NTT DATA
Trusted Global Innovator

令和４年度ヘルスケアサービス社会実装事業（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等に関する調査）報告書

2023年３月24日

株式会社ＮＴＴデータ経営研究所

目 次

背景と目的

背景と目的

本調査の背景

- 経済産業省・総務省においては、事業者向けの「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（令和２年８月）」（以下、「2省GL」という。）を策定・公表している。
- 医療情報システムに関する安全管理については、厚生労働省において医療機関等向けの「医療情報システムの安全管理に関するガイドライン（5.2版は令和４年３月）」（以下、「厚生労働省GL」という。）を策定・改定しており、現在も第6.0版に向けて改定作業を行っている（なお、これらのガイドラインを「3省2GL」という。）　。
- こうしたガイドラインの改定等の背景には、近年のサイバー攻撃の多様化・巧妙化や、クラウドサービスの普及などに対する技術的な対応の必要性などがある。特にサイバー攻撃については、その手法の巧妙化や、攻撃による被害の重大性（例えば診療行為の停止）などが現実的なものとなっている。
- このよう状況を踏まえ、3省2GLにおいても対応の必要性が高まっている。厚生労働省GLにおいては、昨年、一昨年と改版を進めたほか、現在も改定の必要性が高まっている。そこで、2省GLにおいても、同様の改定の要否及びその内容に関する検討が求められている。特に医療機関等と情報システム・サービス事業者との責任分界のあり方や、リスクコミュニケーションのあり方については、サイバー攻撃による被害への防止策と、発生した場合の対応措置との関係で、極めて重要であることが、医療機関等において実際に生じた攻撃でも明らかになっていることから、2省GLにおいてもこの観点での対応が不可欠と考えられる。
- 他にも、医療情報の連携方法の多様化により、病院における電子カルテシステムやAI医療機器が外部と情報通信するケースが増えてきており、事業者が事業展開する上で3省2GLによりサービスの設計が過度に制限されている等といった事実がないか、あるいは必要な対応策としてのあり方はどうか、等の検証も求められている。
- さらに2省GLについては、情報システム・サービスの多様化や、医療情報の周辺領域におけるDXの拡大等に伴い、ガイドラインの適用範囲が的確に認知されないことによる課題なども生じている。そのため、事業者の利便性を向上させる資料の作成等により、医療情報システムの安全性を確保する環境整備を進めることが期待される。
- 本調査においては、このような観点から、3省2GLの課題整理と、2省GLの改定・普及に必要な作業等を行うことを目的とする。

背景と目的

本調査の目的

3省2GL

- **3省2GLの共通の課題等とその現状、特に情報システム・サービス事業者における現状**などの把握を行う。
- **医療情報システムを取り巻く**環境の変化、例えばサイバー攻撃の巧妙化や、医療情報システムに用いられるシステム・サービスの多様化への対応を踏まえた**課題を整理**して、ガイドラインとしてあるべき対応について検討を、**各種文献、国内外の制度動向などを踏まえて行う**。
- 医療情報システムを取り巻く課題に関しては、**有識者における意見や助言**のほか、**情報システム・サービス事業者における現状の対応状況や、対応上の課題等を整理**して、**実効性のあるGLの改定検討の資料**とする。

2省GL

- 2省GLの改定に係る**意見公募（パブリックコメント）対応支援**、あるいは**情報システム・サービス事業者からの問い合わせ対応支援**を行うほか、事業者が**ガイドラインを確認し、あるいは準拠するのに資する資料の作成**等を行う。
- また情報システム・サービス事業者における2省GLの対応のうち、**外部保存通知に対する対応状況などを確認するための調査**を実施する。特に**医療情報の保存場所などに関する実態などを把握**するための調査を実施する。

１．３省２ＧＬに関する課題等調査･改定案の提案

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査

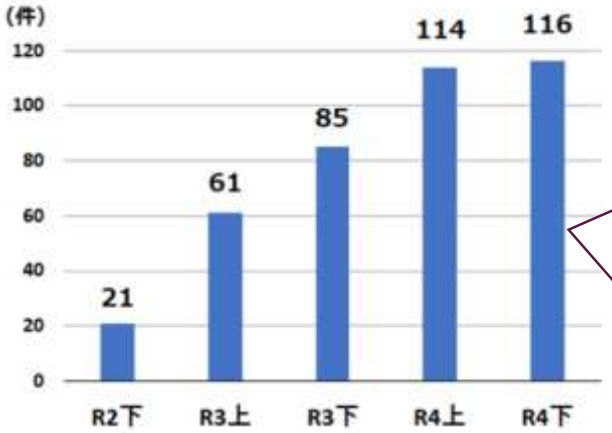
■　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況に関し、特に現状のサイバー攻撃の状況を整理するとともに、医療情報を取り扱うための事業者の選定に関する状況について整理を行った。

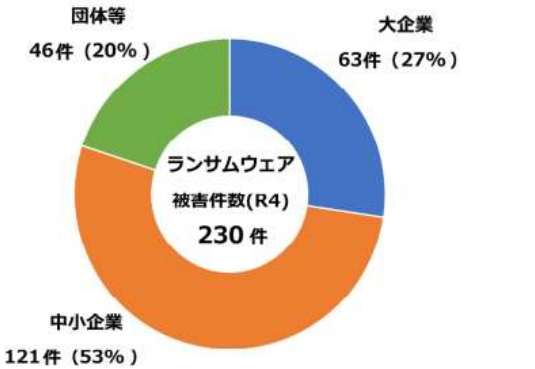
１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査

①医療情報システムを取り巻く脅威の増加～サイバー攻撃の増加と巧妙化

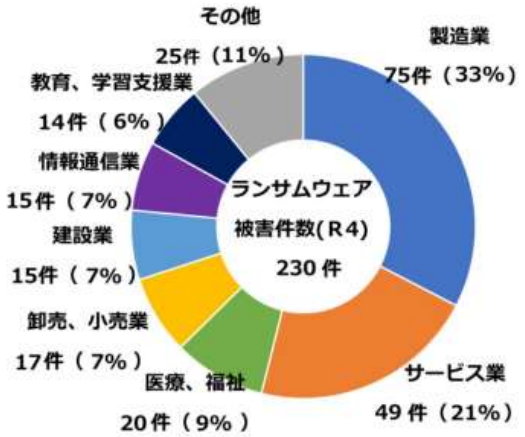
- サイバー攻撃のうち、特に被害が顕著であるランサムウェアの被害状況を以下に示す。
- わが国におけるランサムウェアの被害が拡大する中で、中小企業などでの被害も多い。
- また医療福祉分野での被害は全産業における被害件数の９％。また情報通信業の被害は７％となっている。

2022年のランサムウェアの被害の推移





ランサムウェアの被害が発生しているのは中小企業が半数



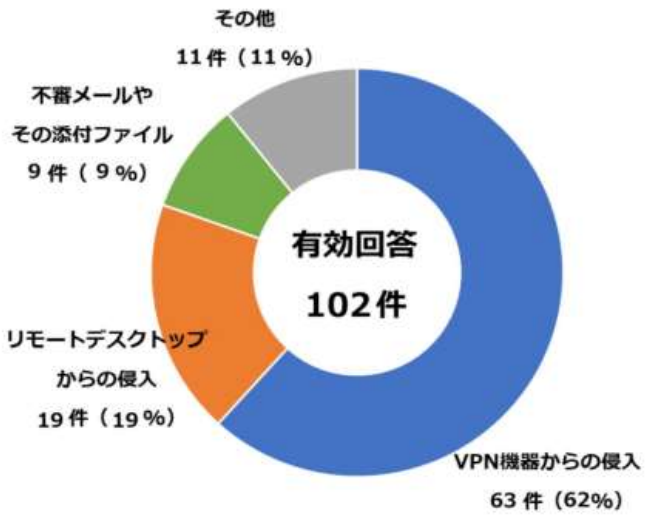
医療・福祉分野での被害は約1割
情報通信業の被害も約1割

出所：「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁、令和５年３月16日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

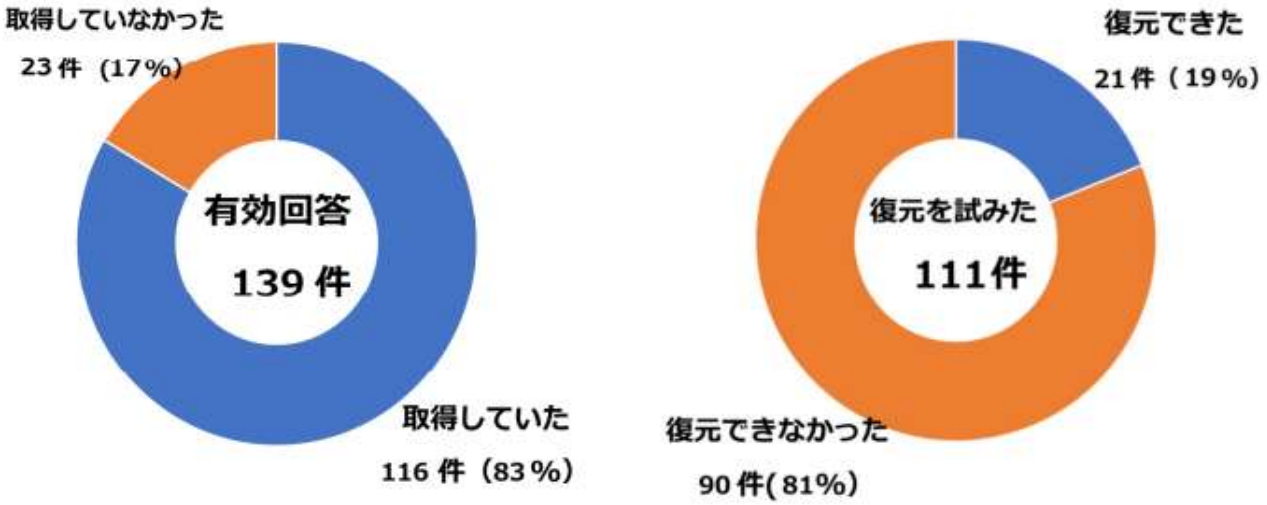
１－１　国内におけるサイバー攻撃の多様化･巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
①医療情報システムを取り巻く脅威の増加～サイバー攻撃の増加と巧妙化

- ■ ランサムウェアの感染経路は、VPN機器やリモートデスクトップなどからの侵入が多く、エンドユーザが気付きにくい経路からの感染が多い
- ■ バックアップについては、すべて利用可能であるとした回答は約2割にとどまる。

感染経路



バックアップの取得状況とその復元結果



出所：「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁、令和５年３月16日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

- ■ ①に示す医療機関等に対するサイバー攻撃により、地域医療の継続を含めて大きな被害が生じた例として、半田病院におけるランサムウェア被害の事案を整理する。
- ■ 本事案においては、いくつかの課題等が報告書（以下「半田病院報告書」）※１において指摘されたところであるが、特に医療情報等システム提供事業者における対応の課題と、医療機関等との合意等に関する課題が指摘された。以下では報告書で示された課題等の整理を示す。

※１ 「徳島県つるぎ町立半田病院　コンピュータウイルス感染事案有識者会議調査報告書について」
https://www.handa-hospital.jp/topics/2022/0616/index.html

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

■ 半田病院報告書では、事案の経緯等を整理したうえで、外部委託を行う上で課題となる事項について、事実関係等を示している。以下その内容を整理する。

課題のカテゴリー		半田病院報告書において示される内容（引用）
責任分界上の課題	医療機関等と事業者間の責任分界等の認識	• （安全管理）ガイドラインに基づけば「通常運用における責任」および「事後責任」を果たす当事者は半田病院だけである。しかし、前述の情報システム管理リソース欠如の状況において、事業者及びベンダーはこの「丸投げ状態の理由」を十分認識していると思われ、事業者及びベンダーは医療情報を扱う当事者でなくとも、システム全体の構成要素の内容を含めたリスクマネジメント実施の提案、または知見が不足するのであれば、第三者への委託を含めそれらを促すなどの善管注意義務は十分にあったと考える（4.1.6 事業者及びベンダーの善管注意義務）
	機器等の管理に関する責任分界	• C 社は、電子カルテシステムのリモートメンテナンス業務の主体であるにもかかわらず、インフラ担当がA 社であることを理由にリモートメンテナンスに利用する VPN 装置の設定仕様書及び通信キャリア、サービスプロバイダー名、経路上の暗号化等の仕様について把握していない。（3.4.5.3 電子カルテシステムのリモートメンテナンス）
	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	• C 社は、アプリケーションの担当が自社、ハードウェア・OS 等のインフラの提供および設定は A 社が担当であるとしている。一方、A 社は(医療情報システムの)全体統括は C 社であり電子カルテシステム(システム全体の意味)の構築は C 社が担当であるとしていることから、この時点で双方に齟齬が見られる。 この齟齬があるにも関わらず、実際には構築時のハードウェア・OS 等のインフラの提供および設定は C 社の指示に従って A 社が作業を実施したとみられ、これらの責任は C 社にあると認識しながら A 社による構築が進められたと見られる。（3.4.5.1 電子カルテシステムに関する双方の意識）
	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	• 本脆弱性は Fortinet 社が 2019 年から 2021 年 6 月までに「4 度にわたり注意喚起を行ってきた」としているが、利用者自身が本情報を収集できずに認知できていなかった体制にも課題があるにせよ、本脆弱性の説明が利用者に行き届いていないことや、本情報を導入や保守を行っている A 社から利用者へ説明が行われていない。（3.4.3.1 初期侵入）

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

課題のカテゴリー		半田病院報告書において示される内容（引用）
初期対応上の課題	初動に関する全体的な対応計画	• システムを導入しているＡ社や、インシデント調査や復旧を行ったＢ社が実施すべきではあるが、調査は基本的にファストフォレンジックツールなどのツールを使用するのみであって、関連する詳細調査が行われていない。（3.4.2 調査方法）
		• 半田病院としてはエンジニア派遣を要望したにもかかわらず、要望に応じなかったこと。侵入経路や被害範囲を想定しながら保全に努めていないこと。輸送によるハードウェアの損傷などが生じる可能性に丁寧な指示がないこと、また当該環境でなければシステムの動作などが正常に行われないなどの可能性があるにもかかわらず、対象端末を院外に持ち出して調査を行っている。（3.4.3.2 内部侵入（概要））
		• 一部の端末やサーバーはＢ社に送付し、フォレンジックの作業が行われているようだが、Ｂ社提出の調査報告書の内容が希薄なため、その全容を解明することはできなかった。（3.4.2 調査方法）
サービス提供上の課題	情報セキュリティにおける脅威対応への知見	• Ｃ社とＡ社双方ともに、脆弱性情報(CVE-2018-13379)の存在は認識があったとしている。Ｃ社は電子カルテシステムのアプリケーションが担当であり範疇外の意識、Ａ社は VPN 装置の担当であるが、ISO27001に準ずる社内運用ルールに基づき管理運営していたとあり、脆弱性情報に関するセキュリティ知識が全く無かったと言わざるを得ない。（3.4.5.4 VPN 装置の脆弱性）
		• 情報システムを取り巻く環境の変化やそれにともなう新たな事業継続リスクに関する情報を組織として入手する仕組みがなかった。（4.1.2 マネジメントシステム）

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

課題のカテゴリー		半田病院報告書において示される内容（引用）
サービス提供上の課題	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	• 電子カルテシステム、医事会計システムの稼働を優先し、脆弱性管理とウイルス対策を実施していなかった。（4.2.2 脆弱性管理の課題）
		• サポート切れの OS を使用していたことは望ましくない一方で、電子カルテを始めとしたシステムを支障なく動かすためには、継続し続けるしかなかった現実もあった。（3.4.3.3 内部侵入（詳細））
		• 半田病院としてはウイルス対策ソフトを導入していたが、電子カルテシステムの導入時に不具合が生じたため、同セキュリティ対策ソフトは動作させていなかった。リモートメンテナンスを許可している環境であれば、導入時にウイルス対策ソフトを動作させる詳細なセキュリティ検証が必要であり、さらには定常的にパターンファイルの更新が行える環境の検討が必要であったと考える。しかし、これは半田病院に限らず、未だに続く閉域網の安全神話、閉域網によるセキュリティ対策の思考停止と言えるであろう。（3.4.3.3 内部侵入（詳細））
設計上の課題	厚生労働省GLに示す安全対策への未対応及び代替策	• 運用に関する委託契約もないことから事業者の監督もない。定期的に見直し必要に応じて改善を行う責任については、サイバー攻撃リスクに関する新しい情報は入手していないため、改善業務はほぼ医療情報システムの利便性に注がれている状況にある。基本的な安全管理の最低限のガイドラインの実施(Webによる、個人情報保護に関する方針の策定・公開、文書による、医療情報システムの安全管理に関する方針の策定)は確認できるが、ISMS の実践を促されているものの、実施はされていない。（4.1.3 厚生労働省のガイドライン）
		【以下は引用ではなく記載内容からのまとめ】 • 「4.2 技術的な課題」において、いくつか厚生労働省GLにおける「C　最低限のガイドライン」に対応していない事項が報告されている。（パスワードルール、脆弱性対策、https対応、媒体管理等）（4.2 技術的な課題）

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

■ 半田病院報告書を踏まえて、外部委託等に関連する課題を以下のように整理した。

【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
- 機器等の管理に関する責任分界が不明瞭
- 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

【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）

【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ができていなかった。
- 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）

【設計上の課題】
- 厚生労働省GLに示す安全対策への未対応及び代替策に対する対応不足（リスクコミュニケーション不足）

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
②半田病院におけるセキュリティ対応上の課題

【3省２GLに関する課題の指摘】

- 半田病院における報告書では、直接2省GLに対する指摘はない。ただし厚生労働省GLについては、以下の指摘がなされている。
  - 対策の具体的内容が示されていない（特にネットワークに関して）。
  - 厚生労働省GLでは、医療情報システム等提供事業者については、管理業務契約がなければ善管注意義務等の対象外となることとなっているが、事業者責任として情報提供義務等があると考えるのが妥当
- また3省2GLを統合し、より具体的な有効な対策を含めた形とすべきという指摘を行っている。

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
③第三者認証の制度概要

■　昨今のサイバー攻撃等を鑑みた場合、医療情報システム等提供事業者の選定が重要となる。3省２GLでは、現在ISMSまたはプライバシーマークの取得を求めているが、より選択の幅を広げる観点から類似する第三者認証の状況を整理した。

制度名	対象	認証団体（付与機関・審査機関等）	目的	証明内容
JIS Q 15001:2017	組織認証	（付与機関） 一般財団法人日本情報経済社会推進協会（JIPDEC）	以下の目的でプライバシーマークの使用を認める ・消費者の目に見えるプライバシーマークで示すことによって、個人情報の保護に関する消費者の意識の向上を図ること ・適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること	【個人情報保護法に基づく適切な個人情報の取り扱いの実施管理に関して認証】 ・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事業者等を評価し、その審査結果が適切であった者に対してプライバシーマークを付与
JIS Q 27001（ISO/IEC 27001）	組織の一部の認証（組織の必要に応じて設定・サービス提供組織のみを含む）	（認定機関） 一般社団法人情報マネジメントシステム認定センター	・組織等が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提供することを目的とする	【情報システムにおける適切な管理体制の構築とその運用について認証】 以下の実現を図るのに必要な要求事項への実施状況を審査し、認証する。 ・ISMSの確立・実施・維持・継続的な改善 ・情報セキュリティのリスクアセスメントおよびリスク対応
ISO/IEC 27017	サービス等	（認定機関） 一般社団法人情報マネジメントシステム認定センター	・クラウドサービスに関するリスクの低減、クラウドサービスを適切に提供/利用する組織体制の確立、認証取得による、組織内外からの信頼向上を目的とする	【クラウドサービスにおける固有の情報システムにおける適切な管理体制の構築とその運用について認証】 ・クラウドサービスについて、ISO/IEC 27001に加えて、クラウドサービス固有の管理策が実施されていることを認証

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
③第三者認証の制度概要

制度名	対象	認証団体（付与機関・審査機関等）	目的	証明内容
SOC (Service Organization Control) 2・3	組織（監査）	AICPA　米国公認会計士協会※1 日本公認会計士協会※2	・外部のサービスを利用する事業者が、自社の内部統制監査対応する際に、自社のIT利用における監査部分を、外部サービス事業者が提供する監査報告書等（SOC２、SOC３）を提出することで、利用者が該当する部分の監査に用いる。 SOC2：サービスに係る評価要素（「証明内容参照」）について保証されていることを監査し、報告書（サービス利用者に対して個別開示） SOC３：SOC２の評価要素と同様であるが、不特定多数への開示が可能であり、）シール等制度により運用	【クラウドサービスにおけるセキュリティ等に関する対応状況を監査し、その適合性を示す。】 サービス利用者の情報を処理するために使用するシステムの評価要素についての対応状況を監査し、適合性を判断する。 ➢ セキュリティ ➢ 可用性 ➢ 処理の完全性 ➢ 情報の機密性 ➢ プライバシー、不特定の者に対して公開する。
CSマーク	サービス等	クラウドセキュリティ推進協議会（JASA）	・公正かつ公平な情報セキュリティ監査がクラウドコンピューティングサービスにおいて実施され、クラウドコンピューティングサービスにとって有益なものとして情報セキュリティ監査が機能し、もって公益の増進に寄与するために、品質が保たれた情報セキュリティ監査を実施したクラウドコンピューティングサービスを標章する制度（クラウド情報セキュリティ監査制度）	【クラウドサービスにおけるセキュリティ等に関する対応状況について実施した監査状況に対して、その適正性（適合監査であること）を示す。】 ・事業者が基本的な要件を満たす情報セキュリティ対策を実施し、事業者がそのとおりに実施しているかを標準的な基準に基づきあらかじめ定められた要件を満たす監査で評価し、安全性が確保されていることを顧客に公開し、証明するもの

※１　SOC2、SOC３いずれも米国公認会計士協会 “Attestation Standards (Clarified) 105, 205” による。
※２　SOC2については、日本公認会計士協会「保証業務実務指針3852『受託業務のセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る内部統制の保証報告書に関する実務指針』」による。
SOC３については、日本公認会計士協会 IT委員会報告第2号「Trustサービスに係る実務指針（中間報告）」による。

１－１　国内におけるサイバー攻撃の多様化・巧妙化や、情報技術の進展、医療情報の連携方法の多様化の状況について文献調査
③第三者認証の制度概要

制度名	対象	認証団体（付与機関・審査機関等）	目的	証明内容
医療情報ASP・SaaS情報開示認定制度	サービス等	ASPIC　一般社団法人日本クラウド産業協会	・クラウドサービス情報開示指針（総務省）に基づき、医療情報ASP・SaaSサービスの活用を考えている企業や地方公共団体などが、事業者やサービスを比較、評価、選択する際に必要な安全・信頼性に係る情報を適切に開示し、かつ一定の要件を満たす医療情報ASP・SaaSサービスを認定するもの	【クラウドサービスにおけるセキュリティに関する情報内容が、適切に開示されていることを示す。】 ・医療情報ASP・SaaSサービスの安全・信頼性に係る情報開示が豊富になるとともに、開示項目が共通化されることで、ユーザーがサービス及び事業者の比較・評価・選択が容易になる ・安全・信頼性に必要な情報開示への需要が高まり、認定を受けたサービスを提供する事業者は、さらにユーザ獲得の機会の拡大 ・医療情報ASP・SaaSサービスが社会経済活動の多くの分野で普及、定着し、情報通信システムの効率的な利用、企業の生産性向上、経済成長につなげる
HISPRO適合証明	組織の一部の認証（組織の必要に応じて設定）	ＨＩＳＰＲＯ　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の専門の知識を持った評価員によって評価を受けることで、事業者が提供しているITサービスが3省２GLのどの部分に該当するか明確化し、ユーザーが安心した IT サービスの選択、利用を可能にする制度	【3省２GLへの対応状況について、その適合性を示す。】 ・サービス提供事業者による各種製品・サービスの紹介・説明にマークが付けられたものは、HISPROにより該当する医療情報関連ガイドライン（厚生労働省、総務省・経済産業省発行）への適合性が評価済であることを証明するもの

