暗号データ回復システムの試作

1L－7

佐野文彦　石原達也　麻野間利行　堀智美　丹羽朗人　青木恵　川村信一　才所敏明

(株) 東芝 SI技術開発センター

1　はじめに

データの暗号化を行うシステムでは，暗号化および復号に用いる鍵の管理が問題となる．システムの利用者はそれぞれの秘密鍵を紛失あるいは破損しないよう管理に注意を要する．このような秘密鍵の破損等のリスクに備える手段として，ユーザの秘密鍵を中立公正な鍵回復機関に寄託する鍵回復システムが提案されている．しかし，鍵回復システムの実用化を考えたとき，鍵回復機関や鍵回復実行者の信頼性といった問題が考えられる．

我々は，ユーザの秘密鍵を寄託するのではなく，暗号データの作成毎に生成されるセッション鍵をShamirの秘密分散法を用いて分割することにより，鍵回復に複数の鍵回復機関を必要とするとともに，鍵回復機関を用いた鍵回復の実行に承認者の承認を必要とすることを特徴とするシステムを考案し，暗号データ回復システムを試作した．また，本試作システムでは，鍵交換や署名にそれぞれ楕円曲線上の演算を用いた．本稿では試作システムの概要について紹介する．

2　システムの概要

試作システムは4つのエンティティから構成される(図1)．

1. **認証局 (CA)** システム共通パラメータである楕円曲線パラメータの作成，公開鍵証明書の発行，CRL管理，証明書情報照会などを行う．
2. **鍵回復エージェント (KRA)** データ回復の申請に対して，あらかじめ届けてあった承認者による承認を確認した後，セッション鍵の分割ピースをKRAの秘密鍵で復号し，利用者に返す．
3. **利用者** 暗号データ作成および復号を行う主体である．データ暗号化の際には，セッション鍵回復フィールドを作成し，データ回復が必要な場合には，承認者の許可を得た後，KRAに対して鍵回復の申請を行い，回復したセッション鍵を用いて暗号データを復号する．
4. **承認者** 複数の承認者により承認者グループを構成する．利用者からのデータ回復の申請を審査し，多重署名によりデータ回復実行の許可を与える．

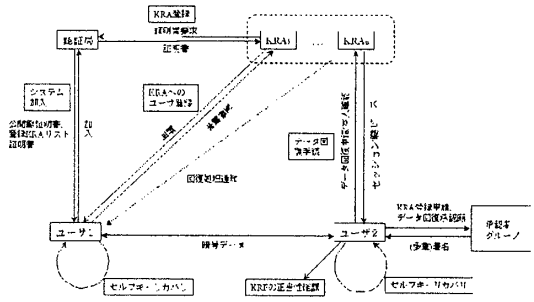

図 1: 鍵回復システムの構成

3　鍵回復の準備および実行の手順

3.1　初期化手順

鍵回復システムを利用するためには，各エンティティについて以下の立ち上げおよび，利用者のKRAやCAへの登録が必要となる．これらは以下の手順で行う．

1. **認証局 (CA) 立ち上げ** 認証局は共通のシステムパラメータである位数 q の楕円曲線 E/F_p を作成し公開する．次に，秘密鍵と公開鍵を作成し，公開鍵を一般に公開する．
2. **鍵回復エージェント (KRA) 立ち上げ** 各鍵回復エージェントは，秘密鍵と公開鍵を作成し，CAに対してKRAの公開鍵証明書の発行を申請する．
3. **承認者立ち上げとグループ作成** 承認者は秘密鍵と公開鍵を作成し，CAに公開鍵を提出して公開鍵証明書を取得する．次に，承認者は，利用者からのデータ回復申請に対して許可を行う承認者のグ

*System Integration Technology Center., TOSHIBA Coporation, 3-22 Katamachi FUCHU-SHI TOKYO 183-8512, Japan

ループを作成する．グループ作成時に，2ラウンド方式多重署名の第1ラウンドを実行し，各承認者に乱数をコミットする．

4. **利用者立ち上げ** 各ユーザは秘密鍵と公開鍵を作成し，CAに公開鍵を提出して公開鍵証明書を取得する．
5. **KRA登録承認申請** 各ユーザはCAの保持するKRAの一覧から，鍵回復に利用するKRAを選択し，k-out-of-n分割のパラメータkおよびnを決定して承認者にKRA登録の承認を申請する．
6. **承認者によるKRA登録承認** 承認者は利用者からのKRA登録の承認申請を審査し，各承認者間で巡回多重署名を行う．多重署名されたKRA登録承認申請はKRA登録承認として申請者に返送される．
7. **KRAへの登録** ユーザは，登録するKRAのリストと承認者から返送された多重署名を各KRAに対して送りKRAへの登録を行う．各KRAはユーザからの申請に対し，承認者の多重署名を確認し，登録を行う場合には，ユーザIDとKRAのリストおよびそれに対する署名から構成されるKRA登録証明書を発行する．KRAはセッション鍵回復の際の確認のために，ユーザからの申請に含まれる承認者のリストを保管する．
8. **登録KRAリスト証明書** ユーザは登録する全てのKRAからKRA登録証明書を受け取った後，ユーザIDと登録するKRAリストおよび各KRAの署名を認証局(CA)に提出し登録KRAリスト証明書を申請する．CAは各KRAの署名を確認した後，ユーザIDと登録KRAリストに対してCAの署名をつけ，登録KRAリスト証明を発行する．

以上の手順により，鍵回復可能な暗号システムが利用可能となる．

3.2 データ暗号化

データ暗号化プログラムはデータ暗号化の際に，暗号化されたデータとともに，鍵回復に用いる鍵回復フィールド(KRF)を作成する．暗号データの作成者をU_Aとし，暗号データを復号する者をU_Bとする．利用者U_Aは暗号化に用いたセッション鍵を複数のピースにk-out-of-n分割し，それぞれをU_Aが登録しているKRAの公開鍵を用いて暗号化し，KRF全体に対してU_Aによる署名を行う．また，暗号データとKRFを受け取った利用者U_BはU_Aの登録KRAリスト証明書とKRFの内容から，KRFの改竄あるいはU_Aによる不正の有無を検出できる．

3.3 鍵回復の手順

暗号化されたデータのセッション鍵情報が破損してデータの復号が出来ない場合には，利用者はKRAの鍵回復サービスを利用することにより，鍵回復フィールドから暗号化に使用したセッション鍵を回復することができる．鍵回復を行うためには，承認者による鍵回復の実行に対する承認が必要である．鍵回復の手続きの手順は以下の通りである．

1. **鍵回復承認願** 鍵回復を行いたい利用者は，暗号データに付属したKRFおよび鍵回復の理由を窓口となる承認者に送り，承認を求める．
2. **鍵回復承認** 窓口となる承認者は申請理由を確認しKRFに対して変形楕円ElGamal署名を用いた多重署名を行い，承認者グループ内の次の承認者に送る．全ての承認者の多重署名を経たKRFと多重署名は窓口承認者から承認者に返送される．
3. **鍵回復申請** KRFおよび承認者グループによる多重署名を各KRAに送り，鍵回復の申請を行う．各KRAは多重署名の確認を行った後にKRFから，KRAの公開鍵で暗号化されたピースを取り出し復号し，申請者の公開鍵を用いて再び暗号化し返送する．
4. **鍵回復実行** k-out-of-n分割の場合，k個以上の復号された鍵ピースP_iが申請者に集まった時点で，ラグランジュ多項式を用いて分割元のセッション鍵Pを求めることが可能である．

4 おわりに

本稿では鍵回復システムの試作について報告した．本システムでは複数の鍵回復エージェント(KRA)を導入し，KRFの作成にk-out-of-n分割を用いる．また，鍵回復の手続きに複数承認者による承認手続きを導入することにより，無制限な鍵回復を制限している．

参考文献

[1] 新保淳, “多重署名に適したElGamal署名の一変形方式,” 暗号と情報セキュリティシンポジウム, SCIS94-2C, (1994).

[2] A. Shamir, “How to Share a Secret,” Communications of ACM, Vol.22 Num. 11, (1979).

[3] N.Koblitz, “A Course in Number Theory and Cryptography, 2nd edition,” Springer-Verlag,(1994).