医療情報システムの安全管理に関する調査報告書

一般社団法人 日本保険薬局協会
デジタル推進委員会

2024年１月

調査概要

- 目的：医療情報システムの安全管理に関する現状調査
- 内容：全40問。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（以下、「ガイドライン」）に記載されている遵守事項を一部抜粋して設問を設計。回答は「4.概ね対応できている」「3.やや対応できている」「2.あまり対応できていない」「1.ほぼ対応できていない」「0.わからない」の選択式。「わからない」以外の回答をした割合を理解度、「概ね対応できている」「やや対応できている」の回答割合を対応率として集計。
- 対象：NPhA加盟の法人（正会員）
- 方法：オンラインWEB調査　１社１回答　※グループで１回答でも可
- 回答期間：2023年11月10日（金）～12月14日（木）
- 回答数：71社（18.8%）*
- 実施主体：一般社団法人日本保険薬局協会　デジタル推進委員会
- 倫理審査：日本薬局学会倫理審査委員会　受付番号23004

調査結果　Summary

医療情報システムの実装及び運用を担当する体制があるのは、65社,91.5%であった。100薬局以上の薬局グループ規模においては複数部署が連携して対応している割合が高く、部署間連携が重要となる。一方で、100薬局未満の規模においては特定の担当部署が対応している割合が高くなり、担当者の見識や労力が課題となると推察される。

各設問に関して全体的に高い理解度が示され、対応率はその内容によってバラツキが大きいが、雇用契約に守秘条項記載や、情報機器等の資産管理、認証・ID等の管理、災害時バックアップ、復旧体制・手順の整備、機器・NWの安全管理措置など、重要性が高いと思われる設問に関して対応率が高い傾向であった。

また、薬局グループ規模によって理解度や対応率に大きな差は見られなかったが、「内部監査の実施」「情報機器等の資産管理」といった設問に関しては、100薬局以上の規模において高い対応率となった。

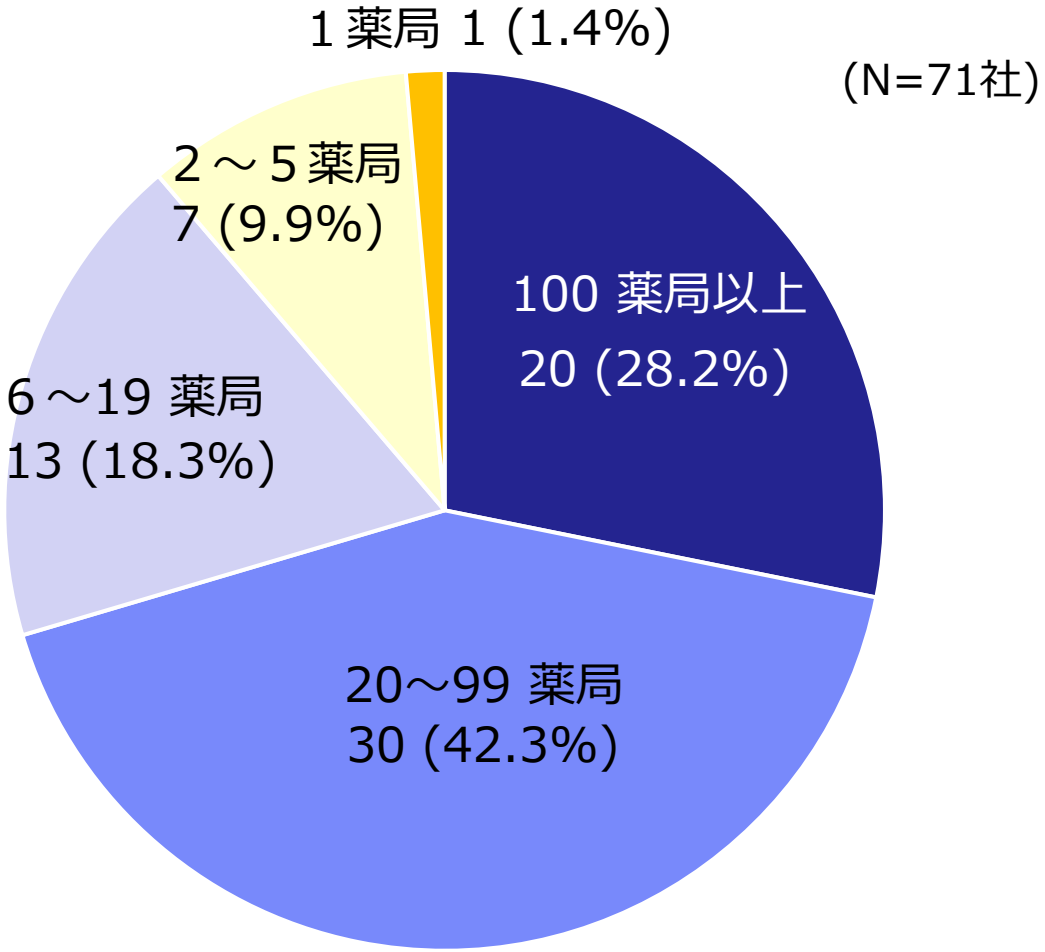
最後に、本調査への回答率は約20%。100薬局以上の薬局グループの回答率は約50%、20～99薬局は約25%、１～19薬局は約10%と、回答率に大きな差があることから、調査内容に対する関心の差が生じていることが懸念される。これらの結果を踏まえて、ガイドラインの周知や対応状況の向上に努めていくとともに、サイバーセキュリティ事故対応に係る保険の案内を通じて、非常時においても持続可能な薬局経営に貢献していく。

