JNSA電子署名WG五月祭
JNSA電子署名WG/スキルアップTF

電子署名入門

2016年5月23日

セイコーソリューションズ株式会社
戦略事業開発部
ST開発2課
村尾　進一

アジェンダ

- 電子署名とは
  - リアルの署名押印と電子署名の対比

- 電子署名の要素技術
  - RSA暗号とは
  - ハッシュ関数とは
  - デジタル署名（RSA）とは
  - 公開鍵基盤（PKI）とは
  - 電子署名の検証
  - デジタル署名の検証方法

- タイムスタンプについて
  - タイムスタンプの概要
  - タイムスタンプの仕組み
  - 認定制度（時刻のトレーサビリティについて）

- 電子署名・タイムスタンプのまとめ

電子署名とは

いきなり、私事で恐縮ですが、昨年、

生まれて初めて車を買いました。一応、新車で！

自動車登録の委任状で実印＋印鑑証明書を使用しました。

生まれて初めて家を買いました。仲介の中古物件で！

売買契約書等で実印＋印鑑証明書を使用しました。

生まれて初めて住宅ローン組みました。ネット銀行で！

住宅ローン契約書で実印＋印鑑証明書を使用しました。

電子署名とは

いきなり、私事で恐縮ですが、昨年、

生まれて初めて車を買いました。一応、新車で！

自動車登録の委任状で実印＋印鑑証明書を使用しました。

販売店が車で行ける所にしか無くて大変！

生まれて初めて家を買いました。仲介の中古物件で！

売買契約書等で実印＋印鑑証明書を使用しました。

重要事項説明を含めて対面で契約！

生まれて初めて住宅ローン組みました。ネット銀行で！

住宅ローン契約書で実印＋印鑑証明書を使用しました。

契約手続きはひたすら郵送と電話！

これらが電子化できたら・・・・

電子署名とは

リアルの世界の署名／記名・押印とは

商法（三十二条）

この法律の規定により署名すべき場合には、
記名押印をもって、**署名に代えること**ができる。

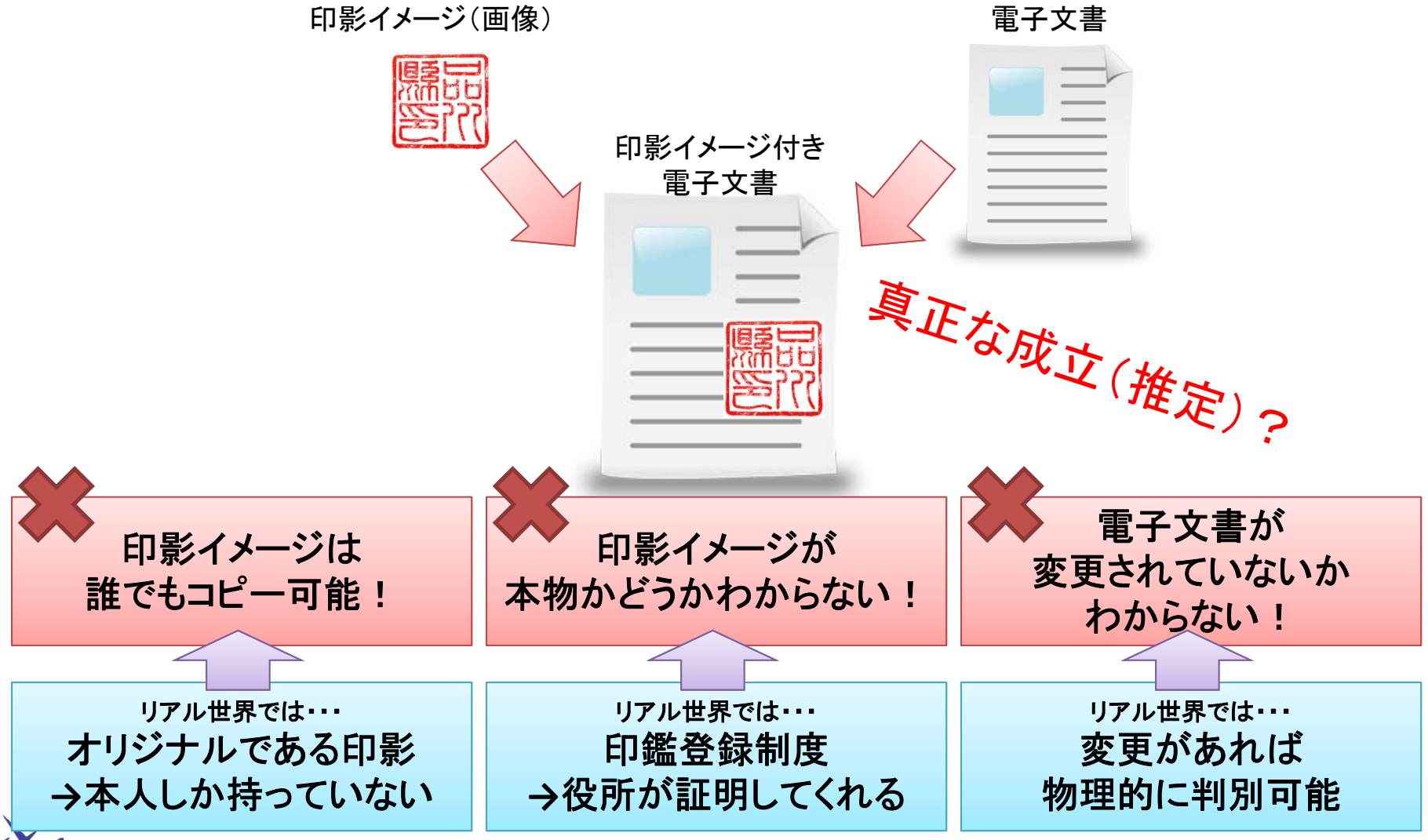
民事訴訟法（第二百二十八条）

１　文書は、その成立が**真正であることを証明**しなければならない。
４　私文書は、本人又はその代理人の署名又は**押印**があるときは、
真正に成立したものと推定する。

