(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2019-102902
(P2019-102902A)
(43)公開日　令和1年6月24日(2019.6.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	2E250
E05B 49/00	(2006.01)	H04L	9/00	601E	5J104
G06F 21/32	(2013.01)	E05B	49/00	J	
H04L 9/32	(2006.01)	E05B	49/00	T	
		G06F	21/32		

審査請求 未請求　請求項の数 15　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2017-229778 (P2017-229778)
(22)出願日　平成29年11月30日 (2017.11.30)

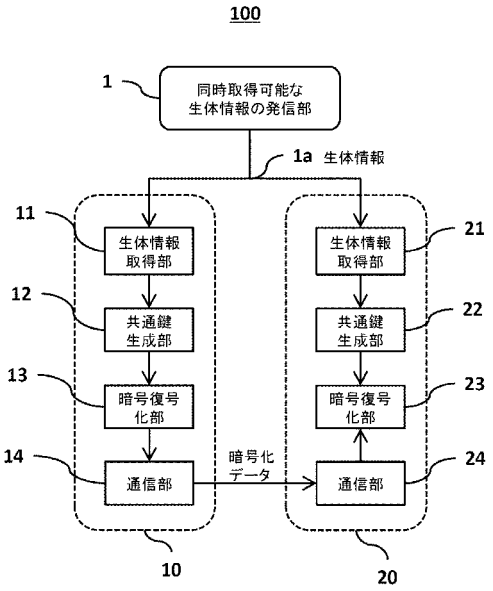
(71)出願人　302062931
ルネサスエレクトロニクス株式会社
東京都江東区豊洲三丁目２番２４号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　富澤　智
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内
(72)発明者　林　喜宏
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内
(72)発明者　丸山　勇一
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内

最終頁に続く

(54)【発明の名称】通信システム

(57)【要約】　（修正有）
【課題】複数の通信装置で同時取得が可能な生体情報を使って共通の暗号鍵を生成するセキュアな通信システムを提供する。
【解決手段】通信システム１００は、２つ以上の離れた通信装置１０、２０を有する。通信装置１０、２０は、同時取得が可能な生体情報１ａの特徴要素に基づいて同一の共通鍵を生成し、共通鍵を使った暗号化や復号化を行う。通信装置１０、２０はそれぞれ、生体情報１ａの特徴要素を取得する生体情報取得部１１、２１と、共通鍵を生成する共通鍵生成部１２、２２と、共通鍵によって送信情報を暗号化する、または受信情報を復号化する暗号復号部１３、２３と、送信情報を受信、または受信情報を送信する通信部１４、２４と、を備える。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
２つ以上の離れた通信装置が、同時取得が可能な生体情報の特徴要素に基づいて同一の共通鍵を生成し、前記共通鍵を使った暗号化や復号化を行う通信システムであって、
前記通信装置は、
前記生体情報の特徴要素を取得する生体情報取得部と、
前記共通鍵を生成する共通鍵生成部と、
前記共通鍵によって送信情報を暗号化する、または受信情報を復号化する暗号復号部と、
前記送信情報を受信、または前記受信情報を送信する通信部と、を備える、
通信システム。
【請求項２】
請求項１の通信システムにおいて、
前記送信情報は、ＩＤ情報を含む、通信システム。
【請求項３】
請求項１の通信システムにおいて、
前記生体情報の特徴要素は、声帯振動の周波数である、通信システム。
【請求項４】
請求項１の通信システムにおいて、
前記生体情報の特徴要素は、声紋である、通信システム。
【請求項５】
請求項４の通信システムにおいて、
前記送信情報は、ＩＤ情報であり、
前記ＩＤ情報と前記声紋の認証結果とによる２段階認証を行う、通信システム。
【請求項６】
ＩＤ情報送信端末装置と、
１または複数のＩＤ情報受信端末装置と、を有し、
前記ＩＤ情報送信端末装置および前記１または複数のＩＤ情報受信端末装置とは、同時取得が可能な生体情報の特徴要素に基づいて同一の共通鍵を生成し、
前記ＩＤ情報送信端末装置は、
前記生体情報の特徴要素を取得する生体情報取得部と、
前記共通鍵を生成する共通鍵生成部と、
前記共通鍵によってＩＤ情報を暗号化する暗号復号部と、
前記暗号化されたＩＤ情報を送信する通信部と、を備え、
前記１または複数のＩＤ情報受信端末装置は、
前記生体情報の特徴要素を取得する生体情報取得部と、
前記共通鍵を生成する共通鍵生成部と、
前記暗号化されたＩＤ情報を受信する通信部と、
前記共通鍵によって前記暗号化されたＩＤ情報を復号化する暗号復号部と、
を備える、
通信システム。
【請求項７】
請求項６の通信システムにおいて、
前記ＩＤ情報送信端末装置は、無線キーデバイスであり、
前記１または複数のＩＤ情報受信端末装置は、施錠／開錠デバイスである、通信システム。
【請求項８】
請求項６の通信システムにおいて、
前記同時取得が可能な生体情報は、同時に、前記ＩＤ情報送信端末装置の前記生体情報取得部と、前記１または複数のＩＤ情報受信端末装置の前記生体情報取得部とに取得され

る、通信システム。
【請求項９】
請求項８の通信システムにおいて、
前記生体情報の特徴要素は、声帯振動の周波数である、通信システム。
【請求項１０】
請求項８の通信システムにおいて、
前記生体情報の特徴要素は、声紋である、通信システム。
【請求項１１】
ＩＤ情報送信端末装置と、
ＩＤ情報受信端末装置と、を有し、
前記ＩＤ情報送信端末装置および前記ＩＤ情報受信端末装置とは、同時取得が可能な特徴要素に基づいて同一の共通鍵を生成し、
前記ＩＤ情報送信端末装置は、
前記特徴要素を取得する特徴取得部と、
前記共通鍵を生成する共通鍵生成部と、
前記共通鍵によってＩＤ情報を暗号化する暗号復号部と、
前記暗号化されたＩＤ情報を送信する通信部と、を備え、
前記ＩＤ情報受信端末装置は、
前記特徴要素を取得する特徴取得部と、
前記共通鍵を生成する共通鍵生成部と、
前記暗号化されたＩＤ情報を受信する通信部と、
前記共通鍵によって前記暗号化されたＩＤ情報を復号化する暗号復号部と、を備える、
通信システム。
【請求項１２】
請求項１１の通信システムにおいて、
前記同時取得が可能な特徴要素は、生体情報の特徴要素であり、
前記生体情報の特徴要素は、声帯振動の周波数、または、声紋であり、
前記同時取得が可能な生体情報は、同時に、前記ＩＤ情報送信端末装置の前記特徴取得部と、前記ＩＤ情報受信端末装置の前記特徴取得部とに取得される、通信システム。
【請求項１３】
請求項１２の通信システムにおいて、
前記ＩＤ情報送信端末装置は、無線キーデバイスであり、
前記ＩＤ情報受信端末装置は、施錠／開錠デバイスである、通信システム。
【請求項１４】
請求項１２の通信システムにおいて、
前記共通鍵は、前記声帯振動の周波数の複数より生成される、通信システム。
【請求項１５】
請求項１１の通信システムにおいて、
前記同時取得が可能な特徴要素は、楽器の音階における音の基本周波数、または、可聴周波数帯域以外の音である、通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は通信システムに関し、２つ以上の通信端末装置を備える通信システムに適用可能である。
【背景技術】
【０００２】
特開２０１６－２１１１５７号公報（特許文献１）は、「複数の携帯情報端末と無線通信を行う情報処理装置であって、データの入出力を行う入出力部と、車両の車両ＩＤと該

