参考資料４

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

（抄）

平成 30 年7月

第１章 本ガイドラインの前提条件及び読み方

本章では、本ガイドラインの目的、前提条件、使用する用語等について記述する。

１．１ 本ガイドラインの目的

１．１．１ 医療情報の特殊性とクラウドサービスの利用

（１） 医療情報の特殊性

一般的に個人情報は、一旦漏洩した場合に回復が困難なものであり、特に医療情報は患者の生命･身体に関わるほか、差別を受ける等、権利利益が侵害される可能性もあるため、高い保護方策が求められる。また、医療従事者が利用する医療情報の完全性が損なわれると、適切な医療行為が行われない危険性がある。そのため、医療機関等や関係者に対しては、罰則を伴う守秘義務が法律で課せられるほか、法令･各種のガイドライン等により格別の安全管理措置を講じることが求められている。

この観点から、医療機関等向けに「医療情報システムの安全管理に関するガイドライン」（以下「厚生労働省ガイドライン」という。）が策定されており、医療情報を取り扱う情報システムを利用する際には、厚生労働省ガイドラインの安全管理対策を講じることが求められる。

医療機関等が対応すべき安全管理対策は、医療機関等から委託を受けた事業者においても、同様の対策を講じる必要がある。

（２） 医療情報の取扱いにおけるクラウドサービスの意義

他方、医療情報の取扱いにおいて、クラウドサービスの利用も普及しつつある。情報システム管理を行う要員が十分確保できない医療機関等においては、適切に管理されたクラウドサービスを利用することにより、医療機関等の内部で医療情報の保存、管理を行うのに比べて、より安全かつ効率的に管理することが期待できる。

クラウドサービスにおいて医療情報を取り扱う場合は、低コストで高いセキュリティを実現することが重要である。また、クラウドサービスは、当初は ASP･SaaS という形で利用されることが多かったが、仮想化技術の進展などもあり、PaaS、IaaS 等、多様な形で提供されるようになってきた。

また、医療機関等は、クラウドサービスを活用することにより、医療情報連携ネットワークやオンライン診療等、新しい形での医療情報の利活用を、低コスト及び高セキュリティで実現できるようになると考えられる。

（３） クラウドサービス事業者向けのガイドラインの必要性

（１）で示したように、医療機関等による委託に基づいて医療情報を取り扱うクラウドサービス事業者は、厚生労働省ガイドラインに示される安全管理対策を講じる義務を、医療機関等を通じて間接的に負うことになる。そのため、この場合のクラウド

サービス事業者が負う義務の範囲は、医療機関等との契約内容等に依存するところが大きい。

その一方で、クラウドサービスの性格上[1]、医療機関等は、クラウドサービス事業者が提示する医療情報システムの安全管理対策の内容に一定程度対策を委ねざるを得ないケースも生じる。

そこで、クラウドサービス事業者が厚生労働省ガイドラインに準拠したサービスを提供するために、クラウドサービス事業者に対して、必要な安全管理対策を講じるためのガイドラインを直接示す必要がある。

これによりクラウドサービス事業者に、厚生労働省ガイドラインで示す内容に準拠した安全管理対策を講じる直接的な責任を生じさせ、医療機関等が安心してクラウドサービスを利用できる環境が整備される。

（４） 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の策定

（３）に示す観点から、クラウドサービスのうち、当時普及が進んでいた ASP・SaaS について、平成 21 年 7 月に「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「総務省 ASP 医療ガイドライン」という）」第 1.0 版が策定された。これは、厚生労働省ガイドラインにおける医療機関等に対する要求事項に対応する形で、クラウドサービス事業者が医療情報を取り扱うサービスを提供する際に安全性の観点から求められる要求事項を示したものである。クラウドサービス事業者が、総務省 ASP 医療ガイドラインを遵守することで、医療機関等に対して、医療情報を適切に取り扱う安全なサービスを提供していることを示せるようにした。

これを踏まえて平成 22 年 2 月に厚生労働省より「『診療録等の保存を行う場所について』の一部改正について」[2]（以下「外部保存改正通知」という。）が示され、診療録等の医療情報を民間事業者が運用するサービスを利用して外部保存することが許容された。

その後、総務省 ASP 医療ガイドラインは、平成 22 年 12 月に第 1.1 版に改定され、クラウドサービス事業者が医療情報を取り扱う際の指針として活用されてきた。

---

[1] クラウドサービスでは、一般的に多数の利用者を対象としてサービス提供をすることを想定していることから、個々の利用者が、個別の状況に従った形で、サービスの内容を調整することができないケースが多い。

