライン：シングルサインオンの要求事項とリスクアセスメントの考え方を記載（FHIRの実装例の追加の検討を実施中）

セキュアトークン実装ガイド・機器認証編：医療機関内おける無線接続機器の機器認証のための考慮事項を記載（リファランスの最新化や最新の技術動向を踏まえた改定を実施）

セキュアトークン実装ガイド・ノード認証編：医療機関内、施設間などにおけるノード認証のための考慮事項を記載（リファランスの最新化や最新の技術動向を踏まえた改定を実施）

サイバーセキュリティに対するセキュリティ委員会の対応

近年は医療機関に対するランサムウェアによる重篤な被害が発生し、マスコミでも大きく報道されている。セキュリティ委員会では関係機関等と協力し各種啓発活動を実施している。

会員向け啓発活動や支援活動

リモートサービスセキュリティガイドライン対応「ISMS準拠リスクアセスメントテンプレート」の公開し、サンプルシステム（MDSの解説に用いるものと同一のモデル）を用いたリモート保守サービスに関するサンプルSLA、サンプルSDSを発行
MDS・SDS書き方セミナーの開催による会員への啓発
毎年6月に開催するセキュリティ標準化セミナーにてセキュリティ関連JAHIS標準類の啓発活動を実施
毎年3回開催の新人教育セミナーのセキュリティ教材にバックアップの考え方を詳述

関係各所への協力や支援活動

医療セプターオブザーバーとして重要インフラレターなどのチェックや重要な脆弱性に関する会員への啓発活動の実施
審査支払基金に対する電子処方箋、電子カルテ共有サービス等のセキュリティリスクアセスメント支援
消防庁に対する患者情報閲覧サービスのセキュリティリスクアセスメント支援
国などの各種有識者会議への参画と意見具申

セキュリティ委員会のJAHIS標準類策定における考え方と対応例

レギュレーションにおいては、厚生労働省の安全管理GLを遵守することを念頭に置き、安全管理GLと整合性を取った規約、ガイドラインを制定する

スタンダードにおいては、ISOとの整合性を確保するため、JAHIS標準類のISOへの提案や、ISO規格のJAHIS標準類への取り込みを実施する

工業会組織であるため、視点はあくまでベンダーの視点であり、医療サービサーや情報システムサービサーの視点ではない。

近年の課題

JAHIS会員が情報システムサービサーとなる事例が多く、クラウドに関する安全管理GLへの準拠性を示す開示書の策定要望やリモート保守における適正な対応が求められている。

課題を受けた対応

JAHIS標準「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」のチェックリストの安全管理GL第6版対応を実施し、並行してJAHIS標準の改定作業を実施

