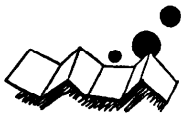
解　説



データベースのセキュリティ†

白石高義†† 中村史朗†† 佐藤和洋††

1. はじめに

コンピュータ・システムの規模の増大，ニーズの多様化に伴い，情報のデータベース化が進行している．

これらの情報には，

（a） 企業の経営計画情報

（b） 設計業務における設計データ・資料

（c） 大学，公共機関における，プライバシ情報や統計，計画情報．

など，データの保護が重大な課題となるものがある．このため，データベースを取りまく環境，管理，制御機密に関し，アクセス権，暗号方式を中心として，データベースのセキュリティ技術について解説する．まず，広くデータベースの保全という立場から，データベースへのアクセス，データ使用の制御，監視をする，データベース管理システム（以下 DBMS と略す）に要求される機能を列挙する．

（1） セキュリティ：不当なデータベースの濫用を防止する機能．

（2） 同時制御 (Concurrency Control)：同時に複数のユーザがデータベースをアクセスしようとした時に，データベース中のデータあるいは検索結果に矛盾が発生しないように制御する機能．

（3） 完全性制約 (Integrity Constraint)：データベース中に格納されるデータに対し，意味的に不当なものを排除する機能．例えば，数値しか許されない項目に対し文字が入ってきたり，“月”の項に対し「13月」など1～12以外の値が入力されたとき，それらを検知し排除する機能である．

（4） リカバリ：データベースが物理的あるいは論理的に破壊された場合，できるだけ最新の正しい状態に回復する機能である．

† Database Security by Takayoshi SHIRAISHI, Fumio NAKAMURA and Kazuhiro SATOO (Systems Development Laboratory, Hitachi, Ltd.).

†† (株)日立製作所システム開発研究所

（2）～（4）は，まとめて，インテグリティと呼ぶこともある．ここでは，（1）のセキュリティについて解説する．

データベースのセキュリティをさらに細分すると，

（1） アクセス制御：立体が対象に対して持っているアクセス権限を規定する機能と，その規定に基づきアクセス要求に対する制御を行う（**図-1**(a)）．

（2） 情報フロー制御：アクセス制御が1組の主体と対象との間の関係を規定，制御するに対し，情報フロー制御では複数の主体と対象の組合せにより情報が不当に洩れ流れる可能性をチェックする（**図-1**(b)）．

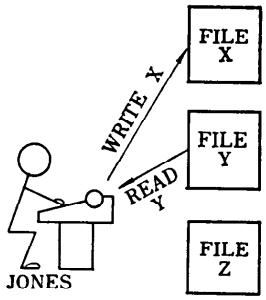
（3） 推論制御：これは特に統計データベースのように，個別レベルで識別できない情報群に対する問合せ結果と，別に得た個人の特徴情報とをマッチングさせることにより，特定個人の秘密情報を推論できることがあるが，これを防止する（**図-1**(c)）．

（4） 暗号制御：情報システム内，外で，直接物理的にファイルを読んだ場合でも，その内容がわからないようにするものである（**図-1**(d)）．

なお，情報に機密度がつけられ，より機密度の高いファイルから，低いファイルへ情報が流出することを防ぐ手段が情報フロー制御である．しかし，従来の DBMS におけるデータベース・セキュリティの基本的な考えは，データベースを構成することが主眼であり，ファイル間の情報の流れについては，一般に DBMS の範囲を越えている．これらのことより本稿では，アクセス制御，推論制御，暗号制御について，以下解説を加える．

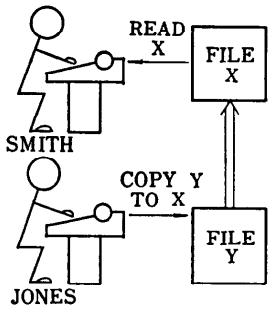
2. データベースのアクセス制御

データベースのセキュリティは，データベースに対する種々の不当なアクセス及びアクセスされたデータの不当な使用を防止することである．このために，DBMS には，データベースへのアクセス及びアクセスされたデータの使用を制御し，監視する機能が存在する．これがセキュリティ管理機能である．セキュリ



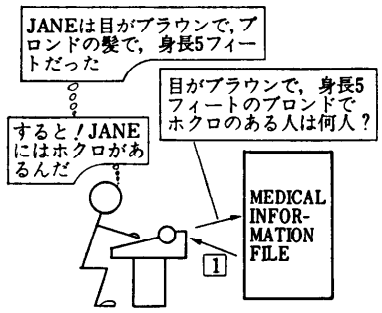
(a)

