

IT監査保証の判断基準 プロジェクト報告

「情報インテグリティ」の概要と
医療分野への適用事例

2016年6月3日

「IT監査保証の判断基準」 研究プロジェクトについて

- 2015年4月開始
- 2015年研究大会「ドラッカーの遺言の事後検証」
- メンバー

氏名	所属等	備考
松尾 明	公認会計士、公認情報システム監査人、 TOGAF9認定アーキテクト	主査
石島 隆	公認会計士、システム監査技術者	
遠藤 正之	博士(システムデザイン・マネジメント学)、システム監 査技術者	
成田 和弘	システム監査技術者、公認内部監査人、公認 情報システム監査人	
長野 加代子	システム監査学会員	

2015年度の活動報告

- Information Integrity
- 金融分野での事例
- 医療分野での事例
- COBIT5によるアセスメント
- →2015年度第2回定例研究会で中間報告



2016年3月28日(月)
システム監査学会2015年度第2回定例研究会

金融の事例 ～Fintechとブロックチェーン技術～

1. 金融
2. Fintech: 金融におけるイノベーション
3. ブロックチェーン技術(分散型台帳)

静岡大学情報学部准教授 遠藤正之
博士(システムデザイン・マネジメント学)
システム監査技術者

Copyright © Masagaki Endo

1

Mon., Mar. 28th, 2016 JSSA 2015年度第2回定例研究会資料 研究会参加者限り

COBIT5 Assessment Programme について

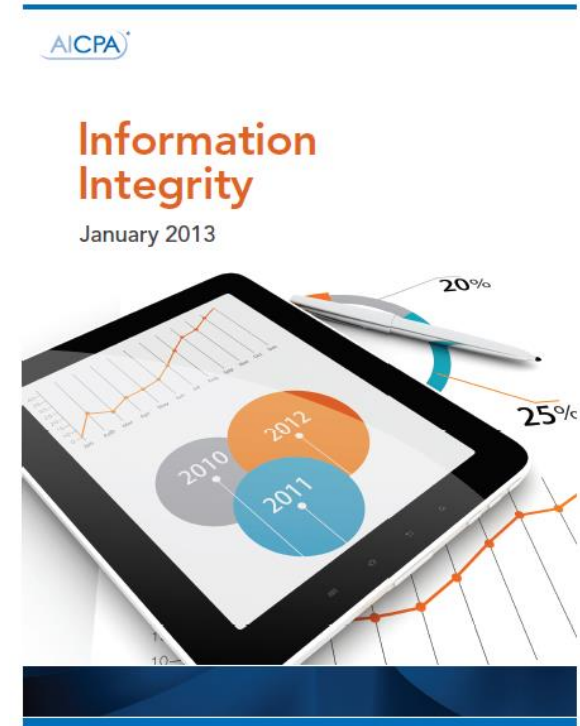
- COBIT5によるプロセス評価の基準 -

Kazuhiro Narita
Certified Internal Auditor (CIA)
Certified Information System Auditor (CISA)
Japan's ITEE System Auditor /
Information Technology Strategist / Project Manager /
Information Security Administrator

3

Information Integrity

- 米国公認会計士協会とカナダ勅許会計士協会協働の
トラスト情報インテグリティ・タスクフォース
- 目次
 - はじめに
 - 範囲
 - 情報ライフサイクルの理解
 - 情報インテグリティリスク
 - 情報インテグリティ保証のための規準
 - 重要性
 - 報告書



【出典：<http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/ASEC-Information-Integrity-White-paper.pdf>】

情報インテグリティ保証のための規準

AT 101.24では、判断規準は、適切でなければならない、ということは、客観的、測定可能、完全で関連付けられなければならないことを意味する。

□ 基準は、主題を測定し提示する業務実施者が主題を評価する標準またはベンチマークである。適切な基準は、以下の属性を持っているなければならない。

- 客観性：基準にはバイアスがかかってはいけない
- 測定可能性：基準は主題に、質的または量的である合理的に一貫した測定を可能としなければならない
- 完全性：主題の結論を変えうる関連要因が省略されないように、基準は十分に完全でなければならない
- 関連性：基準は主題に関連していなければならない

はじめに

本ペーパーは、情報インテグリティを有するとはどのような意味か、そしてどのように情報インテグリティを達成し、維持できるのかに、焦点を当てている。

- 利害関係者は、意思決定を行う時にこの情報を利用し、解釈し、又は他の情報を利用して、一般的に主題に関する彼らの知識を増やす。最高意思決定を行うために、利用者は情報のインテグリティを信頼している必要がある。
- 第3者保証業務実施者による情報インテグリティの検証を通して付加価値を与えるためには、幾つかの重視すべきことがある。

情報インテグリティの範囲

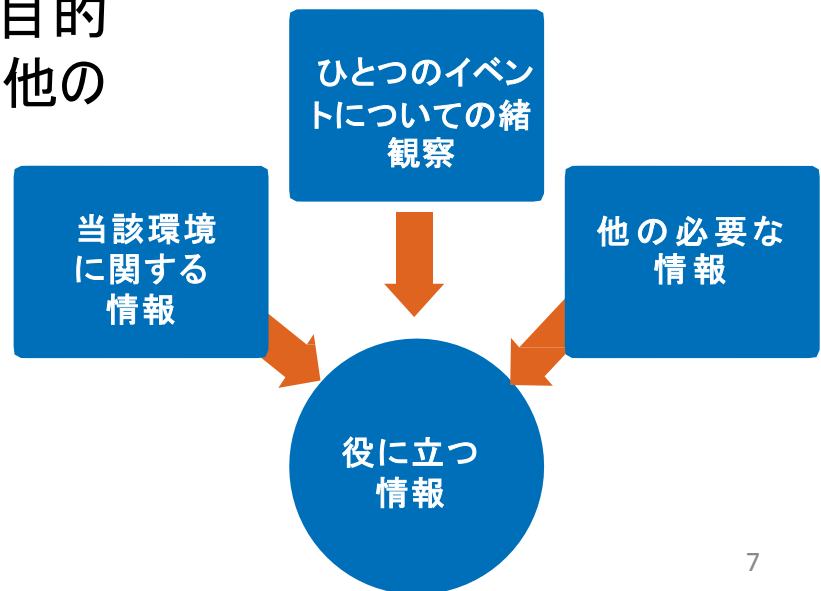
情報インテグリティは、情報の対象としている対象物への表現的健全性のある情報、およびその意図する利用への情報の一貫性と定義される。

