(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2007-172294
(P2007-172294A)
(43)公開日　平成19年7月5日(2007.7.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104
H04L 9/10	(2006.01)	H04L	9/00	621A	
		G06F	15/00	330C	

審査請求 未請求　請求項の数 13　ＯＬ　（全 8 頁）

(21)出願番号　特願2005-369021 (P2005-369021)
(22)出願日　平成17年12月22日 (2005.12.22)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　三村　昌弘
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　高橋　健太
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5B285 AA04　CA41　CB12　CB91
5J104 AA07　KA01　KA16　NA42　PA07

(54)【発明の名称】利用者の認証機能を備えた情報処理装置

(57)【要約】
【課題】
攻撃者の生体認証センサの偽装による不正な生体情報の取得を防止する。
【解決手段】
利用者しか知りえない秘密情報を暗号化し、復号鍵を生体情報センサ100に保持し、そして生体情報センサ100が秘密情報の復号化部125および秘密情報を利用者に提示する秘密情報表示部105、生体情報の入力部に生体情報が提示されたことを検知する生体情報検知部110、秘密情報が提示される前に生体情報が検知された場合、利用者に対して警告を発する警告報知部107を持つ。
【選択図】　図１

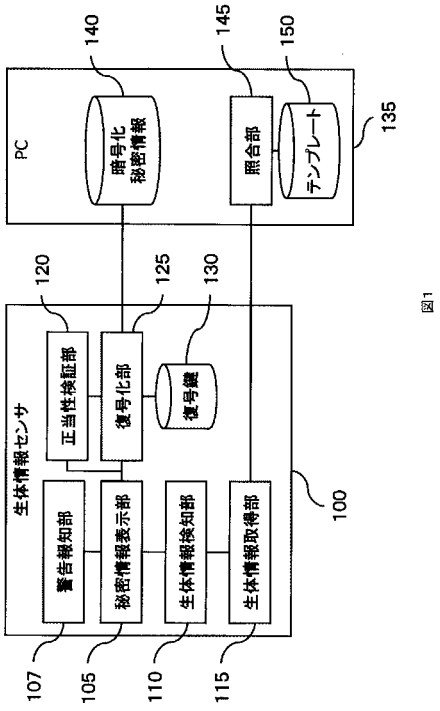

図1

【特許請求の範囲】
【請求項１】
利用者の身体的あるいは行動的特徴を含む生体情報を利用して利用者を認証する情報処理装置において、
前記利用者に対応付けられた前記利用者が知り得る秘密情報を暗号化して記録する手段と、
前記秘密情報を復号化する手段と、
前記復号化された秘密情報を前記利用者に提示する手段とを有することを特徴とする情報処理装置。
【請求項２】
請求項1に記載の情報処理装置において、
秘密情報の正当性を確認する手段を有し、
前記提示する手段は、前記秘密情報の正当性が確認できた場合に前記秘密情報を利用者に提示することを特徴とする情報処理装置。
【請求項３】
請求項1に記載の情報処理装置において、
前記生体情報を取得するセンサ部を有し、
前記復号化する手段と前記提示する手段は、前記センサ部に含まれることを特徴とする情報処理装置。
【請求項４】
請求項2に記載の情報処理装置において、
前記生体情報を取得するセンサ部を有し、
前記確認する手段は、前記センサ部に含まれることを特徴とする情報処理装置。
【請求項５】
請求項1から請求項4に記載の情報処理装置において、
前記利用者に対応付けられた秘密情報を提示する前に前記利用者が生体情報を入力した場合に前記利用者に警告を発する手段を有することを特徴とする情報処理装置。
【請求項６】
請求項1から請求項5に記載の情報処理装置において、
前記秘密情報は、前記情報処理装置に登録された利用者ごとに異なることを特徴とする情報処理装置。
【請求項７】
請求項1から請求項６に記載の情報処理装置において、
前記秘密情報は、異なる複数の色の光の発光パターンであることを特徴とする情報処理装置。
【請求項８】
請求項１から請求項７に記載の情報処理装置において、
前記復号化する手段は、耐タンパ性が高いことを特徴とする情報処理装置。
【請求項９】
請求項２又は請求項４に記載の情報処理装置において、
前記確認する手段は、耐タンパ性が高いことを特徴とする情報処理装置。
【請求項１０】
利用者の認証機能を備えた情報処理装置において、
前記利用者の認証情報を記憶する記憶装置と、
前記利用者の認証情報を入力する入力装置と、
前記記憶装置内の前記認証情報に基づいて、前記入力装置からの前記認証情報を照合する照合装置とを備え、
前記記憶装置は、前記利用者が知り得る秘密情報を記憶し、
前記入力装置は、前記利用者から前記認証情報を受け付ける前に、前記記憶装置内の前記秘密情報を前記利用者へ提示することを特徴とする情報処理装置。

