

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6567258号
(P6567258)

(45) 発行日 令和1年8月28日 (2019.8.28)

(24) 登録日 令和1年8月9日 (2019.8.9)

(51) Int. Cl.

F I

H O 4 L 9/32 (2006.01)

H O 4 L 9/00 6 7 5 B

H O 4 W 4/029 (2018.01)

H O 4 L 9/00 6 7 3 B

H O 4 W 48/16 (2009.01)

H O 4 W 4/029

H O 4 W 12/08 (2009.01)

H O 4 W 48/16

H O 4 W 12/08

請求項の数 12 外国語出願 (全 19 頁)

(21) 出願番号 特願2014-166463 (P2014-166463)

(22) 出願日 平成26年8月19日 (2014.8.19)

(65) 公開番号 特開2015-43570 (P2015-43570A)

(43) 公開日 平成27年3月5日 (2015.3.5)

審査請求日 平成29年7月27日 (2017.7.27)

(31) 優先権主張番号 13/975, 936

(32) 優先日 平成25年8月26日 (2013.8.26)

(33) 優先権主張国・地域又は機関

米国 (US)

前置審査

(73) 特許権者 500520743

ザ・ボーイング・カンパニー

The Boeing Company

アメリカ合衆国、60606-2016

イリノイ州、シカゴ、ノース・リバーサイ

ド・プラザ、100

(74) 代理人 110002077

園田・小林特許業務法人

(72) 発明者 アヤガリ、 アルン

アメリカ合衆国 イリノイ 60606-

2016, シカゴ, ノース リバーサ

イド プラザ 100

最終頁に続く

(54) 【発明の名称】 信頼されるモバイル通信のためのシステム及び方法

(57) 【特許請求の範囲】

【請求項 1】

モバイルデータ通信のための方法であって、

ネットワークシステムが、アプリケーションごと及びモバイル無線通信装置ごとの安全性パラメータを収集することと、

前記ネットワークシステムが、収集された前記安全性パラメータを用いてモバイルクライアントシステムを設定することと、

前記モバイルクライアントシステム及び航空機システムが前記ネットワークシステムに関してオフラインであったとしても、前記航空機システムが、収集された前記安全性パラメータに基づいて、前記航空機システムに対するアクセスを、前記モバイルクライアントシステムに提供することとを含み、

前記安全性パラメータが、前記モバイル無線通信装置の位置又は飛行フェーズの制約を含む、方法。

【請求項 2】

前記ネットワークシステムが、前記モバイルクライアントシステムを評価することを含み、収集された前記安全性パラメータを用いて前記モバイルクライアントシステムを設定することは、前記モバイルクライアントシステムの前記評価に基づく、請求項 1 に記載の方法。

【請求項 3】

前記ネットワークシステムのデジタル公証人が、収集された前記安全性パラメータに署

10

20

名すること又は押印することのうちの少なくとも1つと、

前記ネットワークシステムが、署名又は押印のうちの少なくとも1つがなされた、収集された前記安全性パラメータを前記モバイルクライアントシステムに提供することと、

前記モバイルクライアントシステムが、署名又は押印のうちの少なくとも1つがなされた、収集された前記安全性パラメータを、前記モバイルクライアントシステムに記憶することと、

前記モバイルクライアントシステムが、前記航空機システムに対するアクセスのためのリクエストを送ることを含み、前記リクエストは、前記署名又は押印のうちの少なくとも1つがなされた、収集された安全性パラメータを含み、

前記航空機システムが、前記デジタル公証人の同一性に基づいて、前記モバイルクライアントシステムから受信した署名又は押印がなされた、収集された前記安全性パラメータを解読することと、

前記航空機システムが、解読された、収集された前記安全性パラメータに基づいて、前記航空機システムに対するアクセスを前記モバイルクライアントシステムに提供するか否かを決定することを含む、請求項1又は2に記載の方法。

【請求項4】

デジタル公証人を使用することが、収集された前記安全性パラメータに対する信頼の連鎖を確立することを含み、前記航空機システムは、前もって前記モバイルクライアントシステムについての情報を有することなしに、確立された前記信頼の連鎖に基づいて前記モバイルクライアントシステムにアクセスを提供する、請求項1から3のいずれか一項に記載の方法。

【請求項5】

モバイルデータ通信のためのシステムであって、

ネットワークシステムと、

モバイルクライアントシステムが前記ネットワークシステムに関してオンラインである場合に、前記ネットワークシステムと通信する前記モバイルクライアントシステムとを備え、

前記ネットワークシステムは、アプリケーションごと及びモバイル無線通信装置ごとに安全性パラメータを収集し、収集された前記安全性パラメータを用いて、前記モバイルクライアントシステムを設定し、

前記モバイルクライアントシステムは、前記モバイルクライアントシステム及び航空機システムが前記ネットワークシステムに関してオフラインであったとしても、収集された前記安全性パラメータに基づいて前記航空機システムにより前記航空機システムに対するアクセスが提供され、

前記安全性パラメータが、前記モバイル無線通信装置の位置又は飛行フェーズの制約を含む、システム。

【請求項6】

前記ネットワークシステムは、前記モバイルクライアントシステムを評価し、前記ネットワークシステムは、前記モバイルクライアントシステムの前記評価に基づいて、収集された前記安全性パラメータを用いて、前記モバイルクライアントシステムを設定する、請求項5に記載のシステム。

【請求項7】

収集された前記安全性パラメータは、デジタル公証人によって署名又は押印され、かつ署名又は押印された、収集された前記安全性パラメータは、前記モバイルクライアントシステムに記憶される、請求項5又は6に記載のシステム。

【請求項8】

デジタル公証人は、収集された前記安全性パラメータに対する信頼の連鎖を確立し、かつ前記航空機システムは、前もって前記モバイルクライアントシステムについての情報を有することなしに、確立された前記信頼の連鎖に基づいて、前記モバイルクライアントシステムにアクセスを提供する、請求項5から7のいずれか一項に記載のシステム。

【請求項 9】

請求項 5 から 8 のいずれか一項に記載のモバイルデータ通信のためのシステムの上で使用するモバイル無線通信装置であって、

1 以上のメモリと、

前記 1 以上のメモリに結合される 1 以上のプロセッサとを備え、前記 1 以上のプロセッサは、

アプリケーションごと及び前記モバイル無線通信装置ごとに収集された安全性パラメータをネットワークシステムから受信し、

前記モバイル無線通信装置及び航空機システムが前記ネットワークシステムに関してオフラインであったとしても、収集された前記安全性パラメータに基づいて前記航空機システムにアクセスするように構成され、

前記安全性パラメータが、前記モバイル無線通信装置の位置又は飛行フェーズの制約を含む、モバイル無線通信装置。

【請求項 10】

前記 1 以上のプロセッサは、前記モバイル無線通信装置が前記ネットワークシステムに関してオンラインである場合に、前記モバイル無線通信装置についての情報を前記ネットワークシステムに送信するように構成され、かつ前記モバイル無線通信装置を設定する際に用いられる、収集された前記安全性パラメータは、送信された前記情報に基づいて前記ネットワークシステムによって決定される、請求項 9 に記載のモバイル無線通信装置。

【請求項 11】

収集された前記安全性パラメータは、前記 1 以上のプロセッサによって受信される前に、デジタル公証人が署名又は押印され、かつ前記 1 以上のプロセッサは、署名され又は押印された、収集された前記安全性パラメータを前記 1 以上のメモリに記憶するように構成される、請求項 9 又は 10 に記載のモバイル無線通信装置。

【請求項 12】

前記航空機システムは、前もって前記モバイル無線通信装置についての情報を有することなしに、前記モバイル無線通信装置にアクセスを提供する、請求項 9 から 11 のいずれか一項に記載のモバイル無線通信装置。

