経済産業省委託調査

署名ポリシー調査報告書

電子商取引推進協議会
財団法人日本情報処理開発協会 電子商取引推進センター

←（背表紙）

（表紙）

経済産業省委託調査

平成１５年度ＥＣ技術基盤の相互運用性に関する調査研究事業
（電子署名生成・検証システムのセキュリティ環境の標準化等調査）

署名ポリシー調査
報　告　書

平成１６年３月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

（表紙裏）

この報告書は、平成１５年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「平成１５年度ＥＣ技術基盤の相互運用性に関する調査研究事業（電子署名生成・検証システムのセキュリティ環境の標準化等調査）」の成果を取りまとめたものです。

はじめに

電子文書の利用や保存において、真正性の確保は重要な課題の一つである。デジタル署名は電子文書の真正性を確保するための事実上唯一の標準技術であり、各国でいわゆる電子署名法が制定されることからも分かるように、この技術に対する期待は大きい。

ところが、仕組みの複雑さや、基礎となる暗号技術が持つ限界などから、「誰もが安心して利用できる技術」との認識を広く得られていないことも事実であろう。

署名ポリシーは、署名フォーマットの一部として ETSI（European Telecommunications Standards Institute：欧州電気通信標準化協会）TC-ESI（Technical Committee-Electronic Signatures and Infrastructures）の技術標準として次の文献に定められている。

ETSI TS 101 733 V1.4.0 (2002-09)：Electronic Signature Formats

この標準には、長期署名フォーマットと、そのフォーマットの一部を構成する署名ポリシーとの両者が規定されている。この標準が IETF（The Internet Engineering Task Force）の S/MINE（S/MIME Mail Security）WG に提案される際、長期署名フォーマットと署名ポリシーに分割され、次の２つの標準となっている。

RFC3126：Electronic Signature Formats for long term electronic signatures

RFC3125：Electronic Signature Policies

署名ポリシーは、個々の署名に対して署名の有効性判定の条件や、署名の持つ意味を明記し、技術的に関連付ける仕組みである。また、ETSI の標準が長期署名フォーマットとの組み合わせで提案されていることからもわかるように、これまで認証・公証 WG にて検討してきた電子署名文書の長期保存にとって署名ポリシーが重要な意味を持つであろうことも想像に難くない。署名ポリシーは、署名の利用や署名文書の長期保存に安心感を与え、その結果として、署名の普及に大いに資することが期待される。

本報告書では、署名ポリシーに関して検討が先行していると思われる ETSI の文献の調査及び一部のユースケースの検討を通して、署名ポリシーの概要、期待される効果、課題等について報告する。

平成 16 年３月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目次

図表一覧目次

1．署名ポリシーの概要

署名ポリシーは、署名者と署名の検証者が守るべき一連の規則である。署名ポリシーには OID が割り振られ、一意に特定できる。署名ポリシーの記述には、次の形式がある。

(1) フリーテキスト形式

人間が読んで理解できる形式。署名文書の外部に記述されている場合（明示的な署名ポリシー）と、それ以外の場合（暗黙的な署名ポリシー）とがある。

(2) コンピュータによる処理が可能な形式的記述

コンピュータで解釈し、処理できるような形式で、ASN.１による記述形式と XML による記述形式が提案されている。

署名ポリシーは、署名文書中の個々の署名値毎に与えることができる。一部の記述内容に重複する部分は存在するが､証明書毎にその使用規則を定める証明書ポリシーとは位置付けが異なる。署名ポリシーの識別子は、OID と署名ポリシー記述のハッシュ値で示され、この OID とハッシュ値は、電子文書の内容や署名に付随するいくつかの属性と共に署名の対象となる。このため、署名ポリシーの OID が他の署名ポリシーの OID に摩り替えられたり、署名ポリシーの内容が改ざんされたりした場合には、それらの事実を検知することができる。

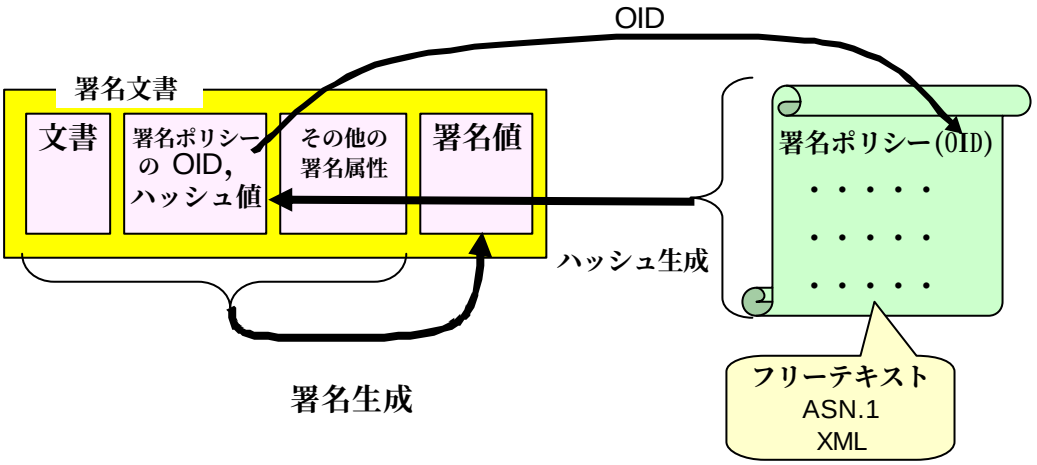


図 1-1 署名と署名ポリシー

署名者は自分の意図と合致する署名ポリシーを取得して署名に含め、検証者は検証処理の一環として署名ポリシーを参照することにより、署名の意味や有効性を確認する。

署名ポリシーには、次に述べるような効果が期待される。

(1) 署名の意図や意味を明示し、電子署名の安全性を強化する。

従来の紙文書に対する手書き署名や押印では、その意味や意図が慣習として暗黙的に合意されているようなケースや、物理的に独立した他の契約書等によって解釈や責任が決まるよ

うなケースがあったが、電子文書においては、そのような慣習は未成熟であり、また多くの背景情報や文脈情報が失われてしまうため、署名により予期せぬ責任が発生してしまうのではないかという不安を抱きがちである。

署名ポリシーは、個々の署名に対して意図や意味を明確に提示することができる。つまり、署名対象の文書やデータに対して単に存在を確認しただけなのか、内容に何らかのコミットしたのか、どのようなコミットをしたのかといった署名者の意図が明確に示されることとなる。また署名者がどのような属性や役割をもって署名したかを記述することも可能(例えば、田中氏がA者の資材課長として発注仕様書に対して署名を添付）である。

このように署名ポリシーを利用することにより、署名に対する意味付けを明確に示し、かつ技術的に検証可能な形で署名データの中に含めることができるため、暗黙的な慣習やアウトオブバンドで交換される契約書に頼ることなく、署名者及び検証者が相互に誤解を生じ難い安全な署名環境を提供することが可能となると思われる。

(2) 署名処理系の汎用利用が可能となる。

従来、複数のPKIベンダが適用領域毎に署名生成／検証用アプリケーションを提供しているが、アプリケーション毎に署名データ形式や署名生成／検証の規則や手順を独自の方法で定義しているため、各APには互換性がなく、汎用性に乏しかった。本来、署名生成／検証処理には高い信頼性が要求されるため、確かな品質を持つ処理系が望まれるが、コスト面を考えると、少数の処理系を多くのアプリケーションで共有できると有利である。

署名ポリシーには、署名生成／検証の規則を定義するために使用されるコンピュータ可読な標準フォーマットが用意されている。各アプリケーションはCMS（Cryptographic Message Syntax: RFC3369）のSignedDataなどの標準化された署名データ形式と署名ポリシーに対応することで互換性を確保し、異なるAPを持つ利用者間における署名データの取り扱いが可能となる。署名ポリシーに対応する署名検証システムの例については３．２で紹介する。

(3) 長期署名の証明力を向上する。

署名の有効性の判定に深刻な影響を与える検証規則や前提条件が署名データと技術的に関連付けられないような契約書や同意書などで定義されている場合、時間の経過に伴い、契約内容の情報そのものや関連付けに関する情報が失われる可能性がある。署名の有効性判定に影響を与えるような情報を署名ポリシーとして記述し、それを署名ポリシー保存局で永続的に保存して、署名ポリシーを特定するための情報を長期署名の形式で署名データと密接に関連付けて保存することにより、長期署名の証明力の向上が期待できる。長期署名検証における署名ポリシーの利用方法について、２章で説明する。

2．長期署名と署名ポリシー

長期署名で利用するアーカイブタイムスタンプを発行する TSA 及びその TSA に証明書を発行する CA の証明書の偽造に関する脆弱性とその対策については H15「電子署名文書長期保存に関する実用化動向」で紹介している。これと同様の脅威であるオリジナル署名向け証明書あるいはその証明書を発行した CA の偽造及び、署名タイムスタンプを発行する TSA 及びその TSA に証明書を発行する CA の偽造に関する脆弱性への対策として署名ポリシーが有効である。

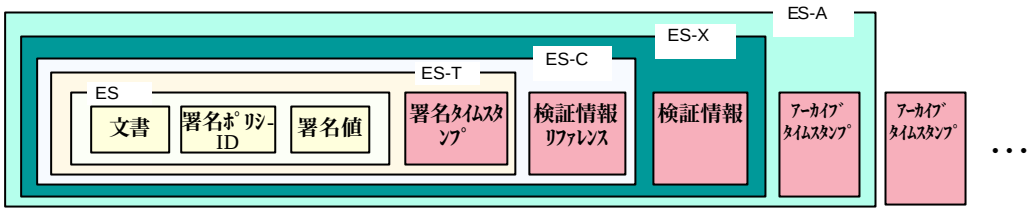


図 2-1 長期署名フォーマット

延長署名の有効性を判定するとき、アーカイブタイムスタンプの検証時には、アーカイブタイムスタンプを発行するTSA及びそのTSAに証明書を発行するCAの偽造に関する脆弱性に対処する必要がある。このためには、アーカイブタイムスタンプのトラストポイント（信頼点）が、正当なものであることを確認するために、「電子署名文書長期保存に関する実用化動向」に示す TSA 向け CA の運用ポリシーに従って CA で永続的に保存されているトラストポイント証明書との照合を行なえばよい。

図 2-2 の例では、元の文書を偽造するために元の署名者及びその CA（CA1）の証明書、署名タイムスタンプ及びその CA（CA2）の証明書、アーカイブタイムスタンプ及びその CA（CA3）の証明書を偽造したケースを示す。文書を書き換え、偽の証明書で署名し、時刻を過去に戻し、偽の署名タイムスタンプと偽のアーカイブタイムスタンプをつけ、外側に正当なアーカイブタイムスタンプを添付する。このようにすると形の上では長期署名は有効であるように見えてしまう。ところが、検証時に有効な外側のアーカイブタイムスタンプが示す時刻に TSA2 の秘密鍵は危殆化していないため、発行者（CA）や所有者の名前まではそっくりと偽造できるが、鍵情報までを偽造することはできない。従って、鍵情報までを含めて過去に利用されたことが保証された証明書と照合を行なうことによって、偽のアーカイブタイムスタンプか否かを判断できる。

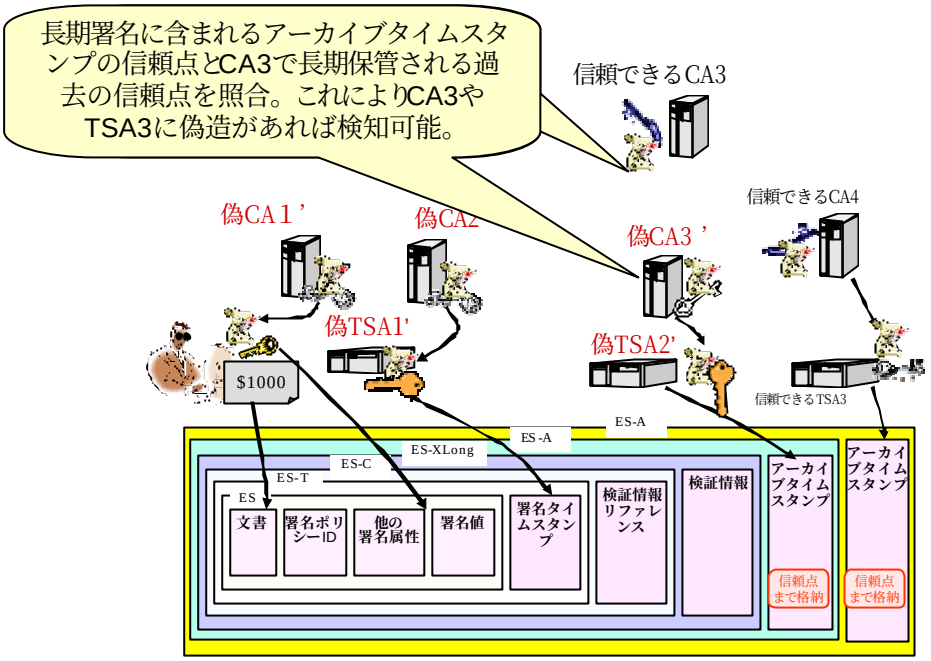


図 2-2 アーカイブタイムスタンプ信頼点の偽造への対処

長期署名全体が真に有効な長期署名であるか、偽造であるかを判断するためには、更に署名タイムスタンプ及びオリジナル署名の検証においても、それぞれの証明書を発行する CA の偽造に対処する必要がある。このためには各トラストポイントの正当性を同様に確認しなければならない。

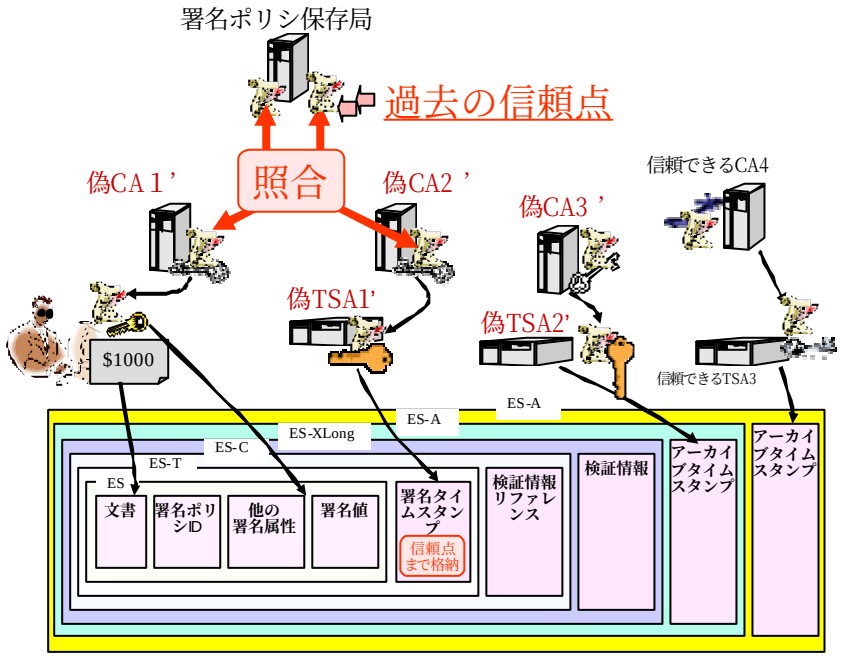


図 2-3 署名及び署名タイムスタンプ信頼点偽造への対処

署名ポリシーには、署名タイムスタンプやオリジナルの署名のトラストポイントに関する情報を記述することができる。また、次章で述べるように、署名ポリシーの保存や公開の仕組みにつ

いての提案もなされている。

署名ポリシー保存局で署名タイムスタンプやオリジナル署名のトラストポイントに関する要件を記述した署名ポリシーを永続的に保存しておき、延長署名に含まれる情報を保存された署名ポリシーと照合を行うことで、上述した偽造に対抗することができる。トラストポイントの保存については、従来、署名の利用されるドメインや AP での運用に任されていたが、署名ポリシーやその保存局を利用することとすれば、ドメインや AP に依存しない統一的な枠組みを与えることができる。

3．署名ポリシーを用いたデジタル署名の生成及び検証

本章では、署名ポリシーを用いたデジタル署名の生成と検証に関わる構成と処理の流れを明らかにした上で、CEN/ISSS WS/E-Sign N 140 “ Procedure for electronic signature verification ” を参考にして、デジタル署名の有効性検証を行う“ 署名検証システム ”を設計する上での要件を整理する。

3.1 構成と処理の流れ

(1) 署名ポリシー発行者（Signature Policy Issuer）

署名ポリシー発行者は、特別なビジネス要求を満たすために、信頼されるサービス提供者としてデジタル署名の生成と検証のための技術上、手続上の要件を定義している署名ポリシーを発行する。

(2) 署名ポリシー公開者（Signature Policy Publisher）

署名ポリシー公開者は、信頼されるサービス提供者として署名ポリシーを公開する。さらに、公開頻度、バージョン、更新と改定の制御、失効などの公開プロセスを管理する。

(3) 署名ポリシー保管者（Signature Policy Archivist）

署名ポリシー保管者は、信頼されるサービス提供者として署名ポリシーのライフサイクル終了後でも署名検証に利用できるように超長期に渡って署名ポリシーを保管する。

(4) 署名者（Signer）

署名者は、署名ポリシーで定義されている規則に従って電子文書に対してデジタル署名を生成する。

(5) 検証者（Verifier）

検証者は、署名ポリシーで定義されている規則に従ってデジタル署名の有効性を検証する。

(6) 仲裁者（Arbitrator）

仲裁者は、署名者・検証者間での紛争を仲裁する。仲裁の際にデジタル署名の再検証を行う場合には検証者としても振舞う。

(7) 信頼されるサービス提供者（TSP：Trusted Service Provider）

信頼されるサービス提供者は、署名者・検証者間の信頼関係構築に貢献する。認証局（CA)、登録局（RA)、リポジトリ、タイムスタンプ局（TSA)、OCSP レスポンダ、属性認証局（AA）などが該当し、各サービスの利用は署名ポリシーによって指定されている。

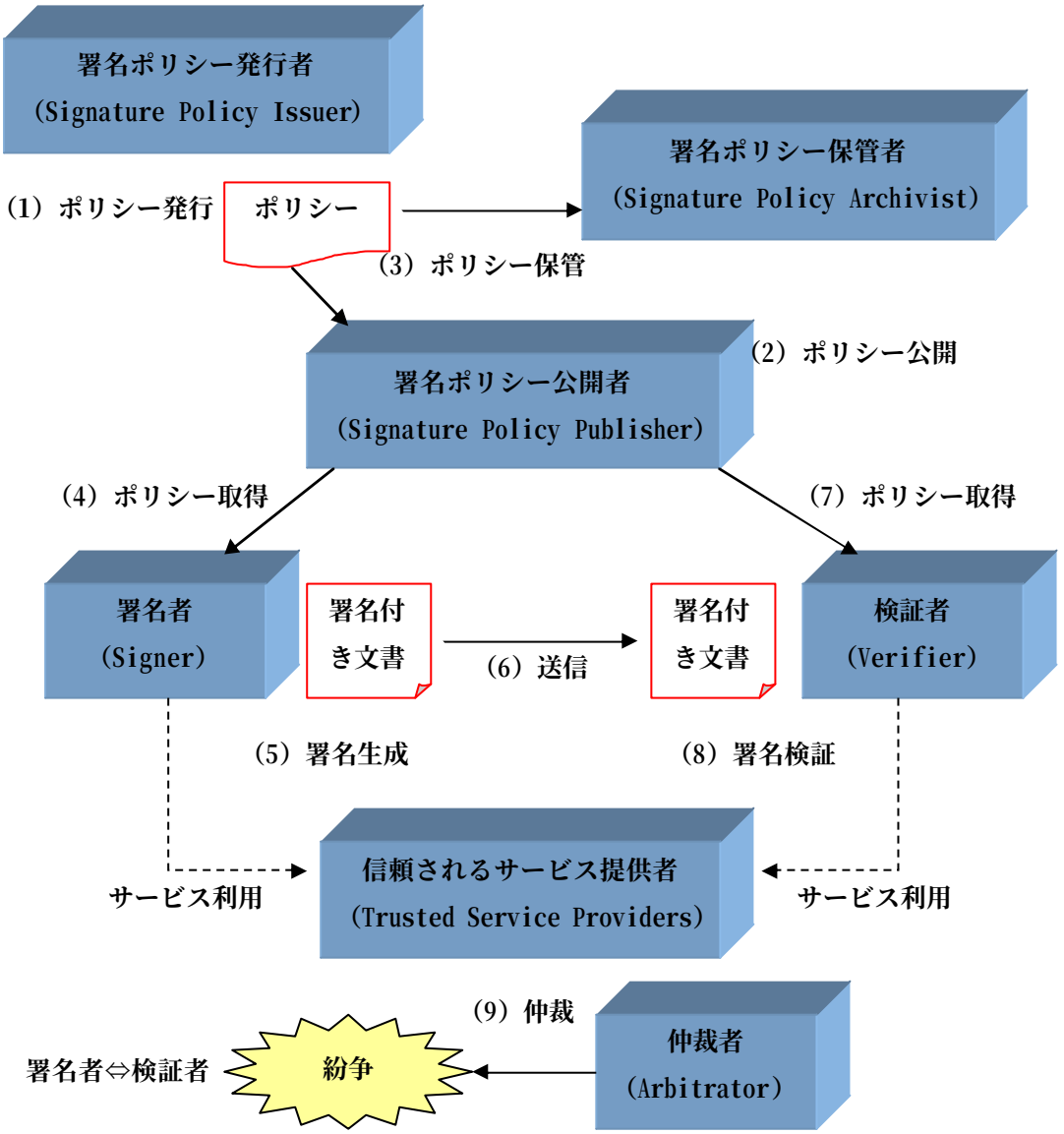


図 3-1 処理の流れ

(1) 署名ポリシー発行者は、署名ポリシーを発行する。
(2) 署名ポリシー公開者は、署名ポリシー発行者から署名ポリシーを入手して公開する。
(3) 署名ポリシー保管者は、署名ポリシー発行者から署名ポリシーを入手して保管する。
(4) 署名者は、署名ポリシー公開者からビジネス要求に適合する署名ポリシーを入手する。
(5) 署名者は、署名ポリシーに記述された規則に従って信頼されるサービス提供者のサービスを利用しながら電子文書に対するデジタル署名を生成する。この際、検証者が検証時に署名ポリシーを識別するための署名ポリシー識別子を含めたデジタル署名を生成する。
(6) 署名者は、検証者に署名付き電子文書を送信する。
(7) 検証者は、署名ポリシー公開者から署名ポリシー識別子に対応する署名ポリシーを入手する。
(8) 検証者は、署名ポリシーに記述された規則に従って信頼されるサービス提供者のサービスを利用しながら電子文書に付与されたデジタル署名を検証する。

(9) 取引後日、署名者と検証者の間で紛争が発生した場合には、仲裁者はデジタル署名の再検証などを行うことによって両者を仲裁する。

3.2 署名検証システム（Signature verification system）

3.2.1 署名検証システム（初回版）

初めてデジタル署名の検証を行う場合に利用する署名検証システムは以下の要素によって構成される。

- 安全な署名検証プロセス
- 署名付き電子文書を入力して検証対象のデジタル署名を選択するための I/F
- 電子文書を提示するための表示系／音声系／動画系の I/F
- 署名ポリシーを提示するための I/F
- 署名検証後に署名者情報および出力ステータスを得るための I/F
- 署名者から提供されなかった情報を TSP（Trusted Service Provider：CA リポジトリ、CRL リポジトリ、OCSP レスポンダ、タイムスタンプ局など）から取得するためのネットワーク I/F
- 追加的な検証データを含む拡張デジタル署名を得るための I/F

