(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-524236
(P2015-524236A)
(43)公表日　平成27年8月20日(2015.8.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04M 11/00	***(2006.01)***	H04M	11/00	302	4C117
G06Q 50/24	***(2012.01)***	G06Q	50/24		5K201
A61B 5/00	*(2006.01)*	A61B	5/00	G	5L099

審査請求 未請求　予備審査請求 未請求　（全 37 頁）

(21)出願番号　特願2015-518648 (P2015-518648)
(86)(22)出願日　平成25年6月25日 (2013.6.25)
(85)翻訳文提出日　平成27年1月27日 (2015.1.27)
(86)国際出願番号　PCT/US2013/047729
(87)国際公開番号　WO2014/004590
(87)国際公開日　平成26年1月3日 (2014.1.3)
(31)優先権主張番号　13/532,588
(32)優先日　平成24年6月25日 (2012.6.25)
(33)優先権主張国　米国 (US)

(71)出願人　513125245
スプリント　コミュニケーションズ　カンパニー　エル．ピー．
アメリカ合衆国、カンザス　６６２５１－２１００　オーバーランド　パーク、メールストップ　ケイエスオーピーエイチエヌ０３１２－３エイ３７１　スプリント　パークウェイ　６４５０
(74)代理人　110000877
龍華国際特許業務法人

最終頁に続く

(54)【発明の名称】信頼されたエンドツーエンド通信インフラストラクチャ

(57)【要約】
信頼されたエンドツーエンド通信リンクを介して、医療データを配信する方法。上記の方法は、第１のセンサにより、人のパラメータの測定を取得する段階と、第２のセンサにより、人からバイオメトリックを取得する段階と、プロセッサの信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションにより、第１のセンサ及び第２のセンサからの入力を受信する段階であって、上記のセキュリティゾーンは、それによって、プロセッサの通常のパーティションにおいて実行する複数のアプリケーションによる、第１のセンサ及び第２のセンサからの入力へのアクセスがブロックされる段階と、第１のセンサ及び第２のセンサからの入力に基づいて、信頼されたエンドツーエンド通信リンクを介して、医療データサーバにメッセージを送信する段階とを有し、第１のセンサ及び第２のセンサからの入力は、パラメータの測定及びバイオメトリックを含み、メッセージを受信するアプリケーションは、医療データサーバの信頼されたセキュリティゾーンにおいて実行する。

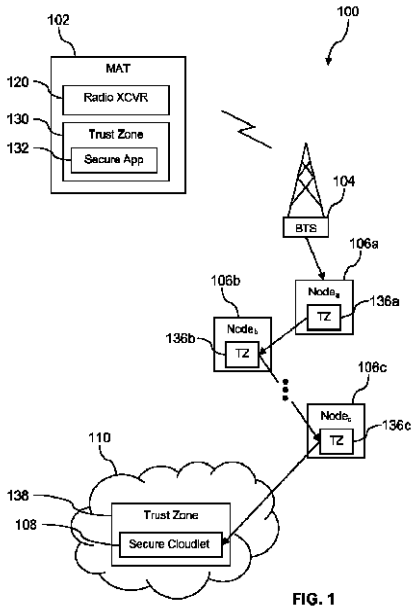


FIG. 1

【特許請求の範囲】
【請求項１】
信頼されたエンドツーエンド通信リンクを介して、医療データを配信する方法であって、
第１のセンサにより、人のパラメータの測定を取得する段階と、
第２のセンサにより、前記人からバイオメトリックを取得する段階と、
プロセッサの信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションにより、前記第１のセンサ及び第２のセンサからの入力を受信する段階であって、それによって、前記プロセッサの通常のパーティションにおいて実行する複数のアプリケーションによる、前記第１のセンサ及び第２のセンサからの前記入力へのアクセスがブロックされる段階と、
前記第１のセンサ及び第２のセンサからの前記入力に基づいて、信頼されたエンドツーエンド通信リンクを介して、医療データサーバにメッセージを送信する段階と、
を有し、
前記第１のセンサ及び第２のセンサからの前記入力は、前記パラメータの前記測定及び前記バイオメトリックを含み、
前記メッセージを受信するアプリケーションは、前記医療データサーバの信頼されたセキュリティゾーンにおいて実行する、
方法。
【請求項２】
前記信頼されたセキュリティゾーンは、前記セキュアなアプリケーションが、前記信頼されたセキュリティゾーンにおいて実行している間、前記プロセッサの前記通常のパーティションにおいて実行する前記複数のアプリケーションによるアクセスが、メモリにアクセスすること、複数の入力を読み込むこと、及び、複数の出力を書き込むことをブロックする前記プロセッサにより提供される、
請求項１に記載の方法。
【請求項３】
前記信頼されたセキュリティゾーンは、第１の仮想プロセッサにより提供され、
前記通常のパーティションは、第２の仮想プロセッサにより提供される、
請求項１又は請求項２に記載の方法。
【請求項４】
前記信頼されたセキュリティゾーンは、第１の物理プロセッサにより提供され、
前記通常のパーティションは、第２の物理プロセッサにより提供される、
請求項１から請求項３までの何れか一項に記載の方法。
【請求項５】
前記人の前記パラメータは、血糖値、血液粘度、血圧、体温、血中酸素飽和度、脈拍数又は心拍リズムである、
請求項１から請求項４までの何れか一項に記載の方法。
【請求項６】
前記バイオメトリックは、指紋スキャン、網膜スキャン又は人相（顔）スキャンである、
請求項１から請求項５までの何れか一項に記載の方法。
【請求項７】
前記医療データサーバは、複数の異なる人に関連する複数の医療記録を有し、
各医療記録は、複数の前記人のうちの特定の人のパラメータの測定、及び、複数の前記人のうちの前記特定の人のバイオメトリックを含み、
前記方法は、医療処置レジュメの効力を実現するべく、前記複数の医療記録を解析する段階をさらに有する、
請求項１から請求項６までの何れか一項に記載の方法。
【請求項８】

信頼されたエンドツーエンド通信リンク確立する方法であって、
移動アクセス端末の信頼されたセキュリティゾーンにおいて通信アプリケーションを実行する段階と、
前記移動アクセス端末から、信頼されたエンタープライズ・エッジノードの信頼されたセキュリティゾーンにおいて実行する信頼された通信アプリケーションに、メッセージを送信する段階と、
前記信頼されたエンタープライズ・エッジノードから、クラウドを利用したサーバの信頼されたセキュリティゾーンにおいて実行する信頼されたクラウドレットに、前記メッセージを送信する段階と、
を有する、
方法。
【請求項９】
前記信頼されたエンタープライズ・エッジノードは、ファイアウォールサーバ又はルータ上のマルチプロトコル・ラベルスイッチング（ＭＰＬＳ）ポートの１つである、
請求項８に記載の方法。
【請求項１０】
前記信頼されたエンタープライズ・エッジノードの前記信頼されたセキュリティゾーンは、前記信頼された通信アプリケーションが、前記信頼されたエンタープライズ・エッジノードの前記信頼されたセキュリティゾーンにおいて実行している間、
前記信頼されたエンタープライズ・エッジノードのプロセッサが、前記プロセッサの通常のパーティションにおいて実行する複数の他のアプリケーションによるアクセスが、メモリにアクセスすること、複数の入力を読み込むこと、及び、複数の出力を書き込むことをブロックすることにより提供される、
請求項８又は請求項９に記載の方法。
【請求項１１】
前記信頼されたエンタープライズ・エッジノードの前記信頼されたセキュリティゾーンは、第１の仮想プロセッサにより提供され、
通常のパーティションは、第２の仮想プロセッサにより提供され、
前記第１の仮想プロセッサが実行している間、前記第２の仮想プロセッサは、命令を実行しない、
請求項８から請求項１０までの何れか一項に記載の方法。
【請求項１２】
前記移動アクセス端末は、前記信頼されたエンドツーエンド通信リンクを介して、信頼された通信アプリケーションに、前記メッセージを送信する、
請求項８から請求項１１までの何れか一項に記載の方法。
【請求項１３】
前記信頼されたエンドツーエンド通信リンクの一部は、セルラー無線通信リンクを含む、
請求項１２に記載の方法。
【請求項１４】
前記セルラー無線通信リンクは、符号分割多重アクセス（ＣＤＭＡ）、グローバルシステム・フォー・モバイルコミュニケーションズ（ＧＳＭ（登録商標））、ロングタームエボリューション（ＬＴＥ）、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（ＷｉＭＡＸ（登録商標））通信プロトコルの少なくとも１つに基づいて提供される、
請求項１３に記載の方法。
【請求項１５】
医療診断情報にアクセスする方法であって、
第１のセンサからの人のパラメータの測定及び第２のセンサからの前記人のバイオメトリックを取得する段階と、

前記第１のセンサ及び第２のセンサからの前記パラメータの前記測定及び前記バイオメトリックを送信する段階と、
移動アクセス端末の信頼されたセキュリティゾーンにおいて実行するプロセッサにより、前記第１のセンサ及び第２のセンサからの前記パラメータの前記測定及び前記バイオメトリックを受信する段階であって、それによって、通常実行モードにおいて実行する複数のアプリケーションによる、前記第１のセンサ及び第２のセンサからの前記パラメータの前記測定及び前記バイオメトリックへのアクセスがブロックされる段階と、
前記移動アクセス端末により、前記パラメータの前記測定及び前記バイオメトリックに基づく第１のメッセージを、信頼されたエンドツーエンド通信リンクを介して、医療データサーバに送信する段階であって、前記信頼されたエンドツーエンド通信リンクは、無線通信リンクを含む段階と、
前記医療データサーバの信頼されたセキュリティゾーンにおいて実行するアプリケーションにより、前記第１のメッセージを受信する段階と、
前記医療データサーバにより、前記パラメータの前記測定及び前記バイオメトリックに基づいて、第２のメッセージを、信頼されたエンドツーエンド通信リンクを介して、医師に関連付けられたコンピュータに送信する段階と、
前記第２のメッセージに基づいて、前記人に対する医療指示を決定する段階と、
を有する、
方法。
【請求項１６】
前記人の前記パラメータは、血糖値、血液粘度、血圧、体温、血中酸素飽和度、脈拍数又は心拍リズムである、
請求項１５に記載の方法。
【請求項１７】
前記バイオメトリックは、指紋スキャン、網膜スキャン又は人相（顔）スキャンのうちの１つである、
請求項１５又は請求項１６に記載の方法。
【請求項１８】
前記第２のメッセージは、検証可能な形で、複数の秘密の医療記録を提供する、
請求項１５から請求項１７までの何れか一項に記載の方法。
【請求項１９】
前記医療データサーバは、複数の異なる人に関連する複数の医療記録のデータストアを維持し、
各医療記録は、複数の前記人の一人に由来するパラメータ及びバイオメトリックを含み、
前記方法は、医療処置レジュメの効力を実現するべく、前記複数の医療記録を解析する段階をさらに有する、
請求項１５から請求項１８までの何れか一項に記載の方法。
【請求項２０】
複数のトラストトークンを含む第１のメッセージを受信する段階であって、各トラストトークンは、前記移動アクセス端末から前記医療データサーバへの前記信頼されたエンドツーエンド通信リンクにおけるネットワークノードの信頼されたセキュリティゾーンに関連する段階と、
前記信頼されたエンドツーエンド通信リンクの信頼レベルを確認するべく、前記複数のトラストトークンを解析する段階と、
をさらに有する、
請求項１５から請求項１９までの何れか一項に記載の方法。
【発明の詳細な説明】
【背景技術】
【０００１】

複数の電子通信は、例えば、電子メール、複数の医療記録、複数の金融取引、及び、その他秘密情報といった多種多様なコンテンツを運搬する。複数の電子通信は、コンテンツが変更又は侵入にさらされる可能性のある、安全対策の施されていない複数の通信リンクを通って、通信用のエンドツーエンド・パスのいくつかに向かって進む可能性がある。セキュリティを向上させ、複数の非道な動作主体による、秘密情報へのアクセスの試みに対する困難性のレベルを上げるべく、様々な複数のセキュリティ測定法が適用されてきた。

【発明の概要】

【課題を解決するための手段】

【０００２】

一実施形態において、信頼されたエンドツーエンド通信リンクを介して、医療データを配信する方法が開示される。上記の方法は、第１のセンサにより、人のパラメータの測定を取得する段階と、第２のセンサにより、上記人からバイオメトリックを取得する段階と、プロセッサの信頼されたセキュリティゾーンにおいて実行しているセキュアなアプリケーションにより、上記第１のセンサ及び第２のセンサからの入力を受信する段階であって、上記のセキュリティゾーンは、それによって、上記プロセッサの通常のパーティションにおいて実行している複数のアプリケーションによる、上記第１のセンサ及び第２のセンサからの上記入力へのアクセスがブロックされる段階と、上記第１のセンサ及び第２のセンサからの上記入力に基づいて、信頼されたエンドツーエンド通信リンクを介して、医療データサーバにメッセージを送信する段階とを有し、上記第１のセンサ及び第２のセンサからの上記入力は、上記パラメータの上記測定及び上記バイオメトリックを含み、上記メッセージを受信するアプリケーションは、上記サーバの信頼されたセキュリティゾーンにおいて実行する。

【０００３】

一実施形態において、信頼されたエンドツーエンド通信リンク確立する方法が開示されている。上記の方法は、移動アクセス端末の信頼されたセキュリティゾーンにおいて通信アプリケーションを実行する段階と、上記移動アクセス端末から、信頼されたエンタープライズ・エッジノードの信頼されたセキュリティゾーンにおいて実行している信頼された通信アプリケーションに、メッセージを送信する段階と、上記信頼されたエンタープライズ・エッジノードから、クラウドを利用したサーバの信頼されたセキュリティゾーンにおいて実行している信頼されたクラウドレットに、上記メッセージを転送する段階とを有する。

【０００４】

一実施形態において、医療診断情報にアクセスする方法が開示される。上記の方法は、第１のセンサからの人のパラメータ及び第２のセンサからの上記人のバイオメトリックの測定を取得する段階と、上記第１のセンサ及び第２のセンサからの上記パラメータ及び上記バイオメトリックの上記測定を送信する段階と、移動アクセス端末の信頼されたセキュリティゾーンにおいて実行しているプロセッサにより、上記第１のセンサ及び第２のセンサからの上記パラメータ及び上記バイオメトリックの上記測定を受信する段階であって、上記のセキュリティゾーンは、それによって、通常実行モードにおいて実行している複数のアプリケーションによる、上記第１のセンサ及び第２のセンサからの上記パラメータ及び上記バイオメトリックの上記測定へのアクセスがブロックされる段階とを有する。上記の方法は、上記移動アクセス端末により、上記パラメータ及び上記バイオメトリックの上記測定に基づいて、第１のメッセージを、信頼されたエンドツーエンド通信リンクを介して、医療データサーバに送信する段階であって、上記信頼されたエンドツーエンド通信リンクは、無線通信リンクを含む段階と、上記医療データサーバの信頼されたセキュリティゾーンにおいて実行しているアプリケーションにより、上記第１のメッセージを受信する段階とをさらに有する。上記の方法は、医療データサーバが、パラメータ及びバイオメトリックの測定に基づく第２のメッセージを、信頼されたエンドツーエンド通信リンクを介して、医師に関連付けられたコンピュータに送信する段階と、当該第２のメッセージに基づいて、人に関する医療指示を決定する段階とをさらに有する。

【０００５】
これら及びその他の特徴は、添付の複数の図面及び複数のクレームと併せて、後述の詳細な説明によって、より明確に理解されるであろう。
【図面の簡単な説明】
【０００６】
ここで、本開示をより完全に理解することを目的として、添付の複数の図面及び詳細な説明と併せて、後述の簡単な説明が参照される。ここで、類似の複数の参照番号は、類似の複数の要素を示す。
【図１】図１は、本開示の一実施形態に係る通信システムの一例である。
【図２】図２は、本開示の一実施形態に係る信頼されたエンドツーエンド通信リンクを通して流れるメッセージの一例である。
【図３Ａ】図３Ａは、本開示の一実施形態に係る人体モニタの一例である。
【図３Ｂ】図３Ｂは、本開示の一実施形態に係る医療情報を配信するためのシステムの一例である。
【図４】図４は、本開示の一実施形態に係る方法のフローチャートである。
【図５】図５は、本開示の一実施形態に係る別の方法のフローチャートである。
【図６】図６は、本開示の一実施形態に係る別の方法のフローチャートである。
【図７】図７は、本開示の一実施形態に係る移動アクセス端末の一例である。
【図８】図８は、本開示の一実施形態に係る移動アクセス端末のブロック図である。
【図９Ａ】図９Ａは、本開示の一実施形態に係るソフトウェアアーキテクチャの一例である。
【図９Ｂ】図９Ｂは、本開示の一実施形態に係る別のソフトウェアアーキテクチャの一例である。
【図１０】図１０は、本開示の一実施形態に係るコンピュータシステムのブロック図である。
【発明を実施するための形態】
【０００７】
１又は複数の実施形態の実例となる複数の実施が以下に説明されるが、開示された複数のシステム及び複数の方法は、現在知られているものであろうと、まだ存在しないものであろうと、任意の数の複数の技術を用いて実現され得るということが、最初に理解されるべきである。本開示は、決して、実例となる複数の実施、複数の図面、及び、以下に説明される複数の技術に制限されるべきではないが、それらの複数の均等物の全範囲と共に、添付の複数のクレームの全体の範囲内において、改造されてもよい。
【０００８】
一実施形態において、信頼されたエンドツーエンド通信リンクを提供するシステム及び複数の方法が開示される。信頼された通信は、２つのデバイスの間で確立され得る。それらのそれぞれは、信頼されたセキュリティゾーンにおいて、それらの通信処理を実行している。さらに後述されるとおり、複数の信頼されたセキュリティゾーンは、対象となるプロセッサ及び／又は電子的処理装置が信頼されたセキュリティゾーンにおいて実行している間に、電子的処理装置に潜入した可能性のある複数の不正なアプリケーションが、メモリからの読み出し若しくはそれへの書き込み、複数の入出力装置からの読み出し若しくはそれへの書き込み、又は、複数の通信ポートからの読み出し若しくはそれへの書き込みを行う能力を低下させる。信頼されたセキュリティゾーンにおいて実行する通信アプリケーションは、信頼されていないアプリケーションが、例えば携帯電話のような電子的処理装置上で同時に実行中ではなく、それゆえ、それが通信アプリケーションの複数の活動に干渉したり、当該活動を監視したりすることが妨げられていることについて、高水準の信頼を有し得る。
【０００９】
ネットワーク層及び／又はより高次の複数の層で実行する、エンドツーエンド通信リンク中の全ての通信アプリケーションが、例えば、携帯電話、基地局、メディア・アクセス

