(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6331528号
(P6331528)

(45)発行日　平成30年5月30日(2018.5.30)　(24)登録日　平成30年5月11日(2018.5.11)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/31	
G06F 3/12	(2006.01)	G06F	3/12	322
H04W 84/10	(2009.01)	G06F	3/12	338
H04W 12/06	(2009.01)	H04W	84/10	110
		H04W	12/06	

請求項の数 18　(全 25 頁)

(21)出願番号　特願2014-52910(P2014-52910)
(22)出願日　平成26年3月17日(2014.3.17)
(65)公開番号　特開2015-176397(P2015-176397A)
(43)公開日　平成27年10月5日(2015.10.5)
審査請求日　平成29年2月28日(2017.2.28)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100110607
弁理士　間山　進也
(72)発明者　豊田　行成
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】認証システムおよび認証方法

(57)【特許請求の範囲】
【請求項１】
利用者に付帯される付帯装置と、前記付帯装置を用いた認証を受け付ける認証受付装置とを含む、認証システムであって、
１または複数の利用者各々の認証情報を登録する登録手段と、
直接通信により、認証を要求する付帯装置に対し、所定符号を送信する前記認証受付装置の送信手段であって、前記所定符号に基づき機械的な振動パターンを通信部位に発生させる振動発生装置を含む、当該送信手段と、
前記送信手段が送信した前記所定符号と、前記登録手段に登録された１または複数の利用者各々の認証情報とから、前記１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成する認証符号生成手段と、
直接通信により、前記付帯装置から被認証符号を受信する前記認証受付装置の受信手段と、
前記受信手段が受信した被認証符号と、前記認証符号生成手段により生成された前記認証符号とを照合し、認証の成否を判定する認証手段と
を含み、前記付帯装置は、
機械的な振動パターンを検知する振動検知装置と、
利用者の認証情報を格納する格納手段と、
前記認証受付装置から受信した前記所定符号と、前記格納手段に格納された認証情報とから、前記認証受付装置へ送信する被認証符号を、前記所定関数を用いて生成する被認証

符号生成手段と
を含む、認証システム。
【請求項２】
前記所定符号として、認証符号を生成するための生成用符号を発生する発生手段をさらに含む、請求項１に記載の認証システム。
【請求項３】
前記認証システムは、前記発生手段が発生させた生成用符号と前記登録手段に登録された認証情報とともに認証符号を与える同期情報を採番する認証側同期採番手段をさらに含み、
前記付帯装置は、前記認証受付装置から受信した生成用符号と前記格納手段に格納された認証情報とともに被認証符号を与える同期情報を採番する被認証側同期採番手段をさらに含み、
前記認証側同期採番手段および前記被認証側同期採番手段は、所定期間中、同一の値を出力する、請求項２に記載の認証システム。
【請求項４】
前記認証側同期採番手段および前記被認証側同期採番手段は、認証開始時点の日付情報を出力する手段である、請求項３に記載の認証システム。
【請求項５】
認証処理を開始させる契機となるイベントを検知する前記認証受付装置の契機検知手段をさらに含む、請求項１～４のいずれか１項に記載の認証システム。
【請求項６】
前記認証手段は、前記被認証符号の少なくとも一部である符号が前記１または複数の利用者各々の認証符号と一致している程度に基づいて、認証の成否を判定することを特徴とする、請求項１～５のいずれか１項に記載の認証システム。
【請求項７】
前記認証手段は、前記被認証符号の全体の受信が完了する前に、前記１または複数の利用者各々の認証符号のうち、前記被認証符号の一部である符号が所定基準以上で一致する認証符号が存在するかを判定し、前記所定基準以上で一致する認証符号が見つかった場合に認証が成功したものと判定する、請求項６に記載の認証システム。
【請求項８】
前記送信手段の直接通信は、通信部位が接触ないし最近接する相手方の受信手段に対し信号を伝達できる通信路を介したものであり、前記受信手段の直接通信は、通信部位が接触ないし最近接する相手方の送信手段から信号の伝達を受けられる通信路を介したものである、請求項１～７のいずれか１項に記載の認証システム。
【請求項９】
前記付帯装置は、前記被認証符号生成手段により生成された被認証符号に基づき機械的な振動パターンを発生する振動発生装置を含み、前記認証受付装置の前記受信手段は、通信部位に伝達された機械的な振動パターンを検知する振動検知装置を含む、請求項１～８のいずれか１項に記載の認証システム。
【請求項１０】
前記付帯装置は、前記被認証符号生成手段により生成された被認証符号に基づき光学的なパターンを発光する発光素子を含み、前記認証受付装置の前記受信手段は、通信部位に入射した光学的なパターンを受光する受光素子を含む、請求項１～８のいずれか１項に記載の認証システム。
【請求項１１】
前記認証システムは、
前記登録手段、前記認証符号生成手段および前記認証手段のうちの少なくとも１つの手段を含み、前記認証受付装置と通信する認証サーバと、
前記認証手段による認証の成否の結果に基づき動作が制御される認証対象装置と
を含み、前記認証対象装置は、前記認証受付装置であるか、または前記認証受付装置に

近接して配置される外部装置である、請求項１～１０のいずれか１項に記載の認証システム。
【請求項１２】
前記認証符号生成手段は、前記所定符号に対して、前記登録手段に登録された前記１または複数の利用者各々に対応する認証符号を予め準備し、前記認証手段は、認証が成功した場合には、前記１または複数の利用者各々に対応する認証符号のうちの一致した認証符号を無効化し、前記所定符号および予め準備された前記１または複数の利用者各々に対応する認証符号の組が再利用されることを特徴とする、請求項１～１１のいずれか１項に記載の認証システム。
【請求項１３】
前記認証情報は、利用者識別値を含み、
前記付帯装置は、さらに、
前記認証受付装置から受信した前記所定符号に基づいて探索基準値を生成する手段と、
前記探索基準値と、前記格納手段に格納された認証情報に含まれる利用者識別値との比較結果を生成する手段と、
前記認証受付装置へ送信する前記被認証符号に対し前記比較結果を付する手段と
を含み、前記認証システムは、さらに、
前記送信手段が送信した前記所定符号に基づき探索基準値を生成する手段と、
前記被認証符号の少なくとも一部である符号から前記比較結果を抽出する手段と
を含み、前記認証符号生成手段は、前記探索基準値と、前記比較結果とに基づいて、認証符号を生成する認証情報の範囲を限定する、請求項１～１２のいずれか１項に記載の認証システム。
【請求項１４】
前記所定関数は、少なくとも前記所定符号および前記認証情報を入力として認証符号または被認証符号を出力するハッシュ関数である、請求項１～１３のいずれか１項に記載の認証システム。
【請求項１５】
認証情報を格納し、機械的な振動パターンを検知する振動検知装置を有する付帯装置を用いた認証を受け付ける認証受付装置を含む、認証システムであって、
１または複数の利用者各々の認証情報を登録する登録手段と、
直接通信により、認証を要求する付帯装置に対し、所定符号を送信する前記認証受付装置の送信手段であって、前記所定符号に基づき機械的な振動パターンを通信部位に発生させる振動発生装置を含む、当該送信手段と、
前記送信手段が送信した前記所定符号と、前記登録手段に登録された前記１または複数の利用者各々の認証情報とから、前記１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成する認証符号生成手段と、
直接通信により、前記付帯装置から、該付帯装置側で受信した前記所定符号と格納された認証情報とから前記所定関数を用いて生成された被認証符号を受信する前記認証受付装置の受信手段と、
前記受信手段が受信した前記被認証符号と、前記認証符号生成手段により生成された前記認証符号とを照合し、認証の成否を判定する認証手段と
を含む、認証システム。
【請求項１６】
機械的な振動パターンを検知する振動検知装置を有し、利用者に付帯される付帯装置と、前記付帯装置を用いた認証を受け付ける認証受付装置とを含む、認証システムで実行される認証方法であって、
前記認証受付装置が、直接通信により、認証を要求する付帯装置に対し、所定符号を送信するステップであって、振動発生装置により前記所定符号に基づき機械的な振動パターンを通信部位に発生させるステップと、
前記認証システムを構成するコンピュータが、登録された１または複数の利用者各々の

認証情報を読み出すステップと、
前記認証システムを構成するコンピュータが、送信した前記所定符号と、読み出された前記１または複数の利用者各々の認証情報とから、前記１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成するステップと、
前記付帯装置が、前記付帯装置が格納する利用者の認証情報と、前記認証受付装置から受信した前記所定符号とから、被認証符号を、前記所定関数を用いて生成するステップと、
前記認証受付装置が、直接通信により、前記付帯装置から前記被認証符号を受信するステップと、
前記認証システムを構成するコンピュータが、受信された前記被認証符号と、準備された前記認証符号とを照合し、認証の成否を判定するステップと
を含む、認証方法。
【請求項１７】
機械的な振動パターンを検知する振動検知装置を有し、利用者に付帯される付帯装置を実現するためのプログラムと、前記付帯装置を用いた認証を受け付ける認証受付装置とを含む、認証システムであって、
１または複数の利用者各々の認証情報を登録する登録手段と、
直接通信により、認証を要求する付帯装置に対し、所定符号を送信する前記認証受付装置の送信手段であって、前記所定符号に基づき機械的な振動パターンを通信部位に発生させる振動発生装置を含む、当該送信手段と、
前記送信手段が送信した前記所定符号と、前記登録手段に登録された１または複数の利用者各々の認証情報とから、前記１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成する認証符号生成手段と、
直接通信により、前記付帯装置から被認証符号を受信する前記認証受付装置の受信手段と、
前記受信手段が受信した前記被認証符号と、前記認証符号生成手段により生成された前記１または複数の利用者各々に対応する認証符号とを照合し、認証の成否を判定する認証手段と
を含み、前記プログラムは、直接通信による送信手段および直接通信による受信手段を含む前記付帯装置のコンピュータを、
利用者の認証情報を格納する格納手段、および
前記付帯装置の前記受信手段により前記認証受付装置から受信した前記所定符号と、前記格納手段に格納された認証情報とから、前記付帯装置の前記送信手段により前記認証受付装置へ送信する被認証符号を、前記所定関数を用いて生成する被認証符号生成手段
として機能させるためのプログラムである、認証システム。
【請求項１８】
機械的な振動パターンを検知する振動検知装置を有し、利用者に付帯される付帯装置を実現するためのプログラムと、前記付帯装置を用いた認証を受け付ける認証受付装置と、前記認証受付装置上、または前記認証受付装置の外部装置上に認証処理手段を実現するためのプログラムとを含む、認証システムであって、前記認証処理手段を実現するためのプログラムは、前記認証受付装置または前記外部装置のコンピュータを、
１または複数の利用者各々の認証情報を登録する登録手段、
所定符号と、前記登録手段に登録された前記１または複数の利用者各々の認証情報とから、前記１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成する認証符号生成手段、および
前記認証受付装置の受信手段が受信した被認証符号と、前記認証符号生成手段により生成された前記１または複数の利用者各々に対応する認証符号とを照合し、認証の成否を判定する認証手段
として機能させるためのプログラムであり、前記認証受付装置は、
直接通信により、認証を要求する付帯装置に対し、前記所定符号を送信する送信手段で