【発明の詳細な説明】

【技術分野】

【0001】

本開示のいくつかの実施例は通信に関し、特に、信頼されるモバイル通信に関する。

【背景技術】

【0002】

航空のプラットフォーム及びインフラは、様々な航空の計算ニーズを実行するために、階層的にネットワークで結ばれる多くの複雑なシステムを有する。電子対応可能アーキテクチャ及びテクノロジーの採用は、ネットワークで結ばれていることによってもたらされる作動上及び性能上の効率を増加させる。さらに、航空埋め込みシステム及び制御装置は、費用を削減し機能を増加させるために、汎用プロセッサ（GPP）用ハードウェアの上でホストされていて、かつ市販のソフトウェア作動システムを使用する。

【0003】

航空システムの間が増加された接続性に加えて、GPP ハードウェア及び市販のソフトウェア作動システムを使用することは、航空プラットフォームのフィーチャー機能及び機能性の向上をもたらしてきた。これらの機能のいくつかは、搭載されている飛行システムから外部のカスタムクライアント装置へデータをアップロード及びダウンロードする能力を含む。現在のところ、これらのカスタムクライアント装置は、目の前の作業のために特に構成され、プログラムされ、かつ管理される特殊化した装置である。

【0004】

現在のところ、特定のハードウェア及びソフトウェア構成要素から成るカスタム装置は、搭載されている航空機システムと接続することが可能である。航空会社は、これらのカ

10

20

30

40

50

スタム装置のための厳密な構成及び手続き上のプロセスに従うことが期待されている。これらのカスタム装置を購入し、管理し、かつ維持することは、人間のオペレータが高度の手続き及びプロセスに対するコンプライアンスを維持している間の手続き上のプロセスを考えると、付加的な支出である。加えて、カスタムクライアント装置によって使用されるハードウェア及びソフトウェアの両者は、短いリフレッシュサイクルを有し、テクノロジーの変化のペースのために急速に時代遅れのものになってしまう。一方、航空機システムは、非常に高い程度の整合性及び安全性に対して構築されており、それゆえ、非常に長いインターバルにおいてまれにアップデートされ、さらにしばしば外部のネットワークと接続されない。結果として、接続されるカスタムクライアント装置のサイバーセキュリティの整合性の有効性は、確立することが困難である。航空機システム及び航空会社の事務管理部門のシステムはまた寿命が長く、航空機の全体のライフサイクルの間に適切な特殊化された装置に取って代わる必要なハードウェア及びソフトウェアを調達することを困難にしている。航空機搭乗員、保守係、及び他の人々は現在のところ、航空機上で様々なタスクを実行するために、手動データ入力プロセスを使用している。手動データ入力は、時間がかかりまた間違いを起ししやすい。

10

【0005】

安全性の観点から装置及びアプリケーションの状態及びステータスを確認するメカニズムが存在するならば、接続されるクライアント装置は、これらのタスクの多くを実行することができる。航空会社のオペレーションの展開及びビジネス上／作業上の制約に忠実である一方、資源に制約のあるクライアント装置からデータを回収する航空機システムが、航空会社の事務管理部門のシステムに接続されないオフラインモードのオペレーションにおいて、資源に制約のあるクライアント装置からのデータの整合性をきちんと確立するという問題を解決する有効なアプローチは存在しない。

20

【0006】

民生品を利用する（COTS）モバイル装置は、エンドユーザにはなじみがあり、飛行と関係ない用途においてすでに使用されている。しかしながら、航空システムの機能及びネットワーク接続における増加はまた、展開されているソフトウェア及びハードウェアの実装において存在している脆弱性につけこむサイバーセキュリティ攻撃のリスクを高めてきた。COTSシステム及びそれらに関係する脆弱性は、サイバー攻撃のベクトルとして使用され得る。

30

【0007】

今日まで、オフラインモードのオペレーションにおいて資源に制約のあるクライアント装置から回収されるデータの整合性をきちんと確立するための単純で効率的で有効なメカニズムが存在してこなかった。オペレーションのオフラインモードは、航空会社の事務管理部門のシステムに対するクライアント装置及び航空機の通信ネットワークの接続性が利用可能でない、現場配置／作業上のシナリオを結果としてもたらすだろう。そのような環境において、資源に制約のあるクライアント装置からのデータの整合性の信頼できる確立は困難である。

【発明の概要】**【0008】**

特許請求の範囲においてより完全に説明されるように、図面の少なくとも1つに関連して実質的に示され及び／又は説明されるように、システム、方法、及び／又は装置が、信頼されるモバイル通信における使用に対して提供される。

40

【0009】

いくつかの実施例は、信頼されるモバイル通信のための方法を提供する。例えば、方法は、ネットワークシステムによって、アプリケーションごとベース及び装置ごとベースの安全性パラメータの収集を用いてモバイルクライアントシステムを設定すること；及びモバイルクライアントシステム及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システムに対するアクセスをモバイルクライアントシステムに提供することを含む。

50

【0010】

いくつかの実施例は、信頼されるモバイル通信のためのシステムを提供する。例えば、システムは、モバイルクライアントシステムがネットワークシステムに関してオンラインである場合に、ネットワークシステム及びネットワークシステムと通信するモバイルクライアントシステムを含むことができる。ネットワークシステムは、アプリケーションごとベース及び装置ごとベースの安全性パラメータの収集を用いてモバイルクライアントシステムを設定することができる。モバイルクライアントシステムは、モバイルクライアントシステム及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システムに対するアクセスが提供される。

【0011】

いくつかの実施例は、モバイル無線通信装置を提供する。例えば、モバイル無線通信は、1以上のメモリ、及び1以上のメモリに結合される1以上のプロセッサを含むことができる。1以上のプロセッサは、アプリケーションごとベース及び装置ごとベースにネットワークシステムから安全性パラメータの収集を受信して、モバイル無線通信装置及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性のパラメータの収集に基づいて航空機システムにアクセスするように構成されることができる。

【0012】

信頼されるモバイル通信のための方法は、ネットワークシステムによって、アプリケーションごとベース及び装置ごとベースの安全性パラメータの収集を用いてモバイルクライアントシステムを設定すること；及びモバイルクライアントシステム及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システムに対するアクセスをモバイルクライアントシステムに提供することを含む。方法はさらに、ネットワークシステムによって、モバイルクライアントシステムを評価することを含み、ここで、安全性パラメータの収集を用いたモバイルクライアントシステムの設定は、モバイルクライアントシステムの評価に基づく。方法はさらに、デジタル公証人によって安全性パラメータの収集に署名又は押印することのうちの少なくとも1つ；及びモバイルクライアントシステムの上に、少なくとも署名されたか又は押印された安全性パラメータの収集を記憶することを含む。

【0013】

方法はさらに、モバイルクライアントシステムによって、航空機システムに対するアクセスのリクエストを送ることを含み、ここで、リクエストは、少なくとも署名されたか又は押印された安全性パラメータの収集を含み；航空機システムによって、デジタル公証人の同一性に基づいてモバイルクライアントシステムから受信した署名されたか又は押印された安全性パラメータの収集を解読すること；及び航空機システムによって、解読された安全性パラメータの収集に基づいて航空機システムに対するアクセスをモバイルクライアントシステムに提供するか否かを決定することを含む。

【0014】

方法では、航空機システムによる決定は、解読された安全性パラメータの収集に基づいて、モバイルクライアントシステムによってアクセス可能となる特定の搭載されているアプリケーション及び特定の搭載されているデータを決定することを含む。方法はさらに、デジタル公証人を使用して、安全性パラメータの収集に対する信頼の連鎖を確立することを含む。方法では、航空機システムは、モバイルクライアントシステムについての情報を前もって有することなしに、確立された信頼の連鎖に基づいてモバイルクライアントシステムに対するアクセスを提供する。

