電子記録応用基盤フォーラム（eRAP）の活動

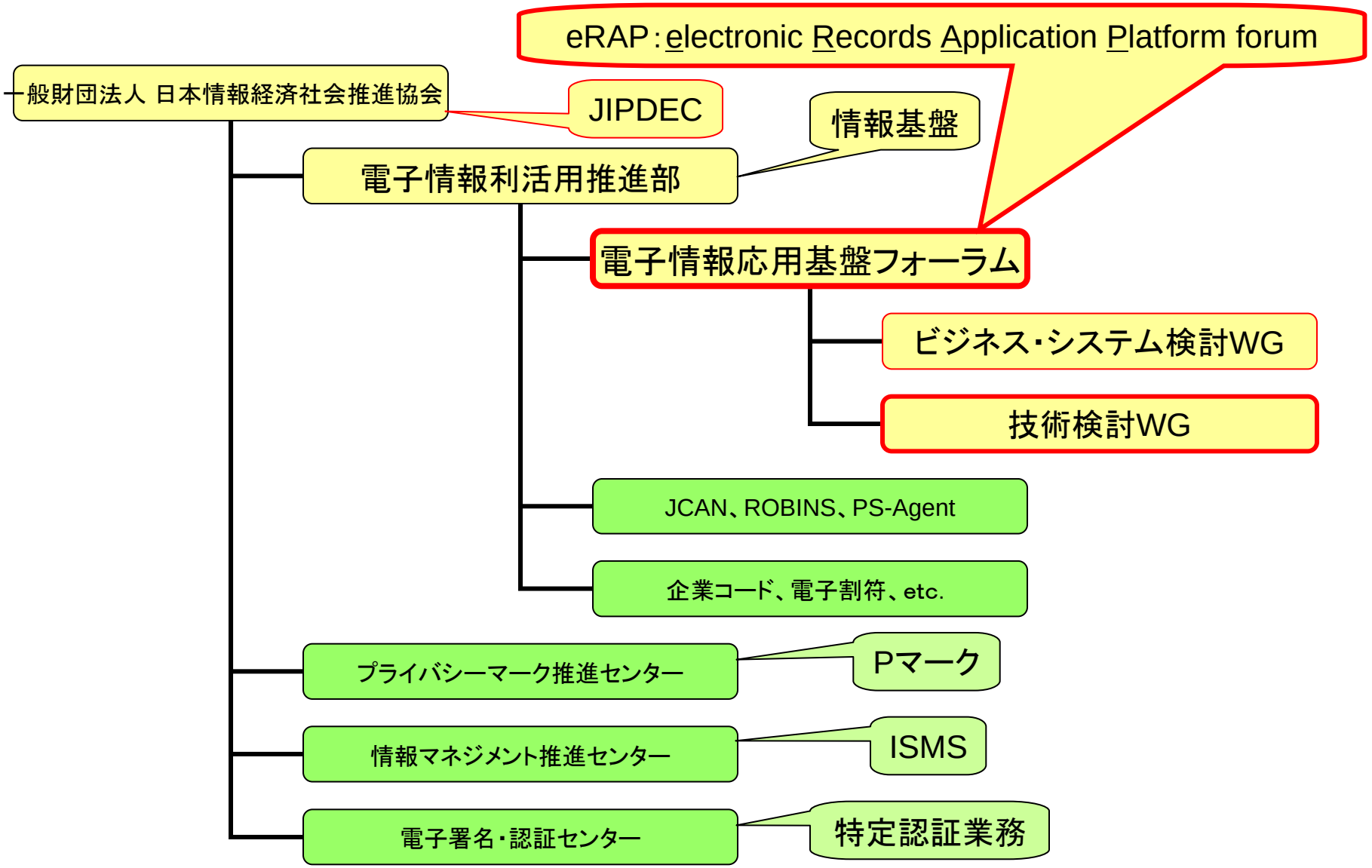
2012.12.13

eRAP 技術検討WG主査
宮崎一哉

講演内容

- eRAPの位置づけ、設立趣旨
- eRAP発足に至る経緯
- 主要成果
- eRAPの活動
- 信頼基盤の連携に向けて

eRAPの組織的な位置付け



eRAP設立趣旨

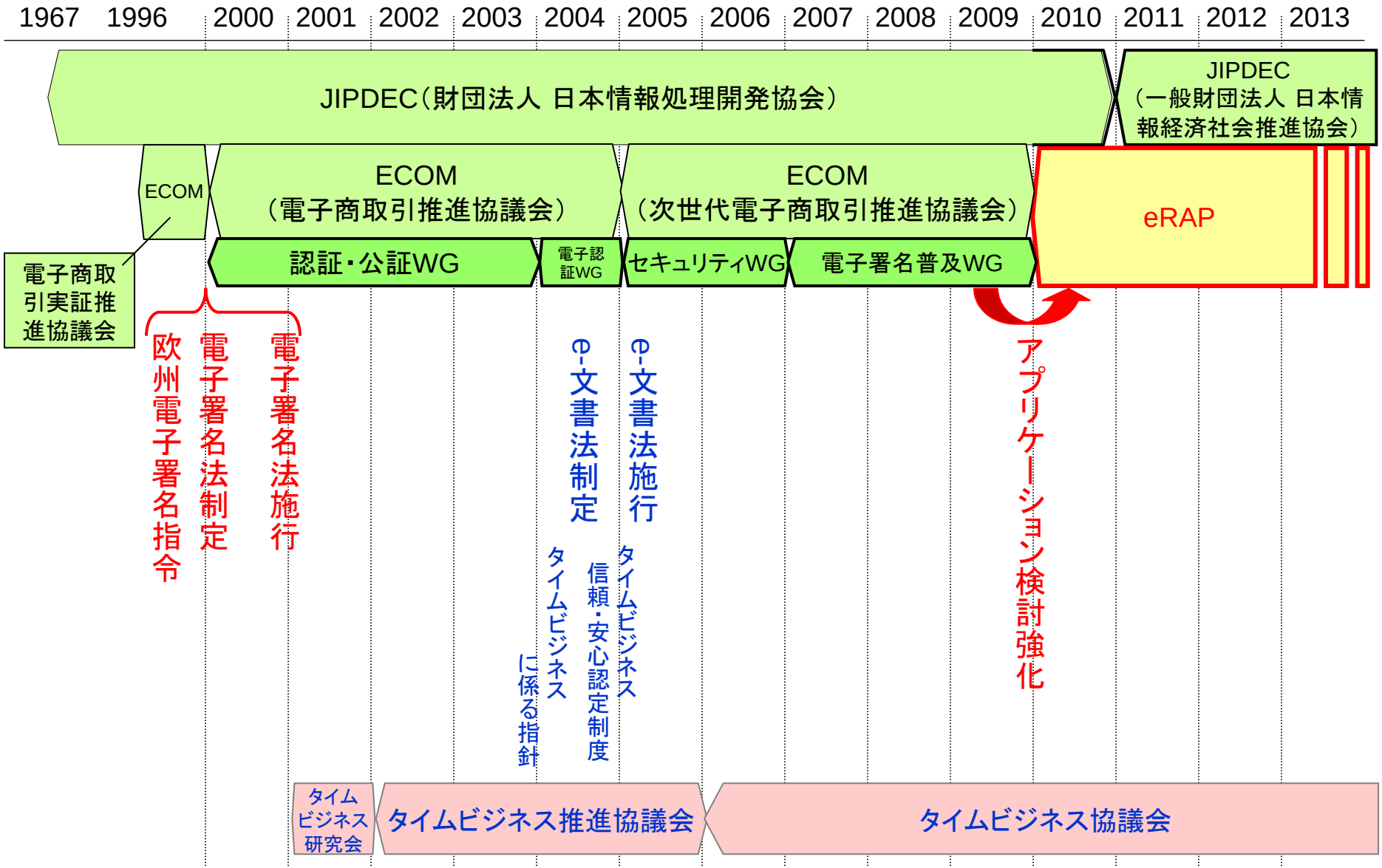
電子空間における情報の生成、利活用は様々な社会において急速に普及してきています。こうした中で、「情報の信頼性」、「安全な保管」、「安心できる取扱」を保証できる仕組みを確立することが喫緊の課題といわれています。また、日本の企業に対しても、企業活動の効率化・透明化、企業秘密の流出防止が求められており、企業の競争力強化を内外で図る上において、電子記録の活用、共有、保護のための電子記録マネジメントシステムの早急な確立が必要な状況にあります。

