1F-3

カード毎の状態遷移と複数の IC カード間の状態連携ルールを用いた IC カード運用管理の構築

山田　耕一　小宮　崇　山足　光義　近藤　誠一
三菱電機(株) 情報技術総合研究所

1. はじめに

近年，入退出や PC へログオンでの利用者本人の確認手段として，IC カードを利用した社員証，職員証等を用いるケースが増大している．しかし，紛失，破損等に備えて，本カード，予備カード等複数の IC カードを切り替えるといった，カード間の状態同期を行うためには，手動で操作を行う必要があった．本稿では，状態遷移図と状態連携ルールを組み合わせ，そのルールを状態遷移イベントにより起動することでカード間の状態同期を実現した IC カード運用管理システムの設計と実装について報告する．

2. 既存 IC カード運用管理システム

2.1. IC カード運用管理の動向

IC カード運用管理システムでは，利用者や IC カードの状態(運用中，一時停止，破棄等)の管理が必要となる．この状態遷移をソフトウェアプロセスやワークフロー[1]の状態遷移と同様に扱うことで，処理の流れや状態遷移をルールや状態遷移図として独立して定義することが可能である．そのため，システムの変更時にはルールと状態遷移図を変更するだけでよく，プログラムを修正する必要はない．

2.2. 課題

既存の IC カード運用管理システムでは，個々の IC カードの状態遷移は扱うことが可能であるが，本カード，予備カード等複数の IC カードを使用する場合，IC カード間の状態同期には手動操作が必要という課題がある．図 1 に状態遷移図を用いた IC カード運用管理の実装例を示す．IC カード運用管理システムは，複数カード(本カード，予備カード等)のそれぞれの状態を管理するプロセス監視機能がある．管理情報データベースはユーザ情報と，ユーザが所有するカード情報を保有する．各カード状態は相互関係なく遷移するためカード間の状態同期を行うには，手動操作が必要となる．そのため，操作誤りなどにより状態の不整合が発生し，安全性が損なわれる可能性がある．

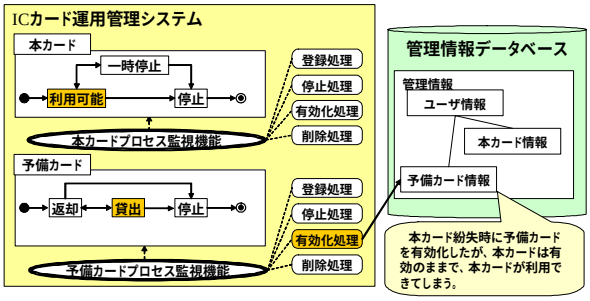

図 1．IC カード運用システム

このような課題に対応するためは，複数の IC カード間の状態連携を行う必要がある．複数の状態遷移を同期させるための手法として，プログラムでの実現，積オートマトン[2] による状態遷移図の融合，状態遷移をルールとして記述する言語である STR (State Transition Rules)[3] などが提唱されている．プログラムでの実装の場合は，状態遷移図が変更される毎にプログラムを修正する必要が生じる．積オートマトンは，複数の状態遷移を組み合わせ 1 つの状態遷移を作る手法である．状態数 n の状態遷移図 A と状態数 m の状態遷移図 B を単純に組み合わせると，状態数 n×m の状態数を持つ状態遷移図が生成される．その中からシステムとして正しい状態のみを選択して求める状態遷移図を作成する．このため，カード種類に対して同期すべき組み合わせが指数的に増加し，正しい状態の選択が困難となるという問題がある．また，STR は遷移前状態とイベントをルールで表現する．このルールは，

ルール：前条件[イベント]後条件

という形式で表現するため，ルールの羅列となり，状態遷移を視覚的に捉えにくいという問題がある．

3. IC カード運用管理システムの概要

3.1. IC カードの状態遷移と IC カード運用ルール

2 章の課題を解決するため，状態遷移図とルールを組み合わせる手法を提案する．本方式では，状態遷移図の記述方式として，処理の流れを表現する UML のアクティビティ図を採用した．ア

Development of smartcard management system which using smartcard state flow and smartcard state cooperate rules.
Kouichi Yamada, Takashi Komiya, Mitsuyoshi Yamatari, Seiichi Kondo
Information Technology R&D Center, Mitsubishi Electric Corporation

クティビティを状態として扱い，矢印の向きに状態遷移可能とする．初期状態は開始点から矢印で結ばれた状態である．IC カードの運用を行うための，IC カード運用ルールは，各状態のタグとして定義する．IC カード運用ルールには以下の 2 種類がある．

