ヘルスケア・イノベーション
公開勉強会 #1

2017年5月31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

https://www.cloudsecurityalliance.jp/

AGENDA

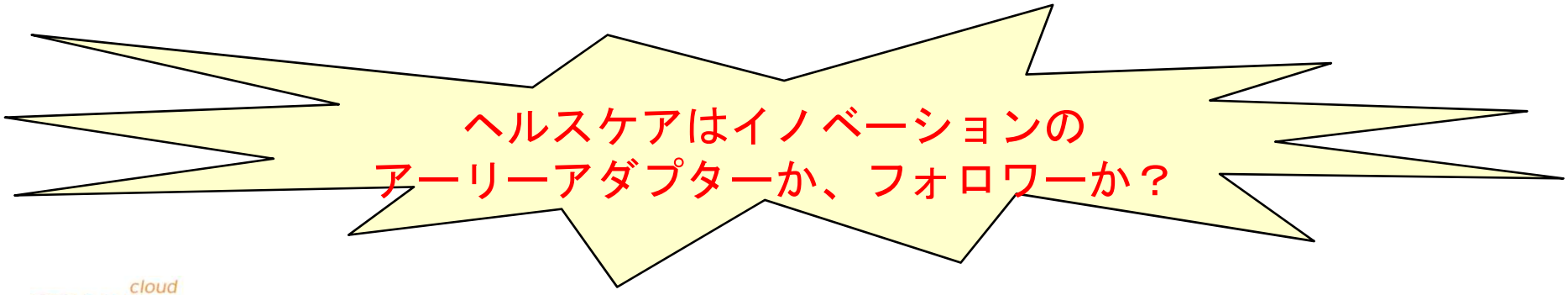
- 1. 勉強会発足の目的
- 2. クラウドを活用したヘルスケア・イノベーションの全体動向とセキュリティ課題
- 3. ディスカッション

AGENDA

- 1. 勉強会発足の目的
  - 1-1.勉強会発足の目的
  - 1-2. CSAセキュリティガイドライン類のヘルスケア分野への適用例

1-1.勉強会発足の目的

- 目的：患者／生活者中心の視点から、クラウドを利用した健康増進／医療／介護分野のイノベーションにおけるセキュリティ／プライバシー保護の課題解決を支援するための基本的な調査研究を提供し、エンドユーザー向けのクラウドセキュリティに関する啓発活動を推進することを目的とする。
- 活動主体
  - 主催：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ワーキンググループ
    責任者：リーダー・博士（医薬学） 笹原英司



1-2. CSAセキュリティガイドライン類のヘルスケア分野への適用例(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/）

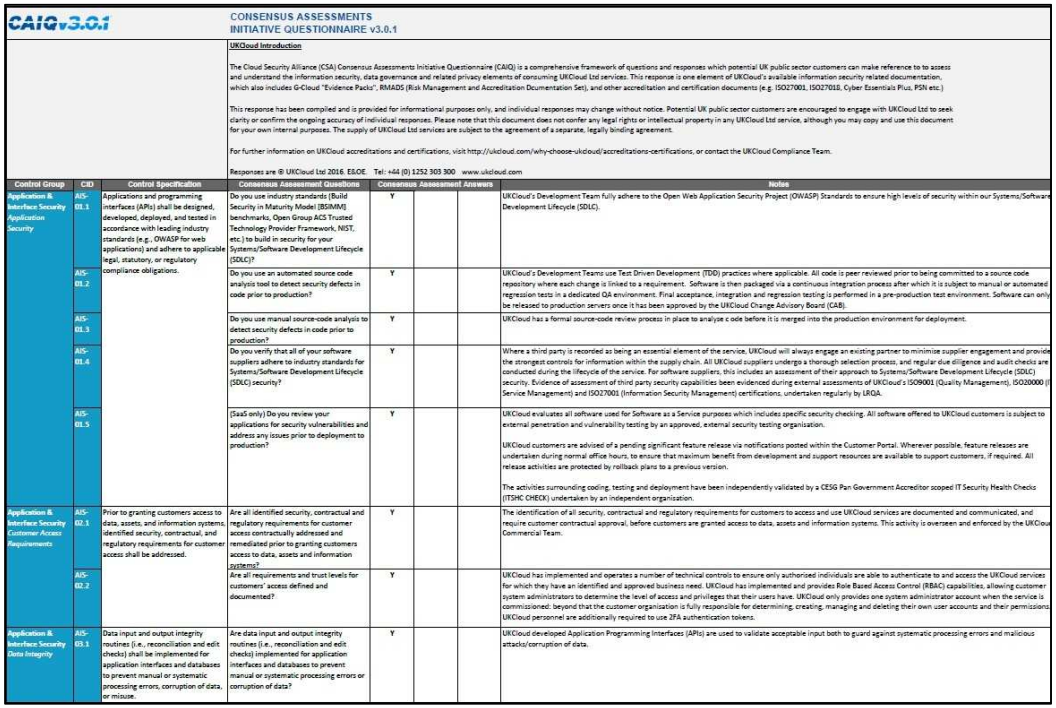
健康医療分野のクラウドセキュリティの視点
例．-HIPAA／HITECH監査への対応:リスク評価
（http://www.hhs.gov/ocr/privacy/）

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）

1-2. CSAセキュリティガイドライン類のヘルスケア分野への適用例(2)

- （例）英国：UKCloud
  （https://cloudsecurityalliance.org/star-registrant/ukcloud-ltd/）
  - ライフサイエンス研究開発のユーザー事例：Genomics England
  - 医療保険者／医療機関のユーザー事例：National Health Service（NHS）



CAIQv3.0.1 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.

