論　文

セキュリティプロトコルのカスタマイズ技術を適用したICカードサービスシステムの開発と評価

内山　宏樹[†,††]　　梅澤　克之[†]　　洲崎　誠一[†]

Development and Evaluation of the System of Smart Card Service Applied the Customization Technology of Security Protocol

Hiroki UCHIYAMA[†,††], Katsuyuki UMEZAWA[†], and Seiichi SUSAKI[†]

あらまし　今後拡大するユビキタス環境においては，セキュリティ要件の変化やセキュリティプロトコルやアルゴリズムの脆弱性の発見に伴い，プロトコルの迅速な更新が求められることが予想される．このような要求を満たすために，ユーザが享受するサービスのセキュリティ要件，脆弱性情報，ネットワークやシステムの環境情報等から，動的にセキュリティプロトコルを生成し，ICカードのセキュリティプロトコルをカスタマイズする技術を提案した．本論文では，提案したカスタマイズ技術を組み込んで開発したより実サービスに近いICカードサービスシステムの概要とその評価結果を示す．

キーワード　セキュリティプロトコル，ICカード，カスタマイズ，ユビキタス

1. まえがき

近年，携帯電話，情報家電，ネットワーク対応ゲーム機等の普及に伴い，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利用す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，セキュリティ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．

このような課題に対し，筆者らはCPU周波数がたかだか数MHzであり，メモリ容量が数十kByte程度しか搭載されていないICカードに適用可能なセキュリティプロトコルの動的なカスタマイズ技術として，ICカード外部でセキュリティプロトコルをカスタマイズする技術及びICカード内部でセキュリティプロトコルをカスタマイズする技術を提案した[3], [4]．その結果，セキュリティプロトコルの動的なカスタマイズを実現する見通しを得ることができた．

本論文では，提案したセキュリティプロトコルのカスタマイズ技術を組み込んだより実サービスに近いICカードサービスシステムの概要及び評価結果に関して示す．以下では，まず，**2.** で従来技術として既に提案済のICカードの内部構成及びセキュリティプロトコルのカスタマイズ技術について記述する．**3.** で提案したセキュリティプロトコルのカスタマイズ技術を組み込んで開発したICカードサービスシステムについて記述し，**4.** で開発したシステムの評価を行う．最後に**5.** でむすびとして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，横浜市
Systems Development Laboratory, Hitachi, Ltd., 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, 244–0817 Japan
†† 京都大学大学院情報学研究科，京都市
Graduate School of Informatics, Kyoto University, 36–1 Yoshida-honmachi, Sakyo-ku, Kyoto-shi, 606–8501 Japan

表 1　セキュリティプロトコルカスタマイズ方式の比較
Table 1　Comparison of security protocol customization method.

方式	外部カスタマイズ方式	内部カスタマイズ方式
特徴	プロトコル定義ファイルを IC カード外部でコンパイルし，生成した SPM を IC カード内部の SPM と置き換えることによりカスタマイズを実現する	プロトコル定義ファイルを IC カード内部に格納されている SPM で逐次解釈して実行することによりカスタマイズを実現する
利点	短時間でのセキュリティプロトコルの実行処理が要求される場合に有効	短時間でのセキュリティプロトコルのカスタマイズ処理が要求される場合に有効
欠点	セキュリティプロトコルのカスタマイズ処理に時間を要する	セキュリティプロトコルの実行処理に時間を要する
適用例	ETC 環境などカード挿入時と利用時のタイミングに違いがあり，カスタマイズ処理時間よりも短時間での実行処理が要求される場合	セキュリティプロトコルはほぼ同様で鍵やアルゴリズムの一部を変更する際など変更範囲が軽微である場合

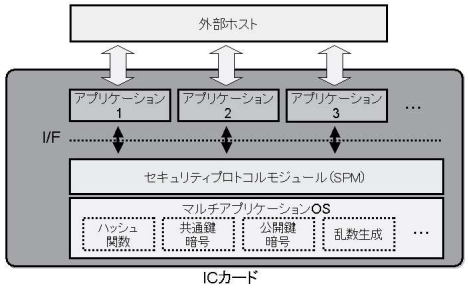

図 1　IC カード内の構成
Fig. 1　Architecture in the smart card.

2. 従来技術

筆者らは，IC カードのセキュリティプロトコル(注1)をカスタマイズするために，まず，カスタマイズに適した IC カードの内部構成を提案した．また，提案した内部構成を用いてセキュリティプロトコルをカスタマイズする技術として，IC カード外部でプロトコルをカスタマイズする技術（以降，「外部カスタマイズ方式」と呼ぶ）と，IC カード内部でプロトコルをカスタマイズする技術（以降，「内部カスタマイズ方式」と呼ぶ）を提案した [3], [4]．これらの技術は表 1 に示すように異なる特徴が存在するため，状況に応じて両者を使い分けることが必要となる．本章ではこれらの技術に関して示す．