□ メタ-情報

情報が有用であるために、情報の目的および情報を利用するのに必要な他の文脈情報

□ 役に立つ情報

特定の目的のために、正確性、関連性、精度、適時性、および完全性のある情報



定義(参考)

- 情報:
ひとりの利用者に意味のあるひとつの文脈(context)で提示されるあらゆるデータをいう、これに対して、原始データは、説明もなくそれに対する情報もない(すなわち、メタデータまたはメタ情報なしにという)。
- メタデータ:
データのためのデータ、もっと特定していえば、メタデータは、内容(content)、文脈(context)、およびデータの構造(structure)を記述したデータである。
- メタ情報:
情報処理システムが処理中に情報インテグリティを維持するために、また、利用者が情報を理解するためにも必要なひとつの情報のセットである。

調査報告書

独立した公認会計士や勅許会計士によって提供された情報インテグリティの調査報告書は、通常最高レベルの信頼を与える。

□ 情報インテグリティに対する信頼は、以下を含む多くのsourceによってもたらすことができる。

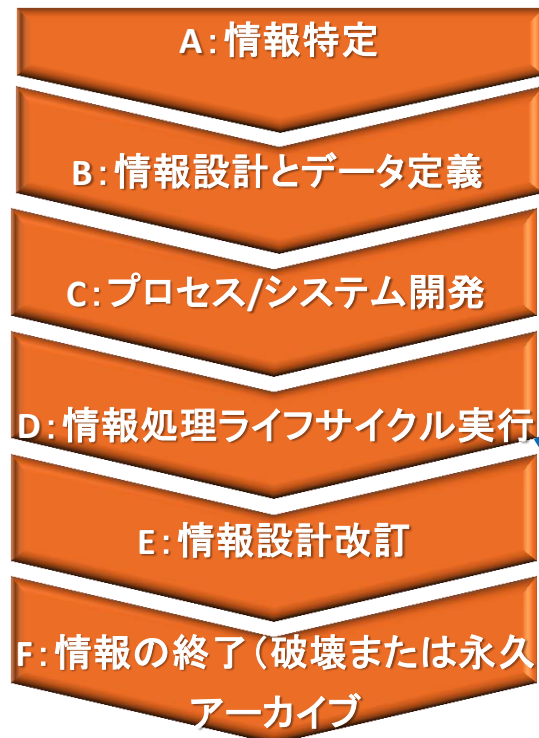
- A. 情報に責任を持つpartyによって提供された情報を生成したプロセスの記述などの情報
- B. the responsible partyの評判
- C. 利用者が保有している知識、インテグリティを評価する目的で特別に入手してもよい
- D. 情報のインテグリティを評価するに十分な知識を持つ第三者による情報のvalidation
- E. 独立した第三者により作成された情報のインテグリティを評価する報告書の入手

□ 情報の当該インテグリティについて新たなガイダンスが必要なように思われる。

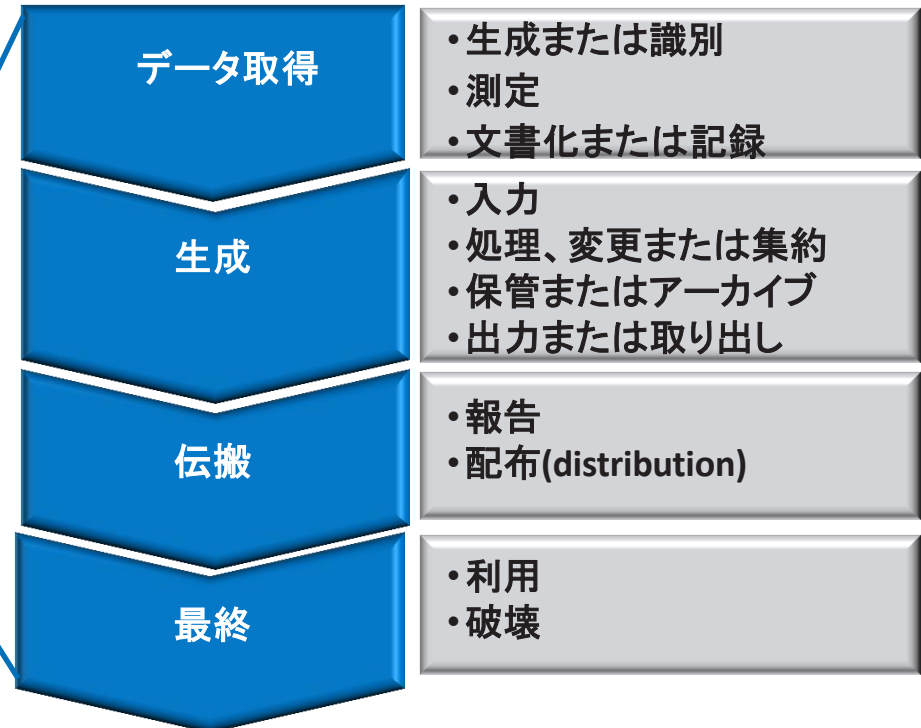
情報ライフサイクルの理解(1)

- 特定の情報の必要性を認識することによって、情報を取得するか、または、情報を開発するプロセスを開始する。

＜情報開発ライフサイクル＞



＜情報処理ライフサイクル＞



情報ライフサイクルの理解(2)

情報がなにであるかを示し、イベントやインスタンスとその属性の理解に貢献するメタ-情報は情報についての情報。

- 環境の特性を考慮した情報の文脈を含める
- 定性的情報は、十分な客観性を確保
- 将来のイベントの発生可能性に留意
- メタ-情報が追加情報を提供し、文脈内で情報を目的に合致させる

情報ライフサイクルの理解(3)

□A:文脈の変更

- 1. 意図の理解が困難になる
- 2. メタ情報との分離
- 3. 異なる規準の使用

□B:システム間の移動

- 品質のバラツキのあるシステムを通過した伝達

情報は異なるシステムを移動でき、システム間のコントロールの質に定めのないことが、そのインテグリティを危うくする。

情報インテグリティリスク(1)

情報が意図する目的のために適切でなく、またはメタ-情報が完全でなく、誤った、ミスリードするものであれば、情報の誤った解釈や誤った適用が起こりうる。

□ 主題リスクの要素

- A: 属性又は環境属性や他のメタ-情報が観察、測定できない
- B: ミスリーディングな情報

□ 利用リスクの要素

- A: 利用者が情報を意図した目的を超えて利用したり利用に失敗する不適切な選択、適切情報の脱落、情報/メタ情報の誤解釈、誤適用、意思決定プロセスの非一貫性、提供者と利用者の意図の非一貫性
- B: 意図した利用者でない者の利用