真正な成立（推定）

電子署名とは

それでは、電子の世界で、印影イメージ（画像）を電子文書に貼り付けたら「電子署名」？



電子署名とは

電子世界の署名／記名・押印とは

電子署名法　第二条（電子署名及び認証業務に関する法律）

この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

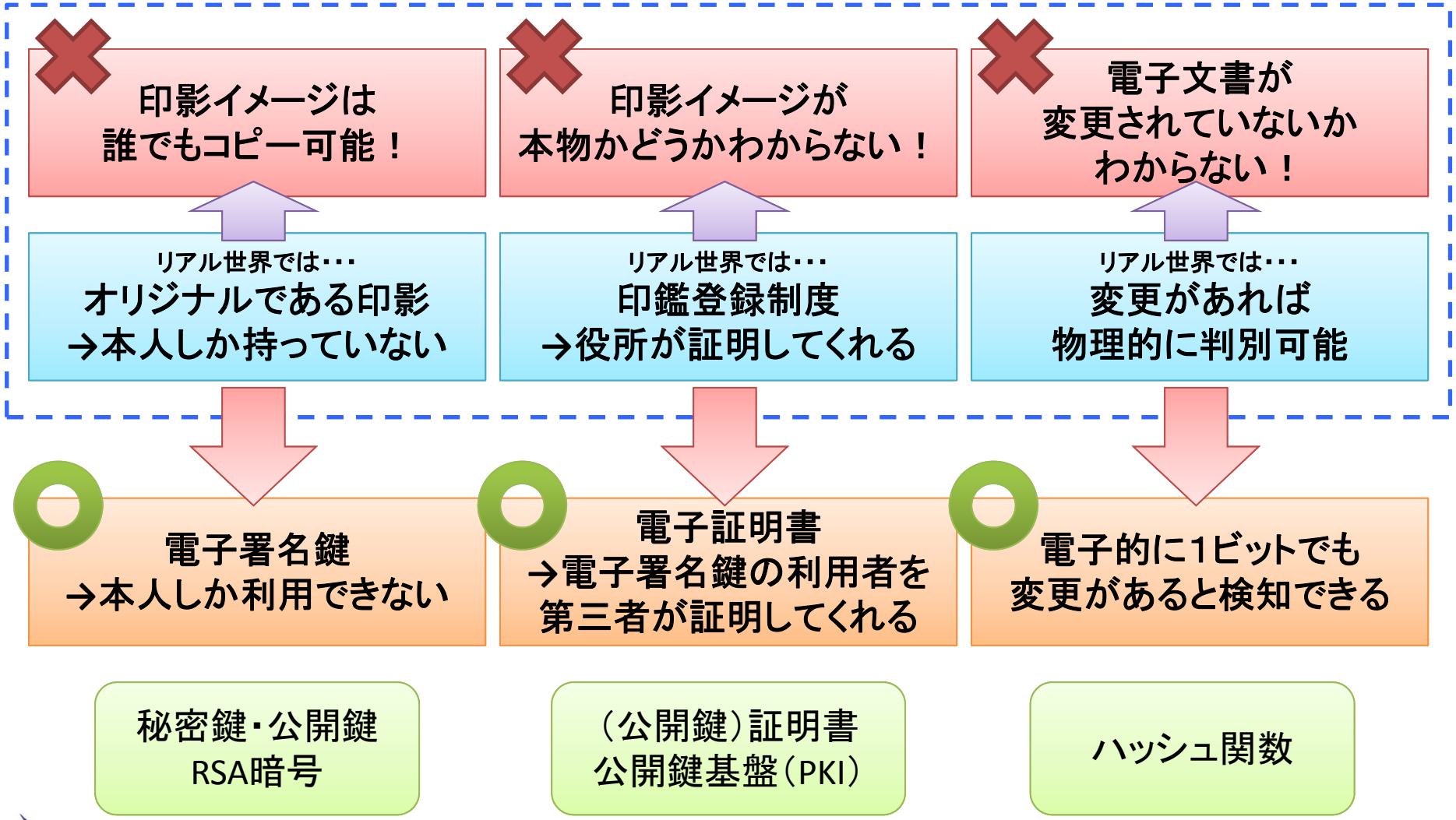
一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
二　当該情報について改変が行われていないかどうかを確認することができるものであること。

