# 複数セキュリティ領域間の暗号通信に適した鍵管理方法

5H－2

橋本和夫[1]　宝木和夫[1]　山下正弘[2]
(株)日立製作所システム開発研究所　同汎用コンピュータ事業部

## 1．はじめに

コンピュータの普及と共に、コンピュータ本体のセキュリティ機能を強化したいというニーズが増大している。従来、コンピュータ内部に暗号化のメカニズムを実現する方法として米国暗号標準DESを用いる方法が有名である[1]。しかし、国際標準化機構ISOでは、暗号化方法は国際規格として一本化しないことに決まり、さらに複数のセキュリティ領域でそれぞれ個別のセキュリティメカニズム等を設定するセキュリティ方策という概念が導入されている[2][3]。このような複数暗号、複数セキュリティ領域の考えに適したセキュリティシステムの構築方法として、手続き秘匿、公開の両暗号化方法を併用した鍵管理方法を開発した。本稿では、この鍵管理方法の基本的考え方、概要、適用例について述べる。

## 2．基本的考え方

今、あるコンピュータAがそれぞれセキュリティ方策の異なる領域1、2、および3に属しているとする(図1参照)。

この時、コンピュータAの内部に次のメカニズムを同時に実現したいことがある。

(1)手続き秘匿型暗号方式による暗号化

ファイル暗号のように同一ユーザが暗号化／復号をする場合(領域3)や、限られた相手としか暗号通信を行わない場合(領域2)、安全性を増すために該領域内で手続き秘匿の暗号方式を用いたい。

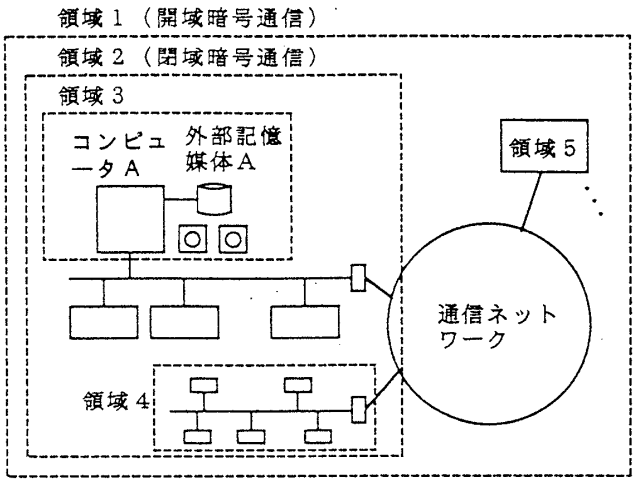


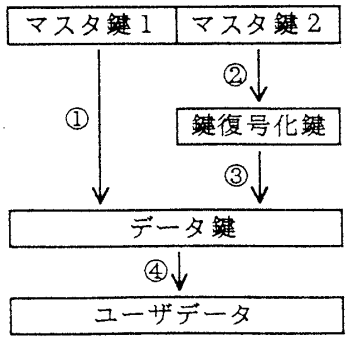

図1．セキュリティ領域の構成例

(2)手続き公開型暗号方式による暗号化

コンピュータAがオープンな環境で不特定多数を相手として暗号通信を行う場合(領域1)、手続き公開の暗号方式を用いたい[4]。

上記、2つの要求を満たすため、コンピュータAの内部のメカニズムを次のように構成する。

(1)一般に、実装、および運用上の負荷が大きい鍵管理のメカニズムはなるべく共通的なものにする。

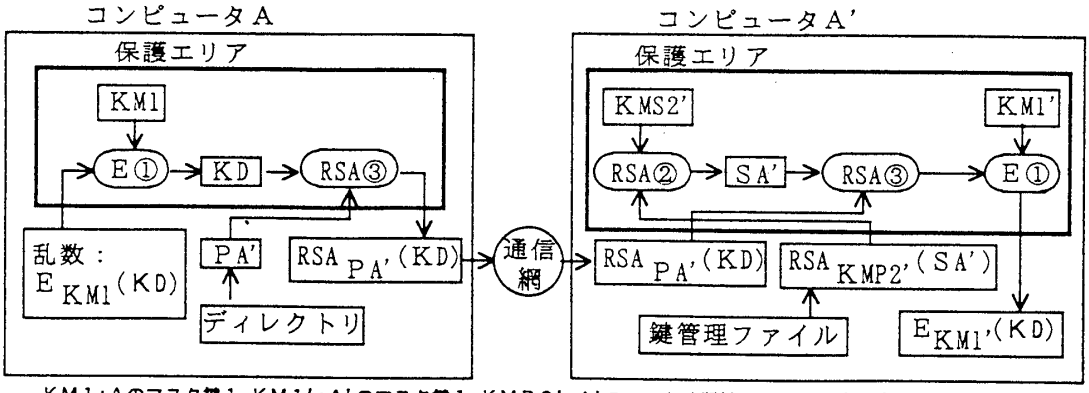



| 暗号化個所 | 暗号化方式 | | |
|---|---|---|---|
| | 領域1 | 領域2 | ･･･ |
| ① | 手続き秘匿 | 手続き秘匿 | 同左 |
| ② | 公開鍵暗号 | 公開鍵暗号 | 同左 |
| ③ | 公開鍵暗号 | 公開鍵暗号 | 同左 |
| ④ | 共通鍵暗号 | 手続き秘匿 | ･･･ |

