社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－DBS－143（2）
2007／7／2

ロールベースアクセス制御におけるロール分散実装方式とそのICカード運用管理への適用

近藤 誠一[†,††] 岩井原瑞穂[††] 吉川 正俊[††] 小宮 崇[†] 大沼 聡久[†]
山田 耕一[†]

† 三菱電機株式会社情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1
†† 京都大学大学院情報学研究科社会情報学専攻 〒606-8501 京都市左京区吉田本町
E-mail: †Kondo.Seiichi@dr.MitsubishiElectric.co.jp, ††{iwaihara,yoshikawa}@i.kyoto-u.ac.jp

あらまし セキュリティ対象のアクセス制御手法として，ロールベースアクセス制御 (RBAC) モデルに基くポリシー適用が，企業情報システムで実践されつつある．しかし，多様なセキュリティ対象へ展開されたアクセス制御情報の一貫性制御，監査ログにおけるユーザの特定が課題となっている．本稿では，実行時のセッションの設定方式として仮想ユーザを導入して，ロールを分散実装するモデルを提案し，ICカード運用管理への適用例を示す．
キーワード ロールベースアクセス制御, セキュリティポリシー, セキュリティ統制, ICカード

A Role Propagation Method for RBAC and its Implementation to Smart Card Management

Seiichi KONDO[†,††], Masatoshi YOSHIKAWA[††], Masatoshi IWAIHARA[††], Komiya TAKASHI[†], Akihisa ONUMA[†], and Koichi YAMADA[†]

† Mitsubishi Electric Corporation, Ofuna 5-1-1, Kamakura, Kanagawa, 247-8501 Japan
†† Kyoto University Yoshidahonmachi, Sakyo-ku, Kyoto 606-8501 Japan
E-mail: †Kondo.Seiichi@dr.MitsubishiElectric.co.jp, ††{iwaihara,yoshikawa}@i.kyoto-u.ac.jp

Abstract Role-Bases Access Control has emerged as an implementation model for users and access contol administration in enterprise IT systems. However, integrity control of access control information which are propagated to various kinds of target systems distributed widely and user identification in their audit log are still challenging tasks. In this paper we introduced new RBAC model which propagate roles using Virtual User and presented an example to implement smart card management.
Key words Role-based access control, RBAC, Security policy, Security governance, Smart card

1. まえがき

企業におけるセキュリティ統制のため，アイデンティティとアクセス制御の集中管理が運用面，統制面で注目されている．アクセス制御の手法としてロールベースアクセス制御 (RBAC) モデルによって設計されたアクセス制御ポリシーが，企業情報システムで実践されつつある．しかし，広域分散拠点に散在する多様なセキュリティ対象へ展開されたアクセス制御情報の一貫性制御，監査ログにおけるユーザの特定が課題となっており，システム構築コスト，運用コストと脅威レベルのトレードオフを考慮した方式が必要とされている．

本稿では，実行時のセッションの設定に仮想ユーザを導入して，ロールを分散実装するモデルを提案し，認証手段としてICカードを採用した場合の運用管理への適用例を示す．

本方式は以下の特長を持つ．

- ユーザを特定しないロール設定済みの仮想ユーザをRBACモデルに加えて，一般によく用いられる来訪者向け入館証，一時貸し出し予備カードを表現した．
- あらかじめロールを設定した仮想ユーザと実ユーザを結びつける手続き型ルールの実行を自動化した．
- 監査ログに残る仮想ユーザと，実ユーザの紐付けを，アイデンティティの多層管理と監査ログ収集時結合で実現した．