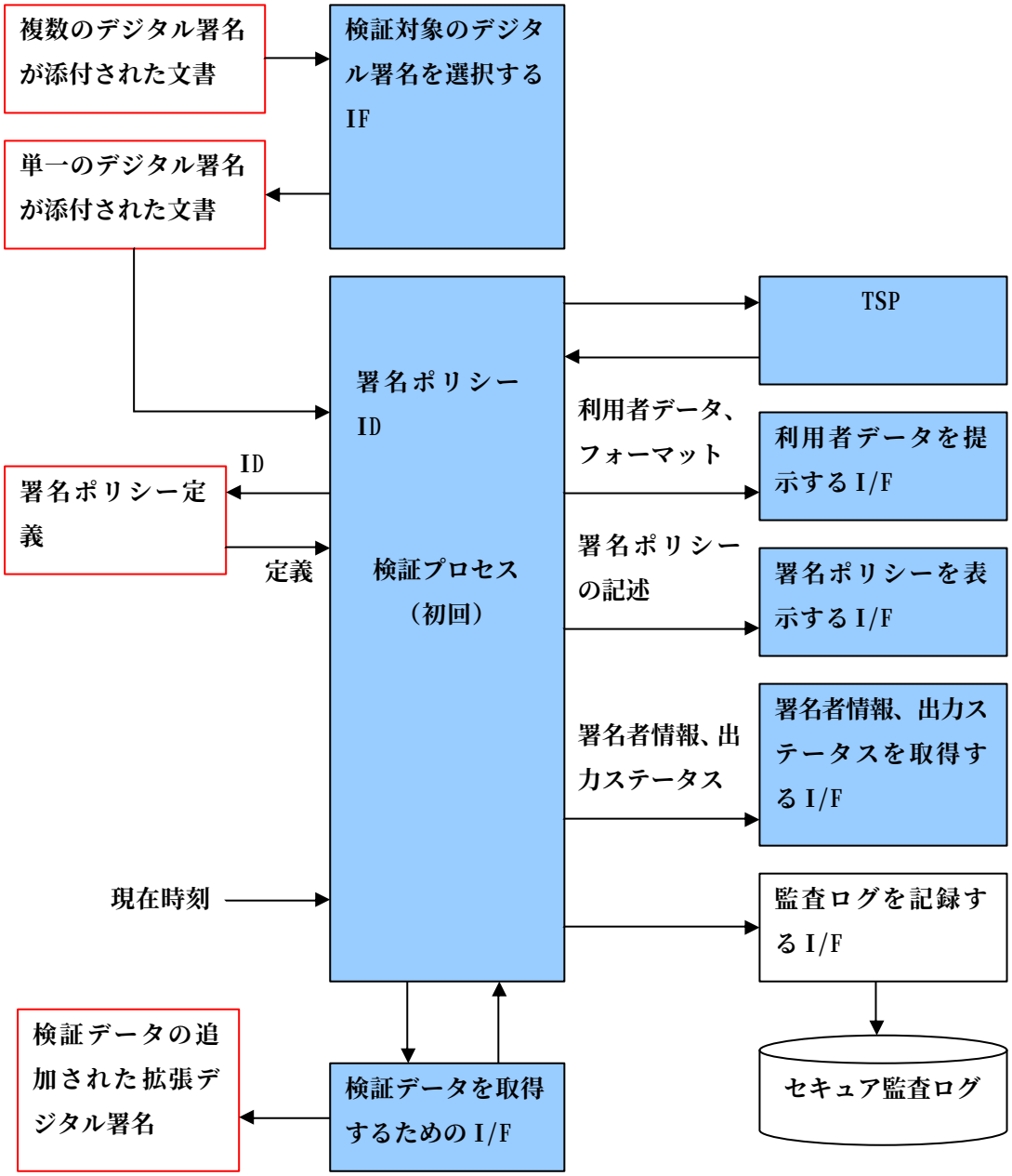


図 3-2 署名検証システム（初回版）

3.2.2 署名検証システム（通常版）

二回目以降にデジタル署名の検証を行う場合に利用する署名検証システムは以下の要素によって構成される。

- 安全な署名検証プロセス
- 署名付き電子文書を入力して検証対象のデジタル署名を選択するための I/F
- 電子文書を提示するための表示系／音声系／動画系の I/F
- 署名ポリシーを表示するための I/F
- 署名検証後に署名者情報および出力ステータスを得るための I/F

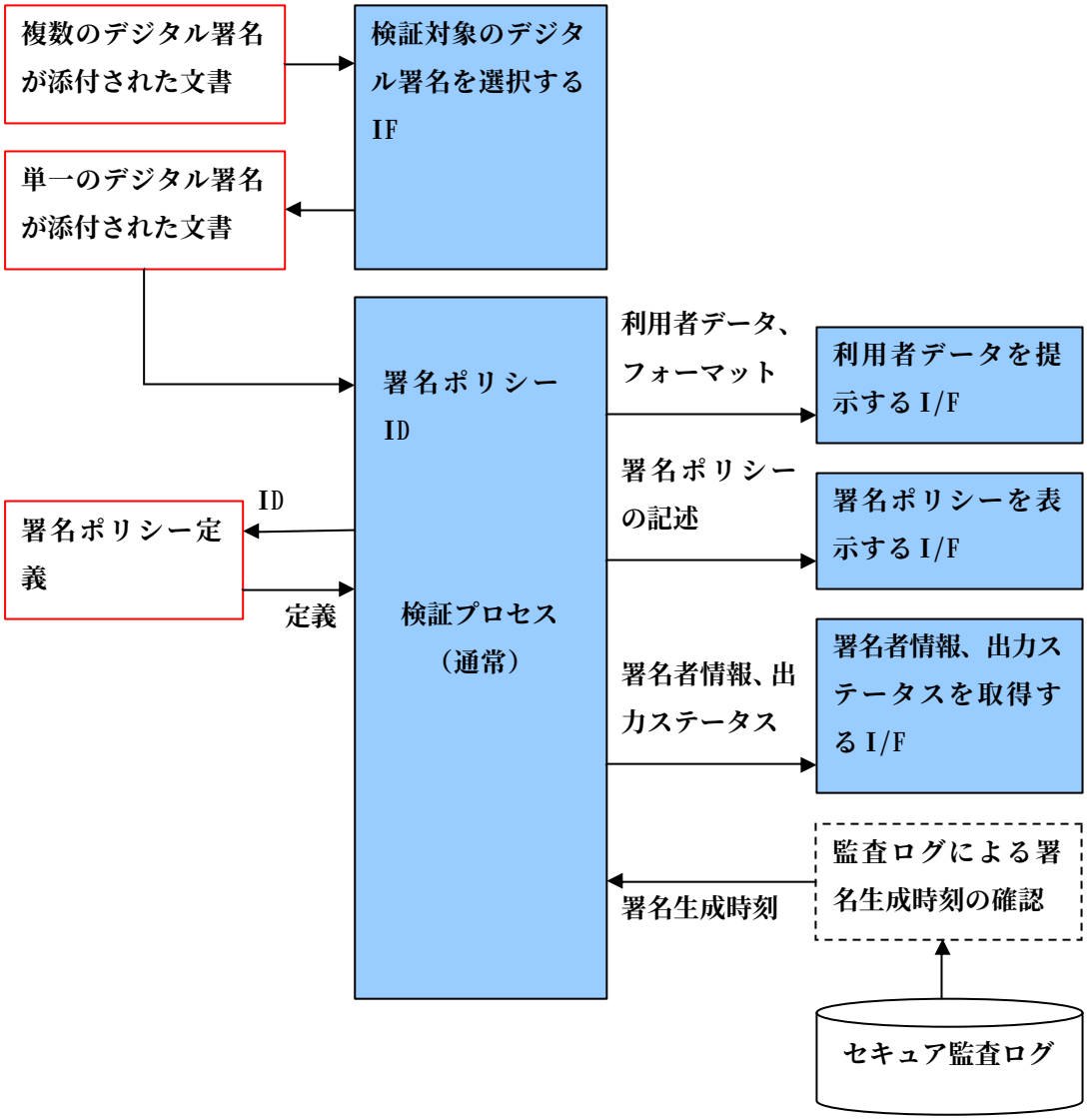


図 3-3 署名検証システム（通常版）

3.2.3 システム要件

(1) 安全な署名検証プロセス

このプロセスでは、デジタル署名に含まれる署名ポリシーIDから署名ポリシーの定義を検索し、その内容に基づいて以下のようなデジタル署名の有効性検証を行う。

- 各種証明書（署名者、CA、TSA、AAなど）の検証
- 署名者署名の検証
- タイムスタンプの検証
- 属性（証明書）の検証
- アルゴリズム制約の検証

もし入力された署名者の文書に検証処理に必要な情報（公開鍵証明書、失効情報など）やタイムスタンプが添付されてなかった場合は、署名検証システムの利用者（※署名検証者）がTSPか

らこれらの情報を入手できなければならない。

署名ポリシーは事前に署名ポリシー公開者から入手してシステム内で管理していたものを利用すればよいが、署名ポリシーIDに該当する署名ポリシーが存在しなかった場合を考慮して、オンラインで署名ポリシー公開者から入手できる手段を持つことが望ましい。

また必要に応じて、初回の署名検証時に監査ログを記録し、二回目以降の署名検証において監査ログを元に署名生成時刻を確認できること。

(2) 署名付き電子文書を入力して検証対象のデジタル署名を選択するためのI/F

署名者の文書には複数のデジタル署名が添付されている場合がある。そのため、利用者が、デジタル署名がいくつ存在しているかを確認し、検証対象のデジタル署名を選択できなければならない。

(3) 電子文書を提示するための表示系／音声系／動画系のI/F

利用者が署名者の文書（テキスト、音声、動画など）の内容を十分に確認するには、文書の内容を適切な方法で提示できるべきである。適切な方法を選び出すためには、データの提示フォーマットが常にデジタル署名の中に指示され、その情報は署名者のデジタル署名によって保護されなければならない。つまり、このI/Fは「提示されるものが署名されるものである」という要件を満たす必要がある。

(4) 署名ポリシーを提示するためのI/F

利用者が、対話的なI/F（例えば、キーボード、マウス、スクリーン）を使用して、署名者の文書が署名ポリシーにて期待される適用分野やデジタル署名への適用条件（例：EU Directiveの5.1節）に関連付いていることを確認できなければならない。

(5) 署名検証後に署名者情報および出力ステータスを得るためのI/F

少なくとも次の署名者情報を提示できるべきである。

- 署名者の公開鍵証明書のDNから抽出した署名者の名前あるいはペンネーム

また、利用者の意志に応じて次の情報も提示できるべきである。

- Qualified Certificateを発行したCSP（認証サービス提供者）の名前と署名者の登録名あるいはペンネーム
- デジタル署名の生成日時

加えて、利用者が対話的なI/Fを使用して次の情報を入手できるべきである。

- 公開鍵証明書（署名者）の他項目の内容
- タイムスタンプの日時
- デジタル署名を生成した場所（location）
- 署名ポリシーの下のコミットメントタイプ
- デジタル署名が生成された際の役割（属性）

利用者が署名ポリシーに従った検証プロセスのステータスを入手できるべきである。出力ステータスは信頼され、ごまかしができない方法で提示されるべきである。初回の署名検証における出力ステータスには次がある。

- 検証完了
- 検証失敗
- 不十分な検証

(6) 署名者から提供されなかった情報を TSP から取得するためのネットワーク I/F

署名検証に利用する公開鍵証明書や失効情報（CRL、OCSP レスポンス）そしてタイムスタンプなどの情報が署名者から提供されなかった場合には、利用者がネットワークを介して TSP から入手できるべきである。

(7) 追加的な検証データを含む拡張デジタル署名を得るための I/F

初回の検証処理の中で署名者から提供された検証情報あるいは TSP から入手した検証情報を拡張デジタル署名に追加することで、二回目以降の検証処理ではこれらの検証情報を利用してデジタル署名の有効性を確認できるようにすべきである。

なお、拡張デジタル署名は前述の長期署名フォーマットを利用することで生成できる。長期署名フォーマットの詳細および利用方法については H14 年度調査（タイムスタンプサービスの利用ガイドライン）を参照して頂きたい。

4．文献調査

署名ポリシーに関する検討は ETSI（欧州電気通信標準化協会）が先行しており、４つの署名ポリシーに関係するレポートが発表されている。ここではこれらの ETSI の文献を調査し、その概要をまとめる。調査対象とした文献は次のとおりである。

(1) ETSI TR 102 041, “Signature Policies Report”, Version 1.1.1, 2002-02
(2) ETSI TR 102 045, “Signature policy for extended business model”, Version 1.1.1, 2003-03
(3) RFC3125, “Electronic Signature Policies”
(4) ETSI TR 102 038, “XML format for signature policies”, Version 1.1.1, 2002-04

ただし(3)は、次の文献：

ETSI TS 101 733, “Electronic Signature Formats”, Version 1.4.0, 2002-09

から署名ポリシーに関する記述のみを抜き出して、IETF に提案された文献であり、今回はこちらを調査対象とした。

4.1 Signature Policies Report

“Signature Policies Report”は、署名ポリシーの技術面、組織面、そして法制度面に関する手引きを与えるものである。この文献が、ETSI TS 101 733,”Electronic Signature Formats” や RFC3125,“Electronic Signature Policies”における署名ポリシー記述仕様のベースとなっている。Annex には、いくつかのユースケースや標準化を更に進めるにあたって考慮すべきポイントが示されており、今後の検討にも大いに参考となる文献である。本文献の要約を資料１に記す。

4.2 Signature policy for extended business model

“Signature policy for extended business model”は、複数の署名を添付するようなビジネスモデルにおける署名ポリシーについて述べている。ETSI TS 101 733,”Electronic Signature Formats”や RFC3125,“Electronic Signature Policies”は、単一の文書に対して複数の署名を添付するようなケースに十分対処できているとはいえない。この文献では、署名ポリシーのコンセプトについて詳述すると共に、この複数署名の問題を提起し、現状の署名ポリシー記述への拡張を提案している。また Annex では多くのユースケースが紹介されている。この文献の要約を資料２に示す。

4.3 Electronic Signature Policies

“Electronic Signature Policies”では、署名ポリシーのコンピュータ処理可能な記述フォーマットを ASN.1 で規定している。要約を資料３に示す。

4.4 XML format for signature policies

“XML format for signature policies”は、署名ポリシーのコンピュータ処理可能な記述フォーマットを XML で規定している。記述内容は RFC3125,“Electronic Signature Policies”で与えられるものとまったく同じであり、ASN.1 による記述を XML による記述にそのまま置き換えた形となっている。したがって本報告書では要約を省略した。

5. 署名ポリシーのユースケース―保険・年金の電子申請システムにおける利用

まだ実装例の無い署名ポリシーが保険・年金の電子申請システムに用いられた場合を想定し、具体的なイメージと効果についてシミュレーションした。

保険・年金の電子申請においては、これらサービスを提供する組織（年金組合等）と契約者（利用者）の間では様々な情報が交わされる。年間数十万件も申請が発生する場合、サービス提供側の受付対応には相当の稼動が発生する。また、添付書類が伴うなどの場合、郵送を併用するケースなどは、申請フローの複雑化を伴うとともに利用者側には時間的な制約を課すなど、申請の完全な電子化が望まれている。

5.1 電子申請と添付文書

申請には、添付文書がつきものだが、保険・年金サービスに必要となる添付文書は自治体や医療機関など、異なる組織による証明文書が必要となる。これら、自治体や医療機関などは、各々独自の PKI ドメインを形成しており、添付文書に付加された署名も各々のドメインによる署名となっており､現在の GPKI では BCA を通じて相互に署名の検証が可能となる基盤が用意されている（図 5-1)。

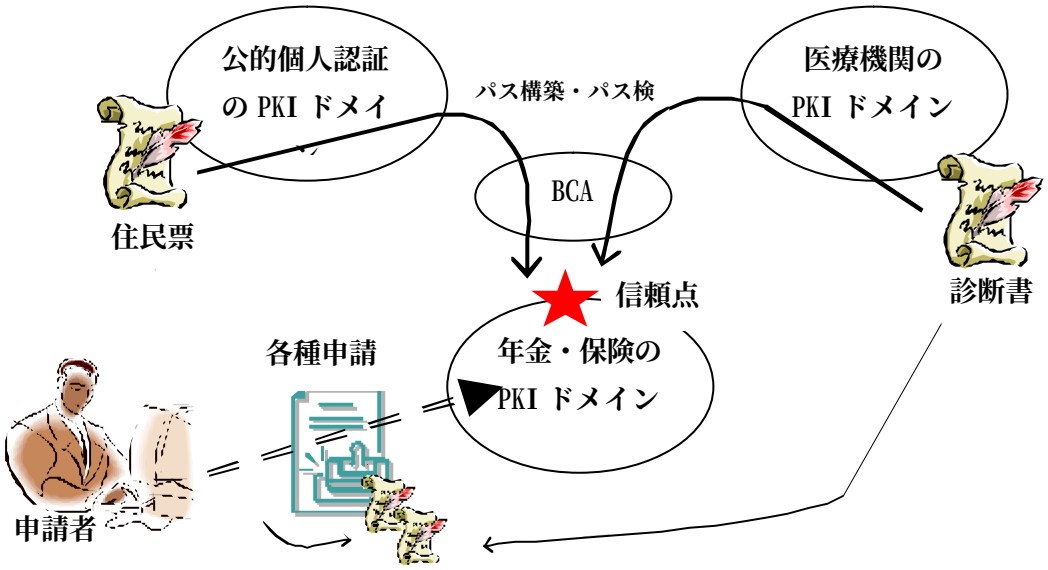


図 5-1 添付書類の署名検証モデル

全ての添付文書が図のモデルであれば問題は無いと考えられるが､BCA に接続されていない PKI ドメインの添付文書を扱うケースや、同じ種類の添付文書であっても PKI ドメインが一つでないなど実際のモデルは複雑な状態になっていることが予想される。

5.2 署名ポリシーの導入

下記は、実在する「ある」年金組合に対する電子申請システムへの利用規模である。

- 組合加入者数：約１１０万人
- 業務数：約１５種類の申請文書の電子化

- 年間件数：電子申請を想定する件数として、年間約８０万件。

このような状況で、財政危機が心配される年金・保険事業において、この規模の申請業務に対応するためには、業務の多くを機械的に行い作業の効率化・コストダウンをはかる必要がある。

しかし、申請文書の本文だけ電子化されても、添付文書が郵送で有効性検証のために「手作業」が残ってしまっては、IT 化投資の意味をなさなくなってしまう場合がある。

署名ポリシーを効果的に導入することで、(1)添付文書も含めた申請の完全電子化、と、(2)定型的な審査業務の自動化、が可能になる。

(1) 添付文書の署名検証時における署名ポリシーの活用

公的個人認証のような全国統一された PKI 環境においては、自治体が発行する証明文書の書面上の形式が異なっていても、PKI は統一されたモデルのため GPKI 経由の証明書検証は可能である。

一方、医療機関については、地域あるいは大学などのグループにより複数の PKI ドメインが、各々独自のポリシーで運営されることが予想される。その場合、ある医療グループの病院で発行された診断書は GPKI 経由の証明書検証が可能であっても、別の医療グループの病院で発行された診断書は、別途信頼点を設定し独自に証明書検証を行わなければならない場合なども想定される。

そのように、同じ「診断書」であっても、証明書検証の方法が異なってしまうと、もはや機械的には検証が不可能となってしまう。

署名ポリシーにより、医療ドメイン毎の署名検証ルールを規定し、双方でこのルールの合意がとれれば、同じ診断書であっても署名ポリシーから検証ルールに応じた署名検証処理が自動化でき、署名の検証が可能となる。これにより「診断書」については電子化された添付文書を用いた申請業務が実現できる。

(2) 添付文書の意味判断を自動化できる署名ポリシーの活用

署名ポリシーには、独自に意味や目的を拡張させることも可能である。この拡張は、予め署名者と検証者の間で合意が形成されていることで、署名の意味や目的を機械的に解釈し、申請フローを自動的に次のフェーズに移行させることが可能となる。

例えば、診断書などは「出生証明書」「死亡診断書」「病気の診断書」など、主に用いられる文書の目的が限定されている。これら文書の目的を署名ポリシーで定めることで、

- 医師が証明書作成時において署名ポリシーから作成権限のある証明文書であるかどうかを自動で判断でき、操作ミス等による証明書の誤発行などを防ぐことができる。
- 申請受領後の審査において、証明資格のある医師による発行であるか、自動的にチェックでき、申請審査業務の効率化がはかれる。
- 証明文書の種類に応じた申請フローへの振り分けが自動で行われ、申請業務の効率化がはかれる。

などが期待できる。

署名ポリシーの効果的な導入により、各種作業の効率化と、人手の作業による誤りなどへの危険性回避が期待できる。

5.3 署名ポリシーの効果

前項までにあげた「作業の効率化」「人為的なミス防止」などは、各々のシステムにおいて簡易な実装による実現も可能と考える。しかし、これをあえて PKI の要素である「署名ポリシー」で実現することで、セキュリティの確保とソフトウェアの拡張性を保つことができる。

署名ポリシーは、署名対象文書同様、署名の対象になる。署名者による署名の意味が安全に検証者に伝わることで、署名ポリシーの判断を機械的に行う際の安全性が確保される。

署名ポリシーは、フリーテキスト形式と電子的処理が可能な形式の二通りがあるが、電子的な形式は RFC3125 のような標準が制定されており、署名ポリシーを判断するソフトウェアの共通化が可能となる。これら署名ポリシーを扱うライブラリのオープンソース化などにより広く共通化を行うことで、PKI を実装したシステムの開発規模削減や、署名ポリシーを判断するロジックの安全性が保たれると考えられる。

6．まとめ

署名ポリシーの有効性や課題について、１章であげた（１）～（３）の期待効果それぞれについて確認する。

(1) 署名の意図や意味を明示し、電子署名の安全性を強化する。

署名の適用分野、コミットメントタイプ、署名者の属性条件などの署名の意味や署名者の条件に関する記述が明示されること、署名者証明書の信頼点やタイムスタンプの信頼点などの条件に関する記述が明示されること、それらの条件が個々の署名に改ざんできない形で関連付けられること、発行、公開、保存などの仕組みが提案されていることなどから、その有効性は期待できる。

ただし、従来、署名者や検証者との間で締結されていた利用者同意書のような契約に置き換えられるだけの内容の記述能力や法的な効力を確保できるのか、それらを確保できるようにするための要件は何か、などについては、法律の専門家などを含めて更なる議論が必要であろうと思われる。

また文献“Signature Policies Report”や“Signature policy for extended business model”で紹介されているユースケースはそのままでは国内の事情に当てはめられないものもあり、有効性を判断するための事例としては十分とはいえない。また５章で紹介した事例についても、概要を示すに留まり、詳細な検討には至っていない。国内におけるユースケースの調査を更に充実させ、署名ポリシーを実際に記述して見るなどの試行を経験し、署名ポリシーの利用や運用における要件を精査していく必要がある。

(2) 署名処理系の汎用利用が可能となる。

署名生成／検証プログラムは本来、極めて高い品質（信頼性、安全性）を要求されるものである。適用分野毎にそれぞれ異なった署名アプリケーションを用意しようとすると、全体として極めて高いコストを要することとなる。

署名ポリシー記述は、フリーテキストの他にコンピュータ処理を可能とするために ASN.1 や XML による記述方法が定義されている。また、これらの記述を解釈して署名検証を実施する処理系に対する提案もある。このような処理系を実装することにより、複数の適用分野に共通して利用できる署名アプリケーションを実現することが期待できる。

ただし、実装例やそれらの利用実績は見られず、その効果は未知の状態である。署名ポリシーの処理を伴う署名生成／検証のための処理系を実装し、それらを各種適用分野において実際に利用してみることにより、その効果の検証を確認する必要がある。

なお、署名の処理系としての品質を保証するような認定制度の導入も検討すべきかもしれない。

(3) 長期署名の証明力を向上する。

署名ポリシーには、署名の有効性を裏付けるための条件が改ざん不可能な形で署名に関連付けて記述できるようになっており、その一部として署名者証明書及び署名タイムスタンプ

の信頼点に関する情報を記述できる。そのことに加えて、署名ポリシーの保存や公開に関する仕組みも提案されており、長期署名の信頼性や証拠としての証明力の向上に結び付けられることが期待できる。

ただし、署名ポリシーの公開や保存の仕組みについての提案はあるものの、長期署名の観点からの要件についてはほとんど議論されていない。何らかの TTP として公開局や保存局を設置すべきなのか、その時の技術要件や運用要件はどのようなものなのか、などなどについて検討する必要がある。

この他、署名ポリシーの決定方法（分野別に定義する、テンプレートを用意する、署名ポリシーに対する認定制度を設けるなど)､コミットメントタイプの洗い出しや個々のコミットメントタイプに対する共通認識の形成、複数署名への対処、OID の割り当て方法、その他、多くの検討すべき課題が残される。文書の電子化の促進に結びつくデジタル署名の普及にとって、大きな効果が期待されるだけに、課題解決に向けた検討を今後更に行うべきであろう。

