

micro:bitを用いた2段階認証オートロックの作成

東京都立調布北高等学校 2年 山崎宗一郎

研究の背景

近年、住宅侵入や鍵の不正利用といった犯罪が問題となっており、防犯対策の高度化が求められている。たとえば、SNS上の鍵の写真から合鍵を作成されたり、テンキー錠の操作をのぞき見されて暗証番号を盗まれるといった事例も報告されている。とくに、従来の鍵や暗証番号のみに依存した認証方式は、盗難やのぞき見などによるリスクを抱えている。この現状から、高度化した犯罪に対する対策が必要であると考えた。その解決策として本研究では、micro:bitを用い、利用者の「動作」を認識するAIジェスチャー認証と、利用者の「知識」および「所有物（スマホ）」を必要とするワンタイムパスコード（OTP）認証を組み合わせたシステムを開発した。

開発方針

利用者が正しいジェスチャーをしたかをmicro:bitがチェックし（①ジェスチャー認証）、合格したら一時的なパスコード（OTP）が作られる（②）。そのパスコードがスマホに送られ（③）、利用者がそれを入力して認証されると（④）、ドアのロックが解除される（⑤）。

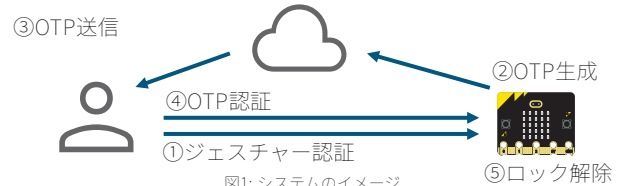


図1: システムのイメージ

方法と実装

ジェスチャー認証

micro:bit Create AIを使い、次の3つのジェスチャーをmicro:bit Bに学習させた。（図2）

- 何もしていない状態
- ジェスチャー①
- ジェスチャー②

micro:bitがジェスチャーを検知するとそのジェスチャーが登録したジェスチャーに近くなるほど、確実性が上昇する。bのジェスチャーの確実性が90パーセントを超えた一定秒後に、cのジェスチャーの確実性も90パーセントを上回ったとき、micro:bit Cに信号を送るようにした。

※ジェスチャー認証をクリアするには2つの定められたジェスチャー（bとc）を連続で行うことが必要

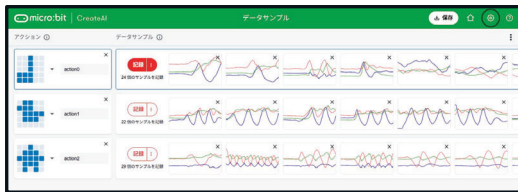


図2: ジェスチャーの学習画面

OTP認証

OTP認証を次のように実装した。（図3）

- 100000から999999の6桁の乱数を生成
- Wi-Fi経由でBlynkに送信、スマホでBlynkの画面を確認（図4）
- 確認したOTPをキーパッドを通してmicro:bit Cに入力
- micro:bit Cで入力されたOTPが正しいものか確認

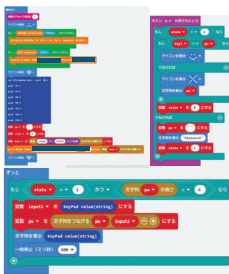


図3: micro:bit Cのプログラム



図4: スマホでOTPを確認

これらの2つの認証が成功したら、micro:bit Aに接続されたモーターがドアの鍵を適切な速度で回転し、ロック解除される。

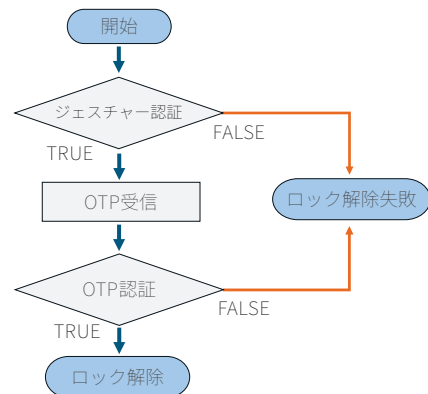


図4: 全体のフローチャート

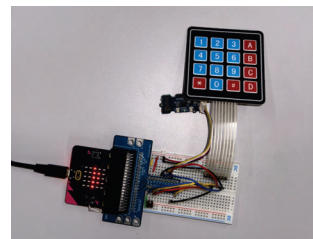


図6: micro:bit Cのイメージ

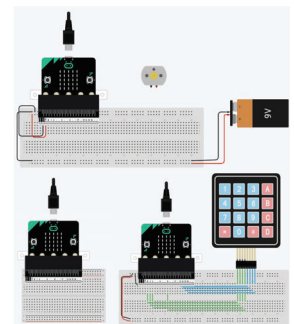


図5: ブレッドボードの概要図

考察

本研究により、「のぞき見による暗証番号の漏洩」や「鍵の盗難・複製」といった問題に対し、「特定のジェスチャー（知識）」と「OTP（所有）」という異なる二つの要素を要求することで、第三者による不正開錠のリスクを軽減できることが分かった。

また、システム全体がWi-Fi環境やBlynkに依存しているため、自宅のインターネット回線が悪かったり、Blynkのサーバーがダウンしているとロックを解除できないという致命的な問題も残っていると感じた。この問題を解決するためには、BluetoothをWi-Fiの代わりに用いたり、そもそもインターネットを必要としないシステムにしたりすることが求められていると考えた。

参考文献

Blynk公式サイト: <https://www.blynk.io/>
micro:bit公式サイト: <https://microbit.org/ja/>
micro:bit Create AI公式サイト: <https://createai.microbit.org/>

謝辞

本研究は、東京都立調布北高等学校と電気通信大学との高大連携教育研究協定書に基づいて行われました。電気通信大学の世合理子先生、TAの大村和輝さんにはたくさんのご協力、表裏についてのアドバイスをいただきました。心よりお礼申し上げます。