M_039

エリア・センシティブなドキュメント認証システムの一検討

A study on area sensitive authentication system

半田 富己男†
Fukio Handa

1. はじめに

セキュアな情報システムでは，アクセス制御機能を用いてドキュメント等の利用者データ保護を実現してきた．アクセス制御機能は，識別され認証された利用者に対して，アクセス制御リスト等に表現されたアクセス制御のセキュリティポリシーを適用して，アクセス対象のオブジェクト(客体)へのアクセスを許可するかどうかを判断し制御する．

ウィルス等に感染している可能性があるセキュリティの低い環境では，従来のアクセス制御だけではセキュリティ上の問題があることを示し，こうした問題を解決するため，オブジェクトのセキュリティ属性にエリア情報を追加したエリア・センシティブなドキュメント認証システムを検討した．

2．アクセス制御

コンピュータの OS 等の情報システムには，システム内で発生したアクセス要求を許可するか，拒否するかを，あらかじめ設定されたセキュリティポリシーに従って決定するメカニズムが搭載されている．

アクセスを要求する能動的なエンティティをサブジェクト，アクセス対象となるエンティティをオブジェクトと呼ぶ．セキュリティポリシーに従ってアクセス制御を実施する抽象マシンをリファレンスモニタと呼ぶ．

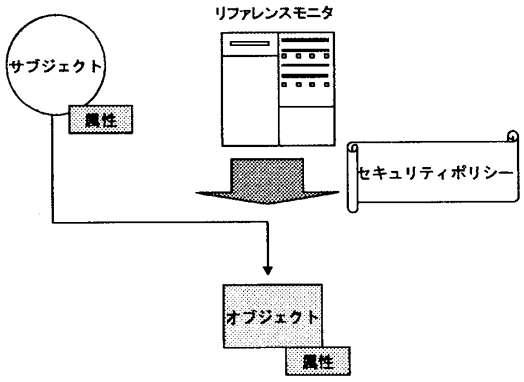

図 1 アクセス制御の概念

リファレンスモニタは，サブジェクトのセキュリティ属性，オブジェクトのセキュリティ属性に基づいて，オブジェクトに対してセキュリティポリシーを実施し，サブジェクトとオブジェクトの間での操作が許可されるかどうかを決定する．

3. エリアの概念

情報セキュリティ・マネジメントシステム(ISMS)の構築に際しては，業務施設及び業務情報に対する許可されていない物理的なアクセスを防止するため，物理的セキュリティ管理策を選択することが要求される．この結果，業務施設の周囲に，いくつかの物理的障壁を設け，セキュリティ境界が定義される．こうした「ゾーニング」を実装する際には，セキュリティが保たれた領域(以下，「セキュリティ・エリア」という．)への出入り口では，許可された者だけにアクセスを許すことを確実にするために，入退室管理装置を設置することが一般的である．入退室管理装置としては，磁気カードリーダや非接触 IC カードリーダで入室しようとする者を識別・認証し，電気錠を開錠する仕組みが多く見られる．最近では，利便性と IC カードの耐タンパー性を兼ね備えた非接触 IC カードを利用した入退室管理装置の普及が進んでいる．

入退室管理装置で制御されたゲートを非接触 IC カードで識別・認証を受けて通過する際に，入退室管理装置が非接触 IC カードにセキュリティ・エリアへの入室情報を書き込むことができる．このように，非接触 IC カードを媒介に，セキュリティ・エリア内に設置された各種セキュリティ機器を連携させた高セキュリティな環境の実現を図る取り組みがある．[1][2]

4. 従来のアクセス制御による問題点

従来のアクセス制御では，サブジェクトのセキュリティ属性とオブジェクトのセキュリティ属性だけに基づいてアクセスを許可するかどうかを決定していたので，識別と認証で正当な利用者と確認され，当該オブジェクトへのアクセス権を持ったサブジェクトに結びつけられた利用者であれば，どこからでも必ず当該オブジェクトへアクセスすることができた．

オブジェクトの作成者等の正当な利用者は，どこからでも当該オブジェクトにアクセスすることができる．このことは，営業機密が格納された会社のパソコンのケースでは，正当な利用者である従業員本人による情報の持ち出しを抑止できないことを意味している．持ち出された情報が自宅のパソコンやインターネット・カフェのパソコンにコピーされ，そのパソコンがウィルス等に感染していた場合には，持ち出された機密情報がインターネット上に流出してしまう危険性がある．このように，利用環境のセキュリティが十分に高いレベルに保たれてい

† 大日本印刷(株), DNP

ない場合には，従来のアクセス制御だけでは情報漏えいを防ぐことができない．

５．エリア・センシティブな認証

前章で述べた課題を解決するために，３章で紹介したエリアの概念の応用を検討する．

セキュリティ・エリアへの入退室アクセス制御に非接触 IC カードを利用した識別・認証を行う入退室管理システムでは，ゲートを通過する際に，入退室管理装置が非接触 IC カードにセキュリティ・エリアへの入室情報を書き込むことができる．

