

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 6 部門第 3 区分

【発行日】平成29年1月12日 (2017.1.12)

【公表番号】特表2014-533395(P2014-533395A)

【公表日】平成26年12月11日 (2014.12.11)

【年通号数】公開・登録公報2014-068

【出願番号】特願2014-533790(P2014-533790)

【国際特許分類】

G 0 6 F 21/57 (2013.01)

【 F I 】

G 0 6 F 21/00 1 5 7 A

【誤訳訂正書】

【提出日】平成28年10月28日 (2016.10.28)

【誤訳訂正 1】

【訂正対象書類名】明細書

【訂正対象項目名】0 0 4 1

【訂正方法】変更

【訂正の内容】

【 0 0 4 1 】

図 1 はこの発明の一実施例による、非安全なランタイム環境 1 0 0 及び安全なランタイム環境 2 0 0 を有すると共に、非安全なランタイム環境 1 0 0 において及び安全なランタイム環境 2 0 0 において部分的に各ケースで実行されるアプリケーション・フィルター・インターフェース Trustlet コネクタ (TLC: Translet Connector) を有する ARM アーキテクチャを有するマイクロプロセッサ・システムを示している。非安全なランタイム環境 1 0 0 は通常のオペレーティング・システム HLOS によって制御される。安全なランタイム環境 2 0 0 は安全保障のオペレーティング・システム MobiCore によって制御される。オペレーティング・システム・レベルでの非安全なランタイム環境 1 0 0 及び安全なランタイム環境 2 0 0 間のアクセスは、安全保障のドライバ MobiCore ドライバを用いることによって行われる。例えば、支払取引アプリケーションのアプリケーション APP の大部分の APP-S は、安全なランタイム環境 2 0 0 で実行可能な方法で安全保障のオペレーティング・システム MobiCore 下で実行される。例えば、支払取引アプリケーションのアプリケーション APP の残部の APP-N は、非安全なランタイム環境 1 0 0 で実行可能な方法で通常のオペレーティング・システム HLOS 下で実行される。この発明によるアプリケーション・フィルター・インターフェース TLC (Translet Connector) は、安全なランタイム環境 2 0 0 で実行可能な方法で安全保障のオペレーティング・システム MobiCore 下で実行されるアプリケーション APP の部分 APP-S と、非安全なランタイム環境 1 0 0 で実行可能な方法で通常のオペレーティング・システム HLOS 下で実行されるアプリケーション APP の部分 APP-N との間の直接のアクセスを、直接にアプリケーション・レベルで可能にする。周辺構造体 PER、例えば、タッチ・スクリーン表示装置用のドライバは図 1 に従って通常のオペレーティング・システム HLOS 下で従来の方法で実行されると共に、せいぜい安全保障のドライバ MobiCore ドライバを介して安全なランタイム環境 2 0 0 と通信することができる。安全保障のオペレーティング・システム MobiCore の下で実行される新規な軽減したドライバ PER-S には、せいぜい安全保障のドライバ MobiCore ドライバを介して非安全なランタイム環境 1 0 0 から達することができる。非安全なランタイム環境 1 0 0 では、周辺ドライバ PER はリナックス (登録商標) (Linux) I2C ドライバで制御される方法で I2C バス・システムを介して通常のオペレーティング・システム HLOS と通信する。安全なランタイム環境 2 0 0 では、軽減した周辺ドライバ PER-S は I2C ドライバによって制御される方法で安全なランタイム環境 2 0 0 で実行される I2C バス・システムを介して安全保障のオペレーティング・システム

MobiCoreと通信する。周辺ドライバPER及びPER-Sの間の通信は、MobiCoreドライバを用いることによってせいぜいオペレーティング・システム・レベルで行うことができる。

【誤訳訂正 2】

【訂正対象書類名】特許請求の範囲

【訂正対象項目名】全文

【訂正方法】変更

【訂正の内容】

【特許請求の範囲】

【請求項 1】

携帯端末で実行可能な又は実行されると共に、

非安全なランタイム環境（100）を発生し、維持するために設計された通常のオペレーティング・システム（HLOS）と、

安全なランタイム環境（200）を発生し、維持するために設計された安全保障のオペレーティング・システム（MobiCore）と、

前記通常のオペレーティング・システム（HLOS）及び前記安全保障のオペレーティング・システム（MobiCore）の間のオペレーティング・システム・インターフェース（MobiCore ドライバ）であって、前記非安全なランタイム環境（100）及び前記安全なランタイム環境（200）の間の通信をオペレーティング・システム・レベルで安全に制御すべく設計された前記オペレーティング・システム・インターフェースと、を具備し、

前記非安全なランタイム環境（100）及び前記安全なランタイム環境（200）の間の通信を前記オペレーティング・システム・レベルと異なるレベルで安全に制御すべく設計された少なくとも1つのフィルター・インターフェースであって、前記非安全なランタイム環境（100）及び前記安全なランタイム環境（200）の間の通信をアプリケーション・レベルで安全に制御すべく設計されたアプリケーション・フィルター・インターフェース（TLC）である、前記フィルター・インターフェースによって特徴付けられてなるマイクロプロセッサ・システム。

