キーリカバリシステムの試作

5G－4　　松田 規　竹原 明　中野 初美　中川路 哲男
三菱電機（株）情報技術総合研究所

1. はじめに

近年、インターネットの爆発的な普及や、電子商取引等の新規ビジネスの出現により、暗号技術が注目を浴びている。今後は、機密事項の漏洩を防ぐため、通信データや蓄積データの暗号化が一般的になると考えられる。しかし、鍵の紛失・遺失時に暗号化データは復号できないという問題点がある。この対策として、キーリカバリ技術が注目されている。キーリカバリとは、暗号化データを作成する際に、これを復号する鍵等の情報（これを Key Recovery Field と呼び、KRF と略す）を暗号化データに添付することにより、鍵紛失・遺失時にもこれを復号できるようにする技術である。本論文では、このキーリカバリ技術を用いる際に考えられる問題点について述べ、鍵回復要求時における問題点を解決するための方式について提案する。

2. キーリカバリのモデル

以下、キーリカバリのモデルと基本方式について述べる。

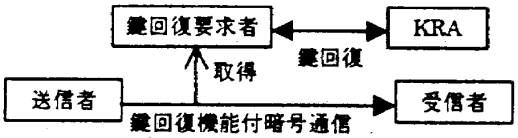

図1：キーリカバリのモデル

図1のモデルでは、送信者と受信者間にて KRF 付き暗号化データによる通信を行っている。この通信データの内容を知る権限を持つユーザとして、従来の通信モデルに新たに鍵回復要求者を定義する。KRA（Key Recovery Agent の略）は、鍵回復要求者からの要求により、送受信者間の KRF 付き暗号化データの鍵回復を行う。

図2は送受信者間鍵回復機能付き暗号化データ作成の処理概要である。送信者は暗号化データの作成時に用いたセション鍵を KRA の公開鍵にて暗号化し暗号化データに添付する。これを KRF と呼ぶ。通常の暗号化データ復号時はこれを無視し復号を行う。

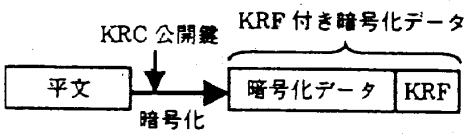

図2：送信者の暗号化処理

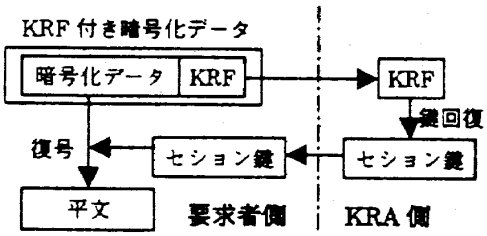

図3：鍵回復処理

図3は鍵回復要求時の処理手順である。鍵回復要求者は KRF 付き暗号化データから KRF を取り出し KRA に鍵回復を依頼する。KRA は鍵回復要求者の要求が正当かどうかを認証し、自秘密鍵にて KRF を復号する事によりセション鍵を取り出し、鍵回復要求者に返却する。鍵回復要求者は、KRA からセション鍵を受け取り、その鍵で暗号化データを復号し平文を得る。

3. 安全面から見た実現上の課題

キーリカバリは鍵紛失・遺失に対する対策として有効であるが、ユーザのプライバシを侵害しかねない技術でもある。そのためシステムの安全性確保は特に重要な課題である。各ユーザにて発生しうる不正のうち、特に検討しなければならない安全面での課題は次の通りである。

(1) 送信者による KRF の未添付、もしくは正しいセション鍵を含まない等の不正な KRF の添付
(2) 鍵回復要求者による、回復する暗号化データを偽った鍵回復要求
(3) KRA による不正なセション鍵返却

A Prototype of Key Recovery System
N.Matsuda, A.Takehara, H.Nakano, T.Nakakawaji
Information Technology R&D Center,
Mitsubishi Electric Corporation

