Healthcare Cloud

健康医療分野の
海外サイバーセキュリティ最新動向

2015年2月16日

博士（医薬学） 笹原英司

特定非営利活動法人ヘルスケアクラウド研究会

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ワーキンググループ

Healthcare Cloud

講師略歴：笹原英司

・特定非営利活動法人ヘルスケアクラウド研究会・理事

・一般社団法人日本クラウドセキュリティアライアンス・代表理事

・在日米国商工会議所ヘルスケアIT小委員会委員長

旧労働省（八王子労働基準監督署含む）、日米のメディア関連企業を経て、B2C／B2Bのデジタルマーケティング実務と、健康医療／介護福祉／医薬品／ライフサイエンス分野のITガバナンス関連調査研究を行った実績を有する。

また東日本大震災後は、東北地方の介護福祉／健康増進／ICT関連ソーシャルビジネス新規立ち上げ支援活動を行っている。

・慶應義塾大学文学部人間科学専攻（産業関係論）卒業

・Boston University Graduate School of Management修了（MBA）、

・千葉大学大学院医学薬学府博士課程先進医療科学専攻修了（博士・医薬学）

（研究実績）

厚生科学研究補助金医薬安全総合研究事業「添付文書等による医療用医薬品に関する情報の提供の在り方に関する研究」平成13年度分担研究「特殊な集団に関する情報提供の在り方」（研究協力者）、「Case study of pharmacist activities in the multidisciplinary practice of outpatient chemotherapy in Japan」（聖路加国際病院との共同研究）など。

AGENDA

1. クラウドセキュリティアライアンスの紹介
2. 健康医療分野のサイバー攻撃に起因する
   海外の情報漏えい事例
3. 健康医療のセキュリティ／プライバシー規制と
   サイバーセキュリティの動向
4. 健康医療へのシビックテクノロジー適用と
   セキュリティ／プライバシーのリスク
5. Q&A／ディスカッション

1. クラウドセキュリティアライアンスの紹介

- クラウドセキュリティのグローバルな非営利組織
  - Individual Members（ソーシャルメディアLinkedInの「Cloud Security Alliance」グループ登録者）：6万人以上
  - Corporate Members: 170以上（ユーザー企業・政府機関含む）
  - Affiliate Members: 28（ASPIC、IPA含む）
  - Chapters worldwide：70以上（日本含む）

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.
（https://cloudsecurityalliance.org/）

1. クラウドセキュリティアライアンスの紹介

- 健康医療情報管理ユーザーワーキンググループの紹介
  - ライフサイエンス／医薬品／医療機器産業、医療機関／介護施設／健康増進サービス事業者、患者／消費者を含む健康医療情報バリューチェーン全体における「Security Guidance for Critical Areas of Focus in Cloud Computing」および「Cloud Security Alliance Cloud Controls Matrix (CCM)」の有効活用の推進活動
  - CSAのワーキンググループが主導するCSAガイダンス、CCMおよびその他発行文書類に関する、業界の視点に立ったピアレビューの実施およびフィードバックの提供
  - 健康医療情報に関わる国内外の主要なステークホルダーコミュニティ（例．フォーカスグループ、業界団体、研究機関、フォーラム、学術団体など）との積極的な協業活動

AGENDA

2. 健康医療分野のサイバー攻撃に起因する
   海外の情報漏えい事例

2. 健康医療分野のサイバー攻撃に起因する情報漏えい事例

●米国国立標準技術研究所（NIST）「重要インフラのサイバーセキュリティを向上させるためのフレームワーク　1.0版（原題：Framework for Improving Critical Infrastructure Cybersecurity Version 1.0）」（2014年2月）より（https://www.ipa.go.jp/files/000038957.pdf）

