(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5897217号
(P5897217)
(45)発行日　平成28年3月30日(2016.3.30)　(24)登録日　平成28年3月11日(2016.3.11)

(51)Int.Cl.　　F I
*G06F 21/60 (2013.01)*　　G06F 21/60 360
*H04M 1/66 (2006.01)*　　H04M 1/66

請求項の数 26　(全 16 頁)

(21)出願番号　特願2015-526770 (P2015-526770)
(86)(22)出願日　平成25年9月10日 (2013.9.10)
(65)公表番号　特表2015-529910 (P2015-529910A)
(43)公表日　平成27年10月8日 (2015.10.8)
(86)国際出願番号　PCT/US2013/058863
(87)国際公開番号　WO2014/043056
(87)国際公開日　平成26年3月20日 (2014.3.20)
審査請求日　平成27年2月10日 (2015.2.10)
(31)優先権主張番号　13/611,862
(32)優先日　平成24年9月12日 (2012.9.12)
(33)優先権主張国　米国(US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　プラカシュ、ギャン
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

最終頁に続く

(54)【発明の名称】センサデータセキュリティを有するモバイルプラットフォーム

(57)【特許請求の範囲】
【請求項１】
コンテキストセンサデータをセキュアに提供する方法であって、
コンテキストデータを提供する１または複数のセンサを構成する段階であり、前記コンテキストデータはモバイルデバイスに関連する、段階と、
アプリケーションプログラミングインターフェース（ＡＰＩ）をセンサドライバに提供する段階であり、前記センサドライバは前記１または複数のセンサを制御する、段階と、
前記モバイルデバイス上で動作する信頼できる実行環境（ＴＥＥ）を提供する段階であり、前記ＴＥＥは、前記センサドライバをホストし、前記センサドライバ及び前記１または複数のセンサへのコントロールアクセス及びデータアクセスを制限する、段階と、
前記ＡＰＩを通じて前記コンテキストデータの要求を生成する段階であり、アプリケーションにより生成された前記要求は前記モバイルデバイスに関連する、段階と、
前記アプリケーションにより、前記ＡＰＩを通じて、要求された前記コンテキストデータおよび正当性インジケータを受信する段階と、
前記アプリケーションにより、要求された前記コンテキストデータを、前記正当性インジケータに基づいて検証する段階と、
前記アプリケーションに関連するポリシーを、検証された前記コンテキストデータに基づいて調整する段階と、
を備える方法。
【請求項２】

前記正当性インジケータは、デジタル署名を含む、請求項１に記載の方法。
【請求項３】
前記センサドライバにより、要求された前記コンテキストデータを暗号化する段階をさらに備える、請求項１に記載の方法。
【請求項４】
前記センサは、加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、および周辺光センサのうちの少なくとも１つである、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記コンテキストデータは、デバイス位置、デバイス所在地、デバイスの動き、ユーザ識別情報、温度、およびノイズレベルのうちの少なくとも１つである、請求項１から３のいずれか一項に記載の方法。
【請求項６】
前記ポリシーは、モバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、およびメディア視聴ポリシーのペアレンタルコントロールのうちの少なくとも１つである、請求項１から３のいずれか一項に記載の方法。
【請求項７】
移動体通信のためのデバイスであって、
コンテキストデータを提供する１または複数のセンサであり、前記コンテキストデータはデバイスに関連する、１または複数のセンサと、
前記コンテキストデータに対する複数の要求を受信し、前記複数の要求に応じて、前記コンテキストデータおよび関連する正当性インジケータを提供するセキュアセンサドライバモジュールと、
前記デバイス上で動作する信頼できる実行環境（ＴＥＥ）であり、前記ＴＥＥは、前記セキュアセンサドライバモジュールをホストし、前記セキュアセンサドライバモジュールおよび前記１または複数のセンサへのコントロールアクセスおよびデータアクセスを制限する、ＴＥＥと、
前記複数の要求を生成し、前記コンテキストデータを受信し、前記正当性インジケータに基づいて前記コンテキストデータを検証し、検証された前記コンテキストデータに基づいてアプリケーションに関連するポリシーを調整する１または複数のアプリケーションモジュールと、
を備えるデバイス。
【請求項８】
前記正当性インジケータは、デジタル署名を含む、請求項７に記載のデバイス。
【請求項９】
前記セキュアセンサドライバモジュールは、さらに、前記コンテキストデータを暗号化する、請求項７に記載のデバイス。
【請求項１０】
前記１または複数のセンサのそれぞれに連結されるセンサ周辺ハブをさらに備え、前記センサ周辺ハブは、前記ＴＥＥおよび前記セキュアセンサドライバモジュールを格納するファームウェアを提供するプロセッサおよびメモリを含む、請求項７に記載のデバイス。
【請求項１１】
前記センサは、加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、および周辺光センサのうちの少なくとも１つである、請求項７から１０のいずれか一項に記載のデバイス。
【請求項１２】
前記コンテキストデータは、デバイス位置、デバイス所在地、デバイスの動き、ユーザ識別情報、温度、およびノイズレベルのうちの少なくとも１つである、請求項７から１０のいずれか一項に記載のデバイス。
【請求項１３】

前記ポリシーは、モバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、およびメディア視聴ポリシーのペアレンタルコントロールのうちの少なくとも１つである、請求項７から１０のいずれか一項に記載のデバイス。

【請求項１４】

コンテキストデータを提供する１または複数のセンサを構成する手順であり、前記コンテキストデータはモバイルデバイスに関連する、手順と、

アプリケーションプログラミングインターフェース（ＡＰＩ）をセンサドライバに提供する手順であり、前記センサドライバは前記１または複数のセンサを制御する、手順と、

前記モバイルデバイス上で動作する信頼できる実行環境（ＴＥＥ）を提供する手順であり、前記ＴＥＥは、前記センサドライバをホストし、前記センサドライバ及び前記１または複数のセンサへのコントロールアクセス及びデータアクセスを制限する、手順と、

前記ＡＰＩを通じて前記コンテキストデータの要求を生成する手順であり、アプリケーションにより生成された前記要求は前記モバイルデバイスに関連する、手順と、

前記アプリケーションにより、前記ＡＰＩを通じて、要求された前記コンテキストデータおよび正当性インジケータを受信する手順と、

前記アプリケーションにより、要求された前記コンテキストデータを、前記正当性インジケータに基づいて検証する手順と、

前記アプリケーションに関連するポリシーを、検証された前記コンテキストデータに基づいて調整する手順と、

をコンピュータに実行させるプログラム。

【請求項１５】

前記正当性インジケータは、デジタル署名を含む、請求項１４に記載のプログラム。

【請求項１６】

前記センサドライバにより、要求された前記コンテキストデータを暗号化する手順をさらにコンピュータに実行させる、請求項１４に記載のプログラム。

【請求項１７】

前記センサは、加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、および周辺光センサのうちの少なくとも１つである、請求項１４から１６のいずれか一項に記載のプログラム。

