2018 年 6 月 21 日

「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）（案）」に対する意見

BSA｜ザ・ソフトウェア・アライアンス

BSA｜ザ・ソフトウェア・アライアンス[1]（以下「BSA」といいます。）は、総務省（以下「貴省」といいます。）より公表された「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）（案）」）（以下「本ガイドライン」といいます。）に対し、以下の通り意見を提出します（以下「本意見」といいます）。

BSAの会員企業は、世界の情報経済を牽引し、かつ、日常生活を改善する、クラウドコンピューティングその他関連サービスを含む革新的な技術、製品及びサービス提供の最前線にいます。クラウドコンピューティングは、日本においても、全産業分野にとって現在かつ将来に渡り最も重要な技術の1つであり、従って、クラウドコンピューティングに関連する法令及び政策は、クラウドサービスの成長・普及を支えるものであるべきと考えます。

クラウドによる堅牢なデータ保護とデータローカライゼーションの問題

BSAは、医療情報が機微な健康データを含み得ること、また、かかるデータに関するプライバシー保護を確実にするために、各国が適切なルールを策定する場合があることを認識しています。しかしながら、当該データを自国に保管することを命じることが、必ずしもプライバシー保護の目的達成に資する訳ではありません。クラウドサービスの大きな利点

[1] BSA｜The Software Alliance（BSA｜ザ・ソフトウェア・アライアンス）は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSAの加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションを創造しています。ワシントンDCに本部を構え、世界60カ国以上で活動するBSAは、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。BSAの活動には、Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, 及び Workdayが加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

の１つである費用効率の便益を最大化するためには、グローバルな規模でデータ移転を最適に行う必要があり、円滑な越境データ移転をグローバル規模で確保することが非常に重要です。電子データのセキュリティは、データの処理又は保存をどこの場所で行うかよりも、処理及び保存を行う事業者により用いられる技術及び実践にはるかに大きく依存します。今日、主要なクラウドサービス事業者は、事業者が自ら合理的に行うことができることよりも更に堅牢なデータ保護を実施し安全管理を実践していることから、データが保存されるデータセンターの場所に拘わらず、データをローカルに保存するよりもクラウド上に保存する方が通常はより安全です。さらに、クラウドサービス事業者によっては、医療機関等を含む利用者に対して、データを保存するリージョンを選択するオプションを提供しているため、これにより、医療機関等は適用されるデータ保護及びその他のルールを遵守することがさらに容易になります。

BSAの見解では、本ガイドライン中の情報および機器の所在地に関する記述は、医療機関等が日本の所管官庁に対して必要な情報を円滑に提出できるようにするという理由で、データ、アプリケーション及びハードウェアが日本に所在することを要求しているとも読むことができ、これは越境データ移転を制限する可能性があります。このような制限は、診療録に関するプライバシー保護およびセキュリティ確保という目的達成のために必要とされる制限よりも大幅に大きな制約であって、医療機関等が需要に応じて必要な情報にアクセスし提供することを可能にするために必ずしも必要なものとは言えません。さらに、そのような要求事項は、クラウドサービスの使用を利用者に思いとどまらせる可能性があります。したがって、貴省に対し、当該記述（以下の「本ガイドラインの具体的な箇所に関するコメント3をご参照下さい）を削除するよう求めます　。

国際標準の重視

本ガイドラインは、2.4において、クラウドサービス事業者が医療情報を取り扱う際に、公正な第三者の認証（例えば、情報セキュリティマネジメントシステム（ISMS））を取得することは、医療機関等に対するクラウドサービス事業者の説明責任を果たす有効な手段であると認識していますが、私どもは、本ガイドライン全体を通して、関連する国際的に認められた標準の重要性をより明確にかつ強調して記載することによって、本ガイドラインがより良いものになると考えます。また、本ガイドライン中のクラウドサービス事業者への要求事項は、国際的に認められた標準の遵守によって満たされ、また、かかる標準で置き換えることが可能である旨、本ガイドラインに明示的に記載することをお奨めします。

ISMS（ISO/IEC27001）の他、そのような国際的に認められた標準の具体例としては、ISO/IEC27017、ISO/IEC27018 が挙げられます。これらの標準は、専門家によって策定され、客観的な審査のシステムを採用しています。また、いくつかの国際標準及び関連する認証は、監査によって、サービスプロバイダーが適合することを確実にしています。このように、広く

採用されている国際的に認められた標準や関連する認証を用いることで、サービスの安全性を高め、医療機関等も安全性についてより確信を得ることができると考えます。

また、私どもは、貴省に対し、このような国際標準の枠組みに従い、かつ、国際標準と一致する用語を用いて、本ガイドラインを策定するようお奨めします。ISMSの他、よりクラウドコンピューティングに適合するように策定された、国際的に認められた標準がいくつかありますので、貴省は、これらを本ガイドラインに明確に取り入れた方が良いと考えられるかもしれません。かかる国際標準の例としては、ISO/IEC 17788 (Cloud computing - Overview and vocabulary)及びISO/IEC 17789 (Cloud computing - Reference architecture)があります。実際、ISO/IEC 27017 は直接この2つの国際標準に言及しています。また、ISO/IEC 19086-1 (Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts)についても、クラウドSLAのガイドラインを作成する際に非常に有益であると思われます。

