一般口演 | セキュリティとプライバシー保護
一般口演20
情報セキュリティ・プライバシー
2021年11月21日(日) 15:10 〜 16:10 G会場 (2号館3階232+233)

[4-G-3-03] 顔認証を用いた病院情報システムの認証における4年間の運用分析

*山ノ内 祥訓[1]、中村 太志[1]、宇宿 功市郎[1] （1. 熊本大学病院）
*Yoshinori Yamanouchi[1], Taishi Nakamura[1], Koichiro Usuku[1] （1. 熊本大学病院）
キーワード：Facial Recognition, Biometrics, Multi-factor authentication

【背景】病院情報システムにおける利用者認証は、多くの場合 IDとパスワードによる認証である。近年、IDカードや指紋等を使用する2要素認証も増えてきているがまだ一般的ではない。当院では2017年に稼働した病院情報システムにおいて本邦では事例のない顔認証システムを採用した。本研究では稼働後4年半が経過した本システムの運用状況について分析したので報告する。【方法】2017年1月～2020年12月で認証システムのログデータを抽出した。抽出件数は36,635,815件である。ここから、顔認証の失敗や別の認証方式への変更等を分析できるように変換し、さらに利用者や端末の属性を付与したデータセットを作成しこれを分析した。【結果】診療用端末(PC及びスマートデバイス)における総ログイン件数12,804,140件のうち、顔認証による認証は10,229,760件であり80%が顔認証でログインされていた。利用率は稼働当初72%だったが、2017年6月に80%に上昇、その後80～84%を推移していたが、2020年4月以降は75%に減少した。毎年4月は他の月と比較して1～2%使用率が減少していた。成功率は導入から6か月間は89~90%で、その後91~92%まで上昇し安定していたが、2020年4月以降は89%に減少した。深夜帯は日中と比較して減少したが2%の低下に留まった。【考察】顔認証は、既存方式と比較して簡便で速度が速く、安定して運用できたことから移行が進んだ。精度も想定通りだった。しかし、 COVID-19対策で認証時にマスクを下げる行為にリスクがあることから、顔認証を使用しない利用者の増加、一部端末で顔認証不要の設定変更、等の影響により、利用率成功率共に僅少した。近年精度向上だけでなくマスク着用時の認証も実用化されており、キーボード等共用物に触れない認証として今後機能強化を図っていく予定である。

顔認証を用いた病院情報システムの認証における 4 年間の運用分析

山ノ内　祥訓[*1]、中村　太志[*2]、宇宿　功市郎[*1,2]
*1 熊本大学病院総合臨床研究部研究データ管理センター、*2 熊本大学病院医療情報経営企画部

A Four-Year Operational Analysis in Face Recognition for Hospital Information System Authentication

Yoshinori Yamanouchi[*1], Taishi Nakamura[*2], Koichiro Usuku[*1,2]
*1 Department of Clinical Investigation, Kumamoto University Hospital,
*2 Department of Medical Informatics and Administration Planning, Kumamoto University Hospital

In hospitals, user authentication is often based on ID and password. In recent years, a two-factor authentication using ID cards or fingerprints has increased, but a standard method is not established yet. Our hospital was the first in Japan to adopt a face recognition in hospital information system, which went into operation in 2017. In this study, we analyzed the operational conditions of the system for last 4.5 years. Log data of the authentication system were extracted from January 2017 to December 2020. Based on the data, we created a dataset that was converted to allow analyses for user's profession, terminal types and the locations, failure logins with face recognition, change histories to another authentication method, and so on. The total record of logins to medical terminals (PCs and smart devices) was 19,019,065. The number of logins with face recognition was 14,533,395, which was accounted for as high as 76% authentication. The use of face recognition in our hospital showed being generally stable because the success rate was 96%. The accuracy was more than 95%, which appeared to be practical enough for normal authentication. However, depending on the user's daily face condition as well as the environment in which the face image was taken, the authentication failed to be performed. We plan to enhance the function without requiring direct contact with common objects as a smooth authentication method since not only has the accuracy been improved but authentication with wearing a mask has been turned to practical use.

