2020.11.18 医療ISAC デジタル・フォレンジック研究会「医療」分科会 共催

「医療機関向けランサムウェア対応検討ガイダンス」の解説

ランサムウェアへの セキュリティ対応の法的側面

田辺総合法律事務所
弁護士 吉峯 耕平

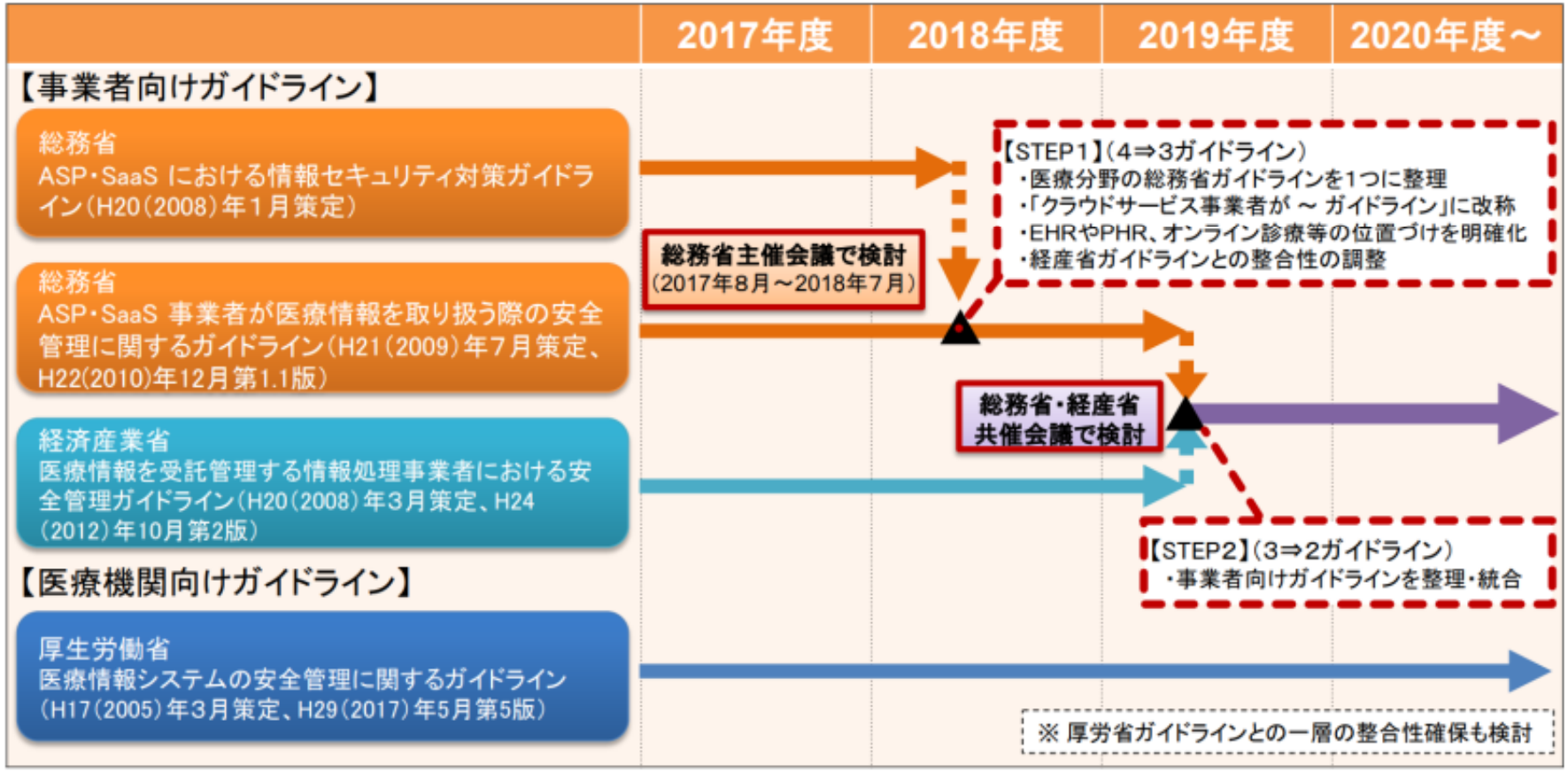
1. セキュリティの基準

2. ランサムウェアへの法的対応

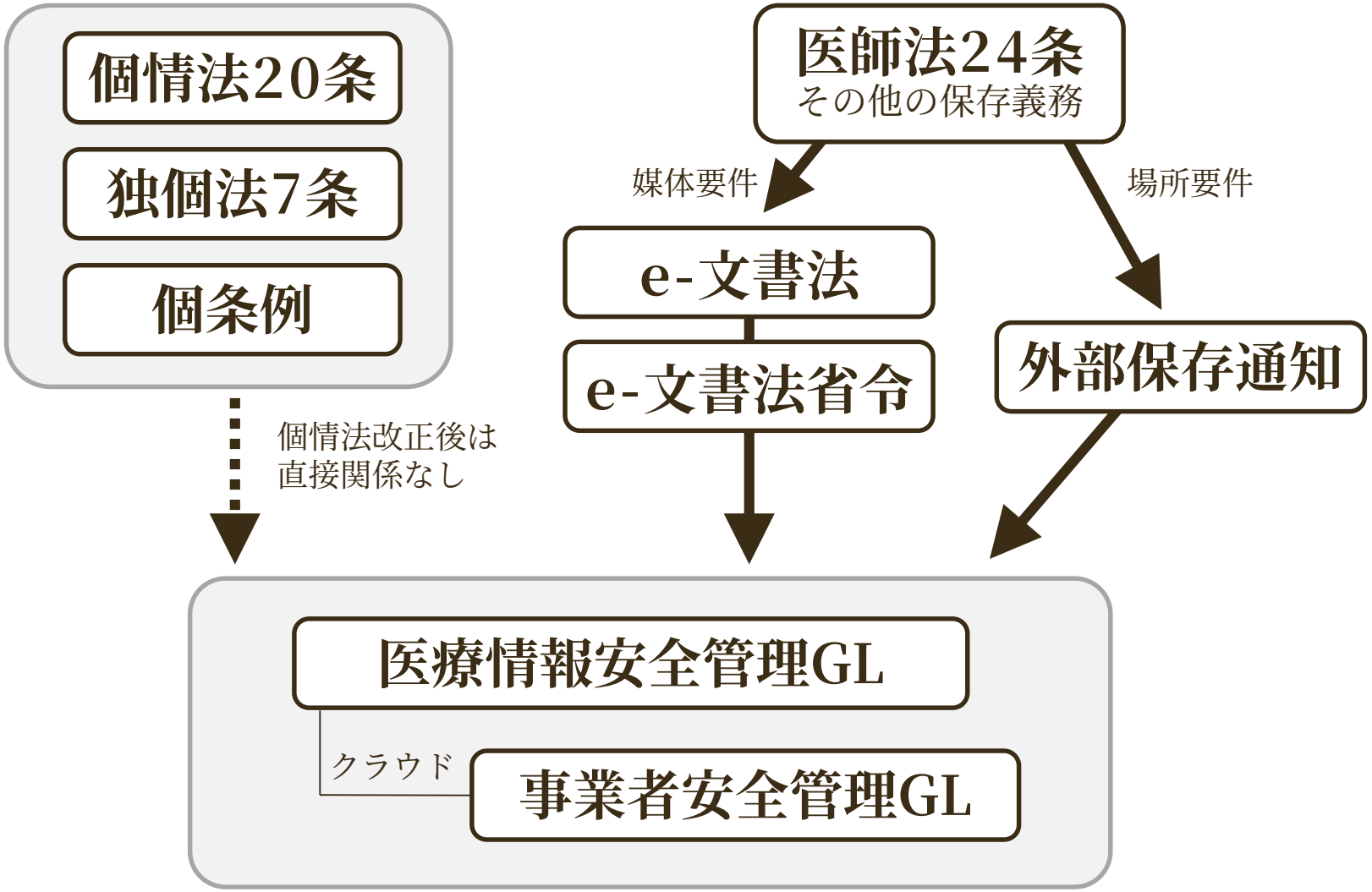
医療情報安全管理関連ガイドライン検討ロードマップ

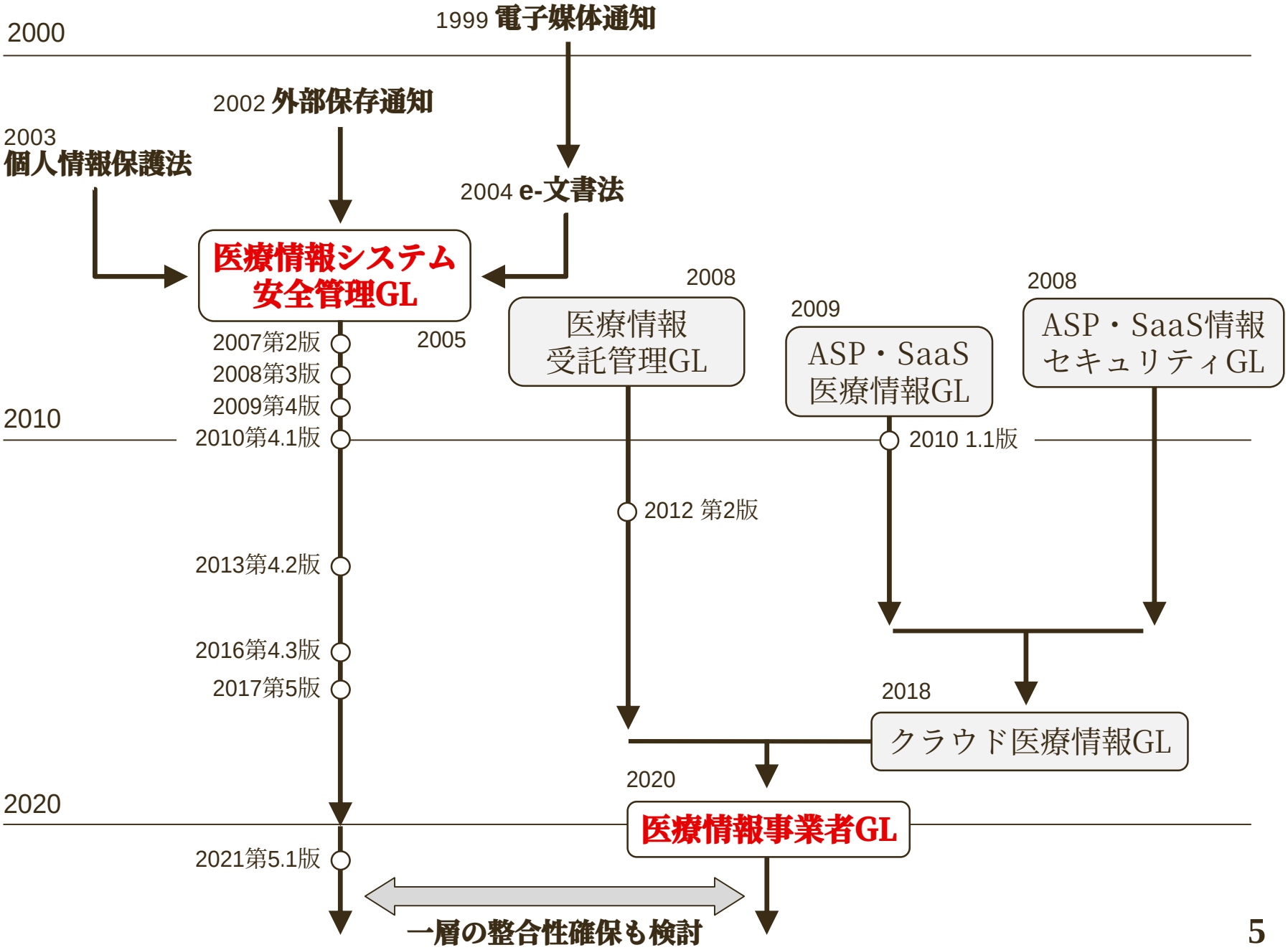
別紙４

- 現在、医療情報の安全管理については、３省の４つのガイドライン（いわゆる３省４ガイドライン）により、必要な対策等を規定。
- 特に事業者向けのガイドラインは３つあり、それぞれ策定・改定時期や対策の記述観点も異なるため、医療機関に対して（情報処理やASP・SaaSを含む）総合的なサービスを提供する場合は、厚労省ガイドラインを含む全てのガイドラインを確認し対策を行う必要があり、大きな負担。
