コンピュータセキュリティ　3－1
（1998．11．27）

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

中野 初美、竹原 明、松田 規、中川路哲男
三菱電機(株) 情報技術総合研究所

近年のインターネットの普及にともない、オープンネットワーク上での情報セキュリティシステム構築が進みつつある。暗号技術を利用するにあたっては、暗号化に利用した「鍵」の管理が必須である。この鍵管理の一方式として、近年、キーリカバリ技術が注目を集めている。キーキーリカバリ技術とは、正規の鍵による暗号化データの復号ができなくなった場合、緊急用の鍵によってデータを回復するシステムである。我々は、このキーリカバリ技術の実現方式を検討、試作し、さらに、この試作システムをもとにビジネスシステムへの適用を検討した。

A prototyping of KEY RECOVERY for business systems

Hatsumi Nakano, Akira Takehara, Nori Matsuda, Tetsuo Nakakawaji
MITSUBISHI Electoric Co., Information Technology R & D Center

In these days, it becomes getting popular that consturacting information systems using cryptography. In this case, we should manage and maintain the KEYs and provide any suggestion for LOST KEY. Key Recovery Technology is a kind of solution for this problem. We construct a Key Recovery System and consider to applicate in real business scene.

1．背景

近年のインターネットの普及により、電子商取引や EDI 等、オープンなネットワーク上でのシステムが急速に展開されつつある。前記システムでは、暗号技術や認証技術を基盤に利用することによるシステムセキュリティの保証が一般的になっている。しかし、暗号技術を利用するにあたっては、暗号化に利用した「鍵」の管理が必須である。この鍵管理の一方式として、近年、キーリカバリ技術が注目を集めている。キーリカバリ技術とは、正規の鍵による暗号化データの復号ができなくなった場合、緊急用の鍵によってデータを回復するものである。本技術は、鍵の紛失／遺失対策としてだけでなく、強制捜査等、違法な暗号化データ交換に対する強制的なデータ開示にも有効である。このような点から、既に米国では、ある鍵長以上の強度を持つ暗号製品輸出にはキーリカバリ機能のサポートが義務づけられている。日本では暗号製品輸出に関する明確な法制度は未だ確立されてないが、米国と同様、キーリカバリ機能サポートを義務付ける可能性があり、キーリカバリ技術に対する注目度は大きい。今回、我々は、

このキーリカバリ技術の実現方式を検討し、試作した。さらに、この試作システムをもとにビジネスシステムへの適用を検討した。

2．目的

キーリカバリは大きく分けて次の二分野への適応が考えられる。すなわち、

(1) 正当なユーザが復号鍵を紛失もしくは遺失した場合(鍵紛失対策)

(2) 上記ユーザ以外で、認められたユーザが暗号化データを復号する場合(Law Enforcement)

である。どちらの場合も、適切なユーザに鍵回復を許可することが大きな命題である。この時、鍵回復の正当性の検証は (a) 鍵回復フィールド(Key Recovery Block, KRB)の正当性、(b) メッセージの正当性、(c) ユーザの正当性、(d) ユーザの回復権限の正当性 について行われる必要がある。そこで我々は以上の点に着目し、システム設計を行った。

3．設計指針

鍵回復の妥当性検証とオープン環境での鍵回復実現を念頭においた上で、我々は鍵回復システムの設計／試作を行った。この時の本システムの設計指針を次に示す。

3．1 ポリシー管理

鍵回復とは、基本的に暗号化データ交換において既定の条件に合致した場合に強制的に適用される機能である。この場合の条件とは個人レベルで設定するものではなく、鍵回復を行なう上で定義される単位毎に設定される。この単位をドメインと呼ぶ。ドメインには最低、一つ以上の鍵回復センタと一つ以上の鍵回復要求者が存在する。

また、鍵回復機能を適用するユーザもドメインへの登録が必要となる。ドメインにおいて設定された鍵回復適用条件を鍵回復ポリシーと呼ぶ。ドメインにエンドユーザを登録すると、登録情報として鍵回復を行う鍵回復センタの公開鍵を含んだ鍵回復ポリシーがユーザに渡される。各ユーザアプリケーションでは、この鍵回復ポリシーにしたがって KRB が作成される。

3．2 クライアントアーキテクチャ

キーリカバリとは、基本的にユーザが意識することのない機能である。そのため、クライアントのアーキテクチャは従来の暗号化・復号I／Fと同様である必要がある。これを実現するためのクライアントアーキテクチャを図3－1に示す。UserApplication からの暗号化データ作成／復号I／Fは従来と同様である。

