総務省 学術雑誌『情報通信政策研究』 第９巻第１号
Journal of Information and Communications Policy Vol.9 No.1

論文（査読付）

医療情報の国際的取扱いの統制

黒田佑輝[1]

要　旨

本論文は、我が国の医療情報システムに関する情報セキュリティを規律する、いわゆる3省2ガイドラインに含まれる「国内規定」、すなわち医療情報や医療情報システムに対し、国内法の適用や執行があることを求める規定について、その沿革、目的及び手段を分析し、問題点を解明するとともに、改善の方向性を提案するものである。

国内規定には、①医療従事者が作成保存義務を負う記録が行政調査等の際に円滑に提出されることと、②医療従事者の守秘義務違反の防止という2つの目的があるが、現行ガイドラインは具体的な遵守要件を明確に示しておらず、特に、規制目的②に対応する手段が欠如している。

本論文は、医療機関にとって、作成保存義務がある記録の中に含まれる患者情報や、守秘義務の対象となる患者の秘密は、多くの場合個人情報保護法上の個人データに該当することに着目する。個人情報保護法の越境移転規制（28条）や安全管理措置（23条）は、外国での取扱いに関する規制を設け、外国制度の調査義務や高リスク時の取扱い回避義務を定めており、国内規定より詳細かつ広範な規制を構築している。これらの規定は、個人データの取扱いを規制することによって、結果的に国内規定の目的を達成し得る。

この分析に基づき、本論文は国内規定を廃止し個人情報保護法の規律に委ねる可能性を示唆する一方、それでもなお、医療情報に関して上乗せ規制を設ける際の選択肢として、①個人情報保護法をベースとした医療情報特有の厳格規制、②ホワイトリスト方式で取扱いを特定国に限定する規制、③医療情報システム事業者に対する独立した業法規制の可能性を検討した。

キーワード：3省2ガイドライン、国内規定、個人情報保護法、越境移転規制、外的環境の把握義務

１．はじめに

日本においては、医療機関が取り扱う「医療情報」や「医療情報システム」[2]は、関係する厚生労働省、経済産業省、総務省の発行する情報セキュリティガイドラインによって規律されている。かつては、3省が4つのガイドラインを公表していたが、現在では厚労省が発行する、医療機関向けの「医療情報システムの安全管理に関するガイドライン」第6.0版[3]（以下「厚労ガイドライン」と呼び、版をつけて「厚労ガイドライン6.0版」などと呼ぶ。

[1] 弁護士法人大江橋法律事務所、京都大学医学部附属病院医療情報企画部
[2] 具体的な内容については、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第6.0版」に関するＱ＆Ａ」12頁参照。
[3] 令和5年3月31日産情発0531第1号厚生労働省大臣官房医薬産業振興・医療情報審議官通知。

版の呼称は他のガイドラインにおいても同様とする。）と、総務省及び経産省が発行する、医療機関に医療情報システムを提供する事業者向けの「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」第 2.0 版[4]（以下「総務経産ガイドライン」と呼ぶ。）の 2 つに集約されている（以下、これらのガイドラインとそれらの前身となったガイドラインを含め、「3 省ガイドライン」と呼ぶ。）。

3 省ガイドラインが対象としている医療情報システムは、電子カルテシステムやオーダリングシステムのような、医療機関の中核となるシステムのみならず、医療機関で使用される医療機器に関する情報システムに広く適用されるほか、総務経産ガイドラインは、患者等の指示によって医療機関から医療情報の提供を受けた事業者にも適用される[5]。

現在の厚労ガイドラインは、個人情報の保護に関する法律（以下「個人情報保護法」と呼ぶ。）23 条の安全管理措置の具体的な内容を定めるとともに[6]、医療法 17 条に基づく医療法施行規則 14 条 2 項に基づき、病院等が「サイバーセキュリティ（中略）を確保するために必要な措置」を講じる際に参照すべき文書であるとされている[7]。したがって、違反をすれば、医療機関はこれらの法律に違反する可能性がある。また、総務経産ガイドラインは厚労ガイドラインと対になっており、事業者が違反すれば、事業者自身が個人情報保護法違反に問われる可能性があるほか、事業者に委託していた医療機関も前述の法違反に問われる可能性がある。ただし、制定の沿革を踏まえても、3 省ガイドラインの全ての規定をこれらの法令の下位指針であると割り切って理解するべきではなく、規定によっては、刑法 134 条等に基づく医療従事者の守秘義務や、医師法 24 条等の記録の作成保存義務など、他の制度の影響を受けているところも見られる。本稿で取り扱う規定も、個人情報保護法から切り離された沿革を持つ規定である。

現在の 3 省ガイドラインの中には、一部の医療情報や医療情報システムが、「国内法」の適用や執行があることを求める記載（以下、前身のガイドラインの中の類似規定を合わせて「国内規定」と呼ぶ。）が含まれている。国内規定は、実務的に重要な要件であることを超えて、日本政府が、外国が関与する情報の取扱いについて、いついかなる場合に規制を及ぼすべきか、またその規制の実効性はどの程度のものか、という法的な問題に関するきわめて興味深い素材でもある。

本稿は、現在の医療情報を取り巻く環境の中で、国内規定の意味とその妥当性を検証することを目的とする。あらかじめ本稿の結論を述べれば、厚労ガイドラインと総務経産ガイドラインの間には、その目的にも対象となる情報・行為にも、看過しがたい相違があること、及びいずれのガイドラインについても、国内規定を達成するための具体的な条件が明示さ

---

[4] 総務省、経済産業省「「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版（案）」に対する意見募集の結果及び当該ガイドラインの公表」（令和 7 年 3 月 28 日）（https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000427.html,令和 7 年 4 月 2 日最終閲覧）。

[5] 総務経産ガイドライン 2.0 版 6 頁。

[6] 個人情報保護委員会、厚生労働省「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（令和 6 年 12 月一部改正））40 頁（以下「医療介護ガイダンス」と呼ぶ。）。

[7] 令和 5 年 3 月 10 日産情発 0310 第 2 号厚生労働省大臣官房医薬産業振興・医療情報審議官通知。

れていないことから、抜本的な見直しが必要である。具体的には、個人情報保護法 28 条（外国にある第三者への提供の制限）及び 23 条（安全管理措置）の規制をベースラインとしつつ、真に必要な規制を再検討する必要がある。

以下、2 節では、まず、3 省ガイドラインの成立過程を振り返りつつ国内規定の沿革をたどる。その上で、3 節で、3 省ガイドラインが述べる国内規定の 2 つの目的を踏まえ、理念的な規制モデルを整理する。ついで、4 節でモデルを念頭におきつつ、現状の国内規定の問題点を明らかにする。最後に 5 節において、国内規定の見直しについて考え得る方向性に関する幾つかの提案を行う。

２．国内規定の沿革

国内規定の沿革を知るためには、3 省ガイドラインに加えて、診療録等の法令上作成保存義務がある記録の電子的作成・保存の歴史を辿る必要がある。もっとも、その経緯はきわめて複雑であるため、本稿では国内規定の沿革をたどるために必要な点に絞って紹介する [8]。

あらかじめその概要を述べておくと、2005 年に、診療録等の医療機関外での保存（外部保存）が認められた際に、医療機関向けの厚労ガイドライン 1 版が制定された。その後、2008 年から 2009 年にかけて、外部保存を受託する事業者向けに、経産省及び総務省がそれぞれガイドラインを制定した。このうち、2009 年の総務医療ガイドラインの中に、国内規定が初めて登場する。次いで、2012 年の経産ガイドライン 2 版にも国内規定が追加される。2020 年に総務省、経産省の各ガイドラインは統合されて、総務経産ガイドラインが制定されたが、その中に、現行の総務経産ガイドライン 2 版と同じ文言の国内規定が含まれている。一方、厚労ガイドラインへの国内規定の追加は、2021 年の 5.1 版で初めて行われ、現時点の最新版である 2023 年の 6 版で修正された。

２．１．厚労ガイドライン１版に至る経緯

そもそも、医師法をはじめとする医療関連法制は、医師や医療機関等に対して一定の記録の作成及び保存義務を課している（医師法 24 条 1 項等）。国内規定は、これらの手書き文書を前提とした義務体系に、電子化の波が押し寄せたことに始まる。

まず、厚労省は、1988 年に、「診療録等の記載方法等について」[9]で、ワードプロセッサー等で診療録等を作成することを認めた。ただし、この時点では保存は印刷した書面で行うことが想定されていた。ついで、1999 年の「診療録等の電子媒体による保存について」[10]は、通達レベルで、診療録など、いくつかの文書について、電磁的記録での保存を認めた。

---

[8] 沿革に関する比較的網羅的な資料として、厚労ガイドライン 6.0 版の付随資料である「ガイドライン改定の経緯に関する年表」がある。ただし、同資料は、後述の経産ガイドライン 2 版を掲載しておらず、完全ではない。

[9] 昭和 63 年 5 月 6 日総第 17 号・指第 20 号・医第 29 号・歯第 12 号・看第 10 号・薬企第 20 号・保険発第 43 号厚生省健康政策局総務課長・指導課長・医事課長・歯科衛生課長・看護課長・薬務局企画課長・保険局医療課長、歯科医療課長通知。