【請求項１１】
請求項10に記載の情報処理装置において、
前記入力装置は、前記利用者の認証情報を検知する検知装置と、前記秘密情報を出力する出力装置とを備え、
前記検知装置は、前記出力装置が前記秘密情報を出力した場合に、値を設定し、
前記検知装置は、前記利用者の認証情報を検知した場合に、前記値が設定されているか否かを判定し、前記値が設定されていない場合に前記報知装置から警告を報知することを特徴とする情報処理装置。
【請求項１２】
請求項10に記載の情報処理装置において、
前記記憶装置は、暗号化された前記秘密情報を記憶し、
前記入力装置は、前記暗号化された秘密情報を復号化する復号化装置を備えることを特徴とする情報処理装置。
【請求項１３】
請求項10に記載の情報処理装置において、
前記秘密情報は、利用者ＩＤと前記出力装置からの出力パターンデータと前記利用者ＩＤと前記出力パターンデータに対するハッシュ値とを含み、
前記入力装置は、前記秘密情報内の前記利用者ＩＤと前記出力パターンデータに対してハッシュ値を生成し、前記秘密情報内の前記ハッシュ値に基づいて、生成された前記ハッシュ値を検証する検証装置を備え、
前記入力装置は、前記ハッシュ値の検証に成功した場合に、前記秘密情報を出力することを特徴とする情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、利用者の認証機能を備えた装置及びその方法に係り、特に、あらかじめ登録された利用者にだけサービスを提供する情報システムへのアクセス管理や課金をともなうサービスを提供する場合の本人確認、および重要な施設や部屋への入退管理などに適用できる装置及びその方法に関する。
【背景技術】
【０００２】
生体認証において、利用者の生体情報は暗号における鍵と同じ機能を有する。したがって、セキュリティの観点から生体情報の漏洩や攻撃者による不正な取得を防止しなければならない。一般に生体情報の漏洩は、生体情報の暗号化などにより対策される。しかし、生体認証システムそのものが攻撃者によって偽装された場合、利用者が気づかずに生体情報を入力することで、攻撃者が不正に利用者の生体情報を取得できる恐れがある。
【０００３】
このような問題に対しては、利用者自身が生体認証システム、特に生体情報を入力するセンサ部の正当性を確認できることが必要となる。利用者が生体情報を入力するセンサ部の正当性を確認できる技術の開示はないが、関連する技術として特許文献1および特許文献2がある。
【０００４】
特許文献1には、生体情報に対して、ユーザのみが理解出来る少なくとも１つの暗号を定めておき、ユーザには無作為に選択した暗号だけを提示し、ユーザからその暗号に対応する生体情報を採取して、暗号に対応する生体情報とユーザから採取した生体情報とを照合する事で第三者による不正な認証を防止する技術が記載されている。つまり、特許文献1は、生体情報の偽造によるなりすましを防止することを目的とし、利用者しか知りえない秘密情報の入力と利用者の生体情報の入力を同時に行う技術を開示している。これにより生体情報のみで認証する場合にくらべ、なりすましへの耐性を向上するものである。
【０００５】

特許文献2は、ICカードがICカードリーダライタの正当性を確認し、ICカードの発行部から利用者に知らせる技術を開示している。これにより、攻撃者が偽装した不正なICカードリーダライタに対して、利用者がパスワードのような本人確認用の情報を入力することを防ぐものである。

