薬局における
サイバーセキュリティ対策
チェックリスト
令和5年度までに
対応しておく内容について

鹿児島県薬剤師会
薬事情報委員会

薬局におけるサイバーセキュリティ対策チェックリスト

薬局確認用

	チェック項目	確認結果（日付）	備考
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。

薬局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
をもとに解説いたします。
令和5年度中に対応すべき内容ですので
まだ対応していない薬局は早急に対応が必要です。

2 医療情報システムの管理・運用	（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）　利用者の属性等に応じた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。				

薬局におけるサイバーセキュリティ対策チェックリストとは

医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「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「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、薬局が優先的に取り組むべき事項をまとめたもの。

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

薬局におけるサイバーセキュリティ対策チェックリスト

薬局確認用

	チェック項目	確認結果 （日付）	備考
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 （　/　）	

本チェックリストが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定します（例：レセコン、電子薬歴システム等）。これには、事業者により提供されるシステムだけでなく、薬局において自ら開発・構築されたシステムが含まれます。
本項目の「いいえ」にマルがつく場合、以下すべての項目は確認不要です。

医療情報を扱っているシステムの確認

医療情報

・・・医療に関する患者情報（個人識別情報）を含む情報

氏名、生年月日、性別など

医療情報を扱う：電子薬歴、レセコン

要確認：自動錠剤分包機、自動散剤分包機、POSレジ

対象外：オンライン資格確認、電子処方箋システム等の国が運営しているシステム

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
概説編

２．３　医療情報システムの範囲

本ガイドラインが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定する。これには、医療情報システム・サービス事業者（※）により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれる。

なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。

（※）本ガイドラインで用いる「医療情報システム・サービス事業者」とは、医療情報システムの製造、開発、販売及び保守を行う事業者や、医療情報システムを活用したサービスの提供、保守等を行う事業者など、医療機関等が医療情報システムを利用・管理する上で関係する事業者全般を想定する。

○　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）			備考
		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等を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

薬局において、医療情報システムの安全管理（企画管理、システム運営）の実務を担う「企画管理者」や医療情報システムの安全管理を直接実行する「医療情報システム安全管理責任者」（以下併せて「システム管理責任者」という。）や、医療情報システムの実装・運用を担う「システム運用担当者」を設置する必要があります。

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
経営管理編

３．１．２　医療情報システムにおける統制上の留意点

【遵守事項】

①　医療機関等の規模や組織構成、特性等を踏まえた統制の内容を検討すること。

②　医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。

③　情報セキュリティ対策に関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。

④　情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。

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
経営管理編

- 医療情報を取り扱う医療情報システムの情報セキュリティを確保するためには、組織全体として適切な統制がなされていることが重要であり、統制の実効性確保に当たっては、医療機関等の規模や組織構成、特性等に応じて留意すべき点が存在する。例えば、小規模の医療機関等や「個人経営」の医療機関等では、担当する業務ごとに区分された組織（部署）がなく、組織運営のための計画等がない場合がある。このような場合、情報セキュリティ対策に係る詳細な計画や規程類を策定したとしても、実効性が伴わず、単に医療機関等の負担が増大してしまうことにつながるため、こうした規程類の策定に当たっては、医療機関等の組織や規模等に鑑みてリスク評価を行い、そのうえで必要な内容を定めることが必要である。

  また、実際の統制が患者等に対する説明や情報セキュリティインシデントが生じた場合の関係者への適切な報告として必要十分な内容となっているか、システム関連事業者に対する適切な管理を行うために必要十分な資料等が確保されているか、といった観点など、医療機関等において情報セキュリティ対策に関する説明責任や管理責任を果たしながら業務を運用できているかどうかも念頭に置きながら、医療機関等の規模や組織構成、特性等を踏まえた上で実効性のある統制の内容を考

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
経営管理編

- 医療機関等において、情報セキュリティ対策に関する統制の実効性を確保するために、安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置する必要があり、必要に応じて、企画管理者等が行う管理を支援するための医療情報システム管理委員会等の組織を設置することも有用である。なお、医療機関等の規模、組織等を勘案して、経営層が企画管理者等の職務を兼務することは妨げられない。

  なお、医療情報システム安全管理責任者としての職務は、経営層が担うことを想定しているが、医療機関等の規模・組織等を考慮して、企画管理者が医療情報システム安全管理責任者を兼務することは妨げられない。
- 医療機関等の組織構成によっては、例えば人事権が各部局に帰属し、各部局でそれぞれ情報セキュリティ対策に係る組織編成を行っているような組織構成となっている場合があるが、情報セキュリティ対策に関する統制は組織全体の問題であり、組織横断的に実現されることが求められるため、情報セキュリティ対策に係る組織編成においては、人事権の帰属先を越えて、組織横断的な実働ができているかどうかに留意が必要である。
- 情報セキュリティ対策に関する統制は、医療機関等に直接雇用されている職員だけではなく、医療情報システムに関係するシステム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も対象に含み、行われる必要がある。

