2016 年 1 月 29 日

「『医療情報システムの安全管理に関するガイドライン』対応のための手引き Ver1.00」に関する意見

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」）は、「『医療情報システムの安全管理に関するガイドライン』対応のための手引き Ver1.00」（以下「本手引き」）に関し、以下の通り意見を提出致します。

BSAは、医療情報が機微な健康情報を含み得ること、また、かかる情報に関しプライバシーを保護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、当該情報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わけではなく、この観点から、診療録を日本にのみ保存すべきと本手引きがしている点については修正・削除すべきと考え、以下意見を述べます。

総論

BSA は、クラウドコンピューティングが、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、クラウドサービスに関連する法令及び政策は、クラウドサービスの普及を支え加速させるものであるべきと考えています。クラウドサービスの普及を支えるためには、関連する法令及び政策において、越境データの自由な移転が確保され、国際的な規制と協調していることが非常に重要であるというのが BSA の基本的な考えです。来月日本を含む参加国による署名が予定されている TPP の電子商取引章において、このデータの自由な移転に関する最新の国際ルールが規定されています。即ち、TPP は、TPP 締約国が、越境データの自由な移転を妨げないという強固な約束を含んでいます。そして、TPP は、個人情報を含む情報の国境を越える移転を許可すること、及び TPP

[1] BSA ｜ The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス）は、世界のソフトウェア産業を代表する業界団体です。70 社を超える BSA 加盟企業は、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・ソリューションの創造に年間数千億円もの投資を行っています。世界各国の政府との意見交換、著作権をはじめとする知的財産権の保護ならびに教育啓発活動を通じて、BSA はデジタル社会の拡大とそれを推進する新たなテクノロジーへの信頼の構築に努めています。BSA のメンバーには、Adobe, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro, Workday が加盟し、活動を行っています。詳しくは、日本の BSA ウェブサイト（www.bsa.or.jp）、または、BSA 本部（米国、英語）のウェブサイト（www.bsa.org/country.aspx）をご覧ください。

域内の企業に対して、ある締約国内で事業を行う条件として国内においてデータセンターを利用又は設置することを要求してはならないこと、を締約国に求めています[2]（以下「TPPにおける約束」）。TPPは、公共政策の正当な目的（例えば、プライバシーや健康データの保護）を達成するために必要な措置を採用し又は維持することを妨げるものではないとしていますが、同時に、当該措置は「目的の達成のために必要である以上に情報の移転に制限を課するものではないこと」を条件としています。

私どもは、本手引における、情報を日本国内に留めるべきとするデータ・ローカライゼーションの推奨は、診療録に関するプライバシー保護及びセキュリティ確保という「目的の達成のために必要である以上に」越境データの移転に制限を課すような誤解を生むことになりかねないと考えます。今後、日本においてクラウドサービスの利用や越境データの移転に関連する法令、ガイドライン及び政策の策定にあたっては、TPPにおける約束とその重要な意義を十分に踏まえ、曖昧又は過度の記載によって利用者のクラウド関連サービスの利用を躊躇させたり、また、越境データの移転を制限することによって、グローバル企業によるクラウドコンピューティング関連の投資やサービス提供を差し控えることにつながるようなものは取り除いていくべきであると考えています。これらの観点から、本手引きについてコメントを述べます。

各論：データセキュリティ及びデータセンターの所在地（17頁及び18頁）

確かに、当初、クラウドに保存されたデータのセキュリティに関し懸念を挙げられることもありました。しかし、今では多くの専門家が、洗練された事業者が自らデータを保護するのに比べても、主要なクラウドサービスプロバイダーは、より高いレベルで顧客データを保護するセキュリティを提供していると認めています。また、多くのクラウドサービスは、顧客事業者がクラウドに保管したデータを暗号化することを認めているため、この場合、クラウドサービスプロバイダーであっても、可読可能な形式のデータにアクセスすることはできません。更に、クラウドサービスプロバイダーによっては、顧客事業者が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、顧客事業者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。以上をまとめると、今日におけるクラウドサービスにおいては、多くの事業者が自ら行うよりも更に堅牢なデータ保護及びセキュリティを提供しています。

BSAは、事業者が、取り扱う診療録を保存する先として、クラウドサービス及びオンプレミスのセキュリティリスクを比較検討すべきという点につき本手引に同意しますが、本手引きでは、クラウドサービスがオンプレミスのシステムと比較してもセキュリティ上の便益を多く提供していることについて触れられていないため、この点も十分に盛り込んでい

[2] http://www.cas.go.jp/jp/tpp/pdf/2015/10/151005_tpp_Summary.pdfhttp://www.cas.go.jp/jp/tpp/naiyou/pdf/zanteikariyaku/160107_zanteikariyaku14.pdf