- これらのガイドラインが求める要件を整理し、利用者視点で（段階的に）統合することにより、クラウドサービス事業者等が遵守すべきガイドライン要求事項を理解しやすくし、より確実な対策の実施を図り、医療情報の効果的・効率的な安全管理を推進。



3省2ガイドラインと法律の関係




2000
1999 電子媒体通知
2002 外部保存通知
2003
個人情報保護法
2004 e-文書法
医療情報システム
安全管理GL
2005
2007第2版
2008第3版
2009第4版
2010第4.1版
2010
2008
医療情報
受託管理GL
2012 第2版
2009
ASP・SaaS
医療情報GL
2010 1.1版
2008
ASP・SaaS情報
セキュリティGL
2013第4.2版
2016第4.3版
2017第5版
2018
クラウド医療情報GL
2020
2020
医療情報事業者GL
2021第5.1版
一層の整合性確保も検討

医療情報安全管理GLの項目

組織安全管理対策（6.3）

①組織体制整備
②規程等の整備と運用
③医療情報の取扱台帳の整備
④安全管理対策の評価、見直し及び改善
⑤情報や情報端末の外部持ち出しに関する規則等の整備
⑥リモートアクセス端末等の管理規程
⑦事故又は違反への対処

技術的安全対策（6.5）

①利用者の識別・認証
②情報の区分管理とアクセス権限の管理
③アクセスの記録
④不正ソフトウェア対策
⑤ネットワーク上からの不正アクセス
⑥医療等分野におけるIoT機器の利用

物理的安全対策（6.4）

①入退館管理
②盗難、覗き見等の防止
③機器・装置・情報媒体等の物理的保護措置（盗難、紛失防止）

人的安全対策（6.6）

ア　従事者への安全管理措置
①秘密保持契約
②定期的な教育訓練
③退職後の守秘義務
イ　委託業者への安全管理措置
①秘密保持契約
②作業者・作業内容・作業結果の確認（医療情報システムにアクセスする場合）
③作業後の定期的なチェック（医療情報システムにアクセスしない場合）
④再委託の安全対策

その他

・情報の破棄（6.7）
・情報システムの改造と保守（6.8）
・情報及び情報機器の持ち出し（6.9）
・災害、サイバー攻撃等の非常時の対応（6.10）
・外部と個人情報を含む医療情報を交換する場合の安全管理（6.11）

