

詳解・電子辞書でLinuxがブートするまで

末田 卓巳 @puhitaku

Brain Hackers Meetup #1 一般発表

自己紹介

末田 卓巳

Takumi Sueda



@puhitaku



フリー開発者。2020年9月に SHARP Brain への Linux ポーティングを発表、翌10月に Brain Hackers を発足。

好きなもの

- 全レイヤーの技術、特に低いレイヤー
- リバースエンジニアリング
- 牛丼
- 音楽





おさらい: SHARP Brain とは？

- SHARP が販売する Windows CE 入り電子辞書
- 公式に販売されるアプリのほか、自分でビルドした CE 向け exe (PE) が追加できる

2011年までに発売されたモデル

- TOSHIBA TMPA910CRAXBG (armv4l) + 64 MiB DRAM
- Windows CE

2012年～2020年のモデル

- NXP i.MX28 (armv5tej) + 128 MiB DRAM
- Windows CE

2021年発売の新モデル～

- NXP i.MX7ULP (armv7-a, armv7e-m) + 128 MiB DRAM
- μ ITRON ベース RTOS



おさらい: Brain への Linux ポーティング

- puhitaku (発表者) が PW-SH1 で Linux のブートに成功
- 続く Brain Hackers 立ち上げ + 有志の努力により i.MX28 搭載機種すべてにポーティングを拡大
- Debian をカスタムしたディストリビューション Brainux をリリースし Raspberry Pi と変わらない手軽さで誰でも Brain で Linux が動かせるようになった

新機種 PW-x1 (i.MX7ULP) の解析とポーティング

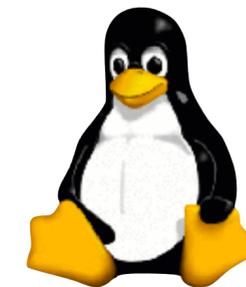
- ガッツリ進んでます
- 多分 @pepepper のトークのネタバレになるので割愛
- 11/20 の Kernel/VM探検隊online part4 で話す予定