2.1　IC カードの内部構成

筆者らは，図 1 に示すセキュリティプロトコルモジュール（以降，SPM と記述する）を IC カード内のアプリケーションと OS の間のミドルウェアとして配置する構成を提案した．SPM は OS に実装されている暗号アルゴリズム等を利用したセキュリティプロトコルの実行と，上位アプリケーションに対するアクセスインタフェースの提供を行う．上位アプリケーションは外部ホストから受信したセキュリティプロトコルコマンドを SPM に転送し，SPM 内で実行したセキュリティプロトコルの実行結果を外部ホストに送信し，認証や鍵交換を実現する．IC カード内をこのような構成にすることにより，セキュリティプロトコル機能を各アプリケーション内に実装する必要がなくなるため，IC カード内のメモリ使用量を削減することが可能となった．また，SPM の置換えや動作変更を実施することにより，セキュリティプロトコルの動的なカスタマイズが実現可能となった．このような構成は，アプリケーションの代わりにセキュリティプロトコルを実現するという意味では GlobalPlatform 仕様 [1] の Security Domain と同様であるが，Security Domain はプロトコルをカスタマイズすることはできなかった．また，プロトコルのカスタマイズは複数の SPM を IC カード内に搭載し，必要に応じて使い分けることによっても実現可能であるが，様々なアプリケーションが搭載される IC カードの場合，要求されるセキュリティプロトコルのパターンが無数に存在するため，メモリ容量に制限がある IC カードには適用が困難であった．

2.2　外部カスタマイズ方式

外部カスタマイズ方式は，清本ら [5] により提案されたセキュリティプロトコルの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及び太田ら [6] により提案されたセキュリティプロトコルの高速検証技術が組み込まれたプロトコル高速検証サーバと連携して動作するものである．具体的には図 2 の点線で囲まれた部分であり，コンパイラサーバ，コンビニエンスストアのレジ端末やクレジット決済端末などの店舗端末，IC カードから構成される．プロトコル自動生成

(注1)：セキュリティプロトコルとは，IC カードと外部エンティティとの間で実行する認証プロトコルや鍵共有プロトコル等の IC カードと外部エンティティ間の通信路の安全性を確保するために利用するプロトコルのことを指す．

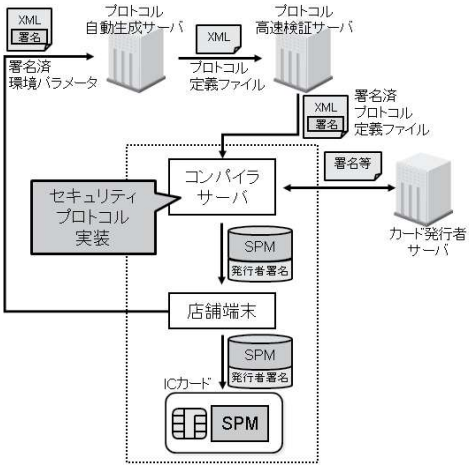

図 2　外部カスタマイズ方式の概要
Fig. 2　Outline of external customization method.

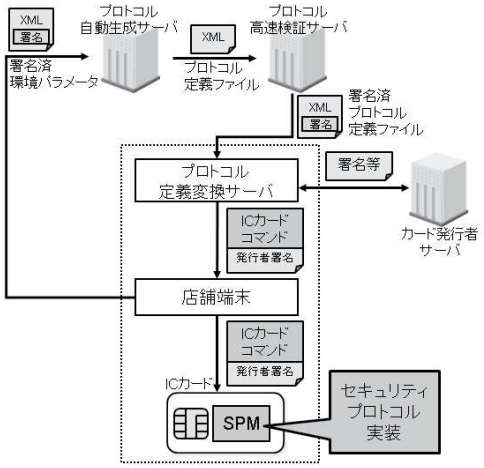

図 3　内部カスタマイズ方式の概要
Fig. 3　Outline of internal customization method.

サーバは店舗端末から，サービスの要件等を記載した署名済環境パラメータ（XML 形式）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，プロトコル高速検証サーバにおいてプロトコル定義ファイルに定義されているプロトコルの安全性を検証し，XML 署名を付与する．次に，コンパイラサーバはプロトコル高速検証サーバから取得したプロトコル定義ファイルの署名を検証し，カード発行者サーバと連携して発行者署名が付与された SPM を生成する．最後に，SPM を各店舗端末に配信し，IC カードにおいて発行者署名を検証した上で搭載されている SPM と置き換える．このような方式を実現することにより，IC カードで使用するセキュリティプロトコルを安全にカスタマイズすることが可能となった．なお，ここではプロトコル自動生成サーバやプロトコル高速検証サーバは研究対象外であるため，両者間のプロトコル定義ファイルの正当性確認については議論の対象外である．

2.3　内部カスタマイズ方式

内部カスタマイズ方式は，外部カスタマイズ方式と同様にプロトコル自動生成サーバ及びプロトコル高速検証サーバと連携して動作するものである．具体的には図 3 の点線で囲まれた部分であり，プロトコル定義変換サーバ，店舗端末，IC カードから構成される．店舗端末が環境パラメータを送信し，プロトコル定義ファイルを受信するまでは外部カスタマイズ方式と同様のフローであり，その後，プロトコル定義変換サーバはプロトコル高速検証サーバから取得したプロトコル定義ファイルの署名を検証し，カード発行者サーバと連携して発行者署名が付与された IC カードコマンドに変換する．最後に，変換した IC カードコマンドを各店舗端末に蓄積し，利用者が店舗端末でサービスを享受する際に IC カードコマンドを IC カードに送信し，IC カード内で発行者署名を検証した上で SPM の動作をカスタマイズする．このような方式を実現することにより，SPM の削除や搭載処理が不要となるため，短時間でセキュリティプロトコルをカスタマイズすることが可能となった．なお，ここではプロトコル自動生成サーバやプロトコル高速検証サーバは研究対象外であるため，両者間のプロトコル定義ファイルの正当性確認については議論の対象外である．