【請求項１８】

前記コンテキストデータは、デバイス位置、デバイス所在地、デバイスの動き、ユーザ識別情報、温度、およびノイズレベルのうちの少なくとも１つである、請求項１４から１６のいずれか一項に記載のプログラム。

【請求項１９】

前記ポリシーは、モバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、およびメディア視聴ポリシーのペアレンタルコントロールのうちの少なくとも１つである、請求項１４から１６のいずれか一項に記載のプログラム。

【請求項２０】

モバイル通信プラットフォームであって、

プロセッサと、

前記プロセッサに連結されたメモリと、

前記プロセッサに連結された入出力システム（Ｉ／Ｏシステム）と、

前記Ｉ／Ｏシステムに連結されたユーザインターフェースと、

前記プロセッサに連結された１または複数のセンサであり、前記１または複数のセンサは、前記モバイル通信プラットフォームに関連するコンテキストデータを提供する、センサと、

前記コンテキストデータに対する複数の要求を受信し、前記複数の要求に応じて、前記コンテキストデータおよび関連するデジタル署名を提供するセキュアセンサドライバモジュールと、

前記モバイル通信プラットフォーム上で動作する信頼できる実行環境（ＴＥＥ）であり、前記ＴＥＥは、前記セキュアセンサドライバモジュールをホストし、前記セキュアセンサドライバモジュールおよび前記１または複数のセンサへのコントロールアクセスおよびデータアクセスを制限する、ＴＥＥと、

前記複数の要求を生成し、前記コンテキストデータを受信し、前記デジタル署名に基づいて前記コンテキストデータを検証し、検証された前記コンテキストデータに基づいてアプリケーションに関連するポリシーを調整する１または複数のアプリケーションモジュールと、

を備えるモバイル通信プラットフォーム。

【請求項２１】

前記センサは、加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、および周辺光センサのうちの少なくとも１つである、請求項２０に記載のモバイル通信プラットフォーム。

【請求項２２】

前記コンテキストデータは、プラットフォーム位置、プラットフォーム所在地、プラットフォームの動き、ユーザ識別情報、温度、およびノイズレベルのうちの少なくとも１つである、請求項２０に記載のモバイル通信プラットフォーム。

【請求項２３】

前記ポリシーは、モバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、およびメディア視聴ポリシーのペアレンタルコントロールのうちの少なくとも１つである、請求項２０に記載のモバイル通信プラットフォーム。

【請求項２４】

前記プラットフォームは、スマートフォン、ラップトップコンピューティングデバイス、またはタブレットのうちの１つである、請求項２０に記載のモバイル通信プラットフォーム。

【請求項２５】

それぞれ無線ネットワークを介して通信する複数の前記プラットフォームをさらに備える、請求項２０から２４のいずれか一項に記載のモバイル通信プラットフォーム。

【請求項２６】

前記ユーザインターフェースは、タッチスクリーンおよびキーボードのうちの少なくとも１つである、請求項２０に記載のモバイル通信プラットフォーム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、センサデータセキュリティを有するモバイルプラットフォームに関し、より詳細には、モバイルプラットフォーム上のコンテキストアウェアセンサデータの保護及び検証のためのシステム及び方法に関する。

【背景技術】

【０００２】

例えばスマートフォンのようなモバイルデバイス及びプラットフォームは、デバイスを取り囲む環境に関する情報から利益を得る電子商取引（ｅコマース）及び他のアプリケーションにおいてますます使用されている。この情報は、場合によっては、コンテキストデータとして参照される。デバイスに関連するセンサにより集められ得るコンテキストデータは、概して、本質的に機密であると考えられ、セキュリティ及びプライバシーに関する問題の増加に伴い、モバイルデバイスのユーザはこのコンテキストデータを認証されていないエンティティに利用可能にしたがらない。

【０００３】

一般的に、暗号化ベースのセキュアなチャネルは、モバイルデバイス上で動作するオペレーティングシステム又はアプリケーションとサーバのような遠隔エンティティの間で無線ネットワークを介して確立される。しかし、この方法は、「中間者（man-in-the-middl

e）」攻撃として知られるタイプの攻撃に対して脆弱である。ここで、悪意のあるソフトウェア（マルウェア）は、デバイスの制御を得て、暗号化される前にコンテキストデータへのアクセスを取得する。マルウェアは、コンテキストデータを認証されていないエンティティにリダイレクトし得る（場合によっては、スヌーピングと呼ばれる）又は認証されたアプリケーション又は意図する宛先への送信に先立ってコンテキストデータを変更し得る（場合によっては、スプーフィングと呼ばれる）。場合によっては、変更（又は偽造）データが、セキュリティ制限を回避するために用いられ得る。

【図面の簡単な説明】

【０００４】

請求される主題の実施形態の特徴および利点は、以下の発明を実施するための形態が進むにつれて、また図面を参照することで、明らかになるであろう。ここで、次の図面において、同じ参照番号は同様の部分を示す。

【図１】本開示に一致する１つの例示的な実施形態のトップレベルシステムダイヤグラムを示す。

【図２】本開示に一致する１つの例示的な実施形態のブロックダイヤグラムを示す。

【図３】本開示に一致する別の例示的な実施形態のブロックダイヤグラムを示す。

【図４】ネットワークにおける本開示の例示的な実施形態に一致するプラットフォームを示すシステムダイヤグラムを示す。

【図５】本開示に一致する別の例示的な実施形態の動作のフローチャートを示す。　以下の発明を実施するための形態は、例示的な実施形態を参照して進むが、それらの多くの代替、修正、及び変形が当業者に明らかであろう。

【発明を実施するための形態】

【０００５】

概して、本開示は、例えばスマートフォン、タブレット、及びラップトップのようなモバイルプラットフォーム上でコンテキストアウェアセンサデータを保護及び検証するためのデバイス、システム、及び方法を提供する。コンテキストデータは、コンテキストアウェアモバイルアプリケーション、例えばコンテキストデータに基づいてポリシー設定を調整し得るｅコマースアプリケーションにセキュアに提供されてよい。信頼できる実行環境（ＴＥＥ）は、センサ及びそれらが生成するコンテキストデータにアクセスするセキュアドライバをホストするために提供されてよい。ＴＥＥは、ＯＳレベル及びより高レベルのアプリケーションで実行するＯＳカーネル、他のモジュール及びドライバを含むＴＥＥの範囲外のエンティティからのセンサドライバ及びセンサの両方へのコントロールアクセス及びデータアクセスを制限してよい。セキュアドライバは、不正及び／又は非セキュアなアプリケーションをコンテキストセンサデータの取得から防ぐ。セキュアドライバは、デジタル署名又は他の暗号化技術の使用を通じて認証された及び／又はセキュアなアプリケーションに配信されるコンテキストデータの有効性の検証を提供してもよい。コンテキストアウェアセンサは、モバイルプラットフォームに関連する位置又は移動情報を提供するグローバルポジショニングシステム（ＧＰＳ）又は他のセンサを含んでよい。コンテキストアウェアセンサの他の例は、カメラ、マイク、又はモバイルプラットフォームを取り囲む環境に関する情報を提供し得るあらゆる他のタイプの適切な環境センサを含んでよい。

