

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2019-20902

(P2019-20902A)

(43) 公開日 平成31年2月7日(2019.2.7)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/33 (2013.01)	G06F 21/33	5 J 1 0 4
H04L 9/32 (2006.01)	H04L 9/00 6 7 3 A	5 K 0 6 7
G06F 21/44 (2013.01)	G06F 21/44	
H04W 12/06 (2009.01)	H04W 12/06	
H04W 8/20 (2009.01)	H04W 8/20	

審査請求 未請求 請求項の数 7 O L (全 9 頁)

(21) 出願番号	特願2017-137094 (P2017-137094)	(71) 出願人	516290748
(22) 出願日	平成29年7月13日 (2017.7.13)		株式会社 L T E - X
			東京都品川区東品川2-2-2 天王洲郵船ビル5F
		(74) 代理人	110002000
			特許業務法人栄光特許事務所
		(72) 発明者	江副 浩
			東京都品川区東品川二丁目2番20号 株式会社 L T E - X 内
		(72) 発明者	伊藤 可久
			東京都品川区東品川二丁目2番20号 株式会社 L T E - X 内
		Fターム (参考)	5J104 AA07 AA16 EA20 KA01 KA21 NA05 NA38 PA02 5K067 AA30 BB21 EE02 HH22

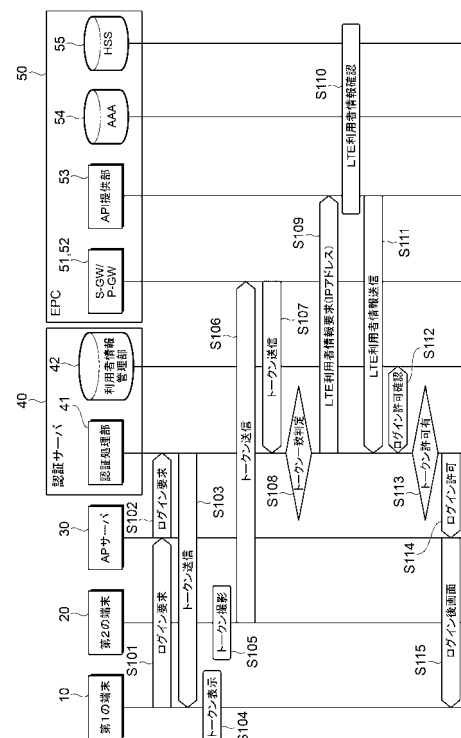
(54) 【発明の名称】 認証サーバ、認証コアシステム、認証システム及び認証方法

(57) 【要約】

【課題】 平易な操作ながらも、安全性が高く通信処理の負担を抑制し得る認証技術を提供する。

【解決手段】 認証サーバは、アプリケーションサーバへのアクセスを要求する第1の端末に第1のトークンを送信し、LTE通信が可能な第2の端末から発信され、EPCを経由して送信された第2のトークンを受信し、第1のトークンと第2のトークンが一致するか否かを判定し、第1のトークンと第2のトークンが一致する場合に、EPCから第2の端末に関するLTE通信の利用者を特定するLTE利用者情報を取得し、LTE利用者情報が、アプリケーションサーバへのアクセスを許可された利用者を特定するアプリケーション利用者情報のデータベースへのログインが許可されている情報か否かを判定し、LTE利用者情報が、アプリケーション利用者情報のデータベースへのログインが許可されている場合、アプリケーションサーバに対し、第1の端末からのアクセス要求を許可するログイン許可を送信する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

認証サーバであって、

アプリケーションサーバへのアクセスを要求する第 1 の端末に第 1 のトークンを送信し

、

L T E 通信が可能な第 2 の端末から発信され、E P C を経由して送信された第 2 のトークンを受信し、

前記第 1 のトークンと前記第 2 のトークンが一致するか否かを判定し、

前記第 1 のトークンと前記第 2 のトークンが一致する場合に、前記 E P C から前記第 2 の端末に関する L T E 通信の利用者を特定する L T E 利用者情報を取得し、

10

前記 L T E 利用者情報が、前記アプリケーションサーバへのアクセスを許可された利用者を特定するアプリケーション利用者情報のデータベースへのログインが許可されている情報か否かを判定し、

前記 L T E 利用者情報が、前記アプリケーション利用者情報のデータベースへのログインが許可されている情報である場合、前記アプリケーションサーバに対し、前記第 1 の端末からのアクセス要求を許可するログイン許可を送信する、