3.　セキュリティプロトコルのカスタマイズ技術を適用した IC カードサービスシステムの開発

本章では，これまでに提案した外部カスタマイズ方式及び内部カスタマイズ方式を組み込んで開発したより実サービスに近い IC カードサービスシステムの概要を示す．以下では，サービスを享受する環境の変化やプロトコルの危殆化といった 2 種類の利用シーンを想定し，それらの利用シーンに適合する IC カードサービスシステムの構成とその処理フローを示す．

3.1　環境変化適応型サービスシステム

3.1.1　利用シーン

ユーザが IC カードを用いて様々なサービスを享受

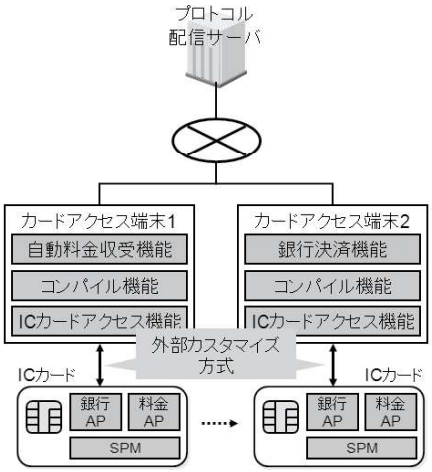

図 4　環境変化適応型サービスシステム
Fig. 4　Service system compatible with environmental variation.

する場合には，サービスの要件として高速な処理や高いセキュリティなどが要求されることが予想される．ここでは，同一の IC カードを用いて，高速処理が要求される自動車等の自動料金収受サービスと高セキュリティが要求される銀行等の決済サービスを享受する利用シーンを想定した．

3.1.2　システム構成

図 4 にシステム構成を示す．本システムは，プロトコル自動生成サーバとプロトコル高速検証サーバの機能を併せ持つプロトコル配信サーバと自動料金収受サービスを提供するカードアクセス端末 1 と，銀行決済サービスを提供するカードアクセス端末 2 と SPM を搭載した IC カードから構成される．なお，本システムでは，セキュリティプロトコルの実行処理時間が短いことが要求される自動料金収受サービスが含まれるため，表 1 より外部カスタマイズ方式を適用することとした．

3.1.3　認証プロトコル

認証プロトコルでは一般的に一方向性関数や暗号が使用される．一方向性関数を用いた認証は処理速度が速い反面，安全性を高めるためには鍵長を長くしなければならないという特徴がある．一方，暗号は処理速度は遅いものの，共通鍵暗号の場合，鍵長がある程度短くても安全性を高めることができるという特徴がある [8], [9]．ここでは自動料金収受サービスと銀行決済サービスという 2 種類の IC カードサービスを提供するために，2 種類の異なる特性をもつセキュリティプロトコルを一方向性関数と共通鍵暗号を用いて実現した．以下では使用したプロトコルの詳細を示す．

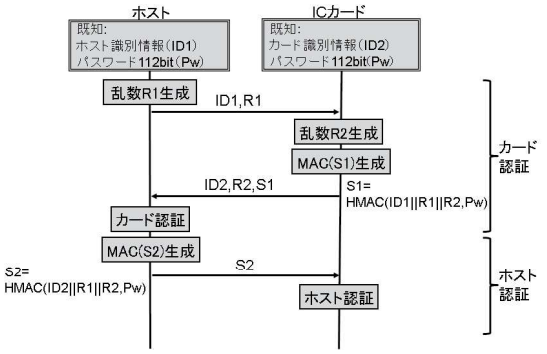

図 5　高速認証プロトコル
Fig. 5　Authentication protocol for high performance.

（a）　自動料金収受サービス向けセキュリティプロトコル

高速処理という要件を満たすために，鍵付き一方向性関数を用いた認証プロトコル（図 5）を使用した．本プロトコルは，CHAP (Challenge Handshake Authentication Protocol) [10] をもとに生成したものである．

まずはじめに，ホストが乱数 (R1) を生成し，ホストの識別子 (ID1) を含めて IC カードに送信する．次に，IC カードは，乱数 (R2) を生成し，受信した乱数 (R1) と識別子 (ID1) を組み合わせて，パスワード (Pw) を用いてメッセージ認証コード (MAC)(S1) を生成する．そして，IC カードの識別子 (ID2) と生成した乱数 (R2) と MAC(S1) をホストに送信する．ホストは，受信した MAC(S1) を送信したホストの識別子 (ID1)，乱数 (R1)，受信した乱数 (R2) とパスワード (Pw) を用いて検証し，カード認証を行う．次に，生成した乱数 (R1) と受信した乱数 (R2) と識別子 (ID2) を組み合わせて，パスワード (Pw) を用いて MAC(S2) を生成し，IC カードに送信する．最後に，IC カードは受信した MAC(S2) を送信したカードの識別子 (ID2)，乱数 (R2)，受信した乱数 (R1) とパスワード (Pw) を用いて検証し，ホスト認証を行う．なお，本プロトコルをプロトコル高速検証サーバ [6] により検証した結果，安全性評価指数(注2)は 95 となることを確認した．

