ＩＳＯ／ＩＥＣ　１５４０８
情報技術セキュリティ評価基準
対応

原本性保証電子保存システム
（ソフトウェア部）
Protection Profile

平成 13 年 3 月

財団法人ニューメディア開発協会

目次

1. イントロダクション (Introduction)

1.1 Protection Profile 識別 (PP Identification)

識別子： <To be filled in upon registration>

書名：原本性保証電子保存システム　Protection Profile

版数：Ver 2.0

保証レベル：EAL 4

作成日：2001 年 3 月

登録日： <To be filled in upon registration>

作者：財団法人ニューメディア開発協会

PP 評価ステータス： <To be filled in upon registration (Part 2 conformant, Part 3 conformant)>

この ProtectionProfile(以下、PP と記す)は、Common Criteria Version 2.1 及び、ISO/IEC 15408 に従って記述している。

1.2 Protection Profile 概要 (PP Overview)

本 PP の目的は、原本性保証電子保存システムのソフトウェア上最低限対策を施さなければならないセキュリティの問題を示し、その問題を解決するための最小限のセキュリティ要件を示すことである。ただし、原本性保証電子保存に特化するために、一般的な情報システムのセキュリティ対策は施されていることを前提とし、また物理的不正に関しては本 PP では考慮しないこととする。

2 TOE の特定 (TOE Description)

2.1 TOE 利用目的 (Purpose)

高度に情報化されたデジタル経済社会を実現するためには、従来の紙による文書・情報の作成・利用・管理から、電子化されたそれへと転換する必要があり、同時に、これらの文書・情報をオンラインでやりとりすることが不可欠であるが、電子化あるいはネットワークの急速な普及に伴う課題への対応が求められているのが現状である。

電子情報のもつ特性として、①改竄が容易でありかつ痕跡が残りにくい、②記録媒体等の劣化による情報の消失などが起きやすいことが挙げられ、電子情報の安全な利用に不安を抱くものも少なくない。これらのことから、一般的に各種の文書を電子的に作成もしくは取得した場合であっても、原本として取り扱われ、保存・管理される文書等は、依然として紙媒体によるものであることが多いと考えられる。この課題に対応し、紙文書と同等の安全性を保ちながら、電子文書を活用していくための対策を講じる必要があると考えられている。

電子文書を活用するにあたって、まずは電子文書を安全に保管する必要があるが、電子文書の保管にあたっては、これを原本として保管するための機能を満足する原本性保証電子保存システムが不可欠である。

2.2 TOE 機能 (TOE Functions)

以下に TOE の主な IT 機能を記す。

a) 原本性保証電子保存機能

原本性保証電子保存機能とは、電子的データを長期間安全に原本として保存する機能である。

b) 電子原本参照機能

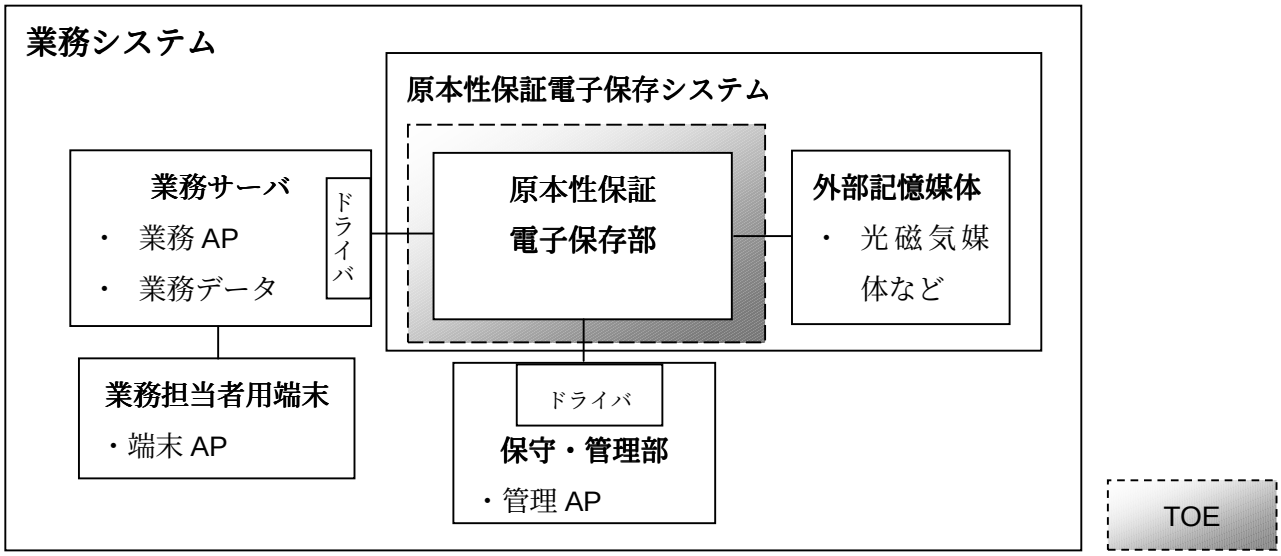
電子原本参照機能とは、原本性保証電子保存システム内に保存されている原本データを、保存した時点のものをそのままの形で取得・表示する機能である。

c) 電子原本廃棄機能

電子原本廃棄機能は、原本性保証電子保存システム内に保存されている原本データを、廃棄(消去)する機能である。

2.3 TOE 構成 (Definition of TOE)

TOE の構成要素を以下に示す。



3 TOE セキュリティ要求条件 (TOE Security Environment)

3.1 前提条件 (Assumptions)

3.1.1 利用環境の前提条件

A.No_Unauthorized_Person

TOE は関係者のみアクセスできるような環境に設置してあるものとし、第三者からの不正なアクセスから守られているものとする。

A.Obey_Policy

TOE 関係者は、セキュリティポリシー／ルールを正確に理解し、重要性を認識し、忠実に遵守しているものとする。

A.Single_Purpose

TOE は原本性保証電子保存にのみ利用するものとし、他の目的で TOE の機能を利用することはないものとする。

3.1.2 物理管理の前提条件

本 PP においては、物理的不正は考慮しない方針であるので、物理管理に関しての前提条件は特に設けない。

3.1.3 人的前提条件

この TOE に関わる人的リソースとして、本 PP では以下を想定する。

識別子	名前
TOE 関係者	
A.Person_Admin	TOE 運用管理者
A.Person_Audit	TOE 運用監査者
A.Person_User	TOE 利用者