本題



いい感じに Linux が動く仕組み





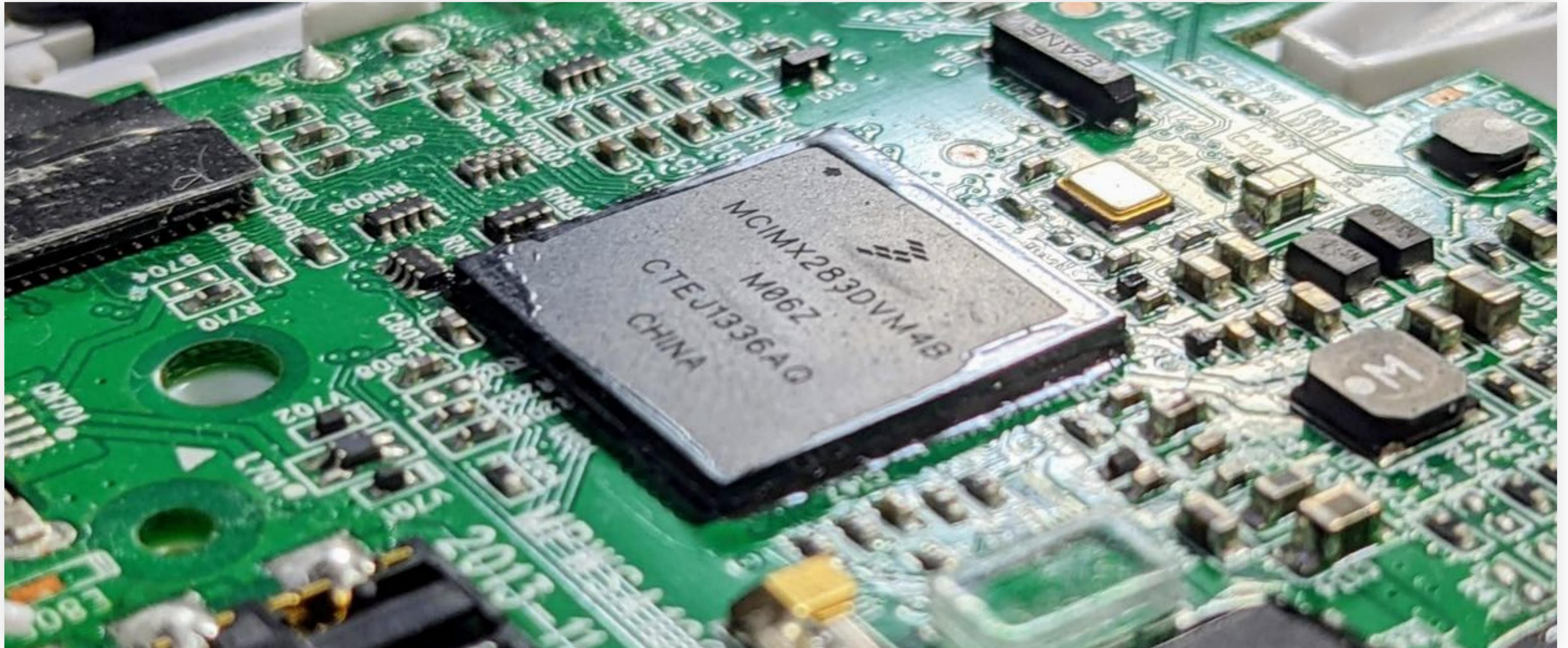
Windows CE を
ブートする仕組み



リセット直後
すべての始まり



1. Windows 以前

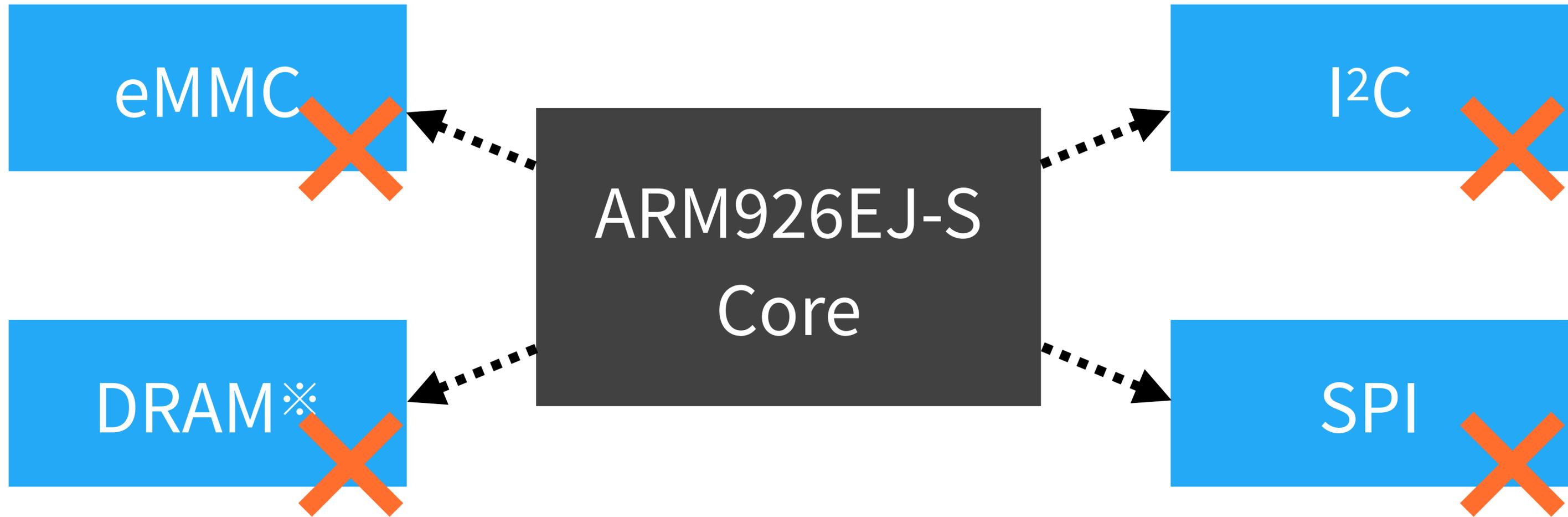


電源が入った直後の ARM SoC は何を実行するのか？

A. Boot ROM

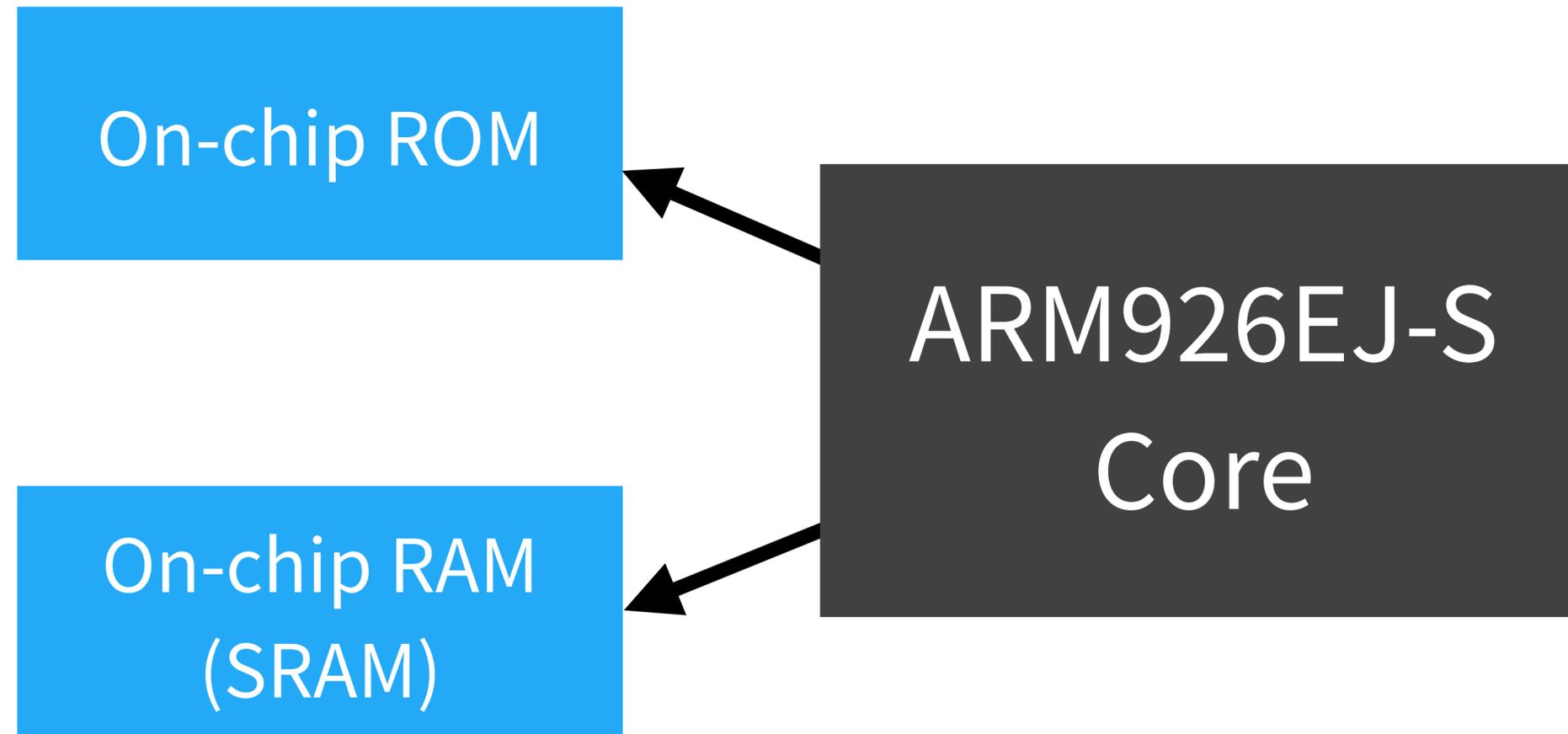
A. Boot ROM

(i.MX28 の場合: On-chip ROM)



電源が入って直後の ARM コアはバスで直接繋がったものしかアクセスできない

※ DRAM はまず初期化が必要; 以降はバス経由で透過的に読み書きできる



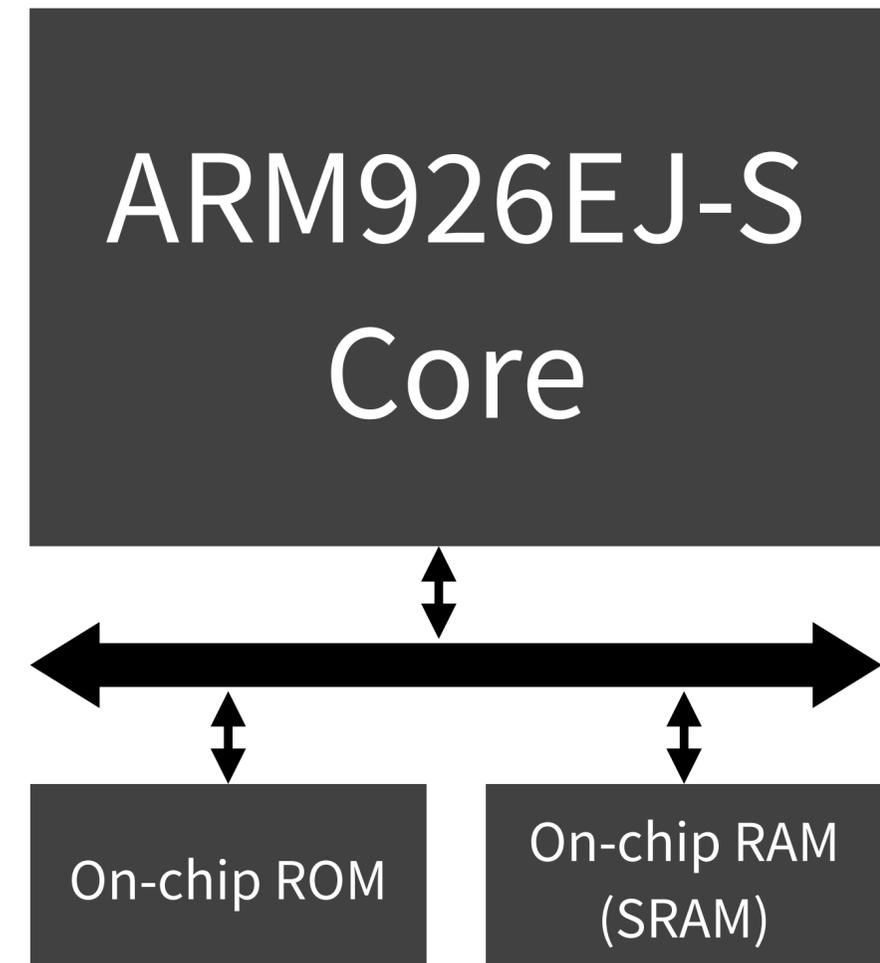
On-chip ROM と On-chip RAM はリセット直後からアクセスできるので最初に実行するコードは On-chip ROM から読み、On-chip RAM を作業領域にする

