コンピュータセキュリティ　10－19
（2000．　7．25）

代理申請における本人認証方式の提案

金岡　文彦　　中原　慎一
kaneoka@dsa.isl.ntt.co.jp　　nakahara@dsa.isl.ntt.co.jp

NTT 情報流通プラットフォーム研究所
〒239-0847　神奈川県　横須賀市　光の丘 1-1

あらまし

オープンなネットワークにおいて、電子データを仲介者経由で送受信する場合、従来は受信者が同じデータを複数回受け取った場合に、仲介者から誤って複数回、送られてきた物なのかあるいは送信者から意図的に複数回送られてきた物なのかの確認が行えなかった。そのため、仲介者が送信者から受け取った同じ電子データを複数回申請しても受信者が受理してしまうという問題があった。そこで、本稿では電子委任状の概念を導入することで、受信者が仲介者から受け取ったデータの一意性を確認し、電子委任状と電子データの関係及びその関係が唯一であることを検証することで、仲介者の誤動作による同一データの複数回申請を検出可能とする代理申請における送信者と仲介者の本人認証方式の提案を行う。

キーワード　　本人認証、　代理申請、　委任状、　識別、　二重登録防止

A proposals of the way of avoiding the duplicated request by an agent on the EDI

fumihiko KANEOKA　　shinichi NAKAHARA
kaneoka@dsa.isl.ntt.co.jp　　nakahara@dsa.isl.ntt.co.jp

NTT Information Sharing Platform Laboratories
1-1 Hikarino-oka, Yokosuka, Kanagawa, 239-0847 Japan

abstract

In the case of receiving some same data from an agent through the open network, it is difficult for recipient to find out that those same data is intentionally sent or any troublesome would happen on the communication. Our approach enables recipient to check out the same request from an agent according to one request of sender's. We propose a new application form and its usage for indirect request through an attorney.

key words　　authentication, attorney application, letters of attorney, identification , duplicated request

1. はじめに

近年の情報技術の発展により、電子メールやWWWに代表されるようなオープンなコンピュータネットワークでは、迅速な情報交換が行え、また情報が電子化されているため、情報の流用が可能である。そのため、電子商取引（EC）や電子データ交換（EDI）などのネットワークにオープンなコンピュータネットワークを導入することにより、業務の生産性、効率性の向上、本格的なペーパレスが可能であると考えられる。また、日本でも電子署名及び認証業務に関する法律案[1]が成立するなど、法制度の面においても文書の電子化に対する障害がなくなりつつある。

現在、コンピュータネットワーク上では電子データを対面ではなくネットワークを介して交換するため、送受信者お互いの顔を確認することができない。

そこで、送信者と受信者がお互いを確認する方法に、公開鍵暗号方式[2]における公開鍵と個人/団体などのユーザ識別子の対応を証明する公開鍵証明証を発行する機能を持つ電子認証システム[3] [4] [5] [6] [7]が発行する公開鍵証明証を利用して、送信者の本人認証し、安全に価値あるデータをやりとりする方法が用いられている。

また、本人認証方法にも送信者と受信者が直接やりとりする時に確認する直接認証方法と送信者と受信者の間を代理人として仲介者が介在している状態でやりとりする間接認証方法がある。

この間接認証方法に関して公的にも民間でも様々な検討が行われている。[8] [9] [10]

しかし間接認証を行う際に、仲介者が送信者の価値あるデータを受信者に転送する場合や、受信者が重複申請を禁止している場合に、仲介者が受信者から受け取った同じ電子データを誤って複数回送信してしまうと受信者が受理してしまう場合がある。

そのため、受信者が同じデータを複数回受け取った場合に、仲介者から誤って複数回、送られてきた物なのかあるいは送信者から意図的に複数回送られてきた物なのかを確認することが必要となってくる。

そこで本論文では、受信者が受信した価値あるデータが仲介者から誤って送信された物であるか、送信者が意図的に送信してきた物かを識別するための送信データの有効性を確認するために、電子委任状を用いた代理申請における本人認証方式を提案する。

