統計的 AD 変換による生体情報を用いた Challenge & Response 型ネットワーク認証の提案

柴田 陽一[†]　中村 逸一[‡]　三村 昌弘[††]　高橋 健太[††]　西垣 正勝[‡‡]

†静岡大学大学院情報学研究科，〒432-8011 静岡県浜松市城北 3-5-1
‡北京 NTTDATA，中国北京市海澱区中関村大街 27 号　中関村大廈 12 階
††株式会社日立製作所システム開発研究所，〒244-0817 神奈川県横浜市戸塚区吉田町 292
‡‡静岡大学情報学部，〒432-8011 静岡県浜松市城北 3-5-1

E-mail: †cs9042@cs.inf.shizuoka.ac.jp, ‡nakamura@nttdatabj.com.cn,
††{mmimura,kenta}@sdl.hitachi.co.jp, ‡‡nisigaki@cs.inf.shizuoka.ac.jp

あらまし　生体情報はユーザと強く結びついた情報であり，ユーザを認証する情報として有効である．ところが，従来の生体認証はパターンマッチングで行われているため，ネットワークを介してユーザ認証を行うためには，生体情報を事前にサーバに登録し，かつ，認証の度に生体情報を送信する必要がある．そのため，プライバシおよび盗聴等の問題があった．これに対し，著者らは生体情報から常に一意なユニーク ID をリアルタイムで抽出する「統計的 AD 変換」という技術を提案している．この統計的 AD 変換によって得られる ID を認証鍵として用いてやることにより，生体情報によるネットワーク認証を実現することができる．本稿では，生体ネットワーク認証の一例として，指紋を用いた Challenge & Response 型ネットワーク認証を説明する．従来の手法との比較を行い，本手法の有効性を示す．

キーワード　ネットワーク認証，生体認証，Challenge & Response 認証，統計的 AD 変換

A challenge-response authentication with a password extracted from a fingerprint

Yoichi SHIBATA[†]　Itsukazu NAKAMURA[‡]　Masahiro MIMURA[††]　Kenta TAKAHASHI[††]
and　Masakatsu NISHIGAKI[‡‡]

† Graduate School of Information Shizuoka University, 3-5-1 Johoku, Hamamatsu-shi, Shizuoka-ken, 432-8011, Japan
‡ BEIJIN NTT DATA SYSTEMS INTEGRATION CO.,LTD, 12F Zhongguancun Building, 27 Zhongguancun Street, Haidian District, Beijin 100080, China
†† Hitach, Ltd., System Development, Lab., 292 Yosidatyou, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817, Japan
‡‡ Faculty of Information, Shizuoka University, 3-5-1 Johoku, Hamamatsu-shi, Shizuoka-ken, 432-8011, Japan

E-mail: †cs9042@cs.inf.shizuoka.ac.jp, ‡nakamura@nttdatabj.com.cn,
††{mmimura,kenta}@sdl.hitachi.co.jp, ‡‡nisigaki@cs.inf.shizuoka.ac.jp

Abstract This paper proposes a biometric challenge-response authentication with a key extracted from a fingerprint. The authentication scheme proposed here employs "statistical A/D conversion", which is an effective technique to convert fingerprint to just one and the same ID in real-time. Then, the ID generated from fingerprint is used as a password for challenge-response authentication. The proposed scheme provides advantages such that (i) the user no longer needs to memorize his/her password because the password is a part of body, (ii) the password does not travel on the network since challenge-response authentication is carried out, (iii) user's private fingerprint information would not be revealed from the password because any password is generated from fingerprint with a random number added. The availability of the fingerprint-based challenge-response authentication is studied by comparing it with existing schemes.

Keyword Network authentication, Biometric authentication, Challenge-Response authentication, Statistical A/D conversion

1. はじめに

生体情報は個人の身体的および行動的特徴であり，一般にその個人差も大きいため，本人確認を行う際に有力な情報となる．実際，指紋を用いた個人識別は古くから犯罪捜査などで用いられてきており，また近年では，様々な生体情報が本人認証に用いられている[1]．生体情報は各個人が先天的／後天的に自分自身の体の中に獲得している情報であり，ユーザが認証を行うための情報を新たに記憶したり，特別なデバイスを所持する必要がない．この点で，生体情報を用いた認証はユーザの負担が小さく，利便性に長けていると言える．

しかし，ネットワーク経由での非対面のユーザ認証（以下，「ネットワーク認証」と呼ぶ）に生体情報を用いることは今まで行われていなかった．（DNA を除いて）一般に，生体情報はアナログ情報であり，読み取り誤差が少なからず混入する．よって，「認証を要求しているユーザの生体情報が，前もって登録されている正規ユーザの生体情報に十分近いかを測る」ことによって認証を行わざるを得ない．この方法は a) プライバシに関わる自分の生体情報を前もって検証者に預けておかなければならない，b) 認証時に生体情報をサーバに送信しなければならない，という問題をはらんでおり，これが生体情報によるネットワーク認証の実現を阻む要因となっていた[2]．

