Risk-based Multimodal FIDO Authenticatorの提案とキーストローク認証手法の評価

山口 修司[1,2,a)]　Khin Win Myat Mon[2,b)]　五味 秀仁[1,c)]　小南 晃太朗[3,d)]　上原 哲太郎[3,e)]

概要：FIDO Authenticator 上でリスクベース認証を行い, その結果に応じて認証手段を変更可能な認証フレームワーク (authentication framework for Risk-based Multimodal FIDO Authenticator; RMFA) を提案する. リスクベース認証には, キーストローク認証等の生体行動認証を採用することで, FIDO 認証のセッションが継続しているデバイスが悪意のあるユーザーに使用された場合に, ユーザーへの明示的な認証行為を求めずにリスクの検出が可能とする. さらに, 本研究では, 提案する認証フレームワークの実現に向けた基盤として, キーストローク認証手法の比較評価を実施し, FIDO Authenticator に最適な手法を考察する.

キーワード：リスクベース認証, パスワードレス認証, キーストローク認証, FIDO 認証

Toward a Risk-based Multimodal FIDO Authenticator: Proposal and Empirical Evaluation of Keystroke Dynamics-Based Authentication

Shuji Yamaguchi[1,2,a)]　Win Myat Mon Khin[2,b)]　Hidehito Gomi[1,c)]　Kotaro Kominami[3,d)]
Tetsutaro Uehara[3,e)]

Abstract: We propose an authentication framework for Risk-based Multimodal FIDO Authenticator (RMFA) that enables risk-based authentication on the FIDO Authenticator itself. The framework allows the authentication method to be dynamically adjusted based on the assessed risk. To implement risk-based authentication, we adopt behavioral biometric techniques such as keystroke dynamics. This approach makes it possible to detect unauthorized use of a device on which a FIDO authentication session remains active, without requiring explicit authentication actions from the legitimate user. As a preliminary investigation for the proposed framework, we conduct a comparative evaluation of keystroke authentication methods and discuss which techniques are most suitable for integration with FIDO Authenticator.

Keywords: Risk-based authentication, Password-less authentication, Keystroke-based authentication, FIDO authentication

1. はじめに

IT サービスにおいて，ユーザー認証は最も重要な課題の一つである．しかし，パスワードをはじめとする従来型の認証方式は，漏洩や推測攻撃による低いセキュリティレベル，および複雑なパスワード管理に起因するユーザビリティの低下といった複数の課題が指摘されてきた [1]．これらの課題に対応するため，Fast IDentity Online (FIDO) 技術が提案され，様々な認証方式を単一のフレームワークに統合し，公開鍵暗号を用いた安全な通信チャネルを確立することでセキュリティレベルを向上させてきた．また，パスワードレス認証を実現することにより，ユーザビリティ向上も実現している [2].

[1] LINE ヤフー株式会社, LY Corporation
[2] 立命館大学 情報理工学科研究科, Graduate School of Information Science and Engineering, Ritsumeikan University
[3] 立命館大学 情報理工学部, College of Information Science and Engineering, Ritsumeikan University
[a)] shyamagu@lycorp.co.jp
[b)] khin@cysec.cs.ritsumei.ac.jp
[c)] hgomi@lycorp.co.jp
[d)] kominami@cysec.cs.ritsumei.ac.jp
[e)] t-uehara@fc.ritsumei.ac.jp

しかしながら，実際の運用環境では複数の認証手段が併存しており，ユーザーや状況に応じてそれらを組み合わせたり，リスクに応じて適切な認証強度を選択することが求められる．このためには，FIDO Authenticator を単体で利用するだけでなく，それを含めて統合的に管理し，状況に応じて制御できる枠組みが必要となる．この観点から考慮すべき点として，(1) 認証セッション確立後にユーザーを継続的に確認する仕組みが存在しないため，セッションハイジャックや認証情報の窃取への対応が難しいこと，および (2) 明示的な認証操作を要求する設計であるため，ユーザーに負担を与えやすいことが挙げられる．

このような背景のもと，先行研究として Context-Aware Multimodal FIDO Authentication (CAMFA) が提案されている [3]．CAMFA は，FIDO 標準に継続的認証技術とマルチモーダル認証技術を統合し，ユーザーのコンテキスト情報（位置情報やデバイス状態など）と生体認証情報（顔，音声，キーストロークパターンなど）を組み合わせることで，明示的な認証要求を軽減しつつ，セッション中にユーザーの正当性を継続的に検証することを可能にした．Android プラットフォーム上でのユーザー調査では，CAMFA の適用により明示的な認証要求回数を約 48 %削減できることが示され，セキュリティとユーザビリティの両面における改善が報告されている．

しかし，CAMFA を含む既存手法にはいくつかの限界が存在する．CAMFA は暗黙的認証の結果に基づき明示的認証をスキップまたは実行するという制御が行えるが，脅威状況に応じた多段階の認証強度調整や柔軟なポリシー変更には課題がある．また，CAMFA の FIDO Authenticator としての実装はモバイル端末のローカル環境に依存しており，高度な機械学習モデルの実行が困難であること，単一端末のローカルデータに限定されるため大規模行動データや脅威インテリジェンスを活用できないこと，複数端末間の統合的リスク評価ができないことなど，構造的な制約が存在する．

本研究では，これらの課題を克服するため，サーバサイドでセキュリティリスクを動的に評価し，その結果に応じて認証手段を最適化する新たな認証フレームワーク (authentication framework for Risk-based Multimodal FIDO Authenticator; RMFA) を提案する．RMFA は，サーバ側での大規模データと高性能機械学習モデルを活用した高度なリスク判定により，複数デバイス間での行動相関分析や異常検知を高精度に行うことを可能にする．

また，本研究では，第一歩としてリスクベース認証の要素技術にキーストローク認証を採用し，入力速度や打鍵間隔といった特徴量を解析することで，FIDO Authenticator におけるリスクベース認証に適した手法の条件を明らかにすることを目的とした実験を行った．この実験のために，Personal Identification Number (PIN) 入力に関するデータセットを収集・構築し，提案手法の評価を行うことでその有効性と汎用性を検証するとともに，当該データセットを研究目的で公開する．

本研究の貢献は下記の通りである．

(1) サーバサイドでリスクを動的に評価し，それに応じて認証手段を最適化する新たな認証フレームワークを提案．
(2) FIDO Authenticator に導入するキーストローク認証の手法について調査．
(3) 51 人の PIN 入力データセットを作成し評価を実施．またデータを公開．

1.1 関連研究との位置づけ

FIDO 認証を拡張しセキュリティを強化する我々のプロジェクトの一環として，CSS 2025 では，Passkey 同期環境におけるセキュリティ強化を目的とした AD-DP Framework [4] を報告する予定である．AD-DP Framework が同期パスキーのデバイス信頼性に焦点を当てるのに対し，本研究は Multimodal なリスクベース認証に主眼を置いており，FIDO 認証を補強する異なるアプローチを提示している．

2. 背景

2.1 FIDO 標準と基本モデル

FIDO 認証は，公開鍵暗号に基づき秘密情報をサーバ側に保持しない安全な認証方式である．パスワード不要であり，かつフィッシングに強い手段として広く注目を集めている．近年では WebAuthn や CTAP2 といった FIDO2 技術が主要なブラウザや OS に実装され，商用サービスでも急速に普及している [5]．FIDO2 は W3C の WebAuthn と FIDO Alliance の CTAP から構成され，クライアント，FIDO Authenticator，および Relying Party (RP) 間の相互運用を規定する．WebAuthn は公開鍵認証における登録と認証の API・データ構造・検証手順を定義し，CTAP はクライアントとローミング認証器を接続するためのプロトコルを定めている [6], [7]．登録時，Authenticator は RP ごとに鍵ペアを生成し，`authenticatorData` と `attestation` を返す．認証時には `clientDataJSON` のハッシュと `authenticatorData` を連結したメッセージに署名し，RP は登録済みの公開鍵を用いて検証する．この設計により，秘密鍵はデバイス外に漏れず，さらに Origin binding によってフィッシング耐性が確保される [6].

2.2 FIDO Authenticator の構造とセキュリティ保証

FIDO Authenticator は，鍵の生成・保護・署名に加え，生体認証や PIN を用いた本人確認をローカルで完結する．FIDO Alliance は実装のセキュリティ保証のために Authenticator Certification Levels (L1/L2/L3 等) を定義

し，ハードウェア・ソフトウェアの保護要件や耐タンパ性の強度を段階的に規定している [8], [9]．また，RP は FIDO Metadata Service (MDS) を通じて AAGUID ごとの情報を取得し，登録・認証ポリシーを柔軟に構成できる [10]．

2.3 拡張機能と運用上の設計

WebAuthn/CTAP には，`credProps` (資格情報の性質通知)，`credProtect` (本人確認必須など最小保護の強制)，`largeBlob` (小容量データの保持)，`prf` や `hmac-secret` (鍵導出) といった拡張機能が整備されている [6], [7]．これにより，パスワードレス認証にとどまらず，より幅広い応用が可能となっている．

2.4 本研究の位置づけ

パスワードを代替する仕組みの必要性は長く議論されてきており [11]，その中核として FIDO2 の産業実装は大きく進展している．しかし，FIDO 標準は認証前後の利用環境の変化に応じて制御するリスクベース認証や，セッション中に継続的に本人性を確認する仕組みを直接的には規定していない．本研究は，FIDO の強みを維持しつつ，サーバサイドでリスクを動的に推定し，必要な場合のみ追加認証を提示する認証フレームワークを提案するものである．

3. 関連研究

3.1 リスクベース認証

リスクベース認証は，ログイン時にネットワーク・デバイス・位置情報・時間帯・行動の特徴などをもとにセキュリティリスクを推定し，低リスクの場合は追加操作を求めず，高リスクの場合のみ追加認証を行う認証方式である．商用サービスでの実運用研究として，Freeman らは履歴的な IP アドレスやユーザーエージェントといった情報から統計的に不正ログインを判定し，二段階認証を提示するタイミングを最適化できることを示した [12]．また，リスクベース認証の使いやすさや設計原則を整理する調査研究も進んでおり，常に二要素認証を課す方式に比べて，ユーザー体験とセキュリティの両立に有効であると報告されている [13], [14]．一方で，リスク推定の仕組みはブラックボックス化しやすく，再現性・公平性・プライバシーの観点から，学術的な定式化は進行中である．