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
経営管理編

３．２　設計

３．２．１　情報セキュリティ方針を踏まえた情報セキュリティ対策の整備

【遵守事項】

①　リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。

②　情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な内容で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。

- 情報セキュリティ方針は、リスク評価及びリスク管理方針に基づいて策定されるものであり、情報セキュリティ方針に基づき、医療機関等は医療情報システムに対する情報セキュリティ対策を実装する。
- 具体的な情報セキュリティ対策の検討や設計等は、企画管理者やシステム運用担当者が実施するが、経営層においても、情報セキュリティ対策の整備に関する理解は必要である。

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
経営管理編

３．２．２　情報セキュリティ対策を踏まえた訓練・教育

【遵守事項】

①　整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。

- 規程類が適切に整備され、また、必要な情報セキュリティ対策が医療情報システム上で実装されているとしても、その内容が医療情報システムの利用者をはじめ、関係者に認知されておらず、適切な対策が実行されていなければ、当該規程類が遵守されていないことと同義であり、情報セキュリティ対策の水準向上を望むことはできない。また災害、サイバー攻撃またはシステム障害に起因する非常時の対策についても、実際の状況下で適切に実行できない可能性が高い。
- このため、整備した規程類及び情報セキュリティ対策については、関係者が認知し、その上で遵守することができるよう、通常時から定期的に教育・訓練することが重要である。この教育・訓練については、医療情報システムに関係する者全員に対して行うことが重要である。