資料１

ETSI TR 102 041,“Signature Policies Report”, Version 1.1.1, 2002-02

原文において、次に示す章の要約を記す。ただし、Annex C は RFC3125 と内容が同じため省略した。

原文	要約
4 Signature policy definition and scope	4 署名ポリシーの定義と適用範囲
5 Signature policy context	5 署名ポリシー要旨
6 Signature policy issuer	6 署名ポリシー発行者
7 Signature policy user	7 署名ポリシーユーザ
8 Signature policy content	8 署名ポリシーの内容
9 Signature policy usage	9 署名ポリシーの利用法
10 Legal aspects	10 法的側面
11 Conclusion	11 結論
Annex A: Signature policy in electronic transactions	Annex A:電子取引における署名ポリシー
Annex B: Recommendations for standardization work	Annex B:標準化活動のための助言
Annex C: Signature policy in an informal free text form	RFC3125 と同等であるため省略

4．署名ポリシーの定義と適用範囲

電子商取引において、電子署名の有効性とビジネス上の契約で定められた条件が必要である。そのような条件やルールは、署名ポリシーと呼ばれるポリシードキュメントのなかで起草される。

署名ポリシーは電子署名を作成し、有効にするルールのセットである。
署名ポリシーは、ASN.1 フォーマットでも、フリーのテキストで記述されてもよい。
署名ポリシーは、電子署名の適用範囲と使用法を記述する。

PKI において署名ポリシーは、与えられた状況下で電子署名の使用方法の条件を定義している。

5．署名ポリシー要旨

5.1　トランザクション context

署名ポリシーがトランザクションと関連する要求を示している場合、そのような形式を要求する特定の署名ポリシーの要素と結びつける必要がある。

トランザクションの内容は、商用、行政、機密内容、または、その組み合わせを含んでいてもよい。トランザクションの内容は、署名方法に関連した一般的に適用可能な規則を決定している。

署名の正当性や、署名の使用方法を承認する状況を問い合わせるトランザクションの内容は、署名ポリシーの中に含むことができる。

5.2　PKI 中でのトランザクション

PKI において署名者がデータに電子署名をする場合、署名者は電子署名に特別な意味を持たせる必要がある。電子署名が特定の意味を持っている場合、署名者は、署名の中に署名が遂行されたことを示す表示を含む必要がある。

そのような表示として、署名ポリシーは、関わっている団体を含む第 3 者へ示し、一般に使用されている規則や条件の通知を行う。

- 署名者が、どの署名ポリシーを適用するかは、ユニークな数値で署名ポリシーで示されており、それは電子署名で保護されている。
- ある情報（例えばドキュメント）が、与えられた署名ポリシーで署名されたデータのセマンティクスとの関連を許された他の箇所で利用可能とするためには、トランザクションのセマンティクスを認識する必要がある。この関係を構築するために以下の 2 つの方法がある。

- ✓ 与えられた署名ポリシーのために示すべきドキュメント（その署名ポリシーの下で規定されたトランザクションの形式）
- ✓ 与えられたトランザクションの形式のために適用可能な署名ポリシーを示すドキュメント

5.2.1 閉じた環境での署名ポリシー

閉じた環境での PKI は、しばしば閉じた取引関係の中で使用される。

閉じた環境において、処理を行うグループは、署名ポリシーの受理内容や状況に対して厳格な管理を行い、合意のどのような条件も形式化することができる。

5.2.2 オープンな環境での署名ポリシー

オープンな環境の下で取り決められた署名ポリシーは、法律によって定められた特定の条件を満たしているのでなければ、意図したトランザクションに対して内容や一貫性、適合性を吟味しなければならない。

署名ポリシーによって、オープンなネットワークのトランザクションを行うグループは、拘束力のある電子署名を行っている条件の通知を提供することが可能となる。

5.3 署名ポリシーのタイプ

- 唯一人の署名者を含むトランザクションの署名ポリシーは、個々の署名者が有効か否かを示す。
- 複数署名の署名ポリシーにおいては、署名データと同様に処理する団体に身元の立証が要求される。

5.4 署名ポリシー vs. 証明書ポリシー

ポリシーが電子商取引の運用上の条件を示す方法であるとともに、署名ポリシーは、証明書ポリシーのような他のタイプのポリシーとの相違を示さなければならない。

署名ポリシーは、証明書ポリシーをそのポリシーの下で受理可能かどうかを示すという規則を含んでいる。証明書ポリシーが署名ポリシーに対応したとき、署名ポリシーと証明書ポリシーは互いに参照するかもしれない。

6. 署名ポリシー発行者

署名ポリシーを発行できる団体は、以下のものである。

- 法人。
- 専門の職務の下で行動する自然人（公証人や専門家など）。これらの人物は、専門の領域内で

行動する場合、電子署名によって拘束できる条件を設定する。

7．署名ポリシーユーザ

7.1　署名者

署名者が電子署名の用途の主な責任を負うように、トランザクション中の署名の用途を形式化する署名ポリシーに影響力がある。署名者は、ビジネスでの特定のトランザクションに当てはまる署名条件の情報を提供する責任がある。

電子署名のための 2 つのタイプの役割がある。

- 要求される役割は、ある役割でのトランザクションを始める署名者のステートメントを含んでいる。（この役割は、例えば署名者が消費者、取引団体などの役割をしたか否かを決定するために法律上重要になるかもしれない。）
- 証明される役割は、署名時に署名者が指定の役割を持っていたことを証明するために情報を持っている。

7.2　証明者

証明者は、署名されたドキュメントをコントロールする団体、または、トランザクションの受給者である。証明者は、署名者によって行使されたポリシーが、自身のビジネス・ニーズに適切であることを確認しなければならない。証明者は、署名ポリシーの信頼性と内容を有効にしなければならない。

証明者の目的は、署名ポリシーの信頼性を確実にし、トランザクションを受理するか否かを判断することである。

8．署名ポリシーの内容

署名ポリシは、特定のビジネスのニーズを満たすように、署名の生成・検証に関する技術的・手続き的要件を明確にするものである。

8.1　署名ポリシーのフォーマット要件

署名ポリシーは、トランザクションの背景と内容を確実に適用可能にするために署名者によって選択されなければならない。
検証者が署名データを受け取った時は、署名者の選択した署名ポリシーを直接的・間接的に確認できるようにすべきである。
署名ポリシーが提示された時は、再度人間が判読可能な形式でなければならない。
デジタル署名の時は、適切な署名ポリシーに対するチェックやすべての条件を検証することができる。

すなわち、署名ポリシーは 2 つの形式で存在しなければならない：
・人間によって理解される形式。
・機械によって処理することができる形式。

8.2 一般的な署名ポリシー情報

法的あるいは契約内容が示す多数の承認は、署名ポリシーと同様の要求に応じている。

署名ポリシー発行者名:
署名ポリシーの発行責任がある組織体の識別子。
これはポリシーが信頼できるかどうかを決断するために署名者か検証者によって使用されるかもしれない。署名者/検証者は、識別された発行者の署名ポリシーなのかを立証するものとする。

署名ポリシー識別子：
署名ポリシーは、識別子によって身元を確認できるものとする。

署名期間：
署名ポリシーが電子署名を生成するために使用されてもよい期間を表す。
開始日時、オプションとして終了日時。

発行日：
署名ポリシがいつ発行されたのかを表す。（オプション）

適用分野：
署名ポリシーが使用される一般的／法的／契約／において適用される背景と、電子署名が適用される特定の目的。

8.3 署名検証

受取人は署名されたドキュメントを受取次第、受け取る以前から、トランザクションの前後以内に収まることを要求する。署名を有効にする当事者は、デジタル署名の検証と署名検証情報を含んでいる情報を収集する。署名ポリシーの有効性検証は、受取人が署名されたデータを受け取った時点に行う。

8.3.1 署名検証ポリシー

電子署名上の技術的に意味する署名ポリシーは、すべての検証データを備えた「署名検証ポリシー」と呼ばれる。署名検証ポリシーは、署名を有効にする規則を指定する。

署名ポリシーは、次のように分割されるかもしれない:

・すべてのコミットメント・タイプに共通の規則。（共通規則）
・いくつかのコミットメント・タイプに特有の規則。（コミットメント規則）

署名検証ポリシーは次の言葉で記述される:
・すべてのコミットメント・タイプに共通の規則を定義する共通規則のセット。これらの規則は、電子署名に含まれているかもしれない属性上の任意の制約と共に、証明書、タイムスタンプおよび属性の信頼条件として定義される。

・与えられたコミットメント・タイプのための、コミットメント規則のセット。それは、電子署名に含まれているかもしれない属性上の任意の制約と共に、証明書、タイムスタンプおよび属性の信頼条件として定義される。

8.3.2 署名検証情報

署名検証情報は、共通規則あるいはコミットメント規則に含むことができる。ただし、それらは互いに矛盾してはならない。

署名有効性検証情報は次のものを含む:
・認証局の使用に関する規則（すなわち認証パス要件）
・ユーザ証明書に対して適用される規則
・証明書が有効だった期間にデジタル署名が生成されたことを確かめるための規則
・警告期間の規則
・失効ステータス情報の使用のための規則
・認証局キーの危殆化および暗号の弱体化を防止するための規則
・署名者の使用する環境に対して関係のある規則
・署名者によって提供される／検証者によって収集される署名検証データ
・署名アルゴリズムおよび鍵長の任意の制約
・役割の使用のための規則
・証明書チェーンの要件

エンドエンティティ証明書の特定の要件
エンドエンティティ証明書に対してのみ当てはまる要件。
例えば、エンドエンティティ証明書は特定の拡張を含んでいなければならない。
例として、証明書がクオリファイド証明書であるかをチェックするために 2 つの方法がある。
・証明書ポリシーの OID が特定の値を含む
・QC ステートメント拡張が存在し、特定の値を含む

タイムスタンプまたはタイムマーキング要件
タイムスタンプあるいはタイムマークの要件。
もし署名値と署名されたデータのハッシュが、証明書の公開暗号キーを使用して検証され、さ

らに下記の条件が両方とも満たされるなら、署名が証明書の有効期間内に生成されたことが証明される。

・タイムスタンプあるいはタイムマークは、証明書の有効期間の終了前に適用された。
・万一その証明書が無効になった場合、タイムスタンプあるいはタイムマークは証明書の取り消し期日の前に適用されていた。

警告期間に関する規則

失効リスト発行の前に署名データの有効性が検証されないよう、（タイムスタンプまたはタイムマークによって得られる）署名時間の後、どれだけ時間が経過した後に署名が有効となるかを示す期間。すなわち、いつ取り消しステータス情報を取って来なければならないかという時間的要件である。

（タイムスタンプあるいはタイムマークされた時間に利用可能だった取り消しステータス情報は使用しない。）

この時刻を経過する前の署名は、条件付きで有効であると考えることができる。一度この時刻が経過し、かつ注意期間の終了時点のステータス情報が、認証パスの証明書のどれも無効にされていないことを示す場合、その署名は有効であると考えられる。

失効要件

失効情報は、CRL、デルタ-CRL あるいは OCSP レスポンスによって得られる。

証明書失効要件は､エンドエンティティ証明書のチェックと CA 証明書のチェックの両方で指定される。

・すべての CRL（またはすべての認証局失効リスト）が収集されていなければいけない。
・OCSP レスポンスが収集されていなければいけない。
・デルタ CRL と、関連のあるすべての CRL（またはすべての認証局失効リスト）が収集されていなければいけない。

失効のチェックは、一旦注意期間が終わってから行なわれるものとする。

認証機関の鍵の危殆化と脆弱暗号に対する保護

署名されたデータに適用された暗号処理が暗号技術の進歩により、危殆化する恐れが発生した場合は、さらなる有効性検証のために、より多くの情報収集が必要になるかもしれない。そのような情報は、タイムスタンプトークンのような追加の署名を含む必要があるかもしれない。また、署名されたデータやその他集めたデータに対しても、より強いアルゴリズムを使用して保護しなければならない。

署名者の使用環境

署名者は、署名を生成するために特定の環境を使用することが要求されるかもしれない。

例）SCCD（安全な署名生成装置）の使用

署名システムが公の環境にあるか、個人の環境であるか（例えば家のコンピューター、ラップ

トップ・コンピューターあるいは PDA）でも、規則は異なるかもしれない。

署名者によって提供される／検証者の収集する検証データ
署名者は、署名されたメッセージに対して証明書を付与したり、タイムスタンプを提供したりするなど、検証者（※原文では、署名者となっているが、検証者と思われる）に役立つ情報を提供することが要求されるかもしれない。

・署名アルゴリズムおよび鍵長の制約
・特定のアルゴリズムおよび鍵長要求の可能性

役割の使用に関する規則
請求役割あるいは認証役割の要求の可能性。

8.4 署名ポリシーの識別

識別参照は、他から与えられたビジネス背景と署名ポリシーを識別するために必要である。

ここで、OID や URL 等の参照だけでは、署名ポリシーの記述が正しいものであるかを確かめることができない。適切な参照は署名ポリシー識別子、ハッシュ・アルゴリズム識別子およびハッシュ値からなる。

8.5 署名ポリシーの発行

署名ポリシーは安全な WWW サイトで発行されるか、あるいは確実に利用可能である。
署名ポリシーの発行は、ポリシー発行者あるいはサードパーティーによって、信頼されたドキュメントリポジトリサービスによって行うことができる。

ユーザのコミュニティーが署名ポリシーを適用する場合、署名ポリシーは公表され、ユーザが利用できなければならない。また、情報の源が信頼されるものであるとともに、それを確証する方法が利用できなければならない。
署名ポリシー発行局は、署名ポリシー発行者によって直接運営されるか、あるいは異なる組織によって運営されるかもしれない。

8.6 署名ポリシーの保管

ユーザのコミュニティーが、(署名ポリシーの有効期間終了後）与えられたポリシーの配下で生成された電子署名の検証を行いたい場合、署名ポリシーは保管しなければならない。その時以後、ポリシーを発行したポリシー発行者が消滅する可能性があるため、この役割は、独立した公平な条件の下で運営される異なる組織によって行われるべきである。
例）公的にアクセス可能なドキュメントのリポジトリ

8.7 署名ポリシー機関

署名者は、使用している署名ポリシーが実際にポリシー機関によって公開されたものであることを確認することが重要である。

ポリシーは信頼されたリポジトリから得られるかもしれないし、あるいは信頼されていないリポジトリで公開されるかもしれない。一度でも確かな保証が得られているなら、ハッシュ値を計算することでポリシー以上に確実に使用できる。

9. 署名ポリシーの利用法

9.1 署名者による署名ポリシーの利用法

署名ポリシーの利用法として、署名ポリシーのリファレンスを利用する場合、署名者は、署名ポリシーの識別子、および署名ポリシーに記載されているハッシュ値と、そのハッシュアルゴリズムの識別子を引用することのみ要求される。争いの際には、使用されている署名が明確なものであると連想する過程において、それを支持する証拠として利用することができる。

署名ポリシーの明示的なリファレンスを利用しない場合、署名者は、署名したドキュメントのストラクチャーもしくはセマンティックがきちんと定義されていること、このストラクチャーもしくはセマンティックが（署名ポリシー識別子、ハッシュアルゴリズム識別子およびハッシュ値により）署名ポリシーで参照できること、またはストラクチャーが署名ポリシーを参照していることを確認しなければならない。

署名者は、署名ポリシーを明確に参照すること、もしくは、out-of-band で与えられた追加情報や、明確なセキュリティポリシーを使用すべきという指示を追加することによって、署名ポリシーの利用法に関しての同意を示すことになる。

9.2 検証者により署名ポリシーの利用法

デジタル署名を検証する際、検証者は以下の手順を踏むことが要求される。:

- 署名データから、もしくはリンクを張った他ドキュメントから、署名ポリシーのリファレンスを得る。
- 署名ポリシーをコピーする。
- 手に入れた署名ポリシーのハッシュと、使用された署名ポリシーのハッシュを比較する。
- 署名ポリシーが取引の目的に合致していることを確認する。

署名ポリシーを利用した検証者は、その署名ポリシーのもとで検証されたデジタル署名を受理することで、署名ポリシーの利用法に関して同意を示すことになる。

9.3 従うべき条件

署名者も検証者も、明示的もしくは暗黙による単一の署名ポリシーに従うことで、電子署名を処理することができるだろう。

署名ポリシーは、その実施要件に関して、あらゆる曖昧表現を回避するため、十分に明確に定義するものである。電子署名が受け入れられるべき状況では、絶対的に明らかであるべきものである。

9.4 組織における署名ポリシーの利用法

組織的な取引においては、下記のような署名ポリシー利用形態を含む場合がある。

- 組織内部（組織の中において）
  購買に関する署名ポリシーの典型的な例では、署名組織に関係する役割を含むことがある。（例：購買担当　会計係　等）

- 組織外部（複数組織間で）
  組織間での購買に関する署名ポリシーの典型的な例では、署名組織と検証組織において関連する役割と属性を含むことがある。

9.5 利用の同意

署名ポリシーの利用者は、その利用方法に関して同意を示すことが求められる。同意は、実施規則といった、適切な契約上もしくはその他の取り決めによって、表現することができる。また、特定の取引において、発行者と署名ポリシーの拘束的な性質を理解しているユーザーとの間で、契約によって同意を示すことも可能である。

9.6 明示的なリファレンス

確かな署名ポリシーのリファレンスは、契約合意のための特定の必要条件に置き換えることができる。例えば、電子署名の生成と検証に関する必要条件が満たされれば、最終通知が電子データで送られてくることにも合意することができる。明示的な署名ポリシーを参照することで、取引の形式的な要件への固執を緩和する。

あるビジネス領域を代表する組織は、ビジネスにおいて明示的に参照するために、彼ら独自のビジネスニーズに従った署名ポリシーを個別に作成することもできる。このような署名ポリシーは、組織のメンバーすべてが明確に参照できるように発行され、そのビジネス領域に属する、同意したすべての取引相手に忠実に利用される。

例えば、ポリシー関連の PKI の情報は、ICC の ICC　ETERMS スキームを通じて公開されている。ICC では、ウェブサイトでビジネス用語の追加的公開を提供している。その仕組みの強みの一つとして、最新ストレージへの定期的な更新と、ICC サーバもしくは発行者のサーバ上の情報へユーザーがアクセスできる仕組みがある。

9.7 暗黙のリファレンス

ビジネス領域のメンバーが、明確な署名ポリシーに固執する場合は、契約相手がこの署名ポリシーに従い、メンバーから他の方法による表明がなければ、メンバー間での取引は有効であると考えられる。

反対する意思表明がない場合、署名ポリシーは暗黙のリファレンスが用いられるため、取引関係者は彼らの通常の取引のやり方にこだわるものと考えられる。

10.法的側面

10.1 署名ポリシーにおける法的側面

Directive 1999/93/EC[4]の 6 条では、次のように述べられている。

”加盟国および欧州委員会は、消費者の利益のためおよび AnnexⅣにおけるⅣにおける推奨に照らし合わせ、署名検証デバイスの開発と使用を促進するため、相互に協力する。”

電子署名の幅広い適用において、Directive はサービスのエンドユーザに有用となりうる、すべての電子署名をサポートした部品の利用を命じている。なかでも署名ポリシーは、信頼性を高め、署名者の本人性の検証をサポートする仕組みと考えられている。

署名ポリシーは、手書き署名と同等とみなされる電子署名の検証に必要である。Directive1999/93EC[4]の 5. 1 条によれば、

”加盟国は署名が電子形式であること、特定証明書（Qualified Certificate）を使用していないこと、信用された認証局によって発行された証明書でないこと、といったような理由だけでは、電子署名の法的効果、有効性、強制力は否定されないことを保証する。”

署名ポリシーを利用することで、取引関係者は署名の意図や署名に関連する相互の形式等に関して、充分な証拠を収集することができる。

5(1)条： 適格な電子署名

同様のことが、適格な電子署名についても言える。Directive の 2（2）条で定義されている”高度電子署名（advanced electronic signature)”の要件を満たすことを徹底しようとする署名ポリシーが多くあるかもしれない。

”高度”であることは、その電子署名が適格なものであることに必要な Criteria の一つである。適格な電子署名のみが、5(2)条における、強い法的効果をもつと評価される。

5(2)条： 適格でない電子署名

The Council Directive 1999/93/EC[4]は、5(2)条において、署名が適格なものでないこと、電子的形式であること、といった理由では、電子署名はその法的効果を否定されない、と述べている。特にすべての電子署名は、ある基準を満たしていようといまいと、その有効性が検証されれば、法的効果を有する、ということである。つまり、ヨーロッパの加盟国は、電子署名が有効である明確な署名ポリシーの利用を、通常は要求されない。

したがって、公的機関によって明らかにされている標準でさえも、一般的には拘束力はない。ある標準を満たしているものでも満たしていないものでも、インターネットユーザは自由に署名ポリシーを選ぶことができる。そのような署名は、基準に従った電子署名と同等のセキュリティ

レベルを実証できれば、それと同等の法的効果が与えられなければならない。

10.2 リファレンスによる署名ポリシーの導入

The American Bar Association[3]は、”以下のような手段により、”あるメッセージを他のメッセージの一部とすること”として、リファレンスによる導入を定義している：

- 導入されたメッセージを識別すること
- 受け手が、メッセージ全体の中で導入された部分にアクセスし、その部分を得るための情報を提供すること
- 他のメッセージの一部であることを示すこと

リファレンスによって法的タームを組み込むことは、電子商取引において、特別な注意を必要とする。リファレンスによる法的タームの組み込みを合法的なものとするには、既存の法規に従っていることを保証することが検討されなければならない。リファレンスにより署名ポリシーを既存契約への導入を保証することで、自動化された取引に新しい可能性が開かれる。

署名ポリシーは、電子署名が生成され、検証される条件を含む。前に述べたように、電子署名有効性の時間枠といったような、法的タームを含むこともできる。むしろ、受け手側との関係を有効とするために、このようなタームが署名者とその受け手との契約に取り込まれるべきである。法的な見解では、電子署名のルールは関係者間で同意されていなければならない。署名者は署名の生成の際に、検証者は署名検証の際に同意するので、同時ではないが、結果的にはお互いの意見が一致する。

署名者と受け手間での同意に署名ポリシーを取り込むことは、以下のように考えられる：

- 署名ポリシーへのリファレンスによって、署名者は特定の署名ポリシーのタームに従うことに同意する
- 受け手は署名者に署名されたドキュメントを受理する場合、根本的な署名ポリシーの条件に同意したと推定される
- しかしながら、特定の署名ポリシーのタームへの同意が有効にされたものであることを確認するためには、結合のルールに従っていなければならない

法的タームは遠隔のリポジトリにストアし、リファレンスによって利用することができる。リポジトリに署名ポリシーを置いておくことで、取引関係者は必要なタームを拾い読みすることができ、また法的ターム、署名の受理の条件、認可もしくは署名必要条件を含むパラメータにより、潜在的な取引関係者を選択することができる。

次の節では、特定の署名ポリシーの署名者と信頼された関係者の合意への導入方法とその条件について調査している。一般的に消費者契約での導入とビジネス契約での導入では、それぞれ異なったルールに従っている。ビジネス契約に包含するのは比較的容易だが、消費者契約に包含す

るためには、厳密なルールに従う必要がある。さらには、民法と慣習法の国では、特に標準条項の内容に関して、区別がされる。民法制度においては、一般的に標準のタームが、法廷で有効とされる公平なテストに合格しなければならないのに対して、the Unfare Contract Terms Act of 1977 により、英国法には分別の概念が導入されており、慣習法管轄においてよりも、さらに自由な方法で解釈されている。

10.3 実行におけるリファレンスの導入

いくつかのタイプの契約において、本質的な情報を記録したうえで、リファレンスによってより詳細なタームを導入する方法が共通の実行手段である。例えば、

- 建築者、建築家、法社会等といった、同業組合の標準の形式契約
- バス、鉄道、航空といった、当事者の一方の標準のターム
- 取引に関するその他契約のターム

電子商取引において、少ない量のドキュメントでは、効率的な導入や、ドキュメントの証明書ポリシーや証明書実施手順といった他のドキュメントのリファレンスを考慮しないことがある。

