社会システムの構成要素としてのデータベースとそのためのセキュリティ

3W-10

猪野和之、河越正弘、山崎　章
(工業技術院　研究開発官室)

1．はじめに

現在、データベースを取り巻く環境として、相互運用技術の実用化（INE'88）・分散技術の開発の進歩により、大規模データベースが益々身近になってきた[1]。

例えば、電子出願、電子投票、公開情報データベース、各種の情報サービスなどの様々な応用形態を取って、個人レベルの国民生活の場に入って行こうとしている。

この場合、今までの会社内・工場内に閉じたデータベースと異なり、セキュリティが一層重要になって来る。

しかし、これまで、上記のような個人生活の場への応用が考えられて無かった上に、責任・負担の混乱（メーカ、管理者、ユーザ）が見られ[2]、現状のシステムでは、自己防衛的に、ユーザレベルでの暗号化程度が一部実施されているだけである。

そこで、データベースにおけるセキュリティについて整理し、今まで関係者のモラルの向上にしか期待できなかった部分の計算機化について考察したので報告する。

2．データベースのセキュリティには何が重要か？

データベースのセキュリティについては、暗号化、多重化、アクセス制御等の技術が、既に開発されているが、主としてシステム管理者の立場に立ったものが多かった。

しかし、データベースの利用者保護のためのＯＥＣＤ理事会勧告を始めとして、国内でも鋭意検討されている、プライバシー保護で代表される、ユーザの立場に立ったセキュリティを考える必要が強まってきた[3]。

現状では、これらは法制・権限分割・監査等の人的手段のみにに頼ろうとしているが、我々は、機械化による、人的な要素の排除が高信頼化、セキュリティの向上につながると考えて、技術的に実現すべき機能として、以下のものが重要であると考える。

1）データの収集制限：例えば、決済を目的とするキャッシュカードにおいて、ユーザが何時、何処で、何をしたか等の情報を暗号化し、目的外に収集・使用を防止する等のように、システムの本来の目的以外に、ユーザの利用に関するデータを収集・使用に対する防止技術[4]

2）データの紛失，
不当なアクセス・破壊・使用・修正・開示の防止

3）データの目的外使用の防止：
目的チェック、意図しない漏洩

4）システムが不正動作しない確認手段

3．どんなテーマが必要か？

1）データベースの正確・完全・最新性の確保

データの一貫性は，従来、更新手法にトランザクション処理を用いて、アプリケーション自身で複数のデータベース間の整合性をとっている。しかし、人手によらずにデータベースシステム自身の機能として，多くの雑多な意味的関連を持つデータベース間にわたる意味的整合性を，データベースのモジュール化，関連情報管理，無矛盾性のチェック技術などにより，複数のデータベースにわたる，最新性，正確性，完全性を保証する技術開発．

Physical Access Control：
ドアロック、ＩＤカード等の計算機内部での制御

Logical Access Control：
データベースのデータに対する
計算機内部での制御

- Syntactic Access Control：
暗号化、password 等
- Semantic Access Control：
権限分割等の組織上の措置

図１　アクセスコントロールの分類

2）不当ｱｸｾｽ・破壊・使用・修正・開示，目的外使用の防止

これらは，図１の広い意味のアクセスコントロールととらえられるものである．特に従来，組織上の措置しか考えられなかった Semantic Access Control に対して，データベースの運営規則（目的，用途，開示先，参照権などを記述したメタな規則）を独立したモジュールとして設定し，データベースに対する質問の，宛先・用途・目的・内容・根拠などに関して評価することにより不審利用をチェックし，偽りの申請では、データベース自身が使用を制限する機能の開発．

3）システムの正当動作の保証・確認

データベースシステムのセキュリティ部分について，デザインレベル及びプログラムレベルにおいて、システムに対するアクセス操作の整合性チェックやプログラムの階層的仕様からの動作保証により、システムが公表された通りのものであり、不正動作しないことの確認・保証する監査技術の開発．

4．おわりに

以上、実現が身近になった大規模データベースにおけるセキュリティのありかたについて、重要性が益々高まってきたユーザの立場にたって考察した。

また、本稿で報告したテーマについては、１９８５年度から実施している大型プロジェクト「電子計算機相互運用データベースシステム」の一環として、本年４月から研究を開始する予定である。

[参考文献]

1）山崎ほか：ＯＳＩの実用化迫る，工業技術,Vol.29, No.11,pp.13-28 (1988).
2）上園:情報ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ，電子情報通信学会誌, Vol.70,No.11,pp.1119-1126 (1987).
3）堀部:ﾌﾟﾗｲﾊﾞｼｰと高度情報化社会,岩波新書 (1988).
4）田中,内田,秋山:資金の流れが追跡不可能な電子送金法,信学技報 IN87-94 (1987).

Database System as a component of Social System and its Security
Kazuyuki INO, Masahiro KAWAGOE, Akira YAMAZAKI
National Research and Developement Program Office, Agency of Industrial Science and Technology