Vol.2016-CSEC-73 No.13
Vol.2016-IOT-33 No.13
2016/5/26

個人認証における認証要素の特性と多要素認証への適用に関する考察

鈴木 宏哉[1,a)]　山口 利恵[1,b)]

概要：個人認証の重要性の高まりと共に，近年，多要素認証の普及が進んでいる．一方で，複数の認証要素を組み合わせる際の指標となるものが無いため，各サービスに適した認証要素の選択やその適切性の評価が困難という課題もある．そこで，本研究では，既存の様々なサービスを元に，個人認証において必要なセキュリティ要件の洗い出しを行い，その要件項目の整理を行った．整理したセキュリティ要件を指標として用いる事で，様々な認証要素が備えるセキュリティ上の特性の違いを示す事が可能となる．各サービスはそれぞれが求めるセキュリティ要件をこの抽象化した要件項目で定義する事で，必要とする特性を備えた認証要素の組み合わせを検討する事ができる．

キーワード：多要素認証，認証要素，モデル化

The evaluation of the characteristics of the authentication factors for multi-factor authentication

Susuki Hiroya[1,a)]　Yamaguchi Shigetomi Rie[1,b)]

Abstract: The growing importance of personal authentication, the multi-factor authentication is more spreading. However, there is no measure to select authentication factors for multi-factor authentication. The reason for this is because the characteristics of the authentication factors are not organized. In this paper, we organized the characteristics and discussed security requirements of authentication factors for multi-factor authentication.

Keywords: Multi-factor Authentication, Authentication Factor, Modeling

1. はじめに

個人認証の重要性の高まりと共に，近年，多要素認証の普及が進んでいる．多要素認証とは，パスワード認証と指紋認証の組み合わせなど，性質の異なる複数の認証要素を組み合わせる事で，安全性の向上を図る仕組みである．一方で，複数の認証要素を組み合わせる際の指標となるものが無いため，各サービスに適した認証要素の選択やその適切性の評価が困難という課題もある．このため，既存の多要素認証では認証システムの導入時，経験的に組み合わせが決定されるなど，その適切性が議論されないままに利用されている．

また，既存の多要素認証システムでは，サービス開始後の認証要素の動的な追加や入れ替えなどの変更は考慮されておらず，固定された認証要素の組み合わせが用いられている．これは，認証要素が変更されると新しい認証要素の利用方法を覚える必要性が生じ，利用者の利便性が下がるためという理由もあるが，認証要素を評価する指標が無い事も一因である．認証要素が変更できないという事は，ある認証要素に脆弱性が発見された場合，その認証要素の脆弱性が解消されるまで認証システム全体の安全性が低下してしまう．安全性が一定以下に下がった場合，利便性の低

[1] 東京大学
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113–8656, Japan
[a)] susuki.hiroya@sict.i.u-tokyo.ac.jp
[b)] yamaguchi.rie@i.u-tokyo.ac.jp

下を許容してでも認証要素を入れ替える事が有効な場合も存在する．

このように，認証要素の組み合わせを評価する際の指標を示す事は，多要素認証の新規導入時だけでなく，運用時においても有用である．そこで，本研究では，既存の様々なサービスを元に，個人認証において必要なセキュリティ要件の洗い出しを行い，その要件項目の整理を行った．整理したセキュリティ要件を指標として用いる事で，様々な認証要素が備えるセキュリティ上の特性の違いを示す事が可能となる．各サービスはそれぞれが求めるセキュリティ要件をこの要件項目で定義する事で，必要とする特性を備えた認証要素の組み合わせを検討する事ができるようになる．

本論文の構成は次のようになっている．2 章では，個人認証における認証要素，多要素認証に関する関連研究について紹介する．3 章では，本稿で用いる用語と認証のモデルについて説明する．4 章では，既存の様々なサービスで用いられる認証手法を元にセキュリティ要件を洗い出し，その要件項目の整理を行う．5 章で考察を行い，6 章で結論を述べる．

