バイオメトリクスを用いた Secure Shell リモートログイン認証 *

古川 英雄† 塙 敏博‡

概要 個人の持つ生体の特徴を利用したバイオメトリクス認証技術がログイン認証に利用されてきているが，リモートログインに利用する場合には，ネットワークを経由することからバイオメトリクスの特徴点データやテンプレートの安全性を確保するために，バイオメトリクスを直接利用するのではなく，PKI と組み合わせての利用が提案されている．

そこで， UNIX で良く用いられる Secure Shell における公開鍵暗号方式の秘密鍵管理にバイオメトリクスを用いることで，バイオメトリクスを リモートログイン認証に利用するシステムを実装した．

Secure Shell をベースに LDAP を用いた認証局を設けて公開鍵を登録し，秘密鍵を用いた処理は全て IC カードがおこなうことで安全性を確保することができる．

1 はじめに

従来，コンピュータシステムへのログインには，主にパスワード認証が用いられてきた．これは本人だけがパスワードを知っていることを前提にした認証方法であり，パスワードを推測され，アカウントを不正に利用されたり，本人がパスワードを忘れる，といった問題があった．

近年，個人の持つ生体の特徴を利用したバイオメトリクス認証技術がログイン認証に利用されてきている．これにより，アカウントの不正利用が困難となり，複数のパスワードを使い分ける必要もなくなる．

しかし，リモートログインに利用する場合には，ネットワークを経由することからバイオメトリクスの特徴点データの安全を確保する必要がある．そのため， PKI とバイオメトリクスを組み合わせる方法が提案され [2]，実際に組み合わせた製品も提供され始めている [5].

そこで，本研究では UNIX システムへのリモートログインによく用いられている Secure Shell に，PKI とバイオメトリクスとを組み合わせた認証を取り入れることで，既存のアプリケーションとの親和性を保ったまま，バイオメトリクスの持つ安全性や利便性を得ることを目的とする．

同時に，様々な情報の集中管理や，オープンソースのソフトウェアをできるだけ利用することで，管理コストの軽減を図る．

2 SSH (Secure Shell)

UNIX システムへのリモートログインには主に telnet, rlogin, SSH (Secure Shell) などが用いられている．ただし telnet と rlogin は通信路が暗号化されず，パスワードの盗聴の危険性などセキュリティ上の問題があるため，近年は SSH が多く用いられている．

SSH は暗号化された通信路を用いており，認証方法には，プレインテキストによりパスワード文字列を送受信する方法，RSA などの公開鍵暗号方式を用いる方法，などを利用することができる．

プレインテキストを用いた場合にもパスワードが直接見えてしまうことは無いが，通常，パスワードとしては長い文字列を使用しないため，辞書攻撃やブルートフォースアタックなどに対して脆弱である．

公開鍵暗号方式はプレインテキストを用いた場合に比べて安全性は高い．しかしながら秘密鍵をクライアントに保存しておく必要があり，秘密鍵が第 3 者に盗み出された場合には危険である．

SSH には秘密鍵の取り扱いを容易にする ssh-agent というエージェントが用意されている．ssh-agent はユーザの秘密鍵を記憶しており，秘密鍵をエージェントの外に出すことなく公開鍵暗号方式の認証をおこなうことができる．

3 バイオメトリクスのリモートログイン認証への利用

コンピュータへのログインの際に，バイオメトリクスをユーザ認証に利用する方法として，

1. バイオメトリクスの特徴点データを認証サーバに送信
2. ログイン元端末自身で認証
3. 認証サーバからテンプレートを受信して端末で認証
4. バイオメトリクス装置内で認証し結果を端末に送る

が考えられる．このうち，1，3 の方法のようにバイオメトリクスの情報がネットワークを流れると，バイオメトリクスの「特徴点データやテンプレートの変更が困難である」という点から通信路を暗号化した場合でも，万が一盗聴さ

---

*An authentication system using biometrics for remote login with Secure Shell

†東京工科大学 大学院 工学研究科

‡東京工科大学 コンピュータサイエンス学部

れると危険となる．また，サーバに個人のバイオメトリクス情報が格納されていることには，抵抗が大きいと予想される．2 の場合は，複数の端末がある場合に管理が困難になるという問題がある．

さらに，バイオメトリクスによる認証をリモートログインに利用する場合には，ネットワーク上を流れるデータと認証を行なう場所によって，様々な組合せが考えられる．この場合もネットワーク上にバイオメトリクスによる特徴点データが流れるのは望ましくない．

そこで，ネットワーク上にバイオメトリクスに基づく情報を流さず，安全に認証情報だけを交換するために，公開鍵暗号方式を利用し，秘密鍵の利用を許可するためにバイオメトリクスを用いる [1, 2].