【０００６】

記載された実施形態のモバイルプラットフォームは、概して、無線ネットワークを介して無線通信可能であってよく、以下の用語の定義が提供される。

【０００７】

本明細書で使用されるように用語アクセスポイント（ＡＰ）は、局（ＳＴＡ）の機能を有し、関連するＳＴＡに対して無線媒体（ＷＭ）を介して配布サービスへのアクセスを提供するあらゆるエンティティとして定義される。

【０００８】

本明細書で使用されるように用語パーソナル基本サービスセットコントロールポイント（ＰＣＰ）は、ミリ波（ｍｍ波）ネットワークのコントロールポイントとして動作するＳ

ＴＡとして定義される。

【０００９】

本明細書で使用されるように用語無線ネットワークコントローラは、ＰＣＰとして及び／又は無線ネットワークのＡＰとして動作する局として定義される。

【００１０】

本明細書で使用されるように用語「トラフィック」及び／又は「トラフィックストリーム」は、ＳＴＡのような無線デバイス間のデータフロー及び／又はストリームとして定義される。本明細書で使用されるように用語「セッション」は、直接物理リンクを確立した一対の局内に保有又は格納される状態情報として定義される（例えば、転送を除く）。状態情報は、セッションを記述又は定義し得る。

【００１１】

本明細書で使用されるように用語「無線デバイス」は、例えば、無線通信可能なデバイス、無線通信可能な通信デバイス、無線通信可能な通信局、無線通信可能なポータブル又は非ポータブルデバイス等を含む。幾つかの実施形態では、無線デバイスは、コンピュータに集積される周辺機器又はコンピュータに取り付けられる周辺機器であってよい又は含んでよい。幾つかの実施形態では、用語「無線デバイス」は、任意選択的に、無線サービスを含んでよい。

【００１２】

本発明は様々なアプリケーションに使用され得ることを理解されたい。本発明はこの点に関して制限されないが、本明細書に開示される回路及び技術は、無線システムの局のような多くの装置に使用され得る。本発明の範囲内に含まれると意図される局は、例としてのみ、無線ローカルエリアネットワーク（ＷＬＡＮ）局、無線パーソナルネットワーク（ＷＰＡＮ）等を含む。

【００１３】

幾つかの実施形態は、様々なデバイス及びシステム、例えば、ビデオデバイス、オーディオデバイス、オーディオビデオ（Ａ／Ｖ）デバイス、セットトップボックス（ＳＴＢ），ブルーレイディスク（ＢＤ）プレーヤ、ＢＤレコーダ、デジタルビデオディスク（ＤＶＤ）プレーヤ、高解像度（ＨＤ）ＤＶＤプレーヤ、ＤＶＤレコーダ、ＨＤ　ＤＶＤレコーダ、パーソナルビデオレコーダ（ＰＶＲ）、ブロードキャストＨＤレシーバ、ビデオソース、オーディオソース、ビデオシンク、オーディオシンク、ステレオチューナ、ブロードキャスト無線レシーバ、ディスプレイ、フラットパネルディスプレイ、パーソナルメディアプレーヤ（PMP）、デジタルビデオカメラ（DVC）、デジタルオーディオプレーヤ、スピーカ、オーディオレシーバ、オーディオアンプ、データソース、データシンク、デジタルスチルカメラ（DSC）、パーソナルコンピュータ（PC）、デスクトップコンピュータ、モバイルコンピュータ、ラップトップコンピュータ、ノートブックコンピュータ、タブレットコンピュータ、スマートフォン、デジタルテレビ、サーバコンピュータ、ハンドヘルドコンピュータ、ハンドヘルドデバイス、携帯情報端末（ＰＤＡ）デバイス、ハンドヘルドＰＤＡデバイス、オンボードデバイス、オフボードデバイス、ハイブリッドデバイス、車両用デバイス、非車両用デバイス、モバイル又はポータブルデバイス、消費者デバイス、非モバイル又は非ポータブルデバイス、無線通信局、無線通信デバイス、無線AP、有線又は無線ルータ、有線又は無線モデム、有線又は無線ネットワーク、ワイヤレスエリアネットワーク、無線ビデオエリアネットワーク（ＷＶＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、WLAN、PAN、WPAN、既存の無線ＨＤＴＭ及び／又はワイヤレスギガビットアライアンス（ＷＧＡ）仕様及び／又は将来のバージョン及び／又はその派生に従って動作するデバイス及び／又はネットワーク、既存のＩＥＥＥ８０２．１１（ＩＥＥＥ８０２．１１・２００７：無線ＬＡＮメディアアクセス制御（ＭＡＣ）及び物理層（ＰＨＹ）仕様）基準及び改正（「IEEE802.11標準」）、Ｗｏｒｌｄｗｉｄｅ　Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ　ｆｏｒ　Ｍｉｃｒｏｗａｖｅ　Ａｃｃｅｓｓ（ＷｉＭＡＸ（登録商標））のＩＥＥＥ８０２．１６規格、ロングタームエボリューション（ＬＴＥ）及びロングタームエボリューションアドバンスト（ＬＴＥ－Ａ）を含む第３世代パートナーシッププロジェク

ト（３ＧＰＰ）、及び／又は将来のバージョン及び／又はその派生に従って動作するデバイス及び／又はネットワーク、上記のネットワーク、一方向及び／又は双方向無線通信システム、セルラー無線電話通信システム、ワイヤレスディスプレイ（ＷｉＤｉ）デバイス、携帯電話、無線電話、パーソナル通信システム（PCS）デバイス、無線通信デバイスを組み込むＰＤＡデバイス、モバイル又はポータブルグローバルポジショニングシステム（GPS）デバイス、GPSレシーバ又はトランシーバ又はチップを内蔵するデバイス、ＲＦＩＤ素子又はチップを内蔵するデバイス、多入力多出力（ＭＩＭＯ）トランシーバ又はデバイス、一入力多出力（SIMO）トランシーバ又はデバイス、多入力一出力（MISO）トランシーバ又はデバイス、１又は複数の内部アンテナ及び／又は外部アンテナを有するデバイス、デジタルビデオ放送（ＤＶＢ）デバイス又はシステム、マルチスタンダード無線デバイス又はシステム、有線又は無線ハンドヘルドデバイス（例えば、ＢｌａｃｋＢｅｒｒｙ（登録商標）、Ｐａｌｍ　Ｔｒｅｏ）、無線アプリケーションプロトコル（ＷＡＰ）デバイス等の一部であるユニット及び／又はデバイスと関連して用いられてよい。