2. 典型的な代理申請方式

典型的な代理申請方式の例として、送信者と受信者が仲介者を仲介しコンピュータネットワークでつながり、電子データを送受信する場合に、受信者が仲介者からの電子データを受領した場合でも送信者からのデータであると識別する方法としては、図1のような確認方法がある。

まず仲介者は受信者側の DB に仲介者として識別可能な仲介者情報を事前に登録されていることを前提にしている。送信者は送信者が作成した電子署名の付与された送信したい電子データを構成要素の一つとした依頼書（図 2）に送信者の電子署名を付与し、仲介者に送付する。仲介者はその依頼書に付与されている電子署名の検証を行い、送信者の本人確認を行った後、その依頼書に付与されている電子署名を、仲介者の電子署名に付け替えた申請書（図 2）を受信者に送付する。

仲介者から送付された申請書を受け取った受信者はその依頼書に付与されている電子署名の検証を行い、仲介者の本人確認を行った際に、その仲介者が受信者側の DB に事前登録されている有効な仲介者であることを仲介者 DB の仲介者情報及び仲介者の電子署名の検証結果を確認した後、電子データに付与されている送信者の電子署名を検証することで、受信者は送信者からの代理申請の送信データとみなし、受理を行っている。

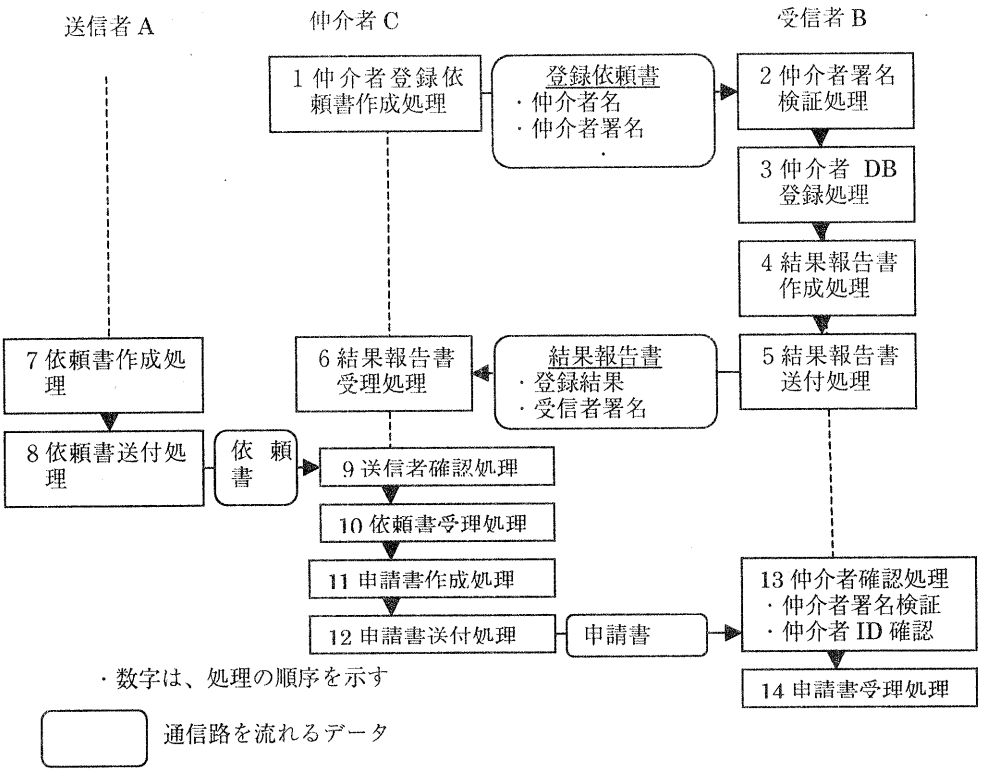

図 1　典型的な代理申請受信処理

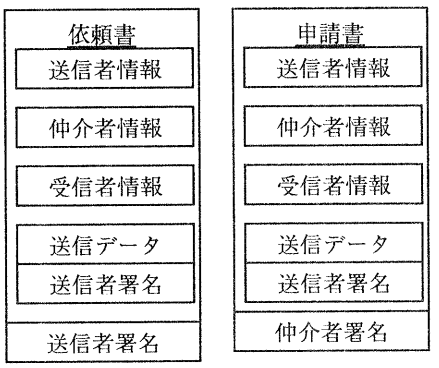

図 2　典型的な申請方法における
依頼書及び申請書構成

3. 課題

こうした典型的な申請方法では、申請書の仲介者署名を検証することで、仲介者の本人性を確認することは可能である。

しかし受信者は送信者が仲介者に送信した送信データと仲介者から受信者に送信された送信データとの一意性を確認できないため、仲介者が受信者から受け取った同じ電子データを誤って複数回、受信者に送信してしまった場合、余分な送付を受信者が受理してしまうという課題があった。

4. 本論文における本人認証方式

送信データの有効性を確認するために、

送信者が仲介者に送付する情報に、送信者の送信意志情報を組みこむ。そして、その送信意志情報は受信者が受理した電子データに対するものであることの関連性の確認及びその関連づいた送信意志情報と受信データが唯一であることの申請の唯一性確認といった2つの確認を行う。

そうすることで、送信者が再度送信依頼を行ってきた物であるかもしくは、仲介者が受信者から受け取った同じ電子データを誤って複数回、受信者に送信してしまった物であるのかを受信者が見分けることを可能とする方式である。