【請求項 2】

請求項 1 に記載のマイクロプロセッサ・システムにおいて、前記設けられたフィルター・インターフェースは、前記非安全なランタイム環境（100）及び前記安全なランタイム環境（200）の間の通信をハードウェア・レベルで安全に制御すべく設計されたハードウェア・フィルター・インターフェースである前記マイクロプロセッサ・システム。

【請求項 3】

請求項 2 に記載のマイクロプロセッサ・システムにおいて、前記ハードウェア・レベルの前記制御は、バス・システム（I2C）を介した制御として行われる前記マイクロプロセッサ・システム。

【請求項 4】

請求項 2 又は 3 に記載のマイクロプロセッサ・システムにおいて、

前記携帯端末の周辺構造体用の少なくとも1つのドライバ（PER）であって、前記通常のオペレーティング・システム（HLOS）によって駆動可能であると共に、前記非安全なランタイム環境（100）にて実行可能である前記少なくとも1つのドライバを更に具備し、

前記周辺構造体用の好ましくは軽減したドライバ（PER-S）であって、前記安全保障のオペレーティング・システム（MobiCore）によって駆動可能であり、前記安全なランタイム環境（200）にて実行可能で、前記非安全なランタイム環境（100）にて実行可能な前記ドライバ（PER）の機能性のサブセットのみを好ましくは有してなる前記ドライバによって特徴付けられると共に、

前記ハードウェア・フィルター・インターフェースが、前記非安全なランタイム環境（100）にて実行可能な周辺構造体用の前記ドライバ（PER）と、前記安全なランタイム環境（200）にて実行可能な前記周辺構造体用の前記好ましくは軽減したドライバ（PER-S）との間の通信を前記ハードウェア・レベルで安全に制御すべく設計されてなること

を特徴とする前記マイクロプロセッサ・システム。

【請求項 5】

請求項 4 に記載のマイクロプロセッサ・システムにおいて、安全保障との関連性に関して周辺構造体用の前記ドライバ（PER、PER-S）に向けられたアクセスを検査し、前記アクセスが安全保障と関連性があるものとして同定される場合、前記安全なランタイム環境（200）での前記好ましくは軽減したドライバ（PER-S）に前記アクセスを運び、かつ、前記アクセスが安全保障と関連性がないものとして同定される場合、前記非安全なランタイム環境（100）での前記ドライバ（PER）に前記アクセスを運ぶべく、前記ハードウェア・フィルター・インターフェースが設計されている前記マイクロプロセッサ・システム。

【請求項 6】

請求項 1 に記載のマイクロプロセッサ・システムにおいて、少なくとも 1 つのアプリケーション（APP）を更に具備し、

該アプリケーション（APP）は前記通常のオペレーティング・システム（HLOS）によって少なくとも部分的に（APP-N）駆動可能であると共に、前記非安全なランタイム環境（100）にて実行可能であり、かつ、前記安全保障のオペレーティング・システム（Mobi Core）によって少なくとも部分的に（APP-S）駆動可能であると共に、前記安全なランタイム環境（200）にて実行可能であることを特徴とすると共に、

前記非安全なランタイム環境（100）で実行可能な前記少なくとも部分的なアプリケーション（APP-N）と、前記安全なランタイム環境（200）で実行可能な前記少なくとも部分的なアプリケーション（APP-S）との間の通信を前記アプリケーション・レベルで安全に制御すべく、前記アプリケーション・フィルター・インターフェース（TLC）が設計されていることを特徴とする前記マイクロプロセッサ・システム。

【請求項 7】

請求項 6 に記載のマイクロプロセッサ・システムにおいて、安全保障との関連性に関して前記アプリケーション（APP）に向けられたアクセスを検査し、前記アクセスが安全保障と関連性があるものとして同定される場合、前記安全なランタイム環境（200）での前記少なくとも部分的なアプリケーション（APP-S）に前記アクセスを運び、かつ、前記アクセスが安全保障と関連性がないものとして同定される場合、前記非安全なランタイム環境（100）での前記少なくとも部分的なアプリケーション（APP-N）に前記アクセスを運ぶべく、前記アプリケーション・フィルター・インターフェース（TLC）が設計されている前記マイクロプロセッサ・システム。

【請求項 8】

請求項 1 から請求項 7 の何れか一項に記載のマイクロプロセッサ・システムにおいて、前記非安全なランタイム環境（100）から前記安全なランタイム環境（200）への又は/及び前記安全なランタイム環境（200）から非安全なランタイム環境（100）への前記フィルター・インターフェースを介して行われるどんなアクセスのときでも、前記マイクロプロセッサのユーザに知覚可能なユーザ・メッセージがユーザ出力装置によって出力されるようにして、前記フィルター・インターフェースが前記ユーザ出力装置に結合されている前記マイクロプロセッサ・システム。

【請求項 9】

請求項 8 に記載のマイクロプロセッサ・システムにおいて、一方で、前記非安全なランタイム環境（100）から前記安全なランタイム環境（200）への、及び他方で、前記安全なランタイム環境（200）から非安全なランタイム環境（100）へのアクセスに対して、前記ユーザに区別可能な異なるユーザ出力が出力されるようにして、前記フィルター・インターフェースが前記ユーザ出力装置に結合されている前記マイクロプロセッサ・システム。