ユーザの有効期限が設定できる安全な匿名認証方式の提案

伊沢，亮一
森井，昌克

(Citation)
神戸大学大学院工学研究科・システム情報学研究科紀要,3:47-53

(Issue Date)
2011

(Resource Type)
departmental bulletin paper

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/81003781

神戸大学大学院工学研究科・システム情報学研究科紀要　第3号　47～53頁　2011年
doi:10.5047/gseku.j.2011.009

ユーザの有効期限が設定できる安全な匿名認証方式の提案

伊沢　亮一[1*]・森井　昌克[2]

[1]自然科学研究科情報・電子科学専攻

[2]工学研究科電気電子工学専攻

(受付:December 26, 2011　受理:February 28, 2012　公開:March 5, 2012)

キーワード：　匿名性，相互認証，鍵交換，無線通信，インターネットプロトコル

無線通信は電波が届く範囲に通信データが発信されるため，有線通信に比べて盗聴が容易である．ユーザを識別する情報が通信データに含まれていると，盗聴により付近にそのユーザがいることを知られることになる．このようなリスクを防ぐために，ユーザの匿名性に着目した匿名認証方式が盛んに研究されている．公開鍵暗号を利用する方法が一般的であるが計算量が大きいことが課題として挙げられる．そこで，Zhuらはユーザとその通信相手に加え，ホームエージェントを導入することでユーザが公開鍵暗号を利用しない方式を提案した．通信相手の代わりにホームエージェントがユーザを認証することで匿名認証を実現している．Zhuらの方式は脆弱性が指摘されているため，KangらやLeeらによって改良された．安全な匿名認証に加え，Kangらはユーザに有効期限を与え，Leeらは利便性を向上させるためにユーザが認証時に入力するパスワードを任意に設定できるようにした．しかしながら，Kangらの方式はホームエージェントに所属するユーザ間で匿名性が確保できない．有効期限に関しても，有効期限後に秘密情報が取り出せないデバイスをユーザに与えているだけで，厳密に有効期限を設定できているとは言い難い．また，Leeらの方式では安全性がユーザの設定するパスワードに依存するといった課題がある．本論文では，これらの欠点を改善することを目的とし，有効期限が設定できる安全な匿名認証を提案する．具体的にはホームエージェントに所属するユーザ間においても匿名性が確保でき，ユーザが設定するパスワードに安全性が依存しない方式である．

緒　　言

ノートPCやスマートフォンなどのモバイル端末が普及するにつれ，無線を用いてネットワークに接続するユーザが増えている．最寄りの無線LANアクセスポイントへの接続やアドホックによるサービス端末への接続が例として挙げられる．有線通信とは異なり，無線通信では電波の届く範囲全てに通信パケットが発信されることから，盗聴や通信相手を偽るなりすましなどのインシデントが容易に発生する．したがって無線環境においても安全な通信を実現するために様々な通信プロトコルが研究されている．

安全な通信を実現するためには相互認証と暗号化通信が基本となる．モバイル端末を持つユーザが周辺のサービス端末へ接続する場面であれば，サービス提供者側が正規のユーザかどうかを認証することに加え，ユーザが接続先のサービス端末を認証することが必要となる．悪意のある第三者がユーザの情報を盗むために不正な端末を設置することがあり，この対策として相互認証は有効である．認証した後，暗号化された通信路を介してデータの送受信を行うことで盗聴を防ぐことができる．二者間でセッション鍵を共有し，その鍵を用いて通信データを暗号化することで暗号化通信が可能となる．

本研究では，より安全な通信を実現するために匿名認証方式に着目する．匿名認証ではユーザの匿名性を確保したまま相互認証と暗号化通信を行う．具体的には，ユーザが自身のIDを秘匿化した上で認証の要求を行い，接続先の端末に特定されることを防ぐ．これに加え，悪意のある第三者が通信を盗聴したとしても，ユーザを特定できないようにする．無線通信ではユーザが周辺のサービス端末に接続するため，サービス端末の物理的な位置とユーザのIDからそのユーザの移動履歴や現在位置が知られてしまう．プライバシ保護の観点からユーザの匿名性を確保する方法が希求されている．一方，サービス提供者はユーザを管理したいという要望がある．これはサービスを運用する上で，ユーザに対して有効期限を設定することや，規約違反時にユーザの権利をはく奪することなどが必要となるためである．

ユーザの管理に適した匿名認証方式としてZhuらの方式[1)]が挙げられる．Zhuらの方式ではモバイルユーザ（以下，MU）が所属する，信頼できるホームエージェント（以下，HA）の存在を仮定することで匿名認証を実現している．MUが外部のサービス端末（以下，FA（Foreign Agent））に接続するとき，秘匿化されたIDを含む認証要求をFAに送信する．FAはその要求をインターネット経由でHAに転送し，HAが代わりにMUを認証する．これによりMUはFAに