4.1. 電子委任状の導入

送信者の送信意志を表現する手段として、電子委任状の概念を導入する。まず送信者の送信意志を示すことを可能とするために、電子委任状の中に送信者署名付き送信依頼電文を加えることで送信者の送信意志を確認可能とした。

電子委任状内に送信依頼電文を加えるだけでは、送信者の送信意志を確認可能となるだけで、仲介者が受信者から受け取った同じ電子データを誤って複数回、送信を行ってきたことを確認できない。

さらに、この電子委任状が送信依頼を行う対象としている送信データと対になる関係を示すことができないため、この電子委任状を使いまわして利用されてしまうという脅威が新たに発生してしまう。

そこで、まず同じデータに対してハッシュを生成した場合に毎回同じ出力結果が生成される性質を利用して、送信依頼を行う対象としている送信データと対になる関係を示すために、送信者署名付き送信データのハッシュ値を電子委任状の構成要素に加える。

さらに改竄防止のために電子委任状に付与されている送信者の電子署名は、同じデータに対して電子署名を生成した場合に毎回異なる出力結果が生成される性質があるため、今回の申請が前回までの申請と異なるかどうかを、この電子署名を比較することで確認し、仲介者が受信者から受け取った同じ電子データを誤って複数回、送信を行ってきたかどうかを確認可能となる。

これらの要素を組みこんだ電子委任状（図3）は、2章で示した依頼書（図2）の構成要素に、有効期限（*2）及び送信者署名付き送信依頼電文（*3）及び送信者署名付き送信データ（*1）のハッシュ値を加えたものから、送信者署名付き送信データ（*1）をはずしたものに送信者署名を付与したものから構成される。

こうすることで、図3に示した依頼書に付与された送信者署名をはずした場合に、同じデータに対しても申請のたびに自動的に異なる電子委任状が作成可能となり、この電子委任状と送信データとの関係及び申請行為の唯一性を確認可能とすることを特徴とする。

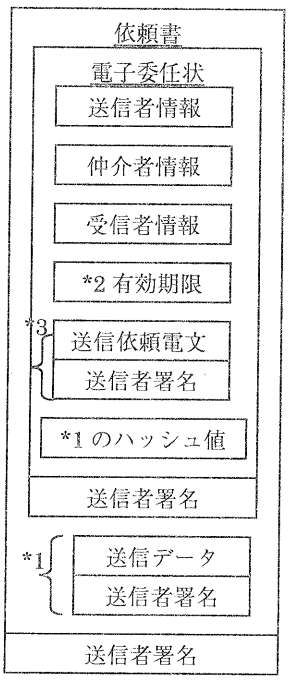

図 3　提案方式における電子委任状及び依頼書の構成

4.2. 電子委任状を用いた本人認証方式

前節で定義された特徴を持つ電子委任状を用いて、課題である受信者が受信した電子データが送信者が再度送信依頼を行ってきた物であるかもしくは仲介者が受信者から受け取った同じ電子データを誤って複数回、受信者に送信してしまった物であるかを識別するために次の確認を行う。

