信頼される安心を、社会へ。
SECOM

タイムスタンプ最新動向

Evidence Record Syntax (ERS) を用いた
タイムスタンプのまとめ押し

セコムトラストシステムズ株式会社

■ 長期署名とERSの標準技術について

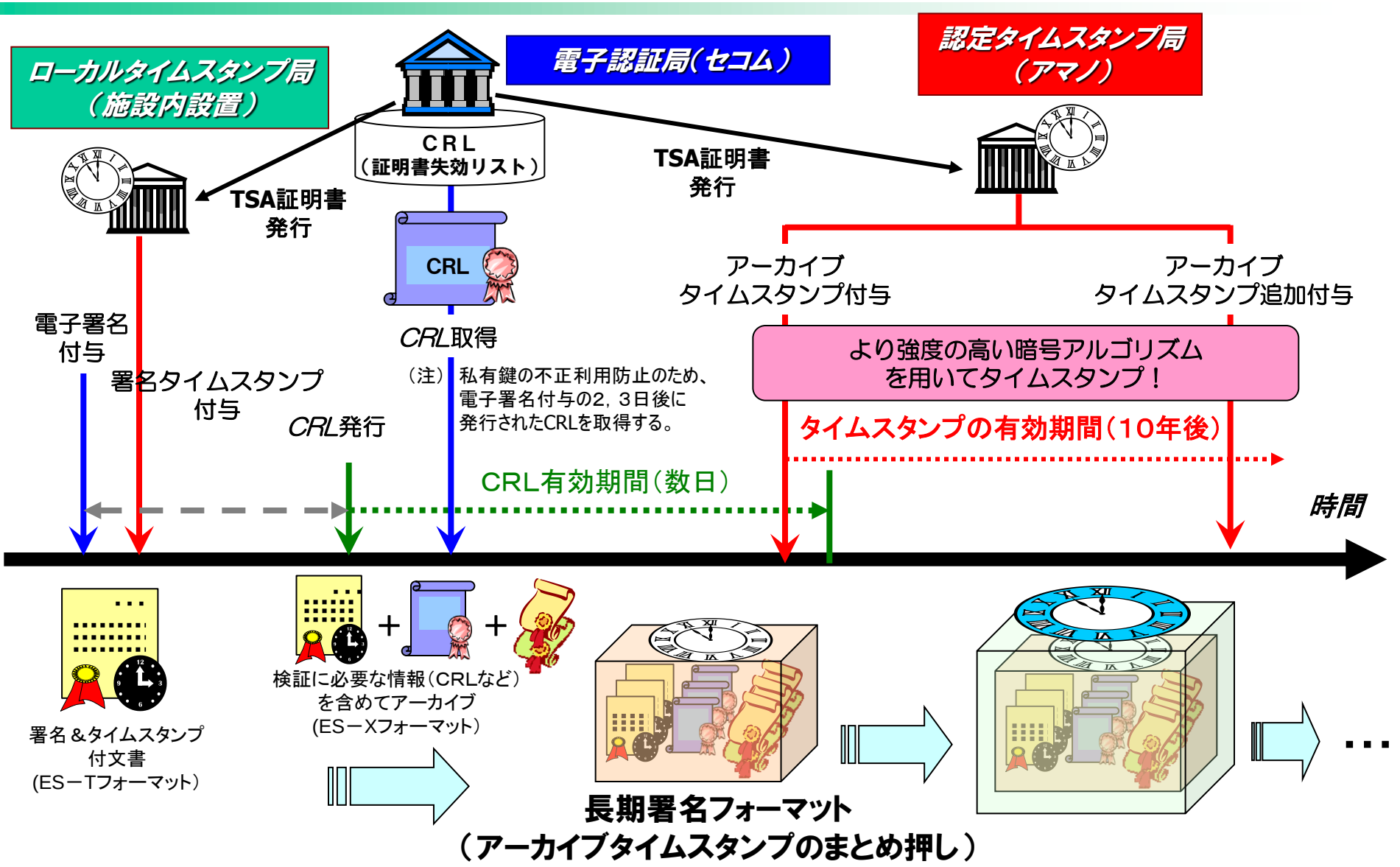
ERS（ Evidence Record Syntax： RFC4998）とは

- ✓複数の電子文書をまとめてタイムスタンプを付与する方式
- ✓タイムスタンプの検証は個々の電子文書ごとに可能
- ✓まとめ押しした一部のデータが破損したとしても、残りは独立して検証可能