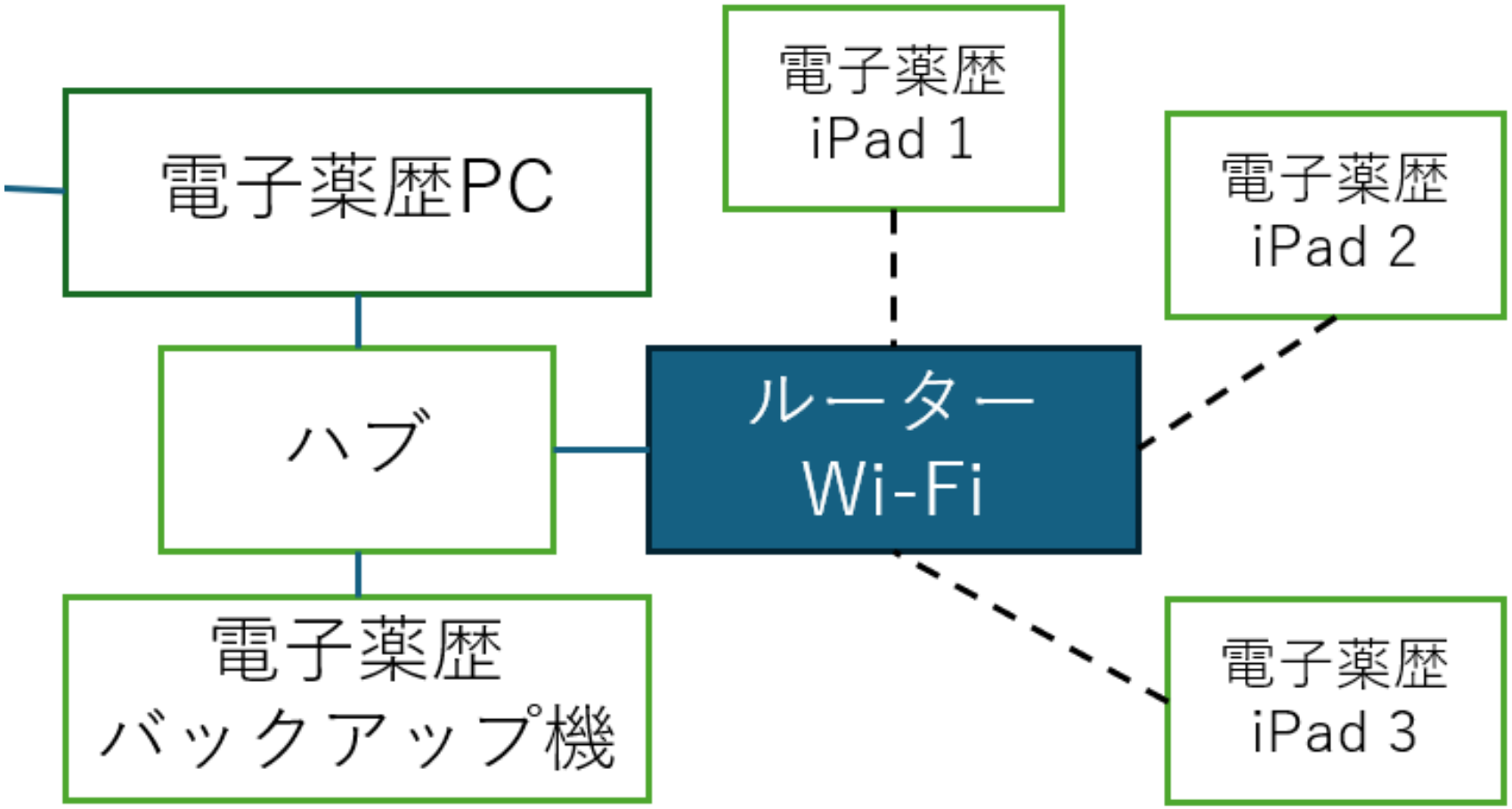
医療情報システムの安全管理に関するガイドライン第 6.0 版
経営管理編

- 具体的な情報セキュリティ対策の整備に当たっては、自医療機関等の実態を踏まえて、実際に運用可能な内容を整備することが求められる。例えば、他の医療機関等で策定された運用管理規程やアクセス管理規程等をそのまま自医療機関等の規程等に転用したとしても、実態と合致していない場合、情報セキュリティ対策の運用ルールが適切に示されていないことになり、却って情報セキュリティリスクが増大する危険性が生じる。また、極端に厳格な内容の規程類を整備しても、実際の運用が困難である場合には、実質的には死文化してしまうこととなり、有効な対策とはならない可能性がある。
- 規程類の整備に際しては、参考資料を利用する場合でも、実態との整合性を図ることが求められ、実際に運用可能なものであって、適切な内容が記載されたものを整備する必要がある。
- 教育・訓練は、過度の負担にならない範囲で定期的に実施することが求められ、医療情報システムを取り巻く情報セキュリティに関する脅威が日々変化していることも踏まえると、その対策も随時更新されるものであるため、更新内容に応じた教育・訓練の実施が重要である。

	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）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 （ / ）	

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、システム管理責任者は薬局で所有する医療情報システムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。また、薬局の開設者は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

社内ネットワーク図の例



●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	主な利用者属性	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	薬剤師・事務職員・システム管理者	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	薬剤師・事務職員・システム管理者	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	薬剤師・システム管理者	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	薬剤師・システム管理者	2021/8/1	稼働	

レセコン・電子薬歴などのメーカーに、薬局に設置した時の構成図やネットワーク図が残っているか確認することをお勧めいたします。

	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 （ / ）	

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、システム管理責任者に報告する必要があります。そのため、システム運用担当者は、機器台帳で整理した情報をもとにリモートメンテナンスを利用している機器の有無を事業者に確認し、システム管理責任者へ報告してください。なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

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

９．１　情報機器等の台帳管理

医療情報システムで用いる情報機器等に関する安全性を確認するためには、医療情報システムで用いることを予定している情報機器等の所在が明らかになっているか、またそれらの情報機器等が使用できる状態なのか否か等を、適切に管理する必要がある。

そのため、企画管理者は、医療情報システムで用いる情報機器等について、台帳管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしておく必要がある。台帳で管理する内容としては、情報機器等の所在や利用者などが想定される。また、医療情報システムの適切な利用という観点では、使用するソフトウェアやサービスのバージョン、ライセンスの状況なども管理対象として想定される。

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

医療情報システムの利用に際しては、医療機関等が管理しない情報機器等の利用も想定される。例えば BYOD（Bring Your Own Device：個人保有の情報機器）の利用などが想定される。企画管理者は、こうした医療機関等が管理しない端末の利用についても、その利用条件や利用範囲、管理方法などについての規則を策定した上で、利用可能としたものについては、併せて台帳管理することが求められる。加えて、BYOD での利用に関する具体的な条件等について担当者と協議し、必要に応じて技術的な対応を講じ、規則の内容に含めることが求められる。

また、整備した台帳を定期的に棚卸して、適切な状況にあることを確認する必要がある。

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
システム運用編

１０．１　保守時の安全管理対策

医療情報システムの適切な稼働を維持するためには、定期的な保守（メンテナンス）が必要である。保守（メンテナンス）作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、保守要員が管理者権限で直接医療情報に触れる可能性があるため、想定される脅威に対する十分な対策が必要になる。