Keywords: Facial Recognition, Biometrics, Multi-factor authentication.

1. 背景

情報システムを利用する場合 ID とパスワードを入力して認証する方式が古くから行われている。これは ID がその情報システムを誰が使うかという利用者を識別し、その ID を使用するために必要な秘匿情報をパスワードとして入力することで、その ID を本当に本人が使用しようとしているのかを検証する仕組みである。しかし、この ID とパスワードによる認証は脆弱であることが知られている。パスワードは使用する本人が覚えておく必要がある知識認証であるため、ランダムな文字列や長い文字列など覚えにくいパスワードは嫌厭される傾向にある。そのため、覚えやすいパスワードは辞書攻撃により、短いパスワードは総当たり攻撃により簡単に突破される。また、複雑で長いパスワードであっても同じパスワードを使いまわしていると、一つのシステムでパスワードが流出したときにすべてのシステムに影響を与えてしまう。これらの問題により最近は多くの業種でパスワードレス運用に移行しつつある。

パスワードや暗証番号に変わる認証方式として本人しか持ちえない身分証やスマートフォンなどを使用する所有物認証、指紋などを使用する生体認証がある。しかし、これらの認証方式であっても、一つの要素で認証を行うリスクは回避できないため、複数の認証方式を組み合わせた多要素認証(二要素の場合は二要素認証)が一般的に用いられる。

病院情報システムにおいても「医療情報システムの安全管理に関するガイドライン　第 5.1 版」において「令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、導入又または更新する場合、原則として二要素認証を採用することが求められる。」という記述が追加されたことからも今後必須となる機能であることが示された [1]。とはいえ、まだ多くの病院情報システムは ID とパスワードによる認証であり移行が困難であることがうかがえる。

当院では、2017 年に現在の病院情報システムが稼働したが、この時の利用者認証で病院情報システムでは初となる顔認証システムを採用した [2]。採用した顔認証システムはグローリー株式会社が開発したものである。本研究では稼働後 4 年半が経過した本システムの運用状況について分析したので報告する。

2. 方法

2.1 顔認証システムの概要

当院が採用した顔認証システムは、職員証である非接触型 IC カード、ID、パスワード、顔画像の 4 つの要素のうち 2 つを使用する二要素認証として構成した。認証のパターンは下記の 4 通りである。

- カード+顔画像
- カード+パスワード
- ID+顔画像
- ID+パスワード

このうち ID+パスワードは、IC カードリーダーもカメラも接続できない一部端末のみ許可された方式である。また、顔認証システムが障害により停止したときの回避手段でもある。そのため、一般には使用できないよう制限されている。

対象となる端末は、2021 年 8 月現在で PC が 1688 台、看

護師用 iPod touch が 622 台、問診票用 iPad が 50 台である。このうち、PC は IC カード+顔画像、iPod touch、iPad は ID+顔画像の認証を基本とした。ノート PC や iPod touch、iPad はもともとカメラが組み込まれているが、デスクトップ PC はカメラがないため USB 接続のカメラデバイスを接続して使用した。

利用者の顔画像の登録は、入職時に身分証を作成するときに撮影する画像を任意で使用する運用とした。実際に使用を始めると認証に成功した画像を次の認証時の照合データとして最大 10 件まで自動追加していくため、常に最新の顔画像を照合データとして使用できる。

顔認証処理の流れは次の通りである。まず、カードもしくは ID 入力により照合対象の利用者を特定する。次に、カメラを起動し顔検出処理を開始する。顔検出処理にて顔が検出されたらあらかじめ複数登録されている照合画像と比較し顔が一致するか判定する。判定は顔の特徴点 100 点を検出しその位置の違いによりスコアを算出し設定された閾値を超えたスコアの場合一致とする。3D 判定や動画(まばたき等)による照合処理は用いていない。この顔検出から顔照合までの処理を 3 回以上失敗するか、顔が未検出で 10 秒を超えたら自動的にパスワード入力画面に遷移する。このとき認証ログには顔認証失敗と記録される。