図2．階層的鍵管理の基本構成

Key Management Method Designed for Multi-domain Cryptographic Communications

Kazuo HASHIMOTO[1], Kazuo TAKARAGI[1]: Systems Development Laboratory, Hitachi. Ltd[1]
Masahiro YAMASHITA[2]: General Purpose Computer Division, Hitachi. Ltd[2]




KM1：Aのマスタ鍵1，KM1'：A'のマスタ鍵1，KMP2'：A'のマスタ公開鍵2，KMS2'：A'のマスタ秘密鍵2，
PA'：A'の鍵暗号化鍵，SA'：A'の鍵復号化鍵，KD：データ鍵，E：手続き秘匿型暗号，RSA：公開鍵暗号

図3．データ鍵の共有フロー例

（2）ユーザデータの暗号化を行うメカニズムは、複数個用意しておき、必要に応じて選択する。

## 3．概要

図2に示すような鍵管理、およびユーザデータの暗号化メカニズムを構成する。

（1）マスタ鍵→鍵復号化鍵→データ鍵の三階層の鍵管理を構成する。

（a）多者間の鍵配送を行うときに使われるメカニズム(図2の②、③)には暗号化の安全性と利便性に優れた公開鍵暗号を採用する。

（b）コンピュータA内部のみでのデータ鍵の保護に単独で用いるメカニズム(図2の①)には安全性と高速性に優れた手続き秘匿型の暗号方式を採用する。

（c）鍵暗号化鍵(公開鍵)は領域毎に設定するようにし、ある領域内の公開鍵は該領域内部でのみ公開し、外部には秘密にする。

（2）ユーザデータの暗号化(図2の④)には、各領域のセキュリティ方策に応じて共通鍵暗号、手続き秘匿型暗号を用いる。

（3）コンピュータ内部を保護エリアと一般エリアに分け、「秘密にすべき鍵は裸の形では保護エリアから外には出さないようにする」という原則[5]を守り、次の鍵共有を行う。

（a）データ鍵の共有

送受信者間でユーザデータの暗号化、復号を行うのに必要なデータ鍵の共有を行う。所定の処理の後、各コンピュータはそれぞれで数値が異なるマスタ鍵KM1およびKM1'で暗号化された状態のデータ鍵をそれぞれの一般エリアにおいて保持する（図3参照)。

（b）鍵復号化鍵の共有

権限委譲等で別のコンピュータで暗号化データの復号を可能とするため、鍵復号化鍵を暗号通信によって配送する。これは、予め設定されたコンピュータでのみ公開されているマスタ公開鍵2を参照することにより行う。

## 4．適用例

本鍵管理方式を実現する暗号装置を開発した。本暗号装置は、上記の保護エリアの機能をハードウェアによって実現するものである。

（1）公開鍵暗号としてRSA[6]、共通鍵暗号としてMulti2[7]、および手続き秘匿型暗号をそれぞれLSI化し、実装した。

（2）外部記憶装置への適用にあたり、データ圧縮の効果を保持するため、データを圧縮した後、暗号化するメカニズムを追加した。これは、外部記憶装置にユーザデータの暗号化メカニズムを追加することにより実現した。

大型計算機日立M-880に本暗号装置を接続し、テストしたところ、良好な処理性能を確認した。

## 参考文献

(1)ｶｰﾙ.H.ﾏｲﾔｰ,ｽﾃｨｰﾌﾞﾝ.M.ﾏﾃｨｽ,瀬戸他訳：暗号/ｺﾝﾋﾟｭｰﾀ・ﾃﾞｰﾀ保護の新展開：自然社 1986年

(2)ISO/IEC9979：Procedures for the Registration of Encipherment Algorithms(1991)

(3)ISO/IEC/SC27/N689:Working Draft13335"Guidelines for the Management of IT Security"(1993)

(4)Bellovin,S.M.：Limitation of the Kerberos Authentication System, Computer Communication Review,Vol.20,No.5,pp119-132(1990)

(5)宝木：暗号方式と応用,情報処理,Vol.32,No.9,pp714-723(1991)

(6)R.L.Rivest et al：A Method for btaining Digital Signature and Public Cryptosystems：Com. of the ACM 21,2,1978

(7)k.Takaragi et al：On Differential Cryptanalysis,IEICE TRANS. VOL.E74 NO.8 AUGUST 1991