測定機器データの長期保存
技術ガイドブック

第 1.0 版

2021 年 5 月 19 日

公益社団法人日本文書情報マネジメント協会
R&D データ保存委員会

目次

1. 目的

本技術ガイドブックは,「測定機器の長期保存ガイダンス」で示された「測定機器データ」の「長期保存」を実現可能とする技術について説明することを目的としている。2 章に適用範囲を、3 章に本技術ガイドブックを作成するに至った背景（規制要件を含む）を記載した後に、本技術ガイドブックの本題を説明する。本技術ガイドブックの本題（4 章～6 章）は、以下のように対象読者別に記載されている。

表 1　本技術ガイドブックの構成

章タイトル	対象読者
2 章 適用範囲の定義 3 章 作成背景と規制要件	全ての方（前提等の共通事項）
4 章 パッケージの運用	「測定機器の長期保存ガイダンス」に従って標準パッケージを利用し運用する現場の人（標準パッケージ利用者向け）
5 章 標準パッケージ	「測定機器の長期保存ガイダンス」に記載の長期保存パッケージの技術的仕様を知りたい人または再解析する人（標準パッケージ実装者向け）
6 章 データ保証の基礎知識	データ保証に必要となる技術について広く一般的な知識を求めている人（一般技術者向けだが、非技術者の方も一読を推奨） ※ 一般的なデータの真正性保証についての基礎知識なので読み飛ばしても良い。

2. 適用範囲

本技術ガイドブックは、製薬業界における再解析の必要な測定機器データを対象として、技術的考察を加えたものである。

3. イントロダクション

「測定機器の長期保存ガイダンス」の目的に「データが再解析される可能性があることを前提として信頼性を保ったまま長期間に渡り安心して保存管理する方法を提示する」と書かれている。ここで大きく 2 つの技術的な項目が必要と考える。

1 つ目の項目は「信頼性の保証」である。信頼性を保証する為には、保存時から変更が無いことを示す為に「内容保証」が、保存時の責任者の確認に「本人保証」が、保存時刻の確認に「時刻保証」が、長期間の保存に対応する為に「長期保証」が、そして全体の運用に問題が無いことを示す為に「運用保証」が必要となる。「内容保証」「本人保証」「時刻保証」「長期保証」「運用保証」は「真正性」の構成要素であり、本技術ガイドブックでは「真正性」を保つ為の技術について解説する。

2 つ目の項目は「データの再解析」である。ここで再解析を行う解析者が保存時の解析者と同一では無い可能性および再解析時の解析環境が同一とは限らない等の点に課題がある。これを解決する技術要素として「標準化されたパッケージ（標準パッケージ)」の導入が必要となる。本技術ガイドブックではコスト面も考慮して標準パッケージの仕様を説明する。

3.1. 製薬関連の規則・ガイダンス

「測定機器の長期保存ガイダンス」では製薬業界を対象としているが、製薬業界の規則・ガイダンスとして、日本の ER/ES 指針（※1）と米国 Part11（※2）があり、また国際的な遵守すべき医薬品製造におけるコンピュータ化システムやデータの基準として、PIC/S GMP Guide ANNEX 11（※3）がある。いずれも電磁的記録またはデータ（Electronic Records / Data）と電子署名（Electronic Signature）の規則・ガイダンスとなっており、求められている内容には共通性がある。

表 2　電磁的記録と電子署名に対する規制要件

電磁的記録	電磁的記録が適切に管理・運用されること
電子署名	手書き署名と同等に取り扱われること 電磁的記録や署名理由と紐づけられ、切り離して利用できないようにすること

電磁的記録またはデータに関しては、主に管理や運用の方法が説明されている。特にいずれの規則・ガイダンスにおいても「運用」の技術は重要となる。オープン・システムとクローズド・システムの管理、信頼性を保証する為に電子署名の明示、電磁的記録と電子署名との紐づけ等が求められている。

電子署名に関してはいずれの規則・ガイダンスにおいても手書き署名と同等のものと定義されている。そもそも電子署名と言う用語は技術的な内容を指すものではなく、主に法的な意味において電磁的記録（データ）に付与する電子的な徴証（証拠）とされている。技術的には公開鍵暗号と PKI（公開鍵インフラ）を利用したデジタル署名以外にも、電子認証（ID とパスワード等）を利用した認証記録等がある。電子署名は狭義ではデジタル署名と同一とする場合もあるが、本技術ガイドブックでは技術に依存しない広義の意味で利用する。つまり関係としては「電子署名コデジタル

署名」であって両者は同等では無い。

電磁的記録の管理・運用の保証および電子署名では、「真正性（authenticity）」が求められているが、これらを保証する為の技術に関しては次の「3.4. 保証技術の概要」にて説明する。

※1 日本 ER/ES 指針：厚生労働省「医薬品等の承認又は許可等に係る申請等における電磁的記録及び 電子署名の利用について」（薬食発第 0401022 号）

https://www.pmda.go.jp/files/000158308.pdf

目次（抜粋）：

３．電磁的記録利用のための要件

3.1. 電磁的記録の管理方法

3.1.1. 電磁的記録の真正性（完全、正確で、信頼でき、作成・変更・削除の責任者が明確であること：セキュリティ保持とバックアップの手順化と実施、責任者の識別、監査証跡）

3.1.2. 電磁的記録の見読性（人が読める形式で出力できること）

3.1.3. 電磁的記録の保存性（保存期間内に真正性と見読性を保って保存できること：記録媒体の管理の手順化と実施、媒体移行時の保存性の維持）

3.2. クローズド・システムの利用

3.3. オープン・システムの利用

４．電子署名利用のための要件

※2 米国 Part11：FDA 発行の 21 CFR Part 11 "Electronic Records; Electronic Signatures"

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11

目次（抜粋）：

サブパート B：電磁的記録（Electronic Records）

SEC. 11.10 CONTROLS FOR CLOSED SYSTEMS.（クローズド・システム管理）

SEC. 11.30 CONTROLS FOR OPEN SYSTEMS.（オープン・システム管理）

SEC. 11.50 SIGNATURE MANIFESTATIONS.（電子署名の要求要素）

SEC. 11.70 SIGNATURE/RECORD LINKING.（電子署名と電磁的記録の紐づけ）

サブパート C：電子署名（Electronic Signature）

SEC. 11.100 GENERAL REQUIREMENTS.

SEC. 11.200 ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS.

SEC. 11.300 CONTROLS FOR IDENTIFICATION CODES/PASSWORDS.

※3 PIC/S GMP Guide ANNEX 11 (Computerised systems)：PE 009-14 (Annexes)

https://picscheme.org/docview/1946

「ＰＩＣ／ＳのＧＭＰガイドラインを活用する際の考え方について」の一部改正について

https://www.pmda.go.jp/files/000202984.pdf

目次（抜粋）：

ANNEX 11　COMPUTERISED SYSTEMS（コンピュータ化システム）

PRINCIPLE（原則）

GENERAL（一般）

1. Risk Management（リスクマネジメント）

2. Personnel（人員）

3. Suppliers and Service Providers（サプライヤーとサービスプロバイダー）

PROJECT PHASE（プロジェクトフェーズ）

4. Validation（妥当性）

OPERATIONAL PHASE（運用フェーズ）

5. Data（電子データ）

6. Accuracy Checks（精度チェック）

7. Data Storage（データストレージ）

8. Printouts（プリントアウト）

9. Audit Trails（監査証跡）

10. Change and Configuration Management（変更および構成管理）

11. Periodic Evaluation（定期的な評価）

12. Security（セキュリティ）

13. Incident Management（インシデント管理）

14. Electronic Signature（電子署名）

15. Batch release（バッチリリース）

16. Business Continuity（事業継続性）

17. Archiving（保管）

3.2. 運用コストと保証レベル

信頼性確保に要する運用コストは、保証レベルに比例する。つまり信頼性の保証レベルを高くする為には運用コストも高くせざるを得ないと言うことである。しかしながら、現実には組織のリソースには限りがあるので、運用コストにも制限が必要になる。そのため、各社では、信頼性保証に関する企業ポリシー（どの程度まで信頼性を要求するか）とリソース（技術の導入に要するコスト、職員による運用管理に要する時間など）に応じた判断が必要になる。本技術ガイドブックで保証レベルの面から 3 段階に分けて 4 章にて説明を行うので、これを参考にして各社で対応を検討いただきたい。なお、既に記載したように真正性を保証する構成要素には「内容保証」「本人保証」「時刻保証」「長期保証」「運用保証」が含まれるが、全体の保証レベルは構成要素の中で一番低い保証レベルによって決定される。例えば、「本人保証」に高い保証レベルの技術を用いたとしても、「長期保証」に低い保証レベルの技術を用いれば、全体の保証レベルは「長期保証」の保証レベルに準じて低下してしまう。そのため、各構成要素に求める保証レベルを合わせることが推奨される。

表 3　標準パッケージの信頼性の保証レベル

保証レベル	概要	説明
レベル１	最低コストの保証運用	出来るだけコストをかけない最低限の運用レベル
レベル２	バランスを考えた運用	コストパフォーマンスに優れた運用レベル
レベル３	最高レベルの保証運用	コストを考えず最高の保証を実現する運用レベル

3.3. パッケージの標準化（標準パッケージ）

測定機器データを長期保存した場合と測定機器データそのものが他社製品にて再解析されることを前提とした場合、自社製品だけで通用するパッケージフォーマットでは完全には対応ができない。検証者が異なる場合を考えると真正性を検証者が確認する為に共通仕様が必要となる。この問題を解決する為にパッケージ構造の標準化を行った標準パッケージの仕様を決めることで相互運用性を保つ。標準パッケージを作成する為に必要となる情報は「標準パッケージ内データ仕様」「目録情報」「追加保証情報」の 3 つがある。

表 4　標準パッケージを作成する為に必要となる情報

情報種別	説明
標準パッケージ内データ仕様	標準パッケージ内に含めるファイルの種類や仕様は本技術ガイドブックには含まない。「測定機器の長期保存ガイダンス」を参照のこと。
標準パッケージ内目録情報	標準パッケージは ZIP 形式を採用し、標準パッケージ内のファイル名一覧と内容保証を行う為に META-INF/Manifest（目録情報）ファイルを標準パッケージ仕様として採用する。基本的に目録情報は必須となる。 また「作成時刻」「作成者」等の情報を META-INF/Index（インデックス情報）も必要となる。
標準パッケージ内追加保証情報	標準パッケージ内の各ファイルの本人保証や時刻保証を行う為の追加保証情報として、META-INF/Signature ファイルと META-INF/Timestamp ファイルを標準パッケージ仕様として採用する。これら追加保証情報は任意である。

3.4. 保証技術の概要

「測定機器の長期保存ガイダンス」の「データが再解析される可能性があることを前提として信頼性を保ったまま長期間に渡り安心して保存管理する方法を提示する」為に、長期保存の標準パッケージを提案している。製薬関連の規則・ガイダンスでは、電磁的記録となる標準パッケージの信頼性を保証する為に「真正性（authenticity）」「見読性（readability）」「保存性（storability）」が求められるが、本技術ガイドブックでは「真正性（authenticity）」を保証するための構成要素として「内容保証」「本人保証」「時刻保証」「長期保証」「運用保証」の 5 つについて 6 章にて説明を行う。「長期保証」には、保存期間内の真正性を保つという意味で「保存性（storability）」も含まれる。「見読性（readability）」については本技術ガイドブックでは解説しない。

表 5　真正性の構成要素

目的	構成要素	説明
何に	6.1. 内容保証	内容が記録時のままであり改ざんされていないことを保証する。 （ALCOA+では Original（原本性）、Accurate（正確性）、Complete（完全性）、 Consistent（一貫性）に関係する）
誰が	6.2. 本人保証	記録の責任者（本人性）を明確化して否認を許さない。（ALCOA+では Attributable（帰属性）、Complete（完全性）に関係する）
いつ	6.3. 時刻保証	記録時刻（タイムスタンプ）の保証（存在確認）。（ALCOA+では Original（原本性）、Contemporaneous（同時性）に関係する）
保存	6.4. 長期保証	長期間に渡る内容保証や本人保証を有効にする為の保証、および保存する為の技術やフォーマット。（ALCOA+では Enduring（永続性） Available（可用性） 、Legible（判読性・見読性）に関係する） ※ 「測定機器の長期保存ガイダンス」では長期保存の期間として 10～30 年を想定しており、本技術ガイドブックも 10～30 年とする。
運用	6.5. 運用保証	全体として適切な運用を行い、運用を文書化し監査して保証する。 ※ 運用に関しては 6.1～6.4 全てに関連するベースとなる保証となる。

4. 標準パッケージの運用

真正性を保証する場合に運用は非常に重要な構成要素となるため、本章では標準パッケージの運用について中心に論じる。標準パッケージの運用を考慮するためには、最初に標準パッケージが作成されてから再解析に至るまでのワークフローを理解する必要がある。その上で標準パッケージの真正性の保証方法を考察する。