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

【本項における調査の目的】

- 3省２GLの課題を整理するに際して、諸外国における医療情報の取り扱いに関するガイドラインの状況を整理した。その結果から得られる示唆を整理し、今後の我が国における医療情報に関連するガイドラインに求められる要素を抽出した。
- 本項では、特に欧米などで同種の課題を踏まえて対応するガイドライン等を策定する国のうち、特に示唆が含まれている国のものを整理した（そのうち、近時のガイドラインを中心に整理した）。
- また昨今のサイバー攻撃への対応という観点からの示唆を整理するため、特に医療情報システムに対するサイバー攻撃への対応を示すガイドラインを中心に整理を行った。

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

調査対象資料（HHS等（米国））

文書名	作成時期	概要
FDA資料 “Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook”	15 Nov.2022	◆FDAがMITRE Corporationと協力し、医療機関がサイバーセキュリティインシデントに備えるのに役立つリソースとして更新したプレイブック。医療機器の機能に影響を与える医療機器のサイバーセキュリティの問題に対する準備と対応に焦点を当てる。
NIST “NIST Cybersecurity Framework (CSF)”	Apr.2018	◆医療機器に限るものではないが、サイバーセキュリティのフレームワークとして2018年4月に公開されているもの。現在CSF 2.0を作成中。
“MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN” The Joint Cybersecurity Working Group of the Healthcare and Public Sector Coordinating Council	Jan.2019	◆米国保健福祉省との官民パートナーシップであるThe Joint Cybersecurity Working Group of the Healthcare and Public Sector Coordinating Councilが2019年1月に作成した医療機器サイバーセキュリティためのベストプラクティス集

調査対象資料（カナダ）

文書名	作成時期	概要
FDCyber security for connected medical devices (ITSAP.00.132)	5 Nov.2021	◆ネットワークに接続する医療機器のベンダー、クラウドサービス事業者向けに、サイバー攻撃から医療機器をより適切に保護するために実装できる対策を推奨事項として示す。

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

医療情報セキュリティ関連（NHS（英国））

文書名	作成時期	概要
Guidance on protecting connected medical devices （コネクテッド医療機器の保護に関するガイダンス ）	3 October 2022	◆臨床ネットワーク（インターネット）に接続する医療機器等におけるセキュリティ対応のためのガイダンス ◆臨床ネットワークに接続する医療機器等の特徴を踏まえた課題を整理して、その課題への対応を整理する。 ◆具体的な対応としては以下のステップに分けて整理する。 ➢ ステップ 1. 接続された医療機器を特定する（ガイドラインが対象とする医療機器の定義や種類の例示を示す） ➢ ステップ 2. 緩和計画を作成する（信頼できないコンテンツへのアクセス制限と、脆弱性を含む機器からの接続を制限することによる計画の必要性を示す） ➢ ステップ 3. 緩和策を適用して侵害の可能性を減らす（信頼できないコンテンツへのアクセス制限の対策例を示す） ➢ ステップ 4. 緩和策を適用して侵害の影響を軽減する（脆弱性を含む機器からの接続を制限するための対策例を示す） ➢ ステップ 5. サードパーティ接続を理解する（外部の第三者組織からの接続への対応を示す） ➢ ステップ 6. 資産を定期的に確認する（機器に関する資産管理対応を示す） ➢ ステップ 7. 廃止/交換計画を立てる（機器の更新等の計画策定について示す）
Cyber security guidance for procuring and deploying Connected Medical Devices （コネクテッド医療機器の調達と展開に関するサイバーセキュリティガイダンス）	13 September 2021	◆英国の医療事業者に対して、コネクテッド医療機器（CMDs）の調達と展開に関するサイバーセキュリティガイダンスを提供するもの ◆このガイダンスでは、CMDは、接続されたネットワーク機能のある医療機器を定義。この定義では、接続を行う技術手段は問わない。基本的に正式な医療目的で人間に使用される物理的な機器またはソフトウェアを対象とする。 ◆主にCMDsの調達プロセスの一環としてのサイバーセキュリティとCMDsの展開、維持、および廃棄におけるサイバーセキュリティに関する対策を示す。
Guidance on protecting against cyber attacks	1 July 2020	◆NHSではサイバーセキュリティ攻撃からの保護に関するさまざまなガイダンス資料を随時公表する。本ガイダンスは、2017年のWannaCry攻撃の後に公開された

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

医療情報セキュリティ関連（ENISA（EU））

文書名	作成時期	概要
Good practices for the security of healthcare services	24　Feb　2020	◆病院の調達責任者およびCISOs/CIOsに対して、病院の調達プロセスの際にサイバーセキュリティの目的達成に採用できる一連の包括的なツールやグッドプラクティスを提供することを目的とする。 ◆調達に関する計画、ソースおよび管理の3つのフェーズにグッドプラクティスをマッピングし、病院の調達プロセスを改善させる使いやすいガイドを提供 ◆調達対象として、サイバーセキュリティの考慮事項が関わる10種のカテゴリーを想定。それぞれについて、サイバーセキュリティの側面をリスト化したうえで、主なサイバーセキュリティの課題を示すことで、調達のサイバーセキュリティに対策例を提供する ◆その他、GDPR、HIPAA、FDA Guidance for cybersecurityなどへの対応なども示す。

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

医療情報セキュリティ関連（IMDRF）※

文書名	作成時期	概要
Principles and Practices for Medical Device Cybersecurity	18 Mar 2020	◆ヘルスケア製品の製造業者、ヘルスケアプロバイダ、ユーザ、並びに規制当局及び脆弱性報告者を含む全ての責任関係者に向けて、医療機器（IVD 医療機器を含む）のサイバーセキュリティに対する一般原則に係る基本的考え方と検討事項、並びに推奨されるベストプラクティスを提供することを目的として作成された。 ◆医療機器を使用する際に起こり得るサイバーセキュリティリスクを最小化することにより、医療機器の安全性及び性能を維持し、継続使用を確保するための具体的な推奨事項を概説する。 ◆ファームウェア及びプログラマブルロジックコントローラ等のソフトウェアを有する医療機器（例：ペースメーカ、輸液ポンプ）、又はソフトウェア単独で存在する医療機器（例：SaMD）についても、対象とする。 ◆本文書の作成方針の特徴として以下の点が挙げられる。 ➢ 適切なサイバーセキュリティ保護を備えた医療機器の設計や開発を行うため、リスクベースのアプローチを採用する。 ➢ 医療機器およびコネクテッドヘルスケアインフラの安全性、パフォーマンスおよびセキュリティを確保する。 ➢ サイバーセキュリティは、医療機器メーカー、医療提供者、ユーザー、規制当局および脆弱性発見者を含む全ステークホルダー間で共有される責任であることを認識する。 ➢ これらのステークホルダーに対して、総合製品ライフサイクル(TPLC)を通じて患者の被害リスク最小化の支援となる推奨事項を提供する。 ➢ 統一の用語を定義し、医療機器サイバーセキュリティ達成のための現在のベストプラクティスを説明する。 ➢ 透明性の向上や対応強化のため、サイバーセキュリティインシデント、脅威および脆弱性に関する幅広い情報共有ポリシーを促進する。

※本ページの作成においては、原文（ https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf ）を和訳を行ったほか、厚生労働省より公表されている邦訳（ https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf ）を参考にした。

１－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

【海外調査による示唆】

［海外におけるガイドラインの概況］

- 海外のガイドライン等のうち、米国や英国では、遵守事項を示すという手法ではなく、主にユースケースやベストプラクティスを示すことにより、事業者や医療機関等における対応を促すものが多くなっている。
- また具体的な実施のために対応ステップを示すことにより、実施方法の示唆になるものを中心に示している。この場合、医療情報システムにおける専門的な内容よりも、むしろ一般的な内容を踏まえて、医療分野の専門性から整理しているものがみられる。
- ENISAのガイドラインのように対象となる事業者を類型化して明示し、それごとに対応することが望ましいベストプラクティスなどを示すものも見られる。

［海外におけるガイドラインからの示唆］

- セキュリティ対応という点で見ると、医療機関等の環境によって、講じるべき対策が異なることから、ルールを示す場合には、各医療機関等におけるリスクに応じた対策を広く包摂するために、その表現は抽象的にならざるを得ない。海外におけるガイドラインでは、この点、ベストプラクティスという形で具体的な内容で示す形となっている。我が国のガイドラインでは、例えば厚生労働省GLでは「Q&A」などの形で、対応事例を示している。医療情報システム等提供事業者を対象とする2省GLにおいても、関連文書等でこのような内容を示すことは有用であると考えられる。
- 2省ガイドラインの対象事業者については、現状の記述では抽象的な表現となっていることから、各事業者が自らのサービスを鑑みて、対象となるか否かを判断する際に、不明瞭となる点が指摘されている。この点、ENISAのガイドラインではガイドラインで想定される調達対象事業者について具体的に示されており、具体的な判断が行いやすくなっている。2省ガイドラインにおいてもこのような具体的な表現を行うことで、対象事業者の予測可能性を高めることが期待できる。
- ENISAのガイドラインやIMDRFの文書では、医療機関等などを対象としつつ、併せて医療情報システム等提供事業者もこれを参照すべきとされている。セキュリティ対応においては、一部の医療機関等を除いては、医療機関等では専門的な知見を有していない。我が国におけるガイドラインにおいてもこのような状況を踏まえて、医療機関等と事業者が同時に参照できるような整理を行うことが望ましい。

1 – 3 国内の事業者・有識者へのヒアリング結果

■ 国内の事業者・有識者へのヒアリング調査を実施した（ヒアリング企業・団体等は次ページ）。また併せて、事業者等から構成される「2省GL有識者委員会　ベンダーワーキング」に対しても同様の内容を確認した。以下、その結果を示す。

■ ヒアリング先は、医療情報システム等の提供事業者については、その2省GLの適用対象事業者のうち

- 電子カルテシステム
- 介護情報システム
- オンライン診療サービス提供事業者
- 医療関連基盤事業者
- PaaS、IaaS事業者
- PHR事業者
- ベンダー団体

等からヒアリングを行った。
またサービス仕様適合開示書の利用によりシステム導入を図っている医療機関等に対してもヒアリングの意見を聴取した。

1 – 3　国内の事業者・有識者へのヒアリング結果

ヒアリング調査先

分類	対象
ベンダー	電子カルテ等、医療情報システム等提供事業者
	介護情報システム事業者
	医療関連基盤事業者
	オンライン診療サービス提供事業者
	PaaS、IaaS事業者
	PHR事業者
	ベンダー団体
利用者	リスクコミュニケーションをサービス仕様適合開示書により実施している医療機関等

1 – 3　国内の事業者・有識者へのヒアリング結果

■ ヒアリング項目について、以下のページに示す。
■ 今回の調査では、主に
- サービス提供とそのためのセキュリティ対応等の状況
- 関係者との責任分界・リスクコミュニケーション等
- 2省GL上の課題等
- その他ガイドラインの遵守状況等

等の観点からヒアリングを行った。なお、事業者が提供する医療情報システム等の内容に応じて、ヒアリング項目についての詳細は調整して、調査を実施した。

1－3　国内の事業者・有識者へのヒアリング結果

ヒアリング項目

分類	ヒアリング項目
サービス提供とそのためのセキュリティ対応等の状況	1．提供するサービスの概要等
	2．取り扱う情報、システムの提供形態、医療情報システムとの接続状況
	3．サイバーセキュリティ対応の内容
	4．第三者認証の取得
	5．提供するシステム・サービスで取扱う医療情報の保存場所
関係者との責任分界・リスクコミュニケーション等	6．他の事業者が提供するシステム・サービスとの連携状況
	7．他の事業者とのコミュニケーション・責任分界の取り決め
	8．医療機関等とのコミュニケーション・情報の開示・責任分界の取り決め
	9．サービス仕様適合開示書、MDS・SDS等の活用
2省GL上の課題等	10．遵守状況とその判断方法、遵守に係るモチベーション等
	11．対象事業者の該当性・範囲
	12．医療情報への該当性・範囲
	13．リスクベースに関する記載
	14．その他2省GLの使い勝手
その他ガイドラインの遵守状況等	15．ベンダ側におけるセキュリティに係る取組状況、課題等
	16．医療機関等側におけるセキュリティに係る取組状況、課題等
	17．2省GL以外のガイドライン（厚生労働省GL等）について

1 – 3　国内の事業者・有識者へのヒアリング結果

■　ヒアリング結果の概要を以下に示す。

テーマ	ヒアリング結果の概要
定義に関して	• 医療情報や医療情報システムの範囲が不明瞭となるケースがある（PHR、介護情報等）
リスクベースアプローチのガイドラインについて	• リスクベースアプローチになったことにより、事業者が採用できる技術の幅が広がり、より適切な技術を選択することもできるのでよかった。 • 医療機関等からは、厚生労働省GLの項目への遵守状況を求められているため、リスクベースアプローチになじまない実態もある。
リスクコミュニケーションの現状	• 2省GLが想定するリスクコミュニケーションは、医療機関等側、事業者側双方で、リスクマネジメントに対する知見がある場合にはなされるが、それ以外の場合には事業者から医療機関等へのリスク情報の提供のみにとどまる。 • リスク情報の提供についても、事業者は必ずしもリスクアセスメント結果等ではなく、MDS/SDS等、厚生労働省GLの要求事項への適合状況に関する情報や、サービス内容などの情報に止まることがみられる。理由としては、医療機関等側、事業者側双方の知見不足がある。 • サービス仕様適合開示書やMDS／SDSを医療機関等から求められるケースが限定的。理由は、必要とする利用者（医療機関等）は、より詳細なものを求め、診療所等は、サービス内容やISMSの説明のみを求めるため。
取得すべき第三者認証	• 現状、取得を求めるISMS、Pマーク以外に、他の認証や監査報告書などでも、事業者のセキュリティ対応状況を示す資料として代替しうる。
責任分界の決定	• 約款契約による場合には、医療機関等とは個別の調整は行わず、所定の資料での対応でよいか否かの形で決定される。 • 事業者間の責任分界は、PaaS事業者が責任分界のための資料等を示している場合には、それによる。

1 – 3　国内の事業者・有識者へのヒアリング結果

■　ヒアリングの各設問における結果の概要を以下に示す。（ヒアリング項目「１」は各社のサービス概要であるため省略）

ヒアリング項目	ヒアリング結果の概要
２．取り扱う情報、システムの提供形態、医療情報システムとの接続状況	• 医療情報システムと、提供している医療情報以外の関連システムと連携しているケースはある。連携方法は、自社内提供システムとの連携や医療機関等内のサーバ等内の連携による。 • API等による連携は見られなかった。
３．サイバーセキュリティ対応の内容	• 各社ともサイバー攻撃、特にランサムウェアなどへの対応は図っている。 • 医療機関等のシステムから直接マルウェアが感染しても、サービス提供をクラウドで行う場合、医療機関等から感染するリスクは低いため、自社のサービスへの影響は少ない、とする回答が多かった。
４．第三者認証の取得	• ISMS、Pマークなど、ガイドラインで求めている第三者認証以外に、より安全性が確保できる認証や監査報告書による対応を求める回答が見られた。
５．提供するシステム・サービスで取扱う医療情報の保存場所	• 回答があった事業者では国内において保存している。ただしデータによっては海外で保存する方が合理性があるとする回答もあった。
６．他の事業者が提供するシステム・サービスとの連携状況	• 自社だけで構築している場合のほか、PaaSやIaaSを利用した事業者も見られる。 • 全体としては、クラウド化を図る事業者の回答が多かった（自社構築を行っている事業者も、一部他社クラウドサービスを利用するケースも見られた）。
７．他の事業者とのコミュニケーション・責任分界の取り決め	• PaaS事業者の中には責任分界に関する資料などが提供するケースがあり、これに基づいて対応する事業者が多くみられた
８．医療機関等とのコミュニケーション・情報の開示・責任分界の取り決め	• 現状では、厳密な意味でのリスクコミュニケーションをとっている例は少ない。 • 一因として、医療機関側においてリスクマネジメントに対する知見が乏しく、またそのための要員がいないことが挙げられる。さらに事業者側においても、必ずしもリスクマネジメントについて、知見が十分ではないケースがみられる。

1－3　国内の事業者・有識者へのヒアリング結果

	ヒアリング結果の概要
9．サービス仕様適合開示書、MDS・SDS等の活用	• 現状、サービス仕様適合開示書やMDS/SDSの活用を行っていない事業者があった。 • その回答の理由として、顧客への提供情報としては、顧客側からより詳細なものが求められる、あるいは逆に詳細なリスク等に関して理解できないため、サービス内容の説明のみを求める等で、必ずしも顧客ニーズに合っていなかったとされる。
10．遵守状況とその判断方法、遵守に係るモチベーション等	• 遵守対応をしている事業者は多いが、ISMSやPマークなどは費用面も含めて負担が大きいとする事業者が多い。 • 事業者によっては、提供サービスや形態によっては、遵守する対象自体が明確ではない・疑問があるというケースも見られるという回答があった。
11．対象事業者の該当性・範囲	• PHR事業者からは、適用対象の判断がわかりにくいほか、2省GLとPHR指針との関係を確認しながら対応を図ることの負担などが挙げられた。
12．医療情報への該当性・範囲	• 医療情報の解釈自体が問題となるとする回答が見られた。 • 今回の調査では、PHRや介護情報などはすべて医療情報と同様の基準となるように整理することで対応がばらつくことを防いでいる事業者が見られた。
13．リスクベースに関する記載	• リスクベースアプローチにより利用しやすくなったとする反面、リスクベースで考えるとしても、想定するリスクを抽出する負担などはあるので、負担が減少したとは限らないとする回答もあった。 • また厚生労働省GLが項目遵守型のものであり、こちらに対する遵守を医療機関等から求められるため、実際のリスク分析の適用が難しいとする回答もあった。 • 医療機関等側においてもリスクベースに対応できる人材の確保が重要であるが、これらは非常に困難ともされている。
14．その他2省GLの使い勝手	• 医療機関等側においては、厚生労働省GLについての対応や理解が中心で、事業者向けである2省GLへの十分な理解がなされていない、あるいは利用しにくいのではないかという意見が見られた。

1 – 3　国内の事業者・有識者へのヒアリング結果

	ヒアリング結果の概要
15.　ベンダ側におけるセキュリティに係る取組状況、課題等	• 中小の医療情報システム等提供事業者においては、必ずしも独力では対応できないのではないかという回答が見られた。
16.　医療機関等側におけるセキュリティに係る取組状況、課題等	• 主にネットワーク対策をはじめ、医療機関等側においてだけでは、セキュリティへの対応を図るのが難しいケースがみられる。 • 介護情報システムの場合には、制度改定の関係などから古いシステムを更新しながら利用しているため、リスクが内在しているケースも見られる。 • 医療機関等においても、診療所だけではなく病院等においても予算などの関係で十分な対応ができていない、実際の管理を事業者に依存せざるを得ない等のケースがみられるという回答があった。
17.　2省GL以外のガイドライン（厚労省GL等）について	• 医療機関等がすべて、厚生労働省GLにおける対策項目を網羅的に対応できるわけではないという回答があった。

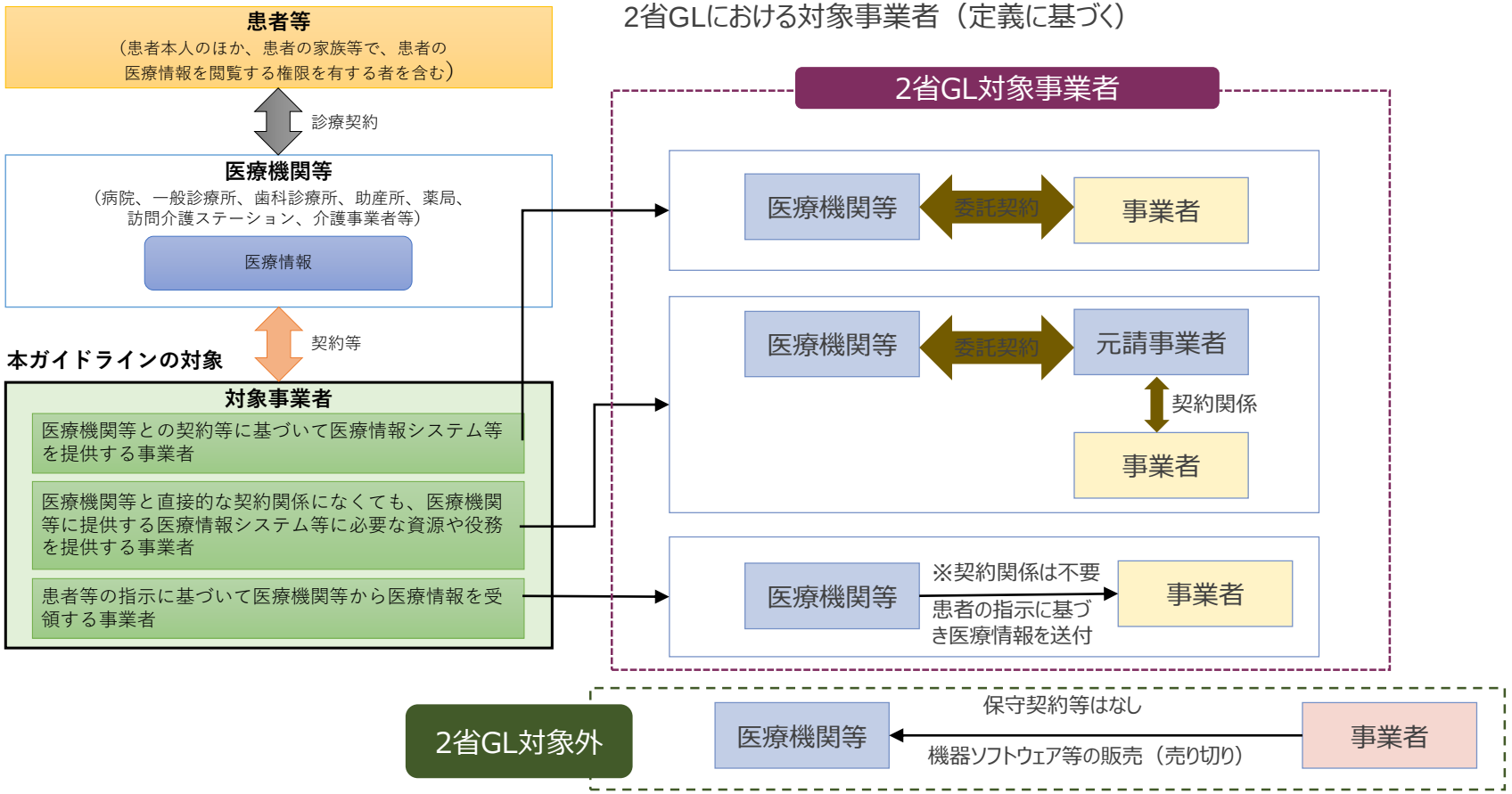
２．２省ＧＬに関する各種調査･整理作業

2－1　事業者の利便性向上に向けた資料作成等

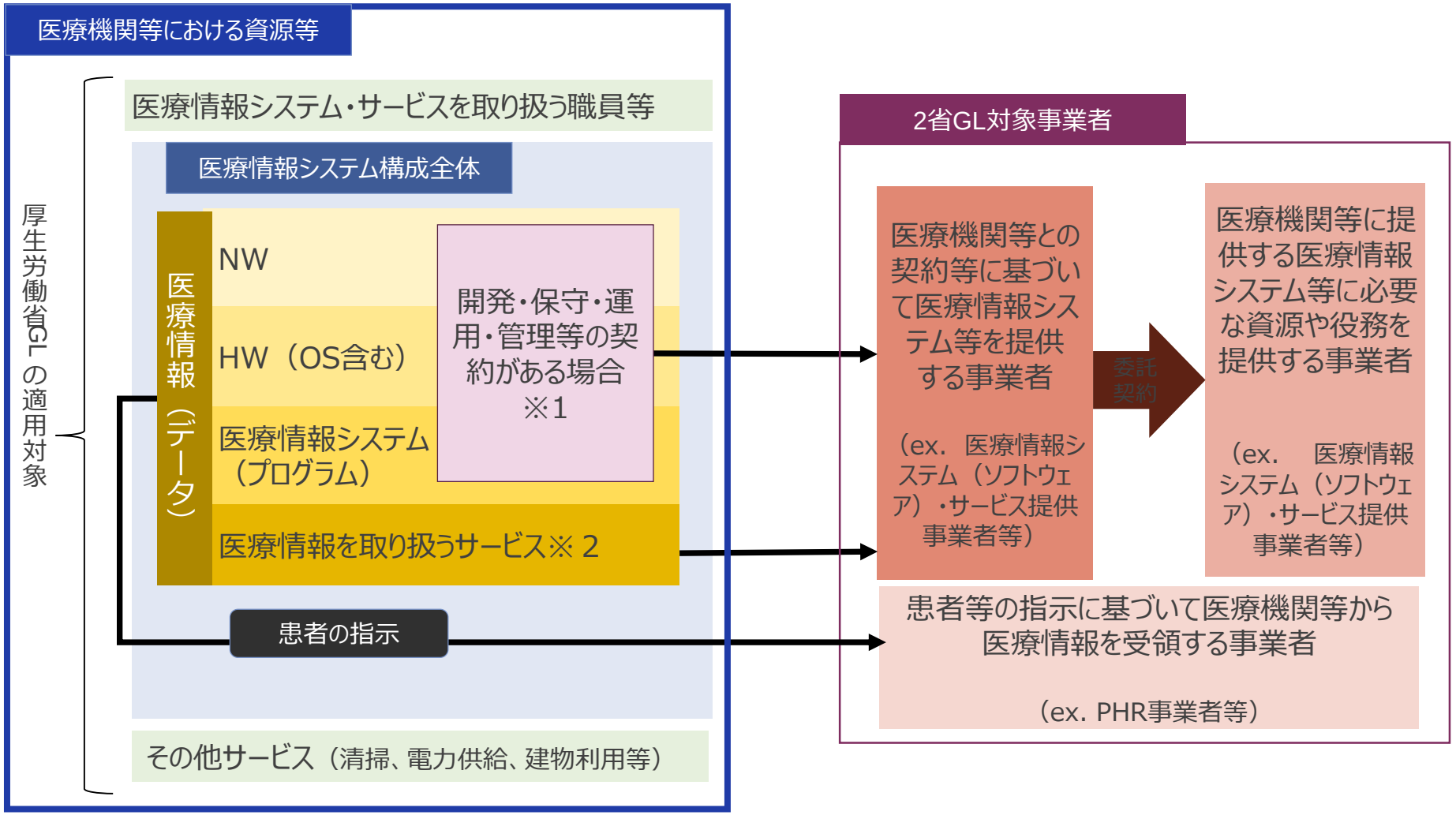
■ 事業者の利便性という点について、特に2省GL適用関係について整理した。具体的には以下の３点について、整理を行った
- 医療情報システム等提供事業者の範囲の概要
- 対象事業者であることの判断を行うことに対するフローチャート
- 2省GLの適用対象の整理