著者等はすでに，公開鍵暗号系の秘密鍵を生体情報から生成する「統計的 AD 変換」という方式を考案し，これにより，秘密鍵を保持することのないディジタル署名方式が実現できることを報告している[3]．本稿では，生体情報から一意な「認証鍵（共通鍵暗号系の鍵）」を生成するためにこの統計的 AD 変換を用いることにより，生体情報を使った Challenge & Response 型のネットワーク認証方式が実装できることを示す．

以下，2 章で従来，生体情報がネットワーク認証に適用できなかった理由とその解決のための方針を示す．3 章で生体情報を一意な認証情報に変換するために用いる統計的 AD 変換を概説し，4 章で生体情報から統計的 AD 変換によって生成される認証鍵を用いた Challenge & Response 型のネットワーク認証方式を提案する．5 章では，従来の方式を示し，安全性，計算量，利便性，プライバシの観点で提案方式との比較検討を行う．6 章で本研究の今後の課題を述べ，7 章で本稿をまとめる．

2. 生体認証とネットワーク認証

2.1. 既存の生体認証

生体情報は個人の身体的および行動的特徴を表すものであり，一般にその個人差も大きいことが分かっているため，本人認証を行うに適した情報と言える．生体情報による本人認証は，認証のために新たな情報を記憶したり専用デバイスを持ち歩く必要がなく，ユーザの利便性も高い．すでに，生体情報を用いた多くの本人認証技術が提案されている[1]．

身体的特徴を表す生体情報としては指紋，虹彩などが挙げられ，行動的特徴を表す生体情報としては（手書きの）署名，声紋などが挙げられるが，DNA を除くほとんどの生体情報はアナログデータであるという特徴を持つ．よって，生体情報においては一般に，その読み取り時に人的および外的要因によって何らかの誤差が混入することが避けられない．例えば生体情報をしきい値で量子化してやることにより，量子化誤差未満の読み取り誤差についてはこれを除去することが可能であるが，しきい値付近のデータが読み取り誤差によって変動してしまうと，量子化の結果が異なってしまうことになる．すなわち，生体情報を常に一意で固有な値として取得することは難しい．

このため，DNA を除く既存の本人認証は，基本的に「認証を要求しているユーザの生体情報が，前もって登録されている正規ユーザの生体情報と同一であるかを検査する」のではなく，「認証を要求しているユーザの生体情報が，前もって登録されている正規ユーザの生体情報に十分近いかを測る」という方式にならざるを得ない．

2.2. ネットワークを介した生体認証

ネットワークを通じた通信は非対面となるため，電子商取引をはじめとした多くの状況で，通信者間相互の本人認証が必須となる．この問題を克服するために，様々なネットワーク認証の研究が盛んに行われており，CHAP 認証，SSL 認証など，すでに実用サービスとして結実した成果も多々存在する[4][5]．

これらネットワーク認証技術は暗号学に基づいており，公開鍵暗号系の秘密鍵（前もって登録してある公開鍵に対応する秘密情報）もしくは共通鍵暗号系の秘密鍵（前もって共有しておいた秘密情報）が本人性を証明する情報となっている．よって，生体情報をこれらネットワーク認証技術における認証用の秘密鍵（以下，「認証鍵」と呼ぶ）として用いることにより，生体情報を用いたネットワーク認証を実装することが可能となる．

原理としては，生体情報を AD 変換することにより得られるディジタルデータを認証鍵として用いてやればよい．しかし，2.1 節で述べたように，DNA を除いた生体情報はアナログデータであり，取得の度に読み取り誤差などにより変動してしまう．したがって，ユーザの生体情報を常に一意なディジタルデータにリアルタイムで変換することは非常に難しい．読み取り誤

差により1ビットでも認証鍵が変わってしまうと，暗号技術に基づいているネットワーク認証技術は機能しなくなってしまう．例えば，Challenge & Response 認証においては，送られてきたチャレンジを認証鍵で暗号化（または鍵付きハッシュ化）することによりレスポンスを生成するが，認証鍵が1ビット異なるだけで生成されるレスポンスは全く異なった値となってしまい，認証は不能となる．

