平成26年度第2回学術情報基盤オープンフォーラム
～デジタルエビデンス：重要なのは信頼できる情報～

2015.2.3

SEIKO
セイコーソリューションズ株式会社

SI統括部
クロノトラスト部

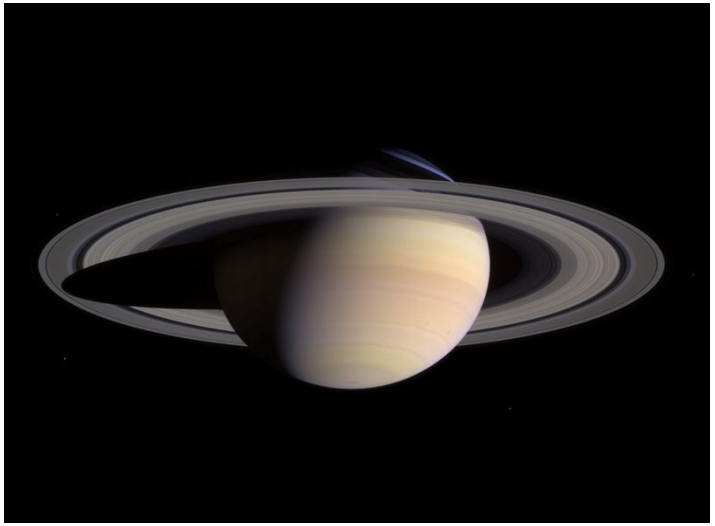
TIME
SMILE
TIME
未来という「時」に、もっと笑顔を。

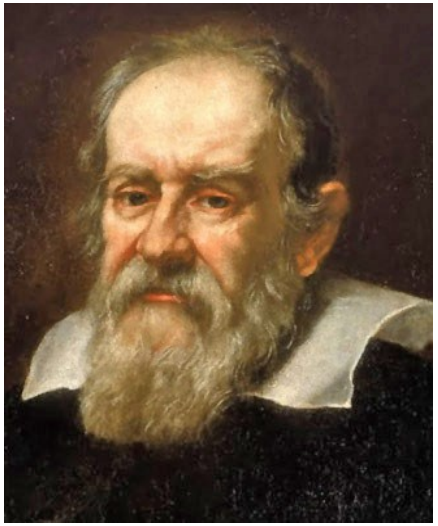
AGENDA

- 情報の証拠保全
- デジタル署名について
- 電子署名とタイムスタンプ
- 最新事例
- まとめ

暗号（アナグラム）と公証（郵便）による権利保全

SMAISMRMILMEPOETALEUMIBUNENUGTTAUIRAS



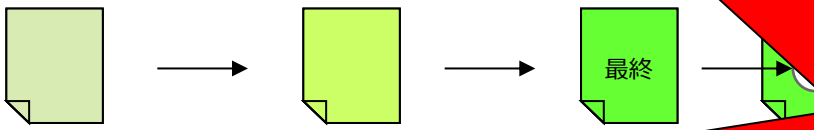


Altissimum planetam tergeminum observavi
("I have observed the most distant planet to have a triple form")

