第6回タイムビジネスシンポジウム
ー 電子社会におけるタイムビジネスの役割と貢献 ー

『電子文書の長期保証とタイムスタンプ』

技術部会

ガイドライン分科会

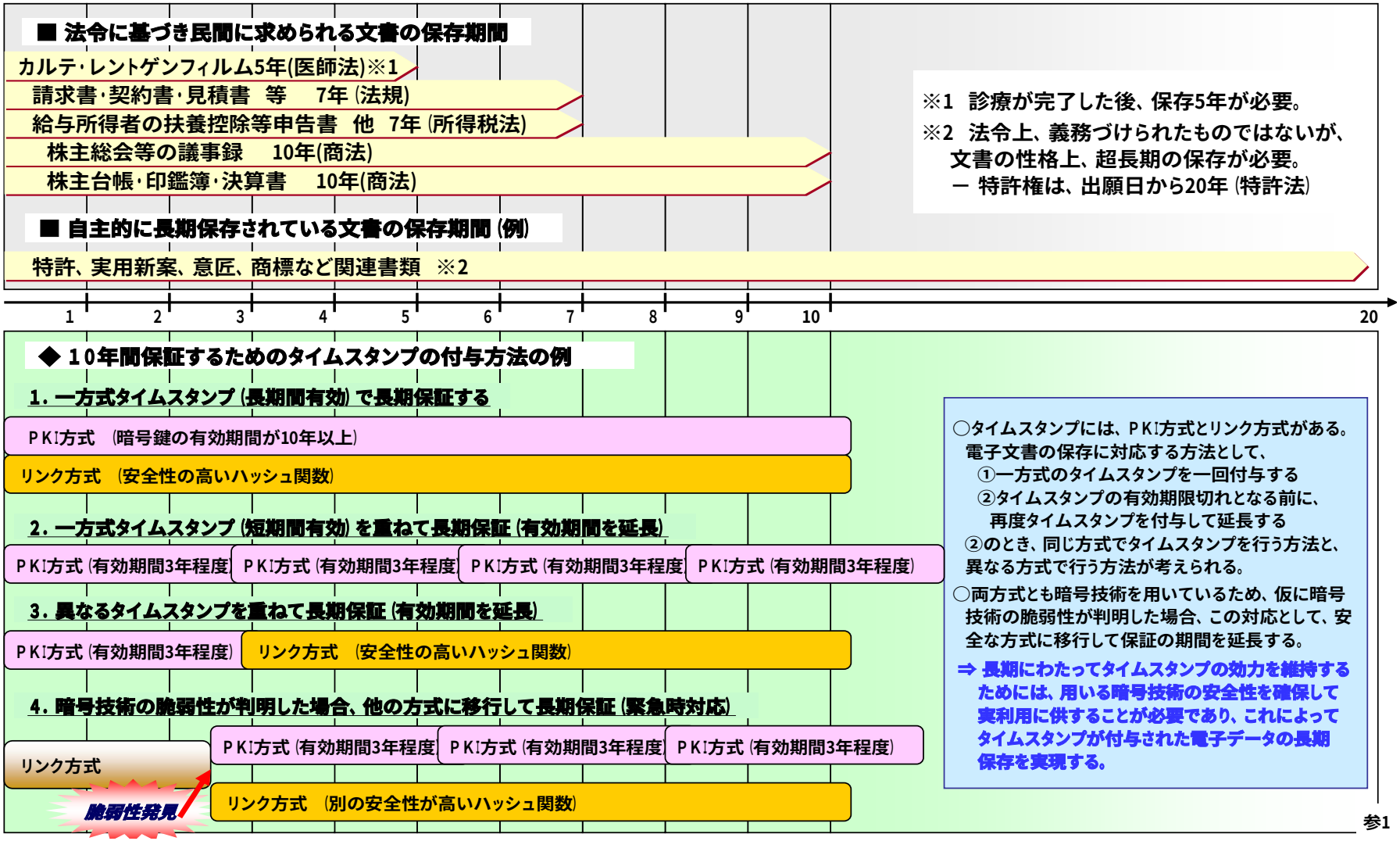
リーダー　宮崎　一哉

『タイムスタンプ長期保証ガイドライン』H17年2月

1　タイムスタンプ長期保証ガイドラインの位置付け

(1) 背景と目的

(参考1)　“文書の保存年数”と“タイムスタンプの保証期間”



出典；第60回ﾃﾚｺﾑ技術情報ｾﾐﾅｰ　時刻認証技術の動向とタイムビジネスの普及 (総務省)

1　タイムスタンプ長期保証ガイドラインの位置付け
(2) 検討の方針

① 長期保証を中心とする
タイムスタンプの「長期保証」に関わる事項に焦点を合わせる

② 中立の姿勢を保つ
代表的なPKI方式とリンク方式の長期保証方法を併記する

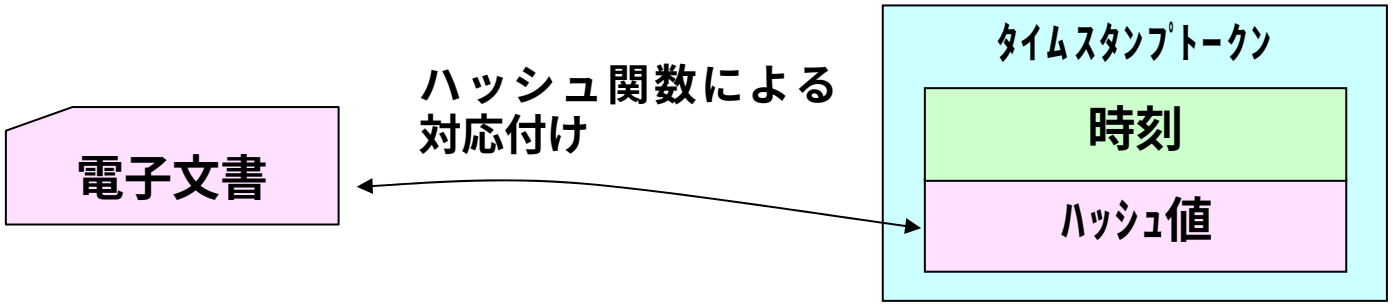
③ 利用・適用の立場から実用を重視する
常に利用の原点に立ち返りつつ、現実的な実装を念頭におく

1　タイムスタンプ長期保証ガイドラインの位置付け
(3) ガイドラインの構成

① 長期保証の要件
　タイムスタンプの有効性と長期保証要件
② 長期保証の方法
　タイムスタンプを重ねる方法、付与対象
③ デジタル署名文書
　ＰＫＩ方式タイムスタンプとの比較
④ 認証局(CA)の要件
　信頼点の問題（ＰＫＩ方式）
⑤ 参考

2　タイムスタンプ長期保証
(1) タイムスタンプの有効性

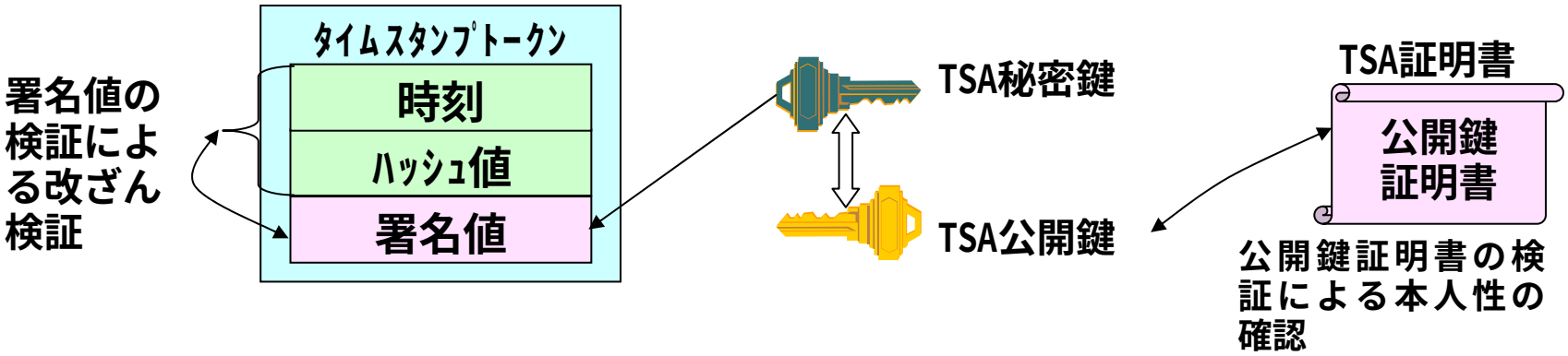
① タイムスタンプがある特定の電子文書のみに対応するものであることを証明できること



