

# Network Security Forum 2019 「署名検証・知ってるつもり」 ～ 真正性 編 ～

2019.01.22

日本トラストテクノロジー協議会（JT2A）真正性保証TFリーダー

三菱電機株式会社

山中 忠和

みなさま、  
この単語、聞いたことはありますか？？

**真 正 性**

この単語の意味は、知っています？？

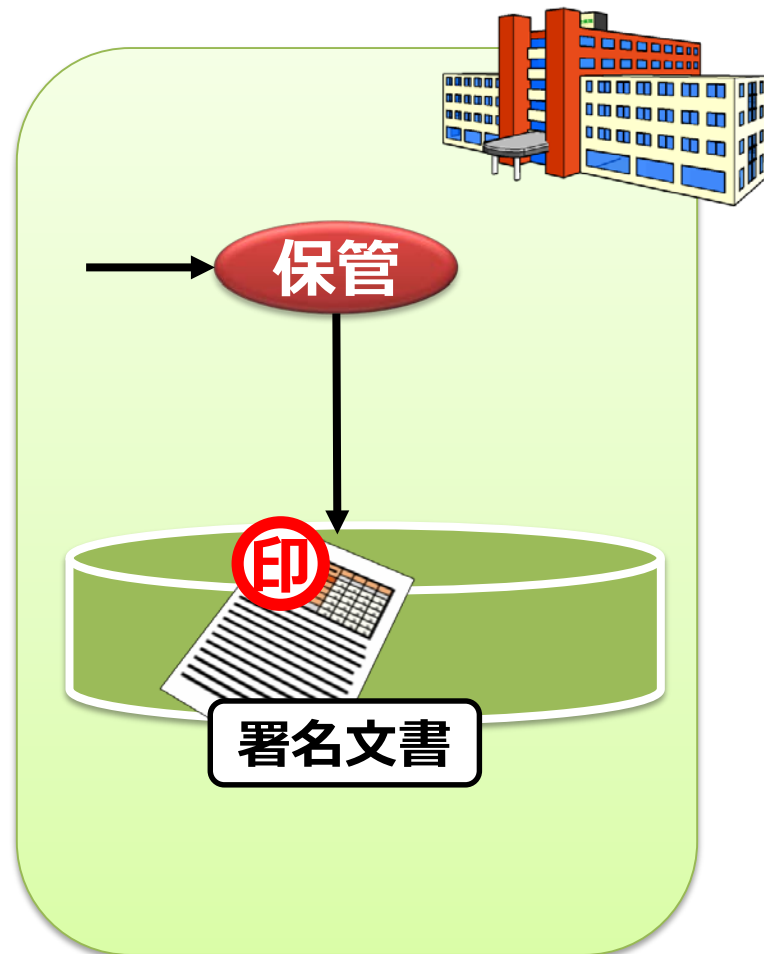
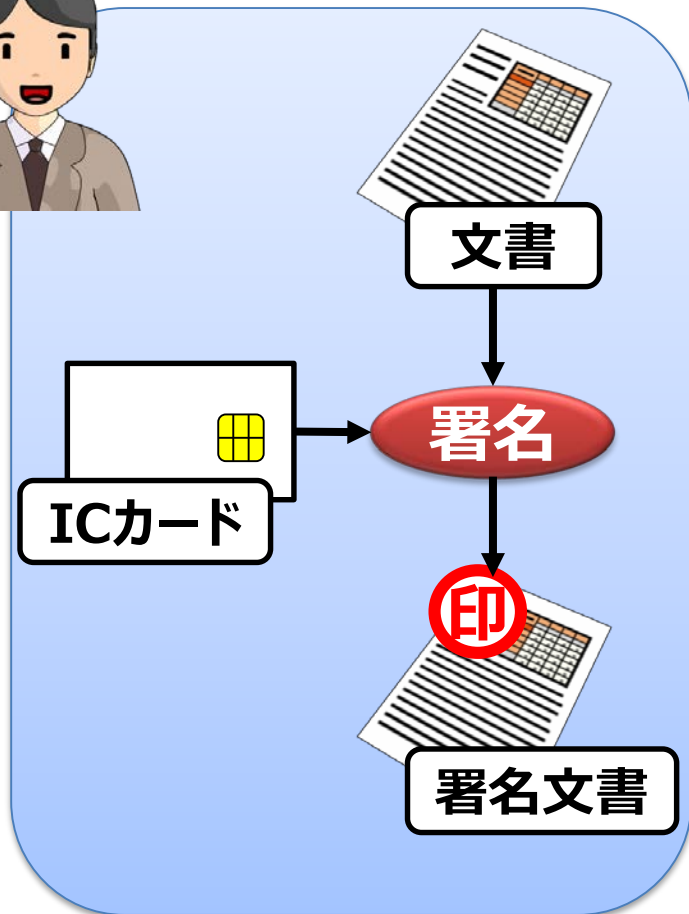
では、みなさまに

