1. 21世紀初頭の暗号技術

7. 個人識別と暗号技術

板倉 征男
情報セキュリティ大学院大学 情報セキュリティ研究科
itakura@iisec.ac.jp

西垣 正勝
静岡大学 情報学部 情報科学科
nisigaki@cs.inf.shizuoka.ac.jp

サイバーワールドは仮想空間であるがゆえに，「個人の識別」が非常に重要な意味を持っており，現代暗号技術に基づくさまざまな認証プロトコルと生体による本人認証が20世紀の個人識別技術の双璧である．21世紀初頭の現在，この2つの個人識別技術が融合し始めた．本稿は，暗号学と生体認証の融合により効果的な個人識別が可能となることを示し，その先駆的な事例としてDNAおよび指紋による暗号／生体融合型認証システムを紹介する．

サイバーワールドにおける個人識別

サイバーワールドの住人をリアルワールドの人物と結びつける「個人識別」は情報社会における必須の技術であり，時空間を超越するというサイバーワールドの性質上，自分が使用する情報機器をアクティベートする際のオフライン認証に加え，ネットワーク越しの通信相手と非対面での相互確認を実現するためのオンライン認証が重要となる．

この社会的要求に対し，20世紀末までに，公開鍵暗号をはじめとする現代暗号技術がサイバーワールドにおける個人識別の基盤として華々しく発展した．また一方で，生体情報を用いた個人識別技術も実用化され，独自の進展を遂げている．その礎となる技術の違いから，この2つの個人識別技術の間には元来，「暗号ベースの個人識別は“相手が秘密鍵所有者であるかを認証する”ものであり，その先，すなわち“秘密鍵所有者が本当の本人であるかを認証する”のが生体ベースの個人識別である」という階層の違いが存在していた．

21世紀初頭の現在，この両者の結びつきが始まり，新しい機能の拡張，効率の向上，安全性の強化やプライバシーの保護のための研究が展開している．

暗号技術と生体情報と個人識別

●暗号技術による個人識別（暗号ベースの認証）

既存の暗号ベースの認証は，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）または公開鍵暗号系の秘密鍵（前もって登録しておいた公開鍵に対応する秘密情報）によって，オフライン認証，オンライン認証を実現する方法である．現在までにさまざまな認証プロトコルが提案されており，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．

暗号ベースの認証は暗号学的にその安全性が証明されているということが大きな特徴であり，「あらゆる不正行為が考えられ得る“オープンネットワーク”の上で“非対面”の相手を認証しなくてはならない」という二重苦を抱えるオンライン認証においてでさえも，安心してこれを使用することができる．また，特にオンライン認証における公開鍵暗号系の寄与は多大であり，公開鍵基盤（PKI）の整備により，ネットワーク越しにまったく面識のない相手を認証する仕組みが確立された．

●生体情報による個人識別（生体ベースの認証）

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．身体的特徴を表す生体情報としては指紋，虹彩などが，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，すでに指紋，虹彩，声紋などによる認証システムが実用化・製品化されている．

アナログデータであるという生体情報（DNAを除く）の性質上，生体ベースの認証は，「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，“十分近いか”を測る」という方式が採られている．このため，生体ベースの認証には本質的に，(i) プライバシーの問題：正規ユーザは，プライバシーにかかわる自分の生体情報を前もって検証者に預けておく必要がある，(ii) 盗聴の問題：認証のたびに，ユーザの生体情報を検

証者に送信する必要がある，(iii) 負荷の問題：検証者は，高級なマッチングアルゴリズムにより (i) と (ii) の生体情報の類似度を検査する必要がある，という弱点が内在しており，オンライン認証は基本的に不得手である．

●秘密鍵と生体情報

生体情報を共通鍵暗号や公開鍵暗号の秘密鍵として用いることにより，暗号ベースの認証と生体ベースの認証の融合が図られる．しかし，一般的に生体情報はアナログデータであるため，生体情報を読み取る際に人的・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．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．読み取り誤差により1ビットでも秘密鍵が変わってしまうと，暗号ベースの認証は機能しなくなってしまう．