情報インテグリティリスク(2)

□情報設計リスク

■ A: 報告される属性/特性

- ・ 不適切な表示、陳腐化、不正確、偏見、不精密、不十分な集約/非集約、非一貫性/反復不可能、標準(norm)や他の源泉(source)と一貫していない

■ B: 測定から報告までの情報処理で発生、C: 保管で発生、D: 回復により発生

□情報処理ライフサイクルリスク

■ A: データの作成または識別、B: 測定、C: 文書化又は記録、D: 入力、E: 処理、変更または集約(aggregation)、F: 保管(storage)またはアーカイブ、G: 出力または回復、H: 利用、I: 破壊(destruction)

いくつかのリスクは、有効なコントロールによって対処できるが、他のものは、その他の回避のようなリスク低減戦略で対処する必要があるかもしれない。

■ 主題が適切な、可用性のある判断規準に照らして評価できない場合、業務を受託しないことで避けるべきである

重要性

□情報をもとに意思決定を行おうする利用者の判断に影響する項目は重要である

重要性のより難しい側面は、量的側面だけでなく質的側面でもあること。

□保証業務においては保証報告書に重要性を開示する

□財務諸表監査では、重要性を判断する方法は十分に確立されているが、他の保証業務では、重要性の情報による利用者の理解の向上が必要

報告書

適切にタグづけされた電子報告書は、マシンからマシン、プラットフォームからプラットフォームへ伝播され、電子的手段で読むことができるという利点がある。

□ 安全な電子出版を利用する

- 1. 承認— タイムスタンプにより電子署名時の適切性が判断できる。
- 2. 認証— 発行者によって作成されたものとの同一性を保証する。
- 3. インテグリティ— 情報が当初から変更されていない。
- 4. 非否認— 報告書の発行、報告書の受け取りを否定できない。

報告書の利用者も、提示された報告書が“業務実施者が発行したものと同じであるかを確かめることに興味を持つかもしれない。

まとめ

- 第三者評価業務を行うときには使用する情報のインテグリティに留意して評価する。
- 情報のインテグリティに関するリスクには、情報処理ライフサイクルプロセスによるものの他に、主題リスク、利用リスク、情報設計リスクがある。
- 報告書の作成に当たっては、どのような情報を元に評価したかを示す。
- 電子報告書自体のインテグリティは電子出版物への電子署名で実現できる。