2. 関連研究

2 章では，個人認証における各認証要素と多要素認証に関する関連研究について紹介する．

2.1 認証の 3 要素と多要素認証

認証手法は，各認証要素の特徴の違いから大きく，知識認証 (Something You Know)，所持認証 (Something You Have)，生体認証 (Something You are) の 3 つに分類されており，「認証の 3 要素」と呼ばれている [1]．多要素認証では特徴の異なる認証要素を組み合わせる事が推奨されており，認証要素の特徴を整理する上でこの認証の 3 要素の違いを考慮する事は重要である．一方で，認証の 3 要素にまたがって比較した研究は無く，生体認証の各認証要素の比較 [2] のように 3 要素の中での評価を行った研究が主となっている．

一般的な多要素認証の事例としては，PIN 認証と IC カードを利用した銀行 ATM が代表的なものである．ビジネス用途では RSA の SecurID などのように，ハードウェアトークンやソフトウェアトークンを利用したワンタイムパスワード (OTM) の普及が進んでいる [3]．認証要素の組み合わせには多くのパターンがあるが，既存の研究やサービスは固定された組み合わせのみを検討しており，組み合わされている認証要素に脆弱性が発見された場合について考慮されていない．我々は先行研究で，サービス継続性を考慮し，認証要素の切り替えにより安全性を担保する多要素認証システムの確率モデルを提案した [4]．しかし，提案モデルでは認証要素の独立性を仮定しており，各認証要素の性質まではモデル化せずに扱った．今後，認証要素を確率的に扱うためにも，各認証要素を評価するための指標が必要である．

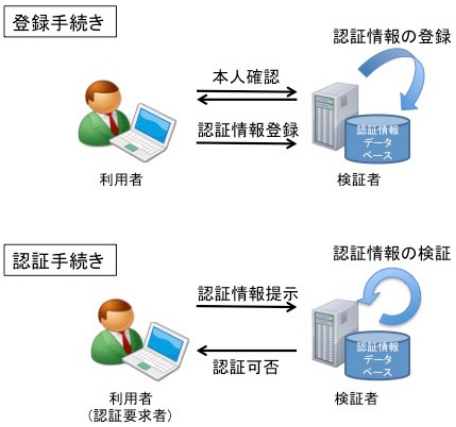

図 1 認証の手続き (登録・認証)
Fig. 1 The procedure of registration and authentication

2.2 行動認証

近年，研究が進んでいる認証手法として，行動的特徴を用いた認証 (以後，行動認証と記す) がある．行動認証には，歩容認証 [5] や署名 [6]，キーストローク [7] を用いた研究があり，歩行や署名，キーボードのタイピングなどの人間の動作や行動に含まれる個人性を用いて認証を行う手法である．行動認証は従来，生体認証の一種に分類されてきたが，本稿では行動認証を認証の 3 要素と同様の分類項目として扱う．

実サービスでの利用が進む行動認証手法としては，リスクベース認証がある．リスクベース認証は，ユーザのアクセス履歴など過去の行動履歴などを元に不正のリスクを評価するもので，利用者自身が明示的な操作を行う必要の無い暗黙的な認証要素が用いられている．代表的な事例として，Google のリスクベース認証がある [8]．Google は，利用者の過去のアクセスにおける IP アドレスや利用している端末，ブラウザなどの利用端末情報を履歴として不審な認証要求に対して警告を行ったり，追加の認証を求める仕組みを提供している．他には，オンラインバンキングやクレジットカードでは購買時の時間帯や金額，送金，購入先が疑わしい場合に操作を停止するようなリスクベース認証が用いられている．

また，スマートフォンや活動量計などのモバイルデバイスの普及により，従来は収集できなかった行動的特徴が収集できるようになっており，位置情報を用いた認証や，Wi-Fi のアクセスポイント情報を用いた認証 [9]，活動量計を用いた認証など [10] が提案されている．

行動認証は近年研究が進んでいる認証手法であり，個別の研究はなされているが体系的に比較したものが無く，従来の認証の 3 要素との違いを示す必要がある．

表 1 認証に関する用語と定義
Table 1 Terms and difinitions about authentication

用語	定義
認証情報	認証要求者が主張する利用者自身である事を立証するための情報
識別情報	認証システム内で利用者を一意に区別するための識別子
認証要求者	認証の対象となる当事者
利用者	認証システムを利用し，認証を行う当事者
検証者	利用者の認証情報を検証する当事者
経路	利用者が入力した認証情報を伝送する道筋
入力装置	認証情報を入力するための装置

