AITC
先端ＩＴ活用推進コンソーシアム

クラウドセキュリティガイドラインと医療情報システムガイドラインの調査
～クラウド上で医療情報を活用するために～

2011年10月21日

ウルシステムズ（株）　深谷　勇次
愛媛大学医学部附属病院　医療情報部　木村　映善

はじめに

- 昨今、各省庁から提示されている医療情報システムに関連するガイドラインが充実してきている。
  - 医療情報システムの安全管理に関するガイドライン4.1版(厚生労働省）
  - 医療情報を受託管理する情報処理事業者向けガイドライン（経済産業省）
  - ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（総務省）
- 公共性が高く、セキュリティの観点で他業種システムより重要な医療情報システムに対するクラウド技術の適用は、注目されるところである。

本活動の検討方針

- クラウドのセキュリティに関するガイドライン調査を行い、医療情報システムガイドラインとの関連を検討する。
  - セキュリティ観点で、医療情報システムがクラウドセキュリティガイドラインに適合するか整理できると良いので？
  - その整理を元に、他のシステムではどうか、と考えることで、クラウド技術を実業務で活用するセキュリティポイントが見いだせるのではないか？
  - 洗い出していく中で、セキュリティを保つための先端情報技術も見いだしていけるのではないか？

公的機関の
医療情報システムガイドラインと、クラウドセキュリティガイドライン

- 【医療情報システムガイドライン】

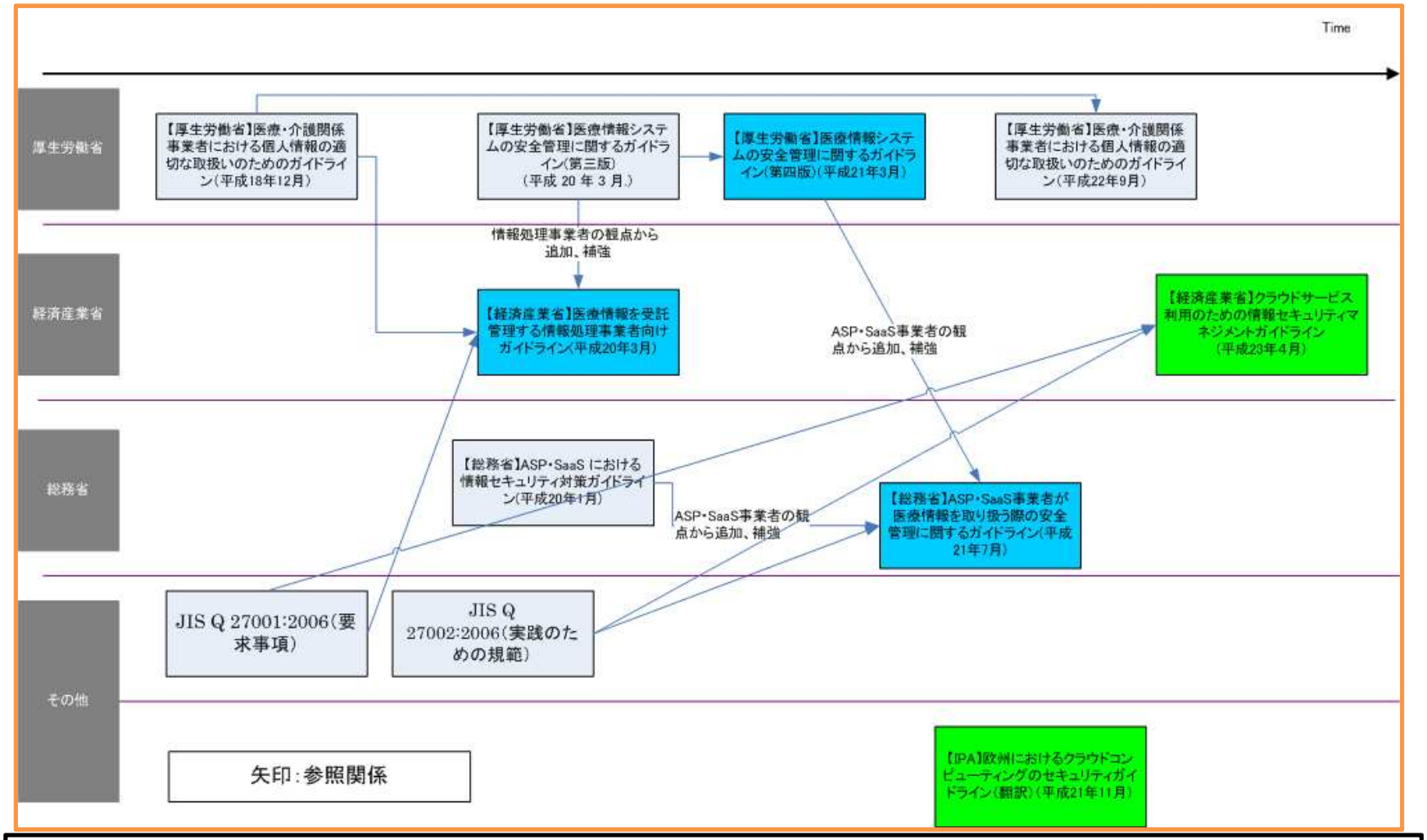
医療情報システムの安全管理に関するガイドライン	厚生労働省	第4.1版	（平成22年2月）
「医療情報システムの安全管理に関するガイドライン　第4.1版」に関するQ＆A	厚生労働省	第4.1版	（平成22年2月）
医療情報を受託管理する情報処理事業者向けガイドライン	経済産業省		(平成20年7月)
ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン	総務省		(平成21年7月)

