

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 7 月 17 日(17.07.2014)



(10) 国際公開番号
WO 2014/109409 A1

- (51) 国際特許分類:
G06F 21/45 (2013.01) *H04L 9/32* (2006.01)
G06F 21/31 (2013.01) *H04M 1/00* (2006.01)
- (21) 国際出願番号: PCT/JP2014/050384
- (22) 国際出願日: 2014 年 1 月 10 日(10.01.2014)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2013-004086 2013 年 1 月 11 日(11.01.2013) JP
- (71) 出願人: 京セラ株式会社(KYOCERA CORPORATION) [JP/JP]; 〒6128501 京都府京都市伏見区竹田鳥羽殿町 6 番地 Kyoto (JP).
- (72) 発明者: 片山 忠和(KATAYAMA, Tadakazu); 〒6128501 京都府京都市伏見区竹田鳥羽殿町 6 番地 京セラ株式会社内 Kyoto (JP).
- (74) 代理人: 正林 真之, 外(SHOBAYASHI, Masayuki et al.); 〒1000005 東京都千代田区丸の内 1-7-12 サピアタワー Tokyo (JP).

- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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, IR, 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, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

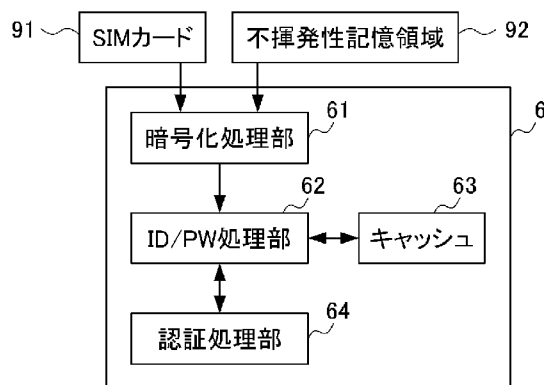
添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: COMMUNICATION TERMINAL AND STORAGE MEDIUM

(54) 発明の名称: 通信端末及び記憶媒体

[図5]



- 61 Encryption processing unit
62 ID/password processing unit
63 Cache
64 Authentication processing unit
91 SIM card
92 Non-volatile storage region

(57) Abstract: Provided are a communication terminal and a storage medium which stores a program, whereby it is possible to shorten processing time to completion of authentication, and to alleviate authentication errors. A smartphone (1) comprises: a cache (63); an encryption processing unit (61) which encrypts prescribed authentication information and generates encrypted data when power is activated; an ID/password processing unit (62) which, upon notification of the encrypted data, writes the encrypted data to the cache (63), and reads the encrypted data from the cache (63) when carrying out an authentication process upon a communication destination; and an authentication processing unit (64) which establishes a communication path with the communication destination, and carries out an authentication request to the communication destination according to a notification to the ID/password processing unit (62) of the commencement of the authentication process and on the basis of data which is acquired from the ID/password processing unit (62). The authentication processing unit (64) carries out the authentication request to the communication destination after the encrypted data is generated.

(57) 要約:

[続葉有]



認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる通信端末及びプログラムを記憶した記憶媒体を提供する。スマートフォン1は、キャッシュ63と、電源起動時に所定の認証情報を暗号化して暗号データを生成する暗号化処理部61と、暗号データが通知されると、当該暗号データをキャッシュ63に書き込み、通信先に対する認証処理を行う際に、キャッシュ63から暗号データを読み込むID/PW処理部62と、通信先への通信経路を確立すると共に、ID/PW処理部62へ認証処理の開始を通知したことに応じて、ID/PW処理部62から取得したデータに基づいて、通信先へ認証要求を行う認証処理部64と、を備え、認証処理部64は、暗号データが生成された後に、前記通信先へ認証要求を行う。

明 細 書

発明の名称： 通信端末及び記憶媒体

技術分野

[0001] 本発明は、通信先へ認証要求を行う通信端末、及び当該通信端末が備える記憶媒体に関する。

背景技術

[0002] 従来、通信端末は、起動時又は通信開始の要求に応じて、通信先との通信経路を確保した後、認証処理を開始する（例えば、特許文献1参照）。このとき、例えば、LTE（Long Term Evolution）では、認証情報である所定のID及びパスワードが暗号化されて用いられる。

先行技術文献

特許文献

[0003] 特許文献1：特開2010-034945号公報

発明の概要

発明が解決しようとする課題

[0004] このような通信端末は、起動時に認証を行う場合、処理時間を短縮するために、認証情報を暗号化してキャッシュに書き込む暗号化処理と、暗号化された情報を読み込んで認証要求を行う認証処理とを並行して実行する場合がある。このとき、暗号化処理によって暗号化された認証情報が書き込まれる前に、認証処理による読み込みが行われると、正しい認証情報が用いられず、認証処理が失敗してしまう。

[0005] 本発明は、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる通信端末及びプログラムを記憶した記憶媒体を提供することを目的とする。

課題を解決するための手段

[0006] 本発明に係る通信端末は、記憶部と、電源起動時に、所定の認証情報を暗号化して暗号データを生成する暗号化処理部と、前記暗号データが通知され

ると、当該暗号データを前記記憶部に書き込み、通信先に対する認証処理を行う際に、前記記憶部から前記暗号データを読み込む認証情報処理部と、前記通信先への通信経路を確立すると共に、前記認証情報処理部へ前記認証処理の開始を通知したことに応じて、当該認証情報処理部から取得したデータに基づいて、前記通信先へ認証要求を行う認証処理部と、を備え、前記認証処理部は、前記暗号データが前記記憶部に記憶された後に、前記通信先へ認証要求を行う。

[0007] 前記認証情報処理部は、前記記憶部に前記暗号データがない場合、前記暗号化処理部から前記暗号データが通知されるまで、前記認証処理を中断してもよい。

[0008] 前記認証処理部は、前記認証情報処理部から前記暗号データが通知された際に、前記通信先への通信経路が切断されている場合、当該通信経路を確立した後、前記通信先へ認証要求を行ってもよい。

[0009] 前記暗号化処理部は、前記暗号データを前記認証処理部へ通知し、前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記暗号化処理部から前記暗号データが通知された後、前記認証情報処理部へ前記認証処理の開始を通知してもよい。

[0010] 前記認証情報処理部は、前記暗号データを前記記憶部に書き込んだことを前記認証処理部へ通知し、前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記認証情報処理部から前記暗号データを前記記憶部に書き込んだことが通知された後、前記認証情報処理部へ前記認証処理の開始を通知してもよい。

[0011] 前記暗号化処理部は、前記暗号データを前記認証処理部へ通知し、前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記暗号化処理部から前記暗号データが通知されると、前記認証情報処理部へ前記認証処理の開始を通知することなく、当該暗号データに基づいて前記通信先へ認証要求を行ってもよい。

[0012] 本発明に係る通信端末は、前記暗号化処理部から前記暗号データが通知さ

れ、前記接続先への接続要求を受け付けたことに応じて、前記認証情報処理部に対して、前記暗号データを通知すると共に当該接続先への接続開始命令を行う接続開始命令部を備え、前記認証情報処理部は、前記接続開始命令に応じて、前記記憶部から前記暗号データを読み込んだ後、前記認証処理部に対して前記接続先への接続要求を行ってもよい。

[0013] 本発明に係る通信端末は、加入者識別情報が記録された媒体を備え、前記所定の認証情報は、前記加入者識別情報に基づくデータであってもよい。

[0014] 本発明に係る記憶媒体は、通信端末が備える記憶媒体であって、前記通信端末の電源起動時に、所定の認証情報を暗号化して暗号データを生成した後、当該暗号データを記憶する暗号化ステップと、通信先への通信経路を確立すると共に、記憶されている前記暗号データに基づいて前記通信先へ認証要求を行う認証ステップと、を前記通信端末に実行させる際に、前記認証ステップにおいて、前記暗号データが記憶された後に、前記通信先へ認証要求を行わせるためのプログラムを記憶する。

発明の効果

[0015] 本発明によれば、通信端末は、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる。

図面の簡単な説明

[0016] [図1]第1実施形態に係るスマートフォンの外観を示す斜視図である。

[図2]第1実施形態に係るスマートフォンの外観を示す正面図である。

[図3]第1実施形態に係るスマートフォンの外観を示す背面図である。

[図4]第1実施形態に係るスマートフォンの構成を示すブロック図である。

[図5]第1実施形態に係る通信ユニットの構成を示すブロック図である。

[図6]第1実施形態に係るスマートフォンの処理を示すシーケンス図である。

[図7]第2実施形態に係る通信ユニットの構成を示すブロック図である。

[図8]第2実施形態に係るスマートフォンの処理を示すシーケンス図である。

[図9]第3実施形態に係る通信ユニットの構成を示すブロック図である。

[図10]第3実施形態に係るスマートフォンの処理を示すシーケンス図である。

。

[図11]第4実施形態に係る通信ユニット及びコントローラの構成を示すブロック図である。

[図12]第4実施形態に係るスマートフォンの処理を示すシーケンス図である

。

発明を実施するための形態

[0017] [第1実施形態]

本発明を実施するための第1実施形態を、図面を参照しつつ詳細に説明する。以下では、通信端末の一例として、スマートフォンについて説明する。

[0018] 図1から図3を参照しながら、実施形態に係るスマートフォン1の外観について説明する。図1から図3に示すように、スマートフォン1は、ハウジング20を有する。ハウジング20は、フロントフェイス1Aと、バックフェイス1Bと、サイドフェイス1C1～1C4とを有する。フロントフェイス1Aは、ハウジング20の正面である。バックフェイス1Bは、ハウジング20の背面である。サイドフェイス1C1～1C4は、フロントフェイス1Aとバックフェイス1Bとを接続する側面である。以下では、サイドフェイス1C1～1C4を、どの面であるかを特定することなく、サイドフェイス1Cと総称することがある。

[0019] スマートフォン1は、タッチスクリーンディスプレイ2と、ボタン3A～3Cと、照度センサ4と、近接センサ5と、レシーバ7と、マイク8と、カメラ12とをフロントフェイス1Aに有する。スマートフォン1は、カメラ13をバックフェイス1Bに有する。スマートフォン1は、ボタン3D～3Fと、外部インタフェース14とをサイドフェイス1Cに有する。以下では、ボタン3A～3Fを、どのボタンであるかを特定することなく、ボタン3と総称することがある。

[0020] タッチスクリーンディスプレイ2は、ディスプレイ2Aと、タッチスクリーン2Bとを有する。ディスプレイ2Aは、液晶ディスプレイ(Liquid Crystal Display)、有機ELパネル(Organic

Electro-Luminescence panel)、又は無機ELパネル(Inorganic Electro-Luminescence panel)等の表示デバイスを備える。ディスプレイ2Aは、文字、画像、記号又は図形等を表示する。