電子署名法　第三条（電子署名及び認証業務に関する法律）

電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

電子署名とは

電子世界の署名／記名・押印の課題を解決する手段は？

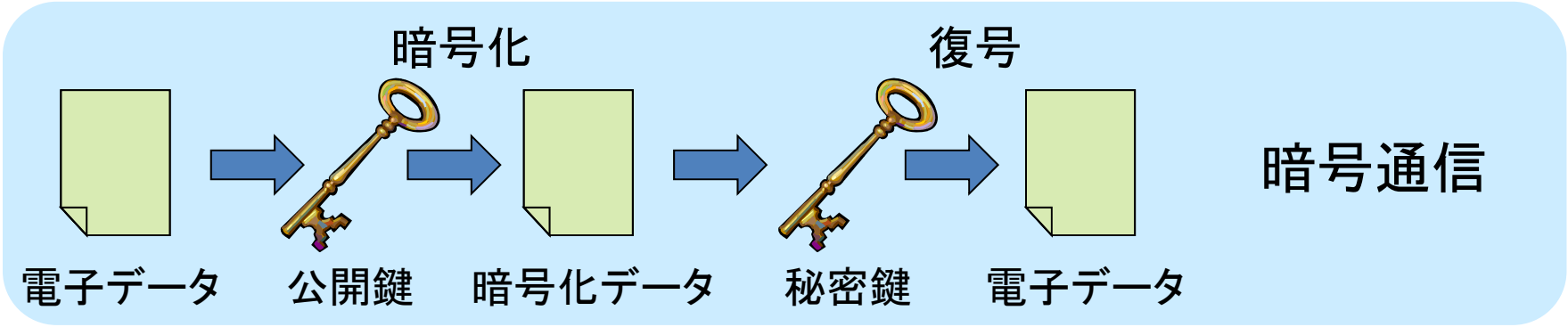


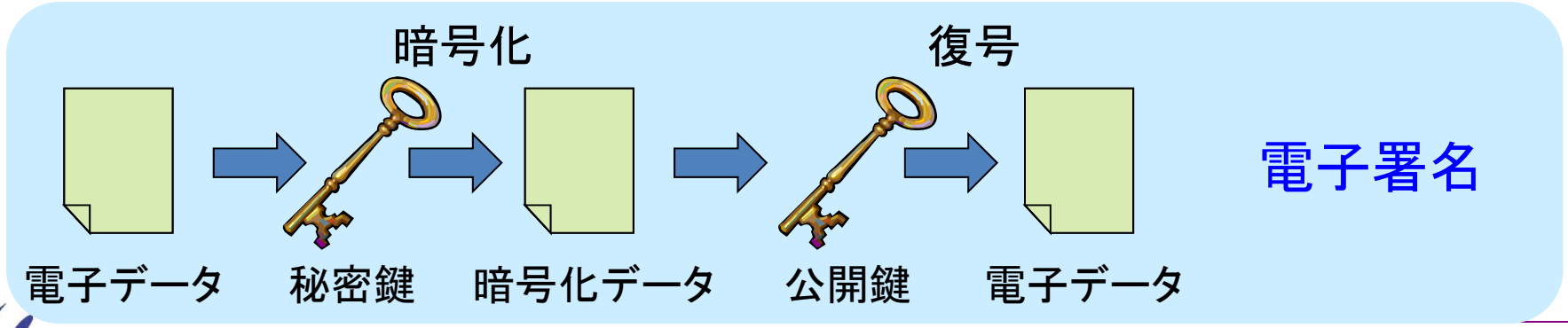
RSA暗号とは

RSA暗号とは、桁数が大きい合成数の**素因数分解問題が困難**であることを安全性の根拠とした**公開鍵暗号**の一つである。暗号 (Cipher) とデジタル署名 (Digital signature) を実現できる方式として最初に公開されたものである。（出典：Wikipedia）

暗号鍵は秘密鍵と公開鍵のペアで作成！

片方の鍵（公開鍵）で暗号化した情報は、
もう片方の鍵（秘密鍵）でないと復号できない！





RSA暗号とは

RSA暗号とは、桁数が大きい合成数の**素因数分解問題が困難**であることを安全性の根拠とした**公開鍵暗号**の一つである。暗号 (Cipher) とデジタル署名 (Digital signature) を実現できる方式として最初に公開されたものである。（出典：Wikipedia）

暗号鍵は秘密鍵と公開鍵のペアで作成！

片方の鍵（公開鍵）で暗号化した情報は、
もう片方の鍵（秘密鍵）でないと復号できない！

・RSA暗号の強度は鍵の長さに依存
鍵の長さ：1024ビット（安全性低下）、2048ビット、3072ビットなど

・鍵の長さより短いデータにのみ利用できる

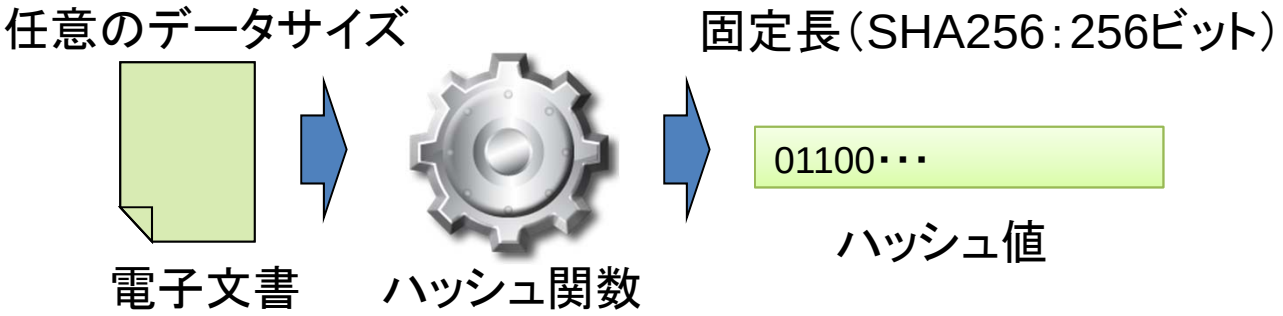
署名対象の電子文書を鍵の長さより短くできれば・・・

ハッシュ関数とは

ハッシュ関数 (ハッシュかんすう、**hash function**) とは、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のこと。