# Quiz

です

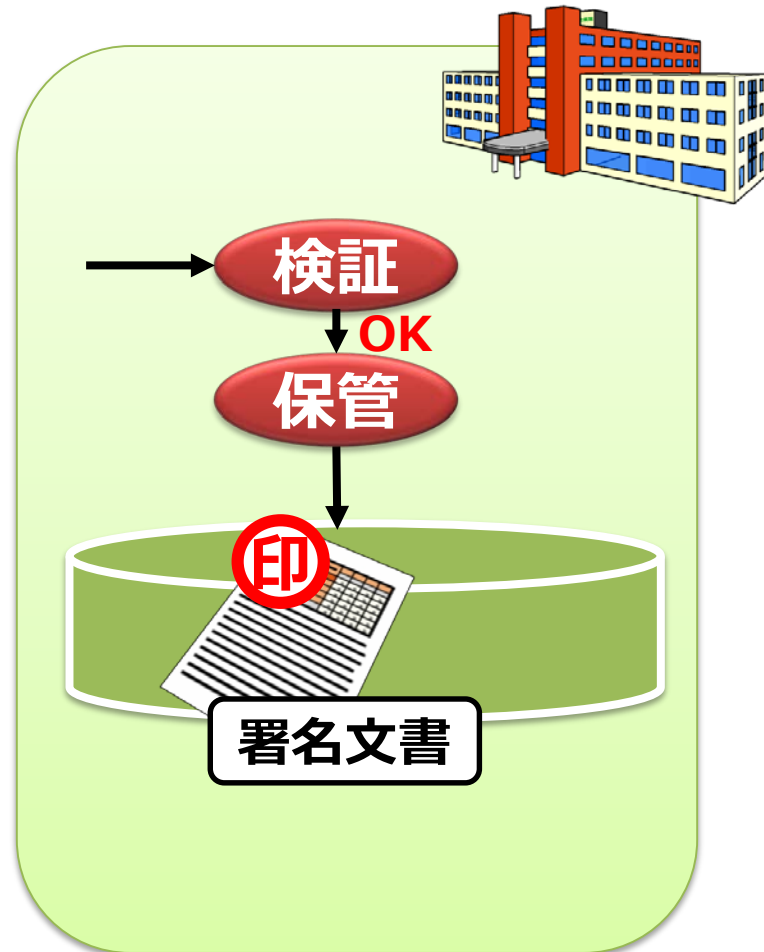
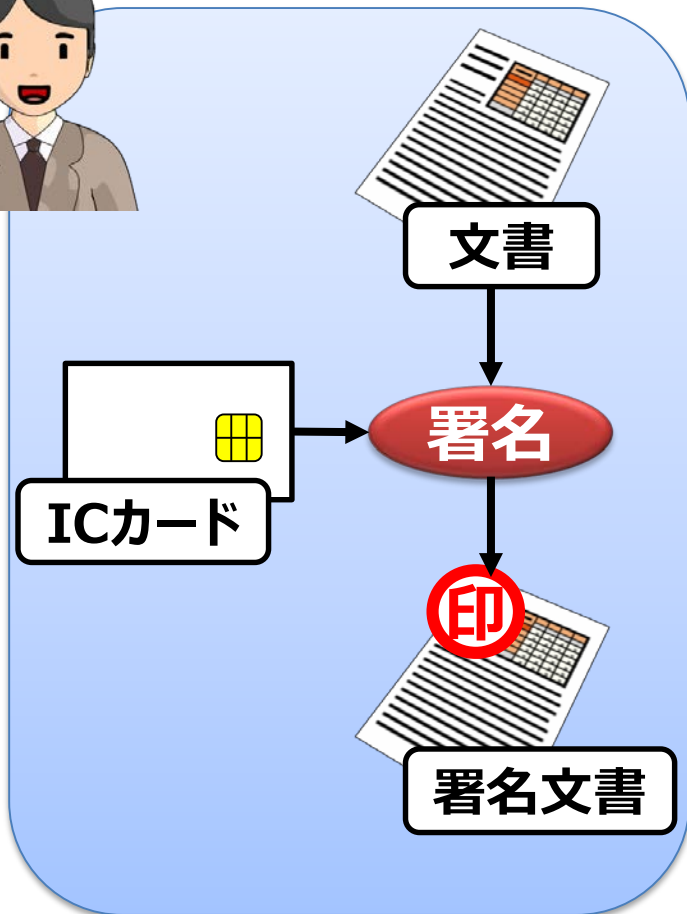
# Question 1

この文書は真正性を保証していると言える??



