4R-3

分散型リレーショナル・データベース指向の図面管理システムM-DRAMA(3)
――セキュリティと運用――

谷内田 仁 , 古谷克二 , 出川 誠 , 渡邊澄江 , 肥後野恵史
株式会社 東芝 総合情報システム部

1. はじめに

図面管理を効率よく行なうM－DRAMA[*1)] は異機種間，ヘテロOS上での分散型のデータベース（以下、DBと呼ぶ）を利用したシステムである。本稿では本システムにおいて多くのユーザが利用するネットワーク環境及びDBにおいて重要な問題であるセキュリティに関して述べる。

2. セキュリティの概要

本システムで考慮したセキュリティの概要を以下に述べる。

(1) 対誤操作セキュリティ
ユーザの過失に対するセキュリティで、データをアクセスあるいは登録中にシステムをアボートさせてしまった場合などのデータ保護。

(2) 対破壊セキュリティ
データの内容を故意に破壊、あるいは消滅させることを許可しない。

(3) 対改ざんセキュリティ
データの内容を不当に変更することを許可しない。

(4) 対不正使用セキュリティ
システム及びデータの無断使用，不正コピー，転売を許可しない。

(5) プライバシー保護セキュリティ
個人や組織の機密データの不正入手，公開を許可しない。

3. セキュリティの実現

本システムは2．で述べたセキュリティを実現するために大部分を次に述べるアクセスセキュリティの技術を利用して実現している。

(1) 認 証

正確に使用可能なユーザであるかを確認するためのものであり、本人確認をユーザID，パスワードにて判断する。通信可能なホストを限定するために、RDBMS[*2)] と連結したDB通信ツールに相手を登録する。

(2) アクセス制御

データのアクセス資格があるか否かを制御し不正アクセスを防止する。管理DB内には以下に示す4種類の図面DB[1] の内容が管理されているが、それらの管理情報に関するアクセス権は次のとおりである。

・ユニバーサルDB（UDB）
JIS部品のDBである。全ユーザに読みこみを許可するが、登録や修正はユニバーサルDB管理者のみが実行できる。

・グローバルDB（GDB）
事業部標準部品のDBである。事業部に所属する全ユーザに読みこみを許可するが、登録や修正はグローバルDB管理者のみが実行できる。

・ローカルDB（LDB）
プロジェクトで使用作成した承認済の部品DBである。プロジェクトのメンバーには読みこみを許可するがその他には読みこみを許可しない。登録や、修正に関してはプロジェクト管理者のみが実行できる。

・インディビジュアルDB（IDB）
個人が現在作成している、あるいは未承認の部品DBである。個人以外に他のメンバには他端末からの読みこみ，登録，修正を許可しない。

以上を表1にまとめる。

*1) M－DRAMA (Mechanical－DRAfts MAnagement system)
*2) RDBMS (Relational Data Base Management System)

Distributed Relational Data Base Oriented Drafts Management System M-DRAMA(1) -Security and Operation-
Hitoshi YACHIDA , Katsuji FURUYA, Makoto DEGAWA , Sumie WATANABE, Shigefumi HIGONO
TOSHIBA Corp.

表1　アクセス資格とＤＢの関係

	一般ユーザ	事業部ユーザ	プロジェクト内ユーザ	設計担当者個人	*3) 特権者
ＵＤＢ	○	○	○	○	ＪＩＳ部品管理者
ＧＤＢ	×	○	○	○	グローバルＤＢ管理者
ＬＤＢ	×	×	○	○	プロジェクト管理者
ＩＤＢ	×	×	×	○	各担当者

*3) 登録・修正は特権者のみに与えられている。

これらのＤＢに関するアクセス資格の実現は以下のとおり二重の関門を用意し、実現している。

① 管理情報テーブルのアクセス権

ＤＢ中に、ＵＤＢ，ＧＤＢ，ＬＤＢ，ＩＤＢに対応するテーブルとアクセス可能なユーザＩＤを対応づけている。

② ＯＳによるファイル許可権

図面ＤＢ中のＵＤＢ，ＧＤＢ，ＬＤＢ，ＩＤＢには表1に示したアクセス資格のあるメンバーをグループとし、そのグループごとに許可権（読み込み許可）を与え、他のユーザには与えない。これにより本システム以外からの侵入をも防止する。

またＩＤＢのアクセスに関しては、ネットワーク中の他のユーザからのアクセスを禁止しているが、ＰＣがシングルタスクＯＳという制約により実現している。

アクセスセキュリティ技術以外で実現したセキュリティに、対誤操作セキュリティがある。これは、データ保護の考えからＲＤＢＭＳに存在するロールバック，コミットにより実現している。データを読み込んでいる途中やその後にシステムがアボートしてもＤＢ中のデータに影響を与えることはない。つまりユーザのデータ操作には問題はないが、特権者の行なうＤＢ中のデータ操作中にシステムアボートが生じた場合が問題である。ある仕事単位（特権者が認識できる作業単位）でコミットをかけているので、その途中でアボートした場合、システムが立上がった時には最終コミット時点まで戻されることを保障実現している。また、コミット前の入力データの確認をシステムより対話式で行なわせるのでその時点で特権者の入力ミスが発見されたときには登録させない、またはロールバックして最後にコミットした時点まで戻すことが出来る。

以上、セキュリティの種類とその実現方法を表2にまとめる。

表2　セキュリティの種類と実現方法

セキュリティの種類	実現方法
対誤操作	ロールバック，コミット
対破壊，対改ざん	認証，アクセス権
対不正使用，プライバシー保護	ファイル許可権

4．おわりに

本システムのセキュリティに関しての考え方と実現方法について述べた。本システムの構想では、異機種間，ヘテロＯＳ間，ヘテロＲＤＢＭＳ間，分散ＤＢを目標としている。このように本システムがサポートする範囲が広くなればなるほどセキュリティの重要性，実現の難しさが増してくる。今後、現状で実現しているセキュリティ以外に本システムの将来展開を考慮したセキュリティの検討を始める予定である。

5．参考文献

[1] 古谷　他：“分散型リレーショナル・データベース指向の図面管理システムM-DRAMA(1)－システムの基本構想－”，情報処理学会　第38回全国大会，1989

[2] “ネットワーク社会めざして”，コンピュータエージ社総合データ通信ネットワーク化構想懇談会編