Healthcare Cloud

コンプライアンス視点で理解する
世界のデータ管理トレンドとこれから

2016年8月5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 理事
一般社団法人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

Healthcare Cloud

AGENDA

- 1. ビッグデータの定義とデータアーカイブの役割
- 2. 海外のデータアーカイブ管理に関わる
  主要ポリシー動向
- 3. データアーカイブを活用したビッグデータ／IoT
  セキュリティ対策のポイント
- 4. まとめ／Q&A

Healthcare Cloud

AGENDA

1. ビッグデータの定義とデータアーカイブの役割

1-1. ビッグデータの定義
1-2. ビッグデータの６つの軸
1-3. ビッグデータの種類と速度の関係
1-4. スモールデータからビッグデータへ
1-5. ビッグデータの包括的フレームワーク
1-6. ビッグデータとIoTの関係

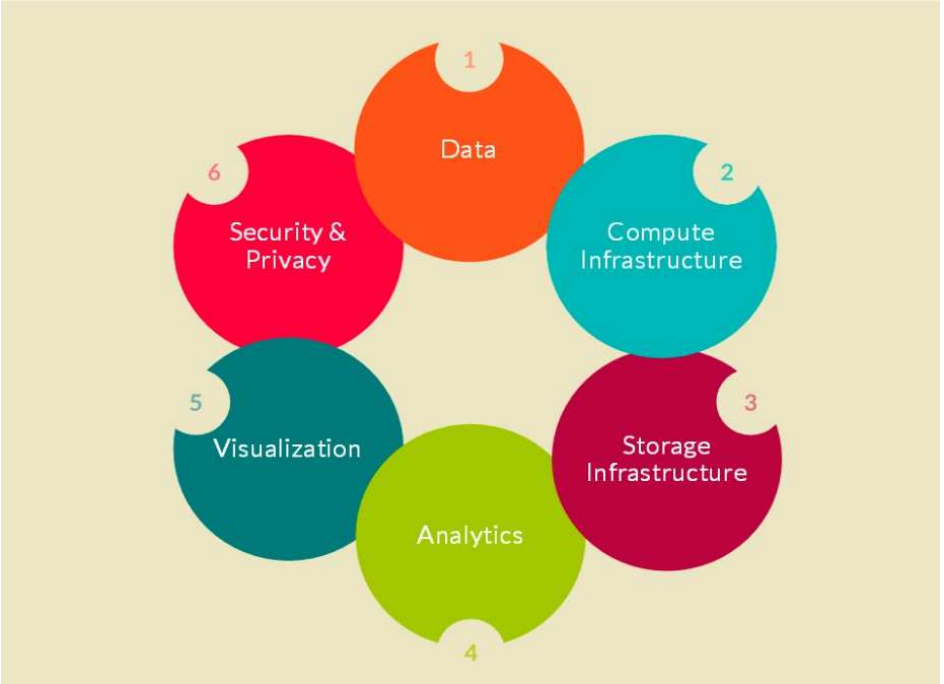
1-1.ビッグデータの定義

- NIST Big Data Interoperability Framework Version 1.0の定義:

Big Data refers to the inability of traditional data architectures to efficiently handle the new datasets. Characteristics of Big Data that force new architectures are **volume** (i.e., the size of the dataset) and **variety** (i.e., data from multiple repositories, domains, or types), and the data in motion characteristics of **velocity** (i.e., rate of flow) and **variability** (i.e., the change in other characteristics).