3.2 継続認証

継続認証とは，初回ログインの後もセッション中にユーザーの行動や環境の特徴をもとに本人性を継続的に推定する仕組みである．スマートフォンでは，キーストロークやタッチ動作，モーションセンサのデータを時系列で組み合わせることで，再ログインの手間を減らしながら，なりすましを検出する試みが行われてきた [15]．FIDO と継続認証を組み合わせた Context-Aware Multimodal FIDO Authenticator (CAMFA) は，スマートフォン上の複数のモダリティを利用してセッション中の信頼度を推定し，再認証を大幅に減らせることを示している [3]．さらに，FIDO2/WebAuthn に継続認証機能を拡張する研究として FIDOnuous が提案されている [16]．

3.3 キーストローク認証

キーストロークに基づく認証は，Gaines らの初期研究 [17] に始まり，Joyce らがキーの保持時間と打鍵間隔が有効な特徴であることを示した [18]．その後，Monrose らがパスワード強化や距離学習の観点から発展させ [19], [20]，Killourhy らは 51 名の固定語列データセットと評価プロトコルを公開し，研究比較の基盤を提供した (CMU データセット) [21]．包括的なサーベイ研究も行われ，特徴抽出・前処理・学習アルゴリズムの選択肢と組み合わせが体系的に整理されている [22]．

スマートフォンやテンキー入力における短い PIN では，キー保持時間や打鍵間隔の個人差，テンキーと数字列の違い，握り方の違いなどが識別に役立つことが報告されている [15], [23]．本研究で扱う PIN 実験は，短い入力文字列かつ学習用データが少ないという制約の中で，テンプレート更新や早期決定の設計を検証する点に特徴がある．

3.4 AI・データ拡張

キーストロークデータはユーザーごとの収集量が限られるため，近年は少ないデータで機械学習モデルを学習させる手法や時系列データ拡張が積極的に導入されている．具体的には，時間伸縮・スケーリング・ジッタ・区間置換などの変換手法がセンサデータで効果を示しており，キーストロークにも応用されつつある [24], [25]．さらに，時系列 GAN による合成データ生成は，未知のデータへの耐性評価やロバストな学習に利用できる可能性が示されている [26], [27]．また，近年の研究では Quantile Transformation (QT) による外れ値抑制と Conditional Tabular GAN (CTGAN) を用いたデータ拡張を組み合わせることで，打鍵パターンをより安定的に学習し，公開ベンチマークデータセットにおいて従来手法を上回る精度と堅牢性を達成している [28]．

3.5 本研究の位置づけ

FIDO 認証は暗号学的な本人確認を強固に実現する一方で，リスク適応や継続認証の仕組みは標準仕様の範囲外に位置している．先行研究では，リスクベース認証や継続認証の有効性が示されており，さらにキーストロークといった行動的特徴は，データが少なく入力文字列が短い条件でも補助的なシグナルとして有用であることが報告されている．本研究はこれらの知見を踏まえ，サーバサイドでの動的なリスク評価と段階的な認証を基盤とする認証フレームワークに，キーストローク認証を統合するものである．

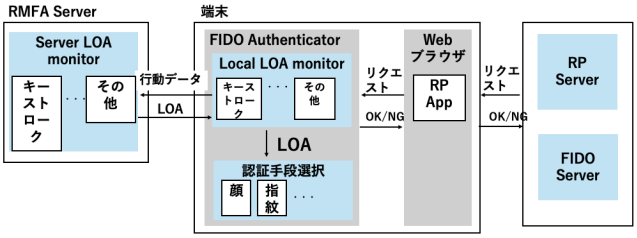

図 1 RMFA の全体構成図

4. 提案手法

サーバサイドでセキュリティリスクを動的に評価し，その結果に応じて認証手段を最適化する認証フレームワーク（authentication framework for Risk-based Multimodal FIDO Authenticator; RMFA）を提案する．RMFA は，端末側での軽量な継続計測とサーバ側での大規模学習を分担させることで，端末依存の方式の弱点を解消する．

4.1 設計と前提

提案手法の設計の前提は次の四点である．

(1) FIDO 認証の公開鍵基盤とフィッシング耐性を維持しつつ，セッション中の真正性を継続的に推定すること．
(2) リスクに応じて必要に応じた追加認証を行い，再認証の提示を最小限に抑えること．
(3) 複数端末・セッションに跨る行動相関を活用し，高精度に異常を検知すること．
(4) プライバシー最小化の原則に従い，端末側で要約しサーバ側で擬匿名化を徹底すること．