リファレンスによる導入は、まだ捉えがたい性質のものだが、法の新しい概念ではない。

慣習法の国ではリファレンスによる導入の利用形式リストが、民法制度におけるものをはるかに超過するが、以下の記述にあるような、EU Listing Particulars Directive（EU 詳細規則リスト）といった証券規則のような、少数の例に従う。

加えて、リファレンスによる導入は、EDI メッセージングで利用されるような様々な標準においてだけでなく、電子商取引における UNCITRAL Model Law（1996）でも引用されている。

民法では、リファレンスによる法的タームの導入の概念を広く受け入れている。顕著な例としては以下のようなものである。ドイツ、イタリア、ルクセンブルク スペインおよび英国においては、有価証券を発行する会社では、発行者の特徴を記載し、必要に応じて更新された（あらゆる資料が変化し、最新の会計年度、中間財務諸表を説明します）ドキュメントに注釈がつけられる場合、新しいドキュメントの代わりに指定された authority に許可され、かつ前の 12 ヶ月以内の発行されたドキュメントを回す。ベルギー、フランスおよびスペインにおいては、会社や財務諸表に関する情報を含んでいる”棚ドキュメント”が、年単位で、指定当局に従い、承認されているような”一括登録制度”の概念がある。発行証券が作成される時、”発行ドキュメント”は、棚ドキュメントを提供し、任意的に更新する文字を含み、監視する authority に承認されなければならない。

リファレンスによる導入を利用する際、取引者は以下を含む要件に注意しなければならない：

- （ハッシュの明白な計算に関する）詳細な記載と署名ポリシーのユニークな識別子
- 相手の同意と知識
- リファレンス節の表現とタームへの容易なアクセスの情報の肯定義務
- 電子商取引における the UNCITRAL Model Law 1996 といった国際法によるサポート
- ドキュメントリポジトリ上での明白な公開

11.結論

署名ポリシーは取引の法的安全性を増すための、必要要素として出現した。署名ポリシーは、その利用とデジタル署名を承認するタームの必要条件を確認するために利用される。署名ポリシーは、署名者から受け手（検証者）まで流れるよう詳細な情報を含み、結果的に取引の透明性を増加させるとともに、PKI のいくつかの管理条件を増強することもできる。

組織における構造化した内部プロセスは、適切に利用条件をバックアップすべきであるので、署名ポリシーは、ドラフト作成および編集の際に必要となる。長期間に渡り、署名ポリシーを管理、保管することは、暗号化の発達に合わせた更新が要求されるとともに、電子商取引の実践に適用するための潜在的なコストがかかるかもしれない。

署名ポリシーは、ビジネス関係を構築するための追加的な（新しい）契約上の道具となる。あるビジネス領域を代表する組織は、特定のビジネスニーズに応じて、取引において参照する署名ポリシーを作成し、識別することができる。

署名ポリシーの理解が足りないと、その中身や適用が曖昧に表現される。そのような署名ポリシーは、PKI の曖昧な表現を助長し、あらゆるタイプの取引に幅広く適合する技術としての機会を危険にさらしてしまうかもしれない。そんな署名ポリシーの利用は、認証を返すニーズがより明白である巨大組織内にとどまってしまうだろう。

調整的な見解では、署名ポリシーは、中身や適用を明確にしている一方で、ある産業界もしくは政府に適合した独自規定のイニシアティヴによって、管理することができる。

署名ポリシーの法的価値は、取引関係者が、取引もしくは署名者に対する契約上の地位を表明する一方の意思宣言とみなすことができる。したがって、そのような署名ポリシーは、デジタル署名を使用する取引に関連する法的条件を発動するために必要な契約上の道具とすることができる。署名ポリシーの慎重なドラフティングは証明書ポリシーのように、PKI の実行をサポートする他のポリシーとともに、矛盾するタームを回避するのに必要となる。

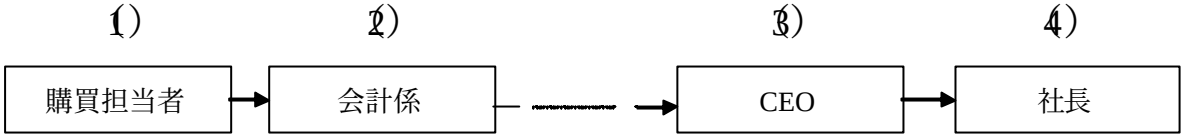
Annex A：電子取引における署名ポリシー

A.1　ケーススタディ１：組織内の取引

(1) 関与者

購買担当者、会計係、CEO、取締役社長など

(2) 署名フロー



図資 1-A-1 組織内の取引の署名フロー例

1. 購買担当者が取引書類に署名する。
2. 取引額が大きい場合は引き続き、会計係が署名する。
3. 会計係の権限によっては、CEO にまで送られる場合もある。
4. CEO では不十分で組織の社長の了承が必要な場合がある。2 人以上が同時に意思決定に関与する場合は同時認証が適切である。

(3) 署名ポリシーの例

- 購買担当者が署名できる取引額
- プロジェクトの期限または購買担当者の雇用期間に応じて、購買担当者の署名が有効であるべき期間
- 組織内すべての人に対する署名の制限
- 組織内すべての取引に適用される規則

A.2　ケーススタディ２：組織間の取引

(1) 関与者

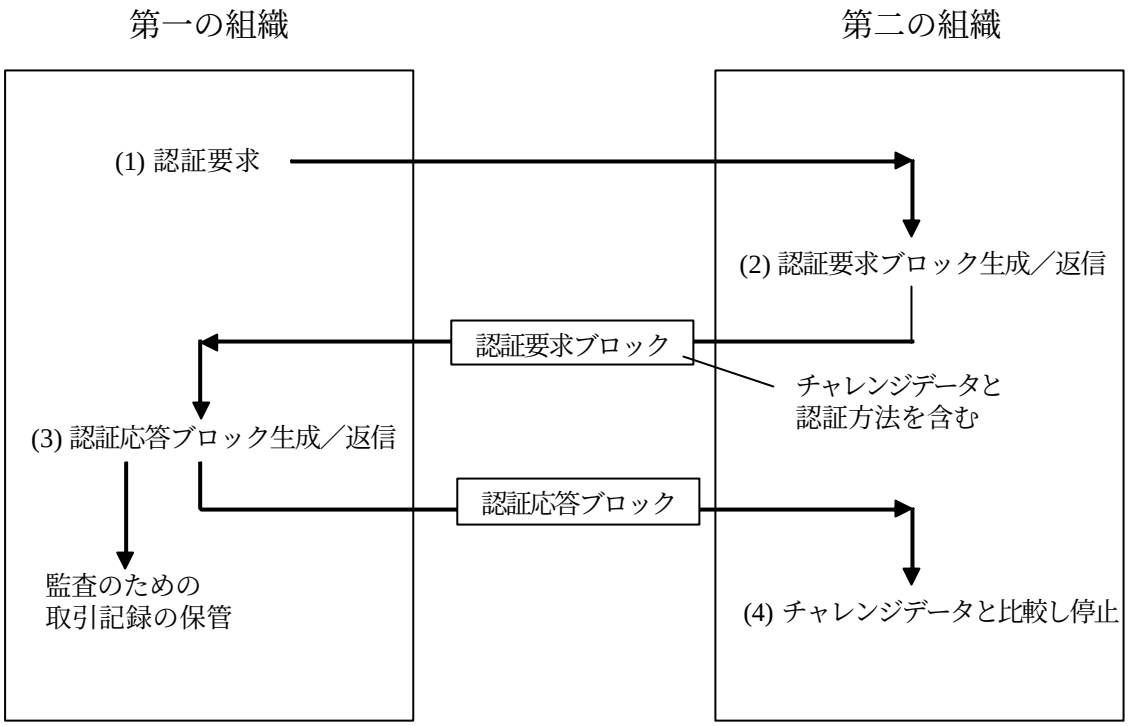
両組織の購買担当者、会計係、CEO、取締役社長

(2) 署名フロー

IETF の Internet Open Trading Protocol において電子署名を用いた組織間取引の枠組みが定義されている。例えば Baseline IOTP における組織間の認証においては以下の取引ブロック（取引時に渡される詳細情報）が定義される。

- 取引プロトコルオプションブロック（Trading Protocol Options Block）
- 認証要求ブロック（Authentication Request Block）
- 認証応答ブロック（Authentication Response Block）

組織間の典型的な認証シナリオを以下に示す。



図資 1-A-2 組織間取引の認証シナリオ例

1. 第一の組織は認証されるための要求をする。

2. 第二の組織はチャレンジデータと使用される認証方法を含む認証要求ブロックを生成し、第一の組織に返す。

3. OTP 対応アプリケーションが第一の組織で起動する。受け取ったデータを使用して認証応答ブロックを生成し、第二の組織に返し、停止する。オプションで監査目的に取引記録を保管する。

4. 第二の組織は第一の組織が正しい相手かを確認するために、認証応答ブロックを認証要求ブロック内のチャレンジデータとチェックし、停止する。

(3) 署名ポリシーの例

- **組織の認証の条件**
- **認証手続**
- **アーカイブの規則**
- **認証データの承諾**
- **電子署名を使う以前に取引を行った組織についての契約の規則**

A.3 ケーススタディ３：銀行取引

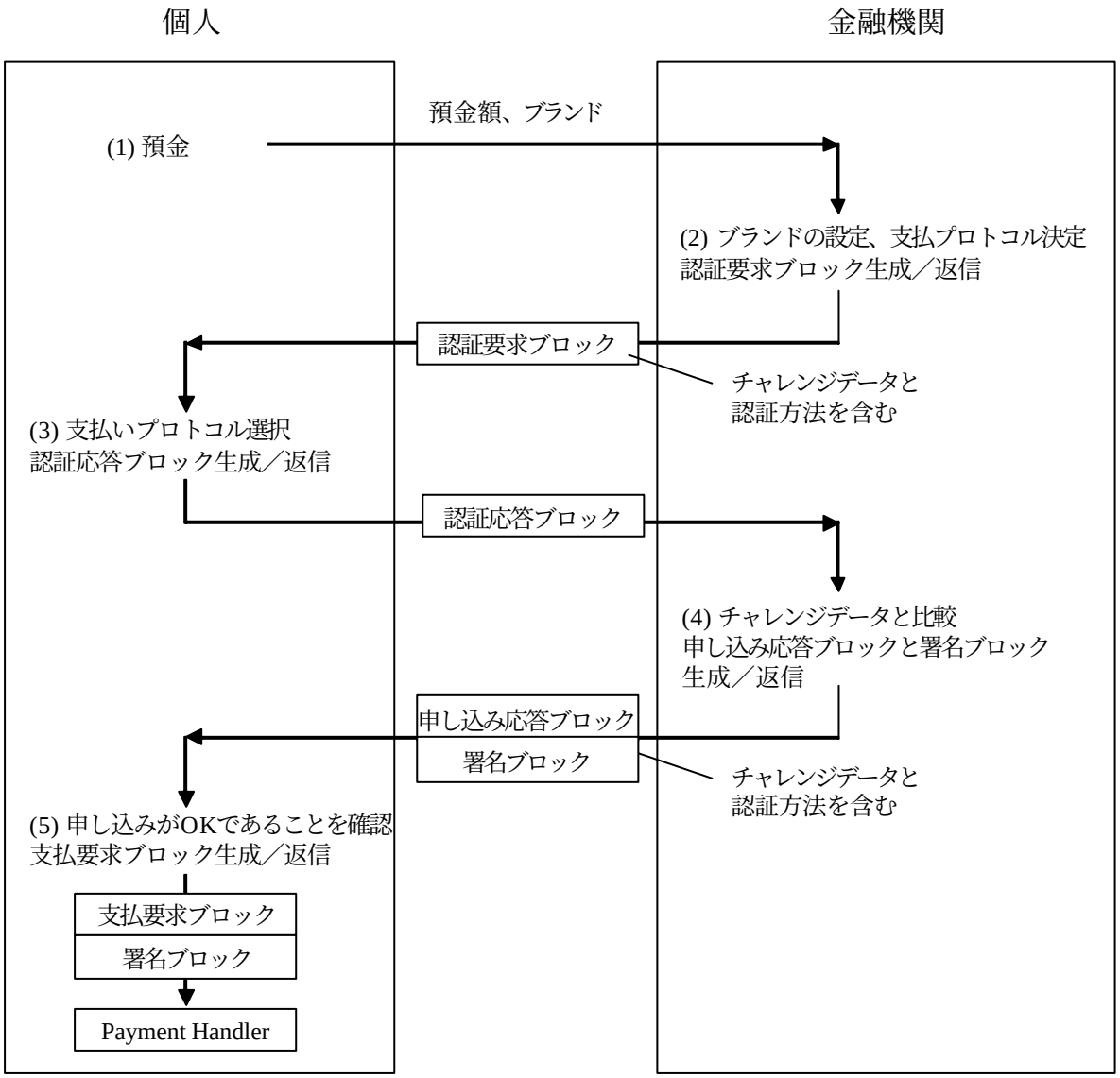
(1) 関与者

個人投資家、銀行、金融機関

(2) 署名フロー

個人投資家が銀行や金融機関との間で投資要求や資金移動に対して署名する場合、個人または銀行が署名ポリシーを発行する可能性がある。Internet Open Trading Protocol ではこの取引の枠組みを以下のように定義している。

1. 個人は電子的に預金するために、金融機関に預金額やブランドなどの情報を送る。
2. 金融機関は支払いブランドを設定し、提案する支払いプロトコルを決定し、チャレンジデータと認証方法を含む認証要求ブロックを生成し、個人に送る。
3. 個人は支払いプロトコルを選択し、認証応答ブロックを生成し、金融機関に送る。
4. 金融機関は認証応答ブロックを認証要求ブロック内のチャレンジデータとチェックし、預金額を含む申し込み応答ブロック、及び署名ブロック（オプション）を生成し、個人に送る。
5. 個人は申し込みが OK であることを確認する。支払要求ブロックを生成し、署名ブロックと共に Payment Handler に送る。



図資 1-A-3 銀行取引の認証フロー例

(3) 署名ポリシーの例

- **組織と顧客間の契約の規則**
- **顧客からの要求の受理**
- **認証手続き**
- **これら取引に含まれるデータ**
- **法的な枠組み**

Annex B：標準化活動のための助言

B.1　複数署名（Multiple signature）

当事者全員の署名が契約や法律により要求される場合がある。また同一文書上に電子署名を持つことは実用的であるため、電子署名が手書き署名を置き換えるためには複数署名のための標準が必要である。

署名の順序の重要性は取引の規定に依存する。複数署名は独立署名と埋め込み署名の二つのタイプに分かれる。すべての対向署名や二重対向署名はこの二つのカテゴリーに分類される。

B.1.1　複数独立署名（Multiple independent signature）

独立署名とは署名の順番が重要ではない並行署名のことであり、企業での取締役の署名の順番が重要ではないという例に見られる。ここでは必要な署名が含まれていればその文書は有効となる。

B.1.2　複数埋め込み署名（Multiple embedded signature）

埋め込み署名は署名の順番が重要な場面で使われる。最初の署名付き文書の受領を証明することが二番目の署名の目的のひとつである場合等である。例としては、土地の売買では双方の意思の署名付き文書を公証人が証明する必要があるが、公証人は双方の署名が付いた文書に対して署名をしなければならない。

しかしながら、法的観点からは独立、埋め込みの両方の複数署名において署名の順番が明白でなければならない。このためには例えば二番目の署名を第一の署名を含む形で行う方法があるが、もう一つの署名があることが受取人にわかりにくい。文書に複数署名がついていることを受取人に知らせるための署名ポリシーが作られる事が望ましい。

B.1.3　複数署名の有効性検証（Multiple signature validation）

今までのところ、署名ポリシーは一つの署名の有効性検証のために定義されてきたが、複数署名をサポートする要求が高まっている。署名ポリシーでは署名者が明確に明記されなければならず、一人以上の署名者が存在するかもしれないことを仮定して、複数並行署名または埋め込み署名をサポートする。複数並行署名の代わりに同時署名（concurrent signature）という用語が使われるだろう。埋め込み署名よりは逐次署名（sequential signature）のほうが理解されやすいだろう。署名ポリシーはハッシュ値以上のものに署名することを可能とすることにより対向署名を可能とし、複数埋め込み署名をサポートする。

複数署名の有効性検証では署名者はどの署名ポリシーとコミットメントタイプが使われるかを示すことができる。すべてのコミットメントタイプに適用可能な共通規則と、証明書、タイムスタンプ、属性のための信頼条件により定義されるコミットメント規則を含む事が望ましい。

B.1.4　複数署名ベリフィケーション（Multiple signature verification）

前述の複数署名の有効性検証のケースと同様に、複数署名のベリフィケーションは今後の課題である。複数並行署名、埋め込み署名をサポートする標準が必要である。

B.2　署名ポリシー公開

署名ポリシー公開者は以下の課題を解決するインフラを持つ事が望ましい。

- 公開の頻度
- バージョン数
- 更新と改訂の制御
- 失効
- 有効期限　など

さらに、これらのタスクを行うための役割、例えばアドミニストレータ、オペレータ、監査者などが必要である。署名ポリシー公開者は公開のプロセスを管理して、署名ポリシーデータの信頼性を保証するために以下の管理業務を行う。

- 保管
- バックアップ
- リカバリ
- 監査
- アクセス制御

署名ポリシー公開者は署名ポリシーのライフサイクルの最後まで管理手続きを実装する。署名ポリシーによっては、署名ポリシーの有効期限切れ以降も署名の検証を可能でありつづける必要があるかもしれない。この場合、署名ポリシーを利用可能とする役割は署名ポリシー保存者に移される。

B.3　署名ポリシー保存

有効期限切れの署名ポリシーを検証可能とするために、管理手続きを実装しておく署名ポリシー保存者が必要である。

リポジトリはデータベースである事が望ましく､管理インフラと共に維持される事が望ましい。データベースを最新に保ち、過去から最新までの参照がなされる事が望ましい。確固とした保存ポリシーを確立し、組織、運営上の課題を解決する事が望ましい。アクセスポリシーによりリポジトリのデータの真正性、可用性、完全性を確実にする事が望ましい。

保存者の公平に対する信頼性は特に法廷で論争の解決が必要になった時に重要である。したがって保存者は全員に受け入れられなければならない。

B.4　認定スキーム

ポリシー発行者の認定スキームも必要である。署名ポリシーを検査する信頼の置ける認定スキームにより、認定された署名ポリシーに基づく電子署名の有効性はより信じられるだろう。

この認定スキームは公的または私的な組織により確立できる。例えば消費者団体が消費者の権利を保護する基準を満たす署名ポリシーを認定することができる。一方、公共機関が認定スキームを作り、ある署名ポリシーに合致する電子署名は公共機関に自動的に受け付けられるとすることができる。

B.5　署名属性要求

現在、署名ポリシーは署名メッセージの意味を検証できる要素を含まない。例えば現在では金額を含むための署名属性が存在しないため、署名ポリシーを使って金額を検証することは不可能である。

この問題の典型的な例は注文書を扱う署名ポリシーである。この署名ポリシーは署名組織の役割（注文担当者、会計係など)、量、物の種類などを含むことができる。したがって、金額を含むための新しい署名属性を追加する要求は適切であろう。

資料２

ETSI TR 102 045, “ Signature policy for extended business model ”, Version 1.1.1, 2003-03

原文において、示す章の要約を記す。なお、参考のために EU DIRECTIVE（EU 電子署名指令）の抜粋を添付する。

原文	要約
4 Overview	4 概要
5 Analysis of signature issues	5 署名問題の分析
6 Formalities of signing	6 署名の形式
7 Roles and attributes	7 役割と属性
8 Commitment types in electronic signatures	8 電子署名におけるコミットメントタイプ
9 Multiple signatures	9 複数署名
10 Signature policies	10 署名ポリシー
11 Conclusions	11 結論
Annex A: Business scenario descriptions	Annex A： ビジネスシナリオ
	DIRECTIVE 1999/93/EC（参考のために添付）

4．概要

4.1　背景調査

目的：複数の署名が付与される広範囲のビジネスモデルにおいて、署名ポリシーの検討を行う。
調査方法は、実世界のシナリオを調査し、仮想世界に変換する方法を考慮。
調査情報源：

- 法的手続きにおける署名解釈の司法アプローチとして、判例を含む法研究や著者の個人的経験。
- 「実世界」、「仮想世界」両方を対象としたビジネスシナリオ範囲内で署名を利用したビジネス業務上の経験。
- 欧州以外の第３国を含んだビジネスシナリオからの情報。
- 情報セキュリティ、特に電子署名のエキスパートからの情報。(ETSI、ESI、CEN/ISSS E-Sign などに限られたものではない。)
- ETSI、CEN/ISSS、IETF、ebXML、OASIS などから出された文献。

調査結果：

- 多様なビジネスモデルを満たすことのできる包括的な署名ポリシーの「モデル」を作ることは難しい。
- 伝統的に手書き署名を要求することは多々あったが、ほとんどの場合はなぜ署名が要求され、コミットメントタイプは何を意図し、どの処理段階で署名を検証するのかが明白に説明できない。
- 電子署名の場合においても上記の情報収集は困難であった。理由は、まだ電子署名は普及の初期段階であること、機密保持や秘密保持契約などによって阻まれたため。

4.2　電子署名 Directive1999/93/EC の含意

Directive は技術的に中立となるように作成され、加盟国は法的手続きにおいて、Art5.1 の下で要件を満たしている電子署名が手書き署名と等価なステータスを持つことを保証しなければならない。しかし、Directive には、署名者がそのような署名を作成するつもりであったという「意思」や、コミットメントを表す「意思」に関しての定義がされていない。

4.3　署名ポリシーの序論

署名ポリシーは、署名を生成、検証するための規則の集合であり、署名者と検証者は同じ署名ポリシーを用いなければならない。

4.3.1　「紙」世界の署名ポリシー

紙の世界では、小切手の署名で支払いが許可されるように、多くの署名の意味は作成される状況や文脈から推論されており、一種の暗黙の署名ポリシーである。

4.3.1.1 法定的署名ポリシー

多くの国々に、署名を有効とするための署名生成に関わる判例（意思、家族事務、土地に関する手続、消費者保護と金融商品等）がある。

- 署名は、署名者の行為によって作成されなければならない
- 署名は対向署名（countersignature）されるか証人署名（witness）を要する。
- 署名手続きを公証されなければならない。

4.3.1.2 慣習的署名ポリシー

ビジネスは慣習的に多くの署名生成における要件（対向署名、証人署名／公証、承認など）を負わせているが、電子化された際に、既存の法令で電子環境の需要に適合する法令はほとんどない。電子署名の有効性を確立するために署名ポリシーは必要であり、署名ポリシーは XML 等機械が処理できる形式に加えて、特に人間にも判読可能である必要がある。

4.3.2 電子署名ポリシー

電子署名ポリシーの例として「Electronic Signature Directive」の Art5.1 があり、すべての加盟国に対して電子署名が手書き署名の相当物として認めるための条件を制定している。Art5.1 を踏襲して、ドイツでは Signatureverordnung-SigV（2001/11/22）が制定され、イタリアでは Italian Public Administration が示されている。

署名ポリシーは異なったベンダ間の業務アプリケーションやソリューションの相互運用の橋渡しとならなければならない。署名利用規則は人間とコンピュータのインタフェースを考慮して作られるべきである。署名が自動で行われる場合でも、署名を行う決定は人間が行うようにプロセスに組み込む必要がある。人間が、署名ポリシーを実装したアプリケーションインタフェースを通して導かれる手段は実現できる。

5．署名問題の分析

法的にも慣習的にも署名のための規則は世紀にわたって発展してきたので、それらの法的基礎の分析は複雑である。そのため、現在に至るまでの詳細比較は本旨の範囲外とし、署名が今日の企業取引の中でどのように使用されるかについての観察に制限する。コミットメントを認める形式は、署名者の手書き氏名以外にも、スタンプ、ゴム印、更には×印でさえ裁判所によって有効な形式として認められている。仮想世界では、電子署名あるいは条件付電子署名の使用で、権限の承認を管理できる可能性がある。

