令和７年度ヘルスケア産業基盤高度化推進事業

（ＰＨＲ基本的指針、医療情報関連ガイドラインに関する調査事業）

調査報告書

2026年2月27日

アクセンチュア株式会社

目次

目次

１．はじめに

はじめに

- 経済産業省は、厚生労働省及び総務省とともに、民間 PHR サービスのさらなる利活用に向けて、「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」を令和 3 年 4 月に策定し、策定から3年を経た令和6年度に、対象範囲やクラウド利用時の情報セキュリティ対策などの見直しを検討した。令和7年度は、検討結果を踏まえた改定版のリリース対応に加え、積み残し課題を整理し、次回改定に向けた準備を進めることが求められている。
- また、経済産業省では、総務省とともに、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（以下「2 省 GL」という。）を令和 2 年 8 月に策定し、その後のサイバー攻撃の高度化やクラウド・IoTの普及など環境変化を踏まえ、令和6年度に対象事業者や合意内容の明確化、リスクコミュニケーション強化の観点から改定を行った。
- 医療情報システムは経済安全保障法上の基幹インフラ制度の追加検証対象とされるなど重要性が高まっており、環境変化に対応した継続的な改定や施策検討が必要である。あわせて、2省GLの実効性を確保し、事業者が適切にサービス提供できる体制整備が強く求められている。
- こうした状況に鑑み、本調査では、「厚生労働省が策定した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「厚労省 GL 」という。）に加え、現在経済産業省及び内閣サイバーセキュリティセンター（NISC。現在の国家サイバー統括室（NCO））が取りまとめたサイバーセキュリティ関連ガイドラインの内容も踏まえ総合的な検討を進めることとし、今後2省GLの改定対応の論点整理を行った。

用語の定義

用語	概要
基本的指針	「PHR サービス提供者による健診等情報の取扱いに関する基本的指針」を指す。
2 省 GL	「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」を指す。
SLA	Service Level Agreement（サービスレベル合意）を指す。
サイバーインフラGL	「サイバーインフラ事業者に求められる役割等に関するガイドライン」を指す。
セキュア・バイ・デフォルト	ソフトウェアのセキュリティ機能や設定を最初から（デフォルトで）組み込んだ状態にする理念又は方策のこと。
セキュア・バイ・デザイン	ソフトウェアの設計段階から情報セキュリティを確保するための理念又は方策のこと。
ランサムウェア	コンピュータやデータを使えなくして、元に戻す代わりにお金（身代金）を要求するマルウェアを指す。
サプライチェーン	情報通信技術（ICT）に関わるシステム・サービス・ソフトウェア等の企画・設計・製造・流通・運用等のライフサイクルに関わる各プロセスとそれらを構成する構成要素（システムやソフトウェアの相互依存関係を含む）および組織のこと。
脆弱性	コンピュータのOSやソフトウェア、ネットワーク機器のファームウェア等のプログラムの不具合や設計ミスが原因で発生する、セキュリティ上の欠陥を指す。
EOL	製品・サービスのライフサイクル終了を指す。
EOS	製品・サービスの販売終了を指す。
プライバシーマーク	日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している組織等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度のこと。
WORM機能	Write Once Read Manyの略であり、一度書き込んだデータは変更・削除できず、読み取りだけできる仕組みを指す。
厚労省GL	「厚生労働省が策定した医療情報システムの安全管理に関するガイドライン」を指す。

目次

２．基本的指針に関する調査

本章のサマリ

- 2021年4月に基本的指針については公開がなされているが、健康・医療・介護情報利活用検討会 健診等情報利活用ワーキンググループ 民間利活用作業班（以下、「民間利活用作業班」という。）の第13回~第16回にて指針改定案の検討・作成後、パブリックコメントを経て2025年4月30日の改定版公表に至っている。
- 背景としては、マイナポータルAPI連携拡大に伴う指針の遵守事業者増加の一方、**指針の策定時には想定されていないケース**への対応等、実態に即した指針改定の要請があったこと、データヘルス改革工程表に基づく**電子カルテ情報等のマイナポータル項目追加**を見据え、新たな連携対応へのニーズの高まりがあったこと、最新のセキュリティ対策や技術動向の変化を踏まえた、現行指針における課題整理及び対応が求められたことにある。
- 結果として、今回の改定では、**指針の対象範囲及び最新の情報セキュリティ対策への対応を中心として見直しが実施**されており、指針の対象となる情報の再定義や、対象となる事業者の範囲拡大、最新の情報セキュリティ対策の取り込み、インポート/エクスポート機能の取扱いに関する記述の見直しがなされた。
- 同パブリックコメントにおいては記述内容の補記を求めるものなど比較的軽微なものも多かったが、民間利活用作業班における協議等において**残論点となっていた下記の事項**については、継続協議が求められるところである。
    - 「健診等情報」の具体例として、
        - 乳幼児検診、特定健診、薬剤情報等が挙げられているが、学校健診が含まれていない。**学校健診の心電図等は今後価値が増すのではないか**
        - **医療情報を含むか否か**（健診等情報の概念に医療情報が含まれることには違和感がある）
    - 利用者の同意撤回を回避する**ダークパターンへの言及を指針上行うべきではないか**
- 他方、ガイドライン等国のスタンスとして表示されるものに対しては、市場委縮の懸案もあるため、①PHRサービス利用者に対する質の高い安定的なサービス提供と②PHR市場の成長のバランスを考慮し、今後見直しを検討していくべきである。

指針改定に係る経緯・検討プロセス

- 民間利活用作業班の第13回~第16回にて指針改定案の検討・作成後、パブリックコメントを経て2025年4月30日の改定版公表に至る

指針改定の背景・前提

指針改定の背景

- マイナポータルAPI連携拡大に伴う指針の遵守事業者増加の一方、**指針の策定時には想定されていないケース**への対応等、実態に即した指針改定の要請有
- データヘルス改革工程表に基づく**電子カルテ情報等のマイナポータル項目追加**を見据え、新たな連携対応へのニーズの高まり
- 最新のセキュリティ対策や技術動向の変化を踏まえた、現行指針における課題整理及び対応

指針の改定履歴

- 2021年4月 指針の初版策定
- 2022年4月 指針の一部改定（個人情報保護法の一部改正に合わせ対応）
- 2025年4月30日 指針の改定

指針改定に係る検討プロセス

作業班 第13回（2024年3月） 指針見直しの必要性の合意
基本的指針の適用状況及び民間PHRサービスの現状調査結果を踏まえ、指針の見直しの必要性・課題感を協議

作業班 第14回（2024年11月） 改定の方針・主要論点の協議
指針の主要課題（①「対象とする情報」及び「対象事業者」の定義、②最新の情報セキュリティ対策への対応、③無害化処理の要否、④インポート／エクスポート機能具備の要否）に対する対応方針を協議

作業班 第15回（2024年12月） 改定案の初稿共有
指針及びQ&Aの改定案が共有され、作業班内で大枠合意。以下に関しては今回の改定案には盛り込まず今後の対応事項とされた
- 「健診等情報」の略称見直し
- 利用者同意取得・撤回に関し消費者庁が示しているダークパターン事例の記載 等

作業班 第16回（2025年2月） 改定案の取りまとめ
指針、Q＆A、チェックシートに係る改正内容の最終的な取りまとめ実施

パブリックコメント（2025年3月7日~2025年4月7日）

改定版公表（2025年4月30日）

出典
1. 「PHRサービス提供者による健診等情報の取扱いに関する基本的指針」 https://www.meti.go.jp/policy/mono_info_service/healthcare/phr.html
2. 健康・医療・介護情報利活用検討会 健診等情報利活用ワーキンググループ 民間利活用作業班（第13、第14、15、16回）を参照 https://www.mhlw.go.jp/stf/shingi/other-kenkou_520716_00009.html

今回の改定における主な改定内容

- 今回の改定では、指針の対象範囲及び最新の情報セキュリティ対策への対応を中心として見直しが実施された

主な改定内容	詳細
1. 指針の対象となる情報の再定義	• 指針の対象である**「健診等情報」の定義を一部修正**（以下の下線部） 「個人情報保護法上の要配慮個人情報の内、①個人がマイナポータル API 等を活用して入手可能な健康診断等の情報、②医療機関等から個人に提供され、個人が自ら入力する情報、③個人が自ら測定又は記録を行うものであって、医療機関等に提供する可能性のある情報のいずれかに該当するもの、及び予防接種歴」 • これにより該当データの取得時点では医療機関等へのデータ提供有無が未定であっても、将来的な提供可能性がある限り本指針の対象とみなすように定義解釈を明確化
2. 指針の対象事業者の範囲拡大	• 指針の対象事業者を「民間事業者」から**「PHRサービス提供者」**とし、健診等情報を取扱う**自治体、健保組合、医療機関等**の民間事業者以外のアクターも対象範囲として射程に含めた。対象事業者の変更に合わせて指針の名称も変更 - 指針名(改定前)：民間PHR事業者による健診等情報の取扱いに関する基本的指針 - 指針名(改定後)：PHRサービス提供者による健診等情報の取扱いに関する基本的指針
3. 最新の情報セキュリティ対策への対応	• 関連ガイドライン（中小企業セキュリティGL、クラウドセキュリティGL、NISCハンドブック）を踏まえ、**遵守すべき情報セキュリティ対策項目を再整理**した上で各対策のポイント・対策例を大幅に追記 • ファイル受領時の無害化処理等、改定前は対応方法が限定されていた事項に関して、対象事業者が適切な対策・技術を採用可能な指針に変更
4. インポート/エクスポート機能具備の要否	• 利用者を介したデータの相互運用性確保の観点から、利用者へのデータエクスポート機能は改定前から変わらず具備を求めている • 一方で利用実態が伴っていない**データのインポート機能（データ取込機能）については実装有無の判断をPHRサービス提供者に委ねる方針**に変更

出典
1. 「PHRサービス提供者による健診等情報の取扱いに関する基本的指針（改定点）」 https://www.soumu.go.jp/main_content/001007730.pdf
2. 健康・医療・介護情報利活用検討会　健診等情報利活用ワーキンググループ　民間利活用作業班（第13、第14、15、16回）を参照　https://www.mhlw.go.jp/stf/shingi/other-kenkou_520716_00009.html

パブリックコメント結果

- パブコメを踏まえ、記述内容の平易化や用語・表現の整合性確保の観点から指針・Q&Aを一部変更
  （募集期間：2025年3月7日~2025年4月7日、提出者数：6名、意見項目数：16項目）

意見の分類	意見項目数	提出された意見の要旨・抜粋	指針の変更有無	意見を踏まえた対応方針
情報セキュリティ対策の明確化	2件	• 指針に記載されている情報セキュリティ対策例について、より優しい表現・記述に変更してほしい	**有**	指針内の意見箇所に関して記載を明確化
		• 外国のサーバーが利用されるリスクは考慮されているのか	無	指針内の「外的環境の把握」にて外国でのデータ取扱時の制度把握・安全管理措置を求める旨を記載済みのため原案通り
相互運用性の確保	2件	• 「データ変換時は互換性を担保するような方式とすること」とあるが、「データ変換」が何を指しているか読み取れず、Q&A等で補足してほしい • 「データ提供先のPHRサービス提供者の本指針への遵守状況を定期的に確認」とあるが、確認方法の具体的な内容を読み取れない	**有**	指針内の意見箇所に関して指針・Q&Aを追記
用語・表現の整合性	7件	• リスクアセスメントの定義に準じ、「リスクアセスメント（リスクの特定・評価・分析）」を「リスクアセスメント（リスクの特定・分析・評価）」に変更する • 「リスク管理」と「リスクマネジメント」の用語を統一する ※ 指針変更の対象となった意見を抜粋・記載	**一部有** （7件中2件）	意見を踏まえ必要修正と判断されたものは指針内の記載を変更。修正不要と判断されたものは指針内の記載意図・根拠を含め回答
データのトレーサビリティ・改ざん防止体制	2件	• トレーサビリティは確保されているのか。PHRの情報の不要な拡散を防ぐ情報の流れをすべて把握できるのか • 大元のPHRデータ改ざん防止は国が対策をとるべきではないか	無	指針内の「データ提供先の適切性の確認」にて、PHRサービス提供者自身が、適切なデータ提供先であることを確認し提供すべき旨を記載済みのため原案通り
PHRサービスの分類	1件	• PHRサービスの分類を明確化・厳密に定義すべき	無	本指針はPHRサービス全体での遵守事項を定めたものである旨、指針内で分類を定めるのは自由なサービス創出を阻害する懸念があるため変更無
個人情報保護・プライバシーに関する懸念・不安の声	2件	• 個人の健康情報をネットに登録したくない • 個人の知らない所で悪用・流出されないか不安	無	本指針はあくまで本人同意に基づいて取得した個人情報を前提としている旨を回答

「PHRサービス提供者による健診等情報の取扱いに関する基本的指針（案）に対する意見と回答」（https://www.soumu.go.jp/main_content/001007729.pdf）に基づき作成。

次回の改定に向けた課題、積み残し事項

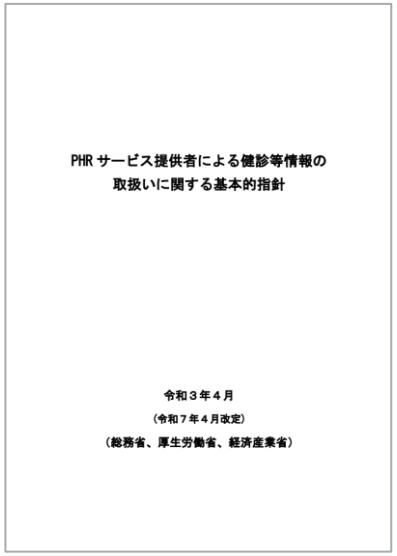
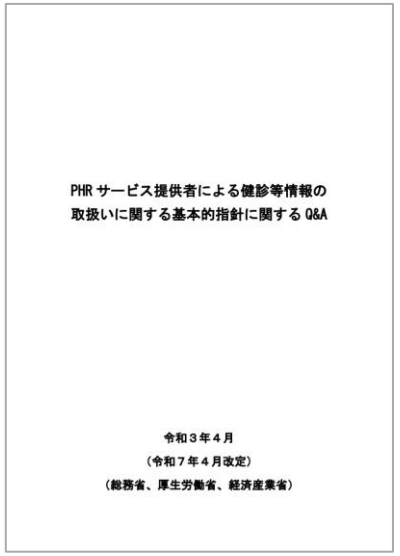
- 作業班では指針の対象情報のあり方や利用者の同意取得/撤回に関する議論がなされたものの、今回の改定では盛り込まれず次回改定への積み残し事項となった

#	論点	課題・積み残し事項	具体的な議論内容
1	**指針対象の情報である「健診等情報」の取り扱い範囲の見直し**	「健診等情報」の具体例に学校健診を追加	• 「健診等情報」の具体例として、乳幼児検診、特定健診、薬剤情報等が挙げられているが、学校健診が含まれていない。学校健診の心電図等は今後価値が増すのではないか
2		「健診等情報」の略称自体の見直し	• 作業班開催当初は健診に焦点が置かれていたために現名称となっている一方で、現在の定義では、健診等情報の例示として「診療情報（なお、薬剤情報、検査情報等も含む）」という記載がある • 医療機関側の目線では診療情報が健診等情報に含まれることに違和感がある。どこからが健診等情報の対象範囲か分かりにくい • 今後医療情報等が含まれることも踏まえて略称を見直すべきではないか
3	**PHRサービス利用者同意の取得/撤回**	利用者の同意撤回を困難にする「ダークパターン」への対策の明記	• 消費者庁にて同意を撤回しにくいダークパターンの事例が挙げられている。指針内でもダークパターンに言及すべきではないか

出典
1. 健康・医療・介護情報利活用検討会 健診等情報利活用ワーキンググループ 民間利活用作業班（第15、16回）を参照 https://www.mhlw.go.jp/stf/shingi/other-kenkou_520716_00009.html

Appendix. 基本的指針、チェックシート、Q&A

- 基本的指針、チェックシート及びQ&Aの最新版については経済産業省HPに掲載されている

	指針	チェックシート	Q&A
文書名	PHRサービス提供者による健診等情報の取扱いに関する基本的指針	PHRサービス提供者による健診等情報の取扱いに関する基本的指針に係るチェックシート	PHRサービス提供者による健診等情報の取扱いに関する基本的指針に関するQ&A
参照リンク	https://www.meti.go.jp/policy/mono_info_service/healthcare/00phrshishin_20250428.pdf	https://www.meti.go.jp/policy/mono_info_service/healthcare/02phrchecksheet_20250428.xlsx	https://www.meti.go.jp/policy/mono_info_service/healthcare/01phrqa_20250428.pdf
イメージ			

目次

３．２省GLに関する調査

①厚労省 GL を踏まえた、2 省 GLの実効性確保のための施策の検討（p.17）
②「サイバーインフラ事業者に求められる役割等に関するガイドライン」を踏まえた、医療情報システムにおける経済安全保障のための調査（p.81）
③2 省 GL の対象事業者についての調査（p.90）

目次

本章のサマリ

- 今後の2省GLの改定に向けて、**焦点をあてて対応すべき観点**と**体裁・書きぶりとして見直しが必要な観点**について整理。
    - 焦点をあてて対応すべき観点：
        - **事業者規模等にも考慮した改定に向けた方向性仮説**を提示
          （サプライチェーン全体のリスク管理と透明性の確保、サイバー攻撃（ランサムウェア）対応型のバックアップと復旧支援、高度な認証方式（多要素認証）の実装など）
        - **実効性確保策の仮説**についても整理を実施
          （「最低限要求事項」と「推奨事項」の明確化（パッケージ化）、「サービス仕様適合開示書」の記載項目の改定、リスクコミュニケーションの義務化に近い規定など）
    - 体裁・書きぶりとして見直しが必要な観点：
        - **対応Lv１：方向性**、**対応Lv2：対応必要事項**を加筆・補足
- セキュリティ専門家及び情報セキュリティ事業者に対し、有識者ヒアリングを実施。
    - 2省GLの改定に当たっては、**サプライチェーン責任の明確化**、**中小事業者への負担軽減とセキュリティ確保のバランス**といった論点を協議していくことが、実効性確保につながると考えられる。
    - 有識者ヒアリング実施結果を踏まえ、2省GLそのものの見直しではないが、実効性を高めるための施策としては、**モデル契約書・仕様書条文の別冊化・提供**といった施策が有効と考えられる。

調査方針・実施内容

- 焦点をあてて対応すべき観点と、体裁・書きぶりとして見直しが必要な観点について整理

1.焦点

焦点をあてて対応すべき観点　p20~p27

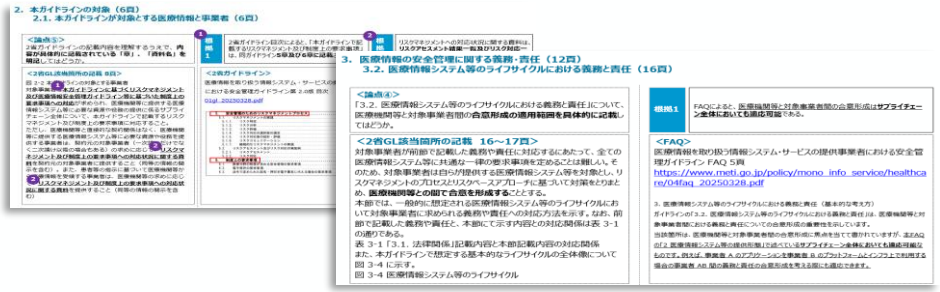
- 焦点をあてて対応すべき観点（※）を抽出、今後のガイドライン改定議論に向けた論点出しを精緻化
- 精緻化にあたっては社内知見者、有識者ヒアリングを通じて実効性の担保としての施策をブラッシュアップ

※焦点をあてて対応すべき観点は、①サプライチェーン全体のリスク管理と透明性の確保、②サイバー攻撃（ランサムウェア）対応型のバックアップと復旧支援、③高度な認証方式（多要素認証）の実装、④安全なネットワーク接続と暗号化通信、⑤保守・運用におけるデータの保護とアクセス管理、⑥非常時における「縮退運用機能」と「緊急用アカウント」の実装、⑦.監査証跡（ログ）の保全性と分析支援機能の提供、⑧ソフトウェア・製品のライフサイクル（EOL/EOS）と脆弱性の能動的通知の8観点を指す。

2.体裁

体裁・書きぶりとして
見直しが必要な観点　p28~p75

- 定義の明確化等にあたって考慮が必要な事項について整理



2省GLの実効性を高める施策の検討の進め方

1.焦点　2.体裁

- 調査内容及び有識者ヒアリング事項については、以下のアプローチで実施

	机上調査（仮説）			有識者ヒアリング		とりまとめ
Output	調査仮説v1	調査仮説v2	ヒアリング仮説v1		ヒアリング議事録、サマリ	本調査まとめ
方針	• 厚労GL踏まえた2省GLの反映すべき観点仮説を作成済み • 現場の実務レベルに精通した論点出しとなっているか、観点の正確性、現場理解・影響度の観点を考慮するべく、弊社内の電カル導入実績がある者等の聞き取りを実施中	• 事前把握対象をリサーチパネル（対外有識者）も含め、クイックに状況を把握 • 1/30、2名の事前インタビューを実施済み	• 全体の観点を整理し、ヒアリング仮説として2/3に提示済み • 現在各ヒアリング対象別のヒアリング内容について整理 • ヒアリング仮説を基に、貴省にて関係者へのお声掛けを行っていただく	• 有識者ヒアリング仮説に基づき、各者ヒアリング実施。 • 有識者ヒアリングにあたっては、既存メンバーとしつつ、社内の電カル導入・担当等を経験したことのある者を同席させ、質疑の質を担保 • 回答の質を担保する観点からは、10件実施/ショートで行うよりも、一定絞って深堀ヒアリングとする		• 左記内容について、今後2省GLの改定議論にあたって協議すべき論点をとりまとめる

