資料7

第４回医療評価委員会資料

医療情報システムに関連する各種ガイドライン等の概要及びその関係性

１．個人情報保護法制等の執行指針としての体系イメージ

２．各ガイドラインの概要

３．各ガイドラインの位置関係

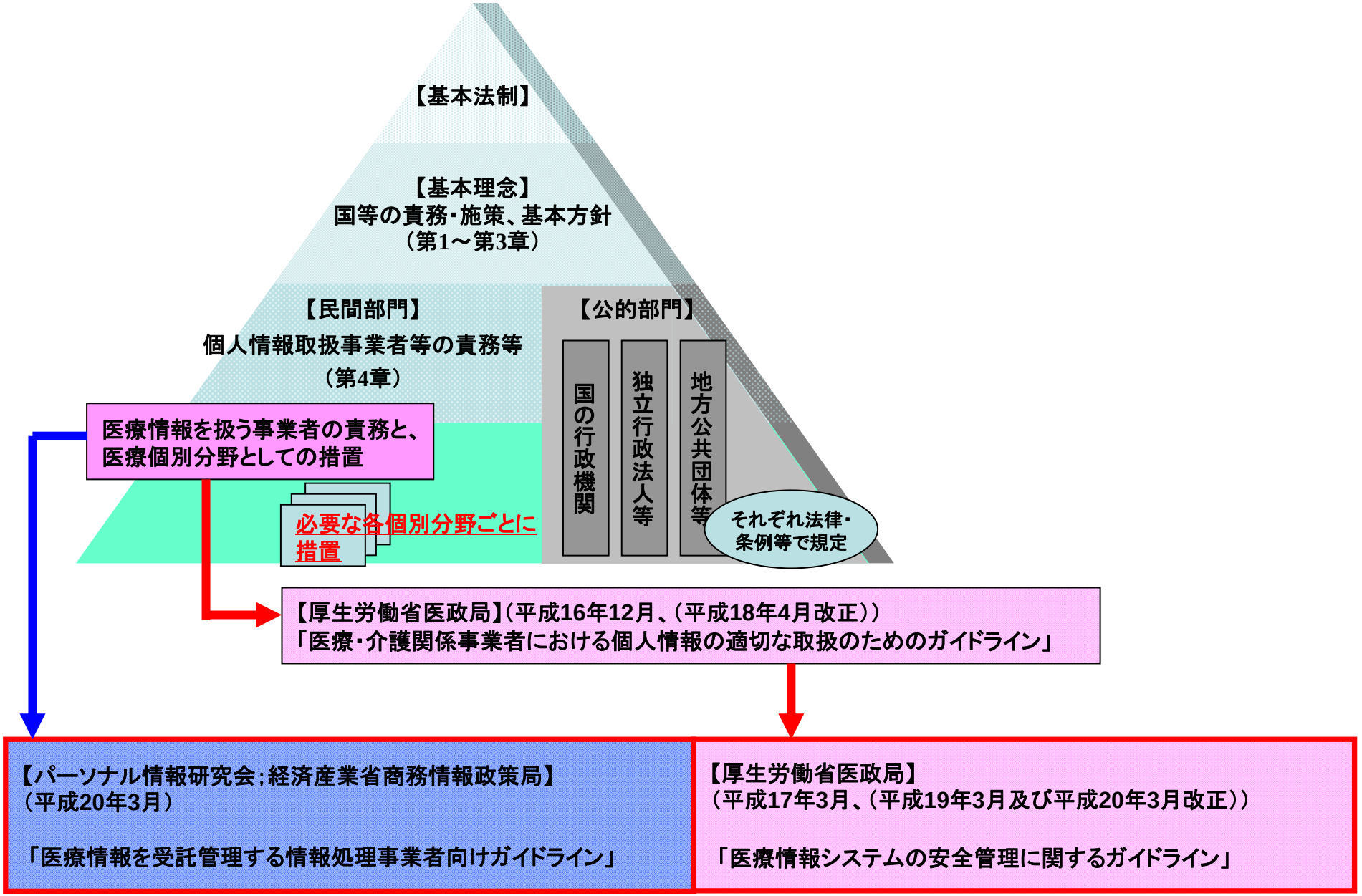
平成20年11月14日

総務省 Ministry of Internal Affairs and Communications

厚生労働省 Ministry of Health, Labour and Welfare

経済産業省 Ministry of Economy, Trade and Industry

1．個人情報保護法制等の執行指針としての体系イメージ



2. 各ガイドラインの概要

名称	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ドライン
発行主体	厚生労働省
概要	**1. 策定目的** 個人情報保護法の趣旨を踏まえ、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確保に関する活動を支援するためのガイドラインとして平成16年12月に作成、その後、他法令の改正に伴い必要に応じ改正。 **2. 対象範囲** 医療・介護関係事業者 **3. 項目、内容等** ①医療・介護関係事業者の個人情報の適切な取扱いの確保のための義務等について ・個人情報の正確性の確保 ・個人情報の第三者提供の方法 ・責任体制の明確化 ・患者・相談窓口の設置等、苦情対応 ・個人情報の利用停止　等 ②遺族への診療情報の提供の取扱い ③個人情報が研究に活用される場合の取扱い ④遺伝情報を診療に活用する場合の取扱い ⑤大臣の権限行使、他の法令等との関係 ⑥その他