(注1) 長期署名
・ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES)
・RFC 3126 (Electronic Signature Formats for long term electronic signatures)
・JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル

(注2) ERSの標準技術
・IETF RFC4998：Evidence Record Syntax (ERS) August 2007
・IETF RFC4810：Long-Term Archive Service Requirements March 2007

■ 長期署名フォーマット生成フロー（ローカルタイムスタンプ併用型）

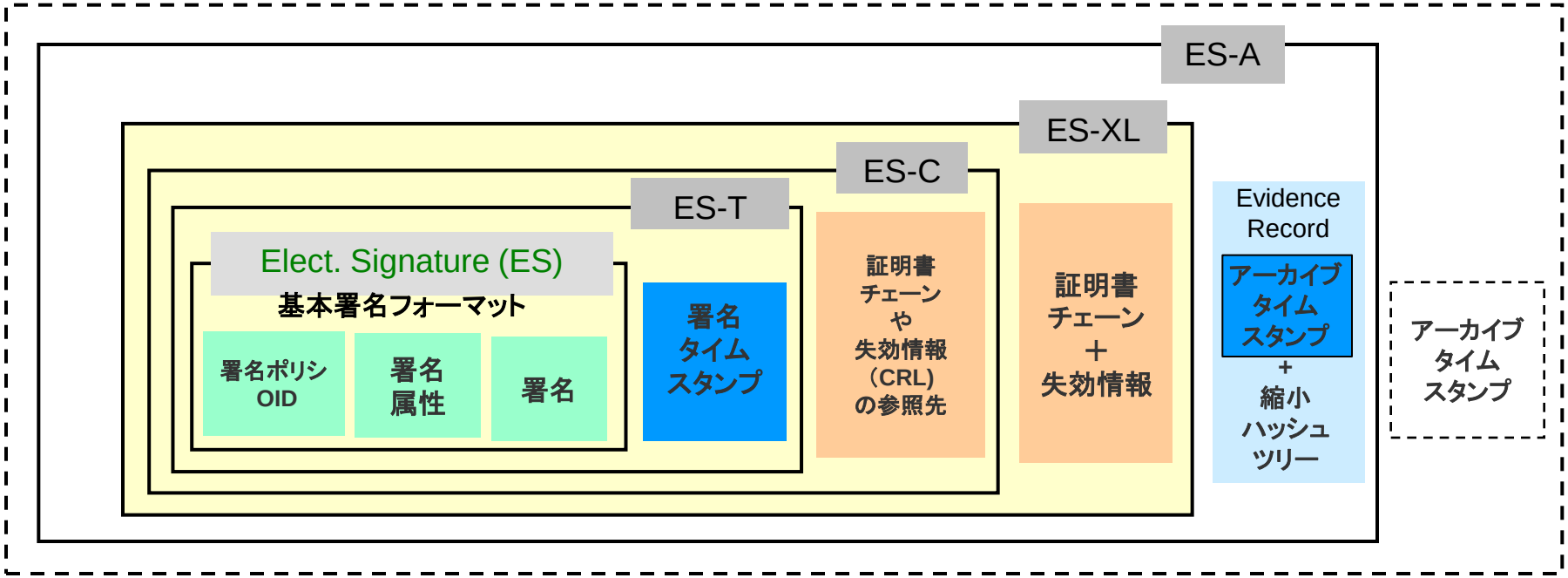


外殻のタイムスタンプが破られない限り、内部の真正性は保たれる

(参考資料) 長期署名フォーマットによるERS(イメージ)

- 長期署名フォーマットファイルがあれば、ファイル単独で署名、タイムスタンプの検証が可能
  (システムに依存する事なく、長期に渡り、署名、タイムスタンプの有効性を継続可能)
- 何十年も保存する署名文書を想定したフォーマット
  暗号強度の弱体化、署名アルゴリズムの危殆化による署名偽造を防ぐ
  - 暗号方式が既に解読されるようになっても署名時点の有効性を検証できる方式

・RFC 3126 (Electronic Signature Formats for long term electronic signatures)
・ETSI TS 101 733 Electronic Signature Formats (CAdES)
・JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル



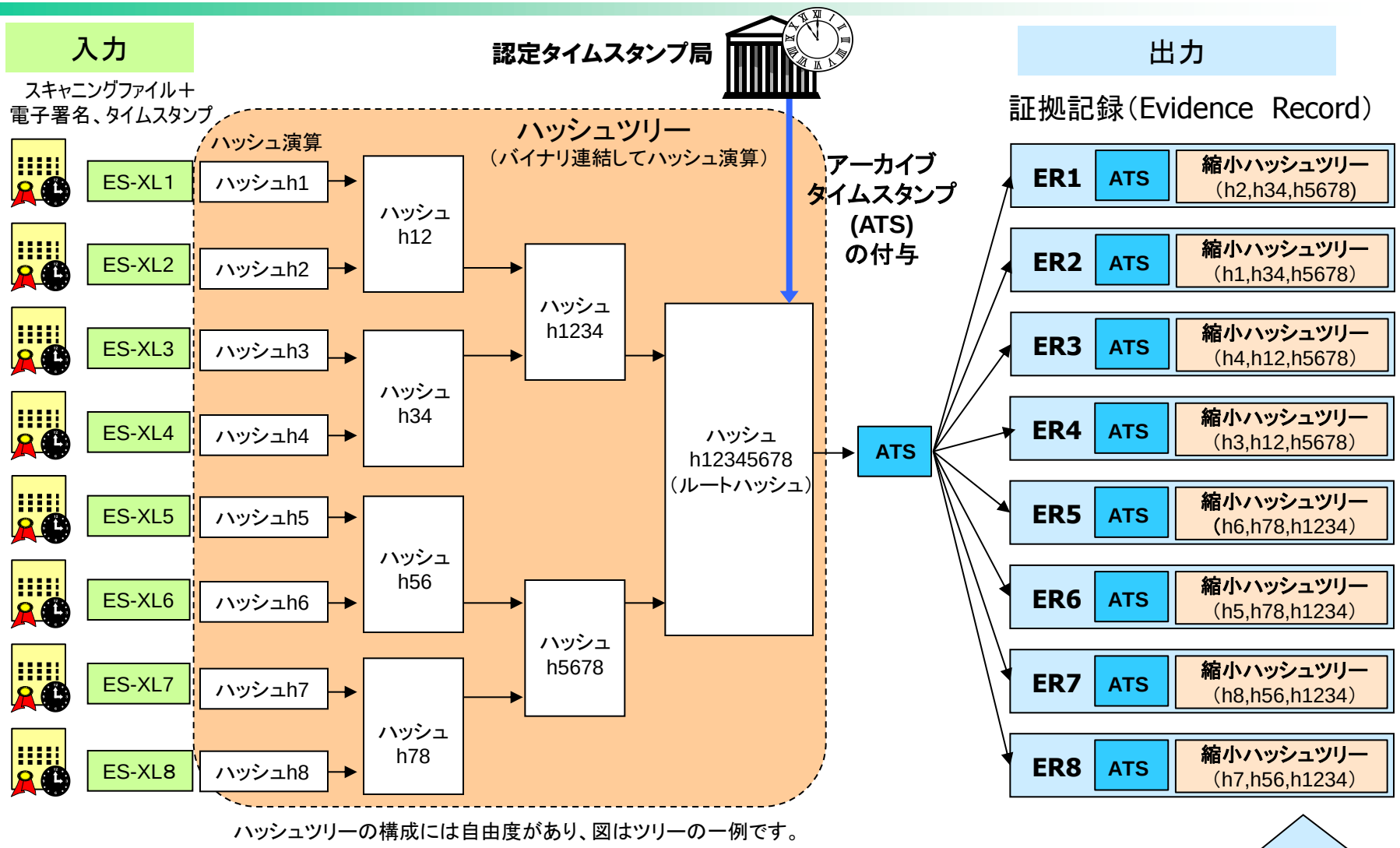
ES-T: Electronic Signature with Time stamp

ES-C: Electronic Signature with Complete validation data

ES-XL: Electronic Signature eXtended Long

ES-A: Electronic Signature Archive

■ Evidence Record Syntax (ERS)によるアーカイブデータ生成

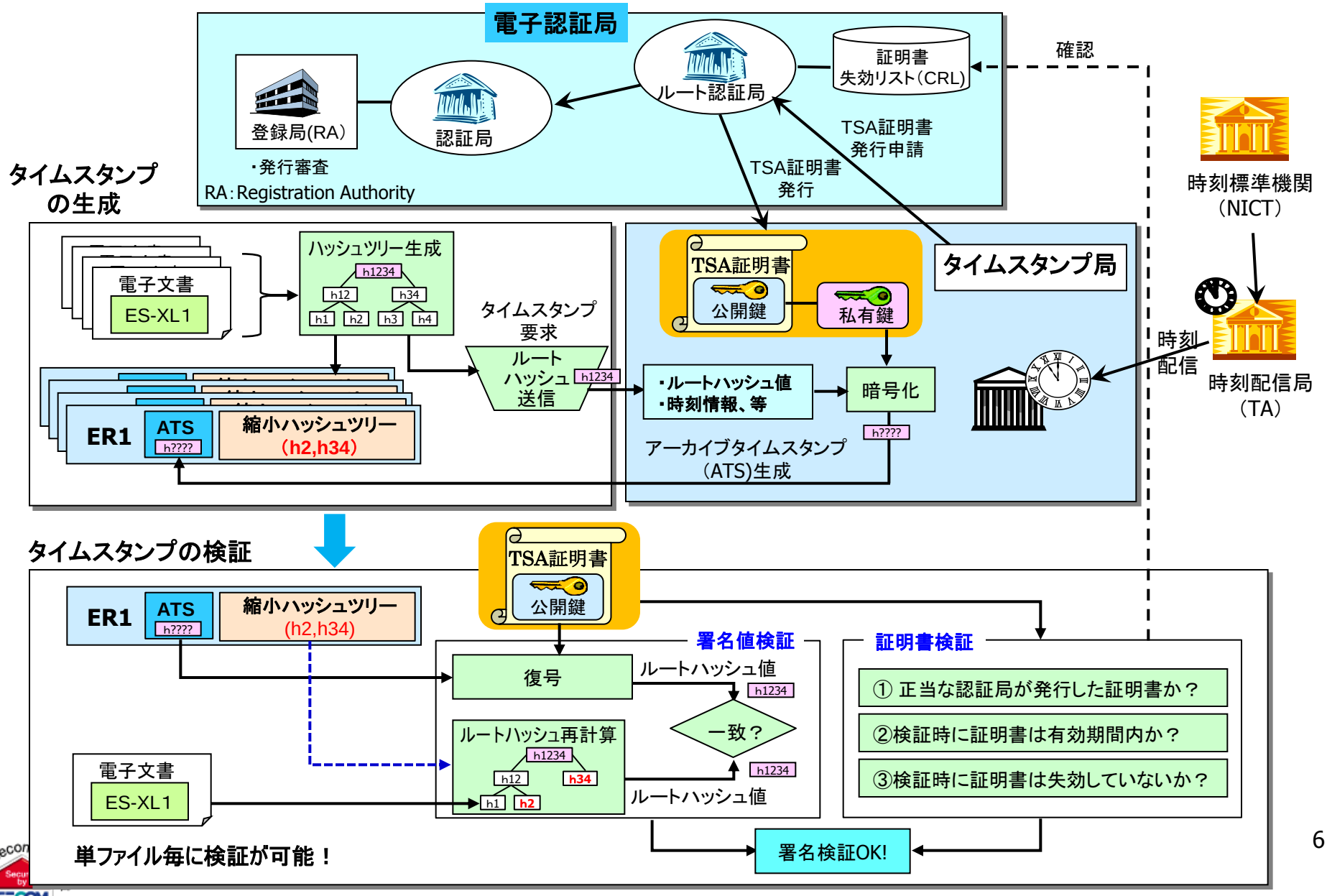


ハッシュツリーの構成には自由度があり、図はツリーの一例です。

① スキャニングファイルには個別に電子署名と署名タイムスタンプを付与します（ES-T→ES-XL）
② ERSの標準規格を用いて、複数のES-XLファイルをまとめてアーカイブタイムスタンプを付与します。
③ 電子署名やタイムスタンプの検証は、各スキャニングファイル個別に実施可能。
④ 10年間署名検証の維持が可能、さらに、アーカイブタイムスタンプの追加により10年単位で署名検証の延長が可能。

