SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

欧米におけるトラストサービスに関わる調査業務

2020/3/31

一般社団法人データ流通推進協議会

Data Trading Alliance

略語

CA	Certification Authority	認証局
CAB	Conformity Assessment Body	適合性評価機関
CAR	Conformity Assessment Report	適合性評価レポート
EA	European co-operation for Accreditation	欧州認定協力機構
EC	European Commission	欧州委員会
EDS	Electronic Delivery Service	電子デリバリーサービス
ENISA	European Union Agency for Network and Information Security	欧州 ネットワーク情報セキュリティ庁
gTSL	Global Trust Service Status List	グローバルトラストサービスステータスリスト

IdP	Identity Provider	アイデンティティ プロバイダ
IO	International Organisation	国際機関
LotL	List of the Lists	リストのリスト
MS	Member State	加盟国
NAB	National Accreditation Body	国家認定機関
QTSP	Qualified Trust Service Provider	適格トラストサービスプロバイダ
SB	Supervisory Body	監督機関
TC	Third Country	第三国
TL	Trusted List	トラステッドリスト
TSA	Time Stamping Authority	タイムスタンプ局
TSP	Trust Service Provider	トラストサービスプロバイダ

目次

- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

目次

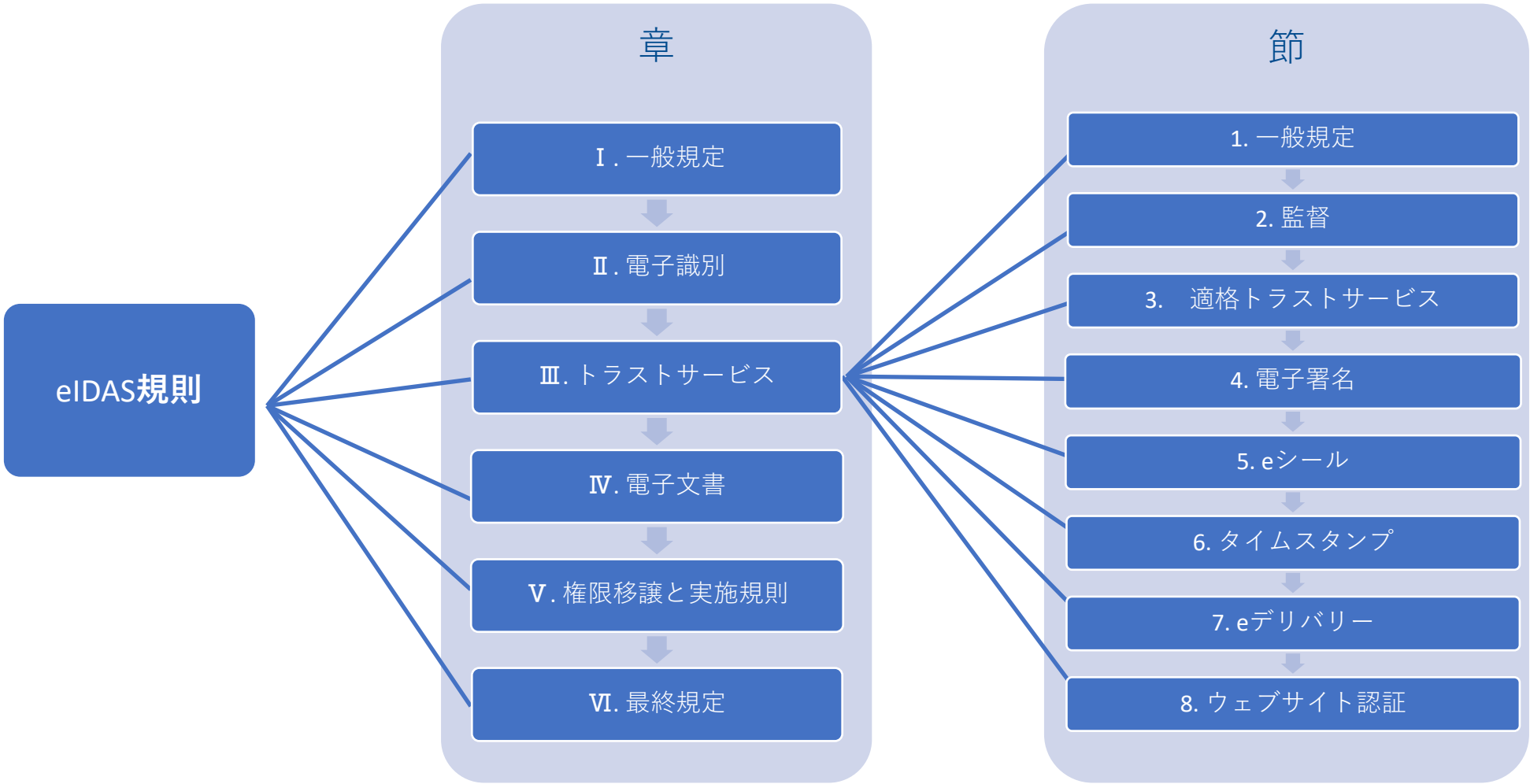
- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

eIDAS規則とは

- eIDAS（electronic Identification and Authentication Services）規則とは、2014年7月に成立し、2016年7月に発効されたEU圏内市場における電子商取引のための電子識別およびトラストサービスに関する規則。

- eIDAS 規則の枠組みの中でトラストサービスが定義されており、それぞれ、法的有効性が定められている。
これらのトラストサービスを利用することで法的確実性を伴った電子取引を行うことができる。