改定に向けた方向性仮説（1/3）

1.焦点　2.体裁

- 規模等にも考慮した改定に向けた論点出しを提示

	概要	改定に向けた方向性仮説	根拠
1. サプライチェーン全体のリスク管理と透明性の確保	• 医療機関等は委託先の監督義務を負うが、クラウドサービス等の普及により、事業者側の再委託先（サプライチェーン）の管理が不可欠	• 事業者は、再委託先を含むサプライチェーン等の管理状況について可視化し、医療機関等へ「サービス仕様適合開示書」等を用いて正確に情報提供すること。特に、SaaSベンダはSaaSベンダが当該再委託先をも含む責任範囲までを含め提示し、事業者は、再委託先の詳細リスト提出が困難な場合、再委託先等に起因するインシデントについても、元請け事業者が一切の免責なく賠償・復旧責任を負う」旨をSLAおよび契約約款に明記すること。 • SaaS利用時において、医療機関が直接関与できない「再委託先（IaaS/PaaS事業者等）」のリスクについて、プライム事業者が「自社の責任において再委託先のセキュリティ状態を監査・保証する」旨を契約条項に盛り込むことを、2省GLのモデル契約等で標準化すべきではないか。 • クラウドサービスの設定ミス（公開範囲など）による事故を防ぐため、事業者は「医療機関向けにセキュアに設定済みのテンプレート」を提供する責務を負い、医療機関側が設定変更しない限り安全が保たれる状態を「納品」の定義とすべきではないか。	• 厚労省GL企画管理編 7.2（委託先事業者管理）、7.4（委託先事業者選定）において、医療機関等は事業者のセキュリティ対策状況を確認し、再委託が行われる場合はその体制も管理することが求められているため
2.サイバー攻撃（ランサムウェア）対応型のバックアップと復旧支援	• ランサムウェア被害の拡大を受け、単なるバックアップではなく「復元可能なバックアップ」が求められる	• 事業者は、バックアップデータがランサムウェアの影響を受けないよう、オフライン保管や不変性（WORM機能）を標準機能またはオプションとして具備し、医療機関等が専門的な設定を行わずともランサムウェア対策が機能する状態を提供すること。また、システム復旧手順を整備し、医療機関等と共同で訓練を実施できる体制を提供すること。 • 他方、災害等の復旧対応、パッチ処理にかかる対応期間は相応に要することから、例えばベンダ切り替え時に行うなど現場のオペレーションに影響のない稼働・運用で行うことについて、事業者から提案を行うこと。加えて、ベンダが不正アクセスを受けている状況を把握する観点から、ベンダのセキュリティ基準も提出させること。	• 厚労省GLシステム運用編 18.1（サイバーセキュリティ対応）において、バックアップデータのネットワークからの切り離しや、3世代以上の管理が強く求められているため。
3.高度な認証方式（多要素認証）の実装	• なりすまし対策として、認証強度を高めることが求められている	• 2027年度を皮切りに原則として二要素認証（多要素認証）を採用したシステムを設計・提供することを明記すること。ただし、導入コストや業務効率への影響が大きい場合、「場所や端末による制限（リスクベース認証）」等の代替策を提案・実装し、段階的な移行計画（2027年に向けたロードマップ）を提示すること。 ※救急対応を考慮し、物理専用カードを有していなければ入ることのできない等の環境上の配慮がなされている場合には、システム自体の２要素認証の運用を緩和することは可能とすることを検討論点として提示すること	• 厚労省GLシステム運用編 14.1.1（利用者の識別・認証）において、令和9年度以降の二要素認証の原則採用が明記された

改定に向けた方向性仮説（2/3）

1.焦点　2.体裁

- 規模等にも考慮した改定に向けた論点出しを提示

	概要	改定に向けた方向性仮説	根拠
4.安全なネットワーク接続と暗号化通信	• 外部からの接続におけるセキュリティ強度の確保	• オープンなネットワーク（インターネット等）を利用する場合は、TLS1.3（または1.2以上）の高セキュリティ設定をデフォルト（初期設定）とし、部門システム等のサブシステムにおいても、不要な通信ポートの閉塞や相互認証機能が有効化された状態で納品すること。なお、これら設定にあたっては、インフラ専門のメンバーを参画させるとともに、変更不可の事項についてはあらかじめ医療機関に伝達し、不本意な設定変更が起きないよう留意すること。	• 厚労省GLシステム運用編 13.1.2（選択すべきネットワークのセキュリティ）および遵守事項⑥において、具体的なプロトコルバージョンと認証方式が指定されているため
5.保守・運用におけるデータの保護とアクセス管理	• リモートメンテナンス時の不正防止	• リモートメンテナンスを行う際は、医療機関等の許可を得た上で行い、アクセスログを記録・保存すること。また、原則として個人情報を含むデータを医療機関外へ持ち出さない（コピーしない）運用を徹底すること。また、医療機関側が操作を許可・監視できる機能、または作業内容（操作ログや画面録画等）を事後的に医療機関側が容易に確認できるレポート機能を提供し、不正がないことを客観的に証明可能とすること。	• 厚労省GLシステム運用編 10（事業者による保守対応等に対する安全管理措置）において、保守作業時のデータ持ち出し禁止やログ収集が義務付けられている
6. 非常時における「縮退運用機能」と「緊急用アカウント」の実装	• ランサムウェア攻撃やネットワーク障害時、電子カルテが全停止すると診療が止まってしまう。厚労省GLでは非常時の対応を求めるが、システム側で「非常時モード」が用意されていないと現場は対応できない	• ネットワーク遮断時でも、ローカル端末やスタンドアローン環境で最低限の診療記録・参照が可能となるローカル端末での参照・入力機能（縮退運用モード）を具備し、その切り替え及び復旧手順をマニュアル化して提供すること。SaaSにおいても同様の措置を講じること • 通常時の認証サーバーが利用できない場合に備え、「非常時用ユーザアカウント」によるログイン機能を実装し、かつ通常復帰後にその利用履歴を監査できる仕組みを提供すること	• 厚労省GLシステム運用編 11.1「通常時における運用対策」および 11.2「非常時における対応」において、非常時用ユーザアカウントの運用や、ネットワーク障害時の代替手段の確保が求められているため

改定に向けた方向性仮説（3/3）

1.焦点　2.体裁

- 規模等にも考慮した改定に向けた論点出しを提示

	概要	改定に向けた方向性仮説	根拠
7. 監査証跡（ログ）の保全性と分析支援機能の提供	• サイバー攻撃発生時、ログが改ざんされたり、解析困難な形式であったりすることが原因究明を遅らせることになる	• アクセスログや操作ログを、利用者（攻撃者）が容易に削除・改ざんできない領域（WORM機能を持つストレージやクラウド上の別領域等）へリアルタイムに転送・保存する機能や、インシデント発生時に医療機関等がログを抽出・提出しやすいツールやインターフェースを標準提供すること。この対応にあたっては、●年●月を目途として、反映を完成させること • 医療機関の担当者が異常を検知できるよう、ログの「分析・可視化ツール」または「アラート機能」を標準提供すること。	• ・厚労省GLシステム運用編 17.1「証跡のレビュー」において、ログの定期的チェックによる不正利用確認が求められており、17.2「監査の実施の支援」で証跡の整理が求められている。 • （また、サイバーインフラGL案 S(1)-4「サービスのモニタリング」でも監視環境の整備が求められている）
8. ソフトウェア・製品のライフサイクル（EOL/EOS）と脆弱性の能動的通知	• 病院調査結果（病院における医療情報システムのサイバーセキュリティ対策に係る調査結果）では、サーバやPCへのパッチ適用率が61%と低く、管理不全が明らか。事業者が「売っておしまい」にしない責務が必要	• 提供するシステムを構成するOS、ミドルウェア、ライブラリのサポート終了期限（EOL/EOS）一覧を契約時および毎年度提示すること。 • 利用中のシステムに影響する脆弱性が発見された場合、医療機関が情報を取りに行くのではなく、事業者から「プッシュ型」で通知し、具体的な回避策やパッチ提供時期、適用計画を具体的に提示すること。なお、一義的には、用いられているPCにかかるOSのアップデートは医療機関の責において行い、その頻度に合わせてベンダもパッチ適用及び影響発生時の対処も含め十分な期間をとり、協調のもと対処することとし、外部のヘルスチェックシステム等も活用しながら対応を図ること。	• 厚労省GLシステム運用編 8.2「情報機器等の脆弱性への対策」において、EOS対象機器への攻撃リスクへの対応が求められているため • （サイバーインフラGL案 S(2)-4.1 において、利用終了（廃棄・提供終了）に係る情報の継続的提供が求められているため）

2省GLの実効性確保策 仮説（1/2）

1.焦点　2.体裁

- 実効性確保策の仮説についても整理を実施

	概要	狙い
1.「最低限要求事項」と「推奨事項」の明確化（パッケージ化）	• サイバーインフラGL案の考え方を取り入れ、2省GLの要求事項を「医療情報システムとして最低限満たすべき必須項目（2要素認証の実装、オフラインバックアップ対応等）」と「推奨項目」に分類して記載する。	• 医療機関等が調達仕様書を作成する際、事業者が「必須項目」を満たしていない場合は選定対象外としやすくし、遵守圧力を高める。
2.「サービス仕様適合開示書」の記載項目の改定	• 厚労省GL 6.0版で重要視されている「ランサムウェア対策（バックアップの世代・媒体管理）」、「サプライチェーン（再委託先）の管理体制」、「緊急時の連絡・支援体制」を具体的なチェック項目として追加し、事業者としての対応・責任範囲を明確化する。さらに、医療機関における他のシステム開発者等と連携して対応が必要となりうる事項を可視化し、医療機関からの照会先が判別しやすくなるよう、他事業者との協力・事前調整に最大限協力することを各事業者に求める	• 医療機関等が事業者を評価する際の「ものさし」を最新の脅威に対応したものに更新する
3. リスクコミュニケーションの義務化に近い規定	• 事業者が医療機関等に対し、自社システムのリスク（残留リスク）や責任分界（どこまでを事業者が守り、どこからが医療機関の責任か）を「契約前に」文書で説明し、合意形成することを、ガイドライン上でより強く求める記述に変更する	• 徳島県つるぎ町立半田病院」の事例にあるような、責任分界の認識齟齬による対策漏れを防ぐ
4.「モデル契約書・仕様書条文」の別冊化と提供	• 医療機関の担当者はITの専門家ではないため、ガイドラインを読んでも「契約書のどこにどう書けばいいか」が分からないため、2省GLの別冊として、「2省GL準拠のためのモデル契約条項」や「調達仕様書にそのままコピー＆ペーストできる非機能要件リスト」を作成・添付する	• 医療機関はこれを提示するだけで、事業者に対して2省GLレベルの要求を行うことができ、遵守圧力が契約ベースで高まる（厚労省GL企画管理編 5.2.1「契約管理」において、責任分界等を契約で明確にすることが求められている）
5.サービス類型別（オンプレ/クラウド/SaaS）の「責任分界点マップ」の標準化	• クラウド利用時、OSのパッチ当てやバックアップが「事業者の責任」か「医療機関の責任」か曖昧なまま運用され、事故時に露呈するケースが多い。AWS等の「責任共有モデル」を参考に、医療情報システムに特化した「責任分界点マップ（標準テンプレート）」を2省GLで定義し、契約時の必須添付資料とする。具体的な項目例として、OSアップデート、ウイルス対策ソフトの更新、バックアップの実施、ログの監視、障害時の復旧作業等。	• 隙間のない責任分担が可視化され、事業者の「やるべきこと」が明確にする

2省GLの実効性確保策 仮説（2/2）

1.焦点　2.体裁

- 実効性確保策の仮説についても整理を実施

	概要	狙い
6.「2省GL適合宣言マーク（仮）」の創設と普及	• 2省GLの「最低限要求事項」を満たしていること（サービス仕様適合開示書を適切に公開していること等）を自己宣言した事業者に対し、ロゴマーク等の使用を認める制度を検討する。	• 医療機関向けに「このマークがある事業者は、厚労省GL 6.0版への対応がスムーズです」と広報し、事業者に対しては「マーク取得が調達の必須条件になりうる」というインセンティブを付与する
7.「医療機関向け 調達チェックリスト」の配布（翻訳ツールとしての活用）	• 2省GLの専門的な内容を、医療機関の担当者が調達時に事業者に突きつけられる「質問票（チェックリスト）」形式に噛み砕いた資料を作成し、配布する。具体的には、「御社のシステムは2027年必須の多要素認証に対応していますか？」「ランサムウェア対策としてバックアップはネットワークから切り離せますか？」といった、Yes/Noで答えさせる形式にする。	• 病院団体やMEDIS等を通じて配布し、事業者に「これに答えられないと契約できない」という危機感を持たせることで、間接的に2省GLの遵守を促す。
8.中小規模事業者向けの「セキュリティ実装ガイド」の提供	• リソースの乏しい中小ベンダー（介護系ソフトや部門システムベンダー等）向けに、2省GLを遵守するための具体的な技術実装例（AWS/Azureでの設定例や、オープンソースでのVPN構築例など）を示した技術ガイドを提供する。なお、部門システムは、基幹システムと一体でセキュリティを担保できる仕組みを実装するなど、安全かつ低廉になる運用を提案する等の付記を行うこと	• JAHIS等の業界団体と連携し、技術セミナーを開催する。単なるルールの押し付けではなく、「どうすれば低コストで安全に実装できるか」という支援策として周知する。
9.「医療情報システム安全管理責任者」向け研修と「事業者認定」の連動	• 事業者への周知だけでは不十分で、発注側（医療機関）の目利き力が不足している。 • 事業者向けには、医療情報システムを提供するベンダーのエンジニアや営業担当向けに「2省GL適合実務者研修（仮）」を実施し、受講修了者を公表する。さらに当該研修修了者が医療情報システム導入/改修に係るプロジェクトに参画することが望ましい。 • 医療機関向けとして、 病院団体や学会（医療情報学会等）を通じて、「システム調達時は、この研修を受けた担当者がいる事業者を選ぶと、厚労省GL対応がスムーズ」など周知	• 事業者にとって「2省GLを理解していること」が営業上の武器となり、自律的な学習と遵守が進むことが見込まれる。また、サイバーインフラGL案S(4)-1 で求められる「各役割のトレーニング」の実践にもなりうる

（参考）２省GLと厚労GLの比較

- 両GLは、医療機関等（発注者）と事業者（受注者）の立場の違いによるギャップを前提に、**医療機関等が厚労省GLに基づき要求を提示し、事業者が2省GLに基づいて契約適合性やリスクを説明・合意することで医療情報の安全性を担保する**共同規制モデルとして整理されている

項目	厚生労働省ガイドライン (厚労GL)	経産省・総務省ガイドライン (2省GL)
対象	医療機関等（病院、診療所、薬局など）	事業者（ITベンダー、クラウド事業者など）
法的性質	医療法等に基づく管理者の義務を具体化したもの（**管理者が遵守すべき最終責任**）	**事業者が**医療機関等の**責任・履行を支援するための技術的・管理的要件**（契約や説明責任の基準）
役割	ガバナンスの主体 「どのような安全対策が必要か」を決定し、事業者を監督する立場	リソースの提供主体 「要求された対策をどう実現するか」を提示し、サービスを提供する立場
関係性	委託先（事業者）を監督する義務を負う	医療機関等に対してリスクや対策状況を説明し、合意形成を図る義務を負う

（参考）２省GLが主眼としているポイント

- 2省GLでは、**事業者と医療機関の間にある情報の非対称性を埋め、信頼関係を構築するための「プロセス」と「境界」に焦点を当てている**と理解

ポイント	概要	2省GL上の記載箇所
1 **リスクベースアプローチとプロセスの重視**	• 一律のセキュリティ対策リスト（チェックリスト方式）を提示するのではなく、**提供するサービスの特性に応じた「リスクマネジメントプロセス（特定・分析・評価・対応）」の実践**に焦点を当てる • 事業者は自らリスクを分析し、なぜその対策が必要なのか（あるいは不要なのか）を論理的に説明することが求められる	• 5. 安全管理のためのリスクマネジメントプロセス （25～55頁）
2 **リスクコミュニケーションと合意形成（SLA）**	• **医療機関等に対する「説明義務」と「合意形成」**に強く焦点を当てる ➢ 透明性の確保：「サービス仕様適合開示書」や「MDS/SDS」等を用い、ブラックボックスになりがちなクラウドサービス等の内部管理状況を可視化すること ➢ 責任分界の明確化： 障害時やサイバー攻撃時に「どこまでが事業者の責任で、どこからが医療機関の責任か」を明確にするため、SLA（Service Level Agreement）の締結や責任分界点の合意を重視	• 5.1.6 リスクコミュニケーション（36～40頁）
3 **サプライチェーン全体のリスク管理**	• 自社だけでなく、**再委託先（IaaS/PaaS事業者など）を含めたサプライチェーン全体の管理**に焦点を当てる • 特にクラウドサービスが多層構造（SaaSがPaaSを利用し、そのPaaSがIaaS上で動く等）になる中、医療機関からは見えにくい下位レイヤーのリスク管理と、その情報の医療機関への伝達を事業者の責務と定義	• 5. 安全管理のためのリスクマネジメントプロセス （25～55頁）
4 **「患者等の指示」に基づくデータ流通への対応** ※近年の焦点	• 従来の「医療機関との契約（BtoB）」だけでなく、PHR（Personal Health Record）のように「患者等の指示に基づいて医療情報を受領する事業者」を新たな対象として定義 • **医療機関との直接契約がない場合でも、医療情報のエコシステムに参画する事業者として、適切な安全管理と説明責任を果たすべきという、データ流通の多様化**に焦点を当てた新しい規制の枠組み	• 2.1 本ガイドラインが対象とする医療情報と事業者（6～9頁）

2省GLの整理　― 目次一覧（1/2） ―

1.焦点　2.体裁

- 作業範囲及び対応レベルを一覧で記載

項目1GL	項目2	項目3	レベル1	レベル2	GL該当頁
2. 本ガイドラインの対象	2.1. 本ガイドラインが対象とする医療情報と事業者	―	○	○	6頁
3. 医療情報の安全管理に関する義務・責任	3.1. 法律関係	3.1.1. 安全管理義務	○	○	12頁
		3.1.2. 対象事業者の説明義務	○	○	14頁
		3.1.3 情報セキュリティ事故等発生時における義務と責任	― （論点なし）	― （論点なし）	15頁
	3.2. 医療情報システム等のライフサイクルにおける義務と責任	―	○	○	16頁
		3.2.1. 契約前の合意形成及び契約中の合意の維持	― （論点なし）	― （論点なし）	17頁
		3.2.2. 通常時の義務	○	○	18頁
		3.2.3. 危機管理対応時の義務及び責任	○	○	19頁
4. 対象事業者と医療機関等の合意形成	―	―	○	○	20頁
	4.1. 医療機関等へ情報提供すべき項目	―	― （論点なし）	― （論点なし）	20頁
	4.2. 医療機関等との役割分担の明確化	―	― （論点なし）	― （論点なし）	22頁
	4.3. 医療情報システム等の安全管理に係る評価	―	― （論点なし）	― （論点なし）	23頁

2省GLの整理　― 目次一覧（2/2） ―

- 作業範囲及び対応レベルを一覧で記載

項目1	項目2	項目3	レベル1	レベル2	GL該当頁
	4.4. 対象事業者の適格性を評価する第三者認証等の取得に係る要件	―	○	○	23頁
5. 安全管理のためのリスクマネジメントプロセス	5.1. リスクマネジメントの実践	―	― （論点なし）	― （論点なし）	27頁
		5.1.1 リスク特定	○	○	27頁
		5.1.2. リスク分析	○	○	29頁
		5.1.3. リスク評価	― （論点なし）	― （論点なし）	30頁
		5.1.4. リスク対応の選択肢の選定	― （論点なし）	― （論点なし）	30頁
		5.1.5. リスク対応策の設計・評価	○	○	32頁
		5.1.6. リスクコミュニケーション	― （論点なし）	― （論点なし）	36頁
		5.1.7. 継続的なリスクマネジメントの実践	― （論点なし）	― （論点なし）	40頁
6. 制度上の要求事項	6.1. 医療分野の制度が求める安全管理の要求事項	―	○	○	56頁

2省GLの整理

1.焦点　2.体裁

論点なし

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜論点無し＞

本ガイドラインが対象とする事業者の定義については、①～③の定義で一定網羅できているため、**論点無しとする**。

＜2省GL該当箇所の記載 6頁＞

本ガイドラインが対象とする医療情報は、「医療に関する患者情報（個人識別情報）を含む情報」である。この定義は医療情報安全管理ガイドラインにおける定義と同一である。医療情報には、医療従事者が作成・記録した情報のほか、医療従事者の指示に基づき介護事業者が作成・記録した情報がある。これらの医療情報は、その情報を作成・記録した者が所属する医療機関等で保管される場合や、その医療機関等から他の医療機関等に提供される場合のほか、患者等（患者本人のほか、患者の家族等で、患者の医療情報を閲覧する権限を有する者を含む。以下同じ）に提供される場合が想定される。

本ガイドラインが対象とする事業者は、①医療機関等との契約等に基づいて医療情報システム等を提供する事業者、②医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者、③患者等の指示に基づいて医療機関等から医療情報を受領する事業者（以下、これらを総称して「対象事業者」という。）である。

2省GLの整理

1.焦点　2.体裁

論点①

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜論点①＞

FAQで回答されている、「保守契約」の記載を注釈に記載してはどうか。

＜2省GL該当箇所の記載 6頁＞

①における「医療機関等との契約等に基づいて」にある「契約等」には、医療情報システム等の運用又は管理、**保守11等に関する契約等が含まれる。**例えば、医療機関等の外部において医療情報の保存等を行うサービス等の提供契約も、「契約等」として挙げられる。しかし、医療情報システム等の売買契約等のみであり、運用又は管理、保守に関する契約等がない場合は、「契約等」に含まれない。

＜注釈部分＞

11 保守契約の具体的な内容については、FAQ に記載。

根拠1

「保守契約」の定義について、**2つのケースに分類し、ここでは請負などの医療情報システム等事業者の判断で保守を行うケースを指している。**

＜FAQ＞

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 FAQ 2頁

https://www.meti.go.jp/policy/mono_info_service/healthcare/04faq_20250328.pdf

1.3. 本ガイドラインの対象となる保守はどのような場合か？

保守の形態については、保守要員を医療機関等に派遣し、医療機関等の指示に基づいて保守を行うケースと、請負などの医療情報システム等事業者の判断で保守を行うケースなどがあります。本ガイドラインでは前者のような、医療機関等の指示に基づいて保守を行うケースは含まれません。