【００１４】

幾つかの実施形態は、無線通信信号及び／又はシステム、例えば、無線周波数（ＲＦ）、赤外線（ＩＲ）、周波数分割多重（ＦＤＭ）、直交ＦＤＭ（ＯＦＤＭ）、時分割多重（ＴＤＭ）、時分割多重接続（ＴＤＭＡ）、拡張ＴＤＭＡ（Ｅ－ＴＤＭＡ）、汎用パケット無線サービス（ＧＰＲＳ）、拡張ＧＰＲＳ、符号分割多重接続（ＣＤＭＡ）、広帯域ＣＤＭＡ（ＷＣＤＭＡ（登録商標））、ＣＤＭＡ２０００、シングルキャリアＣＤＭＡ、マルチキャリアＣＤＭＡ、マルチキャリア変調（ＭＤＭ），離散マルチトーン（ＤＭＴ）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、グローバルポジショニングシステム（ＧＰＳ）、Ｗｉ－Ｆｉ、Ｗｉ－Ｍａｘ、無線メトロポリタンエリアネットワーク（WMAN）、無線広域ネットワーク（WWAN）、ＺｉｇＢｅｅTM、ウルトラワイドバンド（ＵＷＢ）、汎欧州デジタル移動電話方式（ＧＳＭ（登録商標））、２Ｇ、２．５Ｇ、３Ｇ、３．５Ｇ、ＧＭＳ進化型高速データレート（ＥＤＧＥ）等のうちの１又は複数のタイプと関連して用いられてよい。他の実施形態は、様々な他のデバイス、システム、及び／又はネットワークにおいて用いられてよい。

【００１５】

幾つかの実施形態は、適当な限られた距離又は短距離無線通信ネットワーク、例えば「ピコネット」、例えばワイヤレスエリアネットワーク、ＷＶＡＮ、ＷＰＡＮ等と関連して用いられてよい。

【００１６】

図１は、本開示に一致する１つの例示的な実施形態のトップレベルシステムダイヤグラム１００を示す。モバイルプラットフォーム１０２は、コンテキストデータを含むデータをセンサ１０８からアクセスセキュリティモジュール１０６を介して取得し得るコンテキストアウェアアプリケーション１０４を備えることが示されている。アクセスセキュリティモジュール１０６は、認証された及び／又はセキュアなアプリケーションへのセンサのアクセスを制限するよう構成されてよい。アクセスセキュリティモジュール１０６は、センサデータの検証を提供してもよいし、以下により詳細に記載するように、信頼できる実行環境（ＴＥＥ）において動作するよう構成されてよい。モバイルプラットフォーム１０２は、例えば、スマートフォン、ラップトップ又はタブレットのようなモバイル又は無線通信デバイスのいずれのタイプであってよい。

【００１７】

コンテキストアウェアアプリケーション１０４は、例えば、コンテキストデータに基づいてポリシー設定を調整し得るｅコマースアプリケーションのようなセキュアな又は認証されたモバイルアプリケーションであってよい。例えば、デバイスの位置は、トランザクションに関連する支払方法又はセキュリティのレベルに影響し得る。別の例のように、デバイスが移動車両内にあることの判断は、安全を考慮して、アプリケーションに、ダイヤリング又はテクスティングに制限を課すことができるようにし得る。さらに別の例は、ペアレンタルコントロール及びデバイス上のアプリケーションを通じて提示される媒体のコ

ンテンツレンティング管理を含んでよい。

【００１８】

センサ１０８は、ＧＰＳレシーバ、加速度計、コンパス、ジャイロスコープ、カメラ、マイク、タッチセンサ、温度センサ、ユーザ認証センサ、またはモバイルプラットフォーム１０２を取り囲む環境に関する情報を提供し得るあらゆる他のタイプの適当な環境センサのような、コンテキストアウェアセンサを含んでよい。これらのタイプのセンサにより提供され得るコンテキストデータは、概して、本質的に機密又は私的であると考えられ、それにより、不正な配布に対する保護を都合良く必要とする。さらに、データの有効性を検証して、悪意のあるソフトウェア（マルウェア）が提示されるコンテキストデータをセキュリティを回避するアプリケーションに変え得る可能性を低減してもよいことが理解される。

【００１９】

図２は、本開示に一致する１つの例示的な実施形態のブロックダイヤグラム２００を示す。モバイルプラットフォーム１０２は、以下により詳細に記載されるように、非セキュア１０４ａ及びセキュア１０４ｂの両バリエーションにおけるコンテキストアウェアアプリケーション、及び、非セキュア１０８ａ及びセキュア１０８ｂの両バリエーションにおけるセンサを備えることが示される。アクセスセキュリティモジュール１０６は、センサアクセスフレームワークアプリケーションプログラミングインターフェース（ＡＰＩ）２０２、センサ管理モジュール２０４、ＴＥＥミドルウェアモジュール２０６、ＯＳカーネル２０８及び関連するドライバ２１４、ＴＥＥアクセスドライバ２１０、及びＴＥＥファームウェアセンサドライバ２１２を含むことがより詳細に示される。

【００２０】

センサアクセスフレームワークＡＰＩ２０２は、コンテキストアウェアアプリケーション、セキュア１０４ｂ及び非セキュア（又はレガシー）１０４ａの両アプリケーションがセンサ１０８にそれを通じてアクセスし得る規格化されたインターフェースを提供するよう構成されてよい。幾つかの実施形態では、センサアクセスフレームワークＡＰＩ２０２は、Ｊａｖａ（登録商標）ベースのソフトウェア開発キット（ＳＤＫ）又はウィンドウズ（登録商標）ランタイム（ＷｉｎＲＴ）又はハイパーテキストマークアップ言語５（ＨＴＭＬ５）ベースのＡＰＩであってよい。