2－1　事業者の利便性向上に向けた資料作成等
①医療情報システム等提供事業者の範囲の概要

- 医療情報システム等提供事業者の範囲の概要を下記の図および次ページ図に整理した。
- 下記の図では2省GLの適用対象となる事業者と医療機関等との関係を整理し、次ページではこれを踏まえて医療情報システム等事業者が提供するシステム・サービス内容を含めて整理した。



２－１　事業者の利便性向上に向けた資料作成等
①医療情報システム等提供事業者の範囲の概要

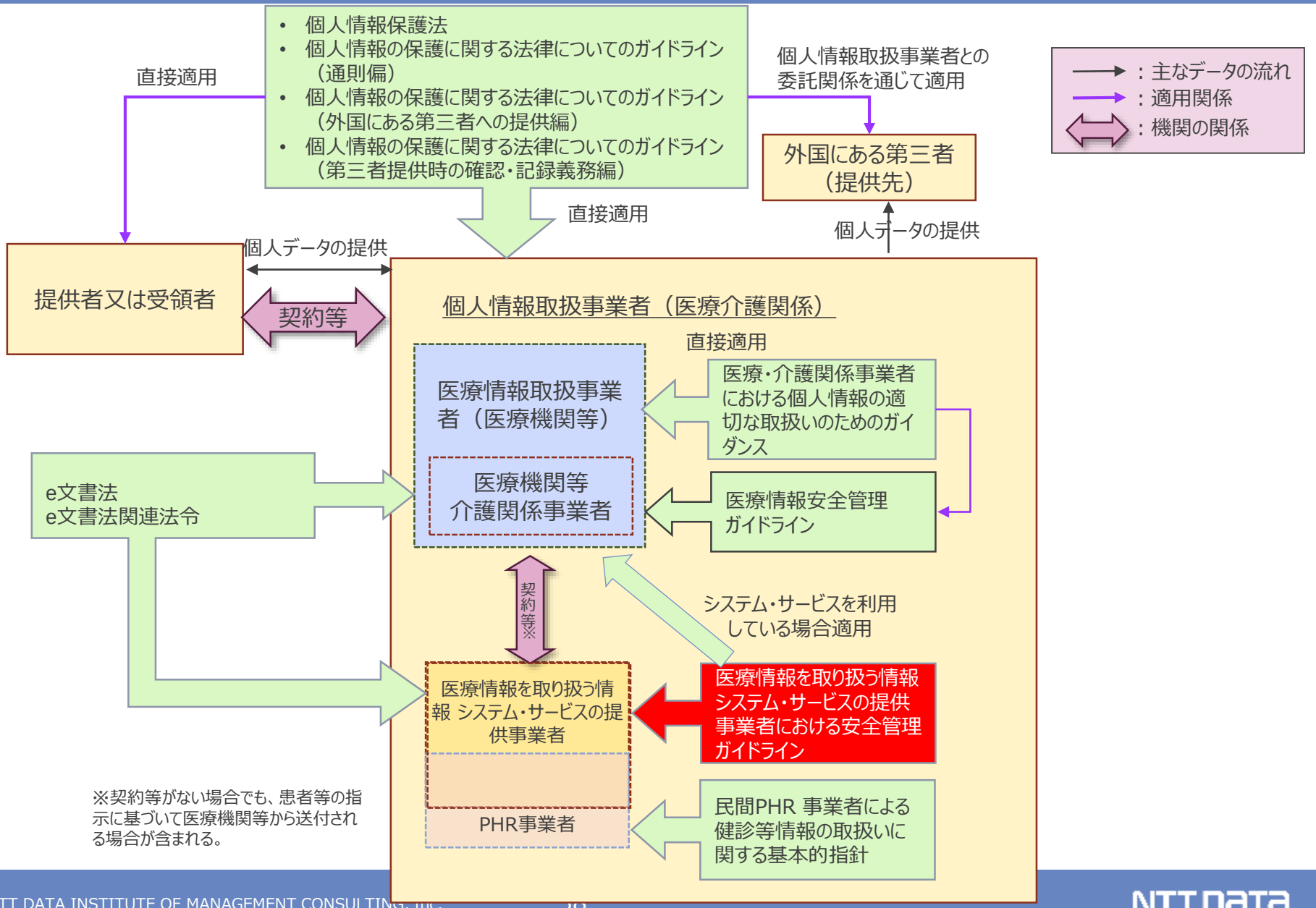


※1　開発・保守・運用・管理などの契約がない場合には、医療機関等が自らの責任範囲となる。なお単なる売買契約は含まない。
※2　医療情報を取り扱わないサービス（例えば電力供給契約や清掃契約等）は含まない

２－１　事業者の利便性向上に向けた資料作成等
②2省GLの適用対象の整理

- 2省GLの適用対象を、次ページに整理した。
- 整理に際しては、基本的には厚生労働省GLが対象とする個人情報保護法に関連するガイドラインと、e文書法及び関連法令の適用関係を中心に整理した。

2－1　事業者の利便性向上に向けた資料作成等
②　2省GLの適用対象の整理



※契約等がない場合でも、患者等の指示に基づいて医療機関等から送付される場合が含まれる。

2－1　事業者の利便性向上に向けた資料作成等
③　PHR指針と2省GLの適用対象の整理

- PHRと医療情報の関係を整理した。
- PHRについては、「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」（以下「PHR指針」）※1において「Personal Health Record の略語。一般的には、生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）である。電子記録として本人等が正確に把握し、自身の健康増進等に活用することが期待される。」と示されている。このうち、「健診等情報」は、PHR指針の適用対象となる。PHR指針は健診等情報を取り扱うPHR サービスを提供する民間事業者を対象とする。
- 一方、医療情報は、3省２GLにおいて「医療に関する患者情報（個人識別情報）」とされ、これらを取り扱う事業者が対象とされる。
- PHRと医療情報の関係についてみると、PHRには、「診療関連情報（※２）」が対象となっていることから、医療情報を患者等が、医療機関等から受領し管理する場合には、PHRに含まれるものと考えられる。
- PHRに該当する医療情報のうち、患者の指示に基づいて、医療機関等から送付され、事業者が受領したものについては、2省GLの対象とされる。受領後、患者の管理となるものは、PHRとして取り扱われる。

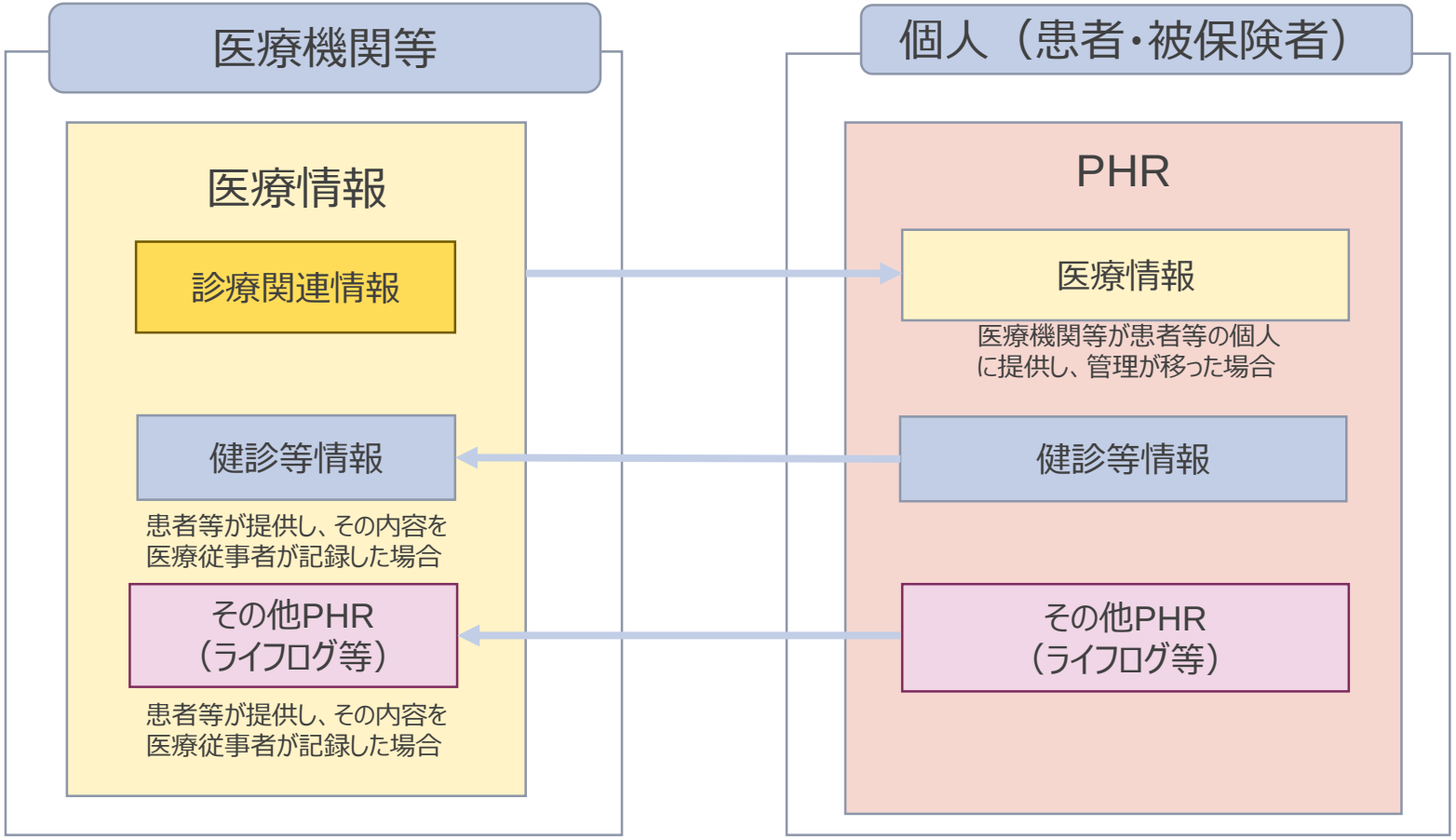
※１　https://www.mhlw.go.jp/content/10904750/000925104.pdf

※２　患者情報、診療関連情報については、法令上の定義はない。なお、「診療情報の提供等に関する指針の策定について」では「「診療情報」とは、「診療の過程で、患者の身体状況、病状、治療等について、医療従事者が知り得た情報をいう。」とされている。この観点から、本調査では診療関連情報に診療情報が含まれると解した。

診療情報の提供等に関する指針の策定について〔医師法〕
https://www.mhlw.go.jp/web/t_doc?dataId=00tb3403&dataType=1&pageNo=1

2－1　事業者の利便性向上に向けた資料作成等
③　PHR指針と2省GLの適用対象の整理

- 前ページにおいて示したPHRと医療情報の関係を、下図のように整理した



2－1　事業者の利便性向上に向けた資料作成等
③　PHR指針と2省GLの適用対象の整理

- 健診等情報は、医療情報として取り込まれない限り、医療情報には含まれないことから、基本的には、2省GLの適用はない。ただし健診等情報を、医療従事者が患者等から受領し、その内容を医療従事者が診療録等に記録した場合には、医療情報となる。この場合には、2省GLの対象となる。
- PHRに該当する医療情報（健診等情報）のうち、患者の指示に基づいて医療機関等から受領したもの以外については、2省GLの対象とはならず、PHR指針の対象となりうる。

PHR に対する2省GL、PHR指針、個人情報保護法等の適用関係の整理

PHRに属する情報の種類	PHR指針の適用	2省GLの適用	個人情報保護法令の適用
医療情報（医療機関等から受領したもの）	×	○	○
医療情報（医療機関等以外から受領・入力があったもの。）	○	×	○
健診等情報	○	×	○
上記以外のPHR（例：個人が自ら日々測定するバイタル等）	△※1	×	○（ただし個人を特定識別しないデータについては一部※２を除き、適用対象外）

※１　PHR事業者が個人関連情報を取り扱う場合や、健診等情報から仮名加工情報や匿名加工情報を作成する場合は適用対象。
※２　「一部」としては、仮名加工情報、匿名加工情報や個人関連情報などが挙げられる。

2－2　医療情報の保管方法・都道府県等による検査の具体的な方法に関する実態調査

- 2省GLの遵守状況を確認する手続の一つとして、各地の保健所が実施する調査がある。具体的には、厚生労働省地方医政局として行う「個別指導」及び「適時調査」が挙げられる。
- これらにおいて、医療情報システムに関する指摘内容などから、2省GLの遵守状況や医療情報の保存場所に関する調査の状況等を確認した。
- 厚生労働省地方医政局として行う各調査において、調査対象として挙げている項目を確認した上で、それらの指摘結果を整理した。

２－２　医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査
①実地調査の対象項目

- 医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査の実施に際して、具体的な調査項目等が厚生労働省より示されている。以下では、個別指導及び適時調査において用いられる調査実施資料等から、各実態調査において対象とされる調査項目を整理した。

２－２　医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査
①実地調査の対象項目
（１）保険医療機関及び保険医療養担当規則（療担規則）に基づく個別指導

- 療担規則による監査を踏まえて個別指導を行う際に、医療機関等向けに対して示される文書（「保険診療の理解のために【医科】（平成３０年度）」）において、厚生労働省GL･2省GLが関連する部分を以下に示す。
- この項目には、厚生労働省GLを遵守する旨は示されているが、保存場所や2省GLに関しては、個別の調査対象とすべき旨は挙げられていない。

Ⅴ 医科診療報酬点数に関する留意事項

１． 診療録（カルテ）

(4) 医療情報システム（電子カルテ等）に関する留意点

「医療情報システムの安全管理に関するガイドライン第 5 版」（平成 29 年 5 月）が厚生労働省から公表されているので、医療情報を扱う際にはこれに十分留意する。

- 診療録等の真正性、見読性、保存性を確保すること。

真正性：修正、消去やその内容の履歴が確認できる。記録の責任の所在が明らか。

見読性：記録事項を直ちに明瞭、整然と機器に表示し、書面を作成できる。

保存性：記録事項を保存すべき期間中、復元可能な状態で保存する。

- 端末使用開始前に、ログアウトの状態であることを確認する。また、席を離れる際はクローズ処理等（ログオフやパスワード付きスクリーンセイバー等）を施すこと。
- パスワードは英数字、記号を混在させた 8 文字以上が望ましい。また、最長でも 2 ヶ月以内に定期的に見直し、不正アクセスの防止に努めること。また、パスワードや ID は、本人しか知り得ない状態に保つようにすること。例えば、それらを記したメモを端末に掲示したり、医師がそれらを看護師に伝達し、食事、臨時処方等のオーダーを代行入力等をさせないこと。
- 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。また、個人情報が保存されている機器や記録媒体の設置、保存場所には施錠し、PC 等の重要機器には盗難防止用チェーンを設置すること。

２－２　医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査
①実地調査の対象項目
（１）保険医療機関及び保険医療養担当規則（療担規則）に基づく個別指導

Ⅴ 医科診療報酬点数に関する留意事項
２． 傷病名
(1) 傷病名記載上の留意点
- 診断の都度、診療録（電子カルテを含む。）の所定の様式に記載すること。なお、電子カルテ未導入の医療機関において、「医療情報システムの安全管理に関するガイドライン」に未準拠のオーダーエントリーシステムに傷病名を入力・保存しても、診療録への傷病名の記載とは見なされないため、必ず診療録に記載すること。

Ⅴ 医科診療報酬点数に関する留意事項
４ 医学管理等
(2) 算定上の留意点
（算定要件の例）
① オンライン医学管理料※
- オンライン診察を行う際には、厚生労働省の定める情報通信機器を用いた診療に係る指針に沿って診察を行う。

Ⅴ 医科診療報酬点数に関する留意事項
５ 在宅医療
(1) 在宅患者診療・指導料
④オンライン在宅管理料
- オンライン診察を行う際には、厚生労働省の定める情報通信機器を用いた診療に係る指針に沿って診察を行う。

※オンライン診療指針には２省ＧＬの遵守を求める記載があるため、その遵守を求める内容も示した。

２－２　医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査
①実地調査の対象項目
（２）療担規則に基づく適時調査

- 療担規則に基づいて適時調査を行う際に医療機関等向けに対して示される文書（調査書　確認事項）において、厚生労働省GL･2省GLが関連する部分を以下に示す。
- 適時調査については、各調査書の中で調査項目が示されており、医療情報システム等に関しては、医療情報システム厚生労働省GLやオンライン診療指針への適合性が示されているが、2省GLに関する内容や、詳細項目については示されていない。

適時調査　調査書　確認事項（重点的に調査を行う施設基準　入院基本料等加算）

◇ 診療録管理体制加算１（Ａ２０７）
◇ 診療録管理体制加算２（Ａ２０７）

中央病歴管理室が設置されており、厚生労働省「医療情報システムの安全管理に関するガイドライン」に準拠した体制である。（　適　・　否　）

２－２　医療情報の保管方法･都道府県等による検査の具体的な方法に関する実態調査
①実地調査の対象項目
（２）療担規則に基づく適時調査

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初･再診料の施設基準等
第１ 情報通信機器を用いた診療
１ 情報通信機器を用いた診療に係る施設基準
(１) 情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア 保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
(２) オンライン指針に沿って診療を行う体制を有する保険医療機関であること。

２－２　医療情報の保管方法・都道府県等による検査の具体的な方法に関する実態調査
②各調査の指摘事項

- 厚生労働省地方医政局が行う個別指導、適時調査において指摘された事項を以下に整理する。
- 主に厚生労働省GLの遵守項目に関するものが指摘の対象となっており、そのうち診療録の認証や組織的対策に関するものが中心
- 保存場所に関する内容や、医療情報システム・サービス提供事業者に対する委託関係で、直接示される内容は見られない

項目	指摘内容
組織等	• 運用管理規程を定めていない。（東北・関東・九州） • 診療記録の保管管理の規定について、診療録等の保存年限を明文化すること。（中国） • 診療録の保管・管理の規程及び診療情報の提供に関する規程を実態に沿った形に見直すこと。（中国） • 情報及び情報機器の持ち出しに係る運用管理規程の内容が不十分である。（九州） • 定期的に職員に対し個人情報の安全管理に関する教育訓練を行っていない。（東北・九州）
認証関係	１．診療録等 • 異動・退職した職員のＩＤの管理が適切に行われていない。（近畿・九州） • パスワードの設定について次の不適切な例が認められた。（東北） • パスワードが８文字未満である（東北・関東・東海・九州） • 英数字、記号を混在させた８文字以上13文字未満の指定困難な文字列を定期的に変更させていない（最長でも２か月以内）（東北・関東・近畿・九州） • 代行入力により記録された診療録等について、確定者による「確定操作（承認）」が行われていない又は実施記録がない。（東北・関東） ・パスワードの更新期限を適切に設定していない。パスワードの更新期限は最長でも２か月以内に設定すること。（東海） • アクセス権限の範囲設定が不適切である又は定められていない。（東北・九州） • 代行入力を認める業務又は誰が誰の代行をしてよいかについて運用管理規程に定めていない。（関東・東海・九州） • 代行操作の承認の仕組みがない。（近畿） • 特定のＩＤを複数の職員が使用している。（東北・関東・東海・九州）
物理的セキュリティ	• 端末から離席する際、他の者による入力ができないよう、クリアスクリーン等による防止策が講じられていない又は講じられているが不十分である。（東北・東海・九州）

２－２　医療情報の保管方法・都道府県等による検査の具体的な方法に関する実態調査
②各調査の指摘事項

項目	指摘内容
システム機能	• 修正履歴が表示されない。（東北・九州）
運用・監査	• 運用管理規程に定めているシステムの監査を実施していない。（東北・関東・近畿・九州）
緊急時	• 緊急時・災害時の連絡などシステム障害時のマニュアルを定めていない。（関東）
その他	• 精神科退院指導料にかかる計画書の保存が適切に行われていない。（関東）

２－２　医療情報の保管方法・都道府県等による検査の具体的な方法に関する実態調査
③実態調査における2省GLへの遵守状況確認の現状についての整理

- 厚生労働省地方医政局が行う療担規則に基づく個別指導、適時調査等の実態調査に関する調査結果を以下のとおり整理する。
- 厚生労働省地方医政局が行う個別指導、適時調査では、調査項目においては主に厚生労働省GLへの適合性への確認が中心であり、2省GLへの遵守状況はその調査内容の一つとして捉えられていると考えられる。
- 一方で詳細調査項目として挙げられているのは、医療機関等における組織的な対策や、人的対策、「施行通知」に関する項目（いわゆる電子保存3原則）に関するものである。詳細調査項目として、「外部保存通知」に関する言及や、2省GLに関する遵守状況などは示されていない。
- 実態調査の結果として、指摘事項についても、詳細調査項目に挙げられているものが中心となっている。なお、電子保存3原則を満たすべき仕様に関する違反も指摘されているが、これは厚生労働省GLを満たしていないのと同時に、2省GLにおける「制度上の要求事項」を満たしていないことになるが、指摘内容として、2省GL違反としては示されていない。また保存場所に関する指摘はなかった。

2－3　医療情報の保管場所について

- 2省GLでは、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にするよう求めている。これは以下の経緯に基づくものである
  - 国内に医療情報が保存されていない場合、医療情報に関する適切な捜査や調査ができない可能性があるのではないか
  - 国外に保存されている医療情報については、保存されている国の政策等により、保存されている国から我が国への移転が難しい、我が国におけて保障している患者等のプライバシーなどを踏まえた手続等によらず、不適切な形で利用される等が生じるのではないか。
  - 国内に保存されている医療情報について、国外の法律の適用がある場合には、わが国の法令では保障されていない形で国外への流出が発生するのではないか。
- 上記の観点から、「医療情報システム等が国内法の執行の及ぶ範囲」に関する議論を整理する。