明確に保守契約を締結しない場合でも、システム等の保守についてリモート保守を行う旨を、サービス規約等に含めている場合には、保守契約がある場合に含まれます。

また、製品やソフトウェアの提供者で、製品保証としてセキュリティパッチの提供等のみを行っている事業者については、本ガイドラインの対象範囲外となります。

2省GLの整理

1.焦点　2.体裁

論点①

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜対応Lv1：方向性＞

- 「保守契約」の定義について、FAQでは、2つのケースに分類したうえで、請負などの医療情報システム等事業者の判断で保守を行うケースを指しているが、**事業者が通常想定している「保守契約」とは異なるため、保守契約の具体的な内容をガイドラインの注釈部分に記載**してはどうか。

＜対応Lv2：対応必要事項＞

- ①における「医療機関等との契約等に基づいて」にある「契約等」には、医療情報システム等の運用又は管理、**保守11**等に関する契約等が含まれる。例えば、医療機関等の外部において医療情報の保存等を行うサービス等の提供契約も、「契約等」として挙げられる。しかし、医療情報システム等の売買契約等のみであり、運用又は管理、保守に関する契約等がない場合は、「契約等」に含まれない。

＜注釈部分＞

- **11 保守の形態については、保守要員を医療機関等に派遣し、医療機関等の指示に基づいて保守を行うケースと、請負などの医療情報システム等事業者の判断で保守を行うケースなどがある。本ガイドラインでは前者のような、医療機関等の指示に基づいて保守を行うケースは含まれない。明確に保守契約を締結しない場合でも、システム等の保守についてリモート保守を行う旨を、サービス規約等に含めている場合には、保守契約がある場合に含まれる。また、製品やソフトウェアの提供者で、製品保証としてセキュリティパッチの提供等のみを行っている事業者については、本ガイドラインの対象範囲外となる。**

2省GLの整理

1.焦点　2.体裁

論点②

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜論点②＞

該当箇所の「医療情報システム等」の説明について、**FAQ記載の「医療情報システム等の提供形態（基本的な考え方）」を追加してはどうか。**

＜2省GL該当箇所の記載 6頁＞

「医療情報システム等」には、原則、検査機器等の医療機器は含まれない。ただし、医療機関等との契約等があり、かつ、医療情報システム等とネットワークにより接続される場合は、医療機器であっても、「医療情報システム等」に含まれる。なお、「医療従事者の指示に基づいて作成・記録した情報」を含む医療情報を取り扱う介護事業者が利用するシステムも、「医療情報システム等」に含まれる。

根拠1

該当ガイドライン箇所に対して、貴省のFAQに「2. 医療情報システム等の提供形態（基本的な考え方）」の記載がされているが、ガイドラインに**「サプライチェーン」等の重要な用語が記載されていない。**

＜FAQ＞

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 FAQ 3頁

https://www.meti.go.jp/policy/mono_info_service/healthcare/04faq_20250328.pdf

2. 医療情報システム等の提供形態（基本的な考え方）
本ガイドラインでは、医療情報システム等は、サプライチェーン全体を通して、適切に運用されるべきというのが基本的な考え方です。本ガイドラインは医療機関等と直接的な契約関係のない事業者も**医療情報システム等のサプライチェーンの一部として機能している場合、本ガイドラインの適用範囲になります**。例えば、事業者 A が病院にクラウド型電子カルテサービスを提供する際、事業者 A はアプリケーションとプラットフォームを事業者A が選定した事業者 B のインフラ上で稼働させる場合、事業者 A は事業者 B のインフラが、医療情報システム等のサプライチェーンの一部として、本ガイドラインに沿ったサービスを提供しているか確認すべきであるというのが基本的な考え方です。

根拠2

貴省のガイドラインの 用語集 60頁では、**「医療情報システム等：医療情報を取り扱うシステムやサービス」**のみの記載である。

＜用語集＞

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第 2.0 版　用語集 60頁

https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20250328.pdf

用語	内容
(Manufacturer / Service Provider Disclosure Statement for Medical Information Security)	ービス事業者による医療情報セキュリティ開示書（SDS）」の略称で、（一社）保健医療福祉情報システム工業会（JAHIS）及び（一社）日本画像医療システム工業会（JIRA）が定めた各製造業者/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）のこと。これらの書式は製品/サービスの説明の一部として製造業者/サービス事業者が作成し、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に用いられることが想定されている。
SLA (Service Level Agreement)	書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書(JIS Q 20000-1:2020)。
VPN（仮想私設網、Virtual Private Network）	不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のこと。
アクセスポイント	通常は、無線 LAN アクセスポイントを指す。ノートパソコンやスマートフォン等の無線 LAN 接続機能を備えた端末を、相互に接続したり、有線 LAN 等、他のネットワークに接続するための機器。
医療機関等	病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等。
医療情報システム等	医療情報を取り扱う情報システムやサービス

2省GLの整理

1.焦点　2.体裁

論点②

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜対応Lv1：方向性＞

1 該当箇所の、**「医療情報システム等」の記載をFAQをもとに記載**を行う。

2 併せて、貴省のガイドラインの用語集60頁の「医療情報システム等」の説明文に上記記載を追記する

＜対応Lv2：対応必要事項＞

- 「医療情報システム等」には、原則、検査機器等の医療機器は含まれない。ただし、医療機関等との契約等があり、かつ、医療情報システム等とネットワークにより接続される場合は、医療機器であっても、「医療情報システム等」に含まれる。なお、「医療従事者の指示に基づいて作成・記録した情報」を含む医療情報を取り扱う介護事業者が利用するシステムも、「医療情報システム等」に含まれる。**なお、医療情報システム等は、サプライチェーン全体を通して、適切に運用されるべきというのが基本的な考え方であり、本ガイドラインでは、医療機関等と直接的な契約関係のない事業者も医療情報システム等のサプライチェーンの一部として機能している場合、本ガイドラインの適用範囲に含まれる。**

1

2 **用語集の「医療情報システム等」の定義も上記の記載に変更する**

2省GLの整理

1.焦点　2.体裁

論点なし

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜論点無し＞

本ガイドラインで対象とする事業者・システムの範囲については、図 2-1でUSB等の可搬媒体でデータをやり取りする場合等も含めカバーできているため、**論点無しとする**。

＜2省GL該当箇所の記載 7頁＞

図 2-1 本ガイドラインで対象とする事業者・システムの範囲

本ガイドラインが対象とする医療情報と事業者に関しては、
「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 FAQ」の「１．ガイドラインの対象範囲」に示す例も参照すること。

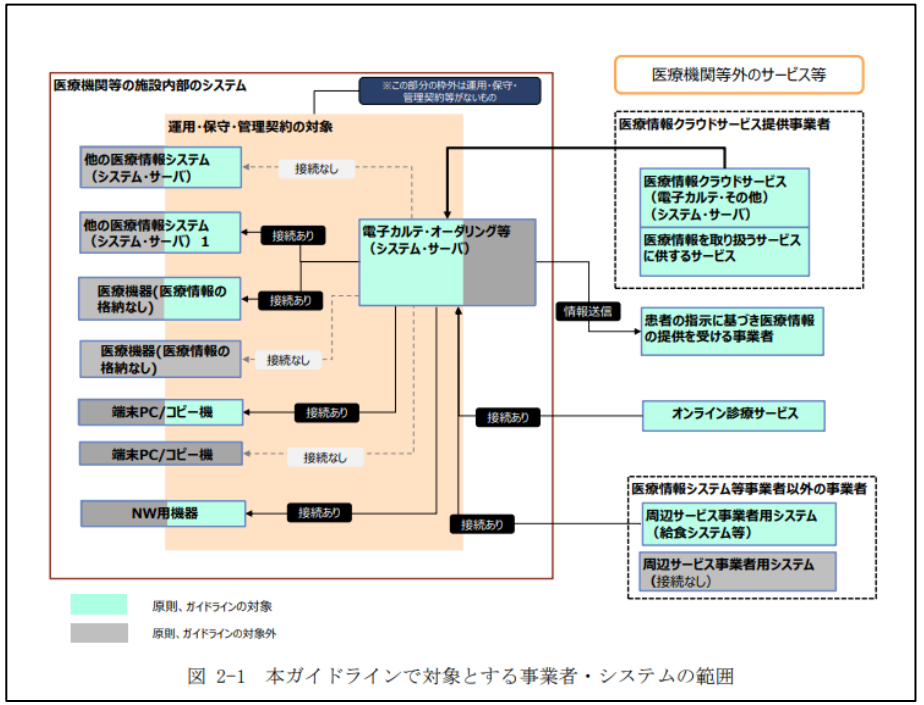


図 2-1　本ガイドラインで対象とする事業者・システムの範囲

2省GLの整理

1.焦点　2.体裁

論点③

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜論点⑤＞
2省ガイドラインの記載内容を理解するうえで、**内容が具体的に記載されている「章」、「資料名」を明記**してはどうか。

＜2省GL該当箇所の記載 8頁＞

図 2-2 本ガイドラインの対象とする事業者

対象事業者は**本ガイドラインに基づくリスクマネジメント及び医療情報安全管理ガイドライン等に基づいた制度上の要求事項への対応**が求められ、医療機関等に提供する医療情報システム等に必要な資源や役務の提供に係るサプライチェーン全体について、本ガイドラインで記載するリスクマネジメント及び制度上の要求事項に対応すること。

ただし、医療機関等と直接的な契約関係はなく、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者は、契約元の対象事業者（一次請けだけでなく二次請け以降の場合もある）の求めに応じて**リスクマネジメント及び制度上の要求事項への対応状況に関する資料**を契約元の対象事業者に提供すること（同等の情報の開示を含む）。また、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は、医療機関等の求めに応じて**リスクマネジメント及び制度上の要求事項への対応状況に関する資料**を提供すること（同等の情報の開示を含む）

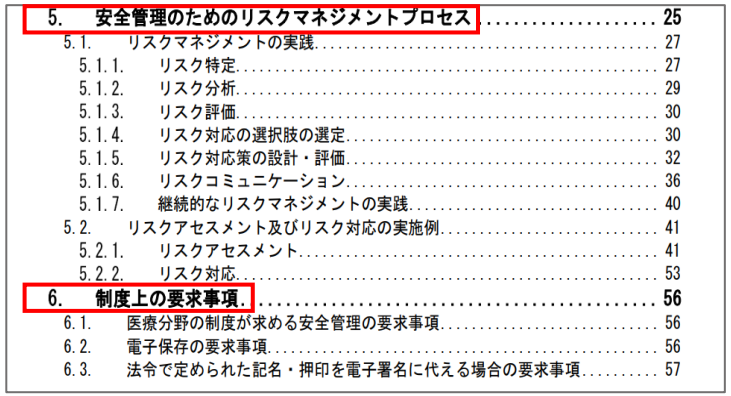
根拠1

2省ガイドライン目次によると、「本ガイドラインで記載するリスクマネジメント及び制度上の要求事項」は、同ガイドライン**5章及び6章に記載**されている。

＜2省ガイドライン＞

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第 2.0版 目次

01gl_20250328.pdf



根拠2

リスクマネジメントへの対応状況に関する資料は、**リスクアセスメント結果一覧及びリスク対応一覧等**を指す。

＜2省ガイドライン＞

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第 2.0版 51-55頁

01gl_20250328.pdf

(3) リスク特定・リスク分析・リスク評価における成果物の作成

リスクアセスメント結果一覧の作成にあたっては、情報流に対し、情報流の分類、関連する脅威、脅威の顕在化を想定して特定したリスク、リスクレベルと対応要否を次に示すような形で整理する。

5.2.2. リスク対応

リスク対応一覧の作成にあたっては、まず、対応するリスクに対し 5.1.4 のプロセスで決定したリスク対応の選択肢を記載する。

次に、「人的・組織的」、「物理的」、「技術的」の複数の観点から決定した対策のうち、対象事業者が実施する対策について記載する36。そして、リスク対応において医療機関等に対応を求める事項を明らかにした上で、残存するリスクを記載する。

2省GLの整理

1.焦点　2.体裁

論点③

2. 本ガイドラインの対象（6頁）
2.1. 本ガイドラインが対象とする医療情報と事業者（6頁）

＜対応Lv1：方向性＞

1 「本ガイドラインに基づくリスクマネジメント及び医療情報安全管理ガイドライン等に基づいた制度上の要求事項への対応」の**具体的な記載個所を明記**する。

2 「リスクマネジメント及び制度上の要求事項への対応状況に関する資料」の具体的な内容を**注釈で補足**する。

＜対応Lv2：対応必要事項＞

図 2-2 本ガイドラインの対象とする事業者

1 対象事業者は本ガイドライン第5章で記載するリスクマネジメント及び第6章で記載する医療情報安全管理ガイドライン等に基づいた制度上の要求事項への対応が求められ、医療機関等に提供する医療情報システム等に必要な資源や役務の提供に係るサプライチェーン全体について、本ガイドラインで記載するリスクマネジメント及び制度上の要求事項に対応すること。

ただし、医療機関等と直接的な契約関係はなく、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者は、契約元の対象事業者（一次請けだけでなく二次請け以降の場合もある）の求めに応じて、リスクマネジメント及び制度上の要求事項への対応状況に関する資料（※1）を契約元の対象事業者に提供すること（同等の情報の開示を含む）。また、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は、医療機関等の求めに応じて、リスクマネジメント及び制度上の要求事項への対応状況に関する資料（※1）を提供すること（同等の情報の開示を含む）

2

※1:リスクマネジメントへの対応状況に関する資料は、本ガイドライン第5章で記載するリスクアセスメント結果一覧及びリスク対応一覧等を指す。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点①

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.1. 安全管理義務（12頁）

＜論点①＞

①適切な委託先の選定について、理解していない事業者がいたため、**2省ガイドライン本文中に具体的な内容を記載**してはどうか。

＜2省GL該当箇所の記載　13～14頁＞

(2)安全管理措置を講じる義務

個人情報保護法では、医療機関等と対象事業者は、それぞれその取り扱う個人データの安全管理のために必要かつ適切な措置を講ずる義務を負う（個人情報保護法 23 条）。そして、医療機関等が対象事業者に対して個人データの取扱いを委託している場合、委託元は、委託先においてその取扱いを委託した個人データの安全管理が図られるよう、委託先を監督する義務（以下、「監督義務」という。）を負うと規定されている（個人情報保護法25 条）。

監督義務の内容としては、①**適切な委託先の選定**、②委託契約の締結、③委託先における個人データ取扱状況の把握という3点が挙げられている。14

なお、対象事業者がクラウドサービスを提供する事業者であって、当該事業者が個人データを取り扱わないこととなっている場合（契約条項によって当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等）には、医療機関等は個人データを「提供」したことにならず、個人情報保護法 25条に基づきクラウドサービス事業者を監督する義務はないが、クラウドサービス事業者は自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。また、医療機関等は、本ガイドラインや医療情報安全管理ガイドラインに従ってクラウドサービス提供事業者を適切に監督する必要があり、クラウドサービス事業者は本ガイドラインに従って安全管理措置を講ずる必要がある。

＜注釈部分＞

14 「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年個人情報保護委員会告 示第 6 号

根拠1

個人情報の保護に関する法律についてのガイドライン（通則編）に①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握の具体的な内容が記載されている。

＜個人情報の保護に関する法律についてのガイドライン＞

「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月（令和 7 年 6 月一部改正）個人情報保護委員会）55頁
https://www.ppc.go.jp/files/pdf/250601_guidelines01.pdf

（1）適切な委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第 23 条及び本ガイドラインで委託元に求められるものと同等であることを確認するため、「10（（別添）講ずべき安全管理措置の内容）」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない。

（2）委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい。

（3）委託先における個人データ取扱状況の把握

委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。また、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱方法等について、委託先から事前報告を受け又は承認を行うこと、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第 23 条に基づく安全管理措置を講ずることを十分に確認することが望ましい（※4）。（略）

2省GLの整理

1.焦点　2.体裁

論点①

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.1. 安全管理義務（12頁）

＜対応Lv1：方向性＞

- **「①適切な委託先の選定」の具体的な内容**を２省GL本文に記載する。

＜対応Lv2：対応必要事項＞

（略）

監督義務の内容としては、①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握という3 点が挙げられている。①適切な委託先の選定については、基本方針の策定、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置、外的環境の把握が委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない。[14] なお、対象事業者がクラウドサービスを提供する事業者であって、当該事業者が個人データを取り扱わないこととなっている場合（契約条項によって当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等）には、医療機関等は個人データを「提供」したことにならず、個人情報保護法 25条に基づきクラウドサービス事業者を監督する義務はないが、クラウドサービス事業者は自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。また、医療機関等は、本ガイドラインや医療情報安全管理ガイドラインに従ってクラウドサービス提供事業者を適切に監督する必要があり、クラウドサービス事業者は本ガイドラインに従って安全管理措置を講ずる必要がある。

＜注釈部分＞

14「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年個人情報保護委員会告 示第 6 号

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点②

3. 医療情報の安全管理に関する義務・責任（12頁）
3.1. 法律関係（12頁）
3.1.2. 対象事業者の説明義務（14頁）

＜論点②＞

医療機関等が患者に対する安全管理義務を履行するために必要な情報について、**具体的な内容の記載箇所を明記**してはどうか。

＜2省GL該当箇所の記載　14～15頁＞

医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべきである。

このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、**医療機関等が患者に対する安全管理義務を履行するために必要な情報**を適時適切に提供する義務（以下、「説明義務」という。）を負う。

説明義務については、契約の対象となっているサービス内容に関して、医療機関等がその内容を十分理解するのに必要な情報を提供するほか、直接契約の対象となっていない事項（例えば、医療機関等が医療情報システム等に用いる機器に関するセキュリティ情報）についても、提供する医療情報システム等との関係で最低限確認を促すべき点等の情報を提供することが想定される。例えば、医療機関等が管理する機器に対する保守契約の要否や、セキュリティ事案が発生した時の対応を取り決めることについても、明示的に医療機関等に対してリスクを示し、そのリスクに対して十分理解を得た上で、責任分界を含めた合意を行うことが求められる。

根拠1

医療機関等へ情報提供すべき項目の具体例として、**サービス仕様適合開示書、MDS/SDS、ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針（平成 29 年 3 月 31 日）**」が挙げられている。

＜2省ガイドライン＞

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第 2.0版 20頁　01gl_20250328.pdf

4.1. 医療機関等へ情報提供すべき項目

対象事業者と医療機関等の合意形成においては、対象事業者から医療機関等への適切な情報提供が必要である。合意形成のために提供すべき情報とは何であるかを表 4-1 に示す**19**。対象事業者は、これら項目に係る情報提供にあたっては、医療機関等が容易に理解可能となるよう努め、適切に共通理解を得ること。

＜注釈部分＞

19 情報提供を行う際の文書例として別紙 1 に示す**サービス仕様適合開示書**等の参考例がある。本参考例の 作成・提供は必須ではないが、本参考例等と同等の内容について情報提供した上で、適切な共通理解に基 づく合意形成を図ることを求める。なお、本節で示す情報提供すべき内容を作成するにあたっては、例えば、一般社団法人日本画像医療システム工業会(JIRA) 及び一般社団法人保健医療福祉情報システム工業会（JAHIS）による「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チェックリスト」（以 下、「**MDS/SDS**」という。）があり、当該チェックリストが対象とする医療情報システム等を提供する対象事業者においては、当該チェックリストを参考とすることが有効である。また、一般社団法人日本クラウド産業協会が運営する「医療情報 ASP・SaaS 情報開示認定制度」よる認定を受け、総務省が定める「**ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針（平成 29 年 3 月 31 日）**」を 満たした情報提供を行うことも有効である。

2省GLの整理

1.焦点　2.体裁

論点②

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.2. 対象事業者の説明義務（14頁）

＜対応Lv1：方向性＞

- 医療機関等が患者に対する安全管理義務を履行するために必要な情報について、**医療機関等へ情報提供すべき項目の記載箇所を明記**してはどうか。

＜対応Lv2：対応必要事項＞

医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識･経験･人材を擁しているべきである。このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報（※）を適時適切に提供する義務（以下、「説明義務」という。）を負う。

説明義務については、契約の対象となっているサービス内容に関して、医療機関等がその内容を十分理解するのに必要な情報を提供するほか、直接契約の対象となっていない事項（例えば、医療機関等が医療情報システム等に用いる機器に関するセキュリティ情報）についても、提供する医療情報システム等との関係で最低限確認を促すべき点等の情報を提供することが想定される。例えば、医療機関等が管理する機器に対する保守契約の要否や、セキュリティ事案が発生した時の対応を取り決めることについても、明示的に医療機関等に対してリスクを示し、そのリスクに対して十分理解を得た上で、責任分界を含めた合意を行うことが求められる。

＜注釈部分＞

（※）想定される提供すべき情報は、本ガイドラインの第４章の「4.1. 医療機関等へ情報提供すべき項目」に記載。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点③

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.2. 対象事業者の説明義務（14頁）

＜論点③＞

医療機関等と対象事業者が責任分界を含めた合意を行うことについて、**合意文書とは何かを具体的に明示**してはどうか。

＜2省GL該当箇所の記載　14～15頁＞

医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべきである。

このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務（以下、「説明義務」という。）を負う。

説明義務については、契約の対象となっているサービス内容に関して、医療機関等がその内容を十分理解するのに必要な情報を提供するほか、直接契約の対象となっていない事項（例えば、医療機関等が医療情報システム等に用いる機器に関するセキュリティ情報）についても、提供する医療情報システム等との関係で最低限確認を促すべき点等の情報を提供することが想定される。例えば、医療機関等が管理する機器に対する保守契約の要否や、セキュリティ事案が発生した時の対応を取り決めることについても、明示的に医療機関等に対してリスクを示し、そのリスクに対して十分理解を得た上で、**責任分界を含めた合意**を行うことが求められる。

根拠1

責任分界を含めた合意のプロセスについて、**合意した内容を契約書やSLA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必要がある**旨記載されている。

＜厚生労働省ガイドライン＞

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　9 頁

https://www.mhlw.go.jp/content/10808000/001102570.pdf

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省GLの整理

1.焦点　2.体裁

論点③

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.2. 対象事業者の説明義務（14頁）

＜対応Lv1：方向性＞

- 責任分界を含めた合意のプロセスについて、**合意した内容を契約書やSLA等の形で双方の合意文書として明らかにする必要がある旨を補足**する。

＜対応Lv2：対応必要事項＞

医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識･経験･人材を擁しているべきである。

このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務（以下、「説明義務」という。）を負う。

説明義務については、契約の対象となっているサービス内容に関して、医療機関等がその内容を十分理解するのに必要な情報を提供するほか、直接契約の対象となっていない事項（例えば、医療機関等が医療情報システム等に用いる機器に関するセキュリティ情報）についても、提供する医療情報システム等との関係で最低限確認を促すべき点等の情報を提供することが想定される。例えば、医療機関等が管理する機器に対する保守契約の要否や、セキュリティ事案が発生した時の対応を取り決めることについても、明示的に医療機関等に対してリスクを示し、そのリスクに対して十分理解を得た上で、責任分界を含めた合意を行うことが求められる。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。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

