1B-6

機器関連携を実現するための 多機能 IC チップチップマネージャーの機能拡張

Multifunction IC chip chip manager's function enhancement of realizing equipment interaction

那須大輔[1]　鈴木裕之[2]　小尾高史[3]　谷内田益義[2]　山口雅浩[2]　大山永昭[1]
Daisuke NASU[1] Hiroyuki SUZUKI[2] Takashi OBI[3] Masuyoshi YACHIDA[2] Masahiro YAMAGUCHI[2] Nagaaki OHYAMA[1]
[1]東京工業大学フロンティア創造共同研究センター　[2]東京工業大学像情報工学研究施設　[3]東京工業大学大学総合理工学研究科

１．はじめに

インターネット等のオープンな環境において安全かつ共通な鍵管理・配送方法の実現を目指し、鍵の保存・管理媒体としての機器搭載型多機能ICチップ(e-Keyチップ)を利用したネットワーク基盤（Secure e-Key Network、以下SeKNWと呼ぶ）の構築が進められている[1]。我々は、SeKNWを利用して、サービスを利用する権利（サービス利用権）を安全にネットワーク経由で配送する手法について研究を進めており、サービスを享受する環境が異なっても、時間・場所などの制約を受けずに、サービス権利権を行使できるシステムの実現を目指している。

ここで、SeKNWを利用したサービス利用形態として、例えば、ある一台のチップ搭載機器で取得したサービスの利用権を，別のチップ搭載機器で利用するなど、家庭内などでネットワーク接続された複数のe-Keyチップ搭載機器を組み合わせて１つのサービスを利用するなどが想定される。そして、その実現には、暗号鍵などのサービスに必要な情報を安全性の担保されたチップ間でやりとりする仕組みが必要になる。

本研究では、シームレスな機器間連携を実現するために必要となるICチップチップマネージャ機能の拡張を行い、利用者やサービス提供者が意識することなく，複数の機器を利用したサービス提供を行う仕組みを提案する。

２．Secure e-Key Network

SeKNWは，図１に示すようにe-Keyチップの状態管理やサービス利用権管理等を行うプレイヤ及び，それらを相互に結ぶ通信網から構成され，各プレイヤが，情報機器に搭載されたe-Key チップを利用して，セキュアなネットワーク通信や情報サービスの利用権管理情報等を配送，管理する。SeKNWを構成する主なプレイヤとしては，e-Keyチップ搭載機器の登録・管理及びe-Keyチップの資源管理を行う機器管理者，e-Keyチップ上で利用権・鍵を管理する利用権管理アプリケーション及び利用権の管理を行う利用権管理者，e-Key チップ搭載機器利用者にサービスを提供するサービス提供者，機器を所有する機器所有者，サービスを享受する主体であるサービス利用者が定義されている。多目的ICカードの管理運用モデルであるNICSSフレームワークと同様にセキュアチップの状態管理とサービス提供に必要な仕組みを分離する2階層PKIの考え方を応用しているが、チップが管理者から貸与されるのではなく完全に所有者の物になる点や利用権管理APを管理する利用権管理者とサービス提供者を分離させた点が大きく異なる。

我々はSeKNWを利用した具体的なサービスとしてコンテンツ配信システムの研究[2]を行っており、システムに要求される基本機能の整理・検討・実装を行ってきた。提案するシステムでは、サービスの利用権は利用者に属するものとし、利用者の要求に応じて場所や時間を問わず利用権を行使することを可能としている。すでに、基本機能を搭載したシステムの開発は終了しているが、利用者の要求する多様な利用シーンに対応するためには、より具体的な利用場面を想定した機能の検討・拡張が必要である。

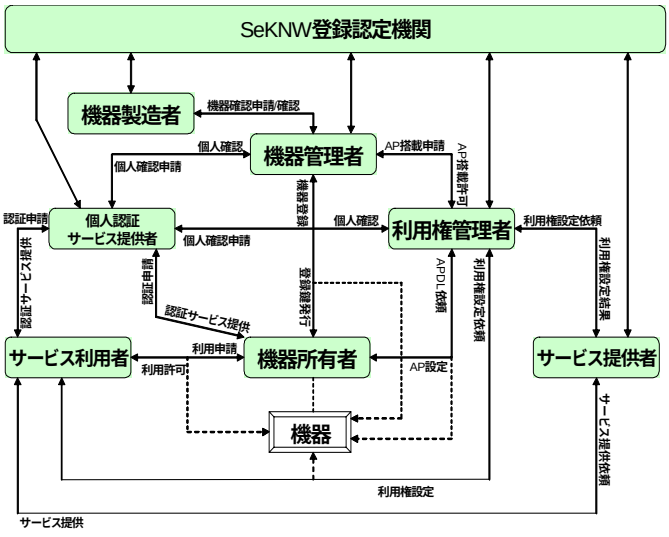

図１　Secure e-Key Networkのプレイヤモデル

３．研究手法

本研究では、家庭内での一般的利用を想定し、複数の機器を用いてサービスを利用する場面や，ポータブル機器などを利用する場面において、機器やICチップに要求される新たな機能の検討を行った。

