確率モデルに基づくリスク評価が容易な多要素認証システムの提案とシミュレーション評価

鈴木 宏哉† 山口 利恵† 坂本 静生‡

†東京大学
113-8656 東京都文京区本郷 7-3-1
susuki.hiroya@sict.i.u-tokyo.ac.jp, yamaguchi.rie@i.u-tokyo.ac.jp

‡日本電気株式会社
108-8001 東京都港区芝 5 丁目 7-1
s-sakamoto@bu.jp.nec.com

あらまし 近年，オンラインバンキングに代表される様々なオンラインサービスの登場により，個人認証の重要性が増している．従来は単一の認証要素のみを用いた認証システムが利用されてきたが，安全性の向上などを目的に多要素認証を用いたシステムの普及も進んでいる．一方で，複数の要素を組み合わせる多要素認証システムの安全性と利便性を評価するための，統一的な評価尺度が確立されていないという課題がある．我々は，確率モデルを用いて，動的に変化する多要素認証システムの安全性と利便性を取り扱う手法を提案する．本稿では，提案した確率モデルに対し，シミュレーションにより，その有効性の評価を行った．

Multi-Factor Authentication and Simulation Evaluation based on Probabilistic Model for Risk Assessment

Hiroya Susuki† Rie Shigetomi Yamaguchi† Shizuo Sakamoto‡

†The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113–8656, JAPAN
susuki.hiroya@sict.i.u-tokyo.ac.jp, yamaguchi.rie@i.u-tokyo.ac.jp

‡NEC Corporation
7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001, JAPAN
s-sakamoto@bu.jp.nec.com

Abstract Online services are increasing, and the use of mobile devices, such as smart-phones and tablets, is spreading. User authentication has an important role for the services, which can evaluate both of security and usability and handle authentication methods. In general, because of the balance of security and usability, the alternatives should be diverse. Although service providers can have a variety of combinations of both single-factor and multi-factor authentication methods, it is not possible to make appropriate management without evaluation methods that can evaluate both security and usability. In this paper, we propose a multi-factor authentication framework using a probabilistic evaluation method based on Bayesian approach.

1　はじめに

近年，オンラインサービスの増加に加え，スマートフォンなどのモバイルデバイスの普及に伴い，オンライン個人認証技術の重要性が増している．従来は単一の認証要素のみを用いた認証システムが利用されてきたが，パスワード認証や指紋認証のような単独の認証要素のみを用いた認証方式では，安全性の担保が困難になって来ている [1][2]．この問題を解決するための手法の一つとして，多要素認証が提案されており，実社会での導入が進められている．多要素認証は，性質の異なる複数の認証要素を組み合わせる事で，安全性を高める事を目的としている [3][4]．一方で，多要素認証システムは認証要素の組み合わせにより，単要素の認証システムと比べて，複雑性が増すという課題もある．そのため，安全性や利便性の評価が困難であり，また，異なる認証システム間での比較が容易ではない．今後，多要素認証システムが普及していく上で，サービス利用者やサービス提供者が利用可能な統一的な評価尺度の確立が必要である．

また，現在の多要素認証では主に二要素認証 (パスワード認証＋ハードウェアトークなど) や 3 要素認証が用いられているが，認証要素を動的に変更する事は考慮されていない．そのため，既存の多要素認証システムでは，ある認証要素に脆弱性が見つかった場合に，柔軟に認証要素を切り替えるという事ができない．著者らは先行研究として，多様で可変な認証要素を扱うために，多要素認証システムのための確率モデルの提案を行っている [5]．例えば，オンラインバンキングの残高照会と送金を考えた場合に，必ずしも同じ認証強度が必要とは限らない．一般に，安全性と利便性はトレードオフの関係にあり，利用者の利便性を考えれば残高照会の場合は簡易な認証を行い，高い安全性が求められる送金では，多少利便性が低下してもより安全な認証方式を利用する必要がある．多要素認証であれば，求められる認証強度に応じて認証方法を変更するという事も，認証要素の数を増減させたり，安全性と利便性が異なる認証要素を切り替える事で，実現可能となる．

更に，認証システムの評価尺度の確立に当たり，頻度論的統計では発生頻度が少ない事象に対する的確な評価は困難である [6]．これは攻撃者による攻撃が観測されていない状態では，そのシステムの安全性評価を行う事が難しいという事を意味する．一方，ベイズ統計を用いた推定では，事前知識を与える事で，少ない観測データでもシステムの評価値を近似的に推定する事が可能であり，認証における攻撃者の攻撃なども推定により導出可能が可能である．