2.2 認証ログデータの抽出と分析

顔認証システムが稼働した 2017 年 1 月から 2021 年 6 月までの認証ログデータを抽出した。このデータは、認証に関するイベントの情報が記録されている。これを分析可能な形式に変換した(図 1)。まず、認証成功のログを基準として、同一利用者の前回の認証成功のログとの間のイベントを抽出した。次にそのイベントに顔認証失敗ログが何回あるか、最初の失敗から端末を変更したのか、最初の失敗から成功までの経過時間、成功した認証方式を取得した。また、2019 年からは出退勤のイベントも認証ログに含まれているため、出勤から何時間経過したか、出勤から何回目の認証成功かも取得した。さらに、その利用者の職種や端末の種類、設置場所の情報を結合してデータセットを作成した。これを Microsoft Power BI を用いて可視化し分析を行った。

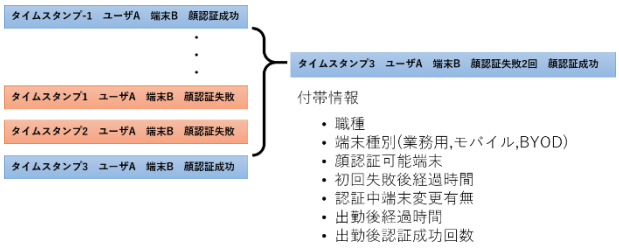


図 1 ログデータから分析用データの変換方法

3. 結果

認証ログデータから分析用に作成したデータセットは 19,019,065 件だった。そこから、認証パターン毎の使用割合を月毎に集計した(図 2)。まず、顔画像を使用しない認証パターンであるカード+パスワードは、稼働当初である 2017 年 1～2 月に 30%弱存在したがその後減少し、半年経過した 2017 年 6 月に 20%程度となったあとしばらくは大きく増減が見られなかった。しかし、2020 年 3 月以降は急激に増加し現時点では稼働当初とほぼ同じく 30%程度となった。次に、ID+顔画像はほぼ看護師の iPod touch で使用されているパターンである。こちらも稼働からは増加していたが、毎年 4 月に急激な減少が発生していた。同月に PC で使用している認証パターンである IC+顔画像が逆に増加していた。2019 年以降は 4 月に減少した認証割合が増加せずそのまま横ばいで推移していた。

顔認証を使用した場合の失敗率について年月に集計した(図 3)。端末タイプ別に失敗率を確認すると、業務用(電子カルテ PC)では稼働当初から 2019 年 3 月までは 5%程度の失敗率だったが、2019 年 4 月以降は 4%程度に減少した。こちらも、2020 年 4 月のみ一時的に失敗率が増加した。モバイル(iPod touch, iPad)ではほぼ全期間にわたって 0.1%未満の失敗率だった。時間帯別の失敗率は業務用端末では 22 時～4 時の深夜帯の失敗率が多かったが、モバイル端末では深夜帯の失敗率はそこまで多くなく、9 時、16 時、22 時、3 時といった特定の時間帯の失敗が多かった(図 4)。出勤からの経過時間別の失敗率は業務用端末及びモバイル端末ともに出勤直後と出勤後の経過時間が長くなるほど失敗率が高い傾向にあった(図 5)。モバイル端末ではそれ以外にも 6～7 時間後、10～11 時間後と特定の時間帯の失敗率も多かった。なお、このデータだけは出退勤データが入手可能となった 2019 年 4 月からのため約 2 年間のデータのみ集計した。職種別の失敗率はその他の職種(治験用、研究用、外部閲覧用、等)や医療事務、介護専門職、栄養士の失敗率が多かった(表 1)。利用者別の失敗率は平均値 4.6%、95%タイル値 15%とほとんどの利用者で失敗が少なかった(表 2)。失敗率が 25%以上の利用者は 169 名だった。端末別の失敗率も平均値 4.06%、95%タイル値 10%値でほとんどの端末で失敗が少なかった(表 3)。失敗率が 25%以上の端末は 24 台だった。顔認証失敗後の行動パターンとして、最終的にどの認証方式で認証を行ったかと端末を変更したかを分析した(図 6)。その結果、最も多いのが同じ端末でカード+パスワード認証を行うパターンで 63%だった、そのまま顔認証を継続するに切り替えたのは 33%だった。途中で別の端末に切り替えたというパターンも 10%程度いた。このとき、失敗から認証成功までの経過時間は業務用端末では失敗後 10 秒未満で多くが認証に成功しており、20 秒を超える場合は少ないが、モバイル端末では 10～19 秒の間が最も多かった(図 7)。

