

BLE を使った簡易的な近距離チャットアプリ

後藤洸樹

目次

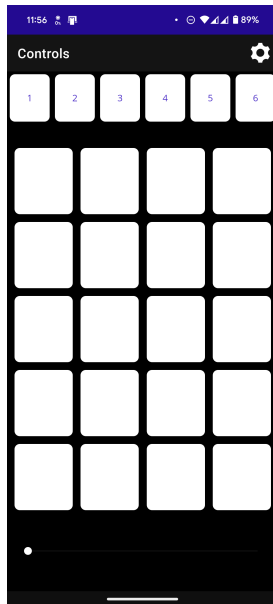
1. 自己紹介
2. 作ろうとした理由
3. BLE の説明
4. 作ったもの
5. 作ったものの欠点
6. 今後の展望

自己紹介

- 名前
 - 後藤洸樹
- 所属
 - 摂南大学 電気電子工学科
 - 摂南大学 情報処理技術研究部
- 好きな技術
 - C#
 - dotnet
 - BLE を使った開発
 - .NET Aspire(普通の開発でも神技術)
- SNS
 - X : @lausiv1024
 - Github : Lausiv1024

これを作ろうとした理由

- スマホを左手デバイスとして使えるアプリケーションを作っている。
- これに応用できないかと考えたから。



そもそも BLE とは

- Bluetooth の省電力規格
- IoT 等の省電力な用途で使われることが多い
- 基本 Gatt プロファイルで通信を行う

ネットワーク構成

ブロードキャスト方式は今回割愛…
コネクション方式について説明

セントラル(主にクライアント側)

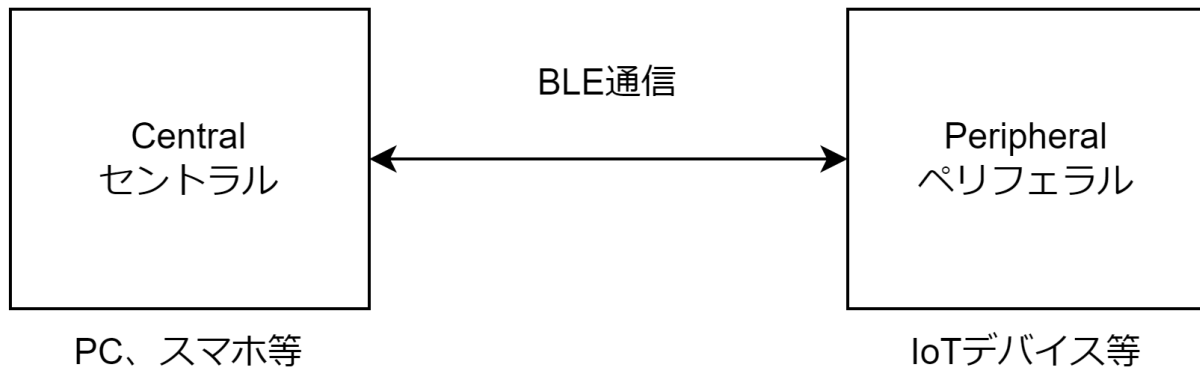
主に PC 等がこちらの役割を果たす場合が多い。
IoT 機器等からデータを受け取る用途に使ったり

ペリフェラル(主にサーバ側)

IoT デバイス等がこちらの役割を果たす場合が多い。主に接続してきたセントラルにデータを送信する用途に使われる。

そもそも BLE とは (ii)