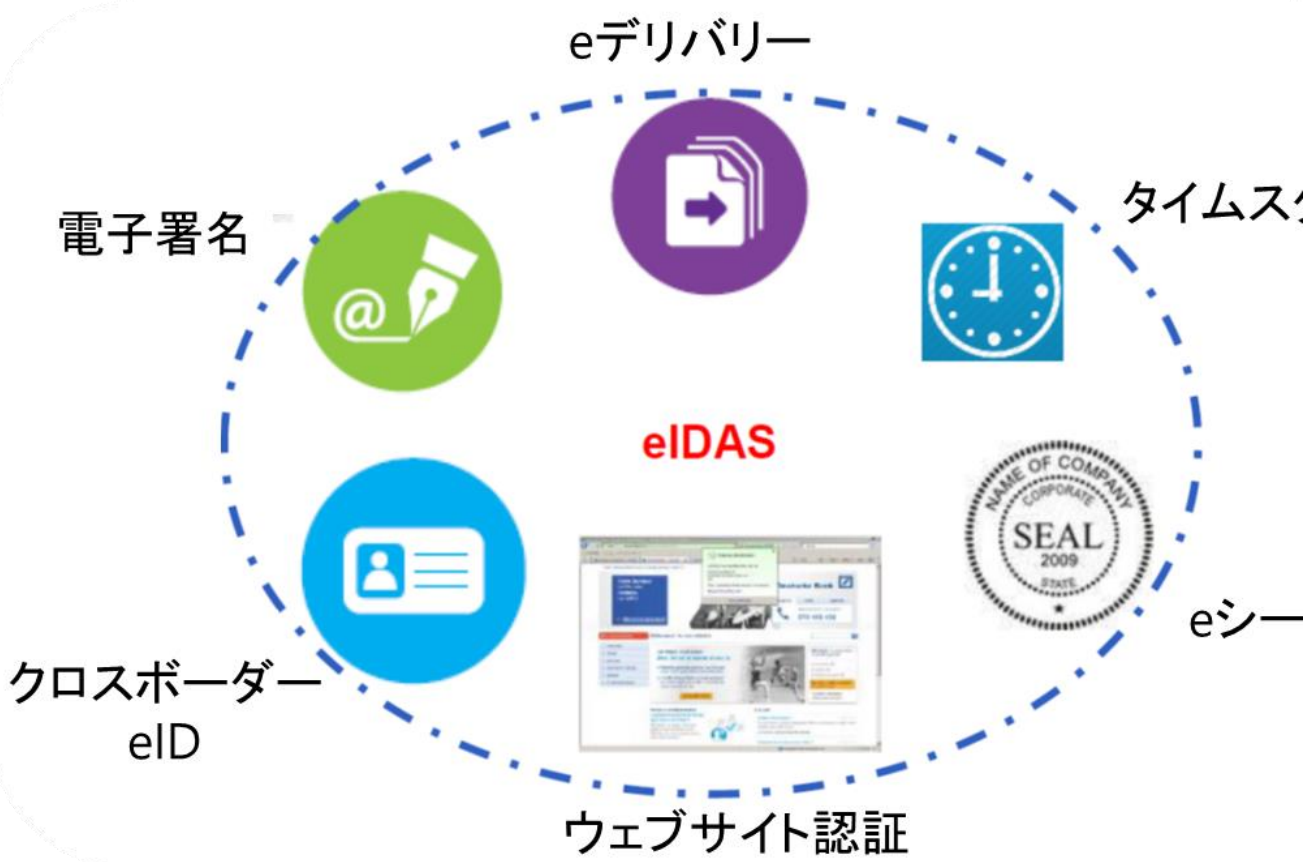
eIDAS規則の構成



eIDとトラストサービス

- eID➡ 電子的に本人確認を行う技術、電子認証（e.g. マイナンバーカード）

- トラストサービス➡ 電子署名／タイムスタンプ等の電子文書／電子取引における信頼性を保証するサービス。　通常は報酬の為に提供される電子サービスをいう：
  a. 電子署名、eシール、又はタイムスタンプの生成、検証、照合又は、eデリバリーサービス及びこれらのサービスに関連する証明書の生成、検証、照合；または、
  b. ウェブサイト認証の為の証明書の生成、検証、照合；または、
  c. これらのサービスに関連する電子署名、シール又は証明書の保存

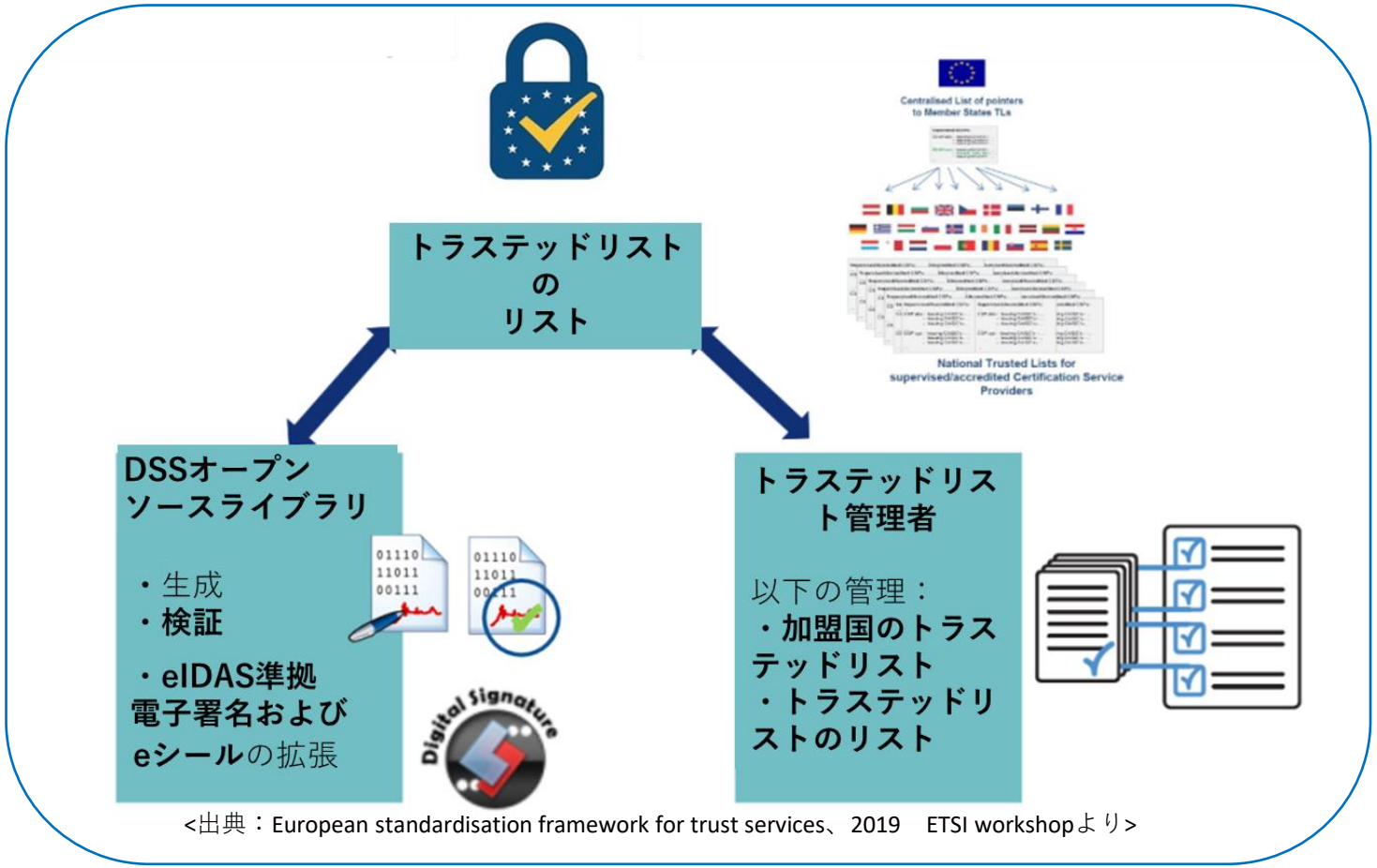


＜出典：eIDAS Regulation in the context of Cybersecurity: https://www.eema.org/wp-content/uploads/entschew-fiedler.pdf

トラストサービスの法的効力

トラストサービス	説明	法的効力
電子署名	自然人が電磁的に記録された情報について、その自然人が作成したことを示すもの。	手書きの署名と同等
eシール	文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの。	データの完全性と起源と正確性の推定
タイムスタンプ	電子データが、ある時刻に存在していたことその時刻以降に改ざんされていないことを示すもの。	時刻の正確性とデータの完全性の推定
eデリバリー	データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの。	送受信者の識別、データの完全性、送受信時刻の正確性の推定
ウェブサイト認証	ウェブサイトが真正で正当な主体により管理されていることが保証できることを示すもの。	ウェブサイトとその管理主体の認証結果の正確性
電子署名、eシール及び証明書の保存	–	電子署名、eシール及び電子署名の技術的有効期限の延長
電子署名、eシール及びウェブサイト認証の検証	–	検証結果の正確性