どうでしょうか？

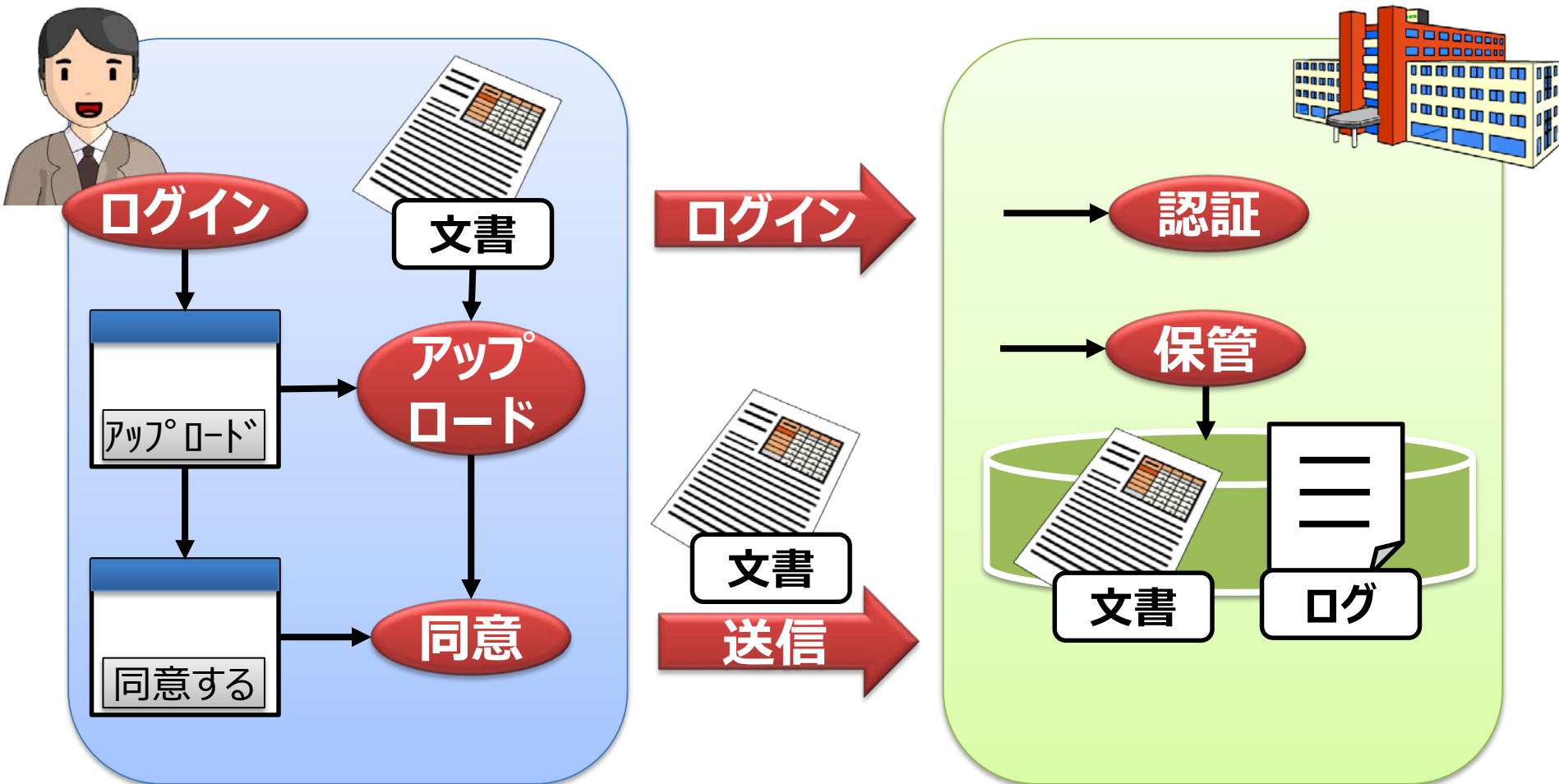
この文書は真正性を保証していると言える??



どうでしょうか？

# Question 3

この文書は真正性を保証していると言える??



どうでしょうか？

- 「**ISO27000**」では、
  - エンティティは、それが主張する通りのものであるという特性。
- 「**Wikipediaの情報セキュリティ**」の項目では、
  - ある主体又は資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
  - 情報システムの利用者が、確実に本人であることを確認し、なりすましを防止すること
- 「**医療情報システムの安全管理に関するガイドライン**」では、
  - 真正性とは、正当な権限において作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。



結構バラバラ...

# 真正性って??

- 「ISO27000」では、

- エンティティは、それが主張する通りのものであるという特性。

主張通り

ISO

- 「Wikipediaの情報セキュリティ」の項目では、

- ある主体又は資源が、主張どおりであることを**确实**にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
- 情報システムの利用者が、确实に本人である**ことを確認**し、なりすましを防止すること

主張通り

Wiki

本人確認

なり防止

- 「医療情報システムの安全管理に関するガイドライン」では、

- 真正性とは、正当な権限において作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。なお、混同とは、患者を取り違えた記録がなされたり記録された情報間での関連性を誤ったりすることをいう。