* NPhA正会員の企業数377社（2023年12月14日現在）グループとして回答いただいている場合の補正は不可のためしていない

規模別回答数

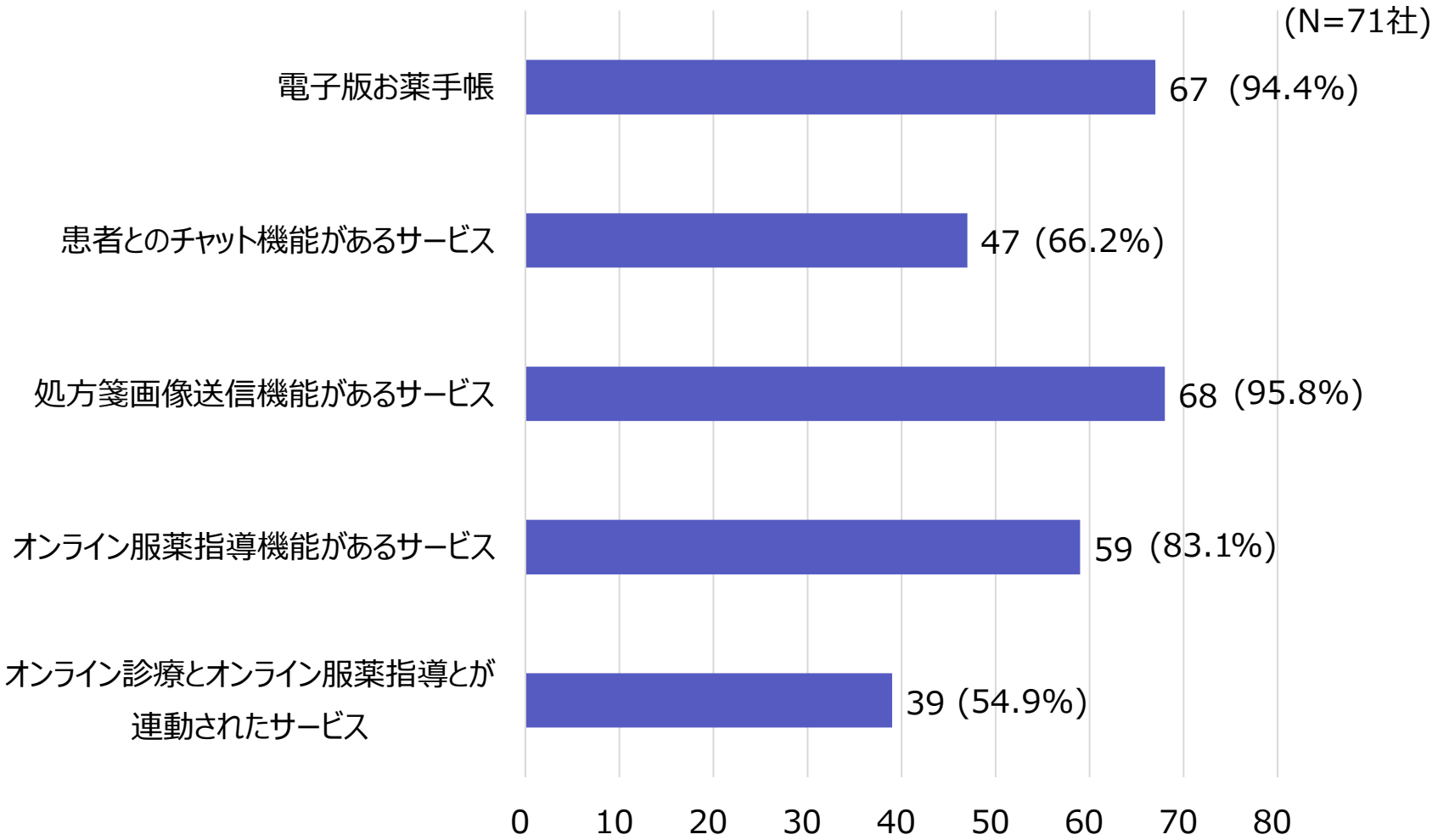
本調査の全体の回答率は約20%。100薬局以上の回答率は約50%、20～99薬局は約25%、1～19薬局は約10%と、回答率に大きな差があることから、調査内容に対する関心の差が生じていることが懸念される。

問１．貴社・薬局グループの総薬局数を教えてください。
□１薬局　□２～５薬局　□６～19薬局　□20～99薬局　□100薬局以上



ICT導入状況

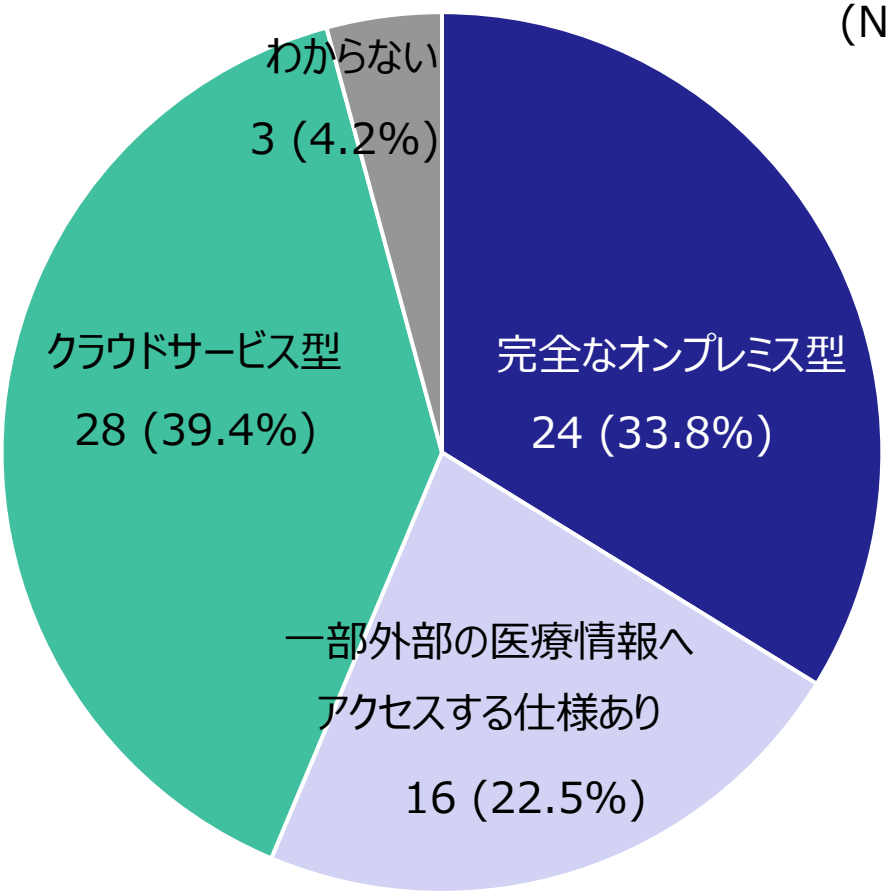
問２．貴社・薬局グループで、患者とのやり取りにおいて導入しているICTを活用したサービスを教えてください。
一部の薬局で導入している場合も選択ください。（複数選択可）



システム形態

問３．医療情報システム（レセコン、電子薬歴等）の保有形態について教えてください。
□完全なオンプレミス型　□一部外部の医療情報へアクセスする仕様あり　□クラウドサービス型　□わからない

(N=71社)



設問の分類

本調査における設問を、下記の４つの領域に分類し回答結果を集計した。

安全な運用及び管理のための体制整備（問４～15）
- 担当部署、関連部署（4,5,14）
- 企画管理者の設置（6）
- 各種方針・規程の策定、運用（7,8,9,13）
- 内部監査の体制（10）
- 委託事業者との責任分担（12,15）
- 外部監査の体制（11）

