社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＰＳ－117　(1)
2004－CSEC－　24　(1)
2004／3／4

階層化セキュアデータベース構築手法の提案

山崎　修司　　宮西　洋太郎

近年、コンピュータやコンピュータネットワーク技術は急激に発展し、個人の情報や企業秘密などもインターネットで行き交うようになった。それに伴いクラッカーなどのネットワークへの不正侵入者、破壊者の技術も発達し、犯罪が悪質化してきている。そのため、盗聴や改ざんなどを防止するためにもセキュリティが重要になってきている。また、企業の人事システムなどは本人と上司のみがデータを見ることができるような階層型のデータベースになっており、ここでもセキュリティは重要である。そこで、本稿では階層データベースを作成する際にアクセス制御を行うだけではなく、PGP 暗号化プログラムを用いて、データ認証、データ保護、データの確定を行うセキュリティの高い階層化データベースの構築手法を提案する。

A Proposal of Hierarchical Secure Database Construction Technique

Shuji Yamazaki　　Yohtaro Miyanishi

Recently, computer and computer network technologies have been developed rapidly, and individual information and company secret are flowing on the Internet. According to it, the technology of the illegal intruder to networks, such as a cracker, and a destroyer also progresses, and a crime is turning wicked. Therefore, security is becoming important, in order to prevent tapping or alteration etc. Moreover, the personnel system of a company etc. is the hierarchical database with which only in person and a superior can see data, and security is important also here. Then, in this paper, we propose construction technique of the hierarchical database of high security when creating a hierarchical database, using encryption program called PGP, it performs not only access control but also data authentication and data protection and data decision.

１．はじめに

近年、コンピュータやコンピュータネットワーク技術は急激に発展し、個人の情報や企業秘密などもインターネットで行き交うようになった。それに伴いアクセス制御や個人認証などのセキュリティが重要になってきている[1]。

また、企業の人事データなどは個人の勤続年数や取得資格などの個人情報が含まれており、本人と上司のみだけが見ることがでるが、他の人には決して見られてはならないような階層型のデータベースになっていて、セキュリティがとても重要になってくる。そこで本稿では PGP

公立はこだて未来大学大学院システム情報科学研究科
Graduate school of system information science, Future University-Hakodate

の特性を利用して、このような階層型のセキュアなデータベースの構築手法についての提案を行う。

本稿では、まず PGP の特性について述べる。次にその PGP の特性を生かした階層化データベースの構築手法を企業の人事システムへの適応例を用いて述べる。本提案の実装、評価は今後の課題である。

２．ＰＧＰについて

PGP（Pretty Good Privacy）は、共通鍵暗号と公開鍵暗号の利点を組み合わせたハイブリッド暗号を用いて、電子メールおよびコンピュータ上に格納されたファイルのセキュリティを保護するプログラムである[2]。

平文を暗号化する際には、PGP はまず平文のハッシュ値を計算する。次に、そのハッシュ値を送信者の秘密鍵により署名を行う。続いて、セッション鍵を作成する。これは、使い捨ての共通鍵である。この鍵は、マウスの動きと打キーから作り出された乱数である。この十分に安全で高速な共通鍵暗号により、平文と署名を暗号化する。暗号化が終わると、セッション鍵は受信者の公開鍵で暗号化される。この公開鍵で暗号化されたセッション鍵は、暗号文とともに受信者に送られる。

復号化は、この手順を逆に行い、最終的に送信されてきたハッシュ値と計算したハッシュ値が一致すれば、送られてきた平文が改ざんされていなく本人が送ったものである。

３．ＰＧＰを用いた階層化セキュアデータベース構築手法

企業の人事システムは本人と上司のみが情報を見ることができる階層型のようなデータベースになっている。一般的にはアクセス制御により管理を行っているだけである。また、データベースの内容を暗号化して盗聴されても大丈夫なデータベースの構築手法[3]もある。しかし、この方法により階層化データベース構築を行う場合、鍵管理サーバが必要になる。

3.1 セキュア人事システムの要件

セキュア人事システムのデータベースは作成者本人が書き換え可能な「暫定データ」と上司による締め切り後の「確定データ」に分ける。「確定データ」は作成者本人もデータを書き換えることができないようにする。セキュア人事システムの要件を以下の４つの項目として設定する。

（１）階層的アクセス制御

パスワードによりアクセス制御は行うが、上司でない人は暗号文を復号化することはできない。上司は自分の秘密鍵と部下の公開鍵を持つことにより、部下のデータを見ることができる。しかし、上司といえどもデータを書き換えることはできない。

（２）データ認証

上司は受信した暗号文に付属していたハッシュ値と復号化した平文から計算されたハッシュ値を比較して一致すれば部下が作成したものであると確認することができる。自分のデータが書き換えられていないかどうかは「暫定データ」と自分のパソコンにあるデータを比較し、確認できる。

（３）データ保護

データベースのレコードを暗号化して格納してあるので不正アクセスされても内容は分からない。

（４）データ確定

上司による締めきり（本書確定）後は、本人といえども「確定データ」は書き換えることができない。ただし、書き換えの結果は「確定データ」を復号化し、自分のパソコンにあるデー

