コンピュータセキュリティ　10－20
（2000．　7．25）

DNA 情報を組込んだ公開鍵暗号方式

板倉 征男 *, 岩田 哲 **, 尾形わかは **, 黒澤 馨 **, 辻井 重男 †

* NTT データテクノロジ (株)	〒107-0052 港区赤坂 2-2-12	yitakura@nttdtec.co.jp
** 東京工業大学	〒152-8552 目黒区大岡山 2-12-1	tez@ss.titech.ac.jp
		wakaha@craft.titech.ac.jp
		kurosawa@ss.titech.ac.jp
† 中央大学	〒112-8551 文京区春日 1-13-27	tsujii@ise.chuo-u.ac.jp

あらまし　生体情報を用いて本人識別を適確に行う手法は，バイオメトリックス認証技術として近年脚光を浴びている課題であり，多角的に研究実用化が進んでいる．

本論文では，個人識別情報として一意性のあるデジタル情報が得られる DNA 情報の採取と取扱及びその特徴について述べ，それを公開鍵暗号体系に組込んだシステム及びその効果について論ずる．次に公開鍵に組込むなどの具体的な事例を数種提案する．

キーワード　生体情報，DNA 情報，公開鍵暗号方式，バイオメトリックス，本人認証，暗号通信方式，署名

A Public-key Cryptosystem based on Biomedical-information DNA

Yukio Itakura*, Tetsu Iwata**, Wakaha Ogata**, Kaoru Kurosawa**, Shigeo Tsujii†

* NTT DATA TECHNOLOGY Corporation	107-0052, Akasaka, Minato-ku 2-2-12
** Tokyo Institute of Technology	152-8552, O-okayama, Meguro-ku 2-12-1
† Chuo University	112-8551, Kasuga, Bunkyo-ku 1-13-27

Abstract　Authentication using biomedical-information is widely studied. Among some biomedical-informations, digital DNA information can be used as an identification data. In this paper, we first discuss about its extraction, treatment, and characteristics. Then we discuss the advantages of implementing DNA information in public key cryptosystems. Finally, we present some concrete implementations.

key words　biomedical-information, DNA, public key cryptosystem, biometry, authentication, communication, signature

1 はじめに

生体情報による個人識別を行う方法は, バイオメトリックス認証技術として近年急速に研究実用化が進展している. 指紋及び虹彩によるものは既に商品化され, 高度な本人認証を必要とする日常のシステムに取り組まれつつある [3]. この他網膜, 顔貌, 声紋, 筆跡などがあるが, いずれもアナログ量のパターンマッチングや特徴点比較が基本原理となるため, システム全体における普遍的な ID となるには至らず, もっぱらローカルな規模, 例えば端末における本人認証に使われるに止まっている.

一方生体情報の中で DNA 情報 (塩基配列) は万人不同で不変であると言われているが, 採取, 分析が難しくプライバシー保護の問題もあるので, 長らくバイオメトリックス認証の要素として取り上げられていなかった. 辻井は 1999 年 1 月に DNA 情報の一意性と不変性に着目してこれを秘密鍵に組込み, 公開鍵暗号体系を実現するアイデアを案出した [1, 2]. これを具体化して 2000 年 1 月に発表したが, 内容は DNA 情報の中から一意性がありかつ病気要因に関係のない個人識別情報の採取方法を提案し, それらを ID として公開鍵暗号体系を構成する一方法を示すものであった [4].

このように人的要素を暗号・認証システムに組込む技術の意義については, 今井らがヒューマンクリプトとして提案しているコンセプトにも示されている [5].

DNA 情報から秘密鍵を生成する方法については, 先に太田の特許が公開されている [10]. これは生体情報例えば DNA 情報を個人の秘密情報と考えて鍵を生成する方法であるが, 現状では DNA 情報はその人の毛髪を入手して分析すれば解読できるので, この方法で作った秘密鍵は実用的には秘密が保てず, 鍵の生成のアルゴリズムについて再検討の必要がある. 一方辻井らの提案についても, DNA 情報を鍵に組込む必然性について問題提起が行われている [6].