➢「サイバーセキュリティ」
＝攻撃を防止、検知し、攻撃に対応することにより情報を保護するプロセス

2. 健康医療分野のサイバー攻撃に起因する情報漏えい事例

●「Update: Top 5 Health Data Breaches」Healthcare Info Security（2015年2月5日）より

企業・団体名	漏洩件数	漏洩の原因	漏洩した情報
Anthem（医療保険者）	8,000万件	外部からのサイバー攻撃	名前、誕生日、医療ID、社会保障番号、住所、メールアドレス、雇用情報、収入データ
TRICARE（政府機関）	490万件	外部委託先のバックアップテープ盗難	社会保障番号、名前、住所、電話番号、臨床ノート、臨床検査、処方箋
Community Health Systems（医療機関）	450万件	外部からのサイバー攻撃	名前、住所、誕生日、電話番号、社会保障番号
Advocate Medical Group（医療機関）	403万件	暗号化していないPCの盗難	名前、住所、生年月日、社会保障番号、診断、電子カルテ番号、医療サービスコード、医療保険情報
Texas HHS（政府機関）	200万件	政府と元外部委託先との訴訟中に漏洩	名前、誕生日、メディケイド番号・電子カルテ・レセプト、診断コード、レポート、写真

2-1. 米国の病院チェーン Community Health Systemsのケース（2014年8月）

- 2014年8月、不正アクセスにより、患者約450万人の個人情報が流出した可能性があることを公表、
- オープンソースのSSL／TLS実装ライブラリ「OpenSSL」の脆弱性を突いた海外からのサイバー攻撃が発端となったことが判明
- ニューヨーク証券取引所（NYSE）の上場企業である
  - 証券取引委員会（SEC）：米国企業改革法（SOX）に基づき、財務報告に係る情報開示や内部統制を義務付ける

2-1. 米国の病院チェーン Community Health Systemsのケース（2014年8月）

- 海外からのサイバー攻撃が発端となった
  - テロ対策を所管する国土安全保障省（DHS）の調査
  - サイバー犯罪を所管する連邦捜査局（FBI）の調査
- 患者の保護対象保健情報（PHI）が流出
  - HIPAAを所管する保健福祉省（HHS）への報告義務
- 顧客らが損害賠償請求の集団訴訟を提起
  - 連邦民事訴訟規則（FRCP）に基づく電子証拠開示（eディスカバリー）への対応

2-2. ソニー・ピクチャーズ・エンタテインメント（SPE）のケース（2014年11月）

- ネットワークが海外からのサイバー攻撃を受け、従業員、芸能人など約47,000件の情報流出被害が発生していることが報じられた
- 東京証券取引所（１部）およびニューヨーク証券取引所（NYSE）の上場企業であるソニーの連結対象米国子会社
  - 米証券取引委員会（SEC）：米国企業改革法（SOX）に基づき、財務報告に係る情報開示や内部統制を義務付ける
  - 日本の金融庁：金融証券取引法・会社法に基づき、財務報告に係る情報開示や内部統制を義務付ける
- 海外からのサイバー攻撃が発端となった
  - テロ対策を所管する国土安全保障省（DHS）の調査
  - サイバー犯罪を所管する連邦捜査局（FBI）の調査

2-2. ソニー・ピクチャーズ・エンタテインメント（SPE）のケース（2014年11月）

- 従業員の保護対象保健情報（PHI）が流出
  - HIPAAを所管する保健福祉省（HHS）への報告義務
- 元従業員らが損害賠償請求の集団訴訟を提起
  - 連邦民事訴訟規則（FRCP）に基づく電子証拠開示（eディスカバリー）への対応

＊日本の医療保険者による「データヘルス計画」を運用するためには、サイバーセキュリティ対策の実行組織（例.Chief Information Officer、Chief Information Security Officer、Chief Privacy Officerの連携）と技術の下支えが不可欠のはずですが・・・。

2-3. 米国の医療保険者Anthemのケース（2015年2月）

- ITシステムが海外からのサイバー攻撃を受け、顧客約8千万件の情報流出被害が発生したことを公表
- ニューヨーク証券取引所（NYSE）の上場企業である
  - 米証券取引委員会（SEC）：米国企業改革法（SOX）に基づき、財務報告に係る情報開示や内部統制を義務付ける
- 海外からのサイバー攻撃が発端となった
  - テロ対策を所管する国土安全保障省（DHS）の調査
  - サイバー犯罪を所管する連邦捜査局（FBI）の調査
- 保険会社から顧客情報が流出した
  - 金融機関を所管するニューヨーク州金融サービス局が州内の全保険会社に対するサイバーセキュリティ検査を開始

