WWWにおけるICカード認証に関する一検討

1J－6　田中俊昭　羽田知史　山田　満
KDD研究所

1．はじめに

近年、電子商取引（エレクトロニックコマース）の実現に向け、インターネットWorld Wide Web（WWW）をプラットフォームとしたセキュリティシステムの研究・実験が盛んに進められている。また、利用者の利便性やセキュリティの向上を目的として、CPU内蔵型のICカードの利用が非常に注目されている。上記の背景を考慮し、筆者らはこれまで、WWWとICカードを組み合わせ、利用者とサーバ間で相手認証、暗号化通信及び相互署名などのセキュリティ機能を提供するシステムの検討を進めてきた[1]。本稿では、そのなかでも認証機構に着目する。具体的には、既存のWWW認証メカニズムに対してICカードを適用する際の問題点を抽出し、その解決法として初期認証と再認証を組み合わせた新たな認証メカニズムを提案する。

2．WWWの通信メカニズム

WWWは、クライアント（ブラウザとも呼ばれる）からサーバに蓄積されたハイパーテキストを検索するシステムである。ハイパーテキストは、ハイパーテキストマークアップ言語（HTML）と呼ばれる言語を用いて記述され、ページ単位で検索される。また、このクライアント／サーバの間で情報検索を行うためのプロトコルがハイパーテキスト転送プロトコル（http）である。httpは、TCP/IPの上で動作するプロトコルであり、例えば、GETと呼ばれるメソッドを用いて、１ページを検索する際に、まず、TCPプロトコルのコネクションを設定し、検索が終了するとTCPコネクションを解放する。つまり、httpレベルではコネクションレス型のプロトコルとして動作している。

3．WWWにおけるICカード認証の問題

相手認証（以後、単に認証とよぶ）とは、悪意をもった利用者が不当な利益を得る、あるいは、正当な利用者が損害を被ることを防止するために、通信相手の正当性を確認する機能である。ここで、WWWでは、上述のようにコネクションレス型の通信を行うため、１つのトランザクション毎（すなわち、ページの検索毎）に相手を認証する必要が生じる。従って、本稿では各利用者がICカードをクライアント（パソコン等）に接続し、ページ検索毎に認証を行うメカニズムについて考察する。まず、既存のWWW認証メカニズムとICカードとを組み合わせた場合の問題点について述べる。

3.1　httpdにおけるパスワード認証

httpdは、httpを処理するためのサーバ側のプロセスである。通常、httpdでは利用者毎のパスワードを管理し、サーバ側で利用者を認証する機能をもつ。しかしながら、サーバが利用者に要求するパスワードは、ネットワーク上を平文のまま流れるため、ICカードの有無にかかわらず、なりすまし攻撃が容易にでき安全性に問題がある。

3.2　SSLの認証メカニズム

現在のWWWにおいて、セキュリティ機能を提供するプロトコルがいくつか検討されている。そのなかでも、SSL（Secure Socket Layer）[2]は、サーバ認証、鍵共有、データ暗号化及びオプションとしてクライアント認証の機能を提供する。ここで、SSLにおける認証メカニズムをICカードと連動させた場合、基本的な認証処理はクライアント側のICカードの中で行なわれるので、安全性が高く、かつ可搬性のあるシステムを実現できる。しかしながら、ICカードへのアクセス時においては、パソコン等のクライアントとICカードの間での情報伝送に時間（通常、約数秒）を要するので、その結果、情報を検索する際に認証処理による遅延を生じ、利用者の利便性を損なう可能性がある。

4．効率的なICカード認証メカニズムの提案

上記の問題を解決するため、本稿では、安全性を保証し、かつ効率的な認証メカニズムを提案する。以下にその概要を示す。

（1）　コネクションレス型のWWWトランザクションにおいて、効率的な認証サービスを実現するため、図１のように１つの物理的なサーバ内において"認証が必要なエンティティ"と認証が不要で誰もがアクセスできる"公開エンティティ"を仮想的に設ける。これらのエンティティは、httpdで管理し、クライアントからのアクセス時に要求された

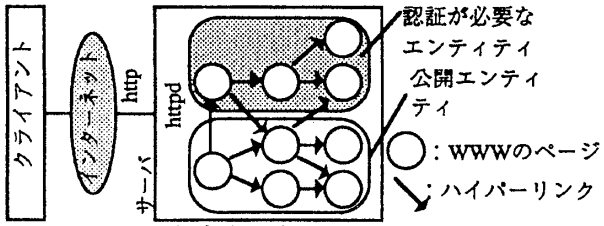


図１　認証を必要とするサーバの構成例

A Study on Authentication Mechanism of WWW System Using IC Cards
Toshiaki Tanaka, Satoshi Hada and Mitsuru Yamada
KDD R&D Labs.
2-1-15 Ohara, Kamifukuoka-shi, Saitama 356, Japan

ページのアドレスによりエンティティを識別する。

（2） 認証処理の応答性を改善するため、セキュリティ処理に関してはICカードとクライアント上のソフトウェアの双方で機能分担を行う。具体的には、上記（1）における"認証が必要なエンティティ"に初めてアクセスする際、ICカードを用いて厳密に相互認証を行う（初期認証と呼ぶ）。一方、初期認証において正常に相手を認証した後、認証が必要な当該エンティティに再度アクセスする場合、クライアント側ではICカードを介さずソフトウェアにて利用者認証を行う（再認証と呼ぶ）。

