鍵回復システムの設計と実装

2T－1

（株）富士通北陸システムズ[1]
（株）日立製作所[2]
（株）富士通研究所[3]
北陸先端科学技術大学院大学 情報科学研究科[4]
谷田　武[1]，土屋 宏嘉[2]，道明 誠一[2]，鳥居 直哉[3]，満保 雅浩[4]，岡本 栄司[4]

1.はじめに

官公庁や民間での医療や金融等、秘匿性の高い情報を扱う業種において、データの保護を目的とした暗号化が一般的になるにつれ、管理者による鍵所有者が不在の場合の緊急データ回復や鍵を紛失した場合のデータ復旧を考慮した暗号システムが必要となってきている。特に、鍵の所有者不在や鍵紛失といった理由で、暗号化された情報が復元できないということは、組織全体に不利益をもたらすことが予想され、業務を遂行する上でも大きな問題となる。本文で提案する鍵回復システムは、このような問題の解決策として、利用者のプライバシーを保護しつつ、暗号運用の管理者が、緊急時にデータ回復を行えるように考案したものである。本文では、まず本システムにおける鍵の回復方式について述べ、次に提案する鍵回復システムの設計方針と機能概要、実装について述べる。

2.鍵回復方式

既存の暗号システムへの適用を容易にするため、提案する鍵回復システムは、

(1)現在、一般的に使用されているＲＳＡ暗号をベースにしたシステムとし、現在標準的な暗号アプリケーションにおいて使用される、PKCS#7[1]で規定された Envelope Data 形式の暗号文を鍵回復（データ回復）の対象とする。

(2)利用者に対する証明書の発行など利用者管理の延長で、秘密鍵を鍵回復システムに登録する。

という方式にすることで、管理者に対して、鍵管理に関する統一的なインタフェースを提供し、既存の運用に対して、その導入を容易なものにする。

3.設計方針

鍵回復システムは、利用者システムから秘密鍵の供託を受け付ける鍵登録機関と秘密鍵を保管する鍵保管機関、また、緊急時に暗号化されたデータの復号を行うデータ回復機関で構成する。以下に、鍵回復システムの設計方針について述べる。

（１）秘密鍵の分割と保管先の選択

利用者が登録する秘密鍵は、鍵登録機関や鍵保管機関が単独で復元することができないようにするため、利用者が分割して鍵保管機関に保管する。なお、鍵保管機関については、信頼度が異なる複数の機関が存在することも想定されるため、利用者の意志によって、鍵保管機関を選択できるようにする。

（２）所有者を秘密にした鍵の保管

秘密鍵を分割保管した鍵保管機関の結託や、鍵保管機関への侵入者による秘密鍵の不正な復元を阻止するため、秘密鍵の所有者と分割した秘密鍵の関係を特定することができないようにする。

（３） 秘密鍵を復元しないデータの復号

登録した秘密鍵は使用者の認証に使用される署名の処理にも使用されるため、データ回復機関の管理者といえども、利用者の秘密鍵を入手することはできないようにする。

4.機能概要と実装

鍵回復システムの機能構成、システム構成を図1に示す。鍵回復システムを構成する各機関はネットワークを介して接続されている。また、暗号システムに加入した利用者は、自身の秘密鍵(d)、公開鍵（e,N）、証明書を保持している。ここでは、図 1を参照して、提案する鍵回復シ

ステムの機能概要と実装について述べる。

4.1.機能概要

（１）鍵登録機能

利用者システムから鍵登録機関に秘密鍵の登録を行う機能を提供する。登録する秘密鍵(d)は、利用者システムが分割し、分割した秘密鍵を保管する鍵保管機関の公開鍵で、それぞれに暗号化して、鍵登録機関を経由して鍵保管機関に保管する。なお、鍵保管機関の信頼性が異なることも想定されるため、秘密鍵の登録では、利用者が鍵登録機関から鍵保管機関の一覧情報を入手し、利用者の意志によって、信頼できる鍵保管機関を選択できる機能も提供する。

（２）鍵保管機能

鍵登録機関から鍵保管機関に分割した秘密鍵の保管を行う機能を提供する。なお、鍵保管機関は、信頼できる第三者の機関、部門によって運営されていることが前提である。しかし、鍵保管機関の管理者の不正、悪意を持った者によるシステム侵入等の脅威も考慮する必要がある。このため、本機能では、秘密鍵の所有者と分割した秘密鍵の関係を特定することができないように、鍵登録機関によって鍵保管機関ごとに異なった識別子を割り当てるようにしている。

（３） データ回復機能

暗号システム全体を管理する鍵登録機関管理者の依頼、もしくは、利用者の依頼によって、データ回復機関が鍵保管機関と連携して、暗号化されたデータの復号を行う機能を提供する。なお、本機能では、

・鍵保管機関では、分割した秘密鍵を用いてデータ鍵の復号を行う。

・データ回復機関では、鍵保管機関によって復号されたデータ鍵を使用してデータ鍵を復元し、復元したデータ鍵でデータの復号を行う。

このため、データ回復機関の管理者といえども、利用者の秘密鍵を入手することはできないようになっている。

4.2.実装

鍵回復システムは、PC 上に実装した。鍵回復システムを構成する各機関に実装した機能は、図 1に示した通りである。各機能は、それぞれに RSA 暗号、DES 暗号を実装した暗号ライブラリを使用し、各機関間の通信は、PKCS#7 の SignedAndEnveloped の形式で暗号化し署名を付けている。なお、鍵回復システムを利用するためには、事前に秘密鍵を登録しておくことが必須の条件となる。このため、利用者システムにおける鍵登録機能については、既成の暗号アプリケーションによる鍵生成や証明書入手と鍵登録の処理を一連の処理として実行できるように、最小単位の機能を実現した関数として提供した。

謝辞

この成果は情報処理振興事業協会（ＩＰＡ）が実施している「創造的ソフトウェア育成事業」の一環として行われたものである。

参考文献

[1] PKCS#7: Cryptographic Message Syntax Standard An RSA Laboratories Technical Note Version 1.5 Revised November 1,1993

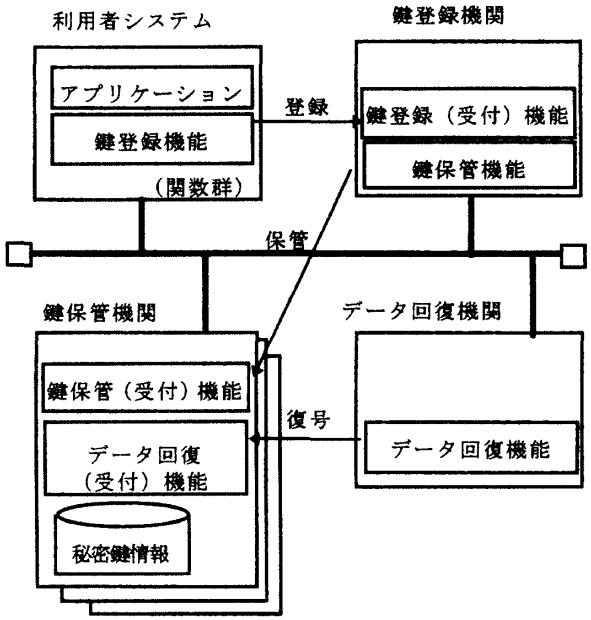

図1 鍵回復システムの構成