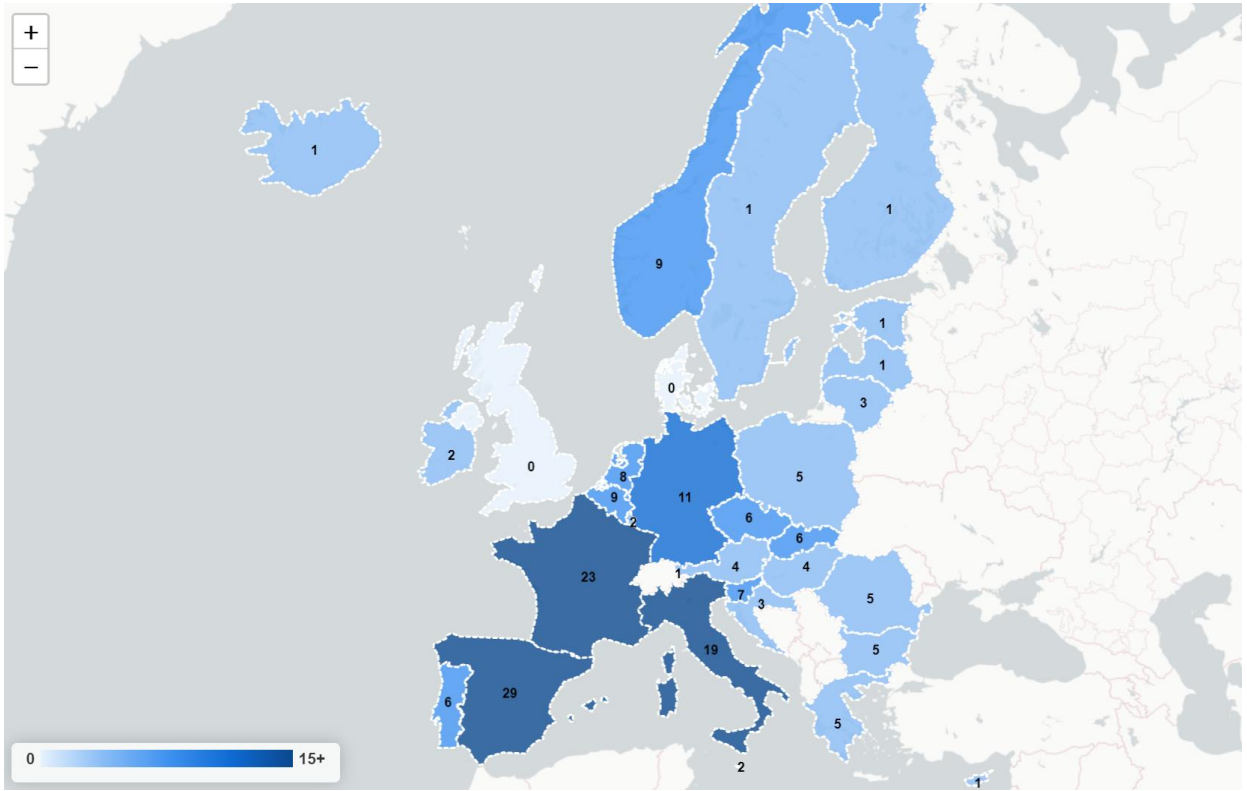
トラステッドリストの構造

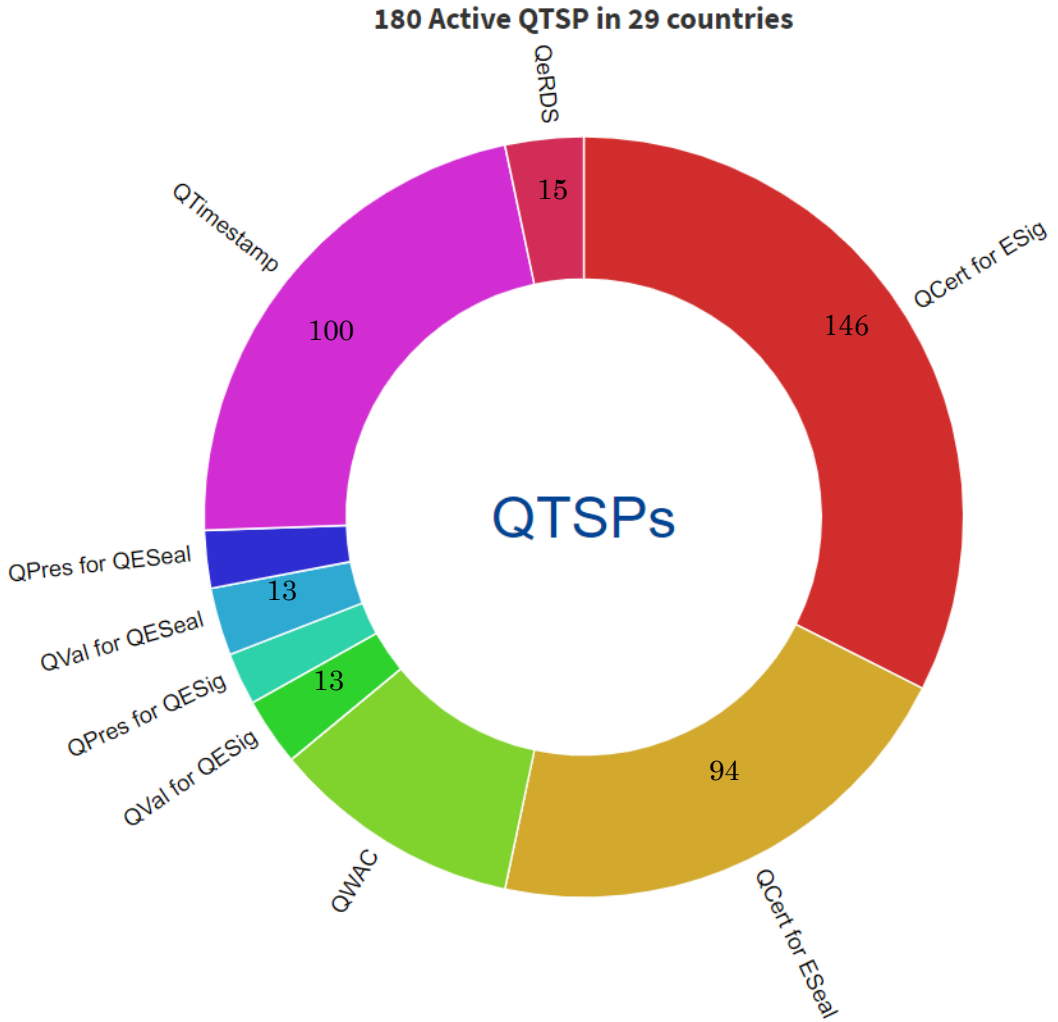


<出典：European standardisation framework for trust services、2019　ETSI workshopより>

統計データ

- 29加盟国、180のQTSP





目次

- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

FutureTrust Project

- FutureTrustは、Horizon 2020の予算で2016年6月１日から2019年8月31日まで実施されたプロジェクト
  - eIDAS規則 の実用的な実装をサポートし、世界中で法的効力に裏付けられた電子取引を実現するために、ヨーロッパ以外で、信頼できるeID及びトラストサービスを普及することが目的。