規範的なガイドラインではなくハイレベルなガイダンスを策定することの有効性

私どもは、貴省が、革新的なクラウドサービスを利用しながら医療情報を保護するためのガイドラインを提供しようとされる努力に対し、感謝申し上げます。しかしながら、私どもは、過度に詳細かつ規範的な要求事項を課すことは差し控えるべきであり、貴省には、より高度なガイダンスに焦点を当てていただきたいと考えております。詳細で統一的な安全管理の方法を定めることは、医療機関等に大きな負担をかけ、医療情報を使用し、保存し、安全性を高めるのに有益で革新的な信頼できるクラウドサービスの利用に際し、大きな制約を課すことにつながります。また、本ガイドラインでは、パブリッククラウドとプライベートクラウドとの違いが十分に説明されておらず、infrastructure-as-a-service（IaaS）、platform-as-a-service（PaaS）、software-as-a-service（SaaS）といった異なるタイプのクラウドサービスの違いを十分に踏まえて記載されていません。

本ガイドラインは様々な種類のクラウドサービスを網羅するものであって、各クラウドサービスの技術や機能はそれぞれ異なることから、本ガイドラインに記載されているクラウドサービス事業者への安全管理の要求事項はあくまでも参考の目的で記載されているにすぎず、実際に医療機関等が選択するクラウドサービスによっては、多くの対策が該当しないか又は関係しない可能性があることを明記するよう、貴省に対し求めます。

本ガイドラインの具体的な箇所に関するコメント

BSAは、上記の基本的な考慮事項に基づき、本ガイドラインに関する以下の具体的なコメントを述べます。

1. 「2.2 クラウドサービス事業者と医療機関等の管理者との責任分解の考え方」及び「2.3　医療情報の管理におけるクラウドサービス事業者の責任」

本ガイドラインでも指摘するとおり、パブリッククラウドの利用に当たっては、医療機関等とクラウド事業者の間で責任分担することは重要であり、クラウドサービス事業者と医療機関等の管理者との間で、責任分界点について合意することが必要です。しかしながら、その責任分界点はサービスの提供形態（IaaS，PaaS，SaaSなど）によって大きく変わらざるを得ません。本ガイドラインは、様々なクラウドサービスを対象とするものである以上、サービスの形態や性質によって責任分界点も変わることを明記していただきたいと考えます。

2. 「第3章 クラウドサービス事業者に対する安全管理に関する要求事項」

適切かつ必要な安全管理は、クラウドサービス事業者が採用する技術及び機能並びに医療機関等によるクラウドの利用状況によって異なります。本ガイドラインが様々なクラウドサービスを対象とするものである以上、本ガイドラインに記載されているクラウドサービス事業者に対する安全管理に関する要求事項は、あくまで参考としての記載であり、医療機関等が実際に利用するクラウドサービスによっては、多くの対策が該当しないか又は関連しない可能性があることを明記していただけるようお願いします。

そのように修正することにより、医療機関等は、本ガイドライン中の不合理または該当しない要求事項遵守の要請なく、自らが利用したいクラウドサービスを採用できることを明確に理解するのに役立ちます。

3. 本ガイドライン本文107頁及びSLA参考例 17頁の記載

前記のとおり、主要なクラウドサービス事業者は、堅牢なデータ保護およびセキュリティを実施しており、電子データのセキュリティは、処理または保存が行われる場所よりも、データを処理及び保存するクラウドサービス事業者によって採用される技術及び実践にはるかに大きく依存します。従って、以下の文章を削除するよう強く求めます。

（ガイドライン本文 107頁）

3.2.8 災害等の非常時の対応についての安全管理対策

（イ） 災害等の非常時の対応についての安全管理対策

「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、サーバー・ストレージ等は国内法の適用が及ぶ場所に設置する。」

（SLA参考例 17頁）

3.3 サービス提供環境・運用に係る前提条件

「乙は本サービスの提供に係る受託情報、プログラム等の保存、及びこれらに関するサーバー等の機器類は、日本国の法令の適用が及ぶ場所に設置する。」

クラウドサービス事業者のハードウェアや委託されたデータを日本国内に留めることを要求する必要はありません。医療機関等は、データおよびサーバー等がどこに存在するかにかかわらず、契約によって、リアルタイムにデータにアクセスして、所管官庁に必要な情報を円滑に提供することを確実にすることができます。

結び

BSAは、本意見が、本ガイドライン案を完成させる上で有益であることを願うとともに、引き続き貴省と協力していけることを願っております。本意見について、ご質問等ございましたらいつでもご連絡下さい。

以　上