【０００６】

【特許文献１】特開2005-92697号公報

【特許文献２】特開2005-92788号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかし、特許文献1では、攻撃者がセンサ部を偽装し入力された生体情報を不正に保持するようにした場合でも、システムに保存した秘密情報を利用者に提示して、利用者に生体情報の入力を促す恐れがある。また、生体認証システムが攻撃者によって偽装されている場合に、秘密情報が提示される前に利用者が誤って生体情報を入力する恐れがある。

【０００８】

特許文献2では、ＩＣカードがICカードリーダライタを認証するため、ICカードが必須となる。

【０００９】

本発明は、ＩＣカードを用いなくても、装置の偽装によって利用者の認証情報が第三者に窃取、盗用されるのを抑制する装置及びその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】

【００１０】

本発明の生体情報の不正取得防止方法および装置は、秘密情報が暗号化され、暗号化のための鍵をセンサ部が保持する、さらにセンサ部が秘密情報を復号化する手段および復号化した秘密情報を利用者に提示する手段を持つ。また、センサ部は生体情報の入力部に生体情報が提示されたことを検知する手段を持ち、秘密情報が提示される前に生体情報が提示された場合、利用者に対して警告を発する手段を持つ。

【発明の効果】

【００１１】

本発明によれば、ＩＣカードを用いなくても、装置の偽装によって利用者の認証情報が第三者に窃取、盗用されるのを抑制する効果がある。つまり、本発明では、センサ部が秘密情報を復号化するための復号化鍵を持つことで、センサ自体が攻撃者によって偽装された場合に、利用者の秘密情報を正しく表示できなくするため、利用者がセンサ部の正当性を確認できる効果がある。また、生体認証システムが秘密情報を提示する前に利用者が生体情報を提示した場合に、利用者に警告を発することで、利用者が偽装されたセンサに誤って生体情報を提示する行動を抑制する効果がある。さらに、秘密情報の正当性を検証する手段を有し、秘密情報の正当性が確認された場合のみに秘密情報を提示することで、利用者が偽の秘密情報を誤って自分の秘密情報と認識して、生体情報を提示してしまう行動を抑制する効果がある。

【発明を実施するための最良の形態】

【００１２】

以下、本発明の実施の形態について、PC（パーソナルコンピュータ）およびPCに外付けの生体情報センサから構成される生体認証システムを例に説明する。

【００１３】

図１は、本発明の実施の形態のひとつである生体認証システムの構成を示す。生体認証システムは、利用者が提示する生体情報を取得するための生体情報センサ１００（入力装置）および生体情報センサから得られた生体情報により利用者を認証するPC１３５を備える。ただし本発明の構成を図１に限定するものではない。

【００１４】

生体情報センサ１００は、利用者が提示する生体情報を電子化あるいは画像化する生体

情報取得部１１５（例えば、マイコン）、生体情報取得部１１５に利用者が生体情報を提示したことを検知する生体情報検知部１１０（例えば、スキャナ）、暗号化秘密情報を復号化する復号化部１２５（例えば、コプロセッサ）、復号化のための鍵である復号化鍵１３０、秘密情報の正当性を検証する正当性検証部１２０（例えば、マイコン）、さらに秘密鍵の正当性が検証できた場合に秘密情報を利用者に提示する秘密情報表示部１０５（例えば、ＬＥＤ）、秘密情報が提示される前に生体情報を検知した場合に利用者に警告を発する警告報知部１０７（例えば、スピーカ）を備える。復号化鍵１３０は、記憶装置（例えば、ＥＥＰＲＯＭ）に記憶される。秘密情報表示部１０５は、本実施例では複数（例えば、３種類）の色をそれぞれ任意の時間発光・消灯させることができるものとするが、この限りではない。例えば、秘密情報表示部１０５は、複数のマークを表示してもよい。秘密情報表示部１０５の代わりに、複数の音（メロディ）を出力する出力部あってもよいし、複数の振動を出力する出力部あってもよい。また、本実施例では、警告報知部１０７は警告音を発するものとするが、この限りではない。警告報知部１０７はは、発光体であってもよい。

