社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－CSEC－33 (12)
2006／5／12

電子認証に基づく情報サービスにおける社会的行為の成立要件の考察

山崎重一郎

近畿大学 産業理工学部

E-mail: yamasaki@fuk.kindai.ac.jp

概要

現在の日本の電子署名法は、自然人による電子署名に対して一定の法的効力を認めるものである。電子認証や自然人以外の主体による電子署名についての制度的枠組みはまだ存在していない。

本論文は、電子認証や自然人以外の主体による電子署名が社会的行為として成立するための共通要件を発話行為論の観点と自動署名や電子認証によるサービス必要とする応用システムの現状から分析する。そしてそのような情報システムによる社会的行為の成立を支える共通アーキテクチャの基本要件について考察する。

A Study for the Requirements of the Formal Social Acts over the Informational Services with Electronic Authorization

Shigeichiro Yamasaki

Kinki University

E-mail: yamasaki@fuk.kindai.ac.jp

abstract

Present Japanese electronic signature law only recognizes the legal effect to the electronic signature by a natural person. The legal framework which regarding the electronic signature other than the natural person such as automatic electronic signature and electronic authentication is still not exist.

In this paper, we examine the requirements of the formal social acts by the information services with electronic authentication or with the automatic electronic signature from the point of view of the speech act theory. We also examine the requirement of the common architecture which supports such kind of social information systems.

1. はじめに

現在の日本の電子署名法は、自然人による電子署名に対してのみ一定の法的効力を認めるものである。クライアントとサーバの間のセッションにおける電子認証の効力や自然人以外の主体による電子署名の効力についての意味を定める制度的枠組みはまだ存在していない。

人間による秘密鍵の活性化オペレーションを必須要件とする電子署名は、紙の書面に対する社会制度をそのまま電子文書に適用しようとするものであると言ってよい。法人や政府機関による電子署名についても、基本的には自然人の電子署名と同様な既存

の制度的枠組みの延長上に位置づけることが可能であろう。このような紙の書面に対する制度を情報化社会にそのまま適用しようとすると、情報システムの観点からは不合理なことが発生する。

例えば、電子政府や電子契約などの社会システムの情報化は、業務の迅速化や省力化やコストダウンなどを目的として実施される。しかし、電子署名が必要な処理を実行する度に人間の介入が必須になるような情報システムは合理的とは言い難い。

今後、電子政府などの社会システムの情報化の中で、情報化の本来の利点を活かしていくためには、自然人による電子署名に限定せずに電子認証や自動的な署名に基づく情報サービスなどを包含する合理的な制度やそれを支えるシステム的な共通基盤が必要になってくると考えられる。

2. 目的とアプローチ

本研究の目的は、電子認証に基づく情報サービスの実行結果やプログラムのエージェントによる自動的な電子署名が、フォーマルな社会的行為として成立するための要件を分析し、今後の情報化社会を支える基盤として位置づけ可能にすることである。

この目的へのアプローチとして、まず我々は言語学の一分野である発話行為論の視点に基づき、実際に情報システムを利用して実施しようとする社会的行為が、言語学的な発話行為として適切に成立するための要件を分析する。そして次に、そのような要件を満たす情報サービスを支えるための共通のアーキテクチャについての考察を行う。

3. 対象とする情報サービスの範囲

インターネット上の情報サービスの中には、匿名性の利点を活用するものやプライベートな人間関係を広げたサービスや地勢的な国境や法に縛られない情報サービスなども存在する。

しかし、本研究が対象とする情報サービスは、フォーマルな社会的行為に関するものに限定する。本研究では、インターネット上の「公の場」にあたる情報サービスと、そこに登場するエンティティの発話が引き起す社会的行為の効果に関するものである。本論文では、そのようなフォーマルな社会的行為に関する情報サービスの実例として、電子申請、電子契約、電子債券を対象とした。

4. 社会的行為の成立要件

まず、申請、契約、債権譲渡などのフォーマルな社会的行為が成立するための要件について分析する。これらがそれぞれ書面として構成され、署名捺印が施されたときに社会的行為としての効力を持つことは言うまでもない。

これに対して、自動処理による署名や電子認証によるセッションの中の処理としてこれらの行為が要求されたときに、それが正しく成立したと見なされるために必要となる要件について考える。

4.1. 発話行為論による分析

発話行為論は、オースティン[1]らによって始められた理論言語学の一分野である。人間は身体を使う行為以外に、発話や書面への言葉の記載だけでも様々な社会的な行為を行っている。そのような行為を「発話行為」という。特に、「命じる」「誓う」のように、それを発話することによって行為が遂行される動詞を遂行動詞と呼ぶ。

4.1.1. 発話行為の適切性条件の分類

サールは、「発話行為は特定の規則に従って遂行される」としている[2]。そしてその規則は、「適切性条件 (felicity condition)」から導くことができるものとしている。適切性条件とは、次の4つの条件から構成されるものとしている。

ただし、ここでは次のような記号を使うことにする。

P:命題内容

X:発話者

Y:聞き手
A:行為

（1）予備条件
発話の状況に関する条件（話し手の聞き手に対する信念など）
（2）誠実性条件
話し手の意図に関する条件
（3）命題内容条件
発話の内容が満たすべき条件
（4）本質条件
発話行為の遂行にとって本質となる条件
ここでは、次のような記号を用いる。
サールによる遂行動詞の分類に基づいて発話行為の適切性条件を次のように整理することができる。

・指示的（directive)
命令、依頼、質問
話し手が聞き手にある行為させようと試みる
（1）予備条件
YはAを遂行する能力がある。
（2）誠実性条件
XはYにAをして欲しいと思っている
（3）命題内容条件
X は Y がこれから行う行為内容を表す命題を言う
（4）本質的条件
Y に A をさせようとする X の試みである。

・表出的（expressive)
感謝、遺憾、歓迎、祝福
話し手の感情を表明する
遂行動詞の例：感謝する（thank)

（1）予備条件
X は P であることが Y にとって良いことだと信じている。
（2）誠実性条件
XはPを喜んでいる。
（3）命題内容条件
PはYに関係した事実である。
（4）本質的条件
X の P に関する喜びの表出。

・断言的（assertive)
陳述、主張、証明、認定
話し手がある命題を現在の事実として述べる
（1）予備条件
X にとって Y が P を知っているか明らかでない。
（2）誠実性条件
X は P が真であることを信じている。
（3）命題内容条件
P は事態や事実の記述
（4）本質的条件
X は Y に P が真実であることを主張する。

・言明的（commissive)
約束、警告、忠告、宣誓、契約
話し手が将来における行為の実行を言明する
（1）予備条件
X は、X 自身が A を行う能力があると信じている。
Y にとっては、X が A を実行することは自明ではない。
（2）誠実性条件
YはXによるAの実行を欲している。
（3）命題内容条件
PはXによる未来の行為。
（4）本質的条件
XはYに対してAを行う義務を負う。

・宣言的（declarative)
布告、命名、宣言
ある社会的慣例に基づき事態に直接的な変化をもたらす発言。

省略

この分類に従うと、利用者の属性認証などの証明行為は、断言的（assertive)な発話行為であり、契約行為は、言明的（commissive)な発話行為であり、債権譲渡の指示は、指示的（directive)な発話行為に分類される。

4.2. 応用システムからの社会的行為の分析

次に、応用システムの観点から、社会的行為の成立要件を分析する。

4.2.1. 電子申請

e-Japan 戦略の成果として、ほとんどの行政手続の電子申請が可能になっている。電子申請を行うには、まず申請者の登録が必要である。この電子申請の申請者の事前登録制度に基づいて、行政機関が登録者に対して行う権限認証は、断言的（assertive)な発話行為である。ここで断言的な発話行為に対する適切性条件の論理的フレームが登場することになる。実際に、SAML など権限認証のための言明証（assertion) を発効するシステムを利用することは、そのような発話行為の実例になっている。

そして権限認証が成功した次の段階として行われる申請行為は、指示的（directive)な発話行為に分類され、その適切性条件が基本的なフレームとなる。

電子申請という社会的行為が適切に行われたことを第三者が検証可能にするためには、この二つの発話行為の適切性条件がともに適正に成立していた証拠となるデータを、安全で信頼できる記録として保存しておき、検証の必要に応じて開示できるようにしておけばよい。ただし、こうして保管される記録の証拠能力を確保する手段については、別途議論が必要である。