・ゲートウェイ、複数のインターネットルータ、複数のスイッチ、複数のサーバコンピュータ及びこれらに類するもののような、対象となる複数の電子的処理装置の複数の信頼されたセキュリティゾーンにおいて実行することを保証することにより、信頼されたエンドツーエンド通信リンクが確立されてよい。第１のノードが、信頼されたエンドツーエンド通信リンクを通して、第２のノードにメッセージを送信する前に、第１のノードは、第２のノードの信頼されたセキュリティゾーンにおいて、第２のノードが第１のノードからの次のメッセージを処理することができるように、前もって準備をするべく、ハンドシェイク又は別の方法で第２のノードと通信を行ってよい。このハンドシェーキングは、第１のノードが第２のノードの信頼されたステータスを確認する段階を含んでもよい。言い換えると、ハンドシェーキングは、第１のノードが、第２のノードが信頼されたエンドツーエンド通信リンクをサポートするように構成されているか否かを評価することを促進する。

【００１０】

電子的なメッセージが、特定のネットワークノードから次のネットワークノードへと通される場合、信頼されたエンドツーエンド通信リンクにおける連続する各ノードは、メッセージが信頼されたエンドツーエンド通信リンクを通過するときにそれによって蓄積された複数のトラストトークンを検査及び確認することで、信頼の連続性（ｃｏｎｔｉｎｕｉｔｙ　ｏｆ　ｔｒｕｓｔ）を確認してよい。複数のトラストトークンは、信頼されたエンドツーエンド通信リンクにおける従前のノード及び／又は複数の従前のノードによって、構築され、提供される。複数のトラストトークンは、例えば、信頼されたセキュリティゾーンにおいて処理されたといった、対象となるメッセージがどのように処理されたかに関する複数の指示又は情報を含み、また、メッセージのある種の出生証明書又は血統書と見做されてもよい。複数のトラストトークンのいくつか又は全部は、複数の信頼されていないノードによる監視又は変更を避けるべく、暗号化されてもよい。複数のトラストトークンは、信頼されたエンドツーエンド通信リンクを介した通信を実施すべく、信頼されたセキュリティゾーンにおいて実行する通信アプリケーション等のセキュアなアプリケーションによって、又は、信頼されたセキュリティゾーン自体によって提供される機能性のベース層及び／又は複数のユーティリティによって、生成されてよい。

【００１１】

例えば、携帯電話の信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションは、第１の信頼されたネットワークノードに、メッセージを送信してよい。メッセージは、コンテンツと、当該メッセージが携帯電話の信頼されたセキュリティゾーンによって生成されたことを確証する、当該携帯電話に関する情報を暗号化する第１のトラストトークンとを含んでよい。メッセージは、第１のトラストトークンを検査することにより、第１の信頼されたネットワークノードによって、信頼され得るものであるか検証されてよい。第１の信頼されたネットワークノードは、次に、第２のトラストトークンを構築し、当該第２のトラストトークンを加えてメッセージを拡張し、当該拡張されたメッセージを第２の信頼されたネットワークノードに送信してよい。メッセージは、第２のトラストトークンを単独で検査することにより、又は、第１及び第２のトラストトークンの両方を検査することにより、第２の信頼されたネットワークノードによって、信頼され得るものであるか検証されてよい。信頼されたエンドツーエンド通信リンクの残りの部分を通して、ネットワーク層、又は、より高次の層においてメッセージを処理する各ネットワークノードは、当該ノードの信頼されたセキュリティゾーンにおいて当該メッセージを処理し、１又は複数のトラストトークンを検査することで信頼の連続性を検証し、付加的なトラストトークンを構築し、当該付加的なトラストトークンを用いて当該メッセージを拡張し、次の信頼されたネットワークノードに、当該メッセージを転送する。信頼されたエンドツーエンド通信リンクの終点（ｅｎｄｐｏｉｎｔ）において、メッセージは、当該メッセージの信頼の連続性が検証されたのち、エンドポイントデバイスの信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションによって使い果たされてよい。代替的な実施形態において、メッセージは、複数のトラストトークンが添付してあるものではなく、メッセージは、連続する信頼されたネットワークノードのそれぞれによって拡

張及び／又は添付されうる単一のトラストトークンが添付してあるものであってもよい。
【００１２】
一実施形態において、信頼されたエンドツーエンド通信リンクは、移動アクセス端末から、仮想プライベートネットワーク（ＶＰＮ）接続を用いた企業ネットワークに向かう基地局（ＢＴＳ）へと広がっていてもよい。基地局の無線インターフェースは、ハッキング攻撃に対して強いと見做されうるので、移動アクセス端末及び基地局の間の接続に関する信頼の連続性は、明確には検証されなくてもよい。企業ネットワークへの仮想プライベートネットワーク接続の信頼の連続性は、同様に、それはハッキング攻撃に対して強いと見做されうるので、明確には検証されなくてもよい。信頼されたエンドツーエンド通信リンクが、その後、ファイアウォールを通して、又は、マルチプロトコル・ラベルスイッチング（ＭＰＬＳ）ポートを通して、企業ネットワークの外へ、インターネットに向かい、また、クラウドコンピューティングサービスにおいて運用されているサーバコンピュータの信頼されたセキュリティゾーン上で実行するセキュアなクラウドレット等のエンドポイントデバイスに向かって拡張する場合、信頼は、複数の対象となるネットワークノード上の複数の信頼されたセキュリティゾーンにおいて実行する複数のアプリケーションのみによって、ネットワーク層又はそれより上の複数の層で処理されている、対象となるメッセージを用いて、上述のようにして提供される。信頼されたセキュリティゾーンのそれぞれは、受信されたメッセージの信頼の連続性を検証し、当該メッセージを次のノードに転送するときに、付加的なトラストトークンを添付し、又は、トラストトークンを拡張する。クラウド中のサーバコンピュータにおいて、セキュアなクラウドレットは、当該サーバコンピュータの信頼されたセキュリティゾーンにおいて実行し、受信されたメッセージ及び／又は信頼されたエンドツーエンド通信リンクの信頼の連続性を検証する。
【００１３】
一実施形態において、モニタ装置は、センサと、バイオメトリック・スキャナ又はセンサとを備える。センサは、血糖値、血液粘度、血圧、体温、血中酸素飽和度、脈拍数、心拍リズム又は別のパラメータ等といった、人のボディパラメータを測定またはサンプリングしてよい。ボディパラメータがサンプリングされるのと同時に、バイオメトリック・スキャナは、ボディパラメータを測定されている人のバイオメトリック署名をキャプチャしてよい。一実施形態において、モニタ装置は、人のボディパラメータのサンプルをとることと、同じ人のバイオメトリック署名をキャプチャすることとが、密接に関連付けられるように構成される。バイオメトリック署名は、人のアイデンティティを確証する及び／又は裏付けるのに用いられてよい。バイオメトリック署名は、指紋、網膜スキャン、人相（顔）スキャン、ＤＮＡ署名又はその他であってよい。移動アクセス端末又はコンピュータの信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションは、モニタ装置から、ボディパラメータのサンプル及びバイオメトリック署名を読み込む。
【００１４】
セキュアなアプリケーションは、その後、ボディパラメータのサンプル及びバイオメトリック署名を医療記録コンテンツにパッケージし、信頼されたトークンを構築し、当該医療記録コンテンツ及び当該信頼されたトークンを含むメッセージを、信頼されたエンドツーエンド通信リンクを通して、医療データサーバの信頼されたセキュリティゾーンにおいて実行し、対応する信頼されたアプリケーションに送信する。代替的に、信頼されたトークンは、信頼されたセキュリティゾーン自体によって提供される機能性のベース層及び／又は複数のユーティリティにより構築されてよい。信頼されたエンドツーエンド通信リンクを介したメッセージの送信は、医療記録コンテンツが、例えば、ＦＤＡ及び／又はＨＩＰＡＡの複数の秘密規定に準じて、秘密に維持されていることを保証し得る。一実施形態において、医療データサーバによって維持される複数の医療記録は、ＦＤＡ及び／又はＨＩＰＡＡの複数の秘密規定に準じていることを保証しながら、様々な目的で、例えば、複数の治効研究を実施する目的で、及び／又は、診断及び患者の治療計画の決定の目的で、複数の医療記録を解析するべく、信頼されたエンドツーエンド通信リンクを通してアクセスされてよい。

【００１５】
信頼されたセキュリティゾーンは、複数のチップセットに、信頼のハードウェア・ルート（ｈａｒｄｗａｒｅ　ｒｏｏｔ）、複数のアプリケーションのためのセキュアな実行環境、及び、複数の周辺機器へのセキュアなアクセスを提供する。信頼のハードウェア・ルート（ｈａｒｄｗａｒｅ　ｒｏｏｔ）は、チップセットが、ただ、機器メーカ又はベンダによって意図された複数のプログラムを実行するだけであるはずであることを意味し、ソフトウェア及び物理的な攻撃に抵抗し、それゆえ、意図されたレベルのセキュリティを提供しているという信頼を維持する。チップセットのアーキテクチャは、複数の有用な資源の機密性及びインテグリティが、複数の特定の攻撃から保護されることを可能にするプログラム可能な環境を促進するように設計されている。信頼されたセキュリティゾーンの複数の能力は、無線及び固定されたハードウェアアーキテクチャの両方の設計における複数の特徴になりつつある。主要なモバイルデバイスのチップセットにおける信頼されたセキュリティゾーンを提供すること、及び、信頼のハードウェア・ルート（ｈａｒｄｗａｒｅ　ｒｏｏｔ）を保護することは、独立したセキュアなハードウェアが、デバイス又はユーザを認証する必要性を取り除く。複数のモバイル金融サービス用のアプリケーション等の信頼されたデータを要求する複数のアプリケーションのインテグリティを確保する目的で、信頼されたセキュリティゾーンは、また、複数の信頼されたアプリケーションのみが動作することができ、複数の攻撃を受ける心配のないセキュアな実行環境を提供する。信頼されたアプリケーションがセキュアな実行環境中で実行されている間、例えば、複数のデータ入力、複数のデータ出力といった、複数の信頼されていないアプリケーションの複数の周辺機器へのアクセスを制限することにより、セキュリティは、さらに促進される。一実施形態において、信頼されたセキュリティゾーンは、ハードウェアによりアシストされたセキュリティとして概念化されてもよい。

【００１６】
完全な信頼された実行環境（ＴＥＥ）は、信頼されたセキュリティゾーンのハードウェア及びソフトウェアアーキテクチャの使用を通じて実現されてよい。信頼された実行環境は、主要なモバイルデバイス用のオペレーティング・システムの実行環境に対応する実行環境である。信頼された実行環境及び／又は信頼されたセキュリティゾーンは、信頼されたセキュリティゾーンにおいて実行する可能性のある複数のアプリケーションを使用するための機能性のベース層及び／又は複数のユーティリティを提供してよい。例えば、一実施形態において、複数のトラストトークンは、複数の通信の信頼の連続性を記録するべく、複数の信頼されたエンドツーエンド通信リンクにおいて使用される信頼された実行環境及び／又は信頼されたセキュリティゾーンの機能性のベース層及び／又は複数のユーティリティによって生成されてよい。複数のアプリケーション・プログラミング・インタフェース（ＡＰＩｓ）の標準化を通して、信頼された実行環境は、複数のセキュアなサービスの拡張性のある配置対象とされ得る場所となった。複数の信頼されたサービス環境において、その上に信頼された実行環境を有するチップセットを備えたデバイスが存在してよい。そこでは、複数の信頼されたサービス環境中の複数のデバイスは信頼されており、複数の攻撃から保護される。信頼された実行環境は、例えば、複数のパーソナルコンピュータ、複数のサーバ、複数のセンサ、複数の医療デバイス、複数のＰＯＳ端末、工業オートメーション、複数の携帯情報端末、自動車用等の複数の他の信頼されたデバイスへの拡張はもちろん、複数の携帯電話及び複数のタブレット上にも実装され得る。

【００１７】
信頼されたセキュリティゾーンは、モバイルデバイスの複数のハードウェア及びソフトウエア資源の全てを、２つのパーティション、すなわち、セキュアなパーティション及び通常の通常のパーティションにパーティショニングすることによって実現されてよい。セキュアなパーティションは、第１の物理プロセッサによって実装されてよく、通常のパーティションは、第２の物理プロセッサによって実装されてよい。代替的に、セキュアなパーティションは、第１の仮想プロセッサによって実装されてよく、通常のパーティションは、第２の仮想プロセッサによって実装されてよい。慎重に扱うべき複数のリソースをセ

キュアなパーティションに配置することで、これらの複数のリソースに対する複数の起こり得る攻撃から保護することができる。例えば、複数の信頼されたソフトウェアアプリケーション等の複数のリソースは、セキュアなパーティションにおいて動作してよく、タッチスクリーン等のハードウェア周辺機器、又は、メモリ中のセキュアな位置にアクセスしてもよい。セキュアなパーティションがアクセスされている間、複数の無線通信機器等の複数の比較的安全性に劣る周辺機器が、完全に機能しないようにされてよい。一方、他の複数の周辺機器は、セキュアなパーティションからのみアクセスされてよい。信頼された実行環境を通してセキュアなパーティションがアクセスされている間、通常のパーティション中のメインのモバイル・オペレーティング・システムは、停止している（ｓｕｓｐｅｎｄｅｄ）。また、通常のパーティション中の複数のアプリケーションは、複数のセキュアな周辺機器及びデータへのアクセスを妨げられる。これにより、複数の不正な（ｃｏｒｒｕｐｔｅｄ）アプリケーション又は複数のマルウェア・アプリケーションが、デバイスの信頼を破壊することを防止する。

【００１８】

信頼されたセキュリティゾーンは、セキュアなサブシステム中に存在し、当該セキュアなサブシステムの外の複数の構成要素にアクセスすることができない複数のハードウェア及びソフトウエア資源をパーティショニングすることで実現される。信頼されたセキュリティゾーンは、信頼されたセキュリティゾーン中に存在するハードウェアロジックを用いて、製造時に、プロセッサ・アーキテクチャ中に構築され、セキュアなパーティションと通常のパーティションとの間の周辺境界（ｐｅｒｉｍｅｔｅｒ　ｂｏｕｎｄａｒｙ）を有効にする。信頼されたセキュリティゾーンは、単に、適切な認証情報を有するものによって操作されるだけであってもよく、一実施形態において、チップの製造後にそれに加えられなくてもよい。セキュアなパーティションをサポートするソフトウェアアーキテクチャは、複数の信頼されたアプリケーションを実行する専用のセキュアなカーネルを用いて提供されてよい。複数の信頼されたアプリケーションは、信頼されたセキュリティゾーンを実現するチップセット上の信頼された実行環境中のアプリケーション・プログラミング・インタフェースを通じて、複数の通常のアプリケーションによりアクセスされうる、独立した複数のセキュアなアプリケーションである。

【００１９】

一実施形態において、複数の通常のパーティション・アプリケーションは、第１の仮想プロセッサ上で実行し、複数のセキュアなパーティション・アプリケーションは、第２の仮想プロセッサ上で実行する。両方の仮想プロセッサは、単一の物理プロセッサ上で動作してもよく、タイムスライスされた方法で実行してもよく、専用のセキュリティ・プロセッサの必要性を取り除いてもよい。タイムスライスされた実行は、セキュアな複数のソフトウェア命令又は複数のハードウェア例外等のしっかりと制御された複数のメカニズムに基づいて、プロセッサの複数のリソースを共有するべく、２つの仮想プロセッサの間の複数のコンテキストを切り替える段階を有する。現在稼動中の仮想プロセッサのコンテキストは保存され、切り替えられた仮想プロセッサのコンテキストは回復され、回復された仮想プロセッサにおいて、処理が再開される。タイムスライスされた実行は、セキュアなパーティションが実行している間、通常のパーティションの実行を中止することにより、信頼されたセキュリティゾーンを保護する。

【００２０】

２つの仮想プロセッサのコンテキストは、現在稼動中の仮想プロセッサを変更するときに、モニタモードと呼ばれるプロセッサモードを介して、切り替わる。プロセッサが、通常のパーティションからモニタモードに入ることを可能とする複数のメカニズムは、しっかりと制御される。　モニタモードへのエントリは、専用の命令若しくはセキュアなモニタのコール（ＳＭＣ）命令を実行するソフトウェアによって、又は、プロセッサのモニタモードへの切替えを引き起こすように構成され得る、複数のハードウェア割込み等の複数のハードウェア例外メカニズムのサブセットによって、引き起こされてよい。モニタモードの範囲内で実行するソフトウェアは、その後、動作している仮想プロセッサのコンテキ