(1) TOE 関連者

A.Person_Admin TOE **運用管理者**

役割： TOE を正常に稼動させることに責任を持つ。そのために必要となる TOE の設定・管理を行う。
権限： TOE の設定・管理を行う権限がある。そのために必要であれば TOE 内部にアクセスすることがある。
信頼度： 信頼を持つものが管理者の任を担う。
不正の危険性： TOE の機能全てを使った不正の危険性あり。
知識： TOE の機能仕様を熟知している。

A.Person_Audit TOE **運用監査者**

役割： セキュリティを保った状態で TOE を稼動させることに責任を持つ。そのために TOE の運用状態を監査する。
権限： TOE の監査を行う権限がある。そのために必要であれば TOE 内部にアクセスすることがある。
信頼度： TOE を利用する組織とは直接利害関係がなく、信頼を持つものが監査者の任を担う。
不正の危険性： TOE の機能全てを使った不正の危険性あり。
知識： TOE の機能仕様を熟知している。

A.Person_User TOE **利用者**

役割： TOE を利用して原本データを保存、参照、または削除する。
権限： TOE が提供する機能を利用する権限をもつ。TOE 内部に直接アクセスする権限はない。
信頼度： 信頼度は低い。
不正の危険性： 運用管理機能を除く TOE の機能を使った不正の危険性あり。
知識： 運用管理に関する機能を除いた TOE の機能仕様を熟知している。

3.2 セキュリティポリシー (Organizational Security Policies)

本 PP では特定のセキュリティポリシーは想定していない。

3.3 セキュリティ脅威 (Threats to Security)

3.3.1 保護対象資産の特定 (Assets)

以下に、原本性保証電子保存時に最低限必要な保護対象となる資産を記述する。

- 原本データ

  原本データとは、TOE へユーザが入力したデータのことを指し、TOE が生成したデータは含まない。

- 原本データの時刻関連情報

  原本データの時刻関連情報とは、原本データ登録日時や登録順番など、原本データの存在時刻を推測するために必要な情報のことである。

3.3.2 TOE の脅威 (Threats to TOE)

以下に想定される脅威を記述する。ただし、脅威の具体的実施手順については特定しない。

識別子	脅威の説明
T.Mod_Data_UseTOE	TOE の機能を使い、原本データの内容を痕跡を残さずに変更(上書き登録・編集・廃棄・すり替え)される
T.Mod_Data_Direct	TOE の機能を介さず、原本データの内容を痕跡を残さずに直接変更(書換え・消去・偽造・すり替え)される
T.Mod_Time_UseTOE	TOE の機能を使い、TOE 内での原本データの時刻関連情報が痕跡を残さずに変更(書換え・偽造)される
T.Mod_Time_Direct	TOE の機能を介さず、TOE 内での原本データの時刻関連情報が痕跡を残さずに変更(書換え・消去)される

T.Mod_Data_UseTOE　TOE **の機能を使い、原本データの内容を痕跡を残さずに変更される**

- TOE が原本データの変更機能を提供していなくても、同じ名前などで後から登録することにより、痕跡を残さず原本データを上書きまたは、混同させられる可能性がある。
- TOE が原本データ編集機能を提供していた場合には、正当に編集しただけでもその痕跡が残らない可能性がある。
- 原本データ編集機能の実行を制限（権限設定など）していたとしても、管理者が一時的に制限を解除して痕跡を残さず原本データを編集する可能性がある。
- 原本データ廃棄（削除）機能を使い、正当に削除しても、痕跡が残らない可能性がある。
- 原本データ廃棄（削除）機能の実行を制限（権限設定・削除不可期間設定など）していたとしても、管理者が制限を一時的に解除（権限変更・期間短縮など）して痕跡を残さず削除される可能性がある。
- 原本データ識別子（ファイル名や原本データ ID など）の変更機能があった場合には、正当に変更しただけでも原本データのすり替えの痕跡が残らない可能性がある。

・ 原本データ識別子（ファイル名や原本データ ID など）の変更機能の実行を制限（権限設定など）していたとしても、管理者が制限を一時的に解除して痕跡を残さず原本データがすり替えられる可能性がある。

T.Mod_Data_Direct TOE **の機能を介さず、原本データの内容を痕跡を残さずに直接変更される**

・ TOE の機能を使わずに原本データを書換えられる可能性がある。
・ TOE の機能を使わずに原本データを消去される可能性がある。
・ 原本データを TOE の登録機能を使わずに TOE 内に送り、それを正しい原本データとして TOE が認識してしまう（偽造される）可能性がある。
・ 原本データ識別子（ファイル名や原本データ ID など）を TOE の機能を使わずに書換えられ、原本データを別の原本データとすり替えられてしまう可能性がある。

T.Mod_Time_UseTOE TOE **の機能を使い、**TOE **内での原本データの時刻関連情報が痕跡を残さず変更される**

・ TOE が TOE システム時計を持ち、それをもとに原本データに時刻情報（登録日時・最終更新日時など）を関連付けていた場合、TOE システム時計を変更して原本データ時刻情報を痕跡を残さず偽造される可能性がある。
・ TOE が時刻関連情報の編集機能を持っていた場合には、時刻情報を普通に編集されても痕跡が残らない可能性がある。
・ 時刻関連情報編集機能の実行を制限（権限設定など）していたとしても、管理者が一時的に制限を解除して痕跡を残さず時刻関連情報を編集する可能性がある。

T.Mod_Time_Direct TOE **の機能を介さず、**TOE **内での原本データの時刻関連情報が痕跡を残さずに変更される**

・ TOE の機能を使わずに原本データの時刻関連情報を書換えられる可能性がある。
・ TOE の機能を使わずに原本データの時刻関連情報を消去される可能性がある。

3.3.3 TOE 環境の脅威 (Threats to TOE Environment)

TOE の環境を利用した不正は、前提条件により生じないものとする。

4 セキュリティ対策方針 (Security Objectives)

