3E-1

サーバ連携 IC カードの検討

村上啓造† 堀正弘† 山本隆広† 庭野栄一‡ 小尾高史†† 谷内田益義†‡ 李中淳†† 大山永昭††
NTT セキュアプラットフォーム研究所† 日本電信電話株式会社 研究企画部門‡
東京工業大学像情報工学研究所†† 東京工業大学社会情報流通基盤研究センター†‡

1. はじめに

近年、公共分野では、電子行政推進の基本方針の一つとしてオンライン利用の拡大を推進しており[1]、パソコンだけでなく、行政キオスク端末や、携帯電話等のモバイル端末、デジタルテレビ等を利用した行政サービスに対するアクセス手段の多様化が検討されている[2]。従来は行政サービスへのアクセスには、IC カードを用いた認証が必要であった。IC カードで認証を行うためには、IC カード R/W が端末に接続できる必要があるため、パソコンに利用が限られ、アクセス手段多様化の妨げとなっていた。

また、認証用途のみならず、公共機関に存在する自己情報を開示する際や、親展情報が届く際に暗号化されて届くことが想定されるが、IC カード R/W が接続できない端末では IC カードのような耐タンパデバイスが接続できず、復号鍵の管理が難しい。

そこで、我々は、暗号機能をサーバ側で代替させ、クライアント側では認証用途のみの単機能 IC カードや回線認証+ID/Password で本人確認させるサーバ連携 IC カードを提唱する。

2. サーバ連携 IC カードの論理モデル

IC カードの機能（署名、認証、暗号化復号の秘密鍵演算）をサーバ上で実現する。サーバは、ユーザの自宅やコンビニエンスストアや役所にある PC やデジタルテレビなどのクライアント端末からインターネット回線を通じて接続されることが想定される。PC には IC カード R/W が接続される場合もあり、サーバへのログインには IC カード+PIN や、IC カード R/W のない端末では、回線認証や ID/Password が組み合わせて使われる。

従来 IC カード内に格納されていた暗号鍵はサーバに格納されるが、サーバ内に直接暗号鍵を格納した場合、暗号鍵の悪用の危険性があるため、利用者の暗号鍵は、耐タンパ性を有するハードウェアである HSM（Hardware Security Module）に格納する。

従来提案されているサーバ連携 IC カードは、VM、セキュア OS、TPM（Trusted Platform Module）を組み合わせる方式と HSM を用いる方式があるが[3]、どちらもサーバでのユーザ認証に IC カードを用いることを前提としている。それでは IC カード R/W が接続できない端末から ID/Password 等でログインするという、要件を満たさないため、本研究では、IC カード以外の認証にも対応することを前提とする。

3. サーバ連携 IC カードの実装案

通常のサーバと HSM では可能な演算・処理、またその性能・速度が異なるため、機能を分担させることを考える。通常の IC カード内に格納されているアプリは通常のサーバに格納し、アプリや共通ライブラリの実行は通常のサーバで処理を行う。秘密鍵は HSM に格納し、暗号関連の処理を HSM 内で行う。HSM のプロセッサは暗号演算処理に特化しているため、上述のように役割分担することで、性能向上が図れることが想定される。図 1 のような構成で、日本国民が各 1 アカウント持つ場合に、年平均 5 回/人、IC カード機能を利用するとし、必要サーバ台数を試算した。日ごとのアクセス数は平準化されているとし、時刻ごとのアクセス数は、その日のアクセス数の 70%がある 1 時間（昼休み等）に集中するとする。1 回の処理は 10 秒かかるとするとピーク時の呼量は、

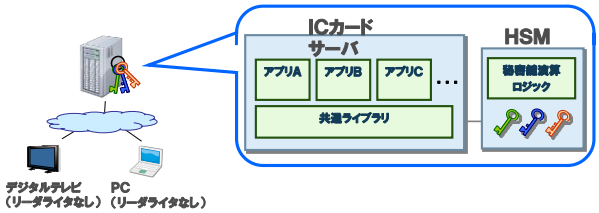

図 1 サーバ連携 IC カードの構成

An investigation of an IC card system cooperating servers.
Keizo Murakami†, Masahiro Hori†, Takahiro Yamamoto†, Takashi Obi, Masuyoshi Yachida, Lee Joong-sun, Nagaaki OHYAMA‡
†NTT Secure Platform Laboratories
‡NTT Research and Development Planning Depart., NTT Corporation
††Imaging Science and Engineering Laboratory, Tokyo Institute of Technology
†‡Advanced Research Center for Social Information Science and Technology,Tokyo Institute of Technology

