医療情報システム安全管理ガイドライン6.0に基づくサイバーセキュリティを重視したシステム保守契約書作成の要点解説

日本医療情報学会
研修企画委員会

福井大学　山下芳範

福井大学
University of Fukui

なぜ契約書？？？

即時対応できない場合や事後対応の保険
対応担当者がいない場合の逃げ道

医療系でのセキュリティ問題

- ウイルス感染が広がって端末が利用不能
- ウイルスによる内部サーバへの攻撃
- 電子カルテのデータが乗っ取られた
  - ファイルの暗号化ロックによる使用不能
  - 身代金の要求
  - バックアップも使用不能・戻せない
- 部門システムのデータが乗っ取られた

セキュリティ問題の背景

- リモートメンテナンス等外部接続の増加
  - バックドア問題
- 医療情報システムと外部との関わりの拡大
- クローズドなネットワークが安全とは言い切れない現実
- 意図しない状況からのサイバー攻撃の可能性

法令改定によって
医療機関に求められている
情報収集

弱点の把握とリスクの認識

・医療機関のチェックシートの作成
・ベンダー（事業者）のチェックシートの収集
・ベンダー（事業者）からのシステムのMDS/SDSの収集

端末や機器のリスト化

機器の把握も
求められる

筐体名	申請者	OS	支払区分	機器名	MACアドレス	IP アドレス	登録情報コンセント番号	初
fhej0002	山下 芳範	Windows 11	病院負担	MS surface	00:d4:9e:3c:3f:d9	172.30.101.4		202
fhej2004	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:73	172.30.103.4		202
fhej2005	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:14	172.30.103.5		202
fhej2006	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:39:62	172.30.103.6		202
fhej2007	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:0f	172.30.103.7		202
fhej2008	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:25:99:96	172.30.103.8		202
fhej2009	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:39:21	172.30.103.9		202
fhej2010	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:08:66	172.30.103.10		202
fhej2011	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:0d:7a	172.30.103.11		202
fhej2012	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:78:e6	172.30.103.12		202
fhej2013	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:38:ef	172.30.103.13		202
fhej2014	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:32:e1	172.30.103.14		202
fhej2015	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:1e	172.30.103.15		202
fhej2016	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:66:1c	172.30.103.16		202

病院内機器の把握
ネットワーク上のリスク把握

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

医療機関確認用

	チェック項目	確認結果（日付）
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）		
		１回目	目標日	２回目
1 体制構築	（1）　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（1）　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（2）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（3）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	サーバについて、以下を実施している。			
	（4）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（5）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（6）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	ネットワーク機器について、以下を実施している。			
	（7）　セキュリティパッチ（最新ファームウェアや更新プログラムを適用している。	はい・いいえ （　/　）	（　/　）	はい （
	（8）　通制限を実施している。	はい・いいえ （　/　）	（　/　）	はい （
3 インシデント発生に備えた対応	（　ンシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）		

● 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。
● 立入検査の際には、必要な事項が記入されているかを確認します。

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

医療機関確認用

○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）		
		１回目	目標日	２回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	（7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（9）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	端末 PC について、以下を実施している。			
	（4）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（5）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
	（9）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）
3 インシデント発生に備えた対応	（2）　インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ （　/　）	/	はい・いいえ （　/　）
	（3）　サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ （　/　）	）	はい・いいえ （　/　）

● 各項目の考え方や確認方法等については、「医療機
け～」をご覧ください。

医療機関で確認するために
事業者（ベンダー）からも収集

ログが取れているか？

セキュリティパッチは
ベンダーに確認

気になる部分

～立入検査時、チェックリストを確認します～

医療法に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

令和 5 年度は、「医療機関確認用」、「事業者確認用」の全ての項目について、１回目の確認の日付と回答等が記入されていることを確認します（※）。このうち、３（１）の連絡体制図は現物を確認しますので、立入検査までに作成してください。

