Cloud Computing と電子カルテについて語る　～診療情報の外部保存について～

Discussion about EMR at Cloud agé -Cloud is suitable as EMR storage?

木村　映善

愛媛大学医学部附属病院医療情報部

1.あらまし

近年、クラウド・コンピューティング技術が台頭しており、そのスケーラビリティとコストは従来の IT 技術によって構築されたシステムを圧倒している。電子カルテのコスト削減のためにクラウド技術を利用することを検討することは当然の流れである。一見、「診療録等の外部保存に関するガイドライン」をはじめとした医療情報システムに向けたガイドラインに基づいて、クラウド上に構築することが可能に思える。しかし、クラウドは専用線・専用ファシリティを提供するサービスと異なり、サーバとデータセンタの場所を特定していないことが多い。このことがどのような問題をもたらすかを考察する。また医療情報システムは今後どのようなガイドラインの策定、法制度の援用をうけるべきかを提案する。

2.背景

本邦は世界的にみても電子カルテの普及率が高いとされる国である。それにしては実感を伴わないのは、電子カルテを導入した医療機関・医師が、コスト、機能、性能的に満足する水準に達していると実感できていないためと思われる。医療機関の運営に支障が生じないように、電子カルテシステムに安定性を求めざるを得ない。そして、長期間にわたって診療記録を保存する必要性があり、事業継続計画への関心も高まっていることから、ストレージやバックアップ体制についても多少の冗長性を見込んだ投資が要求されている。これらをすべて勘案したシステムへの投資は、医療機関にとって大きな負担となっている。

翻って、近年のネットワークの高速化によるリソース配置の地理的制約からの解放と、クラウド技術の出現によって、従来では考えられなかった性能対費用効果の大きいシステムが入手できるようになった。コスト削減と、安定性・性能の向上を同時に達成したい医療機関にとっては願ってもない機会ととらえ、電子カルテシステムのクラウド移行を検討するところもでるだろう。しかし、下記に述べるようにいくつかの問題点が存在する。

3.問題

3.1 データセンタと法規制

クラウドを提供している事業者はセキュリティを理由にデータセンタの場所を開示していないところがある。データセンタは冗長性・コスト効率化のために、世界的規模で運用コストの低い場所に立地していることが多い。そして、適切な配置場所をシステムが自動的に決定し、データを複数のデータセンタに分散配置していることがある。

データセンタは、それが立地している場所を支配している法制度の制約下に置かれており、様々な問題を起こす原因となっている。例えば、欧州ではデータの移動が国外を経由する可能性があるサービスの利用について規制をしている。また、米国の米国愛国者法(USA Patriot Act)や英国の捜査権限規制法(Regulation of Investigatory Powers Act)などでは、それぞれの自国内に所在する超法規的なデータの開示、捜査権限を認めている。外国とはいえ、個人情報が含む診療記録が第三者に開示される余地があるということをどう受け止めるか。

また、データセンタの所在地のみならず、事業者、取引先の本社が所在する場所の法律に対しても注意しなければならない。

3.2 DaaS/IaaS への配慮

本邦では、クラウドの範疇に分類されるサービスについて、ガイドライン上で言及されているのは、Software as a Service(SaaS)までである（2010 年 4 月現在）。Data Storage as a Service(DaaS)、Infrastructure as a Service(IaaS)については明確なガイドラインはみられない。SaaS では業者がアプリケーションおよびデータ保管について責任を持つモデルであり、顧客と業者の責任境界についてガイドラインが規定されている。しかし、DaaS や IaaS では、業者はアプリケーションの提供を行わずに、データをコントロールするための API をユーザに提供している。その結果、DaaS/IaaS ではデータの管理責任は顧客寄りに帰する。DaaS/IaaS に限ったことではないが、データ保存について Service Level Agreement(SLA)を結ばない限りは、データ保持については Best Effort であるし、SLA を結んだとしてもサービスが提供できなかった場合のペナルティについては触れているものの、データそのものの補償については触れていないものが多い。すなわち、クラウド化しても究極的にはデータの真正性、保存性についてはユーザが最終的に責任を持つことにはかわりはない。

3.3 データの回収リスクと残存リスク

クラウド事業者との契約には、契約終了などに先立っての事前通知などが保証されているものがある。しかし、外部に保管したデータの容量が大きくなると、データの回収のために機器の準備やダウンロードに要する時間がかかり、サービス停止までに回収が完了できないリスクが存在する。また、ユーザの操作に基づき、データの作成・変更・削除が行われるが、それがユーザの意図通りになっているかは別の話である。パソコンでファイルを削除してもファイルシステムのフラグが変更されただけで、実際には削除が完全になされていないのは周知の通りである。クラウドでユーザがデータを削除したつもりでも、ずっと後になってクラウド事業者からデータ漏洩し、その中に削除した筈のデータが入っていた場合は、ユーザはどこまで責任を負うべきなのだろうか？

3.4 個人情報の定義のずれ

厚生労働省は「個人情報に関するガイドラインに関する事例集」において、『「個人に関する情報」であっても、暗号化により特定の個人を識別できなければ「個人情報」に該当しません。』と述べている。しかし、経済産業省の個人情報保護のガイドラインでは、暗号化されているかどうかを問わないと書かれており、省庁間においての「個人情報」の扱いについて解釈が分かれているようである。

4.提言

4.1 暗号化アルゴリズムの安全性評価に基づいた年限設定と運用に関するガイドラインの策定

暗号化アルゴリズムの計算量的安全性、情報処理論的安全性は、計算能力の進歩と解読アルゴリズムの改善によって変動しうる。一般利用者にとって、暗号化アルゴリズムの安全性と、当該アルゴリズムの適用の社会的受容性の検討は負担である。専門家による各種暗号化アルゴリズムの評価と具体的な運用ガイドラインについて提示すべきである。また、3.3 で述べたように、ユーザのコントロール下におけない部分において、データ流出があった場合についての免除や時効の概念についても議論を深めるべきである。

4.2 データ保全についての契約および制度の整備

現状の Cloud 事業者との契約では、データ回収ができずユーザが泣き寝入りせざるを得ない可能性がある。通常の SLA、サービス・契約終了時の条件整理に加え、確実に顧客にデータを返却する義務を課するか、義務化がそぐわなければ下段に述べるように、Cloud の API の標準化を図り、相互にデータのバックアップをとれるようにしてリスク分散をユーザが図れるようにするべきである。

4.3 Cloud の API の標準化

現在、Cloud の API は標準化が進んでいない。このままでは、ベンダー・ロックインの主戦場が院内から院外に移っただけである。

4.4 Cloud 事業者に関する規制

個人情報を含むデータの保管場所の開示、データの国内限定配置などを求めるなど、透明性の確保と、諸外国への無断転送による各種法的規制からの保護措置を求めるべきである。