3. 医療情報の安全管理に関する義務･責任（12頁）
3.1. 法律関係（12頁）
3.1.3. 情報セキュリティ事故等発生時における義務と責任（15頁）

＜論点無し＞

情報セキュリティ事故等発生時における義務と責任について参照すべきドキュメントが明記されており、分かりにくいと感じる点がないため、**論点無しとする**。

＜2省GL該当箇所の記載　15頁＞

(1)危機対応義務

個人情報保護法上、個人情報取扱事業者である対象事業者は、個人情報保護法施行規則7 条各号に該当する個人データの漏えい等事案が生じたときは、個人情報保護委員会に報告し、また本人に通知等する義務を負うとされている（個人情報保護法 26条）。「個人情報の保護に関する法律についてのガイドライン（通則編）」を参考に、必要な対策を講ずることが求められる。

(2)民事責任

情報漏洩等のセキュリティ事故が発生し、患者等に被害が生じると、患者等は医療機関等に対し、契約責任または不法行為責任に基づき損害賠償を請求することがある。また、患者等は、直接の契約関係がない対象事業者に対しても、不法行為責任に基づき損害賠償を請求する可能性がある。

契約責任の場合、事業者がいかなる債務を負っていたのかという、委託契約（サービス提供契約、開発委託契約等）の解釈問題となる。また、不法行為責任の場合、事業者の過失の存否（すなわち、いかなる注意義務を負っていたか。）として判断される。

図 3-3 事後の対応における民事責任について

2省GLの整理

1.焦点　2.体裁

論点④

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）

＜論点④＞

「3.2. 医療情報システム等のライフサイクルにおける義務と責任」について、医療機関等と対象事業者間の**合意形成の適用範囲を具体的に記載**してはどうか。

＜2省GL該当箇所の記載　16～17頁＞

対象事業者が前節で記載した義務や責任に対応するにあたって、全ての医療情報システム等に共通な一律の要求事項を定めることは難しい。そのため、対象事業者は自らが提供する医療情報システム等を対象とし、リスクマネジメントのプロセスとリスクベースアプローチに基づいて対策をとりまとめ、**医療機関等との間で合意を形成する**こととする。

本節では、一般的に想定される医療情報システム等のライフサイクルにおいて対象事業者に求められる義務や責任への対応方法を示す。なお、前節で記載した義務や責任と、本節にて示す内容との対応関係は表 3-1 の通りである。

表 3-1「3.1. 法律関係」記載内容と本節記載内容の対応関係

また、本ガイドラインで想定する基本的なライフサイクルの全体像について図 3-4 に示す。

図 3-4 医療情報システム等のライフサイクル

根拠1

FAQによると、医療機関等と対象事業者間の合意形成は**サプライチェーン全体においても適応可能**である。

＜FAQ＞

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 FAQ 5頁

https://www.meti.go.jp/policy/mono_info_service/healthcare/04faq_20250328.pdf

3. 医療情報システム等のライフサイクルにおける義務と責任（基本的な考え方）

ガイドラインの「3.2. 医療情報システム等のライフサイクルにおける義務と責任」は、医療機関等と対象事業者間における義務と責任についての合意形成の重要性を示しています。

当該箇所は、医療機関等と対象事業者間の合意形成に焦点を当てて書かれていますが、本FAQの「2 医療情報システム等の提供形態」で述べている**サプライチェーン全体においても適応可能**なものです。例えば、事業者 A のアプリケーションを事業者 B のプラットフォームとインフラ上で利用する場合の事業者 AB 間の義務と責任の合意形成を考える際にも適応できます。

2省GLの整理

1.焦点　2.体裁

論点④

3. 医療情報の安全管理に関する義務･責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）

＜対応Lv1：方向性＞

- FAQを踏まえ、医療機関等と対象事業者間の合意形成の適用範囲について、**サプライチェーン全体においても適応可能である旨を記載**する。

＜対応Lv2：対応必要事項＞

対象事業者が前節で記載した義務や責任に対応するにあたって、全ての医療情報システム等に共通な一律の要求事項を定めることは難しい。そのため、対象事業者は自らが提供する医療情報システム等を対象とし、リスクマネジメントのプロセスとリスクベースアプローチに基づいて対策をとりまとめ、医療機関等との間で合意を形成することとする。

上記合意形成については、医療機関等と対象事業者間の合意形成だけではなく、サプライチェーン全体の合意形成において適用される。例えば、事業者 A のアプリケーションを事業者 B のプラットフォームとインフラ上で利用する場合の事業者 AB 間の義務と責任の合意形成を考える際にも適用される。なお、「サプライチェーン」とは、医療機関等に提供する医療情報システム等に必要な資源や役務の提供に係るプロセス全体を指す。

本節では、一般的に想定される医療情報システム等のライフサイクルにおいて対象事業者に求められる義務や責任への対応方法を示す。なお、前節で記載した義務や責任と、本節にて示す内容との対応関係は表 3-1 の通りである。

表 3-1「3.1. 法律関係」記載内容と本節記載内容の対応関係

また、本ガイドラインで想定する基本的なライフサイクルの全体像について図 3-4 に示す。

図 3-4 医療情報システム等のライフサイクル

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）
3.2.1. 契約前の合意形成及び契約中の合意の維持（17頁）

＜論点無し＞

3.2.1.において、「医療機関等との間で「共通理解」と「明示的な合意」の形成において、対象事業者は、4.1 にて示す「医療機関等へ情報提供すべき項目」について、医療機関等と共通理解を形成すること。」と記載があり、**4.1にて論点整理を行うため論点無しとする。**

＜2省GL該当箇所の記載　17頁＞

対象事業者はは説明義務を果たすために、医療機関等との間で「共通理解」と「明示的な合意」の形成を行うこと。

契約前の合意形成において、対象事業者は、4.1 にて示す「医療機関等へ情報提供すべき項目」について、医療機関等と共通理解を形成すること。このとき、対象事業者は、医療機関等との間で適切な共通理解が形成されるよう、ICT やセキュリティに係る専門知識の差異があることを踏まえ、用語集や解説を加える等の工夫に努めること。なお、本ガイドラインにおける「共通理解」とは、契約書や SLA 等の契約上の文書による明示的な合意とは別に、共通の理解を形成することであり、その取組みの記録として議事メモや作業記録等の文書等に残すことは重要である。対象事業者は、医療機関等との共通理解の上で、契約書や SLA 等の契約上の文書を作成し、医療機関等と明示的な合意を形成すること。明示的な合意の内容には、医療機関等と事業者の間での責任分界に関する内容が含まれる。合意の内容については、医療情報システム等の機能や性能、仕様などの内容については明示的に示されることが多い。一方でそれ以外の情報提供範囲や非常時における対応などについては、具体的な内容や責任分界はあいまいなままになるケースがあることが指摘されており、このことがサイバー攻撃などの非常時への対応において課題になることがある。これらについても責任分界の共通理解を得て、医療機関等と事業者が履行に際して遵守すべき範囲を明示して文書化等を図ることが望ましい。

合意形成にあたって情報提供すべき内容については、4.1 に示す。

また、契約中においても、医療機関等からの要求内容や環境に変化が生じた場合や、情報セキュリティ事故発生により開発・運用内容等を見直す必要が生じた場合等には、共通理解や明示的な合意に基づく合意形成を改めて実施し、合意を維持すること。

2省GLの整理

1.焦点　2.体裁

論点⑤

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）
3.2.2. 通常時の義務（18頁）

＜論点⑤＞

通常時の義務について、**運用フェーズと開発フェーズで事業者が異なる場合の対応方針について記載**してはどうか。

＜2省GL該当箇所の記載　18頁＞

通常時の医療情報システム等のライフサイクルは「開発フェーズ」「運用フェーズ」「契約終了フェーズ」に分けられる。したがって、対象事業者が必要な対応を抜け漏れなく洗い出すにあたっても、これら 3 フェーズに分け、当該フェーズでの実施内容を踏まえた上で、想定されるリスクや対応方針について整理することが有効である。

「**開発フェーズ**」は、対象事業者が医療機関等との契約中に、医療機関等に提供する医療情報システム等の開発を実施するフェーズである。「開発フェーズ」には新規の開発（新規開発）だけでなく、機器・端末のアップデートや機能更新に伴う開発（保守開発）や各医療機関等での初期設定といった、運用フェーズの前段階も広く含むものとする。したがって、開発フェーズは 1 度のみ発生するとは限らず、運用フェーズから再度開発フェーズに移行することや、運用中に開発フェーズが並行発生することも考えられる。対象事業者は、安全管理義務へ対応するために医療機関等との合意に基づいて医療情報システム等の開発と情報の取扱いを行わなくてはならない。なお、クラウドサービスについては、利用者側の調達に応じて、新たな開発を伴わず、サービス導入に必要な検討や設定等を行うためのフェーズを設けることがある。本ガイドラインにおいては、これらも開発フェーズに相当するものと位置付ける。

「**運用フェーズ**」は、対象事業者が医療機関等との契約中に、医療情報システム等の運用作業を実施するフェーズである。対象事業者は、安全管理義務へ対応するために、自らが提供する医療情報システム等の運用状況等について医療機関等に対して定期的な報告を実施するとともに、実施しているセキュリティ対策に関しては定期的に自己点検し、その結果の報告を必要に応じて実施しなければならない。

「契約終了フェーズ」は、対象事業者が医療機関等との契約中に、医療情報システム等に関する契約を終了する際のフェーズである。対象事業者は、安全管理義務へ対応するために、予め医療機関等と合意した手順に則って情報（プログラム等も含む）の返却・移管・破棄を実施しなければならない。また、当該手順に則って情報の返却・移管・破棄を適切に実施したことの証跡を取得しておくことも必要である。なお、対象事業者が各フェーズで実施する具体的な対応事項については、後述の通り、第 5 章で記載するリスクマネジメントの実践手順に従って洗い出し、医療機関等への情報提供と合意形成を行うこととしている。

根拠1

FAQにて、**運用フェーズと開発フェーズで事業者が異なる場合において、医療情報システム等のライフサイクルにおける義務と責任について関係者間で合意形成を図る例**が記載されている。

＜FAQ＞

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 FAQ 6頁

https://www.meti.go.jp/policy/mono_info_service/healthcare/04faq_20250328.pdf

3.1. **運用フェーズと開発フェーズで事業者が異なる場合**があるのではないか？

医療情報システム等のライフサイクルは、運用フェーズだけでなく、運用開始前もしくは運用開始後の開発（保守）フェーズがあります。医療情報システム等の運用と開発が別事業者になる場合があり、そのような複数事業者が関与する場合においても、医療情報システム等のライフサイクルにおける義務と責任について関係者間で合意形成しておく必要があります。例えば、**事業者 A が運用を担当し、事業者 B が開発を担当し、医療機関等は事業者A のみとの契約関係にある場合（契約内容に運用と開発を含む）です。医療機関等は事業者A との間で運用と開発に関する義務と責任について明確化し、合意形成しておく必要があります。事業者Aは事業者Bとの間で開発に関する義務と責任について内部的に明確化し、合意形成しておく必要があります。**

2省GLの整理

1.焦点　2.体裁

論点⑤

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）
3.2.2. 通常時の義務（18頁）

＜対応Lv1：方向性＞

- 運用フェーズと開発フェーズで事業者が異なる場合の対応例について、本来事業者が認知しておく方が望ましいところ、FAQに記載している場合、この問題に直面した事業者しか参照しないため、**2省ガイドラインの本文に具体的に記載**する。

＜対応Lv2：対応必要事項＞

通常時の医療情報システム等のライフサイクルは「開発フェーズ」「運用フェーズ」「契約終了フェーズ」に分けられる。したがって、対象事業者が必要な対応を抜け漏れなく洗い出すにあたっても、これら 3 フェーズに分け、当該フェーズでの実施内容を踏まえた上で、想定されるリスクや対応方針について整理することが有効である。

（略）

「契約終了フェーズ」は、対象事業者が医療機関等との契約中に、医療情報システム等に関する契約を終了する際のフェーズである。対象事業者は、安全管理義務へ対応するために、予め医療機関等と合意した手順に則って情報（プログラム等も含む）の返却・移管・破棄を実施しなければならない。また、当該手順に則って情報の返却・移管・破棄を適切に実施したことの証跡を取得しておくことも必要である。

なお、対象事業者が各フェーズで実施する具体的な対応事項については、後述の通り、第 5 章で記載するリスクマネジメントの実践手順に従って洗い出し、医療機関等への情報提供と合意形成を行うこととしている。

また、医療情報システム等の運用と開発が別事業者になる場合があり、そのような複数事業者が関与する場合においても、医療情報システム等のライフサイクルにおける義務と責任について関係者間で合意形成しておく必要がある。例えば、事業者Aが運用を担当し、事業者Bが開発を担当し、医療機関等は事業者Aのみとの契約関係にある場合（契約内容に運用と開発を含む）、医療機関等は事業者A との間で運用と開発に関する義務と責任について明確化し、合意形成しておく必要がある。また、事業者Aは事業者Bとの間で開発に関する義務と責任について内部的に明確化し、合意形成しておく必要がある。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点⑥

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）
3.2.3. 危機管理対応時の義務及び責任（19頁）

＜論点⑥＞

情報セキュリティ事故が発生した場合における医療機関等への情報提供について、**個人情報が漏えいした可能性がある場合に必要な措置を記載**してはどうか。

＜2省GL該当箇所の記載　19頁＞

医療情報システム等の提供に際しては、特段の問題が発生しないことが本来期待されているが、上述の各フェーズにおける脅威が顕在化した場合、医療情報の漏洩や改竄、医療情報システム等の停止等の情報セキュリティ事故が生じる可能性がある。本ガイドラインでは、このような情報セキュリティ事故が生じ、当該問題への対処が必要となる場合を、危機管理対応時と定義する。

対象事業者は、何らかの情報セキュリティ事故が発生した場合、発生した情報セキュリティ事故に関する詳細な情報を医療機関等へ提供することとなるが、この際、**発生した情報セキュリティ事故の原因・範囲等、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために必要となる情報の収集をサポートできるよう、できる限り詳細な情報を提供するべき**である。

また、対象事業者は、発生した情報セキュリティ事故について、速やかに善後策を講じなければならない。さらに、発生した情報セキュリティ事故自体に対応するための施策を講じるに留まらず、同様の情報セキュリティ事故が以降発生しないように再発防止策を医療機関等に提案すること。提案した内容については、医療機関等と適切に合意（再合意）形成を行った上で実行すること。

根拠1

個人情報の保護に関する法律についてのガイドライン（通則編）に**漏えい等事案が発覚した場合に講ずべき措置**が記載されている。

＜個人情報の保護に関する法律についてのガイドライン＞

「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月（令和 7 年 6 月一部改正）個人情報保護委員会） 58～59頁

https://www.ppc.go.jp/files/pdf/250601_guidelines01.pdf

3-5-2 **漏えい等事案が発覚した場合に講ずべき措置**

個人情報取扱事業者は、漏えい等又はそのおそれのある事案（以下「漏えい等事案」という。）が発覚した場合は、漏えい等事案の内容等に応じて、次の（1）から（5）に掲げる事項について必要な措置を講じなければならない。

（1）事業者内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

（2）事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

（3）影響範囲の特定

上記（2）で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

（4）再発防止策の検討及び実施

上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

（5）個人情報保護委員会への報告及び本人への通知

根拠2

岡山県精神科医療センターがランサムウェア攻撃を受けた事例において、個人情報が流出したことを受け、**調査報告書にて情報を公開**し、**再発防止策の検討及び実施**を含めて報告されている。

＜事例＞

ランサムウェア事案調査報告書（地方独立行政法人 岡山県精神科医療センター）20～27頁

24bb9b94f7eb10eff58b605c01c384ad.pdf

5.8 復旧方針と再発防止策

技術的対策	組織的対策	人的対策
1. 基幹システム脆弱性対策 2. 部門システム脆弱性対策 3. 医療機器脆弱性対策 4. ベンダーのセキュリティポリシーの見直し	1. IT ガバナンスの確立と強化 2. システム管理台帳の作成と定期的な更新 3. データー分類、ラベル付け基準の策定とアクセス制御等 4. 部門システムベンダー、医療機器ベンダーへのセキュリティ対策ヒヤリングの実施と是正 5. ベンダーとの契約の見直し 6. IT-BCP の策定	1. 定期的なセキュリティ教育の実施と脅威情報の共有を実施 2. 脅威情報の入手先を JPCERT/CC、CISA、CIS、MITRE とし、攻撃事例や初動対応の訓練を中心に教育コンテンツを策定

2省GLの整理

1.焦点　2.体裁

論点⑥

3. 医療情報の安全管理に関する義務・責任（12頁）
3.2. 医療情報システム等のライフサイクルにおける義務と責任（16頁）
3.2.3. 危機管理対応時の義務及び責任（19頁）

＜対応Lv1：方向性＞

- 注釈にて、個人情報の保護に関する法律についてのガイドライン（通則編）に記載の**漏えい等事案が発覚した場合に講ずべき措置の記載箇所を注釈に記載**する。

＜対応Lv2：対応必要事項＞

医療情報システム等の提供に際しては、特段の問題が発生しないことが本来期待されているが、上述の各フェーズにおける脅威が顕在化した場合、医療情報の漏洩や改竄、医療情報システム等の停止等の情報セキュリティ事故が生じる可能性がある。本ガイドラインでは、このような情報セキュリティ事故が生じ、当該問題への対処が必要となる場合を、危機管理対応時と定義する。

対象事業者は、何らかの情報セキュリティ事故が発生した場合、発生した情報セキュリティ事故に関する詳細な情報を医療機関等へ提供することとなるが、この際、発生した情報セキュリティ事故の原因・範囲等、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために必要となる情報の収集をサポートできるよう、できる限り詳細な情報を提供するべきである。（※）

また、対象事業者は、発生した情報セキュリティ事故について、速やかに善後策を講じなければならない。さらに、発生した情報セキュリティ事故自体に対応するための施策を講じるに留まらず、同様の情報セキュリティ事故が以降発生しないように再発防止策を医療機関等に提案すること。提案した内容については、医療機関等と適切に合意（再合意）形成を行った上で実行すること。

＜注釈部分＞

（※）個人情報が漏えいした可能性がある場合には、個人情報取扱事業者は、「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月（令和 7 年 6 月一部改正）個人情報保護委員会）を参照。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

4. 対象事業者と医療機関等の合意形成 （20頁）
4.1. 医療機関等へ情報提供すべき項目（20頁）

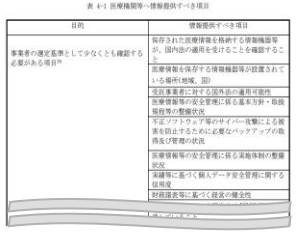
＜論点無し＞

医療機関等へ情報提供すべき項目について、表4-1や注釈にて具体的に記載されているため、**論点無しとする**。

＜2省GL該当箇所の記載　20～22頁＞

対象事業者と医療機関等の合意形成においては、対象事業者から医療機関等への適切な情報提供が必要である。合意形成のために提供すべき情報とは何であるかを表 4-1 に示す19。対象事業者は、これら項目に係る情報提供にあたっては、医療機関等が容易に理解可能となるよう努め、適切に共通理解を得ること。

表 4-1 医療機関等へ情報提供すべき項目 →



＜注釈部分＞

19 情報提供を行う際の文書例として別紙 1 に示すサービス仕様適合開示書等の参考例がある。本参考例の作成・提供は必須ではないが、本参考例等と同等の内容について情報提供した上で、適切な共通理解に基づく合意形成を図ることを求める。なお、本節で示す情報提供すべき内容を作成するにあたっては、例えば、一般社団法人日本画像医療システム工業会(JIRA) 及び一般社団法人保健医療福祉情報システム工業会（JAHIS）による「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チェックリスト」（以下、「MDS/SDS」という。）があり、当該チェックリストが対象とする医療情報システム等を提供する対象事業者においては、当該チェックリストを参考とすることが有効である。また、一般社団法人日本クラウド産業協会が運営する「医療情報 ASP・SaaS 情報開示認定制度」よる認定を受け、総務省が定める「ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針（平成 29 年 3 月 31 日）」を満たした情報提供を行うことも有効である。

2省GLの整理

1.焦点　2.体裁

論点なし

4. 対象事業者と医療機関等の合意形成 （20頁）
4.2. 医療機関等との役割分担の明確化（22頁）

＜論点無し＞

「対象事業者は、合意形成にあたり、具体的には、4.1 で示した医療機関等の運用管理規程に定める必要がある事項として、医療機関等へ対応を求める内容を含めること。」と記載があり、**4.1にて論点整理を行うため論点無しとする**。

＜2省GL該当箇所の記載　22～23頁＞

医療情報システム等の安全管理には、対象事業者と医療機関等の双方における適切な運用管理を行うこと。例えば、医療情報システム等が堅牢なアクセス制御機能を持っていたとしても、医療機関側の利用者がパスワードを利用端末に貼っていたり、アカウントを複数で共有していたりすれば、医療情報を守ることはできない。また、医療機関等が購入した機器等については、別途、事業者と当該機器についての保守契約を締結しない場合には、原則、管理責任は医療機関等にあり、事業者との間での分担は生じない。

したがって、**対象事業者は、合意形成にあたり、医療機関等における運用管理も踏まえた形で、役割分担を定めること。具体的には、4.1 で示した医療機関等の運用管理規程に定める必要がある事項として、医療機関等へ対応を求める内容を含めること。**

2省GLの整理

1.焦点　2.体裁

論点なし

4. 対象事業者と医療機関等の合意形成 （20頁）
4.3. 医療情報システム等の安全管理に係る評価（23頁）

＜論点無し＞

「医療情報システム等関連業務に関与する担当者自らが評価を行うと、信頼性及び客観性が低下するため、対象事業者内部の独立した監査部門や第三者機関21が評価を行うことが望ましい。」と記載があり、**第三者機関評価が注釈で例示されているため論点無しとする。**

＜2省GL該当箇所の記載　23頁＞

対象事業者は、医療情報システム等の安全管理の妥当性について、医療機関等と適切な共通理解を得るため、医療情報システム等の安全管理に係る評価を行い、評価結果を医療機関等へ情報提供すること。このとき、医療情報システム等関連業務に関与する担当者自らが評価を行うと、信頼性及び客観性が低下するため、対象事業者内部の独立した監査部門や第三者機関**21**が評価を行うことが望ましい。