このため，暗号学に基づくネットワーク認証技術に生体認証を融合することができず，生体情報を用いてネットワーク越しの認証を実施するには，既存の生体認証の仕組みを単純に遠距離にて行う以外に方法がないというのが現状であった．この場合の認証手順は次のとおりである．

i. 正規ユーザは，前もって検証者に生体情報を登録しておく．
ii. 認証を希望するユーザは，自分の生体情報を検証者に送信し，
iii. 検証者が，認証を要求しているユーザの生体情報が，前もって登録されている正規ユーザの生体情報に十分近いかを測る．

しかしこの方法は，本質的に

a) プライバシの問題：
正規ユーザは，プライバシに関わる自分の生体情報を前もって検証者に預けておかなければならない．（暗号学に基づくネットワーク認証技術における認証鍵は基本的にはランダムなビット列であり，プライバシ情報にはあたらない．）

b) 盗聴の問題：
認証時には生体情報を検証者に送信しなければならないため，送信路の安全性を確保する必要がある．（暗号学に基づくネットワーク認証技術においては，認証鍵そのものが通信路に流れることはない．）

という大きな障害を内包しており，これが生体情報によるネットワーク認証の実現を阻む要因となっていた[2]．

2.3. 生体認証を用いたネットワーク認証の実現

このような状況の中で，生体情報を暗号化鍵に変換する技術の研究開発が進められている[3][6][7]．本稿では，著者らが文献[3]で考案した統計的 AD 変換技術を用い，指紋から認証鍵を生成して Challenge & Response 方式のネットワーク認証を実現する方法を示す．

生体情報に基づく認証と暗号技術に基づく認証が融合した「生体ネットワーク認証」により，以下のメリットが得られる．

a) プライバシの保護：
正規ユーザが前もって検証者に預けておかなければならない情報は，プライバシに関わる自分の生体情報そのものではなく，生体情報と乱数から生成された認証鍵である．

b) 盗聴に対する耐性：
暗号学に基づくネットワーク認証技術（本稿の例では Challenge & Response 認証）を実現することが可能であるため，認証鍵そのものが通信路に流れることはなく，認証を行うにあたり送信路の安全性を確保する必要がない．

c) 利便性の向上：
認証の際に生体情報から認証鍵を動的に生成してやることにより，ユーザは認証鍵の管理から解放される．

d) ヒューマンクリプトの実現：
ユーザと認証鍵が直接リンクするため，認証鍵の紛失や盗難にある程度の耐性を持つ．

e) 証明可能な安全性：ネットワーク認証のプロトコルに関しては暗号学的に安全性が証明される．

3. 統計的 AD 変換

統計的 AD 変換[3]は，正規ユーザの生体情報の特徴量の平均や標準偏差が，不特定多数の生体情報の特徴量の平均や標準偏差と異なるという統計的な性質に基づき，ユーザ各々の生体情報をリアルタイムで常に一意なユニーク ID に変換することができる技術である．本章では，生体情報として指紋を用いて，方式の概要を説明する．

・指紋の特徴量

指紋の特徴量としては，様々な候補が考えられるが，ここでは指紋を小さなブロックに分割し，各ブロック内の隆線の傾きを特徴量とする（図1参照）．

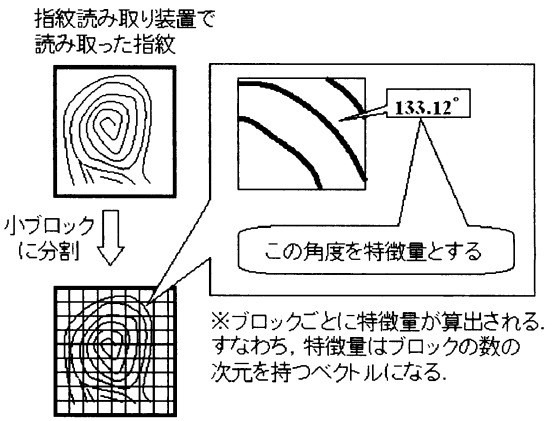

図 1：指紋の特徴量

・指紋の登録

(1) 正規ユーザの指紋を複数回読み取る．同一の生体情報であるが，読み取り誤差が混入するため，異なった生体情報のデータが得られる．

(2) 複数個の指紋データのそれぞれについて，「特徴量」を算出する．

(3) 算出された特徴量の統計を測り，正規ユーザの指紋の特徴量の平均μと分散σを計算する．

(4) 統計的な性質から（特徴量の誤差が正規分布に従っていると仮定して），正規ユーザの指紋であれば誤差が混入しても指紋の特徴量は区間[μ-3σ,μ+3σ]の中に（約 99.7%の確率で）収まることが期待できるため，正規ユーザの特徴量の許可範囲を区間[μ-3σ,μ+3σ]であるとする．そして，特徴量空間におけるその他の区間を許可範囲と同じ大きさに分割する(図 2 参照)．

