個人／企業向けキーリカバリシステムのための認証方式

5G－3

中山恭與、沼尾雅之

日本アイ・ビー・エム株式会社　東京基礎研究所

1. はじめに

筆者らのグループでは、インターネット上におけるデータアーカイブサービスとキーリカバリのシステムを提案し[1]、試作した。ここでいうキーリカバリは、鍵を喪失した場合でも、暗号化して保存されているデータを復元できるようにするためのもので、主に個人や企業での使用を目的としている。本稿では、このシステムの概要、そこで用いられたキーリカバリのしくみ、およびキーリカバリサービスの要求の際の認証方式について述べる。

2. システムの概要

本システムは、利用者ＰＣ(SKR-PC)、アーカイブセンタ(AC)、キーリカバリサービスセンタ(KRSC)、およびキーリカバリエージェント(KRA)の四つのコンポーネントから構成される。これらのコンポーネントはインターネットを介してTCP/IPで接続されている。

利用者ＰＣでは、利用者用のクライアントプログラムによって、データの暗号化／復号化、アーカイブセンタへの暗号化データの預入／引出、およびKRSCへのキーリカバリ要求などが行われる。

アーカイブセンタは、利用者ＰＣからのデータの保管業務を行う。

KRSCは、利用者ＰＣからのキーリカバリ要求に対し、要求の正当性の確認を行い、KRAと協力の上、セッション鍵を復元し要求者に送り返す。

KRAは、KRSCからの要請に応じて、鍵の復元に必要な情報を送り返す。

利用者ＰＣ、KRSC、KRAはDenningらの分類

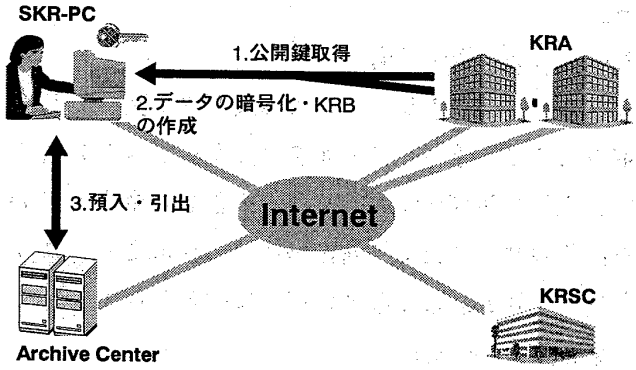

図１．アーカイブサービス

[2]ではそれぞれUser Security Component(USC), Data Recovery Component(DRC), Key Escrow Component(KEC)に相当する。また、すべてのコンポーネントは各自、認証局(CA)から証明書を取得しており、通信の際にはそれを用いて相互に認証を行う。さらに、認証後に鍵交換を行い、機密の保持が必要な情報は暗号化した上で送信する。

3. キーリカバリのしくみ

本システムのキーリカバリは、IBM Secure Key Recovery[3]をもとに、キーリカバリ要求の際の認証方法などに拡張を加えたものである。また、商用使用が目的のため、暗号化の際Data Recovery Field[2]の添付を強制する機能は無い。以下に、本システムで使用したキーリカバリの方式の概要を述べる。

3. 1. キーリカバリエージェントの選択

KRAは自らの公開鍵を公開してユーザが使用できるようにしておく。利用者は、データを暗号化する前にどのKRAを利用するかを決める。一般的に、安全性を高めるため複数のKRAを選択することが好ましい。利用者はあらかじめすべてのKRAの公開鍵を取得しておく。

3. 2. キーリカバリブロックの作成

利用者が任意のデータを暗号化する際、これと同時に、復号用の鍵（セッション鍵）を回復するための情報も作成する。具体的には、まず乱数をKRAの数だけ作成し、次にそれぞれの乱

Authentication Methods for a Key Recovery Service for Personal and Enterprise Use.
Yasutomo NAKAYAMA, Masayuki NUMAO
Tokyo Research Laboratory, IBM Japan
1623-14 Shimotsuruma, Yamato,
Kanagawa 242-8502, Japan