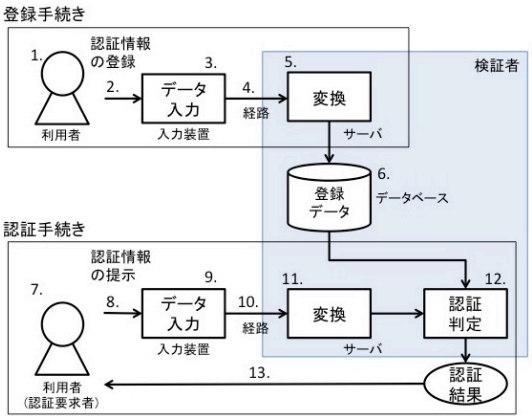

図 2 認証手続きの構成要素と手順のモデル
Fig. 2 Authentication Model

3. 用語の定義と認証のモデル

3 章では，本稿で用いる用語と認証のモデルについて説明する．

3.1 用語の定義

表 1 は，本稿で用いる用語の定義である．NIST の Electronic Authentication Guideline (NIST SP 800-63-2) [11]，及び，情報処理推進機構の「オンライン本人認証方式の実態調査報告書」[12]，日本国政府の「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」[13] などを参考としている．

「認証」とは，「認証要求者」が提示する「認証情報」と，事前に「登録」されている「利用者」の認証情報の同一性を検証する事により，認証要求者が主張する利用者である事の信用を確立する手順である．図 1 は，認証における「登録」と「認証」の手続きの概略を示している．本稿では，図 1 の登録手続きにおける本人確認手続きについては検討せず，正しく行われているものとする．

利用者は，事前に自身を識別可能な認証情報を登録し，認証システムのサービスを受ける．検証者は，サービス事業者などの認証を実施する主体であり，登録された認証情報を管理する．認証情報は，認証要求者が主張する利用者自身である事を立証するための情報である．認証情報には，他人と容易に識別できる容易識別性と，なりすましを防ぐための機密性の両方が求められる．更に，スマートフォンのロック解除のように頻繁に認証を行うシステムの場合，利用者にとって使い易い認証情報である事も重要である．他人が知り得ない秘匿された情報であれば，認証情報は利用者が一意に識別可能な情報である必要はない．

また，本稿における認証情報には識別情報も含む．識別情報とは，認証システムが利用する ID であり，システムに指定された ID を利用する場合と，利用者自身が任意にシステム内で重複しない ID を決定する場合などがある．近年では，識別情報としてメールアドレスを利用するシステムが増えている．これはメールアドレスの一意性を利用して，システム内で一意な識別情報として利用できるためである．1 対 1 認証の場合，識別情報とその識別情報と紐付けて登録されている利用者の認証情報を照合する事で認証を行う．1 対 n 認証の場合，識別情報は必要とせず，提示された認証情報に一定の閾値以上で適合する利用者がいれば，その利用者として認証を行う．

利用者は入力装置を用いて認証情報を入力する．入力装置には，PC やスマートフォンなどの機器に加えて，各種センサや読み取り機が含まれる．本稿では，PC のマウス，キーボード，スマートフォンのタッチパネル，携帯電話のキーについては専用センサ，専用入力装置には含まない．専用の入力装置とは，IC カードリーダや生体認証の読み取り機，GPS センサなどを指す．

3.2 認証のモデル

図 2 は，本稿で想定する認証システムのモデル図である．認証システムを利用するためには，事前の「登録」と「認証」の 2 段階がある．

(a) データ入力
認証情報を入力装置を用いて入力する．登録は図 2 の 1. から 3. の範囲，認証は 7. から 9. の範囲である．
入力された認証情報は経路上を流れて検証者のサーバに届く．入力装置とサーバが直接繋がっているシステムもあれば，経路がインターネットを通っている場合もある．登録は図 2 の 4. の範囲，認証は 10. の範囲である．

(b) 変換
入力された認証情報をデータベースに格納するために変換する．指紋認証などの生体認証では，指紋から特徴を抽出し，テンプレート化を行う．パスワードなどの認証情報では，攻撃などによるデータベースからの情報漏洩対策としてハッシュをかけて変換を行う．登録は図 2 の 5. の範囲，認証は 11. の範囲である．

(c) データベース登録

テンプレートやハッシュにかけられた認証情報をデータベースに登録する．図 2 の 6. の範囲である．本稿では 5. と 6. の間の経路に対する攻撃は検討しない．