4.1. 標準パッケージのワークフロー

以下の図表にて、標準パッケージのワークフローを示す。

表 6　標準パッケージのワークフロー

ステップ	利用	説明	目的
⓪ 測定・解析	測定ソフト 解析ソフト	測定し、最初の解析を行う。	
① エクスポート	HPLC データ管理システム	解析に必要となるデータ群をエクスポート用フォルダに出力する。	保管
② パッケージ作成	パッケージツール	エクスポート用フォルダ中のファイルと必要に応じて外部から与えられた情報も使ってメタデータを作成し、ZIP で固めて標準パッケージファイルを作成し記録する。 エクスポートから標準パッケージ作成までデータが改ざんされないようにアクセス権の設定や運用を考える。 エクスポート用フォルダは一時領域でありパッケージ作成後に削除する。	
③ アップロード（書き込み）	データ保管サーバー（リライト不可媒体）	標準パッケージファイルをサーバー上にアップロードする。サーバー側では誰がいつアップロードしたか記録する。 アップロードされたファイルが改ざんされないようにアクセス権の設定や運用を考える。 リライト不可媒体に保存しても良い。	
④ ダウンロード（読み出し）	データ保管サーバー（リライト不可媒体）	再解析するデータの標準パッケージを検索してダウンロードする。サーバー側では誰がいつダウンロードしたか記録する。リライト不可媒体からの読み出しの場合もある。	再解析
⑤ 検証と解凍	パッケージツール	標準パッケージファイルの検証を行い、真正性（改ざん等）を確認して、インポート用フォルダに標準パッケージ内データを出力する。	

ステップ	利用	説明	目的
⑥ インポート	HPLC データ管理システム	インポート用フォルダからデータ群をインポートして記録する。 検証解凍からインポートまでデータが改ざんされないようにアクセス権の設定や運用を考える。 インポート用フォルダは一時領域でありインポート後に削除する。	
⑦ 再解析	解析ソフト	再解析を行う。	

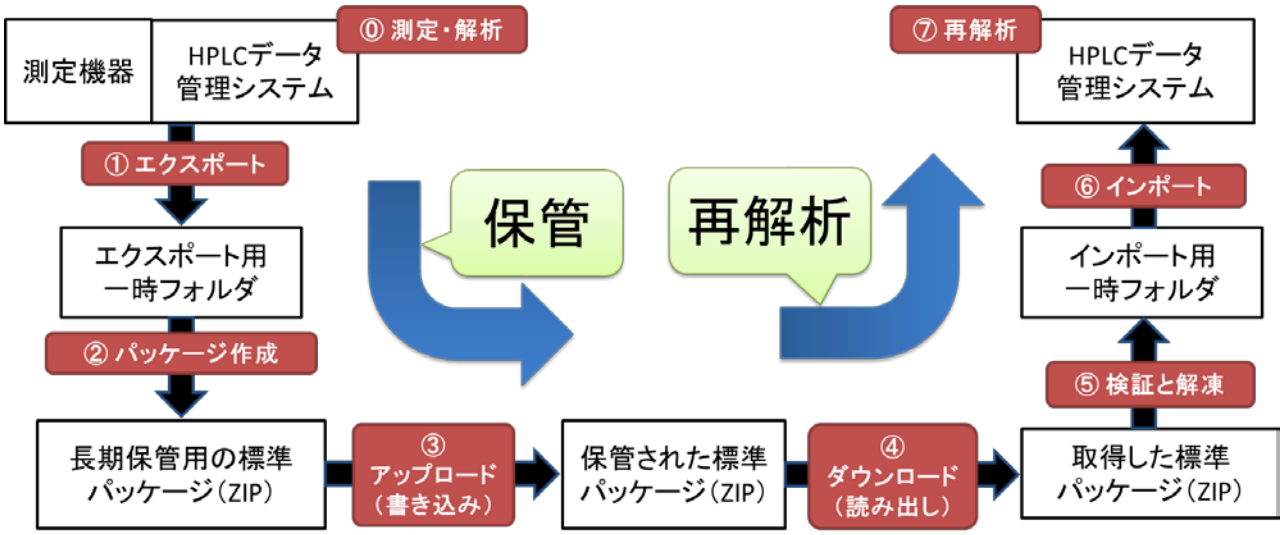

図 1　測定機器データの流れ

この際、測定機器データが長期保存された後に社内で利用される場合と、社外に測定機器データを送付して利用する場合の 2 種類が想定される。また、保存方法には、サーバーと電磁的記録媒体の 2 種類が想定される。この組み合わせを考慮すると以下の 4 種類の運用パターンが想定されるが、これに限定されない。

表 7　想定される運用パターン

	エクスポート時のデータ処理サーバー	ストレージ	インポート時のデータ処理サーバー
パターン 1	社内サーバー	社内サーバー	社内サーバー
パターン 2	社内サーバー	電磁的記録媒体（CD、DVD 等） ※　リライト不可	社内サーバー
パターン 3	A 社内サーバー	クラウドサーバー	B 社内サーバー
パターン 4	A 社内サーバー	電磁的記録媒体（CD、DVD 等） ※　リライト不可	B 社内サーバー

これらの 4 パターンにおける標準パッケージのワークフローは、以下のように図式化される。

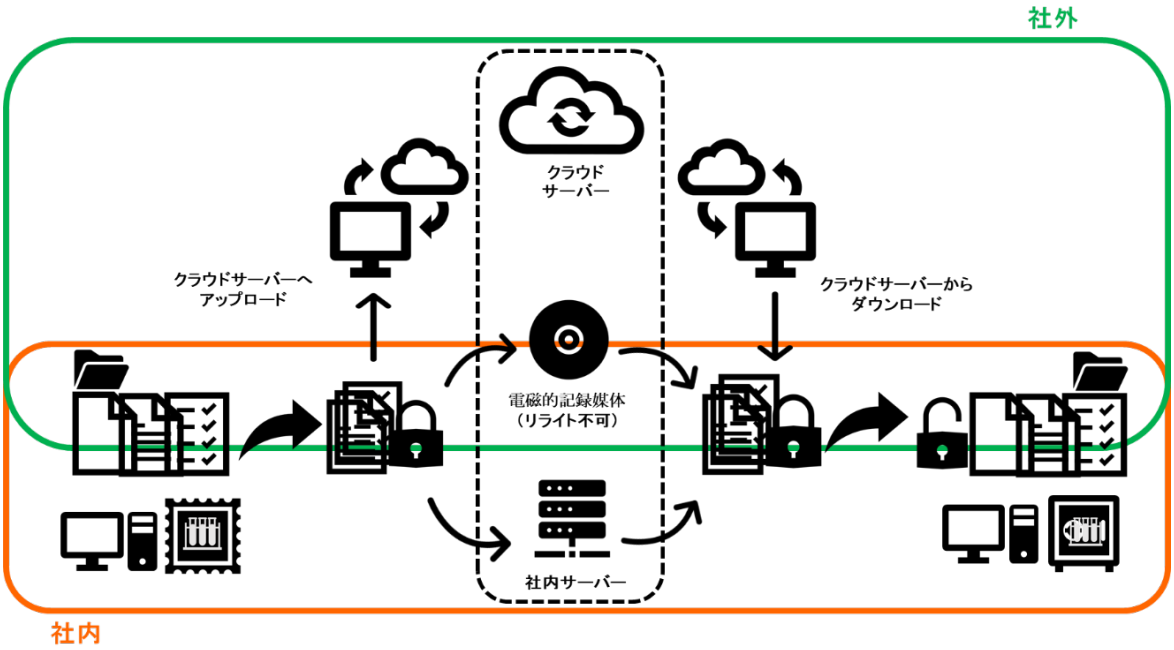

図 2　運用の概念図

実際に運用する例として、社内等のクローズド環境で運用する場合とクラウドを利用したオープン環境も使って運用する場合のワークフローを示す。

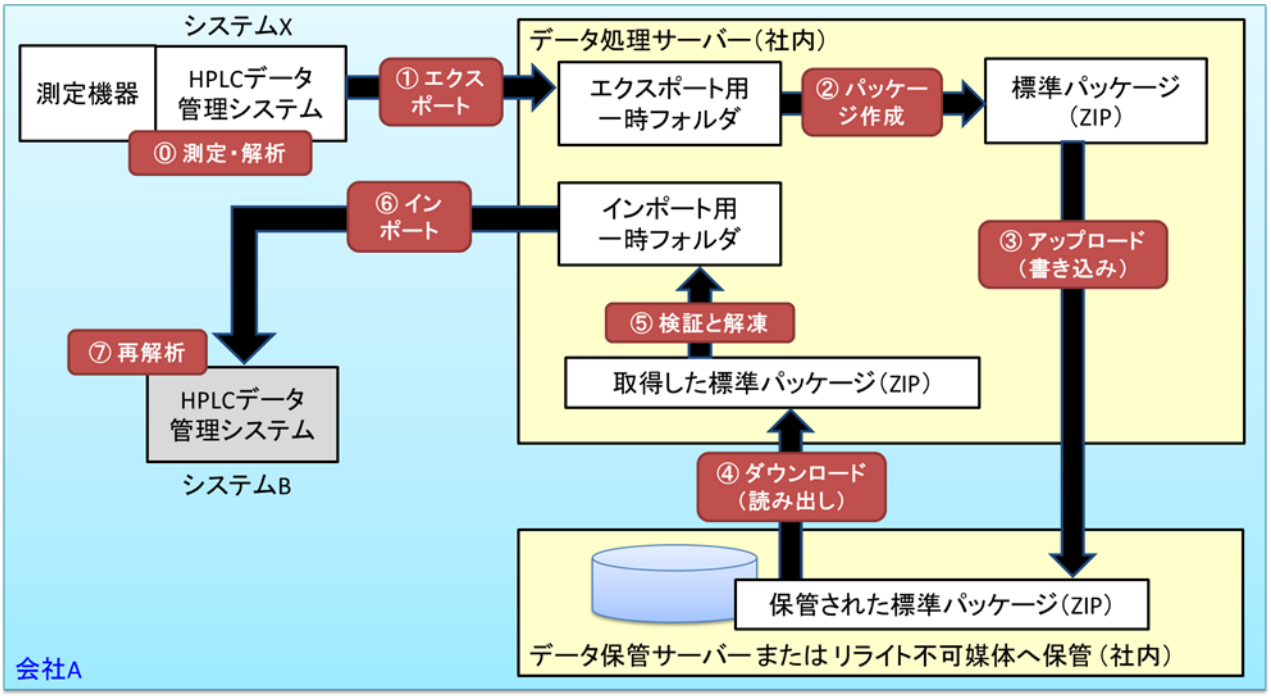

図 3　測定機器データの流れ：社内のクローズド環境の例

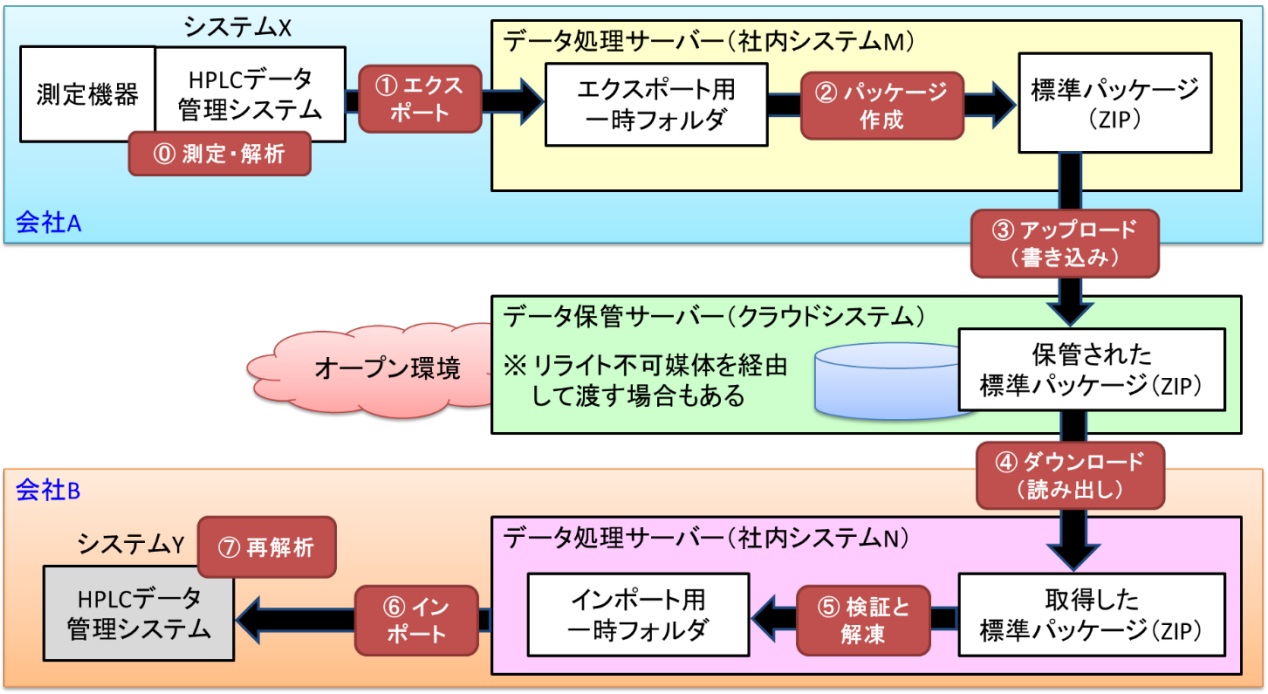

図 4　測定機器データの流れ：オープン（クラウド）環境の例

クローズド環境とオープン環境では求められるセキュリティ要件の内容が異なる。「ER/ES 指針」や「米国 Part11」では、これらは別の章として要件がまとめられている。一般的にはオープン環境の方がより高いセキュリティのレベルを求められる。しかし、パッケージの利用する状況を考えた時には、いずれも同等な管理が必要になる可能性がある。以下で段階を追って説明する。

社内にあるようなクローズド・システム（測定機器を含む）を利用する場合には、電子署名等による内容保証と本人保証が求められる。クラウドのように外部に置かれるオープン・システムを利用する場合には、クローズド・システムに求められる要件に加えて暗号化等による機密性や、作成手順や利用手順において真正性を保てるような運用保証の検討も求められる。