[0021] タッチスクリーン2Bは、タッチスクリーンディスプレイ2に対する指、又はスタイラスペン等の接触を検出する。タッチスクリーン2Bは、複数の指、又はスタイラスペン等がタッチスクリーンディスプレイ2に接触した位置を検出することができる。

[0022] タッチスクリーン2Bの検出方式は、静電容量方式、抵抗膜方式、表面弾性波方式(又は超音波方式)、赤外線方式、電磁誘導方式、及び荷重検出方式等の任意の方式でよい。以下では、説明を簡単にするため、タッチスクリーン2Bがタッチスクリーンディスプレイ2に対する接触を検出する指、又はスタイラスペン等を単に「指」ということがある。

[0023] スマートフォン1は、タッチスクリーン2Bにより検出された接触、接触位置、接触時間又は接触回数に基づいてジェスチャの種別を判別する。ジェスチャは、タッチスクリーンディスプレイ2に対して行われる操作である。スマートフォン1によって判別されるジェスチャには、タッチ、ロングタッチ、リリース、スワイプ、タップ、ダブルタップ、ロングタップ、ドラッグ、フリック、ピンチイン、ピンチアウト等が含まれる。

[0024] タッチは、タッチスクリーンディスプレイ2(例えば、表面)に指が接触するジェスチャである。スマートフォン1は、タッチスクリーンディスプレイ2に指が接触するジェスチャをタッチとして判別する。ロングタッチとは、タッチスクリーンディスプレイ2に指が一定時間以上接触するジェスチャである。スマートフォン1は、タッチスクリーンディスプレイ2に指が一定時間以上接触するジェスチャをロングタッチとして判別する。

[0025] リリースは、指がタッチスクリーンディスプレイ2から離れるジェスチャである。スマートフォン1は、指がタッチスクリーンディスプレイ2から離れるジェスチャをリリースとして判別する。スワイプは、指がタッチスクリ

ーンディスプレイ 2 上に接触したままで移動するジェスチャである。スマートフォン 1 は、指がタッチスクリーンディスプレイ 2 上に接触したままで移動するジェスチャをスワイプとして判別する。

[0026] タップは、タッチに続いてリリースをするジェスチャである。スマートフォン 1 は、タッチに続いてリリースをするジェスチャをタップとして判別する。ダブルタップは、タッチに続いてリリースをするジェスチャが 2 回連続するジェスチャである。スマートフォン 1 は、タッチに続いてリリースをするジェスチャが 2 回連続するジェスチャをダブルタップとして判別する。

[0027] ロングタップは、ロングタッチに続いてリリースをするジェスチャである。スマートフォン 1 は、ロングタッチに続いてリリースをするジェスチャをロングタップとして判別する。ドラッグは、移動可能なオブジェクトが表示されている領域を始点としてスワイプをするジェスチャである。スマートフォン 1 は、移動可能なオブジェクトが表示されている領域を始点としてスワイプをするジェスチャをドラッグとして判別する。

[0028] フリックは、タッチに続いて指が一方方向へ高速で移動しながらリリースするジェスチャである。スマートフォン 1 は、タッチに続いて指が一方方向へ高速で移動しながらリリースするジェスチャをフリックとして判別する。フリックは、指が画面の上方向へ移動する上フリック、指が画面の下方向へ移動する下フリック、指が画面の右方向へ移動する右フリック、指が画面の左方向へ移動する左フリック等を含む。

[0029] ピンチインは、複数の指が互いに近づく方向にスワイプするジェスチャである。スマートフォン 1 は、複数の指が互いに近づく方向にスワイプするジェスチャをピンチインとして判別する。ピンチアウトは、複数の指が互いに遠ざかる方向にスワイプするジェスチャである。スマートフォン 1 は、複数の指が互いに遠ざかる方向にスワイプするジェスチャをピンチアウトとして判別する。

[0030] スマートフォン 1 は、タッチスクリーン 2 B を介して判別するこれらのジェスチャに従って動作を行う。したがって、利用者にとって直感的で使いや

すい操作性が実現される。判別されるジェスチャに従ってスマートフォン 1 が行う動作は、タッチスクリーンディスプレイ 2 に表示されている画面に応じて異なる。

[0031] 図 4 は、スマートフォン 1 の構成を示すブロック図である。スマートフォン 1 は、タッチスクリーンディスプレイ 2 と、ボタン 3 と、照度センサ 4 と、近接センサ 5 と、通信ユニット 6 と、レシーバ 7 と、マイク 8 と、ストレージ 9 と、コントローラ 10 と、カメラ 12 及び 13 と、外部インタフェース 14 と、加速度センサ 15 と、方位センサ 16 と、回転検出センサ 17 とを有する。

[0032] タッチスクリーンディスプレイ 2 は、上述したように、ディスプレイ 2 A と、タッチスクリーン 2 B とを有する。ディスプレイ 2 A は、文字、画像、記号、又は図形等を表示する。タッチスクリーン 2 B は、ジェスチャを検出する。

[0033] ボタン 3 は、利用者によって操作される。ボタン 3 は、ボタン 3 A ～ ボタン 3 F を有する。コントローラ 10 はボタン 3 と協働することによってボタンに対する操作を検出する。ボタンに対する操作は、例えば、クリック、ダブルクリック、プッシュ、及びマルチプッシュである。

[0034] 例えば、ボタン 3 A ～ 3 C は、ホームボタン、バックボタン又はメニューボタンである。例えば、ボタン 3 D は、スマートフォン 1 のパワーオン／オフボタンである。ボタン 3 D は、スリープ／スリープ解除ボタンを兼ねてもよい。例えば、ボタン 3 E 及び 3 F は、音量ボタンである。

[0035] 照度センサ 4 は、照度を検出する。例えば、照度とは、光の強さ、明るさ、輝度等である。照度センサ 4 は、例えば、ディスプレイ 2 A の輝度の調整に用いられる。

[0036] 近接センサ 5 は、近隣の物体の存在を非接触で検出する。近接センサ 5 は、例えば、タッチスクリーンディスプレイ 2 が顔に近付けられたことを検出する。

[0037] 通信ユニット 6 は、無線により通信する。通信ユニット 6 によって行われ

る通信方式は、無線通信規格である。例えば、無線通信規格として、2 G、3 G、4 G等のセルラーフォンの通信規格がある。例えば、セルラーフォンの通信規格としては、LTE (Long Term Evolution)、W-CDMA、CDMA2000、PDC、GSM (登録商標)、PHS (Personal Handy-phone System) 等がある。例えば、無線通信規格として、WiMAX (Worldwide Interoperability for Microwave Access)、IEEE802.11、Bluetooth (登録商標)、IrDA、NFC (Near Field Communication) 等がある。通信ユニット6は、上述した通信規格の1つ又は複数をサポートしていてもよい。

[0038] レシーバ7は、コントローラ10から送信される音声信号を音声として出力する。マイク8は、利用者等の音声を音声信号へ変換してコントローラ10へ送信する。なお、スマートフォン1は、レシーバ7に加えて、スピーカをさらに有してもよい。スマートフォン1は、レシーバ7に代えて、スピーカをさらに有してもよい。

[0039] ストレージ9は、プログラム及びデータを記憶する。また、ストレージ9は、コントローラ10の処理結果を一時的に記憶する作業領域としても利用される。ストレージ9は、半導体記憶デバイス、及び磁気記憶デバイス等の任意の記憶デバイスを含んでよい。また、ストレージ9は、複数の種類の記憶デバイスを含んでよい。また、ストレージ9は、メモ리카ード等の可搬の記憶媒体と、記憶媒体の読み取り装置との組み合わせを含んでよい。

[0040] ストレージ9に記憶されるプログラムには、フォアグラウンド又はバックグラウンドで実行されるアプリケーションと、アプリケーションの動作を支援する制御プログラムとが含まれる。アプリケーションは、例えば、ディスプレイ2Aに所定の画面を表示させ、タッチスクリーン2Bによって検出されるジェスチャに応じた処理をコントローラ10に実行させる。制御プログラムは、例えば、OSである。アプリケーション及び制御プログラムは、通信ユ

ニット6による無線通信又は記憶媒体を介してストレージ9にインストールされてもよい。

[0041] ストレージ9は、例えば、制御プログラム9A、メールアプリケーション9B、ブラウザアプリケーション9C、設定データ9Zを記憶する。メールアプリケーション9Bは、電子メールの作成、送信、受信、及び表示等のための電子メール機能を提供する。ブラウザアプリケーション9Cは、WEBページを表示するためのWEBブラウジング機能を提供する。テーブル9Dは、キーアサインテーブル等の各種テーブルが格納されている。配置パターンデータベース9Eは、ディスプレイ2Aに表示されるアイコン等の配置パターンが格納されている。設定データ9Zは、スマートフォン1の動作に関する各種の設定機能を提供する。

[0042] 制御プログラム9Aは、スマートフォン1を稼働させるための各種制御に関する機能を提供する。制御プログラム9Aは、例えば、通信ユニット6、レシーバ7、及びマイク8等を制御することによって、通話を実現させる。制御プログラム9Aが提供する機能には、タッチスクリーン2Bを介して検出されたジェスチャに応じて、ディスプレイ2Aに表示されている情報を変更する等の各種制御を行う機能が含まれる。なお、制御プログラム9Aが提供する機能は、メールアプリケーション9B等の他のプログラムが提供する機能と組み合わせて利用されることがある。

[0043] コントローラ10は、例えば、CPU (Central Processing Unit) である。コントローラ10は、通信ユニット6等の他の構成要素が統合されたSoC (System-on-a-chip) 等の集積回路であってもよい。コントローラ10は、スマートフォン1の動作を統括的に制御して各種の機能を実現する。

[0044] 具体的には、コントローラ10は、ストレージ9に記憶されているデータを必要に応じて参照しつつ、ストレージ9に記憶されているプログラムに含まれる命令を実行して、ディスプレイ2A及び通信ユニット6等を制御することによって各種機能を実現する。コントローラ10は、タッチスクリーン

2 B、ボタン 3、加速度センサ 1 5 等の各種検出部の検出結果に応じて、制御を変更することもある。

[0045] コントローラ 1 0 は、例えば、制御プログラム 9 A を実行することにより、タッチスクリーン 2 B を介して検出されたジェスチャに応じて、ディスプレイ 2 A に表示されている情報を変更する等の各種制御を実行する。

[0046] カメラ 1 2 は、フロントフェース 1 A に面している物体を撮影するインカメラである。カメラ 1 3 は、バックフェース 1 B に面している物体を撮影するアウトカメラである。

[0047] 外部インタフェース 1 4 は、他の装置が接続される端子である。外部インタフェース 1 4 は、USB (Universal Serial Bus)、HDMI (High-Definition Multimedia Interface) (登録商標)、ライトピーク (サンダーボルト)、イヤホンマイクコネクタのような汎用的な端子であってもよい。外部インタフェース 1 4 は、Dock コネクタのような専用に設計された端子でもよい。外部インタフェース 1 4 に接続される装置には、例えば、外部ストレージ、スピーカ、通信装置が含まれる。