(d) 認証判定
登録データと認証要求者によって入力されたデータを照合し，照合の条件を満たすかどうか判定し，認証要求の結果を返す．図 2 の 6. と 12. から 13. の範囲である．

次章では，図 2 の認証システムを用いて認証を行う認証要素の整理を行う．

4. 認証要素の整理とセキュリティ要件

4 章では，既存のサービスで利用される認証要素を元にセキュリティ要件の洗い出しを行い，その要件項目の整理について説明する．

4.1 なりすまし

認証システムにおける主な脅威は，攻撃者が不正に入手した認証情報を用いて認証を行うなりすましである．なりすましは，秘匿されるべき認証情報の機密性を脅かす攻撃であり，認証情報の入手方法や入手先により分類できる．

表 2 は，なりすましに相当する攻撃をまとめたものである．各種攻撃と認証要素の関係性を安全性の観点で整理しており，「×」はその攻撃に対して脆弱性がある事を示し，「○」はその攻撃に対して脆弱性が無い，もしくは「×」と比較して十分に安全な事を示す．「△」は脆弱性はあるが，攻撃が成功するために条件があるなど，限定的な脆弱性を持つ事を示す．表 2 により，「×」がある認証要素を選択した場合は，その「×」を補う「○」がある別の認証要素を組み合わせる事で，より安全な組み合わせの多要素認証システムとする事が可能である．

攻撃者がなりすましを成功させるには，正規の利用者が持つ認証情報が必要である．認証情報の入手には大きく，攻撃者が利用者本人から入手する方法と，攻撃者が推定により認証情報を見つける方法がある．または，利用者と検証者の間の経路上で不正を行う事で，認証情報そのものを入手せずになりすます手法がある．なりすましは図 2 の 1. から 4. と 7. から 10. に相当する範囲に対する攻撃である．

表 2 の模倣，模造と偽造は利用者本人から認証情報を入手する攻撃である．ここで「覗き見」と「観察」はいずれも視覚的に認証情報を得る攻撃であり，その違いは，利用者により入力された認証情報を見るか，入力している利用者本人または入力手段を見るかで区別した．

認証情報を推定する攻撃に関して，総当たり攻撃・辞書攻撃・ウルフ攻撃は攻撃対象となる利用者の情報を使わずになりすます方法で，推測攻撃・リスト型攻撃は，利用者の情報を間接的に使い認証情報を推定する．リスト型攻撃は他の認証システムから漏洩などで入手した情報を利用し，利用者がパスワードなどで使い回しを行っている際に攻撃が成功する．

4.2 認証要素の特徴

前節の表 2 で検討した各認証要素のその他の特徴を，表 3 にまとめた．各種特徴と認証要素の関係性を安全性・利便性の観点で整理しており，「×」はその特徴が安全性や利便性を低下する要因を示し，「○」は安全性や利便性に影響が無い，もしくは「×」と比較して影響が少ない事を示す．「△」は軽微な影響があるなど，限定的な事を示す．

専用機材の有無については，認証システムのコストやユーザビリティに影響する要件である．入力のゆらぎに関しては，生体認証のように利用者が正しく入力していても認証精度が 100%にならないような認証要素もあるため，求められる精度に合わせて認証要素を選択するために必要となる．

経年変化は，時間により認証情報が変化するかどうかの永続性について表している．認証情報が変化する認証要素の場合，登録情報が実際の利用者の認証情報と一致しなくなる前に更新する必要がある．生体認証では成長に伴い，声変わりや顔形が変化する．また，所持認証においても，長期視点で見た場合に IC カードの劣化などが起こり得る．行動認証は特に出張や引越しなどで環境が変わると収集される情報が変化するという特徴があり，認証の更新が重要となる．

履歴長とは，認証情報として必要とするデータの長さ (Window 幅) を示している．パスワード認証や指紋認証のように，利用者が認証を要求するその時点での認証情報だけを提示できるものと，一定期間の履歴を必要とする行動認証とでは履歴長が異なっている．

社会的受容性についてはプライバシーに関わる問題であり，社会全体としての受容性と個々人の受容性には差異がある．そのため，一概に決定する事はできないが，生体認証のように個人に強く結びつき，かつ任意に変更できない認証要素に関して受容性が低下する傾向にある．