4.1 TOE の技術的セキュリティ対策方針 (Security Objectives for the TOE)

ここでは、TOE で機能として実現するセキュリティ対策を示す。

識別子	対策方針の説明
O.Control_Doc_Access	原本データへのアクセスを制御する
O.Control_Timer_Access	時刻関連情報へのアクセスを制御する
O.Audit_Doc_Access	原本データへの処理の履歴を記録する
O.Audit_Timer_Access	時刻関連情報への処理の履歴を記録する
O.Detect_Integrity_Error	改竄を検知する
O.Protect_Timer	時刻関連情報の取得機能を保護する
O.Doc_Identification	原本データを一意に特定できるようにする

O.Control_Doc_Access **原本データへのアクセスを制御する**

具体的には以下のような目標が考えられる。

（1） 原本データは一定の条件が満たされなければ廃棄（削除）できないように制御する。例えば以下のような条件が考えられる。

- 原本データの保存期限を設定し、その期限が過ぎるまでは削除できない。
- 原本データ登録者や特別な権限を持った者などのみ削除機能を実行できる。

（2） 原本データが上書き更新されないように制御する。

- 原本データの編集機能を TOE が持つ場合は、上書き更新ではなく編集前の原本データを残すようにして更新データを保存する。
- 原本データ登録時に原本データ識別子（ファイル名や原本データ ID など）が重なった場合には、エラーを返すか重複時処理を実行する。

O.Control_Timer_Access **時刻関連情報へのアクセスを制御する**

具体的には以下のような目標が考えられる。

i. **原本データに関連付けられた時刻情報は一般利用者、管理者など誰も作成・変更・削除できないように制御する。**

ii. TOE **システム時計を時刻の拠り所としている場合は、ある条件を満たす場合のみ時計を調整できるよう制御する。**

例えば以下のような条件が考えられる。

- 特別な権限をもった者のみが時計を調整できる。
- 誰も恣意的に調整することはできず、システムが自動的に標準時刻に合わせる。

O.Audit_Doc_Access　**原本データへの処理の履歴を記録する**

具体的には以下のような目標が考えられる。

（1） 原本データに対するアクセスの履歴を記録する。
例えば以下のようなアクセスが考えられる。

- 原本データ登録
- 原本データ参照
- 原本データ更新（TOE が更新機能をもつ場合）
- 原本データ廃棄（削除）

O.Audit_Timer_Access　**時刻関連情報への処理の履歴を記録する**

具体的には以下のような目標が考えられる。

（1） 原本データに関連付けられた時刻情報に対するアクセスの履歴を記録する。
例えば以下のようなアクセスが考えられる。

- 原本データに関連付けられた時刻情報の閲覧

（2） TOE システム時計を時刻の拠り所としている場合は、システム時計に対するアクセスの履歴を記録する。
例えば以下のようなアクセスが考えられる。

- システム時計変更

（3） 時刻情報の拠り所となる情報（TOE システム時計など）を変更した場合には、変更量（30 分戻した、3 日進めたなど）を記録する。

O.Detect_Integrity_Error　**改竄を検知する**

具体的には以下のような目標が考えられる。

（1） 原本データに対して直接的に行われる改ざん・削除・偽造・すり替えを含むインテグリティエラーを検出できるようにする。

（2） 原本データに関連付けられた時刻情報に対して直接的に行われる改ざん・削除・偽造・すり替えを含むインテグリティエラーを検出できるようにする。

O.Protect_Timer　**時刻関連情報の取得機能を保護する**

具体的には以下のような目標が考えられる。

（1） 原本データに関連付けられた時刻情報の拠り所となる情報（TOE システム時刻など）に対して直接的に行われる改ざん・削除・偽造・すり替えを含むインテグリティエラーを検出できるようにする。

O.Doc_Identification　**原本データを一意に特定できるようにする**

具体的には以下のような目標が考えられる。

（1） 原本データを特定する一意な識別子（ファイル名や原本データ ID など）を原本データへ割り当てる。

（2） 原本データを特定する一意な識別子（ファイル名や原本データ ID など）を変更できないようにする。

4.2 環境セキュリティ対策方針 (Security Objectives for the Environment)

ここでは、TOE の運用・管理上におけるセキュリティ対策を以下に示す。

識別子	対策方針の説明
OE.No_UnAuthorized_Person	第三者からのアクセスを防止する
OE.Obey_Policy	セキュリティポリシー／ルールの教育
OE.Physical	TOE の利用目的の限定

OE.No_Unauthorized_Person　第三者からのアクセスを防止する

TOE に対しての物理的・論理的アクセスを関係者に限定し、第三者がアクセスできないような環境に TOE を設置する。

OE.Obey_Policy　セキュリティポリシー／ルールの教育

セキュリティポリシー／ルールを正確に理解し、重要性を認識し、忠実に遵守できるよう TOE 関係者を教育する。

OE.Single_Purpose　TOE の利用目的の限定

TOE は原本性保証電子保存にのみ利用するよう不必要なソフトウェアなどはインストールしない。また、他の目的で TOE の機能を利用しないよう利用者を教育する。

5 IT セキュリティ要件 (IT Security Requirements)

5.1 TOE セキュリティ要件 (TOE Security Requirements)

5.1.1 TOE セキュリティ機能要件

以下に、ISO15408 より抽出した機能要件を示し、後にその内容を示す。

コンポーネント	コンポーネント名称
Class FAU － Security Audit	
FAU_GEN.1	Audit Data Generation (**監査データ生成**)
FAU_SAR.1	Audit Review (**監査レビュー**)
FAU_STG.2	Guarantee of Audit Data Availability (**監査データ可用性の保証**)
Class FDP － User Data Protection	
FDP_ACC.2	Complete access control**（完全アクセス制御）**
FDP_ACF.1	Security attribute based access control (**セキュリティ属性によるアクセス制御**)
FDP_DAU.1	Basic data authentication (**基本的データ認証**)
FDP_SDI.2	Stored data integrity monitoring and action (**蓄積データ完全性監視およびアクション**)
Class FPT － Protection of the TOE Security functions	
FPT_RVM.1	Non-bypassability of the TSP (TSP **の非バイパス性**)
FPT_STM.1	Reliable time stamps (**信頼タイムスタンプ**)
FPT_TST.1	TSF testing (TSF **自己テスト**)
Class FMT － Security Management	
FMT_MOF.1	Management of security functions behaviour (**セキュリティ機能のふるまいの管理**)
FMT_MSA.1	Management of security attributes (**セキュリティ属性の管理**)
FMT_MSA.3	Static attribute initialization (**セキュリティ属性の初期化**)
FMT_MTD.1	Management of TSF data (TSF **データの管理**)
FMT_SMR.1	Security roles (**セキュリティの役割**)
Class FIA － Identification and Authentication	
FIA_UID.1	Timing of identification**（識別のタイミング）**

ISO15408 では、セキュリティ要件中に以下のオペレーションがある。

割当て（assignment）： セキュリティ要件に対して詳細なパラメータ仕様を含めることが出来る。

繰返し（iteration）： PP/ST 内で詳細な機能及び保証要件コンポーネントを一回以上使用することが出来る。

選択（selection）： 与えられた選択肢から、１つ以上の詳細な仕様を選択することが出来る。

詳細化（refinement）： PP または ST の作者が、機能または保証要件に詳細仕様を加えることが出来る。

FAU_GEN.1 Audit data generation (**監査データ生成**)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b. All auditable events for the ***basic*** level of audit.; and

c. [assignment: other specifically defined auditable events].