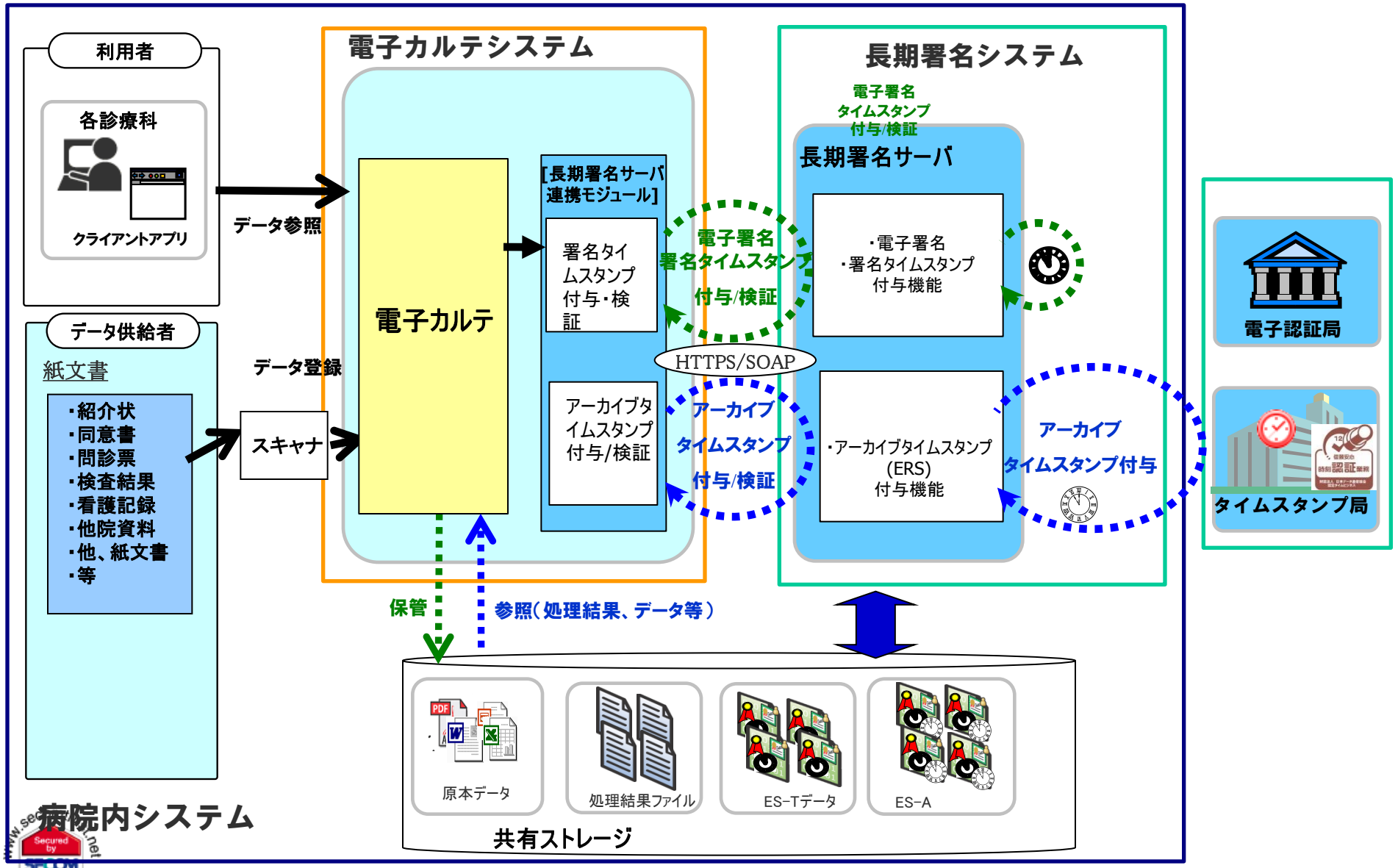
それぞれの対象ファイルに対してアーカイブタイムスタンプの検証に必要となる最小限のハッシュ群(縮小ハッシュツリー：reducedHashtree)を個別に生成します。

■ ERS方式によるタイムスタンプとタイムスタンプの検証のしくみ



タイムスタンプの活用事例：医療

USE CASE：医療関連文書のスキャナー保存



■ 概要

- ✓ 医療関連文書をスキャナで読み取り、厚労省ガイドラインに従って長期署名を付与して電子保存

■ 導入前の課題

- ✓ 電子カルテを導入しても、同意書や紹介状などの紙文書は、患者ごとにファイルして保存する必要があり、電子と紙の二重管理となっている
- ✓ カルテ庫にもう保存する余裕がない
- ✓ 例えばオペ前に必要書類が揃っているか照会、確認に手間と時間がかかる