あって、前記所定符号に基づき機械的な振動パターンを通信部位に発生させる振動発生装置を含む、当該送信手段と、
直接通信により、前記付帯装置から被認証符号を受信する受信手段と
を含み、前記付帯装置を実現するためのプログラムは、前記付帯装置のコンピュータを、
利用者の認証情報を格納する格納手段、および
前記認証受付装置から受信した前記所定符号と、前記格納手段に格納された認証情報とから、前記認証受付装置に送信する前記被認証符号を、前記所定関数を用いて生成する被認証符号生成手段
として機能させるためのプログラムである、認証システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証技術に関し、より詳細には、利用者の認証を行う認証システムおよび認証方法に関する。
【背景技術】
【０００２】
従来、情報機器を利用する利用者を認証するシステムとして、ＩＣ（Integrated Circuit）カードや携帯情報端末に利用者の認証情報を記録し、情報機器が備えるリーダに接近させることで利用者認証をおこなう認証システムが既に知られている。このようなシステムでは、ＩＣカードや携帯情報端末などの付帯装置およびリーダは、電波による近距離無線通信方式に対応しており、近距離無線通信により、これらの間で認証情報のやり取りを行っている。
【０００３】
また近年、ネットワークを介して物理的に近接する情報機器同士を接続する技術として、点滅パターン、発光パターン、音声パターン、振動パターンといった限定された範囲にのみ信号が到達可能な特殊な通信路を介して、機器を特定するためのＩＰアドレスといった通信情報を符号化して伝送する技術が知られている。
【０００４】
例えば、特開２００７‐２４９４２５号公報（特許文献１）は、デジタルカメラを固有に識別可能なユニークパターンを生成する生成部と、ユニークパターンを出力する報知部と、無線通信を行う通信部とを備えるデジタルカメラを開示する。特許文献１では、さらに、ユニークパターンの入力を受け付ける入力部と、ユニークパターンに基づいてデジタルカメラの接続認証を行う認証部と、無線通信を行う通信部とを備えるプリンタを開示する。
【０００５】
また、特開２００７－２２８５５４号公報（特許文献２）は、他の機器の接触による第一の物理量の変化を検出する物理量検出手段と、他の機器で検出された第二の物理量の変化情報を含む信号を受信する物理量受信手段と、検出された第一の物理量の変化と、受信した第二の物理量の変化とを比較して類似性の有無を判断し、類似性を有すると判断された場合に、他の機器との通信を確立する通信確立手段とを有するデータ通信装置を開示する。
【０００６】
しかしながら、上記近距離無線通信を用いる認証システムでは、通信方式に対応したＩＣカードや携帯情報端末を所持していない利用者は、自身の認証情報を記憶し、機器を利用する際にキーボードなどを用いて、認証情報を入力する必要があった。
【０００７】
また、特許文献１および特許文献２に開示されるような、特殊な通信路を介して情報を通信する技術では、情報機器同士は、無線通信ＬＡＮなどのネットワークを介して別途相互に通信可能となっている必要があり、接続の設定に手間がかかるという問題があった。

さらに、特殊な通信路を介してアドレスなどの情報を通信する際に、通信内容の傍受が容易である可能性があり、セキュリティ上の観点から充分なものではなかった。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

本発明は、上記従来技術における不充分な点に鑑みてなされたものであり、本発明は、利用者に付帯される付帯装置と、該付帯装置を用いた認証を受け付ける認証受付装置との間の認証のための通信路のセキュリティを向上することができる、認証システムおよび認証方法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】

【０００９】

本発明は、上記課題を解決するために、下記特徴を有する認証システムを提供する。本認証システムは、利用者に付帯される付帯装置と、付帯装置を用いた認証を受け付ける認証受付装置とを含む。

【００１０】

認証システムは、１または複数の利用者各々の認証情報を登録する登録手段と、直接通信により、認証を要求する付帯装置に対し、所定符号を送信する認証受付装置の送信手段と、上記送信手段が送信した所定符号と、上記登録手段に登録された１または複数の利用者各々の認証情報とから、１または複数の利用者各々に対応する認証符号を、所定関数を用いて生成する認証符号生成手段と、直接通信により、付帯装置から被認証符号を受信する認証受付装置の受信手段と、上記受信手段が受信した被認証符号と、上記認証符号生成手段により生成された認証符号とを照合し、認証の成否を判定する認証手段とを含む。

【００１１】

付帯装置は、利用者の認証情報を格納する格納手段と、上記認証受付装置から受信した所定符号と、上記格納手段に格納された認証情報とから、認証受付装置へ送信する被認証符号を、上記所定関数を用いて生成する被認証符号生成手段とを含む。

【発明の効果】

【００１２】

上記構成により、利用者に付帯される付帯装置と、該付帯装置を用いた認証を受け付ける認証受付装置との間の認証のための通信路のセキュリティを向上することができる。

【図面の簡単な説明】

【００１３】

【図１】第１の実施形態による認証プリントシステムの概略構成図。

【図２】第１の実施形態による認証プリントシステムのハードウェア構成図。

【図３】第１の実施形態による認証プリントシステムの機能ブロック図。

【図４】第１の実施形態による認証プリントシステムにおいて、プリンタおよび携帯情報端末間で実行される、利用者認証処理を示すフローチャート。

【図５】第１の実施形態による認証プリントシステムで用いられる情報のデータ構造を例示する図（１／２）。

【図６】第１の実施形態による認証プリントシステムで用いられる情報のデータ構造を例示する図（２／２）。

【図７】変形例の実施形態による認証プリントシステムで用いられる情報のデータ構造を例示する図。

【図８】第２の実施形態による認証プリントシステムの概略構成を示す図。

【図９】第２の実施形態による認証プリントシステムの機能ブロック図。

【図１０】第２の実施形態による認証プリントシステムで用いられる情報のデータ構造を例示する図。

【発明を実施するための形態】

【００１４】

以下、本実施形態について説明するが、以下に説明する実施形態に限定されるものでは

ない。
【００１５】
［第１の実施形態］
以下に説明する第１の実施形態では、利用者に付帯される付帯装置と、認証受付装置とを含む認証システムとして、システムの利用者に付帯される携帯情報端末１５０と、認証を受け付け、認証処理を行い、認証結果に基づき動作が制御されるプリンタ１１０とを含む認証プリントシステム１００を一例として説明する。
【００１６】
図１は、第１の実施形態による認証プリントシステム１００の概略構成を示す図である。図１に示すように、認証プリントシステム１００は、認証によって利用者が制限されているプリンタ１１０と、利用者が付帯し、利用者に代わって認証情報を保持する携帯情報端末１５０とを含み構成される。
【００１７】
本実施形態による認証プリントシステム１００においては、プリンタ１１０および携帯情報端末１５０の間の通信は、機械的な振動パターンを用いて行われる。プリンタ１１０に設けられた積載台１１０ａ上に携帯情報端末１５０が置かれることで、互いの通信部位同士が接触し、プリンタ１１０および携帯情報端末１５０間の通信が可能となる。プリンタ１１０および携帯情報端末１５０間では、機械的な振動パターンによって認証のための情報が交換されて、プリンタ１１０への利用者認証が行われる。
【００１８】
説明する実施形態では、認証プリントシステム１００とし、認証を受け付け、認証処理を行い、認証結果に基づき動作が制御される装置としてプリンタ１１０を用い、利用者が付帯する付帯装置として携帯情報端末１５０を用いている。しかしながら、認証システムの構成は、特に限定されるものではなく、他の実施形態では、プリンタに代えて、スキャナ、複写機、複合機、ファクシミリ、プロジェクタ、デジタルカメラなど如何なる情報処理装置や、入出管理装置などのような他の装置であってもよい。付帯装置としても、スマートフォン、タブレット・コンピュータ、ＰＤＡ（Personal Digital Assistance）などの携帯情報端末１５０のほか、ラップトップ・コンピュータ、専用キーなど利用者などの個体に付帯される如何なる装置であってもよい。
【００１９】
また、説明する実施形態では、プリンタ１１０が、認証を受け付ける認証受付装置、認証処理を行う認証処理装置、および認証結果に基づき動作が制御される認証対象装置としての役割を有している。しかしながら、認証受付装置、認証処理装置および認証対象装置は、それぞれ分離された別の装置として構成されてもよい。例えば、認証処理を行う認証サーバ、認証を受け付けるとともに認証結果に基づき動作が制御されるプリンタを含むシステムとして構成したり、認証を受け付ける認証受付装置をプリンタに近接して配置され、接続される外部装置と構成したりしてもよい。
【００２０】
図２は、第１の実施形態による認証プリントシステム１００のハードウェア構成を示す図である。図２に示すように、プリンタ１１０は、振動発生装置１１４と、振動検知センサ１１６と、近接検知センサ１１８とを備えており、それぞれプログラムにより制御される。携帯情報端末１５０は、振動検知センサ１５４と、振動発生装置１５６とを備えており、同様に、プログラムにより制御される。
【００２１】
プリンタ１１０が備える振動発生装置１１４は、携帯情報端末１５０と接触させる通信部位に振動パターンを発生させて、携帯情報端末１５０が備える振動検知センサ１５４に対し、振動パターンを伝達する装置である。振動発生装置１１４は、特に限定されるものではないが、振動の強さ、周波数、時間を制御可能な振動発生装、または所定の時間精度で振動のオンまたはオフのみを制御可能なバイブレーション・モータなどとして構成することができる。また、振動発生装置１１４としては、プリンタ１１０が備えるプリントエ

ンジンなどの動力を利用してもよい。

【００２２】

プリンタ１１０が備える振動検知センサ１１６は、携帯情報端末１５０が備える振動発生装置１５６で発生されて、携帯情報端末１５０と接触させる通信部位に伝達されてきた振動パターンを検知する装置である。振動検知センサ１１６は、特に限定されるものではないが、圧電抵抗を使用した加速度センサ、またはバネと可動部、スイッチを組み合わせた変位検出装置として構成することができる。