[2] 平成 22 年 2 月 1 日　医政発 0201 第 2 号／保発 0201 第 1 号

（５） 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策定の意義

総務省 ASP 医療ガイドライン第 1.1 版を策定した当時は、医療情報を取り扱うクラウドサービスは、現在のクラウドサービスのうち、ASP･SaaS が中心であった。したがって、総務省 ASP 医療ガイドライン第 1.1 版では ASP･SaaS がクラウドサービスの代表例として取り扱われていた。しかし（２）で示したように、今日では ASP･SaaS のほか、PaaS、IaaS 等、様々なレイヤーのクラウドサービスが提供されている。また、プライベートクラウド、パブリッククラウド、ハイブリットクラウドなど、多様な実現形態が存在している。加えて、それぞれのサービスは、必ずしも１社で提供するとは限らず、複数の事業者が相互に連携して提供されることも多くなっている。

このような状況を踏まえ、医療機関等が安心してクラウドサービスを利用できるようにするため、事業者向けのガイドラインも、ASP･SaaS 事業者だけではなく、広くクラウドサービス事業者を対象とする旨を明示するほうが適切である。

さらに、平成 29 年には、改正個人情報保護法の施行に併せ、医療･介護分野における個別の対応を記した、「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」が策定されたほか、厚生労働省ガイドラインも改定され、第 5 版[3]として内容面でも大きな変更が行われた。

このようなクラウドサービスの多様化や、それを支える技術の進展、各種の法令等の改正等を背景に、総務省 ASP 医療ガイドラインについても改定し、「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」（以下「本ガイドライン」という。）として公表することとした。

[3] 「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」（厚生労働省　平成 29 年 5 月）

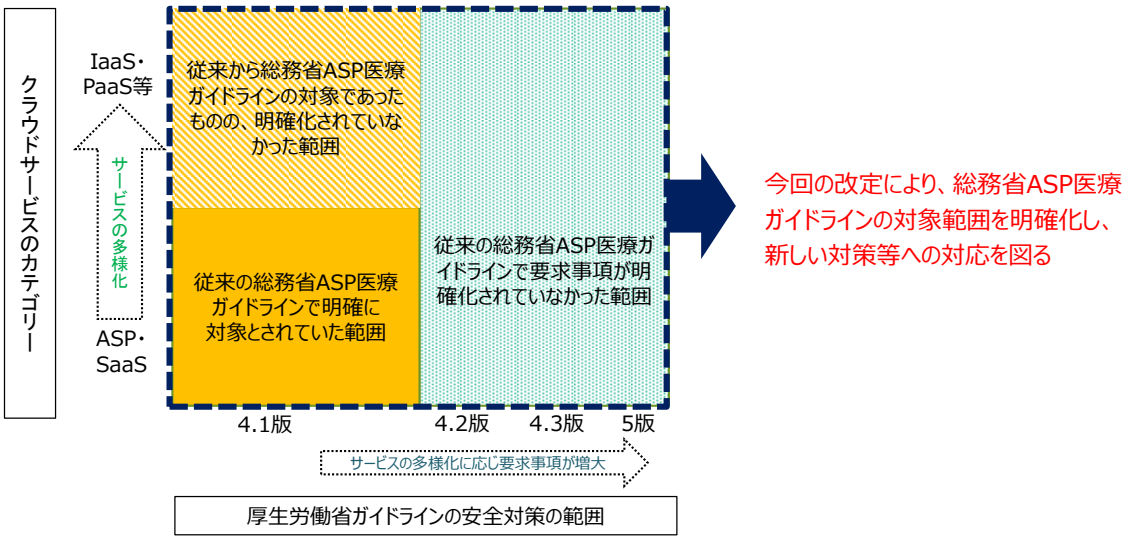

図 1　本ガイドライン策定の意義

策定当時の総務省 ASP 医療ガイドラインは、提供されていたサービスの中心であった ASP･SaaS に焦点を当てて策定された。総務省 ASP 医療ガイドラインの内容は、ASP･SaaS 以外のクラウドサービスの類型に対しても適用しうるものであったが、クラウドサービスが多様化する中で、その旨が必ずしも明らかではなかった。また厚生労働省ガイドラインが改定を重ねる中で、新規に設けられた厚生労働省ガイドライン第 5 版の条項に対応する事業者側への要求事項についても不明確な点や不足している点があった。本ガイドラインにより、これらを改善することとした（図 1）。

１．１．２　本ガイドラインの目的

本ガイドラインでは、１．１．１に示す医療情報の特殊性から来る高度な安全性の要求を踏まえ、クラウドサービス事業者が医療情報を取り扱う際に求められる責任、安全管理対策、医療機関等との合意形成の考え方等を示す。

本ガイドラインでは上記を通じて、クラウドサービス事業者が医療情報を適正かつ安全に取り扱うことにより、医療情報におけるクラウドサービスの利用の促進を図ることを目的とする。