(a)アクセス：JONES はファイルYを読出し，ファイルXを書き込むことが許されているが，ファイルZへはアクセスできない．



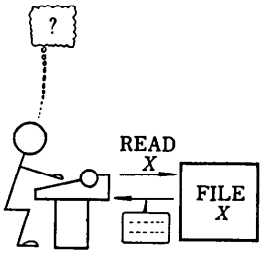
(b)

(b)フロー：SMITH はファイルYのアクセスが許されていないので JONES にコピーを作るよう頼む．フロー制御がこれを防ぐ．



(c)

(c)推論：質問者は，統計的計数情報から機密情報を導出するために，既知の知識を利用する．推論制御がこれを防ぐ．



(d)

(d)暗号：JONES は不正によりファイルXのコピーをとるが，暗号化されているので，内容がわからない．
注）参考文献14)より引用

図-1 データベースのセキュリティ

ティ管理者が複数か否かに従った制御方式の分類として分散制御方式と集中制御方式がある．本章では，このDBMS機能としてのいわゆる，内部セキュリティ[14]におけるアクセス制御に関し下記事項について主に述べる．

- ユーザ識別及び認証
- アクセス制御の基本モデル
- 既存 DBMS の実現形態

2.1 ユーザ識別及び認証

データベースアクセスにおける第1レベルでの制御及び監視機能は，ユーザ識別 (identification) 及び認証 (authentication) である．

(1) ユーザ識別 (user identification)

通常，計算機システムを利用するユーザには，当該ユーザを一意に識別するためのユーザ識別番号（一般に，ユーザ ID と言われる）が与えられ，システムを利用する時に入力しなければならない．このユーザ識別番号は，システム内でユーザ登録簿 (user profile あるいは user catalog ともいわれる) として管理されている．したがって，システムは，ユーザ識別番号の入力時には，このユーザ登録簿を参照して，入力されたユーザ識別番号が既登録か否かのチェックを行い，未登録であることが判明した場合には当該ユーザによるシステム利用を拒否する．これをユーザ識別プロセス (user identification process) という．また，システム利用を許可されたユーザのユーザ識別番号は，データベースアクセスの証跡あるいはシステムアカウンティング，等を把握するためにも使用される．

(2) ユーザ認証 (user authentication)

入力されたユーザ識別番号がユーザ登録簿に既登録の場合，当該ユーザ識別番号を入力したユーザが真にユーザ自身であるか否かを確認するために，当該ユーザしか知らない情報の入力をユーザに要求する．この情報が通常パスワード (password) といわれるものであり，前述のユーザ登録簿あるいはデータベースアクセス制御表などに管理されている．このパスワード入力による妥当性チェックのことをユーザ認証プロセス(user authentication process) という．また，パスワードの設定は，ユーザまかせがほとんどであるが，システムで設定することも可能である．さらに，ユーザ認証は手続きを利用しても実現することができる．この例を図-2 に示す[4]．Hoffman に他の多くの例が述べられている[6]．

パスワードによるユーザ認証を十分に行うためには，パスワードの不正入力への対策が必要で，データベースに対する不当アクセスを監視するという点からも，1) 各ユーザ ID ごとに，パスワード不正入力に対する履歴を取得し，2) 不正入力回数がある回数行われた場合には当該ユーザ ID の使用を禁止すると共に，システム管理者に報告する，などの方法が考えられる．

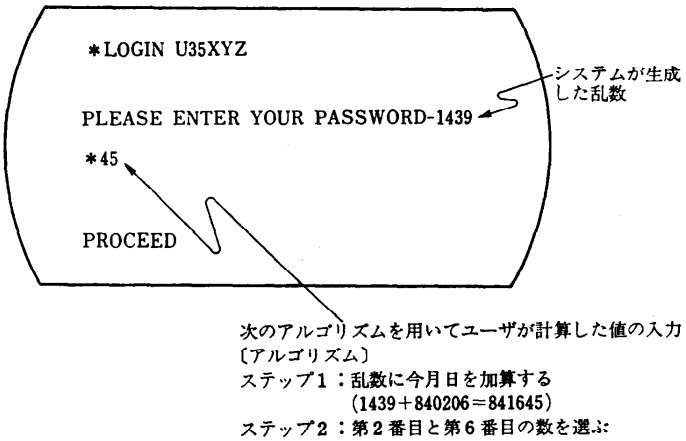


図-2　ユーザ認証手続きの例[4]

S \ O	O_1	…	O_i	…
S_1	T_{11}	…	T_{1i}	…
⋮	⋮	⋮	⋮	⋮
*S_j	T_{j1}	…	T_{ji}	…
⋮	⋮	⋮	⋮	⋮

* S_j のアクセス規則を表わす.