【0015】

信頼されるモバイル通信のためのシステムは、ネットワークシステム；及びモバイルクライアントシステムがネットワークシステムに関してオンラインである場合に、ネットワークシステムと通信するモバイルクライアントシステムを備え、ここで、ネットワークシステムはアプリケーションごとベース及び装置ごとベースの安全性パラメータの収集を用いてモバイルクライアントシステムを設定し、モバイルクライアントシステムは、モバイ

10

20

30

40

50

ルクライアントシステム及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システムに対するアクセスが提供される。システムでは、ネットワークシステムがモバイルクライアントシステムを評価し、ここで、ネットワークシステムは、モバイルクライアントシステムの評価に基づいて、安全性パラメータの収集を用いてモバイルクライアントシステムを設定する。

【0016】

システムでは、安全性パラメータの収集がデジタル公証人によって署名又は押印され、署名又は押印された安全性パラメータの収集が、モバイルクライアントシステムの上に記憶される。システムでは、デジタル公証人が、安全性パラメータの収集に対して信頼の連鎖を確立する。システムでは、航空機システムは、モバイルクライアントシステムについて10
の情報を前もって有することなしに、確立された信頼の連鎖に基づいて、モバイルクライアントシステムに対するアクセスを提供する。

【0017】

システムでは、モバイルクライアントシステムは、航空機システムに対するアクセスのためのリクエストを送り、ここで、リクエストは安全性パラメータの収集を含み、航空機システムはデジタル公証人の同一性に基づいて、モバイルクライアントシステムから受信した安全性パラメータの収集を解釈し、航空機システムはモバイルクライアントシステムについて20
の情報を前もって有することなしに、解釈された安全性パラメータの収集に基づいて航空機システムに対するアクセスをモバイルクライアントシステムに提供するか否かを決定する。システムでは、航空機システムが、解釈された安全性パラメータの収集に基づいて、モバイルクライアントシステムによってアクセスされる特定の搭載されているアプリケーション及び特定の搭載されているデータを決定する。

【0018】

モバイル無線通信装置は、1以上のメモリ；及び1以上のメモリに結合される1以上のプロセッサを備え、ここで、1以上のプロセッサは、アプリケーションごとベース及び装置ごとベースにネットワークシステムから安全性パラメータの収集を受信して、モバイル無線通信装置及び航空機システムがネットワークシステムに関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システムにアクセスするように構成される。モバイル無線通信装置では、1以上のプロセッサは、モバイル無線通信装置がネットワークシステムに関してオンラインである場合に、モバイル無線通信装置について30
の情報をネットワークシステムに送信するように構成され、どの安全性パラメータの収集を用いてモバイル無線通信装置を設定するかが、送信された情報に基づいてネットワークシステムによって決定される。

【0019】

モバイル無線通信装置では、安全性パラメータの収集が、1以上のプロセッサによって受信される前に、デジタル公証人によって署名され又は押印され、1以上のプロセッサは、署名され又は押印された安全性パラメータの収集を1以上のメモリに記憶するように構成される。モバイル無線通信装置では、航空機システムが、モバイル無線通信装置について40
の情報を前もって有することなしに、モバイル無線通信装置に対するアクセスを提供する。

【0020】

モバイル無線通信装置では、1以上のプロセッサが、航空機システムに対するアクセスのためのリクエストを送り、ここで、リクエストは、少なくとも署名されたか又は押印された安全性パラメータの収集を含み、リクエストに反応して航空機システムによって送信された1以上のキーを受信し、1以上のキーを使用して1以上のメモリに記憶された他のパラメータ又はデータを解釈し、ここで、1以上のキーは、アプリケーション特有のものであり、かつ解釈された他のパラメータ又は解釈されたデータを使用してモバイル無線通信装置及び航空機システムの間の通信を容易にするように構成される。モバイル無線通信装置では、航空機システムが、解釈された安全性パラメータの収集に基づいて、モバイル無線通信装置によってアクセスされる特定の搭載されているアプリケーション及び特定の50

搭載されているデータを決定する。

【0021】

これら及び他の利点、態様、及び新規な特徴は、それらの説明される実施例の詳細と同様に、後述の説明及び図面からより完全に理解されるであろう。

【0022】

上述の特徴、機能、及び利点は、様々な実施例において独立に実現することが可能であり、また別の実施例において組み合わせることも可能であり、これらの実施例について、以下の説明および図面を参照してさらに詳細に説明する。

【図面の簡単な説明】

【0023】

【図1】図1は、航空会社の事務管理部門のシステム及び航空機システムに対する信頼されるモバイル装置及びアプリケーションサービスの相互接続性のためのシステムの実施例を示している。

【図2】図2は、航空会社の事務管理部門のシステムに対する信頼されるモバイル装置及びアプリケーションサービスの相互接続性のための方法の実施例の流れ図を示している。

【図3A】、及び

【図3B】図3A及び図3Bは、航空機システムに対する信頼されるモバイル装置及びアプリケーションサービスの相互接続性のための方法の実施例の流れ図を示している。

【図4】図4は、モバイルクライアントシステムの実施例を示している。

【発明を実施するための形態】

【0024】

いくつかの実施例は、信頼されるモバイル通信のためのシステム及び方法を提供する。特定の実施例の多くの具体的な詳細が、このような実施例の完全な理解を促すために、図面と同様に後述の説明の中で説明される。しかしながら、当業者は、付加的な実施例が存在し、又は特定のこれらの実施例が以下の説明におけるいくつかの詳細なしに実施され得ることを理解するだろう。同じ参照番号は、図面全体において同じ要素を示す。

【0025】

いくつかの実施例は、モバイルクライアントシステム及び航空機システムが航空会社の事務管理部門のシステムに対するリーチバックネットワークの接続性を有していないと想定する一方で、航空機システムに対するネットワークの接続性又はアプリケーションの相互作用のいずれかを可能にする前に、サイバーセキュリティの観点から、モバイルクライアントシステム及びクライアントアプリケーションの整合性及び状態を評価する。実施例において、航空会社の事務管理部門のシステムによってアクセスされるデジタル公証人は、モバイルクライアントシステムの健全性及び状態を評価するため、かつ航空機の内側のシステムにアクセス制御パラメータを割り当てるために、搭載されている航空機システムによって後に使用される、システムの安全性の属性の収集のための信頼の連鎖を確立するために使用される。アクセス制御パラメータは、モバイルクライアントシステムが前もって特定の航空機システムに登録されていなくても、かつモバイルクライアントシステム及び航空機システムが航空会社の事務管理部門に対するリーチバックの接続性を有していないと想定されていても、モバイルクライアントシステムに割り当てられることができる。

【0026】

いくつかの実施例は、航空会社の企業ネットワークの中に存在する航空会社の事務管理部門に対して接続される一方で、モバイルクライアントシステムの上に集められる一連の安全性パラメータのための信頼の連鎖を確立する。その後、安全性パラメータは、モバイルクライアントシステム及び航空機システムの両者が、ネットワーク化された認証、認可、及びアカウントティング(AAA)の目的で、航空会社の事務管理部門に対するリーチバックの接続性を有しないと想定されるところで、搭載されている航空機システムによって様々なアクセス制御制約を、搭載されているシステム、データ、及びアプリケーションに割り当てるために使用される。信頼の連鎖は、特定の搭載されている航空機システムに前

10

20

30

40

50

もって登録されておらず、かつ航空会社の事務管理部門に対するリーチバックの接続性が存在しない場合であっても効果的であり得る、モバイルクライアントシステムのための信頼のレベルを確立する基礎である。