そこで、当協会では次世代電子商取引推進協議会（ECOM）安全安心グループの電子署名普及WG を中心に、セキュリティWG、個人情報保護WG の活動成果やネットワークを活用し、電子記録の利活用や応用を可能とする安全・安心な電子記録の応用基盤を確立して新たなビジネスを展開すべく、「電子記録応用基盤フォーラム」を設立します。

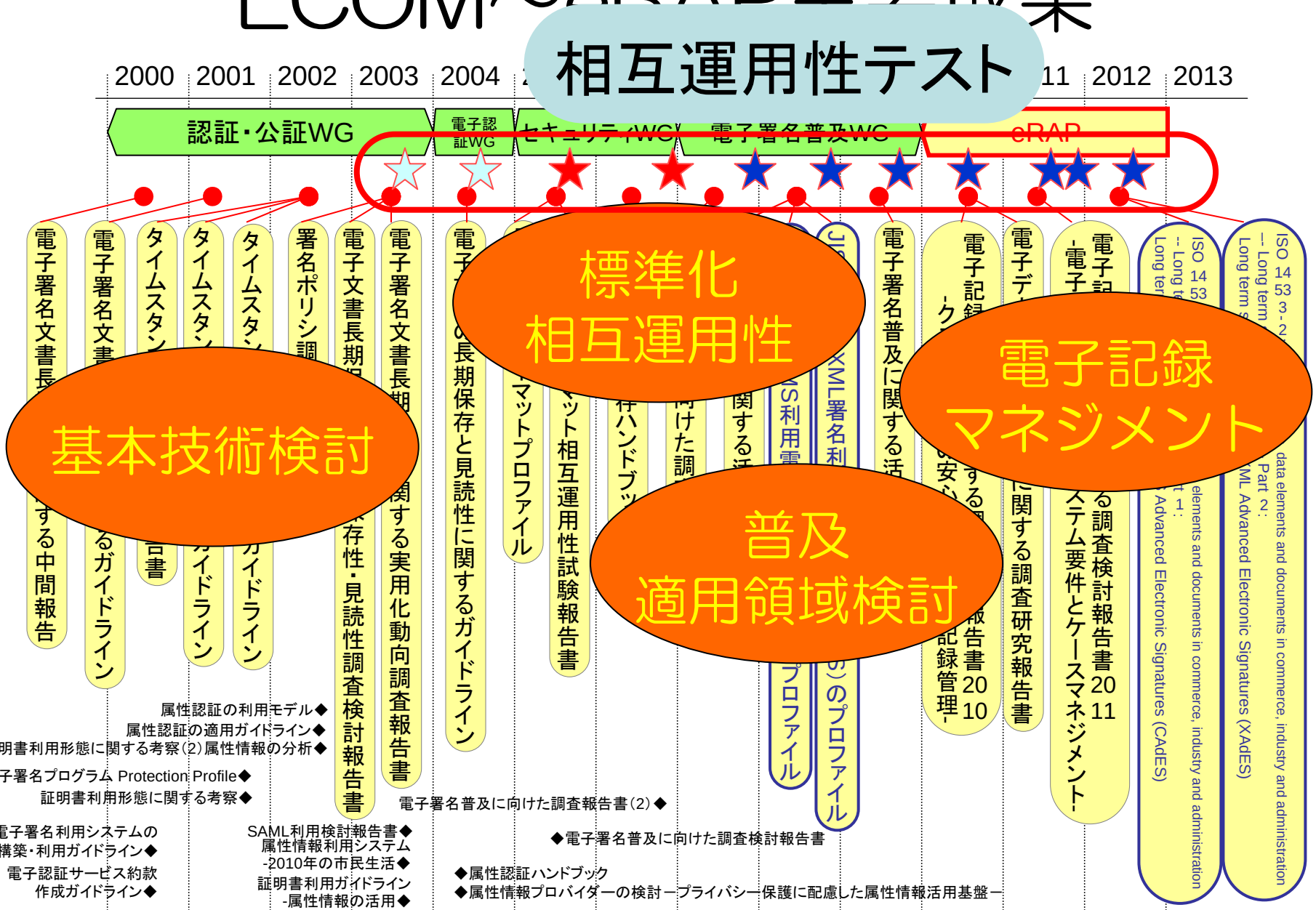
本フォーラムは、関係省庁との協調をとりながら、ユーザ企業、ベンダ企業およびサービスプロバイダが協力して進めるもので、他に先駆けて先進的な技術情報の収集と検討およびユーザニーズの収集と整理を行い、セキュアなクラウドファイリングのガイドラインや認証基準の作成を進めるなど、新しいビジネスの創出を意識した先導的な役割を果たします。

