属性証明のあり方

平田健治

はじめに

電子署名制度ないし公開鍵基盤は、リアルの世界の本人性確認をデジタル情報のみで実現しようとするものである。しかし、現実のリアルな世界での取引は、抽象的な主体同士の行為ではありえず、必ず何らかの資格ないし権限を前提として行われる。例えば、当該売買取引をそれぞれの組織を代表して行う権限ないし資格である。このような資格ないし権限をバーチャルな世界でもデジタル情報のみで実現しようとするのが、いわゆる属性証明であり、そのための手段が属性証明書[1]と呼ばれる。

もっとも、現段階では、本人性証明の手段である公開鍵証明書ないし公開鍵基盤自体すらビジネスの世界に浸透しているとは言い難いため、公開鍵基盤を前提とした属性証明スキームの問題は多分に将来的要素を含んでいる。とはいえ、既にこれに関する実験プロジェクトや製品も出始め、標準化を議論する団体[2]では、そのスキームを検討したものが出つつある。本稿は、この、法的世界と技術的世界が結び会う先端的領域につき、法的観点に重点を置

（阪大法学）53（1-27）27〔2003.5〕

いて検討するものである。[3]

作業としては、国際電気通信連合国際標準規格検討部門、インターネット・タスクフォース、ヨーロッパ電気通信標準化機構が出した四つの文書[4]を比較検討する。

Ⅰ　X.509

この勧告文書は、表題「デイレクトリ　―　公開鍵証明書と属性証明書のフレイムワークス」が示すように、構造化された情報の管理スキーム（これをディレクトリ[5]と呼ぶ）に公開鍵基盤等を付け加えることでより信頼性のあるものとする汎用的な試みである。第一章一般、第二章公開鍵証明書フレイムワーク、第三章属性証明書フレイムワーク、第四章両フレイムワークのディレクトリ上での利用[6]となっているが、以下では、本稿の対象と対応する、属性証明書を扱う第三章[7]を要約的に紹介する。

権限とエンティティ[8]の関連づけは、属性証明書による場合と拡張領域を含む公開鍵証明書による場合がある。属性証明書による場合は、属性証明書の有効期間が短いので、必ずしも廃棄処理を必要としない。拡張領域を含む公開鍵証明書による場合は、本人性証明サービスと結合した公開鍵証明書が、権限証明サービスを直接与える場合である。これは、認証局が同時に権限局であり、かつ公開鍵証明書と権限の有効期間が対応する場合に適する。しかし、通常は、両者は非同期であり、別個の機関が本人性と権限をそれぞれ証明することが適する。

権限ルート局[9]（Source of Authority＝SOA）は自身も権限局（Attribute Authority＝AA）であるが、権限付与についての最終責任をともなうエンティティである。公開鍵基盤における、ルート認証局ないしトラスト・アンカーに類似する。以下のような異なるタイプの環境を考えることができる。

（a）すべての権限が、単一の権限局から直接に個別のエンティティに与えられる場合。

（b）オプションである役割（role）をサポートする場合（後掲図2参照）。ここでは、特定のエンティティに特定の役割が付与され、当該役割と結びついた諸権限が黙示に当該エンティティに付与される。役割とそこに含まれる権限の結びつけは、そのための属性証明書においてなされるか、その他の方法でなされる。

（c）オプションである権限委譲(privilege delegation)をサポートする場合（後掲図1参照）。この場合には、権限ルート局が、あるエンティティに権限を付与し、権限を付与された当該エンティティも自ら権限局として行動することができ、かつさらに権限を委譲できるというものである。委譲は、さらに委譲ができないエンド・エンティティに至るまで、中間の権限局を通して、続けることができる。中間の権限局は、委譲後に自ら権限主張者として行動できる場合とできない場合がありうる。

（d）ある環境では、同一の物理エンティティが権限局と認証局を兼ねることがある。この同一の物理(physical)エンティティの二重の論理的（logical）役割は、権限が公開鍵証明書の拡張領域において付与される場合には常に妥当する。それ以外の環境では、異なる物理エンティティがそれぞれ認証局と権限局として行動する。この場合には、権限は、公開鍵証明書ではなく、属性証明書を用いて付与される。