特定されることなく認証を受ける事ができる．このときHAはMUのIDを知ることができるためMUの有効期限の確認などが可能となる．Zhuらは単に匿名性を確保するだけでなく，HAが認証データベースを利用しない，つまり，MU毎の認証情報を保持しない方式を与えた．具体的にはHAはある秘密情報 N を保存しており， N と受信した認証要求を用いてHAに所属するMUを認証する． N は全てのMUの認証に用いられるため，HAの記憶容量やデータベースを検索する時間などのコストが大幅に削減できる．

Zhuらの方式は脆弱性が指摘されているため，Wuら[2]はZhuらの方式を改良した．その後，Kangら[3]とLeeら[4]はWuらの方式の脆弱性を指摘し改良を与えた．Kangらは安全な匿名認証とMUに有効期限を与えることを目的とし，その実現方法を提案した．しかしながら，Kangらの方式は同一のHAに所属するMU間では匿名性を確保することができない．これは全てのMUが共通の値とXOR演算を用いてIDを秘匿化しているためである．悪意のあるMUが別のMUの通信を盗聴し，共通の値によりIDを求めることができる．また，有効期限に関しても，有効期限後にMUのデバイスが動作しないことを仮定しているだけであって目的を達成しているとは言い難い．Leeらは安全な匿名認証とMUが任意のパスワードを選択できることを目的とした．Leeらは認証データベースをHAに与えることでこれらを実現している．Zhuらの方式やKangらの方式では認証時にMUが入力したパスワードを基に認証要求が作成される．これはデバイスを紛失したときの対策であり，デバイスだけでは認証要求が作成できない仕様となっている．Zhuらの方式やKangらの方式でのパスワードとして，MUのIDと，特に N のハッシュ値が用いられる事から，MUが任意に設定する事ができず，扱いが容易でない．すなわちMUの知識のみに基づく固有情報にならず，記憶する事が容易でなく，この点が運用上の大きな難点となり得る．そこで，LeeらはMUが任意のパスワードを設定できるように改良し，この点を克服した．しかしながら，Leeらの方式ではMUが設定する任意のパスワードに安全性の強度が依存している．一般のユーザはパスワードを暗記する煩雑さを避けるため，簡単な文字列を設定する傾向がある．このことからLeeらの方式は安全な方式とは言い難い．

本論文では，認証データベースを用いることなく，有効期限が設定できる安全な匿名認証方式を提案する．具体的にはHAに所属するMU間においても匿名性を確保することができ， MUが設定する任意のパスワードに安全性の強度が依存しない方式である．提案方式ではZhuらの方式と同様，HAは N しか保持していないため，MUが自身の認証情報をHAに伝える必要がある．提案方式の要点は次の通りである．MUのデバイスに，有効期限と乱数 M ， ID，任意のパスワードを連結した値を暗号化し，自身の認証情報として保存しておく．暗号鍵にはHAのみが知りえる N を用いる．各MUは異なる認証情報を保持しているためKangらの方式での脆弱性はなく，有効期限は暗号化されているため，MUは改ざんできない．暗号化された値に加え，MUのデバイスには乱数 M とパスワードをXOR演算した値を保存しておく．MUはパスワードを入力することで乱数 M を取得し， M を用いて認証要求を作成する．すなわちLeeらの方式におけるパスワードの役割を乱数が担うことで安全な方式となっている．認証時にはMUが暗号化された認証情報を，FA経由でHAに送信することによって認証に必要な情報を伝えることができる．

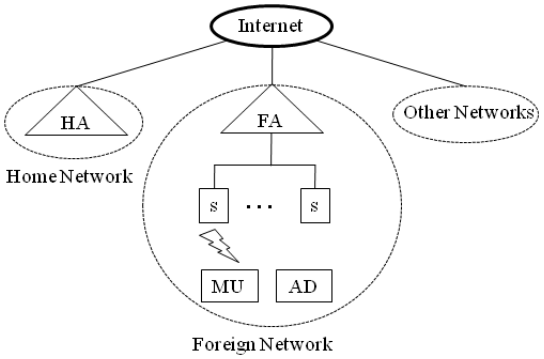

Fig. 1 匿名認証が利用される環境のモデル

１．匿名認証が利用される環境のモデル

匿名認証が利用される環境のモデル[1]をFig. 1に示す．HAは認証用のサーバのことを指し，HAが存在するネットワークのことをHome Networkと呼ぶ．FAは外部のネットワーク（Foreign Network）を統括するサーバで，サービスを提供する端末sが接続されている．MUはHAに登録することで各sからサービスを受けることができる．MUは所持しているモバイル端末を用いて，sと無線で通信を行う．AD（Adversary）は悪意のある第三者であり，MUとsの無線通信を盗聴してMUのIDを取得するなどの攻撃を行う．Other NetworksはForeign Networkが他にも複数存在することを示している．