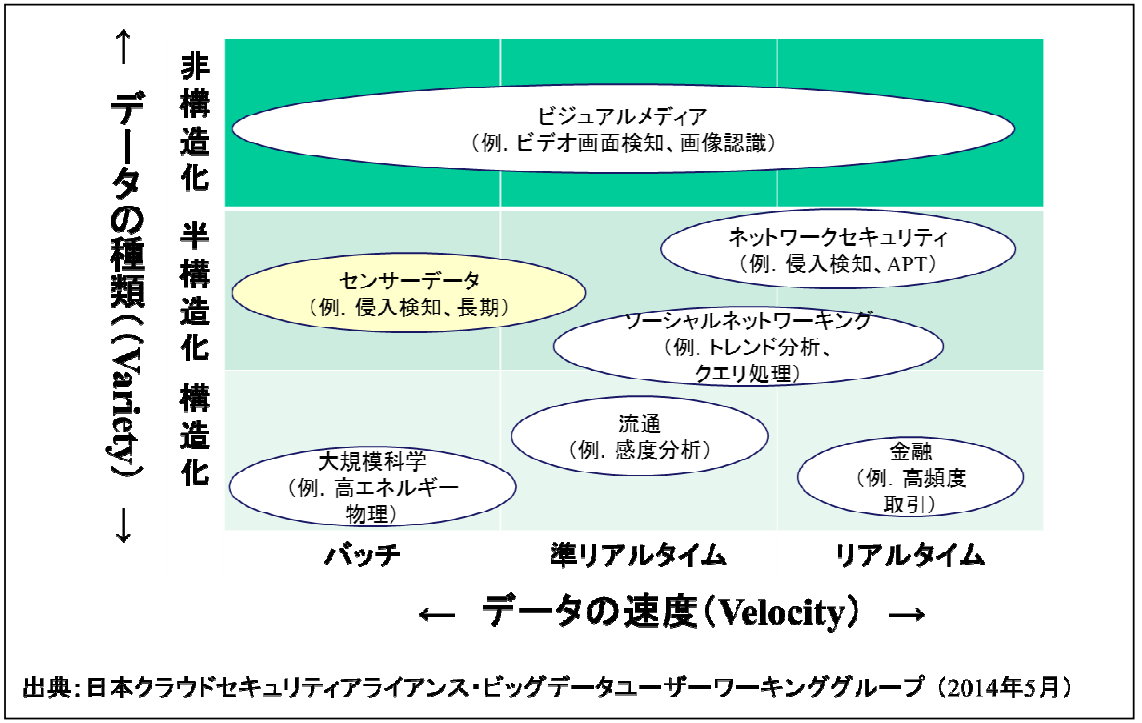
1-2.ビッグデータの6つの軸

- ●データ
- ●計算処理インフラストラクチャ
- ●ストレージインフラストラクチャ
- ●分析
- ●可視化
- ●セキュリティとプライバシー



1-3.ビッグデータの種類と速度の関係

- データアーカイブの役割
  - ➢長期的な記録保管庫
    （データ・インテグリティ）
  - ➢ビッグデータ利活用の起点



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）

1-4.スモールデータからビッグデータへ

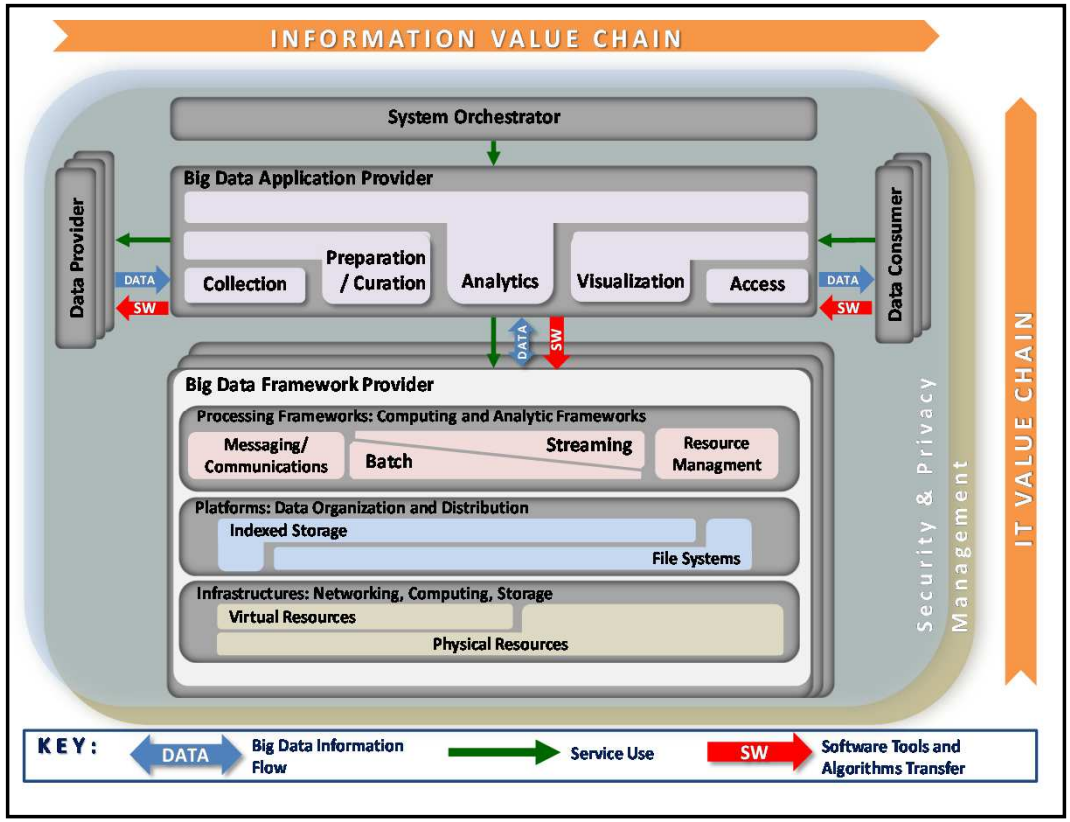
- ソーシャルメディア利活用の成熟度とビッグデータの3Vの関係

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：ヘルスケアクラウド研究会「ビッグデータで使われるNoSQLとセキュリティ課題」（2015年3月）

1-5.ビッグデータの包括的フレームワーク

- NIST「ビッグデータ相互運用性フレームワーク・バージョン1.0」



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

1-5.ビッグデータの包括的フレームワーク(続き)

