Vol.2019-IOT-44 No.38
2019/3/8

スマートウォッチの竜頭型コントローラを用いた暗証番号入力方法

稲村 勝樹[1,a),b)]　市村 泰佑[1]

概要：スマートウォッチは小型のタッチパネルと CPU を搭載した，多機能な腕時計型のウェアラブルデバイスで，近年このスマートウォッチの利用が大きく広がっている．スマートウォッチは様々な入力装置を備えており，Bluetooth などにより様々なデバイスと通信を行えることから，スマートウォッチを使った認証機能が実装・検討されている．本研究では，覗き見攻撃耐性を向上させつつユーザにとって操作が優しい認証方法の実現を目的とし，スマートウォッチに搭載されている竜頭型コントローラを用いた暗証番号入力方法を提案する．また評価アプリケーションを作成し，一般的なタッチパネルでの暗証番号入力による認証との比較検証を行う．

A PIN Input Method with a Crown on a Smartwatch

Abstract: A smartwatch is one of the wearable devices, which are equipped with a small touchscreen and a CPU, and have become widespread in recent years. Because the smartwatch has some types of input unit and can communicate with other devices through Bluetooth and so on, some user authentication methods with smartwatch are proposed and implemented. In this paper, we propose a new PIN input method with a crown on a smartwatch in order to improve protection against shoulder surfing and convenience. Furthermore, we develop an application and evaluate the security and usability compared with a general input method with a touchscreen.

1. はじめに

近年，スマートウォッチと呼ばれるウェアラブルデバイスの普及が急速に進んでいる．スマートウォッチとはスマートフォンやタブレット端末等のスマートデバイスと連携する腕時計型のデバイスのことであり，主に時間，メール，カレンダー等の確認が行なえる他，連携しているスマートフォンが受け取る通知をバイブレーションで利用者に伝える機能を有している．スマートデバイスの急速な普及に牽引される形でスマートウォッチの普及も広がっており，2022 年には国内で約 120 万台，全世界で約 1 億 9 千万台ものスマートウォッチが出荷されるとの予測も出ている [1]．最新のデバイスでは情報の確認だけでなく，身につけていることでコンピュータのログイン管理を行ったり，あらかじめ登録を行ったクレジットカードにより店頭での支払いを行ったりすることができ，機能性の向上に伴いより重要度の高い情報や権限を扱うことが可能になっている．

上記にあるように，デバイスが扱える情報の重要度が増加すると，そのデバイスが起因となる情報漏洩や金銭的損害等のリスクが高くなる．そのため，現在普及しているスマートウォッチの多くは第三者による不正利用を防ぐため，装着時にユーザ認証を行う機能が付加されている．この認証方式として一般的に利用されている代表的なものとして，タッチパネル上のテンキーによる暗証番号入力，タッチパネル上の点をなぞるパターンロック等がある．これらの認証方式は端末にタッチパネルが装備されていれば利用可能であるため，多くのスマートウォッチに実装されている．また，認証を行う際にユーザが記憶する情報も比較的少なく，テンキーの配置等スマートフォンのユーザ認証と共通点が多いといった特徴がある．一方で，タッチパネル上に入力情報が表示されるため，認証操作を第三者に覗き見され認証情報が漏洩してしまう危険性が高いと考えられる．

本研究では，スマートウォッチをはじめとするウェアラブルデバイスのユーザ認証時における覗き見攻撃への耐性

[1] 東京電機大学理工学部
School of Science and Engineering, Tokyo Denki University, Ishizaka, Hatoyama, Hiki-gun, Saitama 350–0394, Japan
[a)] minamura@rd.dendai.ac.jp
[b)] minamura@sec.ee.kagu.tus.ac.jp

を向上させることを目的とし，認証情報入力にタッチパネルを用いない新たな方式として，時計型デバイスの多くで入力方式として採用されている竜頭型のコントローラを用いた認証方式を提案する．これにより，視覚ではなく触覚を用いた認証により，覗き見の効果を減少させる効果が期待できる．この提案方式を実装し，既存の認証方式で広く用いられているタッチパネル上のテンキーによる PIN（Personal Identification Number）入力方式との比較検証を行う．

以下，2 章では携帯端末で採用されている認証方式の関連技術について紹介し，3 章では提案方式について述べる．4 章では提案方式の実装実験とその結果を示し，5 章で考察を行う．最後に 6 章でまとめとする．