車両の鍵の鍵ＩＤとに基づく認証が成功し、かつ、複数の携帯情報端末のうち車両に最も近い場所に存在する携帯情報端末に対してワンタイムパスワードが送信された後、該ワンタイムパスワードが発声されたことが検出された場合に、車両のドアを解錠する制御信号を入出力部に出力させる制御部と、を備える。」という技術を提案している。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１６－２１１１５７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、特開２０１６－２１１１５７号公報（特許文献１）では、スマートキーが発信する解除キー(ＩＤ情報)の暗号化について言及されていない。したがって、解除キーの発信時に、第三者によって解除キーの内容を盗み読まれると、２段階認証の１つが容易に看破されることが危惧される。
【０００５】
本開示の課題は、複数の通信装置で同時取得が可能な生体情報を使って共通の暗号鍵を生成するセキュアな通信システムを提供することにある。
【０００６】
その他の課題と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。
【課題を解決するための手段】
【０００７】
本開示のうち代表的なものの概要を簡単に説明すれば下記の通りである。
【０００８】
すなわち、通信システムは、２つ以上の離れた通信装置を有する。前記通信装置は、同時取得が可能な生体情報の特徴要素に基づいて同一の共通鍵を生成し、前記共通鍵を使った暗号化や復号化を行う。前記通信装置は、前記生体情報の特徴要素を取得する生体情報取得部と、前記共通鍵を生成する共通鍵生成部と、前記共通鍵によって送信情報を暗号化する、または受信情報を復号化する暗号復号部と、前記送信情報を受信、または前記受信情報を送信する通信部と、を備える。
【発明の効果】
【０００９】
上記通信システムによれば、複数の通信装置で同時取得が可能な生体情報を使って共通の暗号鍵を生成するセキュアな通信を行うことが可能である。
【図面の簡単な説明】
【００１０】
【図１】実施形態に係る通信システムを示す図である。
【図２】実施例１に係る通信システムを示す図である。
【図３】実施例１に係るフローチャートを示す図である。
【図４】「あ」と発音したときの時間波形を示す図である。
【図５】図４の波形を、横軸を時間、縦軸を周波数成分で表したサウンドスペクトログラムを示す図である。
【図６】図５の時間波形を、パワースペクトルで表した結果を示す図である。
【図７】図５の時間波形を、ケプストラム分析した結果を示す図である。
【図８】音声源と集音するマイクの距離が変わった場合の基本周波数とピークが現れるケフレンシ値との関係を説明する図である。
【図９】高音を意識して”あ”と発音した場合と、低音を意識して”あ”と発音した場合の基本周波数とピークのケフレンシ値との関係を示す図である。
【図１０】実施例２に係る通信システムを説明するための図である。

【図１１】実施例２に係るフローチャートを示す図である。
【図１２】実施例３に係る２段階認証を行う通信システムを説明するための図である。
【図１３】実施例４に係る通信システムを説明するための図である。
【発明を実施するための形態】
【００１１】
以下、実施形態、および実施例について、図面を用いて説明する。ただし、以下の説明において、同一構成要素には同一符号を付し繰り返しの説明を省略することがある。なお、図面は説明をより明確にするため、実際の態様に比べ、模式的に表される場合があるが、あくまで一例であって、本発明の解釈を限定するものではない。
【００１２】
＜実施形態＞
図１は、実施形態に係る通信システムを説明するための図である。
【００１３】
通信システム１００は、２つ以上の離れた通信装置として、通信装置（ＩＤ情報送信端末装置）１０と通信装置（ＩＤ情報受信端末装置）２０と、を有する。通信装置１０と通信装置２０とは、同時取得可能な生体情報の発信部１から生体情報１ａの特徴要素を取得し、取得した生体情報１ａの特徴要素に基づいて同一の共通鍵を生成し、生成した共通鍵を使った暗号化や復号化を行う。
【００１４】
通信装置１０は、同時取得可能な生体情報の発信部１からの生体情報１ａの特徴要素を取得する生体情報取得部（特徴取得部）１１と、取得した生体情報１ａの特徴要素に基づいて共通鍵を生成する共通鍵生成部１２と、を有する。通信装置１０は、また、共通鍵生成部１２により生成された共通鍵を用いてＩＤ情報などの送信情報を暗号化する暗号復号部１３と、暗号化された送信情報（データ）を無線信号として送信する通信部１４と、を有する。
【００１５】
通信装置２０は、同時取得可能な生体情報の発信部１からの生体情報１ａの特徴要素を取得する生体情報取得部（特徴取得部）２１と、取得した生体情報１ａの特徴要素に基づいて共通鍵を生成する共通鍵生成部２２と、を有する。通信装置２０は、また、共通鍵生成部２２により生成された共通鍵を用いて受信情報の復号化を行う暗号復号部２３と、通信装置１０の通信部１４から送信された暗号化送信情報を無線信号として受信し、暗号復号部２３へ供給する通信部２４と、を有する。
【００１６】
ここで、生体情報１ａの特徴要素は、例えば、正規のユーザーの音声の声帯振動周波数、あるいは、声紋等を採用することが可能である。
【００１７】
実施形態によれば、同時取得可能な生体情報１ａの特徴要素（例えば、音声の声帯振動周波数、声紋等）を、通信を行う２つ以上の通信装置１０、２０が、例えば、同時に取得し、その特徴量に基づいた共通鍵（暗号鍵）をそれぞれの通信装置１０、２０で生成することかできる。
【００１８】
通信装置１０、２０間で通信する際は、生成した共通鍵を使って暗号化したセキュアな通信を行う。それぞれの通信装置１０、２０が共通鍵（暗号鍵）を持つ過程で、共通鍵を共有するためのセキュアな通信ネットワークを必要としないため、導入コスト、管理コストの削減が期待できる。
【００１９】
また、ユーザーによって生体情報の特徴を意図的に変更することも可能であり、共通鍵を容易に変更できる。このため、悪意のある第三者による共通鍵の推測が困難となり、耐タンパ性も期待できる。
【実施例１】