【0027】

図1を参照すると、航空会社の事務管理部門のシステム及び航空機システムに対する信頼されるモバイル装置及びアプリケーションサービスの相互接続性のためのシステムの実施例が図解されている。例えば、システム100は、モバイルクライアントシステム110、ネットワークシステム120、及び航空機システム130を含むことができる。

【0028】

モバイルクライアントシステム110は、無線リンク及び／又は有線リンクを介して、ネットワークシステム120及び／又は航空機システム130に結合されることができる。例えば、モバイルクライアントシステム110は、モバイル無線通信装置、携帯電話、スマートフォン、ラップトップ、タブレット、個人用デジタル補助装置などである。モバイルクライアントシステム110はまた、民生品を利用した(COTS)モバイル装置であり得る。実施例において、モバイルクライアントシステム110は、種々の種類の無線通信及び有線通信に対して構成されることができる。図1を参照すると、モバイルクライアントシステム110は、民間航空サービス(CAS)のアプリケーション140及び信頼されるネットワーク接続(TNC)のアプリケーションラッパー150などのモバイルアプリケーションを提供する。CASのアプリケーション140は、本明細書の中において議論を容易にするためのモバイルアプリケーションの単なる実施例である。実施例において、モバイルクライアントシステム110は、CASのアプリケーション140の代わりに又はCASのアプリケーション140に加えて、1以上の他のモバイルアプリケーションを提供することができる。例えば、CASのアプリケーション140は、航空サービスのプロバイダーのアプリケーションを含むことができ、かつ航空機の運航、整備、及び保守のために使用されることができる。TNCのアプリケーションラッパー150は、証明書を管理するため、アプリケーションコントロールを管理するため、かつモバイルクライアントシステム110の上に記憶されるデータを加え、削除し、及び／又は解読するために、モバイルクライアントシステム110のシステム監査(例えば、受動的及び／又は能動的なシステム監査)を実行するために使用されることができる。CASのアプリケーション140及びTNCのアプリケーションラッパー150は、互いに通信するように構成される。TNCのアプリケーションラッパー150はまた、ネットワークシステム120及び航空機システム130と通信するように構成される。例えば、TNCのアプリケーションラッパー150は、主たるアプリケーションの遂行の前に遂行されることができ、かつ他のシステムとどのようにして接続するか及び他のシステムへ若しくは他のシステムからどのようにしてデータを移動するかを決定することができる。

【0029】

図1を参照すると、例えば、ネットワークシステム120の実施例は、航空会社の情報技術(IT)の企業ネットワーク160、デジタル公証人170、及び企業ポリシー施行点(EPEP)180を含むことができる。航空会社のITの企業ネットワーク160、デジタル公証人170、及びEPEP180は、互いに通信するように構成されることができる。航空会社のITの企業ネットワーク160及びモバイルクライアントシステム110は、互いに通信するように構成されることができる。ネットワークシステム120又はその一部は、航空会社の事務管理部門のシステムの一部となることができる。例えば、航空会社の事務管理部門のシステムは、ネットワークシステム120を含むことができる。航空会社の事務管理部門のシステムの別の実施例は、航空会社のITの企業ネットワーク160及びEPEP180を含むことができる。航空会社の事務管理部門のシステムのさらに別の実施例は、航空会社のITの企業ネットワーク160を含むことができる。

【0030】

図1を参照すると、例えば、航空機システム130の実施例は、ポリシー施行点(PEP)190、孤立した搭載されているネットワーク(ION)TNCチャレンジャー20

10

20

30

40

50

0、及び搭載されているアプリケーション210を含むことができる。航空機システム130は、搭載されている及び搭載されていないアプリケーションに対して、ブロードバンドの搭載されている及び搭載されていない接続性を提供することができる。航空機システム130は、電子対応可能サービスを実行するために航空機システム130と接続する、COTSラップトップ、タブレット、スマートフォン、モバイル無線通信装置などに対応している。例えば、航空機システム130は、以下のうちの1以上を提供することができる：すなわち、有線イーサネット（登録商標）ポート、サーバ、コアネットワーク、プリンター、ローカルエリアネットワーク（LANs）、ワイドエリアネットワーク（WANs）、パーソナルエリアネットワーク（PANs）、LAN/WAN/PANターミナル装置、無線LANs/WANs/PANs、及び無線LAN/WAN/PANターミナル装置である。例えば、航空機システム130は、以下のうちの1以上のために構成される、及び／又は以下のうちの1以上を提供することができる、電子対応可能の搭載されている装備及び装置を提供することができる：すなわち、搭載されている保守及びモニタリング；検査、データ、ログ又はファイルのアップロード又はダウンロード；クルー情報システム；無線保守アクセス；無線オペレーションアクセス；搭載されている性能ツール；電子文書ブラウザ；並びにソフトウェア、データ、チャート、及びマニュアルの遠隔展開である。

10

【0031】

実施例において、PEP190、IONTNCチャレンジャー200、及び搭載されているアプリケーション210は、ION220の一部となることができる。例えば、実施例において、IONTNCチャレンジャー200は、アプリケーションチャレンジャーサーバ（ACS）及びポリシー定義点（PDP）を含むことができる。PEP190及びIONTNCチャレンジャー200は、互いに通信するように構成されることができる。PEP190及び搭載されているアプリケーション210は、互いに通信するように構成されることができる。PEP190及びモバイルクライアントシステム110は、互いに通信するように構成されることができる。

20

【0032】

図1から図3を一緒に参照すると、実施例にしたがったシステム100のオペレーションが、説明されている。

【0033】

ステップ230において、モバイルクライアントシステム110は、無線リンク及び／又は有線リンクを介して、ネットワークシステム120に結合する。実施例において、モバイルクライアントシステム110のTNCのアプリケーションラッパー150は、ネットワークシステム120とのトランスポート層セキュリティ（TLS）/TNC接続をセットアップすることができる。

30

【0034】

ステップ240において、モバイルクライアントシステム110のTNCのアプリケーションラッパー150は、モバイルクライアントシステム110のシステム監査を実行することができる。例えば、システム監査は、アップデートされたシステム監査とすることができる。監査の結果は、ネットワークシステム120に送られる一連のパラメータである。例えば、パラメータは、以下のうちの1以上を示すことができる：すなわち、作動システム、アプリケーション、アプリケーションパラメータ、モバイルクライアントシステムの状態、ハードウェア構成、ブートパラメータ、及びモバイルクライアントシステム110の同一性である。実施例において、一連のパラメータは、航空会社のITの企業ネットワーク160に送られる。例えば、一連のパラメータはまた、単純なプレイバック攻撃を妨げるために、航空会社のITの企業ネットワーク160によって提供される暗号法のノンスを含むことができる。

40

【0035】

ステップ250において、ネットワークシステム120は、モバイルクライアントシステム110を評価する。例えば、評価は、モバイルクライアントシステム110からネッ

50

トワークシステム120によって受信された一連のパラメータを分析することを含む。実施例において、航空会社のITの企業ネットワーク160は、モバイルクライアントシステム110から一連のパラメータを受信して、一連のパラメータを分析することによってモバイルクライアントシステム110を評価する。実施例において、航空会社のITの企業ネットワーク160は、モバイルクライアントシステム110の同一性をモバイル機器管理(MDM)データベースと比較することによって、航空会社のITの企業ネットワーク160がモバイルクライアントシステム110となじみがあるかどうかを決定する。航空会社のITの企業ネットワーク160は、受信した一連のパラメータからモバイルクライアントシステム110の健全性及び状態を評価する。