2. 携帯端末で採用されいている認証方式

2.1 タッチパネルを用いたユーザ認証

スマートフォンやタブレット端末等におけるタッチパネルを用いたユーザ認証方式として，PIN と呼ばれる暗証番号や，特に Android が搭載されている端末ではテンキー状に表示された数字や記号を指でなぞるパターンロックが採用されている．このパターンロックについては，オンライン時あるいはオフライン時に他人の監視下ではない状況における安全性の考察が行われている [2,3]．しかし，屋外など不特定多数の他人がいる環境でログイン操作が行われることもあり，パターンロックによる認証方式では携帯端末を持つユーザの後方からユーザの操作を盗み見する覗き見攻撃（ショルダーサーフィン，またはショルダーハッキング）が懸念される．

この覗き見攻撃への対策について，スマートフォンが普及する以前からいくつかの方式が検討されている [4–11]．さらに，東川・満保らによってスマートフォンのパターンロックに特化した覗き見攻撃耐性のある認証方式が提案されている [12]．この方式には，パスパターンに対応する数字を認証時に毎回変更し，入力画面でその数字に合わせて画面をなぞっていくといった特徴がある．これにより認証時に入力パスパターンが毎回異なるため，認証情報をそのまま入力していた従来の方式に対して覗き見攻撃耐性が高くなる．我々はこの方式を基に，

- パスパターンに対応して記憶する数字の規則を変更
- 入力画面での入力規則の追加

を行うことで利便性の低下を抑えた改良方式を提案している [13]．

また，スマートウォッチに特化した覗き見攻撃耐性のある PIN 入力型の認証方式も提案されている [14]．これは，画面が小さいことに起因する入力の難しさを考慮し，認証情報入力における画面表示をできるだけ簡素化することで利便性の低下を抑えながら，入力する位置を毎回変化させることで覗き見攻撃耐性を持たせている．

2.2 タッチパネル以外によるユーザ認証

近年になって採用されている認証方式としては，指紋による生体認証が上げられる [15, 16]．これは指紋認証用のセンサーが小型化され，携帯端末に搭載できる指紋認証機能が実現できるようになったためである．一方で，指紋認証に対する攻撃手法は以前から研究されており，人工物を用いた指紋の偽造 [17]，写真で撮影した指の画像から指紋を特定する攻撃 [18] などが知られている．特に，写真撮影による攻撃手法では，3 メートル離れたところからの撮影でも指紋を特定できており，指紋を撮影する機会は携帯端末利用時以外にも多く存在することから，覗き見攻撃耐性が高いとは言えないと考えられる．

指紋認証以外の生体認証としては，顔認証や虹彩認証を搭載した携帯端末の例が上げられる [19, 20]．しかし，顔認証に対する攻撃手法 [21] や虹彩認証に対する攻撃手法 [22–24] が知られている．

3. 提案方式

3.1 提案方式の概要

2.1 節で紹介した認証方式は，いずれもユーザの記憶を認証情報とし，その情報を入力してユーザ認証を行う方式であるが，秘匿されるべき認証情報の入力時において，覗き見が可能であれば画面上に表示された情報とその入力時のユーザの動作からこの認証情報が漏洩する可能性がある．こういった覗き見攻撃への対策として，以下のコンセプトによる認証方式の検討を行った．

入力に関する情報を画面に表示しない：
入力情報を画面上に表示することで覗き見攻撃に対し脆弱となると考え，入力情報を画面に表示しないこととする．

入力にタッチパネルを使用しない：
タッチパネルを使用しないことで，特徴的な入力時の手の動きを覗き見攻撃により見られることを防ぐことが可能になると同時に，入力時に画面を見る必要がなくなることから認証時の入力操作の姿勢に自由度が増し，操作を見られにくい姿勢での認証操作が可能となると考えられる．

このような検討の結果，以下の特徴を持つ認証方式を提案する．

竜頭型コントローラによる認証情報入力：
腕時計の時刻設定等で使用する竜頭は時計型デバイスとの親和性が高く，多くのスマートウォッチで採用されている．提案方式では，回転距離（あるいは回転数）を取得できる竜頭型コントローラを用い，PIN の値を回転距離により表すことで，認証情報の入力を行う．

振動機能による入力情報フィードバック：
入力操作において，どのような情報が入力されているかをユーザが知ることができなければ，誤入力が増え

利便性が著しく低下することが考えられる．提案方式では，スマートウォッチにユーザへの通知用として採用されている振動機能を用いることで，画面表示を用いずにユーザのみが入力情報を知ることができるようにする．

