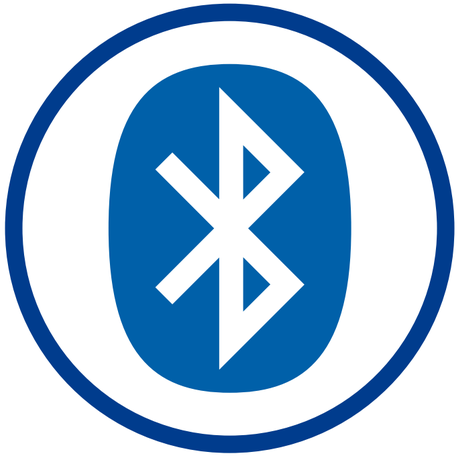
IE3A 山本和樹
中間発表

2025/11/25

目次

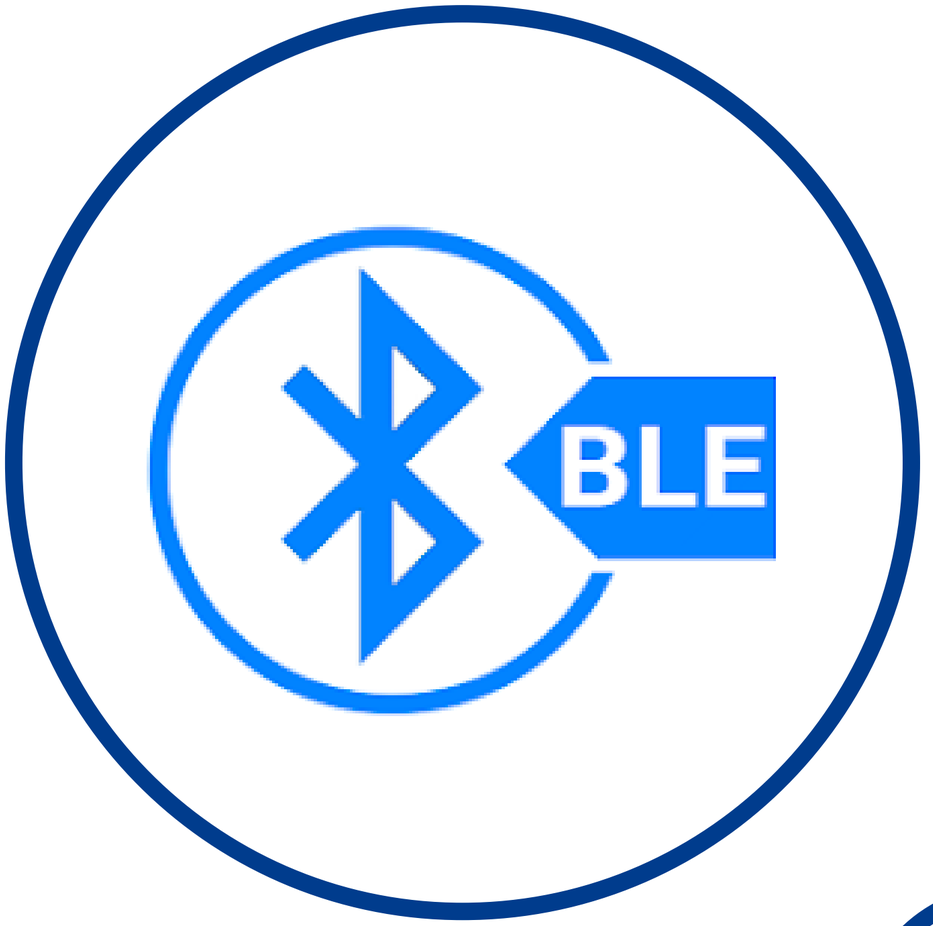
研究テーマ

BLEの通信技術研究と検証
(暗号化、自動接続の仕組み)



研究進捗

- 自動接続は完了
- 暗号化はRSAの復号化ができた



研究内容
BLEの自動接続

M5stack

```
#define SERVICE_UUID        "12345678-1234-1234-1234-1234567890AC"
```

Swift

```
private let targetService = CBUUID(string: "12345678-1234-1234-1234-1234567890AC")
```