以上のような背景のもとで, 本稿では DNA 情報をシステムに組込んだ公開鍵の暗号体系について提案し, 生体情報を暗号・認証システムに組込む意義と効果について述べる. また合わせてその具体的な方法をいくつか示す.

2 DNA 情報の採取とその取扱い

2.1 DNA 情報の定義とそのしくみ

DNA の塩基配列は, 個人によって著しく差違を有する部分があるが, その中で病気要因と無関係な部分で親子鑑定等に用いる STR (short tandem repeat) と呼ばれる部分がある. STR は, 特定の塩基配列パターンの繰返しとなっており, その回数は個人によって特有の値を示し, かつ個人間で均等にバラついている. そこでこの STR を複数箇所決めて, そのパターンの繰返し回数をデータとして配列すれば, 個人を識別するデジタル情報として利用することができる [4]. 本稿ではこれを DNA 情報と呼ぶ. 個人ユーザ A の DNA 情報を記号 δ_A で示すこととする.

STR を 11 ヶ所とすれば, DNA 情報は 100 ～ 150 ビット程度の識別情報となる. このような STR は約 5000 ヶ所あるので, もし上記の識別情報の情報量が不足の場合は, 特定する STR の箇所を増やせばよい.

2.2 DNA 情報の採取と取扱い

本稿で取り上げる DNA 情報は, 以下のように採取し取扱う.

(1) **採取.** DNA 情報は, 指紋と同様に個人のプライバシー情報であり, 特に STR 以外の部分は将来医学的な視点から本人の医療行為の基礎情報となるので, DNA 情報の採取と登録は, 公的な生体情報採取・登録機関 (RA：Registration Authority) を設け, 適切な倫理法の元に, 厳重な管理を行うことが必要である.

個人の DNA 情報を採取する場合は, 本人がパスポートや免許証を持参して RA に出頭し, 医師の立会の元に, 口腔の粘膜から綿棒でこすりとった細胞を分析装置にかけて採取する.

採取し配列した生の識別情報を α_A とする.

(2) **登録及び開示.** 採取した個人の識別情報 α_A は, RA に登録し非公開とするが, 個人識別情報のような社会システムの共通基盤的情報については, 特定の資格を持った医療機関や後述の DNA 情報を組込んだ公開鍵を登録する CA 機関等には条件付きで開示する. なお, プライバシー保護の観点から

α_A を生で開示することを避け, α_A に SHS 等によるハッシュ関数演算を行って δ_A とする. 本稿では δ_A を個人識別用情報として取扱い, "DNA 情報" と呼ぶことにする. この場合 δ_A は 160 ビットとなる.

(3) 秘匿演算. DNA 情報は毛髪などからも採取できるので, そのまま個人の秘密情報として利用することは不適切である. 秘密情報とする場合は必ず別に用意する秘密乱数を加えるなど, 何らかの秘匿演算を施さねばならない.

(4) 法的規制. 将来は, 取扱上の法的規則が必要である. 他人の DNA 情報を何らかの方法で採取し, これを不正に利用した者は, 相当な重罰を受けるような法的保護手段が必要である.

2.3 個人識別用生体情報としての DNA 情報の特徴

DNA 情報 δ_A は, 他の個人識別用生体情報 (指紋, 虹彩等) と比較して, 次のような著しい特徴を持つ.

(1) 原情報の属性はデジタル情報である.

DNA 情報は, 特定塩基配列の繰り返し回数を基に生成する識別情報であるから, 本質的にデジタル情報である. 他の生体情報はいずれもアナログ情報であり, このパターンや特徴点の相関一致を基本アルゴリズムとする方式とは元となる情報の属性が異質である.

(2) 有効情報量が多く一意性の精度向上が可.

STR の採取箇所を増やすだけでビット数を容易に増やせる. 即ち, $10^{数ケタ} \sim 10^{5000}$ のデジタル情報が採取可能であり, 高精度の個人識別が可能である. ちなみに他の生体情報はアナログ情報なので精度向上には測定技術の抜本的改善の必要がある. 例えば指紋では, 照合精度について他人許容量が $\sim 1/10^6$ 程度が限度である.

(3) 一生不変情報である.

STR のような DNA 情報は一生不変である. 他の生体情報のうち顔貌, 声紋や筆跡のように経年変化の可能性のある情報とは異質であり, 不変性がある.