タと比較し、確認できる。データの確定は稟議書やカルテなどでも行われている[4]。

この４つの要件を達成するために PGP を用いた階層化データベースの構築手法について示す。

本稿では企業の 3 階層の人事システムについて述べる。（図１）

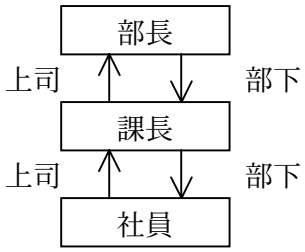

図 1　企業の 3 階層

3.2 PGP による暗号化と復号化

人事システムの PGP を用いた暗号化と復号化の方法を以下の記号を用いて記述する。

HP_{ij} ：第 i 課の第 j 番社員の公開鍵

HS_{ij} ：第 i 課の第 j 番社員の秘密鍵

KP_i ：第 i 課の課長の公開鍵

KS_i ：第 i 課の課長の秘密鍵

また、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）

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。

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

上記の式を用いて社員 11 のデータの書込みと課長 1 のデータ読取りを行い確定データができるまでの流れを記述する。

（１）データ書込

社員 11 は個人データ d_{11} を作成し、PGP で暗号化個人データ d^*_{11} を作成して「暫定データ」に書込む。

$$d^*_{11} = PGP_{K_{ss}K_{pp}}(d_{11})$$
$$K_{ss} = HS_{11}$$
$$K_{pp} = KP_1$$

ここで社員 11 は「暫定データ」を読取り、自分のパソコンにあるデータを比較し、書き換え（改ざん）がないことを確認できる。

（２）データ読取り

課長１は「暫定データ」から暗号化個人データ d^*_{11} を PGP で復号化し、個人データ d_{11} を得る。

$$d_{11} = PGP^{-1}_{K_{ss}K_{pp}}(d^*_{11})$$
$$K_{ss} = KS_1$$
$$K_{pp} = HP_{11}$$

（３）データの確定

データの確定は暗号化個人データ d^*_{11} を課長１が PGP で暗号化し、d^{**}_{11} を作成して「確定データ」に書込む。

$$d^{**}_{11} = PGP_{K_{ss}K_{pp}}(d^*_{11})$$
$$K_{ss} = KS_1$$
$$K_{pp} = HP_{11}$$

データの確定後において、社員 11 はデータの書き換えを行うことはできないが、PGP の復号化で暗号化個人データ d^*_{11} を得ることはできるので、自分のパソコンに格納されてある d^*_{11} と比較して書き換えがないことを確認することができる。

$$d^*_{11} = PGP^{-1}_{K_{ss}K_{pp}}(d^{**}_{11})$$
$$K_{ss} = HS_{11}$$
$$K_{pp} = KP_1$$

課長 1 は同様に他の第１課の社員のデータの読取りやデータの確定が可能である。

課長のデータ書込むと部長のデータ読取りやデータの確定は前述した方法と同様に行うが、課長が書込むときには、課長は復号化した個人データに自分のデータを加え、それを PGP で暗号化し、課内データと部内データベースの「暫定データ」に書込む。従って、部長は社員の公

開鍵は知らなくても社員のデータを見ることがでる。この構築手法では公開鍵が必要になる相手は自分の上下の階層の人で、階層が深くなっても鍵は多くならない。

課内データベースの概略を図２に示し、書込み、読取り、確定、確認の詳細は図３に示す。

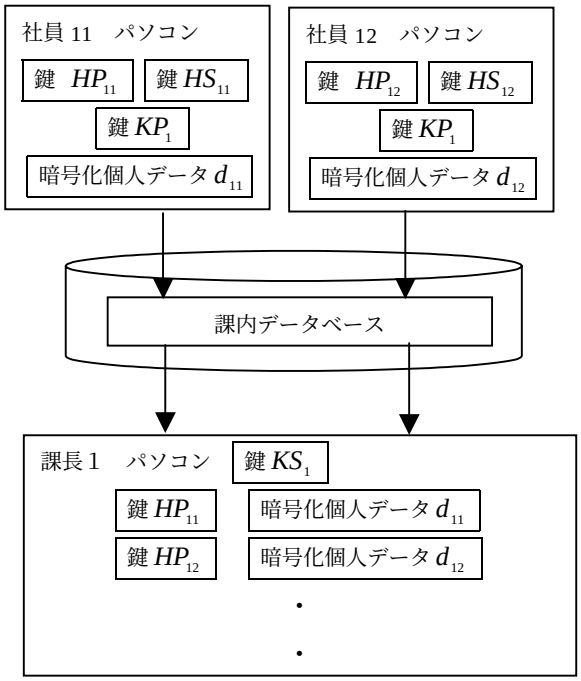

図 2　課内データベース

本稿で提案する階層化データベース構築では、公開鍵が知られても送付先の秘密鍵がなければ復号できないが、より安全なシステム構築のために公開鍵は直属の上司と部下のみに公開する。

４．今後の課題

今後の研究の計画としては、まず実際に PGP を使用してみる。次に PGP のソースの解析を行い、PGP の機能を最低限持ったソフトを作成する。その後、作成したソフトを用いて階層化セキュアデータベースを構築し、性能評価を行う。

５．まとめ

本稿では、階層化データベースを作成する際にアクセス制御を行うだけではなく、PGP という暗号化プログラムを用いて、ユーザ認証、データ保護、データ確定を行い、セキュリティの高い階層化データベースの構築手法の提案を行った。

今後はこの構築手法によりプロトタイプシステムの構築を行い、性能に対する評価を行う予定である。

参考文献

[1] 山口 英, 鈴木 裕信 編, 「情報セキュリティ」, 共立出版(2001).