【００２３】

これに対して、携帯情報端末１５０が備える振動検知センサ１５４は、プリンタ１１０が備える振動発生装置１１４が発生させ、プリンタ１１０と接触させる通信部位に伝達された振動パターンを検知する装置であり、同様に、加速度センサまたは変位検出装置として構成することができる。携帯情報端末１５０が備える振動発生装置１５６も、プリンタ１１０と接触させる通信部位に振動パターンを発生させて、プリンタ１１０が備える振動検知センサ１１６に対し振動パターンを伝達する装置であり、同様に、振動発生装置、またはバイブレーション・モータなどとして構成することができる。バイブレーション・モータや加速度センサは、典型的なスマートフォンなどの携帯情報端末に備えられており、このような既存のハードウェアを活用することで、コストを低減することができる。

【００２４】

プリンタ１１０が備える近接検知センサ１１８は、通信部位に近接して設けられており、物体の接近を常時または定期的に監視しており、認証手続を開始しようとして利用者が携帯情報端末１５０を近づけたことを検知する。説明する実施形態では、近接検知センサ１１８は、認証手続を開始する契機となるイベントとして、携帯情報端末１５０の近接を検知する。近接検知センサ１１８は、特に限定されるものではないが、赤外線反射を検出する赤外線センサ、または磁束変化を検出する磁気センサとして構成することができる。

【００２５】

利用者が、携帯情報端末１５０の通信部位（振動発生装置１５６および振動検知センサ１５４と連動する筐体）と、プリンタ１１０の通信部位（振動発生装置１１４、振動検知センサ１１６および近接検知センサ１１８が設けられる積載台）とを接触させることによって、プリンタ１１０の近接検知センサ１１８が作動し、振動パターンによる直接通信が開始される。

【００２６】

なお、説明する実施形態では、利用者が携帯情報端末１５０をプリンタ１１０の積載台１１０ａの上に置くなどして、携帯情報端末１５０が近接検知センサ１１８に検知されることによって、プリンタ１１０が備える振動発生装置１１４から振動パターンが発生されて、認証手続が開始される。しかしながら、認証手続の要求の検知方法は、これに限定されるものではない。他の実施形態では、振動発生装置１１４が定期的に振動パターンを送信し、携帯情報端末１５０側で、振動パターンのスタートを検出し、これに応答して振動パターンを送信することで、プリンタ１１０側で認証手続の開始の要求を検知してもよい。この場合に、近接検知センサ１１８は、必ずしも要さない。

【００２７】

また、説明する好適な実施形態では、振動発生装置１１４および振動検知センサ１１６を用いて、機械的な振動パターンに乗せて認証に必要な情報を伝達するものとして説明する。これは、機械的な振動パターンは、プリンタ１１０および携帯情報端末１５０の通信部位を物理的に接触させる必要がある点で、送信者のなりすましを防止し、また、通信内容の改ざんを防止する観点から好ましいためである。

【００２８】

しかしながら、プリンタ１１０および携帯情報端末１５０が採用する直接通信方式としては、必ずしも機械的な振動を用いた方式に限定されるものではなく、プリンタ１１０と携帯情報端末１５０との間の直接通信を可能とする種々の通信方式を採用することができる。ここで、直接通信とは、送信者と受信者とが他の中継装置を媒介せずに通信する形態

をいう。プリンタ１１０および携帯情報端末１５０が採用する直接通信方式としては、より好ましくは、信号の到達範囲の限定されており、通信部位が接触ないし最近接する相手方のみに対し信号を伝達することができ、または通信部位が接触ないし最近接する相手方のみから信号の伝達を受けられる通信路を介した通信方式とすることができる。つまり、信号の到達範囲には、ただ一つの相手方装置しか配置することができないような構成とするとよい。

【００２９】

例えばＬＥＤや冷陰極管などの光を放射する発光素子と、照度センサやフォトダイオードなどの光を検出する受光素子とを用いて、光パターンを伝達する方式としてもよい。この場合において、例えば光の放射や受光の指向性を高めたりすることにより、通信部位が所定の位置関係に配置された端末のみが、光によりプリンタと通信できるように構成し、プリンタ１１０および携帯情報端末１５０の通信部位の物理的な近接を担保するようにすることが好ましい。その他、スピーカなどの音波発生装置と、マイクロフォンなどの音波受信装置とを用いて、音波パターンを伝達する方式としてもよく、同様に、音波の送信や受信の指向性を高めたりすることにより、通信部位が所定の位置関係に配置された端末のみが、音波によりプリンタと通信できるように構成してもよい。

【００３０】

ＬＥＤや、照度センサ、スピーカ、マイクロフォンは、典型的なスマートフォンなどの携帯情報端末に備えられており、このような既存のハードウェアを活用することで、コストを低減することができる。また、プリンタ１１０から携帯情報端末１５０への通信路と、携帯情報端末１５０からプリンタ１１０への通信路とは、異なる直接通信方式を採用してもよい。

【００３１】

図２に示すように、プリンタ１１０のハードウェア構成としては、さらに、コントローラ１１２と、記憶装置１２０と、ＲＴＣ（Real Time Clock）１２２と、操作パネル１２４と、通信インタフェース（以下、インタフェースをＩ／Ｆと参照する。）１２６と、プリンタ・エンジン１２８とを含み、これらの要素は、コントローラ１１２のＲＯＭなどに格納された制御プログラムによって制御される。

【００３２】

ＲＴＣ１２２は、日付を出力し、通常、携帯情報端末１５０のＲＴＣ１６０と同じ日付を示す。コントローラ１１２は、近接検知時点の日付の出力を受ける。説明する実施形態では、コントローラ１１２は、ＲＴＣ１２２から日付を取得しているが、他の実施形態では、ＲＴＣ１２２に代えて、通信Ｉ／Ｆ１２６を用いて外部の時刻提供システムから日付を取得するよう構成してもよい。

【００３３】

記憶装置１２０は、プリンタ１１０に登録されたすべての利用者の認証情報が登録される認証データベース（以下、データベースをＤＢと参照する。）を記憶する。記憶装置１２０は、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Memory）、不揮発性メモリなどの記憶装置である。なお、説明する実施形態では、プリンタ１１０が備える記憶装置１２０が、認証ＤＢを格納するものとして説明するが、他の実施形態では、プリンタ１１０の外部の認証サーバが認証ＤＢを格納し、プリンタ１１０と通信回線で接続されていてもよい。さらに他の実施形態では、複数のプリンタと通信回線で結ばれ、認証ＤＢが共有または同期されていてもよい。

【００３４】

操作パネル１２４は、利用者の印刷指示などの指示を受け付けるとともに、処理結果を表示するものであり、ディスプレイなどの表示装置、ボタンなどの入力装置を含み構成される。通信Ｉ／Ｆ１２６は、プリンタ１１０をＬＡＮ（Local Area Network）などのネットワークに接続し、印刷データを受信する際に用いられる。通信Ｉ／Ｆ１２６は、ＮＩＣ、無線ネットワーク・アダプタなどである。プリンタ・エンジン１２８は、印刷データに基づき作像動作を行い、紙などの転写部材上に画像形成を行う。

【００３５】
説明する実施形態では、プリンタ１１０は、通信Ｉ／Ｆ１２６より印刷データを受信した後、携帯情報端末１５０を用いて正当な利用者が認証された場合に、操作パネル１２４が利用者に使用可能となる。その後、利用者が操作パネル１２４より印刷開始を指示すると、この指示を受けて、プリンタ・エンジン１２８により印刷出力が行われる。
【００３６】
コントローラ１１２上には、図示しないＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）などのハードウェアが備えられている。ＣＰＵが、ＲＯＭや、ＨＤＤやＳＳＤなどの記憶装置に格納された制御プログラムを読み出し、ＲＡＭが提供する作業空間上に展開することにより、後述する各機能手段および各処理を実現する。
【００３７】
図２に示すように、携帯情報端末１５０のハードウェア構成としては、さらに、コントローラ１５２と、記憶装置１５８と、ＲＴＣ１６０と、タッチパネル１６２とを含み、これらの要素は、コントローラ１５２のＲＯＭなどに格納された制御プログラムにより制御される。
【００３８】
ＲＴＣ１６０は、日付を出力しており、通常、プリンタ１１０のＲＴＣ１２２と同じ日付を示す。コントローラ１５２は、認証開始時点の日付の出力を受ける。説明する実施形態では、携帯情報端末１５０がＲＴＣ１６０を備えているが、他の実施形態では、ＲＴＣに代えて、他の通信Ｉ／Ｆを用いて外部の時刻提供システムから日付を取得するよう構成してもよし、利用者が、タッチパネル１６２などの入力装置を用いて日付の値を入力することで、日付を取得するよう構成してもよい。
【００３９】
記憶装置１５８は、当該携帯情報端末１５０の付帯者であり当該携帯情報端末１５０を用いて認証を行うために予め登録された利用者の認証情報を記憶する。記憶装置１５８は、不揮発性メモリ、ＳＤカード（登録商標）などのリムーバブルメディア、ＨＤＤやＳＳＤなどの補助記憶装置である。この認証情報は、利用者もしくは管理者が予め入力したものを用いてもよいし、認証開始前にその都度利用者が入力する態様としてもよい。タッチパネル１６２は、利用者の認証情報を入力するために用いられ、ディスプレイやボタンなどで構成される。
【００４０】
コントローラ１５２上には、図示しないＣＰＵ、ＲＡＭ、ＲＯＭなどのハードウェアが備えられており、ＣＰＵが、ＲＯＭや、外部の不揮発性メモリ、ＨＤＤ、ＳＳＤ、リムーバブルメディアなどの記憶装置に格納された制御プログラムを読み出し、ＲＡＭが提供する作業空間上に展開することにより、後述する各機能手段および各処理を実現する。
【００４１】
図３は、第１の実施形態による認証プリントシステム１００の機能ブロック図である。以下、図３を参照しながら、まず、プリンタ１１０の機能ブロックについて説明する。図３に示すように、プリンタ１１０の機能ブロック２１０は、認証開始部２１２と、生成用符号発生部２１４と、符号化部２１６と、直接送信部２１８と、認証符号対応表準備部２２０と、認証ＤＢ２２２と、日付保持部２２４と、ハッシュ関数２２６とを含み構成される。
【００４２】
認証開始部２１２は、認証処理を開始させる契機となるイベントを検知し、認証処理を開始させる契機検知手段である。認証開始部２１２は、説明する実施形態では、図２に示した近接検知センサ１１８と、近接検知センサ１１８からの出力を処理するプログラムとによって構成される。
【００４３】
生成用符号発生部２１４は、後述する一時認証符号を生成するための源符号となる認証