http://www.jipdec.or.jp/dupc/forum/erap/nyu.html

eRAP発足にいたる経緯



ECOM～eRAP主要成果



基本技術検討

- 電子署名（デジタル署名）の技術的課題
  ◆印鑑、手書き署名とのギャップ補完
  ⇒長期署名：ETSI標準に着目
  ⇒ETSI/ESI（欧州通信規格協会/電子署名基盤技術委員会）との関係
  ◆補完のためのキー要素
  ⇒タイムスタンプをTBFに先行して検討
  ◆署名の有効性や意味付けの定義
  ⇒署名ポリシ　検討途上

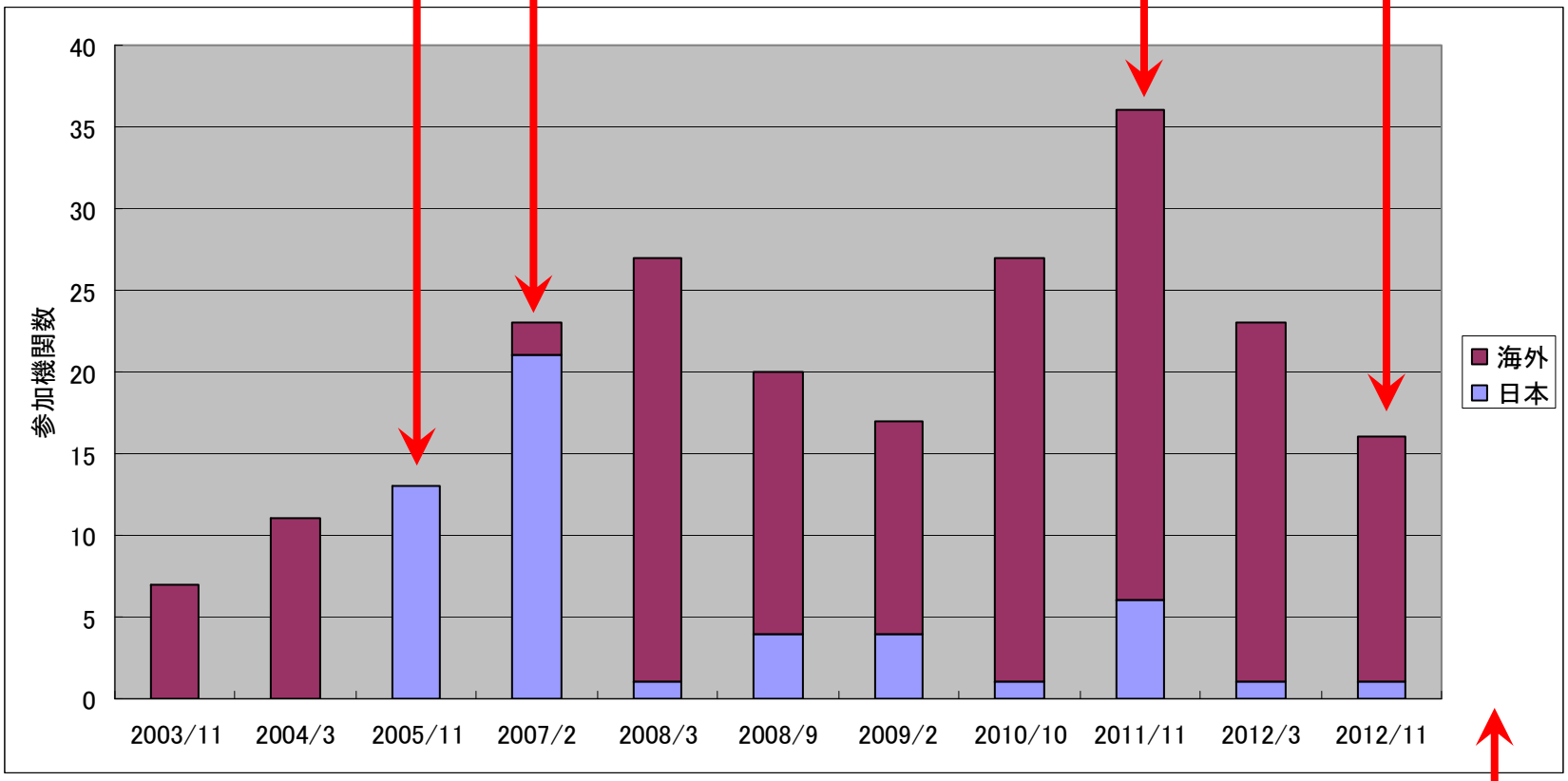
標準化、相互運用性

- 標準化
  ◆長期署名フォーマット（CAdES/XAdES）のECOMプロファイル[2005]
  ◆JIS化（JIS X 5092/5093）[2008]
  ⇒e-文書法の国税要件への具体的な対応方法
  ◆ISO化（ISO 14533-1/2）[2012]
  ⇒国内標準から国際標準へ
  ⇒JAHIS：医療分野のISOへ（ISO 17090-4）
  ◆「電子文書長期保存ハンドブック」[2006]では署名検証プロセスの標準仕様も検討
- 相互運用性テスト
  ⇒ECOMのリモートテストのノウハウをETSIに提供

相互運用性テスト

実施時期	主催	対象	形態	参加機関数(日本)
2003/11	ETSI	XAdES	face to face	7(0)
2004/3	ETSI	XAdES	face to face	11(0)
2005/11	ECOM	CAdES/XAdES	remote	13(13)
2007/2	ECOM	CAdES/XAdES	remote	21(19)
2008/3	ETSI	XAdES	remote	27(1)
2008/9	ETSI	XAdES	remote	20(4)
2009/2	ETSI	CAdES/XAdES	remote	17(4)
2010/10	ETSI	CAdES/XAdES	remote	27(1)
2011/11	ETSI	PAdES	remote	36(6)
2012/3	ETSI	XAdES	remote	23(1)
2012/11	ETSI	ACiS	remote	16(1)

参加機関数の推移



CAdES, PAdES?

