生体認証によるネットワーク個人認証システム

妹尾 尚一郎[†] 厚井 裕司[††] 貞包 哲男[†]
中谷 直司[††] 馬場 義昌[†] 鹿間 敏弘[†]

ネットワークを利用した犯罪が急激に増加しており，不正アクセスを防止するための認証技術の重要性がますます高まっている．現在，サービスの利用者を特定するための個人認証手段として用いられている磁気カード・IC カードとパスワードの組合せは，安全性の面から必ずしも確実な手段とはいえず，最近では生体認証が利用されるようになった．本論文では，複数の生体認証を組み合わせるとともに，ワークフローに従って上司と部下，関係窓口等の認証を順番に行うことができるネットワーク個人認証システムを提案し，実際にネットワーク認証プラットフォームを実現・評価することによりその有効性を示す．

A Network Authentication System by Multiple Biometrics

Shoichiro Seno,[†] Yuuji Koui,[††] Tetsuo Sadakane,[†]
Naoshi Nakaya,[††] Yoshimasa Baba[†] and Toshihiro Shikama[†]

In view of the recent increase of crimes over networks, authentication techniques to counter access attempts by malicious users become very significant. User authentication methods can be classified into three categories. The first one is based on human memory such as passwords or PID. The second one is based on physical devices such as magnetic or IC cards. As these two cannot escape vulnerabilities caused by forgetfulness or losses, the third category, biometrics based identification methods such as finger and iris-scan, is increasingly adapted in recent years. In this paper, we propose a network authentication system that can use multiple biometrics as authentication methods as well as provide authentication services to workflow processes from subordinate to his/her superiors to related parties. The paper also discusses the prototypes developed upon this system and evaluation of response time for user authentication.

1. はじめに

高度情報化社会の急速な進展によって，社会サービスの多くはコンピュータネットワークにより提供されるようになってきており，利用者がインターネットを通じて自宅のパソコンからサービスを受けることも可能となってきている．しかしながらネットワークを利用した犯罪も急激に増加しており，不正アクセスを防止するための認証技術の重要性がますます高まっている．現在，サービスの利用者を特定するための個人認証手段として用いられている磁気カード・IC カードとパスワードの組合せは，安全性の面から必ずしも確実な手段とはいえず，最近では生体認証が利用されるようになった．

生体認証は，指紋・網膜・虹彩・顔・音声等の人間が保有する生物学的な個性を自動判別することにより個人認証を行うもので，盗用が困難である，また認証手段を携帯する必要がない等の特徴に基づき，実用化が進んでいる．従来，生体を用いた本人認証は装置の小型化やコストの面で不利であったが，素子や部品の小型化，LSI 化により今後普及に弾みがつくものと予想される．しかしながら現時点では生体認証は精度，装置規模，コスト，適した利用環境等に違いがあり，さらに指紋認証に対する拒否反応を示す者さえ存在する．こうした生体認証における特有の課題は，パスワードやカードと違い認証の過程で本質的に誤りが入り込む余地がある点である．他人を本人と誤認する率を他人受入率，本人を他人と誤認する率を本人拒否率と呼び，これら 2 つの誤りをいかに小さくするかが課題であるが，複数方式を組み合わせるのであれば個々の方式の誤り率はある程度大きくても信頼度を高めることがで

† 三菱電機株式会社情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation
†† 岩手大学工学部
Faculty of Engineering, Iwate University

きる．たとえばある建物の中に入るときに指紋によって認証して，さらに機密度の高い部屋への入室時には別途網膜認証で検査する等の組合せが考えられる．

また近年，生体認証の技術がワークフローと結び付く傾向がある．ワークフローとは，情報や文書の受付，申請から査閲，承認，保存に至る一連の業務とその流れを電子化し，実行管理する情報システムである．ワークフローの各業務責任者が情報や文書の処理後に職務印を押したりサインしたりする代わりに，生体認証を行うシステム導入例が増えている．この場合には，各業務の特性に合った認証方法を採用する必要があり，さらに複数の認証者間の関係付けをあらかじめ定義しておくことが不可欠である．

本論文では，複数の生体認証を組み合わせるとともに，ワークフローに従って上司と部下，関係窓口等の認証を順番に行うことができるネットワーク個人認証システムについて論ずる．以下，2 章で従来のマルチ生体認証技術を概説した後，3 章でネットワーク個人認証システムの基本設計方針を，4 章でその実現方式を述べ，5 章でシステムの試作と評価結果について示す．6 章はむすびである．

2. 従来の生体認証技術

2.1 既存の生体認証に関する研究

生体認証に関する研究は大きく以下の 3 つに分けられる．

(1) **生体の形状を認識する研究**

人間が保有する生物学的な個性を抽出する研究は 1960 年代に開始され，80 年代には米国の連邦警察が指紋認識を犯罪捜査に採用するに至った．その後次第に犯罪捜査以外を対象とするようになり，利用する生体の種類も多くなってきた[1]．90 年代に入り，生体の特徴をソフトウェアで抽出できるようになり，研究成果が次々に実用化されるようになった[2),3)]．最近では，指紋[4)~9)]，虹彩[10)~12)]，網膜[13)]，手形状[14),15)]，声紋[16),17)]さらには顔[18),19)]等の多くの研究が行われている．これらの研究の延長として，サイン等の特定の図形を描くときのペンの動きや手指動に含まれる癖を解析した研究事例[20),21)]も存在する．