(注2)：安全性評価指数とはプロトコルで使用する鍵の偽造確率を 2^{-k} としたときの k の値を示し，値が大きいほど安全性が高いことを示す [11]．ここでは，パスワードは英数字（62 種類）の組合せであると仮定した．

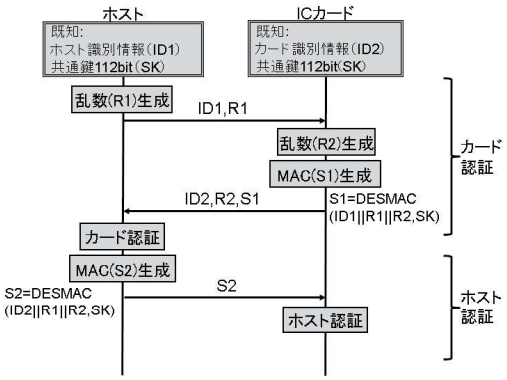

図 6　高セキュリティ認証プロトコル
Fig. 6　Authentication protocol for high security.

（b）銀行決済サービス向け高セキュリティプロトコル

高セキュリティという要件を満たすために，共通鍵暗号を用いた認証プロトコル（図 6）を使用した．本プロトコルは，GlobalPlatform 仕様 [1] で規定されている認証プロトコル SCP01 (Secure Channel Protocol 01) をもとに生成したものである．

まずはじめに，ホストが乱数 (R1) を生成し，ホストの識別子 (ID1) を含めて IC カードに送信する．次に，IC カードは，乱数 (R2) を生成し，受信した乱数 (R1) と識別子 (ID1) を組み合わせて，共通鍵 (SK) を用いてメッセージ認証コード (MAC)(S1) を生成する．そして，IC カードの識別子 (ID2) と生成した乱数 (R2) と MAC(S1) をホストに送信する．ホストは，受信した MAC(S1) を送信したホストの識別子 (ID1)，乱数 (R1)，受信した乱数 (R2) と共通鍵 (SK) を用いて検証し，カード認証を行う．次に，生成した乱数 (R1) と受信した乱数 (R2) と識別子 (ID2) を組み合わせて，共通鍵 (SK) を用いて MAC(S2) を生成し，IC カードに送信する．最後に，IC カードは受信した MAC(S2) を送信したカードの識別子 (ID2)，乱数 (R2)，受信した乱数 (R1) と共通鍵 (SK) を用いて検証し，ホスト認証を行う．なお，本プロトコルをプロトコル高速検証サーバ [6] により検証した結果，安全性評価指数は 112 となり，図 5 の認証プロトコルよりも安全性が高いことを確認した．

3.1.4　サービス提供フロー

環境変化適応型サービスシステムにおいてサービス提供時に実行するフローを図 7 に示す．

まずはじめに，IC カードを自動料金収受サービスを提供する IC カードアクセス端末 1 に挿入する．次に，IC カードアクセス端末 1 は，IC カードアクセス機能を使用して IC カード内の SPM を削除し，高速なセキュリティプロトコルを実装した自動料金収受サービス用 SPM を搭載する．その後，サービスを享受する際に自動料金収受機能を使用して IC カードと高速認証プロトコルを実行し，認証に成功した場合に自動料金収受サービスを提供する．その後，ユーザは銀行決済サービスを享受するために，IC カードを IC カードアクセス端末 1 から取り出し，銀行決済サービスを提供する IC カードアクセス端末 2 に挿入する．次に，IC カードアクセス端末 2 は，IC カードアクセス機能を使用して IC カード内の SPM を削除し，安全性の高いセキュリティプロトコルを実装した銀行決済サービス用 SPM を搭載する．その後，サービスを享受する際に銀行決済機能を使用して IC カードと高セキュリティ認証プロトコルを実行し，認証に成功した場合に銀行決済サービスを提供する．

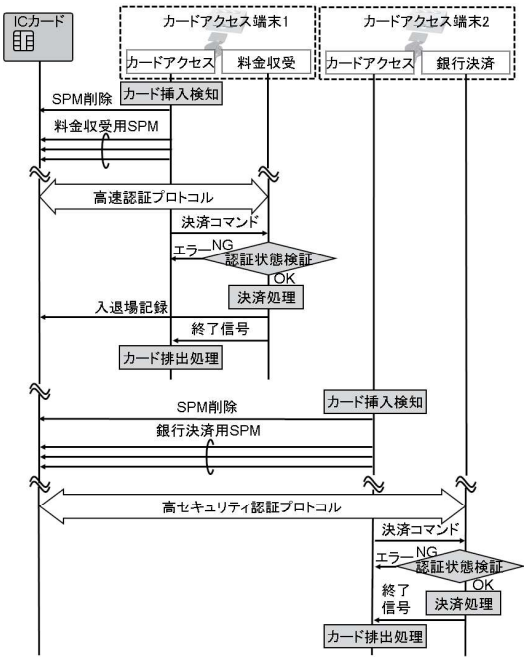

図 7　サービス提供フロー
Fig. 7　Service providing flow.