3.1 バイオメトリクスによる秘密鍵の管理

バイオメトリクスによる秘密鍵の管理を行なう場合でも，秘密鍵を用いた暗号操作を計算機上で行なう場合には，計算機の安全性が確保できない場合に，秘密鍵が危険になってしまうという問題がある．

そこで本研究では，IC カード内に秘密鍵を保存しておき，カード内でそのまま暗号操作を行なうことができる Standard-9 IC カード [5] を利用する．

その際，秘密鍵の有効化に PIN の替わりにバイオメトリクスによる認証を利用することのできるシステムを用いるのが望ましい．

IC カードに保存できる秘密鍵の数が限られるため，多数のシステムにログインする場合に用いるのは困難であるが，IC カードが ID として使われている場合を想定すると，IC カードの利用範囲を 1 組織と仮定しても差し支えないと考えられる．

3.2 バイオメトリクス認証の有効期間

秘密鍵の操作を行なうためにバイオメトリクスによる認証が成功した後，その認証の権限をいつまで残すかを考慮しなければならない．

1. 認証後 1 回のみ
   この方法では，認証が成功して秘密鍵の利用を 1 回行なった時点で権限が無くなる．利用者が席を離れた際などに秘密鍵が利用可能な状態で残ることは無いが，秘密鍵を利用する場合に毎回認証が必要になり，利用者に負担をかける．
2. 一定時間有効
   この方法では，認証が成功してから一定時間が経過するまで，権限が残る．利用者が席を離れた際などに秘密鍵が利用可能な状態で残ってしまう．

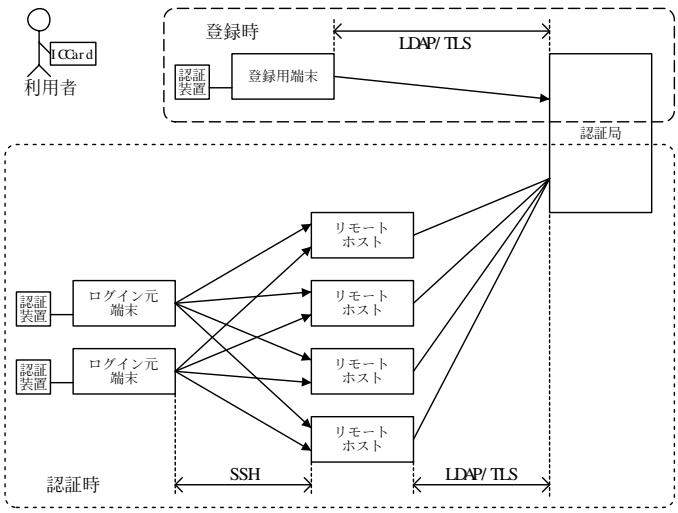

図 1: 構成要素

3. 利用者が無効にするまで有効
   この方法では，利用者が意図的に無効にするまで，権限が残る．利用者が無効にせずに席を離れた際などに秘密鍵が利用可能な状態で残ってしまう．
4. 認証装置から IC カードを取り出すまで有効
   この方法では，利用者が IC カードを認証装置から取り出すまで有効になる．IC カードを常に持ち歩くのであれば，利用者が席を離れる際に秘密鍵が利用可能な状態で残ることは無い．

利用者に応じて 4 の方法と 1〜3 の方法を組み合わせて利用することが望ましいため，組み合わせと有効期間情報を IC カードに記録しておく．

4 設計と実装

本研究では，バイオメトリクス認証装置と IC カードリーダとを組み合わせて， SSH による UNIX リモートログインに応用する．

あらかじめ， IC カードに管理者がバイオメトリクスの特徴点データと，社員番号や学籍番号など組織内で一意に決められる識別情報を書き込んでおく必要がある．その後利用者は，登録用端末を利用して SSH の認証に利用する公開鍵と秘密鍵のペアを作成し，公開鍵を認証局に，秘密鍵を IC カードに，それぞれ登録する．

利用時には手元の端末（ログイン元端末）でバイオメトリクス認証をおこない，許可されると IC カード中の秘密鍵を SSH の認証に利用する．

リモートホストでは，識別情報を元に該当する利用者の公開鍵を認証局から取り出し， SSH の認証をおこなう．

4.1 構成要素

この認証方法に必要な構成要素を図 1 に示す.