[10] 平成 11 年 4 月 22 日健政発第 517 号・医薬発第 587 号・保険発第 82 号厚生省健康政策局長、医薬安全局長、保険局長通知。

その後、厚労省は、2002 年に「診療録等の保存を行う場所について」[11]（以下、本通知を「外部保存通知」と呼ぶ。）を発出した。外部保存通知は、通知発出以前は、診療を行う医療機関内で記録を保存すべきであると解釈されていたという従来の解釈を振り返った上で、診療録等を医療機関外に保存しつつ、「ネットワーク等を利用することにより、必要に応じて直ちに利用することが技術的に可能となって」いることを理由に、医療機関外での保存（外部保存）を認めることに踏み出した。また、同通知に併せて、「診療録等の外部保存に関するガイドライン」[12]が示された。同ガイドラインは、その後の厚労ガイドラインのうち、法令上作成保存義務がある記録に関する特則につながっていく。

外部保存通知は、大きく、外部保存を認める記録等のリストと、外部保存を行う際の基準の 2 つから成り立っており、後者の中に、電子媒体での外部保存を行う際に認められた保存場所の記載がある。制定時には、病院又は診療所に準じる場所での外部保存しか認められていなかったが、2005 年 [13]及び 2010 年 [14]の改定で外部保存場所が順次拡大された [15]。

その後、2005 年に大きな変革が生じる。同年、2003 年に制定された個人情報保護法や、独立行政法人等の個人情報の保護に関する法律など、個人情報保護関係の法律が施行されるとともに、2004 年に制定された、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（以下「e 文書法」と呼ぶ。）も施行された。

e 文書法に関する厚労省令である、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」は、すでに 1999 年の「診療録等の電子媒体による保存について」が、電子媒体での作成・保存を認めていた文書に加えて、幾つかの文書を電磁的記録で作成・保存することを認めた。そして、e 文書法の施行通知である「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」[16]の一部として、厚労ガイドライン 1 版が定められた。このように、厚労ガイドラインは、診療録等の電磁的記録としての保存が法令上認められたことに紐づけられて成立した。もっとも、厚労ガイドライン 1 版は作成保存義務がある記録のみを対象としたわけではなく、大きく、作成保存義務がない情報を含む「医療情報」一般に関するセキュリティ対策を論じた前半部（1-6 章）と、診療録など作成保存義務のある文書特有の問題を論じた後半部（7-9 章）に区別して論じられている。本稿が着目する外部保存場所の要件については、8 章の 8.1.2 節に記載されている。この全体の章構成と 8.1.2 節の性質は、2022 年の厚労ガイドライン 5.2 版まで 15 年以上維持されることになる。

2005 年には、上記のとおり外部保存通知も合わせて改正され、外部保存場所は、医療機

---

11 平成 14 年 3 月 19 日医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長通知。
12 平成 14 年 5 月 31 日医政発第 0531005 号厚生労働省医政局長通知。
13 平成 17 年 3 月 31 日医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長通知。
14 平成 22 年 2 月 1 日医政発 0201 第 2 号・保発 0201 第 1 号厚生労働省医政局長・保険局長通知。
15 外部保存通知は 2013 年にも改正されているが、保存場所の定めに変更はない。平成 25 年 3 月 25 日医政発 0325 第 15 号・薬食発 0325 第 9 号・保発 0325 第 5 号厚生労働省医政局長・医薬食品局長・保険局長通知参照。
16 平成 17 年 3 月 31 日医政発第 0331009 号厚生労働省医政局長通知。

関に準じる場所、行政機関等が開設したデータセンター等、及び医療機関等が震災対策等の危機管理上の目的で確保した安全な場所の、3 つに拡張された。外部保存通知は、保存場所が日本国内であることを明示的に求めていないものの、医療機関外への外部保存が認められて 3 年しか経過していないことや、当時の情報通信技術の発達の状況などから考えれば、当然の前提であったと推測される[17]。

２．２．3 省ガイドラインの確立と国内規定の登場

厚労ガイドライン 1 版で定められた外部保存先のうち、「震災対策等の危機管理上の目的で確保した安全な場所」の説明の中には、すでに民間企業に委託することを想定した記載が存在する。もっとも、2005 年時点では、受託する民間企業向けの医療情報に関する固有の規制は存在しなかった。その後、経済産業省と総務省はそれぞれ規制を制定した。

まず、経済産業省は、2008 年に、パーソナルデータ情報研究会の下「医療情報を受託管理する情報処理事業者向けガイドライン」（以下「経産ガイドライン」と呼ぶ。）を作成し、それに基づいて経済産業省告示[18]を制定した。同ガイドラインは、外部保存の受託事業者向けのガイドラインとして作成されたが、特に保存場所を日本とする明示的な記載はない。

一方、総務省は、2008 年に、「ASP・SaaS における情報セキュリティ対策ガイドライン」（以下「総務一般ガイドライン」と呼ぶ。）という、医療に限定しない、一般的な ASP（Application Service Provider）及び SaaS に関する情報セキュリティガイドラインを公表し、ついで、2009 年に「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」（以下「総務医療ガイドライン」と呼ぶ。）を示した[19]。これによって、厚労省 1、経産省 1、総務省 2 の 3 省 4 ガイドライン体制が確立する。

総務省は、経産省とは異なり、まず、業種を問わず、およそ SaaS サービスに関するセキュリティ対策を総務一般ガイドラインで整理した上で、医療情報について、総務一般ガイドラインに上乗せをするべき事項を総務医療ガイドラインで追加する形で規律を及ぼした。

総務一般ガイドラインには、「ASP・SaaS サービスの提供にあたり、海外にデータセンターがある場合等、海外法が適用される場合があるので注意する必要がある」（25 頁）との記載がある。総務一般ガイドラインは注意喚起にとどまっていたのに対し、総務医療ガイドラインは、「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。」（67 頁）との要件を定めた。この記載が、現在につながる最初の明文の国内規定である。

２．３．2010 年の外部保存通知の改正とそれ以降の動向

経産ガイドラインと、総務医療ガイドラインの制定を受けて、当時厚労ガイドライン等を担当していた、厚労省の検討会は、2009 年末に、外部保存通知を改正し、保存場所の規制

---

17 厚労ガイドライン 1 版 8.1.2 節では、「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」で保管する際には、「医療機関等が、保存に係る情報処理機器を自らの所有物として保持」するなど、きわめて厳しいルールを設けていることも指摘できよう。

18 平成 20 年 7 月 24 日経済産業省告示第 167 号。

19 総務医療ガイドライン内でASP・SaaSは実質的に同じものとして扱われている（4-5 頁）。

を緩和するべきことを提言する[20]。これを受けて厚労省は、2010 年に 3 省 4 ガイドラインを遵守していることを前提として、「医療機関等が民間事業者等との契約に基づいて確保した安全な場所」に保存することを認める外部保存通知の改正を行った[21]。この改正によって、外部保存通知の性格は大きく変化した。すなわち、2005 年改正までは、外部保存通知が保存場所を決めており、3 省 4 ガイドラインは、その決められた場所における情報セキュリティ対策を具体化するという役割を負っていた。しかし、2010 年の改正によって、外部保存通知上は、3 省 4 ガイドラインを守っていれば、どこにでも保存できることになり、医療情報の保存場所を決めるイニシアティブは、3 省 4 ガイドラインの方に移ることとなった。

その後、2012 年に、経産省は、経産ガイドライン 2 版と、その要約としての経産省告示[22]を制定した。経産ガイドライン 2 版には「扱う情報として、法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。また、法令により作成や保存が定められていない文書であっても、個人情報保護に十分に留意して適切な管理を行うことが必要である。」（16 頁）との国内規定が登場した。また、別の個所では、医師法 24 条の診療録の作成保存義務とその刑罰規定を引用した上で「通常の業務であれば、業務記録を作成や保存を行わなかったからといって刑罰に処されることは考えにくい。このような厳しい規定は、生命に関わる情報を扱う医療分野に特有の要求であり、これらの国内法の円滑な執行のためにも、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。」（44 頁）と述べている。

2012 年の時点で、総務医療ガイドライン・経産ガイドラインに国内規定が明記された。その後、総務省は、2018 年に、総務一般ガイドラインと総務医療ガイドラインの両者を統合し、「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」を作成した（以下「総務統合ガイドライン」と呼ぶ。）（3 省 3 ガイドラインへの変化）。この際に、「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。」（109 頁）と文言が若干修正されている。

２．４．現行の国内規定の成立

2020 年に、総務省及び経産省は、各々のガイドラインを統合し、「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」（総務経産ガイドライン）0 版[23]を制定した（3 省 2 ガイドラインへの変化）。その、「6　制度上の要求事項」と

---

[20] 厚生労働省医療情報ネットワーク基盤協議会「診療録等の保存を行う場所に関する提言」（平成 21 年 11 月 2 日）。
[21] 前掲注 14。
[22] 平成 24 年 10 月 15 日経済産業省告示第 228 号。
[23] 総務経産ガイドラインは 2020 年の制定時には版数が付されておらず、その後 2022 年に改定されたものが 1.0 版、2023 年に再改定されたものが 1.1 版と呼称され、2025 年に 2.0 版が公表された。このため、正式な名称ではないが、本稿では、2020 年の制定時の版を 0 版と呼ぶ。

題する章に、「医療分野において法令等で作成・保存が義務付けられた医療情報の安全管理にあたり、全ての対象事業者」が守るべき事項が列挙されており、その中に以下のような節が設けられた（44 頁）。