【００２０】
図２は、実施例１に係る通信システムを説明するための図である。
【００２１】
実施例１に係る通信システム１００ａは、通信装置（ＩＤ情報送信端末装置）１０ａを無線キーデバイスとし、通信装置（ＩＤ情報受信端末装置）２０ａを施錠/開錠デバイスとした場合の通信システムの一例である。通信システム１００ａにおいて、無線キーデバイス１０ａから無線信号(例えば、ビーコン（Ｂｅａｃｏｎ）信号)を施錠/開錠デバイス２０ａに送信し、施錠/開錠デバイス２０ａが受信した無線信号が所望の信号（ＩＤ）と一致すれば、施錠/開錠デバイス２０ａが鍵を施錠/開錠する。
【００２２】
実施例１の具体的な用途としては、以下が考えられる。
１）部屋の扉、ロッカー、倉庫、保管庫、 南京錠、アタッシュケースなどの鍵の施錠や開錠、
２）パソコン、タブレット、スマホ、電子装置などのロック解除、
３）ＩｏＴ（Ｉｎｔｅｒｎｅｔ Ｏｆ Ｔｈｉｎｇｓ）装置などのオン／オフ制御、
４）現金自動預け払い機（Ａｕｔｏｍａｔｉｃ Ｔｅｌｌｅｒ Ｍａｃｈｉｎｅ）での認証や自動車のロック解除の際の認証、および
５）多重化されたユーザー認証の１つ。
【００２３】
図２の各ブロックの構成について説明する。
【００２４】
無線キーデバイス１０aは、通信開始を制御するための通信開始制御部１６ａ、同時取得可能な生体情報の発信部１から生体情報１ａを取得するための生体情報取得部（特徴取得部）１１ａと、取得した生体情報１ａに基づいて共通鍵（暗号鍵）を生成する共通鍵生成部１２ａと、を有する。無線キーデバイス１０aは、また、施錠/開錠を行うために施錠/開錠デバイスに登録しているＩＤ情報を格納するＩＤ情報格納部１５ａと、生成した共通鍵によってＩＤ情報を暗号化する暗号復号化部１３ａと、暗号化したＩＤ情報を送信するための通信部１４ａと、を有する。
【００２５】
無線キーデバイス１０aにおいて、例えば、生体取得情報部１１ａはマイクで構成可能である。通信開始制御部１６ａ、共通鍵生成部１２ａおよび暗号復号化部１３ａは、半導体装置に形成された中央処理装置（ＣＰＵ）で構成可能である。ＩＤ情報格納部１５ａは、半導体装置に形成された記憶装置で構成可能である。また、通信部１４ａは、半導体装置に形成されたＢＬＥ（Ｂｌｕｔｏｏｔｈ（登録商標） Ｌｏｗ Ｅｎｅｒｇｙ）規格のビーコン（Beacon）通信部で構成可能である。
【００２６】
施錠/開錠デバイス２０ａは、通信開始を制御するための通信開始制御部２６ａと、生体情報１ａを取得するための生体情報取得部（特徴取得部）２１ａと、取得した生体情報１ａに基づいて共通鍵（暗号鍵）を生成する共通鍵生成部２２ａと、を有する。施錠/開錠デバイス２０ａは、また、無線キーデバイス１０ａから送付された無線情報を受信する通信部２４ａと、受信した暗号化されたＩＤ情報を生成した共通鍵を使って復号する暗号復号化部２３ａと、予め登録された施錠/開錠を行う場合のＩＤ情報を格納するＩＤ情報データベース２７ａと、を有する。施錠/開錠デバイス２０ａは、また、復号したＩＤ情報とデータベース２７ａに登録されているＩＤ情報を比較判定するＩＤデータ判定部２８ａと、所望のＩＤ信号を受信したと判定された場合に鍵の施錠/開錠を行うための施錠/開錠部２９ａと、を有する。
【００２７】
施錠/開錠デバイス２０ａにおいて、例えば、生体取得情報部２１ａはマイクで構成可能である。通信開始制御部２６ａ、共通鍵生成部２２ａ、暗号復号化部２３ａおよびＩＤデータ判定部２８ａは、半導体装置に形成された中央処理装置（ＣＰＵ）で構成可能であ

る。ＩＤ情報データベースは半導体装置に形成された記憶装置で構成可能である。また、通信部２４ａは、半導体装置に形成されたＢＬＥ（Ｂｌｕｔｏｏｔｈ Ｌｏｗ Ｅｎｅｒｇｙ）規格のビーコン（Beacon）通信部で構成可能である。また、施錠/開錠部２９ａは、半導体装置に形成された施錠/開錠制御回路と、施錠/開錠制御回路により制御される、例えば、ドアに設けられた鍵等の機械部分とで構成することが可能である。

【００２８】

図３は、実施例１に係るフローチャートを示す図であり、以下このフローチャートについて説明をする。

【００２９】

無線キーデバイス１０ａと施錠/開錠デバイス２０ａとは、それぞれの通信開始制御部１６ａ、２６ａを用いて、両デバイス１０ａ、２０ａを起動させて、生体情報１ａを収集できる状態にする（ステップＳ１）。通信開始制御部１６ａ、２６ａは、例えば、無線キーデバイス１０ａと施錠/開錠デバイス２０ａとに実装されたそれぞれのボタンが押されたことを検出することで通信開始を制御する方法がある。

【００３０】

次に、同時取得可能な生体情報の発信部１ａによって発信された生体情報１ａを無線キーデバイス１０ａ、施錠/開錠デバイス２０ａの両デバイスがそれぞれ取得する（ステップＳ２＿１、Ｓ２＿２）。生体情報１ａについての詳細は後述する。

【００３１】

次に、両デバイス１０ａ、２０ａそれぞれで、生体情報１ａから特徴量を抽出し、その特徴量を反映した共通鍵を生成する（ステップＳ３＿１、Ｓ３＿２）。共通鍵・暗号化についての詳細は後述する。

【００３２】

次に、無線キーデバイス１０ａは、生成した共通鍵を使ってＩＤ情報の暗号化を行う（ステップＳ４）。生体情報１ａの取得失敗や特徴量抽出に失敗し、暗号化を行うことができなかった場合（ステップＳ５、ＮＯ）、通信終了（ステップＳ６）へ遷移する。

【００３３】

次に、無線キーデバイス１０ａで暗号化に成功した場合（ステップＳ５、ＹＥＳ）、暗号化したＩＤ情報を施錠/開錠デバイス２０ａに送信する（ステップＳ７）。ここでの通信方法の例として、ＢＬＥ Ｂｅａｃｏｎを使ったブロードキャスト通信がある。データ送信後、無線キーデバイス１０ａは通信終了（ステップＳ６）となる。

【００３４】

次に、施錠/開錠デバイス２０ａでは、共通鍵の生成に失敗した場合（ステップＳ８、ＮＯ）、通信終了（ステップＳ６）へ遷移する。共通鍵の生成に成功した場合（ステップＳ８、ＹＥＳ）、暗号化されたＩＤ情報を受信し（ステップＳ９）、生成した共通鍵を復号鍵として利用することにより受信したデータの復号を行う（ステップＳ１０）。無線キーデバイス１０ａと施錠/開錠デバイス２０ａとで同じ生体信号１ａから特徴量を抽出し、共通鍵を生成しているため、無線キーデバイス１０ａで暗号化されたＩＤ情報は施錠/開錠デバイス２０ａで復号できる。

【００３５】

次に、施錠/開錠デバイス２０ａでは、復号したＩＤ情報とデータベース２７ａに格納されているＩＤ情報とをＩＤ判定部２８ａで比較・判定し（ステップＳ１１）、両者が一致すれば（ステップＳ１１、ＹＥＳ）、鍵の施錠/開錠の操作（ステップＳ１２）を行い、通信終了（ステップＳ６）となる。ＩＤ情報が一致しなければ（ステップＳ１１、ＮＯ）、そのまま通信終了（ステップＳ６）となる。

