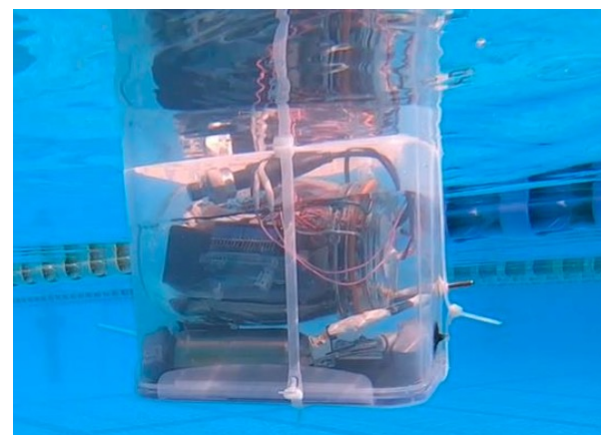
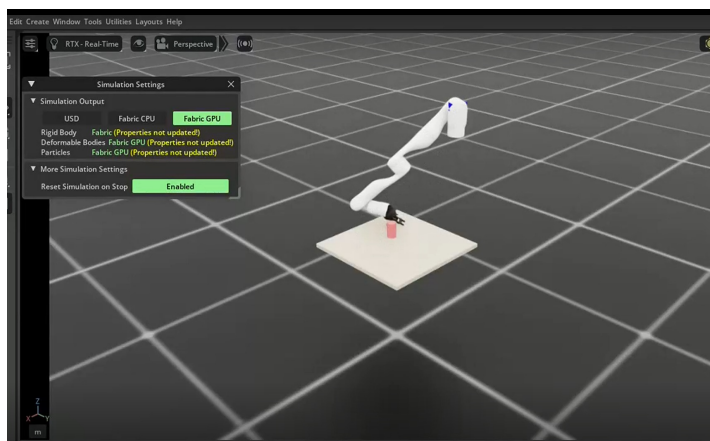
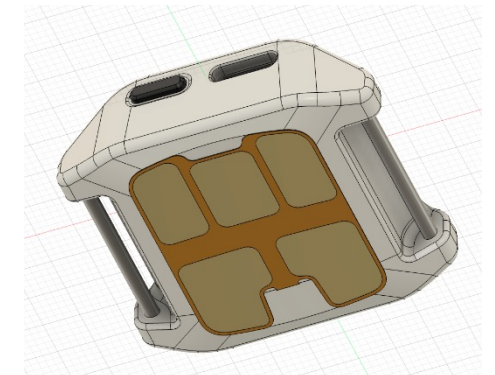
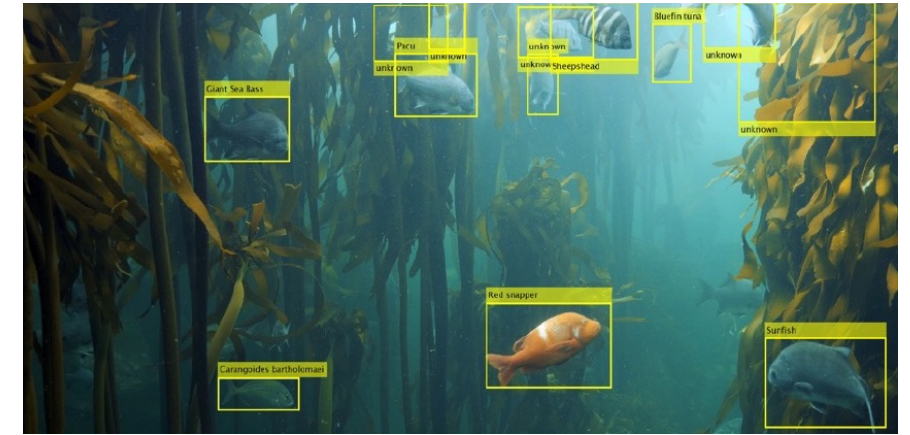


ファームウェアアップデート サーバの実装

自己紹介

- 小松琢磨
- 所属：筑波大学情報学群情報科学類3年(AC)
ultracoins,WORD編集部
- 出身：京都(滋賀)
- 趣味：触覚モーショントラッカー開発,時計,
ドライブ



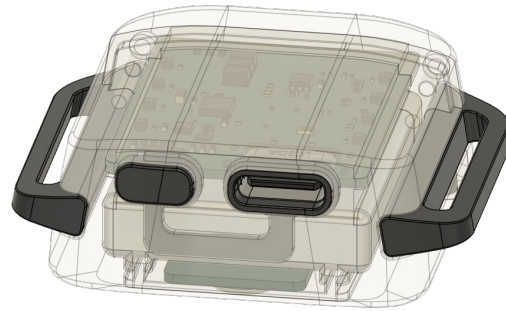
Ultracoin



MoBits

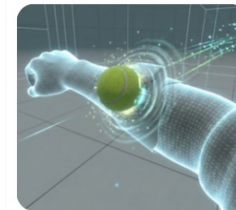
電気刺激とモーションキャプチャを用いた
VR触覚フィードバックシステムの開発

村松 拓人 / 小松 琢磨
(PM) 稲見 昌彦



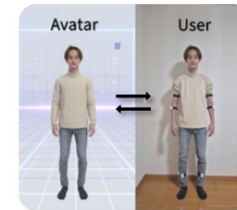
物体の固さを、ぶつかる衝撃を、身体で直接感じる体験。

MoBits は、モーションキャプチャと EMS（電気刺激）を融合させた、双方向型ウェアラブルデバイス。
あなたの動きを VR 空間に伝え、VR 空間からのリアクションを「触覚」としてフィードバックします。