医療分野への適用事例

social

- 米国OpenGroupの取り組み
- オープンプラットフォーム3.0の世界で患者中心のヘルスケアを設計
- 患者中心のケア
- 背景

cloud
computing

big data

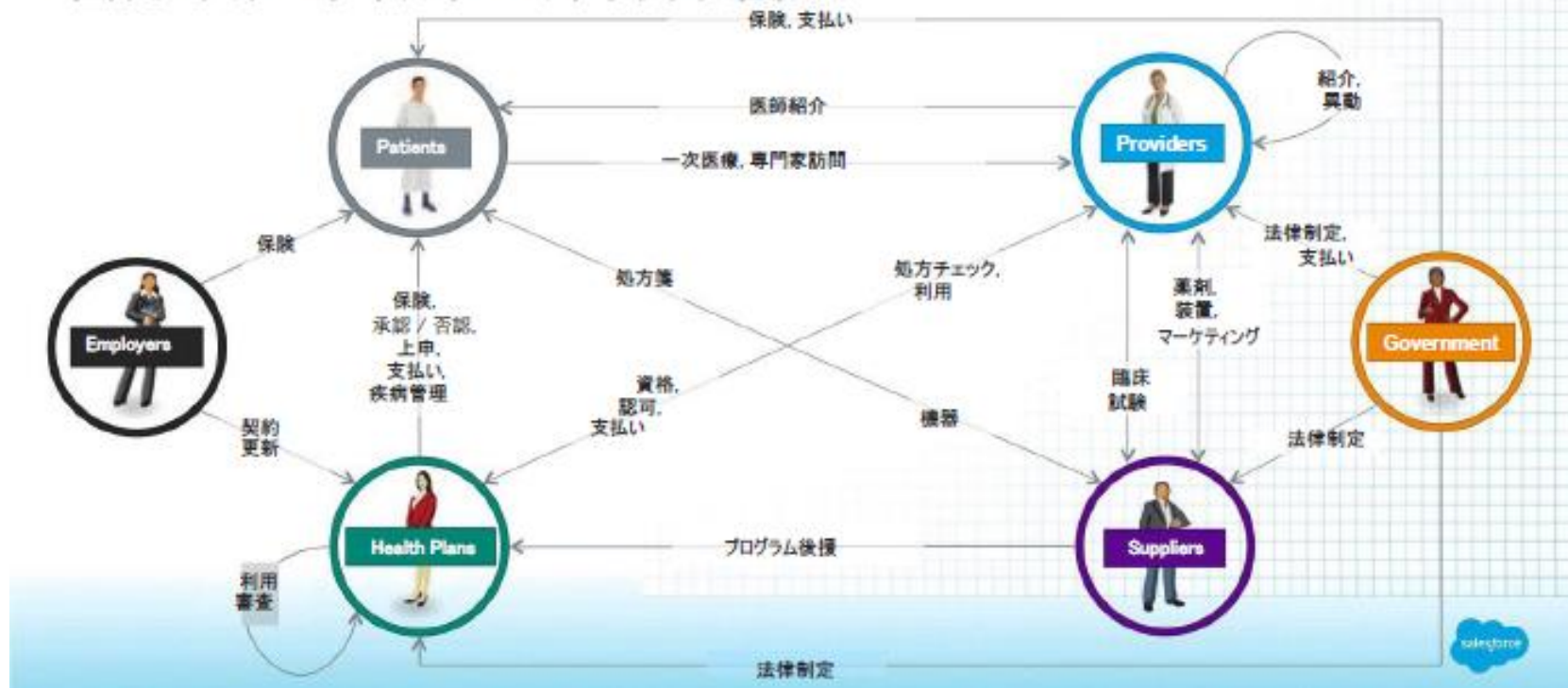
mobile

internet
of things



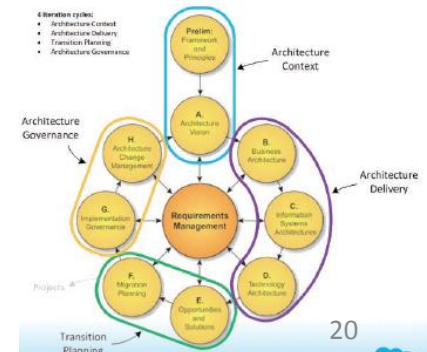
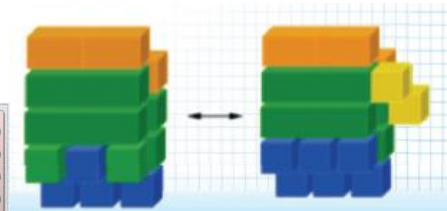
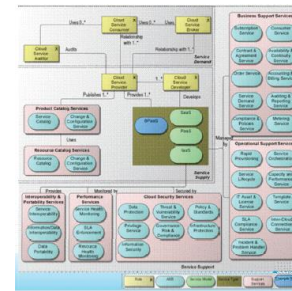
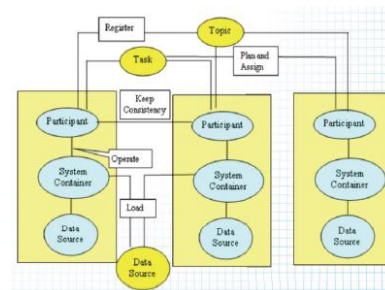
患者中心の医療のステークホルダーの特定

出力: ステークホルダーマトリックス 

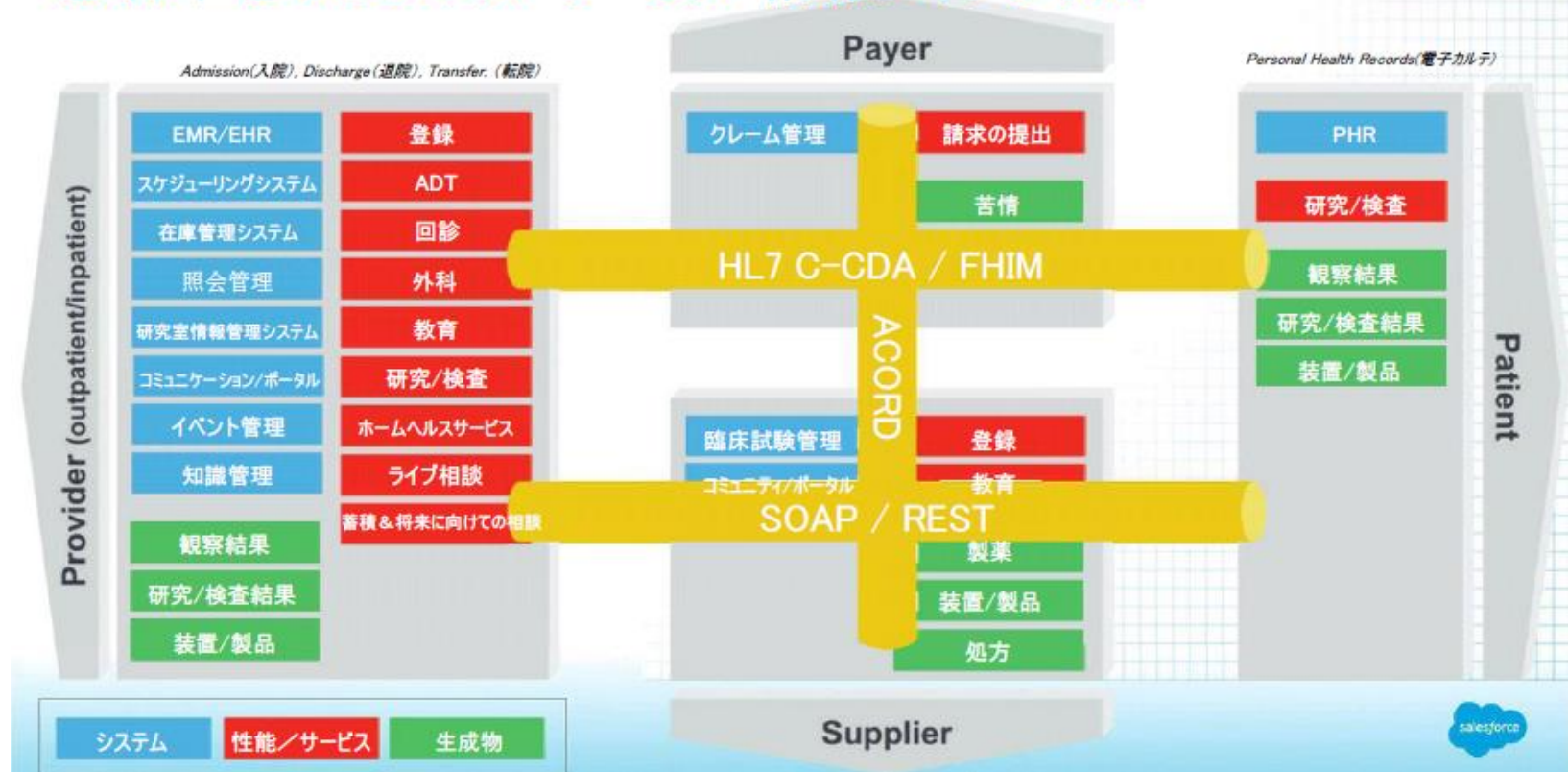


適用参照アーキテクチャ/モデル

- Open Group のアーキテクチャ連続
- Open Group のクラウドの生態系参照モデル
- 連邦保健情報モデル
- ACORD保険情報モデル
- 社会的共同モデル



患者中心のビジネス・サービス/情報ダイアグラム



標準

- HL7 (Health Level Seven)
- C—CDA (Consolidated—Clinical Document Architecture)
- FHIM (Federal Health Information Model)
- ACORD (Association for Cooperative Operations Research and Development)
- SOAP (Simple Object Access Protocol)
- REST (Representational State Transfer)

相互運用性 Interoperability

- 2つ以上のシステムで情報交換する能力
- それらのシステムが交換された情報を利用する能力 (IEEEの定義)

意味
(Meaning)

← 意味論的な相互運用性
(Semantic Interoperability)

コンテンツ構造
(Content Structure)

← 統語的な相互運用性
(Syntactic Interoperability)