＜注釈部分＞

21 第三者機関による評価として、例えば、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）による、民間事業者による医療情報に係るクラウドサービスの評価が挙げられる。

2省GLの整理

1.焦点　2.体裁

論点①

4. 対象事業者と医療機関等の合意形成 （20頁）
4.4. 対象事業者の適格性を評価する第三者認証等の取得に係る要件（23頁）

＜論点①＞

「特にプライバシーマーク認証を取得していることが望ましい」について、具体的に制度の理由を記載してはどうか。

＜2省GL該当箇所の記載　23～24頁＞

医療情報の機微性に鑑み、対象事業者は、医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、情報セキュリティに係る公的な第三者認証等として、プライバシーマーク認定またはISMS認証を取得すること。**特に、プライバシーマーク認定を取得していることが望ましい。**また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。そのため、ISMS認証のみを取得する場合には、事業者における具体的な管理方法の説明等を検討する等、医療機関等から有効性を示す資料の提供を求められた場合に対応できる状態としておくことが望ましい。医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定または ISMS 認証の取得が強く求められる。

なお、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 3 年3 月 30 日各府省情報化統括責任者（CIO）連絡会議決定）で示されている「クラウドセキュリティ認証等」（表 4-1 参照）は、プライバシーマーク認定や ISMS 認証と同等の認証等と認められるため、これに代えることも可能である。ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではないことに留意すること。

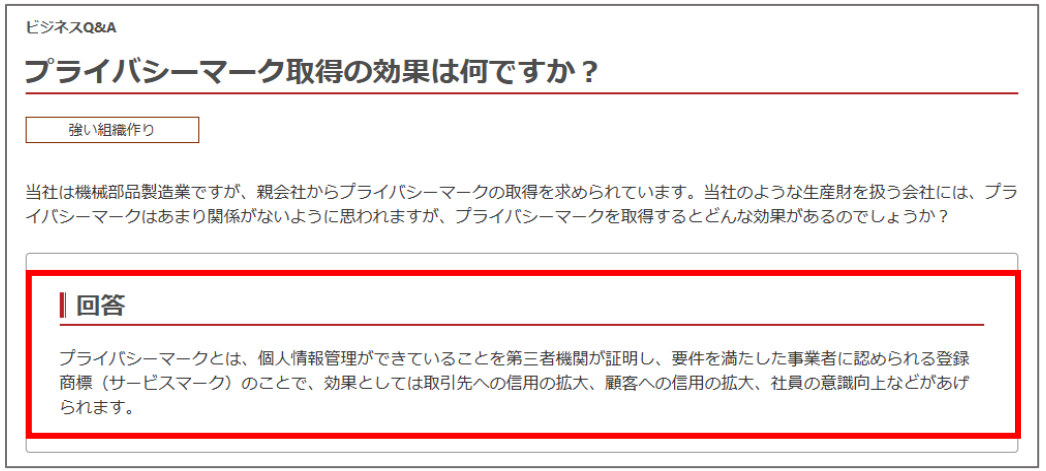
根拠1

J-Net21（中小企業ビジネス支援サイト）は、プライバシーマークについて**事業者が個人情報を適切に取り扱う体制を構築・運用していることを示す制度**である旨回答している。

＜その他ドキュメント＞

J-Net21（中小企業ビジネス支援サイト）のFAQ

https://j-net21.smrj.go.jp/qa/org/Q0718.html



ビジネスQ&A

プライバシーマーク取得の効果は何ですか？

強い組織作り

当社は機械部品製造業ですが、親会社からプライバシーマークの取得を求められています。当社のような生産財を扱う会社には、プライバシーマークはあまり関係がないように思われますが、プライバシーマークを取得するとどんな効果があるのでしょうか？

回答

プライバシーマークとは、個人情報管理ができていることを第三者機関が証明し、要件を満たした事業者に認められる登録商標（サービスマーク）のことで、効果としては取引先への信用の拡大、顧客への信用の拡大、社員の意識向上などがあげられます。

2省GLの整理

1.焦点　2.体裁

論点①

4. 対象事業者と医療機関等の合意形成 （20頁）
4.4. 対象事業者の適格性を評価する第三者認証等の取得に係る要件（23頁）

＜対応Lv1：方向性＞

- **プライバシーマーク認証を取得していることが望ましい理由を具体的に記載**する。

＜対応Lv2：対応必要事項＞

医療情報の機微性に鑑み、対象事業者は、医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、情報セキュリティに係る公的な第三者認証等として、プライバシーマーク認定またはISMS認証を取得すること。特に、事業者が個人情報を適切に取り扱う体制を構築・運用していることを示す制度であるプライバシーマーク認定を取得していることが望ましい。また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。そのため、ISMS認証のみを取得する場合には、事業者における具体的な管理方法の説明等を検討する等、医療機関等から有効性を示す資料の提供を求められた場合に対応できる状態としておくことが望ましい。医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定または ISMS 認証の取得が強く求められる。
なお、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 3 年3 月 30 日各府省情報化統括責任者（CIO）連絡会議決定）で示されている「クラウドセキュリティ認証等」（表 4-1 参照）は、プライバシーマーク認定や ISMS 認証と同等の認証等と認められるため、これに代えることも可能である。ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではないことに留意すること。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点②

4. 対象事業者と医療機関等の合意形成 （20頁）
4.4. 対象事業者の適格性を評価する第三者認証等の取得に係る要件（23頁）

＜論点②＞

対象事業者が**「安全対策の有効性」、「安全管理水準」を満たす対応が必要**であるため、**具体的な対応策が記載されているガイドラインの該当箇所の明記**が必要ではないか。

＜2省GL該当箇所の記載　23～24頁＞

医療情報の機微性に鑑み、対象事業者は、医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、情報セキュリティに係る公的な第三者認証等として、プライバシーマーク認定またはISMS認証を取得すること。特に、プライバシーマーク認定を取得していることが望ましい。また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。そのため、ISMS認証のみを取得する場合には、事業者における具体的な管理方法の説明等を検討する等、医療機関等から有効性を示す資料の提供を求められた場合に対応できる状態としておくことが望ましい。医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定または ISMS 認証の取得が強く求められる。

なお、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 3 年3 月 30 日各府省情報化統括責任者（CIO）連絡会議決定）で示されている「クラウドセキュリティ認証等」（表 4-1 参照）は、プライバシーマーク認定や ISMS 認証と同等の認証等と認められるため、これに代えることも可能である。**ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではない**ことに留意すること。

根拠1

2省ガイドラインの目次によると、**第５章にて「安全管理のためのリスクマネジメントプロセス」、第６章にて「制度上の要求事項」が記載**されている。

＜2省ガイドライン＞

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第 2.0版 目次

01gl_20250328.pdf

2省GLの整理

1.焦点　2.体裁

論点②

4. 対象事業者と医療機関等の合意形成 （20頁）
4.4. 対象事業者の適格性を評価する第三者認証等の取得に係る要件（23頁）

＜対応Lv1：方向性＞

- **安全管理水準を満たすために必要な対策等が記載されている箇所を明記**する。

＜対応Lv2：対応必要事項＞

医療情報の機微性に鑑み、対象事業者は、医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、情報セキュリティに係る公的な第三者認証等として、プライバシーマーク認定またはISMS認証を取得すること。特に、プライバシーマーク認定を取得していることが望ましい。また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。そのため、ISMS認証のみを取得する場合には、事業者における具体的な管理方法の説明等を検討する等、医療機関等から有効性を示す資料の提供を求められた場合に対応できる状態としておくことが望ましい。医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定または ISMS 認証の取得が強く求められる。

なお、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 3 年3 月 30 日各府省情報化統括責任者（CIO）連絡会議決定）で示されている「クラウドセキュリティ認証等」（表 4-1 参照）は、プライバシーマーク認定や ISMS 認証と同等の認証等と認められるため、これに代えることも可能である。ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではないことに留意すること。

本ガイドラインが求める安全管理水準に関しては、本ガイドライン第5章記載の安全管理のためのリスクマネジメントプロセス、同ガイドライン第6章記載の制度上の要求事項を参照すること。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）

＜論点無し＞
対象事業者が実施すべきリスクマネジメントのプロセスとして「リスクアセスメント」、「リスク対応」、「リスクコミュニケーション」等の各プロセスで実施する内容の定義及びプロセスの詳細な実施方法について述べているため、**論点無し**とする。

＜2省GL該当箇所の記載 27頁＞
本節では、対象事業者が実施すべきリスクマネジメントのプロセスとして「リスク特定、リスク評価、リスク分析」（以下、「リスクアセスメント」という。）や「リスク対応」、「リスクコミュニケーション」等の各プロセスで実施する内容について定義する。また、対象事業者は 5.1.1～5.1.5 のプロセスの実施にあたり、詳細な実施方法については 5.2 に記載する実施例を参考にし、抜け漏れなく対策をとりまとめること。なお、対象事業者は、リスクマネジメントの実践にあたり、医療情報システム等及び医療機関等との責任分界のあり方も含めて考慮すべき観点（医療情報の重要性を鑑みた高い機密性、医療の継続性を確保するための可用性、法定保存義務を担保するための完全性、等）を踏まえて内容の設計を行うこと。

2省GLの整理

1.焦点　2.体裁

論点①

5．安全管理のためのリスクマネジメントプロセス （27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.1 リスク特定（27頁）

＜論点①＞

今後のクラウドコンピューティングサービスの形態が変化することを想定し

ASP・SaaS と PaaS、IaaSの表現のみでよいか？

＜2省GL該当箇所の記載　27～29頁＞

対象事業者は、自らが提供する医療情報システム等の全体構成図を作成することで、医療情報システム等の全体構成を明らかにすること。その上で、医療情報システム等の全体構成図をもとに、医療情報システム等のライフサイクルにおけるフェーズ毎の情報流を特定すること。本ガイドラインでは、医療情報システム等の提供に関わる情報の流れを「情報流」と定義する。情報流にはネットワークを介した電子的な情報の流れだけでなく、記憶媒体の搬送により発生する情報の移動も含まれる。全体構成図をもとに情報の作成及び参照、更新、保存、移送、廃棄等の処理を洗い出すと、構成要素間で情報がどのように流れるのかが明らかになるため、結果として情報流が特定される。このとき、情報流を洗い出す範囲には、ICT サプライチェーン全体を含めること。特に、医療情報システム等をクラウドサービス等として提供するケースにおいては、**ASP・SaaS と PaaS、IaaS** をそれぞれ別の事業者が提供する等、ICT サプライチェーンが複雑となる傾向にあるため、抜け漏れがないよう十分留意すること。

次に、対象事業者は、洗い出した情報流について、当該情報流で処理を行う対象の情報の安全管理上の重要度に応じて分類すること。例えば、診療録や診療諸記録、処方箋、レセプト情報等は、「患者情報」等として分類し、「アプリケーションの設定情報」や「テストデータ」等とは区別した分類とすること。このとき、アプリケーションを提供する等により、情報の中身を意識した情報の処理を行う対象事業者においては、医療機関等が医療情報安全管理ガイドラインに基づき実施する情報の分類の結果について、医療機関等へ情報提供を求め、分類の参考とすることが望ましい。逆に、プラットフォームやインフラのみを提供する等により、処理する詳細な情報の中身が不明な場合「アプリケーション提供に係る情報（医療情報を含む可能性のある情報）」とそれ以外の情報（機器や OS/ミドルウェアの設定情報等）を最低限区別した分類とすること。

さらに、対象事業者は、洗い出した情報流に対して、表 5-1 に示す「医療情報システム等提供上の代表的な脅威」（以下、「代表的な脅威」という。）をあてはめ、当該情報流に対してそれぞれの脅威が顕在化した場合に生じ得るリスクを特定すること。ただし、代表的な脅威については、ISO /IEC 27005:2018 の附属書 C「典型的な脅威の例」を参考に、本ガイドラインにて独自に整理したものであり、医療情報に関する全ての脅威を網羅しているものではない。したがって、対象事業者は、代表的な脅威以外の脅威についても、提供する医療情報システム等の構成に応じて検討し、リスクを特定すること。

表 5-1 医療情報システム等提供上の代表的な脅威

根拠1

NISTのクラウドコンピューティングの定義において、サービスモデルは、ASP・SaaS と、PaaS、IaaS、**その他のクラウドコンピューティングサービス**で構成されている。

＜その他の資料＞

NISTのクラウドコンピューティング定義
https://csrc.nist.gov/Projects/cloud-computing

クラウドコンピューティングは、構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービスなど）の共有プールへの便利なオンデマンドネットワークアクセスを可能にするモデルです。これらのリソースは、最小限の管理作業やサービスプロバイダーとのやり取りで迅速にプロビジョニングおよびリリースできます。このクラウドモデルは可用性を高め、5つの基本特性（オンデマンドセルフサービス、広範なネットワークアクセス、リソースプーリング、迅速な柔軟性、計測されたサービス）、3つのサービスモデル（クラウドSaaS（Software as a Service）、クラウドPaaS（Platform as a Service）、クラウドIaaS（Infrastructure as a Service）、そして4つの導入モデル（プライベートクラウド、コミュニティクラウド、パブリッククラウド、ハイブリッドクラウド）で構成されています。主要な実現技術としては、（1）高速な広域ネットワーク、（2）高性能で安価なサーバーコンピュータ、（3）汎用ハードウェア向けの高性能仮想化などが挙げられます。

2省GLの整理

1.焦点　2.体裁

論点①

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.1 リスク特定（27頁）

＜対応Lv1：方向性＞

- ASP・SaaS と PaaS、IaaSに加え、将来的にサービス形態が増える可能性も考慮し、**「その他のクラウドコンピューティングサービス」の記載を追記**してはどうか。

＜対応Lv2：対応必要事項＞

対象事業者は、自らが提供する医療情報システム等の全体構成図を作成することで、医療情報システム等の全体構成を明らかにすること。その上で、医療情報システム等の全体構成図をもとに、医療情報システム等のライフサイクルにおけるフェーズ毎の情報流を特定すること。本ガイドラインでは、医療情報システム等の提供に関わる情報の流れを「情報流」と定義する。情報流にはネットワークを介した電子的な情報の流れだけでなく、記憶媒体の搬送により発生する情報の移動も含まれる。全体構成図をもとに情報の作成及び参照、更新、保存、移送、廃棄等の処理を洗い出すと、構成要素間で情報がどのように流れるのかが明らかになるため、結果として情報流が特定される。このとき、情報流を洗い出す範囲には、ICT サプライチェーン全体を含めること。特に、医療情報システム等をクラウドサービス等として提供するケースにおいては、ASP・SaaS と PaaS、IaaS、その他のクラウドコンピューティングサービスをそれぞれ別の事業者が提供する等、ICT サプライチェーンが複雑となる傾向にあるため、抜け漏れがないよう十分留意すること。

（略）

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点②

5．安全管理のためのリスクマネジメントプロセス （27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.2. リスク分析（29頁）

＜論点②＞

ISO/IEC 27005:2018の最新版である2022規格が発行されたため、

ISO/IEC 27005:2022規格を参考にする必要があるのではないか。

＜2省GL該当箇所の記載　29～30頁＞

対象事業者は、特定したリスクについて、「医療情報システム等への影響の度合い」（以下、「影響度」という。）と「当該リスクが顕在化する可能性」（以下、「顕在化率」という。）をもとに、「リスクの大きさの度合い」（以下、「リスクレベル」という。）を算出すること。

リスク分析の手順として、まず、対象事業者は、特定したリスクについて、リスクを洗い出す際のもととなった情報流の分類を参考に、当該リスクが顕在化した場合の医療情報システム等への機密性、完全性、可用性への影響度合いを総合的に判断し、リスクの影響度を特定すること。例えば、リスクを洗い出す際のもととなった情報流の分類が「患者個人情報等」であり、当該情報が頻繁かつ大量に処理されるような場合は、リスクの影響度は極めて大きいと考えられる。

次に、対象事業者は、被害が発生する際の前提条件等をもとにリスクの顕在化率を特定すること。例えば、サイバー攻撃においては、インターネット経由で直接的な攻撃が可能である場合や、認証を要求していない場合、既に攻撃手法が知られており被害が発生している場合等は、顕在化率は高いと考えられる。一方、施設へ物理的な侵入を行わないと攻撃ができない場合や、多要素認証を要求している場合、攻撃手法が知られておらず攻撃難易度が高い場合等は、顕在化率が低いと考えられる。

本ガイドラインでは、リスク分析手法の実践例として、影響度と顕在化率をもとに、5段階のリスクレベルに分類する例を表 5-2 に示す。対象事業者は**ISO/IEC 27005:2018** の規格等も参考に自ら適切なリスク分析手法を選択し適用すること。

表 5-2 リスクレベルの分類例

根拠1

ISO/IEC 27005:2022 第4版の日本語版が発行された。これは、情報セキュリティマネジメントシステム (ISMS) の国際規格である ISO/IEC 27001の2022年版改定に合わせて更新されたものである。

＜その他の資料＞

2024年12月4日一般財団法人日本情報経済社会推進協会
ISO/IEC 27000 ファミリー規格について（10頁）
27000family_20241204.pdf

日本規格協会グループより邦訳版が発刊されている
ISO/IEC 27005:2022 情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティリスクの管理に関する手引 | 日本規格協会 JSA Group Webdesk

補足
SO/IEC 27001 は、組織が情報セキュリティマネジメントシステム (ISMS) を確立し、実施し、維持し、継続的に改善するための要求事項を定めた規格。一方、ISO/IEC 27005 は、その ISO/IEC 27001 の中で要求されている「情報セキュリティリスクアセスメント」および「リスク対応」のプロセスを、どのように実施すればよいかの具体的なガイダンスを提供する規格。

2省GLの整理

1.焦点　2.体裁

論点②

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.2. リスク分析（29頁）

＜対応Lv1：方向性＞

- ISO/IEC 27005:2018のみならず、**ISO/IEC 27005:2022**として改定されているので、本規格も参考に自ら適切なリスク分析手法を選択し適用するよう記載してはどうか。

＜対応Lv2：対応必要事項＞

対象事業者は、特定したリスクについて、「医療情報システム等への影響の度合い」（以下、「影響度」という。）と「当該リスクが顕在化する可能性」（以下、「顕在化率」という。）をもとに、「リスクの大きさの度合い」（以下、「リスクレベル」という。）を算出すること。

リスク分析の手順として、まず、対象事業者は、特定したリスクについて、リスクを洗い出す際のもととなった情報流の分類を参考に、当該リスクが顕在化した場合の医療情報システム等への機密性、完全性、可用性への影響度合いを総合的に判断し、リスクの影響度を特定すること。例えば、リスクを洗い出す際のもととなった情報流の分類が「患者個人情報等」であり、当該情報が頻繁かつ大量に処理されるような場合は、リスクの影響度は極めて大きいと考えられる。

次に、対象事業者は、被害が発生する際の前提条件等をもとにリスクの顕在化率を特定すること。例えば、サイバー攻撃においては、インターネット経由で直接的な攻撃が可能である場合や、認証を要求していない場合、既に攻撃手法が知られており被害が発生している場合等は、顕在化率は高いと考えられる。一方、施設へ物理的な侵入を行わないと攻撃ができない場合や、多要素認証を要求している場合、攻撃手法が知られておらず攻撃難易度が高い場合等は、顕在化率が低いと考えられる。

本ガイドラインでは、リスク分析手法の実践例として、影響度と顕在化率をもとに、5段階のリスクレベルに分類する例を表 5-2 に示す。対象事業者は ISO/IEC 27005:2018及びISO/IEC 27005:2022の規格等も参考に自ら適切なリスク分析手法を選択し適用すること。

表 5-2 リスクレベルの分類例

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.3. リスク評価（30頁）

＜論点無し＞

対象事業者は、各リスクについて、リスクレベルをもとに対応要否を検討し、各社が通常用意していると考えられる「リスクアセスメント結果一覧」を作成することを記載しているため、**論点無し**とする。

＜2省GL該当箇所の記載 30頁＞

対象事業者は、各リスクについて、リスクレベルをもとに対応要否を検討し、リスクアセスメント結果一覧を作成する。この際、リスクレベルに応じた対応基準（以降、「リスク基準」という。）を定めておくのも一案である。例えば、表 5-2 のように S ランク～D ランクにリスクレベルを分類した場合のリスク基準の例として、S ランクについては複数の対策による対応を必須、A ランクは対応を必須、B～C ランクはリスクレベルの高いものを優先しつつも個別事情も勘案した上で対応の要否を検討、D ランクは対応を不要とする等のリスク基準が考えられる。

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.4. リスク対応の選択肢の選定（30頁）

＜論点無し＞

リスク対応の選択肢の選定について4種類に分類され、それぞれ具体例も挙げながら分かりやすく記載されているため、**論点無し**とする。

＜2省GL該当箇所の記載 30～32頁＞

対象事業者は、5.1.1～5.1.3 に係るリスクアセスメントの結果を踏まえ、リスク対応の選択肢を選定すること。このとき、リスク対応の選択肢としては、表 5-3 に示す「リスク低減」、「リスク回避」、「リスク共有」、「リスク受容」の 4 種類に分類される。
表 5-3 リスク対応の選択肢
図 5-2 に影響度と顕在化率に応じた選択肢の考え方を示す。対象事業者は、リスク低減を中心としつつ、費用対効果を念頭に置いた上で最適なリスク対応の組み合わせを検討すること。なお、対象事業者の判断のみによってリスク共有やリスク受容を選択することは適当ではなく、医療機関等への説明や合意形成の上、これを選択すること。このとき、それぞれのリスク対応において、対象事業者に求める事項を次の(1)～(4)に記載する。
図 5-2 影響度と顕在化率に応じた選択肢の考え方
(1)リスク低減
対象事業者は、対応が必要とされたリスクについては、原則として、リスク低減について検討すること。このとき、費用対効果を踏まえつつ、脅威に応じて適切なリスク低減が行えるよう、対策を複数組み合わせることによる多層防御（多重防御ともいう）を講じることが望ましい。
(2)リスク回避
対象事業者は、影響度及び顕在化率ともに極めて高いリスクについては、リスク回避を検討すること。例えば、「外部と大量の個人情報の電子メールによる受け渡し」が頻繁に発生する場合、誤送信による情報漏洩リスクの影響度及び顕在化率は極めて高いと判断することができる。こういったケースでは、教育や誤送信対策システムの導入等によるリスク低減策よりも、別の手段により個人情報を受け渡すリスク回避策のほうが有効となることもあり得る。
(3)リスク共有
リスク低減を行った結果、顕在化率の低減は可能だが影響度の低減は困難なリスクについては、リスク共有を検討することが有効である。例えば、情報流の一部を他社に委託することにより、サイバー攻撃で被害を受けたとしても、契約等により被害に対する損害賠償責任の一部を委託先に移転することができる。また、リスクが顕在化し損害賠償を求められた時に備えて、サイバー保険等により金銭的な損失を補填することができる。ただし、サイバー保険等によるリスク共有は、あくまでも金銭面での損失にのみ有効な対応であり、情報セキュリティ事故発生時の被害や、医療機関等の信用失墜を防ぐものではない。このため、リスク共有はリスク低減を行った上で残存するリスクに対して適用を検討すべきである。
(4)リスク受容
対象事業者は、リスクアセスメントの結果、リスク低減等のリスク対応を検討した上で、残存するリスクについては、当該リスクを認識した上でリスク保有を検討すること。

