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

古川 英雄† 塙 敏博††

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，Windowsでのみ利用可能なシステムがほとんどであり，UNIXで利用可能なものは少ない．また，UNIXで良く用いられる遠隔地へリモートログイン時には，ネットワークを経由することからバイオメトリクスの持つ安全性を保つことが重要である．そこで，Secure Shellの暗号化通信を元にして，バイオメトリクスを用いた認証をUNIXリモートログイン認証に利用するシステムを提案する．Secure Shellの暗号化通信をベースに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カードが行なうことで安全性を確保することができる．

Proposal on UNIX remote login authentication system using biometrics

HIDEO FURUKAWA† and TOSHIHIRO HANAWA††

A biometric technology is available as the user authentication in case of the login sequence. However, it is important that the secure property of the biometrics is preserved on the occasion of remote login. In this study, we propose the user authentication system for remote login using the biometrics. The public key generated from the biometric template is registered to certification authority using the LDAP, and the public key is transfered through the secure connection based on the Secure Shell. On the other hand, the operation using the private key is treated inside the Smart Card to secure.

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ると同時に複数のパスワードを管理する必要もなくなる．しかし現状では，Windowsでのみ利用可能なシステムがほとんどであり，UNIXで利用可能なものはほとんど存在していない．さらに，遠隔地のUNIXへのリモートログインの際には，ネットワークを経由するため、バイオメトリクスの持つ安全性を保つことが重要である．

そこで，本研究ではバイオメトリクスを用いた認証をUNIXリモートログイン認証に利用し，既存のアプリケーションとの親和性を保ったまま，安全性や利便性を高めることを目的とする．

2. UNIXシステムへのログイン

UNIXシステムのログインには，手元にある端末からのログインと，ネットワークを介したホストへのログインの2種類がある．ここでは前者をローカルログイン，後者をリモートログインと呼ぶことにする．

ローカルログインにおいては，CUIではlogin，GUIではxdm (X Display Manager) やgdm (Gnome Display Manager) のようなディスプレイマネージャが用いられている．

リモートログインにはCUIのtelnet, rlogin, SSH (Secure Shell)[6] 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ていないため，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．一方SSHは暗号化された通信路を用いており，リモートログイン (slogin) だけでなくファイル転送 (scp, sftp)，X-Windowプロトコルパケットの転送なども利用可能である．

† 東京工科大学 大学院 工学研究科
Graduate School of Engineering, Tokyo University of Technology
†† 東京工科大学 コンピュータサイエンス学部
School of Computer Science, Tokyo University of Technology

リモートログイン時の認証方法には，

(1) ホスト名やIPアドレスで接続元の計算機を信頼するrhost方式

(2) 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

(3) RSAなどの公開鍵暗号方式を用いる方法

がある．

このうちrhost形式は，ホスト名やIPアドレスを偽って接続することにより，容易に他のユーザになりすますことが可能となり，危険である．

プレインテキストを用いた場合，telnet, rloginのように通信路が暗号化されていないと，パスワードが文字列として直接見えてしまう．SSHの場合には通信路上では暗号化されるが，通常，パスワードとしては8文字しか使用しないため，ブルートフォースアタックや辞書攻撃などに対して脆弱である．

公開鍵暗号方式は1, 2の方式と比較すると安全性は高い．しかしながら秘密鍵をログイン元の計算機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ために，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，秘密鍵を外に出すことなく，公開鍵を利用して暗号化されたチャレンジを，秘密鍵で復号化してレスポンスとして送り返すことで，リモートログイン先からさらに遠方のホストにリモートログインするような場合にも対応することができる．

ローカルログイン，リモートログイン共に，認証の際は，ユーザ毎にあらかじめ登録されたパスワードに関する情報と，キーボードから入力されたパスワードとの比較を行なう．従来は，パスワード情報は単一のホスト毎に管理するpasswdファイルや，ネットワーク上でユーザ情報を共有するためのNIS (Network Information System)が利用されてきた．

近年は，より柔軟なユーザ管理が可能なLDAP (Lightweight Directory Access Protocol)[1]が用いられるようになってきている．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．

3. バイオメトリクスのログイン認証への利用

3.1 ローカルログイン

従来のパスワード認証に代えて，バイオメトリクスをログイン認証に利用する場合には，認証を行なう箇所，テンプレートを保存する箇所の違いにより，以下の3つの方法が考えられる．