参考項目は令和５年度の立入検査では確認しません。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関は事業者からチェックリストを回収しておきましょう。

（※） 事業者と契約していない場合には、「医療機関確認用」２（２）及び２（３）についての確認は求められません。

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*１回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）		
		１回目	目標日	２回目
1 体制構築	（１）　医療情報システム安全管理責任者を設置している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	医療情報システム全般について、以下を実施している。			
	（１）　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（２）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（３）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	サーバについて、以下を実施している。			
	（４）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（５）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（　/　）	（　/　）	はい・いいえ
	（６）　アクセスログを管理している。	はい・いいえ（　/　）	（　/　）	
	ネットワーク機器について、以下を実施している。			
	（７）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	（　/　）
	（８）　接続元制限を実施している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
3 インシデント発生に備えた対応	（１）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（　/　）		

MDS/SDSの備考欄に記載して明示してもらいたい項目

連絡先一覧の作成

「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」とは

- 各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）をJAHIS/JIRA で定めた物です
  - 製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、以下の用途に用いられることを想定しています
    - （1）製造業者が提供する医療情報システム、又はサービス事業者が提供する医療情報システムを用いたサービス（以下、「対象とするシステム/サービス」とする。）のセキュリティに関して、厚生労働省から発行されている「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、「安全管理ガイドライン」）への適合性を示すことにより、医療機関等側において必要な対策の理解を容易にすること。
    - （2）安全管理ガイドラインを遵守しなければならない医療機関等にとって有用な情報を提供すること。当該システム/サービス導入医療機関等においてセキュリティマネジメントを実施するにあたって、製造業者/サービス事業者により提供される情報がリスクアセスメントの材料となること。
    - （3）各製造業者/サービス事業者にとって、安全管理ガイドラインへの適合性への自己評価手段として利用すること。
    - （4）医療機関等が製造業者/サービス事業者にセキュリティの説明を求める際の、要求のベースとして利用すること。

「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」

Ver.4.1

医療機関等向けユーザーズガイド

（「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）

2023年9月

JAHIS -JIRA 合同開示説明書 WG

目次

「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」（MDS/SDS）の入手と利用

医療機関等は製造業者/サービス事業者に対し、対象とするシステム（医療機器を含む）/サービス毎にMDS/SDS を要求し入手してください。なお、オンプレミスのシステムでリモートメンテナンスを受けている場合は、SDS を要求し入手してください。対象とするシステム/サービスの MDS/SDS が未作成の場合は、作成するよう要求してください。

医療機関等は「安全管理ガイドライン」の遵守が求められており、医療機関等全体としては医療機関等が主体となって、医療情報システムの製造業者/サービス事業者の協力を受けつつ、安全管理ガイドラインに則って機密性・完全性・可用性を確保するために対象とするシステム/サービスの安全管理を行う必要があります。

一方、医療機器に関しては、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（以下、薬機法という。）における製造販売業者が厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」に則ってサイバーセキュリティの確保を行う必要があります。

さらに、医療法施行規則の改正により、病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならないとされました。

このように医療機関等は対象とするシステム/サービスのリスクアセスメントを行うことが必要となります。MDS/SDS はリスクアセスメントを行う際に利用でき、安全管理ガイドラインに対する準拠性が確認できます。対象とするシステム/サービスの情報セキュリティに関する情報を入手することによって、効果的にリスクアセスメントを実施し、有効な技術的対策や運用的対策を立てることができます。

「製造業者による医療情報セキュリティ開示書」チェックリスト

(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)

