公開鍵暗号を用いたファイル鍵管理

5H－5

栗田 和豊*　NEC宮城
宮内 宏**　NEC

1．はじめに

ファイルの機密保護手段の一つとしてファイルの暗号化がある。簡単な保護方法として、鍵(パスワードなど)を入力しその鍵で暗号化するものが考えられる。この方法はワープロに組み込むことが可能であるが、鍵を忘れた時にファイルを復元できなくなるという欠点がある。本稿では鍵喪失に対処できる鍵管理法を提案する。

2．従来技術の問題点

鍵管理法には、IBM の[1] や RSA暗号のマスタ鍵[3] として知られている方式がある。前者は、ファイルを暗号化する個別鍵を管理用の鍵で暗号化する方式で、ファイルの安全性の強化や鍵の集中管理を狙った者である。後者は鍵-錠のマスタ鍵に対応する RSA 暗号のマスタ鍵であり、個別鍵の紛失や破壊を考慮したものである。しかしこれらの方式には以下のような欠点がある。

・IBM の方式
　管理用の鍵を保護するため、特殊なハードウエアが必要である。
・RSA 暗号のマスタ鍵
　ファイルを暗号化する個別鍵が増える度にマスタ鍵を作り直さねばならない。

3．提案方式

本章では特別なハードを必要とせず、個別鍵が増えた場合にも特別な変更を必要としない鍵管理法を提案する。

3．1 基本構造

本方式はデータの暗号化及び復号には秘密鍵暗号を用い、その鍵の暗号化・復号に公開鍵暗号を用いる。また各々の暗号系では図1に示す様に三種類の鍵が使われる。

・個別鍵
　ファイルを暗号化／復号する鍵(秘密鍵暗号)。
　各ユーザが秘密に管理(記憶)しておく。
・マスタ公開鍵、マスタ秘密鍵
　上記の個別鍵を暗号化／復号する鍵(公開鍵暗号)。
　信頼できる管理者が作成する。暗号化鍵は公開し、復号鍵は管理者が秘密に保管する。

3．2 暗号化

本方式のファイルの暗号化の手順を図2に示した。暗号化にあたっては、利用者が暗号化されるファイルと個別鍵を入力し、以下の手順がとられる。

(1)平文ファイル(データ)を個別鍵で暗号化する。
(2)ファイルの所有者情報(所有者名など)を個別鍵で暗号化する。
(3)個別鍵をマスタ公開鍵で暗号化する。
(4)(1)で得られた暗号文に(2)、(3)で得られたID 情報、鍵情報を付加し暗号ファイルを得る。

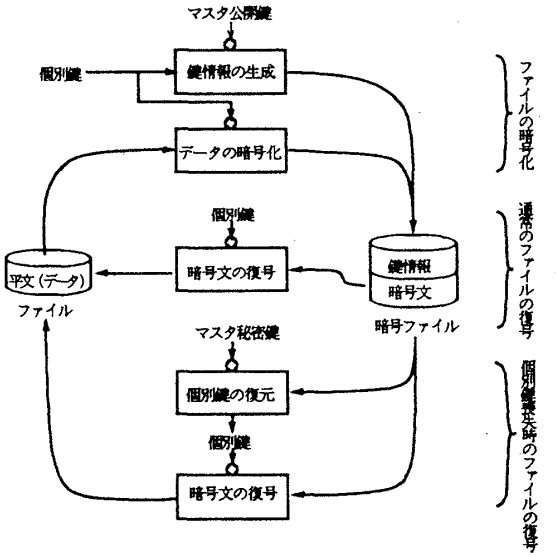

図1．基本構成

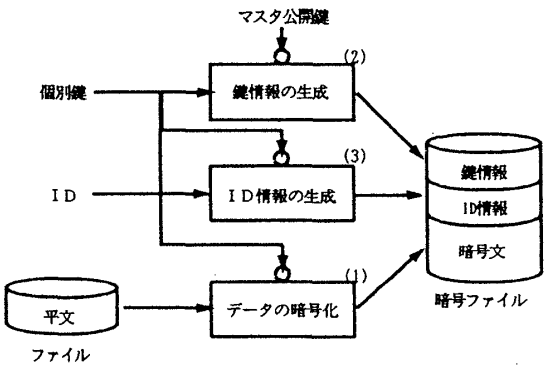

図2．暗号化

File Encryption System
Using Public Key Cryptography
*NEC Miyagi, Ltd.
2, Raijin, Yoshioka, Taiwa, Miyagi, 981-36, JAPAN
**NEC Corporation
4-1-1, Miyazaki, Miyamae, kawazaki, 21, JAPAN