- USB slave (recovery)
- I²C
- SPI
- SSP (eMMC / SD)
- GPMI (NAND)
- JTAG

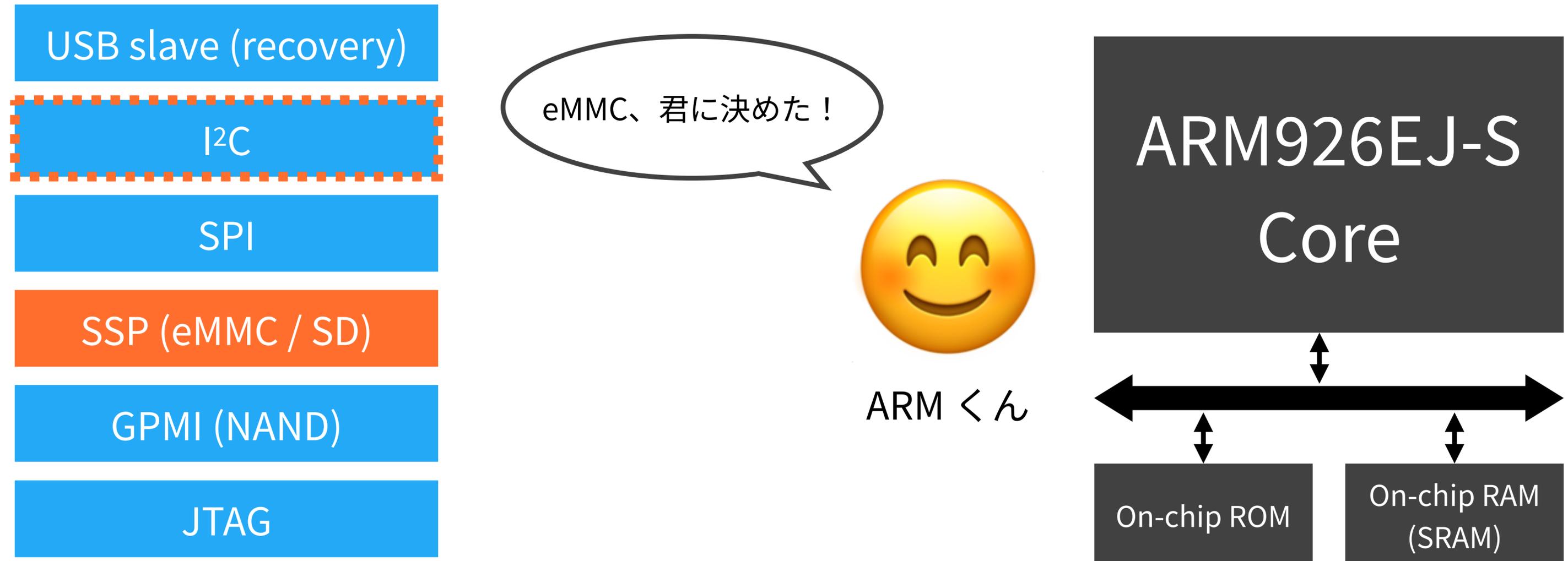
どれで起動しようかな



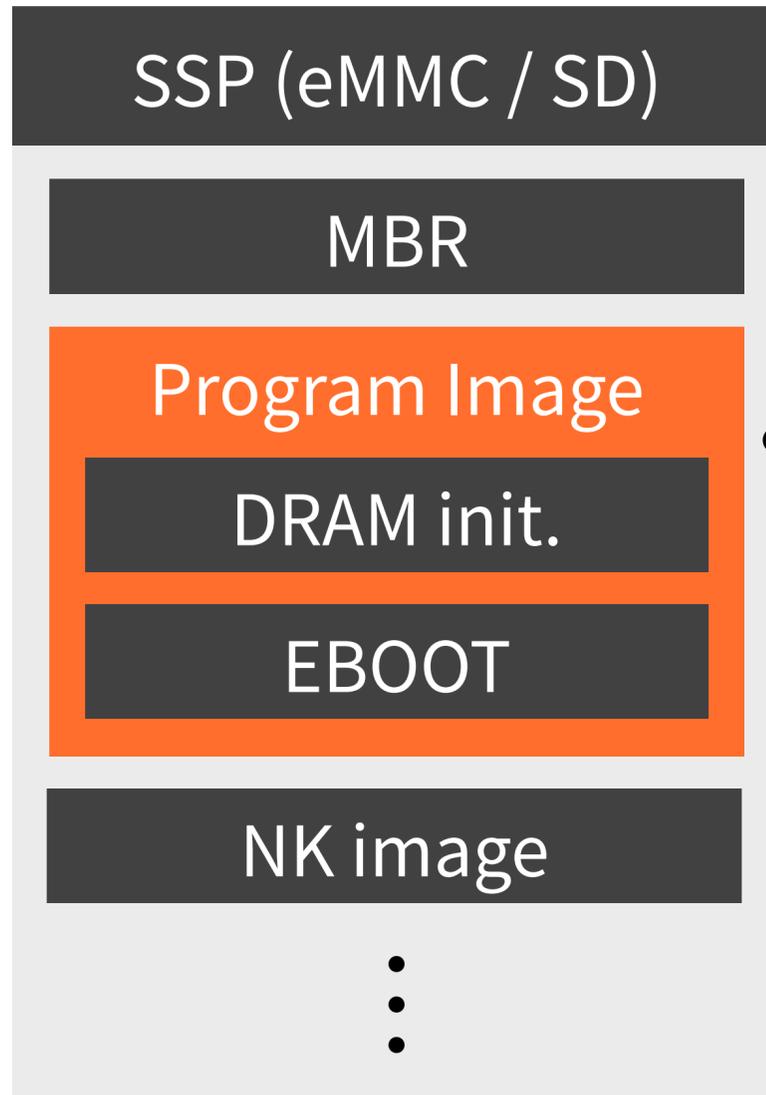
ARM くん



On-chip ROM に書かれた最初のブートローダーを使って
起動デバイスを選択・ペリフェラル初期化・次のブートローダーを読み込む



Brain では One-Time-Programmable ROM に「eMMC で起動せよ」と書かれている
(機種によって I²C EEPROM から起動して eMMC に移行するものもある)



Program Image を解釈・実行するよ

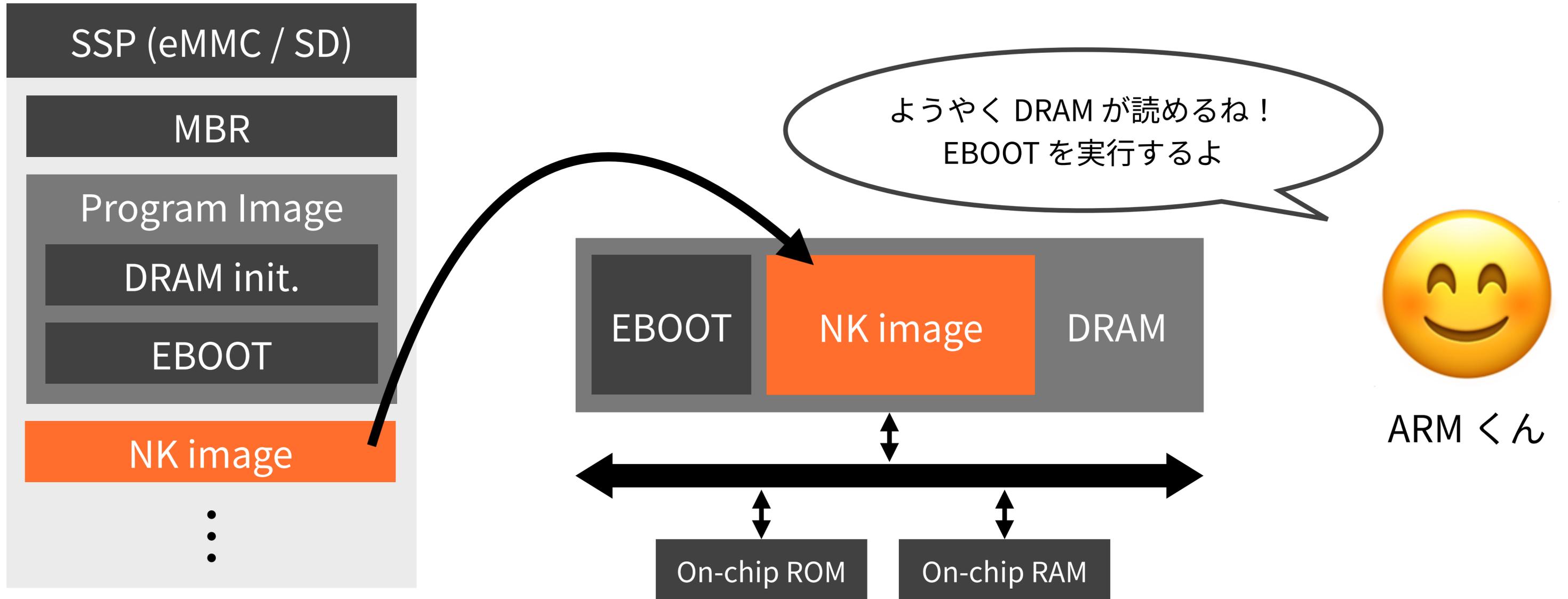
```
1 DISPLAYPROGRESS
2 SECTION 0x0 BOOTABLE
3 TAG LAST
4 LOAD 0x1000 spl/u-boot-spl.bin
5 LOAD IVT 0x8000 0x1000
6 CALL HAB 0x8000 0x0
7 LOAD 0x40200000 u-boot.bin
8 LOAD IVT 0x8000 0x40200000
9 CALL HAB 0x8000 0x0
```



ARMくん

Boot ROM が実行するコマンドの例
(注: Windows のものではありません)

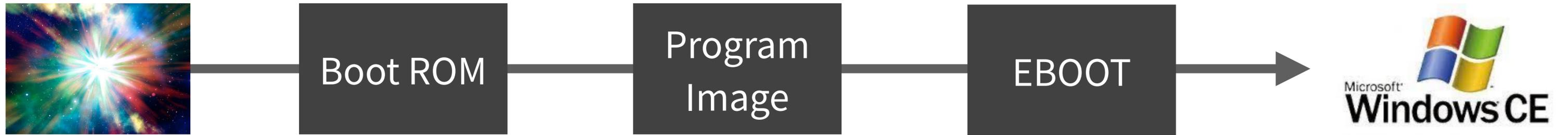
eMMC にある Program Image に記述されたコマンドを逐次実行し
DRAM の初期化プログラムや次のブートローダー (EBOOT) のロードを行ってジャンプ



EBOOT が NK image (Windows のシステムを固めたもの) を
先程初期化した DRAM に展開しジャンプ



こうしてめでたく Windows CE がブートする

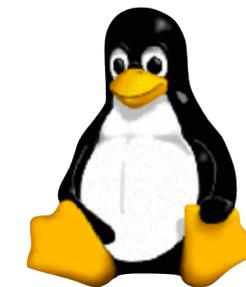


Windows 以前の流れのおさらい

2. Windows 以降



いい感じに Linux が動く仕組み



おさらい: SHARP Brain とは？

- SHARP が販売する Windows CE 入り電子辞書
- **公式に販売されるアプリのほか、自分でビルドした CE 向け exe (PE) が追加できる**

2011年までに発売されたモデル

- TOSHIBA TMPA910CRAXBG (armv4l) + 64 MiB DRAM
- Windows CE

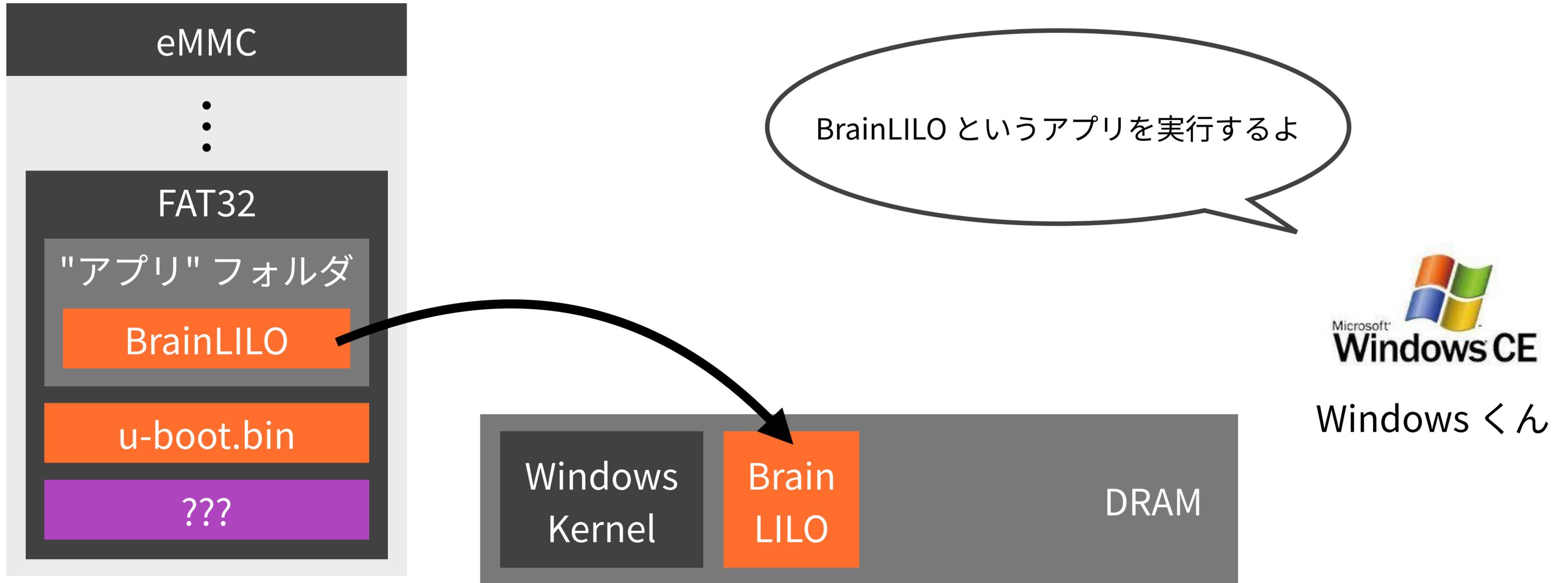
2012年～2020年のモデル

- NXP i.MX28 (armv5tej) + 128 MiB DRAM
- Windows CE

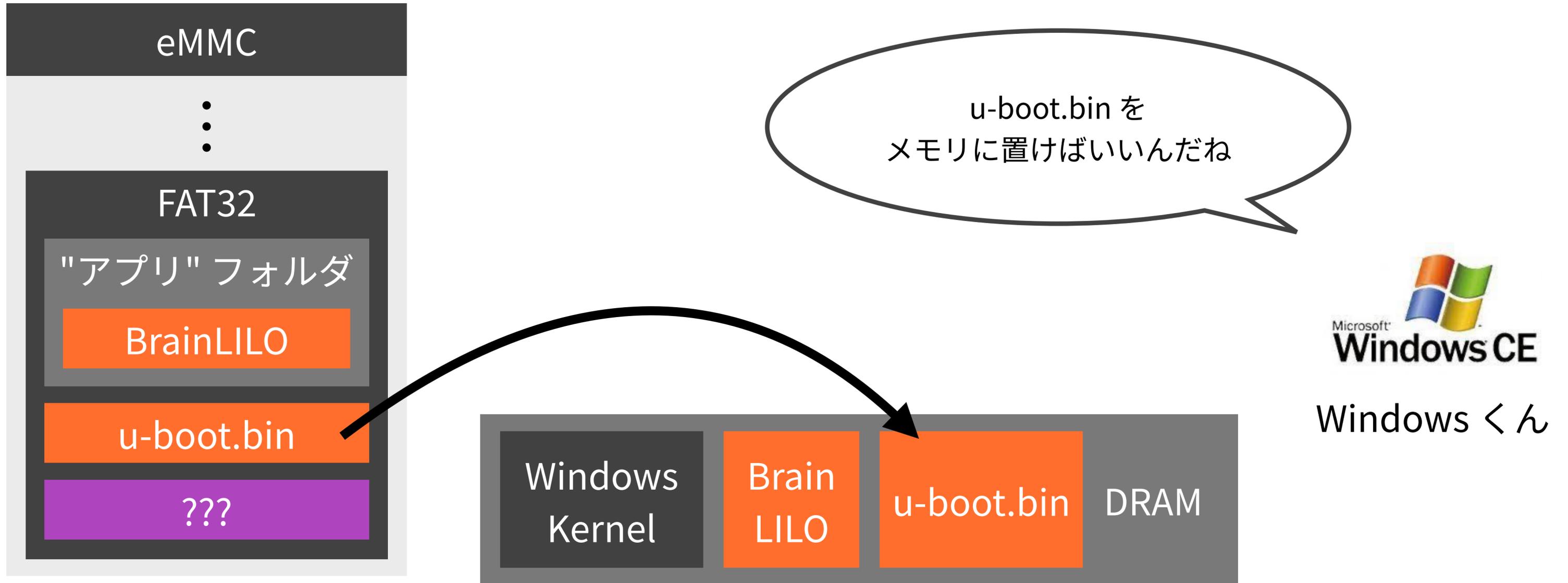
2021年発売の新モデル～

- NXP i.MX7ULP (armv7-a, armv7e-m) + 128 MiB DRAM
- μ ITRON ベース RTOS

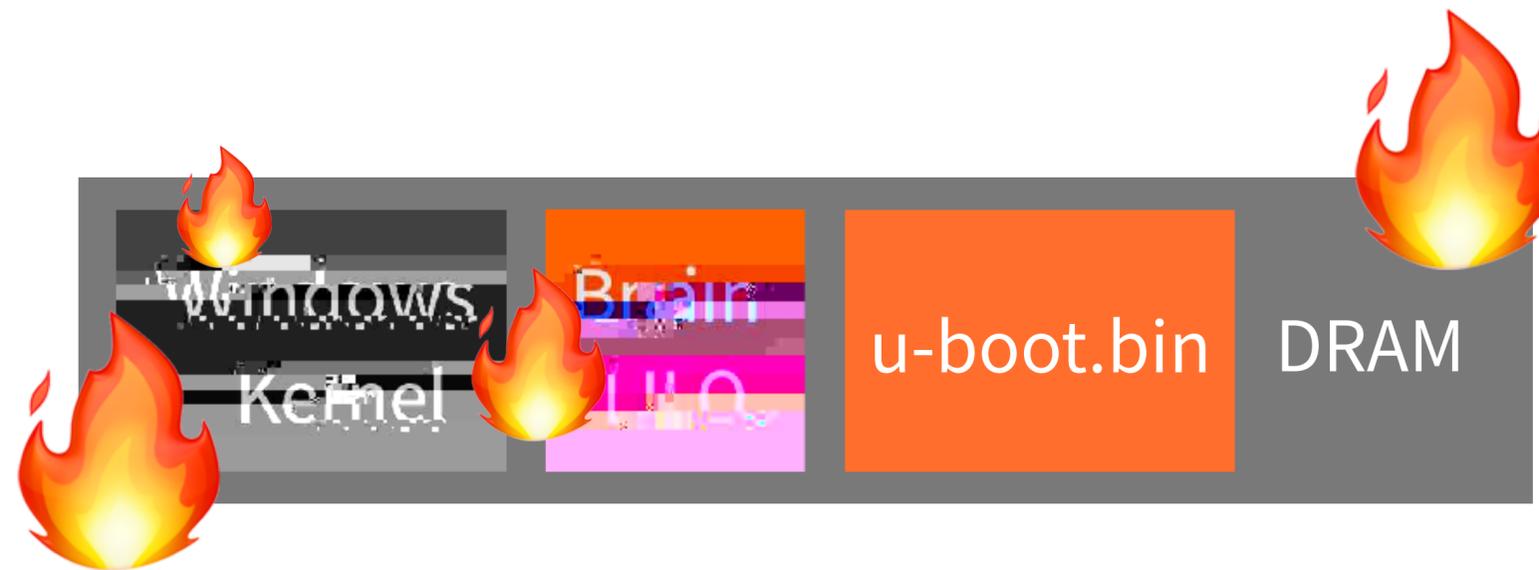
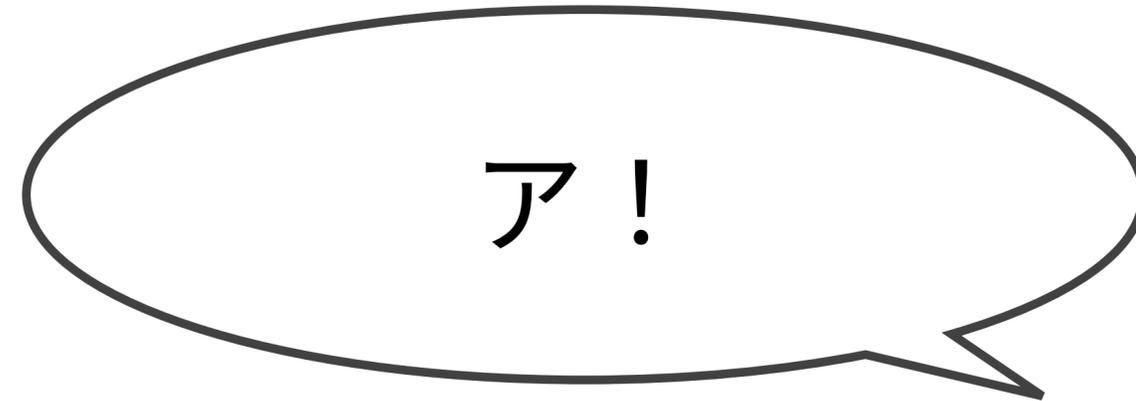
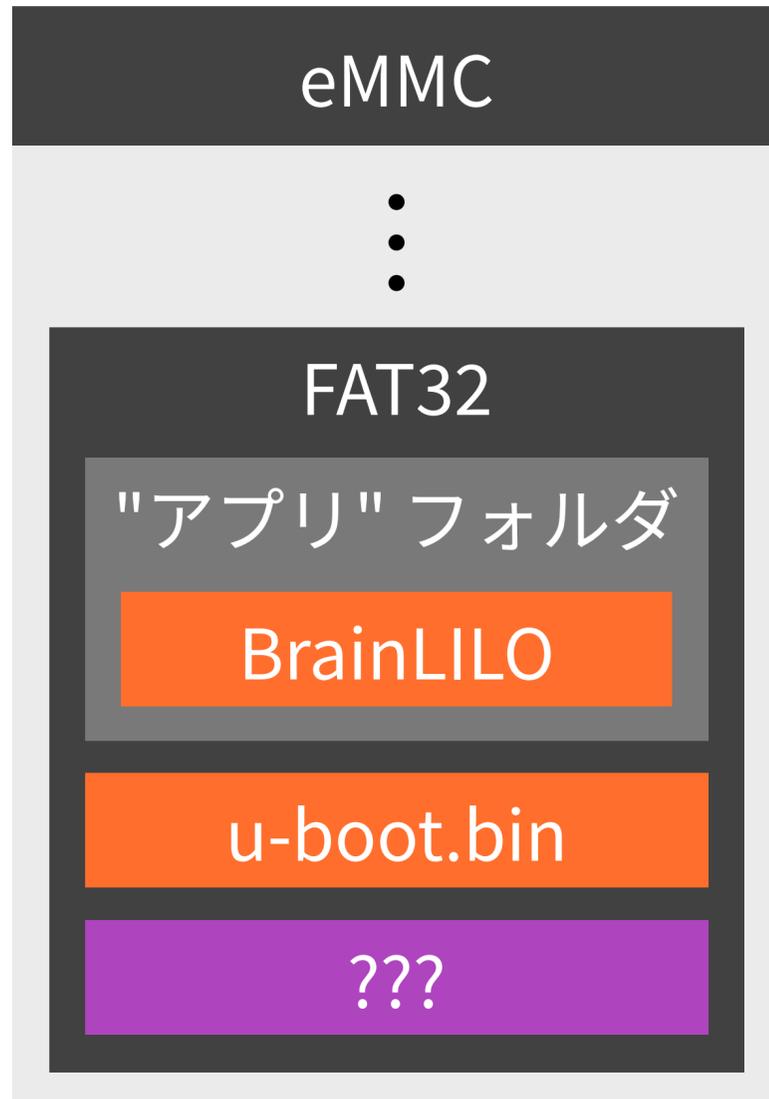




"アプリ" フォルダに入れられた怪しげなアプリ BrainLILO をメニューから実行すると…

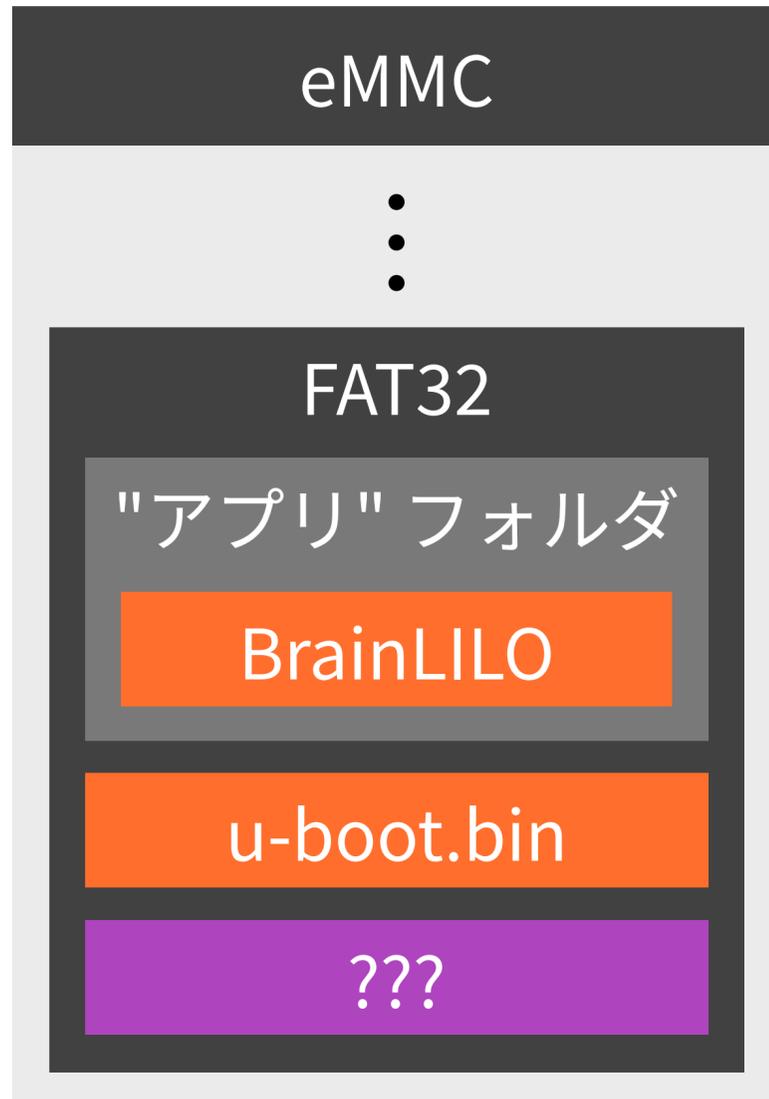


ブートローダー U-Boot (u-boot.bin) が DRAM にロードされ…

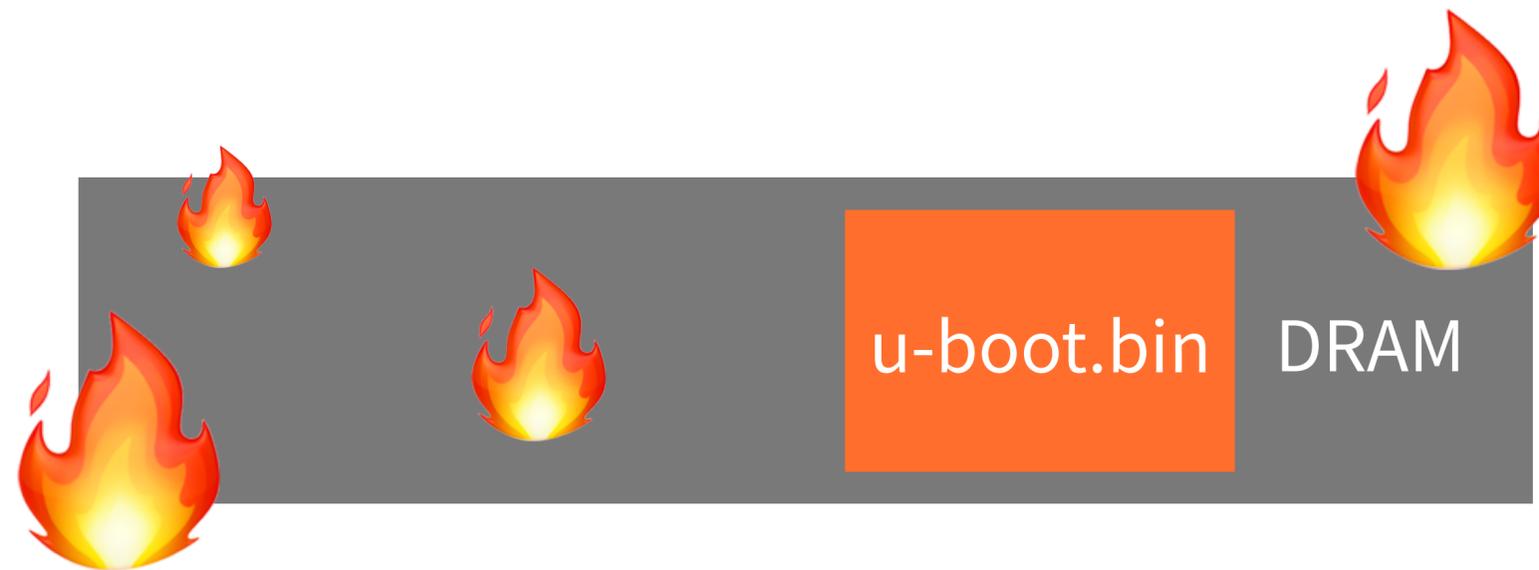


Windows くん

MMU (Memory Management Unit) の無効化 etc. が行われ…

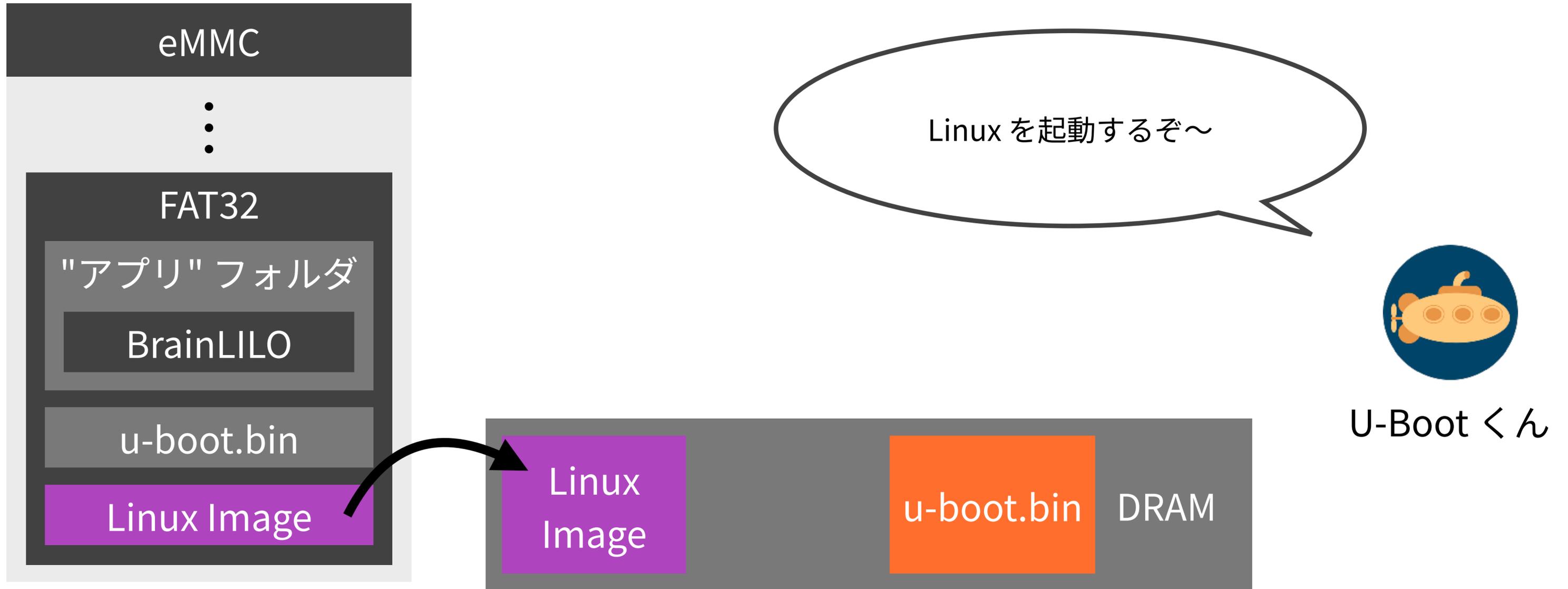


さようなら...