竜頭型コントローラによる入力回転距離のランダム変化： 認証操作において，万が一竜頭型コントローラの操作を見られても入力情報が漏洩しないためには，同じ PIN の値であっても毎回入力パターンを変更することが効果的であると考えられる．提案方式では，竜頭型コントローラを操作する手の動作が見かけ上毎回変化するように，入力の値に連動して振動が発生する回転距離をランダムに変化させる機能を付加する．

3.2 提案方式の認証手順

提案方式において，認証情報となる PIN の値の登録は既存の方式と変わらないため，本稿ではその登録手順の説明は省略する．

提案方式における認証手順は，以下の通りとなる．

(1) 竜頭型コントローラを上方向に回転させ．1 桁目の入力を開始する．
(2) 入力したい数値の分だけ端末が振動するまで回転操作を続ける．
(3) 竜頭型コントローラを反対方向に切り返すことで現在の桁の PIN 入力を完了し，切り替えた方向に回転操作を行い，次の桁の PIN 入力を開始する．
(4) 手順 2,3 を PIN の最終桁まで繰り返し行う．
(5) 最終桁の入力後，竜頭型コントローラを反対方向に切り返すと端末が 3 回振動し，すべての PIN 入力が完了となる．

例えば「3456」の 4 桁を入力する場合は，以下の通りとなる．

(1) 竜頭型コントローラを上方向に回転させ，1 桁目の入力を開始する．
(2) 端末が 3 回振動するまで回した後，下方向に切り返し，切り返した方向で回転させる．
(3) 端末が 4 回振動するまで回した後，上方向に切り返し，切り返した方向で回転させる．
(4) 端末が 5 回振動するまで回した後，下方向に切り返し，切り返した方向で回転させる．
(5) 端末が 6 回振動するまで回した後，上方向に切り返す．
(6) 端末が 3 回振動し，すべての PIN 入力が完了となる．

また，一般的な PIN による認証方式では入力する数字は 0 から 9 となるが，提案方式においては回転操作で入力を行うため，扱える数字は 1 から 10 とする．したがって，設定上 PIN の登録時に「0」を選択する場合は，実際の認証時には「10」として扱うといった事前説明がユーザに対して必要となる．

4. 実装実験

4.1 実験概要

3 章で提案した認証方式の評価のため，スマートウォッチとして Apple Watch Series 2 を用意し，アプリケーションとして提案方式を実装し，覗き見攻撃耐性と利便性評価との 2 点についてタッチパネルによる一般的な PIN 入力による認証方式との比較実験を行った．覗き見攻撃耐性については，正規ユーザの入力操作を攻撃者が覗き見をした時の攻撃成功率の比較を行った．利便性評価については，認証時間や誤入力率を計測し，認証時間が短く誤入力率が低いほど利便性が高いと判断した．

なお，本実験において被認証者が決める PIN の番号に「0」が含まれていた場合，PIN では「0」を，提案方式は「10」を入力することとした．

4.2 覗き見攻撃耐性実験

4.2.1 覗き見攻撃耐性実験手順

被験者は正規ユーザ役と攻撃者役の 2 人を 1 組とし，ユーザ役が行う認証操作に対し攻撃者役は右隣から覗き見を行い，その後攻撃者役はスマートウォッチに対し認証操作を試行し，その成否を記録した．その際に攻撃者役には以下の条件を与えるものとした．

- 攻撃者役は認証方式の操作方法を知っている．
- 攻撃者役はユーザ役が成功する認証操作を 2 回見ることができる．
- 攻撃者役が行う認証試行回数は 5 回までとする．

この覗き見攻撃耐性実験の手順を以下に示す．

(1) 攻撃者役はスマートウォッチの画面と操作が見えるようユーザ役の右隣に立つ．
(2) 攻撃者役はユーザ役の成功した認証操作を 2 回見る．
(3) 攻撃者役はユーザ役よりスマートウォッチを受け取り，認証操作を 5 回試行する．
(4) 試行 5 回までの攻撃成否を記録する．

この手順を，提案方式と一般的な PIN 入力による認証方式とで行った．

4.2.2 覗き見攻撃耐性実験結果

4.2.1 節の攻撃実験について，20 歳から 23 歳の男女 20 人の被験者のうち何人が覗き見攻撃に成功したかを検証した．その結果を図 1 に示す．

この実験により，タッチパネルによる一般的な PIN 入力による認証方式の覗き見攻撃成功率は 100 %だったのに対し，提案方式の覗き見攻撃成功率は 10 %となった．