正当権限

医療ガイド

主張通り

書換防止

消去防止

混同防止

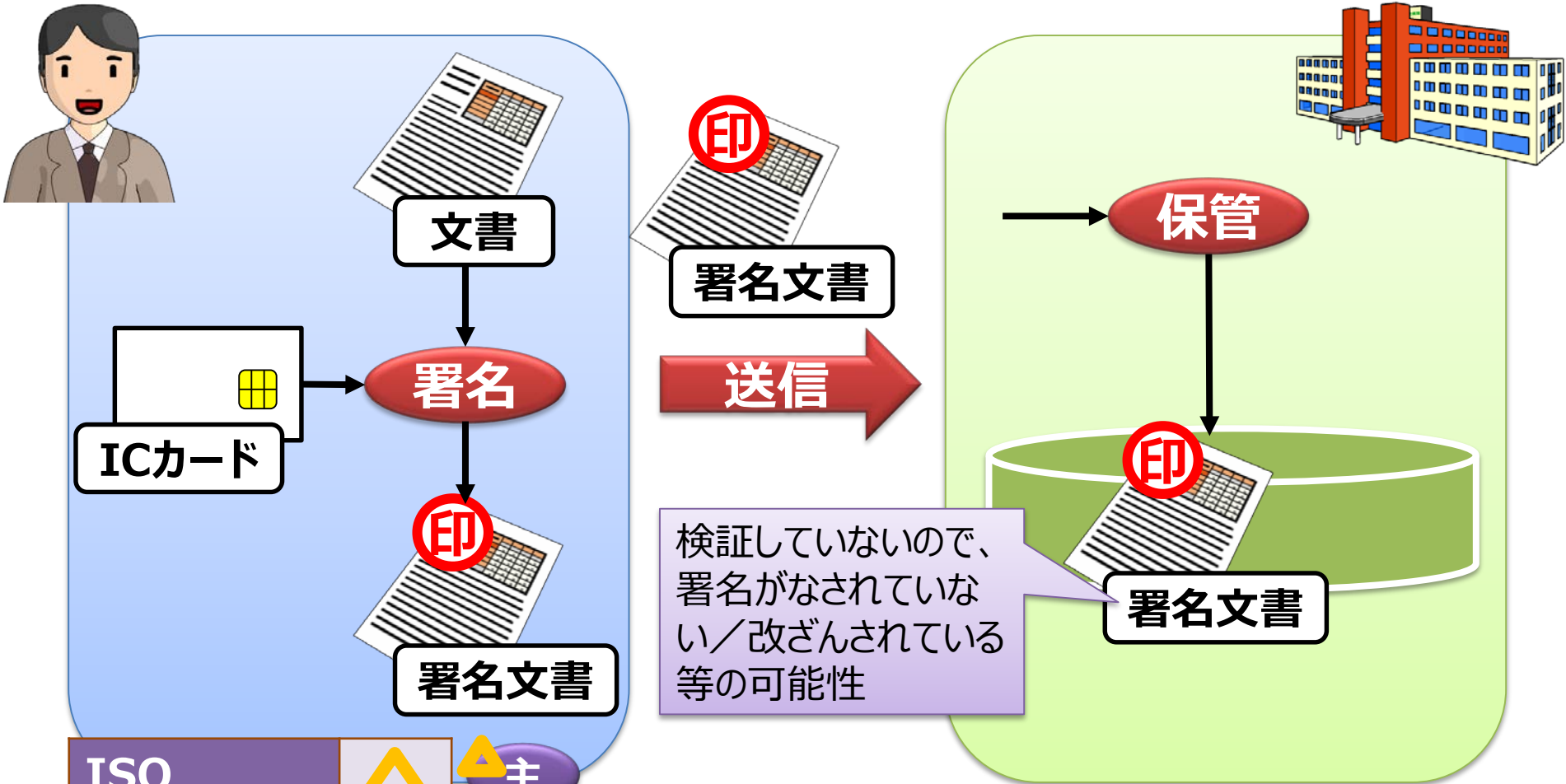
本人確認

なり防止

否認防止



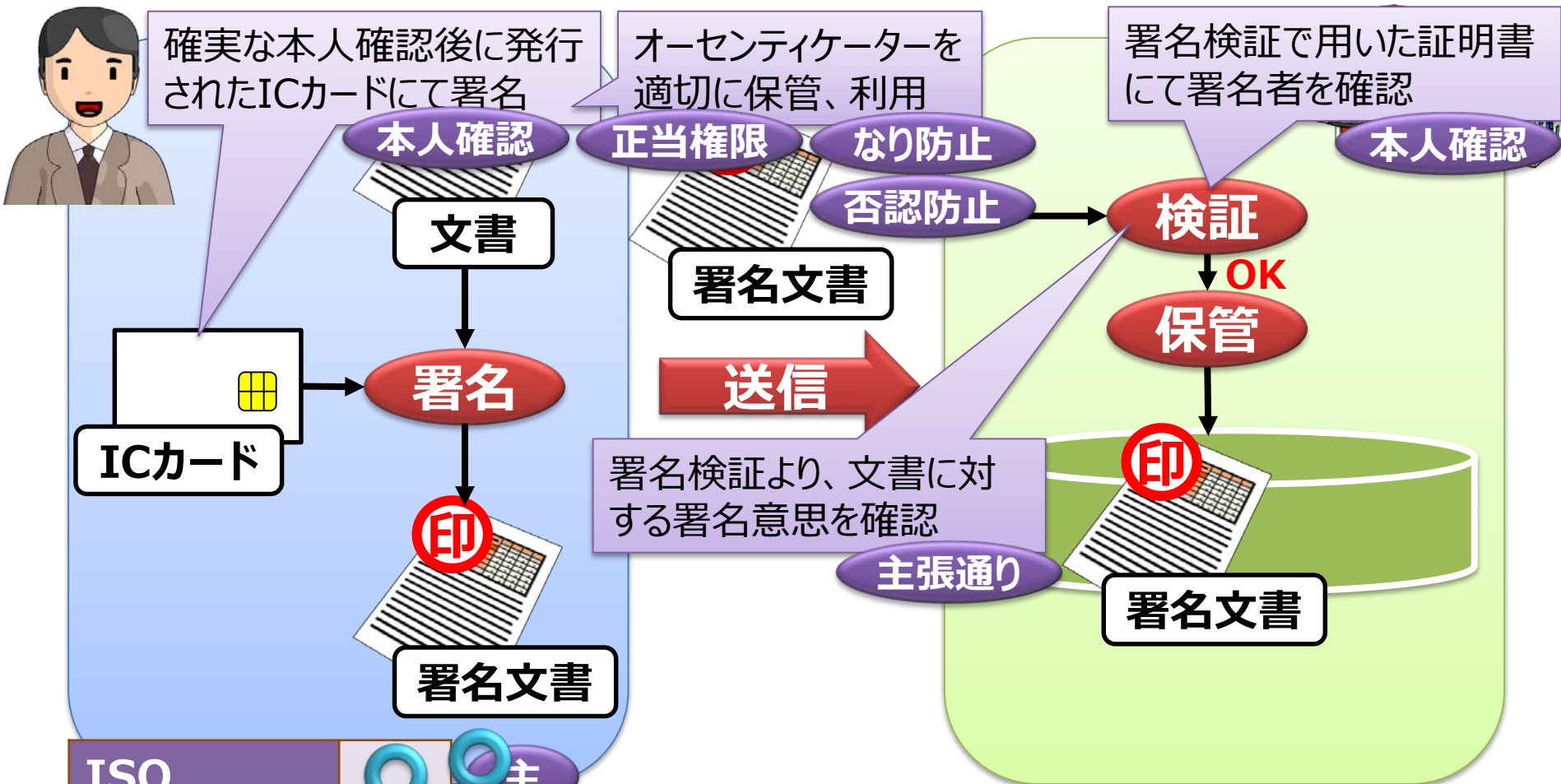
この文書は真正性を保証していると言える??