認証サーバによる認証

バイオメトリクスの特徴点データをネットワークを介して認証サーバへ送信し，認証サーバでテンプレートと照合した後，その結果を手元の端末に返答する方法である．

利点として，テンプレートをネットワーク上の1ヶ所のサーバに保存しておくだけで済むが，実際にバイオメトリクスの特徴点データがネットワーク上を流れるため，特徴点データの転送時の安全性確保が大変重要になる．バイオメトリクスデータは本人の不変的な特徴を用いるため，特徴点データを盗聴されるなどして第3者に知られた場合，変更することが非常に難しくシステムが破綻する原因になる可能性がある．また指紋を利用した場合には，指紋の特徴点データをサーバにおいておかなければならないという心理的負担になる．特徴点データにハッシュ関数を利用して，生体情報そのものを扱わない方式[2]もあるが，実証データが少なく，実際に利用できる段階ではない．

端末による認証

バイオメトリクスの特徴点データを端末上の認証プログラムでテンプレートと照合し，認証を行なう方法である．

ネットワーク上を特徴点データが流れることはないが，テンプレートを各端末に置く必要があるため，テンプレートの管理が困難になる．

また特徴点データが端末内に一旦取り込まれるため，その際に特徴点データを複製されてしまうおそれがある．

バイオメトリクス認証装置内で認証

バイオメトリクスの特徴点データをバイオメトリクス認証装置内でテンプレートと照合し，認証を行なう方法である．

バイオメトリクスの特徴点データが認証装置の外に流れることはないため，特徴点データが漏洩することがなく安全である．

しかし，認証の結果を端末に返すのみであり，端末と認証装置間の認証が重要となる．

3.2 リモートログイン

バイオメトリクスをネットワークを介して利用する

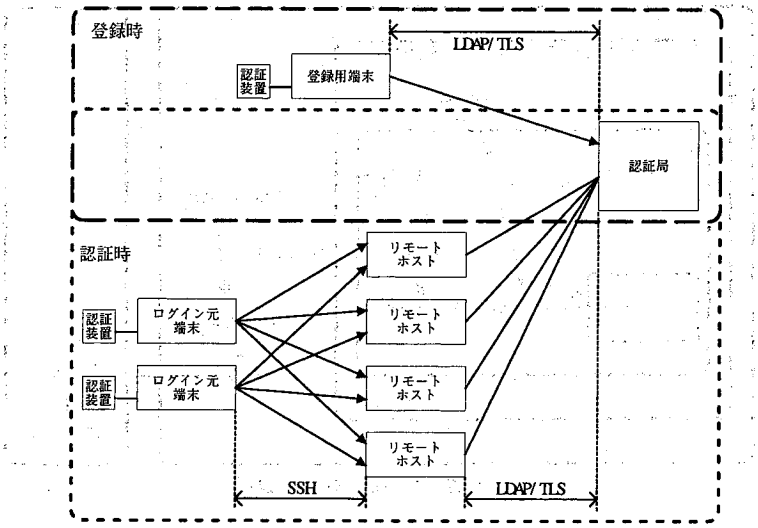

図1　提案するシステム

場合には，ローカルログインの3方法を，ログイン元端末，リモートホストで利用し，さらに別の方法を組み合わせることもできる．

バイオメトリクスの特徴点データを送信

リモートホストに特徴点データを直接送信し，リモートホストがテンプレートと照合を行なう．この方法は，認証サーバで認証を行なう方法とほぼ同じであり，同様の危険性がある．

バイオメトリクスで認証した結果を送信

ログイン元端末でバイオメトリクスによる認証を行ない，その認証の可否と認証を許可された利用者の情報をリモートホストに送信する．

この場合，バイオメトリクスの特徴点データがネットワーク上を流れることはないが，認証をおこなうログイン元端末をリモートホストが信頼できるかどうかの問題がある．もしログイン元端末が第3者に乗っ取られていた場合や，信頼できない者が管理していた場合には，その端末で認証した結果は信頼できなくなるし，その端末で特徴点データを盗み取られる可能性もある．

バイオメトリクスで認証し秘密鍵を取り出す

この方法は，ICカード内に秘密鍵を保存しておき，その秘密鍵の取り出しにバイオメトリクスによる認証を利用する方法[4)5)]である．

この場合，バイオメトリクスの特徴点データがネットワーク上を流れることもなく，公開鍵暗号方式により認証をおこなうため，正当な利用者であることを，正しい秘密鍵を所持していることで確認できる．

しかしICカードに保存できる秘密鍵の数に制限があるため，複数のシステムへのログイン時に問題がある．また，秘密鍵を一旦計算機へ取り出し，公開鍵暗号操作を行なう場合には，バイオメトリクスで認証した結果を送信する場合と同様の問題がある．