【0036】

10

ステップ260において、ネットワークシステム120は、モバイルクライアントシステム110の評価に基づいて、安全性パラメータの収集を決定する。例えば、実施例において、EPEP180は、以下のうちの1以上を含む安全性パラメータの収集を決定する：すなわち、モバイルクライアントシステム110に対する、認証情報、規則、及び限定（例えば、アクセスの限定、位置の限定など）である。ネットワークシステム120はまた、装置の同一性の証明書をモバイルクライアントシステム110に割り当てる。

【0037】

ステップ270において、ネットワークシステム120は、安全性パラメータの収集をデジタル公証人170に送る。実施例において、EPEP180は、安全性パラメータの収集をデジタル公証人170に送る。デジタル公証人170は、よく知られた又は個人的な認証機関（例えば、ベリサイン、航空会社など）であり得る。例えば、デジタル公証人170は、複数の認証機関を含むことができる。

20

【0038】

ステップ280において、デジタル公証人170は、安全性パラメータの収集に署名及び／又は押印する。実施例において、デジタル公証人170は、現在データの証明書をを用いて安全性パラメータの収集を暗号化する。実施例において、デジタル公証人170は、1以上のキーを用いて安全性パラメータの収集に署名及び／又は押印する。実施例において、安全性パラメータの収集は、ハッシュ関数を通り抜けさせられることができる。例えば、実施例において、署名された及び／又は押印された安全性パラメータの収集は、プロフィール及び署名されたパラメータの種類・長さ・値(TLV)の収集を設定することを含む。例えば、デジタル公証人170によって署名されたパラメータのTLVの収集は、以下のうちの1以上を含むことができる：すなわち、装置の同一性の証明書、署名の日時、満了期間（例えば、タイムトゥライブパラメータ）、ジオフェンシング目的のための使用位置（例えば、位置の限定）、航空機の飛行フェーズの制約、及び暗号化されたアプリケーション詳細データである。デジタル公証人170は、安全性パラメータの収集のための信頼の連鎖を確立するために使用されることができる。

30

【0039】

ステップ290において、ネットワークシステム120は、安全性パラメータの収集を用いてモバイルクライアントシステム110を設定する（例えば、署名及び／又は押印された安全性パラメータの収集）。実施例において、ネットワークシステム120は、アプリケーションごとベース及び／又は装置ごとベースの安全性パラメータの収集を用いてモバイルクライアントシステム110を設定する。実施例において、署名及び／又は押印された安全性パラメータの収集は、デジタル公証人170から、航空会社のITの企業ネットワーク160を介して、例えば、モバイルクライアントシステム110のTNCのアプリケーションラッパー150に署名及び／又は押印された安全性パラメータの収集を送るEPEP180に送られる。例えば、実施例において、モバイルクライアントシステム110は、企業ポリシーを実施するMDMプロフィール；及び／又は、例えば、装置の同一性を含みデジタル公証人170へチェーンバックする1以上のTNC証明書を用いて、設定されることができる。それゆえ、モバイルクライアントシステム110の設定は、ネットワークシステム120によるモバイルクライアントシステム110の評価に基づき、今

40

50

度は、モバイルクライアントシステム 110 の設定が、TNC アプリケーションラッパーによるモバイルクライアントシステム 110 のシステム監査に基づく。

【0040】

図 3A を参照すると、ステップ 300 において、モバイルクライアントシステム 110 は、無線リンク及び／又は有線リンクを介して、航空機システム 130 に対するアクセスのためのリクエストを送る。実施例において、モバイルクライアントシステム 110 は、航空機システム 130 を有する航空機の中又は近くにある。実施例において、モバイルクライアントシステム 110 も航空機システム 130 も、ネットワークシステム 120 と通信しない。モバイルクライアントシステム 110 は、割り当てられた装置の同一性の証明書を使用して、TLS/TNC 接続を確立することができる。証明書は、データを解読するために使用されることができる。例えば、リクエストは、航空機システム 130 に対する署名及び／又は押印された安全性パラメータの収集を含むことができる。実施例において、リクエストは、デジタル公証人 170 によって署名されたパラメータの TLV の収集を含む。例えば、リクエストはまた、モバイルクライアントシステム 110 のシステム監査を含むことができる。システム監査は、例えば、TNC のアプリケーションラッパー 150 によって実行された以前のシステム監査であってよく、又はシステム監査は TNC のアプリケーションラッパー 150 によって実行されるアップデートされた若しくは新しいシステム監査であってもよい。実施例において、モバイルクライアントシステム 110 の TNC のアプリケーションラッパー 150 は、リクエストを航空機システム 130 の PEP 190 に対して送る。例えば、リクエストはまた、単純なプレイバック攻撃を妨げるために、ネットワークシステム 120 によって以前に提供された暗号法のノンスを含むことができる。実施例において、モバイルクライアントシステム 110 によって記憶される署名及び／又は押印された安全性パラメータの収集は、航空機システム 130 に対して提示される前に、モバイルクライアントシステム 110 の内側の安全性の高いハードウェアモジュール（例えば、信頼されるプラットフォームモジュール）によって新たに署名された一連のパラメータのマッチングに同伴される。この方法は、航空機システム 130 がモバイルクライアントシステム 110 の安全性の状態の新しさを確認することを可能にする。

【0041】

ステップ 310 において、航空機システム 130 は、モバイルクライアントシステム 110 が信頼できるかどうか、かつ航空機システム 130 がモバイルクライアントシステム 110 に対するアクセスを提供するかどうかを決定するために、リクエストを分析する。実施例において、PEP 190 は、モバイルクライアントシステム 110 からリクエストを受信して、リクエストを IONTNC チャレンジャー 200 に送る。例えば、IONTNC チャレンジャー 200 は、デジタル公証人 170 によって署名されたパラメータの TLV の収集、及びモバイルクライアントシステム 110 のシステム監査を含むリクエストを解釈することができる。IONTNC チャレンジャーはまた、装置の同一性の証明書の有効性、位置、及び／又は装置の飛行フェーズの制約をチェックすることができる。

【0042】

クエリー 320 において、航空機システム 130 は、安全性パラメータの収集が、認識される及び／又は信頼されるデジタル公証人 170 によって、押印及び／又は署名されたかどうかを決定する。実施例において、IONTNC チャレンジャー 200 は、安全性パラメータの収集が、認識される及び／又は信頼されるデジタル公証人 170 によって、押印及び／又は署名されたかどうかを決定する。IONTNC チャレンジャーは、信頼される及び／又は認識されるデジタル公証人 170 の搭載されているデータベースに対するアクセスを有することができる。IONTNC チャレンジャーは、モバイルクライアントシステムデータと照合することによって、署名されたデータの有効性を確認することができる。

【0043】

ステップ 330 において、航空機システム 130 が安全性パラメータの収集に押印した及び／又は署名したデジタル公証人 170 を認識及び／又は信頼できない場合、その後、

航空機システム 130 は、モバイルクライアントシステム 110 に対するアクセスを航空機システム 130 に提供しない。例えば、実施例において、IONTNC チャレンジャー 200 は、認識及び／又は信頼されたデジタル公証人が安全性パラメータの収集に押印及び／又は署名しなかったと決定することができる。その後、IONTNC チャレンジャー 200 は、PEP 190 に、モバイルクライアントシステム 110 に対するアクセスを航空機システム 130 に提供しないという情報を与える。