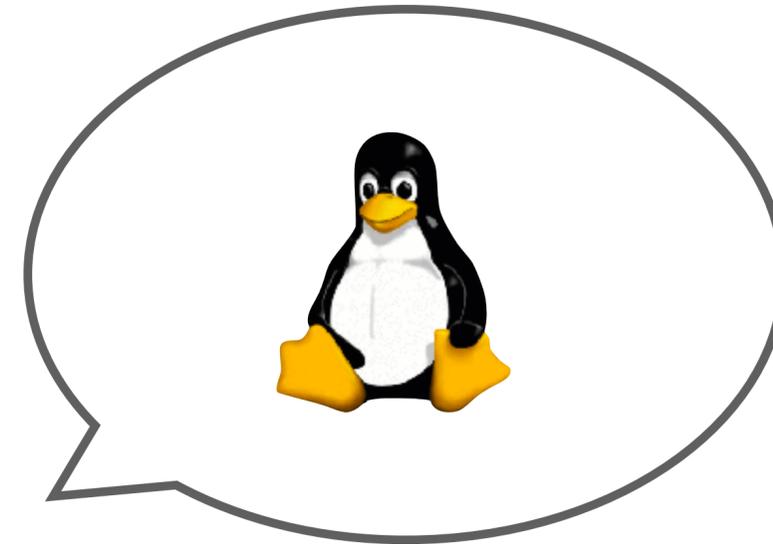


Windows くん

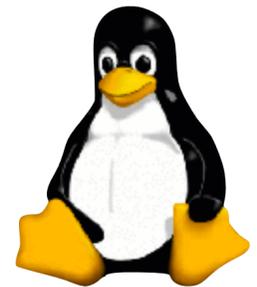
U-Boot へジャンプする



U-Boot が改めてハードの初期化を行ったあと
Linux をメモリに置いてジャンプ



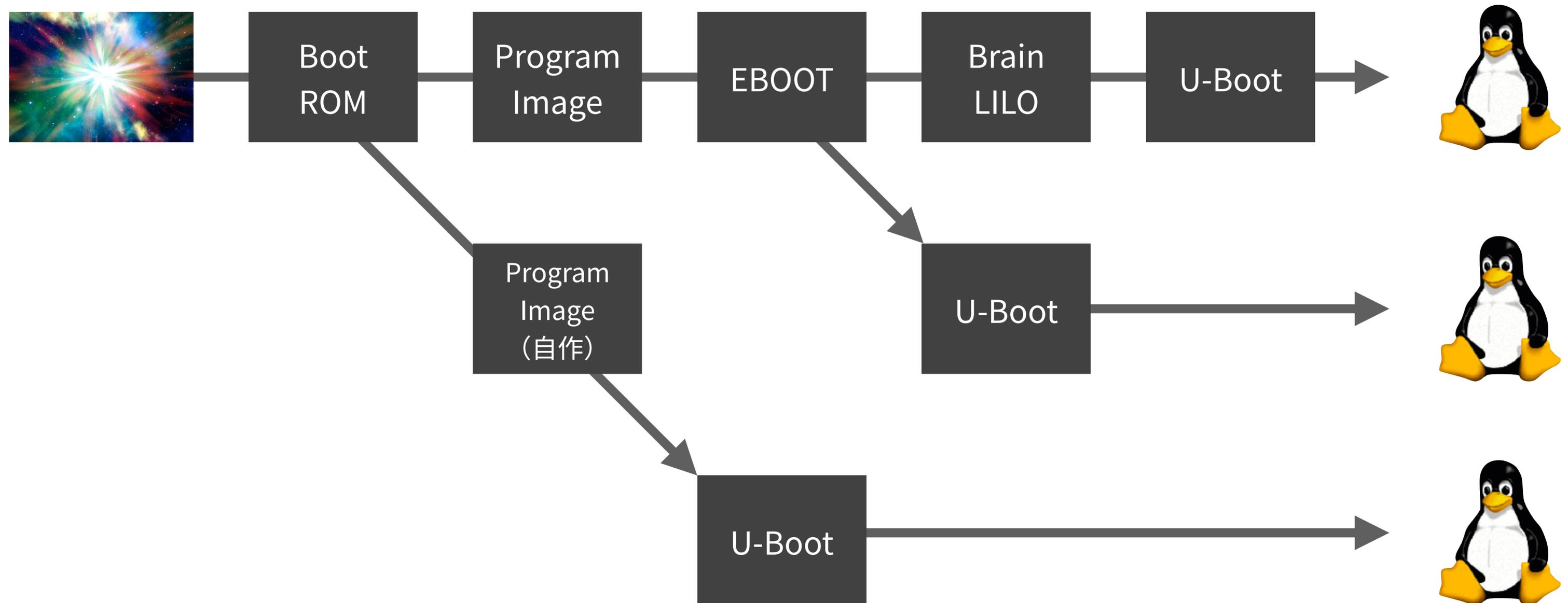
こうしてめでたく Linux がブートする



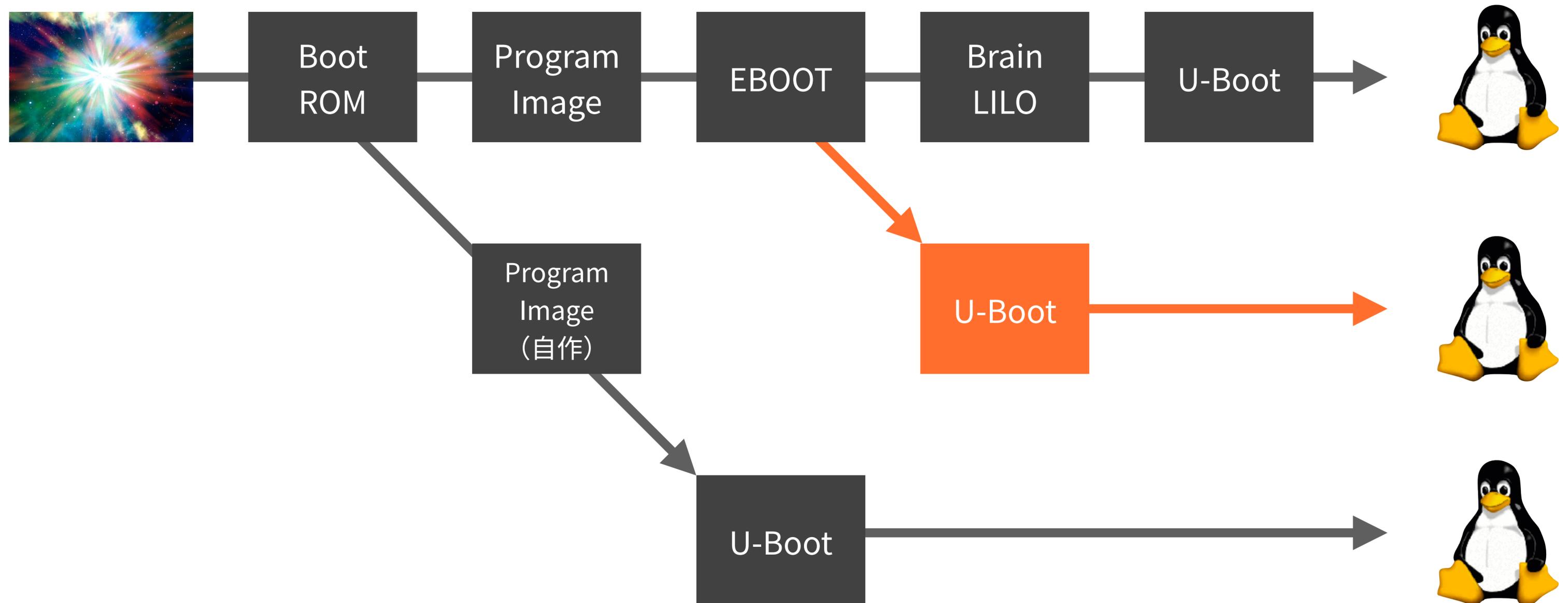
Windows 以降の流れのおさらい

3. Linux ブートのさまざまな方法

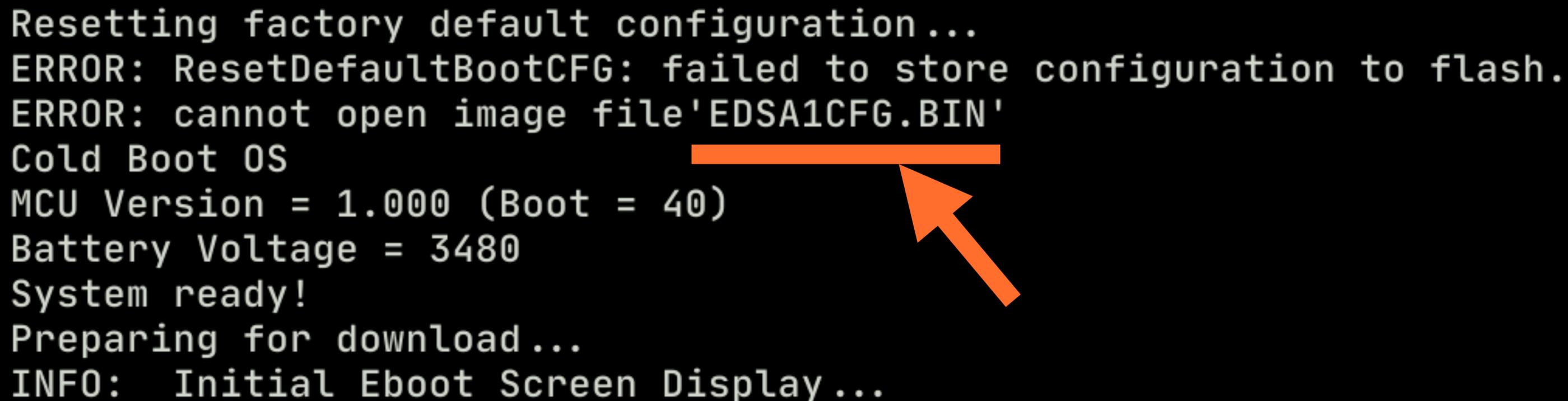
実は Linux のブートに至る道は1つではない