- 【クラウドセキュリティガイドライン】

クラウドセキュリティガイドライン	経済産業省		平成23年4月1日
ENISAクラウドセキュリティガイドライン	IPA（日本語化）/ENISA（欧州）		平成21年11月
CSA クラウド・セキュリティ・ガイダンス（日本語なし）	CSA（米国Cloud Security Alliance）	V2.1	平成21年4月
DRAFT Cloud Computing Synopsis and Recommendations（日本語なし）	NIST （National Institute of Standards and Technology）		平成23年5月

前述したガイドラインの関連

- 前述したガイドラインと関連するドキュメントを時系列で記載



- “ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン“を軸に、何らか観点で整理を行ってみようと考えた

- 【目的】(ガイドラインからの抜粋)
  - “医療情報に求められる高度なセキュリティ”、“医療情報取扱におけるASP・SaaS の意義”の観点から、ASP・SaaS 事業者が医療情報を取り扱う際に求められる責任等、ASP・SaaS 事業者への要求事項等、合意形成の考え方等を示す
  - 医療情報がASP・SaaS によって適正かつ安全に利用され、医療情報におけるASP・SaaS の利用の適切な促進を図ることを目的とする

“ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン“の前提事項

- 【前提事項】（ガイドラインからの抜粋）
- （1）医療情報を処理するすべてのASP・SaaS 事業者における前提事項
  - ・守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと。
  - ・ネットワーク回線を含めてASP・SaaS 事業者がサービスを提供する場合、そのネットワークの安全性に関しては、厚生労働省ガイドラインの「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守すること。
  - ・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。
- （2）外部保存を提供するサービスにおける前提事項
  - ・受託した医療情報を閲覧しないこと。ただし、保守等のために必要な場合は、その閲覧範囲を明確化して医療機関等に示すこと。
  - ・受託した医療情報は、匿名化されたものを含めて分析、解析等を実施しないこと。ただし、医療機関等の委託がある場合は、実施範囲について委託契約等で明確にしておくこと。

- クラウド（SaaS含む）では、顧客から預かったデータを顧客に断り無しに勝手に使ってはいけない。匿名化して安全と言っても。
- データを活用したい場合は、ただし書き通り「顧客から預かったデータでデータ処理をする契約を結んでおく」ことが必要になる。

