長期署名検証ツール認証制度検討会報告書

平成２１年３月２５日

財団法人日本データ通信協会

タイムビジネス協議会

目　　次

はじめに

2005 年 4 月に e-文書法が施行され、証憑類の保管が紙から電子へと容認されたことで、紙を廃棄した電子データによる保管ビジネスが加速するものと期待されていた。ところが、施行後約 4 年が経過した現在でも、e-文書法対応が遅々として進んでいない問題を抱えている。e-文書法対応が進んでいない技術的な原因としては「難解な国税要件を満たすことが困難」あるいは「電子署名およびタイムスタンプを付与したシステム構築が困難」等々、が考えられる。技術的に高度な知識が要求される案件対応では、実装リスクが伴うことから、SI ベンダー側での対応が出遅れている感が強い。このような影響から、相変わらず大半の企業で、旧態依然のシステムによる紙保管が続いているものと思われる。

ところが、一方で電子帳簿保存法に対応した電磁的記録による保存等の承認件数としては、90,132 件（平成 19 年度）も承認されている。つまり、SI ベンダー側としては電子帳簿保存法に対応したシステム案件を受注しながらも、e-文書法に適合したシステム開発だけは意図的に避けている実態が明らかになっている。

また、間近に迫ってきた暗号アルゴリズムの危殆化に伴う証明書の失効問題は、電子署名システムのすべてに影響することから、早期に次世代暗号アルゴリズムへの切り替えとともに、既存の電子署名文書あるいは移行前文書については、長期署名システムによる保管システムの構築が急務といえる。

そこで、タイムビジネス協議会では、タイムスタンプサービスを活用したタイムビジネスの普及促進を目的としたアプリケーション開発支援と技術的な障壁を取り除くための施策として、長期署名検証ツールの認証制度を検討した。また、SI ベンダー側へのインセンティブとして、効果的な認証制度のしくみと課題についても検討した。

タイムビジネスの普及促進には、誰にでも手軽に電子署名およびタイムスタンプを付与したシステムの利用環境が整備されていることが前提条件であり、社会的価値として広く認知されていなければならない。

そのためにも一般利用者レベルで簡単に判断できる認証マークの普及効果は大きく、製品購入時の判断材料として、活用されることが望ましい。

本長期署名検証ツール検討会では、上記 e-文書法に対応したシステム開発の促進や暗号アルゴリズムの危殆化問題への対応策として、長期署名検証ツールの普及と共に認証制度の確立に向けた取り組みが必要不可欠であると結論づけた。

第１章　長期署名検証ツール認証制度の必要性

長期署名検証ツールの認証制度の確立は、従来難解とされていた国税要件を満たした業務アプリケーション開発が容易になる他、効果的なICT化支援策となる可能性がある。

1.1　認証制度の必要性と目的

認証制度が確立した社会を想定した場合、高度な実装技術が要求される電子署名およびタイムスタンプ付与のシステム開発部分については、コンポーネント化による流通が加速し、認証を取得した業務アプリケーション開発が容易になると思われる。また、一般利用者にとっても認証を取得した業務アプリケーションの選択枝が増えることで、健全な競争社会が発展し、社会的コスト削減の効果が期待できる。

従って、JISに準拠した長期署名システムを広く普及させることが重要であり、そのためには、第三者機関による公正な認証制度による認証製品の流通が必要不可欠となる。

長期署名検証ツールの認証制度が広く認知され、アプリケーション開発が活性化することで､電子データの信頼性を確保する環境が整備され、ICT化の普及促進を狙うものである。

1.2　基準を満たした製品の流通と健全な競争社会の実現

長期署名システムについては、長期署名プロファイルが2008年3月にJIS化されたことで、利用者はJISに準拠した製品の選択で、安心して導入できるようになった。ただし、JISに準拠した製品は、開発者側の自己宣言でしかなく、利用者側でのJIS準拠に関する適合性の評価については、判定が難しいといった問題を抱えていた。

また、長期署名システムのJIS準拠による互換性の問題は、導入して数年から数十年後に表面化する恐れもあり、問題が発覚してからでは手遅れとなるリスクも抱えている。従って、長期署名システムの正しい選択方法としては、適正な準拠性の試験を行った製品を選ばなければならない。さらに長期署名検証ツールの適正試験を行う場合、一般利用者がJIS基準を精読し、準拠性を評価することは非常に困難であり、SIベンダー任せとなる。そこで、健全な競争社会を実現するためにも長期署名の検証に関する認証制度の仕組みが必要となる。