3.1. EBOOT → U-Boot とは？



```
Resetting factory default configuration...
ERROR: ResetDefaultBootCFG: failed to store configuration to flash.
ERROR: cannot open image file 'EDSA1CFG.BIN'
Cold Boot OS
MCU Version = 1.000 (Boot = 40)
Battery Voltage = 3480
System ready!
Preparing for download...
INFO: Initial Eboot Screen Display...
```



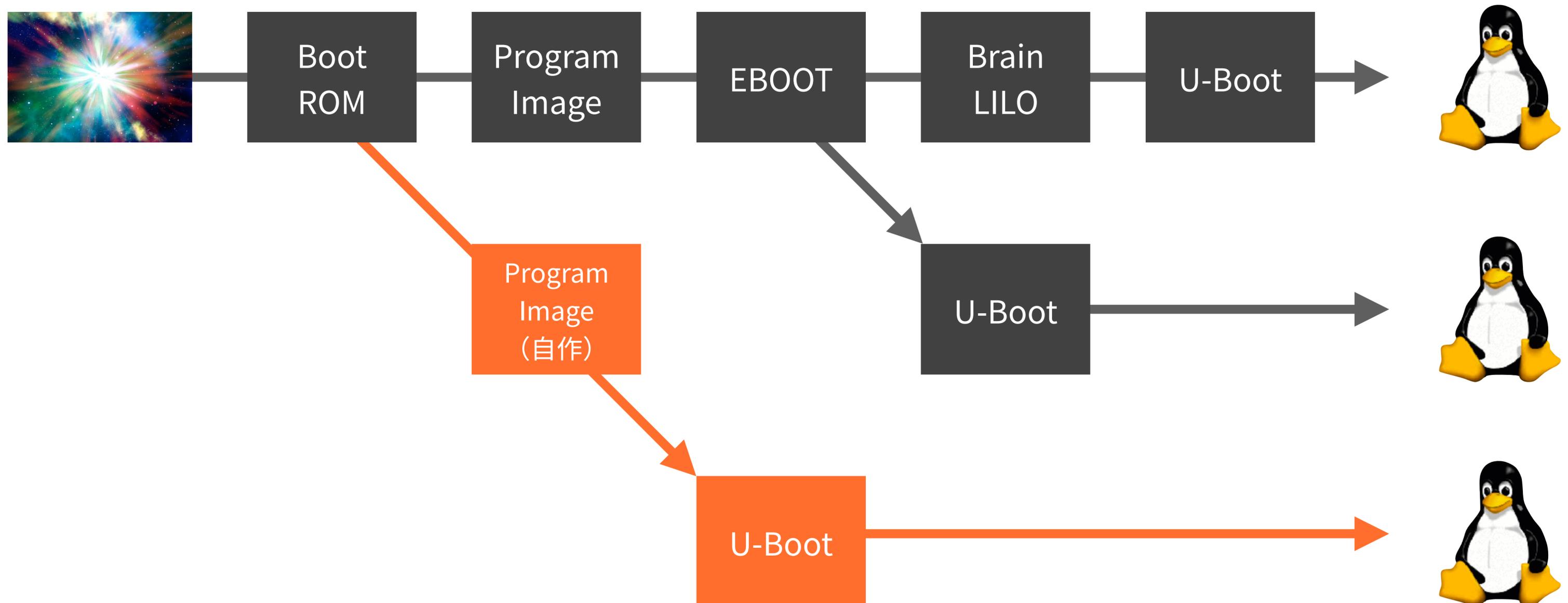
PW-SH1 の EBOOT のログ (一部)