しかしながら、クローズド・システムで標準パッケージが作成されたとしても、システム外に提供する場合がある（例えば、試験受託者（CRO）からスポンサーに対してパッケージを提供する場合など）。この場合には標準パッケージにオープン・システムに求められる追加要件への対応（デジタル署名やタイムスタンプによる内容保証など）を行うことが望ましい。

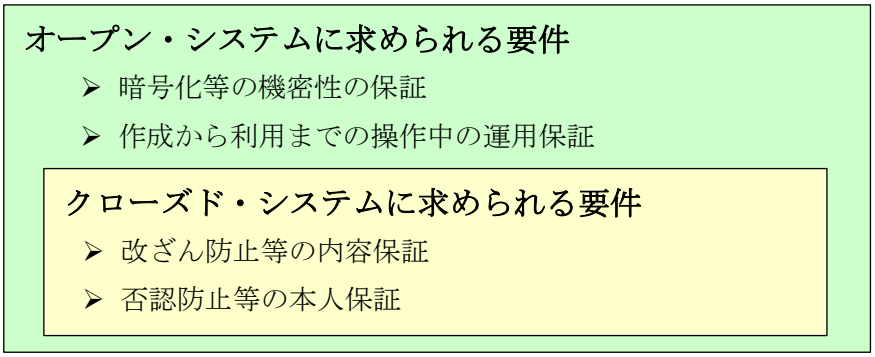

図 5　クローズド・システムとオープン・システムに求められる要件

4.2. 標準パッケージの真正性保証の前提条件

標準パッケージ格納前の測定機器データは、各施設において、保存目的に応じたレベルでの適切な信頼性が確保されていることが必須である。GxP 準拠で運用を行う場合、パッケージ化前の測定機器データのデータインテグリティが確保されているという前提の下で、測定機器データをエクスポートしてから新たなシステムにインポートするまでのプロセスの適切性を第三者（QA など）が保証する必要がある（測定機器の長期保存ガイダンス 4.3 項参照）。なお、このプロセスが自動化できる場合、自動化に関わるプログラムの導入時に適切にバリデーションを実施して自動化されたプロセスの信頼性を確保することにより、運用時の第三者による保証業務を軽減することができる。

4.3. 運用コスト別の標準パッケージの保証方法の例

6 章で説明する真正性保証の各構成要素と、5 章で説明する標準パッケージの仕様を、選択して組み合わせることで自社の運用仕様を決める必要がある。本項では運用仕様を検討する際に参考となるように、運用コスト別に 3 段階の運用方法を提案する。

4.3.1. 保証レベル１：最低コストの保証

運用コストを抑えて最低限達成すべき運用をここに示す。基本的に外部サービスや PKI（認証局）は使わない。標準パッケージの改ざんは可能であるが、ハッシュ値が各プロセスで変更されていないか監視することにより改ざんを検知し、改ざんを検知した場合にはそのパッケージを利用しないなどの運用により改ざんを防止する。ハッシュ値計算により作成時からの改ざんに関しては第三者によるチェックが可能となる。

表 8　ケース１：自社でデータ保管サーバーを構築して運用

項目	内容
内容保証	ハッシュ値または操作記録による改ざん検知を行う。参照：6.1.3 / 6.1.1 ※　改ざん保証は保管するサーバーの運用等で対応する必要がある。 ※　操作記録による改ざん検知による内容保証でも構わない。

項目	内容
本人保証	認証記録を利用する。参照：6.2.1 ※ 例えば ID とパスワードによる認証管理と監査ログ保管
時刻保証	システム時刻を利用する。参照：6.3.1
長期保証	データ保管サーバー内に保管する。参照：6.4.1 または電磁的記録媒体に保管する。参照：6.4.2
運用保証	運用ポリシーを作成し、監査証跡として監査ログの保管を行い、運用監査を受ける。 参照：6.5.1 / 6.5.2/ 6.5.3
パッケージ仕様	ハッシュ値計算の Manifest ファイルにより内容保証する。 参照：5.1.1
コスト	外部サービスを使っていないので運用コストはほぼかからない。 それを補完するプロセスにリソースが必要になる可能性はある。

4.3.2. 保証レベル２：バランスを考えた運用

運用コストと保証レベルのバランスを考えた 3 種類の運用方法をここに示す。

4.3.2.1. 電子文書管理システムを利用する場合

ベンダー提供されている電子文書管理システムを導入するコストの負担が許容される場合は、最小限の機能は実現が出来る。パッケージソフトウェアを自社に導入する場合には一般に初期費用と保守費用が必要となる。これに対して、クラウドサービスを利用する場合には、定期的な運用コストが必要となるが、既に機能実装がされているソフトウェアやサービスを利用出来るので、導入が容易であると言う利点がある。標準パッケージ化したファイルを電子文書管理システムに保管しても構わないし、保管時には標準パッケージ化せずそのまま保管しておき外部にデータを提供する時に標準パッケージ化しても良い。

表 9　ケース２：市販されている電子文書管理システムを利用

項目	内容
内容保証	操作記録による改ざん検知による内容保証を行う。参照：6.1.1 ※ ベンダー提供の電子文書管理システムを利用する。
本人保証	認証記録を利用する。参照：6.2.1 ※ ベンダー提供の電子文書管理システムの認証機能を利用する。
時刻保証	システム時刻を利用する。参照：6.3.1 ※ 電子文書管理システムをパッケージソフトウェアとして自社に導入する場合には、自社サーバーのシステム時計を利用する。 ※ クラウドサービスを利用する場合には、ベンダー提供の電子文書管理管システムのシステム時計を利用する。

項目	内容
長期保証	電子文書管理システム内に保管する。参照：6.4.1
運用保証	運用ポリシーを作成し、監査証跡として監査ログの保管を行い、運用監査を受ける。 参照：6.5.1 / 6.5.2/ 6.5.3
パッケージ仕様	外部にデータを提供する場合には標準パッケージを利用する。必要に応じてハッシュ値計算の Manifest ファイルとタイムスタンプの Timestamp ファイル、またはデジタル署名の Signature ファイルにより内容保証する。参照：5.1.1 / 5.1.2 / 5.1.3 / 5.1.4
コスト	電子文書管理システム利用（運用）のコストが必要となる。

4.3.2.2. タイムスタンプサーバーを利用する場合

タイムスタンプを利用することで標準パッケージの改ざん防止を行うこともできる。タイムスタンプサーバーの運用コストはかかるが保証レベル１に比較して標準パッケージ単体として改ざん防止性は高くなる。外部のタイムスタンプサービスを利用すれば高保証レベルが保証されタイムスタンプサーバーの運用が不要となるがサービス利用の運用コストはかかる。

表 10　ケース３：タイムスタンプサーバーを利用

項目	内容
内容保証	タイムスタンプによる改ざん防止を行う。参照：6.3.2
本人保証	認証記録を利用する。参照：6.2.1 ※　例えば ID とパスワードによる管理と監査ログ保管
時刻保証	タイムスタンプサーバーを利用する。参照：6.3.2 ※　外部のタイムスタンプサービスは有償であることが多いので、運用コストを削減するために社内でタイムスタンプサーバーを運用することを検討しても良い。
長期保証	データ保管サーバー内に保管する。参照：6.4.1 または電磁的記録媒体に保管する。参照：6.4.2
運用保証	運用ポリシーを作成し、監査証跡として監査ログの保管を行い、運用監査を受ける。 参照：6.5.1 / 6.5.2/ 6.5.3
パッケージ仕様	ハッシュ値計算の Manifest ファイルとタイムスタンプの Timestamp ファイルにより内容保証する。参照：5.1.1 / 5.1.2 / 5.1.4
コスト	タイムスタンプサーバーの構築コストまたは外部タイムスタンプサービスの利用の運用コストが必要となる。ただし、外部タイムスタンプサービスを利用すれば、より高いレベルの保証が得られるのでコスト増に見合う保証となる。

4.3.2.3. プライベート認証局によるデジタル署名を利用する場合

バランスを考えた運用として、デジタル署名に社内認証局（プライベート PKI）を構築して運用する方法も考えられる。

表 11　ケース４：プライベート認証局によるデジタル署名を利用

項目	内容
内容保証	デジタル署名による改ざん防止を行う。参照：6.2.2
本人保証	社内認証局（プライベート PKI）を構築して発行した証明書を利用する。 参照：6.2.2 ※　例えば利用者毎に署名用の証明書/秘密鍵を用意してデジタル署名する。 外部に対するコストは無くなるが、社内での運用コストは必要となる。
時刻保証	システム時刻を利用する。参照：6.3.1
長期保証	データ保管サーバー内に保管する。参照：6.4.1 または電磁的記録媒体に保管する。参照：6.4.2 ※　社内タイムスタンプサーバーがあれば長期署名化も可能となる。
運用保証	運用ポリシーを作成し、監査証跡として監査ログの保管を行い、運用監査を受ける。 参照：6.5.1 / 6.5.2/ 6.5.3
パッケージ仕様	ハッシュ値計算の Manifest ファイルとデジタル署名の Signature ファイルによる内容保証をする。Signature ファイルにはデジタル署名のみ。 参照：5.1.1 / 5.1.2 / 5.1.3
コスト	プライベート認証局の場合には運用コストはあまりかから無いが、構築と運用にはある程度以上の専門知識を必要とする為に人的コストは必要となる。

4.3.3. 保証レベル３：最高レベルの保証（高コスト）

公的な認証局やタイムスタンプサービスを利用することで運用コストはかかるが最高レベルの保証を行うことができる。

表 12　ケース５：外部の公的な認証局とタイムスタンプサービスを利用

項目	内容
内容保証	デジタル署名による改ざん防止を行う。参照：6.2.2
本人保証	公的な認証局（パブリック PKI）を利用して発行した証明書を利用する。 参照：6.2.2 ※　公的な認証局より証明書/秘密鍵を購入してデジタル署名する。

項目	内容
時刻保証	外部のタイムスタンプサービス（タイムスタンプサーバー）を利用する。 参照：6.3.2 ※ 第三者が保証する時刻であり信頼性は高いがサービスを契約する必要があり運用コストがかかる。
長期保証	データ保管サーバー内に保管する。参照：6.4.1 または電磁的記録媒体に保管する。参照：6.4.2 どちらに保管するにしても長期署名により保証期間を延長して行く。 参照：6.4.3
運用保証	監査証跡として監査ログの保管を行い、運用監査も受ける。 参照：6.5.1 / 6.5.2 / 6.5.3
パッケージ仕様	ハッシュ値計算の Manifest ファイルとデジタル署名の Signature ファイルによる内容保証をする。Signature ファイルはデジタル署名＋タイムスタンプによる長期署名の形式とする。参照：5.1.1 / 5.1.2 / 5.1.3 / 6.4.3 ※ 長期署名化することで内容保証・本人保証・時刻保証・長期保証を標準パッケージ単位で保証や検証することが可能となる。この為に標準パッケージ単体で流通（社外への提供等）にも最適な形式となる。
コスト	認証局からの証明書購入コストに加えて、タイムスタンプサービスの運用コストが必要となる。また長期署名を利用する為に必要タイムスタンプ数も増加するので回数課金のタイムスタンプサービスではよりコスト増となる。

5. 標準パッケージ

本章では相互運用性に関して、「5.1. 標準パッケージ仕様」と「5.2. 標準パッケージのワークフロー」の 2 つに分けて技術的な説明を行う。

5.1. 標準パッケージ仕様

測定機器データの為の標準パッケージ仕様として、ZIP 形式と XML を採用する。標準パッケージに関するメタ情報は META-INF ディレクトリの中に置く。これは多くの既存の標準化されたパッケージ（OOXML, ODF, EPUB 等）の仕様でも採用されている方式である。ただし META-INF の中に何を置くのかは標準化された仕様毎に異なる。

表 13　META-INF 中に追加するファイル

ファイル名	作成	種類	説明
Index.xml	必須	インデックス情報	補足的情報を記載する。
Manifest.xml	必須	目録情報	対象となる測定機器データの参照先（URI）とそのハッシュ値を記録するファイル。
Signature.xml	任意	デジタル署名情報	目録情報をデジタル署名で保証する為のファイル。本人保証と改ざん防止が可能（タイムスタンプを追加すれば更に時刻保証も可能になる）
Timestamp.tst	任意	タイムスタンプ情報	目録情報をタイムスタンプで保証する為のファイル。改ざん防止と時刻保証が可能。