(4) 情報の採取と分析に長時間を要す.

最近 3 時間まで短縮された機器が開発されたが, On Site でリアルタイムによる分析は現技術ではできない. 今後の採取分析時間短縮に向けた研究のブレークスルーが必要である.

3 提案するシステムの構成と効果

3.1 基本的なシステム構成要素

図 1 に本稿で提案する DNA 情報をシステムに組込んだ公開鍵暗号システムの構成を示す. ここでは A 氏と B 氏の間で署名, 暗号通信及び本人認証を行う場合を想定したもので, A 氏側の鍵の生成と登録から, その適用の概念を描いている.

基本となる構成要素を説明する.

(1) RA (生体情報採取登録機関). 2.2 で述べたように, RA は CA とは独立した機関であり, 生体情報の採取と登録を行う. DNA 情報 δ_A は本人 A に渡される.

(2) 秘密鍵及び公開鍵. δ_A は直接あるいは間接的に秘密鍵, 公開鍵 (公開情報) に組込まれる.

(3) CA (公開鍵登録機関). 公開鍵を登録し, 本人とその結びつきを証明する機能は従来と同じであるが, 本提案方式では登録の際, RA との間で δ_A の真正性を確認するインターラクションが加わる.

(4) IC カード. RA で登録を終えた DNA 情報 δ_A は, IC カードに書き出されて本人に渡される.

この IC カードには秘密鍵, 公開鍵なども書き込まれ, 署名, 暗号通信及び本人認証を行う際必要な情報を読み出して使う.

(5) A 氏・B 氏端末. 一般の PC 又は UNIX 端末でよいが, これに接続された IC カードリーダライターを備えている.

(6) BIOP. 端末機に付加して設置する BIOP (生体情報処理装置) [4] はブラックボックス化したハードウェアで構成された装置であり, DNA 情報 δ_A の採取・分析, 及び IC カードに直接・間接的に記録された δ_A と本人の δ_A の照合を行う機能を

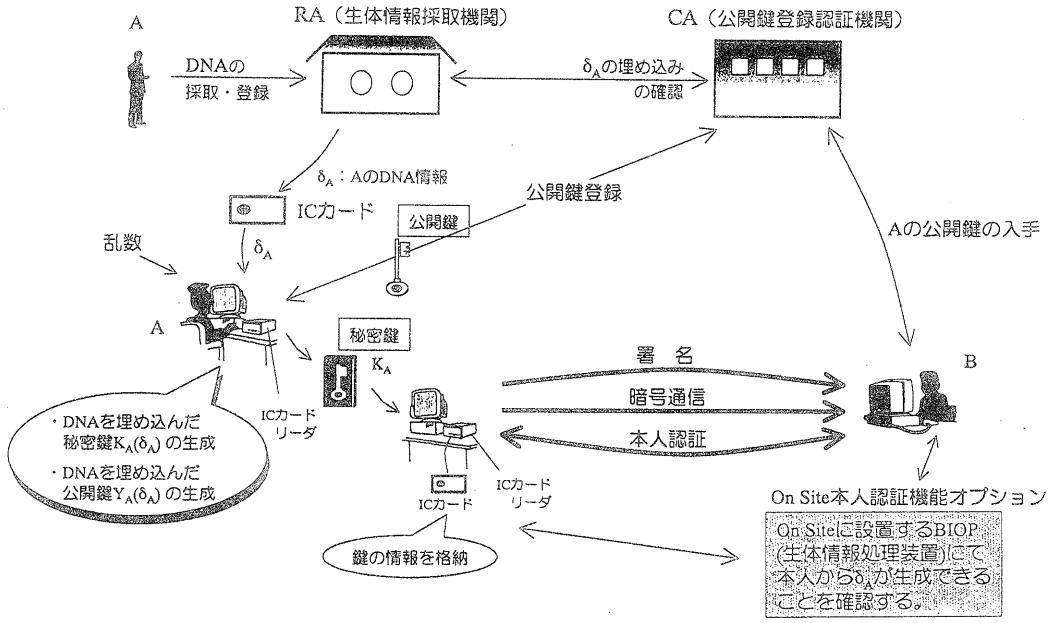

図 1: 提案方式のシステム構成図

有している. いわゆるバイオメトリックス認証機能はこの装置を使って On Site による本人認証を行うことによって実行される.