対症療法的には，「耐タンパデバイスに秘密鍵を格納しておき，生体ベースの認証によりデバイスをアクティベートする」というアプローチが提案されているが，これでは両方式を併用しているにすぎず，融合に至っていない．

暗号ベースの認証と生体ベースの認証の融合

●暗号／生体融合型認証システム

このような状況の中で，生体情報を秘密鍵に変換する技術の研究開発が進められており，21世紀初頭の現在，いよいよ両認証方式を融合した認証システムが実現しつつある．特に公開鍵暗号ベースの認証と生体ベースの認証が融合することにより，次のような数多くのアドバンテージが得られる．

- ユーザビリティの向上：認証の際に生体情報から秘密鍵を動的に生成してやることにより，ユーザは秘密鍵の管理から解放される．普段はどこにも秘密情報が格納されていない．
- プライバシーの保護：秘密鍵である生体情報は各ユーザが秘密に保持する情報となるため，プライバシー保護の観点からも理に適っている．公開鍵から生体情報（秘密鍵）を推測することも不可能である．
- PKIとの親和性：生体情報（秘密鍵）に対応する公開鍵を登録し，公開鍵証明書を得ることにより，（生体情報そのものは秘密に保持したままで）万人の生体情報の正当性を確認することができる．当然，まったく面識のない相手とのネットワーク越しの非対面相互認証も機能する．なお，生体情報の盗用や鍵の失効および更新に対応するために，生体情報＋乱数を秘密鍵とするなどの方策を採る必要がある．
- ヒューマンクリプトの実現：ユーザと秘密鍵が直接リンクするため，秘密鍵の紛失や盗難に耐性を持つ．
- 証明可能な安全性：暗号ベースの認証の「認証プロトコルの安全性が暗号学的に証明できる」という特長を引き継ぐ．

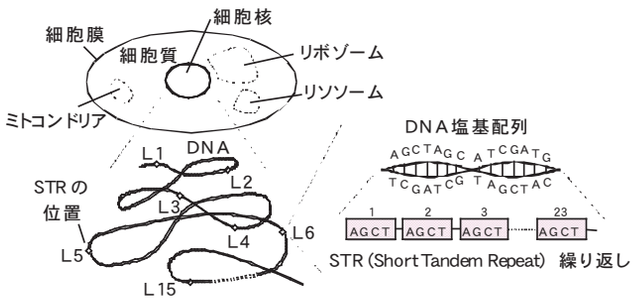

図 -1　細胞の構造と DNA

以下，生体情報を秘密鍵に変換する技術の事例として，ディジタルデータであるDNA情報およびアナログデータである指紋情報から秘密鍵を抽出する方法による認証システムを紹介する．

●DNAからの秘密鍵抽出と認証システムへの適用

個人認証に用いるDNA情報には，**図-1**のように，STR (Short Tandem Repeat) と呼ばれる2～5の短い塩基配列の繰り返しがある部分があり，その繰り返し回数には著しい個人差が見られる．STRの位置はDNAの中で多数存在するが，順番を決めておけば，そのSTRの繰り返し回数の数値を並べるだけで，本人と他人を識別でき，DNA個人IDを生成することができる．このIDはいつ，誰が，どこで測っても同じ数値となり，しかも一生不変である．DNA個人IDは，その人の生体情報ディジタルデータであり，貴重な本人のバイオメトリクス秘密鍵とも言うべきものである[1)]．

このDNA個人IDにハッシュ関数をかけて，生体情報保護とデータ圧縮を行う．生体情報漏洩に対する防御策を考え，従来の秘密鍵に（ハッシュ化された）DNA個人IDを組み込む方法で個人の秘密鍵を生成する．公開鍵の生成はエルガマル暗号方式などによるが，DNA個人ID情報が組み込まれている公開鍵を取り扱う認証局は，生体情報の管理にも関与するバイオメトリクスPKIとなる．