5.1 署名するという調印／意思の形式

署名の重要な特性のうちの１つはその生成方法であり、しばしば「署名セレモニー」と呼ばれる。その手続きの中では、意識的に署名されたことの証明が求められ、署名者に確認させるように署名の前に署名の意図を書く手段や署名者自身の言葉を書く手段(「私は×××が真実だと宣誓します」」など）がある。Directive がこの要素に対応していないことは注目すべきであり、電子署名の法的な認識および同等な他の管轄の法律と照らしあわせると、それは高度な電子署名や効

力のある電子署名においても、特に署名する際の意志か意図を示す証拠を要求していない。

5.2 署名者の同一性

意図した署名者の署名と確認できなければ署名は無効である。従って、署名が指定された個人のものであることを保証することは重要である。紙の世界では、署名の下に本人名称が印刷されることにより達成されるが、いくつかのビジネスシナリオでは、署名者の役職等属性を記述することが本人名称の記述と同じくらい重要である。

5.3 署名者の役割と属性

多くのビジネスシナリオでは、契約する団体は、交渉している相手個人の地位や権限の確認を必要とせず、署名者が組織を代表して行為を行う「明白な権限」をもつことで十分である。いくつかの例外もあり、土地の販売のための処理などは、その処理を有効とするために、任命された会社役員の署名の証明を要求（権限の確認）する。実際、電子環境において、公開鍵証明書、属性証明書の形式において、あるいは他のある保証された情報によっても可能である。もし標準化されたビジネス規則が OID（Object Identifier）によって分類や参照されるのであれば、この種の情報は適時の立証が可能であるべきであり、自動処理によって行われるのが好ましく、それはビジネスプロセスを促進する。

5.4 署名コミットメントタイプ

署名から生じる責任は、しばしば署名生成の状況から推論されなければならない。しかし電子化された際には、本人の意図的なコミットメントを認めにくい電子化もあり、ウェブサイトデザイナーや弁護士を悩ませている。「署名する」という方法から推論されるコミットメント、つまり契約上拘束するための意図を証拠づける内容が曖昧である。

5.5 タイミングと順序

タイミングと順序は、署名確認プロセスにおける証拠としても重要な役割を果たす可能性があり、第一署名者（primary signer）および証人署名者（witness）の署名が短時間に、正確な順序で行われた場合、証人署名者は実際に第一署名者が署名を行なうのを見たといえる合理的な証明となる。いくつかのビジネスシナリオでは、順序とタイミングは、単一のドキュメント上の署名に明確な関係がない場合もあるが、単一のプロセスか処理の部分を形成する多数のドキュメント上では関連する場合もある。

5.6 ロケーション

慣習法管轄における従来の手書きの署名は、署名を記述した地理的な証拠を要求および提供しない場合がある。しかし、署名がなされた場所や管轄は、争いがどの管轄の法律で審問され／適用されるのかを決める際に、法的な結果を持つ可能性がある。しかし、物理的な場所を立証するメカニズムをもった署名ポリシーを構築することは、ほとんど不可能である。現在、解決法がない状態で場所の記述を要求されるが、第三者の証明なしで簡単に証明はできないように思われる。

5.7 有効期間

署名を再度確認することを要する状況、例えば訴訟では、不正行為の主張あるいは電子署名自体の危殆化の場合などがあるが、長期証明問題に取り組む 2 つの手段がある：

- 署名アルゴリズム自体を強化する手段
- 初期に署名を検証し立証データの安全なアーカイブおよび監査証跡を維持する手段

5.8 技術的およびセキュリティに関する考察

「現実」と電子署名の関係において本質的な役割を演じ、電子署名や署名の付いたデータが変更されず危険にさらされていないという信用と信頼が増加する。

紙世界のセキュリティ考察：

- 手書きの署名を必要とすること
- 署名見本があるチェックカードを必要とすること
- データベースに署名見本を維持すること
- 身分証明や個人の立会い要求（例えば立会い／対向署名／公証書）

電子世界のセキュリティ考察：

- ホルダーの身分証明に関して、証明書の許可された範囲での使用、例えば Directive における資格証明書の問題
- 安全な署名生成装置の開発

Directive の下では、広いカテゴリーの電子署名タイプを識別することが可能：

- simple e-signature (Art 5.2)
- advanced electronic signature (Art 2.2)
- advanced electronic signature + qualified certificate
- advanced electronic signature + PK certificate +scd (or sscd)
- advanced electronic signature + qualified certificate + scd
- qualified e-signature (Art 5.1)
- qualified e-signature + CA accreditation

5.9 複数署名（Multiple signatures）

契約書等で示されるように複数の署名の順序およびタイミングは企業取引に対して重要な意味を持っており、1 つの署名は他方の前に適用される必要がある場合がある。紙の世界では、署名に日付をつけることが慣例であり、日付は個別の要素であるが緊密に署名と結びついており、署名ポリシーを考慮する中でその重要性を無視することはできない。さらに、実世界の電子環境の中では署名が作成された環境が失われる可能性があり、順序やタイミングは、その状況のいくつかを示す証拠を提供する重要性を持っている。

5.9.1 対向署名（Countersignatures）

対向署名は、効力を与えるために別の署名が要求される場合や第一署名を活性化させるために使用される。対向署名の作成方法に関しては要件があり、時間、順序および場所は重大な要因である。対向署名する過程は、署名確認の状況においても関連があり、多くのシナリオでは、対向

署名者が第一署名者の身分と権限のチェックを意味する。

- 署名の有効性（署名者本人の署名であることと認められる）
- 署名者の本人確認
- 署名によって示されたコミットメントをするための署名者の権限
- 含意（署名を行なうことにおける署名者のビジネス役割）

これらは署名ポリシーの下の電子署名を検証にすることで反映される事項であるが、技術的な観点から対向署名を扱うことにおいて、必ずしもその方法に影響する必要はない。ビジネスニーズに実装される対向署名と、技術的センスにおける対向署名を明瞭に区別する必要がある。署名ポリシーで、何が署名されているか、ビジネス／法的な観点からなぜそれは署名されるのかに関して、レベルを決定しなければならない。

5.9.2 証人署名（Witnesses）

仮想世界では、証人署名者の役割は、署名を実施する人が確かに正しい人であることを保証する立場である。これは署名を検証する証明書（署名されたデータ自体に含まれている）に含まれた名前が確かに存在することを、証人署名者が確認することである。しかし署名の時、署名者および証人署名者の両方の実在が義務的ではないことが提言されるべきである。署名が付けられた後でも証人署名はすることができる状況にあり、これは紙の世界における状況（証人署名人は実際に署名実施の確認を要する）との主な違いである。

5.9.3 公証人の署名（Notarial signatures）

公証人は信頼される立場であり、公証書はめったに異議申し立てされない。電子署名検証でも、公証人のプロセスの検証をする補足要求があってはならず、唯一公証人の署名は有効であるいう見解を考慮する。一旦、公証人の署名がそのとき確認あるいは有効になったならば、それ以上の確認をする理由があってはならない。公証人は信頼されたオフィサーであり、それらの信頼性に異議をとなえることは意味をなさない。

6．署名の形式

署名をするという物理的な行為は、署名者が試みているコミットメントの重要性が意識されている。もし電子署名が使用される場合、同様の状況や意味を提供する追加のステップがなければ、この「警告」メカニズムが失われる。これは純粋な技術的な手段によって達成は不可能な場合もある。Art5.1.に宣言された、キーを活性化する PIN の署名者による選択は、それ自体署名者が法律上拘束力のある電子署名を作成するつもりだったことを証明するのに不十分である。署名者にドロップダウンリストからコミットメントタイプの選択を強いることは、より大きなセーフガードや確実性を提供しない。

解決策は、署名者にあるテキストを書き加えることを要求することである。署名する結果に関して警告をあらわし、自身が手書きの署名の相当物を作成するという事実に対して、署名者の注意を引き付けるためである。これ（あるいはそのハッシュ値）も現実に署名されたデータに組み入れられる場合、「手書きのものに相当する物であることを意図した電子署名を作成した」という

署名者の意識を示す証拠を提供する。

7．役割と属性

7.1　「役割」、「属性」、「特権」の意味

役割と属性の概念は誤解されやすく混乱する。最も一般的な誤りは、状況から役割を導き出すことである。また、ある状況において役割であるものは、別の状況では属性になる。

Role（役割）：役割は、特定のオペレーションかプロセス、あるいはプロトコルで演じられる役である。別の人がその役割を引き受けてもよいが、役割はそのまま残る。取引では、各役割がその役割が行うと予想されるか、その役割によって意味付けられる責任やコミットメントを行う行為を表す。

Attribute（属性）:属性は、固有の特性あるいはオブジェクト（人または企業）に緊密に関連した特質の塊としてさらに定義される。従って、ビジネス役割（つまり権限と責任のセット）は、業務取引役割の属性になる。

Privilege（特権）:特権はアクセス権、もしくは署名するべき権限などで表現される。いくつかの状況では、特権、つまりある種類の処置を講じたり、ある機能（署名など）を実行する権利は属性にもなることができる。

7.2　ビジネス役割もしくは属性が公認される要求

紙の世界の取引関係は、商取引の経歴として蓄積された信頼の上に築かれる。普遍的である法則は、組織がその従業員あるいは代理人の行動に対して最終的な責任を負うので、多くの場合では、要求されたビジネス役割、ステータス、実行権限の真実性は信頼される。

互いに相当な地理的距離にある場合の処理は、先の知識、一貫したパターンの行為などから信頼性が得られる場合もあるが、単に処理が電子的に署名されるというだけでは取引する理由にならないため、信頼できる証明を要求される場合もある。

7.3　属性としての権威

販売責任者などのビジネス役割は、組織を代表してある機能を実行する権限を意味する。専門の役割はさらにこれらの機能（例えば薬剤師は薬を処方する権限がある）も満たす。権限の証拠は、事業協定の一部として要求される場合もあるが、法律においては、確かな権威やステータスを持っている人だけが、実行権限があることを要求する。

7.3.1　委任された権威

委任された権限は、署名の有効性に関連する署名者の属性であり、委任は署名者によって明示的に付与されるか、単に推論されるだけの場合もある。従って署名ポリシーが、委任された署名を考慮に入れる場合、実際の認可が要求されるか、要求された認可（推論された認可を含む）が十分かどうか明示することは重要である。

一般的に署名するべき権威が委任される状況として、以下の 3 つがある。

政府機関：役人の行為は特別な状況を除いて、長官の実行していることとして長官に結び付けられる。役人が別の組織の代理をする場合、その表現や行為は、その受けている訓令や権限に従っていなくてもその組織に結び付けられる。
委任権：委任状は、有効期間が短く、変更不可で、無効にされる見込みがないよう意図される。また、高齢者や障害者のための委任状のように、より長期間および広い委任権限を備えた委任状がある。
代理人ごとの署名：部下が上司の代理で署名することは、会社の意図内であるかどうかに関係する。日常のビジネスにおいて即時の行動が要求され、主要な権限ある人が行動不可能な場合などによく利用される。さらに、多くの場合それが使用される状況は予見が最も困難であるので、それを規則に定義するのは最も困難なものである。

代理人や委任状経由で許可されたような実際の委任された権限は、公開鍵暗号証明書の発行（それは証明書拡張として属性情報を含んでいる）によって扱われる。証明書はさらに権限の源である「ドキュメント」へのポインター、OID や他の言及を含んでいるべきである。証明書の有効期間は、委任された権限の意図した期間に相当するべきである。従って、実行権の取り消しは、証明書の取り消しによって便利に扱うこともできる。

代理経由で署名するような要求や推論により委任された権限は、仮想世界の中では管理することが困難になる可能性がある。

7.3.2 制限された権威

通常、組織を代表して行動する従業員や同様の能力の人は、彼らに与えられた権限の範囲を知っている。彼らが権限を超過しても、雇用者は雇用条件における従業員の行動に対して責任がある。取引相手が従業員権限の範囲を知ることを可能にするような信頼できる方法が電子商取引では必要だと認識されることは明らかである。

7.4 役割の分類

7.4.1 ビジネス役割

分析によれば、ビジネス界を横断できるビジネス役割を定義することは、ビジネス役割に一貫性がないためできない。理由は、役割より明確な職務表現は、ビジネスの大きさや組織的な構造に依存した権限や責任に広い幅があるからである。ビジネス役割の分類はこの範囲外であるが、次の勧告は本タスクが引き継がれることを考慮して記述する。

加盟国の中で同様なビジネス役割を識別し、分類できる場合、国内市場のビジネス利益を促進する可能性があるために、既存の法令による定義や概念と矛盾してはならない。そして、すべての加盟国で認識でき、採用できる必要がある。

7.4.2 国際貿易における取引の役割

TR 102 044 の Annex B に、役割証明における Italian Assocertificatori ドキュメントの抜粋が含まれる。これは、OID のようなコードがどのように役割を分類し識別することができるかの実例である。

7.4.3 署名行為役割（Signing roles）

署名行為役割は、署名ポリシーの下での複数の署名生成および確認を管理する手段として存在する。それらは、署名ポリシー内のビジネス役割あるいは処理役割のいずれかと評されることもある。プロトコル内では、それらは常に割り振られた、もしくは要求された役割である。証明される役割が識別される必要がある場合、これは署名行為役割の属性になり、そういうものとして管理されるべきである。

8. 電子署名におけるコミットメントタイプ

正規の手続きのもとに行われる署名は、なんらかのコミットメントを意図するものとみなすことができる。そこで、電子署名で必要と思われるコミットメントタイプの種類を検討する。実世界（紙の世界）においては、それらはコンテキストにより暗黙のうちに了解される場合が多い。そして、その解釈に存在するあいまい性は効率を重視していることによる。しかし、仮想世界（電子署名の世界）では、手書きのそれよりも、より広い範囲のアプリケーションで利用される可能性があるため、その利用目的を署名者が正しく示すことができる方法が提供されなければならない。さらに、署名を正確に解釈するためのコンテキスト情報、あるいはそれに代わる情報の提供も必要である。

また、コミットメントタイプ（署名タイプ属性）は、署名ポリシーの下での複数署名の管理や検証のためにも有用である。

8.1 実世界のコミットメントタイプ

手書き署名の意味はそのコンテキストから暗黙的に示される。署名者の意図するところを科学的に厳密に解釈することはできない。また、署名の解釈について扱う法律やビジネス習慣も確立されたものはない。しかし、ある程度のあいまい性が実際には有用で、おそらくは不要な争いを避ける助けになっているなど、議論の余地がある。

8.2 電子コミットメントタイプ

電子署名におけるコンテキスト情報の欠落の問題について考えるにあたって、ここでは署名者の署名行為の有意性と、署名対象に対する認識の存在は前提とした上で、署名目的の潜在的な曖昧性に関して、以下の三つの可能性があり得る。

- データの出所を保証するための署名
- 手書き署名と同等の署名だが、署名とデータ内容を法的に結びつける意思のないもの
- 署名とデータ内容の法的な結びつきの意思表明

よって、これらをはっきり区別することが重要で、そのためにはコミットメントタイプの指定

が必要となる。例えば、手書き署名と同等の署名でも、以下の場合は区別しなければならない。

- ドラフトへの署名。その内容に関して知っているということ、そしておそらくはその著者であることの表明。
- 受領確認の署名
- 法的な約束を意図した署名

これらを署名者が署名を行う時点で明示的に選択または承認するべきである。

先の署名に対して、さらに署名して複数署名とする対向署名についても、以下のコミットメントタイプを署名者が明示的に選択することになるかもしれない。

- 認可
- 証人署名
- 公証

また、管理目的の電子署名のコミットメントタイプもある。

- 電子公証や（記録保存の）管理目的署名

ここに上げているようなコミットメントタイプの定義は、ビジネス上、明白な必要性がある場合にのみ行うべきであり、またそれが妥当であれば、どのような定義もあり得る。

8.2.1 電子公証

電子ビジネスアプリケーションをサポートする「信頼」のインフラストラクチャの一部として電子公証サービスの重要性が増してきている。ここで、「公証」や「電子公証」という語は特別な意味を持ち、必ずしも、伝統的な民法上の公証サービスや、米国の公証人制度などの電子的な等価物であることを意味しない。より一般的な意味での、信頼される第三者によって、データの真正性と完全性を、特定の時点において証明するものであり、また将来参照可能な有効性の証拠となる記録を与えるサービスである。このサービスで使う電子署名には、それを反映ししたコミットメントタイプを選ぶことが有用かもしれない。サービスはデータ内容についての直接の関与はしないが、サービス対象となるデータに炊いて潜在的に信頼性を与えている。その信頼性は電子公証の署名によって裏付けされる。

8.2.2 有効性検証プロセスの一環としての電子署名

いくつかの状況下では、信頼されるサービスの１つとして、特に自分自身では署名検証の手段を持たないリライイングパーティの代わりに、検証を行ってあげるようなものが有用かもしれない。それは複数署名を扱うアプリケーションの一翼を担うものにもなりうる。この電子公証人（検証者）は、署名を、それが作成された後の適当な時点で検証し、検証したデータやその結果を記録の上、署名してタイムスタンプを付与する。そうすれば、これは将来参照可能な証拠となる。

8.2.3 単純な管理目的の電子署名

これも電子公証署名の一形態かもしれないが、ここでは署名対象に関して、いかなる検査や検討も行うことを意図しない。署名はただ保管したり記録したりする目的に限定される。これは、紙の世界における法的な擬制を模擬するもので、それを行う権限をもった特定の人物によって、その記録が作成されたことを認めるものである。

例えば、正しく署名された、取引上の複数のドキュメントをまとめて扱えるように署名するような場合は、取引を完了し次の段階にプロセスをすすめるために、ドキュメントをまとめる電子的な「ホチキス」となることが署名者の役割になる。

9．複数署名

「複数の」署名はいくつかの異なるカテゴリに分類でき、それぞれ利用目的が異なる。

9.1　並列署名

並列署名とは、お互いに「独立な」署名で、ここではその順序は重要ではない。

これらの署名は、それが付されたドキュメントあるいは関連の取引において、すべての必要な署名がなされていて（かつ、それが有効で)、効果をもつ場合に限り、相互に関係性をもつ。もっともわかりやすい例として、売買契約における買い手と売り手の双方の署名の必要性がある。（注：技術的見地からすれば、これは埋込署名で実現されるべきである。）

その他の例としては、会社法で、２人（またはそれ以上）の企業取締役の署名を要件とする場合がある。この場合、署名の順序は全く重要ではない。そのドキュメントに必要とされる全ての署名がそろっていれば有効である。

9.2　順序付き（並列）署名

ここでの順序付き署名は並列署名のバリエーションで、署名の順序が重要なものである。署名が順番に同じデータ内容に適用される場合もあるし、そうでない場合もある。これはその署名対象に他の署名も含むかもしれないが、それはあくまでも署名対象データの一部として、であり、後で述べる副書や埋込署名の代わりとなるものではない。

注：並列署名と埋込署名は過去の文献でも述べられているが、順序付き署名についてはまだ広く受け入れられたものにはなっていない。

9.3　埋込署名

埋込署名のシナリオでは、ある署名が別の署名に対して行われる。すなわち、一つの署名の中に別の署名が埋め込まれる。この場合、署名が適用される順序が重要で強い相互関係性を持つ。つまり先の署名の有効性は後の署名のそれに依存する。例えば、ある署名に対する証人として、別の者がその第一署名に対する対向署名を行う。（これは埋込署名である）このタイプの署名は、最初の署名付きドキュメントの受理を証明することが二番目の署名の果たす役割の一つであるような場合に、必要となる。対向署名は、さらに以下のような証明を行うことになる可能性がある。

- 最初に署名されたデータの意味の検証または承認
- 第一署名者の身元の検証
- 第一署名の有効性の検証（証明書の有効性や署名ポリシーへの準拠性の検証）

埋込署名の必要性に関する例は、公証サービスで見つかる。この場合、公証人は署名に対してだけでなく、署名されたドキュメントに対しても署名する必要がある。また別の例で、例えば、ある者が他者の署名に証人として署名するような場合、その文書の内容には全く関知せず、単に

その署名に対して対向署名するという場合も考えられる。

9.4 複数署名管理

署名ポリシーは（あるいはより正確に言えば署名ポリシーの下で展開される規則は）、複数署名の管理に関するフレームワークを提供することができる。ポリシーに基づく署名規則は、作成時のものと検証時のものの両方が提供されなければならない。しかし、ビジネスアプリケーションによっては、そのどちらにより重点を置くかは異なってくる。例えば、組織内アプリケーションの一部として署名が用いられる場合のポリシーは、署名作成時の規則がより重要かもしれない。つまり、間違った署名の行われることがないようにする署名作成ポリシーである。この場合の有効性検証規則については、品質管理のための無作為抽出試験の安全対策にしかすぎないかもしれない。一方、署名が取引相手からのものである場合には、署名の信頼性を確立するために十分なデータの検証規則の方に、その重要性が存在するかもしれない。

複数署名の管理の問題を考える出発点として、まず個々の署名を、そのドキュメントや取引に対して有効なものとして作成する方法を記述して定める必要がある。さらにそれらは、まず個々に署名ポリシーに従って検証されることになるかもしれない。

次に考える点は、署名間関係の定義である。これは実際には二つのステップで行われる。最初に「署名を行う（署名行為）」役割を個々の署名に関して割当てる。次に個々の署名にいくつかのデータ属性を関連づける。それらの属性に、その署名手順またはプロトコルのコンテキストにおける署名目的が記述される。

9.4.1 署名行為役割（signing roles）

署名行為役割は署名ポリシーで指定される役割で、署名者に割り当てられるか、あるいは自身で選択した役割として、その署名と署名ポリシーが要求する他の署名との間の関係を定義する。署名行為役割は、複数署名の管理を目的とするものである。ここで述べる「署名行為役割」signing role と「署名役割」signature role（TR 101 733）はきちんと区別する必要がある。署名役割がなにかの属性の署名者への関連づけを意味するのに対して、署名行為役割の方は、その署名者の役割に対するなにかの属性の関連づけを必ずしも意味しない。ただし、署名者の属性への関連づけを妨げるものではない。

署名行為役割は、本質的には、以下のいずれかである。

- Primary signatures（PS）第一署名:
  これは並列署名で用いられる。ただし、第一署名には対向署名が要求される場合もあるかもしれない。また、署名順序の要件が存在する場合もあり得る。
- Countersignatures（CS）対向署名:
  ここでは、これは１つ以上の並列署名や順序付き署名に対する署名に対して用いる。

例えば、１人の買い手と１人の売り手の間で売買契約が行われるような場合には、次のような署名行為役割が必要になるだろう。

- PS/1＝買い手
- PS/2＝売り手

原則的に割り当てられる役割の数に制限はない。例えば、土地の売買などで売り手と買い手が

それぞれ二人の人物が関わっている場合の役割は次のようになる。

- PS/1 と PS/2＝買い手 1 と買い手 2
- PS/3 と PS/4＝売り手 1 と売り手 2

もしこの取引が法律上、公証人の署名を必要とする場合は、公証人の署名は CS/1 になる。(ASN.1 データとしては（各署名に対して対向署名されるので)、CS/1-4)

署名役割は取引上の観念的な役割やビジネス役割で表現される場合もあるが、あくまでも署名手順における主張された役割（“claimed role”）である。例えば、経費の請求を想定した場合、必要となる署名役割としては、次のようなものが考えられる。

- PS/1＝従業員
- CS/1＝管理者
- CS/2＝会計係

これらの役割のビジネス役割や属性としての認証については、本節の範囲外の事項であるが、例えば署名ポリシーが、従業員が自分で自身の管理者として CS/1 の署名を行うことがないように保証する手段を指定することもあるかもしれない。

9.4.2 電子署名のコミットメントタイプ

複数署名間の関係を検証する上で、コミットメントタイプは有用な役割を果たす。

第一署名に関するコミットメントタイプは以下が上げられる。

- 最終（法的）約束
- データ内容の承認
- 原本性証明
- 受理証明または受領確認

最終（法的）約束やデータ内容の承認では、常に署名者への通知と署名者によるコミットメントタイプの選択または承認が行われるべきである。そうでない場合、署名者の意思を確認する証拠が残されていなければ、署名の法的に有効なものとして扱えないだろう。(たとえ、その署名が署名ポリシーの下で「有効」であることや、手書き署名と同等のものであることが証明できたとしても、上記は変わらない）それに対して、原本性を証明するための署名は、状況によっては、必ずしも署名者の明示的な選択を必要としない場合もあるだろう。

