1Y-8

申請者と決裁者が代理決裁の可否を選択可能な電子決裁の提案

永原 裕之 †　　岡村真吾 ‡
† 奈良工業高等専門学校 専攻科　　‡ 奈良工業高等専門学校 情報工学科

1 はじめに

近年企業や組織で行われている決裁処理が，コンピュータネットワークを通じて行われる機会が増えている．このコンピュータネットワークを通じて行う決裁（以下，電子決裁）は従来の紙媒体に比べ，多くの利点を備えている．例えば，距離にかかわらず素早く相手に依頼，処理の応答を行うことができる．電子媒体なので，紙代などのコストを削減できる．そして，紙媒体で行っていたファイリングやスペースの確保が，電子データではサーバーやストレージなどに保管すれば，省スペースで済み，データベース管理をすれば，検索なども容易に実現ができる．これらの特徴から，電子決裁は従来の紙媒体の決裁に比べ，決裁処理の効率を大幅に向上することが可能であると考えられ，電子決裁は将来的に幅広く普及すると思われる．しかしながら，電子決裁を普及させるには，現在の紙媒体で実現されている決裁処理を，電子決裁上でも実現することが求められる．そのひとつに代理決裁がある．

代理決裁とは，決裁者が不在の際に代理人が委任を受け，代わりに決裁を行うという処理である．この代理決裁によって，決裁待ちを大幅に減らすことができ，他の作業にきたす支障を少なく抑えることが可能となる．しかし，代理決裁は決裁者に代わり代理人が行うため，決裁者は委任の際，自身の希望する期間や条件などの制約を代理人に課す必要がある．一方申請者は，決裁者本人に依頼を希望する重要な案などに対して，代理決裁ではなく通常の決裁を行うよう依頼をする必要がある．これらの要件を満たす電子決裁について，本研究では取り組む．

2 関連研究

電子決裁において代理決裁を実現する方法に，委任を示す情報 (以下，委任状) を用いた手法がある [1]．決裁者は代理人に対し委任状を発行し，代理人はその委任状を用いて代理決裁を行う手法である．この手法にもとづいて，満保氏は [2] にて離散対数問題ベースの実現方法について述べている．この手法では決裁者と代理人をひとつのグループと考えている．これにより，決裁者と代理人の代理関係を示し，さらにこの２人のどちらが決裁したかを特定可能にしている．

一方 [2] の手法では，決裁者の委任を制御することは言及していない．つまり代理人は決裁者の代理として常に決裁が可能であり，決裁者が希望しない場合でも代理決裁を行う可能性がある．

3 提案方式

3.1 モデル

【定義】

本手法で登場するのは表 1 のとおりである．

表 1: 提案手法の参加者の定義

人物	説明
申請者	決裁依頼を行う
決裁者	依頼を受けた決裁対象に決裁を行う 代理人に自身の決裁権限を委任する
代理人	決裁者から委任を受けた際， 代理決裁を行う
検証者	代理決裁を検証する

また本手法全体で使用する値を定義する．素数 p, q (但し，$q|p-1$), q を位数とする $g \in Z_p^*$，ハッシュ関数 H を決定する．これら (p, q, g, H) は各処理で使用する共通な値として公開する．

加えて，申請者 r，決裁者 o，代理人 p のそれぞれの秘密鍵を $s_r, s_o, s_p \in \mathbb{Z}_q^*$ とする．そして，$v_r = g^{s_r} \bmod p$, $v_o = g^{s_o} \bmod p$, $v_p = g^{s_p} \bmod p$ をそれぞれの参加者の公開鍵とする．各参加者は他の参加者の公開鍵を知っているものとする．

【決裁の種類】

本手法では通常決裁と代理決裁の２種類の決裁がある．通常決裁は決裁者が行う決裁のことである．決裁者は代理の可否にかかわらず，常時決裁が可能である．代理決裁は決裁者の委任を受けた代理人が行う決裁である．この決裁は決裁者の委任と申請者の代理を認め

Proxy Signature for the delegations by the original signer and the proposer
†Hiroyuki NAGAHARA　‡Shing OKAMURA
†Nata National College of Technology, Factory of Advanced Engineering
‡Nara National College of Technology, Information Engineering

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

る意思の両方が揃ったときにのみ行われる．

3.2 通常決裁

【決裁】

決裁者 o は申請者 r より決裁対象 m に対する決裁依頼を受け，その内容を承認する場合，この処理を行う．決裁者 o は乱数 $r_o \in \mathbb{Z}_q^*$ を決定し $x_o = g^{r_o} \bmod p$, $e_o = H(m, x_o)$ から，$y_o = s_o + r_o e_o \bmod q$ を求める．ここで，(m, v_o, x_o, y_o) を通常決裁情報として公開し，r_o は決裁者 o が秘密に保持する．

【検証】

検証者は決裁対象 m，通常決裁情報 (x_o, y_o)，および決裁者 o の公開鍵 v_o を用い，$e_o = H(m, x_o)$ を計算後，$g^{y_o} \equiv v_o x_o^{e_o} \pmod p$ が成立するかを確認する．成立した場合，決裁者 o は m を承認したものとみなす．