2-3. 米国の医療保険者Anthemのケース（2015年2月）

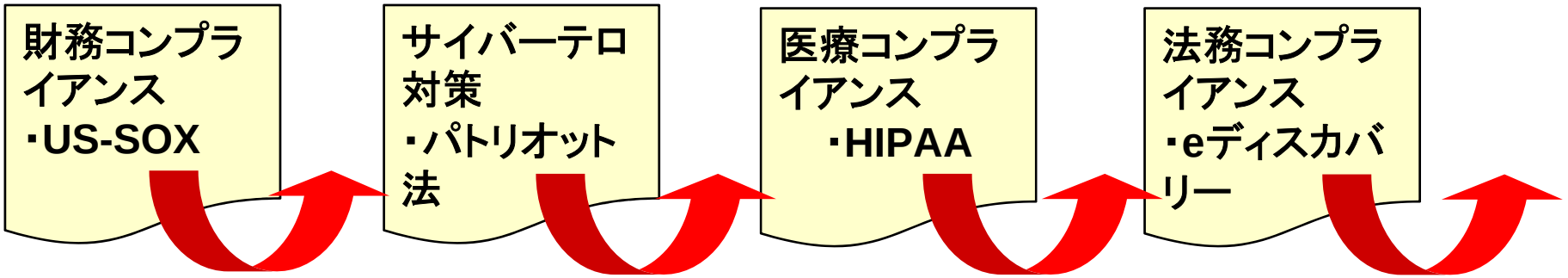
- ●顧客の保護対象保健情報（PHI）が流出
  - ➢HIPAAを所管する保健福祉省（HHS）への報告義務
  - ➢過去にHIPAA違反で170万ドルの民事制裁金を科せられたことがある（当時の社名はWellpoint）
  - ➢暗号化していなかった保存データがサイバー攻撃を受けて外部流出
    - ◆HIPAAは、保存データの暗号化を規定しているが、完全な強制ではない
    - ◆2015年より、ニュージャージー州が、保存データの暗号化を義務付けた（Anthemは州内で事業を行っていない）

      ＊ニュージャージー州には、グローバル製薬・医療機器企業の本社機能が集中している

2-3. 米国の医療保険者Anthemのケース（2015年2月）

- 顧客らが損害賠償請求の集団訴訟を提起
  - 連邦民事訴訟規則（FRCP）に基づく電子証拠開示（eディスカバリー）への対応
- 漏洩後、顧客を標的にしたフィッシング攻撃が発生
  - 消費者保護を所管する連邦取引委員会（FTC）が注意喚起

＊インシデントレスポンスで真相が分かるにつれて、コンプライアンスのバリューチェーン全体に火が付く（ICTサプライチェーン管理の不備が拍車をかける）



AGENDA

3. 健康医療のセキュリティ／プライバシー規制と
   サイバーセキュリティの動向

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

- 米国HIPAA／HITECH総括的規則の沿革
  - 1996年にHIPAA（Health Insurance Portability and Accountability Act of 1996；医療保険の携行性と責任に関する法律）が制定。
  - HIPAAにより、米国HHS（保健福祉省）は健康情報に関するプライバシールール及びセキュリティルールを策定
  - 2013年9月より、新たなHIPAA／HITECH総括的規則の適用を開始
  - （参考）HIPAA／HITECHの民事制裁金
    - ◆知らなかった場合：100ドル～5万ドル
    - ◆合理的な理由がある場合：1,000ドル～5万ドル
    - ◆故意に怠り、修正した場合：1万ドル～5万ドル
    - ◆故意に怠り、修正しなかった場合：5万ドル

