ヘルスケア・イノベーション
公開勉強会 #2
海外事例に学ぶプレシジョンメディシンの
クラウド利用とITリスク管理

2017年7月3日

一般社団法人　日本クラウドセキュリティアライアンス
健康医療情報管理ユーザーWG

AGENDA

- 1. 英国のオープンガバメント戦略とプレシジョンメディシン
- 2. 英国のプレシジョンメディシンにおけるクラウド利用事例
  - 2-1. ライフサイエンス事例：Genomics England on UKCloud
  - 2-2. 臨床医療事例：NHS Digital on UKCloud
- 3. CSA STARを活用した共通クラウド基盤のITリスク管理策
- 4. 日本のヘルスケア・イノベーションとクラウド利用に向けて
  - 4-1. シチズン・ドリブン・アプローチの視点から
  - 4-2. データ・ドリブン・アプローチの視点から

AGENDA

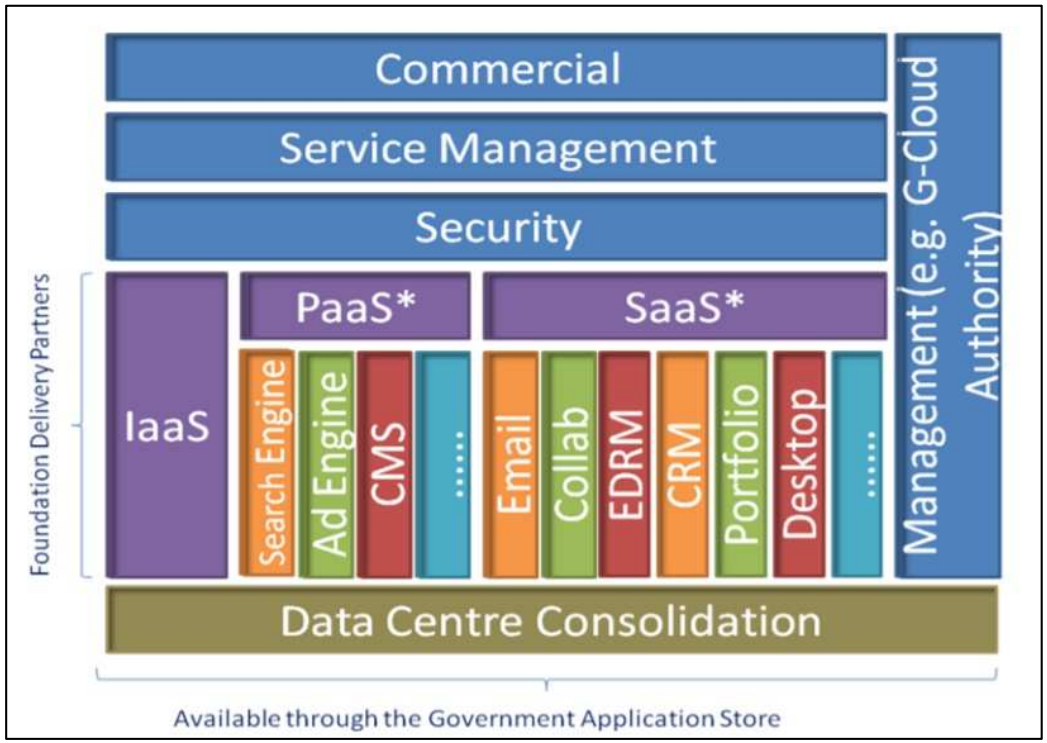
- 1. 英国のオープンガバメント戦略とプレシジョンメディシン
- 2. 英国のプレシジョンメディシンにおけるクラウド利用事例
  - 2-1. ライフサイエンス事例：Genomics England on UKCloud
  - 2-2. 臨床医療事例：NHS Digital on UKCloud
- 3. CSA STARを活用した共通クラウド基盤のITリスク管理策
- 4. 日本のヘルスケア・イノベーションとクラウド利用に向けて
  - 4-1. シチズン・ドリブン・アプローチの視点から
  - 4-2. データ・ドリブン・アプローチの視点から

1. 英国のオープンガバメント戦略とプレシジョンメディシン(1)

- 英国内閣府「政府ICT戦略」(2011年3月)
  (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-8/uk-government-government-ict-strategy_0.pdf)
  - 無駄とプロジェクトの失敗を削減し、経済成長を刺激する
  - 共通ICTインフラストラクチャを構築する
  - ICTを利用して変化を実現し、提供する
  - ガバナンスを強化する
- 英国内閣府「政府クラウド(G-Cloud)戦略」(2011年10月)
  (https://www.gov.uk/government/publications/government-cloud-strategy)
  - コモディティサービスの特定と委託に向けた共通の戦略とアプローチ
  - コモディティICTサービスの形成・採用・管理に向けた、一貫性のある包括的なアプローチと標準規格
  - 単純で包含的なガバナンスのアプローチ
  - センター・オブ・エクセレンスに権限委譲された管理と責任

1. 英国のオープンガバメント戦略とプレシジョンメディシン(2)

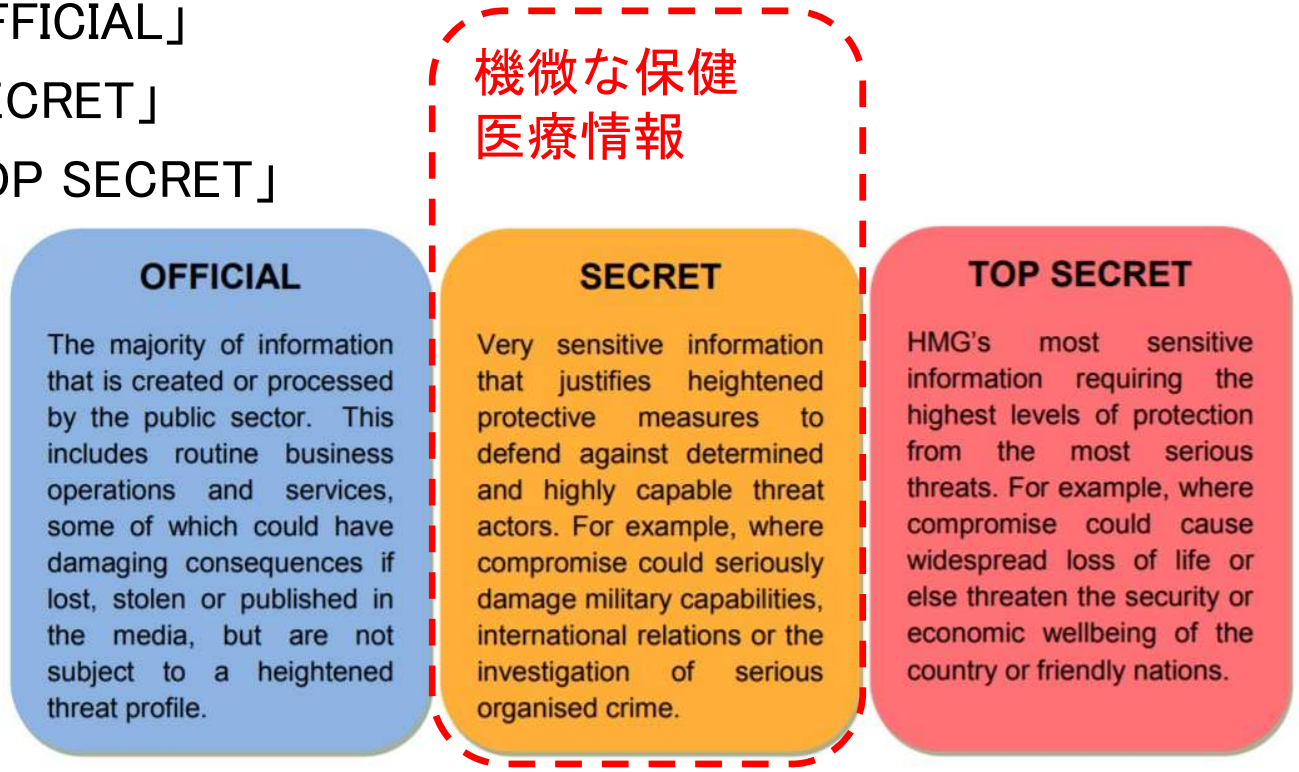
- 英国内閣府「政府クラウド（G-Cloud）戦略」（続き）
  （https://www.gov.uk/government/publications/government-cloud-strategy）
  - G-Cloudプログラムの共通フェデレーションモデル