事業者ガイドラインの目次概要

プライバシーと個人情報保護法制

個人の権利利益

プライバシー権
名誉権その他の人格的利益
経済的利益
……

個人情報保護法制

主体ごと

- 個人情報保護法 — 民間企業・私立大学
- 独立行政法人個人情報保護法 — 国立病院・国立大学ナショナルセンター
- 個人情報保護条例 — 公立病院

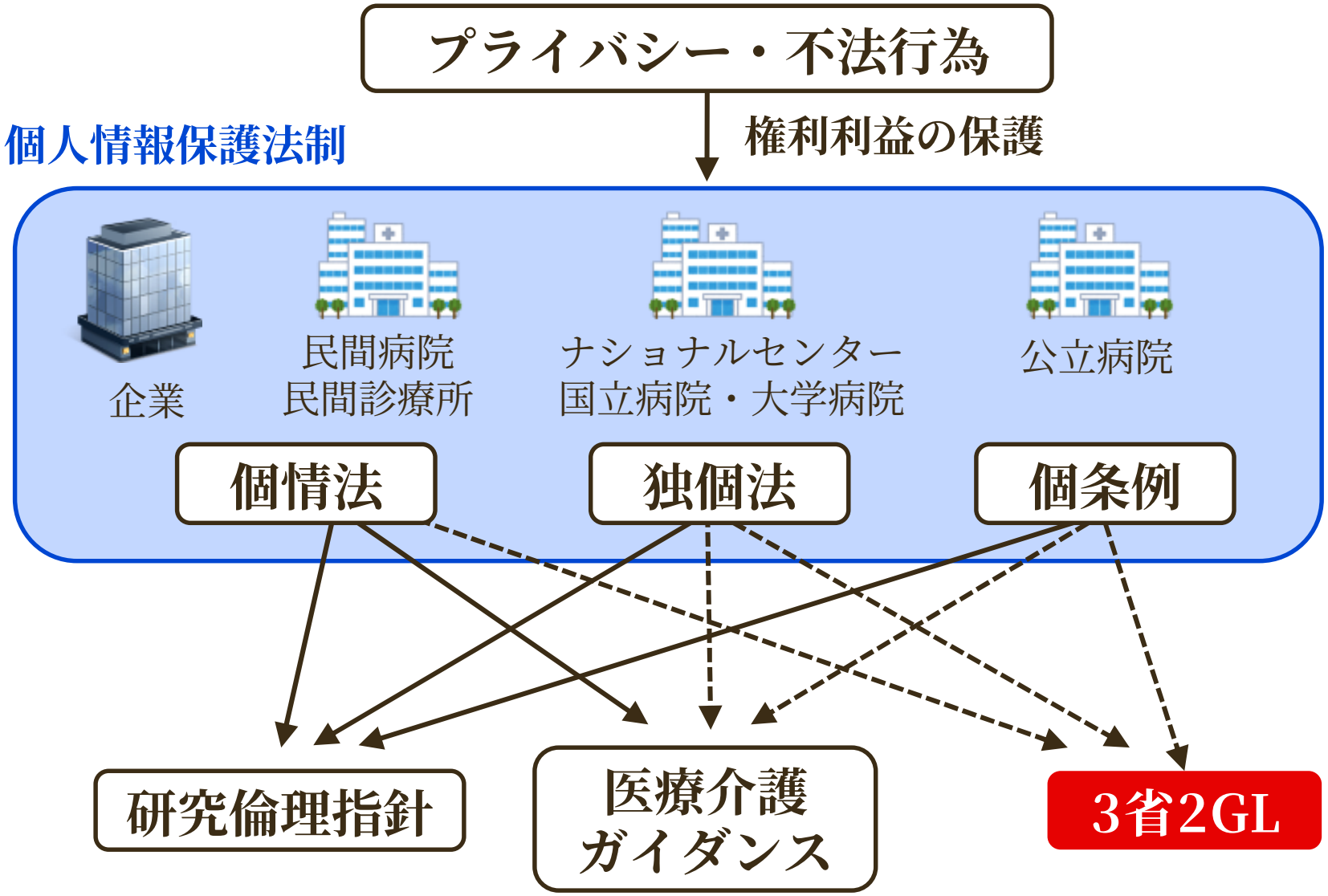
令和3年改正で個情法に一本化

プライバシーは民法の世界

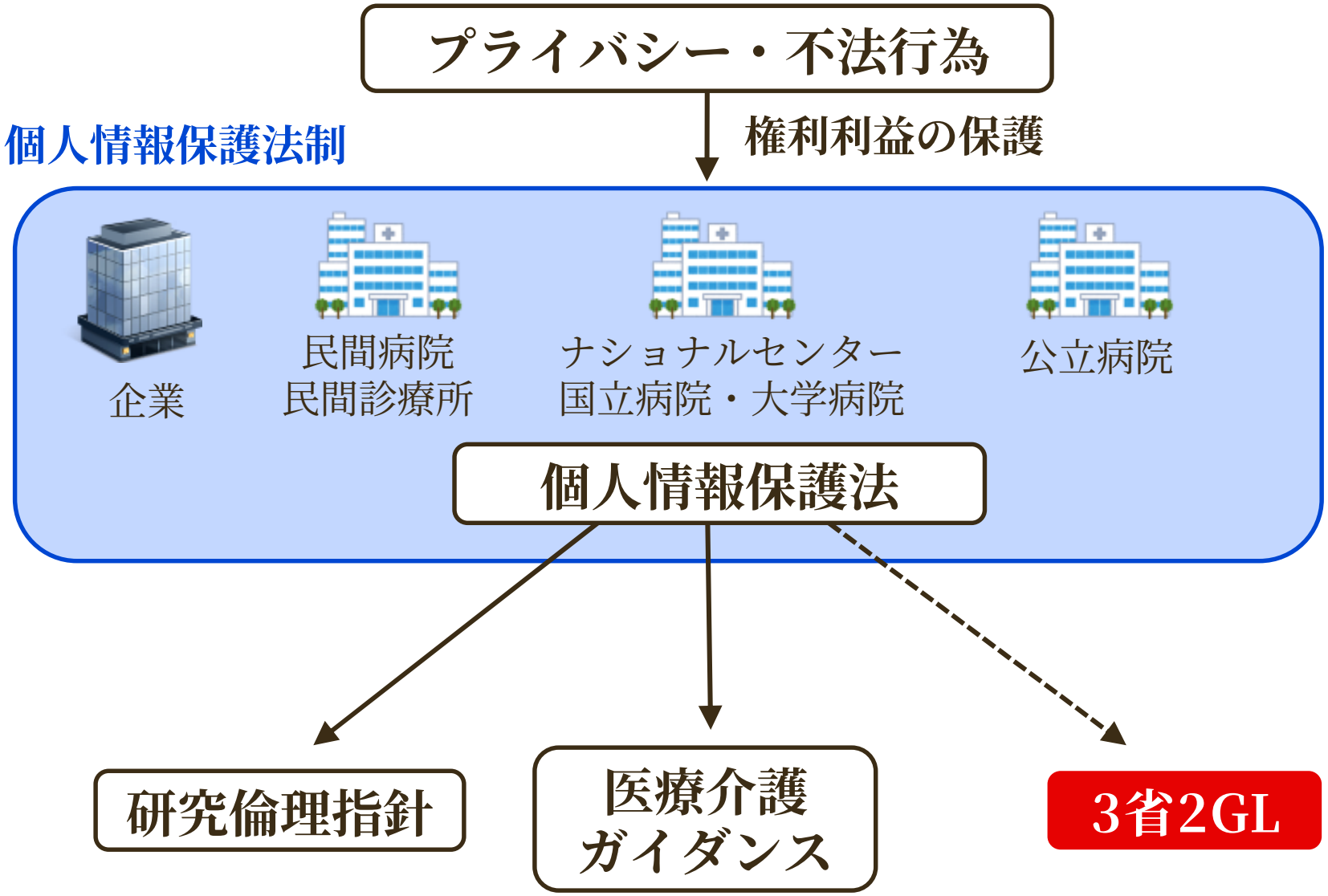
（不法行為による損害賠償）
第七百九条　故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。

- 基本的に明文のルールはこれだけ
- 裁判所が柔軟に解釈する
- 個人情報保護法制と比べて実質的

医療・医学研究分野全体での位置づけ



令和3年改正（三法統合）の後



個人情報保護法のルールとセキュリティ基準