我々は，確率モデルとベイズ推定を用いて，動的に変化する多要素認証システムの安全性と利便性を取り扱う手法を提案する．本稿では，提案した確率モデルに対し，シミュレーションにより，その有効性の評価を行った．

本論文の構成は次のようになっている．2 章では，多要素認証システムの安全性と利便性に関する関連研究について紹介する．3 章では，提案する認証の確率モデルについて述べる．4 章では，提案する確率モデルの評価を行う．5 章で考察を行い，6 章で結論を述べる．

2　関連研究

2.1　安全性と利便性

個人認証技術の研究では安全性に着目した手法の提案が多くなされているが，実社会での利用という観点において，ユーザの利便性の考慮も重要な要素である．実社会において個人認証が必要とされる状況には様々なものがあり，それぞれに求められる安全性と利便性は同じではない [7]．入力手段の限られるスマートフォンなどのモバイルデバイスの利便性を考慮し，ユーザの位置情報や端末の操作履歴，アプリケーションの利用状況などの履歴情報の組み合わせを元に，暗黙的に認証を行う手法が提案されている [8][9][10]．また，利便性を考慮した認証手法として，行動認証 [11] や位置情報を用いたリスクベース認証 [12] が提案されている．

このように，安全性と利便性を考慮した研究はなされているが，いずれの研究も双方を評価するための尺度に関する検討や提案はなされていない．

2.2 多要素認証

Hayashi らは，2 段階で処理する多要素認証として，1 段階目に位置情報を用いた暗黙的な認証を行い，その結果に応じて 2 段階目の認証要素の強度を変える手法を提案している [13]. Hayashi らの手法は，自宅のように安全であると仮定できる環境では簡易な認証を用い，公共の場のように安全性が低い環境では安全性が高い認証を用いる事で，安全性と利便性の両立を行っている．しかし，認証要素の組み合わせに関しては，主観的な評価に基づいて使い分けを行っているだけであり，その安全性がどのように変動しているかの評価はなされていない．

著者らは先行研究にて，多様かつ可変な認証要素の組み合わせをシナリオとして定義し，確率モデルの定義を行った [5]．著者らの研究では，認証要素の組み合わせに焦点を当て，その確率モデルの検討を行っている．しかし，この確率モデルは評価済みの認証成功確率を前提とした静的な確率を元にしており，適切な認証の成功確率が不明なシステム導入時や特定の認証要素の安全性や利便性が変化する場合は検討の対象外としていた．実社会でのユースケースを想定すると，システム導入時のように実運用によるデータ収集がなされていない状況であっても，システムに対して何らかの評価が行える手法が必要となる．

2.3 ベイズ統計

ベイズの定理を用いた主観確率に基づく統計的手法は，ベイズ統計と呼ばれている [6]．主観確率とは，まだ起こっていない事象や，発生頻度の低い事象のように，頻度統計による分析では評価が困難な事象に対しても分析が可能になるという利点がある．近年，その有効性は広く知られており，スパムメールのフィルタリングや金融などの分野で利用されている．

これらの統計的手法は，事前確率と事後確率，尤度からなる下記のようなベイズの定理に基づいている．

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)}$$

3 確率モデルの定義

3 章では，提案する多要素認証システムの確率モデルを定義する．

3.1 認証システム

本稿における認証システムのモデル化では，一対一認証を考える．今回のモデルでは，あるユーザ ID に対する認証試行は，そのユーザ ID の所有者である本人，または悪意のある他人 (ここでは攻撃者と定義する) による試行の 2 種類と仮定する．悪意の無い他人により，誤ってあるユーザ ID に対して行われた認証試行については，攻撃者による試行に含めた．

また，システム利用者の個人毎の認証確率については，今回は検討しない．

3.2 認証要素

各認証要素は，ユーザからのパスワード入力など，何らかの入力を受けて出力を返す．出力として，連続値を返すものもあるが，本稿では認証の成否の 2 値を返すモデルを考える．