  - 以下によってeIDASのエコシステムを拡張する

①オープンソースコンポーネントの開発

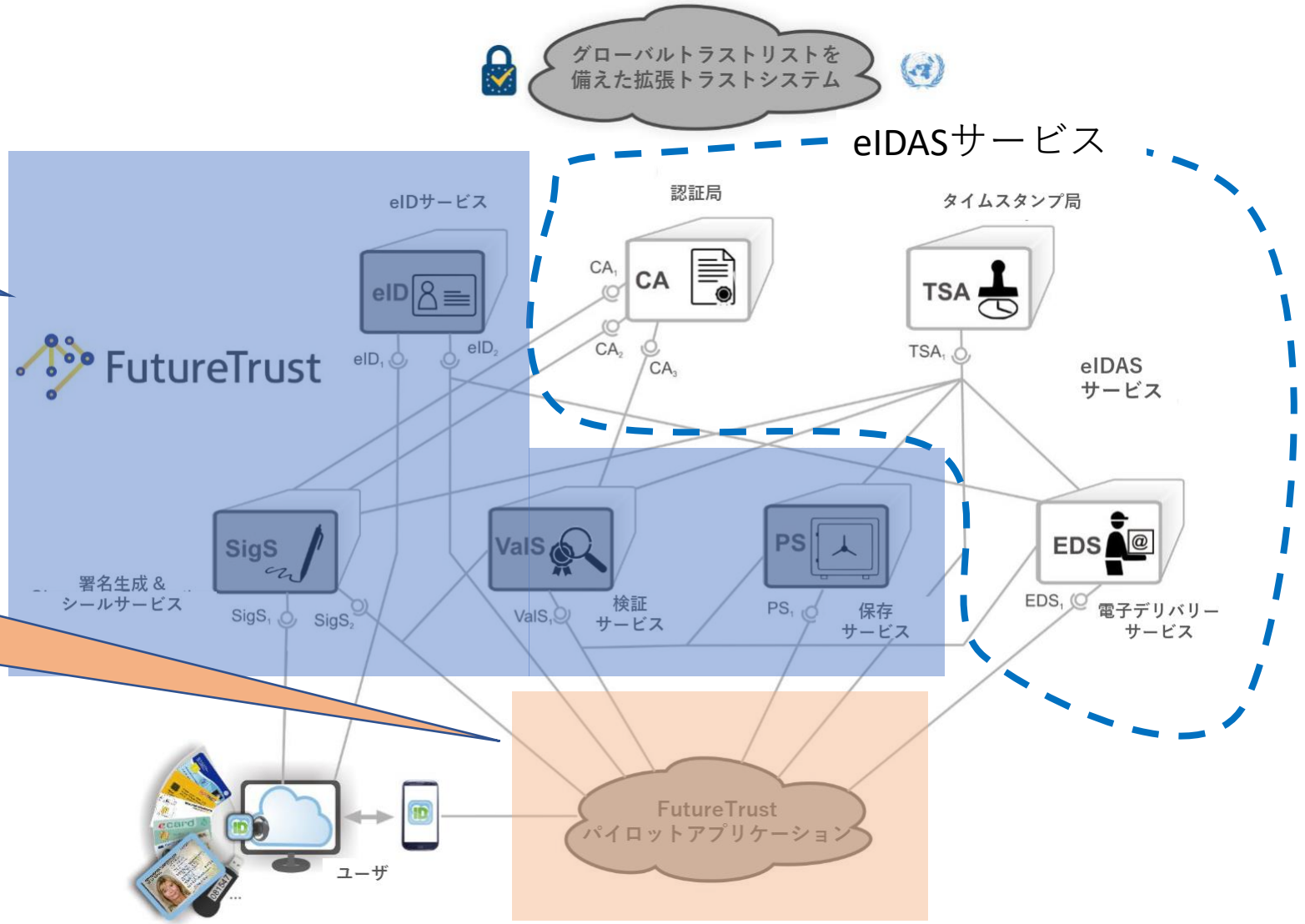
②パイロットアプリケーション

③GTSL(グローバルトラストサービスステータスリスト)の設計

FutureTrust Project

①オープンソースコンポーネントの開発

②パイロットアプリケーション



FutureTrustアーキテクチャプランと成果
＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverablesより＞