情報管理における**リスク**と**対処**

時の流れ

生成　登録　更新　承認　確定　保存　活用　廃棄

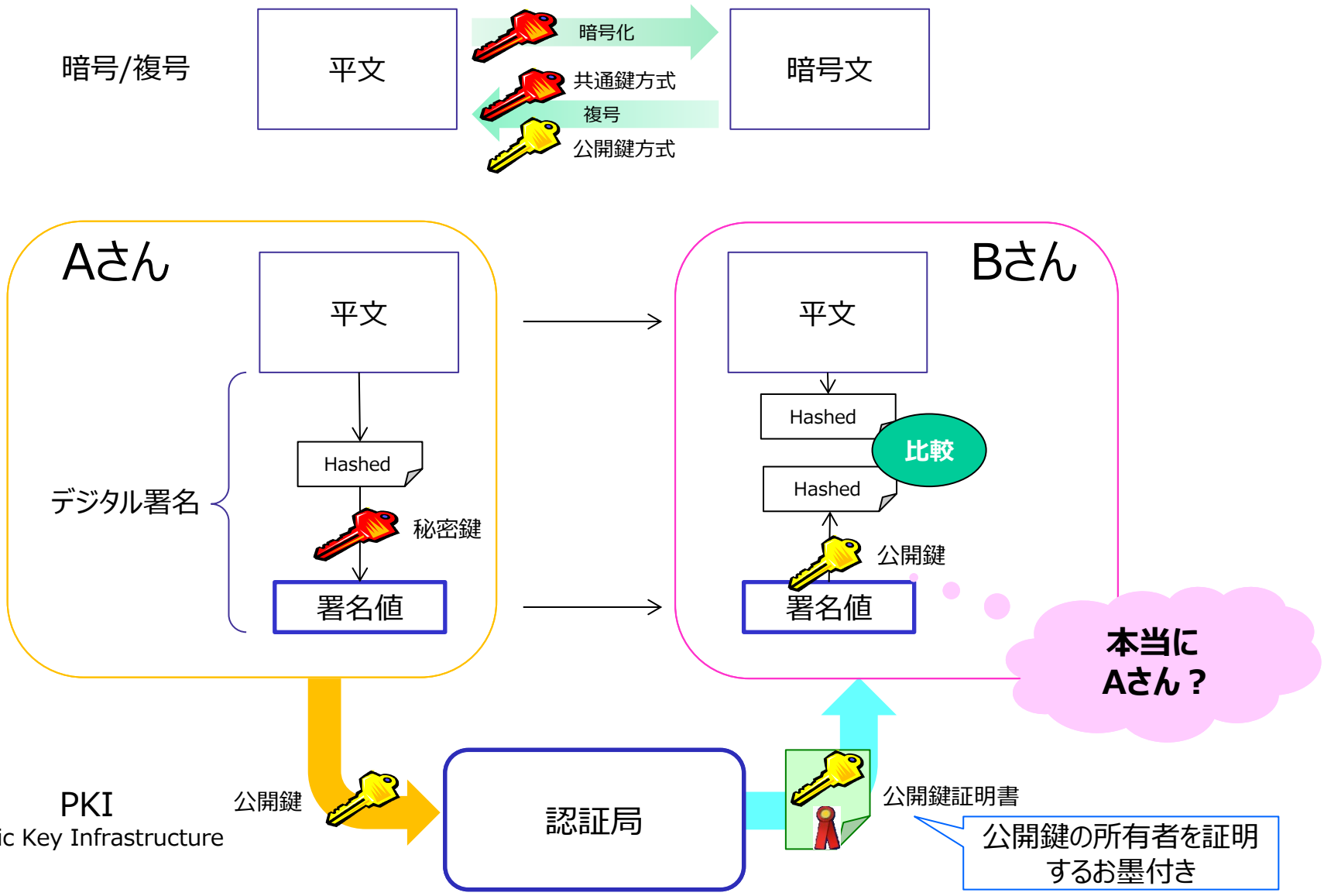


情報爆発
代わるステイクホルダ
関係者不在
2次利用、3次利用
何が正しい？

- なりすまし
- 情報鮮度の低下
- 情報精度の低下
- 改ざん
- ねつ造
- 劣化・破壊
- 見読性の喪失
- 漏洩・紛失
- 検索困難
- 誤廃棄

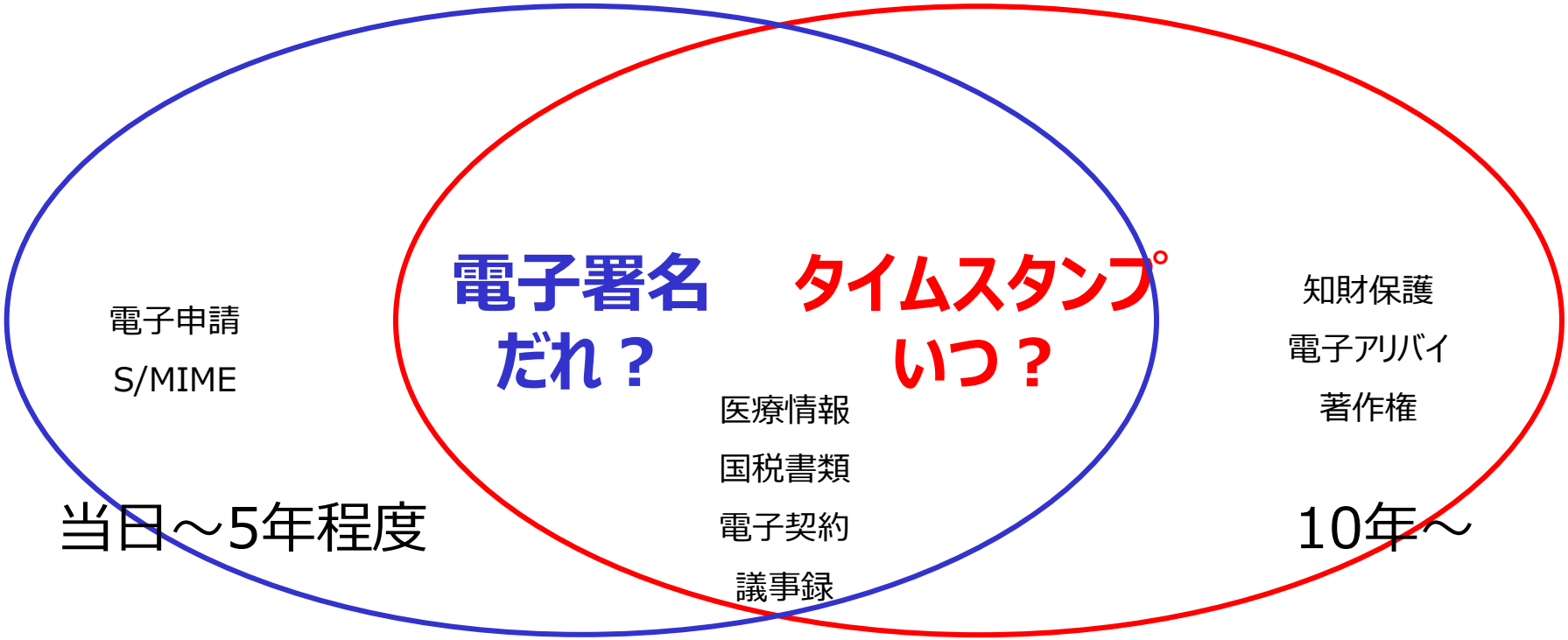
世界共通の尺度
正しい時刻 で
情報を固めること＝タイムスタンプ
改ざん・ねつ造防止！