4.3 利便性評価実験

4.3.1 利便性評価実験手順

被験者がユーザ役として，認証情報となる 4 桁の PIN 番号を自分で決定して設定し，その後 5 回の認証操作の試行

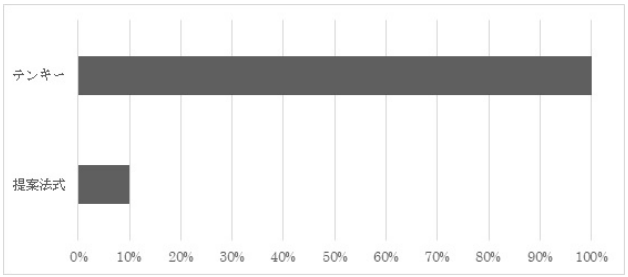

図 1　覗き見攻撃成功率
Fig. 1　Acceptance ratio of shoulder surfing.

を行う．この時の入力時間と誤入力率を計測した．また，スマートウォッチを装着する腕は，被験者が普段腕時計をつける側の腕とした．

この利便性評価実験の手順を以下に示す．

(1) ユーザ役が PIN 番号を登録する．
(2) 認証操作を 5 回試行する．
(3) 入力時間と認証の成否を記録する．

4.3.2　利便性評価実験結果

4.3.1 節の利便性評価実験について， 4.2.2 節と同様に 20 歳から 23 歳の男女 20 人を被験者とし，その入力時間と認証の成否を記録した．認証の成否については，その計測結果から誤入力率を計算した．

図 2 に一般的な PIN 入力による認証方式と提案方式との平均入力時間を示す．一般的な PIN 入力による認証方式による入力時間の全被験者の平均は 1.98 秒であったのに対し，提案方式による入力時間の全被験者の平均は 16.98 秒であった．これは一般的な PIN 入力がいずれの番号であっても 1 つの数字あたりの入力時間に差がないのに対し，提案方式の入力では数字が大きくなるにつれて入力にかかる時間が増えることが原因として考えられる．

そこで，提案方式における回転距離ごとの入力時間の平均値を測定した．その結果を図 3 に示す．なお，本実験では入力に際し必要となる回転操作において振動 1 回分の距離を 1 とし，4 桁全部の入力における回転距離を測定した（例えば入力番号が「3456」である場合は，回転距離は 18 となる）．この結果から，回転距離が 18 までは入力時間が減少しているが，18 を超えると入力時間が増加していることが判明した．

また，図 4 に一般的な PIN 入力による認証方式と提案方式との誤入力率を示す．一般的な PIN 入力による認証方式による誤入力率が 1 %であったのに対し，提案方式による誤入力率は 16 %であった．

5.　考察

5.1　覗き見攻撃耐性

4.2.2 節の実験結果より，提案方式は一般的な PIN 入力による認証方式よりも覗き見耐性は大幅に向上したと言える．今回の実験では腕を上げて攻撃者役がユーザ役の認証

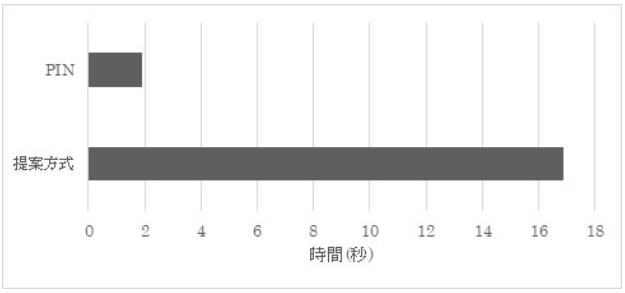

図 2　PIN の平均入力時間
Fig. 2　Average input time of PIN.

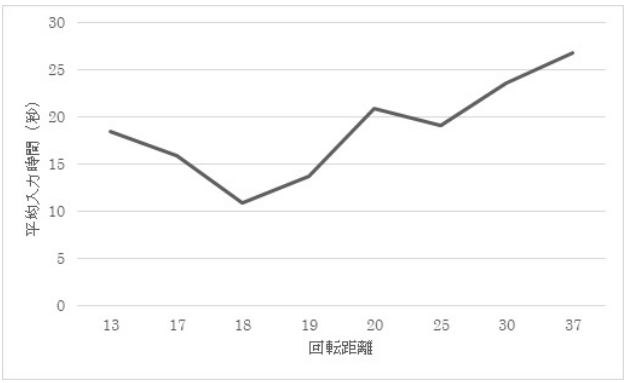

図 3　回転距離別入力時間
Fig. 3　Input time of PIN according to winding distance of the crown.