属性証明書における権限

エンティティは二つの方法で権限を取得できる。一つは、権限局が、自らまたは第三者のリクエストに応じて、属性証明書の作成を通じて、特定のエンティティに権限を付与する。この証明書は一般にアクセス可能なリポジトリに保管され、権限確認判断をするために権限検証者により処理される。これらの作業は、当該エンティティが知

(10)

らず、または積極的な行動がなくとも、生じうる。第二に、エンティティがある権限局の有する権限を要求する場合である。この際の証明書は、当該エンティティに引き渡され、保護されたリソースへのアクセスを要求する場合に提示される。

このような、属性証明書に基礎を置く権限管理インフラ（PMI = Privilege Management Infrastructure）は、以下のような場合に適合的である。

公開鍵証明書発行者と異なるエンティティが権限付与する場合。多様な発行者から付与されるべき多くの権限属性が存在する場合。公開鍵証明書の有効期間が権限の寿命と異なる場合。ある権限が、利用者の公開鍵または他の権限の有効期間と非同期な、一定期間のみ有効な場合。

公開鍵証明書における権限

このメカニズムが適合的な環境は以下のような場合である。同じ物理エンティティが認証局と権限局を兼ねる場合。権限の寿命が公開鍵のそれと連動している場合。権限委譲が許されているが、証明書の拡張領域に含まれる権限のすべてが、同一の委譲パラメータを有し、委譲に関するすべての拡張が証明書に含まれる権限のすべてに等しく適用される場合。

SOA --> AA --> AA --> ....--> end entity

図1

権限管理インフラの諸モデル

一般モデル

オブジェクト、権限主張者、権限検証者の三つのエンティティからなる。オブジェクトの例としては、アクセスコントロールアプリケーションにおける保護されたリソース、ファイアウォール、ファイル、否認不可アプリケーションでサインされたものなどがある。検証決定が依存する四要素は、主張者の権限、権限ポリシー、現在の環境

変数、オブジェクトメソッドのsensitivityである。権限ポリシーは、一定の権限セットが承認に十分かどうかを判断する閾値を設定する。環境変数は、何らかのローカルな手段で検証者に提供される、検証の成否を決定する際に必要となるポリシーの諸側面（例えば、時刻や現在の口座残高）を把握する。オブジェクトメソッドのsensitivityは、処理されるドキュメントやリクエストの属性、例えば、許可する資金移転の額やドキュメントの機密性を反映する。このモデルは、さらに、アクセスコントロールの文脈で用いられる場合と否認不可の文脈で用いられる場合に細分できる。

委譲モデル

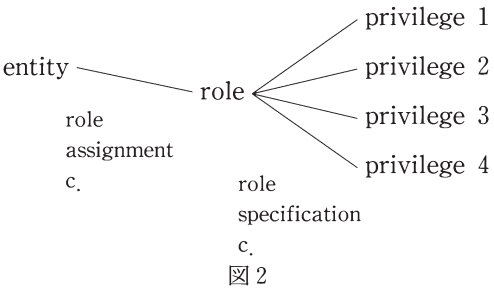


図2

このオプションを含むモデルでは、以下の四要素が含まれる。権限検証者、ルート権限局、それ以外の権限局、権限主張者である。この場合には、ルート権限局は、あるエンティティに権限を付与し、同時に権限局として行動することを認め、当該権限局は、さらにその権限ないしサブセットを他のエンティティに委譲できる。ルート権限局等は、パス長やネームスペースを制限することで委譲に制約を加えることができる。

検証者は、ルート権限局を、リソースに関する権限セットの典拠(Authority)として信頼する。権限主張者の証明書がルート権限局によって発行されたものではない場合には、権限主張者の証明書からルート権限局発行の証明書まで、証明書の委譲パスを跡づけなければならない。この作業には、個々の権限局が十分な権限を有していたこと、かつ、個々の権限局がこれらの権限の委譲につき承認されていたことの確認が