【００３６】

（同時取得可能な生体情報）

同時取得可能な生体情報１ａの特徴量に求められる方向性として下記２つがある。

【００３７】

１）生体情報１ａの特徴量が観測条件で変わらないこと

２）生体情報１ａの特徴量が変化幅を持つこと
仮に、上記１）が満たせない場合、生体情報１ａの取得条件(測定場所や測定デバイス)で生成される共通鍵が送信側通信装置（無線キーデバイス１０ａ）と受信側通信装置（施錠/開錠デバイス）とで異なるため、暗号化データを復号できない問題が発生する。
【００３８】
仮に、上記２）が満たせない場合、同じ共通鍵を使って通信を行う可能性が高くなり、第三者による共通鍵の推測が容易になる懸念がある。
【００３９】
本明細書では、具体性を持たせるため、生体情報１ａの特徴量の例として、音声の声帯振動を用いる。音声の音色、高さ、大きさなどといった特徴には個人差があり、この個人差は、声帯の振動周期や声道と呼ばれる声帯から唇までの形状の違いに起因した先天的なものと、方言、話し方のくせ、音声トレーニングといった後天的に発生したものがある。
【００４０】
この特徴の解析には、通常、音声のサウンドスペクトログラムが使われる。
【００４１】
図４に「あ」と発音したときの時間波形を示す。図４において、横軸は時間、縦軸は振幅強度を失している。図４の波形を、横軸を時間、縦軸を周波数成分で表したサウンドスペクトログラムを図５に示す。図５の色の違い（濃淡）は、音声信号の周波数成分が集中しているところと、していないところの違いを示している。
【００４２】
図５のサウンドスペクトログラムを解析することで個人が持つ音声パターンの特徴を抽出することができる。ここでは一般的な解析方法であるケプストラム分析を行う。ケプストラム分析では、音声波形をフーリエ変換して得たパワースペクトルについて、その値の対数を取り、さらに逆フーリエ変換を行う。
【００４３】
ケプストラム分析の結果、声道の形状に起因した部分は低域側、声帯振動に起因した特徴は高域側に現れる。低域側の特徴は音声認識に利用されるが、特徴が複雑で観測条件依存性もあるため、本発明の生体信号の特徴量としては不適切である。高域側に現れる特徴量は声帯振動周に対応したものであり、後述するように、観測条件の依存性が小さく、ユーザーが比較的容易に特徴量を変化させることができるため、本発明の生体情報の特徴量として適している。
【００４４】
図５の時間波形を、パワースペクトルで表した結果を図６に示し、ケプストラム分析した結果を図７に示す。図７の横軸は次元としては時間と同じになるが、対数値にして逆フーリエ変換を行っているため、数値は時間に対応せず、ケフレンシ（ｑｕｅｆｒｅｎｃｙ）と呼ばれる場合がある。ここではケフレンシと呼ぶ。
【００４５】
図６の最も大きいピーク値が、基本周波数と呼ばれる声帯振動周波数に対応する周波数で、周波数が高いほど声は高音になり、逆に低いほど低音になる。一般的に男性の平均値は１２５Ｈｚ程度で、女性の平均は男性の２倍の２５０Ｈｚ程度になる。男性の声である図６の基本周波数はたとえば、１１８Ｈｚとなる。
【００４６】
図７でのケフレンシ値のピークは、声帯振動周波数に対応する特徴量であり、図７の場合は１１０近傍にピークを持つ。ケプストラム分析を行うことで、図６の基本周波数が、図７を見てわかるように、特徴量がより見つけやすくなるという利点がある。本明細書では、生体信号１ａの特徴量として、このピークが現れるケフレンシ値(声帯振動周波数)を一例として考えている。
【００４７】
実際の使用を考えた場合、無線キーデバイス１０ａと施錠/開錠デバイス２０ａのそれぞれの生体情報１０ａの発生源１(例えば、音声源１)からの距離は異なることが想定され

る。この距離の違いから両デバイス１０ａ、２０ａで取得される生体情報１ａの特徴量が異なる場合、生成される共通鍵も異なるため、暗号化データの復号が失敗する虞がある。

【００４８】

図８は、音声源と集音するマイクの距離が変わった場合の基本周波数とピークが現れるケフレンシ値との関係を説明する図である。図８（ａ）は、「あ」と発音したときの振幅強度と音声源とマイクの距離と関係との関係を示している。音声源とマイクの距離が近い場合、振幅強度は大きく、音声源とマイクの距離が遠い場合、振幅強度は小さくなる。図８（ｂ１）は、音声源とマイクの距離が近い場合における時間波形をパワースペクトルで表した結果を示す。図８（ｃ１）は、音声源とマイクの距離が近い場合におけるケプストラム分析した結果を示す。図８（ｂ２）は、音声源とマイクの距離が遠い場合における時間波形をパワースペクトルで表した結果を示す。図８（ｃ２）は、音声源とマイクの距離が遠い場合におけるケプストラム分析した結果を示す。

【００４９】

音声の声帯振動周波数の場合、図８（ａ）に示すように、音声源と集音するマイクの距離が変わったとき、振幅強度は変化するが、図８（ｃ１）（ｃ２）に示すように、声帯振動周波数(ピークのケフレンシ値)は変わらないため、声帯振動周波数(ピークのケフレンシ値)を元に共通鍵を生成すれば、音源とマイクの距離によらず同じ共通鍵を生成できることが期待できる。

【００５０】

悪意のある第三者により暗号鍵を推測されるのを防ぐ(耐タンパ性)ために、生成する共通鍵を頻繁に変えられることが望ましい。異なる共通鍵を生成するためには、生体信号１ａの特徴量を変える必要がある。

【００５１】

図９は、高音を意識して”あ”と発音した場合と、低音を意識して”あ”と発音した場合の基本周波数とピークのケフレンシ値との関係を示す図である。図９の（ａ１）、（ｂ１）、（ｃ１）は、高音を意識して”あ”と発音した場合を示し、図９の（ａ２）、（ｂ２）、（ｃ２）は、低音を意識して”あ”と発音した場合した場合を示している。図９の（ａ１）、（ａ２）は、横軸を時間、縦軸を周波数成分で表したサウンドスペクトログラムを示す図である。図９の（ｂ１）、（ｂ２）は、時間波形を、パワースペクトルで表した結果を示す図である。図９の（ｃ１）、（ｃ２）は、ケプストラム分析した結果を示す図である。

【００５２】

図６、図７および図８に示されるように、意識せずに”あ”と発音した場合の声帯振動周波数は１１４Ｈｚ～１１８Ｈｚだったのに対し、図９の（ｂ１）、（ｃ１）に示されるように、高音を意識して”あ”と言った場合、声帯振動周波数は３０１Ｈｚまで上がり、ピークが現れるケフレンシ値も３０１近傍となる。一方、図９の（ｂ２）、（ｃ２）に示されるように、低音を意識して”あ”と言った場合、声帯振動周波数は１０１Ｈｚまで下がり、ピークが現れるケフレンシ値も１０１近傍となる。このように、ユーザーが意識して声帯振動周波数(特徴量)を変えられるため、意図的に生成する共通鍵に多様性を持たせることで、耐タンパ性の向上が期待できる。

【００５３】

（特徴量に基づいた暗号化について）

生体信号１ａの特徴量を使ってＩＤ情報を暗号化する簡単な方法として、特徴量分のＮ倍だけをＩＤ情報のコードをシフトする方法がある。

【００５４】

例として、iBeacon（登録商標）を使った場合を考える。iBeaconでは任意のデータを格納できるスペースは、Ｍａｊｏｒと呼ばれる１６ｂｉｔと、Ｍｉｎｏｒと呼ばれる１６ｂｉｔのスペースである。仮に、Ｍａｊｏｒの１６ｂｉｔはサービスやアプリ自体を区別するために使うとすると、ＩＤ情報はＭｉｎｏｒの１６ｂｉｔ（６５５３６通り)で管理することになる。