コンポーネント	監査記録対象となる事象
FDP_ACF.1	SFP.USER-DATA-ACCESS-CONTROLで扱われるオブジェクトに対する操作の実行におけるすべての要求。
FDP_DAU.1	データの有効性の証拠の生成の成功・不成功すべて。
FDP_SDI.2	利用者データ完全性チェックのすべての試み（結果も含む）。
	生じた完全性誤りの種別。
FPT_TST.1	アクセス制御テーブルへの改竄検証の実行とその結果。
FMT_MOF.1	TSFの機能のふるまいに対するすべての改変。
FMT_MSA.1	セキュリティ属性の値に対するすべての改変。
FMT_MSA.3	許可的あるいは制限的規則のデフォルト設定の改変。
	セキュリティ属性の初期値に対するすべての改変。
FMT_MTD.1	TSFデータの値に対するすべての改変。
FMT_SMR.1	役割の一部をなす利用者のグループに対する改変。
FIA_UID.1	提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: *other audit relevant information*]**

Application Notes:

本コンポーネントでは、原本性保証電子保存システム(TOE)の機能の実行履歴は基本レベルで全て記録することを目的としている。特に、原本データと時刻関連情報に関しての操作は全て記録をとること。

また､他のコンポーネントを選択することによって生じた記録対象になる操作は表としてまとめてあるが、追加する形で事象を変更することは問題ない。

FAU_SAR.1 Audit review (**監査レビュー**)

FAU_SAR.1.1 The TSF shall provide **[*authorised users listed below*]** with the capability to read **[*audit information listed below*]** from the audit records.

[Authorized users]

a) A.Person_Admin

b) A.Person_Audit

c) [assignment: その他役割]

[Audit information]

a) 監査証跡すべて

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Notes:

特になし。

FAU_STG.2 Guarantee of audit data availability (**監査データ可用性の保証**)

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to ***detect*** modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that **[assignment: *metric for saving audit records*]** audit records will be maintained when the following conditions occur:

a) Audit storage exhaustion

b) *Failure,*

c) *Attack*

Application Notes:

特になし。

FDP_ACC.2 Complete access control (**完全アクセス制御**)

FDP_ACC.2.1 The TSF shall enforce the **[assignment: *access control SFP listed below*]** on **[assignment: *subjects and objects listed below*]** and all operations among subjects and objects covered by the SFP.

Access control SFP	Subject	Object
SFP.USER-DATA-ACCESS-CONTROL	[assignment: *list of subjects*]	[assignment: 原本データ]
[assignment: *access control SFP*]	[assignment: *list of subjects*]	[assignment: *list of objects*]

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Application Notes:

本PPでは原本性保証電子保存システム(TOE)におけるsubjectを明確に定義できないため、subjectを特定していない。また、「原本データ」も各製品で若干内容が異なることが予想されるので、STを記述する際には「原本データ」も明確に定義すること（以降のコンポーネントでも同様）。

FDP_ACF.1 Security attribute based access control (1) (**セキュリティ属性によるアクセス制御**)

FDP_ACF.1.1 The TSF shall enforce the **[SFP.USER-DATA-ACCESS-CONTROL]** to objects based on **[assignment: *security attributes, named groups of security attributes listed below*].**

a) [assignment: 保存期限情報]

b) [assignment: *other security attributes, named groups of security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects listed below*].**

Rule		Detail
Rule.Deny_Delete	selection	[assignment: 原本データ]に付随する[assignment: 保存期限情報]を用いて、現在時刻が保存期限を過ぎているかどうかを判別し、過ぎていない場合には削除（廃棄）操作をさせないよう制御する。
		[assignment: その他削除（廃棄）拒否ルール]
Rule.Prevent_OverWrite	TOE内に保存している[assignment: 原本データ]に対して、データが上書きされることが無いように制御する。	
[assignment: *rules*]	[assignment: その他ルール]	

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***None*.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules: **[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**

Application Notes:

本コンポーネントは原本データに対するアクセス制御を対象としている。原本性保証電子保存システム(TOE)では、保存期限が過ぎる前に原本データを削除することは絶対にあってはならない。STを記述する際には保存期限を表す情報が何であるかを特定すること。また、原本性保証電子保存システム(TOE)では、正当な権限を持った者が不正した際にもデータをもとに戻せるように、一度保存した原本データを上書きするような内部実装をしてはならない。

特例的に原本データへのアクセスを許すようなルールは設定してはならないが、原本データへのアクセスを拒否するようなルールは必要に応じて設定しても構わない。

FDP_ACF.1 Security attribute based access control (2) (**セキュリティ属性によるアクセス制御**)

FDP_ACF.1.1 The TSF shall enforce the **[assignment: *access cotrol SFP*]** to objects based on **[assignment: *security attributes, named groups of security attributes*].**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules: **[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**

Application Notes:

本コンポーネントは対象が原本データ以外のアクセス制御を対象としている。

FDP_DAU.1 Basic data authentication (**基本的データ認証**)

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of:

a) [assignment: 原本データ]

b) [assignment: *list of objects or information types*].