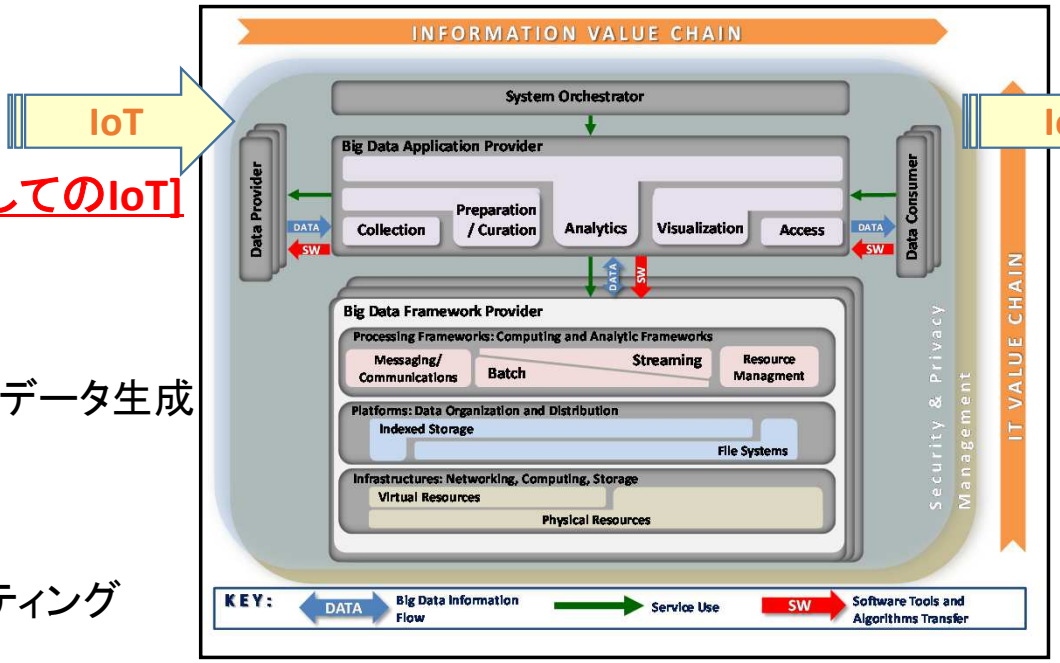
- 下位レイヤで運用管理やセキュリティ機能を持たせる流れが主流に

ロール	役割
システム オーケストレーター	システムが充足すべき要求事項の橋渡し役となり、データシステムの要件、設計、モニタリング機能を提供する
データプロバイダー	さまざまなソースから抽象データ型を生成し、異なる機能インタフェースで利用できるような形で提供する
ビッグデータアプリケーション プロバイダー	システム・オーケストレーターが設定した要求事項を充足するために、データライフサイクルの操作を実行する
ビッグデータフレームワーク プロバイダー	特定のアプリケーションを開発するビッグデータアプリケーションプロバイダーに、インフラストラクチャフレームワーク、データプラットフォーム、処理フレームワークを提供する
データコンシューマー	ビッグデータの出力値を受け取る
セキュリティ／プライバシー ファブリック	ポリシー、要求事項、監査でシステムオーケストレーターと連携し、開発、導入、運用でビッグデータアプリケーションプロバイダーおよびビッグデータフレームワークプロバイダーと相互連携する
マネジメントファブリック	ビッグデータ環境に関連するシステムおよびビッグデータのライフサイクルを管理する

1-6.ビッグデータとIoTの関係

- NIST「ビッグデータ相互運用性フレームワーク・バージョン1.0」（前掲）

[データプロバイダーとしてのIoT]
- ソースからのデータ収集
- データの持続性
- データのスクラブ
- データの注釈付与／メタデータ生成
- アクセス権限管理
- アクセスポリシー契約
- データ配信API
- 機能（例：クエリ）のホスティング



IoT

[データコンシューマーとしてのIoT]
- 検索／取得
- ダウンロード
- ローカルでの分析
- レポーティング・可視化

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

AGENDA

2. 海外のデータアーカイブ管理に関わる主要ポリシー動向

2-1. 米国のデータアーカイブ管理に関わる主要ポリシー動向
2-2. 欧州のデータアーカイブ管理に関わる主要ポリシー動向
2-3. 欧米比較
2-4. 英国のEU離脱がデータアーカイブ管理にもたらすインパクトは？

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（1）

Healthcare Cloud

年月	機関名	内容
2012年2月	大統領行政府	「ネットワーク世界における消費者情報プライバシー：国際的デジタル経済におけるプライバシー保護と技術革新の促進」を公表
2012年3月	連邦取引委員会（FTC）	「急速に変化する時代における消費者プライバシーの保護」を公表
2012年3月	大統領行政府	「ビッグデータ研究開発イニシアティブ」を公表
2013年6月	国立標準技術研究所（NIST）	NISTビッグデータワーキンググループ（NBD-WG）のキックオフミーティングを開催
2013年7月	FTC	13歳未満の子どもを対象とした児童オンラインプライバシー保護法（COPPA）の改正規則を施行
2013年11月	FTC	ワークショップ「Internet of Things：接続された世界におけるプライバシーとセキュリティ」を開催
2014年5月	大統領行政府	「ビッグデータ: 機会を捉え、価値を保護する」を公表
2014年5月	FTC	「データブローカー：透明性と説明責任を求める」 を公表