図-3　アクセスマトリックス表現

2.2 アクセス制御の基本モデル

データベースのアクセス制御モデルは，OS におけるリソース保護の理論として提案された Lampson[7),8)] らのモデルによるところが大である．彼らのモデルの基本は，アクセス規則であり，これは主体 (Subject) が対象 (Object) に対して行い得るアクセスタイプを指定するものである．図-3 に示すように，アクセス規則の集合はアクセスマトリックスとして表現でき，そのエントリなどはアクセスタイプのリストを含み，対象 O_i に対する主体 S_j のもつアクセス権限を表わすものとして考えられる．

データベースへの上記議論の適用の前に，まず OS におけるセキュリティとの相違点について示し，次にアクセス制御モデルについて述べる．

(1)　OS セキュリティとの相違点[1),5)].

次のような相違点が考えられる：

- データベースには保護すべき対象が多い．
- データ寿命がデータベースの方が長い．
- データベースセキュリティは，ファイル，レコード，フィールド，といった種々の異なるレベルの保護単位 (Granularity) に関係している．
- データベースの複雑な論理構造も保護対象となり，これが同一の物理的対象に写像されている．
- 内部，概念及び外部スキーマといった異なるアーキテクチャレベルでのセキュリティ要求がある．
- データベースセキュリティはデータの物理的特徴ではなくその意味に関係している．

以上のような相違点を考慮して，次のようなデータベースアクセス制御モデルが Fernandez[1),3),5)] らにより議論されている．

(2)　アクセスマトリックスモデル

前述のようにアクセスマトリックスモデルでは，セキュリティ保護対象の集合 O (要素を O_i とする)，保護対象利用者(物)の集合 S (要素を S_j とする) 及びアクセスタイプの集合 T (要素を T_{ji} とする) を用いて，アクセス規則を表現する．例えば，リレーショナル DBMS においては，i) O として，リレーション，アトリビュートなどで，ii) S として，ユーザ，プログラムなどで，iii) T として，SELECT, UPDATE, INSERT, DELETE 権限などを用いてアクセス規則が表現される．この一例を図-4 に示す．

しかしながら，上記表現だけでは前述したようなデータベースの論理構造，データの意味などに関連したセキュリティは実現できない．そこで，保護対象をより意味的に指定可能とするために，アクセス規則にアクセス対象を制限する述語 (predicate) を含むように上記モデルが拡張される．すなわち，アクセス規則は (S, O, T, P) なる4つ組で表現され，当該 S のアクセス T が可能な対象は，述語 P を満足する O の集合として表わされる．このようにして表現されたア

S \ O	EMP-NAME	PERS-NO	ADDRESS	SALARY
PERSONNEL-MANAGER	ALL	ALL	ALL	ALL
K. SATO, Jr.	SELECT	SELECT	SELECT	NONE
⋮	⋮	⋮	⋮	⋮

図-4　データベースアクセスマトリックスの例

S	O	T	P
F. NAKAMURA	EMPLOYEE	SELECT	SALARY≦30000
⋮	⋮	⋮	⋮

図-5 アクセス規則の例

クセス規則の例を図-5 に示す.

基本的なアクセス制御モデルは上記のようなものであるが，さらに，アクセス権限の認可/取消，保護対象の保護対象利用者(物)間でのフロー，等を考慮した場合には本モデルとを拡張する必要がある[1),5)].

(3) アクセス制御ポリシの種類[1),3),5)]

アクセス制御ポリシには，大きく分けて次の2つがある.

(i) need-to-know policy：最小権限ポリシとも呼ばれ，処理に要する必要最小限の権限のみを付与する方法である.

(ii) maximized sharing policy：データベース情報の最大限の利用を提供する方法である．但し，ある種の制約は存在する.

本章で述べてきた方法は上述の(i)に入るものである．この最小権限ポリシにおけるアクセス制御ポリシにはある対象の値に独立した制御を行う方式 (content-independent control)，ある対象の値に依存した制御を行う方式 (content-dependent control)，複数の対象の組合せ値に依存した制御を行う方式 (context-dependent control)，などがある．さらに，上記制御方式に関連させ，時間因子を加味したものとして，有効時間制約を利用した制御方式 (time-dependent control)，ある過去の時点でのある対象値に依存した制御方式 (history-dependent control)，などがある．図-6 に，アクセス権の主体間認可を許す環境でのアクセス制御 (discretionary access control) と許さない環境でのアクセス制御 (nondiscretionary access control) を考慮した need-to-know ポリシ体系を示す (実際のアクセス制御は，各ポリシの組合せにより実現される).