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

この記載は、現行の総務経産ガイドライン 2.0 版でもそのまま維持されている（56 頁）。
厚労ガイドラインは、この頃までに累次の改正を経ているが、国内規定は未導入であった。初めて導入されたのは、2021 年の厚労ガイドライン 5.1 版であり、「8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」に以下のような記載がある。

「外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、 所管する行政機関の調査等に供するため、提出等を行う必要が生じ得ることから、これを円滑に実現できることが求められる。そのため外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められる。」（117-118 頁）

「(8) 保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。
(9) 外部保存を受託する事業者を選定する際は、(1)から(8)のほか、少なくとも次に掲げる事項について確認すること。
（中略）
g 医療情報を保存する機器が設置されている場所(地域、国)
h 受託事業者に対する国外法の適用可能性 」（121 頁）

その後、2023 年に策定された厚労ガイドライン 6 版では、医療情報一般と、作成保存義務のある記録に関する章を分けるという初版以来の構成が廃止され、両者は一体的に記載されるようになった。もっとも、個別の要求事項の中では、外部保存に関する要求事項とそれ以外の要求事項は書き分けられている。国内規定については以下の記載がある。

「⑤ 外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。
（中略）
－ 保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。
⑥ 外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。
（中略）
h 医療情報を保存する情報機器が設置されている場所(地域、国)
i 委託先事業者に対する国外法の適用可能性」（企画管理編 27-28 頁）

外部保存と結び付けられていること、国外法の適用について確認することが求められていることは厚労ガイドライン 5.1 版と同様である。もっとも、「阻害するような国外法の適用がない」ということまでは明確に求められていない。

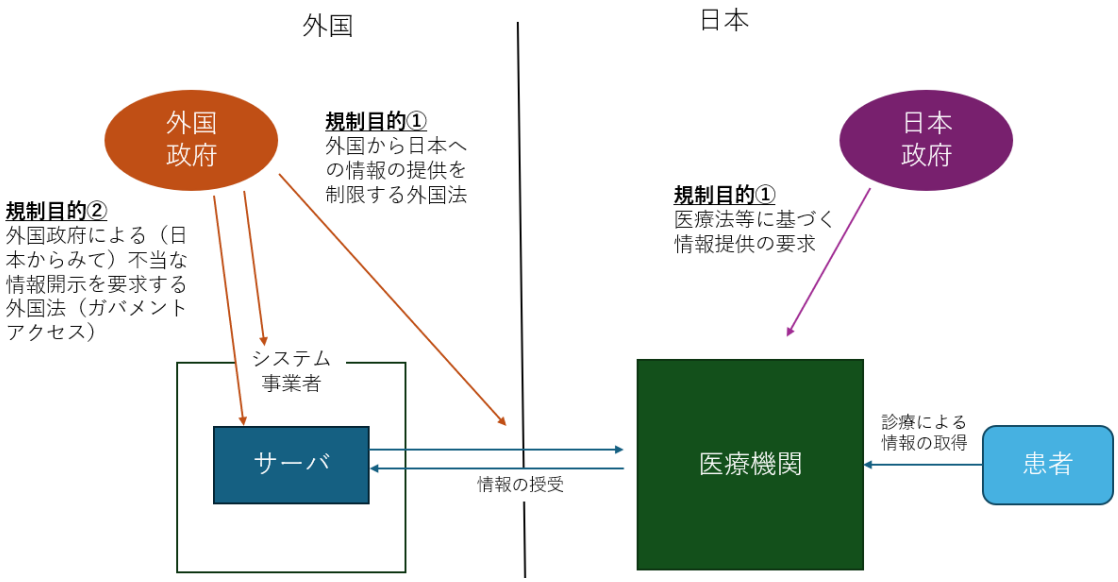
３．国内規定の目的及び理念的に想定される規制手段

以上の沿革からわかるとおり、国内規定は、2009 年の総務医療ガイドラインを皮切りに、各ガイドラインの中に登場した。各ガイドラインの内容は、ある程度類似しているものの、徐々に変化してきており、また、個々の文言の意義が詳細に説明されているわけではない。このため、分析の見通しをよくするべく、各ガイドラインの国内規定の規制目的から、理念的に想定される規制手段を整理する。

現在の総務経産ガイドライン 2.0 版は、規制目的として、①医療従事者が作成保存義務を負う記録が行政による調査等に際して円滑に提出されることに加えて、②医療従事者の守秘義務違反の防止という 2 つをあげる。対して、現在の厚労ガイドライン 6 版は根拠を明確にしていないものの、直前の厚労ガイドライン 5.1 版は、①に対応する規制目的のみを挙げていた。規制目的①は、3 省ガイドラインに共通しており、3 省のパブリック・コメントの回答の中でも言及され続けていることから、これが規制目的であることは疑いがない。他方、規制目的②は、総務経産ガイドラインの本文のみで言及されており、それらに関するパブリック・コメントの中では言及されておらず、その重要性を評価することが難しい。ともあれ、総務経産ガイドラインの記載は無視できず、②も規制目的であると考えられる。

ところで、医療機関から事業者が受託した医療情報システムの在り方を非常に単純にモデル化すれば、システムの運営者・サーバ設置場所について、(1)日本法人・国内サーバ、(2)日本法人・外国サーバ、(3)外国法人・国内サーバ、(4)外国法人・外国サーバという 4 パターンを想定できる。

図１．国内規定の目的に関する概念図



両規制目的の違いを図 1 に基づき検討する。図 1 では、パターン(4)、すなわち患者が日本国内に所在する医療機関を受診し、その情報が外国に設立されたシステム事業者が管理する外国サーバに保管される状況を想定している。この場合において、規制目的①は、日本の公的機関が、医療機関や医療従事者に対して、外国サーバに保存された情報の提出を命じた際の実効性を確保することを目的としている。対して、規制目的②は、医療従事者の守秘義務違反を問題にしている。その趣旨は、本規定が日本国外における情報の取扱いに関連して指摘されていることから、システム事業者やサーバを通じて、医療情報が、システム事業者の設立国の政府などの第三者の手に渡ることを警戒しているものと解される [24]。比喩的

[24] なお、医療従事者の守秘義務は刑法 134 条や、保健師助産師看護師法 42 条の 2 などに散在している。代表例である刑法 134 条の議論を参照すると、医師等の個人に対して守秘義務を課していることから、患者の秘密を他の医師に開示することも構成要件に該当するとされる（佐久間修『最先端法領域の刑事規制 医療・経済・IT 社会と刑法』42 頁、50 頁(現代法律出版、2003)）。したがって、当然ながら、医師が、電子カルテ等の医療情報システムのベンダーに対して患者の秘密の取扱いを委ねることも構成要件に該当し、「正当な理由」がなければ刑事罰に問われ得る。佐久間・同 38 頁や同 51 頁は医療情報の管理の外部委託などが、秘密漏示罪と緊張関係があることを指摘する。具体的な刑法上の守秘義務に関する議論を検討すると、情報システムベンダーへの医療情報の提供に関連するものとして、少なくとも検査会社への業務委託を患者の推定的同意で正当化するとの説明が試みられているほか（村山淳子「医療情報の第三者提供の体系化（一）」　西南学院大学法学論集 39 巻 3 号 1 頁、11 頁以下　2006）、チーム医療における情報共有を端的に同条の「正当な理由」に該当すると位置づけるものなどがある（甲斐克則「医療情報と刑法」甲斐克則編『医療情報と医事法【医事法講座 9】』47 頁、66 頁（信山社、2019））。したがって、医師が、システム事業者が外国政府に情報を提供していることを知りつつ患者の秘密を預けた場合や、そこまで至らなくとも、あまりにもずさんなセキュリティしか講じていないことを認識しつつ秘密を預けたような場合には、本人の推定的同意がないと整理したり、正当な理由を欠

にいえば、規制目的①は、日本の公的機関の権限を確実に及ぼそうという攻めの姿勢によるものであるのに対し、規制目的②は、秘密に対する外国政府のアクセスを阻止しようとする守りの姿勢によるものであり、意図する方向が異なる。

そして、規制目的から導き出される規制手段の構想も異なり得る。すなわち、規制目的①の場合、規制は、作成保存義務がある診療録等の「記録」を対象にし、その具体的な手段も記録の「保存」や、そのために用いられるハードウェア等に焦点を当てることが自然である[25]。他方で、規制目的②では、規制手段は、本来医師等が知りえた「秘密」を中心に組み立てる必要が出てくる。このため、少なくとも、作成保存義務のある記録よりは、2 つの点で対象は広くなる。まず、記録に関する規制は、記録が作成保存されていれば、記録の内容である情報が複製され利用されることに関知しない。しかし、守秘義務の側から見れば、記録の内容である情報こそが秘密に当たり、複製された情報についても等しく保護する必要がある。また、刑法 134 条にいう「秘密」の範囲については議論があるものの[26]、「記録」に含まれないが、明らかに秘密に該当する情報が存在する。そのような例としては、法定保存年限を経過した記録や、「診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像」などがあげられる[27]。そして行為としても、守秘義務が、各医療従事者個人が秘密を「漏らす」行為を禁止する以上、保存だけではなく、他者に開示することを伴う行為を広く規制する必要がある。すなわち、外部事業者が行う秘密の取扱いは、医療従事者による秘密開示行為を前提とする以上、すべからく規制対象となり、そのために用いられるハードウェアやソフトウェアも全て規制対象となることが自然である。