【００２１】

セキュアなトランザクション（例えば、アプリケーション１０４ｂからの要求と応答）は、センサアクセスフレームワークＡＰＩ２０２及びＴＥＥアクセスドライバ２１０の間に追加のインターフェースレベルを提供するＴＥＥミドルウェアモジュール２０６を通じて処理されてよい。非セキュアなトランザクション（例えば、アプリケーション１０４ａからの要求及び応答）は、センサアクセスフレームワークＡＰＩ２０２及びＯＳカーネル２０８内に集積される非ＴＥＥドライバ２１４間の代替の追加のインターフェースレベルを提供するセンサ管理モジュール２０４を通じて処理されてよい。センサ管理モジュール２０４及びＴＥＥミドルウェアモジュール２０６は、ＯＳカーネル２０８の外部にあり、これらのコンポーネントへのソフトウェアの更新を促して、概してより困難であり且つ時間を消費する全ＯＳ２０８の再インストールを要しないで、新しい機能及び／又はバグフィックスを実装するコンポーネントとして提供されてよい。

【００２２】

例えば、ファームウェア２１２を備え得る信頼できる実行環境は、セキュアコンテキストセンサ１０８ｂのセンサドライバに対して提供されてよい。ＴＥＥファームウェアセンサドライバ２１２は、ＯＳカーネル２０８内に集積され得るＴＥＥアクセスドライバ２１０を通じてアクセスされてよい。ＴＥＥファームウェアセンサドライバ２１２は、アプリケーション１０４ｂにより生成されるセンサコンテキストデータの要求を検査して、アプリケーションが認証されてそのようなデータを受信及び／又はそれをセキュアに処理することを検証してよい。検証は、秘密／公開鍵暗号化、デジタル署名、パスワード、認証情報、又はあらゆる他の適したセキュリティ技術の使用を通じて遂行されてよい。同様に、

ＴＥＥファームウェアセンサドライバ２１２は、秘密／公開鍵暗号化、デジタル署名、パスワード、認証情報、又はあらゆる他の適したセキュリティ技術の使用を通じて、アプリケーション１０４ｂに向けて生成されるセンサコンテキストデータの応答の検証を提供してよい。

【００２３】

例えば、信頼できる又はセキュアなコンテキストアウェアアプリケーション１０４ｂは、センサコンテキストデータの要求を生成し、アプリケーションが認証されて、そのようなデータを受信することを示す認証情報を与えてよい。要求及び認証情報は、センサアクセスフレームワークＡＰＩ２０２、ＴＥＥミドルウェアモジュール２０６、ＴＥＥアクセスドライバ２１０を通じて、そして認証情報が検証されるＴＥＥファームウェアセンサドライバ２１２に、伝えられてよい。ＴＥＥファームウェアセンサドライバ２１２は、センサハードウェアを制御して、所望のデータを取得し、例えば、それをセキュアなアプリケーション１０４ｂまで提供して戻す前に、セキュアなアプリケーション１０４ｂに利用可能な公開／秘密鍵の組み合わせを用いてデータを暗号化してよい。

【００２４】

ＴＥＥファームウェアセンサドライバ２１２は、マルウェアにより乱される可能性を有するＯＳカーネル２０８内のドライバ２１４と独立のセンサハードウェア及びセンサデータに直接アクセスするよう構成されてよい。コンテキストデータは、ＴＥＥファームウェアセンサドライバ２１２内で守られる又は暗号化されるので、プラットフォーム１０２上の信頼できない又は悪意のあるアプリケーション又はＯＳサービスは、意図するセキュアなアプリケーション１０４ｂへの送信に先立って又はその間に、情報にアクセス又は変更することを防止され得る。

【００２５】

ＴＥＥは、例えばＯＳ２０８及び信頼できないアプリケーション１０４ａのようなＴＥＥの範囲外にあるモバイルプラットフォーム１０２上で、他のエンティティからのセキュリティ及び隔離を提供するよう構成されてよい。隔離は、外部エンティティが、センサドライバ２１２又はセキュアセンサ１０８ｂの管理を遂行する、又はアクセスを取得することを防止し得る。幾つかの実施形態では、ＴＥＥは、別個の物理的ハードウェア、例えば、プラットフォーム１０２に関連するＩＣから隔てられる集積回路（ＩＣ）を備えてよい。幾つかの実施形態では、ＴＥＥは、プラットフォーム１０２と共有されるＩＣ内の別個のコントローラ又はプロセッサを備えてよい。幾つかの実施形態では、ＴＥＥは、プラットフォーム１０２と共有されるコントローラ又はプロセッサ内に別個のドメインを備えてよい。様々な技術を採用して、ハードウェアがＴＥＥとプラットフォーム１０２の間に共有されている状況を含むＴＥＥをセキュアに隔離してよい。これらの技術は、プロセッサに関連する特権実行モード、メモリに関連するアクセス保護メカニズム、及び／又はセンサドライバ２１２の変更を防ぐためのファームウェアの使用を含んでよい。

【００２６】

レガシードライバ２１４は、非セキュア（又はレガシー）センサ１０８ａへのアクセスを提供するＯＳカーネル２０８内に集積されてもよい。本明細書に開示されるセキュリティシステムの採用及び実装を促すために、幾つかの実施形態は、レガシーアプリケーション及びドライバが、開示されたセキュアなアクセス技術と並行して、コンテキストセンサの幾つか又は全てへの非セキュアなアクセスを提供する間の移行期間を実装してよい。移行期間が終了した後、センサマネージャ２０４及び／又はレガシードライバ２１４は、情報技術（ＩＴ）管理者、デバイスユーザ、又はコンテキストセンサへのセキュアなアクセスパスのみ残す他の認証エンティティにより削除又はディセーブルされてよい。

【００２７】

図３は、本開示に一致する別の例示的な実施形態のブロックダイヤグラム３００を示す。この実施形態は、センサ周辺ハブ３０２が設けられていることを除いて、図２に関連する上述の実施形態とほとんどの点において類似している。センサ周辺ハブ３０２は、セキュアセンサ１０８ｂのほとんど又はすべてが、ＴＥＥプロセッサ又はマイクロコントロー

ラ３０４及びＴＥＥファームウェアセンサドライバ２１２により提供される信頼できる実行環境にそれを通って連結され得る中心点を提供する。この実施形態においてプラットフォーム１０２の他のコンポーネントから隔離される物理ハードウェアとして実装されるセンサ周辺ハブ３０２は、信頼できる実行環境に対して追加の隔離及びセキュリティを提供する。

【００２８】

図４は、ネットワークにおける本開示の例示的な実施形態に一致するプラットフォームを示すシステムダイヤグラム４００を示す。プラットフォーム１０２は、例えば、スマートフォン、タブレット、ラップトップコンピューティングデバイス、または無線信号を送信又は受信するよう構成されたあらゆる他のデバイスのような移動体通信デバイスであってよい。プラットフォーム１０２は、コンテキストアウェアセンサ１０８とともに構成されてよく、信頼できる実行環境（ＴＥＥ）２１２を通じてセキュアなアクセス及び検証機能を提供してよい。幾つかの実施形態では、プラットフォーム１０２は、プロセッサ４０４、メモリ４０６、入出力（Ｉ／Ｏ）システム４０８、ディスプレイ／キーボード、又は例えばタッチスクリーンのような他のタイプのユーザインターフェース（ＵＩ）４０２を備えてよい。任意の数のプラットフォーム１０２は、無線ネットワークであり得るネットワーク４１２を介して、トランシーバ４１０を通じて信号を送信又は受信してよい。