プライバシーのルール

取得のルール	個人情報	個人情報
利用目的のルール	個人情報	保有個人情報
第三者提供のルール	個人データ	保有個人情報
開示・訂正のルール	保有個人データ	保有個人情報

セキュリティのルール

安全管理措置	個人データ	保有個人情報

⇨ 基準

適切かつ必要な措置

セキュリティ関係の条文

個人情報保護法

（安全管理措置）

第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の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なければならない。

（従業者の監督）

第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

（委託先の監督）

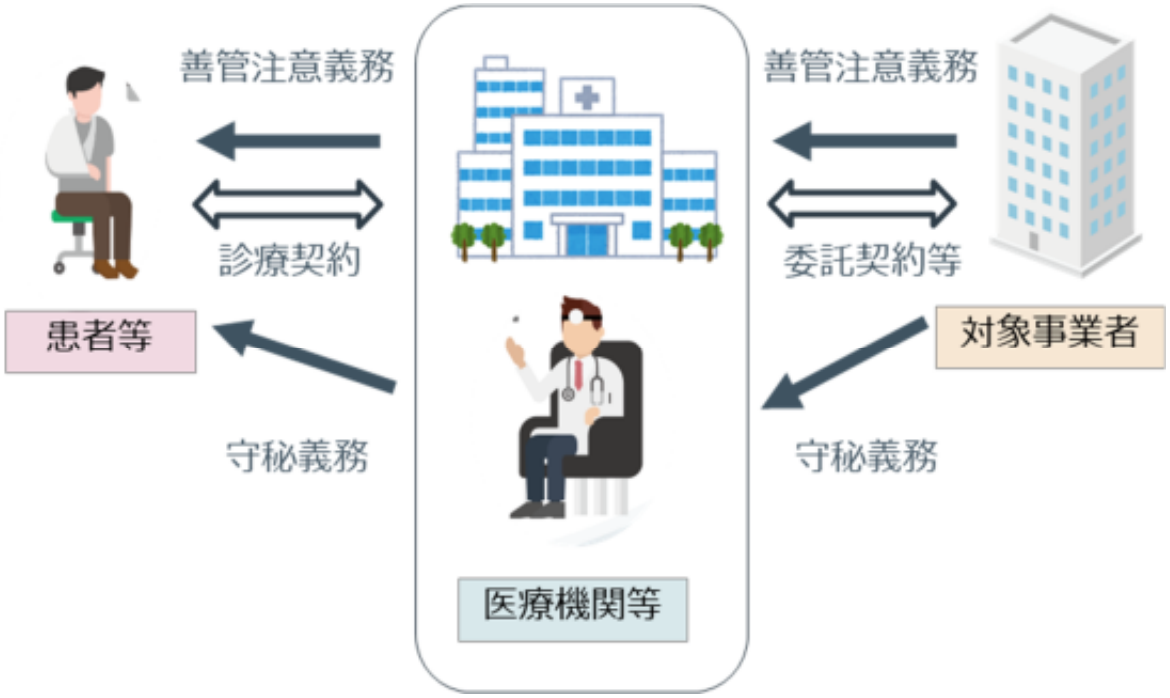
第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