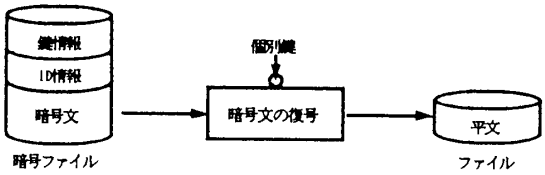

図３．通常の復号

3.3 通常時の復号

通常時の復号は、暗号ファイルの中の暗号文を個別鍵で復号するものである(図３参照)。

3.4 鍵喪失時の復号

ファイルを暗号化した個別鍵をなくした(忘れた)場合には、マスタ秘密鍵を管理している管理者に暗号ファイルの復号を依頼して暗号ファイルを復号することが可能である。その手順を図４に示す。

(1)鍵鍵情報をマスタ秘密で復号し個別鍵を得る。
(2)復元された個別鍵で ID 情報を復号しファイルの所有者情報を得る。
(3)管理者は得られた所有者情報とファイルの復号依頼者が同一であるかの確認を行なう。
(4)所有者が同一ならば、暗号文を個別鍵で復号し平文ファイルを得る。

上記の(3)で所有者の確認を行なう理由は、不正に得た暗号ファイルをあたかも自分のファイルであるかのように管理者に復号を依頼し、復号されることを防止するためである。

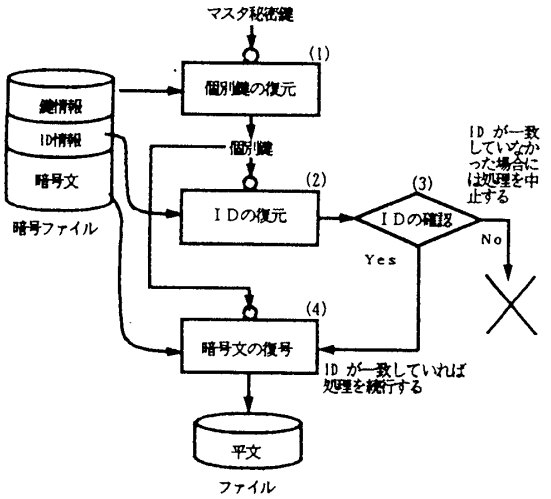

図４．個別鍵喪失時の復号

4．試作

本方式をソフトウエアで試作・評価した結果を以下に示す。

4.1 試作プログラムの概要

試作ソフトの構成は以下の通りである。

・システム構成
- EWS4800/210(R3000ｺﾝﾊﾟﾁ VR3600A, 25MHz)
- Ｃ言語で作成

・暗号系
- 公開鍵暗号として RSA 暗号[2]を使用
- 秘密鍵暗号として DES を使用

4.2 結果

前節に示した構成で試作を行い、RSA 暗号の法が 256bit 、公開鍵が 40bit 、秘密鍵が 252bit という条件のもとで暗号化／復号の速度の実測を行った。その結果を以下に示す。

・ファイルの暗号化
- 鍵情報の生成　… 約 8.5Kbit/s(=0.03秒)
- データの暗号化 … 約 1300Kbit/s

・通常時のファイルの復号
- データの復号　… 約 1300Kbit/s

・個別鍵喪失時のファイルの復号
- 個別鍵の復元　… 約 0.4Kbit/s(=0.62秒)
- データの復号　… 約 1300Kbit/s

例えば 1Mbyte のファイルを暗号化した場合、データの暗号化に約 6 秒、鍵情報の生成に約 0.03 秒であり実用に耐えうる速度といえる。

5．評価

本方式は以下に示すように、従来技術の問題点を解決している。

・ハードウエアの制限
本方式は IBM の方式で必要となるような特殊なハードウエアを特に必要としない。

・暗号化速度
本方式はデータの暗号化に秘密鍵暗号を用いているので高速である。

・ファイルの暗号化／復号に必要な鍵
本方式は、通常のファイルの暗号化／復号に暗号(復号)鍵以外の秘密情報を必要としない。

6．まとめ

公開鍵暗号を用いた鍵管理法を提案した。本方式の特長は通常のファイルの暗号化／復号に個別鍵以外の秘密情報(マスタ秘密鍵)を必要としないため、マスタ秘密鍵は必要になるまで IC カード、フロッピーディスクなどで厳重に保管しておけるという点である。また、IBM の方式と違って特別なハードウエアや設定が必要ないので、計算機の機種、構成にかかわらず利用可能という点も特長の一つである。

以上述べたように、本方式は個別鍵の喪失に対応でき、容易に導入・運用できる実用的な方式であると結論することができる。

参考文献

[1] W.F.Eharsam, S.M.Matyas, C.H.Mayer, and W.L.Tuchman, "A cryptographic key management scheme for impremenring the Data Encryption Standard", IBM Systems Journal, Vol.17, No.2, 1978.
[2] R. L. Rivest, A. Shamir and L. Adleman: "A method of the obtaining digital signature s and public key cryptosystems", Comm. of ACM, pp.120-126 (Feb. 1978).
[3] 小山 謙二：「RSA公開鍵暗号法のマスター鍵」, 電子情報通信学会論文誌, Vol.J65-D, No.2, 89/2.