出典：U.K. Cabinet Office「Government cloud strategy」（2011年10月27日）

1. 英国のオープンガバメント戦略とプレシジョンメディシン(3)

- 英国内閣府「政府セキュリティ分類」(2014年4月施行)
  (https://www.gov.uk/government/publications/government-security-classifications)
  - 政府機関が保有する情報資産の取扱いルール:3区分のセキュリティ分類
    - 「OFFICIAL」
    - 「SECRET」
    - 「TOP SECRET」



出典:U.K. Cabinet Office「Government Security Classifications April 2014」(2013年10月18日)

1. 英国のオープンガバメント戦略とプレシジョンメディシン(4)

- 英国内閣府「政府セキュリティ分類」(2014年4月施行)
  - セキュリティ分類の4原則

原則	内容
原則1	英国政府が、サービスを提供し、政府事業を運営するために、収集、保存、処理、生成または共有する必要があるすべての情報は、内在的価値を保有しており、適切な程度の保護が要求される。
原則2	政府とともに働くすべての人(スタッフ、外部委託先、サービスプロバイダーを含む)は、印が付いているか否かに関係なく、彼らがアクセスするいかなる英国政府の情報またはデータについて、機密保持の義務と保護する責任があり、適切な訓練を受けさせなければならない。
原則3	機微な情報へのアクセスは、純粋な「need to know」原則と適切な従業員のセキュリティコントロールに基づいてのみ付与されなければならない。
原則4	外部パートナーから受け取るまたは交換する資産は、国際的同意・責務を含む、適切な法律または規制の要求事項に応じて保護されなければならない。

出典:U.K. Cabinet Office「Government Security Classifications April 2014」(2013年10月18日)を基にヘルスケアクラウド研究会作成

1. 英国のオープンガバメント戦略とプレシジョンメディシン(5)

- 英国デジタルサービス(GDS)「マーケットプレイスのためのG-Cloudフレームワーク」(初版:2013年9月12日、最新版:2017年5月22日)
  (https://www.gov.uk/guidance/the-g-cloud-framework-on-the-digital-marketplace)
  - 政府機関が利用可能なデジタルマーケットプレイス上のサービス
    - 「G-Cloud」フレームワークを介したクラウドサービス
    - 「Digital Outcomes and Specialists 」フレームワークを介したデジタルアウトカム、デジタルスペシャリスト、ユーザー調査サービス
    - 「Crown Hosting Data Centres」フレームワークを介した物理的なデータセンター空間
  - 「G-Cloud」フレームワーク(最新版はG-Cloud 9)
    - クラウドホスティング
    - クラウドソフトウェア
    - クラウドサポート

「G-Cloud」フレームワークに準拠したクラウドが政府機関の調達対象

1. 英国のオープンガバメント戦略とプレシジョンメディシン(6)

- 政府通信本部(GCHQ)・国家サイバーセキュリティセンター(NCSC)「クラウドセキュリティ原則導入ガイドライン」(2016年9月21日)
  (https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles)
  - 「G-Cloud」フレームワークのセキュリティに関する要求事項14原則
    - クラウドサービス事業者が、「G-Cloud」認定サプライヤーとなるためには、クラウドセキュリティ14原則について自己評価を行い、対象となるサービスがその原則に準拠していることを証明するドキュメントを準備した上で、証拠を提出する必要がある
      ⇒英国政府機関向け調達窓口のデジタルマーケットプレイスで、各事業者のクラウドセキュリティ管理策などが公開される

1. 英国のオープンガバメント戦略とプレシジョンメディシン(7)

- 「G-Cloud」フレームワークのセキュリティに関する要求事項14原則(1)

原則	表題	内容
原則1	転送中のデータの保護	ネットワーク転送中のユーザーデータは、改ざんや傍受に対し、適切に保護されるべきである。
原則2	資産の保護とレジリエンス	ユーザーデータと保存または処理する資産は、物理的な改ざん、損失、損害または占拠に対して保護されるべきである。
原則3	ユーザー間の分離	悪意のあるまたは感染したサービス・ユーザーは、他のサービスまたはデータに影響が及ばないようにすべきである。
原則4	ガバナンス・フレームワーク	サービスプロバイダーは、そのサービスと情報の管理を調整して方向づける、セキュリティガバナンス・フレームワークを有するべきである。このフレームワーク外に導入された、いかなる技術的コントロールも、根底から覆されるであろう。
原則5	運用セキュリティ	攻撃を妨害・検知・予防するために、サービスを、セキュアに運用・管理する必要がある。優れた運用セキュリティは、複雑、官僚的、時間の浪費、高額のプロセスを必要とすべきではない。

1. 英国のオープンガバメント戦略とプレシジョンメディシン(8)

- 「G-Cloud」フレームワークのセキュリティに関する要求事項14原則(2)

原則	表題	内容
原則6	従業員のセキュリティ	信頼するのに高い信頼性が必要なデータやシステムに、サービスプロバイダーの従業員が、アクセスするところ。適切なトレーニングによりサポートされた審査により、サービスプロバイダーの従業員による偶発的もしくは悪意のある漏えいの可能性を少なくする。
原則7.	セキュアな開発	サービスは、セキュリティに対する脅威を特定して低減するために、設計・開発されるべきである。そうでない場合、セキュリティ課題に対する脆弱性があって、データを漏えいしたり、サービスの損失を引き起こしたり、その他悪意のある行動を可能にしたりすることがある。
原則8	サプライチェーン・セキュリティ	サービスプロバイダーは、サービスが実行を要求するすべてのセキュリティ原則を、サプライチェーンが満足のいくようにサポートすることを保証すべきである。

1. 英国のオープンガバメント戦略とプレシジョンメディシン(9)

- 「G-Cloud」フレームワークのセキュリティに関する要求事項14原則(3)

原則	表題	内容
原則9	セキュアなユーザー管理	サービスプロバイダーは、ユーザーがサービス利用をセキュアに管理するためのツールを提供すべきである。管理インタフェースと手順は、権限のないアクセスやユーザーのリソース、アプリケーション、データの変更を予防する、セキュリティの壁の重要な部分である。
原則10	アイデンティティと認証	サービス・インタフェースへのアクセスはすべて、認証されて権限が付与された個人に制限すべきである。
原則11	外部インタフェースの保護	サービスの外部または信頼できないインタフェースをすべて特定して、適切に防御すべきである。
原則12	セキュアなサービス運営	クラウドサービスの運営に使用するシステムは、高い特権が付与されたサービスにアクセスする。これらの漏えいは、セキュリティコントロールを回避して大容量のデータを盗むまたは操作する手段となるなど、重大なインパクトを及ぼすことがある。

1. 英国のオープンガバメント戦略とプレシジョンメディシン(10)

- 「G-Cloud」フレームワークのセキュリティに関する要求事項14原則(4)

原則	表題	内容
原則13	ユーザーの監査情報	サービスへのアクセスをモニタリングする必要がある監査記録とその中に保有するデータを提供すべきである。ユーザーが利用できる監査情報のタイプは、相当の時間的尺度内で、不適切または悪意のある活動を検知して対応する機能に直接インパクトをもたらすことがある。
原則14	サービスのセキュアな利用	クラウドサービスとその内部に保持されるデータのセキュリティは、貧弱なサービスを利用した場合、覆されることがある。その結果として、ユーザーのデータが適切に保護されるためのサービスを利用する時、一定の責任を負うことになる。

出典：GCHQ - NCSC「Guidance - Implementing the Cloud Security Principles」（2016年9月21日）を基にヘルスケアクラウド研究会作成（2017年6月）

1. 英国のオープンガバメント戦略とプレシジョンメディシン(11)

- 英国内閣府「国家サイバーセキュリティ戦略2016-2021年」（2016年11月1日）
  (https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021)
  - 保健・社会医療データの収集、転送、保存、分析、普及のための戦略（NHS傘下の保健機関、NICE、病院、診療所などが対象）
    - 政府、国の重要インフラストラクチャ、広い経済の防御力を強化
    - 官民セクター共通のセキュリティ標準規格を押し上げる一方、サイバー攻撃を低減する技術を適用するために、産業界と連携して取組む
    - 政府とセキュリティが依存する、最も機微な情報およびネットワークが保護されることを保証する