独立行政法人個人情報保護法

（安全確保の措置）

第七条　独立行政法人等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。

事業者GL図3 善管注意義務と守秘義務



- 安全管理義務・民事責任は診療契約・委託契約上の善管注意義務と守秘義務に由来する

3つの「責任」

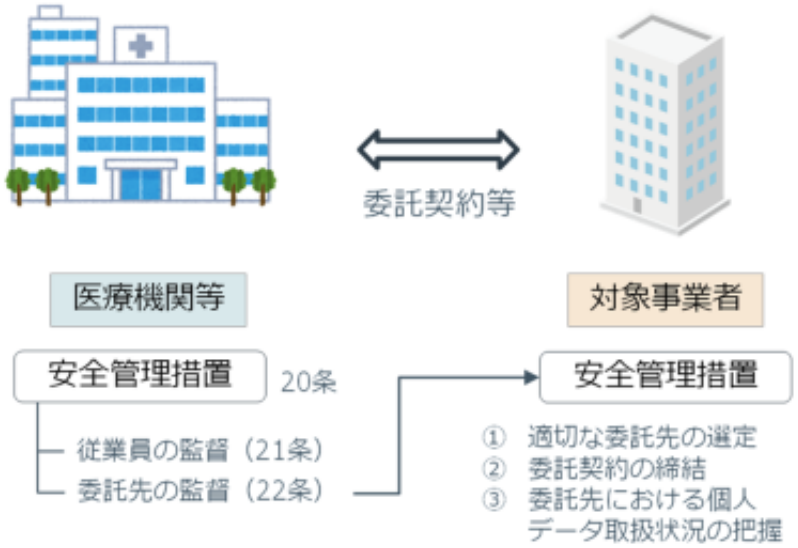
Accountability いわゆる説明責任

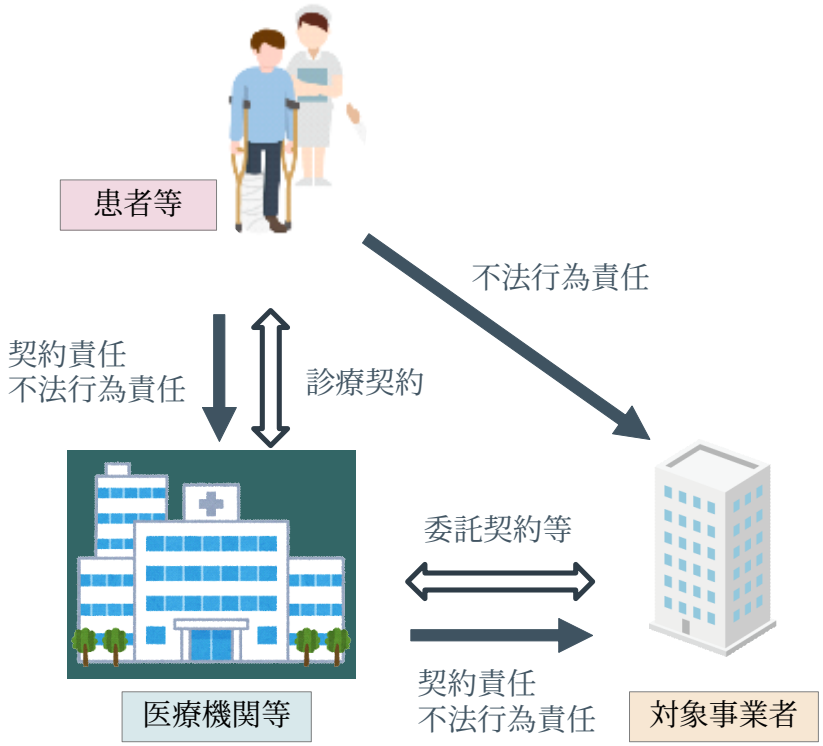
Responsibility 安全管理義務

⇩ 義務違反

Liability 事後的な責任（民事責任）

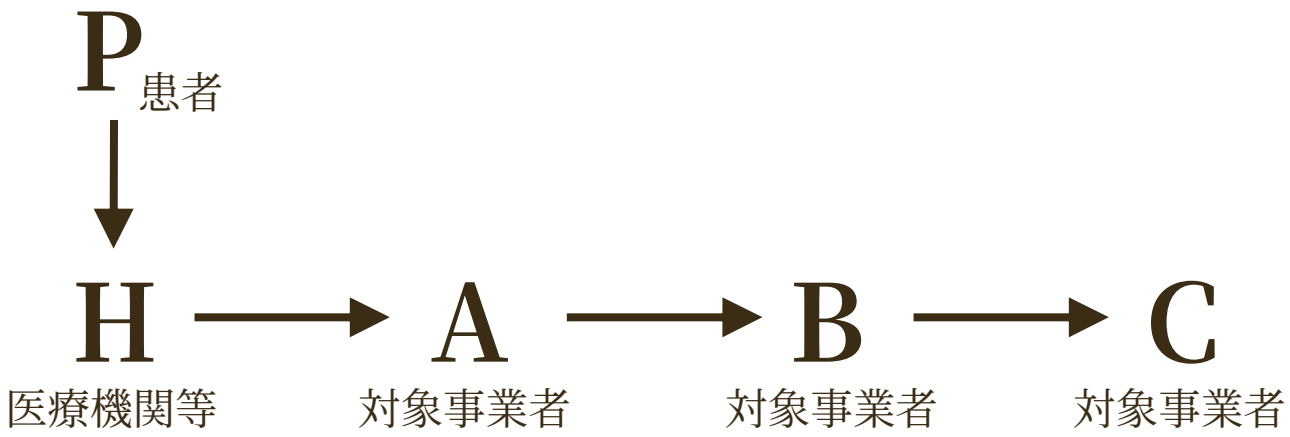
安全管理義務と民事責任

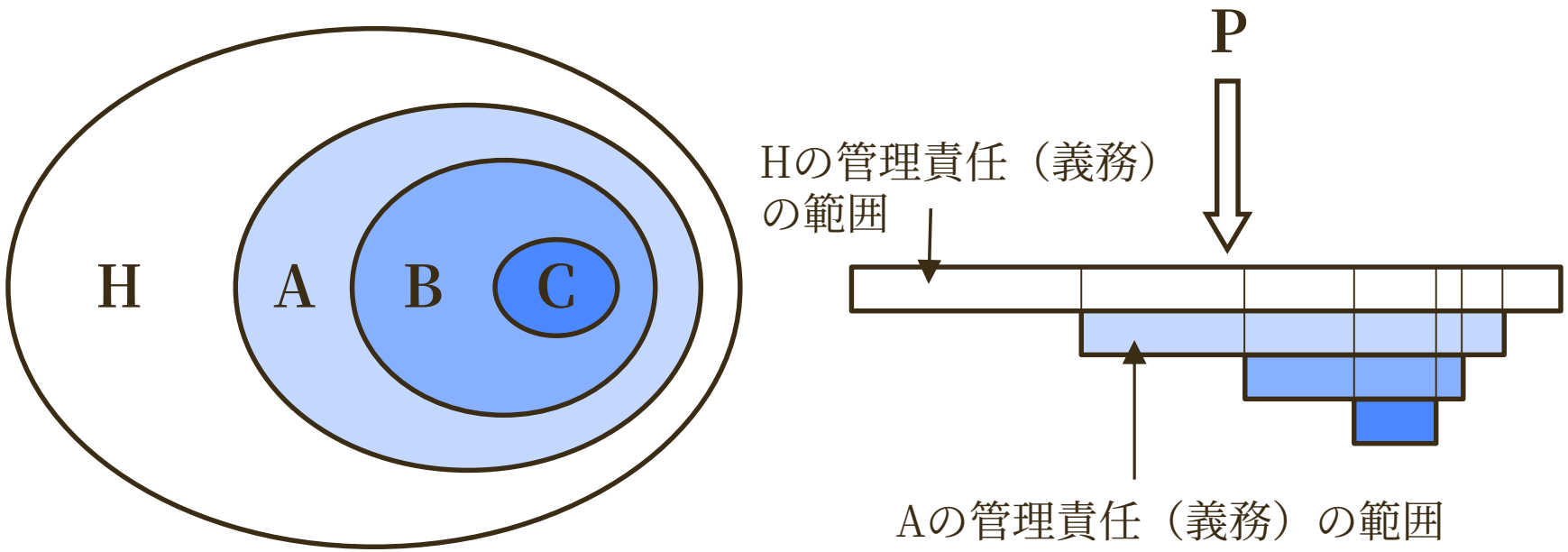