② タイムスタンプトークンの非改ざん性を確認できること。

2　タイムスタンプ長期保証
(1) タイムスタンプの有効性

③ タイムスタンプの発行主体を確認できること。

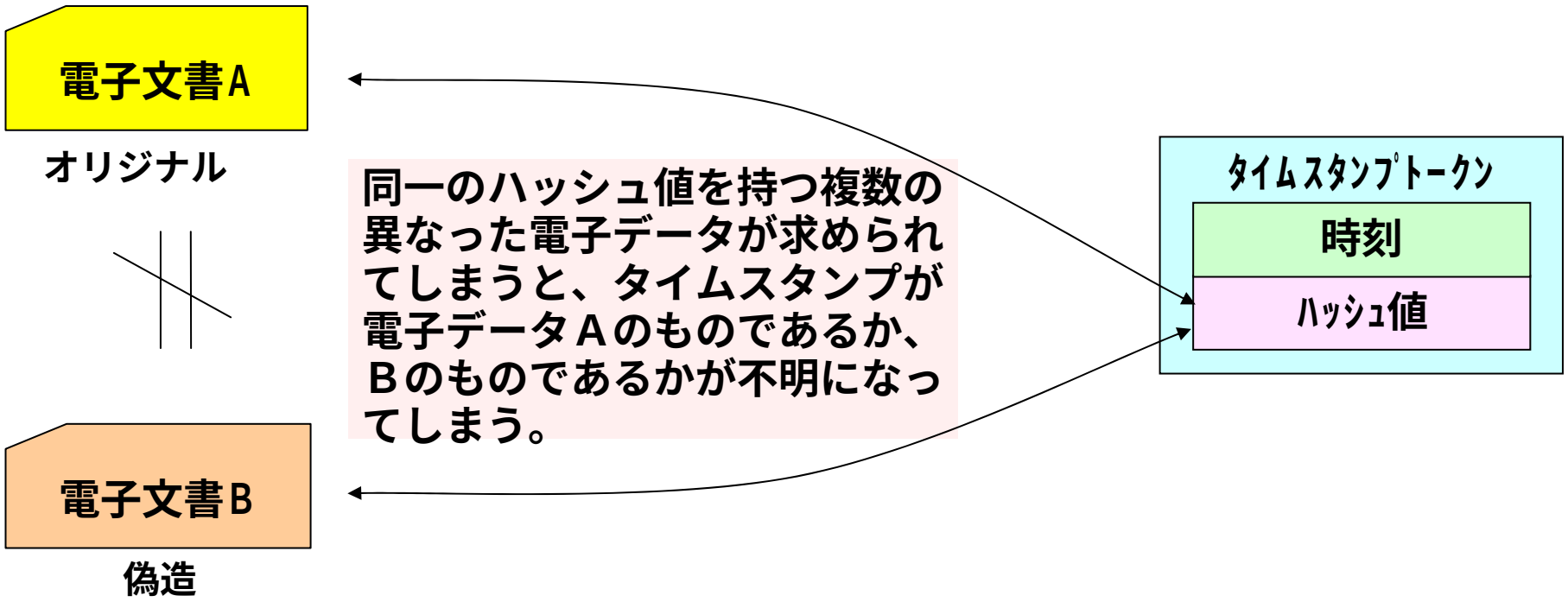


④ 信頼点の正当性を確認できること。

⑤ TSAが適切に運用されていることを確認できること。

2　タイムスタンプ長期保証
(2) タイムスタンプ長期保証の要件

①　長期経過後に電子文書とタイムスタンプとの対応関係を証明できること



2　タイムスタンプ長期保証

(2) タイムスタンプ長期保証の要件

② 長期経過後にタイムスタンプトークンの非改ざん性を確認できること

[PKI方式] アルゴリズムの脆弱化を想定した対処

[リンク方式] 照合用データの滅失／毀損を防止

③ 長期経過後にタイムスタンプの発行主体を確認できること

[PKI方式] 公開鍵証明書の有効期限、失効

[リンク方式] TSAの運営が継続、中断の場合、照合用データ、リンク情報及び検証方法の公開

2　タイムスタンプ長期保証