表 1 職種別の顔認証失敗率

職種	失敗率 [%]
医師・歯科医師	4
看護師	3
助産師	2
薬剤師	3
検査技師	2
放射線技師	3
療法士	3
栄養士	5
臨床工学技士	3
歯科衛生士	3
歯科技工士	1
介護専門職	5
医療事務	6
クラーク	3
事務	4
学生	4
その他	8

表 2 利用者の顔認証失敗率

利用者数	6715
平均値	4.6
標準偏差	10.13
最小値	0
最大値	100
四分位数	0, 2, 5
95%タイル値	15

表 3 端末の顔認証失敗率

端末数	2,213
平均値	4.06
標準偏差	5.66
最小値	0
最大値	100
四分位数	2, 3, 5
95%タイル	10

4. 考察

当院の認証システムにおける顔認証の利用状況は、4 年半の間およそ 70～80%の利用実績があり主要な認証方式として運用できたと評価した。顔画像の登録は任意であるため、稼働当初は様子見と思われる未使用者がいたがその後顔認証への切り替えが進んだことで利用率が増加した。しかし、2020 年の 4 月から利用率が低下した。これは、COVID-19 の感染対策が本格化した時期と一致する。この時期に、認証時にマスクを下げる行為に感染リスクがあるため顔認証を使用しないよう端末の設定を変更してほしい、という要望があった。そのため、外来や重症系病棟の一部の端末において顔認証を使用しない設定に変更したほか、レッドゾーンなど IC カードの取り出しも困難な場所では ID+パスワード認証を可能とする設定も行った。これにより、顔認証の利用率の減少が見られた。次に、毎年 4 月は ID+顔画像の利用率が減少しカード+顔画像の利用率が上昇した。認証パターンから考えるとモバイル端末の使用頻度が減り業務用端末の使用頻度が上がっていた。この時期は入職や部署異動が多く発生する時期であり、その影響と考えられるが、ログ分析では要因が不明なため今後現場へのヒアリングが必要である。また、モバイル端末では 4 月から来年の 3 月にかけて利用率が上昇しているが 2019 年は横ばいとなり他年と異なる傾向を見せた。その要因として、この時期に iPod 内の証明書有効期限が切れてエラーが頻発し、解消するまで半年程度 iPod の使用を制限した障害があり、この影響で認証回数が減ったものと考えられる。

顔認証の失敗率を分析すると、業務用端末とモバイル端末で失敗するタイミングが異なることが分かった。業務用端末は夜間の失敗率が高く、モバイル端末は日中と夜間で顕著な違いは見られないが、いくつかの時間に集中して失敗率が高かった。もともと顔認証が失敗しやすい要因の一つとして、照明の明るさや光源の位置により顔画像が暗くなった場合の精度が低下することが知られている [3]。そのため、端末やカメラ位置に注意して設置したが、良好な環境に設置できない端末は失敗しやすい傾向があったと考えられる。端末別の失敗割合を確認しても一部の端末は失敗することが多いため、今後できる限り環境の改善を行う必要があると考える。

次に 2019 年以降の出勤時刻データが入手できたことから、出勤後の経過時間で分析した。その結果出勤直後と長時間勤務時に失敗率が高かった。ここから、勤務開始直後に失敗率が高いことが示唆された。本システムは直前に認証が成功した顔画像を保存し次回認証に使用するという仕組みとなっている。そのため、前回勤務の最後に認証したときの顔画像を次の勤務の最初の認証に用いるため、日々の表情の変化が認証精度に影響したのではないかと考えている。また、モバイル端末では出勤時刻から、6～7 時間後、10～11 時間後の失敗率も高かった。同じ勤務時間帯でも勤務時間が長くなるにつれて失敗率が高くなる傾向にあるため、疲労による表情の変化も影響していることが示唆された。先行研究においても表情や姿勢、髪型(特に前髪)、眼鏡の有無、化粧、加齢といった変化で認証率が落ちることが知られている [3]。顔画像により疲労度を検出できる技術も存在することから [4]、これらが認証精度に影響を与えていると考えられる。しかし、本研究は匿名化処理で利用者の実 ID や顔画像を収集していないため、この仮説を検証することができなかった。