(5) 分割されたすべての区間に対して，それぞれ乱数を割り当てる．各区間の境界と各区間の乱数のみを記憶する(図 3 参照)．以下，各区間の境界と各区間の乱数を特徴量の「スケール」と呼ぶ．

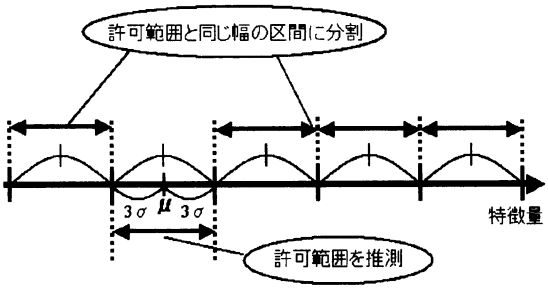

図 2：許可範囲の決定と他の区間の分割

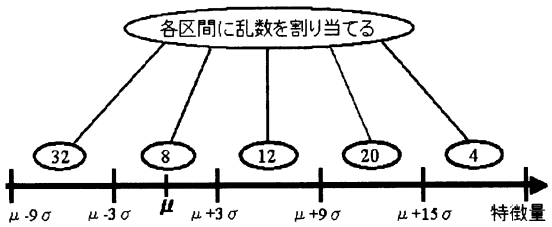

図 3：各区間への乱数の割り当て

・指紋からの ID 抽出

(1) 指紋を読み取り，特徴量を算出する．

(2) 特徴量が含まれる区間に割り当てられた乱数が ID となる．

登録時に一つの指紋から何度も指紋データを読み取って統計量を算出することにより，その指紋に対する読み取り誤差の混入の期待値を測定している．このため，正規ユーザの指紋であれば，ID 抽出時に算出された特徴量はほぼ確実に許可範囲の中に入る．すなわち，正規ユーザの ID は常に同じ値となる．なお，同じ指紋から複数の指紋データを読み取る必要があるのは登録時のみであり，ID 抽出時には毎回，1 つの指紋データを読み取るだけであることに注意されたい．もし本人拒否率が大きい場合には，許可範囲を幾分大きくしてやればよい．

他人受入率を減らすためには，指紋から複数の特徴量を抽出し，十分な数の特徴量ベクトルを用意すれば，ある特徴量のみが許可範囲の中に入る者は正規ユーザ以外にも多数存在するが，それぞれの特徴量がすべて許可範囲の中に入る者は高い確率で正規ユーザのみとなる．今回の例では，指紋を 100 個の小ブロックに分割しており，各ブロックから特徴量（指紋の隆線の傾き）が算出され，特徴量は 100 次元のベクトルとなる．

なお，登録時にユーザごとに作成される特徴量のスケール（デバイスに記憶される各区間の境界と乱数）は秘密情報に当たらないことに注意されたい．境界は特徴量を量子化するためのしきい値に過ぎず，指紋が入力されない限り，どの乱数が正しい ID であるかの確からしさは全て等確率である．

文献[3]で実施されている初期実験の結果からは，100 分割された各指紋ブロックの隆線の傾きから 150 ビット程度のユニーク ID が抽出でき，かつ，本人拒否率と他人受入率をともにゼロとすることが達成できることが確認されている．

4. 生体ネットワーク認証

統計的 AD 変換によって生体情報から常に一意なユニーク ID をリアルタイムで抽出できるため，この ID を認証鍵とすることにより，既存の暗号技術に基づくネットワーク認証を実装することが可能である．これにより，生体情報に基づく認証と暗号技術に基づく認証が融合し，「生体ネットワーク認証」が実現する．本章では，その一例として，指紋を認証鍵とした Challenge & Response 方式の認証システムを説明する．

4.1. 指紋からの認証鍵の生成

統計的 AD 変換によって，指紋を常に一意なユニーク ID（以下，「指紋 ID」と呼ぶ）に変換することができるため，この ID を Challenge & Response 認証の認証鍵として使用することができる．ただし，指紋は変更することができないため，他の何らかの仕組みによって認証鍵の失効および更新に対処する必要がある．

例えば，指紋 ID に乱数を結合したデータを認証鍵

とする方法が考えられる．具体的には，指紋 ID に乱数を連結したデータをハッシュ化してやればよい．以降，統計的 AD 変換の特徴量のスケール(図 3)の中で各区間に割り当てられている乱数と区別するために，指紋 ID に結合される乱数のことを「パスナンバー」と呼ぶこととする．