4.3 認証に対する攻撃と影響する構成要素

表 4 では，認証システムに対する攻撃とその攻撃が影響を及ぼす認証システムの構成要素について整理を行った．この表を用いる事で，利用している認証要素がどの攻撃に対して，どの構成要素を守れば良いかを検討する事ができる．「×」は各種攻撃の影響がある構成要素を示し，「-」は影響がない事を示す．

表 4 では，表 2 で検討したなりすまし以外の攻撃についても評価した．なりすまし以外の攻撃としては，認証システムのサービスそのものを不能にする種類の攻撃と，データを破壊したり，改ざんする種類の攻撃について検討を行った．

Vol.2016-CSEC-73 No.13
Vol.2016-IOT-33 No.13
2016/5/26

表 2 各認証要素のなりすましに対する安全性評価
Table 2 Security evaluation of spoofing of authentication factors

種別		模倣・模造・偽造						推定					経路			利用者	
詳細		覗き見	キーロガー	盗聴	観察	残留物	盗難	総当たり攻撃	辞書攻撃	ウルフ攻撃	推測攻撃	リスト型攻撃	再送攻撃	中間者攻撃	パケット盗聴	ソーシャルエンジニアリング	強要
知識	パスワード	×	×	○	○	○	○	△	×	○	×	×	×	×	×	×	×
	PIN	×	×	○	○	○	○	×	×	○	×	×	×	×	×	×	×
	パターンロック	×	○	○	○	○	○	×	×	○	×	×	×	×	×	×	×
	秘密の質問 [a]	×	×	○	○	○	○	△	×	○	×	×	×	×	×	×	×
	属性情報 [b]	×	×	○	○	○	○	×	×	○	×	×	×	×	×	×	×
	画像	×	○	○	○	○	○	×	○	○	×	×	×	×	×	×	×
生体	指紋	○	○	○	△	×	△	○	○	×	○	×	×	×	×	×	×
	網膜	○	○	○	△	○	○	○	○	×	○	×	×	×	×	△	×
	虹彩	○	○	○	△	○	○	○	○	×	○	×	×	×	×	△	×
	静脈	○	○	○	△	○	○	○	○	×	○	×	×	×	×	△	×
	顔	○	○	○	×	○	○	○	○	×	○	×	×	×	×	×	×
	声紋	○	○	×	○	○	○	○	△	×	○	×	×	×	×	×	×
	DNA	○	○	○	○	×	×	○	○	△	○	×	×	×	×	×	×
行動	歩容	○	○	○	×	○	○	○	○	×	○	△	×	×	×	△	×
	署名	△	○	○	△	△	△	○	○	×	△	△	×	×	×	×	×
	キーストローク	○	×	○	○	○	○	○	○	×	○	△	×	×	×	×	×
	活動量	○	○	○	△	○	△	○	○	×	○	△	×	×	×	△	×
	位置情報 [c]	○	○	○	△	○	△	○	○	×	△	△	×	×	×	△	×
	行動履歴 [d]	○	○	○	△	○	○	○	○	△	△	△	×	×	×	△	×
	利用端末情報 [e]	○	○	○	△	○	△	○	△	×	△	△	×	×	×	△	×
所持	利用端末	○	○	○	△	○	×	○	○	○	○	○	×	×	×	×	×
	IC カード [f]	○	○	○	○	○	×	○	○	○	○	○	×	×	×	×	×
	乱数表	×	○	○	○	○	×	○	○	○	○	○	×	×	×	×	×
	暗号鍵	○	○	○	○	○	×	○	○	○	○	○	×	×	×	×	×
	OTP [g]	○	○	○	○	○	×	○	○	○	○	○	○	×	○	△	×
	SMS [h]	○	○	○	○	○	×	○	○	○	○	○	×	×	○	×	×

[a] 質問の回答を自由記述で設定可能な認証手法
[b] 生年月日，住所，電話番号などの個人情報を用いた認証手法
[c] GPS，IP アドレス
[d] 利用時間帯，金額，振込先
[e] OS，ブラウザ情報
[f] クレジットカード，銀行カード
[g] ワンタイムパスワード，トークンの種類については考慮せず
[h] SMS や Mail を使った 2 経路認証