ハッシュ関数から得られた数値のことを**ハッシュ値**または単に**ハッシュ**という。

（出典：Wikipedia）



電子データに対する電子的な指紋

（1ビットでも違うとまったく異なる値になる）

ハッシュ値から元電子文書は再現できません

・文字「1」(0x31)のSHA256ハッシュ値（16進数）：

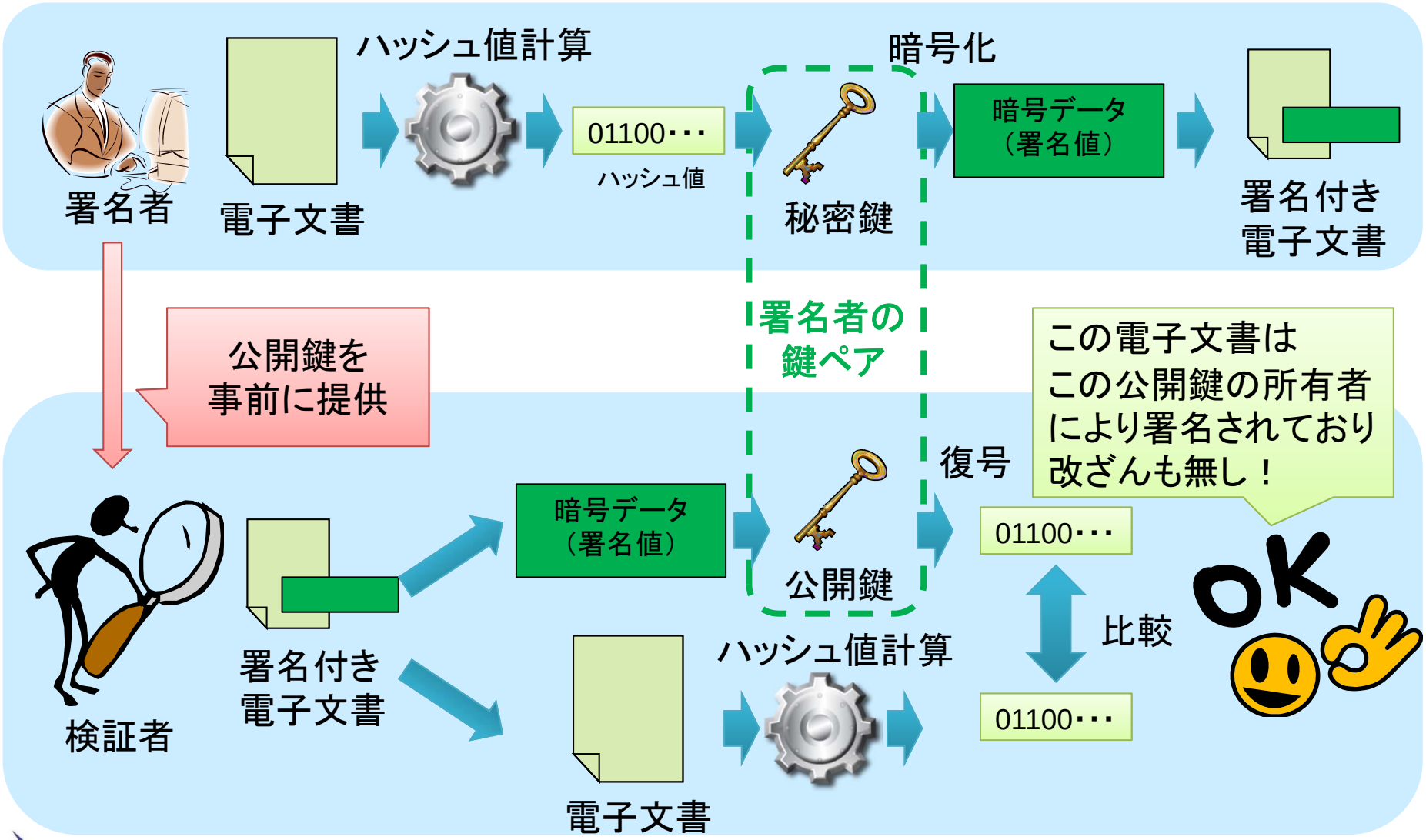
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

