クラウドにおける医療情報セキュリティ、セキュリティ規格　及び　リスクアセスメント

アジェンダ

- 医療分野におけるクラウド利用の理由とリスク
- 医療アプリケーションが要求するクラウドのセキュリティ項目
- セキュリティ規格の状況とシンガポールでの動向
- 医療アプリケーションの視点からのクラウドサービスに対するリスクアセスメント
- 結論

Andreas Gehrmann
Managing Director
SRMS & Associates (Pte) Ltd. Singapore
www.srms.asia

本プレゼンテーションの目的

- 医療分野におけるクラウドサービス利用可能な例を示す
- 医療におけるリスク基準の明確化
- 関連規格と動向の概略
- シンガポールがすすめるクラウドに関するセキュリティ規格の説明
- クラウド利用のためのリスクアセスメントの例示

Contact: ag@srms.asia or mt@srms.asia (jp)

クラウドの利便性

– 様々な利用を可能とする

- Telemedicine – 遠隔医療
  - アクセス可能な機器の多様性
  - 国境を越えたアクセスが可能
  - 医療情報・データの共有化
  - 在宅でのモニターを可能とする
  - 遠隔地からの緊急対応を可能とする
  - セキュリテイの属性　: Availability （可用性）

- 医療ツーリズム
  - アジアでは、この面での旅行は増加する一方である
  - セキュリテイの属性　: Confidentiality（機密性）, Integrity（完全性）

クラウドの利便性とリスク

- 電子カルテ(EHR　- Electronical Health Record)
  - クラウド上のEHRは、保存分も含めてアクセスは容易である
  - セキュリテイの属性　:

    Confidentiality（機密性）, Availability (可用性）, Integrity（完全性）

- ビッグ・データ
  - クラウド上には、EHRと共にX線写真、DNA情報等も保管することが容易である
  - セキュリテイの属性　: Integrity（完全性）

クラウドの利便性

- 医療サービスのパフォーマンスの改善
  - より有効な協力体制の構築
  - 地域を超えた医者、病院間で電子カルテ（EHR）を共有することを可能とすることにより、検査の重複を避けることができ、迅速な対応が可能となる
  - 的確な情報の管理態勢により、情報の分析、追跡は容易に、少ないコストで、しかし迅速にして効率的となる
  - セキュリテイの属性　: Confidentiality（**機密性**）, Integrity（**完全性**）

クラウドの利便性

- 臨床研究
  - 次世代シーケンシングに起因する「データの爆発」だけでなく、研究プロセスにおける生物製剤の重要性の高まりから、「R＆Dのますます重要な側面」がクラウド基盤のコンピューティングで行われています
  - セキュリテイの属性　: Integrity（完全性）

- 協力態勢
  - クラウドにより、医療者は遠隔対応或いは災害地での救援活動が可能である
  - セキュリテイの属性　: Availability （可用性）

クラウドの利便性とリスク

- 分析
  - クラウド・コンピューティングは、リアルタイムで様々な活動、情報の大規模な共有を支援することができる
  - この機能は、医療関係者に関連情報を提供し、幅広い状況を示し、最適な判断を導く助けになるであろう
  - セキュリテイの属性　：Availability (可用性), Integrity（完全性）

- 医療情報の共有
  - 医療機関の間での医療情報の共有は、効率的な医療態勢に不可欠である。シンガポールはEHRシステムの展開を　進めている
  - セキュリテイの属性　：Availability (可用性), Integrity（完全性）

クラウドの利便性とリスク

- 費用の節約
  - 老齢社会に対応
  - 費用削減も可能
    - 遠隔対応
    - 迅速で効率的な処理

例：Azureを利用した12リード心電図システム（12-lead ECG）のテレ医療

“携帯電話により心電図情報の送信。
　これは、患者が臨床医から専門心臓外科医或いは病院に向かう救急車の中にいる時に、テレ診断を可能にする。
　最も重要なことは、この進んだサービスは簡単で効率的、そして費用がかからないということである。“