相互運用性テストの効用

- 標準仕様の曖昧性、不具合を発見
  ⇒標準へのフィードバック

- 各社実装の不具合確認
  ⇒標準への準拠性のアピール

  ⇒ユーザによる製品の選択指針

普及、適用領域検討

- 見読性、保存性を含めた長期保存
  - ファイルフォーマット、媒体、、
- 普及に向けた調査
  - 官民連携サービス基盤、文書管理、、

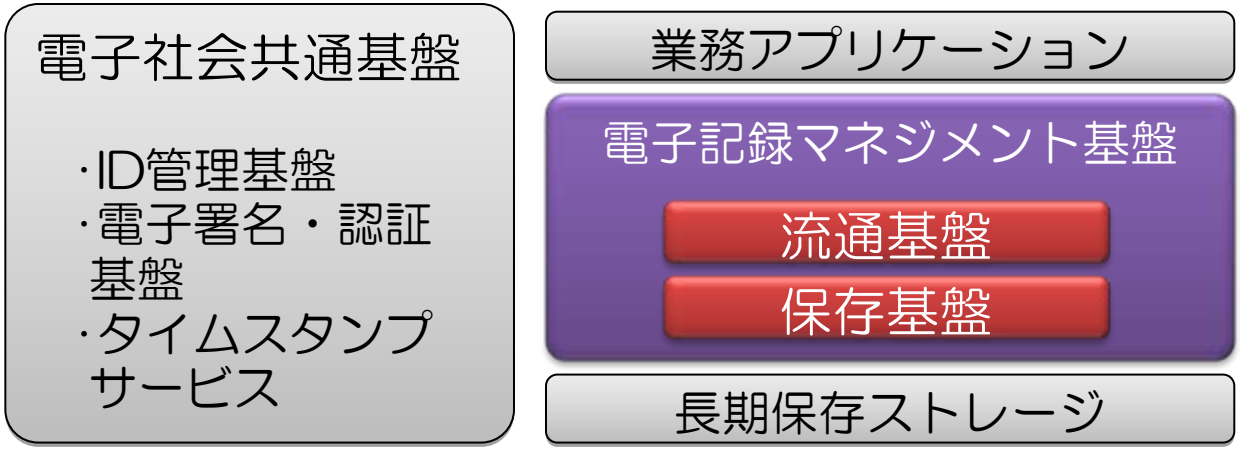
⇒eRAPにおける電子記録管理の検討へ

eRAPの活動

- 応用として電子記録管理を中心に据え、ビジネス創出を視野に入れた検討
  - 電子記録管理システムの100要件、成熟度モデル
  - ケース管理
  - パッケージ
- 電子署名関連活動の継続
  - 標準化
    - CAdES/XAdESプロファイルのISO化を達成
    - PAdESプロファイル標準化に着手
    - TBFの署名検証プロセスの標準化に協力
  - 将来像：クラウド/モバイル署名など