1.3　e-文書法に基づく国税要件の定義と基準

e-文書法に適合した電子帳簿システムを開発するには、基準が定義されていない難解な国税要件を満たすことが必要条件であり、システムを開発するSIベンダーにとっても大きな障壁となっている。さらに電子

署名やタイムスタンプを付与したシステム開発となると、難解な PKI 技術を習得しなければならず、エンジニアのスキルアップという問題も抱えている。

そこで、JIS 基準をベースとした認証制度を確立することで、電子署名およびタイムスタンプ付与の部分については、国税要件を満たした基準および仕様等々の定義が可能となり、SI ベンダーにとっても得意とする業務システムの開発に専念できる効果が得られる。

1.4 認証マークの普及による社会的コストの低減

国税要件の基準を満たした製品あるいは JIS 基準に準拠した製品の選択は、利用者にとって重要な問題であり、誰にでも簡単に判断できる仕組みが必要となる。また、製品を開発する SI ベンダー側にとっても他社との差別化になることから、インセンティブの効果は大きく、競って認証を取得する可能性がある。従って、認証マークを取得した製品が多数流通することで、健全な競争的市場が醸成され、長期署名検証ツールのコストが下がる可能性が高い。

そこで、本認証制度および認証マークを普及させることで、社会的コストの低減を狙うものである。

第２章　認証制度の概要

長期署名検証ツールの認証制度とは、IT ベンダー等が開発した長期署名システムが JIS に適合した製品であることを、JIS 基準である JIS X 5092:2008 及び JIS X 5093:2008 に基づいて第三者機関（評価機関）が評価し、その評価結果を認証機関が認証する制度である。

2.1　認証制度の類型

電気通信機器、電気用品等、様々な製品に関して設けられている基準認証制度については、認証の実施主体に着目すると次のような類型に分類されている。

（１）国の認証制度
国又は国の代行機関が、製造業者等から申請を受けて認証を行う制度。

（２）第三者認証制度
国の代行機関でない第三者機関が、製造業者等から申請を受けて認証を行う制度。

（３）自己適合宣言制度
製造事業者等が自ら技術基準への適合性の評価を行う制度。

注：ISO/IEC ガイド 2（標準化及び関連活動－一般的な用語）において、「認証」とは「製品、方法又はサービスが所定の“要求事項”に適合していることを、“第三者”が文書で保証する手続」と定義されている。
引用：端末機器及び特定無線設備の基準認証制度に関する研究会報告書（案）

2.2　認証制度案

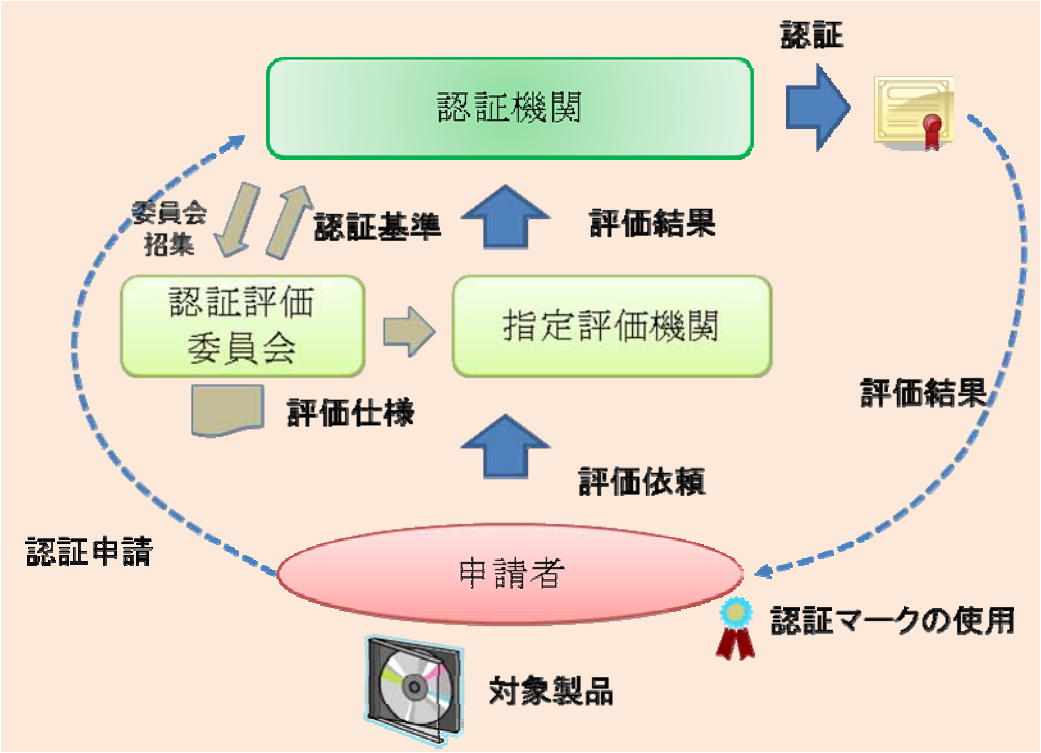
上記の背景を踏まえ、本調査研究では具体的な認証体制として、以下の第三者機関による認証制度を検討した。