ただし、暗号化データ取得時に KRB が添付された状態で取得される。鍵回復フィールドの作成等は鍵回復機能付き暗号ライブラリ(Key Recovery Library)上で行う。KRB 作成はユーザに配布される鍵回復ポリシーによって決定される。

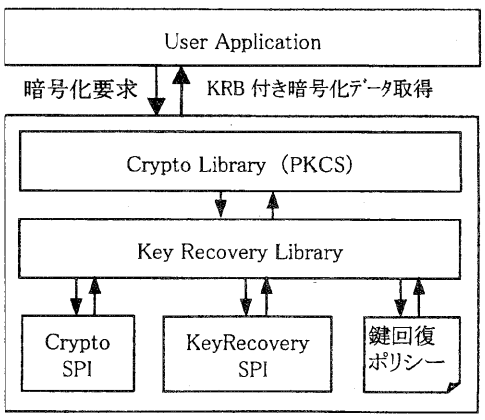

図3－1 クライアントアーキテクチャ

3．3 メールによる鍵回復プロトコルの実現

鍵回復において、鍵回復を要求するユーザの要件はその回復権限保持の如何であり、LAN 内／外等の要求発行場所に依存するべきではない。そのため、本システムでは、鍵回復プロトコルを S/MIME 形式のメール(EnvelopedData 及び SignedData)として、WindowsNT 上のメール API である MAPI を利用した汎用メール上での実現を採用した。これによってインターネット上のどこからでも鍵回復要求発行可能となり、さらに S/MIME 形式のメールを採用したことによって、送信者／受信者認証を実現した。

3．4 データ整合性検証機能の実現

本システムで解決すべき命題として KRB およびメッセージの正当性検証が挙げられることは上で述べた。データ改竄への対策として暗号化データや KRF に対するメッセージ署名が挙げられるが、各データに対する改竄検証への対応のみでは、暗号化データと KRB の対応に関する検証ができず、正しい復号データが得られる保証はない。本システムでは、回復対象メッセージと KRB が正しく対応しているかどうかを検出するため、検証用フィールド(Key Recovery Validation, KRV)を用意している。上記検証を行うためには、KRV 中に平文データを識別するための情報が含まれていなければならない。そのため、KRV は、KRB と暗号化対象データ(平文データ)に対するハッシュデータとした。暗号化データ復号者は、データ復号後に得られた平文と、暗号化データに同封された KRB からそのハッシュデータを取り、検証用データ(KRV')を作成する。KRV と KRV'が一致すれば検証に成功し、そうでなければ途中でなんらかのデータ改竄が行われたことを検出することが可能となり、得られた平文が正しくないことが証明される。

3．5 回復権限検証

キーリカバリシステムにおいて、鍵回復要求者は多大な権限を持つ。そのため、鍵回復要求者の回復権限については、木目細かい設定ができることが必要である。本システムでは、鍵回復センタでの鍵回復時に

(1) 鍵回復要求者の妥当性
(2) 回復対象メッセージの妥当性
(3) KRB の妥当性
(4) 回復条件

の四段階で回復権限をチェックすることにより、不正な回復要求を防ぐ。

鍵回復要求者の正当性は、二種類の方法によって検証される。(1) あらかじめ有効な鍵回復要求者の公開鍵を鍵回復センタに登録しておき、回復要求を鍵回復要求者から鍵回復センタへの署名親展データとすることでチェックできる手法がその1つである。しかし、(1)のように全鍵回復要求者を鍵回復センタに登録しなければならず、正当な鍵回復要求者が変更された場合などに緊急に対処するのが困難となり、システムの柔軟性に欠ける恐れがある。上記ケースへの対策として (2)然るべき認可機関によって鍵回復要求者からの回復要求に認可が与えられている場合、鍵回復センタではその鍵回復要求者を正当とみなす手法を用意している。

回復対象メッセージの妥当性検証には、KRB中に回復対象メッセージのメッセージ署名を含めることにより対処した。鍵回復要求者は、回復対象メッセージ中から、該当するメッセージ署名を取得し、鍵回復要求中に挿入した上でKRCに送付する。これによって鍵回復センタでは、KRB中のメッセージ署名と、鍵回復要求中のメッセージ署名のマッチングを行い、鍵回復要求者が正しく鍵回復要求を申告

しているかどうかをチェックすることが可能となる。

さらに、KRB が鍵回復要求者によって偽造／改竄されていないことは、暗号化データ内から鍵回復要求者が取得できる情報と同じ情報を KRB に入れておくことによって、鍵回復センタでの確認が可能である。