人的管理（問16～19、26～28）
- 雇用中及び退職後の守秘・非開示（16）
- 教育・訓練（17）
- アクセス権限、ID等の管理（19,26）
- 入退室管理（27）
- 記録媒体の運用管理（18,28）

非常時対応（問20～25、37、38）
- 非常時の定義やBCPとの整合性（20,23）
- 大規模災害への備え（21）
- ランサムウェア等への備え（22）
- サイバーセキュリティ対応計画の策定と実践（24）
- サイバー攻撃時の社内外連絡体制の整備（25）
- 保険への加入（37,38）*

システム・ネットワークの運用及び管理（問29～36）

（システムの運用及び管理）
- 機能や利用方法、セキュリティに関する資料を整備（29）
- システム全体構成図と責任者・関係者一覧を整備（30）

（機器・サービス）
- 情報機器、サービス、ライセンス等の資産管理（19,31）
- 不正なソフトウェア対策のスキャン用ソフトウェアの導入（31）
- セキュリティパッチの適用、脆弱性の確認・対応（31）
- 不要なソフトウェア等の停止（32）

（ネットワーク）
- 境界防御的な対応（FW、IDS、IPSの導入、接続元制限）（33）
- 内部脅威監視やEDRの導入（34）
- 回線及び情報の暗号化（35）
- アクセスログの記録と確認（36）

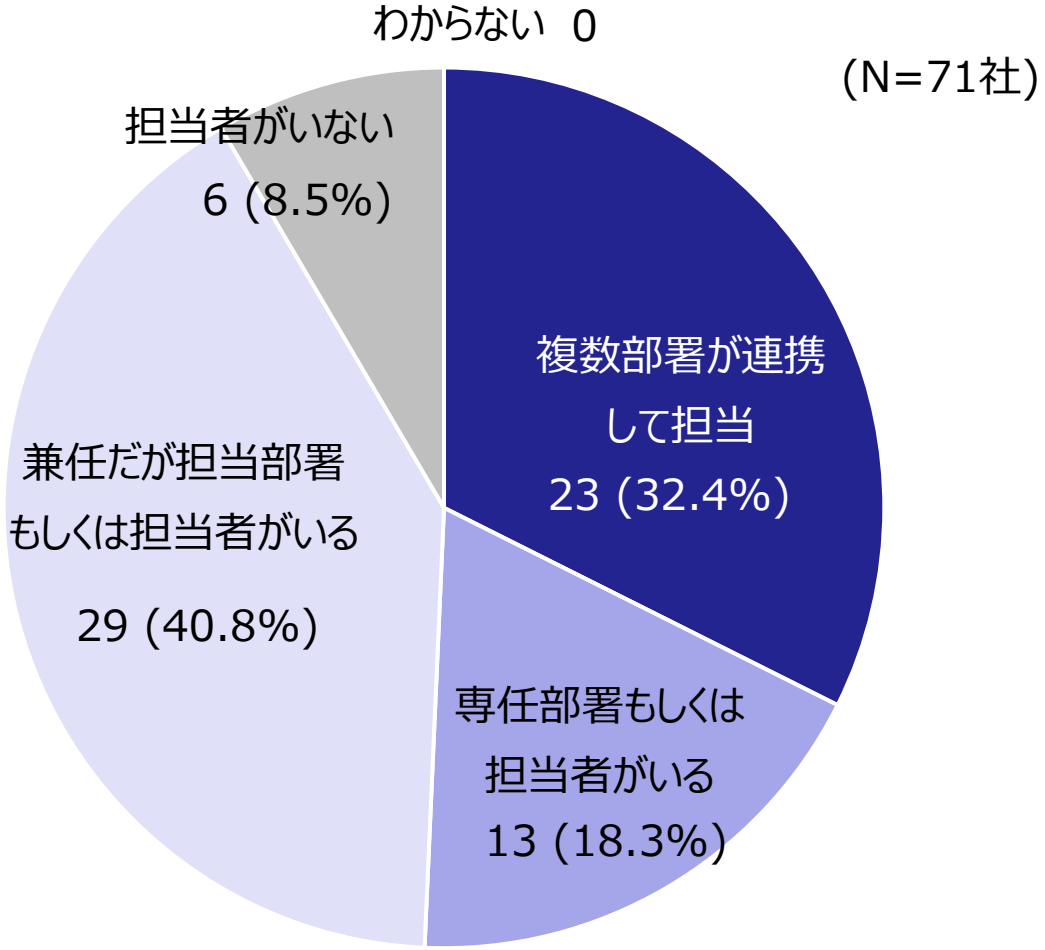
* 問37、38の保険への加入に関する設問以外は、「医療情報システムの安全管理に関するガイドライン第6.0版」に記載されている遵守事項を一部抜粋して設問を設計

システムに係る体制

問４：担当部署・担当者
問５：医療情報システム安全管理責任者の選任
問６：企画管理者の職務を担う者の選任

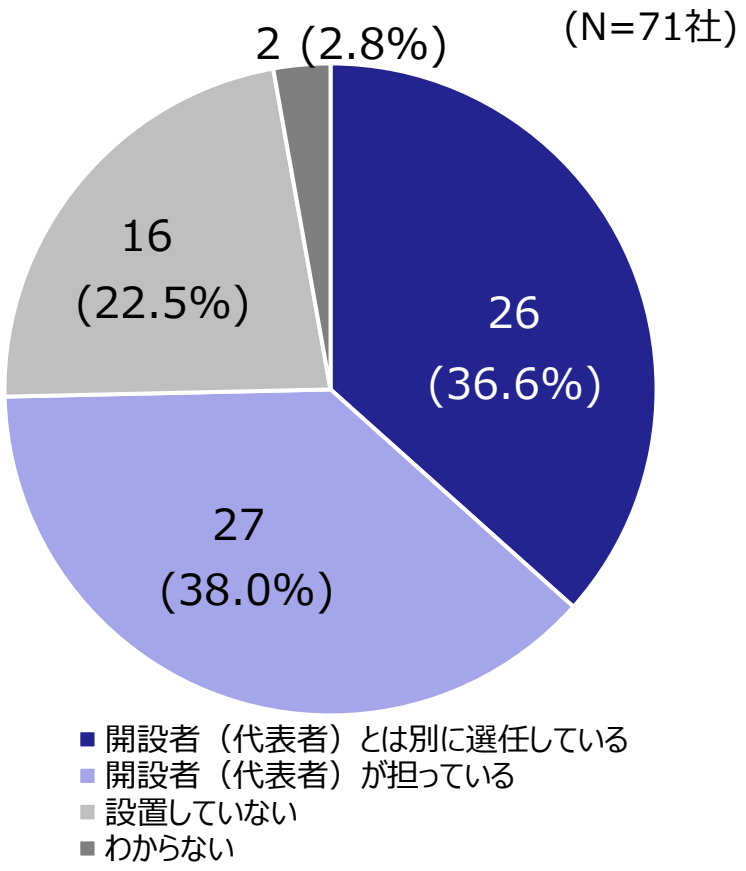
担当部署・担当者

問４．医療情報システムの実装及び運用を担当する部署もしくは担当者について教えてください。
□複数部署が連携して担当　□専任部署もしくは担当者がいる　□兼任だが担当部署もしくは担当者がいる
□担当者がいない　□わからない