[0048] 加速度センサ 1 5 は、スマートフォン 1 に働く加速度の方向及び大きさを検出する。方位センサ 1 6 は、地磁気の向きを検出する。回転検出センサ 1 7 は、スマートフォン 1 の回転を検出する。加速度センサ 1 5、方位センサ 1 6 及び回転検出センサ 1 7 の検出結果は、スマートフォン 1 の位置及び姿勢の変化を検出するために、組み合わせて利用される。

[0049] このように構成されるスマートフォン 1 は、通信ユニット 6 により、接続先との間で認証処理を行った後、所定の通信方式で通信を行う。以下、所定の通信方式は LTE であるとして説明する。

[0050] 図 5 は、本実施形態に係る通信ユニット 6 の構成を示すブロック図である。

通信ユニット 6 は、暗号化処理部 6 1 と、ID/PW 処理部 6 2 (認証情報処理部) と、キャッシュ 6 3 (記憶部) と、認証処理部 6 4 とを備える。

[0051] 暗号化処理部61は、スマートフォン1の電源起動時に、スマートフォン1又はユーザに固有の所定の認証情報を暗号化して暗号データを生成する。

なお、所定の認証情報は、加入者識別情報を記録するための媒体であるSIM (Subscriber Identity Module) カード91に格納されているMSN (Mobile Subscriber Number)、IMSI (International Mobile Subscriber Identity) 若しくはICCID (IC Card ID)、又はスマートフォン1の内部の不揮発性記憶領域92に格納されているIMEI (International Mobile Equipment Identity) 等のいずれかを使用して生成されるID及びパスワード(PW)である。

[0052] ID/PW処理部62は、暗号化処理部61により生成された暗号データが通知されると、この暗号データをキャッシュ63に書き込む。そして、ID/PW処理部62は、通信先に対する認証処理を行う際に、キャッシュ63から暗号データを読み込み、認証処理部64へ提供する。

[0053] 認証処理部64は、通信先である基地局への通信経路を確立すると共に、ID/PW処理部62へ認証処理の開始を通知したことに応じて、ID/PW処理部62から取得した暗号データに基づいて、基地局へ認証要求を行う。

このとき、認証処理部64は、暗号データが暗号化処理部61により生成された後に、基地局へ認証要求を行う。

[0054] 具体的には、ID/PW処理部62は、キャッシュ63に暗号データがない場合、暗号化処理部61から暗号データが通知されるまで、認証処理を中断する。

また、認証処理部64は、ID/PW処理部62から暗号データが通知された際に、タイムアウトによって基地局への通信経路が切断されている場合、再度通信経路を確立した後、基地局へ認証要求を行う。

[0055] 図6は、本実施形態に係るスマートフォン1が電源起動時に実行する処理

を示すシーケンス図である。

- [0056] ステップS 1において、暗号化処理部6 1は、S I Mカードの情報を読み込んで、認証情報（I D／P W）を生成する。
- [0057] ステップS 2において、認証処理部6 4は、通信可能な基地局を捕捉すると、信号同期を行って通信経路を確保する。
- [0058] ステップS 3において、暗号化処理部6 1は、ステップS 1で生成されたI D／P Wの暗号化処理を開始する。
- [0059] ステップS 4において、認証処理部6 4は、I D／P W処理部6 2へ認証開始を命令する。
- [0060] ステップS 5において、I D／P W処理部6 2は、キャッシュ6 3から暗号化されたI D／P Wを取得する。
- [0061] ステップS 6において、I D／P W処理部6 2は、ステップS 5で暗号化されたI D／P Wを取得できたか否かを判定する。この時点で暗号化処理部6 1による暗号化処理は終了していないため、判定はN Oとなり、処理はステップS 7に移る。
- [0062] ステップS 7において、I D／P W処理部6 2は、認証開始命令の発生を示すフラグをT R U Eにセットする。
- [0063] ステップS 8において、I D／P W処理部6 2は、認証処理を中止し、暗号データの生成を待機する。
- [0064] ステップS 9において、暗号化処理部6 1は、ステップS 3で開始されたI D／P Wの暗号化処理を完了する。
- [0065] ステップS 1 0において、暗号化処理部6 1は、暗号化されたI D／P Wを、I D／P W処理部6 2へ通知する。
- [0066] ステップS 1 1において、I D／P W処理部6 2は、ステップS 1 0で通知された暗号化されたI D／P Wを、キャッシュ6 3へ書き込む。
- [0067] ステップS 1 2において、I D／P W処理部6 2は、認証開始命令の発生を示すフラグがT R U Eか否かを判定する。ステップS 7においてフラグはT R U Eにセットされているため、判定はY E Sとなり、処理はステップS

13に移る。

[0068] ステップS13において、ID/PW処理部62は、認証開始命令の発生を示すフラグをFALSEにセットして初期化する。

[0069] ステップS14において、ID/PW処理部62は、キャッシュ63から暗号化されたID/PWを取得する。

[0070] ステップS15において、ID/PW処理部62は、ステップS5で暗号化されたID/PWを取得できたか否かを判定する。この時点で暗号化処理部61による暗号化処理は終了しているため、判定はYESとなり、処理はステップS16に移る。

[0071] ステップS16において、ID/PW処理部62は、暗号化されたID/PWを認証処理部64へ通知して認証要求を行う。これに応じて、認証処理部64は、基地局との間で認証処理を行い、スマートフォン1は、待ち受け状態へ移行する。

[0072] なお、ステップS5～S8と、ステップS14～S15とは、共通の処理ルーチンAとして実現される。

[0073] 本実施形態によれば、スマートフォン1は、暗号化処理と認証処理とを並行して実行しつつも、暗号データを確実に取得できるので、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる。

また、本実施形態は、既存の通信ユニット6の暗号化処理部61、キャッシュ63及び認証処理部64を変更することなく、ID/PW処理部62のソフトウェア変更によって実現されるため、改修が容易である。

[0074] [第2実施形態]

本発明を実施するための第2実施形態を、図面を参照しつつ詳細に説明する。なお、第1実施形態と同様の構成については同一の符号を付し、説明を省略又は簡略化する。

[0075] 図7は、本実施形態に係る通信ユニット6aの構成を示すブロック図である。

暗号化処理部61aは、ID/PWを暗号化した暗号データを認証処理部

64 aへ通知する。

認証処理部64 aは、スマートフォン1の電源起動時に認証処理の実行を待機し、暗号化処理部61 aから暗号データが通知された後、ID/PW処理部62 aへ認証処理の開始を通知する。

[0076] 図8は、本実施形態に係るスマートフォン1が電源起動時に実行する処理を示すシーケンス図である。

[0077] ステップS21において、暗号化処理部61 aは、SIMカードの情報を読み込んで、認証情報(ID/PW)を生成する。

[0078] ステップS22において、認証処理部64 aは、通信可能な基地局を捕捉すると、信号同期を行って通信経路を確保する。

[0079] ステップS23において、認証処理部64 aは、認証開始命令の発生を示すフラグをTRUEにセットする。

[0080] ステップS24において、認証処理部64 aは、認証処理を中断し、暗号化処理部61 aから通知があるまで、認証処理の継続を待機する。

[0081] ステップS25において、暗号化処理部61 aは、ステップS21で生成されたID/PWの暗号化処理を開始する。

[0082] ステップS26において、暗号化処理部61 aは、ステップS25で開始されたID/PWの暗号化処理を完了する。

[0083] ステップS27において、暗号化処理部61 aは、暗号化されたID/PWを、認証処理部64 aへ通知する。

[0084] ステップS28において、認証処理部64 aは、認証開始命令の発生を示すフラグがTRUEか否かを判定する。ステップS23においてフラグはTRUEにセットされているため、判定はYESとなり、処理はステップS29に移る。

[0085] ステップS29において、認証処理部64 aは、認証開始命令の発生を示すフラグをFALSEにセットして初期化する。

[0086] ステップS30において、認証処理部64 aは、ステップS24で中断した認証処理を再開する。

- [0087] ステップS 3 1において、認証処理部6 4 aは、ステップS 2 7で取得した暗号化されたID/PWをID/PW処理部6 2 aへ通知すると共に、認証開始を命令する。
- [0088] ステップS 3 2において、ID/PW処理部6 2 aは、ステップS 3 1で通知された暗号化されたID/PWを、キャッシュ6 3へ書き込む。
- [0089] ステップS 3 3において、ID/PW処理部6 2 aは、キャッシュ6 3から暗号化されたID/PWを取得する。
- [0090] ステップS 3 4において、ID/PW処理部6 2 aは、ステップS 3 3で暗号化されたID/PWを取得できたか否かを判定する。この時点で暗号化処理部6 1 aによる暗号化処理は終了しているため、判定はYESとなり、処理はステップS 3 5に移る。
- [0091] ステップS 3 5において、ID/PW処理部6 2 aは、暗号化されたID/PWを認証処理部6 4 aへ通知して認証要求を行う。これに応じて、認証処理部6 4 aは、基地局との間で認証処理を行い、スマートフォン1は、待ち受け状態へ移行する。
- [0092] なお、ステップS 3 3～S 3 4は、第1実施形態と共通の処理ルーチンAとして実現される。
- [0093] 本実施形態によれば、スマートフォン1は、暗号化処理と認証処理とを並行して実行しつつも、暗号データを確実に取得できるので、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる。

また、認証処理部6 4 aは、暗号化処理部6 1 aから直接に暗号データを通知されるので、暗号化処理の完了後、即座に認証処理を再開できる。これにより、基地局への接続がタイムアウトとなるのを抑制できる。

[0094] [第3実施形態]

本発明を実施するための第3実施形態を、図面を参照しつつ詳細に説明する。なお、第1実施形態と同様の構成については同一の符号を付し、説明を省略又は簡略化する。

- [0095] 図9は、本実施形態に係る通信ユニット6 bの構成を示すブロック図であ

る。

I D / P W 処理部 6 2 b は、暗号データをキャッシュ 6 3 に書き込んだことを認証処理部 6 4 b へ通知する。

認証処理部 6 4 b は、スマートフォン 1 の電源起動時に認証処理の実行を待機し、I D / P W 処理部 6 2 b から暗号データをキャッシュ 6 3 に書き込んだことが通知された後、I D / P W 処理部 6 2 b へ認証処理の開始を通知する。

[0096] 図 1 0 は、本実施形態に係るスマートフォン 1 が電源起動時に実行する処理を示すシーケンス図である。

[0097] ステップ S 4 1 において、暗号化処理部 6 1 b は、S I M カードの情報を読み込んで、認証情報 (I D / P W) を生成する。

[0098] ステップ S 4 2 において、認証処理部 6 4 b は、通信可能な基地局を捕捉すると、信号同期を行って通信経路を確保する。

[0099] ステップ S 4 3 において、認証処理部 6 4 b は、認証開始命令の発生を示すフラグを T R U E にセットする。

[0100] ステップ S 4 4 において、認証処理部 6 4 b は、認証処理を中断し、I D / P W 処理部 6 2 b から通知があるまで、認証処理の継続を待機する。