(2) **生体認証の特徴・強度の研究**

個々の生体認証にかかわらず，横断的な特徴抽出と重み付け，さらには各種の攻撃に対する強度を分析した研究が実施されるようになった．これらの研究[22)~24)]は認証精度を向上するとともに，認証の入力装置に対する攻撃を想定した対応策を考察して信頼性の高い生体認証システムの実現を図ることを目的としている．

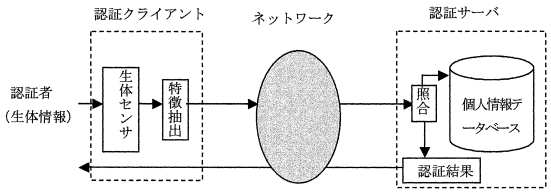


図 1 生体認証システムの構成
Fig. 1 Configuration of a network authentication system by biometrics.

(3) **複数の生体認証を組み合わせた研究[25),26)]**

個々の方式の誤り率はある程度大きくても複数の生体認証を組み合わせることによって認証精度を向上しようとするもので，米国ではすでに実用化も始まっている．組合せ方法によって論理的方法，統計的方法，識別的方法の 3 つに分類される．論理的方法は，各認証結果の出力の AND や OR をとり，統計的方法は各認証結果の類似度に対して確率密度関数を計算して，識別的方法は密度関数で与えられる識別境界のみを推定することで精度の向上を図ろうとするものである．

2.2 ネットワークを介した生体認証に関する課題

生体認証の安全性は認証装置の精度はもちろん，どのようにシステムを構成・運用しているかといったことも考慮することが大切である．**図 1** に示す生体認証システムの構成においては，認証の判定はネットワークを経由した認証サーバで行われており，入力された生体情報は認証者から認証クライアント，ネットワーク，認証サーバへと転送されていく．さらに認証結果は認証サーバから返送される．これらの情報転送経路の途中のどこかで，欺きや成りすましといった不正行為が行われる恐れがあり，十分な注意が必要である．このためには，ネットワークを含めたシステム全体として認証の仕組みやその強度を検討することが不可欠である．現在までの研究開発においては，主に生体認証の入力系における精度の向上に力点がおかれていたが，本論文ではネットワークを利用した個人認証システム全体について検討する．

2.3 生体認証の利用形態における変化

生体認証を利用した適用業務も従来のイントラネット中心からインターネットを含めたアクセスに広がっており，Web アクセスへの適用が不可欠になっている．このようなアプリケーションサーバ型の認証システムを構築するには，入力された認証情報の秘匿方法や暗号鍵の管理が重要な課題となる．さらに前述したように，複数の生体認証を組み合わせた構成やワークフロー作業の一環として生体認証を利用する形態が今後次第に増加するものと予想される．本論文ではこれ

らの要求に対応したネットワーク個人認証システムを提案・評価するものである．

3. ネットワーク認証システムの基本設計方針

ネットワーク認証システムの設計に際して，我々が設定した基本設計方針は下記のとおりである．

(1) 生体認証単体による個人の識別や，生体情報を鍵に個人情報データベースを検索する検索照合はもちろん，複数の生体認証やパスワード認証の手段を自由に組み合わせた個人認証も可能とする．

(2) 個人情報や認証情報等の重要情報を一元的に管理して，人事異動等の物理的な位置の変更に左右されない統一的な認証サービスを提供する．

(3) インターネットの急速な普及を考慮して，クライアント/サーバ型の Web アクセス時のユーザ認証として生体認証を適用する．

(4) 認証装置から認証サーバまでの安全な認証プロトコルにより，ネットワークを悪用した成りすましやリプレイ攻撃から守る．

(5) ワークフロー作業の一環として生体認証を利用できる形態とする．

4. ネットワーク認証システムの実現方式

4.1 ネットワーク認証システムの構成

我々は種々の認証アプリケーションを分析して，ほとんどの利用形態に対応できる一体モデルと分離モデルの 2 つのモデルを抽出した．

(1) **一体モデル**

一体モデルは**図 2** に示すように入室検査等のローカルな個人認証環境を提供するものである．認証クライアント内に存在する入室検査アプリケーションが認証装置から認証情報を得て，リモートの認証サーバにユーザの認証を依頼する．

(2) **分離モデル**

一方，**図 3** の分離モデルはユーザがリモートのサーバにアクセスするときに個人認証環境を提供するものである．クライアント内に存在するブラウザが認証装置から認証情報を得て，認証クライアントでもあるリモートの HTTP サーバ経由で認証サーバにユーザの認証を依頼する．認証サーバは認証クライアントから受け取った認証依頼に含まれている認証情報と個人情報データベースの情報を照合して，認証クライアント経由でクライアントに認証結果を返送する．

4.2 ネットワーク認証プラットフォーム

図 4 は上記 2 つのモデルを共通のプラットフォームで実現した仕組みを描いている．分離モデルのクライアント内に存在するブラウザによって認証クライアントから読み込まれた認証クライアントエージェントの働きで，クライアントは認証クライアントの一部として動作する．いい換えれば，一体モデルの認証クライアントを物理的にクライアントと認証クライアントに分離して，両方の装置をネットワークとエージェントソフトウェアで結び付けたものが分離モデルといえる．

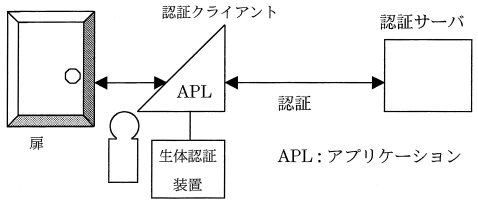


図 2 一体モデル
Fig. 2 Unified model.