含まれる。

役割モデル

役割は、個人に間接的に権限を付与する手段である。個人は役割割当証明書(role assignment certificate)により、当該証明書に含まれる役割属性を通じて、一つもしくは複数の役割を割り当てられる。特定の諸権限が役割特定証明書(role specification certificate)により、一つの役割名に割り当てられる。この方法で、個人に役割を割り当てる証明書に影響を与えずに、当該役割に含まれる権限のアップデートが可能となる。役割割当証明書は、属性証明書または公開鍵証明書である。役割特定証明書は属性証明書のみである。

II　RFC 3281

権限に関する情報は、公開鍵証明書の拡張領域あるいは別個の属性証明書の中に置くことができる。しかし、公開鍵証明書に権限情報を収めることは以下の二つの理由で望ましくない。第一に、権限情報は、しばしば本人と公開鍵の結びつきと同じ寿命をもたない。権限情報を公開鍵証明書の拡張部分に収めることは、公開鍵証明書の有効な寿命を縮めることとなる。第二に、公開鍵証明書発行者は、常に権限情報について典拠となるわけではない。このため、公開鍵発行者は権限情報をその典拠者から得るという手数が増えることとなる。

属性証明書は、アクセスコントロール、データオリジン証明、否認不可を含め、様々なセキュリティサービスとともに利用可能である。

公開鍵証明書は、アクセスコントロール判断のために、本人性を提供できる。しかし、多くの文脈で、アクセスコントロール判断に用いられる基準は、本人性ではなく、アクセス者の役割やグループ帰属である。アクセスを要

求した者が、属性証明書の正当な保有者であることの確保は、公開鍵証明書への参照を属性証明書に含めることと、アクセスリクエストの中で、公開鍵証明書に対応する秘密鍵を証明のために使用することである。

データオリジン証明や否認不可の文脈では、属性証明書に含まれる属性が、署名エンティティに関する付加的情報を与える。これによって、当該エンティティが当該データに署名する権限を有していることの確認ができる。

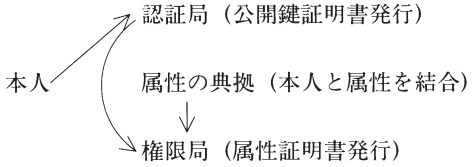
権限委譲について

属性証明書の連鎖と結びついた管理や処理は複雑であり、現在なお属性証明書の使用はインターネット上でかなり限定されているため、本仕様書は、属性証明書の連鎖使用を推奨しない。本仕様書は、特定の属性セットのための属性証明書のすべてを一つの権限局が発行するという単純な場合を扱う。もっとも、異なる属性セットを複数の権限局が扱うことを排除するものではない。例えば、ある権限局発行の属性証明書にはグループ帰属が含まれ、他の権限局発行の属性証明書にはセキュリティクリアランスが含まれるといった例がそれである。

III　ETSI TR 102 044

パブリックコメント用ドラフトと公表版をまとめて扱う。前者では「属性証明のための要件の特定」、後者では「電子署名とインフラ、役割と属性の証明書の要件」と表題が変わっているが、内容に大きな変化はない。

本文書の目的は、主として電子署名の文脈における属性証明とする。[11] 属性の種類として、グループのメンバー帰属と役割がまず挙げられる。役割は、個人とは独立に定義される。役割は比較的安定したものであるが、役割と個人の関係・結びつけは可変的である。その他の権限付与情報としては、代理(proxies)と資格(capabilities)を挙げる。前者は、他人に代わり署名する主体である。



矢印は情報の流れる方向を示す
図3

他人の名で、または他人の属性の下で署名する。このための技術的手段としては、第一に、権限局が、代理人に、委譲者のすべてのあるいは一部の属性を含む属性証明書を発行する方法、第二に、委譲者自身が、代理人に、自己の役割の全部または一部を委譲するために、自ら署名した属性証明書を発行する方法がある。

属性は、属性証明書発行者(attribute certification authority＝ACA)が同時に属性の典拠(attribute issuing authority＝AIA)である場合には直接証明されることができる。例えば、学位を含む証明書を発行する大学、裁判官について証明する裁判所など。これに対して、そうでない場合には、承認される前に、属性証明書発行者が合理的疑いをもちえない程度に証明される必要がある。すなわち、その属性の登録時に、当該個人が特定の属性を保持する資格があることの証明である。発行者が属性証明書の正確性について責任を負うのだから、属性の正確性について確認する方法の選択は当該発行者に依存する。