ストを保存し、セキュアな仮想プロセッサに切り替える。

【００２１】

信頼されたセキュリティゾーンは、複数のデバイスユーザにアクセスすることができない独立したオペレーティング・システムを実行する。セキュリティの目的で、信頼されたセキュリティゾーンは、複数のアプリケーションのインストールに関して、複数のユーザに開放されていない。つまり、複数のユーザは、信頼されたセキュリティゾーンに複数のアプリケーションをインストールする手段をもたない。これにより、複数の不正な（ｃｏｒｒｕｐｔｅｄ）アプリケーション又は複数のマルウェア・アプリケーションが、予約された複数の強力な命令を信頼されたセキュリティゾーンに対して実行することを防止する。そして、それにより、デバイスの信頼を保護する。携帯電話の複数のハードウェア及びソフトウエア資源を、それらが、セキュリティサブシステム用途向けのセキュアなパーティション及び他の全ての用途向けの通常のパーティションという２つのパーティションの一方に存在するようにパーティショニングすることにより、少なくとも部分的に、システムのセキュリティが達成される。信頼されたセキュリティゾーンをセキュアなパーティション中に配置して、通常のパーティションからのアクセスを制限することにより、ソフトウェア及び基本ハードウェアへの複数の攻撃から保護する。ハードウェアロジックは、セキュアなパーティションのリソースが、通常のパーティションの複数の構成要素又は複数のアプリケーションによって、全くアクセスされることがないことを確保する。専用のセキュアなパーティションのオペレーティング・システムは、同様にそれ用の仮想プロセッサにおいて実行する通常のパーティションのオペレーティング・システムから独立した仮想プロセッサ上で動作する。複数のユーザは、上述の通常のパーティションのオペレーティング・システムにおいて実行しうる複数のアプリケーションを、モバイルデバイス上にインストールしてよい。信頼されたセキュリティゾーンは、モバイルデバイスの製造業者又はベンダによってインストールされた、セキュアなパーティション向けの独立したオペレーティング・システムを実行し、複数のユーザは、新たな複数のアプリケーションをインストールしたり、信頼されたセキュリティゾーンの複数のコンテンツを変更することができない。

【００２２】

ここで、図１に戻ると、信頼されたエンドツーエンド通信リンクを提供するための第１のシステム１００が開示される。一実施形態において、システム１００は、移動アクセス端末（ＭＡＴ）１０２と、基地局（ＢＴＳ）１０４と、複数のネットワークノード１０６と、クラウドコンピューティング設備１１０内に配されたサーバコンピュータの信頼されたセキュリティゾーン１３８において実行するセキュアなクラウドレット１０８とを備える。ＭＡＴ１０２は、携帯電話、パーソナルデジタルアシスタント（ＰＤＡ）、メディアプレーヤ、ラップトップコンピュータ、タブレットコンピュータ、ノートパッドコンピュータ又はその他のポータブル通信デバイスの何れかであってよい。複数のネットワークノード１０６は、第１のネットワークノード１０６ａと、第２のネットワークノード１０６ｂと、第３のネットワークノード１０６ｃとを有してよい。システム１００は、任意の数のネットワークノード１０６を有してよいことが理解される。複数のネットワークノード１０６は、複数のネットワークルータ、複数のネットワークスイッチ、複数のメディア・アクセス・ゲートウェイ（ＭＡＧｓ）、及び、その他のデータ通信ネットワーク装置の何れかであってよい。複数のネットワークノード１０６は、ネットワーククラウドとして、又は、通信インフラストラクチャとして抽象化されてよい。後述の説明はＭＡＴ１０２に言及する一方、その内容の少なくともいくらかは、無線接続によってではなく、有線接続によって複数のネットワークノード１０６と連結されるデスクトップコンピュータ又は他の実質的に動かせないコンピュータによって実現されてもよいことが理解される。

【００２３】

基地局１０４は、ＭＡＴ１０２への無線通信リンクを提供してよく、ＭＡＴ１０２から複数のネットワークノード１０６、例えば、第１のネットワークノード１０６ａへのエッジアクセスを提供してもよい。基地局１０４は、符号分割多重アクセス（ＣＤＭＡ）、グ

ローバルシステム・フォー・モバイルコミュニケーションズ（ＧＳＭ（登録商標））、ロング・ターム・エボリューション（ＬＴＥ）、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス］（ＷｉＭＡＸ（登録商標））、又は、その他の無線通信プロトコルのうちの１又は複数に準じた無線通信リンクを提供してよい。

【００２４】

一実施形態において、ＭＡＴ１０２は、無線トランシーバ１２０と、信頼されたセキュリティゾーン１３０と、セキュアなアプリケーション１３２とを備える。例えば、無線トランシーバ１２０は、符号分割多重アクセス（ＣＤＭＡ）、グローバルシステム・フォー・モバイルコミュニケーションズ（ＧＳＭ（登録商標））、ロング・ターム・エボリューション（ＬＴＥ）、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス］（ＷｉＭＡＸ（登録商標））、又は、その他の無線通信プロトコルのうちの１又は複数に準じた無線通信リンクを提供するよう機能するセルラー通信トランシーバを含んでよい。ＭＡＴ１０２は、無線トランシーバ１２０に加えて、例えば、近距離無線通信（ＮＦＣ）無線トランシーバ、ブルートゥース（登録商標）無線トランシーバ、ＷｉＦｉ無線トランシーバ、又は、その他の短距離無線トランシーバといった、複数の他の無線トランシーバを備えてよい。

【００２５】

上述のとおり、信頼されたセキュリティゾーン１３０は、物理的に分離したプロセッサによって、又は、仮想プロセッサによって、提供されてよい。セキュアなアプリケーション１３２は、秘密情報を処理及び／又は送信する様々なアプリケーションの何れかであってよい。秘密情報は、電子メール、マーケティング資料、複数のビジネスプラン、複数のクライアントリスト、複数のアドレス、従業員データ、複数の知的財産文書及びこれらに類するもの等の複数の慎重に扱うべきビジネス文書を含んでよい。秘密情報は、複数の政府規制機関又は複数の商業規格によって強制されるプライバシー要求事項（ｐｒｉｖａｃｙ　ｒｅｑｕｉｒｅｍｅｎｔｓ）の対象となる複数の個人の医療記録又は医療データを含んでよい。秘密情報は、複数の口座番号、複数の認証用識別情報、勘定残高情報及びこれらに類するもの等の金融情報を含んでよい。

【００２６】

秘密情報を処理及び／又は送信する場合、セキュアなアプリケーション１３２は、少なくとも部分的に、信頼されたセキュリティゾーン１３０において実行する。さらに十分に上述されたとおり、セキュアなアプリケーション１３２が信頼されたセキュリティゾーン１３０において実行する場合に、複数の信頼されていないアプリケーションによる、実行、並びに／又は、複数の信頼されたメモリパーティションへのアクセス及び／若しくはＭＡＴ１０２のディスプレイ若しくは複数の入力デバイスへのアクセスが妨げられ、それによって、ＭＡＴ１０２に潜入していた可能性があるマルウェアが、秘密情報を破損したり、監視したりする機会を減少させることは、信頼されたセキュリティゾーン１３０の特性又は特徴である。セキュアなアプリケーション１３２により、秘密情報が、信頼されたエンドツーエンド通信リンクを介して、セキュアなクラウドレット１０８に送信された場合、信頼されたセキュリティゾーン１３０は、内容部又はメッセージのコンテンツと称されてもよい秘密情報と、第１のトラストトークンとを含むメッセージを構築する。いくつかの文脈において、メッセージは、内容部及び第１のトラストトークンを結合する又はカプセル化すると称されてもよい。第１のトラストトークンは、別の信頼されたセキュリティゾーンによって、メッセージの信頼レベルを検証するべく用いられる可能性のある情報を含んでよい。第１のトラストトークンは、例えば、信頼されたセキュリティゾーン１３０において処理されたといった、メッセージがどのように処理されたかに関する複数の指示（インジケータ）又は情報を含んでよく、また、メッセージのある種の出生証明書又は血統書と見做されてもよい。複数のトラストトークンのいくらか又は全部は、複数の信頼されていないノードによる監視又は変更を避けるべく、暗号化されてよい。いくつかの文脈において、メッセージに結合、カプセル化又は添付されたトラストトークン又は複数のトラストトークンを解析することによる、メッセージの信頼レベルの検証は、メッセージの

信頼の連続性の検証、及び／又は、信頼されたエンドツーエンド通信リンクの少なくとも一部の信頼の連続性の検証と称されてよい。

【００２７】

複数のネットワークノード１０６のそれぞれは、信頼されたセキュリティゾーン１３６を含む。いくつかの文脈において、複数のネットワークノード１０６は、複数の信頼されたネットワークノード又は複数の信頼されたノードと称されてよい。第１のネットワークノード１０６ａは、第１の信頼されたセキュリティゾーン１３６ａを含み、第２のネットワークノード１０６ｂは、第２の信頼されたセキュリティゾーン１３６ｂを含み、第３のネットワークノード１０６ｃは、第３の信頼されたセキュリティゾーン１３６ｃを含む。一実施形態において、複数のネットワークノード１０６は、単独で、専ら、複数の信頼されたエンドツーエンド通信リンクを提供してもよく、信頼されていないメッセージ・トラフィックを全く運搬しなくてもよい。代替的に、複数のネットワークノード１０６は、信頼されたメッセージ・トラフィック及び信頼されていないメッセージ・トラフィックの両方を運搬してもよく、信頼されたメッセージを処理するときに、全ての信頼されていない信頼されていないメッセージ・トラフィックの処理を一時的に停止してもよい。一実施形態において、開放型システム間相互接続（ＯＳＩ）モデルのネットワーク層又はより上位の層でメッセージを処理しない複数の通信装置は、信頼されていると推定され、信頼されたエンドツーエンド通信リンクに従ってメッセージを転送する前に、メッセージの信頼の連続性を検証する義務はない。

【００２８】

インターネット・プロトコルは、ネットワーク層プロセスの一例であり、転送制御プロトコル（ＴＣＰ）は、ネットワーク層より上位の層で複数のメッセージを処理するプロセスの一例である。複数のデータ通信ハブ及び基地局１０４は、ネットワーク層又はより上位の層で複数のメッセージを処理しない複数の通信装置又は複数のノードの複数の例である。しかしながら、別の実施形態において、より下位の層の複数の通信装置は、メッセージの信頼の連続性をいくらか検証する。

【００２９】

一実施形態において、特定のネットワークノード１０６において、ネットワーク層又はより上位の複数の通信層のそれぞれでメッセージを処理することが、対象となるネットワークノード１０６の信頼されたセキュリティゾーン１３６において、少なくとも部分的に実行する１又は複数のアプリケーションによって実施される。例えば、第１のネットワークノード１０６ａが、ＩＰ層及びＵＤＰ層の両方においてメッセージを処理する場合、ＩＰ層における処理は、信頼されたセキュリティゾーン１３６ａにおいて少なくとも部分的に実行するアプリケーションにより実施され、ＵＤＰ層におけるメッセージの処理は、信頼されたセキュリティゾーン１３６ａにおいて少なくとも部分的に実行するアプリケーションにより実施される。一実施形態において、信頼されたトークンが生成され、第１の通信層でメッセージを処理するアプリケーションによって、メッセージと関連付けられてよい。第２の信頼されたトークンが生成され、第２の通信層でメッセージを処理するアプリケーションによって、メッセージと関連付けられてよい。例えば、ＩＰ通信層でメッセージを処理し、信頼されたセキュリティゾーン１３６ａにおいて少なくとも部分的に実行する第１のアプリケーションは、第１のトラストトークンを生成して、それをメッセージに関連付けてよい。ＵＤＰ通信層でメッセージを処理し、信頼されたセキュリティゾーン１３６ａにおいて少なくとも部分的に実行する第２のアプリケーションは、第２のトラストトークンを生成して、それをメッセージに関連付けてよい。　一実施形態において、第１及び第２のトラストトークンは、第１及び第２のアプリケーションによって呼び出される、信頼されたセキュリティゾーン１３６ａの機能性のベース層及び／又は複数のユーティリティによって生成されてよい。

【００３０】

メッセージがネットワークノード１０６によって受信されると、当該メッセージは、信頼されたセキュリティゾーン１３６によって処理されるべきメッセージとして認定される

。例えば、メッセージは、メッセージのフィールドによって、又は、メッセージ中のトラストトークンの存在によって、信頼されたメッセージとして認定されてよい。メッセージは、例えば、メッセージ中にカプセル化されている、又は、メッセージと関連付けられている可能性のある１又は複数のトラストトークンを検査することによって、メッセージの信頼レベルを決定するべく、信頼されたセキュリティゾーン１３６によって解析される。メッセージの処理、トラストトークンの生成及びメッセージの送信は、ネットワークノード１０６の信頼されたセキュリティゾーン１３６において実施される。新たなトラストトークンは、メッセージの信頼レベルを検証するべく、例えば、対象となるネットワークノードが、メッセージの信頼連続性を維持するように、当該メッセージを処理したことを検証するべく、別の信頼されたセキュリティゾーンによって用いられうる情報を含む。

【００３１】

メッセージが信頼されたエンドツーエンド通信リンクを通過して、クラウドコンピューティング設備１１０内に配されたサーバの信頼されたセキュリティゾーン１３８により受信されると、当該メッセージの信頼の連続性が維持されてきたことと、当該メッセージの信頼レベルが十分であることとを決定するべく、メッセージの信頼レベルが解析される。一実施形態において、信頼レベルは、例えば、０から１、０から１０、１から１０、０から１００、１から１００又はいくらかの他の数値範囲にわたるような、複数の数値の範囲にわたって変動する性能指数であってよい。複数の数値は、複数の整数の値又は複数の小数の値であってよい。代替的に、信頼レベルは、信頼されている又は信頼されていないのどちらかといった、２進値であってよい。別の実施形態において、いくらかの他の信頼レベルの尺度が実装されてよい。メッセージの信頼レベルが十分である場合、メッセージは、信頼されたセキュリティゾーン１３８において実行するセキュアなクラウドレット１０８に提供され、セキュアなクラウドレット１０８は、当該メッセージを消費する。例えば、セキュアなクラウドレット１０８は、メッセージのコンテンツのデータストアへの格納、コンテンツの解析、コンテンツと既に受信された他のコンテンツとの統合、及び／又は、他の処理を含む、様々な方法のうちの任意のもので、メッセージを処理してよい。

【００３２】

メッセージを処理する前に、まず、当該メッセージの信頼の連続性を検証する信頼されたセキュリティゾーンにおいて、少なくとも部分的に実行する複数のアプリケーションによって、ネットワーク層及び上位の層におけるメッセージの処理が実施されるので、上述の通信インフラストラクチャ及び処理方法は、信頼されたエンドツーエンド通信リンクを提供すると言える。上記のインフラストラクチャ及び処理方法は、例えば、セキュアなクラウドレット１０８のような、メッセージの内容が傍受、コピー及び／又は変更されていないという高水準の信頼を有することができる通信エンドポイントの普及を推進する。

【００３３】

次に、図２に移ると、信頼されたエンドツーエンド通信リンクを用いたメッセージ伝搬の一例が開示される。ＭＡＴ１０２は、コンテンツ１５２及び第１のトラストトークン１５４ａを含む第１のメッセージ１５０を構築する。例えば、信頼されたセキュリティゾーン１３０、及び／又は、信頼されたセキュリティゾーン１３０において実行するセキュアなアプリケーション１３２は、コンテンツ１５２を生成し、第１のトラストトークン１５４ａを構築し、コンテンツ１５２及び第１のトラストトークン１５４ａから第１のメッセージ１５０を組み立てる。上述のとおり、複数のトラストトークンは、メッセージの信頼レベルを検証するべく、別の信頼されたセキュリティゾーンにより用いられる可能性のある情報を含む。複数のトラストトークンは、出生証明書及び／又は血統書と類推されるものであってよい。トラストトークンは、暗号化データ、及び／又は、送信ネットワーク要素がメッセージの信頼の連続性を維持してきたことを保証するべく、信頼されたセキュリティゾーンによって復号されうる複数の識別コードを含んでよい。複数の識別コードは、ネットワークノード１３６、又は、信頼されたエンドツーエンド通信リンクのパス中の他の通信装置を特定する。ＭＡＴ１０２及び／又は信頼されたセキュリティゾーン１３０は、第１のメッセージ１５０を第１のノード１０６ａに送信する。