対向署名のコミットメントタイプは、以下がある。

- 認可
- 証人署名
- 公証

経費請求の例で言えば、上司が従業員の行った第一署名に対して対向署名する際は、コミットメントタイプとして「認可」を選択することになるだろう。

上司が部下の役割を代わりに果たすような場合もあるかもしれない。例えば、従業員の署名が足りない時にその上司が署名を行うなどである。そのような場合は、コミットメントタイプとしてはやはり「認可」を選択し、署名ポリシーの検証規則でそれを許可するやり方と、対向署名者にも、第一署名に関連するコミットメントタイプを（「原本性証明」を除いて）選択できるようにするやり方もある。

上述のものに加えて、紙の世界の代理人署名のようなコミットメントタイプを選択し、署名者が代理署名権限を主張するようなこともありうる。しかし、このような代理のコミットメントタイプは、認可や証言、公証のような署名タイプには決して適さない。

管理上の署名タイプ属性としては、以下がある。

- （単なる）管理目的
- （電子公証的な意味での）管理目的
- 電子署名有効性検証

9.5 複数署名の有効性検証

署名の付けられた各々の情報は、それが署名ポリシーとともにまとめられたかどうかを証拠として提供することができる。署名の信頼性を評価するために、署名作成規則から有効性検証の結果を予想して、それを実際の結果と比較するやり方が考えられる。よって、複数署名の有効性検証は次の三つの段階を踏む。

1. 適切な署名検証データが作成され、まとめられていることを確認する
2. そのデータに基づき有効性検証の結果を予測する
3. 予測結果を実際の結果と比較する

最初に、個々の署名を単独で、(単独の)署名ポリシーに従って有効性検証しなければならない。署名間の関係はその後で検証すべきである。これは以下で実現できる。

- 必要な個々の署名の存在をチェックする。
- 役割属性がそれぞれ、特定の署名役割に対応していることをチェックする。
- 署名コミットメントタイプが署名ポリシーの要件に対応し、かつ各署名役割に適当なものであることをチェックする。
- 個々の署名が必要なデータに対して行われていることをチェックする。(例えば、対向署名が先の署名に正しく署名されているなど)
- 順番やタイミングが重要な場合は、全てのタイムスタンプが予期される結果と矛盾のないこと。

10.署名ポリシー

署名ポリシーは、署名の妥当性を判断するために必要な電子署名の生成と有効性検証の規則をセットにしたものである。それゆえに、署名ポリシーは、承認された電子署名の取引に関係した同意と条件設定を必要とし、２つに構成（署名生成ポリシーと署名検証ポリシー）された署名ポリシーが一般的に受け入れられる。

1. 署名ポリシーは、暗黙的に２つのビジネス目的に役立つかも知れない。
   - 組織化または実体によって使われた手順の宣言における生成、それ自身の利益に基づく電子署名の利用と検証
   - 電子署名がその構成によって有効になるように受け入れられる条件の宣言

10.1 署名ポリシーの法的効力

必読要求は、署名ポリシーと署名上の法的効力、それ自身に複雑な法的問題が含まれている。署名ポリシーを読み従うことへの不履行は、契約条件を読み応じることへの不履行と同一行為であり、訴訟で扱われないかもしれない。契約との関連では、多数の司法権で共通した法律の主文であり、取引に付帯する強制的な標準契約や"細字部分"を扱い、必ずしも拘束された当事者によって読まれないかもしれない。

10.2 明示的あるいは明白な署名ポリシー

署名ポリシーは、明示的あるいは明白な方が望ましく、例えば、準拠法や税関に含まれた、あるいは書類の構造に含まれた詳細な規制をセットにした形の方が望ましい。ただし、署名ポリシーは、ユーザーにとって透過的な感覚で、明示的、技術的な実装で組み込まれる。これは、紙社会における個人的な小切手の例に類似している。従って、暗黙の仮定として、署名ポリシーに対するいかなる説明も必要ないかもしれない。

1. 署名ポリシーの例として
   - 銀行小切手に署名する場合
   - 課税ファイリング
   - 公証された書類

10.3 署名ポリシーの草案

署名ポリシーの草案作成のために必要なガイダンスを提供し、異なるビジネスニーズに応じて適当に調整することができる。ただし、すべてのオプションを要求する、というのではなく、ビジネス規則から、オプションの場所を選び、署名ポリシー規則（管理および操作上、と技術的な規則の両方）から対応する規則によって追加するべきである。従って、もし署名ポリシーが対向署名を要求することを示せば、高水準の宣言は、署名ポリシー規則の下位のセットによって追加してもよい。このドキュメントは、このような規則を草案するためのガイドラインを提供している。

1. 大綱

   ポリシーは、基礎的なプロシージャの目標について述べる高水準のプランである。全般的なプロセスの青写真ともいえる。下位のポリシーは、規則またはプロシージャで、どのようにポリシーの目標がなし遂げられるか、または実装されるかを述べる。

2. 要求された事実

   基本的にビジネス業界で簡単には確認できないことやタイムリーな検証等々が要求される可能性がある。また、いくつかの要因を立証することが困難という事実は、必ずしも無視されるということを意味しているわけではない。事実宣言により、事実関係の立証ができる、できないにかかわらず、証拠としての能力を持つ。作成者が作成した宣言文の主張は、事実関係が変わった場合、暗黙的に損失の原因となる恐れがある。また、宣言文を受領した段階

でそれに頼る権利があると考えられる。

3. 署名検証

紙文化で、署名を取り巻く環境は、署名が生成され時点で真実でなければなりない。稀なケースとして、後日、関係者の影響を受けた同意で欠陥が正しく認識されるかもしれない。従って、署名の有効性は、受け取り時間ではなく生成時間でなければなりない。また、署名またはデータのどちらかに信頼される時間を付与しなければならない。

- 依存者の有効性
- 処理過程の部分的な有効性
- 電子文書の完成後の部分的な有効性

10.4 署名ポリシーの重要な要素

ひとつのポリシーで書かれたドキュメントは、大半のビジネスアプリケーションになく、技術的なインプリメンテーションを人の読みやすいポリシードキュメントによって補足されることにより、有益で効果的なソリューションを提供する。従って、デザインされた有益な署名ポリシーは３つのレベルがあり、それぞれ下位レベルを描いてから、そのパラメーターを高次元から思い描く。

- ビジネス商習慣（会社全体）で、ハイレベルな条件配下で電子署名がビジネスで使われる記述
- 署名使用の規則で、管理と操作の両方を一致させた手順、技術的な規則、ビジネス内の詳細プロセスアドレッシング（内部および外部）
- 技術的な仕様

10.4.1 ビジネス規則

ビジネス規則が最も高い水準にセットされ、契約レベルの取引関係間で同意された期間は、内部プロセスの運用と同等に適用されるかもしれない。あるいは実際に取引関係間で、標準ビジネス期間や電子署名に関連したポリシーの参考事項など、実質的な契約の範囲が取り決められるかもしれない。組織によっては、電子署名が使われる背景の規則をセットする以上に責任があるかもしれない。

そこで、こだわる人のために、これらの規則は、電子署名の妥当性受け入れ要求を重視した署名ポリシーにすべきかもしれない。ただし、「署名利用規定」に含めてきたように目的やリファレンス、事柄に埋め込むことで、一体化されるかもしれない。いくつかの事例で、ビジネス規則は、現存する技術的な実装の使用法を明示的に述べる可能性がある。

1. ビジネス規則に含まれる情報を以下に示唆する。
   - 署名ポリシーのタイトル/ID
   - 署名ポリシー発行者

- ビジネスアプリケーションドメイン
- トランザクションの背景
- 電子署名を受け入れるための同意
- 提案された署名者
- オーソリティの証拠
- 署名契約義務タイプ
- 署名の形式
- 強制タイミング
- 前でもなく/後でもない
- 考慮すべきセキュリティ仕様
- "信用"モデル
- 署名の検証/有効性に対する責任の割り当て
- 読者条件
- アクセスコントロール管理
- 紛争解決プロシージャ
- 顧客（消費者）関係と不満
- 会社内部の事件
- 「長年の取引相手との商取引、サプライヤー、販売業者など」
- 決まり文句

10.4.2 署名ポリシー規則

これらの規則はビジネス規則に実装すべきである。ビジネス規則と業務報告がおおよそ類似しているのであれば、実施ステートメントもおおよそ等価である。ここで、ポリシーの配下でどのように署名を生成し、検証すべきか等々考えられる。

1. 管理練習とプロシージャ
   - ビジネス役割への署名特権と属性のアロケーション
   - 属性証明書と識別使用の管理
   - 署名生成トークン、スマートカードなどの使用
   - トークン、スマートカードなどの保管
   - 署名生成プロシージャ（権限付与、署名形式など)、
   - 対向署名の検証と有効性
   - 電子署名の検証データ（適切な場所）のアーカイブと証明
   - 懲戒手順

2. 技術的な規則

これらは通知の実装に関連した技術的な規則である。ビジネス規則の期待値よりも大きなレベルを提供すべきである。それらは専門外の人員によって取り決められたかもしれない。しかしながら、これら規定は、ビジネス規則を企業内で参照することで、先に存在する組織/実体の標準に

関する電子署名が使用される可能性がある。それらは、下記の事項に関連して規則の考察を含んでいるかもしれない。

- 身分証明と署名役割の割付け
- 証明書に関する信頼と使用
- 署名者属性情報の証明
- タイムスタンプ
- 署名属性:

10.5 署名ポリシー規則のイラスト

10.5.1 権限付与の対向署名

適切な規則を考案するために､特定のビジネス/業務処理の背景を備えた対向署名の目的を考慮した事前準備が要求される。なぜ対向署名が要求されるのか？　対向署名者は署名を生成するに先立ってどんなアクションを実行するのか？　対向署名は実際に何を意味するのか？　つまりそれから何が推量されるべきものか？

- 署名者による部分的な処理プロセスの実行した行為を示す
- 署名者の重要な行動あるいは権限の確認
- 他の署名の妥当性の確認?

1．タイムスタンプの検証

2．"主要な"署名の検証/有効性
- 何を調べるべきか?
- 署名者の識別
- 証明書に含まれた識別の照合
- 証明書の状態と有効性
- 証明書により示される署名者の権限
- （包含した）ビジネス職務

3．他のどんなデータをチェックしなければならないか?
- 主要な署名者によって署名されたデータ
- 属性の任意要求
- ビジネスアプリケーションで進む優先出来事
- 署名前の事前有効性結果

4．有効性結果のアーカイブ
- どんな有効性データを保存しなければならないか（規則・セット）？

- 準拠法があるか？
- 有効性データは、C/S によってサインされるべきか？
- タイムスタンプ？
- さらに、有効性結果のアーカイブ規定をセットすべきである
- どこにデータを保存すべきか？
- 誰がアーカイブの責任を負うのか？
- 有効性の保存期間をいつまでにすべきか？
- 要求される安全対策は何か？
- データバックアップの整理は何か？
- アクセス権の保有者は誰か？
- データの情報検索規定

5．対向署名の生成

- 識別（証明書要求の分類）
- 役割/属性（証拠）
- 代表権の権力（実際/要求）
- C/S による宣言
- コミットメント・タイプ（権限付与）
- 署名の形式
- タイムスタンプ

6．何が署名されるべきか？

- 主要な署名
- 主要な署名者によってサインされる既存データ
- 追加データ（オプション）
- C/S（オプション）による宣言

7．主要な署名の基礎的な有効性は？

- 対向署名の有効となる信頼によって：
- 対向署名者によってサインされた有効性結果を調べることで
- 全体の有効性プロセスを繰り返すことで

10.5.2 ドキュメント・フローの対向署名

ここで想定する対向署名は、署名やデータが存在すること以外除いては、優先的に興味を持たないとうことである。(並列署名）このシナリオは、ビジネスアプリケーションに含まれる機能の実行やそれぞれの署名者がデータに追加、加工しているデータの環境を保護するかもしれない。この場合、署名は並列に行われるかもしれない。ただし、直列とのタイミングは重要かもしれない。管理と操作規則は、ひとつの署名に関係があるように類似しているかもしれない。対向署名の順序の有効性とタイムスタンプに関連した問題については、技術的な規則により保護される可

能性がある。

10.5.3 代表権の権限

代表権の権限の配下で生成された署名が受け入れられるかどうかにかかわらず、ポリシー（適切なら）の中で記述する必要がある。あるいはそうでない場合、もしイエスならば、署名ポリシー規則は、どのような条件下で受け入れられるべきかを明言するべきである。

- 実際の権限が付与されなければならない
- 要求された権限が付与されているのか

10.5.4 公証人の署名

公証人は、民事法の公証人（ヨーロッパ人/ラテンアメリカ人）として就任する。北米のタイプの公証人は本質的に専門家としての証言をしない。公証人条例と公証人の要求については、国毎に微妙な差異が認められる。この理由により、どんな署名ポリシーも公証人の署名を必要としていて、国あるいは司法権を明確に述べる必要があるかもしれない。

1. 以下に漠然とした公証人の義務を要約することができる。
   - データ（書類）の法的な正当性を保証しなければならない
   - 署名者には署名する権限がある
   - 意識していることと引き受けている約束を理解する
   - 精神的・法律的に約束できる能力がある
   - 彼らの自由意志でそうする
   - 安全なコミュニケーションの書類/公証人からの
   - 公証の安全なシステム
   - 公証人の署名に関連した安全性
   - 安全なアーカイブ
   - 公証人の署名の永続性
   - アーカイブの永続性

11.結論

下記要約で多くの結論を引き出すことができる。

1. 署名ポリシーは、法的、技術的な両方の署名関する多様な様子を保護することができる。特に、署名ポリシーは電子署名の配下で条件を示した関係団体の代わりによって承認され利用することができるといえる。

2. 意思表示を考慮した上で署名する署名者に対して直接的ではない指示を与える。署名の形式を作る段階、また、署名者が署名を作成したことの否認を不正に試みる機会を最小限にす

るための技術的・手続き的な手段は署名ポリシーに組み入れることができる。

3. 署名ポリシーは、ひとつの署名に関係があるかもしれない。

4. すべての典型的なビジネスモデルに適用される能力のある署名ポリシーは、ひとつの署名（一般的）で書くことはありない。またはすべての状況を取り扱うために複数署名を使ってもよい。

5. 署名ポリシーは、一文書署名（例　TS 101 733）あるいは、一文書上（例　契約書など）の複数署名の有効性に関係するかもしれない。その一方で潜在的に非常に複雑化する可能性があることから、管理している署名のある処理（例えば輸出/輸入管理を含む世界通商処理）や複数段階で要求しているいずれかの取引に影響を与える必要がある。これらのポリシーは、業務処理の署名ポリシーあるいは契約署名ポリシーと命名し、互いに区別するべきかもしれない。

6. 署名ポリシーは、ビジネス規則で構成され、多くの部下による署名を受けたポリシーが共存するかもしれない。

7. 慣例によって再建された電子署名に関連したビジネス規則になるまでは、ビジネス商取引のコースの前文で署名ポリシーの条項に同意し、取引相手に必要なもっともらしい法律によって支持される。

8. 法的見地：署名ポリシーは、普通（契約）条項と同等のビジネス状態と考えてはいけない。それら内容の理解や現実の見識を持っていない、署名者に対して実施できるかもしれない。

9. ビジネスアプリケーション内の自動手段によって実装される場合、署名ポリシーが最も効果的といえる。

11.1 署名ポリシーフォーマットに推奨変更

現在のドキュメントは、複数署名の支配による署名ポリシーの技術的な実装との関連で、可能ならば、基礎提供する以上の働きによってビジネスニーズを調査することで、電子署名フォーマット「ETSI TS 101 733」、署名ポリシーの XML フォーマット「ETSI TR 102 038」を追加するように意図している。いくつかの点で、このドキュメントは以前のドキュメントの状態を支持しないことが明白である。しかし、それら異なる部分については、将来のプロジェクトの結果として容認される可能性が高い。とはいえ、この段階で修正または変更の示唆については、時期尚早かもしれない。

11.2 将来の活動のための推奨

電子署名に焦点を合わせた技術的な報告書は、法的効果を意図している。それは、署名の用途

に関連したビジネス上の問題を明らかにし、それ以上の働きは、電子フォーマットでソリューションを提供する必要がある。また、ビジネスを可能にするには、プロトコル開発の形式をとる以上の働きが推奨される。

- 複数署名の管理に
- 電子署名の提供と条件を受理し､相互運用可能なフォーマットを評価した上で公開する。

このテクニカルレポートは電子商取引のための国際的な意義を持っている。OASIS と ebXML で進行中の本質的に類似したな活動だと仮定すれば、この報告と EESSI がフォーカスしているこの領域が社会から取り残されることのないことが重要である。協調方法について検討する機会が与えられるのであれば、これらのグループと一緒に達成できるかもしれない。

Annex A：ビジネスシナリオ

A.1　概要

本節では、署名のユースケースについて述べる。署名は、下記のように分類される。

- 単一署名（Single）
- 複数署名（Multiple parallel）
- 対向署名（Counter signatures）
- 連続署名（Sequential）
- 上記を複合した署名（Combination of the above）

以下のユースケースが全てとは限らないことに留意されたい。また、ユースケースの説明には、標準記法として UML（Unified Modelling Language）を用いており、開発と運用を関連付けて概要を説明している。