符号生成用符号を発生する発生手段である。生成用符号発生部２１４は、特に限定されるものではないが、例えばメルセンヌ・ツイスタ、キャリー付き乗算、ラグ付フィボナッチ法などの疑似乱数生成プログラムによってコントローラ１１２上に構成される。あるいは、ハードウェア乱数発生器によって構成されてもよい。

【００４４】

符号化部２１６は、生成用符号発生部２１４が発生した認証符号生成用符号に対し、誤り訂正の冗長性を付加し、かつ、クロック埋め込みを行う符号化を行う。符号化部２１６は、特に限定されるものではないが、例えば、リードソロモン符号、ＢＣＨ符号などの誤り訂正符号アルゴリズムと、８ｂ／１０ｂなどの変換アルゴリズムを組み合わせた送信符号生成プログラムによってコントローラ１１２上に構成される。あるいは、回路などのハードウェアによって構成されてもよい。リードソロモン符号では、例えば、符号語の構成として１シンボルに４ビット、４個のシンボルと２個の冗長シンボルで、１符号語で２４ビットの符合語を使用することができる。

【００４５】

直接送信部２１８は、生成用符号発生部２１４が発生させ、符号化部２１６で符号化された認証符号生成用符号を、電気信号に変換し、振動発生装置１１４を駆動して、振動パターンとして、認証を要求する携帯情報端末１５０に送信する手段である。直接送信部２１８は、特に限定されるものではないが、図２に示した振動発生装置１１４と、振動発生装置１１４を駆動する駆動回路やプログラムとを含み構成される。

【００４６】

プリンタ１１０は、認証符号生成用符号を振動パターンとして携帯情報端末１５０に対し送信すると、携帯情報端末１５０からのその応答を受信することになる。認証符号対応表準備部２２０は、これと並列して、携帯情報端末１５０からの応答に対し認証の成否判定を行うための情報を生成する認証符号生成手段である。より具体的には、認証符号対応表準備部２２０は、生成用符号発生部２１４が発生させた認証符号生成用符号に基づき、プリンタ１１０のすべての利用者各々に対応する一時認証符号を準備する。

【００４７】

認証ＤＢ２２２は、当該プリンタ１１０の正当な利用者を登録するデータベースであり、プリンタ１１０のすべての利用者各々の認証情報を登録する。認証情報は、利用者固有に割り当てられる情報であり、認証符号生成用符号とともに、利用者各々に対応する一時認証符号を生成するために用いられる。

【００４８】

日付保持部２２４は、ＲＴＣ１２２から認証開始時点（近接検知時点）の日付を取得し、同期情報を採番する認証側同期採番手段である。ここで、日付は、携帯情報端末１５０と同期するための同期情報であり、認証符号生成用符号および利用者の認証情報とともに一時認証符号を生成するために用いられる。日付情報を用いることで、一般的な情報処理装置や携帯情報端末において既存のＲＴＣを用いて同期を行うことが可能となり、コストを削減することができる。

【００４９】

ハッシュ関数２２６は、出力から入力への逆算困難性を有する関数であり、上記認証符号生成用符号と、日付情報と、利用者の認証情報とを入力として、固定長である一時認証符号を出力する。ハッシュ関数２２６は、携帯情報端末１５０側と共有されており、同一入力に対して同一出力が得られるように構成されている。ハッシュ関数２２６は、特に限定されるものではないが、ＳＨＡ（Secure Hash Algorithm）－１、ＳＨＡ－３、ＳＨＡ－２５６、ＭＤ－５（Message Digest Algorithm 5）などのハッシュ関数プログラムによってコントローラ１１２上に構成される。

【００５０】

上述した日付保持部２２４は、所定期間中、被認証側の同期採番手段と同一の値を出力しており、期間をまたいで値が変更されることにより、その期間内での一時認証符号から認証情報への逆算の困難性を担保している。なお、説明する実施形態では、同期情報は、

１日単位の値であり、１日単位で同一の値を出力するものとするが、一時認証符号の長さや、求められるセキュリティ強度に応じて、時や分までを含めたより詳細な単位としてもよいし、より大まかな単位とすることを妨げない。

【００５１】

本実施形態による認証符号対応表準備部２２０は、生成用符号発生部２１４が発生させた認証符号生成用符号と、日付保持部２２４が保持する日付情報と、認証ＤＢ２２２に登録された認証情報とをハッシュ関数２２６に入力し、すべての利用者各々の認証情報に対応する一時認証符号を準備する。準備された一時認証符号は、認証情報に対応づけた対応表として、例えば認証ＤＢ２２２などのデータベースに記憶される。認証符号対応表準備部２２０は、認証ＤＢ２２２から認証情報を取り出し、ハッシュ関数２２６を呼び出して計算結果を得るプログラムによってコントローラ１１２上に構成される。

【００５２】

プリンタ１１０から携帯情報端末１５０へ振動パターンが伝送されると、上記一時認証符号の対応表の準備と並列して、携帯情報端末１５０から応答が行われる。機能ブロック２１０は、さらに、この応答を処理するため、直接受信部２２８と、復号部２３０と、認証処理部２３２とを含み構成される。

【００５３】

直接受信部２２８は、振動検知センサ１１６を駆動して、携帯情報端末１５０から振動パターンを検知し、電気信号に変換する手段である。説明する実施形態では、直接受信部２２８は、図２に示した振動検知センサ１１６と、振動検知センサ１１６からの出力をデジタル信号に変換する回路やプログラムとを含み構成される。

【００５４】

復号部２３０は、受信した振動パターンの信号から、埋め込まれたクロックを再生し、符号を復号し、追加された冗長性に基づき符号の誤り検出および誤り訂正を行う。復号部２３０は、特に限定されるものではないが、携帯情報端末１５０側のアルゴリズムに対応して、例えば８ｂ／１０ｂ変換アルゴリズムと、リードソロモン誤り訂正符号アルゴリズムとを組み合わせた送信符号復号プログラムによってコントローラ１１２上に構成される。あるいは、回路などのハードウェアによって構成されてもよい。

【００５５】

認証処理部２３２は、直接受信部２２８で振動パターンとして受信し、復号部２３０で復号された被認証符号の少なくとも一部である符号と、上記認証符号対応表準備部２２０により準備されて認証ＤＢ２２２に格納された一時認証符号の対応表とを照合し、認証の成否を判定する認証手段である。説明する実施形態では、被認証符号の少なくとも一部である符号が、対応表の一時認証符号と一致している程度に基づいて、認証の成否が判定される。

【００５６】

より具体的には、認証処理部２３２は、携帯情報端末１５０からの被認証符号の全体の受信が完了する前に、対応表の一時認証符号のうち、被認証符号の一部の符号が所定基準以上で一致する符号が存在するか否かを判定し、所定基準以上で一致する認証符号が見つかった場合に認証が成功したものと判定する。一致する程度を基準に追加の符号が必要か否かを判定することができ、通信エラー率に応じて認証にかかる時間を調整することができるので、通信エラーが少ない場合は認証にかかる時間が短縮される。認証処理部２３２は、関係データベース管理システムなどの対応表検索プログラムによってコントローラ１１２上に構成される。

【００５７】

説明する実施形態では、図３に示すように、プリンタ１１０の機能ブロック２１０として、利用制御部２３４が含まれ、認証処理部２３２による認証結果に基づき当該プリンタ１１０の画像機能の利用が制御される。利用制御部２３４は、認証処理部２３２による認証結果を受けて、当該プリンタ１１０が操作者に対し操作パネル１２４上で提供するユーザ・インタフェースを制御して、認証した利用者に許可された画像機能へのアクセスを提

供する。
【００５８】
認証に失敗した操作者に対しては、操作パネル１２４上のディスプレイに、認証に失敗したメッセージを表示し、プリント、スキャンなどの画像機能に関する一切の操作を受けない。認証に成功した正当な利用者に対しては、操作パネル１２４上のディスプレイに、利用者の権限に応じた画像機能にアクセスするための操作画面を表示し、プリント、スキャン、コピー、ファクシミリなどの権限に応じた画像機能に対する操作を受ける。
【００５９】
以下、図３を参照しながら、携帯情報端末１５０の機能ブロックについて説明を続ける。携帯情報端末１５０の機能ブロック２５０は、直接受信部２５２と、復号部２５４と、被認証符号生成部２５６と、認証情報格納部２５８と、日付保持部２６０と、ハッシュ関数２６２と、符号化部２６４と、直接送信部２６６とを含み構成される。
【００６０】
直接受信部２５２は、振動検知センサ１５４を駆動して、プリンタ１１０からの、認証符号生成用符号を伝送する振動パターンを検知し、電気信号に変換する手段である。直接受信部２５２は、特に限定されるものではないが、図２に示した振動検知センサ１５４と、振動検知センサ１５４からの出力をデジタル信号に変換する回路やプログラムとを含み構成される。
【００６１】
復号部２５４は、直接受信部２５２で受信された振動パターンの電気信号から、埋め込まれたクロックを再生し、符号を復号し、送信側で追加された冗長性に基づき符号の誤り検出および誤り訂正を行う。復号部２５４は、特に限定されるものではないが、プリンタ１１０側に対応した送信符号復号プログラムによってコントローラ１５２上に構成される。あるいは、回路などのハードウェアによって構成されてもよい。
【００６２】
被認証符号生成部２５６は、直接受信部２５２がプリンタ１１０から振動パターンとして受信し、復号部２５４により復号された認証符号生成用符号に基づき、被認証符号を生成する。認証情報格納部２５８は、当該携帯情報端末１５０の付帯者である利用者に対して割り振られた認証情報を格納する格納手段である。認証情報は、予めシステム管理者や管理者からの配布を受けた付帯者が携帯情報端末１５０に予め入力するものとする。認証情報格納部２５８に格納された認証情報は、認証符号生成用符号とともに、被認証符号を生成するために用いられる。
【００６３】
日付保持部２６０は、ＲＴＣ１６０から認証開始時点（プリンタからの振動の検知時点）の日付を取得し、同期情報を採番する被認証側同期採番手段である。ここで、日付は、認証符号生成用符号および利用者の認証情報とともに被認証符号を生成するために用いられる。
【００６４】
ハッシュ関数２６２は、出力から入力への逆算困難性を有する関数であり、上記認証符号生成用符号と、日付情報と、利用者の認証情報とを入力として、固定長である被認証符号を出力する。ハッシュ関数２２６は、プリンタ１１０側と共有されており、同一入力に対して同一出力が得られるように構成されている。
【００６５】
本実施形態による被認証符号生成部２５６は、プリンタ１１０から受信した認証符号生成用符号と、日付保持部２６０が保持する日付情報と、認証情報格納部２５８に格納された認証情報とをハッシュ関数２６２に入力し、被認証符号を生成する。ハッシュ関数２６２は、プリンタ１１０との間で共有されているので、したがって、正しい認証情報を保持していれば、認証側で準備されている一時認証符号と同一の被認証符号が得られる。被認証符号生成部２５６は、プログラムによってコントローラ１５２上に構成される。
【００６６】