つまり、規制目的①②は、その意図が異なるだけではなく、導き出される規制手段も異なっている。当然、この違いは、着目すべき法制度にも影響する。規制目的①からすれば、司法機関や行政機関が医療機関に対して記録の提出を要請した際に、委託先事業者が適時にその情報を提供できるかという問題が中心となり、副次的に、このような日本の公的機関の権限行使を阻害するような外国法の存在が問題となる。他方で、規制目的②からすれば、まず、日本から見て、情報の不当な取得であると評価されるような外国法があるかどうかこそが大きな問題となり、副次的に、そのような外国政府の権限行使をどのように回避できるか、もしくは日本法により阻止できるかという点が問題となり得る。

次節では、こうした、規制目的と規制手段の理念的な関係を前提に、3 省ガイドラインの内容を検討する。あらかじめ結論を述べれば、規制手段は規制目的①と親和的なものが多く、そもそも規制目的②に対応すると評価できる規制手段はほぼ存在しない。もっとも、規制目的①との関係でも、具体的な行為規範が曖昧であり、規制としては明確性を欠いている。こ

くとしたりして、システム事業者への開示が刑事上の守秘義務違反となる可能性は想定できよう。

[25] 厳密には、外部保存通知が定める記録の中には、医療法 46 条 2 項に定める医療法人の財産目録など、患者の情報を含まないものもあるが、本稿では、外部保存通知の対象となる記録のうち診療録に代表される患者情報を含むものを前提に論ずる。

[26] 刑法 134 条における「秘密」の意義に関する学説について、大塚仁ほか編『大コンメンタール刑法(第三版)第 7 巻』365 頁以下〔米澤敏雄〕（青林書院、2014)。医師が精神鑑定の過程で知り得た秘密の漏示が問題となった最決平成 24 年 2 月 13 日刑集 66 巻 4 号 405 頁は、秘密の定義を示していない。

[27] 厚労ガイドライン 6 版に関する Q&A11 頁（概 Q-3)。

のため、いずれの目的との関係でも合理的なルールが定められているとはいいがたい。

４．国内規定の内容

４．１．国内規定の対象となる情報・記録の範囲

2 節で検討した沿革からわかるとおり、国内規定はその初めから外部保存通知の対象となる情報と結びついていた。そして、2.4 節の通り、現行の 2 ガイドラインは、いずれも、国内規定の対象を、医療情報一般ではなく、外部保存通知の対象となる情報に限定している。3 節で整理したとおり、このような対象の設定方法は、規制目的①には整合しているが、規制目的②を実現しようとするのであれば対象範囲が十分ではない。

４．２．国内規定の対象となる機器・システムの範囲

現行のガイドラインは、国内規定の対象を以下のとおり定める。

厚労ガイドライン 6 版(企画管理編)「保存された情報を格納する情報機器等」
総務経産ガイドライン 2.0 版「医療情報及び当該情報に係る医療情報システム等」

規制目的①のみに言及する厚労ガイドラインは、文言上、外部保存通知の対象となる保存された情報を格納する情報機器、すなわち記録を保存するという行為と、その際に利用されるストレージ機器を対象としている。これは保存された「記録」への公的機関のアクセス可能性を確保することを求める規制目的①と整合しているといえよう[28]。

対して、総務経産ガイドラインの「医療情報及び当該情報に係る情報システム等」については、その対象を特定することは容易ではない。総務統合ガイドラインでは、国内規定の対象は、「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」と記載されていた。ここでは、「情報システム」という言葉の一般的な意義からしても、ひとまず、「情報システム」とは、総務統合ガイドラインが言うような「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」の、システムを構成するハードウェアやソフトウェアを意味しているものと仮定する。そして、医療情報とは、外部保存通知の対象となる記録に記載された医療情報ということになる。

総務経産ガイドラインが規制目的①②の両方を挙げることからすれば、総務経産ガイドラインは、単に記録ではなく、記録の中に含まれる情報については、その複製を含め広く保護し、行為態様としては、保存のみならず、取扱い一般を規制しようとすることが自然であるが、記載文言はそのような解釈を一応許容しよう。

この両ガイドラインの規制の広狭は、例えば、電子カルテから一定の情報を抽出し、それ

---

[28] ただし、厚労ガイドライン 5.1 版のパブリック・コメント回答 149 番（以下、パブリック・コメントについては、パブリック・コメントの対象となったガイドラインと、意見の整理番号で特定する。）は、「法の適用を受けるのは通常は組織」であり、機器ではないのではないかという質問に対し、「機器等の実際の物理的な管理状況により、管理者や処分権限者など、対象となる者の範囲は異なるとことを想定しており」と述べていることから、純粋に機器を対象とするのではなく、機器を管理する者を対象とすることも想定しているようにも理解できるが、詳細は不明である。

を AI に分析させ、医師に診療上の示唆を提示するシステムを想定した場合などに問題となる。国内規定は記録の保存のみに適用されると考えるのであれば、当該システムに国内規定は適用されないであろうが、記録内の情報の取扱いに適用されるとすれば、当該システムも国内規定の対象となろう。

つまり、この問題については、厚労ガイドラインは規制目的①に親和的な文言であるといえる。他方で、総務経産ガイドラインは規制目的①②に親和的な文言と解釈することもできるが、その場合、厚労ガイドラインの適用範囲よりも対象が広くなることになる。

４．３.「国内法」の「適用」又は「執行」

ついで、国内規定の中核をなす、「国内法」の「適用」又は「執行」について両ガイドラインを検証する。論点は大きく 3 つに分けられる。

４．３．１.「国内法」が指す法律

「国内法」とは具体的に何法を意味するのであろうか。まず、総務経産ガイドラインが、医療法 25 条 1 項及び 3 項の立入検査権を念頭に、「医療法では（中略）医療機関等に対し、構造設備や診療録、帳簿書類その他の物件等の提出等を命じることができるとされており、当該命令に適切に対応しなかった場合の罰則も規定されている。」(51 頁)と述べているとおり、医療法等を根拠とした行政による立入検査等が念頭に置かれていることは明確である。

また、ガイドライン本文では必ずしも明確ではないが、以下のパブリック・コメントから、司法手続が含まれていることも理解できる。ただし、民事・刑事いずれの手続が主として念頭に置かれているかははっきりしない。

「医療機関等が行政機関等や司法機関等からの求めに応じて、証拠を提供する際に、これを円滑に行えるようにする観点から国内法の適用を受ける」(厚労ガイドライン 5.1 版 149 番)
「本項の目的は、行政等による調査や争訟において、医療情報格納する機器等が証拠等として利用できなくなるなどのリスクを想定して」（厚労ガイドライン 5.2 版 179 番）

被調査主体としては、上記 5.1 版のパブリック・コメントのとおり、「医療機関等」[29]が想定されていることは間違ない。ただし、それ以外の情報システムのベンダー等に対して、直接公的機関が調査を行ったり、資料の提出を求めたりといった状況が想定されているのかどうかははっきりしない。

以上から、3 省の想定する国内法は、規制目的①に対応するものであることが理解できる。なお、規制目的②に関して、総務経産ガイドライン及びそのパブリック・コメントを見ても対応する法制度を示唆する言及はない。

[29] ここでいう医療機関等とは、厚労ガイドラインが定義する「医療機関等」（厚労ガイドライン 6.0 版概説編 1 頁）、すなわちガイドラインの直接の名宛人となる医療機関や介護施設等を意味し、情報システムのベンダーを含んでいないと考えられる。

４．３．２.「国内法」の「適用」か「執行」か

現行の厚労ガイドラインは国内法の「適用」という言葉を用い、他方で総務経産ガイドラインは、国内法の「執行」という言葉を用いている。

沿革を確認すると、2009 年の総務医療ガイドラインは「適用」であったが、2012 年の経産ガイドラインは「執行」と表現した。その後、2018 年の総務統合ガイドラインは、パブリック・コメント案は「適用」であったが、パブリック・コメントの結果「執行」に変更された（総務統合ガイドライン 1 版 74 番 [30]）。この時点で総務省と経産省では用語が統一され、以降の総務経産ガイドラインは一貫して「執行」と述べる。他方で、厚労ガイドラインは、国内規定が登場した 5.1 版以降「適用」という言葉を用いている。両者の間には、どのような違いが存在するのか。ガイドラインやパブリック・コメントからは明確ではない。

規制対象となる人や事物が日本国内で完結している場合には、適用か執行かという用語選択を問う意味は乏しい。しかし、国内規定のように、国外の事象をも射程に入れた規律を考える場合には、一般に、ある法令が自国の領域外に適用されることと、司法当局や行政当局が、具体的事案に対して法を執行できるかは区別され、法令の域外適用が一定の場合に認められるとしても、それを自国外で執行することには大きな制約があることに留意する必要があろう [31]。つまり、文言だけを見れば、厚労ガイドラインは、国内法が観念的に「適用」されていればよいとするのに対し、総務経産ガイドラインは、国内法が現実的に「執行」できる必要があるとして、日本の領域により密接に結び付くことを求めているとも考え得るのである [32]。

４．３．３.「国内法」の「適用」又は「執行」があることの具体的な意味

以上のとおり、「国内法」が指す具体的な法はある程度推測できるとしても、「適用」又は「執行」の意義は不明であることなどから、ガイドラインの対象者から、この要件を満たすための具体的条件について疑問が出ることは当然であろう。実際、パブリック・コメントにおいては、ベンダーが外国事業者である場合や、海外のクラウドサーバを使う場合など、様々なケースを想定した質問が行われているが、残念ながら、3 省は、ほとんどのケースにおいて、具体的な回答をしていない。