顔認証を失敗した後に利用者がとる行動は、早々に見切りをつけてパスワード認証に変更することが多かった。もともと 10 秒以上認証できなかったら別の認証方式に変更する仕組みとなっているが、業務用端末では失敗からの経過時間は 10 秒未満が最も多いため、認証方式の自動切り替えより早く自分で切り替えていると考えられる。モバイル端末では 10 秒から 19 秒が最も多いため切り替えまでに利用者が待っている可能性が高い。認証成功までの経過時間は 30 秒未満がほとんどであるが、一部 30 秒以上経過している場合もあった。実運用として認証にこれだけ時間がかかることは考えにくいため、ログオフ後のカード置き忘れや、パスワード忘れなどが原因と考えられる。

5 結論

当院における顔認証の利用状況について調査を行った。認証方式別では 70～80%が顔認証を日常的に使用しており、認証精度も 96%と高いことから十分に実用的であると考える。しかし、COVID-19 の感染対策で常時マスクを着用することが多くなった影響で、当初想定したスムーズな認証の実現は完全に達成されたわけではない。マスク着用以外でも利用者の表情の変化や、撮影環境の違いなど認証精度に影響を与える要素が考えられた。近年、マスク着用時でも認証可能な技術や、ステレオカメラによる 3D 判定、動画を用いた検出等、顔認証システムの精度向上が図られている。次期システムの更改の時期が近くなっていることもあり、スムーズな認証が実現できるよう検討を進めていきたい。

参考文献

1) 厚生労働省. 医療情報システムの安全管理に関するガイドライン 第 5.1 版. 2021. [https://www.mhlw.go.jp/stf/shingi/0000516275.html (cited 2021-Aug-25)].
2) 廣瀬準,山ノ内祥訓,宇宿功市郎. 病院情報システムにおける 2 要素認証の実装と利用状況 - 顔認証の有用性 -. 2017, 第 37 回日本医療情報学連合大会論文集; 455-457.
3) 内田 薫. 携帯電話における生体認証とカメラ画像処理(チュートリアル講演,通信品質,メディア・インタフェース及び一般). 映像情報メディア学会技術報告. 32(58), 2008;33-40
4) Uchida MC, Carvalho R, Tessutti VD, et al. Identification of muscle fatigue by tracking facial expressions. PLoS One. 13(12), 2018;e0208834.