パスナンバーの目的は一つの指紋 ID から複数の認証鍵を派生させることにあるので，パスナンバーの長さはユーザが記憶できる程度のもの（従来のパスワードと同程度のもの）としてかまわない．ただし，長いビット長のパスナンバーを採用して，指紋が漏洩してしまった場合にもパスナンバーによってある程度の安全性を維持するというアプローチをとることも可能である．しかしこの場合は，ユーザに長いパスナンバーの保管を強いることになるため，利便性とのトレードオフを考えなければならない．

また，統計的 AD 変換の特徴量のスケール(図 3)を更新する方法でも，同じ指紋から異なる認証鍵を生成することができる．特徴量のスケールにおいて，各区間に割り当てられている乱数を適宜変更するだけで認証鍵を変更できるので，3 章に示した指紋の登録操作をやり直す必要はない．

4.2. 指紋による Challenge & Response 認証

3 章で概説した統計的 AD 変換を通じて得られる指紋 ID を用い，生体情報による Challenge & Response 認証のプロトコルを示す．今回は，4.1 節で示した認証鍵の生成方法の内，指紋 ID とパスナンバーを連結したデータをハッシュ化する方法を例に採って説明する．なお，Challenge & Response 認証においては，「認証鍵」は「パスワード」と同義である．

以下，認証鍵（パスワード）の登録手順と，接続要求時の認証手順を記す．ここで，H(･)は一方向性ハッシュ関数，H_k(･)は k を鍵とする鍵付き一方向性ハッシュ関数であり，記号'|'はデータの連結を意味する．図 4 に登録処理の流れを示し，図 5 に認証の流れを示す．

・パスワードの登録手順

（1） ユーザ A はクライアント端末 C に指紋を複数回入力する．

（2） C は統計的 AD 変換の登録を行い，特徴量のスケール（図 3）を生成するとともに，指紋 ID を出力する．スケールを sc，指紋 ID を id とする．C は sc を記憶する．

（3） A は C にパスナンバーpn を入力する．C は H(id|pn)を計算し，認証鍵（パスワード）pw とする．C は即座に id を消去する．

（4） C は pw をサーバ S に送る．この通信に限っては秘密チャネルを使用する．C は即座に pw を消去する．S は pw を保存する．

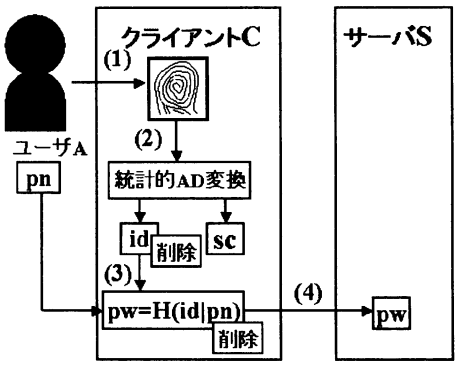

図 4：パスワードの登録

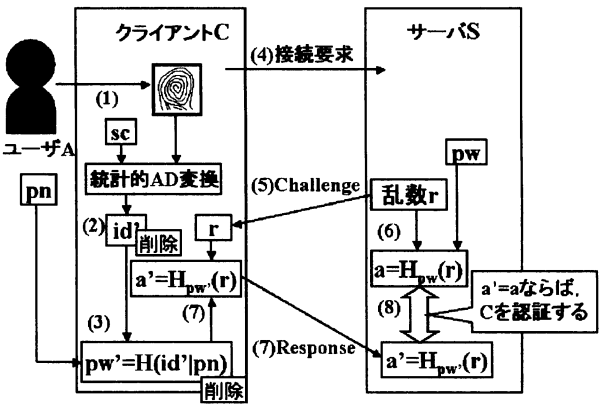

図 5：認証手順

・認証手順

（1） ユーザ A はクライアント端末 C に指紋を 1 回入力する．

（2） C は指紋から特徴量を算出する．スケール sc を参照して，その特徴量が含まれる区間に割り当てられた乱数を指紋の ID として出力する．この指紋 ID を id'とする．統計的 AD 変換の性質上，正規ユーザの指紋であれば id'=id となる．

（3） A は C にパスナンバーpn を入力する．C は H(id'|pn)を計算し，認証鍵（パスワード）pw'とする．C は即座に id'を消去する．正規ユーザの指紋であれば id'=id であるので，pw'=pw となる．

（4） A は C を通して，S に接続要求をする．

（5） S は乱数 r を生成し，チャレンジとして C に送る．

（6） S は，r と所持している pw から a= H_{pw}(r)を計

算する．

（７） Cは，受け取ったrと（３）で生成したpw'を使って，a'=$H_{pw'}$(r)を計算する．Cは即座にpw'を消去する．Cはa'をレスポンスとしてSに送る．