【0044】

ステップ 340 において、航空機システム 130 が安全性パラメータの収集に押印した及び／又は署名したデジタル公証人 170 を認識及び／又は信頼する場合、その後、航空機システム 130 は、押印及び／又は署名された安全性パラメータの収集を解読する。実施例において、押印及び／又は署名された安全性パラメータの収集の解読は、デジタル公証人 170 の同一性に基づく。実施例において、航空機システム 130 は、押印及び／又は署名された安全性パラメータの収集を解読するために、認識及び／又は信頼されたデジタル公証人 170 に関連する 1 以上のキー（例えば、1 以上のデータ解読キー）を提供することができる。例えば、実施例において、IONTNC チャレンジャー 200 は、認識及び／又は信頼されたデジタル公証人が、安全性パラメータの収集に押印及び／又は署名したことを決定することができ、かつ航空機システム 130 のデータベースに記憶された 1 以上のキーを取得することができる。実施例において、1 以上のキーは航空機システム 130 の上に前もって記憶されている。実施例において、IONTNC チャレンジャー 200 は、例えば、モバイルクライアントシステム 110 から受信したデータを解読するために使用されることができる、航空機システム 130 のデータベースの中に記憶されるデータの証明書を提供することができる。

【0045】

クエリー 350 において、航空機システム 130 は、モバイルクライアントシステム 110 から受信した解読された安全性パラメータの収集に基づいて、航空機システム 130 に対するアクセスをモバイルクライアントシステム 110 に提供するかどうかを決定する。実施例において、モバイルクライアントシステム 110 に対して提供されるアクセスは、前もってモバイルクライアントシステム 110 についての情報を有することなしに、又はリクエストを受信することに先立って、かつネットワークシステム 120 に対するリンクなしに、送信された安全性パラメータの収集に基づく。

【0046】

ステップ 360 において、航空機システム 130 は、航空機システム 130 に対してモバイルクライアントシステム 110 に対するアクセスを否定する。実施例において、少なくとも PEP 190 及び IONTNC チャレンジャー 200 の PDP は、受信した解読された安全性パラメータの収集に基づいてアクセスを否定することができる。例えば、受信された解読された安全性パラメータの収集は、満足されない特定のフィールド位置（例えば、「シアトルだけで働く」）を示すことができる。

【0047】

図 3B を参照すると、ステップ 365 において、航空機システム 130 は、航空機システム 130 に対してモバイルクライアントシステム 110 に対するアクセスを提供する。実施例において、少なくとも PEP 190 及び IONTNC チャレンジャー 200 の PDP は、受信した解読された安全性パラメータの収集に基づいてモバイルクライアントシステム 110 に対するアクセスを提供することができる。例えば、受信した解読された安全性パラメータの収集及び受信したモバイルクライアントシステム 110 のシステム監査に基づいて、航空機システム 130 は、モバイルクライアントシステム 110 によってアクセスされる特定の搭載されているアプリケーションおよび特定の搭載されているデータを決定することができる。航空機システム 130 にアクセスする一方で、モバイルクライアントシステム 110 は、モバイルクライアントシステム 110 の上に記憶されたデータをシェアして、航空機システム 130 の上に記憶されたデータをダウンロードし、航空機システム 130 の上にデータをアップロードし、及び／又は航空機システム 130 の上で作

動するソフトウェア（例えば、アプリケーション、作動システムなど）をインストールし若しくはアップデートすることができる。例えば、C A S のアプリケーション 1 4 0 などのモバイルクライアントシステム 1 1 0 の上で作動するアプリケーションは、航空機システム 1 3 0 の上のアプリケーション及びサービスを維持して作動させるために使用されることができる。

【0048】

ステップ 3 7 0 において、航空機システム 1 3 0 は、モバイルクライアントシステム 1 1 0 に対して 1 以上のキーを送信する。実施例において、航空機システム 1 3 0 から受信された 1 以上のキーは、ステップ 3 4 0 において、押印及び／又は署名された安全性パラメータの収集を解読するために、航空機システム 1 3 0 によって使用された 1 以上のキーとは同じではない。モバイルクライアントシステム 1 1 0 によって受信された 1 以上のキーは、装置特有及び／又はアプリケーション特有のものであり得る。それゆえ、実施例において、モバイルクライアントシステム 1 1 0 は、モバイルクライアントシステム 1 1 0 及び航空機システム 1 3 0 のアプリケーション（例えば、パイロットアプリケーション、保守アプリケーション、他のモバイルアプリケーションなど）の間の通信を容易にする、1 以上のキーの複数のセットを受信することができる。

【0049】

ステップ 3 8 0 において、モバイルクライアントシステム 1 1 0 は、航空機システム 1 3 0 によって送信された 1 以上のキーを受信する。

【0050】

ステップ 3 9 0 において、モバイルクライアントシステム 1 1 0 は、安全性パラメータの収集及び／又は他のパラメータ及び／又はそこに記憶されているデータを解読するために、1 以上のキーを使用する。実施例において、1 以上のキーは、安全性パラメータの収集、安全性パラメータの収集の一部、又はモバイルクライアントシステム 1 1 0 に記憶されている他のパラメータ及び／又はデータを無押印及び／又は無署名にするために、モバイルクライアントシステム 1 1 0 によって使用されることができる。実施例において、1 以上のキーは、モバイルクライアントシステム 1 1 0 を評価するために航空機システム 1 3 0 によって使用された安全性パラメータを解読するために使用されることはできない。実施例において、T N C のアプリケーションラッパー 1 5 0 は、モバイルクライアントシステム 1 1 0 の中に存在するデータ（例えば、アプリケーションデータセクション）を解読又は除去するために、1 以上のキーを使用する。実施例において、1 以上のキーによって解読されることができるパラメータ及び／又はデータは、例えば、ポート番号（例えば、航空機システム 1 3 0 のネットワークに基づくサービスに対するポート）、サービスに対して接続するための接続認識情報（例えば、ユーザログイン及びパスワードなど）、モバイルアプリケーションがその機能を実行するために必要な補助的なデータなどの、航空機システム 1 3 0 との通信を容易にする極秘のパラメータ及び／又はデータを含む。そのような情報は、例えば、ネットワークシステム 1 2 0 によって、及び／又は特定のアプリケーションがモバイルクライアントシステム 1 1 0 の上にインストールされる場合に、モバイルクライアントシステム 1 1 0 の上に記憶されてきたはずである。

【0051】

ステップ 4 0 0 において、モバイルクライアントシステム 1 1 0 は、解読された安全性パラメータの収集、解読された安全性パラメータの収集の一部、及び／又は他の解読されたパラメータ及び／又はデータを使用して、航空機システム 1 3 0 と通信する。実施例において、1 以上のキーは、アプリケーション特有及び装置特有であり、かつモバイルクライアントシステム 1 1 0 及び航空機システム 1 3 0 の特定のアプリケーションの間の通信を容易にするために使用されることができる特定の情報を解読する。実施例において、1 以上のキーはまた、モバイルクライアントシステム 1 1 0 及び航空機システム 1 3 0 の間の通信を暗号化及び／又は解読するために使用されることができる。モバイルクライアントシステム 1 1 0 はまた、航空機システム 1 3 0 に対して提供されるシステムデータに署名するために使用されることができる安全性構成要素（例えば、信頼されるプラットフォ

10

20

30

40

50

ームモジュール)を含むことができ、安全性構成要素は、安全性の状態情報の新しさを保証することができる。

【0052】

図4は、モバイルクライアントシステム110の実施例を示している。モバイルクライアントシステム110は、1以上のプロセッサ410及び1以上のメモリ420を含む。1以上のプロセッサ410及び1以上のメモリ420は、1以上のバス430を介して結合されることができる。入力／出力(I/O)装置又はインターフェース440が、1以上のバス430に結合される。例えば、I/O装置又はインターフェース440は、ディスプレイ、タッチスクリーン、スピーカー、マイクロフォン、キーボードなどを含むことができる。通信装置又はインターフェース450はまた、1以上のバス430に結合される。例えば、通信装置又はインターフェースは、無線送信機及び有線送信機(例えば、イーサネット(登録商標)インターフェース)を含むことができる。例えば、無線送信機は、IEEE802.11無線通信、ブルートゥース通信、赤外線通信、無線ローカルエリアネットワーク通信、移動体通信、衛星通信などをサポートすることができる。無線送信機は、各々が1以上のアンテナをサポートすることができる。

