3A-3

階層的一方向性データのセキュアな管理方式とその評価

山崎　修司†　　高橋　修†　　宮西　洋太郎‡　　小西　修†　　宮本　衛市†

公立はこだて未来大学†　宮城大学‡

１．はじめに

近年、企業内情報の流出事件多発などにより情報の安全性についての関心が高まっている。データ保護に関して、企業の人事考課システムにおいては、セキュリティの一般的な要件であるデータの守秘、完全性、認証、否認防止の機能の他に、上司のみ部下のデータを閲覧できる階層的アクセス制御が求められる。この階層的アクセス制御は一方向性を持つ。ここでの一方向性とは上司といえども部下データの読み込みはできるが、書込みができないこと、及び上司の確定操作が行われた後は、作成者自身も書き換えをできない機能を意味する。

従来、このような機能はアクセス制御や運用方法により実現してきた。しかし、アクセス制御が破られた場合に、データが流出する恐れがある。そこで、本研究では企業の人事データなどのような階層型のデータに対して、単にアクセス制御を行うのではく、PGP 暗号[1]の仕組みを用いてデータの守秘、完全性、認証、否認防止を実現し、PGP 暗号に用いる公開鍵と秘密鍵のペアを 2 種類持つことで階層的アクセス制御を実現できる手法を提案する。また、提案した方式のプロトタイプシステムを構築し、評価を行う。

２．階層型セキュアデータベースの要件

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。

(1)階層的アクセス制御

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。また、上司は部下が作成したデータに対してコメント（考課）を付け加えることはできるが、部下が記述した部分については書き換えることはできない。

(2)守秘

データを暗号化し、アクセス権のない不正ユーザがデータを読み込んだとしても、解読できないことを保証する。

(3)完全性

偶然または故意に行われる不正なデータ変更がなされていないことを保証する。

(4)認証

データを作成した人が本人であることを保証する。

(5)否認防止

上司の確定操作が行われた後は、作成者自身も書き換えることができない。

３．階層型セキュアデータベースの構築手法[2]

(1)鍵の設定方式

通常の PGP 暗号は 1 対 1 の暗号化方式であるので、同じ暗号文に対して 1 人のみ閲覧可能である。そこで、次の 2 つの鍵を使用することで階層的アクセス制御を行う方式を提案する。

鍵 1：自分のデータ保護の鍵ペア

鍵 2：上司に自分のデータを読み取らせる鍵ペア

(2)鍵管理方法

・鍵 1 と鍵 2 の公開鍵はサーバで管理し、必要に応じて誰でも取得できるようにする。
・鍵 1 の秘密鍵は自己管理とする。
・鍵 2 の秘密鍵は上司がデータを確定する際にデータの中に組み込む。

鍵 2 の秘密鍵をデータの中に組み込むことにより、どの階層の人でも管理する鍵が 2 種類で済み、システムのスケーラビリティを実現できる。

(3)提案方式による暗号化の流れ

企業の３階層（部長－課長－担当者）について担当者が作成したデータを 2 階層上の部長が閲覧するまでの流れを以下に示す。ここで使用する鍵の種類を表 1 に示す。

表１　3 階層で使用する鍵の種類

第 i 課の第 j 番の担当者の公開鍵	TP_{ij}
第 i 課の第 j 番の担当者の秘密鍵	TS_{ij}
第 i 課の課長の公開鍵 1	KP_i
第 i 課の課長の秘密鍵 1	KS_i
第 i 課の課長の公開鍵 2	KP_i'
第 i 課の課長の秘密鍵 2	KS_i'
部長の公開鍵	BP
部長の秘密鍵	BS

また、平文 D を PGP により 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）

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

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

①データ作成・更新(担当者 ij)

担当者 ij はデータ d_{ij} を作成し、PGP で暗号データ d_{ij}^* を作成してデータベースに登録する。

$$d_{ij}^* = PGP_{K_{ss}K_{pp}}(d_{ij}),\ K_{ss} = TS_{ij},\ K_{pp} = KP_i'$$

②担当者データ閲覧(課長 i)

課長 i は暗号化データ d_{ij}^* をデータベースから取得し、PGP 復号処理を行い、データ d_{ij} を閲覧する。

$$d_{ij} = PGP^{-1}_{K_{ss}K_{pp}}(d_{ij}^*),\ K_{ss} = KS_i',\ K_{pp} = TP_{ij}$$

A Secure Management System for Hierarchical and Unidirectional Data, and its Evaluation