認証サーバ。

【請求項 2】

請求項 1 に記載の認証サーバと、前記 E P C とを含む認証コアシステム。

【請求項 3】

20

請求項 2 に記載の認証コアシステムであって、

前記認証サーバは、前記第 2 の端末の I P アドレスを前記 E P C に送信し、

前記 E P C は、前記 I P アドレスに対応した前記 L T E 利用者情報が、当該 L T E 利用者情報のデータベースに登録されているか否かを判定し、

前記 L T E 利用者情報が、前記 L T E 利用者情報のデータベースに登録されている場合、前記 E P C は、前記 I P アドレスに対応した前記 L T E 利用者情報を前記認証サーバに送信する、

認証コアシステム。

【請求項 4】

請求項 3 に記載の認証コアシステムであって、

30

前記 L T E 利用者情報のデータベースが少なくとも前記第 2 の端末の I P アドレスを保持する A A A サーバを含む、認証コアシステム。

【請求項 5】

請求項 4 に記載の認証コアシステムであって、

前記 L T E 利用者情報のデータベースが H S S を更に含む、認証コアシステム。

【請求項 6】

請求項 2 から 5 のいずれか 1 項に記載の認証コアシステムと、前記第 1 の端末と、前記第 2 の端末と、前記アプリケーションサーバと、を含み、

前記第 2 の端末は、前記第 1 の端末が表示する前記第 1 のトークンを撮影可能であって、撮影した前記第 1 のトークンに基づき、前記第 2 のトークンを前記 E P C に送信する、

40

認証システム。

【請求項 7】

認証サーバが実施する認証方法であって、

アプリケーションサーバへのアクセスを要求する第 1 の端末に第 1 のトークンを送信し

、

L T E 通信が可能な第 2 の端末から発信され、E P C を経由して送信された第 2 のトークンを受信し、

前記第 1 のトークンと前記第 2 のトークンが一致するか否かを判定し、

前記第 1 のトークンと前記第 2 のトークンが一致する場合に、前記 E P C から前記第 2 の端末に関する L T E 通信の利用者を特定する L T E 利用者情報を取得し、

50

前記 L T E 利用者情報が、前記アプリケーションサーバへのアクセスを許可された利用者を特定するアプリケーション利用者情報のデータベースへのログインが許可されている情報か否かを判定し、

前記 L T E 利用者情報が、前記アプリケーション利用者情報のデータベースへのログインが許可されている場合、前記アプリケーションサーバに対し、前記第 1 の端末からのアクセス要求を許可するログイン許可を送信する、

認証方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、認証サーバ、認証コアシステム、認証システム及び認証方法に関する。

【背景技術】

【0002】

不正なアクセス等の防止のため、セキュリティの強固な認証方法が求められている。その一方で、一般に用いられている認証方法においては、パスワードや生体認証情報等の入力が必要であり、煩雑な操作が必要になることも多い。

【0003】

特許文献 1 は、少なくとも 2 台の端末を組み合わせたプッシュ認証を採用した認証システムを開示している。これにより、セキュリティを高めつつ平易な操作による認証の実現を目指している。

【先行技術文献】

【特許文献】

【0004】

【特許文献 1】特許第 6 1 0 4 4 3 9 号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

特許文献 1 に開示された様な認証システムは、その認証の信頼性が、端末の固有の識別情報である端末 I D に依存している。このような端末 I D は偽装の防止に限界があり、偽装がされてしまうとセキュリティが低下するおそれがある。

【0006】

本発明は、平易な認証操作と高度なセキュリティを両立し得る認証技術を提供する。

【課題を解決するための手段】

【0007】

本発明の認証サーバは、アプリケーションサーバへのアクセスを要求する第 1 の端末に第 1 のトークンを送信し、L T E 通信が可能な第 2 の端末から発信され、E P C を経由して送信された第 2 のトークンを受信し、前記第 1 のトークンと前記第 2 のトークンが一致するか否かを判定し、前記第 1 のトークンと前記第 2 のトークンが一致する場合に、前記 E P C から前記第 2 の端末に関する L T E 通信の利用者を特定する L T E 利用者情報を取得し、前記 L T E 利用者情報が、前記アプリケーションサーバへのアクセスを許可された利用者を特定するアプリケーション利用者情報のデータベースへのログインが許可されている情報か否かを判定し、前記 L T E 利用者情報が、前記アプリケーション利用者情報のデータベースへのログインが許可されている情報である場合、前記アプリケーションサーバに対し、前記第 1 の端末からのアクセス要求を許可するログイン許可を送信する。