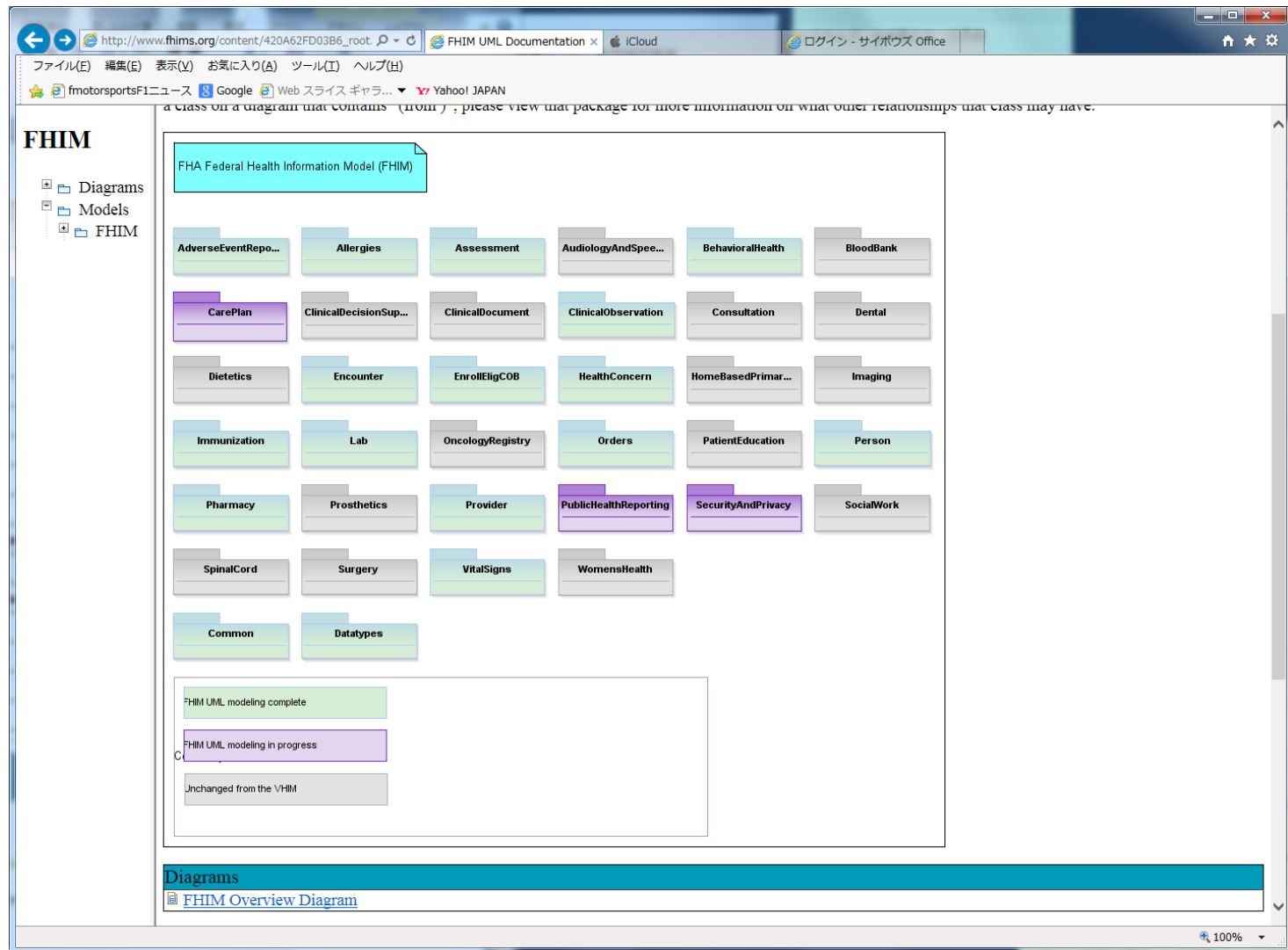
標準を通じたデータ共有

ヘルスケアの分野では標準を利用することで、

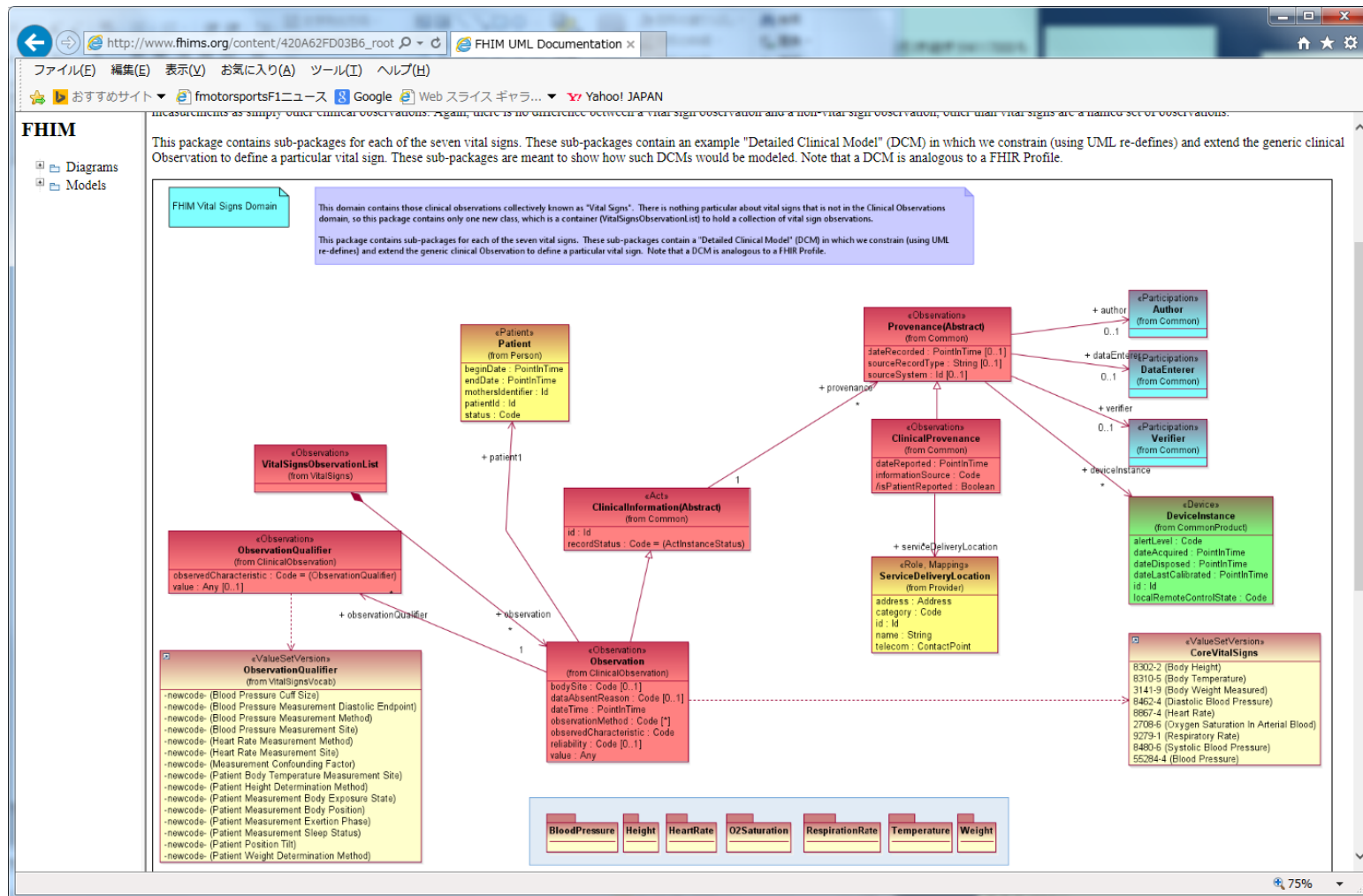
情報のインテグリティを確保し、健康情報の相互運用を実現！

23

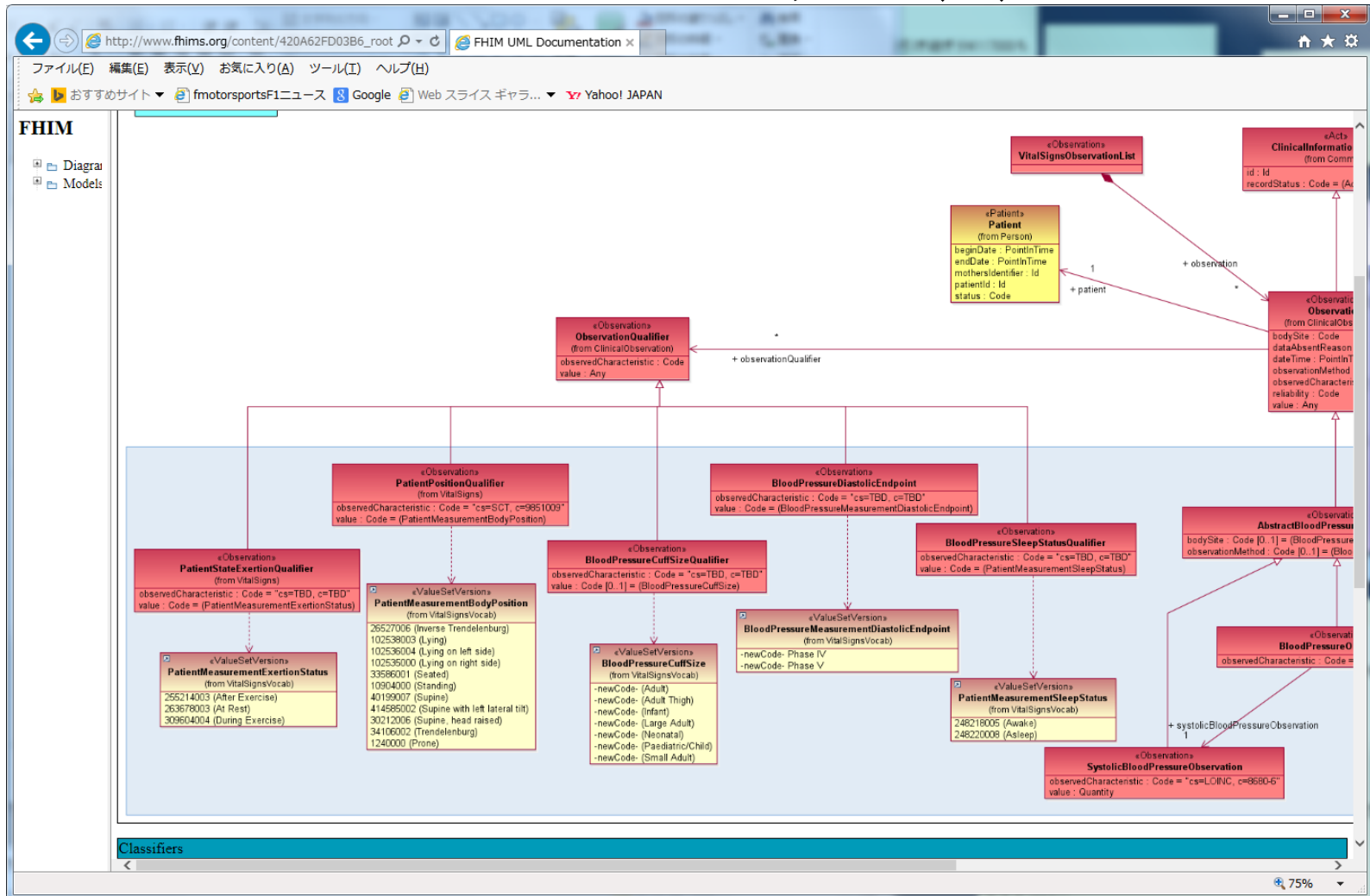
FHIMのドメイン



FHIMのモデル(1)



FHIMのモデル(2)



構成要素の定義

http://www.fhims.org/content/420A62FD03B6_root FHIM UML Documentation

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)

おすすめサイト fmotorsportsF1ニュース Google Web スライス ギャラ... Yahoo! JAPAN

FHIM

Diagrams
Models

ClinicalObservation UML Documentation

Overview Top Package Element

Summary: [Attributes](#) [Properties](#) Detail: [Attributes](#)

ClinicalObservation
Class Observation

An event in which a Clinical Observation is recorded.

