4T−10

Virtual Officeにおける セキュリティ管理の基本概念

上林弥彦　稲森豊
京都大学工学部

1　まえがき

Virtual Office（仮想オフィスシステム）は、ワークステーション、ネットワーク、FAX、電話、TV等をデータベースを中心に統合し、複数の利用者が相互に関連し合いながら仕事を行う環境（オフィス空間）をコンピュータ上に仮想的に実現するものであり、誰でも快適に作業できるような利用者インタフェースを有し、また、多彩な通信機能、共同作業環境など、オフィスに必要な様々な機能を提供することを目指す。

実際のオフィスでは、常に大量のオブジェクト（データや書類など）が扱われる。その中には様々な種類のオブジェクトがあり、機密文書や個人的書類も含まれる。Virtual Officeにおいてこれらのデータを扱うためには、実際のオフィスと同様、それらを管理、保護するためのセキュリティ機能が極めて重要である。また、様々な機器や仮想空間を管理するためにもセキュリティが必要となる。

そこで本稿では、Virtual Officeにおけるセキュリティ管理の様々な基本概念について提案する。

2　Virtual Officeのセキュリティの構成

通常のオフィスでは大量のオブジェクトが、多数の利用者によって共用される。そのため、Virtual Officeでそれらを管理するためにはデータベースを利用するが、データベースで様々なデータを共用するにあたり問題となるのが、いかにセキュリティ管理を行うかということである。

データベースのセキュリティとして、代表的なものにはMultilevel SecurityとDiscretionary Securityがあるが[1]、オフィス環境に適したセキュリティを考えると、両者の性質を併せ持ったようなセキュリティが必要であると思われる。その理由はまず、オフィスの構成員は全体でなんらかの階層構造を成しており、データベースはそれに合わせて階層的なセキュリティを提供すべきだからである。しかし、セキュリティが階層的な構造だけであるならば、例えば利用者は個人的にオブジェクトを管理、保護することができないなど、セキュリティ管理として柔軟性に欠ける。

そこで考えられるのが鍵によるセキュリティの導入である。自分の所有する空間（部屋や引出しなど）に鍵を付けることによってその空間の中へのアクセスを制限するのである。これにより、利用者中心のセキュリティ管理を行うことができる。鍵によるセキュリティは実世界と直接対応し、理解し易いため、利用者は簡単にセキュリティ管理を行うことができる。

本稿では、Virtual Officeのセキュリティに、データベースの階層的なセキュリティと、鍵を用いたセキュリティを統合した方式を提案する。

3　データベースの階層的なセキュリティ

この章では、Virtual Officeのセキュリティを構成する1つとして、データベースでよく用いられる、セキュリティレベルの違いによる階層的なセキュリティを提案する。

このセキュリティは、データベースにおけるMultilevel Securityに基づいているが、特徴的な点はアクセス権の種類及び、セキュリティレベルの付け方である。以下ではこの二点について述べる。

3．1　アクセス権の種類

普通のデータベースのアクセス権の種類は、読む権利、変更する権利（追加する権利、削除する権利）が一般的である。しかし、このオフィスシステムでは、オブジェクトを持ち出す権利をそれらに加える。

このシステムの利用者は、必要なオブジェクトを自分の所有する仮想空間で普通は管理をする。そのため、自分の所有する空間にあるオブジェクトを勝手に持ち出されては安全とはいえないので、このようなアクセス権が必要となる。

その他、コピーをとる権利やaliasをとる権利、プリントする権利などオフィスで必要なものを加えるべきである。

3．2　セキュリティレベル

このオフィスシステムでは、オフィスの仕事（プロジェクト）と利用者の複雑な関係と構造から、人およびオブジェクトのセキュリティレベルが複雑な階層を成している。以下では、オフィスの構造を説明し、人、オブジェクトのセキュリティレベルを定義した後、人がオブジェクトにアクセスできる条件を定義する。

3．2．1　オフィスの構造

オフィスには複数のプロジェクトが存在し、人はそのいくつかに属している。各プロジェクトごとに、地位などによる階層構造が独立に存在する。

3．2．2　人のセキュリティレベル

先ず、人のセキュリティレベルを定義する。人のセキュリティレベルは、その人が属しているプロジェクトP_mとそ

Basic Concepts of Security Management for Virtual Office
Yahiko KAMBAYASHI, Yutaka INAMORI
Faculty of Engineering, Kyoto University

