

令和 6 年度 医療機関における サイバーセキュリティ確保事業 ～取り組み事例集～

2025年 3 月

厚生労働省医政局医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

- I. はじめに
 - 1. 本書の目的
 - 2. 事例調査方法について

- II. 取り組み事例紹介
 - 1. 取り組み事例の全体像
 - 2. 医療機関ごとの取り組み事例

I .はじめに

ひと、くらし、みらいのために



厚生労働省
Ministry of Health, Labour and Welfare

本書の目的

この度は、外部接続回線の一覧化及び現地での調査、脆弱性診断など、ご協力ありがとうございました。

本書は、今後のサイバー攻撃への備えとして、医療機関様自らが継続して外部接続回線やネットワーク

機器の管理・運用、並びに脆弱性対策が実施できることを目的として、他の医療機関の取り組みを事例集として作成しております。

貴院のサイバー攻撃対策等の参考にして頂ければ幸いです。

※なお、必ず貴院にマッチするものではありません。

参考にして頂き、最適な対策を継続頂くようお願いします。

事例調査方法について

区分	概要	備考
調査時期	2025年1月～2月中旬	
調査方法	インタビュー形式（対面、またはオンライン）	
対象医療機関	可能な範囲で八地方区分／病床数の規模等で偏りのないように選定し、承諾を頂いた28の医療機関で実施 ・ 400床以上 : 5件 ・ 200床～400床未満 : 11件 ・ 400床未満 : 12件	関東（10）、近畿（7）、九州・沖縄（1）、中国・四国（1）、東海（5）、東北（2）、北海道（2）
インタビュー内容	1. 医療情報システムに関する全体管理 医療情報システム全体の情報を把握・管理するにあたってのルールや規定 情報システム部門の体制 2. 情報機器や端末、その他情報資産の整備・維持管理 情報機器や回線情報、機器の情報など管理の方法 ネットワーク機器や、システムで利用する端末PCのセキュリティ対策状況 3. 保守契約、サービス利用契約における責任分界点、SLA整備 システム委託やサービス利用における技術的な対応の責任分界点の状況 保守契約やSLA（仕様）等による定期的な更新や確認の状況（故障対応以外）	

Ⅱ. 取り組み事例紹介

ひと、暮らし、みらいのために



厚生労働省
Ministry of Health, Labour and Welfare

取り組み事例の全体像 1/2

No	区分	事例の概要	参照事例
1	医療情報システムに関する 全体管理	システムや回線を一元化し管理対象を最小化	取り組み事例①
		電子カルテ委員会(月1回)を通じ、部門毎のシステム導入情報が共有できる体制を構築	取り組み事例①
		情シス内の情報がデータで共有されるよう、会話も含めてドキュメント化するルールを構築	取り組み事例②
		法人本部でガイドラインに準じた統一の規定・ルールを整備し各病院が規定に沿って運営	取り組み事例③
		外部リソース(委託など)を活用したヘルプデスク運営(常勤SE)に変更	取り組み事例③
		電子カルテ委員会や、兼務者を中心とした他部門との連携強化	取り組み事例⑤
		電子カルテ以外の部門システムも取扱いが可能なベンダーに集約	取り組み事例⑤
		医療情報システム系、事務系に区分してそれぞれのセキュリティ対策、保守・運用を規定	取り組み事例⑥
		システムベンダー、ネットワークベンダーの委託を区分しそれぞれの管理対象を最小化	取り組み事例⑦