触覚フィードバック

VR 空間で物に触れた瞬間、
感覚や衝撃を EMS(電気刺激)
で現実世界に伝えます。



双方向の没入体験

動きがアバターに反映され、
アバターの接触が返ってくる
境界のない一体感。



腕時計レベルの小型さ

重たく、大型な設備は不要。
Apple Watch ほどのサイズで
「感じる」を実現します。



Status

Connection

● 未接続

Battery

🔋 0%

BLE Tracking Rate

📶 0.0 Hz

DEBUG

Firmware

最新バージョンです

最新

詳細

IMUキャリブレーション

Address

8FE66B2B-6647-F9C8-858F-9159C719BD10

Firmware Version

1500

Serial Number

1

Device Type

1

取り付け位置

左前腕



Status

Connection

● 未接続

Battery

🔋 0%

BLE Tracking Rate

📶 0.0 Hz

DEBUG

Firmware

デモ表示

更新を開始

デモ用表示（更新対象が見つかった場合に実行できます）

詳細

IMUキャリブレーション

Address

8FE66B2B-6647-F9C8-858F-9159C719BD10

Firmware Version

1500

Serial Number

1

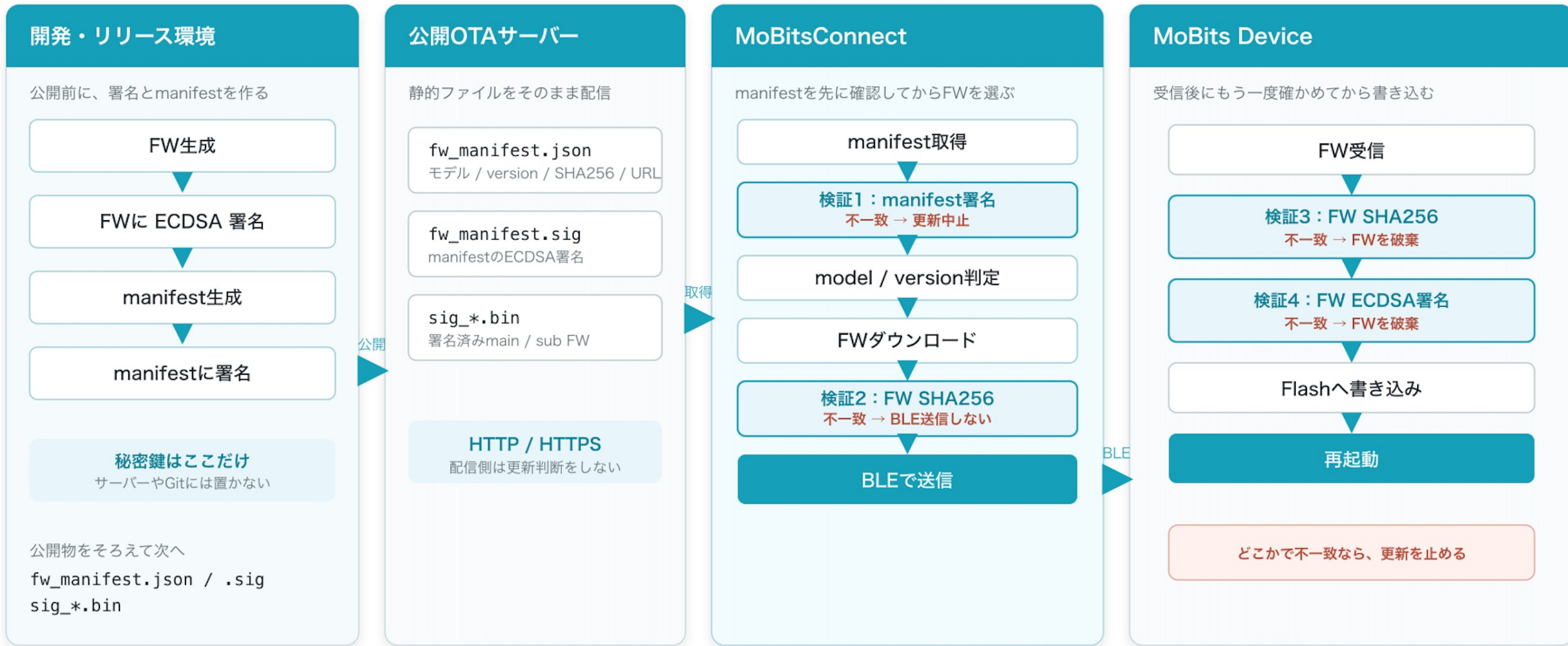
Device Type

1

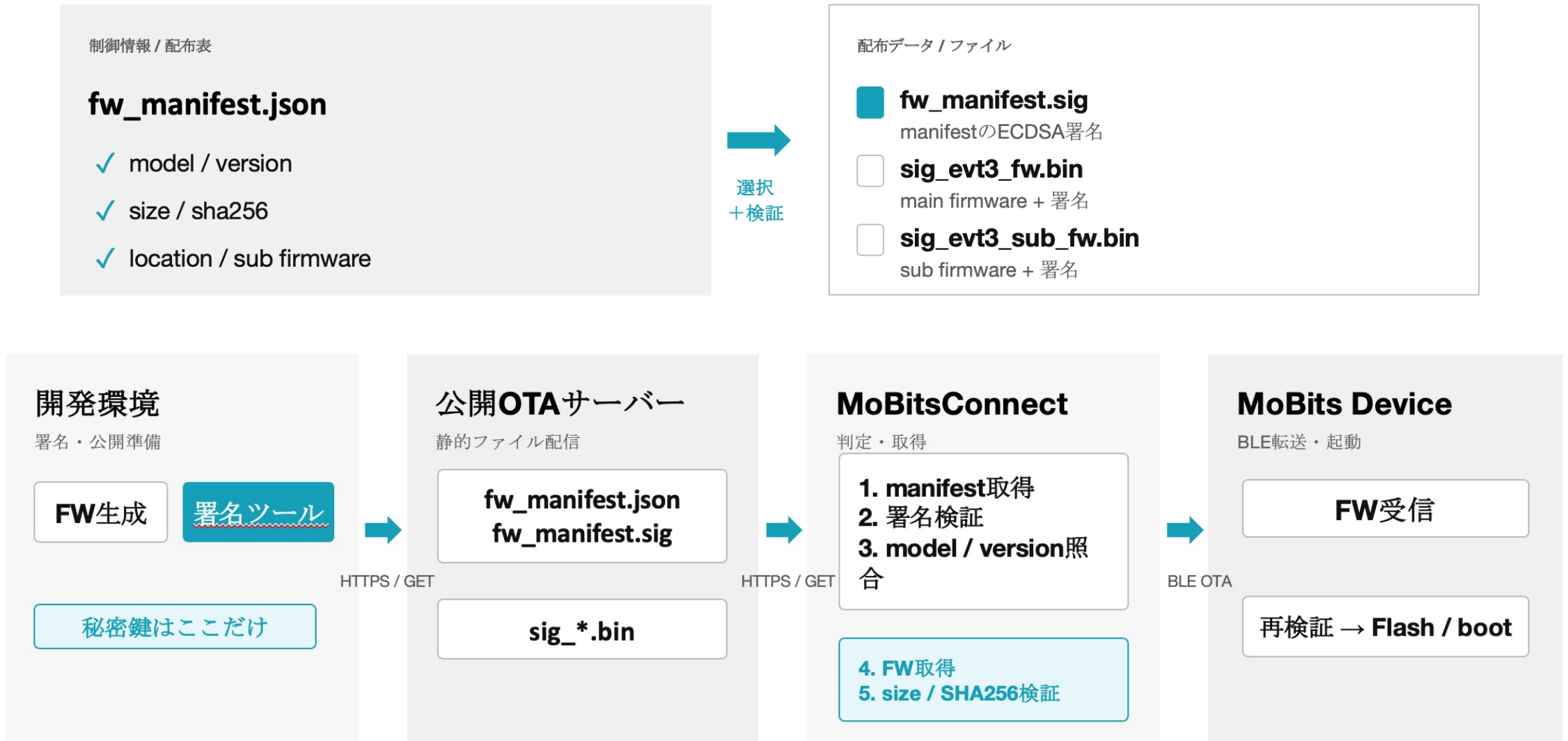
取り付け位置

左前腕

フロー図



システム構成



実際の公開手順



アプリからの挙動

01

manifest + sig
を取得

ota_manifest_init()

02

ECDSA署名を
検証

public key + SHA256

03

modelを照合
versionを比較

manifest.version > device.fw_version

04

FW URLを
採用

main / sub を選択

FAIL