デジタル署名について（暗号～PKI）



電子認証、タイムスタンプ、そして電子署名

電子署名法：2001年　　JIS化：2008年　　e文書法：2005年



認証	署名	存在証明
その場で検証	後日検証	後日検証
本人性		第三者性

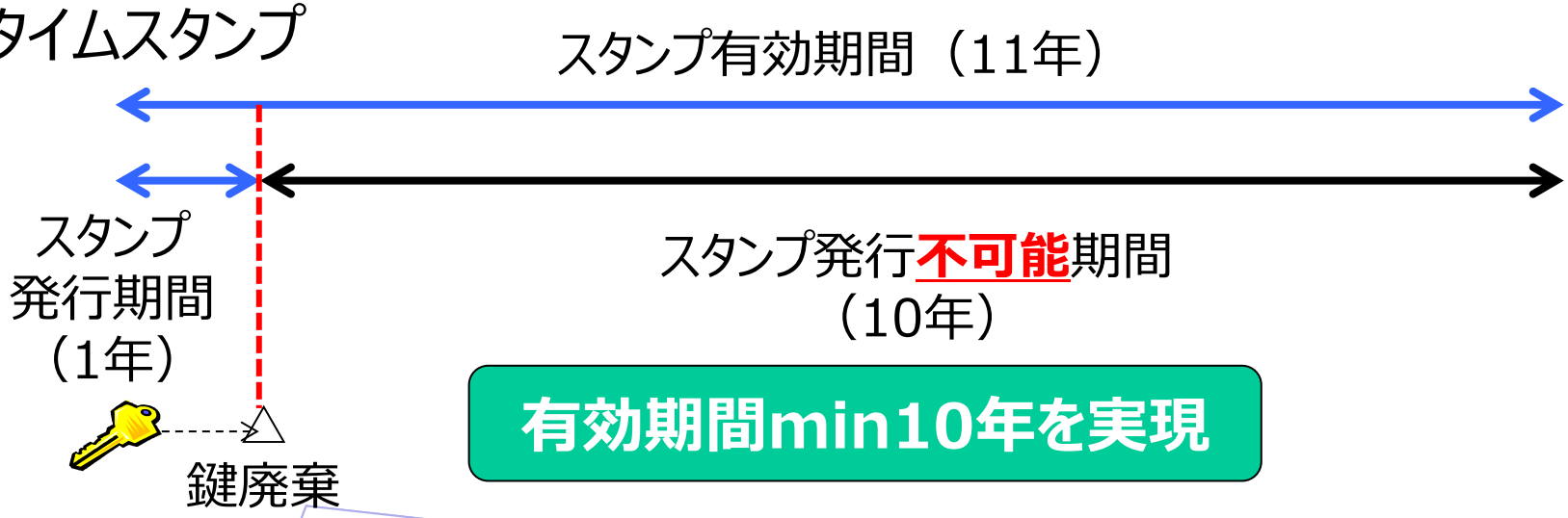
有効期間について

有効期間とは、CAが発行する公開鍵証明書の有効期間です。

電子署名

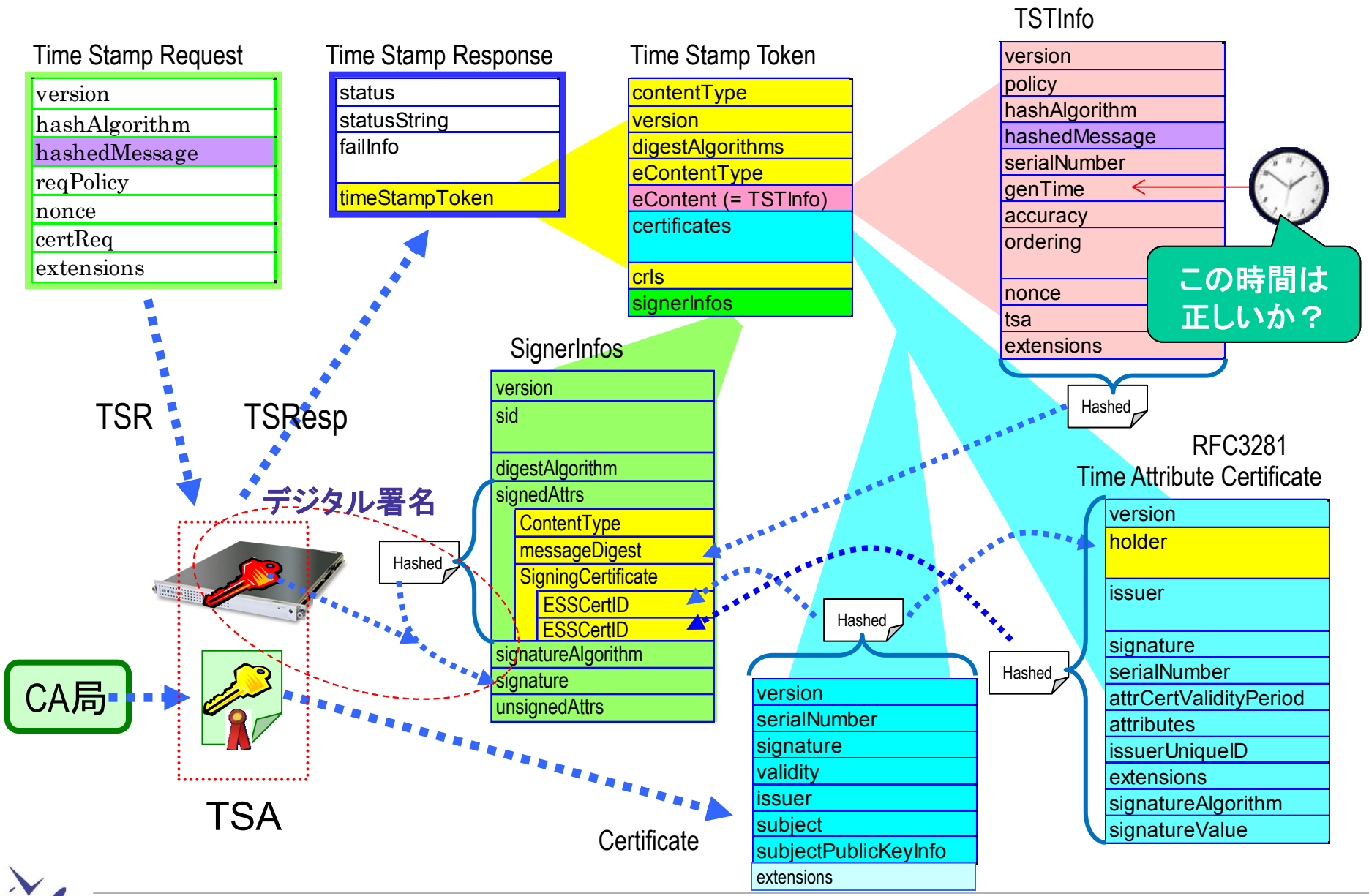
鍵の運用（管理、廃棄）は、署名者自身：いつでも利用できる
⇒ 鍵の漏洩/紛失などのリスクや、証明書の記載事項変更が考えられ、法令で5年以下に制限

タイムスタンプ



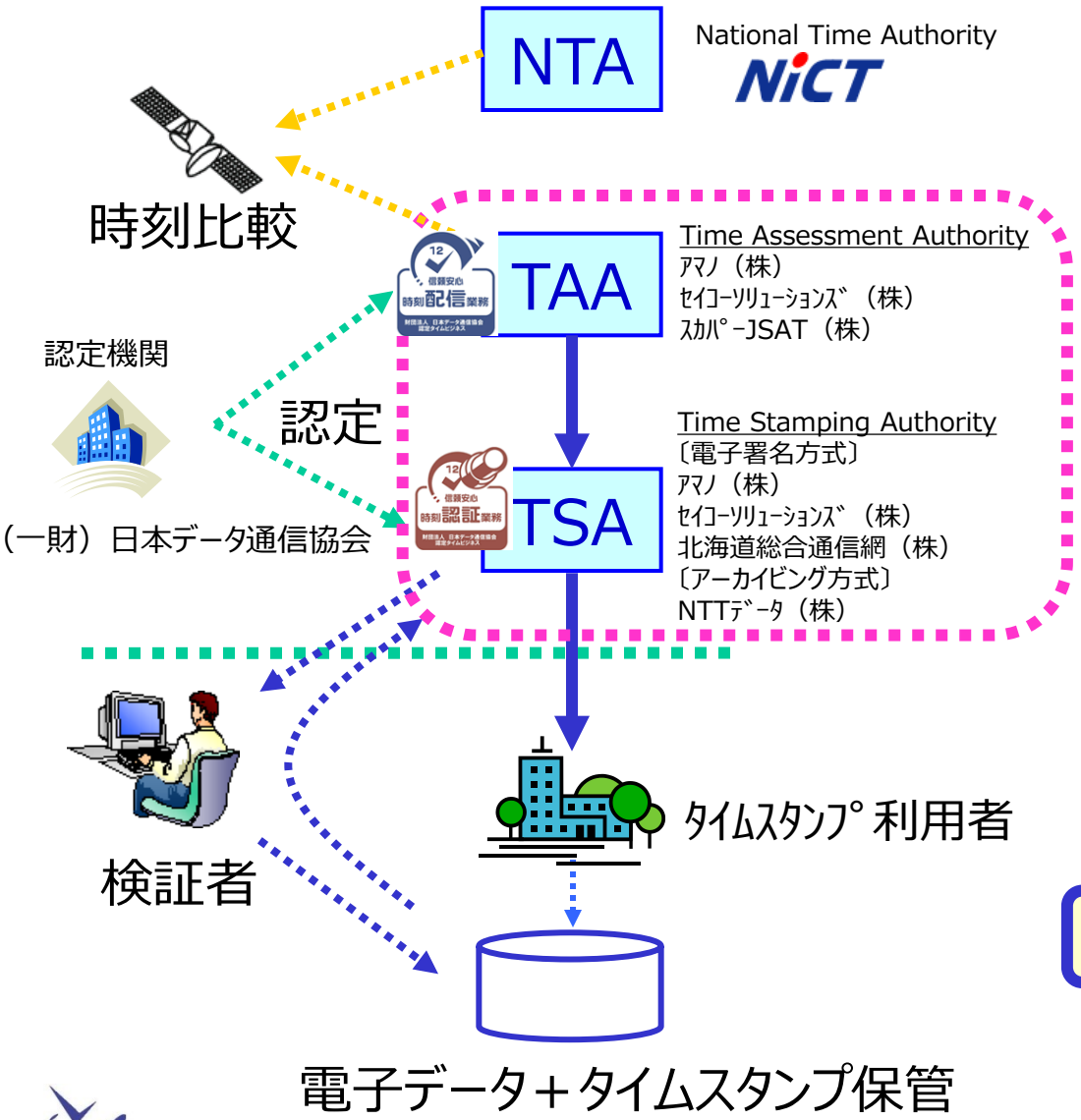
鍵の運用（生成、管理、廃棄）を第三者機関が監査：CAが長期有効証明書を発行できる

タイムスタンプ（RFC3161/ISO18014/JISX5063）のデータ構造



タイムビジネス信頼・安心認定制度

-JISX5094：2011年5月20日制定
-ISO化推進中ISO18014-4：Stage50.00 2014年11月



「タイムビジネスに係る指針～ネットワークの安心な利用と電子データの安全な長期保存のために～」（総務省指針）

一般財団法人日本データ通信協会が定める基準を満たした技術・システム・運用体制によって、TSA・TAA業務が厳正に実施されていることを認定する制度。
2005年2月制定
<http://www.dekyo.or.jp/tb/tbtop.html>