そして、新たな機能として，チップ搭載機器間でのサービス利用権移動機能や，利用者認証機能の有しない端末においてサービス利用を可能とするために別のチップ搭載機器が有する利用者認証機能を利用する機能などが必要となることを明らかにした。

これらの実現には、ICチップ搭載機器間で機器が連携するために必要な情報をやりとりする必要があるが、そのためには、通信を行う機器相互が信頼できる機器であることの確認や，機器間で送受信されるデータの信頼性を確保できることが必要となる。本研究において、これらは、e-keyチップを利用した機器認証や、送受信データの暗号化・署名などにより実現される。

ここで、ＩＣチップ内には図２に示すように、機器認証に用いる鍵（機器認証鍵）の管理やチップ内でアプリケーションの管理などを行うチップマネージャ（CM）と、実際のサービスを利用する際に利用されるチップアプリケーション（AP）が存在する。機器間連携では、相互で機器認証を行うため，機器認証鍵を内部で管理するCMがその役割を担うものとした。

そして機器間連携を利用したサービスを実装する際に必要となる機能の明確化を行った。図３に、従来のCMの機能及び今回新しく拡張すべきCMの機能をそれぞれ示す。

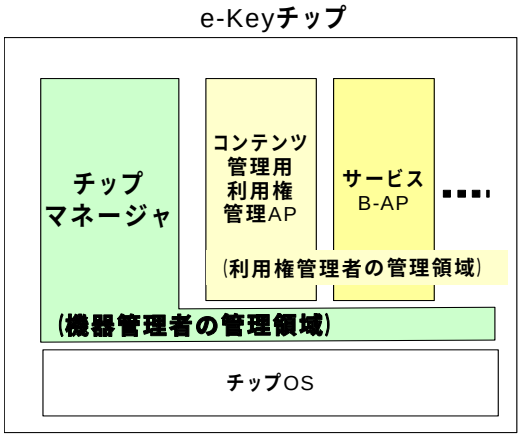

図２　チップ内部のソフトウエア構成

チップ認証	乱数生成機能
	署名データ生成機能
	機器間連携を行う CM 公開鍵証明書検証機能
	機器間連携を行う CM の公開鍵を利用した署名データ検証機能
暗号化生成・復号化	暗号データ生成機能
	暗号データ復号化機能
署名データ生成・検証	署名データ生成機能
	CM の公開鍵を利用した署名データ検証機能
チップ内蔵機器の限定・認証	機器間連携を行う機器を限定する機能
	限定された機器であることを認証する機能

図３　機器間連携に行うために必要となる CM の機能

※　　新しく追加された機能

このように、CM に機器連携の機能を実装させることにより、AP の違いによらず同一の機器間連携を実現することができると考えられるため、利用者が意識することなく，複数の機器を利用したサービスを享受することが可能となる。

４．実験

サービスの有効性を確認するため，２章で述べたコンテンツ配信システムに，機器間連携を利用した利用者認証を組み合わせたシステムを構築した。実験システムでは、利用者認証機能を有しないチップ搭載ポータブル機器と利用者認証機能を有するチップ搭載機器を連携させることを想定し，利用者認証時には，チップ認証を相互に行った後，機器間では，ポータブル機器から利用者認証端末へ送付される PIN データを暗号化する仕組みとした。そして，利用権管理者・利用者認証端末間でやりとりされる利用者認証子は機器間において署名データを付けてやりとりされる仕組みとし，それぞれを実装した。

５．まとめ

SeKNW を利用したシステムにおいて，機器間連携を実現するために必要なチップ搭載機器の機器認証や機器間での送受信する鍵データの暗号化・署名作業をチップマネージャー（CM）が行うこととし，それに必要な機能拡張を行った。そして，これらを利用したシステムの構築を行い，有効性を確認した。

参考文献

[1]　小尾，他：“ オープンなネットワーク環境で安全な鍵配送を実現するネットーワーク基盤 ”，電子情報通信学会 2004 総合大会予稿集，2004 年 3 月

[2]　那須，他：“ オープンなネットワーク環境で安全な鍵配送を実現するネットワーク基盤～Secure e-Key Network を利用した講義配信システムの開発～ ”，電子情報通信学会 2004 総合大会予稿集，2004 年 3 月