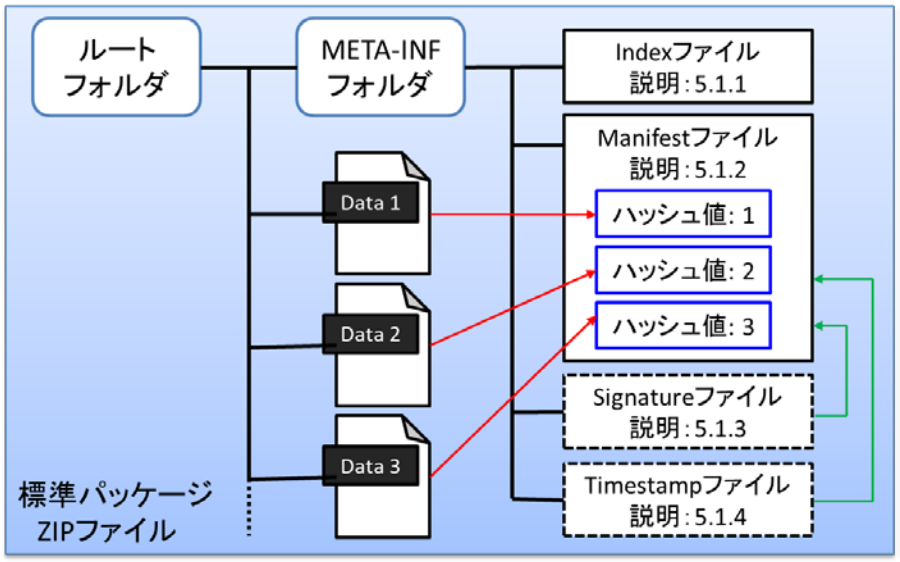

図 6　標準パッケージ内の構造例

5.1.1. META-INF/Index ファイル（必須：インデックス情報）

本標準パッケージのために、META-INF/Index ファイルという独自の仕様を検討した。このファイルの拡張子を.xml とし、ファイルのフルパスは META-INF/Index.xml とした。Index ファイルには、最低でも作成日時と作成者 ID の情報を記載する必要があるが、ファイルの内容の理解のために測定データの名称や検索キーワードなどを格納することが望ましい。更に必要であれば、本仕様に追加の情報を指定することができる。Index ファイルは Manifest の参照対象に含まれないので、署名後に更新しても差し支えない。

表 14　Index の XML 仕様

XML タグ名		指定	属性	説明
Index		必須	（Id="識別子"）	Index ルート要素。
	Title	任意	---	測定データの名称。
	Date	必須	---	作成日時。利用しているシステムの時刻で良い。
	User	必須	---	作成者 ID（ログインユーザ ID 等） ※　認証時のユーザ ID が使えると最適。
	Host	任意	---	作成システム名（コンピュータ名や IP アドレス等）
	Keyword	任意	---	検索用のキーワード（複数指定可）。
	（任意）	任意	---	その他任意の XML タグ名を追加可能。

※　Index ファイルの形式は本標準パッケージの独自仕様。

Index ファイルの例：

```
<Index>
 <Title>サンプルデータ</Title>
 <Date>2021-02-26T13:50:20</Date>
 <User>hanako</User>
 <Host>MyPC1</Host>
</Index>
```

5.1.2. META-INF/Manifest ファイル（必須：目録情報）

標準パッケージでは必須となる Manifest（マニフェスト）ファイルは目録情報とも呼ばれる。測定機器データの為の標準パッケージでは、XML 署名（W3C 勧告の標準仕様）に含まれる Manifest 形式を採用する。この為に拡張子を xml とし、ファイルのフルパスを META-INF/Manifest.xml とした。このファイルには、複数の測定機器データおよび関連情報ファイルが指定され、各対象ファイルのハッシュ値が記録される。そのため、各対象ファイルが改ざんされた場合には、Manifest 中のハッシュ値と再計算されたハッシュ値が一致しなくなるので、対象ファイルの改ざんの検知が可能となる。当然のことながら、Manifest ファイルによって Manifest ファイル自体を改ざん防止することは不可能である。Manifest ファイルの改ざん防止の為には、別途 Signature ファイルや Timestamp ファイルによる保護が必要となる。

表 15　Manifest の XML 仕様

XML タグ名	指定	属性	説明
Manifest	必須	（Id="識別子"）	Manifest ルート要素。
Reference	必須	URI="対象"	参照先の URI 指定（複数指定可）。
DigestMethod	必須	Algorithm="ハッシュ方式"	ハッシュ計算のアルゴリズム指定。
DigestValue	必須	---	ハッシュ値を Base64 化して格納。

※ XML 署名仕様では Reference タグの下に Transforms タグの利用が可能であるとバイナリファイルとして扱う場合は省略可能。もし XML ファイルが対象に含まれる場合には Transforms タグを指定しても良い。

※ XML Signature Syntax and Processing Version 1.1 - W3C Recommendation 11 April 2013
https://www.w3.org/TR/xmldsig-core1/

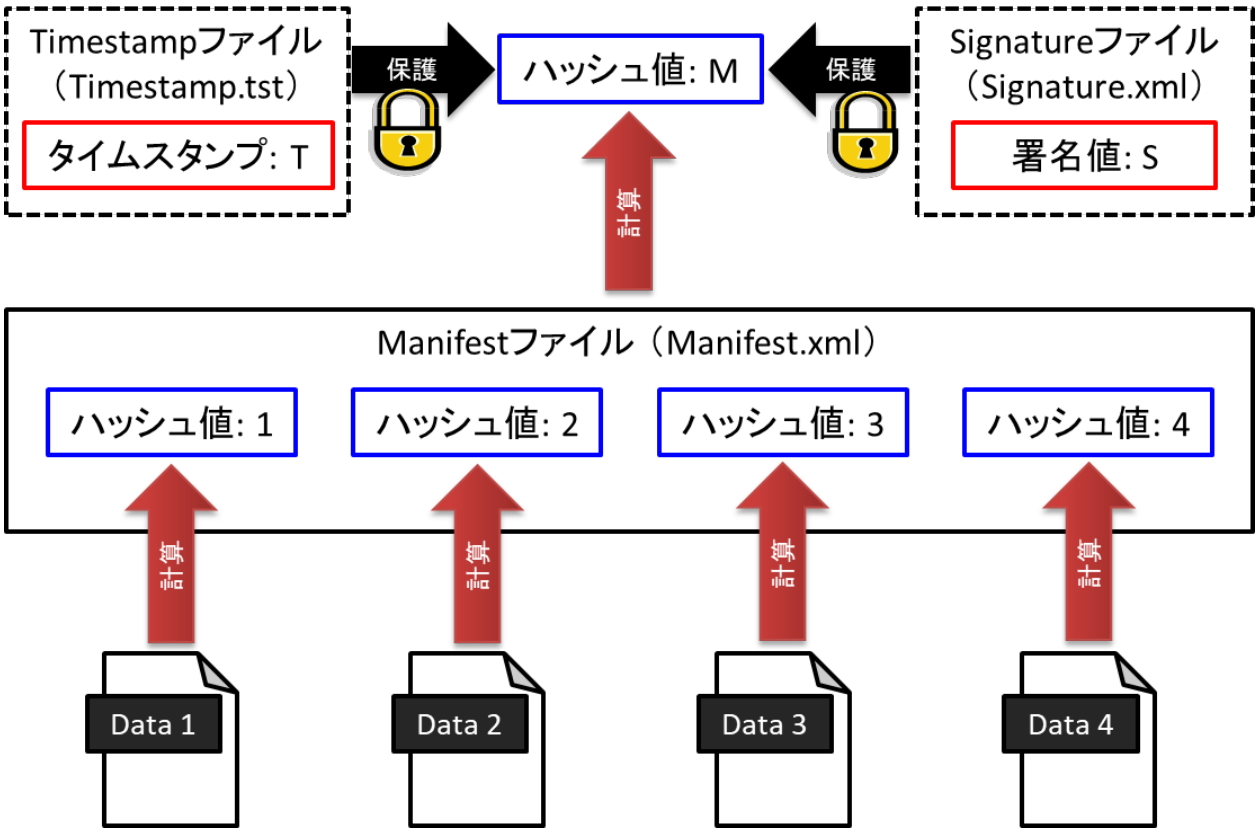

図 7　各ファイルによる内容保証の関連図

Manifest ファイルの例：

```
<?xml version="1.0" encoding="utf-8"?>
<Manifest Id="Id-Manifest-0" xmlns="http://www.w3.org/2000/09/xmldsig#">
 <Reference URI="../Demo_Data-001.lcd">
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512" />
  <DigestValue>
   EA7YFkhjtpUDcCC+SwK9A1lHW+Swxh4G1dUMmLsAItyCj5y8SLhvzRcvK/jOf9+5k2R6W6N7n6WL+vUx5eTRRQ==
```

```
  </DigestValue>
 </Reference>
 <Reference URI="../Result File/Demo_Data-001.pdf">
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512" />
  <DigestValue>
   3nJV5vSblaRvUffKPoCiDkZE1mYI4KozwWZxrEpzY84M6fi0a7LY07fy7G5cYbgzkQ0hlJAKoc0do2xIgLFq1A==
  </DigestValue>
 </Reference>
 <Reference URI="../Result File/Detector-A-Ch1.CDF">
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512" />
  <DigestValue>
   azc6e4JEdku0wmiilWKDcJl7hvBebt8ORB12pqumdvDhx2CfYochudHzwJjvKUzAJyTlHBTWU7YZk6s2Udk+iQ==
  </DigestValue>
 </Reference>
</Manifest>
```

5.1.3. META-INF/Signature ファイル（任意：追加本人保証情報）

本人保証の為のデジタル署名を標準パッケージに付与する場合に Signature ファイルを追加する。ここでは、XML 署名を長期署名化した XAdES（ISO 14533-2）を採用する。拡張子を.xml とし、ファイルのフルパスは META-INF/Signature.xml とする。署名のみであれば XAdES-BES 形式を利用し、XAdES-T を採用することでタイムスタンプを追加して時刻保証をすることも可能である（XAdES-BES / XAdES-T に関しては 6.4.3 項で説明）。署名対象（SignedInfo/Reference）として、META-INF/Manifest.xml と XAdES 署名対象属性（SignedProperties）の 2 つを指定する。

表 16　XAdES の XML 仕様

XML タグ名	指定	属性	説明
Signature	必須	（Id="識別子"）	Signature ルート要素。
---	必須	---	※ XAdES 仕様に従う

※ ISO/DIS 14533-2 - Part 2: profiles for XML Advanced Electronic Signatures (XAdES)
https://www.iso.org/standard/79129.html

5.1.4. META-INF/Timestamp ファイル（任意：追加時刻保証情報）

時刻保証の為のタイムスタンプを標準パッケージに付与する場合に Timestamp ファイルを追加する。タイムスタンプだけを付与する XML ベースの仕様は存在しない為に、タイムスタンプトークン（RFC 3161 仕様、6.3.2 項で説明）を採用する。タイムスタンプトークンの対象となるハッシュ値（MessageImplint）は、Manifest.xml をバイナリファイルとして計算した値となり、ファイルのフルパスは META-INF/Timestamp.tst となる。

※ RFC 3161 - Time-Stamp Protocol (TSP)
https://tools.ietf.org/html/rfc3161

5.2. 標準パッケージの利用手順

本章では、4,1 項で論じた標準パッケージのワークフローを達成するための技術的な考え方を記載する。この手順に基づいて職員が手作業で標準パッケージの作成や解凍を行うこともできるし、自動化ツールに基づいてこの手順を達成することもできる。現在、本技術ガイドブックに基づくパッケージの作成や検証のために本委員会の委員により自動化ツールとデータ保管サーバーが提供されたので、それを用いてこのワークフローが実現可能か否かを検討している。後日、そのトライアルの結果を別添資料として提供する予定のため、そちらも参照していただきたい。

標準パッケージの作成に至るプロセスを 5.2.1 項に、再解析のために標準パッケージを解凍・検証するためのプロセスを 5.2.2 項に示す。

5.2.1. 標準パッケージ作成手順（保管時）

標準パッケージを作成するには「インデックス作成機能」「目録情報作成機能」「ZIP 化機能」が最低限必要となる。加えて真正性を保証する為のオプション機能として「デジタル署名作成機能」や「タイムスタンプ取得機能」を必要に応じて準備する。

表 17　標準パッケージの作成手順

手順	概要	説明
1	前準備	標準パッケージ化する全測定機器データを任意のフォルダに用意する。
2	作成１	作成日時や検索キーワード等のインデックス情報（META-INF/Index.xml）を作成する。
3	作成２	フォルダ内の全ファイルを Reference してハッシュ値を計算した目録情報（META-INF/Manifest.xml）を作成する。
4	真正性	省略可能：標準パッケージの真正性を保つためのファイルとして、デジタル署名（META-INF/Signature.xml）やタイムスタンプ（META-INF/Timestamp.tst）を作成する。
5	パッケージ	フォルダ内の全ファイル（META-INF フォルダ含む）を ZIP 化する。
6	後始末	作成した標準パッケージ（ZIP ファイル）以外のファイルを削除する。 ※　手順１～４で用意または作成した一時ファイルを削除する。
7	保管	作成した標準パッケージの保管操作を行う。

5.2.2. 標準パッケージ検証手順（再解析時）

標準パッケージを検証するには「ZIP 解凍機能」「目録情報検証機能」が最低限必要となる。加えて必要に応じて「デジタル署名検証機能」や「タイムスタンプ検証機能」を用意する。

表 18　標準パッケージの検証手順

手順	概要	説明
1	前準備 1	標準パッケージ化されたファイルを指定する。
2	前準備 2	標準パッケージ化されたファイルを ZIP 解凍して、任意のフォルダに標準パッケージ内の全ファイルを展開する。
3	検証 1	目録情報（META-INF/Manifest.xml）に記載されている全ファイルの存在と、ハッシュ値を計算して記載されているハッシュ値と突合する。一致しない場合には内容を確認して対応を検討する。
4	検証 2	標準パッケージにデジタル署名（META-INF/Signature.xml）やタイムスタンプ（META-INF/Timestamp.tst）のファイルが含まれている場合には、それぞれの内容を検証する。検証エラーを生じた場合には内容を確認して対応を検討する。
5	利用	解凍された測定機器データを使って再解析を行う。

6. データ保証の基礎知識

本章では測定データの信頼性を保証する為に必要となる真正性の基礎知識として「内容保証」「本人保証」「時刻保証」「長期保証」「運用保証」の 5 つの保証内容毎に一般的な技術の説明をする。