・文字「2」(0x32)のSHA256ハッシュ値（16進数）：

d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35

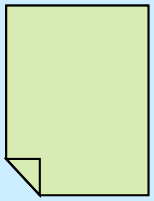
デジタル署名（RSA）とは

RSA暗号とハッシュ関数を組み合わせることで



公開鍵の配布問題

署名者



電子文書

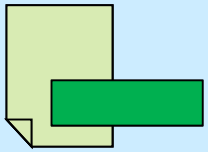
例えば、署名者から検証者に**電子メール**で送付？

なりすまし・差し替えの危険性
（送信元が本人かどうか・・・）

公開鍵を
事前に提供

署名者本人から直接手渡しなどの**安全な方法**で
入手する必要がある

検証者

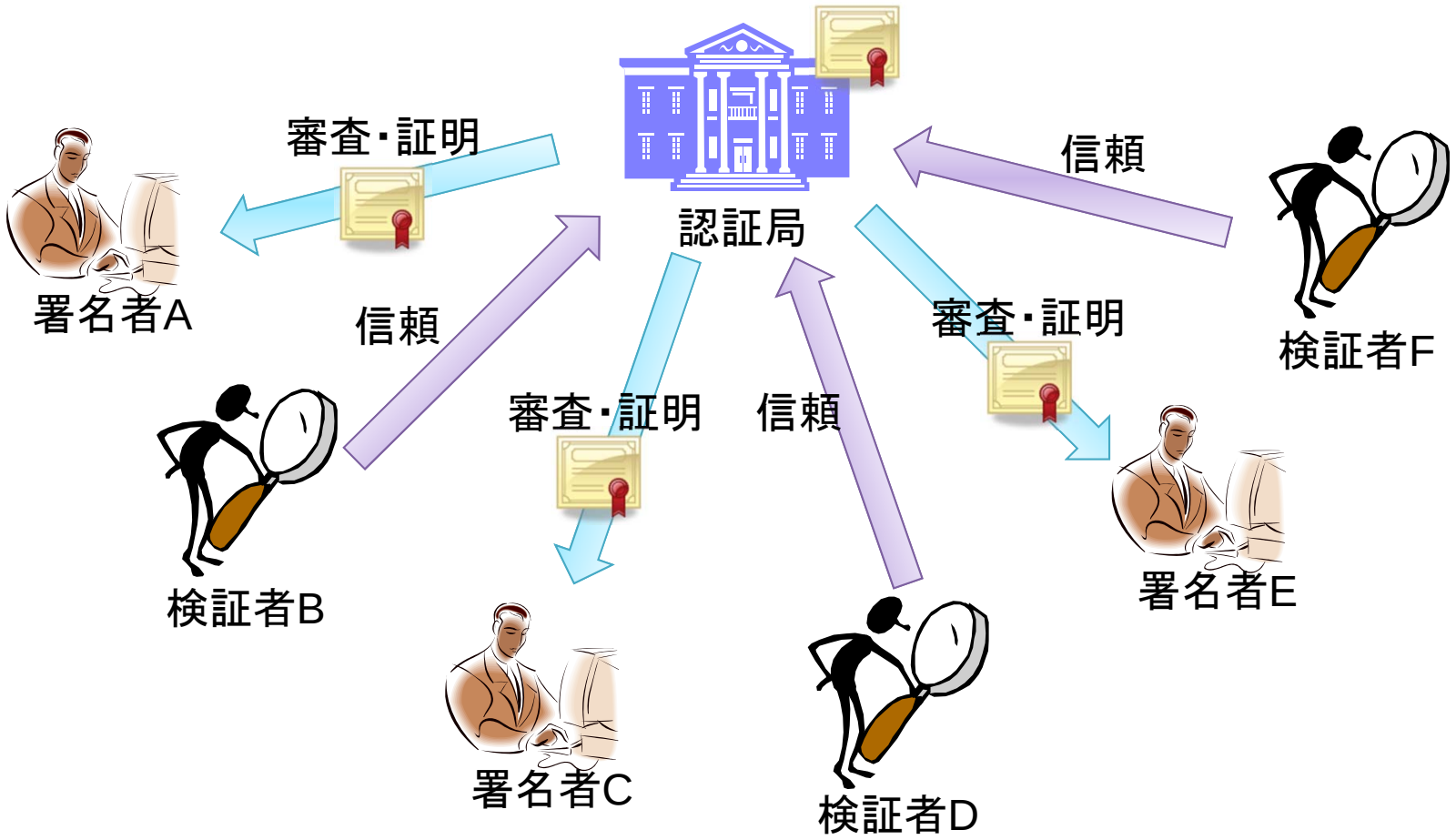


署名付き
電子文書

個人同士（1対1）ならさほど問題無いが、
ビジネス（N対N）となると実用的でない！

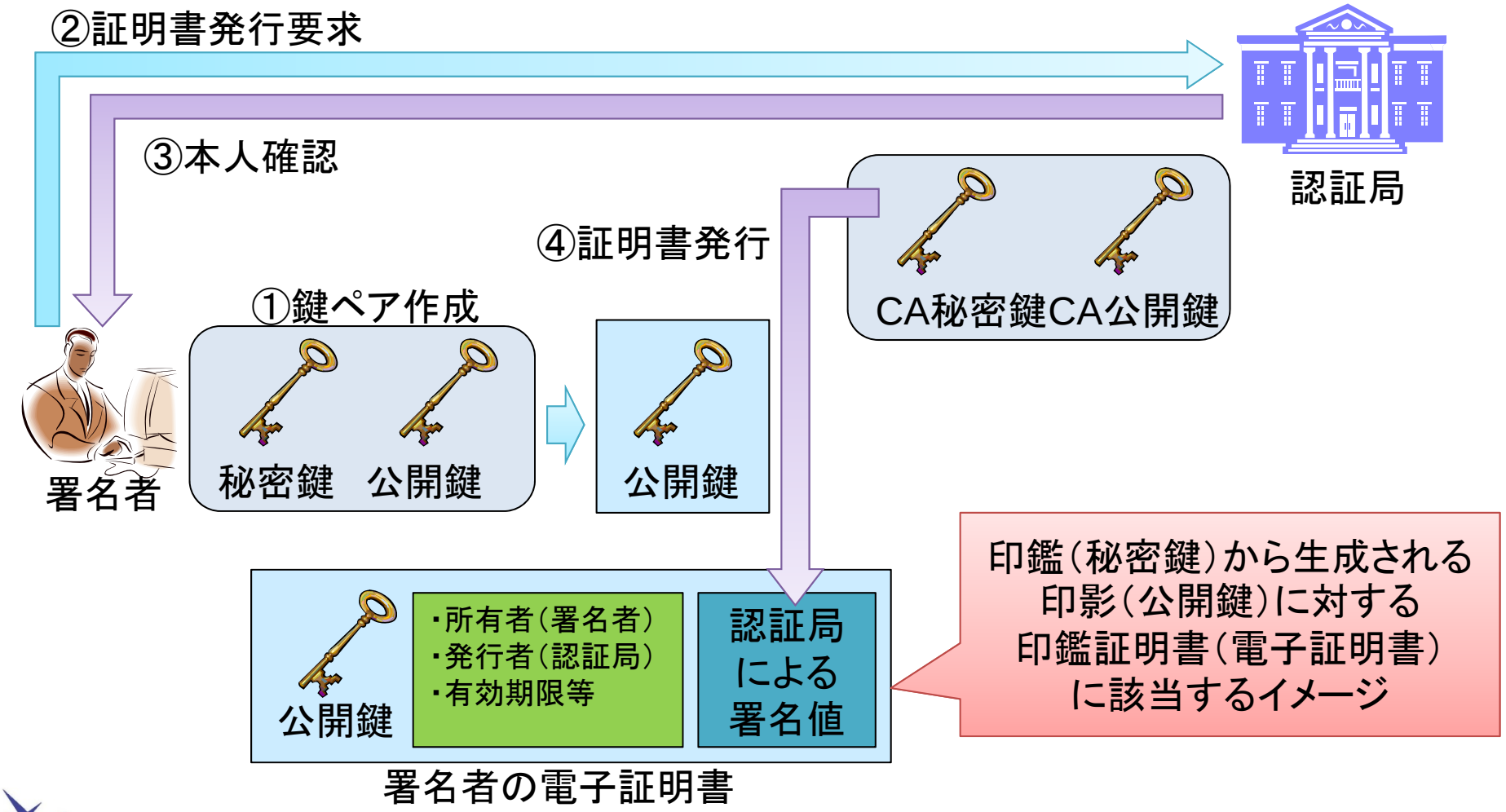
公開鍵基盤（PKI）とは

暗号技術において、**公開鍵基盤**（こうかいかぎきばん、英: public key infrastructure、以下**PKI**）は、利用者の身元について**「信頼できる第三者」**（英: trusted third party）が審査を行い、保証を実現する仕組みのことである（出典：Wikipedia）