【0008】

本発明の認証サーバが実施する認証方法は、アプリケーションサーバへのアクセスを要求する第 1 の端末に第 1 のトークンを送信し、L T E 通信が可能な第 2 の端末から発信され、E P C を経由して送信された第 2 のトークンを受信し、前記第 1 のトークンと前記第 2 のトークンが一致するか否かを判定し、前記第 1 のトークンと前記第 2 のトークンが一致する場合に、前記 E P C から前記第 2 の端末に関する L T E 通信の利用者を特定する L

10

20

30

40

50

T E利用者情報を取得し、前記L T E利用者情報が、前記アプリケーションサーバへのアクセスを許可された利用者を特定するアプリケーション利用者情報のデータベースへのログインが許可されている情報か否かを判定し、前記L T E利用者情報が、前記アプリケーション利用者情報のデータベースへのログインが許可されている情報である場合、前記アプリケーションサーバに対し、前記第1の端末からのアクセス要求を許可するログイン許可を送信する。

【発明の効果】

【0009】

本発明の認証技術は、ユーザ操作の負担を抑制しつつも、より安全性を高めるとともに、通信処理の負担を抑制することが可能となる。

10

【図面の簡単な説明】

【0010】

【図1】本発明の一実施形態である認証システムの概要図。

【図2】実施形態の認証システムが実行するシーケンスを示すシーケンス図。

【発明を実施するための形態】

【0011】

以下、図面を用いて、本発明に係る通信方法の具体的な実施の形態について詳述する。特許文献1に記載された従来技術は、認証時に、例えばユーザIDやカードIDといった識別情報以外の知識認証情報、所有物認証情報、及び生体認証情報の入力が必要としない簡便な認証方法を実現することを目的としている。また、プッシュ認証が要求されると、プッシュIDを生成し、第1の端末及び第2の端末に送信し、第1の端末経由のプッシュIDと第2の端末経由のプッシュIDを照合することにより、セキュリティの強固な認証方法を実現することを目的としている。

20

【0012】

ところが、上記従来技術は、その認証の信頼性が、第2の端末4の固有の識別情報である端末IDに依存している。このような端末IDは、偽装（例えば他人の端末のMACアドレスの複製など）に対する防衛策に限界があり、ある程度の偽装の可能性が否定できないという意味から、依然として安全性に懸念が残る。

【0013】

また、第1の端末3の操作を契機とする第2の端末4へのプッシュ通知が、任意のタイミングで発生する可能性があるため、第2の端末4に対して、常時ログインの許可がなされている状態を維持するための通信が必要となる。これにより、通信シーケンス、通信コストの増加といった通信負担の増加を招くおそれがある。

30

【0014】

図1は、本発明の一実施形態の認証システム100の概要図であり、上述した様な課題の解消を実現するものである。図示した認証システム100はあくまで一実施形態であり、本発明が適用される認証システムはこのような形態に限定されるものではない。実施形態の認証システム100は、第1の端末10と、第2の端末20と、アプリケーションサーバ（APサーバ）30と、認証サーバ40と、EPC（Evolved Packet Core）50と、を含む。また、認証サーバ40とEPC50は、認証コアシステム60を構成する。尚、本明細書において、「サーバ」は、1つのサーバのみならず、複数のサーバにより構成されるものも含む。

40

【0015】

第1の端末10及び第2の端末20は、PC、スマートフォン、タブレット端末、ICカードリーダーを備える端末、携帯端末と通信可能な端末等の任意の適切な端末を用いることができる。ここで、少なくとも第2の端末20はLTE（Long Term Evolution）通信が可能であり、通信プロトコルとしてLTEプロトコルのデータ（具体的にはパケットデータ）を通信対象としたLTE通信システム下で通信を行う端末である。LTEは、3GPP（Third Generation Partnership Project）により制定された、第3世代移動体通信規格（3G）を更に高速化させたものであり、3.9Gまたは4Gと呼ばれる。

50

【0016】

また、第2の端末20は撮影機能を持つ撮影装置（カメラ）を有している。撮影装置は、第2の端末20の内部に組み込まれるものであっても、第2の端末20とは別体で、第2の端末20に接続されるものであってもよい。

【0017】

アプリケーションサーバ（APサーバ）30は、ユーザが第1の端末10を用いてアクセスを要求するアプリケーション（サイト等）を記憶するサーバであり、アプリケーションによるサービスを提供する事業者等が設置する。本実施形態による認証後に、第1の端末10は、アプリケーションサーバ30に実質的にアクセス可能となる。