【００５５】
仮に、ＩＤ情報を１０００としたとき、ピークのケフレンシ値(特徴量)が１５０で、暗号化アルゴリズムを特徴量の１０倍分コードをシフトさせることとすると、１０００+１５０*１０=２５００より暗号化されたＩＤ情報は２５００となる。ここで、暗号化後のコードが６５５３６を超えた場合は0に戻るとする。
【００５６】
この様にすることで、ＩＤ情報の類推の困難性を高めることが可能である。
【００５７】
共通鍵の長さ（ｂｉｔ数）を十分に長くすれば安全性は向上するが、処理が重たくなり暗号化・復号が遅くなるという欠点がある。このためアプリが求めるセキュリティレベルに応じた共通鍵の長さを選択することが望ましい。
【００５８】
仮に、ＩＤ情報（１６ｂｉｔ）を暗号化するのに、平文と同じ長さの共通鍵（１６ｂｉｔ）を使うことを考える。図９にある基本周波数の変化幅は２００Ｈｚ（=３０１Ｈｚ-１０１Ｈｚ）で、測定誤差を考慮して、１２．５Ｈｚごとに特徴量として区別すると、２００Ｈｚ/１２．５Ｈｚ=１６=４ｂｉｔとなる。
【００５９】
つまり、１回の有声音(声帯振動を伴う音)を発音すると、共通鍵の長さは４ｂｉｔとなる。このため、１６ｂｉｔ（=４ｂｉｔ×４）の共通鍵を作るには、４回の有声音を声の高さを変えながら発音すればよい。何回有声音を発音するかは、ユーザーが求めるセキュリティレベルから決めることが可能になる。
【００６０】
実施例１によれば、同時取得可能な生体情報１ａの特徴要素（例えば、音声の声帯振動周波数、声紋等）を、通信を行う２つ以上の通信装置１０ａ、２０ａが、例えば、同時に取得し、その特徴量に基づいた共通鍵（暗号鍵）をそれぞれの通信装置１０ａ、２０ａで生成することかできる。
【００６１】
生体情報の特徴量（例えば、声帯振動周波数）に基づいて共通鍵を生成するため、通常共通鍵の共有に必要なセキュアなネットワークが不要となり、導入コスト、管理コストの削減が期待できる。
【００６２】
また、生体情報１ａの特徴を意図的に変更する（例えば、声帯振動周波数なら意図的に高い声、低い声を出す）ことで、異なった共通鍵が生成することが出来るので、悪意を持った第三者による共通鍵の推測が難しくなり、耐タンパ性の向上が期待できる。
【実施例２】
【００６３】
図１０は、実施例２に係る通信システムを説明するための図である。
【００６４】
図２に示されるように、実施例１の通信システム１００ａでは、無線キーデバイス１０ａと施錠/開錠デバイス２０ａとの１対１の通信システムを示した。実施例２に示される通信システム１００ｂでは、ＩＤ情報送信端末装置１０ｂと、複数のＩＤ情報受信端末装置２０ｂ＿１、２０ｂ＿２、・・・、２０ｂ＿Ｎ－１、２０ｂ＿Ｎと、を有する。
【００６５】
ＩＤ情報送信端末装置１０ｂの構成は、無線キーデバイス１０ａと同じであり、通信開始制御部１６ａ、生体情報取得部（特徴取得部）１１ａと、共通鍵生成部１２ａと、ＩＤ情報格納部１５ａと、暗号復号化部１３ａと、通信部１４ａと、を有する。
【００６６】
複数のＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの各々は、通信開始を制御するための通信開始制御部２６ｂ、生体情報１ａを取得するための生体情報取得部（特徴取得部）２１ｂと、取得した生体情報１ａに基づいて共通鍵（暗号鍵）を生成する共通鍵生成部

２２ｂと、ＩＤ情報送信端末装置１０ｂから送付された無線信号を受信する通信部２４ｂと、を有する。ＩＤ情報送信端末装置１０ｂから送付された無線信号は、たとえば、ＢＬＥ（ＢｌｕｔｏｏｔｈＬｏｗ Ｅｎｅｒｇｙ）規格のビーコン（Beacon）とすることが可能である。

【００６７】

複数のＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの各々は、さらに、受信した暗号化されたＩＤ情報を生成した共通鍵を使って復号する暗号復号化部２３ｂと、予め登録されたＩＤ情報を格納するＩＤ情報データベース２７ｂと、を有する。複数のＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの各々は、さらに、復号したＩＤ情報とデータベース２７ｂに登録されているＩＤ情報を比較判定し、所望のＩＤ信号を受信したと判定された場合に、ＩＤ情報送信端末装置１０ｂの送信者をＩＤ情報に紐づいた個人情報の持ち主と認証する個人情報認証部３０と、を有する。

【００６８】

なお、個人情報認証部３０は、図２のＩＤデータ判定部２８ａと施錠/開錠部２９ａへ変更してもよい。

【００６９】

図１１は、実施例２に係るフローチャートを示している。

【００７０】

通信開始制御部１６ａ、２６ｂとして、例えば、実施例１で示したデバイス１０ａ、２０ａに実装されたボタンを押して通信開始させることもできるが、複数台のＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎのそれぞれに実装されたボタンを押していくのは手間となる。このため、例えば、ＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの通信部２４ｂは常に起動させておき、ＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの通信部２４ｂが、予め登録しておいた通信開始を知らせる無線信号(平文)を、ＩＤ情報送信端末装置１０ｂから受信した場合、通信を開始して（ステップＳ２０）、生体情報１ａを取得するモードに遷移させる方法が有効である。

【００７１】

それ以降の生体情報取得からＩＤ情報の照合までのフローについては、実施例１で説明した通りである。

【００７２】

すなわち、同時取得可能な生体情報の発信部１ａによって発信された生体情報１ａをＩＤ情報送信端末装置１０ｂ、複数のＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎの両デバイスがそれぞれ取得する（ステップＳ２１＿１、Ｓ２１＿２）。

【００７３】

次に、両デバイス１０ｂ、２０ｂ＿１－２０ｂ＿Ｎそれぞれで、生体情報１ａから特徴量を抽出し、その特徴量を反映した共通鍵を生成する（ステップＳ２２＿１、Ｓ２２＿２）。

【００７４】

次に、ＩＤ情報送信端末装置１０ｂは、生成した共通鍵を使ってＩＤ情報の暗号化を行う（ステップＳ２３）。

【００７５】

次に、ＩＤ情報送信端末装置１０ｂは、暗号化したＩＤ情報をＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎに送信する（ステップＳ２４）。ここでの通信方法の例として、ＢＬＥ Ｂｅａｃｏｎを使ったブロードキャスト通信がある。データ送信後、ＩＤ情報送信端末装置１０ｂは通信終了（ステップＳ２５）となる。

【００７６】

次に、ＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎは、ＩＤ情報送信端末装置１０ｂから暗号化されたＩＤ情報を受信し（ステップＳ２６）、生成した共通鍵を復号鍵として利用することにより受信したデータ（ＩＤ情報）の復号を行う（ステップＳ２７）。