ある属性は委譲不可なものとして個人に割り当てられ、他の属性は委譲可能なものとして割り当てられる。典型的には属性サブセットの委譲である。しかし、委譲期間や委譲の対象となる人をできるだけ限定することが望ましい。また、委譲を一レベルのみとして、再委譲を制約することが望ましい。委譲チェインが長くなれば、信頼は低減するか消滅する。また、制限によって、属性を用いうる文脈を限定することができる。

四　Draft ETSI TR 102 045

このテクニカルレポートのドラフトは、「拡張された諸ビジネスモデルのための諸署名ポリシー」[12]という表題を

有している。その趣旨は、当初、単一のモデル署名ポリシーの作成が考えられたが、まもなくそれは多様な現実のビジネスモデルの需要に対応できないという認識から出発している。すなわち、売買契約では、売主と買主のように、二つの相互に独立した署名(parallel independent signatures)が問題となる。さらには、証人が既に存在する署名に、または上司が部下の作成した署名になすような、埋め込まれた連署ないし副署(embedded, counter-signatures)の場合がある。したがって、複数署名の有効化のための方法に関する一般的ガイドを提供することが目的とされる。また、リアルワールドの手書き署名の諸特徴をバーチャルワールドに移し、電子署名に等価の信頼を作り出すビジネス上の必要があるが、前者の点はなお十分究明されていない。多様なビジネス文脈における、リアルワールドの署名の意味と黙示に含まれている諸帰結を分析することも目的とする。この際、リアルワールドにおける署名行為の解釈において重要な意味をもっている文脈的情報を再現することが必要である。(13)

4・1　背景リサーチ

異なるビジネスモデルの需要に対応する単一のモデル署名ポリシーを作成することは不可能であることが明らかとなった。リアルワールドでの署名の必要な理由、意図される関与タイプの記述の困難、すなわち取引の各段階で署名がなされるがそれが有効化されるしくみ、署名が取引の安全性にどのように寄与しているかが明らかではないことからである。

5　署名の諸ケースの分析

それはスタンプや印章の代替であるが、法的効果は加盟各国で様々である。イギリスでは、現在では印章はほとんど法的要件として要求されなくなったが、他の諸国では依然印章は署名の重要な付加物である。特に、公証人、政府、会社が用いる印章が好例である。

5・1　取引文脈／適用の場

契約時の署名と交渉過程でのドラフトへの署名。これらは文脈において理解されるが、それは、署名の意味についての日常理解に含まれており、その微妙さは容易に見逃されやすい。

5・2　署名の形式／署名の意図

単なる署名、署名スペースの次に印字された表示、証人の署名、公証人の署名、署名儀式

5・4　署名者の役割、属性

多くのビジネスシナリオでは、署名者は「表見権限」(apparent authority) を有することで十分である。多くの場合、相手の地位や権限を検証する必要はない。その例外は、土地取引やその他の重要な取引である。

5・10　複数署名 (multiple signatures)

多くの取引は、有効で拘束力をもつためには、一つ以上の署名が必要である。

7・1　役割と属性の意味

この点で多くの誤解がある。特に、役割を文脈から取り出そうとするのがその好例である。役割は、一定の属性セットに基礎を置く「比較的安定した」行動パタンと結論づけうる。

7・2　要求された役割と証明された役割

リアルワールドでは、ビジネス関係は一連のやりとりにより蓄積された信頼の上に成り立っている。役割や属性が署名時に検証されることはまれである。名刺やレターヘッドが要求された権限の証拠として受容される。法的には、かような表見権限にもとづいた行動に対して組織は最終的に責任を負うというルールが普遍的に存在することで説明される。しかし、遠隔地間での取引では、先のように、従来の知識や安定した行動パタンによる信頼もあり