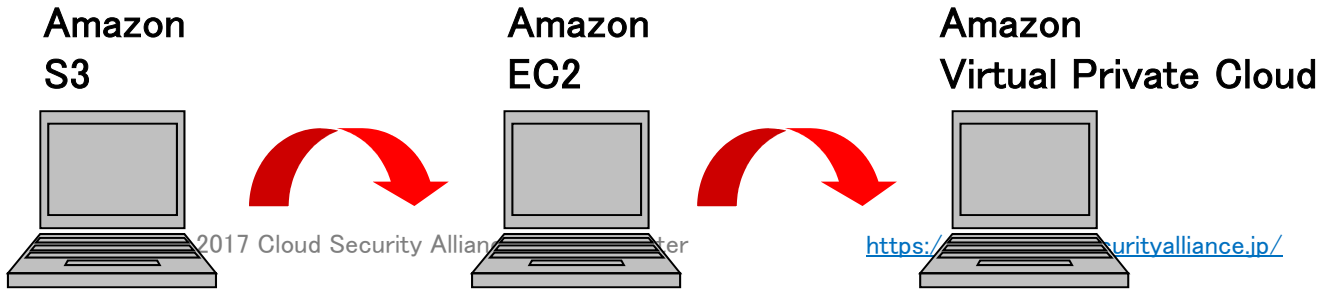
出典：Cloud Security Alliance「STAR Registrant UKCloud Ltd」（2016年10月28日）

AGENDA

- 2.クラウドを活用したヘルスケア・イノベーションの全体動向とセキュリティ課題
  - 2-1. ライフサイエンス／医薬品／医療機器産業の視点
  - 2-2. 医療機関／介護施設／健康増進サービス事業者の視点

2-1. ライフサイエンス／医薬品／医療機器産業の視点(1)

- 米国医薬品企業のR&Dにおけるクラウド導入（例）
  “*The New Computing Pioneers*” Chemical & Engineering News（2009年5月25日）
  (http://pubs.acs.org/cen/email/html/cen_coverstory_87_8721cover.html)
  - Eli Lilly社～研究者向けにAmazon Web Servicesを利用したハイパフォーマンスコンピューティングを導入
  - 特許情報や個人／患者情報が含まれない、R&Dのターゲット探索フェーズでパブリッククラウドを利用
  - 64ノードのLinuxクラスタシステムが5分で立ち上げ可能に
  - （利用例）バイオインフォマティクス配列解析プロジェクト
  - Eli Lilly社は、Jericho Forumの主要メンバー（「オーケストレーター」）
  - 他に、Pfizer社、J&J社、Genentech社でもクラウドを導入



2-1. ライフサイエンス／医薬品／医療機器産業の視点(2)

- “*Low cost, scalable proteomics data analysis using Amazon's cloud computing services and open source search algorithms.*”
  Halligan BD, Geiger JF, Vallejos AK, Greene AS, Twigger SN.
  J Proteome Res. 2009 Jun;8(6):3148-53.
  (/http://www.ncbi.nlm.nih.gov/pubmed/19358578)

ViPDAC (Virtual Proteomics Data Analysis Cluster)

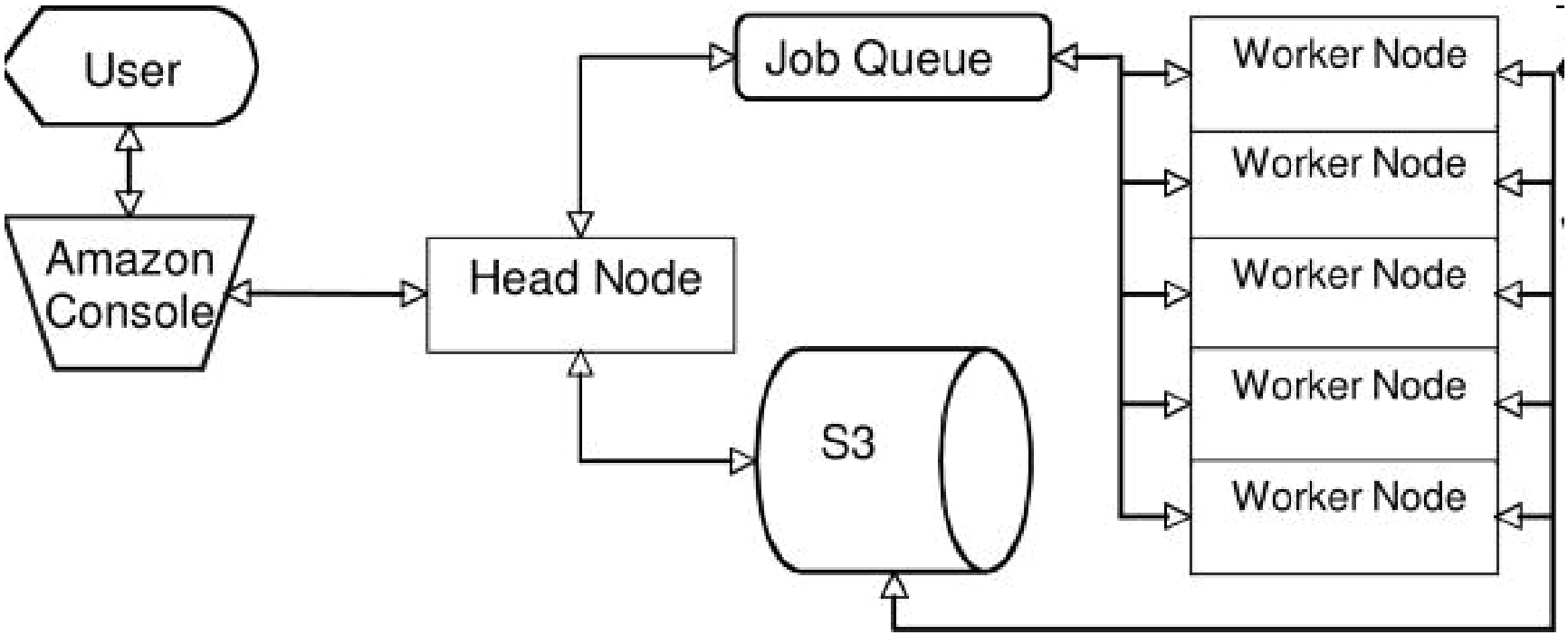
プロテオミクスデータベース検索用オープンソースソフトウェア
- Open Mass Spectrometry Search Algorithm（OMSSA）
- X!Tandem