---

30 もっとも、当該パブリック・コメントの質問内容は、「適用」から「執行」への文言の修正を求めたものではなく、質問内容とこの修正は対応していない。回答の中で経産ガイドライン 2 版を引用していることから、担当官が回答を起案する際に、表現の違いに気づき、「適用」から「執行」に修正したのではないかと思われる。

31 小松一郎（外務省国際法局関係者有志補訂）『実践国際法(第 3 版)』24-25 頁（信山社、2022)、小寺彰『パラダイム国際法-国際法の基本構成-』95 頁(有斐閣、2004)、小寺彰ほか著『講義国際法(第 2 版)』171-174 頁（有斐閣、2010）竹内真理「国際法における国家管轄権行使に関する基本原則 」鶴田順編『海賊対処法の研究』83 頁、84 頁（有信堂高文社、2016 年)。

32 もっとも、厚労省も、あるパブリック・コメントにおいて、「我が国の行政権が優先される必要があることの確認を行うため、国内法の適用の有無を確認して事業者選定の資料にするという趣旨としております」（厚労ガイドライン 5.2 版 186 番）と述べ、観念的な法適用を超えた何らかの実効性を問題にしているようでもあり、用語の選択がどこまでの意図に基づくか必ずしも明確ではない。

3 節で述べた通り、医療情報システムの構成としては、(1)日本法人・国内サーバ、(2)日本法人・外国サーバ、(3)外国法人・国内サーバ、(4)外国法人・外国サーバという 4 パターンを想定できる。このうち、(1)が国内規定に抵触しないことは明らかであるが[33]、(2)から(4)が禁止されているのかどうか明確ではない。一つの理解は、国内規定は国内「保存」規定であり、(1)(3)は許されるが(2)(4)は許されないというものである。もともと、国内規定が、外部保存場所を医療機関外に拡張する中で発生したという沿革から考えても、厚労ガイドライン 5.1 版に関連する資料である「医療情報システムの安全管理に関するガイドラインの概要及び主な改定内容」6 頁に、「医療情報が保存された情報を格納する機器等に国内法適用に関するイメージ」として、日本列島を国内法の適用範囲とし、外国をイメージした「国内法適用対象外地域」に情報を保存することを否定する図が掲載されていることからしても、国内規定が情報の保存場所を日本国内に限定する規定であるという考えは根強い。実際、厚労省は、2025 年になって、生成 AI に関連して、「「保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。」としているが、医療情報が保存されないことが、契約等において担保されている場合は国内法の適用を受けていないサーバを利用可能です」との見解を示した。これは国内保存規定であるという解釈に親和的である[34]。

もっとも、厚労省のパブリック・コメントの中には、海外のクラウドサーバを使用できないのか、という問いに「クラウドサーバの存在位置が問題ではな」いと述べたものがある（厚労ガイドライン 5.2 版 186 番）ことから、必ずしもサーバ所在地を国内に限定するものではないようであり、また、別のパブリック・コメントにおいても、海外事業者への委託可能性を否定しないものがある（厚労ガイドライン 5.1 版 103 番）ことからしても、医療情報を取り扱うベンダーが日本法人であることを求めるものでもないようである。このため、遵守すべき具体的な条件はきわめて不明確である[35]。

４．３．４．外国法の適用の有無

国内法と対になる問題として、外国法の適用に関する問題がある。まず、第 3 で述べたとおり、規制目的①②ともに、外国法の影響を無視することはできないが、それぞれの規制目的によって、その目的達成を阻害し得る外国法は全く異なっている。

厚労ガイドラインを見ると、6 版には以下のような記載がある。

「⑥ 外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認す

---

[33] もちろん、法人の設立国のみならず、法人の資本構成や経営陣について外国の影響があるかどうかを問題とするルールも想定し得るが、現状の 3 省ガイドラインがそこまで踏み込んでいるとは言えないであろう。

[34] 厚労ガイドライン 6 版に関する Q&A44 頁（企 Q-26）。

[35] 事業者側において、これに近い理解を示すものについて、内閣府健康・医療戦略推進事務局ほか「「医療分野の研究開発に資するための匿名加工医療情報に関する法律施行令の一部を改正する政令（案）」、「医療分野の研究開発に資するための匿名加工医療情報に関する法律施行規則の一部を改正する命令（案）」、「医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律についてのガイドライン（案）」及び「医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する基本方針（案）」に対する意見募集の結果について」（令和 6 年 3 月 21 日）別紙 6 頁。

ること。
（中略）
i 委託先事業者に対する国外法の適用可能性」（企画管理編 27-28 頁）

加えて、厚労ガイドライン 6 版には存在しないが、5.1 版(117-118 頁)及び 5.2 版(別冊 73-74 頁)には以下のような記載があった。

「外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、所管する行政機関の調査等に供するため、提出等を行う必要が生じ得ることから、これを円滑に実現できることが求められる。そのため、外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められる。」

また、留意すべき外国法については、以下のパブリック・コメントがある。

「医療機関等が行政機関や司法機関等の求めに対して、円滑に資料を提供しえない、ないしは保護措置がとれなくなるリスクを勘案して、各医療機関の実態に即して、事業者の選定を求めるための確認事項として示すものです。特に海外事業者において、本国と日本の国内法から同時に責務を負う場合には、当該事業者の判断に委ねられることになることから、医療情報管理に対して、医療法上の責務を負う医療機関においては、そのリスクを確認して、外部保存の委託先を選定することを求める趣旨です。」（厚労ガイドライン 5.1 版 103 番）

ここでの「阻害するような国外法の適用」とは、データが日本の行政機関や司法機関に提供されることを禁止又は制限するような外国法を問題視していると考えられる [36]。これは規制目的①に整合している。もっとも、具体的にどのような制度がこれに該当するか、またどのような条件であれば、それを回避できるかについて、明確な議論はなされていない。

これに対し、規制目的②との関係では、日本から見て受け入れられないような情報収集活動を可能にする外国法の影響があるかどうかが問題となるが、具体的な議論はない。この点に関連して 2 つの問題を指摘しておく。

まず、3 省ガイドラインは、日本法の「適用」又は「執行」を強調するが、そのことは、外国法の適用やそれに基づく執行がないことを何ら保証しない。4.3.3 節で述べた 4 パターンのシステム構成のうち、例えば、外国法人・国内サーバのパターン(3)を検討しよう。この場合、属地主義により日本国内のサーバに日本法が適用されるが、このサーバに対して外国法が域外適用され得る。実際、日本の最高裁判所の決定において、捜査段階で警察官が日本国内から所在地不明のサーバにアクセスして得た証拠を、違法収集証拠として排除せず採用したものがある [37]。同決定の事案の反対として、外国法人の設立国の政府が、同種の手続

[36] 日本から外国への越境捜索において、外国の個人情報保護制度と緊張が生じ得ることについては、板倉陽一郎「個人情報保護法の観点から」指宿信=板倉陽一郎編『越境するデータと法　サイバー捜査と個人情報保護を考える』202 頁（法律文化社、2023）参照。
[37] 最決令和 3 年 2 月 1 日刑集 75 巻 2 号 123 頁。

で日本国内のサーバから情報を収集するということも十分に想定し得る[38]。つまり、国内法の「適用」や「執行」があること、ひいてはデータを国内にとどめるという単純なローカリゼーションは、当然には、利用目的②のようなデータの収集活動を抑制することには貢献しない[39]。

また、パブリック・コメントの中で、意見申述者から、契約準拠法が日本法であることによって、国内規定が遵守できるかのような理解が示されている（厚労ガイドライン 5.1 版 103 番）。しかし、契約準拠法は国内規定とは無関係といえよう。確かに、契約の当事者は、あらかじめ当該契約の解釈において適用される法を合意しておくことができる（法の適用に関する通則法 7 条）。ここで定められる準拠法は、あくまでも当該契約やそれに関連する紛争についての民事紛争の実体的な側面を、当該準拠法に基づいて解釈するというに過ぎない。他方で、国内規定は、日本の主権と他国の主権との競合を問題としている。そもそも私人には、主権を処分する権限はないから[40]、日本国内の医療機関と外国にある事業者が、契約の準拠法として日本法を採用することに合意していたとしても、事業者所在国やサーバ設置国の主権や法規制を排除できるわけではない。

したがって、規制目的②に関連して、外国法の影響を懸念するのであれば、外国法の問題を正面から取り扱う必要がある。ところが、総務経産ガイドラインは外国法について言及しておらず、重要な規制手段が欠落している。

５．国内規定の見直しの方向性

５．１．国内規定の問題点と改正の方向性

これまで、国内規定に関する 3 省ガイドラインの沿革及びその内容・根拠を検討してきた。その結果、現在の国内規定の問題は以下のようにまとめられる。

国内規定は、3 省が述べる①医療従事者が作成保存義務を負う記録が行政による調査等に際して円滑に提出されることに加えて、総務経産ガイドラインのみが言及する②医療従事者の守秘義務違反の防止という 2 つの目的に基づく。これらの目的は、正当なものであるといえよう。

しかし、具体的な規制手段をみると、規制目的①については、主として厚労ガイドラインの中に、同目的に親和的な記載があるものの、関係者が遵守するべき要件が具体的に定めら