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

[3] 清本 晋作他, 「暗号化 DB 構築におけるデータ暗号化手法の検討」,FIT(情報科学フォーラム)2003,pp587-588.

[4] 藤川 真樹他,「追記が付される文書の電子化とその長期的保存のための一考察」, 情報処理学会論文誌,Vol.42,No.11, pp2789-2799 (2001).

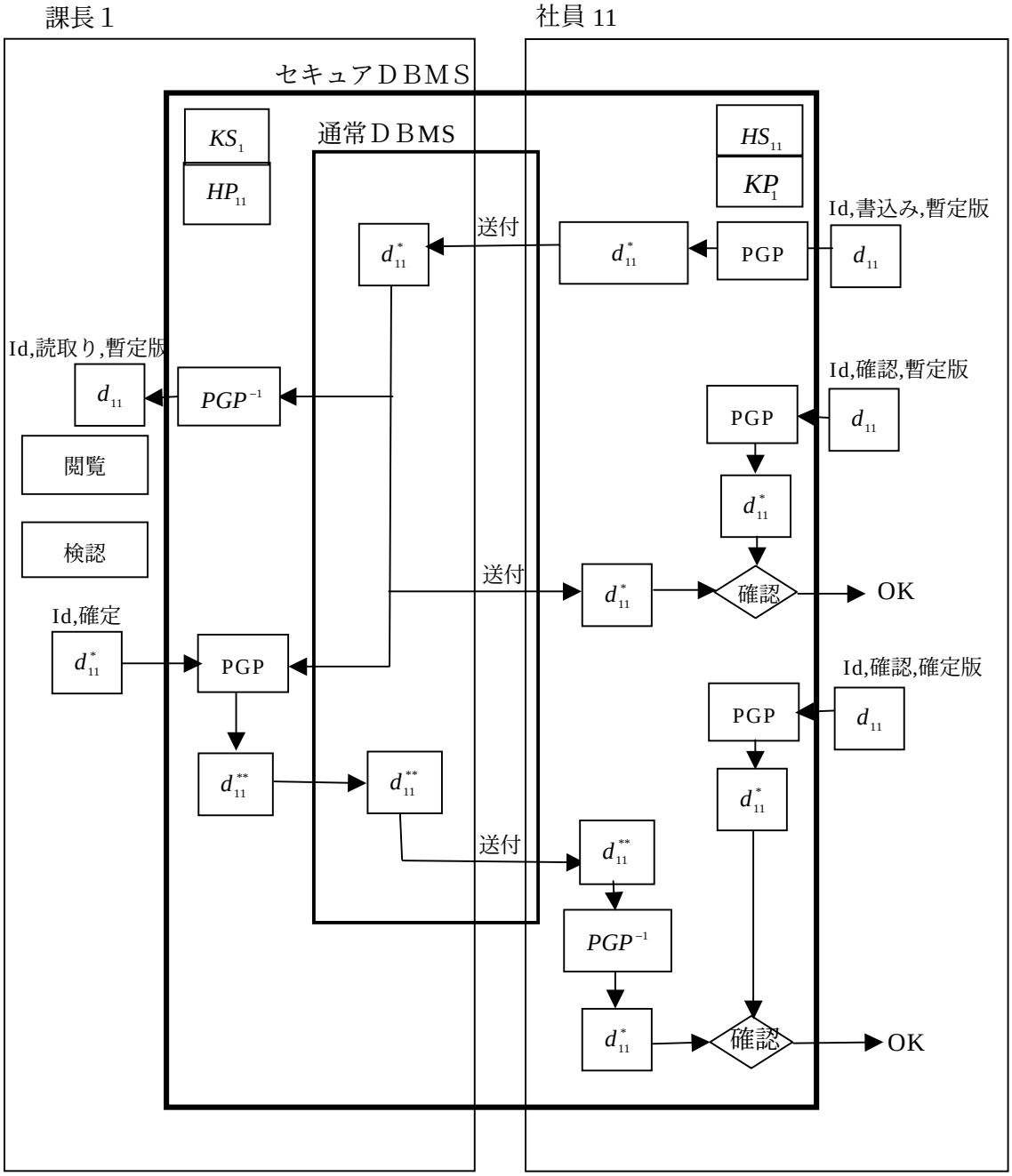

図３．社員 11 と課長１のデータ書込み、読取り、確定の詳細図（Id は社員の識別子）