検証していないので、  
署名がなされていない/  
改ざんされている  
等の可能性

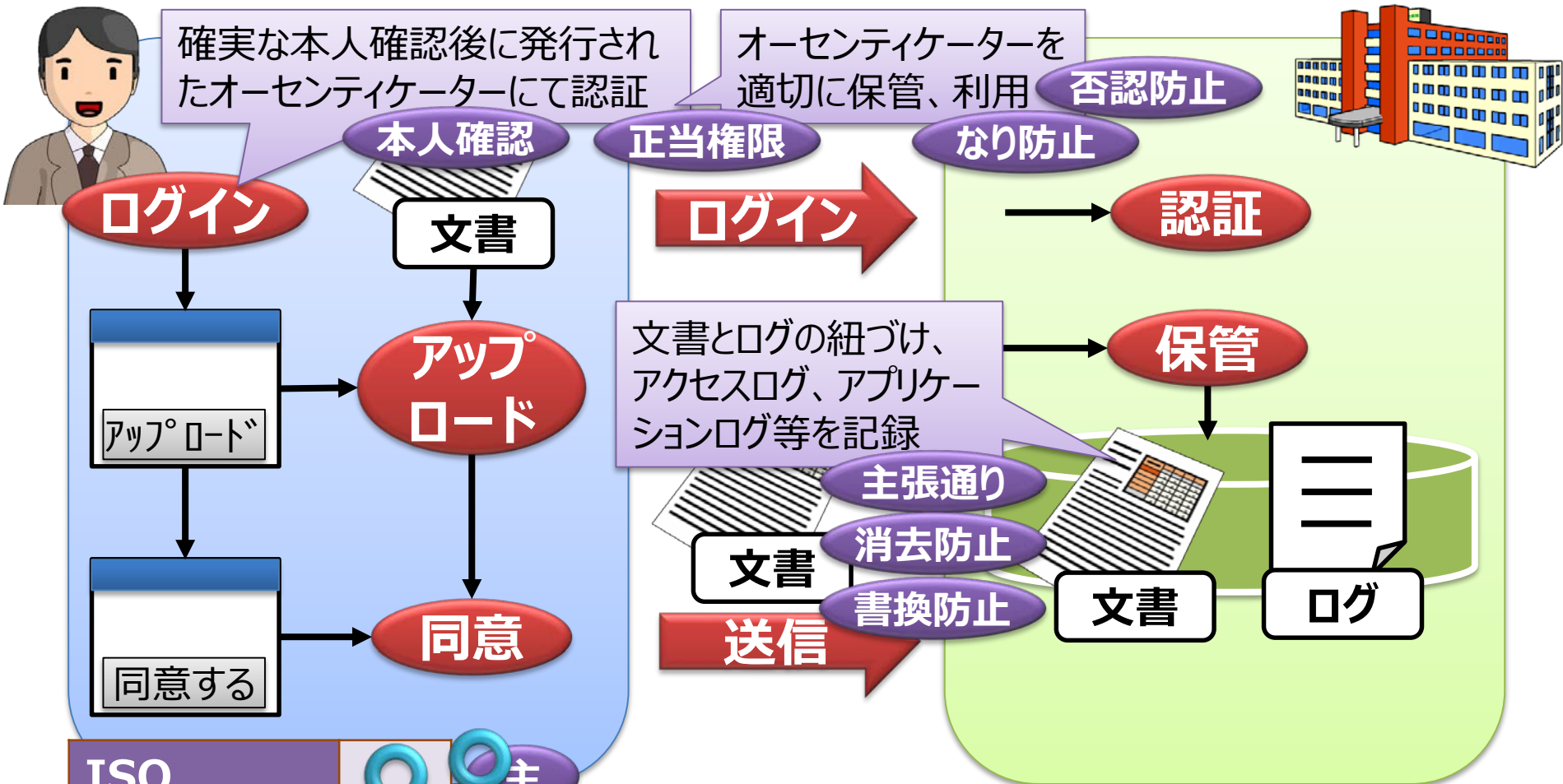
ISO	△	主																		
Wiki	△	主	本	な																
医療ガイド	×	主	本	な	否	正	書	消	混											

