バイオメトリクス情報とプライバシー

金森 祥子† 川口 嘉奈子‡ 田中 秀磨†

†NICT ネットワークセキュリティ研究所
184-8795 東京都小金井市貫井北町 4-2-1
{kanamori , hidema}@nict.go.jp

‡東邦大学
274-8510 千葉県船橋市三山 2-2-1
kanakothird@hotmail.com

あらまし バイオメトリクス情報を扱うシステムを検討する場合、プライバシーに関する定義を明確にする必要がある。本論文では、情報倫理的観点から、プライバシー定義の再検討を行い、バイオメトリクス技術に関し、これまでに指摘された課題を整理した。その結果、ユーザ保護視点の手法が主であり、それに基づいた技術開発が進められてきたことが明らかとなった。一方で、ユーザ保護のプライバシーを有効にするためには、運営管理者側が、ユーザ情報に干渉しないという視点での技術開発が不可欠である。現行の法的拘束力だけに依存するのではない、システム開発・運営に対する手法の必要性とその要件について示す。

Biometrics authentication technology and Privacy

Sachiko Kanamori† Kanako Kawaguchi‡ Hidema Tanaka†

†Network Security Research Institute, NICT
4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795, JAPAN
{kanamori , hidema}@nict.go.jp
‡Toho University
2-2-1 Miyama, Funabashi City, Chiba, 274-8510, JAPAN
kanakothird@hotmail.com

Abstract When we examine the system that treats biometric information, we have to clarify the definition concerning privacy. In this paper, we reexamine the privacy definition from information ethics aspect, and make clear the problems of biometrics technologies that have been studied before. As a result, it becomes obvious that the system has been developed to protect user privacy, mainly. On the other hand, to activate the protection of user privacy, it is necessary for operation and management to value the user's right. We show the necessity and the requirement of the system development that doesn't depend only on the legal action.

1　はじめに

バイオメトリクス情報による個人認証は、情報は紛失・盗難・失念の心配がないという特徴がある。一方で、バイオメトリクス情報は、個人情報やプライバシーと深い関係があり、バイオメトリクス情報を扱うシステムを検討するにあたり、プライバシーに関する議論は不可欠である。

本論文では、情報倫理的観点から、プライバシーの定義を見直し、バイオメトリクス情報を取り扱うシステムにおいて、これまでに指摘された課題を整理する。また、バイオメトリクス情報は個人情報とプライバシーの問題を兼ね備え、ユーザ視点での情報保護が中心に議論されてきたことを明示する。ユーザ保護のプライバシーを有効にするためには、運営/管理者側が、ユーザ情報に干渉しないという視点での技術開発が不可欠である。現行の法的拘束力だけに依存するのではない、システム開発・運営に対する手法の必要性とその要件について示す。

2　個人情報とプライバシー

バイオメトリクス情報を取り扱うシステムを検討する際に、プライバシーに関する検討が必要である。情報倫理学の分野では、1950 年代から、プライバシーに関して、様々な定義がなされてきた。一方、情報通信分野では、個人情報の保護とプライバシーを同義で扱い、システムを設計している場合が多い。ここでは、情報倫理的観点から、プライバシーを再検討する。

2.1　個人情報とプライバシーの範囲

プライバシーは、個人情報と同義に扱われる場合が多い。そこで、プライバシーと個人情報の違いを明確にする。

表1では、個人情報は、個人を識別する属性を指し、個人情報保護法などで定義されるものとしている。

一方、プライバシーは、法律で定義されるものではない。個人情報の取扱い手続きは法律の定めに従うことで解決するのに対し、プライバシーには明確な法律の規定が存在しない。プライバシーの価値に対する考え方が個々人異なることから、その判断基準も主観的な要素に影響される状況により、扱われ方があいまいな性質を持つ[1]。

表1.個人情報とプライバシーの範囲

情報の公開度	内容	公私の領域	個人情報	プライバシー
公知	・法令等に基づいて公開される場合がある ・氏名、性別	公	○	×
	・住所、生年月日	中間		
非公知	・社会生活上、必要に応じて取得される場合がある ・資格、職業、所得、健康状態、学歴、趣味など	中間	○	△
機微	・本人同意に基づかなければ通常は取り扱われることはない。 ・思想信条、宗教、性癖、労組加入など	私	○	○

○:該当する、△:不明瞭、×:該当しない

2.2　プライバシーの諸定義

プライバシー権は文献[2]に示されている「一人にしておいてもらう権利」の規定が始まりとされている。一方、コンピュータ、ネットワークの発達に伴い、文献[3]では「プライバシー権とは、個人、グループ又は組織が自己に関する情報を、いつどのように、またどの程度他人に伝えるかを自ら決定できる権利である」、「プライバシーとは、自己に関する情報の流通を制御できる個人の能力のことである」と定義された。さらに、文献[4]では、「ある人への接触が何らかの仕方で制限されている状態」と変遷した。その他、文献[5]において、「ある状況において、一個人あるいは集団が他人に対する規範的プライバシー