2. 基本事項

2.1 アイデンティティ管理とアクセス制御

情報漏洩対策として，従来，個別にセキュリティ対策が施さ

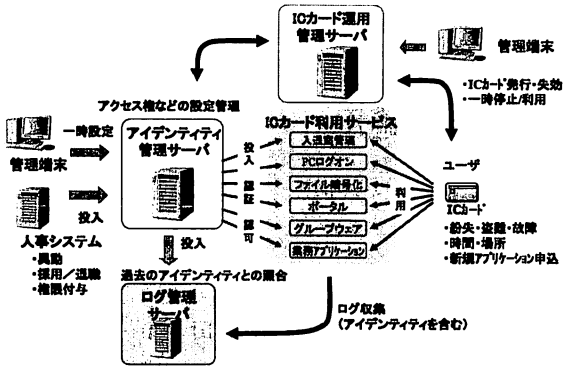

図 1　アイデンティティライフサイクル管理

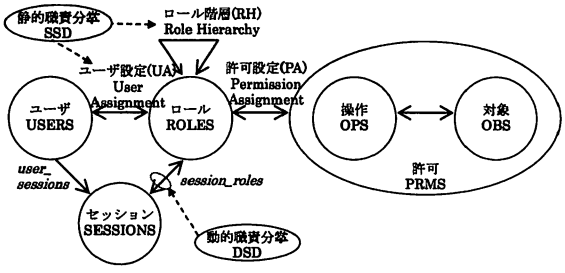

図 2　NIST 階層 RBAC

れてきたが，様々な脅威に対して継続的に維持・向上させていくためには，体系的な導入が有効であると考えられている．そのひとつとして，ユーザをキーとして，機器，情報，業務アプリケーションに対する行為の実行前のアクセス制御，実行後の監査を行うための基盤であるアイデンティティ管理システムが導入されはじめている．ユーザを中心として統制を行うシステムでは，図 1 に示すように，導入後の人事異動等の変化，及びユーザを識別するために導入される IC カード等の認証デバイスの変化に対して確実に，かつ，速やかに追随するライフサイクル管理が必要とされる [1].

また，内部統制のフレームワークである COBIT4.0 [2] では，システムセキュリティの保証を実現するための手段として，(1) セキュリティ要件と，脆弱性，脅威の認識，(2) 標準化された方法によるユーザの識別と認可の管理，(3) 定期的なセキュリティテストの実施をあげている．さらに，IT 成果を効果的管理するためのモニタリングプロセスの必要性が示されている．

2.2　RBAC モデル

ロールベースアクセス制御 (RBAC:Role-Based Access Control) モデル [3] は，セキュリティ管理の一般的な手法として広く用いられている．RBAC では，ユーザ情報と，セキュリティ対象を直接ではなく，ロールを介して設定する．その効果として，組織，役職といったユーザ情報と，セキュリティ対象となるファイル，業務アプリケーションの変更管理を独立して行うことができる点があげられる．

標準的な RBAC である NIST(National Institute of Standards and Technology) の階層 RBAC [4] を図 2 に示す．階層 RBAC は以下の要素からなる．

- **ユーザ (USERS)**：人そのものが定義される．エージェント等擬似的なものへの拡張が可能である．
- **ロール (ROLES)**：組織，役職など，意味的な役割を示すグループが定義される．ロール階層を導入することにより，ロールの継承関係を定義することが可能である．
- **対象 (OBS)**：セキュリティで守るべきファイル，フォルダ等のデータの格納場所，プリンタ等のシステムリソースが定義される．
- **操作 (OPS)**：参照，編集，印刷など，対象に対して行われる操作が定義される．
- **許可 (PRMS)**：RBAC で保護される対象への操作の許可が定義される．対象と操作は，多対多の関係にある．
- **セッション (SESSIONS)**：ユーザとユーザに設定されたロールの部分集合とのマッピングが定義される．

RBAC では，図 2 に示すように，ユーザとロールとの関係であるユーザ設定：UA(User Assignment)，許可とロールとの関係である許可設定：PA(PermissionAssignment) から成る．図中，両矢印は多対多の関係を示す．ユーザは，各セッションにおいて，(1) 設定されているロールのいくつかを要求，(2) 要求されたロールが，要求時点で許されている場合は，そのロールを獲得，(3) ロールに関連づけられている許可にしたがったアクセス制御が行われる．