●仲介者の本人性確認

事前登録した仲介者 DB に既登録の仲介者からの申請であること

●送信データの一意性確認

A. 電子委任状内の送信者署名付き送信データのハッシュ値と実際申請されてきた送信者署名付き送信データのハッシュ値が一致すること（電子委任状と送信データの関連性確認）

B. 今回の申請に使用された電子委任状に付与された電子署名と仲介者 DB に登録されている過去の申請に使用された電子委任状の電子署名が異なること（申請の唯一性確認）

の２つの確認を行う。

この一連の確認を行うことで初めて、仲介者が受信者から受け取った同じ電子データを誤って複数回、送信を行ってきたことを検出可能となり、正式な送信者から依頼された仲介者の代理申請であることを確認可能となる。

4.3. 代理申請における本人認証方式

前節、前々節で提案した代理申請における電子委任状と送信データの関連性及び申請の唯一性確認を行う本人認証方式の実際の一連の確認処理を表したものが図 4 であり、その各処理を以下に説明する。

まず、図 4 の①～③の処理においては、従来通りに仲介者は自分の仲介者情報を含んだ登録依頼書を作成し、仲介者署名を付与して受信者に送付する。受信者は受信した登録依頼書の署名検証を行い、仲介者の本人性を確認を行った後、仲介者 DB に仲介者の仲介者情報を登録する。その後、受信者は登録結果報告書を作成し、受信者署

