ビジネスアプリケーションのための新しいアクセス管理の視点

A new viewpoint of access control for business application

桑原 悟*

Way of Access control for business application systems was firstly implemented from computer systems or their operating systems' viewpoint. Then, for business use, several types of methodology for application systems have been created and any of these access control ability remains only inside of the methodology. These are natural and understandable. But, for the next stage of business application, it is necessary to introduce new sight or viewpoint from business administration.

In this paper I observe some main existent access control and show their limit, then propose new viewpoints. They are "Richness on description of real organization", "Flexibility on dynamic administration", "Balance of convenience and security", "Rest from human vulnerable ness" and "Information management".

1．はじめに

情報通信技術（IT）の発展とインターネットの拡大の中，商用利用に加え行政での利用も含めた，ビジネスアプリケーションにおける情報セキュリティへの関心が高まっている。

情報セキュリティ上の脅威とこれに対する対策は，一般的に表1のように整理される。

表1　情報セキュリティ上の脅威

脅威	対策	効果
盗聴，漏洩	アクセス管理，暗号化	防止
改ざん	アクセス管理，電子署名	検知
成りすまし	アクセス管理，電子署名	防止
否認	電子署名の応用	防止
破壊，妨害	アクセス管理，ワクチンソフトウェア	防止，排除，追跡

*KUWAHARA, Satoru［情報システム学科］

表1中の対策は，具体的には，それぞれ情報処理技術とその応用製品，組織内の運用，利用者の教育及び，外部による監査などを組み合わせて行うことになる。このうち，アクセス管理に分類される対策で利用されるアクセス制御の技術は，さまざまな研究が成されているが，残念ながら，実際のビジネスシステムに対しては，必ずしも貢献できる状況にはない。

本論文では，これまでの技術的アプローチの成果である各種のアクセス制御技術を取り上げ，ビジネスシステムでの有効性を評価し，加えて，この方面の新たな尺度としての評価項目について提案する。

2．既存のアクセス制御モデル

アクセス制御のモデルの最も基本的なものとしては，①Discretionary Access Control（自由裁量アクセス制御）モデルと②Mandatory Access Control（強制アクセス制御）モデルの二つのモデルをあげることができる。

また，最近では，Webアプリケーションの拡大にともない，いわゆる「eコマース」での利用や企業内での情報共有に関するポリシとの整合と使いやすさの視点及び，ワークフローマネジメントシステム（WFMS）の観点からのアプローチも出てきている。その代表的なものとしては，WFMS特有の概念である③ロールに基づいたアクセス制御モデル，④タスクとワークフローのためのアクセス制御モデルがある。

さらに，⑤エージェントに基づくアプローチ及び，⑥オブジェクト指向に基づくアプローチが登場してきている。この章では，これらについて概観し，ビジネスシステムの視点からその有効性を考える。

2．1　自由裁量アクセス制御モデル

自由裁量アクセス制御モデルでは，その存在が既知であるシステム内のすべてのアクセスする側（アクセス主体）とアクセスされる側（アクセス対象）について，アクセス権を決めるものである。

アクセス主体は，利用者，利用者のグループ及び，これらに代わって処理を行うプロセスであり，このモデルでは，あるアクセス主体が，あるアクセス対象の所有権をもっている場合，このアクセス主体は，このアクセス対象へのアクセス権を他のアクセス主体に自由に与

える権限及び無効にする権限がある。

これは，融通性はあるが，これで実現できるセキュリティのレベルは高いとはいえない。たとえば，アクセス主体A（以下　A）が，アクセス対象X（以下　X）に対するアクセス権があり，アクセス主体B（以下　B）は，Xに対するアクセス権がない場合を考える。Xの所有権をもつAは，コピーが許されるので，Xのコピーをアクセス対象Y（以下　Y）として作成することができる。さらにこの所有権に基づいて，Bにアクセス対象Yのアクセス権を与えることができるが，この場合，本来Xのアクセス権のないBが，Xと同等の内容に触れる結果となる。

Web環境は，このような不都合を大きく広げる特性をもっており，その結果，重大なセキュリティ侵害につながる危険がある。

このモデルに属すものに，Harrison, Ruzzo and Ullman（HRU）アクセス制御マトリクス（ACM）モデル[3]がある。このモデルでは，ACMで，アクセス主体のアクセス対象に対するアクセス権を設定し，ACMを連結統合する形で，全体のアクセス権スキームを構築している。