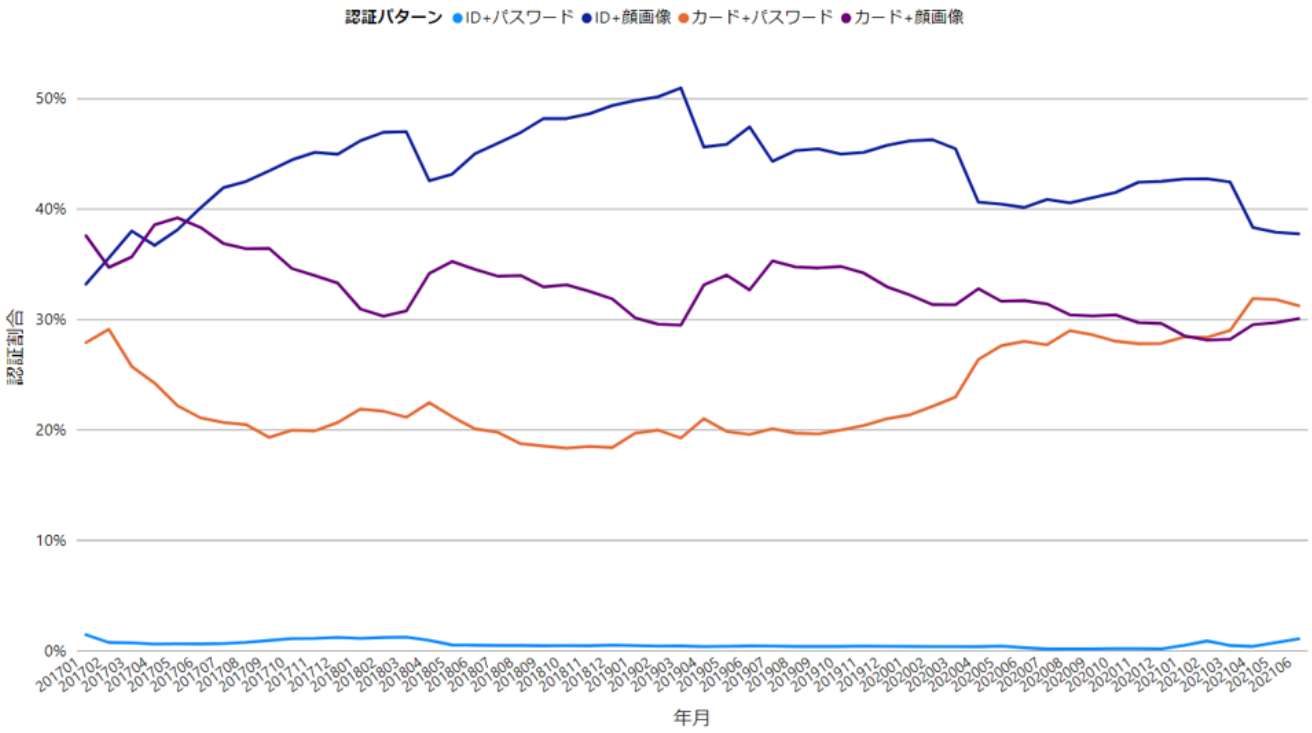


図 2 認証パターン別の年月推移

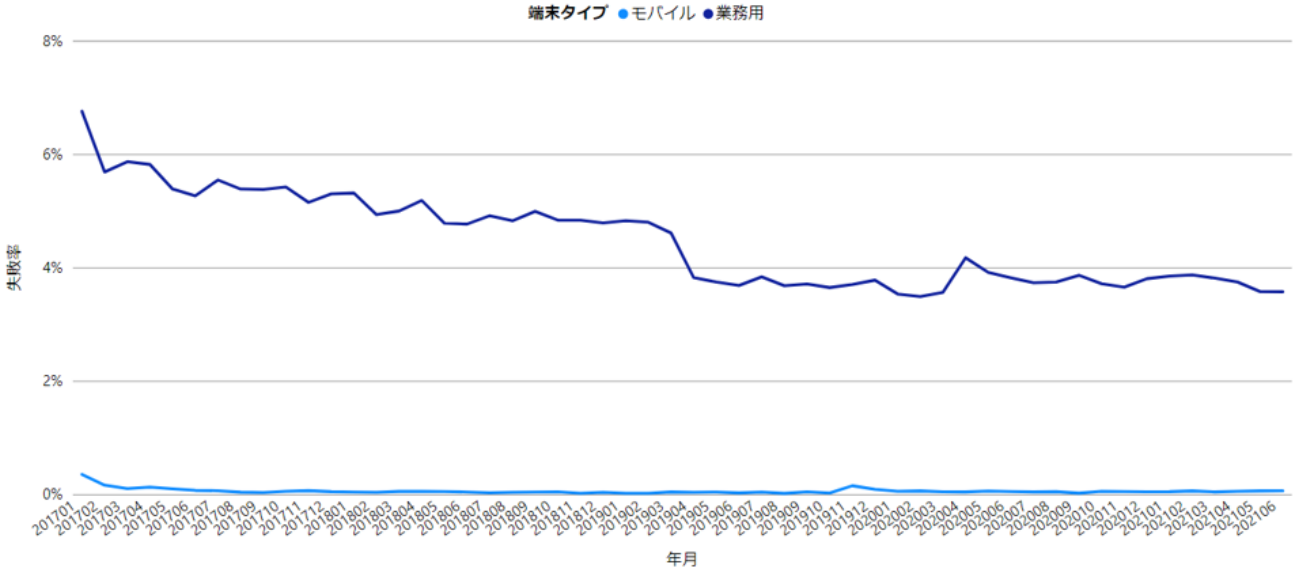