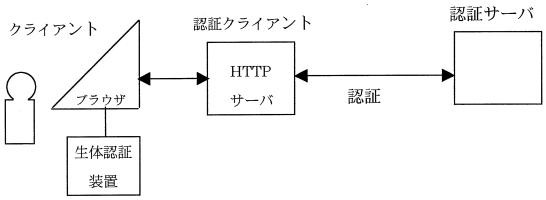


図 3 分離モデル
Fig. 3 Separated model.

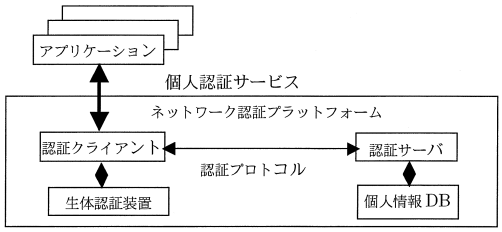


図 4 認証プラットフォーム
Fig. 4 An authentication platform.

ネットワーク認証プラットフォームの外部に位置付けられるアプリケーションは，一体モデルの入室検査ソフトウェアや分離モデルの HTTP サーバおよびブラウザが相当する．このような構成を採用することにより，ネットワーク認証プラットフォームのソフトウェアをモデルによらず統一的に実装することができた．

なお本プラットフォームでは複数の生体認証を提供可能とするため，各構成要素において**表 1** に示す生体情報の識別・処理を行う．

4.3 ネットワーク認証システムの構築例

図 5 に示すように一体モデルでは，認証クライアントに存在するアプリケーションは認証装置から認証情報を取得した後に，認証 API を通してリモートの

表 1 生体情報の識別・処理
Table 1 Identification and processing of biometrics information.

構成要素	生体情報への依存性	複数の生体情報のサポート	備考
認証クライアント	生体認証装置のドライバ以外は非依存	生体情報を識別し対応する生体認証装置から生体情報を取得	アプリケーションから生体情報種別を指定可能
認証プロトコル	非依存	生体情報に識別子をつけて転送	
認証サーバ	非依存	生体情報を識別し対応する照合アルゴリズムを適用	
個人情報 DB	非依存	生体情報に識別子をつけて格納	
生体認証装置	依存	生体情報種別ごとに別装置	

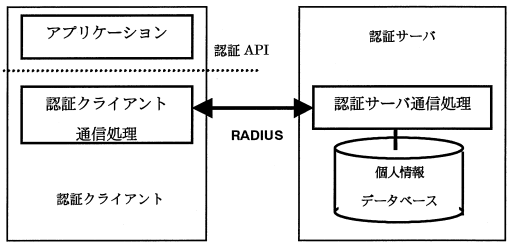


図 5 一体モデルのシステム構築例
Fig. 5 A system construct of the unified model.

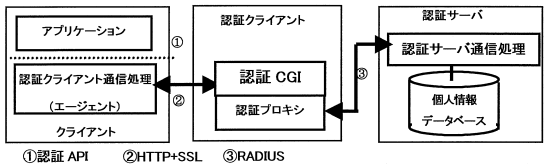


図 6 分離モデルのシステム構築例
Fig. 6 A system construct of the separated model.

認証サーバにユーザの認証を依頼する．認証 API は，認証サービスを受ける複数のアプリケーションに対してセキュアな通信機能を提供するインタフェースであり，認証に用いる生体情報種別を指定可能としている．

図 6 は認証クライアントに HTTP サーバを搭載した分離モデルにおけるシステムの構築例を示している．このようなシステムでは，クライアントに存在するアプリケーションが認証 API を通してリモートの認証サーバにユーザの認証を依頼する場合に，HTTP サーバのパスワード認証機構を拡張する方式と Common Gateway Interface（以後，CGI と呼ぶ）を用いる方式が考えられる．我々は種々のタイプの OS を実装した HTTP サーバにおいてもシステムを構築できるように，HTTP サーバ自体を改造するのではなく CGI 機構を利用して生体認証機能を組み込んだ．この方法により，認証 CGI が中核となって認証情報や認証結果の中継制御を行う．具体的には**図 7** に示すように，クライアントにはブラウザ，プラグインとドライバをインストールしておき，個人認証が必要なときだけ認証クライアントエージェントとなる JAVA Applet が HTTP サーバから転送される．ここでドライバ以外は生体情報種別に依存しない．認証情報を取得するためのブラウザ拡張は，主に JAVA Applet によって実現する．JAVA Applet はセキュリティ上の制限によりドライバに直接アクセスできないので，プラグインを通してアクセスする．また JAVA Applet は認証情報を認証 CGI に送る場合にも，同じく HTTP サーバから転送される JAVA Script を経由して届ける構成とする．これにより認証 CGI は認証情報を認証プロキシ経由で認証サーバに渡し，その認証結果を Web ページとしてブラウザに戻すことができる．なお CGI のセッション管理には，CGI の環境変数を用いる．

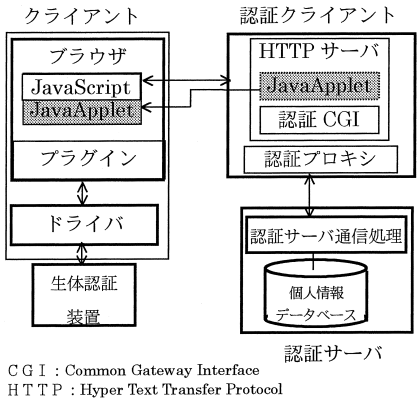


図 7 分離モデルのシステム構成
Fig. 7 Components of the separated model system.