時刻に関する認定基準
- TSAは、認定TAAからの時刻配信業務を利用すること
- TAAは、NTAが指定した時刻比較および保管すること

信頼できるTAA・TSAの時刻

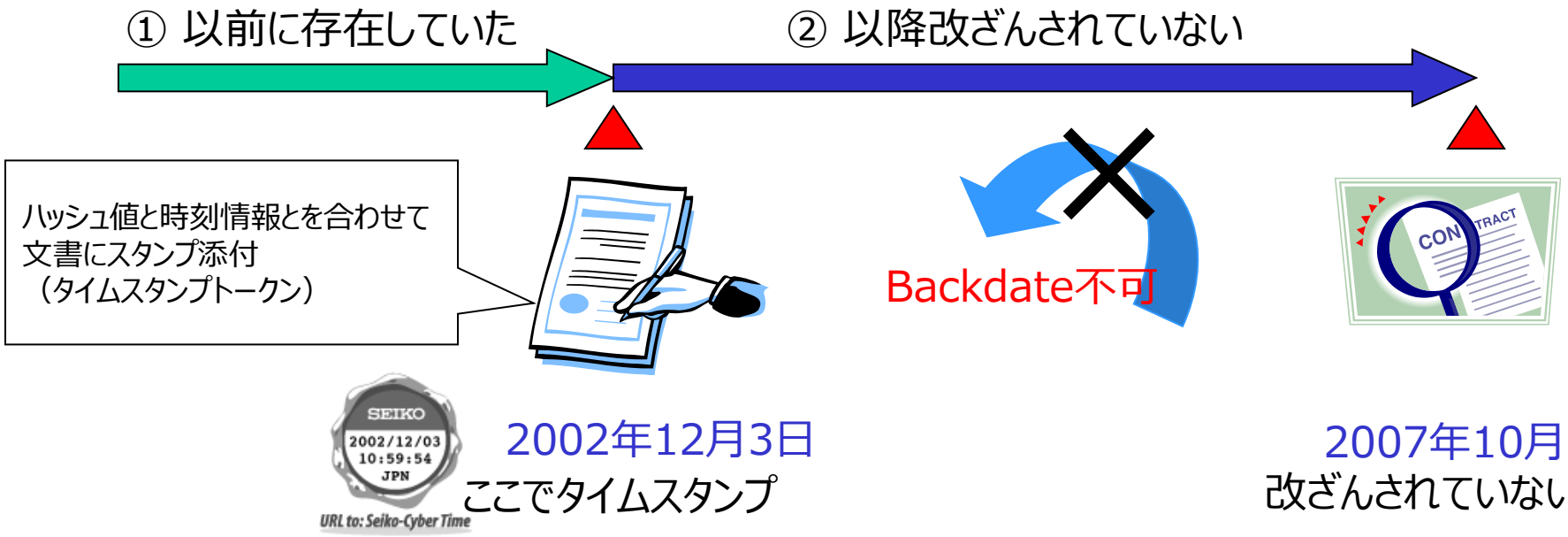
タイムスタンプの特徴

電子文書が

① スタンプ時以前に存在していたこと

② スタンプ時以降改ざんされていないこと

を証明する仕組み。

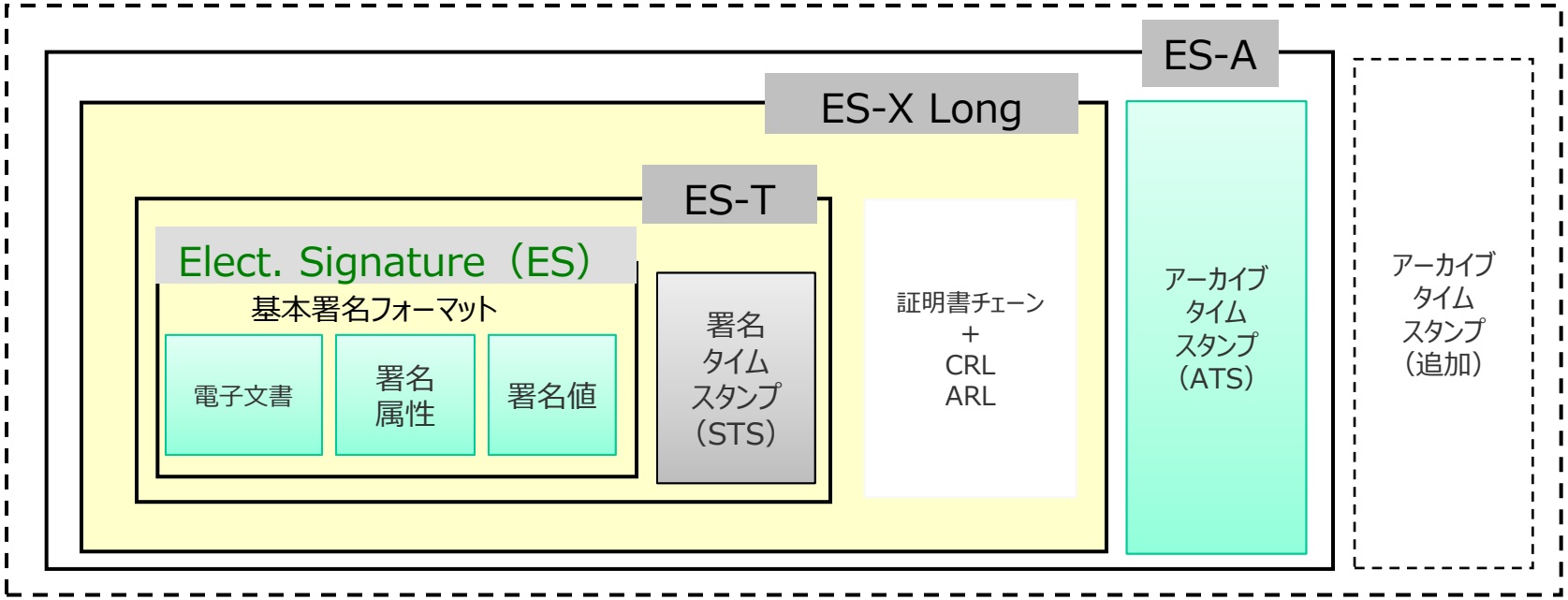


タイムスタンプは、**信頼できる時刻** を利用した電子文書の証拠性を確保する技術です。

長期署名プロファイルの規格　（JIS：2008年3月、ISO：2012年9月）

JIS-X5092、ISO14533-1　CMS利用電子署名（CAdES）の長期署名プロファイル
JIS-X5093、ISO14533-2　XML署名利用電子署名（XAdES）の長期署名プロファイル

【ポイント】
・署名タイムスタンプ（STS）により署名時刻の証拠性を確保
・失効情報や証明書を署名データ内に格納し、証明書検証の継続性を確保
・アーカイブタイムスタンプ（ATS）の暗号アルゴリズムにより、署名データや失効情報等を保護



ES：
Electronic Signature

ES-T：
Electronic Signature with Time stamp

ES-X Long：
Electronic Signature eXtended

ES-A：
Electronic Signature Archive

タイムスタンプに関する法律・ガイドライン

国税庁：
国税関係書類のスキャナ保存及び電子取引記録要件
（財務省令第22号：電子帳簿保存法施行規則第三条第5項第2号ハ、第八条）
「帳簿、決算関係書類、契約書・領収書の一部を除く国税関係書類に、（財）日本データ通信協会が認定するタイムスタンプ付与」

厚生労働省：
医療情報システムの安全管理に関するガイドライン
Ver4.2（2013年10月）
「医療情報の真正性確保の為に、（財）日本データ通信協会が認定するタイムスタンプ付与」

特許庁：
ガイドライン「先使用権制度の円滑な活用に向けて」65page
「タイムスタンプは先使用権の立証のための、時刻の先後に関する一つの証拠として、簡便な手法であり、有益」

文部科学省：
指導要録等の電子化に関する参考資料
電子署名や暗号化技術，タイムスタンプ等を用いて記録することにより真実性を保ち，改ざんを防止することが望まれます。

国土交通省：国住指第394号（2014/5/7）
建築確認手続き等における電子申請の取り扱い（技術的助言）
建築基準法での法定保存期間に有効性を確保するため長期署名すること。

総務省：
ASP・SaaS における情報セキュリティ対策ガイドライン
「サービス種別に関わらず、完全性への要求は「高」いものと考えられる。・・・原本性（真正性）確保の手段としては、時刻認証による方法・・・等が考えられる。」