この種の問題は，Harrisonらが提示した，「安全性の問題」すなわち，「あるアクセス主体が，以前にはもっていなかった権限をもつようになる状況が存在するかどうか」という問題に属する。

この「安全性の問題」に対しては，一般には決定不能であることが示されているが，安全性が決定可能であり，かつ，扱い易いいくつかの新しいモデルも提案さてれている。

代表的なものとしては，セキュリティの型の概念を導入した，スキマティック防御モデル（SPM），型アクセスマトリクス（TAM）モデル及び，動的型アクセス制御（DTAC）モデルがある。[5]

このうち，DTACは，アクセス主体の型とアクセス対象の型の両方を用意しているので，アクセス主体とアクセス対象の間の区別をなくすことができるという特徴がある。実体を型でグループ分けすることで，コンフィグレーションを簡単にし，管理しやすくしようとしているといえる。また，DTACモデルは，動的な型付けの仕組みを使っているので，インターネットのような動的環境に適していると言える。さらに，DTACでは，セキュリティ型の静的解析に加え，動的チェックをすることで，システムのセキュリティを実現している。

James B.D. Joshiらも述べている[2]ように，これらACMに基づくモデルの展望は広がりつつあるが，これらはまだ理論的開発段階であり，実証的成果はまだ期待できない。

2．2　強制アクセス制御モデル

強制アクセス制御モデルでは，アクセス主体とアクセス対象は，予めアクセスの決定のもとになる，機密性レベルによって分類される。DACモデルのように，利用者の裁量の入り込む余地はない。MACモデルの目指すものは，情報の秘匿性と完全性を確かなものにするために，情報流れを制御することであり，これはDACモデルでは成し得ないものである。

MACモデルでは，Bell-LaPadulaの制約としても知られる，"No-read up and no-write down"規則を使った多層セキュリティを実装することができる。この規則によって，情報が上位の機密レベルの層から下位の機密レベルの層に流れ込まないことが確実になる。

また，情報の完全性を達成するためには，"No-read down and no-write up"規則が使われる。この目的は，完全性の低い情報が，完全性の高い層のアクセス対象に流れ込まないようにすることである。このような機密レベルの多層化は，Webベースのアプリケーションにとっては，有効かつ不可欠であると考えられる。

MACモデルは，DACモデルとは違い，より強固なデータ防御メカニズムを提供し，同時に情報制御ポリシのような，より細かい規定を扱うことができる。

しかし，実際のMACポリシの施行は，相当難しいものになり，また融通性がないので，実用的Webアプリケーションへの適用は，難しいと言わざるを得ない。さらに，実在の組織のセキュリティは，特に可用性の実現において単純なものでは実現はできない側面をもっている。DACとMACの両方を必要とするようなものかもしれないし，ポリシの混合など，DACでもMACでも実現できない類の解決案が必要になる可能性がある。

また，もともとこれらのモデルは，Webアプリケーションを前提にしたものではないので，ハイパーテキストベースのシステムを意識していない。ハイパーテキスト情報は，リンク，フレーム，スロット，ドキュメントノードなどのアクセス対象を使用するが，これらはすべて防御される必要がある。

ハイパーテキストシステムの特徴は，「データ項目間の接続」，「独特なナビゲーション的側面」及び，「スキームのないこと」である。James B.D. Joshiらも述べている[2]ように，これらに対するセキュリティ関連の拡張は提案されているが，情報のコピーと拡散の制御，アクティブなアクセス対象の管理及び，多重データ型と複雑な内部関係のサポートなどのことがらは，実用的なWebアプリケーションのための解決案としては，まだ研究段階である。

2．3　ロールに基づくアクセス制御モデル

ロールに基づくアクセス制御（RBAC）モデルは，一般化されたアクセス制御のアプローチとして注目されている。ここでいうロールとは，アプリケーションシステム上に写像された組織の責任と機能を代理するものである。

ロールに基づくモデルは，直接的，恣意的であり，ロールの階層化と制限を行えるので，ポリシから独立であり，逆に言うとどんなセキュリティポリシにも対応できると言える。また，DACとMACを包含しており，利用者が設定可能である。