ここでの認証機関とは、申請者からの申請を受理する機関であり、指定評価機関からの評価結果に基づく認証を行う機関をいう。また、認証機関から指定された評価機関は、申請者からの評価対象に対して、調査および評価を行う機関をいう。

申請者は、申請書を認証機関に提出すると同時に評価機関に対して、評価対象の製品を提供する。評価機関において適正な評価が実施され、

基準に対して適合していれば、認証機関より認証が得られ、認証マークの使用が認められる。

図表Ⅱ-2-3-1　認証制度の体制案



2.3　認証内容

本稿における認証制度としては、以下の内容となる。

（１）認証機関

申請者からの認証申請を受理し、指定評価機関に対して評価依頼を行う。評価機関からの評価結果を受け、定められた基準に対する適合性を判定後、対象製品の認証を行う機関。

（２）指定評価機関

認証機関から指定を受けた評価機関であり、対象製品がある定められた基準に適合しているかどうかの評価を行う。

（３）認証表示（マーク）

対象製品が定められた基準に適合していた場合、認証機関から認証マークの使用が認めら、製品のパッケージやカタログ、Web 等での掲載が認められる。

（４）認証の公開（認証製品）

認証機関では、認証した製品については、すべて公開され、利用者側からでも認証製品が容易に確認できるようにする。

（５）認証基準

認証基準は、認証評価委員会にて合理的な認証基準が策定され、認証機関が判定を行う。認証基準は、認証評価委員会にて専門技術者および有識者による合理的な認証基準が策定される。

（６）評価仕様

長期署名検証ツールの評価に必要な評価仕様は、認証評価委員会にて策定される。

（７）認証評価委員会

認証機関は、長期署名検証ツールの評価に適切な技術者および有識者による、評価委員会を招集し、評価仕様および認証基準の策定を行う。

第３章　評価対象

3.1 評価対象の実装形態

検証機能を提供する実装の形態には例えば、次に示すように様々なものが考えられる。

（１）ライブラリ
汎用性の高い検証機能をひとまとめにしたものであり、単体では動作しない。
ライブラリを組み込んだプログラムを作成することで検証機能を提供するツールの形態をとることができる。3.3.2 項で述べるように対象とするライブラリの範囲については検討する必要がある。

（２）パッケージ製品
単体で実行可能なソフトウェア、もしくは、既存のソフトウェアから起動されるアドオンプログラム。
(例 1)長期署名検証コマンドラインツール
(例 2)GUI を備えた長期署名検証アプリケーション
(例 3) PDF などの文書閲覧ソフトウェアから起動される長期署名検証アドオン

（３）ソリューション
業務ごとに構築・カスタマイズされたシステム。既存のライブラリやパッケージ製品を用いて構築されている場合が考えられる。システム全体ではなく長期署名の検証機能を提供するモジュールのみが評価対象になることが考えられる。
(例 1)社内業務システム
(例 2)企業間、もしくは、政府機関や公的機関との取引システム

（４）サービス
ASP や Web サービスなどにより検証機能を提供するサービス。
(例 1)文書保管サービスなどの機能の一つとして検証機能を有するもの
(例 2)利用者に対して長期署名フォーマットの検証機能を提供するサービス