2－3　医療情報の保管場所について

【国内の捜査権等の海外への適用について】

- 我が国の刑事事件の捜査（公判における補充捜査を含む。）に必要な証拠が外国に存在する場合、共助に関する条約により別のルートを定めていない外国に対しては、外交ルートを通じて国際令状による捜査共助を要請することとされる※１。
- これを行うため、「国際捜査共助等に関する法律」※２が定められており、同法が定める手続きを通じて、海外における証拠収集等を行うことになる。また刑事事件に関しては、国際刑事警察機構（ICPO）ルートによる方法もあるとされる。
- なお「サイバー犯罪に関する条約」第32条※３による場合には、上記の方法によらず、直接わが国の捜査機関が、海外における証拠の差し押さえを行うことができるとされる。
- 判例は、刑事事件で日本国内で押収した資料に基づき、上記サイバー犯罪に関する条約第32条によらない捜査方法で取得した事案では、収集した情報の違法性を認める（東京高判平成28年12月7日）。他方、サイバー犯罪に関する条約第32条を踏まえ、「記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に」は、収集した証拠が適法であることを認める（最決令和3年2月1日）。※４
- 行政法上の事件に関しては、明確な規定はない。なお、「個人情報保護法いわゆる３年ごと見直し制度改正大綱」※5における個人情報保護委員会の検討過程では、「国内サーバ保存義務付けに関する意見」についても検討されたが※6、同大綱では、域外適用の強化等の対応による国内設置に関する強化などは示していない。なお外国事業者への検査は「委員会による外国の事業者に対する立入検査を可能とする。もっとも、外国主権との関係から、他国の同意がない限り、他国領域内における公権力の行使はできない」とし、捜査共助に準じた対応を行うこととしている。

※１「３．捜査・司法に関する国際共助」（法務省（https://hakusyo1.moj.go.jp/jp/48/nfm/n_48_2_2_6_3_1.html）
※２　国際捜査共助等に関する法律（昭和55年法律第69号）
※３「サイバー犯罪に関する条約」(https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf)
第32条「締約国は、他の締約国の許可なしに、次のことを行うことができる。
a 公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所のいかんを問わない。）。
b 自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。」
※４　次ページ
※５「個人情報保護法いわゆる３年ごと見直し制度改正大綱」個人情報保護委員会（令和元年12月13日）P29
（https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf）
※６　第127回 個人情報保護委員会「資料1 個人情報保護を巡る国内外の動向」P3（https://www.ppc.go.jp/files/pdf/191125_shiryou1.pdf）

2－3　医療情報の保管場所について

【国内の捜査権等の海外への適用について】

判例	事案概要	判旨の概要
東京高判平成28年12月7日（https://www.courts.go.jp/app/hanrei_jp/detail3?id=86761）	• 警察官らは，本件パソコンを解析したところ，偽造文書を作成，販売するとしている「M」と称するインターネットサイト（以下「Mサイト」という）で，注文の連絡先とされていたメールアドレス（以下「Mメールアドレス」という）のアカウント（以下「Mアカウント」という）へのアクセス履歴の存在等が認められたことから，本件パソコンからインターネットに接続し，メールサーバにアクセスすることなどを企画し，検討の結果，メールサーバへのアクセスも検証のために必要な処分として許容されると考え，上記別件を被疑事実とする本件パソコンの検証許可状の発付を得た。 • 本件パソコンの内容を複製したパソコンからインターネットに接続し，Mアカウントにログインし，Mメールアドレスに係る送受信メールを抽出してダウンロードし，保存するという本件検証を行った。	• 本件検証は，本件パソコンの内容を複製したパソコンからインターネットに接続してメールサーバにアクセスし，メール等を閲覧，保存したものであるが，本件検証許可状に基づいて行うことができない強制処分を行ったものである。 • しかも，そのサーバが外国にある可能性があったのであるから，捜査機関としては，国際捜査共助等の捜査方法を取るべきであったともいえる。そうすると，本件パソコンに対する検証許可状の発付は得ており，被告人に対する権利侵害の点については司法審査を経ていること，本件パソコンを差し押さえた本件捜索差押許可状には，本件検証で閲覧，保存したメール等について，リモートアクセスによる複写の処分が許可されていたことなどを考慮しても，本件検証の違法の程度は重大
最決令和3年2月1日（https://www.courts.go.jp/app/hanrei_jp/detail2?id=89995）	• 捜索差押えの実施に先立ち，Yではアメリカ合衆国に本社がるA社の提供するメールサービス等が使用されている疑いがあり，令状に基づきメールサーバ等にアクセスすることは外国の主権を侵害するおそれがあると考えられたことから，日本国外に設置されたメールサーバ等にメール等の電磁的記録が蔵置されている可能性があることが判明した場合には，令状の執行としてのリモートアクセス等を控え，リモートアクセス等を行う場合には，当該パソコンの使用者の承諾を得て行う旨事前に協議していた。 • 警察のパソコンでメールサーバ等にアクセスできるアカウントを付与するなどして被告人事務所以外の場所でダウンロード等ができるようにすることについて、被告人の幹部と警察官との間で，被告人の顧問弁護士も交えて協議が行われ、最終的に被告人が承諾書を作成した。警察官は，これに基づき，被告人事務所外の適宜の機器からリモートアクセスを行い，電磁的記録の複写を行った。	• 刑訴法99条２項、218条２項の文言や，これらの規定がサイバー犯罪に関する条約（平成24年条約第７号）を締結するための手続法の整備の一環として制定されたことなどの立法の経緯，同条約32条の規定内容等に照らすと，刑訴法が，上記各規定に基づく日本国内にある記録媒体を対象とするリモートアクセス等のみを想定しているとは解されず，電磁的記録を保管した記録媒体が同条約の締約国に所在し、同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に，国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許されると解すべきである。

2－3　医療情報の保管場所について

【国外に保存されているわが国の医療情報等に関するリスクについて】

- 国外に保存されているわが国の医療情報等に関するリスクとして、保存している国における政策により、我が国への移転が制限されたり、あるいは保存している行政機関等による検査や押収などが想定される。
- そのため、医療情報に関する事故等が生じた場合に、対象となる情報が適切に取得できない場合が生じたり、あるいは医療情報が、わが国の個人情報保護法や、3省２GLで想定している保護が図られない形で取り扱われるリスクがある。
- 具体的なリスクの可能性があるものとして代表的なEU、米国、中国の例を示す。なお制度によっては既に廃止しているものや、我が国との関係では、実質的にリスクとなっていないものも含む。

国等	法令名	条項	内容等	備考
EU	GDPR	44 条	域内保存のデータに関する域外への越境移転規制（域内保存データが、域外在住の者である場合含む）	我が国は相互認証により域外移転可能
米国	PATRIOT Act	第220条	電子監視のための捜査令状の全国的発付 捜査対象となる犯罪を管轄する裁判所は、プロバイダの住所地の裁判所の介入を求めることなく、政府がプロバイダ等から電子的通信を入手するための捜査令状を発する権限を有する。	2015年失効

2－3　医療情報の保管場所について

【国外に保存されているわが国の医療情報等に関するリスクについて】

国等	法令名	条項	内容等	備考
中国	サイバーセキュリティー法※１	第37条	• 重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。 • 業務の必要性により、国外に対し確かに提供する必要のある場合には、国のネットワーク安全情報化機関が国務院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。	個人情報保護法の国内保存義務とほぼ同じ
	個人情報保護法※２	第40条	• 個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならないとされている。 • そして、確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価に合格しなければならない	
	データセキュリティ法）※３	第31条	• 重要情報インフラの運営者が中国国内における運営において収集および生成した重要データの国外移転に係るセキュリティ管理については、「サイバーセキュリティ法」の規定を適用 • その他のデータ取り扱い者が中国国内における運営において収集および生成した重要データの国外移転に係るセキュリティ管理については、国家インターネット情報機関が国務院関係機関と共同で制定する管理弁法を適用する	
		第36条	• 「中華人民共和国の主管機関の認可を経ない限り、国内の組織、個人は、外国の司法または法執行機関に中華人民共和国国内に保管されるデータを提供してはならない	
	中国暗号法※４		• 国が暗号を分類管理	

※１　2016 年制定（https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf を参考に作成）
※２　2021年制定　2021年11月1日施行（ https://www.soumu.go.jp/main_content/000800520.pdf　を参考に作成）

※３　2021 年 6 月 10 日公布、2021 年 9 月 1 日施行（https://www.soumu.go.jp/main_content/000800520.pdf　を参考に作成）
※４　2019 年 10 月 26 日公布、2020 年 1 月 1 日施行（https://www.soumu.go.jp/main_content/000800520.pdf　を参考に作成）

2－3　医療情報の保管場所について

【国内に保存されているわが国の医療情報等に対する国外法適用に関するリスクについて】

- 我が国の国内に保存されているにもかかわらず、国外の法律が適用されることにより、国内の医療情報等が国外に提供されるリスクが存在する。
- 一つは米国におけるCLOUD法（The Clarifying Lawful Overseas Use of Data Act）であり、これはデータを取扱う米国内プロバイダに対して、米国内外を問わずデータの保全や開示を求めるものである（企業側は拒否する権限を有しない）。
- また中国の「中華人民共和国国家情報法」は、中国の国内外を問わず国民に対して、「必要な支持、援助及び協力の提供」を求めることができるとする。

国等	法令名	条項	内容等	備考
米国	CLOUD法※1	第2713条	• 「電子通信サービスあるいは遠隔コンピューティングサービスを行うプロバイダーは、顧客や契約者に関係する有線又は電子通信、その他のいかなる記録や情報についてもこれを所有し、管理し、又は制御している場合、その通信や記録、その他の情報が米国の内外のいずれにあろうとも、［令状等に基づき］保全（preserve）、バックアップ、又は開示（disclose）をするという義務に服さなければならない • （i）「顧客又は契約者が米国民でなく、かつ、米国に所在していない場合」及び（ii）「要請された開示によって、適格（qualifying）外国政府の法令に違反する重大な危険が生じる場合」に該当すると合理的に信じる場合、プロバイダーは、14 日以内に令状等の修正又は却下（modify or quash）を申し立てることができる	通信保存法（SCA）を改正した形で制定
中国	中華人民共和国国家情報法※2	第14条	• 国家情報活動機構は、法に従い情報活動を行うに当たり、関係する機関、組織及び国民に対し、必要な支持、援助及び協力の提供を求めることができる。	

※1　“Clarifying Lawful Overseas Use of Data Act of 2018”（「域外リモートアクセスによる証拠収集にかかる米国 CLOUD 法に基づく行政協定に関する一考察」（有本 真由）（https://www.jstage.jst.go.jp/article/inlaw/18/0/18_180002/_pdf ）を参考に作成）
※2　2017年制定 「中国の国家情報法」（岡村　志嘉子）（外国の立法 274（2017.12））（https://dl.ndl.go.jp/view/download/digidepo_11000634_po_02740005.pdf?contentNo=1 を参考に作成）

2－3　医療情報の保管場所について

【我が国の情報システム・サービス調達における国内法・国外法の適用に関する規定】

- 我が国の情報システム・サービス調達における国内法・国外法の適用に関する規定として、医療情報関係では、総務省から公表されていた
  - ASP・SaaS事業者が医療情報を取り扱う際の安全管理ガイドライン
  - 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ガイドライン

  がある。
  また、近時では政府システムの調達に関して国内法・国外法の適用に関する規定が設けられている。
- 以下ではその内容を紹介する。

2－3　医療情報の保管場所について

- 「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第 1.1 版」※１では、「医療情報システムの安全管理に関するガイドライン第4.1版」における「4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。」という遵守事項に対応するASP・SaaS 事業者の要求事項として、医療情報システム等を国内法の適用が及ぶ地域に設置することを示した。この場合、設置場所の制限を行うという趣旨に基づく。
- 「 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」を統合・改定した「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第1版」では、同様の規定を設けるとともに、適用関係を明らかにするため「適用」から「執行」に修正した。

記載箇所	ASP・SaaS 事業者への要求事項 （情報セキュリティ対策ガイドラインの記述と下線部は本ガイドラインで追記した記述）	付記事項
表 3-8 災害等の非常時の対応における ASP・SaaS 事業者への要求事項	所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。	追記理由： • 所管官庁に対して法令に基づく資料提出のため、機器等の設置場所を制限するため

記載箇所	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第1版の要求事項	備考
３．２．８災害等の非常時の対応についての安全管理対策（２）（イ）	3.サイバー攻撃等への対応 ④ ③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する。	「SLA参考例」における設置場所に関する規定に合わせる観点から「適用」から「執行」に変更

※１　https://www.soumu.go.jp/main_content/000095031.pdf
※２　https://www.soumu.go.jp/main_content/000567229.pdf

2－3　医療情報の保管場所について

- データの設置場所に関して規定する例として、政府システムで用いる情報システム・サービスでは、管理している情報により、国内法や国外法の適用に関する規定が設けられている。その内容を次ページ以下で整理した。
- 「政府機関等の対策基準策定のためのガイドライン　令和3年度版」では、委託業務に関して、国外法が適用される場合には、国内法では認められないアクセスがあることに対する可能性に留意することとし、また行政機関個人情報保護法などが適用される場面では、国内法のみが適用される場所に制限される必要があるとする。クラウドサービス以外の利用についても、情報管理等に関するカントリーリスクがあることを踏まえた措置（暗号化等）を講じることを求める。
- 「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」では、ガバメントクラウドに関しては、国内に閉じた利用とすることを求めるが、それ以外の場合には、国内設置を基本としつつ、合理的な理由があり、争訟リスクが低い場合には、契約にデータ保護を設けることを条件として、例外を認める。

2 – 3　医療情報の保管場所について

政府機関等の対策基準策定のためのガイドライン（令和３年度版）令和３年７月７日
令和４年12月12日一部改定　内閣官房 内閣サイバーセキュリティセンター

	目的
(1) 業務委託に係る規定の整備 (a) 統括情報セキュリティ責任者は、業務委託に係る以下の内容を含む規定を整備すること。 (ア) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本款において「委託判断基準」という。）	• 特に、委託業務で取り扱われる情報に対して国外の法令等が適用される場合があり、国内であれば不適切と判断されるアクセス等が行われる可能性があることに注意が必要である。 • 機関等における「行政機関の保有する個人情報の保護に関する法律」（平成 15 年法律第 58 号）が規定する保有個人情報、「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号）が規定する保有個人情報及び「個人情報の保護に関する法律」（平成 15 年法律第 57 号）が規定する個人データについては、国内法令のみが適用される場所に制限する必要があると考えられるため、当該個人情報を取り扱う委託業務においては、保存された情報等に対して国内法令のみが適用されること等を業務委託の際の判断条件としておくべきである。
(3)外部サービスの選定（クラウドサービス以外の場合） (e)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの利用を通じて機関等が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて機関等の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。	• 国内法以外の法令及び規制が適用されるリスクとして、データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が機関等のデータを含んだまま没収されるなどが考えられる。なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、機関等の管理する暗号鍵で情報を暗号化するなどの措置を検討する必要がある。

https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf

2 – 3　医療情報の保管場所について

政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針
（2022 年（令和４年）12 月 28 日デジタル社会推進会議幹事会決定）

目的
３.６ セキュリティについて 「セキュリティと利便性とコストでバランスをとる」、「扱う情報の機密性等に応じたセキュリティ対策をとる」等の基本的な方針は普遍であり、「政府機関等のサイバーセキュリティ対策のための統一基準群」や個人情報の保護に関する法律等の個人情報等の適正な取扱いに関する関係法令等への準拠が求められる1ことはオンプレミスと変わらない 当該民間事業者が外国にある事業者の場合や当該民間事業者が国内にある事業者であっても外国に所在するサーバに保有個人情報が保存される場合においては、「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」（令和４年２月個人情報保護委員会事務局）等も参照しつつ、外的環境の把握等の対応が必要となる点に留意が必要である。
1) ガバメントクラウドに選定されているクラウドサービス ガバメントクラウドのポリシーで許可されている範囲（リージョン、サービス）での利用とすることで、国内に閉じた利用となる。 2) その他のクラウドサービス 当該クラウドで利用するデータセンタの設置場所に関しては、国内であることを基本とする。 ただし、システムの可用性、データの保存性、災害対策等から冗長化やバックアップ用のデータセンタが海外にあることが望ましい場合、準拠法や国際裁判管轄を確認し、かつ具体的な争訟リスクが低い場合又は別途、契約等において利用者データの保護が担保される場合はこの限りではない。 なお、利用者データ（利用者が作成・管理するデータ）を国外に設置されるクラウドに保管する場合は以下の対策を行うこと。 ・利用者データの保護 ・利用者データ可用性の確保
３.２ クラウド利用者のデータが所在する地域と適用される法令等について クラウドの利用にあたっては、国内法以外の法令及び規制が適用されるリスクを評価し、情報が取扱われる及び契約に定める場所と準拠法・国際裁判管轄に留意する必要がある。このため、こうしたリスクを低減する観点から、利用するサービスや、データセンタの設置場所等を選択する必要がある。

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/17ef852e/20221228_resources_standard_guidelines_guideline_01.pdf

２－４　別紙２の取扱いに関するニーズ調査

- １－３の調査と併せて別紙２の取扱いに関するニーズ調査等を確認した（調査項目８～10、13参照）、その結果を以下に示す。
- 厚生労働省GLがルールベースアプローチであり、2省GLがリスクベースアプローチであり、遵守事項に関しては従前のような要求事項としての対応関係には立っていない。
- リスクベースアプローチを実施している事業者では、医療機関等へ提供する情報については、ルールベースによる適合性を確認し、別紙2で確認しながら、対応する項目についてリスクベースでの対策を講じるという手法が採られることが想定された。
- 一方、今回の調査では、医療情報システム等事業者においては、必ずしもリスクベースアプローチに対して、適切なリスクマネジメントを実施するだけの知見を有していない事業者も存在することが多いことが分かった。そのため、厚生労働省GLにおける遵守項目の対応のみを行う事業者も、特に中小事業者においては多いのが現状である。
- なお、医療機関等との責任分界や役割分担を定める際、事業者が行うべき対策の整合性を確認するために用いているというケースも見られた。
- 以上から、現時点では現状の利用方法としては、ルールベースである厚生労働省GLを示しながら、その具体的な手法を整理するために、2省GLにおける対応内容やリスクシナリオを示すほうが、事業者の利用実態に即している状況であった。

【付録】
海外調査結果

医療機器のサイバーセキュリティ地域のインシデントの準備および対応のプレイブック バージョン2.0（2022年11月15日）

（Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook）

（FDA（米国））

1.2. 事業実施方法

（１）３省２ＧＬに関する課題等調査･改定案の提案

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

医療機器のサイバーセキュリティ地域のインシデントの準備および対応のプレイブック バージョン2.0

	Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
対象者	• この地域プレイブック（以下プレイブック）の主な対象者は、医療提供機関（HDOs）である。 • 本プレイブックは、特に医療機器のサイバーインシデントの準備と対応に携わるスタッフ、これらに限定するものではないが、臨床医、医療技術管理(HTM)専門家、情報技術 (IT)、緊急対応、リスク管理および施設のスタッフ • サイバーセキュリティの準備および対応計画の策定目的での利用を想定
	• デバイスメーカーやHDOsの対応の取り組みをサポートするメンテナンス請負業者や医療システム、地域および国の対応パートナーなどを含む、その他の外部機関のステークホルダーにも有用
目的	• このプレイブックは、患者ケアや安全性のための臨床業務の継続性に影響を与える可能性のある医療機器に影響を与えるサイバー脅威へのHDOsの対処を支援するために、地域の準備と対応活動のためのツールとしての役割を果たすことを意図している。 • 地域がサイバー脅威の生み出すリスクを認識し、サイバーインシデント準備活動を組織し始めているため、地域のサイバーおよび緊急リスク管理に関する議論や提案も行う。 • 自然災害による緊急事態への備えや対応との類似点があるものの、サイバーセキュリティには、HDOsの緊急時計画内およびケア提供への影響に対応する責任を負うさまざまなステークホルダーグループ全体でのサイバーインシデント計画の特定の統合を必要とする方法でリスクを高める独自の特性がある。
スコープ	• 本プレイブックは、デバイスの機能に影響を及ぼす医療機器のサイバーセキュリティの問題に対する準備と対応に焦点を当てる • 特に懸念しているのは、患者の安全性への懸念を引き起こし、複数の患者に大規模な影響を及ぼす可能性がある脅威または脆弱性である。 • 本プレイブックは、デバイスの日常的なリスク管理の支援を目的とするものではない。

1.2. 事業実施方法

（１）３省２ＧＬに関する課題等調査･改定案の提案

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

医療機器のサイバーセキュリティ地域のインシデントの準備および対応のプレイブック バージョン2.0

	Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
対応等	 Figure 1. Incident Response Lifecyle • HDO医療機器サイバーインシデントの準備と対応として、対応のライフサイクルモデルを提示。 ➢ 準備段階:「インシデント対応能力[の確立]により、組織はインシデント対応準備を行うだけでなく、システム、ネットワークおよびアプリケーションの十分な安全性を保証することでインシデントを回避する 」 ➢ 検知と分析段階:「インシデント発生の有無、発生した場合は問題のタイプ、範囲および規模を[決定する] 」 ➢ 封じ込め、撲滅および復旧:封じ込めにより、インシデントがリソースを圧倒し、ダメージが拡大することを回避する; 撲滅により影響されたホストを修正する; そして復旧により「システムを通常運用に修正し、該当システムが正常に機能することを確認し、（当てはまる場合は）同様なインシデントが起きないように脆弱性を修正する」 ➢ インシデント後の活動:「…何が起きたのか、介入のために何を行ったのか、また介入結果をレビューすることで、セキュリティ対策とインシデント対応プロセスを改善する 」

コネクテッド医療機器のサイバーセキュリティ(ITSAP.00.132)(2021年11月)
（CYBER SECURITY FOR CONNECTED MEDICAL DEVICES**(ITSAP.00.132)**）
（カナダ）

1.2. 事業実施方法

（1）３省２ＧＬに関する課題等調査･改定案の提案

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

コネクテッド医療機器のサイバーセキュリティ(ITSAP.00.132)(2021年11月)

	CYBER SECURITY FOR CONNECTED MEDICAL DEVICES
対象	• コネクテッド医療機器の保護は、メーカー、医療機関および患者で共有される責任であるとし、多くのデバイスがクラウドベースであることから、医療機器と接続されているネットワークの間に相互依存性があり、クラウドサービスプロバイダー(CSPs)もこれらのデバイスのセキュリティについて責任を負うとする。 • 下記の表はメーカー、CSPsおよび医療機関にサイバー攻撃から医療機器をより適切に保護するために実装できる対策を示すものである。これらの対策は、Health Canada要件、規制および勧告に基づいている。なお詳しくはHealth Canadaの医療機器ページを参照のこと。

	内容
メーカーおよびCSPsへの推奨事項	• リスクを管理する: 従来のデバイスリスク管理プロセスと並行して、サイバーセキュリティ管理プロセスを作成する。リスクは一方のプロセスで軽減されるため、軽減が他方のプロセスに及ぼす影響も考慮する必要がある。例えば、セキュリティ制御なしでのデバイスへのネットワーク接続の追加は、物理的な安全性には影響を及ぼさないかもしれないが、サイバー脅威アクターのベクターとして機能する可能性がある。 • 設計を保護する: サイバーセキュリティ制御を開発プロセスの設計段階に組み込む。患者の安全に対する脅威が発生した場合は、手動によるデバイスのオーバーライドオプションを検討する。設計の選択は、デバイスの安全面を妨げることなくサイバーセキュリティを最大化すること。デバイスのライフサイクル計画を作成し、組織をサポートし、脆弱性の更新やパッチを行い、古くなったまたは廃止されたデバイスの使用を停止することを確保する。 • デバイスの確認と認証: デバイスのふるまいや性能が設計要件に準拠しているかテストして確認する。デバイスがサイバーセキュリティ要件を満たしていることを正確に実証する侵入テストおよび脆弱性スキャンなどのサイバーセキュリティテストを実施する。 • 展開されたデバイスの監視:医療機器に影響を及ぼす恐れがある脆弱性の追跡と報告を行う。定期的にパッチおよび更新を提供し、デバイスが安全で悪用可能な脆弱性がないようにする。設計段階でソフトウェア更新メカニズムを実装することを検討する。 • プラットフォームを保護する: クラウドプラットフォームには、顧客データおよびデバイスの保護に必要なセキュリティおよびプライバシー制御を実装する。例えば、堅牢なバックアッププロセスを設置し、全てのシステムおよびアプリケーションにMFAを適用して、完全性と安全性を確保する。クラウドインフラが不正侵入されると、デバイスまたはそれらのネットワークが感染する可能性がある。