このようなフローを実現することにより，要件の異なるサービスを享受する場合でも同一の IC カードでシームレスにサービスを享受することが可能となる．

3.2 プロトコル危殆化適応型サービスシステム

3.2.1 利用シーン

ユーザがICカードサービスで利用するセキュリティプロトコルの安全性は，コンピュータ技術や解読技術の進展に伴い，低下していくことが予想される．ここでは，セキュリティプロトコルで使用する暗号アルゴリズムの鍵長が計算機パワーの向上により，実時間で解けてしまう危殆化シーンを想定した．また，具体的なサービスとして電子マネーのチャージサービスを想定した．

3.2.2 システム構成

図 8 にシステム構成を示す．本システムは，プロトコル自動生成サーバとプロトコル高速検証サーバの機能を併せ持つプロトコル配信サーバと，電子マネーサービスを提供するチャージサーバとチャージ端末，及び SPM を搭載した IC カードから構成される．なお，本システムではプロトコルのカスタマイズに伴う変更が鍵長のみで軽微であるため，表 1 より内部カスタマイズ方式を適用することとした．また，チャージサーバ側のセキュリティプロトコルの動的なカスタマイズは，太田ら [7] により開発された動的コンパイラ技術を使用した．

3.2.3 認証プロトコル

危殆化前と危殆化後で使用する鍵長の異なる 2 種類のセキュリティプロトコルを使用した．使用したプロトコルを図 9 に示す．

まずはじめに，ホストは乱数 (R1) を生成し，ホストの識別情報 (ID1) と併せて IC カードに送信する．IC カードは乱数 (R2) を生成し，受信した識別情報 (ID1) と乱数 (R1) とカードの秘密鍵 (SK2) からカード署名 (S1) として RSA 署名を生成し，ホストにカード署名 (S1) とカードの識別情報 (ID2) と生成した乱数 (R2) を送信する．ホストは，受信したカード署名 (S1) をカードの公開鍵 (PK2) を用いて検証し，カード認証を行う．次に，受信した識別情報 (ID2) と乱数 (R2) とホストの秘密鍵 (SK1) からホスト署名 (S2) として RSA 署名を生成し，IC カードに送信する．IC カードは，受信したホスト署名 (S2) をホストの公開鍵 (PK1) を用いて検証し，ホスト認証を行う．この署名生成や署名検証で利用する RSA の鍵長を危殆化前は 1024 bit とし，危殆化後は 2048 bit とした．なお，本プロトコルの安全性評価指数をプロトコル高速検証サーバ [6] により検証した結果，危殆化前は 80 であり，危殆化後は 112 であるため，安全性が向上していることを確認した．

3.2.4 サービス提供フロー

プロトコル危殆化適応型サービスシステムにおいてサービス提供時に実行するフローを図 10 に示す．

ここでは，既にプロトコルの危殆化が生じており，チャージサーバ側のセキュリティプロトコルは動的コンパイラ技術により 2048 bit に更新されている一方で，カード内のセキュリティプロトコルは 1024 bit のままであるとする．

まずはじめに，IC カードをチャージ端末に挿入する．次に，チャージ金額を入力する．するとチャージ端末は，プロトコル識別子取得コマンドを IC カード

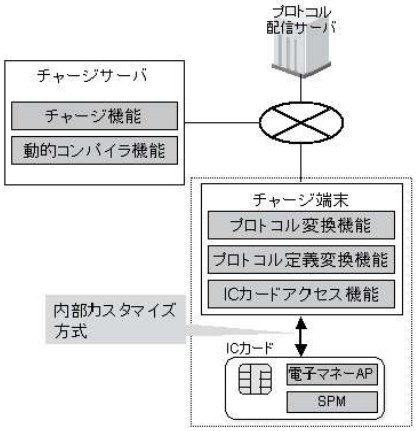

図 8 プロトコル危殆化適応型サービスシステム
Fig. 8 Service system compatible with protocol vulnerability.

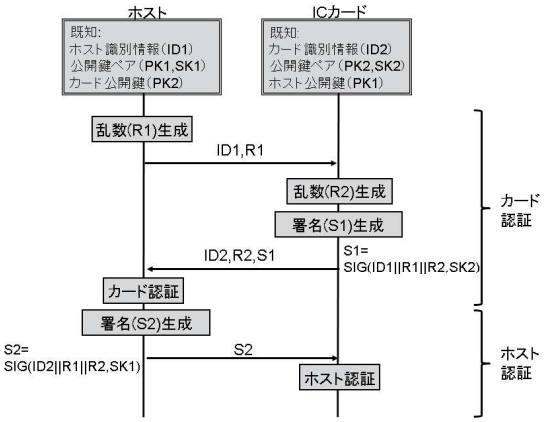

図 9 チャージ用認証プロトコル
Fig. 9 Authentication protocol for charge service.