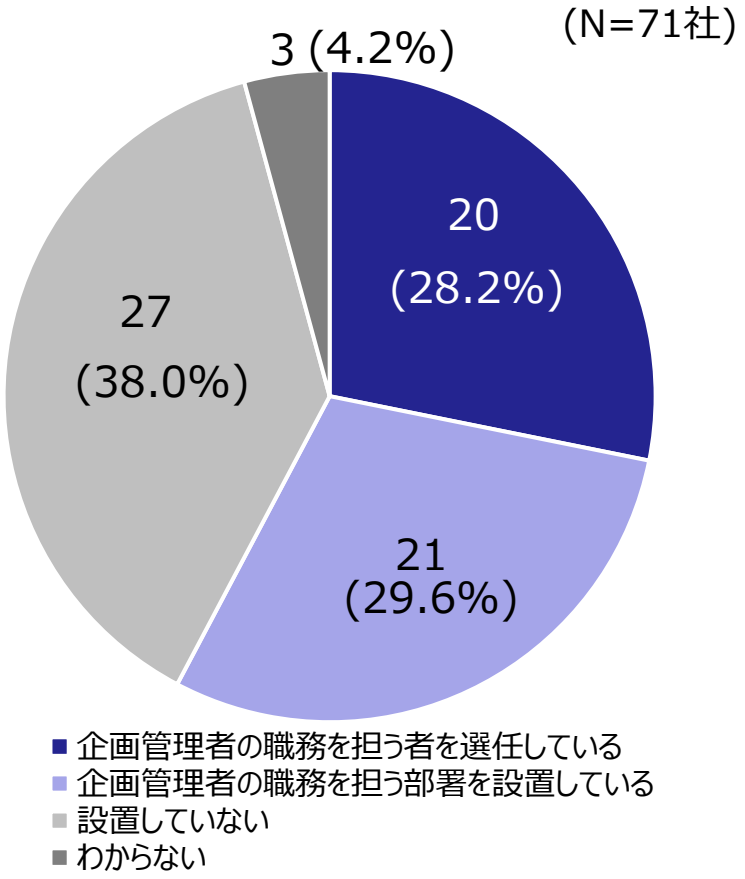
安全管理責任者 / 企画管理者

問５．医療情報システム安全管理責任者※を選任していますか？



▶ 対策の実効性の観点から一定の権限をもった経営層が担う想定

問６．医療情報システムの安全管理を行うために必要な企画管理者※の職務を担う者を選任していますか？

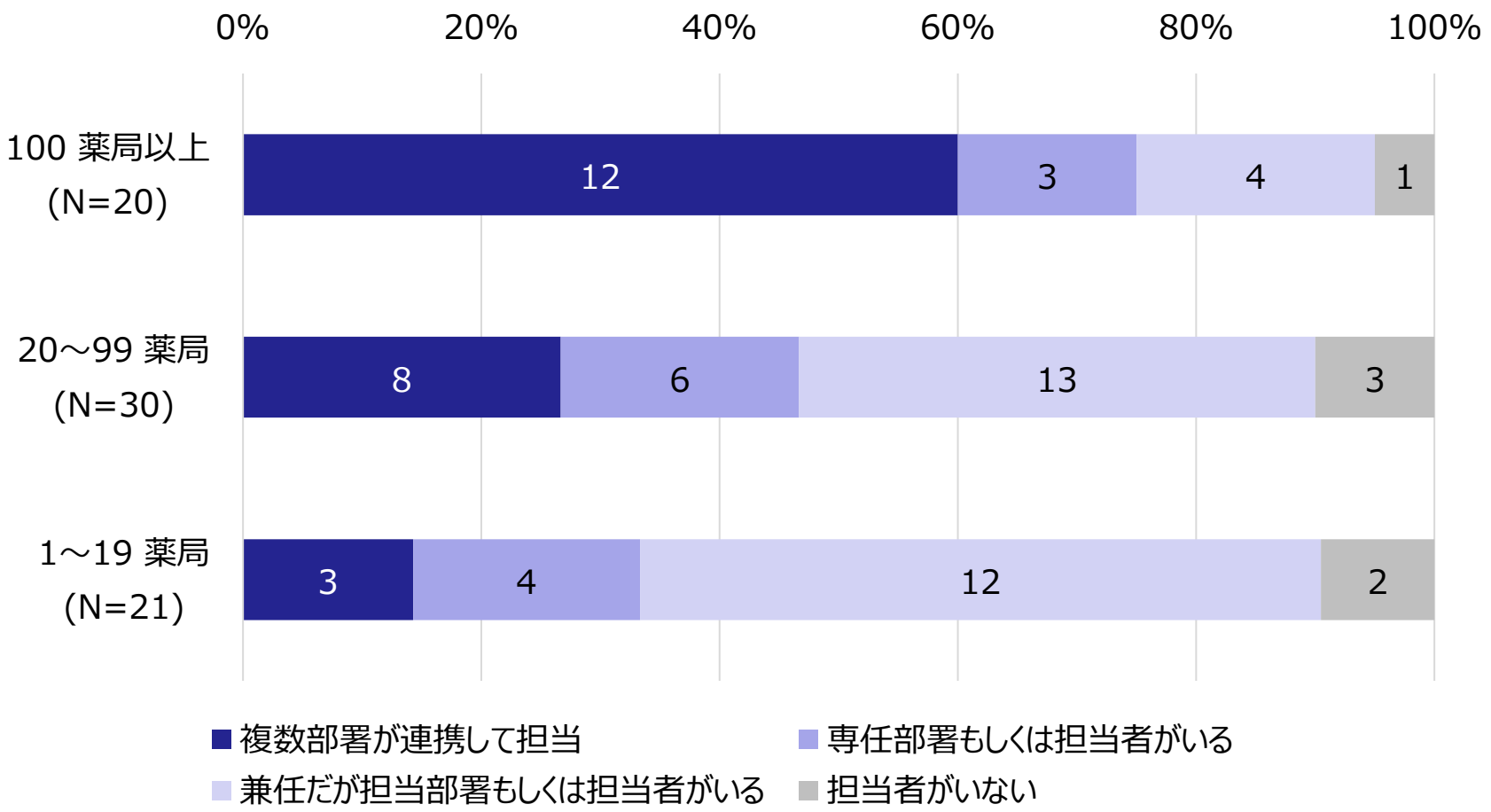


▶ 企画管理者の業務範囲と権限について：経営層は医療情報システムにおける安全管理について医療機関としての最終的な管理責任を負うが、企画管理者はその経営層の判断をサポートし、医療機関等において円滑に安全管理を行うことができるようにすることが重要な業務である。具体的な企画管理者の業務範囲としては、医療機関等の医療情報システムの安全管理について、経営層が行う管理をサポートするために必要な資料の作成や報告、日常的な医療情報システムの安全管理が想定される。また、これらを行うのに必要な承認権限等を有することが想定される。