FDP_DAU.1.2 The TSF shall provide **[assignment: *list of subjects listed below*]** with the ability to verify evidence of the validity of the indicated information.

a) [assignment: TSF]

b) [assignment: *list of subjects*]

Application Notes:

本コンポーネントでは、原本性保証電子保存システム(TOE)内に保存されている原本データが、TOEの機能を介して正当に保存されたものと、TOEを介さずに偽造の目的で保存されたものを区別するための証拠を生成することが目的である。よって、証拠を検証するsubjectとしてはTSF以外には特に規定せず、STに委ねる。

FDP_SDI.2 Stored data integrity monitoring and action (**蓄積データ完全性監視及びアクション**)

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for **[assignment: *integrity errors listed below*]** on all objects, based on the following attributes: **[assignment: *user data attributes*].**

[Integrity error]

a) 変更

b) 追加

c) 消去

d) [assignment: *other integrity error*]

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **[assignment: *action to be taken*].**

Application Notes:

本コンポーネントで完全性エラーの中にすり替えが入っていないのは、FDP_DAU.1で検知できるためである。

FPT_RVM.1 Non-bypassability of the TSP (TSP **の非バイパス性**)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Notes:

本コンポーネントはTSFデータである時刻関連情報に対するセキュリティポリシーが完全にかかっていることを保証するためのものである。

FPT_STM.1 Reliable time stamps (**信頼タイムスタンプ**)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Application Notes:

本コンポーネントで求めるタイムスタンプの信頼度とは､物理世界での絶対的な時刻との同期までは求めず、原本性保証電子保存システム(TOE)内で生成したタイムスタンプ間での前後関係が狂わない程度でよい。

FPT_TST.1 TSF testing (TSF **自己テスト**)

FPT_TST.1.1 The TSF shall run a suite of self tests **[selection*: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]** to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application Notes:

本コンポーネントはTSFデータの完全性テストのためだけに使用する｡よってFPT_TST.1.1とFPT_TST.1.3は特に必要とはしない。よって、依存関係にあるFPT_AMT.1は依存関係が成り立たないと判断し、本PPでは選択していない。なお、TSFデータにはFMT_MSAでの「時刻関連情報」、「アクセス制御テーブル情報」、「利用者識別子」、「一意な原本データ識別子」や、FMT_MTDでの「改竄検知用情報」などがある。

FMT_SMR.1 Security roles (**セキュリティの役割**)

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: *the authorised identified roles listed below*]**.

[Ahthorized identified role]

a) Role.Administration (３章のA.Person_Adminの役割と同じ)

b) Role.Audit (３章のA.Person_Auditの役割と同じ)

c) Role.User (３章のA.Person_Userの役割と同じ)

d) [assignment: *list of roles*]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Notes:

本PPでは、３章での人的前提条件以外の役割は想定しない。

FMT_MOF.1 Management of security functions behaviour (**セキュリティ機能のふるまいの管理**)

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: *determine the behaviour of, disable, enable, modify the behaviour of*]** the functions **[assignment: *list of functions listed below*]** to **[assignment: *the authorised identified roles listed below*].**

Role	Functions	Action
Role.Administration	[assignment: 原本データ]の完全性誤りが検知された際のアクション	[selection: *determine the behaviour, disable, enable, modify the behaviour*]
	監査証跡記録機能	なし
	[assignment: *list of functions*]	[selection: *determine the behaviour, disable, enable, modify the behaviour*]
Role.Audit	[assignment: 原本データ]の完全性誤りが検知された際のアクション	[selection: *determine the behaviour, disable, enable, modify the behaviour*]
	監査証跡記録機能	[assignment: disable以外]
	[assignment: *list of functions*]	[selection: *determine the behaviour, disable, enable, modify the behaviour*]
Role.User	[assignment: 原本データ]の完全性誤りが検知された際のアクション	なし
	監査証跡記録機能	なし
	[assignment: *list of functions*]	[selection: *determine the behaviour, disable, enable, modify the behaviour*]

Application Notes:

本コンポーネントではFDP_SDI.2で定義されるアクションが管理要件として入るほかに、追加として、監査証跡の記録機能を誰もOffにできないように規定している。これによって、必ず監査証跡が記録されることになり、TOEの機能を使った上での操作の履歴は全て残ることになる。

FMT_MSA.1 Management of security attributes (**セキュリティ属性の管理**)

FMT_MSA.1.1 The TSF shall enforce the **[SFP.USER-DATA-ACCESS-CONTROL]** to restrict the ability to **[selection: *change_default, query, modify,* [assignment: *other operations*]]** the security attributes **[assignment: *list of security attributes listed below*]** to **[assignment: *the authorised identified roles listed below*].**

Role	Security attribute	Action
Role.Administration	[assignment: 時刻関連情報]	Query
	[assignment: 時刻関連情報]に対する[assignment: アクセス管理テーブル情報]	[assignment: *change_default, query, modify,delete,clear以外の操作*]
	[assignment: 利用者識別子]	Query, [assignment: *change_default, modify,delete,clear以外の操作*]
	[assignment: 一意な原本データ識別子]	Query, [assignment: *change_default, modify,delete,clear以外の操作*]
	[assignment: *list of security attribute*]	[selection: *change_default, query, modify,* [assignment: *other operations*]]
Role.Audit	[assignment: 時刻関連情報]	Query
	[assignment: 時刻関連情報]に対する[assignment: アクセス管理テーブル情報]	なし
	[assignment: 利用者識別情報]	Query, [assignment: *change_default, modify,delete,clear以外の操作*]
	[assignment: 一意な原本データ識別子]	Query, [assignment: *change_default, modify,delete,clear以外の操作*]
	[assignment: *list of security attribute*]	[selection: *change_default, query, modify,* [assignment: *other operations*]]
Role.User	[assignment: 時刻関連情報]	Query
	[assignment: 時刻関連情報]に対する[assignment: アクセス管理テーブル情報]	なし
	[assignment: 利用者識別情報]	[selection: Query, [assignment: *change_default, modify,delete,clear以外の操作*]]
	[assignment: 一意な原本データ識別子]	Query, [assignment: *change_default, modify,delete,clear以外の操作*]
	[assignment: *list of security attribute*]	[selection: *change_default, query, modify,* [assignment: *other operations*]]

Application Notes:

本コンポーネントは、セキュリティ属性に関するアクセス制御を行う観点で記述してあり、最低限アクセスを制御すべきセキュリティ属性を記述した。ここで「時刻関連情報」、「アクセス管理テーブル情報」はPPでは特定できないので、STを記述する際には定義すること。なおアクセス管理テーブル情報とは、テーブル状のデータ形式でなくてもよく、アクセス管理のよりどころとなる情報のことを指す。

また、「利用者識別情報」「一意な原本データ識別子」についてもSTを記述する際には定義を行うこと。その際、一意になる根拠も合わせて明記すること。

FMT_MSA.3 Static attribute initialisation (**セキュリティ属性の初期化**)

FMT_MSA.3.1 The TSF shall enforce the **[SFP.USER-DATA-ACCESS-CONTROL]** to provide **[selsction: *restrictive, permissive, other property*]** default values for security attributes that are used TOEnforce the SFP.