(2) タイムスタンプ長期保証の要件

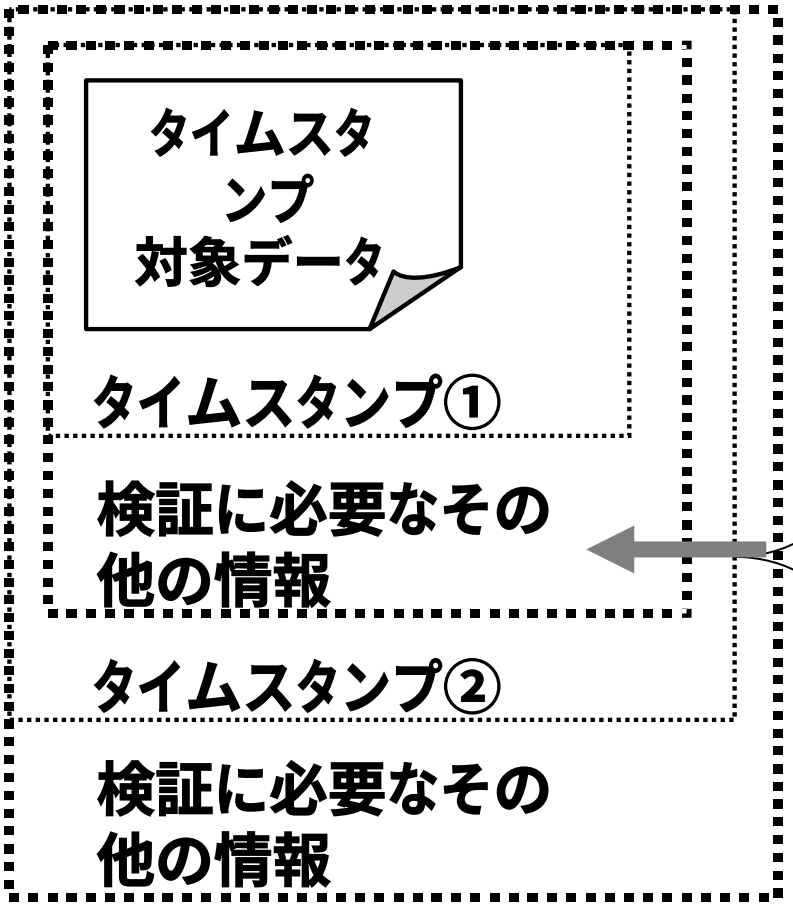
④　長期経過後に信頼点の正当性を確認できること

[PKI方式] 当時の信頼点であることが確認可能

[リンク方式] 公開情報が確認可能

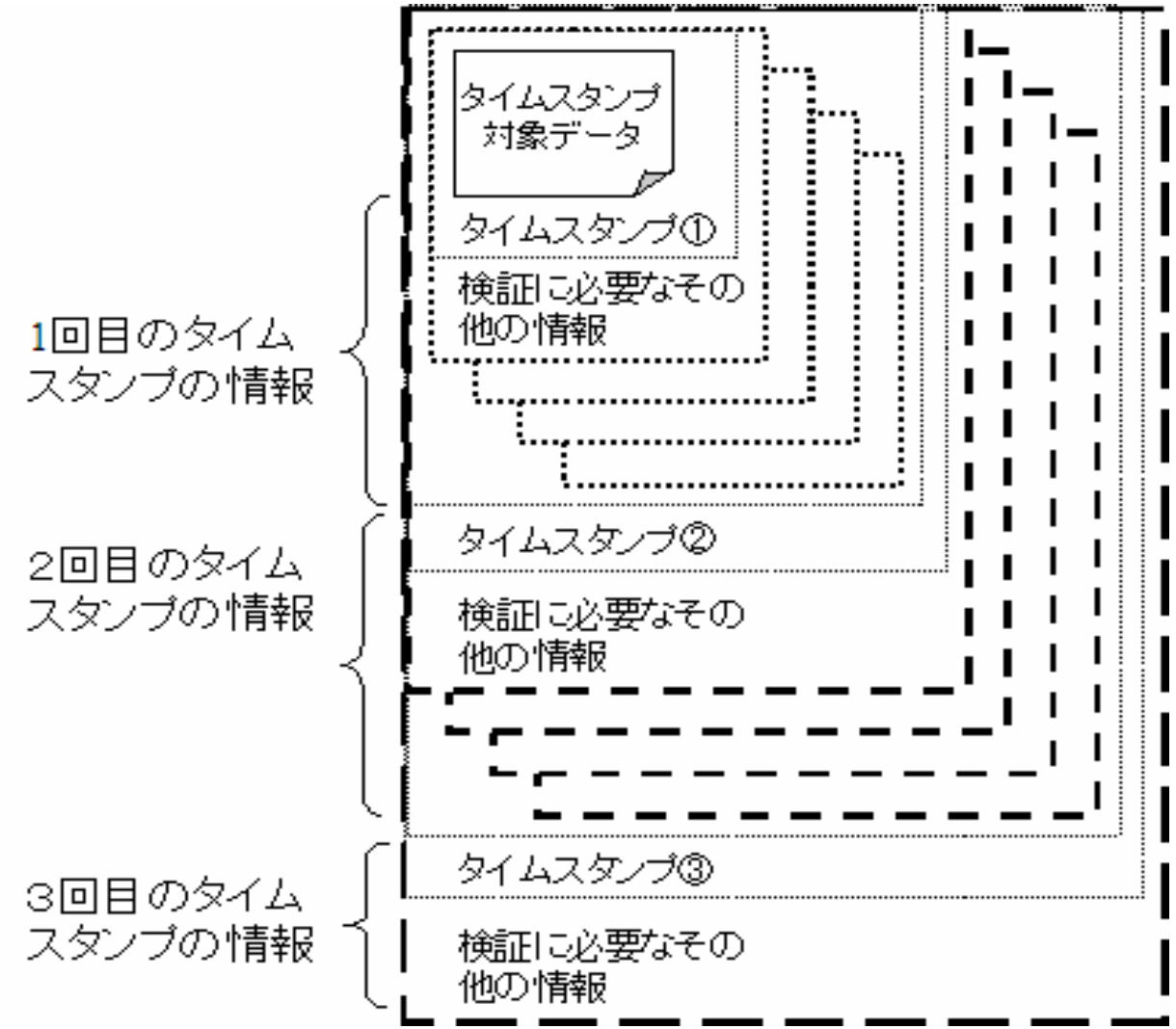
⑤　長期経過後にTSAが適切に運用されていたことを確認できること
当時のTP/TPS等を確認できること

3　タイムスタンプによる長期保証の方法
(1) PKI方式タイムスタンプ

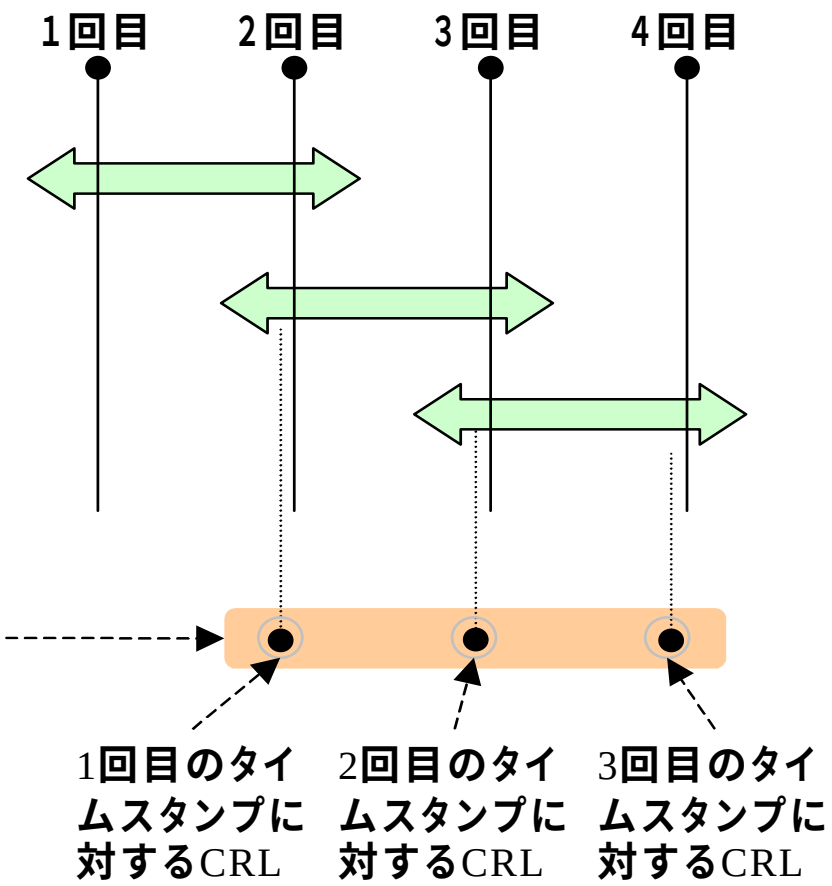


- TSA公開鍵証明書
- TSA公開鍵証明書に対するCRL (ARL)
- TSA公開鍵証明書の認証パス及び、その構築に必要な情報
  - Root-CAに至るまでのCA公開鍵証明書
  - Root-CAに至るまでのCA公開鍵証明書に対するCRL (ARL)
  - Root-CAに至るまでのCAに対するCP/CPS
- TSAのTP/TPS