具体的には、

- 保守要員等からの医療情報の流出・漏洩
- 保守に伴う医療情報システムにおける医療情報の破壊・破棄
- 保守に伴う医療情報システムの破壊、障害の発生
- 保守作業または保守環境に対するサイバー攻撃

等が想定される。

システム運用担当者は、このようなリスクに対応するために必要な措置を講じるほか、手順等を作成し、企画管理者に報告する必要がある。

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
システム運用編

システム運用担当者は、保守に当たって以下の内容について、確認することが求められる。

- 保守計画等の策定・確認
- 影響確認
- 作業の監督
- 作業報告・確認
- アクセス権限管理
- ログ取得
- 動作確認時のテストデータに個人情報が含まれる際の対策
- リモートメンテナンス（保守）時の対策

保守に関する手続きは、原則として事前申請・承認であるが、障害時や緊急を要する脆弱性対応などにおいては、事後承認などによることも想定される。

オンプレミスの場合には、保守に関しては個別の申請や承認により行うことが可能であるが、パブリッククラウドによるサービスにおいては、個々の利用者に対する保守の申請や承認によることが難しい場合がある。システム運用担当者は、クラウドサービスにおける保守の場合には、保守の対象時間について事業者に確認したうえで、医療機関等内部で利用している情報システムへの影響範囲、必要があれば代替措置等について確認し、企画管理者に報告の上、医療機関等内部及び関係者に周知することが求められる。

（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 （ / ）	

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。システム管理責任者は事業者へ当該医療情報システムに関するMDS/SDSの有無を確認し、事業者から回収してください。
レセコン・電子薬歴などのメーカーは既に医療情報セキュリティ開示書を作成していますので、入手方法がわからない場合はメーカーにお問い合わせください。
なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

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
概説編

４．５　リスク評価とリスク管理

安全に医療情報システムを管理し、医療情報を取り扱うに当たっては、安全を脅かす又は損なう原因となる「脅威」を認識する必要がある。この脅威としては、地震等の自然災害や、サイバー攻撃、システム障害などの環境要因によるもの、医療情報の漏洩や改ざんなどの人的要因によるものが挙げられる。

また、これらの脅威によって生じる被害等が発生する可能性がリスクとして表される。

医療情報は、患者の生命・身体の安全に関わるものであり、これらの脅威にさらされると、医療の提供が停止するといった影響が生じることも考えられる。各医療機関等においては、自組織にとっての脅威を特定し、そのリスクを評価した上で対策を講じることが重要である。特に、自然災害やサイバー攻撃、システム障害などについては、被害の影響がより大規模となる可能性が高いため、高度なリスク評価を踏まえた対策が求められる。

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：Japanese Engineering Standards of Radiological Apparatus）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。また、合意した内容を契約書や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）等の形で双方の合意文書として明らかにした上で、具体的な責任分界を踏まえた運用を行うことが求められる。

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。					
	（4） 利用者の属性等に応じた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	不要なアカウントを	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	（6） アクセスログを		はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	

医療情報システムの利用権限は、薬局内の権限規程等に応じて設定することが重要です。システム管理責任者は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。利用者に付与したID等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、利用者属性・氏名・ユーザーID・権限等が想定されます。
なお、端末PCについては、令和５年度は参考項目としています。令和6年度中に対応できるよう取り組んでください。

●利用者 ID 台帳の例

No	利用者属性	性	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年 3 月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

管理薬剤師、勤務薬剤師、非常勤薬剤師、事務職などで使用するデータは異なります。
例えばレセコンを使用する際は管理薬剤師は処方箋枚数、技術料、売上など細かいデータを確認する権限が必要だと思いますが、事務職は処方内容入力の権限があれば業務に支障はないかもしれません。

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

１３．医療情報システムの利用者に関する認証等及び権限

【遵守事項】

① リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規程を整備し、管理すること。

② 医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。

③ 医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者の ID 等を付与する等の必要な手順を作成するよう指示すること。

④ 医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程に応じたものとなっていることが前提となるよう管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。

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

１３．１．３　医療情報システムの利用者の権限設定

医療情報システムを利用する際には、実際には利用者に応じてアクセスできる情報の範囲や、作業の内容（参照のみ、作成権限あり、更新権限あり等）に関する権限が付与される。権限の付与に際しても、基本的には医療機関等の内部の人事で定めた権限規程や、医療従事者の資格などに応じて設定される必要がある。