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（2）

Healthcare Cloud

年月	機関名	内容
2014年8月	NIST	IoTに関連してNISTサイバーフィジカルシステム公開ワーキンググループ（CPS-PWG）の第1回会議を開催
2014年9月	FTC	ワークショップ「ビッグデータ：包含、排除いずれの手段か?」を開催
2014年10月	NIST	IEEEビッグデータカンファレンスにて、NISTビッグデータパブリックワーキンググループ（NBD-PWG）のワークショップを開催
2015年1月	FTC	「Internet of Things：接続された世界におけるプライバシーとセキュリティ」を公表
2015年3月	NIST	IoTに関連して「時間認識アプリケーション、コンピューター、通信システム（TAACCS）」を公表
2015年3月	FTC	プライバシー、データセキュリティ、スマートホーム、ビッグデータ、IoTなど次世代の消費者保護を目的とした技術研究・調査室（OTRI）を新設
2015年4月	NIST	NISTビッグデータパブリックワーキンググループ（NBD-PWG）が、ビッグデータ相互運用性フレームワーク・バージョン1.0草案を公表
2015年6月	NIST	外部委託先向けの機微な政府情報保護ガイドライン(SP 800-171）最終版を公表

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（3）

Healthcare Cloud

年月	機関名	内容
2015年9月	NIST	NISTサイバーフィジカルシステム・パブリックワーキンググループ（CPS-PWG）が、サイバーフィジカルシステムのフレームワーク0.8草案を公表
2015年9月	NIST	NISTビッグデータパブリックワーキンググループ（NBD-PWG）が、ビッグデータ相互運用性フレームワーク・バージョン1.0(SP 1500)最終版を公表
2015年9月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、属性ベースアクセス制御（ABAC）に関するガイドライン（SP 1800-3）草案を公表
2015年10月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、金融サービス業界向けのIT資産管理に関するガイドライン（SP 1800-5）草案を公表
2015年11月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、クラウド／ハイブリッド環境の医療機器セキュリティに関するガイドライン（SP 1800-4）草案を公表
2015年11月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、金融サービス業界向けのデータ・インテグリティに関する白書草案を公表
2015年12月	NIST	重要インフラのサイバーセキュリティ向上のためのフレームワーク利用に関する情報提供依頼書（RFI）を公表

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（4）

Healthcare Cloud

年月	機関名	内容
2015年12月	NIST	乱数生成に利用するエントロピー源の提言（SP 800-90B）草案を公表
2015年12月	大統領行政府	オバマ大統領が、「2015年サイバーセキュリティ情報共有法」を含む連邦政府包括支出パッケージに署名
2016年1月	FTC	ビッグデータに関する報告書を公表
2016年2月	大統領行政府	「サイバーセキュリティ国家行動計画」を公表
2016年3月	NIST	クラウドアクセシビリティ公開ワーキンググループが、クラウドコンピューティングとアクセシビリティに関する考慮（SP 500-317）草案を公表
2016年3月	NIST	連邦政府における暗号基準利用ガイドライン：暗号メカニズム（SP 800-175B）草案を公表
2016年3月	NIST	企業のテレワーク、遠隔アクセス、BYODセキュリティに関するガイドライン（SP 800-46 Rev. 2）草案を公表
2016年3月	NIST	データ中心システムの脅威モデリングに関するガイドライン（SP 800-154）草案を公表
2016年3月	NIST	信頼できる電子メールに関するガイドライン(SP 800-177）草案を公表

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（5）

Healthcare Cloud

年月	機関名	内容
2016年4月	FTC	保健福祉省（HHS）傘下の国家医療IT調整室（ONC）、公民権局（OCR）、食品医薬品局（FDA）と共同で、モバイルヘルスアプリケーション開発者向けのガイドラインを公表
2016年4月	NIST	連邦政府における暗号基準利用ガイドライン:指令、義務、政策（SP 800-175A）草案を公表
2016年4月	NIST	乱数生成構築の提言（SP 800-90C）草案を公表
2016年4月	NIST	サイバー脅威情報共有ガイドライン(SP 800-150）草案を公表
2016年5月	NIST	システムセキュリティ・エンジニアリングガイドライン（SP 800-160）草案を公表
2016年5月	NIST	電子署名ガイドライン（SP 800-63-3）草案を公表
2016年5月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、小売業界向けの電子商取引の多要素認証に関するプロジェクト案を公表
2016年5月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、小売業界向けのクレジットカード以外のセキュア化、消費者データセキュリティに関するプロジェクト案を公表

2-1.米国のデータアーカイブ管理に関わる主要ポリシー動向（6）

Healthcare Cloud

年月	機関名	内容
2016年6月	FTC	IoTの発展促進における政府の利点、課題と潜在的役割に関する文書を、商務省に提出
2016年6月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、スマートホームデバイスのアイデンティティ／アクセス管理に関する白書草案を公表
2016年6月	NIST	サイバーセキュリティのイベント・リカバリーに関するガイドライン（SP 800-184）草案を公表
2016年6月	NIST	ITプロフェッショナル向けApple OS X 10.10 システムのセキュリティガイドライン（SP 800-179）草案を公表
2016年6月	NIST	NISTサイバーフィジカルシステム・パブリックワーキンググループ（CPS-PWG）が、サイバーフィジカルシステムのフレームワーク1.0最終版を公表
2016年7月	NIST	セキュリティ設定共通化手順（SCAP）バージョン1.3の仕様に関するガイドライン（SP 800-126A、SP 800-126 Revision 3）草案を公表
2016年7月	NIST	国立サイバーセキュリティセンターオブエクセレンス（NCCoE）が、モバイルアプリケーションのシングルサインオンに関する白書草案を公表