2.3 既存 DBMS における実現形態

上述のようにデータベースアクセス制御に関して種種の検討が行われており，実システムへの適用も実施されている．しかし，その実現の程度は各システムにおいて様々である．表-1 に，関係型，階層型，及び網型の主な DBMS である下記システム，

- SQL/DS[12),13)]：関係型
- IMS[9),10)]：階層型
- CODASYL タイプ[9),11)]：網型

における実現形態の概要を示す．本表の詳細は省略するが，特徴的な点についていくつか説明する.

DBMS におけるセキュリティ管理の特徴は，保護対象 (あるいは保護単位 (granularity))，権限タイプの豊富さに加えて，保護対象をデータの意味内容を考慮して自在に設定でき，それに対するアクセス制御ができることである．特に，関係型 DBMS においては，内容/文脈に依存した形でビュー定義が可能となっており，きめの細いアクセス制御を実現している．例えば，SQL/DS においては，次のようにビュー定義が行われる[9),12),13)].

CREATE VIEW LONDON-SUPPLIERS **AS**
SELECT S#, SNAME, STATUS
FROM *S*
WHERE CITY="LONDON"

(供給者テーブル *S* から，供給者が“ロンドン”にいる供給者の供給者番号，供給者名，ステータス情報からなるタプル集合としてのビュー・テーブル LONDON-SUPPLIERS の定義)

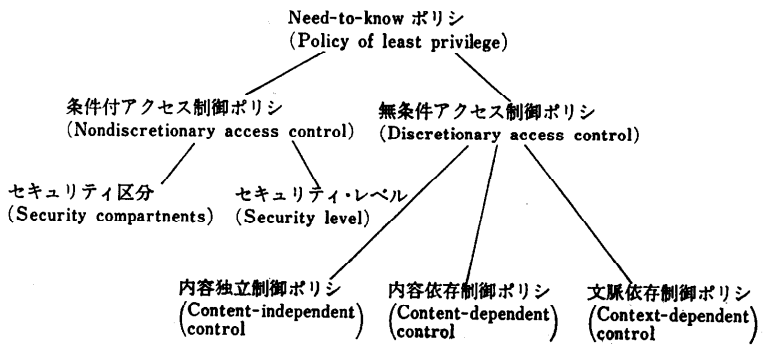


図-6 Need-to-know ポリシ体系

表-1 主な DBMS における実現形態

項目＼システム名	SQL/DS	IMS	CODASYL タイプ
1 セキュリティ管理方式	・分散制御方式 ・データディクショナリに権限管理テーブル保持	・集中制御方式 ・PSB ライブラリ/ACB ライブラリ ・サインオンライブラリ DB (ADF), etc.	・集中制御方式 ・DDL (スキーマ, サブスキーマ)
2 ユーザ認証方式	・パスワード	・パスワード (DBA 付与)	・パスワード
3 アクセス制御方式	◎内容/文脈依存制御 (但し, 履歴, 時間依存はなし) ・view 機構 (ビュー・テーブル) ・認可 (Grant)/取消 (Revoke) 機構	◎内容独立制御 ・view 機構 (PSB-PCB) ・PROCOPT 句	◎内容独立制御 ・view 機構 (サブスキーマ) ・lock & key procedure
3.1 権限付与者 (A)	データベース管理者 (以下 DBA と略), テーブル作成者, 認可オプション所有者	DBA	DBA
3.2 権限保有者 (S)	ユーザ (DBA 含), プログラム	DBA, プログラム (トランザクション) ターミナル, etc.	DBA, ユーザ, プログラム, etc.
3.3 保護対象 (O)	テーブル, ロー, カラム, プログラム, etc.	セグメントタイプ, レコード, フィールド, ターミナル, プログラム (トランザクション) etc.	スキーマ, サブスキーマ, 記憶スキーマ, レコードタイプ, セットタイプ, データ項目, etc.
3.4 権限タイプ (T)	SELECT, UPDATE, INSERT, DELETE, EXPAND, INDEX, DBA, RUN, etc.	INSERT, DELETE, REPLACE, etc.	DISPLAY, GET, COPY, STORE, MODIFY, ERASE, FIND, ALTER, etc.
3.5 アクセス制御述語記述法 (P)	・CREATE VIEW～AS 問合せブロック ・GRANT 権限 TO ユーザ WITH GRANT OPTION ・REVOKE 権限 FROM ユーザ	・IMS 論理 DB レコード定義 ・SECURITY 文	・DDL, DSDL, サブスキーマ記述 } における ACCESS 制御句
3.6 アクセス規則チェック時	コンパイル時, 実行時	実行時	(コンパイル時/実行時)

また, SQL/DS では, アクセス権限の認可 (Grant)/取消 (Revoke) 及び認可権の認可 (認可オプション) 等新しい機能も提供しており, 高度でかつ複雑なアクセス制御が必要となっている.