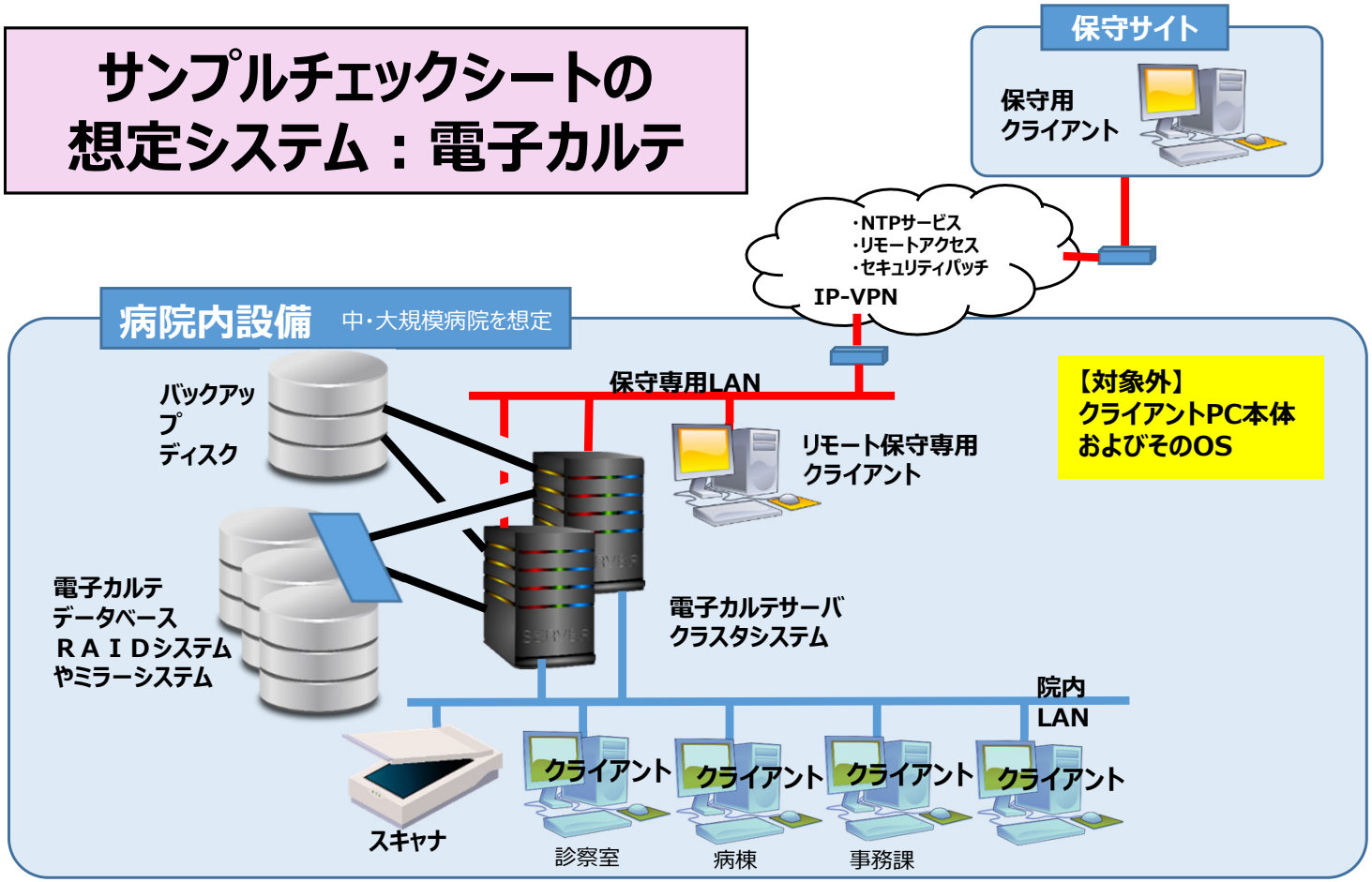
課題を受けた対応

JAHIS標準「リモートサービスセキュリティガイドライン」に基づくサンプルSLA、SDSを策定。また国からの要望に応じて様々なリモートサービスのリスクアセスメントに活用

MDS作成支援のため、一般的な構成と考えられるサンプルシステムを構成し、それに対応したサンプルMDSを作成している。JAHISのWebページに公開するとともに啓発セミナー等でサンプルの解説を行い、会員各社の自社製品のMDS作成作業が円滑に行えるよう支援している。

サンプルMDSにおける想定システム（電子カルテ）の構成例

サンプルチェックシートの想定システム：電子カルテ



リモートサービスセキュリティガイドライン

本ガイドラインでは、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す。それにより、医療機関の管理者、および遠隔保守を行うベンダが、実施例を参考にリスクアセスメントを実施することにより、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ることを期待している。
策定にあたっては、JIPDEC（一般財団法人日本情報経済社会推進協会）と連携し、JAHIS標準改定作業の際にはISMSの最新動向・規格の内容の確認などで連携を実施。

ポイント：
・標準的なリモート保守モデルを定義（予防保守、ソフトウェア改定、故障対応、監視）
・JISQ27001：2014ならびにJISQ27002：2014に対応したリスクアセスメントを実施
（現在JISQ27001：2023ならびにJISQ27002：2023対応に向けた改定を実施中）
・汎用的なリモートサービスのリスクアセスメントに利用可能なテンプレートを作成