10

【0053】

データ、コード、及び／又は指示は、1以上のメモリ420の上に記憶されることができ、コード及び／又は指示は1以上のプロセッサ410によって遂行されることができ、本明細書の中において説明される又は当業者に知られているアプリケーション、特徴、オペレーション、及び／又は機能を提供する。実施例において、データ、コード、及び／又は指示は、1以上のプロセッサ410によって遂行されることができ、1以上のプロセッサ及びモバイルクライアントシステム110(例えば、モバイル無線通信装置)を構成して、アプリケーションごとベース及び装置ごとベースにネットワークシステムから安全性パラメータの収集を受信し、モバイルクライアントシステム110及び航空機システム130がネットワークシステム120に関してオフラインである場合に、安全性パラメータの収集に基づいて航空機システム130にアクセスする。1以上のプロセッサ410はまた、本明細書の中において説明される他のオペレーションを実行するように構成されることができる。

20

【0054】

実施例において、ネットワークシステム120及び航空機システム130は、図4に示されるような類似の構成を有するサーバ又はコンピュータシステムを含むことができる。データ、コード、及び／又は指示は、1以上のメモリ420の上に記憶されることができ、コード及び／又は指示は1以上のプロセッサ410によって遂行されることができ、本明細書の中において説明される又は当業者に知られているネットワークシステム120及び航空機システム130のためのアプリケーション、特徴、オペレーション、及び／又は機能を提供する。

30

【0055】

いくつかの実施例は、航空機ネットワークのプロセス及びシステムに対する信頼される接続を履行するアプリケーションを提供する。

【0056】

いくつかの実施例は、航空会社の事務管理部門のシステムにおけるアプリケーションごとベース及び装置ごとベースの安全性パラメータの収集を確立するために、包括的なアプリケーションおよびシステムの評価を提供する。

40

【0057】

いくつかの実施例は、モバイル無線装置などのモバイルクライアント装置の中に記憶される安全性パラメータの収集に署名及び押印するデジタル公証人の構成を使用することによって、安全性パラメータの信頼の連鎖を確立する。

【0058】

いくつかの実施例は、航空会社のシステムとの接続性のオフラインモードにおける資源に制約のあるモバイルクライアントシステム(例えば、資源に制約のあるモバイルクライ

50

アント装置) から回収されるデータのための、データの整合性の信頼できかつ拒否できない確立を可能にする。

【0059】

いくつかの実施例は、資源に制約のあるモバイルクライアントシステムから回収されるデータの整合性を立証する複数のデータの整合性の情報源の使用を許容する。

【0060】

いくつかの実施例は、先立つ情報及び／又は航空機システムによるモバイルクライアントシステムの認知なしに、複数の航空機システムが電子対応可能な機能に対してモバイルクライアントシステムを使用することを可能にする、航空会社の事務管理部門のシステムの信頼できるキャッシュメモリの履歴を維持して提供する、資源に制約のあるモバイルク

10

【0061】

いくつかの実施例は、航空機上の検証された安全性パラメータの収集を使用して、モバイルクライアントシステムを前もって知ることなしに、様々な航空機のネットワーク、データ、及びアプリケーションに対して、モバイルクライアントシステム及びアプリケーションのためのアクセス制御パラメータを動的に確立する。

【0062】

いくつかの実施例は、COTSモバイル装置の整合性が、航空会社の事務管理部門によって定義されたスケジュールにしたがってサイバーセキュリティの観点から検証されることを確実にする。特定のCOTSモバイル装置の整合性の検証は、電子対応可能な航空機システム及びCOTSモバイル装置が作動に関して制約があり、かつ航空会社の事務管理部門に接続できない場合に、特定のCOTSモバイル装置が電子対応可能な航空機システムに接続することを許容されるべきかどうかを決定することにおいて1つの要因となる。

20

【0063】

いくつかの実施例は、モバイルクライアントシステムがセキュリティモジュール又はプロセッサを含むと定めている。例えば、セキュリティモジュール又はプロセッサは、航空機システムがリクエストした時に、キャプティブキーを用いて航空機システムからの安全性パラメータ及び一意のメッセージに署名するように構成されることができる。これは、パラメータが認可された装置に由来することを保証する(例えば、署名及び／又は押印されたパラメータの収集が、単純に欠陥のある装置から外に出されてこなかった)。これはまた、パラメータが、航空機からの署名された一意のメッセージ(例えば、ノンス)を介して、装置の、いくらか古びたものではない、現在の状態を表現することを保証する。

30

【0064】

他の実施例は、非一時的なコンピュータ可読媒体及び／又は記憶媒体、並びに／又は非一時的な機械可読媒体及び／又は記憶媒体を提供し、それらはそこに機械及び／又はコンピュータによって実行可能な少なくとも1つのコードセクションを有する機械コード及び／又はコンピュータプログラムを記憶し、それによって、機械及び／又はコンピュータが回転するシャフトの上のセンサ及びデータ伝送のための統合されたアンテナ送信機のため

40

【0065】

したがって、本開示の実施例は、ハードウェア、ソフトウェア、又はハードウェア及びソフトウェアの組合せにおいて実現可能である。本実施例は、少なくとも1つのコンピュータシステムに集中させて、又は相互接続した複数のコンピュータに異なる要素を分散させた分散型で実現される。本明細書の中において記載された方法を実行するために適合された任意の種類のコンピュータシステム又は他のシステムが適している。ハードウェアとソフトウェアの通常の組み合わせは、読み込まれ実行されるときに、本明細書の中において述べられた方法を実行するためにコンピュータシステムを制御するコンピュータプログラムを含む汎用コンピュータシステムとされる。

50

【0066】

本開示の実施例はまた、本明細書の中において記載された方法の実施を可能にするすべての特性を含み、かつコンピュータシステムに読み込まれるときにこれらの方法を実行することができるコンピュータプログラム製品に埋め込むこともできる。本文脈でいうコンピュータプログラムとは、情報処理能を有するシステムに、直接的に、又はa)別の言語、コード、又は表記法への変換と、b)異なる材料形態での再生産の一方又は両方を行った後で、特定の機能を実行させることを目的とする一連の命令の、あらゆる表現、あらゆる言語、コード、又は表記法を意味する。

【0067】

特定の実施例を参照しながら説明してきたが、当業者であれば、本開示の実施例の範囲から逸脱することなく変形例が可能であること、及びその要素を同等物に置換することが可能であることを理解するだろう。加えて、本開示の範囲から逸脱することなく、特定の状況又は材料を本教示に適合させるために、多くの修正が加えられることが可能である。したがって、本開示の実施例は、開示された特定の実施例に限定されるものではなく、添付された特許請求の範囲内に含まれる全ての実施例を含む、ことが意図されている。