1 億人÷365 日×70%×5 回×10 秒÷3600 秒＝2663 アーラン
サーバ 1 台で 500 アクセス同時処理できるとすると、6 台のサーバで収容可能となる。プロトタイプの実装を行い、性能測定を行ったところ、サーバ 1 台での 500 アクセス同時処理は可能であった。本実装は、HSM を用いていないため、HSM を用いた場合、処理能力が落ちることが想定されるが、必要サーバ台数という点では十分実現可能な範囲であると考えられる。

4. サーバ連携 IC カードの利点

前述の通り、IC カード R/W が接続できない端末でも、認証・署名等の IC カードの機能を利用することが可能となる。サービス提供者側は利用者が IC カードを用いてログインしているのか、サーバ連携 IC カードを用いてログインしているのかを区別する必要はないため、システム更改が最小限で済む。

また、従来の IC カードは容量に制限があったため、新たに暗号鍵やアプリを追加できる機能を持った高機能 IC カードであっても、無限に追加できるものではなかったが、サーバ連携 IC カードの場合、中央のサーバの容量は増設が可能なため、理論上は容量を気にせず機能追加が行える。

さらに、従来の IC カードサービスでは，利用者に IC カードを配布後に IC カード内のアプリケーションを更新・追加・削除を行う際には利用者に個別に対応してもらう必要があるが、サーバ連携 IC カードの場合、サーバ内のアプリの更新・追加・削除はサービス提供者が一括で行うことが可能となる。

5. サーバ連携 IC カードの問題点と解決案

サーバ連携 IC カードは、IC カード R/W が接続できない端末でも利用できることを想定しているため、サーバ連携 IC カードサービスへのログインは回線認証や ID/Password を用いてもできることとなる。その場合、セキュリティ強度が IC カードを用いた場合と比べて低下する。そこで、サーバ連携 IC カードのサーバに、利用者のログインの方法により、利用者が利活用できる情報・利用可能なアプリの制限を変える機能を持たせることを提案する。認証用途のみの単機能 IC カードでサーバ連携 IC カードサービスにログインした際には全ての情報・アプリが閲覧・利用できるが、ID/Password でログインした際には機微な情報の閲覧や機微な情報を扱うアプリ

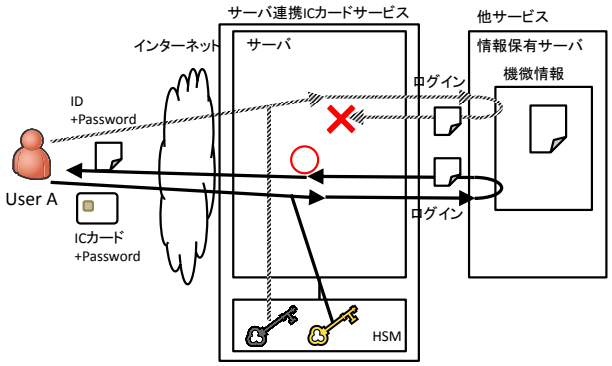

図 2 ログイン方法によるアクセス権制御

の利用はできない、と制限することで、セキュリティ強度の低下を抑える方法である。図のようにログイン方法によって HSM 内に格納されている鍵のうち使用するものを変える。

また、暗号鍵を HSM で保護しても、HSM にアクセスするサーバのソフトウェアが攻撃される可能性がある。そこでサーバに格納されるソフトウェアも保護する必要がある。これは、ソフトウェアを暗号化してサーバに置き、実行時に HSM 内で復号して実行する形にすることで、安全性を確保できると考えている[4]。

6. まとめ

以上のことからサーバ連携 IC カードは、現実的なサーバ台数で実現可能であることを、プロトタイプを用いて確認した。また、利用者のログイン方法によって利用できる情報を制御することでセキュリティ強度の低下を抑える方法について提案を行った。

参考文献

[1] 高度情報通信ネットワーク社会推進戦略本部, “行政キオスク端末のサービス拡大のためのロードマップ,” 2011.
[2] 高度情報通信ネットワーク社会推進戦略本部, “新たなオンライン利用に関する計画,” 2011.
[3] 本間祐次、小尾高史、谷内田益義、李中淳、大山永昭「様々なサービスへの対応を可能とするサーバ連携型 IC カードシステムの実現方式の検討」『コンピュータセキュリティシンポジウム 2009 予稿集』
[4] 村上啓造、岸晃司、山本隆広「ハードウェアと連携したセキュアインタプリタ技術の提案」『コンピュータセキュリティシンポジウム 2012 予稿集』