検証機能が全てソフトウェア上で実現される場合もあれば、検証機能の一部がハードウェア上で実現される場合も考えられる。

3.2 検討課題

3.3.1 項のように様々な実装形態があるなかで、評価方法の実現可能性を考慮して、評価対象について検討する必要がある。以下のような課題が考えられる。

◆ 課題１：ライブラリの対象範囲の明確化

【課題】機能提供の範囲がライブラリによって異なるため、評価対象の範囲を明確化する方法が必要である。

【課題の背景】ライブラリの実装によっては、長期署名フォーマットの基本的な構造を解釈するもの、公開鍵による署名値検証や証明書のパス検証を行うものといったプリミティブな機能のものから、長期署名フォーマットの標準に従った一連の検証処理を完結する高度な機能を有するものまで、その機能提供の幅は広い。

ライブラリ単体では動作しないため、実際の評価はライブラリを組み込んだ評価用のサンプルプログラムを実行して実施することになる。ライブラリの機能とサンプルプログラムとの関係について、以下の２つのケースを比較した場合､評価対象の範囲に差が生じてしまうことになる。

(a)プリミティブな機能のライブラリに対して、検証機能の大部分をサンプルプログラム側で構築したケース

(b) 検証機能の大部分を提供する高機能なライブラリに対して､単純なサンプルプログラムで構築したケース

利用者が評価の対象となったライブラリの機能について適切に判断できるように、ライブラリの評価の範囲を明確化する方法を検討しなければならない。

【解決案】例えば、以下のような案が考えられる。

(案 1) 評価に用いたサンプルプログラムのソースコードをライブラリ利用者に対して提供したり、公開することを義務付ける制度とする。ライブラリ利用者はサンプルプログラムを吟味することで評価対象の機能について判断することができるようになる。

(案 2) ライブラリの機能要件や API（関数など）への入出力データの基準を設ける。

◆ 課題２：認証済み製品を用いて実装された製品の扱い

【課題】認証済みの既存製品を構成要素にもつ製品に対して、再度評価を必要とするかどうかなど適切な評価方法を検討する必要がある。

【課題の背景】パッケージ製品、ソリューション、サービスなどは既に認証を受けているライブラリやパッケージ製品などを用いて構築されることも考えられる。このような場合、下位の構成要素が認証済みであ

るからといって、その上位の実装をそのまま認証済みとして扱ってよいというわけではない。認証済み製品の検証機能をそのまま使用している場合もあれば、カスタマイズによって検証機能の重要な機能が失われている可能性もあるからである。例えば、検証時のエラー表示をさせないように構築してしまうケースなどである。

上位の実装に対しても評価を行うことが確実な方法ではあるものの、再度一から評価を必要とした場合には、再評価のために全体的なコストが増えることになる。特にソリューションのように派生物が増えるケースでは再評価のためのコスト増が問題になり、逆に長期署名製品の普及を阻害する要因になってしまうおそれもある。上位の実装に対する効果的な評価方法や制度を検討する必要がある。

【解決案】例えば、以下のような案が考えられる。
(評価方法案 1) 認証済みの製品を構成要素として構築した製品に対しては評価手順をある程度簡略化する。
(評価方法案 2) 評価手順の簡略化などはせずにそのまま上位の実装に対しても通常の評価を行う。評価方法案 1 のように評価手順を簡略化する場合には、評価対象の提供者に評価項目を自己申告してもらう、あるいは、評価機関が評価項目を選定する、などの作業が発生するために、逆にコストが増えてしまう可能性もある。認証済み製品が構成要素であるかどうかは区別することなく、上位の実装に対しても評価を実施するほうが効率的であろうという考え方もある。
(制度案 1) 認証済み製品を構成要素とした製品に対して評価費用での優遇措置を与える制度。

◆ 課題 3 : 製品のバージョンアップへの対応
【課題】製品がバージョンアップした場合の再評価方法を検討する必要がある。

【課題の背景】製品は機能拡張やバグ修正などでバージョンアップしていくことが考えられる。一度、認証を受けた製品でもその後のバージョンアップによって検証機能の内容が変更される可能性もある。製品のバージョンアップが検証機能に影響を与えるものなのかどうか、また、どのような影響を及ぼすものなのかを利用者が判断することは極めて困難である。利用者に混乱を与えぬよう、バージョンアップの修正範囲に関係なくバージョンアップ後の製品に対して再評価を行うことが望ましいが、バージョンアップ頻度の高い製品は再評価のコスト増が問題となることも考えられる。再評価のためのコスト増が問題でバグ修正を避けるなどの状況が発生することは好ましくない。バージョンアップに対して効果的な再評価の方法や制度を検討する必要がある。