名称	医療情報システムの安全管理に関するガイドライン（第3版）
発行主体	厚生労働省
概要	**1. 策定目的** 法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン及び医療機関等における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインとして平成17年3月に作成。 その後、ネットワークのセキュリティ要件や災害等の非常時の対応等を新設・改正するなど、必要に応じ改正等を行っている。 **2. 対象範囲** 医療機関等の責任者、情報システム管理者 **3. 項目、内容等** ①個人情報を含むデータを扱う医療機関等で参照されるべき内容 ・医療情報を扱う医療機関等における責任のあり方 ・情報システムの基本的な安全管理等 ②保存義務のある診療録等を電子的に保存する場合の指針等 ③運用管理規程の作成について

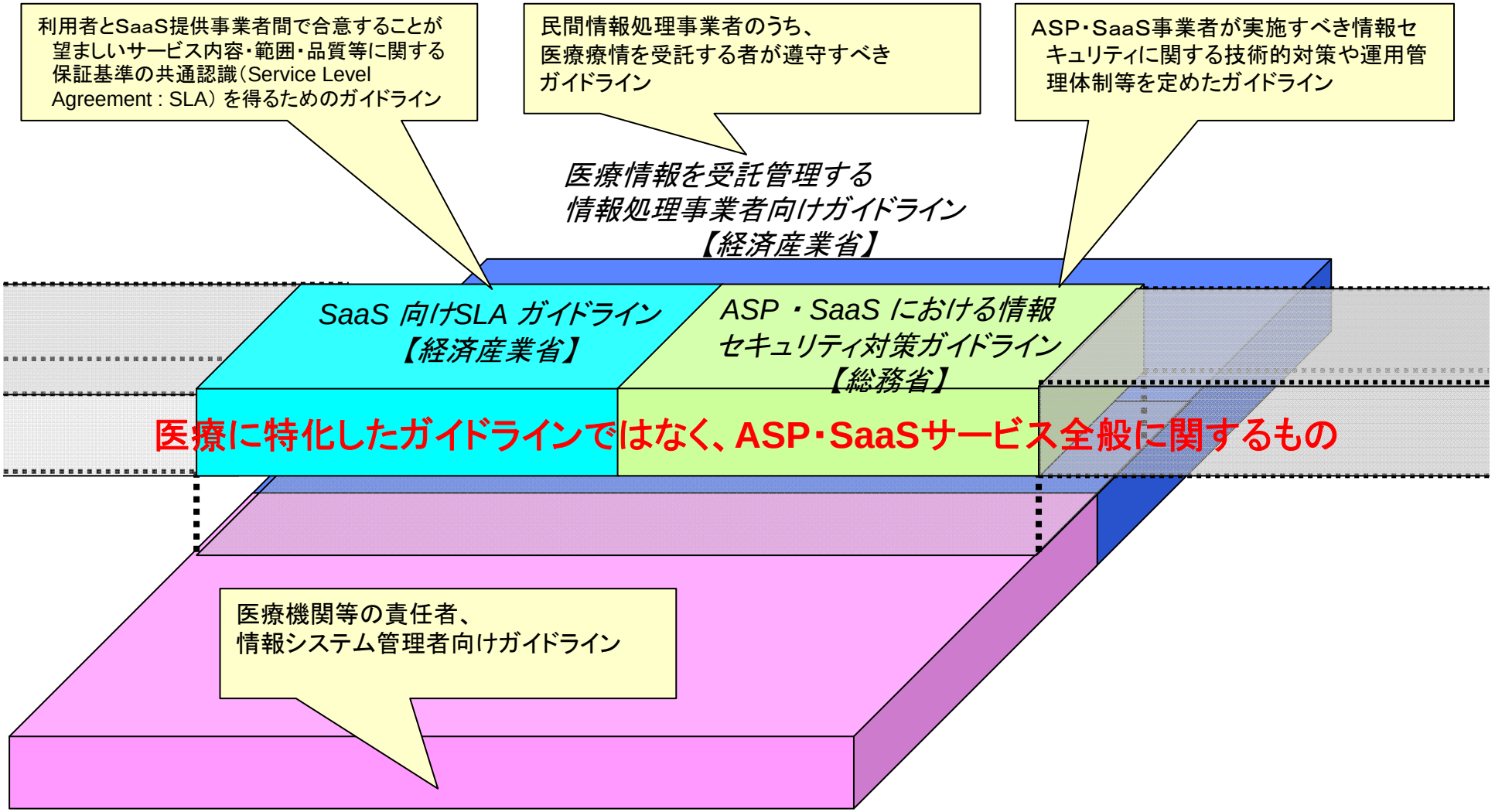
名称	医療情報を受託管理する情報処理事業者向けガイドライン
発行主体	経済産業省
概要	**1．策定目的** 医療情報については、厚生労働省から発出されている「医療情報システムの安全管理に関するガイドライン」が平成20年3月に改正され、医療情報の外部保存に関するルールを明確化されたところ。これに対応するため、医療機関から医療情報を受託する事業者（以下、「医療情報受託者」という。）となる立場の情報処理事業者について、医療情報の機微性の大きさにかんがみ、通常よりも高度な安全管理措置を規定し、医療情報の外部保存の万全を期そうとするもの。 **2．対象範囲** 医療情報受託者 **3．項目、内容等** ①医療情報受託者に対する責任の充実 ②医療情報受託者の安全管理体制に対する第三者認証 ③情報セキュリティ対策に関する外部監査の実施