キーストローク認証は，ユーザビリティを損なわない補助要素として位置づけ，必要時のみ顔や指紋，WebAuthn の追加認証などを提示する．

4.2 全体構成とリスク評価モジュール

RMFA は，端末側での軽量な継続計測と，RMFA Server での高度なリスク評価モジュールを組み合わせて構成される（図 1）．端末側では，LOA (Level of Authentication; CAMFA に準拠 [3]) を求めるため，Local LOA monitor が行動情報（保持時間や打鍵間隔など）の統計を取得し，内容を含まない特徴ベクトルに変換して RMFA Server へ送信する．RMFA Server では，Server LOA monitor がこれらの特徴とネットワーク・デバイス・地理・履歴などの環境情報を統合し，瞬時のリスクスコア $r \in [0, 1]$ を算出する．

RMFA Server はリスク評価モジュールとして，このスコアを基に LOA を決定し，FIDO Authenticator は LOA の値に応じて認証手段を最適化し，必要最小限の追加認証を提示する．

4.2.0.1 信頼境界

FIDO Authenticator は秘密鍵生成・署名と本人確認（生体・PIN）を担う．Local LOA monitor はテキスト内容を保持せず，タイミング情報のみを扱う．RMFA Server は RP から独立したリスク評価機能として動作し，RP は RMFA Server の応答に基づき，WebAuthn の認証要求をいつ提示するかを決定する．

4.3 処理フロー

(1) **初回登録**：RP で通常通り FIDO 登録を行う．並行して Local LOA monitor は擬似識別子 pid を生成し，行動情報の要約 $\mathbf{x}$ を RMFA Server へ送信する（同意ベース）．RMFA Server は pid 単位でテンプレート $\mathcal{T}_0$ を生成する．
(2) **認証要求**：アクセス時に Local LOA monitor は最新 $\mathbf{x}_t$ を生成し送信する．Server LOA monitor はこれと文脈 $\mathbf{c}_t$，履歴 $\mathcal{H}$ を入力して r_t を算出し，RMFA Server は LOA に変換して Local LOA monitor へ返す．
(3) **段階的な追加認証**：必要 LOA に達しない場合，Local LOA monitor は最小コストの追加要素（生体認証など）を推奨する．
(4) **継続評価**：認証後も操作ごとに r_t を更新し，閾値を超えた場合は再認証を要求する．
(5) **テンプレート更新**：高信頼時のデータのみで $\mathcal{T}$ を更新する．

4.4 キーストローク認証の統合

RMFA では，キーストローク認証を明示的な認証方式の置換ではなく，ユーザビリティを損なわない補助的シグナルとして利用する．具体的には，Local LOA monitor が打鍵イベント列から生成した特徴ベクトルをサーバサイドのリスク推定に統合することで，セッション中の本人性を連続的に補強する．

この仕組みにより，低リスク時には追加認証を省略し，高リスク時には WebAuthn による本人確認を要求するなど，状況に応じた柔軟な LOA の調整が可能になる．特に，短い数値列や入力回数が限られる条件においても，キーストロークは補助的なシグナルとして LOA 推定を改善できることが期待される．

4.5 認証手段の最適化

RMFA は，サーバサイドでリスクに応じた認証手段の最適化を行う．リスクスコアが低い場合は既存セッションを継続し，中程度の場合は短時間のキーストローク入力などユーザーに追加の負担がない追加手段を提示する．一方，高リスクが検出された場合には，ユーザー検証 (例：生体認証) を要求する．このように RMFA は，状況に応じて最小限のユーザー負荷で LOA を満たすよう認証手段を選択し，ユーザビリティを維持しながらセキュリティを確保する．

4.6 プライバシー保護

RMFA は，(a) 内容非依存の時刻差分のみを扱う，(b) 端末内で要約し擬似識別子のみを送信する，(c) 保持期間を最小限とする，(d) テンプレート更新は高信頼時に限定する，(e) 学習は匿名統計データで行う，といった原則を徹底する．これにより，行動特徴の活用とプライバシー保護を両立する．

5. FIDO Authenticator へのキーストローク認証導入

FIDO Authenticator にキーストローク認証を導入するための設計の要件は以下の点に整理できる．

- **認証精度**．FIDO の対話は短くサンプル数も限られるため，6 桁前後の固定列入力であっても個人性を抽出できる必要がある [21], [22], [23].
- **低遅延**．追加認証が発生するとユーザー体験を大きく損なうため，サーバサイドでのリスク推定を妨げない応答の低遅延性が不可欠である．
- **ドメイン頑健性**．プラットフォーム差や入力方式（上段数字列・テンキー差）を跨いでも安定した性能を示すことが求められる [24].
- **攻撃耐性**．なりすましや AI による合成データを使用した攻撃に耐えられること．
- **プライバシー保護**．送信される情報は保持時間や打鍵間隔といった要約統計に限定し，テンプレート更新も高信頼時のみ行うことで，ユーザーの入力内容を保護しつつ特徴量を活用する．
- **リスクベース認証との整合性**．キーストローク由来のスコアは，IP や端末，地理などの環境特徴と統合し，サーバサイドのリスクベース認証の一要素として活用する [12]．これにより，LOA の動的調整が可能となる．