符号化部２６４は、被認証符号生成部２５６により生成された被認証符号に対し、誤り訂正の冗長性を付加し、かつ、クロック埋め込みを行う符号化を行う。符号化部２６４は、特に限定されるものではないが、プリンタ１１０側に対応した方式の送信符号生成プログラムによってコントローラ１５２上に構成される。あるいは、回路などのハードウェアによって構成されてもよい。

【００６７】

直接送信部２６６は、被認証符号生成部２５６が生成し、符号化部２６４で符号化された被認証符号を電気信号に変換し、振動発生装置１５６を駆動して、振動パターンとしてプリンタ１１０に送信する手段である。直接送信部２６６は、特に限定されるものではないが、図２に示した振動発生装置１５６と、振動発生装置１５６を駆動する駆動回路やプログラムとを含み構成される。

【００６８】

以上、第１の実施形態による認証プリントシステム１００におけるハードウェア構成および機能構成について説明した。以下、図４に示すフローチャート、図５および図６に示すデータ構造を参照しながら、第１の実施形態による認証プリントシステム１００で行われる利用者認証処理について、より詳細に説明する。

【００６９】

図４は、第１の実施形態による認証プリントシステム１００において、プリンタ１１０および携帯情報端末１５０間で実行される、利用者認証処理を示すフローチャートである。図４には、携帯情報端末１５０側で実行される処理（Ｓ１００～Ｓ１０８）と、プリンタ１１０側で実行される処理（Ｓ２００～Ｓ２１５）とが併せて示されている点に留意されたい。

【００７０】

図４に示す携帯情報端末１５０側の処理は、電源投入などに応答して、ステップＳ１００から開始され、ステップＳ１０１では、携帯情報端末１５０は、システム起動処理を実行する。プリンタ１１０側の処理も同様に、電源の投入などに応答して、ステップＳ２００から開始され、ステップＳ２０１では、プリンタ１１０は、システム起動処理を実行する。

【００７１】

プリンタ１１０が起動すると、ステップＳ２０２では、プリンタ１１０は、認証開始部２１２により、認証開始の契機となるイベントである近接物の検知を試みる。ステップＳ２０３では、プリンタ１１０は、近接物の有無を判定し、近接物を検知していない場合（ＮＯ）は、ステップＳ２０２へループさせて、物体の近接を待ち受ける。一方、ステップＳ２０３で、近接物があると判定された場合（ＹＥＳ）は、ステップＳ２０４へ処理を分岐させる。利用者が、携帯情報端末１５０をプリンタ１１０の近接検知センサ１１８に接触させると、近接物があると判定されることになる。

【００７２】

ステップＳ２０４では、プリンタ１１０は、生成用符号発生部２１４により、認証符号生成用符号を発生させる。図５（Ａ）は、第１の実施形態による認証プリントシステム１００で用いられる認証符号生成用符号のデータ構造を例示する。図５（Ａ）に示す認証符号生成用符号は、４バイトの乱数のバイト列として構成されている。

【００７３】

ステップＳ２０５では、プリンタ１１０は、符号化部２１６により、認証符号生成用符号に誤り訂正符号の付与とクロック埋め込み符号化を行い、振動パターンとして安定に送信可能な送信符号を生成する。図６（Ａ）は、第１の実施形態による認証プリントシステム１００において、プリンタ１１０が生成する送信符号のデータ構造を例示する。図６（Ａ）に示す送信符号は、図５（Ａ）に示すような４バイトの認証符号生成用符号に対し、１６ビットの誤り訂正符号を付与し、８ｂ／１０ｂ符号変換をした６０ビット（２語）のビットパターンとして構成することができる。

【００７４】

ステップＳ２０６では、プリンタ１１０は、直接送信部２１８により、振動発生装置１１４から送信符号が示す振動パターンを発生させる。

【００７５】

また、ステップＳ２０５およびステップＳ２０６と並列して、ステップＳ２０７では、プリンタ１１０は、認証ＤＢ２２２に登録されるすべての利用者の認証情報に対し、認証符号生成用符号と、日付情報と、それぞれの認証情報とをハッシュ関数２２６に入力して一時認証符号を生成し、認証情報と一時認証符号の対応表からなる一時認証符号対応表を生成する。

【００７６】

図５（Ｂ）は、第１の実施形態による認証プリントシステム１００で用いられる日付情報のデータ構造を例示する。図５（Ｂ）に示す日付情報は、ＡＳＣＩＩコードで記述された８バイトの日付の文字列（バイト列）として構成されている。

【００７７】

図５（Ｃ）は、第１の実施形態による認証プリントシステム１００で用いられる認証情報のデータ構造を例示する。図５（Ｄ）は、第１の実施形態による認証プリントシステム１００で用いられる認証ＤＢのデータ構造を例示する。図５（Ｃ）に示す認証情報および図５（Ｄ）に示す認証ＤＢで列挙される利用者数各々の認証情報は、認証情報が格納された可変長の文字列（バイト列）として構成されている。認証ＤＢは、利用者数分の認証情報の配列として構成されてもよいが、説明する実施形態では、ユーザ識別値に対応付けられている。

【００７８】

図５（Ｅ）は、第１の実施形態による認証プリントシステム１００で用いられる一時認証符号のデータ構造を例示する。図５（Ｅ）に示す一時認証符号は、第１の実施形態で用いるハッシュ関数が出力する固定長ビットのビットパターンとして構成されている。本実施形態で用いられるハッシュ関数は、固定長の認証符号生成用符号、固定長の日付情報、可変長の認証情報を結合した可変長のバイト列が入力され、固定長の一時認証符号を出力する。

【００７９】

図５（Ｆ）は、第１の実施形態による認証プリントシステム１００で用いられる一時認証符号の対応表のデータ構造を例示する。対応表は、認証ＤＢ２２２に登録されたすべての認証情報と、その認証情報から生成された一時認証符号とのテーブルとして構成され、説明する実施形態では、さらに対応するユーザ識別値が付されている。

【００８０】

ステップＳ２０６で振動パターンが出力された後、プリンタ１１０は、ステップＳ２０８およびステップＳ２０９で、相手からの応答の振動を待ち受ける。

【００８１】

一方で、携帯情報端末１５０が起動すると、ステップＳ１０２では、携帯情報端末１５０は、直接受信部２５２により、振動の検知を試みる。ステップＳ１０３では、携帯情報端末１５０は、振動の有無および復号の可または不可を判定し、振動が無いあるいは復号が不能である場合（ＮＯ）は、ステップＳ１０２へループさせて、復号可能な振動を待ち受ける。環境ノイズとしての振動など、振動パターンではない振動は、ここで排除される。

【００８２】

一方、ステップＳ１０３で、復号可能な振動が検知されたと判定された場合（ＹＥＳ）は、ステップＳ１０４へ処理が分岐される。ステップＳ１０４では、携帯情報端末１５０は、復号部２５４により、プリンタ１１０から送信された認証符号生成用符号を復号する。

【００８３】

ステップＳ１０５では、携帯情報端末１５０は、プリンタ１１０から受信した認証符号生成用符号と、振動検知時の日付情報と、認証情報格納部２５８に格納された利用者の認

証情報とを結合した可変長のバイト列をハッシュ関数に入力し、被認証符号を生成する。被認証符号は、図５（Ｅ）に示した一時認証符号と同じく、本実施形態で用いるハッシュ関数が出力する固定長ビットのビットパターンとして構成される。

【００８４】

ステップＳ１０６では、携帯情報端末１５０は、符号化部２６４により、被認証符号に誤り訂正符号の付与とクロック埋め込み符号化を行い、振動パターンとして安定して送信可能な送信符号を生成する。図６（Ｂ）は、第１の実施形態による認証プリントシステム１００において、携帯情報端末１５０が生成する送信符号のデータ構造を例示する。図６（Ｂ）に示す送信符号は、図５（Ｅ）に示す固定長ビットパターンに対し、誤り訂正符号を付与し、８ｂ／１０ｂ符号変換をした固定ビット長のビットパターンである。

【００８５】

例えば、一時認証符号が１６０ビット長とし、１シンボルに４ビット、４個のシンボルと２個の冗長シンボルで、１符号語で２４ビットの符合語のＲＳ符号を使用すると、１６０ビット長の一時認証符号に８０ビットの誤り訂正符号を付与し、８ｂ／１０ｂ符号変換をした３００ビット長のビットパターンとなる。

【００８６】

ステップＳ１０７では、携帯情報端末１５０は、直接送信部２６６により、振動発生装置１５６から送信符号が示す振動パターンを発生させ、ステップＳ１０８で待機状態に移行する。

【００８７】

一方、プリンタ１１０側では、上述したように、ステップＳ２０６で振動パターンを発生させた後、ステップＳ２０８およびステップＳ２０９で、相手からの応答の振動が待ち受けられる。ステップＳ２０８では、プリンタ１１０は、直接受信部２２８により振動の検知を試みる。ステップＳ２０９では、プリンタ１１０は、振動の有無および復号の可または不可を判定し、一定期間以上振動が無いあるいは復号できない場合（ＮＯ）は、ステップＳ２０２へ処理をループさせる。携帯情報端末１５０ではなく、他の物体が検知された場合などは、再び、近接検知から待ち受けが行われる。

【００８８】

一方、ステップＳ２０９で、振動パターンの一部を検知して復号し、復号可能な振動があると判定された場合（ＹＥＳ）は、ステップＳ２１０へ処理が分岐される。ステップＳ２１０では、プリンタ１１０は、復号部２３０により、被認証符号のうちのその時点で受信が完了した符号を復号し、部分被認証符号を準備する。