規模×担当部署・担当者

100薬局以上の規模においては複数部署が連携して対応している割合が高く、部署間連携が重要となる。一方で、100薬局未満の規模においては特定の担当部署が対応している割合が高くなり、担当者の見識や労力が課題となると推察される。

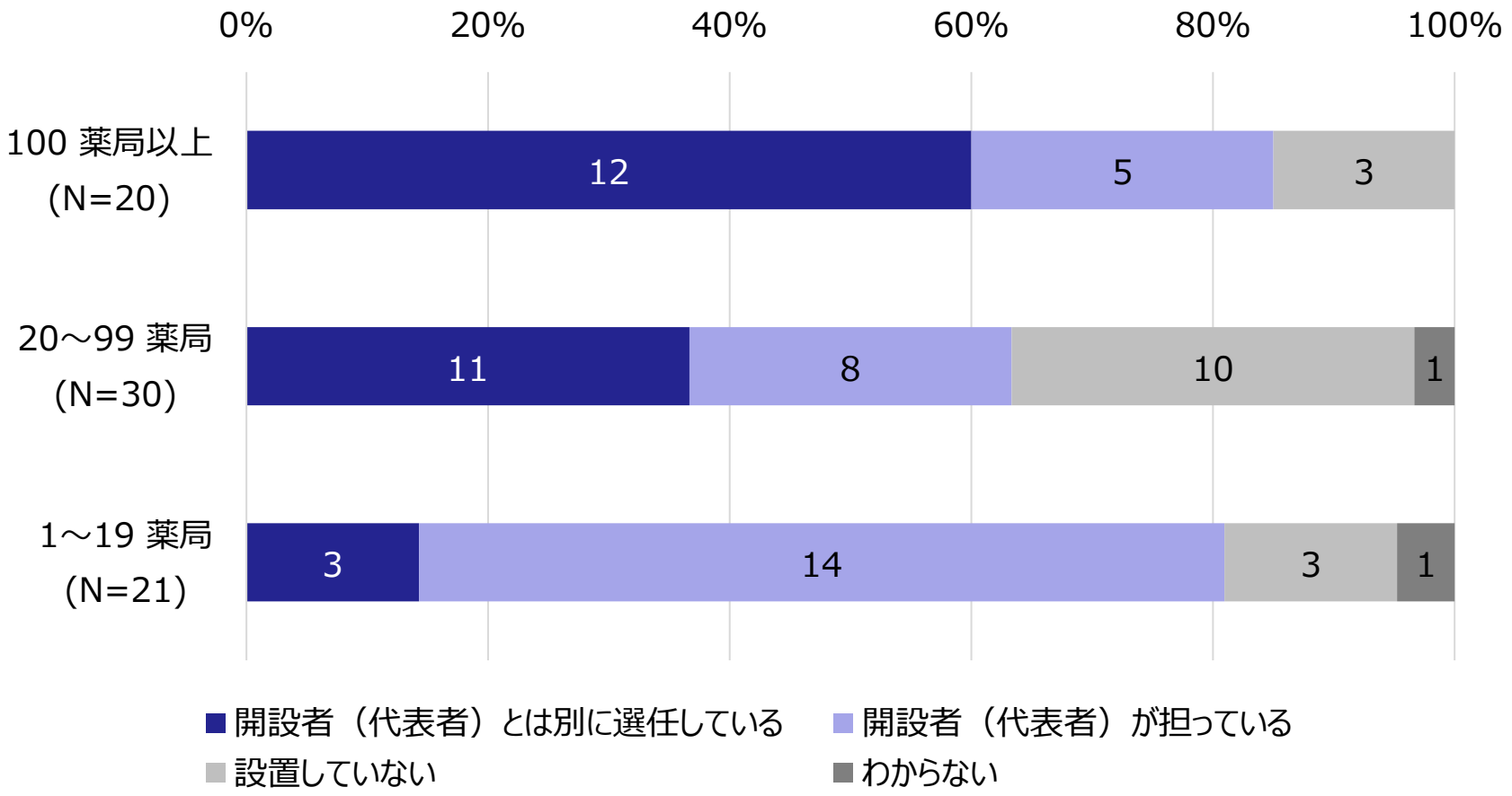
問４．医療情報システムの実装及び運用を担当する部署もしくは担当者について教えてください。