1. 英国のオープンガバメント戦略とプレシジョンメディシン(12)

- 保健省NHSデジタル(旧保健・社会医療情報センター(HSCIC))「ケア向上のための情報技術:保健・社会医療情報センター戦略2015～2020年」(2015年7月21日)
  (https://www.gov.uk/government/publications/hscic-strategy-2015-2020)
  - 保健・社会医療データの収集、転送、保存、分析、普及のための戦略(NHS傘下の保健機関、NICE、病院、診療所などが対象)
    - 全ての市民のデータが保護されていることを保証する
    - みんなに便益のある共有アーキテクチャや標準規格を構築する
    - 国および地域のニーズを満たすサービスを実行する
    - 技術、データ、情報から最善のものを得るように保健医療組織を支援する
    - 保健医療情報をより上手に活用する

1. 英国のオープンガバメント戦略とプレシジョンメディシン(13)

- 全ての市民のデータが保護されていることを保証する（再掲）
  - 全ての市民が、保健・社会医療専門家との正式な対面診察以外に、個人データを共有するための選択を表明できるようにする
  - データフローに関する異なる選択を処理することができ、市民が自分の選択を変えることができるようにする
  - 単独または複数の保健医療提供者と、アプリケーションまたは医療機器からのデータを共有するか否か、市民が意思決定できるようにする
  - いつ、なぜ、自分のデータが直接の医療以外の目的のために利用されたか。市民がわかるようにする
- 「NHSデジタルサイバーセキュリティプログラム（CSP）」
- 「CareCERT (Care Computing Emergency Response Team)」
  (https://www.igt.hscic.gov.uk/CyberWhatIs.aspx)

1. 英国のオープンガバメント戦略とプレシジョンメディシン(14)

- 保健省・全英情報委員会（NIB）
  「個別化された保健医療2020：行動のためのフレームワーク」
  （2014年11月13日）
  （https://www.gov.uk/government/news/introducing-personalised-health-and-care-2020-a-framework-for-action）
  - 市民自身の選択に基づく個人データの共有モデルを採用
    - 2017年までに個人100,000人分のゲノムシーケンス解析を実施
      （ゲノミクス・イングランド）
    - 2018年までに、医師が、総合診療、緊急・救急医療およびその他の医療状況の主要な推移において紙の記録を使用することなく、業務を遂行するようにする
    - 2020年までに、すべての医療記録がデジタル化、リアルタイム化され、相互運用可能になることを目標とする

AGENDA

- 1. 英国のオープンガバメント戦略とプレシジョンメディシン
- 2. 英国のプレシジョンメディシンにおけるクラウド利用事例
  - 2-1. ライフサイエンス事例：Genomics England on UKCloud
  - 2-2. 臨床医療事例：NHS Digital on UKCloud
- 3. CSA STARを活用した共通クラウド基盤のITリスク管理策
- 4. 日本のヘルスケア・イノベーションとクラウド利用に向けて
  - 4-1. シチズン・ドリブン・アプローチの視点から
  - 4-2. データ・ドリブン・アプローチの視点から

2-1. ライフサイエンス事例：Genomics England on UKCloud(1)

- 保健省「ゲノミクス・イングランド」（https://www.genomicsengland.co.uk/）
  - ゲノミクス・イングランドは、参加者の自発的同意と公的支援とともに、10万ゲノムのシーケンス解析を通して、患者、NHS（国民保健サービス）、英国経済の永続的な蓄積を構築する
  - 目的
    - 患者に便益をもたらす
    - コンセントに基づく倫理的で透明性のあるプログラムを構築する
    - 新たな科学的発見と医療的洞察を可能にする
    - 英国ゲノム産業の構築を一気にスタートさせる
  - 2012年、「10万ゲノム解析プロジェクト」を開始
    ＜注力領域＞
    - 希少性疾患
    - がん

2-1. ライフサイエンス事例：Genomics England on UKCloud(2)

- （続き）
  - プロジェクトの課題
    - ゲノム解析の課題：提供する情報の品質保証
    - データの課題：ゲノムの差異の意味と重要性の解釈
    - セキュリティの課題：大容量のゲノムデータのセキュアな保存
    - 患者に対する便益の提供
  - 懸念事項
    - 倫理問題：独立した倫理諮問委員会によるチェック
    - 商用化による便益を誰が受けるか：インフォームドコンセント取得時の説明で納得が得られるか
    - プライバシーと機密保持の問題：データ諮問委員会による監視、患者固有識別子の匿名化

2-1. ライフサイエンス事例：Genomics England on UKCloud(3)

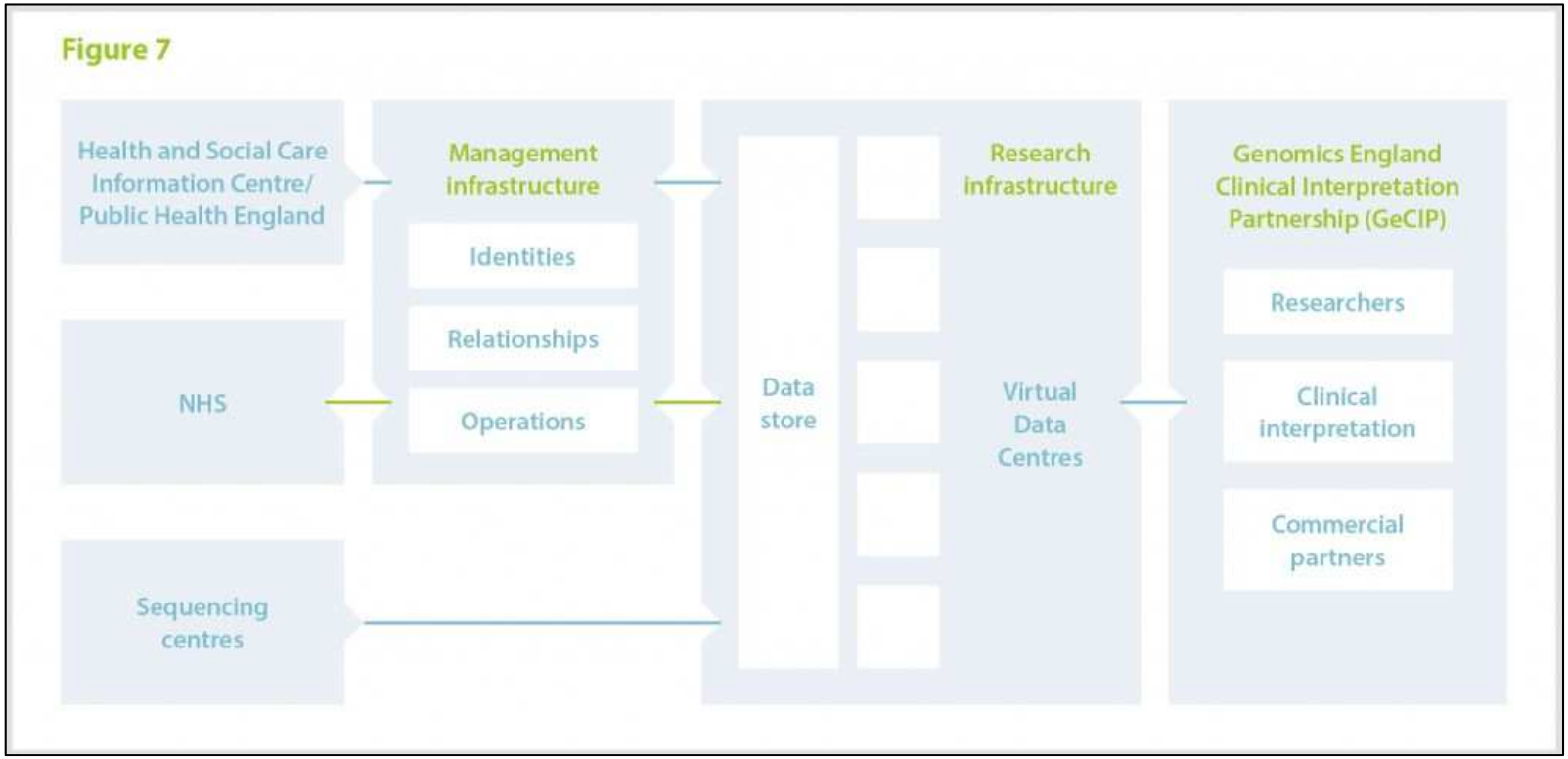
- 「ゲノミクス・イングランド」の情報／データガバナンス対策
  - 10万ゲノム解析プロジェクト・プロトコル（https://www.genomicsengland.co.uk/100000-genomes-project-protocol/）
  - 主要データソース（構造化データ、半構造化データ、非構造化データ）（https://www.genomicsengland.co.uk/the-100000-genomes-project/data/data-types-and-storage/）
    - NHSデジタル
      - 病院活動統計（HES）
      - 患者報告アウトカム測定データ（PROMs）
      - メンタルヘルスおよび障がい学習セット（MHLDS）
      - 診断画像データセット（DID）
      - 死亡率データ
    - パブリックヘルス・イングランド
      - 国立がん登録サービスの収集データ