“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“では、

- “匿名化”に関する記載は無し
- 個人情報の保護に関して、以下のような記載あり
  - 15.1.4 個人データ及び個人情報の保護
  - 【解決策】
    - 個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にすることが望ましい。
  - 【クラウド利用者のための実施の手引】
    - クラウド利用者は，クラウドサービスで個人情報を利用する際には，法令及び組織の個人情報保護方針に従って利用できるように**適切な手順を策定すること**が望ましい。
  - 【クラウドサービスの関連情報】
    - クラウドサービスでは国内外問わず様々なクラウド事業者を利用することができる。しかし日本の個人情報保護に対する要求事項によっては，情報管理機能について自らが定める規程などに対応できないクラウド事業者が多く存在するかもしれない。そのため，個人情報保護に関する基準や手順がクラウド事業者の提供するクラウドサービスに合致するかどうかを検討することが望ましい。

- クラウドサービス利用者は、法令及び組織の個人情報保護方針に従い、個人データおよび個人情報の扱いには適切な手順を策定すること

さて、セキュリティと言えば

- セキュリティといった場合に、テクノロジー観点（SSL、暗号化等）以外で最も最初に思い出されるのが、個人情報（個人情報保護法）である。

- 皆さん、以下の質問の回答は？
  - Q1.「個人情報」とは、何ですか？
  - Q2.暗号化情報は個人情報ですか？
  - Q3.個人が特定できない情報（「匿名化」した情報）は、規制の対象になりますか？

さて、セキュリティと言えば

- Q1.「個人情報」とは、何ですか？
  - A1.個人情報の保護に関する法律（個人情報保護法）では「生存する個人に関する情報であって、特定の個人を識別できるもの」（第２条第１項）と定義されている
- Q2.暗号化情報は個人情報ですか？
  - A2.個人情報に当たると解釈されている
  - 【経産省】個人情報に相当する
    - “個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン”, 経済産業省, 2004
  - 【厚労省】個人情報に相当しない
    - “「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に関するＱ ＆ Ａ（ 事例集） ",厚生労働省, 2005
- Q3.個人が特定できない情報（「匿名化」した情報）は、規制の対象になりますか？
  - A3.匿名化情報は、個人情報ではないと解釈されているため、規制の対象にならない

まとめ：
クラウド上で医療系の情報を活用するための3つの条件

- 医療情報に求められる高度なセキュリティを保ち、医療系の情報を活用するための考慮点を端的に表現すると、以下3つと言える

1. 顧客から預かったデータでデータ活用を行う契約を結んでおく
2. 法令及び組織の個人情報保護方針に従い、個人データおよび個人情報の扱いには適切な手順を策定する
3. 個人情報は、暗号化するだけではなく、匿名化を行うことが望まれる（※）

（※）暗号化しても、処理するときには復号して処理するので必ず平文に戻るタイミングがある。運用上の穴のリスクを軽減するためにも、可及的に匿名化することが望まれる

- 次ページから、クラウド上で個人情報を扱う際のポイントとなる匿名化に関する動向を、掘り下げて報告する

何をどこまで匿名化すれば十分なのか？

- 厚労省
  - 「医療介護分野の個人情報保護ガイドライン」
  - 「氏名、生年月日、住所等を消去することで匿名化されると考えられる」といった程度の言及
- 経産省
  - 匿名化に関する具体的施策に関する言及はない？
- 総務省

  「匿名データの作成・提供に係わるガイドライン」

  別紙 「匿名化処理の考え方」「匿名化処理の技法」「匿名化処理の目安」
- 米国・医療分野ではHIPAA(Health Insurance Portability and Accountability Act)に2つの匿名化アプローチが提示されている
  - Safe Harbor　匿名化手法に準じた方法（後述）
  - 統計学的手法を用いた匿名化（現在進行で議論）

1 http://www.stat.go.jp/index/seido/pdf/35glv3.pdf

匿名化とは名前を隠すだけか？

- 匿名化は名前を隠すだけではない。個人情報を形成する属性は多数ある。
- 匿名化の処理の手法・粒度も重要。
- Ex. 地域特性の分析
  - 患者の住所を番地までそぎ落として市町村まで縮退させたものを使う？
  - 郵便番号を使う？
  - HIPAAでは住所の機械的加工処理だけではなく、人口動態に注意するように勧告（後述）
    - 人数が少ないケースの場合、それだけでも割り出しの手がかりになってしまう可能性がある。

HIPAAにおける匿名化(1)