このモデルでは，ロールがアクセス権をもっているので，セキュリティ管理が単純化される。たとえば，利用者が組織内で新しいロールに異動したなら，その利用者を，単純に新しいロールに割り付け，前のロールからはずすだけで，権限は正しく設定される。

RBACモデルがなければ，この利用者の以前のアクセス権を一つ一つ無効にし，新しいアクセス権を一つ一つ設定しなければならない。

特別な管理のロールとして，他のロールを設定するロールがある。この管理のロールも階層化が可能であるので，セキュリティ管理の構造とうまく適合させることができる。セキュリティ管理が複雑な大規模なWeb活用を行っている企業が望むものであると言える。

ここで，情報の誤用の防止や不正行為を防ぐためには，いくつかの権限の制限が必要となる。セキュリティの領域で，よく知られている権限の制限に，職務の分離（SOD）がある。

これは，どの個人にも，システムに対して，単独で詐欺行為ができるような大きな権限を許さないというものである。詐欺行為のリスクを減らすことが，SODの趣旨である。

このような制限は，RBACモデルに，利用者のロールの設定とロールと権限の割付のSOD制限を行えば，容易に実現することができる。さらに，必要最小限のアクセス権限をロールに割付けることで，サインオン中の偶発的誤りによる被害を最小限に押さえることもできる。

RBACシステムにおいて重要な点は，一時的な制限つまり，ロールの開始日時と有効期間，他のロールからの起動によるロールの時間指定の有効化である。RBACモデルを使うと，Webベースアプリケーション一般にとってもそうであるが，特にWFMSにとって鍵となる高いセキュリティを達成できる可能性がある。

「WFMSで，ロールをワークフローのタスクに割り当て，利用者は，このタスクを実行するために必要なすべてのロールをもつということで，その権限を与えられる」という仕組みにすることで上手く対応できる可能性がある。

しかしながら，WFMSの複雑なセキュリティ上の要求を扱うための，強固なRBACフレームワークでは，ロールとタスクの間の一時的，非一時的制限や従属の制限などが必要となる。現段階で，これを開発しようとすることは，相当に時間と労力がかかる挑戦であるといわざるを得ない。

2．4　タスクとワークフローのためのアクセス制御モデル

前出の各モデルでは，アクセス主体とアクセス対象という見方がされていた。これらのモデルでは，情報の内容によるアクセス管理，すなわち，WFMSにおけるタスク／トランザクションの性質に適用するには，融通性の点で不十分である。WFMSは，広範囲な自動トランザクション機能が要求されるアクティビティ集中Webアプリケーションを可能にする重要技術として登場してきた。このようなアプリケーションは，典型的に，組織内の部門や地理的，文化的な境界を越えて行き来するトランザクションとタスクとの複合物として構成され，Webでのセキュリティをさらに悪くする。

アクティビティ集中とタスク集中のアプリケーションを強力にサポートするアクセス制御モデルの開発は熱望されているが，これらのアプリケーションに関連した主要なセキュリティ問題を解決するアクセス制御モデルは，まだ存在していない。

WFMSに関しては，いくつかの認証のモデルで，ワークフロータスクの実行中のセキュリティを強制的なものにするため，ロールをワークフロータスクに割り当てる方法が提案されている。Webベースのアプリケーションのワークフロータスクは，多様なセキュリティドメインに広げられ，厳密な一時的でありタスク間の従属性の制限をもつと考えられる。タスクに割り当てられたロールは，静的又は動的な自分自身の一時的，非一時的制限をもつことも考えられる。ワークフローにセキュリティを強要するためのRBACの枠組みは提案されているが，実際の適用には，WebアプリケーションとWFMSに関するセキュリティ問題に集中的に焦点をあてた議論を進める必要がある。

このようなタスク指向システムの独特な要求を効果的に解決するセキュリティを実現するため，Thomas, R.K.らは，階層化したアクセス制御モデルのファミリを提案している[8]。これは，Task-Based Authorization Controls（TBAC）と呼ばれ，TBAC0～TBAC3モデルのファミリで構成されている。