## この文書は真正性を保証していると言える??




ISO	<input type="radio"/>	<input type="radio"/>	主
Wiki	<input type="radio"/>	<input type="radio"/>	主 本 な
医療ガイド	<input checked="" type="radio"/>	<input type="radio"/>	主 本 な 否 正 書 消 混

## この文書は真正性を保証していると言える??



ISO	<input type="checkbox"/>	<input type="checkbox"/>	主
Wiki	<input type="checkbox"/>	<input type="checkbox"/>	主
医療ガイド	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	主

主  本  な  否  正  書  消  混

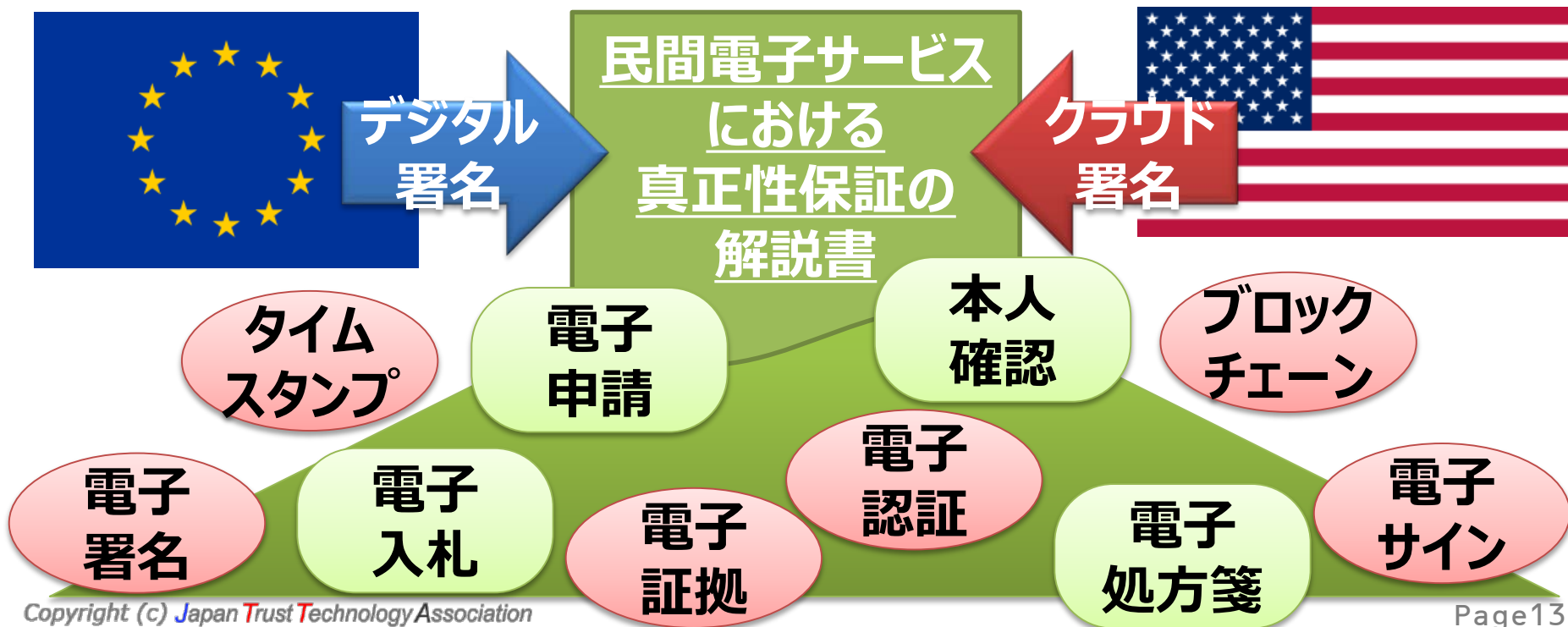


真正性って  
どうすれば  
保証できるんだろう？

真正性って  
定義がバラバラ  
だな。。。。

いい解説書  
ないかなあ。。。。

- JT2A真正性保証TFでは、民間電子サービスを対象とした、開発者／ユーザ向けの真正性保証の解説書を作成。真正性に関連するユースケースや技術を解説。
- 解説書には欧米で主に利用されている技術も含む。
  - 欧州型：**デジタル署名**ベース
  - 米国型：**クラウド署名（電子認証＋電子証拠）**ベース



