ＰＣを利用する多重電子決裁プログラムの一構成方法

7K－6

村田祐一　斉藤泰一　宮口庄司

ＮＴＴ情報通信網研究所

１．はじめに

オフィスでは各種文書の電子化が進んでおり、事務処理用の決裁伝票なども計算機上で作成されることが多い。しかし、決裁印を押すためだけにいったん紙に打ち出さなければならない場合も多く、非常に作業効率が悪い。ディジタル署名を用いて電子的な印鑑を作成できるようにすれば、ネットワークを介して直接電子決裁文書を転送することも可能になり、ペーパレス効果も持った電子決裁システムを構成することができる。

システムを実現するにあたっては、１つの決裁文書に複数名が多重に決裁署名を施せる機能が必須であり[1]、各人の署名鍵，検証鍵をどのように管理するかも重要な課題となる。

本稿では、実際にオフィスで利用されているPC上の勤務票作成システムを対象として、多重署名を行う電子決裁システムの構成法を提案する。

２．鍵管理

本プログラムの実現にあたっては、極力従来の印鑑の原則は崩さないようにする。すなわち、

・自分の署名鍵（印鑑に相当する秘密情報）は自分で作り自分で保管する、
・検証鍵（公開可能情報）は信頼できる認証オーソリティ（ＣＡ：Certification Authority）に提出して印鑑証明（certificate）を発行してもらう（印鑑登録に相当）、

こととする。

１）署名鍵の管理

各ユーザが、自分のパスワードで暗号化した署名鍵ファイルを管理する。以後パスワードを正しく投入しなければ署名鍵を使用することができなくなる。セキュリティ上はICカードに格納することが望ましい。

２）検証鍵の管理

ディジタル署名を用いる場合、検証鍵の正当性を保証することが重要になる。検証鍵の正当性を保証する管理法としては以下のような方式が考えられる。

（方式１）オンライン鍵センタ利用型
・検証鍵は鍵センタのデータベースで管理
・必要になった時点でユーザが問い合わせて入手
・検証鍵の正当性はセンタが保証

（方式２）印鑑証明利用型（Kohnfelder方式[2]）
・ユーザは自分の検証鍵をＣＡに提出し、印鑑証明を受け取る。
・必要になった時点でユーザが自分の検証鍵とその印鑑証明を一緒に相手に送る。
・システム加入者全員に配布しておくＣＡの公開鍵で、だれでも印鑑証明の正当性が検証できる。

本提案においては、検証鍵データベースが不要になり、システム加入時に一回だけＣＡにアクセスすれば良い（方式２）を採用する。

３．多重署名

複数の署名者が順番に署名を行う多重署名方式としては、(1)署名順序規定型と(2)順序任意型がある[3]が、本提案においては署名順序を規定することを前提とする。なお、署名情報は順次結合していき上位署名者の署名対象に含めるようにする。

４．システムの概要

本提案での電子決裁処理の流れを、多重署名が起票者と決裁者の二階層である場合を例として以下に示す。

１）機能構成

以下の機能モジュール群で構成する。

① 勤務票作成システム（表計算ソフト上のAP）
② 鍵生成モジュール
③ 印鑑証明発行モジュール（ディジタル署名生成モジュールを使用）
④ ディジタル署名生成モジュール
⑤ ディジタル署名検証モジュール

・開発環境

② ～⑤はいずれもPC上C言語で作成

A structure of the system using personal computer for multiple electronic approval
Yuichi MURATA、Taiichi SAITO、Shoji MIYAGUCHI：
NTT Network Information Systems Laboratories