【００１５】

PC１３５は、処理装置、入力装置、表示装置、記憶装置、メモリ、これらを接続するバスを備えるのが好ましい。PC１３５は、さらに、通信装置を備えてもよい。 PC１３５は、利用者しか知りえない利用者固有の秘密情報を暗号化した暗号化秘密情報１４０、あらかじめ登録された利用者の生体情報であるテンプレート１５０、生体情報センサ１００で得た利用者の生体情報とテンプレートを照合する照合部１４５（処理装置）を備える。暗号化秘密情報１４０及びテンプレート１５０は、記憶装置（例えば、ハードディスク）に記憶される。利用者の生体情報は、利用者によって予め登録されるのが好ましい。利用者の秘密情報は、利用者によって予め登録されてもよいし、ＰＣ140が生成して利用者へ提示すると共に登録してもよい。テンプレート１５０は、利用者ＩＤごとに生体情報を保持するのが好ましい。

【００１６】

図２は、本発明の実施例の概略フローを示す。以下ステップごとに説明する。

【００１７】

生体認証を開始すると、生体情報センサ１００は、その内部の保持部（例えば、レジスタ）に保持した秘密情報フラグを解除する（ステップＳ２０７０）。秘密情報フラグは秘密情報の提示を利用者に対して行ったか否かを判定するフラグであり、解除された状態では、秘密情報を提示していないことを、設定された状態では提示済みであることを示す。また、同時に生体情報センサ１００の生体情報検知部１１０は、生体情報の検知を開始する（ステップＳ２０１０）。

【００１８】

まず、ステップＳ２０７０以降の処理を説明する。復号化部１２５は、ＰＣ１３５に要求してＰＣ１３５の暗号化された秘密情報１４０を読み取り、記憶装置から復号鍵130を読み出し、復号鍵１３０を使用して秘密情報１４０を復号化し、秘密情報を一時的にワークメモリなどに保持する（ステップＳ２０８０）。

【００１９】

図３は、暗号化する前の秘密情報のデータ構造例を示す。暗号化された秘密情報１４０は、秘密情報３００を暗号化することで生成する。秘密情報３００は利用者ID３１０、利用者に提示する発光パターンデータ３２０、利用者IDと発行パターンデータのハッシュ値３３０を含む。利用者ID３１０やハッシュ値３３０は、必須ではない。本実施例では、利用者に提示する秘密情報として発光パターンを用いているが、この限りではない。発光パターンデータは、例えば図３のテーブル３２１のように、発光させる色のIDとその発光時間から構成される。ここで発光色IDが０の場合は消灯状態を意味し、１から３の値はそれぞれの発光色に対応するものとする。ステップＳ２０８０が終了した時点では、秘密情報３００が一時的に保持される。

さらに正当性検証部１２０は、秘密情報３００の利用者ＩＤ３１０および発行パターン

データ３２０から、ハッシュ関数を用いてハッシュ値を生成し（ステップＳ２０９０）、生成したハッシュ値が秘密情報３００のハッシュ値３３０と同一であれば秘密情報は正当であるとして次のステップに進み、それ以外の場合（例えば、一致しない場合）は、処理を終了する（ステップＳ２０９５）。

【００２０】

次に秘密情報表示部１０５は秘密情報３００の発光パターンデータ３２０に従い、３色からなる発光パターンを発光させる（Ｓ２１００）。その後、生体情報センサ１００内の保持部に保持した秘密情報フラグを設定して処理を終了する（ステップＳ２１１０）。尚、発光パターンの正当性は、利用者によって確認される。

【００２１】

ＰＣ135は、秘密情報表示部１０５が発光パターンを発光させた場合に、発光パターンが正当か否かの確認メッセージをＰＣ135の表示装置へ表示し、ＰＣ135の入力装置を介して利用者から発光パターンが正当である旨の入力を受けてもよい。この場合、ＰＣ135は、秘密情報表示部１０５が発光パターンを発光させた場合に、秘密情報表示部１０５から通知を受信し、その通知に応答して確認メッセージを表示し、利用者から発光パターンが正当である旨の入力を受けた場合に。生体情報センサ１００へ通知してもよい。

【００２２】

一方、Ｓ２０１０以降の処理は以下の通りである。生体情報検知部１１０は生体情報を検知した場合、次の処理に進む。それ以外はステップＳ２０１０に戻り処理を繰り返す（ステップＳ２０２０）。