【００７７】

ＩＤ情報照合（ステップＳ２８）では、ＩＤ情報に紐づいて個人情報を格納したＩＤ情報データベース２７ｂを有する。個人情報認証部３０において受信したＩＤ情報とＩＤ情報受信端末装置２０ｂ＿１－２０ｂ＿Ｎが持つID情報データベース２７ｂ内のＩＤ情報を照合し、ＩＤ情報が一致すれば（ステップＳ２８、ＹＥＳ）、ＩＤ情報送信端末装置１０ｂの送信者をＩＤ情報に紐づいた個人情報として読み出し（ステップＳ２９）、通信終了（ステップＳ３０）となる。ＩＤ情報が一致しなければ（ステップＳ２８、ＮＯ）、そのまま通信終了（ステップＳ３０）となる。

【００７８】

したがって、実施例２でも、実施例１と同様な効果を得ることが可能である。

【実施例３】

【００７９】

図１２は、実施例３に係る通信システムを説明するための図である。図１２の通信システム１００ｃは、ＩＤ情報送信端末１０ｃと、個人認証装置２０ｃと、を有する。実施例１、２の同時取得可能な生体情報の発信部１は、音声発生源として示されており、個人認証対象者（ユーザ）の音声と見做すことが出来る。

【００８０】

実施例３のＩＤ情報送信端末１０ｃにおいて、実施例１、２の同時取得可能な生体情報１ａが声紋１ｃへ変更されることに伴い、実施例１、２の生体情報取得部１１ａが声紋検出部（特徴取得部）１１ｃへと変更される。その他の構成は、実施例１、２と同じであるので、説明は省略する。

【００８１】

実施例３の個人認証装置２０ｃは、実施例２のＩＤ情報受信端末装置２０ｂ＿１とほぼ同じであるが、同時取得可能な生体情報１ａが声紋１ｃへ変更されることに伴い、生体情報取得部２１ａが声紋検出部（特徴取得部）２１ｃへ変更され、新たに声紋情報データベース２１１ｃおよび声紋認証部２１２ｃが追加されている。他の構成は、実施例２のＩＤ情報受信端末装置２０ｂ＿１と同じであるので、説明は省略する。

【００８２】

これにより、個人認証装置２０ｃにおいて、ＩＤ情報送付端末１０ｃが発信するＩＤ情報に加えて、ユーザーの声(声紋)による声紋認証を利用することで、２段階の認証システムを行うことができる。

【００８３】

個人認証装置２０ｃに声紋情報のデータベース２１１ｃを用意しておき、取得した声紋パターンとデータベース２１１ｃの声紋パターンを声紋認証部２１２ｃで照合し、声紋の持ち主を識別することができる。

【実施例４】

【００８４】

図１３は、実施例４に係る通信システムを説明するための図である。

【００８５】

実施例１、２、３では、共通鍵を生成するために生体情報の特徴パターンを想定していたが、生体情報以外の同時取得が可能な特徴パターン（特徴要素）を実施例４に示す。

【００８６】

同時取得可能な特徴パターンの発信部５０としては、例えば、楽器の場合、各音階で音の基本周波数が異なるため、演奏パターンの違いから共通鍵の生成に使う特徴パターンを作ることができる。すなわち、ドレミファソラシドの音階を考えたとき、最後の”ド”の基本周波数は初めの”ド”の２倍大きい。

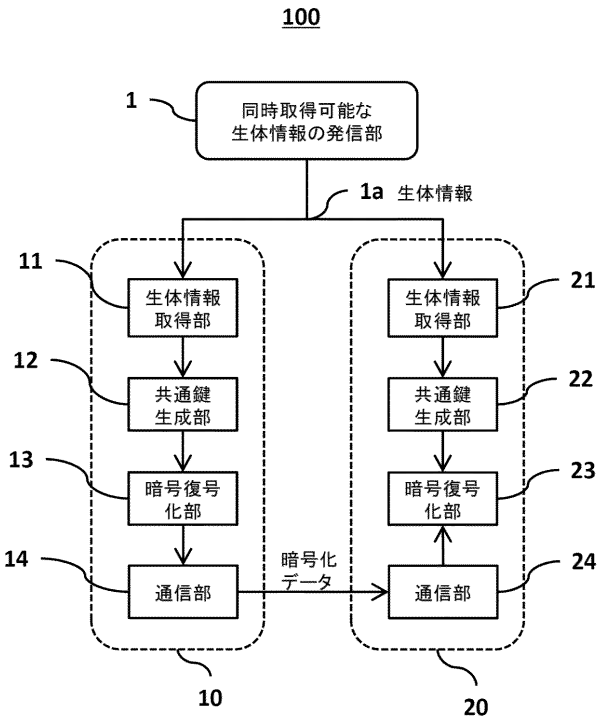
【００８７】

また、発信部５０の他の例として、人の可聴波数帯域（２０Ｈｚ程度から２０ｋＨｚ程度まで)だと、演奏パターンを悪意のある第三者に聞かれる懸念や、騒音として第三者に不快感を与える懸念があるため、可聴周波数帯域以外の音（２０Ｈｚ以下もしくは２０ｋＨｚ以上の音)を出せる、例えば、超音波発生器などがある。

【００８８】
実施例４に示す通信システム１００ｄにおいて、同時取得可能な特徴パターンの発信部５０の変更されたことに伴い、ＩＤ情報送付端末装置１０ｄにおいて、実施例１の生体情報取得部１１ａが特徴パターン取得部（特徴取得部）５１へと変更され、また、ＩＤ情報受信端末装置２０ｄにおいて、実施例１の生体情報取得部２１ａが特徴パターン取得部（特徴取得部）５２へ変更されている。他の構成は、実施例１と同じであるので、説明は省略する。
【００８９】
このような構成においても、実施例１と同様な効果を得ることが可能である。
【００９０】
以上、本発明者によってなされた発明を実施例に基づき具体的に説明したが、本発明は、上記実施形態および実施例に限定されるものではなく、種々変更可能であることはいうまでもない。
【符号の説明】
【００９１】
１：同時取得可能な生体情報の発信部
１ａ：生体情報（音声）
１０、１０ａ、１０ｂ、１０ｃ、１０ｄ：通信装置（ＩＤ情報送信端末装置）
２０、２０ａ、２０ｂ、２０ｃ、２０ｄ：通信装置（ＩＤ情報受信端末装置）
１１、２１：生体情報取得部（特徴取得部）
１２、２２：共通鍵生成部
１３、２３：暗号復号化部
１４、２４：通信部
１５ａ：ＩＤ情報格納部
１６ａ、２６ａ：通信開始制御部
２７ａ：ＩＤ情報データベース
２８ａ：ＩＤデータ判定部
２９ａ：施錠/開錠部
１００、１００ａ、１００ｂ、１００ｃ、１００ｄ：通信システム