【0018】

認証サーバ40は、認証の実行主体となるサーバであり、本実施形態ではアプリケーションサーバ30にログインを試みる端末がアクセスを許可されたものか否かを判定（認証）し、ひいては不正なアクセスを防止するためのものである。アプリケーションサーバ30は、上述したサービスの事業者等が設置することが多い。アプリケーションサーバ30と認証サーバ40は一体になって提供されてもよい。

【0019】

認証サーバ40は、認証処理部41と、利用者情報管理部42とを含む。認証処理部41は認証サーバ40による認証処理の主要部分を担う制御部である。利用者情報管理部42は、個々の端末固有のID（例えば端末のMACアドレスの様な物理アドレス）ではなく、認証システム100の利用者、特にアプリケーションサーバ30が提供するアプリケーションを利用するため、アプリケーションサーバ30へのアクセスが予め許可された利用者を特定する情報（アプリケーション利用者情報）を記憶し、管理する。すなわち、利用者情報管理部42は、アプリケーション利用者情報のデータベースとして機能する。ここでの利用者情報には、例えば、IMSI（International Mobile Subscriber Identity）、電話番号、他の契約者情報（認証システム用に独自に付与された独自ID等）があり、例えば通信会社が顧客毎に提供する回線ID（顧客ID）を含む。

【0020】

EPC50は、3GPPのRelease8で標準化されたコアネットワークであり、3GPPにより制定されたLTEと同時期に制定され、多様な無線アクセスを収容することができる。EPC50は、S-GW（Serving Gateway）51と、P-GW（Packet Data Network-Gateway）52と、API（Application Programming Interface）提供部53と、AAAサーバ（トリプルエーサーバ）54と、HSS（Home Subscriber Server）55と、MME（Mobility Management Entity）56とを含む。ただし、EPC50はこのような構成には限定されず、他の付随的な要素を含むことができる。

【0021】

S-GW51、P-GW52は、例えばユーザデータであるUプレーンデータの伝送を処理するEPC50（EPC Serving and PDN Gateway）を構成する。S-GW51は3GPPアクセスシステムを収容し、データを伝送するパケットゲートウェイである。P-GW52は外部ネットワーク（PDN）との接続点でIPアドレスの割り当てや、パケット転送等を行うゲートウェイである。

【0022】

MME56はS-GW51に接続され、EPC50に接続されたアクセスポイントを収容し、移動制御などを提供する論理ノードであって、位置登録、ページング、ハンドオーバー等の移動制御およびベアラ（データの伝送経路）の確立または削除を行う。

【0023】

HSS55は、LTEにおける加入者管理データベースであって、LTE通信のサービスに加入し、LTE通信を利用する利用者を特定するLTE利用者情報を登録するデータベースである。HSS55は、LTE利用者情報として、回線ID等と共に、利用者の契約情報、認証情報、位置情報等の管理をも行う。MME56は、HSS55から通知される認証情報に基づき、ユーザ認証を実施する。このようなLTE利用者情報は、一般的に

10

20

30

40

50

第2の端末20等に装着されるSIM (Subscriber Identity Module) にも記憶されLTE通信システムを利用する利用者を特定する。

【0024】

AAAサーバ54はP-GW52に接続され、認証に基づき、データベースなどのリソースに対するアクセス制御を行うものであり、RADIOUS (Remote Authentication Dial In User Service) 等が含まれる。また、AAAサーバ54は、各端末に対するIPアドレスの払い出し (付与) を行うIPアドレス払出部として機能するとともに、各端末の電話番号および／又はIMSIとIPアドレスを対応付けて記憶している。特にAAAサーバ54は、LTE通信の利用者が用いる第2の端末20のIPアドレスを少なくとも予め保持しており (例えば利用者のLTE通信サービスへの加入時に登録)、IPアドレスを保持していないHSS55とは異なる。AAAサーバ54はHSS55と同様にLTE利用者情報のデータベースとして機能する。後述するように、AAAサーバ54、HSS55を含むLTE利用者情報のデータベースに登録されたLTE利用者情報は、認証サーバ40の利用者情報管理部 (アプリケーション利用者情報のデータベース) 42に登録されたアプリケーション利用者情報と、共通する情報の形式 (種々の回線ID等) を有しており、両者は対比可能である。

10

【0025】

API提供部53は、認証サーバ40の認証処理部41と、EPC50のAAAサーバ54及びHSS55との間の情報のやり取りに関するインターフェースの役割を担う。特にAPI提供部53は、認証サーバ40から受信した第2の端末20のIPアドレスを、最初にAAAサーバ54に問い合わせる。