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.5. リスク対応策の設計･評価（32頁）

＜論点無し＞

GL本文から別紙２の位置づけも含め、リスク対応策の設計の基本的な考え方が読み取れるため、**論点無し**とする。

＜2省GL該当箇所の記載 32～33頁＞

(1)リスク対応策の設計
対象事業者は、リスク対応策について、次に示す基本的な考え方と医療情報システム等特有の考慮事項を踏まえて設計すること。
(ア)基本的な考え方
対象事業者は、対策の設計にあたっては、医療機関等が医療情報安全管理ガイドラインを遵守できるような設計となっていることについて、3.1.2 で述べた説明義務を有していることに留意しなければならない。ここで、対策の設計や、設計した対策の妥当性を判断するにあたっては、高度な専門性が要求されるが、従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を医療情報安全管理ガイドラインとの対応関係を踏まえ対策項目として整理・統合した別紙 2 を用い、その全ての対策項目について対応していることを確認をすることは、対象事業者による対策の設計や妥当性の判断、説明義務への対応において必須である。また、リスク対応策を取りまとめる際には、「人的・組織的」、「物理的」、「技術的」の 3 つの対策の観点について、特定の観点の対策に依らず、複数観点を組み合わせた対策の設計が重要である。例えば、不正な閲覧・操作を防止するための技術的対策として、利用者認証を講じるような場合は、併せて人的・組織的対策として利用者の教育を行い、利用者認証に用いる IC カードやパスワード等の認証情報の適切な管理を求める必要があると考えられる。また、IC カードと静脈認証等により特定の医療従事者のみを入室可能とする物理的対策を講じた区画においては、入室記録および作業記録で、当該医療従事者と作業内容を結びつけることが可能な場合はパスワード等による認証は不要と判断することも考えられる。
さらに、対策を設計する際に、別紙 2 に書かれている「対策項目で対応できるリスクシナリオ（例）」を参考にすることも有効である。ただし、当該リスクシナリオ例はあくまで参考例であり、関連するリスクと対策が他にも存在しないかを対策の設計を行う際に確認すること。

2省GLの整理

1.焦点　2.体裁

論点③

5．安全管理のためのリスクマネジメントプロセス （27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.5. リスク対応策の設計･評価（32頁）

＜論点③＞
(イ)医療情報システム等特有の考慮事項について、**他に考慮すべき事項**はないか。

＜2省GL該当箇所の記載　33～34頁＞

(イ)医療情報システム等特有の考慮事項
対象事業者は、対策の設計にあたっては上記で示す基本的な考え方に加え、以下に記載する医療情報システム等特有の考慮事項を参照し、必要な対策を設計すること。
① 利用者認証における考慮事項
医療情報の機密性の高さや攻撃手法の高度化に鑑み、多要素認証（知識認証、物理認証、生体認証のうち異なる 2 つ以上の要素を用いる認証方式）を可能な限り早期に採用すべきである。医療情報安全管理ガイドラインでは、令和 9 年度時点で稼働していることが想定される医療情報システムでは、二要素認証（又はこれに相当する対応）を採用することとしている。
② ログの保存期間における考慮事項
取り扱う医療情報に法定保存年限が設けられている場合は、当該医療情報に関するアクセスを記録したログについて、原則として法定保存年限以上の保存期間を設けること。なお、対応すべき法定保存年限が超長期にわたる等、特殊な場合、医療機関等においてログを利用する目的やリスクに関して医療機関等と協議し、適切な保存期間を設けること。
③ ネットワーク経路における考慮事項
対象事業者は、提供するサービスに応じ、原則としてセキュアなネットワークを採用し、ネットワーク経路を適切に選択することが必要である。また、医療情報の機密性の高さや攻撃手法の高度化に鑑みた上で、様々な攻撃を想定し、適切な暗号化手法を選択すべきである。例えば医療情報安全管理ガイドラインでは、特にオープンなネットワークにおける接続に際して HTTPS 利用における TLS を用いた暗号化等が例示されている。そこでは、HTTPS 接続を利用する場合、TLS の設定はサーバ/クライアントともに CRYPTREC が定める「TLS 暗号設定ガイドライン（第 3.1 版）令和 2 年 7 月 8 日」（以下、「TLS 暗号設定ガイドライン」という。）に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと、また、SSL-VPN を原則として利用せず、やむを得ず SSL-VPNを利用する場合は、TLS 暗号設定ガイドラインに基づき、「クライアント型」での VPN とすること、そして、IPsec を用いる場合は、IKE を組み合わせる等して、確実にその安全性を確保するように求めている。
④ 無線 LAN の端末接続制限における考慮事項
無線 LAN の端末接続制限に係る対策として、MAC アドレスを用いた端末接続制限が一般的に知られているが、MAC アドレスは容易になりすまし可能であるため、医療情報の機密性の高さや攻撃手法の高度化に鑑み、MAC アドレスを用いた端末接続制限に加えてIEEE 802.1X と電子証明書を組み合わせる等のより安全な方法を採用すべきである。
⑤ 小型半導体メモリやクラウド上のストレージサービスの利用における考慮事項
記憶媒体のうち、小型で記憶容量が大きい小型半導体メモリは、衣服等のわずかな隙間にも隠すことができるため、不正な情報の持ち出しに利用しやすいものといえる。対象事業者は、原則として医療情報を格納する記憶媒体として小型半導体メモリの使用を行うことができないよう配慮することが望ましい。また、最近はクラウド上のサービスで容易に外部にデータを保存したり、送付することができるものも多くみられる。このようなサービスについては、許可したもの以外はサービスへのアクセス制限を講じる、重要なデータについては外部に転送できないよう、ネットワークの分離を図るなどに配慮することなども求められる。
⑥ 事業継続計画の策定における考慮事項
事業継続計画の策定において、医療機関等が想定する医療の継続性の観点を入れて計画を策定すること。また、対象事業者は、「災害等によりシステムが停止した場合」だけでなく、システムが正常であったとしても「災害等により多数の傷病者が医療サービスを求める状態となり、通常の手段では著しい不都合が生じる場合」や「一定期間停止したシステムを復旧して運用を再開する際に、情報の一部欠損の発生や情報の連続性が担保されないことにより不都合が生じる場合」についても考慮すること。

根拠1
データのバックアップをしっかり管理していた医療機関はランサムウェア攻撃の被害を避けられた事例があるが、データバックアップと復元は近年重要性を増している。

根拠2
医療従事者の人為的なミスにより患者情報が漏えいした事例があるが、人為的ミスによるインシデントはなくならず、従業員教育と意識向上については徹底する必要がある。

＜その他の資料＞
PHCホールディングス株式会社のHP
https://www.phchd.com/jp/medicom/park/tech/ehr-backup-security
厚生労働省による電子カルテのバックアップの独立保管
近年、医療機関を狙うランサムウェア攻撃は増加しています。厚生労働省は2023年4月に医療法を改正し、医療機関は医療の提供に著しい支障が及ばないよう、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ることが求められるようになりました。
また、**ランサムウェア攻撃後の被害拡大や復旧までの期間、費用などを事例ごとに分析するとバックアップデータをオフラインで管理している医療機関は甚大な被害を避けられた**ことがわかっています。そのため、厚生労働省は万が一サイバー攻撃を受けたときに、甚大な被害を避けるためバックアップデータは複数の方式で管理すること、さらに少なくとも一つはネットワークから切り離した状態で管理することを新たに定めました。
また、ランサムウェアには感染後しばらくしてから攻撃をするタイプのものもあります。バックアップデータは週単位、月単位、年単位など複数の時点までさかのぼれるように世代で管理することも求められています。

＜事例＞
フィッシング詐欺による患者情報漏洩インシデントの発生について
https://www.okayama-u.ac.jp/user/hospital/news/detail284.html

令和3年7月23日，**岡山大学病院の医師が個人で使用していたクラウドサービス用ID及びパスワードをフィッシング詐欺により窃取され，当該ID・パスワードで紐づけられた個人のクラウド上の保存データ等にアクセスできなくなった**ことが判明しました。
当該クラウドサーバには，大学の規定に反して，治療経過を確認する資料として収集された延べ269人の個人情報を含む患者情報を記したファイルが保存されており，攻撃者により閲覧可能な状態になっています。
なお，現時点で情報の悪用等は確認されていません。また，大学基幹システム，電子カルテなどの医療情報システムへの不正アクセスも確認されていません。
引き続き，岡山県警察本部及び関係各所に協力を仰ぎながら，問題解決に努めます。
患者の皆さまや関係の皆さまにご心配ご迷惑をおかけし，誠に申し訳ございません。
8月2日から，該当する患者の皆さまに事実関係の説明とお詫びの文書を発送し，順次電話にて説明と謝罪を行っております。
本学では全職員に対して定期的に個人情報保護及び情報セキュリティの確保について，セキュリティ教育や研修を通じて継続的に啓発してまいりましたが，今回の事案では，**当該医師において本学の規定を遵守できておりませんでした。**本学の情報管理体制に不備があったことを深く反省し，今後このようなことが起きないよう，全職員への個人情報の管理及び情報セキュリティ意識に関する指導を徹底してまいります。

2省GLの整理

1.焦点　2.体裁

論点③

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.5. リスク対応策の設計･評価（32頁）

＜対応Lv1：方向性＞

- 医療情報システム等特有の考慮事項⑦として、**データバックアップと復元における考慮事項を明記**してはどうか。
- 医療情報システム等特有の考慮事項⑧として、**従業員教育と意識向上における考慮事項を明記**してはどうか。

＜対応Lv2：対応必要事項＞

(イ)医療情報システム等特有の考慮事項

対象事業者は、対策の設計にあたっては上記で示す基本的な考え方に加え、以下に記載する医療情報システム等特有の考慮事項を参照し、必要な対策を設計すること。

（略）

⑥ 事業継続計画の策定における考慮事項

事業継続計画の策定において、医療機関等が想定する医療の継続性の観点を入れて計画を策定すること。また、対象事業者は、「災害等によりシステムが停止した場合」だけでなく、システムが正常であったとしても「災害等により多数の傷病者が医療サービスを求める状態となり、通常の手段では著しい不都合が生じる場合」や「一定期間停止したシステムを復旧して運用を再開する際に、情報の一部欠損の発生や情報の連続性が担保されないことにより不都合が生じる場合」についても考慮すること。

⑦データバックアップと復元における考慮事項

医療情報の重要性を踏まえ、定期的なデータバックアップを実施し、バックアップデータの保管場所や方法を慎重に選定すること。また、バックアップデータの復元手順を確立し、定期的に復元テストを行い、データの完全性とアクセス可能性を確認することが必要である。

⑧従業員教育と意識向上における考慮事項

医療情報の取り扱いに関する従業員の教育と意識向上を図ること。定期的なセキュリティトレーニングの実施や、情報漏洩防止のためのガイドラインを従業員に周知することで、内部からのリスクを軽減することができる。

※下線を追記

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.5. リスク対応策の設計･評価（32頁）

＜論点無し＞

リスクの評価やリスク対応の文書化については、具体的な内容が他章にて記載されているため、**論点無し**とする。

＜2省GL該当箇所の記載 35頁＞

(2)医療機関等へ対応を求める事項の整理
対象事業者は、設計したリスク対応策のうち、医療機関等による対応が必要となる内容について、医療機関等へ対応を求める事項として整理すること。
(3)残存するリスクの評価
対象事業者は、医療機関等へ対応を求める事項を整理した上で、それでも残存するリスクについて改めてリスク評価（5.1.3）を実施すること。リスク評価の結果、残存するリスクの評価結果が対象事業者として許容できないと判断する場合は、リスク対応方法について再度検討すること。
(4)リスク対応の文書化
対象事業者は、リスク対応の選択肢についての選定結果及び、選定結果に基づき設計した対応策を「リスク対応一覧」として文書化すること。

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.6. リスクコミュニケーション（36頁）

＜論点無し＞

医療機関等とのリスクコミュニケーションの実施について、医療機関等に対して情報提供すべき内容に関して明確に記載されているため、**論点無し**とする。

＜2省GL該当箇所の記載 36頁＞

(1)医療機関等とのリスクコミュニケーションの実施

対象事業者は、自らが提供する医療情報システム等の安全管理に係る説明義務を果たし、医療機関との共通理解を形成するために、医療機関等に対して第 4 章で情報提供すべき内容として示した事項を含む必要な情報を文書化して提供すること。具体的には、5.1.5 で作成した「リスク対応一覧」や後述の運用管理規程に定められた事項に係る情報提供を通して、医療機関等との役割分担、対象事業者として受容したリスクの内容等について、医療機関等と合意形成すること。なお、その際には、対象事業者は、医療機関等が容易に理解可能となるよう内容を工夫する等、適切に共通理解を得ること。

医療機関等と対象事業者との間で合意形成する場合、事業者が提供するシステム・サービスの内容や、その契約形態などに応じて、具体的なコミュニケーションについて留意する必要がある。例えば医療機関等と対象事業者との間で、個々に契約内容等の調整を行うことを想定した医療情報システム等の提供と、パブリッククラウドサービスのように約款契約による画一的な契約内容による場合では、コミュニケーションの進め方は異なる。特に約款契約による場合には、個々の契約内容の調整が難しいことから、対象事業者は医療機関等に対して、より丁寧にサービス内容やリスクについて、わかりやすい情報提供を行うことが求められる。具体的には、以下のような対応を行うことが挙げられる。

- リスク判断に必要な基礎資料の提供（MDS/SDS 等の提供、主なセキュリティ事項に関するチェック結果の提供等）
- 医療機関等側から説明を求められた場合の対応の表示約款契約におけるリスクの表示（民法 548 条の 2 関係）
- 医療機関等が、リスクや役割分担等を確認した上でサービス利用する旨を明示し、合意すること

なお、医療機関等と合意に至らなかった場合は、対象事業者はリスク対応事項の見直し結果に基づく再協議、残存するリスクの共通理解に向けた再協議等、医療機関等と再度合意形成を図り、合意すること。

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.6. リスクコミュニケーション（36頁）

＜論点無し＞

リスクコミュニケーション不足がサイバー攻撃による被害発生の一因となった例の紹介にとどまるため、**論点無し**とする。

＜2省GL該当箇所の記載 37～38頁＞

【コラム：リスクコミュニケーション不足がサイバー攻撃による被害発生の一因となった例】
通常時や非常時へ対応するために、医療機関等と医療情報システム等事業者の間でリスクコミュニケーションを行い、リスク内容やその対応に関する認識や、両者での責任分界などについて共通理解を得ることが求められる。特に昨今のサイバー攻撃に対しては、両者の間で不一致がある場合、行うべき対策が漏れてしまう危険性もある。
その事案例として、「徳島県つるぎ町立半田病院」において発生したランサムウェア攻撃による被害事案を紹介する。本事案ではランサムウェアによる被害により、長期間診療が停止したほか、復旧に多額の費用を要した。また、その原因を分析するための報告書が示されている。
以下では同報告書において、課題として挙げられている内容をまとめた。この中では、いくつかの点について、医療機関等と事業者の間でリスクへの対応などについてのコミュニケーションが不足し、それが原因となって適切な対策が講じられなかったことがみられる。
1. 責任分界上の課題
医療機関と事業者の間でのセキュリティ対策及び緊急時の対応に関する責任分界や委託業務範囲が不明瞭
機器等の管理（脆弱性対策）に関する管理責任の範囲が不明瞭
電子カルテシステム等を導入した事業者と保守事業者の間での責任分界が不明瞭
セキュリティ情報の取り扱いに関する当事者間での責任分界が不明瞭
2. 初動対応上の課題
初動に関する全体的な対応計画が不足（事業者における情報不足に伴う不適切な対応等）
3. サービス提供上の課題
事業者における脆弱性情報の取り扱いに対する知見不足
情報セキュリティにおける脅威対応への知見不足を補うための体制構築
情報システム・サービスの運用において考慮すべき基本的セキュリティ（機密性）についての意識不足（可用性優先に伴い、脆弱性対策がおろそかになっていた）と、これに関する医療機関側との共通認識が不足
4. 設計上の課題
「医療情報システムの安全管理に関するガイドライン」に示す安全対策への未対応（バックアップ対応等）及び代替策に対する対応不足への認識が不明瞭（リスクコミュニケーション不足）

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.6. リスクコミュニケーション（36頁）

＜論点無し＞

リスクコミュニケーションにおける文書・規程の作成について、最低限必要な事項が具体的に述べられているため、**論点無し**とする。

＜2省GL該当箇所の記載　38～40頁＞

(2)文書・規程の作成
対象事業者は、医療機関等と合意したリスクへの対応を踏まえ、リスクに対する対応計画を策定すること。また、対象事業者が安全管理義務を果たすために、医療機関等と合意形成した結果を文書化し、**最低限、以下の(ア)～(サ)を含む運用管理規程を定めること。**
(ア)医療情報システム等の安全管理に係る基本方針
対象事業者は、医療情報システム等の安全管理に係る基本方針として、以下の事項を運用管理規程に含めること。
- 本ガイドライン及び医療情報安全管理ガイドラインの遵守
- 個人情報保護法やその他最新の関連法令等の遵守
- 個人情報に関して他の情報と区別した適切な管理
- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（平成 29 年 4 月 14 日通知、令和 6 年 3 月 27 日最終改正）」に基づき、患者等が死亡した後においても、当該患者等の情報を保存している場合には、死者に係る情報であっても、個人情報と同等の安全管理措置の実施
- 情報セキュリティに関する基本方針等の情報セキュリティポリシーの策定
- 情報セキュリティポリシーの遵守を担保する組織体制の構築

(イ)医療情報システム等の提供に係る体制
対象事業者は、医療情報システム等の提供に係る体制として、最終的な管理責任者や、十分な技術的能力及び経験31を有する責任者（システム管理者）、医療情報システム等の運用に関する事務を統括する責任者、個人情報保護に係る責任者を定め、これら責任者の役割や任命・解任等のルール、緊急時の対応と併せて運用管理規程に含めること。また、再委託を行う場合は、再委託先の体制に関する情報も運用管理規程に含めること。
(ウ)契約書・マニュアル等の文書の管理方法
対象事業者は、契約書や運用管理規程を含むマニュアル等の管理については、必要に応じて速やかに内容を確認できるようにすること。また、文書の不正な閲覧・操作をアクセス制限等により防止することを運用管理規程に含め、第三者による不正な閲覧・操作を防止すること。なお、アクセス制限を侵害する行為については、検出・記録できるような仕組みが実装されていることが望ましい。
(略)
(サ)医療機関等の管理者からの問い合わせ窓口
対象事業者は、医療機関等の管理者からの問い合わせ窓口として、医療機関等の管理者からの一元的な問い合わせ窓口となる連絡先及び連絡方法のほか、問い合わせを受け付ける時間帯について運用管理規程に含めること。

2省GLの整理

1.焦点　2.体裁

論点なし

5．安全管理のためのリスクマネジメントプロセス　（27頁）
5.1. リスクマネジメントの実践（27頁）
5.1.7. 継続的なリスクマネジメントの実践（40頁）

＜論点無し＞

5.1.1～5.1.6の総まとめとして、継続的なリスクマネジメントの実践について記載されているため、**論点無し**とする。

＜2省GL該当箇所の記載 40頁＞

5.1.1～5.1.6 に示したプロセスは、一度だけ実施すれば良いというものではない。対象事業者は、医療情報システム等における情報流や脅威の変化、想定外の事態の発生等に応じて、医療機関等との契約締結後も継続的に実施し、見直しを行うこと。
リスクコミュニケーションの対象となるリスクについては、事業者の選定時に認識された内容が、その後のサービス提供時において、変化しうることが指摘される。特にサイバーセキュリティにおいては、攻撃方法の巧妙化に伴い、選定時に想定したリスクよりも大きくなり、これに伴いリスク対応を改めて検討することが求められる。そのため、リスクコミュニケーションにおいては、対象事業者が行うリスクの管理体制や、リスクが選定時以降に上昇した場合の対応も含めた、随時の情報提供等を含めることが重要である。

2省GLの整理

1.焦点　2.体裁

論点①

6. 制度上の要求事項 （56頁）

6.1. 医療分野の制度が求める安全管理の要求事項（56頁）

＜論点①＞
医療情報及び当該情報に係る医療情報システム等は国内法の適用を受けるとの記載があるが、**データを海外に設置したサーバ等に転送、保存する場合における情報種別に関する記載**が必要ではないか。

＜2省GL該当箇所の記載　56頁＞
医療情報は患者の身体・生命に関わるものであり、その作成や保存は、医療従事者の責務として、医師法及び歯科医師法、薬剤師法、医療法等の法令において規定されている。また、医療従事者に対する業務上知り得た秘密の漏洩に関する罰則が刑法等において規定されている。
医療法では適切な医療提供体制の確保の一環として、都道府県知事等は必要に応じて医療機関等に対し、構造設備や診療録、帳簿書類その他の物件等の提出等を命じることができるとされており、当該命令に適切に対応しなかった場合の罰則も規定されている。したがって、医療機関等は調査機関等の検査に対し、適切に対応できるようにしなければならない。
以上のような法令で定められた医療機関等に対する義務や行政手続の履行を確保するために、**医療情報及び当該情報に係る医療情報システム等が国内法の執行の及ぶ範囲にあることを確実とすること。**

