生体認証のネットワーク利用におけるリスク評価

宮田孟　任旭輝　吉田太一
(アドバイザー教員：亀山啓輔)

１．はじめに

1.1　研究背景

現在，ネットワーク上で，ユーザーの「財」を守る為に，様々な個人の認証方式が採用されている[1].

現在，最も普及している認証方式はパスワード認証である．パスワードの導入コストが低いので，導入が容易である．ユーザーも扱い慣れている．そして，異なるサイトの安全要求によって，違うパスワードの設定もできる．

しかし，近年，人々のネットワーク利用がますます盛んになるにつれて，大量の情報がネットワーク上に登録されている．それらには個人のプライバシーに関する情報，金銭に関する情報等も含まれる．それに伴って，ネットワーク上の安全性要求も向上してきている．

パスワードの安全性を向上させる研究は現在も進められているが，ユーザーはパスワードという方法の安全性に対し，安全性要求を満たせなくなりつつあるという現状がある．一方で，ユーザーの生体特徴を利用して，認証を行う方法が注目されるようになっている．

生体認証とは，指紋をはじめ，静脈，顔，虹彩，腕振り，筆跡など人の体の一部[9]，またはその人特有な行動を鍵として用いる認証方法である[1][9]．認証する際，パスワードなどと異なることは，モダリティ機器という，生体情報を読み取る機器を通して認証することである．利用の用語定義によって，形態・生理的モダリティを利用する方式と行動的モダリティを利用する方式の２種類の認証方式に分けられる．この中で行動的モダリティの研究は現在も行われているが，実装が少ないため，形態・生理的モダリティの方式を中心に以下では述べることとする．

生体認証に用いられる生体特徴は（1）一人一人に固有であり，同一のものがほとんどない，（2）偽造されにくい，（3）簡便さ，（4）認証を行う本人以外は利用不可という利点があるので，新しい認証方法として研究が進められている．

このように近年研究が進められている生体認証であるが，生体認証は果たして先述したネットワーク利用を安全に行うことはできるのであろうか．ユーザーは生体認証の利用時に潜んでいる危険性を理解していない場合，被害を受ける可能性がある．

1.2　目的

生体認証のネットワーク利用は高い利便性と安全性から，研究や実用化が今後進展することが予想されるが，ユーザーが生体認証の特性を十分に把握せずに利用した場合には思わぬ被害を受ける可能性が考えられる．そこで本研究では，生体認証のネットワーク利用に関するリスクを提示した後，安全な利用に関する提言を行うことで，より安全な生体認証の利用の一助となることを目的とする．

２．セキュリティに関する情報漏洩事件

生体認証の大規模な利用はまだ開始されていないので，生体認証に関連する情報の漏洩事件も報告されていない．従って，そのリスクを評価するために，まず今までに報告されているセキュリティに関する情報漏洩事件を紹介する．

2.1　サーバからの漏洩事件-YAHOO[2]

2012年7月，ある企業のYAHOO社にサーバ運用を委託していく企業がネットワーク経由で不正に侵入されて，およそ50万のユーザーのIDとパスワードが漏洩するという事件が発生した．　事後の調査によると，YAHOOはユーザーのパスワードをプレーンテキストでそのまま保管しており，暗号化されていなかった．　このことにより，侵入者はユーザーのパスワードまで知ることができてしまった．　しかし本来ならば，パスワードは暗号化されているべきであり，そのような場合，サーバがハッキングされたとしてもパスワードが漏洩することは起こらないと思われる．

この事件をきっかけに，GOOGLEのGmailアカウント，MICROSOFTのHotmailのアカウント等のユーザー情報も漏洩した．　その原因は，ネットワーク上で，ユーザーの情報がサイト間で共有されていた為である．　その結果，一つのサイトから情報漏洩が発生すると，他のサイトも被害がおこることが明らかになった[3]．

2.2　個人情報販売事件

2003年に，イギリス政府のInformation Commissioner’s Office (ICO) は，人々の個人情報の保護状況およびイギリスでの個人情報売買を調査するためにOperation Motorman[4]という名前の調査を行った．

その調査の結果からわかったことは，警察や政府機関スタッフが政府のシステムから得た国民の個人情報をある組織に違法に販売し，その組織はさらに情報を新聞記者，探偵，保険会社等に販売していたことであった．　販売された情報は個人の住所，電話番号，電話中の内容，電話する時の場所，友人と家族情報，運転履歴，個人の違法行為記録等を含んでいた．　個人情報に価値がある現代社会ではこのような例が後をたたない[5]．

図1　NECの暗号化指紋認証機器[6]

以上の漏洩事件はパスワードに関する漏洩事件である．　しかし，生体認証などのパスワードと異なる認証方法においても，データの保管方法や認証環境等が同一であるならば[10]，同じようにデータの漏洩事件は起こり得るだろう．