以上, データベースの内部セキュリティとしてのアクセス制御について概説した.

3. 推論制御

2章で述べたデータベース・アクセス制御は, データベース中の全データのうち, アクセスできるデータの集合とアクセス権の種類 (検索, 更新など) とを規定・制御する. 与えられたアクセス権限の範囲内であれば, 直接個々のデータ値を検索・更新したり, 合計値を得るなどの統計操作を行ったりすることが許される.

これに対し推論制御[14] (inference control) では, 許された一連のデータベースへの問合せから, 本来見てはならないデータを導出するのを防ぐことを目的としている. このような推論制御が特に問題になるのは, 統計データベースである. 統計データベースというのは, 例えば国勢調査データのように, 個人のプライバシ情報を含んでいるため直接個々のデータ値を見ることは許されず, ある条件を満たす人数や平均年令を求めるといった統計的な問合せのみが許されているデータベースである.

3.1 推論の例

一連の統計的な問合せのみを用いて, 特定個人の情報を導き出せることがある. このような例を, 表-2 のデータベースを用いて以下に示す.

Dodd が女の CS (計算機学科) の教授であることを知っている質問者が, 次の2つの問合せを発行する.

COUNT(F·CS·Prof) =1.

COUNT(F·CS·Prof·$15KSal)=1.

表-2 例題データベース

No.	Unique identifier	Categories			Data	
		Sex	Dept.	Position	Salary ($K)	Political contribution ($)
1	Adams	*M*	*CS*	*Prof*	20	50
2	Baker	*M*	*Math*	*Prof*	15	100
3	Cook	*F*	*Math*	*Prof*	25	200
4	Dodd	*F*	*CS*	*Prof*	15	50
5	Engel	*M*	*Stat*	*Prof*	18	0
6	Flynn	*F*	*Stat*	*Prof*	22	150
7	Grady	*M*	*CS*	*Adm*	10	20
8	Hayes	*M*	*Math*	*Prof*	18	500
9	Irons	*F*	*CS*	*Stu*	3	10
10	Jones	*M*	*Stat*	*Adm*	20	15
11	Knapp	*F*	*Math*	*Prof*	25	100
12	Lord	*M*	*CS*	*Stu*	3	0

注) 参考文献 15) より引用

これにより，Dodd の給料が $15 K であることが判明してしまう[15]．

したがって，問合せ条件を満足するレコード数（これをキュアリセットサイズという）の上限と下限（これを k とする）を設けなければならない．

3.2 トラッカ

しかしながら，許されるキュアリセットサイズが $[k, n-k]$，$1<k\leq n/2$ および n はデータベース中のレコード数，の範囲にある場合でも，個人情報を推論可能であることを Schlörer[16] は示した．質問者は，ある個人 I が条件 C によりユニークに識別されることを知っており，更に a という特徴を有しているかどうか知りたいとする．最小キュアリセットサイズが k であるため，直接条件 $C\cdot a$ で問合せることができない．しかしながら，もし条件 C が $A\cdot B$ の形に分解でき，かつ

$$k\leq \mathrm{COUNT}(A\cdot\bar{B})\leq \mathrm{COUNT}(A)\leq n-k$$

となるように A と B を選べるならば，回答可能な一連の問合せから I についての情報を推論できる．例えば，条件 C を満たすのが I だけであることを確かめるには，次式を用い右辺の 2 個の回答可能な問合せから計算できる（ここで $T=A\cdot\bar{B}$ である）．

$$\mathrm{COUNT}(C)=\mathrm{COUNT}(A)-\mathrm{COUNT}(T)$$

また，I が a という特徴を有しているかどうかは，次の式の右辺の問合せから計算できる．

$$\mathrm{COUNT}(C\cdot a)=\mathrm{COUNT}(T+A\cdot a)-\mathrm{COUNT}(T)$$

T は I についての個人情報を推論する手助けとなるので，トラッカ（tracker）と呼ばれる．

3.1 節の問合せ例で $k=3$ とすると，直接 $F\cdot$CS$\cdot$Prof の条件で問合せることはできない．そこで，これを $F\cdot$Prof と CS とに分け，$T=F\cdot\mathrm{Prof}\cdot\overline{\mathrm{CS}}$ とすると，