6.1. 内容保証（改ざん検知・改ざん防止）

内容保証では、主に保存時から改ざんが無いことを保証する為に改ざん検知を行う。なお保存時において正しい内容であると言う前提があるので運用においては注意すること。

表 19　内容保証方式概要

方式	説明
6.1.1. 操作記録	データに対する操作イベントをログとして記録することで不正な操作による改ざんが無かったことを保証する。他の内容保証方式との併用も推奨される。運用システムの構築時にどのような記録を残すのか設計する必要がある。
6.1.2. 暗号化	データの移動経路において、暗号化することで改ざんされないこと（機密性）を保証する。暗号化したまま保管することも可能であるが、その場合には復号鍵の管理を行う必要がある。
6.1.3. ハッシュ値	データの指紋となる値。データが 1 ビットでも変更された場合には全く異なる値となり改ざんを検出できる。
6.1.4. ハッシュ木	複数データのハッシュ値をまとめて 1 つのハッシュ値にする方法。複数かつ大量のデータの改ざん検知を 1 つのハッシュ値で行うことができる。
6.1.5. ハッシュチェーン	ハッシュ値を含むデータのハッシュ値を計算することでチェーン状に連鎖する方法。1 つでもハッシュ値が変更されるとそれ以後全てに影響を与えるので改ざん検知ができる。デジタル署名を利用することでブロックチェーンとすることができる。
6.1.6. デジタル署名	ハッシュ値にデジタル署名することで改ざん防止を実現する。

6.1.1. 操作記録による保証

データに対する「認証」「作成」「参照」「変更」「確認」「承認」等の操作記録を保存しておき、不正なアクセスによる改ざんが無かったことを保証する。アクセス制御とも呼ばれる。システムの運用のみで対応できる基本的な改ざん検知の手法であり、運用する全てのシステム（サーバー）において操作記録を保存することが推奨される。最初のシステム構築時に手順やポリシーを決めて後はそれらを守るだけで済む為に、運用コストも低い。

ベンダー提供されている電子文書管理システムではアクセスコントロールの為に、認証機能と操作記録の保管機能が提供されているので、運用ポリシーを策定して操作記録をきちんと保管することで内容保証を容易に実現できる。ただし電子文書管理システムの導入時には必要十分な情報が保

管されることを確認すべきである。

6.1.2. 暗号化（機密性）

オープンな環境にてデータを保存または移動する場合には、暗号化し暗号鍵を秘匿することで不正なアクセスや改ざんを防止することができる。ただし暗号鍵が移動先に安全に渡されるようにする必要がある。暗号化ではデータの保護は出来るが改ざん検知は出来ないので改ざん検知の為には、操作記録やハッシュ値による保証と組み合わせる必要がある。暗号化したまま長期間保管する場合には暗号アルゴリズムの危殆化（暗号が破られることで 6.1.3.にて説明）にも注意する必要がある。現在推奨される暗号方式は、AES 暗号は鍵長 128bit 以上、RSA 暗号は鍵長 2048bit 以上となる。一般に鍵長が大きい程安全性は高くなるが処理が遅くなる傾向がある。

6.1.3. ハッシュ値（改ざん検知）

改ざんからデータを守るにはハッシュアルゴリズム（ダイジェストアルゴリズムとも言われる暗号アルゴリズムの一種）を利用することが一般的である。ハッシュアルゴリズムは暗号アルゴリズムの 1 種であり、現在は SHA-2 方式が推奨ハッシュアルゴリズムとして使われている。ハッシュアルゴリズムでは対象となるデータが 1 バイトでも変更されると全く異なる関連性が無いハッシュ値となる。このことからハッシュ値は「データの指紋（フィンガープリント）」とも呼ばれる。ハッシュ値単体ではハッシュ値自体も変更が可能である為に改ざん防止はできないので、別途デジタル署名やタイムスタンプ等で保護した方が良い。

ハッシュ値は数学的に計算されるが、天文学的な確率では異なるデータで同じハッシュ値となる場合（ハッシュ値の衝突）もあり得る。しかしながら同じハッシュ値を持つデータを作成することは極めて困難であるが、もし意図的に同じハッシュ値のデータを作成できるようになった場合にはそのハッシュアルゴリズムは「危殆化」したと判定されて利用が非推奨となる。例えばこれまで良く使われて来たハッシュアルゴリズムとして、MD5 は既に意図的に同じハッシュ値を持つデータ生成が可能（危殆化）となっており、SHA-1 も危殆化の可能性が高くなって来ていることから、MD5 と SHA-1 の利用は、米国の NIST や日本の CRYPTREC にて非推奨となっている。長期間保存する場合に利用するハッシュアルゴリズムは以下の 2 点に注意する必要がある。

表 20　暗号アルゴリズム利用時の注意点

1	保存必要期間内にアルゴリズムが危殆化する恐れが少ないこと。
2	もしも危殆化した時に新しいアルゴリズムで再度計算し直せること。

この 2 点はハッシュ値に限らず全ての暗号アルゴリズムにおいて共通するとても大事な注意点である。暗号アルゴリズムにも有効期限が存在することを理解した上で利用する必要がある。

※　日本：CRYPTREC 暗号リスト(電子政府推奨暗号リスト)
https://www.cryptrec.go.jp/list.html

※ 米国：NIST SP800 シリーズ(セキュリティ関連 NIST 文書)
https://csrc.nist.gov/publications/sp800

※ 日本：セキュリティ関連 NIST 文書
https://www.ipa.go.jp/security/publications/nist/

6.1.4. ハッシュ木（複数対象の改ざん検知）

1 つのハッシュ値では通常 1 つのデータのみを改ざんから守ることになる。しかし対象となるデータが多数になると管理するハッシュ値の数も増えてしまう。この為にハッシュ値を木（ツリー）状に組合せて全体を守る 1 つのハッシュ値を得る「ハッシュ木（マークル木とも呼ばれる）」と言う技術がある。ハッシュ木では頂点に位置する 1 つのハッシュ値（トップハッシュ値）を守ることで、下位にある全てのハッシュ値を守り、全ての対象データの改ざん検知を行うことができる。

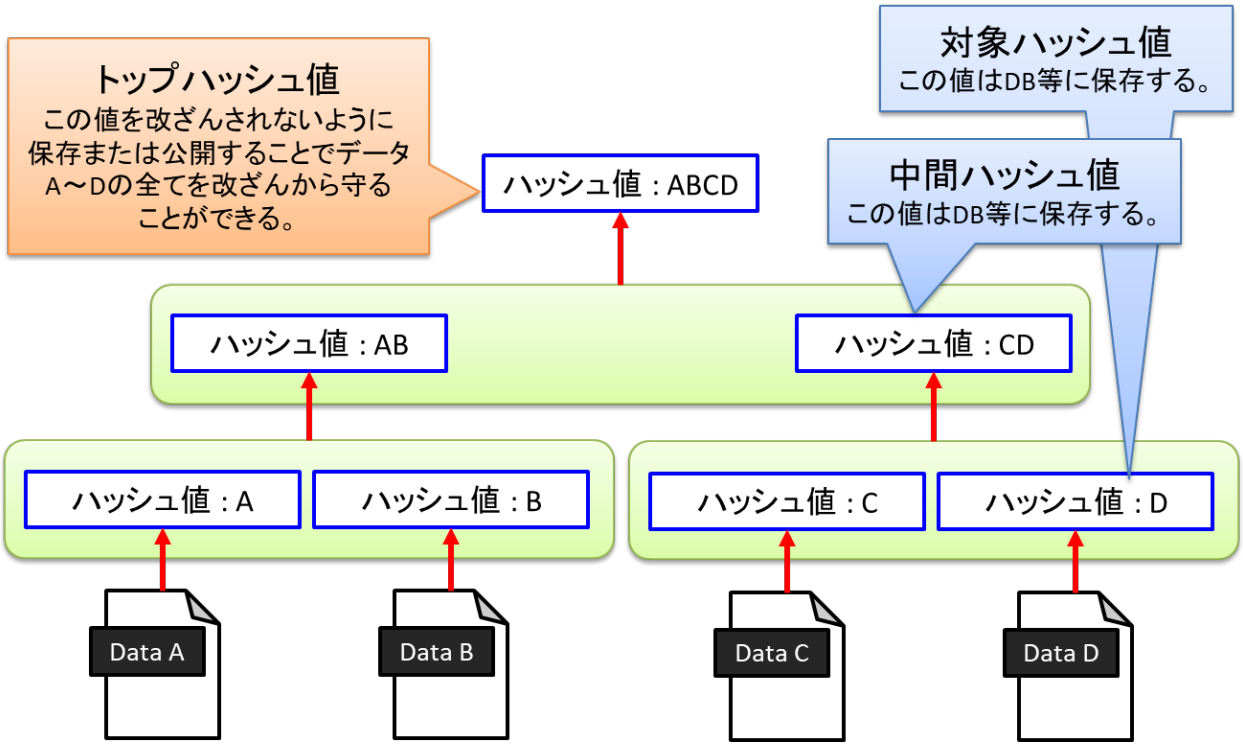

図 8　ハッシュ木の概念図（3 層の場合）

標準パッケージで利用している META-INF/Manifest ファイルもこのハッシュ木の構造（2 層）となっている。これによりデジタル署名やタイムスタンプを使って、複数のデータを一括して守ることができる。

6.1.5. ハッシュチェーン（ブロックチェーン）

ハッシュ値を含むデータのハッシュ値を計算することでチェーン状に連鎖することができる。1 つでもハッシュ値が変更されるとそれ以後全てに影響を与えるので改ざんが困難となる。また各ハ

ッシュ値によりデータの改ざん検知ができる。最後のハッシュ値（最終ハッシュ値）のみ改ざんされないように保管または公開しておく必要がある。

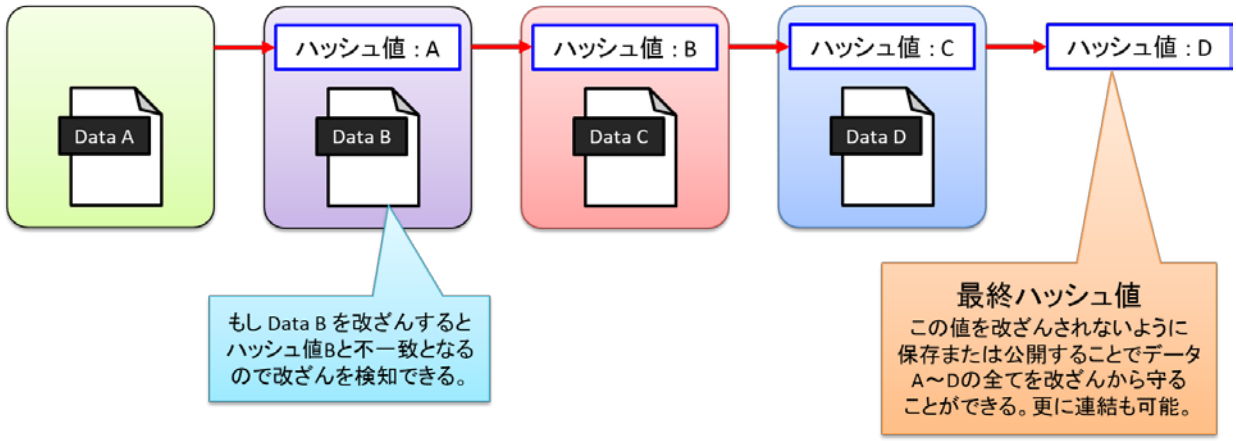

図 9　ハッシュチェーンの概念図

更にハッシュ値では無くデジタル署名による署名値にすることでブロックチェーンとすることも可能となる。ブロックチェーン化することで PKI とは異なる形での本人保証も可能ではあるが、現時点では外部に公開されない測定機器データへの適用は困難であり将来への課題であろう。

6.1.6. デジタル署名（改ざん防止）

ハッシュアルゴリズムと公開鍵暗号アルゴリズムによる署名鍵（秘密鍵とも呼ばれる）を使ったデジタル署名により署名値を計算して保存することで、改ざん防止を実現することができる。署名値を署名鍵とペアとなる公開鍵で検証することで改ざん検知（改ざん有無）できるので改ざん防止が実現できる。デジタル署名として利用可能な公開鍵暗号アルゴリズムとしては RSA 暗号方式が一般的だが、近年は ECC（楕円曲線）暗号方式も使われている。将来的に安全とされている鍵長として、RSA 暗号方式では 2048～4096bit 以上を、ECC 暗号方式では 224～320bit 以上が、推奨される。なお ECC 暗号方式には対応していないソフトウェアやハードウェアが多いので注意が必要である。

デジタル署名では、署名値と公開鍵（電子証明書の形の場合が多い）をまとめて保存する署名フォーマットが用意されている。詳しくは「6.4.3. 暗号技術利用（長期署名）」を参照。

6.2. 本人保証（本人性保証と否認防止）

本人保証では、自然人だけでは無く組織（法人や部署）やシステム保証も含めて「誰が」保証しているかを示す。電磁的記録の本人保証には一般的には電子署名が利用される。電子署名は、広義では「本人性」と「非改ざん性」の保証を意味する。これを実現する具体的な技術（狭義）として認証記録やデジタル署名がある。

電子署名の本人性について大事な概念として「本人確認」と「当人確認」がある。本人確認はシステムに利用者のアカウントを登録する際に確かにその本人であることを確認するものであり、本

人確認された利用者に認証クレデンシャルを提供する。利用者がシステムにアクセスする際や署名を付与する際にはシステムが利用者の認証クレデンシャルをその都度照合することで、本人確認済みの当人である事を確認する。

