2009 年 1 月 14 日
株式会社 KDDI 研究所
株式会社日立製作所
独立行政法人情報通信研究機構

利用環境や危殆化[*1] 状況に応じてセキュリティプロトコルを動的に生成･カスタマイズするセキュリティ技術を開発

株式会社 KDDI 研究所（代表取締役所長：秋葉　重幸／以下、KDDI 研）と株式会社日立製作所（執行役社長：古川　一夫／以下、日立）は、2006 年度から、独立行政法人情報通信研究機構（理事長：宮原　秀夫／以下、NICT）の委託研究として「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[*2] の自動生成･カスタマイズ技術に関する研究開発」プロジェクトを進めてきました。このたび、3 年間の研究成果として、世界で初めて、利用環境や危殆化状況に応じてセキュリティプロトコルを動的に生成･カスタマイズするセキュリティ技術を開発しました。

■背景

携帯電話や IC カードなどの電子機器が様々な形で外部のネットワークに接続されるユビキタス社会では、ユーザが利用環境に応じて安全にサービスを利用可能であることが望まれます。また、サービスに適用されているセキュリティ技術が危殆化した場合には、安全対策を迅速に行うことが求められます。従来、セキュリティプロトコルはセキュリティの専門家によって時間をかけて設計され、また、様々な機器やサービスごとに個別の技術が用いられてきました。そのため、セキュリティプロトコルの危殆化への対策を迅速に施すことも、多種多様なサービスに柔軟に対応することも困難でした。

■今回の成果

今回、委託を受けた KDDI 研と日立は、利用環境や危殆化状況に応じてセキュリティプロトコルを動的に生成･カスタマイズするセキュリティ技術を世界で初めて開発しました。本技術では、通信機器の処理性能やネットワーク状況に応じて、セキュリティプロトコルを自動的に生成し、その安全性をリアルタイムに検証することにより、利用環境に最適なセキュリティプロトコルにカスタマイズすることができます。また、セキュリティプロトコル自体や使用されている暗号アルゴリズムが危殆化した場合、IC カードのような制約の厳しいデバイスであっても、別の安全なセキュリティプロトコルへ迅速に置換することが可能です。これにより、ユーザは単一デバイスで様々なサービスを受けることができ、サービス提供者はサービス変更に伴うコストの大幅な削減が可能になることから、安全かつ低コストでユビキタス社会を実現することができます。

■今後の展望

本技術を利用した実証実験は、1 月 20 日（火）～23 日（金）に、滋賀県大津市で開催される「2009 年暗号と情報セキュリティシンポジウム（SCIS2009）[*3] 」内において実施される予定です。

■用語解説

*1 危殆化：セキュリティ上の安全が脅かされ得る状態になることを危殆化という。その場合、直ちに対策をとって安全な状態にする必要がある。
*2 セキュリティプロトコル：暗号アルゴリズムをもとに、認証や鍵共有などのセキュリティ機能を提供する手順。
*3 「2009 年暗号と情報セキュリティシンポジウム（SCIS2009）」：（社）電子情報通信学会情報セキュリティ研究専門委員会が主催する国内最大の情報セキュリティに関するシンポジウム

■補足資料

本技術の概要は以下のとおりです。

⑴ セキュリティプロトコル自動生成・最適化・高速検証手法

様々な端末が異なる環境下で相互に接続される際、最適なセキュリティプロトコルを動的に生成・最適化し、生成したセキュリティプロトコルの安全性をリアルタイムに高速検証する手法です。

⑵ セキュリティプロトコルコンパイラ及びセキュリティプロトコルのセキュアなカスタマイズ・実装方式

自動生成されたセキュリティプロトコルを解釈し、実行プログラムへと変換するためのコンパイラ機能およびそのままプロトコルを実行するためのインタプリタ機能を実装する方式です。また、実装するデバイスとして、メモリ容量面及び計算効率面の制約が最も厳しい IC カード内に、セキュリティプロトコルモジュールを安全に実装する方式です。