【００２３】

次に生体情報センサ１００はその内部に保持した秘密情報フラグをチェックし、秘密情報フラグが設定されていれば次のステップＳ２０４０に進み、それ以外はステップ２０６０に進む（ステップ２０３０）。秘密情報フラグが設定されている場合、生体情報取得部１１５は生体情報を取得し、取得した生体情報を照合部１４５に送信して（ステップ２０４０）、処理を終了する。秘密フラグが解除されている場合、警告報知部１０７は警報音を発生する（ステップ２０６０）。その後、ステップＳ２０１０へ進み、処理を繰り返す。

【００２４】

照合部145は、生体情報取得部１１５から利用者ＩＤと共に生体情報を受信し、その利用者ＩＤを基にテンプレート150から利用者ＩＤに対する生体情報を読み出し、生体情報取得部１１５からの生体情報をテンプレート150の生体情報と照合する。つまり、生体情報取得部１１５からの生体情報がテンプレート150の生体情報と対応（例えば、一致）するか比較する。照合部145は、両者が対応した場合は、照合成功と判断し、両者が対応しない場合は、照合失敗と判断する。ＰＣ135の処理装置は、照合成功である場合に、利用者からの要求に応じて処理を実行し、照合失敗である場合は。利用者からの要求を拒否する。ＰＣ135の処理装置は、照合成功である場合に、ＰＣ135の利用を許可する。

【００２５】

秘密情報検知部105は、生体情報検知部110に近傍に配置されるのが好ましい。例えば、秘密情報検知部105は、生体情報検知部110の上下左右の何れかに隣接して配置されるのが好ましい。秘密情報は、生体情報ごとではなく、利用者ごと、即ち利用者ＩＤに対応するのが好ましい。つまり、秘密情報は、１人の利用者に１つであるのが好ましい。

【００２６】

尚、ＰＣ135と生体情報センサ100は、一体であってもよい。秘密情報は、ＰＣ135内の記憶装置の代わりに、生体情報センサ100内の記憶装置に記憶されてもよい。秘密情報が生体情報センサ100内の記憶装置に記憶される場合は、暗号化されていなくてもよい。照合部145及びテンプレート150は、ＰＣ135内に配置される代わりに、ネットワークを介してＰＣ135に接続された他のコンピュータ（例えば、サーバ）内に配置されてもよい。

【００２７】

本発明の技術的思想は、ＰＣに限らず、ＡＴＭ（自動現金預払機）や、ロック装置にも

適用可能である。本発明の技術的思想は、生体情報に限らず、暗証番号にも適用可能である。

【産業上の利用可能性】

【００２８】

本発明は、利用者が明示的に生体情報の提示を行うことで利用者認証を行う生体認証システムに適用可能である。例えば、体の一部を生体認証システムに対して提示する動作を伴う生体認証技術、指紋認証、静脈パターン認証、掌形認証などに利用できる。また、利用者の動作を元にした生体認証技術、音声（声紋）認証や動的署名認証などにも利用可能である。また、生体情報の提示に特別な動作を必要としない顔認証のような生体認証技術においても、利用者が明示的に顔の撮影を指示する手段を備えていれば、本発明を利用できる。本発明はこれらの生体認証技術を適用して利用者認証を行う任意のアプリケーションに対して適用可能である。例えば社内ネットワークにおける情報アクセス制御、インターネットバンキングシステムやＡＴＭにおける本人確認、会員向けWebサイトへのログイン、保護エリアへの入場時の個人認証、パソコンのログイン、重要施設や部屋への入退室管理などへの適用が可能である。

【図面の簡単な説明】

【００２９】

【図１】本発明の実施例における生体認証システムの構成例である。

【図２】本発明の実施例における生体認証センサ部の処理フローである。

【図３】本発明の実施例における秘密情報の構成例の図である。

【符号の説明】

【００３０】

１００ 生体情報センサ
１０７ 警告報知部
１０５ 秘密情報表示部
１１０ 生体情報検知部
１１５ 生体情報取得部
１２０ 正当性検証部
１２５ 復号化部
１３０ 復号鍵
１３５ ＰＣ
１４０ 暗号化秘密情報
１４５ 照合部
１５０ テンプレート
３００ 秘密情報
３１０ 利用者ＩＤ
３２０ 発光パターンデータ
３３０ ハッシュ値
３２１ 発光パターンテーブル