静的職責分掌 (SSD:Static Separation of Duty) は，ロールの集合と 2 以上の自然数の対から成り，ロールの集合から指定された個数以上のロール設定が許されないことを示す．動的職責分掌 (DSD:Dynamic Separationn of Duty) は，セッション内にて，活性化できるロールを動的に制限することを示す．

GRBAC(Generalized RBAC) では，ユーザ設定，許可設定を決定する条件として，RBAC における主体ロールに，対象ロール，環境ロールを加えて，アクセス仲介ルールを定めて一般化したものである [5]〜[7]．特に，環境ロールでは，たとえば，就業時間，休日，システム障害発生時，オフィス外のモバイル環境といった時間，場所のコンテキストを条件に加えることにより，企業活動に合わせたモデルを表現することが可能となった．

2.3　RBAC の企業情報システムへの拡張

2.3.1　階層型組織 RBAC

著者らは，[8] にて，図 3 に示すように人事情報にあたるユーザ，組織をロールから独立させた階層型組織 RBAC モデルと，その実装方式を示した．ユーザ設定，許可設定をルールで表現し，セッション開設時にルールを解釈して，活性化される Web アプリケーションのリストを出力する方式と，Web アプリケーション起動時にルールを解釈して，認可するか否かを出力する 2 種類の方式を提案した．性能評価の結果，いずれの場合も負荷が 5%以内で，実用上，問題ないことを示した．

2.3.2　企業向け RBAC

企業の IT 環境におけるすべてのシステムにおけるユーザとアクセス権の管理のために，ERBAC(Enterprise RBAC) モデルが提唱された [9]．複数ターゲットシステムでは，ロールは，

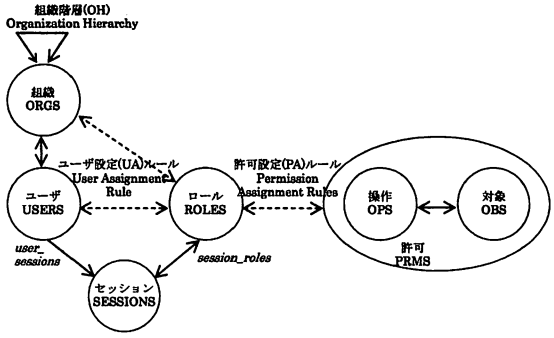

図 3 階層型組織 RBAC

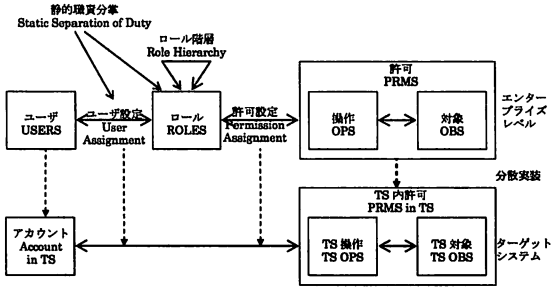

図 4 エンタープライズ RBAC

システム固有で多様な許可より構成される．図 4 に ERBAC モデルを示す．ロールへの設定を通してユーザに割り当てられた許可が，ターゲットシステムへ分散実装される．ターゲットシステムにおけるアカウントのロール定義に応じて決定された許可がターゲットシステムに伝えられる．

さらに，文献 [10] では，業務アプリケーションへの拡張を示した．企業におけるシステムのセキュリティ領域では，ユーザ，対象が大規模の場合においても，操作の数は限られている（たとえば，ファイルシステムにおいては，read, write, execute）．しかし，業務アプリケーションにおける操作は，業務ごとに定義される手続きとなり複雑度が上がる．その結果，認可決定の機構として，さらに次の制約が同時に満たされることが必要となる．

- 銀行のトランザクションシステムのようなクリティカルなアプリケーションでは，最適性能と可用性が求められる．
- コンプライアンス，組織のセキュリティポリシー遵守のため，有効な監査機能が必要である．

そこで，[9], [10] は，これらの相反する制約に対して，図 4 に示すような二層構造であるエンタープライズ RBAC モデル (ERBAC) を提唱した．認可設定を通して決定されたユーザが受理する認可が，ターゲットシステムに伝播される．

また，アクセス権の委譲，取消，アクセス制御の一貫性保持のため，ルールを用いる手法が提唱されている [11]〜[13].