（８） Sは，a'=aであればCを認証する．

5. 考察

本章では4章で示した提案方式と従来の認証方式を比較検討する．ここでは，安全性，計算量，利便性，プライバシ保護の各検討項目について議論する．

5.1. 比較対象

本稿では，以下の3つの認証方式を比較する．認証鍵（パスワード）の登録は済んでいるものとし，各方式の認証手順における安全性，計算量，利便性，プライバシの問題を検討する．

（A） C&R認証：既存のChallenge & Response認証

ユーザAは前もってパスワードpwをサーバSに登録しておく．Sがチャレンジである乱数rを生成し，A（クライアント端末C）が正しいレスポンスを返すことができれば認証する．

（B） OL生体認証：ネットワークを介してオンラインで既存の生体認証を行う方式

ユーザAは前もって指紋情報fpをサーバSに登録しておく．Aはクライアント端末Cを通じて，Sに指紋情報fp'を送る．Sに送られてきたfp'が，Sが保持しているfpに十分近ければ認証する．指紋情報がネットワークを流れるため，盗聴を防ぐ必要があるが，ここではfpを送信の際に公開鍵暗号方式により暗号化する方法を採ることとする．

（C） 生体C&R認証：4章で示した本方式

認証鍵（パスワード）pwの登録は済んでいるものとする．認証時には，ユーザAは統計的AD変換によって指紋から生成される認証鍵pw'を用いてChallenge & Response認証を実行する．

議論を正確にするために，以下に，（A）および（B）のプロトコルを示しておく．（C）のプロトコルは4.2節の「認証手順」に示したとおりである．

・C&R認証（図6）

（1） ユーザAはクライアント端末Cを通して，サーバSに接続要求をする．

（2） Sは乱数rを生成し，チャレンジとしてCに送る．

（3） AはCにパスワードpw'を入力する．

（4） Sは，rと所持しているpwからa= H_{pw}(r)を計算する．

（5） Cは，受け取ったrと（３）で入力されたpw'を使って，a'=$H_{pw'}$(r)を計算する．Cはa'をレスポンスとしてSに送る．

（6） Sは，a'=aであればCを認証する．

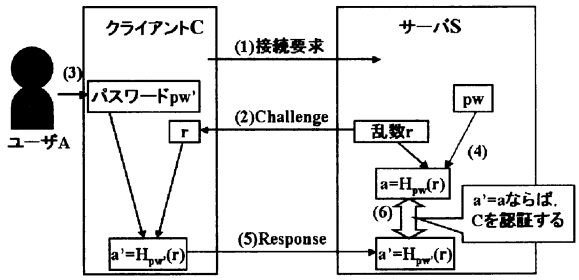

図6：**Challenge & Response**認証

・OL生体認証（図7）

（１） ユーザAはクライアントCに指紋情報fp'を入力する．

（２） Cはfp'を通信路暗号化鍵kで暗号化し，E_k(fp')を得る．ここで，E_k(・)はkを鍵とする暗号化関数である．

（３） AはCを通して，サーバSに接続要求をする．CはSにE_k(fp')を送信する．

（４） Sは受け取ったE_k(fp')を復号して，fp'を得る．

（５） Sは，（４）で得られたfp'が登録されているfpに十分近いかどうか検査する．ここで，マッチング検査関数M(x,y)を，xとyが十分近い場合に1を，そうでなければ0を返す関数として定義することにする．すなわち，M(fp,fp')＝1であればCを認証する．

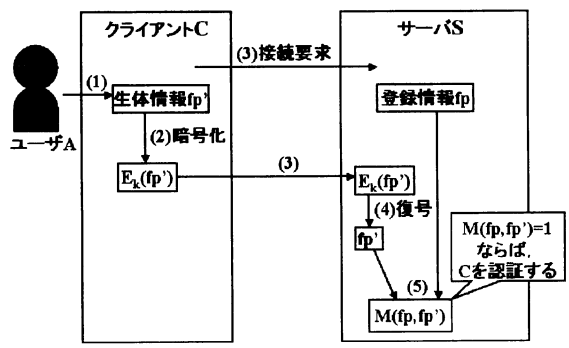

図7：オンライン生体認証

5.2. 比較検討

5.2.1. 安全性

・通信路からの認証情報・生体情報の漏洩

C&R認証と生体C&R認証は，どちらもChallenge &

Response 方式の認証となっており，通信路に認証鍵は流れない．よって，通信路からの情報漏洩に関しては両方式とも暗号学的に差異はなく，リプレイ攻撃にも耐性を有する．

OL 生体認証は，通信路の暗号化により指紋情報の盗聴に対処しており，暗号学的には通信路からの情報漏洩に対して安全である．しかし，ユーザとサーバの間で通信路暗号化用の鍵が共有できているのであれば，その鍵をパスワードとして通常の Challenge & Response 認証を実施すれば用が足りるわけであり，その実効性に疑問が残る．