名称	レセプトのオンライン請求に係るセキュリティに関するガイドライン
発行主体	厚生労働省
概要	**1．策定目的** オンライン請求業務に際し、レセプトに含まれる個人情報を適切に保護するとともに、オンライン請求業務の円滑な遂行に資することを目的として、平成１８年４月に作成。 その後、ネットワーク要件等の対応等を新設・改正するなど、必要に応じ改正を行っている。 **2．対象範囲** 保険医療機関・保険薬局、審査支払機関、保険者 **3．項目、内容等** レセプトオンライン請求に携わる保険医療機関・保険薬局、審査支払機関、保険者で参照されるべき内容 ・ 適用範囲 ・ 物理、人的、技術的セキュリティ等 を規定 安全対策の規程例を明示

名称	ASP・SaaSにおける情報セキュリティ対策ガイドライン
発行主体	総務省
概要	**1．策定目的** ASP・SaaS事業者が、提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、平成20年1月に策定。 利用者が、ASP・SaaSサービスを選定する際の指標としても活用。 **2．対象範囲** ASP・SaaS事業者（及びASP・SaaSサービスの利用者） **3．項目、内容等** ①運用管理体制、外部組織との契約における留意事項、利用者に対する責任等の組織・運用に関する対策。（主に経営者等の組織管理者 向け） 【項目例】 ・情報セキュリティのための組織　・情報資産の管理 ・従業員に係る情報セキュリティ　・ユーザサポートの責任 ・情報セキュリティインシデントの管理　等 ②アプリケーション、サーバ・ストレージ、ネットワーク、建物・電源等、ASP・SaaSの典型的なシステム構成に基づく、物理的・技術的な情報セキュリティ対策。（主に現場の技術者 向け） 【項目例】 ・アプリケーション、プラットフォーム、ハードウェアのセキュリティ対策 ・外部ネットワークからの不正アクセス防止 ・サービスデータの保護　・運用管理端末のセキュリティ対策 ・媒体の保管と廃棄　・建物の災害対策　等

名称	SaaS向けSLAガイドライン
発行主体	経済産業省
概要	**1．策定目的** SaaS事業者が提供するオンラインサービスを利用する際に、当事者間の適切な取引関係を確保し、SaaSの普及を図るため、サービス提供企業とユーザ企業間で合意することが望ましいサービス内容・範囲・品質等に関する保証基準の共通認識（Service Level Agreement : SLA）を得るための指針を平成20年1月21日に策定。 **2．対象範囲** SaaSを利用する企業の経営者及び情報システム担当者、及び、SaaS提供事業者 **3．項目、内容等** ①SaaS利用におけるSLAの重要性 SaaSを利用する際にSLAを締結することによる利用者及びSaaS提供事業者双方のメリットや重要性について解説。 ②SaaS利用におけるSLA上の確認事項 完全性、可用性、運用保守性等に関する確認事項やコンプライアンス対応における考慮事項等を記述。 ③SaaS向けSLA におけるサービスレベル項目のモデルケース アプリケーション運用（可用性、信頼性、性能、拡張性）、サポート（サービス提供時間）、データ管理（バックアップ方法、保存期間、データ消去要件）等

3. 各ガイドラインの位置関係



医療情報システムの安全管理に関するガイドライン　第3版
【厚生労働省】