TBAC0モデルは，基本すなわち最小のものとしてのタスクと認証手順とそれらの従属物を

与え，TBAC1モデルは，TBAC0の拡張であって2以上の認証手順の合成を含んでいるものである。TBAC2モデルは，TBAC0の別の拡張であり，静的及び動的な制限を許している。TBAC3モデルは，TBAC1モデルとTBAC2モデルの両方の性質をもった連結モデルである。

2．5　オブジェクト指向に基づくアプローチ

オブジェクト指向のソフトウェアでのアクセス管理の場合，オブジェクト指向の特徴である継承に関連する問題が懸念される。実世界の権限と照らすと，それは，必ずしも単純に継承されればよいということにはならない。アクセス権の継承については，Izakiらによって，次の3種類が提案されている。[9]

Instance-ofの関係では，オブジェクトxは，クラスcから生成されるとすると，クラスcのアクセスルールαcは，オブジェクトxに継承される。その後オブジェクトxのオーナは，クラスcから継承されたアクセスルールに対し制限をつけたり無効にしたりすることができる。ここで，クラスのアクセスルール<c,opi>が無効にされたならば，オブジェクトのアクセスルール<x,opi>も無効になる。

Is-aの関係のクラスでは，クラスdをクラスcのサブクラスとし，αcをクラスcのアクセルルールの集合とする場合に対して，次の三つの考え方を示している。

ケース1：αcは，dに継承され，その後のαcの要素に変更があれば，それはdにも反映される。

ケース2：αcはコピーされて継承されるが，このコピーは，もとのαcとは独立のものとなる。

ケース3：αcは，dに継承されない。

Is-aの関係のオブジェクトにおいては，クラスdのオブジェクトyがオブジェクトxから生成された場合に対して，二つの考え方が示されている。

一つの考え方は，xの値とメソッドはyにコピーされない。すなわち，yはxの値もメソッドももたないというものである。sがメソッドopを使ってクラスcのオブジェクトyを操作することを考えると，sにアクセス権<x,op>だけが許されている場合にだけ，sは，opをxに対して実行することが許される。この場合，アクセス権の付与の関しては，オブジェクトyのオーナSy

は，クラスcのオブジェクトyのアクセス権を他に与えることはできず，あるオブジェクトxにアクセス権を与えることができるのは，オブジェクトxのオーナSxだけということになる。この考え方では，アクセスルールα cは，オブジェクトyのなかのオブジェクトxの値とメソッドを操作するために使われる。

Is-aの関係のオブジェクトに関してのもう一つの考え方では，値とメソッドはコピーされるというものである。この考え方では，クラス間の継承の議論と同様である。

Part-ofの関係においては，クラスdが，クラスc1，c2，c3，･･･，cmから構成されるとすると，個々のクラスciのアクセス規則は，次の三つが考えられる

ケース1：α ciは，dに継承され，その後のα ciの要素に変更があれば，それはdにも反映される。

ケース2：α ciはコピーされて継承されるが，このコピーは，もとのα ciとは独立のものとなる。

ケース3：どのα ciも，dには継承されない。

これらは，Is-aの関係のクラスの場合と同様である。

2．6　エージェントに基づくアプローチ

適用性，協調性，自立性，可動性などの特徴をもつソフトウェアエージェントは，システム構築パラダイムとして，一般的になりつつある。このパラダイムは，Webアプリケーションのためのセキュリティ上の性質を提供するのに有効に使われる可能性があり，サーバ及びクライアントにセキュリティ実現のタスクを割り付けることに利用できるであろうエージェント通信言語もある。

可動性と適用性は，インターネットの資源の効果的な利用には必要ではあるが，そこにはセキュリティ上の脅威も存在する。たとえば，悪意のある振る舞いをするエージェントが存在する可能性もあり，そうなれば，ホストの動作が混乱させられる。同様に，ホストが，ローカル資源に対してのアクセス要求を拒否して，エージェントの動きに影響を及ぼす場合もあり得る。

3．実利用局面での有用性の項目

2章では，6種類のアクセス制御モデルについて，その概要と特徴及びビジネスシステムへの適用についての考察を行った。ここでは，ビジネス上の実際業務の観点から，アクセス管理の備えるべき能力について考える。