[0101] ステップ S 4 5 において、暗号化処理部 6 1 b は、ステップ S 4 1 で生成された I D / P W の暗号化処理を開始する。

[0102] ステップ S 4 6 において、暗号化処理部 6 1 b は、ステップ S 4 5 で開始された I D / P W の暗号化処理を完了する。

[0103] ステップ S 4 7 において、暗号化処理部 6 1 b は、暗号化された I D / P W を、I D / P W 処理部 6 2 b へ通知する。

[0104] ステップ S 4 8 において、I D / P W 処理部 6 2 b は、ステップ S 4 7 で通知された暗号化された I D / P W を、キャッシュ 6 3 へ書き込む。

[0105] ステップ S 4 9 において、I D / P W 処理部 6 2 b は、暗号化処理が完了し暗号化された I D / P W をキャッシュ 6 3 に書き込んだことを、認証処理部 6 4 b へ通知する。

- [0106] ステップS 5 0において、認証処理部6 4 bは、認証開始命令の発生を示すフラグがT R U Eか否かを判定する。ステップS 4 3においてフラグはT R U Eにセットされているため、判定はY E Sとなり、処理はステップS 5 1に移る。
- [0107] ステップS 5 1において、認証処理部6 4 bは、認証開始命令の発生を示すフラグをF A L S Eにセットして初期化する。
- [0108] ステップS 5 2において、認証処理部6 4 bは、ステップS 4 4で中断した認証処理を再開する。
- [0109] ステップS 5 3において、認証処理部6 4 bは、I D / P W処理部6 2 bへ認証開始を命令する。
- [0110] ステップS 5 4において、I D / P W処理部6 2 bは、キャッシュ6 3から暗号化されたI D / P Wを取得する。
- [0111] ステップS 5 5において、I D / P W処理部6 2 bは、ステップS 5 4で暗号化されたI D / P Wを取得できたか否かを判定する。この時点で暗号化処理部6 1 bによる暗号化処理は終了しているため、判定はY E Sとなり、処理はステップS 5 6に移る。
- [0112] ステップS 5 6において、I D / P W処理部6 2 bは、暗号化されたI D / P Wを認証処理部6 4 bへ通知して認証要求を行う。これに応じて、認証処理部6 4 bは、基地局との間で認証処理を行い、スマートフォン1は、待ち受け状態へ移行する。
- [0113] なお、ステップS 5 4～S 5 5は、第1実施形態と共通の処理ルーチンAとして実現される。
- [0114] 本実施形態によれば、スマートフォン1は、暗号化処理と認証処理とを並行して実行しつつも、暗号データを確実に取得できるので、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる。
- また、暗号データの書き込み及び読み込みに係る一連の処理が既存の処理ルーチンと共通にできる。
- [0115] [第4実施形態]

本発明を実施するための第4実施形態を、図面を参照しつつ詳細に説明する。なお、第1実施形態と同様の構成については同一の符号を付し、説明を省略又は簡略化する。

[0116] 図11は、本実施形態に係る通信ユニット6c及びコントローラ10の構成を示すブロック図である。

コントローラ10は、接続開始命令部101を備える。接続開始命令部101は、暗号化処理部61cから暗号データが通知される。また、接続開始命令部101は、ユーザの操作入力等により基地局への接続要求を受け付けたことに応じて、ID/PW処理部62cに対して、暗号データを通知すると共に基地局への接続開始命令を行う。

ID/PW処理部62cは、接続開始命令に応じて、キャッシュ63から暗号データを読み込んだ後、認証処理部64cに対して基地局への接続の要求を行う。

[0117] 図12は、本実施形態に係るスマートフォン1が電源起動時に実行する処理を示すシーケンス図である。

[0118] ステップS61において、暗号化処理部61cは、SIMカードの情報を読み込んで、認証情報(ID/PW)を生成する。

[0119] ステップS62において、認証処理部64cは、通信可能な基地局を捕捉すると、信号同期を行って通信経路を確保する。

[0120] ステップS63において、暗号化処理部61cは、ステップS61で生成されたID/PWの暗号化処理を開始する。

[0121] ステップS64において、認証処理部64cは、ID/PW処理部62cへ認証開始を命令する。

[0122] ステップS65において、ID/PW処理部62cは、キャッシュ63から暗号化されたID/PWを取得する。

[0123] ステップS66において、ID/PW処理部62cは、ステップS65で暗号化されたID/PWを取得できたか否かを判定する。この時点で暗号化処理部61cによる暗号化処理は終了していないため、判定はNOとなり、

処理はステップS 6 7に移る。

- [0124] ステップS 6 7において、ID/PW処理部6 2 cは、認証開始命令の発生を示すフラグをTRUEにセットする。
- [0125] ステップS 6 8において、ID/PW処理部6 2 cは、認証処理を中止し、暗号データの生成を待機する。
- [0126] ステップS 6 9において、認証処理部6 4 cは、ID/PW処理部6 2 cから認証処理中止の通知を受けると、基地局に対して通信経路の切断を要求する。あるいは、認証処理部6 4 cは、明示的な切断要求を行うことなく、タイムアウトによって通信経路を切断してもよい。
- [0127] ステップS 7 0において、暗号化処理部6 1 cは、ステップS 6 3で開始されたID/PWの暗号化処理を完了する。
- [0128] ステップS 7 1において、暗号化処理部6 1 cは、暗号化されたID/PWを、接続開始命令部1 0 1へ通知する。
- [0129] ステップS 7 2において、接続開始命令部1 0 1は、ユーザ又はアプリケーションからの通信要求に応じて、ステップS 7 1で取得した暗号化されたID/PWをID/PW処理部6 2 cへ通知し、接続開始を命令する。
- [0130] ステップS 7 3において、ID/PW処理部6 2 cは、ステップS 7 2で通知された暗号化されたID/PWを、キャッシュ6 3へ書き込む。
- [0131] ステップS 7 4において、ID/PW処理部6 2 cは、認証開始命令の発生を示すフラグがTRUEか否かを判定する。ステップS 6 7においてフラグはTRUEにセットされているため、判定はYESとなり、処理はステップS 7 5に移る。
- [0132] ステップS 7 5において、ID/PW処理部6 2 cは、認証開始命令の発生を示すフラグをFALSEにセットして初期化する。
- [0133] ステップS 7 6において、ID/PW処理部6 2 cは、キャッシュ6 3から暗号化されたID/PWを取得する。
- [0134] ステップS 7 7において、ID/PW処理部6 2 cは、ステップS 7 6で暗号化されたID/PWを取得できたか否かを判定する。この時点で暗号化

処理部 6 1 c による暗号化処理は終了しているため、判定は Y E S となり、処理はステップ S 7 8 に移る。

[0135] ステップ S 7 8 において、I D / P W 処理部 6 2 c は、暗号化された I D / P W を認証処理部 6 4 c へ通知すると共に、基地局への接続要求を行う。これに応じて、認証処理部 6 4 c は、再度、通信可能な基地局を捕捉すると、信号同期を行って通信経路を確保した後、基地局との間で認証処理を行い、スマートフォン 1 は、待ち受け状態へ移行する。

[0136] なお、ステップ S 6 5 ～ S 6 8 と、ステップ S 7 6 ～ S 7 7 とは、第 1 実施形態と共通の処理ルーチン A として実現される。

[0137] 本実施形態によれば、スマートフォン 1 は、暗号化処理と認証処理とを並行して実行しつつも、暗号データを確実に取得できるので、認証完了までの処理時間を短縮し、かつ、認証の失敗を抑制できる。

また、スマートフォン 1 は、一旦通信が切断された後に、ユーザ又はアプリケーションからの通信要求に応じて、生成済みの暗号データを用いて即座に認証処理を再開できる。

[0138] 以上、本発明の実施形態について説明したが、本発明は前述した実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、前述の実施形態に記載されたものに限定されるものではない。

[0139] 第 1、第 2 及び第 3 実施形態において、認証処理部 6 4、6 4 a 又は 6 4 b は、ステップ S 1 6、S 3 5 又は S 5 6 で認証要求を受けた際に、タイムアウト等の理由により通信経路が切断されていないかを確認してもよい。通信経路が切断されている場合には、認証処理部 6 4、6 4 a 又は 6 4 b は、再度通信経路を確立した後、基地局へ認証要求を行う。これにより、スマートフォン 1 は、電源起動時に、より確実に通信可能な状態へ移行できる。

[0140] 第 2 実施形態又は第 3 実施形態において、共通ルーチン A は省略可能である。

具体的には、認証処理部 6 4 a 又は 6 4 b は、ステップ S 3 1 又はステッ

プS 5 3において認証開始を通知することなく、ステップS 2 7で暗号化処理部6 1 aから、又はステップS 4 9でID/PW処理部6 2 bから通知された暗号データに基づいて、基地局へ認証要求を行ってもよい。このことによれば、処理手順及び時間が短縮される。

[0141] 第4実施形態において、接続開始命令部1 0 1は、通信要求が生じた際に、基地局との通信経路が確立しているか否かを判断してもよい。通信接続が継続している場合には、ステップS 7 2及びステップS 7 8は認証要求となる。この場合、認証処理部6 4 cは、新たに接続を試みることなく、既にある通信経路を用いて基地局へ認証要求を行う。

[0142] 図4に示したスマートフォン1の構成は一例であり、本発明の要旨を損なわない範囲において適宜変更してよい。

例えば、図4においてストレージ9が記憶することとしたプログラムの一部又は全部は、通信ユニット6による無線通信で他の装置からダウンロードされてもよい。また、図4においてストレージ9が記憶することとしたプログラムの一部又は全部は、ストレージ9に含まれる読み取り装置が読み取り可能な記憶媒体に記憶されていてもよい。また、図4においてストレージ9が記憶することとしたプログラムの一部又は全部は、外部インタフェース1 4に接続される読み取り装置が読み取り可能なCD、DVD、又はBlu-ray（登録商標）等の記憶媒体に記憶されていてもよい。

また、図4に示した各プログラムは、複数のモジュールに分割されていてもよいし、他のプログラムと結合されていてもよい。

[0143] また、前述の実施形態では、通信端末の一例として、スマートフォンについて説明したが、通信端末は、スマートフォンに限定されない。例えば、通信端末は、モバイルフォン、携帯型パソコン、デジタルカメラ、メディアプレーヤ、電子書籍リーダ、ナビゲータ又はゲーム機等の携帯電子機器、あるいは通信機能に特化した通信専用モジュールであってもよい。また、通信端末は、デスクトップパソコン、テレビ受像器等の据え置き型の電子機器であってもよい。