取り組み事例の全体像 2/2

No	区分	事例の概要	参照事例
2	情報機器や端末、 その他情報資産の整備・管理	システムや機器の導入前に各部門から情報共有をしてもらうことをルール化	取り組み事例②
		情報資産管理だけでなく、端末などの情報機器を制御する仕組みを導入	取り組み事例③
		院内のLAN配線図(CAD)と紐づけた資産管理台帳の作成	取り組み事例④
		端末変更時などの管理台帳の更新と、端末の更新、制御をルール化	取り組み事例④
		ベンダーによる機器の一元管理と、事業者サービスを利用した外部接続機器の維持管理	取り組み事例⑦
3	保守契約、サービス利用契約 における 責任分界点、SLA整備	医療情報システム全体を設計し、長期的な導入・運用計画を策定	取り組み事例①
		システム毎に敷設された回線や機器を可能な限り一元化するため、保守専用の接続点を構築	取り組み事例②
		保守用のリモート接続には、指定のネットワークとソフトウェアを利用することを条件化	取り組み事例④
		リモートアクセスの事前登録、申請書提出を義務化し情シスによる作業内容のチェック	取り組み事例⑥

医療機関ごとの取り組み事例①

医療機関種別	急性期／回復期 200～400床未満(290床)	情シス体制	職員：5名体制 (全員常勤)	事例掲載 区分	☒ 医療情報システムに関する全体管理
キーワード	システムや院内ネットワーク・回線数の集約、ベンダーの一元化、 電子カルテの更改タイミング				☐ 情報機器や端末、その他情報資産の整備・管理
					☒ 保守契約、サービス利用契約の責任分界点、SLA整備

区分	医療情報システムに関する全体管理		医療情報システムに関する全体管理	保守契約、サービス利用契約の責任分界点、SLA整備
課題	①情シスでシステムや機器、回線、保守契約などの情報を把握できていない Before システム・回線が多数存在 After 可能な限り仮想化サーバ上へシステム集約し回線も一元化		② 部門独自でシステム導入・管理を実施 Before 部門ごとに独自にシステム導入 After 電子カルテ委員会を通じて情シス経由で導入	②医療情報システム全体の導入方針に一貫性がない Before 保守の取り決めや責任分解点が不明確 After ベンダー管理(導入・保守)が可能な病院のルールを策定
取り組み内容	システムや機器、回線を一元化し管理対象を最小化した		電子カルテ委員会(月1回)を通じ、部門毎のシステム導入情報が共有できる体制を構築した	法人全体の医療情報システム全体を設計し、長期的な導入・運用計画を策定、実行した
取り組みの工夫点	- 電子カルテの更改を契機に法人全体で見直し - 電子カルテベンダー選定時にサーバ仮想化による各システムを統合可能なベンダーを選定(可能な限り1社へ集約) - 院内LANも含めたネットワーク統合、保守・運用が実施できるネットワークベンダーを選定		- 新システムの企画・設計を情シスだけではなく、電子カルテ委員会のメンバーの意見を汲んで実施 - 電子カルテ委員会メンバーにITに明るい各部門の医師も加え、部門の意見・情報を集約	- 情シスが、部門から委員会に参画しているリーダーの意見を汲み取り、導入・運用の全体計画を策定 - 電子カルテの更改を契機に計画を実行、部門システムも更改時に統合 長期計画の実現、運用が可能なベンダーを選定
効果(メリット)	- システム最小化に伴うトータルコストの縮小サーバ数55%減、導入コスト40%減(旧システム比) - コミュニケーション対象のベンダー最小化 - 情報システム部の情報資産管理の稼働削減		部門毎の新たなシステムの導入状況の把握が可能となる 部門横断でセキュリティ対策等に関する情報の周知・展開が可能となる - 部門間のコミュニケーションの醸成	- リモート接続も含めたシステムや回線集約の実現 - 医療情報システム全体の把握、管理が可能となる

医療機関ごとの取り組み事例②

医療機関種別	急性期 200～400床未満(382床)	情シス体制	職員:8名(常勤7、非常勤1) 委託:1名常駐	事例掲載 区分	■ 医療情報システムに関する全体管理
キーワード	情シス内の情報のドキュメント化、導入システムの情報把握、 保守専用回線に集約				■ 情報機器や端末、その他情報資産の整備・管理
					■ 保守契約、サービス利用契約の責任分界点、SLA整備