2-1. ライフサイエンス事例：Genomics England on UKCloud(4)

- 「ゲノミクス・イングランド」の情報／データガバナンス対策
  - 情報セキュリティの責任分担
    - 上級情報リスクオーナー（SIRO）
    - 情報ガバナンス・リード（IG Lead）
    - 情報資産オーナー（IAO）
    - ラインマネージャー（*非常勤スタッフ、外部委託先の管理）
    - 全スタッフ　など
  - ポリシー集
    （https://www.genomicsengland.co.uk/the-100000-genomes-project/data/）
    - 情報ガバナンス管理フレームワークとポリシー
    - 機密保持とデータ保護ポリシー
    - 情報セキュリティポリシー
    - 情報品質および記録管理ポリシー
    - データアクセスおよび許容される利用ポリシー　など

2-1. ライフサイエンス事例：Genomics England on UKCloud(5)

- 「ゲノミクス・イングランド」のデータ保存・分析システム
  - システムの全体イメージ（クラウドを活用）



出典：Genomics England「Data types and storage in the 100,000 Genomes Project」
（https://www.genomicsengland.co.uk/the-100000-genomes-project/data/data-types-and-storage/）

2-1. ライフサイエンス事例：Genomics England on UKCloud(6)

- アウトリーチ活動：市民への便益の還元・可視化
  - 「*The Challenges of Genome Analysis in the Health Care Setting*」
    Anneke Lucassen, and Richard S. Houlston
    Genes (Basel). 2014 Sep; 5(3): 576–585.
    (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4198918/)
  - 「*The DNA of a nation*」
    Vivien Marx
    Nature 524, 503–505 (27 August 2015) doi:10.1038/524503a
    (https://www.nature.com/nature/journal/v524/n7566/full/524503a.html)


genes
ISSN 2073-4425
www.mdpi.com/journal/genes
Review
The Challenges of Genome Analysis in the Health Care Setting
Anneke Lucassen [1,*] and Richard S. Houlston [2]
1 Clinical Ethics and Law Unit, Wessex Clinical Genetics Service, The Princess Anne Hospital, Southampton, SO16 5YA, UK
2 Division of Genetics and Epidemiology, The Institute of Cancer Research, Sutton, Surrey SM2 5NG, UK; E-Mail: richard.houlston@icr.ac.uk
* Author to whom correspondence should be addressed; E-Mail: A.M.Lucassen@soton.ac.uk; Tel.: +44-0-0238-777-7222.
Received: 27 May 2014; in revised form: 4 July 2014 / Accepted: 7 July 2014 /
Published: 22 July 2014
Abstract: Genome sequencing is now a sufficiently mature and affordable technology for clinical use. Its application promises not only to transform clinicians' diagnostic and predictive ability, but also to improve preventative therapies, surveillance regimes, and tailor patient treatment to an individual's genetic make-up. However, as with any technological advance, there are associated fresh challenges. While some of the ethical, legal and social aspects resulting from the generation of data from genome sequencing are generic, several nuances are unique. Since the UK government recently announced plans to sequence the genomes of 100,000 Health Service patients, and similar initiatives are being considered elsewhere, a discussion of these nuances is timely and needs to go hand in hand with formulation of guidelines and public engagement activities around implementation of sequencing in clinical practice.
Keywords: genome sequencing; clinical practice; incidental findings; consent; disclosure
1. Introduction
The speed by which a person's genome can be analysed has increased phenomenally over recent years, while the attendant costs have plummeted. As a result, genetic testing is shifting from a targeted approach analysing specific genes based on particular symptoms or family histories to sequencing of an entire exome or genome (whole exome sequencing [WES], whole genome sequencing [WGS]).


THE DNA OF A NATION
The United Kingdom aims to sequence 100,000 human genomes by 2017. But screening them for disease-causing variants will require innovative software.
BY VIVIEN MARX

2-1. ライフサイエンス事例：Genomics England on UKCloud(7)

- ゲノミクス・イングランドで利用されるパブリック・クラウドサービス（例）
  - UKCloud
    - 2011年、イングランド南部のハンプシャー州ファーンボローに設立されたスカイスケープ・クラウドサービス（クラウドセキュリティアライアンスのコアメンバー）が前身の英国企業
      （2016年8月、「UKCloud」に社名変更）
    - 政府機関向けのパブリッククラウド・サービス提供が主要事業 （英国内2か所のデータセンターで対応）
    - UKCloud上に、ゲノミクス・イングランド・プラットフォームを構築
      （仮想デスクトップ環境をクラウド上に構築し、ゲノミクス・イングランドが運用）
    - UKCloudのHybridConnectサービスを利用して、ゲノミクス・イングランドの10Gbit/sの接続を実現
    - （参考）「*The secrets of a successful big data implementation*」
      （https://ukcloud.com/wp-content/uploads/2016/08/UKCloud WhitePaper RGB Digital Secrets of a successful Big Data implementation.pdf）

2-2. 臨床医療事例：NHS Digital on UKCloud(1)

- **2015年1月8日：HSCIC（現NHSデジタル）が、NHS全国ネットワーク（N3）のアグリゲーターに、スカイスケープ・クラウドサービス（現UKCloud）を採用**
  ⇒ UKCloudは、下位レイヤからのクラウド化を支える
  （https://ukcloud.com/news-resources/news/recent-press-releases/assured-cloud-services-now-available-nhs-via-n3）
- **2017年4月13日：NHSデジタルが「総合診療データハブ」を開設**
  （https://www.digital.nhs.uk/GP-Data-Hub）
  - 総合診療レベルのデータをオープンデータライセンスで公開
    - Quality Outcomes Framework in the GP data hub
      （https://www.digital.nhs.uk/GP-data-hub/quality-outcomes-framework-in-GP-data-hub）
    - Workforce data in the GP data hub
      （https://www.digital.nhs.uk/GP-data-hub/workforce-data-in-GP-data-hub）
    - GP list size in the GP data hub
      （https://www.digital.nhs.uk/GP-data-hub/GP-list-size-in-GP-data-hub）

2-2. 臨床医療事例：NHS Digital on UKCloud(2)

- 総合診療レベルのデータをオープンデータライセンスで公開（続き）
  - Health and care of people with learning disabilities in the GP practice data hub
    （https://www.digital.nhs.uk/GP-data-hub/health-care-learning-disabilities-in-GP-data-hub）
  - Dementia 65+ Estimated Diagnosis Rate Indicator in the GP data hub
    （https://www.digital.nhs.uk/GP-data-hub/Dementia-65-Estimated-Diagnosis-Rate-Indicator）
  - Patient Online Management Information in the GP data hub
    （https://www.digital.nhs.uk/GP-data-hub/patient-online-management-information）
- **2017年5月10日：UKCloudが、医療産業向けの新部門としてUKCloud Healthの創設を発表**
  （https://ukcloud.com/news-resources/news/news/ukcloud-replicates-public-sector-success-new-healthcare-division）
- **2017年6月6日：UK Cloud Healthが、米国の医療保険の携行性.と責任に関する法律（HIPAA）を遵守したクラウドホスティング・サービスを提供していることを公表**
  （https://ukcloud.com/news-resources/news/rss-news/ukcloud-health-offers-hipaa-compliant-cloud-hosting）