うるが、このような信頼性に依拠できない場合もありうる。電子環境が不確定要素を付け加え、従来のものに加え、補強的証明を要求する場合がありうる。

7・3・1　委譲された権限

現実の権限や要求された権限で十分かを明記する必要がある。

7・3・2　制限された権限

法的には、使用者責任（vicarious liability）でカバーされる。

7・6・1　ビジネス役割

会社法に見られるように、同種のビジネス役割の標準化の必要がある。それは既存の法令や概念と矛盾せず、かつ全加盟国の承認を得る必要がある。

8　電子署名における関与タイプ

リアルワールドと異なり、ここでは、明示に、署名の意味や関与タイプを示す必要がある。特に、権限確認のみの場合の電子署名と法的行為の証拠としてのそれとの区別が必要である。バーチャルワールドでは失われてしまう、署名時の文脈的情報を提供する代替手段が必要である。

8・2　電子関与タイプ

データオリジンの証明のみの場合、手書きと等価であるが法的に拘束される意図がない場合（例：ドラフトへのサイン、受領認め、書面の作成者ないし責任所在の明示のため）、署名が付加されたデータ内容に法的に拘束される意図がある場合がある。

8・2・3　電子公証署名

ある時点での署名の本人性と完全性の有効化と、将来の参照のための有効化証拠の保管をするための信頼された第三者(trusted third party)。

8・2・6　行政上の電子署名

記録保存、電子ステープル

9　複数署名

リアルの世界では、署名された書面を比較的簡単に検討するだけで、その有効性を判断できるが、バーチャルな世界では、同様にはいかない。複数の署名の扱い方と署名ポリシーの下での有効化を扱う。

9・1　パラレル署名

相互に独立した署名であるから、署名の順序は問題でない。

9・2　シーケンシャル・パラレル署名

順序が重要な場合。

9・3　埋め込み署名

署名相互に順序と強い関連性がある場合を扱う。最初の署名の有効性が、他の署名の有効性に依存する場合（例として証人の副署）である。

9・4　複数署名の処理

署名ポリシーが複数署名処理のフレイムワークを提供する。署名生成、有効化、署名相互の関係の定義（各署名における署名ロールの割り当て、署名目的を記述するような属性との結びつけ）を内容とする。

9・4・1　署名ロール(signing roles)

正署(primary signatures＝PS)と副署(countersignatures＝CS)がある。例えば、売買では、売主（PS/1）と買主（PS/2）である。経費請求では、被用者（PS/1)、管理者（CS/1)、会計（CS/2）となる。

9・4・2　関与タイプ

署名の目的を記述する情報セットと定義される。これは検証者に署名者の署名作成意図に関する情報を提供する。正署については、最終的な（法的）約束、データ内容の承認、権限付与、受領の証拠もしくは承認のタイプがある。副署については、権限付与、証人、公証のタイプがある。

10・1　署名ポリシーの法的効力

契約条項と異なり、署名ポリシーの場合には、署名者が署名前に読んでいなかった場合には、有効な署名がないと考えるべきである。

10・2　黙示の署名ポリシーと明示の署名ポリシー

署名プロセスが十分確立したルールによって定義されている場合（例：銀行小切手への署名)、署名の文脈がその申請書類によって単一に特定される場合（例：納税申請)、署名の及ぶ範囲と署名者の役割が署名の対象である書面に明確に述べられている場合（例：公証された書面）においては、明示の署名ポリシーは必要ではない。

五　若干の検討

まず、一から四で紹介した四文書の意味と関連をまとめておく。これらは、広い意味で、公開鍵証明書と属性証明書を用いて、ヴァーチャルな世界を運用するスキームを描いているといえる。しかし、それぞれの組織が置かれている沿革や趣旨から、念頭に置かれているモデルや適用範囲が異なり、それゆえに、アクセントが異なっている。

X.509 の場合には、最も広い意味でのネットワークにおけるデータ交換の場が前提とされており、公開鍵証明書や属性証明書はそこでの認証を強化する一選択肢としての意味しかない。これに対して、RFC 3281 はインターネット上での運用を前提としており、属性管理や権限委譲について、実装を想定した単純化を意識している。ETSI TR 102 044 の場合には、電子署名指令を前提としたものであるため、否認防止やデータオリジン証明という、より取引ないし法的問題となる場面に限定されている。そこでの電子署名自体も上級証明書、適格証明書のように、より限定されたものを想定している。これに対応して、権限委譲については、委譲される人の範囲、時間、再委譲等につき、より限定的なスタンスとなっている。最後の、ETSI TR 102 045 は、なおドラフト段階ではあるが、より実際の取引とその法的側面を注視し、リアルの取引の文脈を忠実にバーチャル取引に移行させる場合に、本人性や属性の証明問題がどう変容するかについて注意を払おうとしている。特に、複数署名の有効化の問題がそうである。

