4E-03

強制された状況における認証技術の耐性に関する一考察

上繁　義史
長崎大学

1. はじめに

認証技術は本人性確認に関するセキュリティ技術であり，その適切な運用はICTのサービスにおいて，正当な利用者が最初に体験する機密性維持の仕組みである．これを回避する不正アクセス等の攻撃が，認証システムの理論上もしくは実装上の脆弱性を突くことにより行われる．認証技術の研究はこのような攻撃リスクを緩和するための対応であった．一方，認証が正当な利用者の意思に反して行われることは必ずしも想定されておらず，先行研究も少ない[1]．認証の段階で強制等による（利用者の意思に反した）認証のリスクを低減することができれば，セキュリティ性が高まるものと期待できる．

本稿では，認証技術の研究開発における問題提起として，正当な利用者が強制のもとに認証を行う状況を考慮する必要性について議論したい．

2. 認証における強制への耐性に関する再考察

認証技術は様々なものがあるが，サービスの内容によって必要とされるセキュリティ強度は異なる．生体認証を例にとると，一般的に他人受入率と本人拒否率がトレードオフの関係にあることから，高いセキュリティ性を要求する用途では他人受入率を小さくとる（一方で本人拒否率が上昇する）方向でパラメータの設定が行われる．逆に，セキュリティよりも利便性を重視する用途では本人拒否率を抑えた運用が考えられる．また運用においては，生体情報を扱うことから，登録情報の管理や利用についてプライバシに配慮する必要がある．

これまで著者は電子投票における耐強制性の議論を延伸して，生体認証における耐強制性を検討してきた．これは認証プロトコル上現れる情報を証拠とみなした議論であった[2]．この議論では無証拠性の定義を土台として，耐強制性を「強制する第三者を納得させる証拠を提示できない性質」としていた．この定義では，「証拠」となる情報の範囲を広くとらえており，直接的に元の情報を復元できない情報であっても，利用者に関する情報から生成されたものであれば「証拠」とみなした．だが実際には，認証が成功すれば，第三者の意思を強制することは成功しているとみなせる．認証に失敗した場合には，上述の証拠を収集することができれば付随的に提示できる．ただし，これによって強制者を納得させることが可能かは明らかではない．

このように，上述のアプローチでは，強制に関する議論の土台としては必ずしも十分ではないと考えられる．そこで本稿では，別のアプローチを考える上での基礎検討として，いくつかの利用状況における強制のケーススタディについて考察する．

3. ケーススタディ：強制が有効となる状況

生体認証は施設の入退出，ATMやパソコン等の端末利用といった，固定された装置による認証や，Webサービスなどのモバイル端末を用いた認証に用いられている．これらの用途において，以下の3つの仮定を置き，第三者が強制を成功できることを説明する．

仮定 1：第三者はソーシャルエンジニアリングなどの手段により，正当な利用者に指示することができる．

仮定 2：正当な利用者は正式なIDをもち，生体認証システムにより認証される．強雨性者の要求に従って行動する．本稿では，認証プロトコルからの逸脱はないものとする．

仮定 3：認証システムは不正アクセスに対してセキュアである．

(1) 施設の入退室において固定端末を用いるケース

施設の入退出で生体認証装置が用いられる場合，セキュリティの観点から重要な施設であるケースが多い．また入室に至るまでに，つまりは生体認証装置を使用するまでに，ICカード認証によるゲートなど，数段階のアクセス制御が行わ

A Study on Resistance of Authentication Techniques for Situation under Compulsion
Yoshifumi Ueshige, Nagasaki University

れることが考えられる．当該施設に入館した後に施設内での防犯カメラによる監視が行われることも考えられる．このことから，外部の第三者が当該施設に直接入室して不正行為を行うのは困難であると考えられる．

別のアプローチとして，外部の第三者自身ではなく，正式な ID を有する正規の利用者に入室させることを考える．これは利用者に施設への入室の権限があれば実現できる．この結果として，利用者の権限の範囲において，当該の第三者の希望する操作や情報収集を行わせることが可能である．この場合，入退出の生体認証システムは，認証によって強制する第三者の行動を予防することは極めて困難と考えられる．

