秘密情報を保持しないクライアントを用いた認証プロトコルの提案

五島　秀典*、鈴木秀和(名城大学)、渡邊　晃(名城大学)

Proposal of the Athemtication Protocol with Client that has No Secret Information

Hidenori Goshima、 Hidekazu Suzuki (Meijo University)、Akira watanabe (Meijo University)

１. まえがき

企業においては内部情報の漏洩防止が重要な課題である。情報漏洩の 4 割はノート PC 等のモバイル機器の盗難、紛失によるものと言われている。そこで社外に情報を持ち出さずに、必要に応じてクライアント PC から社内システムにリモート接続する方法が注目されている。このようなシステムでは確実な認証と暗号化が要求される。これを実現するには方式として、IC カードを使った認証方式がある。しかし、この方式ではクライアント PC に認証情報を埋め込んでおく必要があり、クライアントから情報が漏えいする懸念がある。そのためクライアントには情報を持たないこと望まれる。本稿では利用者の利便性の向上のため、スマートフォンに認証情報を保持させ、初期情報を一切所持しないクライアントを利用可能とするプロトコルを提案する。

２. 提案方式の概要

図 1 に提案方式の概要を示す。スマートフォン-クライアント間は Blue Tooth にてクライアント-サーバ間は任意のネットワークを介して行う。提案方式の前提条件としてスマートフォン、クライアント間の通信は近距離であり、この間での中間者攻撃は成り立たないものとする。

従来の方式として IC カードを用いた認証方式がある。この方式では IC カードとクライアントが事前共有鍵を保持する必要があり、クライアントから情報が漏洩する可能性がある。提案方式では事前共有鍵をやめ、スマートフォンが自らの公開鍵を保持するものとする。Table 1.に従来方式と提案方式の初期情報の違いを示す。

Table 1. Initial information

	事前鍵共有方式	提案方式
スマートフォン	ユーザ ID パスワード 生体テンプレート サーバ公開鍵 SP 秘密鍵 事前共有鍵	ユーザ ID パスワード 生体テンプレート サーバ公開鍵 SP 秘密鍵 SP 公開鍵
クライアント	事前共有鍵	なし
サーバ	サーバ秘密鍵 SP 公開鍵 ユーザ ID	サーバ秘密鍵 SP 公開鍵 ユーザ ID

スマートフォン、サーバには初期情報として認証用の情報をもたせるがクライアントには初期情報を一切所持させない。

Fig.1.を用いて動作を説明する。 まずスマートフォンから

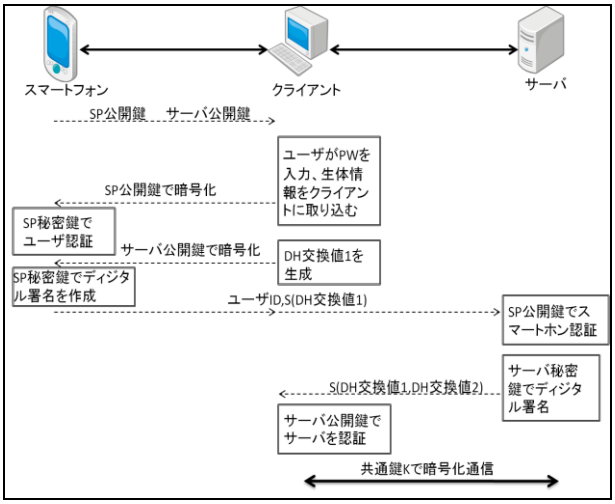

Fig.1. Outline of operation.

SP 公開鍵、サーバ公開鍵をクライアントへ送信する。次にユーザはパスワード及び生体情報を入力する。クライアントではユーザ情報を SP 公開鍵で暗号化する。また、Diffie-Hellman 鍵交換の交換値 DH1 を生成し、サーバ公開鍵で暗号化後、スマートフォンに送信する。スマートフォンでは SP 秘密鍵を用いてユーザ情報を確認することによりユーザ認証を行う。次にスマートフォンは SP 秘密鍵を用いてサーバ公開鍵で暗号化されている情報にディジタル署名を付加し、クライアントを通してサーバへ送信する。サーバではユーザ ID から対応する SP 公開鍵を用いてディジタル署名の検証を行い、スマートフォンを認証する。サーバは同時に DH 交換値 1 を取得する。最後にサーバは DH 交換値 2 を生成し、先ほど取得した DH 交換鍵 1 とともにディジタル署名を行い、クライアントへ送信する。クライアントではスマートフォンから最初に受け取ったサーバ公開鍵を利用しディジタル署名を検証することでサーバの認証を行う。

以上 3 ヶ所の認証を行うことでクライアント-サーバ間で相互認証を実現できる。クライアント-サーバ間では DH 交換値 1、2 によって共通鍵 K が得られるため、以後の通信は安全に情報のやり取りを行うことができる。

３. むすび

本稿ではスマートフォンによるクライアント-サーバ間の重要情報を安全に配送する認証プロトコルを提案した。今後は実装を完了させ、評価を行っていく予定である。

(1) 宮崎 雄介、”中間者攻撃に対する安全性の検討” 、2007