Application Notes:

特になし。

FMT_MTD.1 Management of TSF data (TSF **データの管理**)

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]** the **[assignment: *list of TSF data listed below*]** to **[assignment: *the authorised identified roles listed below*].**

Role	TSF data	Action
Role.Administration	[assignment: 時刻関連情報]	Modify, Query
	監査証跡	Query
	[assignment: 改竄検知用情報]	なし
	[assignment: *list of TSF data*]	[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
Role.Audit	[assignment: 時刻関連情報]	Modify, Query
	監査証跡	Change_default, Query
	[assignment: 改竄検知用情報]	なし
	[assignment: *list of TSF data*]	[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
Role.User	[assignment: 時刻関連情報]	Query
	監査証跡	Query
	[assignment: 改竄検知用情報]	なし
	[assignment: *list of TSF data*]	[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

Application Notes:

本コンポーネントは、TSFデータに関するアクセス制御を行う観点で記述してあり、最低限アクセスを制御すべきTSFデータを記述した。ここでいう「時刻関連情報」とはタイムスタンプを生成する際に拠り所とする時刻情報のことであり、例えばOSのシステムタイマなどがある。STを記述する際には「時刻関連情報」を定義すること。「時刻関連情報」がModify可能にしているのは、TOEの時刻がずれた場合に時刻を補正することを考慮したものであるので、それ以外の目的でModifyは行ってはならない。

また、「改竄検知用情報」とはユーザデータやTSFデータなどに対する改竄を検知するための情報のことである。STを記述する際にはこれも定義すること。

FIA_UID.1 Timing of identification （識別のタイミング）

FIA_UID.1.1 The TSF shall allow **[assignment: *list of TSF-mediated actions*]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Notes:

特になし。

5.1.2 TOE セキュリティ保証要件

以下に、ISO15408 より EAL4 を満たすために必要なセキュリティ保証要件を示す。機能強度は SOF-medium とする。

表5．2 TOE IT セキュリティ保証要件

コンポーネント	コンポーネント名称
ACM_AUT.1	Partial CM automation（一部自動化された構成管理）
ACM_CAP.4	Generation support and acceptance procedures（生成の支援と受入れ手続き）
ACM_SCP.2	Problem tracking CM coverage（問題追跡のための構成管理適用範囲）
ADO_DEL.2	Detection of modification（変更の検出）
ADO_IGS.1	Installation, generation, and start-up procedures（設置、生成、立上げ）
ADV_FSP.2	Fully defined external interfaces（外部インタフェース定義の十分性）
ADV_HLD.2	Security enforcing high-level design（セキュリティ実施上位レベル設計）
ADV_IMP.1	Subset of the implementation of the TSF（TSF の一部の実装）
ADV_LLD.1	Descriptive low-level design（記述的下位レベル設計）
ADV_RCR.1	Informal correspondence demonstration（非形式的対応の実証）
ADV_SPM.1	Informal TOE security policy model（非形式的な TOE セキュリティ方針モデル）
AGD_ADM.1	Administrator guidance（管理者用ガイダンス）
AGD_USR.1	User guidance（ユーザガイダンス）
ALC_DVS.1	Identification of security measures（セキュリティ対策の識別）
ALC_LCD.1	Developer defined life-cycle model（開発者によるライフサイクルモデルの定義）
ALC_TAT.1	Well-defined development tools（開発ツール定義の十分性）
ATE_COV.2	Analysis of coverage（カバレージの分析）
ATE_DPT.1	Testing: high-level design（上位レベル設計テスト）
ATE_FUN.1	Functional testing（機能テスト）
ATE_IND.2	Independent testing – sample（独立テストーサンプリング）
AVA_MSU.2	Validation of analysis（分析の確認）
AVA_SOF.1	Strength of TOE security function evaluation（セキュリティ機能強度評価）
AVA_VLA.2	Independent vulnerability analysis（独立脆弱性試験）

5.2 IT 環境セキュリティ要件 (Security Requirements for the IT Environment)

IT 環境セキュリティ要件は特に設けない。

6 根拠 (Rationale)

6.1 セキュリティ対策方針根拠 (Rationale for Security Objectives)

このセクションでは、不必要なセキュリティ対策方針がないこと、ならびに、すべての脅威、前提条件が考慮されていることを示すと共に、セキュリティ対策方針と脅威、前提条件との対応関係を補足説明する。

6.1.1 セキュリティ対策目標とセキュリティ環境との対応

以下に、各セキュリティ対策方針毎に、対抗する脅威、関連する前提条件を示すことにより、不必要なセキュリティ対策方針がないことを示す。さらに、すべての脅威、および前提条件が1つ以上のセキュリティ対策方針によって対策されていることを示すことにより、セキュリティ環境が漏れなく考慮されていることを示す。

表6．1 セキュリティ対策方針とセキュリティ環境の対応

セキュリティ対策方針	対抗する脅威	対応する前提条件
O.Control_Doc_Access	T.Mod_Data_UseTOE	
O.Control_Timer_Access	T.Mod_Time_UseTOE	
O.Audit_Doc_Access	T.Mod_Data_UseTOE	
O.Audit_Timer_Access	T.Mod_Time_UseTOE	
O.Detect_Integrity_Error	T.Mod_Data_Direct T.Mod_Time_Direct	
O.Protect_Timer	T.Mod_Time_Direct	
O.Doc_Identification	T.Mod_Data_UseTOE	
OE.No_Unauthorized_Person		A.No_Unauthorized_Person
OE.Obey_Policy		A.Obey_Policy
OE.Single_Purpose		A.Single_Purpose

表6．2 脅威とセキュリティ対策方針の対応

脅　　威	セキュリティ対策方針
T.Mod_Data_UseTOE	O.Control_Doc_Access, O.Audit_Doc_Access, O.Doc_Identification
T.Mod_Data_Direct	O.Detect_Integrity_Error
T.Mod_Time_UseTOE	O.Control_Timer_Access, O.Audit_Timer_Access
T.Mod_Time_Direct	O.Detect_Integrity_Error, O.Protect_Timer