■ 導入効果

- ✓ 患者ごとの紙ファイルの管理が無くなり省力化できた
- ✓ 保存スペースを新規に増やす必要が無くなった
- ✓ 検索性が劇的に向上、術前確認が迅速に可能となった

■ その他

- ✓ 厚労省の「医療情報システムの安全管理に関するガイドライン」で長期署名が要件になっており、その遵守が必要

■検証結果の詳細表示（CAdES+ERS）

詳細な検証結果は検索結果一覧の署名アイコンから表示します。

文書情報

文書番号	00000000000000000000000000000008
検証者	admin2
検証日	2012/09/14 11:17:00
文書ファイルパス	C:/secom/packs/data/egc/fix/img/0000005436/doc_00000000000000000000000051231.pdf

検証結果

検証結果メッセージ	成功
署名タイムスタンプ時刻	2012/09/14 10:53:11
アーカイブタイムスタンプ時刻	2012/09/14 11:16:20
署名アルゴリズム	SHA1WITHRSA
署名タイムスタンプの署名アルゴリズム	SHA256WITHRSA
署名タイムスタンプのTSAシリアル番号	13300057863253153900
署名タイムスタンプのTSA所有者識別子(SubjectCN)	CN=Test TSA, OU=eco, O=secomtrust.net, ST=tokyo, C=jp
署名タイムスタンプのTSA有効期間終了時刻	2022/03/17 11:27:11
署名タイムスタンプのTSA発行者識別子(IssuerDN)	CN=Test SubCA, OU=eco, O=secomtrust.net, ST=tokyo, C=jp
アーカイブタイムスタンプの署名アルゴリズム	SHA512WITHRSA
アーカイブタイムスタンプ時のTSAシリアル番号	13300057863253153900
アーカイブタイムスタンプ時のTSA所有者識別子	CN=Test TSA, OU=eco, O=secomtrust.net, ST=tokyo, C=jp
アーカイブタイムスタンプ時のTSA有効期間終了時刻	2022/03/17 11:27:11
アーカイブタイムスタンプ時のTSA発行者識別子	CN=Test SubCA, OU=eco, O=secomtrust.net, ST=tokyo, C=jp
署名者証明書シリアル番号	5889745798476227102
署名者証明書所有者識別子(SubjectCN)	CN=arita kan, OU=STS SS2G, OU=Denshi Syoko Service2, O=SECOM Trust Systems CO. LTD., C=JP
署名者証明書有効期間終了時刻	2015/04/23 12:23:04
署名者証明書発行者識別子(IssuerDN)	CN=SECOM Passport for Member PUB CA3, OU=SECOM Passport for Member 2.0 PUB, O="SECOM Trust Systems CO.,LTD.", C=JP
署名時データハッシュ値	2dfb575de412f364ab89f94ae0e6454ac8235ff7
検証時データハッシュ値	2dfb575de412f364ab89f94ae0e6454ac8235ff7
署名時タイムスタンプハッシュ値	a6ede3b4e3f060d987c99cae26a7d12474ac11ec40b4701ff9bf32cf3ac1eeef
検証時タイムスタンプハッシュ値	a6ede3b4e3f060d987c99cae26a7d12474ac11ec40b4701ff9bf32

署名対象ファルの名称（フルパス表示）

電子署名、署名タイムスタンプ、アーカイブタイムスタンプのすべての検証結果

署名タイムスタンプ時刻、電子署名を行った日時を特定（ローカルタイムスタンプ）

アーカイブタイムスタンプ時刻。証明書の有効期間内かつ失効していないうちに検証情報を取得した上で、全体にタイムスタンプを付す（認定タイムスタンプ）

ローカルタイムスタンプ局の名称（TSA名）

認定タイムスタンプの有効期間

認定タイムスタンプ局の名称（TSA名）

認定タイムスタンプの有効期間

署名者の氏名、所属等の情報

署名者の証明書の有効期間

認定認証局の名称

署名対象ファイルの非改ざん性の証明（ハッシュ比較）

タイムスタンプ対象データの非改ざん性の証明（ハッシュ比較）