

階層型セキュアデータベースの提案とプロトタイプシステムの実装
**A Proposal of Hierarchical Secure Database, and Implementation of
 Prototype System**

山崎 修司†

宮西 洋太郎†

高橋 修†

Shuji Yamazaki

Yohtaro Miyanishi

Osamu Takahashi

1. はじめに

近年、企業の顧客情報流出などの問題でデータの保護が重要になってきている。データ保護に関して、企業の人事情報システムにおいては、上司は部下のデータを閲覧できるが、部下は上司のデータを閲覧できない「データの階層型」と、上司でも部下のデータを書き換えたりすることができない「データの一方向性」が求められている。そこで本研究では単にアクセス制御を行うのではなく、PGPを使用してデータ認証やデータ保護に伴う「データの一方向性」を実現し、PGPに使用する暗号鍵を階層的に持つことで「データの階層型」を実現する方式を考案し^[1]、プロトタイプシステムの構築を行ったので報告する。

2. 階層型セキュアデータベースの要件

本稿では企業の3階層（部長、課長、担当者）での人事情報システム（個人データの閲覧）を例にして、提案方式の適応を述べる。ここで、階層型セキュアデータベースの要件を以下の5つとする。

・階層的アクセス制御

個人の情報は本人と上司のみが閲覧することができ、他の人は閲覧できない。

・データ認証

閲覧している個人情報が確かに本人の記述したものであるとわかる。

・データ保護

不正アクセスされても暗号化で内容がわからない。

・データ確定（否認防止）

上司によってデータ確定が行われたら、たとえ本人でも書き換えできない。

・データの一方向性

上司でも部下のデータを閲覧することはできるが、書き換えることはできない。

3. PGPを用いた階層型セキュアデータベースの構築手法

PGP (Pretty Good Privacy) は共通鍵暗号と公開鍵暗号を組み合わせたハイブリッド暗号で共通鍵暗号の暗号化の速さと公開鍵暗号による電子署名を行う機能を持つ

ている^[2]。

階層型セキュアデータベースを構築するためにデータベースと暗号鍵の管理方法や種類等と暗号化方法を以下に記述する。

(1) データベース

データの区別を行うために暫定データベースと確定データベースを作成する。暫定データベースに登録してあるデータは作成した本人であれば変更可能である。確定データベースに登録されているデータは直属の上司により確定操作（暗号化）が行われ、作成した本人でさえ変更することができないようになる。確定データは、さらに上の上司が閲覧するものとする。

(2) 暗号鍵

通常のPGP暗号では1対1の暗号化方式があるので、同じ暗号文に対して、1人しか見ることができない（担当者が課長の公開鍵でPGP暗号化した場合に部長は見ることができない）ので、以下の2種類の鍵のペアを使用する方法を考案した。

・自分のデータ保護の鍵ペア

・上司に部下のデータを読み取らせる鍵ペア

また、階層型に対して上位になればなるほど、所有する鍵の数が増加する。管理する鍵の数を減らす方法として、マスタ鍵を使用する方法がある^[1]。しかし、この方法では個人ごとの電子署名の復号はできるが、個人ごとの認証を行うことができない。本稿では、2階層下の部下のデータを復号する為に必要な鍵を1階層下の部下のデータに加えて登録することにより管理する鍵の数を少なくした。

3階層の場合の鍵の種類を図1に示す。

TP	担当者の公開鍵
TS	担当者の秘密鍵
KP	課長の公開鍵-1(課長データ用)
KS	課長の秘密鍵-1(課長データ用)
KP'	課長の公開鍵-2(担当者データ用)
KS'	課長の秘密鍵-2(担当者データ用)
BP	部長の公開鍵
BS	部長の秘密鍵

図1. 3階層の場合の鍵の種類

†公立はこだて未来大学大学院システム情報科学研究所

(3) 暗号化方法

平文 D を PGP で D^* に暗号化するときの表記を以下のようにする。

$$D^* = PGP_{K_{ss} K_{pp}}(D)$$

K_{ss} : self(自己)の secret key(秘密鍵)

K_{pp} : partner(相手)の public key(公開鍵)