署名を付与している箇所には、UML メッセージ呼び出しの記法で強調している。

A.2　生命保険

本節では、イタリアの生命保険購入について考えている。

A.2.1　ユースケース

アクタは下記の通りである。

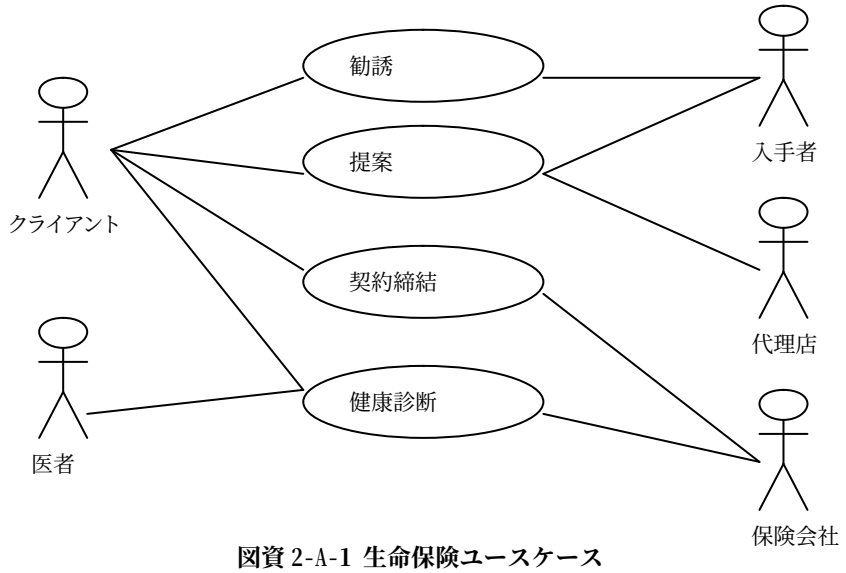
クライアント：保険を購入して病気に備えることを考えている個人。

入手者：代理店からクライアント向け健康保険を入手する組織/個人。

代理店：保険会社から保険商品の販売許可を得ている組織/個人。

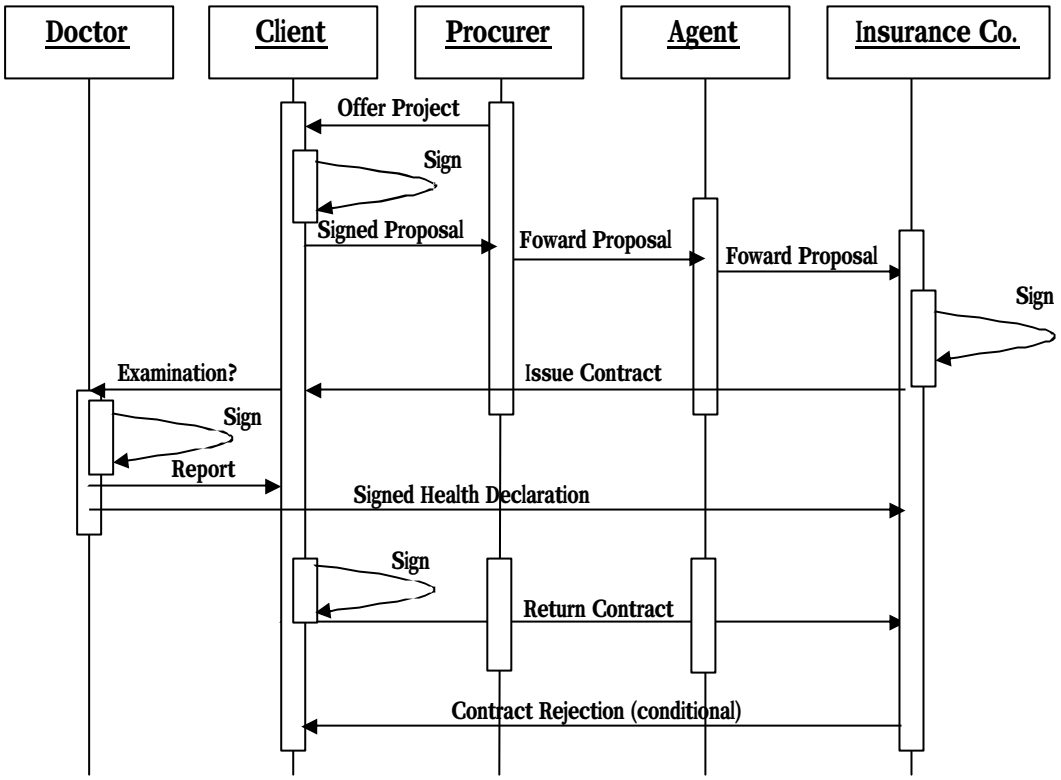
保険会社：保険商品を保有し、原価に対し手数料を付けて価格を設定する組織。

医者：保険会社から依頼を受けて、健康診断を実施する人。



図資 2-A-1 生命保険ユースケース

A.2.2　シーケンス図

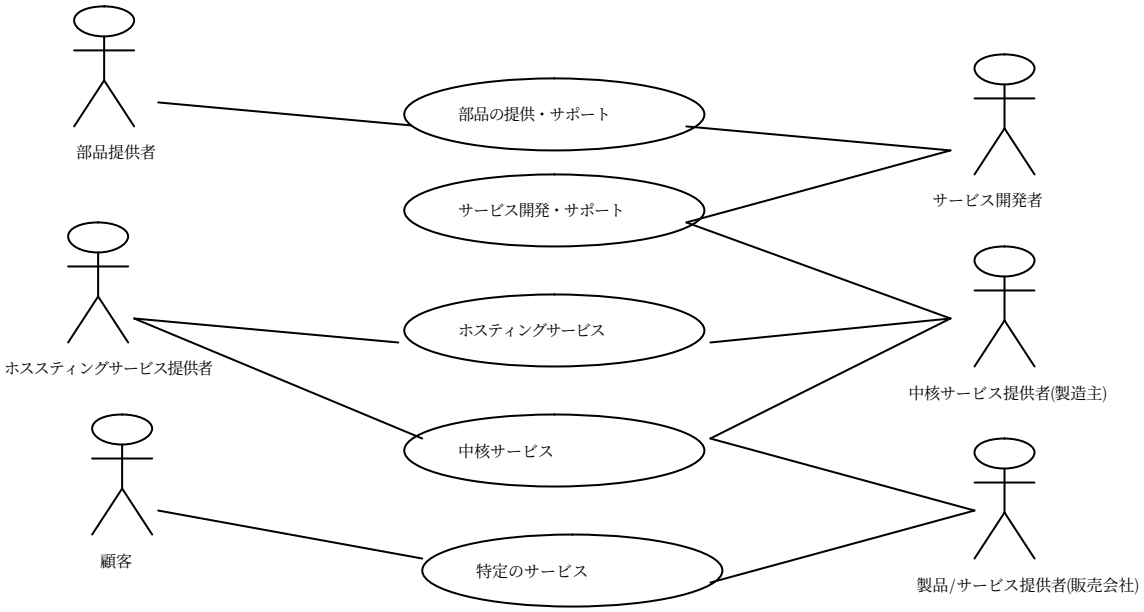


図資 2-A-2 生命保険シーケンス図

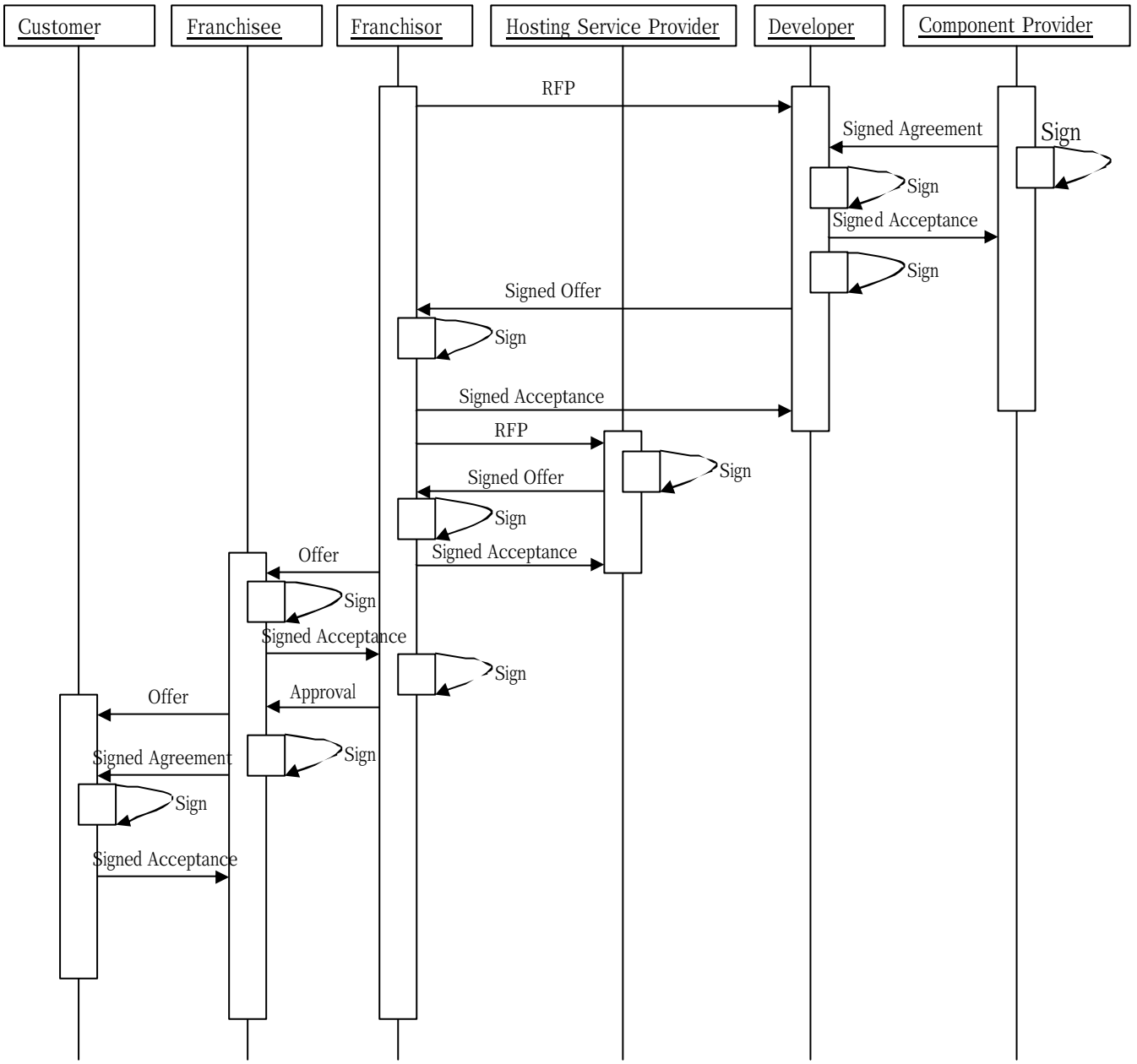
1.入手人（Procurer）は、クライアント（Client）に健康保険を勧誘する。
2.クライアントは、提案書に署名をして、入手人に返送する。
3.署名された提案書は代理人から代理店（Agent）へ転送され、代理店から保険会社（Insurance Co.）に転送される。
4.保険会社は、依頼を受理した後で署名を付与して、契約書を発行する。契約書は代理店および入手人を経由してクライアントに渡される。
5.保険会社が、健康診断を要請する。医者（Doctor）はクライアントの診療を行った後、健康診断書に署名を付与して保険会社に対してプライバシー法のもと送付する。同時にクライアントへは健康診断書のコピーが送付される。
6.クライアントは、入手人や代理店を経由して保険会社に契約書を送付する。
7.もし診察が不要であれば､発病するまで有効期間を延ばすことができる(たとえば 6 ヶ月など)。
8.もし会社が契約を否認する場合、条項によりその契約を拒否することができる。

A.3　サプライチェーン（関連するサービスレベルアグリーメントを経由して説明）

代理店がサービスを顧客に再販するというシナリオを考える。これらのサービスは体系化されており、それゆえ代理店によりサービス提供されるものではない。顧客に最も近いカスタマサポートはアウトソースされている。サービス開発は遠隔地の組織で行われており，代理店へサービスを提供している組織に向けにサポートを行っている。サービス開発部門は，プラットフォームや OS といった部品提供者は，サービス開発部門に対してサポートを行っている。



図資 2-A-3 サプライチェーンユースケース



図資 2-A-4 サプライチェーンシーケンス図

1. **製造主は要件を記してサービス開発者に対して契約を要求する**
2. **サービス開発者は部品提供者とライセンス契約に署名する**
3. **サービス開発者は（交渉済の）申請書に署名を付与して製造主に送付する**
4. **製造主は署名を付与した受諾通知書を返送する**
5. **製造主はホスティングサービスの RFP を発行する**
6. **ホスティングサービス提供者は（交渉済の）申請書に署名を付与して製造主に送付する**
7. **製造主は販売会社にサービスを申し出る**
8. **販売会社は申し出を受けて市場に製品/サービスを提供する準備をする。これにより，製品/サービスは，製造主の認可を受けることになる**
9. **製造主はサービスを調査し，販売会社がサービスを提供できているのであれば販売会社がサ**

ービス提供することを認可する目的で署名を付与する
10．販売会社は、顧客にサービスを勧誘する
11．消費者は販売会社のライセンス契約に署名する

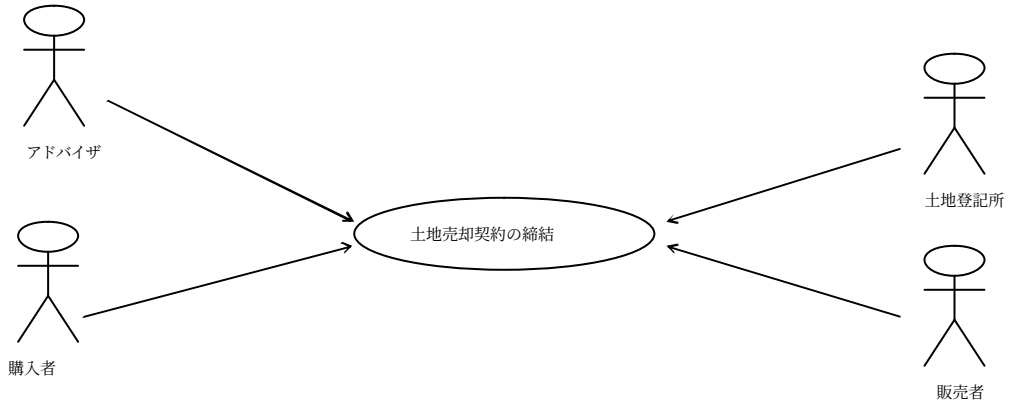
本ユースケースで重要な点は、販売会社が顧客にサービスを勧誘した際に、過去に製造主から販売会社まで組織間でサービス提供が認可されたことを示す署名が付与されていること，およびその署名が有効であることを，顧客が確認できるということである。

A.4　土地購入

本節では、不動産業者の選択、土地の選択、契約交渉を除外して考える。契約の締結は、企業の法務部門により行われると想定する。ユースケースの中核である契約書の交換・締結のための「仕組み」が存在しないという点で、本ユースケースを利用する機会はさらに多くなることであろう。本ユースケースでは組織間の土地取引を想定して，取引成立に対向署名を利用するケースを想定する。

A.4.1　ユースケース

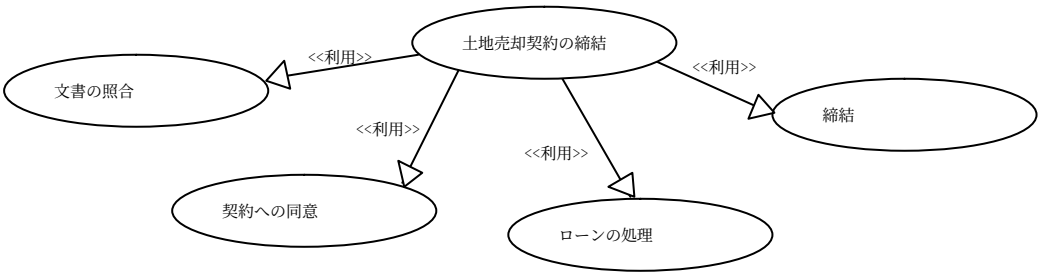
購入者、販売者、アドバイザ、土地登記所（英国のみ）というアクタを考える。購入者には、土地を購入する組織の代表者や証人も含まれる。販売者には、土地を販売する業者の代表者や証人も含まれる。アドバイザには、購入者および販売者それぞれの弁護士、査定代理人、財務顧問、抵当業者も含まれる。図資 2-A-5 は，土地売却契約の締結に関するユースケースとして，システム側から見たユーザに提供する機能について示している。本ユースケースは関連する複数のユースケースから成り，その階層については後述する。



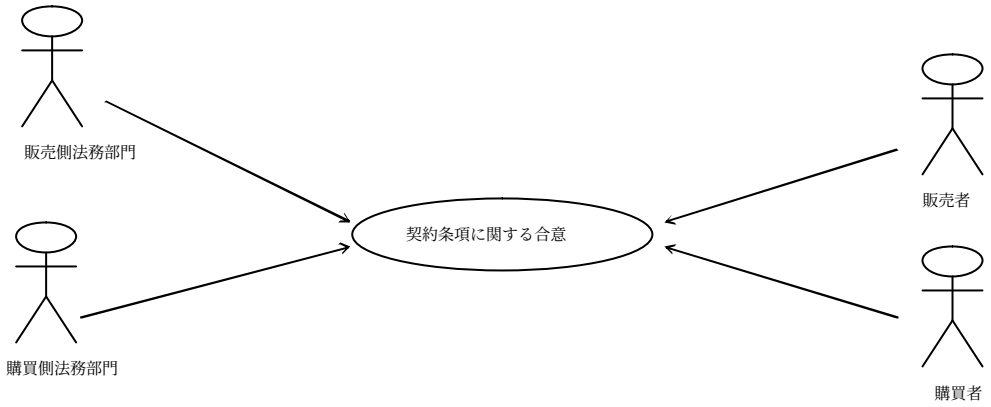
図資 2-A-5 土地売却契約の締結ユースケース

ユースケース名	土地売却契約の締結
イテレーション	Filled.
イベントの基本的な流れ	1）販売側法務部門が契約書を作成して、販売者や購入側法務部門に配布する。 2）販売者と購入者は契約書に署名する。 3）購入者は、土地の担保について交渉する。 4）契約書を取り交わす。 5）合意がとれた時点で契約成立となる。 6）書類を照合した後、土地登記所に必要書類を送付する。
Alternative Paths:	民法が処理
例外パス：	なし
拡張ポイント：	なし
トリガ：	なし
想定：	英国の土地購入
前提条件：	なし
後条件	なし
関連ビジネスルール：	なし
筆者：	Jeremy Hilton/Jane Hill
日付：	August 19, 2002-Facade; August 20, 2002-Filled

図資 2-A-6 に，土地売却契約の締結のユースケース階層を示す。これは，土地売買契約の締結ユースケースが，関連する複数のユースケースから構成されていることを示している。



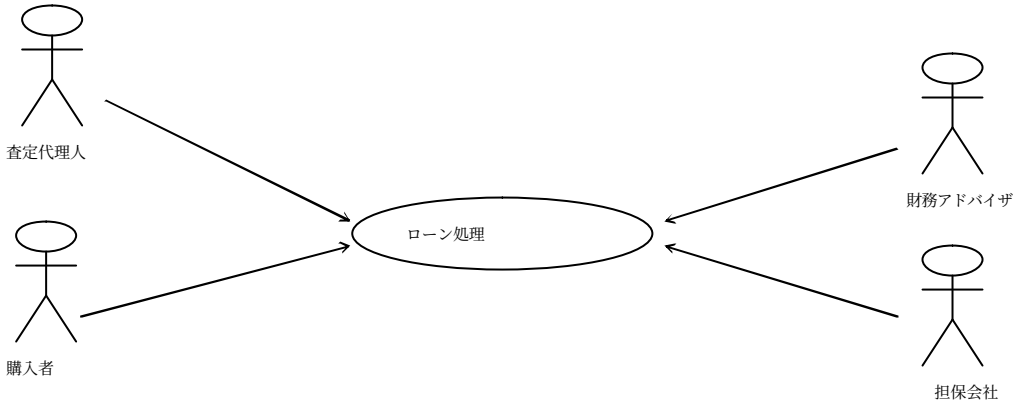
図資 2-A-6 土地売却契約の締結のユースケース階層



図資 2-A-7 契約条項に対する合意ユースケース

ユースケース名：	契約条項に対する合意
イテレーション：	Filled.
要約：	購買者と販売者が販売に関する条項に対して合意する。この条項には，既存の土地，その土地に関係する全項目，所有日，販売に関する財務および他の条件など全て含まれる。
イベントの基本的な流れ：	1）購買者や販売者が、契約条項に対する合意が発生する旨を、各々の法務部門に連絡する。 2）販売側法務部門は、契約書を準備して、そのコピーを販売者および購買側法務部門に送付する。 3）購買側法務部門は契約書を購買者に送付する。 4）販売者１は契約書に署名し，証人によって対向署名をした後、販売者２に送付する。 5）販売者２は契約書に署名し，証人によって対向署名をした後、販売側法務部門に送付する。 6）購買者１は契約書に署名し，証人によって対向署名をした後、購買者２に送付する。 7）購買者２は契約書に署名し，証人によって対向署名をした後、購買側法務部門に送付する。 8）購買側法務部門は、販売側法務部門に契約の合意があったことを通知する。
Alternative Paths：	2）で、購買側法務部門は購買者の申し出を受けて契約を開始する。
例外パス：	3）で、購買者が合意できない契約条項を発見した場合、購買者と販売者は各々の法務部門に申し出を行い、各々の法務部門間で交渉する。修正済の契約に購買者が合意したら、4）に進む。
拡張ポイント：	なし
トリガ：	購買者や販売者が、契約条項に対する合意が発生する旨を申し出る。

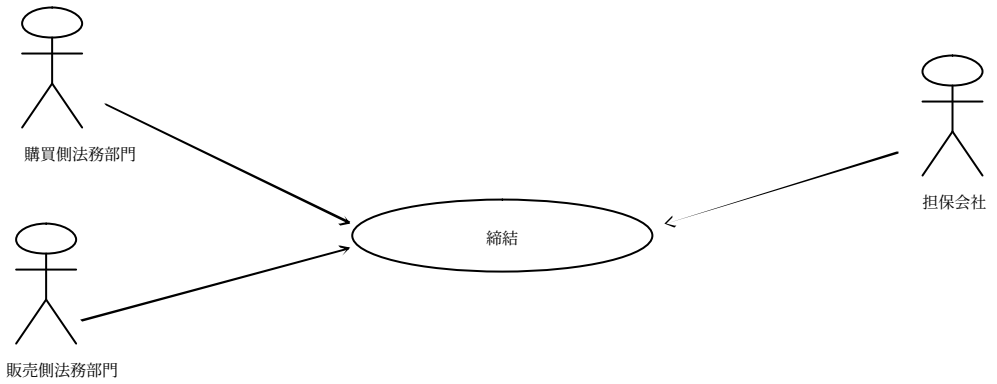
想定：	なし
前提条件：	申し出を受理
後条件	購買者と販売者が契約合意
関連ビジネスルール：	なし
筆者：	Jeremy Hilton/Jane Hill
日付：	August 19, 2002-Facade; August 20, 2002-Filled



図資 2-A-8 ローン処理ユースケース

ユースケース名：	ローン処理
イテレーション：	Filled.
要約：	財務アドバイザ、担保会社および購買者は、ローンに関する条項を購買者が必要とする場合作成する。条項には、関税や、条文、保証などが含まれる。
イベントの基本的な流れ	1）販売者と購入者が契約条項に合意する。 2）購買者は、査定代理人に対し土地価格の査定を要求する。 3）査定代理人は、購入者に対して土地の見積書に署名を付与して送付する。 4）購入者は、財務アドバイザよりローンを要求し、資産の詳細、利用可能な資金と必要な資金および希望する条項について説明する。 5）財務アドバイザは、担保会社および関連するローンの提案を行う。 6）購入者は、財務アドバイザを介して担保会社と交渉する。 7）担保会社は、購入者に対して申し出を行う。 8）購入者は、ローンを受諾する。
Alternative Paths:	6）で購入者が初期提案を受諾した場合、8）に進む。
例外パス：	5）でローンの提案がない場合、購入者は 4）に戻り、代替の財務アドバイザを探すか、代替の担保会社を探すか、申し出をキャンセルするかのいずれかを行うことができる。

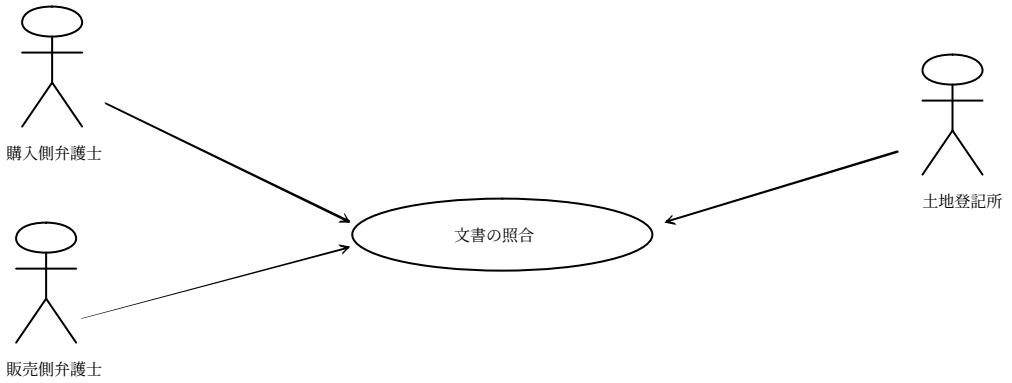
拡張ポイント：	なし
トリガ：	購入者が融資を要求し，ローン探しを行う
想定：	なし
前提条件：	購入者が融資を要求する
後条件	ローンが受諾され記録される
関連ビジネスルール：	なし
筆者：	Jeremy Hilton/Jane Hill
日付：	August 19, 2002-Facade; August 20, 2002-Filled



図資 2-A-9 締結ユースケース

ユースケース名：	締結
イテレーション：	Filled.
要約：	購買側法務部門と販売側法務部門が契約成立したことに合意してから、融資金が譲渡される。購買側法務部門は販売側部門に対して譲渡証書を送る。両方の販売者はその譲渡証書に署名し、両方の販売者の証人となる。購入者に譲渡証書が返送される。購入者と販売者の間で契約成立日を設定することができる。
イベントの基本的な流れ	1）購入側法務部門と販売側法務部門は、共に契約が成立して署名が付与されていることを確認する。 2）販売側法務部門は、融資が可能であることを確認する。 3）購入側法務部門と販売側法務部門との間で契約の交換が行なわれ、購入者と販売者にその内容が伝えられる。 4）購入者と販売者の間で契約成立日を合意する。 5）譲渡証書は購入側法務部門により準備され、販売側法務部門に送付した後、販売者に送付される。 6）譲渡証書は販売者により証人署名で署名され、販売側法務部門に送付した後、購入側法務部門に返送される。 7）満期日には締結が行われ、必要書類が土地登記所に送付され、担保会社に土地が譲渡される。

Alternative Paths：	なし
例外パス：	3）で、購買側法務部門と販売側法務部門との間で合意がなかった場合、購買側と販売側の両方に通知された上で、取引は中止される。
拡張ポイント：	なし
トリガ：	購入者と販売者が、締結が発生する旨を申し出る
想定：	なし
前提条件：	購入者と販売者とで条項に合意する。購入者の資金源は保証される
後条件	満期が発生して所有権が譲渡される
関連ビジネスルール：	なし
筆者：	Jeremy Hilton/Jane Hill
日付：	August 19, 2002-Facade; August 20, 2002-Filled

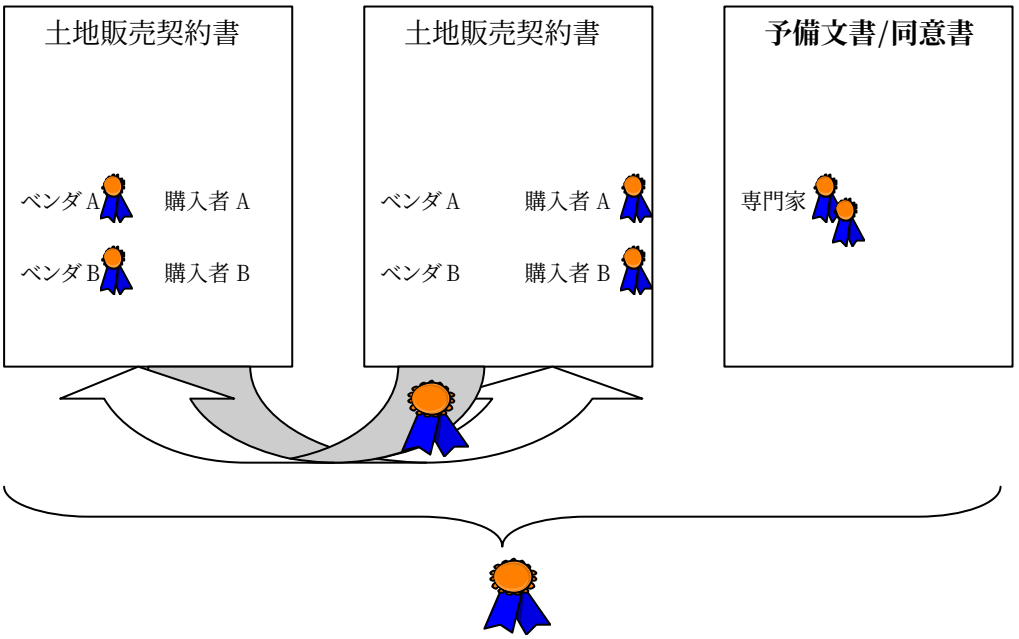


図資 2-A-10 文書の照合ユースケース

ユースケース名：	文書の照合。
イテレーション：	Filled.
要約：	文書を収集し，満期の印を付けて保管する。
イベントの基本的な流れ	1）販売側法務部門は、販売者により署名された契約書のコピー、購入者により署名された契約書のコピー、他の関連文書を収集する。 2）販売者の文書一式は、満了を示すために署名され、（A.4.2 のように）保管される。 3）購買側法務部門は、販売者に署名された契約書のコピー、購入者により署名された契約書のコピー、ローンの合意のある査定書および他の関連文書を収集する。 4）購買側の文書一式は、満了を示すために署名され、保管される。
Alternative Paths:	なし
例外パス：	なし
拡張ポイント：	なし
トリガ：	満期が発生

想定：	**なし**
前提条件：	**満期が発生**
後条件	**取引完了**
関連ビジネスルール：	**なし**
筆者：	Jeremy Hilton/Jane Hill
日付：	August 19, 2002-Facade; August 20, 2002-Filled

A.4.2 文書一式



DIRECTIVE 1999/93/EC

これまでの文献調査の中では、以下の文献（以後、DIRECTIVE）の参照が行われている場合がある。

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

文献調査において DIRECTIVE への参照が多く行われていることから難解な部分があるため、本節においては、特に DIRECTIVE が参照されている箇所（二条、五条、及び付属書Ⅰ）の内容を示す。