本人確認と当人確認の保証レベルに関しては、NIST（米国標準技術研究所）が「NIST SP 800-63-3：Digital Identity Guidelines」にて保証レベルを定義しているので参考にするべきである。本人確認は Identity Proofing や KYC とも呼ばれ、当人確認は Authentication となる。

表 21　本人性の確認

種類	説明
本人確認 （身元確認）	利用者が提示した属性情報の確かさを確認する。エンタープライズの場合には、自社の社員であることや協力会社の社員であることを確認する。本人確認の完了後に登録して認証クレデンシャル（認証なら ID とパスワード等の発行、署名なら証明書の発行と署名鍵の紐づけ）を発行する。 参考：SP 800-63-3A 本人確認保証レベル/IAL（Identity Assurance Level）
当人確認 （認証処理）	本人確認後に発行された認証クレデンシャルを利用して確認することで、本人確認された当人であることを確認する。 参考：SP 800-63-3B 当人認証保証レベル/AAL（Authenticator Assurance Level）

認証記録では認証クレデンシャルによる当人確認を行いその記録（操作ログ）を保存する。デジタル署名では秘密鍵の行使により当人確認を行い、結果として署名値を保存する。なおいずれの方法においても事前に本人確認が必要であることは共通している。

表 22　本人保証方式概要

方式	説明
6.2.1. 認証記録	事前に本人確認された利用者に対して認証クレデンシャルを提供しておき、利用時の当人確認に関する操作ログを記録することで本人確認する方式。
6.2.2. デジタル署名と PKI	事前に本人確認された利用者に対して証明書と署名鍵を割り当てておき、利用時に署名鍵によりデジタル署名することで本人確認する方式。同時に改ざん防止も実現できる。本人確認と証明書の発行による保証レベルは、PKI（公開鍵インフラ）の認証局（CA）のレベルに依存する。公的またはパブリックな認証局を利用することで第三者でも本人性を保証できる。

6.2.1. 認証記録（電子認証による当人確認）

電子認証は本人確認済みの当人がログイン（接続）していることを保証する技術である。電子認証ログと当人の操作ログを組み合わせて保存する操作記録（参照：6.1.1.）を利用することで、簡易な電子署名としての本人保証が可能となる。これに認可のステップを加えるとデータのアクセスコントロールまでが可能となる。電子認証はデジタル ID と呼ばれることもあり、NIST（米国標準技

術研究所）が発行した SP 800-63 シリーズが事実上のデファクト標準となっている。SP 800-63 シリーズは本人確認から当人確認さらにはサービス間の連携までが解説されている。

表 23　SP 800-63 シリーズの構成

番号	タイトルと概要	内容
SP 800-63-3	Digital Identity Guidelines 「デジタル ID ガイドライン」　全体の概要	電子認証の概要
SP 800-63A	Enrollment and Identity Proofing 「登録と身元情報の検証」　本人確認のガイドライン IAL（Identity Assurance Level）の定義	本人確認
SP 800-63B	Authentication and Lifecycle Management 「認証とライフサイクル管理」　当人確認のガイドライン AAL（Authenticator Assurance Level）の定義	認証 （当人確認）
SP 800-63C	Federation and Assertions 「連携とアサーション」　連携時の認証/認可/属性情報 FAL（Federation Assurance Level）の定義	連携

※ SP 800-63：NIST の米国政府機関向けデジタル ID 実装ガイドライン
https://pages.nist.gov/800-63-3/

※ 日本：行政手続におけるオンラインによる本人確認の手法に関するガイドライン
https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf

当人確認の詳細は、SP 800-63-3B にて AAL（当人認証保証レベル：Authenticator Assurance Level）と技術が解説されており参考になる。AAL のレベル 1 では単要素認証となり、レベル 2 以上では 2 要素認証が求められる。なお認証要素には「知識」「所有」「生体」の 3 種類があり、2 要素認証ではこのうちの 2 つの組み合わせを要求する。同じ要素である「知識」を 2 つ利用する場合には 2 段階認証と呼ばれ、2 要素認証とはならない。

表 24　認証要素の種類

認証要素名	内容
知識	当人しか知り得ない情報（PIN 番号・パスフレーズ 等）
所有	当人しか所有していない物に依存（IC カード・トークン 等）
生体	当人の生体としての情報（指紋・光彩・顔認識 等）

6.2.2. デジタル署名と PKI（公開鍵インフラ）

デジタル署名は公開鍵暗号アルゴリズムを利用した電子署名の 1 種である。デジタル署名に PKI（公開鍵基盤）を利用することで、高レベルの本人保証を行うことができる。デジタル署名では秘密鍵の管理が重要となる。最近ではリモート署名と呼ばれるサーバーに秘密鍵を預けて電子認証と併用して利用する形態も広まりつつある。

デジタル署名を本人（当事者）が自ら行う当事者署名と、デジタル署名を外部で運用された第三者システムが行う第三者署名の 2 種類に分けられる。第三者署名では本人性は署名をした第三者が保証する必要がある。

表 25　認証局の種類とレベル

認証局の種類	レベル	説明
公的認証局	最高	国（政府）の認定による認証局。日本では民間利用可能な認証局として、認定認証の認証局、商業登記認証局、公的個人認証局（マイナンバーカード）がある。取得までに手間がかかることが多い。
標準認証局 （パブリック認証局）	高い	世界的に標準化された認定を取得した認証局。WebTrust や欧州 ETSI 等の認定がある。本人確認のレベルによって信頼性の高さも異なるが一般的に高いレベルとなる。
プライベート認証局	中程度 （運用次第）	独自に運用する認証局。例えば会社内認証局として身元を確認した上で社員に証明書を発行するようなケース。可能であれば CP/CPS（6.5.2 参照）を作成すべき。運用次第ではある程度高い信頼性のレベルも実現可能となるが、運用には一定以上の知識やノウハウが必要となる。
自己署名 （オレオレ認証局）	最低	署名者証明書がルート証明書となり認証局とは呼べない。信頼性を保証する為には運用を厳密にする必要がある。デジタル署名ではあるので改ざん防止効果はある。

認証局と電子証明書および PKI に関しては、認証局会議が公開している「電子署名活用ガイド」が分かりやすく説明しており、参考になる。

※ 認証局会議「電子署名活用ガイド」
https://www.c-a-c.jp/download/guidebook.html

電子証明書は自然人に対して発行することも、法人や組織または役職に対して発行することもできる。自然人の証明書と秘密鍵を使って行ったデジタル署名は 3.1 項に示した規制で定義された電子署名の一部とみなされるが、法人等の証明書と秘密鍵を使って行ったデジタル署名は当該規制で定義される電子署名とはみなされない。両者を区別するために後者は電子シール（e シール）と呼

ばれる。この場合の電子署名と電子シールの違いは署名証明書を発行する対象だけであり、いずれも共通のデジタル署名技術を利用する。電子シールは欧州の eIDAS 規則では公的に認められており、日本においても民間レベルで利用することに問題は無い。ただし、GxP 規制に基づき個人が行う業務を記録する際に共有の認証を用いるとデータの帰属性が特定できなくなるため、製薬業界ではそのような場面で電子シールを利用することは推奨されない。これに対し、データをパッケージ化してもパッケージ内データの帰属性は維持されるため、標準パッケージに対しては共有の認証を用いた電子シールを使用することは許容されると考えられる。逆に個人を対象とする電子署名の場合には、本人の退職により将来的に利用が不可能になることが推測されるため、標準パッケージの長期保存の際に電子署名を用いる場合には注意深く運用する必要がある。

表 26　用途による分類

法的名称（用途）	電子署名	電子シール（e シール）
英語名称	eSignature (Electronic Signature)	eSeal (Electronic Seal)
署名者（証明書）	自然人	法人（組織・部署）
説明	署名者は自然人であり「本人性」を保証する（例：電子契約書）	署名者は法人等であり「発行元」を保証する（例：レシート）
デジタル署名形式	CAdES/XAdES/PAdES Digital Siganature Format 等 （ISO 14533-1/2/3 プロファイル） ※ 電子署名と電子シールの違いは署名証明書のみ	

デジタル署名には「電子証明書」と証明書に紐づいた「署名鍵」を利用するが、署名鍵をどこで保管するかによって「ローカル署名」と「リモート署名」に分けられる。

ローカル署名は署名鍵を署名者自体が保持する方法であり、例としては IC カードを使うケースがある。この場合には署名者は署名時に IC カードに格納された署名鍵でデジタル署名を行う。

リモート署名はリモート（サーバーやクラウド）上に預けた署名鍵を利用してデジタル署名を行う方式であり、電子認証により署名者に署名鍵の利用を認可する。リモート署名に関しては JT2A（日本トラストテクノロジー協議会 http://www.jt2a.org/）がガイドラインを出しているので参考になる。

※ JT2A/日本トラストテクノロジー協議会「リモート署名ガイドライン」
https://www.jnsa.org/result/jt2a/2020/index.html

6.3. 時刻保証（存在証明）

実世界での時刻保証に比較するとデジタル世界での時刻保証は比較的容易に実現できる。ただし時刻保証にもレベルがあり、最も簡単な時刻保証はデータファイルの作成日時情報となるが、これは改ざんも容易である。これに対して第三者が時刻保証をする仕組みとして PKI ベースのタイムス

タンプ（RFC 3161）がある。しかし PKI ベースのタイムスタンプには運用コストが必要となる。

表 27　時刻保証方式概要

方式	説明
6.3.1. システム時刻	データの操作を行うシステムまたは端末 PC が持つ時刻情報をそのまま利用する。運用ポリシーを決めておき利用者が時刻を変更できないか変更が検知できるようにしたり、時刻同期をしたりしておくとより信頼性が高まる。
6.3.2. タイムスタンプ（PKI ベース）	データのハッシュ値に対して第三者であるタイムスタンプ局が内容と時刻を保証するデータ（タイムスタンプトークン）を発行する仕組み。利用者が時刻を変更することが出来ない為に高い信頼性を実現できる。タイムスタンプ局の保証には PKI を用いるが、パブリック認証局の方がプライベート認証局やオレオレ認証局よりも信頼性が高い。外部ではなく自前でタイムスタンプ局（タイムスタンプサーバー）を運用することもできる。

6.3.1. システム時刻

パッケージ化を行うサーバーシステムまたは端末 PC の時刻をそのまま利用することも出来る。端末 PC の時刻よりもサーバーシステムの時刻の方が信頼度は高い。NTP（Network Time Protocol）利用等によるシステム時刻の外部時刻との同期が運用ポリシーで保証されている場合には、より高い信頼性があると考えても良い。時刻情報にはタイムゾーンを含む形式を利用すべきである。

※ NICT による日本標準時に直結した時刻サーバーの情報（NTP 利用）
https://jjy.nict.go.jp/tsp/PubNtp/index.html

6.3.2. タイムスタンプ（PKI ベース）

デジタル署名技術を使い、内容保証と同時に署名時刻を第三者（タイムスタンプ事業者）が行うサービス（RFC 3161）。自前でタイムスタンプサーバーの運用も可能であるが真正性の保証レベルは下がる。信頼した外部の第三者による保証を受けられる点で高い信頼性が得られる。「6.4.3. 暗号技術利用（長期保証）」ではタイムスタンプの利用は必須となる。

現在日本においては時刻認証業務（電子データに係る情報にタイムスタンプを付与する役務を提供する業務）について、総務大臣による認定制度が制定された（令和 3 年 4 月 1 日から指定の申請を受付け）。これまでは日本データ通信協会のタイムビジネス認定センターにより、認定タイムスタンプサービスが公開されていた。これらの認定タイムスタンプサービスのほとんどは利用において有償となる為に運用コストが必要となる。

※ タイムスタンプについて（総務大臣による認定制度）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

※ タイムビジネス認定センター 認定事業者一覧
https://www.dekyo.or.jp/tb/contents/list/index.html

※ FreeTSA：OpenSSL を使ったオープンソースのタイムスタンプサーバー（試験利用可能）
http://eswg.jnsa.org/sandbox/freetsa/

6.4. 長期保証

長期間の保存には電磁的記録媒体に移して管理する方法と、運用システムを長期間利用する方法がある。運用システムを長期間利用する場合には次章「運用保証」を参照する。ここでは電磁的記録媒体に保存する場合について説明する。長期署名等の技術により長期保証する場合は真正性の保証を行う情報もデータと一緒に保存することが望ましい。なお真正性保証の技術の多くには暗号アルゴリズムが使われている。これを 10 年以上の長期保存に利用する場合には暗号アルゴリズムの寿命（危殆化）や有効期限の問題がある。

なお認証記録を利用している場合には、運用するシステムの監査ログと共に保存する必要がある。監査ログに関しては 6.5.2 章で説明する。

表 28　長期保証方式概要

方式	説明
6.4.1 データ保管サーバー運用	データ保管サーバーのシステム運用を長期間続けて行く方法。運用中に不正なアクセス等が無いことを操作記録（参照　：6.1.1）等で別途保証する必要がある。
6.4.2. 電磁的記録媒体	後から変更が出来ない電磁的記録媒体（例：光メディアやテープ）にデータを保存することで長期保管に対応する。電磁的記録媒体を管理することで保証する。電磁的記録媒体には寿命があるので適切な媒体を選択する。
6.4.3. 暗号技術利用	デジタル署名等の暗号技術によりデータを保存することで長期保管に対応する。デジタル署名には長期間の保管を前提とした長期署名がある。暗号技術は時間が経つと危殆化する可能性が高くなる為に寿命と有効期限がある。長期署名は有効期限を延長する技術となる。 長期署名フォーマットとして XML ベースの XAdES や PDF ベースの PAdES 等が標準化されており高い信頼性を実現できる。