3.3 代理決裁

【決裁者による委任】

決裁者 o は委任状 ω を作成する．ω には決裁者名，代理人名，代理決裁を認める期間などを記述する．さらに，乱数 $r_\omega \in \mathbb{Z}_q^*$ を選び，$x_\omega = g^{r_\omega} \bmod q, e_\omega = H(\omega, x_\omega)$ を求め，$y_\omega = s_o + r_\omega e_\omega \bmod q$ を作成する．ここで，$(\omega, y_\omega, x_\omega)$ を決裁者 o が代理決裁を認める証明として公開し，r_ω は決裁者 o が秘密に保持する．

【申請者による代理可否の決定】

申請者 r は決裁対象 m に対する代理決裁可否の希望 ρ を作成する．そして乱数 $r_\rho \in \mathbb{Z}_q^*$ を選び，$x_\rho = g^{r_\rho} \bmod p, e_\rho = H(m \| \rho, x_\rho)$ を求める．これらと s_r を用い，$y_\rho = s_r + r_\rho e_\rho \bmod q$ を計算する．ここで，(ρ, y_ρ, x_ρ) を申請者 r の代理決裁可否の情報として公開し，r_ρ は申請者 r が秘密に保持する．

【代理決裁】

代理人 p は ρ が代理決裁を認め，ω が有効な場合に代理決裁を行う．代理人 p は決裁者 o より y_ω，申請者 r より (m, y_ρ) を受け取り，代理人 p が決裁対象 m を承認する場合，m, σ_p, y_ρ を用いてこの処理を行う．乱数 $r_p \in \mathbb{Z}_q^*$ を選び，$x_p = g^{r_p} \bmod p$ を決定し，$e_p = H(m, x_p)$ を求める．そして，$y_p = y_\omega + y_\rho + r_p e_p \bmod q$ を求める．$(m, \omega, \rho, v_p, y_p, x_p)$ を代理決裁情報として公開し，r_p は代理人 p が秘密に保持する．

【代理決裁の検証】

検証者によって行われる代理決裁の検証は，ω と ρ の内容と，署名 y_p が代理人 p によって生成されたものかを確認することで行われる．検証者は $e_p = H(m, x_p)$, $e_\omega = H(\omega, x_\omega), e_\rho = H(m \| \rho, x_\rho)$ を求め，
$g^{y_p} \equiv (v_o x_\omega^{e_\omega})(v_r x_\rho^{e_\rho})(v_p x_p^{e_p}) \pmod p$ を確認する．等式が成立する場合，y_p は代理人 p が作成した署名とみなす．そして，ω の内容が有効で，ρ が代理決裁を認める場合，代理人 p が決裁対象を承認したものとみなす．

3.4 評価

本評価は，離散対数問題を解くことが困難であるという前提のもと，提案手法の安全性について評価する．提案手法では，代理決裁が決裁者の委任と申請者の可否にもとづき，適切に行われることが目的である．

代理決裁 y_p には，決裁者 o の委任 ω と申請者 r の意思 ρ それぞれの電子署名 y_ω，y_ρ を含んでいる．y_ω を作成できるのは s_o を有する決裁者 o 本人だけである．すなわち，y_ω は決裁者 o が ω に記述された条件のもとで決裁者 o が代理人 p に決裁を委任したことを意味する．y_ρ は s_r を知る申請者 r のみが作成できる．よって，ρ の意思は申請者 r のものであるとみなせる．また，代理決裁には代理人 p が有する秘密鍵 s_p を使用する．y_p は s_p を用いて作成されるため，s_p を知る者以外は作成できない．よって，y_p は代理人 p による代理決裁であることを示す．

y_p には y_ω と y_ρ が含まれているため，y_p を検証することで，y_ω と y_ρ も同時に検証できる．ω と ρ の内容が代理人 p による代理決裁を認め，かつ，y_p の検証に成功した場合，代理人 p によって正しく行われた代理決裁とみなせる．

4 まとめ

本手法により，申請者と決裁者による代理決裁可否の意思を反映することが可能になる．代理決裁の権限は決裁者の定めた期間に限ることができ，それにより代理人が行う決裁を制御することが可能となっている．申請者は決裁対象に対し，代理決裁可否についての希望を反映することが可能となる．よって，決裁対象に対する代理を認めて迅速な処理を希望するのか，あるいは決裁は決裁者本人に限定することを指定することができる．これにより，電子決裁で求められる操作の一部である代理決裁について，実用的な使用に一歩近づくことができた．

参考文献

[1] Manik Lal Das et al. Algorithms and approaches of proxy signature: A survey. *eprint arXiv:cs/0612098*, 2006.

[2] 満保雅浩. 閾値（委任）署名の匿名性に関する考察. 信学技報, Vol. 99, No. 699, pp. 95–100, 2000-03-16.

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.