GTSLによるeIDASの拡張

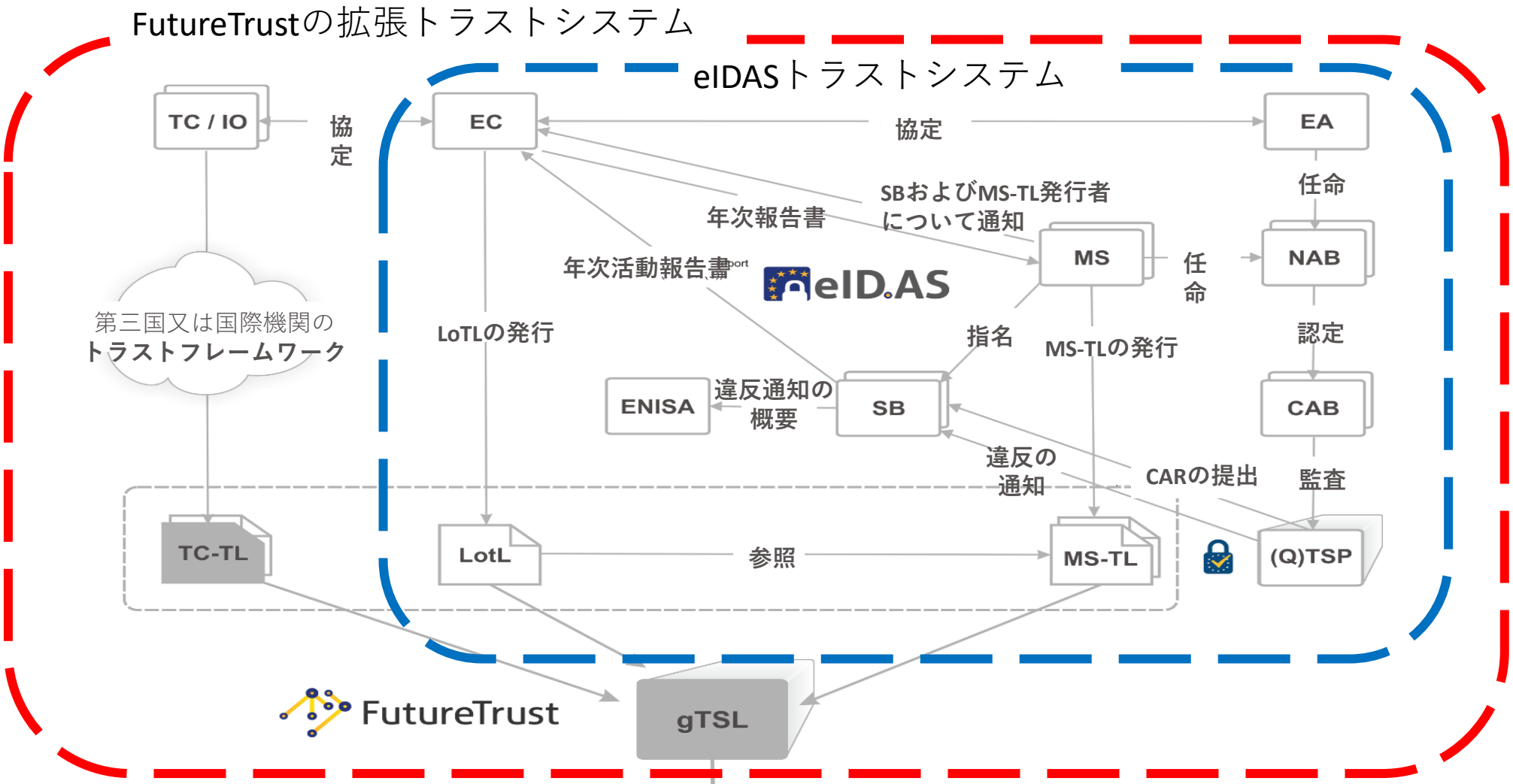


図　GTSLによるeIDASの拡張

＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverables より変更＞

eIDAS規則とFutureTrust Project及びUNCITRALの関係性

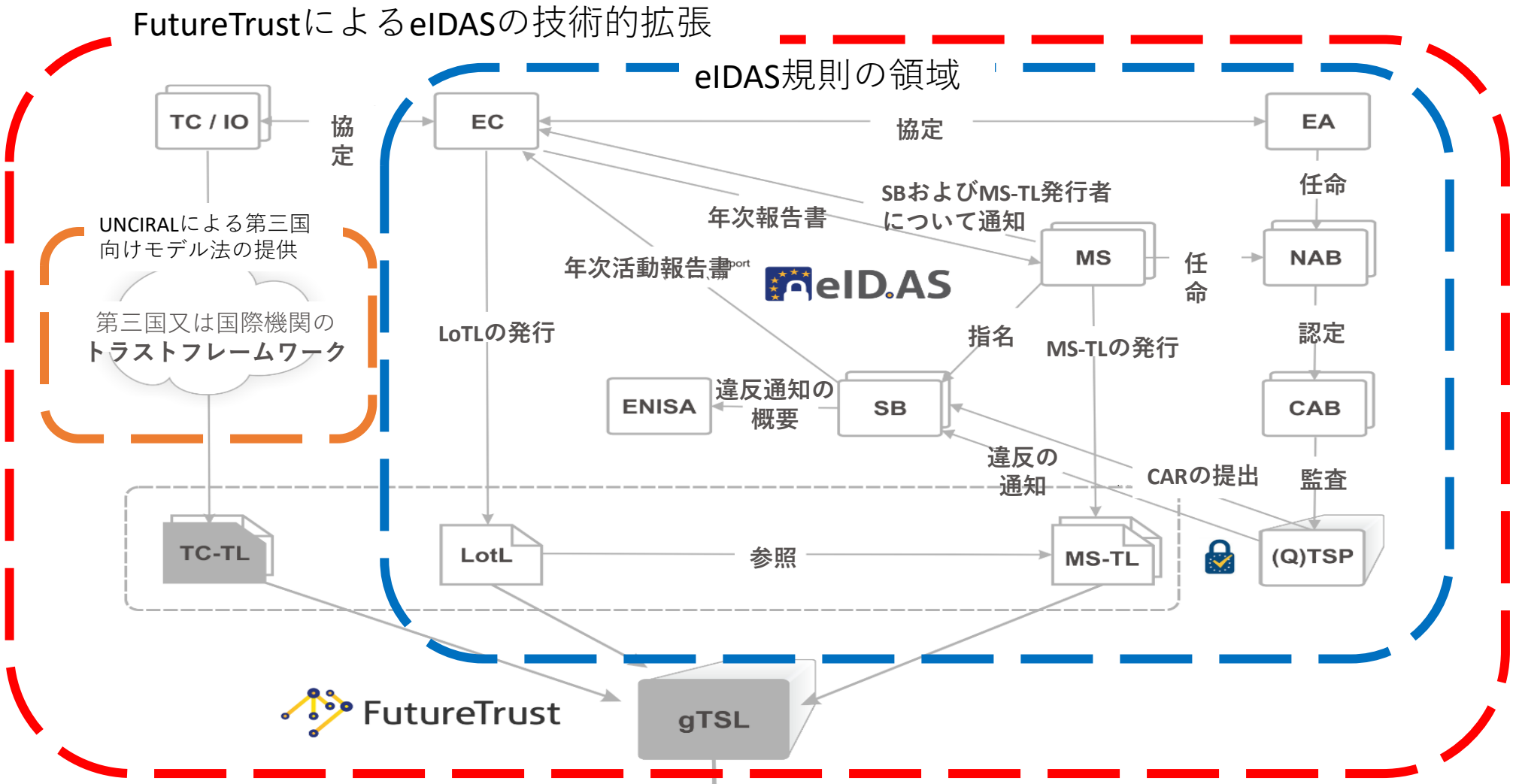


図　GTSLによるeIDASの拡張

＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverables より変更＞

目次

- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

トラストマークフレームワークの概念図

トラストマーク及びトラストマークフレームワークは、米国のNSTIC(National Strategy for Trusted Identity in Cyberspace)、サイバー空間における信頼できるアイデンティティに関する国家戦略)のパイロットプロジェクトの一つとして、ジョージア工科大学において2013年から2016年にかけて検討／開発された。