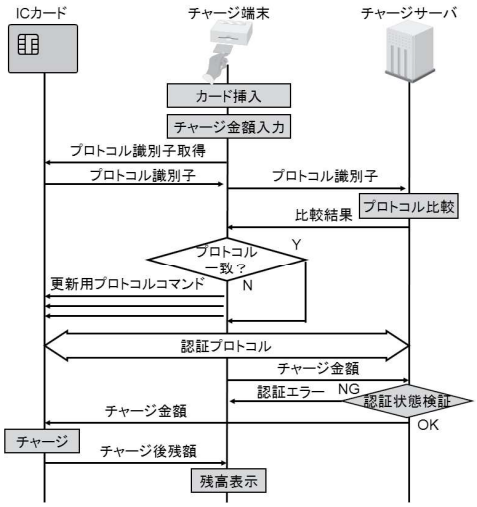

図 10　サービス提供フロー
Fig. 10　Service providing flow.

に送信し，1024 bit を示すプロトコル識別子を取得する．次に，取得したプロトコル識別子をチャージサーバに送信する．チャージサーバは受信したプロトコル識別子と，自身で保持している 2048 bit を示すプロトコル識別子を比較する．そして，比較した結果をチャージ端末に送信する．チャージ端末は，受信した比較結果から，IC カードとチャージサーバのプロトコルが一致していないと判断し，チャージ端末に格納されている更新用プロトコルコマンドを IC カードに送信し，セキュリティプロトコルのカスタマイズを行う．その後，IC カードとチャージサーバ間で認証プロトコルを実行する．次に，チャージ端末は入力されたチャージ金額をチャージサーバに送信する．チャージサーバは認証に成功しているかを検証し，失敗している場合にはチャージ端末にエラーを返し，成功している場合には IC カードに対してチャージ金額データを送信する．IC カードは認証に成功している場合にのみチャージ処理を行い，チャージ端末に残高を送信する．最後にチャージ端末は残高の表示を行う．

このようなフローを実現することにより，IC カードで利用するセキュリティプロトコルが危殆化した場合でもサービス提供時に動的にセキュリティプロトコルをカスタマイズし，安全性の低下を防ぐことが可能となる．また，サーバ側は危殆化後のシステムを運用すればよいため，従来のような危殆化前と危殆化後のシステムの二重化が不要となり，サーバ側の負荷を小さくすることも可能となる．

表 2　評価環境（サーバ）
Table 2　Evaluation environment (server).

項目	プロトコル配信サーバ	チャージサーバ
OS	Windows XP SP3	Linux Fedora Core release 6
CPU	Core2Duo 2.4 GHz	PentiumM 1.73 GHz
HDD	80 GByte	40 GByte
RAM	1 GByte	480 MByte

表 3　評価環境（端末）
Table 3　Evaluation environment (terminal).

項目	IC カードアクセス端末	チャージ端末
OS	Windows XP SP3	Windows XP SP3
CPU	Core2Duo 2.93 GHz	PentiumM 1.73 GHz
HDD	160 GByte	40 GByte
RAM	2 GByte	480 MByte

表 4　評価環境（IC カード）
Table 4　Evaluation environment (smart card).

項目	IC カード	
	GlobalPlatform	MULTOS
OS	JavaCard 2.1.1 GlobalPlatform 2.1	MULTOS 4.2
CPU	AE46C1	AE45C1
EEPROM	68 kByte	36 kByte
RAM	2.7 kByte	1.3 kByte

4. 評　　価

本章では，開発した 2 種類のプロトタイプシステムの性能評価を行う．

4.1　評価システム仕様

評価で使用したサーバ及び端末の仕様を表 2 と表 3 に示す．また，評価では GlobalPlatform 仕様 [1] と MULTOS 仕様 [2] の 2 種類の IC カードを使用した．その仕様を表 4 に示す．なお，GlobalPlatform 仕様の IC カードには暗号アルゴリズムとして RSA 2048 bit が実装されていないため，プロトコル危殆化適応型サービスシステムでは MULTOS 仕様の IC カードのみで評価を行うこととした．

4.2　評 価 項 目

4.2.1　環境変化適応型サービスシステム

図 4 に示す環境変化適応型サービスシステムにおける評価項目を図 11 に示す．評価は，プロトコルの配信から実サービスの提供の直前までを範囲とし，処理時間の評価は，(1) プロトコル定義ファイル配信時間，(2) SPM コンパイル時間，(3) プロトコルカスタマイズ時間，(4) プロトコル実行時間の 4 点に関して実施した．また，評価は高セキュリティ認証プロトコ

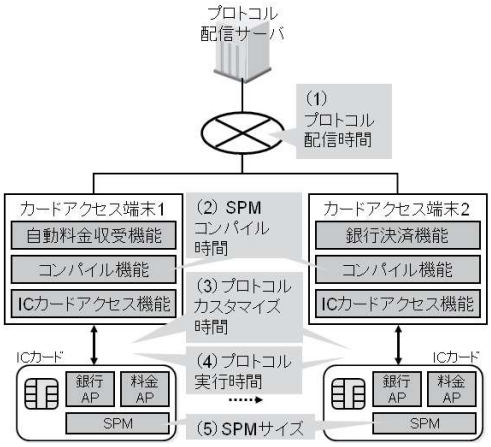

図 11　環境変化適応型サービスシステム評価項目
Fig. 11　Evaluation item of service system compatible with environmental variation.