を持つのは、その状況において、当該の個人あるいは集団が他人による侵害、干渉、情報アクセスから規範的に保護されている場合であり、その場合に限る。」と定義している。

このように、プライバシーの考え方は、とりまく環境や時代の変化に応じて、変遷してきている。プライバシーは、当初は物理的な私的領域であったと考えられ、社会の発達につれ、精神面での内的な不可侵性にまで拡がってきたと考えられている。一般的な理解としては、「他人に知られたくない個人的事項」を指すため、プライバシーを情報と等価にイメージしてしまいがちであるが、私的領域の保護という観点においては、他人からの過剰な接触・干渉などもプライバシー侵害に入ると考えられる。例えば、監視などによる心理的プレッシャーのように、物理的被害や、金銭的損失を伴わない被害であり、これらは無形のプライバシー侵害と呼ばれる[6]。

2.3 受動的及び能動的プライバシー

プライバシーの定義を考える際に、受動的プライバシーと能動的プライバシーに分ける考え方がある。[7]

受動的プライバシーは、前述の「一人にしておいてもらう権利」の行使には他人の協力が必須であり、自分ではどうにもできないという意味で受動的なものである。この権利が守られれば、プライバシー概念の基本的要素である私的領域は侵されない。特に無形のプライバシー侵害を排除するために、必須の概念である。また、個人の自立した活動を保障するための基盤・環境と言える。

プライバシーは、明確な法律で守られてはいないが、侵害されたくないものである。一方、権利とは法律で守られるものであると考えられるので、本来ならば、受動的プライバシーは、権利とは言えないはずである。しかし、ネットワーク上の個人の活動を保障する仕組みを確立するために、ここでは受動的プライバシーを権利と定義する。

一方、能動的プライバシーは、プライバシー侵害に対して、自分を守るために、自分の情報を自分自身で制御するというものである。ネットワークにおいては、自分の情報が知らぬ間に収集され、新たなデータとして利用されることもある。能動的プライバシーの考え方は、このような問題の対策として、個人の情報を制御する権利が必要とされ、重要視されてきた。個人情報の公開/非公開などの選択は、ユーザ自身に委ねられているので、個人情報の扱われ方と、能動的プライバシーの混同の原因の一つと考えられる。

現在では、プライバシーに係わるシステムを検討する際に考えられているプライバシーは、能動的プライバシーを指すことが多い。もともと、プライバシーというものは、前述のように、データという目に見えるものだけではないはずであるが、プライバシーを個人情報と同様に扱う場合がある。ネットワークに流れた情報は制御できないという前提で、ユーザのプライバシーを守ることを考えると、能動的プライバシーに基づいた対策では限界がある。また、現在のように個人情報保護法に基づいた運営/管理側の対策にも限界があるのは明らかである。そこで、受動的プライバシーに基づいたシステムの検討が必要と考えられる。

3 バイオメトリクスと個人認証の課題

バイオメトリクス情報を個人認証に利用するシステムが一般的になってきた。バイオメトリクス情報を個人認証に利用するためには、社会的影響に関する課題、法的課題、運用体制に関する課題等、いくつか挙げられるが、ここでは、プライバシーに関する課題を取り上げる。

3.1 プライバシーに関する課題

文献[8]によると、バイオメトリクス情報も個人情報であると指摘している。しかし、プライバシーに関して、能動的プライバシーの考え方に則

表 2. バイオメトリクス情報に関するプライバシー問題

脅威	説明
取り替え不能な情報の提示	バイオメトリクス情報は取り替えのきかない身体的な特徴であり、そのような究極の個人情報を提示させること自体がプライバシーの侵害である、という考え方がある。
同意なき情報入力	バイオメトリクス情報の非接触入力が可能なシステムでは、不特定多数の個人を対象としたバイオメトリクス情報が、本人の同意を得ないまま入力される可能性がある。
副次的情報の抽出	健康状態、人種情報、対人的印象等、利用目的外の情報が一目瞭然、あるいは抽出され、知られてしまう可能性がある。
個人情報とのリンク	生のバイオメトリクス情報を保持、あるいは他の個人情報とリンクして保持することにより、個人が特定される可能性がある。
同意なき二次利用	監視、犯歴調査、病歴の追跡等、本人の同意を得ないまま、当初の利用目的を逸脱した二次的な使われ方をされる可能性がある。
データの一元管理	一元的にバイオメトリクス情報が管理されるデータベースでは、全ての保存情報が瞬時に検索され、着目の対象となる。
データの漏洩	本人が知られたくない相手、あるいは全く知らない第三者に、自分のバイオメトリクス情報が同意なく漏洩する可能性がある。
不必要なデータ保持	目的とする運用終了後、あるいは本人の要望に反して、入力済みのデータが不必要に保持されたままになる可能性がある。