認証局と登録用端末，リモートホストは組織の管理者が運用をおこなう必要がある．ログイン元端末とバイオメトリクス認証装置は，組織の管理者が運用をおこなう必要はない.

認証局 UNIX で通常利用されているユーザの情報と公開鍵証明書を関連付けて保存するため， LDAP を利用する.

LDAP は多数の OS やアプリケーションにまたがるアカウントなどの情報を一元管理するためのディレクトリアクセス用プロトコルであり，従来の UNIX のログイン認証の際に必要な情報だけでなく，メールアドレスなどの様々な情報を管理することができる．オブジェクトクラスとして posixAccount を利用し，これに証明書を利用するための userCertificate 属性を追加する.

IC カードと IC カードリーダ カード内で秘密鍵操作が可能な Standard-9 を利用する．その際に，バイオメトリクスによる認証を行ない，正当な利用者であれば，秘密鍵操作を可能とする.

登録用端末 信頼できる登録用端末を用意し，ユーザは IC カードとバイオメトリクスにより認証される．SSH の認証に利用する秘密鍵と公開鍵のペアを IC カード内で作成し，秘密鍵はそのまま IC カードに保存する．公開鍵は IC カード中の識別情報を元に LDAP を用いて認証局へ登録する.

この方法はユーザの権限で IC カードに書き込むため，管理者が立ち会う必要がなく，任意に公開鍵と秘密鍵のペアの再作成が可能になる.

ログイン元端末 手元の端末でバイオメトリクスによる認証をおこなって秘密鍵を利用可能状態にする.

秘密鍵は，IC カードに記録されている有効期限内であれば再度の認証無しで利用でき，期限が切れると再度認証を要求する.

ssh-agent が秘密鍵を利用した処理の依頼を受け取ると，IC カード内で 秘密鍵操作を実行する．ここでは， ssh-agent から Standard-9 対応の IC カードを操作し，秘密鍵が必要な処理を IC カードに依頼する.

リモートホスト ログイン元端末からの SSH 接続要求を受け，公開鍵を認証局から取り出し，ログイン元端末に署名要求を送信する．ログイン元端末から署名結果を受け取ると，公開鍵を利用して検証し，認証をおこなう.

4.2 検証のための実装

本手法では IC カードから，秘密鍵を取り出さずに秘密鍵操作が可能で，かつバイオメトリクスによる認証によって操作を許可するものが必要であるが，実際にそのような装置が入手できなかったため，2 通りの実装をおこない検証を行なった.

実装 1： バイオメトリクス認証の後，通常の IC カードから秘密鍵を取り出し外部で操作を行う

実装 2： バイオメトリクスを使わずに Standard-9 IC カードを単独で用いて内部で秘密鍵操作を行う

4.2.1 実装 1

利用する生体の特徴は指紋である．登録用端末では，SSH の認証に利用する秘密鍵と公開鍵のペアを IC カード内ではなく登録用端末自体で作成する点が異なる．また，ログイン元端末では， IC カードに秘密鍵操作を依頼するのではなく，あらかじめ， IC カード内に保存してある秘密鍵をバイオメトリクスによる認証をおこなって取り出し，端末内で操作をおこなう点が異なる.

4.2.2 実装 2

登録用端末とログイン元端末で，秘密鍵操作や正当な利用者かどうか確認するために，バイオメトリクスによる認証ではなく， PIN による認証をおこなう点が異なる.

4.2.3 共通項目

ログイン元端末 認証装置のドライバが提供されている Windows を対象とし，SSH の実装として PuTTY[4] を採用した．さらに pagent と呼ばれる ssh-agent を用いて，IC カードを利用した秘密鍵操作がおこなえるように変更した.

認証局 LDAP の実装には，OpenLDAP を利用し，LDAP 認証局の認証，認証局と端末間の通信の暗号化には，TLS (Transport Layer Security) プロトコルを用いた.

リモートホスト SSH の実装として LDAP から公開鍵を読み出すことができる，OPENSSH LDAP PUBLIC KEY PATCH[3] を適用した OpenSSH を採用した.