3　タイムスタンプによる長期保証の方法
(1) PKI方式タイムスタンプ



3　タイムスタンプによる長期保証の方法
(1) PKI方式タイムスタンプ



1回目に押すタイムスタンプに対するTSA証明書の有効期間

2回目に押すタイムスタンプに対するTSA証明書の有効期間

3回目に押すタイムスタンプに対するTSA証明書の有効期間

TSA証明書のCRLの収集タイミング

タイムスタンプを押した時点以降かつ、次回タイムスタンプ直前にCRLを収集する。

※CRL以外に、TSA証明書、CA証明書の収集タイミングは、それらの有効期限内ならいつでも良いが、システム構築上、CRL収集時点が妥当かと思われる。

3　タイムスタンプによる長期保証の方法
(1) PKI方式タイムスタンプ

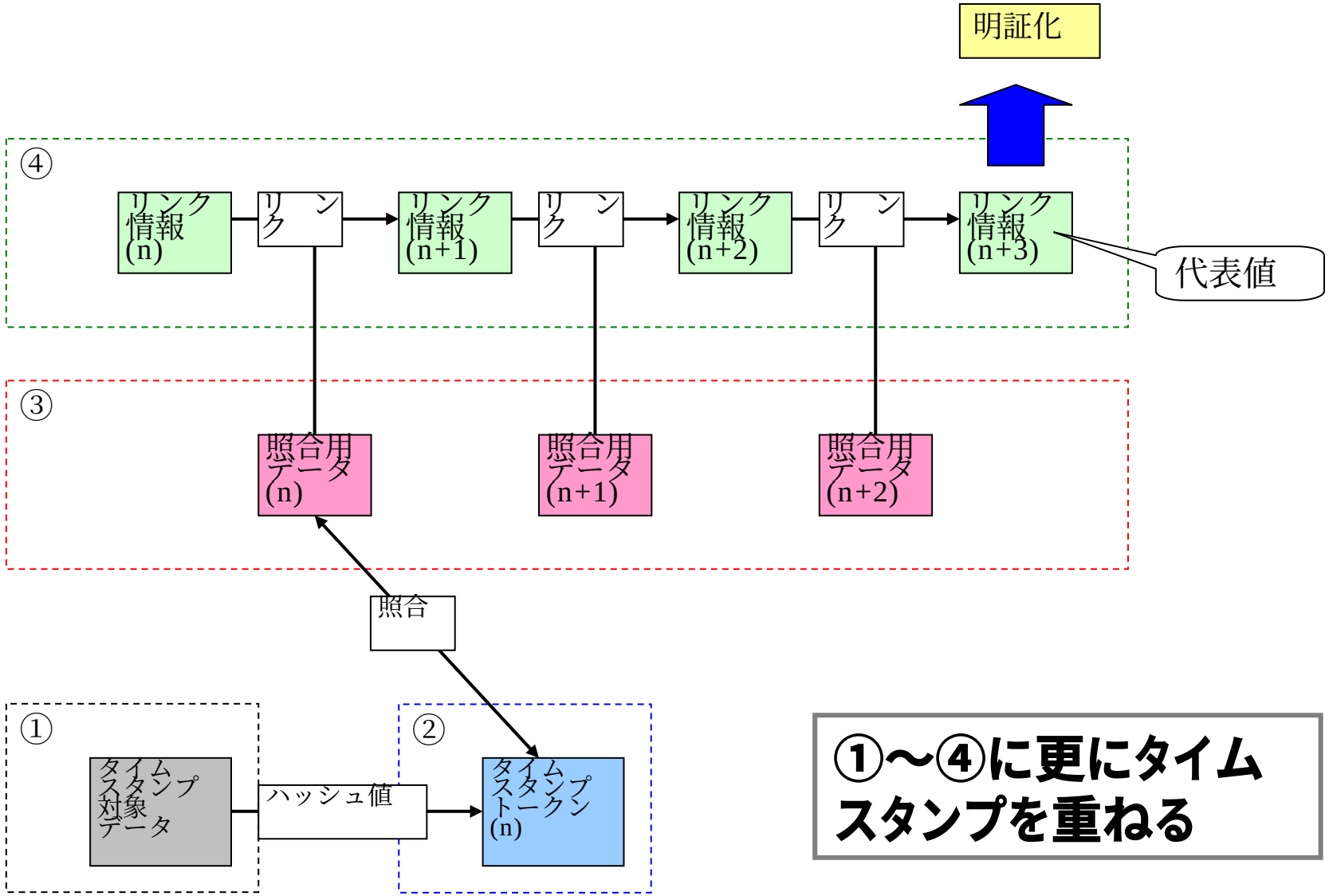
① 各証明書は、予め保存され、その上にタイムスタンプされたCRLを参照して検証する事により、CA及びTSAの公開鍵証明書がタイムスタンプを押した時点では失効されていなかった事を確認する。

② TSA公開鍵証明書に対するCRLの発行日時は、タイムスタンプ日時以降である事を確認する。

③ ルートCA公開鍵証明書に関しては、公知されている情報と比較する。

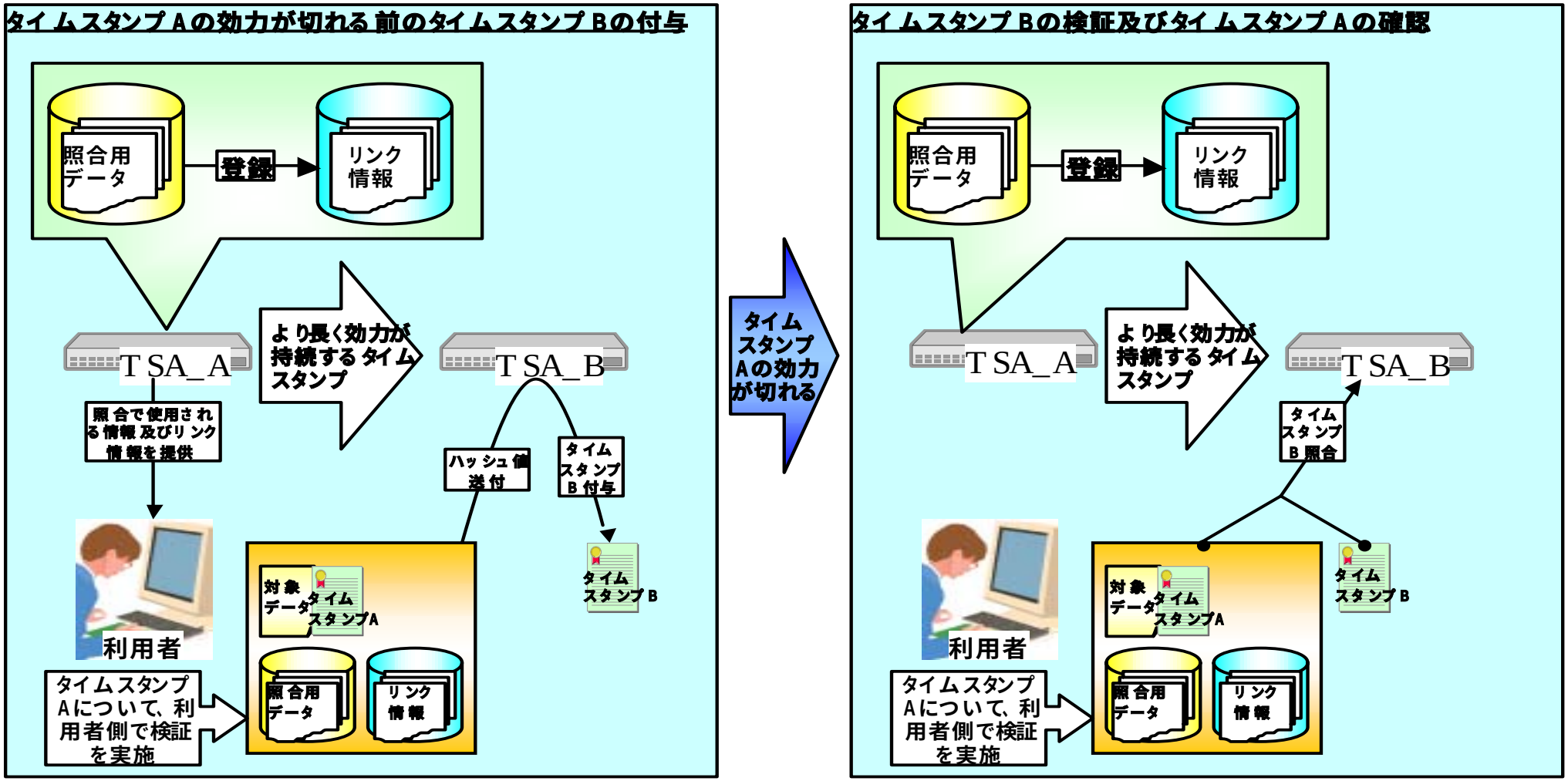
④ 検証者が過去に取得したTP/TPS、もしくは新たにタイムスタンプを重ねた対象データ内のTP/TPSの内容について必要に応じて確認する。