【００８９】

図６（Ｃ）は、第１の実施形態による認証プリントシステム１００において、プリンタ１１０が生成する部分被認証符号のデータ構造を例示する。図６（Ｃ）に示す部分被認証符号は、固定ビット長の被認証符号のうちの受信した部分を格納する格納ビット列と、被認証符号の各ビットの受信状態を示す受信状態ビット列の組として構成される。

【００９０】

受信状態ビット列は、上述した固定ビット長の被認証符号のビットパターンの受信状態を示しており、例示の実施形態では、２ビット表現されている。「００」は未受信を示し、「０１」は受信完了を示し、「１０」は受信したが誤りを検出したことを示し、「１１」は受信し誤りがあったが、誤り訂正符号で訂正されたことを示す。したがって、部分被認証符号は、上述した１６０ビット長の認証符号が用いられる場合は、１６０ビットの格納ビット列と、３２０ビットの受信状態ビット列との組として構成される。

【００９１】

復号開始時には、受信状態を示すビット列の各２ビットは、すべて「００」で初期化される。プリンタ１１０で送信符号を復号する際に、正常に受信できたビットは、格納ビット列に書き込み、受信状態ビット列の対応するビットの値を変更することで、現時点でどこまで受信されたか、またどのビットが受信したが誤りを検出したか、どのビットが誤りを訂正されたかが管理される。

【００９２】
ステップＳ２１１では、プリンタ１１０は、対応表から部分被認証符号ともっとも一致するものを検索する。この際、部分被認証符号のうち誤り訂正符号によって誤りが訂正された部分を検索に用いるようにしてもよい。受信完了「０１」または訂正して受信完了「１１」となったビットパターンを使用して、対応表に対して部分検索が行われ、一致する認証情報が検索され、一致度も求められる。
【００９３】
ステップＳ２１２では、プリンタ１１０は、部分被認証符号と、基準以上の一致度のものが対応表に存在するか否かを判定する。部分被認証符号の元となる一時認証符号は、ハッシュ関数により生成され、ほぼランダムなビットパターンを有する。このため、他の利用者と間違って認証するのを避けるためには、利用者数の二乗と比較して充分な長さのパターンが一致したことをもって認証を成功とみなしてもよい。例えば利用者数１０万人のシステムという特定の用途を考えると、一時認証符号を１６０ビットとした場合、４８ビット以上の一致があれば、すべての利用者が１回ずつ利用したとき、偶然に一致する確率が２万８千分の１（約２８１兆分の１０万×１０万）と充分に低いため、４８ビット以上を基準として用いることができる。なお、基準は、特定の用途における求められるセキュリティ強度に応じて決定すればよい。
【００９４】
ステップＳ２１２で、一致した長さが認証強度として充分ではなく基準以上の一致度を有するものが無いと判定された場合（ＮＯ）は、ステップＳ２１３へ処理が分岐される。ステップＳ２１３では、プリンタ１１０は、すべての被認証符号の受信が完了したか否かを判定する。ステップＳ２１３で、すべての被認証符号を受信していないと判定された場合（ＮＯ）は、ステップＳ２０９へ処理を分岐させて、追加の振動パターンを待ち受ける。これに対して、ステップＳ２１３で、一時認証符号の固定長の最後まで受信していたと判定された場合（ＹＥＳ）は、すべてを受信しても一致していないため、ステップＳ２１５で、認証失敗とみなす。これに対して、ステップＳ２１２で、すべての被認証符号を受信する前に、基準以上の一致度のものが存在すると判定された場合（ＹＥＳ）は、ステップＳ２１４で、プリンタ１１０は、認証成功とみなす。これにより、送信符号のすべてを受信していない段階でも、認証を行うことが可能となる。
【００９５】
上述した第１の実施形態による利用者認証処理においては、プリンタ１１０は、近接検知センサ１１８で携帯情報端末１５０の近接を検知し、利用者認証に用いる源符号を生成し、符号に基づき振動パターンを振動発生装置１１４から発生させる。この振動パターンは、携帯情報端末１５０の振動検知センサ１５４で検知される。携帯情報端末１５０は、検知した源符号をもとに被認証符号を生成し、符号に基づき振動パターンを振動発生装置１５６から発生させる。この振動パターンは、プリンタ１１０の振動検知センサ１１６で検知される。プリンタ１１０は、検知した認証符号の少なくとも一部の符号がいずれの利用者を示すものかを特定し、認証符号の検証をおこなうことで、利用者認証が行われる。
【００９６】
上述したような利用者認証においては、例えば、利用者が認証しようとした情報機器ではない他の機器で認証されてしまい、他の機器で当該利用者の権限で第三者が利用されてしまったりすることは望ましくない。また、利用者ではない第三者が当該利用者としてプリンタ１１０に認証されてしまったりすると望ましくない。さらに、振動パターンを用いる場合、携帯情報端末１５０に備えられているデバイスでは、振動パターンの生成、および検知の制御間隔や検知間隔を短くできないことから、低い通信速度を余儀なくされ、認証に時間がかかる可能性がある。
【００９７】
これに対して、上述した第１の実施形態によれば、プリンタ１１０と携帯情報端末１５０とは、信号が到達する範囲が限られた、好ましくは通信部位が互いに接触する範囲でしか信号が到達しない振動パターンを用いて情報が伝送される。したがって、携帯情報端末

１５０を用いてあるプリンタ１１０に認証しようとしたが、誤って隣の機器に認証してしまったりするような、機器側および端末側の送信者のなりすましが防止され、また、外部の攻撃者が意図した形での通信の内容の改ざんも防止される。

【００９８】

また仮に、通信内容が傍受されたとしても、一時認証符号は、一時的なものであり、またハッシュ関数は、逆算困難性を有するので、認証情報を復号することが困難である。さらに、特定の実施形態では、日付情報がハッシュ関数の入力として用いられるため、認証情報を復号することがより困難になる。適当な固定ビット長の一時認証符号を用いることにより、その日付情報が示す有効な期間のうちに、現実的な計算資源で、認証符号を再利用できる形で解読できないからである。

【００９９】

このように、上述した第１の実施形態による認証システムによれば、利用者に付帯される携帯情報端末１５０および認証を受け付けるプリンタ１１０間の通信路のセキュリティが向上され、さらに、該通信路を介して認証処理を成功裏に完了させるまでに必要となる時間を短縮することができる。

【０１００】

［第１の実施形態の変形例］

上述した第１の実施形態では、認証手続きを開始するたびに、プリンタ１１０側で発生させた認証符号生成用符号に基づき、すべての利用者の認証符号を準備していた。このような構成は、特に、小規模ないし中規模な組織において有効である。一方、上述した対応表の生成負荷は、典型的には、利用者数の二乗で増大するため、大規模な組織や、コンビニエンスストアなど公衆設置に設置する用途では、生成負荷が大きくなる可能性がある。以下、生成すべき対応表の範囲を制限し、対応表の生成負荷を軽減することができる変形例の実施形態について説明する。

【０１０１】

図７は、変形例の実施形態による認証プリントシステム１００で用いられる（Ａ）認証ＤＢおよび（Ｂ）一時認証符号の対応表のデータ構造を例示する。図７（Ａ）に示す認証ＤＢは、第１の実施形態と同様に、認証ＤＢ２２２に登録されたすべての認証情報を含む。一方、変形例の実施形態においては、認証情報は、利用者ＩＤの後ろにパスワードを付加したような形で構成されている。

【０１０２】

変形例の実施形態では、携帯情報端末１５０は、プリンタ１１０から受信した認証符号生成用符号に基づいて、まず探索基準値を生成する。そして、携帯情報端末１５０は、この生成した探索基準値と、認証情報格納部２５８に格納された認証情報に含まれる利用者ＩＤとの比較結果を生成し、生成した被認証符号の前に比較結果を付して、プリンタ１１０に振動パターンとして送信する。ここで、比較結果は、探索基準値に対して、認証情報に含まれる利用者ＩＤが大きい値か小さい値かを判定した結果である。

【０１０３】

一方、プリンタ１１０では、生成用符号発生部２１４が発生させた認証符号生成用符号に基づき、同様に、同じ方法で探索基準値を生成する。変形例の実施形態では、認証符号生成用符号が生成された直後に、図４に示したステップＳ２０７で対応表の生成を開始しない。その代り、被認証符号の受信中、比較結果に相当する符号の受信を完了させた段階で、比較結果を抽出し、比較結果に基づき限定された範囲の利用者ＩＤの認証情報のみを対象として、一時認証符号の対応表を生成する。図７（Ｂ）に示す例では、ユーザＩＤの先頭が「７」未満の認証情報に対してのみ対応表が生成されている。

【０１０４】

探索基準値は、携帯情報端末１５０側と同一の方法で生成されるため、生成された認証符号生成用符号に対して携帯情報端末１５０およびプリンタ１１０では同一の値が出力される。このため、プリンタ１１０側では、比較結果に基づき、携帯情報端末１５０側の利用者の認証情報が含まれるグループの認証情報を特定することができる。対応表が生成さ

れた以降は、第１の実施形態と同様である。

【０１０５】

上記変形例の実施形態によれば、限定された範囲の認証情報のみを対象として一時認証符号の対応表が生成されるため対応表の生成負荷を軽減し、認証時間も短縮することができる。特に利用者数が膨大であった場合に好適に適用することができる。また、探索基準値を認証符号生成用符号に基づいて生成することで、探索基準値を固定値とした場合に比較して、ユーザＩＤに偏りがあった場合でも、効率的に一時認証符号の対応表を生成する範囲を制限することができる。なお、説明する実施形態では、１つの探索基準値を用いるものとしたが、ユーザＩＤの最初の２文字を対象とするなど、複数の探索基準値および複数の比較結果を用いることにより、さらに、対応表の生成範囲を制限してもよい。

【０１０６】

［第２の実施形態］

上述した第１の実施形態では、利用者に付帯される携帯情報端末１５０と、認証を受け付け、認証処理を行い、認証結果に基づき動作が制御されるプリンタ１１０とを含む認証プリントシステム１００を用いて説明した。以下、利用者に付帯される携帯情報端末１５０と、認証を受け付けるリーダ１４０と、認証結果に基づき動作が制御される複数のプリンタ１１０と、認証処理を行う認証サーバ１７０とを含み構成される、第２の実施形態による認証プリントシステム１００を一例として説明する。

【０１０７】

図８は、第２の実施形態による認証プリントシステム１００の概略構成を示す図である。図８に示すように、第２の実施形態による認証プリントシステム１００は、認証によって利用者が制限されている複数のプリンタ１１０ａ～１１０ｚと、各々のプリンタ１１０に設けられるリーダ１４０ａ～１３０ｚと、ネットワーク１０２を介して複数のプリンタ１１０ａ～１１０ｚに接続される認証サーバ１７０と、利用者が付帯する携帯情報端末１５０とを含み構成される。