1.2. 事業実施方法

（1）３省２ＧＬに関する課題等調査･改定案の提案

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

コネクテッド医療機器のサイバーセキュリティ(ITSAP.00.132)(2021年11月)

	内容
医療機関への推奨事項	• 境界を保護する: ファイアウォール、アンチウィルスおよびアンチマルウェアソフトウェアをインストールするなどのセキュリティ対策を全ネットワークに講じる。ネットワークをセグメント化し、ゲストネットワークおよび運用ネットワークを検討する。 • デバイスを保護する: パスフレーズや強力なパスワードでシステムおよびデバイスを保護する。デバイス及びアカウントごとに異なるパスフレーズやパスワードを使用する。アカウントやデバイスを多要素認証(MFA)で保護する。MFAを有効にすると、デバイスのロック解除やアカウントのサインインの際に2つ以上の認証要素が必要になる。また、機密情報を含む、または機密情報にアクセスするデバイスの暗号化も検討する。最後にパッチおよび更新が利用可能になったら適用し、OSが確実にアップデートされるようにする。 • フレームワークを開発する: データを保護し、PHIの使用を管理するためのセキュリティポリシーおよび手順を確立する。最小特権の原則を検討する。個人には、許可されたタスクに不可欠な一連のアクセス権限のみを提供する。 • セキュリティ文化の確立: スタッフのセキュリティおよびプライバシー訓練を行い、ユーザーにサイバー脅威が医療機器やそこに含まれるPHIに及ぶ恐れがある影響について教育する。組織のすべてのメンバーが機密情報を保護する責任があるという事実を強調する。Get Cyber Safeウェブサイトに有用な情報がある。 • アセットの管理: 情報は、ネットワークに接続されていないストレージサイト（外付けハードディスクまたはクラウドベースのバックアップサイトなど）にバックアップする。可能ならばサポートされていないデバイスを廃止する。サポートされていないデバイスはベンダーからのパッチや更新を受けられず、サイバー脅威に対して脆弱である。

コネクテッド医療機器の保護に関するガイダンス (2022年10月3日)
(Guidance on protecting connected medical devices)
（ NHS（英国） ）

1.2. 事業実施方法

（1）３省２ＧＬに関する課題等調査･改定案の提案

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

コネクテッド医療機器の保護に関するガイダンス (2022年10月4日)

	Guidance on protecting connected medical devices (4 October 2022)
対象	• このガイダンスは、非常に幅広い検討事項をカバーしている。各トラストや医療提供者は、この情報を解釈し、意味のある方法でセキュリティ対策を適用する必要がある。英国全体の医療提供者に同じ緩和策を適用することは適切ではないからである。
医療ネットワークで使用する医療デバイスの課題	• ハードウェアの依存やソフトウェアのドライバーの問題のため、オペレーティングシステム（OS）のアップグレード（例えば、Windows 7 からWindows 10への移行など）が不可能な場合がある。 • 医療機器は、ソフトウェアの複雑性、複数の接続手段を使用する可能性、他の領域の機器と比較すると機器を利用可能にしておくというプレッシャーが大きく、機器寿命が長く（10年以上）、病院のICT部門に課されるデバイスの更新に対するより大きな制限のため、より脆弱である可能性がある。 • 医療機器として、セキュリティ更新、パッチ、潜在的なウイルスシグネチャは、医療機器メーカーによって適切な評価がなされ、それらが医療機器に実装される前に安全性を確認する必要がある。これには、セキュリティ更新の公開後、3か月（あるいはそれ以上）の時間がかかる可能性がある。一部のパッチは、個別のパッチではなく、ソフトウェア全体のアップグレードとしてのみ実装されるため、さらに修正プロセスが遅れることがある • セキュリティの更新が公開された時に攻撃者によってレトロ分析がなされ（レトロ分析はレトロスペクティブ分析（retrospective analysis）の略であり、ネットワーク監視に適用される場合、過去のデータセットを再調査し、発生した、または発生した疑いのあるイベントに関する詳細情報を取得すること）、悪用可能な脆弱性が知られる可能性が高くなる。 • 最新のセキュリティ緩和策が存在しないと、脆弱性の影響が増加し、悪用の成功率が高くなるため、悪用の検知がより難しくなる. • 医療機器のメーカーによるサポート（サポート終了）は終了しているものの、機器が引き続き使用されている。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

コネクテッド医療機器の調達と展開に関するサイバーセキュリティガイダンス(2021年9月13日)

目的	• 英国のプロフェッショナル医療プロバイダーに対して、コネクテッド医療機器（CMDs）の調達と展開に関するサイバーセキュリティガイダンスを提供するもの • このガイダンスでは、CMDは、接続されたネットワーク機能のある医療機器として定義されている。この定義では、接続を行う技術手段は問わない。「医療機器」という用語はEU医療機器規則2017/745で与えられた意味を持つ。基本的に正式な医療目的で人間に使用される物理的な機器またはソフトウェアのことである。
対象	• CMDsの調達プロセスの一環としてのサイバー セキュリティ • CMDsの展開、維持、および廃棄におけるサイバーセキュリティ(調達方法に関係なく、サポートが不十分なデバイスを含む)。 • サポートが不十分なデバイスは、「レガシー」と呼ばれることがある。 • このガイダンスは、小型の「埋め込み型」などよりも大きな機器に適用される。これは、リスク軽減手段の多くが、低コストのデバイス (特にレガシーデバイス) や、ネットワークアーキテクチャをサポートする柔軟性のないデバイスには実行できないためである。
構成	• 次ページ以下6つの文書から構成される。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

コネクテッド医療機器のサイバーセキュリティのための推奨ガイダンス

	NHSデータセキュリティと保護ツールキット（NHS data security and protection toolkit） 2019-2020 V1.9.6, 21 June 2019
目的	• National Data Guardianの10のデータセキュリティ基準に対する組織のパフォーマンスを測定するための組織向けオンラインの自己評価ツール • ガイダンスの提供よりも要件に重点を置いている
利用場面	• National Data Guardianの10のデータセキュリティ基準に対するCMDセキュリティプロセスをチェックしたい時 • 機器の展開、維持、および廃棄に関連する時（調達には関連が低い）。
留意点	• CMDsの侵害から生じる可能性のある安全性の懸念よりも、データセキュリティの機密性に関するもの • 医療ITでは一般的であるため、CMDsについてはほとんど言及されていないものの、原則はCMDsに適用されることが多い。分離したシステムではなく、システムのコレクションを実行する際の課題をうまく考慮している。

	臨床リスク管理：ヘルスITシステムの展開および使用の適用（Clinical risk management: its application in the deployment and use of health IT systems） DCB0160 implementation guidance v4.2　2 May 2018 仕様: DCB0160 Specification v3.2.docx, 02May 2018
目的	• NHS内の医療ITシステムの展開、使用、保守または廃止を担当する医療機関によって、臨床リスク管理が確実に実行されるようにすること。一連の要件を提示し、役割、責任およびプロセスを強調する。 • 臨床リスク管理の適用を通じて医療ITシステムの安全性の責任者である医療機関の人々を対象
利用場面	• （CMDsを含む）医療ITシステムの展開、使用、維持、または廃止に臨床リスク管理を適用するための役割と責任の決定時。 • 機器からのリスクが、廃棄が必要とされる時期の判断。
留意点	• 管理機器のサイバーセキュリティ技術についてはアドバイスしていない • 「EU Regulations on Medical Devices 2017/745」および「ISO 14971:2012 Medical Devices: Application of Risk Management to Medical Devices」を参照している 。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

	NCSSセキュリティ設計原理: サーバーセキュリティシステムの設計ガイド（NCSC security design principles: guides for the design of cyber secure systems） 1.0 21 May 2019
目的	• 安全なネットワークおよび技術の設計と構築を行うこと
利用場面	• 機器の調達時。説明されている原則に従って、検討中の機器を配備できるという証拠を求めることができる場合。
留意点	• 医療のみではなく、クロスセクター向けであるため、原則をどのようにCMDsに適用するのか決定する必要がある • 医療提供者のIT環境が原則に則している場合、最も役立つ可能性があり、その場合、既存の環境と一致する方法で展開できる見込みがあるCMDsについてチェックを行うことができる

	医療業界のサイバーセキュリティ対策: 脅威の管理と患者の保護（Health industry cybersecurity practices: Managing threats and protecting patients）
目的	• ヘルスケアの幹部、開業医、プロバイダーおよび提供組織のサイバーセキュリティ意識を高めること • あらゆるタイプや規模の医療機関。管理および技術面を対象
利用場面	• CMDsの調達、展開、維持および廃棄時 • ヘルスケアに対するサイバーセキュリティの重要性を幹部や非技術系スタッフに納得してもらいたい時 • CMDs特定の要件を理解したい時
留意点	• 幹部や非技術系スタッフにヘルスケアに対するサーバーセキュリティの重要性を説得する場合は、本文の‘Cybersecurity attacks continue to affect the health care industry’（pp. 7-10, 13-27）を参照する。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査

	機器とヘルスITの共同セキュリティ計画（Device and health IT joint security plan） January 2019 (first publication)
目的	• 組織の規模や成熟度に関係なく、サイバーセキュリティを強化する医療機器メーカーおよびベヘルスケアITベンダーおよび医療提供者の支援 • 医療提供者、医療機器メーカーおよびベンダー– 管理および技術面を対象
利用場面	• 接続された医療機器を調達する際に考慮すべきサイバーセキュリティ要素を決定する時
留意点	• 文書全体を読むことは推奨しない • 顧客のセキュリティ文書化の推奨要素については、section VII: B.: vi: b) ‘Customer Security Documentation’ (i.e. Lines 492-527) & Appendix G • 医療提供者が調達時に検証する必要のあるセキュリティ設計要件の例についてはappendix E

	医療機器のサイバーセキュリティのポストマーケット管理（Postmarket management of cybersecurity in medical devices）
目的	• 市販および流通している医療機器の市販後のサイバーセキュリティの脆弱性を管理するためのFDAの推奨の明確化 • メーカーおよびFood and Drug Administration (FDA) スタッフ。管理&技術面、リーダーシップを対象
利用場面	• 接続された医療機器を調達する際に考慮すべき稼働中の機器に対するサイバーセキュリティサポートの望ましいレベルの決定時
留意点	• 文書の多くは米国特有のものであるため、上記セクションを選んで読むことを推奨する。この文脈では、必ずしも共通脆弱性評価システム（CVSS）を勧めるものではないが、この文書では、悪用の可能性を評価するためのツール例としてのみCVSSを引用している。FDAは、メーカーが機器を安全に設計および開発するのを支援するため、市販前の文書も発行している。 • 本文書はメーカーを対象としているため、医療提供者の関連性は、調達を検討している製品に十分なサイバーキュリティ対策が含まれているかどうかを判断することに役立つ。医療提供者は、メーカーにどの程度ガイダンスに沿っているかを問い合わせて、その回答を臨床リスク評価に知らせることができる。

病院のサイバーセキュリティのための調達ガイドライン
（2020年2月24日）
（Good practices for the security of healthcare services）
ENISA(欧州ネットワーク・情報セキュリティ機関）

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

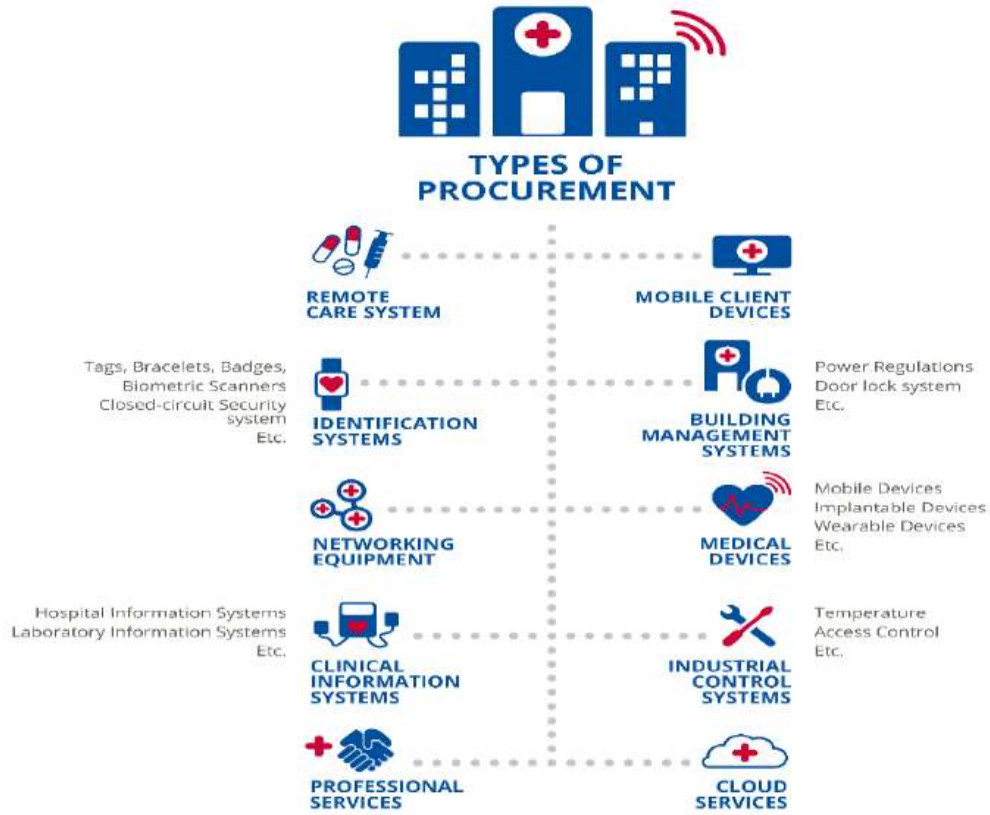
病院のサイバーセキュリティのための調達ガイドライン
ENISA(欧州ネットワーク・情報セキュリティ機関）（2020年2月24日)

	Good practices for the security of healthcare services
対象	• このレポートは、病院で技術職に就いている医療プロフェッショナル、つまり最高レベルの幹部であるCIO 、CISO、CTO、ITチームおよび医療機関の調達担当者を対象としている。 • このレポートは病院に製品を提供する医療機器メーカーにとっても興味深いものになる可能性がある。その場合、製品はこれらに限るものではないが、医療機器、臨床情報システム、ネットワーク、クラウドサービスなどが考えられる。これらのメーカーがサービスや製品を提供する際に病院がメーカーの期待するセキュリティ要件を知り、サービスや製品を提供する際に病院が期待しているセキュリティ要件を把握しており、それを証明する証拠を提供することができる。
目的	• 医療エコシステムの一部である病院に焦点を当てるものである。病院はアセット（インフラ、ソフトウェア、システムデバイスなど）の集合体と見なされ、サイバーセキュリティは、異なるコンポーネントすべてに明示的に対処される必要がある。 • 目的は、病院の医療プロフェッショナルに、サイバーセキュリティの目標を満たすため、調達プロセスを改善する方法に関するガイドラインを提供することである。 • これらのガイドラインでは、医療機関自体の優れた組織的プラクティスから、システムやサービス調達の際にサイバーセキュリティの「証拠」としてサプライヤーに要求する情報に至るまで複数のトピックをカバーしている。
スコープ	• スコープは、最も複雑で重要な医療機関であり、調達の主要ステークホルダーである病院である。また病院はリソース不足に直面することが多いため、本レポートは医療プロフェッショナルのための「ガイドブック」であることを目指している。 • 調達プロセスが非常に似ていると考えられるため、プラクティスや勧告の多くは、他の医療機関にとっても有益である。このレポートで提案されている調達ガイドラインは、サイバーセキュリティの影響を与える可能性がある医療機関の調達スコープ全体をカバーしている。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

■ 本ガイドラインで想定している調達対象である医療情報上の資源は、医療機器のほか、医療情報システム及び関連サービス、医療情報システムを格納するビル等におけるサービスなど幅広いものがふくまれている。

Figure 2: Types of procurement (asset taxonomy)



② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

各調達対象の概要

調達のタイプ	タイプの説明
臨床情報システム（CIS） Clinical information systems	あらゆる種類の医療向けソフトウェアの調達を含む: -病院情報システム＆電子医療記録 (HIS-EMR), -ラボラトリー情報管理システム(LIS), -放射線科情報システム(RIS), 画像保存通信システム(RIS-PACS), - 調剤 – 医薬品データベース, - ケア管理, - ダイエットソフトウェア, -医師向け電子化オーダーエントリー(CPOE), - ビッグデータ分析など。CISは、医療センターのIT部門の完全な管理下にある医療ビルまたはデータセンター施設に配置する必要がある。クラウドベースのシステムには独自のカテゴリーがある。
医療機器 Medical devices	病気の治療、管理または診断専用のハードウェアの一部: 放射線機器, 放射線治療, 核医学, 手術室またはインテンシブケア機器, 手術用ロボット, 電気医療機器, 輸液ポンプ, スパイロメータ, 医療用レーザー, 内視鏡機器など。患者埋め込み型デバイス (ホルター, ペースメーカー, インシュリンポンプ, 人工内耳, 脳刺激装置（brain stimulators）, 心臓除細動器,胃刺激装置（gastric stimulators）などを含む。または病院のITシステムと電子的に通信を行うウェアラブル機器(体外式EKGまたはホルター血圧計, グルコースモニターなど) 。
ネットワーク機器Network equipment	ネットワーク回線 (同軸、光ファイバー), ゲートウェイ,ルーター,スイッチ,ファイアウォール,VPNs, IPS, IDSなど。
リモートケアシステム Remote care systems	病院環境の外でケアを提供する施設または装置、特に現在「病院ベースの在宅ケアサービス」と呼ばれるもの。自宅で一人暮らしする高齢者の支援に使用するリモート通信「非常ボタン（press-for-help）」デバイスを含めることも可能。
モバイルクライアントデバイス Mobile client devices	病院のネットワークに直接接続されていない、健康支援または医療データ収集を提供するすべてのソフトウェア。例えば遠隔医療アプリなど。健康ウェアラブル機器は別のカテゴリーである。モバイルクライアントデバイスは、病院ネットワークへの接続のための定義されたプロトコルが必要である。
識別システム Identification systems	患者または医療関係者 (生体認証スキャナー、カードリーダーなど) を一意に識別し、ITシステムへのアクセスの識別および/または承認を保証するシステム。
ビル管理システム Building Management Systems	医療施設を収容できるあらゆるタイプの建造物。電線、水道、ガス、医療用ガス、家具など。ただし、「ネットワーク機器」の分類に含まれるネットワーク回線は除く。ビル管理システム（BMS）は、主に制御システムであるため、次の調達のタイプに含まれる。
産業用制御システムIndustrial control systems	電力調整システム、ドアロックシステム、閉回路セキュリティ システム、HVACシステム、警報システム、水道、暖房、補助電源装置、セキュリティアクセス、エレベーター、消火などセンターの物理的側面すべてを制御するシステム。現在、これらすべてのシステムの制御は、ソフトウェアシステムであるビル管理システム (BMS) により管理されている。BMSは、個別に取得することも、建物の改修プロジェクトの一部として取得することも可能。
プロフェッショナルサービスProfessional services	外注の有無を問わず、専門家や企業から提供されるあらゆるサービス: 医療サービス, 運輸, 経理, エンジニアリング, IT, 法務, メンテナンス, 清掃, ケータリングなど。
クラウドサービスCloud services	医療センターのIT部門の完全な管理下にある医療ビルやデータセンター施設に配置されていないCISその他の情報システム。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

- ■ 本ガイドラインでは、セキュリティ管理のためのグッドプラクティスが提示されているが、各グッドプラクティスが該当する資源や関連する脅威が整理されている。
- ■ 事業者は担当する資源に該当するグッドプラクティスを参照することで医療機関に対応することになる。

	関連する調達のタイプ										関連する脅威				
グッドプラクティス（GP）	臨床情報システム（CIS）	医療機器	ネットワーク機器	リモートケアシステム・リモートクライアントデバイス	モバイルクライアントデバイス	識別システム	ビル管理システム	産業用制御システム	プロフェッショナルサービス	クラウドサービス	悪意ある行為	サプライチェーン障害	システム障害	人的ミス	自然現象・災害
GP 1. 調達へのIT部門の関与	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
GP 2. 脆弱性の特定と管理プロセスの実装	○	○	○	○	○	○		○		○	○	○	○	○	○
GP 3. ハードウェアとソフトウェアの更新に関するポリシー策定	○	○	○	○	○	○		○		○	○	○	○		
GP 4. 無線通信のセキュリティ管理強化		○		○		○				○	○			○	
GP 5. テストポリシーの確立	○	○	○	○	○	○	○	○		○	○	○		○	
GP 6.事業継続計画の確立	○	○	○	○	○	○		○		○	○	○	○		
GP 7. 相互運用性の問題の考慮	○	○		○	○	○		○		○	○		○	○	
GP 8. すべてのコンポーネントのテストの有効化	○	○	○	○	○	○	○	○		○	○	○	○	○	
GP 9. 監査とロギングの許可		○		○	○	○		○			○	○	○		
GP 10.保管中および転送中の機密個人データの暗号化	○	○	○	○	○	○		○		○	○	○	○		
GP11. 調達プロセスの一環としてリスク評価の実施	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
GP 12. ネットワーク、ハードウェア、およびライセンス要件の事前計画	○		○			○		○				○	○	○	○
GP 13.調達製品またはサービスに関わる脅威の特定	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	関連する調達のタイプ										関連する脅威				
グッドプラクティス（GP）	臨床情報システム（CIS）	医療機器	ネットワーク機器	リモートケアシステム・リモートクライアントデバイス	モバイルクライアントデバイス	識別システム	ビル管理システム	産業用制御システム	プロフェッショナルサービス	クラウドサービス	悪意ある行為	サプライチェーン障害	システム障害	人的ミス	自然現象・災害
GP 14. ネットワークの分離	○	○	○	○	○	○		○		○	○	○	○		
GP 15. ネットワーク要件の決定	○		○	○	○	○		○		○		○	○		○
GP 16. サプライヤーの適格基準の確立	○	○	○	○	○	○		○		○	○	○	○		
GP 17. クラウドサービス調達のための専用 RfPの作成										○	○	○			
GP 18. サイバーセキュリティ認証の要求	○	○	○	○	○	○		○		○	○	○	○		
GP 19. 新製品またはサービスのデータ保護影響評価の実施	○	○	○	○	○	○			○	○	○			○	
GP 20.レガシーシステム/マシンの接続維持のためのゲートウェイ設定		○		○	○	○		○			○	○	○		
GP 21. 組織のセキュリティ慣行に関するサイバーセキュリティトレーニングの提供（スタッフおよび外部コンサルタント対象）	○	○	○	○	○	○	○	○	○	○	○			○	
GP 22.インシデント対応計画の策定	○	○	○	○	○	○		○		○	○	○	○		
GP 23. インシデント管理へのベンダー/メーカーの関与	○	○	○	○	○	○		○		○	○	○	○		
GP 24. すべての機器の保守作業のスケジュールと監視	○	○	○	○	○	○	○	○		○			○	○	○
GP 25. リモートアクセスを最小限に抑えて管理	○	○	○	○	○	○		○		○	○	○	○	○	
GP 26. すべてのコンポーネントにパッチを適用	○	○	○	○	○	○		○		○	○	○	○		