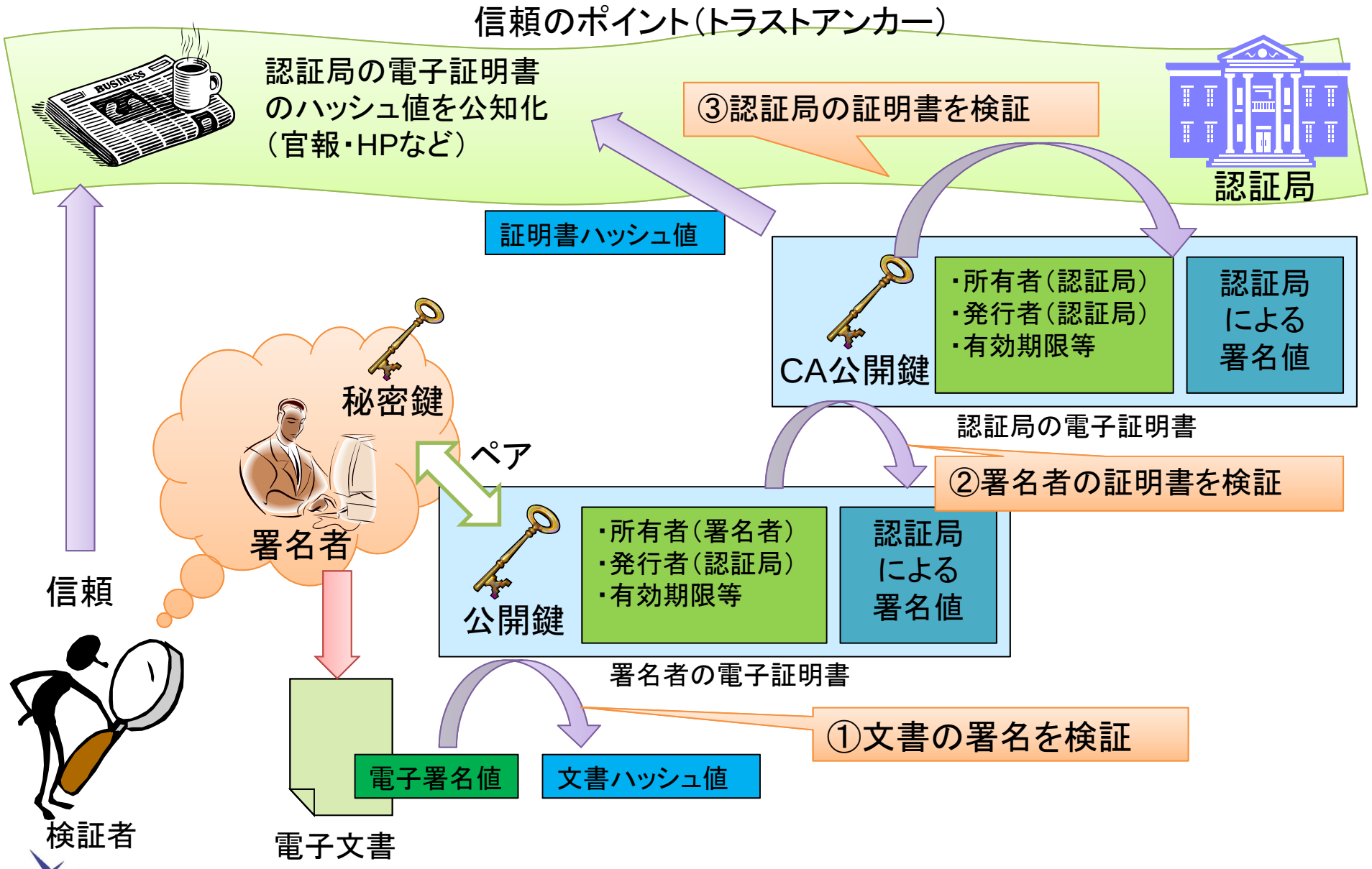


公開鍵基盤（PKI）とは

暗号技術において、**公開鍵基盤**（こうかいかぎきばん、英: public key infrastructure、以下**PKI**）は、利用者の身元について**「信頼できる第三者」**（英: trusted third party）が審査を行い、保証を実現する仕組みのことである（出典：Wikipedia）



デジタル署名の検証方法



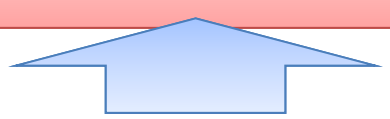
デジタル署名の有効期限・失効について

1. 電子証明書には有効期限が設定されています（通常5年未満）
   - ・鍵の暗号アルゴリズムの危殆化、紛失・漏えいリスクへの対応のため
   - ・認証情報のリフレッシュのため

2. 電子証明書に紐付く秘密鍵を紛失・漏えいした場合は失効申請ができます
   - ・失効情報（CRL：Certificate Revocation List）が公開されます
   - ・失効情報は電子証明書の有効期限内のみ失効状態が記載されます