Vol.2016-CSEC-73 No.13
Vol.2016-IOT-33 No.13
2016/5/26

表 3 認証要素の特徴

Table 3 The other features of authentication factors

種別		入力装置		認証情報						社会的受容性
詳細		専用機材の有無 [a]	入力のゆらぎ [b]	秘匿不能性 [c]	変更可能性 [d]	類似性 [e]	経年変化 [f]	履歴長 [g]	忘却，紛失	プライバシー
知識	パスワード	○	○	○	○	○	○	○	×	○
	PIN	○	○	○	○	○	○	○	×	○
	パターンロック	○	○	○	○	○	○	○	×	○
	秘密の質問	○	○	○	○	○	○	○	×	△
	属性情報	○	○	○	△	○	△	○	△	○
	画像	○	○	○	○	○	○	○	×	○
生体	指紋	×	×	×	×	△	×	○	○	△
	網膜	×	×	△	×	△	×	○	○	△
	虹彩	×	×	△	×	△	×	○	○	△
	静脈	×	×	△	×	△	×	○	○	△
	顔	×	×	×	△	△	×	○	○	△
	声紋	×	×	△	×	△	×	△	○	△
	DNA	×	×	×	×	△	×	○	○	×
行動	歩容	×	×	△	△	○	×	△	○	○
	署名	×	×	×	△	△	×	△	○	○
	キーストローク	×	×	×	△	△	×	△	○	○
	活動量	×	×	△	△	△	×	×	○	○
	位置情報	×	×	△	△	×	×	×	○	△
	行動履歴	○	×	△	△	△	×	×	○	△
	利用端末情報	○	○	×	○	×	△	×	○	○
所持	利用端末	×	○	△	○	△	○	○	×	○
	IC カード	×	○	○	○	○	△	○	×	○
	乱数表	×	○	○	○	○	○	○	×	○
	暗号鍵	×	○	○	○	○	○	○	×	○
	OTP	△	○	○	○	○	○	○	×	○
	SMS/Mail	×	○	○	○	○	○	○	×	○

[a] 専用の入力装置を必要とするかどうか
[b] 利用者の操作や入力装置の性能，周辺環境の影響により認証精度が変わるかどうか
[c] 認証情報を隠す事ができるか
[d] 認証情報を変更できるかどうか
[e] 同一または類似の認証情報を持つ他の利用者が存在するか
[f] 経年変化と表記しているが，時間変化全般を指す
[g] 一定期間の認証情報を必要とするかどうか

表 4　認証に対する攻撃と認証システムの構成要素
Table 4　Attacks and the components of the authentication system

	利用者	入力装置	経路	サーバ	データベース
なりすまし	×	×	×	-	-
標的型攻撃 (利用者)	×	-	-	-	-
標的型攻撃 (検証者)	-	-	-	×	×
マルウェア感染 (利用者)	×	-	-	-	-
マルウェア感染 (入力装置)	-	×	-	-	-
マルウェア感染 (検証者)	-	-	-	×	×
ランサムウェア	×	-	-	-	-
中間者攻撃	-	×	×	-	-
ソーシャルエンジニアリング	×	-	-	-	-
改ざん		×	×	-	×
DoS 攻撃	-	×	×	×	×
データ汚染攻撃	-	-	-	-	×

標的型攻撃やマルウェア感染は，大きく利用者を狙った攻撃と検証者を狙った攻撃に分ける事が可能であり，それぞれに対策は異なる．

5. 考察

5 章では，4 章で示した認証要素とその要件項目について考察する．

5.1 認証要素の独立性

認証要素の中には，要素間で独立でないものもある．生体認証の場合，同じ個人の異なる身体的部位を用いているため，認証要素間の関係がある．例えば，声紋は犯罪捜査でも用いられているように，性別や顔形，身長，年齢の推定が可能である．本稿では，要素間の関係性について個別に検討を行わなかったが，知識，所持，生体，行動の各認証要素はそれぞれ独立性の高い認証要素となっている．更に，従来推奨されてきた知識，所持，生体，行動の組み合わせで認証要素の欠点を補う手法の有効性が，表 2 からも確認できた．

5.2 経路に対する攻撃

表 2 において，経路上の攻撃には多くの認証要素が安全でないとなっているが，多くの認証システムでは経路上の安全性を担保するために，チャレンジレスポンス認証などの仕組みが利用されている．本稿では，認証要素単独の特徴を評価するため，チャレンジレスポンス認証などは除外して検討した．この結果，経路に対する対策が無くとも安全性を保てる認証手法として，ワンタイムパスワードの有効性が確認できた．