$$\mathrm{COUNT}(F\cdot\mathrm{Prof})=4.$$

$$\mathrm{COUNT}(F\cdot\mathrm{Prof}\cdot\overline{\mathrm{CS}})=3.$$

となりいずれも回答可能である．両者の差から，COUNT($F\cdot$CS$\cdot$Prof) が 1 であることが計算できる．同様に COUNT($F\cdot$CS$\cdot$Prof$\cdot$\$15 KSal) も計算可能である．

3.3 トラッカの汎用化

上述の議論では，質問者が特定個人の識別のための情報を基にトラッカを作り上げた．Denning[15]は，この制約をなくし任意の回答不可能な条件 C に関する問合せを推論できるような汎用のトラッカを提案した．そのようなトラッカ T とは，次の不等式を満たす任意の条件式である．

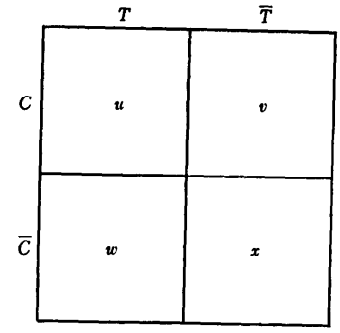
$$2k\leq \mathrm{COUNT}(T)\leq n-2k.$$

したがって，汎用のトラッカを用いることができるのは，キュアリセットサイズの最小値 k が $n/4$ 以下の時だけである．$\mathrm{COUNT}(c)<k$ なる回答不可能な条件 C に関する問合せ $q(C)$ (例えば COUNT(C), SUM(C) など) は，次式の右辺の一連の回答可能な問合せから計算できる（図-7 のベン図参照）．

$$Q=q(T)+q(\overline{T})$$

$$q(C)=q(C+T)+q(C+\overline{T})-Q$$

以上から明らかなように，統計データベース中の原



$Q=q(T)+q(\overline{T})=(u+w)+(v+x)$
$=(u+v)+(w+x)$
$=q(C)+q(\overline{C})$
$q(C+T)+q(C+\overline{T})=(u+v+w)+(u+v+x)$
$=(u+v)+(u+v+w+x)$
$=q(C)+Q$

注) 参考文献15) より引用

図-7 汎用トラッカによる推論のベン図

データが個々人の情報を保持している限り，特定情報を推論することを防ぐのは難しい．この対処方法としては，データベース分割やエラー混入などもあるが不都合も多く，現実的な方法としてはもし国勢調査のように母数が非常に大きいものであれば，そのすべてを原データとして用いるのではなく，ランダムにサンプリングしたものを用いたり，問合せ履歴を監視して異常な問合せパターンを検出したりする方法が効果的である[14]．

4. データベースの暗号方式

暗号技術は，伝文内容の機密保護のために，古くより，使用され，情報の伝達技術とともに進展してきた．

データベースに格納された情報を保護するために，暗号技術を利用しようとする動きは，従来よりあるがまだ，実用されているのは，まれのようである．しかし，媒体自体の盗難などの危険に対応するには暗号化が重要であるという認識である．

暗号の目的は，

- 情報を伝えたい相手にのみに伝達し，他には秘密にする．
- 情報を伝えたい相手に一番先に伝え，他には出来るだけ知られないようにする．
- 受け取った相手が，この情報による行動を行う場合，この行動に必要な時間を確保する．データベースの場合，保管期間のデータの保護を行う．

等である．

暗号系モデル上，データベース系を伝送系でモデル化すると，同報通信系に近いものになる．すなわち，長時間にわたって，多数の相手に，情報を送りつづけるものである．

したがって，従来の1対1伝送系暗号よりは複雑で困難な暗号システムである．しかし，暗号アルゴリズム上は，従来の暗号方式の適用が可能であるから，ここでは，一般の暗号方式を解説する．

4.1 暗号アルゴリズム

暗号アルゴリズムは，古くシーザの使用した暗号から最近話題になっている，DES（米国商務省による標準暗号システム）[18]，暗号化鍵と復号化鍵が異なる公開鍵暗号方式（または，非対称暗号方式）など多くの方式がある[3),20)]．