（2） モバイル端末等を利用した場合

旧来の ID・パスワード認証はセキュリティ維持に限界があることはよく知られている．そこで近年では，ID・パスワード認証，所有物認証（スマートデバイス上のアプリなど），生体認証のうち 2 種類以上を組み合わせた多要素認証の導入が進んでいる．これにより通信路からの介入によって不正アクセスを行うことがより困難となった．FIDO2[3]準拠の認証システムの場合は，通信路上に送受信が発生する時点で，端末上での認証が成功しているのであって，認証に失敗した場合にはこうした通信は発生しない．

当該の利用者が認証成功後に重要情報にアクセスできると仮定して，強制が可能となる状況について考察する．近年クラウドサービスが様々な業種で業務上の用途で利用されており，なおかつこれらのサービスにおいては多要素認証が用いられることから，現実的な事象と考えられる．この重要情報の窃取を目的とする第三者が当該利用者を誘導して多要素認証を実行させて重要情報にアクセスさせれば，当該の第三者は目的を達成することが可能となる．当該の情報自体（例えば電子ファイルそのもの）を外部に送信せずとも，カメラで画面を撮影したり，メモしたりすることにより，持ち出しが可能となるためである．

4. 認証システムでの耐強制性の必要性

上で挙げた認証システムが不正アクセスに対してセキュアだったとしても，それ単独では，第三者による強制を伴う行動（アクセス）を防ぐことは想定できないと考えられる．一般的には多層的に対策されるべきものであることから，ユーザの権限に基づいて情報へのアクセス制御が適用されるが，技術的にはアクセスが行われた事後の追跡を可能とするものであり，犯行を予防する機能とは言えない．利用者の挙動（アクセス状況）から不正の実行を把握することも考えられるが，当該利用者がアクセス可能な情報の範囲が広い場合には，そうした判定自体が困難になるものと考えられる．

（独）情報処理推進機構が公開している「10 大脅威」の 2022 年版において，内部犯行による情報流出が挙がっており[4]，人間系についてのセキュリティ対策の必要性が指摘されている．その対策においては，組織的な管理体制をはじめ，犯行を思いとどまらせることが重視されており，技術的な予防策は必ずしも十分とはいえない．

現時点で強制及び耐強制の定義はできていないが，このような側面に注目した技術的な研究が必要であると考える．

5. まとめ

本稿では認証技術における強制への耐性について，特に生体認証を中心に考察を行った．外部の第三者が正当な利用者を何らかの方法で強制して認証を行わせることに成功すれば，正当な利用者のアクセス権の範囲で情報を得たりシステムを操作させたりすることが可能であることを紹介した．

今後本稿で述べた強制及び耐強制性について厳密な定義を行い，耐強制性を持つ認証プロトコルの要件について検討を行う予定である．

謝辞

本研究は科研費（課題番号 18K11297）の支援を受けて行われた。

参考文献

[1] R. Satish, N. Rajesh, A. Chakrabarty, A. Jain, S. Bafna, A. Mondal, D. Gupta, "NEUROCRYPT: Coercion-Resistant Implicit Memory Authentication", Proceedings of the AAAI Conference on Artificial Intelligence, 36(11), pp. 13041-13042. https://doi.org/10.1609/aaai.v36i11.21657

[2] Y. Ueshige, K. Sakurai, "Analysis of "Receipt-Freeness" and "Coercion-Resistance" in Biometric Authentication Protocols", AINA2016, pp. 769-775, 2016

[3] FIDO Alliance,“FIDO Alliance”, 更新 2022-12-8, https://fidoalliance.org/, （参照 2023-1-12）

[4] (独)情報処理推進機構, “情報セキュリティ 10 大脅威 2022”, 更新 2022-3-10, https://www.ipa.go.jp/security/vuln/10threats2022.html（参照 2023-1-12）