製造業者　：	作成日　：			
製品名称　：	バージョン　：			
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の実践(6.2)				
1　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＿＿
物理的安全対策(6.4)				
2　個人情報が入力・参照できる端末の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＿＿
技術的安全対策(6.5)				
3　離席時の不正入力防止の機能があるか？(6.5.C4)	はい	いいえ	対象外	備考＿＿
4　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＿＿
4．1　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＿＿
・上記のうちの二要素を組み合わせた認証	はい	いいえ	対象外	備考＿＿
（具体的な組み合わせを備考に記入してください）				
・その他（具体的な認証方式を備考に記入してください）	はい	いいえ	対象外	備考＿＿
4．1．1　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)	はい	いいえ	対象外	備考＿＿
4．1．2　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	対象外	備考＿＿
4．2　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＿＿
4．3　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＿＿
4．3．1　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

別途対応可能なら備考が欲しい

要チェック

実際の提出書類から

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

事業者確認用

○　令和５年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考
1 体制構築	（1） 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	（3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	（6） アクセスログを管理している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	
	（8） 接続元制限を実施している。	はい （ 8 / 2 ）	（ / ）	はい・いいえ （ / ）	

事業者名：

● 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。

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

事業者用

○令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）		
		１回目	再確認	２回目
1 体制構築	（1） 事業者内に、医療情報システム等の取扱に係る管理責任者を設置している。	いいえ（9/20）	（3/31）	はい・いいえ（/）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい（9/20）	（/）	はい・いいえ（/）
	（3）－１ 医療機関に責任者による医療情報セキュリティ開示書（MDS）を提出した。	はい（9/20）	（/）	はい・いいえ（/）
	（3）－２ 医療機関にサービス事業者による医療情報セキュリティ開示書（SDS）を提出した。	いいえ（9/20）	（3/31）	はい・いいえ（/）
	サーバについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	－（/）	（/）	はい・いいえ（/）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	－（/）	（/）	はい・いいえ（/）
	（6） アクセスログを管理している。	－（/）	（/）	はい・いいえ（/）
	ネットワーク機器について、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや最新プログラム）を適用している。	－（/）	（/）	はい・いいえ（/）
	（8） 接続元制限を実施している。	－（/）	（/）	はい・いいえ（/）

コメント：（1）につきまして、弊社が医療情報システム・サービス事業者に該当の是非に関して該当する方向で社内で検討中ですので、目標日は3月31日にしました。
（3）につきまして、弊社はMDSの提出が可能ですが、SDSについて、医療情報システム・サービス事業者に該当の是非に関して該当する方向で社内で検討中ですので、目標日は3月31日にしました。
（4）～（8）につきまして、施設ご提供・設定の機器を利用、及び弊社ではリモートメンテナンス用のルーターを設置していませんので「－」としています。

事業者名：[redacted]

未記載がないように

MDS/SDSとの整合も確認

製造業者による医療情報セキュリティ開示書チェックリスト（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7月21日
製造業者	
製品名称	
バージョン	02-12以降

※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。

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の実践(6.2)					
1 扱う情報のリストを医療機関に提示できるか？(6.2.C1)	**はい**	いいえ	対象外	備考	1
物理的安全対策(6.4)					
2 個人情報が入力・参照できる端末の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	
技術的安全対策(6.5)					
3 離席時の不正入力防止の機能があるか？(6.5.C4)	はい	**いいえ**	対象外		
4 アクセス管理の機能があるか？(6.5.C1)	**はい**	いいえ	対象外		
4．1 アクセス管理の認証方式は？(6.5.C1、6.5.C13)					
・記憶（ID・パスワード等）	**はい**	いいえ	対象外		
・生体認証（指紋等）	はい	**いいえ**	対象外		
・物理媒体（ICカード等）	はい	**いいえ**	対象外	備考	
・上記のうちの二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	
・その他（具体的な認証方式を備考に記入してください）	はい	**いいえ**	対象外	備考	
4．1．1 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)	はい	**いいえ**	対象外	備考	3
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	**対象外**	備考	4
4．2 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	
4．3 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	
4．3．1 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
4．3．2 アクセスログへのアクセス制限機能があるか？(6.5.C8)	**はい**	いいえ	対象外	備考	
5 時刻情報の正確性を担保する機能があるか？(6.5.C9)	**はい**	いいえ	対象外	備考	6
6 不正ソフトウェア対策を行っているか？(6.5.C10)	はい	**いいえ**	対象外	備考	
7 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	7
情報及び情報機器の持ち出しについて(6.9)					
8 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.C9)	はい	**いいえ**	対象外	備考	8
9 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	
10 管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？(6.9.C6、6.9.C7)	はい	いいえ	**対象外**	備考	9