X.509 以降、属性証明のオプションとして役割という概念が用いられる。これは権限の包括化・定型化として、法の世界にはなじみのある発想である。代表取締役（商法二六一条）などとりわけ商法の分野で多くの例が見られる。これに関連して、このような包括的権限の内部的制限から外部の第三者を保護する規定（商法二六二条）も多くある。商法の分野では商業登記記載事項への信頼（商法一四条）もこれに該当する。ひいては、民法上の表見代理（民法一〇九条、一一〇条、一一二条）も権限の存在する外観に対する信頼を保護する制度として関連する。

これに対して、権限委譲は、民法における復代理（民法一〇四条ないし一〇七条）・復委任が扱うところである。[14] そこでの代理人による復代理権の設定は、実務上は例が少ないと思われるが、（復）委任状が用いられることとなろう。この点で参考となるのが、白紙委任状に対する裁判実務の対応である。[15] ただ、そこで問題とされている

のは、委任事項や受任者欄が空白であった場合に濫用がなされ、発行者本人にどこまで濫用の結果のつけを負わせるかという点であり、アブノーマルな事態の評価を個々の当事者の文脈や行動から補充しつつ行うというきわめて法的な世界に入ってしまう。ここでは、権限委譲の制約をそもそも解釈で事後的に発見する作業がなされているのである。

さて、X.509での権限委譲スキームが後の諸文書ではその扱いがだんだん制約的なものに移行していったと述べた。これはいかなることを意味するのであろうか。

第一に、既に述べたところでもあるが、それぞれの文書が念頭に置くモデルが異なることにあろう。ディレクトリはもともと（信頼を前提とした善意の）情報管理スキームであって、情報の内容の真正さを担保ないし証明するスキームではなかった。公開鍵基盤や権限管理基盤はそれを補い、情報の真正さを担保する手段として導入された。法的ルールの多くは不信を前提とし、争いがある場合には、自己証明が直ちに法的に考慮されるわけではなく、本人から離れた客観的な素材（証拠、証人）による裏付けを必要とする。そうすると、権限ないし属性をある主体に結びつける者とその結びつきを確認する者とが分離されることが仕組上要請されることとなる。認証局や権限局は、本人性ないし本人の権限を第三者として客観的に担保しようとする仕組だからである。情報管理ないし権限管理スキームと権限認証（ないし証明）スキームを同一の主体が行うことが矛盾を有するためである。本人性の場合は後者のみであるが、属性の場合には、結びつけとその存否確認の二段階をとる必要がある。属性付与者(attribute issuing authority＝AIA)と属性証明書発行者(attribute certification authority＝ACA)が分離するゆえんである。これによって、本人性のずれ、すなわちなりすまし等の場合、原則として、検証者と本人の間の問題としてではなく、本人と認証局の問題に限定されたが、権限のずれは、属性付与者のもとでのずれと属性証明書発行者のも

とでのずれとが生ずることになる。前者は、属性付与者が誤った権限情報を属性証明書発行者に提供した場合であり、後者は、提供された情報と異なる誤った内容の属性証明書を発行してしまった場合である。これらの場合にも、公開鍵証明書の場合と同様に、本人、属性付与者、属性証明書発行者、検証者という、利用にかかわる各当事者の注意義務を基準とする責任判断がなされよう。

第二に、第一とも関連しているが、対象とする行為の性質にも関係がある。電子商取引で典型的に署名が問題となるのは、契約交渉の最終段階で、双方が契約書に署名する場合であるが、そこに至るまでに様々な法的行為がなされる。また、付随的に、事実的行為もなされる。これらが果たして法的に正当であったか。それぞれの行為につき、行為時点で、なす権限を持つ者が実際にしていたか。これらの事実は、一旦後日紛争が当事者間で起こった場合、広く考慮されうる要素となる。その際、当事者は法廷内外でこれらの点につき自己の有利に援用できるためには、その素材を保存しておく必要がある。(16) 行為の評価にかかわる文脈情報すべてが大なり小なり証拠価値をもつわけである。行為規範であると同時に裁判規範であるゆえんである。これに対して、デイレクトリにおけるアクセス許可等の問題は、後日法的紛争となる可能性が皆無ではないにせよ、電子商取引の場合とは異なり、行為時のチェックが正当になされれば十分で、その判断の当否を後日また問題とする必要はあまりないといえ、行為規範としての意味をもつにすぎないだろう。このような場面では、権限管理と権限認証をスキームとして分離させる慎重さは通常不必要である。