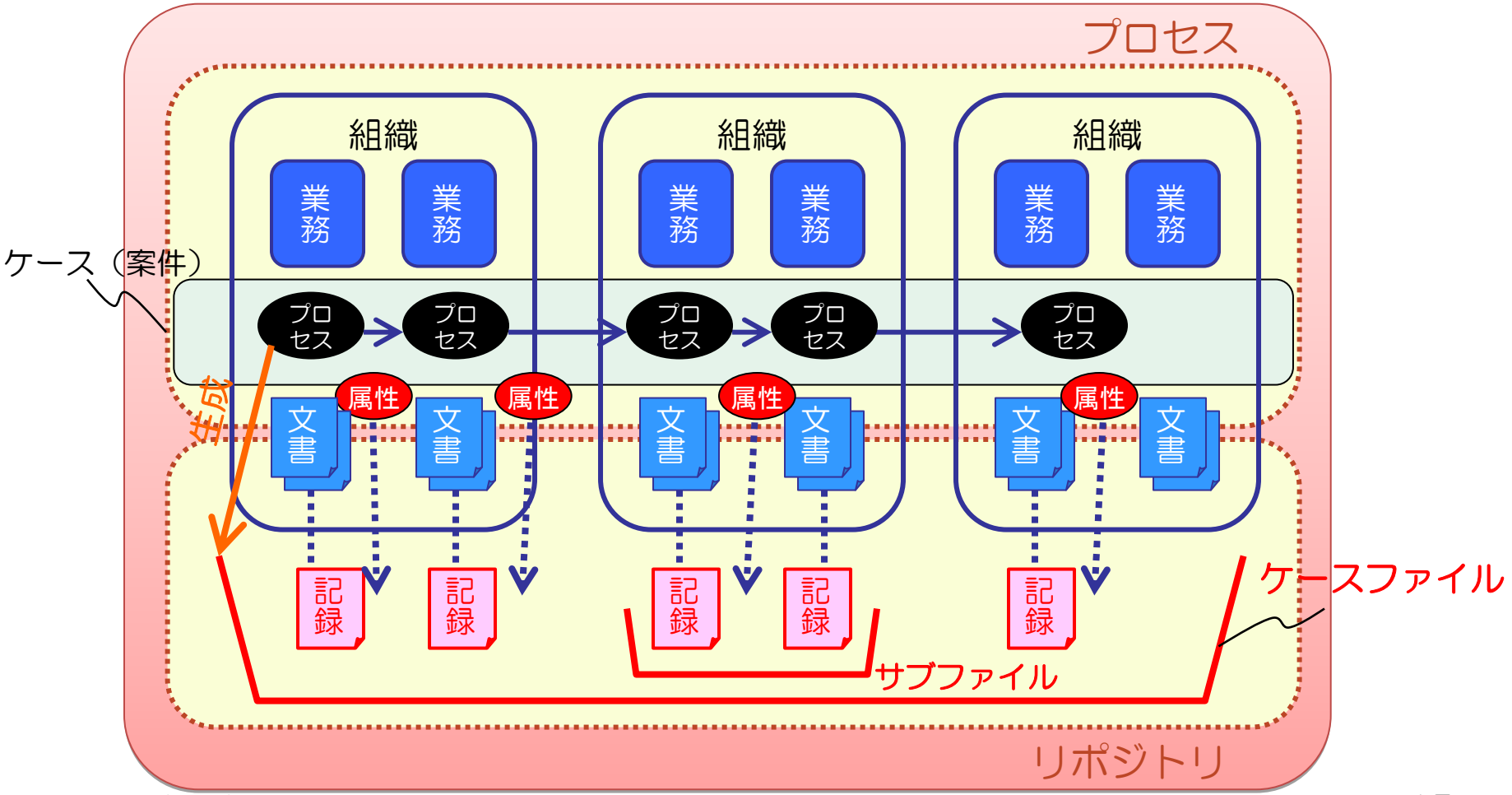
電子記録管理

- 記録
  - 文書の中でも特に外部に対する証拠として保存・管理するもの
- 電子記録マネジメント基盤
  - 電子的な記録の流通及び保存のための基盤



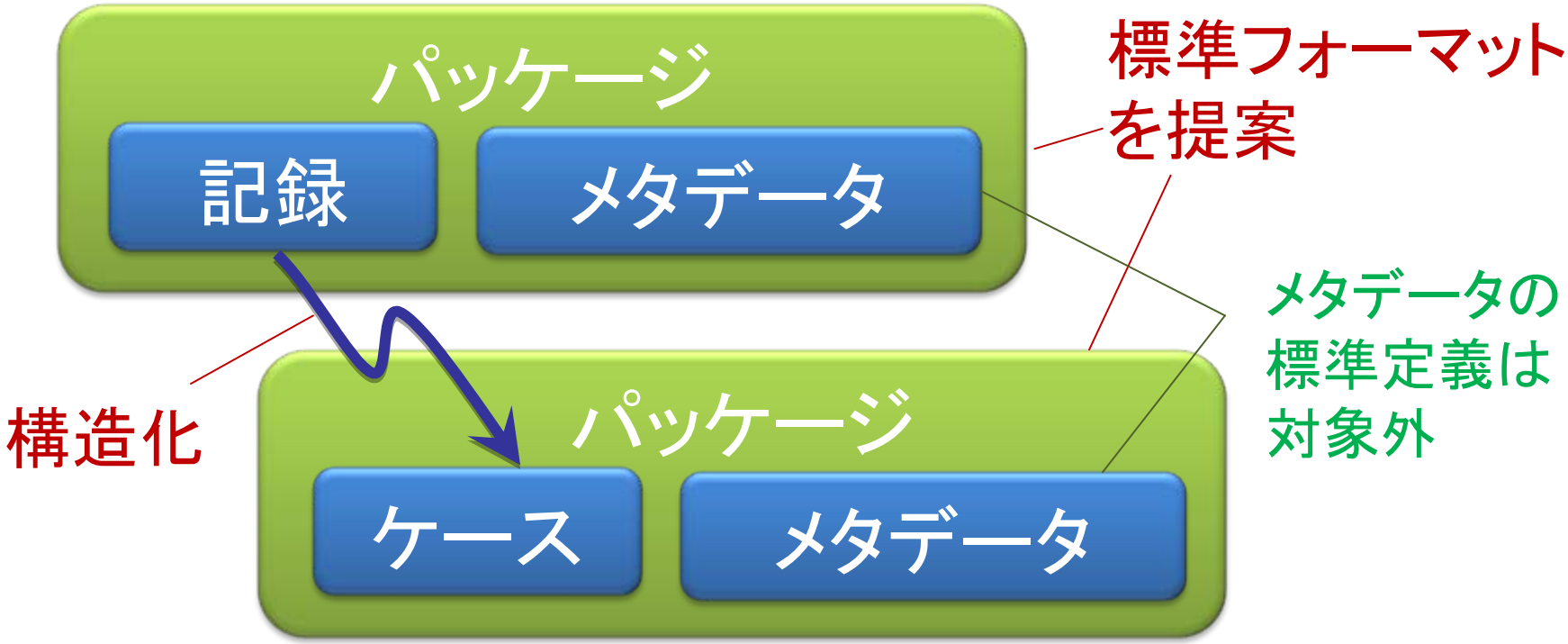
ケース管理