また、暗号文 D^* を PGP で D に復号化するときの表記を以下のようにする。

$$D = PGP_{K_{ss} K_{pp}}^{-1}(D^*)$$

上記の記号を用いて 2 種類の鍵ペアを使用して 3 階層の場合の PGP 暗号化方法を図 2 に示す。

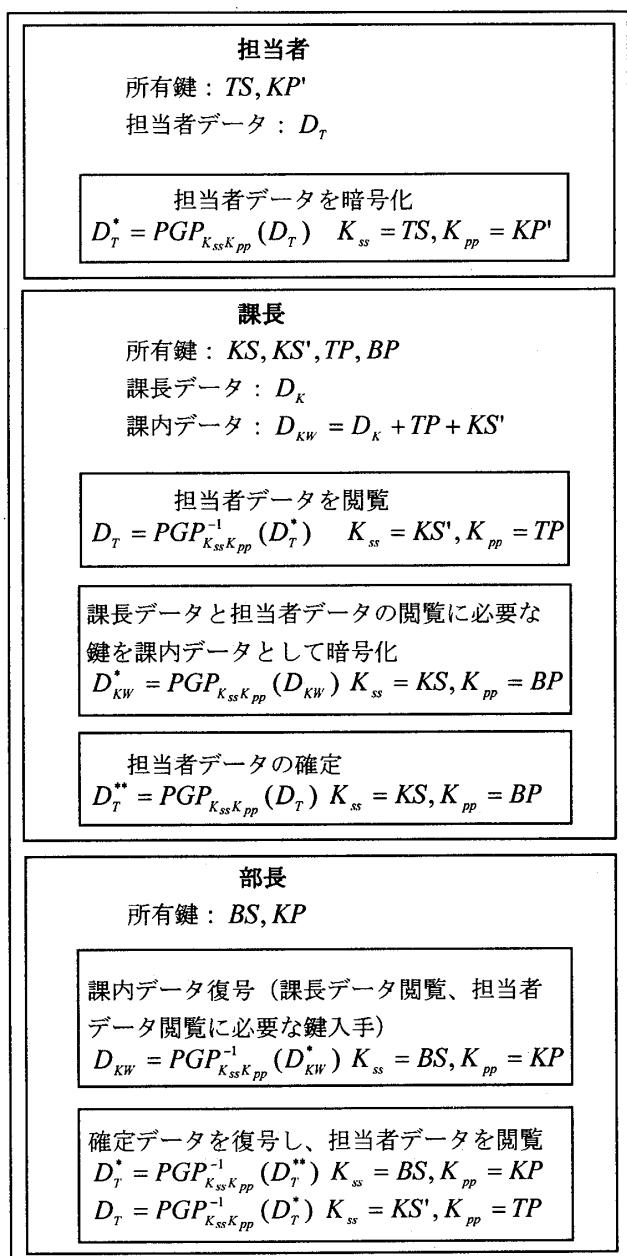


図 2. 3 階層の場合の PGP 暗号化方法

4. プロトタイプシステムの実装と動作確認

PGP 暗号を行うには公開鍵暗号、秘密鍵暗号、ハッシュ関数が必要である。本プロトタイプシステムでは公開鍵暗号には RSA、秘密鍵暗号の代用としてランダム数との XOR、ハッシュ関数には MD5 を使用した。RSA 暗号の鍵の長さを 16 ビット、XOR に使用する鍵の長さを 128 ビットで作成し、システムとして動きを確認したところ、正常に動作していることが確認できた。本稿では課長 1 人、担当者 1 人の場合を記述したが、複数の課が存在し、複数の担当者が課に属している場合においても、要件を満たす動きをした。

次に、5 つの要件が満たされているか記述する。

・階層的アクセス制御

上司の公開鍵を使用して PGP 暗号化することにより直属の上司のみ閲覧可能にする。2 階層以上の上司に対しては 2 種類の鍵ペアを使用することで解決できる。

・データ認証

PGP 暗号に含まれる電子署名により実現できる。

・データ保護

暗号化で実現できる。

・データ確定(否認防止)

部下が登録したデータを上司が再 PGP 暗号化することで作成した本人も変更不可能にことができる。

・データの一方向性

PGP 暗号化により閲覧できるが、電子署名が含まれるので書き換えはできない。

5. まとめと今後の課題

本稿では、企業の人事情報システムにおいて求められる「データの階層型」と「データの一方向性」を単にアクセス制御を行うのではなく、PGP 暗号と暗号鍵を階層的に持つことを利用して実現する方式を考案した。また、提案した方式を用いてプロトタイプシステムの構築を行った。

今後の課題としては、暗号鍵の長さを変化による暗号、復号化の時間変化などのシステムの性能評価方法の考案と、それに基づいた性能評価を行う予定である。また、鍵の変更、変更に伴う再暗号化や配送など鍵の管理方法の検討を行う必要がある。

参考文献

- [1] 山崎 宮西 「階層化セキュアデータベース構築手法の提案」 DPS/CSEC(2004)
- [2] Simon Garfinkel 「PGP 暗号メールと電子署名」 オーム社(1996)
- [3] 小山 「RSA 公開鍵暗号法のマスタ鍵」 電子情報通信学会論文誌 D(1982)