本研究では，NIST SP 800-63B に示される認証保証レベル（Authenticator Assurance Level; AAL）の考え方に則り，まず基盤となる認証精度と低遅延に焦点を当てて評価を行う [29]．これは，PIN 入力等では入力文字列が短くサンプル数も限られるため，高い精度を維持することが運用上必須であり，またユーザー体験を大きく損なうため，応答の低遅延性も同様に不可欠だからである．一方で，ドメイン頑健性，攻撃耐性，プライバシー保護，リスクベース認証との整合性については，将来的な課題として位置づける．

6. 実験

RMFA の設計要件のうち基盤となる認証精度と低遅延の達成可能性を検証することを目的とする．PIN 入力データを用いたオフライン評価により，モデルの識別性能と推論速度を計測した．

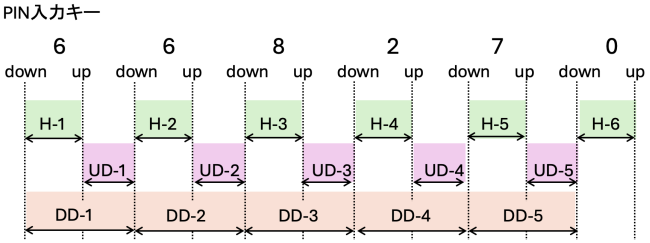

図 2 CMU データセットの特徴量変換手法

6.1 データセットの作成方法

実験に用いる PIN 入力データセットは，実験参加者を募り新規に収集した．入力ログ収集プログラムを作成し，実験参加者はログイン画面を模したアプリケーション上で，PIN を想定した 6 桁の番号を繰り返し入力した．各入力イベントはキーの押下・解放時刻と入力回数として記録した．PIN は Excel の RANDBETWEEN 関数により乱数生成し，全員が共通の 6 種類の PIN をそれぞれ 80 回入力，最後の 5 回は 5 秒の休止を挟んで入力した．誤って Enter を押し忘れた記録や Backspace を使用した入力は除外し，正しく入力されたデータのみを保持した．

実験環境は大学内の指定座席において着席した状態で整えた．使用した PC は Dynabook SJ73/KU である．入力方法として，数字キーによる入力は Dynabook 本体のキーボードを用いて実施し，テンキーによる入力は FUJITSU KU-0325 を使用した．

6.2 実験参加者

本実験は，立命館大学の学生と教職員が閲覧できる掲示板を用いて実験参加者を募集した. 対象者は立命館大学大阪いばらきキャンパスに所属する学生および教職員とした. 参加の報酬は 1000 円とした. 2024 年 11 月から募集をし，応募のあった 51 名を対象として実験を行った. 実験参加者の属性は，性別では男性 48%，女性 52%，使用 PC は Windows ノート PC が 73%，MacBook が 27%であった. 数字入力方法については，上部の数字キー利用が 92%，テンキー利用が 8%であった．実験参加者には事前に研究の目的と内容を説明し，同意を得た上で実験に参加した．

6.3 機械学習

6.3.1 特徴量

CMU データセット [21] のフォーマットを採用し，収集した PIN 入力データを変換し特徴量として使用した．各ユーザーの入力試行について，キー入力を H (Hold Time: キーが押されてから離されるまでの時間) , UD (UP–Down Time: キーを離してから次のキーを押すまでの時間)，DD (Down–Down Time: キーを押してから次のキーを押すまでの時間) の 3 種類の特徴量として変換し 16 次元のベクトルとした (図 2).

6.3.2 QT を用いた前処理

入力データには外れ値が含まれるため，Quantile Transformation (QT) を適用し，分布を標準正規分布に写像することで学習の安定化を図った．QT の適用前後でデータ分布が改善されることは先行研究でも確認されている [28].

6.3.3 CTGAN を用いたデータ拡張

モデルの性能を高めるため，Conditional Tabular GAN (CTGAN) によるデータ拡張を導入した [30]．以下のように教師あり学習の正例・負例を定義した．

- 正例（本人）：ユーザー本人の PIN 入力試行 80 回
- 負例（攻撃者）：他ユーザーの PIN 入力試行からランダムに選択した 80 回

各ユーザーに対して合計 160 行（正例 80 行＋負例 80 行）を基礎データセットとした．CTGAN を 200 エポック学習させ，それぞれの 80 行を 38,400 行に拡張した結果，正例・負例あわせて 76,800 行の拡張データセットが得られた．

6.3.4 学習モデルと評価方法

学習モデルには決定木 (DT)，k 近傍法 (KNN)，Naive Bayes (NB)，Support vector machines (SVM) を用いた．先行研究 [28] では CNN や転移学習ベースの画像処理手法を採用しているが，これらは計算負荷が高いため，本研究では対象外とした．

評価は，先行研究 [28] と同様，Accuracy (ACC)，Precision，Recall，F1-score，Equal Error Rate (EER)，AUC の値に加え，処理速度（1 試行あたりの処理時間）の指標を用いた．加えて，CTGAN によるデータ拡張の有無を組み合わせ，データ拡張の効果を検証した．