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●米国HIPAA／HITECH総括的規則のスコープ

- ➢漏えい発生時の通知基準の改正
- ➢電子健康記録（EHR）に含まれる情報に対する患者のアクセス
- ➢事業提携者（BA：Business Associates）および下請け事業者に対する規制
- ➢許諾のないマーケティングにおける保護対象保健情報（PHI：Protected Health Information）の利用／開示の制限
- ➢許諾のない保護対象保健情報（PHI）の販売の禁止
- ➢データの研究利用　- 複合的、より一般的な許諾
- ➢患者が保険者とのデータ共有を制限する権利
- ➢プライバシーの取り扱いの通知を修正／再配布するための要件
- ➢契約査定のための遺伝子情報利用に対する制限の包含
- ➢民事制裁金（CMP：Civil Money Penalty）の執行／賦課および代理人行為の民事制裁金負債における保健福祉省（HHS）長官の役割の明確化

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●米国HIPAA／HITECH総括的規則と事業提携者（BA）

- ➢事業提携者（BA：Business Associates）＝適用主体に代わって、保護対象保健情報（PHI）を生成、収集、維持、交換する者
  - ◆事業提携者（BA）に代わって保護対象保健情報（PHI）を生成、収集、維持、交換する、事業提携者（BA）の下請け事業者も該当する
  - ◆事業提携者（BA）としての位置づけは、契約上の相手関係ではなく、役割や責任に基づく
- ➢事業提携者（BA）に該当する例
  - ◆保健情報連携組織、電子処方箋ゲートウェア、適用主体の個人健康記録（PHR）ベンダー（全てのPHRではない）
  - ◆日常的に、保護対象保健情報情報（PHI）へのアクセスを必要とするデータ交換プロバイダー
- ➢事業提携者（BA）に該当しない例
  - ◆単にデジタル管路を提供する、データ交換サービス事業者は該当しない
  - ◆ただし、実際に閲覧する意図がなくても、PHIを保存する事業者は該当する

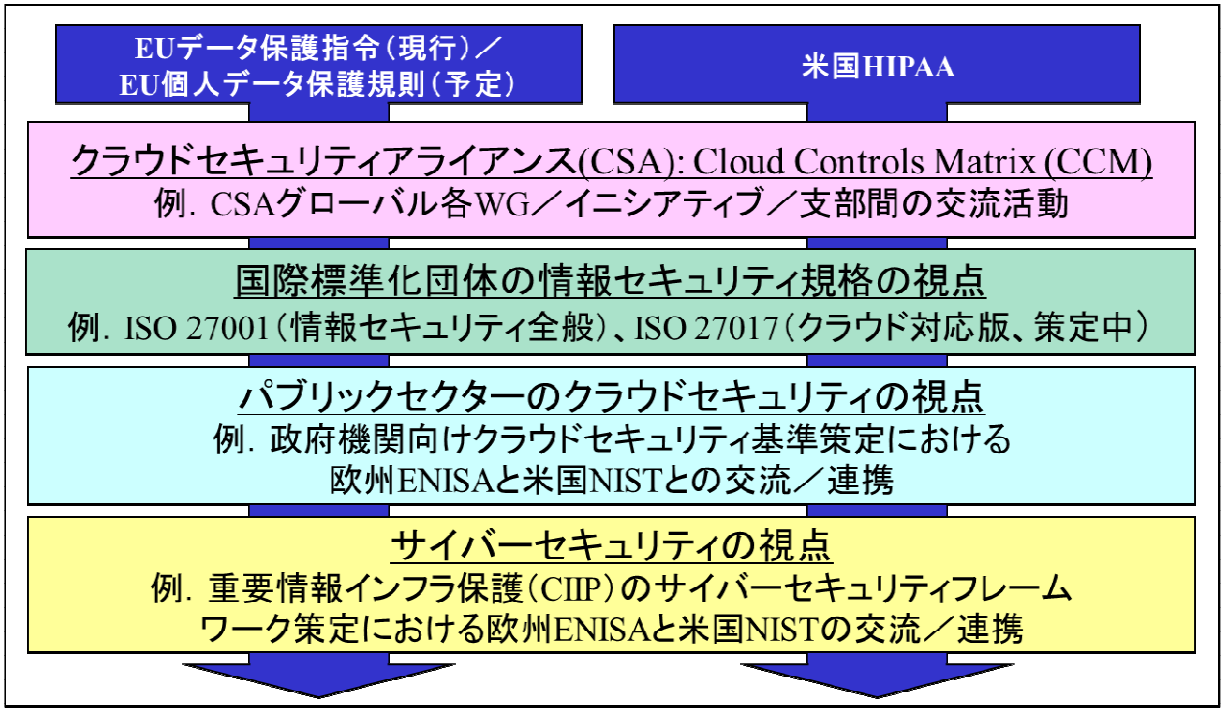
3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●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