3　タイムスタンプによる長期保証の方法
(2) リンク方式タイムスタンプ



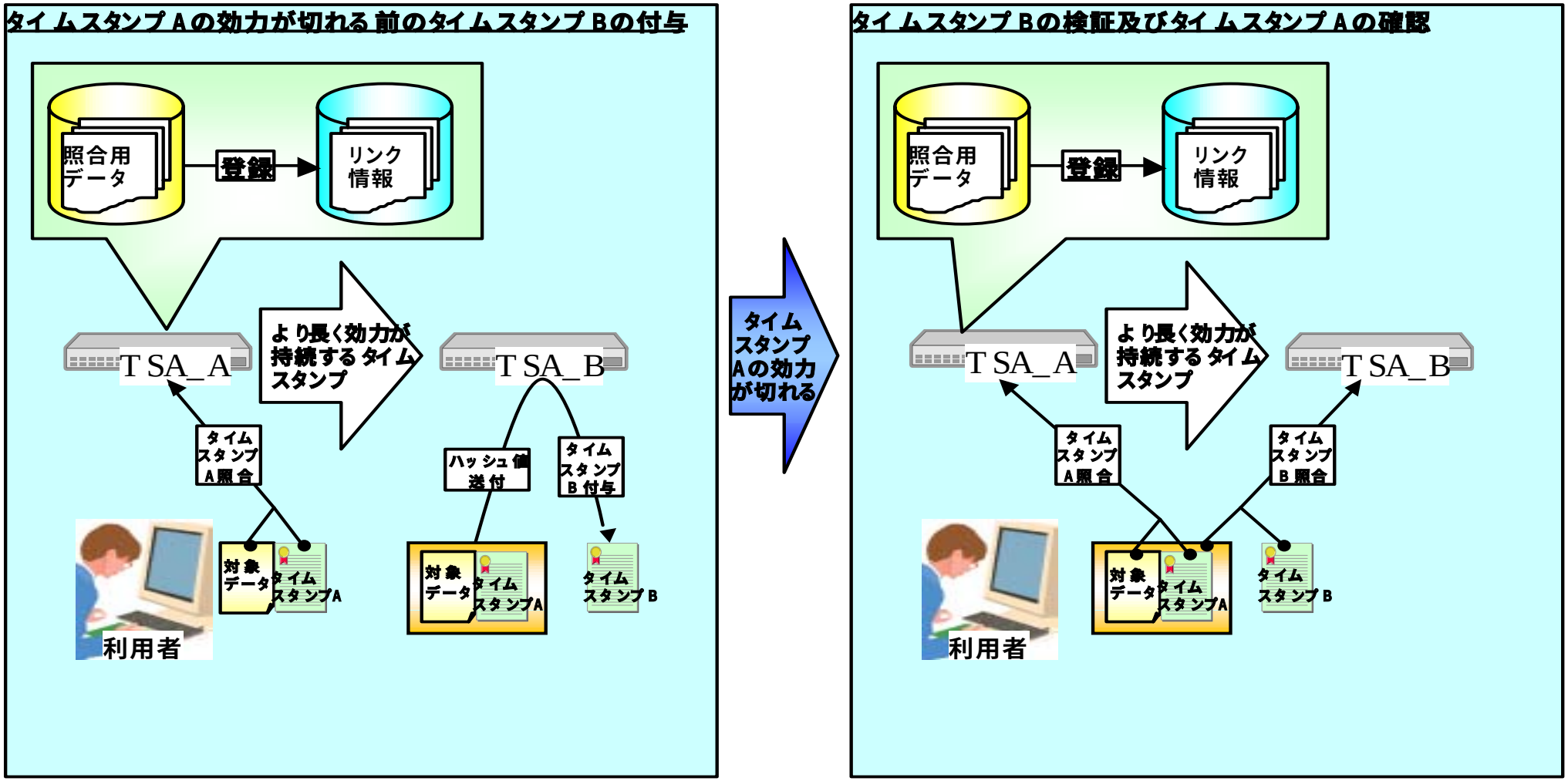
①～④に更にタイムスタンプを重ねる

3　タイムスタンプによる長期保証の方法
(2) リンク方式タイムスタンプ



利用者が全ての情報を収集する実現例

3　タイムスタンプによる長期保証の方法
(2) リンク方式タイムスタンプ

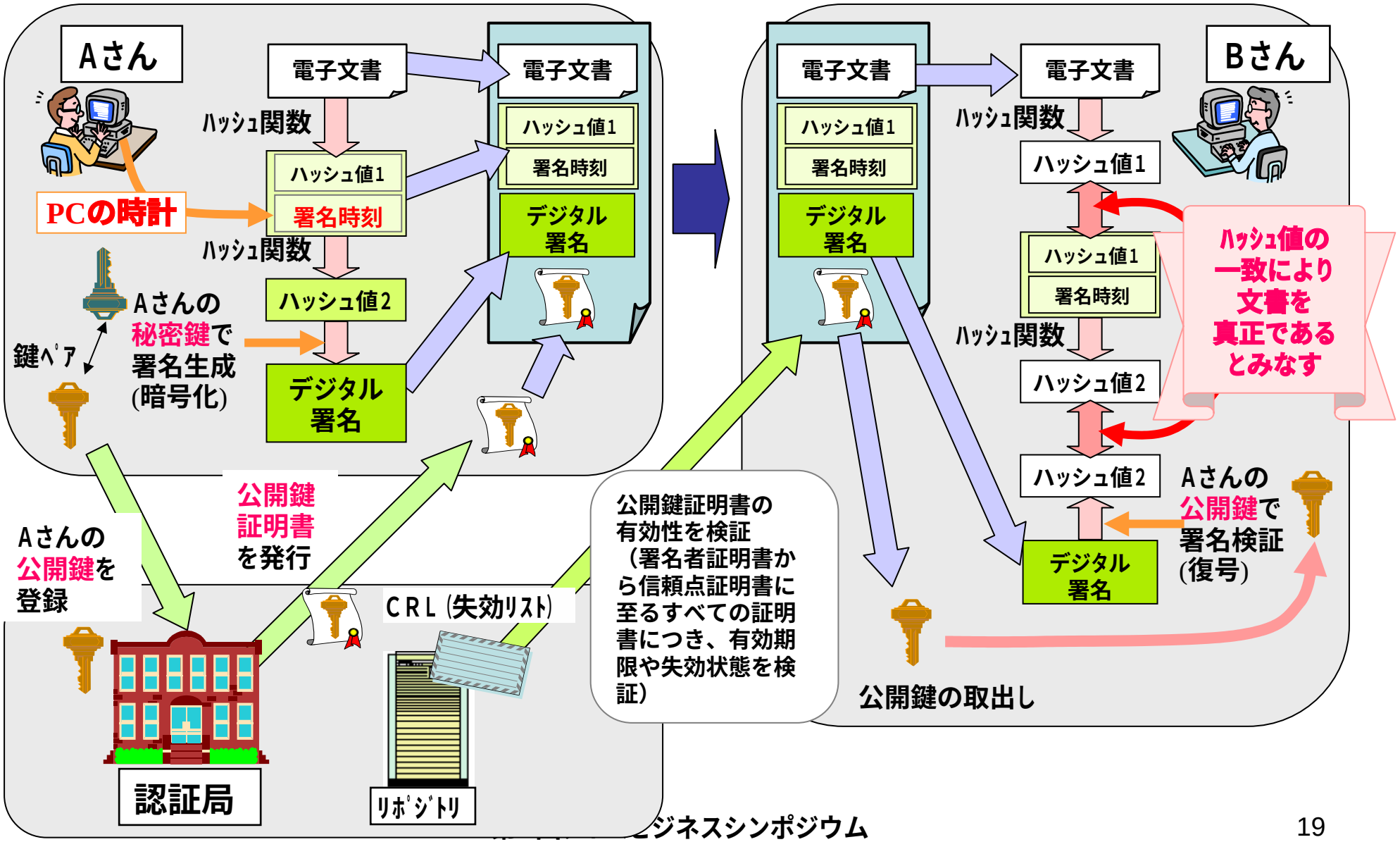


照合業務が継続される場合の実現例

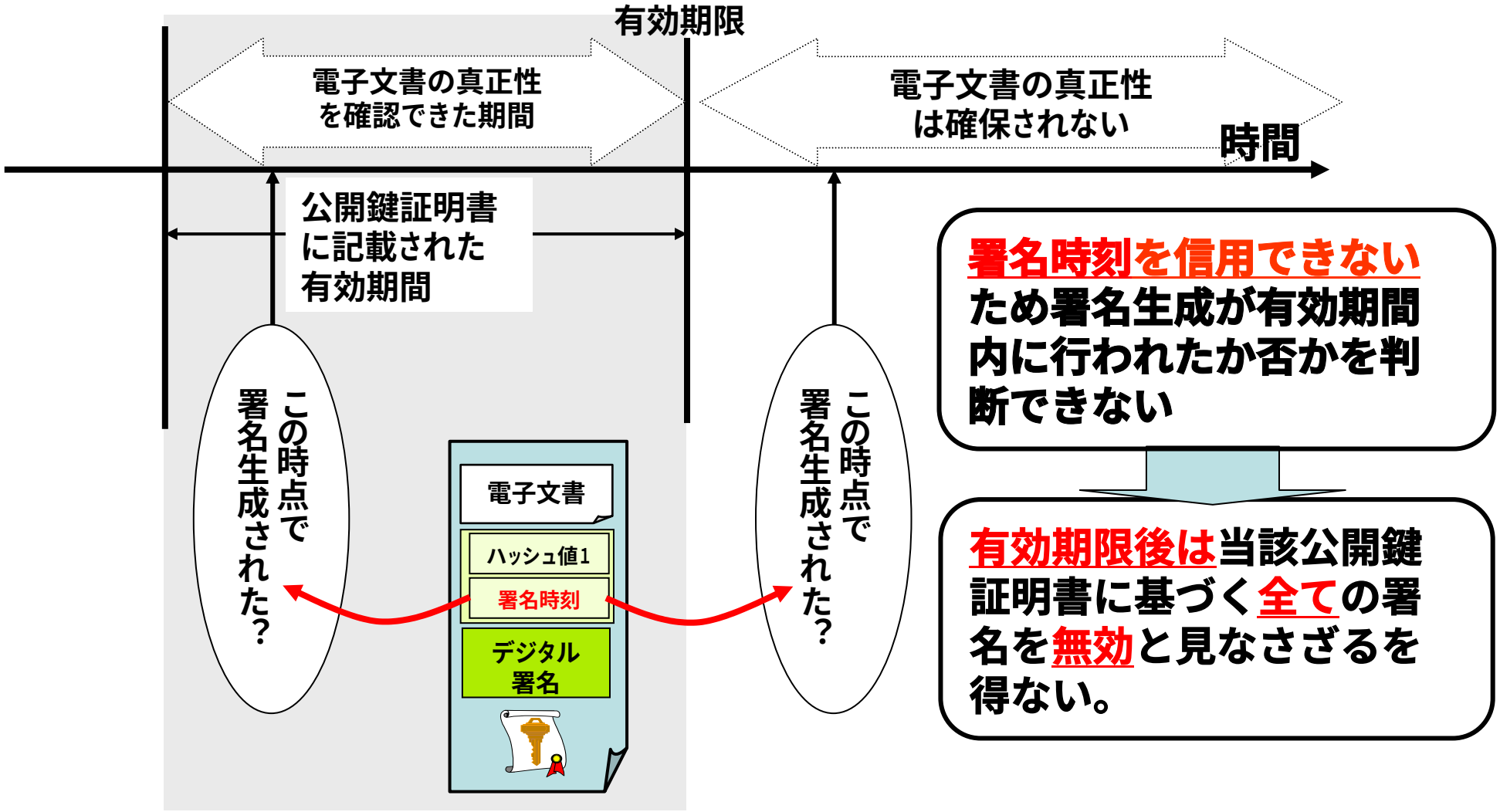
4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付文書の長期保証との関係

	PKI方式タイムスタンプ	その他のデジタル署名付文書
1	電子データとタイムスタンプとの関係を証明できること	－ （電子データがデジタル署名付文書に含まれていれば、デジタル署名付文書の非改ざん性の確認で十分。）