【００２９】

幾つかの実施形態では、１又は複数の仮想マシン（ＶＭ）がプラットフォーム１０２上に提供されてよい。ＶＭは、共通プロセッサ４０４及びメモリ４０６を共有してよいが、センサアクセスに対して独立のセキュリティポリシーを実装してよい。

【００３０】

図５は、本開示に一致する別の例示的な実施形態の動作５００のフローチャートを示す。動作５１０では、１又は複数のセンサが、モバイルデバイスに関連するコンテキストデータを提供するよう構成される。動作５２０では、ＡＰＩがセンサドライバに提供される。ＡＰＩは、センサを制御するよう構成されてよい。動作５３０では、信頼できる実行環境（ＴＥＥ）が提供されて、モバイルデバイス上で動作する。ＴＥＥは、センサドライバをホストし、センサドライバへの及びセンサへのコントロールアクセス及びデータアクセスを制限するよう構成されてよい。動作５４０では、要求が、ＡＰＩを通じて、コンテキストデータに対して生成される。要求は、モバイルデバイスに関連するアプリケーションにより生成される。動作５５０では、アプリケーションは、ＡＰＩを通じて、要求されたコンテキストデータ及び正当性インジケータを受信する。動作５６０では、アプリケーションは、正当性インジケータに基づいて要求されたコンテキストデータを検証する。動作５７０では、アプリケーションに関連するポリシーが適合される。適合は、検証されたコンテキストデータに基づく。

【００３１】

本明細書に記載された方法の実施形態は、１又は複数のプロセッサにより実行されると、方法を実行する命令を、個別に又は組み合わせて、その中に格納する１又は複数の記憶媒体を含むシステム内で実装されてよい。ここで、プロセッサは、例えば、システムＣＰＵ（例えば、コアプロセッサ）及び／又はプログラマブル回路を含んでよい。従って、本明細書に記載される方法による動作は、幾つかの異なる物理的位置で構造を処理するような複数の物理デバイスを越えて分配されてよいことが意図される。また、方法の動作は、当業者に理解されるように、個別に又はサブコンビネーションで実行されてよいことが意図される。従って、フローチャートのそれぞれの動作のすべてが実行される必要はなく、本開示は、明確に、当業者の一人により理解されるように、そのような動作のすべてのサブコンビネーションが有効とされることを意図する。

【００３２】

記憶媒体は、あらゆるタイプの有形の媒体、例えば、フロッピー（登録商標）ディスク、光ディスク、コンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、コンパクトディスクリライタブル（ＣＤ－ＲＷ）、デジタル多用途ディスク（ＤＶＤ）、及び磁気光デ

ィスクを含むあらゆるタイプのディスク、リードオンリメモリ（ＲＯＭ）のような半導体デバイス、ダイナミック及びスタティックＲＡＭのようなランダムアクセスメモリ（ＲＡＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、磁気又は光カード、又は電子命令を格納するのに好適なあらゆるタイプの媒体を含んでよい。

【００３３】

「回路」は、本明細書のあらゆる実施形態において用いられるように、例えば、ハードワイヤード回路、プログラマブル回路、ステートマシン回路、及び／又はプログラマブル回路により実行される命令を格納するファームウェアを単独で又は任意に組み合わせて備えてよい。アプリケーションは、ホストプロセッサ又は他のプログラマブル回路のようなプログラマブル回路上で実行され得るコード又は命令として具現されてよい。本明細書のあらゆる実施形態において用いられるように、モジュールは、回路として具現されてよい。回路は、集積回路チップのような集積回路として具現されてよい。

【００３４】

従って、本開示は、コンテキストセンサデータをモバイルプラットフォームアプリケーションにセキュアに提供するためのデバイス、方法、システム、及びコンピュータ可読記憶媒体を提供する。

【００３５】

方法は、モバイルデバイスに関連するコンテキストデータを提供する１又は複数のセンサを構成することを含んでよい。この例の方法は、センサを制御するよう構成されたＡＰＩセンサドライバを提供することを含んでもよい。この例の方法は、さらに、モバイルデバイス上で動作するＴＥＥを提供することを含んでよい。なお、ＴＥＥは、センサドライバをホストし、センサドライバへの及びセンサへのコントロールアクセス及びデータアクセスを制限するよう構成される。この例の方法は、さらに、ＡＰＩを通じてコンテキストデータの要求を生成することを含んでよい。なお、要求は、モバイルデバイスに関連するアプリケーションにより生成される。この例の方法は、さらに、アプリケーションにより、要求されたコンテキストデータ及び正当性インジケータを、ＡＰＩを通じて受信することを含んでよい。この例の方法は、さらに、アプリケーションにより、要求されたコンテキストデータを正当性インジケータに基づいて検証することを含んでよい。この例の方法は、さらに、アプリケーションに関連するポリシーを、検証されたコンテキストデータに基づいて調整することを含んでよい。

【００３６】

別の例の方法は前述の処理を含み、正当性インジケータはデジタル署名を含む。

【００３７】

別の例の方法は、前述の処理を含み、さらに、センサドライバにより、要求されたコンテキストデータを暗号化することを含む。

【００３８】

別の例の方法は前述の処理を含み、センサは加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、又は周辺光センサである。

【００３９】

別の例の方法は前述の処理を含み、コンテキストデータはデバイス位置、デバイス所在地、デバイスの動き、ユーザ識別情報、温度、又はノイズレベルである。

【００４０】

別の例の方法は前述の処理を含み、ポリシーはモバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、又はメディア視聴ポリシーのペアレンタルコントロールである。

【００４１】

別の態様によれば、デバイスが提供される。デバイスは、デバイスに関連するコンテキストデータを提供するよう構成された１又は複数のセンサを含んでよい。この例のデバイ

スは、コンテキストデータの要求を受信し、要求に応じてコンテキストデータ及び関連する正当性インジケータを提供するよう構成されたセキュアセンサドライバモジュールを含んでもよい。この例のデバイスは、さらに、デバイス上で動作するＴＥＥを含んでよい。ＴＥＥは、セキュアセンサドライバモジュールをホストし、セキュアセンサドライバモジュールへの及びセンサへのコントロールアクセス及びデータアクセスを制限するよう構成される。この例のデバイスは、さらに、要求を生成し、コンテキストデータを受信し、正当性インジケータに基づいてコンテキストデータを検証し、検証されたコンテキストデータに基づいてアプリケーションに関連するポリシーを調整するよう構成された１又は複数のアプリケーションモジュールを含んでよい。