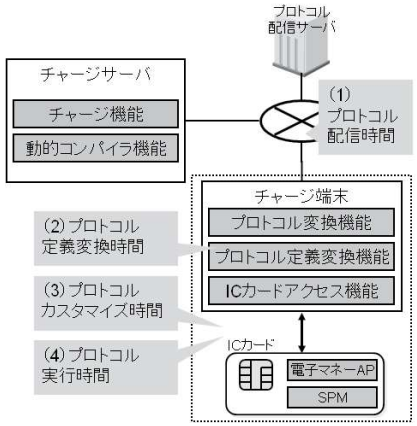

図 12　プロトコル危殆化適応型サービスシステム評価項目
Fig. 12　Evaluation item of service system compatible with protocol vulnerability.

ル，高速認証プロトコルのそれぞれについて実施した．更に，(5) IC カードに搭載される SPM のサイズについても評価を行った．

4.2.2　プロトコル危殆化適応型サービスシステム

図 8 に示すプロトコル危殆化適応型サービスシステムにおける評価項目を図 12 に示す．評価は，プロトコルの配信から実サービスの提供の直前までを範囲とし，処理時間の評価は，(1) プロトコル定義ファイル配信時間，(2) プロトコル定義変換時間，(3) プロトコルカスタマイズ時間，(4) プロトコル実行時間の 4 点に関して実施した．また，比較のためにアルゴリズム危殆化前の処理時間に関しても評価を行った．

表 5　高速認証プロトコルの評価結果
Table 5　Evaluation result for high performance authentication protocol.

評価項目	Global Platform	MULTOS
(1) プロトコル配信時間	0.189 s	
(2) SPM コンパイル時間	1.144 s	0.867 s
(3) プロトコルカスタマイズ時間	8.278 s	6.479 s
(4) プロトコル実行時間	0.372 s	1.071 s
カード認証	0.259 s	0.741 s
ホスト認証	0.113 s	0.330 s
(5) SPM サイズ	3.962 kByte	5.005 kByte

4.3　評価結果

4.3.1　環境変化適応型サービスシステム

(a)　高速認証プロトコル

図 5 のフローを外部カスタマイズ方式により GlobalPlatform カードと MULTOS カードに実装した場合の評価結果を表 5 に示す．なお，測定は 10 回行い，表にはその平均値を記載している．

この結果，カスタマイズ時間は，約 6〜8 秒程度の処理時間が必要となることが判明した．しかしながら，今回対象としている IC カードサービスでは，カードの挿入からサービスの享受まで時間差があるため，問題とはならないと考えられる．また，実行時間については約 0.4〜1 秒程度であることが判明した．自動料金収受サービスの一例である ETC サービスではサービス全体で約 4 秒の処理時間が必要であるが [12]，今回の評価結果はこの処理時間よりも短時間で認証処理が完了しているため，高速の要件を満たしているということができる．更に，公的分野における標準的なアプリケーションのサイズの上限は 5 kByte [13] であることを考慮すると，GlobalPlatform カードでは SPM 以外に 12 個のアプリケーションを搭載可能であり，MULTOS カードでは SPM 以外に 6 個のアプリケーションを搭載可能であるため十分実用性があることを確認した．

(b)　高セキュリティ認証プロトコル

図 6 のフローを外部カスタマイズ方式により GlobalPlatform カードと MULTOS カードに実装した場合の評価結果を表 6 に示す．なお，測定は 10 回行い，表にはその平均値を記載している．

この結果，カスタマイズ時間は，両カードとも約 9 秒程度であり，高速認証プロトコルよりもカスタマイズ時間が必要となることが判明した．また，実行時間については，アルゴリズムの複雑さにより約 0.8〜

表 6　高セキュリティ認証プロトコルの評価結果
Table 6　Evaluation result for high security authentication protocol.

評価項目	Global Platform	MULTOS
(1) プロトコル配信時間	0.191 s	
(2) SPM コンパイル時間	1.173 s	0.910 s
(3) プロトコルカスタマイズ時間	9.383 s	8.926 s
(4) プロトコル実行時間	0.796 s	1.519 s
ホスト認証	0.379 s	0.844 s
カード認証	0.417 s	0.675 s
(5) SPM サイズ	4.255 kByte	9.122 kByte

表 7　チャージ用認証プロトコルの評価結果
Table 7　Evaluation result for charge authentication protocol.