2	タイムスタンプトークンの非改ざん性を確認できること	デジタル署名付文書の非改ざん性を確認できること
3	タイムスタンプの発行主体を確認できること	デジタル署名の本人性を確認できること
4	信頼点の正当性を確認できること	信頼点の正当性を確認できること
5	TSAが正しく運用されていることを確認できること	－ （署名者の自己責任により正しく運用されていることが前提）
6	－ （上記（５）により正確な時刻が付与されていることが前提）	デジタル署名存在時刻を確認できること

4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付文書の長期保証との関係



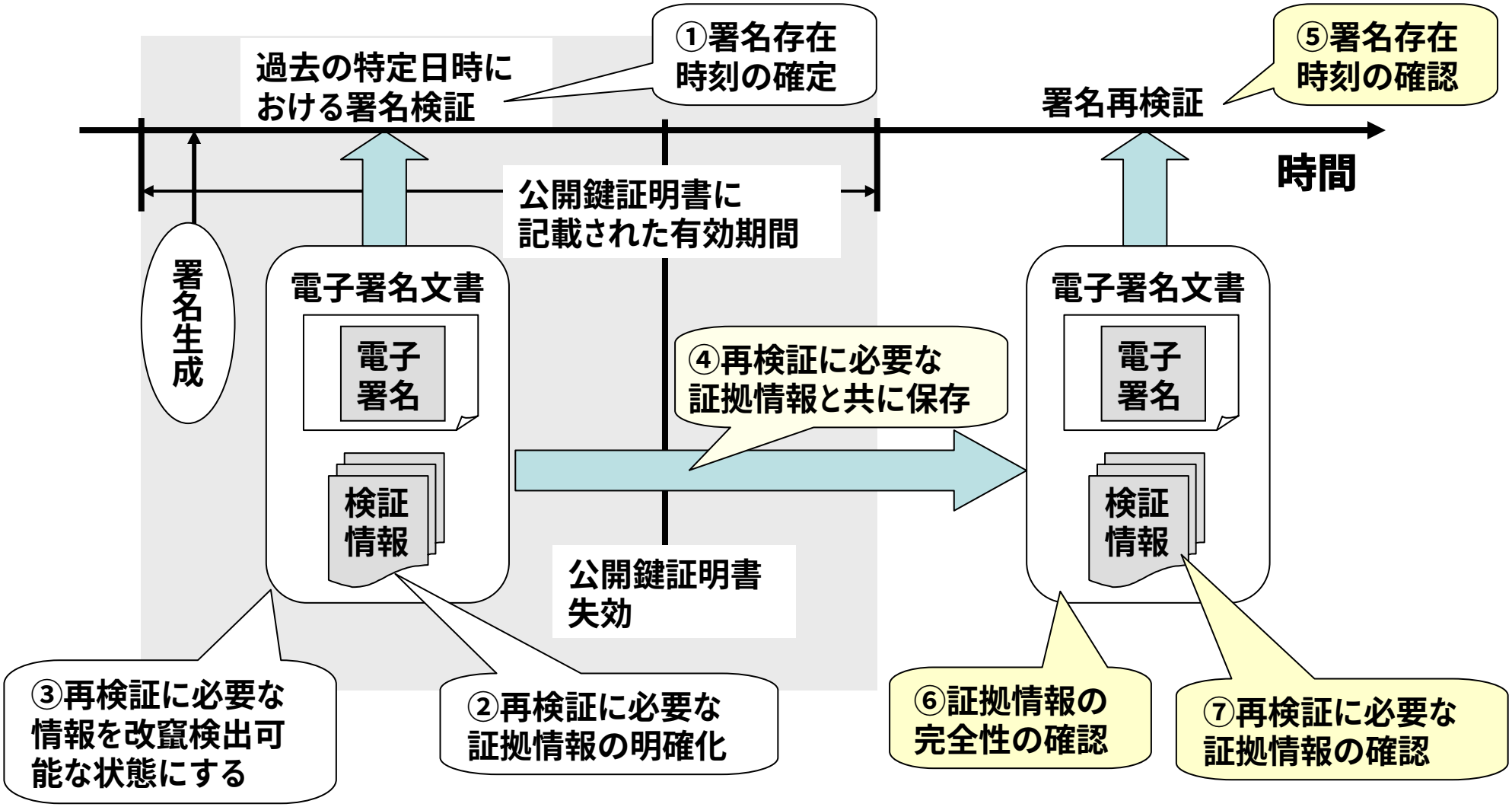
4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付文書の長期保証との関係