3．1　実際業務からの視点

自由裁量アクセス制御モデルと強制アクセス制御モデルは，コンピュータシステムのオペレーティングシステムへの実装の視点から発想された，もっとも基本的な能力と捉えることができる。それは逆に言えば，実際のビジネス又は業務における利用者側の要求を満たすものとはなっていないということである。

また，オブジェクト指向に基づくアプローチとエージェントに基づくアプローチは，それぞれに，オブジェクト指向及びエージェントという新しいパラダイムの登場を得て，基本的な，そして実装可能なアクセス管理機能の実現という視点から発想されており，利用者側のアクセス管理に対する要求を満たしているわけではない。

この点，ロールに基づくアクセス制御モデルとタスクとワークフローのためのアクセス制御モデルは，ビジネスの実際業務を意識したロールの概念や，業務アプリケーションの技術基盤のひとつと考えることできるワークフローを前提としているので，ビジネスでの利用を考える場合，より利用者の要求にそったアプローチであると言える。しかし，ロールやワークフロー自身が，実際業務の記述性あるいは，実際業務への適用性の点で，利用者の期待に対し，まだまだ課題を含んでいる現状から見ても，これらのアクセス管理ですべてが解決されるわけではない。

そこで，OSなどの基本機能への実装の視点ではなく，また，ビジネスアプリケーションを構築する技術基盤を前提にするのでもなく，純粋に利用者の要求を満足するために必要なアクセス管理の考え方や機能を出発点とする必要がある。

そこで，このためにアクセス制御に必要な要素項目として，次の五つを考える。

（1）静的記述性

（2）融通性（動的変更対応性）

（3）強さと扱いやすさのバランス設定性

（4）人間系の脅威からシステムを守る能力

（5）情報管理性

3．2　静的記述性

実際の業務では，情報の管理が役割と権限と関連して行われ，この点は，ワークフローにも取り込まれている。ある程度以上の規模の企業などであれば，その中に役割に応じた部門が設定されており，部門にはそれぞれ責任者が割り当てられている。部門は，階層的に構成されることがあるが，下位部門の責任者は，その上位部門の責任者が必ずもっているというような単純な権限の包含関係であるとは限らない。

たとえば，当該の個人に事故などがあった場合などの非常時の権限代行は，複数の者に，一人ではその権限が行使できないような仕組みとして，分割されている場合などもある。またこのときは，何をもって非常時とするのか，権限行使と同時に記録や届け出などの不正防止及び記録のための行為が義務付けられているものをどのようにアプリケーションシステムに反映するのかの問題もある。

ここでの権限の行使は，当然ながら情報へのアクセス及び情報システムの機能の利用を含むわけであるから，アクセス管理に求められる能力の一つとして，このような，情報システム以前に存在する，あるいは，明示的には存在しないかもしれない，組織のなかの役割と権限を記述できる力があげられる。

3．3　融通性（動的変更対応性）

静的記述性で述べた非常時に備えるためのアクセス管理の能力として，非常時の識別又は非常時であることの記述の能力と，その記述を宣言又は公表する能力が必要である。これにより，非常時の処置の正当性を証明する，あるいは責任を明らかにすることができる。また，この能力は利用者にその存在と適用を周知することにより，乱用の抑止にも繋げることができる。場合によっては，公知とすることで，外部の悪意をもつ者に何らかの攻撃を諦めさせる効果も期待できる。

3．4　強さと扱いやすさのバランス設定

情報システムである以上，事前に決定された条件に従って動作することは，情報システムを構成しているプログラムがそうであるように排除することのできない性質の一つであると

言える。しかし，マンマシンインタフェースの部分においては，セキュリティレベルの設定を，“する”と“しない”の二者択一の設定を利用者にせまることは，本来必要なセキュリティレベルとは関係のないものとなる危険性があり，設定したのは利用者であるということから，システムの能力不足を利用者側に転化してしまうことにもなり得る。

実際の業務での利用を考える場合は，理想的には2次元程度の座標に値をプロットするようなセキュリティレベルの値の決定を決定するマンマシンインタフェースが望まれるが，少なくとも重大な誤解を与えない範囲で，セキュリティレベルとシステムの使い安さのトレードオフの理解を与える仕組みとマンマシンインタフェースが必要である。