評価項目	危殆化前	危殆化後
(1) プロトコル配信時間	-	0.132 s
(2) プロトコル定義変換時間	-	0.575 s
(3) プロトコルカスタマイズ時間	-	1.264 s
(4) プロトコル実行時間	5.105 s	12.746 s
カード認証	3.237 s	9.810 s
ホスト認証	1.868 s	2.936 s

1.5 秒程度必要となるものの，クレジットカード等の決済処理で利用されている EMV 仕様では決済完了までに約 10 秒程度必要であるため [14]，十分短時間で認証処理が完了しているということができる．更に，公的分野における標準的なアプリケーションのサイズの上限は 5 kByte [13] であることを考慮すると，GlobalPlatform カードでは SPM 以外に 12 個のアプリケーションを搭載可能であり，MULTOS カードでは SPM 以外に 5 個のアプリケーションを搭載可能であるため十分実用性があることを確認した．

4.3.2　プロトコル危殆化適応型サービスシステム **3.2.3** のフローを内部カスタマイズ方式により MULTOS カードに実装した場合の評価結果を表 7 に示す．なお，測定は 10 回行い，表にはその平均値を記載している．また，比較のため，危殆化前のプロトコル実行時間も評価した．

この結果，危殆化後は危殆化前よりも鍵長の増加に伴い実行時間は増加しているものの，カスタマイズ時間は約 1.3 秒という短時間で実現できることが判明した．よって，従来の窓口等での再発行作業に比べると十分短時間で処理できているということができる．

5. むすび

本論文では，セキュリティプロトコルのカスタマイズ技術である外部カスタマイズ方式及び内部カスタマイズ方式を適用した IC カードサービスシステムについて記述した．サービス環境の変化やアルゴリズムの危殆化に対応するために，外部カスタマイズ方式や内部カスタマイズ方式を使い分け，様々な IC カードサービスにおいて提案したカスタマイズ方式が有効であることを明らかにした．また，処理時間を評価した結果，セキュリティプロトコルのカスタマイズ処理に約 9 秒程度の処理時間が必要となる場合があるものの，状況に応じて複数の IC カードを適切に使い分ける手間や危殆化に伴う IC カードの再発行処理が不要となるため，大幅なユーザビリティの向上を達成しているということができる．

今後は，外部カスタマイズ方式と内部カスタマイズ方式を動的に変更するシステムや実サービス適用への課題抽出を行う予定である．

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」の一環として行われた．

文　献

[1] “GlobalPlatform card specification version 2.2,” GlobalPlatform, March 2006.
[2] “MULTOS カード発行ガイド,” マルトス推進協議会, March 2003.
[3] 内山宏樹，梅澤克之，洲崎誠一，“セキュリティプロトコルの変更が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,” 信学論（B），vol.J92-B, no.7, pp.1030–1038, July 2009.
[4] 内山宏樹，梅澤克之，洲崎誠一，“IC カード内部でセキュリティプロトコルの変更を実現する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,” 信学論（B），

vol.J92-B, no.12, pp.1823–1831, Dec. 2009.
[5] S. Kiyomoto, H. Ota, and T. Tanaka, “On-the-fly automatic generation of security protocols,” Proc. ICEIS 2008, INSTICC, June 2008.
[6] 太田陽基，清本晋作，田中俊昭，“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 IV〜認証・鍵交換プロトコルの安全性検証,” コンピュータセキュリティシンポジウム 2008 論文集，pp.575–580, Oct. 2008.
[7] 太田陽基，清本晋作，田中俊昭，“環境に応じた暗号プロトコルの動的変更方式の実装・評価,” コンピュータセキュリティシンポジウム 2009 論文集，pp.277–282, Oct. 2009.
[8] 岩田 彰，鈴木孜洋，奥野琢人，若山公威，高須紀樹，杉江 修，村瀬晋二，“インターネット暗号化技術—PKI, RSA, SSL, S/MIME, etc.,” ソフト・リサーチ・センター，May 2002.
[9] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: Keyed-hashing for message authentication,” Network Working Group Request for Comments: 2104, Feb. 1997.
[10] W. Simpson, “PPP Challenge Handshake Authentication Protocol (CHAP),” Network Working Group Request for Comments: 1994, Aug. 1996.
[11] S. Kiyomoto, H. Ota, and T. Tanaka, “Design of an efficient security protocol analyzer,” International Journal of Computer Science and Network Security, vol.7, no.6, pp.74–87, June 2007.
[12] 江口 理，遠藤和彦，“自動料金収受システム (ETC),” デンソーテクニカルレビュー，vol.6, no.1, pp.18–23, March 2001.
[13] “公的分野における連携 IC カード技術仕様,” 高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部），March 2002.
[14] 国土交通省国土技術政策総合研究所，“次世代道路サービス提供システムに関する共同研究報告書,” 国土技術政策総合研究所資料，no.319, March 2006.

（平成 22 年 7 月 29 日受付，11 月 24 日再受付）

内山 宏樹 （正員）

2003 京都大学大学院情報学研究科通信情報システム専攻修士課程了．同年（株）日立製作所システム開発研究所入所．以来，情報セキュリティ技術，保全技術などの研究・開発に従事．情報処理学会会員．

梅澤 克之 （正員）

1996 早稲田大学大学院理工学研究科機械工学専攻修士課程了．同年（株）日立製作所システム開発研究所入所．以来，分散オブジェクトシステム，モバイルセキュリティ技術，スマートカードセキュリティ技術などの研究・開発に従事．情報処理学会，電気学会各会員．博士（工学）．

洲崎 誠一

1991 横浜国大・電子情報卒．同年（株）日立製作所システム開発研究所入所．以来，情報セキュリティ技術の研究・開発に従事．1996 情報処理学会第 52 回全国大会優秀賞，2000 年度山下記念研究賞受賞．情報処理学会会員．博士（工学）．