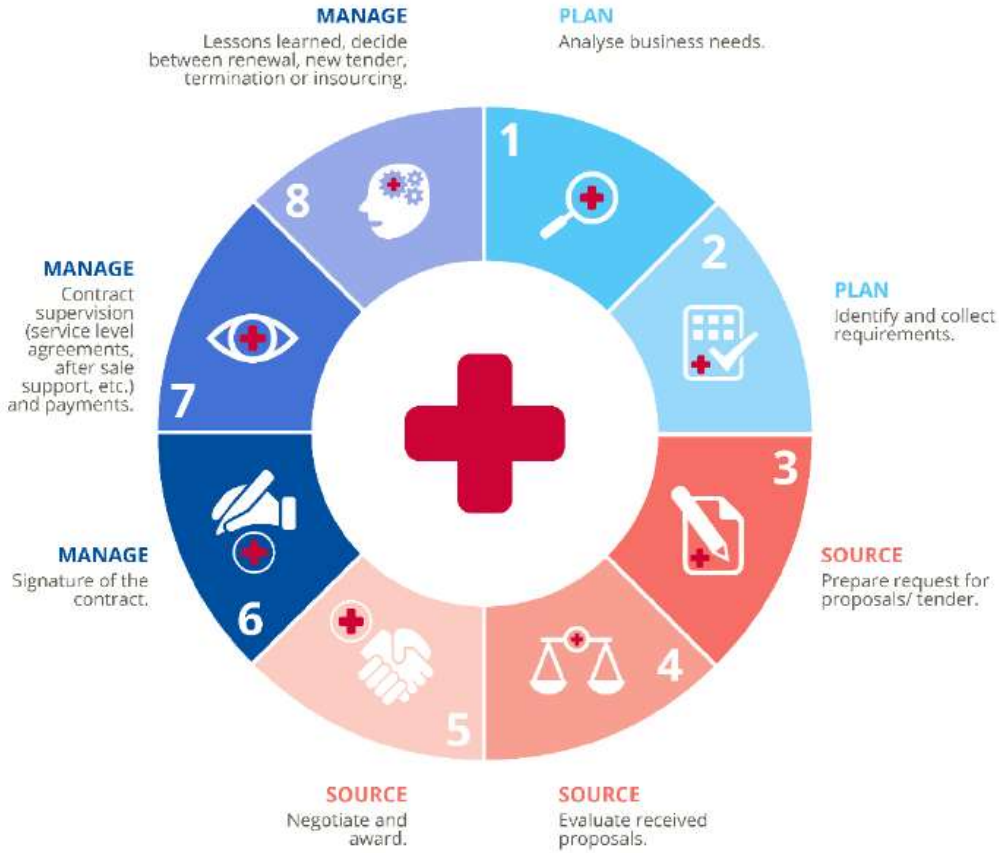
② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

グッドプラクティス（GP）	関連する調達のタイプ										関連する脅威				
	臨床情報システム（CIS）	医療機器	ネットワーク機器	リモートケアシステム・リモートクライアントデバイス	モバイルクライアントデバイス	識別システム	ビル管理システム	産業用制御システム	プロフェッショナルサービス	クラウドサービス	悪意ある行為	サプライチェーン障害	システム障害	人的ミス	自然現象・災害
GP 27. スタッフのサイバーセキュリティ意識向上	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
GP 28. 資産インベントリと構成管理の実行	○	○	○	○	○	○					○		○	○	
GP 29. 医療機器施設専用のアクセス制御メカニズムを確立		○				○	○				○			○	
GP 30. 侵入テストのスケジュール（頻繁、またはアーキテクチャ/システムの変更後）	○	○	○	○	○	○		○		○	○	○	○		

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

- 本ガイドラインでは、セキュリティ管理のためのグッドプラクティス（GP）が提示されており、その内容を以下に示す。
- GPは全般、計画フェーズ、ソース導入フェーズ、管理フェーズなどごとに30のものが示されている。

Figure 1: Procurement process lifecycle for hospitals



② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 1. 調達へのIT部門の関与	GP 2. 脆弱性の特定と管理プロセスの実装
	調達のさまざまな段階でIT部門が関与することで、サイバーセキュリティの側面に関する専門知識が考慮されるようにする	新しい製品またはサービスを調達の前に脆弱性が考慮されていること、および既存の製品/サービスの脆弱性がライフサイクル全体にわたって監視されていることを確認する
例/証拠	● サイバーセキュリティ要件の起草にITスタッフを関与させる ● 新規調達を計画する際にIT部門に相談し、サイバーセキュリティの考慮事項を統合する ● サイバーセキュリティ要件をRfPの一環とする ● 医療機関の調達ポリシーの一環として、すべてのシステム、サービス、またはデバイスの取得を行う委員会にIT部門を含める必要がある	● ICT品/サービスの脆弱性を監視し、対処する脆弱性管理プロセスを確立する ● 既存の脆弱性に関する情報は、メーカーまたはNIST脆弱性データベースなどの公開情報源から入手可能27 ● 新たに特定された脆弱性に対処し、RFP/契約にタイムリーなパッチ適用により脆弱性に対処するサプライヤーの責任に関する規定を含める ● 医療機関は、取得したシステムまたは製品で使用される部品表（BOM）の要件を含めることを検討する場合がある。これは、公開されている脆弱性情報に基づき、医療機関のインフラ内の脆弱なシステムの追跡に役立つ。
関連する調達のタイプ	すべて	臨床情報システム，医療機器，ネットワーク機器，リモートケアシステム，モバイルクライアント機器，識別システム，産業用制御システム，クラウドサービス
関連する脅威	すべて	すべて

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 3. ハードウェアとソフトウェアの更新に関するポリシーを策定する	GP 4. 無線通信のセキュリティ管理の強化
	OSとソフトウェアに最新のパッチが適用され、ウイルス対策ソフトウェアが更新されるように更新ポリシーを作成する	病院のWi-Fiネットワークへのアクセスを制限し、厳密に管理する。接続されているデバイスの数を監視し、医療機器の場合は検証して制限する必要がある。 許可されていない担当者は Wi-Fiにアクセスできないようにする。
例/証拠	● インストールされているSWおよびHWのバージョンを含む、現在実行中のすべてのSW およびHW のレジストリ/IT アセットインベントリを作成する ● 新しいパッチがリリースされていないか定期的に調査する ● 新規リリースなどがあった場合、CISO/ISOに通知する ● 全マシンへのパッチ適用を決定する前に、いくつかのマシンで提案されたパッチをテストする ● ネットワークのセグメントごとに、パッチ適用に最適なタイミングを決定する ● パッチの適用できないマシンの回避策を決定する ● アップデート手順を文書化する ● 第三者プロバイダーの関与を定義する ● パッチを適用したマシンが期待どおりに動作しない場合に状況を元に戻すために実行する行動を定義する	● デフォルトとして、強力なWi-Fiパスワード（パスワードが変更された頻度のログを保持する）。ポリシーとリンクする必要がある ● 2ファクタ認証を義務化する ● 無線通信を必要とする医療機器には、厳格なアクセス制御と専用ポリシーをサポートする専用の無線ネットワークがある ● 公共デバイスからのアクセスは禁止する
関連する調達のタイプ	医療機器, 臨床情報システム, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス	医療機器, リモートクライアントデバイス, 識別システム, クラウドサービス
関連する脅威	悪意ある行為, サプライチェーン障害, システム障害	悪意ある行為, 人的ミス

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 5. テストポリシーの確立	GP 6.事業継続計画の確立
	医療機関は、製品/システムの種類に応じて、取得した製品またはシステムに対して実行するセキュリティテストの最小限のセットを確立する必要がある。また、新たに入手した製品または構成された製品は、実際にインストールされた環境で侵入テストを受ける必要があることに注意することも重要である。 同様に、実行される修復行動は、実際の環境の運用パラメーターに沿ったものである必要がある。	システム障害が病院の中核サービスを混乱させる可能性がある場合は常に事業継続計画を確立する必要がある。そのような場合には、サプライヤーの役割を明確に定義する必要がある。
例/証拠	● あらゆる種類の製品またはシステムに対して一連のセキュリティテストとさまざまな閾値が医療機関により定義されている ● テストポリシーは、調達の全段階をカバーし、定期的なセキュリティ監査と、既に運用環境にあるシステムの侵入テストを含む場合がある ● テストおよび閾値はサプライヤーに伝達され、RfPの一環である ● 受け入れ基準は、調達の最終決定前にセキュリティテストに基づき定義されている ● RfP/契約には、本番環境のシステムのセキュリティテスト後の調査結果に対処するため、特定のサプライヤーの責任が記載されている ● テストポリシーはすべてCISOによって改訂、承認される ● 一部のシステムは、負荷に応じて課金される。 コストがかかる可能性のある負荷テストを実行する前に、プロバイダーと話し合う ● テスト中にサーバー、通信システムまたは医療機器が停止した場合の緊急時対応計画を常に準備しておく ● テスト負荷によって医療機器または医療システムが永続的に停止する可能性がある場合は、メンテナンス計画にデバイス/システムのリセットと再起動が含まれているかどうかを確認する	● RfPから、サービス中断の際のサプライヤーの支援サービスがどうなるかを明確にする必要がある。サプライヤーのサービスのコスト（保証中および保証後）および予想される応答時間(SLA) を含む。 ● 事業継続を計画する際には、さまざまな災害シナリオを考慮する必要があり、事業継続戦略にサプライヤーの支援を含む場合は、RFPに明確に記載し、最終契約に含める必要がある。 ● ビジネス継続性サービスのコストとサービスレベル要件は、RFP プロセス中に明確にする必要がある ● 新たに取得したシステムの障害により、病院の中核サービスを提供する能力が危険にさらされる可能性がある場合、事業継続計画は、組織が最悪の状況下で重要なサービスを利用できるために必要な戦略（デバイス交換、または障害のあるコンポーネントの交換)、手段や手順を確立する必要がある
関連する調達のタイプ	臨床情報システム（CIS）, 医療機器, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, ビル管理システム, 産業用制御システム, クラウドサービス	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, システム障害, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 7. 相互運用性の問題の考慮	GP 8. すべてのコンポーネントのテストの有効化
	相互運用性は、医療機関にとって最も重要なサイバーセキュリティリスクのひとつである。病院の ITエコシステムは、医療機器、ネットワーク機器、リモートケアシステムなどのさまざまなコンポーネントで構成されている。これらのコンポーネントの一部は既に存在しており（レガシー IT)、新しいコンポーネントと接続することにより、セキュリティギャップが生じる可能性がある。	情報システムは、約束されたものを提供することを保証するため、徹底的にテストする必要がある: 使いやすさの検証、負荷がかかった状態での結果の正確さのチェック、およびセキュリティ上の欠陥のチェック（弱いパスワードポリシー, SQLインジェクション)。テストは、テスト中の監視だけでなく、調達要件でもあること。テストはテストポリシーに沿ったものである必要がある。
例/証拠	● サプライヤーは、提案されたソリューションが既存のシステムに統合されている方法を示す必要がある。必要に応じて、統合方法を説明する技術文書をオファーに含める必要がある ● サプライヤーは、データ損失を防ぐために、(少なくとも事前に定義された期間)通信を監視することを確認する必要もある	● サプライヤーは、提供されるデバイス/システムのテストシナリオを含める必要がある。テストの実施方法や調整方法を説明すること。各テストのベンチマークを定義する ● テストの報告は秘密裏に共有可能である ● テスト中にサーバー、通信システムまたは医療機器が停止した場合に備えて、常に緊急時対応計画を準備する ● テスト負荷により、医療機器または医療システムが永続的に停止する可能性がある場合は、メンテナンス計画にデバイス/システムのリセットと再起動が含まれているかどうかを確認する
関連する調達のタイプ	臨床情報システム（CIS）, 医療機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス	臨床情報システム（CIS）, 医療機器, リモートクライアントデバイス, 識別システム, クラウドサービス, 産業用制御システム, リモートケアシステム, ビル管理システム, モバイルクライアントデバイス
関連する脅威	システム障害, 人的ミス, 悪意ある行為	悪意ある行為, 人的ミス, システム障害, サプライチェーン障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 9. 監査とロギングの許可	GP 10.保管中および転送中の機密個人データの暗号化
	ログは、セキュリティのセキュア-テスト-分析-改善-戦略で重要部分である。システムが遅かれ早かれ危険にさらされると想定した場合、ログは、攻撃者がシステムにアクセスした方法の追跡に使用できる最も有用なツールのひとつである。また情報がどの程度の侵害されたのかを評価することもできる。ログを安全に保つことは、セキュリティの最も重要なタスクのひとつではあるものの、これがなくとも既に実装されているセキュリティが損なわれることはない。	少なくともGDPRのArticle 9の個人データの特別なカテゴリーを処理するシステム、サービスまたはデバイスのポリシーを定義する。これらのタイプの情報は常に暗号化する必要がある（保存または送信時）。他の個人データのカテゴリーについては、該当データが組織を離れる際に暗号化が必要である。注意すること。多くの場合、この要件はシステム、サービス、またはデバイスのサプライヤーではなく、組織自体に課せられることに注意すること。代替サイトに保管するために、データが外部ディスクドライブにコピーされる場合がある。この場合は、暗号化メカニズムの提供は組織の責任である。 システム間の通信プロセスとしてデータが組織の施設を離れなければならない場合(データ結果を離れた処理センターに送付する)、暗号化された安全な通信プロトコルの提供はサプライヤーの責任である
例/証拠	● 安全なCentral Logging Systemを作成し、ログのコピーを保持して、これらのファイルをオフサイトの安全な場所に安全に保管できるようにする ● 外部のログシステムを維持することも便利である。例えば、クラッシュして応答しないサーバーがある場合は、集中管理された syslogサーバーでカーネル エラーログを確認できる ● サプライヤーは監査目的でログへのアクセスを可能にできる	● 保存時または送信時にデータの暗号化が必要かどうかを定義する。この要件をRfPに含める。サプライヤーが提供するオファーで、アルゴリズムと暗号化方法を探求する。この段階で、Data Protection Officerに通知する必要がある ● サプライヤーは保管中のデータ、転送中のデータ、およびさまざまな種類のデータの暗号方法を明確に定義する(機微な健康データi vs 個人データ) ● 提供されるデータの暗号化が不可のデバイスもある。デバイスとネットワーク間には、暗号化のための適切なゲートウェイを用意する必要がある
関連する調達のタイプ	医療機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, サプライチェーン障害, システム障害	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP11. 調達プロセスの一環としてリスク評価の実施	GP 12. ネットワーク、ハードウェア、およびライセンス要件の事前計画
	調達プロセスの一環として、医療機関はリスク評価を行う必要がある。	新しいシステム、サービスまたはデバイスまたはコンポーネントがサードパーティソフトウェアを必要とするか、システムが現在のソフトウェアを使用するものの、追加ライセンスが必要かどうかを評価する。RFP の際にサプライヤーから収集したハードウェアの要件(ディスク容量,帯域, CPU機能,メモリー) を現在および既に計画されている容量使用量と照合し、新しいシステムに対応するため、インストール前に追加のアップグレードおよび/または購入の要否を判断する
例/証拠	● 医療機関は、新たな調達プロセスの前に新たな入手によるITセキュリティリスクへの影響を評価する必要がある(e.g. 新しいリスク, 既存のリスクの増加/減少の可能性や影響) ● システム、サービスまたはデバイス調達に関わるリスクの特定後は、それらの対処戦略を設計し、それぞれの調達に統合する必要がある(予算変更、仕様変更などを含む.) ● リスクの特定は調達プロセスの初期に行う必要がある ● 計画された調達に関連して、ITセキュリティ リスクが大幅に増加した場合、調達計画のキャンセルまたは代替ソリューションを検討する必要がある	● 一部のデバイスには、ライセンス不要で独自のソフトウェアが付属する場合とまた同じ企業から追加ソフトウェアを取得する必要がある場合がある。法務部門にライセンスの条件とそのスコープを確認してもらう ● ソフトウェアが提供された状態で直接使用できるか、あるいは設定が必要かどうかを調査する ● ライセンス更新の要否、および更新がカバーされているかどうかをチェックする ● データセンターに新しいサーバーを収容できるスペースの有無を確認する ● 外部 ITプロバイダーの一部は、データセンター内にスペースが必要な場合がある。予期せぬ今後のニーズに備えて、スペースを予約する(および IPS/IDSサーバーなど) ● 既存の電源システムに十分な容量があることを確認する（補助電源装置を含む）。新規デバイス用のプラグが不足していることが多い ● 新規デバイスのネットワークへの物理的な接続方法を計画する
関連する調達のタイプ	すべて	臨床情報システム（CIS）, ネットワーク機器, 識別システム, 産業用制御システム
関連する脅威	すべて	サプライチェーン障害, システム障害, 自然現象, 人的ミス

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 13.調達製品またはサービスに関わる脅威の特定	GP 14. ネットワークの分離
	新たなシステム、サービスまたはサービスの調達計画の際は、サイバーセキュリティの脅威を検討する必要があり、脅威の特定は調達ライフサイクルで継続する必要がある。	時にはネットワークに接続されたデバイス固有の脆弱性が軽減されない場合がある:例えば、Windows NTを使用するレガシーデバイスを新しいOSにアップデートすることはできない。これらのデバイスから既存のITインフラを保護するため、補完コントロールを実装する必要がある。ネットワークに接続された全デバイスをネットワークの残りの部分から分離することが重要である。そのためにはネットワークセグメンテーションを実装する。ネットワークセグメンテーションにより、ネットワークのトラフィックは分離および/またはフィルタリングして、ネットワークゾーン間のアクセスを制限および/または防止できる。
例/証拠	● 構造化されたアプローチを使用し、関連する脅威を正確に特定する ● 新規調達に関わる脅威の評価の際には、関連する全ステークホルダーを含める ● 新しい製品またはサービスの調達後、該当する場合は、医療機関の脅威モデリングプロセスのアップデートを行う必要がある	● In the RfPの中で、病院は現在のネットワークトポロジーのおおまかな概要を提供しり、潜在的なベンダーに、ネットワーク分離を考慮した新しいトポロジーを求める必要がある ● ベンダーは、接続されている医療機器に基づいて、ネットワークのセキュリティ境界の情報を提供する必要がある。この情報はRfPに含まれること
関連する調達のタイプ	すべて	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	すべて	時にはネットワークに接続されたデバイス固有の脆弱性が軽減されない場合がある:例えば、Windows NTを使用するレガシーデバイスを新しいOSにアップデートすることはできない。これらのデバイスから既存のITインフラを保護するため、補完コントロールを実装する必要がある。ネットワークに接続された全デバイスをネットワークの残りの部分から分離することが重要である。そのためにはネットワークセグメンテーションを実装する。ネットワークセグメンテーションにより、ネットワークのトラフィックは分離および/またはフィルタリングして、ネットワークゾーン間のアクセスを制限および/または防止できる。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 15. ネットワーク要件の決定	GP 16. サプライヤーの適格基準の確立
	病院のプロフェッショナルは、ネットワークとコンポーネントのトポロジー（デバイスやコンポーネントがシステムに接続されている方法）を作成後、相互運用性の確保や、ギャップを回避するため、さまざまなコンポーネントごとにセキュリティ要件をリストする必要がある（帯域要件など）。 病院は事前に、ネットワーク機器に必要なセキュリティ機能を知る必要がある。	セキュリティベースライン要件を確立し、サプライヤー選択の際に資格基準に変換する。
例/証拠	● スイッチを確認する。新しいサーバーとデバイスを接続するための空き容量があることを確認する ● 必要に応じて、バーチャルネットワークを作成する ● コンセント数は十分か、またはデバイスは無線通信を行うのか？ ● 帯域は十分か？新規回線を設置するかどうか、またはワイヤレスルーターに十分な速度と機能があるかどうかを検証する ● 一部のデバイスはTCP/IP以外のプロトコルを使用する場合がある。ネットワークの通信に特別なゲートウェイが必要かどうかをチェックする ● デバイスの一部はデフォルトで暗号通信を行わないものもある。どのデバイスに暗号化機能があるか、またはデータがネットワークに入る前にゲートウェイを介して自分で提供する必要があるかをチェックする ● デバイスがサードパーティーと予期せぬ通信を開始しないことを確認する ● 外部デバイスは専用エントリーゲートウェイまたはファイアウォールが必要か？ ● 使用するポートの確認と文書化を行う ● 主要通信回路障害時に備えて、冗長化したトポロジーを設計する	● 調達の目的で、医療機関は、PC、OS、通信プロトコル(HTTPは不許可など)、認証メカニズム(シングルファクタ認証または2ファクタ認証など)、データベース、暗号化などの共通コンポーネントのベースラインを用意する必要がある。ベースラインに準拠していないメーカーは調達プロセスに参加できない ● さまざまな種類の調達について、サプライヤーの最低限のセキュリティ認証要件を決定する（例えばセキュリティサービスの提供, ISO 27001の認定サプライヤーであること など） ● RFP文書の一部としてセキュリティベースラインを含める(適格基準)
関連する調達のタイプ	臨床情報システム（CIS）, ネットワーク機器, 識別システム, 産業用制御システム, クラウドサービス, リモートケアシステム, モバイルクライアントデバイス	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	サプライチェーン障害, システム障害, 自然現象	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 17. クラウドサービス調達のための専用 RfPの作成	GP 18. サイバーセキュリティ認証の要求
	クラウドサービスを調達する際、特に病院の場合は、規制およびポリシー要件を考慮して、特定の RfP を導入する必要がある。いくつかの加盟国（MS）では、クラウドサービスを購入する際の確認点について、ガイドラインを発行している。	医療機関は、サイバーセキュリティスキーム/標準に対して認定されたアセットの調達を優先する必要がある。
例/証拠	● クラウドサービスプロバイダー（CSP)は、病院データの保存先を具体的に記載する必要がある。病院は、機微情報がEU国境内に留まることを要求する必要がある（これにより EUデータ保護規制が適用される)。また使用する暗号化メカニズムの説明も必要である ● CSPは、インシデントが発生した場合の冗長性と業務の継続性を証明する。またインシデント報告のプロセスを共有する必要がある(NIS Directiveの要件に基づく) ● CSPは監査と侵入テストの結果を病院と内密に共有することができる	● 調達された医療機器はthe Medical Devices Regulationに準拠する必要がある(調達には、メーカーに証拠の提供を求める必要がある) ● 調達は、該当する場合、EUサイバーセキュリティ認証スキームについて認証された製品を優先する必要がある ● クラウドサービスなどの外部サービスは、サービスの提供者がISO 27001/ ISO 27018/ CCMなどのセキュリティ認証を受けていることが重要である ● 認証を見る際は、認証のスコープや契約するサービスのスコープを理解することが重要である。クラウドサービスのプロバイダーは、サービスの一部（カスタマーサポートサービス）で ISO 27001 認定を受けている場合があるが、組織にとってより重要な他のサービスについては認定されていない ● 医療機関は、オンラインで入手できる場合、調査結果を詳述した認証局からの完全な報告に付属するベンダー証明書を確認する必要がある。通常、報告書のスコープの章で範囲内の各サービスについて詳しく説明している。これらの文書は提供サービスの保証のために提供される
関連する調達のタイプ	クラウドサービス	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, サプライチェーン障害	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 19. 新製品またはサービスのデータ保護影響評価の実施	GP 20.レガシーシステム/マシンの接続を維持のためのゲートウェイ設定
	新規サービスまたはサービス調達の際は、データ保護とコンプライアンス問題の影響を評価する。	脆弱性が知られているOSを使用しなければならない医療機器は、常にネットワークから切り離して維持する必要がある。代わりにこのデバイスと通信してデータを取得し、それをネットワークに渡し、暗号化を実装する PC ゲートウェイを開発する必要がある。 ネットワーク全体のセグメントがこのゲートウェイを通して通信する必要がある場合もある（例えば研究所のすべての機器など）。 このゲートウェイは、これらのグループ内で問題が発生した場合に優れたフロンティア制御を提供する。ゲートウェイをブロックすると、上流のすべてのマシンが隔離される。1つまたは2つのCIS サーバーを除いて、セグメント内のマシンがネットワークの残りの部分と通信する必要がない場合は、常にこの勧告に従うこと。
例/証拠	● 検討中のシステム、デバイスまたはサービスが大量の特別なカテゴリーの情報を処理する際はいつでもデータ保護インパクト分析（data protection impact assessment (DPIA)）を実施する必要がある ● 特定のサプライヤーが個人データを処理する必要性を文書化し、該当データは必要なものに限定する ● 新しい製品/システムで処理する必要があるデータの種類を完全に文書化し、RFP要件に制限を適用する	● 医療機器には、ハードウェアまたはその他の要件により、アップグレードが許されていないものがある(例えば、超音波機器の一部は古いバージョンのWindowsで動作する場合がある) ● 医療機器のライフスパンは長い。マシンと通信するためのドライバは新しいバージョンのOSでは利用できない可能性があり、マシン内のデータにアクセスするために古いバージョンのOSを維持する必要がある ● コミュニティセンターやデイケアセンターでは、病院用としては廃棄となったデバイスを使用している可能性がある。これらのセンターのようにそれほど要求の厳しくない環境では、まだ役立つ
関連する調達のタイプ	臨床情報システム（CIS）, 医療機器, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, プロフェッショナルサービス, クラウドサービス	医療機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム
関連する脅威	悪意ある行為, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 21. 組織のセキュリティ慣行に関するサイバーセキュリティトレーニングの提供（スタッフおよび外部コンサルタント対象）	GP 22.インシデント対応計画の策定
	施設内で作業する内部スタッフまたは外部の請負業者/コンサルタントが、医療機関のセキュリティ慣行について十分なトレーニングを受けているようにする。	新たに入手した製品またはシステムをカバーするインシデント対応計画を開発する。
例/証拠	● 技術スタッフは、運用や保守を行うシステムに関わるセキュリティトレーニングを定期的に受ける ● 技術スタッフは、新たに調達した製品を操作または保守する必要がある場合、特別トレーニングを受ける ● 一般スタッフ (医師, 看護スタッフなど)は組織の情報セキュリティポリシーと手順に関するトレーニングを受ける必要がある ● オンプレミスでの作業する契約を結んでいる外部の請負業者/コンサルタントは、医療機関のセキュリティポリシーとその機能に関連するセキュリティ慣行について必須トレーニングを受ける	● 組織のスタッフがサイバーセキュリティインシデント発生時に実施するべき対応計画を開発し、各自の役割や責任を確立する ● ソフトウェアのパッチやウイルス対策ソフトが最新状態であることを保つことを含む重要なアップデートが実装されるようにする ● インシデントに備えて、病院とサプライヤーを含む適切な通信チャネルを決定する ● 全製品/システムのインシデント対応計画の定期テストを実施し、新たに取得した製品/システムに対して少なくとも1回はインシデント対応計画テストを実施する
関連する調達のタイプ	すべて	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 23. インシデント管理へのベンダー/メーカーの関与	GP 24. すべての機器の保守作業のスケジュールと監視
	システムおよびデバイスは、不正確なコーディング、不適切な取り扱い、または単なる消耗により最終的には故障する。RfPから、これらの不測の事態におけるサプライヤーの支援サービス、そのサービスの費用（最初の年とその後)および予想される応答時間（SLA）を明確にする必要がある。	HWおよび SWアップデートポリシーに基づき、ビル管理システムを構成するものを含む異なるすべてのタイプの機器に保守作業を実施する。保守では、機器の適切なレベルの機能を確保し、更新/パッチなどを決定する必要がある。
例/証拠	● サプライヤーは、オファーにインシデント処理の際の役割の詳細を含める必要がある（誰の責任かにもよる） ● サプライヤーは、規制上の義務を考慮して、病院に報告する必要があるケースをオファーに含める必要がある ● 他の国家機関、すなわちセクター固有の国家CSIRTの関与について説明し、公式化する必要がある	● サプライヤーからのオファーには保守スケジュールの目安が含まれている必要がある。病院のIT専門家の役割の説明する必要がある（操作の監視） ● 保守のログ ● 保守操作でパッチまたは更新の必要性が明らかになった場合は、別の手順をトリガーする必要がある
関連する調達のタイプ	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス	臨床情報システム（CIS）, ネットワーク機器, 医療機器, ビル管理システム, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, サプライチェーン障害, システム障害	人的ミス, システム障害, 自然災害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 25. リモートアクセスを最小限に抑えて管理	GP 26. すべてのコンポーネントにパッチを適用
	すべてのサプライヤーは、病院のネットワークにアクセスするためのプロトコルを定義する必要がある。アクセスは事前に定義され、承認や監視が行われる必要がある。緊急事態の際には、特定のアラートを発生させること。ポリシーは、プロバイダーがデバイスにアクセスできる時や方法を含むこと。リモートアクセスは保守目的のみとする。このプロセスで個人情報を取得することは一切ない。システム外に出てサプライヤーが処理できる情報は、契約で明確に定義する必要がある。ルーターおよびゲートウェイは、サプライヤーとの外部通信が制御する必要のあるデバイスのみに制限されるように構成する必要がある。	パッチの適用は、病院がサプライヤーに設定する基本的な要件である。パッチの適用は、任意の期間に行うことはできないが、従うべき手順がある。パッチ適用のための情報はRfPに含める必要がある。
例/証拠	● すべてのネットワークコンポーネントと医療機器の構成ファイルを確認する ● PET/CATスキャナーおよびMRI装置 にアクセスするリモートアクセスに2ファクタ認証を有効にする ● VPN経由のリモートアクセスのみを有効にする ● アクセス制御の実施: サプライヤーは、提供されたデバイスでのみ事前に設定された期間にアクセスできる必要がある ● これらの条項は、ベンダーのオファーで説明する必要がある	● オファー中のサプライヤーは、パッチ適用の手順を説明する必要がある。また、このプロセスに病院のIT専門家の役割も含める必要がある。本プロセスはコンポーネントごとに明確化すること ● サプライヤーは、パッチが予想通りに機能しなかった際に備えて冗長化計画も提示する。ロールバック手順も整備する必要がある ● 提案されたパッチは、一部のマシンでテストを実施した後に全マシンへの適用を決定する。テスト結果は病院のIT専門家に提供する必要がある
関連する調達のタイプ	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, サプライチェーン障害, システム障害, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 27. スタッフのサイバーセキュリティ認識の向上	GP 28. 資産インベントリと構成管理の実行
	スタッフが、新たに入手した製品またはサービスに伴うサイバーセキュリティリスクを認識するようにする。	コンポーネントがICT環境に追加または削除された際にITインベントリが適切にアップデートされ、ICTコンポーネントのベースラインセキュリティ構成が存在し、適切に管理されているようにする。
例/証拠	● 新たに調達した製品やサービスを含めるため、定期的または臨時の意識向上キャンペーンを適応させる ● 新たに調達した製品やサービスに関わる意識向上キャンペーンを実施する ● 新たに調達された製品またはサービスが臨床スタッフの日常の作業方法に変化をもたらす場合、適切なグッドサイバーハイジーン慣行の意識向上キャンペーンを実施する（サービスのクラウドへの移行またはプロセスのデジタル化など）	● ITアセットインベントリ管理プロセスが存在し、新たなコンポーネントが追加、変更、削除された際は、ITアセットインベントリがアップデートされることを確認する ● ITコンポーネントのベースラインセキュリティ構成が存在し、それに応じて更新されるようにする ● 本番環境に導入する前に取得した新タイプの製品/システムベースラインセキュリティ構成を作成する
関連する調達のタイプ	すべて	臨床情報システム（CIS）, 医療機器, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム
関連する脅威	すべて	悪意ある行為, 人的ミス, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 29. 医療機器施設専用のアクセス制御メカニズムを確立	GP 30. 侵入テストのスケジュール（頻繁、またはアーキテクチャ/システムの変更後）
	PET/CTスキャナーや手術用ロボットなどの医療機器は、物理的な保護も必要である。アクセスは専門の担当者のみに許可し、各担当者は専用アカウントを持つ必要がある。 IT部門は、各デバイスのアクセス制御ポリシーを監視する必要がある。このデバイスを調達する際は、サプライヤーはこれらの規定を考慮する必要がある。	サプライヤーは、病院がその権限の下で必要なセキュリティチェック（セキュリティ監査、侵入テストなど）を実施する権利を認め、必要な文書への機関または病院の権限のある代表者への無制限のアクセスを保証するものとする。RfPには特定の条項を含める必要がある。また新たに入手または設定した製品は、実際の設置された環境で、侵入テストを実施する必要があることに注意することも重要である。
例/証拠	● 役割に基づくアクセス制御、厳格な管理を行う医療機器を扱う担当者専用のアカウント(2回誤入力後はアクセスを拒否する、2ファクタ認証など.) ● 医療機器設備への物理的なアクセス制御手段を確立する（バイオメトリクスを利用したアクセス)。この条項は技術的な説明に含める必要がある。	● 製品やシステムを実際の運用環境に設置し、構成した後にテストを行うことが重要である。これに続く問題修復の際は、この環境特有の運用パラメーターを考慮する必要がある ● サプライヤーは、（RfPで求められる場合）サードパーティーによる侵入テストのオプションを提供する必要がある。これには、ブラックボックステストおよびホワイトボックステストの両方を含めること。サプライヤーは、これらのテストのコストをオファーに含めること ● 病院はサプライヤー側で実施したテストの結果を要求する権利がある。サプライヤーは、テストの場合に通知し、透明性を高める必要がある
関連する調達のタイプ	医療機器, ビル管理システム, 識別システム	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（病院のサイバーセキュリティのための調達ガイドライン）