つまりSwiftがこのUUID“12345678-1234-1234-12341234567890AC”と
同じUUIDを持ってるペリフェラルを探しているだけ
バックグラウンド接続もSwiftのinfo.plistで宣言すれば自動接続可能

しかしアプリが必要

研究内容

BLEの自動接続

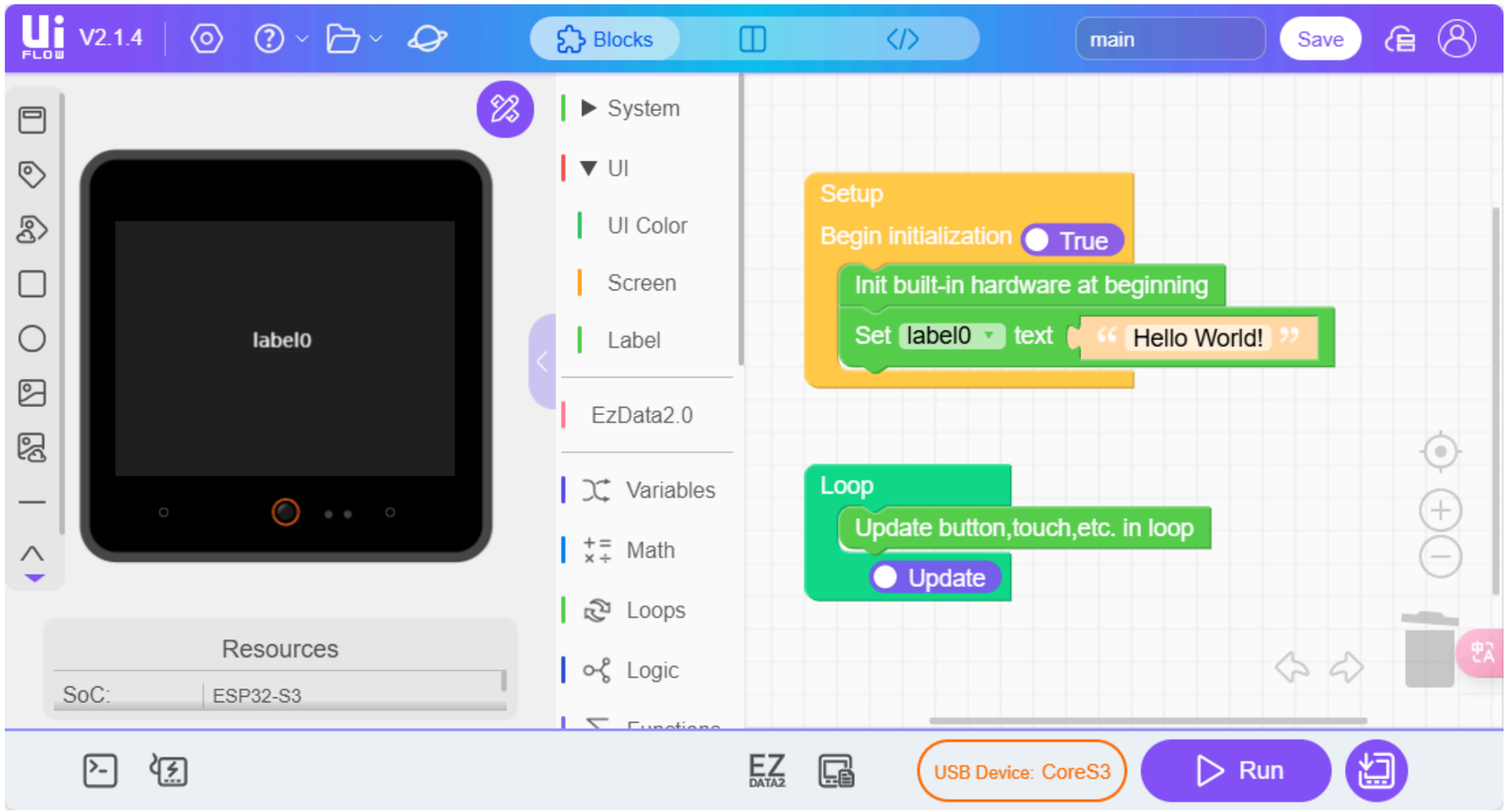
普通のblutoothとの自動接続の違い

	アプリが必要	初回から接続	kill状態での接続
BLE	○	○	×
Bluetooth	×	×	○

研究内容
M5での暗号化

UIFLOW = micropython

micropythonにはRSA対応ライブラリが存在しないので言語をC++に変更



研究内容

M5での暗号化

キャラクタスティック

```
Serial.println("Characteristic UUID: beb5483e-36e1-4688-b7f5-ea07361b26a8");
```