2-2. 臨床医療事例：NHS Digital on UKCloud(3)

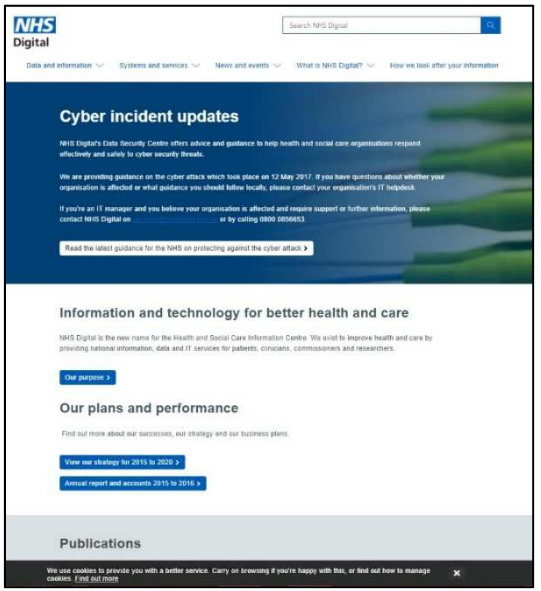
- **2016年：主要グローバル・クラウドサービスプロバイダーの英国内データセンター開設ラッシュ（G-Cloudフレームワーク対応）**
  - Microsoft「Microsoft announces plans to offer cloud services from the UK」（2015年11月10日）
    （https://news.microsoft.com/en-gb/2015/11/10/microsoft-announces-plans-to-offer-cloud-services-from-the-uk/）
  - Google Blog「Google Cloud Platform sets a course for new horizons」（2016年9月29日）
    （https://cloudplatform.googleblog.com/2016/09/Google-Cloud-Platform-sets-a-course-for-new-horizons.html）
  - Amazon Web Services「Now Open – AWS London Region」(2016年12月13日）
    （https://aws.amazon.com/jp/blogs/aws/now-open-aws-london-region/）

2-2. 臨床医療事例：NHS Digital on UKCloud(4)

- 病院や地域の医療サービスの運営母体であるNHSトラストのクラウド化（アプリケーション主導）事例
  - 南ロンドン・モーズレイNHS財団トラスト × Microsoft Office 365
    ・「SLAM gets connected with Office 365」
    （https://enterprise.microsoft.com/en-gb/customer-story/industries/public-sector/health/slam-gets-connected-office-365/）
  - ロンドン・ロイヤルフリー病院 ×Google DeepMind
    ・「Working with the NHS」
    （https://deepmind.com/applied/deepmind-health/working-nhs/）
    ・「Working with the NHS to build lifesaving technology」
    （https://deepmind.com/blog/working-nhs-build-lifesaving-technology/）
    ・「DeepMind Health and the Royal Free」
    （https://deepmind.com/applied/deepmind-health/working-nhs/how-were-helping-today/royal-free-london-nhs-foundation-trust/）
  - ロンドン・ムーアフィールド眼科病院 ×Google DeepMind
    ・「DeepMind Health research partnership」
    http://www.moorfields.nhs.uk/landing-page/deepmind-health-research-partnership

2-2. 臨床医療事例：NHS Digital on UKCloud(5)

- 2017年5月：
  英国・国民保健サービス（NHS）関連の医療施設で、マルウェア「WannaCry」に起因する被害が多発
  （＊NHSのクラウド側の被害に関する報告はなし）
  - 政府通信本部（GCHQ）傘下の国家サイバーセキュリティセンター（NCSC）、保健省、NHSイングランドと連携して、各組織の支援に当たっていることを公表
    ＜NHSデジタルの対策＞
    - サイバー攻撃に対する保護策としてのパッチに関する説明文書、テクニカルガイドライン、FAQ集
    - 予防策としてインターネットから遮断したネットワークの再接続に関するテクニカルガイドライン
    - NHSmail
    - CareCERT bulletin



出典：NHS Digital（2017年5月18日更新）

2-2. 臨床医療事例：NHS Digital on UKCloud(6)

＜NHSデジタルが傘下の関連施設向けにとった緊急マルウェア対策＞

- このインシデントのケースと同様に、既知のサイバーセキュリティ脅威およびこれらのリスクを最小化するための適切なステップに関する情報を、NHSの組織に拡散する
- 強固なセキュリティ措置を有するように全て設計された、国のNHS ITサービスのシステムに対する予防的なリアルタイムのモニタリング
- NHS組織向けの無料サイバーセキュリティ検証に着手し、彼らが採ることができる適切なステップに関する特別なアドバイスをする
- 最前線の従事者が、組織におけるサイバーセキュリティの保証に向けた自分自身の責任を認識するとともに、組織のセキュリティ維持に役立てるために採ることができる簡単なステップを知ることを確実にするように設計された、保健医療スタッフ向けのトレーニング

AGENDA

- 1. 英国のオープンガバメント戦略とプレシジョンメディシン
- 2. 英国のプレシジョンメディシンにおけるクラウド利用事例
  - 2-1. ライフサイエンス事例：Genomics England on UKCloud
  - 2-2. 臨床医療事例：NHS Digital on UKCloud
- 3. CSA STARを活用した共通クラウド基盤のITリスク管理策
- 4. 日本のヘルスケア・イノベーションとクラウド利用に向けて
  - 4-1. シチズン・ドリブン・アプローチの視点から
  - 4-2. データ・ドリブン・アプローチの視点から

3. CSA STARを活用した共通クラウド基盤のITリスク管理策(1)

- 米国：健康医療固有の法規制＋パブリックセクターのセキュリティ要件＋サイバーセキュリティ要件

CSA Cloud Controls Matrix (CCM)

（https://cloudsecurityalliance.org/research/ccm/）

健康医療分野のクラウドセキュリティの視点
例．-HIPAA／HITECH監査への対応:リスク評価
（http://www.hhs.gov/ocr/privacy/）

パブリックセクターのクラウドセキュリティの視点
例．Federal Risk and Authorization Management Program (FedRAMP)
（http://www.fedramp.gov/）

ホームランドセキュリティ／重要情報インフラの視点
例．Federal Information Security Management Act（FISMA）
（http://csrc.nist.gov/groups/SMA/fisma/index.html）

3. CSA STARを活用した共通クラウド基盤のITリスク管理策(2)

- 英国：健康医療固有の法規制＋パブリックセクターのセキュリティ要件＋サイバーセキュリティ要件

CSA Cloud Controls Matrix (CCM)

（https://cloudsecurityalliance.org/research/ccm/）

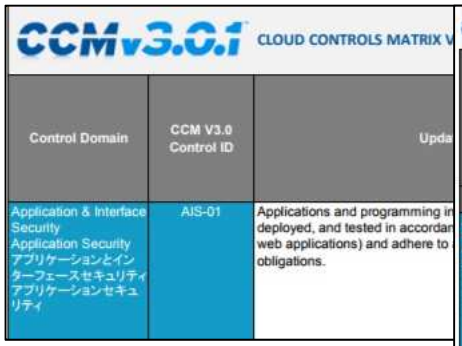
健康医療分野のデータ保護の視点
例.「ケア向上のための情報技術：保健・社会医療情報センター戦略2015～2020年」、「個別化された保健医療2020：行動のためのフレームワーク」

パブリックセクターのクラウドセキュリティの視点
例.「政府クラウド戦略」、「マーケットプレイスのためのG-Cloudフレームワーク」、「クラウドセキュリティ原則導入ガイドライン」