また、回復条件については、鍵回復センタ側で鍵回復要求に対する正当性チェック項目として

- 回復対象の暗号化データの作成ユーザ
- 回復対象の暗号化データの復号ユーザ
- 回復対象の暗号化データに対して鍵回復処理が有効な時間(帯)

を用意した。上記各項目にはさらに詳細な条件の設定が可能になっており、これによって鍵回復要求者による回復条件の柔軟な設定ができる。

3．6 回復処理ログの改ざん検証

鍵回復センタが鍵回復を行った場合、誰からの要求でどのように鍵回復処理を実施したか、その処理ログを残す必要がある。さらに、鍵回復センタが不正な処理を行っていないことを証明するためには、回復処理ログに対して改竄が行われた場合にその検出ができることが最低限必要である。本システムでは、回復ログレコード毎の署名、回復ログテーブル全体の署名を利用することによって、期限付きの回復ログテーブルの非改竄を保証している。

4．開発システム概要

4．1 システム構成

上記の設計指針をもとに試作したシステムのシステム構成を図4－1に示す。各構成要素とその役割は次の通りである。

(1) クライアント
暗号化データの交換を行うユーザである。KRB 付き暗号化データの生成／復号、および KRB 付き暗号化データにおける KRB の改ざん検証などを行う。

(2) 鍵回復要求者(KRR)
鍵回復センタへの鍵回復要求の発行、鍵回復センタからの鍵回復応答をもとに鍵またはデータを回復する機能を持つ。認可機関からの認可をもとに鍵回復要求を作成／発行する機能も併せ持つ。

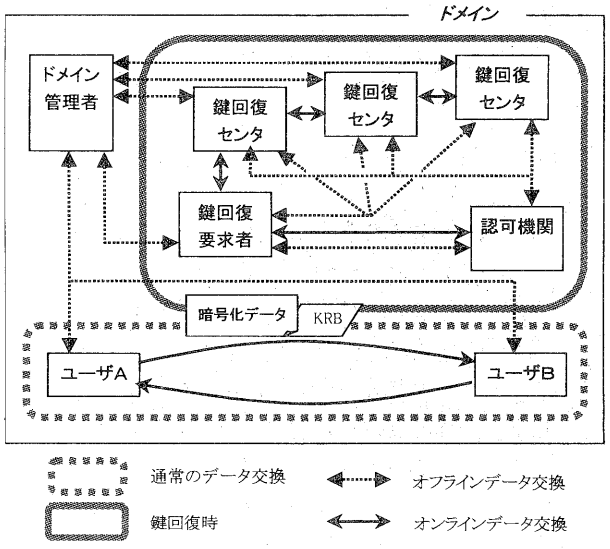

図4－1 システム構成図

(3) 鍵回復センタ(Key Recovery Center, KRC)
鍵回復要求から鍵もしくは鍵断片を抽出し、鍵回復の妥当性を検証した上で鍵回復要求者に返却する。認可機関が発行した認可証による鍵回復要求を受信した場合は、認可証の検証等も行う。

(4) 認可機関

鍵回復要求に対して認可を与える、すなわち認可証を発行する機能を持つ。

(5) ドメイン管理者

鍵回復センタとそのユーザが所属するドメインに関する情報を管理する機能を持つ。

4．2 処理概要

鍵回復に至る一連の動作は次のように実施される。

◆ 環境設定

ユーザをドメインに登録する。この時、ユーザはドメインマネージャによって発行された鍵回復ポリシーを自マシン中に設定する。

◆ 暗号化データ交換

KRB付き暗号化データの作成／復号処理を行う。これは通常の暗号化データ交換処理と同様である。

◆ 鍵回復

鍵回復要求者は、ユーザが作成したデータからKRBを抽出して鍵回復要求を作成する。この時、ドメイン内での鍵回復要求者の定義によって鍵回復ルートが異なる。

◇ 鍵回復要求者がKRCに静的に登録されていた場合

鍵回復要求者はユーザが作成したデータからKRBを抽出して鍵回復要求を作成し、鍵回復センタに送付する。 鍵回復センタでは鍵回復の妥当性検証を行い、正当な鍵回復と認められた場合には抽出した鍵を鍵回復要求者に返却する。鍵回復要求者では、鍵回復センタから返却された鍵でデータ回復を実施する。