	GP 29. 医療機器施設専用のアクセス制御メカニズムを確立	GP 30. 侵入テストのスケジュール（頻繁、またはアーキテクチャ/システムの変更後）
	PET/CTスキャナーや手術用ロボットなどの医療機器は、物理的な保護も必要である。アクセスは専門の担当者のみに許可し、各担当者は専用アカウントを持つ必要がある。 IT部門は、各デバイスのアクセス制御ポリシーを監視する必要がある。このデバイスを調達する際は、サプライヤーはこれらの規定を考慮する必要がある。	サプライヤーは、病院がその権限の下で必要なセキュリティチェック（セキュリティ監査、侵入テストなど）を実施する権利を認め、必要な文書への機関または病院の権限のある代表者への無制限のアクセスを保証するものとする。RfPには特定の条項を含める必要がある。また新たに入手または設定した製品は、実際の設置された環境で、侵入テストを実施する必要があることに注意することも重要である。
例/証拠	● 役割に基づくアクセス制御、厳格な管理を行う医療機器を扱う担当者専用のアカウント(2回誤入力後はアクセスを拒否する、2ファクタ認証など.) ● 医療機器設備への物理的なアクセス制御手段を確立する（バイオメトリクスを利用したアクセス)。この条項は技術的な説明に含める必要がある。	● 製品やシステムを実際の運用環境に設置し、構成した後にテストを行うことが重要である。これに続く問題修復の際は、この環境特有の運用パラメーターを考慮する必要がある ● サプライヤーは、（RfPで求められる場合）サードパーティーによる侵入テストのオプションを提供する必要がある。これには、ブラックボックステストおよびホワイトボックステストの両方を含めること。サプライヤーは、これらのテストのコストをオファーに含めること ● 病院はサプライヤー側で実施したテストの結果を要求する権利がある。サプライヤーは、テストの場合に通知し、透明性を高める必要がある
関連する調達のタイプ	医療機器, ビル管理システム, 識別システム	医療機器, 臨床情報システム（CIS）, ネットワーク機器, リモートケアシステム, モバイルクライアントデバイス, 識別システム, 産業用制御システム, クラウドサービス
関連する脅威	悪意ある行為, 人的ミス	悪意ある行為, サプライチェーン障害, システム障害

医療機器サイバーセキュリティの原則及び実践
（2020年３月18日）
（Principles and Practices for Medical Device Cybersecurity）
IMDRF(International Medical Device Regulators Forum：国際医療機器規制当局フォーラム）

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（医療機器サイバーセキュリティの原則及び実践）

医療機器サイバーセキュリティの原則及び実践
IMDRF(国際医療機器規制当局フォーラム）（2020年３月18日)

	Principles and Practices for Medical Device Cybersecurity
対象	• ヘルスケア製品の製造業者、ヘルスケアプロバイダ、ユーザ、並びに規制当局及び脆弱性報告者を含む全ての責任関係者を対象としている。 • 対象となるシステムの構成要素については、ファームウェア及びプログラマブルロジックコントローラ等のソフトウェアを有する医療機器（例：ペースメーカ、輸液ポンプ）、又はソフトウェア単独で存在する医療機器（例：SaMD）とされる。
目的	• サイバーセキュリティに対する一般原則に係る基本的考え方と検討事項、並びに推奨されるベストプラクティスを提供することを目的として作成された。 • 医療機器を使用する際に起こり得るサイバーセキュリティリスクを最小化することにより、医療機器の安全性及び性能を維持し、継続使用を確保するための具体的な推奨事項を概説する。
作成方針	• 適切なサイバーセキュリティ保護を備えた医療機器の設計や開発を行うため、リスクベースのアプローチを採用する。 • 医療機器およびコネクテッドヘルスケアインフラの安全性、パフォーマンスおよびセキュリティを確保する。 • サイバーセキュリティは、医療機器メーカー、医療提供者、ユーザー、規制当局および脆弱性発見者を含む全ステークホルダー間で共有される責任であることを認識する。 • これらのステークホルダーに対して、総合製品ライフサイクル(TPLC)を通じて患者の被害リスク最小化の支援となる推奨事項を提供する。 • 統一の用語を定義し、医療機器サイバーセキュリティ達成のための現在のベストプラクティスを説明する。 • 透明性の向上や対応強化のため、サイバーセキュリティインシデント、脅威および脆弱性に関する幅広い情報共有ポリシーを促進する。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（医療機器サイバーセキュリティの原則及び実践）

- 本資料では、医療機器メーカーが製品設計の際に考慮すべき設計原則が示されている。
- セキュリティ要件は、ライフサイクル設計プロセスの要件取得段階においても特定する必要があるとされ、設計原則はこれに資する目的で示されている。

医療機器の設計で考慮すべき設計原則の選択

設計原則	説明
安全な通信	• メーカーは、デバイスが他のデバイスやネットワークと接続する方法を検討する必要がある。 • インターフェースには、有線接続および/または無線通信を含む。接続方法の例としてWi-Fi, Ethernet, Bluetooth, USBなどを含む。
	• メーカーは、（外部のみでなく）すべての入力を検証する設計機能を検証し、安全性の低い通信のみをサポートするデバイスや環境（ホームネットワークに接続されたデバイスやレガシーデバイスなど）との通信を考慮する必要がある。
	• メーカーは、不正なアクセスや変更、リプレイを防ぐデバイスへの通信およびデバイスからのデータ通信方法を検討する必要がある。 例えばメーカーは以下を決めること。 ➢ デバイスシステムの通信を互いに認証する方法 ➢ 暗号化の要否; 以前に送信されたコマンドやデータの不正リプレイを回避する方法 ➢ 通信セッションを中断する場合、事前に定義された時間の後に通信セッション終了することの適切性
データ保護	• メーカーは、デバイスに保存、デバイスから、あるいはデバイスに通信される安全関連のデータが暗号化などの保護が必要かどうかを検討する必要がある。例えばパスワードは、暗号的に安全なハッシュとして保存される必要がある。
	• メーカーは、通信プロトコルにおけるメッセージ管理/シーケンス分野を保護するため、または暗号化キーマテリアルの侵害を防ぐ機密性リスク管理対策の要否を検討する必要がある。
デバイスの完全性	• メーカーは、データの否認防止確保のための設計機能の要否について、システムレベルアーキテクチャの評価が必要である。(e.g.,監査ロギング機能のサポート)
	• メーカーは、デバイスソフトウェアの不正変更など、デバイスの完全性に対するリスクを考慮する必要がある。
	• メーカーは、ウイルス、スパイウェア、ランサムウェアその他の悪意あるコードがデバイスで実行されることの防止として、マルウェア対策などの管理を検討する必要がある。
ユーザー認証	• メーカーは検討する必要がある。デバイスを使用できる人またはさまざまなユーザーの役割に権限を付与したり、緊急時にユーザー クセスを許可したりするユーザーアクセス制御を検討する必要がある。 • さらにデバイス間および顧客間で同じ資格情報を共有しないこと。認証やアクセス認証の例として、パスワード、ハードウェアキーまたはバイオメトリクス、あるいは他のデバイスでは生成できない目的の信号（a signal of intent）が含まれる。

② １－２　海外における３省２ＧＬと同様の対象者を想定した同旨のガイドラインの存在有無と概要について文献、ウェブによる調査（医療機器サイバーセキュリティの原則及び実践）

設計原則	説明
ソフトウェアのメンテナンス	• メーカーは、定期的な更新の実行や展開のプロセスを確立し、連絡する必要がある。
	• メーカーは、OSソフトウェア、サードパーティソフトウェアまたはオープンソースソフトウェアの更新または管理方法を検討する必要がある。またメーカーは、自分の管理外にあるソフトウェアの更新または期限切れの運用環境への対応方法を計画する必要がある。（e.g. 安全でないOSバージョン上で実行されている医療機器ソフトウェア）
	• メーカーは、新たに見つかった脆弱性からデバイスを保護するためにソフトウェア更新方法を検討する必要がある。 • 例えば、更新がユーザーの介入を必要とするか、デバイスによって開始されるか、および更新がデバイスの安全性とパフォーマンスに悪影響を及ぼさないことを確認する方法の考慮が考えられる。
	• メーカーは、更新を行うために必要な接続方法およびコード署名またはその他の同様な方法による接続または更新の信憑性を検討する必要がある。
物理的なアクセス	• メーカーは、権限のない人がデバイスにアクセスすることを防止する制御を検討する必要がある。例えば、制御には物理的なロック、ポートへのアクセスの物理的な制限、または認証を必要としない物理ケーブルによるアクセスの許可を含めることができる。
信頼性と可用性	• メーカーは、デバイスが基本パフォーマンスを維持するためにサイバー攻撃の検知、抵抗、対応および攻撃から復旧できる設計機能を検討する必要がある。

【付録】
第三者認証制度に関する概要

ISO/IEC 27017　概要

ISO/IEC 27017:クラウドサービスに関する情報セキュリティ管理策のガイドライン規格

◆ 認証団体
　JQA　日本品質保証機構

◆ 目的
　クラウドサービスに関するリスクの低減、クラウドサービスを適切に提供/利用する組織体制の確立認証取得による、組織内外からの信頼向上を目的とする

◆ 証明内容
　情報セキュリティ全般に関するマネジメントシステム規格であるISO/IEC 27001の取り組みをISO/IEC 27017で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築していることを証明する

◆ 証明に必要な手続き
　次項参照

◆ 費用
　ISO/ IEC 27001をベースとした若干の追加審査工数分の費用を要する
※ISO/ IEC 27001は認証の対象となる組織の人員数や事業所数などに応じて審査料金を算出

ISO/IEC 27017　認証取得までの流れ

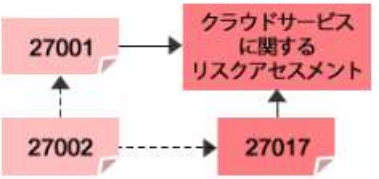
認証取得までの流れ

● （1）適用範囲の決定

ISO/IEC 27001の適用範囲内またはISO/IEC 27001と同一とする。

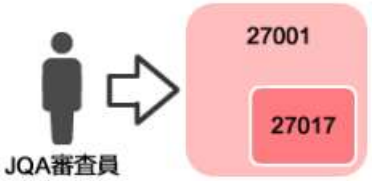
● （2）要求事項への対応（リスクアセスメント）

ISO/IEC 27002を参照しながら、ISO/IEC 27001とISO/IEC 27017に基づくリスクアセスメントを実施する。



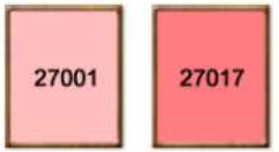
● （3）審査の受審

ISO/IEC 27001とISO/IEC 27017の審査を同時に受審する。



● （4）認証取得

ISO/IEC 27001とISO/IEC 27017の登録証が別々に発行される。



SOC (Service Organization Control) 概要

◆ 認証団体
AICPA 米国公認会計士協会

◆ 目的
事業者における財務諸表やシステム運用に関する適切な内部統制 を監査法人が作成した報告書により保証するもの

◆ 証明内容
SOC報告書には3種類存在する
SOC1：財務統制に関する報告書のため割愛
SOC2：顧客及びステークホルダー向けに、事業者がサービス利用者の情報を処理するために使用するシステムのセキュリティ、可用性、処理の完全性、情報の機密性とプライバシーに関連するサービスに係る保証報告書
SOC 3：SOC2と同様にセキュリティ等の統制について報告するものであるが、不特定の一般人向けの保証報告書

◆ 証明に必要な手続き
監査法人がセキュリティの5要素（セキュリティ、可用性、完全性、機密性、プライバシー）の内部統制の評価をした上で報告書を作成

◆ 費用
監査費用の見積もりによる

CSマーク　概要

◆ 認証団体
JASA　クラウドセキュリティ推進協議会

◆ 目的
公正かつ公平な情報セキュリティ監査がクラウドコンピューティングサービスにおいて実施され、クラウドコンピューティングサービスにとって有益なものとして情報セキュリティ監査が機能し、もって公益の増進に寄与するために、品質が保たれた情報セキュリティ監査を実施したクラウドコンピューティングサービスを標章する制度（クラウド情報セキュリティ監査制度）

◆ 証明内容
事業者が基本的な要件を満たす情報セキュリティ対策を実施し、事業者がそのとおりに実施しているかを標準的な基準に基づきあらかじめ定められた要件を満たす監査で評価し、安全性が確保されていることを顧客に公開する。

◆ 証明に必要な手続き
P8参照

◆ 費用
P10参照

外部監査を終えたもの（ゴールド）

内部監査を終えたもの（シルバー）

CSマーク（登録第629428号）

CSマーク制度　取得手順

外部監査評価までを終えたものはゴールド、内部監査までを終えたものはシルバーのCSマークを取得することができる。

CSマークの取得手順

※取得要件については次項参照

CSマーク制度　取得要件

外部監査を終えたもの（ゴールド）

適合監査が実施されたCS言明をした者の申請を協議会が受理したとき、協会がその使用を許諾するもの。

（適合監査の要件）

下記自主監査の要件を満たすこと。

クラウド情報セキュリティ外部監査人により、外部評価手続に従って自主監査の品質が評価されること。

内部監査を終えたもの（シルバー）

自主監査が実施されたCS言明をした者の申請を協議会が受理したとき、協会がその用を許諾するもの。

（自主監査の要件）

対象とするクラウドコンピューティグサービス及び情報セキュリティ対策を施施した基本リスクを明確にしたCS言明が、所定の様式書に記載されていること。

上記のCS言明に対し、下記の要件を満たす標準と定める情報セキュリティ監査が実施され、言明通りであることが確認されていること。

- 情報セキュリティ監査基準に準拠した監査であること。
- 基本リスクに対して、クラウド情報セキュリティ管理基準に準拠した管理策が実装され、運用されていることについての監査であること。
- クラウド情報セキュリティ監査人が行う監査であること。
- クラウド情報セキュリティ監査人の独立性が確保されていること
- 監査標準手続に準拠した監査手続により行われた監査であること。
- 所定の様式で監査のプロセスが記録されて、第三者がその妥当性を評価できること。
- 上記6つの要件を満たすことについて、根拠資料に基づき説明が可能であること。

CSマーク制度　各種申請手数料

附則

第１条　（手数料）

申請手数料は下表のとおりとする（消費税別）。

条番号	申請内容	項番	金額
第２条	自主監査の届出と CS シルバーマークの申請		15,000 円
第３条	自主監査の追加届出と CS シルバーマーク使用対象の追加申請		15,000 円
第４条	適合監査の届出と CS ゴールドマークの申請	第１項	15,000 円
		第２項	100,000 円
第６条	自主監査更新の届出と CS マーク使用許諾継続の申請		15,000 円
第７条	適合監査の届出と CS マーク使用許諾継続の申請		15,000 円
第８条	言明書記載内容の変更と CS マークの使用継続	第１項	5,000 円
		第２項	5,000 円
		第３項	10,000 円

JASA - クラウドセキュリティ推進協議会
適合監査等の認定手続き及び CS マーク使用許諾手続に関する規則
https://jcispa.jasa.jp/wp-content/uploads/docs/jcispa_regulation/jcispa_regulation_management03.pdf

医療情報ASP・SaaS情報開示認定制度

◆ 認証団体
ASPIC　一般社団法人日本クラウド産業協会

◆ 目的
- 医療情報ASP・SaaSサービスの安全・信頼性に係る情報開示が豊富になるとともに、開示項目が共通化されることで、ユーザーがサービス及び事業者の比較・評価・選択が容易になる
- 安全・信頼性に必要な情報開示への需要が高まり、認定を受けたサービスを提供する事業者は、さらにユーザ獲得の機会の拡大
- 医療情報ASP・SaaSサービスが社会経済活動の多くの分野で普及、定着し、情報通信システムの効率的な利用、企業の生産性向上、経済成長につなげる

◆ 証明内容
医療情報ASP・SaaSサービスの活用を考えている企業や地方公共団体などが、事業者やサービスを比較、評価、選択する際に必要な安全・信頼性に係る情報を適切に開示し、かつ一定の要件を満たす医療情報ASP・SaaSサービスを認定するもの
※　現在認定されているサービス一覧
https://www.aspicjapan.org/nintei/service_list.html