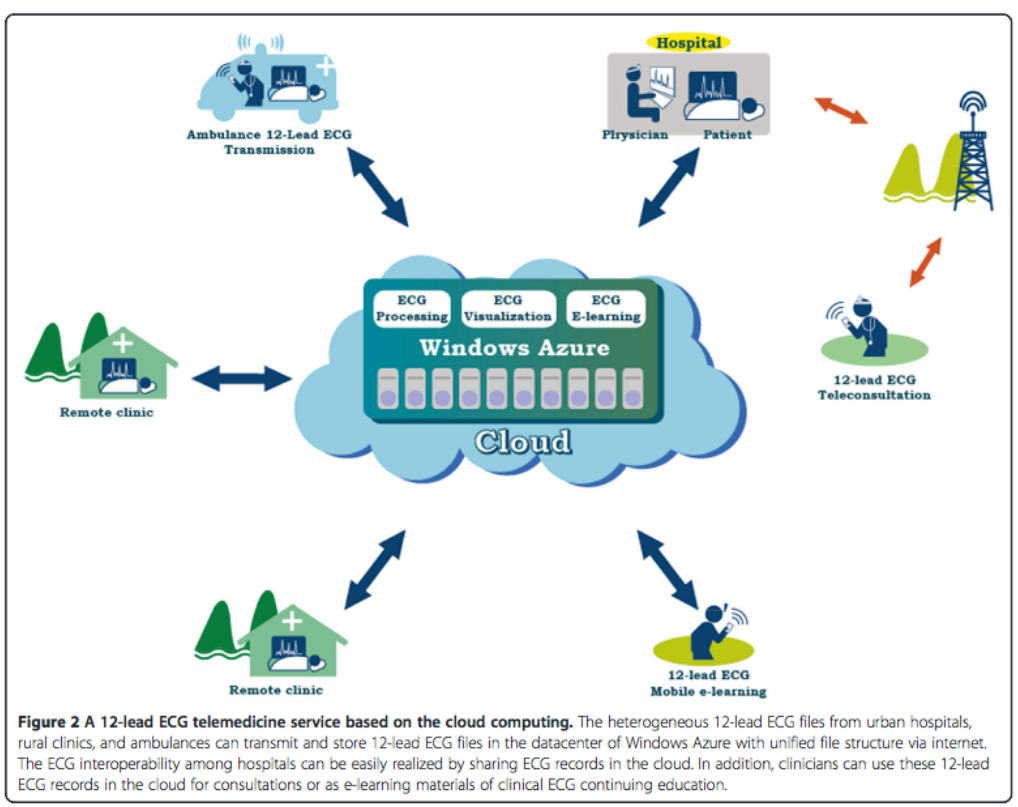


Figure 2 A 12-lead ECG telemedicine service based on the cloud computing. The heterogeneous 12-lead ECG files from urban hospitals, rural clinics, and ambulances can transmit and store 12-lead ECG files in the datacenter of Windows Azure with unified file structure via internet. The ECG interoperability among hospitals can be easily realized by sharing ECG records in the cloud. In addition, clinicians can use these 12-lead ECG records in the cloud for consultations or as e-learning materials of clinical ECG continuing education.

http://www.biomedcentral.com/content/pdf/1472-6947-12-77.pdf

クラウドに対するセキュリティの要求事項

- **医療分野におけるリスク**
  - 各国の個人情報保護に関する法令
  - 管理外のデヴァイスによるアクセス
  - 国境を越える医療データと様々な法的環境
  - クラウド・サービス網における不十分な信頼性
  - システムの相互運用性の欠如
  - プライバシー侵害のおそれ
  - Availability（可用性）, Integrity （完全性）and confidentiality（機密性）は全体の中で、調整する必要がある

セキュリティ規格の概要とシンガポールの動向

- **一般的な規格、クラウドを対象としていない**
  - ISO/IEC 27001　ISMS認証規格。基本的な要求事項
  - ISO/IEC 27002　情報セキュリティマネジメントの実践のための規範
  - ISO/IEC 27005　情報セキュリティに関するリスクアセスメントのガイダンス
  - ISO 31000　一般的なリスクマネジメントのガイダンス

セキュリティ規格の概要とシンガポールの動向

- **医療分野における情報セキュリティ規格**
  - ISO 27799　医療分野におけるセキュリティ管理策導入のガイダンス（現在改訂中）
- **クラウド技術に関する規格**
  - ISO/IEC 27017　クラウドのセキュリティに関して審議中
  - ISO/IEC 27018　CSP（Cloud Service Provider ）に対する個人情報の扱いに関する要求事項
  - ISO/IEC 27036-4　クラウドのセキュリティに関するガイドラインとして審議中

セキュリティ規格の概要とシンガポールの動向SS 584:2013 (MTCS)

Shingapore Standard Multi-tiered Cloud computing Security

Category	Control category	SaaS / PaaS / IaaS / User									
		Physical	Governance	Network	Storage	Hardware	Virtualisation	Operating system	Middle ware	Application	User
Core information security											
Cloud governance	Information security management		X								X
	Human resources		X								X
	Risk management		X								X
	Third party		X								X
	Legal and compliance		X								X
	Incident management		X								X
	Data governance		X							X	X
Cloud infrastructure security	Audit logging and monitoring			X	X	X	X	X	X	X	X
	Secure configuration			X	X	X	X	X	X		X
	Security testing and monitoring			X	X	X	X	X	X	X	X
	System acquisition and development			X	X	X	X	X	X	X	X
	Encryption			X	X	X	X	X	X	X	X
Cloud operations management	Physical and environment security	X	X								
	Operations	X		X	X	X	X	X	X	X	X
	Change management			X	X	X	X	X	X	X	X
	BCP and DR			X	X	X	X	X	X	X	X
Cloud specific information security											
Cloud services administration	Cloud services administration			X	X	X	X	X	X	X	
Cloud user access	Cloud user access				X	X	X	X	X	X	X
Tenancy and customer isolation	Tenancy and customer isolation	X	X	X	X	X	X				

