暗号通信における監査機能の実現方式に関する考察

4T－5

松田 規　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

近年のインターネット等インフラ技術の発展に伴い、インターネットビジネスへの期待度は急速に高まりつつある。その現状において、データの秘匿通信は必須であると考えられている。秘匿通信により、インターネット上の不特定多数ユーザからの開示攻撃からは安全になるが、同時に機密情報の外部への漏洩等の検出が困難になるという側面も持つ。このような事態を防ぐためには、データの監査機能の実現が必須である。暗号化データ監査の一方式として有効と考えられているのがキーリカバリ技術である。キーリカバリとは、暗号化データ作成時に、これを復号するための情報（KRB：Key Recovery Block）を付加することにより、第三者による暗号化データ復号を実現し、内容の監査を可能にする技術である。本論文では、キーリカバリ技術を監査機能として機能させるために必要な要件について検討する。

2. システムモデル

キーリカバリのモデルを図1に示す。

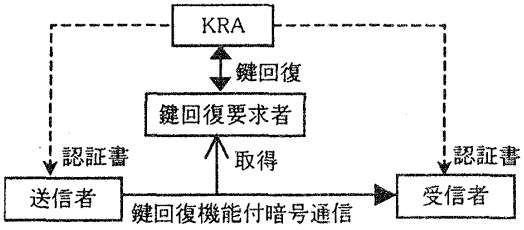

図1：キーリカバリのモデル

図1のモデルでは、送信者ー受信者間にてKRB付き暗号化データ通信を行っている。この通信データの内容を監査する権限を持つユーザとして定義されるのが鍵回復要求者である。鍵回復要求者は、送受信者間で交換されるKRB付き暗号化データを取得し、KRA（Key Recovery Agent）と呼ばれる第三者機関に対して当該暗号化データの復号鍵の回復を依頼し、結果として得られた復号鍵により当該暗号化データを復号し、データの監査を行うものである。KRB中には、暗号化に用いた鍵がKRAの公開鍵によって暗号化されたデータが含まれており、KRAではこの情報を抽出して、復号鍵を取得することが可能になる。

3. 監査機能実現の必要条件

キーリカバリが監査機能実現の十分条件であることは、上で述べた通りである。しかし、監査機能として必要十分に動作するには、必ずキーリカバリが有効に動作することを保証しなければならない。そのためにはキーリカバリシステム側（鍵回復要求者ーKRA間）での不正が行われないことを保証することは勿論、送受信者側で想定される次の不正を検出／排斥しなければならないといえる。

■ KRB除去

送信者側で暗号化データに対して添付されたKRBを、受信者に届く以前で除去されてしまう不正。これにより、たとえ鍵回復要求者が暗号化データを取得しても、キーリカバリは実現されない。

■ 不正なKRBの添付

正しいKRBには、暗号化データ作成時に使用された鍵が、正当なKRAの公開鍵によって暗号化された状態で含まれている。しかし、正当なKRA以外の公開鍵を使用した場合、不正な内容のKRBが生成される。これは、結果的にKRAでキーリカバリが実現できないことになる。

4. 提案

上で述べた不正に対する対策を検討する。

■ KRB除去の防止

A method of audit for Cryptographic system
N.Matsuda, H.Nakano, T.Nakakawaji
Information Technology R&D Center,
Mitsubishi Electric Corporation

KRB 除去への対策として有効なのは、KRB と暗号化処理とを不可分にすることである。例えば、暗号化データ作成時に、利用者もしくはアプリケーションから与えられた鍵ではなく、KRB と前述の鍵から生成した内部鍵を利用することが考えられる。本方式の概要を図2に示す。

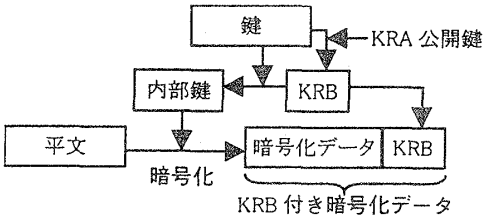

図2：KRB 除去防止の提案方式

KRB 付き暗号化データ作成手順は次のようになる。

(1) 利用者もしくはアプリケーションから平文・鍵・KRA 公開鍵を受け取り、(2) 鍵を KRA 公開鍵にて暗号化して KRB を生成、(3) KRB と鍵から、実際に平文を暗号化するための内部鍵を生成し、(4) 内部鍵にて平文を暗号化し、KRB を付加する事により KRB 付き暗号化データを生成する。

このように、KRB と鍵から生成した内部鍵を利用して暗号化データを作成することにより、復号時にも同様の処理によって内部鍵を生成する必要が生じ、KRB と鍵が必須となる。そのため、常に暗号化データには正しい KRB が付加されていなければならず、容易に監査機能を無効にすることは出来ない。

KRA 公開鍵の正当性検証

KRA 公開鍵の正当性を保証するには、KRA の認証書に関して次のような条件を設定することが有効になると考えられる。

(a) KRA 認証書発行元 CA の限定

KRA は、鍵回復という、ある意味でデータ秘匿に相反する機能を実現するため、その存在は認定制度などにより限定されるべきである。そのためには、KRA は KRA 用の RA により認定され、KRA 用の CA によりその認証書を発行される等の機構が必要である。

(b) KRA 認証書発行元 CA の正当性検証手段の提供

ユーザ（送受信者）は、配布された KRA 認証書の検証が必要である。の正当性を検証しなければならないが、(a)で述べた理由により、KRA 認証書を発行した CA と、ユーザ本人の認証書を発行した CA が同一であるとは限らない。そのため、KRA 認証書発行 CA の認証書（もしくは KRA 認証書発行 CA の認証書検証用データ等）は、KRA 認証書取得手段とは別の手段により、ユーザに配布されるべきである。

(c) KRA 認証書の正当性

KRA 認証書発行元 CA から発行された KRA 認証書は、その内部に KRA 権限を持つエンティティへの認証書であることを明記すべきである。また、KRA 認証書を配布されたユーザによって、当該認証書が KRA 権限を持つエンティティへの認証書であることを検証できなければならない。

上で述べた各手段を実現することにより、キーリカバリが監査機能として動作することが可能になる。

5. まとめ

本論文では、キーリカバリ技術による暗号通信の監査機能の実現においてどのような点に考慮しなければならないかについて検討した結果について報告した。今後は、暗号アルゴリズム内鍵スケジュール部への組込み方式の検討などを行う必要があるだろう。

参考文献

[1] 松田, 竹原, 中野, 中川路："キーリカバリシステムの試作",情処学会第 57 回全国大会講演論文集(3),pp494-495, Oct. 1998

[2] 中野,竹原,松田,中川路："キーリカバリシステムの試作と商用システムへの応用に関する検討",情処学会研究報告 98-CSEC—3, Nov. 1998