区分	医療情報システムに関する全体管理		情報機器や端末、その他情報資産の整備・管理		保守契約、サービス利用契約の責任分界点、SLA整備
課題	① 情シス担当者毎に保有する情報が属人化 Before 会話のやりとりが多く情報が可視化されていない After 情報のドキュメント化・インデックス化		② 部門独自で導入するシステム情報がわからない Before 部門が独自にシステム導入し、事後に情報が共有される After 導入前に情シスへ共有するルール化		③ システム毎に機器や回線等があり管理対象が多い Before 保守用の機器や回線がシステム毎に存在 After 保守専用の接続点をつくり、アクセスを一元化(可能な範囲で要求)
取り組み内容	情シス内の情報がデータで共有されるよう、会話も含めてドキュメント化するルールをつくった		システムや機器の導入前に各部門より情報共有をしてもらうことをルール化した		システム毎に敷設された回線や機器を一元化するため、保守専用の基盤(接続点)をつくった
取り組みの工夫点	- 情報のドキュメント化と同時に決められた場所への保存、インデックス化による検索しやすい工夫 - 日々の引継ぎの際に漏れがないようにメモもドキュメント化し伝達		- 部門が医療機器を導入する際に情シスに連絡を入れてもらい導入前にベンダーに直接確認 - 情シスがセキュリティ対策状況も含めてルールに適合しているかを確認		複数ベンダーが利用可能な保守専用の基盤を利用する事で管理する回線、機器の数を最小化(医療機器類はリプレース時に変更を検討) - 保守専用の基盤が利用できない場合はベンダーからセキュリティ対策状況を提出してもらい確認
効果(メリット)	- 担当者が不在時でも必要な情報を他メンバーで把握が可能 - メンバーの引継ぎや変更があった際の情報の漏れ防止、効率化		導入システムや保守回線の把握漏れを防ぐ事ができ、セキュリティリスクの把握と対策が可能 - システム導入時のルールに合わせられるベンダーを選定する事で、医療機関がイニシアチブを持った導入、契約ができる		接続点を減らすことによる管理の最小化 病院が決められたセキュリティ設定(ルール)によるアクセスが実現 - 回線やネットワーク機器の管理稼働削減

医療機関ごとの取り組み事例③

医療機関種別	精神科救急・急性期 200～400床未満(274床)	情シス体制	兼務 1名 (外部委託3名常勤)	事例掲載 区分	☒ 医療情報システムに関する全体管理
キーワード	法人本部と病院間の連携、ガイドライン改定、病院の新築タイミング、ヘルプデスク設置、USB紛失のインシデント				☒ 情報機器や端末、その他情報資産の整備・管理
					☐ 保守契約、サービス利用契約の責任分界点、SLA整備

区分	医療情報システムに関する全体管理		医療情報システムに関する全体管理	情報機器や端末、その他情報資産の整備・管理
課題	① 法人内の病院毎のルールで運営し実態が不明 Before 病院毎に独自にルールを決めて運営 After 法人本部でガイドラインに準じた規定を整備して各病院で運営		② 情報システム担当の人材不足(専任者なし) Before システム刷新に伴い人員が削減された After ヘルプデスク運営(外部委託)に切替	③ 院内の機器や回線等の管理対象が多すぎる Before 病院内の端末把握、制御が行えない After 端末管理と端末制御が行える資産管理ツールを導入
取り組み内容	法人本部でガイドラインに準じた規定を整備して統一の規定・ルールで各病院が運営		外部リソースを活用したヘルプデスク運営(常勤SE)に変更	情報資産管理だけでなく、端末などの情報機器を制御する仕組みを導入
取り組みの工夫点	- 法人本部(規定・ルール策定)と病院(ルールに沿った運営)間の役割の明確化(病院新築タイミング) - 病院独自で導入するシステムや回線は病院側で管理するルールとし法人本部で統合して管理 - 事務、医師、看護師の意見も確認して、運用の変更や実態に合わせ、改定を年1回行っている		- 法人内の病院3施設にヘルプデスク(外部委託SE1名)がいて連携して対応(職員は1名が兼務) - ヘルプデスクは院内トラブル時の問い合わせ、一次切り分け、ベンダー対応を一元的に行なっている - IT知識のある医療情報技師を病院に複数名配置	- USB紛失のニュースをきっかけにUSB利用の制限を一元設定できる資産管理ツールを導入 - 制御設定を反映する仕組みが柔軟で、結果が正確に把握できる製品を選定した - 導入が行えない医療機器などは台帳管理し、USB制御は物理的に利用できない対応をしている
効果(メリット)	- 現場の意見も聞き、運用の更新を行うことで、理解されやすい規定・ルールの策定が実現 - 統一の規定・ルール設定により、病院側にとっても運用の範囲が明確になった。		- 法人内の病院を全体で管理する体制の為、病院毎の情報管理面が効率化 - 技術的な業務は外部委託を活用することで、兼務、または少人数でも対応する事が可能	端末制御の設定を一括で行えるため作業効率が格段に向上 - 設定漏れの管理ができ、その他の設定情報も資産管理で収集できるので台帳管理・更新が容易