6.4.1. データ保管サーバー運用

データ保管サーバーのシステム運用を続けて行くことで長期保管を実現する。運用中に不正なアクセスが無かったことを保証する為にはログを保管しておく必要がある（参照：6.1.1.）。また運用の監査も受ける必要がある（参照：6.5.3.）。ファイル保管の外部サービスやシステムを利用するこ

とも可能だが、ネットワーク障害、サービスの終了、仕様変更に伴うトラブルなどが生じる可能性もあるので事業継続性に関しても確認して検討する必要がある。

運用ポリシーを策定してきちんと運用を続けるのであれば、システム維持以上のコストはかからない利点がある。

6.4.2. 電磁的記録媒体

データの長期保存にはシステムの運用を続けて行く以外に、外部の電磁的記録媒体にバックアップして保存する方法がある。この時の電磁的記録媒体として書き込み後に変更や削除ができない媒体を選択することで、長期保証することが可能となる。

電磁的記録媒体に長期保存した場合には、時間の経過とともに見読性が損なわれる危険性や、陳腐化して媒体の読み取り装置がなくなる危険性がある。そのため、以下の検討が必要である。

- 複数の媒体への保存を検討すること。
  - 複数の媒体に保存していれば、片方が読み取れなくなっても、残りの媒体が読み取れる可能性もある。
  - この場合、どれが正本であるかを特定する必要がある。
- 定期的（毎年など）に見読性が損なわれていないことを確認すること。
  - 正本か副本のいずれかで見読性が損なわれていたら、見読性が担保されていた媒体を複製し、再度、どちらが正本かを定義し直す必要がある。
- 定期的（5 年毎など）に新たな媒体にデータを複製すること。
  - 媒体の陳腐化を避けるために、必要に応じて、新しい種類の媒体を用いることを検討する必要がある。

6.4.3. 暗号技術利用（長期署名）

暗号アルゴリズムには寿命がある。暗号化されたデータの解読や改ざんが可能になった時が寿命と言える。理由としては「新しい攻撃方法が見つかった場合」と「コンピュータの性能が上がった場合」がある。この場合には「新しい暗号アルゴリズムに移行する」か「暗号の強度（ビット数）を上げる」必要がある。

真正性を保証する為の情報は、対象である測定データと紐づけて保存する必要がある。情報と紐づけた保存に良く用いられるデジタル署名のフォーマットとしては XML・PDF・JSON・ASN.1/DER 等がある。それぞれ一長一短があるが、以下の理由から本技術ガイドブックでは XML と PDF を中心に説明する。ASN.1/DER はタイムスタンプ等の暗号系で使われているフォーマットであり、一般的な保存フォーマットでは無い。XML と JSON はほぼ同じことが実現できるが JSON のデジタル署名の標準化はまだ発展途上である。

表 29　デジタル署名のフォーマット

フォーマット	説明
XML	テキスト形式のタグと属性を利用してデータを指定する。古くから使われておりテキスト形式であるので内容の確認が容易である利点がある。 ※ 標準パッケージにも XML を利用。
PDF	印刷イメージをそのままファイルに出来るので視認性が高い。バイナリ形式であるので内容を操作する為のソフトウェアが限定されるが、無償利用可能なビューアが色々なベンダーから提供されている。 電子封筒としての機能（添付ファイル）もあり、複数のデータファイルを 1 つの PDF ファイルに添付してまとめることもできる。添付ファイル付きの PDF ファイルにデジタル署名を付与すると添付ファイル全ても含めて守ることができる。
JSON	テキスト形式の階層構造でデータを指定する。XML よりもシンプルに記述ができ、最近クラウドシステム等で使われている。利点は XML と共通である。新しいフォーマットである為にデジタル署名（JWS）の仕様ではドキュメント用途としては不足がある。
ASN.1/DER	暗号系データで良く使われるバイナリ形式のフォーマット。X.509 の電子証明書や RFC 3161 のタイムスタンプトークン等で利用される。一般のデータに利用することはほとんどない。

ここでは暗号技術を利用したデジタル署名等の保存フォーマットに関して説明する。暗号技術を利用したデジタル署名のフォーマットとしては XML の XAdES と PDF の PAdES とタイムスタンプが使われている。

表 30　暗号技術を利用したデジタル署名等の保存フォーマット

名称	説明
XAdES デジタル署名	XML 形式の XML 署名をベースとする。 複数対象データを 1 つの XAdES ファイルで署名できる。 タイムスタンプの付与も可能な長期署名フォーマットである。 タイムスタンプのみの付与はできない。 仕様：ETSI EN 319 132 / ISO 14533-2
PAdES デジタル署名	PDF 形式に埋め込む PDF 署名をベースとする。 PDF 文書 1 つにつき 1 つの署名が必要となる。 タイムスタンプの付与も可能な長期署名フォーマットである。 タイムスタンプのみの付与も可能。 仕様：ISO 32000-2 / ISO 14533-3
タイムスタンプ	バイナリベース（ASN.1/DER 形式）のデジタル署名の 1 種。 署名者は常にタイムスタンプ局となる。

	1 つのハッシュ値に対して 1 つのタイムスタンプとなる 単独利用も可能だが、XAdES/PAdES と組み合わせて使われることが多い。 仕様：RFC 3161

XAdES と PAdES は長期署名と呼ばれている。これは暗号技術の寿命や有効期限がある事を前提として、有効期間を延長する仕組みを提供する。10 年以上の長期保存を行う場合には長期署名フォーマットを利用すべきである。

表 31　長期署名プロファイル（XAdES の場合）

仕様	内容	説明
XAdES-BES	デジタル署名のみ	XML 署名とほぼ同じだが、XML 署名は長期署名化できないのでデジタル署名のみであっても XML 署名では無く XAdES-BES の利用が望ましい。改ざん検知と本人保証が行われる。
XAdES-T	デジタル署名＋タイムスタンプ	XAdES-BES に加えて署名時刻を保証。
(XAdES-X Long)	XAdES-T の検証情報の埋め込み	XAdES-T の検証に必要となる情報を全て取得して埋め込むことで、オフラインでも検証が可能となる。
XAdES-A	XAdES-X Long に全体を守るタイムスタンプを加えたもの	加えられたタイムスタンプの有効期限までデジタル署名の有効期限を延長することができる。

※　PAdES の場合もほぼ同じ長期署名プロファイルとなる。

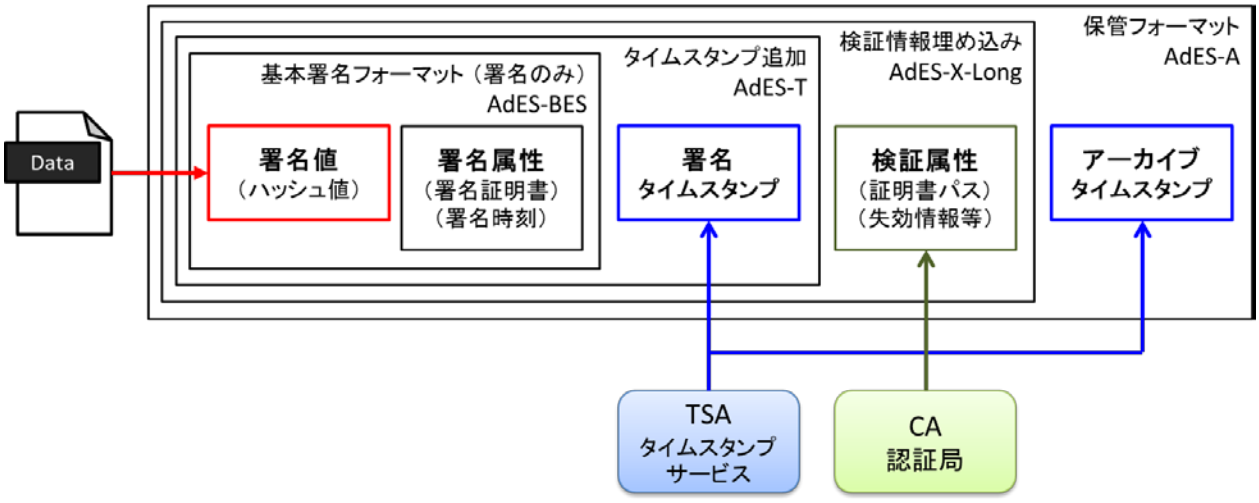

図 10　長期署名フォーマットの構造

長期署名はデジタル署名（証明書）の有効期限を延長する仕組みではあるが、利用している暗号アルゴリズムが危殆化していない状況であれば、証明書の有効期限が切れていても直ちに内容が保証されないと言うことにはならない。10～20 年を見据えた暗号アルゴリズムを採用することにより長期署名の延長をしないと言う選択肢もある。例えばハッシュアルゴリズムの SHA-2 の場合であれば、ハッシュ長を最大の 512bits を選択しておき、SHA-2 が危殆化した時のみ長期署名の延長処理を行うような運用をすることもできる。

6.5. 運用保証

真正性を保証する為には適切な運用が必要となる。システムによる運用を行う場合には、クローズド・システムかオープン・システムかによって必要となる保証が異なる。

クローズド・システムとは、システム上の電磁的記録の内容に責任を持つ者によって完全にアクセスが管理されている環境を意味する。これが可能な社内 LAN 上に構築されたシステムは、この前提に立ち真正性の保証に関する要件を設計する。一般的には運用コストは高額になりがちだが、真正性の保証には有利と言える。

オープン・システムとは、システム上の電磁的記録の内容に責任を持つものによってシステムへのアクセス管理が全てに及ばない状況がある環境を意味する。不特定多数のシステムを経由するインターネットを利用するシステムは、クローズド・システムと同じ真正性保証の要件に加えて、利用経路や利用手順においても真正性の保証を可能とする必要がある。例えば Web サービスの通信経路においては TLS による経路暗号化の利用が望ましい。また電磁的記録へのアクセスの制御管理をクローズド・システムよりも厳密に行うことが望ましい。クラウドサービスは、オープン・システムと見なされる。クラウドサービスを用いる場合には、予めサービスプロバイダーを品質マネジメントシステム、情報セキュリティ・事業継続性、提供されるサービスなどの観点で評価し、利用目的に合ったサービスを選定することが推奨される。

表 32　運用保証方式概要

方式	説明
6.5.1. 監査証跡（監査ログ保存）	検証時に利用者の操作（イベント）を確認する為のログを用意することで運用保証を行う。
6.5.2. 運用ポリシー（運用方針）	事前に指針となる運用ポリシーを策定し、その上で操作手順を整備する。運用時にポリシーと操作手順を順守することで運用保証を行う。監査ログの内容等も決めておく。
6.5.3. 運用の監査	運用ポリシーに従って整備された操作手順のもとで正しく運用されているか逸脱が無いか監査を受けることで運用保証のレベルを更に上げる。

6.5.1. 監査証跡（監査ログ保存）

システムを運用している場合には各種ログが発生するが、どのようなログを監査証跡として記録

するかをシステム導入時に検討しておく必要がある。ER/ES 指針や GLP 運用通知では、電磁的記録に対する監査証跡は、記録、変更の都度、「いつ、誰が、何を、理由(必要に応じて)、変更前の記録、変更後の記録」を記録することが求められる。GCP ガイダンスでは、入力済みのデータを消去することなしに修正でき、そのデータ修正の記録をデータの入力者及び修正者が識別されるログとして残せるようにデザインされていることを保証することが要求される。

監査証跡が削除や改ざんされないように真正性を保証した措置を行う必要がある。ここで、測定機器データの長期保存ガイダンスでは、利用目的に応じて標準パッケージに含めることが推奨される監査証跡は異なる。要求レベルの最も高い GxP 規制に準拠する業務に利用する場合であっても、システムに関する監査証跡を標準パッケージに含める必要はない。

監査証跡に関する要求事項については以下が含まれる。

- 監査証跡機能が、システムの導入時又は変更時に検証されていること。
- データに利害関係を持つ者（作成者、承認者など）が監査証跡に関する設定変更に関与できないこと。
- 監査証跡の設定管理を適切に行うこと。これには以下が含まれるが、この限りではない。
  - 手順に基づく監査証跡の設定管理
  - 監査証跡の停止の防止（ベンダーが業者点検時にやむを得ず監査証跡を停止する場合には、業者点検の後に確実に監査証跡を有効にされたことを確認する）
- システム時計の正確性とセキュリティを確保すること（6.3 項参照）。
- 監査証跡がレビューされること。これには以下の 3 種類が含まれる。
  - 日常業務におけるデータレビューの一環として、監査証跡が適切に記録されていることをレビューする。
  - 監査証跡が有効かつ効果的に利用されていることを確認するためにレビューする。これには定期的な監査証跡のレビューが含まれる。
  - 問題が明確になった際に、その原因の追究のために監査証跡をレビューする。

6.5.2. 運用ポリシー・手順（運用方針）

システム運用において管理者と利用者の各操作において、あらかじめ脅威を想定した上で運用ポリシーを作成する必要がある。特にセキュリティポリシーは真正性の保証の根幹となる部分である為に、可能であれば制改訂時のセキュリティ専門家の関与が望ましい。運用ポリシーに従い操作手順書を整備した上で運用を行う。例えば、システムの運用に際しては、以下のようなポリシーや手順書の整備が想定されるが、この限りではない。