(4) KRA オペレータによる不正な鍵回復や、鍵回復事実の隠滅・改竄

上記不正のうち、(1) は送信者による暗号化データ作成時、(2), (3) は鍵回復処理時、(4) は KRA 運用時に起こりうる不正である。

4. 提案方式とその実装

キーリカバリを鍵紛失・遺失対策として用いる場合、不正な鍵回復を防止する事が最重要課題である。そこで、本システムでは前述の問題点のうち、以下の 2 点に対して対策を検討した。

(1) 鍵回復要求者による、回復する暗号化データの KRF を偽った鍵回復要求

鍵回復要求者が、回復するメッセージの KRF として他メッセージの KRF を用いて KRA に鍵回復を要求する不正

(2) KRA による不正なセション鍵返却

KRA が鍵回復要求者からの鍵回復要求処理時に、不正なセション鍵を返却する

KRA や鍵回復要求者側における上記不正を検出するため、以下のデータを KRF 等に含める事を提案する。

(1) KRF へメッセージ署名等挿入

鍵回復要求者によって回復対象の暗号化データを偽られた鍵回復要求を検出するため、メッセージと一意に対応する情報としてメッセージ署名等を KRF に含める。これにより、KRA で回復要求されたメッセージと KRF の対応の認証が可能となる。

(2) メッセージ検証情報の挿入

KRA による不正なセション鍵返却を検出できるように、KRB に回復後メッセージを検証するためのメッセージ検証情報を付加する。これにより、鍵回復要求者は鍵回復後に正しく鍵回復が行われた事を確認できる。

次に、試作したシステムにおいて、上記不正を検出するため定めたデータフォーマット概要について述べる。図 4 に KRF のデータ構造概要を示す。

KRF には KRA 識別情報が平文の状態で含まれる。また、送信者情報・受信者情報・KRF 作成時刻・メッセージ署名・セション鍵が暗号化された状態で含まれる。これは、KRA 識別情報にて示される KRA のみ復号できる。

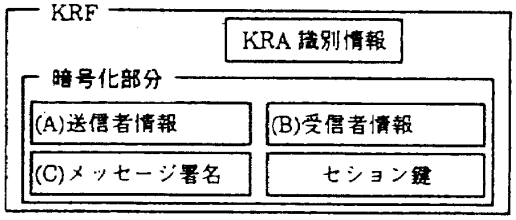

図 4：KRF データ構造概要

次に、KRF 付き暗号化データの構造概要を示す。

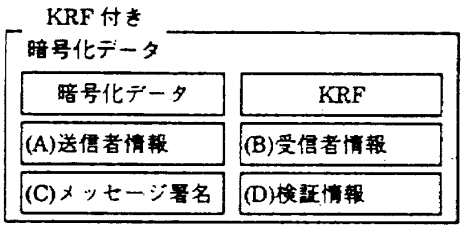

図 5： KRF 付き暗号化データ構造概要

図 5 に示すように、KRF 付き暗号化データには KRF 以外にメッセージ署名・送信者情報・受信者情報・検証情報が含まれる。検証情報とはメッセージと KRF の正当性を検証するために必要な情報である。鍵回復要求者は鍵回復要求時に KRF 以外にメッセージ署名と送信者・受信者情報を KRA に送信する。KRA は図 4(A)と図 5(A)等、鍵回復要求者から受信したデータを KRF 内のデータと比較する事によって、回復する暗号化データを偽った鍵回復要求が行われていない事を検証できる。また、鍵回復要求者は鍵回復後に検証情報よりメッセージが正しく回復されたかどうかを検証する。

これにより、以下の不正を防止できる。

・鍵回復要求者による、回復する暗号化データを偽った鍵回復要求

・KRA による不正なセション鍵返却

5. まとめ

本論文では、当社にて試作したキーリカバリシステムで用いた不正検出方式に関して述べた。

今後は、KRF 付き暗号化データの作成者における不正の検出方式等について検討を行う。

参考文献

[1] "A Common Key Recovery Block Format Promoting Interoperability between Dissimilar Key Recovery Mechanisms," Version X.0, Key Recovery Alliance, May 28, 1998