---

38 各国において、相手国の同意を得ない越境リモートアクセス捜査が普及しつつあることについて、石井由梨佳「国際法学の観点から―越境リモートアクセス捜査の評価」指宿=板倉編前掲注 36 171 頁以下。

39 Treasury Board of Canada Secretariat, Government of Canada White Paper: Data Sovereignty and Public Cloud (2020 年)
（https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html,令和 7 年 4 月 2 日最終閲覧）は、データを国境内に保管させることは、外国法の適用を緩和しない旨を指摘する。

40 横溝大「インターネットを通じた域外的証拠収集－執行管轄権との関係を中心に（上）」法曹時報 74 巻 8 号 1 頁、4 頁（2022）、川出敏裕「コンピュータ・ネットワークと越境捜査」酒巻匡=大澤裕=川出敏裕『井上正仁先生古稀祝賀論文集』411 頁、428 頁（有斐閣、2019）石黒一憲『現代国際私法　上』220-221 頁（東京大学出版会、1986）。

れておらず、規制手段が明確ではない。さらに、規制目的②については、総務経産ガイドラインには、日本法上許容できないような外国法の影響が及ぶことを排除するための手段が言及されていない。

では、これらの規制目的を実現するための手段としては、どのようなものが考え得るであろうか。本稿では、ここまで、規制目的①及び②を独立させてその内容を検討してきた。これは、それぞれの規制目的が結び付く「記録」と「秘密」という 2 つの概念を前提にした議論である。これらの概念を維持したままそれぞれの目的に合わせた規制手段を検討することもあり得るが、より統一的な制度設計ができるのであれば望ましいであろう。

そこで本稿は、「個人情報（個人データ）」に着目する。そもそも現在の 3 省ガイドラインは、冒頭で述べたとおり、医療介護ガイダンスを介して、個人情報保護法 23 条の安全管理措置の具体化としての性質も有している。確かに、3 省ガイドラインが、国内規定の根拠として個人情報保護法を挙げたことはなく、また総務経産ガイドラインのパブリック・コメントは、国内規定について、個人情報保護委員会との協議の必要性を否定している（総務経産ガイドライン 0 版 155 番）。しかしながら、個人情報保護法は、本当に規制目的①及び②に貢献しないであろうか。

５．２．ベースラインとしての個人情報保護法

５．２．１．国内規定の対象事項への個人情報保護法の適用可能性

まず、前提として「個人情報」と「記録」及び「秘密」の広狭について検討する[41]。外部保存通知が挙げる作成保存義務がある記録の中には、医療法上の定款や財産目録等そもそも個人情報ではないものが含まれるが、患者の情報という観点で見た場合には、患者の個人情報の一部が、作成保存義務がある記録の中に記載されているということになろう。すなわち、個人情報は「記録」内の情報を包含している。他方、「秘密」については、医師等が知りえた患者の情報のうち、どの範囲が秘密になるか学説がわかれる。しかし、どの説でも、守秘義務の対象となる秘密は、医師等にとって特定の患者を識別できる情報であることが求められると考えられるから、このような情報は医療機関にとっては患者の個人情報に該当する。つまり、秘密の範囲を広く解釈したとしても、個人情報と秘密の範囲は近接するものと解される[42]。したがって、個人情報は、記録を包含し、秘密も基本的に包含しているものと考えられる。

ついで、個人情報保護法のうち、本稿に特に関連するのは、23 条及び 28 条であり、これらは、個人情報のうち、「個人情報データベース等」を構成する個人データのみに適用され

---

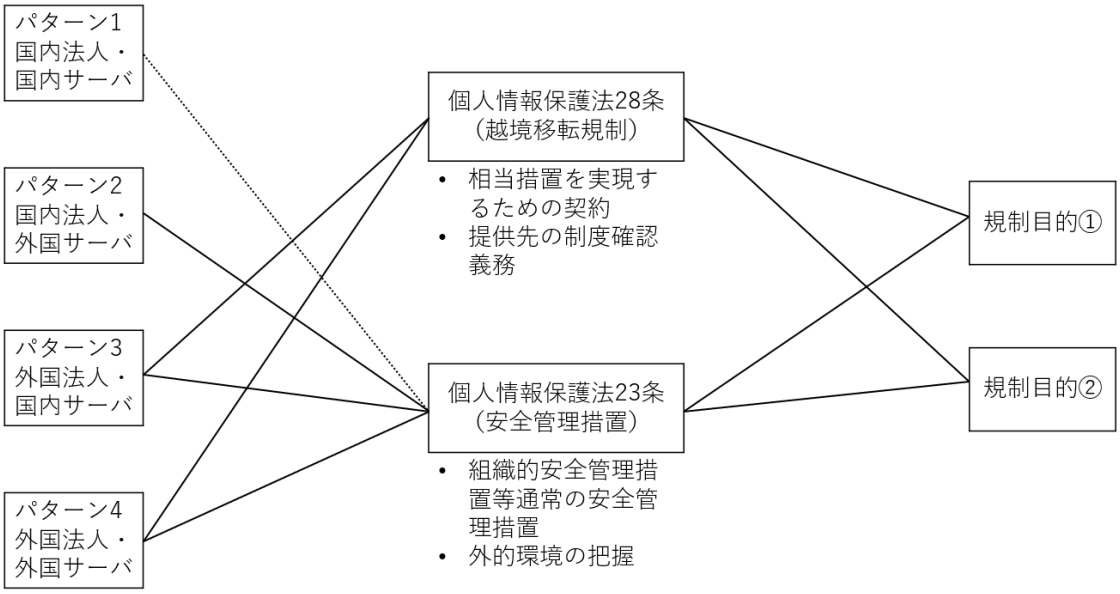
41 厳密には、3 省ガイドラインの対象情報は、「医療に関する患者情報（個人識別情報）を含む情報」と定義する「医療情報」とされているが（厚労ガイドライン 6.0 版概説編 1 頁、総務経産ガイドライン 1.1 版 6 頁）、個人情報保護法 2 条 1 項に定める「個人情報」との関係性は必ずしも明らかではない。とはいえ、医療機関が個人情報保護法の適用を受けることは明らかであるから、本稿では個人情報に着目し、「個人情報」と 3 省ガイドラインが述べる「医療情報」の異同には踏み込まない。

42 甲斐前掲注 24 60 頁は、「情報群の広狭を示すと、個人情報＞医療情報＞診療情報＞遺伝情報、ということになる。しかし、日本刑法 134 条 1 項が対象とする「秘密」は、これらのうち、多くの場合は医療情報・診療情報・遺伝情報に関係するであろうが、理論的には、必ずしもそれらに直結するとは限らず、広く個人情報（中略）を含むことになる」と述べる。

る。もっとも、3 省ガイドラインは、医療情報システムを規律しており、それらの中では、患者情報は患者個人を検索可能なデータベースの形で保管されていることが通常であることから、ひとまず患者情報のうち枢要なものは、個人データであると解釈してよいであろう（医療介護ガイダンス 19 頁参照）。さらに、個人情報保護法は、個人情報の「取扱い」を規制する。個人情報保護法は取扱いの定義を定めていないが、情報の保存のみならず、取得、編集や分析といった多様な行為を含んでいると一般的に理解されている[43]。したがって、個人情報保護法は、対象情報と対象となる行為の両面から見て、基本的に国内規定を包含する関係にあると解される。

3 節及び 4.3.3 節で述べた単純化されたモデルによれば、システムの運営者・サーバ設置場所について、(1)日本法人・国内サーバ、(2)日本法人・外国サーバ、(3)外国法人・国内サーバ、(4)外国法人・外国サーバという 4 パターンを想定できる。個人情報保護法は、これらの状況における外国の介在について、28 条の越境移転と 23 条の安全管理措置によって対応しており、いずれの規制内容も、国内規定の規制目的①②に貢献し得る。

図２．医療情報システムのモデル、個人情報保護法の規制及び
3 省ガイドラインの規制目的の関係



その関係を示せば図 2 のようになる。以下規制内容の詳細を検討する。

５．２．２．越境移転規制

医療機関が外国法人に対して患者の個人データの取扱いを委託すると、原則として、個人情報保護法 28 条の越境移転規制の対象となる[44]。越境移転には複数のルートが存在するが、

[43] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」(平成 28 年 11 月（令和 7 年 4 月一部改正）)3-4-4、同「「個人情報の保護に関する法律についてのガイドライン」 に関するＱ＆Ａ」（以下「個情法 Q&A」と呼ぶ。）Q2-3 参照。
[44] 例外的に、外国法人が「日本国内で個人情報データベース等を事業の用に供していると

医療機関が外国法人に取扱いを委託する場合には、通常、当該法人が日本法と同程度の保護措置（相当措置）を講ずる体制を整備していることを根拠に移転する（個人情報保護法 28 条 1 項 3 項）ことになる。具体的には、医療機関は、当該法人が日本法と同程度の措置を講じることを内容とする契約を締結する。委託先が委託元である医療機関の指示にしたがって取り扱うことや、医療機関の指示があれば、委託先が保管している情報を提供することは、当然に委託先の義務に含まれると解される[45]。これらの契約内容は、医療機関が日本の公的機関の要求を受けて情報を提供しようとする際に、委託先が医療機関の指示にしたがって提出することを確保することによって国内規定の規制目的①に、委託先が医療機関の指示がないにもかかわらず第三者に提供することを禁止することによって、国内規定の規制目的②に貢献し得る。