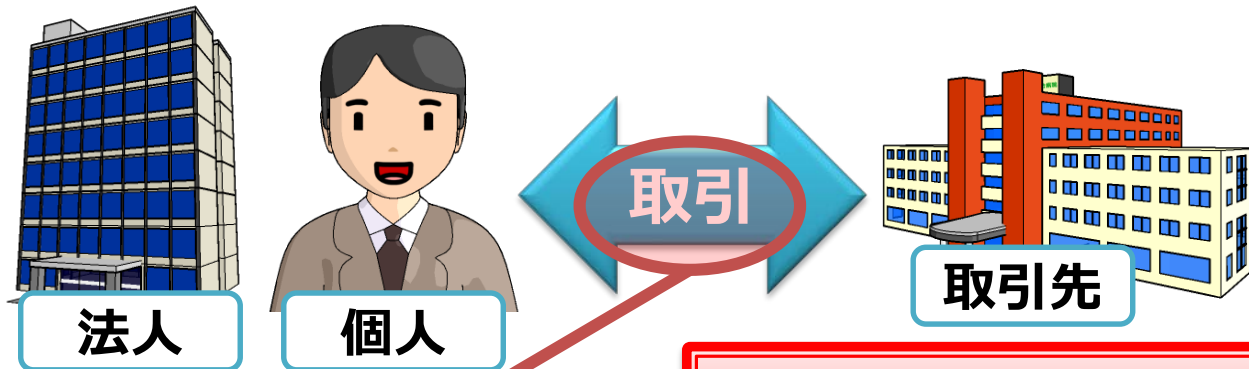
## 民間電子 サービス における 真正性保証の 解説書

### 目次

1. はじめに
2. 真正性とは
3. 真正性の保証が求められるケースの一例
4. 真正性保証レベルの定義
5. 真正性を保証するための実装方法



## 3. 真正性の保証が求められるケースの一例（本人確認を例に）



利用される**真正性保証に関する技術**の記載

• 預貯金口座の開設  
• 大口現金取引  
• クレジットカード交付契約の締結  
などの取引の場合、  
**犯罪による収益の移転防止に関する法律**  
の対象となり、**本人特定事項の確認**  
が求められる。

• **商業登記法**に基づく電子証明書による**電子署名**の確認  
• ...