また、医療情報システムのシステム上は利用権限が付与されているにもかかわらず、医療機関等内の個別のルールなどによって、その利用場面が限定されていたり、原則として利用しないこととされていたりする場合もある。このような場合には、システムの利用ルールについては規程等として文書化するなどにより、権限の範囲を明確にすることも重要である。

企画管理者は、このような権限設定に関するルールについても、アクセス管理に関する規程等で示すことが求められる。

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。				
	（4） 利用者の属性等に応じた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	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	

システム管理責任者はアクセス利用権限について整理した情報を元に、退職者や使用していないID等が含まれていないかを確認してください。長期間使用されていない等の不要なIDは不正アクセスに利用されるリスクがありますので、速やかに削除してください。
退職者等のIDを削除した場合に過去の記録にどのような影響が出るかメーカーに確認してから対応することをおすすめします。
なお、端末PCについては、令和５年度は参考項目としています。令和6年度中に対応できるよう取り組んでください。

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

企画管理編13⑦

⑦　医療情報システムで利用する ID 等についての棚卸を定期的に行い、不要なものについては削除すること。棚卸については、担当者に具体的な手順等の策定を指示すること。また、棚卸結果を経営層に報告し、承認を得ること。

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。**				
	（4） 利用者の属性等に応じた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 （ / ）	

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに、システム管理責任者はそのログを定期的に確認してください。例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録することが必要です。
アクセスログを薬局側で手動で確認することが可能なのかレセコン・電子薬歴のメーカーに確認してください。

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
経営管理編

４．２　必要な措置

【遵守事項】

①　医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。

- 対策項目の分類として、予防的措置と発見的措置が挙げられる。予防的措置は、想定されたリスクが実際に生じないようにするための措置であり、例えば許諾された者以外に患者の医療情報を閲覧できないようにするためのデータに対するアクセスコントロールなどが挙げられる。発見的措置は、仮にリスクとして想定する事象が発生しても、速やかに事象の発生を検知することで、具体的なリスクの発生を防止したり、被害拡大を防止したりするための措置であり、例えば医療情報に対するアクセス状況をシステム操作ログ等を用いて監査し、不審なアクセスがないかどうかを確認の上、必要に応じて措置を講じることなどが挙げられる。
- 対策項目としては、可能な限り予防的措置を講じることが望ましい。リスクの発生を未然に防止することが妥当であるし、また費用や労力の点からも、発見的措置に比べて負担が大きくならない場合が多いことが想定されるためである。
- 多様化・巧妙化が進む昨今のサイバー攻撃に対しては、必ずしも予防的措置だけでは十分な対応が難しいため、速やかに攻撃、あるいは攻撃された痕跡を検知するなどの発見的措置も、適宜組み合わせることが求められる。

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

５．３　証跡のレビュー

証跡には不正利用の探知の起点として利用することも想定されるため、単に収集するだけではなく、適宜レビューを行うことが重要である。そのため、企画管理者は、適宜証跡のレビューを行うことが求められる。

また、証跡のレビューは、証跡の性格上、レビューする対象が多いことなどで作業負担が大きくなる場合があるほか、発見までの間に不正な利用が継続してしまうなどのリスクがあることから、レビューの対象や周期などについては、バランスを勘案する必要がある。そのため企画管理者は、担当者と協議の上でレビューの対象や周期などを決定することが求められる。

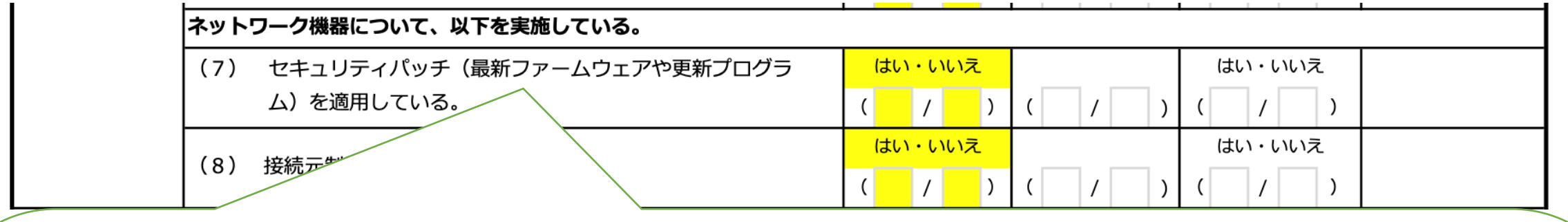
医療情報システムの安全管理に関するガイドライン第 6.0 版
システム運用編

１７．証跡のレビュー・システム監査　［Ⅰ、Ⅲ］

【遵守事項】

① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。

② アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。



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・いいえ （ / ）	
（8） 接続元制	はい・いいえ （ / ）		（ / ）	はい・いいえ （ / ）	