できればリストをもらう

多要素が必要なシステムかの確認

災害、サイバー攻撃等の非常時の対応(6.10)					
１１　非常時アカウント又は、非常時機能を持っているか？(6.10.C4)	はい	**いいえ**	対象外	備考	
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)					
１２「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？(6.11)	**該当**	非該当			
１２．１　なりすましの対策（認証）機能を有するか？(6.11.C3)	**はい**	いいえ	対象		
１２．２　データの暗号化が可能か？(6.11.C5)	**はい**	いいえ	対象		
１２．３　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？(6.11.C4)	**はい**	いいえ	対象		
１２．３．１　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？(6.11.C4)	**はい**	いいえ	対象		
１２．３．１．１　対応している通信方式はいずれか？(6.11.C4、6.11.C11)					
・専用線	該当	**非該当**		備考	
・公衆網	**該当**	非該当		備考	12
・IP-VPN	該当	**非該当**		備考	
・IPsec-VPN	該当	**非該当**		備考	
・TLS1.2以上 高セキュリティ型、クライアント認証	該当	**非該当**		備考	
１２．３．２　ネットワークの経路制御・プロトコル制御に関わる機能の適正さ（回り込み対策を含む）を証明できる文書があるか？(6.11.C4、6.11.C10)	はい	**いいえ**	対象外	備考	
１２．４　リモートメンテナンス機能を有するか？(6.11.C7)	**該当**	非該当		備考	
１２．４．１　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機能があるか？(6.11.C8)	**はい**	いいえ	対象外	備考	13

できれば
構成や運用の説
明書類をもらう

その他の欄の活用

- 項目は、ガイドラインの項目の対応のみ

- 脆弱性としての認知ができない
  - 考慮すべきリスクの記載を求める
  - 責任範囲を明確にする

責任分界点

契約内容での確認
例：範囲・非常時

その他・備考欄の例

	備考記載欄
1	ご要求に応じて提出可能です。
2	第三者に対する対策が必要な場合は、市販のそき見防止のフィルム等の利用を検討ください。 また、一定時間操作されない時に、ログアウトする機能が有ります。
3	一定時間操作されない時に、ログアウトする機能が有ります。
4	運用開始時に予め非常用アカウントの作成をお願いします。
5	ユーザID毎にアクセス権限を設定できます
6	データベースへの直接アクセスに関しては、ログが残りません。ただし、一般ユーザーはデータベースへの直接アクセスできないように管理設定しています。
7	ご施設のNTPサーバーへのアクセスが必要になります。
8	弊社推奨のウイルス対策ソフトウェアの導入が可能です。パターンファイルの定期更新作業は、お客様と作業分担の取り決めを行わせていただきます。
9	ご施設の方でソフトウェアのインストールは絶対に行わないで下さい。
10	リモートメンテナンス時のなりすまし対策は、生体認証（静脈認証）になります。
11	データベース・ファイルサーバーのHDD冗長化及びバックアップを行います。（オプション）
12	ユーザーによるアクセスはできないので、サービスにご相談ください。
13	