この問題は、権限の対象が事実的なものか、法的なものに関するのかという側面とも関連する。前者であれば、事実的権限であり、代理（民法九九条は意思表示を対象とする）や委任（民法六四三条は法律行為の代行を対象とする、もっとも六五六条はそれ以外の事務委託に委任規定を準用する）の直接的対象とはならず、また民法一一〇

条の表見代理の基礎とはならないとされる。[17] 後者がいわゆる法的権限であり、何らかの意思表示を中に含むものである。もっとも、法的権限と事実上の権限（代行権）の限界は、意思表示自体が準法律行為という観念ないし分類を必要としているように、連続したものである。また、登記申請や官庁への申請等も含めるならば、より柔軟な概念スキームが必要とされよう。このような概念再構成をも迫るものを含んでいるのである。

また、権限管理で尽きるような場面では、権限委譲は定型化でき、さほど困難な作業とはならない。例えば、オブジェクト指向プログラミングにおけるプロパティの継承などにみられる。他方では、権限認証をも含む場合で権限委譲オプションを採る場合、それが法的行為に関連する重要な取引に導入される場合、処理のオーバーヘッドのみならず、権限濫用の可能性という不必要なリスクを背負い込むこととなる。

この点は、リアルの世界とバーチャルの世界の関係にも連なる。前者で実現されている点をすべて後者でも対応して技術的に実現できるからといって、常にそうすべきであるとはいえない。その逆もそうである。X.509における権限委譲の例として、上司が属性証明書を発行して休暇中だけ部下に権限を委譲する例[18]があったが、リアルの世界で日常的な行為が、バーチャルの世界の手段でも実現できるからといって、そうすべきとはいえない好例であろう。

最後の文書で扱われた問題は、署名がなされた文脈をできるだけ定型化されたデジタル情報として提供しようとするスキームにかかわる。その手段として、署名ポリシーが活用される。署名ロールや関与タイプがその具体例である。署名とそれが対象とするデータ内容をどう関係づけるかのスキームであるが、リアルな世界では、この点は、同一紙上の、データ内容と署名者の肩書・職名記載を総合して判断された。バーチャルな世界では、（通常のPKIを前提とする限り[19]）データ内容と署名が分離されるので、このような配慮が必要とされるわけである。ただ、

このようないわば署名属性ないし署名文脈情報とでもいうべきものは、データ内容から推論できない場合には、そもそも問題があるというべきである。黙示の署名ポリシーで解決されない場合に、署名や文書内容の外にある署名ポリシーが署名プロセスの文脈や署名の意味解釈を補うというのであろうが、このスキーム自体が署名、ひいては文書の法的効力を質的に強化すると考えることができるのかは疑問である。また、ここでは、署名をなす際の署名者の意図をも問題とするが、それ自体定型化されたデジタル情報であるのだから、なりすましや盗用の場合をも考慮すれば、意思確認の強度に質的な違いが生ずるとは一概に考えがたいのである。紙情報の場合でも、署名者の意図は情報内容が記載されたものと同一紙上（同一空間）にあるという事実自体から定型的に判断されているのだから。

（1）類似のものとして、プロクシー証明書（proxy certificate）があるが、アクセスコントロールに主眼がある。cf. Internet Draft (draft-ietf-pkix-proxy-05) (Revised April 2003).