現在の電子政府の電子申請には、電子署名を要求するものが多いが、国土交通省などでは、事業報告などの軽度の申請に関しては電子署名を要求していない。この措置は、電子申請の利用率を向上させるために大きな貢献をしている。

基本的に、電子申請が行われるサーバは信頼できる機関が運営しているものであり、また利用者も事前に登録された申請の権限を持った有資格者に限られるため、利用者認証を適切に受けた上で、そのサーバ内で一連の手続を実行し、それらの行為がその時点で適切性条件をみたしていたことを証明する記録が保存されていれば、一応、社会的な行為の成立要件を満たしていると考えてよいであろう。我々は、このような現実的な対応の中で、必要十分な安全性と信頼性を確保する方法を見つけていくことが重要であると考えている。

4.2.2. 電子契約

契約行為は、言明的（commissive)な発話行為に分類され、その適切性条件が基本的なフレームとなる。

膨大な数の契約書に対する署名押捺のハンドリングコストが日常業務の大きな問題になっているリース業界などは、電子署名の自動的な付与に強い興味を持っている。

また、建設業界の工事入札では、PKI を使った電子入札コアシステムによる電子入札がすでに一般化しており、このシステムが国、都道府県、政令市、県庁所在市まで適用される 2007 年度までに 12 万社から 15 万社が PKI 署名用の IC カードを利用するようになると予想されている。

そして、入札後の次のステップとしての契約やさらにその後の工事施工段階、維持管理に繋がる一連の手続を入札と同様の形で PKI をベースにした形で電子化しようとするのは自然なながれである。

このような動向を受けて、電子契約システムを使ったサービスは、金融機関やリース会社や認証機関やメーカなどが開発し商用サービスを実施している。

しかし、公共工事の電子入札のために建設会社の社長や企業の担当者が署名用 IC カードの秘密鍵の活性化オペレーションを行うような処理と、リース会社が大量に納品したパソコンのマウス一つ一つにも対応した膨大な数のリース契約書に署名捺印する処理とを同様に扱うのは合理的でない。

契約行為に対する適切性条件という基本フレームのみを維持した形で、用途に応じた検証可能性を保持する手段を検討することが重要であると考える。

4.2.3. 電子債券

電子債券とは、売買契約に伴って発生する瑕疵担保責任と分離した単純な債権債務関係にした新たな債権である。このように単純化することによって流通を促進させることを目的としている。電子債券システムは、債権の発生、譲渡、消滅までの管理を電子債券管理機関によって集中的に管理するしくみになっている。電子債券は、債券譲渡の大きな障害になってきた「二重譲渡」の問題などを解消するものとして期待されている。

また、米国では、チェックトランケーションという電子債権に近いシステムが構築されサービスが実施されている。これは、手形交換所の電子化であり、手形や小切手の現物を取り立て銀行に溜置いておき、データのみを取り立て銀行から支払い銀行に送付するというものである。

電子債権における債権譲渡などの指示は、契約行為と同様な、言明的（commissive）な発話行為に分類され、その適切性条件が基本的なフレームとなる。

5. 「公の場」の共通基盤

発話行為が公な意味で社会的な効力を持つためには、それが発せられる「場所」などの状況的条件が必要となる。

例えば、裁判官が自宅で判決文を読み上げても判決という行為は成立しない。

行政機関に対する電子申請や電子債券における債券譲渡の指示などは、インターネット上の「公の場」における発話行為であると見ることができる。

我々は、今後の情報化社会では、ネットワーク上にもプライベートな場や自由な場と共に公的な場が適切に配置される必要があると考えている。

そして、このような公的な場は、自然発生的に創られるのではなく、都市計画に近いような、社会の共通基盤として位置づけられた一貫性を持った開発が必要なのではないかと考える。

さらに踏み込むと、現在の自然人の責任を根拠とする電子署名の枠組みを超える手段として、このような公的な場で行われた「行為」は、一定の技術的な記録手段を講じていれば、真正に成立したものとみなせるのではないか、あるいは将来的にはそのような社会通念が形成可能ではないかという我々の主張を含んでいる。

5.1. 共通アーキテクチャの必要性

共通基盤の一貫性の中でも、特に重要なものがアーキテクチャの一貫性である。

現在の電子申請システムは、省庁ごとに独立したベンダーによって開発されているために、様々な不統一の弊害がでている。

例えば電子申請におけるクライアント側の申請ソフトのJAVAの指定バージョンが省庁によって異なっており、一つのPC内では共存できないために申請省庁ごとに別のPC端末を用意しなければならないという多端現象もそのような弊害の一つである。

