鍵寄託型キーリカバリシステムの設計と評価

4T－3

鬼頭 宏幸　植田 広樹　関野 公彦
NTT 情報流通プラットフォーム研究所
E-mail: {kito, ueda, sekino}@dsa.isl.ntt.co.jp

1. はじめに

ネットワークを通じた商業活動を安全に実現するために、暗号技術を利用したセキュリティ製品が市場に出始めている。企業では財務情報や顧客情報などの重要情報を暗号化して安全に保管する。しかし暗号鍵（以下鍵とする）を紛失、破損すると情報の回復が不可能となり、大きな損害につながる。また鍵の所有者の不在時、不慮の事故時も同様である。そこで鍵を復旧するキーリカバリが重要となる。

本稿では企業向けに提案、実装したキーリカバリシステムについて述べる。

2. 企業向けシステムの要件分析

企業の重要情報を暗号化する場合は、鍵の紛失などの緊急時に暗号化した情報を必ず復旧できることを保障しなければならない。また、企業によってキーリカバリ対象となる鍵は以下のように異なると考えられ、それぞれに対応する必要がある。

・従業員の全ての鍵が対象
・署名用鍵は個人所有物であり対象外。暗号化用鍵は企業の所有物であり対象
・全ての鍵は個人の所有物であり対象外

また、企業では業務毎に機密情報の管理を行うが、情報が業務に関係ない者へ流出するのを防がなければならない。そのためキーリカバリ時には部外者へのリカバリを制限することが重要となる。

一方、キーリカバリシステムは企業の機密情報を解読するための格好の攻撃対象となりやすいため、その対策が重要となる。

3. 設計方針

今までに鍵寄託型[1]と鍵カプセル化型[2]のキーリカバリ方式、製品が提案されている。しかし、従来の製品では前述の企業システム向け要件を十分に満たしていない。そこでこの要件を満たすため、以下の方針で設計を行う。

・**キーリカバリポリシ**の導入（強制鍵寄託）
・**キーラベル／キーリカバリグループ**の導入
・攻撃対象（サーバ）の分散

また、本キーリカバリシステムは同じく開発した鍵管理システム[3]と連携して実現する。

3. 提案するキーリカバリシステム

システム構成

本キーリカバリシステムは、鍵寄託サーバ、キーリカバリサーバ（以下 KR サーバとする）から構成される。システム構成を図１に示す。

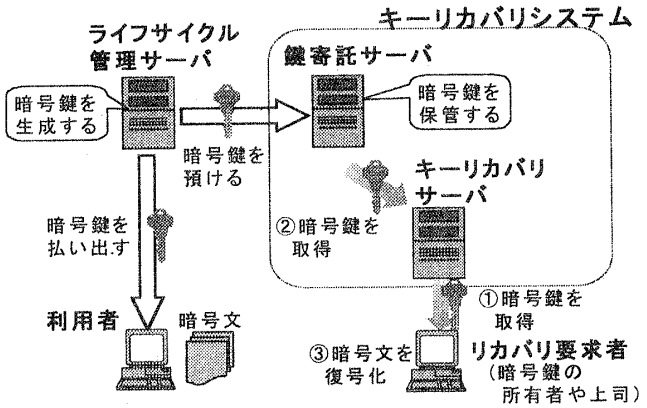

図１ システム構成と処理概要

鍵寄託

鍵管理システムでは鍵の生成はライフサイクル管理サーバ（以下 LC サーバとする）で行う。この LC サーバで保持する**キーリカバリポリシ**を設定することにより、暗号化用、署名用鍵の寄託有無を選択する。以下に鍵 K を生成、寄託する手順を示す。

1. 利用者は LC サーバに鍵生成要求を送信する
2. LC サーバは鍵 K を生成する
3. LC サーバはキーリカバリポリシに基づき以下の手順で鍵 K を寄託する
   3-1. KR サーバの公開鍵で鍵 K を暗号化する（鍵 K を暗号化した情報を K'とする）
   3-2. K'を鍵寄託サーバに送信、鍵寄託サーバは K'を保管する
4. 利用者に鍵 K を送信する

A Key Recovery System for enterprise.
Hiroyuki KITO, Hiroki UEDA, Kimihiko SEKINO
NTT Information Sharing Platform Labs.