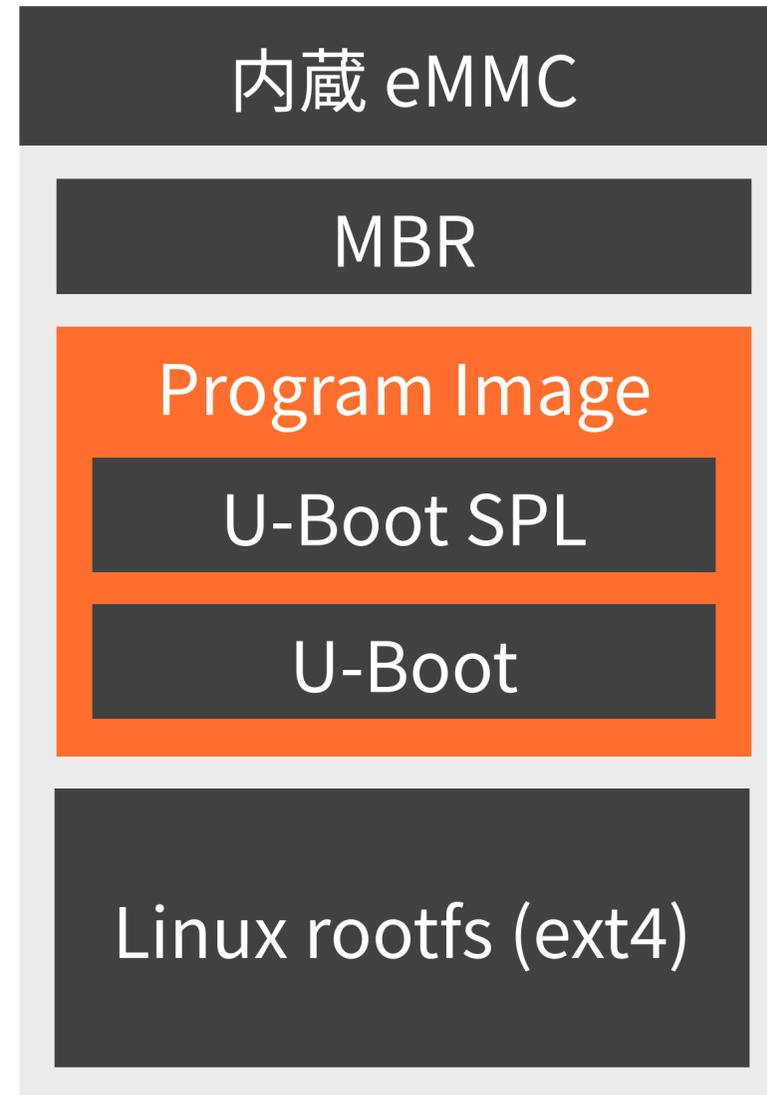
一部の機種では eMMC の NK image を読む前に
SD の NK image を読みに行く仕様がある (工場では使っていると推測)



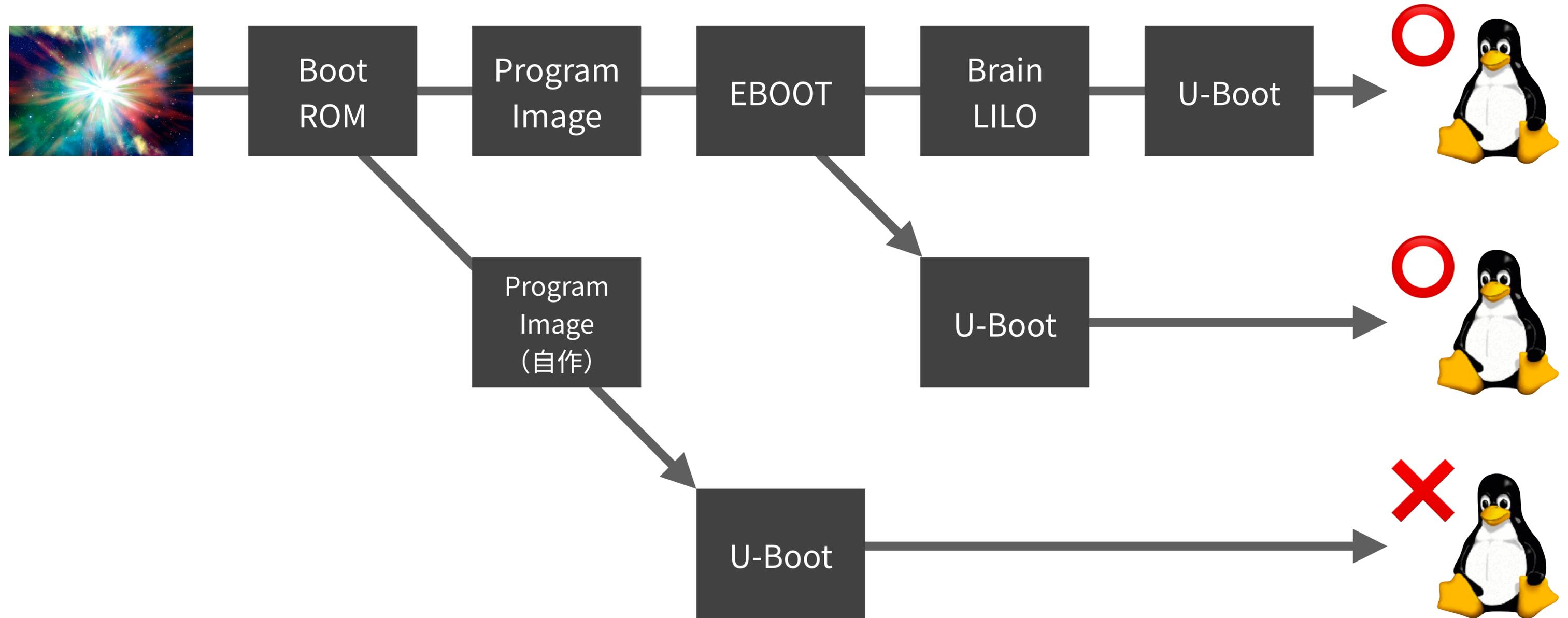
なら、NK image のフリをした U-Boot を置けばいいんじゃない？
というのが EBOOT → U-Boot チェーンブートのテクニック

3.2. Boot ROM → 自作 Program Image → U-Boot とは？





eMMC の本来 EBOOT がある箇所に U-Boot 入りの Program Image を上書きして
順当に Linux を起こす手法



現在実装があるのは EBOOT 経由 と BrainLILO のみ・Program Image 自作は未着手

4. Program Image 自作の展望

Program Image 自作ができたなら何が嬉しいのか？

- **内部の eMMC に Linux をインストールできる**
 - SD よりもディスク I/O が速くなる
- SD を外部ストレージにできる
- SDIO を使って Wi-Fi ドングルを接続できる
 - Linux にドライバがあって技適が通っているモジュールがある！
- データピンをただの GPIO にして好きな回路を接続できる
 - もはや開発ボードかな？

5. まとめ

まとめ

- SHARP Brain で Linux を起動するにはいくつか方法がある
 - Windows から BrainLILO 経由で U-Boot を起こす
 - EBOOT (Windows のブートローダー) から U-Boot を起こす
 - Boot ROM から U-Boot を起こす
- Boot ROM からの起動は実装されていない
 - 実装できた暁にはすごく楽しい世界が待ってそう
- 乞うご期待



Brain Hackers