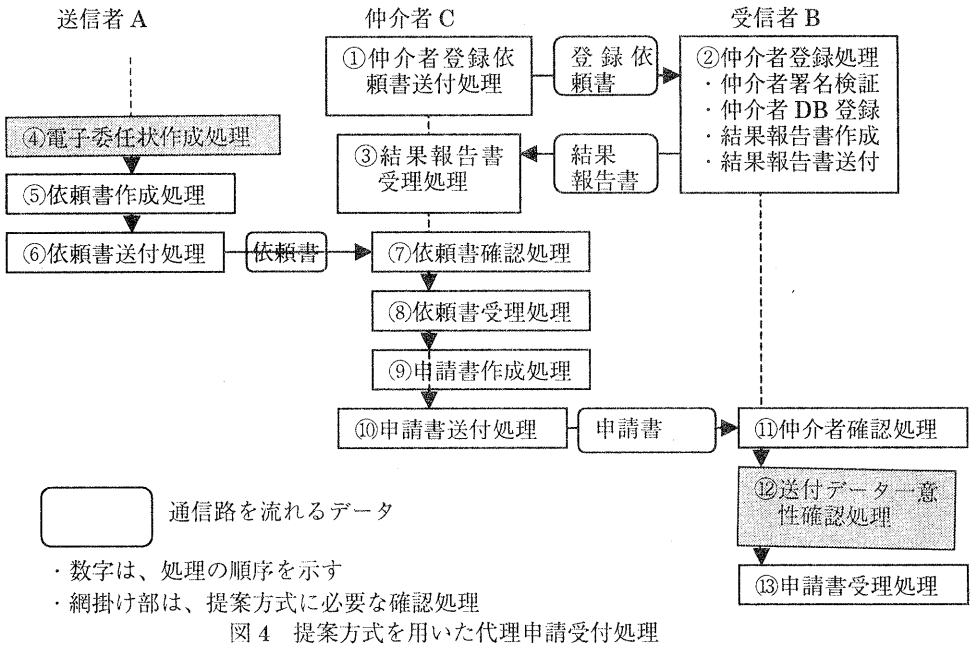

図 4　提案方式を用いた代理申請受付処理

名を付与して仲介者に送付する。まずこの仲介者の事前登録を行う。

④.電子委任状作成処理

送信者は自分が仲介者を仲介して受信者に電子データを送信したい意志を示すために、図３に示すように送信者は送信者署名が付与された送信依頼電文を作成する。また、今回申請したい送信データに対して、作成する電子委任状が１対１に対応していることを示すために、ユニークな送信者署名付き送信データのハッシュ値作成し、構成要素の一つとして加える。この作成した送信依頼電文及び送信者署名付き送信データのハッシュ値及び本人の送信者情報及び受信者情報及び仲介依頼したい仲介者情報及び電子委任状の有効期限情報からなる電子委任状を作成し、これに送信者署名を付与する。

⑤.依頼書作成処理

送信者は④.で作成した電子委任状を及び送付したい送信者署名付き送信データからなる依頼書を作成し、これに送信者署名を付与する。

⑥.依頼書送付処理

送信者は⑤.で作成された依頼書を仲介者へ送付する。

⑦.依頼書確認処理

仲介者は送信者からの依頼書を受信し、依頼書に付与されている送信者署名を検証することで送信者確認を行い、電子委任状及び送信者署名付き送信データを確認し代理申請依頼であることを確認する。

⑧.依頼書受理処理

⑦.の確認後、仲介者は送信者からの依頼書を受理する。

⑨.申請書作成処理

仲介者は送信者からの依頼書を受理した後、この依頼書に対して、仲介者署名を付与し、図５に示す申請書を作成する。

⑩.申請書送付処理

仲介者は依頼書内のある受信者情報に基づき、⑨.で作成された申請書を受信者へ送付する。

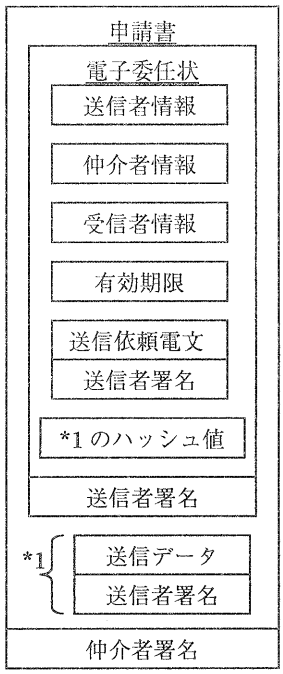

図５　提案方式における申請書の構成

⑪.仲介者確認処理

受信者は受信した申請書が仲介者から送付されてきたことを、申請書に付与された仲介者署名の検証を行うことで確認を行った後、署名検証で本人確認された仲介者が仲介者 DB に事前に登録されている仲介者と一致することを確認し、正規の仲介者からの申請であることを確認する。

⑫.送信データ一意性確認処理（A、B）

⑪.の仲介者確認後、今回の申請において、仲介者が受信者から受け取った同じ電子データを誤って複数回、送信を行ってきた申請でないことを確認するために、電子委任状が送信依頼を行う対象としている送信データと対になる関係であること及び今回の申請が当該データに対して、唯一の申請であることを確認する。

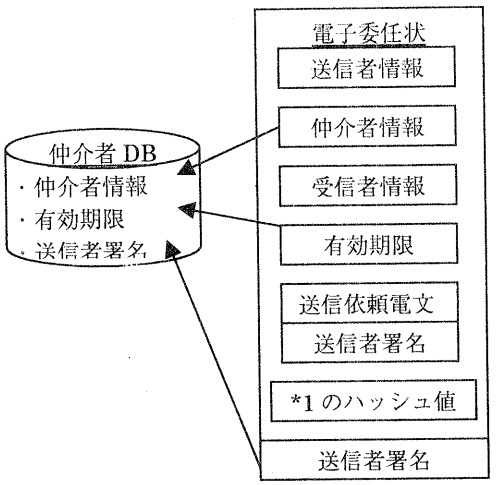

図 6　提案方式における電子委任状と仲介者 DB の関係

そのため申請書内に含まれる電子委任状及び送信者署名付き送信データに対して、次の二つの確認処理を行う。

i）電子委任状と送信データの関連性確認（A）

受信者は実際申請されてきた申請書内にある送信者署名付き送信データのハッシュ値を生成し、そのハッシュ値が電子委任状内の送信者署名付き送信データのハッシュ値と一致することを確認することで、電子委任状と送信データの関連性確認を行う。