【００４２】

別の例のデバイスは前述のコンポーネントを含み、正当性インジケータはデジタル署名を含む。

【００４３】

別の例のデバイスは前述のコンポーネントを含み、セキュアセンサドライバモジュールはさらにコンテキストデータを暗号化するよう構成される。

【００４４】

別の例のデバイスは前述のコンポーネントを含み、さらに、センサのそれぞれに結合されるセンサ周辺ハブ、ＴＥＥを提供するプロセッサ及びメモリを含むセンサ周辺ハブ、セキュアセンサドライバモジュールを格納するよう構成されるファームウェアを含む。

【００４５】

別の例のデバイスは前述のコンポーネントを含み、センサは加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、又は周辺光センサである。

【００４６】

別の例のデバイスは前述のコンポーネントを含み、コンテキストデータはデバイス位置、デバイス所在地、デバイスの動き、ユーザ識別情報、温度、又はノイズレベルである。

【００４７】

別の例のデバイスは前述のコンポーネントを含み、ポリシーはモバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、又はメディア視聴ポリシーのペアレンタルコントロールである。

【００４８】

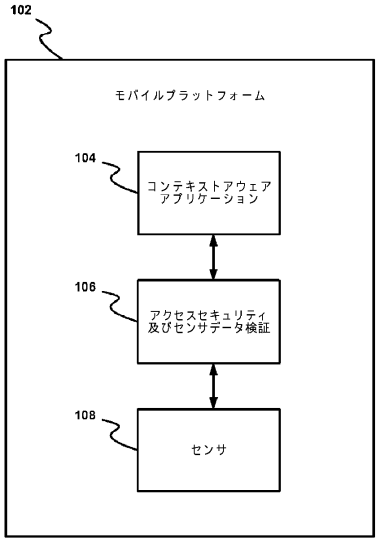
別の態様によると、プロセッサにより実行されると、プロセッサに、上に例において記載されるような方法の動作を実行させる格納された命令を有する少なくとも１つのコンピュータ可読記憶媒体が提供される。

【００４９】

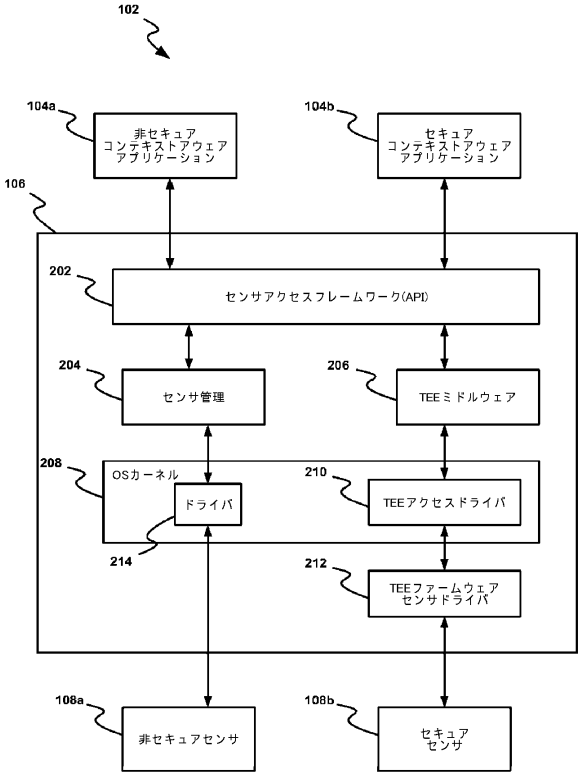
別の態様によると、モバイル通信プラットフォームが提供される。モバイル通信プラットフォームは、プロセッサ、プロセッサに連結されたメモリ、プロセッサに連結されたＩ／Ｏシステム、及びＩ／Ｏシステムに連結されたユーザインターフェースを含んでよい。この例のモバイル通信プラットフォームは、プロセッサに結合される１又は複数のセンサを含んでもよい。センサは、プラットフォームに関連するコンテキストデータを提供するよう構成されるこの例のモバイル通信プラットフォームは、さらに、コンテキストデータの要求を受信し、要求に応じてコンテキストデータ及び関連するデジタル署名を提供するよう構成されたセキュアセンサドライバモジュールを含んでよい。　この例のモバイル通信プラットフォームは、さらに、プラットフォーム上で動作するＴＥＥを含んでよい。ＴＥＥは、セキュアセンサドライバモジュールをホストし、セキュアセンサドライバモジュールへの及びセンサへのコントロールアクセス及びデータアクセスを制限するよう構成される。この例のモバイル通信プラットフォームは、さらに、要求を生成し、コンテキストデータを受信し、デジタル署名に基づいてコンテキストデータを検証し、検証されたコンテキストデータに基づいてアプリケーションに関連するポリシーを調整するよう構成された１又は複数のアプリケーションモジュールを含んでよい。

【００５０】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、センサは加速度計、グローバルポジショニングセンサ、コンパス、カメラ、近接センサ、マイク、ジャイロスコープ、タッチセンサ、周辺温度センサ、又は周辺光センサである。
【００５１】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、コンテキストデータはプラットフォーム位置、プラットフォーム所在地、プラットフォームの動き、ユーザ識別情報、温度、又はノイズレベルである。
【００５２】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、ポリシーはモバイルコマース決済ポリシー、モバイルコマースセキュリティポリシー、又はメディア視聴ポリシーのペアレンタルコントロールである。
【００５３】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、プラットフォームはスマートフォン、ラップトップコンピューティングデバイス、又はタブレットである。
【００５４】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、さらに、それぞれ無線ネットワークを介して通信するよう構成される複数のプラットフォームを含む。
【００５５】
別の例のモバイル通信プラットフォームは前述のコンポーネントを含み、ユーザインターフェースはタッチスクリーン及び／又はキーボードである。
【００５６】
本明細書で採用されている用語及び表現は、制限ではなく、説明の用語として用いられるものであり、そのような用語及び表現の使用において、示され及び記載される特徴のあらゆる均等物（又はそれらの一部）を除く意図はなく、様々な修正が特許請求の範囲の範囲内で可能である。従って、特許請求の範囲は、そのような均等物のすべてをカバーするよう意図される。様々な特徴、態様、及び実施形態が、本明細書に記載されている。特徴、態様、及び実施形態は、互いに組み合わせること、及び当業者により理解されるような変形及び修正を受け入れる。従って、本開示は、そのような組み合わせ、変形、及び修正を包含するよう考慮されるべきである。

