イントラネットを用いた社内決裁システムの構築*

7S－9

近藤 麻里子†
日立ソフトウェアエンジニアリング‡

1　はじめに

イントラネット構築が国内企業でも一般化し、ダウンサイジングの要求と共に、社内業務システムでのイントラネット利用が進みつつある。しかし、既存の社内業務システムでは、イントラネットでの使用を考慮しておらず、新たにセキュリティ対策として、ユーザ認証やデータの暗号化が必要となってくる。本発表では、こうした状況を背景に、イントラネット内でのなりすましやデータの改竄防止が可能な社内決裁システムの構築を検討する。ユーザ認証には、従来のパスワードに加えて、個人鍵とユーザ属性を用い、さらにそれらを用いた情報の暗号化を行うことで、アクセスレベルの設定と盗聴防止が可能になり、不正アクセスの防止とデータの安全性を確保できる。

2　社内決裁の現状

現在、社内で行われている決裁処理では、以下の決裁当事者が存在する。

(1) 提案者：決裁事項を提案する。
(2) 合議者：決裁事項を合議する。
(3) 決裁者：決裁事項を決裁する。

また、決裁処理手順は以下のようになっている。尚、各項目の末尾の（　）は、必要なセキュリティ対策である。

(1) 提案者が決裁文書を作成する。
(2) 提案者が作成した決裁文書に押印する。(認証)
(3) 提案者が作成した決裁文書の控えを取る。(改竄防止)
(4) 提案者が決裁文書を決裁者に送付する。(漏洩防止)
(5) 決裁者が合議が必要と判断した場合は、控えを取り、合議者に送付する。(改竄・漏洩防止)
(6) 合議者が合議する場合は、合議印を押印する。(認証)
(7) 合議者が合議した合議結果の控えを取る。(改竄防止)
(8) 合議者が合議結果を決裁者に返送する。(漏洩防止)
(9) 決裁者が合議内容を確認する。(なりすまし・改竄有無のチェック)
(10) 決裁者が決裁する場合は、決裁印を押印する。(認証)
(11) 決裁者が決裁結果の控えを取り、提案者に返送する。(改竄・漏洩防止)
(12) 提案者が決裁結果を確認する。(なりすまし・改竄有無のチェック)

これまで、認証には個人を特定する印鑑による書類への押印、漏洩防止には封印(親展扱い等)、改竄防止には控え(カーボンコピー等)を取るといった方策が採られてきていた。しかし、情報の電子化やイントラネット上での情報送受信を行うシステムへの転換を行うためには、これらの方策も電子化する必要がある。

3　社内決裁システム

前章で述べた社内での決裁処理をイントラネット上で電子化するために、なりすましやデータの改竄防止が可能な社内決裁システムを検討した。

3.1　システム構成

社内決裁システムのシステム構成を図1に示す。

決裁サーバは、決裁クライアントからの要求を随時受け付け、決裁当事者の確認や、なりすまし及び改竄チェック等のために、必要に応じて認証サーバや鍵管理サーバにアクセスを行う。また、決裁クライアントでは、漏洩防止のため暗号化及び復号化の処理を行う。サーバークライアント間のネットワーク上での情報の送受信は、既存のイントラネットを用いて、特に両者間でのアクセス制御やファイアウォール的な通信内容のチェックは行わない。認証サーバは、印鑑に代わるユーザ認証として、電子署名等に用いる証明書を発行する。鍵管理サーバは、認証や暗号・復号化で用いるユーザ毎の公開鍵の管理を行う。[2]

3.2　暗号化方式

*Sanction System on Intranet in a Company
†Mariko Kondo
‡Hitachi Software Engineering Co.,Ltd.