医療機関ごとの取り組み事例④

医療機関種別	高度急性期／急性期 400床以上(604床)	情シス体制	常勤2名	事例掲載 区分	☐ 医療情報システムに関する全体管理 ☒ 情報機器や端末、その他情報資産の整備・管理 ☒ 保守契約、サービス利用契約の責任分界点、SLA整備
キーワード	電子カルテの導入タイミング、保守用回線の集約、 接続ソフトウェアの指定、病院のインシデント				
区分	保守契約、サービス利用契約の責任分界点、SLA整備			情報機器や端末、その他情報資産の整備・管理	情報機器や端末、その他情報資産の整備・管理
課題	① 院内の機器や回線等の管理対象が多すぎる Before システム・回線が多数存在する After 保守用の回線と接続ソフトを指定して 可能な限り管理対象機器を減らした			② 院内LAN構成と資産管理で情報に差異がある Before LANは施設課管理、台帳は情シス管理 After 施設課の図面と資産台帳を関連付けて 管理	③ 資産管理のルール・規定が明確でなかった Before 端末の定期的な更新、端末の制御などの ルールが明確でない After バージョンアップや禁止事項をルール化
取り組み 内容	保守用の接続には、特定のネットワークと ソフトを利用することを条件化			LAN配線図(CAD)と紐づけた 資産管理台帳の作成	端末変更時などの管理台帳の更新と、 端末の更新、制御をルール化
取り組みの 工夫点	・原則ベンダー毎に回線を引かせずに 病院が用意した回線に指定のソフトウェアで接続 させる ・指定ソフトによる アクセス方式に限定することで、セキュリティを確保 した接続を実現 (全て電子カルテ導入タイミングで実施)			・従来から施設課が利用していたLAN配線図面 (CAD)を活用 ・サーバールーム構築時に LAN配線図面(CAD)と資産管理台帳の紐づけ を実施 (どのHUBのポートがどのようなIPかなども連携)	・端末入替え時の情報連携には、 必要な情報をどこから入手するかをルール化 した ・ベンダーから情報入手しアップデートがある たびに情シスが確認して更新 (医療機器はベンダーが実施) ・電子カルテの端末は、USB接続が出来ないよ うに自動で制限(診療情報の抽出時は許可制)
効果 (メリット)	・回線、機器などの管理対象の集約等、 セキュリティ対策の一元化が実現			・システムの変更時に図面、台帳共に情報の差異 なく更新を行うため適切に院内全体の情報 資産の管理が可能	・ルール化、制限(自動化)によるセキュリティ の確保 ・台帳の更新・見直しの際に、作業が簡便

医療機関ごとの取り組み事例⑤

医療機関種別	回復期／慢性期 200床未満(53床)	情シス体制	職員:4名(常勤・兼務) ※実働2名	事例掲載 区分	■ 医療情報システムに関する全体管理
キーワード	回線数の集約、有スキル人材の有効活用、担当者の兼務、 電子カルテ導入のタイミング				☐ 情報機器や端末、その他情報資産の整備・管理 ☐ 保守契約、サービス利用契約の責任分界点、SLA整備