5.3 ソーシャルエンジニアリング・強要

ソーシャルエンジニアリングは情報通信技術を使用せず，ユーザを直接騙して認証情報を入手する攻撃手法である．強要は，脅迫などの手段により，利用者本人に正規の手続きで認証を行わせる攻撃手法である．いずれも，正規の利用者本人が直接認証を行う，または間接的に認証の幇助を行っており，各認証要素が持つ特徴では攻撃かどうかを判別する事が困難である．これらの攻撃に対しては，別途，防犯カメラのような仕組みがなければ防げない．同様に，悪意ある利用者による認証システムに対するなりすましや替え玉などの行動を防ぐにも，認証要素とは別の仕組みが必要となる．このような攻撃に対しては，予防ではなく発生後の事後対策に重点を置き，責任追及性や否認防止の観点も必要である．

6. まとめ

近年，普及が進む多要素認証において認証要素の適切な組み合わせを決めるための指標が必要である．本研究では，既存の様々なサービスを元に，個人認証において必要なセキュリティ要件の洗い出しを行い，その要件項目の整理を行った．今回整理したセキュリティ要件を元に，必要とする特徴を備えた認証要素の組み合わせを検討する事ができる．

今後の課題としては，認証要素の選択のための指標として，各認証要素の安全性だけでなく利便性についても整理が必要である．

謝辞　本論文の研究は，次世代個人認証技術講座（三菱 UFJ ニコス寄付講座）による．

参考文献

[1] 板倉征男，外川政夫：ネット社会と本人認証–原理から応用まで–，電子情報通信学会 (2010).
[2] 瀬戸洋一：バイオメトリックセキュリティ認証技術の動向と展望，情報処理，Vol. 47, No. 6, pp. 571–576 (2005).
[3] RSA: RSA SecurID, RSA (online), available from ⟨https://www.rsa.com/ja-jp/products-services/identity-access-management/securid⟩ (accessed 2016-04-19).
[4] Susuki, H., Yamaguchi, R. S. and Sakamoto, S.: Multi-

Factor Authentication Updating System Evaluation Dynamically for Service Continuity, *The 2nd International Conference on Information Systems Security and Privacy* (2016).

[5] Iwama, H., Okumura, M., Makihara, Y. and Yagi, Y.: The OU-ISIR gait database comprising the large population dataset and performance evaluation of gait recognition, *Information Forensics and Security, IEEE Transactions on*, Vol. 7, No. 5, pp. 1511–1521 (2012).

[6] Schimke, S., Vielhauer, C. and Dittmann, J.: Using adapted levenshtein distance for on-line signature authentication, *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, Vol. 2, IEEE, pp. 931–934 (2004).

[7] Bergadano, F., Gunetti, D. and Picardi, C.: User authentication through keystroke dynamics, *ACM Transactions on Information and System Security (TISSEC)*, Vol. 5, No. 4, pp. 367–397 (2002).

[8] Google: 前回のアカウントアクティビティ，Google（オンライン），入手先 ⟨https://support.google.com/mail/answer/45938?hl=ja⟩（参照 2016-02-28）.

[9] Kobayashi, R. and Yamaguchi, R.: A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User, *2015 Third International Symposium on Computing and Networking (CANDAR)*, IEEE, pp. 463–469 (2015).

[10] Susuki, H. and Yamaguchi, R. S.: Cost-Effective Modeling for Authentication and Its Application to Activity Tracker, *Information Security Applications*, Springer, pp. 373–385 (2015).

[11] Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S. and Nabbus, E. A.: NIST Special Publication 800–63–2 Electronic Authentication Guideline, National Institute of Standards and Technology (online), available from ⟨http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf⟩ (accessed 2016-04-07).

[12] 情報処理推進機構：オンライン本人認証方式の実態調査報告書，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/security/fy26/reports/ninsho/⟩（参照 2016-04-15）.

[13] 電子政府ガイドライン作成検討会：オンライン手続におけるリスク評価及び電子署名・認証ガイドライン，内閣高度情報通信ネットワーク社会推進戦略本部（オンライン），入手先 ⟨https://www.kantei.go.jp/jp/singi/it2/guide/⟩（参照 2016-04-12）.