ホームランドセキュリティ／重要情報インフラの視点
例.「政府ICT戦略」、「国家サイバーセキュリティ戦略2016-2021年」

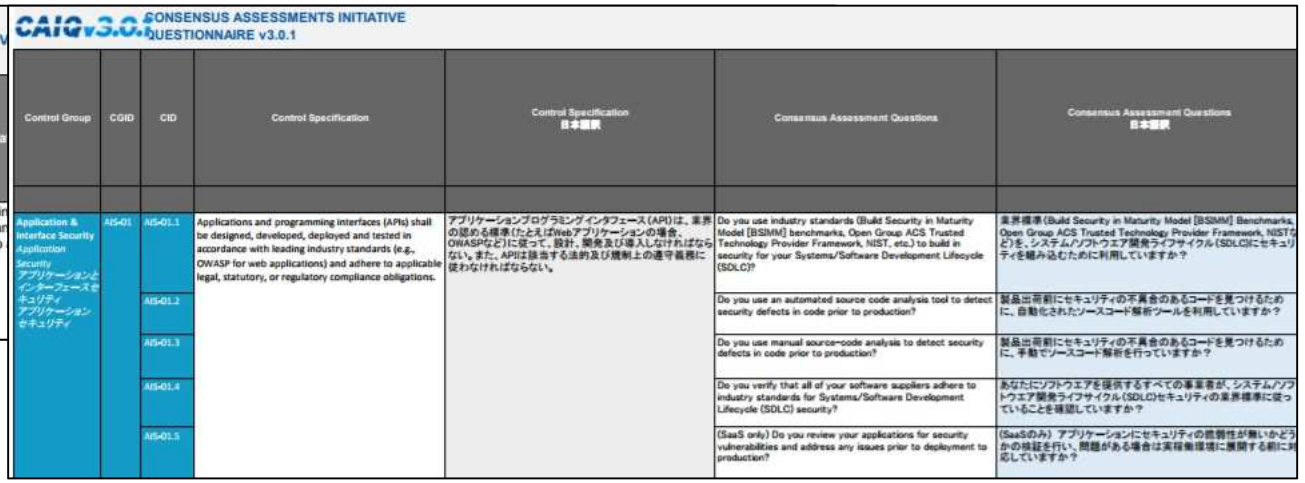
3. CSA STARを活用した共通クラウド基盤のITリスク管理策(3)

- CCS-STAR認証プログラム
  - ISO/IEC 27001の要求事項(情報セキュリティマネジメントシステム)とCSAのクラウドコントロールマトリックス(CCM)を用いて、クラウドサービス事業者のセキュリティを第三者が評価する制度
  - CCMにはクラウドサービスのセキュリティの成熟度を測る具体的な基準が定められており、11の管理エリアにおける成熟度が審査される
  - CAIQ(Consensus Assessments Initiative Questionnaire):
    CCMに基づくサービス事業者に対する質問事項



CCM v3.0.1 CLOUD CONTROLS MATRIX V

Control Domain	CCM V3.0 Control ID	Upda
Application & Interface Security Application Security アプリケーションとインターフェースセキュリティ アプリケーションセキュリティ	AIS-01	Applications and programming in deployed, and tested in accordar web applications) and adhere to obligations.



CAIQ v3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Control Specification 日本語訳	Consensus Assessment Questions	Consensus Assessment Questions 日本語訳
Application & Interface Security Application Security アプリケーションとインターフェースセキュリティ アプリケーションセキュリティ	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーションプログラミングインタフェース(API)は、業界の認める標準(たとえばWebアプリケーションの場合OWASPなど)に従って、設計、開発及び導入しなければならない。また、APIは該当する法的及び規制上の遵守義務に従わなければならない。	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	業界標準(Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NISTなど)を、システム/ソフトウエア開発ライフサイクル(SDLC)にセキュリティを組み込むために利用していますか?
		AIS-01.2			Do you use an automated source code analysis tool to detect security defects in code prior to production?	製品出荷前にセキュリティの不具合のあるコードを見つけるために、自動化されたソースコード解析ツールを利用していますか?
		AIS-01.3			Do you use manual source-code analysis to detect security defects in code prior to production?	製品出荷前にセキュリティの不具合のあるコードを見つけるために、手動でソースコード解析を行っていますか?
		AIS-01.4			Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	あなたにソフトウエアを提供するすべての事業者が、システム/ソフトウエア開発ライフサイクル(SDLC)セキュリティの業界標準に従っていることを確認していますか?
		AIS-01.5			(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	(SaaSのみ) アプリケーションにセキュリティの脆弱性が無いかどうかの検証を行い、問題がある場合は実稼働環境に展開する前に対応していますか?

3. CSA STARを活用した共通クラウド基盤のITリスク管理策(4)

- （CSA STAR認証の例）英国：UKCloud
  （https://cloudsecurityalliance.org/star-registrant/ukcloud-ltd/）

＊CCM／CAIQ／CSA STAR認証関連公開情報を共通の評価指標として活用すると、クラウド事業者間の相対的な比較が可能

⇒ ユーザー側の評価にも活用できる

CAIQ v3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

UKCloud Introduction

The Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) is a comprehensive framework of questions and responses which potential UK public sector customers can make reference to to assess and understand the information security, data governance and related privacy elements of consuming UKCloud Ltd services. This response is one element of UKCloud's available information security related documentation, which also includes G-Cloud "Evidence Packs", RMADS (Risk Management and Accreditation Documentation Set), and other accreditation and certification documents (e.g. ISO27001, ISO27018, Cyber Essentials Plus, PSN etc.)

This response has been compiled and is provided for informational purposes only, and individual responses may change without notice. Potential UK public sector customers are encouraged to engage with UKCloud Ltd to seek clarity or confirm the ongoing accuracy of individual responses. Please note that this document does not confer any legal rights or intellectual property in any UKCloud Ltd service, although you may copy and use this document for your own internal purposes. The supply of UKCloud Ltd services are subject to the agreement of a separate, legally binding agreement.

For further information on UKCloud accreditations and certifications, visit http://ukcloud.com/why-choose-ukcloud/accreditations-certifications, or contact the UKCloud Compliance Team.

Responses are © UKCloud Ltd 2016. E&OE. Tel: +44 (0) 1252 303 300 www.ukcloud.com

Control Group	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
Application & Interface Security Application Security	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Y			UKCloud's Development Team fully adhere to the Open Web Application Security Project (OWASP) Standards to ensure high levels of security within our Systems/Software Development Lifecycle (SDLC).
	AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	Y			UKCloud's Development Teams use Test Driven Development (TDD) practices where applicable. All code is peer reviewed prior to being committed to a source code repository where each change is linked to a requirement. Software is then packaged via a continuous integration process after which it is subject to manual or automated regression tests in a dedicated QA environment. Final acceptance, integration and regression testing is performed in a pre-production test environment. Software can only be released to production servers once it has been approved by the UKCloud Change Advisory Board (CAB).
	AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	Y			UKCloud has a formal source-code review process in place to analyse code before it is merged into the production environment for deployment.
	AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Y			Where a third party is recorded as being an essential element of the service, UKCloud will always engage an existing partner to minimise supplier engagement and provide the strongest controls for information within the supply chain. All UKCloud suppliers undergo a thorough selection process, and regular due diligence and audit checks are conducted during the lifecycle of the service. For software suppliers, this includes an assessment of their approach to Systems/Software Development Lifecycle (SDLC) security. Evidence of assessment of third party security capabilities been evidenced during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001 (Information Security Management) certifications, undertaken regularly by LRQA.
	AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Y			UKCloud evaluates all software used for Software as a Service purposes which includes specific security checking. All software offered to UKCloud customers is subject to external penetration and vulnerability testing by an approved, external security testing organisation. UKCloud customers are advised of a pending significant feature release via notifications posted within the Customer Portal. Wherever possible, feature releases are undertaken during normal office hours, to ensure that maximum benefit from development and support resources are available to support customers, if required. All release activities are protected by rollback plans to a previous version. The activities surrounding coding, testing and deployment have been independently validated by a CESG Pan Government Accreditor scoped IT Security Health Checks (ITSHC CHECK) undertaken by an independent organisation.
Application & Interface Security Customer Access Requirements	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Y			The identification of all security, contractual and regulatory requirements for customers to access and use UKCloud services are documented and communicated, and require customer contractual approval, before customers are granted access to data, assets and information systems. This activity is overseen and enforced by the UKCloud Commercial Team.
	AIS-02.2		Are all requirements and trust levels for customers' access defined and documented?	Y			UKCloud has implemented and operates a number of technical controls to ensure only authorised individuals are able to authenticate to and access the UKCloud services for which they have an identified and approved business need. UKCloud has implemented and provides Role Based Access Control (RBAC) capabilities, allowing customer system administrators to determine the level of access and privileges that their users have. UKCloud only provides one system administrator account when the service is commissioned; beyond that the customer organisation is fully responsible for determining, creating, managing and deleting their own user accounts and their permissions. UKCloud personnel are additionally required to use 2FA authentication tokens.
Application & Interface Security Data Integrity	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Y			UKCloud developed Application Programming Interfaces (APIs) are used to validate acceptable input both to guard against systematic processing errors and malicious attacks/corruption of data.