符号の説明

- [0144] 1 スマートフォン（通信端末）
- 6 通信ユニット
- 1 0 コントローラ
- 6 1、6 1 a、6 1 b、6 1 c 暗号化処理部
- 6 2、6 2 a、6 2 b、6 2 c I D／P W処理部（認証情報処理部）
- 6 3 キャッシュ（記憶部）
- 6 4、6 4 a、6 4 b、6 4 c 認証処理部
- 9 1 カード（媒体）
- 9 2 不揮発性記憶領域
- 1 0 1 接続開始命令部

請求の範囲

- [請求項1] 記憶部と、
- 電源起動時に、所定の認証情報を暗号化して暗号データを生成する暗号化処理部と、
- 前記暗号データが通知されると、当該暗号データを前記記憶部に書き込み、通信先に対する認証処理を行う際に、前記記憶部から前記暗号データを読み込む認証情報処理部と、
- 前記通信先への通信経路を確立すると共に、前記認証情報処理部へ前記認証処理の開始を通知したことに応じて、当該認証情報処理部から取得したデータに基づいて、前記通信先へ認証要求を行う認証処理部と、を備え、
- 前記認証処理部は、前記暗号データが生成された後に、前記通信先へ認証要求を行う通信端末。
- [請求項2] 前記認証情報処理部は、前記記憶部に前記暗号データがない場合、前記暗号化処理部から前記暗号データが通知されるまで、前記認証処理を中断する請求項1に記載の通信端末。
- [請求項3] 前記認証処理部は、前記認証情報処理部から前記暗号データが通知された際に、前記通信先への通信経路が切断されている場合、当該通信経路を確立した後、前記通信先へ認証要求を行う請求項2に記載の通信端末。
- [請求項4] 前記暗号化処理部は、前記暗号データを前記認証処理部へ通知し、
- 前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記暗号化処理部から前記暗号データが通知された後、前記認証情報処理部へ前記認証処理の開始を通知する請求項1に記載の通信端末。
- [請求項5] 前記認証情報処理部は、前記暗号データを前記記憶部に書き込んだことを前記認証処理部へ通知し、
- 前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記認証情報処理部から前記暗号データを前記記憶部に書き込んだこと

が通知された後、前記認証情報処理部へ前記認証処理の開始を通知する請求項 1 に記載の通信端末。

[請求項6] 前記暗号化処理部は、前記暗号データを前記認証処理部へ通知し、
前記認証処理部は、電源起動時に前記認証処理の実行を待機し、前記暗号化処理部から前記暗号データが通知されると、前記認証情報処理部へ前記認証処理の開始を通知することなく、当該暗号データに基づいて前記通信先へ認証要求を行う請求項 1 に記載の通信端末。

[請求項7] 前記暗号化処理部から前記暗号データが通知され、前記通信先への接続要求を受け付けたことに応じて、前記認証情報処理部に対して、前記暗号データを通知すると共に当該接続先への接続開始命令を行う接続開始命令部を備え、

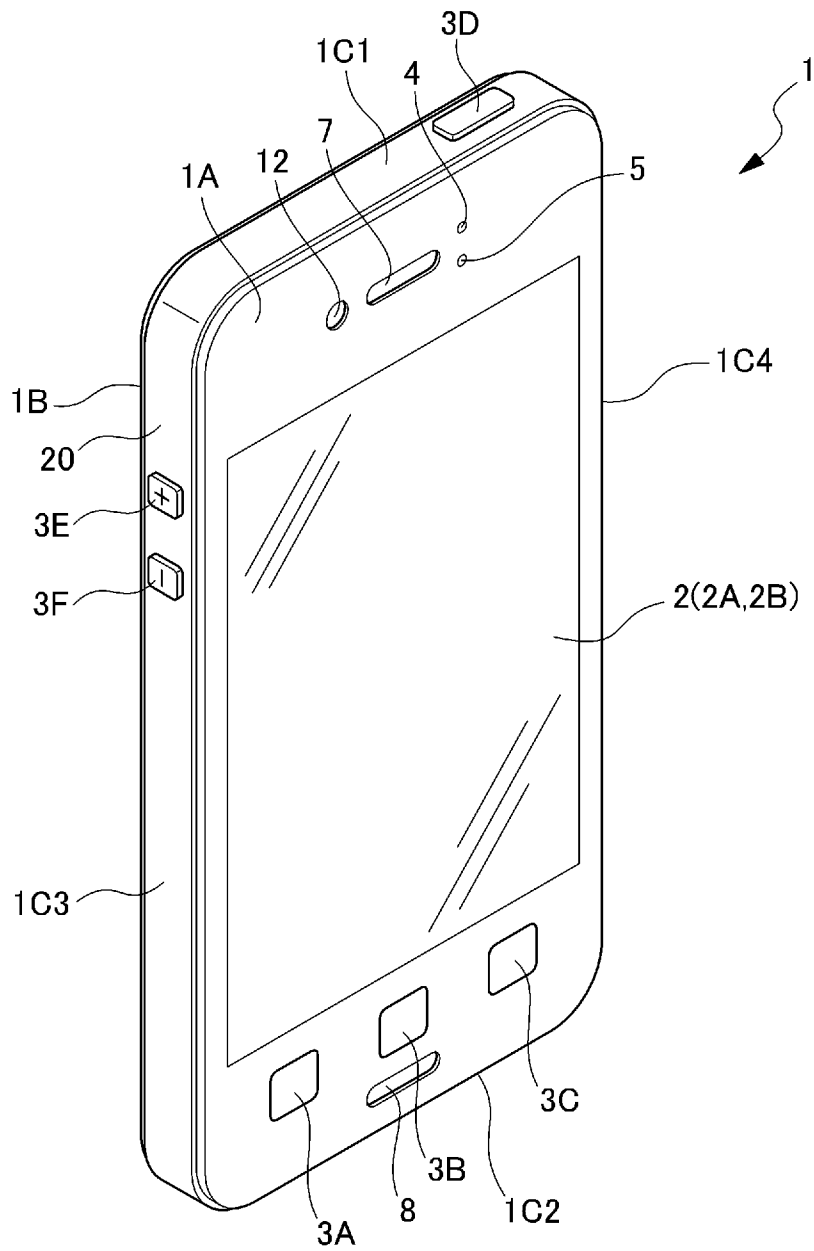
前記認証情報処理部は、前記接続開始命令に応じて、前記記憶部から前記暗号データを読み込んだ後、前記認証処理部に対して前記接続先への接続要求を行う請求項 1 に記載の通信端末。

[請求項8] 加入者識別情報が記録された媒体を備え、
前記所定の認証情報は、前記加入者識別情報に基づくデータである請求項 1 に記載の通信端末。

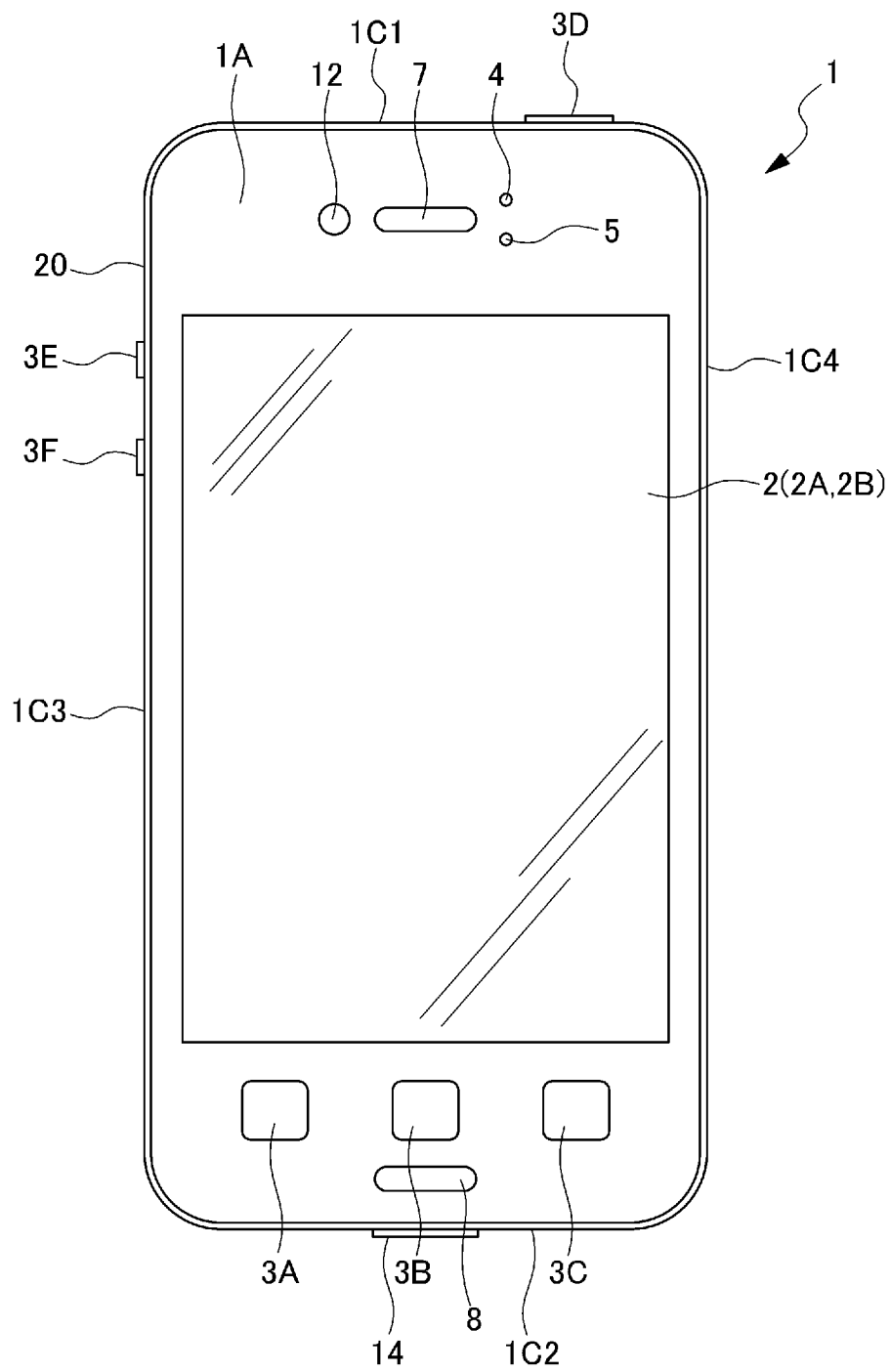
[請求項9] 通信端末が備える記憶媒体であって、
前記通信端末の電源起動時に、所定の認証情報を暗号化して暗号データを生成した後、当該暗号データを記憶する暗号化ステップと、
通信先への通信経路を確立すると共に、記憶されている前記暗号データに基づいて前記通信先へ認証要求を行う認証ステップと、を前記通信端末に実行させる際に、