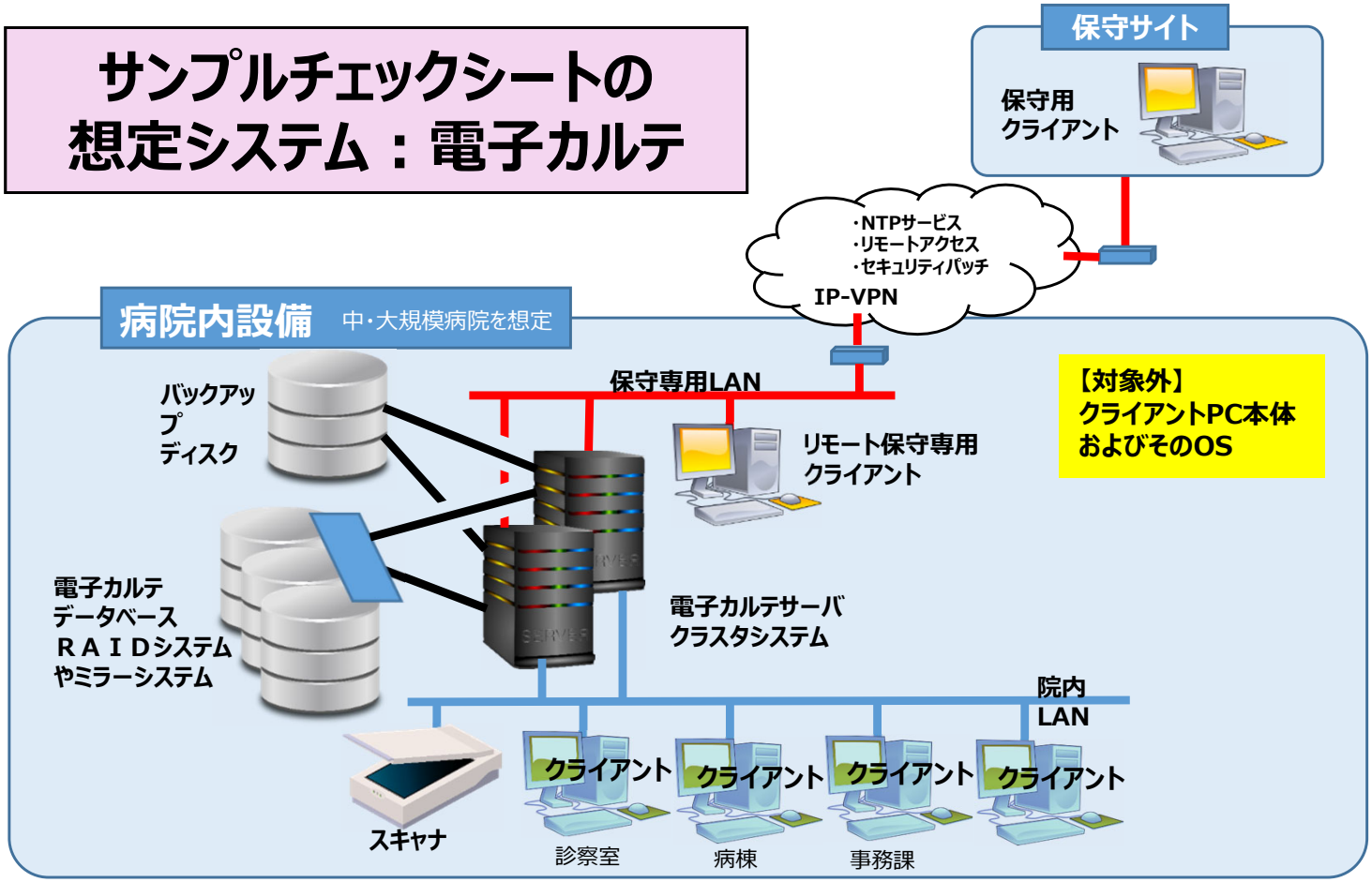
利活用例：
・医療情報システムベンダー各社のリモート保守のリスクアセスメントに活用
・オンライン資格確認のリスクアセスメントのベースに本ガイドラインを活用
・電子処方箋のリスクアセスメントのベースに本ガイドラインを活用
・電子カルテ共有サービスのリスクアセスメントのベースに本ガイドラインを活用
・消防庁の救急隊の患者情報閲覧サービスのリスクアセスメントのベースに本ガイドラインを活用
・ISO/TS11633-1：2019、ISO/TR11633-2:2021として2分冊されてISO規格化