◆ 証明に必要な手続き
次ページ参照

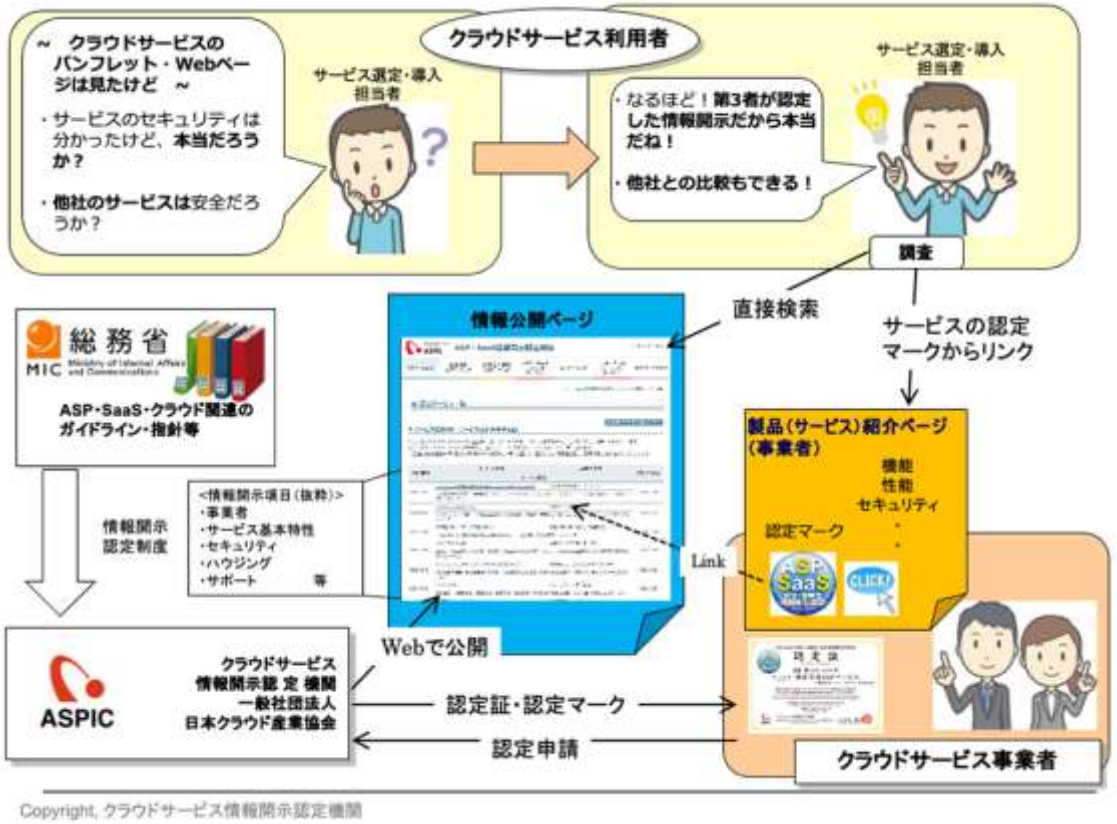
◆ 費用
次々ページ参照

図2　認定マーク

（注）認定マークはロゴと認定番号から構成されます。なお、認定番号は「医療」の識別子に上4桁は認定サービス通番、下4桁は認定年月（西暦）を表します。

医療情報ASP・SaaS情報開示認定制度
【参考】クラウドサービスの安全・信頼性に係る情報開示認定制度　取得手順

事業者の申請に基づいてASPICが認証することなるが、審査対象項目・審査基準は認証種別により異なる。



ASPIC「情報開示認定制度の全体像」
https://www.aspicjapan.org/nintei/index.html

例　医療情報 ASP・SaaSの場合の審査対象項目

ア. 審査対象としている情報開示項目
- 事業者の安全・信頼性に関する情報開示項目
- 開示情報の時点

- 事業所・事業
- 人材
- 財務状況
- 資本関係・所属団体
- コンプライアンス

イ. サービスの安全・信頼性に関する情報開示項目
- サービス基本特性
- アプリケーション、プラットフォーム、サーバ・ストレージ等
- ネットワーク
- 保守・運用
- ハウジング（サーバ設置場所）
- サービスサポート

全認定種別の認定に係る手数料は以下とおりである。

（別表１）認定に係る手数料

① 審査手数料　＜新規申請費用＞	1サービスにつき209,000円（消費税込み）
（内訳）審査手数料（税別）190,000円+消費税（10%）19,000円	
② 更新審査手数料　＜2年ごとに更新する際の費用＞	
	1サービスにつき104,500円（消費税込み）
（内訳）更新審査手数料（税別）95,000円+消費税（10%）9,500円	
③ 認定証再発行手数料	1サービスにつき10,450円（消費税込み）
（内訳）更新審査手数料（税別）9,500円+消費税（10%）950円	

なお、すでにASP・SaaS情報開示認定を取得しているサービスが新たに医療情報ASP・SaaSの認定取得を希望する場合は、更新審査手数料と同額といたします。

ASPIC　医療情報 ASP・SaaS の安全・信頼性に係る 情報開示認定制度の概要
https://www.aspicjapan.org/nintei/iryo-nintei/data/gaiyo.pdf

HISPRO適合証明

◆ 認証団体
HISPRO　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

◆ 目的
HISPROの専門の知識を持った評価員によって評価を受けることで、事業者が提供しているITサービスがガイドラインのどの部分に該当するか明確化し、ユーザーが安心した IT サービスの選択、利用を可能にする制度

◆ 証明内容
サービス提供事業者による各種製品・サービスの紹介・説明に下記マークが付けられたものは、HISPROにより該当する3省2GL（厚生労働省、経済産業省、総務省発行）への適合性が評価済であることを証明するもの

◆ 証明に必要な手続き
次項参照

◆ 費用
不明

HISPRO

HSP-C-Cxxxx-20xx

HISPRO適合証明　評価方法

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をする場合について

評価の流れ

1. 事業者からHISPROに評価希望機器、サービスの概要を通知
2. 事業者が通知した内容が評価業務範囲に含まれる場合には、HISPROから「費用見積もり等の条件」への同意後に、事業者記載のチェックシート等を提出して評価を受ける。

※チェックシート
https://hispro.or.jp/open/pdf/201903Cloud%20services%20koumoku.pdf#toolbar=0

提出書類

- 評価申請書
- サービス概要説明書
- 評価対象範囲説明書
- 記入済みチェックリスト
- チェックリストでエビデンスとした書類(※ルールの整備状況を見る場合、フォーマット等の存在をエビデンスとして扱う)
- 責任分界点の説明書
- ユーザーへのセキュリティ遵守事項説明書(重要事項説明書等)
- 「HISPRO 評価」によりガイドライン適合性を標榜する場合の文章等(標榜する場合のみ)

【付録】
適時調査の各調査書において示されている医療情報システムの安全性に関する項目

適時調査　調査書　確認事項
重点的に調査を行う施設基準

一般事項、初・再診料、入院基本料

◇　情報通信機器を用いた診療に係る基準（Ａ０００、Ａ００１、Ａ００２）

情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たしている。
（　適　・　否　）
ア　保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能である。
イ　対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有する。
ウ　患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できる。

当日準備

情報通信機器を用いた診療を実施する医師が、オンライン指針に定める「厚生労働省が定める研修」を修了していることが確認できる文書を見せてください。

適時調査　調査書　確認事項
重点的に調査を行う施設基準

入院基本料等加算

◇　診療録管理体制加算１（Ａ２０７）
◇　診療録管理体制加算２（Ａ２０７）

中央病歴管理室が設置されており、厚生労働省「医療情報システムの安全管理に関するガイドライン」に準拠した体制である。（　適　・　否　）

◇　診療録管理体制加算１（Ａ２０７）

★（７）以下の項目を全て含む電子的な一覧表を有し、保管・管理された診療記録が、任意の条件及び・コードに基づいて速やかに検索・抽出できる。（　適　・　否　）
ア　退院患者の氏名、生年月日、年齢、性別、住所（郵便番号を含む。）
イ　入院日、退院日
ウ　担当医、担当診療科
エ　ＩＣＤ（国際疾病分類）コードによって分類された疾患名
オ　手術コード（医科点数表の区分番号）によって分類された当該入院中に実施された手術
※　当該データベースは、各退院患者の退院時要約が作成された後、速やかに更新されている。
※　当該一覧表及び診療記録に係る患者の個人情報の取扱いについては、「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（個人情報保護委員会、厚生労働省））に基づく管理が実施されている。

◇　診療録管理体制加算１（Ａ２０７）
◇　診療録管理体制加算２（Ａ２０７）

許可病床数が400 床以上の保険医療機関については、厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づき、専任の医療情報システム安全管理責任者を配置する。
また、当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティに関する研修を行っている。さらに、当該保険医療機関は、非常時に備えた医療情報システムのバックアップ体制を確保することが望ましい。（　適　・　否　）
※　ただし、令和４年３月31日において、現に当該加算に係る届出を行っている保険医療機関（許可病床数が400床以上のものに限る。）については、令和５年３月31 日までの間、当該基準を満たしているものとみなす。

当日準備
専任の医療情報システム安全管理責任者の出勤簿（直近１か月分）を見せてください。

◇　医師事務作業補助体制加算１（Ａ２０７－２）
◇　医師事務作業補助体制加算２（Ａ２０７－２）

責任者は、医師事務作業補助者を新たに配置してから６か月間は研修期間とし、業務内容について必要な研修を行っている。（　適　・　否　）

※　当該研修期間内に次の項目を含む３２時間以上の研修を実施している。
ア　医師法、医療法、医薬品医療機器等法、健康保険法等の関連法規の概要
イ　個人情報の保護に関する事項
ウ　当該医療機関で提供される一般的な医療内容及び各配置部門における医療内容や用語等
エ　診療録等の記載･管理及び代筆、代行入力
オ　電子カルテシステム（オーダリングシステムを含む。）
※　当該責任者は、医師事務作業補助者に対する教育システムを作成していることが望ましい。

当日準備
新任の医師事務作業補助者に対する研修の実施状況が確認できる書類を見せてください。

◇　医師事務作業補助体制加算１（Ａ２０７－２）
◇　医師事務作業補助体制加算２（Ａ２０７－２）

医療機関内に次の診療体制がとられ、規程を整備している。（　適　・　否　）

ア　医師事務作業補助者の業務範囲について、規程を定めており、個別の業務内容を文書で整備している。
イ　診療録並びに手術記録、看護記録等の記載について、規程を文書で整備している。
ウ　個人情報保護について、院内規程を文書で整備している。・個人情報保護について院内規程を見せてください。
エ　電子カルテシステム（オーダリングシステムを含む。）について、規程を文書で整備している
※　医師事務作業補助者が電子カルテシステムに入力する場合は代行入力機能を使用し、代行入力機能を有しないシステムの場合は、業務範囲を限定し、医師事務作業補助者が当該システムの入力業務に携わっていない。

当日準備
医師事務作業補助者の業務範囲について規程を見せてください。
診療録並びに手術記録、看護記録等の記載について院内規程を見せてください。
個人情報保護について院内規程を見せてください。
電子カルテシステム（オーダリングシステムを含む。）について院内規程を見せてください。

◇ 感染対策向上加算１（Ａ２３４－２）
◇ 感染対策向上加算２（Ａ２３４－２・２）
◇ 入退院支援加算１（Ａ２４６）

ビデオ通話を用いる場合において、患者の個人情報を当該ビデオ通話の画面上で共有する際は、患者の同意を得ている。
また、保険医療機関の電子カルテなどを含む医療情報システムと共通のネットワーク上の端末においてカンファレンスを実施する場合には、厚生労働省「医療情報システムの安全管理に関するガイドライン」に対応している。
（　適　・　否　）

適時調査　調査書　確認事項
重点的に調査を行う施設基準

特定入院料

◇　脳卒中ケアユニット入院医療管理料（Ａ３０１－３）

当該保険医療機関内に、神経内科又は脳神経外科の経験を５年以上有する専任の医師が常時１名以上いる。

　夜間又は休日において、神経内科又は脳神経外科の経験を５年以上有する医師が、当該保険医療機関の外にいる場合であって、当該医師に対して常時連絡することや、頭部の精細な画像や検査結果を含め診療上必要な情報を直ちに送受信することが可能であり、かつ、当該医師が迅速に判断を行い、必要な場合には当該保険医療機関に赴くことが可能である体制が確保されている時間に限り、当該保険医療機関内に、神経内科又は脳神経外科の経験を３年以上有する専任の医師が常時１名以上いればよい。

※　なお、患者の個人情報を含む医療情報の送受信に当たっては、端末の管理や情報機器の設定等を含め、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保すること。

適時調査　調査書　確認事項
重点的に調査を行う施設基準

特掲診療料

◇ 外来データ提出加算（生活習慣病管理料の注４）（Ｂ００１－３注４）
◇ 在宅データ提出加算（Ｃ００２注13・Ｃ００２－２注７）
◇ リハビリテーションデータ提出加算（Ｈ０００注５、Ｈ００１注７、Ｈ００２注７及びＨ００３注５）

診療記録の保管・管理につき、厚生労働省「医療情報システムの安全管理に関するガイドライン」に準拠した体制であることが望ましい。

◇ ニコチン依存症管理料（Ｂ００１－３－２）

情報通信機器を用いて診察を行う保険医療機関にあっては、厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に沿って診療を行う体制を有している。（ 適 ・ 否 ）

◇　療養・就労両立支援指導料の注５（Ｂ００１－９注５）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」別添１の第１の１に掲げる情報通信機器を用いた診療の届出を行っていること。
（適・否）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初・再診料の施設基準等
第１ 情報通信機器を用いた診療
１ 情報通信機器を用いた診療に係る施設基準
(１) 情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア **保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。**
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
(２) **オンライン指針に沿って診療を行う体制を有する保険医療機関であること。**

◇ 画像診断管理加算１（Ｅ 通則５）
◇ 画像診断管理加算２（Ｅ 通則５）
◇ 画像診断管理加算３（Ｅ 通則５）

電子的方法によって、個々の患者の診療に関する情報等を送受信する場合は、端末の管理や情報機器の設定等を含め、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保している。（ 適 ・ 否 ）

適時調査　調査書　確認事項
重点的に調査を行う施設基準

入院時食事療養（Ⅰ）

適時調査　調査書　確認事項
重点的に調査を行う施設基準　入院時食事療養（Ⅰ）

◇入院時食事療養（Ⅰ）及び入院時生活療養（Ⅰ）
一般食における栄養補給量について、患者個々に算定された医師の食事箋**（◆）**による栄養補給量又は栄養管理計画に基づく栄養補給量を用いている。（ 適 ・ 否 ）

（◆）医師の署名捺印がされたもの又はオーダリングシステム等により医師本人の指示によるものであることが確認できるもの

適時調査　調査書　確認事項
重点的に調査を行う施設基準以外

基本診療料

適時調査　調査書　確認事項
重点的に調査を行う施設基準以外

特掲診療料－１
（医学管理等、在宅医療、検査、画像診断、投薬、注射、リハビリテーション、精神科専門療法、処置）

適時調査　調査書　確認事項（特掲診療料－１）

◇　ウイルス疾患指導料の注３（Ｂ００１・１注３）
◇　外来緩和ケア管理料の注５（Ｂ００１・２４注５）
◇　移植後患者指導管理料の注３（Ｂ００１・２５注３）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」別添１の第１の１に掲げる情報通信機器を用いた診療の届出を行っている。（　適　・　否　）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初・再診料の施設基準等
第１　情報通信機器を用いた診療
１　情報通信機器を用いた診療に係る施設基準
（１）情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア **保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。**
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
（２）**オンライン指針に沿って診療を行う体制を有する保険医療機関であること。**

適時調査　調査書　確認事項（特掲診療料－１）

◇　移植後患者指導管理料の注３（Ｂ００１・２５注３）
◇　糖尿病透析予防指導管理料の注６（Ｂ００１・２７注６）
◇　がん治療連携計画策定料の注５（Ｂ００５－６注５）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」別添１の第１の１に掲げる情報通信機器を用いた診療の届出を行っている。（　適　・　否　）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初・再診料の施設基準等
第１　情報通信機器を用いた診療
１　情報通信機器を用いた診療に係る施設基準
（１）情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア **保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。**
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
（２）**オンライン指針に沿って診療を行う体制を有する保険医療機関であること。**

適時調査　調査書　確認事項（特掲診療料－１）

◇　外来がん患者在宅連携指導料の注３（Ｂ００５－６－４注３）
◇　肝炎インターフェロン治療計画料の注３（Ｂ００５－８注３）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」別添１の第１の１に掲げる情報通信機器を用いた診療の届出を行っている。（　適　・　否　）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初・再診料の施設基準等
第１ 情報通信機器を用いた診療
１ 情報通信機器を用いた診療に係る施設基準
（１）情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア **保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。**
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
（２）**オンライン指針に沿って診療を行う体制を有する保険医療機関であること。**

適時調査　調査書　確認事項（特掲診療料－1）

◇　在宅時医学総合管理料（Ｃ００２）及び施設入居時等医学総合管理料（Ｃ００２－２）
【在宅時医学総合管理料の注12及び施設入居時等医学総合管理料の注６に規定する情報通信機器を用いた診療】

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」別添１の第１の１に掲げる情報通信機器を用いた診療の届出を行っている。（　適　・　否　）

「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
別添１　初・再診料の施設基準等
第１ 情報通信機器を用いた診療
１ 情報通信機器を用いた診療に係る施設基準
（１）情報通信機器を用いた診療を行うにつき十分な体制が整備されているものとして、以下のア～ウを満たすこと。
ア **保険医療機関外で診療を実施することがあらかじめ想定される場合においては、実施場所が厚生労働省「オンライン診療の適切な実施に関する指針」（以下「オンライン指針」という。）に該当しており、事後的に確認が可能であること。**
イ 対面診療を適切に組み合わせて行うことが求められていることを踏まえて、対面診療を提供できる体制を有すること。
ウ 患者の状況によって当該保険医療機関において対面診療を提供することが困難な場合に、他の保険医療機関と連携して対応できること。
（２）**オンライン指針に沿って診療を行う体制を有する保険医療機関であること。**

適時調査　調査書　確認事項（特掲診療料－１）

◇　遠隔連携診療料（Ｂ００５－１１）
◇　在宅酸素療法指導管理料の遠隔モニタリング加算（Ｃ１０３注２）
◇　遺伝カウンセリング加算（Ｄ０２６注６）
【遠隔連携遺伝カウンセリングに係る基準】

オンライン指針に沿って診療を行う体制を有する保険医療機関である。（　適　・　否　）

◇　在宅持続陽圧呼吸療法指導管理料の遠隔モニタリング加算（Ｃ１０３注２）

リアルタイムでの画像を介したコミュニケーション（ビデオ通話）が可能な情報通信機器を用いて指導を行う場合は、オンライン指針に沿って診療を行う体制を有する保険医療機関である。
（　適　・　否　）

適時調査　調査書　確認事項（特掲診療料－1）

◇　検査･画像情報提供加算及び電子的診療情報評価料（Ｂ００９･注１６、Ｂ００９-２）

電子的方法によって、個々の患者の診療に関する情報等を他の保険医療機関に提供する場合は、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保している。
（　適　・　否　）
□　**保険医療機関において、個人単位の情報の閲覧権限の管理など個人情報の保護が確実に実施されている。**

◇　長期脳波ビデオ同時記録検査１（Ｄ２３５－３）
◇　脳波検査判断料１（Ｄ２３８）
◇　遠隔脳波診断（Ｄ２３８注３）
(１）送信側（◆）においては、以下の基準を全て満たしている。（　適　・　否　）
（◆）脳波検査が実施される保険医療機関
(２）受信側（◆）においては、以下の基準を全て満たしている。（　適　・　否　）
（◆）脳波検査の結果について診断が行われる病院である保険医療機関

電子的方法によって、個々の患者の診療に関する情報等を他の保険医療機関に提供する場合は、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保している。
（　適　・　否　）

適時調査　調査書　確認事項（特掲診療料－１）

◇　遠隔画像診断（Ｅ　通則６・７）

【送信側】

（１）離島等に所在する保険医療機関その他の保険医療機関であって、次のいずれも満たしている。

（　適　・　否　）

【受信側】

（１）画像診断を行う病院であって、次のいずれも満たしている。　（　適　・　否　）

電子的方法によって、個々の患者の診療に関する情報等を他の保険医療機関に提供する場合は、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保している。

（　適　・　否　）

適時調査　調査書　確認事項（特掲診療料－１）

◇　検査･画像情報提供加算及び電子的診療情報評価料（Ｂ００９･注１６、Ｂ００９-２）

常時データを閲覧できるネットワークを用いる際に、ストレージを活用する場合には、原則として厚生労働省標準規格に基づく標準化されたストレージ機能を有する情報蓄積環境を確保している。
（　適　・　否　）
※　当該規格を導入するためのシステム改修が必要な場合は、それを行うまでの間はこの限りでない。
□　診療情報提供書を送付する際には、原則として、厚生労働省標準規格に基づく診療情報提供書様式を用いている。

情報の提供側の保険医療機関においては、提供した診療情報又は閲覧可能とした情報の範囲及び日時が記録されており、必要に応じ随時確認できる。（　適　・　否　）

情報を提供された側の保険医療機関においては、提供を受けた情報を保管している、又は閲覧した情報及び閲覧者名を含むアクセスログを１年間記録している。（　適　・　否　）
□　これらの記録について、（１）のネットワークを運営する事務局が保険医療機関に代わって記録を行っている場合は、当該加算･評価料を算定する保険医療機関は、当該事務局から必要に応じて随時記録を取り寄せることができる。

適時調査　調査書　確認事項
重点的に調査を行う施設基準以外

特掲診療料－２
（手術、麻酔、放射線治療、病理診断）

適時調査　調査書　確認事項（特掲診療料－２）

◇　遠隔放射線治療計画加算（Ｍ０００注４）
(１) 放射線治療を行う施設は、次の施設基準を満たしている。（　適　・　否　）
エ　当該治療を行うために必要な次に掲げる機器及び施設を備えている。

セキュリティ対策を講じた遠隔放射線治療システム

◇　遠隔放射線治療計画加算（Ｍ０００注４）
(２) 放射線治療を支援する施設は、次の施設基準を満たしている。（　適　・　否　）

セキュリティ対策を講じた遠隔放射線治療システムを備えている。

適時調査　調査書　確認事項（特掲診療料－２）

◇　遠隔放射線治療計画加算（Ｍ０００注４）
（１）放射線治療を行う施設は、次の施設基準を満たしている。（　適　・　否　）

遠隔放射線治療及び医療情報のセキュリティ対策に関する指針が策定されている。

◇　遠隔放射線治療計画加算（Ｍ０００注４）
（２）放射線治療を支援する施設は、次の施設基準を満たしている。（　適　・　否　）

遠隔放射線治療及び医療情報のセキュリティ対策に関する指針が策定されており、実際の遠隔放射線治療の支援が当該指針に沿って行われているとともに、公開可能な遠隔放射線治療の実施に係る記録が保存されている。

適時調査　調査書　確認事項
重点的に調査を行う施設基準以外

歯科

適時調査　調査書　確認事項（歯科）

◇　歯科画像診断管理加算１（歯Ｅ通則６）
◇　歯科画像診断管理加算２（歯Ｅ通則７）

電子的方法によって、個々の患者の診療に関する情報等を送受信する場合は、端末の管理や情報機器の設置等を含め、厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保している。（　適　・　否　）

NTT DATA

Trusted Global Innovator

（様式２）

二次利用未承諾リスト

令和４年度ヘルスケアサービス社会実装事業（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等に関する調査） 報告書

令和４年度ヘルスケアサービス社会実装事業（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等に関する調査）

株式会社NTTデータ経営研究所

頁	図表番号	タイトル
P8		2022年のランサムウェアの被害の推移
P9		感染経路
P9		バックアップの取得状況とその復元結果
P11		半田病院報告書において示される内容
P12		半田病院報告書において示される内容
P13		半田病院報告書において示される内容
P44		Ⅴ 医科診療報酬点数に関する留意事項
P45		Ⅴ 医科診療報酬点数に関する留意事項
P46		適時調査 調査書 確認事項（重点的に調査を行う施設基準 入院基本料等加算）
P47		「基本診療料の施設基準等及びその届出に関する手続きの取扱いについて」
P66		Incident Response LIfeycle
P78		Types of procurement
P83		Procurement process lifecycle of hospital
P106		認証取得までの流れ
P108		CSマーク
P109		CSマークの取得手順
P110		CSマーク
P112		認定マーク
P113		ASPIC 「情報開示認定制度の全体像」
P114		ASPIC ［医療情報 ASP・SaaS の安全・信頼性に係る 情報開示認定制度の概要］