（2）標準化の最新の状況につき、鈴木優一「各国における電子署名・認証の推進と標準化活動」電子署名・認証利用パートナーシップ（JESAP）シンポジウム二〇〇三（二〇〇三年二月二〇日）講演資料二八頁以下に詳しい。

（3）筆者は、電子商取引推進協議会（通称 ECOM）内の認証・公証ワーキンググループに参加しており、他の参加者より様々な機会に電子署名にかかわる諸問題について教示を受ける機会があった。もとより、技術的側面にはうといため、思わぬ誤解をおかしているおそれがある。ご教示をお願いする次第である。

（4）ITU-T Recommendation X.509: Information technology — Open systems interconnection — The Directory: Public-Key and attribute certificate frameworks. (03/2000); S. Farrell and R. Housley, An Internet Attribute Certificate Profile for Authorization. RFC 3281, (04/2002); Draft ETSI TR 102 044 v0.0.7 (07/2002) Identification of requirements for attribute certification. Version for public comments; ETSI TR 102 044 v1.1.1 (12/2002) Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute

certificates; Draft ETSI TR 102 045 STF 209-T1 draft M(14/2/2003) Signature Policies for Extended Business Models. 以下では、それぞれを、X.509、RFC 3281、Draft ETSI TR 102 044、ETSI TR 102 044、Draft ETSI TR 102 045と略記する。なお、XMLベースのセキュリティ情報交換フレームワークとして、SAML(Security Assertion Markup Language)がある。詳しくは、鈴木優一「Webサービスのセキュリティ　第四回」(http://www.atmarkit.co.jp/fsecurity/rensai/webserv04/webserv01.html)。

(5) 塚田孝則『企業システムのためのPKI』(二〇〇一年)三八頁は、分散ネットワーク環境でシステムの情報をユーザーに提供するクライアントサーバー型データベースシステムと定義する。

(6) ディレクトリは、公開鍵情報の保管場所(repository)として用いられる(p.80)。

(7) p.53-77.

(8) エンティティは通常、人であるが、アクセスコントロールの文脈では、クライアント等も含む。

(9) 本人性認証を担う認証局の源であるルート認証局との対応がわかるように仮に本文のように訳出した。

(10) 物理、論理と直訳したが、一般的にわかりやすくしようとするならば、具体的、抽象的と言った方がよいであろう。

(11) 欧州連合電子署名指令を前提とした標準化機構の作業であることによる。RFC 3281はアクセスコントロールサービスをターゲットとしており、否認防止やデータ尾オリジン証明の文脈ではないとする。したがって、電子署名のための属性証明書プロファイルの作成が必要とする。

(12) 署名ポリシー(signature policy)は、当該署名が有効と判断されるための、署名生成と有効化に関する一連のルールと定義される(ETSI TR 102 041 v1.1.1 (2002-02) p.6; ETSI TS 101 733 v1.4.0 (2002-09) p.10.)。署名ポリシーの発行者は、署名者をはじめ、様々な主体が考えられる。署名のなされた文脈情報を明確化させるための手段であり、署名者と署名検証者間で署名の解釈につき争いが生ずるのを予防する意味があるとされる。また、証明書ポリシー(certificate policy)とは相互に関連しつつ、一応目的の異なるものとして独立しているものとされる。このあたりは、法的文脈でのとらえ直しないし整頓が必要であろう。

(13) 同様の試みの動きとして、OASIS(www.oasis-open.org)とebXML(www.ebXML.org)を挙げて強調の必要性を指摘する(p.46)。

(14) アメリカ法の状況については、樋口範雄『アメリカ代理法』（二〇〇二年）九六頁以下。

(15) 最判昭三九年五月二三日民集一八巻四号六二一頁、最判昭四一年四月二二日民集二〇巻四号七五二頁、最判昭四二年一一月一〇日民集二一巻九号二四一七頁など。

(16) 証明書や署名自体に当初から有効期間があるという、リアルワールドと異なる制約を克服して、法的紛争の場での証拠として使えるようにしようとする努力は、近時、署名フォーマットを段階的に考える動き（ETSI TS 101 733, RFC 3126）となって現れている。

(17) 最判昭三五年二月一九日民集一四巻二号二五〇頁など。

(18) X.509 15.1.2.1 (p.63)

(19) 情報のXML化は、そのような文脈をあらかじめ埋め込みうるが、今度は逆に、自分がしている行為が作成プロセスに正確に反映されつつあるのかといった、利用者側からのブラックボックス化の危険が生じよう。