上記構築例において，一体モデルの認証プロトコルには RADIUS，分離モデルの認証プロトコルには HTTP+SSL と RADIUS を適用しており，いずれも生体情報に識別子をつけて転送することで複数の生体情報をサポート可能としている．**図 8** に認証動作のシーケンスを示す．

4.4 生体情報の入力

(1) 生体情報の構造

生体認証では，指紋や虹彩等のユーザの身体から生成されるデータ（以後，生体情報と呼ぶ）を認証情報として採取し認証を依頼する認証クライアントと，認証を施す認証サーバが，ネットワークで接続されたリモート環境で個人認証を実施する．認証装置としては

表 2 ユーザファイルの構成
Table 2 A user file structure.

ユーザ ID	状態	ユーザ情報	ユーザ種別	生体情報 1	生体情報 2	パスワード	使用可能アプリケーション	有効期限
User1	Status 1	Name 1	K1	Finger 1-1	Finger 1-2	Pwd1	Appi, Appj	
User2	Status 2	Name 2	K2	Iris2-1	Finger 2-1	Pwd2	Appk, Appj	
・	・	・	・	・	・	・	・	・
Userm	Status m	Name m	Km	Retina m-1	Finger m-1	Pwdm	Apph, Appj	

状態：生体情報登録待ち/アクセス禁止
ユーザの情報：名前/所属/TEL
ユーザ種別：システム管理者/一般ユーザ

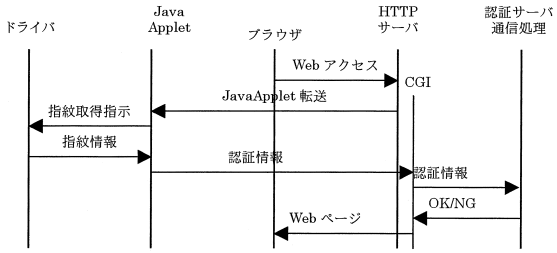


図 8 分離モデルの動作シーケンス
Fig. 8 Protocol sequence of the separated model.

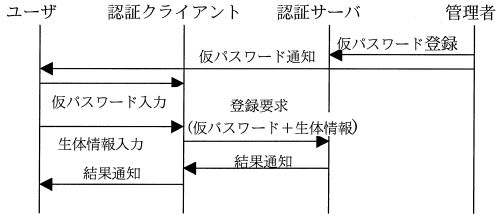


図 9 生体情報登録シーケンス
Fig. 9 Registration sequence of biometric information.

指紋用がより一般的であるが，生体情報に関するユーザファイルに複数の生体情報を識別する共通領域を設けるようにすれば，いずれの生体情報にも対応できるようになる．また，生体情報は怪我等のため一時的に採取不可能となる場合がある．そのため，認証情報として 1 ユーザあたり複数の生体情報をあらかじめ登録し，それらのうちの 1 つと一致した場合に認証が許可される．認証が許可された場合でも，ユーザファイルに記入された使用可能アプリケーションしかアクセスできない．

なお，生体認証をどうしても適用できない対象者にはパスワードで代用できるようにしたが，このパスワードの発行は管理者の特別の許可が必要である．**表 2** に上記を実現するユーザファイルの例を示す．

(2) **生体情報の登録**

リモートからの生体認証情報の初期登録時には，仮パスワードを用いる．管理者によって登録された仮パスワードはユーザに通知され，該当するユーザはその仮パスワードを利用して生体情報を登録することができる．この仮パスワードには有効期限があり，この期間中に生体情報の登録を行う必要がある．また，第 3 者が仮パスワードを不正に入手しても直接アプリケーションにはアクセスできず生体情報登録が必要であり，そのためには生体認証装置も不正に入手して生体情報を入力するか，認証装置自体を偽装しなければならず，パスワード認証と比べ成りすましが困難である．すなわち前者については，攻撃者が生体認証装置へ生体情報を入力すればそれを用いた追跡が可能なことから，抑止効果が期待できる．なお指紋認証装置について人工指を用いた生体情報の偽造実験例が報告されているが[27]，本システムが扱う生体情報は指紋に限定されないので，偽造が困難な他の生体情報と組み合わせる等の対策が可能である．また後者については，4.6 節に述べるように認証装置が出力する認証情報は暗号化によって秘匿されるので，偽装の技術的障壁が高い．これらより，登録に仮パスワードを用いても認証情報が生体情報であれば，パスワードに比べセキュリティが高い．**図 9** に，仮パスワードを用いた生体情報登録の流れを示す．

なお仮パスワードは漏洩・紛失の危険性を免れないので，本システムはこれに代えて管理者の監視のもとでユーザが生体情報を登録することも可能としている．

4.5 生体情報の認証

(1) **生体情報の管理**

個人のプライベートな生体情報や後述のアクセス制御情報を個人情報データベースとして，認証サーバ上に構築した．さらに認証サーバは他の認証サーバが管理

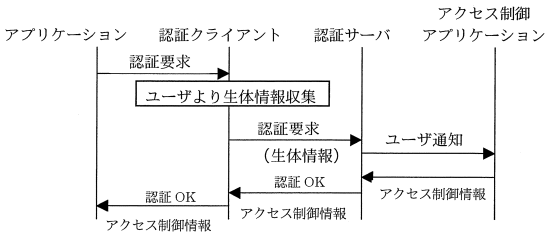


図 10 アクセス制御情報を用いた認証シーケンス
Fig. 10 Authentication sequence with access control information.