- 定型、非定型を問わず一連の業務に関する記録を収集し構造化して管理する。
  ⇒結果だけではなく過程も確認可能、説明責任、より有効な利活用

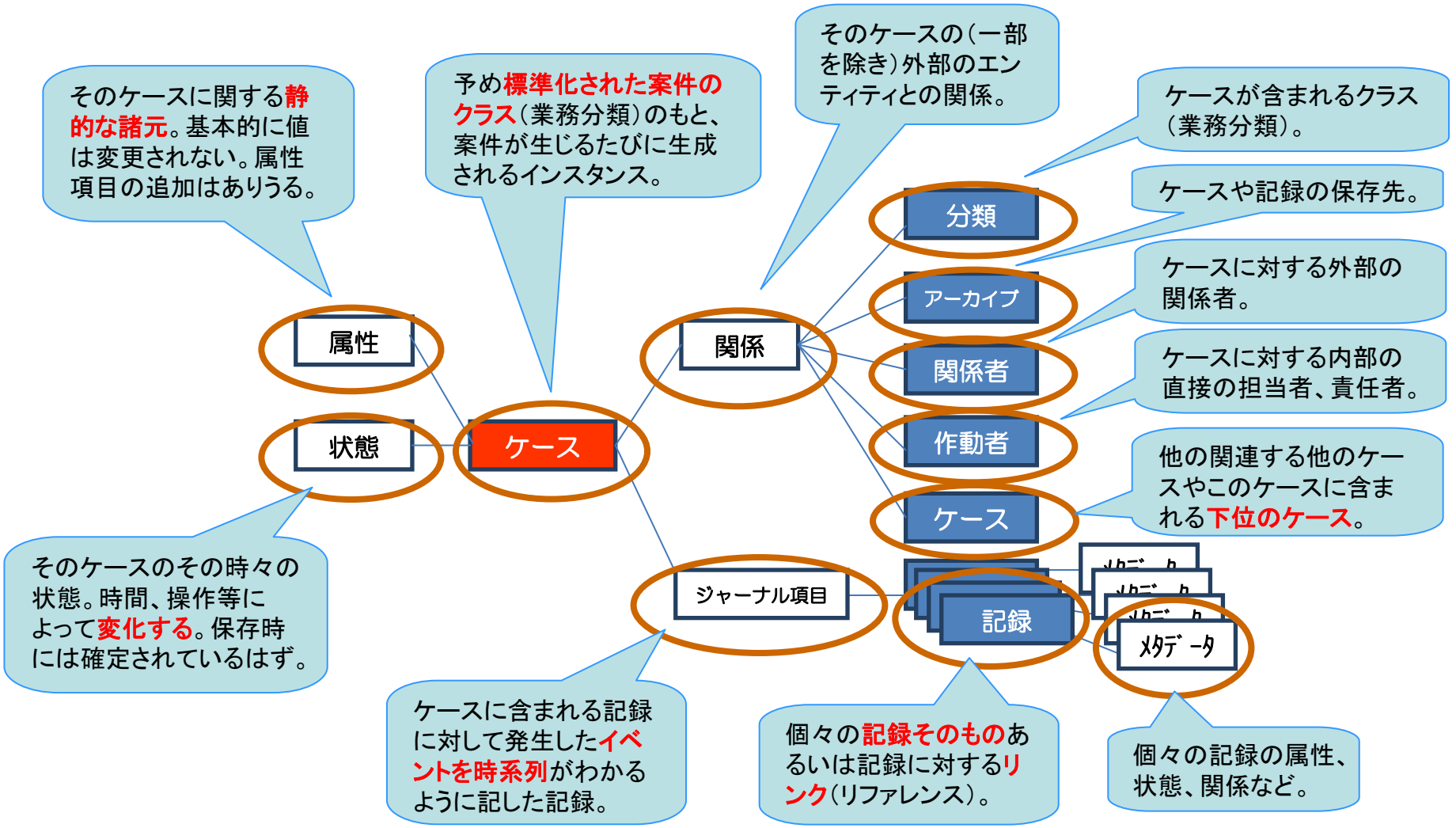


パッケージ

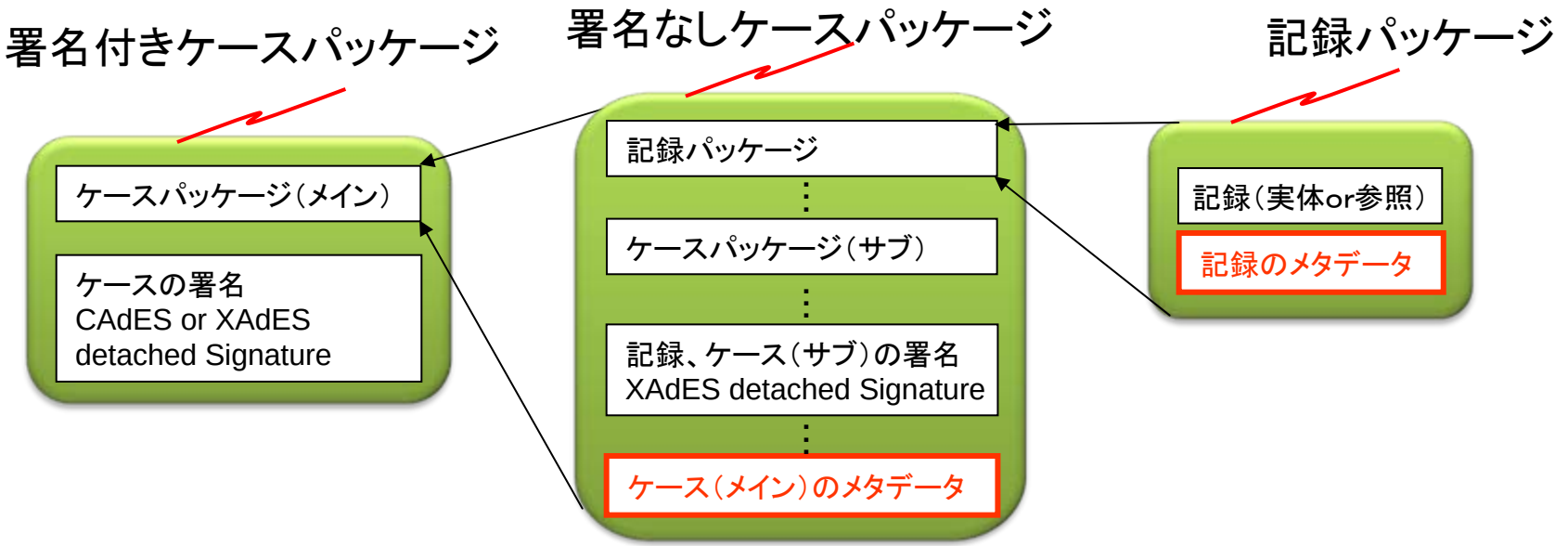
- メタデータを伴う電子的な「記録」と、それを構造化する「ケース」の標準的な交換形式。