背景

- 個人情報保護とクラウドのセキュリティに関する関心
- 医療分野でのクラウド利用の広まり
- 医療費用削減
- 効率性と品質の改善

- リスクマネジメントを含めて19の項目から構成
- リスク共有に関して詳細に言及
- リスクの領域確定のガイダンスを提供

SS 584:2013 (MTCS)

Level	Overview	Security control focus	Typical usage	Example data types
1	Designed for non-business critical data and systems.	Baseline security controls – "security 101" to address security risks and threats in potentially low-impact information systems using cloud services.	• Hosting web site • User control of application security • Test and Development • Simulation • Non-business critical systems	• Web site hosting public information • Data encrypted and protected from provider
2	Designed to address the needs of most organisations that run business critical data and systems.	A set of more stringent security controls required to address security risks and threats in potentially moderate-impact information systems using cloud services.	• Business critical systems	• Confidential business data • Personally Identifiable Information • Email • Customer Relationship Management (CRM) • Credit card data
3	Designed for regulated organisations with specific requirements and more stringent security requirements. Industry specific regulations may be applied in addition to these controls.	Additional set of security controls necessary to supplement and	• Hosting applications and systems with sensitive information	• Highly confidential business data

Impact level	Description	Financial	Operational	Individuals
High	**Major damage:** Loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.	Major financial loss	Severe degradation in or loss of mission capability to an extent and duration that the organisation is not able to perform one or more of its primary functions .	Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	**Significant damage:** Loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.	Significant financial loss	Significant degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.	Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	**Minor damage:** Loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	Minor financial loss	Degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.	Minor harm to individuals.

- 要求事項について3つのレベルと評価方法を定義する
- 医療記録の扱いはレベル3の要求事項
- レベル3は、ISO/IEC 27001 (2005)の認証に対応
- 影響度についてもレベル毎に詳述

SS 584:2013 (MTCS)

- Cloud governance:
  1. Information security management
  2. Human resources
  3. Risk management
  4. Third party
  5. Legal and compliance
  6. Incident management
  7. Data governance
- Cloud infrastructure security:
  8. Audit logging and monitoring
  9. Secure configuration
  10. Security testing and monitoring
  11. System acquisition and development
  12. Encryption
- Cloud operations management:
  1. Physical and environment security
  2. Operations
  3. Change management
  4. Business continuity planning and disaster recovery
- Cloud specific information security:
  1. Cloud services administration
  2. Cloud user access
  3. Tenancy and customer isolation

SRMS & Associates

Contact: ag@srms.asia or mt@srms.asia (jp)

MTCSと医療セキュリティ

シンガポール情報通信開発庁

Ministry of Healthcare（厚生省）

- IDA (Infocomm Development Authority of Singapore）と　MOHH (holding company of Singapore's public healthcare assets) の間で作業グループが作られ、医療分野でのセキュリティをMTCSに求められうるか検討中

- 医療分野でのCSPのサービスに関連して、MTCSの認証制度が議論されている

医療業務クラウドのリスクアセスメント

- **基本的な資産の特定**
  - 医療データ、医療プロトコルと規程
  - 業務プロセス

- **補助的資産の特定と相関関係**
  - クラウド・サービス
  - インフラストラクチュア、外部サービス、プラットフォーム

医療業務クラウドのリスクアセスメント

- **クラウド利用の基本的な立場**
  - セキュリティ属性
    - Availability（可用性）
      - 医療業界にとって情報の可用性は絶対条件であり、生死の問題である
      - 簡便なアクセス
      - 第三者の利用に関するSLA（service level agreements）は、必須である
      - パフォーマンスは可用性を決定する
    - Integrity（完全性）
      - 情報の完全性、信頼性は生死に関わる