【００３４】
第１のノード１０６ａは、第１のメッセージ１５０を解析して、第１のメッセージ１５０の信頼の連続性を検証することにより、第１の信頼されたセキュリティゾーン１３６ａにおいて第１のメッセージ１５０を処理する。例えば、第１の信頼されたセキュリティゾーン１３６ａ、又は、第１の信頼されたセキュリティゾーン１３６ａにおいて実行するセキュアな通信アプリケーションが、第１のトラストトークン１５４ａを読み込み、妥当性を確認する。そして、それは、第１のメッセージ１５０の信頼の連続性の検証と称されてもよい。一実施形態において、第１の信頼されたセキュリティゾーン１３６ａは、第１のメッセージ１５０の信頼レベルを決定してよい。第１のメッセージ１５０が許容範囲内の信頼レベルを有する場合、第１の信頼されたセキュリティゾーン１３６ａは、第２のトラストトークン１５４ｂを構築し、コンテンツ１５２、第１のトラストトークン１５４ａ及び第２のトラストトークン１５４ｂから第２のメッセージ１５６を組み立てる。代替的に、第２のメッセージ１５６は、第１のトラストトークン１５４ａを含まなくてもよく、第２のトラストトークン１５４ｂは、第１のメッセージ１５０の信頼の連続性を検証するときに第１の信頼されたセキュリティゾーン１３６ａによって決定された、信頼のレベルに関する情報を含んでよい。第１のネットワークノード１０６ａ及び／又は第１の信頼されたセキュリティゾーン１３６ａは、第２のメッセージ１５６を第２のネットワークノード１０６ｂに送信する。
【００３５】
第２のネットワークノード１０６ｂは、第２のメッセージ１５６を解析して、第２のメッセージ１５６の信頼の連続性を検証することで第２のメッセージ１５６を第２の信頼されたセキュリティゾーン１３６ｂにおいて処理し、第３のトラストトークン１５４ｃを構築し、第１のトラストトークン１５４ａ、第２のトラストトークン１５４ｂ及び第３のトラストトークン１５４ｃを含む第３のメッセージ１５８を構築する。代替的に、第３のトラストトークン１５４ｃのみが第３のメッセージ１５８中にカプセル化されていてもよく、第１のネットワークノード１０６ａにより決定された第１のメッセージ１５０に関連付けられた信頼レベルと、第２のネットワークノード１０６ｂにより決定された第２のメッセージ１５６に関連付けられた信頼のレベルとに関する情報は、第３のトラストトークン１５４ｃに含まれていてもよい。第２のネットワークノード１０６ｂ及び／又は第２の信頼されたセキュリティゾーン１３６ｂは、第３のメッセージ１５８を、第３のネットワークノード１０６ｃに送信する。
【００３６】
第３のネットワークノード１０６ｃは、第３のメッセージ１５８を処理し、同様の方法で、第４のトラストトークン１５４ｄを含む第４のメッセージ１６０を構築し、第４のメッセージ１６０を信頼されたセキュリティゾーン１３８及び／又はセキュアなクラウドレット１０８に送信する。信頼されたエンドツーエンド通信リンクを用いたコンテンツ１５２の伝搬が、異なる話し方又は異なる抽象化に従って、異なるけれども関連する複数のメッセージ－第１のメッセージ１５０、第２のメッセージ１５６、第３のメッセージ１５８及び第４のメッセージ１６０－の話によって開示され、そのリンクを通過中のメッセージが拡張される又は漸進的に組み立てられる、信頼されたエンドツーエンド通信リンクを通して、メッセージが伝搬すると言えるであろう。一実施形態において、トラストトークン又は複数のトラストトークンが、複数のメッセージ１５０、１５６、１５８及び１６０中にカプセル化されるのではなく、トラストトークン及び／又は複数のトラストトークンが、複数のメッセージ１５０、１５６、１５８及び１６０に関連付けられてもよい。例えば、ＩＰパケットの単一のペイロード内に含まれることによって関連付けられる。
【００３７】
複数のメッセージ１５０、１５６、１５８及び１６０のそれぞれは、データパケットのペイロードとして、例えば、ＩＰパケット又はＩＰデータグラムのペイロードとして、カプセル化されてよい。コンテンツ１５２及び１又は複数のトラストトークン１５４のサイズに応じて、コンテンツ１５２は、複数のセグメントに分割されてよく、上述のとおり、

メッセージにおいて、各セグメントは、別々に送信されてよい。信頼されたエンドツーエンド通信リンクが、任意の数のネットワークノード１０６を含んでよいこと、及び、任意の数の対応するメッセージが、ＭＡＴ１０２からセキュアなクラウドレット１０８へのコンテンツ１５２の通信中に構築されてよいことが理解される。

【００３８】

次に、図３Ａ及び図３Ｂに移ると、モニタ１７２と、信頼されたエンドツーエンド通信リンクを提供する第２のシステム１７８とが開示される。一実施形態において、モニタ１７２は、生体認証センサー１７４と、人体パラメータセンサ１７６とを含む。複数の信頼されたネットワークノード１０６ａ、１０６ｂ及び１０６ｃは、ネットワーク１９０の複数の部分として抽象化されてよい。ネットワーク１９０は、複数の付加的なノード及び／又は複数の通信装置を含んでよく、１又は複数のパブリック・ネットワーク、プライベート・ネットワーク又はそれらの組合せを含んでもよい。ボディパラメータセンサ１７６は、血糖値、血液粘度、血圧、体温、血中酸素飽和度、脈拍数、心拍リズム又は別のボディパラメータ等の人１７０のボディパラメータを測定又はサンプリングしてよい。いくつかの文脈において、ボディパラメータセンサ１７６は、トランスデューサ、又は、トランスデューサを含むものと見做されてよい。ボディパラメータセンサ１７６は、標準的な測定値に直接的には関連しない可能性のある複数の未処理データの値をキャプチャしてもよく、当該複数の未処理データの値は、別のデバイスにより処理されてもよい。例えば、検知されたパラメータの値を、複数の標準的な又は普通の単位で示すべく、ＭＡＴ１０２の信頼されたセキュリティゾーン１３０において実行するセキュアなアプリケーション１３２によって処理されてよい。例えば、セキュアなアプリケーション１３２は、未処理データに基づいて、血液粘度の国際標準化比（ＩＮＲ）の値を決定するべく、モニタ１７２及び／又はボディパラメータセンサ１７６から受信された血液粘度の未処理データを処理してよい。　代替的に、ボディパラメータセンサ１７６及び／又はモニタ１７２は、未処理データ（生データ）を処理して、これらのボディパラメータ値を、複数の標準的な単位で出力してもよい。

【００３９】

生体認証センサー１７４は、例えば、指紋、網膜スキャン、人相（顔）スキャン、ＤＮＡ署名又はその他のバイオメトリック署名といった、人１７０のバイオメトリック署名をキャプチャする。いくつかの文脈において、生体認証センサー１７４は、バイオメトリック・スキャナと称されてよい。一実施形態において、生体認証センサー１７４及びボディパラメータセンサ１７６は、バイオメトリック署名及びボディパラメータの値を、実質的に同時にキャプチャしてよい。一実施形態において、モニタ１７２は、ボディパラメータセンサ１７６によりボディパラメータの値を感知するプロセスと、生体認証センサー１７４によりバイオメトリック署名をキャプチャするプロセスとが、分離できない複数のプロセスであるように構成されてよい。例えば、一実施形態において、ボディパラメータセンサ１７６及び生体認証センサー１７４は、例えば、指紋のバイオメトリックをもキャプチャする酸素濃度計のクランプのように、単一のパッケージに統合されている。当業者に知られているように、標準的な酸素濃度計のクランプは、脈拍数及び血中酸素飽和の割合を読むべく、指に固定されてよい。バイオメトリック署名は、人１７０のアイデンティティを特定及び／又は裏付けることを目的として、ボディパラメータの値に関連付けられてよい。

【００４０】

モニタ１７２は、例えば、有線通信リンクを用いて、又は、ＮＦＣ、ブルートゥース（登録商標）若しくは複数のＷｉＦｉ（登録商標）無線リンク等の短距離無線通信リンクを用いて、ＭＡＴ１０２に通信可能に連結されてよい。モニタ１７２は、ボディパラメータの値及びバイオメトリック署名を、ＭＡＴ１０２の信頼されたセキュリティゾーン１３０において実行するセキュアなアプリケーション１３２に送信する。モニタ１７２からＭＡＴ１０２への通信は、信頼されている及び／又は実質的にハッキングに強いと想定される。セキュアなアプリケーション１３２は、ボディパラメータの値及びバイオメトリック署

名を含む医療記録コンテンツを生成してよい。バイオメトリック署名は、１又は複数の方法で、符号化及び／又は圧縮されてもよく、プログラムの形態で医療記録コンテンツ中にカプセル化されてもよい。一実施形態において、医療記録コンテンツは、日付及びその日における時間等の付加的なサポート情報を含んでよい。セキュアなアプリケーション１３２は、医療記録コンテンツ及びトラストトークンを含むメッセージを生成して、当該メッセージを信頼されたエンドツーエンド通信リンクを通して、医療データサーバ１８０の信頼されたセキュリティゾーン１８２において実行するセキュアなアプリケーション１８４に送信してよい。信頼されたエンドツーエンド通信リンクを通したメッセージの伝搬は、上述のプロセスと実質的に同様であってよい。

【００４１】

セキュアなアプリケーション１８４は、医療記録コンテンツを、医療データサーバ１８０に連結されたデータストア１８６に格納することを提供してよい。セキュアなアプリケーション１８４、又は、医療データサーバ１８０の信頼されたセキュリティゾーン１８２において実行する異なるセキュアなアプリケーションは、人１７０の慢性的な状態を追跡するべく、単一の人１７０の複数の医療記録コンテンツを処理してよい。代替的に、セキュアなアプリケーション１８４は、例えば、治療又は薬物の有効性を計算するべく、複数の選択された人１７０に関連付けられた複数の医療記録コンテンツを処理する。

【００４２】

一実施形態において、医療データ解析装置１９２の信頼されたセキュリティゾーン１９４において実行するセキュアなアプリケーション１９６は、医療データサーバ１８０からの複数の医療記録コンテンツを要求する。そして、医療データサーバ１８０は、要求された複数の医療記録コンテンツを、上述したような信頼されたエンドツーエンド通信リンクを介して、送信する。複数の医療記録は、複数の検証可能な形で秘密な医療記録と称されてよい。状況しだいで、ＦＤＡ等の複数の規制機関は、複数の医療記録秘密規定に準じていることを裏付けるべく、複数の医療記録の使用及び通信を調査してよい。セキュアなアプリケーション１９６は、人１７０の状態を診断する、及び／又は、その人のための治療プログラムを提言するべく、複数の医療記録コンテンツを解析してよい。医療データ解析装置１９２を使用する医師は、例えば、人１７０向けの処方箋を書いて、人１７０によって習慣的に用いられている薬局に処方箋を送信してよい。セキュアなアプリケーション１９６は、治療又は薬物の有効性を決定するべく、複数の人１７０の複数の医療記録を解析してよい。

【００４３】

次に、図４に移ると、方法２００が開示される。ブロック２０２において、第１のセンサにより人のパラメータの測定が取得され、第２のセンサにより人のバイオメトリックが取得される。例えば、上述したとおり、ボディパラメータセンサ１７６により人のパラメータが取得され、生体認証センサー１７４により人のバイオメトリック署名が取得される。ブロック２０４において、複数のセンサからの入力は、プロセッサの信頼されたセキュリティゾーンにおいて実行するセキュアなアプリケーションにより受信される。そこでは、プロセッサの通常のパーティションにおいて実行する複数のアプリケーションによる複数のセンサからの入力へのアクセスがブロックされる。複数のセンサからの入力は、人のパラメータの測定と、人のバイオメトリックとを含む。ブロック２０６において、複数のセンサからの入力に基づくメッセージは、信頼されたエンドツーエンド通信リンクを介して、医療データサーバに送信される。メッセージを受信するアプリケーションは、サーバの信頼されたセキュリティゾーンにおいて実行する。メッセージは、上述の第１のメッセージ１５０と実質的に同様であってよく、内容部と、１又は複数のトラストトークンとを含んでよい。

【００４４】

次に、図５に移ると、方法２２０が開示される。ブロック２２２において、通信アプリケーションは、移動アクセス端末の信頼されたセキュリティゾーンにおいて実行される。例えば、上述のとおり、セキュアなアプリケーション１３２は、ＭＡＴ１０２の信頼され

たセキュリティゾーン１３０において実行する。ブロック２２４において、メッセージが、移動アクセス端末から、信頼されたエンタープライズ・エッジノードの信頼されたセキュリティゾーンにおいて実行する信頼された通信アプリケーションに送信される。例えば、セキュアなアプリケーション１３２及び／又は信頼されたセキュリティゾーン１３０は、コンテンツ１５２及びトラストトークン１５４を含むメッセージ１５０を構築し、メッセージ１５０を第１のネットワークノード１０６ａに送信する。一実施形態において、メッセージは、仮想プライベートネットワーク（ＶＰＮ）セッションを介して、ＭＡＴ１０２から、企業の通信ネットワーク（ｅｎｔｅｒｐｒｉｓｅ ｃｏｍｍｕｎｉｃａｔｉｏｎ ｎｅｔｗｏｒｋ）に送信されてよい。メッセージは、企業の通信ネットワーク（ｅｎｔｅｒｐｒｉｓｅ ｃｏｍｍｕｎｉｃａｔｉｏｎ ｎｅｔｗｏｒｋ）の外側のデバイス又はサービスに向けられてもよく、それから、外部のインターネット中を伝搬してよい。第１のネットワークノード１０６ａは、企業のファイアウォール又はルータのマルチプロトコル・ラベルスイッチング・ポートであってもよい。 このように、この実施形態において、企業ネットワーク・エッジは、企業ネットワークから、複数の外部デバイス及び／又は複数の外部の機能への信頼されたエンドツーエンド通信リンクをサポートするべく、信頼されたセキュリティゾーンを有してよい。ブロック２２６において、メッセージは、上述したようなメッセージの伝搬中の信頼の連続性を提供するための複数のプロセスにしたがって、信頼されたエンタープライズ・エッジノードから、クラウドベースのサーバの信頼されたセキュリティゾーン上で実行する信頼されたクラウドレットへと送信される。

【００４５】

次に、図６に移ると、方法２４０が開示される。ブロック２４２において、第１のセンサにより人のパラメータの測定が取得され、第２のセンサにより人に由来するバイオメトリックが取得される。例えば、ボディパラメータセンサ１７６は、パラメータ値を取得し、生体認証センサー１７４は、人１７０のバイオメトリック署名を取得する。ブロック２４４において、パラメータの測定及びバイオメトリック署名が、複数のセンサから送信される。例えば、パラメータ値及びバイオメトリック署名が、モニタ１７２からＭＡＴ１０２へと送信される。ブロック２４６において、パラメータの測定及びバイオメトリック署名が、複数のセンサから、移動アクセス端末の信頼されたセキュリティゾーンにおいて実行するプロセッサによって受信される。そこでは、通常実行モードにおいて実行する複数のアプリケーションによる、複数のセンサからのパラメータの測定及びバイオメトリックへのアクセスがブロックされる。例えば、パラメータ及びバイオメトリック署名は、ＭＡＴ１０２の信頼されたセキュリティゾーン１３０において実行するセキュアなアプリケーション１３２によって受信される。

【００４６】

ブロック２４７において、第１のメッセージは、移動アクセス端末によるパラメータ及びバイオメトリックの測定に基づいて、信頼されたエンドツーエンド通信リンクを介して、医療データサーバに送信される。信頼されたエンドツーエンド通信リンクは、無線通信リンクを含む。例えば、第１のメッセージは第１のメッセージ１５０であり、無線通信リンクは、無線トランシーバ１２０と基地局１０４との間で確立される。

【００４７】

ブロック２４８において、第１のメッセージは医療データサーバの信頼されたセキュリティゾーンにおいて実行するアプリケーションによって受信される。ブロック２５０において、パラメータの測定及びバイオメトリックに基づく第２のメッセージは、医療データサーバにより、信頼されたエンドツーエンド通信リンクを介して、医師に関連付けられたコンピュータに送信される。ブロック２５２において、人のための医療指示が、第２のメッセージに基づいて、決定される。例えば、医療データ解析装置１９２を使用する医師は、人１７０の状態又はステータスを診断し、当該状態又はステータスを治療するための医薬品を処方する。

【００４８】

図７は、モバイルデバイス４００を含む無線通信システムを示す。図４は、モバイルデ

バイス４００を描写する。それは、本開示の複数の側面を実装するために動作可能であるが、本開示は、これらの複数の実装に制限されるきではない。一実施形態において、移動アクセス端末１０２は、モバイルデバイス４００として実現されてよい。携帯電話として説明されているが、モバイルデバイス４００は、無線ハンドセット、ポケットベル（登録商標）、パーソナルデジタルアシスタント（ＰＤＡ）、ゲーム機又はメディアプレーヤを含む、複数の様々な形態を成してもよい。モバイルデバイス４００は、ディスプレイ４０２と、ユーザによる入力のためのタッチセンサ面及び／又は複数のキー４０４とを備える。モバイルデバイス４００は、ユーザが選択するための複数のオプション、ユーザが作動させるための複数の制御、及び／又は、ユーザが指図するための複数のカーソル若しくは複数の他の指標（インジケータ）を提示してよい。モバイルデバイス４００は、さらに、複数のダイヤル番号又はハンドセットの動作を設定するための複数の様々なパラメータ値を含む、ユーザからのデータ入力を受け取ってよいモバイルデバイス４００は、さらに、複数のユーザコマンドに応じて、１又は複数のソフトウェアアプリケーションまたはファームウェアアプリケーションを実行してよい。これらの複数のアプリケーションは、ユーザとのインタラクションに応じて、様々な複数のカスタマイズされた機能を実行するようにモバイルデバイス４００を構成してもよい。更に、モバイルデバイス４００は、例えば、無線基地局、無線アクセスポイント、又は、ピア・モバイルデバイス４００から、無線通信でプログラム及び／又は構成されてもよい。モバイルデバイス４００は、ディスプレイ４０２がウェブページを示することを可能にするウェブブラウザアプリケーションを実行してもよい。ウェブページは、基地局、無線ネットワークアクセスノード、ピア・モバイルデバイス４００又は任意のほかの無線通信ネットワーク若しくはシステムとの無線通信を介して、取得されてもよい。