20

【0026】

図2は、実施形態の認証システム100が実行するシーケンスを示すシーケンス図である。まず、ユーザがPCの如き第1の端末10を利用して、アプリケーションサーバ30に対し、提供するアプリケーションのサイトにアクセスするため、ログインの要求を試みる (ステップS101)。この要求を受けたアプリケーションサーバ30は、認証サーバ40に対し、このログイン要求を通知して問い合わせる (ステップS102)。認証サーバ40の認証処理部41は、ログインのための第1のトークンを生成し、ログイン要求元の第1の端末10に対し送信する (ステップS103)。ここでのトークンは、認証サーバ40等の装置が生成する、一度の認証処理のみに利用可能なワンタイムパスワードに相当し、認証に必要な情報を意味する。

30

【0027】

第1のトークンを受信した第1の端末10は、トークンをQRコード (登録商標) 等のような、外部の撮影装置等が読み取り可能な表示形式に変換し、その表示画面に表示する (ステップS104)。ユーザは、スマートフォンの如き第2の端末20の撮影装置を用いて、表示されたQRコード等を読み取り、撮影し、第1のトークンを第2の端末20に収納する (ステップS105)。第2の端末20は、撮影した第1のトークンに基づき、実質的に同一の第2のトークンをEPC50に送信する (ステップS106)。

【0028】

EPC50のS-GW51及びP-GW52は、受信した第2のトークンを、第2の端末20のIPアドレスと共に認証サーバ40に送信する (ステップS107)。認証サーバ40の認証処理部41は、第2の端末20から発信され、EPC50を経由して (ステップS106参照) 送信された第2のトークンと、自らが生成し、第1の端末10に送信した第1のトークン (ステップS103参照) とが一致するか否かを判定する (ステップS108)。第1のトークンと第2のトークンが一致する場合、認証処理部41は、ステップS106において第2のトークンを送信した送信元の第2の端末20の利用者情報、特にLTE利用者情報を要求する問い合わせを、第2の端末20のIPアドレスと共にEPC50に送信する (ステップS109)。

40

【0029】

問い合わせを受信したEPC50のAPI提供部53は、LTE利用者情報のデータベ

50

ースであるA A Aサーバ5 4及びH S S 5 5に対し、受信した第2の端末2 0のI Pアドレスに対応するL T E利用者情報が登録されているか否かについて問い合わせる（ステップS 1 1 0）。ここでA P I提供部5 3は、認証サーバ4 0から受信したI Pアドレスを、まずはI Pアドレスを保持しているA A Aサーバ5 4に問い合わせる（H S S 5 5はI Pアドレスを保持していない）。ここで、認証サーバ4 0の利用者情報管理部4 2には、アプリケーション利用者情報として電話番号が登録されており、A A Aサーバ5 4にはI Pアドレスに対応したL T E利用者情報として、1）電話番号、または、2）I M S I、が登録されているケースを想定する。

【0030】

1）のケースにおいて、A P I提供部5 3は、I Pアドレスに基づき電話番号を取得することができる。A P I提供部5 3がこの取得した電話番号を、後述するステップS 1 1 1で認証サーバ4 0に送信することにより、認証サーバ4 0は利用者情報管理部4 2に登録された電話番号を参照してログイン許可の確認が可能となるため（後述するステップS 1 1 2）、ステップS 1 1 0はここで終了する。

【0031】

一方、2）のケースにおいて、A P I提供部5 3は、A A Aサーバ5 4への問い合わせのみでは、I M S Iを取得できても電話番号を取得することはできず、後述するステップS 1 1 2が不可能となる。

【0032】

そこで2）のケースにおいては、A A Aサーバ5 4への問い合わせから、まずA P I提供部5 3はI Pアドレスに対応するI M S Iを取得し、次に当該I M S Iから、H S S 5 5に登録されているL T E利用者情報としての電話番号を取得する。この取得した電話番号により、後に説明する様にステップS 1 1 1以降の処理が可能となる。

【0033】

尚、利用者情報管理部4 2のアプリケーション利用者情報の種別と、A A Aサーバ5 4のL T E利用者情報の種別には、それぞれ以下のようなものが挙げられる。

【0034】

- ・利用者情報管理部4 2のアプリケーション利用者情報・・・（A）電話番号、（B）I M S I、（C）他の契約者情報
- ・A A Aサーバ5 4のL T E利用者情報・・・（1）電話番号、（2）I M S I