6.3.5 実行環境

実験は MacBook Air (13 インチ, 2024, Apple M3, メモリ 24 GB, macOS 14.4.1) 上で，Python 3.8，scikit-learn，SDV を利用して実装・実行した [31], [32]．検証方式はホールドアウト法，処理時間は，学習済みモデルとテスト行列がメモリ上に常駐した状態で，開始・終了時刻を CPU 上で計測し，5 回の反復平均を求めた．

6.4 結果

表 1 に基礎データセットを用いた場合，表 2 に拡張データセットを用いた場合のモデル別の性能比較を示す．

データ拡張を行わない場合，いずれのモデルも十分な性能を発揮できなかった．特に DT および NB は ACC が 50〜56%，EER が 40〜64%と高く，実用的な認証には不十分であることが分かる．KNN および SVM は比較的良好な結果を示したものの，Recall が 40〜50%，AUC が 0.29〜0.76 と低水準な結果となった．

一方，CTGAN によるデータ拡張を導入した場合，すべてのモデルで性能が大幅に向上した．ACC は 90%以上を達成し，Precision，Recall，F1 もほぼ同等の値を示したことから，バランスのよい分類が可能であることが確認できた．AUC は 0.90〜0.99 に達し，EER も 10%以下に低減した．特に SVM は ACC 94.78%，AUC 0.99，EER 5.22%と最良の結果を示した．これらの結果は，CTGAN による拡張が少数の入力試行からでも高精度な学習を可能にし，モデルの汎化性能を著しく向上させることを示している．

また，表 1 および表 2 に示すように，すべてのモデルでデータ拡張後であっても推論時において極めて高速に動作した．DT および NB は，拡張の有無にかかわらず 1 サンプルあたり 0.00 ms と，ほぼ瞬時に分類が可能であった．KNN と SVM はデータ拡張後やや処理時間をかかったが，いずれも 1 ms 未満である．これらの結果は，(1) PIN のような短い文字列であっても特徴量（H/UD/DD）の個人差が有効な識別手掛かりであること，(2) サンプル不足の影響を CTGAN が緩和し精度と汎化を向上できることを示している

7. 考察

7.1 FIDO 認証への適用可能性

実験では，CTGAN 拡張を用いることで全モデルが EER ≈ 5–10%以下，推論時間はいずれのモデルも 1 ms 未満であった．これらの数値は，高い認証精度と低遅延が必要であるという条件において，FIDO Authenticator に実装上無理なく統合できることを示す．

7.2 サーバサイド実施の意義

RMFA の設計（4 章）において，キーストローク認証はローカルの明示的本人確認の代替ではなく，サーバサイドのリスクベース認証を補強する暗黙的な認証として組み込まれる．サーバサイドで実施する利点は以下の通りである．

- 大規模学習とモデル更新：CTGAN を含む生成・学習処理をサーバに集約することで，データ拡張・またユーザー横断のデータを利用した学習が可能となり，認証の精度を向上できる．
- 文脈特徴との統合：ネットワーク・端末・地理・履歴などの信号とキーストロークスコアを統合し，LOA を柔軟に計算可能となる．
- 多端末・多セッションの相関：同一アカウントの複数端末間での行動相関を統合可能となり，乗っ取り等の兆候の早期検知が期待できる．

以上より，サーバサイド実施は FIDO Authenticator の認証の精度を向上させる選択となっている．

7.3 処理速度

本実験の推論は極めて高速であり，オンライン経路の遅延要因にはなりにくい．ただし，学習用データの増大には課題があることが考えられる．本設定では，1 ユーザーあたり基礎データ 160 行（正 80/負 80）を CTGAN で約 480× に拡張し 76,800 行とした．16 次元の特徴で概算すると約

表 1 基礎データセットを用いた場合の各学習モデルの性能比較（平均値 ± 標準偏差）

モデル	ACC (%)	Precision (%)	Recall (%)	F1 (%)	EER (%)	AUC	処理時間 (ms/sample)
DT	56.30 ± 6.45	39.88 ± 8.21	40.47 ± 11.30	39.79 ± 9.09	40.51 ± 9.13	0.50 ± 0.07	0.00 ± 0.00
KNN	72.11 ± 5.97	70.67 ± 18.44	41.55 ± 12.61	47.80 ± 11.98	28.77 ± 10.81	0.73 ± 0.08	0.04 ± 0.08
NB	49.80 ± 4.44	22.96 ± 7.14	21.24 ± 6.18	21.66 ± 5.46	64.44 ± 5.87	0.29 ± 0.04	0.00 ± 0.00
SVM	72.52 ± 6.02	65.75 ± 20.33	49.44 ± 11.70	50.01 ± 11.19	29.09 ± 8.64	0.76 ± 0.08	0.00 ± 0.00

表 2 拡張データセットを用いた場合の各学習モデルの性能比較（平均値 ± 標準偏差）

モデル	ACC (%)	Precision (%)	Recall (%)	F1 (%)	EER (%)	AUC	処理時間 (ms/sample)
DT	90.01 ± 3.88	90.00 ± 3.88	90.03 ± 3.89	90.01 ± 3.88	10.01 ± 3.89	0.90 ± 0.04	0.00 ± 0.00
KNN	93.51 ± 3.28	93.53 ± 3.30	93.50 ± 3.34	93.51 ± 3.29	6.48 ± 3.31	0.97 ± 0.02	0.06 ± 0.02
NB	94.00 ± 2.99	94.08 ± 3.06	93.92 ± 2.98	93.99 ± 2.99	6.00 ± 2.99	0.98 ± 0.01	0.00 ± 0.00
SVM	94.78 ± 2.65	94.79 ± 2.64	94.76 ± 2.69	94.78 ± 2.66	5.22 ± 2.65	0.99 ± 0.01	0.18 ± 0.09