・クライアント端末からの認証情報・生体情報の漏洩

C&R 認証と生体 C&R 認証は，認証時にユーザがパスワードまたは指紋を入力する方式となっており，普段はクライアント端末内には認証情報・生体情報が存在しない．このため，(パスワードや指紋が入力される認証実行時をピンポイントで狙われない限り，)クライアントへの攻撃に対する耐性は高いと言える．

なお，生体 C&R 認証においては，統計的 AD 変換を行うために指紋の特徴量のスケール（図 3）をクライアント端末に保持させる必要があるが，3 章で述べたようにスケールは秘密情報にあたらないので，クライアントが攻撃された場合にも問題は生じない．

一方，OL 生体認証では，指紋情報を暗号化するための暗号鍵はクライアント端末側で管理されることが多いため，クライアントへの攻撃に対する何らかの対処を取り入れる必要があると思われる．

・サーバからの認証情報・生体情報の漏洩

3 つの方式はいずれもサーバに認証鍵または指紋情報が格納されているため，サーバが攻撃を受けた場合にそれらの情報が脅かされる危険性は同程度であると考えられる．

ただし，C&R 認証と生体 C&R 認証ではサーバに認証鍵が保存されるのに対し，OL 生体認証では指紋情報そのものが保持される．C&R 認証の認証鍵は基本的にはランダムなビット列であり，生体 C&R 認証の認証鍵は指紋情報に乱数が加えられているため，サーバが攻撃された際には，今までの認証鍵を失効して，新しい認証鍵を再発行することができる．しかし，OL 生体認証では，サーバに登録されている指紋情報が漏洩した場合に指紋の変更はできない．また，指紋情報の漏洩はプライバシ保護の観点からも問題である．よって，サーバが攻撃された場合の被害の深刻度は OL 生体認証方式が一番大きいと言える．

以上より，安全性の観点からは，

OL 生体認証＜C&R 認証＝生体 C&R 認証

の関係が成り立つ．

5.2.2. 計算量

C&R 認証では，レスポンスの算出のためにクライアントとサーバの両方でハッシュ関数の計算が必要である．したがって，ハッシュ関数の計算量を CUL_{hash} とすると，C&R 認証の総計算量 $CUL_{C\&R}$ は $2CUL_{hash}$ となる．

OL 生体認証では，クライアント側の処理は指紋情報の読み取り，指紋情報の暗号化であり，サーバ側の処理は指紋情報の復号と指紋情報のマッチング検査となる．これらの計算量をそれぞれ CULread, CULencrypt, $CUL_{decrypt}$, CULmatch とすると，一般的に CULencrypt ＝ $CUL_{decrypt}$ であるため，OL 生体認証の総計算量 $CUL_{OL\text{-}BIO}$ は 2CULencrypt + CULread+ CULmatch となる．

生体 C&R 認証は，クライアント側で指紋から認証鍵を生成した後に Challenge & Response 認証を行うので，C&R 認証の総計算量 $CUL_{C\&R}$ に認証鍵生成の計算量が加わることになる．認証鍵生成は指紋の読み取り，統計的 AD 変換，指紋 ID とパスナンバーのハッシュ化から成るが，統計的 AD 変換は単なるテーブル参照操作であるので，指紋の読み取り CULread とハッシュ化 CULhash が支配的となる．よって，生体 C&R 認証の総計算量 $CUL_{BIO\text{-}C\&R}$ は 3CULhash + CULread となる．

一般に共通鍵暗号処理とハッシュ化処理の計算量はオーダとしては同じくらいであると考えてよいので，OL 生体認証における通信路暗号化が共通鍵暗号で行われていると仮定すれば，CULencrypt＝CUL_{hash} である．また，マッチング検査の計算量は使用アルゴリズムと登録ユーザ数（探索空間の広さ）によって変わってくるので，ここでは大雑把に CULmatch＝CUL_{hash} としておく．この結果，3 つの方式の計算量には，

$CUL_{C\&R} < CUL_{OL\text{-}BIO} = CUL_{BIO\text{-}C\&R}$

という関係が成り立つ．したがって，計算量の効率性という観点では

C&R 認証＞OL 生体認証＝生体 C&R 認証

となる．

5.2.3. 利便性

C&R 認証では，ユーザが認証鍵（パスワード)を入力することになる．したがって，ユーザは認証鍵を安全に管理しておく必要がある．しかし，短い長さの認証鍵は総当たり攻撃に，何らかの意味を持つ認証鍵は辞書攻撃に脆弱となる[8][9]．このため，安全性を確保するためには，ある一定以上の長さのランダムな認証