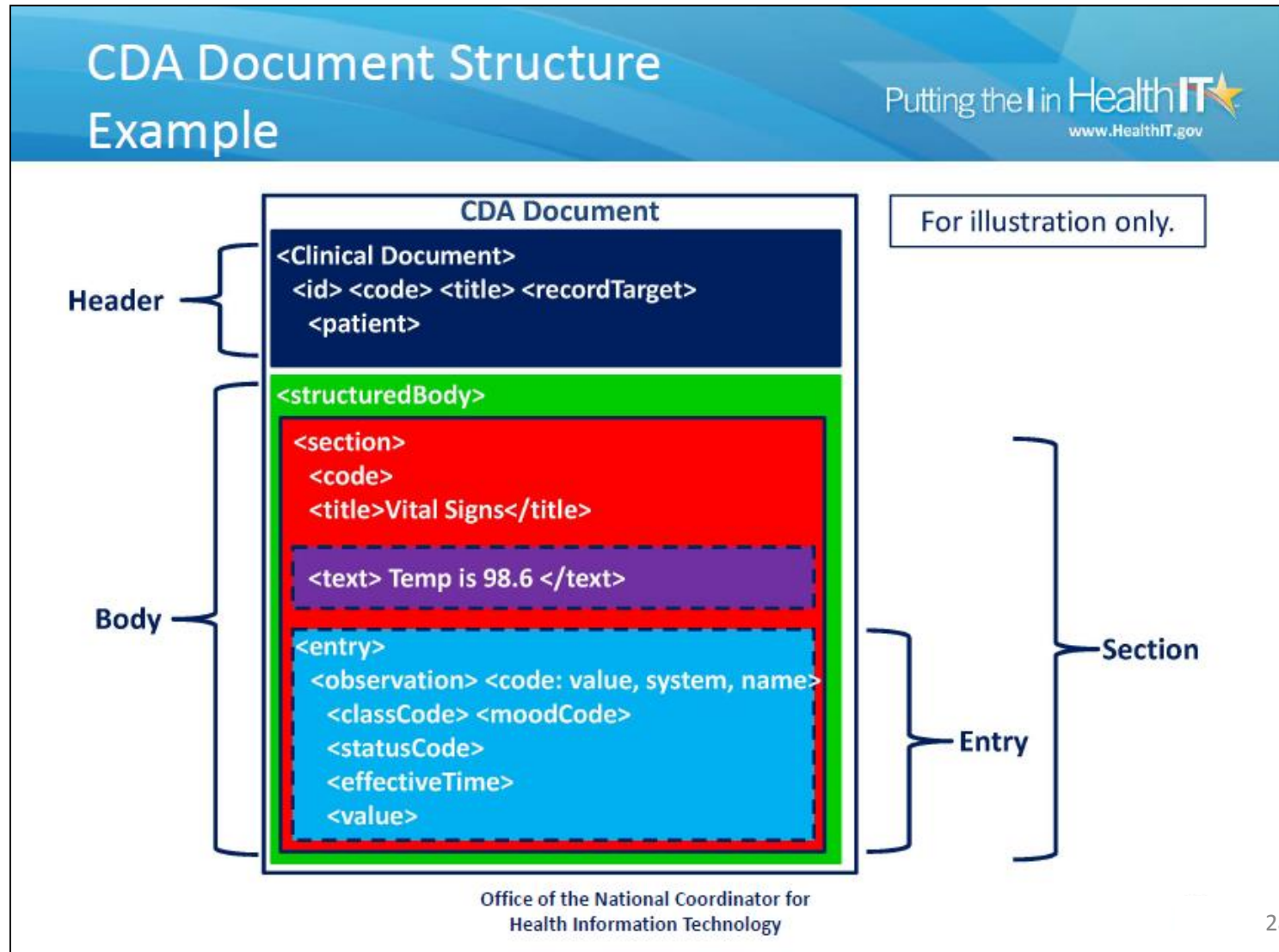
"Measurements and simple assertions made about a patient, device or other subject." - HL7 FHIR, Observation resource.