表6．4 前提条件とセキュリティ対策方針の対応

前提条件	セキュリティ対策方針
A. No_Unauthorized_Person	OE.No_Unauthorized_Person
A. Obey_Policy	OE.Obey_Policy
A. Single_Purpose	OE.Single_Purpose

6.2 セキュリティ要件根拠 (Rationale for Security Requirements)

このセクションでは、各セキュリティ対策方針が少なくともひとつのセキュリティ機能要件によって実現されると同時に、各セキュリティ機能要件が少なくともひとつのセキュリティ対策方針の実現に係わることを示す。さらに、セキュリティ機能要件が各セキュリティ対策方針に対して必要十分である根拠を補足説明する。

6.2.1 セキュリティ対策方針とセキュリティ要件の対応関係

各セキュリティ対策方針が少なくとも一つのセキュリティ機能要件によって実現されることと各セキュリティ機能要件が少なくとも一つのセキュリティ対策方針の実現に関わることを表6．5に示す。また、表6．6にセキュリティ機能要件の依存関係を示す。

表6．5 セキュリティ対策方針とセキュリティ機能要件の対応関係

	O.Control_Doc_Access	O.Control_Timer_Access	O.Audit_Doc_Access	O.Audit_Timer_Access	O.Detect_Integrity_Error	O.Protect_Timer	O.Doc_Identification
FAU_GEN.1			○	○			
FAU_SAR.1			○	○			
FAU_STG.1			○	○			
FDP_ACC.2	○						△
FDP_ACF.1	○						
FDP_DAU.1					○		
FDP_SDI.2					○		
FPT_RVM.1		○					
FPT_STM.1			○	○			
FPT_AMT.1	△	△			△	△	
FPT_TST.1	○	○			○	○	
FMT_MOF.1			○	○			
FMT_MSA.1	○	○					○
FMT_MSA.3	△						
FMT_MTD.1		○	○	○			
FMT_SMR.1	△	△	△	△			△
FIA_UID.1	△	△	△	△			△

（△は依存性により追加されたコンポーネントを示す。）

表6．6 セキュリティ機能要件の依存関係

コンポーネント	依存するコンポーネント
FAU_GEN.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1
FDP_ACC.2	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1、FMT_MSA.3
FDP_DAU.1	なし
FDP_SDI.2	なし
FPT_RVM.1	なし
FPT_STM.1	なし

FPT_TST.1	なし（FPT_AMT.1 が依存しない理由は FPT_TST.1 の ApplicationNote 参照）
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1、FMT_SMR.1
FMT_MSA.3	FMT_MSA.1、FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FIA_UID.1	なし

6.2.2 セキュリティ機能要件の補足説明

1) O.Control_Doc_Access（原本データへのアクセスを制御する）は、以下の要件により実現される。

FDP_ACC.2、FDP_ACF.1、(FMT_MSA.3、FMT_MSA.1、FMT_SMR.1、FIA_UID.1)

- FDP_ACC.2 により、原本データとそれを利用するサブジェクトとの間の全ての操作をアクセス制御の対象とする。
- FDP_ACF.1 により、原本データの廃棄（削除）に関する制御を規定することで、TOE の機能を利用した不正な削除から保護する。
- FDP_ACF.1 により、原本データの上書き更新に関する制御を規定することで、TOE の機能を利用した不正な上書き更新から保護する。

FPT_TST.1、(FPT_AMT.1)

- FPT_TST.1 により、アクセス制御のための管理情報の完全性をチェックすることで、アクセス制御テーブルデータを改竄しての不正アクセスを防止する。

FMT_MSA.1、(FMT_SMR.1、FIA_UID.1)

- FMT_MSA.1 により、アクセス制御のための管理情報の管理（登録・変更・削除など）を行うものを限定することで、アクセス制御テーブルデータの内容を変更しての不正アクセスを減らす。

2) **O.Control_Timer_Access（時刻関連情報へのアクセスを制御する）は、以下の要件により実現される。**

FMT_MTD.1、(FMT_SMR.1、FIA_UID.1)

- FMT_MTD.1 により、時刻関連情報へのアクセスを制御し、TOE の機能を利用しての不正な削除から保護する。
- FMT_MTD.1 により、時刻関連情報へのアクセスを制御し、TOE の機能を利用しての不正な改竄から保護する。

FPT_TST.1、(FPT_AMT.1)

- FPT_TST.1 により、アクセス制御のための管理情報の完全性をチェックすることで、アクセス制御テーブルデータを改竄しての不正アクセスを防止する。

FMT_MSA.1、(FMT_SMR.1、FIA_UID.1)

- FMT_MSA.1 により、アクセス制御のための管理情報の管理（登録・変更・削除など）を行うものを限定することで、アクセス制御テーブルデータの内容を変更しての不正アクセスを減らす。

FPT_RVM.1

- FPT_RVM.1 により、時刻関連情報に対して上記のアクセス制御が常に実施されることを保証することで、TOE の機能を利用しての不正アクセスを防止する。

3) **O.Audit_Doc_Access（原本データへの処理の履歴を記録する）は、以下の要件により実現される。**

FAU_GEN.1、FAU_SAR.1、(FPT_STM.1)

- FAU_GEN.1 により、原本データへの処理の履歴（監査証跡）を記録することで、TOE の機能を利用しての有権限者の不正行為（アクセス制御テーブルデータを変更しての不正アクセスなど）を追跡できるようにする。
- FAU_SAR.1 により、監査証跡の閲覧を支援し、不正行為の追跡が容易になるようにする。

FMT_MOF.1、(FMT_SMR.1、FIA_UID.1)

- FMT_MOF.1 により、監査証跡記録機能の停止を誰もできないようにすることで、監査証跡の記録機能を停止した上での TOE の機能を使った不正行為を防止し、必ず不正行為の追跡を可能にする。

FAU_STG.2*、*FMT_MTD.1*、*(FAU_GEN.1*、*FPT_STM.1*、*FMT_SMR.1*、*FIA_UID.1)