2-2.欧州のデータアーカイブ管理に関わる主要ポリシー動向（1）

Healthcare Cloud

年月	機関名	内容
2009年6月	欧州委員会	RFIDから医療、環境・エネルギーなど様々な分野に対象を拡張した「Internet of Things行動計画」を公表
2010年2月	閣僚理事会	司法・内務理事会が「EU域内セキュリティ戦略」を採択
2010年3月	欧州委員会	「EU域内セキュリティ戦略」を承認
2010年4月	欧州ネットワーク情報セキュリティ庁（ENISA）	飛行機の旅行をシナリオに用いたIoTおよびRFIDのリスクに関する評価結果を公表
2012年1月	欧州委員会	プライバシーに関わるEUデータ保護指令改正案を公表
2013年2月	欧州委員会	「ネットワーク・情報セキュリティ（NIS）指令」提案を盛り込んだ「EUサイバーセキュリティ戦略：オープン、安全、セキュアなサイバースペース」を公表
2013年10月	欧州議会	市民的自由・司法・内務（LIBE）委員会が、EUデータ保護指令改正案の修正案を可決
2014年3月	欧州議会	LIBE委員会の修正案を反映させたEUデータ保護指令改正案およびEU決議案を可決

2-2.欧州のデータアーカイブ管理に関わる主要ポリシー動向（2）

Healthcare Cloud

年月	機関名	内容
2014年9月	データ保護指令第29条作業部会	「ビッグデータの発展の個人データ保護への影響に関する声明」を採択
2014年9月	データ保護指令第29条作業部会	「近年のIoTの発展に関する意見書」を採択
2014年12月	閣僚理事会	司法・内務理事会が「改正EU域内セキュリティ戦略」を採択
2015年1月	欧州委員会	2015年欧州データ保護デーを開催
2015年2月	ENISA	「スマートホームとメディアコンバージェンスの脅威動向とグッドプラクティスガイド」を公表
2015年3月	データ保護指令第29条作業部会	欧州委員会の要請を受けて「アプリケーションとデバイスにおけるヘルスデータ」を公表
2015年3月	欧州委員会	IoTイノベーションを推進する官民連携組織として、AIOTI(Alliance for Internet of Things Innovation)を設置
2015年4月	欧州委員会	ファクトシート「EUデータ保護改革とビッグデータ」を公表
2015年4月	欧州委員会	「セキュリティに関する欧州の行動計画」を公表

2-2.欧州のデータアーカイブ管理に関わる主要ポリシー動向（3）

Healthcare Cloud

年月	機関名	内容
2015年5月	欧州委員会	EU域内デジタルマーケットの障壁撤廃を目指す「欧州デジタル単一市場戦略」を公表
2015年5月	欧州データ保護監視官局（EDPS）	「モバイルヘルスに関する意見書」を公表
2015年6月	閣僚理事会	司法理事会がEUデータ保護指令改正案を承認し、EUデータ保護規則提案に暫定合意
2015年6月	欧州委員会、欧州議会、閣僚理事会	EUデータ保護規則提案に係る三者対話を開始
2015年10月	EU司法裁判所	EU・米国間のセーフハーバー協定を無効とする判決を下す
2015年10月	欧州委員会	AIOTIが、EUの研究開発戦略「Horizon 2020」のプログラムとして、IoTのイノベーションと導入に関する提言を公表
2015年11月	欧州委員会	AIOTIが、IoTの標準化とアーキテクチャに関するワークショップを開催
2015年11月	欧州データ保護監視官局（EDPS）	「ビッグデータの課題への対応」と題する意見書を公表

2-2.欧州のデータアーカイブ管理に関わる主要ポリシー動向（4）

Healthcare Cloud

年月	機関名	内容
2015年12月	ENISA	「スマートホーム環境のセキュリティとレジリエンス」を公表
2015年12月	欧州委員会、欧州議会、閣僚理事会	「ネットワーク・情報セキュリティ（NIS）指令」提案に合意
2015年12月	ENISA	「ビッグデータにおけるプライバシー・バイ・デザイン」と題する報告書を公表
2015年12月	欧州委員会	AIOTIが、IoTに関する長期戦略草案を策定
2016年1月	ENISA	「スマートシティのサイバーセキュリティ：公共交通のアーキテクチャモデル」と、「インテリジェント公共交通のサイバーセキュリティとレジリエンス：優れた取り組みと提言」と題する研究報告書を公表
2016年1月	ENISA	「ビッグデータの脅威動向とグッドプラクティスガイド」と題する報告書を公表
2016年7月	欧州委員会	サイバーセキュリティの欧州官民連携組織（PPP）を構築し、2020年までに180万ユーロを投資する計画を公表
2016年7月	欧州議会	「ネットワーク・情報セキュリティ（NIS）指令」を採択
2016年7月	データ保護指令第31条委員会	「EU-米国間プライバシーシールド」法律文書草案を修正の上、導入することに同意

2-3. 欧米比較

- 米国：
  複数の所管官庁を前提としたマルチステークホルダーアプローチ
  ⇒省庁横断的な取組、情報共有の拡大

- 欧州（EU）：
  3階層の法規制の組み合わせ
  - 全EU加盟国に適用される統一ルール（〇△規則）
  - EU加盟国共通のミニマム・スタンダード（〇△指令）
  - EU各加盟国が個別に定める法規制

