M-027

プロトコル変更可能なマルチアプリケーション IC カードシステム
Multi-application Smart Card System with Protocol Change Function

内山 宏樹† 梅澤 克之† 洲崎 誠一†
Hiroki Uchiyama Katsuyuki Umezawa Seiichi Susaki

1. はじめに

近年，携帯電話，情報家電，ゲーム機や非接触 IC カード等の普及にともない，個人が利用する電子機器が様々な形で外部のネットワークと接続されるユビキタス環境がますます進展しつつある．このようなユビキタス環境では，多種多様な端末やネットワークが利用されるため，利用環境に応じた「安全」の提供が必要となる．例えば，電子決済のような高度なセキュリティが要求されるサービスや，IC 乗車券のような迅速な認証が要求されるサービスなど，提供されるサービスによって様々なレベルのセキュリティが必要となる．

また，実サービスの開始後にサービスが利用している認証方式等に脆弱性が発見される場合がある．例えば，SSL のセキュリティプロトコルが用いる暗号アルゴリズム（RSA 暗号モード）において，脆弱性の発見に伴い仕様変更が実施された事例がある．このような背景から，更新が容易には実施できないプロトコルを迅速に更新する技術の開発が急務となっている．

本研究では，利用可能なリソースなどに制約がある IC カードに適用可能なセキュリティプロトコルモジュール（以降，「プロトコルモジュール」と呼ぶ）の動的生成技術を研究している．具体的には，様々なサービスのセキュリティレベルに対応するために短時間で動的にプロトコルを更新する技術として，IC カード内部でプロトコルをカスタマイズする「内部カスタマイズ方式」と，アルゴリズムやプロトコルの危殆化に迅速に対応するための技術として，IC カード外部でカスタマイズしたプロトコルモジュールを安全に IC カード内のプロトコルモジュールと置換する「外部カスタマイズ方式」に関して研究を推進している．

上記の方式のうち，外部カスタマイズ方式を実現することにより，IC カードのプロトコルをカスタマイズする上で必要となる処理量を大幅に削減でき，アルゴリズムやプロトコルの脆弱性への迅速な対応が可能になる．また，長期的な視点でみると，プロトコルモジュールの開発コスト削減も可能となると考えられる．ところが，外部カスタマイズ方式は，プロトコルモジュールの自動生成に伴うプログラムサイズやプロトコルの実行時間の増大が予想され，実用可能レベルであるかどうかは不確かであった．

本稿では，外部カスタマイズ方式に関して検討し，その実用性を評価した結果を示す．

以下では，まず，2 章で提案する外部カスタマイズ方式に関して記述する．3 章でその方式の評価を行い，実用性の評価を実施する．最後に 4 章でまとめと今後の課題を示す．

† （株）日立製作所 システム開発研究所
Hitachi, Ltd., Systems Development Laboratory

2. 外部カスタマイズ方式

2.1 従来技術の課題

従来，IC カードに実装されているプロトコルを更新する場合には，（1）IC カードの回収，（2）更新用プロトコルの設計，（3）プロトコルモジュールの生成，（4）プロトコルモジュールの搭載，といった一連の流れを人手により行う必要があり，非常に時間とコストがかかっていた．また，マルチアプリケーション IC カードには，カードアプリケーション（以降，AP）やカードのステータス等を管理するために複数のスキームが存在するため，プロトコルモジュールの更新時には両者のスキームを意識して実装しなければならないという問題点があった（代表的なスキームとして，GlobalPlatform[3]や MULTOS[4]などが挙げられる）．

2.2 提案方式

（1）概要

図 1 に本研究で提案する外部カスタマイズ方式の概要を示す．

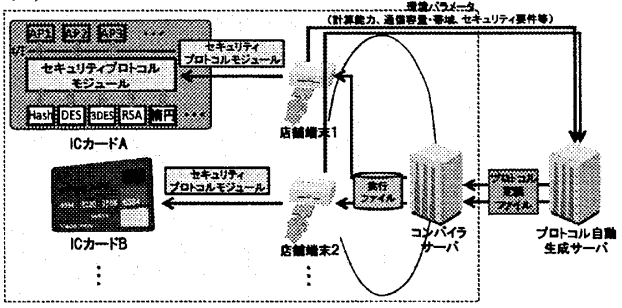

図 1：外部カスタマイズ方式概要

提案する外部カスタマイズ方式は，清本ら[5]により提案されたプロトコル自動生成技術が組み込まれたプロトコル自動生成サーバと連携して動作するものである．具体的には図 1 の点線で囲まれた部分であり，コンパイラサーバ，店舗端末，IC カードから構成される．プロトコル自動生成サーバは，店舗端末から，サービスの要件等を記載した“環境パラメータ”を取得し，そのパラメータに応じて，IC カードの種類に依存しないプロトコル定義ファイル（XML 形式）を出力する．次に，コンパイラサーバは，プロトコル自動生成サーバからプロトコル定義ファイルを取得し，実行ファイルに変換する．変換した実行ファイルを各店舗端末に配信し，プロトコルモジュールとして GlobalPlatform や MULTOS スキームの IC カードに搭載されているプロトコルモジュールと置き換える．