出典：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（2015年2月）

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●健康医療のクラウドセキュリティにおけるEUと米国のハーモナイゼーションに向けた取組み例



出典：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（2014年12月）

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●CSAのクラウド・コントロール・マトリクス（CCM）の使い方
（http://www.cloudsecurityalliance.jp/ccm_wg.html）

Control Area (CSA)	Control ID (CSA)	Control Specification (CSA)	Scope Applicability		
			HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP Security Controls --LOW IMPACT LEVEL—
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	45 CFR 164.312(b)	CA-2 CA-7 PL-6	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7

HHS　NIST　GSA

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

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

●米国の健康医療サイバーセキュリティに関連するリソース

- 国立標準技術研究所（NIST）「Framework for Improving Critical Infrastructure Cybersecurity Version 1.0」（前掲）（http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf）
- 連邦政府一般調達局（GSA）「FedRAMP」（http://cloud.cio.gov/fedramp）
- 保健福祉省（HHS）「HIPAA」（http://www.hhs.gov/ocr/privacy/）
- アメリカ病院協会（AHA）：CYBERSECURITY RESOURCES（http://www.aha.org/advocacy-issues/cybersecurity.shtml）

3. 健康医療のセキュリティ／プライバシー規制とサイバーセキュリティの動向

- 食品医薬品局（FDA）
  - 「Content of Premarket Submissions for Management of Cybersecurity in Medical Devices」（2014年10月）
  - 「Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software」（2005年1月）
- 国土安全保障省（DHS）
  - US-CERT：「Alert (TA-310A): Microsoft Ending Support for Windows Server 2003 Operating System」（2014年11月）
  - ICS-CERT：医療機器のセキュリティ脆弱性を監視している

AGENDA

4. 健康医療へのシビックテクノロジー適用と
セキュリティ／プライバシーのリスク

4. 健康医療へのシビックテクノロジー適用と セキュリティ／プライバシーのリスク

●シビックテクノロジー

- ITを活用して、地域の社会課題を解決していく技術群
- 「$6.4 Billion to be Spent on Civic Tech in 2015, Report Says」（2014年12月5日付Government Technology）
  ＊米国の政府・自治体IT市場規模の24%を占める
- 代表的なイニシアティブ＝***Code for America***