電子契約システムについても、金融系企業や認証業務を行っている企業や大手リース会社などが独自にシステムを開発しているが、利用する契約システムごとに使用する証明書が異なるという弊害がでている。また、電子契約書の原本性の保証方法がベンダーごとに独自方式をとっているため、電子原本としての有効性を保ったまま契約書をアーカイブから取り出すことができないなどの問題がある。

小規模契約でも、企業運営上の会計帳簿書類になるため、異なるシステムの乱立は電子契約普及の大きな障害になり、特に、中小企業が主なターゲットである電子債券は、電子取引や電子契約と連携した企業の取引事務の一部となることではじめて有用なものになる。

電子署名では、署名のフォーマットの統一によって電子署名の意味や効力の検証可能性が保証できたが、電子認証に基づく情報サービスで実行された社会的行為が検証可能になるためにはどのような要件が必要なのだろうか。

まず、最初に挙げることができるのは、電子認証に基づく情報サービスは、同じ社

会的行為ならば、ベンダーやサービスに因らず、同じ方法で処理できるということ、つまり発話行為に関するアーキテクチャの共通化である。

このとき気をつけなければならないのは、ソフトやシステムの統一ではないということである。そのような「コード」は常に改良を重ねるのが普通である。重要なことは、そのようなコードがきちんと整合性を持って動作できるようにするために、まずデータの構造やプロトコルの基本構造を決めるアーキテクチャのレベルでの統合が必要であると考えられる。

5.1.1. 「公の場」の公開

また、インターネット上の「公の場」がどのような社会的機能を持っているのかという情報は、その場の公共的な使命に基づいて WSDL のような Web サービスのリフレクション定義言語などによって公開されるべきであろう。

5.2. 社会的行為記録の基本構造

発話行為の予備条件、誠実性条件などは、情報システムの観点から見ると、権限認証や RBAC におけるロール割り当てなどのアクセス制御に近い処理として扱うことができる。

また、発話内で行われた行為の遂行にも、一連の手順が含まれるものがある。

さらに、そのようにして遂行された結果として完成された発話行為も対象化しておく必要がある。

例えば、契約行為であれば、まず、当事者が適切な能力や権限を持っていることが前提になり、正統な契約手続があり、それらがすべて正常に完了したときに、そこから効力を発生はじめる契約内容がある。もし、これらのうちどれかが不成立でも契約は不成立になってしまう。したがって、このような行為の成立を第三者によって検証可能にしておくためには、これらすべてを記録しておく必要がある。

このような根拠に基づき、我々は、社会的行為の成立に必要な記録の基本構造として、次の 3 つの要素を定めることにする。

（1）事前条件
（2）事態の推移
（3）事後条件

電子契約の場合を例にとると、事前条件は、契約成立に必要となる前提であり、場の登場人物の役割割り当てなどもこれに含まれる。

事態の推移は、場のシナリオに沿った処理であり、契約のための手続のステップを意味している。

そして、事後条件は、成立して効力を持っている契約内容を意味している。

電子契約において、事前条件や事態の推移のどれか一つでも成立しなければ、契約は成就しないことになる。

6. まとめ

従来の紙の書面による制度をそのまま維持して電子化するのではなく、情報システムとしての利便性を最大限に活かせるような情報化社会の時代に最適化された社会的な情報サービスのための共通アーキテクチャの必要性とその構成について論じた。

本研究は、まだその必要性が理解されたという段階であり、論点の整理や根拠などはまだ不十分である。特に、公的サービスに対するフィッシングなどの攻撃に対するセキュリティ的な要件やプライバシなどの人間の尊厳の保護に関する要件などは未着手である。また、記録の信頼性を確保するための技術的、制度的手段や保管や開示手段などの具体的な構成についても議論を深めたい。

文　献

[1] John L Austin、坂本百大訳『言語と行為』大修館書店、1978 年

[2] John R Searle、An essay in the philosophy of language. 1969.

[3] OASIS, Security Assertion Markup Language SAML 2.0, http://www.oasis-open.org/specs/index.php#samlv2.0 March 2005.