・状態連携ルール
「カード名.状態名」という形式で表現する．ルールが存在する状態へ遷移したときに，カード名に該当するカードの状態を，状態名へと遷移させる．

・ユーザ割り当て変更ルール
ルールが存在する状態へ遷移したときに，カードのユーザ割り当てを設定または解除する．

状態遷移図と IC カード運用ルールを用いて，IC カード運用セキュリティポリシーを記述する．図 2 に例を示す．

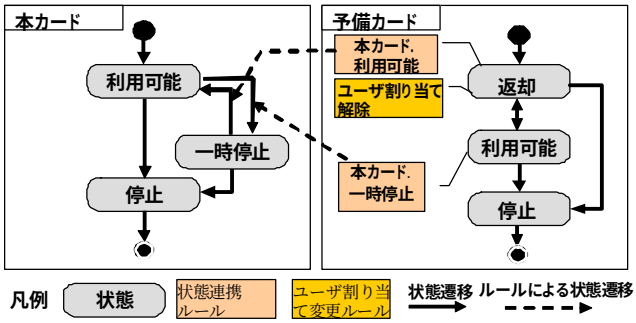

図 2 複数 IC カードの状態遷移図

図 2 では，「本カードは，予備カードが利用可能になると，自動的に一時停止する」というセキュリティポリシーを表現するため，予備カードの「利用可能」状態に，「本カード.一時停止」の状態連携ルールを記述している．

3.2. 状態遷移イベントによるルールの駆動

本方式では IC カード運用ルールは IC カードの状態遷移をトリガとして起動する．そのため，状態遷移をイベントとするイベント駆動ルールエンジンで実装した．図 3 に構成図を示す．

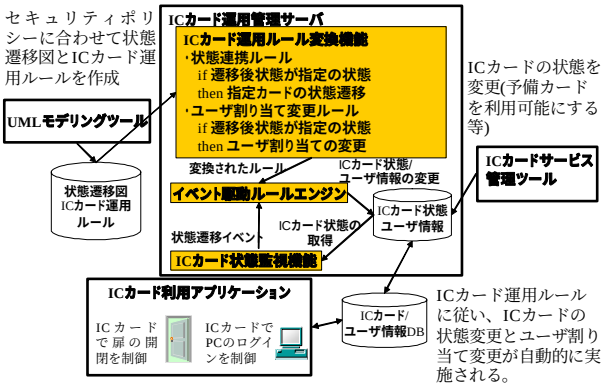

図 3.IC カード運用管理構成図

UML モデリングツールで作成した状態遷移図を IC カード運用管理サーバが読み込み，IC カード運用ルール変換機能が，状態遷移図のタグに記述されている IC カード運用ルールをイベント駆動ルールエンジンのルール形式へ変換する．IC カードの状態が変化すると，IC カード状態監視機能が状態遷移イベントを発生し，イベント駆動ルールエンジンがルールを実行する．ルールの実行結果による状態遷移もイベントとして扱うため，状態連携ルールを連鎖的に適用することが可能である．イベント駆動ルールエンジンを使用することにより，IC カード運用ルールを統一して動作させることが可能となった．

4. 効果

以上の機能を開発したことにより，本システムは以下の効果を持つ．

・複数 IC カード状態の同期による自動運用
状態遷移図に状態連携ルールを持たせることにより，IC カードの状態が変化した場合に，他の IC カード状態や，ユーザへの割り当て解除を自動的に行うことが可能である．

・処理とセキュリティポリシーの分離
IC カード運用管理システムへの入出力はプログラムで記述し，セキュリティポリシーは状態遷移図と状態連携ルールとして記述するため，処理を記述する開発担当者とセキュリティポリシーを設定する管理者の開発の分離，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が可能である．

5. おわりに

状態遷移図に IC カード運用ルールを持たせることで，複数の IC カード間の状態同期とユーザ割り当て変更を実現する方式について報告した．今後は状態連携ルールに，IC カードに対する処理を起動させるルールを追加するなど，システム自動化による安全性の追求を進めていきたい．

参考文献

[1] 「ここまで来たワークフロー管理システム」3. ワークフロー製品の実際 (速水 治夫 他) 情報処理学会誌 (学術雑誌, 1999) 40/5,507-513

[2] 竹村司 他，“ビジネスオブジェクトの状態遷移に基づくビジネスプロセスの導出”，日本ソフトウェア科学会第 22 回大会

[3] Y. Hirakawa et al., “Telecommunication Service Description Using State Transition Rules”, Proceedings of the Sixth International Workshop on Software Specification and Design, Oct. 1991.