3．5　人間系の脅威からシステムを守る能力

あらゆる業務を扱う中心は，人間であることに間違いはない。人間には，当然，機械やコンピュータにはない能力があるが，同時に人間のもつ弱点が，ビジネスシステムの情報セキュリティ上の脅威となりうることも否定できない。ここで考えるのは，人間が関与することで発生するシステムの脆弱性に対し，アクセス管理の側でこれを補う能力である。

そして，実は，このことは，人間をストレスから解放するものでもある。

逆に言えば，残念ながら情報セキュリティは，これまで利用者である人間にストレスを与えてきたと言うこともできる。

パスワードは，意味の無い文字列の記憶と頻繁な変更への追随を人間に強いてきた。これは，たいていの人間にとってストレスとなり，その影響がシステムのセキュリティに，その程度の差はあるものの，悪い影響として跳ね返ってくることは，否定できない。またWebアプリケーションの登場は，操作の権限をもつ人間を拉致，脅迫あるいは，誘惑して，遠隔地からその権限を不当に行使させる類の犯罪被害というリスクを生み出すことも考えられる。

これらの人間の脆弱性への対応が，今後よりいっそう拡大し，価値の高いことがらを扱うようになるビジネスシステムにとって，重要な能力となることは疑う余地がない。

3．6　情報管理性

実際の業務においては，情報とデータ又はファイルが同じではない点に，情報の管理の難しさがある。

例えば，清涼飲料の味を決定する成分割合，半導体製品の歩留まり，出荷先で異なる値引

き率など，外部にもれることによって企業活動に重大な影響を与える可能性のある情報は様々である。

ここで，たとえば，いわゆるトレードシークレットとされる機密の情報として，「製品Aの原料Bの割合が18%である」という情報を管理する場合を考える。ここでは，この情報と等価な情報は，すべてコピーをさせないという機能が求められるが，このままの記述すなわち文字列をコピー不可にするだけでは当然ながら不十分である。

それでは，等価な情報を構成する，「製品A」や「原料B」とういう単独の情報がセキュリティレベルの低い場所に存在できなくすることでよいかと言えば，別の，例えば資材部門の調達リストなどには，原料Bあるいはそれがコード化されたものが存在しなければ，発注業務は行うことができない。また，機密情報から抜き出された情報の管理（コピーやカットアンドペースト機能の管理），類推されたり形を変えたりして出て行く（消去法などで分かってしまう）情報の管理も重要な視点である。

また，内部監査や外部監査の証跡としての情報を提供することも今後のビジネスシステムのアクセス管理を考える上で，重要な視点となる。

4．おわりに

本論文では，情報セキュリティ上重要な，アクセス管理について，歴史的なコンピュータシステムの側からの発想と業務指向の基本的機能をもつインフラストラクチャでの発想について，その考え方と，組織内の本格的ビジネスシステムへの適用の視点からの課題をあげ，最後に，今後本格化するビジネスシステムでのアクセス管理に求められる新たな視点について述べた。

今後の研究は，この新たな視点での評価尺度の構成と，実際の情報システムでの実現を目指すものとしていく考えである。

参考文献

(1) James B.D. Joshi "SECURITY MODELS FOR WEB-BASED APPLICATIONS" CACM pp.38-44, Feb. 2001

(2) Harrison, Ruzzo, and Ullman, "Protection in operating system", CACM19,8 Oct. 1976

(3) Ferraiolo, Barkley and Kuhn, "A role-based access control model and reference implementation within a corporate intranet", ACM Trans. Info. Syst. Security 2,1, pp.34-64, Feb. 1999

(4) Proceedings of The Fifth ACM Workshop on Role-based Access Control, Jul. 2000

(5) Sandhu, "Lattice-Based access control model". IEEE Computer26,11 1993

(6) Bertino, Pagani, Rossi and Samarati, "Protecting information on the Web." CACM Nov. 2000

(7) Thomas, "Task-Based Authorization Controls (TBAC)" IFIP WG11.3 Workshop on Database Security (Lake Tahoe, CA), Aug. 1997

(8) Izaki, Tanaka and Takizawa "Access Control Model in Object-Oriented Systems" 情報処理学会, 研究報告「コンピュータセキュリティ」 pp.81-86, Vol8 (2000)

(9) AJ. Menezes, PC. Van Oorschot, SA. Vanstone, "Handbook of Applied Cryptograpy, CRC Press, 1997"