5 MB/人のデータ拡張が生じるため，ユーザー数 N に対し $\approx 5N$ MB の一時的学習データを扱う計算となる（100 万ユーザー規模で数 TB）．学習パイプライン設計でデータ拡張をオンデマンドで実施しない，データを特徴量として圧縮した形で保存するなどの検討が必要である．

7.4 リスクベース認証との統合

RMFA において，キーストローク認証のスコアをリスクベース認証に組み込み，LOA の動的調整を可能とする点が重要な特徴である．しかし，本研究では PIN 入力の認証精度と遅延のみを評価対象としたため，リスクベース認証との統合シナリオは扱っていない．今後は，環境特徴（IP，端末情報，地理的変化など）とキーストロークスコアを融合し，LOA に応じた追加認証を最適化する必要がある．

7.5 Limitation

本研究の Limitation を整理する．

- 対象と入力環境の偏り：日本在住者かつ JIS 配列キーボードに限定して収集しており，文化・言語・スクリプトや配列（ANSI/ISO），入力デバイス（ノート上段列／外付けテンキー／モバイル）差の影響を評価していない．国・地域ごとのモデルあるいはドメイン適応の導入が有望である．
- 実験条件：研究室環境・6 桁 PIN 固定・短時間収集という制約下であり，疲労/姿勢/設置の影響を見ていない．
- 攻撃耐性の未評価：提示攻撃・合成データ（GAN）による模倣・リプレイ等の攻撃に対する実験を未実施．
- プライバシー実装：本実験では PIN を収集したが，4.6 章で挙げた仕組みの実装が前提となる．その環境下での精度再検証が必要．
- データセット：国内で公開されている PIN 入力データセットが存在しなかったため，本研究で新規作成した．これは日本語圏の研究基盤としての貢献であるが，規模・多様性の拡充が望まれる．

8. PIN 入力データセット

本研究で用いた PIN 入力データセットを公開する．データの収集方法は 6 章で述べた通りである．データは GitHub で入手可能であり，研究目的に限り利用可能である[*1]．

9. 研究倫理

本研究は，実験を実施するにあたり所属機関の研究倫理規程及びサイバーセキュリティ研究倫理に関するチェックリスト[*2]を確認し，それに則って計画・実施を行った．実験参加者には事前に研究の目的と内容を説明し，同意を得た上でデータ収集を行っている．また，実験参加者のプライバシーには十分に配慮している．収集・公開したデータは PIN 入力におけるキー操作ログのみであり，個人情報は一切取得していない．

10. おわりに

FIDO Authenticator とサーバサイドのリスク判定を組み合わせ，状況に応じて認証方法を切り替える 認証フレームワーク (authentication framework for Risk-based Multimodal FIDO Authenticator; RMFA) を提案した．キーストロークの情報を用い，FIDO のセッションが続いている間も本人性を確認することで，ユーザーに追加の操作を求めずに不正利用の兆候を検知できる．実装の基礎検討として，6 桁 PIN の入力データを 51 名から収集し，CTGAN による拡張を適用して DT/KNN/NB/SVM を比較した．CTGAN を使わない場合は精度が不足したが，適用により EER 5–10%へと大きく改善し，推論はすべて 1 ms 未満となった．これらの結果から，RMFA はキーストロークを用いたリスク判定を FIDO Authenticator に自然に統合でき，セキュリティリスクに応じた認証の実行に有用であることを確認した．

[*1] https://github.com/cysec-lab/PIN_input_dataset
[*2] https://www.iwsec.org/csec/ethics/checklist.html

参考文献

[1] 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, *Proc. of S&P*, pp. 553–567 (2012).

[2] 山口修司，五味秀仁，大神　渉，日暮　立：WebAuthn ベース生体認証のユーザビリティの分析と評価，情報処理学会論文誌，Vol. 64, pp. 904–918 (2023).

[3] Kim, S., Choi, D., Kim, S.-J., Cho, S. and Lim, K.: Context-Aware Multimodal FIDO Authenticator for Sustainable IT Services, *Sustainability*, Vol. 10, No. 5, p. 1656 (online), DOI: 10.3390/su10051656 (2018).

[4] Khin, W. M. M., Yamaguchi, S., Gomi, H. and Uehara, T.: AD-DP: Device-Aware Anomaly Detection for Securing WebAuthn Passkey Authentication, *Proc. of Computer Security Symposium* (2025).

[5] Feng, H., Li, H., Pan, X., Zhao, Z. and Cactilab, T.: A Formal Analysis of the FIDO UAF Protocol., *NDSS* (2021).