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。
しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが挙げられます。
なお、サーバと端末 PC については、令和 5 年度は参考項目としています。令和 6 年度中に対応できるよう取り組んでください。

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
システム運用編

8．利用機器・サービスに対する安全管理措置　［Ⅰ～Ⅳ］

【遵守事項】

① システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。

② 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。

③ 医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。

④ メールやファイル交換にあたっては、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、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること 。

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
システム運用編

8．１　不正ソフトウェア対策

コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に入る可能性がある。不正ソフトウェアの侵入に際して適切な保護対策が行われていなければ、セキュリティ機構の破壊、システムダウン、情報の漏洩や改ざん、情報の破壊、資源の不正使用等の重大な問題が引き起こされる。また不正ソフトウェアの侵入は、何らかの問題が発生して初めて気付くことが多い。

対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できる。

システム運用担当者は、企画管理者と協働して、このような不正ソフトウェア対策についての措置を講じるほか、これに必要な規則等の策定を行うことが求められる。

ただし、これらの不正ソフトウェアは常に変化しているため、検出するためのパターンファイル等を、医療機関等のシステムの環境等の状況を勘案して、可能な限り、常に最新のものに更新しておく必要がある。システム運用担当者は、パターンファイルの更新に先立ち、医療情報システムへの影響等に関する情報を収集することも求められる。

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
システム運用編

また、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、医療情報システム側の脆弱性を可能な限り小さくしておくことや被害拡大の防止策を講じておくことが重要である。そのために実施すべき対策として、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの非活性化、ネットワークの構成分割やネットワーク間のアクセス制御、マクロ等の利用停止、メールやファイルの無害化がある。また、EDR（Endpoint Detection and Response）や「振る舞い検知」などの方策も有効である。なお、いずれの対策を行う場合も、対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要である。

また、医療機関等の外部で利用する端末や PC 等についても同様のリスクがあることから、これらの情報機器等についても、上記の対応を行うことが求められる。

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
システム運用編

８．２　情報機器等の脆弱性への対策

企画管理者は、医療情報システムが利用する情報機器等の脆弱性に関する情報を常に収集し、脆弱性への対応を速やかに行う必要がある。

医療機関等において、医療情報システムが利用する情報機器等には、利用者が直接利用する PC 等の端末のほか、医療情報システムで利用する機能等のサービスを提供するサーバや、ネットワークに関連する機器等、様々なものが挙げられる。

サイバー攻撃においては、近年は、情報機器等に内蔵されるファームウェアや、情報機器等に格納されるプログラム等の脆弱性、EOS（End of Sales, Support, Service：販売終了、サポート終了、サービス終了）の対象となった情報機器等を攻撃して、外部から攻撃するなどが多くみられている。特にランサムウェアなどのケースでは、必要な脆弱性対策が見逃されたことに起因するものも見られる。

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
システム運用編

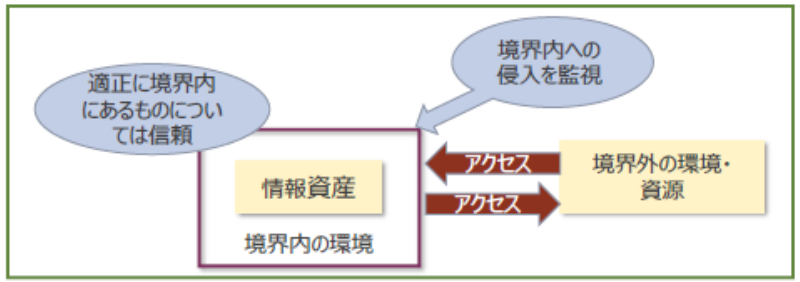
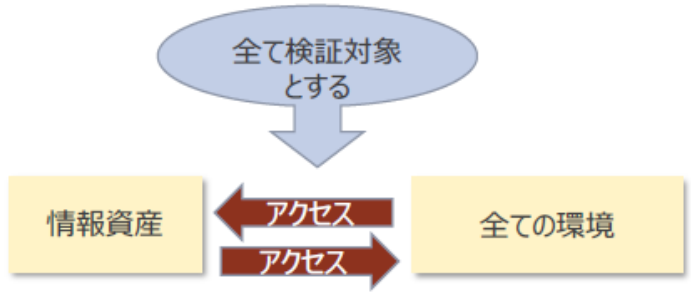
１３．２　不正な通信の検知や遮断、監視