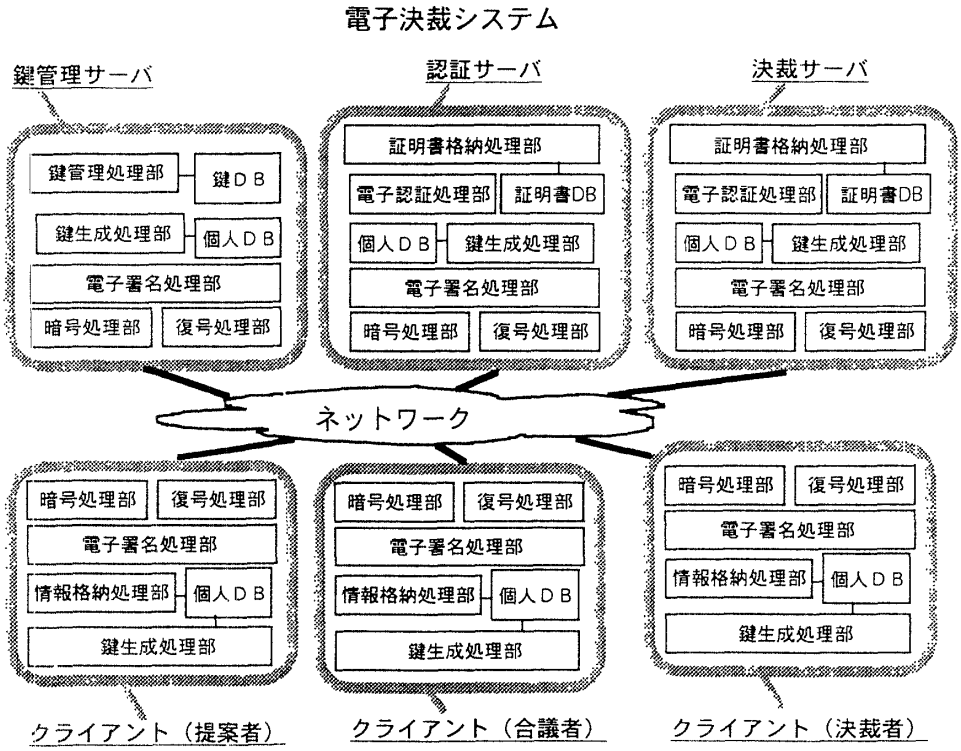

図1　システム構成

本発表の社内決裁システムでは、今後の VPN 等の普及により、インターネット経由によるイントラネットへのアクセスが行われることを考慮し、決裁の当事者間で暗号に用いる鍵を交換せずに済むように、公開鍵暗号を用いることにした。[1]

個人鍵は、将来的には IC カード等への移行を検討するが、現在は各ユーザが自分の鍵を格納した FD を保持し、決裁処理を行う際に、その FD をアクセス時に用いる。ユーザは自身の公開鍵を鍵管理サーバに登録し、暗号化した情報の受信者が復号化できるようにしておく。これにより、決裁文書をネットワーク上で送受信しても盗聴や漏洩を防止できる。

3.3　ユーザ認証

イントラネット上でのユーザ認証には、従来までのパスワードのみを用いていたが、社内決裁システムではこれに加えて、個人鍵とユーザ属性を用いる。[3]

ユーザ認証は、ユーザ属性を登録し、認証サーバが発行する証明書を個人鍵で暗号化したものを電子署名として印鑑の代りに使用する。決裁事項を受け取った決裁者或は合議者は、鍵管理サーバに登録されている提案者の公開鍵を取り寄せ、復号に用いる。これにより、なりすましの防止や決裁文書の改竄チェックを行える。

4　おわりに

イントラネット内でのなりすましやデータの改竄防止が可能な社内決裁システムについて検討した。ユーザ認証には、従来のパスワードに加えて、個人鍵とユーザ属性を用いた。また、情報の暗号化にも個人鍵とユーザ属性を用い、アクセスレベルの設定と盗聴防止が可能になった。これにより、不正アクセスの防止とデータの安全性を確保でき、社内での電子決済が円滑に行えるようになる。今後は、社内適用のため、実際に今回検討した社内決裁システム構築を進める予定である。

参考文献

[1] Laboratories, R. RSA Encryption Standard, PKCS-1 (1993).

[2] Linn, J. Privacy Enhancement for Internet Electronic Mail:Part I-Message Encrytions and Authentication Procedures, RFC 1421, Internet Activities Board (10 1993).

[3] Telegraph, T. I. and Commitee, T. C. The Directory-Selected Attribute Types, CCITT Recommendation X.520, CCITT (10 1988).