【００４９】

図８は、モバイルデバイス４００のブロック図を示す。複数のハンドセットの複数の様々な周知の構成要素が描写される。一方で、一実施形態において、列挙される複数の構成要素のサブセット及び／又は列挙されていない複数の付加的な構成要素が、モバイルデバイス４００内に含まれてよい。モバイルデバイス４００は、デジタル信号プロセッサ（ＤＳＰ）５０２と、メモリ５０４とを含む。示されるように、モバイルデバイス４００は、さらに、アンテナ及びフロントエンドユニット５０６と、無線周波数（ＲＦ）送受信機５０８と、ベースバンド処理ユニット５１０と、マイク５１２と、イヤホンスピーカ５１４と、ハンドセットポート５１６と、入／出力インタフェース５１８と、取り外し可能メモリカード５２０と、ユニバーサルシリアルバス（ＵＳＢ）ポート５２２と、赤外線ポート５２４と、バイブレータ５２６と、キーパッド５２８と、タッチセンサ面５３０を有するタッチスクリーン液晶ディスプレイ（ＬＣＤ）と、タッチスクリーン／ＬＣＤコントローラ５３２と、カメラ５３４と、カメラコントローラ５３６と、グローバルポジショニングシステム（ＧＰＳ）レシーバ５３８とを含んでもよい。一実施形態において、モバイルデバイス４００は、タッチセンサスクリーンを提供しない別の種類のディスプレイを含んでよい。一実施形態において、ＤＳＰ５０２は、入／出力インタフェース５１８を通過することなく、メモリ５０４と直接通信してもよい。更に、一実施形態において、モバイルデバイス４００は、他の機能性を提供する複数の他の周辺機器を備えてよい。

【００５０】

ＤＳＰ５０２又は他の何らかの形態のコントローラ若しくは中央処理装置は、メモリ５０４に格納された又はＤＳＰ５０２自体の中に含まれるメモリに格納された組み込みソフトウェア又はファームウェアに従って、モバイルデバイス４００の様々な複数の構成要素を制御するように動作する。組み込みソフトウェア又はファームウェアに加えて、ＤＳＰ５０２は、メモリ５０４に格納される、又は、取り外し可能メモリカード５２０のようなポータブルデータ記憶媒体等の情報搬送媒体を介して、若しくは、複数の有線または無線のネットワーク通信を介して、利用可能になる、他の複数のアプリケーションを実行してよい。アプリケーションソフトウェアは、所望の機能性を提供するようにＤＳＰ５０２を構成する、コンパイルされた機械可読命令セットを備えてもよく、又は、アプリケーショ

ンソフトウェアは、インタープリタまたはコンパイラによって処理され、ＤＳＰ５０２を間接的に構成する、複数の高水準ソフトウェア命令であってもよい。

【００５１】

ＤＳＰ５０２は、アナログベースバンド処理ユニット５１０を用いて無線ネットワークと通信してよい。いくつかの実施形態において、通信は、インターネット接続を提供し、ユーザが、インターネット上のコンテンツへのアクセスを取得したり、電子メールまたはテキストメッセージを送受信したりすることを可能にしてもよい。入／出力インタフェース５１８は、ＤＳＰ５０２と、様々な複数のメモリ及び複数のインタフェースを相互接続する。メモリ５０４及び取り外し可能メモリカード５２０は、ＤＳＰ５０２の動作を構成するためのソフトウェア及びデータを提供してよい。インタフェースの中には、ＵＳＢポート５２２及び赤外線ポート５２４があってよい。ＵＳＢポート５２２は、モバイルデバイス４００を周辺機器として機能させて、パーソナルコンピュータ又はその他のコンピュータシステムと情報を交換させることを可能にしてよい。赤外線ポート５２４、及び、ブルートゥース（登録商標）インタフェース、ＩＥＥＥ８０２．１１に準拠する無線インタフェース等のオプションである複数のその他のポートは、モバイルデバイス４００が、他の近くの複数のハンドセット及び／又は複数の無線基地局と無線通信することを可能にしてよい。

【００５２】

キーパッド５２８は、インタフェース５１８を介して、ＤＳＰ５０２に連結し、ユーザが、複数の選択を行う、情報を入力する、及び、別の方法でモバイルデバイス４００に入力を提供するための１つのメカニズムを提供する。別の入力メカニズムは、また、テキスト及び／又はグラフィックをユーザに表示し得るタッチスクリーンＬＣＤ５３０であってもよい。タッチスクリーンＬＣＤコントローラ５３２は、ＤＳＰ５０２をタッチスクリーンんＬＣＤ５３０に連結する。ＧＰＳ受信機５３８は、ＤＳＰ５０２に連結され、複数のグローバルポジショニングシステム信号を復号することで、モバイルデバイス４００が、その位置を決定することを可能にする。

【００５３】

図９Ａは、ＤＳＰ５０２により実現され得るソフトウェア環境６０２を説明する。ＤＳＰ５０２は、オペレーティングシステムソフトウェア６０４を実行して、そこからソフトウェアの残りが動作するプラットフォームを提供する。オペレーティングシステムソフトウェア６０４は、アプリケーションソフトウェアによってアクセス可能である複数の標準化インタフェースを有する、ハンドセットのハードウェア向けの複数の様々なドライバを提供してよい。オペレーティングシステムソフトウェア６０４は、モバイルデバイス４００上で動作する複数のアプリケーション間で制御を転送する複数のアプリケーション管理サービス（ＡＭＳ）６０６と連結され、情報を送受してよい。また、ウェブブラウザアプリケーション６０８、メディアプレーヤアプリケーション６１０及び複数のＪＡＶＡ（登録商標）アプレット６１２が、図９Ａに示される。ウェブブラウザアプリケーション６０８は、例えば、モバイルデバイス４００が無線リンクを介して、ネットワークに連結された場合に、コンテンツ及び／又はインターネットを閲覧するべく、モバイルデバイス４００によって実行されてよい。ウェブブラウザアプリケーション６０８は、ユーザが、複数のフォームに情報を入力したり、複数のリンクを選択したり、複数のウェブページの取得及び閲覧することを可能にしてよい。メディアプレーヤアプリケーション６１０は、音楽又はオーディオビジュアルのメディアを再生するべく、モバイルデバイス４００によって実行されてよい。複数のＪＡＶＡ（登録商標）アプレット６１２は、複数のゲーム、複数のユーティリティ及びその他の機能性を含む様々な機能性を提供するべく、モバイルデバイス４００により実行されてよい。

【００５４】

図９Ｂは、ＤＳＰ５０２によって実現され得る代替的なソフトウェア環境６２０を説明する。ＤＳＰ５０２は、オペレーティングシステムソフトウェア６２８及び実行ランタイム６３０を実行する。ＤＳＰ５０２は、実行ランタイム６３０において実行し、アプリケ

ーションフレームワーク６２４により提供される複数のサービスを頼りにしてよい複数のアプリケーション６２２を実行する。複数のアプリケーション６２２及びアプリケーションフレームワーク６２４は、複数のライブラリ６２６を用いて提供される機能性を頼りにし得る。

【００５５】

図１０は、本明細書に開示された１又は複数の実施形態に適したコンピュータシステム３８０を説明する。コンピュータシステム３８０は、二次記憶装置３８４、リードオンリーメモリ（ＲＯＭ）３８６、ランダムアクセスメモリ（ＲＡＭ）３８８を含む複数のメモリデバイス、複数の入／出力（Ｉ／Ｏ）デバイス３９０及び複数のネットワーク接続デバイス３９２と通信するプロセッサ３８２（中央演算処理装置又はＣＰＵと称されてよい。）を含む。プロセッサ３８２は、１又は複数のＣＰＵチップにより実現されてよい。

【００５６】

コンピュータシステム３８０上に複数の実行可能命令をプログラム及び／又はロードすることにより、ＣＰＵ３８２、ＲＡＭ３８８、ＲＯＭ３８６の少なくとも１つが変更され、コンピュータシステム３８０を、部分的に、本開示により教授された新たな機能性を有する特定の機械又は装置に変換することが理解される。実行可能なソフトウェアをコンピュータにロードすることによって実装されうる機能が、周知の複数の設計ルールにより、ハードウェア実装に変換されうることは、電気工学及びソフトウェア工学の技術において基本的なことである。ハードウェアとソフトウェアによりコンセプトを実現することの間の複数の決定は、一般的に、ソフトウェアのドメインからハードウェアのドメインへの翻訳中に引き起こされる何らかの複数の論点というよりはむしろ、設計の安定性及び生成され得る複数のユニットの数についての複数の検討事項によって決まる。概して、ハードウェア実装をリスピンすることは、ソフトウェアの設計をリスピンするよりもコストが高いので、未だに頻繁に変更にさらされるような設計は、ソフトウェアにより実現されることが好適である場合がある。概して、大量生産の実施に関して、ハードウェア実装は、ソフトウェア実装よりコストが低い場合があるので、大量に生産されるであろうことがはっきりしているような設計は、ハードウェア、例えば、特定用途向け集積回路（ＡＳＩＣ）により実現されることが好適である場合がある。しばしば、設計は、ソフトウェアの形態で開発及び試験され、その後、複数の周知の設計ルールによって、複数のソフトウェアの命令をハードウェアに組み込む特定用途向け集積回路により、均等なハードウェア実装に変換される。同様に、新たなＡＳＩＣにより制御された機械は、特定の機械又は装置であるので、複数の実行可能命令をプログラム及び／又はロードされたコンピュータは、同様に、特定の機械又は装置と見做されてよい。

【００５７】

二次記憶装置３８４は、典型的には、データの不揮発性記憶の用途に用いられたり、ＲＡＭ３８８が全ての作業用データを十分に保持できるほど大きくない場合にはオーバーフローデータ記憶装置として用いられたりする１又は複数のディスクドライブ又はテープドライブを含む。二次記憶装置３８４は、そのような複数のプログラムが実行のために選択された場合にＲＡＭ３８８いロードされる複数のプログラムを格納する目的で用いられてよい。ＲＯＭ３８６は、複数の命令と、場合によっては、プログラムの実行中に読み込まれるデータとを格納する目的で用いられてよい。ＲＯＭ３８６は、典型的には、二次記憶装置３８４の大きな記憶容量に対して、小さな記憶容量を有する不揮発性メモリデバイスである。ＲＡＭ３８８は、揮発性データを格納する目的で、また、場合によっては、複数の命令を格納する目的で用いられる。ＲＯＭ３８６及びＲＡＭ３８８へのアクセスは、典型的には、二次記憶装置３８４に対するものよりも速い。二次記憶装置３８４、ＲＡＭ３８８及び／又はＲＯＭ３８６は、いくつかの文脈において、コンピュータ可読記憶媒体及び／又は非一時的コンピュータ可読媒体と称される場合がある。

【００５８】

複数のＩ／Ｏデバイス３９０は、複数のプリンタ、複数のビデオモニタ、複数の液晶ディスプレイ（ＬＣＤｓ）、複数のタッチスクリーンディスプレイ、複数のキーボード、複

数のキーパッド、複数のスイッチ、複数のダイヤル、複数のマウス、複数のトラックボール、複数の音声認識装置、複数のカードリーダ、複数の紙テープリーダ、又はその他周知の複数の入力デバイスを含んでよい。

【００５９】

複数のネットワーク接続デバイス３９２は、複数のモデム；複数のモデムバンク；複数のイーサネット（登録商標）カード；複数のユニバーサルシリアルバス（ＵＳＢ）インタフェースカード；複数のシリアルインタフェース；複数のトークンリングカード；複数のファイバ分散データインタフェース（ＦＤＤＩ）カード；複数の無線ローカルエリアネットワーク（ＷＬＡＮ）カード；符号分割多重アクセス（ＣＤＭＡ）、グローバルシステム・フォー・モバイルコミュニケーションズ（ＧＳＭ（登録商標））、ロングタームエボリューション（ＬＴＥ）、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（ＷｉＭＡＸ（登録商標））、第４世代、第５世代、及び／又は、他の無線インタフェースプロトコルの複数の無線トランシーバカードなどの複数の無線トランシーバカード；並びに、他の複数の周知のネットワークデバイスの形態を成してもよい。これらの複数のネットワーク接続デバイス３９２は、プロセッサ３８２が、インターネット、又は、１若しくは複数のイントラネットと通信することを可能にしてよい。上述された方法の複数の段階を実施する過程において、そのようなネットワーク接続と一体となって、プロセッサ３８２が、ネットワークから情報を受信する場合があったり、又は、ネットワークに情報を出力する場合があったりすることが予期される。そのような情報は、しばしば、プロセッサ３８２を用いて実行されるべき一連の複数の命令として表され、例えば、搬送波において具現化されたコンピュータデータ信号の形態で、ネットワークから受信されたり、ネットワークに出力されたりしてよい。

【００６０】

そのような情報は、プロセッサ３８２を用いて実行されるべきデータ又は複数の命令を含んでもよく、例えば、搬送波において具現化されたコンピュータデータベースバンド信号又は信号の形態で、例えば、ネットワークから受信されたり、ネットワークに出力されてもよい。搬送波に埋め込まれたベースバンド信号若しくは信号、又は、現在用いられている若しくは将来開発された複数の他の型の複数の信号は、当業者にとって周知のいくつかの方法に従って、生成されてよい。搬送波に埋め込まれたベースバンド信号及び／又は信号は、いくつかの文脈において、一時的な信号と称されてよい。

【００６１】

プロセッサ３８２は、ハードディスク、フロッピー（登録商標）ディスク、光ディスク（これらの様々なディスクを利用した複数のシステムは、全て、二次記憶装置３８４と見做されてもよい。）、ＲＯＭ３８６、ＲＡＭ３８８、又は、複数のネットワーク接続デバイス３９２からアクセスして、複数の命令、複数のコード、複数のコンピュータプログラム、及び／又は、複数のスクリプトを実行する。１つのプロセッサ３８２が図示されているけれども、複数のプロセッサが存在してもよい。このように、複数の命令は、プロセッサによって実行されるものとして議論されているけれども、複数の命令は、同時に、連続的に実行されてもよく、又は、別の方法では、１又は複数のプロセッサにより実行されてもよい。例えば、複数のハードドライブ、複数のフロッピー（登録商標）ディスク、複数の光ディスク及び／若しくは他のデバイス、ＲＯＭ３８６、並びに／又は、ＲＡＭ３８８といった二次記憶装置３８４からアクセスされ得る複数の命令、複数のコード、複数のコンピュータプログラム、複数のスクリプト、及び／又は、データは、いくつかの文脈において、非一時的な複数の命令及び／又は非一時的な情報と称されてよい。

【００６２】

一実施形態において、コンピュータシステム３８０は、互いに通信し、協調してタスクを実施する、２又は複数のコンピュータを備えてよい。限定するわけではないが、例えば、アプリケーションの複数の命令を平行に及び／又は並列に処理することを可能にするように、当該アプリケーションが分割されてもよい。代替的に、２又は複数のコンピュータによって、データセットの複数の異なる部分を同時に及び／又は並列に処理することを可

能にするように、アプリケーションにより処理されたデータが分割されてもよい。一実施形態において、コンピュータシステム３８０中の多数のコンピュータと直接的には結合されていない多数のサーバの機能性を提供するべく、コンピュータシステム３８０により、仮想化ソフトウェアが使用されてよい。例えば、仮想化ソフトウェアは、４個の物理コンピュータ上に２０個の仮想サーバ提供してよい。一実施形態において、上記において開示された機能性は、クラウドコンピューティング環境中のアプリケーション及び／又は複数のアプリケーションを実行することで提供されてもよい。クラウドコンピューティングは、動的に拡張可能な複数のコンピュータリソースを用いて、ネットワーク接続を介して、複数のコンピューティングサービスを提供することを含んでよい。クラウドコンピューティングは、少なくとも部分的にて、仮想化ソフトウェアによりサポートされてよい。クラウドコンピューティング環境は、企業によって確立されてもよく、及び／又は、必要に応じて、サードパーティのプロバイダから借りてもよい。複数のクラウドコンピューティング環境は、サードパーティのプロバイダから借りた及び／又はリースされた複数のクラウドコンピューティングリソースだけでなく、企業によって所有及び運用される複数のクラウドコンピューティングリソースを含んでよい。

【００６３】

一実施形態において、上記において開示された機能性のいくつか又は全ては、コンピュータプログラム製品として提供されてよい。コンピュータプログラム製品は、上記において開示された機能性を実現するべく、その中に具現化されたコンピュータ利用可能プログラムコードを有する、１又は複数のコンピュータ可読記憶媒体を含んでよい。コンピュータプログラム製品は、複数のデータ構造体、複数の実行可能命令及び他のコンピュータ利用可能プログラムコードを含んでよい。コンピュータプログラム製品は、取り外し可能コンピュータ記憶媒体、及び／又は、取り外し可能でないコンピュータ記憶媒体の形態で具現化されてよい。コンピュータ可読記憶媒体は、これに限定されるものではないが、例えば、アナログ磁気テープ、複数のコンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）ディスク、複数のフロッピー（登録商標）ディスク、複数のジャンプドライブ、複数のデジタルカード、複数のマルチメディアカード、及び、複数のその他のものといった、紙テープ、磁気テープ、磁気ディスク、光ディスク、及び／又は、ソリッドステートメモリチップを含んでよい。コンピュータプログラム製品は、コンピュータシステム３８０による、二次記憶装置３８４、ＲＯＭ３８６、ＲＡＭ３８８、並びに／又は、コンピュータシステム３８０の他の不揮発性メモリ及び揮発性メモリへの、コンピュータプログラム製品の複数の内容の少なくとも一部のロードに適していてよい。プロセッサ３８２は、コンピュータプログラム製品に部分的に直接アクセスすることによって、例えば、コンピュータシステム３８０のディスクドライブ周辺機器に挿入されたＣＤ－ＲＯＭディスクから読み出すことによって、複数の実行可能命令、及び／又は、複数のデータ構造体を処理してよい。代替的に、プロセッサ３８２は、コンピュータプログラム製品に遠隔アクセスすることによって、例えば、複数のネットワーク接続デバイス３９２を通して、遠隔サーバから、複数の実行可能命令、及び／又は、複数のデータ構造体をダウンロードすることによって、複数の実行可能命令、及び／又は、複数のデータ構造体を処理してよい。コンピュータプログラム製品は、データ、複数のデータ構造体、複数のファイル、及び／又は、複数の実行可能命令の、二次記憶装置３８４、ＲＯＭ３８６、ＲＡＭ３８８及び／又はコンピュータシステム３８０の他の不揮発性メモリ及び揮発性メモリへの、ロード及び／又はコピーを促進する複数の命令を含んでよい。