現時点ではDNAから識別情報を抽出するのに最低3時間を要し，分析コストも高価であるが，いずれ解析技術の進歩により秘密鍵の動的生成が可能となり，絶対的精度を誇るリアルタイム個人識別方式が実現するであろう．

●指紋からの秘密鍵抽出と認証システムへの適用

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

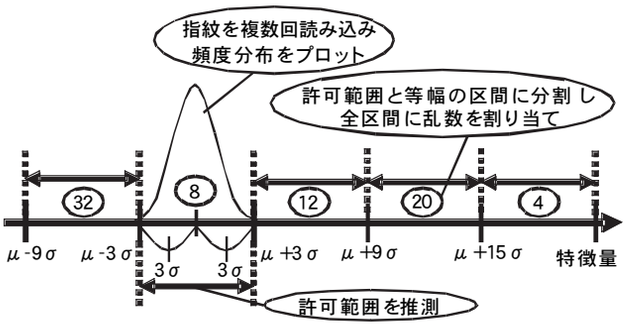

図-2　許可範囲の決定と他の区間の分割

るという統計的な性質を利用することにより，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に変換することが可能である[2]．ここでは，生体情報として指紋を例にとり，その概要を説明する．指紋の特徴量としてはさまざま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（0～180°）を特徴量とする．

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（指紋の各小ブロックの隆線の傾き）を算出する（以降の処理は，各小ブロックごとに行われる）．
(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［$\mu-3\sigma$，$\mu+3\sigma$］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［$\mu-3\sigma$，$\mu+3\sigma$］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**）．
(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（図-2）．各区間の境界値と乱数のみを記憶する．各区間の境界値と乱数は，これらを公開しても，指紋が入力されない限り，どの区間の乱数が正しいIDなのか分からない．

指紋からのID抽出

(1) 指紋を読み取り，特徴量を算出する．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．
(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．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ので，正規ユーザのIDは常に同じ値となる（実際には，すべての小ブロックから同じ方法により抽出された乱数を連結したものがIDとなる）．

指紋から抽出されたIDをそのまま秘密鍵とすることも可能であるが，鍵の失効と更新に対処するため，IDに乱数を加え，これをハッシュ化したものを秘密鍵とする．共通鍵暗号系の認証プロトコルにおいては，この秘密鍵をそのまま使用すればよい．公開鍵暗号系の認証プロトコルの場合には，たとえばエルガマル署名のスキームによって，この秘密鍵に対応する公開鍵を生成して使用する[2]．

今後の課題と展望

●技術的課題

第1に，生体情報は毛根や残留指紋から容易に漏洩する．根本的に漏洩しやすい生体情報をいかに守るかの検討が必須となる．本稿で紹介した認証システムでは生体情報に乱数を加えて秘密鍵を生成しているため，生体情報が漏洩しても乱数が守られれば不正に直結しないといえる．しかし，乱数のみに依拠する認証は，もはや暗号ベースの認証であり，暗号／生体融合型認証システムが有するメリットは消失してしまう．

また，DNAによるシステムには，少なくとも現時点ではDNA抽出のリアルタイム性が欠けるという問題が，指紋によるシステムには，指紋から抽出されるディジタルデータのビット長がまだ短い，指紋が有する情報エントロピの量の正確な見積りができていないという問題が残っている．

●将来的展望

本稿では，暗号学と生体認証の融合により，効果的な個人識別が可能となることを示した．残る技術的課題も少なくないが，今後，ハードルは1つずつ克服されていくものと思われる．21世紀は，今まで閉じた世界で発展を遂げてきた暗号学が，さまざまな他領域の素材や学問と融合し，無限の飛躍をみせる時代になると期待される．

参考文献
1) 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（Aug. 2001）．
2) 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, pp.1833-1844（Aug. 2004）．

（平成16年9月30日受付）