2-4. 英国のEU離脱がデータアーカイブ管理にもたらすインパクトは？

- 領域・業種によって、法規制の適用対象が異なるEU

≪2018年時点の想定例≫

法規制領域	規則：EU域内 統一ルール	指令：EU域内 ミニマム・スタンダード	各加盟国個別法規制
プライバシー	一般個人データ保護規則 （2018年5月より、EU域内一律に適用）		
サイバー セキュリティ		ネットワーク情報 セキュリティ（NIS）指令	NIS指令に準拠して 各加盟国が法規制を改正
特許	欧州特許条約（EPC）　＊EUとは別の枠組 （欧州特許庁（EPO）所管下で加盟国一律に適用）		
商標・意匠	商標・意匠関連規則 （欧州連合知的財産庁（EUIPOEU）所管下でEU域内一律に適用）		
著作権		著作権関連EU指令	著作権関連指令に準拠した 各加盟国個別の法規制

2-4. 英国のEU離脱がデータアーカイブ管理にもたらすインパクトは？

- 複雑化する医薬品と医療機器と臨床試験の関係

≪2018年時点の想定例≫

法規制領域	規則：EU域内 統一ルール	指令：EU域内 ミニマム・スタンダード	各加盟国個別法規制
プライバシー	一般個人データ保護規則 （2018年5月より、EU域内一律に適用）		
サイバー セキュリティ		ネットワーク情報 セキュリティ（NIS）指令	NIS指令に準拠して 各加盟国が法規制を改正
医薬品	人用および動物用薬品の 認可手続きと監視、並びに 医薬品庁の設立に関する 規則 臨床試験規則　他	医薬品関連EU指令 （欧州医薬品庁（EMA）所管下でEU域内一律に適用）	医薬品関連規則／指令に 準拠した各加盟国内市場 向け法規制
医療機器	臨床試験規則 （施行時期未定）	医療機器関連EU指令	医療機器関連規則／指令 に準拠した各加盟国個別 の法規制

AGENDA

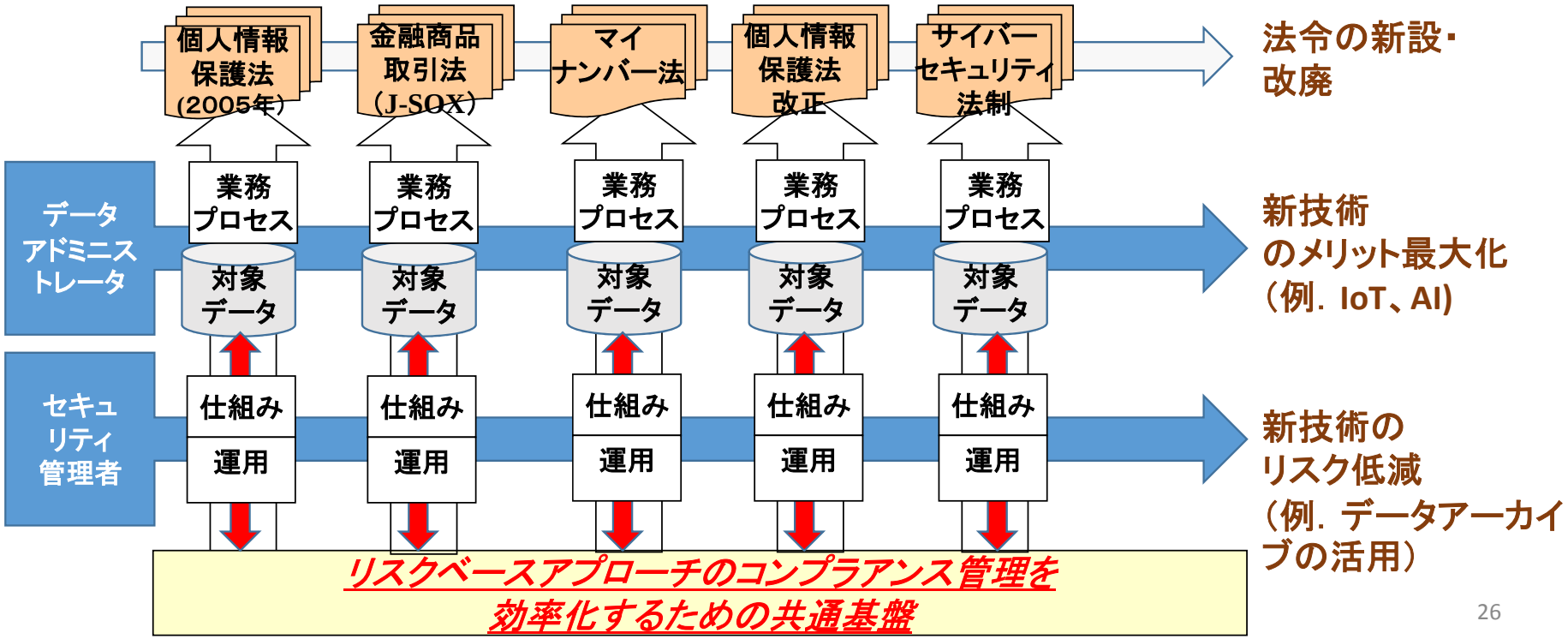
3. データアーカイブを活用したビッグデータ／IoT コンプライアンス対策のポイント

3-1. 持続可能なリスクベースの コンプライアンス管理基盤の必要性
3-2. ビッグデータセキュリティの 基本的考え方（CSA　Big Data WG）
3-3. ビッグデータ／IoTの融合局面における セキュリティ対策の方向性

3-1. 持続可能なリスクベースのコンプライアンス管理基盤の必要性

Healthcare Cloud

- データアドミニストレータとセキュリティ管理者の連携

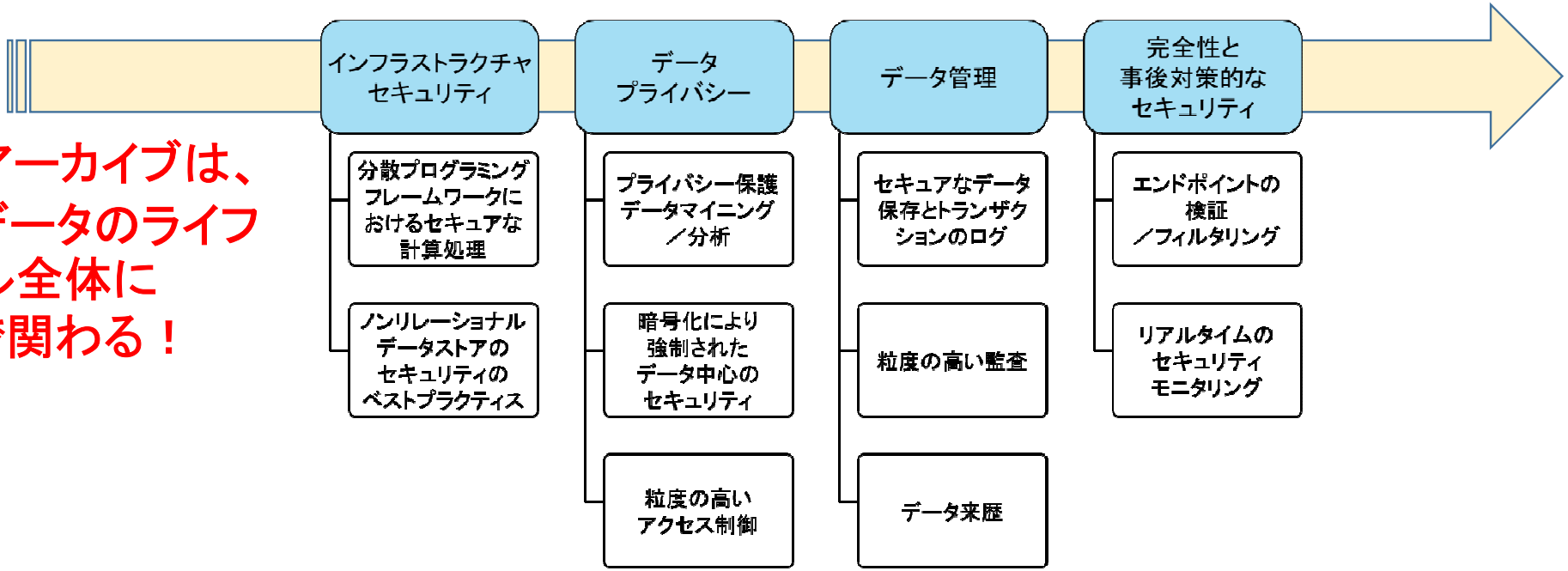


3-2. ビッグデータセキュリティの基本的考え方（CSA　Big Data WG）

Healthcare Cloud

- ビッグデータのセキュリティ／プライバシーにおける十大脅威

データアーカイブは、ビッグデータのライフサイクル全体にヨコ串で関わる！



出典：Cloud Security Alliance Big Data Working Group「Expanded Top 10 Big Data Security and Privacy Challenges」（2013年4月）
を基に、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が作成（2014年5月）

3-2. ビッグデータセキュリティの基本的考え方（CSA　Big Data WG）（続き）

Healthcare Cloud

- （例1）セキュアなデータ保存とトランザクションのログ
  - 分散型自動階層化ストレージ技術の課題
    - ≪メリット≫一貫した可用性の保証
      利用頻度の高いデータを上位の層、低いデータをより下位の層に格納することによって、可用性を高め、経費の節約を実現することが可能になる
    - ≪デメリット≫ 様々な脆弱性の問題
      低位層におけるセキュリティの脆弱性を狙ったDoS（サービス妨害）攻撃にさらされたり、低位層と高位層の間のパフォーマンスのギャップにより、高速再保存や災害復旧時のバックアップウィンドウが拡張されたりする可能性がある
  - ➢機密性と完全性の対策例：堅牢な暗号化技術やメッセージダイジェスト（暗号学的ハッシュ関数）など
  - ➢可用性の対策例：簡易的な復元可能性証明（POR）や動的で委任可能なデータ所有（DPDP）の手法の導入による改善など