オプションや別運用が必要なものに注意
これらの責任は？？
契約？？

その他･備考欄の例

	備考記載欄
1	基本仕様書（患者情報、検査情報他）、システム概念図（機器構成）、ネットワーク構成図（IPアドレス）を、
2	利用者ID/パスワードによるログイン機能を有しております。
3	ID/パスワードの登録に関する管理機能は有していますが、パスワードの「強度」を管理する機能は有しておりません。 なお、HIS等基幹システムとの連携、シングルサインオン(SSO)での連携などの場合、上位システムの管理に依存します。
4	セキュリティデバイスによる認証には対応していません。
5	アクセスログは、管理者が、サーバ上で確認できます。
6	病院指定のntpサーバ、もしくは弊社メインサーバとの時刻同期機能を有しております。
7	無線LAN環境を提供しておりません。
8	病院ポリシーに沿って、資産管理ソフトウェアを導入する場合は、別途検証の上、インストールの可否を判断させて
9	管理区域外（施設外）で運用はできません。
10	リモートメンテナンス機能のみ提供しております。 病院で用意される保守用ネットワーク回線を利用する場合は、病院ポリシーに従います。 リモートメンテナンス作業においてISMS管理下のもと作業を行っております。
11	弊社提供のリモートメンテナンスでは、暗号化可能なアプリケーションを使用しています。
12	弊社提供のリモートメンテナンスでは、NTTフレッツ光データコネクト回線を標準としています。
13	弊社提供のリモートメンテナンスでは、リモート接続時、発信元電話番号＋事前共有キー＋ID/PWにて接続認証を行っております。

導入システムでの状態が不明

実際の運用が不明
メンテ契約に入っている

医療情報部門・医療情報担当者が担うべきセキュリティ対応

- チェックシートだけで大丈夫か？
- MDS/SDSをもらうだけで大丈夫？

- セキュリティの本質的対応が必要
- 経営層も含めて重要インフラとしての対応を考える必要あり

契約内容も

福井大学
University of Fukui

すべき対応とは

- GL6にある項目
  - リスク評価とマネジメント
    - 脆弱性などの把握・報告　→　MDS/SDS、チェックリスト
  - 異常事象発生時の対応
    - システムのログの扱い
    - 事故発生時の報告・原因究明・対策
  - 事業者からの情報提供
    - 経時的に発生するリスク
  - 非常時体制とリカバリ方法の確立

契約書とあるが・・・

- 契約書が必須ではない
  - 後付けの文章（覚書や誓約書など）も可能
- 契約先との間での明文化が重要
- 特に責任分界点の明確化を考えることと、非常時の対応を想定する

責任分界点

- GL6　経営管理編

5．3　責任分界管理

【遵守事項】

① システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。

契約書
仕様書
覚書　など

現状ではほとんど明記されていないので
今後の契約などでは考慮すべき点！！

責任分界点

- GL6　企画管理編

2．責任分界

【遵守事項】

① 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。

② 取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。

③ 責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。

④ 委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。

⑤ 委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、関与する関係者への管理なども責任分界の取決めに含めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。

⑥ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。

責任分界点

- GL6　システム運用編

３．３．２　非常時の運用における責任分界

非常時の運用における責任分界は、技術的な対応という点で見ると主に、被害の拡大防止や原因究明などシステム対応に関する内容のほか、外部への説明責任に関する支援などについて、取り決めることが求められる。

被害拡大防止や原因究明などに関しては、医療機関等側で把握できる運用に関する情報と、委託先である事業者が管理するシステム運用上のデータ等の資料などを併せて検討することが求められるため、それぞれの役割の分担などを取り決めておくことが求められる。

特にサイバー攻撃による被害を受けた場合には、原因究明に際して専門的な知見が必要となり、この場合の責任分担などは非常に重要である。

外部への説明責任についても、事業者でしか、技術的にもわからない部分が存在することがあるため、専門的な観点から適切な資料の準備と提供に関する内容も含めた、責任分担を行うことが求められる。

インシデント発生時

- GL6　経営管理編

1．2．2　非常時における責任

【遵守事項】

＜説明責任＞

① 情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。

＜善後策を講ずる責任＞

① 情報セキュリティインシデントが生じた場合、医療機関等内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。