環境省・経済産業省：
事業者向け公害防止ガイドライン
「データ改ざんが物理的に不可能な計測システムや、電子署名、タイムスタンプを活用する。」

各府省情報化統括責任者（CIO）連絡会議：
オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン
「長期保存した文書の完全性及び非否認性を示すためには、タイムスタンプ署名を定期的に施すなどの処置をすべきである。」

日本公認会計士協会：ＩＴ委員会研究報告第38号
電子的媒体又は経路による確認に関する監査上の留意点
「電子的回答と監査証拠の証明力として、電子的回答においては、信頼しうるPKIとタイムスタンプのような情報技術を組み合わせる」

総務省：
地方税関係帳簿書類の電磁的記録による保存等
（総務省令第八五号：地方税法施行規則第25条第5項第2号ハ）
「地方税関係書類をスキャナで読み取る際に、電子署名が行われている当該地方税関係書類に係る電磁的記録の記録事項に（財）日本データ通信協会が認定するタイムスタンプ付与」

- デジタルエビデンス
- デジタル署名について
- 電子署名とタイムスタンプ
- 最新事例
- まとめ

主な事例のご紹介

デジタルエビデンスソリューションは
様々な分野で好評をいただいています。

否認対策

先使用権

説明責任

冒認出願対策

スキャナ保存

紙廃棄

真正性確保

訴訟対策

慶應義塾大学病院：医療文書の電子化保存（XAdES）

外来・病棟等

①２次元バーコード付仕切紙や１次元バーコードが付いた文書を印刷

診断書
紹介状
同意書

②搬送

病歴室

③スキャナから一括取込み

業務用イメージスキャナ

<電子カルテ>

9.1、9.2 記載の運用

外来・病棟等

<電子カルテ>

⑥電子カルテから取込んだ文書を参照

④保存

運用管理規定

医療機関向け文書管理システム

6.12 記載の
(財)日本データ通信協会認定TSA局

医療情報は院外には転送されない

作業責任者の署名

⑤長期署名処理（自動連携）

入力 署名 長期

TSA

CA

eviDaemon

長期署名クラウドサービス

JIS X 3093準拠長期署名データ

見読性
TIFF形式

真正性
6.12 記載の長期署名方式

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）

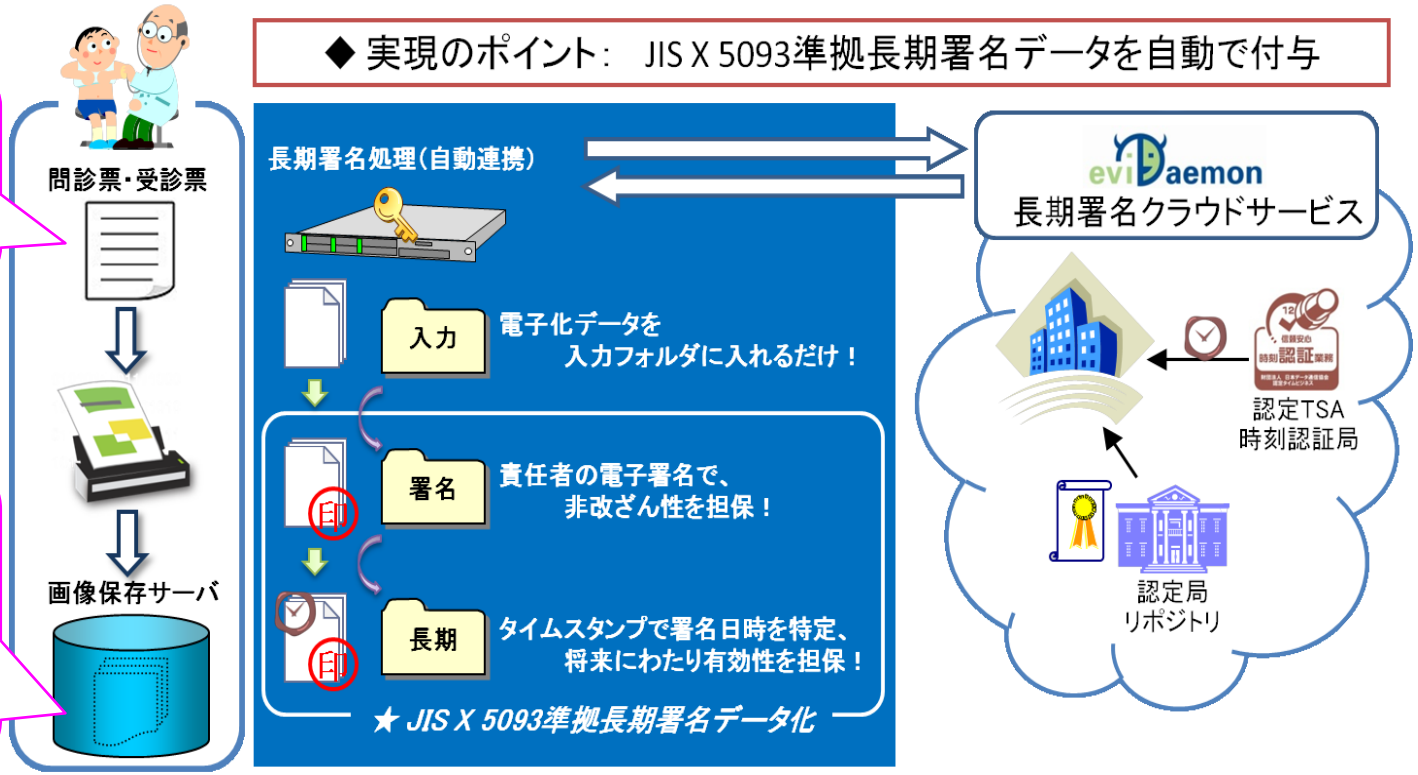
愛知健康増進財団：問診票・受診票の電子化保存

簡単・リーズナブル

◆ 実現のポイント： JIS X 5093準拠長期署名データを自動で付与

個人情報であるため漏えい/紛失対策を施した保管場所の確保が求められる。

医療情報システム安全管理に関するガイドラインに準じた施策で電子化
・事務上のセキュリティリスク軽減
・コスト削減



検査記録のスキャナ保存（XAdES）

紙の検査結果表をスキャナに
通して電子化

検査資料

検査作業者

検査作業者が設備内で
検査し紙に記載

原本保管システム

文書管理システム

File

原本

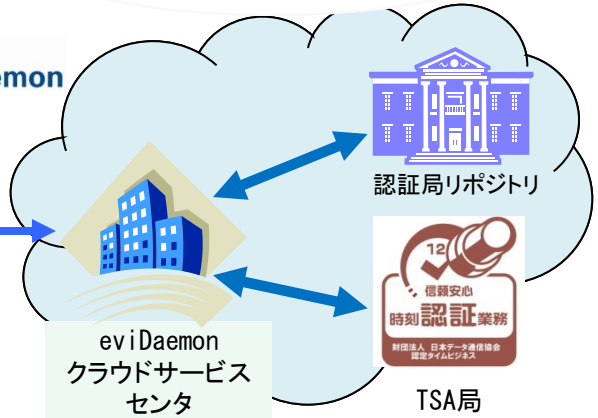
eviDaemon
サーバ

長期署名
データ
（XML）

エビデンス

DB

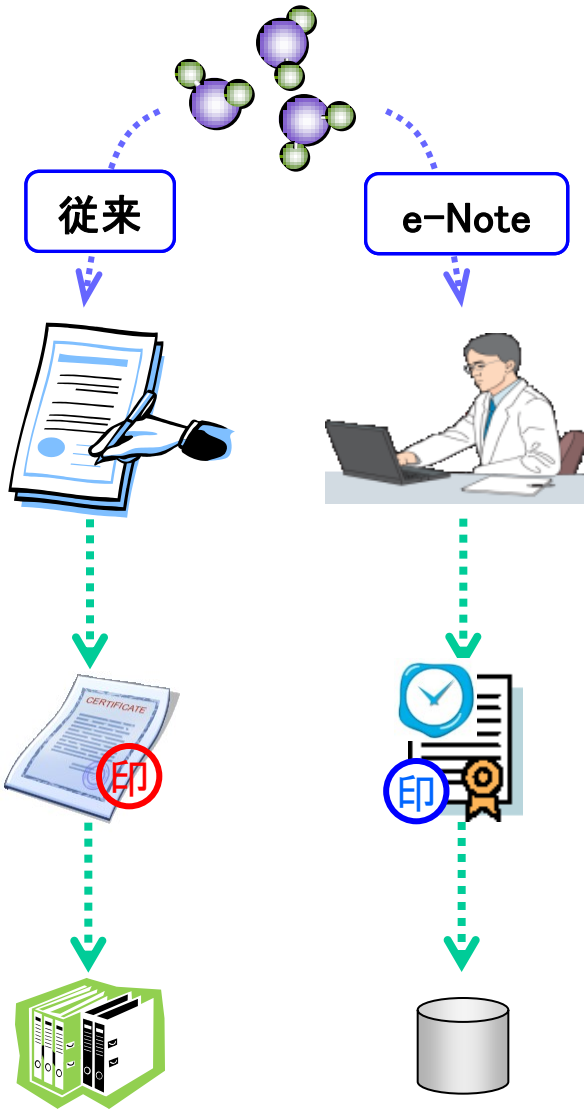
eviDaemonクラウドサービス



管理者

課題：
①膨大な検査記録の管理（紛失・滅失のリスク）
②検査記録は事故発生時に過去に遡って提示する必要がある。
③**対外的に説明責任が求められる、自身で自身が正しいことを証明できない。**
解決：
①証拠性を担保し電子化を行うことで、複数箇所に保管可能
②③国際標準の長期署名により真正性確保して長期的に証拠性を担保していることを提示できる。