トラストマークフレームワークとは、多様なトラストフレームワークをモジュール化し、再利用可能なコンポーネントとして扱うフレームワークである。

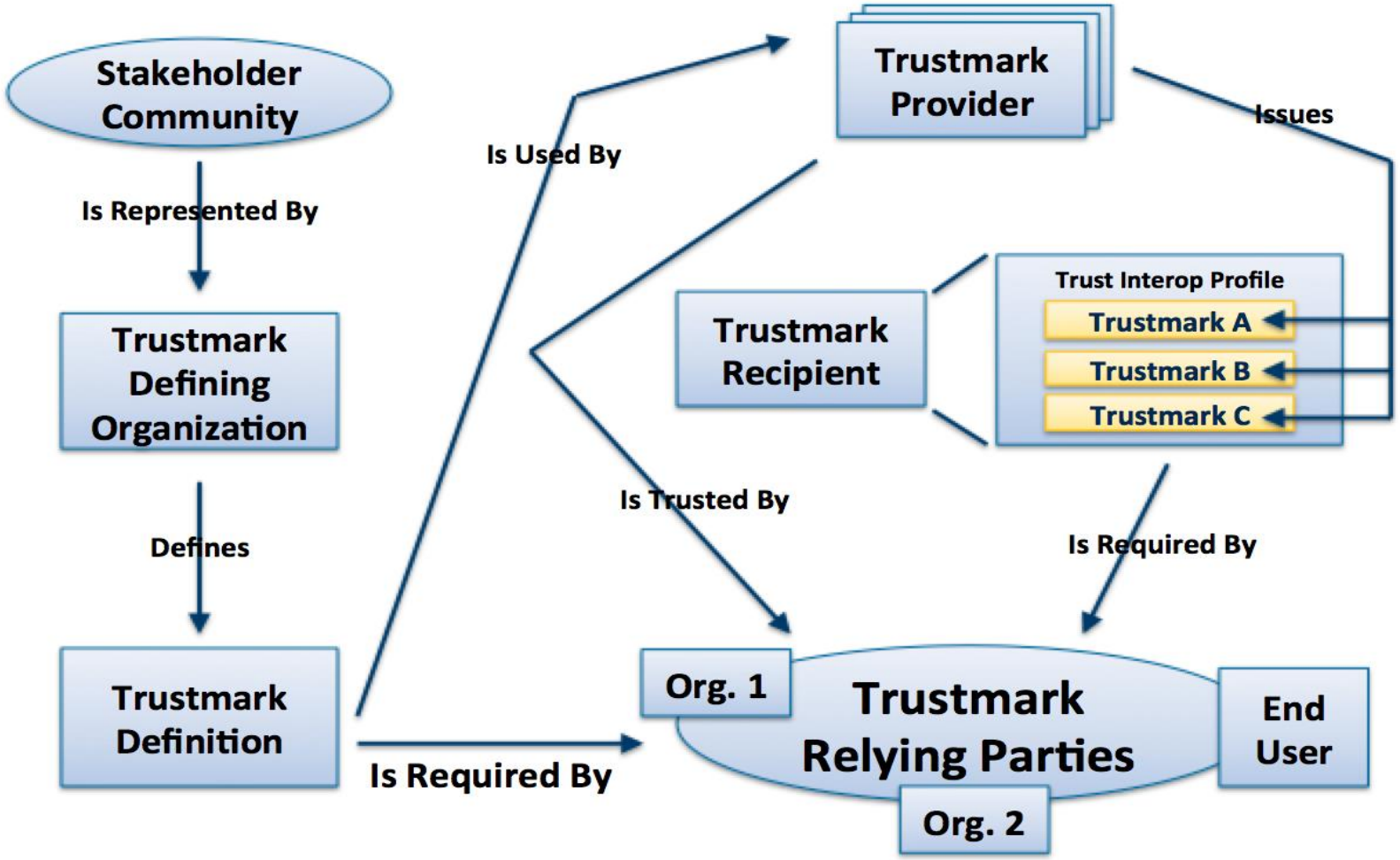


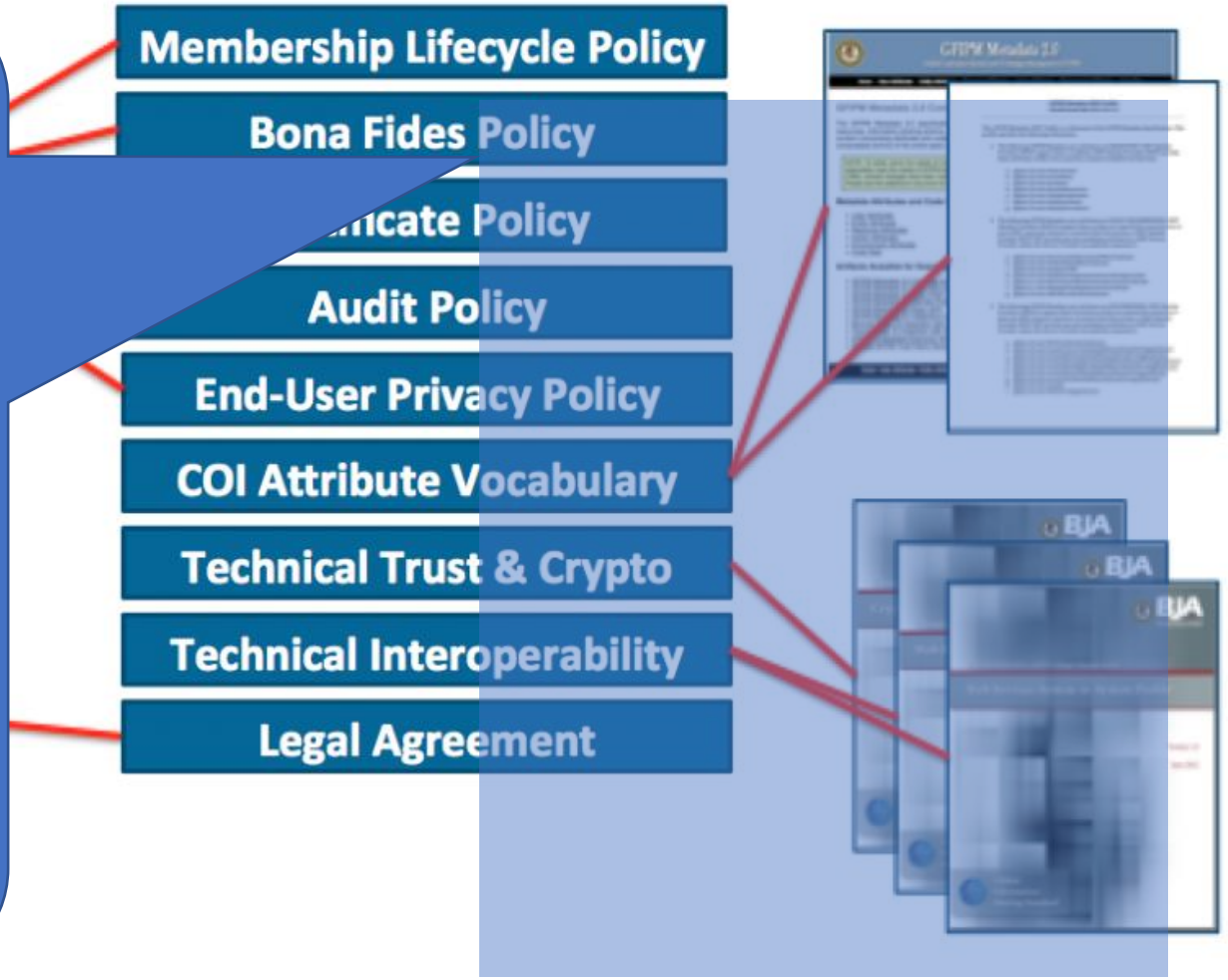
図７　トラストマークフレームワークの概念図
（出典： TRUSTMARK FRAMEWORK TECHNICAL SPECIFICATIONより）

NIEFにおけるトラストマークの適用例

①要件一つ一つをトラストマークとして定義し、コンポーネント化

②第三者機関（Trust Mark Provider）が各要件の適合性を評価し、トラストマーク（署名付きXMLオブジェクト）を発行

③依拠当事者はトラストマークを検証し、トラストマーク受領者を信頼する



トラストマークとPKIの類似性

Trustmark Framework Concept	Analogous Concept from PKI
Trustmark	Certificate
Trustmark Provider	Certificate Authority
Trustmark Recipient	Subscriber
Trustmark Relying Party	Certificate Relying Party / Audience
Trustmark Policy	Certificate Policy
Trustmark Recipient Agreement	Subscriber Agreement
Trustmark Relying Party Agreement	Certificate Relying Party Agreement
Trustmark Defining Organization	N/A
Trustmark Definition	N/A
Trust Interoperability Profile	List of Trusted Certificate Authorities
Trustmark Framework Technical Spec	X.509 Specification