- ポリシー：セキュリティポリシー、コンピュータ化システムバリデーション（CSV）ポリシー
- 手順書：セキュリティ対策のための手順（これには、利用者のアカウントの登録・変更・無効化の手順が含まれる）、CSV 実施や電子記録・電子署名の管理に関わる手順書（監査証跡の取り扱いに関する手順も含まれる）
- マニュアル：個別システムの利用や管理に関する手順書

認定を必要とする公的 PKI の電子認証局では CP（証明書ポリシー）と CPS（認証局運用規定）

を公開して順守を約束している。CP/CPS のフレームワークとして RFC 2527（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework）が利用可能である。独自のプライベート認証局を運用する場合にも参考にして運用ポリシーを定めることが望ましい。

6.5.3. 運用の監査

事前に設定された運用ポリシーのもとで策定済みの操作手順に従って運用が行われているかを、管理者以外の監査者から定期的または不定期に運用監査を受けることで信頼性のレベルを上げることができる。運用ポリシーと操作手順にて決められた監査証跡（監査ログ保存）が必要となる。監査は外部（社外）の専門会社に依頼すると信頼性を高くできるが、社内であっても直接運用に関係しない運用者・利用者以外（例えば、監査部門）が関与し、その独立性を維持できれば、十分な信頼性が確保できる。

7. 用語集

表 33 に，本技術ガイドブックで使用している用語の説明を示す。

表 33　用語の説明

用語	説明
電磁的記録 Electronic Record	法的な定義では、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、とされている。一般には電子データを指す。
電子署名 Electronic Signature	法的な（広義の）意味においては、電磁的記録（データ）に付与する電子的な徴証（証拠）。狭義ではデジタル署名を指す場合もある。
デジタル署名 Digital Signature	公開鍵暗号とハッシュ関数を使った電子署名の一種であり非改ざん性と否認補防止を可能とする技術。PKI（公開鍵基盤）を利用することで本人性の保証も可能となる。 参照：6.1.6. デジタル署名（改ざん防止）
データ保管サーバー	サーバー上にデータ（ファイル）を保管（保存）するシステム。ファイル・サーバーのようにアクセスコントロールされていないシステムも含む。電子文書管理システムも含まれる。
電子文書管理システム	電子文書（データ）を保存、管理するシステムであり、アクセスコントロールも行われる。近年では、21 CFR Part 11 や厚労省 ER/ES 指針を準拠する電子文書管理システムが開発されたことにより製薬業界で利用が推進されている、
認証記録	電子認証の結果を記録することで実現し、簡易な電子署名として利用できる。例えば ID とパスワードによる認証結果のログを保存（記録）することで実現する。 参照：6.2.1. 認証記録（電子認証による当人確認）
ハッシュ値（ダイジェスト値） Hash Value（Digest Value）	メッセージダイジェスト値と呼ぶ場合もあるが本書中ではハッシュ値に統一している。 参照：6.1.3. ハッシュ値（改ざん検知）
ハッシュ木（マークル木） Hash Tree（Merkle Tree）	複数のハッシュ値をトーナメント式に組み合わせることで、トップハッシュ値だけで全ての対象データを守る仕組み。 参照：6.1.4. ハッシュ木（複数対象の改ざん検知）
ハッシュチェーン Hash Chain	複数のハッシュ値を連結的に繰り返し組み合わせることで、全ての対象データを守る仕組み。ハッシュ値にデジタル署名を組み合わせることでブロックチェーンとなる。 参照：6.1.5. ハッシュチェーン（ブロックチェーン）
ブロックチェーン Block Chain	デジタル署名等の暗号技術によりブロックと呼ばれるレコード（情報）を連結的に繰り返し結合することで、内容を保証する。複数のシステム間でブロックを分散管理することで耐改ざん性と透明性を実現できる。一方で単独利用しても手間に比較して十分なメリットが得にくい。仮想通貨等で利用されている。 参照：6.1.5. ハッシュチェーン（ブロックチェーン）

用語	説明
Base64	バイナリ形式のデータを 64 種類の印字可能な英数字のみを用いてエンコードする為の仕様。16 進数の 16 種類の英数字を使う Base16（Hex）形式よりもサイズを小さくできる利点があり、ネットワークや XML 等でよく用いられる。
本人確認 Identity Proof	本人が持つ属性情報の確かさを確認（身元確認）すること。KYC（Know Your Customer）と呼ばれる場合もある。認証要素 (パスワード) や電子証明書を発行する前には必ず本人確認を行う。本人確認には、メール到達性・運転免許書・マイナンバーカード等の ID カードを利用することが多い。 仕様：SP 800-63A 参照：6.2. 本人保証（本人性保証と否認防止）
認証（電子認証） Authentication / AuthN	当人確認として、端末の前にいる実体（人）がサービス側の認識するどの ID（Identity）と紐付いているかの確証を得ること。利用者の識別を行う為に利用する。 仕様：SP 800-63B 参照：6.2.1. 認証記録（電子認証による当人確認）
認可 Authoraization / AuthZ	当人確認された端末の前にいる実体（人）の ID（Identity）が、サービス側の提供するリソースにアクセスをする権限を持っているか確認すること。
アクセス制御 Access Control	データへのアクセスを制御（コントロール）する仕組みであり、認証＋認可＋記録の組み合わせで実現される。 参照：6.1.1. 操作記録（改ざん検知）
公開鍵インフラ（PKI） Public Key Infrastructure	公開鍵基盤とも呼ばれる。公開鍵とその所有者との関係を保証する為の仕組み。認証局がルート証明書や中間 CA 証明書を公開し電子証明書を発行することで構築される。 参照：6.2.2. デジタル署名と PKI（公開鍵インフラ）
認証局（CA） Certification Authority	電子証明書（Certification）を発行する機関。登録・発行・失効を行う。公開されたパブリック認証局と、独自に運用するプライベート認証局がある。他にも様々なレベルの認証局があり、目的とコストに合った認証局を利用する。 参照：6.2.2. デジタル署名と PKI（公開鍵インフラ）
時刻認証局（TSA） Time Stamping Authority	タイムスタンプを発行する機関。一般的には RFC 3161 方式のタイムスタンプ発行を行う。日本では認定されたタイムスタンプサービスがあるが、信頼性は低くなるが自前で運用することも可能。 参照：6.3.2. タイムスタンプ（PKI ベース）
信頼性保証（QA）	GxP 実施施設において施設およびデータの監査を行い、適切に試験が実施されていることを保証する活動
脆弱性 Vulnerability	1 つ以上の脅威によって付け込まれる可能性のある、資産または管理策の弱点のこと。
危殆化 Compromise	主に暗号アルゴリズムに脆弱性が見つかり破られること。危殆化した暗号アルゴリズムは使ってはいけない。
相互運用性 Interoperability	さまざまなシステム間に互換性があり連携できること。標準化された仕様を元に相互に運用（利用）することができる。
陳腐化 Obsolescence	商品や技術について、目新しさがなくなったり時代遅れの印象がついたりして価値が減ること。例えば、以前はフロッピーディスクが用いられていたが、現在は販売されておらず、読み取り装置もないため、利用されなくなった。

用語	説明
ハッシュ関数（アルゴリズム） Hash Function Hash Algorithm	入力されたデータに一定の手順で計算を行い、決められた固定長の出力データを得る関数のこと。ハッシュアルゴリズムとも呼ばれる。
SHA-2（ハッシュアルゴリズム） Secure Hash Algorithm 2	米国（NSA/NIST）が採用した標準ハッシュ方式。ハッシュ長は 512bits だが、224bits/256bits/384bits に短くした形式もあり、SHA-224, SHA-256, SHA-384 や AES-512 と呼ばれる場合もある。2020 年現在での利用が推奨されている。更に SHA-3 も標準化されているが SHA-2 で現状十分な安全性があり普及はしていない。
SHA-1（ハッシュアルゴリズム） Secure Hash Algorithm 1	米国（NSA/NIST）が SHA-2 の前に採用していた標準ハッシュ方式。ハッシュ長が 160bits と SHA-2 より短く、一部では破られるケースも出ている為に 2020 年現在での利用が非推奨となっている。ただしまだまだあちこちで利用され続けている。
MD5（ハッシュアルゴリズム） Message Digest 5	SHA-1 の前に業界標準として使われていたハッシュ方式。ハッシュ長は 128bits と短く、既に偽装方法が見つかっている為に利用してはいけないとされている。
共通鍵暗号（暗号化） Common-key Cryptography	暗号化と複合において同じ鍵を使う暗号方式で、対象鍵暗号（Symmetric-key Cryptography）とも呼ばれる。現在は AES 方式がよく使われている。 参照：6.1.2. 暗号化（機密性）
AES（共通鍵暗号） Advanced Encryption Standard	米国（NSA/NIST）が採用した標準暗号方式。鍵長が 128bits と 256bits の 2 種類があり、AES-128 や AES-256 と呼ばれる場合もある。2020 年現在での利用が推奨されている。
DES（共通鍵暗号） Data Encryption Standard	米国（NSA/NIST）が AES の前に採用していた標準暗号方式。鍵長が 56bits と短い為に 2020 年現在での利用が非推奨となっている。DES 暗号化を 3 回行うトリプル DES がまだ一部では使われている。
公開鍵暗号（暗号化/署名） Public-key Cryptography	暗号化と復号または署名と検証において異なる鍵を使う暗号方式。署名においては署名鍵（秘密鍵とも呼ばれる）と公開鍵の 2 つがペアとして利用され、署名鍵は署名に利用され、公開鍵は検証に利用する。 参照：6.1.6. デジタル署名（改ざん防止）
RSA（公開鍵暗号）	現在一般的に利用されている公開鍵暗号の方式。特許の期限は切れているので自由に利用することができる。鍵長は現在では最低でも 2048bit が、推奨としては 4096bit となっている。
ECC（公開鍵暗号） Elliptic Curve Cryptography	楕円曲線暗号と呼ばれ RSA 方式に比較して鍵長が短くすむ利点があり一部では使われはじめている。鍵長は現在では最低でも 224bit が、推奨としては 256bit となっている。
署名方式 Signature Method	公開鍵暗号アルゴリズムとハッシュアルゴリズムの組み合わせを署名方式と呼ぶ。例としては RSA-SHA256 等がある。
電子証明書 Digital Certificate	より正確にはデジタル証明書だが一般には電子証明書と呼ばれる。公開鍵とその所有者の情報を発行者である認証局が保証するために発行するデータ形式。 仕様：X.509（RFC 2459）

用語	説明
TLS（SSL） Transport Layer Security	TLS と SSL（Secure Sockets Layer）はインターネットの HTTP 通信を暗号化して、HTTPS 通信とする為の暗号化プロトコル。SSL の方が古く、SSL 全てと TLS1.0/1.1 は現在利用が推奨されない。TLS1.2 以降の利用が推奨されている。
XML 署名 XML Digital Signature	XML（eXtensible Markup Language）デジタル署名形式 テキスト形式で可読性に優れている。 仕様：W3C 勧告
PDF 署名 PDF Digital Signature	PDF（Portable Document Format）デジタル署名形式 バイナリ形式で各種リーダーが普及しており見読性に優れている。 仕様：ISO 32000
CMS 署名 CMS Digital Signature	CMD（Cryptographic Message Syntax）デジタル署名形式 バイナリ（ASN.1/DER）形式でコンパクトな形式。 仕様：RFC 5652
長期署名 Long-term Signature	電子証明書の有効期限切れや暗号方式の危殆化にも対応できるデジタル署名の方式。長期間の保管に向いている。タイムスタンプを利用する。 参照：6.4.3. 暗号技術利用（長期署名）
XAdES（XML 長期署名） XAdES Digital Signature	XML 署名を長期署名化した仕様。 仕様：ETSI EN 319 132-2 / ISO 14533-2
PAdES（PDF 長期署名） PAdES Digital Signature	PDF 署名を長期署名化した仕様。 仕様：ISO 32000-2 / ISO 14533-3
CAdES（CMS 長期署名） CAdES Digital Signature	CMS 署名（ASN.1/BER/DER 形式）を長期署名化した仕様。 仕様：ETSI EN 319 122-2 / ISO 14533-1
eIDAS 規則 Electronic Identification and Trust Services Regulation	2014 年 7 月に成立し、2016 年 7 月に発効した EU 圏内市場における電子商取引のための法的枠組みと電子識別（eID）およびトラストサービス（電子署名やタイムスタンプ・電子シール等）に関する規則。EU 加盟各国間にまたがる電子商取引では遵守する必要がある。
URI Uniform Resource Identifier	ファイルの場所を示す為の仕様。システム上のファイルパスや Web 上の場所を示す URL（Uniform Resource Locator）が含まれる。

8. 改訂履歴

日付	版番号	改訂内容
2021.05.19	1.0	初版発行

Ｒ＆Ｄデータ保存委員会　技術ガイドブック作成メンバー（敬称略）

朝烏　章	あすか製薬（株）
泉　浩二	リコージャパン（株）
上原　小百合	アステラス製薬（株）
大野　治恵	旭化成ファーマ（株）
小川　泰弘	（株）LSI メディエンス
荻本　浩三	（株）島津アクセス
木村　道弘	(公社)日本文書情報マネジメント協会
芝　　清隆	（株）大塚製薬工場
鈴木　美代	生化学工業（株）
武田　幸雄	Ｒ＆Ｄデータ保存委員会
平石　嘉昭	テルモ（株）
平城　里香	日本ウォーターズ（株）
三浦 淳平	ビジネスエンジニアリング（株）
宮地　直人	（有）ラング・エッジ
守野　智	エーザイ（株）
山崎　晃	協和キリン（株）
山田　宜昭	（株）日立ハイテクサイエンス