知的財産保護（XAdES）



エンドユーザ：武田薬品工業（株）様

事例：製薬研究データの記録に対する真正性確保

まず、化学合成部門技術者対象

臨床実験データの記録・保管にも使用予定

目的：知財保護、訴訟リスク対応

解決：長期署名フォーマット**XAdES**

XML **Ad**vanced **E**lectronic **S**ignatures

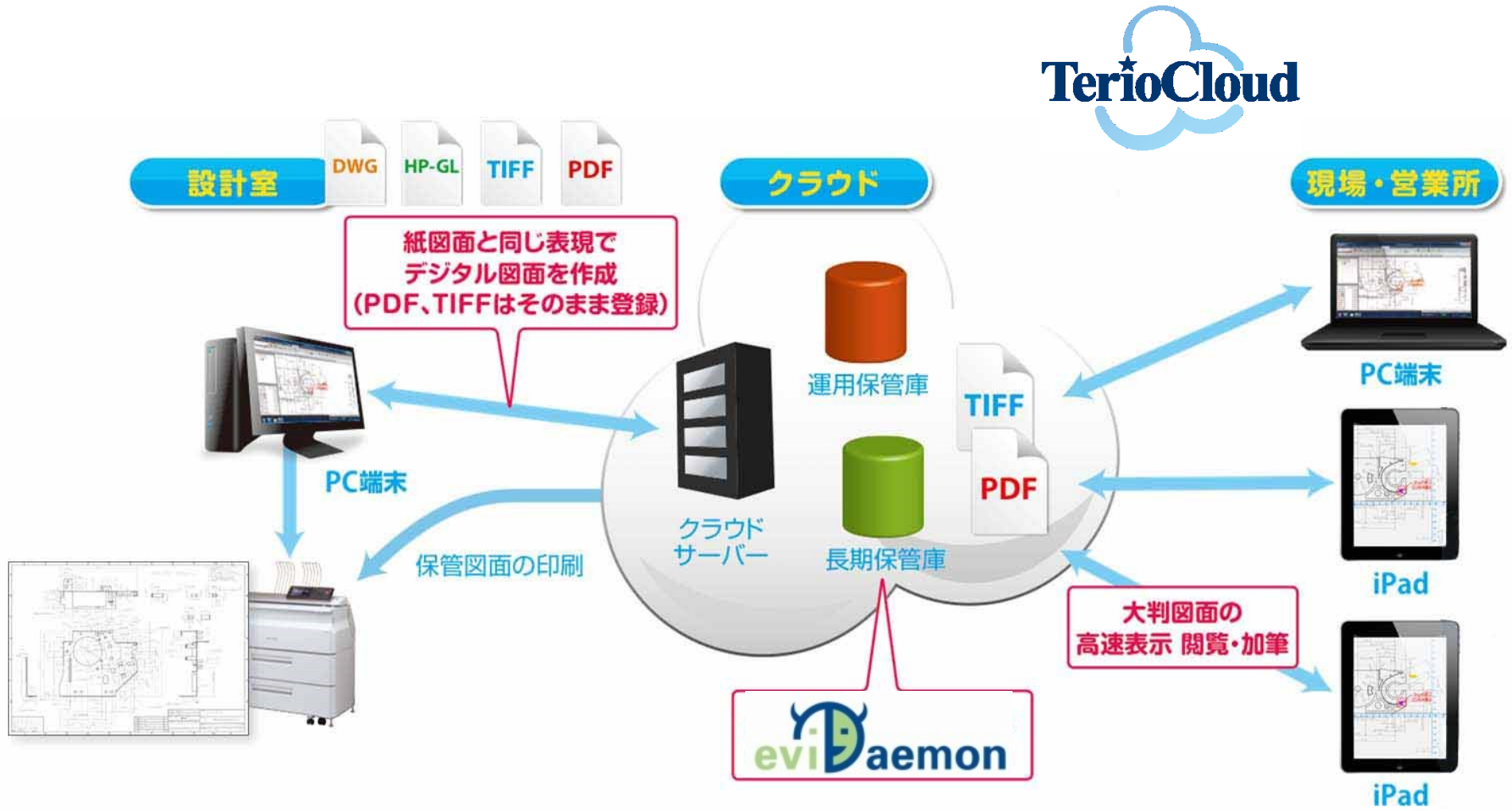
電子署名＋タイムスタンプにて長期に亘って

電子データの証拠性を担保する技術

Globalに通用する仕組み！

研究効率の向上！
1、実験作業時間の短縮
2、過去研究成果を活用（重複実験を省く）

大判デジタル図面の作成 および iPadによる活用と、長期保管のクラウドサービス



紙図面とデジタル図面を境目なく利用可能

iPadアプリはApple Appストアーより無料ダウンロード

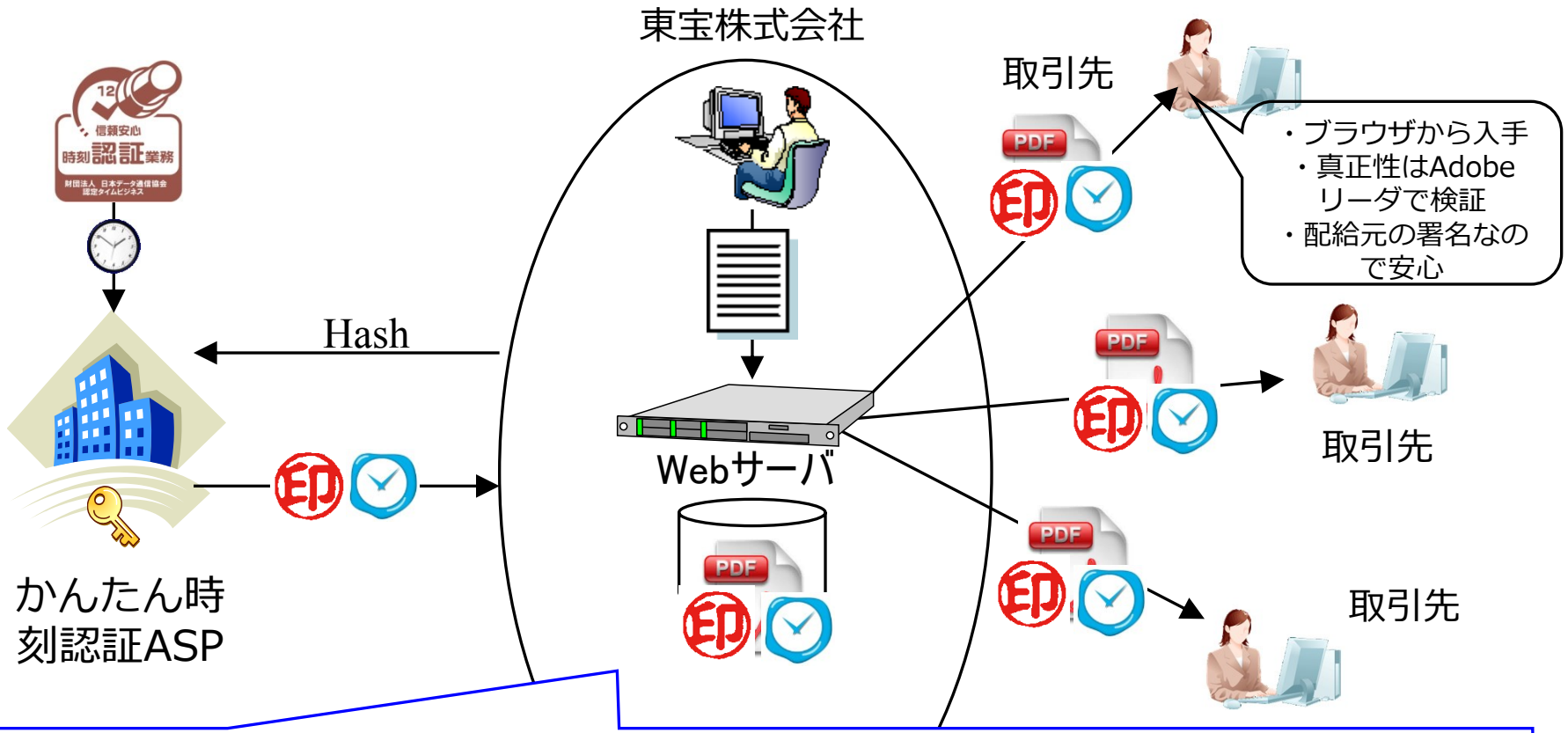
コミュニケーションプラン協同組合：書類BANKサービス（PAdES）

組合加入事業者の相互扶助のため協同で利用できる電子契約システム

組合加入事業者のメリット
- 印紙税削減
- リーズナブルな運用コスト
- Web/メールなので簡単に利用
- 面倒な鍵の運用を任せられる
- 真正性が担保されているので安心
- 長期間保存でき、いつでもダウロードできる

組合側の導入背景
目的：組合加入事業者へのサービス拡充
課題：ICTリテラシレベル差を埋めるICT支援

東宝株式会社：コンテンツ配給契約（PAdES）



課題：
①取引先とのコンテンツ毎の契約業務をコストダウンしたい。締結に係る業務量を減らしたい。
②契約の電子化だけではデータの真正性が担保できず契約期間トラブルやコンプライアンス問題がある
③秘密鍵の管理は運用が大変でコストがかかる
解決：
①紙の契約からWebシステムで、郵送費、運用費のコストダウン、締結業務のスピードアップ、業務量の激減
②真正性を電子署名・タイムスタンプを付与することで担保
③ASPで秘密鍵管理