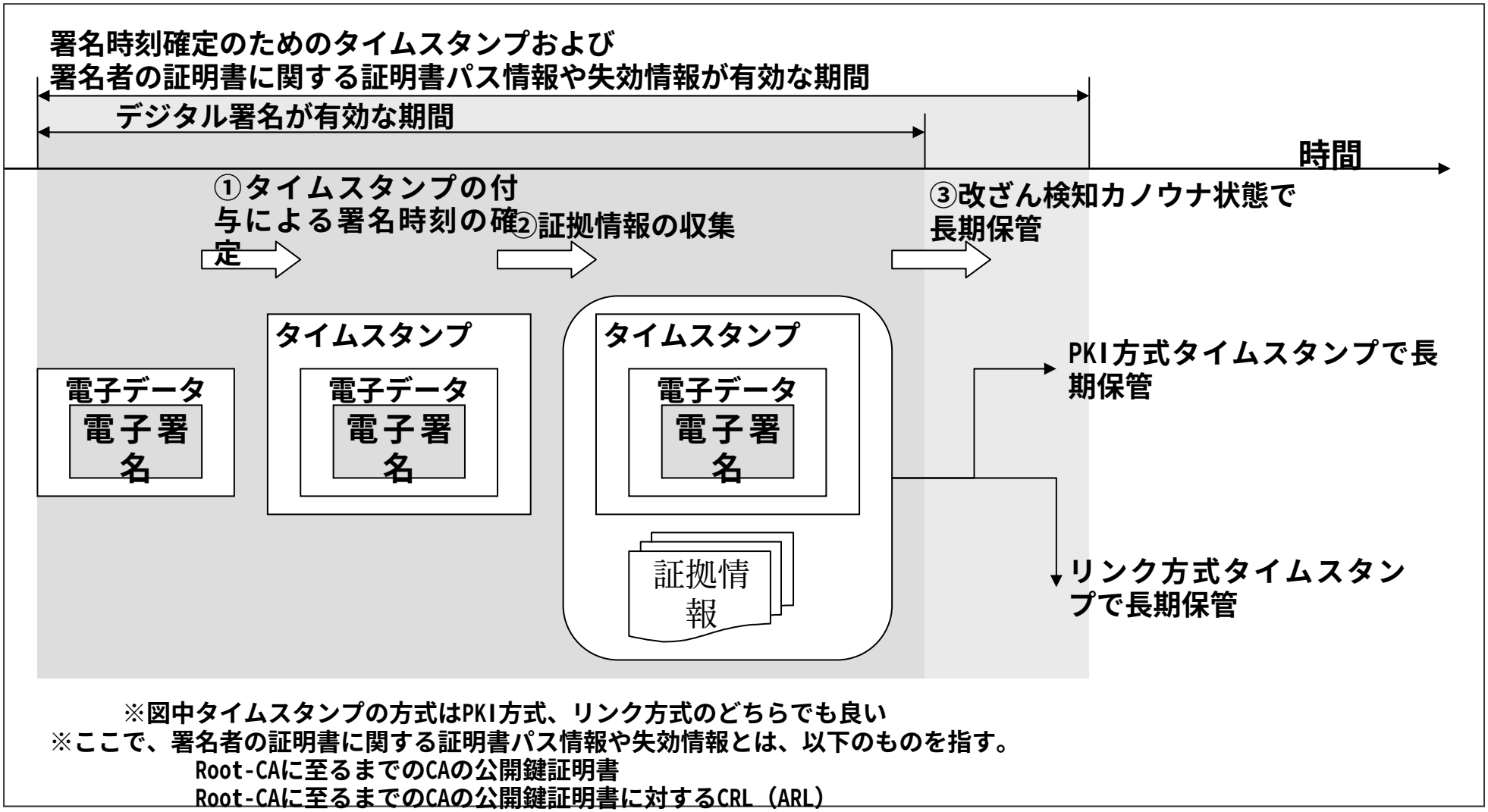
署名時刻を信用できないため署名生成が有効期間内に行われたか否かを判断できない

有効期限後は当該公開鍵証明書に基づく**全て**の署名を**無効**と見なさざるを得ない。

4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付き文書を対象とする場合の方法



4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付き文書を対象とする場合の方法

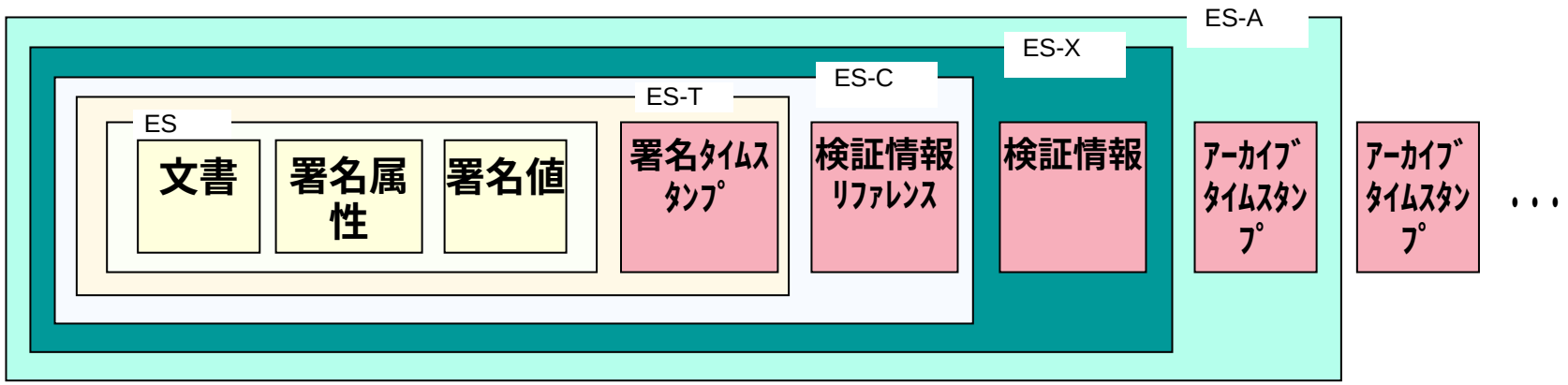


※図中タイムスタンプの方式はPKI方式、リンク方式のどちらでも良い
※ここで、署名者の証明書に関する証明書パス情報や失効情報とは、以下のものを指す。
Root-CAに至るまでのCAの公開鍵証明書
Root-CAに至るまでのCAの公開鍵証明書に対するCRL（ARL）