【０１０８】

第２の実施形態による認証プリントシステム１００においては、携帯情報端末１５０とのインタフェースは、プリンタ毎に設けられ、対応するプリンタ１１０と通信するリーダ１４０であり、リーダ１４０が認証を受け付ける認証受付装置である。プリンタ１１０のリーダ１４０に設けられた積載台上に携帯情報端末１５０が置かれることで、互いの通信部位同士が接触し、リーダ１４０および携帯情報端末１５０間の通信が可能となる。リーダ１４０および携帯情報端末１５０間では、機械的な振動パターンによって認証のための情報が交換される。リーダ１４０とプリンタ１１０との間は、例えばＵＳＢなどにより接続され、ネットワーク１０２を介してプリンタ１１０と認証サーバ１７０とが通信し、プリンタ１１０への利用者認証が行われる。

【０１０９】

図９は、第２の実施形態による認証プリントシステム１００の機能ブロック図である。以下、図９を参照しながら、プリンタ１１０、リーダ１４０、携帯情報端末１５０および認証サーバ１７０の機能ブロック２１０，２４０，２５０，２７０について説明する。

【０１１０】

図９に示すように、第２の実施形態によるプリンタ１１０の機能ブロック２１０は、利用制御部２３４を含み構成される。リーダ１４０の機能ブロック２４０は、認証開始部２４１と、符号化部２４２と、直接送信部２４３と、直接受信部２４４と、復号部２４５とを含み構成される。認証サーバ１７０の機能ブロック２７０は、生成用符号発生部２７２と、認証符号対応表準備部２７４と、認証ＤＢ２７６と、日付保持部２７８と、ハッシュ関数２８０と、認証処理部２８２とを含み構成される。携帯情報端末１５０の機能ブロック２５０は、第１の実施形態と同一である。

【０１１１】

第２の実施形態による認証サーバ１７０上の生成用符号発生部２７２は、予め１以上の認証符号生成用符号を生成する。認証符号対応表準備部２７４は、生成用符号発生部２７

２により予め発生された１以上の認証符号生成用符号各々について、プリンタ１１０のすべての利用者各々に対応する一時認証符号の対応表を予め準備する。

【０１１２】

認証サーバ１７０上の生成用符号発生部２７２は、リーダ１４０上の認証開始部２４１からの認証開始の指示に応答して、リーダ１４０上の符号化部２４２に対し、今回の認証で用いる認証符号生成用符号を送信する。リーダ１４０と、認証サーバ１７０との間の通信は、通信Ｉ／Ｆによりプリンタ１１０を経由して行われる。

【０１１３】

リーダ１４０の符号化部２４２は、認証サーバ１７０の生成用符号発生部２７２から受信した認証符号生成用符号を符号化する。直接送信部２４３は、符号化部２４２で符号化された認証符号生成用符号を電気信号に変換し、振動発生装置を駆動して、振動パターンとして携帯情報端末１５０に送信する。

【０１１４】

リーダ１４０の直接受信部２４４は、振動検知センサを駆動して、携帯情報端末１５０からの振動パターンを検知し、電気信号に変換する。復号部２４５は、受信した振動パターンの信号から、埋め込まれたクロックを再生し、符号を復号し、追加された冗長性に基づき符号の誤り検出および誤り訂正を行い、認証サーバ１７０上の認証処理部２８２に随時送信する。

【０１１５】

図１０は、第２の実施形態による認証プリントシステム１００で用いられる一時認証符号の対応表のデータ構造を例示する。第２の実施形態による認証符号対応表準備部２７４が準備する対応表は、図１０に示すように、認証ＤＢ２２２に登録されたすべての認証情報と、その認証情報から生成された一時認証符号と、その有効無効を保持するフラグとを含むテーブルとして構成される。また、対応表は、発生された１以上の認証符号生成用符号各々とペアで管理される。

【０１１６】

認証処理部２８２は、リーダ１４０の直接受信部２４４で振動パターンとして受信し、復号部２４５で復号され、通信Ｉ／Ｆを介して随時送信される被認証符号の少なくとも一部である符号と、上記認証符号対応表準備部２７４により準備されて認証ＤＢ２７６に格納された、対応する一時認証符号の対応表とを照合し、認証の成否を判定する。第２の実施形態でも同様に、随時受信する被認証符号の少なくとも一部である符号が、対応表の一時認証符号と一致している程度に基づいて、認証の成否が判定される。

【０１１７】

第２の実施形態による認証処理部２８２は、認証に成功すると、送信した認証符号生成用符号に対応する対応表において、一致した認証符号に対するフラグを「ｔｒｕｅ」に設定し、当該認証符号を無効化する。無効にされた認証符号は、もう使用することができず、例えば、携帯情報端末１５０が送信する一時認証符号を傍受した攻撃者が、同一の一時認証符号を送信しても、仮に同じ認証符号生成用符号が送信されたとしても、認証に通ることはない。一方、他のプリンタ（例えば、最初の利用者が認証を求めたプリンタと離間するプリンタ）に対し、次に認証を求めてきた別の携帯情報端末に対する認証においては、同じ認証符号生成用符号を送信してもよく、その際に対応表を再利用することができる。

【０１１８】

第２の実施形態による利用制御部２３４は、認証サーバ１７０の認証処理部２８２による認証結果を受信し、当該プリンタ１１０が操作者に対し操作パネル１２４上で提供するユーザ・インタフェースを制御して、認証した利用者に許可された画像機能へのアクセスを提供する。

【０１１９】

なお、同じプリンタ１１０から連続して同一の認証符号生成用符号を送信すると、同じ利用者が２回目の認証をしようとしても既に一時認証符号が無効化されているため、正規

の認証情報でも認証に失敗してしまい、再度の手続きを要求することとなり、利便性が低下する可能性がある。そこで、好適な実施形態では、同一のプリンタからは、連続して同じ認証符号生成用符号を送信せず、一方で、各プリンタについて管理される位置情報に基づき、同じ利用者が利用することがまずない、一定基準以上の距離を有するプリンタからは、当該利用者について一度送信したものと同一の認証符号生成用符号を送信し、対応表を再利用するよう構成することができる。これにより、対応表の再利用を可能とするとともに、同じ利用者が２回目の認証をしようとする際の利便性の低下を防止することができる。

【０１２０】

上述した第２の実施形態によれば、複数のプリンタ１１０間で認証サーバ１７０が共有され、対応表が再利用されるため、全体としての対応表の生成負荷を低減することができる。第２の実施形態によれば、複数のプリンタ１１０の認証処理を１つの認証サーバに集約することで、規模の増大に伴う対応表の生成負荷増加および認証を要する時間に与える影響を、複数のプリンタ１１０間で対応表を再利用することで緩和することができる。また、複数のプリンタの利用者情報が共有されるので、管理性や利便性が向上する。

【０１２１】

以上説明した実施形態によれば、利用者に付帯される付帯装置と、該付帯装置を用いた認証を受け付ける認証受付装置との間の認証のための通信路のセキュリティを向上することができる、認証システムおよび認証方法を提供するが可能となる。

【０１２２】

なお、上述までの実施形態では、伝送されるパターンとして機械的な振動の時間的なパターンを一例として説明した。しかしながら、伝送されるパターンとしては時間的なパターンに限定されず、複数のチャネルを使用した空間的な成分が含まれてもよい。

【０１２３】

なお、上記機能部は、アセンブラ、Ｃ、Ｃ＋＋、Ｃ＃、Ｊａｖａ（登録商標）などのレガシープログラミング言語やオブジェクト指向プログラミング言語などで記述されたコンピュータ実行可能なプログラムにより実現でき、ＲＯＭ、ＥＥＰＲＯＭ、ＥＰＲＯＭ、フラッシュメモリ、フレキシブルディスク、ＣＤ－ＲＯＭ、ＣＤ－ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ブルーレイディスク、ＳＤカード、ＭＯなど装置可読な記録媒体に格納して、あるいは電気通信回線を通じて頒布することができる。

【０１２４】

これまで本発明の実施形態について説明してきたが、本発明の実施形態は上述した実施形態に限定されるものではなく、他の実施形態、追加、変更、削除など、当業者が想到することができる範囲内で変更することができ、いずれの態様においても本発明の作用・効果を奏する限り、本発明の範囲に含まれるものである。

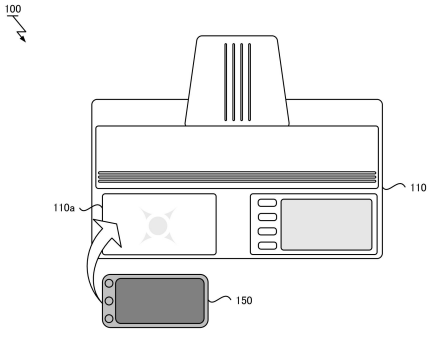
【符号の説明】

【０１２５】

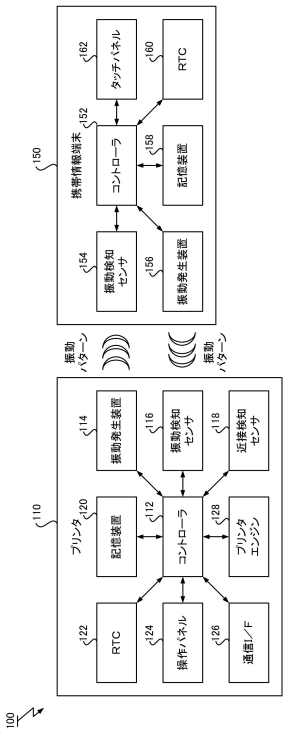
１００…認証プリントシステム、１１０…プリンタ、１１０…積載台、１１２…コントローラ、１１４…振動発生装置、１１６…振動検知センサ、１１８…近接検知センサ、１２０…記憶装置、１２２…ＲＴＣ、１２４…操作パネル、１２６…通信インタフェース、１２６…通信Ｉ／Ｆ、１２８…プリンタ・エンジン、１４０…リーダ、１５０…携帯情報端末、１５２…コントローラ、１５４…振動検知センサ、１５６…振動発生装置、１５８…記憶装置、１６０…ＲＴＣ、１６２…タッチパネル、１７０…認証サーバ、２１０，２４０，２５０，２７０…機能ブロック、２１２，２４１…認証開始部、２１４，２７２…生成用符号発生、２１６，２４２…符号化部、２１８，２４３…直接送信部、２２０，２７４…認証符号対応表準備部、２２２，２７８…認証ＤＢ、２２４，２７６…日付保持部、２２６，２８０…ハッシュ関数、２２８，２４４…直接受信部、２３０，２４５…復号部、２３２，２８２…認証処理部、２３４…利用制御部、２５０…機能ブロック、２５２…直接受信部、２５４…復号部、２５６…被認証符号生成部、２５８…認証情報格納部、２６０…日付保持部、２６２…ハッシュ関数、２６４…符号化部、２６６…直接送信部