⑶ プロトタイプシステム構築及び評価

ユビキタスネットワークや IC カードの利用を想定したサービスにおいて、項目 1 と項目 2 を統合したプロトタイプシステムをそれぞれ構築することにより、上記技術の機能及び性能評価試験を行います。なお、IC カードを利用するサービスとして想定したクレジットショッピングを行うデモシステムが、2008 年 11 月 4 日（火）～6 日（木）に、「CARTES & IDentifications 2008」において出展され、金融分野の企業から 多数の意見を頂戴しました。

■適用例

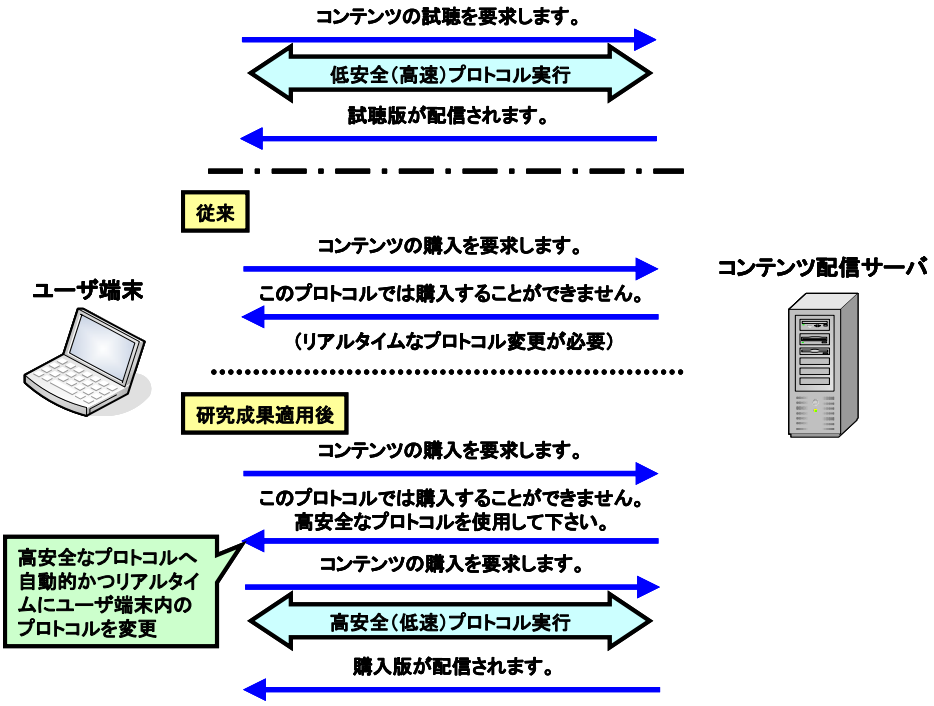

図 1:KDDI 研の研究成果の概要

本技術の適用例として、図 1 は動画コンテンツの配信サービスを想定しています。
まず、ユーザが動画コンテンツを試聴したい場合には、利便性を考慮して、安全であることよりも高速であることが要求されます。そこで、ユーザ端末とコンテンツ配信サーバ間において、安全性は低いが高速であるプロトコルを実行することにより、ユーザは効率良く動画コンテンツを試聴することができます(図 1 上)。

次に、ユーザが上記の試聴した動画コンテンツを購入したい場合、セキュリティの観点から、安全性の低いプロトコルをそのまま使用することは適切ではなく、安全性の高いプロトコルに変更する必要があります。しかしながら、従来技術では、ユーザ端末やコンテンツ配信サーバには個別にプロトコルが実装されているため、双方で使用可能な同じプロトコルに手動で変更しなければならず、自動的にもリアルタイムにもプロトコルを変更することができませんでした(図 1 中)。