○○生命：保険契約/控えの縦覧・交付（PAdES）

再発行手間の削減
ペーパーレス

顧客：
サイン時点から契約締結
Adobe Acrobat/Readerで検証確認できる。
保険契約申込書控えの手持ち保管不要

営業支援システム

Webサーバ

顧客情報

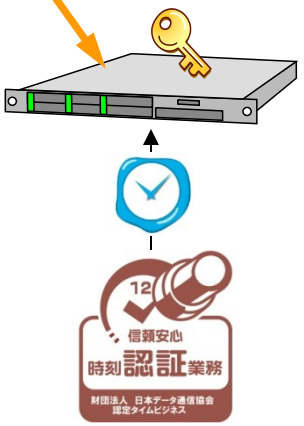
受付サーバ

PDF

印

AdobeCDS署名

evidaemon

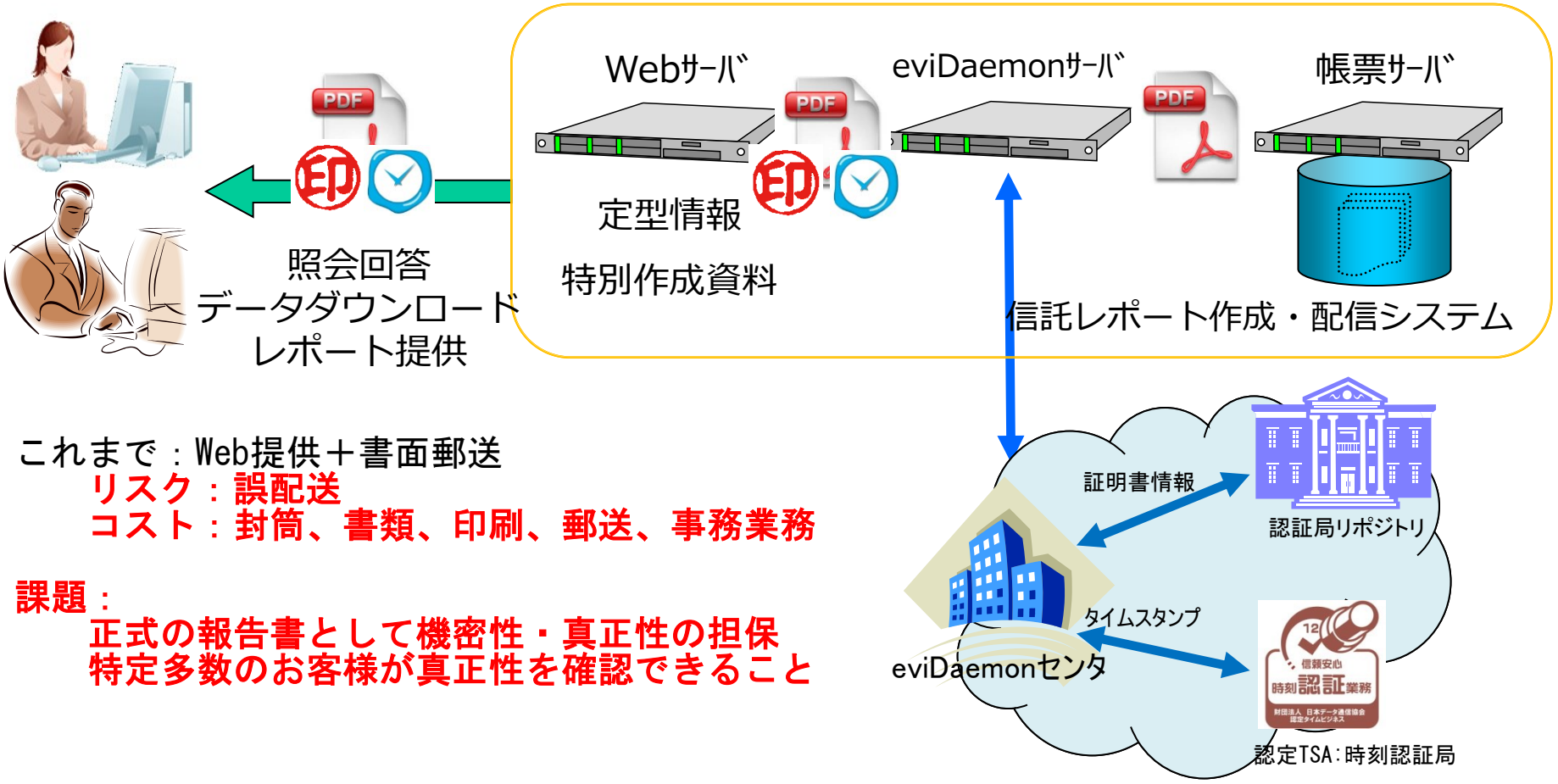


最終契約：対面
タブレット上でサイン（契約成立）
事前に必要情報は入手済み

保険員：
契約締結業務の効率化
説明抜け/確認抜け等のミス無し
リスクの高い資料を持ち歩く必要なし
記載ミスによるトラブル未然防止

エビデンス生成ASP

○○信託銀行:情報提供サービス(PAdES)



これまで：Web提供＋書面郵送

リスク：誤配送

コスト：封筒、書類、印刷、郵送、事務業務

課題：

正式の報告書として機密性・真正性の担保

特定多数のお客様が真正性を確認できること

解決：AdobeCDSを利用したPAdES方式による配信

Acrobat/Readerで検証できる

国際標準で長期に亘って真正性を検証できる

個人顧客向け定期サービスの電子契約&現地決済

・簡便で安心な契約締結
・免許書の写真で本人確認完結
・印鑑不要
・口座振替書の記入不要

サービス事業者様

・キャッシュフローの改善
・営業機会損失の低減
・契約締結業務の効率化
・再訪問等のロス低減

Webサーバ　本部　顧客情報

Internet
SSL通信

ファイア
ウォール

受付サーバ

Internet
SSL通信

eviDaemon

顧客

営業員

・データはセンター転送後
端末から自動削除
（個人情報は残らない）

・契約締結業務のスピードアップ
・記載ミスによるトラブル未然防止
（必須項目のチェック可能）
・Option等もその場で対応
・営業が帰社後データ入力不要

・インターネットに
個人情報は流れない
ので安全

信頼安心 時刻認証業務

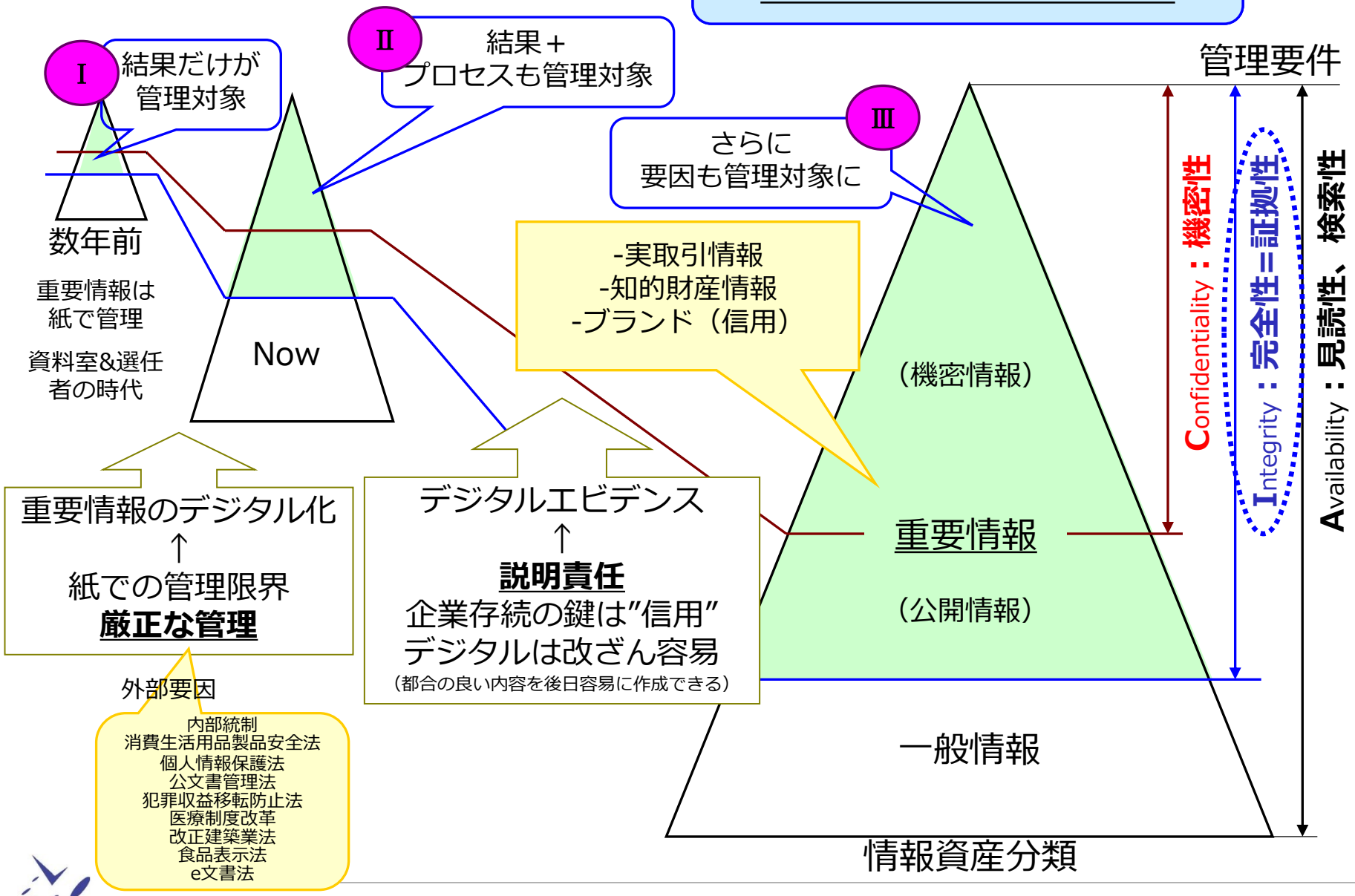
エビデンス生成ASP

契約内容確認・本人認証・口座振替手続きを現場で完結！

- デジタルエビデンス
- デジタル署名について
- 電子署名とタイムスタンプ
- 最新事例
- まとめ

情報資産管理

情報は信頼性が問われる時代に
Trustedであることが重要



まとめ：電子データが本物か？を長期に担保できれば・・・

- **電子データのままで運用可能**
  - 保存コストの削減（書類保管倉庫の削減など）
  - 輸送費の削減
  - 印紙税の削減（電子契約）
  - 検索性の向上による顧客対応力の強化および人件費の削減
  - 電子データの一括管理による個人情報管理等への活用が可能
  - 紙の削減による環境コストの削減
  - e-文書法による電子保存の法的容認
- **企業の権利保護**
  - 知的財産における先使用権確保や冒認出願対策
  - 内容証明郵便、公証人による公証等のコスト・工数の削減
- **訴訟リスクの軽減**
  - 信頼性のある電子情報の活用による顧客対応力の強化
- **内部統制への活用、監査証拠の証明力強化**
  - 安全・安心な電子情報による不正のできない環境創出
- **事業継続性運用の確保**
  - 複数原本化による、情報の紛失・滅失リスクの回避

デジタルエビデンスがあなたの情報資産を守ります。