よくある構成



BLE の通信方法

Service

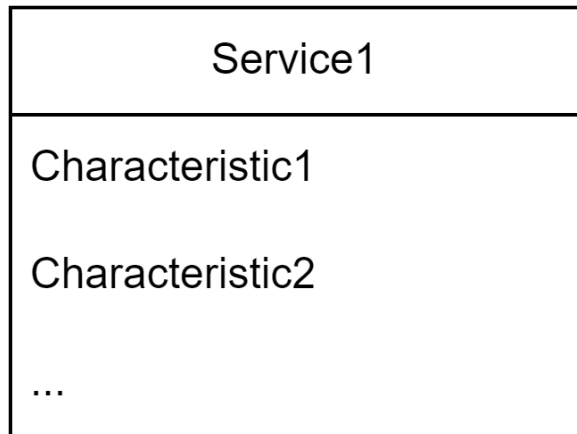
機能の単位で作られる定義

例：キーボード単体

Characteristic

実際にやり取りするデータが入る場所

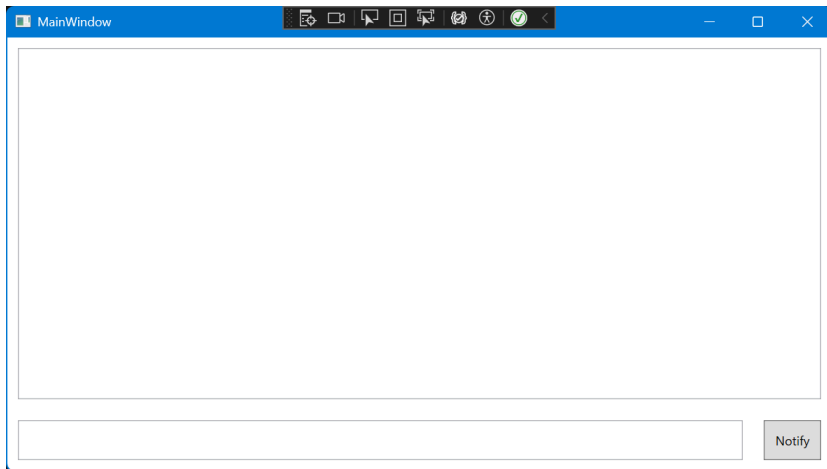
例：押されたキーの情報



早速よくある構成と逆で作しましょう

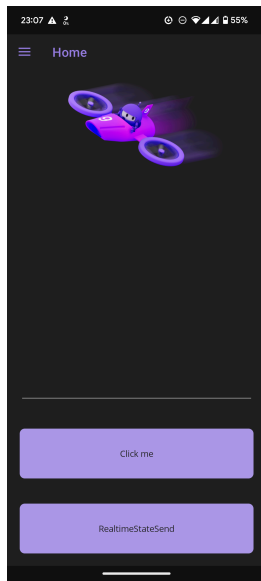
デスクトップ App(WPF)

- Peripheral として動作
- Central からのデータを受信
- Central へのデータ送信(Notify 機能を利用)



スマホ App(.NET MAUI)

- Central として動作
- Notify 機能(ペリフェラルからセントラルへ送信)による通知情報の受信
- データ送信



逆にした理由

スマホ側のライブラリがセントラルとして動作させることを目的に作っており、それに準拠する形で作ったから

スマホをセントラルにする欠点

Write(Sentral→Peripheral の通信)が遅い！！

とても左手デバイスとして使おうとは思えないレベル。逆に Notify は割と行ける。

ペアリング機能(現在実装中)

BouncyCastle を用いた ECDH 鍵合意機能を用いて、公開鍵の交換と計算で共通鍵を導出。これで導出された共通鍵をペアリングの鍵として使用したい。

BouncyCastle に頼っているものの楕円曲線暗号に対応している。

現状迷っていること

- 果たしてこの暗号技術で大丈夫なのか
 - 中間者攻撃の懸念
 - 署名等を使う？
 - その他セキュリティ関係の穴

今後の展望

スマホをペリフェラルとして使う

遅延の問題に対してはこれが1番早いと思います。

使用したライブラリ・フレームワーク

Mobile App

- .NET MAUI
- Bluetooth LE plugin for Xamarin & MAUI

今回紹介したプロジェクト

今回紹介したプロジェクトは以下のリンクから確認できます。

ペアリング機能を実装中(ブランチ名が MessagePack だけど気にしないで)

BLETest