本モデルを実環境に対応させた一例を説明する．Home NetworkはMUの情報を扱う会社のネットワークに対応する．Foreign Networkは提携している会社のネットワークに対応し，サービスはForeign Networkで提供される．sは街頭や店舗に設置されている有料の無線LANアクセスポイントや周辺の役立つ情報を発信する端末などに対応する．MUはHAに登録するだけで全てのsからサービスを受けることができる．MUがsに接続したとき，FAがHAに問い合わせることでHAがMUを認証し，同時にMUもsが不正な端末でないことを確認する．このとき，MUがsを利用したことが，FAやADに知られると，現在地を把握されるなどのリスクが懸念される．認証後にMUとFAは暗号化された通信路上でのサービスの授受によってデータの盗聴を防ぐ必要がある．以下に匿名認証の目的をまとめる．

- MUとFAの双方向認証
- FAおよびADに対するMUの匿名性の確保
  （HAに対してはMUのIDを知られてもよい）
- MUとFAのセッション鍵の共有
- セッション鍵の更新

ここで，セッション鍵はMUとFAは暗号化された通信路を確立するために利用する鍵を指す．なお，Zhuらの方式ではMUの有効期限は考慮されていない．

２．Wuらの方式

本章ではWuらの方式のプロトコルを説明する．次章でその欠点およびKangらの方式とLeeらの方式についてWuらの方式を基に説明する．本論文で使用する記号の定義をTable 1に示す.

２．１ 概要

Wuらの方式は登録処理と認証処理，セッション鍵更新フェイズで構成される．登録処理では，HAがMUの秘密情報をスマートカードなどのデバイスに格納してMUに配布する．認証処理では，MUとFAがHAを介して相互認証すると同時にセッション鍵を共有する．MUが認証要求を作成するとき，共通鍵暗号と一方向性ハッシュ関数，XOR演算，情報の連結を使用し，公開鍵暗号は使用しない．これは公開鍵暗号の計算量が極めて大きく，モバイル端末の中でも計算能力が特に低い端末を利用しているMUに対応するためである．FAとHAの通信には，安全性の検証を容易にするため，数学的に安全性が保証されている公開鍵暗号を利用する．公開鍵暗号で作成したデジタル署名によりFAとHAはお互いに認証することができ，検証子により通信データの改ざんを検知することができる．セッション鍵更新フェイズではMUとFAが暗号化された通信路上でサービスを送受信すると同時にセッション鍵を更新する.

２．２ プロトコル

2.2.1 登録処理

登録処理では，MUとHAが安全な経路でデータの送受信を行う．ここで，安全とは盗聴や改ざんなどのインシデントが発生しないことを意味する．例として，物理的なデバイスの手渡しや輸送が挙げられる．その他の処理ではデータ通信（安全でない通信路）を用いる．登録処理の手順は次の通りである．MUは ID_{MU} をHAに送信する．HAは $PW_{MU}=h(N\|ID_{MU})$ と $r=h(N\|ID_{HA})\oplus h(N\|ID_{MU})\oplus ID_{HA}\oplus ID_{MU}$ を計算する．ここで，N はHAのみが知りえる秘密情報である．HAは ID_{HA} と r をMUのデバイスに格納し，デバイスと PW_{MU} をMUに送信する．このとき，HAは ID_{HA} と N，$h(N\|ID_{HA})$ を保持している.

2.2.2 認証処理

1. MUは PW_{MU} を入力する．次に，MUは乱数 x_0 と x を生成し，以下の値を計算する.
$$L=h(T_{MU}\oplus PW_{MU})=h(T_{MU}\oplus h(N\|ID_{MU}))$$
$$n=r\oplus PW_{MU}=h(N\|ID_{HA})\oplus ID_{HA}\oplus ID_{MU}$$
$$(h(ID_{MU})\|x_0\|x)_L$$
ここで，T_{MU} は現在の時刻である.
2. MU → FA: n，$(h(ID_{MU})\|x_0\|x)_L$，ID_{HA}，T_{MU}.
3. FAは T_{MU} の正当性を確認する．正しければ，乱数 b を生成してからデジタル署名 $Cert_{FA}$ と検証子 $E_{S_{FA}}(h(b,n,(h(ID_{MU})\|x_0\|x)_L\|T_{MU}\|Cert_{FA}))$ を作成する.
4. FA → HA: b，n，$(h(ID_{MU})\|x_0\|x)_L$，T_{MU}，$Cert_{FA}$，T_{FA}，$E_{S_{FA}}(h(b,n,(h(ID_{MU})\|x_0\|x)_L\|T_{MU}\|Cert_{FA}))$.
5. HAは T_{FA} と $Cert_{FA}$ の正当性を確認する．それらが正しければ，以下の式より ID_{MU} と L を求める.
$$ID_{MU}=n\oplus h(N\|ID_{HA})\oplus ID_{HA}$$
$$L=h(T_{MU}\oplus h(N\|ID_{MU}))$$
次に，HAは $(h(ID_{MU})\|x_0\|x)_L$ を復号する．ID_{MU} のハッシュ値を求め，復号した $h(ID_{MU})$ を比較する．一致すればMUを認証し，乱数 c と $W=E_{P_{FA}}(h(h(N\|ID_{MU}))\|x_0\|x)$ を作成する.
6. HA → FA: b，c，W，$Cert_{HA}$，T_{HA}，$E_{S_{HA}}(h(b,c,W,Cert_{HA}))$.
7. FAは T_{HA} と $Cert_{HA}$ の正当性を確認する．それらが正しければ，S_{FA} で W を復号してから $TCert_{MU}$ を作成する．ここで，$TCert_{MU}$ は認証処理後のデータ通信で利用する一時的な証明書である．次に，以下の値を計算する.
$$k=h(h(h(N\|ID_{MU}))\|x\|x_0)=h(h(PW_{MU})\|x\|x_0)$$
$$(TCert_{MU}\|h(x_0\|x))_k$$
8. FA → MU: $(TCert_{MU}\|h(x_0\|x))_k$.
9. MUは k を計算して $(TCert_{MU}\|h(x_0\|x))_k$ を復号する．次に，$h(x_0\|x)$ が一致すればFAを認証する.