仮想コンピューターリソース
Amazon Elastic Compute Cloud (EC2)

クラウドデータストレージ
Amazon Simple Storage System (S3)

2-1. ライフサイエンス／医薬品／医療機器産業の視点(3)

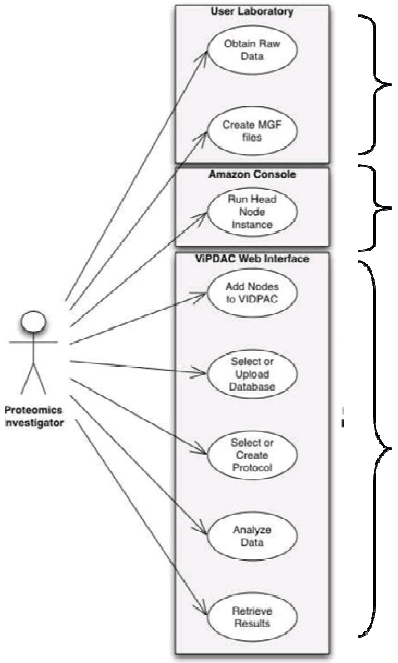
- J Proteome Res. 2009 Jun;8(6):3148-53.（続き1）
  (/http://www.ncbi.nlm.nih.gov/pubmed/19358578)
  - クラウドサービスの構成



出典：*"Low cost, scalable proteomics data analysis using Amazon's cloud computing services and open source search algorithms."*
Halligan BD, Geiger JF, Vallejos AK, Greene AS, Twigger SN.
J Proteome Res. 2009 Jun;8(6):3148-53.
http://www.ncbi.nlm.nih.gov/pubmed/19358578

2-1. ライフサイエンス／医薬品／医療機器産業の視点(4)

- J Proteome Res. 2009 Jun;8(6):3148-53.（続き2）
  (/http://www.ncbi.nlm.nih.gov/pubmed/19358578)
  - クラウド利用のリスク



一連の業務プロセスが、
–オンプレミス型環境
–パブリッククラウド環境
–プライベートクラウド環境
を組み合わせたボーダレスな
ハイブリッド環境で展開される

⇔業務プロセスのアンバンドル化
・スタートアップ企業の参入

出典：*"Low cost, scalable proteomics data analysis using Amazon's cloud computing services and open source search algorithms."*
Halligan BD, Geiger JF, Vallejos AK, Greene AS, Twigger SN.
J Proteome Res. 2009 Jun;8(6):3148-53.
http://www.ncbi.nlm.nih.gov/pubmed/19358578

2-1. ライフサイエンス／医薬品／医療機器産業の視点(5)

- クラウドインテグレーションとSLA

・【Amazon S3のサービスコミットメント】(発効日：2007年10月1日)

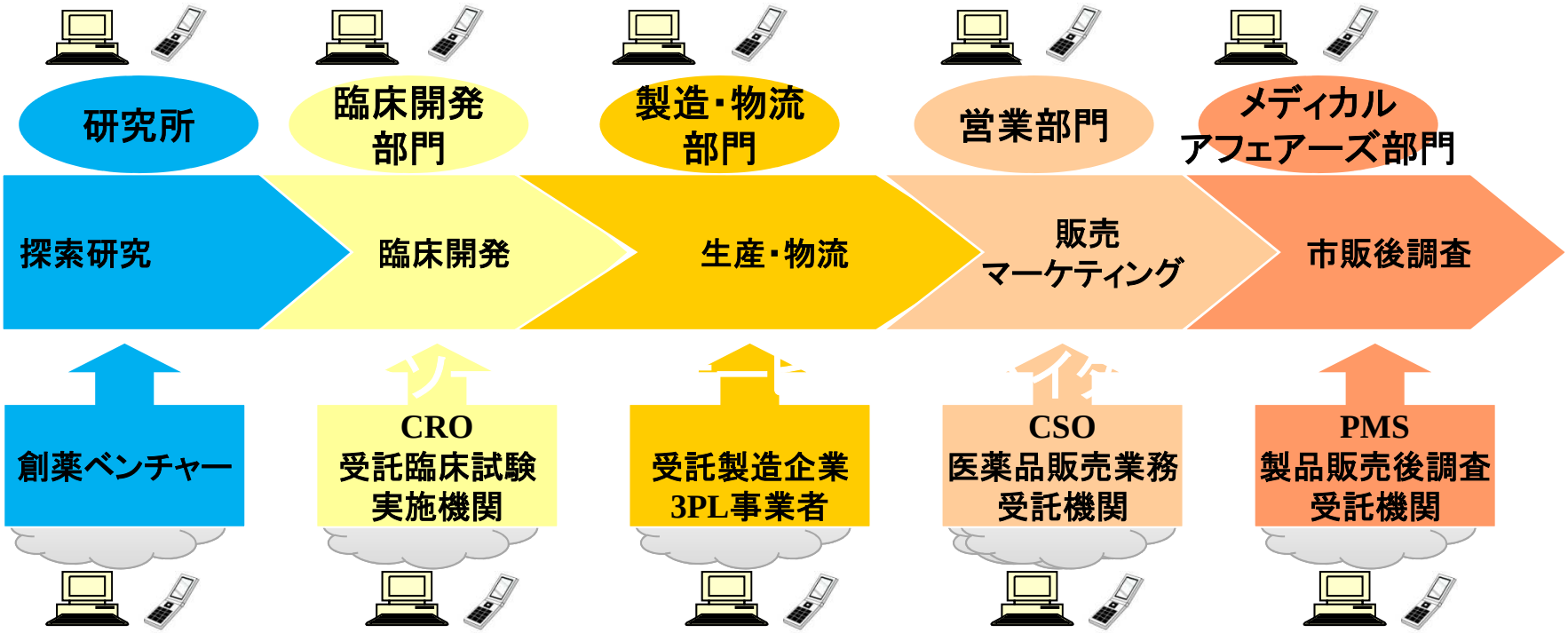
·AWSは、いずれの月間請求期間においても、Amazon S3を月間使用可能時間割合（以下に定義する）99.9%以上にて使用できるようにするため商業上合理的な努力をする（以下「サービスコミットメント」という）。Amazon S3が99.9%以上のサービスコミットメントを満たさない場合には、サービス利用者は以下に定めるサービスクレジットを受領することができる。