ネットワークの選択においては、オープンではないセキュアなネットワークを選択し、境界防御的な対応を原則とするが、巧妙化するサイバー攻撃に対しては、境界防御的な対応だけでは十分ではない。例えば VPN 装置の脆弱性を攻撃することにより、ランサムウェアによる被害なども見られることから、境界防御だけでサイバー攻撃への対応を図ることは困難と言える。

近年は、境界防御の思考による安全性のみに限らず、すべてのトラフィックについての安全性を検証するという「ゼロトラスト」の概念による考え方も出てきている。ゼロトラスト思考では、利用者の行動も含めてすべて検証し、異常とみられる事象が発生したタイミングで、利用者の正当性などを確認するなどの仕組みで構成される。

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
システム運用編

表１２－１　境界防御型思考とゼロトラスト思考の比較

境界防御型思考 	・　オープンな環境（管理者により管理されていない環境）とオープンではない環境（管理者により管理されている環境）を想定したうえで、オープンではない環境については、その境界部分への侵入を防ぐため、監視を行う。 ・　オープンではない環境では、医療情報等、特に重要な情報の管理を行う。
ゼロトラスト思考 	・　オープンではない環境とオープンな環境のいずれにおいても、情報資産へのアクセスについては、不正なものが含まれうることを前提（ゼロトラスト）に、すべてを検証対象とする。 ・　検証は、情報資産に対するアクセスにおいて、不正なトラフィックやアクセス等の異常行動などを起点として捉える。

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
システム運用編

ゼロトラスト思考の有効性は、認められているものの、これを実装するためには、現時点では費用や管理に対する負担が大きいとされており、医療機関等においても小規模の医療機関等で導入することは必ずしも容易ではない。また医療機関等の場合、接続先が多方面にわたっていない医療機関等が多いことから、導入に当たってはリスク分析の結果を踏まえて判断することが望ましい。

但し、境界防御ではサイバー攻撃への対応としては十分ではないことから、境界防御を採用する場合でも、トラフィックの監視等、多層防御の考え方を導入することが、医療機関等においては求められる。

クラッカーや不正ソフトウェアによる攻撃から情報を保護するための一つの手段として、ファイアウォールの導入があるが、これに加えて、不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）などの採用もシステム運用担当者は、検討する必要がある。またシステムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ適用等の対策を講じておくことも重要である。これは、「８．２　情報機器等の脆弱性への対策」と併せて実施することが求められる。

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
システム運用編

さらに、外部からのサイバー攻撃の高度化・多様化に鑑みると、境界防御の対策を行っていたとしても、不正ソフトウェア等の攻撃や侵入があることから、このような場合を想定して、内部脅威監視や EDR などの措置を講じることも、有効な対策として挙げられる（「８．１　不正ソフトウェア対策」参照）。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。

	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・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 （ / ）	

外部ネットワークに接続する際には、ネットワークや機器等を適切に選定し、監視を行うことが必要です。特に、無線LANを使用する際は不正アクセス対策として適切な利用者以外に無線LANを利用されないようにすることが重要です。システム運用担当者は、例えば、ネットワーク機器に接続出来るMACアドレスを限定すること等、不正アクセス対策を実施してください。

レセコン・電子薬歴メーカーが設定した端末・方法以外で外部ネットワークに接続する際は医療情報システムで利用する回線とは別にプロバイダ契約をする、社員や来局者の個人端末は会社のネットワークには接続しない等の対策も考えられます。