【解決案】例えば、以下のような案が考えられる。
（案１）バージョンアップの再評価は新規に評価する場合よりも少ない費用で実施できる、もしくは、ある程度のバージョンアップは無料で再評価できる制度とする。

◆ 課題４：製品に依存した長期署名データ保存形式への対応
【課題】製品依存の長期署名データ保存形式に対応できる評価方法の検討が必要である。

【課題の背景】評価対象が長期署名データをそのままファイルとして入力できる製品であれば、通常のテストベクターによる審査が可能である。しかし、評価対象によっては業務の目的に合わせた長期署名データ保存形式を採用している可能性があり、評価機関が提供するテストベクターをそのまま入力できないこともありえる。例えば、PDF や OOXML(Office Open XML)、ODF(Open Document Format)などの文書フォーマットに長期署名データを格納して保存するケースなどである。将来、新たな文書フォーマットの標準規格として長期署名データの格納方法が定義され、それを実装した製品が登場してくる可能性もある。
また、特にソリューションのようなケースでは、業務上の目的から、独自の方法で保存する可能性も考えられる。例えば、文書データと長期署名データを組にしてまとめてデータ圧縮したファイル形式を入力とする実装などである。
このようなケースに柔軟に対応できる評価方法を検討することや、評価対象とする保存形式を定めていくことが必要である。

【解決案】例えば、以下のような案が考えられる。
（案 1）標準的な文書フォーマットに対しては、そのフォーマットに応じたテストベクターを用意する。新たな文書フォーマットに対応するためには、テストデータ生成ツールの追加開発が必要となる。
（案２）長期署名データの保存形式への対応は評価対象の提供者にまかせる。評価機関は、評価対象の提供者が提示する署名対象データに応じて長期署名データを生成するかたちでテストベクターを提供する。評価対象の提供者が、そのテストベクターを評価対象に入力可能な形式に変換したうえで評価を実施する。
（案３）案２に加え、相互運用性の観点から、製品固有の保存形式を採用している場合には、評価対象の提供者が保存形式の仕様を利用者に提示もしくは公開するようにする。

第４章　評価内容

長期署名検証ツール認証制度における評価内容は、

前章で述べた評価対象の、「対象とする規格」への「対象とする処理」に関する「適合性」

である。以下、「対象とする規格」、「対象とする処理」、及び「適合性」の評価方法等について考え方や課題を記す。

4.1　対象とする規格

対象とする規格は次の２つとする。

- JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル
- JIS X 5093:2008 XML 署名利用電子署名(XAdES)の長期署名プロファイル

これらの規格のオリジナルの規格はそれぞれ、

- ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES) v1.7.3
- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) v1.1.1, v1.2.2 及び v.1.3.2

である。オリジナルの規格は仕様の規定範囲が広く、実用上、過剰または不要と思われる部分があったため、JIS 規格としては「プロファイル」として、実用上必要十分と思われる仕様を規定として定めた。本認証制度では、上記 JIS 規格を対象とするのが適当であると思われる。

ところが、上記 JIS 規格では、署名タイムスタンプ付署名である CAdES-T／XAdES-T 及びアーカイブタイムスタンプ付署名である CAdES-A／XAdES-A のみを規定しており、中間形式である CAdES／XAdES、CAdES-C／XAdES-C、CAdES-X／XAdES-X を規定していない。これらの中間形式のデータが実運用の中で利用されることも考えられるため、本認証制度でこれらの中間形式をどのように扱うかを検討する必要がある。

また、上記 JIS 規格中で「要別途規定」と位置付けられている要素についても、本認証制度でどのように扱うかを検討する必要がある。

4.2 対象とする処理

上記 JIS 規格では､長期署名のデータ形式についてのみ規定しており、その処理については規定していない。関連する処理には、長期署名データの生成処理と検証処理がある。長期署名データを本来の意図を反映して正しく生成することは極めて重要であるが、先に（3.1 節に）示した主旨に基づき、本認証制度では検証処理のみを対象とする。