② 情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。

③ ①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。

（2）善後策を講ずる責任

医療機関等が果たすべき善後策を講ずる責任の中には、「情報セキュリティインシデントの原因を究明する責任」、「再発防止策を講ずる責任」がある。

医療情報システム・サービスを委託している場合には、情報セキュリティインシデントの原因が直ちに判明しない場合が想定されることから、医療機関等と委託先事業者とで協力して対応する必要があり、これらの責任分界についても医療機関等と委託先事業者とであらかじめ取り決めておく必要がある。具体的には、情報セキュリティインシデント発生後から収束に至るまでの期間の対応における分担や協力の内容に関して、あらかじめ委託先事業者と取り決めておくことで、的確かつ迅速な原因究明が可能となるとともに、究明された原因に応じた再発防止策を講じる際の分担や協力についても取り決めておくことで、情報セキュリティインシデントの発生後、システム関連事業者への医療情報システム・サービスの委託を継続する場合に、再発防止策を含むインシデントを踏まえた委託内容の更新を的確かつ迅速に行うことが可能となる。

以上のとおり、企画管理者はこれらの責任を適切に果たすことができるよう、システム関連事業者との間での役割分担を含む責任分界を定める必要がある。

リスク評価

- GL6　企画管理編

２．１．４　リスク分析を踏まえた要求仕様適合性の確認への対応

医療機関等とシステム関連事業者との間で、役割分担、当該事業者が受容したリスクの内容等について合意形成を図るため、医療情報システムについて、医療機関等におけるリスクアセスメントを踏まえた医療機関等の要求仕様への適合性を確認する必要がある。

医療機関等によるリスクアセスメントの結果、一部のリスクを委託先事業者で負うことになることが想定される。その際に、委託先事業者が想定していたリスクの内容とリスクアセスメントを踏まえたリスクの内容に不一致があると、医療機関等におけるリスク管理が適切にできないことになる。そこで、医療機関等が責任分界を定めるに際しては、その前提としてそれぞれが負うことが想定されるリスクの内容について、合意を得るための調整を行うことになる。

実際には、システム関連事業者が提供する情報やサービス仕様適合開示書等の内容を踏まえて、遵守している対策項目等の状況が医療機関等で求める内容と乖離があるかどうかを把握し、乖離がある場合にはその部分についてどのように対応するのかを両者で協議し、合意した上で、医療情報システム・サービスの提供を受けることが想定される。

企画管理者は、このような要求仕様適合性の調整・確認に必要な情報をシステム関連事業者から収集し、必要な調整を行った上で、責任分界に関する取決めを行うことが求められる。

リスク評価

- GL6　システム運用編

4．リスクアセスメントを踏まえた安全管理対策の設計　　[Ⅰ～Ⅳ]

【遵守事項】

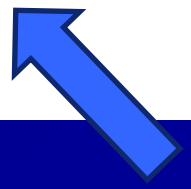
① 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。

② 事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「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」を利用することが考えられる。

4．2　リスクアセスメントを踏まえた安全管理対策の設計

システム運用担当者は、医療機関等が保有する医療情報等の情報種別や重要度を整理したうえで、リスクアセスメント（リスク分析、リスク評価）を企画管理者と行い、その結果を踏まえて、具体的な安全管理のための技術的な対応について、実装し、運用することになる。

医療情報システムの安全管理のための対策を、リスクアセスメント結果を踏まえて講じる場合には、医療機関等ごとの組織や規模等の実情や、医療情報システムの利用形態等のリスクに応じて、さまざま方法が挙げられる。また実装の検討に際しては、医療機関等における対応できる負担（要員、費用等）などを踏まえることも求められる。