【図１】

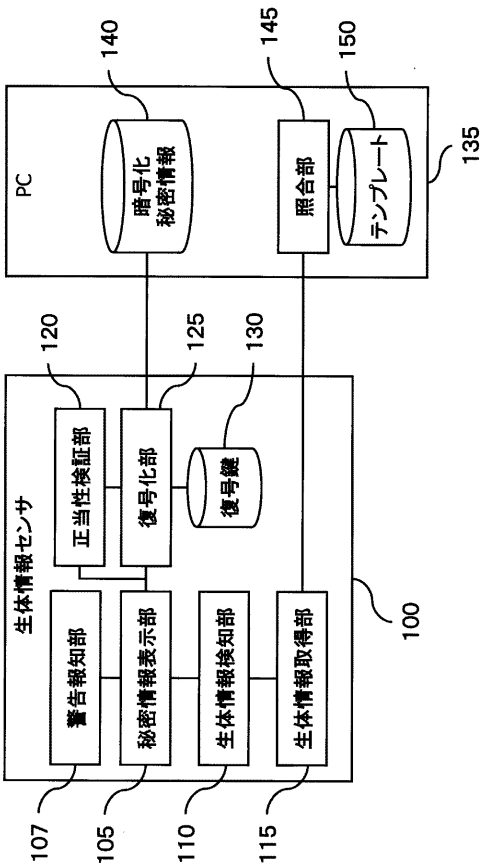

図1

【図２】

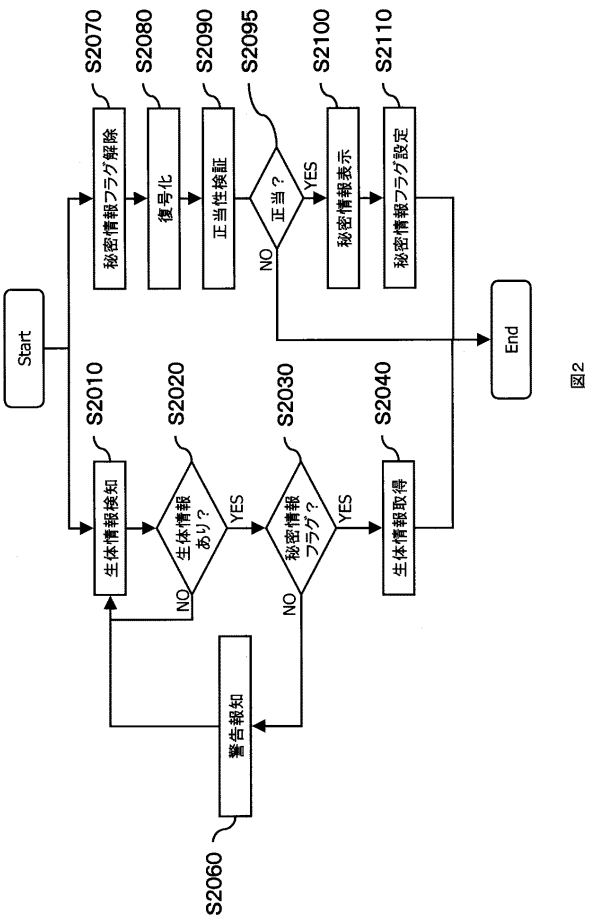

図2

【図３】

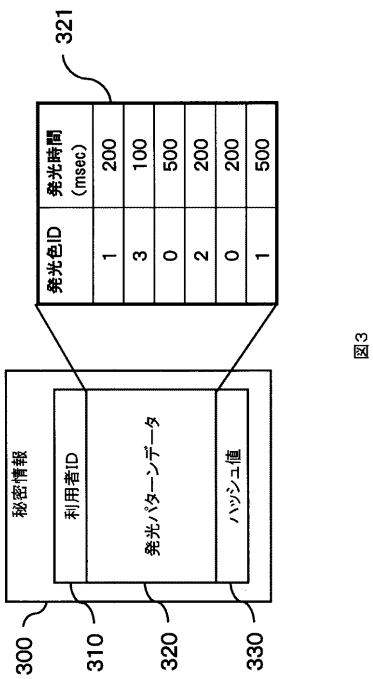

図3