前記認証ステップにおいて、前記暗号データが記憶された後に、前記通信先へ認証要求を行わせるためのプログラムを記憶した記憶媒体。

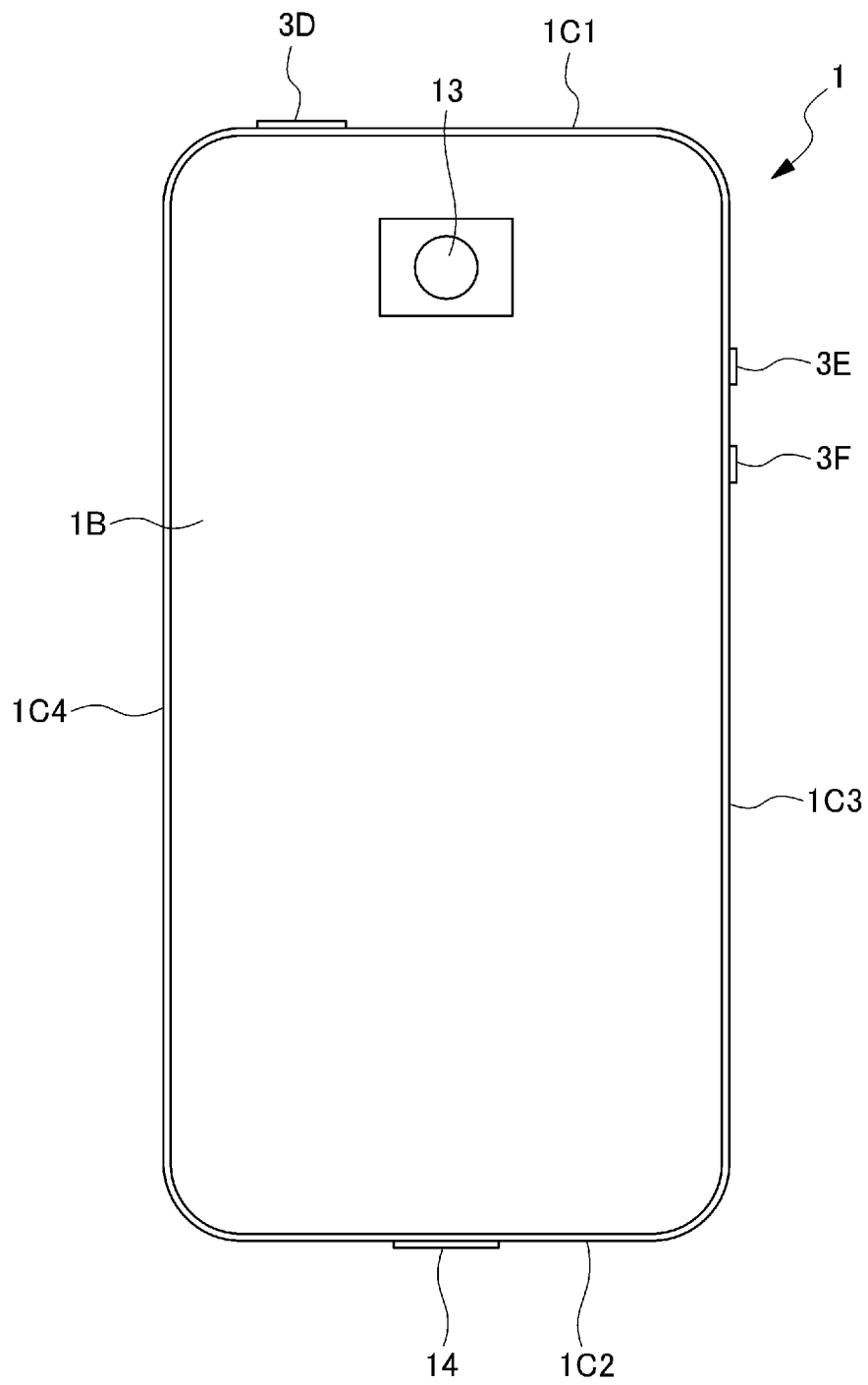
[図1]



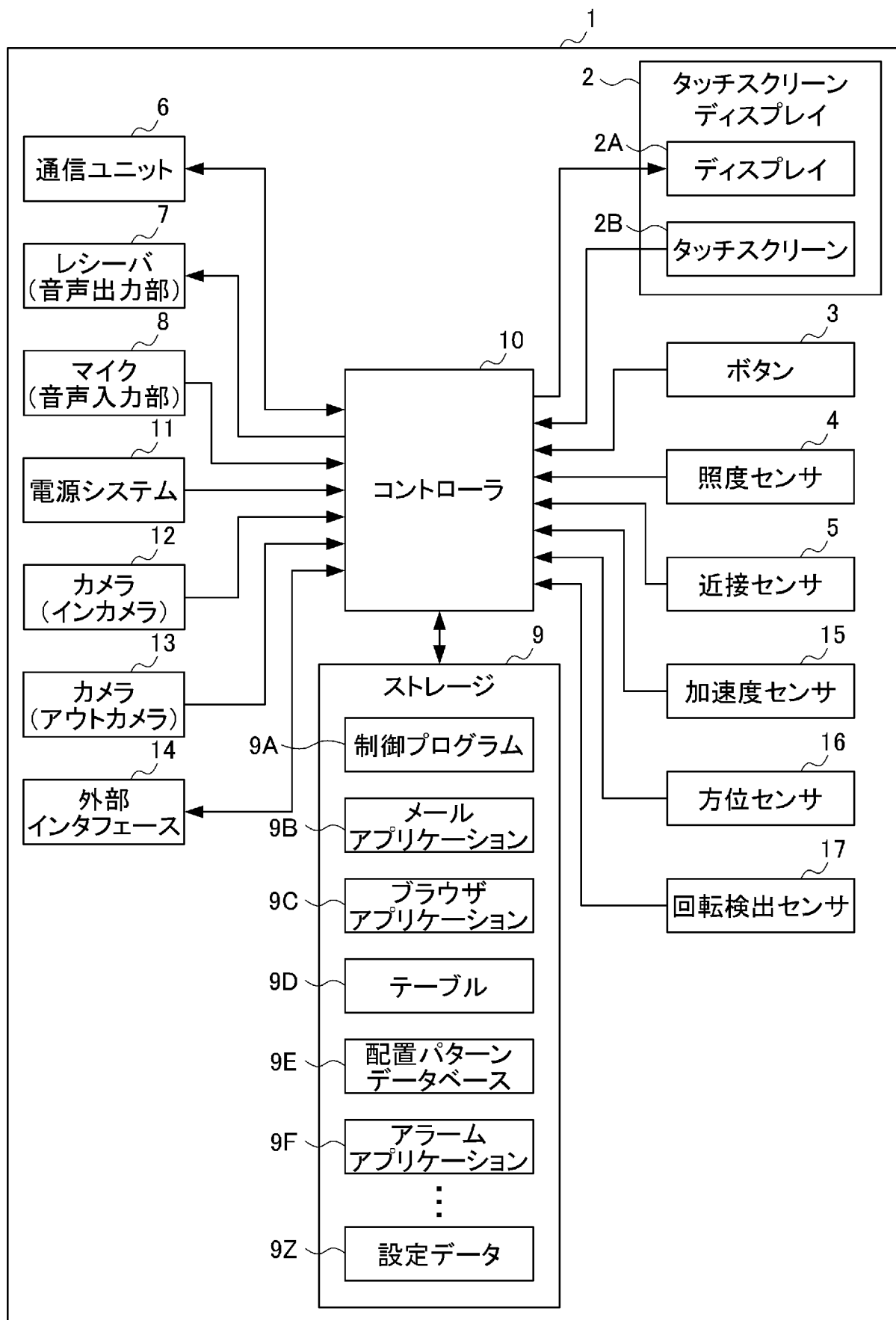
[図2]



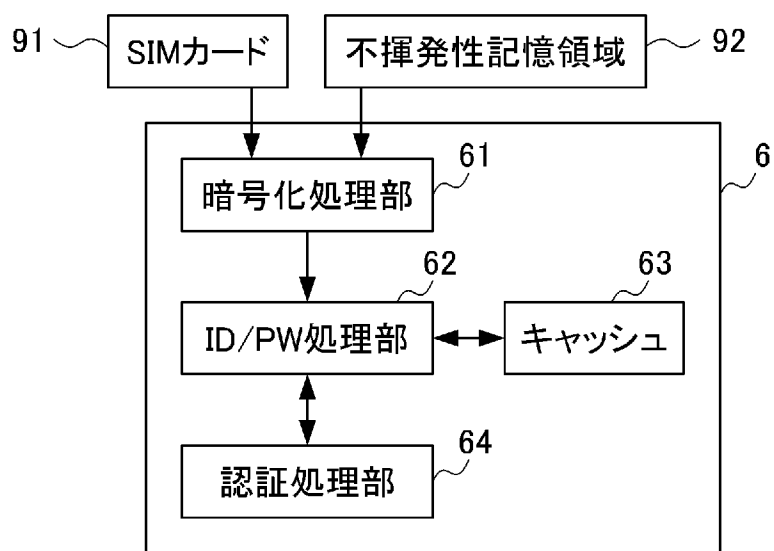
[図3]