CVEとCVSSスコア

- CVE
  - ベンダー依存しないセキュリティ報告
  - 共通化

- CVSSスコア
  - 統一した危険度の評価
    - 共通脆弱性評価システム

深刻度	CVSS v3基本値
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

ID	タイトル	CVSSv3	CVSSv2	公表日
JVNDB-2023-007400	マイクロソフトの複数の Microsoft 製品 におけるサービス運用妨害 (DoS) の脆弱性	7.5	-	2023/11/
JVNDB-2023-007153 (JVNVU#94195279)	Hitachi Energy 製 MACH System Software における複数の脆弱性	6.5	-	2023/11/
JVNDB-2023-007152 (JVNVU#98954968)	CLUSTERPRO X における複数の脆弱性	8.8	-	2023/11/
JVNDB-2023-000117 (JVN#15005948)	LuxCal Web Calendar における複数の脆弱性	7.3	7.5	2023/11/
JVNDB-2023-007150 (JVNVU#99077347)	ファースト製 DVR における複数の脆弱性	9.8	-	2023/11/
JVNDB-2023-007044 (JVNVU#98585341)	Apache ActiveMQ にリモートコード実行の脆弱性	9.8	-	2023/11/
JVNDB-2023-000118 (JVN#22220399)	CubeCart における複数の脆弱性	9.1	6.5	2023/11/
JVNDB-2023-000116 (JVN#13618065)	Redmine におけるクロスサイトスクリプティングの脆弱性	6.1	4.3	2023/11/
JVNDB-2023-000114 (JVN#17806703)	Cisco Firepower Management Center Software における複数の脆弱性	7.2	7.1	2023/11/
JVNDB-2023-006588 (JVNVU#94119876)	エレコム製およびロジテック製ルーターにおける複数の脆弱性	6.8	-	2023/11/
JVNDB-2023-006578 (JVNVU#96079387)	ASUSTeK COMPUTER 製 RT-AC87U における不適切なアクセス制御の脆弱性	6.5	-	2023/11/

取り決め例

- CVSSスコア7以上は、報告を行い、対応は協議による。
- CVSSスコア９以上は、緊急の通知を行うとともに、対応策を提示し、実施方法を検討する。

脆弱性診断の基本

- システム基本的な問題がないかの確認
  - 期待している動作だけでなく、予期しないトラフィックでの問題の有無
  - 設計通りの通信の状態の確認
- 意図しない（利用しない）出入口の有無
- OSとしての安全性確認
  - パッチの適用状態
- アプリケーションの安全性確認
  - 不要サービスなどの有無
  - 異常通信時の対応状況
  - アクセス権の妥当性

ペネトレーション・テスト

- 現実的なサイバー攻撃での耐性試験
  - 既知の脆弱性を検出するための特徴的なパターンでの疑似攻撃
  - 既知の侵入パターンによる不正侵入の試行
  - 既知の攻撃パターンによるサービス妨害の試行
  - 外部からのコマンド実行、情報操作、データ取得の試行
  - Web系の弱点への総攻撃