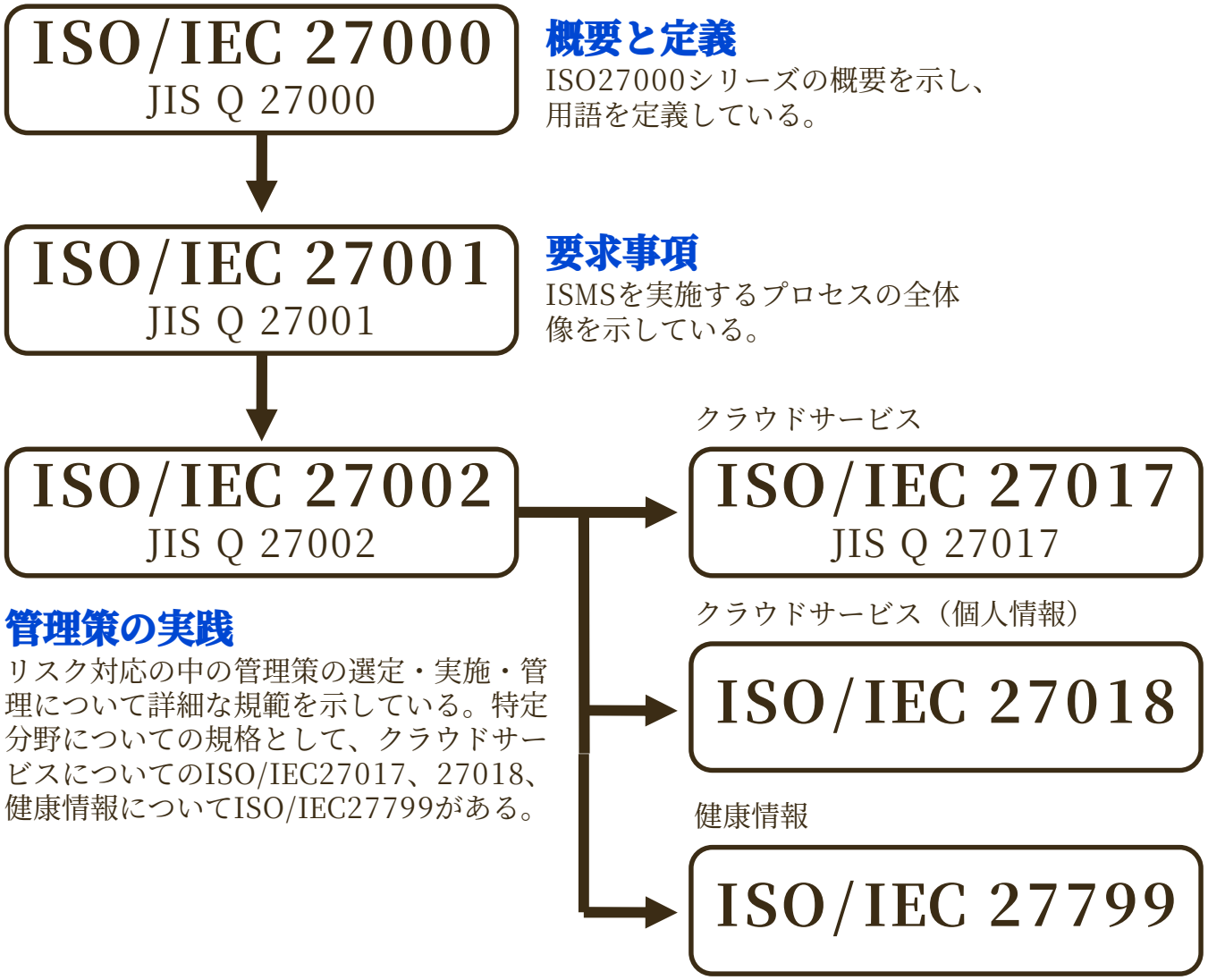
- 安全管理義務も民事責任も、重複する
- 責任分界とは、委託元の単独分担と委託元・受託先重複分担の境界である

責任分界（点）の概念・イメージ





安全管理義務の内実 —— ISMSの国際規格



情報セキュリティマネジメントのサイクル

①基本方針の策定

情報セキュリティリスクに対する基本方針を定める。

②リスクアセスメント

組織の保有する資産（情報）をリストアップして、リスクを特定する。リスクの大きさ（影響の程度×発生可能性）を分析し、受容可能かどうかを決定する（リスク評価）。
リスク特定→リスク分析→リスク評価のプロセスを、リスクアセスメントと呼ぶ。

③リスク対応

リスクへの対応（Risk Treatment）を決定する。一般的には、①管理策（Control）の適用、②リスク受容、③リスク回避、④リスク移転の選択肢があるとされる。管理策は、ISO/IEC 27001附属書Aに、管理目的と対応してリストアップされている。

④継続的改善

情報セキュリティ体制は、PDCAサイクル等によって、継続的に改善することを要する。そのために、マネジメントレビューや監査も必要となる。

対象事業者の説明義務

医療機関等と事業者（元請・下請）において、契約がルールとなるのが原則

⇩

個情法も適切な契約を通じた委託者の監督を求めている

合意形成が極めて重要

⇩

医療機関等は情報セキュリティの専門性を有さないため、事業者の情報提供・協力が必須

対象事業者の説明義務

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

※①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握

行政機関のガイドラインにおいて委任契約または信義則に基づく説明義務の存在を明記したもので、かなり踏み込んだ記載