3. 生体認証のネットワーク上での利用の危険性

3.1　モダリティ機器

指紋，虹彩などの生体特徴をモダリティという．そこで，各々の生体特徴を用いて生体認証を行う機器をモダリティ機器(認証機器)と定義する．　例えば指紋認証の場合，次ページのような機器である．さらに最新式のモダリティでは，企業側サーバやPC に依存せず，モダリティ機器内で暗号化することもでき，情報漏洩に対して強いと言われている．また，トークンという，使用者を識別できる機器もつけることが可能で，ライセンス(権限)を持った人のみが生体情報を送ることができるという技術などがある．

3.1　現在の研究状況

生体特徴は生涯不変な情報なため，利用する時に極力漏洩しないことが望ましい．　研究者はこれを意識して，生体認証を利用する際のネットワーク上

のサーバでの生体情報の保管方法に関する研究が進んでいる．

一つ目の研究は secure sketches[7]である． 生体情報にほかの要素を加え，暗号化してサーバに保管する． 加えた要素は変えられるので，サーバに保管された情報も更新できることになる． 認証するときには，ユーザーは自分が持っているライセンス（トークン等）で暗号化された情報の暗号を解き，スキャンされた生体情報と照合して認証を行う．この方法で，ライセンスとサーバ上の暗号化の二つの要素で，ユーザーの生体情報を守る． 現在，この方法で，虹彩や指紋認証を行う方法に関する研究を行っている．

二つ目の研究は biometrics as secure multiparty computation[7]である． この方法では，生体情報も暗号化されてサーバに保管される． 暗号化する関数は公開的だ． 認証する前に，ユーザー側が持っている秘密鍵を確認したら，認証段階に入る． 認証の段階で，スキャンされた生体情報もその関数で暗号化される． この結果と保管された情報を比較して，その間の差が一定の閾値より小さければ，認証を通過する． この方法で，顔認証，指紋認証，虹彩に関する研究が行われている．

三つ目の研究は cancelable biometrics[7]である．この方法は，ユーザーの生体情報の画像を一定の関数で故意に変えてサーバに保管する． 認証の段階には，スキャンされた生体情報を同じ関数で変えて，保管された情報と照合する． この方法で，顔や指紋認証を行う方法に関する研究が行われている．

このように，生体情報も暗号化や変換された状態ならば漏洩したとしても，損害は最小限で抑えられるといえる．

3.2 パスワード方式と生体認証の安全性の比較

3.2.1 サーバ漏洩のリスク

パスワード方式の暗号化と生体認証の暗号化は，暗号化される階層が異なる． パスワードは，企業側が暗号化するかどうかを決める権限がある． それゆえに，Yahoo の事例のようにサーバから暗号化されていない情報が漏洩するとユーザーの個人情報や財などに損害が発生する． しかし，生体認証の暗号化は，モダリティ観測（認証機器）段階で行われるため，そのような機器が一旦主流派を占めてしまえば，企業側が受け取る生体情報はすべて暗号化されたものとなる． この点では，サーバ漏洩のリスクに関しては，パスワード方式よりも安全であると考えられる． しかし，生体情報には一回でも真の情報が漏れたら変えられないというパスワードには無い欠点がある． そして，悪質な業者が様々な方法でユーザーの生体情報を取得しようとすることが想定できる． 以下には，いくつか考えられる例を挙げる．

3.2.2 街中での採取や訪問販売などでの採取

カメラの技術やモダリティの読み取り技術も将来は向上するので，顔や虹彩などの情報は，街を歩く通行人を認証機器と同じ機能をもつカメラなどで撮影したものからでも取れるようになるかもしれない．また，このようにとった情報を Facebook などで掲示されている本人の画像と照合することで，個人を特定できることが想定できる． さらに，カメラなどで通行人の行動を読み取った場合，腕振りなどの行動的モダリティも盗まれる危険がある．

指紋や静脈パターンは接触したり近距離から測定したりすることでしか取得できないものであるが，例えば訪問販売や宅配便などを装って，印鑑の代わりに指紋認証や静脈認証によって本人確認を行う場合には，生体情報を取られる可能性がある．

3.2.3 有害なアプリ

スマートフォンや PC にモダリティ機器がついていた場合，そこから盗まれる可能性もある． ウィ

表１　アンケート概要

実施日程	7 月 24 日，25 日，26 日
調査対象	筑波大学の学群生
回収方法	授業の履修者を対象にアンケート調査
サンプル数	134

ルスなどの方法で，モダリティ機器の暗号化技術を使用不能にして，暗号化されていない真の情報を読み込み，アプリケーション経由で悪質業者が回収するなどのシナリオが考えられる．また，ウィルスそのものでネットワーク上へ生体情報が漏洩してしまう危険もある．