- 1.Names. 氏名
- 2.All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
  - a.The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
  - b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
  - 州より小さい区画（ストリート、市、カウンティ、構内、郵便番号等。）はNG。
  - 但し、Censusデータから提供されているデータと下記に定める規則に従い、郵便番号の最初の3桁を利用することが可能である。
  - a. 人口が二万人より多い場合は、その郵便番号の最初の3桁はそのまま流用可能。
  - b. 人口が二万人より小さい場合は、000とする。
- 3.All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
  - 誕生日、入院日、退院日、死亡日等、個人特定に結びつけられる可能性のある日付（但し年単独は除く）。
  - 89歳以上に関して言えば、そのような年齢を示唆させる全ての日付（年も含む）も対象となるが、
  - 90歳以上の1つのカテゴリに集約すればOKである。
- 4.Telephone numbers. 電話番号
- 5.Facsimile numbers. FAX番号
- 6.Electronic mail addresses. 電子メール
- 7.Social security numbers. 社会保障番号(SSN)
- 8.Medical record numbers. 電子カルテの患者ID (出典*1)

De-identifying Protected Health Information Under the Privacy Rule http://privacyruleandresearch.nih.gov/pr_08.asp より。

HIPAAにおける匿名化(2)

- 9.Health plan beneficiary numbers. 保険証番号相当か？（具体的な説明みつからず。調査中。）
- 10.Account numbers. 口座番号
- 11.Certificate/license numbers. 運転免許証、各免許証の番号
- 12.Vehicle identifiers and serial numbers, including license plate numbers. 車両識別番号、ライセンスプレート番号も含む。
- 13.Device identifiers and serial numbers. 機器番号、製造番号等
- 14.Web universal resource locators (URLs). URL
- 15.Internet protocol (IP) address numbers. IPアドレス！？
- 16.Biometric identifiers, including fingerprints and voiceprints. 指紋や声紋など、生体識別情報
- 17.Full-face photographic images and any comparable images. 顔写真、個人を認識可能な画像全般
- 18.Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification. その他個体識別番号、個体を識別可能な特徴、コード、さらにPrivacy Ruleによってre-identificationが認められていないもの。

- References
  - 1. http://www.azumc.com/body.cfm?id=872 Medical Records and Health Information Management

- 以上のように、個人情報を形成する属性は多数ある

匿名化に関する先行研究(一例)

- 米国医療情報学会
  - El Emam Khaled, Dankar Fida Kamal. Protecting Privacy Using k-Anonymity. Journal of the American Medical Informatics Association. 2008 September 1, 2008;15(5):627-37.
  - El Emam Khaled, Dankar Fida Kamal, Issa Romeo, Jonker Elizabeth, Amyot Daniel, Cogo Elise, et al. A Globally Optimal k-Anonymity Method for the De-Identification of Health Data. Journal of the American Medical Informatics Association. 2009 September 1, 2009;16(5):670-82.
  - Malin Bradley, Benitez Kathleen, Masys Daniel. Never too old for anonymity: a statistical standard for demographic data sharing via the HIPAA Privacy Rule. Journal of the American Medical Informatics Association. 2011 January 1, 2011;18(1):3-10.
- 情報大航海プロジェクト
  - 株式会社 日立コンサルティング.「行動情報活用型クラウドサービス振興のためのデータ匿名化プラットフォーム技術開発事業」事業報告書. 平成22年度次世代高信頼・省エネ型 IT 基盤技術開発事業. 2011.
  - 廣田 啓一, 保木野 昌稔, 藤木 由里, 松崎 和賢, 吉田 圭吾, 赤井 健一郎, et al. 情報大航海プロジェクトにおける個人情報匿名化基盤の構築と検証. 情報処理学会研究報告 CSEC, [コンピュータセキュリティ]. 2010;2010(48):1-12.
- 情報セキュリティ関連論文・
  - 永井 彰, 五十嵐 大, 濱田 浩気, 松林 達史. クロネッカー積を含む行列積演算の最適化による効率的なプライバシー保護データ公開技術. 暗号と情報セキュリティシンポジウム 2010 (SCIS2010). 2010;CD-ROM:6.