サンプルモデルに対応したSLA例とSDS例の作成

リモート保守サービスの適正化に向けたリモート保守サービサ支援活動として、標準的なサービスモデルに基づくSLA例ならびに当該SLAに基づくSDS例を作成し、各社のリモート保守サービス設計を支援する活動を行っている。

（ SLA: Service Level Agreement SDS: Servicer Disclosure Statement ）

サンプルチェックシートの想定システム：電子カルテ



リモート保守のサンプルモデルではMDSで用いられた電子カルテシステムに対するリモート保守を行うサービスを前提にSLAとSDSが作成されており、MDSと整合を取ることで会員各社の理解を促進するようにしている。

リモート保守サンプルモデルに対応したSLA

リモート保守サービスのサンプルSLA作成に当たっては業界において比較的一般的と考えられるサービス条件を設定し、その条件を踏まえたうえで、総務省・経済産業省の「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」別紙1のSLA参考例をベースとして作成している。

SLA参考例項目と考え方	SLA参考例記載	RSS SLA sample 記載案	解説
6．6 サポート			
【本項を定める上での考え方】 ・本項では、サポート内容を明示する。 ・対象事業者は、一般に利用者からの問合せに対する問合せ受付を用意する。その際、どの範囲の内容を受け付けるのかをあらかじめ合意する必要がある。 ・クラウドサービスの利用では、その前提として利用者側のOSやネットワークに関する設定、Webブラウザ等の設定等が正しくなされていることが求められる。一方で利用者によっては、OSやブラウザの利用方法自体に精通していない場合も多く想定される。 ・サポートセンターの受付内容として、利用者の幅広い問い合わせを受け付ける場合には、一般的にはそのための人員や受付時間のための負担が多くなり、サービスコストの上昇が余儀なくされる。そのため、受付内容の範囲を明確にし、利用者の利便性とサービスコストとのバランスを図ることが求められる。 ・本例で示した報告項目は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、追記することが想定される。また受付方法や応答時間との関係で、受付内容の範囲を区分することも想定される（急を要しない内容については受付内容の範囲を広くする等）。	(1) 利用者に対するサポート ① サポート内容 本サービスの利用に関し、乙は、甲から下記の問い合わせを受け付け、サポート対応をする。 ・本サービスで提供するアプリケーションの使用方法等に関する内容 ・本サービスの利用環境及びその設定に関する確認（OS、Webブラウザ等。ただし、以下は含まない。本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等、乙が管理しないパソコンの機器の使用方法等に関する内容） ・本サービスの利用上の障害に関する内容 ・本サービスの利用に起因する甲のシステムの障害に関する内容	(1) 利用者に対するサポート ① サポート内容 本サービスの利用に関し、乙は、甲から下記の問い合わせを受け付け、サポート対応をする。 1．医療機関が障害等の一次切り分けの支援を実施する際に、リモート保守ベンダに対しSaaSサービスの状況等これに必要な情報を提供する 2．本サービスの利用上の障害に関する内容 3．本サービスの利用に起因する甲のシステムの障害に関する内容	1．医療機関の一次切り分け支援 2．リモート保守サービス自体の障害 3．リモート保守サービスに起因する保守対象機器の障害（マルウェア感染等）に対するサポート を指します。
【本項を定める上での考え方】 ・本項では、サポート対応時間等を明示する。なお、「I.参考例編（サービス仕様適合開示書）」では、問合せ対応について（2）⑭で示している。 ・サポート対応時間は、通常電話によるものが想定されるが、例えば、時間外や、急を要しない照会内容等は、メールによる受付を行う対象事業者もある。このような場合には、本項で問合せ用のWebページ等を併せて明示する。	② サポート対応時間 本サービス提供に関し、乙は、甲からの問い合わせを受けるため、下記において受付対応を行う。 【乙サポートセンター】 連絡先 （受付対応時間、曜日）	② サポート対応時間 本サービス提供に関し、乙は、甲からの問い合わせを受けるため、下記において受付対応を行う。 【連絡先】（連絡先を記入） 【平日】 9:00～17:00 【土曜日・日曜・祝日】 提供なし	