・【Amazon EC2のサービスコミットメント】(発効日：2008年10月23日)

·AWSは、Amazon EC2を、サービス年度における年間使用可能時間割合（以下に定義する）が99.95%以上で使用できるようにするため商業的に合理的な努力をする。Amazon EC2が99.95%以上の年間使用可能時間割合を満たさない場合には、サービス利用者は以下に定めるサービスクレジットを受領することができる。

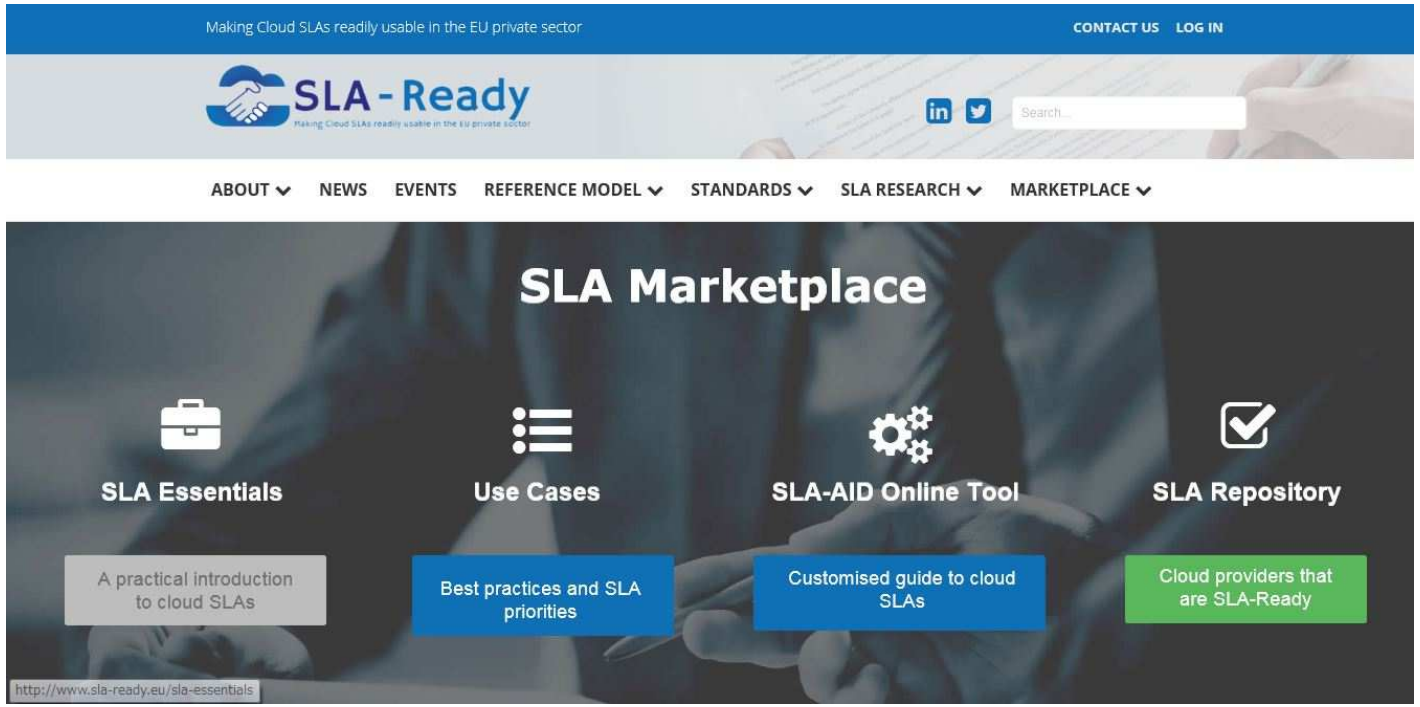
2-1. ライフサイエンス／医薬品／医療機器産業の視点(6)