するユーザからの認証要求を受け取ったときに，該当する認証サーバに転送して認証してもらう認証サーバ群連携機能を有する．なお認証サーバは，認証要求に含まれる生体情報の種別を識別して対応する照合アルゴリズムを適用することで，複数の生体認証をサポートしている．

(2) **アクセス制御**

就業時間外や緊急事態発生時のアクセスを禁止・許可する等，ユーザによるアクセス動作をより細かに制御できるように，認証サーバに特別のアクセス制御アプリケーションを登録可能とした．認証サーバは認証許可後にアクセス制御アプリケーションからアクセス制御情報を受け取り，認証結果とともにアクセス制御情報をアプリケーションに戻す．**図 10** は，このアクセス制御情報を用いた認証シーケンスである．

4.6 生体情報のセキュリティ

生体情報はパスワードと違って頻繁な更新が不要である反面，意図的な変更が不可能であり個人を明示するため，生体情報を入力する認証装置から照合する認証サーバに至るシステム全体を暗号化によって外部から秘匿し，安全性・プライバシーを確保する必要がある．生体情報の流れは認証装置とクライアント/認証クライアント間，クライアントと認証クライアント間，認証クライアントと認証サーバ間に大別されるので，それぞれ下記に述べる対応を図った．図 5 に一体モデルの対応を，図 6 に分離モデルの対応を示す．

(1) **認証装置とクライアント/認証クライアント間**

認証装置はクライアント（一体モデル）または認証クライアント（分離モデル）とシリアルインタフェースで接続されてスタンドアロン形態でも使用される．しかも認証装置は低価格化が進み，認証装置に内蔵される CPU が高性能とは限らない．したがって，計算量の少ない秘密鍵暗号方式 MISTY [28] を実装している．

(2) **クライアントと認証クライアント間**

多数のクライアントがインターネット経由で認証クライアントに秘密鍵を使って暗号通信を行う場合に，鍵の設定や秘密鍵の秘匿方法が問題になる．このため，我々はクライアントと認証クライアント間の暗号通信に SSL（Secure Socket Layer）V2 を適用した．SSL [29] はインターネット上の通信またはクライアントとサーバとの間の情報を暗号化して送受信するプロトコルである．現在インターネットで広く使われている HTTP や FTP 等のデータを暗号化し，プライバシーにかかわる情報やクレジットカード番号，企業秘密等を安全に送受信するために利用されている．SSL を用いることで，クライアントを一般のパソコンで実現することが容易になり，また鍵の設定や管理の問題が解決される．

(3) **認証クライアントと認証サーバ間**

一般にユーザ認証は RADIUS [30] サーバや TACACS [31] サーバが業界標準となっており，現在までの開発資産の活用を考慮して我々も RADIUS プロトコルを適用した．このプロトコルは IETF によって RFC 2865 として標準化され，暗号として独自の MD5 方式を用いてセキュリティを高めている．今回，認証クライアントと認証サーバ間の RADIUS プロトコルを複数の生体情報に対応できるよう拡張した．すなわち，従来の RADIUS ではパスワード認証しかなく暗号化されるパスワードの長さが限られていたものを，生体情報の識別子を追加し暗号化フォーマットを変更して複数の長大な生体情報であっても暗号化できるようにするとともに，ユーザ ID やアクセス制御情報も暗号化範囲に含めプライバシーを確保した．

4.7 ワークフローに対するインタフェース

ワークフローにおける認証は，Web アクセスやメール等を組み合わせて上司や関係窓口等へ順番に文書や伺いの承認を要求・処理することで行われる．これらの承認の順序や手順はすべてワークフロー側で行われる．ワークフローがネットワーク個人認証システムに生体認証を要求する場合には，分離モデルの形態でアクセスされる．そのときにワークフロー側からネットワーク個人認証システムには複数の認証者間の関係付けが受け渡される．これらの情報はアクセス制御アプリケーションで妥当性がチェックされ，認証結果とともにアクセス情報としてアプリケーションに戻される．**図 11** にアクセス制御によるチェック例を示す．

一例として，ユーザ X がクライアントから認証クライアント 1 経由で生体認証を認証サーバに依頼したと想定する．認証要求を受け取った認証クライアント 1 は，図 10 の認証シーケンスに従って認証サーバさらにはアクセス制御アプリケーションに認証要求を転送する．アクセス制御アプリケーションでは，ワーク

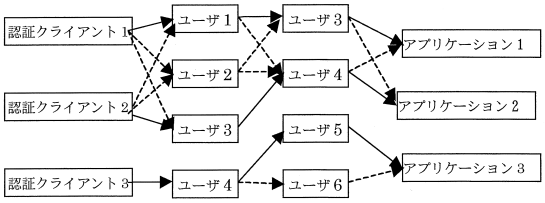


図 11 ワークフローの認証関係
Fig. 11 Authentication according to the workflow.