3.2 システムの機能概要

(1) 署名及び暗号通信の基本機能. A 氏と B 氏の間で署名, 暗号通信及び本人認証を行う場合, 基本機能の動作は従来の方式と同等である. 即ち, 後述の例では署名及び暗号方式として ElGamal, または RSA の署名及び暗号方式 [9, 7] を採択しているが, 他の公開鍵暗号方式でも DNA 情報を組込む方法及びその動作に関する基本的な考え方は同じである.

この基本機能に加えて, DNA 情報を使った本人確認機能を強化するが, その方法として直接 On Site で本人の δ_A を採取し照合する, いわゆるバイオメトリックス認証を行う本格的な方法と, RA に登録済の δ_A と照合する簡易な方法がある.

(2) バイオメトリックス認証機能. 本人認証に用いる DNA 情報の採取は, 綿棒で口腔の粘膜をこすり, 付着した細胞から分析する. 分析は, ブラックボックス化したハードウェア：BIOP (生体情報処理装置) [4] で行うことにより, 人手による人為的ミスや不正を防止する. この装置のオペレーションは登録した係員によってのみ扱われる.

一方, 個人識別に必要な情報の採取分析時間は多くかかるので, 指紋のようにリアルタイムではできない. 従って, On Site によるバイオメトリックス認証機能を (1) の基本機能に取り込むことは, 例えば裁判や特別なネットワーク決裁における本人確認のような特別な用途に限られる.

この場合, 法廷やネットワーク決裁の窓口に BIOP を設置し, 裁判官または登録係員立会の下で, 本人確認を行う. 例えば, 本人から採取した δ'_A から IC カードに記録された公開鍵が生成できるか否かの判定を時間をかけて行う. 公開鍵はもともと δ_A から作られているので, この判定により, δ'_A と δ_A の一致が確認される.

採取分析時間は, 数年前の 1 ～ 数日間のオーダか

ら, 最近は 3 時間まで短縮されてきたので, 近い将来は DNA 情報によるリアルタイム型の本人認証機能が実システムへの適用領域に入ると期待される.

(2) による機能をレベル 2 (バイオメトリックス) 認証機能と呼ぶ.

(3) RA 登録の DNA 情報照合による本人認証機能.
直接バイオメトリックス認証は行わないが, 署名及び暗号通信において鍵等に組込まれた δ_A と RA に登録された δ_A を照合し, 間接的に本人確認を行う方法が考えられる. この方法は, CA における公開鍵証明書の不正発行や, ある条件でのなりすましを検証できるが, 他人の δ_A を採取することが可能なことから, (2) の機能がいざという時発揮できるしくみにしておかねば安全とはいえない.

また RA は本来 δ_A を無条件で開示する機関ではないので, 照合の方法を十分検討する必要がある.

(3) による機能をレベル 1 (RA 照合) 認証機能と呼ぶ.

DNA 情報による (2), (3) の本人認証機能は, 実際に適用するシステムの用途によって実装方法や各部のプロトコルがカスタマイズされる. 具体的システム構築の例は別稿にゆずることとし, 本稿では考え方を述べるにとどめる.

3.3 DNA 情報をシステムに組込む効果

DNA 情報をシステムに組込むことによる不正防止等, システムの信憑性向上の効果は次のように考えられる.

(1) CA 登録時.

1. 公開鍵等の不正登録の抑制.
   本人の動かぬ証拠である δ_A を認証機関である CA に登録し, 証拠として記録管理されるので, 不正登録 (重度の犯罪行為となる) に対する抑止効果が大きい.
2. 公開鍵等登録時の本人確認の確度向上.
   公開鍵等を CA に登録する際, CA・RA 間で本人の δ_A が埋め込まれていることを確認するので, 従来の生体情報無しの登録時より強い本人確認が行われることになる.

(2) 署名時の効果.

