2004年1月23日
株式会社日立製作所

ドイツ研究機関と公開鍵暗号基盤を用いた認証技術に関する共同研究に着手
－国内外を問わず通信相手の認証を可能にする検証技術を開発－

株式会社日立製作所システム開発研究所（所長：小坂満隆　以下：日立）とドイツの Fraunhofer Institute for Secure Telecooperation[*1)]（代表者：Heinz Thielmann および Claudia Eckert　以下：FhI-SIT）は、公開鍵暗号基盤(以下：PKI)を用いた認証技術に関する共同研究を行うことで合意しました。本共同研究は、世界ではじめて、国による PKI（Public Key Infrastructure）環境の違いを意識することなく、通信相手の認証を可能とする検証技術の確立を目的としています。

PKI とは公開鍵暗号技術を使用した電子機器やネットワーク上のセキュリティ基盤技術の中で、特に電子証明書を利用する認証システムのことをいい、インターネット・イントラネットでのセキュリティを確保するセキュリティ基盤技術として業界標準となっています。そのため、電子商取引やインターネットバンキングなどのビジネス、電子行政サービスや電子申請サービスなどの電子政府プロジェクトなどに、幅広く使用されています。最近では、電子署名法が施行され、電子署名に法的な根拠を与えることができるようになり、電子署名を支える技術としても注目されています。

特に、すべての日本国民が情報通信技術を活用できる日本型 IT 社会を目指した“ e-Japan Ⅱ ”や“ 電子政府 ”に代表される次世代 IT 社会構想においては、高いレベルのセキュリティ社会を構築することが必要であり、PKI を用いた認証技術は、なりすましや改ざんを防止し、情報社会における高度な安全性を確保する技術として期待されています。

日立は、複雑な処理を必要とする電子証明書の検証作業を、証明書のユーザーに代わって行う日立証明書検証サーバ(Certificate Validation Server　以下：CVS)を用いた、ユーザー代行証明書検証サービスを世界ではじめて発売しました。この CVS はこれまで PKI を適用する際に課題となっていた、ユーザー側の検証作業の負担を大幅に軽減するとともに、検証速度の大幅な向上を実現し、既に、国内の多くのユーザーに採用されています。

今後、世界市場で CVS を展開するために、日立は今回、ドイツの FhI-SIT と共同研究を行うことで合意しました。

日立と FhI-SIT との共同研究では、以下の技術開発を進めます。

（1）海外検証手法への対応

日本の政府認証基盤では、認証局間において、単一の認証局を信頼し、相手の認証局に対して相互に発行する証明書である相互認証証明書を用いた検証技術を利用する、相互認証証明書モデルが採用されています。一方、海外では、多信頼点配布モデルを採用する国があります。本共同研究では、従来 CVS が持っている相互認証証明書モデル対応の機能に加え、この多信頼点配布モデルにも対応する機能を CVS に付加します。

（2）ドイツのブリッジ認証局[*2)]における多信頼点配布モデル環境での効果の検証

ドイツは多信頼点配布モデルの PKI システムが稼動している代表的な国です。しかし、ドイツでは CVS のような証明書検証サービスはなく、検証時におけるユーザー側の負担の軽減が研究課題の一つとしてあげられていました。そこで、上記(1)で付加した機能を用いることにより、日立の相互認証証明書モデルにおける証明書検証技術を、FhI-SIT が提供するドイツのブリッジ認証局での多信頼点配布モデルの環境に適用させ、その作業の負担軽減効果を検証します。

本共同研究は、世界ではじめて、多信頼点配布モデルの環境下における CVS の証明書検証技術を確立するものです。これにより、国ごとの PKI 環境の違いを意識することなく通信相手の認証を可能とする、国内外共通の証明書検証技術を実現することが可能となります。

【注釈】

*1) Fraunhofer Institute for Secure Telecooperation:
受託研究・開発、コンサルティング等を主要業務とするドイツの非営利応用研究機関 Fraunhofer Gesellschaft の下部組織の一つで、セキュリティに関する部門。ドイツ主要企業、政府機関、大学と連携しながらセキュリティ技術を開発・促進させ、それらを既存の製品に適用することを目的とした研究を行っている。

・所在地:Dolivostrasse 15、 D-64293 Darmstadt、 Germany

・URL:http://www.sit.fraunhofer.de/

*2) ブリッジ認証局:複数の認証ドメインを相互接続するための仲介を行う認証局。

■照会先

株式会社 日立製作所 システム開発研究所企画室 [担当:鈴木]
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
電話:044−959−0219 (ダイヤルイン)

以 上

このニュースリリースに掲載されている情報は、発表日現在の情報です。
発表日以降に変更される場合もありますので、あらかじめご了承ください。