このとき、検証処理が正しく実施されたことを評価することが必要であることは当然のことであるが、更に、検証結果を表示する処理あるいは表示のために必要なデータを取得することの可能性についての要件が求められることも考えられる。

また、長期署名の検証の適合性を評価するためには、長期署名データフォーマットの整合性や長期署名データに格納される各種データ間の整合性の検証に加え、そこに含まれるよりプリミティブなデータの検証処理の適合性を評価する必要がある。ここで対象とすべきプリミティブなデータには次のデータが含まれると考えられる。

（１）タイムスタンプトークン

長期署名プロファイルの JIS 規格では、タイムスタンプトークンとして RFC3161 に準拠する標準タイムスタンプのみが明記されており、このほかの形式のタイムスタンプについては要別途規定とされている。他の形式のタイムスタンプの扱いについても検討する必要があることも考えられる。

また、RFC3161 も CMS の廃止された規格を引用するなど、陳腐化しつつある。新たな規格も検討されている最中であり、本認証制度を検討する際においても準拠すべき規格として注視していく必要があると思われる。

（２）公開鍵証明書

公開鍵証明書の検証処理については RFC5280 に規定があるため、これに基づいた評価を実施することになると思われる。

（３）属性証明書（TAC）

RFC3161 に基づいて国内でサービスされるほとんどのタイムスタンプ局が発行するタイムスタンプには、時刻配信局(TA)からの時刻監査結果を示す TAC（Time Attribute Certificate : 時刻監査証明書）が属性証明書の形式で格納されている。現在、エンドユーザには TAC の検証を要求されていないが、評価における扱いについて、検討する必要があることも考えられる。

（４）署名値

長期署名のような署名のメッセージ形式に含まれる署名値は、署名に採用するアルゴリズムによって生成や検証の規則が詳細に規定されている。国内で多く利用される署名値の形式には RSASSA-PKCS1-v1_5 があるが、パディングに係る処理を適切に実施しなかったために脆弱性が露見したケースが過去に見られた。これは電子署名の信頼性に影響する重要な部分であり、評価内容としても軽視できないものと思われる。

前記したとおり、3.4.1 項に示した長期署名フォーマットの JIS 規格及びオリジナルの規格では、フォーマットの規定はあるものの、検証処理に関する規定はない。プリミティブとして示したデータのうちタイムスタンプトークンや TAC についても同様である。本認証制度策定に先立ち、これらの検証処理に関する指針(ガイドライン)を文書として明確に示す必要があると思われる。

4.3 評価方法

検証処理が正しく実施されていることを確認するためには、直接ソースコードを解析する方法や、間接的に開発プロセスやその過程で出力される各種ドキュメントを評価する方法が考えられる。また、不正な抜け道がないことや脆弱性がないことを確認するために、アタックテストを実施することも考えられる。しかし、これらの方法は、いずれも要請されるスキルは極めて高く、確認にかかるコストも膨大になることが予想される。

現実的な手段として、テストベクターを利用する方法が考えられる。この方法では例えば、各種の長期署名データをテストベクターとして、またそれらのテストベクターの各値に対して期待される検証処理結果(期待値)を用意し、各種長期署名データを評価対象となる製品に入力し、得られた出力と期待値との一致度合いによって評価結果を決定する。

このとき、テストベクターは非公開とすることが望ましいと思われる。それは、本来必要とされる実装とは別の方法で、テストベクターのみに対して正しい値を出力するような実装が考えられるからである。

評価対象となる製品を評価主体が入手し、評価主体がテストベクターを製品に入力し、出力を確認する方法と、評価対象となる製品のベンダーに対して、期待される出力値を伏せてテストベクターを提供し、出力結果を評価主体が得て評価することによって評価結果を示す方法が考えられる。評価対象となる製品の形態はさまざまであり、テストベクターを製品に入力する手段が必ずしも公開されていたり利用しやすい形で提

