6J-5 文書管理におけるセキュリティ実現の一手法

樋口 好隆　安田 英人　大山 茂春　冨樫 喜和
富士通株式会社

1. はじめに

大規模な企業では，ＯＡマシンとしてホストシステム（以降，ホストと呼ぶ）を導入し，複数部門にまたがる全社レベルのＯＡシステムの構築が一般化してきた．

この場合，ワークステーション（以降，ＷＳと呼ぶ）は文書の編集処理，ホストは文書管理機構という役割をになう．

本稿では，作成した文書管理機構の中で重要な位置を占める機密保護機能に対する実現の手法について紹介する．

2. 実現へのアプローチ

機密保護は，文書や格納庫にアクセスを許されていない利用者から，不当なアクセスを受けることを防ぐものである．機密保護に対する我々のアプローチを以下に示す．

1)　顧客要件のパターン化

顧客からホストの文書管理機構に対する機密保護機能の要件を調査し，主要なものを以下のようにパターン化した．

－　部門共有型

組織にマッピングした部門（部や課）単位に，文書を保管し参照はその部門内のメンバなら誰でも可能．

－　広報型

不特定多数の人に文書を参照させたい．文書の更新／削除は特定の管理者のみ可能．

－　コミニュケーション型

特定の人同志で情報を交換するため，そのメンバは誰でも文書の参照／更新／削除が可能．

－　メールボックス型

文書を作成した人は，格納庫に文書を登録する事はできるが，登録後はその文書の参照／更新／削除等の一切のアクセスを禁止される．

2)　アクセス制御モデルへのマッピング

機密保護の一般的なアクセス制御モデルに，パターン化で抽出した機能をマッピングした．その内容を図１に示す．

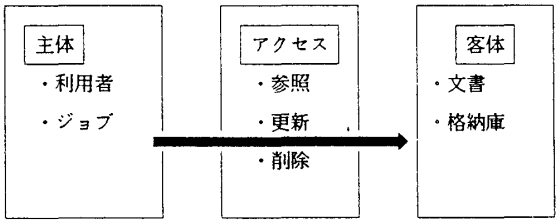

図１　アクセス制御モデルへのマッピング

客体　⇨　格納庫及び文書

主体　⇨　計算機利用者のユーザＩＤ／パスワードで識別

アクセス権　⇨　削除権，更新権，参照権

アクセス権の定義　⇨　客体に対してどの主体がどのようなアクセスをするかを定義する．

3)　実現時にあたっての考慮事項

実際の機能の実現時に考慮した事には以下のものがある．

－　アクセス検査の性能重視

－　運用容易性

－　2）でマッピングできないケースの実現方法

3. 実現機能と方式

1)　制御構造

ホスト上に図２に示すような文書／格納庫のアクセス制御機構を作成し，機密保護機能を実現した．

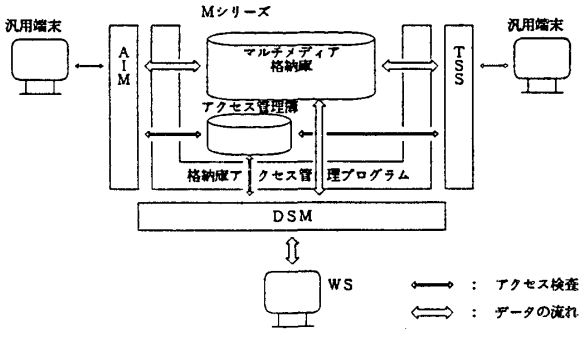

図2　マルチメディア格納庫の機密保護の制御構造

An example of Security for Document Management
Yoshitaka Higuchi
FUJITSU Ltd.

2） 格納庫の階層化

機密保護のためには，文書の格納庫を分ける方法が有効である．しかし，物理的に分けたのでは，管理が繁雑になってしまう．そこで，格納庫を図3に示すように論理的に階層構造にして，個々の格納庫の単位で保護を可能にした．

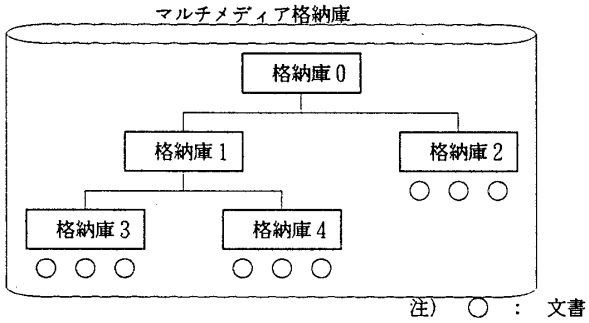

図3 マルチメディア格納庫の論理構造

3） アクセス権の設定

アクセス権の設定は，文書と格納庫の両方に行えるようにし，アクセス検査の性能及び運用容易性を考慮して，以下のような方法とした．

文書は，一般に作成，更新，削除等が頻繁に行われるため，特定の利用者にアクセス権を与える定義を行う方法をとらず，不特定の利用者に対して許可するか否かを文書自身が持つ方法を採用した．

格納庫は，文書に比べて作成，更新，削除の機会が少ないため，個々の格納庫ごとに特定の利用者へのアクセス権の定義を持つアクセスリスト方式を採用した．

4） アクセス制御

この格納庫に格納された文書をアクセスする場合，格納庫アクセス管理プログラムは以下の手順でアクセス検査を行う．

まず，格納庫のアクセス検査を行う．そこで，アクセスが許された場合，その下位にまた格納庫があればその格納庫のアクセス検査を行い，なければ次に文書のアクセス検査を行う．

従って，文書のアクセスを行うためのアクセス権検査は，格納庫と文書のアクセス権の組合せで検査される．

5） 利用者の一意な識別

利用者の識別は，個々の文書や格納庫をアクセスするごとに行うのではなく，ＷＳからホストを利用する一連の操作の集まりを一つの単位（これをセションと呼ぶ）として，そのセションを開設する時点で行うようにした．これにより，利用者の識別に要するオーバヘッドを少なくすることを可能にした．

6） 標準のアクセス制御で実現できないアクセス制御に対する考慮

メールボックス型のように今回，作成した機密保護のアクセス制御では実現できないものについては，センタ出口の組込みによりユーザカストマイズを可能にした．

4． 問題点

今回，作成した機密保護機能では，以下のような問題を残している．

1） システムにまたがる機密保護状態の引継ぎ

これは，文書が他のホストに移動された場合や，ＷＳへ取り出された場合に，文書の機密保護の状態が保障されないことである．これを実現するためには，ＷＳとホストで統一された機密保護機構の作成が必要となる．

2） 文書の機密の強度を管理した機密保護

今回実現した機密保護は，アクセス制御による機密保護である．そのため，保護の対象のすべての文書が一律の機密の強度を持つものとしてアクセスを制御されるのみである．しかし，現実の世界では，文書の内容に応じて保護の強度が要求される分野がある．

5． おわりに

計算機システムの大規模化とともに，機密保護はますます重要になりつつある．今回，我々が実現した機密保護機能は，アクセス制御機能の範囲であるが，国内の主要顧客要件を実現できたと考えている．

今後，より強度な機密保護が求められると予想されるため，フロー制御機能まで発展させる予定である．

6．参考文献

1） Landwehre, C. E. : Formal Models for Computer Security, Comput. Surv. Vol. 13, No 3

2） 大山，川口，冨樫：ＷＳ－メインフレーム連携におけるホスト文書格納庫の実現手法，情報処理学会第32回全国大会