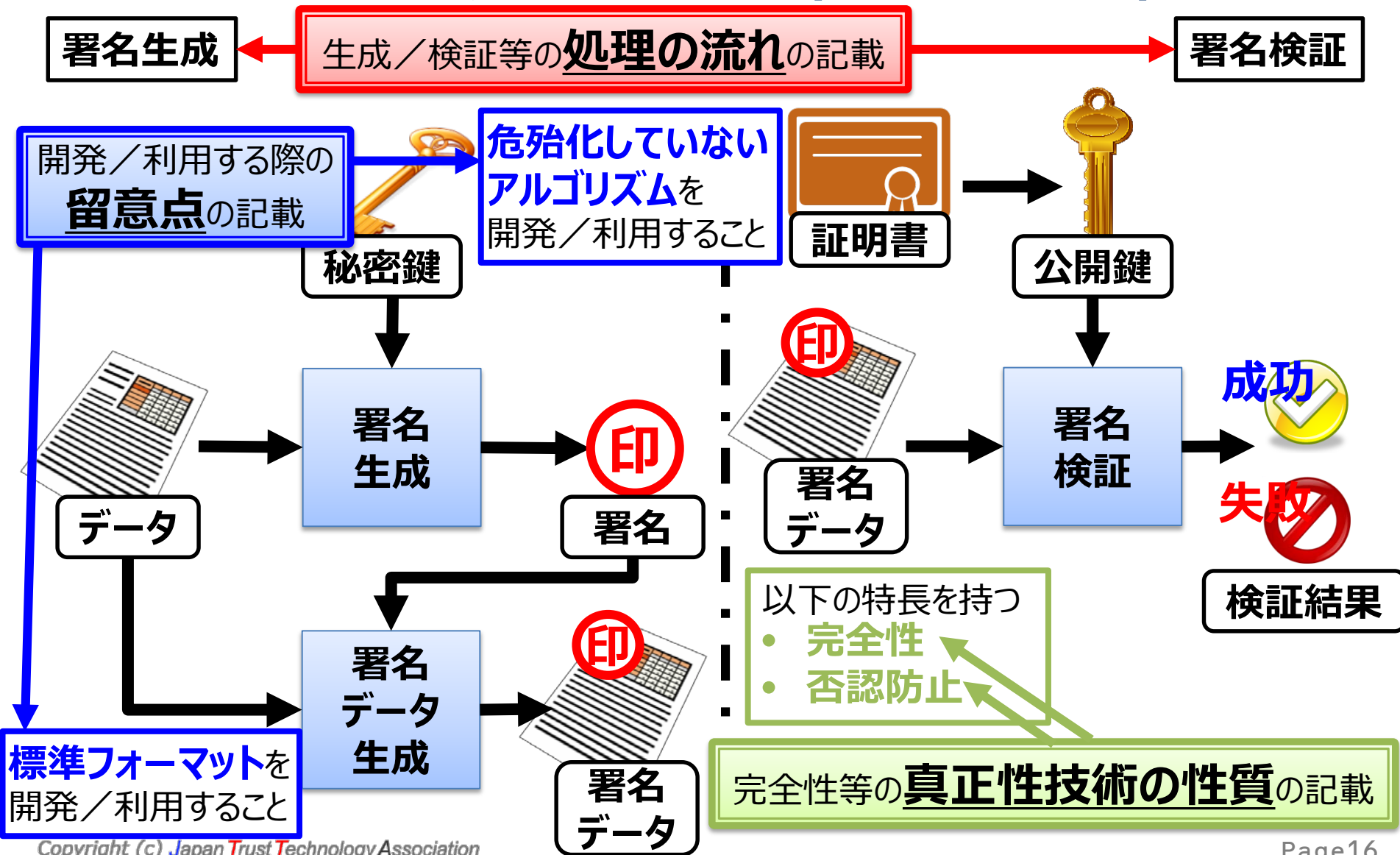
法人

• **電子署名法／公的個人認証法**  
に基づく電子証明書による**電子署名**  
の確認  
• ...

個人

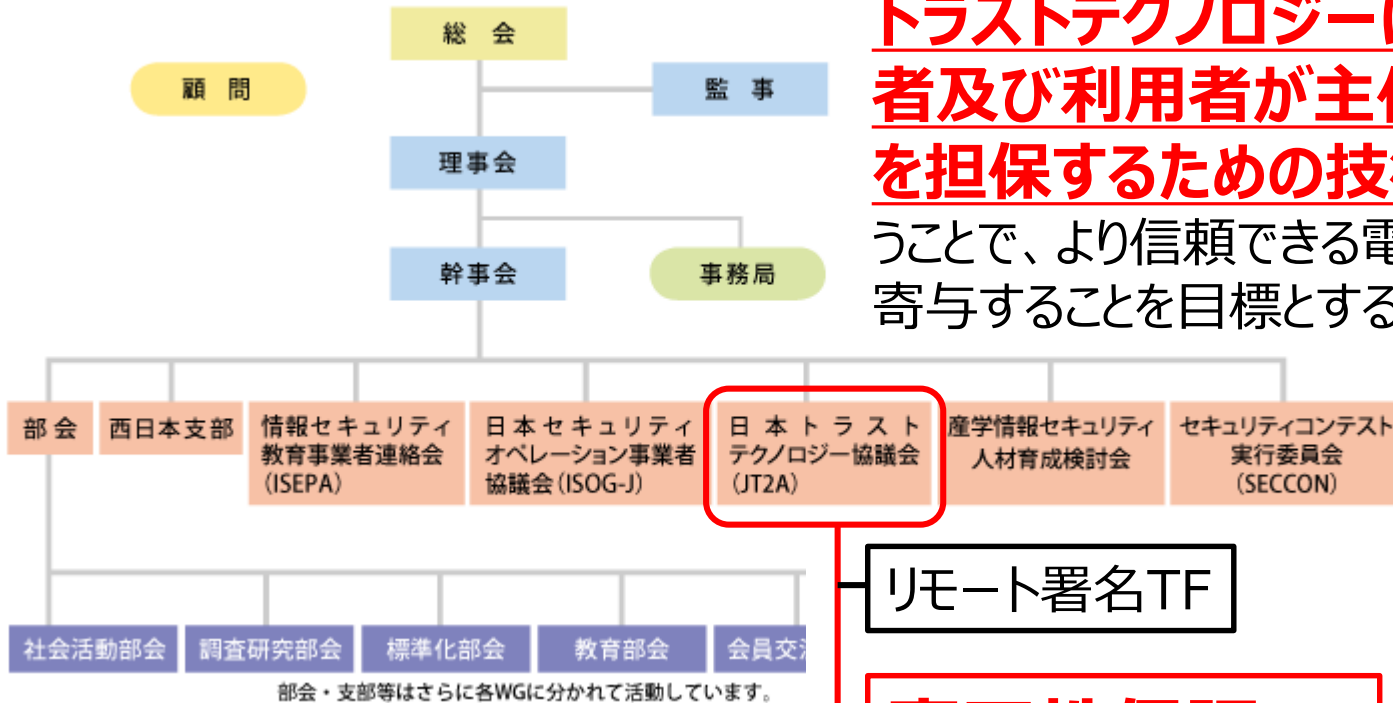
関係する**法規則／ガイドライン**の記載

## 5. 真正性を保証するための実装方法（電子署名を例に）





電子署名・電子証明書や電子認証などの  
**トラステクノロジーに関連する事業者及び利用者が主体となり、信頼性を担保するための技術等の検討**を行うことで、より信頼できる電子社会の促進に寄与することを目標とする団体



リモート署名TF

**真正性保証TF**

リーダー  
山中（三菱電機）  
サブリーダー  
宮地（ラング・エッジ）

## 18年度活動

1. 「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の改定

2. 真正性保証の解説書を作成

ご興味ある方は・・・



**JT2Aで  
ぜひ一緒に活動  
しましょう！**

ご清聴ありがとうございました