出典：Cloud Security Alliance「STAR Registrant UKCloud Ltd」（2016年10月28日）

AGENDA

- 1. 英国のオープンガバメント戦略とプレシジョンメディシン
- 2. 英国のプレシジョンメディシンにおけるクラウド利用事例
  - 2-1. ライフサイエンス事例：Genomics England on UKCloud
  - 2-2. 臨床医療事例：NHS Digital on UKCloud
- 3. CSA STARを活用した共通クラウド基盤のITリスク管理策
- 4. 日本のヘルスケア・イノベーションとクラウド利用に向けて
  - 4-1. シチズン・ドリブン・アプローチの視点から
  - 4-2. データ・ドリブン・アプローチの視点から

4-1. シチズン・ドリブン・アプローチの視点から(1)

- **UKCloud「Key characteristics of cloud applications」（2016年7月）**
  （https://ukcloud.com/wp-content/uploads/2016/07/UKCloud_Blueprint_UKC-GEN-132_Key-characteristics-of-cloud-applications.pdf）
  - **クラウドアプリケーションの特徴**
    - **プロビジョニングの自動化（ユーザーから要求があった場合や障害時などに、必要な分だけ、コンピュータリソースを自動的に別のシステムに割り当てられる）**
    - **レジリエンスと冗長性（影響を受けないようにする対応力と、影響を受けても早期に元通りの状態に戻れるようにする復旧力の強化）**
    - **高可用性（エラーチェックと代替機能の確保）**
    - **マイクロサービス（簡素化と拡張性）**
    - **疎結合（SOA、メッセージクエリなどの導入）**

出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

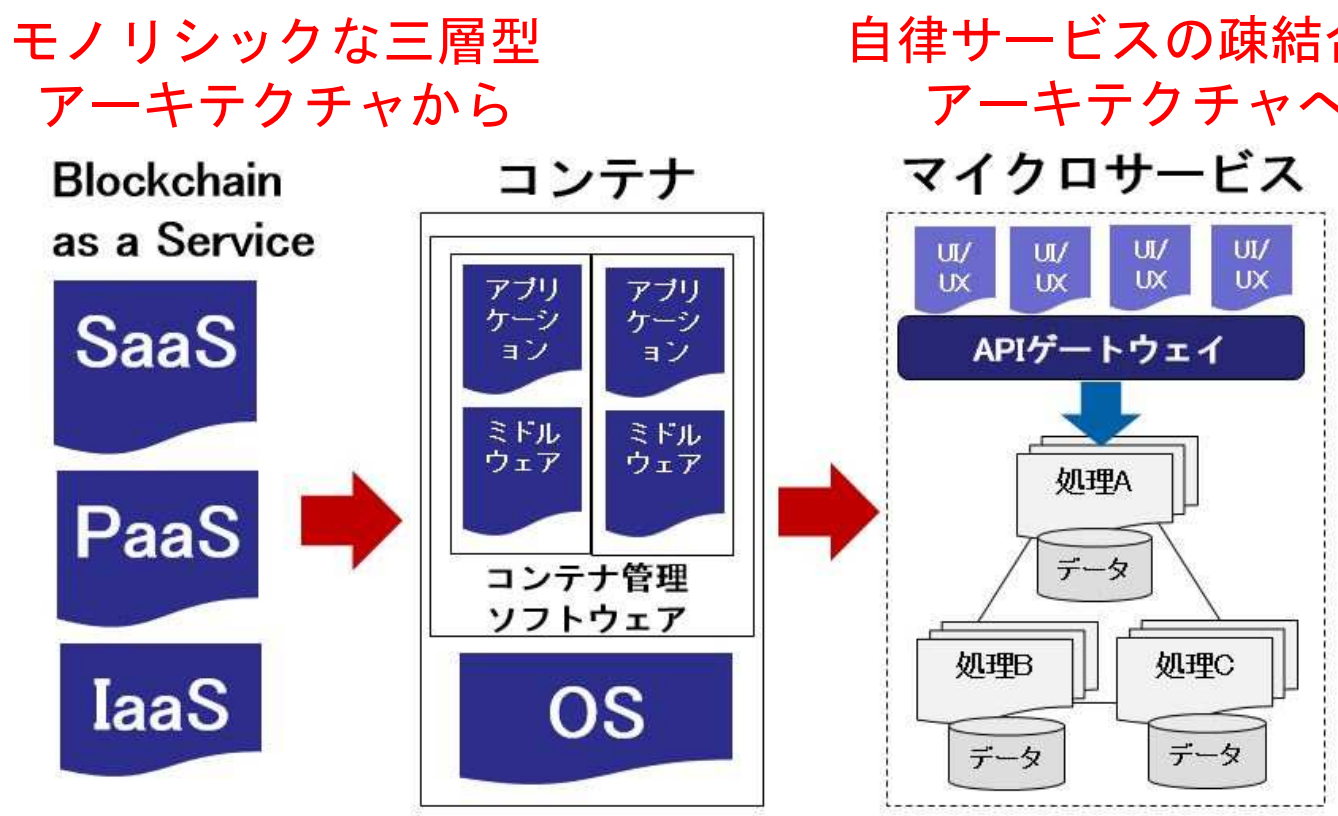
4-1. シチズン・ドリブン・アプローチの視点から(2)

- クラウドアプリケーションの特徴（続き）
  - 水平拡張性（自動拡張）
  - 非依存性（標準化によるロックインの防止）
  - 状態を保持しないシェアード・ナッシング・アーキテクチャ
  - 拡張性のあるオブジェクトストレージ
  - ライセンシングとオープンソース
  - クラウドセキュリティ（「G-Cloud」フレームワークのセキュリティに関する要求事項14原則）

出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

4-1. シチズン・ドリブン・アプローチの視点から(3)

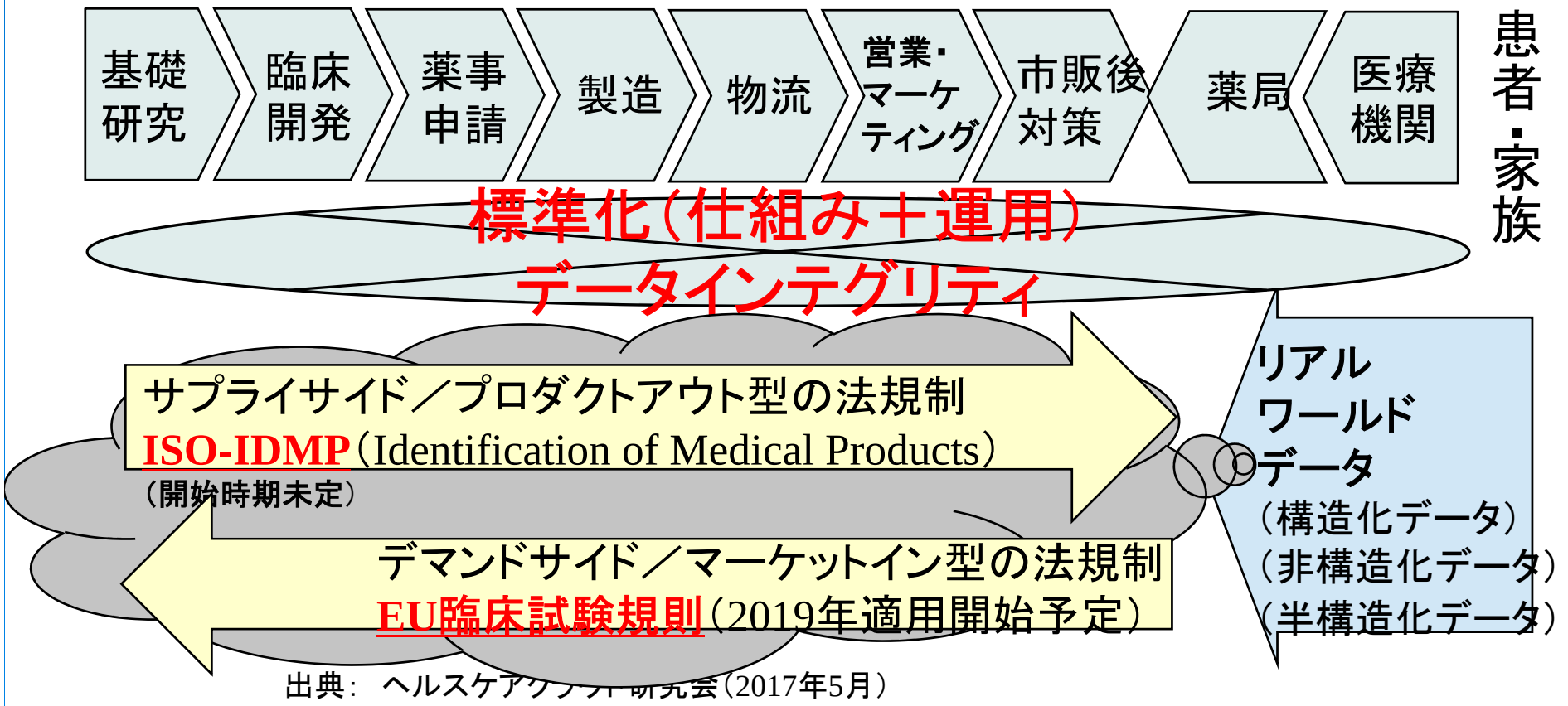
- コンシューマードリブンなxTechサービス（HealthTech含む）のビジネスモデルはSaaSからマイクロサービスへ