- 医薬品バリューチェーンと外部委託管理
  - “Time Is Money” ～外部委託利用の拡大
  - 外部委託先が利用するクラウドサービスのセキュリティや品質を担保できる手段はSLA



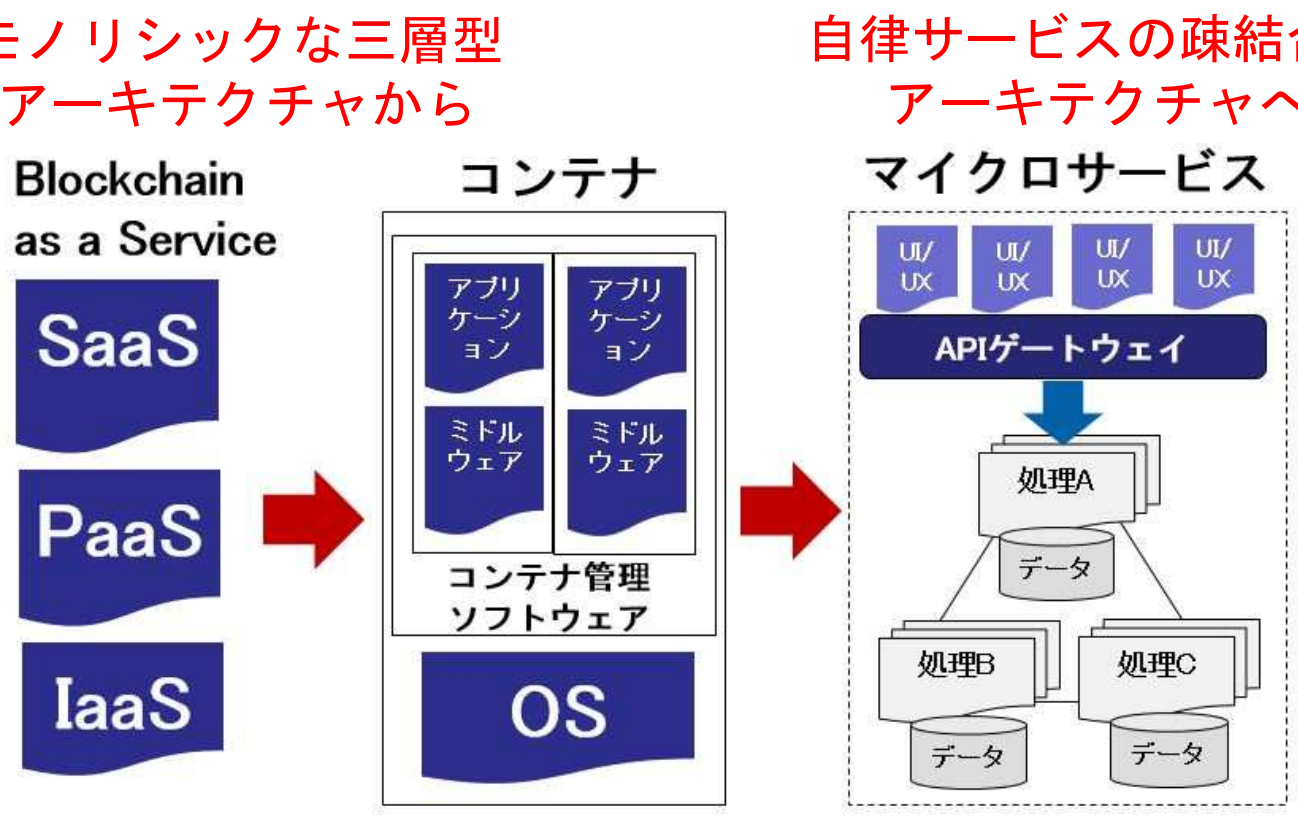
2-1. ライフサイエンス／医薬品／医療機器産業の視点(7)

- 欧州連合とCSA EMEAなどの協働プロジェクト「SLA-Ready」
  - クラウドを利用したイノベーションをめざすスタートアップ企業向けのクラウドSLA策定・運用支援ツールの開発
  - EUの中小企業支援政策の最重点業種の一つが医療機器



2-2. 医療機関／介護施設／健康増進サービス事業者の視点(1)

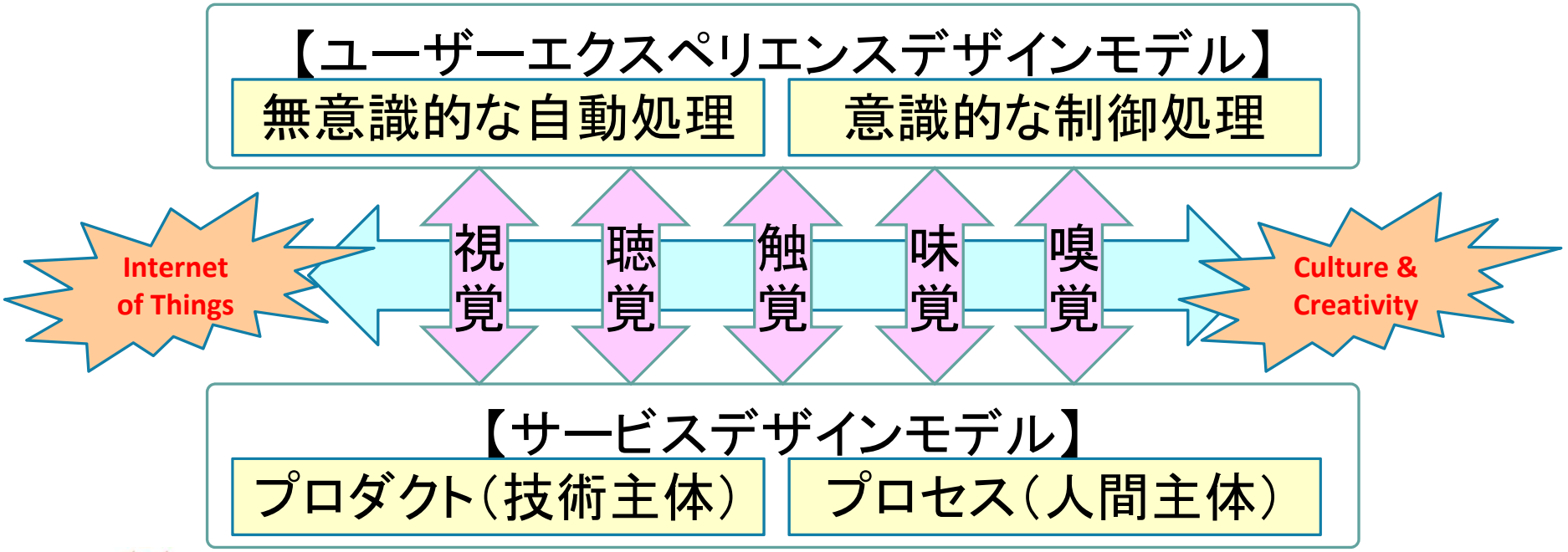
- コンシューマードリブンなxTechサービス（HealthTech含む）のビジネスモデルはSaaSからマイクロサービスへ