それに対し、本技術を適用した場合、動画コンテンツを購入したいユーザ端末は安全性の低いプロトコルから安全性の高いプロトコルに自動的かつリアルタイムに変更されます。そのため、ユーザは効率良くかつ安心して動画コンテンツを購入することができます(図 1 下)。

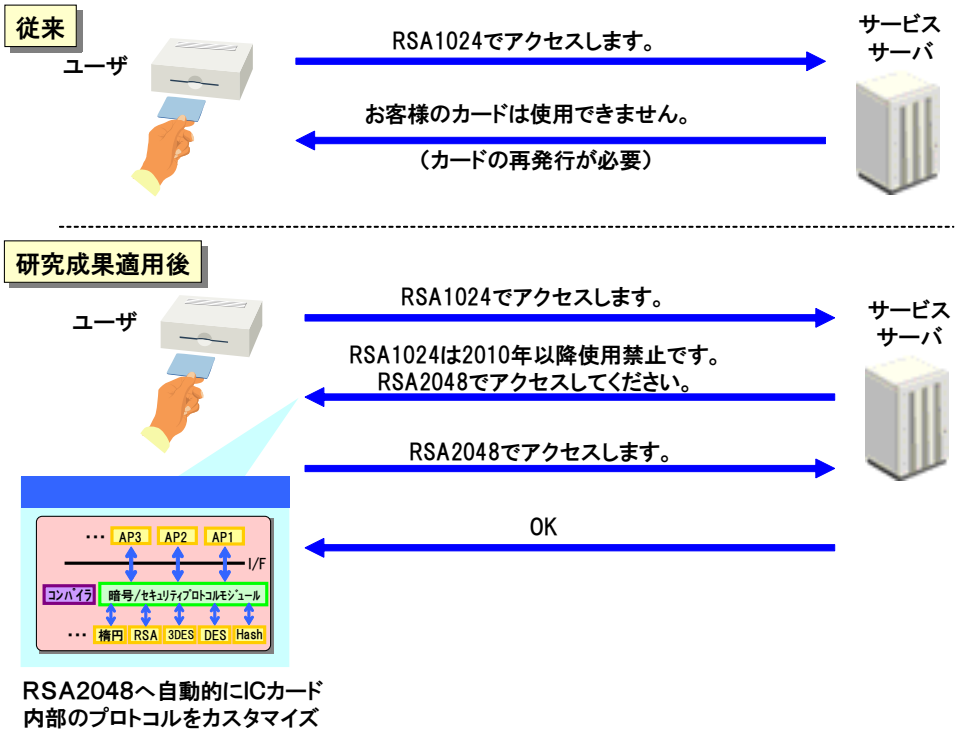

図 2:日立の研究成果の概要

本技術の適用例として、図 2 は IC カードの更新を想定しています。

具体的には、2010 年以前に配布された IC カード（1024 ビットの暗号アルゴリズムを使ったプロトコルが実装された IC カード）を使って、2010 年以降に、新サービス（2048 ビットの暗号アルゴリズムを使ったプロトコルを用いたサービス）を受ける際に想定されるプロトコル変更手順を示しています。

従来技術では、サービスの変更などに伴いプロトコルの変更が必要になった場合、IC カードの再発行及び再配布が必要でした（図 2 上）。

それに対し、本技術を適用した場合、サーバ側からの指示に基づいて自動的に IC カード内のプロトコルが更新されるため、IC カードを再発行及び再配布する必要がありません（図 2 下）。

これにより IC カード発行者の負担を軽減することが可能です。また、本更新処理は自動的に行うことができるため、ユーザの手間を省くことができます。

■お問い合わせ先

株式会社 KDDI 研究所 営業企画グループ 小島 淳一
Tel：049-278-7450　E-mail：inquiry@kddilabs.jp

株式会社日立製作所 システム開発研究所 企画室 塚越 雅人
Tel：044-959-0325

以上

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