供されていなかったりすることが考えられるため、後者の方法が適当であることも考えられる。

テストベクターとしては、単に対象とする規格に準拠した有効な長期署名を提供するだけではなく、次のようなデータを用意する必要があるものと考えられる。

・長期署名データとして有効なデータ／無効なデータ
・必須要素のみを含むデータ／オプション要素を含むデータ
・エラーを引き起こすデータ
・署名やハッシュの各種アルゴリズムで作成された値を含むデータ
・過去・現在・未来にわたる様々な時刻を含むデータ

また、評価結果についても CAdES-T や CAdES-A などの形式ごとに合否を示すのか、オプションや要別途規定と位置付けられた要素のサポート範囲などについてより詳細に示すのか等を検討する必要がある。

4.4 評価用ツール及び環境

テストベクターを利用する方法では、テストベクター及びそれらの検証結果の期待値の適切なセットを用意する必要がある。

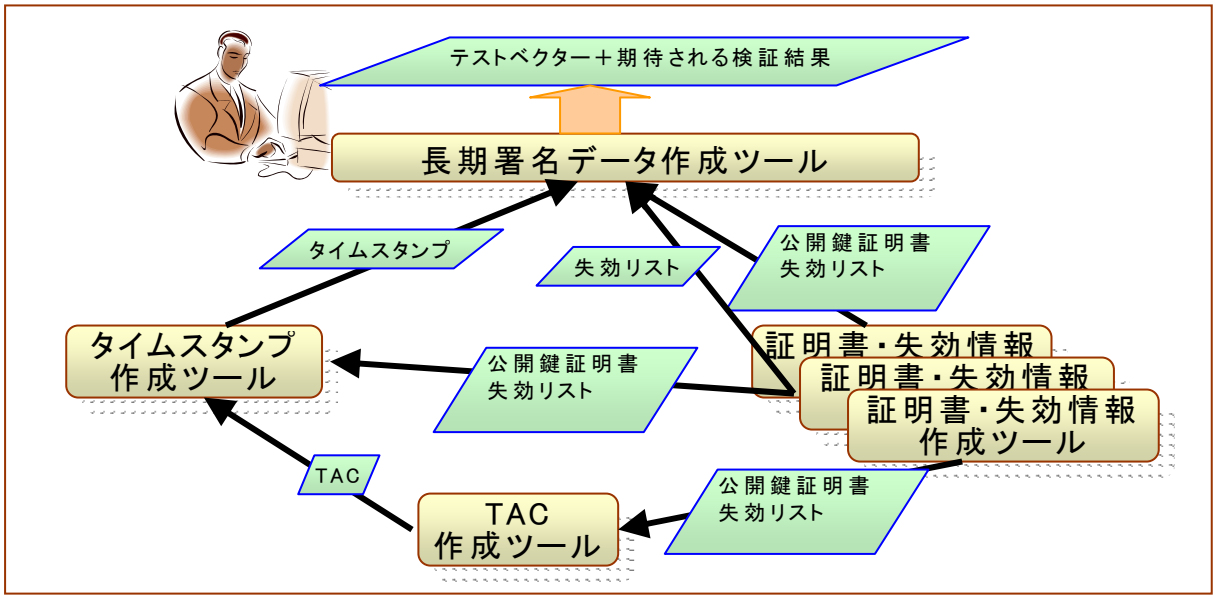
3.4.3 項で示したように､テストベクターには有効なデータでない様々なデータが含まれるため、専用のツールがなければ適切なデータセットを用意することが極めて困難となることが予想される。また、長期署名には 3.4.2 項で示したような様々なプリミティブデータが格納され、しかもそれらのデータ間に密接な関係がある（例えば署名タイムスタンプは署名の中に含まれる署名値を元に生成しなければならない）ので、長期署名やプリミティブデータを生成するツールが独立して存在すればよいというものではなく、それらのツールを連携させた環境が必要になるものと思われる。

必要になると予想される評価用ツールを次に示す。

・各種長期署名データの作成ツール
・各種証明書、失効情報の作成ツール
・各種タイムスタンプの作成ツール
・各種 TAC の作成ツール

そしてこれらを連携させた環境が必要となる。このような環境例を図表Ⅱ-2-3-2 に示す。

図表Ⅱ-2-3-2 評価用データ構築のための環境例



4.5 評価の限界と課題

これまで示したように、テストベクターを用いる方法が評価方法として現実的であると思われるが、テストベクターによる方法には限界がある。テストベクターは有限であり、規格への適合性を完全に確認することはできない。テストベクターの網羅性を高め、適合性をより確実に説明できるようにすることが重要だと思われる。網羅性を示す指標や、網羅性を高めるためのテストベクターの生成方法についての検討が課題となると思われる。