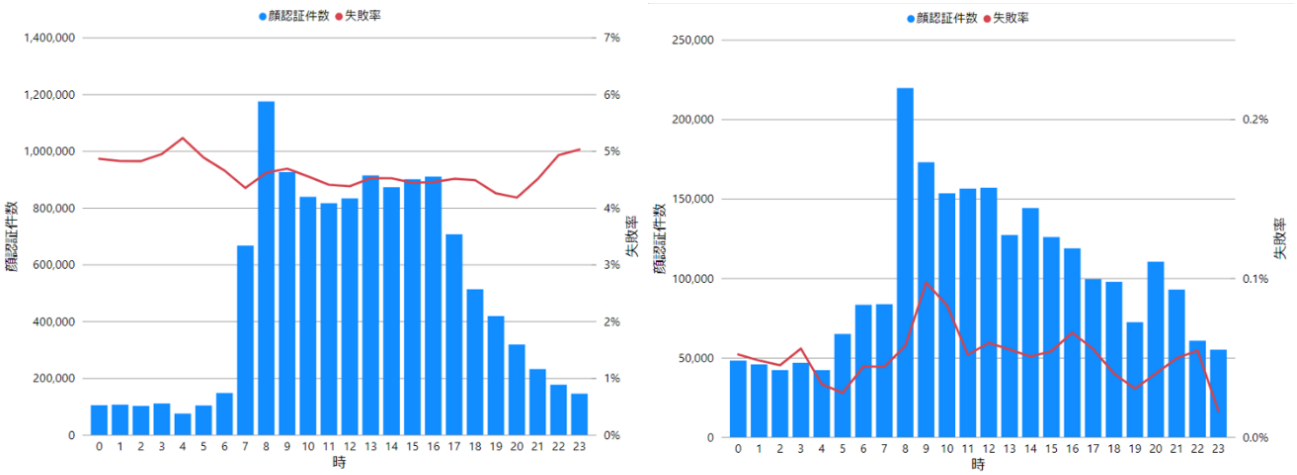
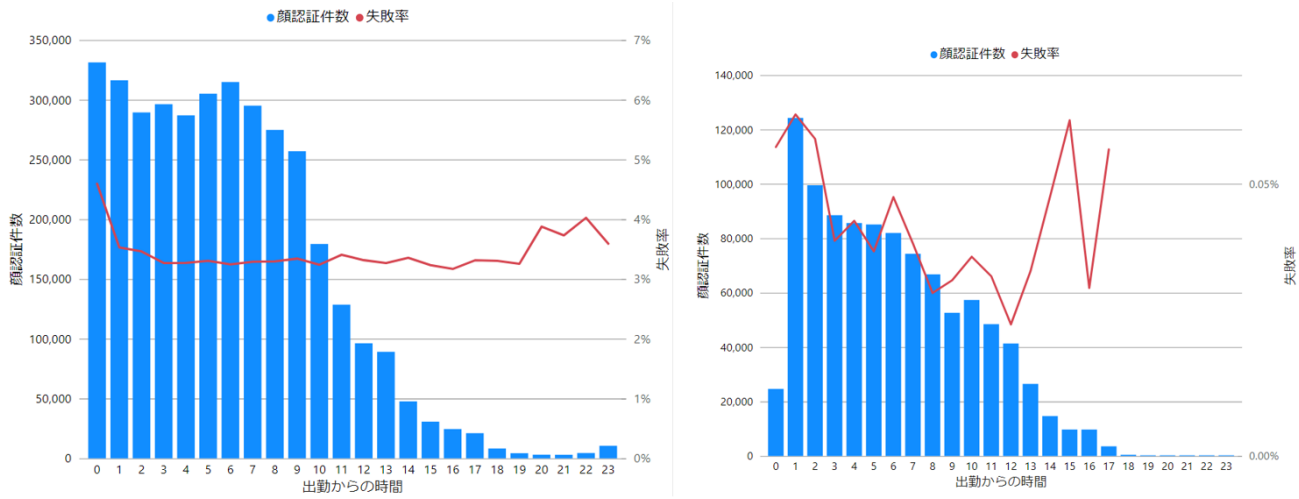