2）電子決裁処理の流れ

決裁処理では、原則としてネットワークを介したファイル転送を利用するが、使えない環境ではFDでの持ち運びで代用することとする。

2-1）準備段階（図1参照）

STEP1．鍵の生成

各ユーザ（起票者、決裁者）は鍵生成プログラムを用いて自分の署名鍵S_u／検証鍵P_uを生成する。

STEP2．検証鍵の登録

検証鍵P_uと自分のID_uをCAに提出する。

STEP3．印鑑証明の発行

CAは、CAの署名鍵S_cを用いてP_uの印鑑証明CER_uを生成する。

$$CER_u = fs\ (ID_u \| P_u、S_c)$$

fs：ESIGN署名生成関数

STEP4．印鑑証明の返却

CAは、$ID_u \| P_u$，CER_u，およびCAの検証鍵P_cをユーザに返却する。

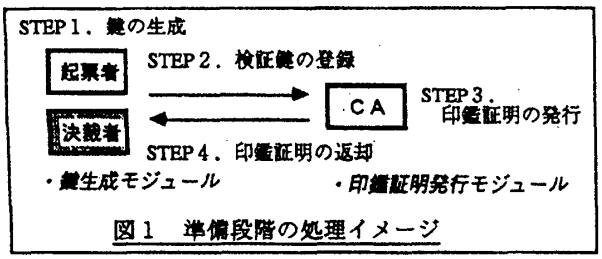

図1　準備段階の処理イメージ

2-2）運用段階（図2参照）

STEP5．起票者署名

起票者は自分の署名鍵S_uで勤務票データDAT_uの署名$DAT_u.SIG$を生成する。

$$DAT_u.SIG = fs\ (DAT_u、S_u)$$

STEP6．提出

起票者は、DAT_u，$DAT_u.SIG$，$ID_u \| P_u$，CER_uをすべて決裁者に提出する。

STEP7．起票者署名の検証

決裁者は、まずCAの検証鍵P_cと印鑑証明CER_uを用いて起票者の検証鍵P_uの正当性を検証する。

$$fv\ (ID_u \| P_u、CER_u、P_c) = OK / NG$$

fv：ESIGN署名検証関数

次に、P_uを用いて起票者の正しい署名であるかどうかを検証する。

$$fv\ (DAT_u、DAT_u.SIG、P_u) = OK / NG$$

STEP8．決裁者署名

決裁者は自分の署名鍵S_aで、勤務票データDAT_uと起票者署名$DAT_u.SIG$の連結に対する決裁署名APRV.SIGを生成する。

$$APRV.SIG = fs\ (DAT_u \| DAT_u.SIG、S_a)$$

STEP9．提出

決裁者は、以下をすべて集計者に提出する。

・起票者からの提出物すべて（STEP6参照）

・決裁署名APRV.SIG

・決裁者のIDと検証鍵$ID_a \| P_a$、印鑑証明CER_a

STEP10．起票者署名の検証（STEP7と同様）

STEP11．決裁者署名の検証

続いて集計者は、決裁者の検証鍵を検証してから、決裁者署名が正しいかどうかを検証する。

$$fv\ (ID_a \| P_a、CER_a、P_c) = OK / NG$$

$$fv\ (DAT_u \| DAT_u.SIG,APRV.SIG,P_a) = OK/NG$$

STEP12．集計

勤務票データの集計を行う。

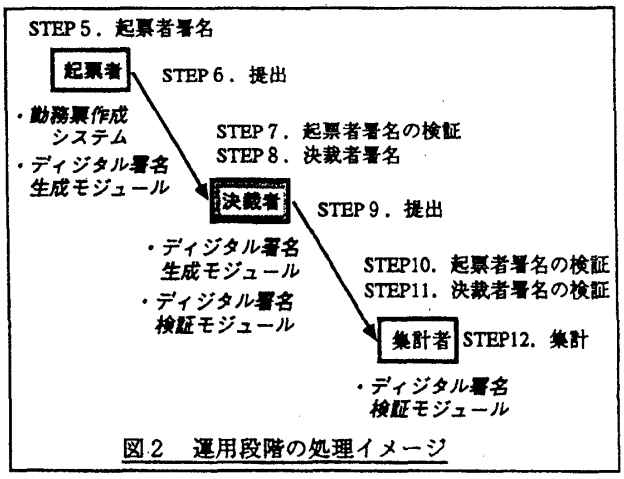

図2　運用段階の処理イメージ

5．おわりに

本稿では、実際にオフィスで使用されている勤務票作成システムを対象とし、多重署名を行う電子決裁システムの一構成方法を示した。電子印鑑方式ESIGNを用いてプログラムを試作し、完成後は社内で運用、評価を行う予定である。WSなど他機種が混在するシステム形態や、CAの階層化[4]、多重署名の階層の増加など、ユーザ数が増えた場合のシステム形態が今後の課題である。

参考文献

[1] 板倉、中村："多重署名に適した公開鍵暗号系"、情処論，24，4，pp.474-480，1983

[2] Kohnfelder.L.M.："Towards a Practical Publickey Cryptosystem"、B.Sc Thesis，MIT Lab.for Computer Science，Cambridge，Mass. May. 1978

[3] 田中、中尾："オンライン型電子契約システムにおける相互署名方式の検討"、ISEC91-46

[4] CCITT Recommendation X.509,"The Directory Authentication Framework",1988