っており、個人情報とプライバシーの混同が見られる。表 2 は、文献[8]で示されているバイオメトリクス情報に関するプライバシー問題である。表 2 に挙げられた問題のうち、「取り替え不能な情報の提示」に関しては、個人情報とプライバシーの両方に係わる問題であるが、「同意なき情報入力」、「副次的情報の抽出」に関してはプライバシーに関する問題である。「個人情報とのリンク」、「同意なき二次利用」に関しては個人情報に関する問題、「データの一元管理」、「データの漏洩」、「不必要なデータ保持」はセキュリティに関する問題に分けられる。

プライバシーの観点からすると、「同意なき情報入力」、「副次的情報の抽出」は、現状では能動的プライバシーの侵害に分類されることになるが、能動的プライバシーが保護できるだけでは、プライバシー保護として十分とは言えない。環境として整備されていないと守られないという意味で、受動的プライバシーの観点も不可欠である。

3.2 バイオメトリクス情報とプライバシー

バイオメトリクス情報はデータとして見れば、個人情報に分類され、個人情報保護法で守られるべきものである。一方、バイオメトリクス情報は採取の手段により、プライバシー問題が発生する。多くの場合、ユーザの同意のもとで情報を採取することになるが、監視カメラによる不同意の情報の収集もあり得る。さらに、バイオメトリクス情報を扱うシステムは、個人情報の「同意なき二次利用」の危険性を含む。バイオメトリクス情報は単一の情報ではなく、生体に関する様々な情報を含む場合がある。例えば、DNA 情報は個人の特定だけでなく、人種、罹患、遺伝など様々な情報も含んでいる。そのため、同意なき二次利用されたバイオメトリクス情報は、プ

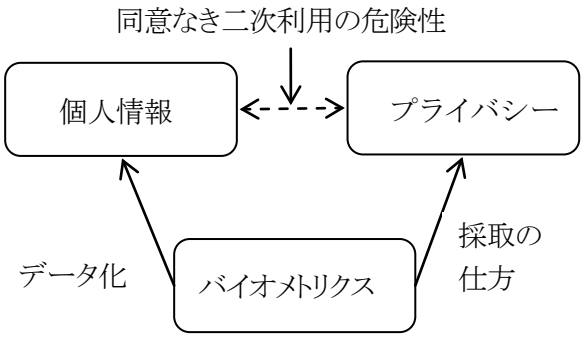

図 1.個人情報、プライバシー、バイオメトリクスの関係

ライバシーを侵害するケースが多いと考えられる。このように、バイオメトリクス情報そのものは、個人情報に分類されるものの、扱われ方や採取の方法はプライバシー関連事項に分類されるものと言える(図 1)。

ユーザ側から見れば、能動的プライバシーにより、情報の採取及び個人情報としてのバイオメトリクス情報の扱われ方がシステムの要件となる。逆に、運営/管理側から見れば、バイオメトリクス情報の採取においては、無形のプライバシー侵害とならないこと、同意なき二次利用を容易に行えないことが要件である。後者は、個人情報保護的な観点だけでなく、データと個人を結びつけないという意味での受動的プライバシー保護の観点によるサービスの提供が重要である。

4 システムの構築と要件

4.1 ユーザ側から見たプライバシー

インターネットの普及に伴い、バイオメトリクス情報を取り扱うシステムを、能動的プライバシーから検討する傾向があることは前述のとおりであるが、これはユーザ側から見たシステムの検討方法である。例えば、「私的な事柄を詮索・開示させない」、「自身の人格的自立を可能とする領域を確保できる」、「一定の私的な事柄について他者の介入なしに独立して決定できる」などがある。ユーザは、自己情報の削除機会や取得の同意などを考慮されている。このように、プライバシー侵害への対処としての機能は考慮されているが、ネットワークで生じた問題を特別視せず、既存の法制度の枠組みで解決することが未だ主である。

4.2 管理/運営者側から見たプライバシー

受動的プライバシーの考え方は、他人が自分のプライバシーに干渉せずに放置してくれることである。従って、ユーザが管理者から一方的な管理、監視と感じることのないよう、管理者はユーザのプライバシーに干渉しない/できない必要がある。網膜パターンから糖尿病患者であることがわかり、顔データから性別、人種がわかるなど、バイオメトリクス情報には、副次的情報を安易に抽出できてしまう。管理/運用者側は、一方的な情報の採取を行わない、バイオメトリクス情報を同意なき二次利用をしないために、受動的プライバシーの考え方を使って、システムを運用することが必要である。