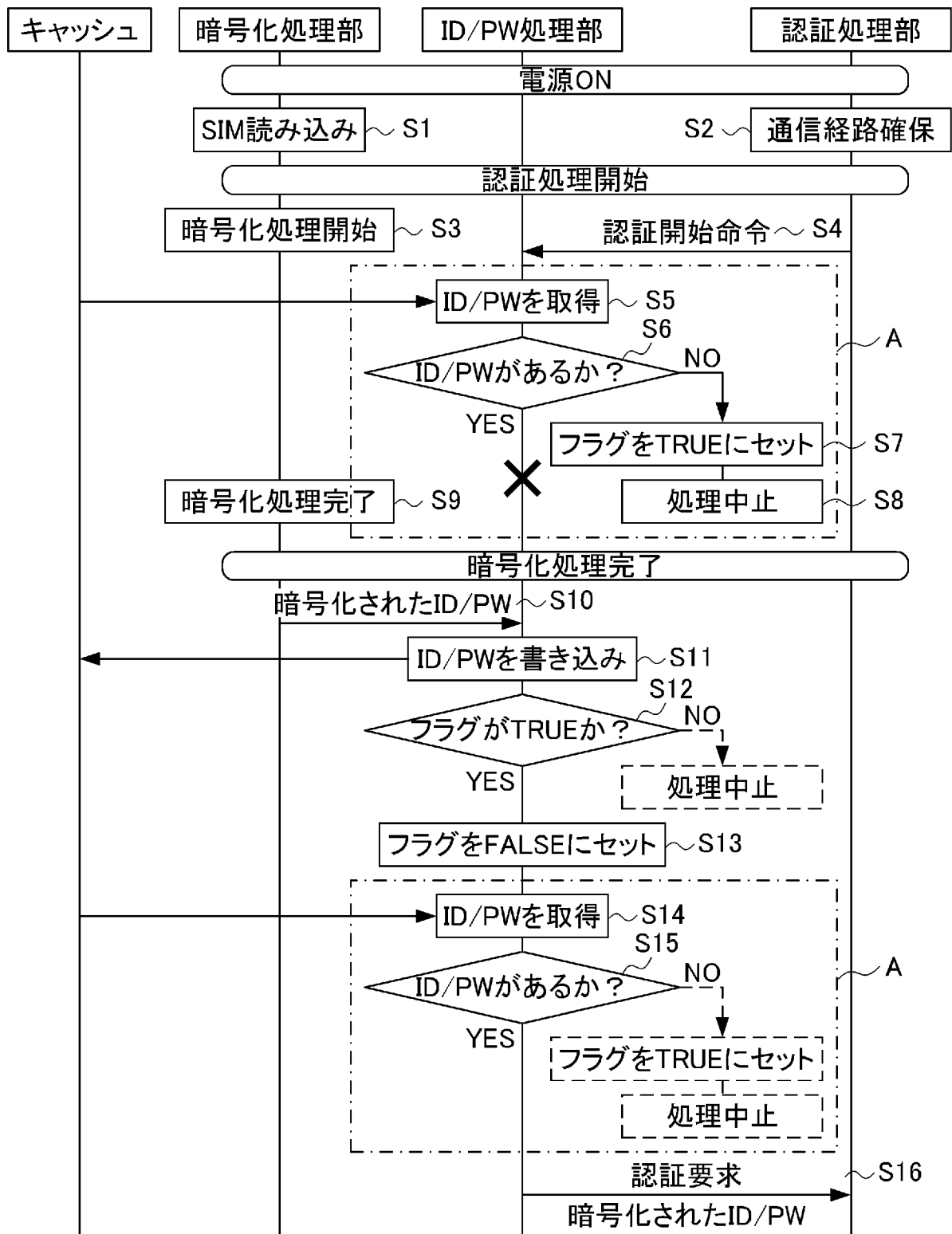
[図4]



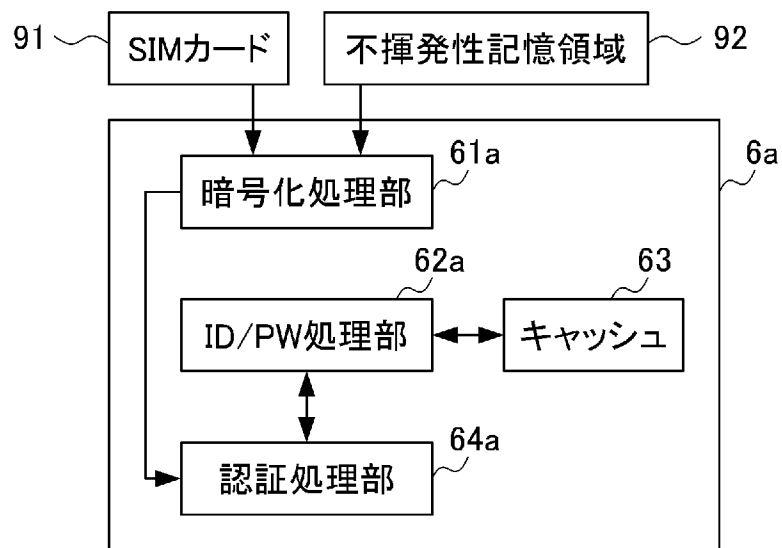
[図5]



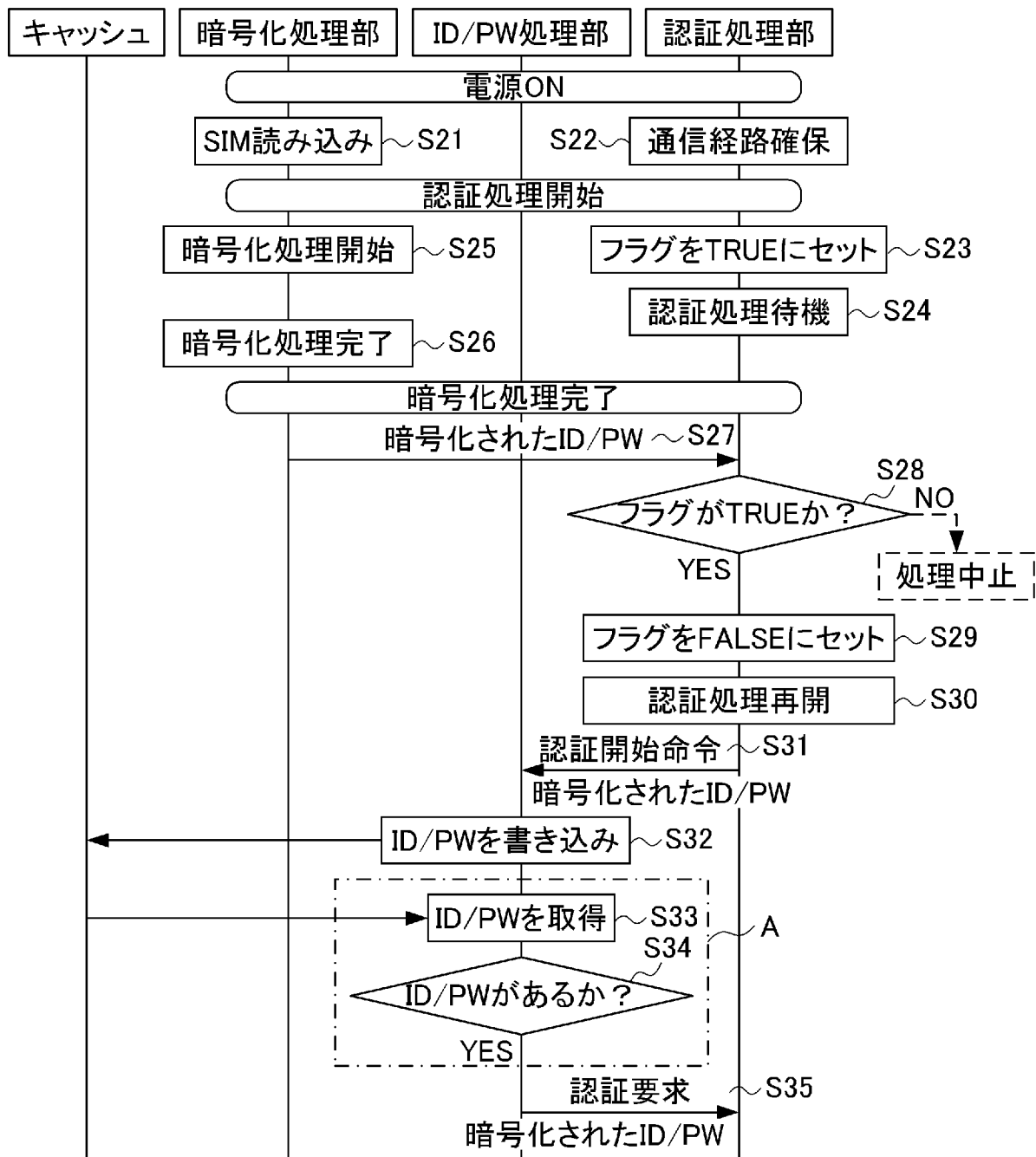
[図6]



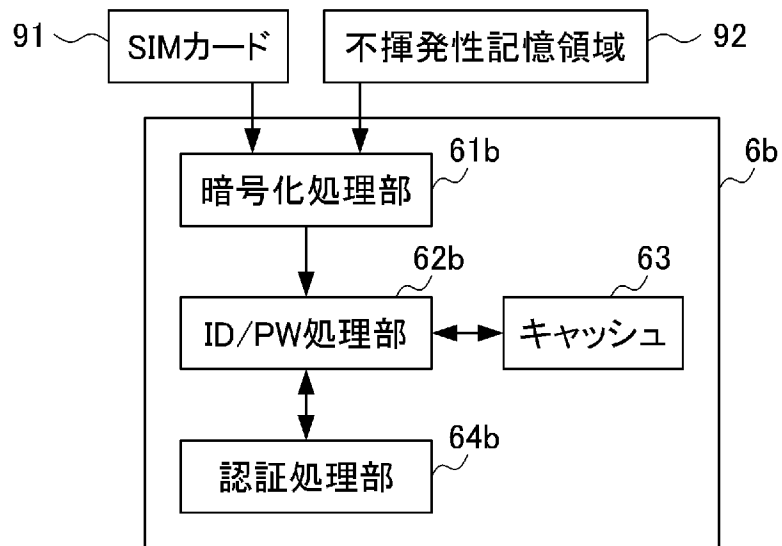
[図7]



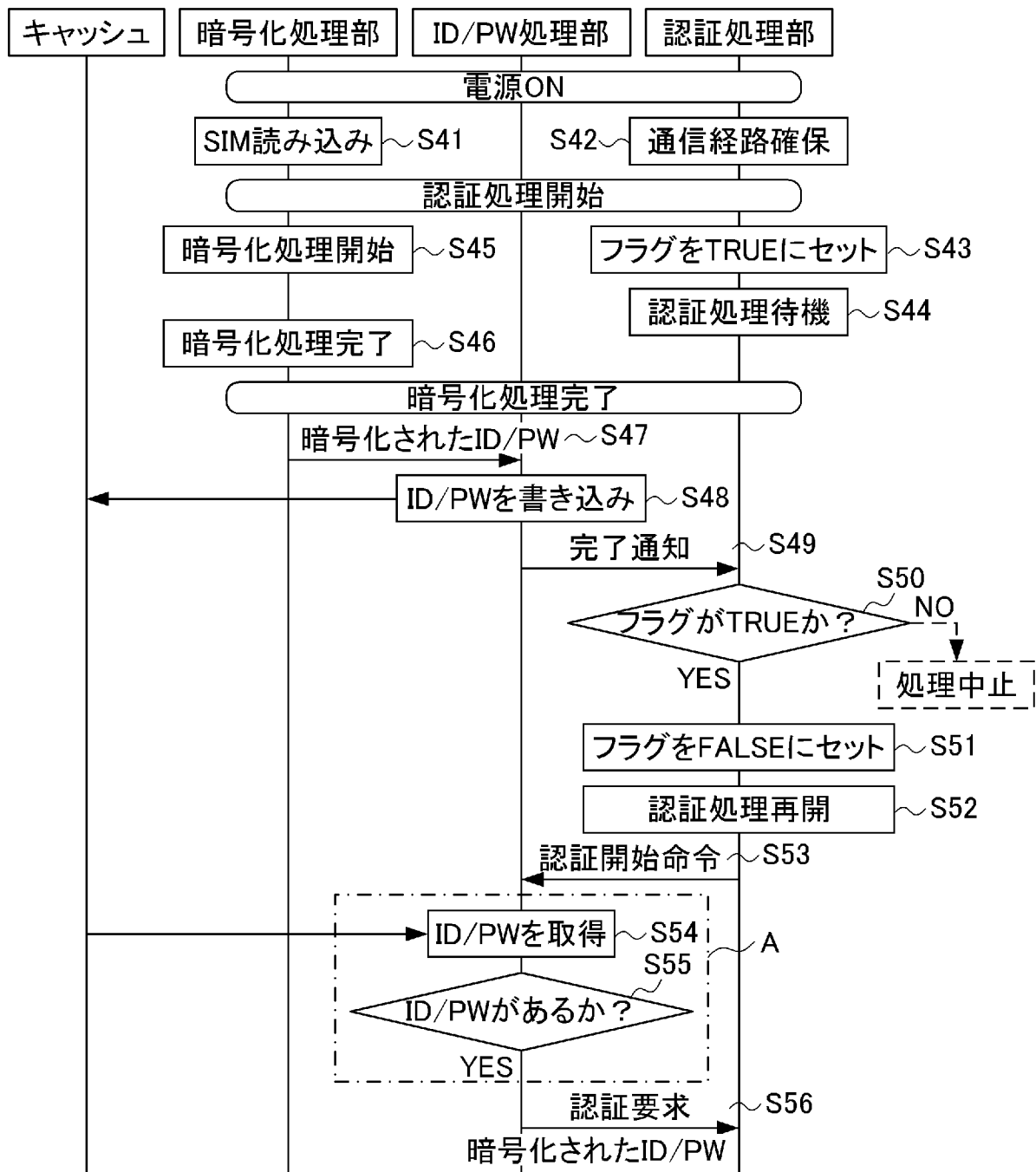
[図8]