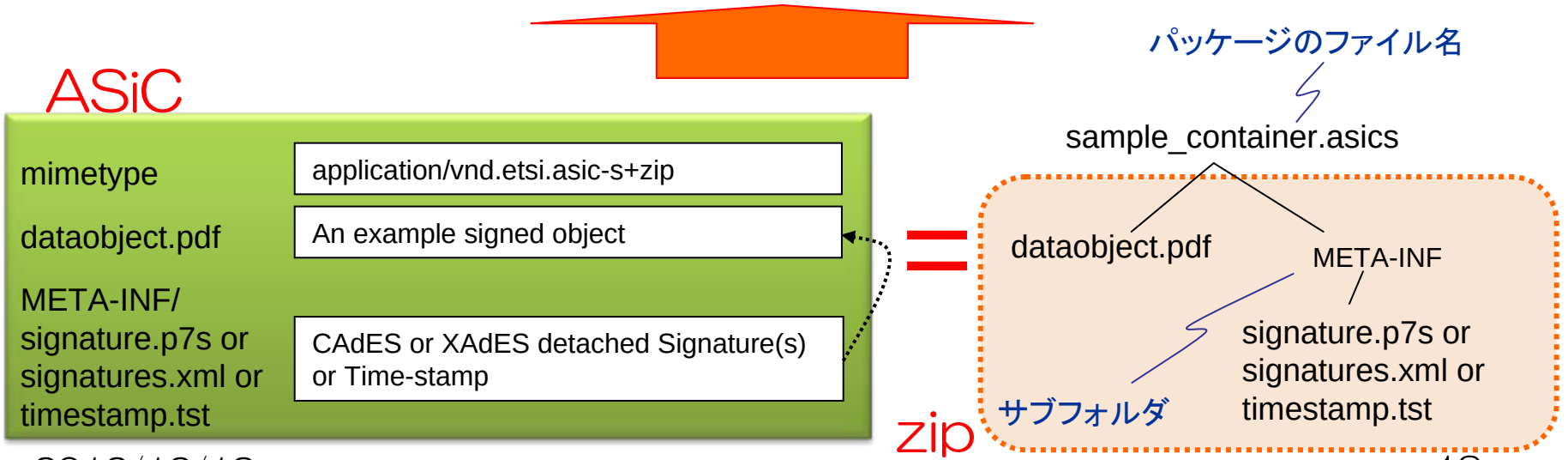


ケースのメタデータ例


そのケースに関する静的な諸元。基本的に値は変更されない。属性項目の追加はありうる。
予め標準化された案件のクラス（業務分類）のもと、案件が生じるたびに生成されるインスタンス。
そのケースの（一部を除き）外部のエンティティとの関係。
ケースが含まれるクラス（業務分類）。
ケースや記録の保存先。
ケースに対する外部の関係者。
ケースに対する内部の直接の担当者、責任者。
他の関連する他のケースやこのケースに含まれる下位のケース。
属性
状態
ケース
関係
ジャーナル項目
分類
アーカイブ
関係者
作動者
ケース
記録
メタデータ
そのケースのその時々の状態。時間、操作等によって変化する。保存時には確定されているはず。
ケースに含まれる記録に対して発生したイベントを時系列がわかるように記した記録。
個々の記録そのものあるいは記録に対するリンク（リファレンス）。
個々の記録の属性、状態、関係など。

パッケージ構造案


署名付きケースパッケージ
署名なしケースパッケージ
記録パッケージ
ケースパッケージ（メイン）
ケースの署名
CAdES or XAdES
detached Signature
記録パッケージ
ケースパッケージ（サブ）
記録、ケース（サブ）の署名
XAdES detached Signature
ケース（メイン）のメタデータ
記録（実体or参照）
記録のメタデータ


ASiC
mimetype
application/vnd.etsi.asic-s+zip
dataobject.pdf
An example signed object
META-INF/
signature.p7s or
signatures.xml or
timestamp.tst
CAdES or XAdES detached Signature(s)
or Time-stamp
zip
パッケージのファイル名
sample_container.asics
dataobject.pdf
META-INF
signature.p7s or
signatures.xml or
timestamp.tst
サブフォルダ