また，多要素認証における認証要素の組み合わせについては，各認証要素を直列に並べて順次処理する多段階認証では無く，並列に扱う一段階の多要素認証とした．

3.3 安全性と利便性

本節では，ある認証要素の安全性と利便性を評価するモデルについて定義する．

本人に関する確率はユーザビリティ評価 (利便性) に用いる．

- 本人を正しく認証する確率: θ_U
- 本人を誤って棄却する確率: $1 - \theta_U$

他人に関する確率はリスク評価 (安全性) に用いる．

- 他人 (攻撃者) を正しく棄却する確率: θ_A
- 他人 (攻撃者) を誤って認証する確率: $1-\theta_A$

一般に，安全性と利便性の間にはトレードオフの関係がある．

3.4 多要素認証システム

今回のモデルでは，個別の各認証要素 (単要素) は認証の成否を表す 2 値を返すものとし，多要素認証システムは各認証要素の認証結果を AND 論理により求め，最終的な認証成否の結果とする．AND 論理による認証成否の判定とは，一つでも棄却された認証要素がある場合，全体としても棄却するモデルである．

なお，各単要素には相関が無いと仮定する．そもそも，多要素認証においては認証要素間の相関は無い方が望ましい．これは，ある認証要素に脆弱性が見つかったとしても他の認証要素はその影響を受けないという事を表しており，多要素認証システムを用いる事で安全性が向上する根拠の一つである．更に，認証要素の数が多くなるという事は，攻撃者の攻撃に必要となるコストを上げるという効果もある．

3.5 ベイズ更新

ある期間におけるシステムの認証履歴を用いて，ベイズ更新を行う．認証の試行回数が n 回あり，x 回成功したとする．この事象を F とする．

事前知識として，認証に成功する確率を θ，θ の事前分布を $P(\theta)$ とする．ベイズ更新により，事象 F が観測された時に，得られる $P(\theta|F)$ を求める．

本稿では事前分布として，ベータ分布を仮定する．この時，事後分布は事前分布と尤度関数の積に比例するため，事前分布と同じ関数形式になる．この性質は共役性と呼ばれる．二項分布の共役分布はベータ分布である．従って，x の事前確率がベータ分布なら，事後分布もベータ分布になる．ベータ分布の形は二つのハイパーパラメータ α, β とに依存し，事後確率は，$\alpha+x$, $\beta+n-x$ のパラメータを持つベータ分布となる．

ベータ事前分布の平均は $m = \alpha/(\alpha+\beta)$，分散は $v = m(1-m)/(\alpha+\beta+1)$ で表され，$\alpha = 1$, $\beta = 1$ のベータ分布は一様分布となる．

二項分布の公式は以下で表され，

$$P(F|\theta) =_n \mathrm{C}_x \theta^x (1-\theta)^{n-x}$$

ベイズの定理より，事象 F が観測された時に，得られる $P(\theta|F)$ は下記のようになる．

$$P(\theta|F) = \frac{P(\theta)P(F|\theta)}{P(F)}$$

$$\propto \theta^{\alpha-1+x}(1-\theta)^{\beta-1+n-x}$$

すなわち，共役分布を用いる事で，ベイズ更新は更新前のハイパーパラメータ α, β から $\alpha+x$, $\beta+n-x$ への更新のみで表される．

4 評価実験

4 章では，提案モデルの有効性をシミュレーションにより示す．

4.1 事前確率の有効性

ベイズ推定によりシステムの評価を行う利点として，事前確率として経験者による主観確率を与える事で，確率の推定が行えるという点がある．

本実験では，事前知識の有効性を示すために，一様分布からベイズ更新を行った場合と管理者の主観を適用した事前確率を元にベイズ更新を行った場合の収束の様子を比較する．本実験ではゼロ知識から推定を行う場合を，一様分布として仮定した．

それぞれの結果を図 1 から図 8 の図で示す．事前知識として，$\alpha = 9$, $\beta = 3$ のベータ分布を仮定した場合の結果が，それぞれ図 1，図 3，図 5，図 7 である．また，一様分布を仮定した場合の結果が図 2，図 4，図 6，図 8 である．

今回の実験では，ベイズ更新の間隔を 10 回の認証試行毎とした．また，ある認証システムの真の認証成功確率 p が 0.8 と仮定し、この認証成功確率に従う乱数を生成する事でシミュレーションを行っている。従って，時間 t_0 における初期の事前確率分布からベイズ更新を繰り返す事で，真の値である 0.8 に収束している様子が