2.3.3 課　　題

RBAC を企業情報システムに適用する場合，許可設定を実行時に解釈して認可判定を行うモデルと，2.3.2 節で示した ERBAC モデルのように，事前にユーザ設定，許可設定を解釈してターゲットシステムに分散実装させるモデルが併用される．前者については，[8] で示した．本稿では，後者 に注目する．まず，入退室管理装置のように，非 PC で，ユーザ認証機能を内蔵するターゲットシステムについて考察する．

- 低コストで，即時性が求められる．安価で能力の低い CPU が用いられることが多いため，ロールを定義したルールの実行時解釈は性能が問題となる．
- 設備系のネットワークと情報システムで用いられる基幹系ネットワークを直接接続することはセキュリティ上，許可されない場合がある．オフラインでの運用では，ユーザ情報の変更管理を即時に行うことは困難である．
- セキュリティ強化，利便性向上を考慮して，IC カードによるユーザ認証が広がっている．一方で，非携帯，紛失，盗難，破損の際の業務の継続，来訪者の対策が必要となる．

さらに，対象が業務アプリケーションの場合は，以下の課題があげられる．

- 操作は，業務アプリケーションごとに多様である．すなわち，対象の属性，操作の種類，許可設定が，業務に依存する．一方で，アカウント管理，ユーザ認証，ロール管理は，コスト，セキュリティ，統制の観点で，業務アプリケーションから独立させて共通化するほうが，運用面，安全性面で利点が大きい．
- 対象の属性に加えて，業務アプリケーションのみから参照可能な値自身によって認可決定を行うコンテンツベースアクセス制御が必要である．

さらに，2 章で述べたように，内部統制の観点から，個人を特定した監査ログを残すことが求められる．すなわち，予備カードを用いた認証・認可，ロールによる認可判定を行った場合においても，ユーザの特定とその行為の記録が必要とされる．

3. 仮想ユーザ RBAC にもとづくロール分散実装方式

本章では，RBAC に仮想ユーザを加えた VURBAC(Virtual User RBAC) モデルを提案し，その実現方式を示す．本実現方式は，IC カードの持つ固有の識別子を用いて，IC カードを所有するユーザを識別し，ユーザに設定されたロールに応じたアクセス権を与えるシステムを対象とする．ターゲットシステムとしてとして以下の 2 種類を仮定する．

(Type1) IC カードに格納された識別子に応じて許可を決定する．

(Type2) IC カードに格納されたロールに応じて許可を決定する．

IC カードの識別子，IC カードに格納されたロールの取り出しは，PIN 認証，バイオ認証等，IC カードの持つ機能を用いるものとする．また，監査のため，行為の実施の結果は，IC カードの持つ固有の識別子，対象，操作を含むログとして出力するものとする．