1. 血判効果.
   デジタル署名を行うとき, δ_A が署名の中に証拠として残されることになる. いわゆる自らの血判を押印したと同等な効果である.
2. 先方信頼効果.
   署名確認を行う際, 相手の DNA 情報を組込んで登録された公開鍵等を使うので, 結果判定の信頼性の向上が期待される. (さらに厳密に確認を行うには, On Site 本人認証のためのオプション機能を使うことができる.)

(3) 本人認証時の効果.

1. DNA 埋込実印効果.
   公開鍵等に DNA 情報が組込まれていることによる本人認証確度の向上があげられる.
2. On Site 本人認証機能による確度向上.
   高額取引や裁判等での本人認証を行う場合, オンサイトで本人より直接 DNA を採取し, 正しい本人であることを確認できる.

4 DNA 情報組込みの諸方式

ここでは, DNA 情報をシステムに組み込むいくつかの具体的な方法を挙げる (表 1 参照).

4.1 方式 A-0 (簡易方式)

この方式では, δ_A そのものを公開情報として公開鍵と共に登録・公開する. どんな暗号方式, 署名方式にも直接応用可能であり, 最も簡単な方式である.

本システムは従来提案されている任意の暗号方式, 署名方式に基づいて構築される. 秘密鍵や公開鍵の生成は基づいている方式 (これを基本方式と呼ぶ) と同様に行う. ただし, 公開鍵の登録の際に, CA に公開鍵と共に δ_A も登録する. すなわち, 基本方式における CA への登録情報を (ID_A, PK_A), CA による公開鍵登録証明書を $(ID_A, PK_A)^{d_{CA}}$ としたとき, 本システムにおける CA への登録情報および公開鍵登録証明書は

$$(ID_A, PK_A, \delta_A) \text{ および } (ID_A, PK_A, \delta_A)^{d_{CA}}$$

表 1: DNA 情報をシステムに組込む方式

	簡易方式	公開鍵に組み込む		秘密鍵に組み込む	
方式	A-0	A-1	A-2	B-1	B-2
秘密鍵	通常通り	K_A	d_A	K_A, X_A $(K_A = g_1^{\boxed{\delta_A}} g_2^{X_A})$	K_A $(K_A = h(\boxed{\delta_A}\|\|r_A))$
公開鍵	通常通り δ_A を併記	Y_A, g, p, r_A $(g_A = h(\boxed{\delta_A}\|\|r_A))$	n, e_A, r_A $(e_A = h(\boxed{\delta_A}\|\|r_A))$	Y_A, g, g_1, g_2, p	Y_A, g, p

となる.

暗号化は基本方式と同様に行うことができる. ディジタル署名は, 平文 m の後に δ_A を加えたものを文書とし, これに基本方式のディジタル署名をすることで行う.

さらに, ディジタル署名を利用し, 公開情報 δ_A の正当性を検証することにより, 以下のように本人認証を行うことができる.

レベル 1 (RA 照会) 認証. 公開鍵を検証したいユーザは RA に照会して δ'_A を取り寄せ, δ_A と等しいことを確かめる.

レベル 2 (バイオメトリックス) 認証. さらに厳密な本人認証はバイオメトリックス, すなわち DNA から分析して得られた DNA 情報を用いて行う. これは On site 本人認証機能オプションにより行う. ただし, 現状ではリアルタイムで DNA 情報の採取, 分析を行うことができないため, 裁判所における本人認証のような特別な用途に限られる.

On site 本人認証機能オプションは, 本方式だけでなく, 以降に挙げる全ての方式で同様に行うことができる. また RA 照会による本人認証は, δ_A を埋め込んだ値が公開されている場合は常に同様に行うことができる.

IETF のインターネット X.509 PKI 分科会で提示されている Qualified Certificates Profile では, Certificate Extensions にバイオメトリックス情報のアイテムが記述されている. 上記分科会では生体情報として写真や手書き署名等の画像イメージにハッシュ関数をかけた情報を挙げているが, 本方式は, 生体情報として DNA 情報を格納することに対応している.

4.2 方式 A-1 (公開鍵に組込む方式 1)

一般に離散対数問題に基づくシステムは, 公開鍵として大きな素数 p と, 位数 q をもつ元 g を持つ. ただし q は $p-1$ を割り切る大きな素数である. 本方式では, 離散対数問題を基にした方式を基本方式とし, 公開鍵 g_A に δ_A を組込む.