2.2.3 セッション鍵更新フェイズ

MUはFAとデータ通信を行うとともにセッション鍵を更新する．MUは $TCert_{MU}$ と $(x_i\|TCert_{MU}\|OtherInformation)_{k_i}$ をFAに送信する．ここで，x_i は乱数，k_i は i 回目のデータ通信に用いる鍵を指す．FAは $TCert_{MU}$ の正当性を確認し，正しければ k_i を以下の k_{i+1} に更新する.
$$k_{i+1}=h(h(h(N\|ID_{MU}))\|x\|x_i),(i=0,1,2...)$$

Table 1 本論文で使用する記号の定義

ID_A	A の識別子
$h(\bullet)$	一方向性ハッシュ関数
$h(x,y,\ldots)$	あるデータ $x,y,\ldots$ を連結し，$h(\bullet)$ に入力したときのハッシュ値．入力データの個数は１以上の任意の値とする．
$(x)_k$	鍵 k により共通鍵暗号で x を暗号化
$E_k(x)$	鍵 k により公開鍵暗号で x を暗号化
S_A,P_A	A の秘密鍵，公開鍵
$X\rightarrow Y:Z$	X が Y に Z を送信（安全でない通信路）
$\|$	連結を示す演算子
$\oplus$	XOR演算子

３．従来方式の欠点

本章では匿名認証方式が満たすべき目標を述べた後，Wuらの方式の欠点およびKangらの方式とLeeらの方式の概略と欠点を述べる.

３．１ 目標

Table 2に目標の一覧を示しており，各方式が達成できていない目標には‘X’を記している．各方式のセッション鍵更新フェイズの安全性はLeeらにより検証されているため[4]，全ての目標は認証処理に関する目標である．以下に各目標の説明を与える.

- **固定値：** MUが送受信するデータに固定値が含まれていると，FAは固定値をもとにMUの通信を追跡できる．通信データは認証する度に更新すべきである.
- **HAに所属するAD：** ADはHAに所属しており，MUの通信

を盗聴できると仮定する．AD自身の秘密情報とMUの通信データから ID_{MU} が求まってはいけない．

- **改ざん攻撃：** ADはHAに所属していないものとする．MUが送受信するデータをADが改ざんしたとしても，MUとHAは改ざんを検知できなければいけない．
- **パスワード推測攻撃：** ADはHAに所属していないものとする．ADはMUの通信を盗聴できると仮定する．通信データから総当たり攻撃で PW_{MU} が推測できてはいけない．
- **認証データベース：** HAがMU毎に秘密情報を保存すると，MUの数が多くなるにつれHAの記憶容量や検索などのコストが増えてしまう．HAは認証データベースを保持するべきではない．
- **MUの有効期限：** これはKangらの方式の目標である．MUに対して有効期限を設定できることが望ましい．有効期限を過ぎた後，HAはMUを認証しない．

３．２ Wuらの方式の検証

Wuらの方式が目標を達成しているかを検証する．Wuらの方式はMUが送信する n が固定値である．加えて，次に示す手順によりHAに所属するADに ID_{MU} が漏えいする．ADは $r \oplus PW_{AD} \oplus ID_{HA} \oplus ID_{AD}$ を計算することで $h(N \| ID_{HA})$ を取得する．次に，ADはMUの n を盗聴することで $n \oplus h(N \| ID_{HA}) \oplus ID_{HA}$ から ID_{MU} が求まる．改ざん攻撃に対しては安全であるとLeeらにより指摘されている[4]．HAは認証データベースを利用していない．