以上のことから，バイオメトリクスで認証してICカードから秘密鍵を取り出し，公開鍵暗号方式の認証に利用する方法が一番安全性が高いといえる．

また，組織内でのログインに利用する場合には，ICカードに保存できる秘密鍵が1つで十分なため，問題ない．

4. バイオメトリクスのUNIXリモートログイン認証への適用

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．

利用するバイオメトリクス認証装置は指紋認証装置を想定しているが，他のバイオメトリクスでも利用可能であると考えられる．

図1に提案するシステムを示す．

利用者はまず，管理者立ち会いの元でICカードに特徴点データと，社員番号や学籍番号などの組織内で一意に決められる識別情報を書き込む．さらに，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，それぞれ記録する．

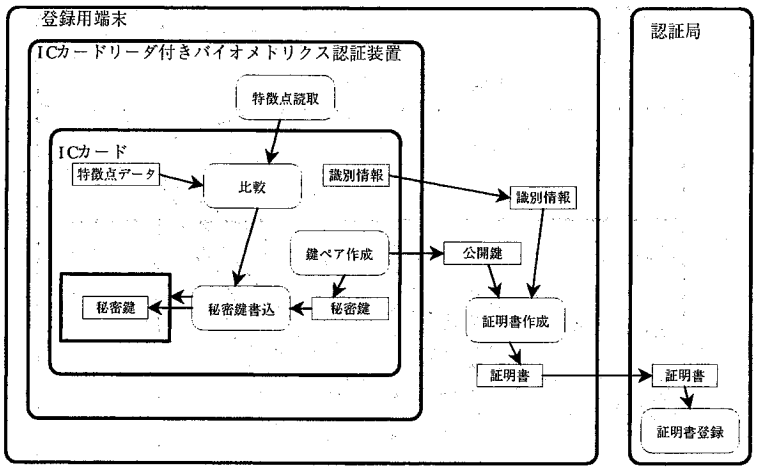

図 2 鍵ペアの作成と証明書の登録

利用時には手元の端末でバイオメトリクス認証を行ない，IC カードから秘密鍵を読み出し，SSH の認証に利用する．

遠隔地の端末では，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 の認証を行なう．

4.1 構成要素

この認証方法に必要な構成要素は，公開鍵と識別情報を結びつけるための認証局，認証局に情報を登録するための登録用端末，実際にログインする対象であるログイン先ホスト，利用者の手元にあるログイン元端末とバイオメトリクス認証装置，各利用者が所持する IC カードである．

認証局と登録用端末，ログイン先ホストは組織の管理者が運用をおこなう．ログイン先ホスト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

認証局には 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，OpenLDAP を利用する．

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．

認証局への登録のためには，専用のアプリケーションが必要である．

認証局からの読み出しには LDAP から公開鍵を読み出すことができる，OPENSSH LDAP PUBLIC KEY PATCH[7] を利用する．

その際の LDAP 認証局の認証には，OpenLDAP で提供されている，公開鍵暗号方式により認証をおこなえる TLS (Transport Layer Security) プロトコルを利用する．

OPENSSH LDAP PUBLIC KEY PATCH の機能により，認証局が停止している場合には，通常のパスワード認証が可能になる．

認証局と登録用端末間の接続にも，OpenLDAP で提供されている TLS を利用する．

IC カード

IC カードには，秘密鍵を取り出さなくても認証が可能なように，IC カード内で認証を行うことのできる，Standard-9[8] のような IC カードを利用する．また，秘密鍵の利用には，特徴点データを用いた認証が必要である．

IC カードは，表 1 の様に操作権限を設定する．認証を行なわなくても識別情報の読み取りを可能にし，利用者が特徴点データを用いた認証をおこなった時のみ，秘密鍵の生成，利用が可能に設定になる．

識別情報と特徴点データの書き込みについては，管理者立ち会いの元での登録を前提とするため，管理者

表 1 IC カードの操作権限

	管理者	利用者
識別情報書き込み	○	×
識別情報読み込み (認証無しでも可能)	○	○
特徴点データ書き込み	○	×
特徴点データ読み込み	×	×
秘密鍵生成	×	○
秘密鍵書き込み	×	×
秘密鍵読み込み	×	×
秘密鍵利用	×	○