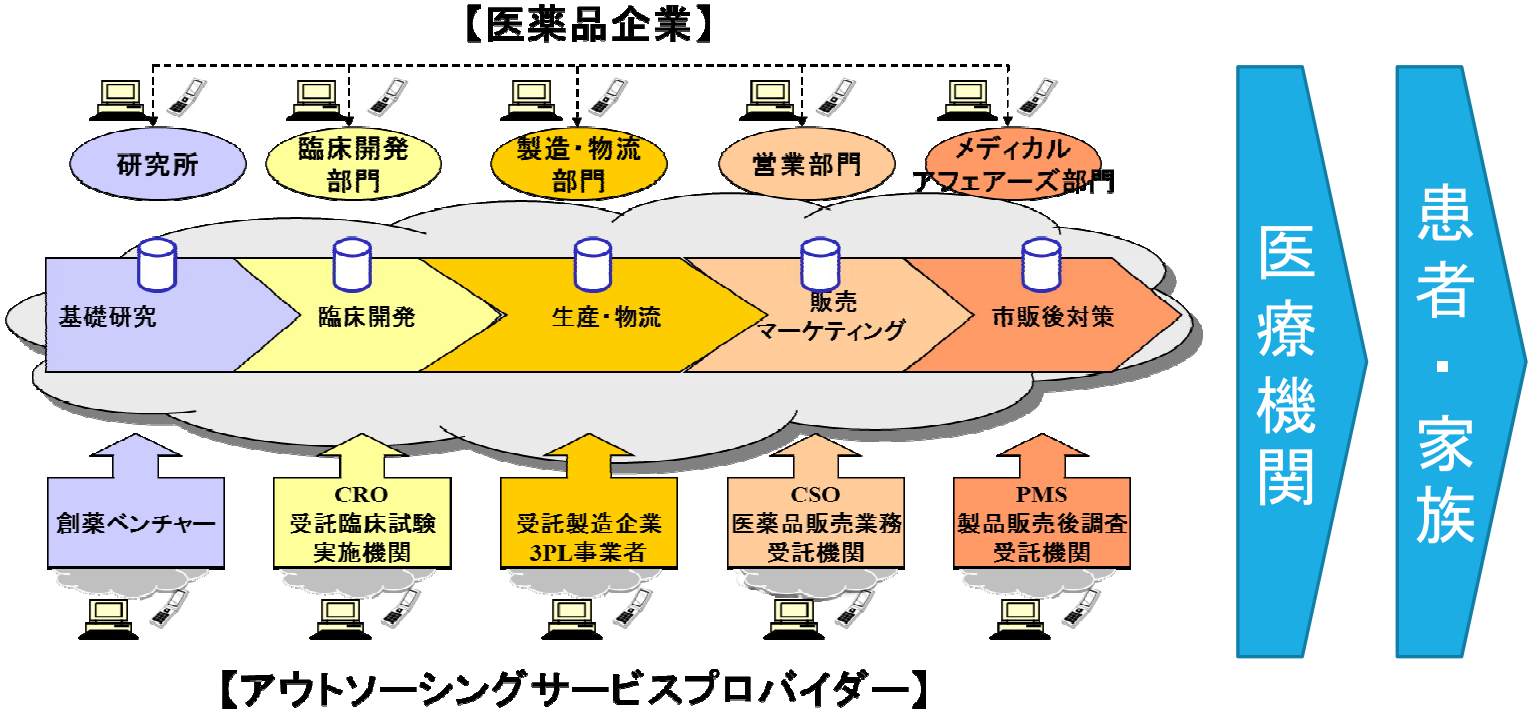
*“Starting in 2015, we are focusing our iterative, user-centered, and data-driven approach to government primarily in three areas: **health**, **economic development**, and **safety & justice**.”*