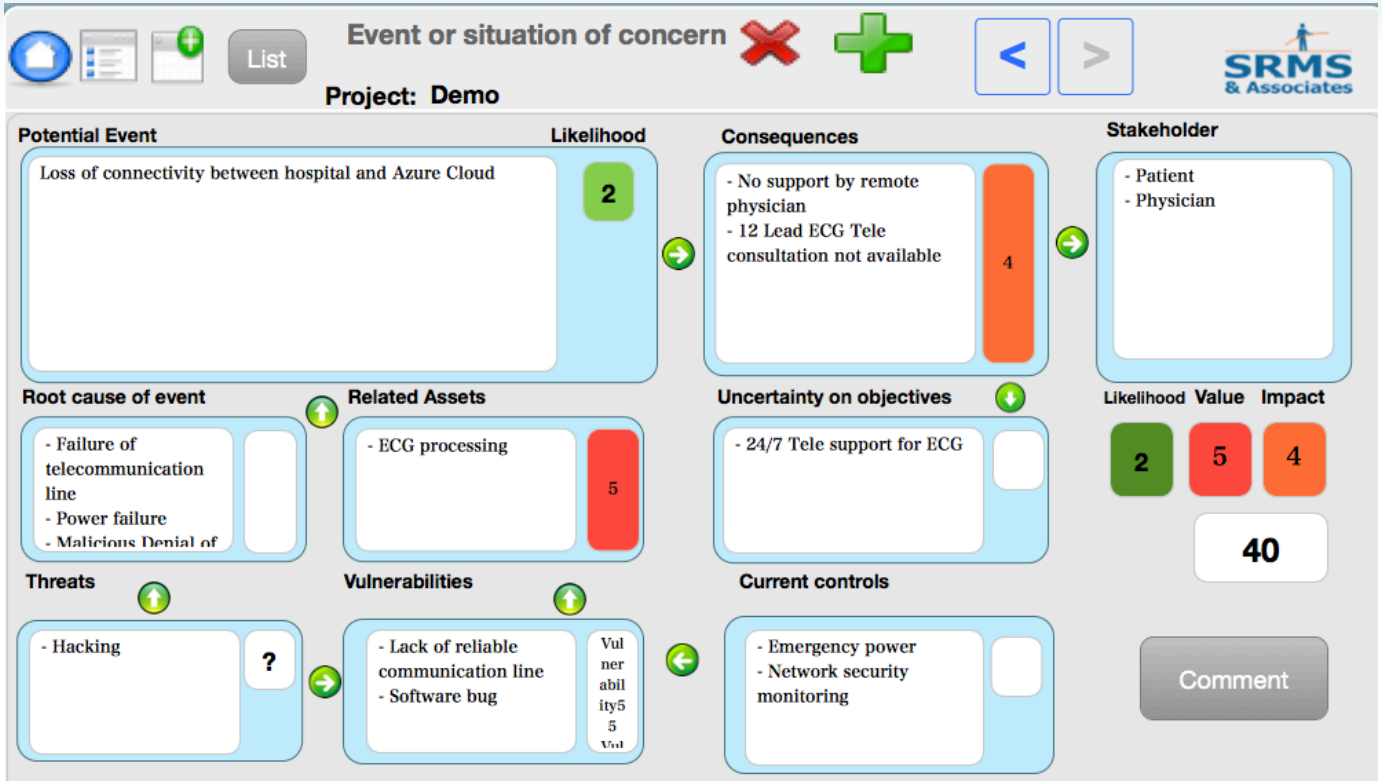
医療業務クラウドのリスクアセスメント

- Confidentiality（機密性）
  - 増大するデータの保護
  - データに関する不始末は、ビジネスを失い損害となる

- 責任
  - 患者のデータ管理者は明確でない場合が多い
  - クラウド・サービス事業者と管理者と責任の共有

医療業務クラウドのリスクアセスメント

- リスクアセスメントは複雑な関連の分析が必要である
- 強力なツールが要求される
- リスクはクラウドICTのサプライチェーンの中で理解し把握されなければならない



- リスク対応の選択
  - 対応の選択は、confidentiality(機密性）とavailability（可用性）に関わるリスクのバランスを考慮して決定すべきである

結論

- 様々な医療問題はクラウドの中で、検討され改善案を考えることができる
- 機密性の問題は、可用性と完全性のバランスから解決される
- 国境を超える医療情報の扱いには、不確かな法律の問題がある
- 医療情報の管理者は不明確である
- シンガポールはCSPに対する要求事項を明確にし、医療分野におけるセキュリティの確保をMTCSとバランスさせている

Reference

- https://ict.govt.nz/assets/Cabinet-Papers/Cab-Paper-Cloud-Risk-Assurance-Framework-Oct-2013.pdf
- http://www.microsoft.com/health/ww/products/Pages/Microsoft-Office-365.aspx
- http://www.hipaasecurenow.com/index.php/microsoft-office-365/
- http://www.wseas.us/e-library/transactions/biology/2007/30-372-WSEAS-EI.pdf
- http://www.cloudstandardscustomercouncil.org/cscchealthcare110512.pdf
- http://www.prnewswire.com/news-releases/asian-medical-tourism-market-outlook-2018-277120751.html
  http://www.cmtcorp.com/blog/medical-tourism-grows-cloud-and-mobile-technology-bridges-overseas-collaboration/