【００６４】

いくつかの文脈において、二次記憶装置３８４、ＲＯＭ３８６及びＲＡＭ３８８は、非一時的コンピュータ可読媒体又はコンピュータ可読記憶媒体と称されてよい。同様に、ＲＡＭ３８８のダイナミックＲＡＭの実施形態は、ダイナミックＲＡＭが電気出力を受け取り、その設計に従って操作され、例えば、コンピュータシステム３８０が作動させられて操作可能である期間において、ダイナミックＲＡＭは、そこに書き込まれる情報を格納することから、非一時的コンピュータ可読媒体と称されてよい。同様に、プロセッサ３８２

は、内部ＲＡＭ、内部ＲＯＭ、キャッシュメモリ、及び／又は、いくつかの文脈において、非一時的コンピュータ可読媒体又はコンピュータ可読記憶媒体と称される、他の複数の内部非一時的記憶ブロック、複数のセクション若しくは複数の構成要素を含んでよい。

【００６５】

本開示において、いくつかの実施形態が提供されてきた。一方で、開示された複数のシステム及び複数の方法は、本開示の精神又は範囲から逸脱することなく、多くの他の複数の特定の形態で具現化されることができることが理解されるべきである。複数の実施例は、制限ではなく、例証として見做されるべきであり、本明細書に与えられる複数の詳細に制限されることを意図するものではない。例えば、様々な複数の要素又は複数の構成要素が組み合わされたり、又は、別のシステムに統合されたりしてもよい。又は、複数の特定の特徴が省略されてもよく、若しくは、実装されなくてもよい。

【００６６】

また、本開示の精神又は範囲から逸脱することなく、様々な複数の実施形態において、別々である若しくは分離しているものとして説明及び示されている複数の技術、複数のシステム、複数のサブシステム、及び、複数の方法が、組み合わされたり、又は、別の複数のシステム、複数のモジュール、複数の技術若しくは複数の方法に統合されたりしてもよい。互いに直接的に連結されている又は通信するものとして開示又は議論されている複数の他のアイテムは、何らかのインタフェース、デバイス又は中間構成要素を通して、電子的に、機械的に又は別の方法であるかにかかわらず、間接的に連結されてもよく又は通信してもよい。複数の変更、複数の置換及び複数の代替の他の複数の例は、当業者によって究明可能であって、本明細書に開示される精神および範囲から逸脱することなく成され得る。

【図７】

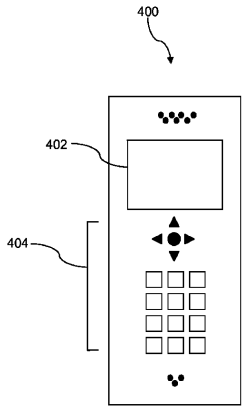
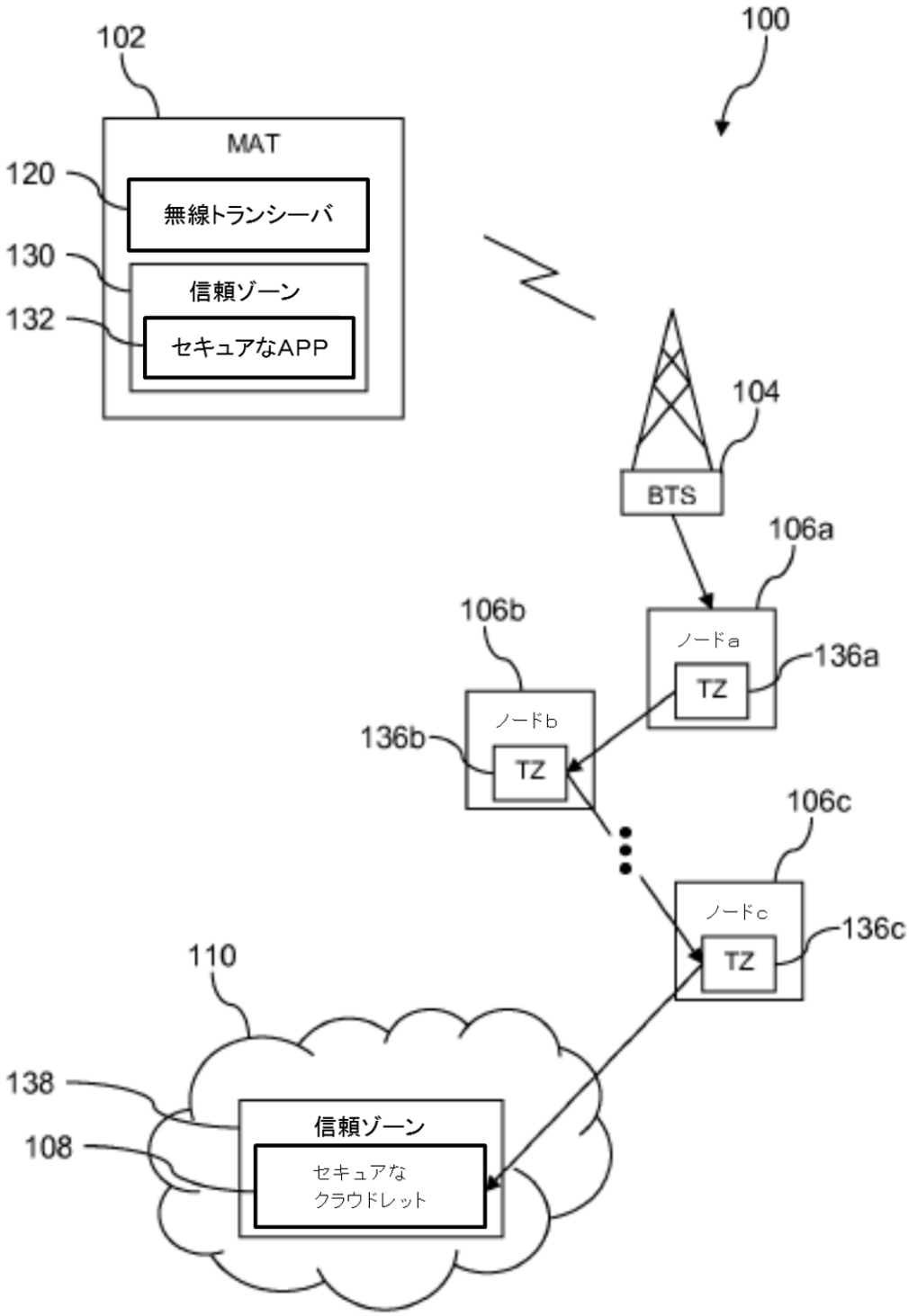
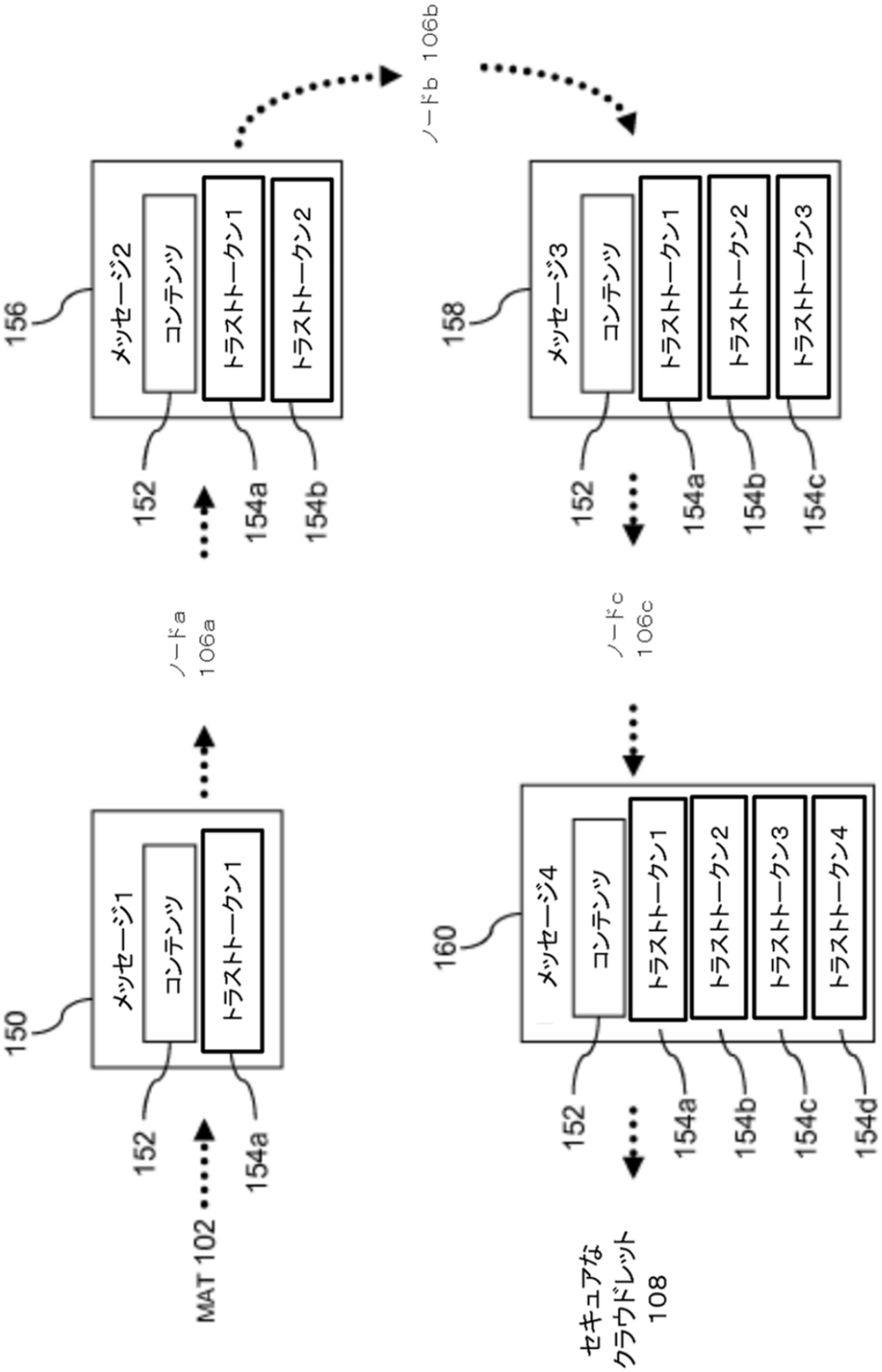


FIG. 7

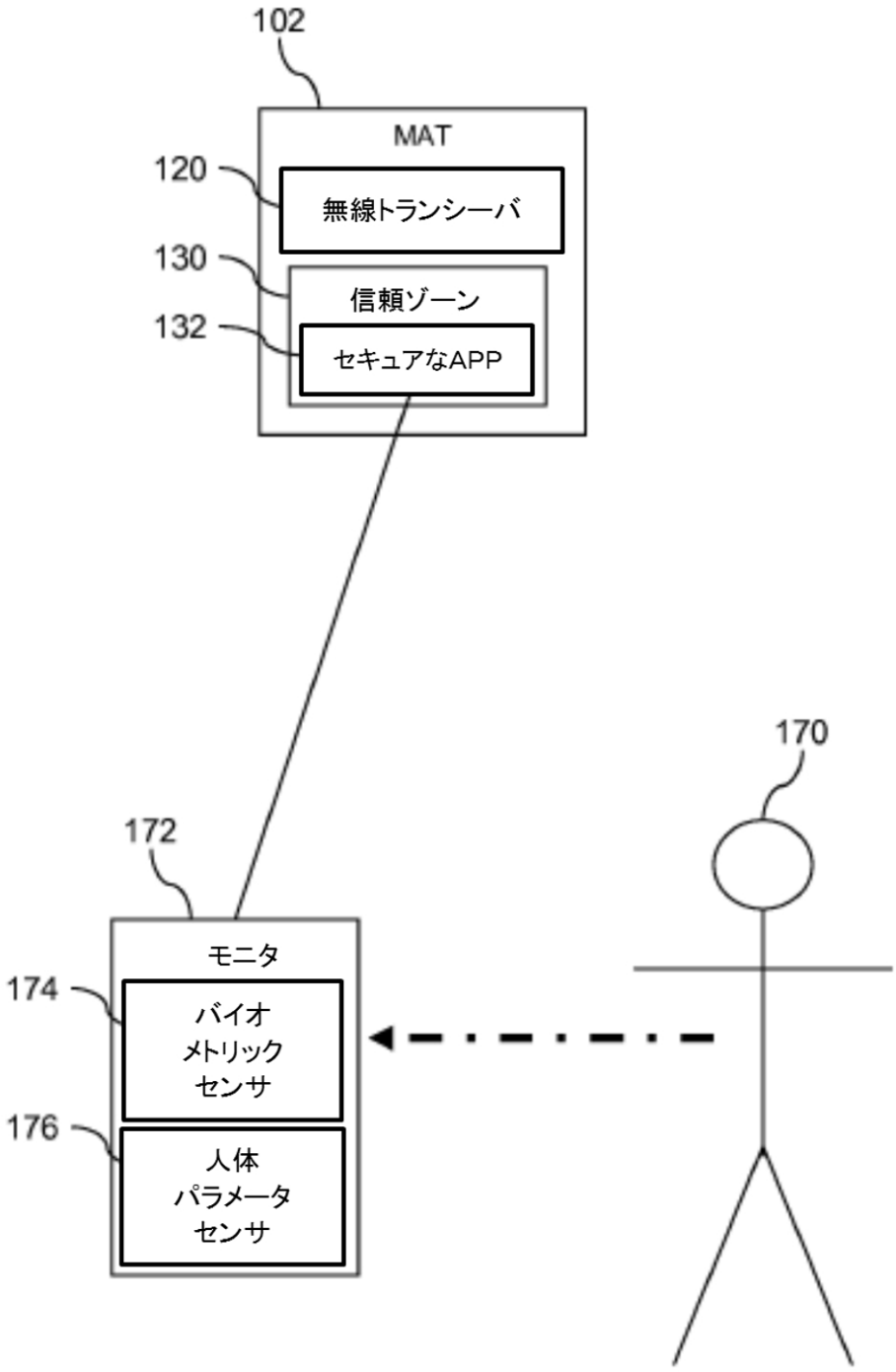
【図１】


100
102
MAT
120
無線トランシーバ
130
信頼ゾーン
132
セキュアなAPP
104
BTS
106a
ノードa
136a
TZ
106b
ノードb
136b
TZ
106c
ノードc
136c
TZ
110
138
信頼ゾーン
108
セキュアな
クラウドレット

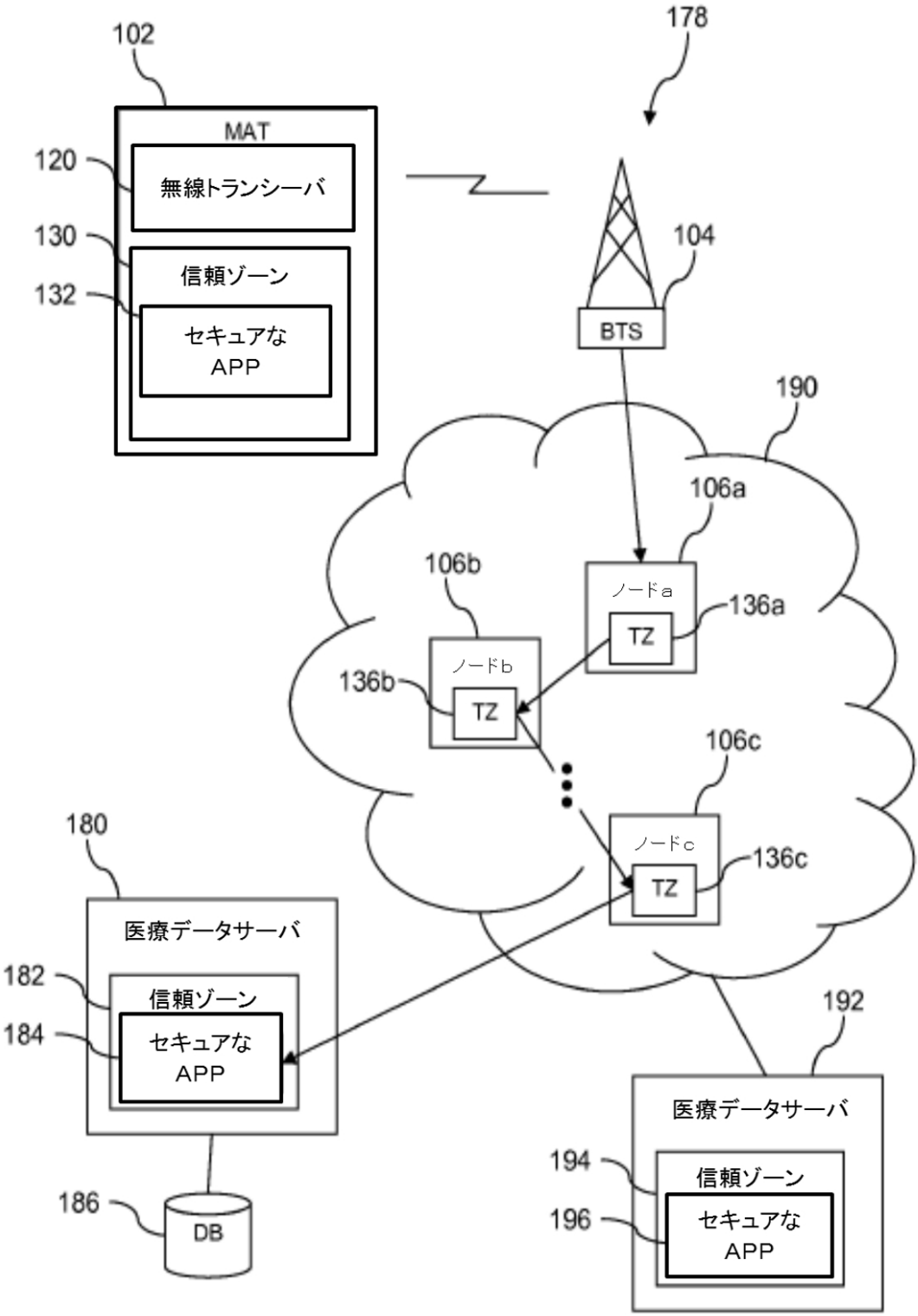
【図２】


150
メッセージ1
コンテンツ
トラストトークン1
152
154a
MAT 102
ノードa
106a
156
メッセージ2
コンテンツ
トラストトークン1
トラストトークン2
152
154a
154b
ノードb 106b
158
メッセージ3
コンテンツ
トラストトークン1
トラストトークン2
トラストトークン3
152
154a
154b
154c
ノードc
106c
160
メッセージ4
コンテンツ
トラストトークン1
トラストトークン2
トラストトークン3
トラストトークン4
152
154a
154b
154c
154d
セキュアな
クラウドレット
108