3.1 非 PC システムのための VURBAC モデル

2 章で示した事前にユーザ設定，許可設定を解釈してターゲットシステムに分散実装する VURBAC モデルを示す．2.3.3 節

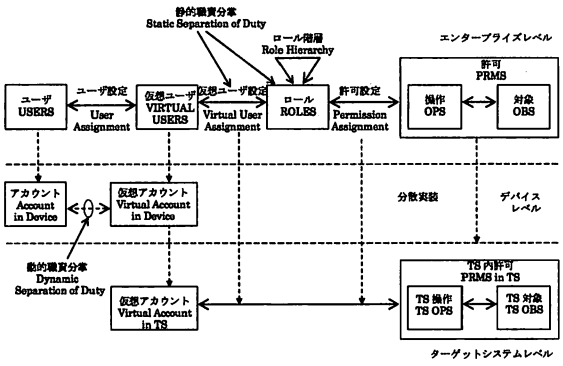

図 5　非 PC システムのための VURBAC モデル

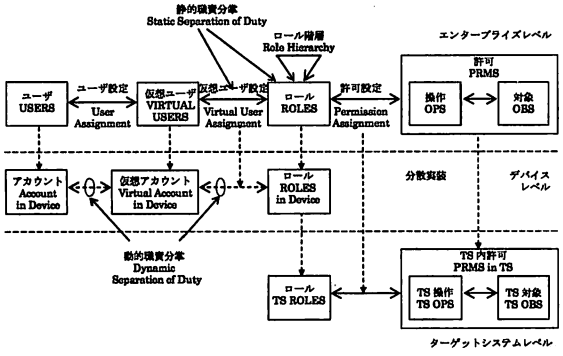

図 6　業務アプリケーションのための VURBAC モデル

で示した課題を解決するため，実システムでは，通常，あらかじめユーザを特定しない IC カードを事前に準備して，システムに登録する方式がとられることが多い．これまでの RBAC では，ユーザ設定が固定のため，このような事前に準備したカードを明に表現することができなかった．そこで，図 5 に示すように，ユーザとロールの間に，仮想ユーザを置いて，事前に準備してシステムに登録する部分と，その後，実ユーザに設定する部分を分離したモデルを提案する．

- **仮想ユーザの分散実装：** ロール側の視点では，仮想ユーザをユーザとして捉え，ユーザ設定，許可設定を ERBAC と同様に解釈して，ユーザと許可を直接の対応付けに変換し，ターゲットシステムへ分散実装する．
- **ユーザへの仮想ユーザの設定：** ユーザへ仮想ユーザの設定を行う．たとえば，来訪者に対して，規則にしたがって受付がカードを手渡す行為がこれにあたる．
- **仮想ユーザのアクセス制御：** ターゲットシステムは，実ユーザと同様に仮想ユーザの持つ IC カードに基いてアクセス制御を行う．

3.2　業務アプリケーションのための VURBAC モデル

前節で示した方式では，ロールの種類に応じた IC カードを準備する必要がある．たとえば，入退室管理システムでは，紛失・非携帯用予備カード，社内出張者カード，来訪者カード等，種類が限られる場合は，有効である．しかし，2.3.3 節で示した業務アプリケーションでは，多様な許可に対応する必要がある．そこで，図 6 に示すように，仮想ユーザではなく，ロールを分散実装するモデルを提案する．

- **ロールの分散実装：** 許可設定のみを解釈してターゲットシステムへ分散実装する．
- **ユーザへの仮想ユーザの設定：** ユーザへ仮想ユーザの設定を行う．
- **カードへのロールの設定：** ユーザの属性情報を解釈してロールを定め，カードへ設定する．
- **仮想ユーザのアクセス制御：** ターゲットシステムは，IC カードに設定されたロールに基いてアクセス制御を行う．さらに，セキュリティレベルに応じて，カードの失効リストの確認，仮想ユーザの ID を付加したログの出力を行う．

近年，多目的カードとして，上述の Type1, Type2 を 1 枚のカードに実現する例が増加している．その際，Type1 で準備したカードに，Type2 の情報を付加する運用が取られる．

一方で，仮想ユーザを導入することにより，以下に示す新たな課題が生じる．

- 実ユーザと仮想ユーザ間の動的職責分掌の制約を定め，それに則った確実な仮想ユーザの設定が必要となる．たとえば，予備カード発行時の紛失カードの確実な失効といった制約がそれにあたる．
- 内部統制で求められる行為実施者を特定した監査証跡のためには，仮想ユーザではなく，実ユーザを付加したログが必要とされる．

4.　IC カード運用管理への適用

4.1　VURBAC モデルにおける仮想ユーザの設定

VURBAC モデルを適用する際に課題となる仮想ユーザの設定方式について示す．実ユーザと仮想ユーザの設定に関する制約として定義される．たとえば，職責分掌の観点から，「ロールの実行が可能な IC カードは 1 枚に限る」という制約に対して，予備カードの貸し出しを行う場合に，以下の操作を不可分で実行することが必要となる．