のみならず、個人情報保護法 28 条は、外国法に着目した制度も有している。具体的には、委託元は、委託先の相当措置の実施状況だけではなく、その「相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容」の確認義務を負う（個人情報保護法施行規則 18 条 1 項 1 号）。さらに、委託元は、外国の法制度の変更を含め、相当措置の実施の確保が困難になった場合には、委託先への提供を停止する義務を負う（個人情報保護法施行規則 18 条 1 項 2 号）。

そして、ガイドライン外国第三者提供編は、確認対象となる法制度の例として、「事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度」及び「事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度」を挙げる（6-1）。このうち、前者は、まさに国内規定の規制目的②が述べる、ガバメントアクセスに関する規定である。対して、後者は、個情委ガイドラインの文言からは明確ではないものの、個人情報保護委員会が外国について実施した制度調査[46]を見ると、例えば中国について、サイバーセキュリティ法等をあげた上で、「域外への情報の移転に際して、当局による安全評価に合格することが要件とされている場合があり、事業者が本人からの開示請求に十分に対応できないおそれがある」とする[47]。このような記載からすれば、外国法のデータローカリゼーションによって、日本国内への円滑な情報提供が困難となるような場面を懸念したものであり、これは国内規定の規制目的①と合致する。

もっとも、個人情報保護法 28 条の相当措置は、必ずしも上記のような懸念がある法制度を有する国への移転を直ちに禁止するものではなく、実際の運用状況等を踏まえて個別に移転の是非について判断するものとされる（個情法 Q&A Q12-17）。

認められる場合には」、当該外国法人は日本国内の個人情報取扱事業者と評価され、越境移転規制の対象とはならない（個情法 Q&A Q12-4）。

45 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（平成 28 年 11 月（令和 7 年 4 月一部改正））（以下「ガイドライン外国第三者提供編」と呼ぶ。）4-2-1、4-2-2 等。

46 個人情報保護委員会「諸外国・地域の法制度」（https://www.ppc.go.jp/enforcement/infoprovision/laws/,令和 7 年 4 月 2 日最終閲覧）。

47 個人情報保護委員会「外国制度（中華人民共和国）」（https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_china/,令和 7 年 4 月 2 日最終閲覧）。

５．２．３．外的環境の把握義務

ついで、個人情報保護法 23 条の規制を確認する。医療機関は、個人情報保護法 23 条に基づき、自己が取り扱う個人データについて安全管理措置を実施する義務を負う。この義務は自己が直接管理する個人データだけではなく、第三者に管理させた自己のデータについても及ぶとされる（個情法 Q&A Q7-54、Q10-24）。

個人情報保護法は安全管理措置の内容について具体的に示していないが、個情委ガイドラインは、組織的安全管理措置や人的管理措置などの項目ごとに複数の実施すべき対策例を挙げている。国内規定の規制目的①に関連して、医療機関が第三者に委託して個人データを取り扱わせたにもかかわらず、当該委託先が医療機関の要請にもかかわらず引き渡しを拒否している場合には、可用性が侵害されていると言い得るし、規制目的②に関連して、医療機関が認識しないままに委託先が外国政府の要請に応じて情報を提供していれば、機密性の侵害になり得る。したがって、医療機関が、委託先との契約等を用いて、こうした事態を防止するための措置を講じていなければ個人情報保護法 23 条に違反したと評価され得るであろう。

さらに、個人情報保護法 23 条は、「外的環境の把握」と呼ばれる義務を置いている（ガイドライン(通則編) 10-7）。これによれば、「個人情報取扱事業者が、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じ」る義務を負っている。この義務で把握すべき法制度や、把握した場合に何をなすべきかは必ずしも明確にされていないが、個人情報保護法 28 条の相当措置と同様のものであると考えられる [48]。

このようにみると、個人情報保護法 23 条から導かれる義務は、移転規制の義務とそれほど変わらず、むしろあいまいである分だけ重要性が低いかのようにも見える。

しかし、個情法 Q&A 等からは、個人情報保護法 23 条の「外的環境の把握」義務を含む安全管理措置の適用範囲は、個人情報保護法 28 条よりも広いことがうかがえる。まず、個人情報保護法 28 条の制度把握は、基本的に移転先（委託先）の法人設立国にフォーカスしているのに対し（個情法 Q&A Q12-11）、個人情報保護法 23 条の外的環境の把握義務は、個人データの取扱いが発生する国として、サーバ設置国や、リモートアクセス元の国までが対象となる（個情法 Q&A Q10-23、Q10-25）。外的環境の把握義務以外の安全管理措置の義務も同様に広く適用されると考えられよう。さらに、日本の個人情報保護法では、ある事業者が別の事業者に対して物理的に情報を移動したとしても、当該別の事業者が「個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならない」という、いわゆる「クラウド例外」と呼ばれる解釈論がある [49]。そして、日本国内の事業者から海外の事業者への情報の移動が、このクラウド例外に該当する場合には、そもそも法的には海外事業者に「提供」したと評価されないため、個人情報保護

[48] 岡田淳ほか『個人情報保護法』203 頁（商事法務、2024）は、「ガバメントアクセス等の本人の権利利益に重大な影響を及ぼす可能性のある制度を把握する必要がある」とする。
[49] 個情法 Q&A Q7-53、小川智史「実務問答個人情報保護法　第 1 回　クラウド例外」NBL1250 号 4 頁、11 頁（2023）、松尾剛行「生成 AI と個人情報保護法(クラウド例外を含む個人データの第三者提供を中心に)」一橋研究第 49 巻 2 号 19 頁以下（2024）、前掲注 48 岡田 319 頁以下。

法 28 条は適用されない。しかし、この場合であっても、国内事業者は、外国において個人データを取り扱っていることから、個人情報保護法 23 条に基づく安全管理措置を講じる義務があり、その中には外的環境の把握義務も含まれる（個情法 Q&A Q7-54、Q10-25）。このように、安全管理措置の義務は、越境移転規制を補完する機能を果たしている。

５．２．４．小括

以上のとおり、個人情報保護法は、記録や秘密を包含し得る概念である個人データの外国における取扱いに関し、越境移転や安全管理措置という規制によって、外国での取扱いが日本の個人情報保護法に適合したものとなるように義務付けるとともに、国内規定の 2 つの目的をカバーする広範な外国制度の調査義務や、調査の結果リスクがある場合には取扱いを差し控える義務を置くことで外国法の影響も考慮している。

その義務が及ぶ範囲を見ると、(1)日本法人・国内サーバ、(2)日本法人・外国サーバ、(3)外国法人・国内サーバ、(4)外国法人・外国サーバという 4 パターンのうち、(3)及び(4)については、越境移転及び安全管理措置の双方が関連し、(2)については、安全管理措置が関係する。さらに、(1)から(4)の全てのシナリオにおける外国からのリモートアクセスについては、安全管理措置規制が及び得る。このように、3 省ガイドラインの国内規定に比して、個人情報保護法は、はるかに多くのシナリオに対して明確な規制を及ぼしている。

このほか、個人情報保護法 171 条は、個人情報保護法が域外適用されることを定めるが、個人情報保護委員会は海外の委託先に対して個人情報保護法が域外適用される可能性も認めている（個情法 Q&A Q11-4）。この場合、実効性はともかくとしても、委託先が、規制目的①が懸念するように、委託元の指示に反して個人情報を提供しないこと、又は規制目的②が懸念するように、我が国から見て正当ではない外国の法制度による情報収集に協力することは、当該委託先自体が個人情報保護法に違反することになり得る。

2 節の国内規定の沿革で述べたとおり、国内規定の初出は 2009 年の総務医療ガイドラインである。この当時の個人情報保護法には、そもそも国外への移転に関する規定がなかった。その後、個人情報保護法が、2015 年に改正された際に、当時の 27 条として移転規制が追加されたものの、この時点でも上記のような制度調査の観点は定められていなかった。しかし、個人情報保護法の 2020 年改正の中で、越境移転に関する制度調査義務が追加され、また安全管理措置の中の外的環境の把握義務は、2020 年改正法の施行に合わせてガイドラインに追加された。そして、これらのルールは個人情報保護法の 2021 年改正によって、国公立の医療機関にも明示的に適用されるようになった。

すなわち、個人情報保護法の制度は、歴史的には国内規定にかなり遅れて整備が始まったが、現在でははるかに整備された詳細な内容を有している。したがって、ベースラインである個人情報保護法を前提にした上で、上乗せの制限を行う必要があるかという観点で、国内規定を全面的に見直すことが適当であろう。筆者としては、国内規定を廃止し、個人情報保護法 28 条及び 23 条の規律にゆだねることもあり得ると考える。