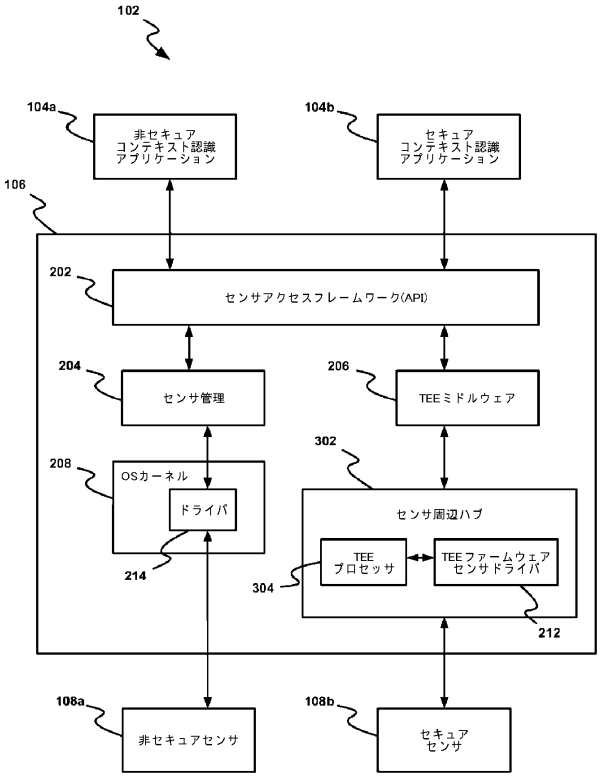
【図１】


102
モバイルプラットフォーム
104
コンテキストアウェア
アプリケーション
106
アクセスセキュリティ
及びセンサデータ検証
108
センサ

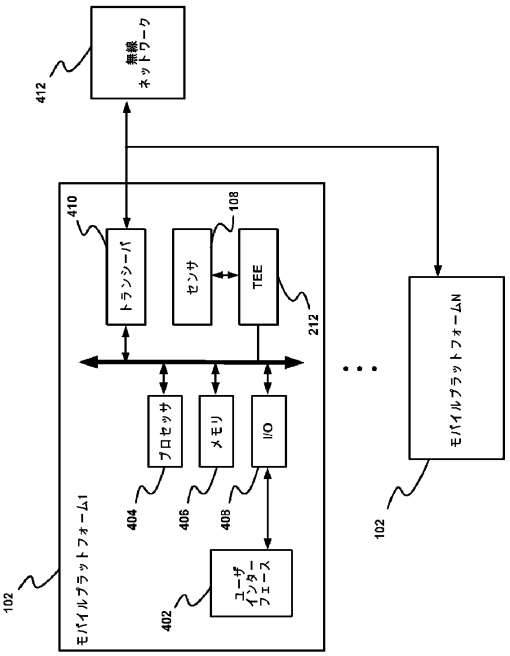
【図２】


102
104a
非セキュア
コンテキストアウェア
アプリケーション
104b
セキュア
コンテキストアウェア
アプリケーション
106
202
センサアクセスフレームワーク(API)
204
センサ管理
206
TEEミドルウェア
208
OSカーネル
ドライバ
210
TEEアクセスドライバ
214
212
TEEファームウェア
センサドライバ
108a
非セキュアセンサ
108b
セキュア
センサ

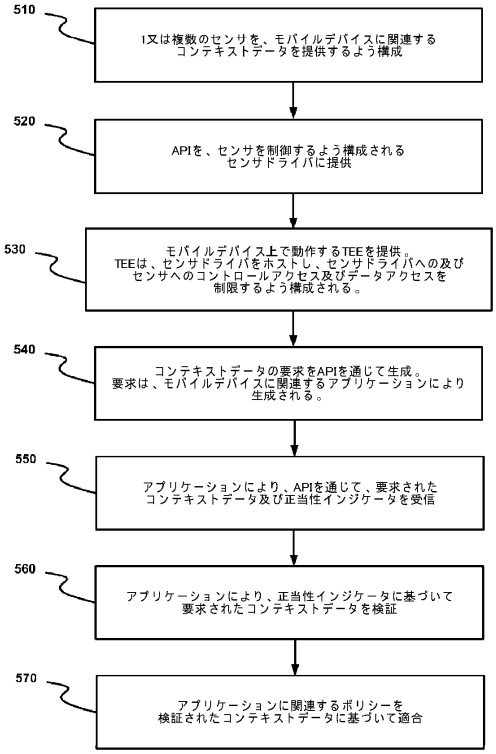
【図３】


102
104a
非セキュア
コンテキスト認識
アプリケーション
104b
セキュア
コンテキスト認識
アプリケーション
106
202
センサアクセスフレームワーク(API)
204
センサ管理
206
TEEミドルウェア
208
OSカーネル
ドライバ
214
302
センサ周辺ハブ
TEE
プロセッサ
TEEファームウェア
センサドライバ
304
212
108a
非セキュアセンサ
108b
セキュア
センサ

【図４】


412
無線
ネットワーク
410
トランシーバ
108
センサ
TEE
212
プロセッサ
メモリ
I/O
404
406
408
ユーザ
インタフェース
402
モバイルプラットフォーム1
102
モバイルプラットフォームN
102

【図５】


510
1又は複数のセンサを、モバイルデバイスに関連する
コンテキストデータを提供するよう構成
520
APIを、センサを制御するよう構成される
センサドライバに提供
530
モバイルデバイス上で動作するTEEを提供。
TEEは、センサドライバをホストし、センサドライバへの及び
センサへのコントロールアクセス及びデータアクセスを
制限するよう構成される。
540
コンテキストデータの要求をAPIを通じて生成。
要求は、モバイルデバイスに関連するアプリケーションにより
生成される。
550
アプリケーションにより、APIを通じて、要求された
コンテキストデータ及び正当性インジケータを受信
560
アプリケーションにより、正当性インジケータに基づいて
要求されたコンテキストデータを検証
570
アプリケーションに関連するポリシーを
検証されたコンテキストデータに基づいて適合

フロントページの続き

(72)発明者　ウォーカー、ジェシー
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内
(72)発明者　ダドゥ、サウラビ
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

審査官　宮司　卓佳

(56)参考文献　特開２００３－１４３１３６（ＪＰ，Ａ）
特開２００７－３３５９６２（ＪＰ，Ａ）
米国特許出願公開第２００８／００２２３７６（ＵＳ，Ａ１）
国際公開第２０１１／０１８９３７（WO，Ａ１）
特開２００３－１６３７３９（ＪＰ，Ａ）
特開２０１０－０２１８０３（ＪＰ，Ａ）
米国特許出願公開第２００８／０２４８７８９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２１／８８
Ｈ０４Ｍ　１／６６