ii）申請の唯一性確認（B）

受信者は今回の申請に使用された電子委任状内にある仲介者情報に示される仲介者に対して、受信者の仲介者 DB に登録されている過去の仲介者が使用した電子委任状の送信者署名と今回の申請に使用された電子委任状の送信者署名が異なることを確認することによって申請の唯一性確認を行う。

ただし、仲介者 DB 内に登録されている電子委任状の送信者署名は電子委任状の有効期限の間、仲介者 DB 内に保管される。この時、図 6 に電子委任状と仲介者 DB の関係を示す。

この二つの確認処理を行い、初めて今回の代理申請の申請有効性確認を行う。

⑬.申請書受理処理

受信者は、⑪、⑫で仲介者の本人性及び送信データの一意性確認後、⑨.で作成された申請書を受理する。

以上が、代理申請における電子委任状と送信データの関連性及び申請の唯一性確認を行う本人認証方式の実際の一連の確認処理の流れである。

5.まとめ

送信者と受信者が仲介者を仲介しコンピュータネットワークでつながり、電子データを送受信する場合に、従来法では受信者は送信者が仲介者に送信した送信データと仲介者から受信者に送信された送信データとの一意性を確認できないため、仲介者が受信者から受け取った同じ電子データを誤って複数回、受信者に送信してしまった場合、送付を受信者が受理してしまうという問題があった。

そこで本論文では、電子委任状の概念を導入し、送信者が作成する電子委任状内に送信者署名付き送信データのハッシュ値を加えることで、受信者が生成する受信した送信者署名付き送信データのハッシュ値と比較し、双方が一致することを確認することで、電子委任状と送信データの関連性を確認し、また受信者は今回の申請に使用された電子委任状の送信者署名と受信者の仲介者 DB に登録されている過去の申請に使用された電子委任状の送信者署名が異なることを確認することによる申請の唯一性確認を行うことで、送信データ一意性を確認可能となる。

こうすることで、仲介者が送信者から受け取った同じ電子データを誤って複数回、受信者に送信してしまった場合、これを受信者が検出可能となった。この認証方式を用いて、繰り返し攻撃の検出手段としても

有効に活用できる。

また従来法では、仲介者が悪意を持って同じ電子データを送信した時、それを受信者は受理してしまうため、受信者が仲介者を仲介者 DB に事前登録する場合に、仲介者は信頼の置ける人物としての審査が必要であった。

しかし、本稿の提案方式を用いることで、仲介者の自動登録が可能となり、オープンで利便性の高いシステムを構築することが可能となる。

最後に、今後として本提案方式を実際に業務 AP に実装し、本提案方式の適用性の評価を行う予定である。

参考文献

[1]電子署名及び認証業務に関する法律案（2000）

[2]W.Diffie and M.Hellman,"New Directions in Cryptography",IEEE Tran.on Information Theory,Vol.IT-22,No.6,pp.644-654,1976

[3] 電子商取引実証推進協議会“電子認証システムガイドライン”, 1997

[4] ITU-T Recommendation X.509(1997 E): Information Technology - Open System Interconnection - The Directory: Authentication Framework, June 1997

[5] Housley, R., Ford, W., Polk, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" , RFC2459, January 1999

[6] Chokhani, S., Ford, W., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework",RFC2527,March 1999

[7] Myers, M.,Ankney, R., Malpani, A.,Galperin, S., Adams, C., "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" , RFC2560, June 1999

[8] 電子認証システム推進検討会“法務省法人代表者証明書の利用に関するガイドライン”, 2000

[9] 電子取引法制に関する研究会“制度関係小委員会報告書”, 法務省民事局、1998

[10] Bradner,S.,"Key words for use in RFCs to Indicate Requirement Levels", RFC2119, March 1997