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
システム運用編

１３．ネットワークに関する安全管理措置

医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。

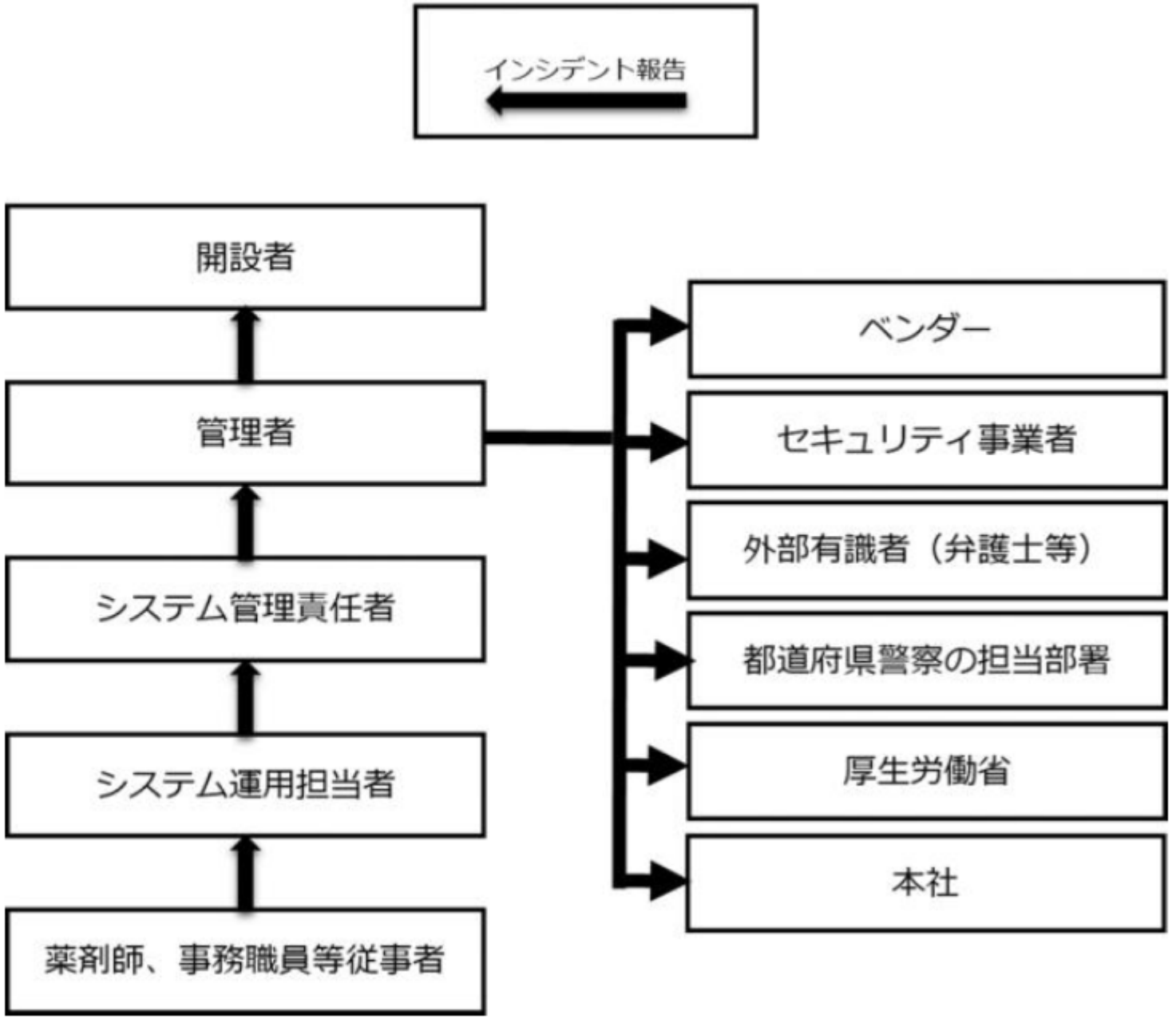
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	（8） 接続元制限を実施している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	

薬局の開設者は情報セキュリティインシデント発生に備え、事業者や外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、システム管理責任者に指示することが重要です。システム管理責任者はサイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成して下さい。連絡体制図には薬局内の連絡先や会社本部の連絡先等に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定されます。

このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

立入検査時は、連絡体制図が作成されていることを確認します。

●連絡体制図の例


インシデント報告
開設者
管理者
システム管理責任者
システム運用担当者
薬剤師、事務職員等従事者
ベンダー
セキュリティ事業者
外部有識者（弁護士等）
都道府県警察の担当部署
厚生労働省
本社

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

３．４．２　情報共有・支援、情報収集

【遵守事項】

① 情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。

② 情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策や EOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示すること。

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

３．４．３　情報セキュリティインシデントへの対応体制

【遵守事項】

① 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。

② 情報セキュリティインシデントが発生した場合に、厚生労働省等への報告のほかに、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。

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

１２．３　サイバー攻撃被害時の対応

サイバー攻撃を受けた際には、あらかじめ策定した対応計画等に従って対応することとなる。場合によっては、医療機関等独自の対応では対処しきれない事案も想定されるため、そのような場合に所管官庁への迅速な連絡や情報共有を行うことができるよう、通常時から連絡先や連絡手順、連絡体制を整備しておく必要がある。また、被害拡大を防止する観点から、医療機関等内の職員やシステム関連事業者だけではなく、非常時対応として臨時的に医療情報システムに接続する関係者に対しても、速やかに連絡・情報共有する体制を講じることも重要である。

チェックリストマニュアル
医療情報システムの安全管理に関するガイドライン
を参照しつつ
チェックリストを活用して、
日頃から実のあるサイバーセキュリティ対策を行って下さい。