【先行技術文献】
【特許文献】
【０１２６】
【特許文献１】特開２００７－２４９４２５号公報
【特許文献２】特開２００７－２２８５５４号公報

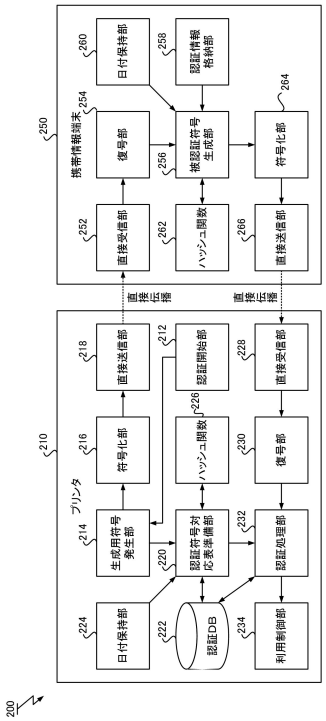
【図１】



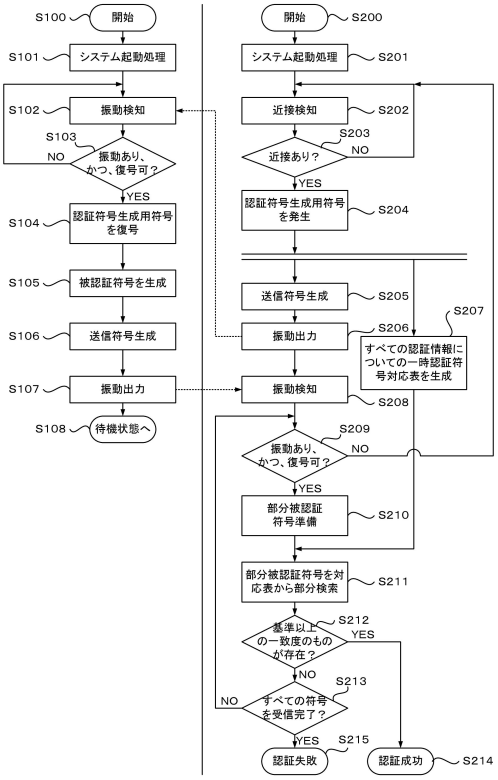
【図２】



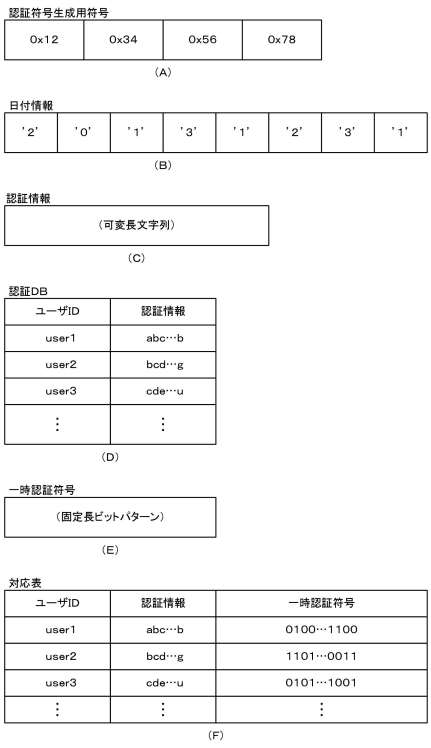
【図３】


250
携帯情報端末
260
日付保持部
258
認証情報格納部
254
復号部
256
被認証符号生成部
264
符号化部
252
直接受信部
262
ハッシュ関数
266
直接送信部
直接伝搬
直接伝搬
210
プリンタ
218
直接送信部
212
認証開始部
228
直接受信部
226
ハッシュ関数
216
符号化部
230
復号部
214
生成用符号発生部
220
認証符号対応表準備部
232
認証処理部
224
日付保持部
222
認証DB
234
利用制御部
200

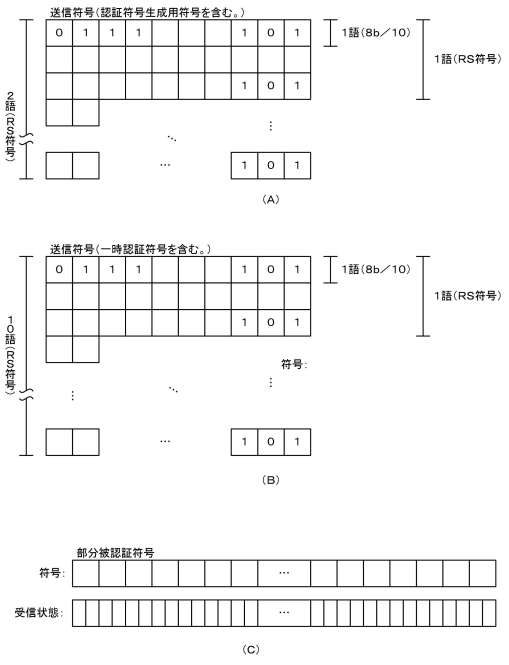
【図４】


S100
開始
S101
システム起動処理
S102
振動検知
S103
振動あり、かつ、復号可？
NO
YES
S104
認証符号生成用符号を復号
S105
被認証符号を生成
S106
送信符号生成
S107
振動出力
S108
待機状態へ
S200
開始
S201
システム起動処理
S202
近接検知
S203
近接あり？
NO
YES
S204
認証符号生成用符号を発生
S205
送信符号生成
S206
振動出力
S207
すべての認証情報についての一時認証符号対応表を生成
S208
振動検知
S209
振動あり、かつ、復号可？
NO
YES
S210
部分被認証符号準備
S211
部分被認証符号を対応表から部分検索
S212
基準以上の一致度のものが存在？
YES
NO
S213
すべての符号を受信完了？
NO
YES
S214
認証成功
S215
認証失敗

【図５】


認証符号生成用符号
0x12
0x34
0x56
0x78
(A)
日付情報
'2'
'0'
'1'
'3'
'1'
'2'
'3'
'1'
(B)
認証情報
（可変長文字列）
(C)
認証DB
ユーザID
認証情報
user1
abc…b
user2
bcd…g
user3
cde…u
(D)
一時認証符号
（固定長ビットパターン）
(E)
対応表
ユーザID
認証情報
一時認証符号
user1
abc…b
0100…1100
user2
bcd…g
1101…0011
user3
cde…u
0101…1001
(F)

【図６】


送信符号（認証符号生成用符号を含む。）
1語（8b／10）
1語（RS符号）
n語（n≧2）
(A)
送信符号（一時認証符号を含む。）
1語（8b／10）
1語（RS符号）
n語（n≧2）
符号:
(B)
部分被認証符号
符号:
受信状態:
(C)

【図７】

認証DB

認証情報
1001abc…b
1002bcd…g
⋮
7003cde…u
7004cde…u
⋮

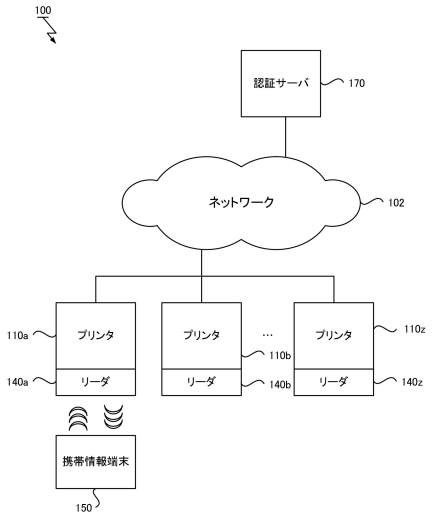
（A）

対応表

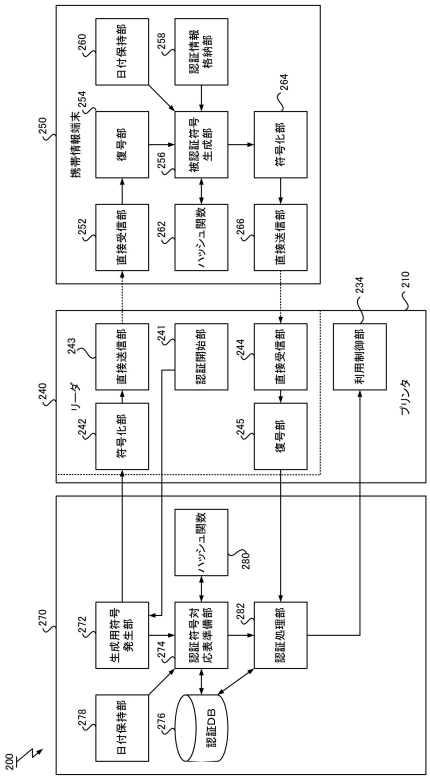
認証情報	一時認証符号
0001abc…b	0100…1100
0002bcd…g	1101…0011
0003cde…u	0101…1001
⋮	⋮
6999ghj…u	0101…1101

（B）

【図８】



【図９】



【図１０】

対応表

一時認証符号	固定長ビットパターン			
ユーザID	認証情報	一時認証符号	無効フラグ
user1	abc…b	0100…1100	False
user2	bcd…g	1101…0011	False
user3	cde…u	0101…1001	True
…	…	…	…

フロントページの続き

(56)参考文献 特開２００９－２４５１２２（ＪＰ，Ａ）
特開２００６－０７２７７８（ＪＰ，Ａ）
特開２０１２－１６６４２８（ＪＰ，Ａ）
再公表特許第２０１１／０９２８２９（ＪＰ，Ａ１）
特開２００６－２７０８０８（ＪＰ，Ａ）
特開２００２－２９７５４９（ＪＰ，Ａ）
特開２００２－２５９９８１（ＪＰ，Ａ）
特開２００５－１６７４１２（ＪＰ，Ａ）
特開２０１２－０６０５４２（ＪＰ，Ａ）
米国特許出願公開第２０１０／０２１８２４９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３１
Ｇ０６Ｆ ３／１２
Ｈ０４Ｗ １２／０６
Ｈ０４Ｗ ８４／１０