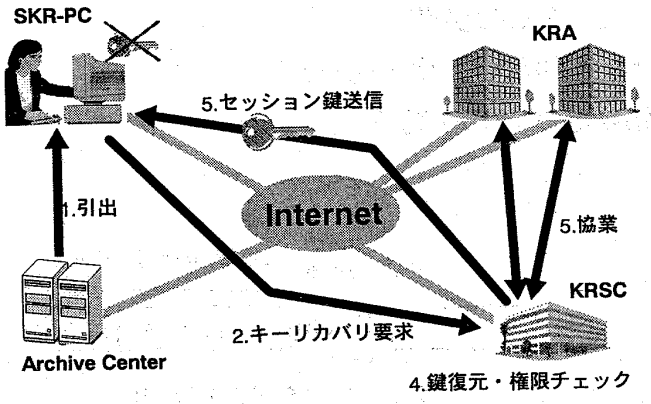

図2．キーリカバリサービス

数から一方向関数を用いてカプセル化鍵を作成する。この鍵でセッション鍵を多重にカプセル化（暗号化）する。また、これとは別に各乱数をそれぞれのKRAの公開鍵で暗号化する。カプセル化されたセッション鍵、暗号化された乱数、および鍵の回復に必要なその他のデータをあわせてキーリカバリブロック(KRB)と呼ぶ(DRFに相当)。KRBは暗号化されたデータと共に保存される。

3.3. キーリカバリプロセス

通常、暗号化されたデータは別個に保管してあるセッション鍵を使って復号化される。しかし、何らかの理由でのこのセッション鍵を喪失してしまったときには、KRBからセッション鍵の回復を行う。まず、利用者はKRBをKRSCに送る。KRSCではKRBの中から暗号化された乱数を取り出し、これを関係するすべてのKRAに送る。各KRAでは自分の秘密鍵を使って乱数を復号化し、これからカプセル化鍵を作成してKRSCに返す。KRSCはこの鍵を使ってセッション鍵を復元し、利用者に送る。

4. 要求権利者に関する情報の記述

4.1. 権利者の認証

利用者からのキーリカバリ要求はインターネットを介して行われる。KRAの中には、キーリカバリを要求する権利のある者の情報（認証情報）が記述されており、要求されたサーバ(KRSC)上で受付の可否が自動的に判定される。要求者の認証方法には以下の2種類がある。

●ID方式

権利者の署名用公開鍵の証明書内に記述された権利者のIDをキーリカバリブロックに記述する。これは各個人毎にユニークなIDでなければならない。すなわち、異なる人物に同一のIDを含んだ証明書が発行されないことが前提となる。要求者は、KRBに署名してKRSCに送る。KRSCでは、署名を検証の上、証明書とKRB内のIDが同一であることを確認する。

●パスフレーズ方式

該当する権利者のみが知っているパスフレーズ（パスワード）のハッシュ値をKRBに記述する。要求者はパスフレーズをKRSCに送る。KRSCではハッシュ値を計算し、これとKRB内の値とが同一であることを確認する。

4.2. 認証情報の書き換えの防止

KRBには、内容全体のハッシュ値が計算されて添付される。この値の計算には、KRBの生成の際に使用された乱数を、ハッシュの鍵として使用している。これにより、認証情報を書き換えて権利者以外の者が不正に要求を行うことを防いでいる。

4.3. キーリカバリ条件

KRBには認証情報として複数の権利者を記述する事ができる。さらに、要求できる権利者の組み合わせをキーリカバリ条件として記述する。たとえば、「データの所有者本人は単独で要求できるが、他の権利者AおよびBの場合は両者の要求が必要である。」といった記述が可能である。

5. おわりに

今回の試作ではキーリカバリのための認証情報をKRB内に記述した。しかし、各ユーザがKRAから専用の鍵の発行を受ける事にすれば、この鍵の証明書内に認証情報を記述するという方法も考えられる。この場合は、認証情報の確認はKRA毎に行われることになる。

参考文献

(1) 沼尾,中山,"復元機能をもつインタネット上のアーカイブサーバ", Symposium on Cryptography and Information Security, SCIS'98-5.2.A, Hamanako, Japan, 1998

(2) Denning, E. D., "A Taxonomy for Key Escrow Encryption Systems", CACM, Vol.39, No.3, 1996.

(3) IBM Corp., "IBM Secure Cryptography and Certificate Services Toolkit", 1997.