３．３ Kangらの方式の概要と検証

Kangらは安全な匿名認証とMUに有効期限を与えるためにWuらの方式を改良した．Wuらの方式に対する改良点は次の通りである．r を $r_1 = h(N \| ID_{HA})$ と $r_2 = h(N \| ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$ に置き換え，n を $h(T_{MU} \| r_1) \oplus ID_{HA} \oplus ID_{MU}$ に置き換えた．Kangらの方式は T_{MU} により n が認証毎に更新されるため固定値の問題を解決している．しかしながら，ADは r_1 を保持しているため $n \oplus h(T_{MU} \| r_1) \oplus ID_{HA}$ から ID_{MU} を求めることができる．ここで，n はMUの通信データである．有効期限に関しては，Kangらが有効期限の仕組みを与えているわけではない．有効期限が切れた後，秘密情報を取り出せないデバイスの存在を仮定しているだけで，目的を達成しているとは言い難い．

３．４ ユーザの有効期限を与える上での困難性

MUに有効期限を与えることは課金サービスなどを実現するために必要となる．自明な方法としてはHAに有効期限のデータベースを持たせることが考えられる．HAはMUを認証するときにデータベースを検索し有効期限を判定する方法である．しかしながら，有効期限のためにデータベースを利用する方法では，Zhuらの方式の認証データベースを利用しないという利点を活かすことができない．そこで，MUのモバイル端末に有効期限を保存しておき，認証時にHAに有効期限を伝える方法が考えられる．このとき，MUが有効期限を改ざんができない仕組みを設ける必要がある．

３．５ Leeらの方式の概要と検証

Wuらの方式では全てのMUが $h(N \| ID_{HA})$ を共有していたため，HAに所属するADに対してMUの匿名性が確保できていなかった．これを解決するためにLeeらは認証毎に変化するテンポラリIDを導入した．

Leeらの方式はMUがテンポラリID q_i と，HAがMU毎に $(h(q_i), ID_{MU}, PW_{MU})$ をデータベースに保存している．ここで，PW_{MU} はMUが設定した任意のパスワードである．認証処理では，MUは ID_{MU} と PW_{MU} を入力して，$L = h(T_{MU} \oplus PW_{MU})$ を計算する．MUは q_i と $(h(ID_{MU}) \| x \| x_0)_L$，その他のデータをFA経由でHAに送信する．HAは $h(q_i)$ によりデータベースを検索する．正規のMUであれば検索が成功し，取り出した ID_{MU} と PW_{MU} を用いてMUを認証する．認証が完了した後，MUとHAは q_i を $q_{i+1} = h(q_i \| PW_{MU})$ に更新する．

Leeらの方式は q_i やその他の情報が認証毎に更新されるため固定値の問題を解決している．また，HAに所属するADが q_i を盗聴したとしても PW_{MU} が分からなければ固定値である $h(ID_{MU})$ を取得できないため，HAに所属するADに耐性がある．しかしながら，Leeらの方式はHAがデータベースを用いる必要があること，パスワード推測攻撃に耐性がないことが課題として挙げられる．以下の手順によりMUの通信データからパスワードを推測される危険がある．

Leeらの方式に対するパスワード推測攻撃

1. ADは i 回目の認証においてMUの通信データ T_{MU} と $(h(ID_{MU}) \| x \| x_0)_L$ を盗聴する．それぞれを T_{MU}^i，$(h(ID_{MU}) \| x^i \| x_0^i)_{L^i}$ とする．ここで，$L^i = h(T_{MU}^i \oplus PW_{MU})$ である．
2. ADは $i+1$ 回目の認証において T_{MU} と $(h(ID_{MU}) \| x \| x_0)_L$ を盗聴する．それぞれを T_{MU}^{i+1}，$(h(ID_{MU}) \| x^{i+1} \| x_0^{i+1})_{L^{i+1}}$ とする．ここで，$L^{i+1} = h(T_{MU}^{i+1} \oplus PW_{MU})$ である．
3. ADは任意のパスワードを PW'_{MU} として，$(L^i)' = h(T_{MU}^i \oplus PW'_{MU})$ と $(L^{i+1})'' = h(T_{MU}^{i+1} \oplus PW'_{MU})$ を計算する．$(L^i)'$ で $(h(ID_{MU}) \| x^i \| x_0^i)_{L^i}$ を復号して得られた値を $(h(ID_{MU}))' \| (x^i)' \| (x_0^i)'$ とし，$(L^{i+1})''$ で $(h(ID_{MU}) \| x^{i+1} \| x_0^{i+1})_{L^{i+1}}$ を復号して得られた値を $(h(ID_{MU}))'' \| (x^{i+1})'' \| (x_0^{i+1})''$ とする．
4. $(h(ID_{MU}))'$ と $(h(ID_{MU}))''$ が一致したならば PW'_{MU} は PW_{MU} である．一致しなければ，3. へ戻り異なるパスワードを試行する．

（手順は以上）

一般にMUは記憶する煩雑さを避けるため，単純な推測しやすいパスワードを設定する傾向がある．そのため，上記のように総当たりすることで PW_{MU} が求まることは十分に考えられる．AD が PW_{MU} を取得すると，MUの匿名性が確保できないだけでなく，x と x_0 が取得できるためADがMUになりすますことが可能となる．