SLA参考例の項目と考え方、SLA参考例の具体的記載内容、リモート保守のSLAサンプルを並べて記載。必要に応じて解説の追記を実施し、会員各社のサービスにカスタマイズしやすいように配慮している。

リモート保守サンプルモデルに対応したSDS

リモート保守サービスのサンプルSLAに基づきそれと合致するサンプルSDSを提供することで会員各社のSDS作成をより円滑に行えるよう支援している。

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5.1版対応）							回答欄	
作 成 日	2023年2月8日						2023/2/8	
サービス事業者	リモートメンテナンス株式会社（仮称）						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						電子カルテシステムリモート保守サービス	
バージョン	1.0						1.0	
※本開示書の適合性をJAHIS/JIRAが証明するものではありません。							プルダウン選択（はい/いいえ/対象外）	備考番号の入力(数字)（なし="-"）
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？(8.1.2)	はい	**いいえ**	対象外	備考	-		2. いいえ	-
本質問の回答が「はい」の場合は、従属質問のいずれかを「はい」としてください。保存場所が複数「はい」の場合は、それぞれ個別のチェックリストを作成してください。								
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？(8.1.2.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？(8.1.2.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提示してあるか？(6.2.C1)	**はい**	いいえ	対象外	備考	-		1. はい	-
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	-		1. はい	-
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	-		1. はい	-
5 個人情報が参照可能な場所においては、入退管理を定めているか？(6.3.C2)	**はい**	いいえ	対象外	備考	-		1. はい	-
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	-		1. はい	-
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	-		1. はい	-

注：現行のサンプルSDSは5.1版対応となっているが、JAHIS標準の改定に合わせて最新版に対応するようアップデートしていく予定である。

リスクアセスメント支援

- 厚生労働省医政局、基金、アクセンチュアに協力して救急時の患者情報閲覧や電子カルテ情報共有サービスのリスクアセスメントに対する支援を実施
- 消防庁、アクセンチュアによる救急隊の患者情報閲覧のリスクアセスメントに対する支援を実施

リモートサービスセキュリティガイドラインのリスクアセスメントを踏襲し、同様のアプローチを行うことでISO/IEC27001 の情報セキュリティマネジメントの考え方を適用

↓

基金によるオンライン資格確認、電子処方箋等の各種サービスはリモートサービスとしてリスクアセスメントが可能なことを受けリスクアセスメント支援を実施

↓

継続的な協力関係のもとで今年度も上記対応を実施

リスクアセスメントの実践

リモートサービスセキュリティガイドラインの付属書Aの内容を基にサイトごとの資産分類を実施（サイトAはリモートサービスセンターだが、この部分を基金のセンターに読み替え）

表 A-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 A-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

リスクアセスメントの実践

以下のリスク評価表に基づいてリスク評価を実施

表 A-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

リスクアセスメントの実践

リスクアセスメント結果をISO27002に準拠する形で展開

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、アクセスさ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）収納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）収納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,なつ追に繋がる	3	3	1	9	—	（管理策）守秘義務は、（機能）操作者の不正行為を牽制するので、（効果）医師等の盗用,差換えを抑制できるが、これだけでは効果が薄い。
						52	E1	a	外部経路RSC側担当	（脆弱性）外部経路からのRSCサービスマンによる保守対象機器内PHIの盗用Cが行われると、（脅威）暴露Cに繋がる	3→2	3	1	9→6	—	（管理策）守秘義務や身元調査（資質の確認）は、（機能）操作者の不正行為を牽制したり予防するので、（効果）RSCサービスマンの盗用を抑制できる。
									内部経路	（脆弱性）内部経路からの医師等,HCFシステム管理者,一次サービスマンによる保守対象機器内PHIの盗用C,差換えIが行われると、（脅威）暴露C,なつ追に	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,なつ追に繋がる	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）収納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）収納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、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元比次の一部として、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,なつ追に繋がる	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。

健康で豊かな国民生活を保健医療福祉情報システムが支えます

ご清聴ありがとうございました