トラストマーク、トラストマークフレームの位置付け

- トラストマークフレームワークはeIDAS規則を含むあらゆるトラストフレームワークをモジュール化し、包含することができる。
- トラストフレームワーク間をつなぐためのフレームワークがトラストマークフレームワークである。

トラストマーク、トラストマークフレームの位置付け

トラストマークプロバイダ

評価とトラストマークの発行

IdP（トラストマーク受領者）

IdPのトラストマークプロファイル

トラストマーク（eIDAS)

トラストマーク（FPKI)

・
・
・

モジュール化

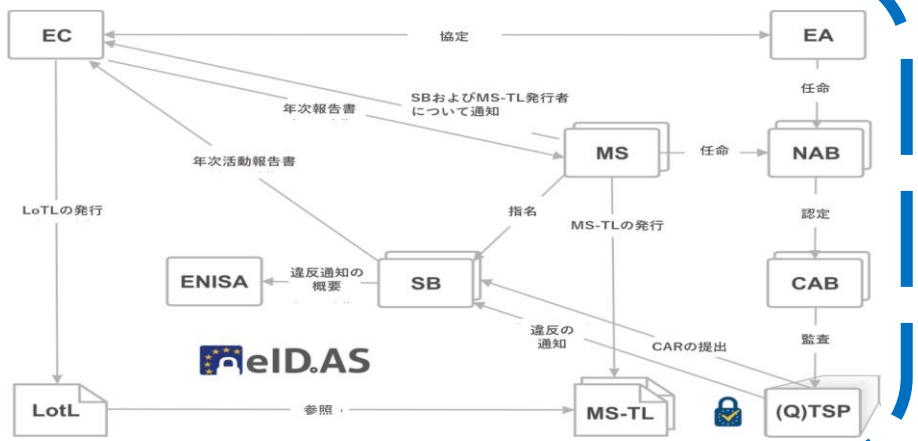
モジュール化

トラストマークに基づいて信頼

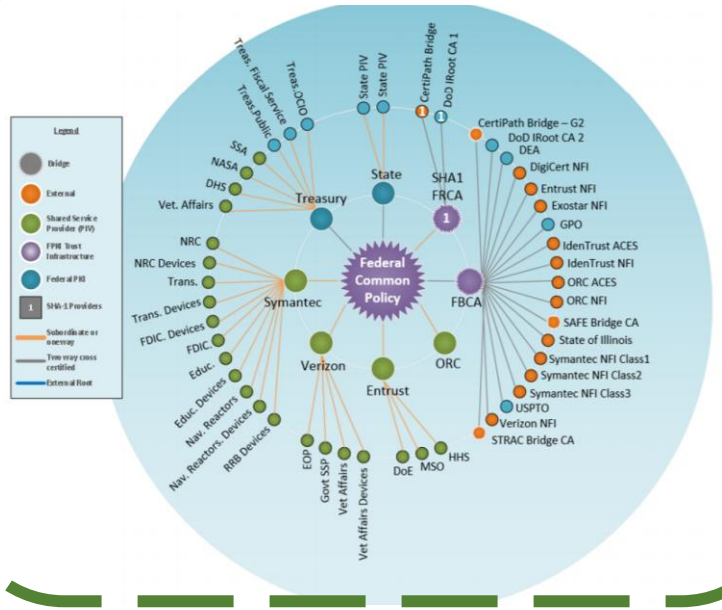
RP（依拠当事者）

IdP：Identity Provider

eIDASのフレームワーク



FPKIのフレームワーク

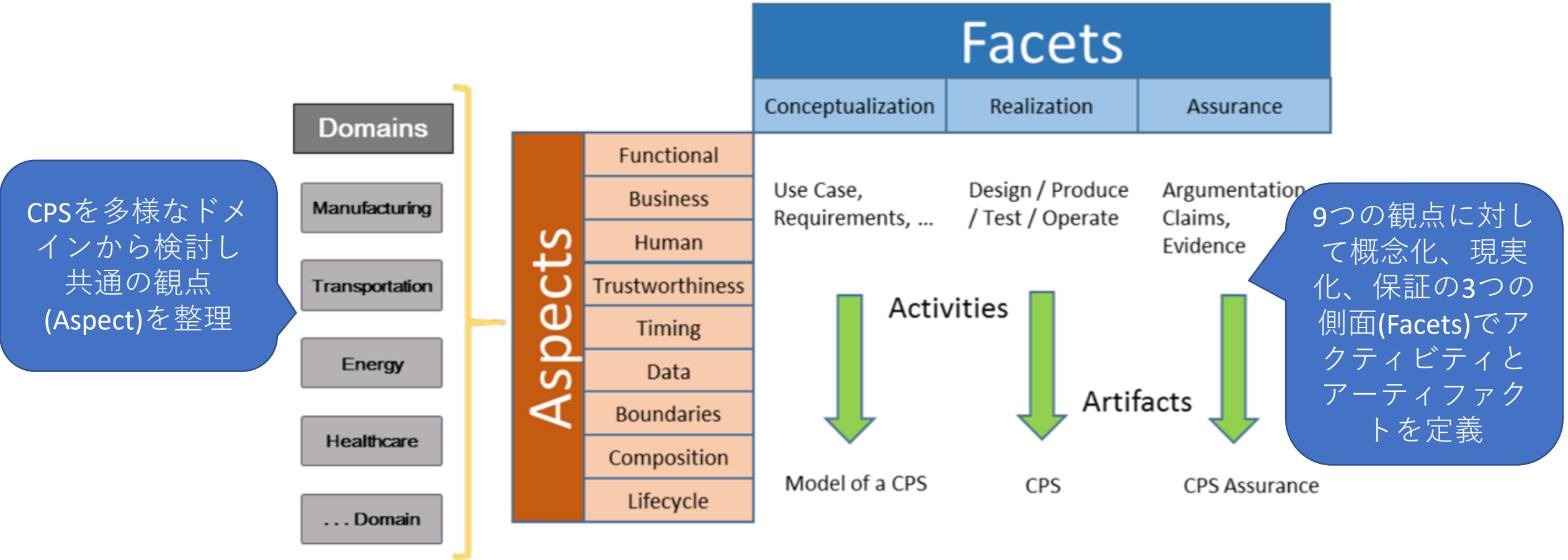


目次

- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

NIST CPS(Cyber Physical System)

- CPS分析の方法論と用語を定義することを主目的としたフレームワーク(NIST SP 1500-201)