3-2. ビッグデータセキュリティの基本的考え方（CSA　Big Data WG）（続き）

Healthcare Cloud

- （例2）粒度の高い監査を左右するログデータの管理
  - 多様化、複雑化するログデータ
    ～ルータ／スイッチのsyslog、OSのログ、データベースのログ、アプリケーションのログ、Webのアクセスログ　など
  - ビッグデータ環境のログデータ監査手法
    ①SIEMツールをビッグデータインフラストラクチャの外部に設定してログ監査を行う
    ②必要な監査情報を抽出して監査レイヤー／オーケストレイヤーを生成し、監査要件を取り込んで、監査人に返す

*監査の根拠になる法令や業種・業界によって、適用範囲や粒度が異なることが多い

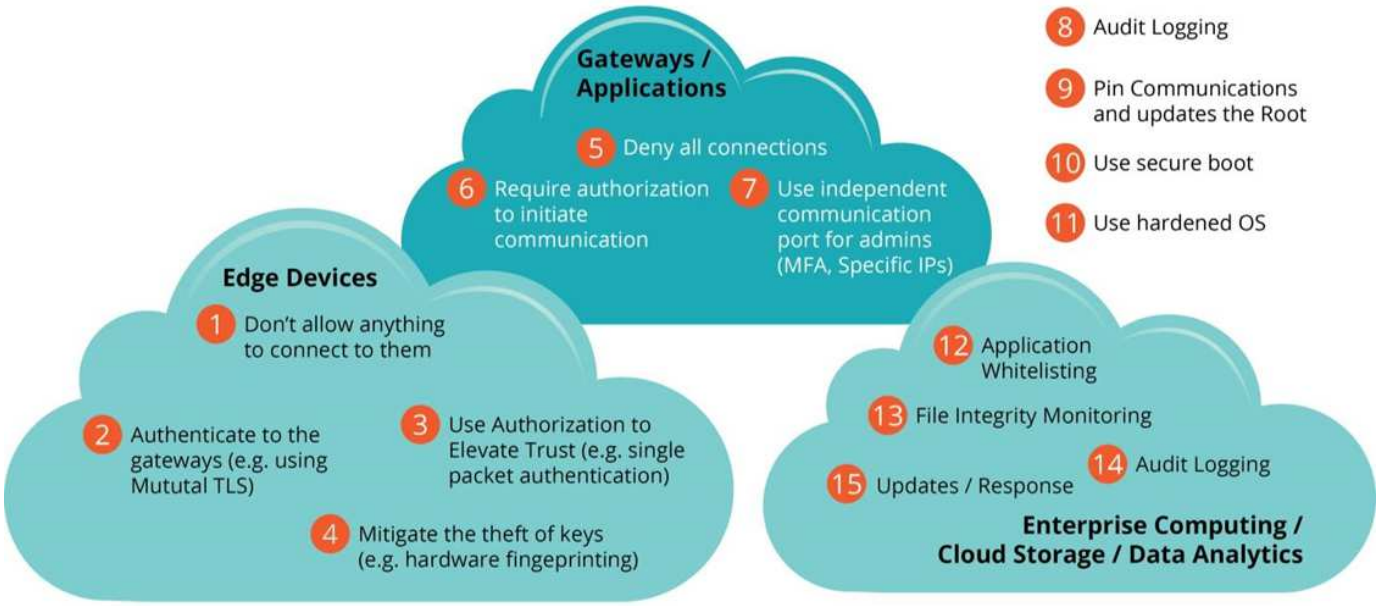
3-2. ビッグデータセキュリティの基本的考え方（CSA　Big Data WG）（続き）

Healthcare Cloud

- （例3）来歴メタデータのセキュアな保存・管理
  - 来歴（Provenance）
    ～データの完全性やデータの起源を証明するデジタル履歴の記録
    *証明、監査証跡、再現性の保証、信頼性、障害検知のために重要
  - 来歴メタデータを保存するストレージシステム
    来歴記録が信頼できるものであり、プライバシーが保護され、アクセス制御が適正に行われていることを保証する機能を追加導入する必要がある
    - アプリが稼働するインフラストラクチャが健全に稼働していることを保証する機能
    - 来歴記録が偽造／修正されていないことを保証する機能が必要となる。
    - 機微なプライバシー情報を保護する暗号化技術　など
  - ロールベースのきめの細かいアクセス制御が必要

3-3. ビッグデータ／IoTの融合局面における セキュリティ対策の方向性

- IoT保護アーキテクチャの構成要素とデータアーカイブの関係
  - ストレージ側に機能を持たせて、デバイスやアプリに極力負荷をかけない（⇒クラウド／ハイブリッド型への期待）



出典：Cloud Security Alliance Mobile Working Group「New Security Guidance for Early Adopters of the IoT」（2015年4月）

4. まとめ／Q&A

- 米国もEUも、個人データ保護／サイバーセキュリティ強化政策と同時並行で、ビッグデータやIoTによるイノベーション創出・事業化の促進政策を実施している
- ビッグデータ／IoTを取り巻くセキュリティ課題の理解を促進するとともに、新技術を導入する先進的な企業向けに、セキュリティコントロールの推奨事項やユースケース例を提供することを目的として、標準化／ガイドライン策定への取組が行われている
- ビッグデータ／IoTの融合局面では、データアドミニストレーターとセキュリティ管理者の相互連携が、企業のIT戦略上の課題となる
  ＊相互連携のインフラとしても、データアーカイブへの期待は大きい