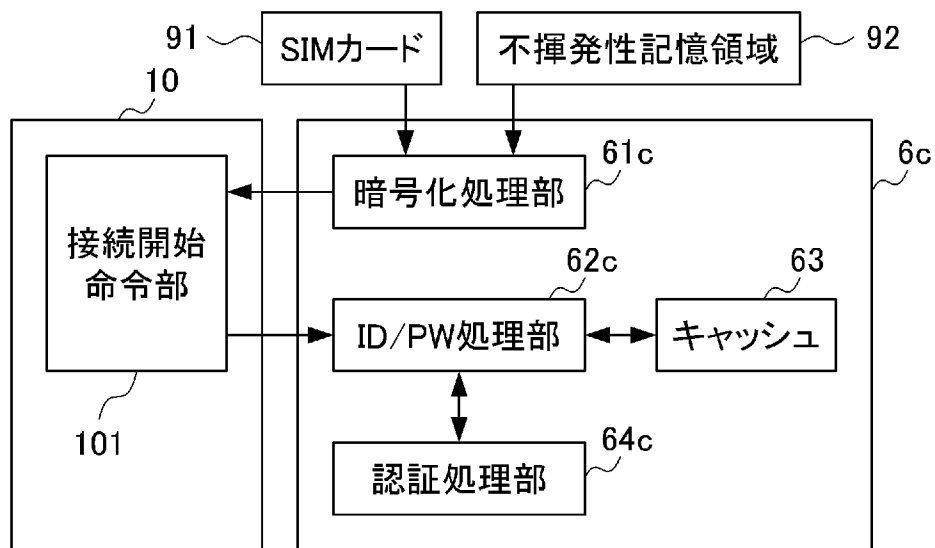
[図9]



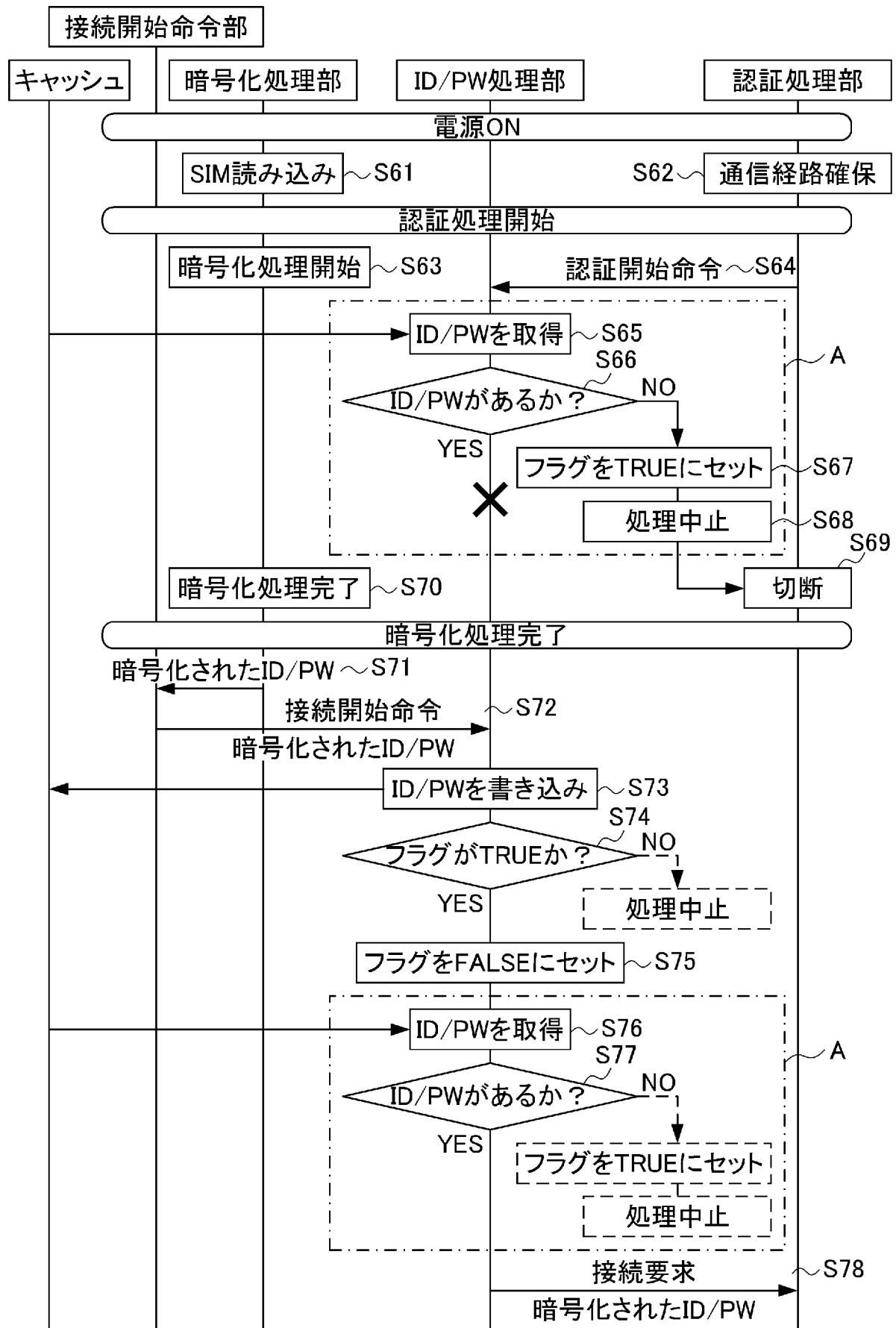
[図10]



[図11]



[図12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/050384

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/45(2013.01)i, G06F21/31(2013.01)i, H04L9/32(2006.01)i, H04M1/00(2006.01)i

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)

G06F21/45, G06F21/31, H04L9/32, H04M1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-114755 A (Ichiro KAZAWA), 09 June 2011 (09.06.2011), paragraphs [0023] to [0074]; fig. 1 to 4 & WO 2011/065217 A1	1, 4-9 2-3
Y A	JP 2011-39970 A (NEC Corp.), 24 February 2011 (24.02.2011), paragraphs [0014] to [0094]; fig. 1, 3, 5A (Family: none)	1, 4-9 2-3
Y A	JP 2009-54189 A (Dainippon Printing Co., Ltd.), 12 March 2009 (12.03.2009), paragraphs [0009] to [0011] (Family: none)	1, 4-9 2-3

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

☐ See patent family annex.

* 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
07 April, 2014 (07.04.14)

Date of mailing of the international search report
15 April, 2014 (15.04.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/050384

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2006-260321 A (NEC Corp.), 28 September 2006 (28.09.2006), paragraphs [0016], [0020]; fig. 1 (Family: none)	1, 4-9 2-3
A	US 2010/0019032 A1 (Kwang-jun KIM), 28 January 2010 (28.01.2010), paragraph [0074] & KR 10-2010-0010843 A	1-9
A	US 2008/0184363 A1 (Sarangan NARASIMHAN), 31 July 2008 (31.07.2008), paragraphs [0027] to [0104] & WO 2006/124666 A2	1-9
A	JP 9-205423 A (Nippon Telegraph and Telephone Corp.), 05 August 1997 (05.08.1997), paragraphs [0052] to [0070]; fig. 1 to 6 (Family: none)	1-9
A	JP 2005-110112 A (NEC Corp.), 21 April 2005 (21.04.2005), paragraphs [0056] to [0096] & US 2005/0076244 A1 & EP 1521491 A2 & CN 1604520 A	1-9

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/45(2013.01)i, G06F21/31(2013.01)i, H04L9/32(2006.01)i, H04M1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F21/45, G06F21/31, H04L9/32, H04M1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2011-114755 A（加沢 一郎） 2011.06.09, 段落 0 0 2 3 - 0 0 7 4, 図 1 - 4 & WO 2011/065217 A1	1, 4-9 2-3
Y A	JP 2011-39970 A（日本電気株式会社） 2011.02.24, 段落 0 0 1 4 - 0 0 9 4, 図 1, 3, 5 A (ファミリーなし)	1, 4-9 2-3

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

0 7 . 0 4 . 2 0 1 4

国際調査報告の発送日

1 5 . 0 4 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

木村 励

5 S

4 0 9 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2009-54189 A (大日本印刷株式会社) 2009.03.12, 段落 0 0 0 9 - 0 0 1 1 (ファミリーなし)	1, 4-9 2-3
Y A	JP 2006-260321 A (日本電気株式会社) 2006.09.28, 段落 0 0 1 6, 0 0 2 0, 図 1 (ファミリーなし)	1, 4-9 2-3
A	US 2010/0019032 A1 (Kwang-jun KIM) 2010.01.28, 段落 0 0 7 4 & KR 10-2010-0010843 A	1-9
A	US 2008/0184363 A1 (Sarangan NARASIMHAN) 2008.07.31, 段落 0 0 2 7 - 0 1 0 4 & WO 2006/124666 A2	1-9
A	JP 9-205423 A (日本電信電話株式会社) 1997.08.05, 段落 0 0 5 2 - 0 0 7 0, 図 1 - 6 (ファミリーなし)	1-9
A	JP 2005-110112 A (日本電気株式会社) 2005.04.21, 段落 0 0 5 6 - 0 0 9 6 & US 2005/0076244 A1 & EP 1521491 A2 & CN 1604520 A	1-9