（Code for Americaは、FISMA/FedRAMP、HIPAA準拠）

4. 健康医療へのシビックテクノロジー適用とセキュリティ／プライバシーのリスク

●ICTバリューチェーンとセキュリティ／プライバシーの関係

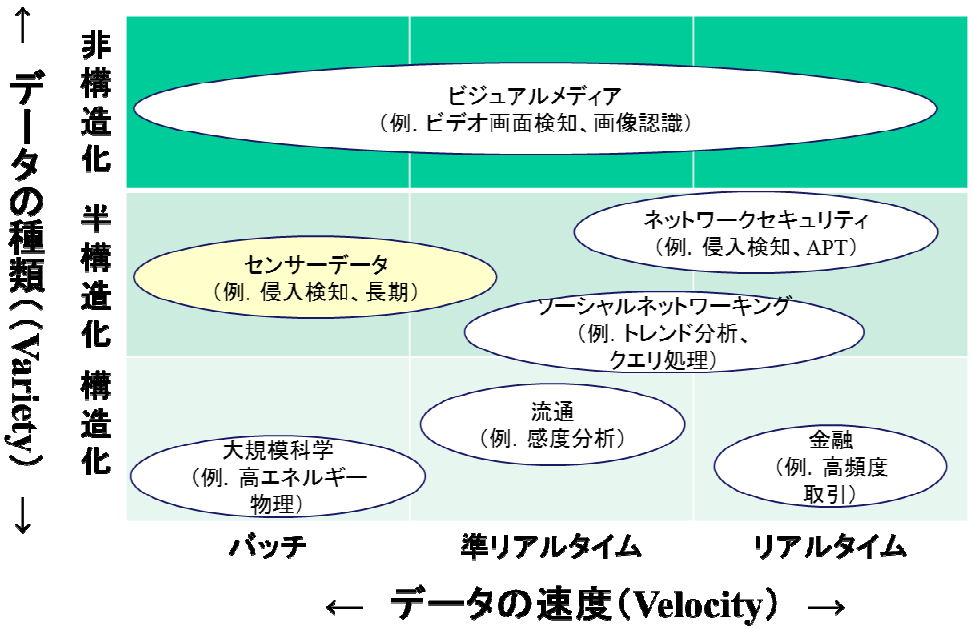
➢下流ほど、個人情報が増えて潜在的リスクが高まる



出典：NPOヘルスケアクラウド研究会（2014年9月）

4. 健康医療へのシビックテクノロジー適用とセキュリティ／プライバシーのリスク

- センサー／IoTとセキュリティ／プライバシーの関係
  - 完全な構造定義を持たない半構造化データの管理が課題に



出典：日本クラウドセキュリティアライアンス・ビッグデータユーザーワーキンググループ（2014年5月）

4. 健康医療へのシビックテクノロジー適用とセキュリティ／プライバシーのリスク

●ソーシャルメディアとセキュリティ／プライバシーの関係

➢関係性が強まれば強まるほど、潜在的なリスクは高まる

ソーシャルメディア利活用成熟度	【ステージ1】一方向型の情報発信	【ステージ2】双方向型の対話	【ステージ3】オンラインコラボレーション	【ステージ4】ステークホルダーエンゲージメント
ビッグデータの3V				
Volume（容量）	ユーザー生成コンテンツにより容量が急増			
Variety（種類）	構造化データから非構造化データへ			
Velocity（速度）	バッチ処理からリアルタイム処理へ			

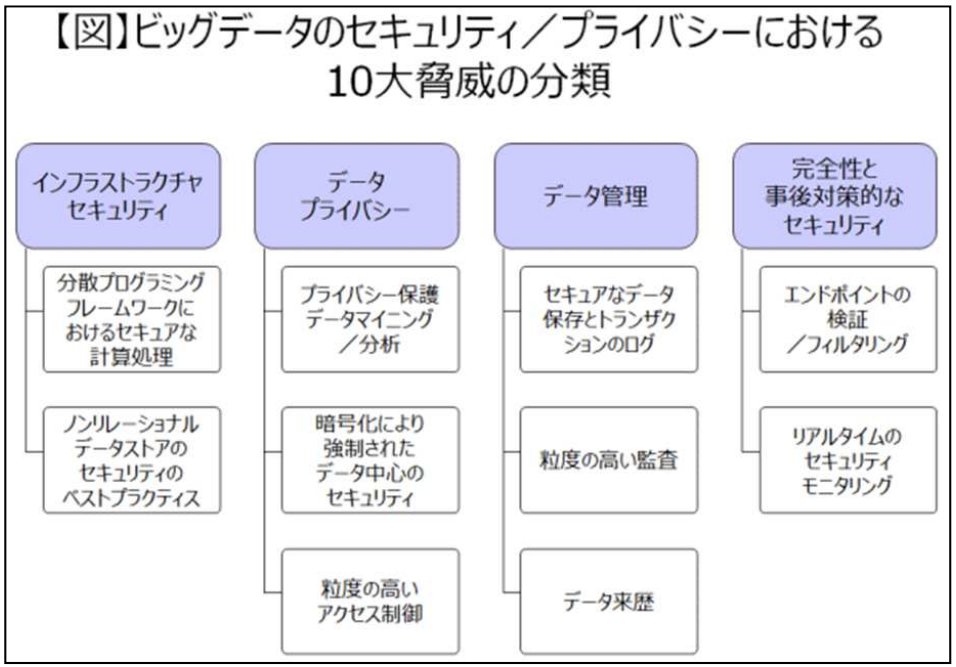
出典：NPOヘルスケアクラウド研究会（2014年6月）

4. 健康医療へのシビックテクノロジー適用とセキュリティ／プライバシーのリスク

●ビッグデータとセキュリティ／プライバシーの関係

➢データベース管理者やデータサイエンティストが狙われる

【図】ビッグデータのセキュリティ／プライバシーにおける10大脅威の分類



出典：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（2015年2月）

5. Q&A／ディスカッション

****

https://www.linkedin.com/in/esasahara
https://www.facebook.com/esasahara
https://twitter.com/esasahara

****