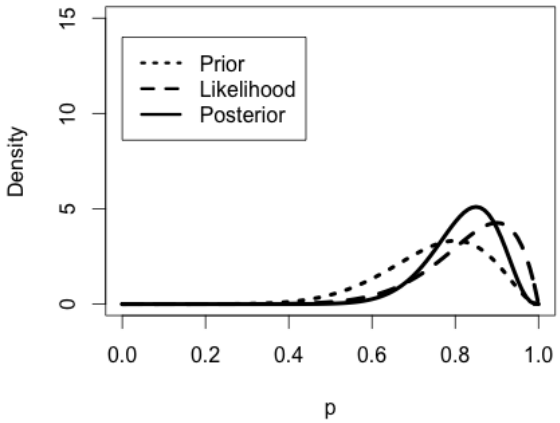

図 1: 時間 t_0、$\alpha = 9$, $\beta = 3$ のベータ分布

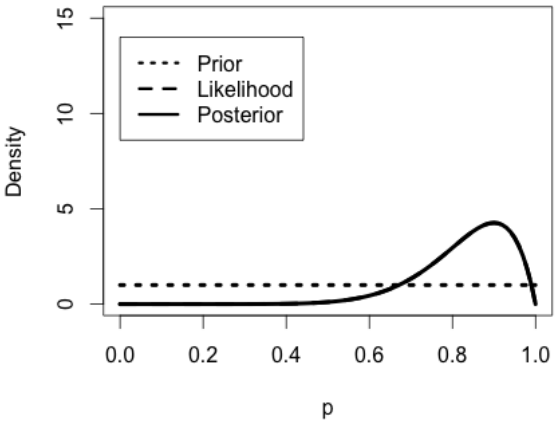

図 2: 時間 t_0、$\alpha = 1$, $\beta = 1$ の一様分布

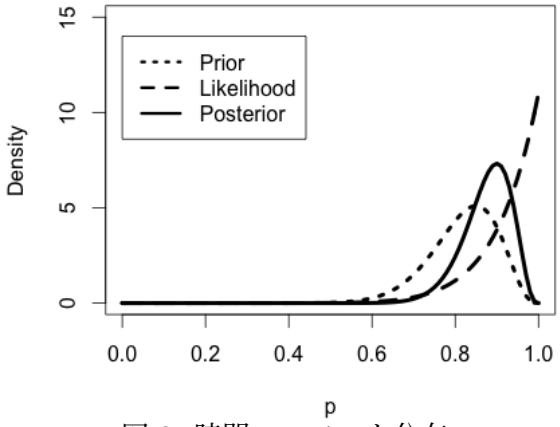

図 3: 時間 t_1、ベータ分布

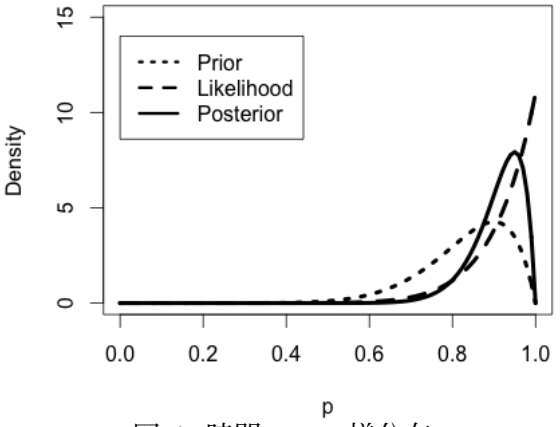

図 4: 時間 t_1、一様分布

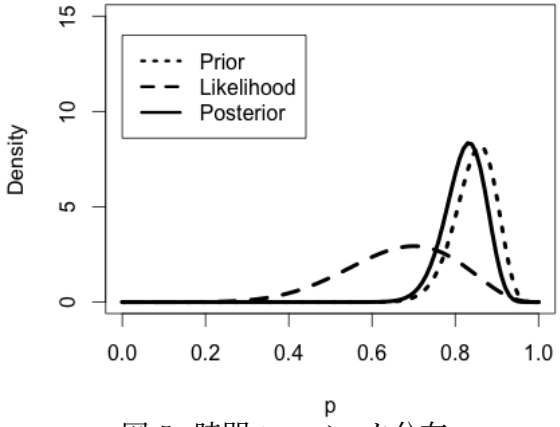

図 5: 時間 t_4、ベータ分布

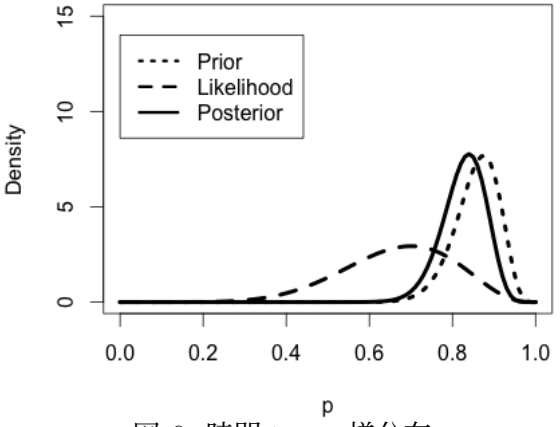

図 6: 時間 t_4、一様分布

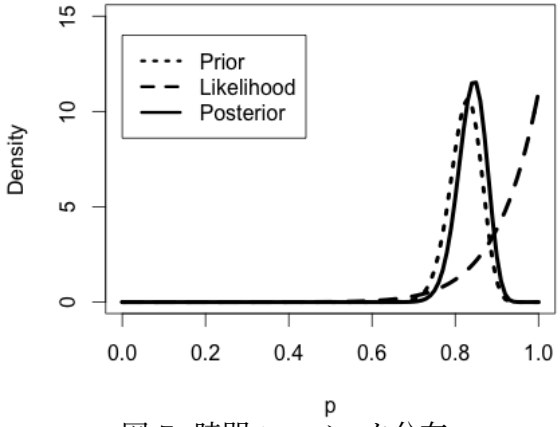

図 7: 時間 t_9，ベータ分布

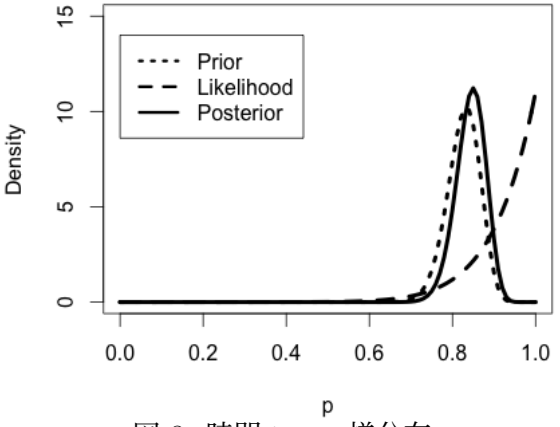

図 8: 時間 t_9，一様分布

実験結果の図から確認できる．なお，図 1，2 は時間 t_0 で認証の試行回数 $n = 0$，図 3，4 は時間 t_1 で認証の試行回数 $n = 10$ である．図 5，6 は時間 t_4 で途中経過を抜いて，認証の試行回数が $n = 40$ の場合を示している．同様に，図 7，8 は時間 t_9 で真の認証成功確率に近付いた後の結果を示している．

5　考察