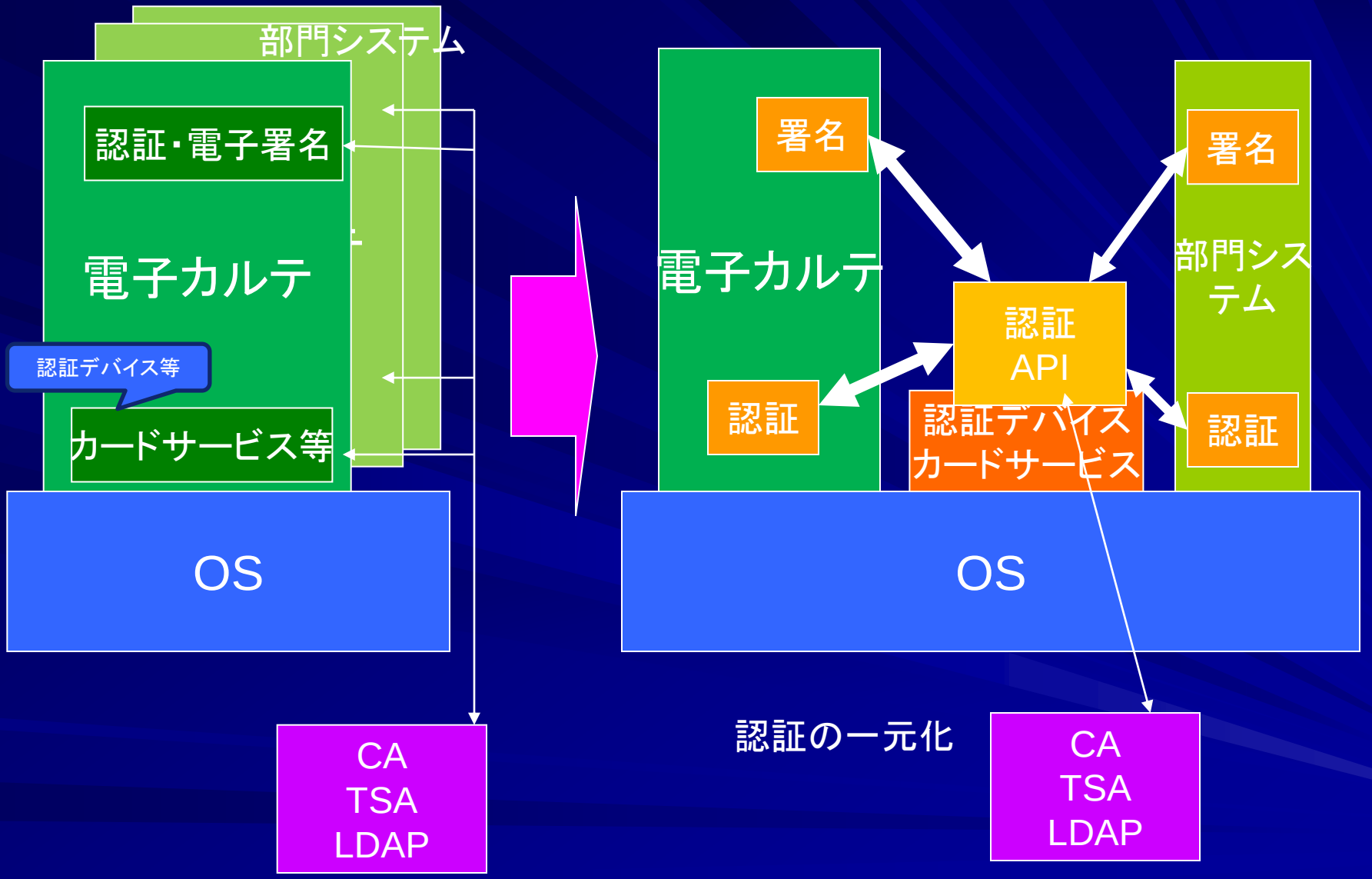
導入時評価としては有効
でもOSやアプリの脆弱性があるので継続的にも必要

契約前の技術仕様でも考慮

- 導入前のセキュリティ開示情報
- 導入前セキュリティ診断と継続性・有効期間
  - 導入前のペネトレーションテストする？？？
- セキュリティ対応のためのupdate対応
  - とはいえOS・アプリの有効期限がある
- システムの有効期限やライフサイクルの担保

- セキュリティ担保の費用の明確化

認証のアプローチ例



電子カルテ上のA先生と部門システム上のA先生は本当に同じ人
なりすまして記録ができないか？

契約だけがすべてではない

- 院内におけるセキュリティのリスクを考える
  - ベンダー側の情報提供が重要！！
- どうしても、リスク評価は100%とはならない
  - 考えうる対策はするが、「お守り」という認識で
  - 継続的な情報提供をどうするか？
- 何かが起こる前提で考える
  - 起こった時の対応を考慮する
  - そのためにも、弱点を知ることが重要
    - 継続的なフォローも必要となる
  - 万一の時の対応手段を考慮する