なお、DIRECTIVE の記述にあたり、神戸大学大学院法学研究科の米丸恒治教授の承諾を得て以下のサイトより引用している。すべての内容を把握したい場合には、以下を参照願う。

http://www.ritsumei.ac.jp/acd/cg/law/lex/99-6/yonemaru.htm

電子署名のための共同体の枠組に関する一九九九年一二月一三日の欧州議会および欧州連合理事会の指令 1999／93／EC

〔定義〕

第二条　本指令においては、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一 「電子署名」　別の電子データに付加されまたは論理的にそれと結びつけられておりかつ真正確認の方法として用いられる電子的形式のデータ

二 「先進電子署名」　以下の要件を満たす電子署名
それがもっぱら署名者のみに帰属させられており、
署名者の同一性確認が可能であり、
署名者がその唯一の統制の下に保持することのできる手段により作成されており、
事後的なデータの変更を認識させ得るように、その関連するデータにリンクされている。

三 「署名者」　署名作成装置を所持しかつ自らの名前でか、またはそれが代表する機関または法人もしくは自然人の名前で行動する者

四 「署名作成データ」　署名者により電子署名の作成のために利用されるコードまたは私的暗号キーのような唯一のデータ

五 「署名作成装置」　署名作成データの具現のために利用される設定されたソフトウェアまたはハードウェア

六 「安全署名作成装置」　付属書Ⅲの要求事項を満たす署名作成装置

七 「署名検証データ」　電子署名の検証のために使われる、コードまたは公開暗号キーのようなデータ

八 「署名検証装置」　署名検証データの具現のために使われる設定されたソフトウェア

またはハードウェア

九 「証明証」ある者の署名検証データに関連させられかつその者の同一性を確認する電子的証明

一〇 「適格証明証」　付属書Ⅰに定める要求事項に適合する証明証を意味し、かつ付属書Ⅱに定める要求事項を充足する認証サービスプロバイダにより発行されているもの

一一 「認証サービスプロバイダ」　証明証を発行しまたは電子署名に関連するその他のサービスを提供する機関または法人もしくは自然人

一二 「電子署名製品」　認証サービスプロバイダにより電子署名サービスの提供のために利用されるよう意図された、または電子署名の作成または検証のために用いられることを意図されたハードウェアもしくはソフトウェアまたはそれらの一部

一三 「任意認定（voluntary accreditation）」　特殊に認証サービスの提供のための権利および義務を課すあらゆる許認可で、当該認証サービスプロバイダの申請に基づいて与えられ、かかる権利および義務の細目を定めかつそれら権利義務の遵守を監督する権限を与えられた公共団体または私的団体により与えられるものを意味し、認証サービスプロバイダが当該許認可団体による決定を受けるまでは許認可から生じる権利を行使する資格が与えられない場合のそれ。

〔電子署名の法的効果〕

第五条　構成国は、適格証明証に基づきかつ安全署名作成装置により作成された先進電子署名が、次の各号の条件をみたすよう確保するものとする。

(a) 手書き署名が紙ベースのデータに関連して求められる要件を満足するのと同様に、電子的形式でのデータに関して署名の法的要件を満足させること、および

(b) 法的な争訟手続において証拠として認められること。

(2) 構成国は、電子署名がもっぱら次の理由に基づいて法的効果および法的争訟手続きにおける証拠としての承認を否定されないことを確保するものとする。それが、

－電子的形式をとっていること、または

－適格証明証に基づいていないこと、または

－認定認証サービスプロバイダによって発行された適格証明証に基づいていないこと、または

－安全署名作成装置により作成されていないこと。

付属書Ⅰ　適格証明証の要求事項

適格証明証は、次の各号を含まなければならない。

(a) 証明証が適格証明証として発行されたことの表示

(b) 認証サービスプロバイダおよびその設立された国の表示

(c) 同一確認されるべき署名者の氏名または仮名

(d) 証明証の意図された目的にかかわり、関連するものであれば含まれるべき、署名者の特殊な属性の条項

(e) 署名者の統制の下にある署名作成データに対応する署名検証データ

(f) 証明証の有効期間の始期と終期の表示
(g) 証明証の特定（ID）コード
(h) 証明証を発行する認証サービスプロバイダの先進電子署名
(i) 適用可能であれば、証明証の使用範囲についての限定、および
(j) 適用可能であれば、証明証が使われ得る目的となる取引の価額についての限定

付属書Ⅲ　安全署名作成装置の要求事項

1. 安全署名作成装置は、適切な技術的および手続的な手段によって、少なくとも次の各号を確保しなければならない。
   (a) 署名の生成に利用される署名作成データが、実際上一回のみ作成され、かつその秘密が合理的に確保されていること、
   (b) 署名の生成に利用される署名作成データが、合理的な保証のもとに、推定されることができず、かつ署名が現在利用可能な技術を用いた偽造から保護されていること、
   (c) 署名の生成に利用される署名作成データが、他人の利用に対して、正当な署名者により確実に保護され得ること、
2. 安全署名作成装置は、署名されるデータを変更してはならず、またはかかるデータが署名手続きの前に署名者に明らかにされることを禁じてはならない。

資料３

RFC3125,“Electronic Signature Policies”

原文において、次に示す章の要約を記す。

原文	要約
3. Signature Policy Specification	3. 署名ポリシー仕様
3.1 Overall ASN.1 Structure	3.1 署名ポリシー
3.2 Signature Validation Policy	3.2 署名検証ポリシー
3.3 Common Rules	3.3 共通規則
3.4 Commitment Rules	3.4 コミットメント規則
3.5 Signer and Verifier Rules	3.5 署名者・検証者規則
3.6 Certificate and Revocation Requirements	3.6 署名用証明書信頼条件
3.7 Signing Certificate Trust Conditions	3.6 署名用証明書信頼条件
3.8 Time-Stamp Trust Conditions	3.7 タイムスタンプ信頼条件
3.9 Attribute Trust Conditions	3.8 属性信頼条件
3.10 Algorithm Constraints	3.9 アルゴリズム制約
3.11 Signature Policy Extensions	3.10 拡張

3．署名ポリシー仕様（Signature Policy Specification）

RFC3125 の Electronic Signature Policies では、ASN.1 を使用して、プログラムで動的に制御可能な署名ポリシーの形式を規定している。

3.1 署名ポリシー（SignaturePolicy）

```
SignaturePolicy ::= SEQUENCE {
        signPolicyHashAlg    AlgorithmIdentifier,
                                                -- ハッシュアルゴリズム
        signPolicyInfo       SignPolicyInfo,
                                                -- 署名ポリシー情報
        signPolicyHash       SignPolicyHash  OPTIONAL
                                                -- ハッシュ値
}
```

signPolicyHashAlg には、署名ポリシーを保護するためのハッシュアルゴリズムが示される。

signPolicyHash には、発行者-署名者間または発行者-検証者間で署名ポリシーが交わされる時に必ず再計算して確認しなければならないハッシュ値が示される（オプション）。

```
SignPolicyInfo ::= SEQUENCE {
        signPolicyIdentifier        SignPolicyId,
                                                -- 署名ポリシーOID
        dateOfIssue                 GeneralizedTime,
                                                -- ポリシー発効日
        policyIssuerName            PolicyIssuerName,
                                                -- ポリシー発行者名
        fieldOfApplication          FieldOfApplication,
                                                -- 適用分野
        signatureValidationPolicy   SignatureValidationPolicy,
                                                -- 署名検証ポリシー（4.3.2）
        signPolExtensions           SignPolExtensions  OPTIONAL
                                                -- 拡張（4.3.10）
}

SignPolicyId ::= OBJECT IDENTIFIER

PolicyIssuerName ::= GeneralNames

FieldOfApplication ::= DirectoryString
```

fieldOfApplication には、この署名ポリシーの適用が期待される分野が示される。

3.2 署名検証ポリシー（SignatureValidationPolicy）

```
SignatureValidationPolicy ::= SEQUENCE {
        signingPeriod       SigningPeriod,
                                                -- ポリシー適用日
        commonRules         CommonRules,
                                                -- 共通規則（4.3.3）
        commitmentRules     CommitmentRules,
                                                -- コミットメント規則（4.3.4）
        signPolExtensions   SignPolExtensions  OPTIONAL
                                                -- 拡張（4.3.10）
}
```

署名検証ポリシーには、署名者が検証者に提示する電子署名に存在しなければならない署名者のためのデータ要素と、検証者が電子署名を有効と見なすために電子署名に存在しなければならない検証者のためのデータ要素が示される。

```
SigningPeriod ::= SEQUENCE {
        notBefore       GeneralizedTime,
                                                -- ポリシー適用開始日
        notAfter        GeneralizedTime OPTIONAL }
                                                -- ポリシー適用終了日
```

SigningPeriod には、署名を生成するために、これ以前とこれ以降に署名ポリシーを使用すべきではない任意の日時が示される。

3.3 共通規則（CommonRules）

```
CommonRules  ::= SEQUENCE {
        signerAndVeriferRules       [0] SignerAndVerifierRules  OPTIONAL,
                                                -- 署名者・検証者規則（4.3.5）
        signingCertTrustCondition   [1] SigningCertTrustCondition  OPTIONAL,
                                                -- 署名用証明書信頼条件
 (4.3.6)
        timeStampTrustCondition     [2] TimestampTrustCondition  OPTIONAL,
                                                -- タイムスタンプ信頼条件
                                                                (4.3.7)
        attributeTrustCondition     [3] AttributeTrustCondition  OPTIONAL,
                                                -- 属性信頼条件（4.3.8）
        algorithmConstraintSet      [4] AlgorithmConstraintSet  OPTIONAL,
                                                -- アルゴリズム制約（4.3.9）
        signPolExtensions           [5] SignPolExtensions  OPTIONAL
                                                -- 拡張（4.3.10）
}
```

共通規則には、すべてのコミットメントタイプ（4.3.4 参照）に共通な規則が示される。

もし、共通規則に以下の領域が存在するならば、その時はコミットメント規則（4.3.4）に同等な領域が存在してはいけない。もし、共通規則に以下の領域が存在しないのであれば、その時は

コミットメント規則に存在しなければならない。

* signerAndVeriferRules　：署名者・検証者規則
* signingCertTrustCondition：署名用証明書信頼条件
* timeStampTrustCondition　：タイムスタンプ信頼条件

3.4 コミットメント規則（CommitmentRules）

```
CommitmentRules ::= SEQUENCE OF CommitmentRule

CommitmentRule  ::= SEQUENCE {
        selCommitmentTypes              SelectedCommitmentTypes,
                                                -- コミットメントタイプ
        signerAndVeriferRules       [0] SignerAndVerifierRules  OPTIONAL,
                                                -- 署名者・検証者規則（4.3.5）
        signingCertTrustCondition   [1] SigningCertTrustCondition  OPTIONAL,
                                                -- 署名用証明書信頼条件
 （4.3.6）
        timeStampTrustCondition     [2] TimestampTrustCondition  OPTIONAL,
                                                -- タイムスタンプ信頼条件
                                                                （4.3.7）
        attributeTrustCondition     [3] AttributeTrustCondition  OPTIONAL,
                                                -- 属性信頼条件（4.3.8）
        algorithmConstraintSet      [4] AlgorithmConstraintSet  OPTIONAL,
                                                -- アルゴリズム制約（4.3.9）
        signPolExtensions           [5] SignPolExtensions  OPTIONAL
                                                -- 拡張（4.3.10）
}
```

コミットメント規則には、特定のコミットメントタイプに適用する規則が示される。

```
SelectedCommitmentTypes ::= SEQUENCE OF CHOICE {
        empty                           NULL,
        recognizedCommitmentType        CommitmentType }

CommitmentType ::= SEQUENCE {
        identifier                  CommitmentTypeIdentifier,
        fieldOfApplication      [0] FieldOfApplication OPTIONAL,
        semantics               [1] DirectoryString OPTIONAL }
```

CommitmentType には、適用分野内でのコミットメントの明確な使用法および意味が示される。

3.5 署名者・検証者規則（SignerAndVerifierRules）

```
SignerAndVerifierRules ::= SEQUENCE {
        signerRules     SignerRules,
                                                -- 署名者規則
        verifierRules   VerifierRules
                                                -- 検証者規則
}
```

署名者・検証者規則には、[ES-FORMATS] で定義された電子署名のフォーマットに対して署名者が付与しなければならない情報と検証者が付与しなければならない情報が示される。

```
SignerRules ::= SEQUENCE {
        externalSignedData              BOOLEAN  OPTIONAL,
                                                -- 署名対象データの場所
        mandatedSignedAttr              CMSAttrs,
                                                -- 必須の CMS 署名属性
        mandatedUnsignedAttr            CMSAttrs,
                                                -- 必須の CMS 非署名属性
        mandatedCertificateRef    [0] CertRefReq  DEFAULT signerOnly,
                                                -- 必須の証明書リファレンス
        mandatedCertificateInfo   [1] CertInfoReq  DEFAULT none,
                                                -- 必須の証明書情報
        signPolExtensions         [2] SignPolExtensions  OPTIONAL
                                                -- 拡張 (4.3.10)
}

CMSattrs ::= SEQUENCE OF OBJECT IDENTIFIER

CertRefReq ::= ENUMERATED {
                                signerOnly (1),
                                                -- 署名者証明書のリファレンス
                                fullpath (2)
                                                -- トラストポイントまでの認証
                                                   パス上証明書のリファレンス
                                                }

CertInfoReq ::= ENUMERATED {
                                none (0)        ,
                                                -- 必須条件なし
                                signerOnly (1)  ,
                                                -- 署名者証明書
                                fullpath (2)
                                                -- トラストポイントまでの認証
                                                   パス上の証明書
                                                }
```

externalSignedDate には、署名者が署名対象データを CMS（Cryptographic Message Syntax）の eContent 内に含めなければならないかが示される（オプション）。

mandatedSignedAttr には、署名者が CMS の署名属性に追加しなければならない属性情報が示される。

mandatedUnsignedAttr には、署名者が CMS の非署名属性に追加しなければならない属性情報が示される。

mandatedCertificaterRef には、署名者が署名者証明書のリファレンスまたはトラストポイントまでの認証パス上の証明書のリファレンスを追加しなければならないかが示される。リファレンスとは、RFC2634（ESS）で定義されている SigningCertificate のことである。

mandatedCertificateInfo には、署名者が署名者証明書またはトラストポイントまでの認証パス上の証明書を追加しなければならないかが示される。

```
VerifierRules ::= SEQUENCE {
        mandatedUnsignedAttr    MandatedUnsignedAttr,
                                                -- 必須の CMS 非署名属性
        signPolExtensions       SignPolExtensions  OPTIONAL
                                                -- 拡張（4.3.10）
}

MandatedUnsignedAttr ::=  CMSAttrs

CMSattrs ::= SEQUENCE OF OBJECT IDENTIFIER
```

MandatedUnsignedAtter には、CMS の非署名属性に追加しなければならない属性情報が示される。もし、署名者が追加しない場合は、検証者が追加しなければならない。

3.6 署名用証明書信頼条件（SigningCertTrustCondition）

```
SigningCertTrustCondition ::=   SEQUENCE {
        signerTrustTrees    CertificateTrustTrees,
                                                -- 証明書信頼ツリー（署名用）
        signerRevReq        CertRevReq
                                                -- 証明書失効要件（署名用）
}
```

署名用証明書信頼条件には、署名用証明書の検証において証明書を有効と見なすための制約条件と失効要件が示される。なお、CertificateTrustTree および CerRevRep は、タイムスタンプ信頼条件（4.3.7）および属性信頼条件（4.3.8）でも使用される。

```
CertificateTrustTrees ::=   SEQUENCE OF CertificateTrustPoint

CertificateTrustPoint ::= SEQUENCE {
        trustpoint                Certificate,
                                                -- トラストポイント
                                                      （CA の自己署名証明書）
        pathLenConstraint     [0] PathLenConstraint   OPTIONAL,
                                                -- パス長制約
        acceptablePolicySet   [1] AcceptablePolicySet OPTIONAL,
                                                -- 受け入れ可能ポリシーセット
```

```
        nameConstraints       [2] NameConstraints      OPTIONAL,
                                                       -- 名前制約
        policyConstraints     [3] PolicyConstraints    OPTIONAL
                                                       -- ポリシー制約
}
```

pathLenConstraint には、１つ以上の CA 証明書によって構成される認証パスの長さが示される（オプション）。

acceptablePolicySet には、認証パス上の CA 証明書の証明書ポリシーに対して受け入れ可能な証明書ポリシーが示される（オプション）。

nameConstraints には、認証パス上の続く CA 証明書の主体者名に対する許可された名前のサブツリーまたは除外された名前のサブツリーが示される（オプション）。

policyConstraints には、認証パス上の CA 証明書の証明ポリシーに対するポリシーマッピング処理を行なう際のパス長が示される（オプション）。

```
CertRevReq ::= SEQUENCE {
        endCertRevReq         RevReq,
                                                       -- エンド証明書失効要件
        caCerts          [0]  RevReq
                                                       -- CA 証明書失効要件
}

RevReq ::= SEQUENCE  {
        enuRevReq  EnuRevReq,
        exRevReq    SignPolExtensions OPTIONAL}

EnuRevReq  ::= ENUMERATED {
        clrCheck         (0),
        ocspCheck        (1),
        bothCheck        (2),
        eitherCheck      (3),
        noCheck          (4),
        other            (5)
          }
```

CertRevReq には、エンド証明書（署名用証明書、TSA 証明書、属性証明書）および CA 証明書の有効検証の方法が（0）CRL、（1）OCSP、（2）OCSP と CRL、（3）OCSP または CRL、（4）チェックなし、（5）その他の方法のいずれかで示される。

3.7 タイムスタンプ信頼条件（TimeStampTrustCondition）

```
TimestampTrustCondition ::= SEQUENCE {
        ttsCertificateTrustTrees   [0] CertificateTrustTrees  OPTIONAL,
                                                       -- 証明書信頼ツリー（TSA）
        ttsRevReq                  [1] CertRevReq  OPTIONAL,
                                                       -- 証明書失効要件（TSA）
        ttsNameConstraints         [2] NameConstraints  OPTIONAL,
                                                       -- 名前制約（TSA）
```

```
        cautionPeriod               [3] DeltaTime   OPTIONAL,
                                                    -- 警告時点
        signatureTimestampDelay     [4] DeltaTime   OPTIONAL
                                                    -- タイムスタンプ生成許容期間
}
```

タイムスタンプ信頼条件には、署名付き電子文書に付与されたタイムスタンプを有効と見なすための条件が示される。

ttsNameConstraints には、ttsCertificateTrustTrees 内で定義されている名前制約に対する追加の名前制約が示される（オプション）。

cautionPeriod には、鍵の有効性について高い確信を得るために、失効情報を入手するまでに待たなければならない時間が示される（オプション）。

signatureTimestampDelay には、署名生成時刻からタイムスタンプ生成時刻までの許容時間が示される（オプション）。

3.8 属性信頼条件（AttributeTrustCondition）

```
AttributeTrustCondition ::= SEQUENCE {
        attributeMandated               BOOLEAN,
                                                    -- 属性指定
        howCertAttribute                HowCertAttribute,
                                                    -- 属性種別
        attrCertificateTrustTrees   [0] CertificateTrustTrees  OPTIONAL,
                                                    -- 証明書信頼ツリー（AA）
        attrRevReq                  [1] CertRevReq  OPTIONAL,
                                                    -- 証明書失効要件（AA）
        attributeConstraints        [2] AttributeConstraints  OPTIONAL
                                                    -- 属性制約
}

HowCertAttribute ::= ENUMERATED {
        claimedAttribute        (0),
        certifiedAttribtes      (1),
        either                  (2) }

AttributeConstraints ::= SEQUENCE {
        attributeTypeConstarints        [0] AttributeTypeConstraints
                                            OPTIONAL,
                                            -- 属性型制約
        attributeValueConstarints       [1] AttributeValueConstraints
                                            OPTIONAL }
                                            -- 属性値制約
```

属性信頼条件には、署名付き電子文書に付与された属性を有効と見なすための条件が示される。AttributeTrustCondition が存在しない場合、どんなに認証された属性であっても、有効とは見なされない。

howCertAttribute には、属性が、署名者が主張した認証されていない属性（例えば X.501 の属性）であるか、認証された属性（例えば X.509 の属性証明書）であるか、[ES-FORMATS]（RFC3126

の 3.12.3 節）が規定している署名者の属性であるかが示される。

3.9 アルゴリズム制約（AlgorithmConstraintSet）

```
AlgorithmConstraintSet ::= SEQUENCE {
        signerAlgorithmConstraints    [0] AlgorithmConstraints OPTIONAL,
                                                -- アルゴリズム制約（署名者）
        eeCertAlgorithmConstraints    [1] AlgorithmConstraints OPTIONAL,
                                                -- アルゴリズム制約
                                                        （EE 証明書発行者）
        caCertAlgorithmConstraints    [2] AlgorithmConstraints OPTIONAL,
                                                -- アルゴリズム制約
                                                        （CA 証明書発行者）
        aaCertAlgorithmConstraints    [3] AlgorithmConstraints OPTIONAL,
                                                -- アルゴリズム制約（AA）
        tsaCertAlgorithmConstraints   [4] AlgorithmConstraints OPTIONAL
                                                -- アルゴリズム制約（TSA）
}

AlgorithmConstraints ::= SEQUENCE OF AlgAndLength

AlgAndLength ::= SEQUENCE {
        algID           OBJECT IDENTIFIER,
                                                -- アルゴリズム ID
        minKeyLength    INTEGER         OPTIONAL,
                                                -- 最小鍵長
        other           SignPolExtensions OPTIONAL
                                                -- その他拡張（4.3.10）
                }
```

アルゴリズム制約には、各エンティティが使用する鍵アルゴリズムとその最小鍵長が示される（オプション）。

3.10 拡張（SignPolExtensions）

```
SignPolExtensions ::= SEQUENCE OF SignPolExtn

SignPolExtn ::= SEQUENCE {
        extnID      OBJECT IDENTIFIER,
                                                -- 拡張 ID
        extnValue   OCTET STRING
                                                -- 拡張値
}
```

拡張は、署名ポリシーの様々な箇所で使用することができる。OID とその値で指定する（オプション）。

メンバーリスト

事務局

川松　和成　電子商取引推進協議会　主席研究員
前田　陽二　電子商取引推進協議会　主席研究員
松山　博美　電子商取引推進協議会　主席研究員

顧問

松本　　勉　横浜国立大学大学院
平田　健治　大阪大学大学院

リーダー

宮崎　一哉　三菱電機株式会社
櫻井　徹　　株式会社 NTT データ
木村　道弘　日本電気株式会社

TF5 メンバー（編集メンバー）

氏名	会社名
磐城　洋介	NTT コムウェア株式会社
野村　　進	NTT コミュニケーションズ株式会社
手塚　優	エントラストジャパン株式会社
上畑　正和	セイコーインスツルメンツ株式会社
雨宮　隆征	セイコーインスツルメンツ株式会社
秋山　将	日本電信電話株式会社
高村　昌興	株式会社 NTT データ
本多　義則	株式会社日立製作所
久保寺　範和	日本電気株式会社
吉川　信雄	富士通株式会社

SWG3 メンバー（参加メンバー）

氏名	会社名
鈴木　優一 ＊	エントラストジャパン株式会社
溝上　卓也	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社
河田　悦生	株式会社 NTT ドコモ
関野　公彦 ＊	株式会社 NTT ドコモ
西田　真	大日本印刷株式会社
近藤　哲生	シャチハタ株式会社
植木　格郎	東京電力株式会社
藤川　真樹	綜合警備保障株式会社
小林　太	株式会社帝国データバンク
相原　敬雄	日本ベリサイン株式会社
尾中　壱行	日本信販株式会社
野口　雄治	日本認証サービス株式会社
柿崎　竜人	NTT コムウェア株式会社
川城　三治	グローバルフレンドシップ株式会社
日向　一人	富士電機株式会社
石原　達也	株式会社東芝

（注）＊はオブザーバー

平成 15 年度　経済産業省　委託事業
ＥＣ技術基盤の相互運用性に関する調査研究事業
（電子署名生成・検証システムのセキュリティ環境の
標準化等調査）
署名ポリシー調査報告書
平成 16 年３月発行

発行所　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館３階
TEL：03(3436)7500
印刷所　新高速印刷株式会社
東京都港区新橋 5-8-4
TEL：03(3437)6365

この資料は再生紙を使用しています。