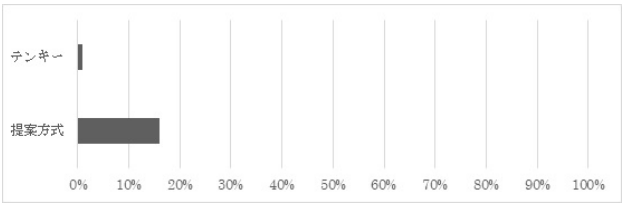

図 4　誤入力率
Fig. 4　Erroneous input ratio.

操作を覗き見できる状態で認証を行ったが，提案方式は認証操作時に画面を見る必要が無いため，腕を下げるなど攻撃者に認証操作を覗き見されにくい姿勢で認証操作を行うことが可能であり，実際にはさらに覗き見耐性の向上が期待できる．

なお，攻撃が成功した 2 回について，主に 1 桁の入力にかかる時間により番号を推測したということが攻撃者役の回答で判明した．認証毎に振動が発生する回転距離の間隔を変化させてはいるが，大きい数字が含まれると全体の桁毎の入力に対し推測が可能となることが考えられる．この対策として，

- 桁毎に回転向きを変えるのではなくランダムに回転方向を変えることで入力の桁を推測されないようにする，
- 大きい数字の入力が小さい数字の入力よりも回転数が少なくなる場合が発生する入力パターンルールを策定する，

等の方法が考えられる．

5.2 利便性

4.3.2 節の実験結果より，平均入力時間，誤入力率ともに提案方式は一般的な PIN 入力による認証方式よりも利便性が低下していると言える．これは一般的な PIN 入力では番号を 1 桁あたり 1 回のタッチパネルへの接触で入力できるのに対し，提案方式では数値に応じた竜頭型コントローラの回転操作が必要である点が大きく影響していると考えられる．このことから，ユーザが個人的な利便性を目的として，入力に必要な回転距離を短く設定する，すなわち桁毎のそれぞれの数字を小さい値にする可能性が考えられ，改善の必要がある．この対策としては， 5.1 節であげた方法がある．

一方で，必要な記憶情報量は提案方式も一般的な PIN 入力による認証方式も違いはなく，差は生じない．また，竜頭型コントローラの操作は腕時計として考えたときに直感的かつ伝統的であることから，どの被験者においても操作方法に誤解が生じることはなかった．このことから，上記の誤入力などが改善できれば，スマートウォッチのユーザ認証方式としては充分適用可能であると考えられる．

6. まとめ

本研究では，覗き見攻撃耐性向上を目的としたスマートウォッチ用の新しいユーザ認証方式を提案した．認証時における PIN の入力をタッチパネルで行わず，竜頭型コントローラの回転操作のみを用いて行える方式を採用することで，入力時の情報が画面に表示されず，また PIN の入力姿勢に自由度を持たせることができ，覗き見攻撃に耐性があると考えられる．このことを実証するためにスマートウォッチの認証アプリケーションを作成し，一般的な PIN 入力による認証方式との比較実験を行った．この結果，従来の認証方式と比較して高い覗き見攻撃耐性を持つことが実証され，スマートウォッチ用の認証方式として有効であることを示した．

今後は，覗き見攻撃耐性のさらなる向上を目指し， 5.1 節で示した改善方法の検討を行う．また， 5.2 節で示した利便性の課題について，入力時間の短縮や誤入力率低下に関する新たな入力ルールの策定について検討する．