旧来からの暗号方式は，大別すると，換字方式と，転置方式になる．換字方式は，AとBにコード変換するようなものであり，転置方式は，文章での，位置関係を変える方法，例えば，カードをシャフルするようなイメージである．最近話題の DES は，この2方式を組合せたものである．

これらのアルゴリズムを整理し，和，積，冪の演算アルゴリズムに結び付けて検討を試みる．いま，平文を X，暗号を Y，鍵を K として，

ⓐ 和アルゴリズム

$Y=X+K \pmod m$
$X=Y+K' \pmod m$
$K+K'=0 \pmod m$

ここに m はコード群の因子数（文字数）である．

ⓑ 積アルゴリズム

$Y=X+K \pmod m$
$X=Y\times K' \pmod m$
$K\times K'=1 \pmod m$

ⓒ 冪アルゴリズム

$Y=X^K \pmod m$
$X=Y^{K'} \pmod m$
$K\times K'=1 \pmod{\lambda(m)}$

ここに $\lambda(m)$ は[21]以下のように定義した函数である．

$\lambda(1)=1,$
$\lambda(2)=1,\ \lambda(2^2)=2,$
$\lambda(2^r)=2^{r-2}$

素数 p のとき，

$\lambda(p)=p-1,\ \lambda(p^r)=(p-1)\cdot p^{r-1}$

素数 p,q のとき

$\lambda(p^r \cdot q^t)=\mathrm{LCM}[\lambda(p^r), \lambda(q^t)]$

LCM[a, b]は，a, b の最小公倍数を示す．

以上のアルゴリズムの複合は，多項式となる．

④ 多項式アルゴリズム

例えば

$$Y=K_a \cdot X^{K_r}+K_b \cdot X^{K_s}+K_c X^{K_t}+K_d$$
$$=((X+K_1)^{K_s}+K_3)K_4 \quad (\mathrm{mod}\ m)$$
$$X=(Y \cdot K_4'+K_3')^{K_2'}+K_1' \quad (\mathrm{mod}\ m)$$
$$K_1+K_1'=0,\ K_3+K_3'=0 \quad (\mathrm{mod}\ m)$$
$$K_4 \cdot K_4'=1 \quad (\mathrm{mod}\ m)$$
$$K_2 \cdot K_2'=1 \quad (\mathrm{mod}\ \lambda(m))$$

である．

公開鍵暗号方式として有名な RSA 方式[19]は，冪アルゴリズムの一例である．なお，この方面の研究開発は急速に進められていて，新しいアルゴリズムが，つぎつぎに現れている[20),22)]．

4.2 暗号鍵管理

暗号システムで重要な問題は，暗号アルゴリズムに並んで，鍵管理方式である．すなわち，暗号化した暗文の復号のために必要な鍵の管理をどうするかである．伝送路においては，

a） あらかじめ，鍵表（コードブック）を配送しておいて，暗文の鍵指定（プロトコル）は，鍵記入位置を指定する，間接方式

b） 暗文に対応した鍵を送る，直接方式

がある．これと同様に，データベースにおいても，ファイル内容を暗号化したとき，復号鍵の保管位置を指定するものと，ファイルの一部に鍵を秘匿しておく方法とがある．後者の例として，IBM が DES を使用したものがある[23)]．

4.3 データベースへの暗号適用に対する問題

データベースにおける暗号方式について述べた．記憶媒体のコピーに対する脅威を考えると，暗号化に対する潜在的ニーズは高いと考えられる．しかし，現在の DBMS では，積極的に暗号化をしようとする動きがない．この原因の1つには，ソフトウェアによるオーバヘットが大きいことが考えられる．このように，データベースに暗号を適用するに多くの問題がある．特に，必要性の評価が低いこと，長期間のデータ保護の困難さ，が隘路となっている．

いま，比較的考えやすい，システムより切り離した，予備用記憶媒体のコピー防止対策に盗難防止策の他に暗号化を考える．

暗号化の時点と復号化の時点は記憶媒体を切り離す時に，暗号化を行い，装着時に復号するものとする．このことにより不幸にして盗難にあい，コピーされたとしても，解読が困難であれば暗号化の目的を達成する．このとき，暗号アルゴリズムは複雑で鍵を一つ一つすべて，テストすること以外に手段がないようにしたい．すなわち，暗号アルゴリズムは和アルゴリズムより，積アルゴリズム，さらに冪アルゴリズムが複雑であり，鍵の数では多項式アルゴリズムである．