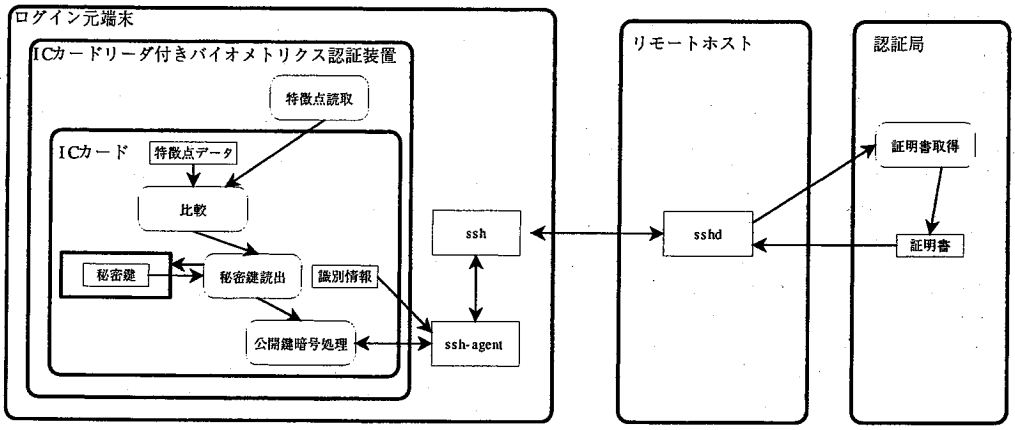

図 3　利用時

が PIN 等での認証をおこなった時のみ書き込みを許可するようにする．

秘密鍵については，IC カード外から読み書きできないように設定する．

4.2 登　録　時

特徴点データの登録

バイオメトリクスの特徴点データを抽出し，利用者の識別情報 (社員番号や学籍番号など個人を特定できる ID) と合わせて IC カードに書き込みをおこなう．

鍵ペアの作成と証明書の登録

信頼できる登録用計算機でバイオメトリクスによる認証を行い識別情報を確認する．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，秘密鍵を IC カードにユーザ権限で書き込む．その後，公開鍵を IC カードの外に取り出し，識別情報を合わせて証明書を作成し，LDAP を用いて認証局へ登録する．

この方法ではユーザ権限で IC カードに書き込むため，管理者が立ち会う必要がなく，証明書の有効期限切れの際などにいつでも証明書と秘密鍵の再作成が可能になる．

またバイオメトリクス認証装置のための UNIX システム用ドライバがほとんど提供されていないため，指紋認証中継システム[3] のような中継システムを利用することも検討する．

4.3 利　用　時

手元の計算機でバイオメトリクスによる認証をおこなう．その結果利用できるようになった秘密鍵を SSH の認証に利用する．

SSH の実装として OpenSSH[6] を用い，RSA や DSA を利用した公開鍵暗号方式を対象とする．SSH に付属している ssh-agent を変更し，従来は，秘密鍵をファイルから読み取り公開鍵暗号処理をおこなっていたものを，IC カード内に保存された秘密鍵を使って，IC カード内で公開鍵暗号処理をおこなった結果のみを通知するようにする．

Windows 環境からリモートログインを行なう場合には，TeraTerm や PuTTY 等の SSH クライアントを変更し，IC カードから秘密鍵を取り出せるようにする必要がある．

ログイン先の計算機では，該当ユーザの公開鍵証明書を認証局から取り出し，証明書の中の公開鍵を利用しユーザが正当な利用者かどうか確認をする．

認証装置がない環境からのログインの場合には，バイオメトリクスによるログインはできない．セキュリティが特別必要ではない環境の場合には，通常のパスワード認証を行うことも可能である．

5. ま　と　め

本研究では，UNIX のリモートログイン認証にバイオメトリクスを用いたシステムを提案した．

Secure Shell の暗号化通信をベースに 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 カード内で行なうことで，従来の Secure Shell よりも安全性を確保することができる．

公開鍵とユーザ情報を認証局で一括管理しているため，ログイン先でユーザ情報を個別に管理する必要もなく，証明書の即時失効も可能である．

また，公開鍵，秘密鍵ペアの再作成が管理者の立ち会い無しで行なえるため，秘密鍵の安全性が失われた際の復旧手順も簡易である．

今後の課題として，認証局が停止した場合に Secure

Shell が利用できなくなることへの対処を検討する必要がある.

参 考 文 献

1) 河津正人, 桑田雅彦, 恒田正哉, 山形昌也, 島村英: LDAP ハンドブック, ソフト・リサーチ・センター, 2002 年 2 月
2) 中村智博, 吉浦紀晃, 小野里好邦:ハッシュ関数を用いた生体情報による認証の実験, 情報処理学会研究報告, 2003-CSEC-20, pp.245-250, 2003 年 2 月
3) 古川英雄, 塙敏博:バイオメトリクスの UNIX ログイン認証への応用, 情報処理学会, 第 65 回全国大会講演論文集 (4), pp.221-222, 2003 年 3 月
4) 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, 2002 年 4 月
5) 板倉征男, 辻井重男:バイオメトリックス暗号鍵を用いた本人認証方式の提案, 情報処理学会研究報告, 2003-CSEC-21, pp.19-27, 2003 年 5 月
6) OpenBSD プロジェクト: OpenSSH, http://www.openssh.com/
7) Eric AUGE: OPENSSH LDAP PUBLIC KEY PATCH, http://ldappubkey.gcu-squad.org/
8) 大日本印刷: DNP Standard-9, http://www.dnp.co.jp/bf/j-iccard/std9.html