また、テストベクターを用いる方法では、検証ツールに意図的にバックドアが組み込まれていた場合、それを検出することは極めて困難である。この対策としては、ソースコード解析あるいはアタックテストを行うことによってバックドアを検出できるようにするか、評価対象の提供者にバックドアがないことを宣言させ、そのことに信頼を置くことに基づくような制度とするかなどが考えられる。後者の方法が現実的であると考えられるが、そのような制度設計につき、検討する必要があると思われる。

第５章　今後の活動スケジュール（案）

5.1　主な作業項目

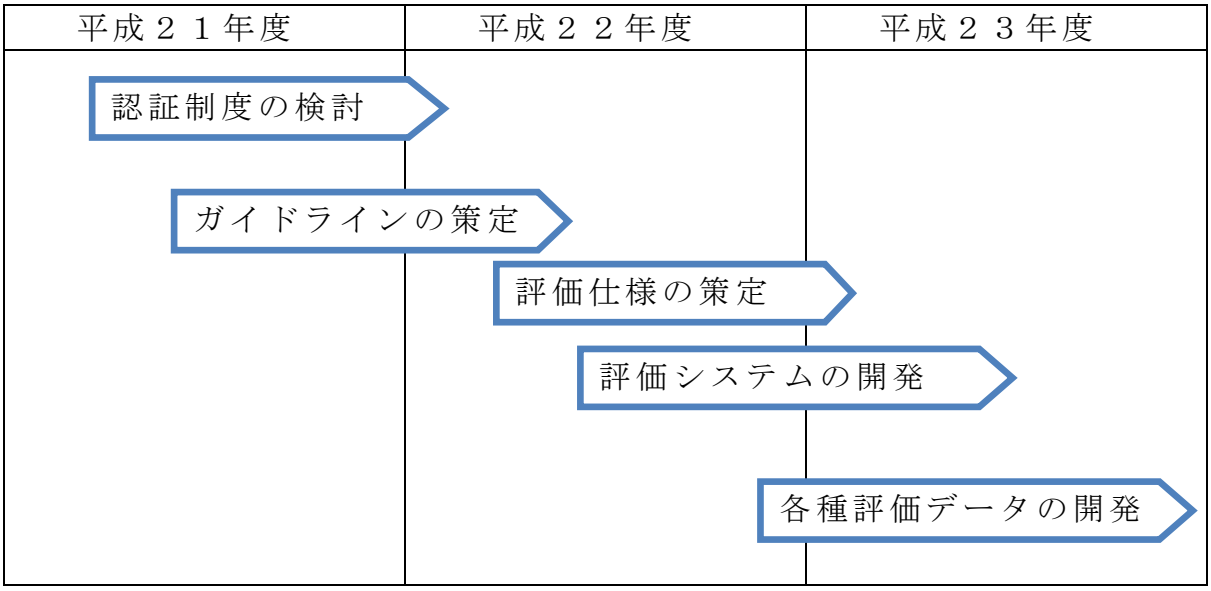
長期署名検証ツール認証制度の実現に向けた、今後の活動としては、以下の項目を検討する必要があると考えられる。

（１）　認証制度の検討
（２）　ガイドラインの策定
（３）　評価仕様の策定
（４）　評価システムの開発
（５）　各種評価データの開発

5.2　作業計画案

検討および開発の作業は以下のように概ね３年の期間が必要と考えられる。

図表Ⅱ-2-3-3　活動スケジュール



長期署名検証ツール認証制度検討会参加者　　（順不同敬称略）

セイコーインスツル株式会社	上畑　正和（主査）
三菱電機株式会社	宮崎　一哉（主査）
セコムトラストシステムズ株式会社	西山　晃
セコム株式会社	佐藤　雅史
株式会社エイベック	本田　雅裕

財団法人 日本データ通信協会
タイムビジネス協議会
〒170-8585 東京都豊島区巣鴨 2-11-1 巣鴨室町ビル
Tel ： 050-5508-1618
E-Mail ： h-ishii@dekyo.or.jp
URL ： http://www.dekyo.or.jp/tbf/