経産省の動き

- 「情報大航海プロジェクト」の開発成果を受けて「匿名化」処理の具体的施策に関するガイドラインを作成する動きあり

経産省の動き 1/2

2-1. 平成22年度 サービス検討WGの活動報告
（1）平成22年度サービス検討WGの活動概要

活動の目的	今後実現が想定されるパーソナルサービスのモデルを示した上で、想定される課題を抽出する
実施内容	➢ パーソナルサービスの類型の作成 ➢ パーソナルサービスのコンセプトモデルの検討 ➢ パーソナルサービスの実現に向けた課題の抽出と対応 ➢ 情報共有基盤の構築に向けた検討
成果	➢ 実現が想定されるパーソナルサービスのコンセプトモデルを作成 ➢ 制度的課題、技術的課題を抽出し、特に制度的課題については制度検討WGに連携し、一部、経済産業省の「匿名情報の安全な利用に関する手引」の検討に反映 ➢ 情報共有基盤の構築について経済産業省を交えた議論を行い、提言を実施

http://www.coneps.org/contents/h23gm001_no3.pdf

経産省の動き 2/2

3-2. 平成23年度制度検討WG活動計画

制度検討WGではゴール、及び検討課題を以下の通り定義しています。
2ヶ月に1回程度の頻度でWGを開催し、検討を進めてまいります。

インプット	制度検討WGでの具体的検討テーマ	制度検討WGのゴール（今年度の検討成果）
✓ 総務省『利用者視点を踏まえたICTサービスに係る諸問題に関する研究会第二次提言』におけるライフログ・サービスに関する配慮原則 ✓ 経済産業省『経済産業分野における匿名情報の安全な利用に関する手引き』 ✓ 会員からの提案（例：行動支援型サービス、情報銀行の提案など）	◆平成22年度の活動で残された課題への対応 ・ 経産省「匿名情報の安全な利用に関する手引」の検証、他のWGの動向や実証実験などを踏まえて改定に向けた提案をする ・ 行動支援型サービスまたはリーチ情報の取扱いに関する業界としてのガイドライン（案）の取りまとめ ◆実証実験 ・ 他のWGと連携し、経産省「匿名情報の安全な利用に関する手引き」に従った実証実験を行う ・ 実サービスを実施するに当たっての課題を抽出 ◆情報銀行・情報共有基盤についての検討（他のWGとの連携） ・ サービス検討WGの情報銀行・情報共有基盤から制度的課題を抽出する ◆経産省の活動との連携 ・ 個人情報保護法や経産省ガイドラインの改正に向けたコメントを提出する	2011/10/07現在 未公表 ■ ガイドライン（案）の公開 ■ パーソナルサービス実現に向けた制度・ルール整備に係る関係府省への提言