３．６ パスワードの利便性と安全性の考察

Wuらの方式とKangらの方式は PW_{MU} を $h(N \| ID_{MU})$ としており，MUのデバイスには保存されていない．認証処

理の開始時にMUが PW_{MU} を入力する必要があるが，ハッシュ値は不規則な文字列であるため人が記憶することは困難である．そのため，PW_{MU} を記憶するデバイスを別途用意するなどの必要がある．これに対して，Leeらは PW_{MU} をMUが選択した任意のパスワードにすることでより実用的な方式に改良した．しかしながら，3.5節で指摘したパスワード推測攻撃に対する脆弱性がある．MUが設定するパスワードに安全性の強度が依存するようでは，認証にデバイスを用いる利点が十分には活かされているとは言い難い．MUが任意のパスワードを設定でき，かつ，安全性の強度がパスワードに依存しないよう設計することが望ましい．

Table 2 従来方式の欠点

	Wu	Kang	Lee
固定値	X		
HAに所属するAD	X	X	
改ざん攻撃			
パスワードの利便性	X	X	
パスワード推測攻撃			X
認証データベース			X
MUの有効期限	—	X	—

X：達成できていない目標
—：考慮していない目標

４．提案方式

４．１ 概要

提案方式は3.1節の目標を全て達成している．提案方式の要点は次の通りである．提案方式ではHAが認証データベースを保持していないため，MUが自身の認証情報をHAに伝える必要がある．提案方式ではMU毎に異なる認証情報 $V_{MU}=(ID_{MU}\|h(PW_{MU})\|t_{MU}\|\ M_{MU})_N$ をMUに与える．ここで，PW_{MU} はMUが設定する任意のパスワード，M_{MU} は乱数，t_{MU} がMUの有効期限を示す．t_{MU} は暗号化されているためMUは改ざんすることができない．認証処理のときに，MUは V_{MU} をHAに送信することで認証に必要な情報を伝える．加えて，認証が完了したあとHAは新たな乱数 M'_{MU} を生成し，V_{MU} を $V'_{MU}=(ID_{MU}\|h(PW_{MU})\|t_{MU}\|M'_{MU})_N$ として更新することで，固定値になることを防ぐ．パスワード推測攻撃に対しては M_{MU} を利用することで防ぐ．Leeらの方式では $L=h(T_{MU}\oplus PW_{MU})$ としているが，提案方式では $L=h(T_{MU}\oplus M_{MU})$ とする．

４．２ プロトコル

4.2.1 登録処理

MUは ID_{MU} と PW_{MU} をHAに送信する．ここで，PW_{MU} はユーザが設定した任意のパスワードである．HAは乱数 M_{MU} を生成したあと，ユーザの有効期限 t_{MU} を生成する．次に，ID_{HA} と $V_{MU}=(ID_{MU}\|h(PW_{MU})\|t_{MU}\|M_{MU})_N$，$M_{MU}\oplus h(PW_{MU})$ をMUのデバイスに保存しMUにデバイスを配布する．このとき，HAは ID_{HA} と N を保持している．

4.2.2 認証処理

1. MUは ID_{MU} と PW_{MU} を入力する．
2. $h(PW_{MU})$ を求めてから，以下により M_{MU} を取得する．
   $M_{MU}=(M_{MU}\oplus h(PW_{MU}))\oplus h(PW_{MU})$
3. MUは現在時刻 T_{MU} を取得してから，$L=h(T_{MU}\oplus M_{MU})$ と $\alpha=(h(ID_{MU})\|x_0\|x)_L$ を計算する．
4. MU → FA: V_{MU}，α，ID_{HA}，T_{MU}．
5. FAは T_{MU} の正当性を確認する．正しければ，FAは乱数 b を生成し，デジタル署名 $Cert_{FA}$ と検証子 $E_{S_{FA}}(h(b,\alpha,V_{MU},ID_{HA},T_{MU}))$ を生成する．
6. FA → HA: b，α，V_{MU}，ID_{HA}，T_{MU}，$Cert_{FA}$，T_{FA}，$E_{S_{FA}}(h(b,\alpha,V_{MU},ID_{HA},T_{MU}))$．
7. **情報の取得:** HAは T_{FA} と $Cert_{FA}$ の正当性を確認する．それらが正しければ，HAは N を用いて V_{MU} を復号することにより ID_{MU}，$h(PW_{MU})$，t_{MU}，M_{MU} を取得する．次に，L を計算し α を復号することで $h(ID_{MU})$，x_0，x を取得する．
8. **MUの認証:** HAは V_{MU} に含まれていた ID_{MU} のハッシュ値を計算し，α に含まれていた $h(ID_{MU})$ と比較する．ハッシュ値が一致すれば，t_{MU} によりMUの有効期限内を確認する．有効期限内であればMUを認証する．
9. **情報の更新:** HAは乱数 M'_{MU} を生成してから，$V'_{MU}=(ID_{MU}\|h(PW_{MU})\|t_{MU}\|M'_{MU})_N$ を計算する．次に，$\beta=(V'_{MU}\|M'_{MU}\|PV)_L$ を作成する．ここで，PV は改ざんを検知するための公開値である．
10. **FAが利用する情報の作成:** HAは $h(ID_{MU}\|x)$，$E_{P_{FA}}(h(ID_{MU}\|x)\|x_0)$ を作成する．
11. HAは乱数 c を生成し，デジタル署名 $Cert_{HA}$ と S_{HA} により検証子を生成する．
12. HA → FA: b，c，β，$E_{P_{FA}}(h(ID_{MU}\|x)\|x_0)$，$Cert_{HA}$，$T_{HA}$，$E_{S_{HA}}(h(b,c,\beta,E_{P_{FA}}(h(ID_{MU}\|x)\|x_0),Cert_{HA}))$．
13. FAは T_{HA} と $Cert_{HA}$ の正当性を確認する．それらが正しければ，FAは認証子 $TCert_{MU}$ を生成する．次に，FAは S_{FA} により $E_{P_{FA}}(h(ID_{MU}\|x)\|x_0)$ を復号してから，$k=h(h(ID_{MU}\|x)\|x_0)$ と $(TCert_{MU}\|h(x_0))_k$ を作成する．
14. FA → MU: β，$(TCert_{MU}\|h(x_0))_k$．
15. MUは k を計算し $(TCert_{MU}\|h(x_0))_k$ を復号する．次に，$h(x_0)$ を計算し，復号した $h(x_0)$ と比較する．一致すればMUはFAを認証する．MUは β を復号して PV が正しければ V_{MU} を V'_{MU} に，$M_{MU}\oplus h(PW_{MU})$ を $M'_{MU}\oplus h(PW_{MU})$ に更新する．