4　デジタル署名付き文書を対象とする場合
(1) デジタル署名付き文書を対象とする場合の方法

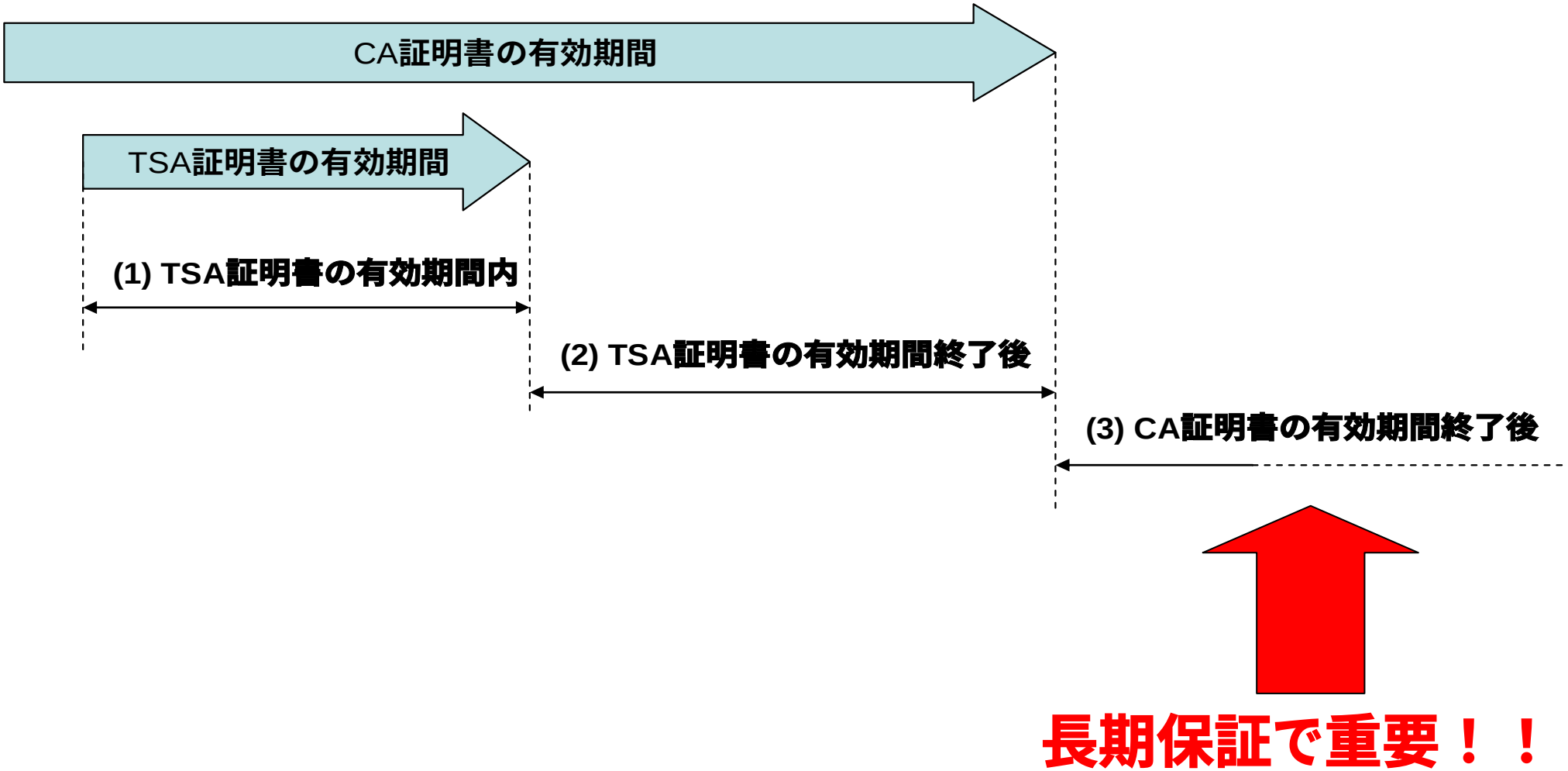
Electronic Signature Formats(ETSI TS 101 733 V1.5.1)

Electronic Signature Formats for long term electric signature (RFC3126)



長期署名フォーマット

5　CAの要件


CA証明書の有効期間
TSA証明書の有効期間
(1) TSA証明書の有効期間内
(2) TSA証明書の有効期間終了後
(3) CA証明書の有効期間終了後
長期保証で重要！！

5　CAの要件

- 当該TSA証明書(あるいはその発行履歴)
- タイムスタンプ付与時から当該TSA証明書の有効期間満了までの間に発行されたいずれかの失効リスト(あるいはその発行履歴)
- 当該TSA証明書を発行したCAの証明書

CA業務の終了

信頼点の永続保存や公知化のための信頼できる方法や機関が望まれる

参考：セキュア保管型タイムスタンプ長期保証

(1) タイムスタンプ付与対象の電子データ
(2) タイムスタンプ
(3) タイムスタンプ検証に使用した情報
⇒一括して厳密な運用の下に管理して保管

- 可搬媒体方式
- 自主運営ストレージ方式
- アウトソーシングストレージ方式
- 長期使用を前提とした電子署名方式

参考：セキュア保管型タイムスタンプ長期保証

(1) 登録時刻の保証

タイムスタンプの有効性が失われる前にそのデータが保管されていたことを証明できること。

(2) 非改ざん性の保証

保管対象データが保管されている間、改ざんされていないことを証明できること。

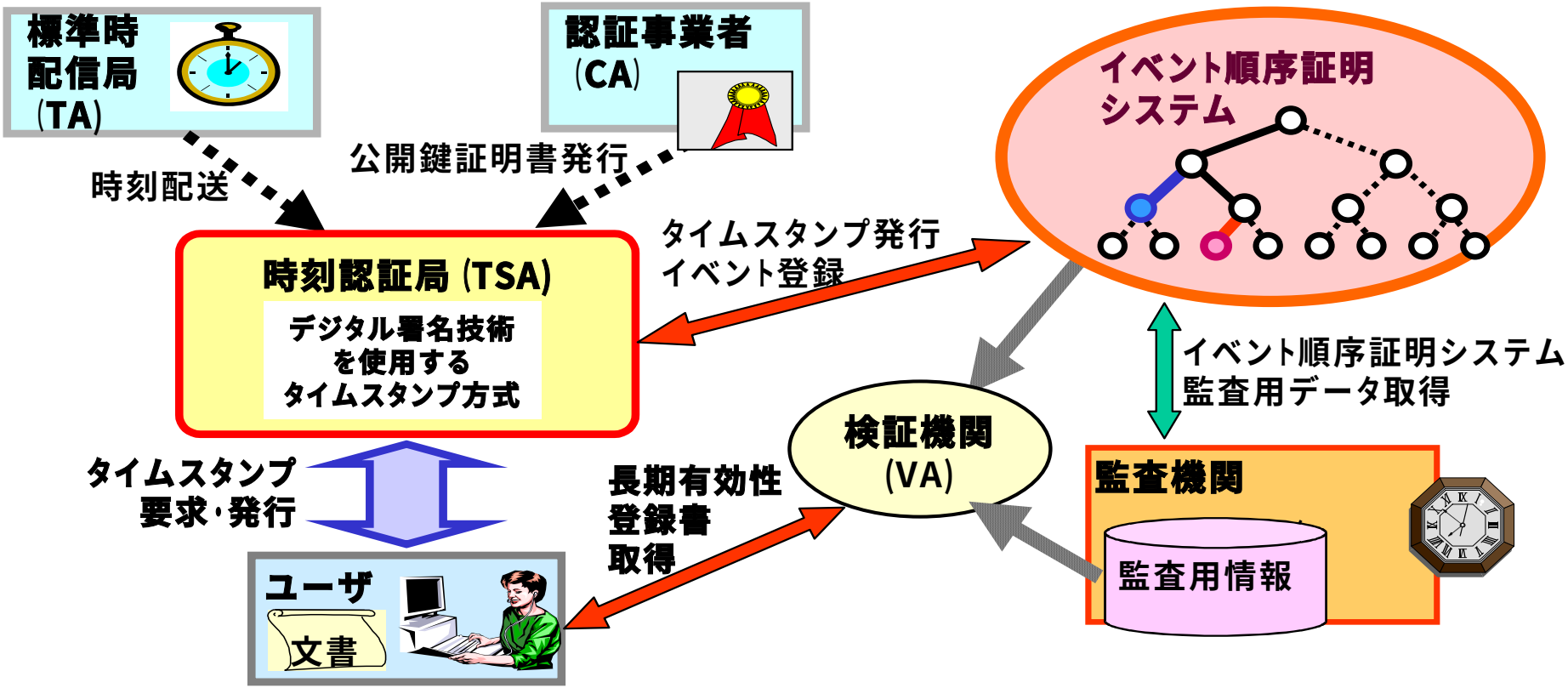
(3) 保存性の保証

後日、保管対象データを読み出すことができるように、保管対象データの損失、破壊、読出しが不可能な状態にならないようにすること。

(4) 保管対象データと取り出しデータの同一性の保証

取り出されたデータが、指定された保管対象データと同一であり、差し替えなどがなされていないことを証明できること。

参考：DS-IMT長期保証技術



DS-IMT 方式を用いたタイムスタンプ長期保証の構成例