区分	医療情報システムに関する全体管理		医療情報システムに関する全体管理		
課題	②情シス担当の人員不足や連携不足で情報管理ができていない Before 総務部が兼務で対応 After 電子カルテ委員会や部門兼務者の配置		①情シスでシステムや機器、回線、保守契約などの情報を把握できていない Before システム・回線が多数存在 After ベンダーを集約しシステムや回線を集約		
取り組み内容	電子カルテ委員会や、兼務者を中心とした他部門との連携強化		電子カルテ以外の部門システムも取扱いでき、トータルコストが縮小可能なベンダーに集約		
取り組みの工夫点	- IT知識がある職員を情シス担当に配置(人材の有効活用) - 検査室等と兼務した職員を情シスに配置(部門間連携促進) - 各部門が参加する電子カルテ委員会を通じた定期的な情報連携の仕組みを構築		- ベンダーの集約にあたり、更改時に導入後10年間の費用(システム運用・保守など)も比較して選定 - 他業界で施設の設計、管理の経験を持つ職員が院内のLAN設計を行い、保守も含めてベンダーや回線を集約		
効果(メリット)	- 兼務者から部門の情報が情シスへ入ってくるようになり、状況把握やコミュニケーションがスムーズ - 電子カルテ委員会を通じた定期的な情報交換が可能		- サーバや機器、回線の管理、システム運用コストが最小化(導入後10年間のコスト比較で7500万の差) - 院内人材の経験やスキルの有効活用		

医療機関ごとの取り組み事例⑥

医療機関種別	急性期／慢性期 400床以上(780床)	情シス体制	職員4名(常勤) 2名企画、2名ヘルプデスク	事例掲載 区分	☒ 医療情報システムに関する全体管理
キーワード	ネットワーク別の対策、リモート保守のルール化、リモート作業チェック、事業者サービスの利用				☐ 情報機器や端末、その他情報資産の整備・管理
					☒ 保守契約、サービス利用契約の責任分界点、SLA整備

区分	医療情報システムに関する全体管理		保守契約、サービス利用契約の責任分界点、SLA整備	
課題	①部門毎のシステム導入、保守契約をしており管理やルールが統一できない Before システムや回線の維持・管理が部門ごと After ガイドラインベースにルール化し対策を一元化		②ベンダー毎にリモート保守の仕様に違いがある Before 仕様や責任分界点、セキュリティ対策が不明確 After 医療機関が主導のリモートアクセス管理	
取り組み内容	医療情報システム系、事務系に区分してそれぞれのセキュリティ対策、保守・運用を規定		リモートアクセス事前登録、申請書提出をルール化し情シスによる作業内容のチェック	
取り組みの工夫点	- 事務系はUTM等の自動検知、医療情報システム系はガイドラインベースの規定を中心に区分して対策 - 個別に設置されたルーターは撤去して集約 - 医療情報システムは無許可のUSB利用を禁止(部門で許可なく利用していたUSBを禁止し、許可されたウイルスチェック機能付きUSBを申請し利用) - 情シスが規定順守の職員研修を行い意識付け		- 病院が要求するセキュリティ対策を行っているベンダーのみリモートアクセスIDを払出し(事前説明し理解が得られないにベンダーはリモート接続を許可しない) - 作業(参照/変更)申請の義務化と情シスの確認 - データセンターに設置されたマネージドVPN機器を利用した接続に限定(事業者サービス側でファームウェアをバージョンアップ)	
効果(メリット)	- 許可なく利用される機器、回線がなくなった - 決められたルールによるシステム導入、保守を実現 - ウイルス感染や情報漏洩につながるおそれの形跡がログ上で見受けられない(ログで確認)		- 病院が要求するセキュリティ対策に対するベンダーの理解が深まる - リモートアクセスのセキュリティリスク低減 - 病院と事業者の責任分界点の明確化(外部接続機器のセキュリティ対策は事業者が対応)	