このように生体認証がより広く用いられるようになると，パスワードでは起こらなかったタイプの漏洩が起こる危険が想定できる．そして，一旦真の情報が漏洩してしまった場合，その被害は，変えられるパスワードより大きいものとなる[8]．

4. ユーザーの安全性に対する意識調査

4.1　調査の実施

パスワードと生体認証の両者において，ネットワークを介するデータの漏洩は同様に起こり得ることが予想される．しかし，ユーザーは生体認証とパスワードの利用に関し，安全性に差があると認識していることが懸念される．そこで，筑波大学の学生を対象に，生体認証とパスワードの利用と安全性に関する意識調査を実施した．

調査概要は表 1 の通りである．

また，アンケート調査における設問項目を以下に示す．

a) 個人属性（所属学類）

b) 知っている生体認証のモダリティ

①指紋認証，②静脈認証，③顔認証，④音声認証，⑤筆跡認証，⑥腕振り認証，⑦その他，⑧知らない

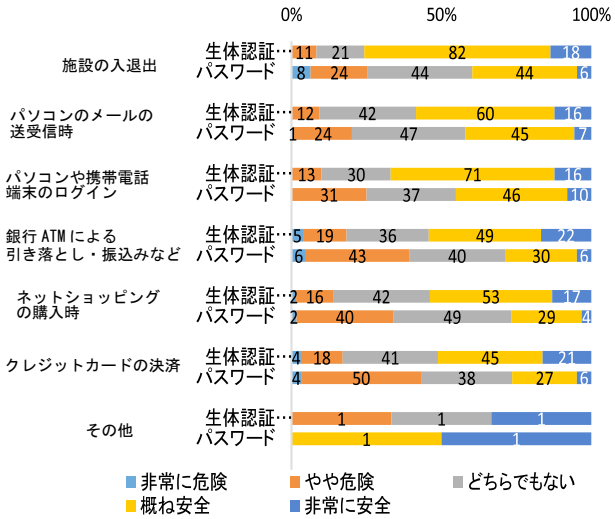

図 2　安全性に関する意識

c) 使用した，もしくはデータを採取された生体認証のモダリティ

b) と同様に回答

d) 生体認証を使用したことがある状況，及び，使用の際に抵抗を感じた認証

①施設の入退出，②パソコンのメール送受信時，③パソコンや携帯電話端末のログイン，④銀行 ATM による引き落とし・振込みなど，⑤ネットショッピングの購入時，⑥クレジットカードの決済

e) 使用状況の違いによる生体認証の安全性に関する意識

d) の各項目について，①非常に危険，②やや危険，③どちらでもない，④概ね安全，⑤非常に安全，のいずれかを選択

f) 使用状況の違いによるパスワードの安全性に関する意識

e) と同様に回答

g) 生体認証のネットワーク上の利用に関する危険性

自由記述

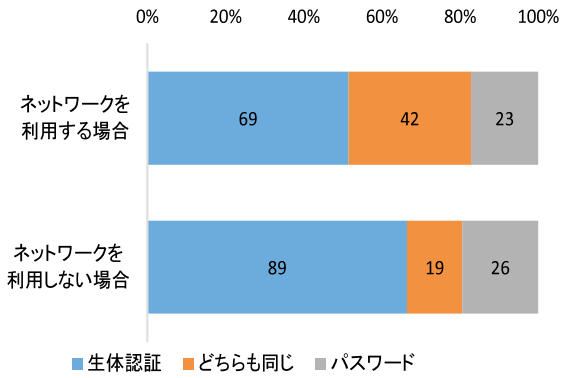

図 3　ネットワーク利用時の安全性

4.2　集計結果と考察

使用状況の違いによる生体認証，及びパスワードの安全性に関する意識の結果を図 2 に示す．生体認証とパスワードのそれぞれで「非常に危険」，「やや危険」と答えた割合と「概ね安全」，「非常に安全」と答えた割合を比較すると，各項目においてに生体認証の方が安全であると判断している傾向にあることが分かる．しかし，前章で述べた通り，生体認証とパスワードには同様の漏洩の可能性があるため，ユーザーは生体認証の安全性を過大評価している可能性があることが考えられる．生体認証の安全性の過大評価が起きてしまうと，情報漏洩などの危機意識が低下してしまう恐れがある．

図 2 の結果は各質問項目に関する安全性の評価の集計結果であるが，各サンプルが生体認証とパスワードのどちらを安全だと考えているのかを示していない．そこで，e)使用状況の違いによる生体認証の安全性に関する意識，f）使用状況の違いによるパスワードの安全性に関する意識の回答から，状況別に各サンプルがどちらの認証方式が安全かを求めた．この結果を用いて，ネットワークを利用する場合とそうでない場合の比較を行う．