図 3 端末タイプ別の顔認証失敗率の年月推移



(A) 業務用　　(B) モバイル

図 4 顔認証件数と失敗率について認証時間分布



(A) 業務用　　(B) モバイル

図 5 顔認証件数と失敗率について出勤時刻からの経過時間分布

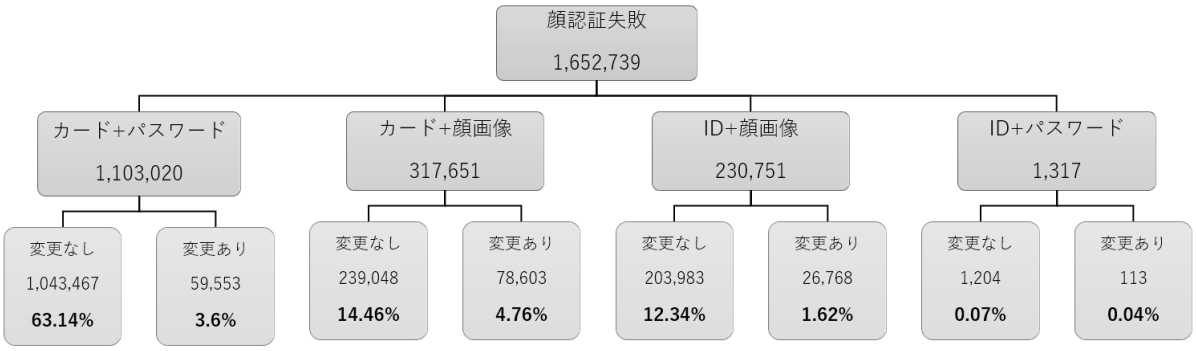
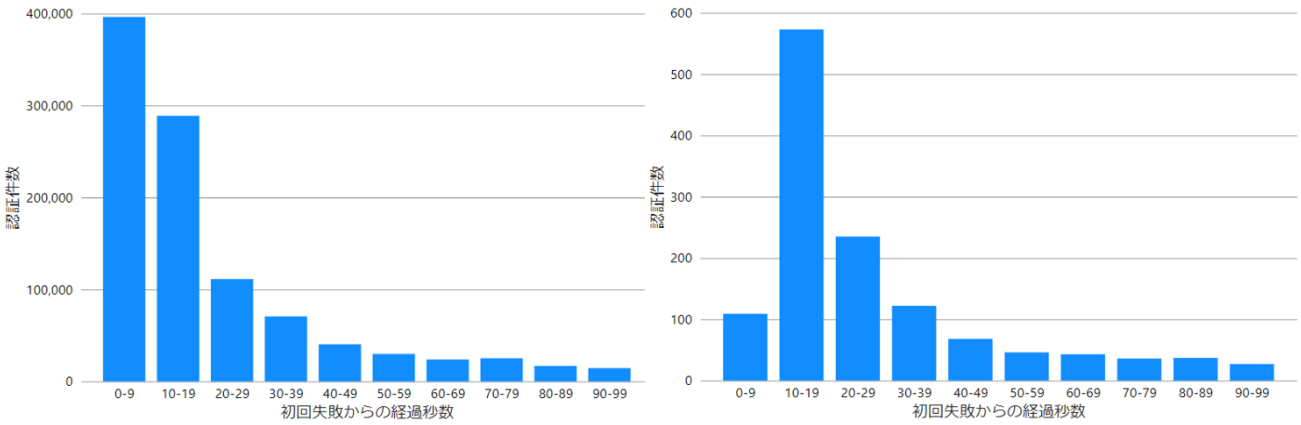


図 6 顔認証失敗後に利用者がとった行動パターン



(A) 業務用　　(B) モバイル

図 7 顔認証の失敗から認証成功までの経過時間分布