これにより，ログイン元端末で入力したユーザ名に該当する公開鍵を認証局から取り出し，正当な利用者かどうか確認をすることができる.

表 1: 実装環境

リモートホスト・認証局	
OS	FreeBSD 5.2.1-RELEASE
LDAP Server/Client	OpenLDAP 2.2.2beta
SSH Server	OpenSSH 3.7.1p2, OPENSSH LDAP PUBLIC KEY PATCH 2.01
ログイン元端末の環境	
CPU	PentiumM 1.8GHz
RAM	512MByte
LAN	100BASE-TX
OS	Windows XP SP2
SSH Client	PuTTY 0.54
実装 1 認証装置	IC カードリーダ内蔵型指紋認証装置 (株) NTT データ SmartBIO
実装 2 認証装置	IC カードリーダライタ (Standard-9 用) 三菱電機 (株) RWD5000-M
公開鍵暗号方式	RSA（SSH2 用，鍵長 1024 ビット）

表 2: 秘密鍵の有効化にかかる時間

認証方法	所要時間
バイオメトリクス（実装 1）	7 秒+再試行 1 回につき 5 秒
PIN 入力（実装 2）	2〜5 秒

5 評価

実環境で運用した際の認証時間を検討するために，現時点で実装が完了している 2 種類の実装による，ログイン元端末での処理時間の測定をおこなった．評価に利用した環境を表 1 に示す．

5.1 秘密鍵の有効化にかかる時間

ログイン元端末で秘密鍵の有効化に要する時間を評価するため，実装 1，実装 2 で秘密鍵の有効化に必要な時間を測定した．結果を表 2 に示す．

このことから PIN による認証をバイオメトリクスによる認証に置き換えても，7 秒+再試行時間で認証を完了できると考えられる．

5.2 公開鍵暗号方式による認証にかかる時間

ログイン元端末で秘密鍵操作に要する時間を評価するため，実装 2 と従来の方法で認証にかかる時間を測定した．

pagent 内で RSA による署名の開始から終了までの時間を，表 3 に示す．

表 3: RSA による署名時間

鍵操作場所	所要時間
従来の方法	平均 0.45 秒
IC カード内	平均 0.60 秒

平均 0.15 秒認証時間が増えてはいるが，1 秒以内に認証が終了しているので，問題ないと考えられる．

5.3 対応するアプリケーション

各アプリケーションを変更するのではなく，ssh-agent を変更したため，PuTTY 以外でも WinSCP，PortForwarder 等のアプリケーションがそのまま利用可能である．

今後 ssh-agent 対応のアプリケーションが増えた際にも，個別に対応する必要が無い．

5.4 利用者による評価

利用者による評価は，パスワード認証を利用する場合や，公開鍵暗号方式単体で利用する場合と比較してアンケートをとることを検討中である．

6 まとめ

本研究では，UNIX の Secure Shell リモートログイン認証の秘密鍵管理に IC カードとバイオメトリクスによる認証を組み合わせたシステムを実装することで，バイオメトリクスを用いたリモートログイン認証を実現した．

ssh-agent に IC カードとの通信機能を持たせることで，ssh-agent 以外の部分に変更を加えることなく，リモートログイン先からさらにリモートログインを行なう場合でも，秘密鍵を用いた処理を ssh-agent に代行させ，秘密鍵の安全性を高めることができる．

バイオメトリクスを IC カード内の秘密鍵管理に利用することで，ログイン後も一定時間毎に公開鍵方式の認証を行うよう Secure Shell を変更しても，パスワードを入力したり，ファイルで秘密鍵を管理する方法と比べて容易に実現することができる．

参考文献

[1] 古川英雄，塙敏博:バイオメトリクスを用いた UNIX リモートログイン認証方法の提案，分散システム／インターネット運用シンポジウム 2004 論文集， pp.1-6，2004 年 1 月

[2] Andrew Nash， William Duane， Celia Joseph， Derek Brink，(株) スリー・エー・システムズ訳: PKI e セキュリティの実装と管理，翔泳社，pp.304,330，2002 年 4 月

[3] Eric AUGE: OPENSSH LDAP PUBLIC KEY PATCH, http://ldappubkey.gcu-squad.org/

[4] PuTTY: A Free Telnet/SSH Client, http://www.chiark.greenend.org.uk/~sgtatham/putty/

[5] 三菱電機：三菱電機 セキュアトークン, http://www.mitsubishielectric.co.jp/security/platform/ic/index_b.html