4.2.3 管理フェイズ

- セッション鍵の更新

セッション鍵の更新はLeeらの方式と同じである．MUはFAとデータ通信を行うとともにセッション鍵を更新する．MUは $(x_i\|TCert_{MU}\|OtherInformation)_{k_i}$ をFAに送信する．ここで，x_i は乱数，k_i は i 回目の認証セッションに用いる鍵を指す．FAは $TCert_{MU}$ の正当性を確認し，正しければ k_i を $k_{i+1}=h(h(ID_{MU}\|x)\|x_i)$ に更新する．

- PW_{MU} の更新

この処理は認証処理と似ているため差異を示す．MUは V_{MU}，$\alpha'=(h(ID_{MU})\|x_0\|x\|PW'_{MU})_L$，$ID_{HA}$，$T_{MU}$ をFA経由でHAに送信する．ここで，PW'_{MU} はMUの新しいパス

ワードである．HAはMUを認証した後，$\tilde{V}_{MU}=(ID_{MU}\|h(PW'_{MU})\|\ t_{MU}\|M'_{MU})_N$ と $\tilde{\beta}=(\tilde{V}_{MU}\|M'_{MU}\|PV)_{L'}$ を作成して，その他の情報とともにFAを経由してMUに送信する．ここで，$L'=h(T_{MU}\oplus PW'_{MU})$ である．MUは $\tilde{\beta}$ を復号し PV が正しければ V_{MU} を $\tilde{V}_{MU}$ に，$M_{MU}\oplus h(PW_{MU})$ を $M'_{MU}\oplus h(PW'_{MU})$ に更新する．

５．安全性の検証と性能評価

本章では提案方式が安全であることを示し，従来方式と性能の比較を行う．

５．１ 安全性の検証

- **固定値：** FAは手順4で $V_{MU}=(ID_{MU}\|h(PW_{MU})\|t_{MU}\|M_{MU})_N$ と $\alpha=(h(ID_{MU})\|x_0\|x)_L$ を取得できる．これらの値は，M_{MU} と x_0，x により認証毎に更新される．手順14で $\beta=(V'_{MU}\|M'_{MU}\|PV)_L$ と $(TCert_{MU}\|h(x_0))_k$ を取得することができる．これらは，M_{MU} と x_0 により更新される．よって，FAが取得できるデータに固定値は含まれていない．
- **HAに所属するAD：** 提案方式ではMU毎に異なる値を与えている．MUが暗号化している通信データはADの秘密情報を用いて復号されることはない．そのため，MUの送受信データをADが盗聴しても ID_{MU} が取得できないことを示す．ADは手順4で V_{MU}，α を盗聴できる．しかしながら，これらの値はそれぞれ N と L で暗号化されているため入力値がADに知られることはない．ADは手順14で β，$(TCert_{MU}\|h(x_0))_k$ を盗聴できる．しかしながら，これらの値はそれぞれ L と k により暗号化されているため入力値がADに知られることはない．
- **改ざん攻撃：** ADが手順4で V_{MU}，α，T_{MU} のいずれかを改ざんしたとすると，手順8で $h(ID_{MU})$ の比較で一致しないためHAは改ざんを検知することができる．ADが手順14で $\beta=(V'_{MU}\|M'_{MU}\|PV)_L$ と $(TCert_{MU}\|h(x_0))_k$ を改ざんすると，β は PV により改ざんを検知でき，$(TCert_{MU}\|h(x_0))_k$ は $h(x_0)$ により改ざんを検知できる．
- **パスワード推測攻撃：** M_{MU} は十分に長いビット長を持つ乱数とする．ADが $(h(ID_{MU})\|x_0\|x)_L$ を盗聴したとしても，L は乱数 M_{MU} を基に作成されているため，3.5節のような総当たり攻撃で求めることは困難である．