5.1　事前確率の有効性

事前知識がある場合のベータ分布を与えた場合と，一様分布から開始した場合の比較について，図 3 から図 4 を見比べると，図 3 のベータ分布の方が早く真の認証成功確率に近付いている事が分かる．図 5 と図 6 では、ベータ分布のハイパーパラメータは $\alpha = 44$、$\beta = 8$ と $\alpha = 36$、$\beta = 6$ になっており、分布を示すグラフの形状が近付いている。図 7 と図 8 では、真の認証成功確率である 0.8 により近付き、尖度が大きくなっている事が分かる。このように，ベイズ統計の枠組みを適用する事で、経験者による知識や認証システムを提供するベンダーが行った POC(Proof of Concept) の結果などの事前知識を活用できる事が分かる．

今回の確率モデルでは，ベータ分布の共役性による更新を用いており，ハイパーパラメータの更新式からも明らかなように，真の確率への収束は認証結果の観測数が増える程に進む事が分かる．従って，ベイズ更新の間隔を長くとっても，短くとっても観測数が同じであれば結果は同じになる．しかし，ベイズ更新が行われていない間はシステムの評価が適切になっていないという事であり，更新間隔は短い方が望ましい．ただし，実システムでは更新が与える認証システムへの負荷も考慮して適切な間隔を決定する必要がある．

5.2　攻撃の観測と対策

ある認証要素に対して，攻撃者による新しい攻撃が観測された場合，取り得る対策には，その認証要素の認証成否を調整可能な閾値を変更する方法と，攻撃の成功確率が上がってしまった認証要素そのものを切り替えるという方法が考えられる．