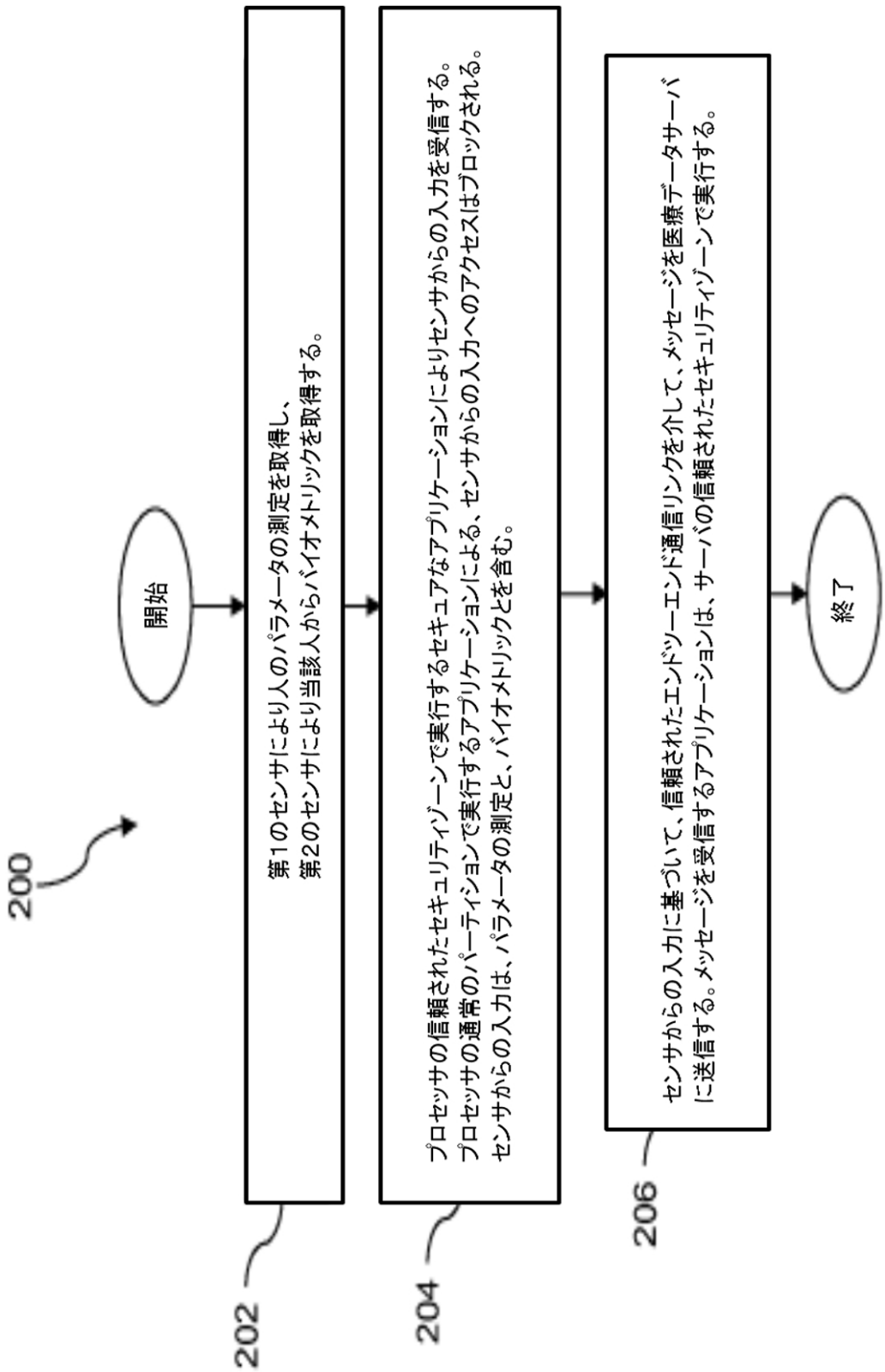
【図３Ａ】


102
MAT
120
無線トランシーバ
130
信頼ゾーン
132
セキュアなAPP
170
172
モニタ
174
バイオ
メトリック
センサ
176
人体
パラメータ
センサ

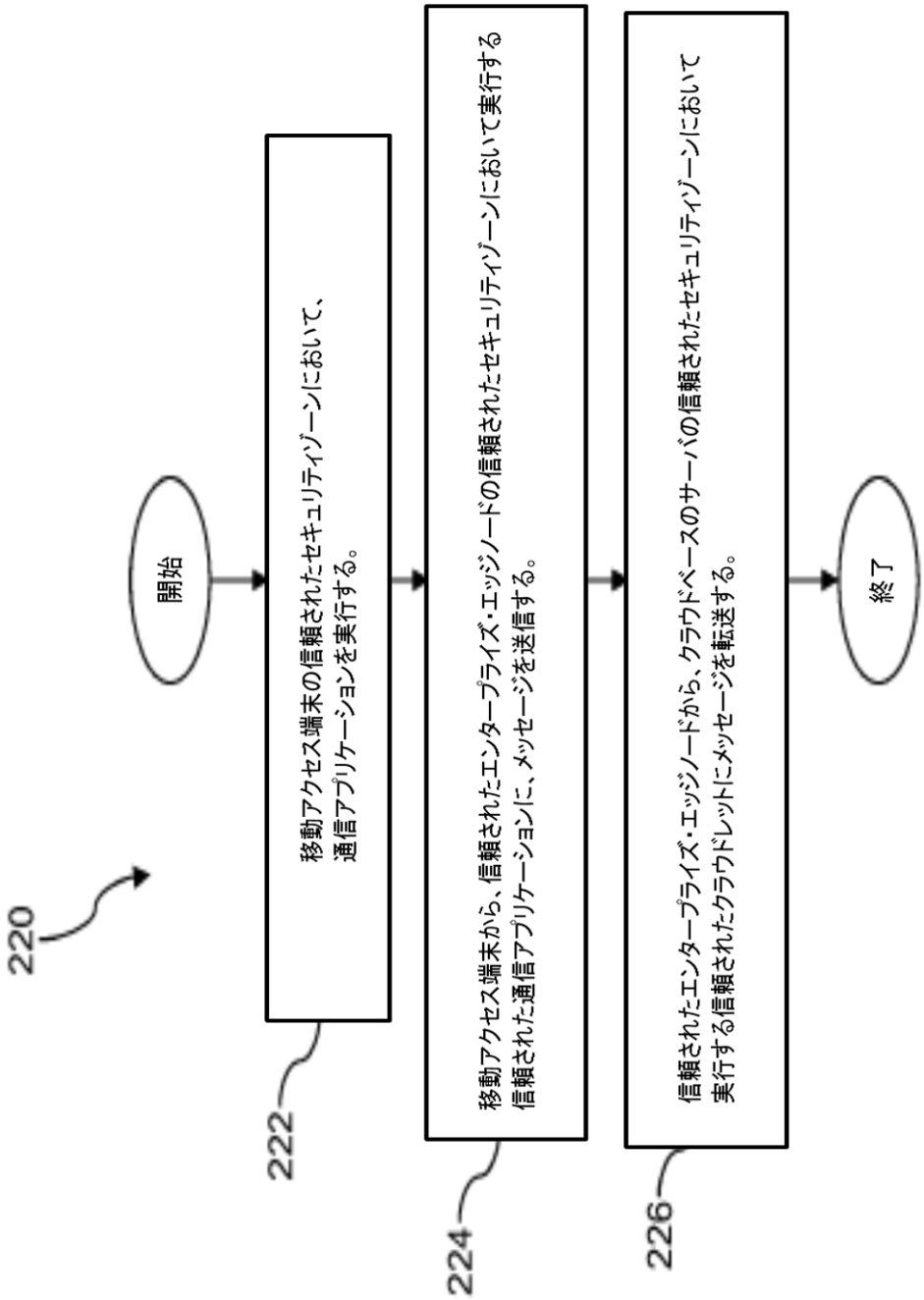
【図３Ｂ】


102
MAT
120
無線トランシーバ
130
信頼ゾーン
132
セキュアな
APP
178
104
BTS
190
106a
106b
ノードa
136a
TZ
ノードb
136b
TZ
106c
ノードc
136c
TZ
180
医療データサーバ
182
信頼ゾーン
184
セキュアな
APP
186
DB
192
医療データサーバ
194
信頼ゾーン
196
セキュアな
APP

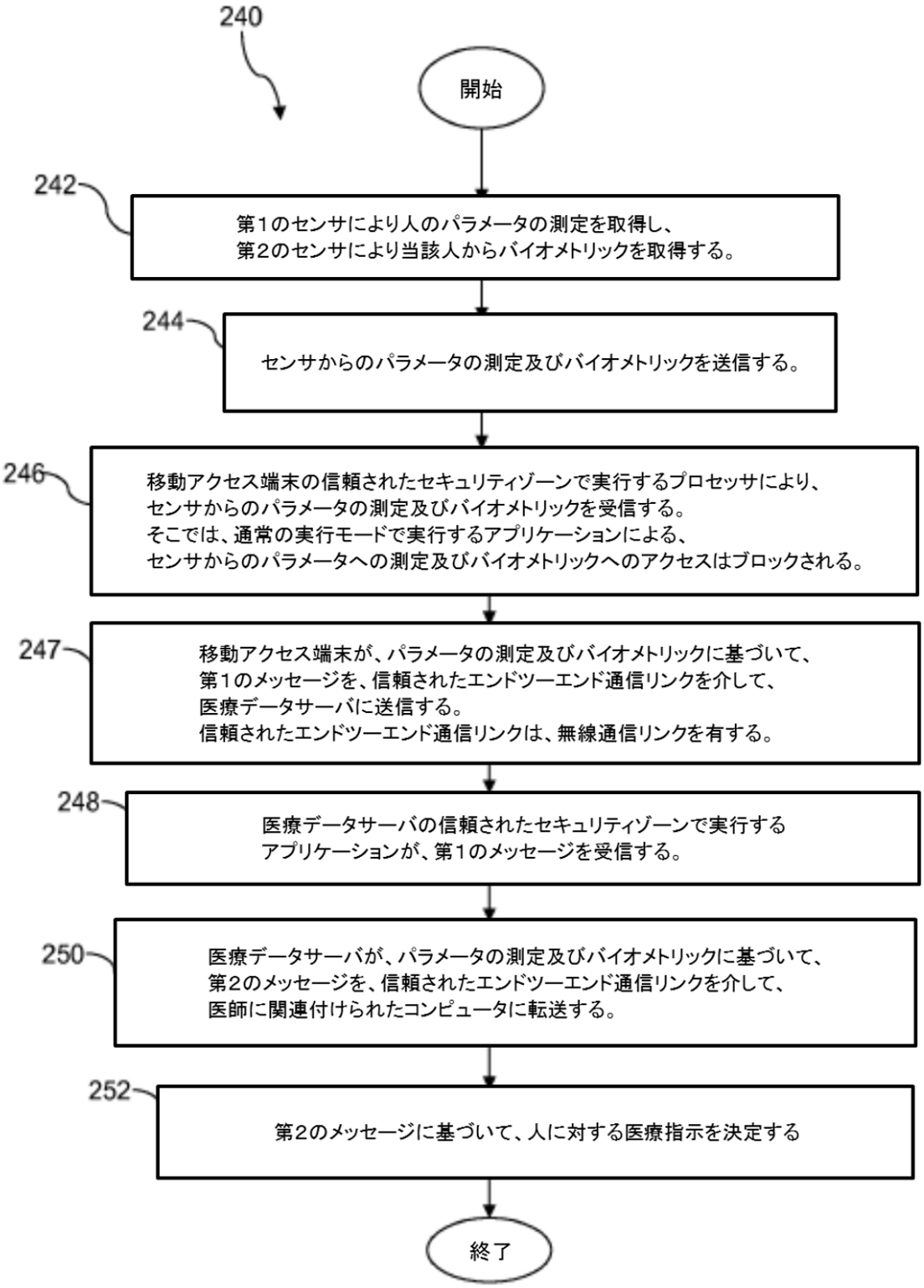
【図４】


200
開始
第1のセンサにより人のパラメータの測定を取得し、
第2のセンサにより当該人からバイオメトリックを取得する。
202
プロセッサの信頼されたセキュリティゾーンで実行するセキュアなアプリケーションによりセンサからの入力を受信する。
プロセッサの通常のパーティションで実行するアプリケーションによる、センサからの入力へのアクセスはブロックされる。
センサからの入力は、パラメータの測定と、バイオメトリックとを含む。
204
センサからの入力に基づいて、信頼されたエンドツーエンド通信リンクを介して、メッセージを医療データサーバに送信する。メッセージを受信するアプリケーションは、サーバの信頼されたセキュリティゾーンで実行する。
206
終了

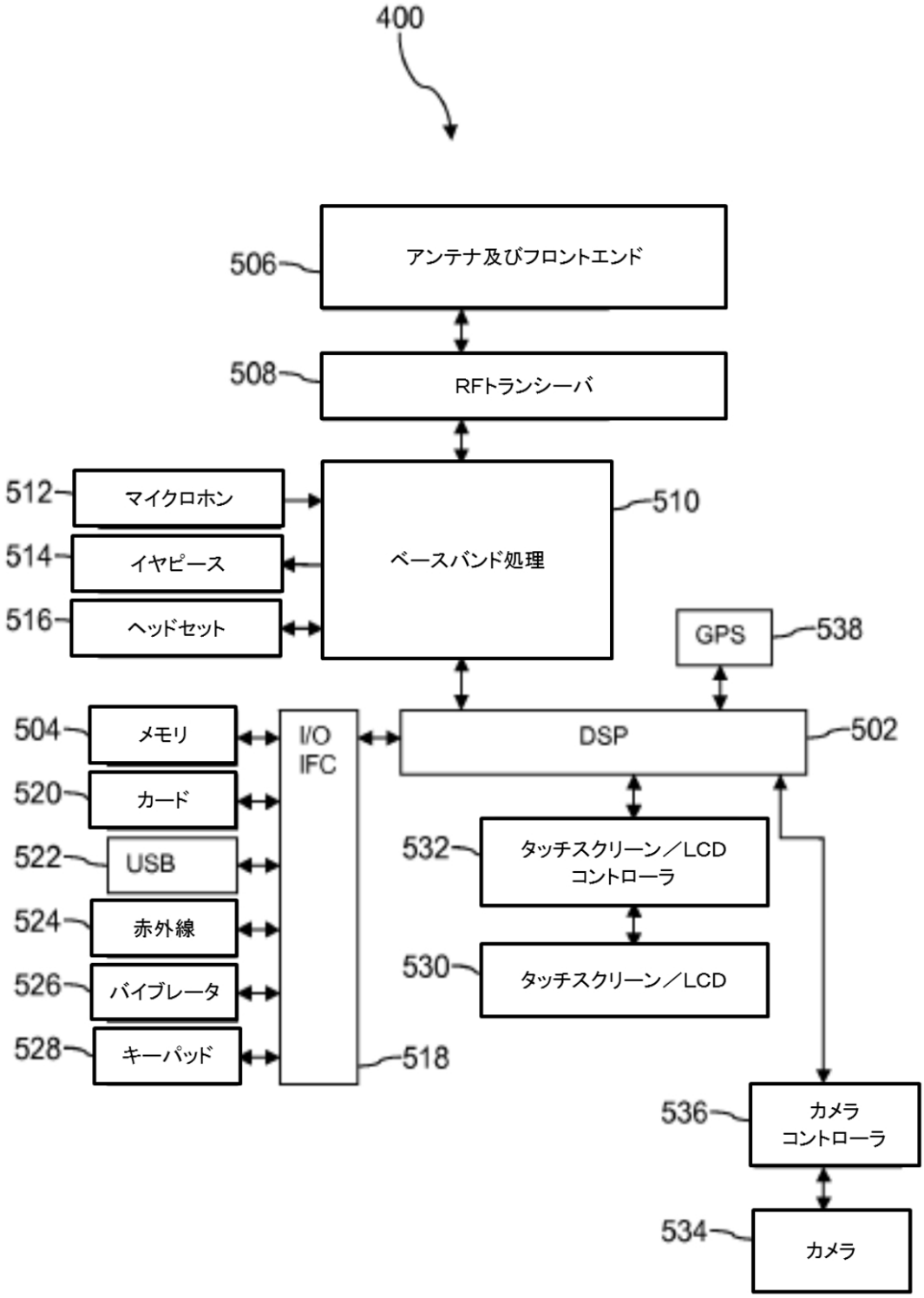
【図５】


220
開始
移動アクセス端末の信頼されたセキュリティゾーンにおいて、
通信アプリケーションを実行する。
222
移動アクセス端末から、信頼されたエンタープライズ・エッジノードの信頼されたセキュリティゾーンにおいて実行する
信頼された通信アプリケーションに、メッセージを送信する。
224
信頼されたエンタープライズ・エッジノードから、クラウドベースのサーバの信頼されたセキュリティゾーンにおいて
実行する信頼されたクラウドレットにメッセージを転送する。
226
終了

