1E－8　開放型文書通信体系におけるセキュリティ機能の位置づけ

中尾康二　田中俊昭　鈴木健二

国際電信電話株式会社　研究所

1. はじめに

テレマティクス通信サービスの統合化を目指して、筆者らはこれまでODA(開放型文書体系)、およびDTAM(文書転送および操作)をベースとした統合テレマティクス通信体系の検討を進めてきた[1]。本研究は、異なる文書体系を保有するシステム間の相互接続性の問題、すなわち開放型文書通信の実現としてITU-T(旧CCITT)およびISOにおいても取り上げられ、これらの国際標準化が進捗した。しかしながら、上記開放型文書通信におけるセキュリティ機能の検討は、十分になされておらず、ISOにおいてセキュリティ機能の要求条件の整理がなされたに止まっている。本稿では、開放型文書通信を実現する環境(ここでは開放型文書通信体系と呼ぶ)の観点から、セキュリティ機能の要求条件を整理するとともに、開放型文書通信体系におけるセキュリティ機能の位置づけについて述べる。

2. 開放型文書通信体系

開放型文書通信体系は図1で示すように、開放型文書処理、開放型通信処理、およびローカル文書処理(利用者プロセス)により構成されると考える。ここで開放型文書処理とは、異なる文書体系(ワープロ等)の間の橋渡しを行なう中間的な標準文書体系への相互変換を実行する処理で、標準文書体系としては、ODAやSGML (Standard Generalized Markup Language)等が挙げられる。また、開放型通信処理とは、ODA文書等を用いた文書通信を実現するOSI(開放型システム間相互接続)に基づく通信機能を提供するものである。さらに、ローカル文書処理は、各文書処理システム(ワープロ等)がそれぞれ保有する固有な文書処理を実現するものである。

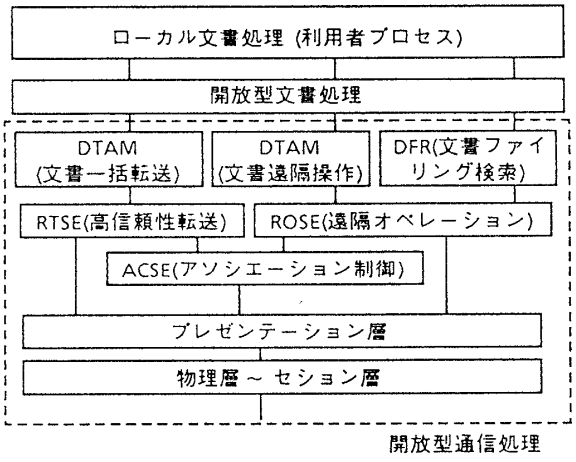

図1 開放型文書通信体系の構成

本体系では、①文書を一括的に相手システムに転送する機能(文書一括転送)、②遠隔システムに存在する文書内容を操作編集する機能(遠隔文書操作)、③遠隔システムから文書を読み出したり、そこへ書き込む機能(文書ファイリング検索)をサポートし、これらを実現するために、DTAM、DFR(文書ファイリング検索)、RTSE、ROSE、ACSEなどのOSI通信機能を使用する。なお、開放型文書処理、開放型通信処理、およびローカル文書処理の各処理モジュールの関係を明確にするために、具体的な処理フローを文書一括転送における送信側の処理を例にとり図2に示す。

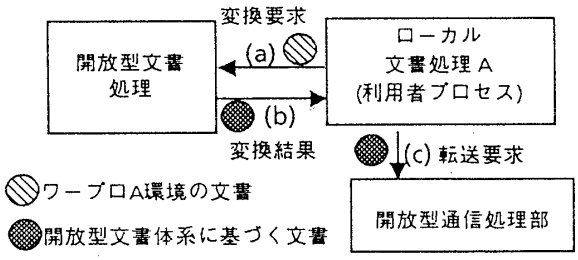

図2 文書一括転送における処理フロー(送信側)

3. セキュリティ要求条件

ISOにおいては、以下に示すような文書通信のためのセキュリティ機能に関する要求条件が検討されている。

①通信相手認証機能：通信開始時/通信途中において通信相手の正当性を確認する機能。

②通信文書の秘匿(暗号化)/改ざん検知機能：通信回線を流れる文書情報を秘匿したり、それに改ざんがなされたことを検知する機能。

③文書作成元証明機能：作成した文書に作成者の署名を付与する機能。署名情報は、通信終了後もローカルにどこででも検証が可能。

"Position of Security Functions for Open Document Communication Architecture"
Kouji NAKAO, Toshiaki TANAKA
and Kenji SUZUKI　KDD R & D Laboratories

④文書リソースアクセス管理機能：遠隔より文書サーバに蓄積される文書(又はその一部)のアクセスにおいて、読出し禁止や書込み禁止等のリソースのアクセス管理を行なう機能。
⑤受信否認不可機能：文書の受信者が、その受取りを拒否できない機能。