これらの方策を適用するためには重要度，保償度，などの評価を含む最良手段の解明は今後の課題である．

5. むすび

セキュリティは DBMS 単独で考えられるものでなく，コンピュータ・システム全体で考えるべき点が多い．したがって，DBMS の機能開発と同時に，統合された，システム管理機構の開発が重要である．

データベースのセキュリティの現状は，ユーザ ID，パスワードによる認証，アクセス制御が主流であり，その他は，検討レベルと考えられる．

ここで，今後の動向を見ると，

（1） アクセス制御

ユーザ認証が重要であり，従来のパスワード方式以外に，声紋，指紋による認証方式などが考えられるがこれは，まだ実用化に至っていない．

（2） 情報フロー制御

本稿では，解説を行わなかったが，情報に機密度の違いがあり，ファイル間での情報の流れが重要であるシステムでは，これに対応した情報フロー制御手段の開発が必要となるであろう．

（3） 推論制御

本機能の開発はまだ研究的レベルと考えられる．今後，プライバシ問題に対処するために推論制御へのニーズが高まることと思われる．

（4） 暗号制御

記憶媒体のコピーに対する脅威を考えると，暗号化に対するニーズは高いと考えられる．暗号鍵管理を含め，これからの課題である．

その他，監査も重要な問題である．

参考文献

1) Fernandez, E. B., Summers, R. C. and Wood, C.: Database Security and Integrity, Addison-Wesley, Reading, Mass. (1981).

2) Date, C. J.: An Introduction to Database Systems, Vol. II, Addison-Wesley, Reading, Mass. pp. 143-180 (1983).
3) Denning, D. E. R.: Cryptography and Data Security, Addison-Wesley, Reading, Mass. (1982).
4) Welden, J. C.: Data Base Administration, Plenum Press, New York, pp. 145-157 (1981).
5) Wood, C., Fernandez, E. B. and Summers, R. C.: Database Security: Requirements, Policies, and Models, IBM Sys. J., Vol. 19, No. 2, pp. 229-252 (1980).
6) Hoffman, L. J.: Computers and Privacy: A Survey, ACM Comp. Survey., Vol. 1, No. 2 (June 1969).
7) Lampson, B. W.: Protection, Proceedings, 5th Annual Princeton Conference on Information Sciences and Systems, pp. 437-443 (1971), Reprinted in ACM Operating Systems Review, Vol. 8, No. 1, pp. 18-24 (Jan. 1974).
8) Graham, G. S. and Denning, P. J.: Protection-Principles and Practice, AFIPS Conference Proceedings, Vol. 40, pp. 417-429 (1972).
9) Date, C. J.: An Introduction to Database Systems, 3rd. ed. Addison-Wesley, Reading, Mass. (1981).
10) IBM Corporation: IMS/VS System/Application Design Guide (SH 20-9025-4).
11) Taylor, R. W. and Frank, R. L.: CODASYL Data Base Management Systems, ACM Computing Surveys 8, No. 1 (Mar. 1976).
12) IBM Corporation, SQL/DS Concepts and Facilities (GH 24-5013).
13) IBM Corporation, SQL/DS Application Programming (SH 24-5018).
14) Denning, D. E. and Denning, P. J.: Data Security, Computing Surveys, Vol. 11, No. 3 (Sept. 1979).
15) Denning, D. E. et al.: The Tracker: A Threat to Statistical Database Security, ACM TODS, Vol. 4, No. 1 (Mar. 1979).
16) Schlörer, J.: Identification and Retrieval of Personal Records from a Statistical Data Bank, Methods of Inform. in Medicine, Vol. 14, No. 1 (Jan. 1975).
17) データベース・システムに関する調査—データベースセキュリティ機能の調査, 日本電子工業振興協会 (Mar. 1983, 1984(予定)).
18) FIPS: Data Encryption Standard, FIPS Pub. 46 NBS (Jan. 1977).
19) Rtvest, R. L., Shamir, A. and Adleman, L.: On Digital Signatures and Public-Key Cryptosystems, IEEE International Symposium on Information Theory, p. 41 (Nov. 1977).
20) Beth, T. (editor): Cryptography, Lecture Notes in Computer Science, Vol. 149 (1982).
21) 白石：RSA 方式における周期性の考察, 信学技報 IT 83-9 (1983).
22) 松本, 今井：公開かぎ暗号系の新しいアルゴリズム, 信学技報 IT 82-24 (1982).
23) Ehrsam, W. F., Matyas, S. M., Meyer, C. H. and Tuchman, W. L.: A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard, IBM Systems Journal, Vol. 17, No. 2, pp. 106-125 (1978).

(昭和59年3月22日受付)