「パソコンのメールの送受信時」と「ネットショッピングの購入時」はネットワークを利用する状況であり，それ以外はオフラインの状況である．この 2 つの状況ごとに生体認証とパスワードのどちらが安全かを判断した結果が図 3 である．ネットワークを利用しない場合の方が生体認証を安全だと判断する割合が高い．この結果より，ユーザーは生体認証のネットワーク利用について，安全ではないと判断する傾向にあるということが考えられる．しかし，過半数のユーザーはネットワーク上でも生体認証が安全であると判断しており，3.2 で述べたリスクを考慮すると，生体認証の安全性を過大評価していると判断できる．

ユーザーの安全性に対する意識調査の結果より，生体認証の安全性はパスワードと比較し過大評価されている傾向にあることが分かった．ネットワーク上の利用に関してはオフラインの場合と比べて危険と回答する割合が若干低くなったが，それでも過半数は安全であると判断するという結果になった．これらの結果より，生体認証の安全性についてユーザー適切なリスク評価を行えるように，ネットワーク上の利用に関する危険性について周知を図る必要があるであろう．

５．提言

生体認証には，一生涯変えられない生体情報の漏洩というリスクがある．これは，簡単に変えられるパスワードや暗証番号とは決定的に異なる．仮に生体情報の漏洩が起こってしまった場合，その部位を使って登録した他のサービスや端末ログイン，建物などへの入退出認証の情報も登録しなおし，または，廃止にする必要がある．このように逆にユーザーが不便になってしまうのを防ぐために，私達は社会や企業，またユーザーに対して提言を行う．

まず，社会に対しては，建物内のアクセスや会社の端末ログインなどを除いて，モダリティ機器は，個人単位で持つものであるということ．これは，3.2.2 章で述べた，悪質業者から提示されたモダリティ機器から真の生体情報を読み取られるのを防ぐ

ためである． また，ネットワークを介するモダリティ機器には，顔認証や虹彩認証など接触や至近距離での読み取り以外の方法で読み取れるモダリティ機器を使わないこと． これは，3.2.2.章で述べた街中などで直接生体情報を観測され，それをネットワーク上で利用されることを防ぐためである． 次に，モダリティを製造する側の企業は，暗号化技術を取り入れたモダリティを作ること． また，運用する側の企業は不正アクセス行為などがないかなどをチェックすることである． また，ユーザーの生体情報が漏れて被害が出るなどして発覚した場合は，すぐにその生体情報で登録したサービスすべてを凍結できるようなシステムがあることが望ましい．

そして，ユーザーに対しての提言は，生体情報が換えの効かないものということを意識するということである． 先ほど述べたように，自分のモダリティ機器をしっかり管理し，安易に他の人から提示されたモダリティ機器を使わないことである． そのために，マスメディアなどでこの問題を取り上げることや，これから使うことになるであろう若い世代などへは教育現場で伝えるなどの対策も重要であると言える．

謝辞

本研究を進めるにあたり，第 9 班アドバイザー教員の亀山啓輔准教授から，大変多くのアドバイス，また丁寧かつ熱心なご指導を賜りました． ここに，感謝の意を表します．

参考文献

[1] 古川宏，佐藤美佳[他]：リスク工学の視点とアプローチ: 現代生活に潜むリスクにどう取り組むか，コロナ社，2009

[2] YAHOO サーバの漏洩事件: http://www.csmonitor.com/Innovation/Horizons/2012/0712/Yahoo-hack-steals-400-000-passwords.-Is-yours-on-the-list

[3] YAHOO サーバの漏洩事件の損害: http://money.cnn.com/2012/07/12/technology/yahoo-hack/

[4] Operation Motorman: http://blogs.journalism.co.uk/2011/02/04/observer-seeks-to-distinguish-operation-motorman-from-the-phone-hacking-scandal/

[5] ICO: What price privacy? - The unlawful trade in confidential personal information, Information, Commissioner to Parliament, 2006

[6] NEC イグアス，暗号化／生体認証と管理ソフトを組み合わせた情報漏洩防止パッケージ http://www.nikkeibp.co.jp/article/news/20030521/351232/

[7] S. Rane, Y. Wang, S. C. Draper and P. Ishwar, "Secure Biometrics - Concepts, authentication architectures and challenges -," IEEE Signal Processing Magazine, Vol. 30, No. 5, pp. 51-64, 2013.

[8] 鈴木雅貴，井沼学，大塚玲：生体認証システムにおける情報漏洩対策技術の研究動向，日本銀行金融研究所，2010

[9] EMC:正しい認証方式の選び方ハンドブック,RSA セキュリティ，2008

[10] 桝野隆平:タキヒラパスワードの脆弱性と対策 -認知心理学の知見を生かして,ニーモニックセキュリティ，2010