- 本人のロールに相当する予備カードの選択
- 予備カードの有効化
- 本カードの無効化

これらの実装には，(1) IC カード，ユーザのコンテキスト管理，(2) カードごとの状態遷移の規定，(3) カード間で可能な状態の組み合わせに強制的に遷移させる操作が必要となる．本章では，(3) の複数カード間の同期方法を特長とする仮想ユーザの実装方式を示す．

図 7 に，ロールが設定された仮想ユーザ＝ IC カードの状態遷移図と，運用ルールを示す．状態遷移を契機として起動されるルールとして，指定した他のカードの状態を強制的に遷移させる状態連携ルールを新たに導入して，同期をとることとした．

図 8 に，データ管理も含めた全体構成図を示す．VURBAC モデルにもとづき，実ユーザ，仮想ユーザ，およびそれらの関係を保持するテーブル「ユーザ-仮想ユーザ設定」から成る．従来，IC カードに代表される認証デバイスは，ユーザの所有物

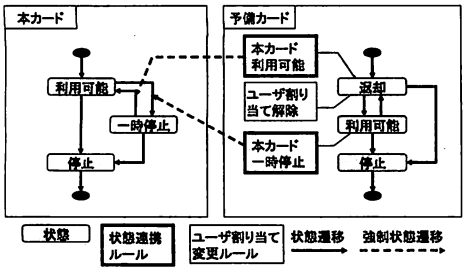

図 7 IC カードの状態遷移図

のように，ユーザの属性のひとつとして扱われていたものを，モデル上，独立させた．その利点を以下に示す．

- ユーザを特定しない IC カードの存在を導入した結果，ユーザ–仮想ユーザ設定の情報は，リアルタイムでターゲットシステムに反映することができないシステムを明に表現することが可能となった．
- ターゲットシステムに反映されない設定変更情報を，5 章で示す監査を目的とした履歴として，実ユーザの属性と独立して管理可能とした．

これらのテーブルの一貫性制御のため，コンテキスト収集，状態遷移チェック，ルール自動実行を行う．これらの構成要素を用いた実ユーザと複数仮想ユーザの設定の同期方式を，手続き 4.1 に示す．

手続 4.1：実ユーザと複数仮想ユーザの設定の同期方式

(1) ユーザ，カードのコンテキスト収集を行う．具体的には，画面からの入力，カード情報の読み込みを行う．

(2) 収集したコンテキストと状態遷移図により状態管理テーブルの該当項目を新しい状態に移す．

(3) 新しい状態に合致するルールを選択する．

(4) ルールで指定されたアクションをすべて実行する．

(4-1) アクションが状態連携ルールの場合，(2) 以降を実行する．

(4-2) アクションがユーザ設定変更ルールの場合，テーブル「ユーザ–仮想ユーザ設定」を更新する．更新する際は，設定開始時の時刻印 (BeginTS)，および設定終了時の時刻印 (EndTS) を更新する．

本方式は以下の特長を持つ．

- 複数 IC カード状態の同期による自動運用

IC カードの状態が変化した場合に，他の IC カード状態や，ユーザへの設定解除を自動的に行い，人為的誤りを除くことが可能である．

- セキュリティポリシーとアクションの分離

セキュリティポリシーをルールとして設定する管理者とアクションを記述する開発担当者を分離した結果，セキュリティポリシーの変更対応，およびポリシーが異なる部門への適用の効率化が可能である．

4.2 GRBAC との関係

GRBAC [5]〜[7] では，主体ロール，対象ロール，環境ロールを組み合わせたアクセス制御モデルを提唱している．本稿で示した VURBAC との関係を以下に示す．