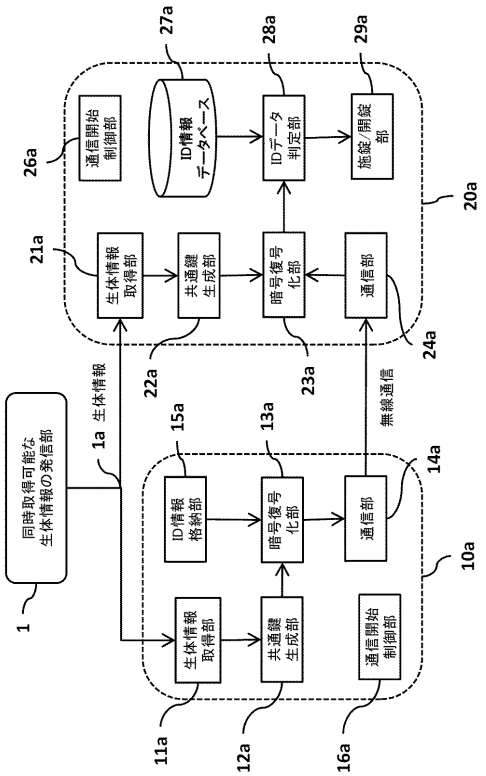
【図１】

図1



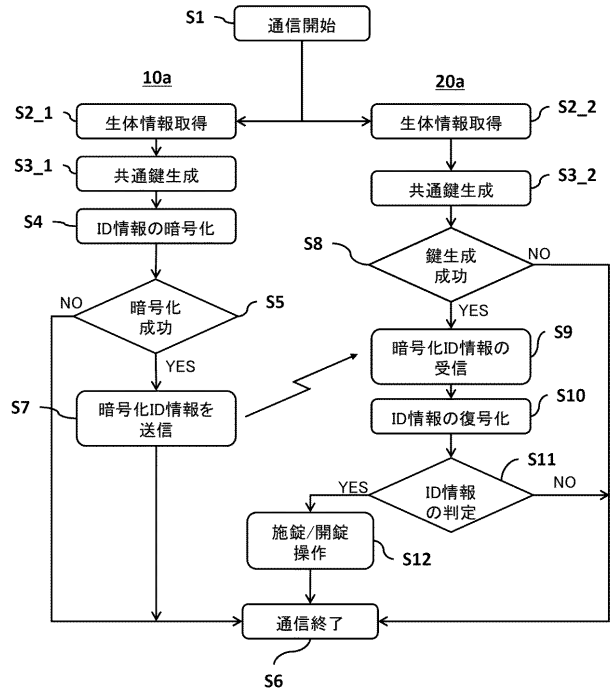
【図２】

図2



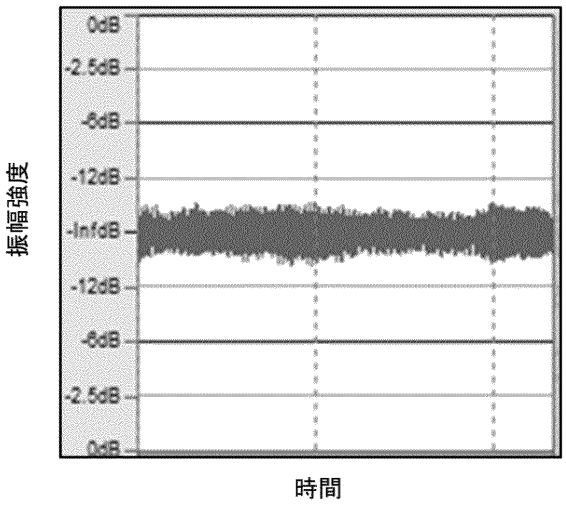
【図３】

図3



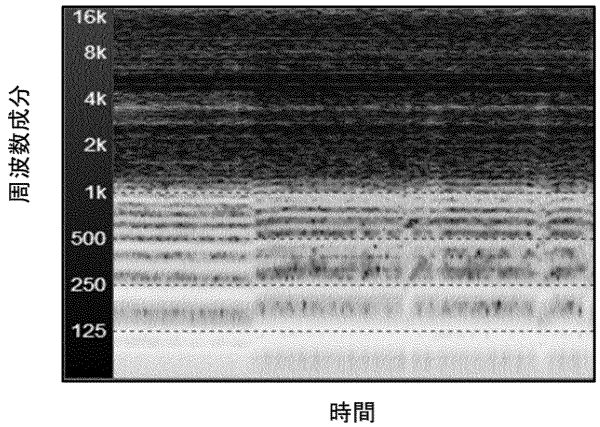
【図４】

図4



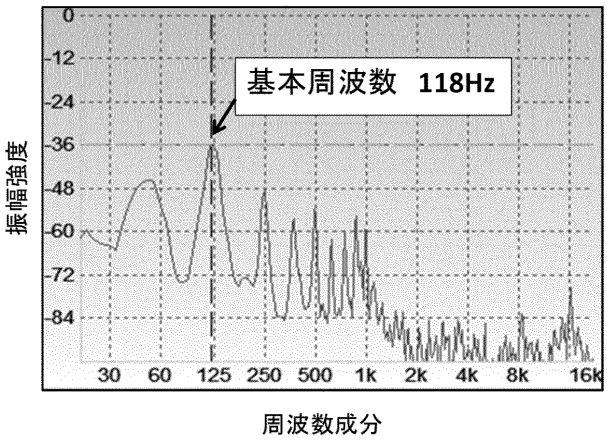
【図５】

図5



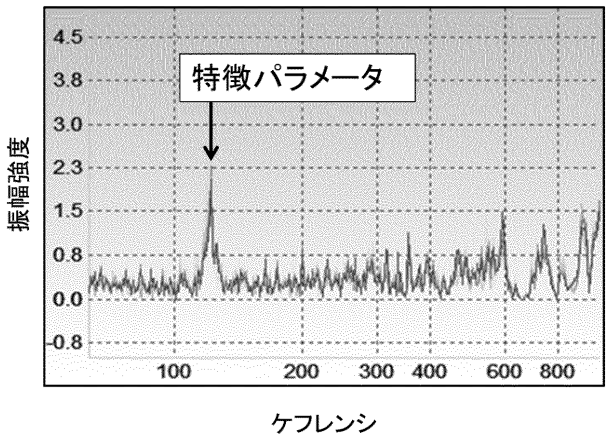
【図６】

図6



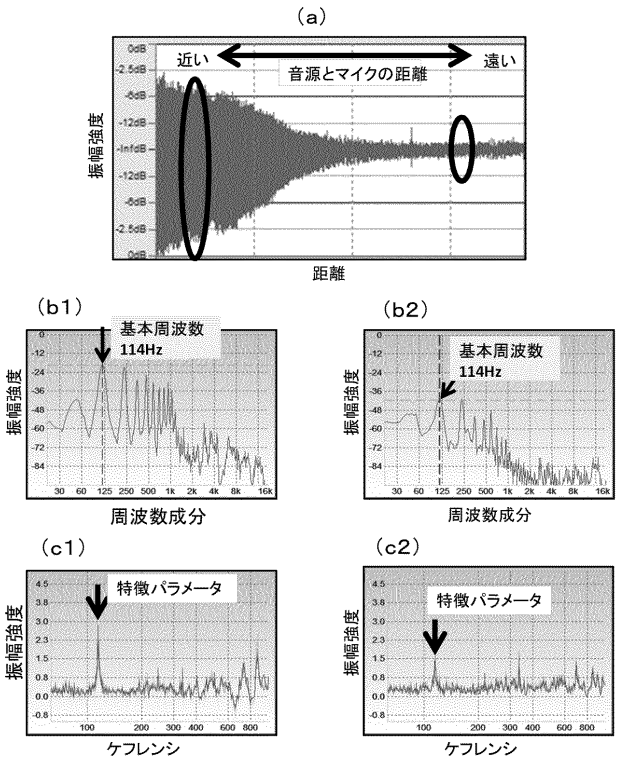
【図７】

図7

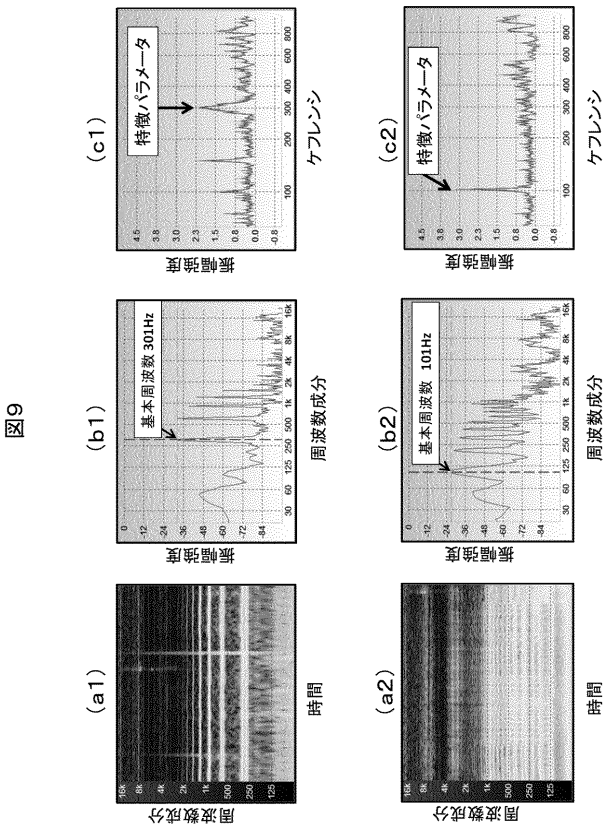


【図８】

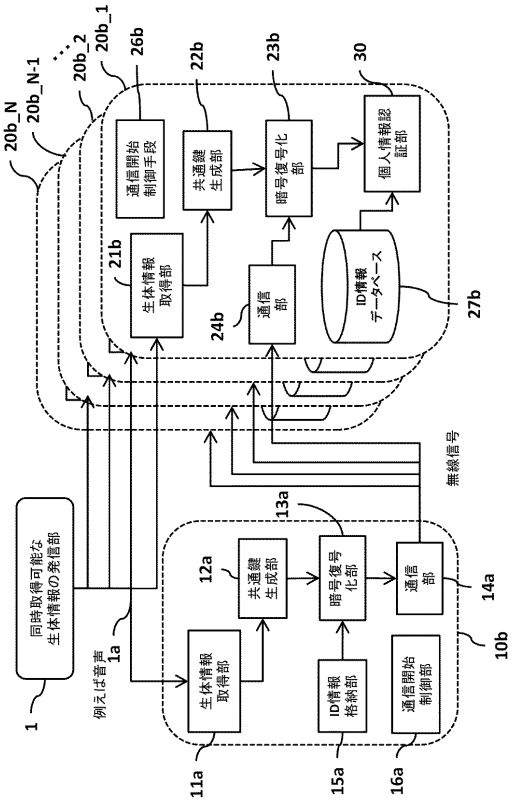
図8



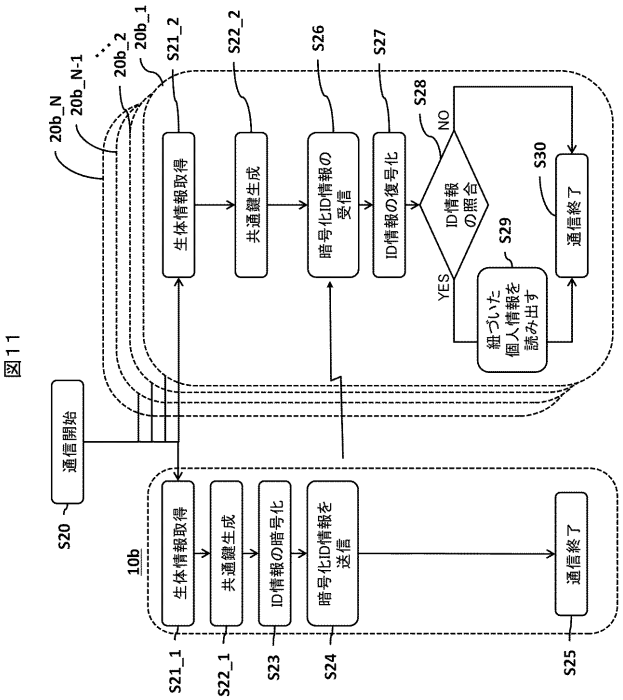
【図９】



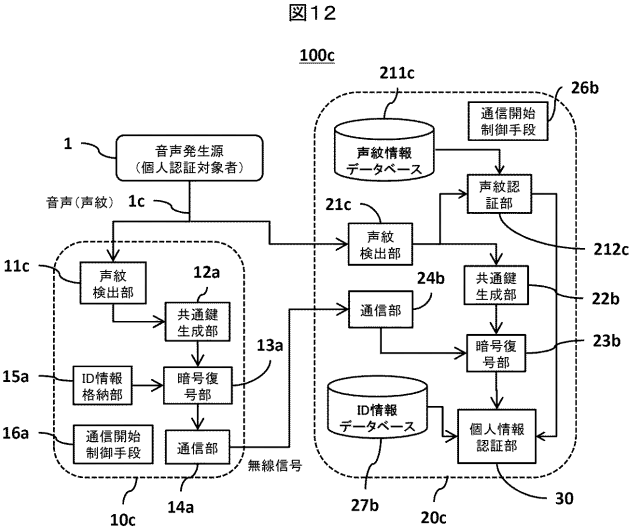