Attributes

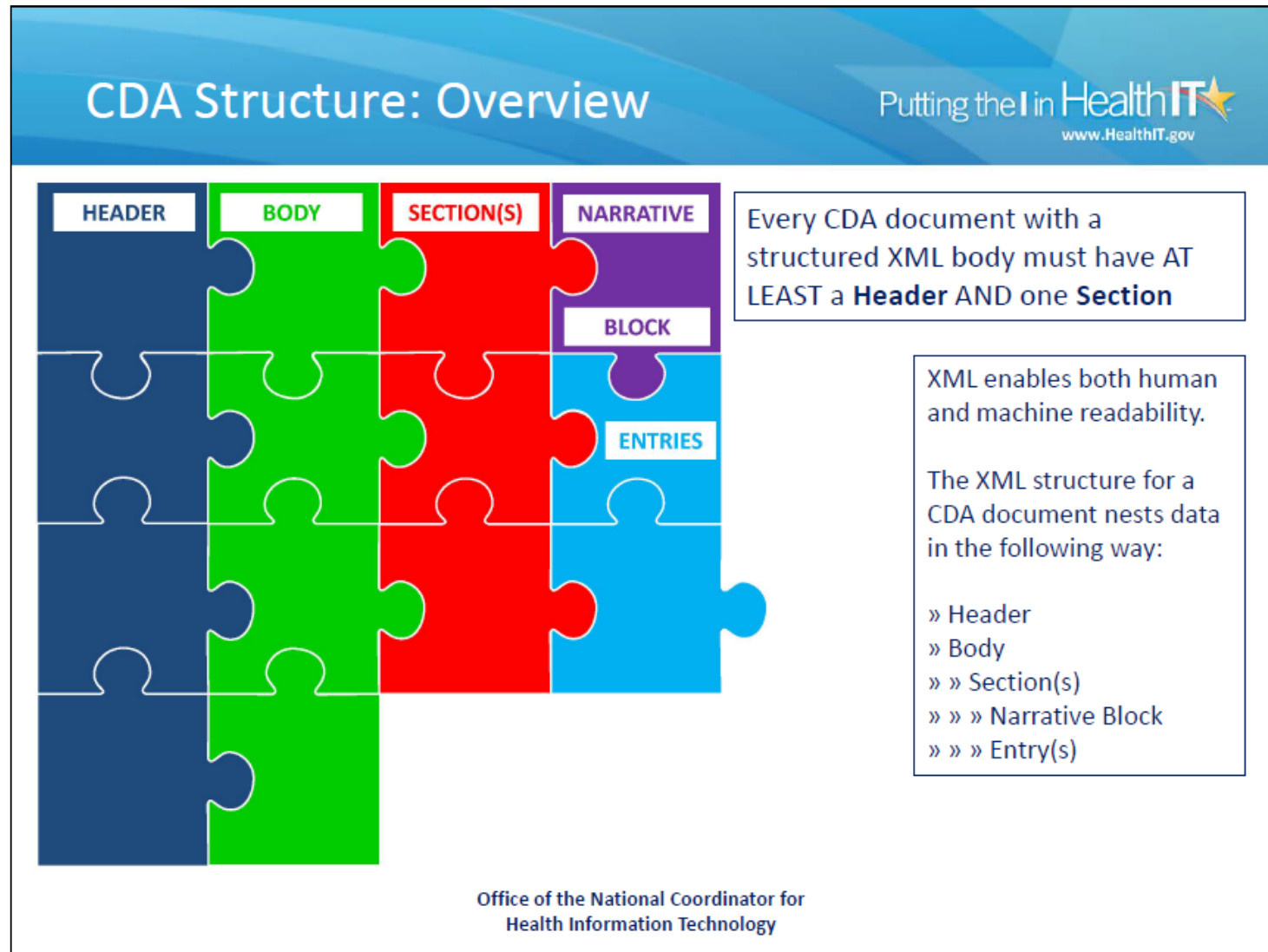
«CS» Code	bodySite	A code specifying detail about the anatomical site or system that is the focus of the Observation. "Indicates the site on the subject's body where the observation was made (i.e. the target site)." - HL7 FHIR, Observation.bodySite.
«CS» Code	dataAbsentReason	"Provides a reason why the expected value in [value] is missing" - HL7 FHIR, Observation.dataAbsentReason.
«TS» PointInTime	dateTime	The date (and optionally, time) that the Observation took place. Note that this is the clinically-relevant time, for example, the clinically relevant time of a result of a lab test on a blood sample is the time the blood was drawn, not when the test was run. Note that in FHIR this can be either a point in time or a period (i.e., a TimeInterval). In the FHIM, this is currently modeled as only a point in time. Note also that when used by the Condition sub-type of Observation, this is the date that the Condition was first detected or asserted. "This field is required in two circumstances. The first is when the observations reported beneath one report header have different dates/times. This could occur in the case of queries, timed test sequences, or clearance studies where one measurement within a battery may have a different time than another measurement.... The observation date-time is the physiologically relevant date-time or the closest approximation to that date-time. In the case of tests performed on specimens, the relevant date-time is the specimen's collection date-time. In the case of observations taken directly on the patient (e.g., X-ray images, history and physical), the observation date-time is the date-time that the observation was performed." - HL7 Version 2.8, OBX-14. "The time or time-period the observed value is asserted as being true. For biological subjects - e.g. human patients - this is usually called the "physiologically relevant time". This is usually either the time of the procedure or of specimen collection, but very often the source of the date time is not known, only the date time itself" - HL7 FHIR, Observation.applies. "Contains the date time when the corresponding problem was initially identified by the caregiver." - HL7 Version 2.8, PRB-7 "Estimated or actual date the condition problem/diagnosis was first detected/suspected." - HL7 FHIR, Condition resource.
«CS» Code	observationMethod	Provides additional detail about the means or technique used to ascertain the Observation. The method used may affect how the observation value is interpreted. "Indicates the mechanism used to perform the observation." - HL7 FHIR, Observation.method.
«CS» Code	observedCharacteristic	Indicates what was observed. This property may be re-defined in sub-classes to explicitly describe a particular kind of observation (e.g., Heart Rate). "Describes what was observed. Sometimes this is called the observation code." - HL7 FHIR, Observation.code.
«CS» Code	reliability	"An estimate of the degree to which quality issues have impacted on the value reported." - HL7 FHIR, Observation.reliability.
«ANY» Any	value	Contains the value of the Clinical Observation. This property is modeled as an Any datatype in the generic Observation; specific subtypes are expected to re-define this property to the appropriate datatype. "The information determined as a result of making the observation, if the information has a simple value." - HL7 FHIR, Observation.value.
«Act» CommentEvent	commentEvent	Pointer to any remarks about the Clinical Observation. "May include statements about significant, unexpected or unreliable values, or information about the source of the value where this may be relevant to the interpretation of the result." - HL7 FHIR, Observation.comments.
«EntryPoint, PatientEncounter» EncounterEvent	encounter	Pointer to the Encounter during which the Observation was made. When used by the Condition Statement sub-type of Observation Statement, this is the Encounter during which the Condition was first asserted. "Encounter during which the condition was first asserted." - HL7 FHIR, Condition resource. "The healthcare event (e.g. a patient and healthcare provider interaction) that relates to this observation." - HL7 FHIR, Observation.encounter.
«Act» InterpretationEvent	interpretationEvent	Pointer to an assessment of the value or result of the Clinical Observation. "The assessment made based on the result of the observation." - HL7 FHIR, Observation.interpretation.

http://www.fhims.org/content/_n.bH1LV.a.eE.d6.rJ7.j.pZ7LBFg-content.html 75%

C-CDAの例



C-CDAの構造

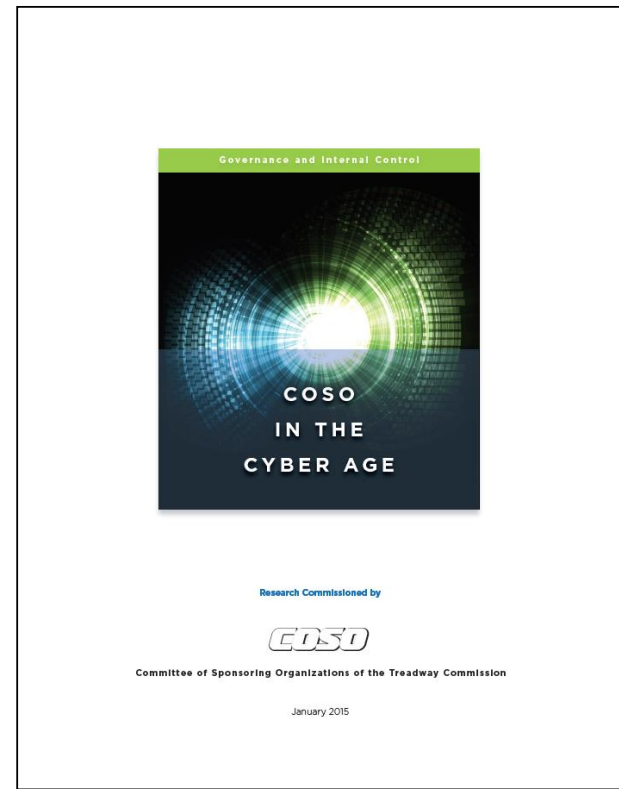


まとめ

- ヘルスケアの分野では標準、スタンダード、を利用することで、情報のインテグリティを確保し、健康情報の相互運用を実現

2016年の活動(予定)

- サイバーセキュリティ時代のガバナンスの評価指針
- COSO
IN THE CYBER AGE



【出典: http://www.coso.org/documents/coso%20in%20the%20cyber%20age_full_r11.pdf】

ありがとうございました。

ご参加をお待ちしております。