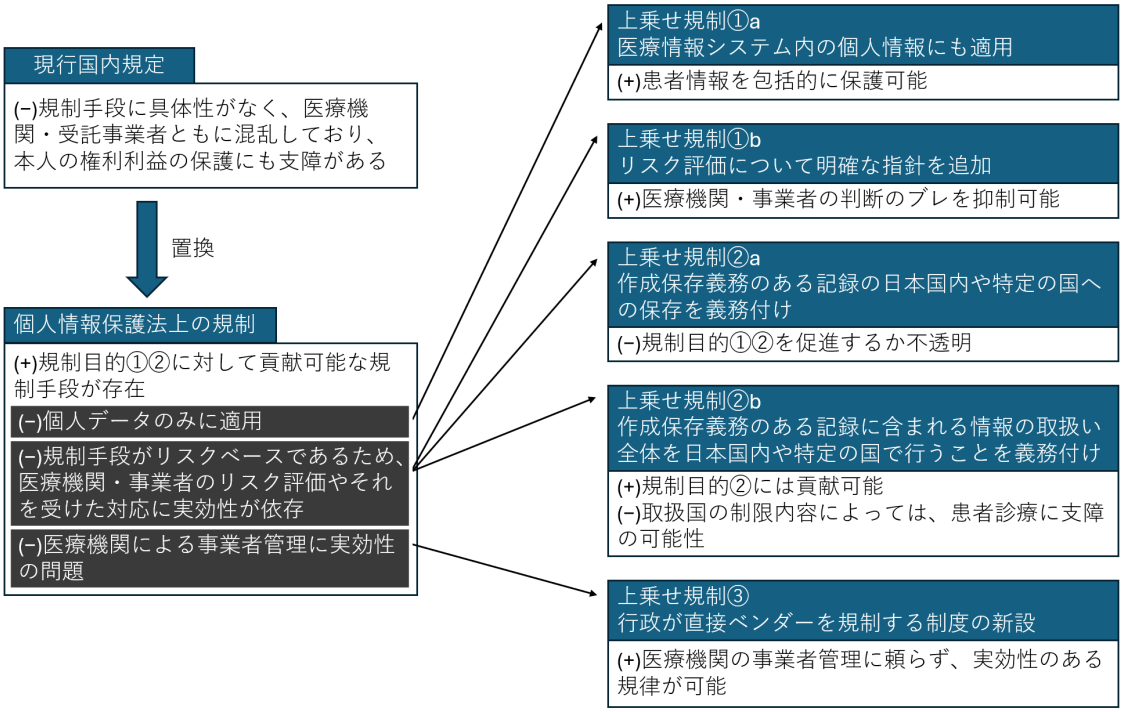
５．３．追加的規制の可能性

５．３．１．想定される追加的規制

他方で、追加的な規制の余地もある。具体的には、大きく、①個人情報保護法の延長とし

ての追加的規制、②3 省ガイドラインの現行の国内規定をベースにした追加的規制、③医療情報システムそのものを対象とする新しい法制度の 3 つが想定し得る。図 3 は、現行国内規定から追加的規制に至る関係性を示したものである。

図３．現行国内規定、個人情報保護法上の規制及び追加的規制の関係



５．３．２．個人情報保護法の延長での追加的な規制の可能性

個人情報保護法の制度の延長では、2 つの追加的規制が考え得る。まず、個人情報保護法 23 条及び 28 条は、個人データにのみ適用される。電子カルテのように、医療情報システムに保存された大半の患者情報は個人データに該当すると考えられるが、個人データではない個人情報が含まれる可能性もある。このため、医療情報システム内の患者情報が個人情報でしかない場合にもこれらの条文を適用するよう、3 省ガイドライン等で明記することはありえる。すでに、医療介護ガイダンスは、死亡した患者情報にも生存している患者と同等の安全管理措置を確保するように規制を拡張しており（3 頁）、これと同種の発想である。

また、前述のとおり 28 条は、規制目的①②を阻害する可能性がある外国法が存在することだけをもって、当該国への移転を禁止しているわけではない。同様に 23 条の外的環境の把握義務も、把握した結果として何をすればよいのかは必ずしも明確ではない。このため、リスク評価と対応を明確化することがありえる。例えば、作成保存義務のある記録については、個人情報保護委員会や各個人情報取扱事業者が実施する制度調査において、規制目的①②に関係する懸念がある法制度があるとされた国については、当該国からのリモートアクセスを含め、医療機関により慎重な判断を求める、場合によっては特定の国が関係する取扱いについてはリスクを回避できないとして取扱いを禁止するといったことが考えられる。

５．３．３．国内規定の明確化としての追加的な規制の可能性

このほか、現行の国内規定を、内容を再度明確化した上で、法やガイドラインに基づき義務付けるかどうかも議論の余地がある。

まず、現行の国内規定に関する根強い理解である、国内「保存」を明確化することがあり得る。さらに、作成保存義務のある記録の国内保存を超えて、記録に含まれる情報について、そのコピーを含め取り扱いを日本や特定の国に限定する、あるいは作成保存義務の有無にかかわらず、およそ患者の個人情報の取り扱いを日本や特定の国に限定するといった制度も構想し得る。前節で述べた個人情報保護法をベースにした上乗せ規制の構想が、ブラックリスト方式でリスクの高い特定の国での取扱いを禁止するというものであったのに対し、ホワイトリスト方式をとり特定の国でのみ取扱いを許容するという制度設計である。

西側諸国の医療分野においても、これらの構想と類似の規制が見られる。例えば、英国のNHS（National Health Service）イングランドは、傘下の組織に対して、クラウドサービスを用いた医療情報の取扱いを、事実上イギリス国内のほか、EU を中心とした特定の国に限定するように求めている[50]。さらに、オーストラリアにおける国単位の電子健康記録サービスである、My Health Record を規律する My Health Record Act77 条も、同様に国内での取扱い規定を有している。また、最近では、2025 年に欧州連合で制定された European Health Data Space 規則 86 条が、EU 加盟国が、医療提供者による医療提供に関する医療情報の保存を EU 域内に制限する国内法を制定することを認めていることも注目される[51]。

しかし、諸外国に類例があり、またこれまで国内規定を、国内「保存」規定と解釈する向きが根強くあるとはいえ、このような規制を追加することには慎重であるべきであろう。

まず、作成保存義務がある記録を、国内や特定の国で保存することを求めるというルールの場合、その義務付けは不可能ではないであろうが、そのルールの効果には限界がある。まずもって、4.3.4 節のとおり、国内保存を義務付けても、その取扱いを行う事業者を制限しなければ、外国政府が、外国事業者や、それに関連する日本法人等を通じて国内に保存されたデータにアクセスする可能性を否定できず、規制目的②との関係で有効とは言いづらい。また、規制目的①との関係では、確かに委託先事業者が情報の提出を拒否した場合、情報が国内保存されていれば、捜査当局による情報が保存されているサーバの差押えなど、一部の捜査手法が可能になることは事実であるが、そもそも医療機関から作成保存義務のある記録の保存を受託している事業者が、ことさらに情報の提出を拒否する独自の利益を持つとは考えにくい。したがって、規制目的①及び②双方との関係で、規制が解決しようとする課題と解決手段が釣り合っているのか疑問があるといえよう。

他方で、より広く、保存のみならず、取扱国や取扱法人を制限するルールを採用すれば、規制目的②との関係で実効性は高まるとはいえよう。しかし、現時点でも、患者の個人情報

---

[50] National Health Service “NHS and social care data: off-shoring and the use of public cloud services Guidance” (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/guidance,令和 7 年 4 月 2 日最終閲覧).

[51] Article 86 of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance).

が海外で取り扱われることは決して珍しくない。例えば、海外で検体検査が実施されていることがあるほか、グローバルで販売されている医療機器について、日本国内で販売された医療機器から収集された患者の情報が、国外のサーバで他国の患者と合わせて一元管理されているといった状況がある。今後、こうした傾向はますます加速することが想定される。このため、こうした広範な取扱い場所の規制の導入を検討する場合には、日本における医療提供の支障となるリスクをも踏まえて慎重に設計する必要がある。

５．３．４．医療情報のベンダーへの規制の可能性

日本では、医療情報システムそのものに特化した法規制はない。このため、独立した業法として、医療情報システムのうち重要なものについて、規制立法を行い、国内外の事業者を統制下に置くことも考えられる。現在の 3 省ガイドラインの基本思想は、医療法等で統制を受ける医療機関が、医療情報の取扱いを委託している医療情報システムの事業者をコントロールするというものである。しかし、現実的には、医療機関側には、技術面・体制面を含め限界があり、必ずしも実効的なコントロールが行われる保証はない。また、患者向けのソフトウェア医療機器などの場合には、そもそも医療機関が医療情報システム事業者に医療情報を委託するという基本的な構図自体が該当しなくなってきている。したがって、日本国内で重要な医療情報サービスを提供する国内外の事業者に対して、届出義務を課して実態を把握するとともに、行政による調査等が可能な制度を構築することは一考に値しよう。

６．結語

本稿は、3 省ガイドラインに含まれる国内規定の沿革と性質を検討し、「記録」と「秘密」という 2 つの概念に結び付いた 2 つの目的が提示されていること、それらの目的は正当であると考えられるが、3 省ガイドラインは具体的な遵守条件を提示できていないことを明らかにした。その上で、個人データに着目し、個人情報保護法上の現行の越境移転規制や外的環境の把握義務に依拠することで、特別のルールを設けずとも、より明確かつ実効的な規制が実現される可能性を指摘した。さらに、個人情報保護法の基本ルールに加えた上乗せ規制の可能性についても、複数のシナリオの可能性を検討した。

謝辞

本稿は，京都大学大学院法学研究科附属法政策共同研究センター医療と法ユニット「医療 DX と法的課題研究会」における報告を基礎としており、ご参加の先生から貴重な意見をいただいた。また、黒田知宏先生（京都大学）、武田理宏先生（大阪大学）、音無知展先生（京都大学）から個別に貴重なご意見をいただいたことに合わせて感謝申し上げる。

（掲載決定日：令和７年 10 月 23 日／オンライン掲載日：令和７年 12 月 23 日）