観点に対する懸念事項

観点（Aspect)	懸念事項（Concerns）
Functional（機能）	Actuation, Communication, Controllability, Functionality, Manageability, Measurability, Monitorability, Performance, Physical, Physical context, Sensing, States, Uncertainty
Business（ビジネス）	Enterprise, Cost, Environment, Policy, Quality, Regulatory, Time to market, Utility
Human（人間）	Human factors, Usability
Trustworthiness（信頼）	Privacy, Reliability, Resilience, Safety, Security
Timing（タイミング）	Logical time, Synchronization, Time awareness, Time-interval and latency
Data（データ）	Data semantics, Identity, Operation on Data, Relationship between Data, Data velocity, Data volume
Boundaries（境界）	Behavioral, Networkability, Responsibility
Composition（構成）	Adaptability, Complexity, Constructivity, Discoverability
Lifecycle（ライフサイクル）	Deployability, Disposability, Engineerability, Maintainability, Operability, Procureability, Producibility

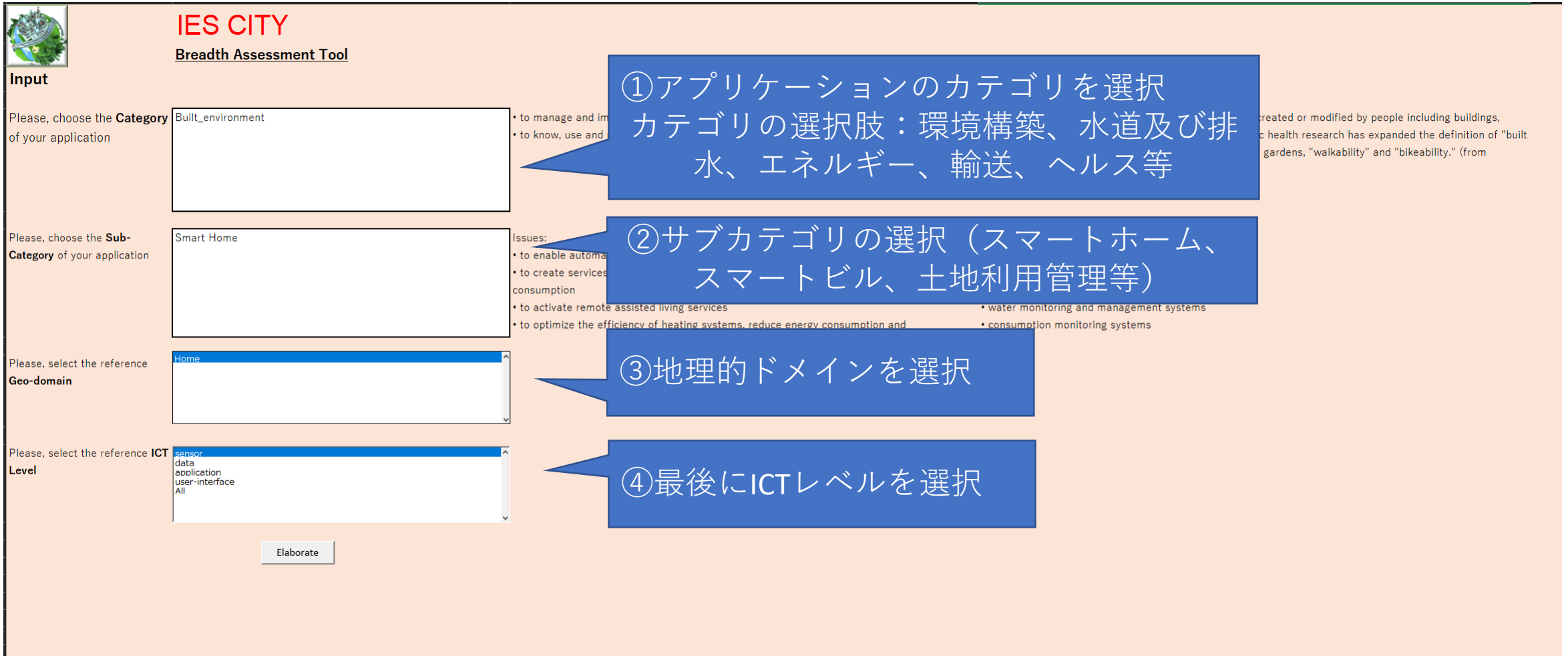
CPSの適用例：IEC-City(Internet of things Enabled Smart City)

- NISTが主体となって米国外のパートナーとスマートシティに関する既存のアーキテクチャを分析し、相互運用性の要点を特定

  ➡スマートシティ向けのコンセンサスフレームワークドキュメントを作成

- NIST CPSフレームワークをベースにスマートシティ向けアプリケーションベンダ、開発者、設計者及び管理者向けにCPSの要件を自動的にリスト化するツールを作成し、公開

IEC CITY Assessment tool



アウトプット

- スマートシティ向け
  アプリケーションが検討すべき
  懸念事項が自動でリスト化される

- 懸念事項に対応するスマートシティ
  における要件が自動で整理される

Aspect	Concern	Abstract requirements	Specific implementation requirements
Functional	Actuation	- capacity to analyze and elaborate received data and make decisions - Device control and configuration (Support of remote monitoring, control and configuration of devices)	- actuation capabilities - smart appliances - turning off electronics devices automatically - secutity device management - lights and thermostats management - motorized shades
	Communication	- capacity to exchange information internal to the system - Heterogeneous communication support (various kinds of wired or wireless technologies (ZigBee, Bluetooth, ···) and support for heterogeneous device related communication technologies) - sensors communication protocols (standard-based) - sensor network communication protocols (based on standard)	- Home management systems - Sensor network
	Functionality	- remote access - service management	- audio/video equipment
	Controllability	- device control and configuration (Support of remote monitoring, control and configuration of devices)	- Internet connection - remote control software
	Performance	- to provide feedback in time to act	- fast and reliable network - real-time systems
	Physical context	- to exactly identify location of people	- placement sensors - motion sensors
	Sensing	- to exactly identify location of people - persistent communications - to get data from home automation and energy systems - to elaborate data received from home automation and energy systems - Autonomic Services (enable automatic capture, communication and processing of data of things based on user configured by service providers or	- placement sensors - motion sensors - persistent communications technology - decision support systems
	Monitorability		

目次

- eIDAS規則とトラストサービス概要
- FutureTrust ProjectとUNCITRAL
- ジョージア工科大学におけるトラストマーク
- NIST CPS（Cyber Physical System）
- シンポジウムの関連プログラム

シンポジウムの関連プログラム

	講演　又は　セッション ＼ 関連テーマ	EU	米国	トラストサービス	サプライチェーン
第8回シンポジウム	【基調パネル】サイバーセキュリティにおけるトラストサービス		○	○	○
	【各国講演】ソフトウェア部品表　ソフトウェアコンポーネントの透明性に関するNTIAの取り組みの概要		○		○
	【INCS-CoEメンバー講演】　信頼できるインターネットへ向けて：頑強なトラスト・オンライン・サービスを構築するステップとは？	○	○	○	
	【講演】サイバーのサプライチェーン：不完全な世界におけるリスク管理		○		○
第9回シンポジウム	【基調パネル】トラストサービスの国際相互認証	○	○	○	
	【各国講演】米国　NIST		○		
	【各国講演】ETSI TC ESI	○		○	
	【セッション】D2-T1-S1　3極委員会：IoTと5G		○		○

EOF