有効期限が切れた電子証明書は有効性を確認できません

署名付き電子文書の有効性が確認できなくなります



タイムスタンプと**長期署名技術**により延長が可能に！

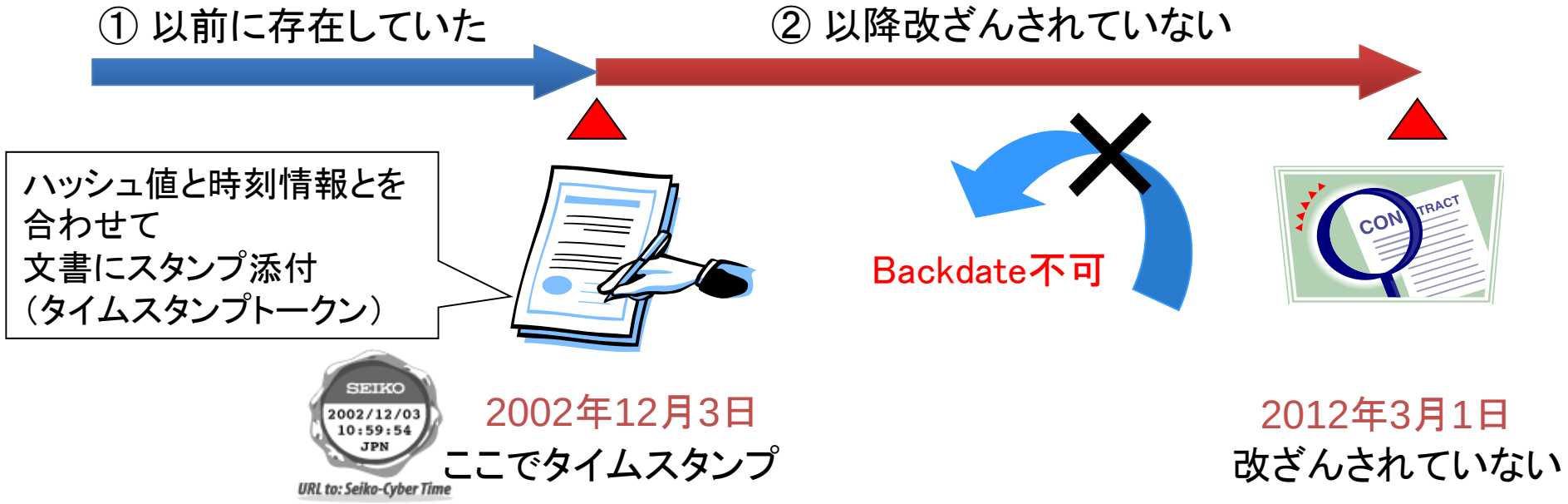
タイムスタンプの概要

電子文書が

① スタンプ時以前に存在していたこと

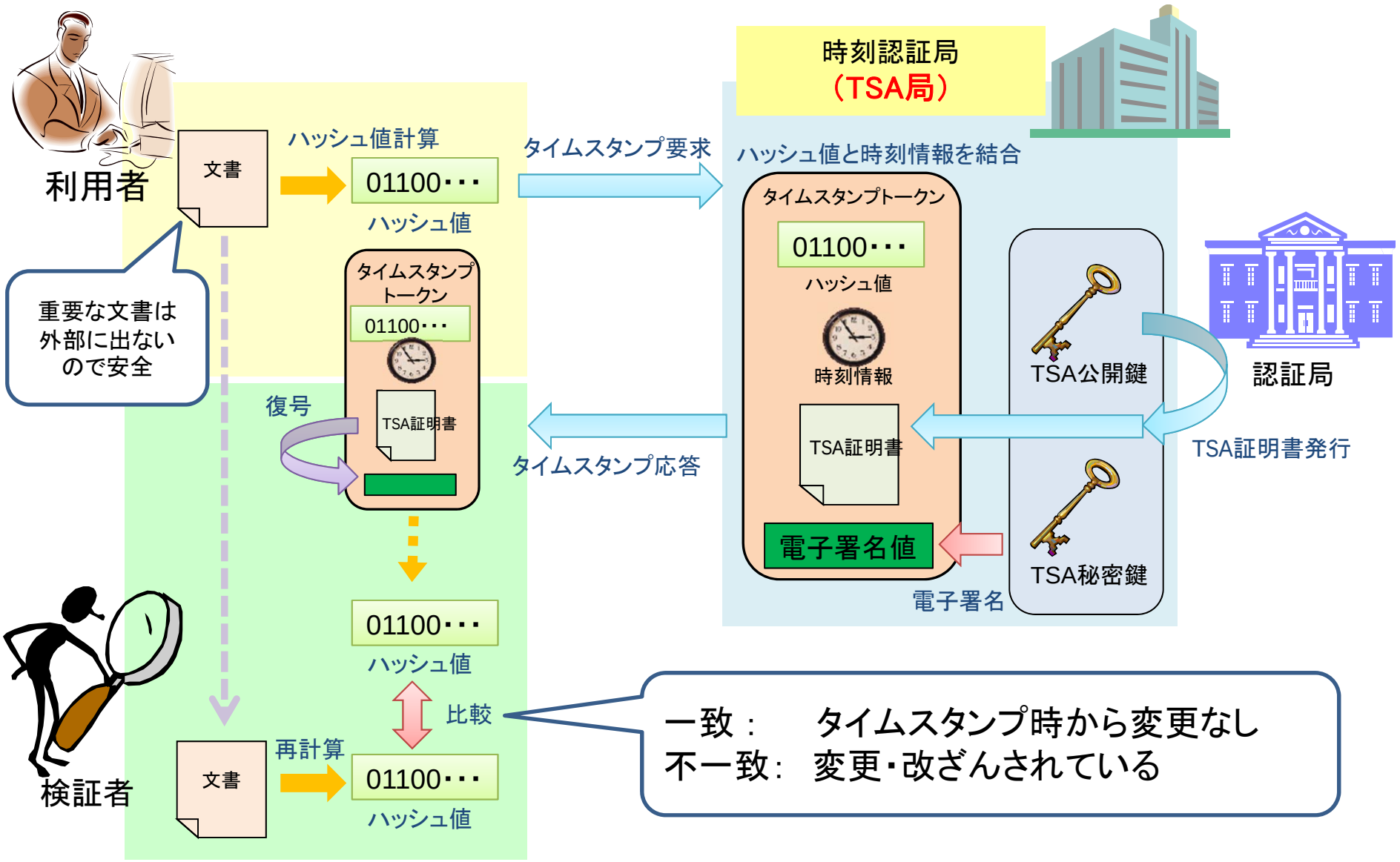
② スタンプ時以降改ざんされていないこと

を証明する仕組み。

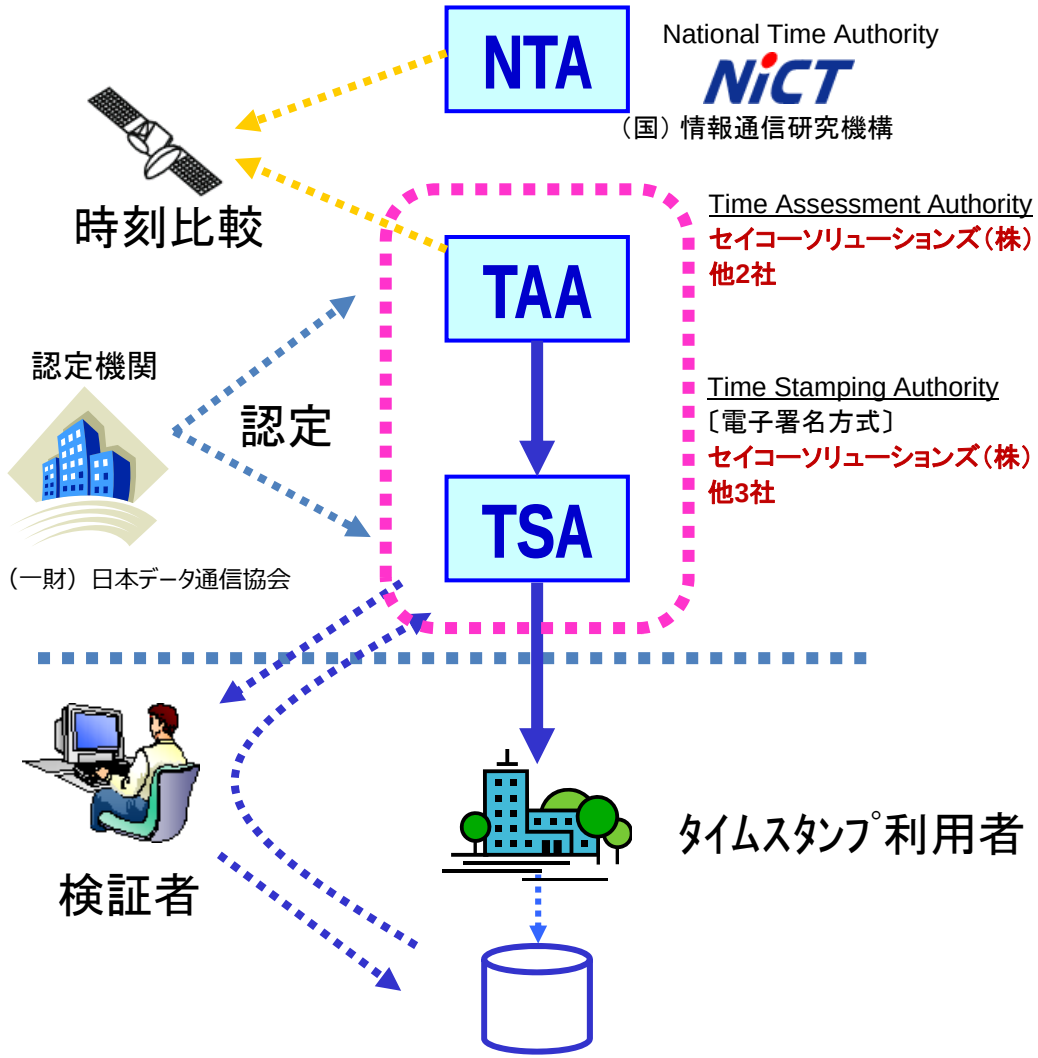


タイムスタンプは、信頼できる時刻を利用した電子文書の証拠性を確保する技術です。

タイムスタンプの仕組み



タイムビジネス信頼・安心認定制度



「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）