規模×安全管理責任者

100薬局以上の規模においては開設者とは別に安全管理責任者を選任している割合が高く、100薬局未満になると開設者が担っている割合が高くなる。

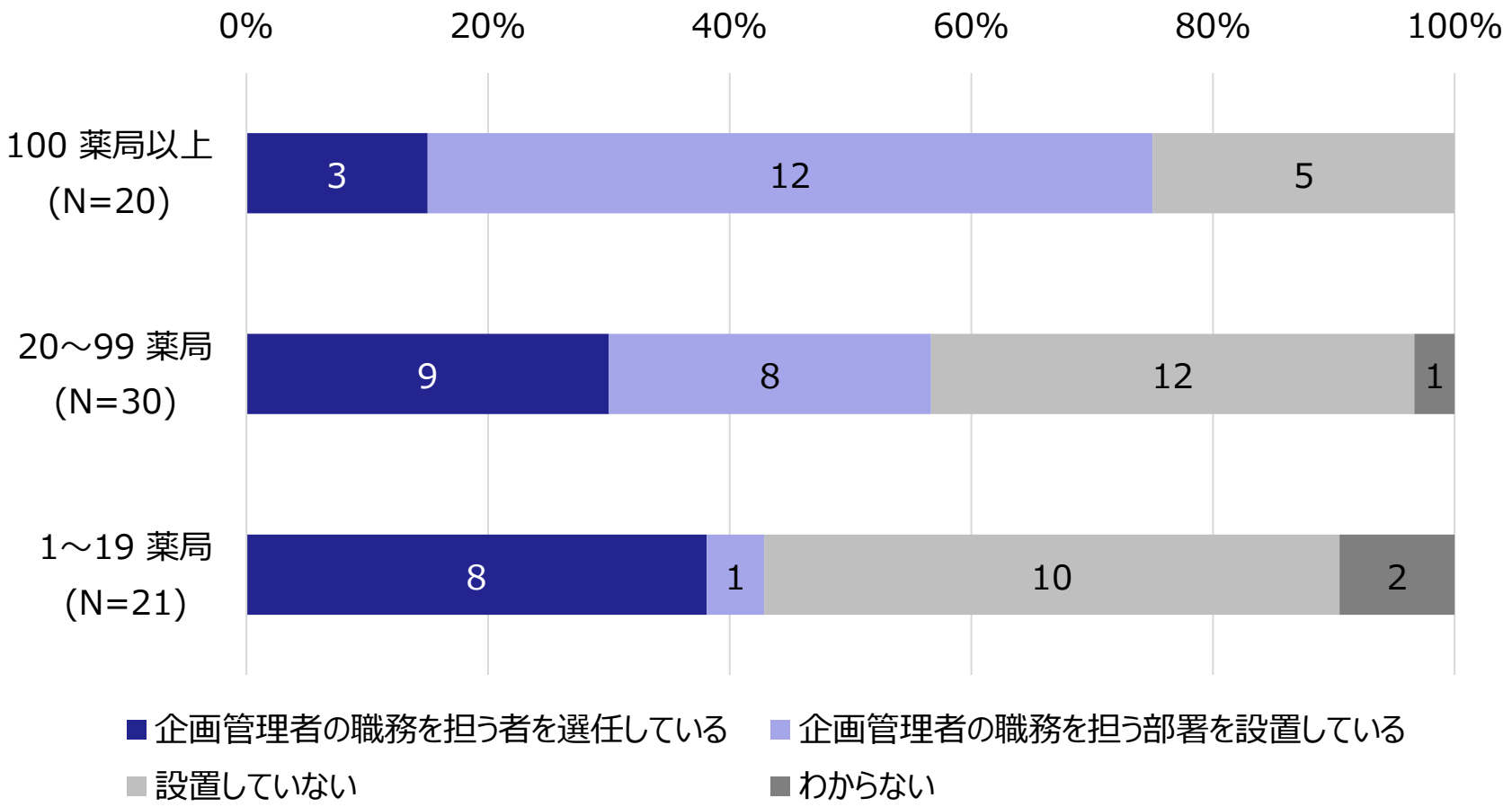
問５．医療情報システム安全管理責任者を選任していますか？



規模×企画管理者

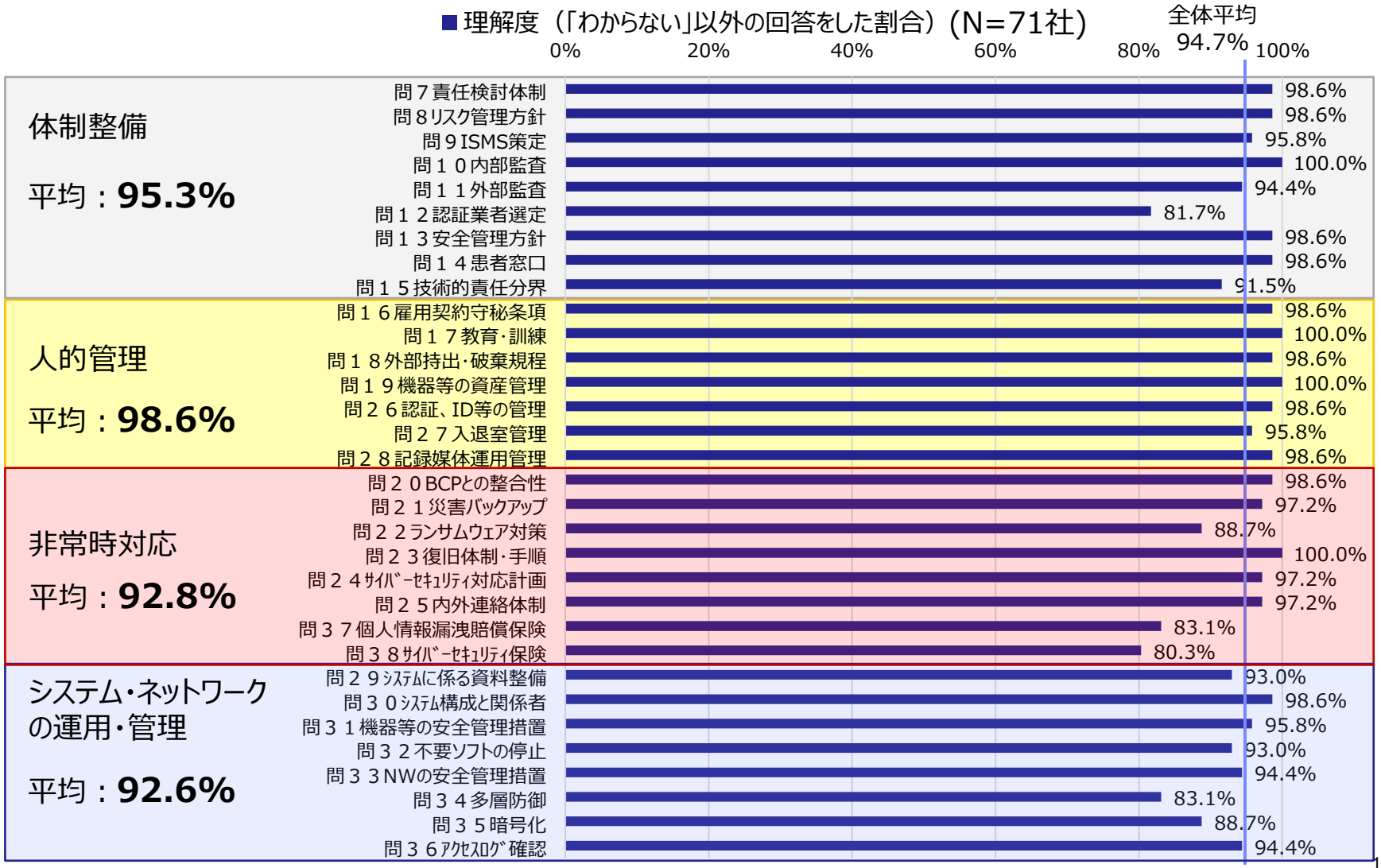
100薬局以上の規模においては企画管理者を選任している割合が高く、100薬局未満では選任していない割合が高くなる傾向が見られた。