出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

4-2. データ・ドリブン・アプローチの視点から(1)

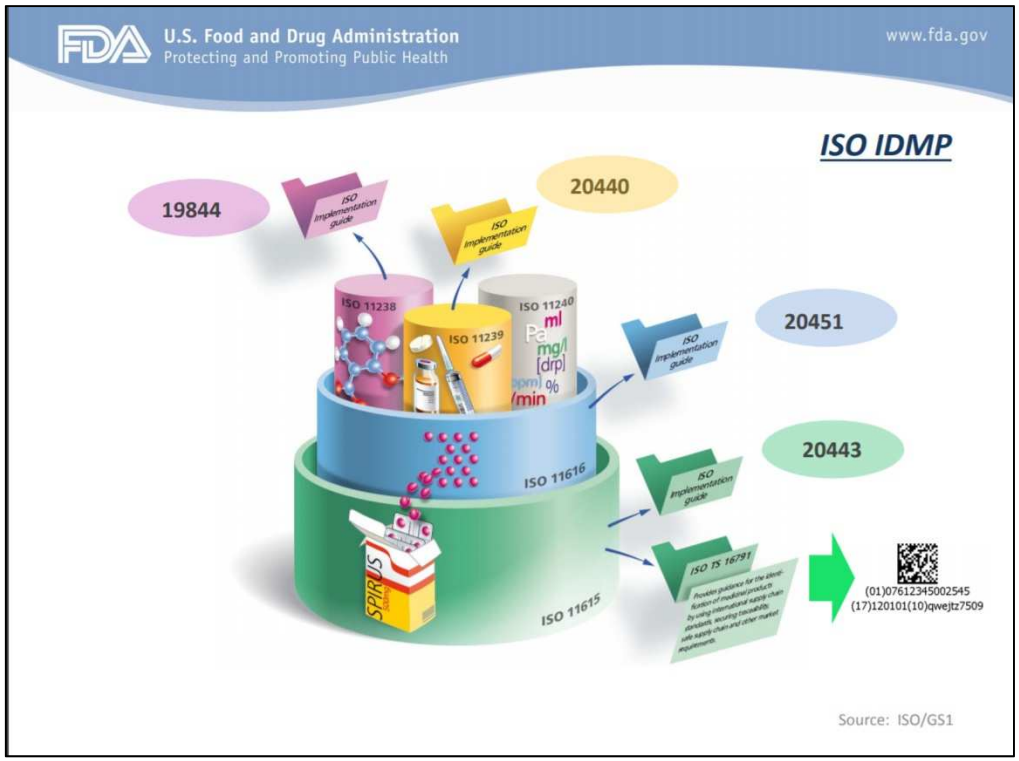
- クラウド環境＝健康医療バリューチェーンを繋ぐ共通基盤
  ⇒イノベーションのエネイブラーとして利活用すべき



出典：ヘルスケアクラウド研究会（2017年5月）

4-2. データ・ドリブン・アプローチの視点から(2)

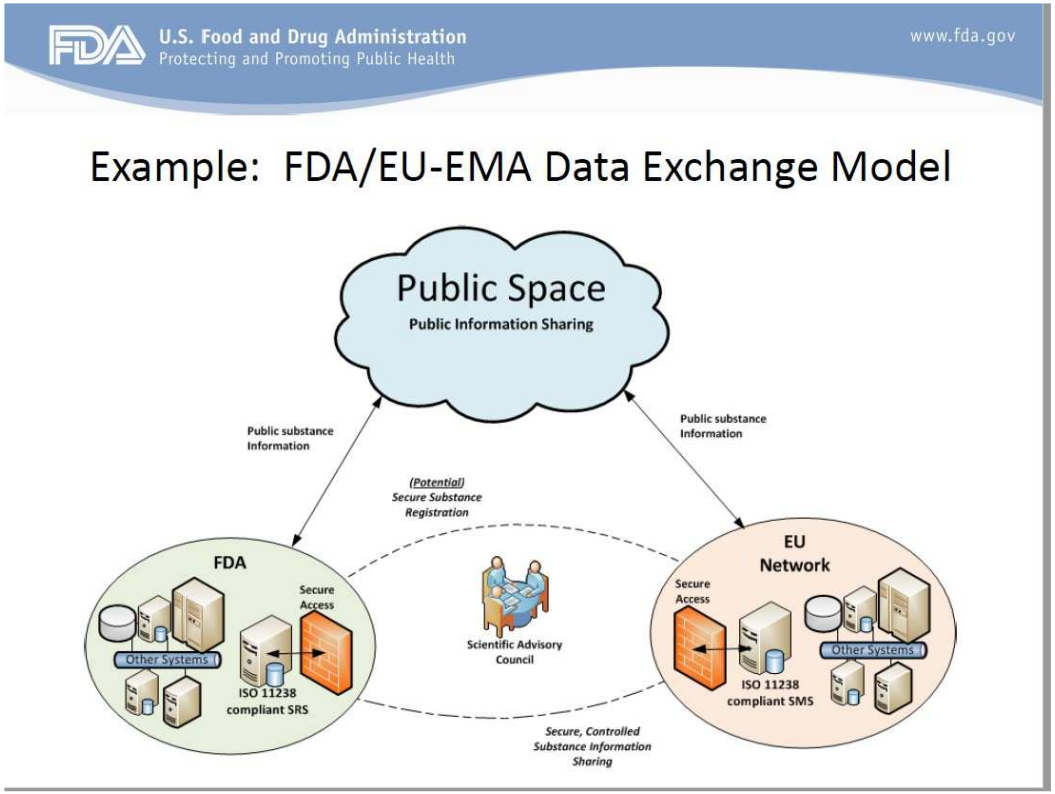
- **ISO-IDMP（Identification of Medical Products）（適用開始時期未定）**



出典： FDA「Global Identification of Medicinal Products (IDMP)」(2016年2月8日）
(https://www.fda.gov/downloads/drugs/developmentapprovalprocess/formssubmissionrequirements/electronicsubmissions/ucm489459.pdf)

4-2. データ・ドリブン・アプローチの視点から(3)

- **ISO-IDMPを介した欧米間のハーモナイゼーションの検討（例）**



出典： FDA「Global Identification of Medicinal Products (IDMP)」(2016年2月8日）
(https://www.fda.gov/downloads/drugs/developmentapprovalprocess/formssubmissionrequirements/electronicsubmissions/ucm489459.pdf)

4-2. データ・ドリブン・アプローチの視点から(4)

EU臨床試験規則（2019年適用開始予定）

出典： European Medicines Agency「Clinical Trial Regulation」
(http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/general/general_content_000629.jsp)