ドキュメント･ファイルを作成・編集するアプリケーション・プログラムでは，非接触 IC カードからエリア情報を読み出し，ドキュメント・ファイルを保存する際にファイルの属性情報としてエリア情報を含めて記録する．

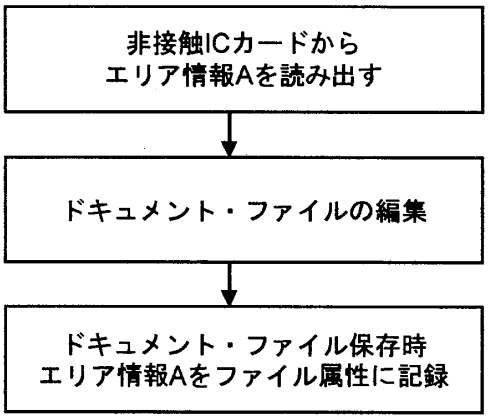

図２　ドキュメント生成時

このようにして作成・編集したドキュメント・ファイルを読み出そうとする場合には，読み出しアプリケーション・プログラムは，まず自己が動作している環境を非接触 IC カード内のエリア情報から読み出す．次に，アクセスを要求されたドキュメント･ファイルの属性情報から当該ファイルが生成されたときのエリア情報を読み出す．

読み出しアプリケーション・プログラムが現在動作している場所のエリア情報と，ドキュメント・ファイルの属性から取り出したエリア情報とを比較し，現在動作している場所のセキュリティ・レベルが，ドキュメント・ファイル属性から取り出したエリア情報のセキュリティ・レベルと等しいか高い場合にのみ，当該ドキュメント・ファイルへのアクセスが許可される．

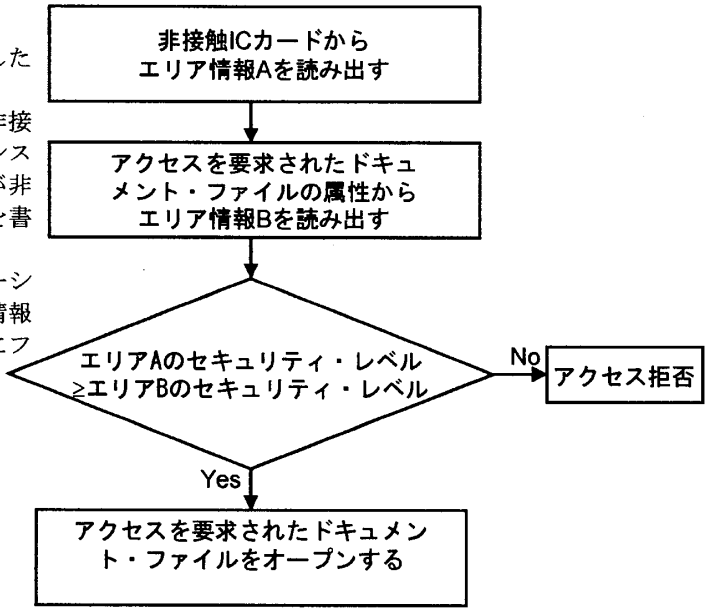

図３　ドキュメント読み出し時の認証

以上のように，従来のアクセス制御に加えて，ドキュメントへのアクセス要求を受けた時点で，読み出しアプリケーション・プログラムが稼働環境のエリア情報と，アクセス対象ドキュメントのエリア情報を比較してアクセスを許可するかどうかを決定するので，機密性の高いドキュメントの場合，たとえドキュメント作成者本人であっても，ドキュメントを作成したエリアよりもセキュリティ･レベルが低いエリアからは当該ドキュメントにアクセスできないので，情報漏えいの危険性を軽減することができる．

６．まとめ

本稿では，利用環境のセキュリティ・レベルが十分に高くない場合に，従来のアクセス制御だけでは情報漏えいを防ぐことができないことを示し，非接触 IC カードを媒介にして得たエリア情報をドキュメント・ファイル作成時に属性として含めておくことにより，ドキュメントを作成したセキュリティ・エリアよりもセキュリティ・レベルが低い場所では，ドキュメントへのアクセスを拒否することが可能なエリア・センシティブなドキュメント認証を検討した．

エリア情報を応用した認証系基盤システムへ発展させていく予定である．

参考文献
[1] SSFC,
http://www.dnp.co.jp/bf/ic_card/service_solution/ssfc.html
(7 July, 2006)
[2] 非接触 IC ソリューションの最先端を追う,
http://www.atmarkit.co.jp/frfid/special/icw2006/index.html
(7 July, 2006)