キーリカバリ

LC サーバでは生成された鍵へ利用目的に応じたラベル（**キーラベル**）を付与する。KR サーバではキーラベルを LC サーバから取得し、キーラベル毎にキーリカバリできる利用者グループ（**キーリカバリグループ**）を管理する。これにより利用目的毎にキーリカバリ権限を制御することができる（図 2）。

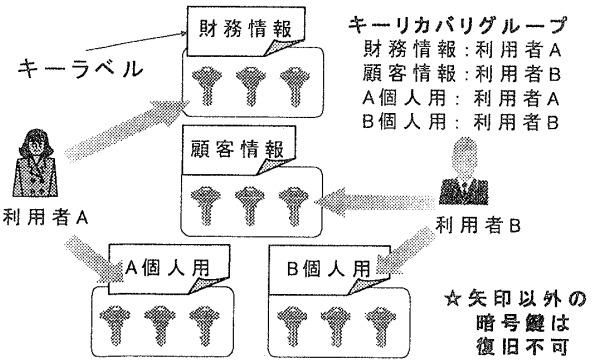

図 2 キーリカバリ可能な鍵の例

以下に鍵 K をキーリカバリする手順を示す。

1. キーリカバリ要求者はキーリカバリサーバに自身がキーリカバリ可能な鍵を問い合わせる
2. KR サーバはキーリカバリ可能な鍵 ID を返す
3. 要求者は KR サーバに鍵 ID を指定してキーリカバリ要求を出す
4. KR サーバはキーリカバリグループによりキーリカバリ権限のチェックを行う
5. KR サーバは鍵寄託サーバに鍵の取得要求を出し、鍵寄託サーバは K'（鍵 K を暗号化した情報）を送信する
6. KR サーバは自身の秘密鍵で K'を復号化し、要求者に鍵 K を送信する

5. 評価

キーリカバリポリシの選択

従来のキーリカバリシステム[1][2]ではキーリカバリの対象は暗号化用鍵に限定し、署名用鍵は対象としていない。これは PKI（Public Key Infrastructure）において署名用鍵は個人を認証するものであり、いかなる理由でも複製をさないという思想で設計されているためである。しかし、明らかに誤って署名用の鍵を消去した場合など本人の責任のもとに署名用鍵の復旧を許すことが考えられる。本システムではキーリカバリポリシの導入により、鍵の強制寄託、署名用鍵の寄託の有無を選択することが可能となる。

キーリカバリ権限

従来のキーリカバリシステムでは、誰の所有する鍵を誰がキーリカバリ可能かを管理しており、鍵毎に種別を行っていない。このためキーリカバリ時には所有者の鍵であれば目的以外の鍵までキーリカバリされる可能性がある。本鍵管理システムでは鍵毎に利用目的に応じたキーラベルの付与を可能とする。またキーリカバリシステムではキーリカバリグループにより利用目的に応じた権限管理を可能とすることで、目的の鍵のみをリカバリさせ、必要以上の機密情報の回復を防ぐことが可能となる。また、キーリカバリグループに鍵所有者の了承を得た上司などを設定することで、鍵所有者の不在時にも業務に支障をきたすことがない。

攻撃対象の分散

従来の鍵寄託型システムでは、鍵寄託サーバで鍵を集中管理しているため、攻撃の対象になりやすい。本システムでは、KR サーバの公開鍵で暗号化した情報を鍵寄託サーバで保管するため、鍵寄託サーバのみが攻撃されても鍵を復旧することはできない。また、KR サーバが攻撃されても鍵寄託サーバへのアクセスを制限、停止することで被害を最小限にすることができる。

6. まとめ

本稿では、企業向けに開発した鍵寄託型キーリカバリシステムについて述べた。これにより、キーリカバリポリシの選択、鍵の利用目的毎のキーリカバリ権限管理、攻撃対象の分散が可能となる。

今回実装したシステムでは、鍵生成時間（RSA 1024bit）のうち寄託に必要な時間は全体の 5.5%（約 0.535ms）となり、LC サーバ処理時間（主に鍵生成）と比較して十分小さい。また今後さらなる性能向上を目指す。

参考文献

[1] Entrust.,"Entrust Key Management Overview," Entrust Technologies White Paper, April 1996.

[2] IBM Corp.,"Key management framework and key recovery technology," IBM White Paper, February 1997.

[3] 田淵洋介他.,"鍵のライフサイクル管理を行う鍵管理プラットフォームの設計と評価," 情報処理学会全国大会, Sep 1999.