の中でのレベルLh_iの組の集合で表され、

$$((Ph_1,Lh_1)(Ph_2,Lh_2)\cdots(Ph_m,Lh_m))$$

と定義する。人は複数のプロジェクトに属している場合があるため、一般にこのような組みの集合となる。

3．2．3　オブジェクトのセキュリティレベル

通常、オブジェクトの重要度（秘密の度合）は、プロジェクトの違いにより変化する。例えば、ある資料は、プロジェクトAではみんなが知ってもよいが、プロジェクトBでは管理者のレベルにしか知ってはいけない、といった管理の必要度は高い。このような性質を表すようにオブジェクトのセキュリティレベルを定義する。オブジェクトが、プロジェクトPd_iではレベルLd_i以上の人にアクセスできるときに、次の形でオブジェクトのセキュリティレベルを定義する。

$$((Pd_1,Ld_1)(Pd_2,Ld_2)\cdots(Pd_n,Ld_n))$$

以上のように、人とオブジェクトのセキュリティレベルは複雑な階層で表される。

3．2．4　アクセスできる条件

人とオブジェクトのセキュリティレベルより、人がオブジェクトにアクセスできる条件を定義する。オブジェクトのセキュリティレベルの定義より、人はプロジェクトPd_1～Pd_nのうちのどれかでレベルがLd_i以上であればそのオブジェクトにアクセスできる。すなわち、

$$Ph_i=Pd_j \quad \text{かつ、} \quad Lh_i \geqq Ld_j$$

であるようなi,jが存在する場合、その人はそのオブジェクトにアクセスできる、と定義できる。

以上のとおり、このセキュリティはオフィスの構造に対応した、複雑な階層のセキュリティを実現する。OSでよく用いられる*-性は問題が多いのでここでは仮定しない[2]。

4　鍵による空間の管理

3章で提案したセキュリティは、オフィスの全体的なセキュリティを提供するものであるが、個々の利用者に対するセキュリティとしては不十分である。そこで、実世界で最も広く使われている鍵によるセキュリティをこのオフィスシステムに取り入れ、併用する。以下では鍵によるセキュリティの概要を説明する。

オフィスの中の単位空間（部屋や引出しなど）には鍵を付けることができる。鍵を付けた場合、その空間の所有者だけが他人に鍵を渡す権利があり、鍵を渡された者だけがその空間内へアクセスできる。鍵には種類があり、普通の鍵、コピー可能な（ほかの人に配ることができる）鍵、又貸しできる鍵などがある。利用者が必要に応じてこれらの鍵を使い分けられるように、柔軟性を持たせている。

鍵によるセキュリティにおいて、最低でも次の機能を備えていなければ十分なセキュリティとは言えない。まず、利用者は、自分の所有する空間の鍵を誰に渡しているかを知る機能が必要である。また、貸した鍵は、相手の意志にかかわらず回収することができなければならない。この二点は、自分の所有する空間のアクセス権の確認と、変更に関わる機能であると言え、必ず必要である。

この鍵による空間の管理は、利用者中心のアクセス管理であり、Discretionary Securityと言える。そして、これによって例えば、秘密にしたい文書を仕舞っておいたり、特定の人のみと空間を共有するなど、様々な形でのセキュリティ管理を行うことが可能となる。

5　その他のセキュリティ

この章では、3、4章で挙げたもの以外のセキュリティを提案する。

仮想空間、オブジェクトと共にオフィスを構成する要素である機器（プリンタなど）を管理するセキュリティが必要である。例えば、機器へアクセスできる利用者を制限したい、という要求を満たすためである。

鍵によるセキュリティを援助するものとして、例えば、いつも鍵の付いた引出しに仕舞ってあるオブジェクトを机の上に出したまま、あるいは、鍵の付いた引出しを開けたまま部屋を出ようとした時、その人に警告を発し、自動的に元の状態に戻す、といったようなセキュリティがも必要である。

また、退室している間に他の人が自分の部屋に入った場合、その人の行動を表すHistory fileを作成する機能も必要である。

6　あとがき

Virtual Officeにおけるセキュリティの基本概念として、データベースの階層的なセキュリティと、鍵による空間の管理の併用を提案し、その意義を述べた。

この方式により、オフィス全体の階層的構造と、利用者個々の権利が両方とも強調されるような、調和のとれたセキュリティが実現できる。

今後は、さらにオフィスシステムにふさわしいセキュリティ機能の追加とその効率的な実現法について研究を進める予定である。

参考文献

[1] Teresa F. Lunt, Eduardo B. Fernandez: Database Secrity, in SIGMOD RECORD, Vol. 19, No.4 (1990).

[2] Somchai Chatvichienchai, Yahiko Kambayashi: Preventing Inference and Unauthorized Modification of Protected Data in Multilevel Relational Databases, in Proc of an International Conference InfoJapan'90.