■クラウド・コンピューティングのセキュリティ評価指標　Ver.1.0 2010/12/01

制作　山野辺裕二
（国立成育医療研究センター病院　医療情報室）

●目的

この評価指標は、（主に保健・医療・介護･福祉分野で）クラウド・コンピューティングを利用したサービスを展開する個人や団体が、利用者や第三者向けに、自分のサービスを載せているクラウド・コンピューティングの仕組みについて、どの程度のセキュリティを確保しているかを大まかにわかりやすく示すためのものである。

クラウド・プロバイダ側のセキュリティ向上策（例えばデータセンターの出入り管理を多要素認証で行なっている、作業員の入室時に携帯電話を預けている等）については、いまのところ評価指標の対象外としている。

●この指標での定義

クラウド・コンピューティング

……インターネット上の、特定が困難なコンピュータ群にデータや処理を委ねること。利用者側から物理機器の存在位置や台数が特定できるレンタルサーバ、ホスティング、コロケーション、ハウジング等は除外する。

●レベル

大きな分類をレベルで表現し、下記の４段階に分ける。

レベル３　プライベートクラウド

……データを置くシステムが他の利用者と混在しない配慮がなされているクラウドサービス。

レベル２　ハイブリッドクラウド

……プライベートクラウドとパブリッククラウドを併用しているもの。

レベル１　有償パブリッククラウド

……データ置くシステムが他の利用者と共有されているサービスで、クラウド･プロバイダに費用を払っているもの。

レベル０　無償パブリッククラウド

……データ置くシステムが他の利用者と共有されているサービスで、クラウド･プロバイダに費用を払っていないもの。

●付加属性

レベル以外の付加属性を、文字で表現したもの。不明な場合は属性なしとなる。

P フィジカル

……（プライベートクラウドにおいて）物理サーバや物理ストレージ装置レベルで他の利用者と隔離されているもの。

V バーチャル

……（プライベートクラウドにおいて）仮想サーバ（バーチャルマシン）レベルで他の利用者と隔離されているもの。

D ドメスティック

……データを格納するコンピュータが国内にあることが保証されているもの。

I インターナショナル

……データを格納するコンピュータが海外にも分散しているもの。

C コンティニュイティ

……サービス提供者が、突然のサービス停止の権利などを留保していないもの。無償クラウドや一部の有償パブリッククラウド等では、提供者は利用者に予告なくサービスを停止できることになっている場合がほとんど。

E イレース

……サービス契約終了後などに、サービス提供者が利用者に対して、利用していたデータを消去した証明書の発行などができること。

Ss シークレットシェアリング

……秘密分散技術を活用できること。

St セキュアトランスミッション

……サービス提供者との間の伝送路が、暗号化されていること。

Sl サービスレベル

……サービスレベル契約(SLA)が存在し、その%から小数点を抜いたもの。

●表記例

最高度な国内限定プライベートクラウドの例
……レベル３-PDCEStSl9999

国内プライベートクラウドだが、隔離状態が不明なもの。
……レベル３-DEStSl9995

個人情報は国内プライベートに置き、個人情報を含まないデータの一部を外国のパブリックに秘密分散させている場合。混在している指標はセキュリティの低い方に合わせている。
……レベル２-ICESsStSl999

dropbox や gmail
……レベル０-ISt

●背景説明

医療分野でクラウド・コンピューティングを活用する気運が高まっているが、時代の流れが速いため、法律やガイドライン等が対応する前にさまざまな使い方がされてくると予想される。

クラウドを利用したある医療サービスが「e−文書法」、「個人情報保護法」といった法律や、「医療情報システムの安全管理に関するガイドライン」などの各種ガイドライン等に準拠している場合はそのことを公言できるが、そうでない場合はそのことを公に口に出しにくいものである。このような法律やガイドラインに非準拠のサービス提供は、提供者だけに非があるのではなく、法律やガイドラインの方が時代に追従できていない場合も考えられる。しかしそれでは利用者や第三者が安心できない。そこで、法規やガイドライン準拠以下のレベルについても分類指標を作り、それを事業者が提示することで提供する医療サービスの理解や比較を促そうと考えた。

例えば従来から、在宅医療や介護サービスの個人情報を平文メールで共有するような医療機関や介護サービス事業者があったのではと予想する。しかし、法規上問題があるためにそれは公言しにくく、結果として、セキュリティ上は問題があっても医療者や患者に有益なサービスが広がるのを妨げてきたかもしれない。逆に、たとえ法規上の問題が存在しても、それを公にすることで議論が進み、より改善された情報共有手段が広がったのではないかとも思える。これがクラウド・コンピューティングの時代になると、システムのバラエティが増え、問題はより複雑になる。今後は従来の轍を踏みたくないと考えている。

このような背景の下、主に医療分野を念頭に置いた、クラウド・コンピューティングのセキュリティ評価指標を提唱した。

●参考資料

欧州 ENISA のクラウドのセキュリティに関するガイドラインの翻訳（情報処理推進機構）
http://www.ipa.go.jp/security/publications/enisa/index.html

クラウドサービス利用のための情報セキュリティマネジメントガイドライン（案、経済産業省）Information security management for the use of cloud computing services based on ISO/IEC 27002
http://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000069865

以上