本稿では，攻撃への対応として，認証要素の入れ替えについて評価する．攻撃者が何らかの攻撃手法を用い，新しい攻撃が成功するようになった場合，確率モデルの観点では，他人 (攻撃者) を誤って認証する確率 $(1 - \theta_A)$ が上昇する事を意味する．この時，サービス提供者，または認証システムの管理者が，$1 - \theta_A$ の値が大きくなった事を観測した場合，対応が必要となる．

5.2.1　単要素認証と多要素認証の比較

認証要素切り替えが行われると新しい認証要素は、認証成功確率を求めるための観測値が無い状態となる．従って，単要素の認証システムの場合，切り替えた直後からベイズ更新が進むまでの一定期間，主観確率のみに基づいたシステムの評価が用いられている事になる．この時、新しい認証要素の $1-\theta_A$ が元の認証要素の $1-\theta_A$ より低ければ、システムの運用上は問題無いが、高い場合もあり得る。そのため、単要素認証では、切り替えに備えて、事前に十分な評価を行った認証要素を準備しておくなどの対応が必要となる。

一方、単要素認証システムと比較して，多要素認証システムは特定の一要素が切り替わっても、残りの認証要素は既にベイズ更新が行われて真の認証確率に近付いており、認証システム全体としての評価は適切な値に更新されている．特に、今回仮定している AND 論理による全体の評価を用いる場合、万一新しい要素の評価が適切でなかったとしても、他の認証要素が攻撃者による認証要求を棄却できるため、要素切り替えによる影響が小さいと言える。

6　おわりに

近年，個人認証の重要性の高まりと共に，多要素認証システムの普及が進んでおり，多要素認証システムの安全性と利便性を評価するための，統一的な評価尺度の確立が求められている．

我々は，確率モデルを用いて，動的に変化する多要素認証システムの安全性と利便性を取り扱う手法を提案し，提案した確率モデルに対し，シミュレーションにより，その有効性の評価を行った．

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] 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）, https://www.ipa.go.jp/security/fy26/reports/ninsho/(2015.03.10 閲覧).

[2] Bonneau, J., Herley, C., Van Oorschot, P. C. and Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, *Security and Privacy (SP), 2012 IEEE Symposium on*, IEEE, pp. 553–567 (2012).

[3] Jin, A. T. B., Ling, D. N. C. and Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number, *Pattern recognition*, Vol. 37, No. 11, pp. 2245–2255 (2004).

[4] Anzaku, E. T., Sohn, H. and Ro, Y. M.: Multi-Factor Authentication Using Fingerprints and User-Specific Random Projection, *Web Conference (APWEB), 2010 12th International Asia-Pacific*, IEEE, pp. 415–418 (2010).

[5] 山口利恵, 鈴木宏哉, 坂本静生: スマートフォンを事例とする多要素認証確率の提案, SCIS2015 暗号と情報セキュリティシンポジウム, 電子情報通信学会, pp. 4C2–5 (2015).

[6] 東京大学教養学部統計学教室（編）: 統計学入門, 一般社団法人東京大学出版会 (1991).

[7] Jakobsson, M., Shi, E., Golle, P. and Chow, R.: Implicit authentication for mobile devices, *Proceedings of the 4th USENIX conference on Hot topics in security*, USENIX Association, pp. 9–9 (2009).

[8] Riva, O., Qin, C., Strauss, K. and Lymberopoulos, D.: Progressive Authentication: Deciding When to Authenticate on Mobile Phones, *USENIX Security Symposium*, pp. 301–316 (2012).

[9] Shi, E., Niu, Y., Jakobsson, M. and Chow, R.: Implicit authentication through learning user behavior, *Information security*, Springer, pp. 99–113 (2011).

[10] Khan, H. and Hengartner, U.: Towards application-centric implicit authentication on smartphones, *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, ACM, p. 10 (2014).

[11] Zhang, F., Kondoro, A. and Muftic, S.: Location-based authentication and authorization using smart phones, *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, IEEE, pp. 1285–1292 (2012).

[12] Google: 前回のアカウントアクティビティ, Google（オンライン）, https://support.google.com/mail/answer/45938?hl=ja(2015.03.10 閲覧).

[13] Eiji H., Sauvik D., Shahriyar A., Jason H., and Ian O.: Casa: context-aware scalable authentication, *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, page 3. (2013).