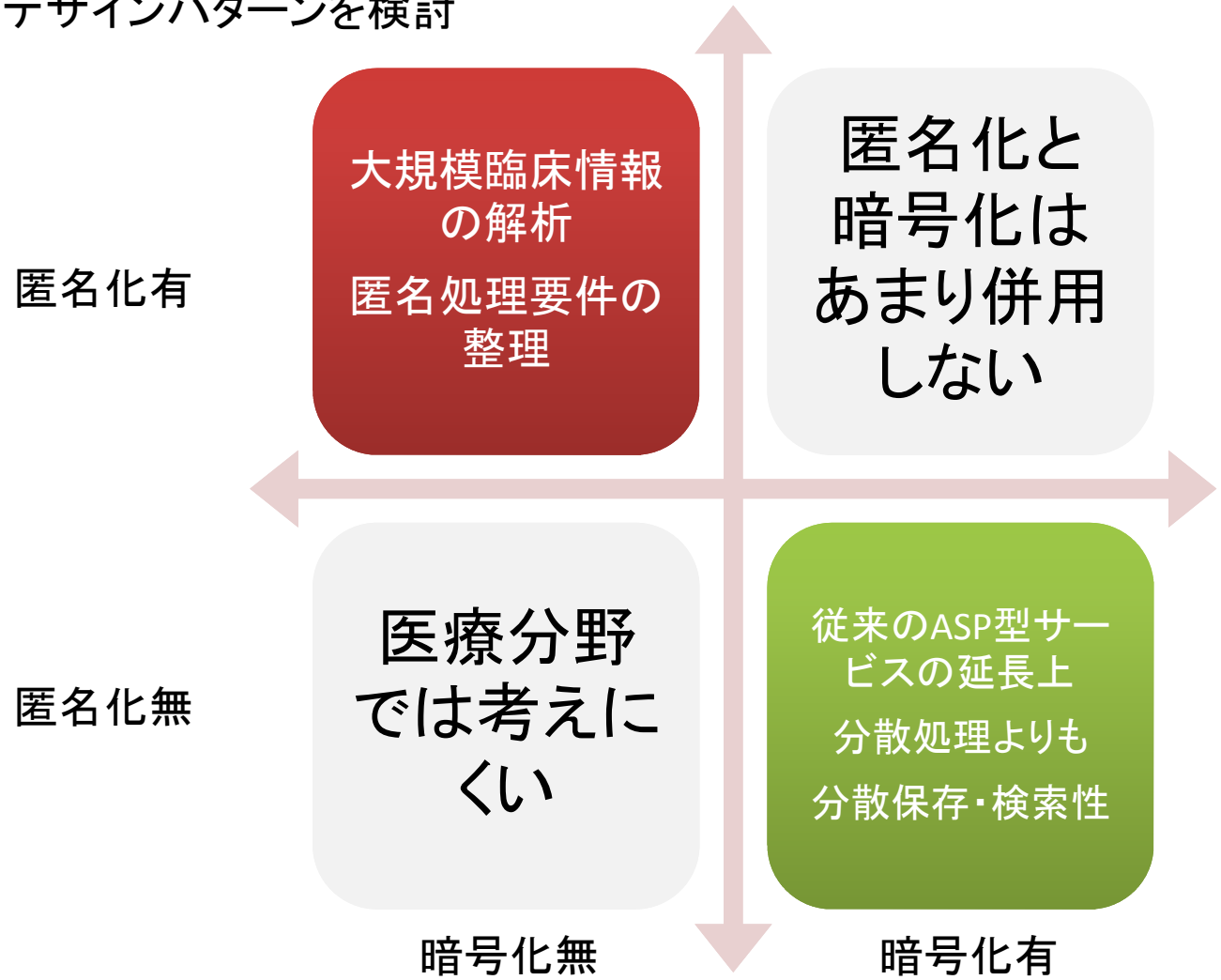
15

匿名化に関する今後の見通し

- 近日中に情報の匿名化に関するガイドラインが経産省から公開されることが予測される。
- 匿名化された医療情報が一般公開される見込みは当面考えにくい。
  - レセプト情報等の提供に関する有識者会議
    - http://www.mhlw.go.jp/stf/shingi/2r9852000000amvy.html#shingi15
    - 研究者のみへの提供。民間提供は現時点では考慮していない。かつ匿名化しても一般公開はしない。
- 民間ベースでは、利用者から匿名化された情報を受け取り、経営分析を提供しているASPサービスが出ている。この辺のビジネスモデルは既にある。
  - 顧客のオンサイトで匿名化処理をしてからアップロードさせている
  - ベンチマークのために集計結果を顧客間で相互開示しているが、オリジナルの情報そのものは開示していない。

今後の整理方針案 (1)