データ通信の際に使用されるUUID。データ通信にこのUUIDを公開して通信する。データ構造を定義しているようなイメージに近い感じ？

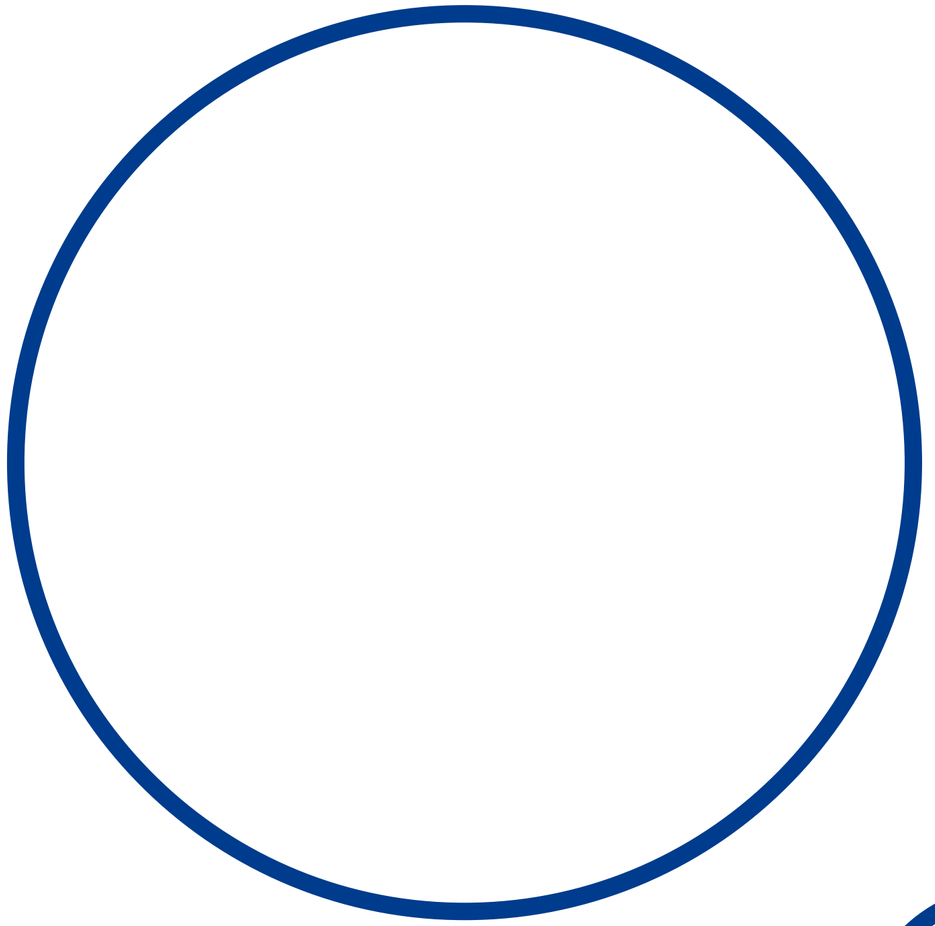
MTUの制限に注意

＊MTUとは・・・簡単にいうと通信の際に遅れるデータの容量

M5は初期20しか使用できず、設定ファイルを変更して許可を出さないと21以上を解放できずに使用できない

これから

- PQC(耐量子暗号)を使用しRSAと比較する
- BLEの他の機能をしらべる



まとめ

- 進捗：自動接続とRSAの復号化できた
- これから：PQC(耐量子暗号)を使用しRSAと比較する

ご清聴ありがとうございました