鍵が要求され，かつ，これを定期的に更新することが要求される．よって，認証鍵の管理はユーザにとって相応の負荷となる．

OL 生体認証と生体 C&R 認証は，どちらも指紋を入力するだけで認証が行われるので,ユーザが認証鍵(に相当する指紋情報）の管理を強いられることはない．なお，生体 C&R 認証においてはユーザは指紋とともにパスナンバーを入力する必要があるが，4.1 節で述べたように，パスナンバーの長さはユーザが記憶できる程度のものとしてかまわないため，パスナンバーを記憶することに対する負担はないとしている．

したがって，利便性の観点からは，

C&R 認証＜OL 生体認証＝生体 C&R 認証

という関係が成り立つと言える．

5.2.4. プライバシの問題

C&R 認証の認証鍵は基本的にはランダムなビット列であり，生体 C&R 認証の認証鍵は指紋情報に乱数が加えられているため，プライバシ情報にはあたらない．

OL 生体認証では，プライバシ情報である指紋情報をサーバに登録する必要があるため，一部のユーザは抵抗感を感じるかもしれない．なお，通信路は暗号化されているため，指紋情報を送信するにあたってのプライバシ情報の漏洩はない．

よって，プライバシ保護の観点からは

OL 生体認証＜C&R 認証＝生体 C&R 認証

である．

5.2.5. 総括

5.2.1 から 5.2.4 の比較結果をまとめると表 1 のようになる．本稿で提案した生体 C&R 認証は，安全性，利便性，プライバシ保護のすべてに優れていることが確かめられた．また計算量的にも，ハッシュ化計算が C&R 認証よりもわずかに 1 回だけ余分にかかるだけであり，実害はないと考えられる．

表 1提案方式と従来の方式の比較

	安全性	計算量	利便性	プライバシ
生体C&R認証	○	△	○	○
C&R認証	○	○	△	○
OL生体認証	△	△	○	△

6. 今後の課題

まず，本方式の重要な要素技術となっている統計的 AD 変換は，まだ研究室レベルでの実験結果しか示されていない[3]．指紋から抽出される ID は高々150 ビット程度であり，かつ，指紋が有する情報エントロピの量も正確な見積りができていない．

第二に，生体情報は毛根や残留指紋から容易に漏洩する[10]．また，怪我や加齢によって，短期または長期で生体情報そのものが変化することがある．

本方式を実用化するために，これらの問題を一つ一つ克服していかなければならない．

7. まとめ

統計的 AD 変換によって指紋情報から生成される認証鍵を使って，Challenge & Response 型の生体ネットワーク認証を実現する方式を示した．生体情報が認証鍵となるので，ユーザは認証鍵の管理から解放され，利便性が向上する．また，既存の関連方式との比較から，利便性だけでなく，安全性，計算量，プライバシの問題といった観点においても本方式が有効であることを確認した．今後は CHAP 認証や SSL 認証をベースに，様々な場面での生体ネットワーク認証を実現することを考えている．

文　献

[1] 瀬戸洋一，"サイバーセキュリティにおける生態認証技術，"共立出版,2002.

[2] 日経 NETWORK 2003 年 2 月号，"特集 1 認証のキホン,問 4 なぜ生体認証をネットワークでもっと使わないのですか？," 日経 BP 社（編）,p.67,2003.

[3] 柴田陽一，三村昌弘，高橋健太，中村逸一，曽我正和，西垣正勝,"メカニズムベース PKI-指紋からの秘密鍵動的生成-," 情報処理学会論文誌，Vol.45, No.8, August 2004（採録決定）．

[4] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol," Netscape Communications Corp., Nov 18, 1996.

[5] Simpson W., "PPP Challenge Handshake Authentication Protocol (CHAP)," RFC 1994, DayDreamer, July 1994.

[6] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B.: "Biometric Encryption," http://www.bioscrypt.com/assets/Biometric_Encryption.pdf.

[7] 板倉征男，辻井重男:"DNA-ID を用いた DNA 個人情報管理システムの提案," 情報処理学会論文誌，Vol.42, No.8, pp.2134-2143 , August 2001.

[8] 三島崇，小森谷良明，Urity，"特集 1 パスワード推測実験室，Part2 ブルートフォースに勝つ”強いパスワード”とは," 日経ネットワークセキュリティ，Vol.2, 2002.

[9] 三輪信雄 監修，白井雄一郎，白濱直哉，又江原恭彦，柳岡裕美 著，"インターネットセキュリティ不正アクセスの手法と防御"，風工舎.

[10] 松本勉:"セキュリティ技術の弱点を発見したらどうしますか？," 電子情報通信学会誌，Vol.84, No.3, pp. 202-204, 2001.