【0035】

上記のような想定において、（A）及び（1）の組み合わせ、又は、（B）及び（2）の組み合わせが認証コアシステム6 0に存在している場合、A P I提供部5 3は、H S S 5 5を参照せずに、取得した電話番号又はI M S Iを認証サーバ4 0に送信すればよい。利用者情報管理部4 2のアプリケーション利用者情報の種別と、A A Aサーバ5 4のL T E利用者情報の種別の組み合わせは任意であり、両者に共通の種別（電話番号又はI M S I）があれば、A P I提供部5 3は、A A Aサーバ5 4のみを参照して取得した電話番号又はI M S Iを認証サーバ4 0に送信すればよい。この部分の処理は、利用者情報管理部4 2、A A Aサーバ5 4への利用者情報の登録の実装に依存し、必要に応じてA P I提供部5 3の処理方法を変更すればよい。

【0036】

上述した様に、L T E利用者情報のデータベース（A A Aサーバ5 4及びH S S 5 5）から第2の端末2 0のI Pアドレスに対応するL T E利用者情報（電話番号又はI M S I）を取得すると、A P I提供部5 3は、当該L T E利用者情報を認証サーバ4 0に送信（ステップS 1 0 9への応答）する（ステップS 1 1 1）。L T E利用者情報を受信した認証サーバ4 0の認証処理部4 1は、利用者情報管理部（アプリケーション利用者情報のデータベース）4 2に対し、L T E利用者情報を問い合わせ、少なくとも当該L T E利用者情報が、利用者情報管理部4 2へのログインを許可されている情報か否か（または利用者情報管理部4 2への登録そのもの）を確認する（ステップS 1 1 2）。利用者情報管理部4 2において、問い合わせたL T E利用者情報のログイン許可（または利用者情報管理

10

20

30

40

50

部４２における当該ＬＴＥ利用者情報の登録）が確認されたら（ステップＳ１１３）、認証処理部４１は、アプリケーションサーバ３０に対し、第１の端末１０からのアクセス要求（ログイン要求）を許可するログイン許可を送信する（ステップＳ１１４）。ログイン許可を受信したアプリケーションサーバ３０は、ログイン後の画面を表示、すなわち第１の端末１０をログイン後の画面にリダイレクトする（ステップＳ１１５）。これにより、ユーザは、第１の端末１０を用いてアプリケーションサーバ３０にアクセス可能となる。

【００３７】

本発明においては、ＥＰＣがトークンを送信する第２の端末の利用者情報（ＬＴＥ利用者情報）を管理しており、認証はこのＬＴＥ利用者情報とアプリケーション利用者情報に基づいて実行される。よって、本発明によれば、端末固有の端末ＩＤ、特に第２の端末の固有ＩＤに依存した認証処理を排除することができ、より安全に認証を行うことが可能となる。

10

【００３８】

本発明においては、認証サーバが第２の端末から送信されるトークンの受信を契機として認証を開始するため、第２の端末に対するプッシュ通知を削除することが可能となり、通信シーケンス、通信コストを削減することが可能となる。

【００３９】

よって、本発明によれば、二つの端末を通じたトークンによる認証により、ユーザ操作の負担を抑制しつつも、より安全性を高め、通信処理の負担を抑制することが可能となる。

20

【００４０】

尚、本発明は、上述した実施形態に限定されるものではなく、適宜、変形、改良、等が可能である。その他、上述した実施形態における各構成要素の材質、形状、寸法、数値、形態、数、配置箇所、等は本発明を達成できるものであれば任意であり、限定されない。

【産業上の利用可能性】

【００４１】

本発明によれば、平易な操作ながらも、安全性が高く通信処理の負担を抑制し得る認証技術が提供され得る。

【符号の説明】

【００４２】

30

- １０ 第１の端末
- ２０ 第２の端末
- ３０ アプリケーションサーバ（ＡＰサーバ）
- ４０ 認証サーバ
- ４１ 認証処理部
- ４２ 利用者情報管理部（アプリケーション利用者情報のデータベース）
- ５０ ＥＰＣ
- ５１ Ｓ－ＧＷ
- ５２ Ｐ－ＧＷ
- ５３ ＡＰＩ提供部
- ５４ ＡＡＡサーバ（ＬＴＥ利用者情報のデータベース）
- ５５ ＨＳＳ（ＬＴＥ利用者情報のデータベース）
- ５６ ＭＭＥ
- ６０ 認証コアシステム
- １００ 認証システム

40