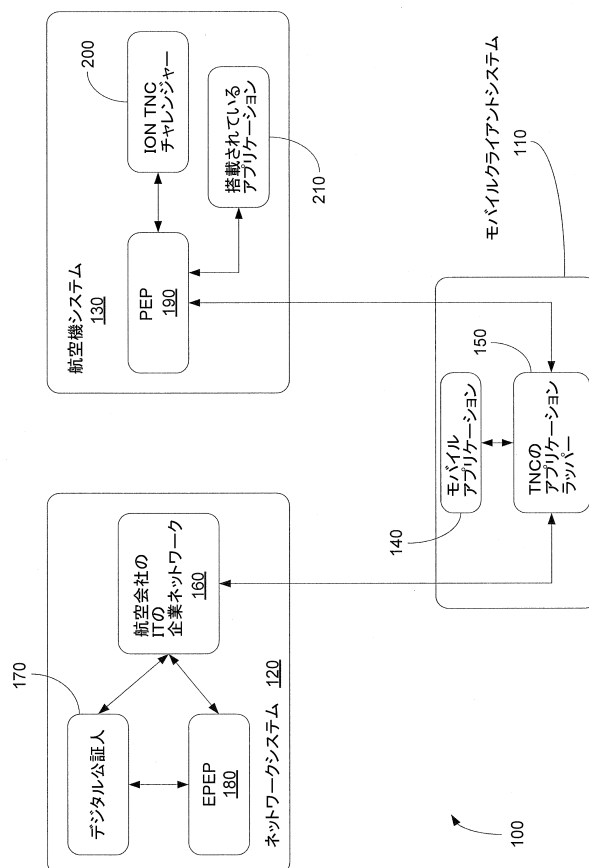
【符号の説明】

【0068】

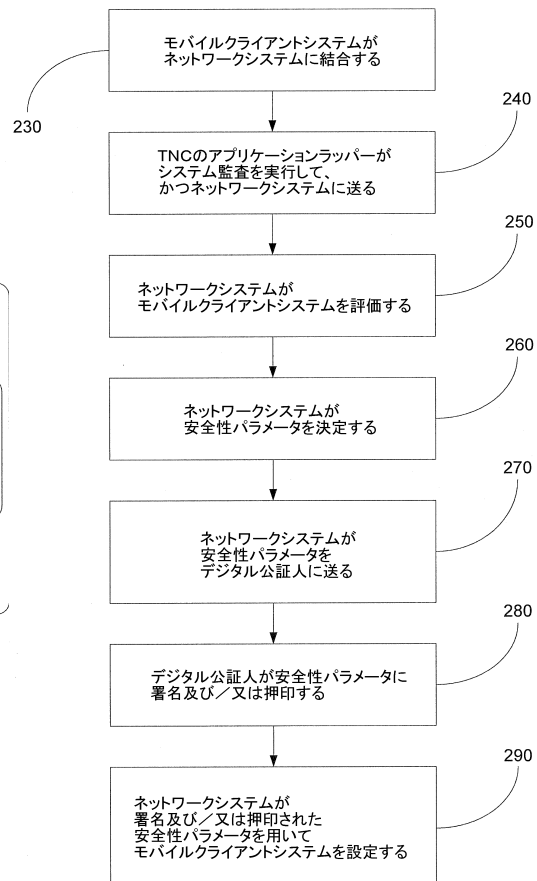
100	システム	
110	モバイルクライアントシステム	
120	ネットワークシステム	20
130	航空機システム	
140	CASのアプリケーション	
150	TNCのアプリケーションラッパー	
160	航空会社のITの企業ネットワーク	
170	デジタル公証人	
180	EPEP	
190	PEP	
200	IONTNCチャレンジャー	
210	搭載されているアプリケーション	
220	ION	30
230	ステップ	
240	ステップ	
250	ステップ	
260	ステップ	
270	ステップ	
280	ステップ	
290	ステップ	
300	ステップ	
310	ステップ	
320	クエリー	40
330	ステップ	
340	ステップ	
350	クエリー	
360	ステップ	
365	ステップ	
370	ステップ	
380	ステップ	
390	ステップ	
400	ステップ	
410	プロセッサ	50

- 420 メモリ
- 430 バス
- 440 入／出力装置又はインターフェース
- 450 通信装置又はインターフェース

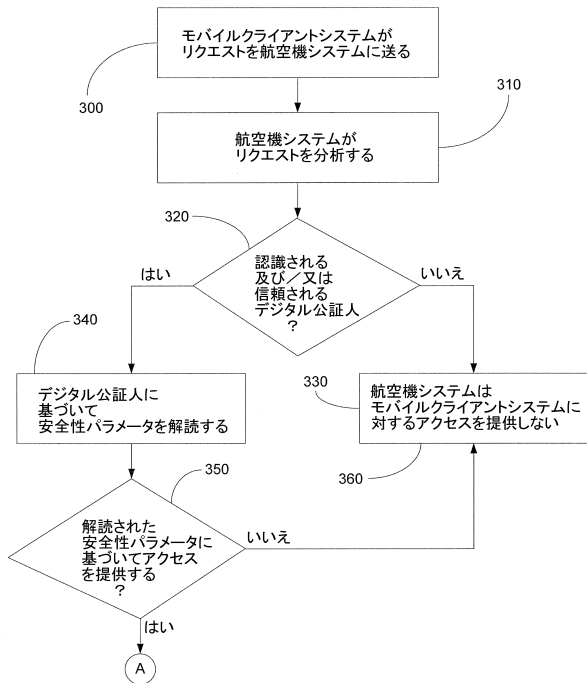
【図 1】



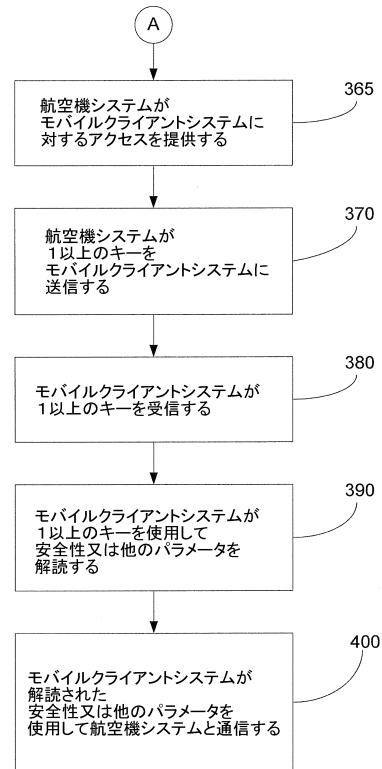
【図 2】



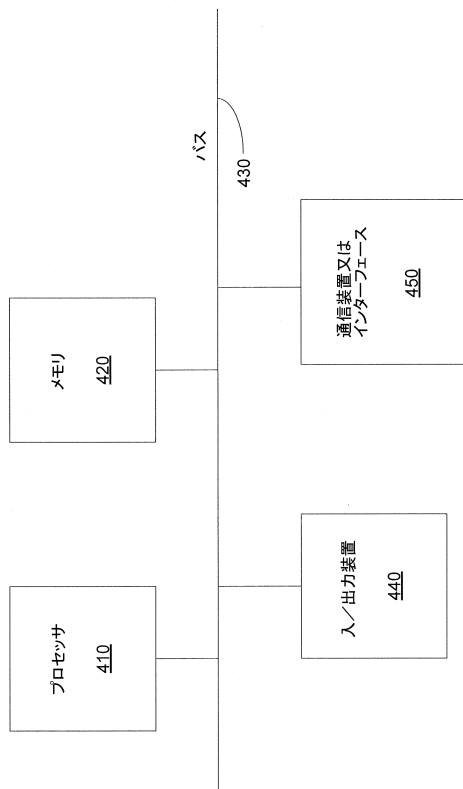
【図 3 A】



【図 3 B】



【図 4】



フロントページの続き

- (72)発明者 ブレア, リチャード エヌ.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 ヒューストン, レスター ルロイ, ザ サード
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 マーテンス, エリック ジェー.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 バッシュ, ジョン イー.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 キンバリー, グレッグ エー.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 レイン, クリスティン ケー.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100
- (72)発明者 コーマン, デーヴィッド イー.
アメリカ合衆国 イリノイ 60606-2016, シカゴ, ノース リバーサイド プラザ
100

審査官 青木 重徳

- (56)参考文献 特表2009-518762 (JP, A)
米国特許出願公開第2011/0145425 (US, A1)
特表2010-534988 (JP, A)
米国特許第08495722 (US, B1)

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32
H04W 4/029
H04W 12/08
H04W 48/16