ただきたいと考えます。また、同様の観点から、海外にデータセンターが設置された場合のリスクにつき、17 頁及び 18 頁の記載は正しいものとは言えず、越境データ移転に萎縮を生じさせるものとなっているため、記載を修正すべきと考えます。さらに、利用契約形態が約款契約であることについては、データセンターの所在地と関係のない記載と考えられることから、今一度記載の整理を行うのが良いと考えます。そもそも、セキュリティ及びサービスの質は、SLA の記載及びその達成度、評判及び実績によって判断し、そのリスクを受容するか否か検討するのが合理的かつ客観的です。本手引きでは、リスクにつき、日本にデータセンターがある場合と海外にデータセンターがある場合に二分して記載されていますが、実際にクラウドサービスプロバイダーにより実施されているセキュリティ対策や技術に関する記載がなされておりません。このことによって、単純に海外データセンターの方が国内における保存よりもリスクが大きいような誤った印象を与えてしまっており、このままだと客観的なものとは言い難いと考えます。

また、本手引きにおいて「海外にデータセンターを設置している情報処理関連事業者においては、データの差し押さえが発生するリスクを常に抱えている。」とありますが、政府が国外のサーバーに保存されたデータにアクセスする権限は通常非常に厳格な制限があります。例えば、データへのアクセスを要求する政府は、しばしば、デュープロセス、証拠上、管轄上及びその他の制約を受けます。また、データが置かれた国では、他国の政府によるデータ開示要求に対して、たとえそれが他国における正当な法的手続きを踏まえた要求であったとしても、制約を設けていることがよくあります。他国に置かれた電子データを取得するには、もっとも適切なメカニズムとして、日米刑事共助条約[3]を含む2国間または多国間の共助条約があります。この条約を用いると、ある国の政府が、取得したいデータが置かれた国の政府に対して、公式にデータ開示を要求でき、データが置かれた国の政府は、適切な法的手続きに従い、そのデータを扱っているプロバイダーに対してデータ開示を求めることができます。この条約は、公共の利益のため、政府による国境を越えた捜査を可能としますが、データが置かれた国の法律に従うことが前提となっています。これは、データの開示請求を受ける情報処理事業者が法の抵触によるリスクを負うことを防ぐためです。さらに、例として挙げられている米国自由法（修正された旧・米愛国者法）は、米政府が一歩踏み込んで情報を入手できるメカニズムを新設したと一般的に信じられているものの、研究報告[4]によれば、これは誤解であり真実と大きくかけ離れた認識です。米国自由法によって政府に認められた捜査手段は、アメリカ合衆国憲法及び法規により多くの制約を受けます。例えば、米政府機関がeメールやその他のコミュニケーションの内容の開示

[3] http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_3a.pdf

[4] Maxwell, Winston, *A Global Reality: Governmental Access to Data in the Cloud*, Hogan Lovells White Paper (2012) *at* http://www.hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique/

を強制したい場合、アメリカ合衆国憲法はほとんどの場合において政府に対し、裁判所が正式に発行する令状又は命令書を取得することを要求しています。米国自由法を使っても、米政府は裁判所の令状や命令書がなければ、クラウドに保存された文書や（eメールを含む）コミュニケーションの内容の知ることができません。すなわち、米政府は独立した裁判所や判事に令状や命令書を出してもらうため、求められる法的要件をすべて満たすという十分な証拠を事前に示さなければなりません。この求められる法的要件も、アメリカ合衆国憲法及びその他の法規制によって定められています。こうした政府によるユーザーのデータ開示要求によって影響を受けるのは利用者のほんの一部であることがこれまで報告されており、クラウド利用者は十分な理解のもと、どこにデータを保存するか（どこの国のデータセンターを利用するクラウドプロバイダーを使うか）を決めることが重要です。

以上をまとめますと、電子データのプライバシー及びセキュリティは、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る実践及び用いられる技術に多く依存します。主要なクラウドサービスプロバイダーは、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セキュリティ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（このことは、政府からのアクセスに対しても同様です）。診療録を取り扱う事業者が、様々なITのオプションについてセキュリティ及びプライバシーのリスクに関し慎重に検討すべきであるということについて同意しますが、本手引きにおいて日本にデータを保存するよりも日本外のデータセンターに保存するだけで安全性が低いかのような記載については正確ではないため修正・削除いただくようお願い致します。

本手引きが引用する、総務省「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」及び経済産業省「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」の該当箇所についても、前記の TPP における約束も併せて検討すれば、「所轄官庁に対して法令に基づく資料を円滑に提出する」という目的を達成するのに必要最小限であり、かつ、越境データへの制限が最小限のものとなるよう、要求事項は解釈されるべきです。そうであれば、クラウド事業者とユーザーとの当事者間の契約において法令に基づく資料提出等求められる事項の履行や日本法の遵守を約束することも可能であり、これらのガイドラインは、絶対的にデータセンターの地理的所在地を規制しているものではないと解釈されるべきです。従って、ガイドライン要求事項はそのまま紹介するにとどめ、「よって、法律により作成・保管が義務付けられた行政文書でもある診療録が海外のデータセンターに保管されることは行政上あってはならない。」との記載は削除すべきであると考えます。

以　上