† Future University-Hakodate

‡ Miyagi University

③担当者データ確定（課長 i）

課長 i は担当者 ij に対してのコメント（考課）と担当者 ij の暗号化データを復号化する為に必要な鍵を担当者 ij の暗号化データに加え、再 PGP 暗号化を行う。

$$d_{ij}^{**} = PGP_{K_{ss}K_{pp}}(d_{ij}^{*} + KS_i^{'} + comment\ )$$

$$K_{ss} = KS_i,\ K_{pp} = BP$$

④担当者 ij データの閲覧（部長）

部長は担当者 ij のデータに対して課長 i が確定したデータを PGP 復号化し、課長 i の担当者 ij に対するコメントと暗号化担当者 ij データを復号化する為に必要な鍵を入手する。次に、その鍵を用いて暗号化担当者 ij データを PGP 復号化して個人データ d_{ij} を閲覧できる。

$$d_{ij}^{*} + KS_i^{'} + comment\ = PGP_{K_{ss}K_{pp}}^{-1}(d_{ij}^{**})$$

$$K_{ss} = BS\ ,\ K_{pp} = KP_i$$

$$d_{ij} = PGP_{K_{ss}K_{pp}}^{-1}(d_{ij}^{*}),\ K_{ss} = KS_i^{'},\ K_{pp} = TP_{ij}$$

ここでは 3 階層について記したが、4 階層以上のモデルに対しても同様の手続きを再帰的に行うことにより、実現できる。

４．プロトタイプシステムの実装[3]

プロトタイプシステムとして以下の機能を持ったシステムを構築した。

①登録機能－自分の情報を入力し、暗号化してデータベースに保存する。

②閲覧機能－閲覧する相手の暗号化データを復号化して閲覧する。2 階層以上の部下のデータを閲覧する為には、閲覧する相手の上司によって確定されたデータを復号化し、さらに復号化する鍵を入手して復号化していく。

③確定機能－部下のデータの閲覧後にコメント（考課）を加えて暗号化してデータベースに保存する。

これらの機能をプログラミング言語 Visual Basic を用いて作成した。システム構成図を図 1 に示す。

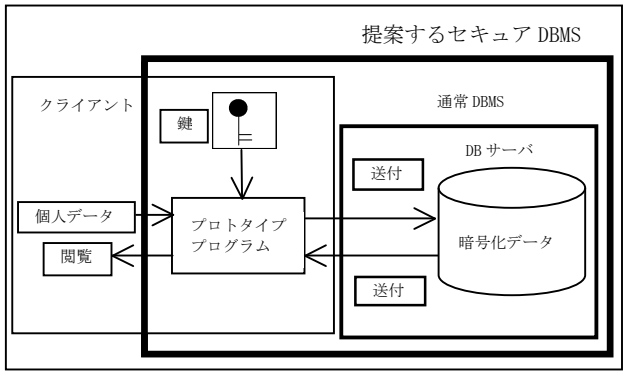

図 1 システム構成図

５．性能評価

5.1 評価条件

システムの評価として階層の深さの変化に伴う処理時間の変化を測定した。ここでの処理時間について、暗号時間はデータの暗号化から DB に書き込むまでの時間を表し、復号時間は DB から暗号化データを取得して、復号化した結果を画面に表示するまでの時間を表す。

今回は以下の条件の下で測定を行った。

個人情報 1600 文字(3200Byte)
追加するコメント 400 文字（800Byte）
公開鍵暗号鍵長 96bit
共通鍵暗号鍵長 128bit
動作環境 OS Windows XP
CPU 1.2GHz　メモリ 256MB

表 2. 階層の深さの変化による処理時間の変化

	階層の深さ	1	2	3	4	5	6
暗号化処理	暗号化回数	1	1	1	1	1	1
	暗号化するデータ(Byte)	3200	5318	8218	12078	17230	24102
	暗号時間(s)	0.2422	0.2446	0.2522	0.2642	0.2726	0.2904
復号化処理	復号化回数	1	2	3	4	5	6
	復号化するデータ(Byte)	4504	7404	11264	16416	23288	32448
	復号時間(s)	0.2724	0.6388	1.2358	2.177	4.2522	8.202

5.2 性能評価の結果と考察

評価結果は表 2 の通りで、階層が深くなっても PGP 暗号化を行う回数は 1 回であるので、暗号化するデータ量が数倍に増えても、要する時間は微増だった。しかし、復号化については階層の深さ分だけ復号化処理を行わなければならないので、復号時間は暗号化回数に比例して増えている。

プロトタイプシステムでは階層が浅い場合は、実用レベルの処理時間で実現できたが、階層が深くなると処理時間が多くなる。しかし、通常の企業形態や運用上はせいぜい 5 階層くらいまでしか使わないと考えられるので、実用で使われる鍵の長さ(256bit 以上)に対しては高速なプログラム言語や暗号アルゴリズムを用いることで、実現可能であると考えられる。

６．まとめと今後の課題

本研究では企業の人事システムで扱う考課データなどの階層型のデータに対して、PGP 暗号を利用し、暗号鍵を階層的に持たせることにより、よりセキュアなデータベースを構築する手法を提案した。さらに、プロトタイプシステムを実装し評価を行った。

今後の課題は、鍵の紛失や人事異動に伴う上司の変更などによる鍵の変更方法の検討を行う。

参考文献

[1] Simson Garfinkel, 「PGP 暗号メールと電子署名」 オーム社(1996)

[2]山崎、宮西、「階層化セキュアデータベース構築手法の提案」情報処理学会DPS、CSEC合同研究会、2004年3月

[3]山崎、宮西、高橋、「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」FIT2004、2004 年 9 月