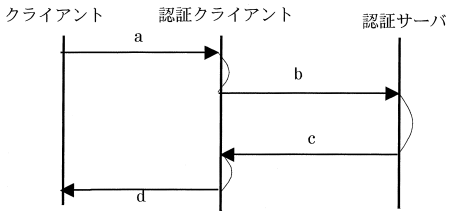


図 12 ネットワーク上を流れる情報と測定時間間隔
Fig. 12 Measurement intervals of information flow over the network.

フローによる認証が必要であることを示す認証結果とともに，このワークフローが実線の正規ルート（認証クライアント 1 → ユーザ 1 → ユーザ 3 → アプリケーション 1）と破線の代替ルート（認証クライアント 1 → ユーザ 2 → ユーザ 3 → アプリケーション 1 または認証クライアント 1 → ユーザ 3 → ユーザ 4 → アプリケーション 1）から成ることを示すアクセス制御情報を認証クライアント 1 に戻す．認証クライアント 1 に存在するワークフローのアプリケーションは，このアクセス制御情報を参照してユーザ 1 に生体認証を依頼し，ユーザ X にユーザ 1 の認証中の状況を連絡する．次にユーザ 1 からの認証要求を受け取った認証クライアント 1 のワークフロー・アプリケーションはアクセス制御情報に従って処理を進める．このようにして，ユーザ 1 からユーザ 3 へと認証を終えた後に，認証クライアント 1 のワークフロー・アプリケーションはアプリケーション 1 がアクセス可能になったことをユーザに伝える．上記において正規ルートのユーザ 1 やユーザ 3 が長期出張等で認証処理ができない場合には，代替ルートが実行される．複数の認証者間の関係付けについては，あらかじめアクセス制御アプリケーションが参照するデータベースとして定義が必要である．なお，ワークフローに対するアプリケーションは本ネットワーク個人認証システムの追加機能として位置付けられる．

5. システムの評価

5.1 処理時間の測定

実際に試作開発した下記分離モデルの 2 つの実装法 A・B にそれぞれ 100 人分の生体情報を登録して指紋による個人認証手続きを行い，各モジュールの処理時間を測定した．認証時にネットワーク上を流れる情報と測定時間間隔の関係を**図 12** に示す．

a. User ID，生体情報等の文字列．POST 形式（約 1 KB）．
b. 認証サーバで必要な認証情報（約 0.6 Kbytes）．生体情報は暗号化されている．
c. 認証結果が OK/NG の情報．
d. 認証結果として出力する HTML 文書．

実装法 A は認証サーバや認証クライアントのオペレーティングシステムに Solaris を，通信部分にフリーソフトウェアを使用し，CGI 部分を perl のスクリプトで記述した．実装法 B は認証サーバや認証クライアントのオペレーティングシステムに Windows NT を，通信部分を自主開発し，CGI 部分を C 言語で記述した．詳細を以下に示す．

(1) **実装法 A の構成**

① 認証サーバのオペレーティングシステム
Solaris
② 認証サーバのデータベース
テキストベースの独自 DB でユーザ ID を検索して対応するテンプレートの生体情報を取り出して照合する方式
③ 認証クライアントのオペレーティングシステム
Solaris
④ 認証クライアントの CGI
perl のスクリプトで記述
⑤ 認証サーバと認証クライアント間の通信部分
Radius のフリーソフトウェアを改修使用（SSL は未実装）

(2) **実装法 B の構成**

① 認証サーバのオペレーティングシステム
Windows NT
② 認証サーバのデータベース
Oracle 上に独自開発した DB ライブラリ（高速検索アルゴリズムを実装）を使用
③ 認証クライアントのオペレーティングシステム
Windows NT
④ 認証クライアントの CGI
C 言語で作成
⑤ 認証サーバと認証クライアント間の通信部分
マルチスレッド対応で自主開発

以上の結果，1 回の認証に実装法 A は 1500 ms かか

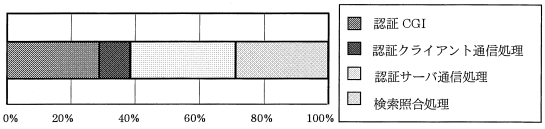


図 13 実装法 A における各モジュールの処理時間
Fig. 13 Processing time of each module in the implementation A.

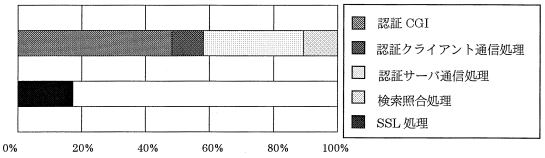


図 14 実装法 B における各モジュールの処理時間
Fig. 14 Processing time of each module in the implementation B.