- クラウドに医療情報をのせる場合のケース分類とビジネスモデル・ソフトウェアのデザインパターンを検討

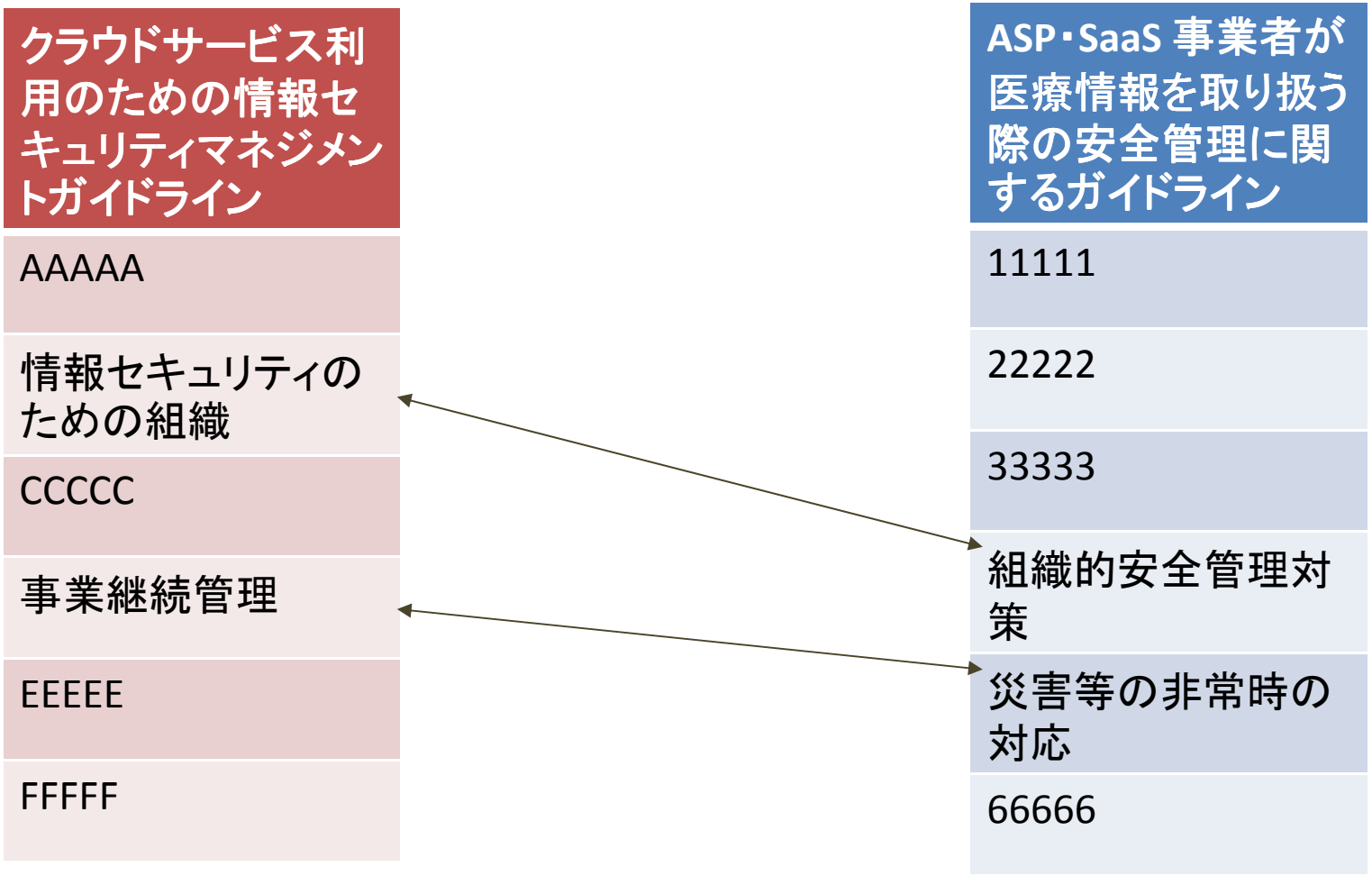


今後の整理方針案(2)

- クラウドの分散処理フレームワーク上に実装するための要件整理
  - (1)個人情報の取り込み
    - クラウドに上げる前にローカルで匿名化させるか？　個人情報があるままでフロントのメモリ領域にアップロードさせ、永久保存層に移行する前に匿名化処理を行うか？
    - ユーザとフロントのチャネル・オブジェクトセキュリティの兼ね合いは？（医療情報システムの安全管理に関するガイドライン)
  - (2) 匿名化処理
    - 何をすれば匿名処理の要件を満たしているか？
    - 匿名処理に関する手法、ライブラリの模索
  - (3) 知見を提供する分析手法と実装
    - データマイニング・フレームワーク(Mahout等）
    - 分散処理フレームワークの苦手な部分と補完手法
      - Ex.ストリーム処理の不得手な部分 -- SQLのJoin結合相当の処理 PigやHive等

今後の整理方針案(3)

- ガイド間の関連を見いだす
  - ガイド間の関連を見いだし、ポイントの明確化



以上
御清聴いただき
ありがとう
ございました