出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

2-2. 医療機関／介護施設／健康増進サービス事業者の視点(2)

- 「インクルージョン」を前提としたIoT時代のUI／UX
  （例）北欧流の五感に訴えるサービスデザイン
  - ノーマライゼーション原則と多感覚統合インタラクション
  - 市民参加型コミュニティとファシリテーター役のデザイナー



出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

2-2. 医療機関／介護施設／健康増進サービス事業者の視点(3)

- 米国アクセス委員会「情報通信技術（ICT）基準およびガイドライン（リハビリテーション法第508条および電気通信法第255条に基づくアクセシビリティ指針改正）」（2017年1月）

＜変更点＞

- ICT製品のタイプに代わり、機能によって規定を再構築する
- W3CのWCAG 2.0を盛り込み、Webサイトだけでなく Web以外の電子文書やソフトウェアに、レベルAおよびレベルAAの成功基準と適合要件を適用する
- 非公表に直面する電子コンテンツが遵守すべきタイプを特定する
- OSが提供する特定のアクセシビリティ機能を要求する
- ソフトウェアおよびOSが支援技術と相互運用性がなければならないことを明確化する
- 認知、言語、学習に障がいのある人々のためのアクセスに取組む
- 国際基準（欧州委員会ICT基準）の要求事項と調和させる

2-2. 医療機関／介護施設／健康増進サービス事業者の視点(4)

（続き）「情報通信技術（ICT）基準およびガイドライン」（2017年1月）

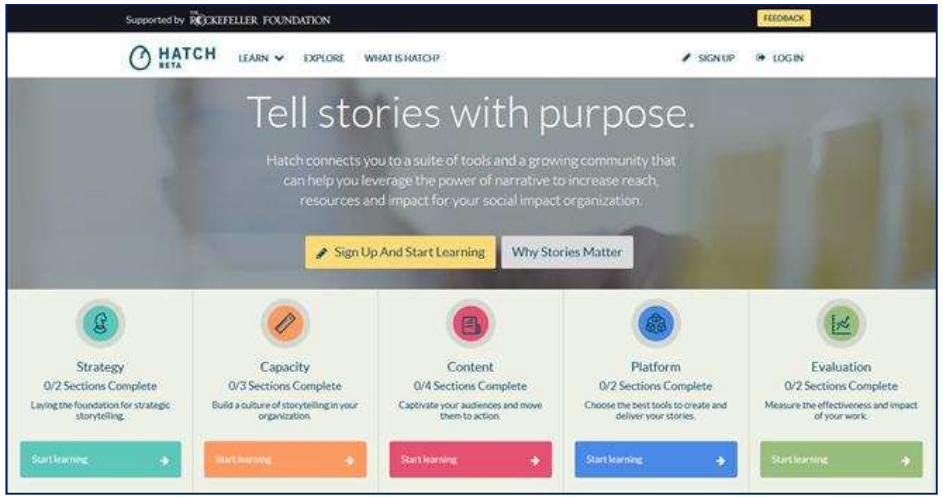
- 適用対象：
  - リハビリテーション法第508条関連～連邦政府機関
  - 電気通信法第255条関連～通信機器の製造者
- 適用対象外：民間企業、州・地方政府機関、公立学校、大学、非営利組織
- 適用開始日：
  - リハビリテーション法第508条関連～2018年1月18日
  - 電気通信法第255条関連～連邦通信委員会（FCC)の採択後

