SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

攻撃発生確率を考慮した生体認証システムのリスク分析手法に関する一検討
A Methodology for Risk Analysis of Biometric Recognition Systems Considering the Attack Occurrence Probability

大木 哲史 * 成田 惇 * 内田 秀継 † 安部 登樹 †
Tetsushi Ohki Jun Narita Hidetsugu Uchida Narishige Abe

山田 茂史 †
Shigefumi Yamada

キーワード 生体認証，なりすまし，リスク分析，コンジョイント分析

あらまし

生体認証はユーザの身体的もしくは行動的特徴に基づく本人認証技術であり，その利便性の高さから近年幅広い領域へと導入が進みつつある．生体認証のセキュリティについては，これまでも認証アルゴリズムを対象として，FAR，なりすまし検知，テンプレート保護など多角的な研究が行われてきた．一方，生体認証を実環境へ導入する際には，認証アルゴリズムのみならず，導入環境におけるセキュリティ対策の有無などにより認証システムのリスクが変動することは明らかであり，これらの要因を想定した上で対策を考える必要がある．

本研究では，FAR や FRR といった既存の生体認証の評価手法に加え，悪意を持った攻撃者による攻撃発生確率と，通常のユーザーによる認証の発生確率との比，および攻撃成功による被害コストを考慮した評価指標 mFPIR により生体認証のリスク評価を行うことを目的とする．

評価基準の検討にあたっては，特定の要因（環境要因の変化，リスクとなり得る要因の追加）が攻撃者による攻撃発生確率に対してどのような変化を与えるかを予測可能であることが重要である．この観点から，実環境をふまえたリスク評価の考え方として，NIST SRE の評価手法を基に，mFPIR を悪意を持った攻撃者による攻撃と，通常のユーザーによる認証の発生確率の比率 $\alpha : 1 - \alpha$ を考慮し，さらに攻撃者による攻撃が成功した場合の被害コスト C を考慮した式で定義する．

一方，mFPIR による生体認証のリスク分析を実際に行うにあたっては，攻撃者による攻撃発生確率 α が計測可能でなくてはならない．NIST SRE では，$\alpha = 0.1$ など，任意の値を設定することで評価を行っているが，これに対する明確な根拠は存在しない．そこで本稿では，生体認証システムの構成，具体的には監視カメラの有無や，店員の有無といったユースケースに応じた攻撃対策が攻撃発生確率 α に与える影響をコンジョイント分析を用いて評価する．コンジョイント分析はサービスにおいて，消費者に対してどのような変更点が，どの程度影響を与えるのかを定量的に評価するための分析手法であり，これにより，たとえば，監視カメラを設置することでどの程度 FAR が高い生体認証システムを許容可能となるか，といった認証システムの構成要素が mFPIR に与える影響を明確化する．また，異なるユースケース間での生体認証システムのリスク評価結果を比較するとともに，任意の mFPIR を達成し得る生体認証システムを，利用者が構成可能とすることを示す．

* 静岡大学大学院 総合科学技術研究科．静岡県浜松市中区城北 3-5-1．Graduate School of Integrated Science and Technology, Shizuoka University. 3-5-1 Johoku, Naka-ku, Hamamatsu, Shizuoka.
† 富士通株式会社．神奈川県川崎市中原区上小田中 4-1-1．Fujitsu Ltd., 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa .