(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6915040号
(P6915040)
(45)発行日　令和3年8月4日(2021.8.4)　(24)登録日　令和3年7月16日(2021.7.16)

(51)Int.Cl.		F I		
H04W 76/12	(2018.01)	H04W	76/12	
G06F 21/44	(2013.01)	G06F	21/44	
G06F 21/50	(2013.01)	G06F	21/50	
H04M 1/00	(2006.01)	H04M	1/00	R
H04W 12/30	(2021.01)	H04W	12/30	

請求項の数 20　(全 25 頁)　最終頁に続く

(21)出願番号　特願2019-502786(P2019-502786)
(86)(22)出願日　平成29年8月15日(2017.8.15)
(65)公表番号　特表2019-528596(P2019-528596A)
(43)公表日　令和1年10月10日(2019.10.10)
(86)国際出願番号　PCT/US2017/046911
(87)国際公開番号　WO2018/035104
(87)国際公開日　平成30年2月22日(2018.2.22)
審査請求日　平成31年3月15日(2019.3.15)
(31)優先権主張番号　201610688098.3
(32)優先日　平成28年8月18日(2016.8.18)
(33)優先権主張国・地域又は機関
中国(CN)
(31)優先権主張番号　15/676,811
(32)優先日　平成29年8月14日(2017.8.14)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110000028
特許業務法人明成国際特許事務所

最終頁に続く

(54)【発明の名称】ワイヤレスネットワークセキュリティのためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
クライアントによる安全なワイヤレスネットワーク接続のための方法であって、
モバイルデバイスで動作するクライアントによって、前記モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得することと、
前記クライアントによって、前記モバイルデバイスが前記ワイヤレスネットワークに接続する頻度に少なくとも部分的に基づいて前記ワイヤレスネットワークの前記タイプが安全でないことを決定することと、
前記ワイヤレスネットワークの前記タイプが安全でないとの決定に応じて、前記クライアントによって、前記モバイルデバイスが安全でない前記ワイヤレスネットワークに接続されている間に前記クライアントが動作する安全モードを、呼び出すことと、
前記安全モードが呼び出されたことに応じて、
前記モバイルデバイスにインストールされているアプリケーションの起動を監視することと、
前記アプリケーションが起動されるべきことを決定することと、
前記アプリケーションが起動されるべき且つ前記ワイヤレスネットワークが安全でないとの決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立することと、
を含む、方法。
【請求項２】

請求項１に記載の方法であって、
前記安全な通信チャネルは、仮想プライベートネットワーク（ＶＰＮ）接続である、方法。
【請求項３】
請求項１に記載の方法であって、さらに、
前記モバイルデバイスが安全でない前記ワイヤレスネットワークに接続されている間に前記アプリケーションがもはや起動されていないと決定することであって、
前記アプリケーションがもはや起動されていないと決定することは、
前記アプリケーションの前記監視中に、前記モバイルデバイスの現在の表示インタフェースが前記アプリケーションのインタフェースを表示していないことを検出することと、
前記現在の表示インタフェースが前記アプリケーションの前記インタフェースを表示していないとの前記検出に応じて、前記モバイルデバイスを前記安全な通信チャネルから切断し、前記ワイヤレスネットワークを介して前記第１サーバとの接続を維持することと、
を含むことと、
前記アプリケーションがもはや起動されていないとの決定に応じて、前記モバイルデバイスと前記第１サーバとの間の前記安全な通信チャネルを切断することと、
を備える、方法。
【請求項４】
請求項３に記載の方法であって、さらに、
前記アプリケーションの前記監視中に、前記クライアントが前記現在の表示インタフェースを監視していることを示すコンテンツを表示することと、
前記モバイルデバイスが前記安全な通信チャネルを切断するときは、前記コンテンツの前記表示を解除することと、
を含む、方法。
【請求項５】
請求項１に記載の方法であって、さらに、
前記アプリケーションの前記監視中に前記クライアントが前記モバイルデバイスの表示インタフェースを終了していることを検出することと、
前記クライアントが前記表示インタフェースを終了しているとの検出に応じて、前記アプリケーションが前記クライアントに監視されていることを示すコンテンツを前記表示インタフェースに表示することと、
を含む、方法。
【請求項６】
請求項１に記載の方法であって、さらに、
前記モバイルデバイスが前記ワイヤレスネットワークから切断されていることを決定することと、
前記アプリケーションが初めて監視されていることを決定することと、
前記アプリケーションが初めて監視されていることの決定に応じて、前記アプリケーションの前記監視が終了したことを示すコンテンツを現在のディスプレイに表示することと、
を含む、方法。
【請求項７】
請求項１に記載の方法であって、さらに、
前記モバイルデバイスが前記ワイヤレスネットワークから切断されていることを決定することと、
前記アプリケーションが少なくとも第２回目に監視されていることを決定することと、
前記クライアントが前記アプリケーションの１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを決定することと、

現在の表示インタフェースにおいて、前記クライアントが前記アプリケーションの前記１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを合図することと、
前記クライアントが現時点までに実行した１つ以上の安全対策を示すコンテンツを前記現在の表示インタフェースに表示することと、
を含む、方法。
【請求項８】
請求項１に記載の方法であって、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得することと、
前記ウェブサイトのＵＲＬが事前構成されたＵＲＬのリストであってフィッシングウェブサイトのＵＲＬが記録されているＵＲＬのリストと、比較することと、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのＵＲＬと一致したときは、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止することと、
を含む、方法。
【請求項９】
請求項１に記載の方法であって、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得することと、
前記ウェブサイトのＵＲＬを前記第１サーバに送信してフィッシングウェブサイトのＵＲＬの事前構成されたリストと比較し、比較結果を生成することと、
前記比較結果を前記第１サーバから受信することと、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのウェブサイトのＵＲＬと一致することを示す前記比較結果に応じて、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止することと、
を含む、方法。
【請求項１０】
ワイヤレスセキュリティシステムであって、
１つ以上のプロセッサであって、
モバイルデバイスで動作するクライアントによって、前記モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得し、
前記クライアントによって、前記モバイルデバイスが前記ワイヤレスネットワークに接続する頻度に少なくとも部分的に基づいて前記ワイヤレスネットワークの前記タイプが安全でないことを決定し、
前記ワイヤレスネットワークの前記タイプが安全でないとの決定に応じて、前記クライアントによって、前記モバイルデバイスが安全でない前記ワイヤレスネットワークに接続されている間に前記クライアントが動作する安全モードを、呼び出し、
前記安全モードが呼び出されたことに応じて、
前記モバイルデバイスにインストールされているアプリケーションの起動を監視し、
前記アプリケーションが起動されるべきことを決定し、
前記アプリケーションが起動されるべき且つ前記ワイヤレスネットワークが安全でないとの決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立するように構成された、１つ以上のプロセッサと、
前記１つ以上のプロセッサに結合され、前記１つ以上のプロセッサに命令を提供するように構成された１つ以上のメモリと、
を備える、ワイヤレスセキュリティシステム。
【請求項１１】
請求項１０に記載のシステムであって、さらに、

前記第１サーバによって転送されるメッセージを処理するように構成された第２サーバを備え、前記メッセージは、前記モバイルデバイスによって生成され、前記安全な通信チャネルを用いて前記第１サーバに送信される、システム。

【請求項１２】

請求項１０に記載のシステムであって、

前記安全な通信チャネルは、仮想プライベートネットワーク（ＶＰＮ）接続である、システム。

【請求項１３】

請求項１０に記載のシステムであって、

前記１つ以上のプロセッサは、さらに、

前記モバイルデバイスが安全でない前記ワイヤレスネットワークに接続されている間に前記アプリケーションがもはや起動されていないと決定し、

前記アプリケーションがもはや起動されていないと決定する際に、

前記アプリケーションの前記監視中に、前記モバイルデバイスの現在の表示インタフェースが前記アプリケーションのインタフェースを表示していないことを検出し、

前記現在の表示インタフェースが前記アプリケーションの前記インタフェースを表示していないとの前記検出に応じて、前記モバイルデバイスを前記安全な通信チャネルから切断し、前記ワイヤレスネットワークを介して前記第１サーバとの接続を維持し、

前記アプリケーションがもはやアクティブでないとの決定に応じて、前記モバイルデバイスと前記第１サーバとの間の前記安全な通信チャネルを切断するように構成される、システム。

【請求項１４】

請求項１３に記載のシステムであって、

前記１つ以上のプロセッサは、さらに、

前記アプリケーションの前記監視中に、前記システムが前記現在の表示インタフェースにおいて監視していることを示すコンテンツを表示し、

前記モバイルデバイスが前記安全な通信チャネルを切断したときは、前記コンテンツの前記表示を解除するように構成される、システム。

【請求項１５】

請求項１０に記載のシステムであって、

前記１つ以上のプロセッサは、さらに、

前記アプリケーションの前記監視中に、前記システムが前記モバイルデバイスの表示インタフェースを終了したことを検出し、

前記システムが前記表示インタフェースを終了したことの検出に応じて、前記アプリケーションが前記システムによって監視されていることを示すコンテンツを前記表示インタフェースに表示するように構成される、システム。

【請求項１６】

請求項１０に記載のシステムであって、

前記１つ以上のプロセッサは、さらに、

前記モバイルデバイスが前記ワイヤレスネットワークから切断されたことを決定し、

前記アプリケーションが監視されているのは初めてかどうかを決定し、

前記アプリケーションが初めて監視されているとの決定に応じて、前記アプリケーションの前記監視が終了したことを示すコンテンツを現在のディスプレイに表示し、

前記アプリケーションが監視されているのが少なくとも２回目であるとの決定に応じて、前記システムが前記アプリケーションの１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを決定し、

前記現在の表示インタフェースにおいて、前記システムが前記アプリケーションの前記１つ以上の事前構成された動作のための前記１つ以上の安全対策を実行したことを合図し、

前記現在の表示インタフェースにおいて、前記システムによって現時点までに実行さ

れた前記１つ以上の安全対策を示すコンテンツを表示するように構成される、システム。
【請求項１７】
請求項１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得し、
前記ウェブサイトのＵＲＬが事前構成されたＵＲＬのリストであってフィッシングウェブサイトのＵＲＬが記録されているＵＲＬのリストと、比較し、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのＵＲＬと一致するときは、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止するように構成される、システム。
【請求項１８】
請求項１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得し、
前記ウェブサイトのＵＲＬを前記第１サーバに送信して、事前構成されたフィッシングウェブサイトのＵＲＬのリストと比較して比較結果を生成し、
前記比較結果を前記第１サーバから受信し、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのウェブサイトのＵＲＬと一致することを示す前記比較結果に応じて、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止するように構成される、システム。
【請求項１９】
ネットワーク攻撃防御のためのコンピュータプログラムであって、
モバイルデバイスで動作するクライアントによって、前記モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得する機能と、
前記クライアントによって、前記モバイルデバイスが前記ワイヤレスネットワークに接続する頻度に少なくとも部分的に基づいて前記ワイヤレスネットワークの前記タイプが安全でないことを決定する機能と、
前記ワイヤレスネットワークの前記タイプが安全でないとの決定に応じて、前記クライアントによって、前記モバイルデバイスが安全でない前記ワイヤレスネットワークに接続されている間に前記クライアントが動作する安全モードを、呼び出す機能と、
前記安全モードが呼び出されたことに応じて、
前記モバイルデバイスにインストールされているアプリケーションの起動を監視する機能と、
前記アプリケーションが起動されるべきことを決定する機能と、
前記アプリケーションが起動されるべき且つ前記ワイヤレスネットワークが安全でないとの決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立する機能と、
を、コンピュータに実現させるためのコンピュータプログラム。
【請求項２０】
請求項１に記載の方法であって、
前記モバイルデバイスと前記第１サーバとの間の前記安全な通信チャネルの確立に応じて、前記アプリケーションに関連付けられた情報を、前記安全な通信チャネルを通じてやりとりし、
１つ以上の他のアプリケーションに関連付けられた情報を、前記安全な通信チャネルを使わない前記ワイヤレスネットワークを介してやりとりする、方法。
【発明の詳細な説明】
【技術分野】
【０００１】

［他の出願の相互参照］
本願は、全ての目的のために本明細書において参照として援用される、２０１６年８月１８日出願の「Ａ ＷＩＦＩ ＳＥＣＵＲＩＴＹ ＳＹＳＴＥＭ ＡＮＤ Ａ ＭＥＴＨＯＤ， Ａ ＭＥＡＮＳ， ＡＮＤ ＡＮ ＥＬＥＣＴＲＯＮＩＣ ＤＥＶＩＣＥ ＦＯＲ ＷＩＲＥＬＥＳＳ ＮＥＴＷＯＲＫ ＳＥＣＵＲＩＴＹ」と題された中国特許出願第２０１６１０６８８０９８．３号に対して優先権を主張する。

【０００２】
本願は、概して、ネットワークセキュリティ技術に関し、特に、ワイヤレスネットワークセキュリティのためのセキュリティシステムおよび方法に関する。

【背景技術】

【０００３】
スマートフォン、タブレット型端末、またはラップトップコンピュータなどのモバイルデバイスが公共の場（例えば、ショッピングモール、レストラン、映画館、ＫＴＶ、バー、空港、ホテル、地下鉄）で公共のワイヤレスフィデリティ（Ｗｉ－Ｆｉ）ネットワークに接続するとき、互いに知らない多数のユーザは、共用Ｗｉ－Ｆｉネットワークを通じてデータトラフィックを送信する。例えば、正規のユーザは、彼または彼女のモバイルデバイスを介して公共Ｗｉ－Ｆｉネットワークに接続し、そのモバイルデバイスで支払いを行うなどのセキュリティにかかわる取引を行う決定をする。公共Ｗｉ－Ｆｉのオープンな性質から、その支払取引は、同様に公共Ｗｉ－Ｆｉに接続している悪意のあるユーザによって傍受またはスヌープされやすく、その結果、正規ユーザのパスワード、アカウント番号などの機密情報が悪意のあるユーザに盗まれる。

【０００４】
そのため、公共Ｗｉ－Ｆｉなどの安全でないワイヤレスネットワークに対するワイヤレスネットワークセキュリティの必要性がある。

【図面の簡単な説明】

【０００５】
以下の発明を実施するための形態および付随の図面において、本発明の様々な実施形態が開示される。

【０００６】
【図１】本開示の１つ以上の実施形態による例示的な安全なワイヤレスネットワークシステムのブロック図。

【０００７】
【図２Ａ】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャート。

【０００８】
【図２Ｂ】本開示の１つ以上の実施形態による動作中の図２Ａのプロセスの例示的なシナリオのスクリーンショットを示す略図。

【０００９】
【図３Ａ】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャート。

【００１０】
【図３Ｂ】本開示の１つ以上の実施形態による動作中の図３Ａのプロセスの例示的なシナリオのスクリーンショットを示す図。

【００１１】
【図４Ａ】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャート。

【００１２】
【図４Ｂ】本開示の１つ以上の実施形態による動作中の図４Ａのプロセスの例示的なシナリオのスクリーンショットを示す図。

【００１３】

【図４Ｃ】本開示の１つ以上の実施形態による動作中の図４Ａのプロセスの別の例示的なシナリオの別のスクリーンショットを示す図。
【００１４】
【図５Ａ】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャート。
【００１５】
【図５Ｂ】本開示の１つ以上の実施形態による動作中の図５Ａのプロセスの例示的なシナリオのスクリーンショットを示す図。
【００１６】
【図５Ｃ】本開示の１つ以上の実施形態による、動作中の図５Ａのプロセスの別の例示的なシナリオの別のスクリーンショットを示す図。
【００１７】
【図６】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャート。
【００１８】
【図７】本開示の１つ以上の実施形態による安全なワイヤレスネットワーク接続のためのプログラムされたコンピュータシステムの実施形態を示す機能図。
【発明を実施するための形態】
【００１９】
本発明は、プロセス、装置、システム、組成物、コンピュータ読み取り可能な記憶媒体で具現化されるコンピュータプログラム製品、および／または、結合されたメモリに格納された命令、および／または、そのメモリによって提供された命令を実行するように構成されたプロセッサなどのプロセッサを含む、多くの方法で実行されうる。本明細書では、これらの実施形態または本発明が取りうる他の形態は、技術とみなされてよい。一般に、開示のプロセスの工程の順序は、本発明の範囲内で変更されてよい。記載されない限り、タスクを実行するように構成されると記載されたプロセッサまたはメモリなどの構成部品は、所定の時間でタスクを実行するように一時的に構成されている一般的な構成部品、または、そのタスクを実行するように製造されている特定構成部品として実装されてよい。本明細書で用いられる「プロセッサ」との用語は、１つ以上のデバイス、回路、および／または、コンピュータプログラム命令などのデータを処理するように構成された処理コアを指す。
【００２０】
本発明の１つ以上の実施形態の詳細な説明は、本発明の原理を示す付随の図と共に以下に提供される。本発明は、かかる実施形態に関連して説明されるが、本発明は、いずれの実施形態にも限定されない。本発明の範囲は、特許請求の範囲によってのみ限定され、本発明は、多くの変更、修正、および同等物を含む。本発明の十分な理解を提供するために、多くの特定の詳細が次の説明に記載される。これらの詳細は、例示の目的で提供され、本発明は、これらの特定の詳細の一部または全てなしで特許請求の範囲により実施されてよい。明確になるように、本発明に関する技術分野において周知の技術材料は、本発明が不必要に曖昧にならないように詳細には説明されていない。
【００２１】
ここでは例示的な実施形態が詳細に説明される。それらの例は、図面で提示される。次の説明が図に関しているときは、特記されない限り、異なる図の同一の番号は、同一または類似の要素を表す。以下の例示的な実施形態で説明される実施形態は、本願と一致する全ての実施形態を表すものではない。むしろ、それらは、特許請求の範囲に詳細に説明される本願のいくつかの態様と一致する手段および方法の例であるにすぎない。
【００２２】
本願で用いられる用語は、特定の実施形態を説明するのに使用されるだけであり、本願を制限する意図はない。本願および付随の特許請求の範囲で用いられる単数形の「ａ」、「ｓａｉｄ」、および「ｔｈｅ」は、文脈で明記されない限り、複数形を含むことも意図

する。また、本明細書で用いられる「および／または」との用語は、１つ以上の関連要素の可能な組み合わせのいずれかまたは全てを指し、また含むことを理解されたい。

【００２３】

本願は、様々な情報を説明するのに「第１」、「第２」、「第３」などの用語を用いるが、この情報は、これらの用語に限定されないことを理解されたい。これらの用語は、同一のカテゴリの情報を区別するのに使用されるにすぎない。例えば、本願の範囲に留まる限りにおいて、第１の情報は、第２の情報と呼ばれうる。同様に、第２の情報は、第１の情報と呼ばれうる。本明細書で用いられる「ｉｆ」との用語は、文脈に応じて「場合」または「確認されると」として解釈されてよい。

【００２４】

本明細書で用いられる「クライアント」との用語は、クライアントのユーザにサービスを提供するために、その対応するサーバと対話するプログラムを指す。

【００２５】

本明細書で用いられる「アプリ」との用語は、スマートフォン、タブレット型端末、着用式デバイスなどのモバイルデバイスにインストールされるアプリケーションを指す。

【００２６】

本明細書で用いられる「仮想プライベートネットワーク」または「ＶＰＮ」との用語は、ネットワーク上の２ポイント間の暗号化された安全な通信を提供するために、公共ネットワーク接続（例えば、有線接続または無線接続）を用いて構築されるプライベートネットワークを指す。

【００２７】

図１は、本開示の実施形態による例示的なワイヤレスネットワークセキュリティシステムのブロック図を示す。図に示されるように、システム１００は、モバイルデバイス１０２、第１サーバ１０６、および第２サーバ１０８を含む。クライアント１０４は、モバイルデバイス１０２にインストールされ、第１サーバ１０６と安全な通信チャネルを確立することができる。第２サーバ１０８は、モバイルデバイス１０２で動作する１つ以上のアプリケーション（アプリ）を提供するように構成される。第２サーバ１０８も第１サーバ１０６と通信する。かかるアプリには、例えば、モバイルデバイス１０２のユーザが操作する機密性の高いアプリが含まれる。図１では、例示の目的で１つのモバイルデバイス１０２、１つの第１サーバ１０６、および１つの第２サーバ１０８が示されるが、本開示の実施形態は、複数のモバイルデバイス、複数の第１サーバ、および複数の第２サーバなどに適用されうる。

【００２８】

モバイルデバイス１０２は、第１サーバ１０６への１つ以上の有線接続、無線接続、またはあらゆる他の適した通信接続を伴う、スマートフォン、タブレット型コンピュータ、パーソナルコンピュータ、ラップトップコンピュータ、携帯情報端末（ＰＤＡ）、着用式デバイスなどでありうる。

【００２９】

この例では、モバイルデバイス１０２は、Ｗｉ－Ｆｉ（８０２．１１）接続を通じてＩＰネットワークに直接アクセスするように構成されている。ＩＰネットワークに接続されると、モバイルデバイス１０２は、１つ以上のエンティティ（例えば、同様にＩＰネットワークと通信する第１サーバ１０６および第２サーバ１０８）と接続して通信する。例えば、モバイルデバイス１０２のユーザは、第２サーバ１０８で管理されるｅコマースサービスと接続してオンラインショッピングを行う、または、第２サーバ１０８で管理されるビデオサービスと接続してムービークリップをストリーミングすることができる。

【００３０】

ネットワーク接続性を用いて、モバイルデバイス１０２は、様々なアプリを介して、アカウント管理、支払い、または、ユーザの機密情報へのアクセス、そのアップデート、その送信を含む様々な他のタスクなど、機密性の高い動作または取引のためにエンティティと対話するように構成される。例えば、ユーザは、マーチャントとのオンライン支払いを

行って、クレジットカード情報をマーチャントと共有してよい。ユーザは、そのオンラインのクレジットカードアカウントをクレジットカード発行者と管理してよい。ユーザは、銀行口座を管理するために、そのモバイルデバイス１０２を通じて金融機関に接続してもよい。

【００３１】

ユーザ機密情報には、例えば、銀行口座へのアクセスや支払いなど安全な取引のための個人情報（誕生日、社会保障番号など）および個人口座情報（クレジットカード番号、口座番号、パスワードなど）が含まれる。かかるユーザ機密情報を利用するモバイルアプリは、本明細書では機密性の高いアプリと呼ばれる。この例では、Ａｌｉｐａｙ（商標登録）が機密性の高いアプリである。

【００３２】

モバイルデバイス１０２がワイヤレスネットワークに接続された後に、クライアント１０４は、既存のワイヤレスネットワークのネットワークタイプが安全なタイプか安全でないタイプかを決定するように構成される。クライアント１０４が既存のワイヤレスネットワークを、例えば、公共Ｗｉ－Ｆｉ、パスワードフリーＷｉ－Ｆｉ、無料Ｗｉ－Ｆｉ、モバイルデバイス１０２に不明なＷｉ－Ｆｉ、モバイルデバイス１０２が頻繁にはアクセスしないＷｉ－Ｆｉなどとして検出する場合は、クライアント１０４は、モバイルデバイス１０２が安全でないタイプのネットワークに接続していることを決定する。一方、クライアント１０４が既存のワイヤレスネットワークを、パスワード保護されたＷｉ－Ｆｉ、または、モバイルデバイス１０２が頻繁にアクセスするＷｉ－Ｆｉとして検出する場合は、クライアント１０４は、モバイルデバイス１０２が安全なタイプのネットワークに接続していることを決定する。既存のワイヤレスネットワークモバイルデバイス１０２が安全でないタイプのネットワークに接続していることを決定すると、クライアント１０４は、モバイルデバイス１０２を安全モードにする。この安全モードでは、クライアント１０４は、ユーザがモバイルデバイス１０２で機密性の高いアプリ（例えば、金融取引アプリ）を起動または立ち上げるべきかを検出するために監視する。クライアント１０４が機密性の高いアプリを起動すべきと検出した場合は、クライアント１０４は、第１サーバ１０６との安全な通信チャネルをモバイルデバイス１０２に確立させる。この例では、安全な通信チャネルはＶＰＮ接続であり、クライアント１０４は、ＶＰＮアプリケーションを立ち上げることによってモバイルデバイス１０２にＶＰＮ接続を確立させる。

【００３３】

機密性の高いアプリが起動されると、クライアント１０４は、機密性の高いアプリの動作または取引を監視して、機密性の高いアプリによって生成されたメッセージを安全な通信チャネルを用いて第１サーバ１０６に送信するように構成される。第１サーバ１０６は、機密性の高いアプリによって生成されたメッセージを安全な通信チャネルを介して受信して、そのメッセージを処理するために第２サーバ１０８に転送するように構成される。この例では、機密性の高いアプリ（例えば、Ａｌｉｐａｙ（商標登録））によって生成されたメッセージは、口座振替関連メッセージ、支払メッセージ、注文メッセージなどでありうる。

【００３４】

いくつかの実施形態では、安全モード中に、クライアント１０４は、さらに、モバイルデバイス１０２の現在の表示インタフェースが機密性の高いアプリのユーザインタフェースを表示しているかを検出するように構成される。その検出は、１つ以上の特定のユーザインタフェースコンポーネントごとにシステム表示の視認性が変化すると通知されるべきリスナを登録するなどの、オペレーティングシステムコールを呼び出すことによって実行されうる。現在の表示インタフェースが機密性の高いアプリのユーザインタフェースを表示していない場合は、クライアント１０４は、モバイルデバイス１０２を安全な通信チャネルから切断させるが、既存の安全でないワイヤレスネットワークを介して第１サーバ１０６との接続を継続させる。

【００３５】

この例では、現在のワイヤレス接続のタイプ（例えば、Ｗｉ－Ｆｉ接続）が安全でないと決定された場合は、クライアント１０４は、安全モードに入る。機密性の高いアプリ（例えば、Ａｌｉｐａｙ（商標登録））が安全モードのクライアント１０４を備えたモバイルデバイス１０２で起動される場合は、クライアント１０４は、第１サーバ１０６と安全な通信チャネル（例えば、ＶＰＮ接続）を確立する。この例では、クライアント１０４は、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）アプリであり、インストールにあたり、クライアント１０４は、安全のために提供するＡｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）のためのモバイルアプリをユーザが選択できるように構成されうる。クライアント１０４は、ユーザ設定のアプリ間通信許可によって、取引および選択されたアプリのステータスにアクセスする権限を付与されうる。この例では、クライアント１０４は、Ａｌｉｐａｙ（商標登録）の動作を監視し始め、Ａｌｉｐａｙ（商標登録）の動作によって生成されたメッセージを安全な通信チャネルを介して第１サーバ１０６に転送し始めることが確実となる。これにより、正規ユーザがＡｌｉｐａｙ（商標登録）を起動して、公共ネットワークでＡｌｉｐａｙ（商標登録）への正規ユーザのパスワードなどの機密情報を送信する場合に、悪意のあるユーザがその機密情報を盗むことを防止する。そのため、ユーザがモバイルデバイス１０２で危険なネットワーク（例えば、公共Ｗｉ－Ｆｉネットワーク）にアクセスしても、モバイルデバイス１０２での安全な取引が確保される。安全な通信チャネル（例えば、ＶＰＮ）接続は、機密性の高いアプリが起動された場合にのみ確立されるため、クライアント１０４は、長期接続を維持することによる第１サーバ１０６への過度のシステム負荷を生じさせない。さらにまた、第１サーバ１０６との間の安全な通信は削減され、システムリソースが保護される。

【００３６】

図２Ａは、本開示の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャートである。図２Ｂは、本開示の実施形態による動作中の図２Ａのプロセス２００の例示的なシナリオのスクリーンショットを示す略図である。プロセス２００は、例えば、図１のモバイルデバイス１０２のクライアント１０４によって実行されうるが、それに限定されない。

【００３７】

図に示されるように、プロセス２００は、モバイルデバイスが接続されるワイヤレスネットワークのタイプが取得される２０１において開始する。

【００３８】

この例では、モバイルデバイスは、現在Ｗｉ－Ｆｉネットワークに接続されている。Ｗｉ－Ｆｉネットワークのタイプには、例えば、無料Ｗｉ－Ｆｉネットワーク、パスワードフリーＷｉ－Ｆｉネットワーク、そのモバイルデバイスが頻繁に訪れないＷｉ－Ｆｉネットワーク、そのモバイルデバイスに不明なＷｉ－Ｆｉネットワークなどが含まれる。上記のタイプのＷｉ－Ｆｉは、安全でないタイプのＷｉ－Ｆｉ接続とみなされる。別の例では、パスワード保護されたＷｉ－Ｆｉ、または、そのモバイルデバイスのユーザが頻繁にアクセスするＷｉ－Ｆｉは、安全なタイプのＷｉ－Ｆｉとみなされる。ワイヤレスネットワークのタイプは、無制限にネットワークの様々な用途または要求に応じて構成されうる。

【００３９】

２０２では、ワイヤレスネットワークのタイプが安全でないタイプと決定された場合、安全な取引向けのアプリを監視するためにプロセス２００が開始する。この例では、このアプリケーションは、Ａｌｉｐａｙ（商標登録）の支払アプリなどの事前構成された機密性の高いアプリである。機密性の高いものに限らず、あらゆるタイプのアプリは、プロセス２００によって監視されうる、または、安全な取引のために事前構成されてプロセス２００によって監視されうる。いくつかの実施形態では、アプリの監視態様には、例えば、アプリが起動されるべきか、アプリを用いてユーザが実行する動作または取引をそのアプリが終了したか、などが含まれる。

【００４０】

２０３では、アプリがモバイルデバイスで起動されるべきことが決定される。例えば、

クライアントは、モバイルデバイスの実行中のプロセスのリストを問い合わせて、アプリがフォアグランドプロセスであるかを決定するために実行されうる。別の例では、クライアントは、アプリが開始されるときにリスナを登録するために実行されうる。さらに別の例では、アプリは、起動が開始されるとクライアントに通知するように構成されうる。

【００４１】

２０４では、仮想プライベートネットワーク（ＶＰＮ）などの安全な通信チャネルを介して、モバイルデバイスに第１サーバとの接続を確立させる。

【００４２】

この例では、ＶＰＮ接続は、モバイルデバイスおよび第１サーバを接続するために指定されたネットワークである。モバイルデバイスで事前構成されたアプリによって生成および出力されたメッセージは、ＶＰＮ接続を通じて第１サーバに送信され、第１サーバは、次にそれらのメッセージを処理のため第２サーバに転送する。

【００４３】

この例では、クライアントとは、セルラデバイスにおけるオンラインショッピングセキュリティのための公式ソフトウェアであるＡｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）である。第１サーバは、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）を提供するように構成される。モバイルデバイスは、公共の場（例えば、ショッピングモール）で提供される公共Ｗｉ－Ｆｉを介してワイヤレスローカルエリアネットワークに接続する。Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）が、現在のＷｉ－Ｆｉ接続のタイプは無料Ｗｉ－Ｆｉであるためモバイルデバイスは現在安全でないネットワークに接続されていると決定するときは、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は安全モードに入る。安全モードにある間、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、安全な取引向けに事前構成された１つ以上のアプリを監視する。ここでＡｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、Ａｌｉｐａｙ（商標登録）などの金融取引アプリがユーザによってモバイルデバイスで起動されるべきかを検出するために監視する。

【００４４】

図２Ｂに示されるように、モバイルデバイス１１は、Ａｌｉｐａｙ（商標登録）を起動させ、現在Ａｌｉｐａｙ（商標登録）のユーザインタフェースを表示している。この時点で、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、Ａｌｉｐａｙ（商標登録）が起動されて、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）が安全モードにあることをモバイルデバイス１１に表示させる決定をしている。この表示は、モバイルデバイス１１の現在の表示インタフェースにおける任意の位置（例えば、時間、セルラキャリア、ネットワーク状況、バッテリレベルなどの他の情報が通常表示されるステータスバー）に任意の適した方法で表示されうる。図に示されるように、安全モードのＡｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）および起動中のＡｌｉｐａｙ（商標登録）によって、ステータスバー１１２は、「Ａｌｉ　ｍｏｎｅｙ　ｓｈｉｅｌｄ　Ｗｉ－Ｆｉ安全モード、支払取引１件の安全確保」と表示する。ここで、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、第１サーバとの安全な通信チャネル（例えば、ＶＰＮ）をモバイルデバイス１１に確立させるため、Ａｌｉｐａｙ（商標登録）に生成されたメッセージは、安全な通信チャネルによって暗号化され、安全な通信チャネルを通じて第１サーバに送信される。モバイルデバイス１１からメッセージを受信すると、第１サーバは、メッセージを復号化し、それらを第２サーバに転送して処理する。

【００４５】

クライアントは、特定のタイプのワイヤレスネットワーク（例えば、安全でないワイヤレスネットワーク）を通じてアプリにより送信された情報の安全を確保するために、モバイルデバイスにおける安全な取引のためのアプリの態様または動作を監視するように構成されうる。安全な通信チャネルは、アプリが起動されるときのみ確立されるため、モバイルデバイスは長期接続の必要がなく、第１サーバにかかるシステム負荷はより少なくなる。このようにして、安全な通信チャネルによる第１サーバとの間のトラフィックも低減される。

【００４６】
図３Ａは、本開示の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャートである。図３Ｂは、本開示の実施形態による動作中の図３Ａのプロセス３００の例示的なシナリオのスクリーンショットを表す。プロセス３００は、例えば、図２Ａのプロセス２００が安全な通信チャネルを用いて第１サーバ１０６との接続をモバイルデバイス１０２に確立させた後に、図１のモバイルデバイス１０２のクライアント１０４によって実行されうる。
【００４７】
図に示されるように、プロセス３００は３０１で始まり、上述のアプリの監視中に、モバイルデバイスがその現在の表示インタフェースの事前構成された位置でコンテンツを表示して、クライアントが安全モードであることが示される。上記の図２Ｂに示されるように、モバイルデバイスのステータスバー１１２は、クライアントのモードおよびステータスを表示するように構成される。この例では、アプリは、監視されるように事前構成されたアプリである。
【００４８】
図３Ａに戻ると、３０２では、モバイルデバイスの現在の表示インタフェースが監視下のアプリのユーザインタフェースを示しているかどうかが検出される。現在の表示インタフェースがアプリのユーザインタフェースを表示していないときは、プロセスは３０３に進む。現在の表示インタフェースがアプリのユーザインタフェースを表示しているときは、プロセス３００は、３０１に戻り、事前構成されたアプリを監視し続ける。
【００４９】
この例では、クライアントは、オペレーティングシステムがサポートする特定の事前定義された関数呼び出しを用いてモバイルデバイスのオペレーティングシステムに問い合わせることによって（例えば、ｇｅｔＶｉｓｉｂｉｌｉｔｙ関数呼び出しなどを行うことによって）、モバイルデバイスの現在の表示インタフェースがＡｌｉｐａｙ（商標登録）のユーザインタフェースを表示しているかどうかを決定する。この例では、図３Ｂに示されるように、モバイルデバイス１１の現在の表示インタフェースは、Ａｌｉｐａｙ（商標登録）のユーザインタフェースではなくオペレーティングシステムのホーム画面を表示している。よって、Ａｌｉｐａｙ（商標登録）は、現在の表示インタフェースにもはや表示されていないと決定される。
【００５０】
３０３では、現在の表示インタフェースがアプリのユーザインタフェースを示していないときは、プロセス３００は、モバイルデバイスに安全な通信チャネル（例えば、ＶＰＮ）を切断させ、既存のワイヤレス接続（例えば、Ｗｉ－Ｆｉ接続）を介して第１サーバとの接続を維持させる。
【００５１】
この例では、Ａｌｉｐａｙ（商標登録）がモバイルデバイスの現在の表示インタフェースにもはや表示されていないときは、表示がないことでクライアントがもはや安全モードにある必要がないことを示している。あるいは、まだ安全モードにあるときは、クライアントがもはやＡｌｉｐａｙ（商標登録）のアクティビティまたは動作を監視する必要がないことを示している。よって、クライアントは、安全な通信チャネルを切断する（例えば、ＣｌｏｓｅＶＰＮ接続関数呼び出しなどを行うことによって）が、既存のＷｉ－Ｆｉ接続を介して第１サーバとの接続を維持し続ける。このようにして、ユーザは、使用されるネットワーク帯域幅の量を節約するために、既存の（無料）Ｗｉ－Ｆｉ接続を通じてビデオアプリやゲームアプリなどのセキュリティリスクの低い他のアプリに確実にアクセスできるようになる。
【００５２】
３０４では、モバイルデバイスが安全な通信チャネルを切断するときは、プロセス３００は、モバイルデバイスがその表示インタフェースに以前に表示された表示を行わないようにする。図３Ｂに示されるように、クライアント１１１（例えば、Ａｌｉ　Ｍｏｎｅｙ

Ｓｈｉｅｌｄ（商標登録））がモバイルデバイス１１に安全な通信チャネルを切断させる場合、または、モバイルデバイス１１が通信チャネルを切断した後は、ステータスバー１１２は、クライアント１１１のモードおよびステータスに関して以前表示した情報をもはや表示しない。図に示されるように、ステータスバー１１２は現在、信号ステータスバー、時間、およびバッテリレベルという一般的な情報を表示している。

【００５３】

この例では、現在の表示インタフェースが、クライアントの監視下で、事前構成されたアプリのインタフェースを示しているかどうかが決定される。現在の表示インタフェースが事前構成されたアプリのインタフェースを示していないときは、通信チャネルからモバイルデバイスを切断させる。このようにして、第１サーバの通信チャネル接続を介してクライアントによって生じたシステム負荷が低減されうる。モバイルデバイスは、もはやクライアント関連メッセージを表示せず、クライアントの現在のステータスを直ちにユーザに知らせる役割もする。

【００５４】

図４Ａは、本開示の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャートである。図４Ｂは、本開示の実施形態による動作中の図４Ａのプロセス４００の例示的なシナリオのスクリーンショットを表す。図４Ｃは、本開示の実施形態による動作中の図４Ａのプロセス４００の別の例示的なシナリオのスクリーンショットを表す。プロセス４００は、例えば、図１のモバイルデバイス１０２のクライアント１０４によって実行されうる。

【００５５】

図４Ａに示されるように、プロセス４００は４０１で開まり、クライアントがその表示インタフェースを終了した（閉じた）かどうかが決定される。クライアントがその表示インタフェースを終了したときは、プロセス４００は４０２に進む。クライアントがその表示インタフェースを終了していないときは、プロセス４００は４０１に戻り、安全モードに留まってアプリを監視し続ける。

【００５６】

４０２では、クライアントがそのインタフェースを終了したときは、対応するアイコンがモバイルデバイスの現在の表示インタフェースに表示されて、アプリが監視されていることが示される。

【００５７】

この例では、図４Ｂに示されるように、クライアント１１１が安全モードになく、その現在の表示インタフェースを終了していない（例えば、図に示されるように、代わりにホーム画面が表示されている）ときは、クライアント１１１に対応するインジケータ１１０は、モバイルデバイス１１の現在の表示インタフェースに表示される。インジケータは、アイコン、アニメーション、トースト、バブル、バルーンなどの任意の適したインタフェースコンポーネントであってよい。いくつかの実施形態では、インジケータは、ユーザインタフェースのクライアント１１１のアイコンと類似または同一の形状を有するアイコンである。この例では、インジケータ１１０は、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）のアイコンと同一のデザイン（傾いた盾）の小型版である。

【００５８】

また、この例では、図４Ｃに示されるように、クライアント１１１が安全モードにあるときであって、クライアント１１１がその現在のインタフェースを終了しているときは、対応するインジケータが表示されて、事前構成されたアプリが監視されていることが示される。同様に、インジケータは、アイコン、アニメーション、トースト、バブル、バルーンなどの任意の適したユーザインタフェースコンポーネントでありうる。この例では、図４Ｃに示されるように、インジケータ１１３はアイコンであり、事前構成されたアプリが監視されていることを示す。いくつかの実施形態では、図４Ｂのインジケータ１１０および図４Ｃのインジケータ１１３は、浮遊アイコンである。ユーザがインジケータ１１０またはインジケータ１１３をクリックして移動したことが検出されると、インジケータ１１

０またはインジケータ１１３は、ユーザが指の動きを用いることで現在の表示インタフェースの任意の位置に移動されうる。さらに、ユーザは、インジケータ１１０またはインジケータ１１３と相互作用することによって、その安全モードおよびステータスに関してクライアント１１１のステータス情報を取得することができる。例えば、ユーザは、監視されているアプリケーションについてのより詳細な情報を取得するために、インジケータ１１０またはインジケータ１１３を回転させて、「Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は安全モード」と示すテキストポップアップを２秒間表示させることができる。

【００５９】

図５Ａは、本開示の実施形態による安全なワイヤレスネットワーク接続の例示的なプロセスを示すフローチャートである。図５Ｂは、本開示の実施形態による動作中の図５Ａのプロセス５００の例示的なシナリオのスクリーンショットを表す。図５Ｃは、本開示の実施形態による動作中の図５Ａのプロセス５００の別の例示的なシナリオのスクリーンショットを表す。プロセス５００は、例えば、図１のモバイルデバイス１０２のクライアント１０４によって、図２Ａのプロセス２００と共に実行されうる。

【００６０】

図５Ａに示されるように、プロセス５００は５０１で始まり、モバイルデバイスが既存のＷｉ－Ｆｉ接続を切断したかどうかが決定される。モバイルデバイスが既存のＷｉ－Ｆｉ接続を切断した場合は、プロセス５００は５０２に進む。モバイルデバイスが既存のＷｉ－Ｆｉ接続で接続されたままのときは、プロセス５００は、図２Ａのプロセス２００を実行し続ける。

【００６１】

いくつかの実施形態では、クライアントは、電子機器のネットワークインタフェースに問い合わせることで、モバイルデバイスがＷｉ－Ｆｉネットワークに接続するかどうかを決定する。

【００６２】

５０２では、モバイルデバイスがＷｉ－Ｆｉネットワークから切断されたときは、クライアントが初めて安全モードに入ったかどうかが決定される。クライアントが初めて安全モードに入ったときは、プロセス５００は、「はい」の進路をたどって５０３に進む。クライアントが安全モードに入ったのが初めてではないときは、プロセス５００は、「いいえ」の進路をたどって５０４に進む。

【００６３】

５０３では、クライアントが初めて安全モードに入ったときは、監視プロセスが終了したことを示すのにインタフェースコンポーネントが用いられる。プロセス５００は、５０３で終了する。インタフェースコンポーネントは、任意の適したインタフェースコンポーネントであってよい。例えば、それは、トースト、ポップアップメッセージウィンドウなどであってよい。

【００６４】

図５Ｂに示されるように、５０３において、クライアントが初めて安全モードに入ったときであって、モバイルデバイス１１が既存のＷｉ－Ｆｉ接続を終了する必要があるときは、モバイルデバイスの表示インタフェースにトースト５０２が表示される。トーストは、限られた時間（例えば、数秒間）にディスプレイに現れて自動的に消えるウィンドウである。ここでトーストは、安全モードが終了したことをユーザに示す。いくつかの実施形態では、モバイルデバイス１１のオペレーティングシステムがクライアントにトーストを開く許可を与える場合は、トーストが表示される。いくつかの他の実施形態では、モバイルデバイス１１のオペレーティングシステムがクライアントにトーストを開く許可を与えない場合は、ポップアップメッセージ（例えば、ユーザが手動で閉じる必要があるウィンドウ）が表示される。

【００６５】

図５Ａに戻ると、５０４では、クライアントがアプリを監視したのが初めてでないときは、アプリの事前構成された動作のための任意のセキュリティ対策をクライアントが実行

したかどうかが決定される。実行した場合は、プロセス５００は５０５に進む。実行していない場合は、プロセス５００は５０４で終了する。

【００６６】

５０５では、アプリの事前構成された動作がクライアントによって安全性が確保されたことを示すのにインタフェースコンポーネントが用いられる。インタフェースコンポーネントは、任意の適したインタフェースコンポーネントであってよい。例えば、それは、トースト、または、ポップアップメッセージウィンドウなどであってよい。

【００６７】

５０６では、クライアントが現時点までに安全モード中に安全性を確保した動作が表示される。プロセス５００は、５０６で終了する。図５Ｃに示されるように、５０４から５０６にわたって、クライアントが安全モードに入ったのが初めてではないとき（例えば、クライアントが２回目に安全モードに入ったとき）は、モバイルデバイス１１が既存のＷｉ－Ｆｉ接続を終了する必要がある場合、Ａｌｉｐａｙ（商標登録）上における口座振替などの任意の動作がクライアントによって安全性が確保されたかどうかが決定される。例えば、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、銀行口座振替や注文などのＡｌｉｐａｙ（商標登録）の動作の取引ログまたは詳細にアクセスする権限を与えられるため、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）は、Ａｌｉｐａｙ（商標登録）のために安全性が確保された取引についての情報を安全モードで保存する。図５Ｃに示されるように、Ａｌｉ　Ｍｏｎｅｙ　Ｓｈｉｅｌｄ（商標登録）がＡｌｉｐａｙ（商標登録）による５件の口座振替を保護し、３つのフィッシングウェブサイトをブロックしたことを示すためにトースト５０４が表示される。いくつかの実施形態では、モバイルデバイス１１のオペレーティングシステムがクライアントにトーストを開く許可を与える場合は、トーストが表示される。モバイルデバイス１１のオペレーティングシステムがクライアントにトーストを開く許可を与えない場合は、ポップアップメッセージが表示される。

【００６８】

この例では、クライアントが既存のＷｉ－Ｆｉ接続を切断するときは、クライアントが以前に安全モードに入ったことがあるかどうかによって、対応する通知メッセージがユーザに表示される。かかるメッセージは、クライアントがアプリに対して提供したステータスおよび結果について知るのに役立つ。

【００６９】

図６は、本開示の実施形態による安全なワイヤレスネットワーク接続のプロセスを示すフローチャートである。プロセス６００は、例えば、図１のモバイルデバイス１０２のクライアント１０４によって実行されうる。

【００７０】

図６に示されるように、プロセス６００は６０１で始まり、安全モード中にウェブサイトのＵＲＬが取得される。

【００７１】

この例では、クライアントは、モバイルデバイスでユーザが立ち上げたブラウザからウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得する。

【００７２】

６０２では、ウェブサイトのＵＲＬは、フィッシングウェブサイトのＵＲＬを記録する事前構成されたリストに特定されたＵＲＬと比較される。

【００７３】

６０３では、ウェブサイトのＵＲＬと事前構成されたリストに含まれるウェブサイトのＵＲＬのうちの１つとの間で一致があるときは、モバイルデバイスは、ウェブサイトのＵＲＬへのアクセスをブロックされる。

【００７４】

いくつかの実施形態では、事前構成されたリストは、フィッシングウェブサイトのＵＲＬのコレクションをコンパイルして維持する第１サーバから得られる。また、第１サーバは、事前構成されたリストを定期的にまたはリアルタイムにアップデートする。第１サー

バは、さらに、クライアントがフィッシングウェブサイトをブロックするために最新の事前構成されたリストを用いることができるように、事前構成されたリストをモバイルデバイスに送信する。

【００７５】

いくつかの他の実施形態では、クライアントは、６０１で得たウェブサイトのＵＲＬを第１サーバ（例えば、図１の第１サーバ１０６）に送信する。上述の事前構成されたリストに照らしてチェックすることによって、第１サーバは、ウェブサイトのＵＲＬが事前構成されたリストに含まれるかどうかを決定する。含まれる場合は、第１サーバは、比較結果を生成し、その比較結果をモバイルデバイスに返信する。クライアントが、比較結果はウェブサイトのＵＲＬが事前構成されたリストに含まれていることを示すと決定したときは、モバイルデバイスは、ウェブサイトのＵＲＬへのアクセスをブロックされる。

【００７６】

クライアントの安全モード中にフィッシングウェブサイトがブロックされることで、モバイルデバイスにおいてＷｉ－Ｆｉ接続もフィッシングウェブサイトから自動的に保護される。これにより、モバイルデバイスのユーザがフィッシングウェブサイトの被害に遭うことを防ぐ。

【００７７】

図７は、本開示の実施形態による、安全なワイヤレスネットワーク接続のためのプログラムされたコンピュータシステムの実施形態を表す機能図である。コンピューティングシステム７００は、モバイルデバイス、第１サーバ、および第２サーバ（図１に示す）を適切に実行するのに用いられうる。明らかなように、ワイヤレスネットワークセキュリティのためのシステムおよび方法を実行するのに、他のコンピュータシステムのアーキテクチャおよび構成が用いられうる。コンピューティングシステム７００には、プロセッサ７０２、バス７０４、ネットワークインタフェース７０６、メモリ７０８、および不揮発性メモリ７１０が含まれる。プロセッサ７０２は、不揮発性メモリ７１０からメモリ７０８への対応するコンピュータプログラムを読み込んで実行する。本開示は、ソフトウェアの実装（例えば、ロジックデバイス、または、ソフトウェアおよびハードウェアの組み合わせ）に加えて、他の実装を排除しない。つまり、プロセスを実行するエンティティは、様々な論理ユニットに限定されず、ハードウェアまたはロジックデバイスであってもよい。

【００７８】

プロセッサ７０２は、モバイルデバイスにアクセスされるワイヤレスネットワークのタイプを取得するのに用いられる。モバイルデバイスは、ネットワークインタフェース７０６を用いて仮想プライベートネットワーク（ＶＰＮ）を介して第１サーバとの接続を確立するように、プロセス７０２によって制御される。

【００７９】

本明細書に開示されている発明および実際に開示されている発明を考慮すると、当業者は、本願を実施するための他の方式を容易に想到するだろう。本願の変更、使用、または適用が、本願の一般原則に従い、本願に開示されていない技術の公知の事実または慣用技術手段を含む場合は、本願は、そのあらゆる変更、使用、または適用を網羅することを意図する。記載および実施形態は、単なる例とみなされる。本願の真の範囲および精神は、以下の特許請求の範囲に示される。

【００８０】

「備える」もしくは「含む」との用語、またはそれらの変形体は、非排他的な意味で解釈されなければならない。そのため、一連の要素を備えるプロセス、方法、商品、もしくは設備は、それらの要素を備えるだけでなく、明示的には列挙されていない他の要素、または、かかるプロセス、方法、商品、もしくは設備に固有の要素も備える。さらなる限定なしで、「～を備える」との表現によって限定される要素は、プロセス、方法、商品、またはその要素を備えるデバイスにおける追加的な同一要素の存在を排除しない。

【００８１】

上述は、本願の好ましい実施形態にすぎず、本願を限定するものではない。実施される

あらゆる変更、同等の代替物、または改良物は、本願の保護範囲に含まれるものとする。

【００８２】

上述の実施形態が明確な理解のためにある程度詳細に記載されてきたが、本発明は、記載の詳細に限定されない。本願を実施する多くの代替方法がある。開示の実施形態は、例示であり限定的ではない。

例えば、以下のような形態によっても実現可能である。

［形態１］

クライアントによる安全なワイヤレスネットワーク接続のための方法であって、

モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得することと、

前記ワイヤレスネットワークの前記タイプが安全でないことを決定することと、

前記モバイルデバイスにインストールされているアプリケーションを監視することと、

前記アプリケーションが起動されるべきことを決定することと、

前記アプリケーションが起動されるべきとの前記決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立することと、

を含む、方法。

［形態２］

形態１に記載の方法であって、

前記安全な通信チャネルは、仮想プライベートネットワーク（ＶＰＮ）接続である、方法。

［形態３］

形態１に記載の方法であって、さらに、

前記アプリケーションの前記監視中に、前記モバイルデバイスの現在の表示インタフェースが前記アプリケーションのインタフェースを表示していないことを検出することと、

前記現在の表示インタフェースが前記アプリケーションの前記インタフェースを表示していないとの前記検出に応じて、前記モバイルデバイスを前記安全な通信チャネルから切断し、前記ワイヤレスネットワークを介して前記第１サーバとの接続を維持することと、

を含む、方法。

［形態４］

形態３に記載の方法であって、さらに、

前記アプリケーションの前記監視中に、前記クライアントが前記現在の表示インタフェースを監視していることを示すコンテンツを表示することと、

前記モバイルデバイスが前記安全な通信チャネルを切断するときは、前記コンテンツの前記表示を解除することと、

を含む、方法。

［形態５］

形態１に記載の方法であって、さらに、

前記アプリケーションの前記監視中に前記クライアントが前記モバイルデバイスの表示インタフェースを終了していることを検出することと、

前記クライアントが前記表示インタフェースを終了しているとの検出に応じて、前記アプリケーションが前記クライアントに監視されていることを示すコンテンツを前記表示インタフェースに表示することと、

を含む、方法。

［形態６］

形態１に記載の方法であって、さらに、

前記モバイルデバイスが前記ワイヤレスネットワークから切断されていることを決定することと、

前記アプリケーションが初めて監視されていることを決定することと、

前記アプリケーションの前記監視が終了したことを示すコンテンツを現在のディスプレイに表示することと、

を含む、方法。

［形態７］
形態１に記載の方法であって、さらに、
前記モバイルデバイスが前記ワイヤレスネットワークから切断されていることを決定することと、
前記アプリケーションが少なくとも第２回目に監視されていることを決定することと、
前記クライアントが前記アプリケーションの１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを決定することと、
現在の表示インタフェースにおいて、前記クライアントが前記アプリケーションの前記１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを合図することと、
前記クライアントが現時点までに実行した１つ以上の安全対策を示すコンテンツを前記現在の表示インタフェースに表示することと、
を含む、方法。
［形態８］
形態１に記載の方法であって、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得することと、
前記ウェブサイトのＵＲＬが事前構成されたＵＲＬのリストであってフィッシングウェブサイトのＵＲＬが記録されているＵＲＬのリストと、比較することと、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのＵＲＬと一致したときは、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止することと、
を含む、方法。
［形態９］
形態１に記載の方法であって、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得することと、
前記ウェブサイトのＵＲＬを前記第１サーバに送信してフィッシングウェブサイトのＵＲＬの事前構成されたリストと比較し、比較結果を生成することと、
前記比較結果を前記第１サーバから受信することと、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのウェブサイトのＵＲＬと一致することを示す前記比較結果に応じて、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止することと、
を含む、方法。
［形態１０］
ワイヤレスセキュリティシステムであって、
１つ以上のプロセッサであって、
モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得し、
前記ワイヤレスネットワークの前記タイプが安全でないことを決定し、
前記モバイルデバイスにインストールされているアプリケーションを監視し、
前記アプリケーションが起動されるべきことを決定し、
前記アプリケーションが起動されるべきとの前記決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立するように構成された、１つ以上のプロセッサと、
前記１つ以上のプロセッサに結合され、前記１つ以上のプロセッサに命令を提供するように構成された１つ以上のメモリと、
を備える、ワイヤレスセキュリティシステム。
［形態１１］
形態１０に記載のシステムであって、さらに、
前記第１サーバによって転送されるメッセージを処理するように構成された第２サーバ

を備え、前記メッセージは、前記モバイルデバイスによって生成され、前記安全な通信チャネルを用いて前記第１サーバに送信される、システム。
［形態１２］
形態１０に記載のシステムであって、
前記安全な通信チャネルは、仮想プライベートネットワーク（ＶＰＮ）接続である、システム。
［形態１３］
形態１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションの前記監視中に、前記モバイルデバイスの現在の表示インタフェースが前記アプリケーションのインタフェースを表示していないことを検出し、
前記現在の表示インタフェースが前記アプリケーションの前記インタフェースを表示していないとの前記検出に応じて、前記モバイルデバイスを前記安全な通信チャネルから切断し、前記ワイヤレスネットワークを介して前記第１サーバとの接続を維持するように構成される、システム。
［形態１４］
形態１３に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションの前記監視中に、前記システムが前記現在の表示インタフェースにおいて監視していることを示すコンテンツを表示し、
前記モバイルデバイスが前記安全な通信チャネルを切断したときは、前記コンテンツの前記表示を解除するように構成される、システム。
［形態１５］
形態１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションの前記監視中に、前記システムが前記モバイルデバイスの表示インタフェースを終了したことを検出し、
前記システムが前記表示インタフェースを終了したことの検出に応じて、前記アプリケーションが前記システムによって監視されていることを示すコンテンツを前記表示インタフェースに表示するように構成される、システム。
［形態１６］
形態１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記モバイルデバイスが前記ワイヤレスネットワークから切断されたことを決定し、
前記アプリケーションが監視されているのは初めてかどうかを決定し、
前記アプリケーションが初めて監視されているとの前記決定に応じて、前記アプリケーションの前記監視が終了したことを示すコンテンツを現在のディスプレイに表示し、
前記アプリケーションが監視されているのが少なくとも２回目であるとの決定に応じて、前記システムが前記アプリケーションの１つ以上の事前構成された動作のための１つ以上の安全対策を実行したことを決定し、
前記現在の表示インタフェースにおいて、前記システムが前記アプリケーションの前記１つ以上の事前構成された動作のための前記１つ以上の安全対策を実行したことを合図し、
前記現在の表示インタフェースにおいて、前記システムによって現時点までに実行された前記１つ以上の安全対策を示すコンテンツを表示するように構成される、システム。
［形態１７］
形態１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得し、

前記ウェブサイトのＵＲＬが事前構成されたＵＲＬのリストであってフィッシングウェブサイトのＵＲＬが記録されているＵＲＬのリストと、比較し、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのＵＲＬと一致するときは、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止するように構成される、システム。
［形態１８］
形態１０に記載のシステムであって、
前記１つ以上のプロセッサは、さらに、
前記アプリケーションによってアクセスされるべきウェブサイトのユニフォームリソースロケータ（ＵＲＬ）を取得し、
前記ウェブサイトのＵＲＬを前記第１サーバに送信して、事前構成されたフィッシングウェブサイトのＵＲＬのリストと比較して比較結果を生成し、
前記比較結果を前記第１サーバから受信し、
前記ウェブサイトのＵＲＬが前記事前構成されたＵＲＬのリストのウェブサイトのＵＲＬと一致することを示す前記比較結果に応じて、前記モバイルデバイスが前記ウェブサイトのＵＲＬに接続することを阻止するように構成される、システム。
［形態１９］
ネットワーク攻撃防御のためのコンピュータプログラム製品であって、前記コンピュータプログラム製品は、有形コンピュータ可読記憶媒体において実現され、
モバイルデバイスが接続されるワイヤレスネットワークのタイプを取得するためのコンピュータ命令と、
前記ワイヤレスネットワークの前記タイプが安全でないことを決定するためのコンピュータ命令と、
前記モバイルデバイスにインストールされているアプリケーションを監視するためのコンピュータ命令と、
前記アプリケーションが起動されるべきことを決定するためのコンピュータ命令と、
前記アプリケーションが起動されるべきとの前記決定に応じて、前記モバイルデバイスと第１サーバとの間に安全な通信チャネルを確立するためのコンピュータ命令と、
を備える、コンピュータプログラム製品。

【図１】

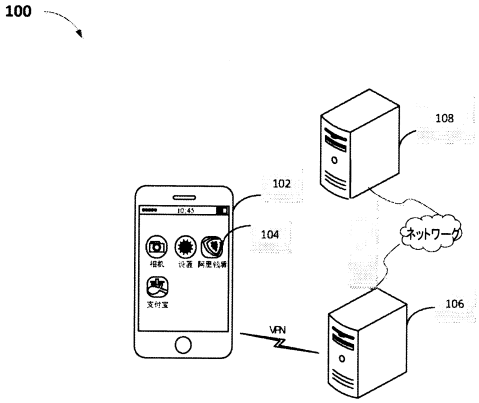

FIG. 1

【図２Ａ】

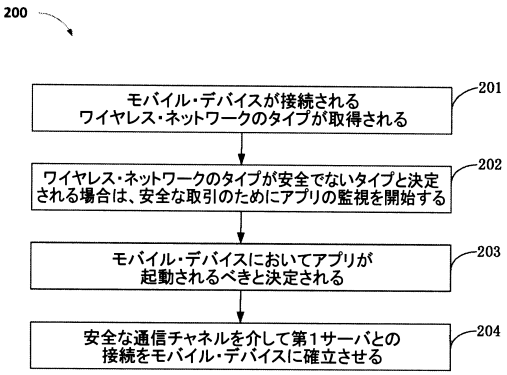

FIG. 2A

【図２Ｂ】

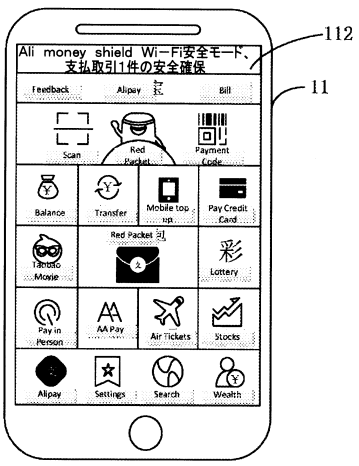

FIG. 2B

【図３Ａ】

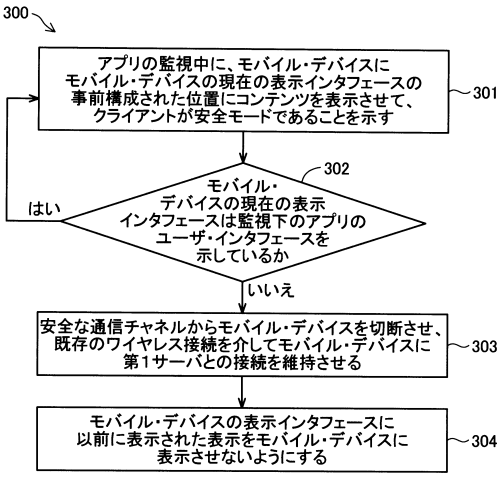

FIG.3A

【図３Ｂ】

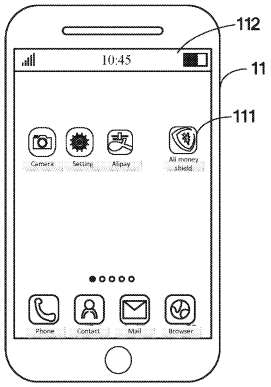

FIG. 3B

【図４Ａ】

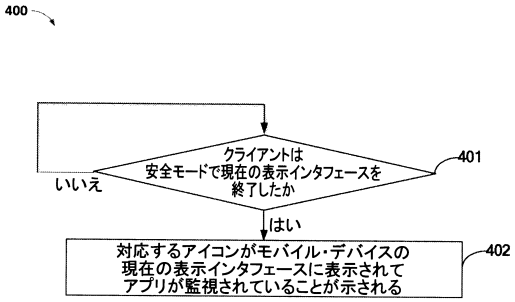

FIG. 4A

【図４Ｂ】

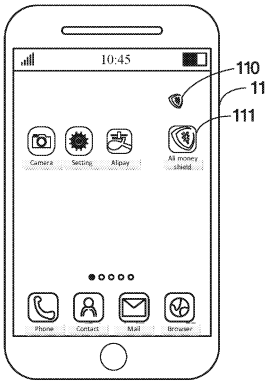

FIG. 4B

【図４Ｃ】

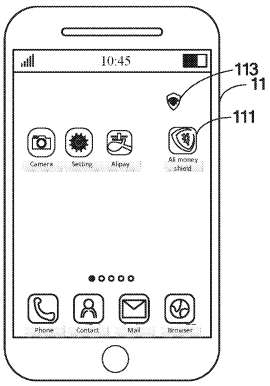

FIG. 4C

【図５Ａ】

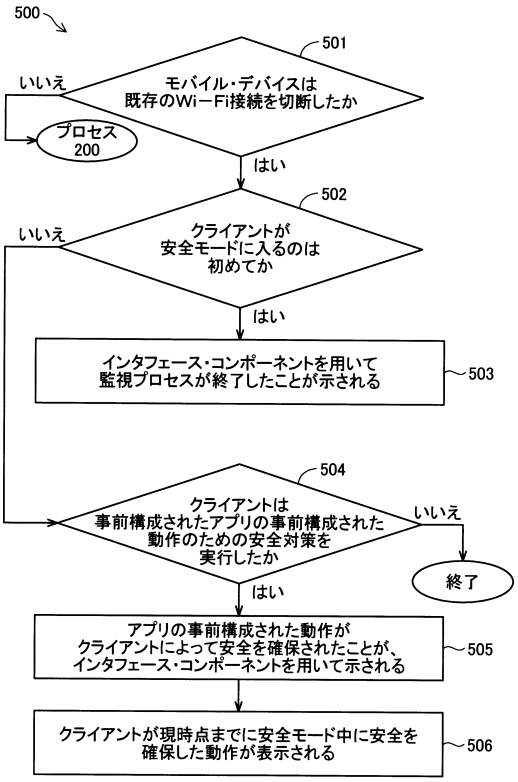

FIG.5A

【図５Ｂ】

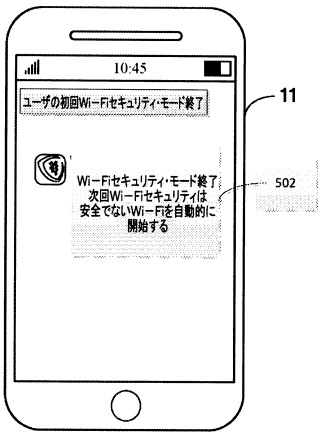

FIG. 5B

【図５Ｃ】

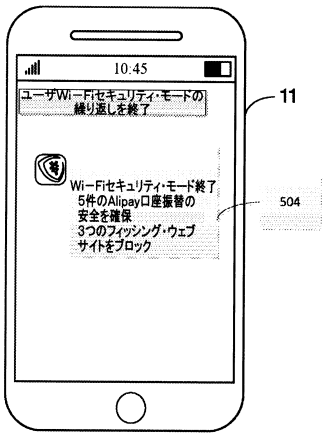

FIG. 5C

【図６】

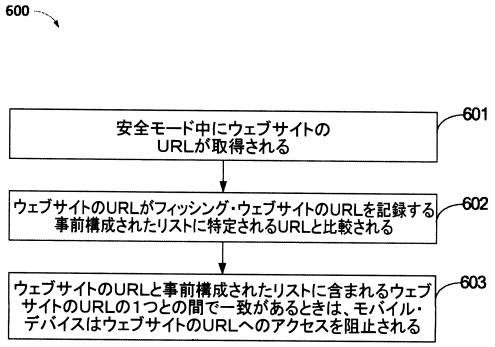

FIG. 6

【図７】

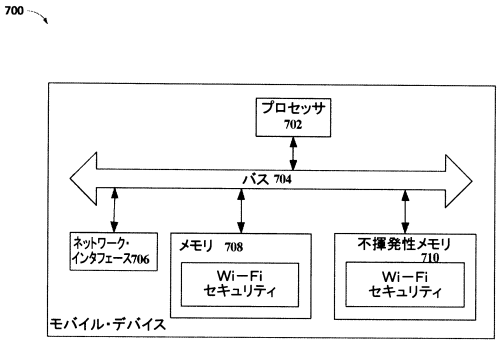
700
プロセッサ
702
バス 704
ネットワーク・
インタフェース706
メモリ 708
Wi－Fi
セキュリティ
不揮発性メモリ
710
Wi－Fi
セキュリティ
モバイル・デバイス

FIG. 7

フロントページの続き

(51)Int.Cl. F I
H04W 88/02 (2009.01) H04W 88/02 131

(72)発明者 グオ・ジョンロン
中華人民共和国 ハンチョウ, ユ・ハン・ディストリクト, ウェスト・ウェン・イー・ロード, ナンバー９６９, ビルディング 3, 5階
(72)発明者 ジャオ・レイ
中華人民共和国 ハンチョウ, ユ・ハン・ディストリクト, ウェスト・ウェン・イー・ロード, ナンバー９６９, ビルディング 3, 5階

審査官 桑江 晃

(56)参考文献 米国特許出願公開第２０１５／０１８８９４９（US, A1）
米国特許出願公開第２０１４／０３４４８８９（US, A1）
米国特許出願公開第２０１５／０３８１６５４（US, A1）
国際公開第２０１５／１０２９６０（WO, A1）

(58)調査した分野(Int.Cl., ＤＢ名)
H04W 4／00 － 99／00
G06F 21／44
G06F 21／50
3GPP TSG RAN WG1－4
SA WG1－4
CT WG1, 4