り，実装法 B は 400 ms を要した．実装法 A では認証サーバと認証クライアント間の通信部分に RADIUS のフリーソフトウェアを流用することを前提とし，認証サーバのデータベース照合も単純なシーケンシャル検索としている．さらに認証クライアントの CGI も性能への配慮を考えずに perl のスクリプトで実現している．**図 13** は実装法 A における各モジュールの処理時間を示すが，認証クライアント通信処理を除く各モジュールの処理時間は全体の 30%程度となっている．これに対して実装法 B では，RADIUS 通信部分をマルチスレッド対応にするとともに，認証サーバのデータベース照合に Oracle 上に独自開発した DB ライブラリ（高速検索アルゴリズムを実装）を適用して性能を向上させている．さらに認証クライアントの CGI も C 言語で作成した．この結果，実装法 A の約 4 倍近くの処理性能を得ることができた．**図 14** は実装法 B における各モジュールの処理時間を示すが，高速検索アルゴリズムの適用で検索照合処理時間を大幅に改善することができた．このように実装方法によって認証遅延は相当に影響を受けることが判明したが，どちらの場合も通常の使用に耐えられる範囲に収まっている．

5.2 異なった生体情報の処理時間への影響

ネットワーク認証システムの生体認証では種々の生体情報が扱われ，認証の精度によっては生体情報長が増加することが予想される．しかしながら我々の実現例や各種の認証装置の機能調査において，各個人の指紋，虹彩，網膜等種々の生体特徴点データは大きいものでも 1,500 Bytes[32)~35)]であった．この結果，図 13 と図 14 で認証クライアントや認証サーバの通信処理は比較的大きくなく，しかも認証サーバの検索処理も実装方法次第で小さく抑えられるので，生体情報が異なってもそれほど影響がないことが判明した．

5.3 SSLV2 追加の影響

本ネットワーク認証システムでは認証情報の取得から認証サーバまでの生体情報の秘匿方法にセキュリティホールがないように，クライアントと認証クライアント間に SSL プロトコルを追加した．図 14 に SSL プロトコルの処理時間の割合が 17%程度になっていることを示している．この値は SSLV2 を利用したインターネットアクセスの利便性を阻害する要因とはならないであろう．

6. むすび

本論文では，生体によるネットワーク個人認証システムの設計と実現方式を述べ，さらにシステムに対する処理時間の評価結果について論じた．ここで述べたネットワーク個人認証システムは複数の生体認証を組み合わせる点，ワークフローに従って上司と部下，関係窓口等の認証を順番に行うことができる点，認証装置から認証サーバまでを安全な認証プロトコルにより守る点，共通のプラットフォームで入室検査等のローカルな個人認証環境とクライアント/サーバ型の Web アクセス時のユーザ認証環境を提供する機構等を兼ね備える点等を特徴としている．今回，実際に実現したネットワーク認証プラットフォームを用いることにより，当初目的としていた安全かつ信頼性の高いネットワーク個人認証システムに拡張することができ，本方式の有効性を示すことができた．なお，ワークフローについては紙面の都合で十分に記述できなかったため，別の論文で発表するつもりである．

今後の課題としては，筆跡認証等様々な認証手段の追加，ユーザごとの生体認証手段の組合せと使用可能アプリケーションの対応付け，ワークフローにおける認証者間の関係をどう管理するか，さらには統一化された暗号方式の開発等が考えられる．

参考文献

1) Davies, D.W. and Price, W.L: *Security for Computer Networks*, pp.169–208, John Wiley & Sons (1986).
2) Galton, F.: Personal Identification and Description, *Nature*, pp.173–177 (1988).
3) Miller, B.: Vital Signs of Identity, *IEEE SPECTRUM*, Vol.2, pp.22–30 (1994).
4) Jain, A., Bolle, R. and Pankanti, S. (Eds): *BIOMETRICS: Personal Identification in Networked Society*, Kluwer Academic Publishers