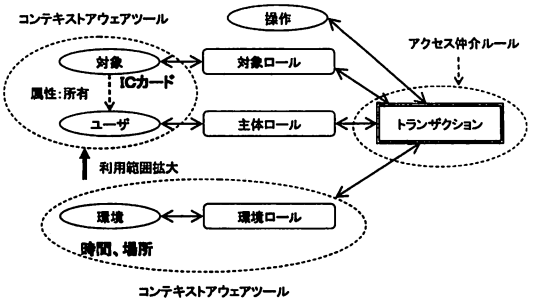

図 9 GRBAC との関係

- **主体ロール**

オリジナルの RBAC, GRBAC と同様に，ユーザの属性である組織，役職をもとに，ロールを決定する．

- **対象ロール**

本稿で提唱した仮想ユーザ設定は，GRBAC 上，図 9 に示すように，対象ロールのひとつの実装方式と解釈することができる．IC カードに代表される認証デバイスにあらかじめロールを設定し，それを主体の属性として扱うことができる．

- **環境ロール**

本稿で示した実ユーザへの仮想ユーザの設定は，セッション開始時の条件として，IC カードの状態，場所（オフィス内，出張先等），時間（就業時間，休日等）といった環境が重要な条件となる．このような，環境を観測してその状態によって判断を行う場合に利用されるコンテキストアウェアツールを，図 9 に示すように，特に課題となる実ユーザと仮想ユーザの設定に関する制約を遵守するための具体的実装方式に適用した．

すなわち，VURBAC では，主体と対象の間に生じる所属の関係といった動的に変化する主体の属性を環境ロールと同様にコンテキストとして観測するように，GRBAC モデルを一般化した．

5. 監査ログ

図 5，図 6 で示した VURBAC モデルを採用したターゲットシステムでは，仮想ユーザ ID で行為のログが記録されるため，個人の特定ができない課題が生じる．本章では，図 8 で示したテーブル「ユーザ–仮想ユーザ設定」を利用したユーザ特定方式を示す．手続 4.1 によって，本テーブルは多バージョン管理されており，以下に示す手続 5.1 により，監査を行うことが可能となる．

手続 5.1：実ユーザと複数仮想ユーザの設定の同期方式

入力：監査ログ，ユーザ–仮想ユーザ設定テーブル

出力：インシデントリストファイル，実ユーザ ID 付ポリシー合致ログファイル

(1) 監査を行うターゲットシステム，および，期間を指定する．

(2) 指定されたターゲットシステム，期間の条件に合うログを，監査ログから選択する．

(3) (2) で選択された各行に対して以下の操作を行う．

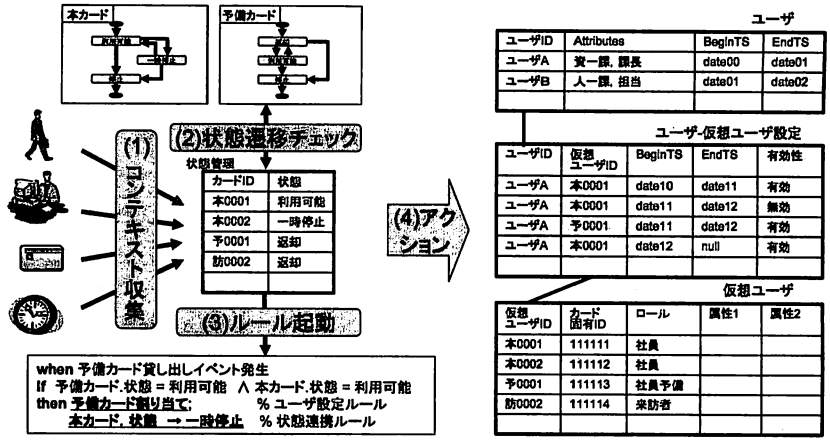

図 8 IC カードの運用管理構成図

(3-1) 仮想ユーザ ID が一致し，$BeginTS \leqq Timestamp < EndTS$ を満足する行をユーザ-仮想ユーザ設定テーブルから選択する．