4. セキュリティ機能の分類

開放型文書通信体系におけるセキュリティ機能は、本体系の構成要素に対応して、(分類1)ローカル文書処理における個人(通信利用者)に依存したもの、(分類2)文書リソースに依存したもの、および(分類3)通信システムに依存したものに分類できる。従って、第3章で述べた①~⑤の要求条件を上記分類の観点より整理し直すことにより、本体系におけるセキュリティ機能の位置づけを明確にする。

①通信相手認証機能　：　利用者個人を認証する場合(分類1)と、通信システム(端末)の認証(分類3)を行なう場合が考えられ、利用する通信応用によって使用形態が異なる。例えば、文書一括転送においては、受信側システムの利用者個人を実時間で認証することは難しいため、通信システム間の認証が適しているが、実時間に会議形式で文書編集を行なう場合は、利用者個人間の認証が重要となる。

②秘匿/改ざん防止機能　：　図2で示すように、本通信体系においては、ローカルな文書処理システムの文書を互いのシステムが共通に理解できる開放型文書に変換するため、ローカルな文書に対する秘匿処理(暗号化)や改ざん防止処理は意味をなさない。従って、本セキュリティ機能は、開放型文書を扱う通信システムで実行するものである(分類3)。

③作成元証明機能：　本セキュリティ機能は、文書を実際に作成した利用者が、個人の秘密情報(例えば秘密鍵)を用いて作成した文書に対して署名処理を施すものである。しかしながら、ローカルな文書への署名は無意味なこと、個人の秘密情報が通信システムへ露呈しないこと、どこででも検証処理ができること などを考慮すると、図3に示すように、ローカルな文書処理環境において利用者の個人情報に基づき、開放型文書に対して署名処理を行なう方法が適している。また、検証処理は、転送された開放型文書から検証情報(ハッシュ結果)を生成し、署名情報とペアで保管することが必要となる。

④リソースアクセス管理機能：　本セキュリティ機能は、アクセスする文書リソースに依存したもの(分類2)であり、文書アクセスを提供するために、アクセスマトリックスや能力管理(特権管理)などを実行する。

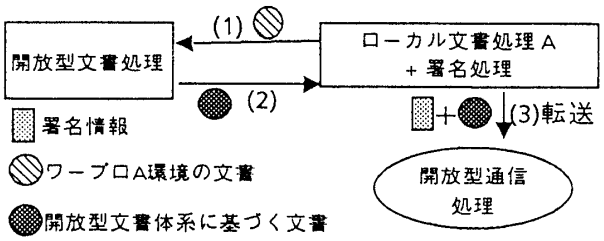

図3 署名処理とその転送

⑤受信否認不可機能　：　本機能は、文書受信側で受け取りの署名処理を行なうもので、上記作成元証明機能と全く同じ検討が必要となる。

5. セキュリティ機能の位置づけ

以上の整理により、開放型文書通信体系におけるセキュリティ機能は、図4に示すように位置づけることができる。(分類1)に属するセキュリティ機能は、開放型文書処理の変換処理をローカルに利用することにより、ローカル文書処理において実行される。また、(分類2)に属するものは、開放型文書のリソース管理属性や開放型通信処理のDFRやDTAMのリソース管理機能によって実現される。さらに、(分類3)に属するセキュリティ機能は、本体系で実行されるすべての通信応用において共通的に利用できるように位置づける必要があり、OSI応用層ACSE/プレゼンテーション層の直上で提供する方法が最も汎用的であると考察できる[2]。

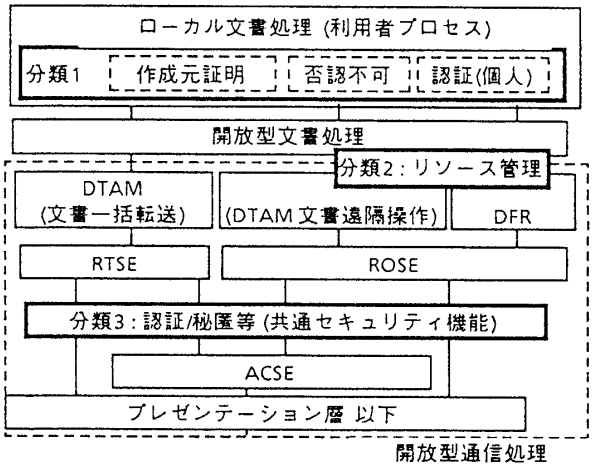

図4 セキュリティ機能の位置づけ

6. おわりに

本稿では、開放型文書通信体系におけるセキュリティ機能の位置づけの明確化を図った。最後に、日頃御指導をいただくKDD研究所浦野所長、眞家次長に感謝致します。

〈参考文献〉

[1] 中尾,小花,浦野,"テレマティクスサービスのための統合通信アーキテクチャ"1986,画像電子学会誌,Vol.15,No.4
[2] 中尾,田中,鈴木,浦野,"OSIセキュリティ通信様SCSEの実装と評価"1993/8,信学会論文誌,Vol.J76-D-I,No.8,No.4