(1999).
5) Germain, R., Califano, A. and Colville, S.: Fingerprint Matching Using Transformation Parameter Clustering, *IEEE Computational Science and Engineering*, Vol.4, No.4, pp.42–49 (1997).
6) Jain, A., Prabhakar, S. and Hong, L.: A Multichannel Approach to Fingerprint Classification, *IEEE Trans. PAMI*, Vol.21, No.4, pp.348–359 (1999).
7) Jain, A., Prabhakar, S. and Chen, S.: Combining Multiple Matchers for a High Security Fingerprint Verification System, *Pattern Recognition Letters*, Vol.20, No.11-13, pp.1371–1379 (1999).
8) 小林哲二：細線化画像パターンマッチングによる指紋照合，信学論（D-II），Vol.J79-D-II, No.3, pp.330–340 (1996).
9) 内田 薫：指紋照合による本人認証，情報処理学会誌，Vol.40, No.11, pp.1078–1083 (1999).
10) Hallinan, P.W: Recognizing Human Eyes, *SPIE Proc. Geometric Methods in Computer Vision*, 1570, pp.214–226 (1991).
11) Lim, S., Lee, K., Byeon, O. and Kim, T.: Efficient Iris Recognition through Improvement of Feature Vector and Classifier, *ETRI Journal*, Vol.23, No.2, pp.61–69 (2001).
12) 塚田光芳：虹彩による本人認証，情報処理学会誌，Vol.40, No.11, pp.1084–1087 (1999).
13) Hill, R.: Retina Identification, *BIOMETRICS: Personal Identification in Networked Society*[4].
14) Jain, A., Ross, A. and Pankanti, S.: A Prototype Hand Geometry-Based Verification System, *2nd International Conference on Audio- and Video-based Biometric Person Authentication*, Washington D.C. (1999).
15) 遊佐博幸，兵庫 明，関根慶太郎：基準抽出による2次元平面上における手形状認識，信学論（D-II），Vol.J80-D-II, No.5, pp.1209–1220 (1997).
16) George, M.H. and King, R.A: A Robust Speaker Verification Biometric, *Proc. IEEE 29th Annual 1995 International Carnahan Conference On Security Technology*, UK, pp.41–46 (1995).
17) 西田昌史，有木康雄：話者固有空間における動的・静的特徴統合による話者照合，信学論（D-II），Vol.J83-D-II, No.12, pp.2536–2544 (2000).
18) Weng, J. and Swets, D.L: Face Recognition, *BIOMETRICS: Personal Identification in Networked Society*[4].
19) 土居元紀，陳 謙，眞溪 歩，大城 理，佐藤宏介，千原國宏：顔画像照合による解錠制御システム，信学論（D-II），Vol.J80-D-II, No.8, pp.2203–2208 (1997).
20) Yamazaki, Y. and Komatsu, N.: A Proposal for a Text Indicated Writer Verification Method, *IEICE Trans. Fundamentals*, Vol.E80-A, No.11, pp.2201–2208 (1997).
21) 長田礼子，尾崎 哲，青木輝勝，安田 浩：手指動からの特徴抽出によるリアルタイム個人認証，信学論（D-II），Vol.J84-D-II, No.2, pp.258–265 (2001).
22) Jain, A., Hong, L. and Pankanti, S.: Biometrics Identification, *Comm. ACM*, Vol.43, No.2, pp.91–98 (2000).
23) Schneier, B.: Inside Risks: The Uses and Abuses of Biometrics, *Comm. ACM*, Vol.42, No.8, p.136 (1999).
24) 山崎 恭，小松尚久：身体的特性に基づく個人認証システムにおける個人性の抽出手法，信学論（B-I），Vol.J79-B-I, No.5, pp.373–380 (1996).
25) Hong, L., Jain, A. and Pankanti, S.: Can Multibiometrics Improve Performance, *Proc. AutoID'99*, Summit, NJ, pp.59–64 (1999).
26) 坂野 鋭，劉 偉傑：多重バイオメトリックスによる個人認証，情報処理学会，CSEC-5-7, pp.37–42 (1999).
27) 山田浩二，松本弘之，松本 勉：指紋照合装置は人工指を受け入れるか，信学技報，ISEC2000-45 (2000).
28) Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Proc. 3rd international workshop of fast software encryption*, Lecture Notes in Computer Science 1039, Springer Verlag (1996).
29) Secure Socket Layer, Netscape Communications.
30) Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC 2865, IETF (2000).
31) Finseth, C.: An Access Control Protocol, Sometimes Called TACACS, RFC 1492, IETF (1993).
32) http://www.smartcardalliance.org/pdf/alliance_activities/Secure_ID_White_Paper.pdf
33) http://rr.sans.org/authentic/biometric3.php
34) http://rr.sans.org/authentic/parts_online.php
35) http://www.networkmagazine.com/article/NMG20020701S0014

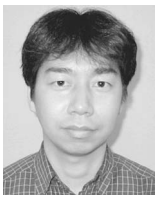
(平成14年4月30日受付)
(平成15年2月 4 日採録)

妹尾尚一郎（正会員）

1981 年東京工業大学理学部応用物理学科卒業，1983 年同大学大学院応用物理学専攻修了．同年三菱電機（株）入社．以来，LAN，プロトコル高速処理，電子メール，ネットワークセキュリティ，光ネットワーク制御等の研究に従事．現在，同社情報技術総合研究所ネットワーク技術部チームリーダー．電子情報通信学会会員．

厚井　裕司（正会員）

1970 年東京理科大学理学部応用物理学科卒業．同年三菱電機（株）入社．2001 年岩手大学工学部情報システム工学科教授，現在に至る．主として，マルチメディアネットワーク，ネットワークセキュリティ，RF-ID タグに関する研究に従事．工学博士．IEEE，電子情報通信学会各会員．



貞包　哲男（正会員）

1995 年東京理科大学情報科学科卒業，1997 年同大学院情報科学専攻修了．同年三菱電機（株）入社，現在に至る．ネットワークセキュリティに関する研究開発に従事．

中谷　直司

1994 年埼玉大学工学部電子工学科卒業，1996 年同大学大学院修士課程修了，1999 年同大学院博士課程修了．同年岩手大学工学部情報システム工学科教務職員，2001 年同科助手，現在に至る．進化型アルゴリズム，ネットワークセキュリティに関する研究に従事．博士（学術）．電子情報通信学会会員．

馬場　義昌（正会員）

1984 年慶應義塾大学工学部計測工学科卒業，1986 年同大学大学院修士課程修了．同年三菱電機（株）入社．以来，ネットワークアーキテクチャ，通信プロトコル，インターネット，ネットワークセキュリティ等の研究開発に従事．現在，同社情報技術総合研究所に勤務．

鹿間　敏弘

1976 年東京工業大学電子システム専攻修士課程修了．同年三菱電機（株）入社．1995 年〜2000 年三菱電機（株）の海外研究所 ITE-TCL（フランス）に出向．LAN，パケット交換，ATM，衛星通信等の研究開発に従事．IEEE，電子情報通信学会各会員．