公開鍵, 秘密鍵の生成は, 基本方式とほぼ同様に行うが, 公開鍵のうち g_A は, δ_A および r_A を用いて

$$g_A = h(g_A||r_A) \tag{1}$$

によって計算する. ここで h は公開のハッシュ関数であり, r_A は, g_A が位数 q となるように選んだ乱数である. また, δ_A と g_A との関係を示すためには r_A も公開鍵として公開する必要がある. 鍵の登録の際には, CA は RA より δ_A を取り寄せ, 式 (1) が成り立つことを確認することで本人の δ_A が g_A に組込まれていることを確認できる.

基本方式としては, 暗号方式として ElGamal 暗号, ディジタル署名として ElGamal 署名を用いることができる. また, CA が登録の際に行う手順と同様に, レベル 1 認証を行うことができる.

基本方式においては g の値は全てのユーザーにおいて共通の値とすることができるが, 本システムにおいてはユーザーごとに異なった値となる. したがって, 各ユーザーは g_A が条件を満たすように乱数 r_A を見つける必要がある. $p = 2q+1$ のとき, 位数が q であるような g_A は $q-1$ 個存在し, r_A をランダムに選んだとき, 得られた g_A が位数 q になる確率は

$$\frac{q-1}{p} = \frac{\frac{p-1}{2}-1}{p} = \frac{1}{2}(1-\frac{3}{p}) \sim \frac{1}{2}$$

となる. 従って, ほぼ 2 回のリトライでユーザーは所望の g_A を得ることができる.

4.3 方式 A-2 (公開鍵に組込む方式 2)

この方式では, RSA 暗号系を基本方式とし, 公開指数に DNA 情報を組込む.

公開鍵, 秘密鍵の生成は, 基本方式とほぼ同様に行うが, 公開指数 e_A は δ_A, 乱数 r_A および公開ハッシュ関数 h を用いて

$$e_A = h(g_A||r_A) \tag{2}$$

によって計算する. ただし, e_A が基本方式の条件を満たすように乱数 r_A を選ぶ. また, r_A も公開鍵として公開する. 鍵の登録の際には, CA は RA より δ_A を取り寄せ, 式 (2) が成り立つことを確認することで本人の δ_A が g_A に組込まれていることを確認できる.

4.4 方式 B-1 (秘密鍵に組込む方式 1)

方式 A-1 と同様に離散対数に基づく暗号方式・ディジタル署名方式を基本方式とするが, 公開鍵でなく秘密鍵に DNA 情報を組込む. ただし, DNA 情報は他人によって容易に抽出可能であるため (たとえば髪の毛 1 本から抽出可能である), DNA 情報をランダム化した値を秘密鍵として利用する.

本方式では, $p = 2q + 1, q = 2r + 1$, r, q は共に素数となるような素数 p を用いる. また, mod$p$ で位数 q の要素を g, mod$q$ で位数 r となるような 2 つの要素を g_1, g_2 とする. 秘密鍵 K_A は, 秘密の乱数 r_A を用いて次式で計算する.

$$K_A = g_1^{\delta_A} g_2^{X_A} \bmod q$$

ただし, 他の δ'_A, r'_A の組み合わせから同じ K_A が生成される可能性を避けるために, g_1, g_2 は ID などから一意に決定可能な値をとる必要がある (たとえば, $g_i = h_i(ID + r_i)$ とし, r_i は g_i が条件を満たすような最少の値とする). 公開鍵は基本方式と同様に

$$Y_A = g^{K_A} \bmod p$$

である.

公開鍵の登録において, ユーザー A は, 「$Y_A = g^{(g_1^{\delta_A} g_2^{r_A})} \bmod p$ となる r_A を知っている」ことを証明する ZKIP [8] を CA に対して行う. これは, $G = g^{g_1^{\delta_A}}$ とおき, 与えられている (Y_A, G, g_2) に対して「$Y_A = G^{g_2^{r_A}} \bmod p$ となる r_A を知っている」ことを証明する ZKIP と考えることができる. CA は A の DNA 情報を RA に照会し, Y_A には確かに δ_A が組込まれていることを確認して登録する.