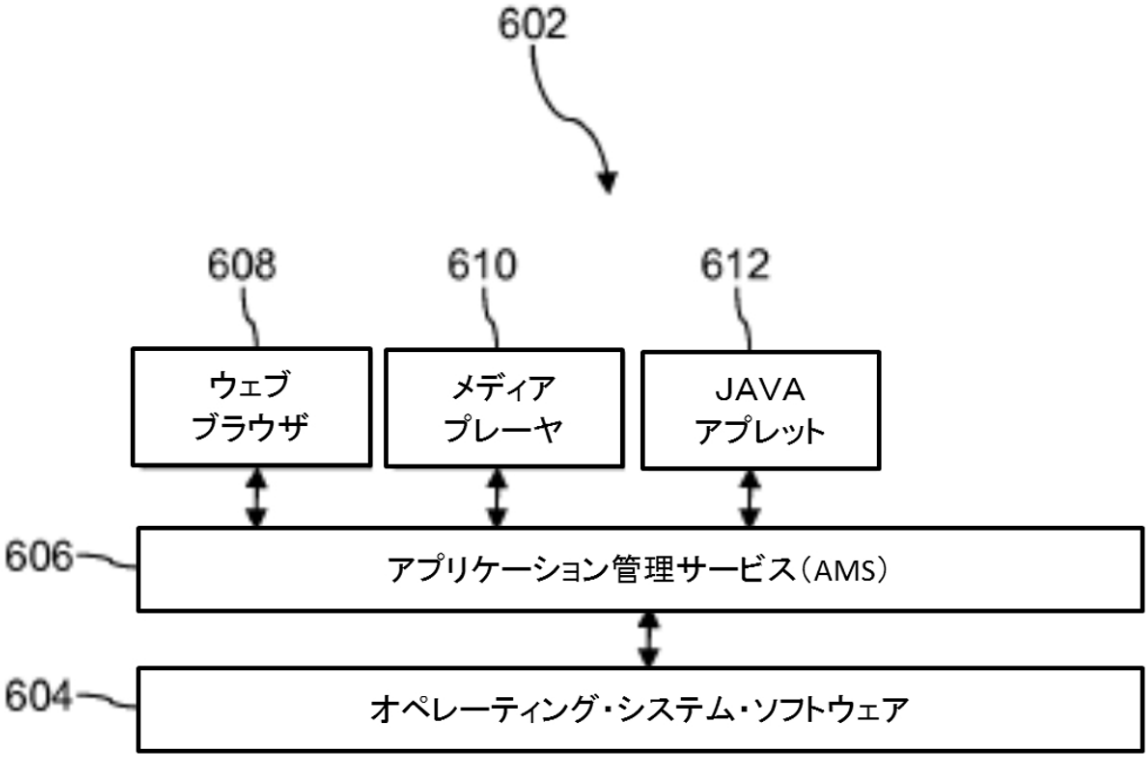
【図６】


240
開始
242
第１のセンサにより人のパラメータの測定を取得し、
第２のセンサにより当該人からバイオメトリックを取得する。
244
センサからのパラメータの測定及びバイオメトリックを送信する。
246
移動アクセス端末の信頼されたセキュリティゾーンで実行するプロセッサにより、
センサからのパラメータの測定及びバイオメトリックを受信する。
そこでは、通常の実行モードで実行するアプリケーションによる、
センサからのパラメータへの測定及びバイオメトリックへのアクセスはブロックされる。
247
移動アクセス端末が、パラメータの測定及びバイオメトリックに基づいて、
第１のメッセージを、信頼されたエンドツーエンド通信リンクを介して、
医療データサーバに送信する。
信頼されたエンドツーエンド通信リンクは、無線通信リンクを有する。
248
医療データサーバの信頼されたセキュリティゾーンで実行する
アプリケーションが、第１のメッセージを受信する。
250
医療データサーバが、パラメータの測定及びバイオメトリックに基づいて、
第２のメッセージを、信頼されたエンドツーエンド通信リンクを介して、
医師に関連付けられたコンピュータに転送する。
252
第２のメッセージに基づいて、人に対する医療指示を決定する
終了

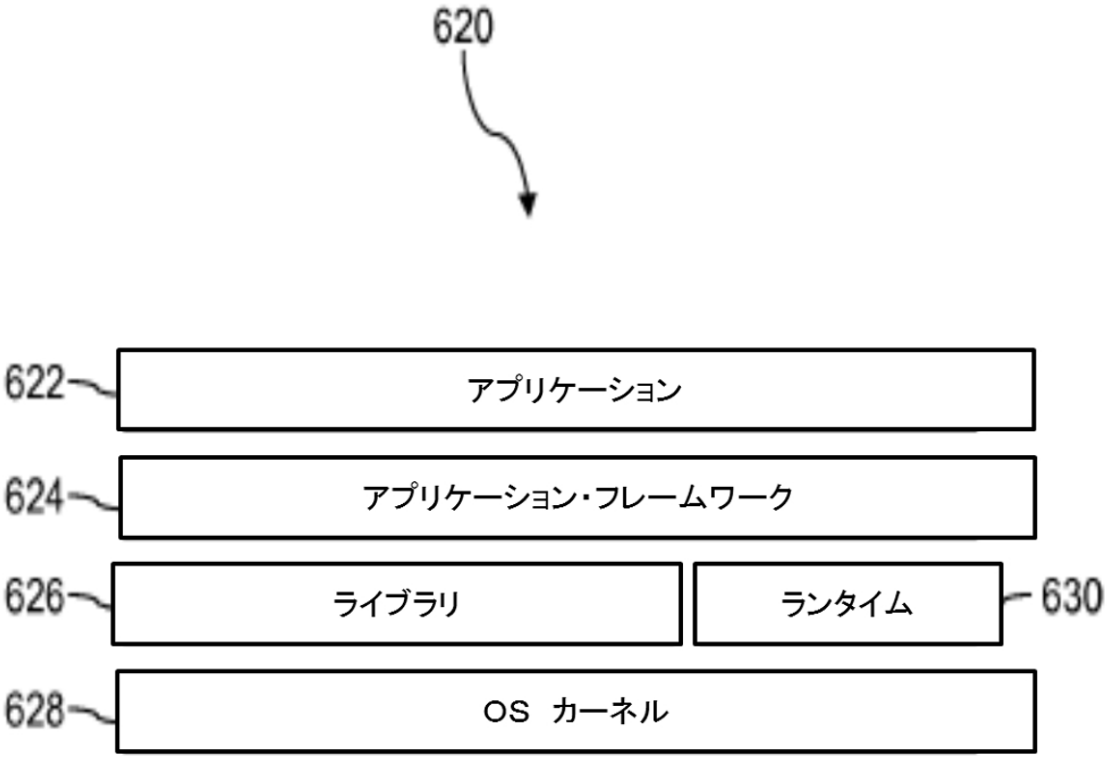
【図８】


400
506
アンテナ及びフロントエンド
508
RFトランシーバ
512
マイクロホン
514
イヤピース
516
ヘッドセット
510
ベースバンド処理
GPS
538
504
メモリ
520
カード
522
USB
524
赤外線
526
バイブレータ
528
キーパッド
I/O
IFC
518
DSP
502
532
タッチスクリーン／LCD
コントローラ
530
タッチスクリーン／LCD
536
カメラ
コントローラ
534
カメラ

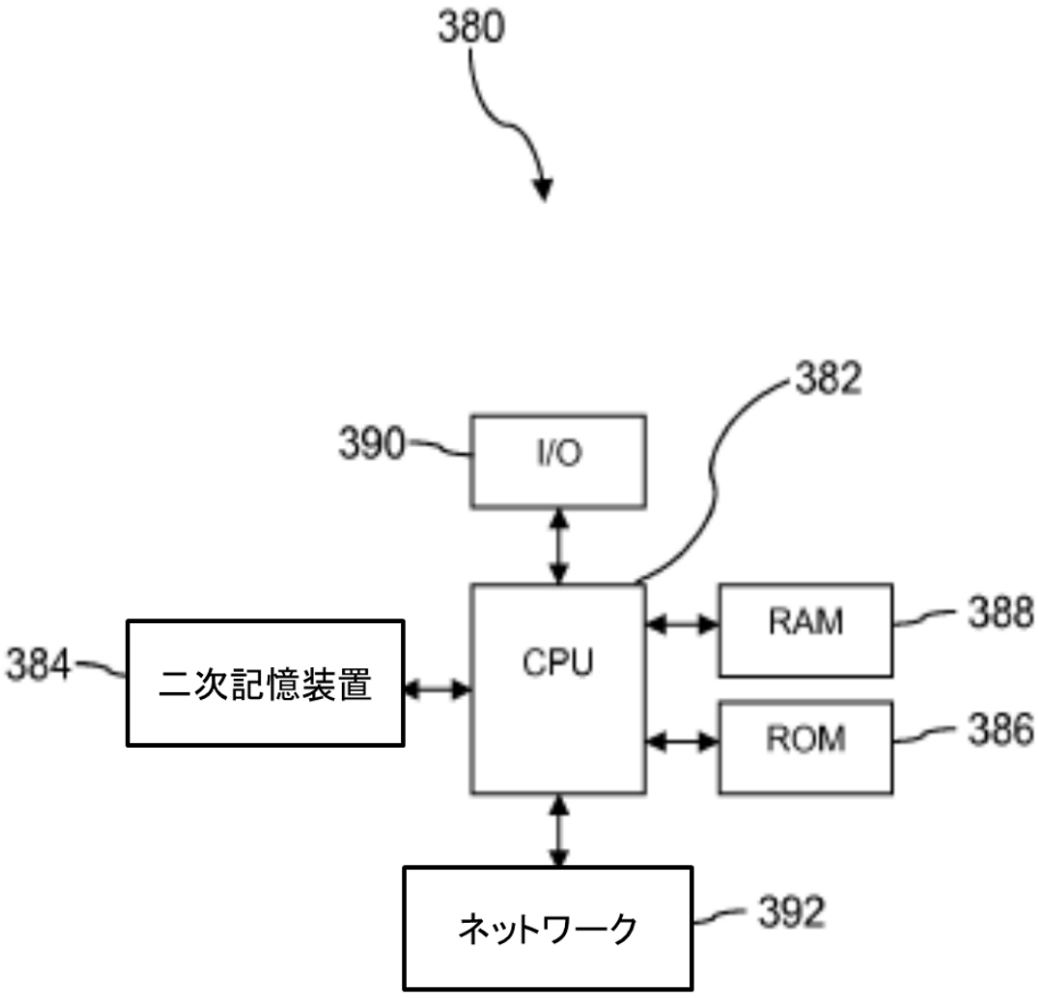
【図９Ａ】


602
608
610
612
ウェブ
ブラウザ
メディア
プレーヤ
JAVA
アプレット
606
アプリケーション管理サービス（AMS）
604
オペレーティング・システム・ソフトウェア

【図９Ｂ】


620
622
アプリケーション
624
アプリケーション・フレームワーク
626
ライブラリ
ランタイム
630
628
OS カーネル

【図１０】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/047729

A: CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 29/06 (2013.01)
USPC - 726/4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - A61B 5/00; G06F 3/00, 7/04, 9/00, 12/00,15/00, 17/00, 17/30; G06Q 10/00, 50/00; H04L 29/06 (2013.01)
USPC - 600/300; 705/ 2, 3; 710/ 15, 16; 713/ 155, 161, 182, 185, 186; 726/ 2, 4, 14,17-21

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G11C 7/00; G06F 21/00 (2013.01)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar, USPTO, PatentLens

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0094273 A1 (Fritsch et. al.) 26 April 2007 (26.04.2007) entire document	1-20
Y	US 2008/0097793 A1 (Dicks et al.) 24 April 2008 (24.04.2008) entire document	1-7, 15-20
Y	US 2012/0084438 A1 (Raleigh et al.) 05 April 2012 (05.04.2012) entire document	1-7, 15-20
Y	US 2012/0131178 A1 (Zhu et al.) 24 May 2012 (24.05.2012) entire document	8-14
A	US 2012/0089700 A1 (Safruti et al.) 12 April 2012 (12.04.2012) entire document	1-20
A	US 2012/0072481 A1 (Nandlall et al.) 22 March 2012 (22.03.2012) entire document	1-20
A	US 2002/0174344 A1 (Ting) 21 November 2002 (21.11.2002) entire document	1-20
A	US 2011/082711 A1 (Poeze et al.) 07 April 2011 (07.04.2011) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 January 2014	04 FEB 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(72)発明者 マックロバーツ、レオ マイケル
アメリカ合衆国、カンザス ６６２５１－２１００ オーバーランド パーク、メールストップ ケイエスオーピーエイチエヌ０３１２－３エイ３７１ スプリント パークウェイ ６４５０ スプリント コミュニケーションズ カンパニー エル．ピー．内
(72)発明者 パクツコウスキー、ライル ダブリュ．
アメリカ合衆国、カンザス ６６２５１－２１００ オーバーランド パーク、メールストップ ケイエスオーピーエイチエヌ０３１２－３エイ３７１ スプリント パークウェイ ６４５０ スプリント コミュニケーションズ カンパニー エル．ピー．内
(72)発明者 ロンドー、デイビッド イー．
アメリカ合衆国、カンザス ６６２５１－２１００ オーバーランド パーク、メールストップ ケイエスオーピーエイチエヌ０３１２－３エイ３７１ スプリント パークウェイ ６４５０ スプリント コミュニケーションズ カンパニー エル．ピー．内

Ｆターム(参考) 4C117 XB11 XE13 XE15 XE23 XE37 XF22 XH16 XH27 XJ03 XL01
XL03 XL26 XQ07
5K201 AA02 AA07 AA08 BA02 BA05 CB14 CC10 ED09
5L099 AA21

专利名称(译)	值得信赖的端到端通信基础设施		
公开(公告)号	JP2015524236A	公开(公告)日	2015-08-20
申请号	JP2015518648	申请日	2013-06-25
申请(专利权)人(译)	斯普林特通信公司，萨尔瓦多，复制.		
[标]发明人	マックロバーツレオマイケル パクツコウスキーライルダブリュ ロンドーデイビッドイー		
发明人	マックロバーツ、レオ マイケル パクツコウスキー、ライル ダブリュ. ロンドー、デイビッド イー.		
IPC分类号	H04M11/00 G06Q50/24 A61B5/00 G16H10/60		
CPC分类号	A61B5/0022 A61B5/01 A61B5/021 A61B5/024 A61B5/145 A61B5/1455 G06F21/32 G16H40/67 H04L63/105 H04W12/06 G06F19/00 H04L63/08 H04L67/141		
FI分类号	H04M11/00.302 G06Q50/24 A61B5/00.G		
F-TERM分类号	4C117/XB11 4C117/XE13 4C117/XE15 4C117/XE23 4C117/XE37 4C117/XF22 4C117/XH16 4C117/XH27 4C117/XJ03 4C117/XL01 4C117/XL03 4C117/XL26 4C117/XQ07 5K201/AA02 5K201/AA07 5K201/AA08 5K201/BA02 5K201/BA05 5K201/CB14 5K201/CC10 5K201/ED09 5L099/AA21		
优先权	13/532588 2012-06-25 US		
外部链接	Espacenet		

摘要(译)

一种通过可信的端到端通信链路传送医疗数据的方法。该方法包括通过第一传感器获得对人的参数的测量，通过第二传感器从人获得生物测量，通过在可信安全区中执行的安全应用接收来自第一和第二传感器的输入。处理器，其中通过在处理器的正常分区中执行的应用程序访问来自第一和第二传感器的输入被阻止，其中来自第一和第二传感器的输入包括参数和生物计量的测量，并且基于消息发送消息。通过可信的端到端通信链路将来自第一和第二传感器的输入连接到医疗数据服务器，其中接收消息的应用程序在服务器的可信安全区域中执行。

(21) 出願番号　特願2015-518648 (P2015-518648)
(86) (22) 出願日　平成25年6月25日 (2013.6.25)
(85) 翻訳文提出日　平成27年1月27日 (2015.1.27)
(86) 国際出願番号　PCT/US2013/047729
(87) 国際公開番号　WO2014/004590
(87) 国際公開日　平成26年1月3日 (2014.1.3)
(31) 優先権主張番号　13/532,588
(32) 優先日　平成24年6月25日 (2012.6.25)
(33) 優先権主張国　米国 (US)

(71) 出願人　513125245
スプリント コミュニケーションズ カンパニー エル. ピー.
アメリカ合衆国、カンザス 66251-2100 オーバーランド パーク、メールストップ ケイエスオーピーエイチエヌ 0312-3エイ371 スプリント パークウェイ 6450
(74) 代理人　110000877
龍華国際特許業務法人

最終頁に続く