本研究では，本提案方式を実現するためにコンパイラサーバに実装する外部コンパイラと店舗端末に実装する

マルチ IC カード AP ローダを開発した．以降では開発した各機能について示す．

（2）外部コンパイラ

外部コンパイラは，XML で記述されたプロトコル定義ファイルを読み込み，GlobalPlatform や MULTOS スキームの仕様に準拠した Java Card のソースコードを出力する．次に，ソースコードをコンパイルし，クラスファイルを生成する．最後に，クラスファイルを IC カードに搭載可能な実行モジュールに変換し出力する．

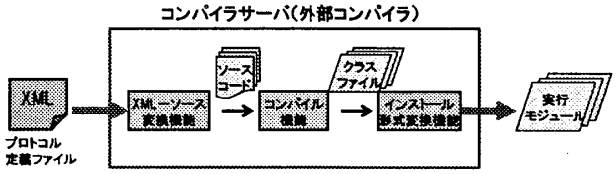

図 2：外部コンパイラ

（3）マルチ IC カード AP ローダ

マルチ IC カード AP ローダは，店舗端末に挿入されている IC カードの種類（GlobalPlatform カード／MULTOS カード）を識別する．次に，外部コンパイラで生成された実行モジュールを読み込む．最後に，IC カードに対して，取得したカード情報を基に実行モジュールの搭載・削除コマンドを発行し，プロトコルのカスタマイズを行う．

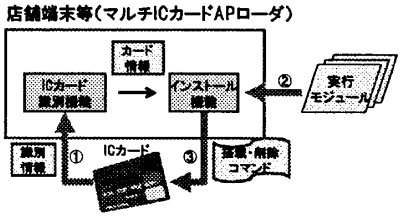

図 3：マルチ IC カード AP ローダ

3. 提案方式の評価

3.1 評価フロー

提案方式の評価には，図 4 に示すチャレンジアンドレスポンス認証方式のプロトコルを利用した．

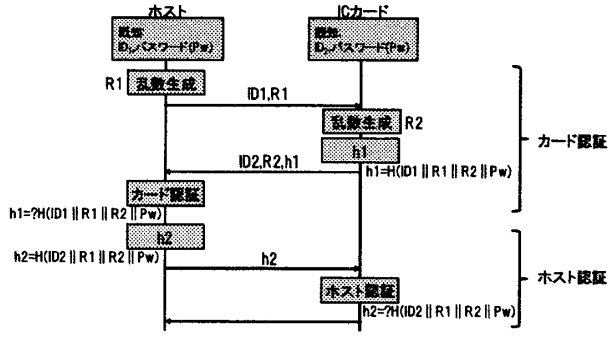

図 4：評価フロー

3.2 評価結果

図 4 に示すフローを実現するプロトコルモジュールを人手により実装した場合を従来方式とし，外部カスタマイズ方式を利用して実装した場合を提案方式として，容量，処理時間を評価した．結果を表 1 に示す．

表 1：外部カスタマイズ方式評価結果

スキーム	方式	容量 (byte)	実行時間(sec)		
			カード認証	ホスト認証	計
MULTOS	従来	2,531	0.521	0.251	0.772
	提案	4,301	0.787	0.369	1.156
	増加率	1.70	1.51	1.47	1.50
Global Platform	従来	3,029	0.179	0.109	0.288
	提案	3,758	0.267	0.138	0.405
	増加率	1.24	1.49	1.27	1.41

この結果，外部カスタマイズ方式を適用し複数のスキームの IC カードに対して，セキュリティプロトコルの動的なカスタマイズを実現し，人手による処理量を大幅に削減した場合でも，容量は 1.7 倍，処理時間は 1.5 倍程度の増加で収まっていることがわかる．これにより，外部カスタマイズ方式の実用性が示されたということができる．

4. まとめと今後の課題

本稿では，提案する IC カード向けプロトコルカスタマイズ方式とその評価に関して記述した．提案方式を適用することにより，従来のように人手を介さずに，プロトコルモジュールを高速に置換することが可能となった．また，提案方式を用いて生成したプロトコルモジュールの容量・処理時間は，許容範囲内に抑えられていることが確認できた．

今後は，外部カスタマイズ方式の検討・実装により得られた知見を用いて，内部カスタマイズ方式に関する検討を推進し，実装・評価を実施する予定である．

謝辞

本研究は，独立行政法人情報通信研究機構（NICT）の委託研究「ユビキタスネットワークにおける環境に応じたセキュリティプロトコルの自動生成・カスタマイズ技術に関する研究」の一環として行なわれた．

参考文献

[1] 内山, 梅澤, 小林, “プロトコル変更可能なマルチアプリケーション IC カードシステムの検討,” 第 36 回コンピュータセキュリティ研究会予稿集, p.p 135-140, 2007 年 3 月

[2] 内山, 梅澤, 洲崎, “セキュリティプロトコルの自動生成・カスタマイズ技術に関する研究開発 III～プロトコル変更可能なマルチアプリケーション IC カードシステムの開発と評価,” コンピュータセキュリティシンポジウム 2007 予稿集, 3B-3, 2007 年 11 月

[3] “GlobalPlatform Card Specification Verison 2.2,” GlobalPlatform Inc., 2006 年 3 月

[4] “MULTOS カード発行ガイド,” マルトス推進協議会, 2003 年 3 月

[5] 清本, 太田, 田中, “セキュリティプロトコル自動生成手法の検討,” 情報処理学会第69回全国大会予稿集, 2007年3月