（3） 広域ネットワークでの利用を可能とするため、初期認証においては、通信相手と秘密情報の共有が不要な公開鍵暗号に基づく認証メカニズムを実現し、再認証においては高速処理が可能な秘密鍵暗号に基づく認証メカニズムを実現する。以下、提案メカニズムの具体的な手順を示す。

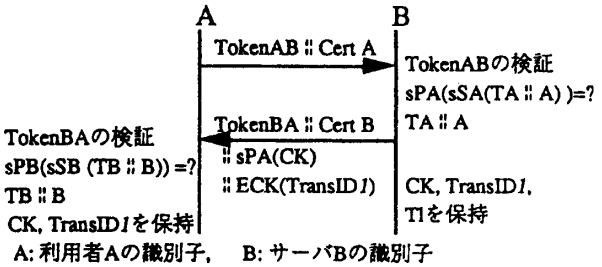
5. 提案メカニズムの認証手順

5.1 初期認証（図2）

初期認証は、公開鍵暗号に基づく標準の認証メカニズムを採用する[3]。なお、ICカードにおいては、利用者の秘密鍵及び対応する公開鍵証明を保管し、かつ内部で公開鍵暗号処理を実現するものとする。

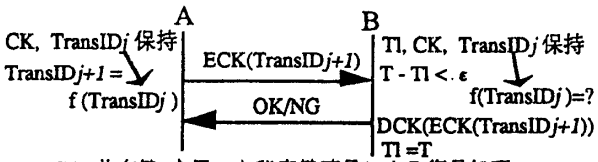
・利用者Aでは、ICカード内で作成した認証情報（TokenAB）と、ICカード内に保管されたAの公開鍵証明（CertA）とをサーバBに送る。

・Bでは、CertAより取り出したAの公開鍵（PA）を用いてTokenABの正当性を検証した後、Aが正しい相手である場合、Bの認証情報（TokenBA）、初期のトランザクションID（TransID*1*）及び通信鍵（CK）を作成し、TokenBA、Bの公開鍵証明（CertB）、通信鍵をAの公開鍵で暗号化した情報（sPA(CK)）及びTransID*1*をCKで暗号化した情報（ECK(TransID*1*)）をそれぞれAに送る。ここで、TransID*1*は再現性のない乱数等の時変情報を用いる。またBはこの時をAの最新アクセス時



A: 利用者Aの識別子, B: サーバBの識別子
Ti : iが付与する時変情報(i=A, B), Tl: Aの最新アクセス時刻
sSi: iの秘密鍵Siを用いた公開鍵暗号による復号処理
sPi: iの公開鍵Piを用いた公開鍵暗号による暗号処理
Cert i : iの公開鍵証明, CK: 通信鍵, ‖ : データの結合
Ek: 共有鍵kを用いた秘密鍵暗号による暗号処理
TransID*j*: j番目のトランザクションID（*j*=1,2....）
TokenAB = TA ‖ A ‖ sSA(TA ‖ A): BがAを認証するための情報
TokenBA = TB ‖ B ‖ sSB(TB ‖ B): AがBを認証するための情報

図2 初期認証の手順



Dk: 共有鍵kを用いた秘密鍵暗号による復号処理
f: トランザクションIDの更新に用いる非公開関数
T : 現在時刻, ε : 初期認証の有効期間

図3 再認証の手順

刻（Tl）とし、Tl、CK及びTransID*1*を保持する。

・Aでは、CertBより取り出したBの公開鍵（PB）を用いてBが作成した認証情報（TokenBA）の正当性を検証した後、ICカード内において、Aの秘密鍵（SA）を用いて通信鍵を復号し、CKを得るとともに、CKを用いて初期のトランザクションIDを復号しTransID*1*を得て、CK及びTransID*1*をクライアント上に保持する。

5.2 再認証（図3）

再認証はA、B双方が保持するトランザクションID（TransID*j*: *j*=1,2,..）を用いて利用者認証を行う。

・初期認証の後、Aが認証の必要なページの検索要求を行う場合、Aが保持するトランザクションIDをある非公開関数fにて次トランザクションIDに更新し（TransID*j+1*）、これを通信鍵CKにて暗号化してサーバBに送る（ECK(TransID*j+1*)）。

・Bでは、現在時刻TとTlとを比較し一定期間（ε）内であれば初期認証を有効とし、トランザクションIDをCKを用いて復号し、TransID*j+1*を得る。これを、Bが保持しているトランザクションID（TransID*j*）を関数fにて更新処理した結果と比較する。一致している場合には利用者認証が成立したと解釈し、Aに対して確認応答を返し、最新アクセス時刻Tlを現在時刻Tに更新する。

・確認応答を送受したB及びAは、更新されたトランザクションID（TransID*j+1*）を各自保持する。

ここで、再認証では初期認証の結果において共有される通信鍵とトランザクションIDを用いるので、初期認証なくして再認証は成立できない。また、再認証に用いるトランザクションIDは暗号化され、しかも、毎回異なる値を用いるので、なりすまし攻撃やリプレイ攻撃を防ぐことができる。

6. むすび

本稿では、WWWにおけるICカードを用いた認証機能について検討し、2種類の認証メカニズムを組み合わせた効率的な手法を提案した。今後は、本方式をWWWに実装し、動作検証を行う予定である。

最後に、日頃ご指導いただく、KDD研究所村上所長、古賀グループリーダに感謝します。

参考文献 [1] 田中, 羽田, 山田 "ICカードを用いたセキュアマルチメディアオンデマンドシステムの実装" SCIS'96 (1996). [2] Alan O. F. 他"Secure Socket Layer Version3.0" Internet Draft (1996). [3] ISO 9798-3(1994).