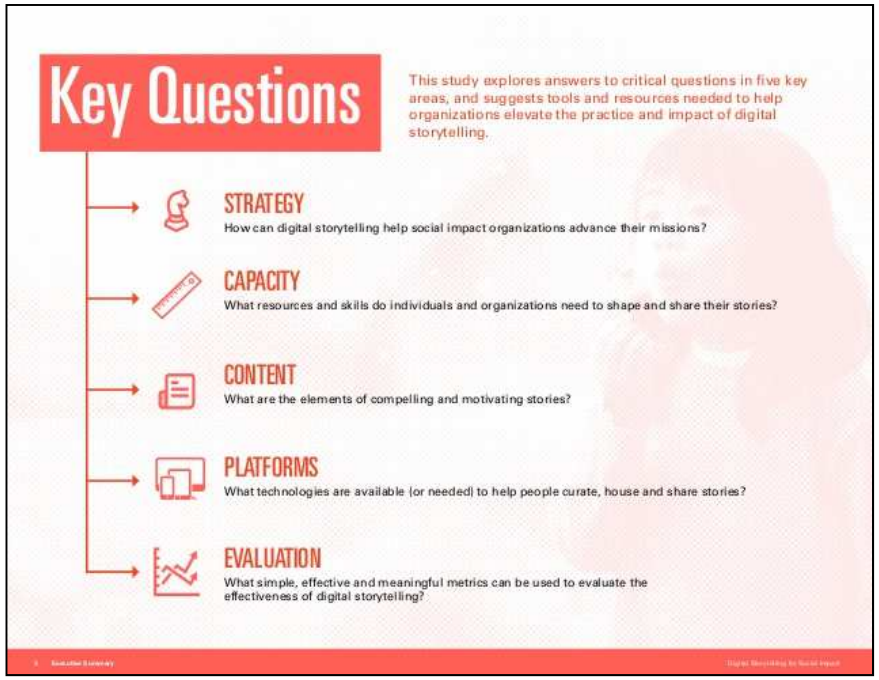
2-2. 医療機関／介護施設／健康増進サービス事業者の視点(5)

- （例）米国保健福祉省（HHS）のHIVケア啓発プログラム「positive.spin」（https://positivespin.hiv.gov/）
  - デジタル・ストーリーテリング手法の活用

2-2. 医療機関／介護施設／健康増進サービス事業者の視点(6)

- （例）ロックフェラー財団
  「ソーシャルインパクトのための
  デジタル・ストーリーテリング」
  （http://www.rockefellerfoundation.org/blog/digital-storytelling-social-impact）





2-2. 医療機関／介護施設／健康増進サービス事業者の視点(7)

- （ソーシャルインパクト）×（デジタルストーリーテリング）
  ⇒ グローバルヘルスへの拡張（例）
  - *“Understanding Specific Contexts of Antiretroviral Therapy Adherence in Rural South Africa: A Thematic Analysis of Digital Stories from a Community with High HIV Prevalence.”*
    PLoS One. 2016 Feb 29;11(2):e0148801. doi: 10.1371/journal.pone.0148801. eCollection 2016.
    - デジタルストーリーテリングによる主題分析を用いて、南アフリカのHIV感染症が流行する過疎地域における抗レトロウイルス療法のアドヘレンスを探究し、課題や支援に関する個人的・構造的要因を特定する

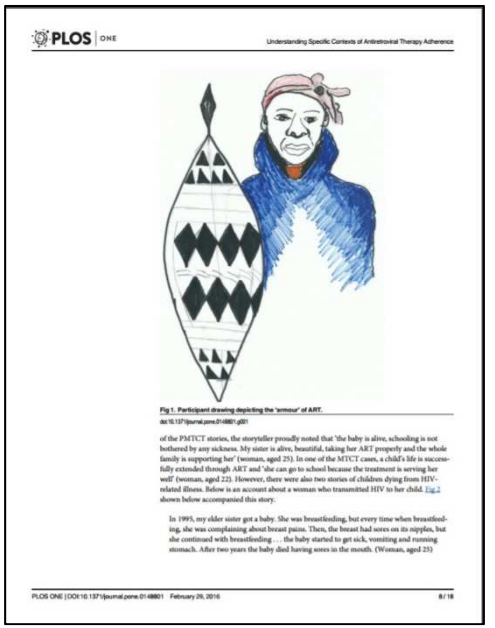

PLOS ONE | Understanding Specific Contexts of Antiretroviral Therapy Adherence

Fig 1. Participant drawing depicting the 'armour' of ART.