4.3 技術的解決策の動向

能動的プライバシーの保護を確立する手法は、現在までに充分検討されていると考えられる。

受動的プライバシーの保護を確立するためには、匿名認証技術と、暗号化データを復号せずに取り扱う準同型技術などがその要素技術として挙げられる。匿名認証技術とは、登録された正規ユーザであることは認証するが、ユーザの特定までは行わないものである[9] 。これにPIR(Private Information Retrieval)等を応用した秘密検索技術を組み合わせることにより、運営/管理者側は、アクセスしたユーザと読み出されたデータの関連づけを行わずに正規ユーザへのサービス提供をできる[10]。特定の情報にしかアクセスさせない手法として、属性暗号技術も注目されている。属性暗号技術は、設定された情報を有する者のみ復号できる鍵を生成する手法であり、同意なき二次利用を防ぐものとして考えられる[11]。

また、バイオメトリクス情報は単独の利用ではなく、他の個人情報との組み合わせることや、別のサービスとリンクして利用されることも考えられる。この時、復号した生データが流出することを防ぐために、準同型暗号や、Proxy 再暗号技術[12]など、暗号文のままで処理ができる手法の応用も必要である。これは、管理/運営者側がユーザの個人情報を直接扱わないことが特徴である。この特徴は、受動的プライバシーの提供に適切なものと言える。既に実装可能な技術であ

り、実用化へのハードルは高くないと考えられる。

一方で、このような技術が正当にユーザへ提供されていることを示す仕組みも必要である。例えば、暗号モジュールに対しては、CMVP (Cryptographic Module Validation Program)[13]があり、ユーザへ正規のモジュールが提供されていることを示す認証制度が確立されている。暗号プロトコルにおいても同様の制度の確立が必要である。

5 まとめ

2011年3月11日に発生した東日本大震災では、自分の体一つで避難した方が多数であり、生活を再建するために必要な身分証明書等の再発行が困難であった。

このような非常時において、バイオメトリクス情報による個人認証が確立していれば、上記問題に対して少ない妥協で解決できたと予想される。バイオメトリクス情報は、個人特有の情報であること、不変であることなどの理由で、今後、個人認証のために、利用される場面は多くなることが予想される。運営/管理者は、バイオメトリクス情報を取り扱うシステムを構築するに際には、ユーザのプライバシーを守るために、技術的な解決方法、法的な解決方法に頼るだけではなく、受動的プライバシーの観点からの検討をすすめるべきである。

謝辞

本論文作成にあたり、ご協力いだいた財団法人未来工学研究所、笠井祥氏に感謝いたします。

参考文献

[1]「プライバシー影響評価のアセスメント手法に関する調査研究」 平成 19 年度産学戦略的研究フォーラム 海外連携型調査研究

[2]S.D.Warren and L.D.Brandeis, “The Right to Privacy”, Harvard Law Review,1890 http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[3]A.F.Westin, “Privacy and Freedom”,New York: Atheneum,1967

[4]F.Schoeman, “Privacy:Philosophical Dimensions”, American Philosophical Quarterly Vol.21, No.3, July 1984

[5]J. H. Moor, “Towards a Theory of Privacy in the Information age”, Computer & Society, Vol.27, No.3, pp.27-32, 1997

[6]川口嘉奈子、「ユビキタス時代のプライバシー－Google ストリートビュー・セカイカメラなどがもたらす問題の倫理的考察－」IEICE Technical Report SITE2009-6(2009-6)

[7]青柳武彦、「情報化時代のプライバシー研究」 NTT 出版 2008 年 4 月

[8]独立行政法人情報処理推進機構、「各国バイオメトリクスセキュリティ動向の調査」2004 年 2 月 http://www.ipa.go.jp/security/fy15/reports/biometrics/documents/biometrics2003.pdf

[9]D.Viet, A.Yamamura, H.Tanaka, “Anonymous Password-Based Authenticated Key Exchange”, INDOCRYPT 2005, 6th International Conference on Cryptology in India, LNCS 3797,pp.244-257

[10]A.Yamamura, T.Saito, “Private Information Retrieval Based on the Subgroup Member ship Problem”, 6th Australasian Conference, ACISP 2001, LNCS 2119, pp.206-220

[11]M.Pirretti, P.Traynor, P.McDaniel, B.Waters, “Secure attribute-based systems” Journal of Computer Security 18(5): 799-837,(2010

[12]L.Wang, J.Shao, Z.Cao, M.Mambo, A.Yamamura, “A Certificate-Based Proxy Cryptosystem with Revocable Proxy De cryption Power”, Progress in Cryptology - INDOCRYPT 2007, 8th International Conference on Cryptology in India, LNCS 4859, pp.297-311

[13]JCMVP 独立行政法人情報処理推進機構 http://www.ipa.go.jp/security/jcmvp/index.html