

京都大学	博士（情報学）	氏名	内山 宏樹
論文題目	ICカードのセキュリティプロトコルカスタマイズ技術に関する研究		
（論文内容の要旨） 近年、ユビキタス環境の進展に伴い、個人が所有するICカードを用いたサービスが広がっている。ICカードはデバイスの正当性を保証するために外部装置との間で認証プロトコルや鍵交換プロトコルといったセキュリティプロトコルを実施することが一般的であるが、使用するセキュリティプロトコルはICカード発行時に固定されるため、サービス・環境の変化や暗号アルゴリズム等の脆弱性発覚に応じてセキュリティプロトコルを動的に変更することができないという課題があった。このような課題に対し、本論文では、ICカードのセキュリティプロトコルを動的に変更する技術に関してまとめている。 第1章では、本論文で取り扱うICカードやICカードに関連する仕様や技術に関する現状を概括し、主要な課題を提示している。 第2章では、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ために必要となるICカード内の構成とその構成においてセキュリティプロトコルをカスタマイズする方式の基本検討を実施している。具体的には、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セキュリティプロトコル機能を提供するセキュリティプロトコルモジュールを配置し、アプリケーションからの要求に応じてセキュリティプロトコルを実行する構成を提案している。また、ICカードのセキュリティプロトコルカスタマイズ方式として、ICカード外部でカスタマイズする方式とICカード内部でカスタマイズする方式の二種類を提案している。さらに、セキュリティプロトコルモジュールが動的にカスタマイズされた場合でもアプリケーションが要求するセキュリティレベルを維持できるように、アプリケーションのセキュリティレベルとセキュリティプロトコルのセキュリティレベルからアクセス可否を判断する方式に関して提案している。 第3章では、第2章で提案したICカードのプロトコルをカスタマイズする方式として、ICカードの外部でセキュリティプロトコルをカスタマイズし、安全にICカード内に格納する外部カスタマイズ方式およびカスタマイズに伴うアプリケーションのセキュリティレベルの低下を防止するアクセス制御方式の詳細について示している。また、提案方式の有効性を確認するため、人手によりセキュリティプロトコルを実装する従来の方式と比較しており、セキュリティプロトコルモジュールの生成時間や実行時間の観点で有用性を示している。 第4章では、第2章で提案した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方式として、ICカード内部に格納したセキュリティプロトコルモジュールの動作を変更することによりセキュリティプロトコルをカスタマイズする、内部カスタマイズ方式の詳細について示している。また、内部カスタマイズ方式の有効性を示すために、外部カスタマイズ方式と処理時間に関する比較を行っている。その結果、外部カスタマイズ方式よりもプロトコル実行時間は増加しているものの、カスタマイズ時間は短縮できていることが示されている。 第5章では、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およ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を提案している。具体的には、環境が変化した場合でも同一のICカードでサービスを楽しむ環境変化適応型サービスシステムと、セキュリティプロトコルで利用する暗号アルゴリズムが危殆化した場合に、ユーザに負荷をかけずに安全なプロトコルに更新する			

(続紙 1)

プロトコル危殆化適応型サービスシステムである．さらに，提案システムの有効性を示すために，プロトタイプシステムを構築し，セキュリティプロトコルのカスタマイズ時間や実行時間の観点で評価している．その結果，ICカードサービスで要求される処理時間と安全性を満足していることを示している．

第6章は，結論であり，本論文により得られた成果を概括している．

(論文審査の結果の要旨)

本論文は、ICカードで使用する認証プロトコルや鍵共有プロトコルといったセキュリティプロトコルをICカードの発行後に動的に変更する技術に関する研究をまとめたものである。得られた主要な研究成果は次の通りである。

(1) 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ために必要となるICカード内の構成について検討を行い、ICカード内のOSとアプリケーションの間のミドルウェアとしてセキュリティプロトコルモジュールを配置する構成を提案した。また、提案した構成を活用した2種類のセキュリティプロトコルのカスタマイズ方式を提案した。

(2) 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方式としてICカード外部でカスタマイズする方式を詳細に検討し、プロトタイプシステムを構築した。また、手動でセキュリティプロトコルを実装する場合と処理時間の比較を行い、プロトコル実装時間の大幅な短縮と実行時間の増加量が目標値以内に収まっていることにより有効性を示した。

(3) 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方式としてICカード内部でカスタマイズする方式を詳細に検討し、プロトタイプシステムを構築した。また、外部カスタマイズ方式を用いた場合と処理時間の比較を行い、プロトコルカスタマイズ時間が大幅に短縮され、目標値を達成していることを示した。

(4) 外部カスタマイズ方式と内部カスタマイズ方式の特徴を生かしたICカードサービスシステムを構築し、ICカードが使用される環境の変化やセキュリティプロトコルの危殆化に対応可能であることを確認した。また、構築したサービスシステムを評価し、各サービスで要求される処理時間と安全性を達成していることを示した。

以上要するに本論文は、ICカードの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ための要素技術である、ICカード内の構成やカスタマイズ技術に関する提案を行うとともに、その有用性ならびに優れた特性を明らかにしたものであり、学術上、實際上寄与するところが少なくない。よって、本論文は博士(情報学)の学位論文として価値あるものと認める。また、平成23年11月14日に実施した論文内容とそれに関連した口頭試問の結果合格と認めた。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。
要旨公開可能日： 年 月 日以降