参考文献

[1] IDC Japan 株式会社：2022 年までのウェアラブルデバイスの世界／国内出荷台数予測を発表，入手先 ⟨https://www.idcjapan.co.jp/Press/Current/201810171Apr.html⟩ (参照 2019.2.4).
[2] Bellovin, S.M. and Merritt, M.: Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks, *Proc. IEEE Computer Society Symposium on Research in Security and Privacy (S&P '92)*, pp.72–84, IEEE press (1992).
[3] 石黒司，福島和英，清本晋作，三宅優：モバイル端末のロック解除向けパターン認証の安全性評価，情報処理学会研究報告, コンピュータセキュリティ (CSEC), Vol.2012-CSEC-58, No.41, pp.1–6 (2012).
[4] Matsumoto T.: Human Identification Through Insecure Channel, *Proc. Advances in Cryptology (EUROCRYPT '91)*, LNCS 547, pp.409–421, Springer (1991).
[5] Matsumoto, T.: Human-Computer Cryptography: An Attempt, *J. Computer Security*, Vol.6, No.3, pp.129–150, IOS Press (1998).
[6] 古原和邦，今井秀樹：均等写像を用いた質問応答型直接個人認証方式ののぞき見攻撃に対するさまざまな安全特性について，電子情報通信学会論文誌，Vol.J79-A，No.8，pp.1352–1359 (1998).
[7] Roth, V., Richter, K. and Freidinger, R.: A PIN-entry Method Resilient against Shoulder Surfing, *Proc. ACM Conference on Computer and Communications Security (CCS 2004)*, pp.236–245, ACM (2004).
[8] Tan, D.S., Keyani, P. and Czerwinsky, M.: Spy-resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays, *Proc. Australia conference on Computer-Human Interaction (OZCHI 2005)*, pp.1–10, ACM (2005).
[9] 高田哲司：fakePointer:映像記録による覗き見攻撃にも安全な認証手法，情報処理学会論文誌，Vol.49，No.9，pp.3051–3061 (2008).
[10] 喜多義弘，岡崎直宣，西村広光，鳥井秀幸，岡本剛，朴美娘：覗き見耐性をもつユーザ認証システムの実装と評価，電子情報通信学会論文誌，Vol.J97-D，No.12，pp.1770–1784 (2014).
[11] 石塚正也，高田哲司：CCC:振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案，情報処理学会インタラクション 2014，pp.501–503 (2014).
[12] 東川創，満保雅浩：パターンロックの覗き見耐性向上手法について，暗号と情報セキュリティシンポジウム (SCIS 2015)，2C1-4 (2015).
[13] 稲村勝樹，新林直樹：改良型パターンロック覗き見耐性向上手法の提案と評価，情報処理学会論文誌，Vol.59，No.1，pp.179–188 (2018).
[14] 長友誠，渡辺一樹，油田健太郎，岡崎直宣，朴美娘：覗き見耐性を持つ小型タッチスクリーン端末における個人認証方式の提案，暗号と情報セキュリティシンポジウム (SCIS 2019)，3E4-2 (2019).
[15] Igaki, S., Eguchi, S., Yamagishi, F., Ikeda, H. and Inagaki, T.: Real-time fingerprint sensor using a hologram, *Applied Optics*, Vol.31, No.11, pp.1794–1802, OSA (1992).
[16] Bahuguna, R.D. and Corboline, T.: Prism fingerprint sensor that uses a holographic optical element, *Applied Optics*, Vol.35, No.26, pp.5242–5245, OSA (1996).
[17] Matsumoto, T.: Gummy and Conductive Silicone Rubber Fingers, *Proc. Advances in Cryptology (ASIACRYPT 2002)*, LNCS 2501, pp.574–576, Springer (2002).
[18] 産経ニュース：「ピースサインは危険!!」3 メートル離れて撮影でも読み取り可能，産経新聞（オンライン），入手先 ⟨http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html⟩ (参照 2019.2.4).
[19] 富士通：arrows NX F-02H，入手先 ⟨http://www.fmworld.net/product/phone/f-02h/⟩ (参照 2019.2.4).
[20] サムソン：Galaxy S8/S8+，入手先 ⟨http://www.galaxymobile.jp/galaxy-s8/⟩ (参照 2019.2.4).
[21] Carman, A.: The Galaxy S8's facial scanner can,

unsurprisingly, be tricked with a photo, *The Verge*, available from ⟨https://www.theverge.com/2017/3/31/15136226/samsung-galaxy-s8-face-scan-security⟩ (accessed 2019.2.4).
[22] 松本勉 : 虹彩照合技術の脆弱性評価（その 1），電子情報通信学会研究報告, ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会第 1 回研究発表会予稿集，pp.53–59 (2003).
[23] 松本勉 : 虹彩照合技術の脆弱性評価（その 2），コンピュータセキュリティシンポジウム (CSS 2003)，pp.187–192 (2003).
[24] 松本勉 : 虹彩照合技術の脆弱性評価（その 3），暗号と情報セキュリティシンポジウム (SCIS 2004)，pp701–706 (2004).