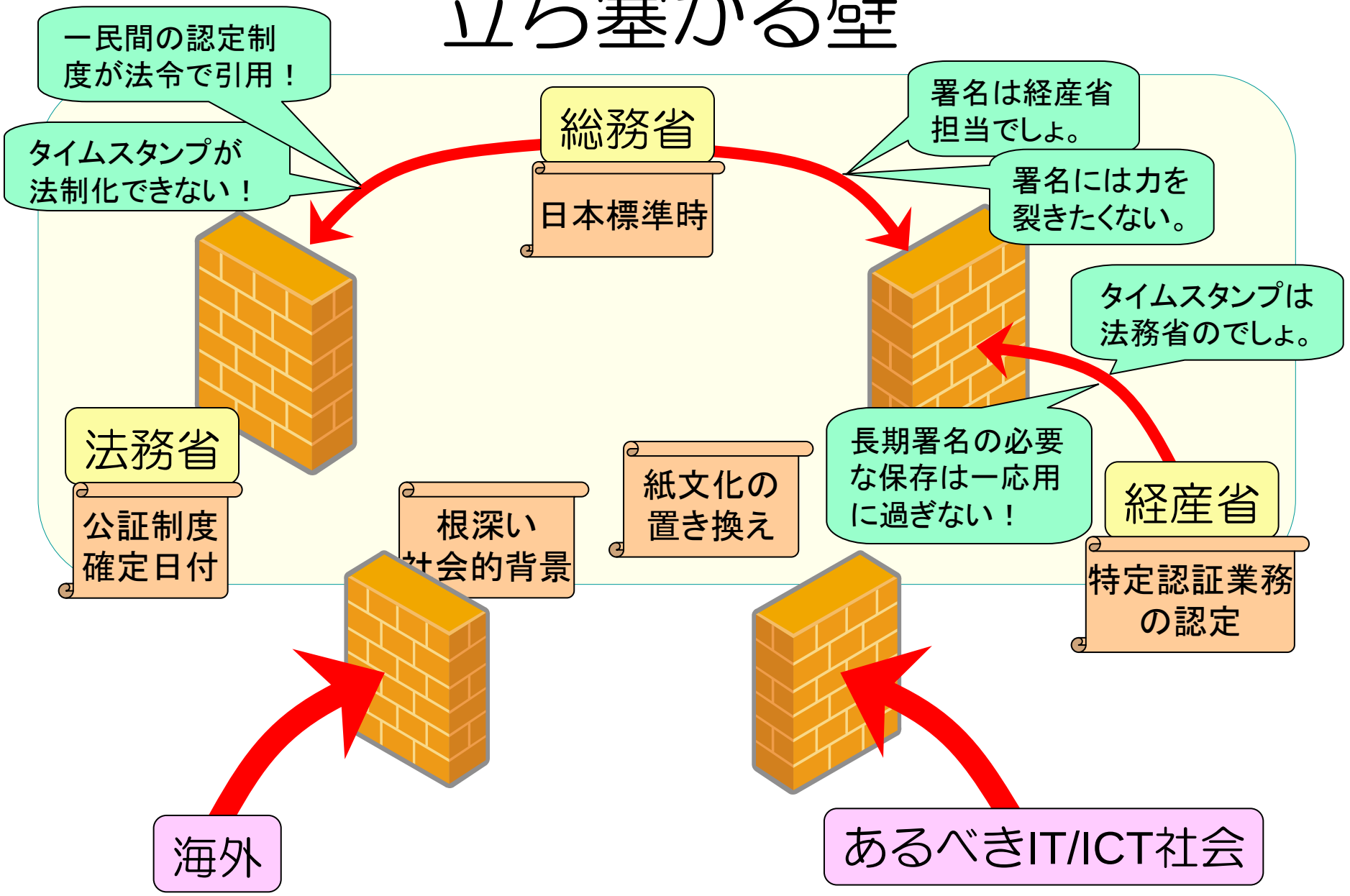
信頼基盤の連携に向けて

『穴と壁』

信頼基盤の穴

- 『トラストアンカ』
  - 欧州ではTSL（Trust-service Status List）で共通化を検討。米MS、Adobeも参画。
- 署名ポリシと検証プロセス
  - 署名の意味にもいろいろ←ECOMでの検討も道半ば
  - どこまで検証すればよいのか？
    - SigningTimeが必須？
    - 「Option」もあれば検証必須？
    - SingningCertificateちゃんと検証してる？
- 『認証』と署名の関係
  - マイナンバー、HPKI認証用証明書、トラストフレームワーク
- 『長期』信頼基盤
  - ［トラストアンカ、失効、安全なアルゴリズム、、］の履歴情報
- 国際的な相互信頼性の確保

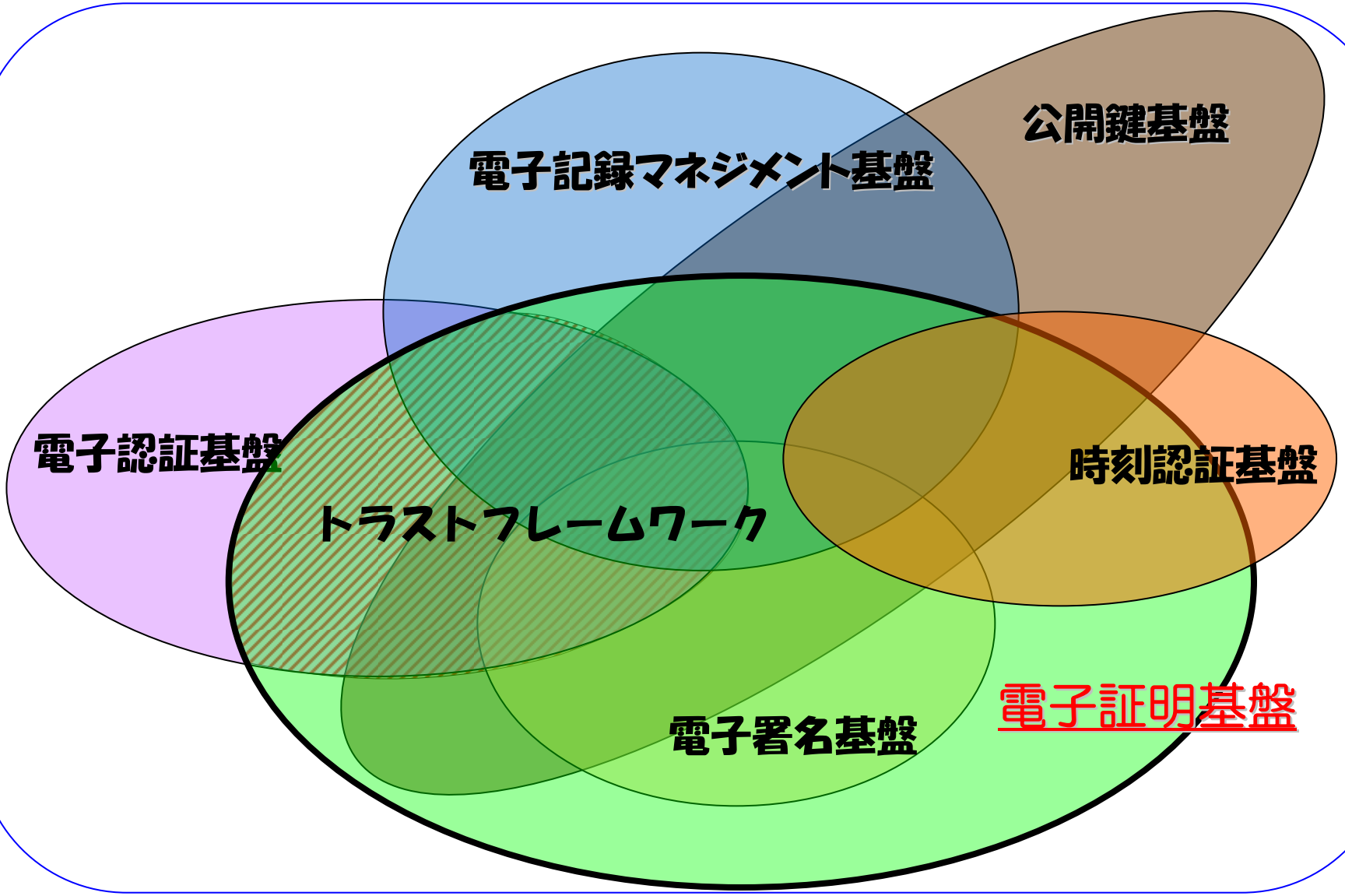
立ち塞がる壁


一民間の認定制度が法令で引用！
タイムスタンプが法制化できない！
総務省
日本標準時
署名は経産省担当でしょ。
署名には力を裂きたくない。
タイムスタンプは法務省のでしょ。
法務省
公証制度
確定日付
根深い社会的背景
紙文化の置き換え
長期署名の必要な保存は一応用に過ぎない！
経産省
特定認証業務の認定
海外
あるべきIT/ICT社会

壁があるから穴ができる！！

⇒ということは？！

安全な情報社会のためのIT/ICT基盤



ご清聴
ありがとうございました。