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

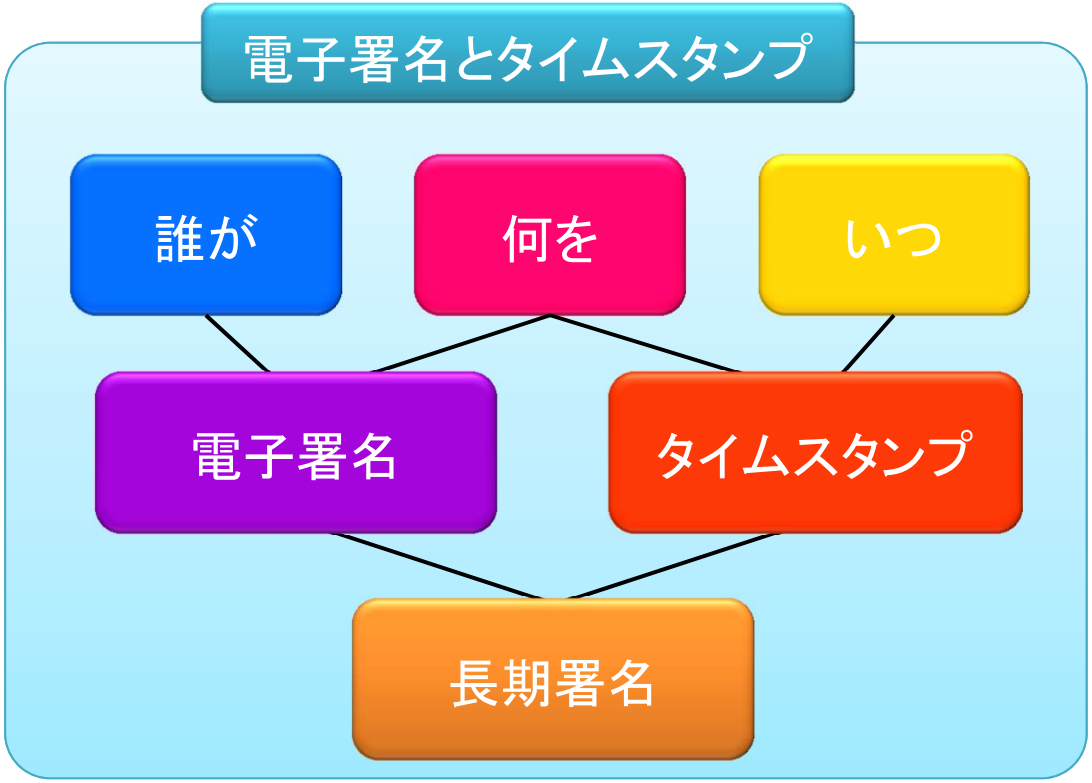
- TSAは、認定TAAからの時刻配信業務を利用すること
- TAAは、NTAが指定した時刻比較および保管すること

信頼できるTAA・TSAの時刻

-JISX5094：2011年5月20日制定
-ISO18014-4：2015/4/15 Published

電子署名・タイムスタンプのまとめ

電子文書の改ざんやなりすましを防ぐための有効な手段として、
電子署名とタイムスタンプがあります。



電子署名は、
「誰が」「何を」
作成したかを証明します。

タイムスタンプは、
「いつ」「何を」
作成したかを証明します。

第三者が発行する電子署名とタイムスタンプを併用することにより、

「誰が」「何を」「いつ」作成したかを**長期的に証明**することができます。

ご清聴ありがとうございました。