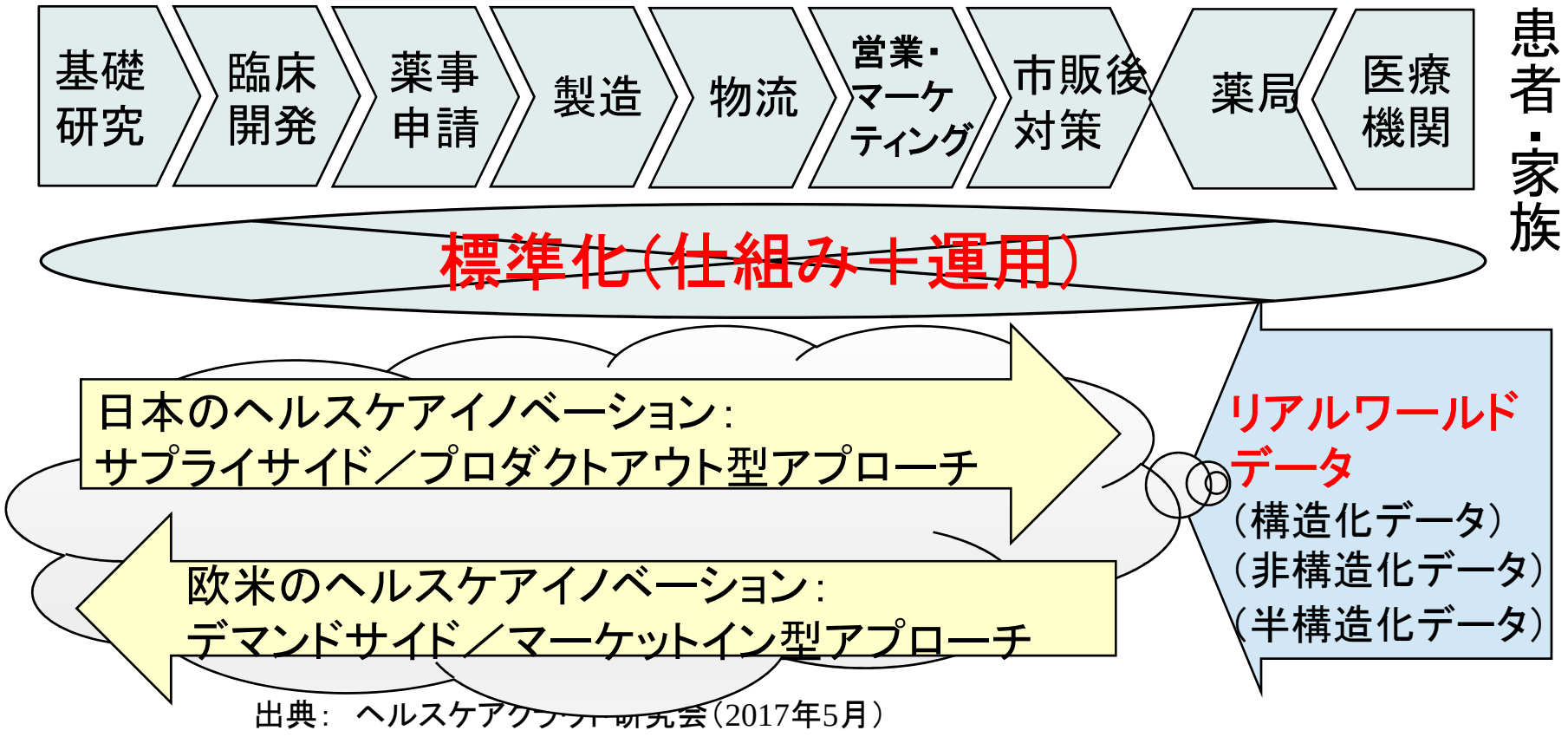
of the PMTCT stories, the storyteller proudly noted that 'the baby is alive, schooling is not bothered by any sickness. My sister is alive, beautiful, taking her ART properly and the whole family is supporting her' (woman, aged 25). In one of the MTCT cases, a child's life is successfully extended through ART and 'she can go to school because the treatment is serving her well' (woman, aged 22). However, there were also two stories of children dying from HIV-related illness. Below is an account about a woman who transmitted HIV to her child. Fig 1 shows below accompanied this story.

In 1995, my elder sister got a baby. She was breastfeeding, but every time when breastfeeding, she was complaining about breast pains. Then, the breast had sores on its nipples, but she continued with breastfeeding … the baby started to get sick, vomiting and running stomach. After two years the baby died having sores in the mouth. (Woman, aged 25)

PLOS ONE | DOI:10.1371/journal.pone.0148801 February 29, 2016 8 / 18

3. ディスカッション(1)

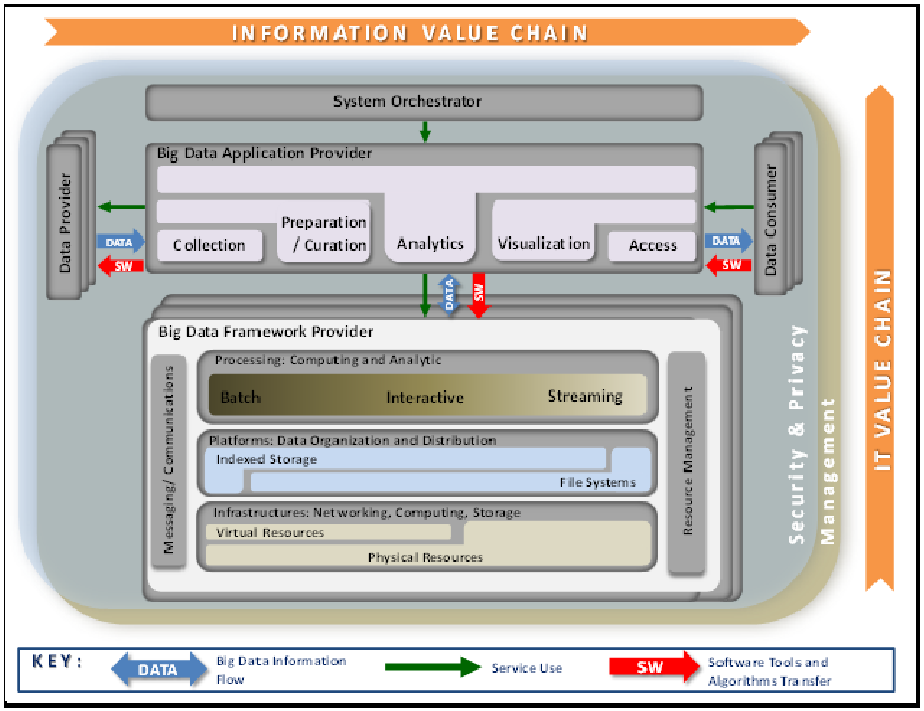
ヘルスケア・イノベーションのリスクの落とし穴



出典：ヘルスケアクラウド研究会（2017年5月）

3. ディスカッション(2)

- 米国NISTビッグデータ・リファレンス・アーキテクチャ
  ⇒マイクロサービス（AI含む）の集合体へと進化
  - 上位レイヤを繋ぐUI/UXやAPIの役割は?
  - 相互運用性の確保は?
  - エコシステム全体のオーケストレーターは?



出典：NIST Big Data interoperability Framework Version 1.0（2015年9月）