(3-2) 該当する行が 1 行でかつ属性有効性が“有効”の場合は，ポリシー合致としており，ユーザ ID の値を加えて，出力する．

(3-3) 以下の場合は，ポリシーに合致しないため，インシデントとして出力する．

- 該当する行がない．
- 該当する行が複数ある．
- 該当する行の属性有効性が“無効”である．

ターゲットシステムへの反映が 1 回／日程度と想定したシステムで，本稿で提案した仮想ユーザによる実装を行った場合，運用コスト削減の効果がある反面，システム上，以下のセキュリティリスクが発生する．

- 運用の問題で予備カードの流出が発生した場合，主体が特定できないまま，ターゲットシステムで利用可能
- 本カードを予備カードに切り替えた際，テーブル「ユーザ-仮想ユーザ設定」上は，本カードが“無効”となるが，ターゲットシステムでは，次回のシステム反映まで利用可能

手続 5.1 の出力であるインシデントリストファイル内に，これらの事象を発見することが可能である．

6. あとがき

本研究では，アクセス制御モデルとして一般的である RBAC を，入退室管理装置，キャビネットといった物理セキュリティ，IC カードに代表されるデバイスを含む企業情報セキュリティへ適用する場合のモデルを示した．本研究で提案した仮想ユーザを付加した RBAC モデルでは，運用，セキュリティの問題で更新頻度の少ないシステムに対して，変更管理を局所化することを可能とした．また，仮想ユーザを導入することによって新たに生じる実ユーザと仮想ユーザの設定制約の自動化，実ユーザを用いたログの監査の実現方式を示した．これらの方式は，一般の動的職責分掌のセッション設定，ログ監査のためのアイデンティティの変更履歴管理に応用することが可能である．

今後は，一般の業務アプリケーションを含む対象の範囲拡大，対象の属性利用を図るとともに，モデルの形式的定義を行う必要があると考えている．

文　献

[1] 近藤, 鶴川, アイデンティティライフサイクル管理技術, 三菱電機技報, Vol.80 No.10, 2006.

[2] IT Governance Institute, COBIT 4.0, 2006.

[3] Feraiolo,D. and Kuhn,R., Role-Based Access Control, Communications of the 15th NIST-NSA National Computer Security Conference, 1992.

[4] Ferraiolo,D., Sandhu,R., Gavrila,S., and Kuhn,R., Proposed NIST standard for Role-Based Access Control, ACM Transaction on Information and System Security, Vol.4 No.3, 2001.

[5] Moyer,M. and Ahamad,M. Generalized Role-Based Access Control. In Proceedings of the 2001 International Conference on Distributed Computing Systems(ICDCS), Mesa, AZ, 2001.

[6] Convington,M., Moyer,M., and Ahamad,M. Generalized role-based access control for securing future applications. In Proceedings of the National Infomation Systems Security Conference (NISSC), October 2000.

[7] Hulsebosch,R., Salden.A, Bargh,M., Ebben,P. and Reitsma,J. Context Sensitive Access Control SACMAT'05, June 2005.

[8] 近藤, 白木, 大沼, 小宮, 五月女, 虎渡, ロールベースアクセス制御情報の多バージョン並行処理制御を利用した監査ログトラッキング手法, 情報処理学会論文誌：データベース, Vol.44 No.SIG 12 (TOD28), 2005.

[9] Kern,A., Kuhlmann,M., Schaad,A., and Moffett,J., Observations on the role life-cycle in the context of enterprise security management, SACMAT'02, June, 2002.

[10] Kern,A., Kuhlmann,M., Kuropka,R., and Ruthert,A., A meta model for authorisations in application security systems and their integation into RBAC administration, SACMAT'04, June, 2004.

[11] Kern,A. and Walhorn,C., Rule support for role-based access control, SACMAT'05, June, 2005.

[12] Zhang,L., Ahn,G., and Chu,B. A rule-based framework for role-based delegation and revocation ACM Transactions on Information and system security (TISSEC), 2003.

[13] Byun,J., Soh,Y., and Bertino,E. Systematic Control and Management of Data Integrity, SACMAT'06, June 2006.