問６．医療情報システムの安全管理を行うために必要な企画管理者の職務を担う者を選任していますか？



各設問の理解度

各設問に関して「わからない」を選択された割合は低く、全体的に高い理解度が示された。一方で、問12「認証を受けている事業者の選定」、問37「個人情報漏洩賠償保険」、問38「ｻｲﾊﾞｰｾｷｭﾘﾃｨ保険」への理解度が若干低い傾向であった。



以降の報告書は
NPhA正会員専用ページの
アーカイブに公表しております。

調査内容

調査内容

－調査概要－

- 目的：医療情報システムの安全管理に関する現状調査
- 対象：NPhA 加盟の法人（正会員）　1社1回答　※グループで1回答でも可
- 内容：ガイドラインに記載されている遵守事項を一部抜粋した設問を調査。全 40 問。
- 方法：WEB フォーム　https://forms.gle/F2DoVZf8aXkeEmdWA
- 回答期日：2023 年 11 月 10 日～2023 年 12 月 14 日
- 実施主体：一般社団法人日本保険薬局協会　デジタル推進委員会
- 倫理審査：日本薬局学会倫理審査委員会 受付番号 23004
- 注意事項：薬局運営や患者へのサービス提供に係る薬局現場も含めた法人全体としての取り組み状況と捉えてご回答ください。また、匿名回答となるため、重複回答にはご注意ください。

本調査のポイント

安全な運用及び管理のための体制整備
- 担当部署、関連部署
- 企画管理者の設置
- 各種方針・規程の策定、運用
- 内部監査の体制
- 委託事業者との責任分担
- 外部監査の体制

人的管理
- 雇用中及び退職後の守秘・非開示
- 教育・訓練
- アクセス権限、ID等の管理
- 入退室管理
- 記録媒体の運用管理

非常時対応
- 非常時の定義やBCPとの整合性
- 大規模災害への備え
- ランサムウェア等への備え
- サイバーセキュリティ対応計画の策定と実践
- サイバー攻撃時の社内外連絡体制の整備
- 保険への加入

システム・ネットワークの運用及び管理

（システムの運用及び管理）
- 機能や利用方法、セキュリティに関する資料を整備
- システム全体構成図と責任者・関係者一覧を整備

（機器・サービス）
- 情報機器、サービス、ライセンス等の資産管理
- 不正なソフトウェア対策のスキャン用ソフトウェアの導入
- セキュリティパッチの適用、脆弱性の確認・対応
- 不要なソフトウェア等の停止

（ネットワーク）
- 境界防御的な対応（FW、IDS、IPSの導入、接続元制限）
- 内部脅威監視やEDRの導入
- 回線及び情報の暗号化
- アクセスログの記録と確認

「安全な運用及び管理のための体制整備」に係る設問：問 4 ～15
「人的管理」に係る設問：問 16～19、26～28
「非常時対応」に係る設問：問 20～25、37、38
「システム・ネットワークの運用及び管理」に係る設問：問 29～36

【アンケートポリシー】
調査に関して、WEB フォームの構築及び回答データの蓄積は、外部に委託し、当協会と受託者は秘密保持契約を締結しています。受託者は回答会社名や回答者名等、個社や個人が特定できる情報を削除し、それらが含まれていないことを確認したうえで、データが当協会事務局へ提供され分析が行われます。データ集計、分析、報告書の作成、情報発信の過程において、ご回答いただいた個社及び回答者の情報が当協会内外に漏れることはございません。また、当調査の報告書は NPhA ホームページへの公開を予定しており、その他、学会発表等の学術活動、行政や医療業界団体への情報提供等の業界活動として活用される可能性がございます。

本調査の目的及びアンケートポリシーにご賛同いただける場合にご回答お願いいたします。回答後に回答データの削除を希望される場合は、下記の問い合わせ先までご連絡ください。なお、ご回答いただけない場合であっても何ら不利益を被ることはございません。

【問い合わせ先】
一般社団法人 日本保険薬局協会　事務局　石井 僚
〒103-0027　東京都中央区日本橋 3-12-2 朝日ビルヂング 4 階
TEL：03-3243-1075　メール：ryo.ishii.jg7@ainj.co.jp

－医療情報システムの安全管理に関する調査（1社1回答）の内容－

注意：薬局運営や患者へのサービス提供に係る薬局現場も含めた法人全体としての取り組み状況と捉えてご回答ください。また、匿名回答となるため、重複回答にはご注意ください。なお、設問は、ガイドラインに記載されている遵守事項の一部を抜粋して作成しており、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 版の詳細に関しては、厚生労働省サイト https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html より、ご確認ください。

企業もしくは薬局グループの基本情報に係る設問

問 1.【企業規模】貴社・薬局グループの総薬局数を教えてください。
□1薬局　□2～5薬局　□6～19 薬局　□20～99 薬局　□100 薬局以上

問 2.【ICT 導入状況】貴社・薬局グループで、患者とのやり取りにおいて導入している ICT を活用したサービスを教えてください。一部の薬局で導入している場合も選択ください。（複数選択可）
□電子版お薬手帳　□患者とのチャット機能があるサービス
□処方箋画像送信機能があるサービス　□オンライン服薬指導機能があるサービス
□オンライン診療とオンライン服薬指導とが連動されたサービス
□その他（　　）

問 3.【システム形態】医療情報システム（レセコン、電子薬歴等）の保有形態について教えてください。
□完全なオンプレミス型　□一部外部の医療情報へアクセスする仕様あり
□クラウドサービス型　□わからない

問 4.【体制 1】医療情報システムの実装及び運用を担当する部署もしくは担当者について

調査内容

教えてください。
□複数部署が連携して担当　□専任部署もしくは担当者がいる
□兼任だが担当部署もしくは担当者がいる　□担当者がいない　□わからない

問５.【体制２】医療情報システム安全管理責任者※を選任していますか。
※安全管理責任者は対策の実効性の観点から一定の権限をもった経営層が担う必要がある
□開設者（代表者）とは別に選任している　□開設者（代表者）が担っている
□設置していない　□わからない

問６.【体制３】医療情報システムの安全管理を行うために必要な企画管理者※の職務を担う者を選任していますか？
※企画管理者の業務範囲と権限について（ガイドライン企画管理編 P17）
経営層は医療情報システムにおける安全管理について医療機関としての最終的な管理責任を負うが、企画管理者はその経営層の判断をサポートし、医療機関等において円滑に安全管理を行うことができるようにすることが重要な業務である。具体的な企画管理者の業務範囲としては、医療機関等の医療情報システムの安全管理について、経営層が行う管理をサポートするために必要な資料の作成や報告、日常的な医療情報システムの安全管理が想定される。また、これらを行うのに必要な承認権限等を有することが想定される。
□企画管理者の職務を担う者を選任している
□企画管理者の職務を担う部署を設置している
□設置していない　□わからない