署名不一致なら、**FWのURL**も**version**も採用せず中止。

更新判定



version

device version

更新対象が
存在する時だけ
次のダウンロードへ進
む

01

GET .bin

manifest.location
から取得

02

size

manifest.size
と一致するか

03

SHA-256

manifest.sha256
と一致するか

04

BLE OTA

main → sub
の順で送信

05

Device

受信側でも
再検証

検証の過程

01

manifest署名

Server → Connect

ECDSA

FW取得を開始しない

02

FWハッシュ

Server → Connect

SHA-256

BLE転送を開始しない

03

受信ハッシュ

Connect → Device

SHA-256

FWを破棄

04

FW署名

Connect → Device

ECDSA

FWを信頼しない

署名は誰が作ったか、ハッシュは受け取った内容が同じかを確認

Manifestの具体例

FW_MANIFEST.JSON / MODEL = 3

```
{
  "model": 3,
  "version": 1000,
  "size": 1082032,
  "sha256": "455b56d5...1fd63079",
  "location": "/sig_evt3_fw.bin",
  "sub": true,
  "sub_size": 120664,
  "sub_location": "/sig_evt3_sub_fw.bin"
}
```

この1レコードが決めること

model 3

version 1000

main 1,082,032 bytes

sub 120,664 bytes

sub = true のときだけ
2本目を取得・転送する。

今後の展望

- HTTPS化・アクセス管理
通信経路と公開先をより安全にする
- 公開手順の自動化
署名、SHA256、manifest生成、公開前チェックを自動化する
- 段階的な配信
対象モデルや端末を分けて、少しずつ更新する
- 監視とロールバック
異常を検知したら配信を止め、必要に応じて前のFWへ戻す