【図１０】



【図１１】

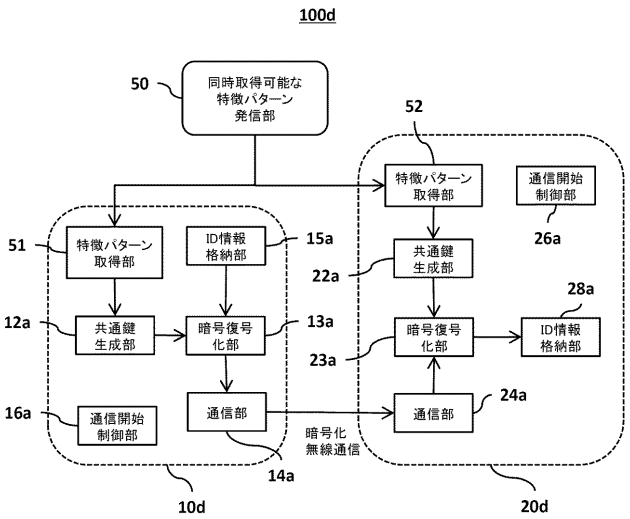


【図１２】



【図１３】

図13


100d
50
同時取得可能な
特徴パターン
発信部
52
特徴パターン
取得部
通信開始
制御部
26a
51
特徴パターン
取得部
ID情報
格納部
15a
22a
共通鍵
生成部
28a
12a
共通鍵
生成部
暗号復号
化部
13a
23a
暗号復号
化部
ID情報
格納部
16a
通信開始
制御部
通信部
24a
通信部
暗号化
無線通信
14a
10d
20d

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｈ０４Ｌ　9/00　６７３Ｄ	

(72)発明者　若田　秀幸
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内

Ｆターム(参考) 2E250 AA01 AA14 AA16 AA25 BB08 BB29 BB46 DD06 DD10 EE10
FF09 FF24 FF27 FF36
5J104 AA16 EA24 NA02