根拠1	根拠2	根拠3	根拠4
医療情報を外部保存する場合は、**国内法の適用を受ける**。	**個人情報**を外国にある第三者に提供する場合は、「外国にある第三者への個人データの提供を認める旨の**本人の同意**」**が必要**である。	**仮名加工情報**は原則として個人情報に該当するため、外国にある第三者に提供する場合は、**本人の同意が必要**である。	**匿名加工情報**は、**本人の同意なく第三者提供可能**である。

＜厚労省ガイドライン＞
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　27頁
https://www.mhlw.go.jp/content/10808000/001102575.pdf
外部の事業者との契約に基づいて**医療情報**を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。
－ 保存した医療情報の取扱いに関して監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。
（略）
－ 保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。

＜個人情報の保護に関する法律についてのガイドライン＞
個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）2章
https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a2-1
2　総論
個人情報取扱事業者は、個人データを外国にある第三者に提供するに当たっては、法第28条第1項に従い、次の(1)から(3)までのいずれかに該当する場合を除き、あらかじめ**「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要がある。**
（中略）2-1 外国にある第三者への個人データの提供を認める旨の本人の同意
ここでいう「本人の同意」とは、**本人の個人データが、個人情報取扱事業者によって外国にある第三者に提供されることを承諾する旨の当該本人の意思表示**をいう。

＜FAQ＞
個人情報保護委員会HPのFAQ
https://www.ppc.go.jp/all_faq_index/faq1-q14-1/
（中略）これに対し、**仮名加工情報**は、他の情報と照合しない限り特定の個人を識別できないように加工した個人に関する情報（法第２条第５項）であり、仮名加工情報を作成した個人情報取扱事業者においては、通常、当該仮名加工情報の作成の元となった個人情報や当該仮名加工情報に係る削除情報等を保有していると考えられることから、**原則として「個人情報」（法第２条第１項）に該当する**ものです。

＜個人情報の保護に関する法律についてのガイドライン＞
個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）付録
https://www.ppc.go.jp/personalinfo/legal/guidelines_anonymous/#a2
＜仮名加工情報と匿名加工情報の取扱いに関する主な規律の差異（概要）（※1）＞の表の記載抜粋

提供に関する規律
- **匿名加工情報**（※3）
  - **本人同意なく第三者提供可能**
  - 提供時に、匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法の公表、並びに匿名加工情報である旨の提供先に対する明示（法第43条第4項、第44条）

2省GLの整理

1.焦点　2.体裁

論点①

6. 制度上の要求事項 （56頁）

6.1. 医療分野の制度が求める安全管理の要求事項（56頁）

＜対応Lv1：方向性＞

- データを海外に設置したサーバ等に転送、保存する場合における情報種別について、**参照すべきドキュメントを注釈に記載**する。

＜対応Lv2：対応必要事項＞

医療情報は患者の身体・生命に関わるものであり、その作成や保存は、医療従事者の責務として、医師法及び歯科医師法、薬剤師法、医療法等の法令において規定されている。また、医療従事者に対する業務上知り得た秘密の漏洩に関する罰則が刑法等において規定されている。

医療法では適切な医療提供体制の確保の一環として、都道府県知事等は必要に応じて医療機関等に対し、構造設備や診療録、帳簿書類その他の物件等の提出等を命じることができるとされており、当該命令に適切に対応しなかった場合の罰則も規定されている。したがって、医療機関等は調査機関等の検査に対し、適切に対応できるようにしなければならない。

以上のような法令で定められた医療機関等に対する義務や行政手続の履行を確保するために、医療情報及び当該情報に係る医療情報システム等が国内法の執行の及ぶ範囲にあることを確実とすること（※）。

＜注釈部分＞

（※）情報の取り扱いに関しての解釈は、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　企画管理編、個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）、個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）を参照し、適切に対応できるようにすること。

※下線を追記

有識者ヒアリング概要

- セキュリティ専門家2人、情報セキュリティ事業者２社の４対象に有識者ヒアリングを実施

ヒアリング先	バックグラウンド	ヒアリング観点
セキュリティ専門家A	• 医師・医学博士 • 医療情報標準化や安全管理を推進	• 医療情報標準化や安全管理を熟知されている認識であり、**医療情報標準化や安全管理**の観点から検討内容に対するヒアリングを実施。
セキュリティ専門家B	• 大手セキュリティソフトウェア会社にて医療機関向けのセキュリティ対策導入支援、医療業種ビジネス開発に従事 • 厚生労働省や経済産業省、総務省の医療情報セキュリティ関連のガイドライン検討班、委員会などにも協力	• インシデント対応・評価など豊富な実績、知見をお持ちの認識であり、**サイバーセキュリティ**の観点から検討内容に対するヒアリングを実施。
情報セキュリティ事業者A	• X線・画像診断装置等の医療機器メーカー	• X線・画像診断装置等の医療機器メーカーとして、安全性・規制遵守を重視されており、長期利用を前提とされた商品／サービス提供をされている認識であり、**医療機器のセキュリティ確保**等から検討内容に対するヒアリングを実施。
情報セキュリティ事業者B	• 医療データの統合・活用を進めるヘルスケアIT企業	• 医療データを安全に連携・統合するプラットフォームを取り扱われており、臨床・研究データの品質保全と解析を柱にしている認識であり、**可用性・即応性**等から検討内容に対するヒアリングを実施。

有識者ヒアリングを踏まえた2省GLの今後の論点案（1/3）

- 有識者ヒアリング実施結果を踏まえ、２省GLの見直しにあたっては、サプライチェーン責任の明確化といった論点を協議していくことが、実効性確保につながると考えられる

	改定に向けた方向性仮説	有識者ヒアリング結果	ヒアリング結果を踏まえた論点
1. サプライチェーン全体のリスク管理と透明性の確保	• 事業者は、再委託先を含むサプライチェーン等の管理状況について可視化し、医療機関等へ「サービス仕様適合開示書」等を用いて正確に情報提供すること。特に、SaaSベンダはSaaSベンダが当該再委託先をも含む責任範囲までを含め提示し、事業者は、再委託先の詳細リスト提出が困難な場合、再委託先等に起因するインシデントについても、元請け事業者が一切の免責なく賠償・復旧責任を負う」旨をSLAおよび契約約款に明記すること。 • SaaS利用時において、医療機関が直接関与できない「再委託先（IaaS/PaaS事業者等）」のリスクについて、プライム事業者が「自社の責任において再委託先のセキュリティ状態を監査・保証する」旨を契約条項に盛り込むことを、2省GLのモデル契約等で標準化すべきではないか。 • クラウドサービスの設定ミス（公開範囲など）による事故を防ぐため、事業者は「医療機関向けにセキュアに設定済みのテンプレート」を提供する責務を負い、医療機関側が設定変更しない限り安全が保たれる状態を「納品」の定義とすべきではないか。	• 医療機関はサービス単位で契約するため、サプライチェーンの管理はプライム事業者が責任を持つべきであり、**契約内容はサービスごとに整理する**必要がある。 • 事業者（特にオンプレ・ディーラー含む）が2省GLを十分理解していないため、**最低限のリスクシナリオや構成例などを示さないと対策が浸透しない**。	• サービス単位での契約実態を踏まえ、**プライム事業者によるサプライチェーン全体の責任範囲や管理のあり方をどのように整理・明確化**するか • オンプレ事業者やディーラーも含めた理解促進に向けて、**最低限のリスクシナリオや構成例など具体的な指針をどこまで提示**するか
2.サイバー攻撃（ランサムウェア）対応型のバックアップと復旧支援	• 事業者は、バックアップデータがランサムウェアの影響を受けないよう、オフライン保管や不変性（WORM機能）を標準機能またはオプションとして具備し、医療機関等が専門的な設定を行わずともランサムウェア対策が機能する状態を提供すること。また、システム復旧手順を整備し、医療機関等と共同で訓練を実施できる体制を提供すること。 • 他方、災害等の復旧対応、パッチ処理にかかる対応期間は相応に要することから、例えばベンダ切り替え時に行うなど現場のオペレーションに影響のない稼働・運用で行うことについて、事業者から提案を行うこと。加えて、ベンダが不正アクセスを受けている状況を把握する観点から、ベンダのセキュリティ基準も提出させること。	• オフラインデータ保管は重要であるが、入力対応には整合性確保の課題があるため、**診療継続に最低限の情報は何か、まず閲覧可能とする範囲を明確に示す**ことが重要である。 • 高価な対策よりも、**強固なパスワード運用・アップデート・運用による監視など基本的なセキュリティ対策を徹底することがランサムウェア対策として重要**である。	• **診療継続の観点から、オフライン環境で確保すべき最低限の情報範囲や「閲覧・入力」の要件をどのように整理・明確化**するか • 高度な対策に偏らず、**パスワード管理やパッチ適用など基本的対策をどのように優先事項として位置づけ、確実な実施を促す**か

有識者ヒアリングを踏まえた2省GLの今後の論点案（2/3）

- 有識者ヒアリング実施結果を踏まえ、２省GLの見直しにあたっては、セキュリティ強化と現場運用の両立といった論点を協議していくことが、実効性確保につながると考えられる

	改定に向けた方向性仮説	有識者ヒアリング結果	ヒアリング結果を踏まえた論点
3.高度な認証方式（多要素認証）の実装	• 2027年度を皮切りに原則として二要素認証（多要素認証）を採用したシステムを設計・提供することを明記すること。ただし、導入コストや業務効率への影響が大きい場合、「場所や端末による制限（リスクベース認証）」等の代替策を提案・実装し、段階的な移行計画（2027年に向けたロードマップ）を提示すること。 ※救急対応を考慮し、物理専用カードを有していなければ入ることのできない等の環境上の配慮がなされている場合には、システム自体の２要素認証の運用を緩和することは可能とすることを検討論点として提示すること	• 多要素認証は重要である一方、救急現場では迅速な情報共有とのバランスが必要であるため、ホワイトボード的な運用も含め、**物理的配慮も含めた現場実態に即した柔軟な運用のあり方をガイドラインで明確化**することが求められる。	• **多要素認証の強化と、救急現場における迅速な情報共有とのバランス**をどのように整理するか • **物理的対策も含めた現場実態に即した柔軟な運用**（例：ホワイトボード的運用）をどこまでガイドラインで許容・明確化するか
4.安全なネットワーク接続と暗号化通信	• オープンなネットワーク（インターネット等）を利用する場合は、TLS1.3（または1.2以上）の高セキュリティ設定をデフォルト（初期設定）とし、部門システム等のサブシステムにおいても、不要な通信ポートの閉塞や相互認証機能が有効化された状態で納品すること。なお、これら設定にあたっては、インフラ専門のメンバーを参画させるとともに、変更不可の事項についてはあらかじめ医療機関に伝達し、不本意な設定変更が起きないよう留意すること。	• 対応が困難な事業者向けに、緩和策・柔軟な対応（リスクアセスメント等）も考慮できるとよい。 • ネットワーク分離やアクセス制御など、基本的な構成設計を行うだけでも被害拡大は大きく抑えられるため、**実践可能な最低限の構成・運用モデル**を明示すべきである。 • 「インターネットに接続していないから安全」という前提は誤りであり、**ネットワーク構成・リスク分析・ベンダーの情報提供などを前提とした設計・運用**を求めるべきである。	• 対応が困難な事業者も考慮しつつ、**最低限実施すべき構成・運用**（ネットワーク分離等）をどのように整理・提示するか • 「非接続＝安全」という前提を見直し、**リスク分析やネットワーク設計を前提とした対策**をどのように位置づけるか
5.保守・運用におけるデータの保護とアクセス管理	• リモートメンテナンスを行う際は、医療機関等の許可を得た上で行い、アクセスログを記録・保存すること。また、原則として個人情報を含むデータを医療機関外へ持ち出さない（コピーしない）運用を徹底すること。また、医療機関側が操作を許可・監視できる機能、または作業内容（操作ログや画面録画等）を事後的に医療機関側が容易に確認できるレポート機能を提供し、不正がないことを客観的に証明可能とすること。	• リモートメンテナンスには多様な形態があるためガイドラインの記載をより具体化しつつ、**過度な対策でコストが増えすぎないよう配慮**する必要がある。	• リモートメンテナンスの多様な形態を踏まえ、具体的な要件や留意点をどの程度まで明確化するか • **セキュリティ確保とコスト負担のバランス**をどのように取るか

有識者ヒアリングを踏まえた2省GLの今後の論点案（3/3）

- 有識者ヒアリング実施結果を踏まえ、２省GLの見直しにあたっては、中小事業者への負担軽減とセキュリティ確保のバランスといった論点を協議していくことが、実効性確保につながると考えられる

	改定に向けた方向性仮説	有識者ヒアリング結果	ヒアリング結果を踏まえた論点
6. 非常時における「縮退運用機能」と「緊急用アカウント」の実装	• ネットワーク遮断時でも、ローカル端末やスタンドアローン環境で最低限の診療記録・参照が可能となるローカル端末での参照・入力機能（縮退運用モード）を具備し、その切り替え及び復旧手順をマニュアル化して提供すること。SaaSにおいても同様の措置を講じること • 通常時の認証サーバーが利用できない場合に備え、「非常時用ユーザアカウント」によるログイン機能を実装し、かつ通常復帰後にその利用履歴を監査できる仕組みを提供すること	• サイバー攻撃時には証拠保全などでシステムを動かせない場合もあるため、最低限の診療情報を別のバックアップ手段で取得できる仕組みを用意しておく必要がある。 • 縮退運用やスタンドアロン対応は重要だが、オンプレ対応はコスト増に直結するため、対象データや要件は慎重に設計すべきである。また、救急指定病院など診療停止の影響が大きい施設では必須対応が必要だが、病院の規模・機能に応じて要件を切り分けるべきである。	• サイバー攻撃時を想定し、**診療継続に必要な最低限の情報を確保するバックアップ手段**をどのように整理・位置づけるか • 縮退運用・スタンドアロン対応について、**コストや医療機関の規模・機能を踏まえた要件の切り分け**をどのように行うか
7. 監査証跡（ログ）の保全性と分析支援機能の提供	• アクセスログや操作ログを、利用者（攻撃者）が容易に削除・改ざんできない領域（WORM機能を持つストレージやクラウド上の別領域等）へリアルタイムに転送・保存する機能や、インシデント発生時に医療機関等がログを抽出・提出しやすいツールやインターフェースを標準提供すること。この対応にあたっては、●年●月を目途として、反映を完成させること • 医療機関の担当者が異常を検知できるよう、ログの「分析・可視化ツール」または「アラート機能」を標準提供すること。	• ー（ご意見無し）	• ー
8. ソフトウェア・製品のライフサイクル（EOL/EOS）と脆弱性の能動的通知	• 提供するシステムを構成するOS、ミドルウェア、ライブラリのサポート終了期限（EOL/EOS）一覧を契約時および毎年度提示すること。 • 利用中のシステムに影響する脆弱性が発見された場合、医療機関が情報を取りに行くのではなく、事業者から「プッシュ型」で通知し、具体的な回避策やパッチ提供時期、適用計画を具体的に提示すること。なお、一義的には、用いられているPCにかかるOSのアップデートは医療機関の責において行い、その頻度に合わせてベンダもパッチ適用及び影響発生時の対処も含め十分な期間をとり、協調のもと対処することとし、外部のヘルスチェックシステム等も活用しながら対応を図ること。	• 運営コスト増大により特に中小事業者の負担が重くなる懸念があるため、通知頻度は固定化せず、合意ベースで柔軟に設定することが望ましい。	• 通知頻度について、運営コストや事業者規模を踏まえ、固定的な要件とせず柔軟に設定するかどうか • **中小事業者への負担軽減とセキュリティ確保のバランス**をどのように取るか

その他の実効性確保のための施策案

- 有識者ヒアリング実施結果を踏まえ、２省GLそのものの見直しではないが、実効性を高めるための施策としては、**モデル契約書・仕様書条文の別冊化・提供**といった施策が有効と考えられる

	有識者ヒアリングでいただいたご意見	有識者ヒアリング結果を踏まえた、実効性確保のための施策案
セキュリティ専門家A	• 実効性の担保としての施策について、いずれも良いと考える。 • 一方で、現実的にはそもそも2省GLをしっかり読んでいる事業者が少ないため、2省GLの実効性を高めるには、**まず事業者にガイドラインをきちんと読ませ、顧客側が準拠状況を確認する仕組みが重要**である。 • 現状は医療機関が**価格を優先することや事業者のメンテナンス等による責任の所在の曖昧さ、認定制度の利用の少なさ**などにより、ガイドラインの実効性が十分に確保されていない。	• 事業者にガイドラインを読ませるため、**事業者研修や動画コンテンツ整備**を行い、事業者が短時間で要点を把握できる仕組みを作る。事業者の準拠状況を顧客側が確認するために**MDS/SDSのチェックリスト、HISPROの適合性評価を活用**する。 • **小規模事業者であっても最低限守られるべき事項**を厚労省GL及び２省GLにおいて明確化し、当該項目の遵守状況を提示させ、かつ今後、**医療安全の文脈から、守れていない場合にペナルティとなるような仕組み・運用を検討**する。
情報セキュリティ事業者A	• 3省2GLにおける「最低限要求事項」と「推奨事項」の明確化（パッケージ化）について、**必須と推奨を整理して明確にする**のが望ましく、現状は対応水準が分かりづらく、過剰対応や未対応が生じている。 • 「医療機関向け 調達チェックリスト」の配布（翻訳ツールとしての活用）について、医療機関は多忙で、日常的なやり取りや逐一確認は現実的に負担が大きいため、**実効性を持たせる運用方法の工夫が必要**。また、**3省2GL全体でロゴマークが貰えると良い**。	• 3省2GLにおける「最低限要求事項」と「推奨事項」の明確化（パッケージ化）については、**必須事項と推奨事項を整理して明確化**したうえで、記載する。 • 「医療機関向け 調達チェックリスト」の配布については**①MDS/SDSのチェックリストを活用し事業者の説明責任を果たす**ことに加え、適切に運用されているかを**②HISPROの行う適合性評価**等により医療機関が確認・把握しやすい状況とし医療機関の負荷を下げつつも実効性を確保する。そのため、2省GLにおいて①MDS/SDSのチェックリストを用いた自己評価・医療機関への提示、②HISPROの「適合性評価済マーク」取得を求める形とする。
情報セキュリティ事業者B	• 特に**「モデル契約書・仕様書条文」の別冊化と提供が重要**と考える。医療機関・ベンダともにITや契約面の理解が十分でない中、実効性確保のためにはセキュリティ要件や契約の標準モデルを整備することが重要である。	• **モデル契約書・仕様書条文を別冊で提供**し、事業者がゼロから検討せずに活用できる形とする。

目次

本章のサマリ

- 昨今のランサムウェア等による医療機関への被害が深刻化していることに加え、医療情報システムは現在、経済安全保障上の基幹インフラ制度への追加検討が進んでいる。この情勢を受け、2省GLにおいても、サイバーインフラ事業者を対象として策定された「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」（以降、サイバーインフラGLと記載）との連携による強化が求められていることから、サイバーインフラGLの要素に関する2省GLへの連携について、検討を行った。
- サイバーインフラGLにおける要求事項のうち、2省GLにおいても強化が必要となる可能性のある全ての要素の洗い出しおよび対応方針の検討を実施した。その中でも、最も重要性が高く着目すべきと思われる項目は以下3点であった。

セキュア・バイ・デザイン

設計段階から一貫したセキュリティを確保することで、場当たり的なリスク対応による対策漏れやコスト増大を防ぎ、中長期的な安全性とコスト最適化を実現する

「セキュリティは運用で補う」という前提ではなく、メーカーやSIerによる設計・設定段階からのセキュリティ確保が実効性の鍵であり、重視すべきと考える

サプライチェーン

サプライチェーンにおける脆弱性や、脅威の侵入リスクが高まっており、サプライチェーンを含むセキュリティ要件の定義・合意が必要である

他方、中小規模事業者にとってはサプライチェーン対応の負担が大きいため、一律の義務ではなく、リスクや与える影響を踏まえて必要に応じて取り組める柔軟な設計の検討が必要である

脆弱性対応

ITインフラの脆弱性を狙ったサイバー攻撃被害の影響が高まっており、市場全体における速やかな強化が必要

「医療情報システムはインターネットに接続しない」という前提に立つことをやめ、メーカーはITインフラがアップデートされる前提で製品を開発・提供するとともに、SIerはアップデートを前提とした運用を講じる前提に変えていく必要がある

※ 2省GLとサイバーインフラGLは、その目的の違いから、対象とする範囲（医療情報システム全体か、ソフトウェア開発に限定するか）および記載粒度の差異があることに留意して対応した。

※ 来年度以降の改定作業に当たっては、医療機関の規模及び特性（例：特定機能病院・救急病院か否か等）に鑑み、求めるレベルを整理するとともに、事業者の負担を考慮の上、実効性を確保できる内容として詰めていく必要がある。

調査方針・実施内容

- 両GLの目的や対象、要求事項の粒度などの差異を考慮し、サイバーインフラGLの各要求事項を2省GLの粒度に整合させる方針で2省GLの改定方針、および改定案を作成

検討前提

- 医療情報システムが経済安全保障法上の基幹インフラ制度への追加検証対象とされるなど重要視される中、2省GLの実効性を確保し、事業者が医療情報を取り扱う情報システム・サービスを適切に提供できるようにすることがより一層求められることから、**サイバーインフラGL等のサイバーセキュリティに関する要求事項等を踏まえた2省GLの改定方針の検討が必要である**
- 2省GLの読み手である事業者がサイバーセキュリティに関する具体的な対応を実施する際は、原則としてサイバーインフラGLを参照・準拠することを想定しているが、サイバーインフラGLは**ソフトウェア開発事業者を対象とし、実装フェーズに重きを置いた詳細な記載**（細かい粒度）で構成される一方、2省GLは**医療情報システム全体に関わる様々な事業者を対象とし、リスクマネジメント等の上位レベルの指針**を中心していることから、相互に補完しあう関係である
- 加えて、サイバーインフラGLの内容を2省GLに連携することで、機微性の高い医療情報を取り扱う医療情報システム等の提供事業者にとっても、**昨今の情勢を考慮した具体的な取り組みがより理解しやすくなる面もある**