以上のことから提案方式は安全な方式である．

５．２ 性能評価

Table 3に認証処理で使用される各演算の回数を示す．表中の‘Sym’は共通鍵暗号，‘Asym’は公開鍵暗号を意味する．提案方式ではMUの演算の回数が他の方式と比べて多い．例えば，Leeらの方式と比較すると，ハッシュ関数が1回，共通鍵暗号が1回，XOR演算子が2回増えている．これは手順2や手順15で M_{MU} に関する演算が主な要因である．演算回数は増加しているがパスワード推測攻撃に対する耐性を持たせるために必要な処理である．HAの演算回数はハッシュ関数の呼び出し回数を他の方式と比べ1回削減しているものの，共通鍵関数の呼び出しが３回，乱数の生成が１回多い．これは V_{MU} の更新が主な要因である．V_{MU} はHAが認証データベースを持たせないために必要である．Leeらの方式のように認証データベースを保持するとMUの数が多くなるにつれHAの記憶容量や検索などのコストが増えてしまう．

結　　言

Kangらの方式ではHAに所属するMU間で匿名性が確保できておらず，有効期限がMUのデバイスの機能に依存していることが課題として挙げられる．Leeらの方式ではパスワード推測攻撃に耐性がなく，HAが認証データベースを保持していることが課題である．提案方式はこれらの課題を全て解決している．従来方式に比べ，MUやHAの演算回数は多少増加するものの，より安全な認証が可能となる．提案方式は無線LANサービスを始めとして様々な無線サービスのセキュリティ基盤の構築に利用できる．

Table 3 各方式の性能評価

		Wu	Kang	Lee	Our
MU	Hash	4	6	6	7
	Sym	2	2	2	3
	XOR	2	3	1	3
	Rand	2	2	2	2
FA	Hash	4	4	4	4
	Sym	1	1	1	1
	Asym	3	3	2	2
	XOR	0	0	0	0
	Rand	1	1	1	1
HA	Hash	6	6	6	5
	Sym	1	1	1	4
	Asym	3	3	3	3
	XOR	3	3	1	1
	Rand	1	1	1	2
	Table	—	—	Use	—

Literature Cited

1) J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environment,” IEEE Trans. Consum. Electron., vol.50, no.1, pp.231-235, June 2004.
2) C.C. Wu, W.B. Lee, and W.J. Tsaur, “A secure authentication scheme with anonymity for wireless communications,” IEEE Commun. Lett., vol.12, no.10, pp.722-723, Oct. 2008.
3) M. Kang, H.S. Rhee, and J.Y. Choi, “Improved user authentication scheme with user anonymity for wireless communications,” IEICE Trans. Fundamentals, vol.E94-A, no.2, pp.860-864, Feb. 2011.
4) J. Lee and T. Kwon, “Secure authentication scheme with improved anonymity for wireless environments,” IEICE Trans. Commun., vol.E94-B, no.2, pp.554-557, Feb. 2011.

伊沢　亮一／神戸大学大学院工学研究科・システム情報学研究科紀要　第 3 号　47～53 頁（2011）

Secure Anonymous Authentication Scheme with Expiration Date for Wireless Environments

Ryoichi ISAWA[1] and Masakatu MORII[2]

[1]*Graduate School of Science and Technology, Department of Informatics and Electronics*

[2] *Graduate School of Engineering, Department of Electrical and Electronic Engineering*

Key words: anonymity, mutual authentication, key establishment, wireless communication, internet protocol

Authentication scheme with user anonymity is an important area of research. In particular, it is required in wireless environments, because an adversary can intercept a user's identity from a wireless network easier than a wired network. An adversary can localize the user using the intercepted identity. In order to avoid such risks, Zhu et al. proposed an anonymous authentication scheme. In their scheme, there are mobile users, foreign agents, and one home agent. When a mobile user visits a foreign agent, the home agent tries to authenticate the user instead of the foreign agent. In exchange for the existence of the home agent, the user does not have to use public key cryptosystems like groups signatures. Because Zhu et al.'s scheme has security weaknesses, Kang et al. and Lee et al. improved Zhu et al.'s scheme independently. In addition to improved security, Kang et al. aim for giving expiration date to the mobile user. However, they just assume that the user's device does not work if it is expired. On the other hand, Lee et al. apply user-chosen passwords. Unfortunately, their scheme is not secure against password guessing attacks. In this paper, we propose a secure anonymous authentication scheme with expiration date. The proposed scheme can overcome the disadvantages of Kang et al. and Lee et al.