[6] W3C: Web Authentication: An API for accessing Public Key Credentials Level 2, W3C Recommendation (2021).

[7] FIDO Alliance: Client to Authenticator Protocol (CTAP) 2.1, FIDO Alliance Proposed Standard (2021).

[8] FIDO Alliance: Authenticator Certification Levels, FIDO Alliance White Paper (2020).

[9] FIDO Alliance: Biometric Requirements (FIDO Certified), FIDO Alliance Requirements (2019).

[10] FIDO Alliance: FIDO Metadata Service (MDS) Version 3, FIDO Alliance Specification (2020).

[11] 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, *2012 IEEE Symposium on Security and Privacy*, pp. 553–567 (online), DOI: 10.1109/SP.2012.44 (2012).

[12] Freeman, D. M., Jain, S., Dürmuth, M., Biggio, B. and Giacinto, G.: Who Are You? A Statistical Approach to Measuring User Authenticity, *Network and Distributed System Security Symposium (NDSS)* (2016).

[13] Wiefling, S., Raschke, P. and Dürmuth, M.: Evaluation of Risk-Based Authentication, *Symposium on Usable Privacy and Security (SOUPS)* (2020).

[14] Wiefling, S., Dürmuth, M. et al.: A Systematic Review of Risk-Based Authentication, arXiv preprint (2020).

[15] Frank, M., Biedert, R., Ma, E., Martinovic, I. and Song, D.: Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 9, pp. 1360–1372 (online), DOI: 10.1109/TIFS.2013.2278712 (2013).

[16] Pöhls, H. C., Herzberg, M., Metz, D. and Banse, C.: FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication, *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pp. 75–84 (online), DOI: 10.1109/DAPPS52256.2021.00017 (2021).

[17] Gaines, R. S., Lisowski, W., Press, S. J. and Shapiro, N.: Authentication by Keystroke Timing: Some Preliminary Results, Technical report, Naval Research Laboratory (1980).

[18] Joyce, R. and Gupta, G.: Identity Authentication Based on Keystroke Latencies, *Communications of the ACM*, Vol. 33, No. 2, pp. 168–176 (online), DOI: 10.1145/75577.75582 (1990).

[19] Monrose, F. and Rubin, A. D.: Password Hardening Based on Keystroke Dynamics, *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 73–82 (online), DOI: 10.1145/266420.266434 (1997).

[20] Monrose, F. and Rubin, A. D.: Keystroke Dynamics as a Biometric for Authentication, *ACM Transactions on Information and System Security*, Vol. 3, No. 4, pp. 367–397 (online), DOI: 10.1145/382912.382914 (2000).

[21] Killourhy, K. S. and Maxion, R. A.: Comparing Anomaly-Detection Algorithms for Keystroke Dynamics, *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 125–134 (online), DOI: 10.1109/DSN.2009.72 (2009).

[22] Teh, P. S., Teoh, A. B. J. and Yue, S.: A Survey of Keystroke Dynamics Biometrics, *The Scientific World Journal*, (online), DOI: 10.1155/2013/408280 (2013).

[23] Buschek, D., De Luca, A. and Alt, F.: Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices, *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 1393–1402 (online), DOI: 10.1145/2702123.2702252 (2015).

[24] Iwana, B. K. and Uchida, S.: Time Series Data Augmentation for Deep Learning: A Survey, *arXiv preprint arXiv:2002.12478* (2021).

[25] Um, T. T., Pfister, F., Pichler, D. et al.: Data Augmentation of Wearable Sensor Data for Parkinson's Disease Monitoring with Convolutional Neural Networks, *Proceedings of the 19th ACM SIGKDD Workshop on Health Informatics (ML4H at KDD)* (2017).

[26] Esteban, C., Hyland, S. L. and Rätsch, G.: Real-valued (Medical) Time Series Generation with Recurrent Conditional GANs, *Advances in Neural Information Processing Systems (NeurIPS) Workshops* (2017).

[27] Yoon, J., Jarrett, D. and van der Schaar, M.: Time-series Generative Adversarial Networks, *Advances in Neural Information Processing Systems (NeurIPS)* (2019).

[28] Raouf, H. A., Fouda, M. M. and Ibrahem, M. I.: Revolutionizing User Authentication Exploiting Explainable AI and CTGAN-Based Keystroke Dynamics, *IEEE Open Journal of the Computer Society*, Vol. 6, pp. 97–108 (online), DOI: 10.1109/OJCS.2024.3513895 (2025).

[29] Grassi, P. A., Garcia, M. E. and Fenton, J. L.: Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B), Technical report, National Institute of Standards and Technology (2017).

[30] Xu, L., Skoularidou, M., Cuesta-Infante, A. and Veeramachaneni, K.: *Modeling tabular data using conditional GAN*, Curran Associates Inc. (2019).

[31] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M. and Duchesnay, E.: Scikit-learn: Machine Learning in Python, *Journal of Machine Learning Research*, Vol. 12, pp. 2825–2830 (2011).

[32] Patki, N., Wedge, R. and Veeramachaneni, K.: The Synthetic data vault, *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, pp. 399–410 (online), DOI: 10.1109/DSAA.2016.49 (2016).