◇ 鍵回復要求者が鍵回復センタに登録されていない場合

鍵回復要求者はユーザが作成したデータからKRBを抽出し、認可機関に対して認可許可依頼を作成／発行する。認可機関では、受け取った認可許可依頼の内容を検討した上で、妥当であれば鍵回復要求者を認可する。鍵回復要求者では、認可機関から発行された認可証とKRBから鍵回復を作成し、鍵回復センタに送付する。鍵回復センタでは認可証の正当性検証を行うことによって鍵回復の妥当性を判断する。正当な鍵回復と認められた場合には、抽出した鍵を鍵回復要求者に返却する。鍵回復要求者では、鍵回復

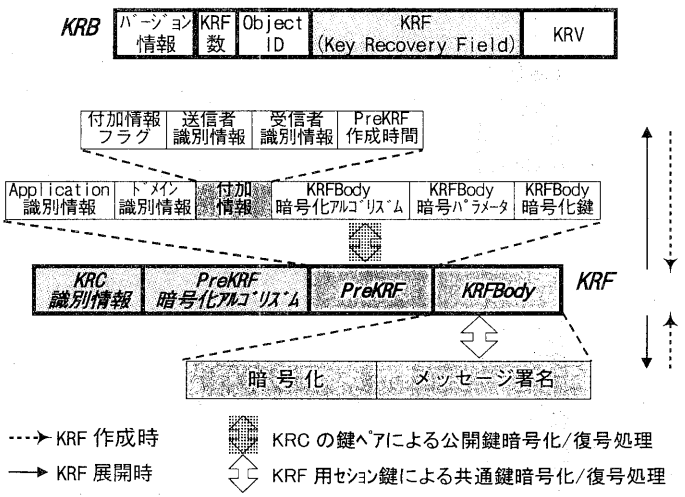

図4－2 KRB 構造

センタから返却された鍵でデータ回復を実施する。

4．3 ＫＲＢの構造

上記の構造・機能をもとに、我々は KRBを図4－2のように設計した。中央のグレー部分のデータがKRF である。KRF の作成時には点線矢印の順に構成され、展開は逆の順で行われる。

5．ビジネスシステムへの適用イメージ

本キーリカバリシステムを実際のビジネスシステムに適用する場合、その適用形態は大きく(1)Law Enforcement、(2)Lost Key、(3)復号条件制御 の三種類に分類される。以下それぞれの形態ごとに(a)暗号化データ作成形式、(b)鍵回復権限、(c)対象データの三点について各システム要件を検討する。

◆ Law Enforcement

システムを Law Enforcement 対応にする場合、最も重要な要件は暗号化データに KRB が付与されない状態を避けることである。つまり、KRB はユーザの意志に関わらず添付され、ユーザがキーリカバリを意識しないようにすべきであるといえる。このため、KRB はドメイン加入時に配布される鍵回復ポリシーによって自動的に作成されることが適当である。鍵回復の観点から見ると、本形態では鍵回復要求者が最も多大な権限を持つため、ドメイン内の組織構造等に即した鍵回復要求者が設定されるべきである。また対象データは通信データ、蓄積データの両データである。

◆ Lost Key

キーリカバリを Lost Key 対策として利用する場合は、鍵バックアップの一種として利用するため、ユーザが意識的に KRB を作成し、暗号化データに添付する形態が望ましい。この時の鍵回復要求者は、本人と本人が認めた第三者であり、各々を鍵回復センタで認証することによって実現できる。また対象データはシステムの性質上、蓄積データに限定されるといえる。

◆ 復号条件制御

上記二形態の他に、キーリカバリを鍵回復の条件制御の一方式として利用する場合が考えられる。この時、KRBは回復対象の鍵と、その復号条件を含む。復号条件はユーザによって意識的に決められるものであるので、ユーザは意識的にKRBの作成を行う必要がある。鍵回復権限は、復号条件を満たす全ユーザに与えられるため、比較的多数の人間に対象データの鍵回復権限を与えることが可能である。また対象データは通信データ、蓄積データの両データである。

6．展望

今回、我々はキーリカバリシステムの試作を行った。だが、現状では試作段階であり、その性能測定は必須である。今後、ディスク容量、鍵回復に要するKRC数、ドメインの規模等に関する評価を行い、どのようなシステムにおいてキーリカバリが適用可能であるのか、さらに検討する必要があると考えている。そのため、前章で示したようなビジネスモデルを複数用意し、性能測定と分析を行う予定である。また、この性能測定をもとに、実際のビジネスへの適用を志向した鍵回復技術のコンポーネント化も検討していく必要があると考えている。