ガイドラインに係る設問　経営管理編

【１.安全管理に関する責任・責務】※このナンバリングはガイドライン上の項目ナンバーとなります。必要に応じてガイドラインをご確認のうえ、ご回答ください。
医療情報システムに対する医療機関等の責任として、医療情報は患者等に関する機微な個人情報であることから、患者等との関係において、医療情報を取り扱う医療情報システムを適正に管理する責任があり、医療は重要な公的社会インフラであり、医療サービスの提供の継続性を確保・維持することは公的な責務と考えられるため、医療サービスの提供を支える医療情報システムを適正に管理する責任がある。

問７. 医療情報システムの安全管理に関する責任として、通常時において対応すべき責任と、非常時において対応すべき責任、業務委託先事業者による業務における責任、医療情報を第三者に提供する際に生じる責任に大別されます。これらの安全管理に関する責任・責務を十分に理解した上で、それを実践するための対策等を継続的に検討する体制は整備されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

【２.リスク評価を踏まえた管理】
問８. 取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

問９. リスク管理方針を踏まえ、医療情報及び医療情報システムといった薬局等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）を策定し、実施されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

【３.安全管理全般】
問 10. 医療情報システムの運用担当者から独立した内部組織により、情報セキュリティ方針に基づき、機能・運用しているかどうかの内部監査は実施されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

問 11. 外部機関により、情報セキュリティ方針に基づき、機能・運用しているかどうかの外部監査は実施されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

【５　医療情報システム・サービス事業者との協働】
問 12. 委託する事業者を選定する場合には、JISQ15001、JISQ27001 又はこれと同等の規格の認証を受けているシステム関連事業者を選定されていますか？
□４．概ね対応できている　□３．やや対応できている　□２．あまり対応できていない
□１．ほぼ対応できていない　□０．わからない

ガイドラインに係る設問　企画管理編

調査内容

【1．管理体系】の頁に記載の遵守事項を一部抜粋

問 13．組織における情報セキュリティ方針や、医療情報の取扱いや保護に関する方針を含む「医療情報システムの安全管理に関する方針」を策定していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 14．患者等からの照会や相談、苦情に対応するために必要な医療情報システムの安全管理に関する窓口等を整備していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【2．責任分界】

問 15．委託先のシステム関連事業者との間で、医療情報システムの実装や運用において発生する技術的な対応に関する責任分担（責任分界）の取り決めがありますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【7．安全管理のための人的管理】

問 16．医療情報を取り扱う者を職員として採用するに当たって、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 17．個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【8．情報管理】

問 18．医療情報及び情報機器の外部への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定めて運用していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【9．医療情報システムに用いる情報機器等の資産管理】

問 19．医療情報システムにおいて用いる情報機器、サービス、ライセンス等の資産管理を行うのに必要な規程等を整備し、台帳管理、定期的な棚卸、滅失状況の確認等を行っていますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【11．非常時対応と BCP 策定】

問 20．医療情報システムの安全管理に関して、非常時の定義や BCP（Business Continuity Plan：事業継続計画）との整合性がとれた対応方針と対応手順・内容の整備をしていますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 21．大規模災害に備えてバックアップは分散して保存していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 22．ランサムウェアなどの対策として、書き換え不可で複数のバックアップを保存されていますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 23．障害対策として、システムの長期停止を回避するべく、調剤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等、すぐに調剤業務を復旧できる体制整備や、復旧手順の確認をされていますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【12．サイバーセキュリティ】

問 24．サイバーセキュリティに関する組織的対策、職員等や委託先事業者などの対策、技術的な対応・措置、リスク評価を踏まえた対策を検討し、攻撃を受ける前の通常時における対応、攻撃を受けた場合の非常時としての対応、被害から復旧・復帰などのフェーズの対応策をサイバーセキュリティ対応計画として策定し、実践していますか？

□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 25．サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し個人

調査内容

情報漏えいや医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合に、組織内と外部関係機関（事業者、厚生労働省、個人情報保護委員会、警察等）への連絡等の必要な対応を行うための連絡体制が整備されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【13．医療情報システムの利用者に関する認証等及び権限】
問 26．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されていますか？　ID 等の棚卸を定期的に行い不要なものを削除していますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【15．技術的な安全管理対策の管理】
問 27．個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 28．記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、保管及び取扱いに関する作業履歴を残されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

ガイドラインに係る設問　システム運用編

【2．システム設計・運用に必要な規程類と文書体系】
問 29．医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法、医療情報セキュリティ開示書（MDS/SDS）に関する資料を整備し、常に最新の状態が維持されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 30．医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態が維持されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【8．利用機器・サービスに対する安全管理措置】
問 31．医療情報システムにおいて利用する情報機器等は、安全管理の観点から、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されていますか？セキュリティパッチ（最新ファームウェア、更新プログラム）を適用していますか？また、利用に適した状況（ソフトウェアのアップデート状況、脆弱性に関する対応状況等）にあることを定期的に確認していますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問 32．医療情報システムにおいて利用する情報機器等の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確認し、停止していますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【13．ネットワークに関する安全管理措置】
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。

問33．不正な通信の検知や遮断、監視においてファイアウォールの導入や、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）の導入など、「境界防御的な対応」を取られていますか？また、接続元制限を実施していますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問34．「境界防御的な対応」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、内部脅威監視やエンドポイントにおける検知と対応（EDR：Endpoint Detection and Response）の導入など、トラフィックの監視、

調査内容

多層防御の考え方を導入されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問35．特にオープンなネットワークを利用する際に、ネットワーク回線の暗号化や、医療情報自体に暗号化を施していますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

【17．証跡のレビュー・システム監視】
問36．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されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

その他の設問

問37．個人情報漏えいに係る賠償保険に加入されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問38．サイバーセキュリティ事故対応に係る保険に加入されていますか？
□4．概ね対応できている　□3．やや対応できている　□2．あまり対応できていない
□1．ほぼ対応できていない　□0．わからない

問39．医療情報システムの安全管理に関するご意見、およびNPhAデジタル推進委員会の活動に関するご意見がございましたら教えてください。（フリーコメント　任意回答）

問40．回答者の電話番号を教えてください。一人で複数社分をそれぞれ回答される場合は、回答のたびに登録する番号を変更ください。※重複回答を是正するために活用します。なお、同じ番号の回答が確認された場合は、後に回答された方を採用いたします。
〇〇〇〇〇〇〇〇〇〇　※ハイフンなしで入力ください。

以上


NPhA
Nippon Pharmacy Association
日本保険薬局協会