対応方針

- 2省GLとサイバーインフラGLは補完関係にあるため、2省GL本体の抜本的な書き換えは行わず、サイバーセキュリティ専門家の観点から、「**サイバーインフラGLの要求事項（21項目）のうち現行の2省GLに追記すべき要素はなにか**」という観点で洗い出しを実施する
- 2省GLに注釈や解説等を設け、サイバーインフラGLの該当記載の趣旨や適用範囲等を補足することで、 2省GLの対象事業者の理解を促進し、適切な対応を講じられる状態を目指す
- 不足している要素の追記にあたり、2省GLとサイバーインフラGLの粒度の違い、また、追記方法（全体方針としての追加／具体的な方法論としての追加／両方）および適用範囲（医療情報システム全体に適用／構成するソフトウェアのみに適用）を考慮して検討する
- 併せて、改定に際しての留意事項（事業者への負担、必要性、参照すべき文献など）を「留意点」として別途整理のうえ付記する

検討結果サマリ

- サイバーインフラGLの各要求事項について2省GLの粒度を考慮しつつ取り込むべき

サイバーインフラGLの概要

- セキュア・バイ・デザインおよびリスクベースの対策をベースとして、ソフトウェアのライフサイクル全体を通じた各プロセスにおいて、より実践的な作業イメージを提示している。
- 特に、継続的な状況把握やモニタリング、開発環境および開発側の責任と役割分担、加えて、昨今特に脅威が表面化し対策が強化されている脆弱性への取り組み、およびサードパーティやサプライチェーン等の自組織・自社製品以外の範囲についても言及がなされている。
- また、自組織外との連携の重要性についても記載されており、業界の縦横での連携や積極的な情報収集・発信等の取り組みの推奨、顧客側の経営層へも理解を求める活動等が示されている。

サイバーインフラGLの概要を踏まえた2省GLへの取り込み検討結果サマリ

- サイバーインフラGLで記載されている要求事項は、基本的に医療情報システムにおいても留意すべき点であった。しかし、2省GLとサイバーインフラGLでは、記載粒度が異なる点が多々あるため、その粒度を合わせながら、前頁の方針に則って対応方針として追記方針をまとめた。また、各要求事項の追記方針の検討に際し、特に留意すべき事項を「留意点」として整理した。
- 来年度における実際のGL改定に当たっては、サイバーインフラGLの各要素（詳細は次頁）について、以下の点について考慮しながら検討を進めるべきと考える。
  1．医療機関の規模および特性（例：特定機能病院・救急病院か否か）ごとに、要求レベルを整理することも検討すべき
  2．事業者の負担と必要性とのバランスを考慮して記載すべき
  3．サイバーインフラGL以外の参照すべき資料をいれるべき

サイバーセキュリティに関する整理　検討結果（1/5）

- 各要求事項について、追記方法・適用範囲を考慮し2省GLへの取り込み方針を検討

	サイバーインフラGL　要求事項				2省GLの取り込み方針（案）		
					2省GLの記載有無	追記方法	適用範囲
1	**セキュアな設計・開発・供給・運用** 脆弱性を抑え、セキュリティを備えたソフトウェアを開発・供給・運用する	1.1.	設計時のリスク評価と対策の追跡	➡	一部記載あり	C 全体方針・方法論 両方に記載	医療情報システム等全体
		1.2.	セキュアなビルド	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
		1.3.	テスト	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
		1.4.	サービスのモニタリング	➡	記載なし	A 全体方針に概要を記載	医療情報システム等全体
2	**ライフサイクル管理、透明性の確保** ソフトウェア管理の透明性をライフサイクル全体で確保しサプライチェーンを含むリスク管理を行う	2.1.	セキュアなコンポーネントの手配	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
		2.2.	リリースファイルやデータのセキュアなアーカイブ	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
		2.3.	関係者間のセキュリティ要件の確立	➡	一部記載あり	C 全体方針・方法論 両方に記載	医療情報システム等全体
		2.4.	利用者への適切な情報提供	➡	一部記載あり	B 方法論として記載	医療情報システム等全体
3	**残続する脆弱性の速やかな対処** リリースしたソフトウェアに残存する脆弱性を特定し、速やかに対応する	3.1.	継続的な脆弱性調査	➡	記載なし	B 方法論として記載	医療情報システム等全体
		3.2.	検知した脆弱性への対処	➡	記載なし	B 方法論として記載	医療情報システム等全体
		3.3.	対処結果を組織のプロセス改善に活用	➡	記載なし	B 方法論として記載	医療情報システム等全体
4	**人材・プロセス・技術の整備** 組織レベルでソフトウェアに関わる人材・プロセス・技術を整備する	4.1.	人材：経営層のコミットメントと人員の整備	➡	一部記載あり	A 全体方針に概要を記載	医療情報システム等全体
		4.2.	プロセス：開発ポリシーの確立と法令順守	➡	一部記載あり	C 全体方針・方法論 両方に記載	医療情報システム等全体
		4.3.	プロセス：運用ポリシーの確立と法令順守	➡	一部記載あり	C 全体方針・方法論 両方に記載	医療情報システム等全体
		4.4.	プロセス：開発・運用基準の策定	➡	記載なし	C 全体方針・方法論 両方に記載	医療情報システム等全体
		4.5.	技術：セキュアな開発ツールの整備	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
		4.6.	技術：セキュアな開発環境の整備	➡	記載なし	A 全体方針に概要を記載	ソフトウェア限定
5	**サイバーインフラ事業者・ステークホルダー間の関係強化** サイバーインフラ事業者・ステークホルダー間の情報連携・協力体制を強化する	5.1.	情報連携のための組織体制	➡	記載なし	A 全体方針に概要を記載	医療情報システム等全体
		5.2.	協力体制の強化	➡	記載なし	A 全体方針に概要を記載	医療情報システム等全体
6	**顧客によるリスク管理とセキュアなソフトウェアの調達・運用** 顧客経営層のリーダーシップによるリスク管理とセキュアなソフトウェア調達、運用を行う	6.1.	顧客経営層のリーダーシップによるリスク管理	➡	記載なし	B 方法論として記載	医療情報システム等全体
		6.2.	顧客経営層のリーダーシップによるソフトウェアの調達、運用	➡	一部記載あり	B 方法論として記載	医療情報システム等全体

サイバーセキュリティに関する整理　検討結果（2/5）

- 検討内容の一例として、「セキュア・バイ・デザイン」に関する内容を以下に示す

サイバーインフラGL要求事項		2省GLへの対応案			
項目	概要	差分	対応方針案	適用範囲	対応案
S(1)-1 設計時のリスク評価と対策の追跡	「セキュアバイデザイン」及び「セキュアバイデフォルト」の原則に則り、開発するソフトウェアのリスクを分析・評価し、リスク対応、セキュリティ要件、設計上の決定事項を追跡し、対策を維持する。	現行の2省GLではセキュアバイデザイン／セキュアバイデフォルトの原則に言及されていない	セキュアバイデザイン／セキュアバイデフォルトは、場当たり的なリスク対応による対策漏れやコスト増大を防ぎ、設計段階から一貫したセキュリティを確保することで、中長期的な安全性とコスト最適化を実現する考え方。 ソフトウェア開発に限らず、個人の生命・健康に直結する医療情報を扱う医療情報システム等は、その性質上、事後的なリスク対応では十分な安全性を確保することが難しく、設計段階から安全性を組み込むセキュアバイデザイン／セキュアバイデフォルトの考え方を前提とすることが合理的であると考える。	医療情報システム等全体	「3.2. 医療情報システム等のライフサイクルにおける義務と責任」の項目に、「医療情報システム等の開発においてもセキュアバイデザイン／セキュアバイデフォルトの原則に則した開発を行うことが重要である」等の主旨を「セキュアバイデザイン」もしくは「セキュリティバイデザイン」いずれかの用語を用いて追記する。 併せて、詳細はサイバーインフラGLの59頁を参照する旨を注釈などで記載する。 ※現在市場には「セキュアバイデザイン」と「セキュリティバイデザイン」の2つの言葉が存在しており、この2つはほぼ同意であるが、「セキュアバイデザイン」はソフトウェア開発にフォーカスして利用するケースがあるのに対して、「セキュリティバイデザイン」はより広範なシステム全体で用いられ、かつデジタル庁でも「セキュリティバイデザイン」を用いている。そのため、2省GLでは「セキュリティバイデザイン」の用語で盛り込むことがより適していると考えられる。

サイバーセキュリティに関する整理　検討結果（3/5）

- 検討内容の一例として、「サプライチェーン」に関する内容を以下に示す

サイバーインフラGL要求事項		2省GLへの対応案			
項目	概要	差分	対応方針案	適用範囲	対応案
S(2)-3 関係者間のセキュリティ要件の確立	関係者間で合意すべきセキュリティ要件を確立し、契約又は共有するポリシーに盛り込む。	2省GLではサイバーインフラGLが求めているセキュリティ要件について、対象事業者と医療機関間での「セキュリティ要件の定義」はなされていないことに加え、サードパーティとのセキュリティ要件の合意等についても言及されていない。	まず事業者と医療機関の間で、サイバーインフラGLの趣旨も踏まえた具体的なセキュリティ要件（サプライチェーンを対象に含む）を定義・合意することが必要である（セキュリティ要件の定義は、#1：S（1）-1設計時のリスク評価と対策の追跡にて明示）。 その上で、合意したセキュリティ要件をサプライチェーン全体でも対応できるよう、契約や共有するポリシーに盛り込む旨を追記する。これにより、医療機関との合意内容を具体的なセキュリティ要件としてサードパーティまで一貫適用できるものと考える。	医療情報システム等全体	「2.1. 本ガイドラインが対象とする医療情報と事業者」の項目に記載されている、「対象事業者は本ガイドラインに基づくリスクマネジメント及び医療情報安全管理ガイドライン等に基づいた制度上の要求事項への対応が求められ、医療機関等に提供する医療情報システム等に必要な資源や役務の提供に係るサプライチェーン全体について、本ガイドラインで記載するリスクマネジメント及び制度上の要求事項に対応すること。（8頁）」の文章に注釈を付し、併せて、詳細はサイバーインフラGLの71頁を参照する旨を注釈として追記する。 「リスクマネジメントの実践」の項目に記載されているリスクマネジメントにおいて、「契約や共有ポリシーで盛り込んだセキュリティ要件」に対応する旨を「リスク対応策の設計・評価（5.1.5.）」等で追記する。 併せて、詳細はサイバーインフラGLの71頁を参照する旨を注釈として追記する。

サイバーセキュリティに関する整理　検討結果（4/5）

- 検討内容の一例として、「脆弱性対応」に関する内容を以下に示す（1/2）

サイバーインフラGL要求事項		2省GLへの対応案			
項目	概要	差分	対応方針案	適用範囲	対応案
S(3)-1 継続的な脆弱性調査	ソフトウェアの脆弱性の開示と是正に関する方針を定め、その方針に必要な役割、責務、プロセスを定義し、実施する。	2省GLではリスク特定における「医療情報システム等提供上の代表的な脅威」として「技術的脆弱性の混入」を示しているものの、脆弱性に対する体制整備や脆弱性調査等の脆弱性に対する具体的な実施策については言及されていない。	サイバーインフラGLでは、開発したソフトウェアについて継続的に脆弱性の開示、修復、脆弱性情報の収集等を行えるよう、脆弱性対応体制や対応ポリシー、コミュニケーション計画を定めるよう求めている。また、その中にはインシデント対応プロセスの整備も含まれる。 医療情報システム等を提供する事業者においても、脆弱性に関する各種対応およびインシデント対応プロセスの整備とそのための体制設置は重要であるため、ソフトウェアに限った考えではなく、医療情報システム全体で必要な取組であり、サイバーインフラGLが示す考えを、適用範囲を広げて取り込んでいく必要があると考える。	医療情報システム等全体	脆弱性対策については、昨今重要な対応であることから、要求事項9～11の内容をまとめて「脆弱性の対応の重要性」として概念を書き込み、そこからサイバーインフラGLの各頁を参照する旨注釈として記載することが望ましいが、現状、2省GL側には脅威に対する取り組みが具体的に記載されている箇所がない状況である。 そのため、「5.1. リスクマネジメントの実践」の項目に記載されている「5.1.5. リスク対応策の設計・評価」において、「脆弱性対策における考慮事項」の項目を新設し、次頁に示す「追記する文章案」等の主旨の記載を追記する。

サイバーセキュリティに関する整理　検討結果（5/5）

- 検討内容の一例として、「脆弱性対応」に関する内容を以下に示す（2/2）

2省GLへの対応案（追記する文章案）

○脆弱性管理における考慮事項
医療情報システム等を構成するOS、ミドルウェア、アプリケーション、ネットワーク機器のファームウェア等について、公開されている脆弱性情報の継続的な収集と、当該脆弱性の有無および対応状況の管理を行い、特に攻撃成功可能性の高い脆弱性に対しては迅速に対応すること。

脆弱性対策では修正プログラム等の適用を原則としつつ、それらの対応が難しい場合は、特定の攻撃パターンに準拠したIDP/IPSによるブロック等の代替策の検討や、通信およびアクセス制御の強化等を組み合わせた低減策を検討すること。

また、攻撃発生時に医療業務への影響が大きいもの等のリスクが特に高い医療情報システム等については、脆弱性対策のための対応体制の構築に加え、情報資産と脆弱性情報等を自動的に収集し可視化する仕組み作りや監視の強化などについて、医療機関等の理解を得ながら協力して強化していくことが重要である。

具体的な対策については、各事業者の立場によって求められる取り組みが異なることも留意の上、IPA（独立行政法人情報処理推進機構）が公開している「脆弱性対策の効果的な進め方（実践編）」や、経済産業省および内閣官房が定める「サイバーインフラ事業者に求められる役割等に関するガイドライン」等を参照すること。

目次

本章のサマリ

- 本調査では、2 省 GL の対象事業者の定義のうち、**「患者等の指示に基づいて医療機関等から医療情報を受領する事業者」**（以下、**「第三類型」**という。）の位置づけおよび想定される事業者分類について、基本的指針の改定案等を踏まえて検討を実施。

- ２省GL策定までの変遷として、**総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下、「クラウド事業者GL」という。）**、および**経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（以下、「情報処理事業者GL」という。）**の2つのガイドラインの統合・見直しが行われた際に、対象事業者の定義について新たに第三類型が追加された。

- 有識者ヒアリング調査として、２省GLの改定に向けた有識者委員会のメンバーにヒアリングを実施し、第三類型の定義記述に至る経緯を伺った。基本的指針の対象である**PHRサービス提供者に加え、地域連携医療ネットワークを含む医療関連情報のデータ連携基盤を有する事業者についても、第三類型の対象に含まれる**との回答を得た。

2省GL策定までの変遷

- 2省GL策定の際、総務省・経済産業省の各GLの見直し・統合に伴い、2省GLの対象事業者の定義に第三類型が追加された

#	ガイドライン名	担当省庁	詳細
1	クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン（クラウド事業者GL）	総務省	• 以下2つのガイドラインを統合し、2018年7月に策定。 - ASP・SaaSにおける情報セキュリティ対策ガイドライン（ASP・SaaSセキュリティGL）（2008年1月） - ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（ASP・SaaS事業者GL）（2009年7月） • ガイドライン対象をASP・SaaS 事業者だけではなく PaaS や IaaS 等も含め、**クラウドサービス事業者**を対象として定義。
2	医療情報を受託管理する情報処理事業者における安全管理ガイドライン（情報処理事業者GL）	経済産業省	• 医療情報を受託管理する**情報処理事業者**を対象として定義。 • 2008年7月の第1版策定後、厚労GLおよびASP・SaaS事業者GL等と整合性を取る形で2012年10月に第2版策定。

1. クラウド事業者GL <総務省>
2. 情報処理事業者GL <経済産業省>

見直し＆統合

2省GL（2020年8月 第1.0版策定）

[対象事業者の定義]
① 医療機関等との契約等に基づいて医療情報システム等を提供する事業者
② 医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者
③ **患者等の指示に基づいて医療機関等から医療情報を受領する事業者**

対象事業者に関する有識者ヒアリング結果

- 2省GL改定班のメンバーに有識者ヒアリングを実施。第三類型の対象にはPHRサービス提供者、地域連携医療ネットワークの管理事業者も含まれるとの回答を得た

有識者ヒアリング先	2 省GLの改定に向けた有識者委員会メンバー
有識者ヒアリング回答内容	• **第三類型として想定される典型的な対象はPHRサービス提供者**。患者からPHRサービス提供者に対して直接PHRデータを提供するのであれば、患者の自由であるため医療機関の責任は介在しえない。一方で患者から情報を受け取れない、医療機関から情報を送ってほしいケースでは医療機関側に責任が発生するために、第三類型として定義した。 • **ガイドライン策定時には医療情報のデジタルデータを医療機関から外部事業者に渡すことは考えにくかった**が、マイナポAPI・オンライン資格確認等の仕組みが出てきた。医療機関から政府には送るが民間事業者にはデータを渡せないとなるのは問題であり、民間事業者へのデータ提供も考慮に入れる必要が出た。万が一トラブルが起きた場合には患者としては医療機関を訴えることになるため、**医療機関は信頼できるPHRサービス提供者を選定する必要**がある。 • 以上のことから、**地域連携医療ネットワークを含む医療関連情報のデータ連携基盤**を有する事業者についても、PHRサービス提供者と同様に**2省GLの対象に含まれる**。

2省GLの対象として想定される事業者分類

- 2省GL及び基本的指針（改定版）の定義を元に、想定される対象事業者を整理

	定義	想定される対象事業者	概要	プロダクト例
2省GL	患者等の指示に基づいて医療機関等から医療情報を受領する事業者	**PHRサービス提供者**	利用者の健康管理のために医療データ（健診結果、診療履歴、投薬履歴など）を電子的に管理し、利用者に提供する仕組みを持つサービスを持つ事業者	• エムティーアイ 「CARADA」 ※1 • オムロンヘルスケア 「OMRON connect」 ※2 等
重複概念	（想定される対象事業者） 医療機関等から患者の指示に基づき医療機関等から医療情報を受領し、利用者に対して直接的もしくは間接的に健診等情報を取り扱うPHRサービス提供者（及びその工程に介在する事業者）			
基本的指針(改定版)	利用者に対して、直接的もしくは間接的に健診等情報を取り扱う PHR サービスを提供する者（PHR サービス提供者）	医療データ連携基盤を提供するIT企業	PHRサービス提供者に医療情報に該当するデータ提供を行う、**地域医療連携ネットワーク**を含む医療関連情報のデータ連携基盤を有する事業者	• TIS「ヘルスケアパスポート」 ※3 • 富士通「Healthcare Personal service Platform」 ※4 等

出典
※1：https://www.mti.co.jp/?page_id=22472
※2：https://www.healthcare.omron.co.jp/smp_omronconnect/
※3：https://www.tis.jp/service_solution/healthcare-passport/
※4：https://global.fujitsu/ja-jp/offering/healthcare-dx-for-patient-experience、および https://docs.fujitsu/documents/3-001173/healthcare-personal-service-platform-brochure-ja.pdf

目次

４．まとめ

今後の２省GLの改定に向けて

- 各調査を踏まえた2省GLへの対応事項について、論点全体として議論しなければならない観点は大きく４つに収斂され、これら観点で専門家、関係省庁含めた議論が必要

1 **システムのライフサイクルを通じたセキュリティ技術・機能要件の強化（技術・機能面）**	セキュリティを後付けの「運用」でカバーするのではなく、システムの設計から開発、運用、非常時対応に至るまで「標準装備（セキュア・バイ・デフォルト/デザイン）」とするための要素	セキュアな設計・開発基盤	セキュア・バイ・デザインへの準拠、セキュアなビルドとテスト環境、開発ツールの保護など、上流工程からの脆弱性排除
		強靭性（レジリエンス）の標準実装	ランサムウェア対応型の復元可能バックアップ、非常時の縮退運用機能と緊急用アカウント、高セキュリティ設定（TLS1.3等）、多要素認証のデフォルト化
		セキュアな運用と能動的保守	稼働中のシステムのモニタリング、継続的な脆弱性の調査・修正と医療機関へのプッシュ型通知、リモート保守時のログの厳格な保全と分析支援
2 **サプライチェーン全体を含むガバナンスと責任分界の明確化（体制・契約・ガバナンス面）**	クラウド化や多重下請け構造を背景に、単一事業者と医療機関の枠を超えた「サプライチェーン全体」の責任と役割分担を定義し、契約レベルで合意するための要素	サプライチェーン全体の統制	サードパーティ製ソフトウェアのセキュアな手配、適切な委託先選定の厳格化、サプライチェーン全体を通じたセキュリティ要件の確立と適用
		契約・SLAを通じた責任分界の明文化	事業者が異なる場合の合意形成、契約書やSLAでのサービス類型別の「責任分界点マップ」の標準化、リスクコミュニケーションによる契約前の合意の義務化
		組織体制とリーダーシップの確立	経営層のコミットメントと要員のトレーニング、開発・運用ポリシーの設定、顧客（病院等）経営層の主体的なリスク管理の促進、外部組織との連携体制
3 **医療機関への透明性確保と説明責任の代行（コミュニケーション・情報開示面）**	IT専門人材が不足する医療機関に対し、事業者が自社システムのリスクや対応状況をわかりやすく開示・翻訳し、医療機関側の安全管理義務の遂行を支援するための要素	情報開示の具体化と標準化	ランサムウェアやサプライチェーン管理体制を追加した「サービス仕様適合開示書」改定、リスクマネジメント対応資料具体化、EOS/EOLや廃棄時ガイダンス提供
		安全管理水準と第三者認証の明確化	プライバシーマーク等第三者認証取得が望ましい理由の明記、ガイドラインが求める安全管理水準の具体的な参照先の提示
		事故・インシデント・法令サポート	情報セキュリティ事故発生時の個人情報漏えい対応の明示、海外サーバ等へのデータ転送時の国内法適用（情報種別ごとの取扱い）の整理
4 **ガイドラインの実効性を担保する制度的・市場的支援（市場・制度・エコシステム面）**	2省GLを「努力目標」から「市場のインフラ（標準ルール）」へと引き上げ、中小規模を含む事業者や医療機関が持続的に対応できるようにするための支援策や枠組みに関する要素	要求事項の明確な層別化	対応水準の曖昧さを排除するための「最低限要求事項（必須）」と「推奨事項」の層別化、対象となるクラウドサービスや保守契約の定義の拡張・明確化
		遵守圧力を高めるツール・認定の提供	調達要件に活用できる「2省GL適合宣言マーク」の創設、医療機関がそのまま使える「調達チェックリスト」、中小規模事業者向け「セキュリティ実装ガイド」提供
		持続可能性を支える支援体制	セキュリティ強化に伴う財政的支援（補助金や診療報酬上の手当）、事業者認定と連動した実務者研修、広域のセキュリティチェック体制や国の標準仕様の策定検討