4.5 方式 B-2 (秘密鍵に組込む方式 2)

本方式では, 方式 B-1 と同様に, 離散対数問題に基づく基本方式の秘密鍵に DNA 情報を組込むが, 秘密鍵を CA が生成する.

秘密鍵の生成において, ユーザー A は DNA 情報 δ_A を CA に渡し, CA は次式によって秘密鍵 K_A を計算する.

$$K_A = h(\delta_A||r_A)$$

ただし, r_A は CA が秘密に選んだ乱数, h は公開ハッシュ関数である. K_A は CA から A に渡される. 公開鍵は, 基本方式と同様に

$$Y_A = g^{K_A} \bmod p$$

となる.

本方式によりバイオメトリックス認証を行うには, 本人の δ_A から秘密鍵 K_A が生成できることを K_A を管理する CA が検証することで行う. 即ち On site 本人認証オプションによって第三者立ち会いの下で採取した本人の δ_A を CA に送り, 本人認証の判定を依頼する方法である. 実際には裁判等における厳密な本人認証を行う場合等が考えられる.

5 まとめ

本稿ではまず DNA 情報の採取とその取扱いについての基本的考え方を整理して述べた. その要点は, このような方法で DNA 情報から個人識別情報を生成すれば, デジタル情報として一意性と普遍性のある情報を取り出すことができ, 後のシステムに組込む方法を論ずるに当って信頼性のある基礎情報となることである.

次に, 本稿で扱う公開鍵暗号体系を実現するシステム構成例を具体的に示した. またその基本機能と実際のシステムでカスタマイズすべき本人認証機能の考え方を示した.

また, DNA のような生体情報をシステムに組込む効果と意義について述べた.

次に DNA 情報をシステムに組込む方式について数例を提案した.

今後の課題は以下の通りである.

(1) **DNA 情報に関する課題.** 筆者らが提案した DNA の STR を個人識別用の情報としてあつかうことは, 個々の STR の示す繰り返し回数の個人別ばらつき事象に依存しているので, その分布の一様性についてさらに実験データの分析による裏付けが必要である.

また一意性, 不変性についてもさらに検証が必要である.

採取分析時間については, On Site 検証をリアルタイムに行えるようになるには今後相当時間を要すと思われるが, DNA 関連研究分野の急速な技術向上も考えられるため, 倫理分野と合わせて今後の展開をフォローする必要がある.

(2) **バイオメトリクス認証を取り込んだ本人認証方式の課題.** 本稿で提案するシステムに DNA 情報を組込む方式の委細の評価, 例えば処理能力, 安全性, IC カード等への実装技術などの追求が必要である.

また, パスポート申請や公職選挙のように, 厳密な本人認証が必要な社会システムへの具体的応用方法の検討も今後の課題である.

特にこれらのシステムに対する各種脅威を階層的に分析し, 各々の脅威に総合的に対処策を検討する必要がある.

参考文献

[1] 辻井重男, "東工大 黒澤 馨教授への私信", 1999.1

[2] 辻井重男, "第 3 回 FAIT 打合せ資料", 1999.8

[3] 管知之編, "特集　ここまできたバイオメトリックスによる本人認証", 情報処理, Vol.40, No.11, 1999.11

[4] 辻井重男, 板倉征男, 山口浩 北沢敦, 齋藤真也 笠原正雄, "生体情報が秘密鍵に埋め込まれた構造を有する公開鍵暗号方式", 信学技報, SCIS2000, D07, 2000.1

[5] 今井秀樹, 古原和邦, "ヒューマンクリプトに関するメモ", マルチメディアのための高度化セキュリティ技術シンポジウム参考資料, 2000.3

[6] 今井秀樹, 古原和邦, 渡辺曜大, "ヒューマンクリプトとは", 信学技報, ISEC2000-17, 2000.5

[7] 辻井重男, 笠原正雄編, "暗号と情報セキュリティ", 産業図書, 1990

[8] 岡本龍明, 太田和夫編, "暗号ゼロ知識証明数論", 共立出版, 1995

[9] 岡本龍明, 山本博資, "現代暗号", 産業図書, 1997

[10] 太田健一, "個人情報管理装置及び方法", 公開特許公報, 特開平 11-215119, 1999.8