- FMT_MTD.1 により、監査証跡への操作（改変・削除など）が誰もできないようにすることで、TOE の機能を利用して監査証跡を改変し証拠隠滅した上での、有権限者の不正行為を検知する。
- FAU_STG.2 により、監査証跡に対する直接的な改竄行為を検知することで、監査証跡を改竄し証拠隠滅した上での、有権限者の不正行為を検知する。

4) O.Audit_Timer_Access（時刻関連情報への処理の履歴を記録する）は、以下の要件により実現される。

FAU_GEN.1*、*FAU_SAR.1*、*(FPT_STM.1)

- FAU_GEN.1 により、時刻関連情報への処理の履歴（監査証跡）を記録することで、TOE の機能を利用しての有権限者の不正行為（アクセス制御テーブルデータを変更しての不正アクセスなど）を追跡できるようにする。
- FAU_SAR.1 により、監査証跡の閲覧を支援し、不正行為の追跡が容易になるようにする。

FPT_STM.1

- FPT_STM.1 により、時刻関連情報の変更内容を記録し、複数の時刻関連情報間での前後関係を保証する。

FMT_MOF.1*、*(FMT_SMR.1*、*FIA_UID.1)

- FMT_MOF.1 により、監査証跡記録機能の停止を誰もできないようにすることで、監査証跡の記録機能を停止した上での TOE の機能を使った不正行為を防止し、必ず不正行為の追跡を可能にする。

FAU_STG.2*、*FMT_MTD.1*、*(FAU_GEN.1*、*FPT_STM.1*、*FMT_SMR.1*、*FIA_UID.1)

- FMT_MTD.1 により、監査証跡への操作（改変・削除など）が誰もできないようにすることで、TOE の機能を利用して監査証跡を改変し証拠隠滅した上での、有権限者の不正行為を検知する。
- FAU_STG.2 により、監査証跡に対する直接的な改竄行為を検知することで、監査証跡を改竄し証拠隠滅した上での、有権限者の不正行為を検知する。

5) O.Detect_Integrity_Error（改竄を検知する）は、以下の要件により実現される。

FDP_DAU.1

・ FDP_DAU.1 により、TOE の機能を介さずに TOE 内へ送られたデータを TOE が正式なデータとして扱わないようにし、原本データ偽造を防止する。

FDP_SDI.2

・ FDP_SDI.2 により、TOE 内に保存されている原本データへの直接的な改竄を検知する。

FPT_TST.1、(FPT_AMT.1)

・ FPT_TST.1 により、TOE 内に保存されている時刻関連情報への直接的な改竄を検知する。

6) O.Protect_Timer（時刻関連情報の取得機能を保護する）は、以下の要件により実現される。

FPT_TST.1、(FPT_AMT.1)

・ FPT_TST.1 により、TOE 内に保存されている時刻関連情報の拠り所となるデータ（TOE システム時間など）への直接的な改竄を検知する。

7) O.Doc_Identification（原本データを一意に特定できるようにする）は、以下の要件により実現される。

FPT_MSA.1、(FMT_SMR.1、FIA_UID.1、FDP_ACC.2)

・ FPT_MSA.1 により、原本データに対して一意に特定できる識別子をセキュリティ属性として関連付けることで、他の原本データとの混同を防止する。

・ FPT_MSA.1 により、原本データ識別子に対する操作（改変・削除など）を誰もできないようにすることで、TOE の機能を利用して識別子を改竄した上での原本データのすり替えを防止する。

6.3 保証要件の根拠 (Rationale for Assurance Requirements)

原本性保証電子保存システムでは、システム内に保存されるデータの重要度が、一般的なシステムに比べかなり高いことが予想される。よって、システムに保存されるデータの完全性に関して高い保証レベルを要求する。よって、民生品が備えるべき保証レベルの中で最高と位置付けられる EAL4 を要求するのが妥当であると考えられる。

2. ANNEX

以下に、CC（Common Criteria）で使用される略語を示す。

EAL　：評価保証レベル（Evaluation Assurance Level）
IT　：情報技術（Information Technology）
PP　：プロテクションプロファイル（Protection Profile）
SF　：セキュリティ機能（Security Function）
SFP　：セキュリティ機能方針（Security Function Policy）
SOF　：セキュリティ機能強度（Strength Of Function）
ST　：セキュリティターゲット（Security Target）
TOE　：評価対象製品（Target Of Evaluation）
TSC　：TSF 制御範囲（TSF Scope of Control）
TSF　：TOE セキュリティ機能（TOE Security Functions）
TSFI　：TSF インタフェース（TSF Interface）
TSP　：TOE セキュリティ方針（TOE Security Policy）

以下に、本編で使用された用語を説明する。

セキュリティ機能要件編

割り当て（Assignment）：コンポーネント内の識別されたパラメータの仕様。
詳細化（Refinement）：　コンポーネントに詳細を追加すること。
繰返し（Iteration）：　様々な操作で２回以上、コンポーネントを利用すること。
選択（Selection）：　コンポーネント内のリストから１つまたは複数の項目を指定すること。
プロテクションプロファイル（Protection Profile、PP）：
ある TOE カテゴリに関して特定の消費者ニーズを満たす、実装に依存しないセキュリティ要件のセット。
セキュリティターゲット（Security Target、ST）：
明らかにされた TOE の評価基準として用いられるセキュリティ要件および仕様のセット。
セキュリティ対策（Security Objective）：
明らかにされた脅威への対抗、または明らかにされた組織セキュリティ方針および前提の履行（あるいはその両方）のための主旨記述書。
TOE セキュリティ機能（TOE Security Functions、TSF）：
TSP の正確な実施のために依存しなければならない TOE のすべてのハード

ウェア、ソフトウェア、およびファームウェアからなるセット。

TOE セキュリティ機能（TOE Security Policy、TSP）：

TOE 内での資産の管理方法、保護方法、および配布方法を規定する規則のセット。

セキュリティ保証要件編

構成管理（CM）：　構成管理（CM）：開発工程がすすむに連れて、機能要件→設計→実装と実体化されるのを確立する方法、手段。

構成要素（configuration item）：

TOE の実装表現、設計書、仕様書、テスト仕様書、検査報告書、利用者マニュアル、運用・管理マニュアル、構成管理文書、セキュリティ欠陥、生成支援ツール等。

構成管理システム：　構成要素の変更、TOE の変更（バージョン）を追跡する手段や、変更の許可を制限することで、構成要素の完全性を保証するもの。